FAKULTÄT FÜR !NFORMATIK

Biometrische Systeme – wie sicher sind sie wirklich?

DIPLOMARBEIT

zur Erlangung des akademischen Grades

Diplom-Ingenieur

im Rahmen des Studiums

Software Engineering/Internet Computing

eingereicht von

Christian Schwarzl
Matrikelnummer 0125494

an der
Fakultät für Informatik der Technischen Universität Wien

Betreuung:
Betreuer: O.Univ. Prof. Dipl.-Ing. Dr. A Min Tjoa
Mitwirkung: Univ.-Ass. Dr. Edgar Weippl

Wien, 19.07.2009

(Unterschrift Verfasser) (Unterschrift Betreuer)

Christian Schwarzl
Franz Pfaringerstraße 9
2486 Pottendorf

„Ich erkläre an Eides statt, dass ich die vorliegende Arbeit selbständig und ohne fremde Hilfe verfasst, andere als die vorliegenden Quellen nicht benützt und die den benutzen Quellen wörtlich oder inhaltlich entnommenen Stellen als solche kenntlich gemacht habe."

Wien, 19.07.2009, Christian Schwarzl

Abstract

The present thesis deals with the security of biometric systems. The goal of the thesis is to question the findings of existing papers and articles which state that it is quite easy to fool fingerprint scanners. Therefore a series of experiments were conducted, where the author tried to fool a fingerprint scanner and thereby to break into the system. In these experiments more than 80 molds were made out of three different materials (Fimo, wax and printed circuit boards). From these molds a total number of 1741 fake fingers were created (with wood glue, silicon, glue and gelatin). With this fake fingers a total of 34820 attempts to log in were conducted. In the concluding chapter the author tries to answer the question raised concerning the security of today's biometric systems on the basis of the collected empirical data. Unlike in most of the existing papers on this topic, the single steps of producing a fake finger and fooling the scanner are explained in every detail in this thesis to assure some kind of reproducibility.

Kurzfassung

Die vorliegende Arbeit beschäftigt sich mit der Sicherheit biometrischer Systeme. Ziel der Arbeit ist es, die vielen Berichte und Arbeiten, welche über die leichte Täuschungsmöglichkeit von Fingerprint-Scannern berichten, kritisch zu hinterfragen. Im Rahmen der Arbeit wird versucht, Fingerprint-Scanner durch Attrappen zu täuschen. Hierfür wurden über 80 Vorlagen aus drei verschiedenen Materialien (Fimo, Wachs und Leiterplatten) hergestellt. Von diesen Vorlagen wurden aus Holzleim, Silikon, Bastelkleber und Gelatine insgesamt 1741 Attrappen erzeugt, mit denen 34820 Einlogversuche durchgeführt und dokumentiert wurden. Die so gesammelten empirischen Daten werden in der Conlusio des Autors interpretiert und es wird versucht, eine Antwort auf die Frage der Sicherheit von gängigen Fingerprint-Scannern zu geben. Im Unterschied zu vielen der bislang existierenden Arbeiten zu diesem Thema werden die einzelnen Schritte des Versuchsablaufes detailliert beschrieben, um eine gewisse Nachvollziehbarkeit zu gewährleisten.

INHALT

1) Einleitung

Immer schon war es den Menschen wichtig, ihren Privatbesitz vor anderen Personen zu schützen. Früher handelte es sich bei den zu sichernden Gütern meist um materielle Besitztümer, wie das eigene Haus, an dessen Zutritt unbefugte Personen gehindert werden sollten. Hierfür reichten meist Schlösser aus. In der heutigen Zeit der Informationsgesellschaft wird die Zahl an zu schützenden Gütern, darunter zunehmend auch nicht materielles Eigentum wie die Daten auf einem Rechner, immer größer. Auch die Technik hat sich entsprechend weiterentwickelt, was ganz neue Möglichkeiten der Zugangsbeschränkung eröffnet, diese jedoch auch nötig macht. Auch wenn alt hergebrachte Systeme der Zugangssicherung wie Schlösser, bei materiellen Gütern, und Passwörtern, bei IT-Systemen, weiterhin nicht ausgedient haben, sind sie mit einem nicht zu verachtenden Nachteil ausgestattet: Das Artefakt, mit dem der Zugang gewährt wird, sei es Schlüssel oder Passwort, kann an eine andere Person weitergegeben werden. Eine Möglichkeit diesem Mangel entgegenzuwirken bilden biometrische Systeme, welche ein personengebundenes Zugangsartefakt, ein biometrisches Merkmal, verwenden, um die Zugangsbefugnis der jeweiligen Person zu überprüfen. Als ein solches Artefakt können all jene (äußerlichen) Charakteristika einer Person herangezogen werden, welche sie als einzigartig auszeichnen. Dies sind, abgesehen von der weithin bekannten DNA-Struktur des menschlichen Genoms, unter anderem Fingerabdrücke, die Iris beziehungsweise Retina des Auges, Gesichts-, Hand- und Fingergeometrie, die Venenstruktur der Hand sowie die Klangfarbe der Stimme. Außer dem beachtlichen Vorteil, dass das Zugangsartefakt biometrischer Systeme personengebunden ist, werden entsprechende Systeme meist für ihre Sicherheit gepriesen. Oft hört man in diesem Zusammenhang, dass die biometrischen Charakteristika eines Menschen gar nicht beziehungsweise nur mit erheblichem Aufwand und entsprechendem Fachwissen zu fälschen sind. Aufgrund der neuen Möglichkeiten, die eine deutlich erhöhte Sicherheit versprechen, tendieren viele Firmen dazu ihre Systeme entsprechend zu verändern beziehungsweise aufzurüsten, um diese Technologien zu nutzen. Durch ständiges Weiterentwickeln ist die Technologie mittlerweile so weit fortgeschritten, dass bereits biometrische Systeme für den Heimgebrauch erstanden werden können. So ist es beispielsweise für Privatanwenderinnen und Privatanwender möglich, ihren Heimrechner mit einem Fingerprint-Scanner zu sichern. Durch die Einfachheit der Verwendung und die versprochene Sicherheit haben sich biometrische Systeme immer weiter verbreitet und finden mittlerweile in allen möglichen Sparten und Branchen Anwendung. Vom modernen Sicherheitsunternehmen bis hin zum Privatgebrauch sind verschiedenste solcher Systeme im Einsatz. Umso interessanter wird damit allerdings die Frage: Wie sicher sind diese Systeme wirklich?
Die Diplomarbeit widmet sich dieser Frage am Beispiel von Fingerabdruck-Scannern, da diese von allen biometrischen Systemen am häufigsten verwendet werden. Es gibt mittlerweile einige Berichte darüber, dass Fingerprint-Scanner durch recht primitive Techniken und Mittel zu überlisten sind (1; 2; 3). Auch wenn die Herangehensweise oder die konkret verwendeten Materialien dieser

Arbeiten sich unterscheiden, haben all diese Arbeiten jedoch eines gemeinsam: Es wird immer nur sehr oberflächlich beschrieben, wie vorgegangen wurde, wobei oft auch der Eindruck entsteht, dass manches durchaus beabsichtigt ungenau beschrieben wird. So werden manche Arbeitsschritte nur durch einen kurzen Satz erwähnt, es wird allerdings nicht genau beschrieben, auf welche Weise vorgegangen wurde beziehungsweise welche Mittel und Geräte verwendet wurden. Dadurch erscheinen manche Phasen viel einfacher und leichter als sie tatsächlich sind. So wird oftmals nur kurz von einer „Nachbearbeitung des Bildes am Computer" gesprochen, es wird jedoch nirgends erwähnt, wie diese konkret aussieht und mit welchen Programmen gearbeitet wurde oder auch wieviel Zeit eine solche Bearbeitung in Anspruch nimmt. Dadurch entsteht natürlich viel mehr der Eindruck, dass das Überlisten eines Fingerprint-Scanners sehr einfach ist.

In dieser Arbeit wird nun untersucht, ob sich die genannten Methoden mit entsprechenden Utensilien von einer praktisch und technisch durchschnittlich begabten Person erfolgreich nachmachen lassen, oder ob diese Berichte, welche zum Teil auch in Zeitschriften abgedruckt wurden, eher eine gewisse Skepsis und Verunsicherung gegenüber biometrischen Systemen unter der Bevölkerung auslösen sollten. Darüber hinaus wird untersucht, ob man durch leichte Abänderungen der Methoden, welche in den Artikeln zu diesem Thema verwendet wurden, oder durch ganz andere Ansätze und Materialien einen Erfolg erzielen kann. Auch wird geprüft, ob ein etwaiger Erfolg vom benutzten Scanner oder der Scanmethode des Gerätes abhängig ist. All diese Versuche finden unter wissenschaftlichen Bedingungen statt und es wird getestet, ob immer mit einem Erfolg zu rechnen ist, ob nur in seltenen Fällen oder ob von einer Methode nie ein positives Ergebnis zu erwarten ist (Nachvollziehbarkeit). Mithilfe all dieser Experimente wird versucht eine Antwort auf die Frage der Sicherheit von biometrischen Systemen (genauer von Fingerprint-Scannern) zu geben. So soll die Conclusio der Arbeit aufzeigen, ob das weitverbreitete Vertrauen in die Sicherheit solcher Systeme gerechtfertigt ist, ob man sich nur zum Teil oder unter bestimmten Bedingungen auf diese Systeme verlassen kann oder ob sie das Vertrauen in sie unter Umständen gar nicht verdienen.

1.1) Lesehinweise

Diese Arbeit richtet sich vornehmlich an ein Zielpublikum mit einer gewissen Vorbildung im Bereich Biometrie beziehungsweise IT Security. Dennoch sollen in Kapitel 2 noch einmal die grundlegenden Begriffe und die Terminologie erläutert werden. Dieses Kapitel soll dem fachkundigen Publikum mehr als allgemeine Information dienen und muss nicht gelesen werden. Zugleich bietet es aber einen Anknüpfungspunkt für Leserinnen und Leser mit weniger bis keinem fachlichen Hintergrundwissen.

In Kapitel 3 werden diverse biometrische Systeme vorgestellt und deren Funktionsweise erläutert. Weiters werden mögliche Angriffspunkte biometrischer Zugangssysteme aufgezeigt. Auch dieses Kapitel ist für Leserinnen und Leser mit einschlägigem Vorwissen lediglich als Wiederholung

zu betrachten und eher für ein Publikum ohne Vorwissen gedacht um einen Einblick in die aktuell verfügbaren Gerätschaften zu geben und ein besseres Verständnis für das Gebiet der Biometrie zu erlangen. Das soll den theoretischen Zugang zum Rest der Arbeit erleichtern.

Kapitel 4 schließlich widmet sich ausführlich dem praktischen Teil dieser Arbeit – den Versuchen, die dieser Arbeit zugrunde liegen. Es wird die Sicherheit von Fingerabdrucksystemen beleuchtet und erläutert, wie versucht wurde, die in den Versuchen verwendeten Scanner zu täuschen und ob dies gelungen ist.

In Kapitel 5 wird aufgezeigt, wieso es wichtig wäre, das aus den Tests gewonnene Wissen an andere Studierende weiterzugegeben, wie diese Informationsweitergabe im Rahmen einer Laborübung durchführbar wäre und welche weiteren Aspekte, außer der bloßen Präsentation der Testergebnisse, den Studierenden mit diesen Laborübungen vermittelt werden könnten.

Im 6. Kapitel werden in der persönlichen Conclusio des Autors die Versuchsergebnisse noch einmal zusammengefasst und bewertet.

2) Grundbegriffe

Bevor man über biometrische Systeme redet, muss zunächst einmal geklärt werden, was man darunter überhaupt versteht, damit man über ein gemeinsames Grundverständnis der Begrifflichkeiten verfügt. Dies wird umso wichtiger, wenn man bedenkt, dass bisher kein genormtes Vokabular für Biometrie existiert. Die Gruppe 1 der ISO/IEC arbeitet noch an einem entsprechenden Dokument (4). Im Folgenden sollen daher die wichtigsten Terminologien erläutert werden.

2.1) Biometrie

Das Wort „**Biometrie**“ (oder auch „Biometrik“) entstand aus den griechischen Wörtern „Bios“ (=Leben) und „Metron“ (=Maß) und bezeichnet somit die Lehre von der Messung beziehungsweise Vermessung von Lebewesen (5; 6). Heute wird allerdings darunter auch „die automatisierte Erkennung von Individuen anhand ihrer verhaltensmäßigen oder biologischen Charakteristika“ verstanden (4).

Ein solches verhaltensmäßiges oder biologisches Charakteristikum wird auch als **biometrisches Charakteristikum** bezeichnet. Genauer versteht man darunter eine Eigenschaft eines Individuums, welche gemessen werden kann (wobei das Messergebnis durch erneute Messung reproduzierbar sein muss) und sich zur Unterscheidung von anderen Individuen eignet. Um als biometrisches Charakteristikum zu gelten, muss eine solche Eigenschaft daher die folgenden fünf Anforderungen erfüllen (5; 7):

- Eindeutigkeit: Die Eigenschaft sollte über eindeutige Merkmale oder Merkmalsmuster verfügen, welche eine Unterscheidung zu anderen Personen erlauben.

- Universalität: Die Eigenschaft sollte bei möglichst vielen Personen vorkommen, sodass die Messung der Eigenschaft an möglichst vielen Individuen möglich ist.

- Konstanz: Die Eigenschaft beziehungsweise die zur Unterscheidung verwendeten Merkmale sollten möglichst keinen zeitlichen Veränderungen unterworfen sein. So sollte eine Person zeit ihres Lebens dieselben Merkmale dieser Eigenschaft aufweisen.

- Messbarkeit: Wie bereits erwähnt, muss die Eigenschaft messbar sein. Dies sollte durch möglichst einfache (technische) Mittel zu bewerkstelligen sein.

- Anwenderinnen-/Anwenderfreundlichkeit: Die Messung der Eigenschaft sollte für die Person, an der sie durchgeführt wird, möglichst bequem und einfach sein.

Die bekanntesten Eigenschaften des Menschen, welche all diese Anforderungen erfüllen und somit als biometrisches Charakteristikum in biometrischen Systemen zum Einsatz kommen können, sind:

- Fingerabdruck
- Gesichtsgeometrie
- Handgeometrie
- Stimme
- Iris
- Retina
- Unterschrift
- DNA

Durch diese Eigenschaften, welche biologisch und/oder verhaltensbedingt sind, können Personen voneinander unterschieden werden. Auf einige dieser Eigenschaften und Methoden wie sie in biometrischen Systemen Anwendung finden wird im weiteren Verlauf der Arbeit noch genauer eingegangen.

2.2) Biometrische Erkennung

Um eine biometrische Erkennung einer Person durchführen zu können, muss diese zunächst die sogenannte **Enrolment**-Phase durchlaufen. Wie das Wort Enrolment (engl. Registrierung/ Einschreibung) bereits andeutet, lernt das System die entsprechende Person in dieser Phase erst kennen, indem es Daten über die jeweilige Person erhält. Dies können beispielsweise Name, Username, Geburtsdatum oder Sozialversicherungsnummer sein. Ob und welche Daten das System benötigt, hängt von der Art und Implementierung der Anwendung ab. Zusätzlich zu diesen Daten wird mithilfe eines Datenerfassungsgerätes ein biometrisches Charakteristikum (oder auch mehrere solcher Charakteristika) dieser Person aufgezeichnet. Dies geschieht je nach Art des Charakteristikums durch eine Kamera, eine Tastatur oder aber durch einen Sensor. Die durch das entsprechende Gerät erfassten Daten werden auch **biometrisches Sample** genannt. Es handelt sich bei einem solchen Sample also um die (analoge oder digitale) Darstellung des jeweiligen biometrischen Charakteristikums. Wie bereits im vorigen Kapitel erwähnt, besitzt jedes biometrische Charakteristikum bestimmte Merkmale, mit deren Hilfe verschiedene Personen unterschieden werden können. Diese Merkmale werden im nächsten Schritt des Enrolments aus dem biometrischen Sample extrahiert (7). Die somit erhaltenen Daten werden als **biometrische Referenz** der jeweiligen Person abgespeichert und können fortan zur biometrischen Erkennung der Person verwendet werden.

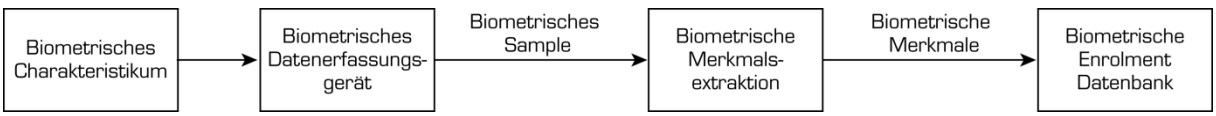

Abbildung 1: typischer interner Enrolment-Ablauf (5)

Sobald eine Person die Enrolment-Phase hinter sich hat, ist sie registriert und wird somit vom System erkannt. Um sich nun an einem biometrischen Erkennungssystem zu authentifizieren, muss die Person eine ähnliche Prozedur wie beim Enrolment durchlaufen. Dem System muss an geeigneten Datenerfassungsgeräten das geforderte biometrische Charakteristikum präsentiert werden. Dieses wird wieder als biometrisches Sample erfasst, aus welchem wiederum die biometrischen Merkmale extrahiert werden. Nun kommt der entscheidende Schritt, welcher einen Authentifizierungsablauf vom Enrolment unterscheidet. Da die Person bereits am System registriert ist, verfügt dieses bereits über ein entsprechendes biometrisches Template, die beim Enrolment gespeicherte biometrische Referenz. Um nun zu entscheiden, ob ein Individuum authentifiziert wird oder nicht, werden nun die vom Sample extrahierten Merkmale mit allen gespeicherten Templates verglichen und die Person wird anschließend, je nachdem ob eine Übereinstimmung gefunden wurde oder nicht, authentifiziert (8).

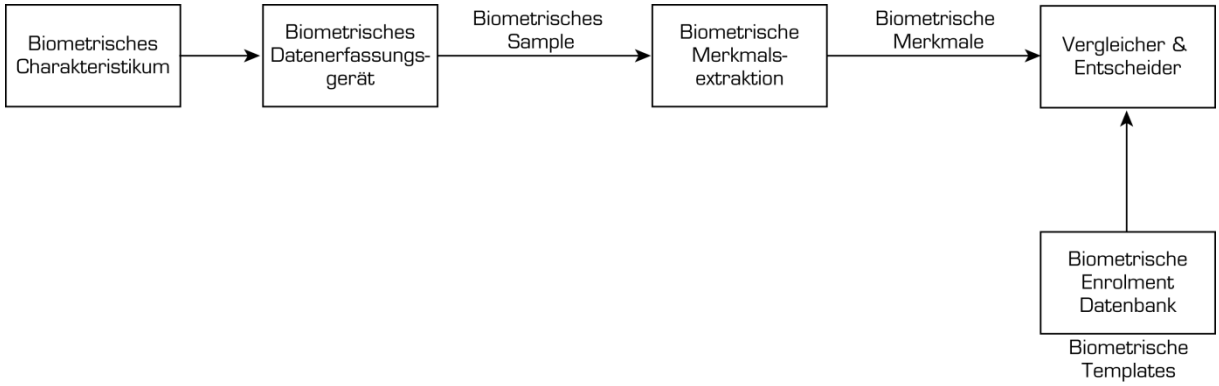

Abbildung 2: typisches biometrisches Erkennungssystem (5)

Grundsätzlich kann man drei Arten von Authentifizierung unterscheiden (5; 9):

- Biometrie „Wer bin ich“: Hier erfolgt die Verifikation durch biometrische Charakteristika, von denen vorausgesetzt wird, dass sie eindeutig sind.

- Geheimes Wissen „Was weiß ich“: Dies sind üblicherweise die bereits erwähnten Passwörter oder PIN-Codes. Die Identität einer Person wird dadurch verifiziert, dass sie über dieses geheime Wissen verfügt. Hierbei wird natürlich davon ausgegangen, dass tatsächlich nur die gewünschte Person über das Wissen verfügt.

- Persönlicher Besitz „Was habe ich“: Bei diesem Verfahren wird die Person dadurch verifiziert, dass sie über einen bestimmten Gegenstand (ein Artefakt) verfügt. Dies kann beispielsweise ein Schlüssel, ein Ausweis oder eine Chipkarte sein.

Wie leicht zu erkennen ist, hat die erste Variante (Biometrie) einen gravierenden Vorteil gegenüber den anderen beiden: Sowohl geheimes Wissen als auch ein Gegenstand, der zur Verifikation dient, können an eine andere Person weitergegeben werden, wodurch das System leicht kompromittiert werden kann. Ein biometrisches Charakteristikum hingegen ist

personengebunden und kann nicht einfach an eine andere Person weitergegeben werden (10).

Da jedoch nicht ausgeschlossen werden kann, dass über kurz oder lang Methoden gefunden werden, oder bereits existieren, mit deren Hilfe auch biometrische Systeme getäuscht werden können, werden heute zumeist sogenannte „Kombinationsverfahren“ verwendet, welche mehrere der drei genannten Verifikationsarten kombinieren. Ein typisches Beispiel dafür ist die Bankomatkarte. Um Geld abzuheben, muss man sowohl über die Karte selbst (persönlicher Besitz) als auch über den zugehörigen PIN-Code (geheimes Wissen) verfügen.

Genauer betrachtet besteht eine solche Authentifizierung daher oft aus zwei Phasen, der Identifizierung und der Verifizierung, wobei das biometrische Charakteristikum normalerweise nur in einer der beiden Phasen, welche im Folgenden kurz erläutert werden, Anwendung findet (5).

2.2.1) Identifizierung

In der Phase der Identifizierung verwendet die Person einen sogenannten Identifikator, um dem System mitzuteilen, wer sie ist. Ein solcher Identifikator ist in den meisten Fällen ein einfacher Username, der es dem System erleichtert, die anschließende Verifizierung durchzuführen. Meistens wird der Identifikator als öffentlich betrachtet, was bedeutet, dass er mehreren Personen bekannt sein kann (5).

Es ist jedoch auch möglich ein biometrisches Charakteristikum zu verwenden (beispielsweise Fingerabdruck oder Retinamuster), um eine Person zu identifizieren. Dies ist allerdings nur dann sinnhaft, wenn die Menge der gespeicherten biometrischen Templates gering ist, da bei einem biometrischen Identifikator die extrahierten Merkmale gegen alle gespeicherten Templates abgeglichen werden müssen. Wird ein biometrisches Charakteristikum zur Identifizierung verwendet, ist es weiters sehr wichtig, dass die Falschakzeptanzrate (siehe Kapitel 2.3.1) möglichst niedrig ist. Viel eher kommt ein biometrisches Charakteristikum daher in der nächsten Phase der Authentifizierung, der Verifizierung, zum Einsatz (5).

2.2.2) Verifizierung

Im zweiten Schritt der Authentifizierung muss ein System noch überprüfen, ob eine Person, welche ihre Identität bereits durch ihren Identifikator bekannt gegeben hat, auch über den sogenannten Verifikator verfügt. Dieser wird üblicherweise als geheim eingestuft, wobei die bekanntesten Beispiele für einen solchen Verifikator wohl das Passwort und der PIN-Code sind (5). Aber auch in dieser Phase kann ein biometrisches Charakteristikum zum Einsatz kommen. So kann eine bereits identifizierte Person, ein solches Charakteristikum als Verifikator benutzen, um dem System zu beweisen, dass man auch die Person ist, welche man vorgibt, zu sein. Es muss daher, um authentifiziert zu werden, jeweils ein Identifikator mit dem dazu passenden Verifikator präsentiert werden.

Im Falle eines biometrischen Charakteristikums als Verifikator muss natürlich darauf geachtet werden, dass es sich dabei um „geheimes Wissen“ handelt, wodurch nicht alle biometrischen Charakteristika sinnvoll zu diesem Zweck eingesetzt werden können. So wäre beispielsweise davon abzuraten, Gesichtsgeometrie zur Verifizierung der Identität zu verwenden, da dieses Charakteristikum für viele Leute zugänglich ist (beispielsweise durch Fotos). Soll dennoch ein solches Charakteristikum als Verifikator eingesetzt werden, ist speziell darauf zu achten, dass das System über eine gute Fälschungserkennung verfügt, um das Original von etwaigen Kopien unterscheiden zu können (5).

Es können jedoch auch beide Phasen zusammengelegt werden, wobei der Identifikator zugleich als Verifikator verwendet wird. Ein Beispiel wäre der Zugang zu bestimmten Räumlichkeiten eines Gebäudes mittels Keycard. Das System prüft in diesem Fall nur, ob die Besitzerin/der Besitzer der benutzten Keycard berechtigt ist, den gewünschten Raum zu betreten (Verifikation) und setzt implizit die Identität der Benutzerin/des Benutzers mit der Keycard voraus. Hier zeigt sich die genannte Schwäche eines solchen Systems, da die Keycard von jedem benutzt werden kann, der sie in die Hände kriegt.

Auch bei biometrischen Erkennungssystemen ist eine solche „Einphasenauthentifizierung“ denkbar. So ist es beispielsweise vorstellbar, und mittlerweile auch durchaus gebräuchlich, dass sich eine Person allein mithilfe des Fingerabdrucks an einem System authentifiziert. In diesem Fall wird zunächst geprüft, ob ein entsprechendes biometrisches Template gespeichert ist. Trifft dies zu, kann die Person dadurch identifiziert werden (Identifikator) und zugleich hat sie durch den Fingerabdruck den zugehörigen Verifikator geliefert, wodurch sie authentifiziert wird. Auch wenn diese Variante bereits durch die Art der Authentifizierung sicherer ist als das erste Beispiel, ist von solchen Systemen abzuraten.

Aus Sicherheitsgründen ist daher auch ein sogenanntes „Mehrfaktorensystem“ denkbar und auch durchaus sinnvoll (11). Hierbei wird eine Person erst dann authentifiziert, wenn sie dem System eine Reihe von Verifikatoren präsentiert hat. Hierbei können mehrere biometrische Merkmale zur Verifizierung dienen oder aber die Verifizierung basiert auf einer Mischung aus biometrischen und nicht biometrischen Verifikatoren (9; 12; 13; 7). So wäre es zum Beispiel auch denkbar, eine Person erst dann zu authentifizieren, wenn sie sowohl über eine Keycard, den zugehörigen PIN-Code und den korrekten Fingerabdruck verfügt. Obwohl das System dadurch sicherer ist, wird diese Sicherheit durch einen gewissen Mehraufwand bei der Authentifizierung erreicht. Daher muss man sich die Frage stellen, ob ein solcher Mehraufwand gerechtfertigt ist. Dies hängt natürlich stark von den durch das System geschützten Daten beziehungsweise Objekten ab.

2.3) Messgrößen biometrischer Systeme

Um die Leistungsfähigkeit eines Systems anzugeben und einen gewissen Vergleich zwischen verschiedenen Produkten zu ermöglichen, bedarf es festgelegter Richt- und Messgrößen. Bei biometrischen Systemen wird die Leistungsfähigkeit in der Regel durch die im Folgenden vorgestellten Vergleichsgrößen gemessen.

2.3.1) Falschakzeptanzrate (FAR)

Eine der wichtigsten Größen bei biometrischen Systemen, welche auch im Zusammenhang mit der durch dieses System gewährleisteten Sicherheit steht, ist die sogenannte Falschakzeptanzrate (FAR = False Acceptance Rate). Diese gibt an, mit welcher Häufigkeit nicht berechtigte Personen als berechtigt akzeptiert werden und somit Zugang zum System erlangen (5). Da dies im Hinblick auf Systemintegrität und Systemsicherheit eines der schwerwiegendsten Probleme darstellt, ist deren Aussagekraft von großer Bedeutung.

2.3.2) Falschrückweisungsrate (FRR)

Ähnlich wichtig wie die Falschakzeptanzrate ist die Falschrückweisungsrate (FRR = False Rejection Rate). Sie bildet faktisch die genaue Umkehrung der FAR und gibt an, mit welcher Häufigkeit einer berechtigten Person kein Zugang/Zugriff gewährt wird (5). Im Gegensatz zur FAR ist die False Rejection-Rate in der Regel nicht so sicherheitskritisch. Zwar wird es oftmals als lästig empfunden, wenn ein biometrisches Charakteristikum nicht auf Anhieb akzeptiert wird, es führt allerdings nicht zu einem kompromittierten Systemzustand.

2.3.3) Falschidentifikationsrate (FIR)

Die Falschidentifikationsrate (FIR = False Identification Rate) gibt die Häufigkeit an, mit welcher ein biometrisches Charakteristikum zwar erkannt, jedoch der falschen Person zugeordnet wird (5). Dieser Fehler kann natürlich nur bei Systemen auftreten, welche ein biometrisches Charakteristikum als Identifikator verwenden. Auch ist zu beachten, dass die FIR in Zusammenhang mit der Anzahl der gespeicherten biometrischen Referenzen steht. Diese Größe ist somit nur bedingt ein Indikator für ein mögliches Sicherheitsrisiko, da im Unterschied zur FAR keine nicht berechtigte Person ins System gelassen wird, sondern lediglich die Identität der Person falsch erkannt wird. Natürlich kann es dadurch auch zu gewissen Sicherheitsverletzungen innerhalb des Systembetreibers kommen, da beispielsweise Personen, die mit wenig Rechten ausgestattet sind, irrtümlicherweise als Personen mit erweiterten Berechtigungen erkannt werden können.

2.3.4) Nutzerausfallrate (FTE bzw. FER)

Die Nutzerausfallrate (FTE = Failure to Enrol, FER = Failure to Enrol Rate) fällt nur bei der Enrolment-Phase ins Gewicht. Sie gibt den Anteil an Personen an, welche nicht enrolt werden können, wobei es nicht auf den Grund für das fehlgeschlagene Enrolment ankommt (5).

2.3.5) Failure to Aquire (FTA)

Wird eine Person vom System abgelehnt, wirkt sich dies auf die bereits erwähnte FRR aus. Es kann jedoch auch ein so genannter „Failure to Aquire" Fehler vorliegen. Dies ist dann der Fall, wenn ein Charakteristikum aus irgendeinem Grund temporär nicht korrekt erkannt wird (5). Dies wäre bei Fingerprint-Scannern beispielsweise denkbar, wenn die Scanneroberfläche verschmutzt ist oder wenn der entsprechende Finger der Person temporär verändert ist, beispielsweise durch eine flächige Wunde oder durch einen Verband.

2.3.6) Equal Error Rate (EER)

Ein weiteres wichtiges Merkmal, welches die Sicherheit eines biometrischen Systems beschreibt, ist die „Equal Error Rate" (ERR). Die Wahrscheinlichkeit einer Falschrückweisung und einer Falschakzeptanz werden abhängig von einem Schwellwert grafisch dargestellt. Dieser Schwellwert gibt an, wie stark die Ähnlichkeit beziehungsweise die Übereinstimmung zweier biometrischer Samples sein muss, um als gleich angesehen zu werden. An einem gewissen Punkt kreuzen sich dabei die beiden Kurven der FAR und der FRR. Dieser Punkt ist die Equal Error Rate und wird aufgrund seines Zustandekommens auch Crossover Error Rate (CER) genannt (14; 5). Je niedriger der Wert für ein bestimmtes System ausfällt, umso sicherer ist dieses einzuschätzen. Somit bildet diese Messgröße eine gute Basis für einen Vergleich verschiedener Systeme bezüglich deren Sicherheit.

3) Biometrische Systeme

In den folgenden Kapiteln sollen verschiedene biometrische Systeme vorgestellt werden, welche mit heutigem Stand der Technik eingesetzt werden können. Hierzu soll zunächst noch darauf eingegangen werden, welche Arten von biometrischen Merkmalen existieren und wodurch sie sich unterscheiden. Es soll erklärt werden, welche Systeme es gibt, wie diese funktionieren und auf welches Charakteristikum sie aufbauen.

3.1) Merkmaltypen biologischer Charakteristika

Wie bereits in Kapitel 2.1 beschrieben, gibt es fünf Kriterien, welche eine Eigenschaft erfüllen muss, um als biometrisches Charakteristikum infrage zu kommen (Eindeutigkeit, Universalität, Konstanz, Messbarkeit und Anwenderinnen-/Anwenderfreundlichkeit). Die Charakteristika selbst unterscheiden sich von Person zu Person, weil sich ihre Merkmale, welche gemessen werden können, unterscheiden. Welche Merkmale bei den einzelnen biometrischen Charakteristika hierbei verwendet werden, kann der folgenden Tabelle entnommen werden:

Biometrisches Charakteristikum	Beschreibung der Merkmale
Fingerprint	Fingerlinienbild, Porenstruktur
Gesichtsgeometrie	Abstände der gesichtsbestimmenden Merkmale (Augen/Nase/Mund)
Iris	Irismuster
Retina	Augenhintergrund (Muster der Adernstruktur)
Handgeometrie	Maße der Finger und des Handballens
Fingergeometrie	Fingermaße (Länge, Breite)
Venenstruktur der Hand	Venenstruktur der Finger, der Handrückenfläche oder der Handinnenfläche
Stimme	Klangfarbe
DNA	Codierung der DNA als Träger der Erbanlagen
Tastenanschlag	Rhythmus des Tastenanschlages
Unterschrift	Schriftzug mit Druck- und Geschwindigkeitsverlauf

Tabelle 1: Merkmale biometrischer Charakteristika (5)

Auch die Entstehung der Merkmale kann unterschieden werden. So gibt es genau genommen drei Entstehungsarten von Merkmalen (5):

- genotypisch: Das Merkmal wird vererbt.
- randotypisch: Das Merkmal entsteht durch Zufallsprozesse in der Frühphase der embryonalen Entwicklung.
- konditioniert: Das Merkmal wird antrainiert.

In der Regel wird jedes Merkmal von allen drei Faktoren bestimmt, allerdings kommt je nach Merkmal den Entstehungsarten eine unterschiedliche Gewichtung zu. Inwiefern die einzelnen Merkmale von den drei Entstehungsarten beeinflusst werden, zeigt die folgende Tabelle (x ist niedrig, xxx hoch):

biometrisches Charakteristikum	genotypisch	randotypisch	konditioniert
Fingerprint	x	xxx	x
Gesichtsgeometrie	xxx	x	x
Irismuster	x	xxx	x
Retina (Blutgefäßstruktur)	x	xxx	x
Handgeometrie	xxx	x	x
Fingergeometrie	xxx	x	x
Venenstruktur der Hand	x	xxx	x
Stimme	xxx	x	xx
DNA	xxx	x	x
Tastenanschlag	x	x	xxx
Unterschrift	xx	x	xxx
Vergleich: Passwort			xxx

Tabelle 2: Entstehungsarten biometrischer Merkmale (5)

Die Entstehungsart eines biometrischen Charakteristikums hat einen gewissen Einfluss auf die Brauchbarkeit und Sicherheit des Merkmals. So ist zu beachten, dass sich rein genotypische Charakteristika beispielsweise nicht zur Unterscheidung von Zwillingen eignen. Rein konditionierte Charakteristika wiederum sind durch die einfache Möglichkeit der Nachahmung als weniger sicher zu erachten. Um den Anspruch der Einmaligkeit gerecht zu werden, sind randotypische Anteile unverzichtbar, da nur so zu gewährleisten ist, dass selbst eineiige Zwillinge unterschieden werden können (5).

Aufgrund der Entstehungsart eines Charakteristikums kann man jedoch nicht ableiten, welche biometrischen Systeme „gut“ und welche „schlecht“ sind. Es muss immer betrachtet werden, zu welchem Zweck das System eingesetzt wird und was damit geschützt werden soll. Konkret müssen in einem solchen Fall vier Punkte genauer betrachtet werden (5):

- Komfort: Wie anwenderfreundlich ist das System, wie lange dauert die Erkennung und wie hoch ist der Aufwand für die Nutzer.

- Genauigkeit: Welche Fehlerraten weist das System auf (FAR, FRR).

- Verfügbarkeit: Wie groß ist die potenzielle Nutzergruppe, die über ein entsprechendes Charakteristikum verfügt.

- Kosten: Wie teuer ist die Anschaffung und Instandhaltung eines entsprechenden Gerätes.

Nur wenn man all diese Kriterien betrachtet, kann man feststellen, ob sich ein bestimmtes System für einen gegebenen Anwendungszweck eignet (15). So ist die menschliche DNA als Charakteristikum zwar sehr zuverlässig (Genauigkeit) und hat eine unschlagbare Verfügbarkeit (jeder Mensch hat seine DNA), es bedarf allerdings einer gewissen Mitwirkung der Benutzerin/des Benutzers, um an die DNA zu gelangen (geringer Komfort), und die Kosten um DNA-Analysen durchzuführen, sind auch erheblich. Auch dauert die Analyse eines DNA-Samples, mit den heute zur Verfügung stehenden Methoden, viel zu lange um die DNA als Identifikator oder Verifikator für biometrische Systeme interessant zu machen. Somit stellt die DNA zwar ein sehr sicheres Charakteristikum dar, wird aber wohl kaum als Zugangssicherung von Räumen oder Computersystemen Verwendung finden.

3.2) Iriserkennung (Iris-Recognition)

Wie bereits aus „Tabelle 2: Entstehungsarten biometrischer Merkmale“ abgelesen werden kann, ist die Iris ein stark randotypisches Merkmal. Ihre Entwicklung setzt bereits im dritten Monat der Schwangerschaft ein und ist bereits im achten Schwangerschaftsmonat abgeschlossen. Lediglich die Pigmentation kann sich noch bis zur Vollendung des ersten Lebensjahres ändern (16; 17). Durch die stark dem Zufall unterworfenen Entwicklung der Iris weisen auch eineiige Zwillinge unterschiedliche Irismuster auf (7). Selbst das linke und rechte Auge einer Person unterscheiden sich in den Merkmalen der Iris.

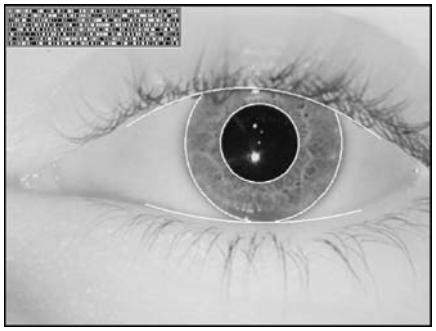

Abbildung 3: Iris-Recognition (9)

Der Ablauf der Iriserkennung wird oft als recht einfach angesehen, da scheinbar „nur“ ein Foto vom Auge einer Person gemacht wird. Tatsächlich verstecken sich aber hinter der Einfachheit komplexe Algorithmen wie jener von John Daugman, einem Professor an der Cambridge University, dessen Algorithmus „Iriscode“ heute von nahezu allen kommerziellen Iriserkennungssystemen eingesetzt wird (18; 19). Dank dieser Algorithmen gibt es nur wenige Bedingungen, die für eine korrekte Iriserkennung gegeben sein müssen. So darf die Kamera, mit der das Auge der zu erkennenden Person aufgenommen wird, nicht weiter als einen Meter vom Auge entfernt sein. Viele andere Faktoren spielen mittlerweile kaum noch eine Rolle. So ist es für einen erfolgreichen Vergleich eines Samples mit den gespeicherten Templates beispielsweise unerheblich, wie groß die Iris auf dem Bild abgebildet und wo sie positioniert ist. Auch kann eine unterschiedliche Ausrichtung der Iris (Diese

wird durch die Position des Kopfes beeinflusst.) ausgeglichen werden. Zudem spielt es bei den meisten Systemen keine Rolle mehr, ob die Person, deren Auge erfasst wird, eine Brille oder Kontaktlinsen trägt.

Bei der Erfassung eines Irismusters werden zunächst der innere und äußere Rand der Iris ermittelt. Die Größe der Pupille, welche sich je nach gegebener Beleuchtung ändert, spielt hierbei keine Rolle, da die Iris nicht von der Pupille verdeckt wird, sondern sich lediglich zusammenzieht. Um dies zu kompensieren, werden positionsbezogene Merkmale nicht in kartesischen Koordinaten sondern in Polarkoordinaten gespeichert, wobei der Irisradius, der Abstand zwischen innerem und äußerem Irisrand ist und Werte zwischen 0 und 1 annimmt. Dadurch ist gewährleistet, dass die Größe der Pupille beziehungsweise Iris und somit die Lichtverhältnisse bei der Erfassung der Iris keine Rolle spielen (17; 16). Einzig die Augenlider und Wimpern können bei der Erfassung eines korrekten Iris-Samples störend Einfluss nehmen, da sie die Iris zum Teil verdecken. Allerdings spielen auch diese Einflüsse bei den meisten Systemen nur noch eine vernachlässigbare Rolle.

Neben der randotypischen Entwicklung der Iris und der großen Unabhängigkeit der Erfassung von Irismustern von äußerlichen Einflüssen ist auch die Geschwindigkeit der Verarbeitung und des Vergleiches von Iris-Templates ein Grund dafür, dass die Iris-Recognition zu den zuverlässigsten und sichersten biometrischen Systemen zählt. So können bereits mit einem 300-MHz-Rechner rund 100.000 Vergleiche pro Sekunde durchgeführt werden (16). Ein Iris-Scan ist somit eines jener biologischen Charakteristika, welche auch als Identifikator eingesetzt werden können, da selbst der Vergleich des Samples mit einer großen Template-Datenbank schnell erfolgen kann.

Die Iris-Recognition hat keine Nachteile an sich, es gibt jedoch wie auch bei allen anderen biometrischen Systemen Kritikpunkte. So gibt es vielfach die Befürchtung, dass mit den erfassten Daten Missbrauch getrieben werden könnte. Diese Befürchtungen sind allerdings insofern unbegründet, da beim Einlesen der Iris lediglich eine Bitdarstellung der Merkmale der Iris gespeichert wird und keinerlei Information über das restliche Auge. Auch können die gespeicherten Daten nicht wieder in ein konkretes Bild umgewandelt werden. Hierbei ist weiters anzumerken, dass die Fotos, die von der Iris gemacht werden, lediglich Schwarz-Weiß-Fotografien sind, da die Augenfarbe nicht als Irismerkmal herangezogen wird, sondern lediglich die diversen Irismuster wie Corona, Krypten, Fasern, Flecken, Narben, radiale Furchen und Streifen (20).

3.3) Retina Erkennung (Retina-Scan)

Beim Retina-Scan dient wie auch schon bei der Iris-Recognition das Auge als biometrisches Charakteristikum. Diesmal wird jedoch die Blutgefäßstruktur im Augenhintergrund als Merkmal herangezogen. Diese ist wie das Irismuster ein vorwiegend randotypisches Merkmal.

Beim Retina-Scan wird der Augenhintergrund mit Infrarotlicht ausgeleuchtet. Da die Blutgefäße dieses Licht stärker reflektieren als der Rest des Auges, entsteht ein charakteristisches Bild, in dem die Intensität des reflektierten Lichts von einem Scanner erfasst wird (8).

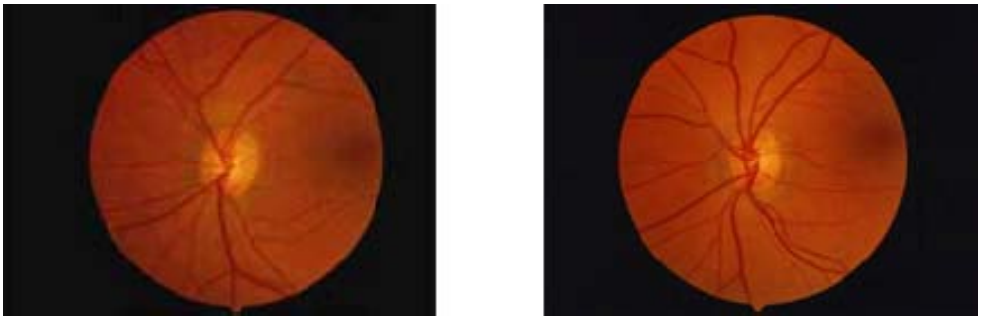

Abbildung 4: Retina-Scan des linken Auges von eineiigen Zwillingen (13)

Ein Vorteil des Retina-Scans liegt auch in der Konstanz der Blutgefäßstruktur, welche sich nur selten (beispielsweise durch entsprechende Kopfverletzungen) ändert. Auch gilt die Retina als sehr fälschungssicher, da es zum einen schwierig ist ein entsprechendes Sample zu erlangen und zum anderen kaum möglich ist, ein passendes künstliches Auge nachzuformen. Durch den randotypischen Merkmalsanteil sind auch die Retina-Scans von eineiigen Zwillingen unterschiedlich (siehe „Abbildung 4: Retina-Scan des linken Auges von eineiigen Zwillingen (13)“). Ein weiterer Vorteil des Retina-Scans liegt in der sehr niedrigen False Acceptance Rate von Retina-Scannern (21).

Es gibt allerdings auch eine Reihe von Nachteilen, die der Retina-Scan mit sich bringt. So sind beispielsweise die Erfassungsgeräte sehr teuer. Ein weiterer Nachteil und zugleich ein Unterschied zur Iris-Recognition liegen darin, dass das Auge der Person, die identifiziert werden soll, nur wenige Zentimeter von der Kamera entfernt sein darf. Dies führt bei vielen Personen zur Ablehnung des Verfahrens, da sie sich unwohl dabei fühlen so nahe an das Gerät herantreten zu müssen (7). Auch darf beim Einlesen des Samples keine Brille getragen werden. Eine weitere Unannehmlichkeit ergibt sich dadurch, dass während des Scanvorgangs, der ein paar Sekunden dauern kann, der Kopf möglichst ruhig gehalten werden muss und die Augen ständig auf einen bestimmten Punkt fixiert sein müssen (22; 8; 23).

3.4) Handgeometrie

Ein biometrisches Charakteristikum, welches durch eine recht wörtliche Übersetzung des Begriffs Biometrie erfasst wird, bildet die Handgeometrie. Hierbei muss die Hand auf eine Auflagefläche in einer vorgegebenen Position platziert werden. Anschließend wird die Hand vermessen, indem am Bild der Hand an vordefinierten Positionen (beispielsweise Fingerspitzen) Messpunkte aufgetragen werden. Durch die Abstandsmessung zwischen diesen Punkten werden die Länge und die Breite der einzelnen Finger so wie der ganzen Hand erfasst (7). Auch werden in der Regel über entsprechende Spiegel die Hand- und Fingerdicke gemessen. Die Summe dieser Abstände, Längen-, Breiten- und Dickenmessungen dient zur Unterscheidung von Personen (24).

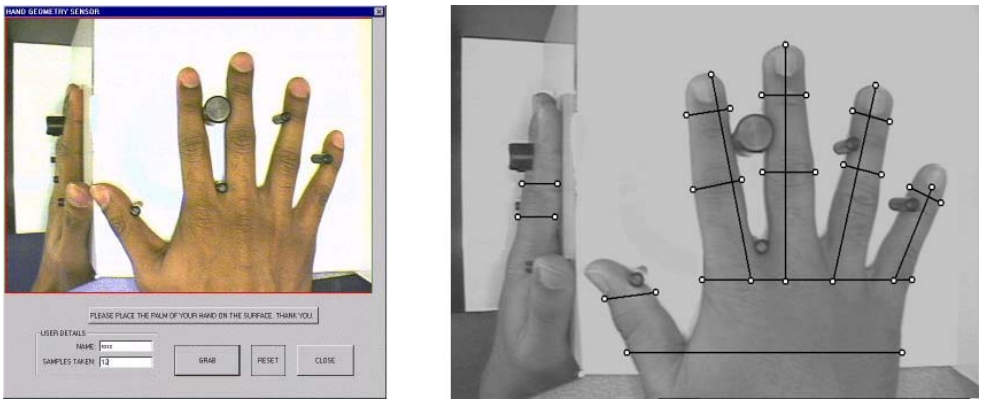

Abbildung 5: richtiges Auflegen und Vermessen der Hand (18)

Es handelt sich bei der Handgeometrie um ein relativ einfaches und benutzerinnen-/benutzerfreundliches Verfahren (8), da die Erfassung sehr schnell erfolgen kann und die Person, deren Daten erfasst werden sollen, lediglich kurz ihre Hand auf das Gerät auflegen muss. Hierdurch entsteht aber zugleich einer der größten Kritikpunkte an diesem biometrischen System. Die Erfassung der Merkmale kann im Gegensatz zu vielen anderen Methoden (wie beispielsweise Iris-, Face- und Voice-Recognition) nicht kontaktlos erfolgen. Somit kann sich ein gewisses hygienisches Problem ergeben, wenn die Auflageflächen nicht oft entsprechend gereinigt werden. Ein weiterer Nachteil ist die hohe FAR, sodass entsprechende Geräte nicht für Hochsicherheitsanwendungen geeignet sind. Außerdem können Alter, Verletzungen und Verschmutzung leicht zu einer falschen Rückweisung von Personen führen (25).

3.5) Gesichtserkennung (Face-Recognition)

Der Mensch verwendet ständig Gesichtserkennung um seine Freunde, Verwandten und Bekannten voneinander zu unterscheiden. Bei der Implementierung von Face-Recognition Systemen wird nun versucht Computersystemen auch die Möglichkeit zu geben Personen aufgrund ihrer Gesichtsstrukturen zu unterscheiden.

Als charakteristische Gesichtsmerkmale gelten bei der Face-Recognition Kinn, Nase, Mund, Augen und Stirn. Die Schwierigkeit bei der Gesichtserkennung ergibt sich dadurch, dass diese Merkmale nicht statisch sind und deren korrekte Erfassung durch Mimik, Make-up, Sonnenbrillen (und zum Teil auch optischen Brillen) aber auch durch Bartwuchs verhindert werden kann (24). Natürlich spielen auch unterschiedliche Lichtverhältnisse eine entscheidende Rolle für Gesichtserkennungssysteme. Daher mussten Wege gefunden werden, wie ein solches System bei der Analyse eines Bildes die veränderlichen Merkmale extrahieren und sich beim Vergleich mit den gespeicherten Templates auf unveränderliche Merkmale stützen kann.

Heute werden bei der Gesichtserkennung vor allem zwei Verfahren eingesetzt, welche im Folgenden kurz beschrieben werden (24).

3.5.1) „Eigen-Faces“- Methode

Die „Eigen-Faces“- Methode wurde bereits 1991 von Matthew Turk und Alex Pentland vorgestellt (26; 27). Bei dieser Methode wird das gescannte Gesicht durch die Kombination gespeicherter sogenannter Basisgesichter nachgebildet (Eine solche Kombination besteht aus ca. 100 – 125 dieser Basisgesichter). Beim Enrolment werden in der Datenbank die Abweichungen des Gesichtes der gewünschten Person gespeichert. Soll nun ein Vergleich stattfinden, wird das gescannte Bild ebenfalls nachgebildet, die Abweichungen des Bildes von den Basisbildern festgestellt und mit den in der Datenbank gespeicherten Werten verglichen (26).

Dieses Verfahren ist leider sehr anfällig in Bezug auf den Blickwinkel der Person zur Kamera und auf die Lichtverhältnisse (8). So hängt die Zuverlässigkeit der Methode stark von den beiden genannten Punkten ab, sodass nur dann wirklich gute Ergebnisse erzielt werden, wenn die gescannte Person möglichst direkt in die Kamera blickt und wenn gute Lichtverhältnisse gegeben sind (26).

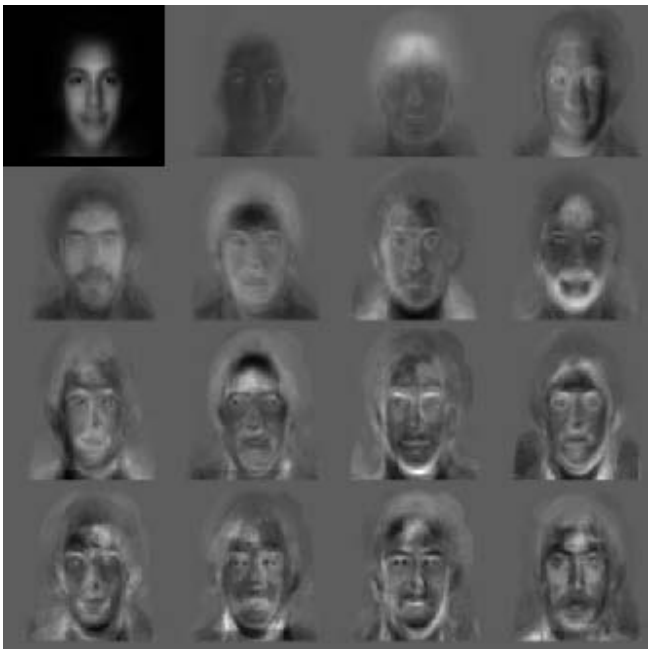

Abbildung 6: typische Basisgesichter der Eigenfaces-Methode (22)

3.5.2) Elastic Graph Matching

Bei der Methode des Elastic Graph Matching wird über das von der Kamera erfasste Gesicht ein Gitter gelegt. Dies passiert, indem an den markanten Gesichtselementen wie Augen, Mundwinkel und Nasenspitze Knotenpunkte eingezeichnet werden (24). Benachbarte Knoten werden durch Kanten verbunden, wodurch ein Gitter entsteht. Bei einem Vergleich wird schließlich der ermittelte gekrümmte Graph mit dem gespeicherten Referenzgraphen verglichen.

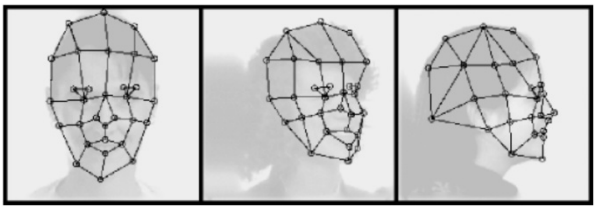

Abbildung 7: gekrümmter Graph mit Referenzpunkten (24)

Generell kann man sagen, dass Gesichtserkennung durchaus Vorteile gegenüber anderen biometrischen Systemen bietet. So ist die Erfassung beispielsweise kontaktlos möglich. Es entstehen kaum Kosten, da lediglich eine Kamera nötig ist, und die Bedienung entsprechender Geräte ist relativ einfach. Allerdings gibt es auch gravierende Nachteile von solchen Systemen. So ist es oftmals nur mit einer gewissen Kooperation der Benutzerinnen/Benutzer möglich, ein brauchbares Sample zu erfassen, das zu Vergleichszwecken herangezogen werden kann, weil die Systeme noch stark von der Blickrichtung und den Lichtverhältnissen abhängig sind (7; 8). Außerdem ist die False Rejection Rate vieler dieser Systeme relativ hoch, da zusätzlich zu der Blickrichtung auch Brillen oder sogar Make-up zu einer Rückweisung führen können (25; 28; 29).

3.6) Stimmerkennung (Voice-Recognition)

Zunächst muss hier klargestellt werden, dass Voice-Recognition ein Synonym für Speaker-Recognition ist und nicht Speech-Recognition gemeint ist. Es ist damit also die Erkennung der sprechenden Person gemeint und nicht die Erkennung des gesprochenen Textes (30).

Da die Stimme des Menschen sowohl anatomisch bedingt ist (z. B. Größe des Mundraumes und des Rachenraumes) als auch während der Entwicklung vom Umfeld geprägt wird (Sprechstil und Aussprache) (7) bildet sie eine menschliche Eigenschaft, welche als biometrisches Charakteristikum verwendet werden kann. Dies macht sich die Voice-Recognition zunutze.

Es handelt sich hierbei um ein sehr kostengünstiges Verfahren der Identifikation oder Authentifizierung, da lediglich ein hochwertiges Mikrofon benötigt wird. Mithilfe dieses Mikrofons wird bei der Voice-Recognition das Sprachmuster aufgezeichnet, wobei Merkmale wie Tonhöhe und Sprechdynamik erfasst werden. Beim Enrolment werden die gesprochenen Wörter in einem zeit- und amplitudenabhängigen Diagramm, dem sogenannten Frequenz-Spektrogramm, abgebildet und in der Datenbank gespeichert. Soll eine Person durch ihre Stimme identifiziert werden, wird ihre Stimme aufgezeichnet und aus der Aufzeichnung wird durch dasselbe Verfahren wiederum ein Frequenz-Spektrogramm erstellt, welches anschließend mit den Templates in der Datenbank verglichen und somit einer bestimmten Person zugeordnet werden kann. Bei einer Verifizierung wird das System oft mit einer Speech-Recognition gekoppelt und die Person wird vom System meist aufgefordert, einen zufällig generierten vorgegebenen Text zu sprechen (7). Zwar ist es für das System egal, welcher Text gesprochen wird, da die nötigen Merkmale des Stimmmusters bei jedem gesprochenen Text erfasst werden können, es sollen

dadurch allerdings mögliche Täuschungsversuche durch die Wiedergabe aufgezeichneter Sprachaufnahmen verhindert werden.

Abbildung 8: biometrisches Charakteristikum Stimme – das Frequenz-Spektrogramm (24)

Probleme ergeben sich für ein solches System jedoch, wenn laute Umgebungsgeräusche vorhanden sind (7), oder wenn die sprechende Person an einer Halserkrankung leidet, wodurch das Stimmmuster verändert werden kann. Auch kann eine einfache Stimmidentifikation leicht durch das Aufnehmen und Wiedergeben der Stimme einer anderen Person getäuscht werden.

3.7) Der Fingerprint

Der Fingerabdruck ist sicherlich eines der bekanntesten biometrischen Charakteristika. Leider werden Fingerabdrücke oft nur mit ihrem Einsatz in der Kriminalistik assoziiert und ihr Einsatz ist somit zu einem gewissen Grad negativ vorbelastet (31; 8). Betrachtet man jedoch die Kombination der Faktoren Komfort, Genauigkeit, Verfügbarkeit und Kosten, wie in Kapitel 3.1 beschrieben, wird schnell klar, warum Fingerabdruck-Scanner den größten Anteil am Marktsegment der biometrischen Systeme innehaben. Dies ist auch gut in der folgenden Grafik ersichtlich, wobei beachtet werden muss, dass auch das Segment „AFIS/Live-Scan“ zu Fingerprintsystemen gezählt werden kann, da es sich hierbei auch um entsprechende Systeme handelt (AFIS = „automatisierte Fingerabdruck Identifikations-Systeme“) (32).

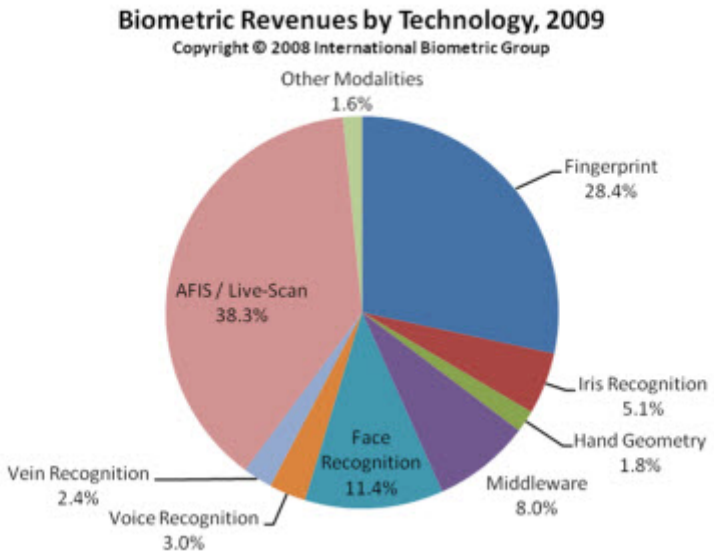

Abbildung 9: Marktanteil der verschiedenen biometrischen Systeme (33)

Als Fingerabdruck wird der Abdruck der sogenannten Papillarleisten der Fingerkuppe verstanden. Die Endungen und Verzweigungen dieser Leisten werden als Minuzien bezeichnet. Das Muster, das durch diese Minuzien entsteht, ist ein randotypisches Merkmal und kann somit eindeutig einer Person zugewiesen werden. Selbst eineiige Zwillinge besitzen unterschiedliche Fingerabdrücke (8). Für Vergleichszwecke in der Kriminalistik sowie der Biometrie werden jedoch nicht nur die feinen Merkmale (die Minuzien) verwendet sondern auch die Porenstruktur und die sogenannten groben Merkmale, von denen die wichtigsten im Folgenden genauer betrachtet werden sollen (31; 34):

- Schleifen: Das am häufigsten auftretende Merkmal ist die sogenannte Schleife, wobei zwischen linker und rechter Schleife unterschieden wird, je nachdem in welche Richtung sich die Leisten winden.

Abbildung 10: linke Schleife (34)

- Wirbel: Ein weiteres sehr verbreitetes Merkmal sind die sogenannten Wirbel. Hierbei bilden die Papillarleisten entweder eine Spirale oder konzentrische Kreise.

Abbildung 11: Spirale (34)

Abbildung 12: Konzentrische Kreise (34)

- Bögen: Bögen sind bei Weitem seltener als Schleifen und Wirbel. Bei diesem Merkmal bilden eine oder mehrere Papillarleisten einen Bogen über einer oder mehreren anderen.

Abbildung 13: Bogen (34)

Abhängig von der Art des Erfassungsgerätes und der zugehörigen Software werden bei Fingerprintsystemen entweder der gesamte Abdruck in der Datenbank hinterlegt und für Vergleichszwecke verwendet, oder es werden Algorithmen auf das erfasste Bild des Fingerabdruckes angewandt, welche die groben und feinen Merkmale erkennen, diese extrahieren und lediglich diese Merkmale speichern. Dies hat den Vorteil, dass die Datenmenge viel geringer ist und somit auch ein Vergleich zweier Fingerabdruck-Samples schneller erfolgen kann. Auch erzeugt es bei der Benutzerin/beim Benutzer ein gewisses Vertrauen, da der Fingerabdruck aus den gespeicherten Merkmalen nicht reproduziert werden kann (20).

Zu beachten ist bei der Verwendung des Fingerabdruckes als biometrisches Charakteristikum allerdings, dass die Qualität des vom Scanner erfassten Fingerabdruckbildes von vielen Faktoren abhängig ist, wie beispielsweise der Feuchtigkeit der Haut (Schweiß). Aber auch das Geschlecht und Alter einer Person können die Qualität deren Fingerabdrücke beeinflussen (35; 7; 8).

Um einen Fingerabdruck zu erfassen, gibt es mehrere Methoden. So kann ein optischer Sensor oder ein kapazitiver Sensor verwendet werden. Ebenso existieren Erfassungsgeräte, welche auf Grundlage der Ultraschalltechnologie operieren. Wieder andere Geräte besitzen thermische Sensoren. All diese unterschiedlichen Arten von Fingerprint-Scannern werden in ihren wesentlichen Eigenschaften und Funktionsweisen nun kurz vorgestellt. Anschließend soll ein Kapitel aufzeigen welche Strategien es gibt um das Täuschen eines Fingerprint-Scanners durch eine Attrappe wie dies in den Experimenten dieser Arbeit versucht wird zu verhindern. Hierfür muss das System eine Lebenderkennung durchführen, um somit zu erkennen, ob es sich um einen echten Finger oder um eine Attrappe handelt. Auch soll gezeigt werden, welche Probleme es bei den jeweiligen Strategien gibt.

3.7.1) Optische Sensoren

Die Erfassung durch einen optischen Sensor entspricht einer relativ intuitiven Methode der Fingerabdruckerfassung. Einfach ausgedrückt wird der Finger von einer Kamera abgelichtet. Dies passiert, indem der Finger auf eine Prismenfläche aufgelegt wird. Der Scanner bestrahlt diese Auflagefläche mit einer Lichtquelle (meistens bilden LEDs diese Lichtquelle) und durch die unterschiedliche Lichtreflexion von an der Fläche aufliegenden Papillarleisten und den zwischen diesen befindlichen Tälern, welche die Auflage nicht berühren, erfasst die Kamera das Bild der Fingerlinien. Hierbei muss unterschieden werden, ob es sich bei dem Scanner um einen sogenannten optisch reflexiven oder aber um einen optisch streuenden Sensor handelt. Bei ersterem werden die Täler des Fingerlinienbildes hell dargestellt, da an allen Stellen, wo die Auflagefläche nicht berührt wird, eine Totalreflexion stattfindet. Die Papillarleisten des Fingerabdruckes hingegen werden als dunkle Flächen abgelichtet, da hier keine Totalreflexion entsteht. Bei einem optisch streuenden Sensor hingegen wird durch eine andere Lichtführung und Kameraanordnung erreicht, dass das emittierte Licht an jenen Stellen, an denen der Finger die Auflagefläche berührt, gestreut wird. Dadurch entsteht ein entsprechend

invertiertes Bild der Fingerlinien, in dem die Papillarleisten hell und die Täler dunkel dargestellt werden (36; 37).

