Praktikumsbericht

Modul: „Forensik in Betriebs- und Anwendungssystemen“

Gruppe	**BER-03**
Franz Julius Albert	191423
Danilo Günzel	329556
Eva-Katharina Müller-Pietsch	329288

Hochschule Wismar

Fakultät für Ingenieurswissenschaften

Bereich für Elektrotechnik und Informatik

31. Juli 2020

Inhaltsverzeichnis

1 Einleitung **4**

1.1 Fallbeschreibung 4

1.2 Vorgehen 5

2 Vorbereitung und Schilderung des Sachverhaltes **7**

2.1 Arbeitsauftrag an das Team BER03 7

2.2 Auflistung der Asservate 8

2.3 Verwendete Werkzeuge 11

2.3.1 Software 11

2.3.2 Sonstiges 12

2.4 Ergebnisse der Ermittlung 12

3 Forensischer Prozess **14**

3.1 Datensammlung 14

3.1.1 Vorbereitung 14

3.1.2 Image erstellen mit FTK Imager 15

3.2 Untersuchung 18

3.2.1 Fallerzeugung in AXIOM Process 18

3.2.2 Fallauswertung in AXIOM Examine 21

3.3 Datenanalyse 24

3.3.1 Dokumente 24

3.3.2 E-Mails 27

3.3.3 Bild-Datei 29

3.3.4 Registry des Anwenders nowaktho 29

3.4 Abschliessende Dokumentation 30

3.4.1 Falldarstellung auf der Zeitachse 30

3.4.2 Einordnung in die CERT Taxonomie 32

3.4.3 Fallrückschlüsse 32

4 Bewertung der Ergebnisse **33**

5 Definition *Fuzzing* **35**

Abbildungsverzeichnis **37**

Tabellenverzeichnis **38**

Literaturverzeichnis **39**

1 Einleitung

Vorwort zum Praktikumsbericht

Der vorliegenden Praktikumsbericht der Gruppe BER03 gliedert sich in zwei Teile. Einerseits eine durch Kapitel Eins beschriebene allgemeine Darstellung des fingierten Falls, sowie der Beschreibung der Vorgehensweise des Teams. Andererseits entwickelt sich der Praktikumsbericht ab Kapitel Zwei in ein neutral fomuliertes Gutachten. Abschliessend werden durch Tabellen-, Abbildungs- und Literaturverzeichnis die verwendeten Quellen strukturiert dargelegt.

1.1 Fallbeschreibung

Im beschaulichen Freiburg im Breisgau befindet sich das Alzheimerforschungszentrum *FabLab Zentrum*. Der Journalistin Nao Yamamoto des *Freiburger Tagblatt* wurden von Unbekannt einige besorgniseregende Dokumente zugespielt die beweisen sollen, dass das *FabLab Zentrum* in illigale Tierversuche verstrickt ist. Anstelle der bei der Aufsichtsbehörde angemeldeten und bewilligten Kaninchen als Forschungsobjekte, wurden gemäss Nao Yamamoto Tierversuche an Katzen aus dem nahegelegenen Tierheim *Glückes Baare* durchgeführt.
Das Forschungszentrum möchte nun alles daran setzen die Quelle zu ermitteln, aus der die zugespielten Dokumente stammen. Das unabhängige Forensik-Team *BER03* wurde durch das Forschungszentrum beauftragt aufzudecken, ob sich die erste Vermutung der Leiterin des Teams *Alzheimerforschung 1* Olivia Taylor, PhD bestätigt. Gemäss ihrer Aussage ist es am Naheliegensten, dass ihr ehemaliger PhD-Studenten Thorben Nowak die fraglichen Dokumente an die Journalistin weitergegeben hat. Nachdem dieser im Mai sämtliche Kaninchen frei gelassen hatte, wurde er wegen Vetragsverstoss und Gefährdung der Tiere mit einer Kündigungsfrist von einem Monat entlassen. Er hat das *FabLab Zentrum* per 22.06.2020 verlassen.
Das Zentrum hat im Zuge der Auftragsvergabe bereits den Laptop des damaligen

Mitarbeiters an das Forensik-Team *BER03* übergeben.[1]

1.2 Vorgehen

Während der forensischen Untersuchung und somit auch gültig für den vorliegenden Praktikumsbericht orientiert sich BER03 an dem Vorgehensmodell nach BSI [BSI,2011].

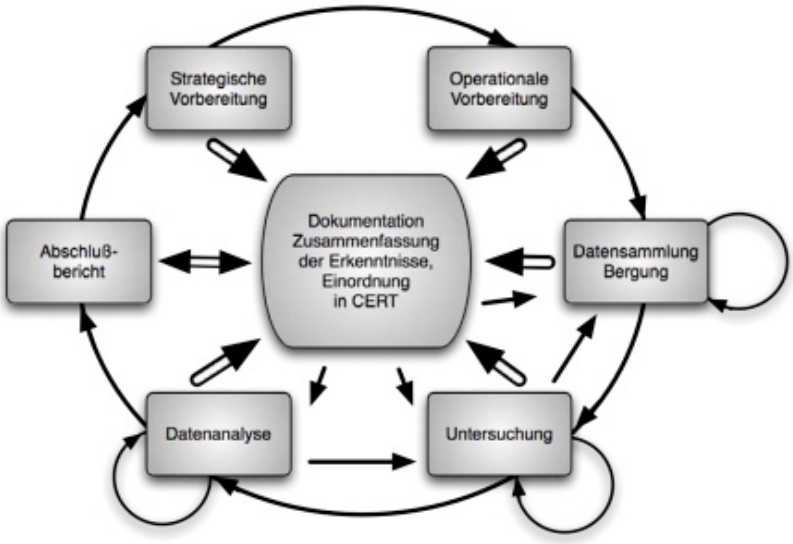


Abbildung 1.1: Abschnitte des forensischen Prozesses nach BSI

1. **Strategische Vorbereitung:**
   Auf Grund des vorliegenden Falls ist dieser Schritt obsolet.

2. **Operationale Vorbereitung:**
   Dieser Prozessschritt spiegelt sich im vorliegenden Kapitel 2 wieder und umfasst die Dokumentation des Auftrages, die Darlegung der Datenquellen in Form von Asservaten, sowie die Vorstellung der verwendeten Werkzeuge. Die Wahl der Werkzeuge wird dabei begründet.

3. **Datensammulung/Bergung:**
   Im Zuge der Datensammlung wird im Kapitel 3 näher aufgezeigt, wie die Sicherung der Datenquelle vorgenommen und welche wichtigen Aspekte dabei berücksichtigt werden mussten

[1] Die Wahl der Personen, Orte und Unternehmungen sind frei erfunden. Ähnlichkeiten zu Objekten des echten Lebens sind nicht beabsichtigt.

4. **Untersuchung:**
   Die Extraktion der relevanten Daten aus dem Abbild wird im Zuge dieses Prozessschrittes ebenfalls im Kapitel 3 beschrieben.

5. **Datenanalyse:**
   Die extrahierten Daten werden einer Detailanalyse unterzogen um Verbindungen zwischen den Ereignissen und den involvierten Personen zu ziehen. Das Vorgehen und die Resultate werden ebenfalls im Kapitel 3 beschrieben.

6. **Abschlussbericht:**
   Abschliessend folgt im Kapitel 3 die Schlussdokumentation des Falls. Dies umfasst die Darstellung entlang einer Zeitachse sowie die Einordnung in die CERT-Taxonomie.

2 Vorbereitung und Schilderung des Sachverhaltes

2.1 Arbeitsauftrag an das Team BER03

Der Auftraggeber *FabLab Zentrum* bestellt ein Gutachten, welches für etwaige weitere rechtliche Schritte verwendet werden kann. Die Abgabe des Gutachtens ist auf den 31.07.2020 terminiert. Das Budget für die forensische Untersuchung spielt für den Auftraggeber keine Rolle.

Dem Team *BER03* wurde im Zuge der Auftragserteilung das Arbeitsnotebook des ehemaligen Mitarbeiters übergeben (Asservat-01). Das Gerät muss per Abschluss der Untersuchung unbeschadet retourniert werden.
Im Wesentlichen umfasst der Arbeitsauftrag folgende Fragestellungen, bezogen auf das Asservat-01 :

1. Darlegung der Dateien, die aus dem Dateisystem rekonstruiert werden können und die in einem Zusammenhang mit potenziellen Tierversuchen stehen.

2. Auflisten eventuell gelöschter Dateien, die in einem Zusammenhang mit potenziellen Tierversuchen stehen.

3. Darlegung vorhandener Emails zum Zeitpunkt der letzten sechs Monate seit Übergabe an die Zeitung, genauer:
   a) Wurde von Thorben Nowaks Email Account die Jouranlistin Nao Yamamoto kontaktiert?
   b) Wurden von Thorben Nowaks Email Account Dateien an Labor-fremde Personen übermittelt?
   c) Wurden Emails mit Hinweisen zu dem Vorfall an interne Personen versendet?

Im Zuge der Verschwiegenheitsklausel, die *BER03* im Zuge der Vertragsunterzeichnung unterschrieben hat, verpflichtet sich das Forensik-Team zu absoluter Verschwiegenheit hinsichtlich des aktuell laufenden präklinischen Entwicklungsprogramms.

2.2 Auflistung der Asservate

Die nachfolgende Auflistung der Asservate umfasst sämtliche dem Forensikteam *BER03* übergebenen Beweise. Sie dienen der Auftragserfüllung und müssen gemäss Vertragsbestimmung wieder an das *FabLab Zentrum* retourniert werden. Folgende Asservate wurden *BER03* im Zuge der Auftragsvergabe übergeben:

Asservat-ID	Bezeichnung	Ort des Erhalts	Datum des Erhalts
01	Lenovo Yoga	FabLab Zentrum, Freiburg	29.06.2020
02	AC Adapter Lenovo	FabLab Zentrum, Freiburg	29.06.2020
03	Samsung 960 EVO	FabLab Zentrum, Freiburg	29.06.2020

Tabelle 2.1: Asservate

Fotodokumentation Asservat-01:

Abbildung 2.1: Asservat-01

Fotodokumentation Asservat-02:

Abbildung 2.2: Asservat-02

Fotodokumentation Asservat-03:

Abbildung 2.3: Asservat-03

Es können gemäss unten aufgeführtem Beweismittelzettel sowie Vor-Ort Dokumentation, die anschliessenden Aspekte festgehalten werden:

- Das *Asservat-01* und das *Asservat-02* wurde am 22.06.2020 um 17:45 Uhr durch den ehemaligen Mitarbeiter am Empfang des Gebäude A auf dem Campus des Forschungszentrums gegen Unterschrift abgegeben.
- Das *Asservat-01* und das *Asservat-02* wurde am 23.06.2020 um 10:00 Uhr an den IT-Service des Campus übergeben und dort in einen Tresor für ehemalige Arbeitsnotebooks eingeschlossen - Das Vorgehen wurde protokolliert.
- Das *Asservat-01* und das *Asservat-02* wurden am 29.06.2020 um 14:10 Uhr aus dem Tresor geholt und an das Team *BER03* um 14:30 übergeben.
- Die Entgegennahme erfolgte im Vier-Augenprinzip (siehe Beweismittelzettel)
- Gemäss Aussage des Verantwortlichen des *IT-Service* wurden an dem Gerät seit Entgegennahme durch den IT-Service keine Handlungen vorgenommen.

- Das *Asservat-01* wurde durch *BER03* sachgemäss verpackt und unter Sichtkontakt in das Labor transportiert.
- Das *Asservat-02* wurde durch *BER03* sachgemäss verpackt und unter Sichtkontrolle in das Labor transportiert.