Eine andere Möglichkeit bieten optisch transmissive Sensoren. Hierbei liegt der Finger auf einer Lichtleiterplatte auf und wird von einer Lichtquelle durchleuchtet. In den meisten Fällen wird der Finger bei diesen Scannern von einer Lichtquelle auf der Fingerrückseite durchleuchtet. Es gibt aber auch Varianten dieser Scanner, bei denen die Lichtquellen an den Rändern des Scanners montiert sind, wodurch das Licht seitlich auf den Finger trifft (38). Durch die Auflagefläche wird verhindert, dass der Sensor berührt wird und zugleich ermöglicht eine entsprechende Auflage, dass das Licht den Sensor verlustfrei erreicht (36).

Sämtliche genannten optischen Sensoren können auch als Zeilensensor, auch Streifensensor genannt, gebaut werden. Hierbei ist der Scanner kleiner als die zu scannende Fläche, da er nur aus einer Zeile von Sensoren besteht. Um einen Fingerabdruck zu scannen, muss die Benutzerin/der Benutzer daher den Finger über diese Sensorzeile bewegen. Die Sensoren scannen so Stück für Stück den ganzen Finger und setzen anschließend aus den gescannten Einzeldaten den Fingerabdruck zusammen (36). Durch diese Bauweise benötigt der Scanner natürlich weniger Platz, was in vielen Fällen ein erheblicher Vorteil ist, jedoch keinen Vorteil gegenüber anderen Scanner-Typen darstellt, da auch die meisten anderen Scanner auf diese Art und Weise gefertigt werden können.

Die genannten optischen Scanner-Typen haben alle den gemeinsamen Nachteil, dass der Finger auf eine Fläche aufgelegt werden muss, um sich zu authentifizieren, womit diverse Nachteile einhergehen. So werden auf solchen Sensoren zum Beispiel Latenzabdrücke hinterlassen und oft gibt es auch gewisse hygienische Bedenken seitens der Benutzerinnen/Benutzer. Es gibt jedoch auch Scannersysteme, welche über einen kontaktlosen optischen Sensor verfügen. Bei einem solchen System wird auf ein Prisma verzichtet und stattdessen direkt ein Bild vom Finger gemacht. Diese Scannerart ist jedoch nur bedingt kontaktlos, da es auch hier Vorrichtungen geben muss, um den Finger in die richtige Position zu bringen und auch die korrekte Distanz zum Scanner einzuhalten. So werden dadurch zwar Latenzabdrücke verhindert, die Bezeichnung kontaktlos ist jedoch nur bedingt gerechtfertigt (36; 38). Ein weiterer Nachteil ergibt sich durch die leichte Beeinflussung des Scanners durch Verunreinigung der Scanneroberfläche oder auch des Fingers der Benutzerin/des Benutzers. Auch können Wunden und Narben am Finger zu einem Problem bei der Erkennung einer Person führen.

Vorteile von optischen Sensoren sind vor allem deren hoher Reifegrad sowie deren gute Bildqualität. Ein weiterer Pluspunkt, vor allem gegenüber kapazitiven Scannern, ist die Unempfindlichkeit optischer Scanner gegen elektrostatische Entladungen, welche leicht auftreten können, wenn sich Personen durch Reibungselektrizität aufladen.

3.7.2) Kapazitive Sensoren

Während bei optischen Sensoren mithilfe einer Lichtquelle, welche den Finger durch- beziehungsweise beleuchtet, ein Bild der Fingerlinien erzeugt wird, verwenden kapazitive Sensoren die Leitfähigkeit der Haut um ein entsprechendes Bild zu erzeugen. Bei kapazitiven Sensoren steht pro Pixel eine Elektrode zur Verfügung. Der Scanner besteht somit aus einer Vielzahl von Elektroden. Der aufgelegte Finger bildet die zweite Elektrode, wodurch eine Vielzahl an Kondensatoren entsteht. Das Dielektrikum (die isolierende Schicht zwischen den beiden Elektroden eines Kondensators) ist, je nachdem ob eine Papillarleiste aufliegt oder nicht, Wasser beziehungsweise Luft. Liegt an einer Elektrode (= ein Pixel) keine Leiste an, so ist das Dielektrikum Luft, wodurch die Kapazität geringer ist als bei jenen Elektroden, welche auf eine Papillarleiste treffen. Ein kapazitiver Scanner stellt diese Unterschiede in der Kapazität bildlich dar, wodurch ein Bild der Fingerlinien entsteht (36; 39).

Eine Sonderform der kapazitiven Sensoren bilden die sogenannten lumineszierenden kapazitiven Sensoren. Hierbei wird wie bei optischen Scannern ein Bildsensorchip verwendet, um das Linienbild des Fingers zu erfassen. Das Bild wird jedoch nicht mithilfe einer Lichtquelle, sondern nach dem gleichen Prinzip erzeugt wie bei anderen kapazitiven Scannern. Der einzige Unterschied besteht darin, dass bei diesem Scanner eine Elektrolumineszenzfolie mit einer durchsichtigen Elektrode verwendet wird. Als Gegenelektrode dient auch hier wieder der Finger. Die Elektrolumineszenzfolie leuchtet nun an jenen Stellen stärker, an welchen die Papillarleisten anliegen, da an diesen Stellen das elektrische Feld am stärksten ist. Somit entsteht wiederum ein Bild der Fingerlinien, das vom Bildsensorchip erfasst wird (36).

Wie optische Scanner können auch kapazitive Scanner als Zeilensensor ausgeführt sein. Der Unterschied liegt wiederum darin, dass der Finger über die Sensorzeile bewegen werden muss. Die Einzeldaten werden auch hier wieder zu einem Gesamtbild zusammengefügt.

Ein gravierender Nachteil von kapazitiven Scannern ist jedoch deren Anfälligkeit gegen elektrostatische Entladung. So kann sich eine Person beispielsweise bereits durch das Gehen über einen Teppich durch Reibungselektrizität aufladen. Diese elektrische Ladung kann sich beim Berühren des Scanners entladen und diesen beschädigen (38; 40).

3.7.3) Ultraschallsysteme

Ultraschall-Scanner operieren nach einem ähnlichen Prinzip wie optische Scanner mit dem Unterschied, dass nicht elektromagnetische Wellen des sichtbaren Spektrums (Licht), sondern akustische Wellen im Ultraschallbereich emittiert werden. So ist ein Ultraschall-Scanner aus einer Reihe von Transceivern aufgebaut, welche eine Kombination aus Transmitter und Receiver darstellen. Diese senden einen kurzen Ultraschallimpuls aus und schalten dann unmittelbar in den Empfangsmodus, um das vom Finger

reflektierte Echo zu empfangen. Die so empfangenen Signale werden anschließend in ein entsprechendes Bild umgewandelt (41).

Eine Eigenschaft von Ultraschallsystemen liegt darin, dass die Ultraschallwellen die oberste Hautschicht (Epidermis) durchdringen und den Fingerabdruck von der darunterliegenden Hautschicht (Dermis) ablesen (38). Daraus ergibt sich einer der größten Vorteile von Ultraschallsystemen: Sie werden durch Verletzungen oder Verunreinigungen der Epidermis nicht beeinträchtigt (41). Nachteile dieser Art von Fingerprint-Scanner ergeben sich jedoch durch die hohen Kosten in der Produktion und durch die Dauer eines Scanvorganges, welche mitunter auch ein paar Sekunden betragen kann (38).

3.7.4) Thermische Sensoren

Thermische Sensoren bestehen aus einem pyroelektrischen Material, welches Temperaturunterschiede in elektrisches Potenzial umwandelt. Hierbei wird jedoch nicht der Temperaturunterschied zwischen den Papillarleisten und den Tälern zwischen ihnen gemessen. Vielmehr registriert der Sensor jene Temperaturänderungen, die durch den Kontakt der Sensoroberfläche mit dem Finger entstehen und durchaus deutlich ausfallen. An jenen Stellen hingegen, wo die Haut den Sensor nicht berührt (Täler), bleibt die Temperatur annähernd gleich. Durch diesen Unterschied kann der Scanner ein Bild der Fingerlinien erfassen. Eine Einschränkung entsteht bei den entsprechenden Scannern jedoch dadurch, dass sich die Temperatur von Finger und Scanneroberfläche innerhalb von Sekundenbruchteilen angleicht, sodass ein Bild nur innerhalb kürzester Zeit abgeleitet werden kann. Aus diesem Grund werden thermale Scanner als Zeilen-Scanner gebaut, sodass die Benutzerinnen und Benutzer ihren Finger über den Scanner bewegen müssen. Dadurch liegt die gescannte Stelle des Fingers nur kurze Zeit auf den Sensoren auf und der Scanner kann den Fingerabdruck erfassen.

3.7.5) Lebenderkennung

Eine wichtige Eigenschaft, welche stark zur Sicherheit eines Fingerprint-Scanners (beziehungsweise eines biometrischen Systems im Allgemeinen) beitragen kann, ist die sogenannte Lebenderkennung. Es handelt es sich dabei um die Möglichkeit eines solchen Systems, den (lebenden) Finger einer Person von einer Fingerattrappe oder von totem Gewebe unterscheiden zu können. In den folgenden Kapiteln soll gezeigt werden, welche Möglichkeiten für eine solche Lebenderkennung existieren und warum sie nur bedingt einsetzbar sind.

3.7.5.1) Wärmemessung

Eine Möglichkeit, einen Lebendfinger von einer Attrappe zu unterscheiden, ist die Messung der Wärme (42). Die Idee dahinter ist, dass ein Lebendfinger üblicherweise eine Temperatur von 26-30° Celsius aufweist, während eine Attrappe oder ein abgetrennter Finger (totes Gewebe) meist kühler sind (43; 44). Diese Methode wäre zwar einfach zu implementieren allerdings ist ihr Einsatz nur bedingt sinnvoll, da die Temperatur eines Lebendfingers stark schwanken kann, wodurch der Temperaturbereich, in welchem ein Finger als

lebend erkannt wird, entsprechend groß sein muss. Hinzu kommt, dass die Temperatur eines Fingers auch von der Umgebungstemperatur abhängig ist. Soll ein Sensor also auch im Freien eingesetzt werden, muss der Temperaturbereich weiter vergrößert werden, da sonst die FRR zu stark ansteigen würde. Der große Akzeptanzbereich wiederum macht es recht leicht, eine Attrappe zu schaffen, welche akzeptiert wird. So würde es beispielsweise bereits reichen, eine sehr dünne Silikon- oder Gelatine-Attrappe herzustellen, wodurch die Temperatur des Fingers, an dem die Attrappe angebracht ist, unwesentlich verringert wird (45; 44). Da der Temperaturbereich der akzeptierten Fingerwärme entsprechend groß ist, könnte so fälschlicherweise auch eine Attrappe als Lebendfinger erkannt werden.

3.7.5.2) Leitfähigkeit

Eine weitere Möglichkeit die Echtheit (Lebendigkeit) eines Fingers festzustellen, ist dessen elektrische Leitfähigkeit zu messen. Die normale Leitfähigkeit (genauer der Widerstand) der menschlichen Haut beträgt in etwa 200 Kilo-Ohm für einen durchschnittlich feuchten Finger. Allerdings ist dieser Wert stark von der Feuchtigkeit der Haut abhängig. So kann der Hautwiderstand eines Fingers je nach dessen Feuchtigkeitsgehalt Werte zwischen wenigen Kilo-Ohm bis zu 2 Mega-Ohm annehmen (45; 43). Durch diesen großen Wertebereich ergibt sich ein ähnliches Problem wie bei der Temperaturmessung: Es ist einfach eine Attrappe herzustellen, welche einen Widerstand aufweist, der im entsprechenden Wertebereich liegt. So weist Gelatine einen ähnlichen Feuchtigkeitsgehalt auf wie ein Lebendfinger (3). Und selbst eine Silikonattrappe könnte durch das Auftragen von ein wenig Speichel einen entsprechenden Widerstandswert vortäuschen (44).

3.7.5.3) Herzschlag

Die Messung des Herzschlags in der Fingerspitze ist eine weitere offensichtliche Methode, um zu überprüfen, ob es sich um einen Lebendfinger handelt (42). Allerdings ergeben sich auch hier Probleme. So müsste eine Person, welche viel Sport betreibt oder aus anderen Gründen einen sehr niedrigen Pulsschlag aufweist, den Finger über eine längere Zeitspanne (mehrere Sekunden) auf dem Scanner belassen, damit die entsprechende Messung vorgenommen werden kann (43). Des Weiteren ist auch diese Methode der Lebenderkennung anfällig für hauchdünne Attrappen, bei denen der Pulsschlag des Fingers auch dann gemessen würde, wenn eine Attrappe aufgebracht ist (45).

3.7.5.4) Blutdruck

Eine andere Möglichkeit den Herzschlag des Menschen auszunutzen, um eine Lebenderkennung durchzuführen, ist die Messung des Blutdrucks. Hierbei ergeben sich allerdings auch die bereits beschriebenen Probleme, dass ein entsprechender Scanner durch eine hauchdünne Attrappe getäuscht werden könnte. Ein viel größeres Handicap stellt jedoch die Tatsache dar, dass heutige Systeme zur Blutdruckmessung auf die Messung an zwei Körperstellen angewiesen sind. Zwar existieren auch Geräte, welche mit einem Sensor

auskommen, diese müssen allerdings in eine Vene eingeführt werden (45) und sind somit aus naheliegenden Gründen ungeeignet, um damit eine Lebenderkennung an biometrischen Systemen durchzuführen.

3.7.5.5) Weitere Methoden

Die bisher vorgestellten Methoden zur Lebenderkennung nutzen alle zusätzliche Hardware (Sensoren), um die Lebenderkennung durchzuführen. Dies ist aber zum einen kostenintensiv und zum anderen ist es immer noch leicht möglich, solche Systeme zu täuschen, da die Lebenderkennung von einem eigenen Gerät und nicht vom Fingerprint-Scanner selbst durchgeführt wird (42; 43).

Ein weiterer Ansatz, eine Lebenderkennung durchzuführen, wäre die Verwendung von Informationen, welche dem erfassten biometrischen Charakteristikum innewohnen. Dies wäre beispielsweise bei einem Gesichtsthermogramm, dem Elektrokardiogramm oder der spezifischen Gangart eine Person denkbar, da zur Messung dieser Charakteristika eindeutig eine lebende Person anwesend sein muss (42). Während eine Lebenderkennung bei solchen Systemen daher leicht durchzuführen wäre, sind diese Charakteristika und entsprechende Systeme noch nicht so gut erforscht, um sie tatsächlich schon einsetzen zu können (43). Bei Fingerprint-Scannern hingegen kann dieser Ansatz nicht verfolgt werden, da der Fingerabdruck als biometrisches Merkmal nicht über solche inhärenten Informationen verfügt.

Als letzte Möglichkeit, eine Attrappe von einem lebenden Sample zu unterscheiden, soll hier die Verwendung der vom biometrischen System erfassten Information vorgestellt werden. Im Hinblick auf Fingerprint-Scanner kann hierbei beispielsweise die Schweißentwicklung lebender menschlicher Haut herangezogen werden (46). Hierbei muss ein Finger mindestens fünf Sekunden lang auf die Scanneroberfläche aufgelegt werden. Es werden zwei Bilder des Fingerabdruckes genommen, eines gleich nach dem Auflegen des Fingers, ein zweites fünf Sekunden danach. Handelt es sich um einen Lebendfinger, so wird der Finger innerhalb dieser fünf Sekunden durch Schweißabsonderungen feuchter. Dadurch erscheint das zweite Bild dunkler als das erste, so die Autoren der zitierten Studie. Bei einer Attrappe oder bei einem toten Gewebe hingegen tritt keine Transpiration auf und die beiden erfassten Bilder weisen keinen solchen Unterschied auf. Ein gravierender Nachteil dieser Methode ist natürlich, dass der Finger über eine so lange Zeit am Scanner verweilen muss, weshalb die Autoren meinen, dass auf diesem Gebiet noch zu forschen ist, ob ein solches Verfahren auch in kürzerer Zeit ein aussagekräftiges Ergebnis liefern kann (46).

3.8) Mögliche Angriffspunkte

Um ein biometrisches System gegen Angreiferinnen und Angreifer beziehungsweise Eindringlinge abzusichern, muss man sich vor Augen führen, an welchen Stellen des Systems ein Angriff möglich wäre. Im Folgenden sollen mögliche Angriffspunkte (47) aufgezeigt und näher beschrieben werden. Auch

wenn hier ein Fingerprintsystem als Beispiel dient, können diese Angriffspunkte auch auf andere (biometrische) Zugangssysteme verallgemeinert werden. Im Allgemeinen existieren bei jedem biometrischen (Zugangs-) System acht Angriffspunkte (siehe Abbildung 14: Angriffspunkte eines biometrischen Systems).

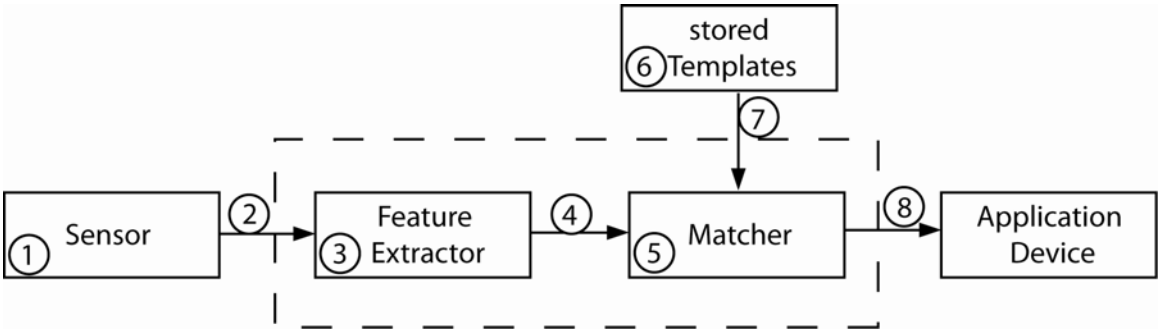

Abbildung 14: Angriffspunkte eines biometrischen Systems (47)

Der erste Angriffspunkt ist Thema dieser Arbeit und wird in den folgenden Kapiteln ausführlich behandelt werden – ein Angriff auf den Fingerprint-Scanner (beziehungsweise den Sensor des biometrischen Systems). Ein Angriff an dieser Stelle erfolgt typischerweise mit einer Nachbildung des erwarteten biometrischen Charakteristikums (48). Ein Fingerprint-Scanner wird dementsprechend durch den Einsatz einer Fingerattrappe zu täuschen versucht. Wie eine solche Attrappe erstellt werden kann und worauf dabei zu achten ist, wird in dieser Arbeit genauer beschrieben. Es soll an dieser Stelle jedoch nochmals erwähnt werden, dass dies nicht die einzige Stelle ist, an der ein mit einem Fingerprint-Scanner gesichertes System überwunden werden kann, sondern lediglich die erste Angriffsmöglichkeit darstellt.

Wurde das biometrische Charakteristikum vom Sensor erfasst, werden als nächstes die wesentlichen Merkmale dieses Charakteristikums ausgelesen. Bei einem Fingerprintsystem wäre dies beispielsweise die Extraktion der Minuzien aus dem Fingerabdruck. Diese Aufgabe übernimmt der sogenannte „feature extractor“. Dazu müssen die vom Sensor erfassten Daten allerdings erst zu diesem übertragen werden. Dieser Übertragungsweg vom Sensor zum „feature extractor“ bildet nach Ratha et al (47) **die zweite mögliche Angriffsstelle** eines solchen Systems. So könnte eine Angreiferin/ein Angreifer versuchen, die Informationen an diesem Übertragungskanal abzuhören (sniffen) und mit den so gewonnenen Daten eine sogenannte „Replay-Attacke“ durchzuführen. Hierzu müsste eine Angreiferin/ein Angreifer lediglich die zu einem früheren Zeitpunkt abgehörten Datenpakete eines erfolgreichen Logins erneut in die abgehörte Leitung einspeisen, um Zugang zum System zu erlangen (49).

Der „feature extractor“ selbst bildet anschließend **die dritte Angriffsmöglichkeit**. Eine Angreiferin/Ein Angreifer kann versuchen den „feature extractor“ des bestehenden Systems zu ändern oder durch einen selbst geschriebenen „feature extractor“ zu ersetzen. In beiden Fällen kann die Angreiferin/der Angreifer bei erfolgreicher Durchführung, unabhängig von den tatsächlich im präsentierten biometrischen Charakteristikum enthaltenen

Merkmalen, beliebige Merkmale als „ausgelesene Merkmale“ ausgeben und an den Matcher senden, um eine Übereinstimmung mit den Merkmalen einer berechtigten Person zu erzeugen und dadurch Zugang zum System zu erhalten (47).

Wie bereits erwähnt, werden die vom „feature extractor“ ausgelesenen Merkmale an den sogenannten „Matcher“ weitergereicht. Die Leitung vom „feature extractor“ zum „Matcher“ bildet somit **den vierten möglichen Angriffspunkt** eines Zugangssystems. Diese Übertragung kann von einer Angreiferin/einem Angreifer abgehört werden und die übertragenen Daten beeinflusst werden. So könnten die zu übertragenden Daten durch von der Angreiferin/vom Angreifer bestimmte Daten ersetzt werden (48). Es könnte somit wiederum eine Replay-Attacke stattfinden, indem die Angreiferin/der Angreifer zuvor gespeicherte Datenpakete einspielt, welche einen Zugang ermöglichen.

Um entscheiden zu können, ob eine Benutzerin/ein Benutzer Zugang zum System erhält oder nicht, müssen die vom „feature extractor“ erfassten Merkmale noch mit den in der Datenbank gespeicherten Templates verglichen werden. Dies wird vom sogenannten „Matcher“ (auch Classifier genannt (48)) erledigt. Dieser ist ein Programm, welches den erwähnten Vergleich durchführt und als Ergebnis einen Wert (Score) ausgibt, welcher die Übereinstimmung (beziehungsweise Ähnlichkeit) der beiden Merkmalsets ausweist. Stimmen die beiden Sets in vielen Punkten überein, so wird ein hoher Score erzeugt und der Benutzerin/dem Benutzer wird der Zugang (beziehungsweise Zugriff) gewährt. Weisen die beiden Sets zu wenige Übereinstimmungen auf, so fällt der vom Matcher erzeugte Score entsprechend niedrig aus und der Zugang/Zugriff wird verweigert. Es ist leicht ersichtlich, dass der Matcher somit auch ein gutes Ziel für einen Angriff abgibt. Er stellt daher **den fünften Angriffspunkt** dar. So könnte eine Angreiferin/ein Angreifer den Matcher manipulieren oder einen eigenen Matcher programmieren und den ursprünglichen damit ersetzten. Dadurch kann sie/er das Ergebnis des Vergleiches steuern und somit auch bei geringer oder keiner Übereinstimmung der beiden Merkmalsets einen hohen Score ausweisen, wodurch der Zugang gewährt würde. Auch das Gegenteil wäre denkbar. So könnte eine Angreiferin/ein Angreifer den Matcher derart ändern, dass unabhängig von den beiden Merkmalsets stets ein niedriger Score erzeugt wird und somit niemand mehr Zugang/Zugriff zum System erhält.

Den sechsten Angriffspunkt stellt die „Datenbank“ dar. In ihr werden die Templates aus dem Enrolment, welche dem Matcher zum Vergleich dienen, gespeichert. Schafft es eine Angreiferin/ein Angreifer daher in die Datenbank einzudringen, so können eines oder mehrere der abgespeicherten Templates geändert werden (47). Damit könnte sie/er beispielsweise statt eines vorhandenen Templates auch ein Template ihres/seines eigenen Abdruckes einspielen und somit Zugang zum System erlangen, da das System fälschlicherweise davon ausgeht, dass der Fingerabdruck der Angreiferin/des Angreifers einer anderen, autorisierten Person zuzuordnen ist.

Die Leitung, welche der Übertragung der gespeicherten Templates von der Datenbank zum Matcher dient, bildet **die siebente Angriffsstelle**. Eine Angreiferin/Ein Angreifer könnte das zu übermittelnde Template abfangen und an dessen Stelle ein anderes Template zum Matcher schicken, welches die von ihr/ihm gewünschten Merkmale aufweist. So könnte eine Angreiferin/ein Angreifer dem System vortäuschen, dass ihr/sein eigener Fingerabdruck die gleichen Merkmale aufweist wie der Fingerabdruck einer autorisierten Person (47).

Als achte und letzte Angriffsmöglichkeit dient die Verbindung des gesamten biometrischen Zugangssystems an das dadurch gesicherte System. Um dem System mitzuteilen, dass eine Person autorisiert ist, auf bestimmte Daten zuzugreifen oder einen bestimmten Teil eines Gebäudes zu betreten, wird das Ergebnis des Matchers an das System weitergeleitet. An dieser Stelle wäre es natürlich möglich, dass eine Angreiferin/ein Angreifer das gesamte Zugangssystem umgeht, indem sie/er sich direkt in die Leitung zwischen Zugangssicherung und System einhackt und dem System ein Signal schickt, mit dem sie/er ihm mitteilt, dass eine erfolgreiche Authentifizierung stattgefunden hat (48).

Betrachtet man diese Angriffsstellen, so stellt man schnell fest, dass sie sich grob in zwei Gruppen unterteilen lassen. Die erste Gruppe bilden Angriffe auf die Systemmodule des Zugangssystems (Angriffspunkte 1,3,5,6) die zweite Gruppe bilden Angriffe auf die Übertragungswege zwischen den Modulen beziehungsweise zwischen der Zugangssicherung und dem System selbst (Angriffspunkte 2,4,7,8). Es gibt jedoch für jeden der genannten Angriffspunkte Maßnahmen, um einem möglichen Angriff entgegen zu wirken. So gibt es verschiedene Ansätze, sich gegen einen Angriff auf einen Übertragungsweg zu schützen (Angriffspunkte 2,4,7,8). Die Daten sollten auf alle Fälle verschlüsselt werden. Allerdings bietet diese Methode nur solange einen Schutz gegen Angreiferinnen und Angreifer, solange diesen nicht der Schlüssel bekannt ist. Ein anderer Ansatz ist das sogenannte Watermarking (50; 48). Hierbei wird den Daten ein digitales Wasserzeichen angefügt. So wäre es beispielsweise auch möglich, die Daten mit einem Zeitstempel (timestamp) zu versehen. Das System könnte in Folge nur auf Daten reagieren, welche innerhalb einer bestimmten Zeit empfangen werden beziehungsweise den richtigen Zeitstempel aufweisen. Ein anderer Vorteil von Watermarking besteht darin, dass das Wasserzeichen nicht aus den Daten entfernt werden kann, ohne die Daten selbst zu unbrauchbar zu machen. Somit wäre ein von einer Hackerin/einem Hacker abgefangenes Paket nutzlos, da sie/er es nicht für eine Replay-Attacke einsetzen kann, da sie/er das Wasserzeichen nicht entsprechend abändern kann. (48)

Eine Möglichkeit, um einen Angriff am Sensor (Angriffspunkt 1) entgegenzuwirken, bildet beispielsweise die Lebenderkennung (siehe Kapitel 3.7.5). Natürlich ist es auch möglich, einem solchen Angriff entgegenzuwirken, indem der Zugang nicht nur von einem biometrischen System gesichert wird,

sondern der Sensor des Systems zusätzlich von einer natürlichen Person (Wachpersonal) beaufsichtigt wird, um zu verhindern, dass Attrappen zum Einsatz kommen.

Weiters kann man Angriffe auf die Punkte 3,4,5,6 und 7 erschweren, da man den Zugang zu diesen recht einfach beschränken kann. Auch muss hier angemerkt werden, dass Angriffe auf die Übertragungsleitungen 4 und 7 eher bei verteilten Systemen oder bei der Authentifizierung über das Internet bedacht werden müssen, da in den meisten Fällen der „feature extractor" im selben Gerät läuft wie der Matcher, und wo zumeist auch die Datenbank installiert ist. Ein Angriff auf die Datenbank ist oft dadurch abzuwehren, dass man die Einstellungen der Datenbank derart anlegt, dass nur beim Erstellen eines neuen Datensatzes auf die Datenbank geschrieben werden kann. Somit kann ein bestehendes Template nicht verändert werden (48).

Auch wenn viele der Angriffspunkte wie soeben beschrieben gut gesichert werden können, muss man sich darüber im Klaren sein, dass sie existieren und darf sich nicht sicher sein, dass der einzige Angriffspunkt eines biometrischen Systems sein Sensor ist.

4) Sicherheit von Fingerabdruck-Scannern

Im folgenden Kapitel soll genauer betrachtet werden, wie „sicher“ ein System durch den Einsatz eines Fingerabdruck-Scanners tatsächlich gesichert wird, das heißt, wie gut die FAR beziehungsweise die FRR tatsächlich sind, wenn versucht wird, mithilfe einer Attrappe in das System einzudringen. So soll aufgezeigt werden, ob es möglich ist und falls es möglich ist, wie schwierig es ist, Fingerprint-Scanner zu täuschen. Hierfür wurden Tests mit verschiedenen Scannern durchgeführt, in denen versucht wurde, die Scanner durch zuvor gefertigte Fingerabdruck-Attrappen zu täuschen, um sich somit Zugang zum durch den Scanner gesicherten System zu erlangen. Im Unterschied zu bereits existierenden Artikeln (34; 1; 22; 25; 51; 2; 52; 3; 53; 45), welche sich diesem Thema widmen und die als kreative Vorlage für die durchgeführten Versuche und Tests indirekt in diese Arbeit einfließen, soll im Folgenden gründlich und detailliert dargelegt werden, welche Mittel und Geräte bei den Tests zum Einsatz kamen und wie die einzelnen Schritte zur Herstellung von Attrappen konkret durchgeführt wurden. Somit soll der Leserin und dem Leser das Nachvollziehen der Ergebnisse sowie eine etwaige Reproduktion von Tests oder einzelner Schritte einfacher gemacht werden.

4.1) Verwendete Fingerprint-Scanner

Bei den Versuchen kamen mehrere Fingerprint-Scanner zum Einsatz, weil nicht nur getestet werden soll, ob ein bestimmter Scanner getäuscht werden kann, sondern versucht wird, die Aussage der Tests möglichst allgemein zu gestalten. Auch wurde nur in wenigen der bisherigen Arbeiten erwähnt, welcher Scanner genau getäuscht wurde, weshalb es sinnvoll erschien, im Zuge dieser Arbeit auch zu testen, welche Scanner getäuscht werden können und welche nicht. Daher wurden die Versuche sowohl an einem Gerät mit optischem Vollflächensensor als auch an einem Gerät mit kapazitivem Zeilensensor durchgeführt, um beide möglichen Scanner-Bauarten abzudecken. Beide Geräte sind für Heimanwenderinnen und Heimanwender gedacht und erlauben keine speziellen Sicherheitseinstellungen. Konkret wurden die folgenden Geräte getestet:

- Microsoft Fingerprint-Reader (Optischer Vollflächenscanner)
- Digitus Desktop Biometric Fingerprint-Reader (kapazitiver Zeilenscanner)

Nachdem es gerade im Bereich des Fingerprint-Scannens eine Vielzahl von möglichen Sensoren gibt, wurde darauf geachtet, sich nicht auf einen Sensor zu konzentrieren. Der Fokus dieser Arbeit wurde auf optische und kapazitive Sensoren gelegt, da diese in einem Großteil der momentan verfügbaren Geräte verbaut sind.

4.1.1) Microsoft Fingerprint-Reader

Bei diesem Gerät aus dem Hause Microsoft handelt es sich um einen vollflächigen optischen Fingerprint-Scanner, welcher über einen USB-Port an den PC angeschlossen werden kann. Gedacht ist der Fingerprint-Reader für

Heimanwenderinnen und Heimanwender. Mit der dem Gerät beiliegenden Software (Digital Persona) kann der Scanner sowohl verwendet werden um sich am System per Fingerabdruck anzumelden als auch um sich auf diversen Webseiten einzuloggen, indem Username und Passwort gespeichert und mit einem Fingerprint verknüpft abgelegt werden. Somit kann sich eine Userin/ein User durch einfaches Auflegen des entsprechenden Fingers auf die Scanfläche bei der entsprechenden Applikation anmelden. Das eben genannte einfache Vorgehen stellt auch den Hauptgrund dar, warum dieses Gerät für die Tests ausgewählt wurde: Es ist leicht zu beschaffen und ist preislich so gestaltet, dass es sich typische Heimanwenderinnen und Heimanwender leisten können (zum Zeitpunkt dieser Arbeit circa 40 Euro). Erwähnt werden muss jedoch, dass sich das Produkt nicht zur Absicherung eines Systems eignet, sondern eher auf die Bequemlichkeit der Benutzerinnen und Benutzer abzielt, welche sich durch den Einsatz des Gerätes keine Passwörter mehr merken müssen. Trotz des Einsatzes des Fingerprint-Readers ist es allerdings weiterhin möglich sich mit Username und Passwort am System anzumelden, wodurch das Gerät keinerlei Sicherheitsverbesserung darstellt, da auch weiterhin durch Knacken des Passwortes einer Benutzerin/eines Benutzers in das System eingedrungen werden kann. Darauf wird auch in der Gerätebeschreibung entsprechend hingewiesen. Des Weiteren kann für das Gerät nicht eingestellt werden, wie genau ein vom Scanner erfasstes Fingerabdruck-Sample mit dem gespeicherten Referenzabdruck übereinstimmen muss, um als gleich angesehen zu werden. Dies ist zum Teil natürlich auch auf die Zielgruppe und den Einsatzbereich des Gerätes zurückzuführen. Dennoch wäre es für Vergleichszwecke mit den Testergebnissen interessant gewesen auf konkrete Werte wie False Reject Rate (FRR) und False Accept Rate (FAR) des Herstellers zurückgreifen zu können.

4.1.2) Digitus Desktop Biometric Fingerprint-Reader

Als zweites Testgerät für die im Rahmen dieser Arbeit durchgeführten Versuche wurde der Digitus Fingerprint-Reader verwendet. Die Wahl dieses Gerätes wurde aus ähnlichen Gründen getroffen wie beim Microsoft Fingerprint-Reader: Das Gerät ist billig in der Anschaffung (zum Zeitpunkt dieser Arbeit circa 35 Euro) und gut verfügbar. Ein weiterer Aspekt war die Bauweise des Gerätes. Da mit dem Microsoft Fingerprint-Reader bereits ein optischer Vollflächenscanner als Testgerät gewählt wurde, sollte das zweite Testgerät über kapazitive Sensoren verfügen und als Zeilenscanner aufgebaut sein. Dies erschien dem Autor auch in der Hinsicht wichtig, weil es auf dem heutigen Laptopmarkt immer mehr Produkte gibt, welche mit einem Scanner dieser Bauart ausgerüstet sind und ihren Benutzerinnen und Benutzern dadurch eine erhöhte Sicherheit versprechen. Die Tests an diesem Scanner sollen daher auch Aufschluss darüber geben, ob diese Sicherheitsversprechen gerechtfertigt oder ein reiner Marketingtrick sind.

Das Gerät selbst wird mit der Software „Fingerprint Autentication Suite“ in der Version 4.2.1.0. ausgeliefert, welche benötigt wird, um das Gerät zu nutzen. Ist die Software installiert, hat die Benutzerin/der Benutzer die Möglichkeit in einer Enrolment-Phase ihre/seine Fingerabdrücke zu registrieren, indem sie/er

die gewünschten Finger mehrmals über das Sensorenarray bewegt. Ist dies getan, hat die Userin/der User die Möglichkeit sich fortan durch seinen Fingerabdruck am System anzumelden. Wie auch beim Microsoft Fingerprint-Reader dient das Gerät allerdings eher der Bequemlichkeit der Benutzerin/des Benutzers, da es ihr/ihm diese einfache Form der Anmeldung bietet, es ist jedoch weiterhin möglich sich auch mit einem Usernamen und zugehörigem Passwort anzumelden, wodurch auch hier weiterhin ein Anknüpfungspunkt für etwaige Angriffe gegeben ist. Durch die Installation des Tools werden der Benutzerin/dem Benutzer allerdings noch weitere interessante Features bereitgestellt. So können künftig Dateien oder ganze Ordner mithilfe des Fingerprint-Scanners verschlüsselt und wieder entschlüsselt werden. Auch können Anwendungen gesperrt werden und so andere Benutzerinnen/Benutzer daran gehindert werden sie zu starten, ohne sich zuvor mit dem entsprechenden Fingerprint zu verifizieren. Allerdings haben auch diese beiden Features den bereits genannten Nachteil, dass sie eine Benutzerin/einen Benutzer ebenso durch das Eingeben eines gültigen Passwortes verifizieren, wie sie dies beim Präsentieren des korrekten Fingerabdruckes tun.

Leider werden wie auch beim Microsoft Fingerprint-Reader kaum technische Daten oder Referenzwerte wie FAR oder FRR für dieses Gerät mitgeliefert. Allerdings können manche dieser Daten der Homepage des Herstellers entnommen werden (54). So wird für den Digitus Fingerprint-Reader eine Falschakzeptanzrate (FAR) von weniger als 1:100000 und eine Erkennungszeit von weniger als einer Sekunde ausgewiesen. Durch diese Werte gibt es zumindest gewisse Anhaltspunkte für die in Rahmen dieser Arbeit durchgeführten Test mit diesem Scanner.

4.2) Fingerabdrücke nehmen

Um einen Fingerprint-Scanner zu täuschen, muss man natürlich über eine Attrappe (im Folgenden auch „künstlicher Finger“ genannt) verfügen, welche möglichst die gleichen Eigenschaften besitzt wie der natürliche Finger jener Person, als die man sich ausgeben will (im Folgenden als Opfer bezeichnet). Die wesentlichste Eigenschaft, die natürlich nachgestellt werden muss, ist die Struktur des Fingers selbst – seine Papillarleisten. Viele Fingerabdruck-Scanner arbeiten nicht mit dem gesamten Fingerabdruck sondern speichern nur die sogenannten Minuzien. Da es aber schwierig ist nur diese nachzubilden wird in der Regel der gesamte Abdruck nachgeformt.

Üblicherweise muss man daher erst einmal versuchen in den Besitz eines Gegenstands zu gelangen, welchen das Opfer zuvor angefasst und auf dem es somit Fingerabdrücke hinterlassen hat. Dabei spielt natürlich die Art und Beschaffenheit des Gegenstands eine entscheidende Rolle (siehe 4.2.1). Des Weiteren sollte beachtet werden, dass es sich dabei möglichst um einen Gegenstand handelt, welcher ausschließlich vom Opfer angefasst wurde, da man sonst im weiteren Verlauf unter Umständen einen Fingerabdruck verarbeitet, welcher von einer ganz anderen Person stammt, was aus naheliegenden Gründen unerwünscht ist. Auch sollte es sich um einen

Gegenstand handeln, welcher vom Opfer nicht zu oft angefasst wurde, da man sonst vor dem Problem stehen kann, dass sich einzelne Fingerabdrücke überlappen und dadurch kaum noch brauchbare Fingerabdrücke genommen werden können.

4.2.1) Einfluss der Oberflächenbeschaffenheit auf das Nehmen von Fingerabdrücken

Die Beschaffenheit des akquirierten Gegenstands ist wie bereits erwähnt von entscheidender Bedeutung. So muss man je nach Oberfläche entscheiden, mit welchem Verfahren (Pulver oder Dampf) man die Fingerabdrücke sichtbar macht, beziehungsweise entscheiden, ob es die Oberfläche des Gegenstands überhaupt zulässt, mit einfachen Mitteln einen brauchbaren Fingerabdruck zu erhalten. Als einfache Grundregel kann man sagen, dass sich Objekte mit glatten Oberflächen wie diverse Glasflächen (beispielsweise auch Trinkgläser) sowie Metallflächen (zum Beispiel Türschnallen) viel eher dazu eignen, Fingerabdrücke zu nehmen als Gegenstände mit rauer oder gemusterter Oberfläche. Hier kann man oft nur Teilabdrücke nehmen (55).

Es ist außerdem zu beachten, dass die Farbe des Gegenstandes möglichst einheitlich ist, um in weiterer Folge ein Digitalisieren des Abdrucks zu vereinfachen (siehe 4.3). So sind beispielsweise auf Fotos oft Fingerabdrücke zu finden, diese sind in Folge allerdings meist schwer zu digitalisieren, da zum Teil, durch die Farbvielfalt des Fotos, kein ausreichender Kontrast zwischen den Farben des Fotos und dem Fingerabdruckmittel besteht.

4.2.2) Grafitpulver

Die wohl bei Weitem bekannteste Methode um Fingerabdrücke zum Vorschein zu bringen, ist das Bestäuben des Fingerabdruckes mit Grafitpulver (1), wie man sie auch in der Kriminalistik verwendet und oft in Filmen sieht. Auch in dieser Arbeit war das eine der Methoden, die verwendet wurden, um Fingerabdrücke sichtbar zu machen. Der Grund hierfür war, dass die Anwendung dieser Methode nicht all zu schwierig zu erlernen ist und mit ein bisschen Übung durchaus brauchbare Resultate erreicht werden können. Ein weiterer für diese Arbeit wichtiger Grund war die Verfügbarkeit von Grafitpulver, welches beispielsweise beim Schmieren von Türschlössern zum Einsatz kommt, was in diesem Kontext nicht einer gewissen Ironie entbehrt.

Um einen Fingerabdruck mit dieser Methode sichtbar zu machen, muss auf der Stelle, an der man den Fingerabdruck ausgemacht hat oder diesen zumindest vermutet, vorsichtig ein wenig Grafitpulver verteilt werden. Am besten eignet sich hierfür ein weicher Haarpinsel. Wichtig hierbei ist, dass man beim Verteilen des Pulvers den Pinsel nicht zu fest auf die Oberfläche drückt, da sonst der Fingerabdruck verschmiert und somit unbrauchbar wird. Ist dies getan, bläst man das überschüssige Pulver am besten vorsichtig vom Objekt. Obwohl sich das Verfahren als nicht so trivial erwies, wie zunächst gedacht, liegt es mit ein wenig Übung durchaus im Bereich des Machbaren den Fingerabdruck mit dieser Methode durch Grafitpulver gut hervorzuheben.

Bei allen mit Grafitpulver durchgeführten Versuchen wurde das Pulver „Graphit“ der Firma Pressol (Nr. 10 589) verwendet.

4.2.3) Eindampfen mit Cyanacrylat

Auch diese Methode, Fingerabdrücke sichtbar zu machen, ist mittlerweile durch diverse Kriminalserien im Fernsehen durchaus bekannt. In diesen Serien wird dabei das Objekt, auf dem Fingerabdrücke vermutet werden, in einer luftdichten Kammer mit einer Chemikalie eingedampft, woraufhin nach gewisser Zeit die Fingerabdrücke sichtbar werden. Was allerdings weniger bekannt ist - für diese Arbeit jedoch ein ausschlaggebender Grund war auch diese Methode zu verwenden – das ist die Tatsache, dass eine solche Kammer in einfacher Form leicht nachgebaut werden kann und auch das entsprechende Mittel zum Eindampfen leicht erhältlich ist: die Chemikalie „Cyanacrylat“ (1). Diese Chemikalie ist beispielsweise Bestandteil vieler Superkleber. Somit können mit wenig Aufwand Fingerabdrücke sichtbar gemacht werden, indem man eine Art Deckel über die Stelle stülpt, an der ein Fingerabdruck vermutet wird. An die Innenseite dieses Deckels wird ein wenig Superkleber angebracht. Somit kann man auf recht einfache Art und Weise einen Fingerabdruck eindampfen.

Das Sichtbarmachen der Fingerabdrücke in diesem Verfahren beruht auf einem chemischen Prozess, bei welchem die Dämpfe der Chemikalie mit den Fettrückständen des Fingerabdrucks reagieren (sich an die Fettpartikel heften) und die Ablagerungen dieser Chemikalie, welche an den Fettrückständen sichtbar werden, somit einen verwertbaren Fingerabdruck liefern.

Auch das Anwenden dieser Methode bedarf einer gewissen Übung, da es sonst leicht passieren kann, dass zu viel Klebstoff aufgebracht wurde, wodurch dieser vom Deckel auf die Oberfläche tropft und den Fingerabdruck unbrauchbar macht. Außerdem muss darauf geachtet werden, dass der Deckel die entsprechende Stelle tatsächlich möglichst luftdicht abschließt, da sonst oft der gewünschte Erfolg ausbleibt. Nach einigen Versuchen kann man aber bereits ganz gut abschätzen, wie viel Klebstoff verwendet werden muss und wie der Deckel ausgewählt und beschaffen sein muss. Somit ist auch diese Methode durchaus dazu geeignet, von weniger versierten Personen angewandt zu werden.

Im Rahmen dieser Arbeit wurden hierfür die Kleber „Super Glue 1200“ der Firma Wiko als auch der Klebstoff „Superkleber“ der Firma Loctite verwendet. Beide lieferten annähernd gleiche Ergebnisse.

4.3) Fingerabdrücke digitalisieren

Nachdem die Fingerabdrücke vom akquirierten Gegenstand genommen beziehungsweise sichtbar gemacht wurden, müssen diese digitalisiert werden, um am Computer weiter bearbeitet zu werden. So ist es beispielsweise je nach Verfahren nötig, den genommenen Fingerabdruck zu spiegeln. Auch kann es nötig sein das Bild des Fingerabdruckes digital aufzubessern (siehe 4.4). Um all

dies machen zu können, muss der Fingerabdruck zunächst einmal digitalisiert werden. Um dies zu bewerkstelligen, wurden in den Tests zwei verschiedene Methoden verwendet, welche im Folgenden genauer beschrieben werden. Ein Problem, dem man bei allen der vorgestellten Methoden begegnet, ist die korrekte Erfassung der Größe des Abdruckes. Dazu ist es beim Fotografieren des Abdruckes beispielsweise sinnvoll, einen Maßstab seitlich und unterhalb vom Abdruck zu platzieren, damit man auch später noch die Größe des Abdrucks ableiten kann. Ist diese Information nicht verfügbar, wird es später umso schwerer den Abdruck korrekt auszudrucken, um damit Attrappen-Vorlagen zu erstellen.

4.3.1) Fingerabdrücke fotografieren

Eine einfache Methode, einen Fingerabdruck zu digitalisieren, ist ihn zu fotografieren (1). Dies klingt zunächst recht einfach, ist in der Durchführung jedoch nicht so trivial. So muss beispielsweise bedacht werden, dass es beim Nehmen der Fingerabdrücke zwar von Vorteil ist, wenn das Objekt eine glatte Oberfläche besitzt, beim Fotografieren des Fingerabdruckes kann sich diese Oberfläche jedoch als Nachteil erweisen, da glatte Oberflächen meist stark spiegeln, daher muss man beim Fotografieren für entsprechend gute Lichtverhältnisse sorgen. Sollte der Einsatz des Blitzes nötig sein, muss dafür Sorge getragen werden, dass man die Oberfläche nicht direkt anblitzt, da sonst meist Spiegelungen auf dem Foto entstehen, welche im Nachhinein, wenn überhaupt, nur mit erheblichem Aufwand beseitigt werden können.

Bei den Versuchen wurden mehrere Digitalkameras verwendet, um die Fingerabdrücke zu fotografieren. Hierbei wurde versucht sowohl aus der Kategorie „Snapshot"-Kamera, als auch aus den Kategorien „Kompaktkamera" und „Digitale Spiegelreflexkamera" ein repräsentatives Modell zu wählen. Konkret kamen folgende Kameramodelle zum Einsatz:

- Sony Cybershot DSC-T3 (Snapshot-Kamera)
- Leica Digilux 1 (Kompaktkamera)
- Nikon D300 (Digitale Spiegelreflex Kamera)

Bei den Versuchen stellte sich bald heraus, dass es durchaus große Unterschiede gibt, zwischen den einzelnen Kameras und natürlich auch zwischen verschiedenen Aufnahmeverfahren. Anfangs wurde versucht, die Fotos freihändig zu machen, da anzunehmen ist, dass eine Durchschnittsanwenderin/ein Durchschnittsanwender kein Stativ einsetzt. Es zeigte sich jedoch recht schnell, dass es sich bei den Papillarleisten (bzw. Minuzien) der Fingerabdrücke um zu feine Muster handelt, sodass sie bei freihändig gemachten Aufnahmen der Fingerabdrücke zu leicht unscharf waren. Dies war vor allem bei der kleinen Snapshot-Kamera problematisch, war aber auch bei den anderen beiden Kameras deutlich merkbar. Daher wurden in späterer Folge sowohl ein Stativ als auch ein Reprotisch verwendet, um scharfe Fotos von den Fingerabdrücken machen zu können. So wurde versucht, Aufnahmen unterschiedlicher Fingerabdrücke auf verschiedenen Hintergründen zu machen. Sämtliche Aufnahmen wurden bei normaler Raumbeleuchtung, mit

geräteigenem Blitzlicht, beziehungsweise mit externem Blitzlicht (nur Nikon D300) geschossen. Die Verschlusszeiten bei Raumbeleuchtung (ohne Blitz) waren allerdings zu lang, sodass die Fotos zumeist unscharf und damit unbrauchbar waren. Bei Blitzlicht kam es zu Problemen, da dieses auf der Glasfläche mit dem Fingerabdruck Spiegelungen erzeugte. Daher wurde bei den Aufnahmen auf dem Reprotisch auf zwei Tageslichtlampen (5300 Kelvin) zurückgegriffen, damit ohne Blitz fotografiert werden konnte.

Des Weiteren wurden die Aufnahmen der Abdrücke sowohl in Farbe als auch (so es der Fotoapparat zuließ) in Schwarz-Weiß, beziehungsweise als Graustufenfoto aufgenommen. Es zeigte sich im späteren Verlauf der Versuche jedoch, dass es von Vorteil ist, die Abdrücke in Farbe zu fotografieren, da sonst bereits bei der Aufnahme Bildinformationen verloren gehen und sich die nachträgliche Bearbeitung schwieriger gestaltet.

4.3.2) Fingerabdrücke einscannen

Eine weitere Methode, mit der ein zum Vorschein gebrachter Fingerabdruck digitalisiert werden kann, ist das Einscannen des Abdrucks (1). Bei den durchgeführten Versuchen wurden zwei Arten von Scannern verwendet – zwei Desktopscanner und ein Dia-Scanner. Hierbei muss beachtet werden, dass in beiden Fällen der zu digitalisierende Abdruck in scanbarer Form vorliegen muss. Das heißt, der Gegenstand, auf dem sich der Abdruck befindet, muss eine flache Oberfläche haben und darf eine bestimmte Maximalgröße (sowie ein etwaiges Maximalgewicht) nicht überschreiten. Beim Diascanner sind diese Einschränkungen noch strikter, da es möglich sein muss, das zu scannende Objekt in einen Diarahmen einzuspannen. Somit ergibt sich in der Regel nur die Möglichkeit den Fingerabdruck nach dem Sichtbarmachen mit einer Klebefolie zu nehmen, diese anschließend auf eine Trägerfolie zu kleben und mit dieser weiter zu arbeiten. Die Trägerfolie kann dann auch in alle nötigen Formen und Größen zurechtgeschnitten werden, sodass sie beispielsweise in einen Diarahmen passt. Ein Nachteil dieser Methode ist jedoch, dass das Abnehmen des Abdruckes mit Klebefolie beim ersten Mal klappen muss, da der ursprüngliche Abdruck dadurch meist zerstört wird. Dies war bei den Versuchen dieser Arbeit weniger schwerwiegend, da mit kooperativen Opfern gearbeitet wurde, im Fall eines ahnungslosen Opfers hat man jedoch oft nur einen brauchbaren Fingerabdruck, wodurch es fatal wäre, diesen zu zerstören.

4.3.2.1) Desktopscanner

Hierbei kamen zwei Geräte zum Einsatz: Der „ScanJet 5300c“ der Firma Hewlett-Packard mit einer optischen Auflösung von 1200 dpi sowie der „Pixma M610“ aus dem Hause Canon mit einer maximalen Auflösung von 4800 dpi.

Der Vorteil bei der Verwendung eines Desktopscanners im Vergleich zum Dia-Scanner liegt darin, dass auch größere flache Objekte direkt gescannt werden können. Hierbei muss allerdings dafür Sorge getragen werden, dass der Abdruck beim Einlegen in den Scanner nicht verwischt wird. Ist das Objekt von dem die Fingerabdrücke stammen jedoch nicht flach oder klein genug, so

müssen auch hier zunächst die Fingerabdrücke mit einer Klebefolie abgenommen und auf eine Trägerfolie aufgebracht werden. Durch die bereits erwähnte Gefahr des Verwischens von Fingerabdrücken ist diese Vorgehensweise auch bei kleinen flachen Objekten ratsam.

4.3.2.2) Dia-Scanner

Als Dia-Scanner wurde das Gerät „Coolscan V ED“ der Firma Nikon verwendet. Ein Vorteil gegenüber Desktopscannern ist zum einen eine recht hohe Auflösung (optische Auflösung von 4000 ppi), vor allem aber, dass der zu scannende Abdruck durch das Einspannen in den Diarahmen nicht verrutschen kann und automatisch „glatt“ aufliegt. Zugleich ergibt sich daraus allerdings auch ein Nachteil, da alle Objekte, auf denen sich Abdrücke befinden, die eingescannt werden sollen, zuerst in die richtige Form und Größe (Diarahmen) gebracht werden müssen. Dabei ist außerdem darauf zu achten, dass der Abdruck beim Einspannen in den Diarahmen nicht nachträglich verunreinigt, beziehungsweise verschmiert oder verzerrt wird.

4.4) Digitalisierte Fingerabdrücke verarbeiten

Was in keinem der bisherigen Artikel zum Täuschen von Fingerprint-Scannern genauer erwähnt wurde, ist die Nachbearbeitung des digitalisierten Fingerprints. Bei den Versuchen hat sich gezeigt, dass dieser Schritt für die weiteren Schritte (siehe 4.5.5) dringend nötig ist. Beim Digitalisieren der Abdrücke ist in der Regel der Kontrast zwischen sichtbar gemachten Papillarleisten und Hintergrund nicht stark genug, sodass sich bei einem Ausdruck des Fingerprints ohne Nachbearbeitung durch ein entsprechendes Programm, die Zwischenräume der Papillarleisten nicht deutlich genug vom restlichen Fingerabdruck abheben. Dies ist allerdings essenziell, da man den erhaltenen Fingerabdruck, wie in Kapitel 4.5.5 erklärt wird, auf Folie ausdrucken will, sodass die Zwischenräume lichtdurchlässig sind. Bei schlechtem Kontrast kann es passieren, dass die Zwischenräume allerdings nicht farblos, sondern als Grauwert dargestellt sind und entsprechend ausgedruckt werden. Ein weiteres Problem kann sich ergeben, wenn der Fingerabdruck keine einheitliche Hintergrundfarbe hat, sondern beispielsweise auf einem Foto vorliegt oder aus anderen Gründen mehrere Farben oder Strukturen (beispielweise Holz) zu erkennen sind. Hier wäre natürlich eine weitere Nachbearbeitung nötig um den Fingerabdruck vom Hintergrund zu trennen. In dieser Arbeit wird dies allerdings nicht näher beschrieben, da hierfür schon professionelle Kenntnisse im Umgang mit Grafikprogrammen erforderlich wären, über die eine Durchschnittsanwenderin/ein Durchschnittsanwender im Normalfall nicht verfügt. Es soll noch beleuchtet werden, mit welchen Programmen versucht wurde, den Fingerabdruck zu verbessern, und aufgezeigt werden, welche Methoden hierbei mehr beziehungsweise weniger Erfolg versprechend sind. Betrachtet werden hierbei lediglich digitalisierte Bilder von Abdrücken mit einheitlichem Hintergrund.

4.4.1 Vorgehensweisen bei der Nachbearbeitung

Bevor auf das Vorgehen und die erzielbaren Ergebnisse konkreter Programme eingegangen wird, sollen in den folgenden Absätzen kurz wesentliche Operationen skizziert werden, welche bei den Versuchen Verwendung fanden (52). Die meisten dieser Methoden erwiesen sich in den Versuchen auch als sehr nützlich, lediglich „Konturen schärfen“ (in Adobe Photoshop) erzeugte nicht die erhofften Resultate und konnte nicht wirklich überzeugen. Natürlich kann man auch mit anderen Methoden brauchbare Resultate erzielen, die vorgestellten Methoden ermöglichten es allerdings bei fast allen Bildern, zum gewünschten Ergebnis zu kommen. Manche der Methoden erwiesen sich auch als essenziell, um ein brauchbares Ergebnisbild zu erhalten. So ist ein Schwellenwertverfahren im Allgemeinen unabdingbar um eine ausdruckbare Schwarz-Weiß-Version des Bildes zu erhalten.

4.4.1.1) Grauwertspreizung/Histogrammspreizung

Bei der Grauwertspreizung (auch Histogrammspreizung genannt) handelt es sich um eine Erhöhung des Kontrasts von Graustufenbildern (56; 52). Diese beruht darauf, dass in solchen Bildern, oft nur ein geringes Spektrum der möglichen Grauwerte der gesamten Grauwertskala vorhanden ist. Durch die Grauwertspreizung werden die vorhandenen Grauwerte auf die gesamte Grauwertskala ausgedehnt, wodurch zuvor nahe beisammen liegende Grauwerte nun weiter auseinander liegen und somit der Kontrast erhöht wird. Durch diese Operation wird auch die weitere Bearbeitung des Bildes erleichtert, da es einfacher ist, einzelne Bereiche anhand des Grauwerts auszuwählen. Mithilfe der Histogrammspreizung können auch die Werte des gesamten RGB-Kanals gespreizt werden, sodass eine vorherige Umwandlung des Bildes in Graustufen nicht nötig ist.

4.4.1.2) Hochpassfilter

Ein Hochpassfilter wird auf ein Frequenzspektrum angewandt und lässt nur einen bestimmten Teil dieses Spektrums passieren (57). Auf ein Bild bezogen können somit nur all jene Teile des Bildes, welche oberhalb einer definierten Grenzfrequenz liegen, passieren, während jene Bildbereiche, die unterhalb dieser Frequenz liegen, abgeschwächt werden. Einfach gesagt hebt der Hochpassfilter somit starke Kontraste hervor, wohingegen ein schleichender Wechsel der Grauwerte unterdrückt wird. Durch das Verstärken der Kantenkontraste erscheint das Bild schärfer.

4.4.1.3) Schwellenwertverfahren (Binarisierung)

Die Binarisierung erzeugt aus einem Grauwert- oder Farbbild ein Schwarz-Weiß-Bild. Dies geschieht durch das sogenannte Schwellwertverfahren (58). Hierbei wird von der Benutzerin/vom Benutzer ein Schwellwert bestimmt, der angibt, ab welchem Wert die Grau- oder Farbwerte des Bildes auf die Farbe Schwarz beziehungsweise Weiß gemappt werden. Dies ist nötig, da die Fingerabdrücke, für die Herstellung einer Attrappen-Vorlage durch Ätzen aus Leiterplatten, auf Folie ausgedruckt werden müssen und dabei lediglich aus schwarzen,

lichtundurchlässigen Teilen und weißen (beziehungsweise transparenten) Teilen, welche das Licht durchlassen, bestehen dürfen.

4.4.1.4) Konturen scharfzeichnen

Bei dieser Operation versucht ein Programm automatisch Konturen im Bild zu finden und diese zu schärfen, während alle anderen Bereiche im aktuellen Zustand belassen werden (52). Nachdem ein Fingerabdruck aus dem Abbild von Papillarleisten besteht, solle ein Programm, welches über diese Funktionalität verfügt, diese leicht als Konturen ausmachen und somit schnell ein gutes Ergebnis erzielen können. Im Verlaufe der Tests musste allerdings festgestellt werden, dass diese Operation nur sehr selten zum gewünschten beziehungsweise erhofften Resultat führt.

4.4.2) Verarbeitung mit einfachen Grafikprogrammen

Da in dieser Arbeit auch getestet werden sollte, ob die Erzeugung von Attrappen mit einfachen Mitteln möglich ist, wurden in diesem Abschnitt auch einfache Programme auf ihre Tauglichkeit zur Verarbeitung der digitalisierten Fingerabdrücke getestet. Konkret wurden hier die Programme „Paint“ und „Gimp“ getestet, da diese beiden Programme bei Windows (Paint) beziehungsweise bei Linux-Distributionen (Gimp) mitgeliefert werden und somit für einen Großteil der Nutzer leicht zugänglich sind. Außerdem wurde mit „Paint.net“ ein weiteres Grafikprogramm getestet, welches gratis im Internet heruntergeladen werden kann und somit auch jeder Benutzerin/jedem Benutzer (mit Internetzugang) zur Verfügung steht.

4.4.2.1) Verarbeitung mit Paint

Bei dem mit dem Betriebssystem Windows ausgelieferten „Paint“ bestätigte sich schnell, was bereits vor Beginn der Versuche zu vermuten war: Das Programm ist für eine entsprechende Verarbeitung der Bilder nicht ausreichend geeignet und ermöglicht weder eine Histogramm- bzw. Grauwertspreizung noch eine Binarisierung durch Schwellenwertverfahren. Somit konnte das Programm bereits nach wenigen Versuchen endgültig als Möglichkeit zur Verarbeitung der Bilder ausgeschlossen werden.

4.4.2.2) Verarbeitung mit GIMP (59)

Gimp (Gnu Image Manipulation Program) ist für jeden zugänglich, da es unter der „GNU General Public Licence“ kostenlos ist und frei verwendet werden darf. In den Versuchen wurde das Programm in der Version 2.6 verwendet. Gimp ist für alle gängigen Plattformen verfügbar und in manchen Linux Distributionen bereits enthalten. Im Gegensatz zu Paint handelt es sich bei Gimp allerdings nicht um ein einfaches „Zeichenprogramm“ sondern tatsächlich um ein Bildbearbeitungsprogramm. Auch wenn manche Funktionen nicht auf Anhieb zu finden sind, verfügt das Programm durchaus über Filter und Operationen, mit welchen die Bilder verbessert werden konnten. Konkret konnten mit zwei Vorgehensweisen brauchbare Ergebnisse erzeugt werden (52): Zum einen über die Operation „Kanten finden“ (mit LaPlace Algorithmus) mit anschließender Invertierung und zum anderen über die Anpassung der Farbkurven im Dialogfeld

„Kurven“. Bei beiden Vorgehensweisen wurde als letzter Schritt ein Schwellenwertverfahren durchgeführt. Im Folgenden sollen beide Vorgehensweisen mit Beispielbildern veranschaulicht werden. Die Bilder der Fingerabdrücke sind hierbei absichtlich vergrößert, damit die Unterschiede und Veränderungen in den feinen Strukturen der Papillarleiste besser zu erkennen sind.

„Abbildung 15: Ausgangsbild“ zeigt das Bild vor Beginn des Verfahrens, als noch keinerlei Veränderungen vorgenommen worden sind. (Rohzustand).

Abbildung 15: Ausgangsbild

Als erster Schritt wurde nun der Dialog „Kurven“ aufgerufen („Abbildung 16: Korrektur der Farbkurve“), welcher das Histogramm des Bildes darstellt und in dem die Farbkurven verändert werden können. Mithilfe dieser Funktion konnten dunkle Farben verstärkt und helle Farben abgeschwächt werden, um einen besseren Kontrast zu erhalten. Das Ergebnis dieser Operation ist in „Abbildung 17: Erzielte Änderungen“ zu sehen.

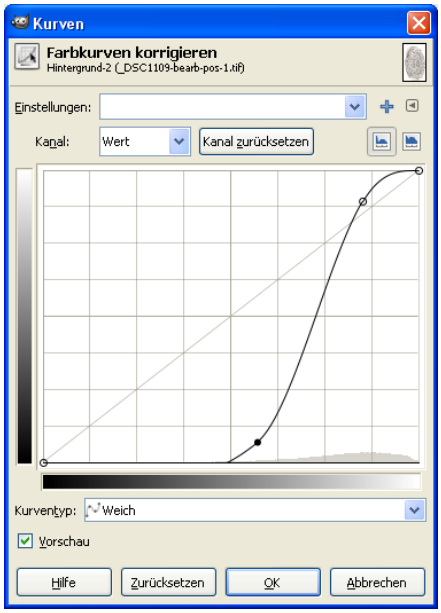

Abbildung 16: Korrektur der Farbkurve

Abbildung 17: Erzielte Änderungen

Abschließend wurde das Bild mithilfe des Schwellenwertverfahrens in ein Schwarz-Weiß Bild umgewandelt. Hierzu wurde über den entsprechenden Dialog („Abbildung 18: Schwellenwertverfahren“) ein Schwellwert definiert. Das Resultat ist in „Abbildung 19: Endergebnis“ zu sehen.

Abbildung 18: Schwellenwertverfahren

Abbildung 19: Endergebnis

Auch die zweite Vorgehensweise soll nun veranschaulicht werden. Um einen besseren Vergleich zu haben, wurde hierbei ebenfalls mit dem Bild aus „Abbildung 15: Ausgangsbild“ gearbeitet. Zunächst wurde bei diesem Verfahren allerdings die Funktion „Kanten finden“ aufgerufen (Abbildung 20: Filter "Kanten finden"). Hier wurde als Algorithmus „LaPlace“ gewählt. Das Anwenden dieses Filters auf das Bild erzeugt jedoch ein Negativbild, bei dem die vom Algorithmus gefundenen Kanten hervorgehoben sind („Abbildung 21: Ergebnis“). Dies wird kompensiert, indem anschließend eine Invertierung ausgeführt wird. Das Ergebnis ist in „Abbildung 22: Invertierung“ zu sehen.

Abbildung 20: Filter "Kanten finden"

Abbildung 21: Ergebnis

Abbildung 22: Invertierung

Abschließend wurde auch hier wie bei der zuvor beschriebenen Vorgehensweise ein Schwellenwertverfahren angewandt, um das Bild zu binarisieren, was noch eine geringfügige Verbesserung bringt („Abbildung 23: Endergebnis nach Schwellwert“).

Abbildung 23: Endergebnis nach Schwellwert

4.4.2.3) Verarbeitung mit Paint.net

Bei „Paint.net“ handelt es sich wie bei GIMP um ein frei verfügbares Programm, welches kostenlos im Internet heruntergeladen werden kann. Das Programm ist im Gegensatz zu GIMP jedoch nicht für mehrere Plattformen verfügbar, sondern auf die Windows-Plattform beschränkt. Wie der Name bereits verrät, ist das Programm eine Art Erweiterung von dem ebenfalls getesteten Programm „Paint“ und war ursprünglich auch als Gratis-Ersatz für das in Kapitel 4.4.2.1 beschriebene Programm gedacht. Im Vergleich zum Original „Paint“ bietet „Paint".net“ durch diverse Erweiterungen einen viel größeren Funktionsumfang, wodurch es auch für die Verarbeitung von digitalisierten Fingerabdrücken infrage kommt. In allen Verarbeitungsschritten dieser Arbeit wurde die Version 3.36 von „Paint.net“ verwendet. Konkret konnten zwei Ansätze gefunden werden, mithilfe derer sich das Fingerlinienbild deutlich verbessern lässt. Ausgehend vom Ausgangsbild, auch hier wird zwecks besserer Vergleichbarkeit mit dem Ausgangsbild „Abbildung 15: Ausgangsbild“ gearbeitet, wurde zunächst eine Umwandlung in ein Schwarz-Weiß-Bild durchgeführt. Die Schwarz-Weiß-Umwandlung erfolgt hierbei automatisch und das Ergebnis der Umwandlung kann in „Abbildung 24: Schwarz-Weiß-Umwandlung in Paint.net“ genauer betrachtet werden.

Abbildung 24: Schwarz-Weiß-Umwandlung in Paint.net

Anschließend wurde durch die Option „manuelle Anpassung“ im Menü „Korrekturen“ eine Tonwertspreizung durchgeführt (siehe „Abbildung 25: Tonwertspreizung in Paint.net“). Durch diese Operation erhält man im Vergleich zum Schwarz-Weiß-Bild bereits deutlich bessere Konturen (siehe „Abbildung 26: Ergebnis“).

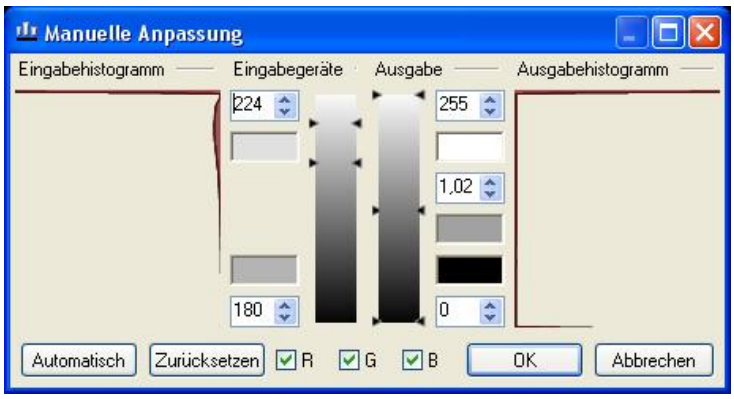

Abbildung 25: Tonwertspreizung in Paint.net

Abbildung 26: Ergebnis der Tonwertspreizung

Abschließend wurde noch eine Tontrennung durchgeführt (siehe „Abbildung 27: Tonwerttrennung in Paint.net“), was jedoch nur noch eine mit freiem Auge kaum merkliche Verbesserung brachte (siehe „Abbildung 28: Ergebnis der Tonwerttrennung“).

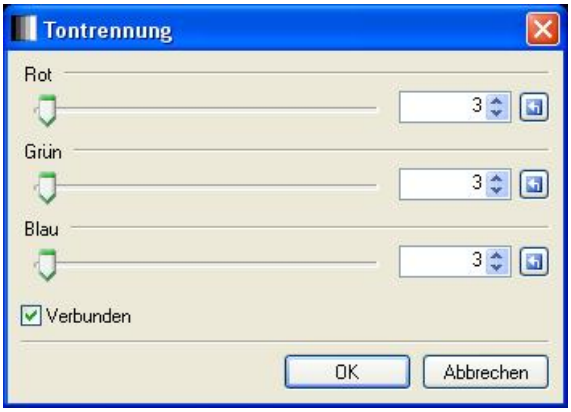

Abbildung 27: Tonwerttrennung in Paint.net

Abbildung 28: Ergebnis der Tonwerttrennung

Eine Variante dieses Vorgehens ist die Verwendung der Option „Kurven“ im Menüpunkt „Korrekturen“. Durch eine entsprechende Einstellung der Kurve wird erreicht, dass dunkle Bereiche noch dunkler und helle Bereiche noch heller dargestellt werden. Wie die Kurve hierfür genau einzustellen ist, kann nicht verallgemeinert werden und muss von Bild zu Bild erneut optimiert werden. Im konkreten Beispiel wurde mit der in „Abbildung 29: Funktion „Kurven“ in Paint.net“ gezeigten Kurve ein gutes Ergebnis erzielt (siehe „Abbildung 30: Ergebnis nach Anpassung der Kurve“). Anschließend wurde auch hier wieder eine Tonwerttrennung durchgeführt, was das Ergebnis jedoch wiederum nur kaum wahrnehmbar verbesserte.

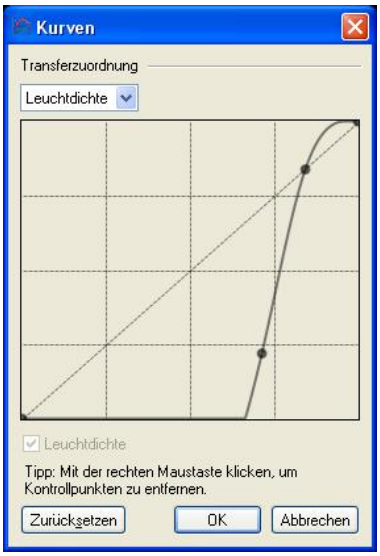

Abbildung 29: Funktion „Kurven“ in Paint.net

Abbildung 30: Ergebnis nach Anpassung der Kurve

4.4.3) Verarbeitung mit professionellen Grafikprogrammen

Im Unterschied zum vorigen Unterkapitel sollen nun auch professionelle Grafikprogramme auf Möglichkeiten getestet werden, einen digitalisierten Fingerabdruck nachzubearbeiten. Die im Folgenden vorgestellten Programme sind alle lizenzpflichtig und ihre Anschaffung ist daher durchaus kostenintensiv. Obwohl aus eben diesem Grund nicht anzunehmen ist, dass eine Durchschnittsanwenderin/ein Durchschnittsanwender die Programme verwendet, sollen die Programme im Rahmen dieser Arbeit beleuchtet werden, weil auch betrachtet werden soll, ob der Einsatz solcher Programme einen entscheidenden Vorteil bringt.

4.4.3.1) Verarbeitung mit Adobe Photoshop

Eines der am weitest verbreitetsten Grafikprogramme ist Adobe Photoshop. In dieser Arbeit wurde zur Bearbeitung der Bilder die Version „Adobe Photoshop CS 3“ verwendet. Das Programm bietet der Nutzerin/dem Nutzer eine Vielfalt von Möglichkeiten an, um ein Bild nachzubearbeiten. Im Folgenden sollen kurz die Werkzeuge und Filter, welche bei der Bearbeitung der Fingerabdruckbilder verwendet wurden, erläutert werden. Außerdem soll gezeigt werden in welcher Reihenfolge sie in den Versuchen angewandt und welche Ergebnisse damit erzielt wurden.

Zu Beginn der Versuche mit Adobe Photoshop CS 3 wurde das zu bearbeitende Foto zunächst auf ein Grauwertbild umgewandelt, falls das Originalfoto nicht bereits in Graustufen oder als Schwarz-Weiß-Bild vorlag. Dies geschah entweder über die Funktion „Graustufen“ oder aber indem im Dialogfeld der Funktion „Schwarzweiß“ die Regler der einzelnen Farbkanäle entsprechend der Erfordernisse angepasst wurden. Es zeigte sich im Verlauf der Versuche jedoch, dass dies nicht zwingend nötig war und die Bearbeitung auch direkt am Farbfoto durchgeführt werden konnte, wie auch in den Beispielen weiter unten zu sehen sein wird.

Anfangs wurde mit den einzelnen Bildern experimentiert, um herauszufinden, welche Bildanpassungen und Filter zum besten Ergebnis führen. Bei den ersten Versuchen mit nennenswerten Ergebnissen wurde lediglich der Filter „Konturen scharfzeichnen“ mehrmals angewendet (52). Obwohl dies bei manchen Bildern durchaus zu einer Verbesserung führte, waren die Ergebnisse, die dadurch erzielt wurden, nicht annähernd so gut wie erhofft. Deshalb wurde dieses Verfahren nach mehreren Versuchen mit verschiedenen Bildern höchstens in Kombination mit anderen Filtern oder Operationen verwendet.

Bessere Ergebnisse wurden in weiterer Folge erzielt, wenn die Bilder mithilfe der Funktion „Tonwertkorrektur“ (Grauwertspreizung) bearbeitet und anschließend mit der Funktion „Schwellwert“ (Schwellwertverfahren) binarisiert wurden (52). Dies führte in den meisten Fällen bereits zu durchaus passablen Ergebnissen. Ähnlich gute Ergebnisse wurden durch die Anwendung eines Hochpass-Filters mit anschließendem Schwellwertverfahren erzielt (52). Welche der beiden zuletzt genannten Methoden das jeweils beste Bild erzeugt, kann nicht konkret gesagt werden und war in den Versuchen von Bild zu Bild unterschiedlich.

Die folgenden Bilder sollen die einzelnen Schritte sowie die dadurch erzielten Ergebnisse ein wenig verdeutlichen. Die abgebildeten Abdrücke entsprechen natürlich nicht dem Original. Sie wurden vergrößert, damit die feinen Strukturen besser sichtbar und somit auch die Unterschiede deutlicher zu erkennen sind.

In „Abbildung 31: Bild und Histogramm vor der Bildverarbeitung“ ist das Bild vor den einzelnen Verarbeitungsschritten zu sehen. Die einzige Bearbeitung, die das Bild erfahren hat, ist die Entfernung der irrelevanten Bildteile (welche nicht Teil des Fingerabdruckes sind). In dieser Phase sind die Strukturen recht blass und nicht gut zu erkennen. Im Histogramm des Bildes ist jedoch zu erkennen, dass ein Großteil der Farben sehr eng beisammen liegt.

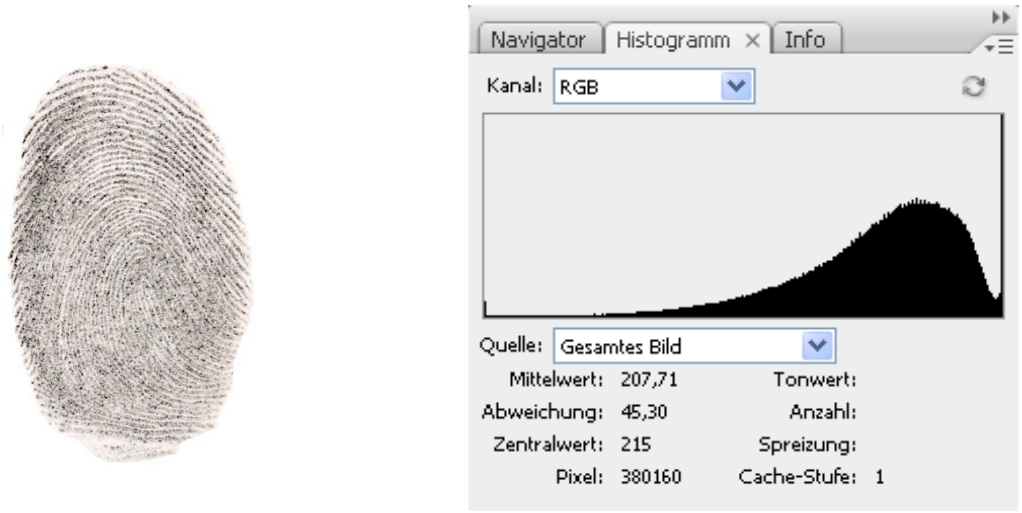

Abbildung 31: Bild und Histogramm vor der Bildverarbeitung

Daher wurde als erster Schritt eine Histogrammspreizung vorgenommen (siehe „Abbildung 32: Histogrammspreizung“). In Photoshop ist dies durch die Operation „Tonwertkorrektur“ zu erreichen. Im entsprechenden Dialogfeld kann

eingestellt werden, welcher Bereich des Histogrammes verwendet werden soll. Dadurch wurde der kleine Bereich der Skala, welcher die meisten Farbanteile enthält, auf die gesamte Skala aufgespannt, wodurch die Granularität der Farbunterschiede feiner wurde und das Histogramm somit flacher.

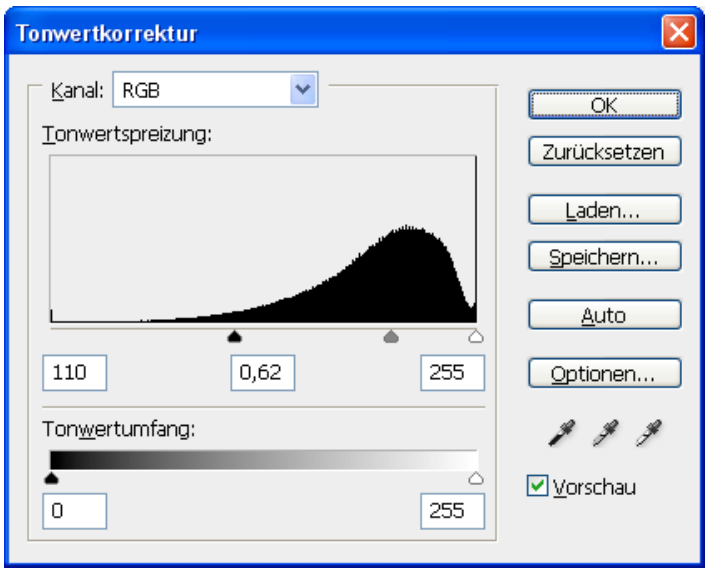

Abbildung 32: Histogrammspreizung

„Abbildung 33: Fingerabdruck und Histogramm nach der Histogrammspreizung“ zeigt, welchen Effekt die Spreizung des Histogrammes auf das Bild des Fingerabdruckes hatte. Die vorhandenen Farben sind nun viel intensiver und auch die Strukturen sind besser erkennbar.

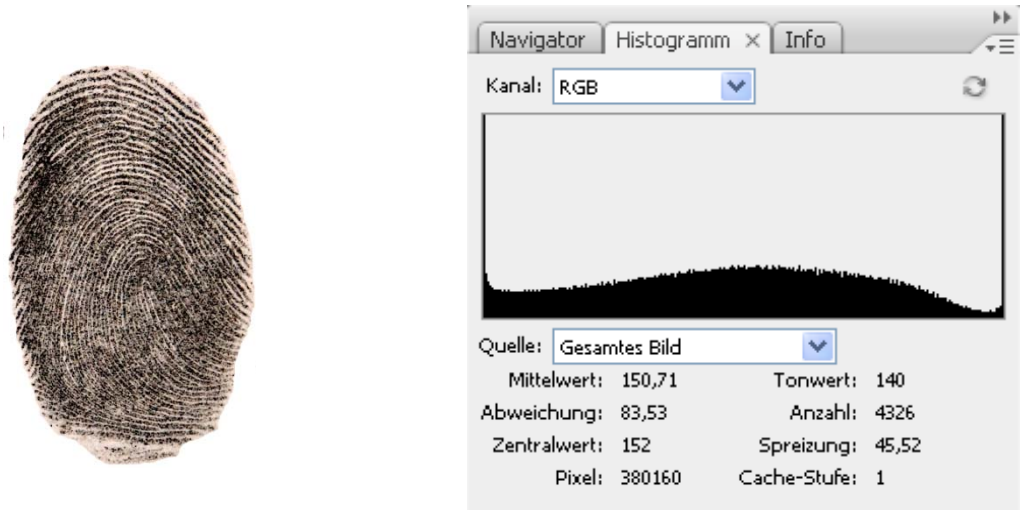

Abbildung 33: Fingerabdruck und Histogramm nach der Histogrammspreizung

Für die Weiterverarbeitung des Fingerabdruckbildes und den dafür nötigen Ausdruck auf Folie muss der Abdruck nun noch binarisiert werden. Dies geschieht wie bereits ausgeführt durch Anwendung des sogenannten Schwellenwertverfahrens. Hierfür wird für die im Bild vorhandenen Farbwerte ein Referenzwert gewählt. Alle Farbwerte, die höher sind als der Referenzwert, werden im Ergebnisbild der Operation weiß dargestellt, alle Werte, die niedriger sind, werden in die Farbe Schwarz umgewandelt. In „Abbildung 34: Schwellwertverfahren - Bestimmung des Referenzpunktes“ ist die Auswahl des

Referenzpunktes zu sehen. So kann der Referenzwert im entsprechenden Dialogfeld entweder durch Eingeben eines konkreten Wertes, oder aber durch Verschieben des Pfeiles unterhalb des Histogrammes definiert werden. Hierbei hat es sich als hilfreich erwiesen, die Vorschauoption einzuschalten und einfach ein bisschen herum zu probieren, um den idealen Referenzwert für das jeweilige Bild herauszufinden.

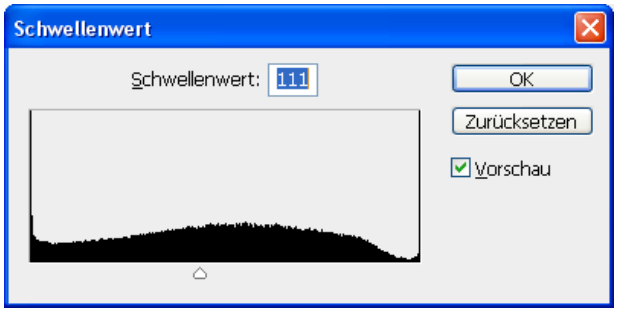

Abbildung 34: Schwellwertverfahren - Bestimmung des Referenzpunktes

„Abbildung 35: Endergebnis der Bildverarbeitung“ schließlich zeigt das Ergebnis des Schwellenwertverfahrens und zugleich das Endergebnis der Bildbearbeitung: Ein Fingerabdruckbild, in welchem klar strukturierte Papillarleisten zu erkennen sind und welches durch die Binarisierung lediglich aus den Farben Schwarz und Weiß besteht. Es kann daher ausgedruckt und zur Belichtung einer Leiterplatte verwendet werden.

Abbildung 35: Endergebnis der Bildverarbeitung

Als Alternative zu diesem Vorgehen kann der Hochpassfilter verwendet werden. Dieses Vorgehen führt in der Regel zu ähnlich guten und zum Teil sogar besseren Ergebnissen. Noch dazu ist es in der Anwendung einfacher. Um ein Bild mit diesem Verfahren zu bearbeiten, muss in Photoshop auf das Ausgangsbild (in diesem Fall wieder das Bild von „Abbildung 31: Bild und Histogramm vor der Bildverarbeitung“) lediglich der Hochpassfilter (Filter -> Sonstige Filter -> Hochpass) angewandt werden. Das Ergebnis dieses Aufrufes ist in „Abbildung 36: Hochpassfilter“ zu sehen. Anschließend kann auch hier wieder mit dem Schwellenwertverfahren (Bild -> Anpassungen -> Schwellenwert) ein Binärbild erzeugt werden, welches sich zur Weiterverarbeitung eignet (siehe „Abbildung 37: Endergebnis nach Schwellenwert“).

Abbildung 36: Hochpassfilter

Abbildung 37: Endergebnis nach Schwellenwert

Eine weitere Methode um in Photoshop zu einem passablen Ergebnis zu kommen ist die Umwandlung in ein Graustufenbild (52). Hierbei ist vom Gebrauch der automatischen Konvertierung (Bild -> Modus -> Graustufen) abzuraten. Viel mehr sollte man die Funktion „Schwarzweiß“ (Bild -> Anpassungen -> Schwarzweiß) benutzen, um selbst einstellen zu können, welche Farbkanäle aufgehellt (weißer) und welche abgedunkelt (schwärzer) dargestellt werden sollen (siehe Abbildung 38: Dialog "Schwarzweiß"). Das Ergebnis dieser Methode ist in „Abbildung 39: Umgewandelt in Graustufen“ zu sehen. Anschließend kann wiederum mit dem Schwellenwert Verfahren ein für den weiteren Versuchsverlauf nötiges Schwarz-Weiß-Bild erzeugt werden (siehe „Abbildung 40: Endergebnis nach Schwellenwert“).

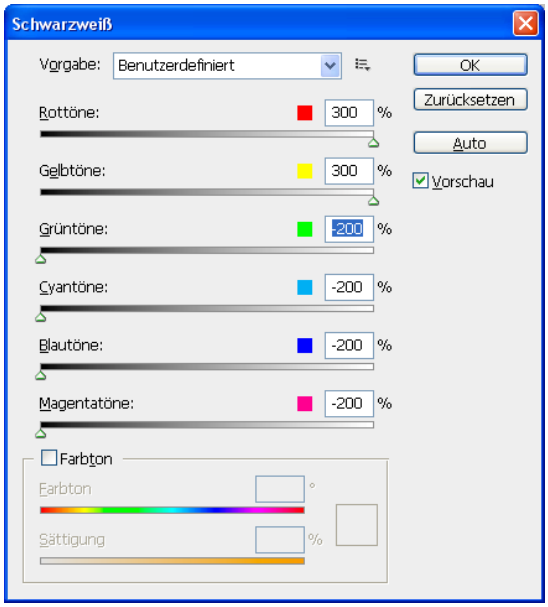

Abbildung 38: Dialog "Schwarzweiß"

Abbildung 39: Umgewandelt in Graustufen

Abbildung 40: Endergebnis nach Schwellenwert

4.4.3.2) Verarbeitung mit Adobe Lightroom

Lightroom ist ein professionelles Fotoverarbeitungsprogramm und wurde ebenso wie das im vorigen Kapitel vorgestellte Programm „Photoshop“ von der Firma Adobe entwickelt. In sämtlichen mit diesem Programm durchgeführten Tests wurde die Version 2.3 verwendet. Obwohl es sich um ein sehr ausgereiftes Programm handelt, mithilfe dessen die unterschiedlichsten Aspekte einer Fotografie verbessert werden können, musste festgestellt werden, dass letztlich eher die nachträgliche Verbesserung von Kameraeinstellungen, wie Belichtung oder Farbtemperatur, möglich ist und weniger Änderungen, wie sie in einem Grafikprogramm möglich sind, getätigt werden können. So ist es mit Lightroom nicht möglich, einen Filter oder ein Schwellenwertverfahren auf das Bild eines Fingerabdruckes anzuwenden. Nach einigen Versuchen wurden allerdings doch noch Möglichkeiten gefunden, wie die Qualität eines Fingerprintbildes verbessert und das Bild entsprechend aufgewertet werden kann. So ist es zwar mit anderen Programmen einfacher Verbesserungen vorzunehmen und die Qualität des Bildes wird bei der Verwendung anderer Grafikprogramme zum Teil besser, es ist jedoch immerhin möglich, eine solche Verbesserung zu erwirken, dass auch dieses Programm durchaus zur Erzeugung einer Folienvorlage zum Belichten einer Leiterplatte genutzt werden kann.

Auch in diesem Kapitel wird die Bearbeitung mit Adobe Lightroom exemplarisch am gleichen Fingerlinienbild durchgeführt wie in den vorherigen Kapiteln zur Bildbearbeitung, um der Leserin/dem Leser eine gute Vergleichsmöglichkeit zu den anderen Programmen und den damit erzielbaren Resultaten zu bieten. Das Ausgangsbild (siehe „Abbildung 41: Bild in Rohzustand“) wurde in einem ersten Schritt zur Nachbearbeitung auch in Lightroom wieder in ein Graustufenbild umgewandelt. Hier muss erwähnt werden, dass die Option, mit welcher diese Umwandlung durchgeführt wird, nicht auf den ersten Blick ersichtlich ist und erst nach einer Weile gefunden wurde. Die Umwandlung funktionierte einwandfrei und lieferte bereits eine erste Verbesserung (siehe „Abbildung 42: Umwandlung in Graustufen“).

Abbildung 41: Bild in Rohzustand

Abbildung 42: Umwandlung in Graustufen

Ist dieser Schritt vollzogen, bietet Lightroom eine Vielzahl an Möglichkeiten, das Bild weiter zu verbessern. All diesen Möglichkeiten ist jedoch gemein, dass sie viel Fingerspitzengefühl und Geduld benötigen. Auch muss hier nochmals das Fehlen eines Schwellenwertverfahrens (einer Umwandlung in ein reines Schwarz-Weiß Bild) in Adobe Lightroom betont werden, weshalb durch die Bildbearbeitung zwar durchaus Verbesserungen erzielt werden können, das Ergebnis allerdings nie ein Binärbild, sondern immer nur ein Graustufenbild, ist.

Eine Möglichkeit das Fingerlinienbild mit Adobe Lightroom zu bearbeiten, bieten die Grundeinstellungen. Hierbei können über Schieberegler die Belichtungszeit sowie der Schwarzanteil erhöht oder verringert werden. Stellt man eine längere Belichtungsdauer ein, wird das gesamte Bild heller. Durch zusätzliches Erhöhen der Schwarzanteile bleiben die dunklen Fingerlinien gut sichtbar, die restlichen Bildteile (die Täler des Fingerlinienbildes) werden jedoch durch die erhöhte Belichtung nahezu weiß. Durch Einstellen der Regler Helligkeit und Kontrast kann das Ergebnis in den meisten Fällen noch ein wenig verbessert werden. Ebenso steigt die Qualität des Bildes noch geringfügig, wenn der Schieberegler der Option „Klarheit“ erhöht wird. Die Einstellungen sowie das dadurch erzielte Ergebnis können in „Abbildung 43: Schieberegler der Grundeinstellungen“ und „Abbildung 44: Erzieltes Ergebnis“ gesehen werden.

Abbildung 43: Schieberegler der Grundeinstellungen

Abbildung 44: Erzieltes Ergebnis

Eine weitere Möglichkeit das Bild zu verbessern ist die Anpassung der Gradationskurve. Hierbei ist es in Adobe Lightroom nicht möglich die Kurve beliebig zu ändern. Die Gradationskurve ist viel mehr in die vier Abschnitte „Tiefen“, „dunkle Farbtöne“, „helle Farbtöne“ und „Lichter“ unterteilt, wobei die Gradationskurve in jedem dieser Teile einzeln angepasst werden muss (siehe „Abbildung 45: Einstellung der Gradationskurve“). Das Programm bietet jedoch noch eine weitere Möglichkeit, die Gradationskurve den jeweiligen Wünschen entsprechend anzupassen. Durch einen Klick auf das Symbol in der linken oberen Ecke kann direkt im Bild operiert werden. Durch das Klicken an eine Stelle des Bildes und anschließendes Bewegen der Maus, während die Maustaste gedrückt bleibt, kann der Graustufenbereich, welcher an dem entsprechenden Bereich gemessen wird, aufgehellt oder abgedunkelt werden. Die dadurch entstehenden Änderungen können zeitgleich in der Darstellung der Gradationskurve verfolgt werden. Durch eine entsprechende Änderung der Kurve auf die eine oder andere Art können die dunklen Bereiche des Bildes noch dunkler gemacht und die hellen Bereiche noch ein wenige aufgehellt werden, wodurch der Kontrast deutlich erhöht und die Qualität dadurch verbessert wird. Das Ergebnis der so herbeigeführten Änderung kann in „Abbildung 46: Ergebnis der Änderung“ gesehen werden.

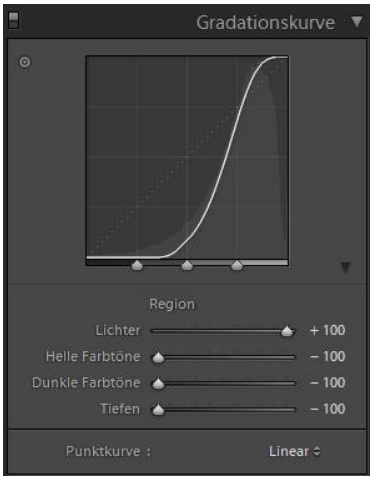

Abbildung 45: Einstellung der Gradationskurve

Abbildung 46: Ergebnis der Änderung

Das Ergebnis kann noch weiter verbessert werden, wenn zusätzlich zur Anpassung der Gradationskurve mithilfe der Regler unterhalb der Kurve eine Tonwertspreizung durchgeführt wird. Dadurch entfallen einige Graustufen aus dem Bild, wodurch ein noch deutlicherer Unterschied zwischen Stegen und Tälern des Fingerlinienbildes zu erkennen ist. Die durch die zusätzliche Grauwertspreizung erzielten Änderungen kann man in „Abbildung 48: Ergebnis der Grauwertspreizung“ sehen.

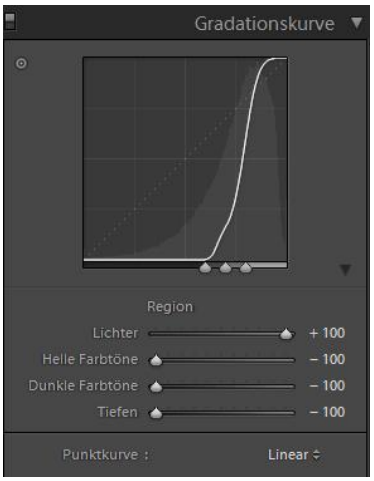

Abbildung 47: Grauwertspreizung

Abbildung 48: Ergebnis der Grauwertspreizung

4.4.3.3) Verarbeitung mit Capture NX 2

Capture NX ist ein Bildbearbeitungsprogramm der Firma Nikon, welches prinzipiell zur Nachbearbeitung von Fotos gedacht ist. Da die Software darüber hinaus auch einige Möglichkeiten zur Anwendung diverser Filter bietet, wurde sie auch für die Versuche im Rahmen dieser Arbeit interessant. In allen Bearbeitungsschritten, welche mit dem Programm Capture NX durchgeführt wurden, um das vorliegende Bild eines Abdruckes digital zu verbessern und für die späteren Arbeitsschritte vorzubereiten, wurde die Version 2.0.1 der Software verwendet.

Auf den ersten Blick erschien die Software nicht sonderlich geeignet, um zur Nachbearbeitung von Fingerprintbildern verwendet zu werden, da sie über keine Bearbeitungsoption verfügt, welche einem Schwellenwertverfahren entspricht. Um diesem Mangel zu begegnen, wurde bei der Verwendung von Farbbildern, zu Beginn der Bearbeitung, die Funktion „Schwarz-Weiß-Konvertierung“ durchgeführt. Diese Anpassungsoption erlaubt zwar nicht den gewünschten Schwellenwert einzustellen, welcher angibt, ab welchem Farbcode die Pixel in Schwarz beziehungsweise Weiß konvertiert werden sollen, es erzeugt aber immerhin ein Schwarz-Weiß-Bild, was für die weitere Verarbeitung und Verwendung als Schablone zur Belichtung von Leiterplatten essenziell ist.

In weiterer Folge konnte mit Capture NX auf zwei Arten eine Verbesserung des Fingerlinienbildes erzeugt werden: Zum einen durch die Anwendung eines Hochpassfilters, ähnlich wie bereits bei Photoshop, zum anderen durch die Anpassungsfunktion „Tonwerte und Kurven“, welche in etwa der Anwendung der Funktion „Kurven“ bei der Bildverarbeitung mit GIMP (siehe Kapitel 4.4.2.2) entspricht. Die Vorgehensweise und die damit erzielten Ergebnisse sollen auch hier kurz durch die folgenden Bilder verdeutlicht werden. Um einen besseren Vergleich zu den durch andere Programme möglichen Änderungen zu haben, wird auch hier wieder die Bearbeitung exemplarisch an demselben Fingerabdruckbild gezeigt wie in den vorigen Kapiteln.

Abbildung 49: Ausgangsbild für Capture NX

Ausgehend vom Bild in „Abbildung 49: Ausgangsbild für Capture NX“ wurde zunächst die Anpassung „Schwarz-Weiß-Konvertierung“ durchgeführt, wobei Helligkeit und Kontrast je nach Bild individuell angepasst werden mussten. Hier im Beispiel konnten mit Helligkeit -66 und Kontrast +19 gute Ergebnisse erzielt werden, wie man in „Abbildung 50: Einstellung der Schwarz-Weiß-Konvertierung“ und „Abbildung 51: Ergebnis der Konvertierung“ sehen kann.

Abbildung 50: Einstellung der Schwarz-Weiß-Konvertierung

Abbildung 51: Ergebnis der Konvertierung

Auf das somit erhaltene Binärbild konnte nun ein Hochpassfilter angewandt werden („Abbildung 52: Einstellung des Hochpassfilters“). Das Ergebnis dieser Operation sieht man in „Abbildung 53: Ergebnis des Hochpassfilters“.

Abbildung 52: Einstellung des Hochpassfilters

Abbildung 53: Ergebnis des Hochpassfilters

Ein ähnlich gutes Ergebnis wird dadurch erzielt, dass in dem durch die Schwarz-Weiß-Konvertierung entstandenen Binärbild die Einstellungen der Anpassungsoption „Tonwert und Kurven“ (siehe „Abbildung 54: Einstellungen „Tonwerte und Kurven“) geändert werden, sodass ein besserer Kontrast erzielt wird. Wie die Einstellungen hierfür geändert werden müssen, ist von Bild zu Bild verschieden. Man kann sich der optimalen Einstellung nur durch mehrere Versuche immer weiter annähern. Eine gewisse Hilfestellung bieten hierbei jedoch die Funktionen „Weißpunkt festlegen“ und „Schwarzpunkt festlegen“, wodurch man recht schnell eine brauchbare Kurvenform erreicht, welche dann nur noch durch weitere kleine Änderungen angepasst werden muss. Allerdings muss man auch beim Setzen der Referenzpunkte Vorsicht walten lassen, da es bei den feinen Strukturen der Fingerlinien oft schwer ist, genau die gewünschte Stelle des Bildes anzuklicken. So bedurfte es oft mehrerer Versuche, bis die Punkte an die jeweiligen Positionen gebracht werden konnten.

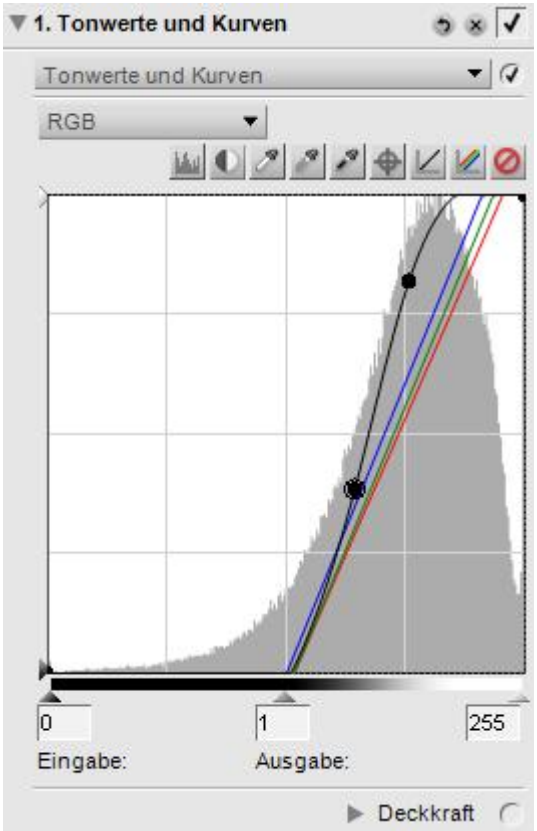

Abbildung 54: Einstellungen „Tonwerte und Kurven“ Abbildung 55: Fingerprint nach der Anpassung

4.5) Erstellen der Vorlagen für Fingerabdruck-Attrappen

Um Fingerabdruck-Attrappen herzustellen, muss zunächst eine Vorlage erstellt werden, mit deren Hilfe letztendlich die Attrappen gegossen werden können. In den Versuchen wurde zunächst von einem kooperativen Opfer ausgegangen (3; 45; 36), weshalb auch Fimo-Vorlagen (siehe 4.5.1) und Wachs-Vorlagen (siehe 4.5.2) in den Versuchen verwendet wurden. Hierfür kann man natürlich alle bisher genannten Punkte (Fingerabdruck nehmen und nachbearbeiten) außen vor lassen und direkt mit dem Erstellen der Attrappen-Vorlage beginnen. Als höher gestecktes Ziel wurde jedoch das Erstellen einer Vorlage eines

ahnungslosen Opfers gesetzt (36; 45; 1). Hierfür sind alle in den vorigen Kapiteln beschriebenen Phasen nötig um eine Vorlage herstellen zu können.

4.5.1) Erstellen von Vorlagen aus Modelliermasse

In den Versuchen wurden die Produkte „Fimo Classic“ und „Fimo Soft“ der Firma „Eberhard Faber GmbH.“ (60) als Modelliermasse verwendet, da diese leicht verfügbar ist und einfach in einem Heißluftherd gebrannt werden kann und dadurch aushärtet. Die Erstellung von Fimo-Vorlagen mit einem kooperativen Opfer ist daher denkbar einfach. Das „Opfer“ muss lediglich einen Finger fest genug auf ein Stück der Modelliermasse drücken und diese muss entsprechend der Anleitung (bei Fimo Classic und Fimo Soft ca. 30 Minuten bei 110 Grad) gebrannt werden. Es ist jedoch darauf zu achten, dass nicht zu fest auf die Masse gedrückt wird, da es dadurch schwieriger wird eine Attrappe zu gießen, da zum Ausgießen der Form mehr Material benötigt wird, wodurch die Attrappe langsamer trocknet und oft nur schwer aus der Form zu lösen ist. Zu achten ist des Weiteren darauf, dass die gefertigten Fimo-Vorlagen auf einem ebenen Untergrund gebrannt werden, da es sonst passieren kann, dass sich die Vorlage während des Brennvorgangs verzieht und somit nicht mehr zu gebrauchen ist.

Dieses Vorgehen findet aus naheliegenden Gründen nur bei Versuchen mit einem kooperativen Opfer Verwendung. In der realen Welt, abseits der Versuchsanordnung, wo man mit einem ahnungslosen Opfer konfrontiert ist, gestaltet sich die Herstellung einer Attrappen-Vorlage entsprechend schwieriger.

4.5.2) Erstellen von Wachs-Vorlagen

Das Erstellen der Vorlagen aus Wachs ist ähnlich dem Vorgehen mit der Modelliermasse. Im Unterschied dazu muss Wachs zunächst erhitzt und der Finger des Opfers ins warme Wachs gepresst werden, welches dann durch seine Abkühlung aushärtet. Dennoch erwies sich dieses Vorgehen als weniger geeignet, da sich die Wachsvorlage selbst im ausgehärteten Zustand noch zu leicht verformen lässt. Hinderlich war auch, dass der Finger bis zum Aushärten der Vorlage ins Wachs gepresst werden musste, um zu verhindern, dass das Wachs nachträglich zusammen rinnt. In den Versuchen wurde das Wachs von Kerzen mit Stearinanteil der Firma „Gala – World of Candles“ verwendet.
Zu beachten ist bei der Erstellung einer solchen Vorlage außerdem, dass das Wachs vor dem Hineindrücken des Fingers bereits ein wenig ausgekühlt sein sollte, da das kooperative Opfer sonst beim Erstellen der Vorlage leicht Brandwunden am Finger erleiden kann.

Auch hier muss angemerkt werden, dass diese Methode zur Herstellung von Vorlagen natürlich nur dann anwendbar ist, wenn man mit einem kooperativen Opfer arbeitet.

4.5.3) Erstellen von Vorlagen durch Ausdruck auf Folie

Das Erstellen einer Vorlage durch einfaches Ausdrucken des Fingerabdruckes auf eine Folie wurde deshalb versucht, da es in einem recht bekannten Artikel des CCC (Chaos Computer Club) als einfache Möglichkeit genannt wird, Fingerabdrücke zu fälschen (1). Die Theorie hierbei war, dass beim Ausdrucken eines Fingerabdruckes auf einer Overhead Folie mit einem Laserdrucker durch die Ablagerungen des Druckers genug Struktur (beziehungsweise Relief) erzeugt wird, um mit Holzleim direkt von der Folie eine Attrappe erzeugen zu können. Nach mehreren Versuchen mit zwei verschiedenen Druckern (LaserJet 1015 der Firma Hewlett-Packard, LaserJet 4 der Firma Hewlett-Packard) und drei verschiedenen Foliensätzen („Overhead Folien" Nr. 3552 der Firma „Avery Zweckform", LaserJet Transparentfolien Nr. 92296U der Firma Hewlett-Packard und „Copy/Laser Film" Nr. 8338 der Firma Durable) stellte sich diese Möglichkeit zur Herstellung von Attrappen allerdings als nicht realisierbar heraus. Es wurden bei keinem der Versuche auch nur ansatzweise genug Strukturen erzeugt, um daraus funktionstüchtige Attrappen herstellen zu können. Somit wurde dieser Ansatz für weitere Versuche verworfen.

4.5.4) Erstellen von Vorlagen aus Silikon

Eine weitere Idee zur Herstellung von Vorlagen war, die Finger in aushärtendes Silikon zu pressen, da sich dieses als Dichtungsmittel sehr gut an alle möglichen Formen und Konturen anpasst. Es musste allerdings nach wenigen Versuchen festgestellt werden, dass es nicht möglich ist, solche Vorlagen zu erstellen. Drückt man nämlich den Finger zu früh in die Silikonmasse, passt sich diese zwar tatsächlich dem Finger an, bleibt an diesem allerdings so haften, dass es nicht möglich ist, den Finger aus der Masse zu ziehen, ohne den Abdruck wieder zu zerstören. Wartet man hingegen lang genug, sodass die Oberfläche der Masse ein wenig getrocknet ist und nicht mehr am Finger kleben bleibt, ist es schon zu spät, da sich die getrocknete Oberfläche der Masse nicht mehr an die Fingerkonturen anpasst und somit kein Abdruck entsteht. Daher wurde auch diese Idee wieder verworfen und es wurde nicht weiterversucht Vorlagen aus Silikon herzustellen. Es wurde in weiterer Folge nur noch dazu verwendet, Attrappen zu gießen (siehe 4.6.2).

4.5.5) Erstellen von Vorlagen durch Ätzen von Leiterplatten

Eine weitere Möglichkeit Vorlagen herzustellen, welche auch in bereits existierenden Arbeiten zu diesem Thema erwähnt wird, ist das Ätzen von (fotosensitiven) Leiterplatten (43; 45). In den Versuchen wurde hierfür einseitig fotobeschichtetes Basismaterial der Firma Bungard verwendet. Solche Leiterplatten sind für jeden leicht in einem Elektronik Fachgeschäft zu erstehen. Auch alle weiteren Utensilien, die im Verlauf der Herstellung benötigt werden (UV-Röhre, Entwickler und Ätzmittel), sind in einem Elektronik Fachgeschäft erhältlich.

Ursprünglich war dieses Verfahren dazu gedacht, mithilfe einer Schablone die Leiterbahnen aus Kupfer auf Leiterplatten für elektronische Geräte herzustellen. Nachdem die Kupferleiterbahnen auf dem Basismaterial ähnlich

dünn ausfallen können wie die Papillarleisten von Fingerabdrücken, wurde das Ätzverfahren auch für die Versuche in dieser Arbeit interessant.

Wie bei der Fertigung von Leiterplatten müssen bei der Herstellung von Fingerabdruck-Vorlagen mehrere Schritte durchgeführt werden (61; 43):

- Belichten der Leiterplatte
- Entwickeln der fotosensitiven Schicht
- Ätzen der Leiterplatte
- Spülen und Trockenen der Leiterplatte

Wurden diese Schritte erfolgreich durchgeführt, so hat man eine Leiterplatte, deren „Leiterbahnen" ein Negativbild des Fingerabdruckes zeigen. Was in den genannten Schritten genau zu tun ist und worauf man achten muss, soll im Folgenden genauer erklärt werden.

Belichten der Leiterplatte
Um eine Vorlage aus Leiterplatten zu fertigen, muss zunächst das bearbeitete Bild (siehe Kapitel 4.4) auf Folie ausgedruckt werden. Hierbei kann vor dem Druck noch eine Invertierung des Bildes notwendig sein, damit auch wirklich die Papillarleisten belichtet werden. Die ausgedruckte Folie wird auf der fotosensitiven Seite der Leiterplatte aufgebracht und so befestigt, dass sie nicht verrutschen kann. Anschließend wird die auf diese Art präparierte Seite der Leiterplatte mit UV-Licht bestrahlt, wodurch die nicht schwarzen Teile des Fingerabdrucks auf der Folie das UV-Licht passieren lassen, sodass die Fotoschicht an diesen Stellen belichtet wird. Je nachdem welche finanziellen Mittel zur Verfügung stehen beziehungsweise aufgebracht werden wollen, kann hierbei ein Belichtungsgerät oder aber, falls dies den finanziellen Rahmen übersteigt, eine einfache UV-Lichtröhre mit entsprechender Halterung verwendet werden. In den Versuchen, die im Rahmen dieser Arbeit durchgeführt wurden, wurde eine 8W UV-Röhre der Firma Phillips verwendet. Abgesehen von den Kosten unterscheiden sich die beiden Varianten natürlich auch in der Belichtungsdauer. Während bei einem durchschnittlichen Belichtungsgerät eine Leiterplatte innerhalb von ein bis zwei Minuten (teilweise sogar kürzer) belichtet ist, kann die Belichtungsdauer bei der Verwendung von einer einzelnen UV-Lichtröhre durchaus fünfzehn Minuten und länger benötigen, da das UV-Licht die Platte nicht so direkt anstrahlt sondern auch in die Umgebung abgegeben wird. Bei der Verwendung einer UV-Röhre ist unbedingt darauf zu achten, nicht direkt in das UV-Licht zu sehen, da es für das menschliche Auge schädlich ist. Es ist aber gesondert anzumerken, dass Schwarzlicht kein UV-Licht im Sinne dieser Arbeit darstellt, da es mit einer Wellenlänge von rund 350 nm (UV-A Strahlung) nicht den gewünschten Effekt erzielt. Um eine Belichtung effizient durchzuführen, wird allerdings UV-Licht von rund 250 nm oder weniger (UV-C Strahlung) benötigt (62).

Zu beachten ist bei der Belichtung der Leiterplatte auch, welche Art von fotosensitivem Material auf den Leiterplatten aufgebracht ist. Hierbei wird zwischen Negativlack und Positivlack unterschieden. Handelt es sich um

Negativlack, so bleiben belichtete Teile erhalten, während bei Positivlack eben diese im späteren Verlauf der Herstellung weggeätzt werden. Dementsprechend muss der Fingerabdruck so ausgedruckt werden, dass mit der Schablone entweder die Papillarleisten (Positivlack) oder die Abstände zwischen diesen (Negativlack) belichtet werden. In den Experimenten zu dieser Arbeit wurde mit Positivlack gearbeitet.

In den Versuchen wurde die UV-Licht-Quelle in verschiedenen Abständen zur zu belichtenden Leiterplatte angebracht und für unterschiedlich lange Zeit belichtet. Als optimal erwies sich in den Versuchen bei der Verwendung von lediglich einer UV-Röhre, ein Abstand von knapp 30 cm und einer Belichtungszeit von 20 – 30 Minuten. Zwar kann man, um Zeit zu sparen, den Abstand zur Leiterplatte verringern, allerdings verändert sich bei geringerem Abstand der Belichtungsgrad der Leiterplatte entsprechend schneller und die Belichtungszeit muss exakter eingehalten werden. So kommt es bei einem Abstand von 5 Zentimetern bereits auf wenige Sekunden an, die entscheiden, ob die Platine überbelichtet ist oder nicht, während bei einem Abstand von 30 Zentimeter eine um 5 Minuten verlängerte Belichtung sich kaum auswirkt. Die in den Versuchen erprobten Kombinationen von Abstand und Belichtungszeit können der folgenden Tabelle entnommen werden:

Abstand zur Leiterplatte	Belichtungszeit	Bemerkungen
50 Zentimeter	2 Stunden	Deutlich zu lange Belichtungszeit – Die gesamte Platine (auch die abgedeckten Teile) wurden belichtet.
50 Zentimeter	1 Stunde	Zu lange Belichtungszeit – Es wurden zum Teil auch abgedeckte Teile belichtet.
50 Zentimeter	30 Minuten	Zu kurze Belichtungsdauer – Teile des abgedeckten Bereiches wurden in der Folge weggeätzt.
30 Zentimeter	1 Stunde	Zu lange Belichtungszeit – Es wurden zum Teil auch abgedeckte Teile belichtet.
30 Zentimeter	30 Minuten	Platine fertig belichtet
30 Zentimeter	10 Minuten	Zu kurze Belichtungsdauer – Teile des abgedeckten Bereiches wurden in der Folge weggeätzt.
5 Zentimeter	30 Minuten	Zu lange Belichtungszeit
5 Zentimeter	10 Minuten	Platine gut belichtet

Tabelle 3: Abstand und Zeit beim Belichten von Platinen

Die Belichtung wurde an 40 Platinen vorgenommen. Wie der Tabelle entnommen werden kann, wurden in den Versuchen manche Leiterplatten zu lange belichtet, weshalb von den anfangs 40 Leiterplatten für den weiteren Verlauf lediglich 35 Leiterplatten zur weiteren Verarbeitung zur Verfügung standen.

Entwickeln des fotosensitiven Materials
Nach der Belichtung der Leiterplatte muss das fotosensitive Material noch entwickelt werden. Hierfür muss eine Entwicklerlösung angerührt werden und die Leiterplatte muss ein paar Minuten darin geschwenkt werden. Dadurch treten die belichteten Teile deutlicher hervor und jene Teile, welche beim Ätzen erhalten bleiben sollen, werden gefestigt.

Bei den Versuchen, die dieser Arbeit zugrunde liegen, wurde als Entwickler 10 g Ätznatron (Natriumhydroxid) in einem Liter Wasser aufgelöst. Die durchschnittliche Entwicklungszeit der Leiterplatten betrug hierbei vier Minuten, abhängig auch vom Grad der Belichtung. So konnten länger belichtete Platinen schneller entwickelt werden als jene, die kürzer der UV-Strahlung ausgesetzt waren.

Ätzen der Leiterplatte
Ähnlich dem Entwickeln wird auch zum Ätzen eine Lösung angerührt, in welche die Leiterplatte gelegt wird. Nun muss die Leiterplatte solange vorsichtig in der Lösung geschwenkt werden, bis sich alle nicht entwickelten Teile gelöst haben. Zu beachten ist beim Ätzen, dass die Ätzlösung erwärmt werden sollte und die Temperatur während des gesamten Ätzvorgangs gehalten werden sollte. Wie warm die Lösung gemacht werden sollte, hängt vom jeweiligen Ätzmittel ab und ist der Anleitung des Ätzmittels zu entnehmen. In der Regel sollte die Temperatur aber zwischen 35 und 55 Grad Celsius betragen. Je kühler die Lösung ist umso länger dauert auch der Ätzvorgang. Um die Temperatur der Ätzlösung zu halten, hilft es, die Schale mit dem Ätzmittel in ein Wasserbad zu stellen, wobei das Wasser erwärmt wird oder ständig warmes Wasser nachfließt. Die Dauer des Ätzens variiert je nach Ätzmittel und Basismaterial sowie nach der Temperatur der Ätzlösung, das kann bis zu 45 Minuten dauern.

Zu beachten ist, dass die meisten Ätzmittel giftig sind und daher als Giftmüll entsorgt werden müssen und nicht einfach in den Abfluss gegossen werden dürfen.

In den Versuchen dieser Arbeit wurde als Ätzmittel Natriumpersulfat verwendet. Es wurden insgesamt 35 Leiterplatten mit unterschiedlichen Temperaturen geätzt. Für jeweils 10 Leiterplatten betrug die Temperatur 30° beziehungsweise 40 °Celsius, für die restlichen 15 Platinen wurde die Ätztemperatur auf 50 °Celsius erhöht. Natürlich wurde versucht, keine Leiterplatten zu verschwenden, weshalb nach den angegebenen Zeitpunkten lediglich der Zustand der Leiterplatte beurteilt wurde und sie bis zur vollständigen Ätzung in der Lösung verblieb. Bei diesen Versuchen wurden die in der Tabelle genannten Zeiten und Ätztemperaturen eingehalten, und dabei wurden folgende Unterschiede festgestellt:

Ätztemperatur	Ätzzeit	Bemerkungen
30 °Celsius	15 Minuten	Deutlich zu kurze Ätzzeit – fotosensitive Schicht kaum abgelöst
30 °Celsius	25 Minuten	Merkliche Besserung zu 15 Minuten - allerdings immer noch zu kurz
30 °Celsius	45 Minuten	Fotosensitive Schicht gut abgelöst - Leiterplatte fertig geätzt
40 °Celsius	15 Minuten	Zu kurze Ätzzeit – Leiterplatte noch nicht zur Gänze geätzt
40 °Celsius	25 Minuten	In seltenen Fällen zu kurz bemessener Zeitrahmen, in den meisten Fällen ist die Leiterplatte allerdings bereits fertig geätzt.
40 °Celsius	45 Minuten	Es wurde nie der gesamte Zeitrahmen von 45 Minuten ausgeschöpft, da sämtliche Leiterplatten bereits zuvor fertig geätzt waren.
50 °Celsius	15 Minuten	In zwei Versuchen reichten bereits 15 Minuten aus um die Leiterplatte zur Gänze zu ätzen, alle anderen benötigten mehr Zeit.
50 °Celsius	25 Minuten	Bis auf 3 Testläufe konnten bei 50 °Celsius alle Leiterplatten innerhalb von 25 Minuten geätzt werden.
50 °Celsius	45 Minuten	Lediglich 3 Leiterplatten benötigten bei 50 °Celsius mehr als 25 Minuten, die veranschlagten 45 Minuten wurden jedoch nie benötigt.

Tabelle 4: Temperatur und Dauer des Ätzens von Platinen

Spülen und Trocknen der Leiterplatte

Das Spülen und Trocknen der Leiterplatte wurde hier in einem Schritt zusammengefasst, da diese Schritte nur der Vollständigkeit halber angeführt werden. So muss die Leiterplatte nach dem Ätzen gründlich gespült werden, damit die letzten Reste der Ätzlösung entfernt werden und keinerlei Rückstände bleiben. Abschließend muss die Platte getrocknet werden, um damit weiterarbeiten zu können.

4.6) Gießen der Attrappen

Wurde eine Vorlage erstellt, kann man mit ihrer Hilfe einen „künstlichen Finger“ erzeugen – eine Attrappe. Um dies zu erreichen, wurden in dieser Arbeit verschiedene Materialien verwendet, welche zum Teil auch in anderer Literatur erwähnt werden (1; 3; 43; 45). Dabei wurde vor allem darauf geachtet, welche Unterschiede es bei den diversen Materialien gibt, welche Vor- und Nachteile mit dem Material einhergehen und wie gut die Fingerprint-Scanner mit den jeweiligen Attrappen getäuscht werden können.

4.6.1) Gießen mit Holzleim

Das Gießen der Abdrücke mit Holzleim funktionierte in den Versuchen sehr gut (Es wurde in den Versuchen „Ponal Express“ der Firma Henkel verwendet.). Es muss jedoch darauf geachtet werden, dass man nicht zu viel Holzleim verwendet, da dieser sonst lange braucht, um ausreichend trocken zu werden. Aus diesem Grund ist es nicht ratsam, eine tiefe Vorlage, wie sie entsteht, wenn der Finger zu fest in die Modelliermasse beziehungsweise Wachs gedrückt wurde, mit Holzleim zu befüllen. In einer solchen Vorlage trocknet der Leim nur sehr langsam und es ist meist sehr schwierig die Attrappe aus der Vorlage zu lösen, ohne sie dabei zu beschädigen.

Ein weiterer Nachteil von Holzleim-Attrappen besteht darin, dass sie nach relativ kurzer Zeit starr und steif werden und dadurch nur noch bedingt verwendbar sind und auch leicht brechen. Je nach Menge des Leimes und Ort der Aufbewahrung kann die Zeit bis zum Brüchigwerden einer solchen Attrappe von wenigen Tagen bis hin zu mehreren Wochen variiert.

4.6.2) Gießen mit Silikon

Auch Silikon schien durch seine Eigenschaften und Beschaffenheit ein geeignetes Mittel zur Herstellung von Attrappen zu sein, weshalb es bei den Versuchen genauer unter die Lupe genommen wurde (45). In den Versuchen wurde allerdings klar, dass hierbei auch darauf zu achten ist, welche Art von Silikon verwendet wird. So war es beispielsweise mit einer in den Versuchen verwendeten Sorte von Bausilikon („Classic Bausilikon“ der Firma Ayrton produziert für die Firma Obi) nicht möglich Attrappen herzustellen, da dieser nicht richtig austrocknete und zu wenig Zusammenhalt besaß. Aus diesem Grund entstanden zweierlei Probleme: Zum einen rissen die Attrappen beim Herauslösen aus den Formen oft und zum anderen blieben sie klebrig und trockneten nicht vollständig aus, wodurch sie unbrauchbar waren. Deshalb wurde in den Versuchen in weiterer Folge ein anderer Silikondichtstoff verwendet. (Transparentes Silicon „Neutral 120“ der Firma „Ramsauer Dichtstoffe“).

Ein Vorteil von Silikon gegenüber Holzleim ist, dass es auch nach dem Trocknen flexibel bleibt, wodurch etwaige Silikon-Attrappen länger verwendbar sind. Auch trocknete die Silikonmasse an der Oberfläche schneller aus. Allerdings konnte dadurch kaum festgestellt werden, ob bereits die gesamte Masse getrocknet war. Eine weitere Schwierigkeit bei der Verwendung von Silikon ist das Füllen der Formen. Dieses gestaltet sich zwar bei Verwendung einer Silikonspritze einfach, allerdings muss darauf geachtet werden, dass das Silikon gut verteilt und die Oberfläche der Form vollständig bedeckt wird. Ist dies nicht der Fall, kann dies dazu führen, dass die Masse die Konturen der Vorlage nicht annimmt und dass die so entstehende Attrappe unbrauchbar ist. Ein weiteres Problem kann dadurch entstehen, dass sich die Silikonmasse teilweise zu stark mit der Vorlage verbindet, wodurch beim Herauslösen der Attrappe Teile der Masse an der Form hängen bleiben und somit Löcher in die Attrappe reißen, wodurch diese ebenfalls unbrauchbar wird. Um dem entgegen zu wirken, kann

es hilfreich sein, die Formen vor dem Befüllen mit einer fetthaltigen Creme oder Sprüh-Öl zu behandeln, wobei darauf zu achten ist, die Creme nur sehr dünn aufzutragen, damit das Silikon noch die Konturen der Vorlage annehmen kann.

4.6.3) Gießen mit Gelatine (34; 3; 43)

Bei der Herstellung von Attrappen mit Hilfe von Gelatine muss darauf geachtet werden die richtige Art von Gelatine zu verwenden. So zeigte sich in den Versuchen, dass es erhebliche Unterschiede zwischen „Instant Gelatine“ (verwendet wurde „Instant Gelatine 30 g“ der Firma Haas) und der Verwendung von Gelatineblättern (verwendet wurde „Gelatine weiß 12 Blatt“ der Firma „Dr. Oetker“) gibt. So war es mit „Instant Gelatine“ nicht möglich Attrappen herzustellen, wenn man sich an die vom Hersteller empfohlene Zubereitung hielt. Die so erzeugte Gelatine riss zu leicht und es war kaum möglich, eine vollständige Attrappe aus der Form zu lösen, ohne sie zu zerstören. Mit Gelatineblättern hingegen konnte man nach den Herstellerangaben sehr gute Attrappen anfertigen. Sie ließen sich leicht aus der Form lösen und trockneten auch sehr schnell. Bei „Instant Gelatine“ stellte sich durch entsprechende Versuche heraus, dass man bessere Ergebnisse erzielt, wenn man sich nicht an die Herstellerangaben hält, sondern weniger Wasser als angegeben verwendet. So wurden statt der angegebenen 250 ml lediglich 30 bis 40 ml verwendet. Bei beiden Gelatinearten musste des Weiteren darauf geachtet werden, dass sich möglichst keine Bläschen in der Substanz bildeten, da diese sonst zu einer unbrauchbaren Attrappe führen können.

Als Pluspunkt von Gelatine wird oft angeführt, dass man die Attrappe nach erfolgreichem Täuschen des Fingerprint-Scanners essen kann und somit alle Beweise vernichtet. Zugleich ist die Genießbarkeit von Gelatine auch ein erheblicher Nachteil, da Gelatine wie andere Lebensmittel dazu neigt zu verderben beziehungsweise Schimmel anzusetzen. Attrappen aus Gelatine können somit auch nur kurz nach deren Herstellung verwendet werden und nicht längerfristig aufbewahrt werden, um sie später noch mal zu verwenden. Ein weiterer Nachteil ist, dass Gelatine-Attrappen bei Erhitzen dazu neigen erneut zu schmelzen und sich aufzulösen. In den Versuchen zeigte sich, dass hierfür bereits die Körperwärme ausreicht, sodass eine entsprechende Attrappe nur kurz an einen Finger geheftet werden kann, bis sie beginnt, zu schmelzen und unbrauchbar wird.