//Forensikteam BER03

Beweismittelzettel

Datum: 29.06.2020 Uhrzeit: 14:30 Uhr ABGESCHLOSSEN			Ort: FabLabZentrum Industriestrasse 96 79108 Freiburg
		Ermittler:	Franz Julius Albert
			Danilo Günzel
		Zeuge:	Eva-Katharina Müller-Pietsch
Objekt ID	Gegenstand	Anzahl	Beschreibung
01	Lenovo Yoga S740-14IIL (15'')	1	Modell: 81RS Seriennummer: PFX9B0323331 Betriebssystem: Windows 10 Eigentümer: FabLab Zentrum Informatik
02	Netzkabel mit AC Adapter Lenovo	1	135W Input: 100-240V Output:20V Seriennummer: 8SSA 10E75864D1SG99P0038 Eigentümer: FabLab Zentrum Informatik

Bemerkungen	
Gegenstand: 01	Der Gegenstand wurde dem Ermittler unter Beisein des Zeugen gegen eine Unterschrift ausgehändigt. Es wurde ein Foto angefertigt. Für den Transport wurde ein gepolsterter Aluminiumkoffer verwendet.
02	Das Ladekabel und der dazugehörende AC Adapter wurden in einer Kiste mit Deckel transportiert. Es wurde ein Foto angefertigt.

Abbildung 2.4: Beweismittelzettel

2.3 Verwendete Werkzeuge

Im Zuge der Entgegennahme der Beweise und während der forensischen Untersuchung wurden die hier aufgelisteten Werkzeuge verwendet. Auf eine detaillierte Beschreibung der verwendeten Software wird an dieser Stelle verzichtet, da es sich um anerkannte Forensik-Tools handelt, deren Akzeptanz und Glaubwürdigkeit gegeben ist. Die detaillieren Angaben zu den von *BER03* verwendete Hardware (Rechner, Speichermedien, Writeblocker, etc.) sowie die grundsätzliche Laborinfrastruktur des Betriebes können auf Verlangen und gegen Unterschrift eingeholt werden. Sie sind aus sicherheits- und datenschutzzwecken nicht Bestandteil des Berichts.

2.3.1 Software

1. *Access Data* - FTK Imager
    - Version: 4.3.0.11
    - Beschreibung: Software für die Erstellung von forensischen Images, inklusive Previewfunktion von Dateien und Verzeichnissen. Unterstützt die Hashwertbildung von Files.
    - Begründung: Als Best-Practise Software für die Erstellung von forensischen Images, ist diese Software aus dem Hause Acess Data für die Untersuchung gesetz.

2. *Magnet* - Axiom Examine und Axiom Process
    - Version: 4.2.020379
    - Beschreibung: Forensische Analysesoftware, die eine professionelle Untersuchung auf unterschiedlichen Betriebssystemen und Dateiverzeichnis-Formaten ermöglicht.
    - Begründung: Gemäss Auftragsstellung müssen neben lokal gespeicherten Dateien auch gelöschte Daten rekonstruiert werden. Ebenfalls muss ein Mailkonto analysiert werden. Die Software aus dem Haus Magnet unterstützt diese Analysen durch seine breitabgestützte Funktionspalette.

2.3.2 Sonstiges

- Kamera eines Iphone SE (2.Generation) für die Vor-Ort Dokumentation
- Kamera eines ZTE Axon 7 Smartphones für die Vor-Ort Dokumentation

2.4 Ergebnisse der Ermittlung

Der Auftragsumfang definierte, wie bereits aufgeführt, die folgenden Fragestellungen, auf die in diesem Kapitel Bezug genommen wird.

1. Darlegung der Dateien, die aus dem Dateisystem rekonstruiert werden können und die in einem Zusammenhang mit potenziellen Tierversuchen stehen.

   Die Analyse hat diverse Dokumente zu Tage gefördert, die im Zusammenhang mit potenziellen Tierversuchen stehen. Hierzu zählen Forschungsberichte, Fotoaufnahme einer Katze, und die im Dateisystem abgelegten Emails, inklusive Anhängen.

2. Auflisten eventuell gelöschter Dateien, die in einem Zusammenhang mit potenziellen Tierversuchen stehen.

   Datei „Tierversuch_Katze.jpeg“ zeigt eine Katze in einem Käfig in einer Laborumgebung.

3. Darlegung vorhandener Emails zum Zeitpunkt der letzten sechs Monate seit Übergabe an die Zeitung, genauer:

   a) Wurde von Thorben Nowaks Email Account die Journalistin Nao Yamamoto kontaktiert?

      Hier konnte eine Email mit elf Anhängen sichergestellt werden (siehe E-Mail vom 22.06.2020, 18:16).

   b) Wurden von Thorben Nowaks Email Account Dateien an Labor-fremde Personen übermittelt?

      Ausschliesslich die in Punkt 3a) erwähnte Email, an die Journalistin Nao Yamamoto.

   c) Wurden Emails mit Hinweisen zu dem Vorfall an interne Personen versendet?

Hierzu wurden Emails sichergestellt, die von Thorben Nowak an Frieda Zimmermann gerichtet sind (siehe E-Mail vom 14.05.2020, 18:21). In diesen werden keine konkreten Hinweise zum Fall genannt.

3 Forensischer Prozess

3.1 Datensammlung

Die Datensammlung erfolgt über die Auswertung des Abbilds der verbauten Festplatte mit Hilfe der genannten forensischen Werkzeuge.

3.1.1 Vorbereitung

Zuerst wurde das Notebook entsprechend der technischen Dokumentation des Herstellers geöffnet. [LEN, 2019]
Anschliessend wurden mögliche Speichermedien identifiziert und diese ausgebaut (Schutzmassnahmen wie Erdung wurden beachtet).
Hierbei wurde als einzige Datenquelle ein M-2-SSD-Modul, eine Spezifikation für interne Computer-Erweiterungskarten und deren Anschlüsse, (Solid State Drive, ein Speichermedium auf Halbleiterbasis) identifiziert.
Zum Auslesen der SSD wurde diese über einen M.2 auf SATA Adapter und einem WriteBlocker per USB an einen Windows 10 PC angeschlossen.
Auf diesem findet die im Folgenden beschriebene Erstellung eines Abbildes, sowie dessen Auswertung statt.

3.1.2 Image erstellen mit FTK Imager

Innerhalb des FTK Imagers wurde die Festplatte als physisches Gerät ausgewählt und drei Partitionen erkannt:

Nummer der Partition	Grösse (MB)	Dateisystem	Beschreibung
1	50	FAT32	Boot Partition, enthält Bootmanager und ggf. Daten für Windows BitLocker-Laufwerksverschlüsselung
2	40385	NTFS	Systempartition, enthält Betriebssystem und Anwenderdaten
3	512	NTFS	Partition, die Informationen enthält, um das Betriebssystem auf Partition 2 wieder in den Auslieferungszustand zurückzusetzen. Wird im Windows vor Anwender versteckt

Tabelle 3.1: Partitionsstruktur

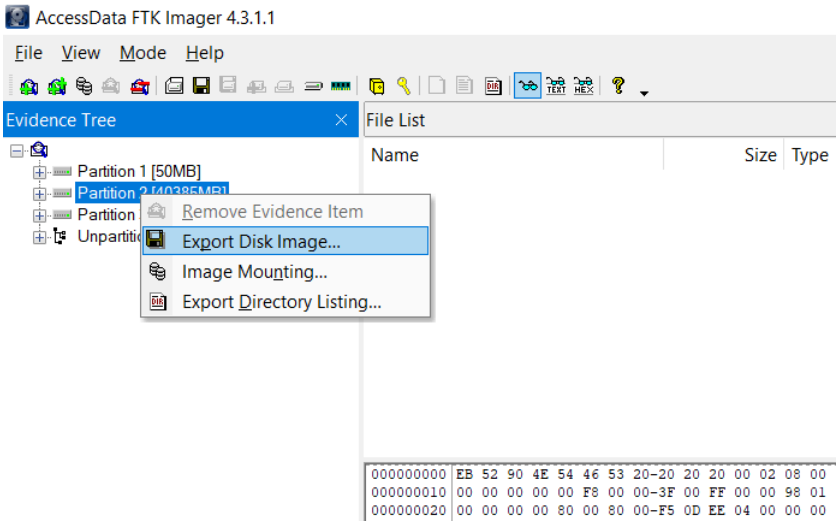


Abbildung 3.1: FTK Imager: Partitionsstruktur

Für unsere Auswertung ist die Partition 2 von Bedeutung. Der Export erfolgte im EnCase-E01-Format mit den Optionen *maximale Kompression* und *keine Segmentierung*.

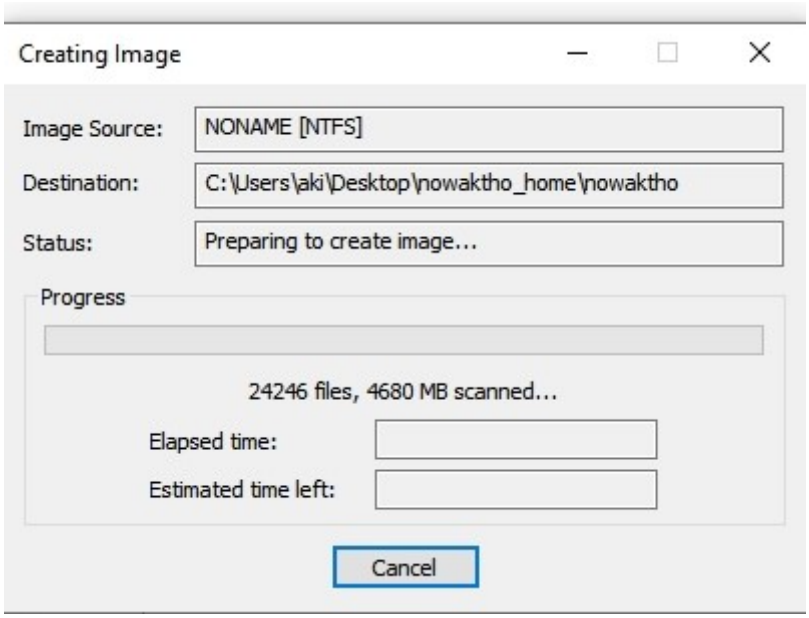


Abbildung 3.2: FTK Imager: Vortschrittsanzeige bei der Image Erstellung

Zum Abschluss des Prozesses berechnet FTK Imager selbstständig Hashwerte im MD5- und SHA-Format

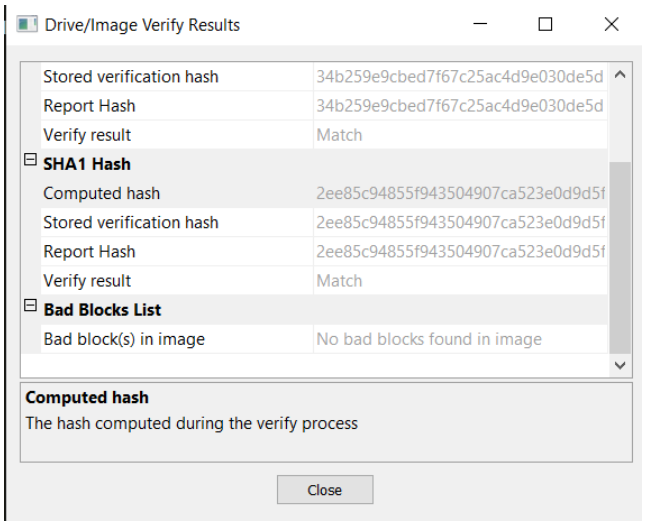


Abbildung 3.3: FTK Imager: Abschlussreport mit Hashwerten

Um das erstellte Image im Fall einer möglichen Modifikation nicht neu erstellen zu müssen, wird von der erstellten Imagedatei eine Kopie (Duplikat) erzeugt und die entsprechenden Hashwerte per Powershell verglichen. Sie gilt als Arbeitsgrundlage für die anschliessende Auswertung.

```
PS C:\Users\aki\Desktop\nowaktho_home> Get-FileHash .\1.E01 -Algorithm
SHA1 | Format-List
Algorithm : SHA1 Hash : 2ee85c94855f943504907ca523e0d9d5f5a4b0d4 Path :
C:\Users\aki\Desktop\nowaktho_home\1.E01
PS C:\Users\aki\Desktop\nowaktho_home> Get-FileHash .\nowakth_case.E01
-Algorithm SHA1 | Format-List
Algorithm : SHA1 Hash : 2ee85c94855f943504907ca523e0d9d5f5a4b0d4 Path :
C:\Users\aki\Desktop\nowaktho_home\1.copy.E01
```

3.2 Untersuchung

Die Untersuchung erfolgte mit der Software AXIOM der Firma Magnet. AXIOM besteht seinerseits aus zwei Anwendungen: AXIOM Process und AXIOM Examine.

3.2.1 Fallerzeugung in AXIOM Process

Mittels AXIOM Process werden Beweise aus Beweisquellen akquiriert und für AXIOM Examime aufbereitet.
Im ersten Schritt wurden Daten zur Fallbeschreibung eingegeben

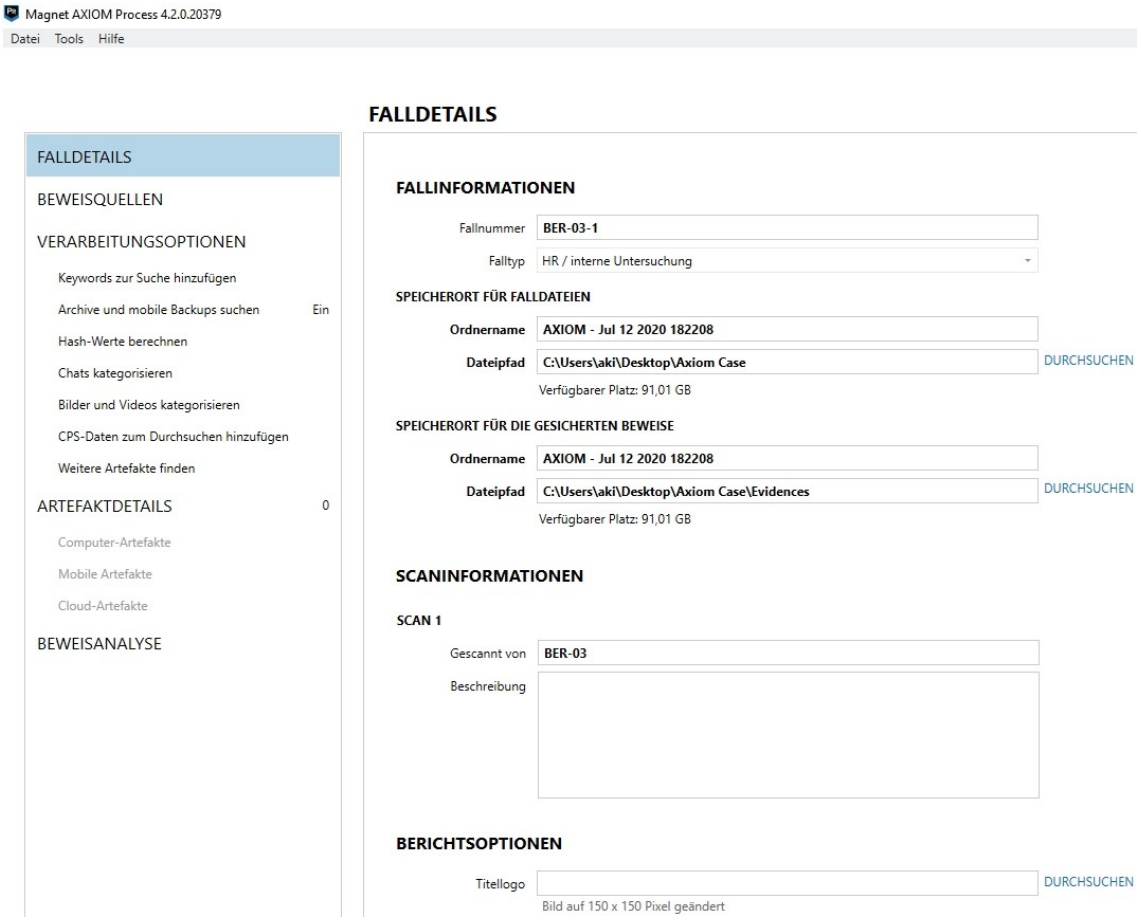


Abbildung 3.4: AXIOM Process: Fallbeschreibung

Anschliessend die Beweisquellen bestimmt.

- Computer
- Windows
- Beweise laden
- Abbild
- Imagedatei *C:\Users\aki\Desktop\nowaktho_home\nowakth_case.E01* ausgewählt

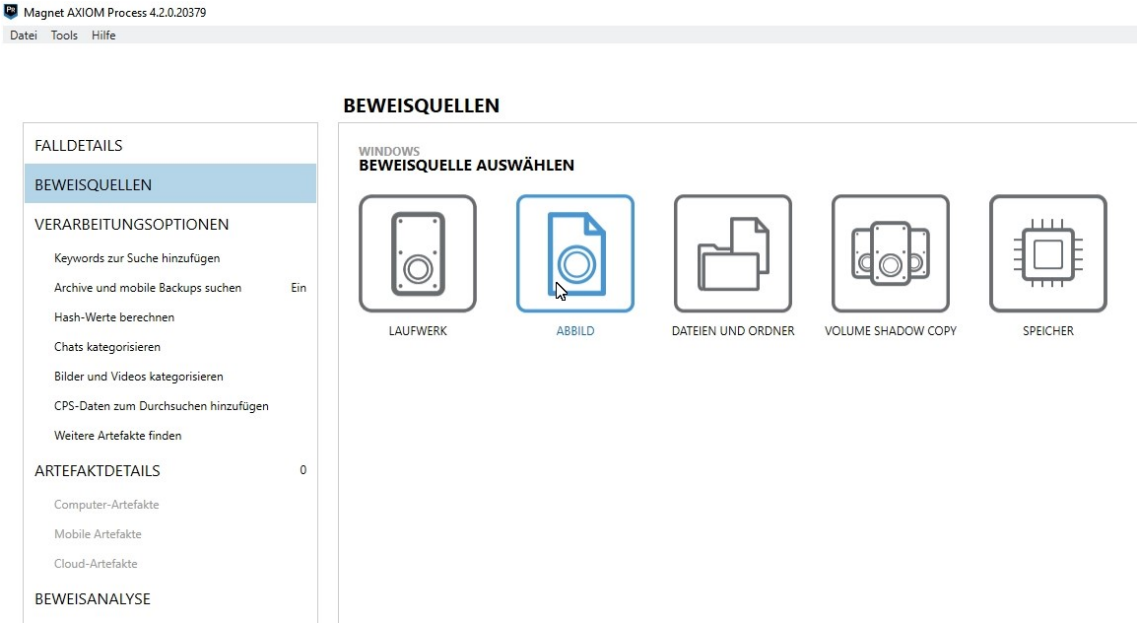


Abbildung 3.5: AXIOM Process: Auswahl der Beweisquellen

Nachdem der Bestimmung der Beweisquelle wurden im folgenden Schritt die Verarbeitungsoptionen festgelegt.
Dazu wurden die Keywords "Tierversuch" und "Yamamoto" definiert.

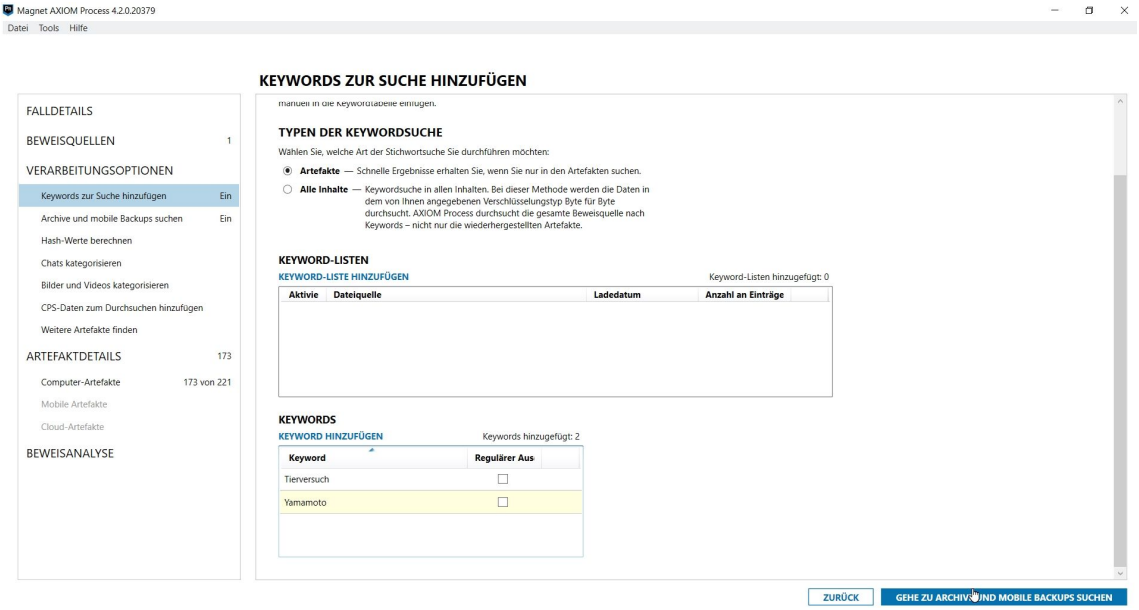


Abbildung 3.6: AXIOM Process: Definition von Keywords

Als weitere Verarbeitungsoption wurde die Suche in gefunden Archiven aktiviert (in bis zu fünf verschalteten Ebenen). Im letzten Schritt wurde die Suche nach möglichen Beweisen, in AXIOM als Artefakte bezeichnet, beschränkt auf:

- Worddokumente und
- gebräuchliche E-Mailformate

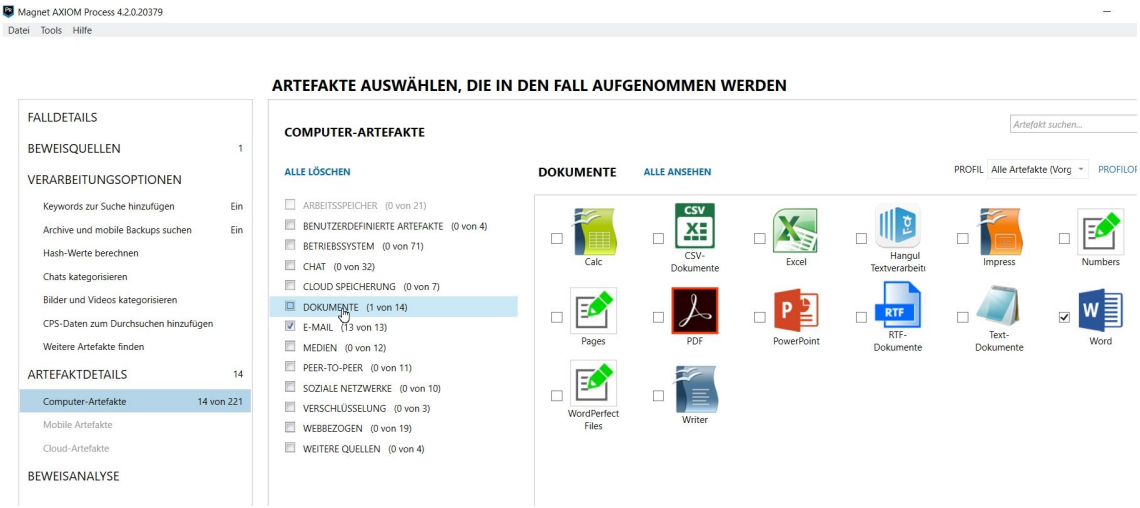


Abbildung 3.7: AXIOM Process: Auswahl der zu berücksichtigen Dateitypen

Die Auswertung der potenziellen Beweise erfolgte anschliessend in AXIOM Examine.