Ein weiteres Problem bei der Herstellung von Attrappen mit Gelatine kann sich daraus ergeben, dass Gelatine nach dem Aufkochen sehr flüssig ist. Während dies bei Vorlagen aus Modelliermasse noch ein Vorteil sein mag, da die Gelatine sich der Vorlage genau anpasst, wird diese Eigenschaft von Gelatine beispielsweise zum Problem, wenn man Vorlagen, welche aus Leiterplatten geätzt wurden, gießen will. Auf der ebenen Leiterplatte verrinnt die Gelatine oft zu sehr, sodass es ratsam ist, zuvor die Stelle, welche gegossen werden soll, einzugrenzen, indem man beispielsweise mit Klebestreifen eine Umrandung bildet, aus der die Gelatine nicht hinausrinnen kann.

Gießen von Attrappen mit geschmolzenen Gummibären
In mehreren Artikeln wird beim Gießen von Attrappen aus Gelatine auf die eine oder andere Art erwähnt, dass Gelatine jenes Material ist, aus dem Gummibärchen hergestellt werden. Zwar wird in keiner der Arbeiten explizit erwähnt, dass für die Versuche Gummibären geschmolzen und zur Herstellung von Attrappen verwendet wurden, es lag jedoch nahe, auch hierfür einen Versuch durchzuführen. So wurden in mehreren Testläufen „Goldbären" der Firma „Haribo" eingeschmolzen und versucht die dadurch entstandene zähflüssige Masse in die Vorlageformen zu gießen. Bei den ersten Versuchen wurden die Gummibären ohne Zugabe weiterer Mittel aufgelöst. Es zeigte sich jedoch recht schnell, dass das Unterfangen zum Scheitern verurteilt war, da die Masse zu klebrig war, was darauf zurückzuführen ist, dass die Gummibären nicht aus reiner Gelatine, sondern zu einem großen Teil aus Zucker bestehen. Bereits das Befüllen der Vorlagen bereitete dadurch Probleme und das Herauslösen der Attrappen nach dem Trocknen der Masse erwies sich als unmöglich. Die Masse hatte sich zu sehr mit der Vorlage verbunden, sodass es sich auch als sehr schwierig gestaltete die Vorlageformen wieder zu reinigen.

In einem zweiten Experiment wurde versucht dem Problem entgegenzuwirken, indem die Gummibären in 5 Teelöffeln Wasser aufgelöst wurden. Tatsächlich war die daraus entstandene Masse weniger klebrig und viel flüssiger. Das Befüllen der Vorlagen war ohne weitere Komplikationen möglich. Das Herauslösen der Attrappen aus den Formen wurde jedoch wieder zum Problem. Die Attrappe ließ sich zwar von der Form lösen, riss jedoch viel zu leicht auseinander, wodurch die Attrappe zerstört wurde.

Aufgrund dieser Fehlschläge wurden keine weiteren Versuche mit Gummibären durchgeführt.

4.6.4) Gießen mit Wachs

Eine weitere Möglichkeit eine Attrappe herzustellen ist das Ausgießen einer Vorlage mit Wachs. Auch hier kam wieder das Wachs von „Qualitätskerzen mit Stearinanteil" der Firma „Gala – World of Candles" zum Einsatz. Um entsprechende Attrappen zu fertigen, musste heißes Wachs in die fertige Vorlagenform getropft werden. Bei den Versuchen stellte sich allerdings bald heraus, dass Wachs sich zwar gut an die Vorlage anpasst, es aber beinahe unmöglich ist, das ausgehärtete Wachs von der Vorlage zu lösen, ohne dabei die Wachsattrappe zu zerstören. Die wenigen Attrappen, die von der Vorlage gelöst werden konnten, erwiesen sich zudem als zu hart um tatsächlich zum Einsatz zu kommen. Aus diesem Grund wurde diese Idee verworfen und keine weiteren Versuche mit Wachs-Attrappen gestartet.

4.6.5) Gießen mit Bastelkleber

Ein weiteres Material, welches sich zur Herstellung von Fingerabdruck-Attrappen eignet, ist Bastelkleber. Hierbei wurde in den Versuchen „Bastelkleber" Nr. 47735 der Marke UHU verwendet. Die Eigenschaften dieses Klebers sind ähnlich jenen von Holzleim, weshalb auch dieses Material ähnliche

Nachteile hat. So ist es beispielsweise auch bei der Erstellung mit Bastelkleber schwierig zu erkennen, wann eine Attrappe zur Gänze getrocknet ist.

Ein Vorteil gegenüber Holzleim ist jedoch, dass Attrappen, die mit Bastelkleber erstellt werden, länger flexibel bleiben.

4.7) Test der Attrappen

Zu Beginn der Versuche wurde durch eine Kombination der in den letzten Kapiteln erläuterten Möglichkeiten eine Vielzahl von Attrappen hergestellt. So wurde sowohl mit einer Testperson als kooperatives Opfer gearbeitet mit dem Fimo- und Wachs-Vorlagen erstellt wurden, als auch das Szenario des ahnungslosen Opfers durchgespielt, in dem die Testperson Fingerabdrücke auf einer Glasfläche hinterlässt, welche durch bereits beschriebene Mittel und Methoden sichtbar gemacht, digitalisiert, anschließend in Grafikprogrammen nachbearbeitet, ausgedruckt und letztendlich als Vorlage auf eine Leiterplatte geätzt wurden. Natürlich wurde hier nicht nur eine Testperson herangezogen, sondern sowohl für Fimo- und Wachs-Vorlagen als auch für das Belichten von Leiterplatten wurden die Fingerabdrücke einer männlichen und einer weiblichen Testperson herangezogen, um die Aussagen allgemein halten zu können und nicht nur Aussagen über einen speziellen Fingerabdruck treffen zu können. Auch wurde so versucht, geschlechterspezifische Unterschiede, welche das Ergebnis der Tests beeinflussen könnten, auszuschließen. Ein solcher Unterschied wäre beispielsweise, im Vergleich zu Männern, die feinere Struktur der Papillarleisten einer weiblichen Testperson, welche unter Umständen zu Problemen bei der korrekten Erkennung führen kann (41).

Um die Vorlage aus der Leiterplatte zu ätzen, wurden alle genannten Varianten des Sichtbarmachens von Fingerprints, über die Digitalisierung dieser bis hin zur Nachbearbeitung am PC kombiniert. So wurde ein Teil der Fingerabdrücke auf der Glasplatte mit Grafitpulver bearbeitet, der Rest wurde mit Cyanacrylat eingedampft. Leider war es nicht möglich beide Methoden an ein und demselben Fingerabdruck durchzuführen. Die sichtbar gemachten Fingerabdrücke wurden sowohl fotografiert als auch mit Klebefolie abgenommen und eingescannt. Hierbei kamen alle bereits genannten Kameras und Scanner zum Einsatz. Jedes so entstandene digitalisierte Bild der Fingerabdrücke wurde so gut wie möglich am PC nachbearbeitet (mit den in Kapitel 4.4 genannten Programmen) um die Fingerlinien noch deutlicher darzustellen und dadurch gute Vorlagen zum Belichten von Leiterplatten zu gewinnen. Wie gut dieses Unterfangen mit den einzelnen Programmen gelang, kann in den Kapiteln 4.4.2 und 4.4.3 respektive deren Unterkapiteln nachgelesen werden. Die so entstandenen Vorlagen wurden anschließend auf Folie ausgedruckt, wobei in späterer Folge nur die besten Vorlagen für die weiteren Versuche verwendet wurden.

Die in den vorigen Kapiteln beschriebenen Methoden der einzelnen Arbeitsschritte können nun auf verschiedenste Art und Weise kombiniert werden. So kann ein einzelner Fingerabdruck auf zwei Arten sichtbar gemacht

werden. Anschließend gibt es wiederum zwei Möglichkeiten diesen zu digitalisieren (Fotografieren oder Einscannen). Der digitalisierte Fingerabdruck kann in jedem der vorgestellten Programme nachbearbeitet werden (wobei es in vielen der Programme wiederum mehrere Arten der Nachbearbeitung gibt). So entstanden bei den ersten zehn Versuchen, bei denen alle diese Kombinationsmöglichkeiten durchprobiert wurden, aus jedem von der Testperson hinterlassenen Fingerabdruck mindestens zehn Folienvorlagen, bei Abdrücken besonders guter Qualität sogar bis zu achtzehn Folienvorlagen. Nach den ersten Versuchen kristallisierte sich bald heraus, dass die Nachbearbeitung mit Adobe Photoshop am zügigsten zu bewerkstelligen ist und auch die besten Ergebnisse lieferte. Diese Erfahrung wurde in weiteren Versuchen berücksichtigt, weshalb die gewonnenen Abdrücke nur noch in Adobe Photoshop nachbearbeitet wurden.

Mit den so entstandenen Folienvorlagen wurden die Leiterplatten belichtet und anschließend entwickelt und geätzt. Die Herstellung von Vorlagen aus Modelliermasse und Wachs bereitete wie in den Kapiteln 4.5.1 und 4.5.2 bereits dargelegt keinerlei Probleme und brachten nur geringen Aufwand mit sich.

Da es nicht möglich ist, eine allgemeine Aussage über die Nützlichkeit der Vorlagen zu treffen, solange nur eine Attrappe jeder Art existiert, wurden auch von den Wachs- und Fimo-Vorlagen mehrere Exemplare erstellt. Obwohl von den Vorlagen auf Leiterplatten bereits mehrere Exemplare erstellt wurden, sind sämtliche Phasen der Herstellung mehrmals durchlaufen worden, da auch Aussagen über die einzelnen Schritte des Fingerabdrucknehmens, Digitalisierens und Nachbearbeitens getroffen werden sollten. Die Ergebnisse und Erkenntnisse dieser Versuche können in den entsprechenden Kapiteln dieser Arbeit nachgelesen werden.

In weiterer Folge wurde für alle gefertigten Vorlagen (aus Modelliermasse, Wachs und Leiterplatte) versucht, aus Holzleim, aus Bastelkleber, aus Silikon und auch aus Gelatine Attrappen herzustellen. Auch hier wurden, um eine treffende Aussage über die Vorlagen machen zu können, von jeder Vorlage und jedem Material mehrere Attrappen hergestellt. Zudem können konkrete Angaben über die Brauchbarkeit einzelner Materialien zur Herstellung von Attrappen sowie die Erkenntnisse, welche im Verlauf der Versuche gewonnen wurden, in den jeweiligen Kapiteln nachgelesen werden.

Nachdem in den Versuchen wie gerade beschrieben etliche Attrappen hergestellt wurden, mussten diese natürlich auch noch an den Fingerprint-Scannern getestet werden, um herauszufinden, ob sich die Scanner tatsächlich so einfach täuschen lassen, wie es in anderen Artikeln versprochen wird (1; 2; 3). Um bei den Versuchen einen besseren Überblick zu behalten, wurde jede erzeugte Vorlage beschriftet. Auch die erzeugten Attrappen wurden beschriftet und es wurde vermerkt, mit welcher Vorlage sie hergestellt wurden.

4.7.1) Tests mit "Microsoft Fingerprint-Reader"

Zunächst wurde der Microsoft Fingerprint-Reader genauer untersucht und eingehend getestet. Wie bereits beschrieben (siehe Kapitel 4.1.1), dient dieser Fingerprint-Reader lediglich dem einfacheren Login und weniger der tatsächlichen Systemsicherheit. Auch ist es weiterhin möglich, auf den Fingerprint-Reader zu verzichten und das Login mittels Username und Passwort durchzuführen. Außerdem verfügt dieser Scanner über keinerlei „Life and Well Detection", kann also per se nicht zwischen natürlichen und künstlichen Fingern unterscheiden. Dennoch wurde dieses Gerät für die Tests in dieser Arbeit ausgewählt, weil es ein guter Repräsentant der Gruppe der optischen Fingerprint-Scanner ist.

Zu Beginn wurden die Fingerabdrücke der Testpersonen mithilfe des Scanners im Computersystem als Referenzabdrücke für einen bestimmten Useraccount angelegt, sodass sich diese Personen durch kurzes Auflegen des Fingers auf die Scanneroberfläche am System anmelden können. Hierfür wurde die mitgelieferte Software „DigitalPersona" in der Version 2.0.1.1843 verwendet.

Nachdem die Abdrücke im System hinterlegt waren, wurde zunächst die primitivste Variante der Täuschung ausprobiert. Hierzu wurde von einer Testperson versucht sich mit einem ihrer nicht im System hinterlegten Fingerabdruck anzumelden. Dafür wurde meist von einem enrolten Finger das nicht hinterlegte Äquivalent der anderen Hand benutzt. Alle diese Versuche scheiterten erwartungsgemäß.

Anschließend wurde von einer weiteren Person versucht, sich mit den wie bereits beschrieben erzeugten Attrappen am System anzumelden. Dies wurde für jede Attrappe zwanzig Mal versucht um Glückstreffer auszuschließen und somit sicherzustellen, dass das Login aufgrund der Attrappe und nicht durch einen anderen zufällig aufgetretenen Fehler möglich war.

Bei dem Versuchsaufbau mit kooperativem Opfer stellte sich im Verlauf der Versuche schnell heraus, dass die Attrappen mancher Vorlagen bessere Ergebnisse erzielten als jene, welche mit anderen Vorlagen erstellt wurden. So musste nachträglich festgestellt werden, dass manche Vorlagen aus Fimo und Wachs sich offenbar bei der Erstellung ein wenig verzogen hatten, was auf den ersten Blick nicht festgestellt werden konnte.

Sonst wurden bei den Täuschungsversuchen in diesem Versuchsaufbau jedoch durchaus Erfolge erzielt. So konnte die Testperson beispielsweise mit knapp der Hälfte der Holzleim- und Bastelkleber-Attrappen, circa einem Drittel der Silikon-Attrappen und auch durch die eine oder andere Gelatine-Attrappe aus Fimo-Vorlagen den Microsoft Fingerprint-Reader täuschen und sich somit Zugang zum System verschaffen. Die Performance von Attrappen aus Wachs-Vorlagen war nicht ganz so gut, da viele Vorlagen durch das Klebenbleiben von Attrappenmaterial zerstört wurden. Die genauen Werte dieser Versuche können den Tabellen in Appendix A entnommen werden. Eine Übersicht sollen aber bereits die folgenden Tabellen bieten.

Die in den Tabellen erwähnten Testpersonen werden dabei wie folgt charakterisiert:

- Testperson 1 – TP1 – männlich, 26 Jahre
- Testperson 2 – TP2 – weiblich, 23 Jahre

Die Spalte „getäuscht“ weist die Gesamtanzahl der erfolgreichen Täuschungen des Scanners mit Attrappen einer Vorlage von der angegebenen Testperson aus. Für die Spalten „nicht getäuscht“ und „nicht reagiert“ gilt Entsprechendes. Die letzte Spalte zeigt prozentuell, wie oft Attrappen einer bestimmten Testperson den Scanner täuschen konnten, wobei hier die Versuche in denen der Scanner nicht auf die Attrappe reagiert hat, nicht gezählt wurden.

Test-person	Verwendete Vorlagen	Erstellte Attrappen	Getäuscht	Nicht getäuscht	Nicht reagiert	%
TP1	12	33	167	214	279	43,8
TP2	12	33	157	213	290	42,4

Tabelle 5: Teststatistik - Fimo - Holzleim – koop. Opfer - MS

Test-person	Verwendete Vorlagen	Erstellte Attrappen	Getäuscht	Nicht getäuscht	Nicht reagiert	%
TP1	11	32	163	200	277	44,9
TP2	12	33	143	211	306	40,4

Tabelle 6: Teststatistik - Fimo – B.-kleber – koop. Opfer - MS

Test-person	Verwendete Vorlagen	Erstellte Attrappen	Getäuscht	Nicht getäuscht	Nicht reagiert	%
TP1	11	27	69	221	250	23,8
TP2	12	29	92	215	273	30,0

Tabelle 7: Teststatistik - Fimo-Vorlagen - Silikon – koop. Opfer - MS

Test-person	Verwendete Vorlagen	Erstellte Attrappen	getäuscht	Nicht getäuscht	Nicht reagiert	%
TP1	11	32	18	242	380	6,9
TP2	12	33	10	255	395	3,8

Tabelle 8: Teststatistik - Fimo - Gelatine – koop. Opfer - MS

Test-person	Verwendete Vorlagen	Erstellte Attrappen	getäuscht	Nicht getäuscht	Nicht reagiert	%
TP1	6	16	52	116	152	31,0
TP2	6	13	26	101	133	20,5

Tabelle 9: Teststatistik - Wachs - Holzleim – koop. Opfer - MS

Test-person	Verwendete Vorlagen	Erstellte Attrappen	getäuscht	Nicht getäuscht	Nicht reagiert	%
TP1	6	16	38	120	162	24,1
TP2	6	16	36	130	154	21,7

Tabelle 10: Teststatistik - Wachs – B.-kleber – koop. Opfer - MS

Test-person	Verwendete Vorlagen	Erstellte Attrappen	getäuscht	Nicht getäuscht	Nicht reagiert	%
TP1	6	14	25	98	157	20,3
TP2	6	15	18	110	172	14,1

Tabelle 11: Teststatistik - Wachs - Silikon - koop. Opfer - MS

Test-person	Verwendete Vorlagen	Erstellte Attrappen	getäuscht	Nicht getäuscht	Nicht reagiert	%
TP1	6	18	19	150	191	11,2
TP2	6	18	0	171	189	0

Tabelle 12: Teststatistik - Wachs - Gelatine - koop. Opfer - MS

Die Versuchsanordnung, bei der von einem unwissenden Opfer ausgegangen wurde, konnte hingegen nicht solche Ergebnisse erzielen. Von allen Versuchen, die hierbei unternommen wurden, konnte sich die Testperson lediglich drei Mal, ein Mal mithilfe einer Gelatine-Attrappe und zwei Mal mithilfe eine Bastelkleberattrappe, Zugang zum System verschaffen. Mit allen anderen Attrappen, welche von Leiterplatten-Vorlagen hergestellt wurden, konnte trotz der Vielzahl der Versuche und der Attrappen kein entsprechendes Ergebnis erzielt werden. Eine Zusammenfassung der Testergebnisse zeigen die folgenden Tabellen. Eine Aufstellung der konkreten Ergebnisse der Testserien kann wiederum Appendix A entnommen werden.

Test-person	Verwendete Vorlagen	Erstellte Attrappen	Getäuscht	Nicht getäuscht	Nicht reagiert	%
TP1	21	60	0	308	892	0
TP2	21	61	0	288	932	0

Tabelle 13: Teststatistik - Platine - Holzleim – unw. Opfer - MS

Test-person	Verwendete Vorlagen	Erstellte Attrappen	Getäuscht	Nicht getäuscht	Nicht reagiert	%
TP1	18	70	2	416	982	0,5
TP2	19	55	0	304	796	0

Tabelle 14: Teststatistik - Platine – B.-kleber – unw. Opfer – MS

Test-person	Verwendete Vorlagen	Erstellte Attrappen	Getäuscht	Nicht getäuscht	Nicht reagiert	%
TP1	17	51	0	313	707	0
TP2	17	51	0	324	696	0

Tabelle 15: Teststatistik - Platine - Silikon – unw. Opfer - MS

Test-person	Verwendete Vorlagen	Erstellte Attrappen	Getäuscht	Nicht getäuscht	Nicht reagiert	%
TP1	21	80	1	367	1232	0,3
TP2	21	63	0	254	1006	0

Tabelle 16: Teststatistik - Platine - Gelatine – unw. Opfer - MS

4.7.2) Tests mit "Digitus Fingerprint-Reader"

Als zweites Testgerät fungierte der „Digitus Fingerprint-Reader", welcher als Repräsentant der kapazitiven Zeilensensoren fungierte. Wie auch der Microsoft Fingerprint-Reader verfügt dieses Gerät über keine „Life and Well" Erkennung im eigentlichen Sinn (Temperaturmessung, Pulsmessung) (43). Da es sich jedoch um einen Scanner mit kapazitiven Sensoren handelt, muss das Material einer Attrappe zumindest eine gewisse Leitfähigkeit bieten, damit der Scanner auf den Fake-Finger reagiert. Die Leitfähigkeit menschlicher Haut kann allerdings sehr einfach dadurch simuliert werden, dass die Testperson ein wenig Speichel auf der Attrappe verteilt (43).

Zu Beginn der Tests wurde auch hier ein Enrolment der Testpersonen durchgeführt, sodass sich diese durch das Ziehen des Fingers über das Sensorarray am System einloggen konnten. Es wurde mit denselben Testpersonen gearbeitet wie bei den Versuchen mit dem Microsoft Fingerprint-Reader. Verwendet wurde hierfür die dem Gerät beiliegende Software „Fingerprint Authentication Suite" in der Version 4.2.1.0. (Genauere Informationen über den Scanner und das Enrolment können Kapitel 4.1.2 entnommen werden).

Als erster Schritt wurde auch hier wie beim ersten Testgerät vorgegangen, indem die Testperson zunächst als einfachstes Testszenario versuchte, sich mit einem nicht registrierten Finger am System Zugriff zu verschaffen. Auch hier scheiterten erwartungsgemäß alle Versuche, den Scanner zu täuschen.

Bei den Tests dieses Gerätes wurden ebenfalls mit jeder Fingerprint-Attrappe zwanzig Versuche unternommen, sich am System anzumelden. Da die Tests der beiden Scanner nicht unmittelbar nacheinander stattfanden, waren zum Zeitpunkt des Tests dieses Gerätes bereits einige Holzleim-Attrappen brüchig geworden. Auch die meisten Gelatine-Attrappen waren zu diesem Zeitpunkt bereits verdorben (siehe Kapitel 4.6.3) und nicht mehr verwendbar. Zwar wurde versucht, diese Attrappen dennoch zu verwenden, es wurden aber zum besseren Vergleich mit dem anderen Gerät, weitere Attrappen als Ersatz für die aus dem einen oder anderen Grund nur noch schlecht oder gar nicht mehr verwendbaren Attrappen hergestellt.

Auch hier wurde in zwei Schritten getestet. Zunächst wurde auch bei diesem Gerät wieder die Variante mit kooperativem Opfer gewählt. Im Unterschied zum ersten Gerät konnten jedoch bereits hier keinerlei positive Ergebnisse verbucht werden. Auch reagierte das Gerät auf viele der Abdruckattrappen überhaupt erst, wenn man sie wie zuvor beschrieben leicht mit Speichel anfeuchtete (43), und selbst dann nicht immer. Die Testperson konnte sich jedoch weder mit

Holzleim-, noch mit Bastelkleber-Attrappen, noch mit Silikon-Attrappen und auch nicht mit Attrappen aus Gelatine erfolgreich am System anmelden. Eine Zusammenfassung der Testergebnisse kann den folgenden Tabellen entnommen werden. Eine detaillierte Auflistung der einzelnen Testergebnisse kann den entsprechenden Tabellen in Appendix B entnommen werden.

Die Bedeutung der einzelnen Spalten und die Charakterisierung der Testpersonen ist die gleiche wie bei den Tests des Microsoft Fingerprint-Readers und kann in Kapitel 4.7.1 eingesehen werden.

Test-person	Verwendete Vorlagen	Erstellte Attrappen	Getäuscht	Nicht getäuscht	Nicht reagiert	%
TP1	11	32	0	58	582	0
TP2	12	33	0	86	574	0

Tabelle 17: Teststatistik - Fimo - Holzleim - koop. Opfer – Digitus

Test-person	Verwendete Vorlagen	Erstellte Attrappen	Getäuscht	Nicht getäuscht	Nicht reagiert	%
TP1	11	32	0	185	455	0
TP2	12	33	0	177	483	0

Tabelle 18: Teststatistik - Fimo – B.-kleber - koop. Opfer – Digitus

Test-person	Verwendete Vorlagen	Erstellte Attrappen	Getäuscht	Nicht getäuscht	Nicht reagiert	%
TP1	11	32	0	48	592	0
TP2	12	33	0	36	624	0

Tabelle 19: Teststatistik - Fimo - Silikon - koop. Opfer – Digitus

Test-person	Verwendete Vorlagen	Erstellte Attrappen	Getäuscht	Nicht getäuscht	Nicht reagiert	%
TP1	11	32	0	156	484	0
TP2	12	33	0	143	517	0

Tabelle 20: Teststatistik - Fimo - Gelatine - koop. Opfer – Digitus

Test-person	Verwendete Vorlagen	Erstellte Attrappen	Getäuscht	Nicht getäuscht	Nicht reagiert	%
TP1	6	14	0	37	243	0
TP2	6	13	0	42	218	0

Tabelle 21: Teststatistik - Wachs - Holzleim - koop. Opfer – Digitus

Test-person	Verwendete Vorlagen	Erstellte Attrappen	Getäuscht	Nicht getäuscht	Nicht reagiert	%
TP1	6	15	0	66	234	0
TP2	6	18	0	89	271	0

Tabelle 22: Teststatistik - Wachs – B.-kleber - koop. Opfer – Digitus

Test-person	Verwendete Vorlagen	Erstellte Attrappen	Getäuscht	Nicht getäuscht	Nicht reagiert	%
TP1	6	18	0	31	329	0
TP2	6	16	0	29	291	0

Tabelle 23: Teststatistik - Wachs - Silikon - koop. Opfer – Digitus

Test-person	Verwendete Vorlagen	Erstellte Attrappen	Getäuscht	Nicht getäuscht	Nicht reagiert	%
TP1	6	17	0	65	275	0
TP2	6	18	0	82	278	0

Tabelle 24: Teststatistik - Wachs - Gelatine - koop. Opfer - Digitus

Auch bei der zweiten Versuchsanordnung, bei deren Szenario von einem unwissenden Opfer ausgegangen wurde, konnten keine Erfolge erzielt werden. So war es mit keiner der mit Hilfe von Leiterplatten-Vorlagen erzeugten Attrappen möglich, den Scanner zu täuschen und sich unrechtmäßig am System anzumelden. Auch hier zeigen die folgenden Tabellen nur eine Zusammenfassung. Eine detaillierte tabellarische Darstellung der konkreten Ergebnisse kann im Appendix B eingesehen werden.

Test-person	Verwendete Vorlagen	Erstellte Attrappen	Getäuscht	Nicht getäuscht	Nicht reagiert	%
TP1	21	59	0	174	1006	0
TP2	21	63	0	207	1053	0

Tabelle 25: Teststatistik - Platine - Holzleim – unw. Opfer – Digitus

Test-person	Verwendete Vorlagen	Erstellte Attrappen	Getäuscht	Nicht getäuscht	Nicht reagiert	%
TP1	19	57	0	203	937	0
TP2	21	61	0	263	957	0

Tabelle 26: Teststatistik - Platine – B.-kleber – unw. Opfer – Digitus

Test-person	Verwendete Vorlagen	Erstellte Attrappen	Getäuscht	Nicht getäuscht	Nicht reagiert	%
TP1	19	57	0	165	975	0
TP2	20	60	0	153	1047	0

Tabelle 27: Teststatistik - Platine - Silikon – unw. Opfer – Digitus

Test-person	Verwendete Vorlagen	Erstellte Attrappen	Getäuscht	Nicht getäuscht	Nicht reagiert	%
TP1	21	63	0	197	1063	0
TP2	21	63	0	249	1011	0

Tabelle 28: Teststatistik - Platine - Gelatine – unw. Opfer - Digitus

5) Die praktischen Aspekte der durchgeführten Tests als Beispiel zur Vermittlung wissenschaftlicher Arbeitsweise

Während der Durchführung der Experimente im Rahmen dieser Arbeit zeigte sich immer wieder, dass solche Tests eine abwechslungsreiche Tätigkeit im Informatikalltag bildeten. Im herkömmlichen Fachstudium wird man mit derartig praktischen Tests, mit ihrer detaillierten Planung und wissenschaftlichen Protokollierung äußerst selten konfrontiert. Dies mag daran liegen, dass eine Informatikstudentin/ein Informatikstudent im Rahmen ihres/seines Studiums zwar lernt, wie eine Dokumentation für Programmcode aussehen muss und wie eine wissenschaftliche Arbeit verfasst werden soll. Im Studium selbst muss sie/er sich allerdings kaum mit der praktischen Durchführung wissenschaftlicher Versuche und deren Dokumentation auseinander setzen. Die Versuche dieser Arbeit eignen sich gut dafür, Studentinnen/Studenten an die wissenschaftliche Durchführung von Versuchen heranzuführen und ihnen zu zeigen, wie eine korrekte und vollständige Beschreibung der Versuchsanordnungen sowie eine detaillierte Dokumentation der Versuchsabläufe auszusehen hat. In diesem Kapitel soll daher dargestellt werden, wie man die durchgeführten Experimente und deren Ergebnisse im Rahmen einer Laborübung an einer Universität dazu verwenden könnte, die genannten Aspekte des wissenschaftlichen Arbeitens an Studierende weiter zu vermitteln. In Kapitel 5.1 sollen hierfür zunächst didaktische Methoden vorgestellt werden, die in einer solchen Übung eingesetzt werden könnten. Im zweiten Unterkapitel (5.2) soll schließlich ein Konzept für eine konkrete Umsetzung vorgeschlagen werden.

5.1) Didaktische Methoden

Die folgenden Unterkapitel geben eine Übersicht über die didaktischen Methoden, welche in dem in Kapitel 5.2 vorgestellten Konzept einer Laborübung eingesetzt werden. Zu jeder Methode soll auch kurz erläutert werden, in welcher Phase der Laborübung sie Anwendung finden soll.

5.1.1) Frontalunterricht/Präsentationen

Der Frontalunterricht ist eine Unterrichtsmethode, in der die Aktivität der Lernenden in den Hintergrund tritt und in der die/der Vortragende die jeweiligen Inhalte in Präsentationsform thematisiert. Oft ist die Methode des frontalen Unterrichtens negativ besetzt, weil damit oftmals eine Unterrichtsform assoziiert wird, in welcher die/der Lehrende seinen Schülerinnen und Schülern die Inhalte aufzwingt (63). Dennoch ist der Frontalunterricht eine wichtige Methode für die im nächsten Unterkapitel beschriebene Laborübung. Sie soll im Rahmen der Übung jedoch in einer Form zum Einsatz kommen, welche diesem negativen Bild in keiner Weise entspricht. So soll der Frontalunterricht nicht die vorherrschende Unterrichtsmethode bilden, sondern lediglich in kurzen, zeitlich begrenzten Sequenzen der Einheiten während der von den Studierenden durchgeführten Übungen eingesetzt werden, um weiterführendes Wissen zur Thematik der jeweiligen Einheit zu vermitteln. Auch sollen die Studentinnen und Studenten jederzeit die

Möglichkeit haben, während der Präsentation Zwischenfragen zu stellen und mit der/dem Vortragenden zu diskutieren. Nur in dieser Form scheint der Frontalunterricht eine passende Methode zu sein, um in der beschriebenen Laborübung Anwendung zu finden.

5.1.2) Problem Based Learning

Beim „Problem Based Learning" wird von der/vom Vortragenden eine Problemstellung an die Lernenden herangetragen. Diese sollen nun von der Problemstellung motiviert werden und versuchen sich selbst Lösungsmöglichkeiten zu überlegen und zu entwickeln (63). Die Methode des „Problem Based Learning" bildet per se eine geeignete didaktische Methode für die Laborübung, weil angenommen werden kann, dass nur Studentinnen und Studenten an der Übung teilnehmen, die an der Thematik interessiert sind und sich somit auch leicht für die Problemstellung begeistern lassen. Auch ist die Aussicht auf die Durchführung praktischer Versuche ein weiterer Ansporn für die Lernenden, sich selbst bei der Problemlösung zu engagieren.

5.1.3) Partnerarbeit/Gruppenarbeit

Die Partnerarbeit als didaktische Methode dient dazu, Studentinnen und Studenten die Möglichkeit zu bieten, ein Problem gemeinsam mit anderen Lernenden zu erörtern und zu lösen (64). Die Partnerarbeit wird im beschriebenen Konzept nicht als Partner- oder Gruppenarbeit im eigentlichen Sinne gesehen. So wird von den Studentinnen und Studenten einer Gruppe nicht gemeinsam eine praktische Übung durchgeführt, sondern jeder Studierende der Gruppe führt eigenständig seine Übungen durch. Die Partnerarbeit hier dient vor allem dazu, dass die Gruppenmitglieder einander bei einer praktischen Übung helfen, wenn Probleme auftauchen oder auch als erste Ansprechstelle fungieren, wenn einer Studentin/einem Studenten eine Aufgabenstellung nicht ganz klar ist. Dadurch wird einerseits die/der Vortragende ein wenig entlastet und kann sich mehr der Gesamtkoordination widmen, andererseits wird die Eigenverantwortlichkeit der Übenden stärker gefordert. Ein weiterer Aspekt, warum eine Gruppenarbeit in der Laborübung sinnvoll scheint, ist eine bessere Koordinierbarkeit der Laborübung, da manche Materialien gemeinsam für eine Kleingruppe zur Verfügung gestellt werden können und nicht für jeden Studierenden einzeln vorhanden sein müssen (siehe auch Kapitel 5.2.2).

5.1.4) Fragend-entwickelnde Methode

Bei der „Fragend-entwickelnden Methode" bedient sich die/der Vortragende einer sokratischen Fragestellung, um die Lernenden zum Nachdenken über das Thema zu bewegen und sie durch das Beantworten der Fragen, selbst mögliche Lösungswege entdecken zu lassen (63). Dennoch ist die „Fragend-entwickelnde Methode" eine gewisse Form des Frontalunterrichts, da die/der Vortragende die Themen durch ihre/seine Frageführung vorgibt und eine sich aus dieser Methode entwickelnde Diskussion lenken und leiten kann. In der Laborübung sind in vielen Einheiten Diskussionen mit den Studierenden eingeplant, um diesen zu ermöglichen, selbst Lösungswege zu kreieren. In

diesen Phasen wird die „Fragend-entwickelnde Methode“ in Kombination mit der Methode des „Problem Based Learning“ verwendet.

5.2) Konkrete Umsetzung

In diesem Kapitel wird ein Konzept für eine mögliche Laborübung mit Studentinnen und Studenten vorgestellt, das auf den Tests und den Ergebnissen dieser Arbeit aufbaut und in dem versucht wird, das aus den Versuchen erworbene Wissen sinnvoll an andere Studierende weiterzugeben, wobei weniger die konkreten Übungen im Mittelpunkt stehen, sondern den Studentinnen und Studenten soll vielmehr eine Einführung in das wissenschaftliche Arbeiten und Dokumentieren vermittelt werden. Über die Ziele der Laborübung gibt Kapitel 5.2.3 genauer Auskunft.

5.2.1) Zielgruppe

Die in diesem Konzept geplante Übung richtet sich an Informatik-Studentinnen und -Studenten aller Informatik-Studienrichtungen, welche sich möglichst, aber nicht zwingend, am Anfang ihres Studiums befinden.

5.2.2) Anforderungen

Anforderungen an die Teilnehmerinnen und Teilnehmer der Übung
Für die geplante Übung wird seitens der Studierenden keinerlei spezielles Vorwissen verlangt. Da die Laborübung auf eine fixe Personenzahl beschränkt ist, wird von den Teilnehmerinnen und Teilnehmern der Laborübung Anwesenheit in den Übungen sowie ein gewisses Maß an Eigenengagement verlangt, um die Übung im Sinne aller Teilnehmerinnen und Teilnehmer erfolgreich durchführen zu können.

Materialien
Zur Durchführung der Laborübung müssen sämtliche für die Versuche notwendigen Mittel bereitgestellt werden. Konkret werden daher für die Versuche benötigt:

Zur Herstellung von Fimo-Vorlagen:

- Fimo (je eine andere Farbe pro Gruppe)
- Stifte zum Beschriften der gebrannten Fimo-Vorlagen
- Backpapier

Zum Sichtbarmachen von Fingerabdrücken:

- eine Glasplatte pro Studentin/Student (wiederverwendbar)
- eine Glasplatte pro Gruppe für die Cyanacrylattests (nicht wiederverwendbar)
- Grafitpulver
- einen Pinsel pro Studentin/Student zum Abpinseln des Grafitpulvers

- ein Superkleber, der Cyanacrylat enthält
- pro Studentin/Student ein Deckel zum Abdecken der mit Cyanacrylat einzudampfenden Stellen

Zur Herstellung von Leiterplatten-Vorlagen:

- pro Studentin/Student eine vorbereitete Folie mit nachbearbeitetem Fingerabdruck zum Belichten der Leiterplatte
- pro Studentin/Student eine einseitig fotobeschichtete Leiterplatte
- Natriumpersulfat (Ätzmittel) in ausreichender Menge entsprechend der Anzahl der teilnehmenden Personen
- Natriumhydroxid (Entwickler) in ausreichender Menge entsprechend der Anzahl der teilnehmenden Personen

Weiters sollten zur Herstellung der Attrappen Holzleim, Bastelkleber und Gelatine vorhanden sein. Aus Sicherheitsgründen sollten für das Ätzen der Leiterplatten Schutzhandschuhe und Schutzbrillen sowie eventuell Labormäntel verfügbar sein.

Anforderungen an die Räumlichkeiten des Labors
In Hinblick auf die Durchführung der Versuche dieser Laborübung gibt es ein paar Anforderungen, welche die Räumlichkeiten, in denen die Übung stattfinden soll, erfüllen müssen. So muss zum Brennen der Fimo-Vorlagen ein Ofen (Heißluft) vorhanden sein. Zur Herstellung von Leiterplatten-Vorlagen sollte ein Belichtungsgerät verfügbar sein sowie die benötigten Einrichtungen zum Ätzen der Leiterplatten. Dazu gehört ein Wasseranschluss mit gradueller Wärmeregelung und Labormaterial, wie Plastikwannen und Zangen sollen verfügbar sein. Da es sich beim Entwicklergemisch und bei der Ätzlösung um Chemikalien handelt und die Ätzlösung zudem giftig ist (wie bereits in Kapitel 4.5.5 erläutert), muss eine umweltgerechte Entsorgung des Ätzmittels und des Entwicklers möglich sein. Des Weiteren sollten für die Versuche mit Gelatine eine Kochplatte und ein Kochtopf sowie ein Kühlschrank, zur längeren Haltbarkeit der Attrappen, vorhanden sein.

Da neben der praktischen Durchführung auch theoretische Aspekte der Versuche erläutert werden, müssen im Labor auch Tische und Sessel sowie eine Leinwand und ein Beamer vorhanden sein. Für die Durchführung der Tests müssen zumindest ein MS Fingerprint-Reader sowie ein Digitus Fingerprint-Reader, sowie je ein PC mit entsprechender Gerätesoftware zur Verfügung stehen. Um effizient arbeiten zu können, wären natürlich mehre PCs und Scanner von Vorteil. Es können natürlich auch andere Scanner als die beiden genannten oder auch nur einer der genannten Scanner getestet werden.

5.2.3) Lernziele

Das vordringliche Ziel der Laborübung ist es, den Studierenden die Ergebnisse dieser Diplomarbeit näher zu bringen und ihnen damit zu zeigen, dass ein Fingerabdruck unter bestimmten Bedingungen durchaus nachgebildet werden kann und dass ein Fingerprint-Scanner keine absolute Sicherheit bietet. Es soll

ihnen jedoch auch gezeigt werden, dass es sehr schwierig ist, eine funktionstüchtige Fingerabdruck-Attrappe herzustellen und dass es von vielen Faktoren abhängt, ob dies überhaupt möglich ist. Den Studentinnen und Studenten wird durch diese Laborübung ermöglicht, einen anderen, mehr praxisorientierten Zugang zu speziellen Problemen der Informatik kennenzulernen.

Darüber hinaus soll den Studierenden auch gezeigt werden, worauf bei der Durchführung wissenschaftlicher Versuche zu achten ist. Wie Versuchsanordnungen dokumentiert und Versuchsabläufe protokolliert werden können und dass man nur unter genau festgelegten Bedingungen zu vergleichbaren Ergebnissen kommen kann. Außerdem lernen sie zu entscheiden, welche Fakten unbedingt festgehalten werden müssen, um einen wissenschaftlichen Anspruch erheben zu können. Es ist daher ein wichtiges Ziel der Laborübung, dass die Studentinnen und Studenten lernen, im praktischen Bereich wissenschaftlich zu arbeiten und nicht nur im (ebenso wichtigen) theoretischen Bereich.

Weiterführende Ziele der Laborübung sind außerdem die Steigerung der Teamfähigkeit der Studierenden, da sie in der Laborübung in Gruppen arbeiten, sowie das Überprüfen und kritische Hinterfragen anderer wissenschaftlicher Arbeiten. Weiters soll den Studentinnen und Studenten die Notwendigkeit eines selbstständigen, eigenverantwortlichen Arbeitens vermittelt werden. Sie arbeiten zwar in einer Gruppe, die einerseits der Selbstkontrolle dient, die andererseits aber auch die Aufgabe hat, einen besseren Wissenserwerb durch kontrollierte Informationsweitergabe innerhalb der Gruppe zu unterstützen. Die Übungen müssen jedoch von jedem Gruppenmitglied einzeln durchgeführt werden.

5.2.4) Ablauf

Im folgenden Abschnitt wird weniger eine konkrete Stundenplanung für die Laborübung vorgestellt, sondern es werden Vorschläge präsentiert, wie einzelne Teile dieser Diplomarbeit für entsprechende Übungen übernommen und adaptiert werden können. Außerdem soll erläutert werden, in welcher Form dies denkbar und sinnvoll erscheint (siehe auch folgendes Kapitel 5.2.5).

Um die Laborübung in einem überschaubaren Rahmen zu halten und zu gewährleisten, dass die Studierenden möglichst viel von der Übung für ihr weiteres Studium mitnehmen können, sollte die Anzahl der Personen für die Übung auf 10-15 Teilnehmerinnen/Teilnehmer beschränkt werden. Für die Zeit der praktischen Übungen sollen die Studentinnen und Studenten sich in Gruppen zu 2-3 Personen zusammenfinden. Dadurch können die Gruppenmitglieder einander helfen, falls es bei einem Übungsablauf zu Unklarheiten oder zu Problemen kommt.

In der **ersten Übungseinheit** wird den Studierenden kurz erläutert, was in der Übung auf sie zukommt und was von ihnen erwartet wird. Im folgenden Schritt

sollte mit einem theoretischen Teil begonnen werden, in dem den Übungsteilnehmerinnen und Übungsteilnehmern ein paar der bisher publizierten Artikel und Arbeiten zum Thema „Täuschen von Fingerprint-Scannern“ präsentiert werden. Auf alle Fälle sollte der Artikel des Chaos Computer Clubs (1) sowie die Arbeit von Tsutomu Matsumoto (3) vorgestellt werden. Im Anschluss daran sollte ein Gespräch darüber stattfinden, welche der präsentierten Arbeiten die Studierenden am „wissenschaftlichsten“ finden und welche der Arbeiten für sie eher populistisch wirken. Natürlich sollen die Studentinnen und Studenten ihre Meinung hierbei auch begründen und erläutern, ob es sich dabei lediglich um ein „Bauchgefühl“ handelt, dass sie eine Arbeit als mehr oder weniger wissenschaftlich ansehen oder ob diese Meinung fundiert begründet werden kann. So sollen die Studierenden darauf hingeführt werden, dass es in wissenschaftlichen Arbeiten wichtig ist, dass alle durchgeführten Versuche nachvollziehbar sind und dass genau nachgelesen werden kann, mit welchen Mitteln, Methoden und Materialien gearbeitet wurde. Nur so ist es möglich, ein Ergebnis, welches in einer Arbeit beschrieben wurde, selbst nachzuprüfen. Hierbei sollte auf einzelne Aspekte der vorliegenden Diplomarbeit übergeleitet und die konkrete Problemstellung erklärt werden. In dieser Phase der Übung werden den Studentinnen und Studenten jedoch noch keine Ergebnisse der Tests präsentiert, sondern es wird ihnen vielmehr erläutert, dass sie selbst im Rahmen der Laborübung versuchen werden, entsprechende Tests durchzuführen.

In der **zweiten Übungseinheit** sollten die Studierenden mit möglichen Herangehensweisen und Testszenarien vertraut gemacht werden. Hierfür bietet sich die „fragend-entwickelnde Methode“ an, welche in Kapitel 5.1 beschrieben wurde. Dabei wird von der/vom Vortragenden die Frage aufgeworfen, wie man Fingerprint-Scanner auf ihre Sicherheit testen kann. Dabei sollen die Übungsteilnehmerinnen und Übungsteilnehmer noch einmal auf die Tests hingewiesen werden, welche sie bereits in den Arbeiten, die in der ersten Einheit vorgetragen wurden, kennengelernt haben. Die Studierenden sollen somit erkennen, dass für einen Test in jedem Fall die Herstellung einer Attrappe als Vorlage notwendig ist und im nächsten Schritt soll die Herstellung einer oder mehrerer solcher Attrappen praktisch erprobt werden. Auch sollen Ideen entwickelt werden, mit welchen Materialien diese Vorlagen und anschließend auch die Attrappen hergestellt werden könnten. Hierbei werden ihnen sicherlich verschiedene Möglichkeiten aus der einen oder anderen Arbeit zu diesem Thema bekannt sein. Interessant wäre es natürlich, wenn die Studierenden auch eigene, vielleicht neue Ideen einbrächten. Letztlich soll sich aus der „fragend-entwickelnden Methode“ eine Diskussion ergeben, welche von der/vom Vortragenden derart gelenkt wird, dass die Studentinnen und Studenten erkennen, dass es abgesehen von den Materialien, welche bei den Versuchen verwendet werden, auch darauf ankommt, wie ein Testablauf gestaltet ist und welche Voraussetzungen angenommen werden. So sollen die Übungsteilnehmerinnen und Übungsteilnehmer erkennen, dass es einen Unterschied zwischen Tests mit einem kooperativen Opfer und Tests mit einem unwissenden Opfer gibt.

Im Anschluss an die Diskussion wird der erste praktische Teil der Laborübung durchgeführt. Die Studierenden haben soeben erörtert, welche Testszenarien es gibt und sollten dabei auch das Szenario des kooperativen Opfers kennengelernt haben. Auch sollten sie aus einer der vorgetragenen Arbeiten oder auch durch eigene Ideen die Möglichkeit erkannt haben, mithilfe von Modelliermasse (in diesem Fall Fimo) Vorlagen zur Herstellung von Attrappen zu erzeugen. Hierzu sollen nun Fimo-Attrappen erzeugt werden, damit die Studentinnen und Studenten selbst die Möglichkeit haben, die entsprechenden Arbeitsschritte kennenzulernen und einen solchen Versuchsablauf und dessen Dokumentation durchzuführen.

Jede Gruppe von Studierenden erhält zu diesem Zweck eine Packung Fimo, welche sich die Gruppenmitglieder untereinander aufteilen müssen. Jede Übungsteilnehmerin/Jeder Übungsteilnehmer soll nun aus dem ihr/ihm zur Verfügung stehenden Fimo zumindest zwei Vorlagen formen. Hierzu sollen die Studierenden das Fimo zunächst in gleich große Stücke teilen. Aus jedem Stück wird anschließend eine Kugel geformt, welche flach gedrückt wird. Dies soll dazu dienen, dass die Vorlagen nicht zu tief werden, wodurch (wie in Kapitel 4.5.1 beschrieben) mehr Attrappenmaterial benötigt wird und meist nicht so gute Ergebnisse erzielt werden. Weiters müssen die Studentinnen und Studenten darauf achten, die Vorlage, sobald der Finger hineingedrückt wurde, möglichst wenig zu bewegen, damit sie sich nicht verformt und somit unbrauchbar wird. Für die fertigen Attrappen erhält jeder Studierende ein Stück Backpapier, auf das der Name geschrieben wird und worauf die Vorlagen platziert werden. Dies soll dazu dienen, dass nach dem Brennen noch jeder/jedem Studierenden ihre/seine eigenen Vorlagen zugeordnet werden können. Um dies weiter zu vereinfachen, sollte nach Möglichkeit die Farbe der Modelliermasse jeder Gruppe unterschiedlich sein. Es sollte auch keine schwarze Modelliermasse verwendet werden, da diese nach dem Brennen nicht so einfach beschriftet werden kann.

Anschließend werden die Vorlagen zum Brennen für 30 Minuten bei 110° in den Heißluftofen gelegt. Während die Fimo-Vorlagen gebrannt werden, erläutert die/der Vortragende den Studentinnen und Studenten, welche anderen Möglichkeiten in dieser Arbeit durchgeführt wurden, um mithilfe eines kooperativen Opfers Vorlagen zu erzeugen. So erläutert sie/er, welche Erfolge oder auch Misserfolge bei der Erstellung von Wachs-Vorlagen erzielt wurden und worauf bei der Erstellung solcher Vorlagen zu achten ist. Es sollte kurz erklärt werden, dass für die Laborübung lediglich Fimo-Vorlagen jedoch keine Wachs-Vorlagen erstellt werden, weil Fimo einfacher zu handhaben ist und weil man länger damit arbeiten kann, als mit Wachs-Vorlagen, da diese beim Herauslösen der Attrappen oft zerstört werden. Auch soll kurz über die Versuche, eine Vorlage aus Silikon herzustellen, geredet und erklärt werden, warum diese nicht erfolgreich verlaufen sind. Während dieser Präsentation sollen die Studierenden jederzeit die Möglichkeit haben, Fragen zu stellen. Nach 30 Minuten werden die gebrannten Fimo-Vorlagen aus dem Ofen genommen. Die Präsentation der genannten Inhalte beziehungsweise eine etwaige Diskussion der zuvor erörterten Themen sollte danach fortgesetzt werden.

Nach der Präsentation werden die fertig gebrannten Fimo-Vorlagen an die Teilnehmerinnen und Teilnehmer der Übung verteilt, sodass jeder Studierende wieder die von ihr/ihm erzeugten Vorlagen erhält. Die Studentinnen und Studenten werden nun aufgefordert, ihre Vorlagen zu beschriften. Hierbei kann über ein geeignetes Beschriftungssystem diskutiert werden, welches eindeutig ist, zugleich aber auch prägnant genug, damit die Beschriftung auf dem Platz, der zur Verfügung steht, notiert werden kann. Gelangen die Studierenden zu keiner entsprechenden Lösung, so kann die/der Vortragende das folgende System vorgeben: „Gr. <Gruppennummer>“ gefolgt von „<Initialen des Gruppenmitgliedes>“ und „<Vorlagennummer>“. So würde die erste Vorlage des Studenten „Max Mustermann“ aus Gruppe 1 wie folgt lauten: „Gr. 1 MM 1“.
Bereits in der Diskussion zu Beginn dieser Einheit sollten unter anderem auch andere mögliche Materialien zur Herstellung von Attrappen genannt worden sein. Die/Der Vortragende soll die Studierenden nun noch einmal daran erinnern und auch erläutern, worauf die Übungsteilnehmerinnen und Übungsteilnehmer beim Füllen der Attrappen achten müssen. So sollten die Attrappen zwar gut gefüllt sein, allerdings nicht zu viel Attrappenmaterial verwendet werden, da das Trocknen sonst sehr lange dauert und die Attrappe beim Herauslösen oft zerstört wird. Nach diesen Erläuterungen werden der Holzleim und der Bastelkleber durchgereicht, und jede Studentin/jeder Student kann ihre/seine Attrappen damit befüllen. Da jeder Studierende zumindest zwei Fimo-Vorlagen gefertigt haben sollte, können beide Attrappenmaterialien von jedem Studierenden benutzt werden. Hat eine Teilnehmerin/ein Teilnehmer der Übung mehr als zwei Vorlagen gefertigt, steht es ihr/ihm frei, mit welchem der beiden Materialien sie/er die verbleibenden Vorlagen befüllt. Die gefüllten Vorlagen müssen anschließend an einem Platz aufbewahrt werden, an dem sie trocknen können und wo nicht die Gefahr besteht, dass sie jemand anderer irrtümlich entsorgt.

Bis zur **dritten Übungseinheit** sollten mindestens ein bis zwei Tage vergehen, damit die Attrappen auch wirklich gut getrocknet sind. Begonnen sollte die Einheit damit werden, dass die Studentinnen und Studenten mithilfe der „fragend-entwickelnden Methode“ erörtern, was bei den folgenden Schritten des Herauslösens der Attrappen und des Testens zu beachten ist. So soll die/der Vortragende sie dazu hinführen, dass für eine wissenschaftliche Dokumentation des Versuchsablaufes die Attrappen eindeutig beschriftet werden müssen, sodass sie sowohl der Person, von der sie stammen, als auch der Vorlage, mithilfe derer sie gefertigt wurden, zugeordnet werden können. Außerdem sollte den Studierenden erklärt werden, dass die Tests, welche anschließend mit den Attrappen durchgeführt werden, genau protokolliert werden müssen, das heißt, dass für jeden Test festgehalten werden muss, mit welcher Attrappe der Versuch durchgeführt wurde, welcher Scanner getestet wurde, um den wievielten Test dieser Attrappe an dem Scanner es sich handelt und natürlich, wie das Testergebnis lautet, also ob der Test erfolgreich war oder fehlgeschlagen ist oder ob der Scanner nicht reagiert hat.

Ein eindeutiges Beschriftungsschema der Attrappen kann von den Studierenden selbst vorgeschlagen werden. Kommt es zu keiner Einigung, welche eine eindeutige Referenzierbarkeit gewährleistet, kann das folgende Schema vorgeschlagen werden: <Beschriftung der Vorlage, aus der die Attrappe stammt> gefolgt von „/“ und <Nummer der Attrappe von dieser Vorlage>. Für die erste Attrappe aus der ersten Vorlage des Studenten „Max Mustermann“, welcher der Gruppe 1 angehört, würde sich so folgendes Schema ergeben: „Gr. 1 MM 1 / 1“.

Anschließend werden die befüllten Vorlagen an die Studentinnen und Studenten aufgeteilt. Diese beschriften die getrockneten Attrappen anhand des besprochenen Schemas und lösen sie vorsichtig aus der Vorlage heraus.
Als nächster Schritt wird den Studierenden erklärt, wie ein Täuschungsversuch an einem Fingerprint-Scanner abläuft. Hierzu wird in einer Präsentation von der/vom Vortragenden erläutert, wie das Enrolment beziehungsweise die Authentifizierung bei einem solchen System abläuft. Je nach Anzahl der zur Verfügung stehenden PCs und Scanner wird jeder Gruppe ein System zugeteilt, an welchem die Übungsteilnehmerinnen und Übungsteilnehmer der jeweiligen Gruppe mit jenem Finger das Enrolment durchführen, von dem die Vorlagen beziehungsweise Attrappen gefertigt wurden. Ist dies getan, sollen die Gruppen versuchen, den Scanner mit den Attrappen zu täuschen. Sämtliche Täuschungsversuche sind hierbei zu protokollieren. Um sicher zu stellen, dass ein etwaiges erfolgreiches Login auch tatsächlich durch die Attrappen zustande gekommen ist, sollten diese für die Tests an einem nicht enrolten Finger angebracht werden. Hierzu kann entweder ein hautfreundlicher Kleber verwendet werden. Alternativ kann versucht werden, die Attrappe ohne Kleber am Finger anzuheften, was bei entsprechender Hautfeuchtigkeit durchaus funktioniert. Die Mitglieder der Gruppe können nun der Reihe nach ihre Attrappen testen, wobei sie entweder selbst das Testprotokoll führen, oder aber ein Gruppenmitglied darum bitten, das Protokoll zu führen, um sich besser auf die Tests konzentrieren zu können.

Wenn alle Gruppen ihre Täuschungsversuche durchgeführt haben, soll jede Gruppe den anderen Gruppen in ein paar Worten mitteilen, welche Testergebnisse erreicht wurden. Natürlich soll auch hierbei darauf geachtet werden, dass die Testergebnisse wissenschaftlich kommuniziert werden. Daher sollen zu etwaig erfolgreichen Täuschungen konkrete Angaben gemacht werden, welche Attrappe verwendet wurde, wie oft der Scanner damit getäuscht werden konnte, ob eventuell etwas anders gemacht wurde, als bei den anderen Versuchen oder ob sonstige Unterschiede zu den anderen Tests beobachtet werden konnten, welche Rückschlüsse auf den Erfolg des Tests im Unterschied zu den anderen Tests zulassen. Die Übungsteilnehmerinnen und Übungsteilnehmer sollen daran erinnert werden, dass sie bisher lediglich das Szenario des kooperativen Opfers durchgespielt haben. Abschließend soll eine Diskussion eingeleitet werden, in der die Studierenden versuchen sollen, Schlüsse aus den Testergebnissen zu ziehen und zu erörtern, welche Aussagekraft die Ergebnisse der Tests hinsichtlich der Sicherheit von Fingerprint-Scannern haben. Auch soll die Relevanz in Hinsicht auf ein reales

Szenario in der Welt abseits der künstlich hergestellten Versuchsanordnung diskutiert werden. Abschließend werden die Fimo-Vorlagen der Studentinnen und Studenten wieder eingesammelt und verwahrt, da sie in einer späteren Einheit noch einmal verwendet werden.

In der **vierten Einheit der Laborübung** soll das Augenmerk der Studierenden auf das zweite große Versuchsszenario gerichtet werden – auf das Täuschen des Fingerprint-Scanners mit unwissendem Opfer. Zunächst soll den Teilnehmerinnen und Teilnehmern der Übung noch einmal erläutert werden, inwiefern sich das Szenario von jenem mit kooperativem Opfer unterscheidet. Dabei soll gezeigt werden, dass es in diesem Szenario einer anderen Vorgehensweise bedarf, da bereits vor dem Herstellen der Vorlagen diverse Schritte durchgeführt werden müssen. Der erste Schritt wäre hierbei das Sichtbarmachen des hinterlassenen Fingerabdruckes des Opfers. Dies soll nun auch mit den Studierenden versuchsweise durchgespielt werden. Ziel hierbei ist es weniger, die Tätigkeit des Sichtbarmachens selbst zu erlernen, sondern viel mehr, dass die Studentinnen und Studenten lernen, einen Prozess zu dokumentieren, welcher scheinbar einfach durchzuführen ist und bei dem kaum signifikante Werte existieren, welche gemessen werden können. Sie sollen dabei erkennen, dass selbst scheinbar triviale Tätigkeiten eines Versuchsablaufes wissenschaftlich dokumentiert werden können, indem zumindest sämtliche verwendeten Materialien genannt werden, und dass man so gut wie möglich beschreibt, wie vorgegangen wurde. Außerdem soll den Studierenden klar werden, dass Erkenntnisse, welche während der Versuche gewonnen wurden, auch als Hinweise in der Dokumentation niedergeschrieben werden müssen, um das Nachstellen eines so dokumentierten Versuches zu vereinfachen.

Um das Sichtbarmachen eines Fingerabdruckes durchzuführen, werden zunächst an jeden Studierenden eine Glasplatte und ein feiner Pinsel ausgeteilt. Die Glasplatte muss lediglich so groß sein, dass zwei oder drei Fingerabdrücke darauf derart hinterlassen werden können, dass sie getrennt voneinander mit Grafitpulver sichtbar gemacht werden können (Es kann beispielsweise die Glasplatte eines kleinen Bilderrahmens verwendet werden). Pro Gruppe steht des weiteren eine Glasplatte zum Eindampfen von Fingerabdrücken zur Verfügung. Da die Cyanacrylatrückstände von eingedampften Fingerabdrücken kaum zu entfernen sind, muss hier damit gerechnet werden, dass diese Glasplatte nach den Tests nicht wieder verwendet werden kann. Außerdem erhält jede Studentin/jeder Student einen Deckel zum Überstülpen der Stelle, an der das Eindampfen eines Abdruckes durchgeführt wird.

Die Studierenden sollen nun zunächst ein paar Fingerabdrücke auf ihrer Glasplatte hinterlassen. Dabei sollen sie unterschiedliche Finger benutzen und versuchen die Aufdruckstärke zu variieren. Interessant wäre hier beispielsweise auch, ob der Größenunterschied der Finger eine Relevanz hat, also ob beispielsweise der Abdruck eines Daumens leichter sichtbar gemacht werden kann als der Abdruck eines kleinen Fingers. Außerdem soll jede Studentin/jeder Student der Gruppe einen Fingerabdruck auf der Glasplatte

hinterlassen, welche zum Eindampfen mit Cyanacrylat gedacht ist. Diese Abdrücke müssen genug Abstand voneinander aufweisen, damit die Deckel zum Eindampfen über die einzelnen Abdrücke gestellt werden können.

Der Superkleber mit Cyanacrylatanteil wird durchgereicht und die Studierenden verteilen ein paar Tropfen des Superklebers auf der Unterseite ihres Deckels. Diesen stülpen sie anschließend über den von ihnen hinterlassenen Fingerabdruck auf der dafür vorgesehenen Glasplatte. Danach sollen sie versuchen, die anderen Fingerabdrücke mit dem Grafitpulver, welches ebenfalls durchgegeben wird, zu bestäuben und mithilfe des feinen Pinsels das Pulver so zu verteilen, dass der Abdruck gut sichtbar ist. Das restliche Pulver sollen sie nach Möglichkeit von der Glasplatte entfernen, ohne den sichtbar gemachten Fingerabdruck zu zerstören. Hierbei soll natürlich darauf geachtet werden, dass das Grafitpulver nicht im ganzen Raum verteilt wird, weil es Flecken hinterlassen kann.

Wenn alle Studentinnen und Studenten ihre Fingerabdrücke zumindest mit Grafitpulver sichtbar gemacht haben, soll jede Gruppe kurz über die gewonnenen Erfahrungen berichten, ob sie es schwierig fanden, die Aufgabe durchzuführen, ob es Probleme gab und worauf man achten muss. Auch sollen sie beurteilen, ob es ihrer Meinung nach einen Unterschied macht, ob ein großer oder kleiner Finger den Abdruck hinterlassen hat oder ob die Stärke des Aufdrückens die Qualität des Abdrucks beeinflusst. Falls einer der eingedampften Abdrücke bereits sichtbar ist, soll natürlich darüber berichtet werden. Es kann jedoch durchaus passieren, dass viele der eingedampften Abdrücke noch ein wenig Zeit benötigen, bis sie gut sichtbar sind. Sollte dies der Fall sein, kann in einem zweiten Durchgang jede Gruppe auch über ihre Erfahrungen mit Cyanacrylat berichten. Die Studentinnen und Studenten sollen durch diese kurze Zusammenfassung der von ihnen durchgeführten Arbeit lernen, einen scheinbar trivialen Ablauf möglichst genau und in wissenschaftlicher Sprache zu beschreiben.

Anschließend werden die Glasplatten abgewaschen, um das restliche Grafitpulver und die Fingerabdrücke zu entfernen. Zudem wird versucht, die Cyanacrylatrückstände zu entfernen. Es ist jedoch, wie bereits erwähnt, damit zu rechnen, dass diese nicht von jeder Glasplatte entfernt werden können, weshalb für diese Versuche von vornherein nur eine Glasplatte pro Gruppe zur Verfügung steht, um so Kosten einzusparen.

Die/Der Vortragende sollte nun versuchen, mit den Studierenden in einer Gesprächsrunde deren Erfahrungen zu diskutieren und mit den Erkenntnissen, die der Autor in dieser Arbeit sammeln konnte, zu vergleichen. Außerdem sollten die Unterschiede zwischen einer Laborsituation und den Abläufen in einem realen Szenario in der Welt abseits der gestellten Versuchsanordnung verglichen werden. In der Diskussion soll darauf hingewiesen werden, dass in einem Szenario, in welchem nicht solche optimalen Bedingungen gegeben sind, wie in den gerade durchgeführten Versuchen, das Nehmen von Fingerabdrücken um einiges schwieriger sein kann. Hier soll den Studentinnen

und Studenten unter anderem klar werden, dass beispielsweise die Oberflächenbeschaffenheit und auch der Hintergrund des Fingerabdruckes beim Fingerabdrucknehmen durchaus eine Rolle spielen. Die/Der Vortragende soll die Diskussion in eine Präsentation überleiten, in der sie/er den Studierenden zeigt, wie die weiteren Bearbeitungsschritte im Szenario eines unwissenden Opfers aussehen würden. Dabei soll auf das Digitalisieren der Abdrücke eingegangen werden, welche Möglichkeiten es dafür gibt und welche Probleme dabei auftreten können. Auch die Nachbearbeitung am Computer soll den Studierenden gezeigt werden und exemplarisch an einem Fingerabdruck vorgeführt werden. Natürlich wäre es auch eine Möglichkeit die Übungsteilnehmerinnen und Übungsteilnehmer dies selbst ausprobieren zu lassen. Dies wurde in diesem Konzept allerdings nicht weiter betrachtet, da hierfür PCs und Lizenzen für die entsprechenden Grafikprogramme verfügbar sein müssten. Zwar wäre es möglich die Bearbeitungsschritte mit den Studierenden in einem lizenzfreien Programm wie Gimp (siehe Kapitel 4.4.2.2) oder Paint.net (siehe Kapitel 4.4.2.3) durchzuführen, es wäre allerdings nicht der Vergleich zu Programmen wie Photoshop möglich. Eine eigenständige Durchführung einer entsprechenden Nachbearbeitung würde zudem den Zeitrahmen der Laborübung sprengen.