3.2.2 Fallauswertung in AXIOM Examine

Die Fallerzeugung zeigt auf 170 gefundene Artefakte. Die Keywordsuche ergab folgendes Ergebnis:

- 16 Treffer "Yamamoto"
- 8 Treffer "Tierversuch"

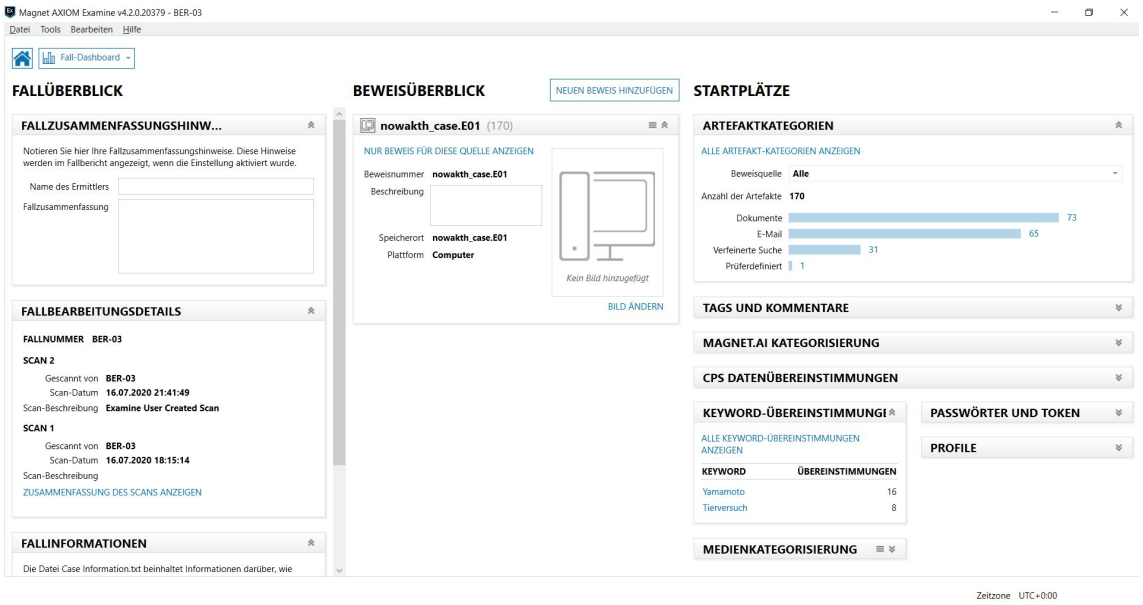


Abbildung 3.8: AXIOM Examine: Fallübersicht

Im ersten Schritt wurden die gefundenen Dokumente einzeln mittels der Vorschaufunktion selektiert. Von den 73 Dokumenten wurden elf für die spätere Datenanalyse exportiert. Die restlichen Dateien stellen Vorlagen dar.

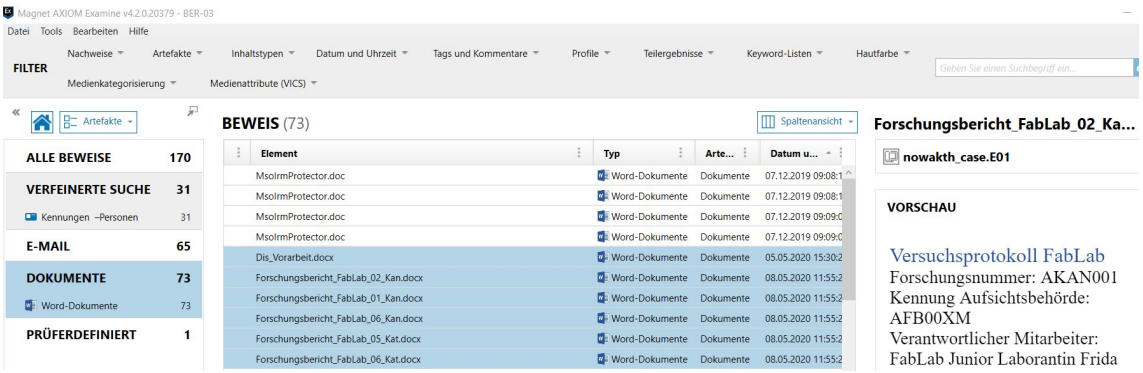


Abbildung 3.9: AXIOM Examine: Ermittelte Dokumente

Die Dokumente wurden zum Teil aus einem zu löschen markiertem Archiv (Windows-Papierkorbfunktion) wiederhergestellt.
Die Quelle lautet: "nowakth_case.E01 - \Users\nowaktho\Documents\02_PhD.zip"

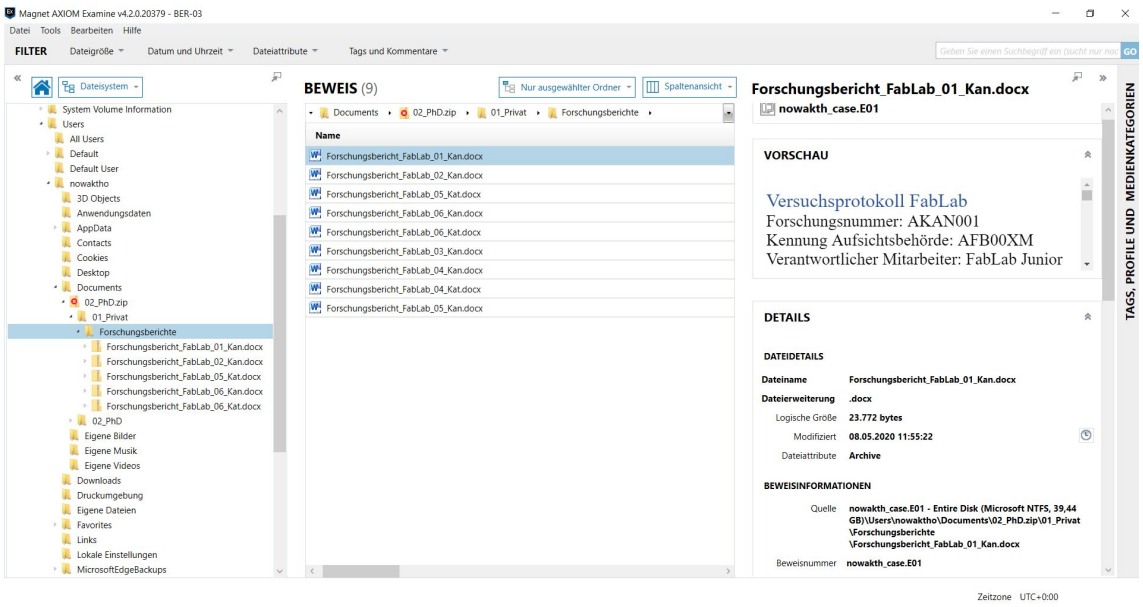


Abbildung 3.10: AXIOM Examine: Inhalt von gelöschtem zip-Archiv

Daneben wurde im Papierkorb noch ein Bild vom Typ *jpeg* gefunden.

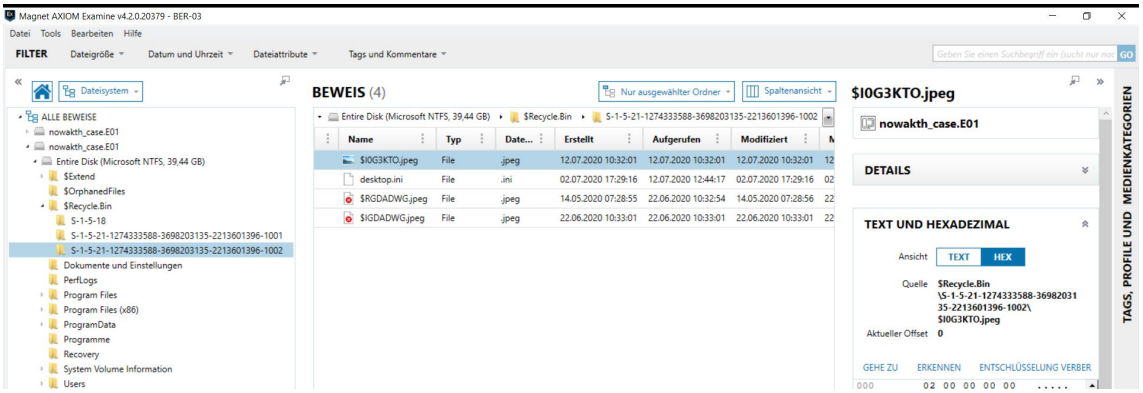


Abbildung 3.11: AXIOM Examine: gelöschte Bild-Datei

Die 65 gefundenen E-Mailartefakte stammen aus einem Mozilla Thunderbird Profil unter "nowakth_case.E01 - \Users\nowaktho\AppData\Roaming\Thunderbird\Profiles\r6abiapt.default-release\ImapMail\".
Sie unterteilen sich in 52 E-Mails, elf Anhänge und zwei leere Mails. Die Daten

wurden für die anschliessende Datenanalyse exportiert.

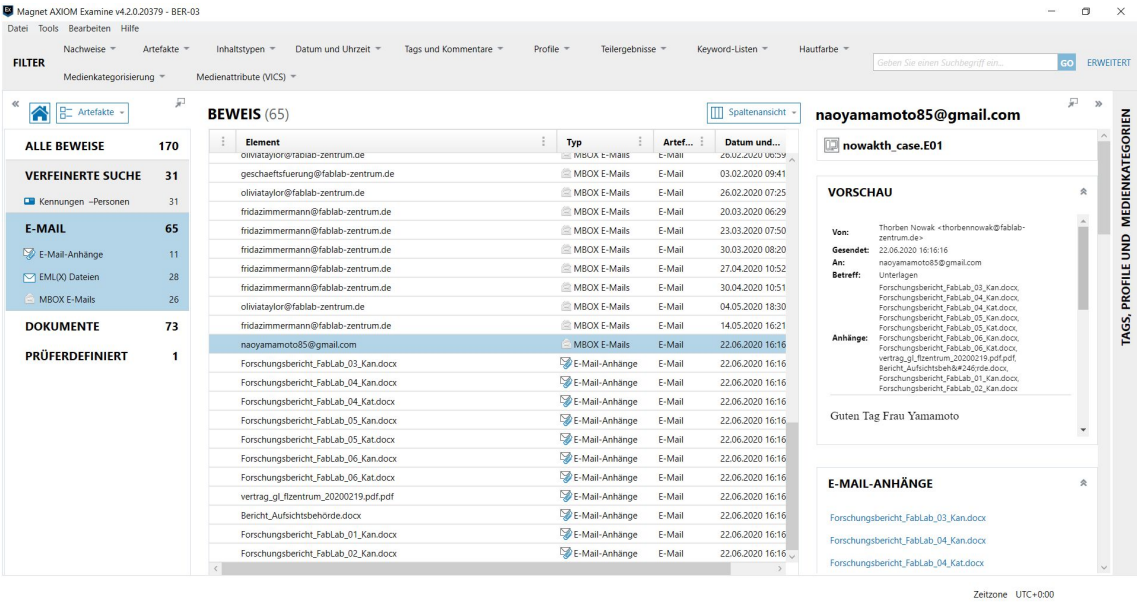


Abbildung 3.12: AXIOM Examine: Gefundene E-Mails und Anhängen

Die Auswertung der Keywords verwies auf die bereits beachteten Dateien.

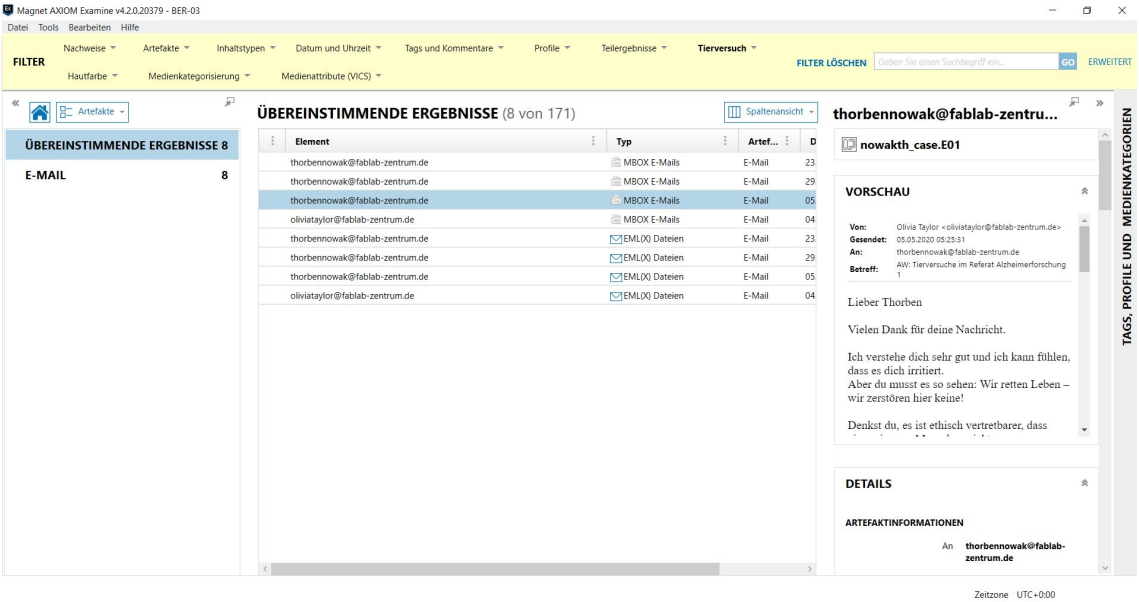


Abbildung 3.13: AXIOM Examine: Ergebnis der Keywordsuche

Neben der Suche nach Dateitypen und Schlüsselwörtern, wurde auch die Registry des Nutzers analysiert.

Die findet sich unter "nowakth_case.E01 - Users\nowaktho\NTUSER.DAT". Diese wurde ebenfalls exportiert.

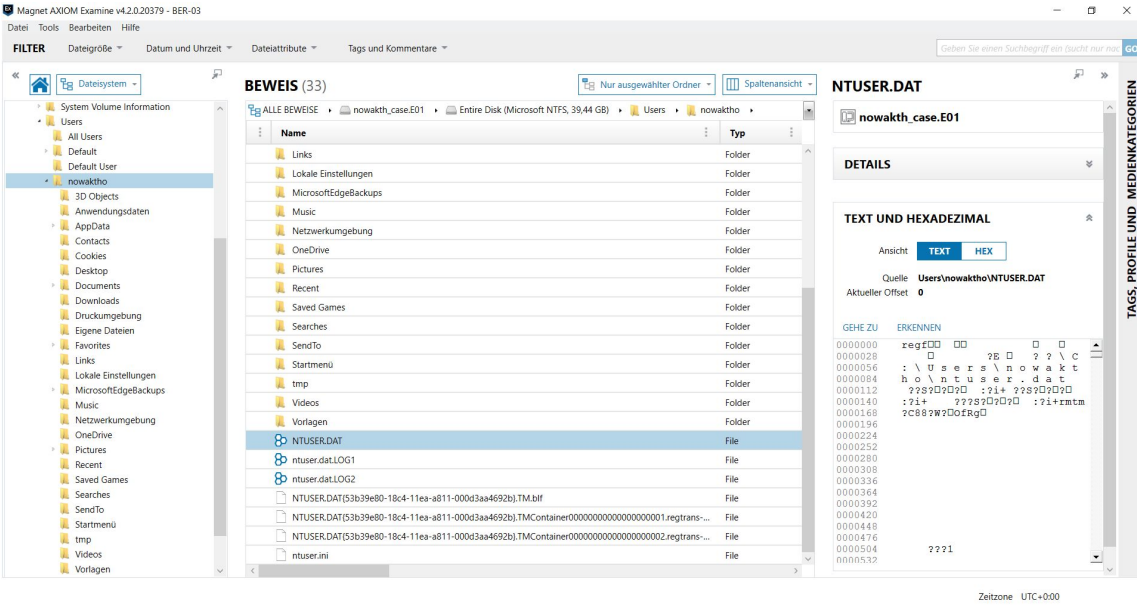


Abbildung 3.14: AXIOM Examine: Registry des Nutzers nowaktho

Unter *Program Files*\, sowie *Program Files (x86)*\ sind nur Standart-Anwendungen installiert.

3.3 Datenanalyse

Im ersten Schritt wurden die ermittelten Dokumente analysiert, im Anschluss die E-Mails und die Windows-Registry des Nutzers *nowakth*.

3.3.1 Dokumente

Es finden sich insgesamt sieben Dokumente vom Typ Office Open XML (docx). Es handelt sich um Versuchsprotokolle der Firma FabLab.

Dateiname	Fundstelle	Author
Bericht_ Aufsichtsbehörde.docx	Attachment	AFB00XM
Forschungsbericht_ FabLab_01_Kan.docx	Attachment, $recyclebin (02_PhD.zip)	F.Zimmerman
Forschungsbericht_ FabLab_02_Kan.docx	Attachment, $recyclebin (02_PhD.zip)	F.Zimmerman
Forschungsbericht_ FabLab_03_Kan.docx	Attachment, $recyclebin (02_PhD.zip)	F.Zimmerman
Forschungsbericht_ FabLab_04_Kan.docx	Attachment, $recyclebin (02_PhD.zip)	F.Zimmerman
Forschungsbericht_ FabLab_04_Kat.docx	Attachment, $recyclebin (02_PhD.zip)	F.Zimmerman
Forschungsbericht_ FabLab_05_Kan.docx	Attachment, $recyclebin (02_PhD.zip)	F.Zimmerman
Forschungsbericht_ FabLab_05_Kat.docx	Attachment, $recyclebin (02_PhD.zip)	F.Zimmerman
Forschungsbericht_ FabLab_06_Kan.docx	Attachment, $recyclebin (02_PhD.zip)	F.Zimmerman
Forschungsbericht_ FabLab_06_Kat.docx	Attachment, $recyclebin (02_PhD.zip)	F.Zimmerman
vertrag_gl_flzentrum_ 20200219.pdf	Attachment	FabLab Geschäftsführung

Tabelle 3.2: Übersicht Dokumente

Die Dokumente finden sich jeweils im Anhang. Die Dokumente wurden dupliziert und in Word geöffnet, damit alle (Meta-) Informationen ermittelt werden konnten.

Ein Beispieldokument:

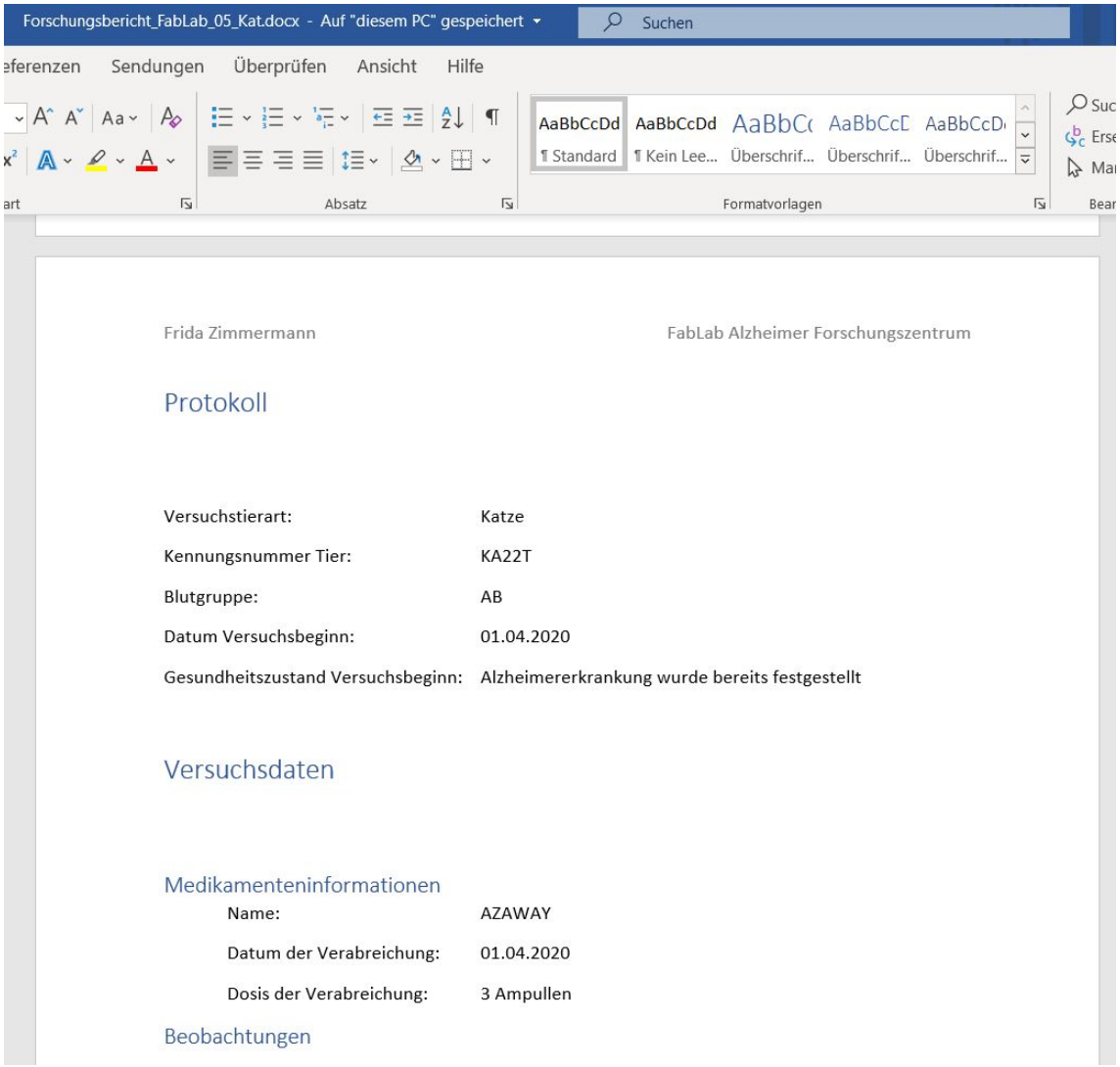


Abbildung 3.15: Auszug aus einem Forschungsbericht

3.3.2 E-Mails

Im folgenden findet sich eine Übersicht der ermittelten E-Mail-Kommunikation aus Mozilla Thunderbird. Aus Gründen der Übersichtlichkeit sind nur die relevanten E-Mails aufgeführt.