In der **fünften Einheit der Laborübung** wird den Studentinnen und Studenten erklärt, wie mit den nachbearbeiteten Fingerlinienbildern nun eine Vorlage zur Erstellung von Attrappen hergestellt werden kann. Hierzu erläutert die/der Vortragende wie mithilfe einer Folienvorlage eine Leiterplatte belichtet werden kann und wie man die belichtete Leiterplatte anschließend entwickeln und ätzen kann.

Es wird nun jedem Studierenden eine fotosensitiv beschichtete Leiterplatte und eine Folie ausgehändigt, wobei auf der Folie 6 nachbearbeitete Fingerlinienbilder eines enrolten Fingers abgedruckt sind. Jede Teilnehmerin/Jeder Teilnehmer der Übung soll somit 6 Vorlagen auf seine Leiterplatte ätzen. Die/Der Vortragende erklärt den Studierenden, wie mit dem Belichtungsgerät zu arbeiten ist. Anschließend können die Leiterplatten mit dem Belichtungsgerät selbstständig belichtet werden. Die Schutzfolie der fotosensitiven Schicht sollte hierbei erst direkt vor dem Belichten abgezogen werden. Während die Leiterplatten belichtet werden, können jene Studentinnen und Studenten, die noch darauf warten, ihre Platine belichten zu können, sowie jene, welche ihre Platine bereits belichtet haben, den Entwickler (Natriumhydroxid) in einer Plastikwanne in Wasser auflösen. Auch das Ätzmittel kann bereits angesetzt werden. Hierfür muss das Natriumpersulfat in heißem Wasser (40 - 50 °Celsius) aufgelöst und auf dieser Temperatur gehalten werden. Das kann dadurch erreicht werden, indem man die Plastikwanne mit der Ätzlösung in ein Wasserbad stellt, dem ständig heißes Wasser zugeführt wird. Wenn es die Gegebenheiten zulassen, ist es sinnvoll, mehrere Wannen mit Entwicklerlösung und Ätzmittel bereitzustellen, damit mehrere Studierende zugleich ihre Leiterplatten ätzen können. Sobald die Entwicklerlösung fertig aufgelöst ist, kann die/der erste Studierende, deren/dessen Leiterplatte belichtet ist, diese für ein paar Minuten im Entwicklerbad schwenken. Schnell wird sie/er

erkennen, dass die fotosensitive Schicht mit dem Entwickler reagiert. Sie/Er muss dazu angehalten werden, die Leiterplatte dennoch nicht gleich wieder aus dem Entwickler zu entfernen, sondern die Platine zumindest drei bis vier Minuten entwickeln zu lassen. Anschließend wird die Platine in die Ätzlösung gelegt und während des Ätzvorganges leicht geschwenkt. Sobald die/der erste Studierende mit dem Entwickeln fertig ist, kann die/der nächste seine Leiterplatte entwickeln. Um schneller voranzukommen, ist es, wie bereits erwähnt, sinnvoll mehrere Plastikwannen mit Entwicklerlösung und Ätzmittel zur Verfügung zu stellen. Wenn eine Übungsteilnehmerin/ein Übungsteilnehmer ihre/seine Platine fertig geätzt hat, muss diese noch abgespült und getrocknet werden. Während die Leiterplatten der letzten Studentinnen und Studenten geätzt werden, kann von der/vom Vortragenden präsentiert werden, zu welchen Ergebnissen und Erkenntnissen der Autor dieser Diplomarbeit in seinen Versuchen gelangt ist. Auch ein Bezug zum Artikel des Chaos Computer Club (1) und die darin beschriebene Methode, Vorlagen herzustellen, ist noch einmal aufzunehmen. In diesem Artikel wird behauptet, dass man lediglich nachbearbeitete Fingerabdruckbilder mit einem Laserdrucker auf Folie auszudrucken müsse, wodurch die Ablagerungen des Toners genug Struktur erzeugen würden, um die Folie als Vorlage zur Herstellung von Attrappen zu verwenden.

Auch diese Theorie kann mit den Studierenden getestet werden. Hierfür werden, nachdem die letzten Studentinnen und Studenten ihre Leiterplatten fertig geätzt, abgespült und getrocknet haben, erneut Holzleim und Bastelkleber ausgegeben. Vor dem Befüllen sollen die Vorlagen auf den Leiterplatten wieder nach einem geeigneten Schema beschriftet werden. Die Studierenden sollen anschließend ein paar der erstellten Leiterplatten-Vorlagen befüllen. Hierbei sollten jedoch nicht alle Vorlagen auf der Leiterplatte verwendet werden, da sich der Holzleim und der Bastelkleber nur in seltenen Fällen gut aus ihnen lösen lassen und die Vorlage dadurch unbrauchbar wird oder zumindest ausgekocht werden müsste, um sie zu reinigen. Um dem vorzubeugen, können die Vorlagen mit einer hauchdünnen Schicht fetthaltiger Creme oder aber mit Sprüh-Öl versehen werden. Auch können die zum Belichten der Leiterplatten benutzten Folien dazu verwendet werden, die Methode, welche im Artikel des CCC erläutert wird, zu prüfen. Hierzu können die darauf befindlichen Abdrucke der Fingerabdrücke, wie im Artikel des CCC beschrieben, mit Holzleim bestrichen werden. Auch die Vorlagen auf der Folie müssen nach geeignetem Schema beschriftet werden. Die Leiterplatten und Folien werden anschließend zum Trockenen bis zur nächsten Einheit weggeschlossen, damit sie nicht unabsichtlich entsorgt werden.

In der abschließenden **sechsten Übungseinheit** sollen die Studierenden die Attrappen testen, welche mit den Leiterplatten-Vorlagen sowie mit den Folienvorlagen erstellt wurden. Außerdem sollen in einem abschließenden Versuch Attrappen aus Gelatine hergestellt und getestet werden. Zunächst werden die befüllten Leiterplatten und die Folien an die Studentinnen und Studenten ausgeteilt. Diese müssen die Attrappen von den Vorlagen lösen und nach geeignetem Schema beschriften. Wie bei den anderen Einheiten sollen die

Studierenden dazu motiviert werden, sich über ein geeignetes Beschriftungsschema Gedanken zu machen. Es ist jedoch damit zu rechnen, dass eine solche Diskussion entfällt, weil es den Studierenden durch die vorangegangenen Übungen mittlerweile sehr leicht fallen sollte, rasch ein geeignetes Beschriftungsschema zu finden. Bevor die von den Vorlagen gelösten Attrappen getestet werden, sollten die Vorlagen zunächst mit Gelatine befüllt werden, damit die Gelatine aushärten kann, während die Übungsteilnehmerinnen und Übungsteilnehmer ihre Holzleim- und Bastelkleber-Attrappen testen. Dazu müssen die Studierenden unter Aufsicht der/des Vortragenden zunächst Gelatine aufkochen und anschließend die Vorlagen damit füllen. Außerdem kann mit verschiedenen Gelatine-Arten experimentiert werden und auch getestet werden, welches Mischverhältnis von Wasser und Gelatine sich am besten zur Herstellung von Attrappen eignet. Zum Befüllen werden auch die in einer der vorigen Laborübungen erstellten Fimo-Vorlagen wieder an die Studierenden ausgeteilt. Somit können sowohl Aussagen über die Gelatine-Attrappen als auch über einen etwaigen Unterschied der Gelatine-Attrappen verschiedener Vorlagen gemacht werden. Nach dem Befüllen werden die Vorlagen zum schnelleren Aushärten in den Kühlschrank gestellt.

Die Studentinnen und Studenten können, während die Gelatine-Attrappen aushärten, an den ihnen zugeteilten PCs und Scannern ihre Holzleim- und Bastelkleber-Attrappen testen. Auch diese Tests sollen protokolliert werden, um einen kontrollierbaren Vergleich zu den bisherigen Tests zu haben. Nachdem die Attrappen getestet wurden, sollten auch die Gelatine-Attrappen ausgehärtet sein. Die Leiterplatten- und Fimo-Vorlagen werden daher wieder an die Übungsteilnehmerinnen und Übungsteilnehmer ausgeteilt, die die Attrappen von den Vorlagen lösen. Anschließend sollen auch sämtliche Gelatine-Attrappen getestet und die Abläufe und Testergebnisse sollen von den Studierenden dokumentiert werden.

In der Folge sollen die Teilnehmerinnen und Teilnehmer der Übung in einer Diskussion ihre Testergebnisse vergleichen und deren Relevanz erörtern. Außerdem soll betrachtet werden, ob und welche Unterschiede zwischen den Tests mit kooperativem Opfer und denen mit unwissendem Opfer existieren. Ebenso soll über die verwendeten Methoden und Materialien reflektiert werden, um noch einmal einen Überblick über die gesamte Übung zu erhalten.

5.2.5) Übersicht eines möglichen Übungsablaufs

Auf den folgenden Seiten werden die vorher ausführlich dargestellten Übungsinhalte zur besseren Übersichtlichkeit tabellarisch zusammengefasst. Konkret sollen dabei noch einmal die Inhalte und Ziele sowie die benötigten Materialien (Medien) und die verwendeten didaktischen Methoden präsentiert werden.

1. Übungseinheit			
Inhalt	**Methode**	**Ziel**	**Medien**
Einführung	Frontalunterricht	Die Studierenden sollen über die Lernziele und den Ablauf der Laborübung informiert werden.	PC, Beamer
Vorstellung bisheriger Arbeiten zum Thema	Frontalunterricht	Die Studierenden sollen einen Überblick über die Thematik erlangen.	PC, Beamer
Diskussion über die vorgestellten Arbeiten	Fragend-entwickelnde Methode	Die Studierenden sollen ein Gefühl dafür entwickeln, was die Wissenschaftlichkeit einer Arbeit ausmacht.	
Einführung in mögliche Testszenarien zum geplanten Thema	Fragend-entwickelnde Methode, Problem Based Learning	Die Studierenden entwickeln Ideen, mit welchen Mitteln und Methoden sie Fingerprint-Scanner testen könnten.	

2. Übungseinheit			
Inhalt	**Methode**	**Ziel**	**Medien**
Erzeugen von Fimo-Vorlagen	Partnerarbeit	Die Studierenden sollen erste Erfahrungen mit der Durchführung und Dokumentation wissenschaftlicher Versuche sammeln.	Fimo, Ofen (Heißluft)
Erläuterung anderer Vorgehensweisen	Frontalunterricht	Die Studierenden sollen andere Möglichkeiten kennenlernen, Vorlagen zu erstellen sowie deren mögliche Nachteile diskutieren.	PC, Beamer
Eindeutige und systematische Kennzeichnung der Fimo-Vorlagen	Fragend-entwickelnde Methode, Problem Based Learning	Die Studierenden sollen das Problem einer eindeutig referenzierbaren Beschriftung erkennen und zu lösen versuchen.	Markierungsstift
Befüllen der Vorlagen	Partnerarbeit	Herstellung von Attrappen aus Holzleim und Bastelkleber.	Holzleim, Bastelkleber

3. Übungseinheit			
Inhalt	**Methode**	**Ziel**	**Medien**
Einleitung und Diskussion über eine eindeutige Beschriftung	Fragend-entwickelnde Methode, Problem Based Learning	Die Studierenden sollen eine eindeutige Beschriftung entwickeln und lernen, wie wissenschaftliche Versuche dokumentiert werden.	
Beschriftung der Attrappen	Partnerarbeit	Die Bezeichnung der Attrappe soll mit der Vorlage und der Person referenzierbar sein.	befüllte Fimo-Vorlagen, Stift
Erläuterung der Tests	Frontalunterricht	Die Studierenden werden über das weitere Vorgehen informiert.	PC, Beamer
Enrolment der Fingerabdrücke	Partnerarbeit	Die Studierenden bereiten die Testsysteme auf die Tests vor.	PC, Fingerprint-Scanner
Tests der Attrappen	Partnerarbeit	Die Studierenden üben das Protokollieren wissenschaftlicher Tests.	PC, Scanner
Diskussion und Präsentation der Testergebnisse	Fragend-entwickelnde Methode	Die Gruppen diskutieren ihre Testergebnisse und lernen etwaige Erfolge wissenschaftlich zu formulieren und mit Fakten zu unterlegen.	
Diskussion der Relevanz der Testergebnisse	Problem Based Learning	Die Studierenden erkennen den Unterschied zwischen Versuchen im Labor und Abläufen in einer Welt außerhalb solch optimaler Voraussetzungen.	

4. Übungseinheit

Inhalt	Methode	Ziel	Medien
Einleitung	Frontalunterricht	Die Studierenden sollen mit dem Versuchsszenario des unwissenden Opfers vertraut werden.	PC, Beamer
Sichtbarmachen von Fingerabdrücken	Partnerarbeit	Die Studierenden sollen lernen, dass selbst bei scheinbar trivialen Arbeiten, auf die wissenschaftliche Beschreibung der Durchführung zu achten ist.	Glasplatten, weicher Pinsel, Grafitpulver, Cyanacrylat, Deckel (Plastik)
Diskussion der Ergebnisse	Fragend-entwickelnde Methode, Problem Based Learning	Die Studierenden erkennen den Unterschied zwischen Versuchen im Labor und Abläufen in einer Welt außerhalb solch optimaler Voraussetzungen.	
Einblick in die weiterführende Bearbeitung	Frontalunterricht	Die Studierenden werden über die weitere Bearbeitung im Szenario des unwissenden Opfers informiert.	PC, Beamer

5. Übungseinheit			
Inhalt	**Methode**	**Ziel**	**Medien**
Einleitung	Frontalunterricht	Die Studierenden werden auf die bevorstehenden praktischen Arbeiten vorbereitet.	PC, Beamer
Belichten der Leiterplatten	Partnerarbeit	Die Studierenden belichten die Leiterplatten.	fotosensitiv beschichtete Leiterplatten, Folie mit nachbearbeitetem Fingerprint zum Belichten
Herstellen der Vorlagen aus Leiterplatten	Partnerarbeit	Die Studierenden entwickeln und ätzen die belichteten Leiterplatten, um daraus Vorlagen zu erstellen.	Natriumhydroxid, Natriumpersulfat, belichtete Leiterplatten, Plastikwannen, Schutzkleidung
Beschriftung der Vorlagen	Partnerarbeit	Die Studierenden beschriften die Vorlagen, damit diese später referenziert werden können.	Markierungsstift
Befüllung der Vorlagen	Partnerarbeit	Die Studierenden erstellen aus den Leiterplatten-Vorlagen sowie den Folienvorlagen Attrappen.	Holzleim, Bastelkleber, Creme/Sprühöl

6. Übungseinheit

Inhalt	Methode	Ziel	Medien
Beschriftung der Attrappen	Partnerarbeit	Die erstellten Attrappen sind mit der Vorlage und der Person, von der sie stammen, referenzierbar.	Markierungsstift
Herstellung von Gelatine-Attrappen	Partnerarbeit	Es sollen Gelatine-Attrappen erzeugt werden, um einen Unterschied zu anderen Attrappenmaterialien feststellen zu können.	Gelatine, Kochplatte, Leiterplatten-Vorlagen, Fimo-Vorlagen, Kühlschrank
Test der Holzleim- und Bastelkleber-Attrappen von Leiterplatten- und Folienvorlagen	Partnerarbeit	Die Studierenden testen die erzeugten Attrappen, um das wissenschaftliche Protokollieren zu üben und Vergleiche zu den vorangegangenen Tests anstellen zu können.	PC, Fingerprint-Scanner
Test der Gelatine-Attrappen	Partnerarbeit	Die Studierenden testen die neu erstellten Attrappen, um einen Vergleich zu anderen Attrappenmaterialien durchführen zu können.	PC, Fingerprint-Scanner
Diskussion über die Testergebnisse und Gespräch über die Erkenntnisse aus den Übungseinheiten	Fragend-entwickelnde Methode	Die Studierenden sollen den Unterschied zwischen den beiden Testszenarien erkennen und die Auswirkung unterschiedlicher Materialien zur Attrappenherstellung beschreiben können.	

6) Conclusio

Biometrie ist gerade in der heutigen Zeit ein aktuelles Thema und keineswegs mehr Science-Fiction. So werden an vielen Flughäfen mittlerweile biometrische Systeme verwendet (65) und in Österreich ist der biometrische Pass bereits Realität. Seit geraumer Zeit ist es nötig, dass das Porträtfoto bestimmten Kriterien entspricht, um als Passfoto verwendet werden zu können. Diese Kriterien dienen jedoch lediglich dazu, ein möglichst gutes Referenzbild zu liefern, mit dessen Hilfe die Identität der Passinhaberin/des Passinhabers kontrolliert werden kann (66). Seit Ende März 2009 werden in den Pässen österreichischer Staatsbürgerinnen/Staatsbürger auch zwei Fingerabdrücke der Passinhaberin/des Passinhabers gespeichert (67). Die allgegenwärtige Präsenz des Themas Biometrie, deren Anwendung sowie der Gefahren, die dadurch entstehen können, gaben den Anstoß zu dieser Arbeit.

Nach dem Studium der Quellliteratur schien es zu Beginn der Arbeit relativ einfach zu werden, einen Fingerabdruck-Scanner zu täuschen. So erweckt der Artikel des Chaos Computer Club (1) den Eindruck, dass ein entsprechendes System im Handumdrehen überlistet werden kann, wobei nur einfachste Büromaterialien vonnöten seien, um dies zu bewerkstelligen. Auch in anderen Arbeiten zu diesem Thema wird dies behauptet, wie in dem wohl bekanntesten und in den meisten Arbeiten zu diesem Thema zitierten Artikel von Tsutomu Matsumoto. Auch hier wird beschrieben, wie einfach ein „Gummy" Finger hergestellt und ein Fingerprint-Scanner mit diesem getäuscht werden kann (3).

Entsprechend hoch waren auch die Erwartungen den Versuchen dieser Arbeit gegenüber. Es stellte sich jedoch bereits nach den ersten Versuchen heraus, dass das Erstellen einer funktionstüchtigen Attrappe nicht ganz so einfach ist, wie es in der Quellliteratur dargestellt wird. Hier muss noch einmal erwähnt werden, dass in den existierenden Arbeiten die Herstellung von Attrappen meist nur ungenau erklärt wurde. So wird zwar meist auf alle wesentlichen Punkte eingegangen, allerdings bleiben (bewusst oder unbewusst) manche Details oft unerwähnt. So wird in kaum einer Arbeit erwähnt, mit welchen Programmen und Methoden digitalisierte Fingerabdrücke weiter verarbeitet wurden. Oft wird nur die Versuchsanordnung mit einem kooperativen Opfer gewählt, um zu zeigen, wie eine Attrappe hergestellt wird, mit der ein Fingerprint-Scanner getäuscht werden kann. Dies ist natürlich ein legitimer Ansatz und wurde auch in dieser Arbeit untersucht. Allerdings ist es ein wenig einseitig, nur diese Versuchsanordnung zu testen, wie dies zum Beispiel bei Johan Blommé (34) der Fall ist.

Auch zeigten die Versuche, dass der Fingerprint durchaus nicht fälschungssicher ist. Er kann in der Tat kopiert werden. Es müssen allerdings immer auch die Rahmenbedingungen betrachtet werden, unter denen ein Kopieren des Abdruckes möglich ist. So ist es relativ einfach möglich, und auch in den Versuchen dieser Arbeit gelungen, eine funktionstüchtige Fingerabdruck-Attrappe anzufertigen, wenn man mit einem kooperativen Opfer arbeitet. Anders sieht die Sache jedoch aus, wenn man versucht, den Fingerabdruck

einer fremden Person ohne deren Einwilligung zu kopieren. Meist wird in diesem Zusammenhang immer davon ausgegangen, dass man über einen Gegenstand verfügt, welcher einen einwandfreien Abdruck der Person aufweist. In der Realität spielen hier jedoch viele weitere Faktoren eine Rolle (36). So darf der Gegenstand möglichst nur von dieser einen Person angefasst worden sein, da man sonst nicht sicher sein kann, wessen Fingerabdrücke man verarbeitet. Auch darf die Person den Gegenstand nicht zu oft angefasst haben, da sich die Abdrücke sonst überlagern oder verwischen. Auch die Oberfläche des Gegenstandes spielt hierbei eine gewisse Rolle, wie in Kapitel 4.2.1 bereits ausgeführt wurde. Weiters ist zu bedenken, dass es sich nach Möglichkeit um einen leicht beweglichen Gegenstand handeln sollte, der entwendet werden kann. Will man einen Fingerabdruck von einem Türgriff oder dergleichen nehmen, wird dies kaum möglich sein, ohne dabei bemerkt zu werden oder zumindest Spuren (Grafitpulver oder Cyanacrylat-Rückstände) zu hinterlassen (36).

Ein weiterer wichtiger Punkt ist, ob man das Prozedere des Nachmachens eines Fingerabdruckes zum ersten Mal durchführt oder ob man bereits Erfahrung mit der Materie gesammelt hat. Denn dementsprechend verändert sich natürlich auch der zeitliche Aufwand beim Herstellen einer Attrappe. In den Versuchen zeigte sich, dass man als Anfängerin/Anfänger auf diesem Gebiet, welche/welcher über wenig oder keine Erfahrung verfügt, relativ viel Zeit benötigt, um zu einer Attrappe zu gelangen. Arbeitet man mit einem kooperativen Opfer, ist es natürlich auch für eine Anfängerin/einen Anfänger leicht möglich, eine Attrappe herzustellen. Lediglich die genaue zeitliche Abschätzung, wann eine Attrappe aushärtet, ist erfahrungsabhängig. Somit wäre der Wiederholungsaufwand beim Erstellen von Attrappen mit kooperativem Opfer, also der zeitliche Aufwand für eine Person mit Erfahrung, nur unwesentlich geringer als der Aufwand einer Anfängerin/eines Anfängers. Genaue Angaben zu der Zeit, die die Herstellung braucht, können nicht gemacht werden, da diese stark von den jeweils verwendeten Materialien abhängig ist. So muss eine Anfängerin/ein Anfänger ebenso wie eine erfahrene Testerin/ein erfahrener Tester bei der Herstellung einer Fimo-Vorlage mit einer Dauer von circa 30 Minuten rechnen. Die Herstellung einer Wachsvorlage kann in knapp 10 Minuten bewerkstelligt werden. Die Zeit, welche die Attrappe zum Trocknen benötigt, ist natürlich abhängig vom verwendeten Material und von der Dicke der Attrappe (Menge des verwendeten Materials). Hier kann eine erfahrene Testerin/ein erfahrener Tester den Vorteil haben, dass sie/er besser abschätzen kann, wann die Attrappe getrocknet ist.

Geht man von einer Versuchsanordnung mit unwissendem Opfer aus, so ergeben sich durchaus zeitliche Unterschiede zwischen einer Anfängerin/einem Anfänger und einer Testerin/einem Tester mit hinlänglicher Erfahrung. Schließlich muss berücksichtigt werden, dass eine Anfängerin/ein Anfänger sich erst in die Materie einarbeiten muss. So muss eine Testerin/ein Tester ohne Vorwissen erst ausprobieren, wie ein Latenzabdruck gut sichtbar gemacht werden kann und worauf beispielsweise bei der Verwendung von Grafitpulver geachtet werden muss. Auch muss sie/er erst erproben, mit

welchen Methoden ein digitalisierter Fingerabdruck verbessert werden kann und welche Methoden weniger Erfolg versprechend sind. Auch das Belichten und Ätzen von Leiterplatten sind für eine Person, die noch nie mit solchen Materialien und den benötigten Chemikalien gearbeitet hat, sicherlich schwieriger als für eine erfahrene Benutzerin/einen erfahrenen Benutzer. So kann es einer Anfängerin/einem Anfänger leicht passieren, dass eine Leiterplatte zu lange oder zu kurz belichtet wurde. Hier ist eine Testerin/ein Tester mit entsprechender Erfahrung und Vorwissen in dieser Thematik klar im Vorteil. Allein das Sichtbarmachen von Fingerabdrücken geht einer geübten Person schneller von der Hand. Die Person erspart sich auch viel Zeit durch ihr Wissen mit welchen Programmen und mit welchen Methoden dieser Programme ein Bild gut nachbearbeiten werden kann. Letztlich kann ebenfalls durch die Erfahrung im Belichten und Ätzen von Leiterplatten Zeit gespart werden. In Summe muss eine Anfängerin/ein Anfänger für eine erste Attrappe mit einem zeitlichen Aufwand von gut zehn Stunden rechnen. Weiß man hingegen bereits, worauf bei den einzelnen Verarbeitungsschritten zu achten ist, so ist lediglich ein Aufwand von circa drei Stunden zu erwarten (Wiederholungsaufwand). In beiden Fällen hält man danach lediglich eine Attrappe in Händen und weiß noch nichts über ihre Funktionstüchtigkeit. So kann es durchaus passieren, dass der Aufwand umsonst war, da die Attrappe gar nicht funktioniert. Auch in den Versuchen musste dies festgestellt werden, da hier bis auf wenige Ausnahmen keine der im Szenario eines ahnungslosen Opfers erzeugten Attrappen den Scanner täuschen konnten.

Die Versuche dieser Arbeit belegen daher, dass viele der bisherigen Arbeiten das Thema sehr oberflächlich behandeln und lediglich zeigen, dass ein Scanner mithilfe eines kooperativen Opfers getäuscht werden kann. Andere Artikel, wie jener des Chaos Computer Clubs, scheinen nach den durchgeführten Versuchen mehr darauf abzuzielen, die Bevölkerung aufzurütteln, damit auch biometrische Systeme kritisch hinterfragt werden und nicht als absolut sicher angesehen werden. Die Versuche zeigten jedoch auch, dass Fingerprint-Scanner nicht so einfach zu täuschen sind, wie dies zu Beginn der Arbeit, beeinflusst durch die Quellliteratur, angenommen wurde. In dieser Arbeit hat sich also gezeigt, dass Fingerprint-Scanner mit einfachen und leicht verfügbaren Mitteln nicht so leicht zu täuschen sind. Abschließend muss jedoch gesagt werden, dass nicht ausgeschlossen werden kann, dass andere, zum Zeitpunkt dieser Arbeit nicht bekannte und im Rahmen dieser Arbeit nicht getestete Methoden und Mittel existieren, mithilfe derer das Fälschen eines Abdruckes beziehungsweise das Herstellen einer geeigneten Attrappe auch ohne kooperatives Opfer möglich ist.

Literaturverzeichnis

1. **Chaos Computer Club.** Wie können Fingerabdrücke nachgebildet werden? [Online] 9. Oktober 2004. http://www.ccc.de/biometrie/fingerabdruck_kopieren.xml?language=de.

2. **Kaseva, Antti und Stén, Antti.** Fooling Fingerprint Scanners. [Online] März 2003. http://www.stdot.com/pub/ffs/GiveMeAFinger.pdf.

3. **Matsumoto, Tsutomu, et al.** Impact of Artificial "Gummy" Fingers on Fingerprint Systems. *Proceedings of SPIE.* 2002. Bd. 4677.

4. **ISO/IEC Group 1.** Harmonized Biometric Vocabulary. [Online] http://www.3dface.org/media/vocabulary.html.

5. **Bromba, Manfred.** Biometrie FAQ. [Online] 16. Februar 2008. http://www.bromba.com/faq/biofaqd.htm.

6. **Wikipedia.** Biometrie. [Online] http://de.wikipedia.org/wiki/Biometrie.

7. **Jain, Anil K., Ross, Arun und Prabhakar, Salil.** An Introduction to Biometric Recognition. *Transactions on circuits and systems for video technology.* s.l. : IEEE, 2004. Bd. 14, 1.

8. **Jain, Anil, Hong, Lin und Pankanti, Sharath.** Biometric Identification. *Communications of the ACM.* s.l. : ACM, 2000. Bd. 43, 2.

9. **Bala, Deepthi.** Biometrics and Information Security. *InfoSecCD Conference'08.* Kennesaw, USA : ACM, 2008.

10. **Sukhai, Nataliya B.** Access Control & Biometrics. *Proceedings of the 1st Annual Conference on information Security Curriculum Development.* Kennesaw, Georgia : ACM, 2004.

11. **Kulkarni, Sujata.** Multimode Biometrics for Personal Identification. *International Conference on Advances in Computing, Communication and Control (ICAC3'09).* Mumbai : ACM, 2009.

12. **Jain, Anil K. und Ross, Arun.** Multibiometric Systems. *Communications of the ACM.* s.l. : ACM, 2004. Bd. 47, 1.

13. **Bhargav-Spantzel, Abhilasha, Squicciarini, Anna und Bertino, Elisa.** Privacy Preserving Multi-Factor Authentication with Biometrics. *Proceedings of the second ACM workshop on Digital identity management.* s.l. : ACM, 2006.

14. **Wikipedia.** Biometrics. [Online] http://en.wikipedia.org/wiki/Biometric.

15. **Heckle, Rosa R., Patrick, Andrew S. und Ozok, Ant.** Perception and Acceptance of Fingerprint Biometric Technology. *Symposium On Usable Privacy and Security (SOUPS).* s.l. : ACM, 2007.

16. **Galkin, Anastasia.** Iriserkennung. [Online] 2002. http://ni.cs.tu-berlin.de/lehre/sem-biometrie/Galkin_Iris.pdf.

17. **Daugman, John.** How Iris Recognition Works. *Transactions on circuits and systems for video technology.* 2004. Bd. 14, 1.

18. **Wikipedia.** Iris Erkennung. [Online] http://de.wikipedia.org/wiki/Iris-Erkennung.

19. **Daugman, John.** John Daugman. [Online] http://www.cl.cam.ac.uk/~jgd1000/.

20. **Petermann, Thomas und Sauter, Arnold.** Biometrische Identifikationssysteme. [Online] 2002. http://www.tab.fzk.de/de/projekt/zusammenfassung/ab76.pdf.

21. **Wikipedia.** Retinal Scan. [Online] http://en.wikipedia.org/wiki/Retinal_scan.

22. **Feltin, Bryan.** Information Assurance Using Biometrics. [Online] 2002. http://www.giac.org/certified_professionals/practicals/gsec/2052.php.

23. Retinography. [Online] http://www.discoveriesinmedicine.com/Ra-Thy/Retinography.html.

24. **Haluschak, Bernhard.** Biometrie Grundlagen - Vom Fingerprint bis zur Gesichtserkennung. *Tec Channel.* [Online] Januar 2009. http://www.tecchannel.de/sicherheit/identity_access/402320/grundlagen_mehr_sicherheit_mit_biometrie/index.html.

25. **Gerdesmeier, Simone.** Biometrische Zugangskontrollen. [Online] 2006. http://www.uni-hildesheim.de/~mandl/Lehre/ubi/biometrie.pdf.

26. **Wikipedia.** Eigenfaces. [Online] http://en.wikipedia.org/wiki/Eigenface.

27. **Turk, Matthew A. und Pentland, Alex P.** Face Recognition Using Eigenfaces. *IEEE Computer Society Conference on Computer Vision and Pattern Recognition, 1991. Proceedings CVPR '91.* 1991.

28. **Cremerius, Ralf und Snurnikov, Leonid.** Biometrie und Datenschutz. [Online] 2006. http://waste.informatik.hu-berlin.de/Lehre/ss06/SE_ueberwachung/vortrag5.pdf.

29. **Johnson, Margret L.** Biometrics and the Threat to Civil Liberties. *IEEE Computer.* 2004, Bd. 37, April 2004.

30. **Wikipedia.** Speaker Recognition. [Online] http://en.wikipedia.org/wiki/Speaker_recognition.

31. —. Fingerabdruck. [Online] http://de.wikipedia.org/wiki/Fingerabdruck.

32. —. AFIS. [Online] http://de.wikipedia.org/wiki/Automatisiertes_Fingerabdruckidentifizierungssystem.

33. **International Biometric Group.** Biometrics Market and Industry Report 2009 - 2014. [Online] 2008. http://www.biometricgroup.com/reports/public/market_report.php.

34. **Blommé, Johan.** Evaluation of biometric security systems against artificial fingers. *Thesis.* [Online] Linköping, 2003. http://www.ep.liu.se/exjobb/isy/2003/3514/.

35. **Theofanos, Mary, et al.** Does Habituation Affect Fingerprint Quality? *CHI '06 Extended Abstracts on Human Factors in Computing Systems.* Montréal, Québec, Canada : ACM, 2006.

36. **Bromba, Manfred.** Fingerprint FAQ. [Online] 2009. http://www.bromba.com/faq/fpfaqd.htm.

37. **Harris, Tom.** How Fingerprint Scanners work. *How stuff works.* [Online] 24. September 2002. http://computer.howstuffworks.com/fingerprint-scanner.htm.

38. **Mainguet, Jean-Francois.** *Fingerprints.* [Online] März 2009. http://pagesperso-orange.fr/fingerchip/biometrics/types/fingerprint.htm.

39. **Wikipedia.** Kondensator. [Online] http://de.wikipedia.org/wiki/Kondensator_(Elektrotechnik).

40. —. Elektrostatische Entladung. [Online] http://de.wikipedia.org/wiki/Elektrostatische_Entladung.

41. **Optel.** Comparing Ultrasound with Conventional Finger-Scan Technologies. [Online] 2002. http://www.optel.pl/article/deutsch/comparing.htm.

42. **Schuckers, Stephanie A. C.** Spoofing and Anti-Spoofing Measures. *Information Security Technical Report.* s.l. : Elsevier Science Ltd., 2002. Bd. 7, 4.

43. **Sandström, Marie.** Liveness Detection in Fingerprint Recognition Systems. *Thesis.* [Online] Linköping, 2004. http://www.ep.liu.se/exjobb/isy/2004/3557/.

44. **Drahansky, M.** Experiments with Skin Resistance and Temperature for Liveness Detection. *International Conference on Intelligent Information Hiding and Multimedia Signal Processing.* s.l. : IEEE, 2008.

45. **van der Putte, Ton und Keuning, Jeroen.** Biometrical Fingerprint Recognition: Don't get your fingers burned. *Proceedings of the Fourth Working Conference on Smart Card Research and Advanced Applications on Smart Card Research and Advanced Applications.* Bristol, United Kingdom : s.n., 2001.

46. **Derakhshani, Reza, et al.** Determination of vitality from a non-invasive biomedical measurement for use in fingerprint scanners. *Pattern Recognition.* s.l. : Elsevier Science Ltd., 2003. Bd. 36, 2.

47. **Ratha, Nalini K., Connell, Jonathan H. und Bolle, Ruud M.** An Analysis of Minutiae Matching Strength. *Proceedings of the Third international Conference on Audio- and Video-Based Biometric Person Authentication.* London : Springer-Verlag, 2001.

48. **Faúndez-Zanuy, Marcos.** On the Vulnerability of Biometric Security Systems. *A&E Systems Magazine.* s.l. : IEEE, 2004.

49. **McMillen, Robert.** Researcher Hacks Microsoft Fingerprint Reader. *PCWorld.* [Online] 2006. http://www.pcworld.com/article/124978/researcher_hacks_microsoft_fingerprint_reader.html.

50. **Jain, Anil K. und Uludag, Umut.** Hiding Biometric Data. *IEEE Transaction on pattern analysis and machine intelligence.* s.l. : IEEE, 2003. Bd. 25, 11.

51. **Hein, Stefan und Mahrla, Markus.** Überwindungsszenarien für biometrische Systeme. [Online] 2004. http://www2.informatik.hu-berlin.de/Forschung_Lehre/algorithmenII/Lehre/SS2004/Biometrie/09Ueberwindung/Ueberwindung/index.html.

52. **Kleine-Albers, Daniel, Tokar, David und Uhe, Pascal.** Versuch: Fingerabdruck (Teil 2). [Online] 2006. http://www.dka-edv.de/dka/cms/index.php?option=com_docman&task=doc_download&gid=6.

53. **Thalheim, Lisa, Krissler, Jan und Ziegler, Peter-Michael.** Körperkontrolle - Biometrische Zugangssicherung auf die Probe gestellt. *c't.* November 2002. S. 114ff.

54. **Digitus.** Digitus USB Fingerprint Reader. [Online] http://www.digitus.info/de/produkte/zubehoer/?c=1215&p=3577.

55. **Bromba, Manfred.** Biometrie und Sicherheit. [Online] 2002. http://www.bromba.com/knowhow/biosich.htm.

56. **Wikipedia.** Histogrammspreizung und -stauchung. *Punktoperator (Bildverarbeitung).* [Online] http://de.wikipedia.org/wiki/Punktoperator_(Bildverarbeitung)#Histogrammspreizung_und_-stauchung.

57. **Barthel, Kai Uwe.** Bildmanipulation II: Filter. [Online] 2007. http://www.f4.fhtw-berlin.de/~barthel/veranstaltungen/SS07/Mete1/vorlesungen/filter.pdf.

58. **Wikipedia.** Schwellwertverfahren. [Online] http://de.wikipedia.org/wiki/Schwellwertverfahren.

59. **Gimp.** GNU Image Manipulation Program. [Online] http://www.gimp.org/.

60. **Eberhard Faber Gmbh.** Eberhard Faber. [Online] http://www.eberhardfaber.de/FIMO_Material.EBERHARDFABER.

61. **Krijnen, Kees.** PCB Etching. [Online] 2008. http://sfprime.net/pcb-etching/index.htm.

62. **Wikipedia.** Ultraviolettstrahlung. [Online] http://de.wikipedia.org/wiki/Ultraviolettstrahlung.

63. **Reich, Kersten.** Konstruktiver Methodenpool der Uni Köln. [Online] http://methodenpool.uni-koeln.de/uebersicht.html.

64. **Einecke, G.** Partnerarbeit. [Online] http://www.fachdidaktik-einecke.de/7_Unterrichtsmethoden/partnerarbeit_neu.htm.

65. **Andreas Grote.** Flughäfen in Amsterdam und Oakland setzen auf Biometrie. *heise online.* [Online] http://www.heise.de/newsticker/Flughaefen-in-Amsterdam-und-Oakland-setzen-auf-Biometrie–/meldung/22147.

66. Passbild Kriterien. [Online] http://www.passbildkriterien.at/oesterreich_neu.html.

67. **Österreichischer Nationalrat.** Der Reisepass mit Fingerabdruck kommt. [Online] 2009. http://www.parlament.gv.at/PG/PR/JAHR_2009/PK0023/PK0023.shtml.

68. **Schneier, Bruce.** Crypto-Gram. *Biometrics: Truths and Fictions.* [Online] August 1998. http://www.schneier.com/crypto-gram-9808.html#biometrics.

69. —. Crypto-Gram. *Fun with Fingerprint Readers.* [Online] Mai 2002. http://www.schneier.com/crypto-gram-0205.html#5.

70. **Biomedical Signal Analysis Laboratory.** Liveness Detection in Biometric Devices. [Online] http://people.clarkson.edu/~biosal/research/liveness.html.

71. **Wikipedia.** Microsoft Fingerprint Reader. [Online] http://en.wikipedia.org/wiki/Microsoft_Fingerprint_Reader.

72. **Bicz, Wieslaw.** Fingerprint structure imaging based on an ultrasound camera. *Instrumentation Science & Technology.* [Online] 1999. http://www.optel.com.pl/article/english/article.htm.

73. **International Biometric Group.** Indipendent Testing of Iris Recognition Technology. [Online] 2005. http://www.biometricgroup.com/reports/public/ITIRT.html.

74. **Bromba, Manfred.** Über die Unbrauchbarkeit der Biometrie. [Online] 5. Februar 2008. http://www.bromba.com/knowhow/KleineAnleitung.htm.

75. **Campell, Edward D.** Fingerprints & Palmar Dermatoglyphics. [Online] 1998. http://www.edcampbell.com/PalmD-History.htm.

76. **Kent, Jonathan.** Malysia car thieves steal finger. *BBC News.* [Online] 31. März 2005. http://news.bbc.co.uk/1/hi/world/asia-pacific/4396831.stm.

77. **Leyden, John.** Gummi bears defeat fingerprint sensors. *The Register.* [Online] Mai 2002. http://www.theregister.co.uk/2002/05/16/gummi_bears_defeat_fingerprint_sensors/.

78. **Mainguet, Jean-Francois.** Movies & Biometrics. [Online] http://pagesperso-orange.fr/fingerchip/biometrics/movies.htm.

79. —. Retinal. [Online] 2009. http://pagesperso-orange.fr/fingerchip/biometrics/types/retinal.htm.

80. **Manhart, Dr. Klaus.** Sicher durch Biometrie. *Tec Channel.* [Online] Januar 2002. http://www.tecchannel.de/sicherheit/identity_access/401777/sicher_durch_biometrie/index.html.

81. **Matsomoto, Tsutomu.** Importance of Open Discussion on Adversarial Analysis for Mobile Security Technologies - A Case Study for User Identification. *ITU-T Workshop on Security.* [Online] 2002. http://www.scribd.com/doc/3622378/Matsumoto-Labratory-Artificial-Fingers-for-Fingerprint-Scanners.

82. **Ratha, Nalini K., Connell, Jonathan H. und Bolle, Ruud M.** Secure Data Hiding in Wavelet Compressed Fingerprint Images. *Proceedings of the 2000 ACM Workshops on Multimedia.* Los Angeles : ACM, 2000.

83. **Ross, Arun, Jain, Anil und Pankanti, Sharat.** A Hand Geometry Based Verification System. *Proceedings of 2nd Int'l Conference on Audio- and Video-based Biometric Person Authentication (AVBPA).* 1999.

84. **Schneier, Bruce.** Inside risks: the uses and abuses of biometrics. *Communications of the ACM.* s.l. : ACM, August 1999. Bd. 42, 8.

85. **Chaos Computer Club.** Hacking biometric systems. *Die Datenschleuder.* 2004. Bd. 84.

86. **Club, Chaos Computer.** Fingerabdrücke nachmachen leichtgemacht. *Die Datenschleuder.* 2005. Bd. 87.

Abbildungsverzeichnis

Tabellenverzeichnis

Appendix A

Die Tabellen zeigen die Testergebnisse der einzelnen Attrappen der Tests des Microsoft Fingerprint-Readers. Die Testpersonen, welche in den Tabellen als TP1 und TP2 bezeichnet werden, sind wie folgt charakterisiert:

- Testperson 1 - TP1 – männlich, 26 Jahre
- Testperson 2 - TP2 – weiblich, 23 Jahre

Bei den Bezeichnungen der Attrappen spiegelt die erste Ziffer die Nummerierung der Vorlagen wider. Die letzte Ziffer steht für die Nummer der Attrappe. Bei den Leiterplatten-Vorlagen wurden stets mehrere Abdrücke pro Platine geätzt. Daher existiert hier auch eine mittlere Ziffer, welche die Position der Vorlage auf der Platine beschreibt. Aus Platzgründen wurde in den Tabellen Testperson mit „TP“, Wachs mit „W_“ und Platine mit „Pl_“ abgekürzt. In den Tabellen bezeichnet „o“ ein geglücktes Login, „x“ ein fehlgeschlagenes Login“ und „n“ heißt, dass der Scanner nicht auf die Attrappe reagiert hat.

Tabelle 29: Testergebnisse - Fimo - Holzleim – koop. Opfer - Microsoft

TP	Attrappe	Testdurchlauf																			
		1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20
TP1	Fimo1_1	n	o	o	o	n	n	x	o	o	o	o	x	n	o	n	o	x	n	n	n
	Fimo1_2	o	o	o	n	n	n	x	x	n	o	o	o	o	o	x	n	n	o	o	o
	Fimo1_3	n	x	x	n	x	x	x	x	x	n	n	x	n	n	n	x	x	x	n	x
	Fimo1_4	n	n	n	n	x	o	o	o	o	o	o	o	n	n	o	o	o	x	x	n
TP2	Fimo2_1	n	o	o	x	o	n	o	o	o	o	o	n	o	x	n	n	n	o	o	o
	Fimo2_2	o	o	x	n	n	x	o	o	o	o	n	n	n	x	x	o	o	o	o	n
TP2	Fimo3_1	n	n	x	x	x	x	x	x	x	n	n	x	x	x	x	n	x	x	x	x
	Fimo3_2	x	x	x	x	n	n	n	n	n	n	n	x	x	n	x	x	x	n	n	n
TP1	Fimo4_1	o	n	o	o	x	x	n	n	o	o	o	o	o	o	o	o	n	n	x	x
	Fimo4_2	n	n	x	o	o	o	o	o	n	n	n	o	o	n	n	x	x	o	o	n
	Fimo4_3	o	o	o	n	n	o	o	o	o	n	x	x	n	n	n	o	x	o	o	o
TP1	Fimo5_1	n	n	n	x	n	x	x	x	x	x	n	n	n	n	n	x	n	n	n	n
	Fimo5_2	x	n	n	n	n	n	n	x	x	x	n	n	x	n	n	n	n	x	x	x
	Fimo5_3	x	x	x	n	n	n	n	x	x	n	n	n	n	n	n	n	x	n	n	n
TP2	Fimo6_1	n	n	o	o	o	n	o	o	o	o	n	x	x	n	n	n	o	o	x	n
	Fimo6_2	o	o	o	o	o	n	n	x	o	o	n	n	o	o	o	o	o	x	x	o
	Fimo6_3	n	o	o	o	n	n	n	n	n	n	o	o	n	n	o	o	o	o	o	n
TP2	Fimo7_1	x	x	x	x	x	n	x	x	x	x	n	n	x	x	x	n	n	n	n	n
	Fimo7_2	x	x	x	x	n	n	n	x	x	x	x	x	x	n	n	n	x	x	x	x
	Fimo7_3	n	x	n	n	n	n	x	x	x	x	x	n	n	x	x	n	n	n	n	x
TP1	Fimo8_1	x	x	x	n	x	x	n	n	n	n	n	x	x	x	n	n	x	x	x	x
	Fimo8_2	x	n	n	n	x	x	x	n	n	n	n	n	x	x	n	x	x	x	n	n
	Fimo8_3	x	x	x	x	n	x	n	n	n	x	x	x	x	x	n	n	x	n	n	n
TP1	Fimo9_1	o	o	o	n	n	n	n	n	n	n	o	o	o	o	o	o	x	o	o	o
	Fimo9_2	o	o	o	o	o	n	x	n	n	n	n	n	o	o	o	o	n	n	n	n

TP	Attrappe	Testdurchlauf																			
		1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20
TP2	Fimo10_1	o	o	n	n	n	n	n	o	o	o	o	x	n	n	x	o	o	n	n	n
	Fimo10_2	n	n	n	n	o	o	o	o	x	n	n	o	o	o	o	o	n	x	x	n
	Fimo10_3	n	x	o	o	o	o	n	n	o	o	o	o	x	n	n	n	o	o	o	x
TP2	Fimo11_1	o	o	n	n	x	x	n	o	o	o	o	n	n	x	o	o	o	n	n	n
	Fimo11_2	n	n	n	o	o	o	o	o	x	n	o	o	o	o	o	x	o	o	n	n
TP1	Fimo12_1	x	n	x	x	n	n	x	x	x	x	x	n	n	n	x	x	x	n	x	x
	Fimo12_2	n	n	n	x	x	x	x	x	x	n	n	n	x	x	n	x	n	n	n	n
TP1	Fimo13_1	o	o	o	n	n	n	n	x	o	o	o	o	o	n	n	n	o	o	x	n
	Fimo13_2	n	o	o	o	n	x	o	o	o	o	n	n	n	n	o	o	o	o	x	x
	Fimo13_3	o	o	o	o	o	o	x	n	n	o	o	o	n	n	x	x	o	o	o	n
TP2	Fimo14_1	x	x	n	x	n	n	x	x	x	n	x	x	n	n	n	n	n	n	n	n
	Fimo14_2	x	x	x	x	n	n	x	x	n	n	n	n	n	n	x	x	x	n	x	x
TP2	Fimo15_1	o	o	o	o	x	n	n	o	o	o	x	n	n	o	o	x	o	o	n	n
	Fimo15_2	o	o	o	n	n	o	o	o	o	x	o	o	x	n	n	n	n	n	n	n
	Fimo15_3	n	n	x	x	x	n	n	x	n	n	n	n	n	x	x	x	x	x	x	x
	Fimo15_4	n	n	n	n	n	o	o	o	x	n	o	o	o	x	n	n	n	x	x	n
TP1	Fimo16_1	o	n	o	x	o	o	o	o	n	n	n	o	n	o	o	x	n	n	n	n
	Fimo16_2	o	o	o	n	n	o	o	o	o	o	x	n	n	o	o	o	n	x	o	o
	Fimo16_3	o	n	o	o	x	n	n	n	o	o	o	o	n	n	x	o	o	o	o	o
TP1	Fimo17_1	x	x	x	x	n	n	x	x	x	n	n	n	n	x	x	x	x	x	x	n
	Fimo17_2	x	x	n	n	n	n	n	n	n	n	n	x	x	x	x	x	n	x	n	n
	Fimo17_3	x	x	x	x	n	n	x	x	x	x	x	x	n	n	n	n	n	x	x	n
TP1	Fimo18_1	x	x	n	n	n	x	x	x	x	n	n	n	n	x	x	x	x	n	n	n
	Fimo18_2	x	x	n	n	x	x	n	x	x	x	x	n	n	n	n	x	x	x	x	x
	Fimo18_3	n	n	n	n	n	x	x	x	n	n	x	x	x	x	x	n	n	n	n	n
TP1	Fimo19_1	x	x	n	n	n	x	x	n	n	n	n	n	x	x	x	n	n	n	n	x
	Fimo19_2	o	o	o	x	n	n	n	o	o	o	x	o	n	n	x	o	o	x	o	o
	Fimo19_3	o	x	n	n	n	o	o	o	o	o	n	n	n	x	o	n	n	x	x	n
TP1 [1]	Fimo20_1	x	x	x	x	n	n	x	x	x	n	n	n	n	n	n	x	x	x	x	x
TP2	Fimo21_1	x	x	n	n	n	n	x	x	x	x	x	n	n	x	x	x	n	n	n	n
	Fimo21_2	x	x	x	x	x	n	n	x	x	x	n	n	n	n	x	x	x	x	n	n
	Fimo21_3	x	x	n	n	x	x	x	x	x	n	n	n	n	x	x	x	n	n	n	n
TP2	Fimo22_1	x	x	x	x	n	n	n	x	x	n	n	x	x	x	n	n	n	n	n	n
	Fimo22_2	n	n	n	x	x	x	x	x	x	x	x	n	n	n	n	x	x	x	x	n
	Fimo22_3	n	n	x	x	x	x	x	n	n	n	n	x	x	x	n	n	n	n	n	n
TP2	Fimo23_1	x	x	n	n	n	x	x	x	x	n	n	n	n	x	n	n	n	n	x	x
	Fimo23_2	x	x	x	x	n	n	n	n	n	n	n	n	x	x	x	x	x	x	n	n
	Fimo23_3	x	x	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n
TP2	Fimo24_1	o	o	o	x	n	n	n	n	o	o	o	o	x	o	n	n	n	x	o	o
	Fimo24_2	n	n	n	n	o	o	x	n	n	n	n	n	x	o	o	o	o	o	x	o
	Fimo24_3	n	n	o	x	o	o	o	n	n	n	n	o	o	o	o	n	n	x	o	o

[1] Vorlage verzogen – keine weiteren Attrappen hergestellt

Tabelle 30: Testergebnisse - Fimo - Bastelkleber – koop. Opfer - Microsoft

TP	Attrappe	Testdurchlauf																			
		1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20
TP1	Fimo1_1	o	o	o	o	x	n	n	n	n	o	o	n	x	o	o	x	o	n	n	n
	Fimo1_2	o	o	o	x	o	o	x	o	o	n	n	n	n	o	o	o	x	n	n	n
	Fimo1_3	n	n	n	o	x	o	o	o	o	o	o	n	n	n	x	o	o	o	n	n
	Fimo1_4	n	n	n	n	n	o	o	o	x	o	o	o	o	o	n	n	n	x	x	n
TP2	Fimo2_1	n	n	n	o	o	o	o	x	n	n	n	o	o	x	o	n	n	n	n	n
	Fimo2_2	n	n	n	n	n	n	n	n	n	o	o	x	o	o	o	o	o	x	o	o
TP2	Fimo3_1	x	x	x	n	n	x	x	n	n	n	n	n	x	x	x	n	n	n	n	n
	Fimo3_2	n	x	x	x	x	x	x	n	n	n	n	n	x	x	x	x	n	n	n	n
TP1	Fimo4_1	n	n	o	o	o	o	o	x	n	n	n	n	n	n	o	o	x	n	o	o
	Fimo4_2	o	n	n	n	n	n	n	n	o	o	o	x	n	n	n	n	o	x	o	o
	Fimo4_3	n	n	n	n	n	o	o	o	x	o	o	n	n	n	n	x	o	o	n	n
TP1	Fimo5_1	x	x	x	x	x	n	n	n	n	x	x	x	x	x	n	x	x	x	n	n
	Fimo5_2	x	n	n	x	x	x	x	x	n	n	n	x	x	x	x	n	n	n	x	x
	Fimo5_3	x	x	x	x	n	n	n	n	n	n	n	n	x	x	x	x	x	x	x	n
TP2	Fimo6_1	n	n	n	n	n	n	n	n	o	o	o	x	o	n	n	n	x	o	o	n
	Fimo6_2	n	n	o	o	o	x	o	n	n	n	o	o	o	x	n	n	n	n	o	o
	Fimo6_3	n	n	n	n	o	o	o	o	x	n	n	n	n	n	o	o	o	n	x	n
TP2	Fimo7_1	n	n	x	x	x	x	n	n	n	x	x	x	x	x	x	x	n	n	x	x
	Fimo7_2	x	x	x	x	x	x	x	x	x	n	n	x	x	x	n	n	n	n	n	n
	Fimo7_3	n	n	n	n	n	x	x	x	n	n	x	x	x	x	x	x	n	n	n	x
TP1	Fimo8_1	x	x	n	n	n	n	n	x	x	x	x	x	x	x	n	n	x	x	x	x
	Fimo8_2	n	x	x	x	x	n	n	n	n	n	n	x	n	n	n	x	x	x	n	n
	Fimo8_3	x	x	x	x	x	n	n	n	n	n	n	x	x	x	x	x	x	n	n	n
TP1	Fimo9_1	n	n	n	o	o	o	o	x	o	n	n	x	o	o	o	n	n	n	n	n
	Fimo9_2	o	o	o	n	n	n	n	n	o	o	n	n	n	n	n	x	o	o	o	o
TP2	Fimo10_1	n	n	o	o	o	n	n	n	n	n	n	o	x	o	o	o	n	n	n	n
	Fimo10_2	n	n	n	n	n	n	x	o	o	o	o	o	n	n	n	n	x	o	o	o
	Fimo10_3	o	o	n	n	n	n	x	o	o	x	n	n	n	n	x	x	o	o	n	n
TP2	Fimo11_1	n	n	n	o	o	o	o	n	n	n	n	o	x	n	n	n	n	o	o	x
	Fimo11_2	n	n	o	o	o	n	n	n	n	x	x	n	n	o	o	o	o	o	n	n
TP1	Fimo12_1	n	n	n	x	x	x	x	n	n	x	x	x	x	x	n	n	x	x	x	n
	Fimo12_2	n	n	n	n	x	x	x	x	x	x	n	n	n	n	x	x	x	n	n	n
TP1	Fimo13_1	o	o	n	n	n	n	n	o	o	o	o	x	n	n	n	n	o	o	x	x
	Fimo13_2	n	n	n	o	o	o	n	n	x	o	o	o	o	n	x	o	o	n	n	n
	Fimo13_3	n	n	o	o	o	o	x	n	n	n	n	n	o	o	o	o	x	n	n	n
TP2	Fimo14_1	n	n	n	n	x	x	x	n	n	x	x	x	x	x	x	n	n	x	x	n
	Fimo14_2	x	x	x	n	n	x	x	x	x	x	n	n	n	x	x	x	x	n	n	n
TP2	Fimo15_1	n	n	o	o	o	o	n	n	x	o	o	o	o	o	x	o	x	n	n	o
	Fimo15_2	n	o	n	o	o	o	n	n	o	o	o	n	n	n	o	o	n	o	x	x
	Fimo15_3	n	n	n	x	o	o	o	o	n	n	n	o	o	n	n	x	o	n	n	n
	Fimo15_4	n	x	o	o	o	x	x	o	o	o	o	o	n	n	n	n	n	o	o	o

TP	Attrappe	Testdurchlauf																			
		1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20
TP1	Fimo16_1	n	n	o	o	o	o	x	n	o	o	x	n	n	n	o	o	o	n	n	n
	Fimo16_2	o	o	o	n	n	o	o	o	o	n	n	n	n	x	o	x	o	o	n	n
	Fimo16_3	n	n	o	o	o	o	n	n	x	o	o	o	o	n	o	o	x	n	n	o
TP1	Fimo17_1	n	n	n	x	x	x	n	n	x	x	x	x	x	x	n	n	x	x	x	x
	Fimo17_2	x	x	x	x	n	n	n	n	x	n	x	x	x	n	x	x	x	x	n	n
	Fimo17_3	x	x	n	n	n	n	x	x	x	x	n	n	n	n	n	x	x	n	n	x
TP1	Fimo18_1	n	n	n	x	x	x	x	x	n	n	x	x	x	x	n	n	x	n	n	n
	Fimo18_2	n	x	n	n	x	x	x	x	n	x	x	n	n	n	x	x	x	x	x	n
	Fimo18_3	x	x	n	x	n	x	x	x	x	n	n	n	n	n	x	x	n	n	x	x
TP1	Fimo19_1	o	o	n	n	n	o	o	o	x	n	n	x	x	o	o	n	n	o	o	o
	Fimo19_2	o	n	o	o	n	n	n	o	o	o	n	o	o	n	n	x	x	o	o	n
	Fimo19_3	n	o	x	o	o	o	n	n	x	o	o	o	o	n	n	o	o	o	n	n
TP2	Fimo21_1	n	n	x	x	x	x	x	x	n	n	x	x	n	n	n	n	x	x	x	x
	Fimo21_2	x	x	n	n	x	n	n	x	n	n	n	n	x	x	x	x	x	x	x	n
	Fimo21_3	x	x	n	x	n	x	x	n	x	x	x	x	x	n	x	n	n	x	n	x
TP2	Fimo22_1	n	n	n	x	n	x	x	x	x	n	n	x	x	x	x	x	x	n	n	x
	Fimo22_2	n	x	n	x	n	n	x	x	n	n	n	x	n	n	x	x	x	n	x	n
	Fimo22_3	n	n	n	n	n	x	x	n	x	x	n	n	n	x	n	n	n	n	x	n
TP2	Fimo23_1	n	n	x	x	x	n	x	x	x	x	n	x	x	n	x	n	n	n	n	n
	Fimo23_2	x	x	x	n	n	x	x	x	x	x	x	n	n	x	n	x	n	n	x	n
	Fimo23_3	x	n	n	x	n	x	n	n	x	x	x	x	n	x	n	n	x	n	x	x
TP2	Fimo24_1	n	x	o	o	o	o	o	o	x	n	o	o	n	n	n	x	o	o	o	o
	Fimo24_2	o	n	o	o	n	n	n	n	o	o	o	o	x	x	o	o	n	n	n	n
	Fimo24_3	n	o	o	x	o	n	o	o	o	n	n	n	n	o	o	n	n	o	x	x

Tabelle 31: Testergebnisse - Fimo - Silikon – koop. Opfer - Microsoft

TP	Attrappe	Testdurchlauf																			
		1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20
TP1	Fimo1_1[2]	x	x	x	n	n	n	x	n	n	n	n	n	n	n	x	x	n	n	n	n
TP2	Fimo2_1	n	n	x	o	o	o	o	o	n	n	n	o	o	x	o	n	n	n	n	n
	Fimo2_2	o	o	n	n	n	o	o	o	o	o	x	n	n	o	o	o	o	x	n	n
TP2	Fimo3_1	n	n	n	x	x	x	x	x	n	n	x	x	x	n	x	n	x	x	n	n
	Fimo3_2	x	x	n	x	x	n	n	x	x	x	n	x	x	n	x	x	x	n	n	x
TP1	Fimo4_1[3]	n	x	x	n	x	x	x	x	n	n	n	x	n	n	n	x	x	x	n	n
TP1	Fimo5_1	x	x	n	n	n	n	n	n	x	x	x	x	x	x	n	n	x	x	x	x
	Fimo5_2	n	n	n	x	x	x	x	x	n	n	x	x	x	n	n	x	x	x	n	n
	Fimo5_3	n	n	x	x	x	n	n	n	n	n	n	x	x	x	x	x	n	n	n	n
TP2	Fimo6_1[4]	n	n	n	n	n	x	x	n	n	n	n	x	n	n	x	x	x	x	n	n
TP2	Fimo7_1[5]	n	n	x	x	x	x	n	n	n	x	n	n	n	x	x	n	n	n	n	n
TP1	Fimo8_1	n	n	x	x	x	x	n	x	n	n	n	x	n	x	x	x	x	n	n	x
	Fimo8_2	x	x	x	n	x	n	n	n	x	n	x	x	n	x	n	x	x	x	x	n
	Fimo8_3	n	x	n	x	x	x	n	n	n	n	n	x	x	n	x	n	x	x	x	x
TP1	Fimo9_1	n	n	o	o	o	x	n	o	x	o	o	o	n	o	o	x	n	n	n	n
	Fimo9_2	n	n	n	x	x	o	o	o	n	n	x	o	o	o	o	n	n	x	o	o
TP2	Fimo10_1	o	x	o	o	o	n	n	o	o	n	n	n	n	x	x	n	o	o	n	n
	Fimo10_2	n	n	n	o	o	o	x	x	o	o	o	o	o	n	n	o	o	x	n	n
	Fimo10_3	n	n	o	x	o	n	o	o	o	n	n	n	o	o	o	o	x	n	n	o
TP2	Fimo11_1	n	n	n	n	x	o	o	o	n	o	o	x	o	o	o	o	n	n	n	n
	Fimo11_2	n	o	o	o	o	x	o	o	o	n	n	n	n	o	n	n	n	o	x	x
TP1	Fimo12_1	n	n	x	x	x	x	n	n	x	x	x	x	n	n	n	n	n	x	x	x
	Fimo12_2	n	n	n	n	x	x	x	n	x	x	n	n	n	x	x	x	x	x	n	x
TP1	Fimo13_1	n	n	x	x	x	x	x	n	n	n	n	x	x	n	n	n	x	n	n	n
	Fimo13_2	n	x	x	n	n	n	x	x	x	x	x	n	n	n	x	n	x	n	n	n
	Fimo13_3	x	x	n	x	x	x	x	n	n	n	x	x	x	n	n	x	n	n	n	n
TP2	Fimo14_1	n	n	x	x	x	x	n	x	x	x	n	n	x	x	n	n	n	n	x	x
	Fimo14_2	x	x	n	x	n	x	x	x	n	n	n	x	x	n	n	x	x	x	x	n
TP2	Fimo15_1	x	n	x	x	x	x	n	n	x	x	x	n	n	n	n	n	x	x	n	n
	Fimo15_2	n	x	n	x	n	x	x	x	x	n	x	n	n	x	x	x	n	x	n	x
	Fimo15_3	n	n	n	n	n	x	x	x	n	x	n	n	n	x	n	x	x	x	x	n
	Fimo15_4	n	n	x	x	x	x	x	n	n	x	x	x	n	x	x	n	n	x	n	n
TP1	Fimo16_1	n	n	n	n	o	o	o	x	o	o	x	n	n	o	o	o	x	n	n	n
	Fimo16_2	o	o	n	n	x	x	o	o	o	x	n	n	n	n	n	n	n	o	o	n
	Fimo16_3	n	n	o	o	o	x	n	o	o	n	n	n	n	o	o	o	x	n	n	n
TP1	Fimo17_1	n	n	n	x	x	x	x	x	x	n	n	n	x	x	x	x	n	n	n	n
	Fimo17_2	n	x	x	x	x	x	n	n	x	x	x	x	n	n	n	n	x	x	x	n
	Fimo17_3	x	x	x	n	n	x	x	x	x	n	n	n	n	n	x	x	n	n	n	x

[2] Fimo1 wurde durch zu klebriges Silikon zerstört – als Ersatz wurde Fimo25 gefertigt
[3] Fimo4 wurde durch zu klebriges Silikon zerstört – als Ersatz wurde Fimo26 gefertigt
[4] Fimo6 wurde durch zu klebriges Silikon zerstört – als Ersatz wurde Fimo27 gefertigt
[5] Fimo7 wurde durch zu klebriges Silikon zerstört – als Ersatz wurde Fimo28 gefertigt

TP	Attrappe	Testdurchlauf																			
		1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20
TP1	Fimo18_1	x	n	n	x	x	x	x	n	n	n	x	x	x	x	x	n	x	x	n	n
	Fimo18_2	x	x	x	x	x	n	n	x	x	x	x	n	n	n	x	x	n	x	x	x
	Fimo18_3	n	n	x	x	x	n	x	x	x	x	n	n	n	n	n	n	x	x	n	x
TP1	Fimo19_1	n	o	o	o	n	x	o	o	o	o	o	x	n	n	o	o	x	n	n	n
	Fimo19_2	n	n	n	n	o	o	o	x	o	n	n	o	o	o	x	n	o	o	o	n
	Fimo19_3	o	o	o	n	n	n	x	o	o	n	n	n	x	x	o	o	o	n	n	n
TP2	Fimo21_1	n	n	x	x	x	n	x	x	x	x	x	n	n	x	n	n	n	x	x	n
	Fimo21_2	x	x	x	x	n	x	n	x	x	x	n	n	n	n	n	x	x	n	n	n
	Fimo21_3	n	n	n	n	x	x	n	n	n	x	n	n	n	x	x	x	x	x	n	n
TP2	Fimo22_1	x	n	x	n	x	x	x	n	n	x	x	x	x	x	n	n	n	n	x	x
	Fimo22_2	n	n	n	x	n	x	n	n	x	x	x	x	n	n	n	n	n	x	n	n
	Fimo22_3	x	x	x	n	x	x	x	n	n	x	x	n	n	n	n	n	x	x	x	n
TP2	Fimo23_1	n	n	x	n	x	x	n	n	x	n	x	n	n	n	n	x	x	x	n	n
	Fimo23_2	n	x	n	x	x	n	x	x	n	n	n	n	x	x	x	x	x	n	n	n
	Fimo23_3	x	x	n	x	x	x	x	n	n	x	x	x	n	n	n	n	n	x	n	x
TP2	Fimo24_1	n	n	n	n	n	o	o	o	x	o	o	n	n	n	x	o	o	o	o	n
	Fimo24_2	n	n	n	o	o	o	x	n	n	o	n	o	o	o	n	n	x	x	o	o
	Fimo24_3	o	o	n	o	o	o	o	o	x	n	n	n	n	o	o	x	n	n	n	n

Tabelle 32: Testergebnisse - Fimo - Gelatine – koop. Opfer - Microsoft

TP	Attrappe	Testdurchlauf																			
		1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20
TP2	Fimo2_1	n	x	n	x	x	n	n	n	n	n	n	x	x	n	n	n	n	x	x	n
	Fimo2_2	n	n	n	x	n	x	x	x	x	n	n	n	x	x	n	x	n	n	n	n
TP2	Fimo3_1	x	x	n	x	n	n	n	x	x	n	n	n	n	x	x	n	n	n	n	n
	Fimo3_2	n	n	x	n	n	x	x	x	x	n	n	n	x	x	x	n	x	x	x	x
TP1	Fimo5_1	n	n	n	n	x	x	n	n	x	n	n	n	n	x	x	n	n	n	n	n
	Fimo5_2	x	x	x	n	n	n	n	x	x	n	n	x	n	n	n	x	n	n	n	n
	Fimo5_3	n	n	x	x	x	n	n	n	n	n	x	n	n	x	x	x	n	n	n	n
TP1	Fimo8_1	n	n	n	x	x	n	n	n	x	x	x	n	n	n	n	n	x	n	n	n
	Fimo8_2	n	x	n	n	n	n	x	x	x	x	n	n	x	x	x	n	n	n	n	n
	Fimo8_3	n	n	n	n	x	x	x	x	n	n	n	n	n	x	x	x	x	n	n	n
TP1	Fimo9_1	x	x	n	n	n	n	x	x	n	n	n	n	x	n	n	n	x	n	n	n
	Fimo9_2	x	x	x	n	n	n	n	x	x	x	x	x	n	x	n	n	n	n	n	n
TP2	Fimo10_1	n	n	x	n	x	x	x	x	n	n	x	x	x	x	x	n	n	n	n	n
	Fimo10_2	n	n	n	x	n	x	x	n	n	x	x	x	n	n	x	x	n	n	n	n
	Fimo10_3	x	x	n	x	x	n	n	n	n	n	x	x	x	x	n	n	x	n	n	n
TP2	Fimo11_1	n	n	n	x	x	x	x	n	n	n	n	n	x	n	n	n	n	n	n	n
	Fimo11_2	n	x	x	x	n	n	x	x	x	n	n	x	x	x	x	n	n	n	n	n
TP1	Fimo12_1	x	x	n	x	n	x	x	n	n	n	n	n	n	x	x	x	n	n	n	n
	Fimo12_2	n	n	n	n	n	x	n	n	x	x	x	x	x	x	x	x	x	x	n	n
TP1	Fimo13_1	n	n	n	x	x	n	x	x	n	x	x	x	x	n	n	x	n	n	n	n
	Fimo13_2	n	n	x	x	n	n	n	x	x	x	x	n	n	n	n	n	x	n	n	n
	Fimo13_3	n	n	x	n	x	x	n	n	n	x	x	x	n	n	x	x	x	n	n	n
TP2	Fimo14_1	n	n	n	x	n	n	x	x	n	n	n	n	x	x	x	n	n	n	n	n
	Fimo14_2	x	x	n	x	x	x	n	n	n	n	x	x	n	n	n	n	x	n	n	n
TP2	Fimo15_1	n	o	o	n	n	n	x	o	o	o	n	n	n	n	n	x	x	x	n	n
	Fimo15_2	n	n	n	x	x	x	x	n	n	x	x	n	n	n	n	x	x	n	n	n
	Fimo15_3	n	x	n	n	x	x	n	n	n	n	n	n	x	x	n	n	n	n	n	n
	Fimo15_4	n	n	n	x	x	n	n	n	n	n	x	x	x	n	n	x	n	n	x	x
TP1	Fimo16_1	n	n	n	x	x	x	n	x	x	x	x	n	n	n	x	x	x	n	n	n
	Fimo16_2	x	x	n	n	n	n	x	x	x	n	n	n	n	x	n	n	x	n	n	n
	Fimo16_3	n	n	x	x	x	x	n	x	x	n	n	n	x	n	x	x	n	n	n	n
TP1	Fimo17_1	n	n	n	n	n	x	x	n	n	x	x	x	n	n	n	x	n	n	n	n
	Fimo17_2	n	n	n	x	x	n	x	x	x	x	n	n	n	x	x	n	n	n	n	n
	Fimo17_3	n	n	x	x	n	x	n	n	x	x	x	x	n	n	n	n	n	n	n	n
TP1	Fimo18_1	x	x	x	n	x	x	n	n	n	n	x	x	n	n	x	x	x	x	n	n
	Fimo18_2	n	n	n	x	x	n	x	x	n	n	n	x	x	x	n	n	x	n	n	n
	Fimo18_3	n	x	n	x	n	n	x	x	n	x	x	x	x	n	x	x	n	n	n	n
TP1	Fimo19_1	n	n	x	n	n	x	x	x	n	n	n	x	x	x	n	x	x	n	n	n
	Fimo19_2	n	n	x	x	n	x	x	n	n	n	n	n	n	x	x	x	n	n	n	n
	Fimo19_3	n	n	n	o	n	n	o	o	o	o	n	n	n	o	n	n	n	n	n	n

TP	Attrappe	Testdurchlauf																			
		1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20
TP2	Fimo21_1	x	x	n	n	x	n	n	n	x	x	x	x	x	n	n	n	x	n	n	n
	Fimo21_2	n	x	n	x	x	x	n	n	n	n	n	x	x	n	n	n	n	n	n	n
	Fimo21_3	n	n	n	n	x	x	x	x	x	n	n	x	x	x	x	n	n	n	n	n
TP2	Fimo22_1	n	n	x	x	x	x	n	n	n	x	x	n	n	n	n	n	x	n	n	n
	Fimo22_2	n	n	x	x	n	n	n	x	x	x	n	n	n	x	x	x	n	n	n	n
	Fimo22_3	n	n	x	x	n	n	x	x	x	x	x	n	n	n	x	n	x	n	n	n
TP2	Fimo23_1	x	x	x	n	x	x	n	n	n	n	x	x	n	x	n	n	n	n	n	n
	Fimo23_2	n	n	n	n	x	n	x	x	x	x	n	n	n	x	x	n	n	n	n	n
	Fimo23_3	n	x	n	x	n	n	n	n	x	x	x	x	n	x	x	x	x	n	n	n
TP2	Fimo24_1	n	n	n	x	x	n	x	x	x	x	n	n	n	x	x	n	n	n	n	n
	Fimo24_2	n	n	n	x	x	n	x	x	x	x	x	n	n	x	x	x	x	x	n	n
	Fimo24_3	n	n	x	x	x	x	n	x	n	n	x	x	x	x	n	n	n	n	n	n
TP1	Fimo25_1[6]	n	n	n	n	x	x	n	x	x	x	x	n	n	n	n	x	x	n	n	n
	Fimo25_2	n	x	o	o	n	n	n	n	o	n	n	o	o	o	x	n	x	n	n	n
	Fimo25_3	n	n	n	n	n	x	n	x	n	n	n	n	x	x	x	x	n	n	n	n
	Fimo25_4	n	n	x	x	x	n	n	n	n	n	x	x	x	x	n	x	x	n	n	n
TP1	Fimo26_1[7]	n	n	x	x	x	x	x	x	x	x	x	n	n	n	n	x	x	n	n	n
	Fimo26_2	o	o	x	n	n	n	n	o	x	x	o	o	n	n	n	n	o	x	n	n
	Fimo26_3	x	n	x	x	x	n	n	n	n	n	x	x	n	n	x	x	x	n	n	n
TP2	Fimo27_1[8]	n	n	n	n	x	n	n	x	x	x	n	n	n	n	n	x	x	n	n	n
	Fimo27_2	n	n	n	o	o	o	x	n	n	n	n	o	o	x	x	n	n	n	n	n
	Fimo27_3	n	x	x	n	n	x	x	x	n	n	n	n	n	n	x	x	n	n	n	n
TP2	Fimo28_1[9]	n	n	n	n	n	n	x	x	x	n	n	n	x	n	x	x	n	n	n	n
	Fimo28_2	n	n	x	n	x	x	x	x	x	x	x	n	x	n	n	n	n	n	n	n
	Fimo28_3	x	x	n	x	x	x	n	n	n	n	x	n	n	n	n	x	n	n	n	n

[6] Ersatz für kaputte Vorlage Fimo1
[7] Ersatz für kaputte Vorlage Fimo4
[8] Ersatz für kaputte Vorlage Fimo6
[9] Ersatz für kaputte Vorlage Fimo7

Tabelle 33: Testergebnisse - Wachs - Holzleim – koop. Opfer - Microsoft

TP	Attrappe	Testdurchlauf																			
		1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20
TP1	W_1_1	n	n	n	x	x	n	x	x	x	x	x	n	n	n	x	x	n	n	n	n
TP2	W_2_1	o	n	x	o	o	o	o	n	n	n	o	o	o	n	n	n	n	x	o	o
	W_2_2	n	n	n	n	o	o	o	x	x	n	n	o	o	o	x	n	n	o	x	n
	W_2_3	x	x	x	n	n	x	n	n	x	x	x	x	n	n	x	n	x	x	x	n
TP2	W_3_1	n	n	n	n	x	x	n	x	x	n	n	n	x	x	x	n	n	x	n	n
	W_3_2	n	n	n	x	x	x	x	x	n	n	x	x	x	x	n	n	n	n	x	x
	W_3_3	n	x	x	x	n	n	x	x	x	n	n	n	n	x	x	x	n	x	n	n
TP1	W_4_1	n	n	x	x	x	n	x	x	n	n	n	x	x	x	n	n	n	n	x	n
	W_4_2	n	n	x	x	x	n	x	x	x	x	x	n	n	x	n	x	x	x	n	n
	W_4_3	n	x	x	x	n	n	n	x	x	n	x	x	n	n	n	x	x	n	n	n
TP1	W_5_1	n	n	n	n	x	x	n	x	x	x	x	n	n	n	n	x	n	n	n	n
	W_5_2	x	x	n	x	n	x	x	n	n	n	x	x	n	x	x	x	n	n	n	x
	W_5_3	n	n	x	n	n	n	x	n	n	x	x	x	x	x	n	n	n	n	x	x
TP2	W_6_1	n	n	o	o	o	o	x	n	n	o	x	o	n	n	n	o	o	o	x	n
	W_6_2	n	n	n	n	x	x	n	x	x	x	x	x	n	n	n	x	x	n	n	n
TP2	W_7_1	n	n	x	x	x	n	x	n	x	n	x	x	x	x	n	n	x	x	x	n
TP1	W_8_1	n	o	o	o	o	x	n	n	n	n	n	x	o	o	o	n	n	n	x	o
	W_8_2	o	o	x	n	n	n	o	o	o	x	n	n	n	o	o	o	n	x	o	o
	W_8_3	o	o	o	o	x	n	n	n	o	x	o	o	o	n	x	x	o	o	n	n
TP1	W_9_1	n	n	x	x	x	x	n	x	x	n	n	n	n	x	x	x	x	n	n	n
	W_9_2	x	x	n	x	n	x	n	x	x	x	x	x	x	x	n	x	n	n	n	n
	W_9_3	n	n	n	x	n	x	n	n	n	n	n	x	x	n	n	x	x	n	n	n
TP2	W_10_1	x	n	x	n	n	n	n	x	x	x	x	n	n	x	x	x	n	n	n	n
TP2	W_11_1	n	n	x	x	x	n	n	n	n	n	x	n	n	n	n	n	n	n	x	x
	W_11_2	n	n	x	n	x	x	x	n	n	n	n	n	x	x	x	n	n	n	n	x
	W_11_3	n	n	n	n	x	n	x	n	n	n	x	x	x	n	n	x	x	n	n	n
TP1	W_12_1	n	n	o	x	o	o	n	o	o	x	o	n	n	n	o	x	x	n	n	n
	W_12_2	o	o	o	n	n	n	n	n	x	o	o	x	o	n	n	o	o	o	x	x
	W_12_3	n	n	n	n	x	o	o	n	n	x	x	o	o	o	o	n	x	o	o	n

Tabelle 34: Testergebnisse - Wachs - Bastelkleber – koop. Opfer - Microsoft

TP	Attrappe	Testdurchlauf																			
		1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20
TP2	W_2_1	n	n	x	x	x	x	n	x	x	x	n	n	n	n	x	n	n	n	x	x
	W_2_2	n	n	x	x	n	x	x	x	n	n	n	n	x	n	n	x	x	n	x	n
	W_2_3	n	n	n	x	x	n	x	x	n	x	n	n	n	n	x	n	x	x	x	x
TP2	W_3_1	n	n	x	x	x	x	n	n	x	x	x	n	x	x	x	x	x	n	n	n
	W_3_2	n	n	x	x	n	x	x	x	x	n	n	n	x	x	n	n	n	n	x	x
	W_3_3	x	n	x	n	x	n	n	n	x	x	x	x	n	n	x	x	x	n	x	n
TP1	W_4_1	x	x	x	n	n	n	x	x	n	x	n	n	n	n	n	x	x	n	n	n
	W_4_2	n	n	x	n	n	x	n	x	x	x	n	n	n	x	x	n	x	n	x	x
	W_4_3	n	n	n	n	n	n	x	n	n	x	x	x	x	n	n	x	n	n	n	n
TP1	W_5_1	n	x	n	n	x	n	n	n	x	x	n	x	x	x	x	x	x	n	n	n
TP1	W_8_1	n	x	o	x	x	x	o	n	n	n	n	x	x	o	o	x	n	n	x	x
	W_8_2	n	n	o	o	n	x	o	o	x	n	n	n	o	o	o	x	n	n	n	n
	W_8_3	x	x	x	x	n	x	x	n	n	n	x	n	x	x	x	n	n	n	n	n
TP1	W_9_1	n	x	x	x	x	x	n	x	x	x	x	n	n	n	x	x	x	x	n	n
	W_9_2	n	n	x	n	x	x	x	x	n	n	x	n	n	x	x	x	x	n	n	n
	W_9_3	x	x	x	n	x	x	n	n	n	n	x	x	x	n	n	x	n	x	x	x
TP2	W_11_1	n	n	x	x	x	x	n	x	n	x	x	x	n	n	n	x	x	n	x	x
	W_11_2	n	n	n	x	x	n	x	x	x	x	n	x	x	n	n	n	n	n	x	n
	W_11_3	x	n	x	x	n	n	n	n	x	x	x	x	n	n	x	n	x	x	n	n
TP1	W_12_1	n	o	o	n	n	x	o	x	n	n	n	x	o	o	n	n	n	n	x	x
	W_12_2	n	n	n	x	x	o	o	o	n	n	o	x	n	n	n	n	n	o	x	o
	W_12_3	n	n	n	n	x	x	o	o	o	o	n	n	n	n	n	x	o	n	n	n
TP1 [10]	W_13_1	n	n	n	n	x	x	n	n	n	x	x	x	x	x	n	n	x	x	x	n
	W_13_2	n	n	o	x	n	n	n	n	n	o	o	o	o	x	n	n	n	n	x	x
	W_13_3	n	o	o	n	n	n	n	o	o	x	n	n	n	n	o	o	n	n	x	x
TP2 [11]	W_14_1	n	x	x	n	x	n	x	x	x	x	x	n	n	n	x	n	x	n	n	n
TP2 [12]	W_15_1	n	n	o	o	o	n	x	x	o	o	n	o	o	o	x	n	n	n	n	n
	W_15_2	n	n	n	o	o	x	o	o	n	n	n	n	n	o	o	o	x	x	n	n
	W_15_3	o	x	x	n	n	o	o	o	n	n	x	n	n	n	n	o	o	x	n	n
TP2 [13]	W_16_1	n	x	o	o	o	o	n	x	n	n	o	o	x	n	n	x	o	n	n	n
	W_16_2	n	o	o	x	o	n	n	n	o	x	x	n	o	o	o	o	n	n	n	n
	W_16_3	x	x	n	x	n	n	n	n	n	x	x	n	x	x	x	x	n	x	n	n

[10] Als Ersatz für kaputte Vorlage Wachs1
[11] Als Ersatz für kaputte Vorlage Wachs6
[12] Als Ersatz für kaputte Vorlage Wachs7
[13] Als Ersatz für kaputte Vorlage Wachs8

Tabelle 35: Testergebnisse - Wachs - Silikon – koop. Opfer - Microsoft

TP	Attrappe	Testdurchlauf																			
		1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20
TP2	W_2_1	n	n	x	x	x	x	n	n	n	x	n	n	n	n	n	x	n	n	n	n
TP2	W_3_1	n	n	n	x	x	n	n	n	x	n	x	n	x	x	x	n	n	x	n	n
	W_3_2	n	n	x	x	x	n	n	x	x	n	n	n	n	n	x	x	x	x	n	n
	W_3_3	x	x	n	n	n	x	x	x	n	x	x	x	n	n	n	n	n	n	n	x
TP1	W_4_1	n	n	n	n	x	x	n	x	x	x	x	n	n	n	x	x	n	n	n	n
TP1	W_8_1	n	n	o	o	x	x	n	x	o	x	n	n	n	n	o	x	x	n	n	n
	W_8_2	n	n	n	n	x	o	o	n	x	o	n	n	n	n	n	o	x	n	n	n
	W_8_3	n	n	x	n	n	n	n	o	x	n	n	o	o	n	n	n	n	o	x	x
TP1	W_9_1	n	n	n	x	x	x	x	x	x	n	n	n	x	x	n	n	n	x	n	n
TP2	W_11_1	n	x	x	x	n	n	n	n	n	x	x	n	x	n	x	n	x	n	n	n
	W_11_2	x	x	x	x	x	n	n	x	x	n	n	n	n	n	x	n	x	n	n	n
TP1	W_12_1	n	x	x	x	x	n	n	n	n	x	x	x	x	x	n	n	n	x	n	n
	W_12_2	n	n	n	n	n	n	o	o	x	o	n	n	n	x	o	o	n	n	n	n
	W_12_3	n	x	x	n	n	n	n	n	x	x	x	x	x	n	n	n	x	x	n	n
TP1	W_13_1	n	o	o	x	x	n	n	n	n	n	n	o	o	x	x	n	n	n	n	n
	W_13_2	n	n	n	n	n	x	x	x	o	o	n	n	n	n	n	n	o	o	x	n
	W_13_3	n	n	x	x	x	x	n	n	n	n	x	x	x	x	x	x	x	n	n	n
TP2	W_15_1	n	n	o	n	n	x	o	o	n	n	n	x	x	n	o	o	o	x	n	n
	W_15_2	o	o	o	x	n	n	n	x	o	o	n	n	n	o	o	x	n	n	n	n
	W_15_3	x	x	n	n	n	n	x	x	n	x	n	n	n	x	x	n	n	n	n	n
TP2	W_16_1	n	n	n	x	x	x	x	x	n	x	x	x	x	x	x	n	n	x	n	x
	W_16_2	x	o	o	n	n	n	n	n	n	n	n	o	o	o	x	x	n	n	n	n
	W_16_3	n	n	x	x	n	n	x	x	x	x	x	n	n	n	x	n	n	n	n	n
TP1 [14]	W_17_1	n	n	n	n	n	x	x	x	x	n	n	x	x	x	x	x	n	n	n	n
	W_17_2	x	x	n	n	n	x	x	x	x	x	x	n	n	n	x	n	x	n	n	n
	W_17_3	n	n	n	n	n	x	n	x	n	x	n	n	x	x	x	n	n	x	x	x
TP2 [15]	W_18_1	n	x	n	x	n	n	n	x	x	n	x	x	x	n	x	n	x	x	n	n
	W_18_2	n	n	n	x	x	x	n	x	n	x	x	n	n	n	x	x	n	n	n	n
	W_18_3	n	x	n	n	x	n	n	n	n	n	x	x	x	n	n	n	n	n	n	n

[14] Als Ersatz für kaputte Vorlage Wachs5
[15] Als Ersatz für kaputte Vorlage Wachs14

Tabelle 36: Testergebnisse - Wachs - Gelatine – koop. Opfer - Microsoft

TP	Attrappe	Testdurchlauf																			
		1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20
TP2	W_3_1	n	n	n	n	n	x	x	n	x	x	x	n	x	n	x	x	x	n	n	n
	W_3_2	n	x	x	x	x	n	x	x	x	x	x	n	n	x	x	x	n	n	n	n
	W_3_3	n	n	x	x	x	x	n	x	x	n	n	n	n	n	x	x	x	x	n	n
TP1	W_8_1	n	n	x	x	x	x	n	n	x	n	x	x	x	n	n	n	n	x	n	n
	W_8_2	n	n	x	x	n	x	n	n	n	x	n	x	n	n	n	x	x	x	n	n
	W_8_3	x	x	n	x	n	n	x	x	x	x	x	n	n	x	x	x	x	n	n	n
TP1	W_12_1	n	n	x	n	x	x	x	n	x	x	x	x	n	x	n	n	n	n	x	x
	W_12_2	n	n	x	x	n	n	n	n	x	x	n	x	n	x	x	x	n	n	n	n
	W_12_3	x	n	x	x	x	x	n	n	n	x	n	x	n	n	n	x	x	x	x	n
TP1	W_13_1	n	x	x	x	n	n	x	x	x	x	x	n	x	x	x	n	n	n	n	n
	W_13_2	n	n	n	o	o	x	n	n	n	o	o	o	o	x	x	n	n	n	n	n
	W_13_3	n	n	n	n	x	x	o	o	o	o	x	o	n	n	n	n	o	n	n	n
TP2	W_15_1	n	n	n	n	x	x	x	n	x	n	x	x	x	n	x	n	n	n	n	n
	W_15_2	n	n	x	x	x	x	n	x	n	x	x	x	x	n	n	n	x	n	x	x
	W_15_3	n	n	x	n	n	n	x	x	x	x	x	n	n	n	x	n	n	n	n	n
TP2	W_16_1	n	x	x	x	x	n	x	n	n	n	x	x	x	x	x	n	n	n	n	n
	W_16_2	n	n	n	x	n	x	x	x	n	x	n	x	x	x	n	x	n	n	n	n
	W_16_3	n	n	x	n	x	x	x	x	x	n	x	n	n	x	n	x	x	n	n	n
TP1	W_17_1	n	n	n	n	n	n	x	x	n	x	x	x	x	x	n	n	n	n	n	n
	W_17_2	x	x	x	n	x	x	n	n	x	n	x	x	x	x	x	n	n	n	n	n
	W_17_3	n	n	x	n	x	n	x	x	x	x	n	x	n	n	n	n	x	n	n	n
TP2	W_18_1	n	n	x	x	x	x	x	x	x	n	n	n	n	x	x	n	n	x	x	n
	W_18_2	n	n	n	x	x	n	n	x	n	n	n	x	x	x	x	n	x	x	n	n
	W_18_3	n	x	x	x	n	n	n	n	x	x	x	x	x	n	x	x	x	x	n	n
TP2 [16]	W_19_1	x	x	n	x	x	x	x	n	n	n	x	x	n	n	n	n	n	x	n	n
	W_19_2	x	n	n	n	x	x	x	x	n	n	n	n	x	x	n	n	n	n	n	n
	W_19_3	n	n	n	x	n	x	x	x	x	x	n	x	n	x	x	n	n	n	n	n
TP1 [17]	W_20_1	n	n	o	x	x	n	n	n	n	o	o	o	o	x	o	o	x	n	n	n
	W_20_2	n	n	x	x	n	x	x	x	x	n	x	x	n	n	n	n	n	x	x	n
	W_20_3	n	x	x	x	x	n	n	x	x	n	n	n	n	n	x	x	n	n	n	n
TP1 [18]	W_21_1	n	n	x	x	x	n	x	n	x	x	x	x	x	n	n	x	n	n	n	n
	W_21_2	n	n	x	n	x	n	x	x	x	x	n	n	x	n	n	n	n	n	n	n
	W_21_3	x	x	x	x	x	n	x	x	n	n	n	n	n	x	x	n	n	n	n	n
TP2 [19]	W_22_1	n	n	n	n	x	n	x	x	x	x	x	n	x	x	n	n	n	n	n	n
	W_22_2	n	n	x	x	x	x	n	x	x	n	n	n	n	x	x	x	x	n	x	n
	W_22_3	x	x	n	x	n	n	n	n	n	x	n	x	x	x	x	n	n	n	n	n

[16] Als Ersatz für kaputte Vorlage Wachs2
[17] Als Ersatz für kaputte Vorlage Wachs4
[18] Als Ersatz für kaputte Vorlage Wachs9
[19] Als Ersatz für kaputte Vorlage Wachs11

Tabelle 37: Testergebnisse – Platine - Holzleim – unw. Opfer - Microsoft

TP	Attrappe	Testdurchlauf																			
		1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20
TP1	Pl_1_1_1	n	n	n	n	x	x	x	n	n	n	n	n	x	n	n	n	n	n	x	n
	Pl_1_1_2	x	n	n	n	n	x	n	n	n	n	n	n	n	x	x	n	n	n	n	x
	Pl_1_1_3	x	x	n	n	n	n	n	n	n	x	n	n	n	n	n	n	x	n	n	n
TP1	Pl_1_2_1	n	n	n	n	n	n	x	x	x	n	n	n	n	n	n	x	n	n	x	n
	Pl_1_2_2	n	n	x	n	n	n	n	x	n	n	n	x	n	n	n	n	n	n	x	n
	Pl_1_2_3	x	x	n	n	n	x	n	x	n	n	n	n	x	x	n	n	n	x	n	x
TP1	Pl_1_3_1	x	x	n	n	n	n	n	n	n	n	n	n	n	x	n	n	n	x	n	n
	Pl_1_3_2	n	n	n	x	n	n	n	x	n	n	n	x	n	n	n	x	n	n	x	n
	Pl_1_3_3	x	x	x	n	x	n	n	n	n	n	x	n	x	n	n	n	n	n	x	n
TP1	Pl_1_4_1	n	n	n	x	x	n	n	n	n	x	n	x	n	n	n	n	n	x	n	n
	Pl_1_4_2	x	x	x	n	n	n	n	x	n	n	n	n	n	n	n	x	x	n	n	x
	Pl_1_4_3	n	n	n	n	n	n	n	n	x	x	n	n	n	n	n	n	n	n	n	n
TP1	Pl_1_5_1	n	n	n	n	n	n	n	n	n	x	n	n	n	n	n	x	n	n	n	n
	Pl_1_5_2	x	n	n	n	n	n	n	n	x	n	n	x	n	n	x	n	n	n	x	n
	Pl_1_5_3	n	n	x	n	n	n	x	n	n	x	n	n	x	n	n	n	x	n	n	x
TP1	Pl_1_6_1	n	x	x	n	n	n	n	x	n	n	n	n	x	x	x	n	n	n	n	n
	Pl_1_6_2	n	n	n	n	n	n	n	x	x	n	n	n	x	n	n	n	x	x	n	x
	Pl_1_6_3	x	n	x	n	n	x	x	n	n	n	n	n	x	x	n	n	n	x	x	n
TP1	Pl_2_1_1	n	x	n	x	n	n	n	n	n	x	n	n	n	n	n	n	n	x	n	n
	Pl_2_1_2	n	x	n	n	x	x	n	n	n	n	n	n	x	n	n	n	n	n	n	n
	Pl_2_1_3	n	n	x	n	n	x	n	n	x	x	n	n	x	n	n	n	n	n	n	n
TP1	Pl_2_2_1	n	x	n	n	n	n	n	x	x	n	n	n	n	n	x	n	n	n	n	n
	Pl_2_2_2	n	n	n	x	n	n	n	n	n	n	n	n	x	x	x	n	n	n	n	n
	Pl_2_2_3	n	x	n	n	n	n	n	x	x	n	n	n	n	n	n	n	n	x	x	x
TP1	Pl_2_3_1	n	x	n	n	n	x	n	x	n	n	n	x	n	n	x	n	n	n	n	x
	Pl_2_3_2	x	n	x	n	n	n	x	n	x	n	x	n	n	n	x	n	n	n	n	x
	Pl_2_3_3	n	x	n	n	n	n	n	n	n	n	x	n	n	x	n	n	n	x	n	n
TP1	Pl_2_4_1	n	n	n	n	n	n	n	x	x	x	n	n	n	n	n	n	n	n	x	x
	Pl_2_4_2	x	x	n	n	n	n	n	n	n	n	n	n	x	n	n	n	x	n	n	n
	Pl_2_4_3	n	n	x	n	n	n	x	x	n	n	n	n	n	x	x	n	n	x	n	x
TP1	Pl_2_5_1	n	n	x	n	n	x	n	n	n	x	x	n	n	n	n	n	n	n	n	n
	Pl_2_5_2	n	x	n	n	n	n	n	n	n	n	n	x	x	n	n	n	n	x	n	x
	Pl_2_5_3	n	n	x	n	n	x	x	x	n	n	x	n	n	n	n	n	x	n	n	n
TP1	Pl_2_6_1	n	n	n	n	n	n	n	n	x	x	n	x	n	n	n	n	x	n	n	n
	Pl_2_6_2	n	n	x	n	n	n	x	x	n	n	n	x	n	n	n	n	n	n	x	x
	Pl_2_6_3	x	n	n	x	x	n	x	n	n	n	n	n	n	n	x	n	n	n	x	n
TP2	Pl_3_1_1	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n	x	n	n	n	n
	Pl_3_1_2	n	n	n	n	x	n	n	n	n	x	n	n	n	n	n	n	n	n	n	x
	Pl_3_1_3	n	n	n	n	n	x	n	n	n	n	n	n	n	n	n	n	n	n	n	n
TP2	Pl_3_2_1	n	n	n	n	x	x	n	n	x	n	n	n	n	n	n	n	x	x	n	n
	Pl_3_2_2	n	x	n	x	x	n	n	n	x	n	n	n	n	n	n	n	n	x	n	n
TP2	Pl_3_3_1	n	n	n	n	x	x	n	n	n	n	x	n	n	n	n	x	x	n	x	n
	Pl_3_3_2	x	n	n	x	n	n	n	n	n	n	n	n	x	n	n	n	n	n	x	n
	Pl_3_3_3	x	x	n	n	n	n	n	x	n	n	x	n	x	x	n	n	n	n	n	n

TP	Attrappe	Testdurchlauf																			
		1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20
TP2	PI_4_1_1	n	x	n	n	n	x	n	n	x	n	n	n	x	n	n	n	n	x	x	x
	PI_4_1_2	n	n	x	x	n	n	n	x	n	n	n	x	x	n	n	n	n	n	n	n
	PI_4_1_3	x	x	n	n	n	n	x	x	n	n	n	n	n	n	n	n	n	n	x	n
TP2	PI_4_2_1	n	x	n	n	n	x	n	x	n	x	n	x	x	n	n	n	n	n	n	n
	PI_4_2_2	n	n	n	n	n	x	x	x	n	n	n	n	x	n	n	n	n	n	n	n
	PI_4_2_3	x	n	x	n	n	n	n	x	x	n	n	x	n	n	n	n	n	n	n	n
TP2	PI_4_3_1	n	n	n	n	n	x	x	x	x	n	n	n	n	x	n	n	n	n	n	x
	PI_4_3_2	x	x	x	n	n	n	n	x	n	n	n	x	n	n	n	n	n	x	n	n
	PI_4_3_3	n	n	x	n	n	n	n	x	n	n	n	n	x	x	x	x	n	n	n	n
TP2	PI_4_4_1	x	n	n	x	x	x	n	n	n	n	n	n	x	n	n	n	n	x	n	n
	PI_4_4_2	x	x	n	n	x	n	n	n	n	x	n	n	n	n	x	x	n	n	n	x
	PI_4_4_3	n	n	x	n	n	n	n	n	n	x	n	x	n	n	n	x	n	n	n	x
TP2	PI_4_5_1	n	n	n	x	x	n	n	n	n	x	n	n	n	n	x	n	n	n	n	n
	PI_4_5_2	x	x	n	n	n	x	n	n	n	x	n	n	x	x	x	n	n	n	n	n
	PI_4_5_3	x	x	x	n	n	n	n	n	n	n	n	x	n	n	n	n	n	x	n	n
TP2	PI_4_6_1	n	n	x	n	n	n	n	n	n	x	x	x	n	n	n	n	n	n	n	n
	PI_4_6_2	n	n	n	n	x	x	n	n	n	x	n	n	n	n	n	n	x	n	n	x
	PI_4_6_3	x	x	n	x	n	n	n	n	n	x	n	n	n	n	n	n	x	n	n	n
TP2	PI_4_7_1	n	n	x	n	n	n	x	n	n	x	x	n	n	n	n	x	n	n	n	n
	PI_4_7_2	x	n	n	n	n	x	n	n	n	n	n	n	n	x	x	x	n	n	n	n
	PI_4_7_3	n	x	n	n	n	n	n	n	n	n	n	n	n	n	x	x	n	n	n	n
TP2	PI_4_8_1	n	x	n	n	n	x	n	x	x	n	n	n	n	x	n	n	x	n	x	n
	PI_4_8_2	n	n	x	x	n	x	n	n	n	x	n	n	n	n	n	n	n	x	n	n
	PI_4_8_3	x	n	n	n	n	n	n	n	n	n	n	n	x	n	n	n	n	n	n	n
TP2	PI_4_9_1	x	n	n	x	n	n	n	n	x	n	n	x	n	n	x	x	n	n	n	n
	PI_4_9_2	n	n	n	n	n	n	x	n	n	n	n	x	n	n	n	x	x	n	n	n
	PI_4_9_3	n	x	x	n	n	n	n	n	n	x	x	x	n	n	n	n	n	n	n	n
TP2	PI_4_10_1	n	n	n	x	n	n	n	n	n	n	n	x	n	n	x	n	n	n	n	n
	PI_4_10_2	x	x	x	n	n	n	n	x	n	n	n	n	x	n	n	n	n	n	n	n
	PI_4_10_3	n	n	x	x	n	n	n	n	n	x	n	n	n	n	x	x	n	n	n	n
TP2	PI_5_1_1	n	x	n	n	n	x	n	n	n	n	n	n	x	n	n	x	n	n	x	n
	PI_5_1_2	n	n	n	x	n	x	x	n	n	n	n	n	x	n	n	x	x	n	n	n
	PI_5_1_3	n	n	x	n	n	n	x	x	n	n	n	n	n	n	x	n	n	n	n	n
TP2	PI_5_2_1	n	x	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n
	PI_5_2_2	x	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n	x
TP2	PI_5_3_1	n	n	x	n	x	n	n	n	n	n	x	n	n	n	x	n	n	n	n	n
	PI_5_3_2	x	n	n	n	n	n	n	n	n	n	x	n	n	x	n	x	n	x	n	n
	PI_5_3_3	x	x	x	x	n	n	n	n	n	x	n	n	n	n	n	n	n	x	n	n
TP2	PI_5_4_1	x	n	n	n	n	n	n	n	n	n	n	n	n	n	n	x	n	n	n	n
	PI_5_4_2	n	n	n	x	n	x	x	x	n	n	n	n	n	x	n	n	n	x	n	n
	PI_5_4_3	n	n	n	x	n	n	n	n	n	n	n	n	n	n	n	x	x	n	n	n

TP	Attrappe	Testdurchlauf																			
		1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20
TP2	Pl_5_5_1	n	n	n	x	n	n	n	n	x	n	x	n	n	x	n	n	x	x	n	n
	Pl_5_5_2	n	n	n	n	x	x	x	x	x	n	n	n	n	n	n	n	n	n	n	n
	Pl_5_5_3	n	x	x	n	n	n	n	n	x	n	n	n	n	x	n	n	n	x	n	n
TP2	Pl_5_6_1	n	n	n	n	n	x	x	n	n	n	n	n	x	n	n	n	x	n	n	n
	Pl_5_6_2	n	n	n	x	x	n	n	n	n	n	x	n	n	x	x	n	n	n	x	n
	Pl_5_6_3	n	n	n	x	n	n	n	x	n	n	n	n	n	x	x	x	n	n	n	n
TP2	Pl_5_7_1	n	n	n	n	n	x	x	n	n	n	n	x	n	n	n	n	n	x	n	n
	Pl_5_7_2	n	n	n	n	n	x	x	n	n	x	n	n	x	x	x	n	n	n	n	n
	Pl_5_7_3	n	x	n	n	n	n	n	n	n	x	x	n	n	n	n	x	n	n	n	x
TP2	Pl_5_8_1	n	n	x	n	n	n	x	n	n	x	n	n	n	n	n	x	n	n	n	x
	Pl_5_8_2	n	n	n	x	n	x	x	x	n	n	n	n	n	x	n	n	x	n	n	n
	Pl_5_8_3	n	n	n	n	n	x	n	n	n	n	n	x	n	n	n	x	n	n	n	n
TP1	Pl_6_1_1	n	n	n	n	n	x	n	n	x	x	n	n	n	x	n	n	n	x	n	n
	Pl_6_1_2	n	n	n	n	x	x	x	n	n	n	n	x	n	n	n	n	n	n	n	n
	Pl_6_1_3	x	n	n	n	x	n	n	n	n	n	n	n	n	n	x	n	n	x	n	n
TP1	Pl_6_2_1	n	n	n	n	n	n	n	n	n	n	n	x	x	n	n	n	n	x	n	n
	Pl_6_2_2	n	n	n	n	x	n	n	x	n	n	n	n	n	n	n	x	x	n	n	n
	Pl_6_2_3	n	n	n	n	x	n	n	n	n	n	x	x	n	n	n	n	n	x	n	n
TP1	Pl_6_3_1	n	n	n	x	n	n	n	n	n	n	n	x	n	x	x	n	n	n	x	x
	Pl_6_3_2	n	n	n	n	n	n	x	x	n	n	n	x	n	n	n	x	x	n	x	n
	Pl_6_3_3	x	n	n	n	n	n	x	x	n	n	n	n	n	n	n	n	n	x	n	n
TP1	Pl_6_4_1	n	x	n	x	x	x	n	n	n	n	n	x	x	n	n	x	n	n	n	n
	Pl_6_4_2	n	n	n	n	n	n	n	x	n	n	x	n	n	n	x	n	n	n	n	n
	Pl_6_4_3	x	n	n	n	x	n	n	n	n	x	n	n	n	n	n	n	n	x	n	n
TP1	Pl_6_5_1	x	n	n	n	n	n	n	n	x	x	n	n	n	n	n	n	n	x	x	x
	Pl_6_5_2	x	n	n	n	n	x	n	x	n	n	x	n	n	n	n	n	x	x	n	n
	Pl_6_5_3	n	n	n	n	x	x	x	x	n	n	n	n	n	n	n	x	n	n	n	n
TP1	Pl_6_7_1	n	n	x	n	n	n	n	n	n	n	x	x	x	n	n	n	n	n	n	n
	Pl_6_7_2	x	n	n	n	x	n	x	n	n	n	n	n	x	n	n	n	x	x	x	n
	Pl_6_7_3	n	x	x	n	n	n	x	n	n	n	n	x	n	n	n	x	x	n	n	n
TP1	Pl_6_8_1	n	n	n	x	n	n	n	x	n	n	n	n	n	n	n	n	x	n	n	n
	Pl_6_8_2	n	n	n	n	n	n	n	n	n	n	x	x	n	x	n	x	n	x	x	n
TP1	Pl_6_10_1	n	x	n	n	n	n	n	x	n	n	n	n	n	n	x	x	n	n	n	n
	Pl_6_10_2	n	x	x	n	x	x	x	n	n	n	n	x	n	n	x	n	n	n	x	n
TP1	Pl_6_11_1	x	n	n	n	x	x	n	n	n	n	x	n	n	n	x	n	n	x	n	n
	Pl_6_11_2	n	x	n	x	x	x	n	n	n	n	x	x	n	n	x	n	n	x	n	n

Tabelle 38: Testergebnisse - Platine – Bastelkleber – unw. Opfer - Microsoft

TP	Attrappe	Testdurchlauf																			
		1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20
TP1	Pl_1_1_1	n	n	x	n	n	x	x	n	n	n	x	x	n	n	n	n	n	x	n	n
	Pl_1_1_2	x	n	n	x	x	x	n	x	n	n	n	x	n	n	n	n	n	x	n	n
	Pl_1_1_3	n	n	x	x	n	n	n	n	x	n	n	x	n	n	n	n	n	n	x	x
TP1	Pl_1_2_1	n	n	x	x	n	x	n	n	n	x	n	n	n	n	n	n	x	n	n	x
	Pl_1_2_2	x	x	n	n	n	x	n	n	x	x	x	n	x	n	n	n	n	n	n	n
	Pl_1_2_3	n	n	x	n	x	x	n	n	n	n	x	x	n	n	n	n	n	n	x	n
TP1	Pl_1_3_1	n	n	n	n	x	n	n	x	n	n	n	x	x	x	n	n	n	n	n	n
	Pl_1_3_2	x	n	n	n	n	n	n	n	x	n	n	n	n	x	x	n	n	x	x	n
	Pl_1_3_3	x	x	n	x	n	n	n	n	x	n	n	n	n	n	n	n	x	n	n	x
TP1	Pl_1_4_1	x	x	n	n	n	n	x	n	n	x	n	n	x	n	n	n	n	n	x	n
	Pl_1_4_2	n	x	n	n	n	n	n	n	n	n	x	x	x	n	n	n	x	n	n	n
	Pl_1_4_3	n	n	x	x	x	n	n	n	n	x	n	n	n	n	n	n	n	x	n	n
TP1	Pl_1_5_1	x	n	n	n	n	n	x	n	n	n	n	x	x	n	n	n	n	x	n	n
	Pl_1_5_2	n	x	x	x	n	n	n	n	n	x	x	n	n	x	x	n	n	n	x	n
	Pl_1_5_3	n	x	x	x	n	n	n	n	n	n	x	x	n	n	n	n	n	n	n	n
TP1	Pl_1_6_1	x	x	x	n	n	n	n	n	n	n	x	n	n	n	x	n	n	n	n	n
	Pl_1_6_2	n	n	n	n	x	n	n	n	x	n	n	n	n	n	x	n	n	n	n	n
	Pl_1_6_3	x	x	n	n	n	n	x	x	x	n	n	n	n	n	n	n	n	x	n	n
TP1	Pl_2_1_1	n	n	x	x	n	n	n	n	n	x	x	n	n	n	n	n	n	n	n	n
	Pl_2_1_2	n	x	n	n	n	n	x	n	n	n	n	n	x	x	n	n	x	n	n	n
	Pl_2_1_3	x	x	n	x	n	n	n	n	n	n	n	n	n	n	n	n	x	n	x	n
TP1	Pl_2_2_1	n	x	n	x	x	n	n	n	x	x	n	n	n	x	x	x	n	n	n	n
	Pl_2_2_2	n	n	n	n	n	n	x	x	o	o	x	n	n	n	x	n	n	n	x	n
	Pl_2_2_3	x	x	n	n	n	n	n	n	n	n	n	n	x	x	x	n	n	n	n	n
	Pl_2_2_4	n	n	x	x	x	n	n	n	n	n	x	n	n	n	x	n	n	n	n	n
	Pl_2_2_5	x	x	n	n	n	x	n	x	n	n	n	n	n	n	n	x	n	n	n	x
	Pl_2_2_6	n	n	n	x	n	x	n	n	n	n	n	n	x	x	n	n	n	x	x	n
	Pl_2_2_7	n	n	n	n	n	n	n	n	x	n	n	x	x	n	n	n	n	n	x	n
	Pl_2_2_8	x	x	n	n	n	x	x	x	n	n	n	n	n	x	n	n	n	x	n	n
	Pl_2_2_9	x	x	n	x	n	n	n	n	n	x	n	n	n	n	n	x	n	n	n	n
	Pl_2_2_10	n	n	n	x	x	x	n	n	n	n	n	x	n	x	x	n	n	x	n	x
	Pl_2_2_11	n	x	n	n	x	n	n	n	n	n	n	n	x	n	n	n	x	x	n	n
	Pl_2_2_12	n	n	x	n	n	n	x	x	n	n	x	n	n	n	x	n	n	x	n	n
	Pl_2_2_13	n	n	n	n	n	n	x	n	n	n	n	x	n	x	x	n	n	n	x	n
	Pl_2_2_14	x	x	n	n	n	n	n	n	n	n	x	n	n	x	n	n	x	x	n	x
	Pl_2_2_15	n	n	n	x	n	n	n	n	n	n	n	x	n	n	x	x	n	n	n	x
	Pl_2_2_16	n	x	n	n	n	n	n	n	n	x	n	n	n	n	n	n	x	x	n	n
	Pl_2_2_17	n	n	n	n	x	x	n	n	n	n	n	n	x	x	x	n	n	n	x	n
	Pl_2_2_18	n	n	x	n	n	n	n	x	x	n	n	x	x	n	n	x	n	x	n	n
	Pl_2_2_19	n	n	n	x	x	n	n	n	n	n	n	x	n	x	x	n	n	x	n	x
	Pl_2_2_20	n	x	x	n	n	n	n	x	n	n	n	x	x	n	n	n	n	n	x	n
TP1	Pl_2_3_1	x	n	n	n	n	n	n	n	n	n	n	n	x	x	x	n	n	n	n	x
	Pl_2_3_2	n	n	n	n	n	n	n	n	n	x	x	n	n	x	n	n	n	n	n	x
	Pl_2_3_3	x	n	n	n	n	x	n	n	x	n	n	n	n	x	x	n	n	n	n	n

TP	Attrappe	Testdurchlauf																			
		1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20
TP1	PI_2_4_1	n	x	x	n	n	n	x	n	n	n	x	n	x	n	n	n	n	x	x	n
	PI_2_4_2	x	n	n	x	n	n	n	n	n	n	x	n	n	n	n	n	n	n	x	n
	PI_2_4_3	n	n	x	n	n	n	n	n	x	x	n	n	n	n	n	x	n	x	n	n
TP1	PI_2_5_1	x	n	n	n	n	x	n	n	n	n	n	x	x	n	n	n	n	x	n	n
	PI_2_5_2	x	n	x	n	n	n	n	x	x	n	n	n	n	n	x	n	n	n	n	n
	PI_2_5_3	n	n	n	x	n	n	n	n	n	n	n	x	x	x	n	n	n	n	n	x
TP1	PI_2_6_1	x	x	x	x	n	n	n	n	n	x	x	n	n	n	n	n	n	x	n	x
	PI_2_6_2	x	n	n	n	x	n	n	n	n	n	n	n	n	n	n	x	x	n	x	x
	PI_2_6_3	x	n	n	x	x	n	n	n	n	n	x	n	n	n	x	n	x	n	n	n
TP2	PI_3_1_1	x	n	n	n	x	x	x	x	n	x	n	n	x	x	n	x	x	x	n	n
	PI_3_1_2	x	n	n	n	n	n	x	n	x	x	x	n	x	n	n	n	x	x	n	x
TP2	PI_3_3_1	n	x	x	x	n	n	n	x	n	n	n	n	x	x	x	n	x	n	n	x
	PI_3_3_2	x	x	x	x	n	n	n	n	n	n	x	n	x	n	n	n	x	n	n	x
TP2	PI_4_1_1	x	x	x	n	n	n	n	n	n	x	n	n	n	n	n	x	n	n	n	x
	PI_4_1_2	x	x	n	n	n	n	n	x	n	n	x	x	x	n	n	n	n	n	x	n
	PI_4_1_3	n	x	n	n	n	n	n	n	n	n	x	x	x	n	n	x	n	n	n	x
TP2	PI_4_2_1	n	x	n	n	n	x	x	n	n	x	n	n	n	x	n	n	x	n	n	x
	PI_4_2_2	x	n	n	x	n	n	n	n	x	x	n	x	n	n	x	n	n	n	x	n
	PI_4_2_3	n	n	n	n	n	n	n	x	x	n	n	n	x	x	x	n	n	n	x	n
TP2	PI_4_3_1	n	n	n	n	n	n	x	n	n	n	n	n	n	n	x	x	n	x	x	n
	PI_4_3_2	x	n	n	n	n	x	n	n	n	n	n	x	n	x	n	n	n	n	n	n
	PI_4_3_3	n	x	x	n	n	x	x	n	n	n	n	x	n	n	n	n	n	x	n	n
TP2	PI_4_4_1	n	n	n	n	n	x	n	n	x	n	n	n	x	n	n	x	x	x	n	n
	PI_4_4_2	n	n	x	n	n	n	n	x	x	x	n	n	n	n	n	x	n	n	n	n
	PI_4_4_3	n	n	n	n	n	n	n	n	n	x	n	n	x	n	n	n	n	n	x	n
TP2	PI_4_5_1	n	n	n	x	n	n	n	n	n	n	n	x	x	x	x	n	n	n	n	n
	PI_4_5_2	x	n	n	n	x	x	x	n	n	x	n	n	n	n	x	n	n	n	n	x
	PI_4_5_3	n	n	n	x	n	n	x	x	x	n	n	n	n	n	x	n	n	n	n	n
TP2	PI_4_6_1	n	n	n	n	x	x	x	x	n	n	n	x	n	n	n	n	x	n	n	n
	PI_4_6_2	n	n	x	n	n	n	n	x	x	n	n	n	x	n	n	n	n	n	x	n
	PI_4_6_3	x	n	n	x	n	n	n	x	x	n	n	n	n	n	n	n	n	n	x	n
TP2	PI_4_7_1	x	n	n	n	x	x	x	n	n	n	n	n	n	x	x	x	n	n	x	n
	PI_4_7_2	n	n	n	n	n	n	x	x	n	n	n	n	x	n	n	n	n	n	x	n
	PI_4_7_3	x	n	n	n	n	n	x	n	n	n	n	n	x	n	n	n	x	n	n	n
TP2	PI_4_8_1	n	n	n	n	n	n	n	n	n	n	n	n	n	x	n	n	n	n	x	n
	PI_4_8_2	n	n	x	x	n	n	x	n	n	n	n	x	n	n	n	n	n	x	n	n
	PI_4_8_3	x	n	n	n	n	n	n	n	n	n	x	x	n	n	n	n	n	x	n	n
TP2	PI_4_9_1	n	n	x	n	n	x	x	x	n	n	n	n	n	x	n	n	n	x	n	n
	PI_4_9_2	x	n	x	n	n	n	x	n	n	x	x	x	n	n	n	n	n	n	x	n
	PI_4_9_3	x	n	n	n	n	n	n	x	n	n	n	n	x	x	n	n	n	n	n	n
TP2	PI_4_10_1	n	n	n	x	x	x	n	n	n	n	x	n	n	x	n	n	x	n	n	n
	PI_4_10_2	n	n	x	n	x	n	n	x	n	n	x	x	x	n	n	n	x	x	n	n
	PI_4_10_3	n	n	n	n	x	x	x	n	n	n	n	x	n	x	n	n	n	n	x	n

TP	Attrappe	Testdurchlauf																			
		1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20
TP2	Pl_5_1_1	n	n	n	n	n	n	x	n	n	n	x	x	x	x	n	n	n	n	n	n
	Pl_5_1_2	n	n	x	x	x	n	n	n	n	n	x	n	n	n	x	n	n	x	n	n
	Pl_5_1_3	n	n	n	n	n	n	n	n	x	x	n	x	n	x	n	n	x	x	n	n
TP2	Pl_5_3_1	n	x	n	n	n	n	n	n	n	n	x	x	x	x	n	n	n	n	x	n
	Pl_5_3_2	n	n	n	n	x	n	n	n	n	n	n	n	n	x	x	n	n	x	x	n
	Pl_5_3_3	n	n	n	n	n	x	x	x	n	n	n	x	n	n	n	n	n	x	n	n
TP2	Pl_5_4_1	x	n	n	n	x	n	n	n	n	x	x	n	n	n	n	n	n	n	n	n
	Pl_5_4_2	n	n	n	n	n	x	n	n	n	x	n	n	n	n	n	x	x	x	n	n
	Pl_5_4_3	n	n	n	x	x	n	n	n	x	x	n	x	n	n	n	x	n	n	n	n
TP2	Pl_5_5_1	x	n	n	n	n	x	n	n	n	n	n	n	n	n	n	n	n	x	n	n
	Pl_5_5_2	x	n	n	n	n	n	n	n	n	x	n	n	n	n	n	n	n	n	n	n
	Pl_5_5_3	n	n	n	n	n	n	n	n	n	n	n	x	n	n	n	x	n	n	x	n
TP2	Pl_5_6_1	n	n	x	x	n	n	n	x	n	n	n	n	x	x	n	n	n	n	n	n
	Pl_5_6_2	x	x	n	x	n	n	n	n	x	n	n	n	n	n	x	n	n	x	n	n
	Pl_5_6_3	n	x	n	n	x	n	n	n	x	n	n	x	n	n	n	x	n	n	n	n
TP2	Pl_5_7_1	n	n	n	n	n	x	n	n	n	n	x	n	n	x	n	n	n	n	n	x
	Pl_5_7_2	n	n	n	n	n	n	x	n	x	n	n	n	n	x	n	n	n	n	x	n
	Pl_5_7_3	x	n	n	n	n	n	x	x	n	n	n	n	x	x	n	n	n	n	x	n
TP2	Pl_5_8_1	n	n	n	n	x	n	x	n	n	n	x	n	n	n	n	x	x	x	x	n
	Pl_5_8_2	x	n	n	n	n	n	n	n	n	n	n	n	x	x	n	x	n	n	n	x
	Pl_5_8_3	n	x	n	n	n	x	n	n	n	n	n	n	n	n	n	n	n	n	x	x
TP1	Pl_6_1_1	x	x	x	n	n	x	n	n	n	x	x	n	x	n	n	n	x	x	n	x
	Pl_6_1_2	n	x	x	x	x	n	n	n	n	x	n	x	n	n	n	x	n	n	n	n
	Pl_6_1_3	x	n	n	n	n	n	n	n	n	x	x	x	n	n	n	n	x	n	n	x
TP1	Pl_6_2_1	n	n	x	x	x	n	n	n	n	n	n	x	x	n	x	n	n	n	x	n
	Pl_6_2_2	n	x	n	n	n	x	x	n	n	n	n	n	x	n	n	x	n	n	n	n
	Pl_6_2_3	x	x	n	n	n	n	x	n	n	n	x	n	n	x	n	n	n	n	x	x
TP1	Pl_6_3_1	n	n	x	x	x	x	n	n	x	n	n	x	n	x	x	n	n	n	x	n
	Pl_6_3_2	n	x	x	n	x	n	n	x	x	x	x	n	n	n	x	n	x	x	n	x
	Pl_6_3_3	n	n	x	x	x	n	x	x	x	n	n	n	x	n	n	n	x	x	n	x
TP1	Pl_6_4_1	n	x	n	n	n	n	n	n	n	x	x	x	n	n	n	n	x	n	n	n
	Pl_6_4_2	x	x	n	n	x	n	n	n	n	n	x	n	x	n	n	n	n	n	n	n
	Pl_6_4_3	x	x	x	x	n	x	x	n	n	n	n	n	n	n	n	n	x	x	n	x
TP1	Pl_6_5_1	n	x	n	n	n	n	n	n	n	n	x	n	x	n	x	x	n	n	n	n
	Pl_6_5_2	x	n	n	n	n	n	n	x	n	n	n	n	n	n	x	n	n	n	x	x
	Pl_6_5_3	n	n	n	n	n	n	n	n	n	x	x	n	n	n	n	x	x	x	n	x
TP1	Pl_6_7_1	n	n	n	x	x	x	n	n	n	n	n	n	n	x	n	n	n	x	n	n
	Pl_6_7_2	x	x	n	n	n	n	n	x	n	n	n	n	x	n	n	x	n	n	n	x

Tabelle 39: Testergebnisse - Platine – Silikon – unw. Opfer - Microsoft

TP	Attrappe	Testdurchlauf																			
		1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20
TP1	Pl_1_1_1	x	x	n	n	n	n	n	n	n	x	n	n	n	x	n	x	n	n	n	x
	Pl_1_1_2	n	n	n	n	n	n	x	n	n	n	x	n	n	n	n	x	x	n	x	n
	Pl_1_1_3	n	n	x	x	n	n	n	n	x	n	n	n	x	n	x	x	n	n	x	n
TP1	Pl_1_2_1	n	x	n	n	x	n	n	n	x	n	n	n	x	n	n	n	n	x	n	n
	Pl_1_2_2	n	n	x	n	n	n	x	n	n	n	n	n	x	n	n	x	x	n	n	n
	Pl_1_2_3	n	n	n	x	x	n	n	x	n	n	n	x	x	n	n	x	x	n	n	n
TP1	Pl_1_3_1	x	x	x	x	n	n	n	n	n	n	x	n	x	n	n	n	n	n	n	n
	Pl_1_3_2	n	n	n	x	n	n	n	x	n	x	x	n	n	x	n	n	n	n	x	n
	Pl_1_3_3	x	n	n	n	n	n	x	n	x	n	n	n	x	n	n	n	n	x	n	n
TP1	Pl_1_4_1	n	n	n	n	n	n	n	x	n	n	x	n	n	x	x	n	n	n	n	n
	Pl_1_4_2	n	n	n	n	n	x	x	x	n	x	n	n	x	x	n	x	n	n	x	n
	Pl_1_4_3	n	x	x	n	n	n	x	n	n	n	x	n	n	x	n	n	x	n	n	x
TP1	Pl_1_5_1	n	n	x	n	n	n	x	x	n	n	n	x	n	n	n	x	n	n	x	n
	Pl_1_5_2	x	n	n	x	n	n	x	x	x	n	n	n	n	x	x	n	n	n	n	n
	Pl_1_5_3	x	n	n	n	n	n	n	n	n	x	n	n	x	n	n	n	x	n	n	x
TP1	Pl_1_6_1	x	n	x	n	n	x	n	n	n	x	n	n	x	n	n	x	x	n	n	n
	Pl_1_6_2	x	x	n	n	n	x	x	x	n	n	n	n	x	n	x	n	n	n	x	n
	Pl_1_6_3	x	n	n	n	n	x	n	n	x	n	n	n	x	n	n	n	n	n	x	n
TP1	Pl_2_1_1	n	n	n	x	x	n	n	n	x	n	n	n	x	x	n	n	n	x	n	n
	Pl_2_1_2	n	n	n	x	x	n	n	n	n	x	n	n	n	x	n	n	n	x	n	n
	Pl_2_1_3	n	x	x	x	x	n	n	n	n	n	n	x	n	n	x	n	n	n	x	n
TP1	Pl_2_2_1	n	x	n	x	n	n	n	n	x	n	x	x	n	n	x	n	n	n	x	n
	Pl_2_2_2	n	n	n	x	n	n	n	n	x	x	x	n	n	n	x	n	n	n	n	n
	Pl_2_2_3	n	n	n	n	x	n	n	x	n	n	x	x	n	n	x	n	n	n	x	n
TP1	Pl_2_3_1	n	n	n	n	x	n	n	x	x	n	n	x	n	x	n	n	x	n	x	x
	Pl_2_3_2	x	x	x	n	n	n	x	n	n	n	n	n	n	n	x	x	n	x	n	x
	Pl_2_3_3	n	n	n	n	x	x	x	n	n	n	x	n	x	n	x	x	n	n	n	n
TP1	Pl_2_4_1	x	n	n	x	n	n	n	n	n	n	x	n	n	x	x	n	n	n	n	n
	Pl_2_4_2	x	x	x	n	n	n	n	n	n	x	n	n	n	x	n	n	n	n	x	n
	Pl_2_4_3	n	n	n	x	n	n	n	n	x	n	n	n	x	x	n	n	x	n	n	x
TP1	Pl_2_5_1	x	n	n	n	n	n	x	n	n	x	x	n	n	n	x	n	n	x	x	n
	Pl_2_5_2	n	n	x	x	n	n	n	n	n	n	n	x	n	x	n	n	n	x	n	n
	Pl_2_5_3	n	n	n	n	n	n	n	x	n	n	x	n	x	n	n	x	n	n	n	n
TP1	Pl_2_6_1	n	x	n	n	n	n	x	n	n	n	x	n	x	n	n	n	x	x	n	n
	Pl_2_6_2	n	n	n	x	n	n	n	x	x	x	n	n	n	x	n	n	x	n	n	x
	Pl_2_6_3	x	x	n	n	n	n	n	n	x	n	n	x	n	n	x	n	n	n	n	x