Sender	Empfänger	Betreff	gesendet Datum / Uhrzeit	Fundstelle
Frida Zimmermann	Thorben Nowak	AW: Vergangenes Wochenend	23.03.2020, 09:19	Posteingang
Thorben Nowak	Frida Zimmermann	Experimente mit Versuchstieren	23.03.2020, 08:50	Postausgang
Thorben Nowak	Frida Zimmermann	Vertragsdokument "vertrag_gl_ flzentrum_20200219.pdf" auf Gruppenlaufwerk	27.04.2020, 12:52	Postausgang
Olivia Taylor	Thorben Nowak	WG: Resultat der Begehung am 29. April 2020	29.04.2020, 18:40	Posteingang
Thorben Nowak	Frida Zimmermann	Begehung unseres Referats durch das Regierungspräsidium Stuttgart	30.04.2020, 12:51	Postausgang
Thorben Nowak	Olivia Taylor	Tierversuche im Referat Alzheimerforschung 1	04.05.2020, 20:30	Postausgang
Olivia Taylor	Thorben Nowak	Re: Tierversuche im Referat Alzheimerforschung 1	05.05.2020, 07:25	Posteingang
Thorben Nowak	Frida Zimmermann	Taten statt Worte	14.05.2020, 18:21	Postausgang
Geschäfts-führung	Thorben Nowak	Kündigungs-bestätigung	15.05.2020, 09:03	Posteingang
Thorben Nowak	Frida Zimmermann	Unterlagen	22.06.2020, 18:16	Postausgang

Tabelle 3.3: Thunderbird-Profil Thorben Nowak

Die letzte E-Mail von Herr Nowak, vom 22.06.2020 um 18:16 Uhr, sei an dieser Stelle beispielhaft aufgeführt:

To: naoyamamoto85@gmail.com From: Thorben Nowak <thorbennowak@fablab-zentrum.de>
Subject: Unterlagen Message-ID: <695934f6-b22b-7573-c9c7-f008ce84ae02@fablab-zentrum.de>
Date: Mon, 22 Jun 2020 18:16:16 +0200
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; rv:68.0) Gecko/20100101 Thunderbird/68.10.0 MIME-Version: 1.0
Content-Type: multipart/mixed; boundary="------------CD24AF6AEC15E0B956202614"
This is a multi-part message in MIME format. --------------CD24AF6AEC15E0B956202614
Content-Type: text/plain; charset=utf-8; format=flowed Content-Transfer-Encoding: 8bit

Guten Tag Frau Yamamoto
Da ich heute meinen letzten Arbeitstag habe, sende ich Ihnen noch schnell die Unterlagen.
Es ist alles so, wie wir es telefonisch besprochen haben.
Sie finden hier alle wichtigen Angaben, die Sie fÃ¼r die Story brauchen!
Bringen Sie die Story zeitnah, dann werden Sie es zu einer richtig grossen Zeitung schaffen â€“ versprochen.
Ich werde mich nun fÃ¼r eine Zeit absetzen. Versuchen Sie nicht mich zu kontaktieren.
Viel Erfolg!
Thorben

3.3.3 Bild-Datei

Es wurde die Datei *$I0G3KTO.jpeg* (keine EXIF-Informationen) im Papierkorb des Nutzers nowakth gefunden:

Abbildung 3.16: Katze in Käfig

3.3.4 Registry des Anwenders nowaktho

Die Analyse der Registry des Benutzers nowaktho zeigt, dass das Dokument *vertrag_gl_flzentrum_20200219.pdf* mit dem Profil aufgerufen wurde. Eine genauere Analyse müsste über ein entsprechendes Registry-Tool erfolgen.

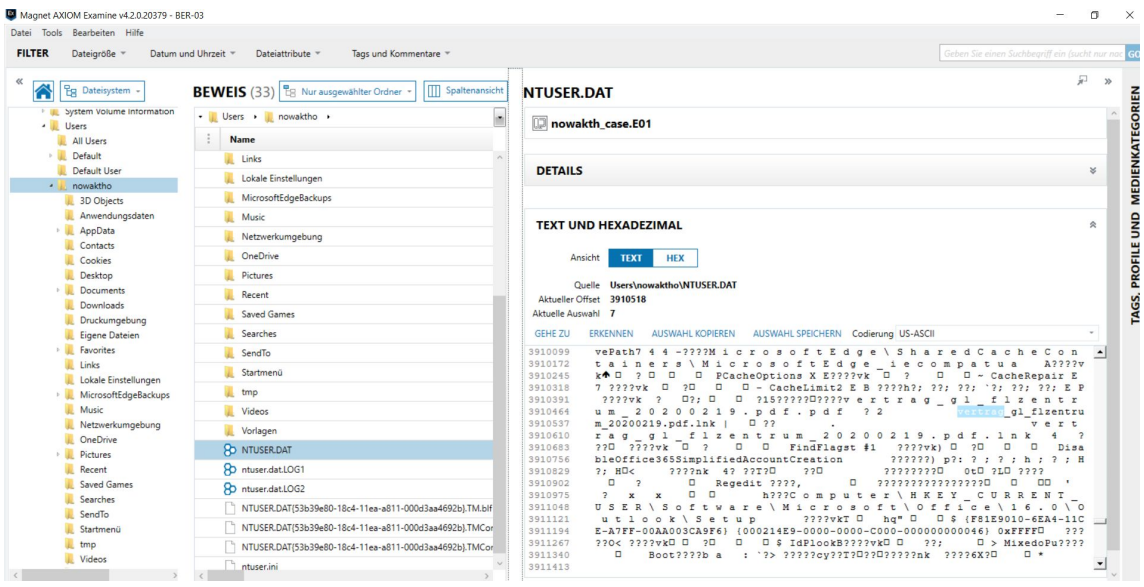


Abbildung 3.17: Auszug aus Windows Registry des Nutzers nowaktho

3.4 Abschliessende Dokumentation

Die Untersuchung des Asservates 03 führte zu folgenden Ergebnissen: Das Untersuchungsimage wurde von der Festplatte des zu untersuchenden Laptops erstellt und besass als installiertes Betriebssystem Windows 10. Im Betriebssystem existiert das Benutzerkonto nowaktho. Der Benutzer ist der einzige angelegte Benutzer auf dem Betriebssystem.

3.4.1 Falldarstellung auf der Zeitachse

Die Rekonstruktion der Abläufe auf einer Zeitachse erfüllt den Zweck, alle Geschehnisse übersichtlich zusammenzufassen. Es wurde aufgrund aller gefundenen Nachweise und Beweise eine zeitliche Einteilung aller Ereignisse vorgenommen und auf der nachfolgenden Zeitlinie abgetragen.

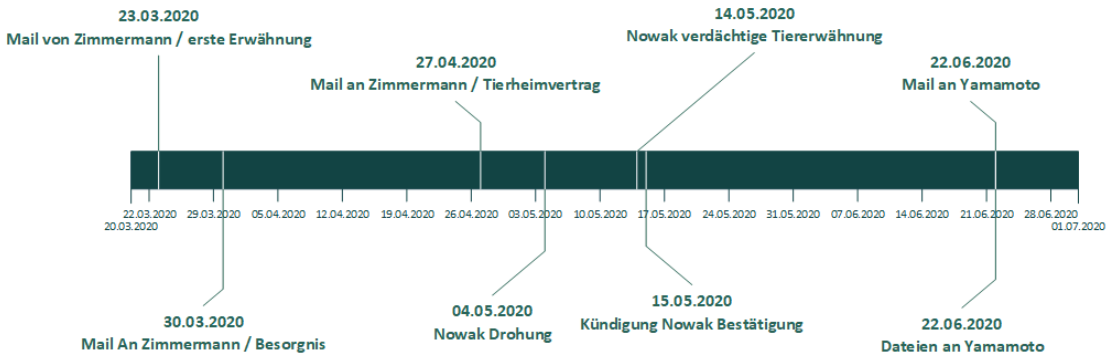


Abbildung 3.18: Darstellung der Ereignisse auf einer Zeitachse

Die Abbildung der erstellten Zeitachse wird durch die folgende Tabelle erläutert.

Datum	Typ	Name/Wert	Beschreibung
23.03.2020	Email	Von Frida Zimmermann	Die erste Erwähnung der Tierversuche im untersuchten Zeitraum.
30.03.2020	Email	An Frida Zimmermann	Nowak bekundet Besorgnis wegen der Versuche
27.04.2020	Email	An Frida Zimmermann	Nowak teilt Dateispeicherort eines Tierheimvertrages, erwähnt lokale Kopie
04.05.2020	Email	An Olivia Taylor	Nowak droht mit Bekanntmachung und Einleitung „notwendiger“ Schritte
14.05.2020	Email	An Frida Zimmermann	Nowak erwähnt Tieren „auf seine Art zu helfen“
15.05.2020	Email	Von Geschäfts-führung FabLab	Bestätigung des Erhalts der Kündigung zum 22.06.2020
22.06.2020	Papierkorb	Löschung	Nowak löscht Bilddatei Tierversuch_Katze.jpeg
22.06.2020	Email	An Nao Yamamoto	Nowak übermittelt Informationen zu Tierversuchen an Yamamoto
22.06.2020	Anhänge	An Nao Yamamoto	Forschungsbericht_FabLab_03_ Kan.docx
			Forschungsbericht_FabLab_04_ Kan.docx
			Forschungsbericht_FabLab_04_ Kat.docx
			Forschungsbericht_FabLab_05_ Kan.docx
			Forschungsbericht_FabLab_05_ Kat.docx
			Forschungsbericht_FabLab_06_ Kan.docx
			Forschungsbericht_FabLab_06_ Kat.docx
			vertrag_gl_flzentrum_ 20200219.pdf.pdf
			Bericht_Aufsichtsbehörde.docx
			Forschungsbericht_FabLab_01_ Kan.docx
			Forschungsbericht_FabLab_02_ Kan.docx

Tabelle 3.4: Zeitlich geordnete Ereignisse mit Beschreibung

3.4.2 Einordnung in die CERT Taxonomie

Die Einordnung in die CERT Taxonomie ermöglicht es, die gewonnen Erkenntnisse über den Vorfall zu Kategorisieren. Nachfolgend wurden die Erkenntnisse in eine grafische Darstellung der CERT Taxonomie übertragen.