TP	Attrappe	Testdurchlauf																			
		1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20
TP2	PI_4_1_1	n	x	x	n	n	n	x	n	x	x	x	n	n	x	x	n	n	n	n	x
	PI_4_1_2	n	n	n	n	x	n	n	n	x	n	x	x	n	n	n	n	x	n	n	n
	PI_4_1_3	n	x	n	n	n	x	x	n	n	n	x	x	x	n	n	n	n	x	n	n
TP2	PI_4_2_1	x	x	n	n	n	n	n	n	n	n	x	x	n	n	n	x	n	n	n	n
	PI_4_2_2	x	x	n	n	n	n	n	x	n	n	n	n	n	x	n	n	n	n	x	n
	PI_4_2_3	n	n	n	n	n	n	x	n	n	n	x	x	n	x	n	n	n	n	x	n
TP2	PI_4_3_1	n	x	n	n	n	n	n	x	x	x	n	n	n	n	n	x	n	n	n	x
	PI_4_3_2	n	x	x	x	n	n	n	n	n	x	x	n	n	x	n	n	n	n	n	x
	PI_4_3_3	n	n	n	n	n	n	n	x	x	x	n	x	n	n	n	x	x	n	n	x
TP2	PI_4_4_1	x	n	n	n	n	n	x	x	n	n	n	n	x	n	n	x	n	n	x	n
	PI_4_4_2	x	x	n	n	n	x	n	n	n	n	x	n	n	n	n	n	x	n	n	n
	PI_4_4_3	n	n	n	n	x	x	n	n	n	n	n	x	x	x	n	n	n	n	x	n
TP2	PI_4_5_1	x	x	n	n	n	x	x	x	n	n	x	x	n	n	n	x	n	n	n	x
	PI_4_5_2	n	n	n	n	x	x	n	n	n	x	n	n	n	x	x	n	n	x	n	x
	PI_4_5_3	n	n	n	x	x	n	n	x	n	n	n	x	n	x	x	n	x	n	x	n
TP2	PI_4_6_1	x	x	n	n	n	x	n	n	n	x	n	n	n	n	n	n	n	x	x	n
	PI_4_6_2	n	n	n	n	n	x	x	n	n	n	n	x	n	n	n	x	n	x	n	n
	PI_4_6_3	x	n	n	n	n	x	x	n	n	n	n	x	n	x	x	n	n	x	n	n
TP2	PI_4_7_1	n	n	x	n	n	n	x	x	n	n	n	x	n	n	n	x	n	x	x	n
	PI_4_7_2	n	n	n	x	x	n	n	n	x	n	n	x	n	n	x	x	x	n	n	n
	PI_4_7_3	n	x	x	n	n	n	n	n	x	n	n	x	x	n	x	n	n	n	x	n
TP2	PI_4_8_1	x	x	n	n	n	n	n	n	n	x	n	n	n	x	n	n	n	x	x	n
	PI_4_8_2	n	n	x	n	n	n	n	x	x	n	n	n	n	n	x	n	n	n	n	x
	PI_4_8_3	x	x	x	n	x	n	n	n	n	n	n	x	n	n	n	n	n	x	n	n
TP2	PI_4_9_1	n	n	n	x	n	n	x	x	n	n	x	n	x	x	n	x	n	n	x	n
	PI_4_9_2	n	n	n	n	x	n	n	n	n	x	n	n	n	x	n	n	x	n	n	n
	PI_4_9_3	n	n	n	n	x	n	n	x	n	n	x	n	n	x	x	n	n	n	x	n
TP2	PI_4_10_1	n	x	x	n	n	x	n	n	x	n	x	x	n	n	x	n	x	n	n	n
	PI_4_10_2	x	n	x	n	n	x	n	x	x	n	n	x	x	n	n	x	n	x	n	n
	PI_4_10_3	n	n	n	x	n	n	n	n	x	x	n	x	x	x	n	n	n	x	n	n
TP2	PI_5_1_1	n	n	n	n	n	n	x	x	n	n	n	n	x	n	x	n	n	n	x	n
	PI_5_1_2	n	n	n	x	n	n	x	x	n	n	n	n	x	x	n	x	n	n	x	n
	PI_5_1_3	n	n	n	x	n	n	n	n	n	n	x	n	x	x	n	x	n	n	n	x
TP2	PI_5_3_1	n	n	x	n	n	n	n	x	n	x	x	n	n	n	n	n	x	n	n	x
	PI_5_3_2	n	n	n	n	n	n	x	n	n	n	n	x	n	x	n	n	x	x	n	n
	PI_5_3_3	n	n	n	x	n	n	n	n	x	n	n	n	x	n	n	n	x	x	x	x
TP2	PI_5_4_1	x	n	x	x	n	n	n	n	x	n	n	x	n	x	x	n	n	n	x	n
	PI_5_4_2	x	n	n	n	n	n	n	x	n	x	x	n	n	x	n	n	x	n	x	n
	PI_5_4_3	n	n	n	n	x	n	n	x	x	n	n	n	x	x	x	n	n	n	n	n
TP2	PI_5_5_1	x	x	n	n	n	n	n	n	n	x	n	n	x	n	n	n	x	n	n	n
	PI_5_5_2	n	n	n	n	x	n	n	x	x	n	n	x	x	n	n	x	n	n	x	n
	PI_5_5_3	n	n	n	n	x	x	x	n	n	n	x	n	n	n	x	n	n	n	x	n

TP	Attrappe	Testdurchlauf																			
		1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20
TP2	Pl_5_6_1	x	x	n	n	n	n	n	x	n	n	n	x	n	n	n	x	n	x	n	x
	Pl_5_6_2	n	x	n	n	n	n	n	x	n	n	x	n	x	x	n	n	n	x	n	n
	Pl_5_6_3	n	n	n	n	n	n	n	x	x	n	n	x	n	n	n	x	x	n	x	x
TP2	Pl_5_7_1	x	n	n	n	n	x	n	n	n	n	n	n	x	n	x	n	n	x	n	n
	Pl_5_7_2	n	n	x	x	n	n	n	x	n	n	x	n	x	n	n	n	n	x	n	n
	Pl_5_7_3	x	n	n	n	n	n	n	n	x	n	n	x	x	n	n	n	n	x	n	x
TP2	Pl_5_8_1	n	n	n	x	n	n	n	x	n	n	x	x	n	n	n	n	n	x	n	x
	Pl_5_8_2	x	x	n	n	n	n	x	n	n	n	x	n	n	x	n	n	x	n	n	n
	Pl_5_8_3	n	n	n	n	n	x	n	n	n	x	x	n	n	n	x	n	n	n	x	n
TP1	Pl_6_1_1	x	x	n	n	n	n	x	x	n	n	n	x	n	n	x	n	n	x	x	n
	Pl_6_1_2	x	n	n	n	n	x	x	n	n	x	n	n	n	x	n	x	n	n	n	n
	Pl_6_1_3	n	n	n	n	x	n	n	x	n	n	x	x	n	n	x	n	x	n	n	n
TP1	Pl_6_2_1	n	x	x	n	n	n	n	x	n	n	n	x	n	n	n	n	x	x	n	n
	Pl_6_2_2	n	n	n	n	n	x	n	n	x	n	n	x	x	n	n	n	x	n	n	n
	Pl_6_2_3	x	n	n	n	n	n	n	x	n	x	x	n	x	n	n	n	x	n	n	n
TP1	Pl_6_3_1	n	n	n	x	n	x	x	n	n	n	n	n	x	n	n	n	x	x	n	n
	Pl_6_3_2	x	x	x	n	n	n	n	n	n	n	n	x	n	x	n	n	n	n	x	n
	Pl_6_3_3	n	n	n	n	n	n	x	n	n	n	x	n	n	x	x	n	n	x	n	x
TP1	Pl_6_4_1	n	n	n	x	n	n	x	x	n	x	n	n	n	n	x	n	n	n	x	n
	Pl_6_4_2	n	n	n	x	x	x	n	n	n	n	n	n	x	n	x	n	n	x	n	x
	Pl_6_4_3	n	n	n	n	n	x	n	n	x	n	x	n	x	x	n	n	x	n	n	n
TP1	Pl_6_5_1	n	n	n	x	x	n	n	n	x	x	x	n	n	n	n	x	n	n	n	n
	Pl_6_5_2	x	n	n	n	n	n	n	x	n	n	n	x	n	x	n	n	n	n	x	n
	Pl_6_5_3	x	x	x	x	n	n	n	n	n	n	n	n	n	x	x	n	n	n	x	n

Tabelle 40: Testergebnisse - Platine - Gelatine – unw. Opfer - Microsoft

TP	Attrappe	Testdurchlauf																			
		1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20
TP1	Pl_1_1_1	n	n	x	x	x	n	n	n	n	n	n	n	x	n	x	n	n	n	x	n
	Pl_1_1_2	x	n	n	n	n	n	n	n	n	n	n	n	n	x	x	n	n	n	n	x
	Pl_1_1_3	n	n	x	n	x	x	n	n	n	n	n	n	n	n	n	x	n	n	x	n
TP1	Pl_1_2_1	n	n	n	n	n	n	n	n	n	n	n	x	x	x	n	n	n	n	x	x
	Pl_1_2_2	n	n	n	n	n	n	n	x	n	n	x	n	n	n	n	n	n	x	x	n
	Pl_1_2_3	n	x	n	n	x	x	n	n	n	n	n	n	n	x	n	n	n	n	n	x
TP1	Pl_1_3_1	n	x	n	n	x	n	x	x	x	n	x	x	x	n	n	n	n	n	x	n
	Pl_1_3_2	n	n	n	x	n	x	x	n	n	n	n	n	n	x	x	n	n	n	n	n
	Pl_1_3_3	x	n	n	n	n	n	x	x	n	n	n	n	n	n	x	n	n	n	n	n
TP1	Pl_1_4_1	n	n	n	n	n	x	n	n	n	n	n	n	x	x	n	n	n	x	n	n
	Pl_1_4_2	n	n	n	x	n	n	n	n	x	n	n	n	x	n	n	n	n	n	n	n
	Pl_1_4_3	n	n	n	n	x	x	x	n	n	n	n	n	x	n	x	x	n	n	n	n
TP1	Pl_1_5_1	n	x	x	n	x	x	x	n	n	n	n	n	n	n	n	n	x	n	n	n
	Pl_1_5_2	n	n	x	n	n	n	x	x	n	n	n	n	n	n	x	n	n	n	x	n
	Pl_1_5_3	n	x	n	n	n	n	n	x	x	n	n	n	n	n	x	o	x	x	n	n
	Pl_1_5_4	n	n	n	x	n	n	x	n	n	n	x	n	n	n	x	x	n	n	n	n
	Pl_1_5_5	n	n	n	x	n	n	n	n	n	x	x	n	x	n	n	n	n	n	n	n
	Pl_1_5_6	x	n	n	x	n	n	n	n	n	n	n	n	x	x	n	n	n	x	n	n
	Pl_1_5_7	n	n	x	n	n	n	x	n	n	n	n	n	x	n	n	x	n	x	n	n
	Pl_1_5_8	x	n	n	n	x	n	x	x	n	n	n	n	x	n	n	n	x	x	n	n
	Pl_1_5_9	x	n	x	n	n	x	n	n	n	n	n	n	x	x	n	n	n	x	n	n
	Pl_1_5_10	n	x	n	n	n	n	x	x	n	x	n	n	n	n	n	x	n	x	n	n
	Pl_1_5_11	n	n	x	n	n	n	x	x	n	n	n	n	n	n	x	n	n	n	n	n
	Pl_1_5_12	n	n	n	n	n	n	n	n	n	n	n	n	n	n	x	n	n	n	n	n
	Pl_1_5_13	n	n	n	n	n	n	x	x	x	n	x	n	n	x	x	n	n	x	n	n
	Pl_1_5_14	n	x	n	n	x	x	n	n	n	n	x	n	n	n	x	n	x	n	x	n
	Pl_1_5_15	n	n	n	n	x	n	x	x	n	x	x	n	n	n	x	n	n	x	x	n
	Pl_1_5_16	n	x	n	n	n	n	n	n	n	x	n	n	n	n	x	n	n	n	n	x
	Pl_1_5_17	n	n	x	n	x	x	n	x	x	x	n	n	x	x	x	x	n	n	n	n
	Pl_1_5_18	x	n	n	n	n	n	n	n	n	n	n	x	x	x	n	x	n	n	x	x
	Pl_1_5_19	n	n	n	x	n	n	n	n	x	n	n	n	n	n	n	n	x	n	n	n
	Pl_1_5_20	n	n	n	x	n	x	n	n	n	n	n	n	x	x	n	n	x	n	n	n
TP1	Pl_1_6_1	n	n	n	n	n	n	n	n	n	n	n	n	n	x	n	x	n	n	n	n
	Pl_1_6_2	n	n	n	n	n	n	x	x	n	n	n	x	n	n	n	n	n	n	n	n
	Pl_1_6_3	n	n	n	n	n	n	n	n	x	n	n	x	n	n	n	n	n	n	n	n
TP1	Pl_2_1_1	n	n	n	n	n	n	n	n	n	x	n	n	n	x	n	n	x	n	n	n
	Pl_2_1_2	x	x	n	n	x	x	n	n	n	n	n	n	n	n	n	n	n	x	n	n
	Pl_2_1_3	n	n	n	n	n	n	n	x	x	n	n	n	n	n	n	x	n	n	n	n
TP1	Pl_2_2_1	n	n	n	n	n	n	n	x	x	x	n	n	x	n	x	n	n	n	x	n
	Pl_2_2_2	n	n	n	n	n	n	n	n	n	n	n	n	x	x	n	x	n	x	x	n
	Pl_2_2_3	n	n	x	n	x	x	x	n	n	x	n	n	n	n	n	x	n	n	n	n
TP1	Pl_2_3_1	n	n	n	n	x	n	n	n	n	n	n	x	n	n	n	n	n	x	x	n
	Pl_2_3_2	n	x	n	n	n	n	x	n	n	n	n	n	x	n	n	n	x	x	n	x
	Pl_2_3_3	n	n	n	n	n	n	n	n	n	n	x	n	n	n	n	n	n	n	n	n

TP	Attrappe	Testdurchlauf																			
		1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20
TP1	PI_2_4_1	n	n	n	n	n	n	n	n	x	x	n	n	x	n	x	n	n	n	x	x
	PI_2_4_2	n	x	x	n	n	n	n	n	n	n	n	n	x	n	n	n	n	x	x	n
	PI_2_4_3	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n	x	n
TP1	PI_2_5_1	x	n	n	x	n	n	n	n	n	n	n	x	x	x	n	n	n	n	x	x
	PI_2_5_2	n	x	n	x	n	n	n	n	x	x	n	x	n	n	x	n	n	n	n	n
	PI_2_5_3	n	n	n	n	n	x	n	n	n	n	n	n	n	n	n	x	x	x	n	n
TP1	PI_2_6_1	n	n	n	n	n	n	n	n	n	n	x	n	n	n	x	n	n	n	x	n
	PI_2_6_2	n	n	n	n	n	n	x	n	n	n	n	n	x	x	n	n	n	n	n	x
	PI_2_6_3	n	n	n	n	n	n	x	n	n	n	n	n	n	n	x	n	n	n	n	n
TP2	PI_3_1_1	n	n	n	n	n	x	n	n	n	n	n	n	n	n	n	x	x	x	n	n
	PI_3_1_2	n	n	n	n	n	n	n	n	n	n	n	x	n	x	n	n	x	n	n	n
	PI_3_1_3	n	n	n	x	n	x	x	n	x	n	n	n	n	n	n	n	n	n	n	x
TP2	PI_3_2_1	n	n	x	x	x	n	n	n	n	x	x	n	n	n	n	n	n	n	x	n
	PI_3_2_2	n	n	n	n	n	n	n	n	n	n	n	n	x	n	x	x	x	n	n	n
	PI_3_2_3	n	n	n	x	n	n	n	n	n	n	n	n	x	x	x	n	n	n	n	n
TP2	PI_3_3_1	n	n	n	n	n	n	x	n	n	n	x	n	n	n	x	x	x	x	n	x
	PI_3_3_2	n	n	x	n	x	n	x	n	n	n	x	n	x	x	n	n	n	n	n	n
	PI_3_3_3	n	n	n	n	x	n	x	x	x	n	n	n	n	n	n	x	n	n	x	n
TP2	PI_4_1_1	n	n	n	n	n	n	n	n	x	n	n	x	n	n	x	x	n	n	n	n
	PI_4_1_2	n	n	x	n	x	n	n	n	n	x	n	n	n	n	n	x	n	n	x	n
	PI_4_1_3	n	n	n	n	x	n	n	n	n	n	n	x	n	n	n	n	n	n	n	n
TP2	PI_4_2_1	n	n	n	n	n	n	n	n	n	n	n	n	x	x	x	n	n	n	n	x
	PI_4_2_2	n	n	n	n	n	n	n	n	n	n	x	n	n	n	x	x	n	n	n	x
	PI_4_2_3	n	n	n	n	n	x	x	n	n	x	n	n	n	x	n	n	n	x	n	n
TP2	PI_4_3_1	n	n	n	n	n	n	n	x	x	n	x	n	n	x	n	x	n	n	x	n
	PI_4_3_2	x	n	x	n	n	x	n	n	n	n	n	n	n	n	n	x	n	x	n	n
	PI_4_3_3	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n	x	n	n	n
TP2	PI_4_4_1	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n	x	n
	PI_4_4_2	n	n	n	n	n	n	n	n	n	n	n	x	n	n	n	n	n	x	n	n
	PI_4_4_3	n	n	n	n	n	n	n	n	n	n	x	n	n	n	n	x	n	x	n	x
TP2	PI_4_5_1	n	n	n	n	x	n	n	n	n	n	n	n	n	n	x	n	n	x	n	x
	PI_4_5_2	n	x	n	x	n	n	n	n	n	n	n	n	n	x	n	n	n	n	n	x
	PI_4_5_3	n	x	x	x	x	n	n	n	n	n	n	n	n	n	n	x	x	n	x	n
TP2	PI_4_6_1	n	n	n	n	n	n	x	n	n	n	n	n	n	n	n	x	n	x	n	n
	PI_4_6_2	n	n	x	x	n	n	n	n	n	n	n	x	n	x	n	n	n	n	n	n
	PI_4_6_3	n	x	n	n	n	n	n	n	n	x	x	x	x	n	n	n	n	x	n	n
TP2	PI_4_7_1	x	n	n	n	x	n	x	n	n	x	n	n	n	n	n	n	n	n	n	n
	PI_4_7_2	n	x	n	n	n	n	n	x	n	x	n	n	n	n	n	n	n	n	x	n
	PI_4_7_3	n	n	x	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n
TP2	PI_4_8_1	n	n	x	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n	x	n
	PI_4_8_2	n	n	n	n	n	n	n	n	x	x	x	n	x	n	n	x	n	n	n	n
	PI_4_8_3	n	n	n	n	n	n	n	n	n	n	n	x	n	n	n	n	n	n	n	x

TP	Attrappe	Testdurchlauf																			
		1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20
TP2	PI_4_9_1	n	n	n	n	n	n	x	n	n	n	n	n	n	n	x	n	n	n	n	n
	PI_4_9_2	n	n	n	n	n	n	x	n	n	n	n	n	n	n	n	n	n	x	n	x
	PI_4_9_3	n	n	n	x	n	n	x	n	x	x	n	n	n	n	n	n	n	x	n	n
TP2	PI_4_10_1	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n	x	x	n	x	n
	PI_4_10_2	n	n	n	n	n	n	n	x	n	x	n	n	n	x	n	n	n	x	n	n
	PI_4_10_3	n	n	n	n	n	n	n	n	n	n	n	x	n	n	n	n	n	n	n	n
TP2	PI_5_1_1	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n	x	n	n	x
	PI_5_1_2	n	n	n	x	n	n	x	n	n	n	n	n	n	n	n	n	n	n	x	x
	PI_5_1_3	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n	x	n
TP2	PI_5_2_1	n	n	n	n	n	n	n	n	n	n	n	n	n	n	x	n	n	x	n	n
	PI_5_2_2	n	n	n	n	n	x	x	x	x	x	x	n	n	n	n	n	x	n	n	n
	PI_5_2_3	n	n	n	n	n	n	n	x	n	n	n	x	x	n	n	n	n	x	x	n
TP2	PI_5_3_1	x	n	n	n	n	x	n	n	n	x	n	n	x	x	n	n	n	x	n	n
	PI_5_3_2	x	n	n	n	x	x	n	n	n	x	n	n	n	x	n	n	n	n	n	n
	PI_5_3_3	n	n	n	x	n	n	n	n	n	n	n	n	x	n	n	n	n	x	x	n
TP2	PI_5_4_1	n	x	n	n	x	x	n	n	n	n	x	n	n	n	n	n	n	x	n	n
	PI_5_4_2	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n	x	x	x	n
	PI_5_4_3	n	n	n	n	n	n	n	n	x	n	n	n	n	n	x	x	x	n	x	n
TP2	PI_5_5_1	n	n	n	n	x	n	n	n	n	x	x	n	n	n	x	n	n	n	n	n
	PI_5_5_2	n	n	n	n	n	n	n	n	n	n	n	n	x	n	n	n	n	n	n	n
	PI_5_5_3	n	n	n	n	n	n	n	n	n	n	n	x	x	n	x	x	n	x	n	x
TP2	PI_5_6_1	x	n	n	x	n	n	n	n	n	n	n	n	n	n	n	n	x	x	x	n
	PI_5_6_2	n	n	n	n	x	n	n	n	n	n	n	x	x	n	n	x	n	n	n	n
	PI_5_6_3	n	x	x	n	n	n	n	n	n	n	n	n	n	n	n	n	x	x	n	x
TP2	PI_5_7_1	n	n	x	n	x	n	n	n	n	n	n	x	n	n	n	n	n	n	x	n
	PI_5_7_2	n	n	n	x	n	x	x	n	n	n	n	n	n	n	n	n	n	n	n	n
	PI_5_7_3	n	n	n	n	n	n	n	n	x	n	x	n	x	n	n	n	n	n	n	n
TP2	PI_5_8_1	n	n	x	x	n	n	x	n	x	x	x	n	n	n	x	n	n	n	n	n
	PI_5_8_2	n	x	x	n	n	x	x	n	n	n	n	n	n	n	n	n	n	n	x	n
	PI_5_8_3	x	n	x	n	n	x	n	n	n	n	x	x	n	n	n	n	n	n	x	n
TP1	PI_6_1_1	x	n	n	n	n	n	n	n	n	x	x	x	n	n	n	n	n	n	n	n
	PI_6_1_2	n	n	n	n	n	n	n	x	x	n	n	n	n	n	n	n	x	n	x	x
	PI_6_1_3	x	x	n	n	n	n	x	x	n	n	n	x	n	n	n	n	n	n	n	n
TP1	PI_6_2_1	x	x	n	n	n	x	n	n	n	n	n	n	n	n	n	x	n	n	n	n
	PI_6_2_2	n	n	n	x	n	n	n	n	n	n	n	n	n	x	n	x	n	n	n	n
	PI_6_2_3	n	n	n	n	x	x	n	n	x	n	n	n	n	n	x	n	n	n	n	n
TP1	PI_6_3_1	n	n	n	n	n	n	n	n	n	x	x	n	n	x	n	n	n	x	x	x
	PI_6_3_2	x	n	x	n	n	n	x	n	n	n	n	n	n	n	n	n	n	x	x	x
	PI_6_3_3	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n	x	n
TP1	PI_6_4_1	x	n	n	x	n	n	n	n	n	x	n	n	n	n	n	n	x	x	n	n
	PI_6_4_2	n	n	n	n	n	x	n	n	n	n	n	n	n	x	x	x	n	n	n	n
	PI_6_4_3	n	n	x	x	n	n	x	x	n	n	n	n	n	n	n	n	n	n	n	n
TP1	PI_6_5_1	n	n	n	n	n	n	n	x	n	n	n	n	x	n	x	n	n	n	n	n
	PI_6_5_2	n	n	n	n	n	x	x	n	n	n	n	n	x	n	n	x	x	n	x	n
	PI_6_5_3	x	n	n	x	x	n	n	n	n	n	x	n	n	n	x	n	n	n	n	x

TP	Attrappe	Testdurchlauf																			
		1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20
TP1	Pl_6_7_1	n	n	n	n	n	n	x	n	n	n	n	n	n	x	n	x	n	n	x	n
	Pl_6_7_2	n	n	n	n	n	n	n	n	n	x	n	x	n	n	n	x	n	n	n	x
	Pl_6_7_3	x	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n	x	x	x	n
TP1	Pl_6_8_1	n	n	n	n	n	n	n	x	n	n	n	n	n	x	n	x	n	n	n	n
	Pl_6_8_2	n	n	n	n	n	n	n	n	x	x	n	n	n	n	n	x	n	n	n	x
	Pl_6_8_3	n	n	n	n	n	n	n	n	n	n	n	n	n	x	n	n	n	x	n	x
TP1	Pl_6_10_1	x	n	n	n	n	n	x	n	n	n	n	x	n	n	n	x	n	n	n	x
	Pl_6_10_2	x	n	x	n	n	n	n	n	n	n	n	n	n	n	x	n	n	x	n	n
	Pl_6_10_3	n	n	n	n	n	n	n	n	n	n	x	x	n	n	x	x	n	n	n	x
TP1	Pl_6_11_1	n	x	n	n	x	n	n	n	n	n	n	n	n	n	x	n	n	n	n	n
	Pl_6_11_2	n	n	n	x	n	x	n	n	x	n	n	x	n	n	n	n	n	n	n	x
	Pl_6_11_3	n	n	n	n	n	n	n	x	n	n	n	n	x	n	n	n	n	n	n	n

Appendix B

Die folgenden Tabellen zeigen die konkreten Testergebnisse der Testreihen mit kooperativem sowie unwissendem Opfer für den Digitus Fingerprint-Reader. Die Abdruckattrappen wurden wieder von Vorlagen derselben Testpersonen wie bereits für den Microsoft Fingerprint-Reader hergestellt. Eine genauere Charakterisierung der Testpersonen sowie eine Erklärung der Attrappenbezeichnungen kann der Einleitung in Appendix A entnommen werden.

Tabelle 41: Testergebnisse - Fimo – Holzleim – koop. Opfer - Digitus

TP	Attrappe	Testdurchlauf																			
		1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20
TP2	Fimo2_1	n	n	n	n	n	n	n	n	n	n	n	n	n	x	n	n	n	n	n	n
	Fimo2_2	n	n	n	n	n	n	n	x	n	n	n	n	n	n	n	n	n	n	n	n
	Fimo2_3	n	n	n	n	n	x	x	n	n	n	n	n	n	n	x	n	n	x	n	n
TP2	Fimo3_1	x	n	n	x	n	x	n	n	n	n	n	n	n	n	x	n	n	n	n	x
	Fimo3_2	n	n	n	n	n	n	x	n	n	x	n	n	n	n	n	x	n	n	n	n
	Fimo3_3	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n	x	x	n	n
TP1	Fimo5_1	n	n	x	n	n	x	n	n	n	n	n	n	n	n	n	x	n	n	n	n
	Fimo5_2	n	n	n	n	x	n	n	n	n	n	n	n	n	n	x	n	n	n	n	n
	Fimo5_3	n	n	n	n	n	n	x	n	n	n	n	n	n	n	n	n	n	n	x	n
TP1	Fimo8_1	n	n	n	n	n	n	n	n	n	n	n	n	x	n	n	n	n	n	n	n
	Fimo8_2	n	n	n	n	n	n	x	n	n	n	n	n	n	n	n	n	n	n	n	n
	Fimo8_3	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n
TP1	Fimo9_1	n	n	n	n	n	x	n	n	n	n	x	n	n	x	n	n	n	n	n	n
	Fimo9_2	n	n	n	n	n	n	n	x	n	n	n	x	n	x	n	n	n	n	n	n
	Fimo9_3	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n
TP2	Fimo10_1	n	n	n	n	n	x	n	n	x	n	n	x	n	n	n	n	x	n	n	n
	Fimo10_2	n	x	n	n	n	n	x	n	n	n	n	n	n	n	x	n	n	n	n	x
TP2	Fimo11_1	n	n	n	n	n	n	x	n	n	n	n	n	x	n	n	n	x	n	n	n
	Fimo11_2	n	n	x	x	n	x	n	n	n	n	n	n	n	n	n	n	n	n	n	n
TP1	Fimo12_1	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n
	Fimo12_2	n	n	n	x	x	n	x	n	n	n	n	n	n	n	n	n	n	n	n	n
	Fimo12_3	n	n	n	n	n	n	n	n	n	x	n	n	n	n	n	n	n	n	n	n
TP1	Fimo13_1	n	n	n	n	n	n	n	n	x	n	x	x	x	n	n	n	n	n	n	n
	Fimo13_2	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n	x	n	n	n	x
	Fimo13_3	n	n	n	n	x	n	n	x	n	n	n	n	n	x	n	n	n	n	n	n
TP2	Fimo14_1	n	n	n	n	n	n	n	n	n	x	n	x	n	n	n	n	n	n	n	n
	Fimo14_2	n	n	x	n	n	n	n	n	n	n	n	n	n	x	n	n	x	x	n	n
TP2	Fimo15_1	n	n	x	x	x	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n
	Fimo15_2	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n
	Fimo15_3	n	n	n	n	n	n	n	x	x	n	n	n	n	n	n	x	n	n	n	n
TP1	Fimo16_1	n	n	n	n	n	n	n	x	n	n	n	n	n	n	n	n	n	x	n	n
	Fimo16_2	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n
	Fimo16_3	n	n	n	n	n	n	n	n	n	n	n	n	x	x	n	n	n	n	n	n

TP	Attrappe	Testdurchlauf																			
		1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20
TP1	Fimo17_1	n	n	x	n	n	n	n	n	n	n	n	n	n	n	n	n	n	x	n	n
	Fimo17_2	x	n	x	n	n	n	n	n	n	n	n	n	n	n	x	n	n	n	n	n
TP1	Fimo18_1	n	n	n	n	n	n	n	n	n	n	x	n	n	n	n	x	n	n	n	n
	Fimo18_2	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n
	Fimo18_3	n	n	n	n	n	n	n	x	n	n	n	n	n	x	n	n	n	x	n	n
TP1	Fimo19_1	n	n	x	n	n	n	n	n	n	n	x	n	n	n	n	n	x	n	n	n
	Fimo19_2	n	n	n	n	n	n	n	x	n	n	n	n	n	n	n	n	n	n	n	n
	Fimo19_3	n	n	n	n	n	n	n	x	n	n	n	n	x	n	n	n	x	n	n	n
TP2	Fimo21_1	n	n	n	x	x	n	n	n	n	n	n	n	n	n	n	n	x	n	n	n
	Fimo21_2	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n
	Fimo21_3	n	n	n	x	n	x	n	n	n	n	n	n	n	n	x	n	n	n	n	n
TP2	Fimo22_1	n	n	n	n	n	n	n	n	n	n	n	x	n	n	n	x	n	n	n	n
	Fimo22_2	n	n	n	n	n	n	n	x	n	n	n	n	n	n	n	n	n	n	n	n
	Fimo22_3	n	n	n	n	n	n	n	n	n	n	n	n	n	x	x	n	n	x	n	n
TP2	Fimo23_1	n	n	n	n	x	n	n	n	n	x	n	n	n	n	n	x	n	n	n	n
	Fimo23_2	n	n	x	n	n	n	n	n	n	n	x	n	n	n	n	n	n	n	n	n
	Fimo23_3	n	n	n	n	n	n	x	x	n	n	n	n	n	n	n	n	n	n	n	n
TP2	Fimo24_1	n	n	n	n	x	n	x	n	n	n	n	n	n	n	n	n	n	n	n	n
	Fimo24_2	n	n	n	n	n	n	n	n	n	n	n	n	n	x	n	x	n	n	x	n
	Fimo24_3	n	n	n	n	n	n	n	x	n	n	n	n	x	n	n	n	n	n	x	n
TP1	Fimo25_1	n	n	n	n	n	n	n	n	x	n	n	n	n	n	n	x	n	n	n	n
	Fimo25_2	x	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n
	Fimo25_3	n	n	n	n	n	n	n	n	n	x	n	x	n	n	n	n	n	x	n	n
TP1	Fimo26_1	n	n	n	n	n	n	x	n	n	n	n	n	n	n	n	n	n	n	n	n
	Fimo26_2	n	n	n	n	n	n	n	n	n	n	n	n	n	n	x	x	n	n	n	n
	Fimo26_3	n	n	n	n	n	n	n	n	n	n	x	n	n	n	n	n	n	n	n	n
TP2	Fimo27_1	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n	x	n	n	n	x
	Fimo27_2	n	x	n	n	n	n	n	n	n	n	n	n	n	n	x	n	n	n	x	n
	Fimo27_3	n	n	n	n	n	n	n	n	x	n	n	n	n	n	x	x	n	n	n	n
TP2	Fimo28_1	n	n	n	n	x	n	n	x	n	n	n	n	n	x	n	n	n	n	n	n
	Fimo28_2	n	n	n	x	n	n	x	n	n	n	n	n	n	n	n	n	x	n	n	n
	Fimo28_3	n	n	n	n	x	x	n	n	n	n	n	n	n	n	n	n	x	n	n	n

Tabelle 42: Testergebnisse - Fimo – Bastelkleber – koop. Opfer - Digitus

TP	Attrappe	Testdurchlauf																			
		1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20
TP2	Fimo2_1	x	n	n	n	x	x	n	n	n	n	x	n	n	x	n	n	n	n	n	n
	Fimo2_2	n	x	n	x	x	x	n	n	x	n	n	x	x	x	x	n	n	n	n	n
	Fimo2_3	n	n	n	n	n	x	n	n	n	n	n	n	n	n	x	n	n	x	n	n
TP2	Fimo3_1	n	n	n	n	n	n	n	n	x	n	n	n	x	x	n	x	n	n	n	x
	Fimo3_2	n	n	n	x	x	n	n	n	n	n	n	n	n	n	x	x	x	n	n	n
	Fimo3_3	n	n	n	n	x	n	n	n	n	n	n	n	n	n	n	n	n	x	n	n
TP1	Fimo5_1	n	n	x	n	x	x	n	n	n	n	x	x	n	n	n	x	n	n	n	n
	Fimo5_2	x	x	n	x	x	n	n	n	n	x	n	n	n	n	n	n	n	x	n	n
	Fimo5_3	n	x	x	n	n	n	n	n	n	x	n	n	x	n	n	n	n	x	n	n
TP1	Fimo8_1	n	n	n	n	n	x	n	n	n	x	n	n	n	n	x	n	n	n	n	n
	Fimo8_2	x	x	x	n	n	x	n	n	n	n	n	n	n	n	n	x	n	n	x	n
	Fimo8_3	n	x	x	x	n	x	n	n	x	n	x	n	x	n	n	x	n	x	n	n
TP1	Fimo9_1	n	n	x	n	n	n	n	n	n	n	n	n	x	x	n	n	n	n	x	n
	Fimo9_2	x	n	x	n	n	n	x	n	x	x	n	x	n	n	n	n	n	x	n	n
	Fimo9_3	x	n	x	n	n	n	n	x	x	n	n	n	x	n	n	n	x	n	n	n
TP2	Fimo10_1	n	n	x	n	n	n	n	n	n	n	x	n	x	n	n	n	n	n	n	n
	Fimo10_2	x	x	x	n	n	x	n	n	n	x	x	n	n	n	n	x	x	n	n	n
	Fimo10_3	x	n	n	n	n	n	x	x	n	x	x	n	n	n	x	n	x	x	n	n
TP2	Fimo11_1	n	n	n	x	n	x	n	n	n	n	n	n	x	n	n	x	n	n	n	n
	Fimo11_2	x	x	n	n	x	x	n	n	n	n	n	n	n	x	n	x	n	n	x	x
	Fimo11_3	n	n	n	n	n	x	x	n	n	n	n	n	n	n	n	x	n	n	n	x
TP1	Fimo12_1	x	n	x	x	n	n	n	n	n	n	x	n	n	n	n	n	x	n	x	n
	Fimo12_2	n	x	x	n	n	n	n	n	x	x	n	n	n	n	n	n	x	n	x	n
	Fimo12_3	n	n	n	n	n	n	n	n	n	x	x	n	n	n	n	x	n	n	n	x
TP1	Fimo13_1	n	n	n	n	x	n	n	x	x	n	n	n	n	n	n	n	n	n	x	n
	Fimo13_2	x	x	x	n	n	n	n	n	n	n	n	x	n	x	n	n	x	x	n	x
	Fimo13_3	n	n	n	x	x	n	n	x	x	n	n	n	x	n	n	n	n	x	n	x
TP2	Fimo14_1	n	n	n	x	x	n	x	n	n	n	x	n	n	n	n	n	n	x	x	n
	Fimo14_2	n	n	n	n	n	x	n	n	n	x	n	x	x	n	n	x	n	n	n	x
	Fimo14_3	n	n	n	n	n	n	x	n	n	n	x	n	x	x	n	x	x	n	n	x
TP2	Fimo15_1	x	n	n	n	n	n	n	n	x	n	n	x	x	n	n	n	x	n	n	n
	Fimo15_2	x	n	x	n	n	n	n	n	n	x	x	n	n	n	n	n	n	n	n	x
	Fimo15_3	n	n	n	n	x	n	n	n	n	n	n	n	x	n	n	n	n	n	n	n
TP1	Fimo16_1	x	n	x	n	n	n	n	n	n	x	n	n	x	n	n	x	n	n	n	n
	Fimo16_2	n	x	x	x	n	n	x	n	n	n	n	x	n	x	n	n	n	n	n	n
	Fimo16_3	n	n	n	x	n	x	n	n	n	n	x	n	n	n	x	n	n	n	n	x

TP	Attrappe	Testdurchlauf																			
		1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20
TP1	Fimo17_1	n	n	x	n	n	n	n	x	n	n	n	x	n	n	x	x	x	x	n	n
	Fimo17_2	x	n	n	n	n	n	n	n	n	n	n	n	n	x	x	x	n	x	x	n
	Fimo17_3	n	n	n	n	n	x	n	n	n	n	n	n	n	n	n	n	n	n	n	n
TP1	Fimo18_1	x	n	n	x	n	x	n	x	x	x	n	n	n	n	n	n	n	n	x	n
	Fimo18_2	x	x	x	n	n	n	x	n	n	n	n	n	n	n	n	n	x	n	x	n
	Fimo18_3	n	n	n	x	n	x	n	x	x	n	n	x	n	x	x	n	n	n	x	n
TP1	Fimo19_1	n	n	x	n	n	n	n	n	n	n	n	n	x	n	n	n	n	x	n	n
	Fimo19_2	n	n	x	n	n	n	n	n	n	n	n	x	x	x	n	n	n	x	n	n
TP2	Fimo21_1	n	n	n	n	n	x	n	n	n	n	n	x	n	x	x	n	n	n	x	n
	Fimo21_2	n	x	n	n	x	n	x	x	n	n	n	n	n	n	n	n	x	n	n	n
	Fimo21_3	n	n	n	x	n	x	x	n	n	n	x	x	n	n	x	x	n	n	n	x
TP2	Fimo22_1	n	x	n	n	n	n	n	x	n	n	n	n	x	n	n	x	x	n	n	n
	Fimo22_2	x	x	x	n	n	n	x	x	n	n	n	n	n	n	n	n	n	n	n	x
	Fimo22_3	n	x	n	n	x	n	n	n	x	n	n	x	x	n	n	n	n	x	n	n
TP2	Fimo23_1	x	n	x	x	n	n	n	n	n	n	n	n	x	n	n	n	n	n	n	n
	Fimo23_2	x	x	x	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n	x	x
	Fimo23_3	n	x	n	n	x	x	n	x	n	x	x	n	n	n	x	x	x	n	n	x
TP2	Fimo24_1	n	n	n	x	n	n	n	n	x	n	n	n	n	x	n	n	n	n	n	n
	Fimo24_2	x	x	n	n	n	n	n	n	n	x	n	x	x	n	n	n	x	n	n	n
TP1	Fimo25_1	n	x	n	n	n	n	n	n	x	n	n	x	n	n	x	n	n	n	n	n
	Fimo25_2	x	n	n	n	n	x	n	x	n	x	n	n	x	n	n	n	n	x	x	n
	Fimo25_3	x	n	x	n	n	n	n	n	n	x	n	x	x	n	n	x	n	n	x	n
TP1	Fimo26_1	x	n	n	n	x	n	n	n	n	x	n	n	n	n	x	n	n	x	x	n
	Fimo26_2	n	x	n	x	n	x	x	x	n	x	n	n	x	x	n	n	x	x	n	x
	Fimo26_3	n	n	n	x	n	n	n	n	x	n	n	n	x	x	n	n	x	n	x	n
TP2	Fimo27_1	n	n	n	n	n	n	n	n	n	n	n	n	n	x	n	x	n	n	n	n
TP2	Fimo28_1	n	n	x	n	n	n	n	n	n	n	x	n	x	x	n	n	n	n	n	n
	Fimo28_2	x	n	n	n	x	n	n	n	n	n	x	n	x	n	n	x	n	x	x	n
	Fimo28_3	n	n	n	n	x	x	n	n	n	n	n	n	x	x	x	x	n	n	n	n

Tabelle 43: Testergebnisse - Fimo – Silikon – koop. Opfer - Digitus

TP	Attrappe	Testdurchlauf																			
		1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20
TP2	Fimo2_1	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n
	Fimo2_2	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n	x	n	n	n	n
	Fimo2_3	n	n	n	n	n	n	n	n	n	n	n	n	n	x	n	n	n	x	n	n
TP2	Fimo3_1	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n	x	x	n
	Fimo3_2	n	n	n	x	n	n	n	n	n	n	n	n	n	n	x	n	n	n	n	n
	Fimo3_3	n	n	n	x	x	n	n	n	n	n	n	n	n	n	n	x	n	n	n	n
TP1	Fimo5_1	n	n	n	x	n	n	n	n	n	n	n	n	x	n	n	n	n	n	n	n
	Fimo5_2	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n
TP1	Fimo8_1	n	n	n	n	n	n	n	n	x	n	x	n	n	n	n	n	n	n	n	n
	Fimo8_2	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n	x	n	x
	Fimo8_3	n	n	n	n	n	x	n	n	n	n	x	n	n	n	n	n	n	n	n	n
TP1	Fimo9_1	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n	x
	Fimo9_2	n	n	n	n	n	n	x	n	n	n	n	n	n	n	x	n	n	n	n	n
	Fimo9_3	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n
TP2	Fimo10_1	n	n	n	x	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n
	Fimo10_2	n	n	n	n	x	n	x	n	x	n	n	n	n	n	n	n	n	n	n	n
	Fimo10_3	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n
TP2	Fimo11_1	n	n	n	n	n	n	n	x	n	n	n	n	n	n	n	n	n	n	n	n
	Fimo11_2	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n
TP1	Fimo12_1	n	x	n	n	x	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n
	Fimo12_2	n	n	n	n	n	n	n	n	n	n	x	n	n	n	n	n	n	x	n	n
	Fimo12_3	n	n	n	x	n	n	n	x	n	n	n	n	n	n	n	n	n	n	n	x
TP1	Fimo13_1	n	n	n	n	n	n	n	n	n	n	n	n	x	x	x	n	n	n	n	n
	Fimo13_2	n	n	x	x	n	n	n	n	n	n	x	n	n	n	n	n	n	n	n	n
	Fimo13_3	n	n	n	n	n	n	n	n	n	n	n	n	n	x	x	n	n	n	n	n
TP2	Fimo14_1	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n	x	n	n	n	n
	Fimo14_2	n	n	n	n	n	x	n	n	n	n	n	n	n	n	n	n	n	n	n	n
	Fimo14_3	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n
TP2	Fimo15_1	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n	x	n	n
	Fimo15_2	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n
TP1	Fimo16_1	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n
	Fimo16_2	n	n	n	n	n	n	n	n	n	n	x	n	n	n	n	n	n	n	n	n
	Fimo16_3	n	n	n	n	n	x	n	n	x	n	x	n	n	n	n	n	n	n	n	n

TP	Attrappe	Testdurchlauf																			
		1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20
TP1	Fimo17_1	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n
	Fimo17_2	n	n	n	n	n	n	n	n	x	n	n	x	n	n	n	n	n	n	n	n
	Fimo17_3	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n
TP1	Fimo18_1	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n
	Fimo18_2	n	n	n	n	n	n	n	n	n	n	n	n	n	x	n	x	n	n	n	x
	Fimo18_3	n	n	n	x	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n
TP1	Fimo19_1	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n
	Fimo19_2	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n
	Fimo19_3	n	n	n	n	n	n	n	x	n	n	x	n	n	x	n	n	n	n	n	n
TP2	Fimo21_1	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n
	Fimo21_2	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n	x	n	n	n	n
	Fimo21_3	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n
TP2	Fimo22_1	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n
	Fimo22_2	n	n	n	n	n	n	n	n	n	x	n	n	n	n	n	n	n	n	n	n
TP2	Fimo23_1	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n
	Fimo23_2	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n	x	n	n	n
	Fimo23_3	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n
TP2	Fimo24_1	n	n	n	n	n	n	n	x	x	n	n	x	n	n	n	n	n	n	n	n
	Fimo24_2	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n
	Fimo24_3	n	n	n	n	n	n	n	n	n	n	n	n	n	n	x	n	n	n	n	n
TP1	Fimo25_1	n	x	n	n	n	n	n	x	x	n	n	n	n	n	n	n	n	n	n	n
	Fimo25_2	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n
	Fimo25_3	n	n	n	n	n	n	n	n	n	n	n	x	n	n	n	n	n	n	n	n
TP1	Fimo26_1	n	n	n	x	x	n	n	n	n	n	n	x	n	x	n	n	x	n	n	n
	Fimo26_2	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n
	Fimo26_3	n	n	n	n	n	n	n	n	n	n	n	n	n	x	n	n	x	n	n	n
TP2	Fimo27_1	n	n	n	n	n	n	x	n	x	x	x	n	n	x	x	n	n	n	n	n
	Fimo27_2	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n
	Fimo27_3	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n
TP2	Fimo28_1	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n
	Fimo28_2	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n	x
	Fimo28_3	n	n	n	n	n	n	n	n	n	n	x	n	n	x	n	n	n	n	n	n

Tabelle 44: Testergebnisse - Fimo – Gelatine – koop. Opfer - Digitus

TP	Attrappe	Testdurchlauf																			
		1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20
TP2	Fimo2_1	x	n	n	n	n	n	x	n	n	n	n	n	n	n	n	n	n	n	n	n
	Fimo2_2	x	x	n	n	n	n	n	n	n	n	n	n	n	n	n	x	n	n	n	n
	Fimo2_3	n	n	n	x	n	n	n	n	n	x	n	n	x	n	n	n	n	n	n	n
TP2	Fimo3_1	n	n	n	n	n	n	n	x	n	x	n	n	n	n	n	n	n	n	n	n
	Fimo3_2	n	x	x	x	n	n	x	x	x	x	n	n	n	x	x	x	n	n	n	n
	Fimo3_3	n	n	n	n	n	n	n	n	x	n	x	n	n	n	x	n	n	n	n	n
TP1	Fimo5_1	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n
	Fimo5_2	n	n	n	x	x	x	x	x	n	n	n	n	n	n	n	n	n	n	n	n
	Fimo5_3	x	n	n	x	n	n	x	x	n	n	n	x	n	x	x	n	x	n	n	n
TP1	Fimo8_1	n	x	n	x	x	n	x	x	x	x	n	n	x	n	n	n	n	n	n	n
	Fimo8_2	n	n	x	n	n	n	n	x	n	n	n	n	n	n	x	n	n	n	n	n
TP1	Fimo9_1	n	n	n	n	x	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n
	Fimo9_2	x	x	x	x	n	n	x	n	x	x	x	x	x	n	n	n	n	n	n	n
	Fimo9_3	n	n	x	n	x	n	n	n	x	n	n	n	n	n	n	n	n	n	n	n
TP2	Fimo10_1	n	n	x	n	n	n	n	n	n	x	n	x	x	n	x	x	x	n	n	n
	Fimo10_2	x	n	x	x	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n
	Fimo10_3	n	n	n	n	x	x	n	n	n	x	x	x	n	n	n	n	n	x	n	n
TP2	Fimo11_1	n	n	n	n	n	n	n	n	n	x	n	x	n	n	n	n	n	n	x	n
	Fimo11_2	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n
	Fimo11_3	n	n	x	x	n	n	n	n	x	n	n	x	n	n	n	x	n	n	n	n
TP1	Fimo12_1	n	n	n	n	x	n	x	n	n	n	n	n	n	n	n	n	n	n	n	n
	Fimo12_2	n	n	n	n	n	n	n	n	n	x	x	x	n	n	n	n	n	n	n	n
	Fimo12_3	x	x	n	n	n	n	x	n	n	n	n	n	x	n	n	n	n	n	n	n
TP1	Fimo13_1	n	n	n	x	x	n	x	n	n	n	n	n	n	n	n	n	n	n	n	n
	Fimo13_2	n	n	n	x	x	x	n	n	n	n	n	n	n	x	x	n	n	n	n	n
	Fimo13_3	n	n	n	n	n	n	n	x	n	n	n	n	n	n	n	n	n	n	n	n
TP2	Fimo14_1	n	x	x	x	x	n	n	n	x	x	x	n	x	x	n	n	n	x	x	n
	Fimo14_2	n	n	n	n	x	n	x	n	n	n	n	x	n	x	x	x	n	x	n	n
	Fimo14_3	n	n	n	x	x	n	n	n	n	n	n	x	x	n	n	n	n	n	n	n
TP2	Fimo15_1	n	n	n	x	n	n	x	x	x	n	x	x	x	n	n	n	n	x	x	n
	Fimo15_2	n	n	n	n	n	x	n	n	n	n	n	n	x	n	n	n	n	n	n	n
TP1	Fimo16_1	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n	x	n	n	n	n
	Fimo16_2	x	x	x	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n
	Fimo16_3	x	n	n	n	n	n	n	n	x	x	n	n	n	n	n	n	n	n	n	n

TP	Attrappe	Testdurchlauf																			
		1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20
TP1	Fimo17_1	n	n	n	n	n	n	n	n	n	x	n	n	x	n	n	n	n	n	n	x
	Fimo17_2	n	n	x	x	x	x	n	n	x	n	n	x	x	x	x	x	n	n	n	n
	Fimo17_3	n	n	n	n	n	n	n	n	n	n	x	x	x	n	n	n	n	n	n	n
TP1	Fimo18_1	n	n	n	n	x	x	n	n	n	n	n	n	n	n	n	n	n	n	n	n
	Fimo18_2	n	n	n	n	n	n	n	n	n	n	n	n	n	x	x	x	n	n	n	n
	Fimo18_3	x	x	x	n	n	x	n	n	x	x	n	n	n	x	x	x	n	n	n	n
TP1	Fimo19_1	n	n	n	x	x	x	n	x	n	n	n	x	x	x	n	n	n	n	n	n
	Fimo19_2	x	x	x	n	x	n	x	x	x	n	x	n	x	x	x	n	n	n	n	n
	Fimo19_3	n	x	x	n	n	n	n	x	n	n	x	x	x	n	n	n	n	n	n	n
TP2	Fimo21_1	n	n	n	n	n	n	x	n	n	n	n	n	n	n	n	x	n	x	n	n
	Fimo21_2	n	n	n	n	x	n	n	x	n	n	n	x	n	x	x	n	n	n	n	n
TP2	Fimo22_1	n	n	n	n	n	n	n	n	n	x	x	n	n	n	n	n	n	n	n	x
	Fimo22_2	n	x	n	n	n	x	n	n	n	n	n	x	n	n	n	x	n	n	x	n
	Fimo22_3	n	x	x	x	n	n	x	x	n	n	n	x	x	n	n	n	n	n	n	n
TP2	Fimo23_1	n	n	n	n	n	n	x	n	n	n	n	n	n	n	n	n	x	x	x	n
	Fimo23_2	n	x	n	x	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n
	Fimo23_3	x	n	n	n	x	n	n	n	n	n	x	x	n	n	n	x	n	n	n	n
TP2	Fimo24_1	n	n	n	n	n	n	x	n	n	n	n	n	x	n	x	n	x	n	n	n
	Fimo24_2	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n
	Fimo24_3	n	x	x	n	n	n	n	x	n	n	n	n	n	n	n	x	n	n	n	n
TP1	Fimo25_1	x	x	x	n	x	n	x	x	x	x	n	n	x	x	n	x	n	n	n	n
	Fimo25_2	x	x	x	n	x	x	x	n	n	n	n	n	x	x	x	x	n	n	n	n
	Fimo25_3	n	n	n	n	n	n	x	x	n	n	n	n	n	n	n	n	n	n	n	n
TP1	Fimo26_1	n	x	x	n	n	x	n	n	n	n	n	x	n	n	n	n	x	x	x	n
	Fimo26_2	x	n	n	n	n	n	n	n	n	n	x	x	n	n	n	x	n	n	n	n
	Fimo26_3	n	n	n	x	x	n	n	n	x	x	n	n	n	n	x	n	n	n	n	n
TP2	Fimo27_1	n	x	x	n	n	n	n	n	n	n	n	x	n	n	n	n	n	n	n	n
	Fimo27_2	n	n	x	n	n	n	x	n	n	x	n	n	n	n	x	n	n	x	n	n
TP2	Fimo28_1	n	n	n	n	n	n	x	n	n	n	n	n	n	x	n	n	n	n	n	n
	Fimo28_2	n	n	x	x	n	x	x	n	x	n	n	n	n	n	n	n	n	x	x	x
	Fimo28_3	n	n	n	x	n	x	n	x	n	x	x	n	n	x	x	n	x	n	n	n

Tabelle 45: Testergebnisse - Wachs – Holzleim – koop. Opfer - Digitus

TP	Attrappe	Testdurchlauf																			
		1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20
TP2	W_3_1	n	n	n	n	n	n	n	n	n	n	x	x	n	x	n	n	n	n	x	x
TP1	W_8_1	n	x	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n
TP1	W_12_1	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n	x	n	x	n
	W_12_2	n	n	n	n	x	n	n	n	n	n	n	x	n	n	n	x	n	n	n	n
TP1	W_13_1	n	x	n	n	n	n	n	x	n	n	n	n	n	n	n	n	n	n	n	n
	W_13_2	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n
TP2	W_15_1	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n
TP2	W_16_1	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n
	W_16_2	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n	x	n	x	x	n
	W_16_3	n	n	n	n	n	x	n	x	n	n	x	n	n	n	x	n	n	n	x	n
TP1	W_17_1	x	x	n	n	n	n	n	n	n	n	n	n	n	n	x	n	n	n	n	n
	W_17_2	n	n	n	n	x	n	n	x	n	n	x	x	n	n	n	n	n	x	n	n
	W_17_3	n	n	n	n	x	x	n	n	n	n	n	n	n	x	n	n	n	n	n	n
TP2	W_18_1	n	n	n	x	x	n	n	n	n	n	n	x	n	n	n	n	n	n	n	n
	W_18_2	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n
TP2	W_19_1	n	n	n	n	x	n	n	n	n	n	n	n	n	n	n	n	x	x	n	n
	W_19_2	n	x	n	n	n	n	n	n	n	x	n	n	n	n	n	n	n	n	n	n
	W_19_3	n	n	x	x	x	n	n	x	n	x	n	x	x	x	n	n	n	x	x	n
TP1	W_20_1	n	n	x	x	n	n	n	n	n	n	x	n	n	n	n	n	n	x	n	n
	W_20_2	n	n	x	x	n	n	n	n	n	n	n	n	n	n	n	n	x	n	n	n
	W_20_3	n	n	n	n	x	n	n	n	x	n	n	n	n	n	n	n	n	n	n	n
TP1	W_21_1	n	n	n	n	n	x	n	n	n	n	n	x	x	n	n	n	n	n	n	n
	W_21_2	n	n	n	n	n	n	x	n	n	n	x	n	n	n	n	n	n	n	x	n
	W_21_3	n	n	n	n	n	x	n	n	n	n	n	n	n	x	n	x	n	n	n	n
TP2	W_22_1	n	n	n	n	n	x	x	n	n	n	n	n	n	n	n	n	n	n	n	n
	W_22_2	x	x	n	n	n	n	n	n	n	n	n	n	x	n	n	x	n	n	n	n
	W_22_3	n	n	x	n	x	n	n	n	n	x	n	n	n	x	n	x	n	n	n	n

Tabelle 46: Testergebnisse - Wachs – Bastelkleber – koop. Opfer - Digitus

TP	Attrappe	Testdurchlauf																			
		1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20
TP1	W_12_1	n	n	n	n	x	x	n	n	x	n	n	n	n	n	x	x	n	n	x	n
	W_12_2	n	n	n	x	x	n	n	n	n	n	x	n	n	x	n	n	n	n	n	n
TP1	W_13_1	n	x	n	x	n	n	n	n	x	n	n	x	n	n	n	n	n	n	x	n
TP2	W_16_1	n	n	n	n	n	n	x	n	n	n	n	n	n	n	n	n	n	n	x	n
	W_16_2	n	n	n	n	n	n	n	n	n	n	n	n	x	n	n	n	n	n	n	n
	W_16_3	n	n	x	x	x	n	n	n	n	n	n	n	x	n	n	x	n	n	n	n
TP1	W_17_1	x	x	n	n	n	n	n	x	n	n	n	n	n	x	n	n	n	x	n	n
	W_17_2	x	n	n	x	n	n	n	n	n	n	n	x	n	n	n	x	n	n	n	x
	W_17_3	n	n	x	x	n	n	n	n	n	n	n	n	x	n	n	n	n	n	n	n
TP2	W_19_1	n	n	n	n	x	x	n	n	n	x	n	n	x	n	x	x	n	n	n	n
	W_19_2	n	n	n	n	n	n	x	n	n	n	x	x	n	x	n	n	n	x	n	n
	W_19_3	n	n	n	n	n	n	n	n	n	n	x	x	x	n	n	n	x	x	n	x
TP1	W_20_1	n	x	n	n	n	n	n	n	n	n	x	n	x	n	n	x	x	x	n	n
	W_20_2	n	n	n	n	n	n	n	n	n	n	n	x	n	n	n	n	n	n	n	n
	W_20_3	n	n	n	n	n	n	n	n	n	n	n	x	n	n	x	n	n	n	n	n
TP1	W_21_1	n	n	n	x	x	n	n	n	n	n	x	n	n	n	n	x	n	n	n	x
	W_21_2	n	n	x	n	n	n	x	x	n	x	n	n	n	n	x	n	n	n	n	n
	W_21_3	x	x	n	x	x	n	n	n	n	n	n	n	n	n	x	n	x	n	n	x
TP2	W_22_1	n	n	x	n	n	n	x	n	n	x	n	x	n	n	n	x	x	n	n	n
	W_22_2	n	n	n	n	n	n	x	n	x	x	x	x	n	n	n	n	n	n	n	n
	W_22_3	x	n	x	n	x	n	n	x	x	n	n	n	x	n	n	x	n	n	x	n
TP2 [20]	W_23_1	n	n	n	n	n	x	x	x	x	x	n	n	n	x	x	n	n	n	n	n
	W_23_2	n	n	n	n	n	n	n	x	x	n	n	n	n	n	n	x	x	n	n	n
	W_23_3	n	n	n	x	x	x	x	n	n	n	x	n	n	n	n	n	n	n	n	n
TP1 [21]	W_24_1	n	n	x	n	x	n	n	n	n	n	n	n	n	x	x	x	x	n	n	n
	W_24_2	n	n	n	n	x	n	x	n	n	n	n	n	x	x	x	n	n	n	n	n
	W_24_3	n	n	x	n	n	n	n	n	n	n	n	n	x	n	n	n	n	n	n	n
TP2 [22]	W_25_1	n	n	x	n	n	n	x	n	n	x	x	n	n	n	x	x	n	n	n	n
	W_25_2	n	x	n	x	x	n	n	n	n	x	n	n	n	n	n	x	n	n	n	n
	W_25_3	n	n	n	n	x	n	x	n	n	n	n	n	x	n	n	n	x	n	n	n
TP2 [23]	W_26_1	n	x	n	n	n	n	n	n	n	n	n	n	n	x	n	n	n	n	n	x
	W_26_2	x	x	x	n	n	x	x	n	n	n	x	x	n	n	n	n	n	n	x	x
	W_26_3	n	n	n	n	n	n	n	n	n	n	n	n	n	x	x	n	n	n	n	n

[20] Als Ersatz für kaputte Vorlage Wachs3
[21] Als Ersatz für kaputte Vorlage Wachs8
[22] Als Ersatz für kaputte Vorlage Wachs15
[23] Als Ersatz für kaputte Vorlage Wachs18

Tabelle 47: Testergebnisse - Wachs – Silikon – koop. Opfer - Digitus

TP	Attrappe	Testdurchlauf																			
		1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20
TP2	W_16_1	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n	x	n	n	n	n
	W_16_2	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n	x	n	n	n	n
TP1	W_17_1	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n
	W_17_2	n	n	n	n	n	n	n	n	n	n	x	n	n	n	x	n	n	n	n	n
	W_17_3	n	n	x	x	n	n	n	n	n	n	n	n	n	n	n	n	n	x	n	n
TP2	W_19_1	n	n	n	n	n	n	n	n	x	x	x	n	n	n	n	n	n	x	n	n
	W_19_2	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n	x	n	n	n	x
TP1	W_20_1	n	n	n	n	n	n	n	n	n	n	n	x	n	n	x	n	n	n	n	n
	W_20_2	n	n	n	n	n	n	n	n	n	n	n	n	x	n	n	n	n	n	n	n
	W_20_3	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n
TP1	W_21_1	n	n	n	n	n	n	n	x	n	x	x	n	n	n	n	n	x	x	n	n
	W_21_2	n	n	n	n	n	n	n	n	x	n	n	n	n	n	n	n	x	n	n	n
	W_21_3	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n
TP2	W_22_1	n	n	n	n	n	n	n	x	n	n	n	n	n	x	n	n	n	n	n	n
	W_22_2	n	n	n	n	x	x	n	n	x	n	n	n	n	n	n	n	n	n	n	n
	W_22_3	n	n	n	x	n	x	x	n	n	n	n	n	n	n	n	n	n	n	n	n
TP2	W_23_1	n	n	n	n	n	n	n	n	n	n	n	n	x	n	n	n	x	n	x	n
	W_23_2	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n	x	n	n	n	n
	W_23_3	n	n	n	x	n	n	n	n	n	n	n	n	n	n	n	x	n	n	n	n
TP1	W_24_1	n	n	n	n	n	n	x	n	n	n	n	x	n	n	n	n	n	n	n	n
	W_24_2	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n
	W_24_3	n	n	n	n	n	n	x	n	n	n	n	n	n	x	n	n	n	n	n	n
TP2	W_25_1	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n
	W_25_2	n	n	n	n	n	n	x	n	n	n	n	x	n	n	n	n	n	n	n	n
	W_25_3	n	n	n	n	n	n	n	n	n	n	x	n	n	n	n	n	n	n	n	n
TP2	W_26_1	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n
	W_26_2	n	n	x	n	n	x	n	n	x	x	n	n	n	n	n	n	n	n	n	n
	W_26_3	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n
TP1[24]	W_27_1	n	n	n	n	n	n	n	n	n	x	x	n	x	x	n	x	n	n	n	n
	W_27_2	n	n	n	n	x	x	n	n	n	n	n	n	n	n	n	x	n	n	x	n
	W_27_3	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n	x	n	n	n
TP1[25]	W_28_1	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n	x	n	n	n
	W_28_2	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n
	W_28_3	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n	x	n	n	n

[24] Als Ersatz für kaputte Vorlage Wachs12
[25] Als Ersatz für kaputte Vorlage Wachs13