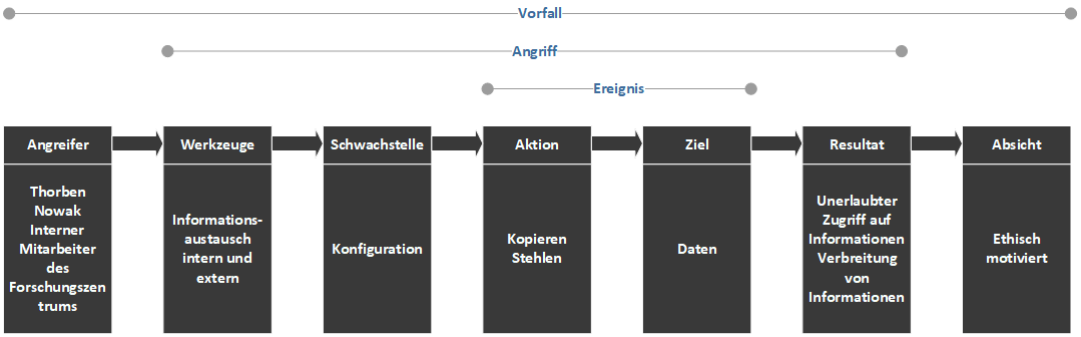


Abbildung 3.19: CERT Taxonomie Adaption für Fall NowakT

Aus der Abbildung der CERT Taxonomie geht hervor, dass der Angreifer, zur Zeit der Vorfalls, ein Mitarbeiter des Forschungszentrums war. Dieser kopierte, verteilte und veröffentlichte vertrauliche Informationen innerhalb und ausserhalb des Forschungszentrum. Er hatte Zugriff auf diese Informationen, da keine ausreichenden Zugriffsbeschränkungen auf die Ressourcen vorhanden waren. Er verfolgte die Absicht der Veröffentlichung der Daten aus ethischen Gründen.

3.4.3 Fallrückschlüsse

Nach der Auswertung der gewonnenen Erkenntnisse ist erkennbar, dass die Netzlaufwerke, welche vertrauliche Forschungsdaten enthalten, nicht ausreichend abgesichert sind und über keine Zugriffsbeschränkung verfügen. Zudem konnte der Täter unbemerkt mehrere dieser vertraulichen Dateien kopieren und versenden. Um zukünftig derartige Vorkommnisse zu vermeiden ist dringend eine strategische Vorbereitung in Betracht zu ziehen, die eine umfassende Ressourcen - Restriktionspolitik beinhaltet und vertrauliche Informationen durch einen Kopierschutz gegen das unerlaubte Replizieren schützt.

4 Bewertung der Ergebnisse

In den nächsten Zeilen möchten wir als Gruppe ein kritisches Fazit zu unserer Praktikumsarbeit ziehen und dabei unsere Erkentnisse offenlegen.

Unsere Arbeit begann bereits Ende März, als wir uns als Gruppe virtuell zusammen gesetz haben und unsere Gedanken zu der vorliegenden Aufgabenstellung sortierten und dokumentierten.
Eine der ersten Überlegungen, die wir uns machten, war die Wahl des Mediums, welches wir forensisch untersuchen und um welches wir dann einen stimmigen Fall herum fingieren wollten. Schnell war uns bewusst, dass wenn wir gemeinsam die Untersuchungen machen wollten und wir jeder für sich das Maximale an Wissensaufbau herausholen möchte, wir eine Lösung benötigen, die auch die rund 750km Luftlinie zwischen uns sowie Corona überwindet.
So entschieden wir uns für eine Windows-Virtualisierung auf einem Laptop eines Gruppenmitglieds, sodass jeder diese bequem per TeamViewer erreichen kann.
Zeitgleich zur Definiton des Mediums überlegten wir uns einen Fall den wir aufbauen wollten. Zu diesem Zeitpunkt waren wir noch in engerem Kontakt, sodass wir diese beiden Grundlagenpunkte im April festhalten konnten.
Kritisch betrachtet ware es wohl unser Zeitmanagement, welches uns an einem zügigen Vorankommen gehindert hat, denn richtig weiter gekommen sind wir erst im Juni wieder.
Wir haben stets darauf geachtet, ein strukturiertes Vorgehen zu wählen, welches alle Mitglieder des Teams gleichermassen involviert und gleichermassen zu Wissensaufbau führt. So waren alle drei von BER03 beim inhaltlichen Aufbau des fingierten „Arbeitsnotebooks“ des ehemaligen Mitarbeiters beteiligt. Zugegebenerweise haben wir den Aufwand für die Inszinierung des Falls etwas unterschätzt. Dokumente inhaltlich nahe der Realität zu fälschen, dabei auf den Ort der Erstellung und vor allem auf die Zeitstempel des Systems und des Windows typischen „letzter Zugriff“ zu achten - dabei berücksichtigen auf dem virtuellen System nicht zu viele Spuren zu hinterlassen, hat sich als hohen Aufwand erwiesen. Es ist an dieser Stelle schwierig zu sagen, was man besser hätte machen können, um nicht so viele Fussabdrücke im System zu hinterlassen. Jedoch haben wir nach Kennt-

nisnahme dieser Spuren einiges an Zeit investiert die Spuren zu verwischen, sodass sie bei der forensischen Analyse keine allzu negative Auswirkung haben sollten und die Aussagekraft mindern oder gar gefährden.

Als eine grössere Herausforderung hat sich das Fingieren der unterschiedlichen Emails herausgestellt. Diese begann bereits mit der Lizensierung und Installation des Officepakets. Das ursprünglich verwendete Microsoft Outlook hat nach automatischer Synchronisierung die Zeit des Mailservers verwendet, was wir leider erst bei der Betrachtung des erstellten Images in Axiom bemerkt haben. Somit wurden wir zeitlich etwas zurückgeworfen.
Doch schlussendlich haben wir alle Daten und Spuren so aufgebaut, wie wir sie für unseren Fall benötigten.
Dieser hier vorliegende Bericht wurde gemeinsam verfasst und gemeinsam redigiert. Für unsere zukünftigen Berichte und Arbeiten werden wir sicherlich unsere postiven und negativen Erfahrungen mitnehmen und berücksichtigen.

5 Definition *Fuzzing*

Als Fuzzing wird eine automatisierte Methode des Softwaretests bezeichnet.
Ziel ist es die Robusheit einer Software zu erhöhen, so dass sich die Software immer in einem definierten Zustand befindet und damit z.B. Sicherheitslücken der Software zu identifizieren.[1]

Entsprechende Anwendungen werden als Fuzzer bezeichnet und laufen in der Regel zyklisch in drei Schritten ab:

1. Als Eingabewert wird eine zufällige Abfolgen von Bits generiert oder eine definierte Abfolge von Bits wird zufällig modifiziert.
2. Der generierte Wert wird zum Test der Eingabeschnittstelle einer Software verwendet.
3. Abschließend wird das Verhalten der Software auf die Eingabe überprüft (Monitoring).

Um gefundene unerwünschte Zustände (Bugs) zusammenzufassen, können über die erfolgte Ausgabe des Systems z.B. Hashwerte gebildet werden. Dies vereinfacht die spätere Analyse und die Kategorisierung entsprechend der Kritikalität des jeweiligen Systemzustands. Das Monitoring kann hierzu zum Beispiel mit einem Bugtracker verbunden sein.
Unterschieden werden kann beim Fuzzing zwischen Blackbox- und Whitebox-Test. Bei ersterem, auch als "dump" Fuzzing bezeichnet ist über die zu testende Software dem Fuzzer nichts über deren Struktur bekannt und es werden völlig randomisierte Eingabewerte verwendet (z.B. aus /dev/urandom).

Fuzzern die Whitebox oder auch "smart" Fuzzing betreiben sind Parameter für die Eingabe vorgegeben, z.B. Dateitypen, Protokolle, etc.
Als Beispiel kann hier die Eingabe auf einem Formular zur Erfassung von Adressdaten dienen. Beim Blackbox Fuzzing kann es passieren, dass bestimmte Zustände in bestimmter Zeit nicht erreicht werden und zum Beispiel das Format einer

[1] Fuzzing von Embedded Software – Grundlagen und Erfahrungen (Stand: 26.01.2020)

Postleitzahl nicht gewissen Parametern entspricht. In Folge kann die Übermittlungsfunktion niemals aufgerufen werden.Fuzzing als Methode von Softwaretests gilt als kostengünstig im Einsatz. Mit ihr ist ein hoher zeitlicher Aufwand verbunden. Dieser kann jedoch durch Parallelisierung reduziert werden. Ebenfalls zeitaufwändig kann die Auswertung der Resultate sein, je nach Automatisierungsgrad des Monitorings bzw. Reportings.
Wie alle Testmethoden können auch mit Fuzzing nicht alle Fehler in einer Software gefunden werden

Abbildungsverzeichnis

1.1 Abschnitte des forensischen Prozesses nach BSI 5

2.1 Asservat-01 8
2.2 Asservat-02 9
2.3 Asservat-03 9
2.4 Beweismittelzettel 10

3.1 FTK Imager: Partitionsstruktur 15
3.2 FTK Imager: Vortschrittsanzeige bei der Image Erstellung 16
3.3 FTK Imager: Abschlussreport mit Hashwerten 16
3.4 AXIOM Process: Fallbeschreibung 18
3.5 AXIOM Process: Auswahl der Beweisquellen 19
3.6 AXIOM Process: Definition von Keywords 20
3.7 AXIOM Process: Auswahl der zu berücksichtigen Dateitypen . . . 20
3.8 AXIOM Examine: Fallübersicht 21
3.9 AXIOM Examine: Ermittelte Dokumente 21
3.10 AXIOM Examine: Inhalt von gelöschtem zip-Archiv 22
3.11 AXIOM Examine: gelöschte Bild-Datei 22
3.12 AXIOM Examine: Gefundene E-Mails und Anhängen 23
3.13 AXIOM Examine: Ergebnis der Keywordsuche 23
3.14 AXIOM Examine: Registry des Nutzers nowaktho 24
3.15 Auszug aus einem Forschungsbericht 26
3.16 Katze in Käfig 29
3.17 Auszug aus Windows Registry des Nutzers nowaktho 29
3.18 Darstellung der Ereignisse auf einer Zeitachse 30
3.19 CERT Taxonomie Adaption für Fall NowakT 32

Tabellenverzeichnis

2.1 Asservate 8

3.1 Partitionsstruktur 15
3.2 Übersicht Dokumente 25
3.3 Thunderbird-Profil Thorben Nowak 27
3.4 Zeitlich geordnete Ereignisse mit Beschreibung 31

Literaturverzeichnis

BSI, 2011 Bundesamt für Sicherheit in der Informationstechnik, Leitfaden „IT-Forensik
https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Cyber-Sicherheit/Themen/Leitfaden_IT-Forensik.pdf?__blob=publicationFile&v=2
03.2011

LEN, 2019 Lenovo, IdeaPad S740-15IRH Hardware Maintenance Manual
https://download.lenovo.com/consumer/mobiles_pub/lenovo_ideapad_s740-15irh_hmm_20190816.pdf
2019

Anhang

Bericht der Zulässigkeitsprüfung der Forschungen des FabLab Zentrum

Kennung der Behörde: AFB00XM

Datum der Prüfung: 29.04.2020

Grund der Prüfung: Quartalsbericht zur Einschätzung auf Zulässigkeit der Versuchsreihen

Die Prüfung wurde: Angekündigt

Detailbetrachtung

Angemeldete Versuchsreihe: AKAN001_AMZ

Angemeldete Tiere in dieser Reihe: KN11T, KN22T, KN33T

Auffälligkeiten: Es wurde ein Katzenklo in einem der Büroräume gefunden, jedoch keine Katze. Auf Nachfrage gelten diese als Haustiere und dürfen von den Mitarbeitern geregelt und abwechselnd mit zur Arbeit gebracht werden. Dabei muss der Mitarbeiter die ordentliche Entsorgung der Ausscheidungen gewährleisten.

Ergebnisse

Die Prüfung wurde erfolgreich bestanden. Es gibt keinen Grund zur Annahme zu gefälschten Unterlagen oder unangemeldeten Versuchen.