Tabelle 48: Testergebnisse - Wachs – Gelatine – koop. Opfer - Digitus

TP	Attrappe	Testdurchlauf																			
		1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20
TP1	W_17_1	x	x	x	n	n	n	n	n	n	n	n	n	x	n	n	n	n	n	n	n
	W_17_2	n	n	n	x	x	x	n	n	n	n	n	n	x	n	n	n	n	n	n	n
	W_17_3	n	n	n	x	n	n	n	n	n	n	x	n	x	x	n	n	n	n	x	n
TP1	W_20_1	n	n	n	n	n	x	n	n	n	x	n	n	n	n	n	x	n	n	n	n
	W_20_2	n	n	n	n	n	n	n	n	x	n	x	n	n	x	n	n	n	n	n	n
	W_20_3	n	n	n	n	n	n	n	x	n	n	n	n	n	n	n	n	n	n	x	n
TP1	W_21_1	n	n	n	n	n	x	n	n	n	n	n	n	n	x	n	n	n	n	n	x
	W_21_2	n	n	n	n	n	n	n	n	n	x	x	n	x	n	n	n	n	n	x	n
TP2	W_22_1	n	n	n	n	n	n	n	n	x	n	n	n	n	x	n	n	n	n	n	n
	W_22_2	n	x	x	x	n	n	n	n	n	n	n	n	n	n	n	n	n	x	x	n
	W_22_3	n	n	n	n	x	n	n	n	x	x	n	n	n	n	x	x	x	n	x	n
TP2	W_23_1	n	n	x	x	n	n	x	n	n	n	n	x	n	n	x	n	n	n	n	x
	W_23_2	n	n	n	n	n	n	n	n	x	x	n	n	n	n	n	x	n	x	n	n
	W_23_3	n	n	n	n	x	n	n	n	n	n	n	n	x	n	n	n	n	n	n	n
TP1	W_24_1	x	n	n	n	n	n	n	n	n	n	x	n	n	n	x	n	n	x	x	n
	W_24_2	n	n	n	n	n	n	n	n	x	n	n	n	n	n	n	x	n	n	n	n
	W_24_3	n	n	n	n	x	n	n	n	n	n	x	n	n	n	n	n	x	n	n	n
TP2	W_25_1	n	n	x	x	n	n	n	x	n	n	n	n	n	n	n	x	x	n	n	n
	W_25_2	n	n	x	n	n	n	x	x	n	n	n	n	x	n	n	n	x	n	n	n
	W_25_3	n	x	n	n	n	n	n	n	x	n	n	n	n	n	x	n	n	n	n	n
TP2	W_26_1	n	n	n	n	x	n	n	x	x	n	x	x	n	n	n	n	n	n	n	n
	W_26_2	n	n	n	n	n	n	x	n	x	x	n	n	n	n	n	n	x	n	n	n
	W_26_3	n	n	x	x	x	n	n	n	x	n	x	x	n	n	n	n	n	x	n	x
TP1	W_27_1	n	n	n	x	n	x	n	n	n	n	n	n	n	n	n	x	n	x	x	x
	W_27_2	n	x	x	n	n	n	x	n	n	n	n	n	x	n	n	x	n	x	n	n
	W_27_3	n	n	n	n	n	n	n	n	n	n	n	x	n	n	n	n	n	n	n	n
TP1	W_28_1	n	n	n	n	n	n	n	n	n	x	n	x	x	n	n	n	n	n	n	n
	W_28_2	n	n	x	n	n	x	n	x	n	n	x	n	n	x	n	n	n	n	x	n
	W_28_3	n	n	n	x	x	n	n	n	n	n	n	x	n	n	x	n	n	x	n	n
TP2 [26]	W_29_1	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n	x	n	n	n
	W_29_2	n	n	n	n	n	n	n	n	n	x	n	n	n	x	n	n	n	n	x	n
	W_29_3	n	n	n	n	n	n	x	n	n	n	n	n	n	x	n	n	n	n	x	n
TP2 [27]	W_30_1	n	n	n	n	n	n	n	x	n	x	n	n	x	n	n	n	n	n	n	n
	W_30_2	n	n	x	n	n	n	n	n	n	n	n	x	x	x	n	n	n	x	n	x
	W_30_3	n	n	x	n	x	x	n	x	x	n	n	n	n	x	n	n	x	x	x	x

[26] Als Ersatz für kaputte Vorlage Wachs16
[27] Als Ersatz für kaputte Vorlage Wachs19

Tabelle 49: Testergebnisse - Platine – Holzleim – unw. Opfer - Digitus

TP	Attrappe	Testdurchlauf																			
		1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20
TP1	Pl_1_1_1	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n
	Pl_1_1_2	n	n	n	n	n	x	n	n	n	x	n	n	n	n	x	n	n	x	n	n
	Pl_1_1_3	n	n	n	n	x	n	x	n	n	n	n	n	x	n	n	n	n	n	n	n
TP1	Pl_1_2_1	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n	x	x
	Pl_1_2_2	n	n	x	n	x	x	n	n	n	n	n	n	n	n	x	n	n	n	n	n
	Pl_1_2_3	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n	x	n	n	n
TP1	Pl_1_3_1	x	n	n	x	n	n	n	n	x	n	n	n	x	n	n	n	x	n	n	x
	Pl_1_3_2	n	n	n	x	n	n	n	n	x	n	n	n	n	n	x	n	n	n	n	n
	Pl_1_3_3	n	n	n	n	n	x	n	n	n	x	n	x	n	n	n	n	x	n	n	n
TP1	Pl_1_4_1	n	n	n	n	x	x	n	n	n	n	n	n	n	n	n	n	x	n	n	n
	Pl_1_4_2	n	n	x	x	n	n	n	n	n	n	n	n	x	n	n	n	n	n	n	n
	Pl_1_4_3	n	n	n	x	n	n	n	x	n	n	n	x	n	n	n	x	n	n	x	n
TP1	Pl_1_5_1	n	x	x	n	n	n	n	n	n	n	x	n	n	n	n	n	n	n	n	x
	Pl_1_5_2	n	n	x	n	x	n	n	n	n	n	n	n	n	x	x	n	x	n	n	n
	Pl_1_5_3	n	n	n	n	n	x	n	n	n	n	x	n	n	x	n	x	n	x	n	n
TP1	Pl_1_6_1	x	n	n	x	x	n	n	n	n	n	x	n	n	n	n	n	x	x	n	x
	Pl_1_6_2	n	n	n	n	n	n	n	n	n	x	n	n	n	x	n	n	n	x	n	n
	Pl_1_6_3	n	n	n	n	x	n	n	n	x	n	n	x	n	n	n	n	n	n	n	x
TP1	Pl_2_1_1	x	n	n	n	n	n	x	x	n	n	n	n	n	n	x	n	n	n	n	n
	Pl_2_1_2	n	n	n	n	x	n	n	n	x	n	n	n	n	x	n	n	x	n	n	n
	Pl_2_1_3	n	n	x	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n
TP1	Pl_2_2_1	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n	x	n	x
	Pl_2_2_2	n	n	n	x	n	n	x	n	x	n	n	n	n	x	n	n	n	x	n	n
	Pl_2_2_3	n	x	n	n	n	n	n	n	x	n	n	x	n	n	n	x	n	n	n	x
TP1	Pl_2_3_1	n	n	n	n	n	x	x	n	n	n	n	n	n	n	n	n	n	n	n	n
	Pl_2_3_2	n	n	n	n	x	n	x	n	n	n	n	n	n	x	n	n	x	n	n	n
	Pl_2_3_3	n	n	n	n	n	n	n	n	n	n	n	n	n	x	n	n	n	n	n	x
TP1	Pl_2_4_1	n	n	n	n	n	x	n	n	n	n	n	n	n	n	n	n	n	n	n	n
	Pl_2_4_2	n	n	n	x	x	n	n	x	n	n	n	n	n	n	x	n	n	n	n	n
	Pl_2_4_3	n	n	n	x	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n
TP1	Pl_2_5_1	x	x	n	n	n	n	n	n	n	n	n	x	n	n	n	n	x	x	n	n
	Pl_2_5_2	n	n	x	n	n	n	x	n	n	n	x	n	n	n	n	x	n	n	x	n
	Pl_2_5_3	n	n	n	n	n	n	x	n	n	n	x	n	x	n	n	n	n	n	n	n
TP1	Pl_2_6_1	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n
	Pl_2_6_2	n	n	n	x	n	n	n	x	n	x	n	n	n	n	x	n	x	n	n	n
	Pl_2_6_3	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n
TP2	Pl_4_1_1	n	x	x	n	n	n	n	n	n	n	n	n	n	n	x	n	n	n	x	n
	Pl_4_1_2	n	n	n	n	x	n	n	n	x	n	n	x	n	n	n	n	n	n	n	n
	Pl_4_1_3	n	n	n	n	x	n	x	n	n	n	n	n	x	n	n	x	n	n	n	n
TP2	Pl_4_2_1	n	n	n	n	n	n	x	x	n	n	n	n	x	n	n	n	n	n	n	n
	Pl_4_2_2	n	n	n	n	x	n	n	n	x	n	n	n	n	n	x	x	n	n	n	n
	Pl_4_2_3	n	n	n	n	n	x	n	n	n	n	n	n	x	n	n	n	n	n	n	n

TP	Attrappe	Testdurchlauf																			
		1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20
TP2	Pl_4_3_1	n	n	n	n	n	n	x	n	n	n	x	n	n	n	n	n	n	x	n	n
	Pl_4_3_2	n	n	n	n	x	n	n	x	n	x	n	n	n	n	n	n	n	n	n	n
	Pl_4_3_3	n	n	n	x	n	x	n	n	n	x	n	n	n	x	n	n	n	n	n	n
TP2	Pl_4_4_1	n	x	n	n	n	n	x	n	n	x	n	x	n	n	x	n	n	n	n	n
	Pl_4_4_2	n	n	n	n	n	n	n	x	n	n	n	n	x	n	x	n	n	n	n	n
	Pl_4_4_3	x	n	n	n	n	n	n	n	n	x	n	n	x	x	n	x	n	n	n	n
TP2	Pl_4_5_1	n	n	n	n	n	n	x	x	n	x	n	n	n	x	x	x	n	n	x	n
	Pl_4_5_2	n	n	n	x	n	n	n	x	n	n	n	x	n	n	n	x	n	n	n	n
	Pl_4_5_3	x	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n
TP2	Pl_4_6_1	n	n	n	n	n	n	n	n	x	n	n	n	n	n	x	n	n	n	n	n
	Pl_4_6_2	x	n	n	n	n	n	n	n	n	x	n	n	n	x	n	x	n	n	n	n
	Pl_4_6_3	n	x	n	n	n	n	n	n	n	n	n	n	n	n	n	n	x	n	n	n
TP2	Pl_4_7_1	n	n	x	n	n	n	x	n	n	n	n	n	n	n	n	n	n	n	n	n
	Pl_4_7_2	n	n	x	n	n	n	n	n	x	n	n	n	x	n	x	n	n	n	x	x
	Pl_4_7_3	n	x	n	n	n	n	n	x	n	n	n	n	n	x	n	n	n	n	n	n
TP2	Pl_4_8_1	n	n	n	n	n	x	n	n	n	n	n	x	n	n	n	n	x	n	n	n
	Pl_4_8_2	n	n	n	n	n	x	n	x	n	n	n	n	n	x	n	n	n	x	n	n
	Pl_4_8_3	n	n	x	n	n	n	n	n	n	n	n	x	n	n	x	n	n	n	n	n
TP2	Pl_4_9_1	n	n	n	n	n	x	n	n	n	x	n	x	x	n	n	n	n	n	n	n
	Pl_4_9_2	n	n	n	n	n	n	x	n	n	n	n	x	n	n	n	n	x	n	n	x
	Pl_4_9_3	n	n	n	n	n	n	n	n	n	x	x	n	n	n	n	n	x	n	n	n
TP2	Pl_4_10_1	n	n	n	n	n	x	x	n	n	n	n	n	n	n	n	n	n	n	n	n
	Pl_4_10_2	n	n	n	n	x	n	n	n	x	n	n	n	n	n	n	x	n	n	x	n
	Pl_4_10_3	x	n	n	x	n	n	n	n	n	n	x	n	n	n	n	n	n	n	n	n
TP2	Pl_5_1_1	n	n	n	x	n	n	n	n	n	n	n	n	n	x	x	n	n	x	n	n
	Pl_5_1_2	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n
	Pl_5_1_3	n	n	n	n	n	n	n	n	n	x	n	n	n	n	n	n	x	n	n	n
TP2	Pl_5_3_1	n	n	n	n	n	n	n	n	x	n	n	n	n	n	x	n	n	n	n	n
	Pl_5_3_2	x	n	x	n	n	n	n	x	n	n	n	n	n	n	n	n	n	n	n	n
	Pl_5_3_3	n	n	n	n	n	n	n	n	x	n	x	n	n	n	x	n	n	n	n	n
TP2	Pl_5_4_1	n	n	x	n	n	n	n	n	n	x	x	n	n	n	n	n	n	x	n	n
	Pl_5_4_2	n	n	n	n	n	n	n	n	x	x	n	n	n	x	n	n	n	n	x	n
	Pl_5_4_3	x	n	n	n	n	x	n	n	x	n	n	x	n	n	n	x	n	n	n	n
TP2	Pl_5_5_1	n	n	n	n	n	n	x	n	n	n	n	n	x	x	n	n	n	n	n	n
	Pl_5_5_2	n	n	n	n	n	n	n	n	n	n	n	n	n	n	x	n	n	n	x	x
	Pl_5_5_3	n	n	n	n	n	n	n	n	n	x	x	n	n	n	n	x	n	n	n	n
TP2	Pl_5_6_1	n	n	n	n	n	x	n	x	n	n	n	n	n	x	n	n	n	n	n	n
	Pl_5_6_2	n	n	n	n	n	n	n	x	n	n	n	n	x	n	n	n	n	n	x	n
	Pl_5_6_3	n	n	n	n	n	n	x	n	n	x	n	n	x	n	n	n	n	n	n	n
TP2	Pl_5_7_1	n	n	n	n	n	x	n	n	x	n	n	x	x	n	n	n	n	n	n	x
	Pl_5_7_2	n	n	n	n	n	n	n	x	n	x	n	n	x	n	n	n	n	x	x	n
	Pl_5_7_3	n	n	n	n	x	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n
TP2	Pl_5_8_1	n	n	n	n	n	n	x	n	x	n	n	n	n	n	n	n	n	n	n	n
	Pl_5_8_2	n	n	n	n	n	n	n	n	x	x	n	n	n	n	n	n	n	n	n	n
	Pl_5_8_3	n	n	n	n	n	n	n	n	x	n	x	n	n	n	n	n	n	n	x	n

TP	Attrappe	Testdurchlauf																			
		1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20
TP1	PI_6_1_1	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n	x	x
TP1	PI_6_2_1	n	n	x	n	n	n	n	n	n	n	n	n	n	x	n	n	n	n	n	n
	PI_6_2_2	n	n	n	n	x	n	x	n	n	n	n	n	n	x	n	n	n	n	x	n
	PI_6_2_3	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n
TP1	PI_6_4_1	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n
TP1	PI_6_5_1	n	n	x	n	x	n	n	n	n	n	n	n	n	x	n	n	n	n	n	x
	PI_6_5_2	n	x	n	n	n	n	x	n	n	x	n	n	n	n	n	n	n	n	n	n
	PI_6_5_3	n	n	n	n	x	n	n	n	x	n	n	x	n	n	n	n	n	n	n	n
TP1	PI_7_1_1	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n
	PI_7_1_2	n	n	n	n	n	n	n	n	n	n	x	n	n	n	n	x	n	x	n	n
	PI_7_1_3	n	n	n	n	x	n	n	n	n	n	n	n	n	n	n	n	x	n	n	n
TP1	PI_7_2_1	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n	x	n
	PI_7_2_2	n	x	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n
	PI_7_2_3	x	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n
TP1	PI_7_3_1	n	n	x	n	n	n	n	x	n	n	n	n	x	n	n	n	x	n	n	n
	PI_7_3_2	n	n	n	n	n	n	n	n	n	n	x	n	n	n	n	n	n	n	n	n
	PI_7_3_3	n	n	n	x	n	n	n	n	x	n	n	n	n	n	n	n	n	n	n	n
TP1	PI_7_4_1	x	n	n	x	x	n	x	n	n	x	n	n	n	x	n	n	x	n	x	n
	PI_7_4_2	n	n	n	n	n	n	x	n	n	x	n	n	n	n	n	n	n	n	n	n
	PI_7_4_3	n	n	x	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n
TP1	PI_7_5_1	n	x	n	n	x	n	n	n	n	n	x	n	n	n	n	x	n	n	n	x
	PI_7_5_2	n	n	n	n	x	n	n	n	n	n	n	x	n	x	n	x	n	n	n	x
	PI_7_5_3	n	n	n	x	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n
TP2	PI_8_1_1	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n
	PI_8_1_2	n	n	n	x	n	n	n	x	n	n	n	n	n	x	n	n	n	n	n	n
	PI_8_1_3	n	n	n	x	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n
TP2	PI_8_2_1	n	n	n	n	x	n	n	n	n	n	n	n	n	n	n	n	n	x	n	n
	PI_8_2_2	n	n	n	n	n	n	x	n	n	n	x	n	n	n	n	n	n	x	n	n
	PI_8_2_3	n	n	n	n	n	n	n	x	n	x	n	n	n	n	x	x	n	n	x	n
TP2	PI_8_3_1	n	n	n	n	n	n	n	n	n	n	x	n	n	x	x	n	n	n	n	n
	PI_8_3_2	x	n	n	n	x	n	n	x	n	n	n	n	x	n	n	n	n	n	n	n
	PI_8_3_3	n	n	n	x	n	x	n	n	n	n	n	n	n	n	n	x	n	n	x	n
TP2	PI_8_4_1	n	n	n	x	n	n	n	x	n	x	n	x	x	n	n	x	n	n	x	n
	PI_8_4_2	n	n	n	x	n	n	n	n	x	n	x	n	n	n	x	n	n	n	n	n
	PI_8_4_3	n	n	n	n	n	n	n	n	n	n	n	n	n	n	x	x	n	x	n	x

Tabelle 50: Testergebnisse - Platine – Bastelkleber – unw. Opfer - Digitus

TP	Attrappe	Testdurchlauf																			
		1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20
TP1	Pl_1_1_1	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n	x
	Pl_1_1_2	n	x	n	n	n	n	x	n	n	n	x	n	n	n	x	n	n	n	n	n
	Pl_1_1_3	n	n	n	n	n	n	n	n	n	x	n	n	n	x	n	n	n	n	n	n
TP1	Pl_1_2_1	x	n	n	n	x	n	n	x	x	n	x	x	n	n	n	n	n	n	n	x
	Pl_1_2_2	x	n	n	n	n	x	n	n	n	n	n	n	n	n	n	n	n	x	n	n
	Pl_1_2_3	n	n	n	n	n	n	n	n	n	n	n	n	n	x	n	n	x	n	n	n
TP1	Pl_1_3_1	n	n	n	n	n	n	x	x	n	n	n	x	n	n	n	n	x	n	x	n
	Pl_1_3_2	n	n	n	n	x	n	n	x	x	n	n	n	n	n	n	n	n	n	n	n
	Pl_1_3_3	n	n	n	n	n	x	n	n	n	x	x	n	n	n	n	n	n	n	n	n
TP1	Pl_1_4_1	n	n	n	n	n	n	n	x	n	x	n	x	n	n	n	n	x	n	n	n
	Pl_1_4_2	n	n	n	x	x	x	n	n	n	n	n	x	n	n	x	n	n	n	n	n
	Pl_1_4_3	n	n	n	n	n	n	n	n	n	n	x	n	n	n	n	n	n	n	n	n
TP1	Pl_1_5_1	n	n	n	n	n	n	n	n	n	n	n	x	n	x	n	n	n	n	n	n
	Pl_1_5_2	n	n	n	n	n	n	n	n	n	x	n	x	x	n	n	x	n	n	n	n
	Pl_1_5_3	n	n	n	x	n	x	x	n	n	n	n	n	n	n	n	n	x	n	n	n
TP1	Pl_1_6_1	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n
	Pl_1_6_2	n	n	n	n	x	n	n	n	n	n	n	n	n	n	n	n	x	n	n	n
	Pl_1_6_3	n	n	n	n	x	x	n	n	n	n	n	x	n	n	n	n	x	n	n	n
TP1	Pl_2_1_1	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n
	Pl_2_1_2	n	n	n	x	n	n	n	n	n	n	x	n	n	n	n	n	n	n	n	n
	Pl_2_1_3	n	n	n	n	n	x	n	n	n	x	n	n	n	n	n	n	x	n	n	x
TP1	Pl_2_2_1	n	n	n	n	n	n	n	n	n	n	n	x	x	n	n	n	x	n	n	n
	Pl_2_2_2	n	n	x	n	x	n	n	n	n	n	x	n	n	n	x	n	n	n	x	n
	Pl_2_2_3	n	n	n	n	n	n	n	n	x	n	n	n	n	x	x	n	x	n	n	x
TP1	Pl_2_3_1	n	n	n	n	n	n	x	n	n	x	n	n	n	x	n	x	n	n	x	n
	Pl_2_3_2	n	n	x	x	n	x	n	n	n	n	n	x	n	n	n	x	n	n	x	n
	Pl_2_3_3	n	n	n	n	n	x	n	n	n	n	n	n	n	n	n	n	n	n	x	n
TP1	Pl_2_4_1	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n	x	n	n	n
	Pl_2_4_2	n	x	n	n	n	n	n	n	x	n	n	n	x	n	n	n	x	n	n	n
	Pl_2_4_3	n	x	x	n	n	n	n	n	x	n	n	n	n	n	n	x	n	n	n	x
TP1	Pl_2_5_1	n	n	n	x	n	x	n	n	n	n	x	n	n	n	n	n	x	n	x	n
	Pl_2_5_2	n	n	n	x	x	n	n	n	x	n	n	n	n	n	n	n	n	n	n	n
	Pl_2_5_3	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n
TP1	Pl_2_6_1	n	n	n	n	n	n	n	n	n	x	x	n	n	n	n	x	x	n	n	n
	Pl_2_6_2	n	n	x	n	n	n	x	n	n	n	x	n	n	x	n	n	n	x	n	n
	Pl_2_6_3	n	n	n	n	n	n	n	n	x	n	x	n	n	n	x	n	n	x	n	n
TP2	Pl_4_1_1	n	n	n	n	n	n	n	n	n	x	x	n	x	n	n	n	x	n	n	n
	Pl_4_1_2	n	n	n	x	n	x	n	n	n	n	n	n	x	x	n	n	n	n	n	n
	Pl_4_1_3	n	n	n	n	x	n	n	n	n	n	n	x	n	n	n	n	n	n	x	n
TP2	Pl_4_2_1	n	n	n	n	n	x	n	n	n	x	n	n	x	n	n	n	x	n	n	n
	Pl_4_2_2	n	n	n	n	n	x	n	n	n	n	n	x	x	n	n	n	x	n	n	n
	Pl_4_2_3	n	n	n	n	n	x	n	x	n	n	n	x	n	n	n	x	n	x	n	n

TP	Attrappe	Testdurchlauf																			
		1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20
TP2	PI_4_3_1	n	n	n	n	n	n	n	n	n	x	n	n	x	x	n	n	n	n	n	x
	PI_4_3_2	n	n	n	x	n	x	n	n	n	n	x	n	n	n	n	x	x	n	n	x
	PI_4_3_3	x	n	x	n	n	n	n	n	n	n	n	x	n	n	n	n	n	n	n	n
TP2	PI_4_4_1	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n
	PI_4_4_2	n	n	n	n	x	n	n	n	n	n	x	n	x	x	n	n	n	n	n	n
	PI_4_4_3	n	x	n	n	n	n	n	n	x	x	n	n	n	n	x	x	n	n	x	n
TP2	PI_4_5_1	n	n	n	n	x	x	n	n	n	n	n	n	n	n	n	x	n	x	n	x
	PI_4_5_2	n	n	n	x	n	n	n	x	n	n	n	n	n	n	n	n	n	x	x	x
	PI_4_5_3	n	n	n	n	x	n	n	n	x	n	x	x	n	x	n	n	x	n	n	n
TP2	PI_4_6_1	n	n	n	n	n	n	n	n	x	x	n	x	n	n	n	x	n	x	n	n
	PI_4_6_2	n	n	n	n	n	n	x	n	x	n	n	x	n	n	x	n	n	n	n	x
	PI_4_6_3	n	n	n	n	n	n	x	x	n	n	n	n	x	n	x	n	n	n	n	n
TP2	PI_4_7_1	n	n	x	x	n	n	n	n	x	x	n	n	n	n	x	x	n	n	x	n
	PI_4_7_2	n	n	n	n	n	x	n	n	x	x	n	x	n	n	x	n	x	x	n	n
	PI_4_7_3	n	n	n	x	x	n	n	n	n	x	n	n	n	n	n	n	n	n	n	n
TP2	PI_4_8_1	n	n	n	n	n	n	n	n	n	n	n	n	n	n	x	n	n	x	n	n
	PI_4_8_2	n	n	n	n	n	x	x	x	n	n	n	n	n	x	n	n	n	n	n	n
	PI_4_8_3	n	n	n	n	n	n	n	n	n	n	n	n	x	x	n	n	n	n	n	n
TP2	PI_4_9_1	n	n	n	n	n	x	n	x	n	n	n	x	x	n	n	n	x	n	n	n
	PI_4_9_2	n	n	n	n	x	n	n	n	n	n	n	n	x	n	x	x	n	n	n	n
	PI_4_9_3	n	n	n	x	n	n	x	n	n	n	n	x	x	n	n	n	n	n	n	n
TP2	PI_4_10_1	n	n	n	n	n	n	n	x	x	n	n	n	n	n	n	n	n	n	n	n
	PI_4_10_2	n	n	n	n	n	x	x	x	x	n	n	n	n	n	n	n	n	n	n	n
	PI_4_10_3	n	n	n	n	x	n	n	x	n	n	n	n	n	n	n	n	n	n	n	n
TP2	PI_5_1_1	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n	x	x	n	x
TP2	PI_5_3_1	n	n	n	n	n	n	n	x	x	x	n	n	n	n	x	n	n	n	n	n
	PI_5_3_2	n	n	n	n	n	x	n	n	n	n	x	x	n	n	x	n	n	n	n	n
	PI_5_3_3	n	n	x	x	n	n	n	n	n	n	n	n	n	n	n	x	x	n	n	n
TP2	PI_5_4_1	n	n	n	n	n	x	n	n	n	x	x	x	n	n	n	n	n	n	x	n
	PI_5_4_2	n	n	n	n	x	x	n	n	x	n	n	x	x	n	x	n	n	n	n	n
	PI_5_4_3	n	n	n	n	x	n	n	n	x	n	n	n	x	n	n	n	x	n	n	n
TP2	PI_5_5_1	n	n	n	x	n	n	n	x	x	n	n	n	n	x	n	x	n	n	n	n
	PI_5_5_2	n	n	n	x	n	n	n	n	n	x	x	n	n	n	n	n	x	n	n	n
	PI_5_5_3	n	n	n	n	x	n	x	x	n	n	n	x	n	n	n	x	x	n	n	x
TP2	PI_5_6_1	n	n	n	n	n	n	x	x	n	n	n	n	n	n	n	n	n	x	x	n
	PI_5_6_2	n	n	n	n	n	n	n	x	n	n	x	n	n	n	n	n	x	n	n	n
	PI_5_6_3	n	n	n	n	n	n	x	x	n	n	n	n	n	x	x	n	n	x	n	n
TP2	PI_5_7_1	n	n	n	n	x	x	n	x	x	n	n	n	n	n	n	x	n	n	x	n
	PI_5_7_2	n	n	n	x	x	n	n	n	x	n	n	n	n	n	n	n	n	n	n	n
	PI_5_7_3	n	n	n	n	x	n	n	n	n	x	x	n	n	x	x	n	n	n	x	x
TP2	PI_5_8_1	n	n	n	n	n	n	n	n	n	n	n	x	x	x	n	n	n	x	n	n
	PI_5_8_2	n	n	x	n	n	n	n	n	n	n	n	n	x	n	n	n	n	n	n	x
	PI_5_8_3	x	n	n	n	n	n	x	n	n	n	x	n	n	n	x	n	x	n	n	n

TP	Attrappe	Testdurchlauf																			
		1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20
TP1	Pl_6_2_1	n	n	n	n	n	x	n	n	x	n	n	x	n	n	n	n	x	n	n	n
	Pl_6_2_2	n	n	n	n	n	n	n	x	x	n	n	n	x	n	n	x	n	n	n	x
	Pl_6_2_3	n	n	n	n	n	n	n	n	n	n	n	n	x	n	n	n	n	n	n	n
TP1	Pl_6_5_1	n	n	n	n	n	n	n	n	x	n	n	n	n	n	n	x	x	x	n	n
	Pl_6_5_2	n	n	n	n	x	n	n	n	n	n	x	x	n	n	n	n	x	n	n	n
	Pl_6_5_3	n	n	n	x	n	n	x	x	n	n	n	n	x	x	n	n	n	n	n	n
TP1	Pl_7_1_1	n	n	n	n	x	x	n	n	n	n	x	n	n	n	n	n	n	n	n	n
	Pl_7_1_2	n	n	x	n	n	n	n	n	n	n	x	n	n	n	n	n	x	n	n	x
	Pl_7_1_3	n	n	n	n	n	n	n	n	n	n	x	n	n	x	n	n	n	n	n	n
TP1	Pl_7_2_1	n	n	n	n	n	n	n	n	n	x	n	n	n	x	x	n	n	n	x	n
	Pl_7_2_2	n	n	n	x	n	n	n	n	n	n	x	n	n	n	x	n	n	x	n	n
	Pl_7_2_3	n	n	n	n	x	n	n	n	n	x	n	x	n	n	n	n	x	n	n	x
TP1	Pl_7_3_1	n	n	n	x	n	n	x	x	n	n	n	n	n	n	x	n	n	n	n	x
	Pl_7_3_2	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n	x	n	n	n	x
	Pl_7_3_3	n	n	n	n	n	n	x	n	x	x	n	n	n	n	n	n	n	n	n	x
TP1	Pl_7_4_1	n	n	x	n	n	n	n	n	n	n	x	x	n	x	n	n	n	n	n	x
	Pl_7_4_2	x	n	n	x	n	n	n	n	x	n	n	n	x	n	n	n	n	n	n	n
	Pl_7_4_3	x	n	n	n	n	n	n	n	n	x	n	n	x	x	n	n	n	x	n	n
TP1	Pl_7_5_1	n	n	n	n	n	x	x	n	n	n	n	n	x	x	n	n	n	x	n	n
	Pl_7_5_2	n	n	n	x	n	n	n	x	n	x	x	n	n	n	n	n	n	x	x	n
	Pl_7_5_3	n	n	n	n	x	n	n	n	n	x	x	n	n	n	n	n	n	n	n	n
TP2	Pl_8_1_1	n	n	n	n	n	n	n	n	n	n	n	x	n	n	x	x	x	n	n	n
	Pl_8_1_2	n	n	n	n	x	n	x	n	n	n	n	n	n	n	n	x	n	x	n	n
	Pl_8_1_3	n	n	n	x	n	n	x	n	n	n	n	n	n	n	n	n	n	n	n	n
TP2	Pl_8_2_1	n	n	n	n	n	n	n	n	n	x	n	x	x	n	n	n	n	x	x	n
	Pl_8_2_2	n	n	n	n	x	x	n	n	n	n	x	n	n	n	n	n	x	n	n	n
	Pl_8_2_3	x	x	x	x	n	n	n	x	n	n	n	n	x	n	x	n	n	x	n	n
TP2	Pl_8_3_1	n	n	x	n	n	n	x	n	n	n	n	n	n	x	n	n	x	n	x	n
	Pl_8_3_2	n	n	n	x	n	x	n	n	x	n	x	n	n	x	x	n	n	n	n	n
	Pl_8_3_3	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n
TP2	Pl_8_4_1	n	n	n	n	n	x	x	n	n	n	x	n	n	n	x	n	n	n	n	x
	Pl_8_4_2	n	n	n	n	x	n	n	n	x	n	n	n	x	n	n	n	n	n	x	n
	Pl_8_4_3	n	n	n	n	x	n	n	n	n	x	n	n	x	n	x	n	n	n	x	n

Tabelle 51: Testergebnisse - Platine – Silikon – unw. Opfer - Digitus

TP	Attrappe	Testdurchlauf																			
		1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20
TP1	Pl_1_1_1	n	n	n	n	n	n	n	n	n	n	n	n	n	n	x	n	n	n	n	n
	Pl_1_1_2	n	n	n	n	n	n	n	n	x	n	n	x	n	x	n	n	n	n	n	n
	Pl_1_1_3	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n	x	n	n	n	n
TP1	Pl_1_2_1	n	n	n	n	n	x	x	n	n	x	n	n	n	n	n	n	n	n	n	n
	Pl_1_2_2	n	n	n	n	x	n	n	n	x	n	n	n	n	x	n	x	n	x	n	x
	Pl_1_2_3	n	n	n	n	n	n	n	n	x	x	n	n	n	n	x	n	n	n	n	n
TP1	Pl_1_3_1	n	n	n	n	n	n	x	x	n	n	n	n	n	n	n	n	n	x	n	n
	Pl_1_3_2	n	n	n	n	n	n	n	x	n	n	x	n	x	n	n	n	n	n	n	n
	Pl_1_3_3	n	n	n	n	n	n	x	n	n	n	x	n	n	n	n	n	n	n	n	n
TP1	Pl_1_4_1	n	n	n	n	n	x	n	n	n	n	n	n	x	n	n	n	n	n	n	n
	Pl_1_4_2	n	n	n	n	n	n	x	n	x	n	n	x	x	n	n	n	n	n	n	x
	Pl_1_4_3	n	n	n	n	x	n	n	n	n	n	n	n	n	n	n	n	n	x	n	n
TP1	Pl_1_5_1	n	n	n	n	n	x	n	n	x	n	n	n	n	n	n	n	n	n	n	n
	Pl_1_5_2	n	n	n	n	n	n	n	n	n	n	n	n	n	n	x	x	n	n	n	n
	Pl_1_5_3	n	n	n	n	x	n	n	n	n	n	x	x	n	x	n	n	n	n	n	n
TP1	Pl_1_6_1	n	n	n	n	n	x	n	n	n	n	n	n	n	x	n	n	x	n	n	n
	Pl_1_6_2	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n	x	x	n	x
	Pl_1_6_3	n	n	n	n	n	n	n	n	n	x	n	x	n	n	n	n	n	x	n	n
TP1	Pl_2_1_1	n	n	n	n	n	n	n	x	n	n	n	n	n	n	n	n	n	n	x	n
	Pl_2_1_2	n	n	n	n	n	n	n	x	n	n	n	x	x	n	x	n	n	n	n	x
	Pl_2_1_3	n	n	n	n	n	n	n	n	n	n	x	n	n	n	n	x	n	n	n	n
TP1	Pl_2_2_1	n	n	n	n	n	n	n	n	n	n	n	n	n	x	n	n	x	n	n	n
	Pl_2_2_2	n	n	n	n	n	n	n	x	n	x	n	n	n	n	n	n	x	n	n	n
	Pl_2_2_3	n	n	n	n	n	n	n	n	n	n	n	x	n	n	n	x	n	n	n	n
TP1	Pl_2_3_1	n	x	n	x	n	n	n	x	n	n	x	n	n	n	n	n	n	n	n	n
	Pl_2_3_2	n	n	n	n	n	x	x	n	n	n	x	n	n	n	n	x	n	n	n	n
	Pl_2_3_3	n	n	n	n	x	n	n	x	x	n	n	n	n	n	n	n	n	n	n	n
TP1	Pl_2_4_1	n	n	x	x	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n
	Pl_2_4_2	n	n	n	n	n	n	n	n	n	x	n	n	n	n	n	n	x	n	n	n
	Pl_2_4_3	n	n	n	n	n	n	n	n	n	x	n	n	n	n	n	n	n	n	x	n
TP1	Pl_2_5_1	n	x	n	n	n	n	n	x	n	n	n	n	n	n	n	n	n	n	n	n
	Pl_2_5_2	n	n	n	n	n	n	n	n	n	n	x	n	n	n	n	n	n	n	n	n
	Pl_2_5_3	n	n	n	n	n	n	n	x	n	n	n	x	n	n	n	n	x	n	n	n
TP1	Pl_2_6_1	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n
	Pl_2_6_2	n	n	n	n	n	x	n	n	n	x	n	x	n	n	n	x	n	n	x	n
	Pl_2_6_3	n	n	n	n	n	n	x	x	n	n	n	x	n	n	x	n	n	n	n	n
TP2	Pl_4_1_1	n	n	n	n	n	n	x	n	x	n	x	n	n	n	x	n	n	x	n	n
	Pl_4_1_2	n	n	n	x	n	x	n	n	n	n	n	n	n	n	n	n	n	x	n	n
	Pl_4_1_3	n	n	x	n	n	x	n	n	n	n	n	n	n	n	n	n	n	x	n	n
TP2	Pl_4_2_1	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n	x	n
	Pl_4_2_2	n	n	n	n	n	n	n	n	x	n	n	n	n	n	n	n	n	x	n	n
	Pl_4_2_3	n	n	n	n	n	n	n	n	n	n	x	n	n	n	n	n	n	n	n	n

TP	Attrappe	Testdurchlauf																			
		1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20
TP2	PI_4_3_1	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n	x	n	n
	PI_4_3_2	n	n	n	n	n	x	n	n	n	n	n	n	n	n	n	n	n	x	n	n
	PI_4_3_3	n	n	x	n	n	n	n	x	n	n	n	n	n	n	n	n	n	n	n	n
TP2	PI_4_4_1	n	n	n	n	n	x	n	n	n	n	n	n	n	n	n	n	x	n	n	n
	PI_4_4_2	n	n	n	n	n	n	n	n	n	n	x	n	n	n	n	n	n	n	n	n
	PI_4_4_3	n	n	n	n	n	x	n	n	n	x	n	n	n	n	n	n	x	n	n	n
TP2	PI_4_5_1	n	n	n	n	n	n	n	x	n	n	n	n	n	n	n	n	n	n	n	x
	PI_4_5_2	n	x	n	n	n	n	n	n	x	n	x	n	n	x	x	n	n	n	n	n
	PI_4_5_3	n	n	n	n	x	n	n	n	n	n	x	n	n	x	n	n	n	n	n	n
TP2	PI_4_6_1	n	n	x	n	n	n	n	n	n	n	n	n	x	n	n	n	n	n	n	n
	PI_4_6_2	n	n	x	n	x	n	n	x	n	n	n	n	n	n	n	n	n	n	x	n
	PI_4_6_3	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n
TP2	PI_4_7_1	n	n	n	n	n	n	x	n	n	n	n	n	n	n	n	n	n	n	n	n
	PI_4_7_2	n	n	n	n	n	n	n	n	n	n	n	x	n	x	n	n	n	n	n	n
	PI_4_7_3	n	n	n	n	n	n	n	n	n	n	n	x	x	n	n	n	n	n	n	n
TP2	PI_4_8_1	n	n	n	n	x	x	n	x	n	n	n	n	n	n	n	n	n	n	n	n
	PI_4_8_2	n	n	n	x	n	n	n	n	x	n	n	n	n	n	n	n	n	n	n	n
	PI_4_8_3	n	x	n	n	n	n	x	n	n	n	n	n	n	n	n	n	n	n	n	n
TP2	PI_4_9_1	n	n	n	n	n	n	x	n	n	n	n	n	n	x	n	n	x	x	x	n
	PI_4_9_2	n	n	n	n	x	n	x	n	n	x	n	n	n	n	n	n	n	x	n	n
	PI_4_9_3	n	n	n	n	n	n	x	n	x	n	n	n	n	n	n	x	n	n	n	n
TP2	PI_4_10_1	n	n	n	x	n	n	n	n	n	x	n	x	x	n	n	x	n	n	n	n
	PI_4_10_2	n	n	x	n	x	n	n	n	n	x	n	x	n	n	n	n	n	n	n	n
	PI_4_10_3	n	n	n	n	n	n	n	x	n	n	n	x	n	n	n	n	n	n	n	n
TP2	PI_5_3_1	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n	x	n	n	n
	PI_5_3_2	n	n	n	n	x	n	n	n	n	n	x	n	n	x	n	x	n	x	n	n
	PI_5_3_3	n	n	n	n	n	n	x	n	n	n	n	n	n	n	n	n	n	x	n	n
TP2	PI_5_4_1	n	n	n	x	n	n	x	n	n	n	n	n	x	n	x	x	n	n	x	n
	PI_5_4_2	n	n	n	n	n	n	n	n	n	n	x	n	x	n	n	x	n	n	n	n
	PI_5_4_3	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n	x	n	n	x	x
TP2	PI_5_5_1	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n
	PI_5_5_2	n	x	n	x	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n
	PI_5_5_3	n	n	x	n	n	x	n	n	n	n	n	x	n	n	n	n	x	n	n	n
TP2	PI_5_6_1	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n
	PI_5_6_2	n	n	x	n	n	n	x	x	n	x	x	n	n	x	n	n	n	n	x	n
	PI_5_6_3	n	n	n	n	n	x	n	n	n	n	n	n	n	n	n	n	n	n	n	n
TP2	PI_5_7_1	n	n	n	n	n	n	n	n	n	x	n	x	n	n	n	n	x	n	n	n
	PI_5_7_2	n	n	n	n	n	n	n	n	x	n	n	n	x	n	n	n	x	n	n	n
	PI_5_7_3	x	n	n	n	n	n	n	x	n	n	x	n	n	n	n	n	x	n	n	n
TP2	PI_5_8_1	n	n	n	x	n	n	n	n	x	n	n	n	n	n	n	n	n	n	n	n
	PI_5_8_2	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n
	PI_5_8_3	n	n	n	n	n	x	n	n	n	n	n	n	n	n	n	x	n	n	n	n

TP	Attrappe	Testdurchlauf																			
		1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20
TP1	PI_6_2_1	n	n	n	n	n	n	n	x	x	n	n	n	x	n	n	n	x	n	n	n
	PI_6_2_2	n	n	n	n	x	n	x	n	n	n	n	n	n	n	x	n	n	x	n	n
	PI_6_2_3	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n	x	x	n	n
TP1	PI_6_5_1	x	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n
	PI_6_5_2	n	n	n	n	n	x	n	n	x	n	n	n	n	n	n	x	n	n	n	n
	PI_6_5_3	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n
TP1	PI_7_1_1	x	x	n	x	n	n	n	n	n	x	n	n	x	n	x	x	x	n	n	n
	PI_7_1_2	n	n	n	n	x	x	n	n	n	x	n	x	x	n	n	n	n	x	n	n
	PI_7_1_3	n	n	n	n	n	n	n	n	n	n	n	x	n	n	x	n	n	n	x	x
TP1	PI_7_2_1	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n	x	n	n
	PI_7_2_2	n	n	n	n	x	n	n	n	n	x	x	n	n	n	n	x	n	n	n	n
	PI_7_2_3	n	n	n	x	x	n	n	n	n	n	n	x	n	n	n	x	n	n	x	n
TP1	PI_7_3_1	n	n	x	n	n	n	n	n	x	n	n	n	n	n	n	n	n	n	n	n
	PI_7_3_2	n	n	n	n	n	n	n	n	x	n	n	n	n	x	n	n	n	n	n	n
	PI_7_3_3	n	n	n	n	n	n	n	n	n	x	n	x	n	n	n	x	n	n	n	x
TP1	PI_7_4_1	n	n	x	n	n	n	n	x	n	n	n	n	x	n	x	n	n	x	n	n
	PI_7_4_2	n	n	n	n	n	n	n	n	n	n	x	n	n	x	n	n	n	n	n	n
	PI_7_4_3	n	n	n	n	n	n	n	n	x	n	n	x	n	n	n	n	n	n	x	n
TP1	PI_7_5_1	n	n	x	n	n	n	n	n	n	n	x	x	n	n	n	n	n	n	n	n
	PI_7_5_2	n	n	n	n	x	n	n	n	n	n	x	n	n	n	n	x	n	n	n	n
	PI_7_5_3	n	n	n	n	n	n	n	n	n	n	n	n	x	n	x	n	x	n	n	n
TP2	PI_8_1_1	n	x	x	x	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n
	PI_8_1_2	n	n	n	n	n	n	n	x	n	n	n	n	n	x	n	x	n	n	n	n
	PI_8_1_3	n	n	n	n	n	n	n	n	n	x	n	n	x	n	n	n	x	n	n	n
TP2	PI_8_2_1	n	n	n	n	n	n	n	n	n	x	n	n	n	n	n	n	n	n	x	n
	PI_8_2_2	n	n	n	n	n	n	n	n	x	n	n	n	n	n	n	n	n	n	n	n
	PI_8_2_3	n	n	n	n	x	n	n	n	n	n	n	x	n	n	n	n	n	n	n	n
TP2	PI_8_3_1	n	n	n	x	n	n	n	n	n	n	n	n	n	x	n	n	n	n	x	n
	PI_8_3_2	n	n	x	n	n	n	n	x	x	n	n	n	x	x	n	n	n	n	x	n
	PI_8_3_3	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n
TP2	PI_8_4_1	n	n	n	n	n	x	n	n	x	n	n	n	x	n	n	n	n	x	n	n
	PI_8_4_2	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n
	PI_8_4_3	n	n	n	n	n	n	n	n	n	n	n	x	n	n	n	n	n	n	n	n

Tabelle 52: Testergebnisse - Platine – Gelatine – unw. Opfer - Digitus

TP	Attrappe	Testdurchlauf																			
		1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20
TP1	Pl_1_1_1	x	x	x	n	n	n	n	n	n	x	n	n	n	n	n	n	n	n	n	n
	Pl_1_1_2	n	n	x	n	n	n	n	n	n	n	n	x	x	n	x	n	x	n	n	n
	Pl_1_1_3	n	n	n	n	n	n	n	n	x	n	x	n	x	n	n	n	n	n	n	n
TP1	Pl_1_2_1	n	n	n	n	n	n	x	x	n	n	x	n	n	n	n	n	n	n	n	n
	Pl_1_2_2	n	n	n	x	n	n	n	n	n	n	x	x	n	n	n	n	n	n	n	n
	Pl_1_2_3	n	n	n	x	n	n	n	n	n	n	n	n	n	n	n	x	n	n	n	n
TP1	Pl_1_3_1	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n
	Pl_1_3_2	n	n	n	n	n	x	n	n	x	n	n	n	x	x	n	n	n	n	n	n
	Pl_1_3_3	n	n	n	x	n	n	n	n	n	x	x	n	n	n	x	n	n	n	x	n
TP1	Pl_1_4_1	n	n	n	n	x	x	n	n	n	n	n	x	n	n	x	x	n	n	n	n
	Pl_1_4_2	n	n	n	n	n	n	n	n	n	n	n	x	n	n	n	n	n	n	n	n
	Pl_1_4_3	n	n	x	x	x	x	n	n	x	x	x	n	n	n	x	n	n	x	n	n
TP1	Pl_1_5_1	n	n	n	x	x	n	n	n	n	x	n	n	n	x	x	n	n	n	n	n
	Pl_1_5_2	n	n	n	n	n	n	n	n	n	n	x	n	x	n	n	x	n	n	n	n
	Pl_1_5_3	n	n	n	n	n	x	n	n	n	n	n	n	n	x	n	n	n	n	n	n
TP1	Pl_1_6_1	n	x	n	n	x	x	x	n	n	n	n	x	n	n	n	x	n	n	n	n
	Pl_1_6_2	n	n	x	x	n	n	n	n	n	n	n	x	x	n	n	n	n	n	n	n
	Pl_1_6_3	n	n	x	n	x	x	n	n	n	n	x	n	n	n	n	n	n	n	n	n
TP1	Pl_2_1_1	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n
	Pl_2_1_2	n	n	n	n	n	n	n	n	x	x	n	n	n	n	n	x	n	n	n	n
	Pl_2_1_3	n	n	n	n	n	x	n	n	n	n	x	n	n	n	x	n	n	x	n	n
TP1	Pl_2_2_1	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n
	Pl_2_2_2	x	x	n	n	n	x	n	n	n	n	n	n	n	n	n	n	n	n	n	n
	Pl_2_2_3	n	n	n	n	n	n	x	n	n	n	n	n	n	x	n	n	n	n	n	n
TP1	Pl_2_3_1	n	n	n	n	n	n	n	n	n	x	n	n	x	n	n	n	n	n	n	n
	Pl_2_3_2	n	x	x	x	n	n	x	n	n	n	n	n	x	n	n	n	n	n	n	n
	Pl_2_3_3	n	n	n	n	n	n	n	n	n	n	n	x	n	x	n	n	n	x	n	n
TP1	Pl_2_4_1	n	n	n	n	x	n	n	n	x	x	n	n	n	n	n	n	x	n	n	n
	Pl_2_4_2	n	n	n	x	x	n	n	n	n	n	n	x	n	n	x	n	x	n	n	n
	Pl_2_4_3	n	n	n	n	n	x	n	n	n	n	n	n	x	n	n	n	x	n	n	n
TP1	Pl_2_5_1	n	n	n	n	n	n	n	n	n	x	n	n	x	x	n	n	n	n	n	n
	Pl_2_5_2	n	n	n	n	n	n	n	n	n	n	n	n	x	x	n	n	x	n	x	n
	Pl_2_5_3	n	n	n	n	n	n	n	n	x	n	x	x	n	n	n	n	n	x	n	n
TP1	Pl_2_6_1	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n
	Pl_2_6_2	n	n	n	n	x	n	n	n	n	n	n	x	x	n	n	n	n	n	n	n
	Pl_2_6_3	n	n	n	n	n	x	n	n	n	n	n	n	x	n	n	n	n	n	n	n
TP2	Pl_4_1_1	n	n	n	n	n	n	x	n	n	n	n	n	x	n	n	n	n	n	n	n
	Pl_4_1_2	n	n	n	n	n	x	x	n	n	n	n	n	n	x	n	n	x	n	n	n
	Pl_4_1_3	n	n	n	n	n	x	n	n	n	n	x	n	n	n	n	n	x	n	n	n
TP2	Pl_4_2_1	n	n	n	x	n	n	n	n	n	n	x	x	n	n	n	n	n	n	n	n
	Pl_4_2_2	n	n	n	x	x	n	n	x	n	x	x	n	n	n	n	n	n	n	n	n
	Pl_4_2_3	n	n	n	n	n	n	n	n	n	n	x	n	n	x	n	x	n	n	n	n

TP	Attrappe	Testdurchlauf																			
		1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20
TP2	PI_4_3_1	n	n	n	n	n	n	n	n	n	n	n	x	n	n	x	x	x	n	n	n
	PI_4_3_2	n	x	n	x	n	n	n	n	n	x	x	x	n	n	x	n	x	n	n	x
	PI_4_3_3	n	n	n	n	n	n	n	x	n	n	x	n	n	n	x	x	n	n	x	n
TP2	PI_4_4_1	n	n	n	n	n	n	n	x	x	n	n	x	n	x	n	n	n	n	n	n
	PI_4_4_2	n	n	n	x	n	x	n	n	x	x	n	n	n	n	n	x	n	x	n	n
	PI_4_4_3	n	n	n	n	x	n	n	n	n	n	n	x	n	n	n	n	n	n	n	n
TP2	PI_4_5_1	n	n	n	n	x	n	n	n	n	x	n	n	n	x	n	n	x	n	n	n
	PI_4_5_2	n	n	n	n	n	n	n	n	n	x	n	x	n	n	n	x	n	n	n	n
	PI_4_5_3	n	n	n	n	n	n	n	n	x	x	x	n	n	x	n	n	x	n	x	x
TP2	PI_4_6_1	n	n	n	n	n	x	x	n	n	n	n	n	n	n	x	n	n	n	n	n
	PI_4_6_2	n	n	n	n	n	n	x	x	n	n	n	x	n	n	n	x	n	n	n	n
	PI_4_6_3	n	n	n	n	n	x	n	x	n	n	n	n	x	x	x	x	n	n	n	n
TP2	PI_4_7_1	n	n	n	n	n	n	n	n	n	x	n	n	n	n	x	x	x	n	n	n
	PI_4_7_2	n	n	n	x	x	n	n	x	n	n	x	n	n	n	x	n	n	x	n	n
	PI_4_7_3	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n	x	x	n
TP2	PI_4_8_1	n	n	x	n	n	n	n	x	x	n	n	n	n	n	n	x	n	n	n	n
	PI_4_8_2	n	n	n	x	n	x	x	n	n	n	n	n	x	x	x	n	n	n	n	n
	PI_4_8_3	n	n	x	n	n	x	x	n	n	n	x	n	n	n	n	x	n	n	n	n
TP2	PI_4_9_1	n	n	n	n	n	n	n	x	x	n	n	n	n	n	n	n	n	n	x	x
	PI_4_9_2	n	n	n	x	n	x	n	n	n	n	n	x	x	n	n	n	x	n	n	n
	PI_4_9_3	n	n	n	x	n	n	n	n	n	n	n	n	n	n	x	n	n	n	n	n
TP2	PI_4_10_1	n	x	n	n	x	n	n	n	n	n	n	n	n	n	x	n	n	n	n	n
	PI_4_10_2	x	n	n	n	n	n	n	n	n	x	n	n	n	n	n	x	n	n	n	n
	PI_4_10_3	n	n	n	n	n	x	x	n	n	n	x	x	n	n	n	x	n	n	n	x
TP2	PI_5_1_1	x	n	n	n	n	n	n	x	n	n	n	n	n	x	n	n	x	n	n	n
	PI_5_1_2	x	n	n	n	n	n	n	n	n	n	n	n	n	x	n	n	n	n	n	n
	PI_5_1_3	n	n	n	n	n	n	n	n	x	n	x	n	n	n	x	n	n	x	n	n
TP2	PI_5_3_1	x	n	n	n	n	n	n	n	n	n	x	n	n	n	n	x	n	n	n	n
	PI_5_3_2	n	n	n	n	n	n	x	n	n	n	n	n	n	n	n	n	n	n	n	n
	PI_5_3_3	n	n	n	n	n	n	n	n	n	n	x	n	n	n	x	n	n	n	n	n
TP2	PI_5_4_1	n	n	n	n	n	n	x	n	n	n	n	n	n	n	n	n	n	n	n	n
	PI_5_4_2	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n
	PI_5_4_3	n	n	x	n	x	n	n	n	n	n	n	x	n	n	n	x	n	n	n	n
TP2	PI_5_5_1	n	n	x	x	n	n	n	x	n	n	n	x	n	n	x	n	n	n	n	n
	PI_5_5_2	n	n	n	n	n	n	n	n	x	n	n	n	n	x	x	n	n	n	n	n
	PI_5_5_3	n	n	n	n	n	n	n	n	n	n	n	x	x	x	n	n	x	x	n	n
TP2	PI_5_6_1	n	n	x	n	n	n	n	n	n	x	n	n	n	n	n	n	n	n	x	n
	PI_5_6_2	n	n	n	n	n	x	n	n	n	n	n	n	n	n	n	x	n	n	n	n
	PI_5_6_3	n	n	n	n	n	x	n	n	n	n	n	n	x	n	n	n	n	n	n	x
TP2	PI_5_7_1	n	n	n	n	n	n	n	x	n	n	x	x	x	x	n	n	x	n	x	n
	PI_5_7_2	n	n	n	n	n	n	n	n	x	n	n	n	n	n	n	n	x	n	n	n
	PI_5_7_3	n	n	n	n	n	x	x	n	n	n	n	x	n	n	n	n	n	n	x	n
TP2	PI_5_8_1	n	n	n	n	n	n	x	x	n	n	n	n	n	x	n	n	n	n	n	n
	PI_5_8_2	n	n	n	n	n	n	n	x	n	n	n	x	n	x	n	n	n	n	n	n
	PI_5_8_3	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n

TP	Attrappe	Testdurchlauf																			
		1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20
TP1	PI_6_1_1	n	n	n	n	n	x	x	n	n	x	n	n	n	n	x	x	n	n	n	n
	PI_6_1_2	n	n	n	n	x	x	n	n	n	n	n	x	n	n	n	x	x	n	n	n
	PI_6_1_3	n	n	n	n	n	n	x	n	n	x	n	n	n	n	n	x	n	n	n	n
TP1	PI_6_2_1	n	n	n	x	x	x	n	n	n	n	x	n	n	n	n	n	n	n	n	n
	PI_6_2_2	n	n	n	n	n	n	n	n	n	n	n	n	x	n	n	n	x	n	n	n
	PI_6_2_3	n	n	n	n	n	n	n	x	n	n	n	x	n	n	n	n	x	n	n	n
TP1	PI_6_4_1	n	n	n	n	n	n	n	x	n	n	x	n	n	n	n	n	n	n	n	n
	PI_6_4_2	n	n	n	n	n	n	n	n	x	n	n	n	n	n	x	n	n	n	n	n
	PI_6_4_3	n	n	n	n	x	n	n	n	n	x	n	n	n	n	n	n	x	n	n	x
TP1	PI_6_5_1	n	n	x	x	n	n	x	n	n	n	n	n	n	n	n	n	n	n	n	n
	PI_6_5_2	n	n	n	n	n	n	n	n	n	n	n	n	x	x	x	n	n	n	n	n
	PI_6_5_3	n	n	n	n	n	n	n	n	n	n	x	n	n	n	n	n	n	n	n	x
TP1	PI_7_1_1	n	x	n	n	n	x	x	n	n	n	x	n	n	n	n	n	n	x	n	n
	PI_7_1_2	n	n	n	n	n	n	n	n	x	n	n	n	n	n	n	n	n	n	n	n
	PI_7_1_3	n	n	n	n	n	n	x	n	n	n	x	n	n	n	x	n	n	x	n	n
TP1	PI_7_2_1	n	n	x	n	x	x	x	n	n	n	n	n	n	n	n	n	n	x	n	n
	PI_7_2_2	n	n	n	n	n	n	n	n	n	n	n	n	n	x	x	n	n	n	n	n
	PI_7_2_3	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n	x	n	x	n	n
TP1	PI_7_3_1	n	n	n	x	x	n	n	n	n	x	n	n	n	n	n	n	n	n	n	n
	PI_7_3_2	x	x	n	n	n	n	n	n	n	n	n	n	n	n	n	n	x	n	n	n
	PI_7_3_3	n	n	n	n	n	n	n	x	x	n	n	n	n	x	n	n	n	n	n	n
TP1	PI_7_4_1	n	n	n	n	x	n	x	n	n	n	n	n	x	x	x	n	n	n	n	n
	PI_7_4_2	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n
	PI_7_4_3	n	n	n	n	x	n	n	n	n	x	n	n	n	n	n	n	n	n	n	n
TP1	PI_7_5_1	n	n	n	n	n	n	x	x	n	n	n	x	n	n	n	n	n	n	n	n
	PI_7_5_2	n	n	n	n	x	x	n	n	n	n	n	n	x	n	n	n	x	n	n	n
	PI_7_5_3	n	n	n	n	n	n	n	n	n	x	x	n	n	n	n	x	n	x	n	n
TP2	PI_8_1_1	n	n	n	x	x	x	n	n	n	n	n	n	x	x	n	x	x	n	n	n
	PI_8_1_2	x	x	x	n	n	n	n	n	n	x	n	n	n	x	n	n	x	x	n	n
	PI_8_1_3	n	n	n	n	n	x	x	n	n	n	n	x	n	n	n	n	n	n	n	n
TP2	PI_8_2_1	x	x	x	n	x	n	x	n	n	n	n	n	n	n	x	n	n	n	x	n
	PI_8_2_2	n	n	n	n	n	x	x	n	n	n	n	x	n	x	n	n	n	n	n	n
	PI_8_2_3	n	n	n	n	n	n	n	n	x	n	x	x	n	n	n	n	n	n	n	x
TP2	PI_8_3_1	x	x	x	n	n	x	n	n	n	n	n	n	n	n	n	n	n	n	n	n
	PI_8_3_2	n	n	n	n	x	x	n	x	n	n	n	n	x	x	x	n	n	n	n	n
	PI_8_3_3	n	n	x	n	x	n	n	x	n	n	n	x	n	n	x	n	x	n	n	n
TP2	PI_8_4_1	n	n	x	n	n	n	n	x	n	x	x	n	n	x	n	n	x	n	n	n
	PI_8_4_2	n	n	n	n	x	n	n	n	n	x	n	x	n	x	x	n	n	n	n	n
	PI_8_4_3	n	n	n	n	n	n	n	x	n	n	x	n	n	n	n	x	n	n	n	n

Appendix C

Die folgenden Fotos zeigen ein paar Materialien, Attrappen und Impressionen der Versuche zu dieser Arbeit.

Abbildung 56: Microsoft Fingerprint-Reader

Abbildung 57: Digitus Fingerprint-Reader

Abbildung 58: Utensilien zum Sichtbarmachen von Fingerabdrücken und Erstellen von Attrappen

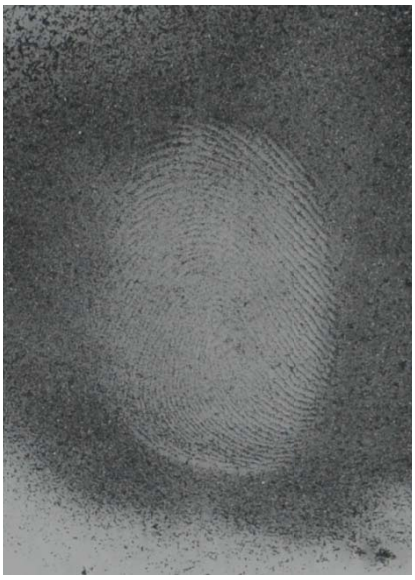

Abbildung 59: Sichtbarmachen mit Grafitpulver

Abbildung 60: Sichtbarmachen mit Cyanacrylat

Abbildung 61: typische Fimovorlage

Abbildung 62: typische Holzleim-Attrappe

Abbildung 63: typische Bastelkleber-Attrappe

Abbildung 64: typische Silikon-Attrappe

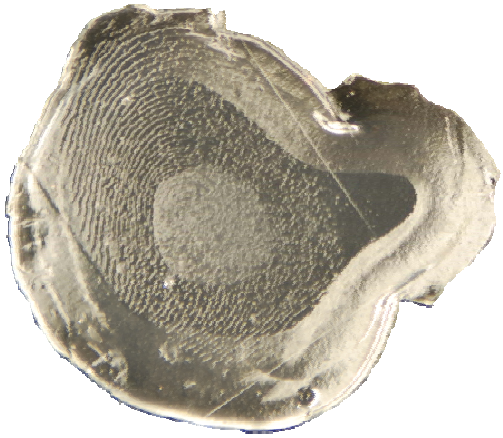

Abbildung 65: typische Gelatine-Attrappe

Abbildung 66: Ätzmittel und Entwickler zur Herstellung von Leiterplatten-Vorlagen

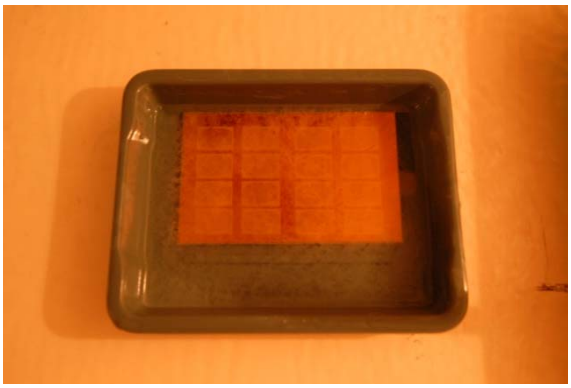

Abbildung 67: Entwickeln einer Leiterplatte

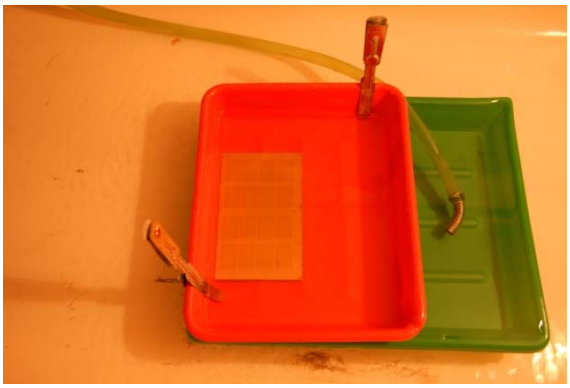

Abbildung 68: Ätzen einer Leiterplatte

Abbildung 69: Impressionen vom Ätzen der Leiterplatten 1

Abbildung 70: Impressionen vom Ätzen der Leiterplatten 2