Versuchsprotokoll FabLab

Forschungsnummer: AKAN001

Kennung Aufsichtsbehörde: AFB00XM

Verantwortlicher Mitarbeiter: FabLab Junior Laborantin Frida Zimmermann

Versuchsreihe: AKAN001_AMZ

Frida Zimmermann FabLab Alzheimer Forschungszentrum

Protokoll

Versuchstierart:	Kaninchen
Kennungsnummer Tier:	KN11T
Blutgruppe:	0-
Datum Versuchsbeginn:	01.01.2020
Gesundheitszustand Versuchsbeginn:	keine Anzeichen einer Alzheimererkrankung

Versuchsdaten

Medikamenteninformationen

Name:	AZGENEHM
Datum der Verabreichung:	01.01.2020
Dosis der Verabreichung:	1 Ampulle

Beobachtungen

Nach 12 Stunden	keine Anzeichen von Einwirkungen des Medikaments auf das Versuchsobjekt
Nach 24 Stunden	KN11T hat keine Änderung des Organismus zu verzeichnen
Nach 48 Stunden	keine weiteren Änderungen

Ergebnis

Das Medikament löste keinerlei Wirkungen aus.

Somit war dieser Versuch erfolglos.

Versuchsprotokoll FabLab

Forschungsnummer: AKAN001

Kennung Aufsichtsbehörde: AFB00XM

Verantwortlicher Mitarbeiter: FabLab Junior Laborantin Frida Zimmermann

Versuchsreihe: AKAN001_AMZ

Frida Zimmermann FabLab Alzheimer Forschungszentrum

Protokoll

Versuchstierart:	Kaninchen
Kennungsnummer Tier:	KN22T
Blutgruppe:	0-
Datum Versuchsbeginn:	01.02.2020
Gesundheitszustand Versuchsbeginn:	bereits leichte Anzeichen einer Erkrankung

Versuchsdaten

Medikamenteninformationen

Name:	AZAWAY
Datum der Verabreichung:	01.02.2020
Dosis der Verabreichung:	2 Ampullen

Beobachtungen

Nach 12 Stunden	keine Anzeichen von Einwirkungen des Medikaments auf das Versuchsobjekt
Nach 24 Stunden	das Blutbild KN22T hat sich verändert
Nach 48 Stunden	KN22T hat eine Erkältung
Nach 72 Stunden	KN22T hat keine Erkältung mehr, das Blutbild hat sich normalisiert

Ergebnis

Das Medikament löste bei KN22T eine Immunreaktion aus, durch welche es eine Erkältung bekam. Nach der Erkältung normalisierte sich das Blutbild wieder. Die leichten Anzeichen einer Alzheimererkrankung blieben bestehen.

Somit war dieser Versuch erfolglos.

Versuchsprotokoll FabLab

Forschungsnummer: AKAN001

Kennung Aufsichtsbehörde: AFB00XM

Verantwortlicher Mitarbeiter: FabLab Junior Laborantin Frida Zimmermann

Versuchsreihe: AKAN001_AMZ

Frida Zimmermann FabLab Alzheimer Forschungszentrum

Protokoll

Versuchstierart:	Kaninchen
Kennungsnummer Tier:	KN33T
Blutgruppe:	0-
Datum Versuchsbeginn:	01.03.2020
Gesundheitszustand Versuchsbeginn:	Alzheimererkrankung wurde festgestellt

Versuchsdaten

Medikamenteninformationen

Name:	AZAWAY
Datum der Verabreichung:	01.03.2020
Dosis der Verabreichung:	3 Ampullen

Beobachtungen

Nach 12 Stunden	keine Anzeichen von Einwirkungen des Medikaments auf das Versuchsobjekt
Nach 24 Stunden	KN33T benimmt sich auffällig (rennt hin und her, frisst nicht mehr)
Nach 48 Stunden	KN33T verliert das Fell
Nach 60 Stunden	KN33T stabilisiert sich
Nach 72 Stunden	KN33T verfiel in einen komatösen Zustand
Nach 84 Stunden	KN33T wurde eingeschläfert

Ergebnis

Das Medikament wurde von KN33T abgestoßen und es löste verschiedene Reaktionen aus. Der Zustand verschlechterte sich zunehmend und der Versuch endete mit dem Einschläfern des bereits komatösen KN33T.

Dieser Versuch war erfolglos.

Versuchsprotokoll FabLab

Forschungsnummer: AKAN001

Kennung Aufsichtsbehörde: AFB00XM

Verantwortlicher Mitarbeiter: FabLab Junior Laborantin Frida Zimmermann

Versuchsreihe: AKAN001_AMZ

Frida Zimmermann FabLab Alzheimer Forschungszentrum

Protokoll

Versuchstierart:	Kaninchen
Kennungsnummer Tier:	KN22T
Blutgruppe:	0-
Datum Versuchsbeginn:	01.03.2020
Gesundheitszustand Versuchsbeginn:	leichte Anzeichen einer Alzheimererkrankung

Versuchsdaten

Medikamenteninformationen

Name:	AZAWAY
Datum der Verabreichung:	01.03.2020
Dosis der Verabreichung:	2 Ampulle

Beobachtungen

Nach 12 Stunden	Das Medikament ruft Änderungen im Blutbild hervor
Nach 24 Stunden	Das Blutbild verbessert sich
Nach 48 Stunden	Die Blutkörperchen verformen sich
Nach 72 Stunden	KN22T hat keine Anzeichen einer Alzheimererkrankung mehr, dafür jedoch offene Stellen in der Haut und Fellausfall

Ergebnis

Der Zustand verbesserte sich stetig, bis das Medikament eine Begleiterscheinung hatte. Es löste Fellausfall aus zerstörte mehrere Hautschichten durch Verformung der Blutkörperchen.

Dieser Versuch war ein teilweiser Erfolg.

Versuchsprotokoll FabLab

Forschungsnummer: AKAT001

Kennung Aufsichtsbehörde: AFB00XM

Verantwortlicher Mitarbeiter: FabLab Junior Laborantin Frida Zimmermann

Versuchsreihe: AKAT001_AMZ

Protokoll

Versuchstierart:	Katze
Kennungsnummer Tier:	KA11T
Blutgruppe:	0-
Datum Versuchsbeginn:	01.03.2020
Gesundheitszustand Versuchsbeginn:	leichte Anzeichen einer Alzheimererkrankung

Versuchsdaten

Medikamenteninformationen

Name:	AZAWAY
Datum der Verabreichung:	01.03.2020
Dosis der Verabreichung:	2 Ampulle

Beobachtungen

Nach 12 Stunden	Das Medikament ruft Änderungen im Blutbild hervor
Nach 24 Stunden	Das Blutbild verbessert sich
Nach 48 Stunden	Die Blutkörperchen verformen sich
Nach 72 Stunden	KA11T hat keine Anzeichen einer Alzheimererkrankung mehr, dafür jedoch offene Stellen in der Haut und Fellausfall

Ergebnis

Der Zustand verbesserte sich stetig, bis das Medikament eine Begleiterscheinung hatte. Es löste Fellausfall aus zerstörte mehrere Hautschichten durch Verformung der Blutkörperchen.

Dieser Versuch war ein teilweiser Erfolg.

Versuchsprotokoll FabLab

Forschungsnummer: AKAN001

Kennung Aufsichtsbehörde: AFB00XM

Verantwortlicher Mitarbeiter: FabLab Junior Laborantin Frida Zimmermann

Versuchsreihe: AKAN001_AMZ

Protokoll

Versuchstierart:	Kaninchen
Kennungsnummer Tier:	KN22T
Blutgruppe:	AB
Datum Versuchsbeginn:	01.04.2020
Gesundheitszustand Versuchsbeginn:	Alzheimererkrankung wurde bereits festgestellt

Versuchsdaten

Medikamenteninformationen

Name:	AZAWAY
Datum der Verabreichung:	01.04.2020
Dosis der Verabreichung:	3 Ampullen

Beobachtungen

Nach 12 Stunden	Das Medikament ruft Änderungen im Blutbild hervor
Nach 24 Stunden	Das Blutbild verbessert sich
Nach 48 Stunden	KN22T kann wieder allein trinken
Nach 72 Stunden	KN22T hat Anzeichen einer Alzheimererkrankung

Ergebnis

Der Zustand verbesserte sich stetig. KN22T konnte wieder allein Flüssigkeit aufnehmen, weitere Änderungen wurden jedoch nicht verzeichnet.

Dieser Versuch war ein teilweiser Erfolg. Bei einer Längeren Studie könnte das Medikament eventuell weitere Besserungen hervorrufen.

Versuchsprotokoll FabLab

Forschungsnummer: AKAT001

Kennung Aufsichtsbehörde: AFB00XM

Verantwortlicher Mitarbeiter: FabLab Junior Laborantin Frida Zimmermann

Versuchsreihe: AKAT001_AMZ

Protokoll

Versuchstierart:	Katze
Kennungsnummer Tier:	KA22T
Blutgruppe:	AB
Datum Versuchsbeginn:	01.04.2020
Gesundheitszustand Versuchsbeginn:	Alzheimererkrankung wurde bereits festgestellt

Versuchsdaten

Medikamenteninformationen

Name:	AZAWAY
Datum der Verabreichung:	01.04.2020
Dosis der Verabreichung:	3 Ampullen

Beobachtungen

Nach 12 Stunden	Das Medikament ruft Änderungen im Blutbild hervor
Nach 24 Stunden	Das Blutbild verbessert sich
Nach 48 Stunden	KA22T kann wieder allein trinken
Nach 72 Stunden	KA22T hat Anzeichen einer Alzheimererkrankung

Ergebnis

Der Zustand verbesserte sich stetig. KA22T konnte wieder allein Flüssigkeit aufnehmen, weitere Änderungen wurden jedoch nicht verzeichnet.

Dieser Versuch war ein teilweiser Erfolg. Bei einer Längeren Studie könnte das Medikament eventuell weitere Besserungen hervorrufen.

Versuchsprotokoll FabLab

Forschungsnummer: AKAN001

Kennung Aufsichtsbehörde: AFB00XM

Verantwortlicher Mitarbeiter: FabLab Junior Laborantin Frida Zimmermann

Versuchsreihe: AKAN001_AMZ

Frida Zimmermann FabLab Alzheimer Forschungszentrum

Protokoll

Versuchstierart:	Kaninchen
Kennungsnummer Tier:	KN33T
Blutgruppe:	AB+
Datum Versuchsbeginn:	01.05.2020
Gesundheitszustand Versuchsbeginn:	Alzheimererkrankung wurde bereits festgestellt

Versuchsdaten

Medikamenteninformationen

Name:	AZAWAY
Datum der Verabreichung:	01.05.2020
Dosis der Verabreichung:	3 Ampullen

Beobachtungen

Nach 12 Stunden	Das Medikament ruft keine Änderungen im Blutbild hervor
Nach 24 Stunden	Weiterhin keine Änderungen
Nach 48 Stunden	KN33T kann wieder allein laufen
Nach 72 Stunden	KN33T hat Anzeichen einer Alzheimererkrankung

Ergebnis

Der Zustand verbesserte sich stetig. KN33T konnte wieder allein Laufen, weitere Änderungen wurden jedoch nicht verzeichnet.

Dieser Versuch war ein teilweiser Erfolg. Bei einer Längeren Studie könnte das Medikament eventuell weitere Besserungen hervorrufen.

Versuchsprotokoll FabLab

Forschungsnummer: AKAT001

Kennung Aufsichtsbehörde: AFB00XM

Verantwortlicher Mitarbeiter: FabLab Junior Laborantin Frida Zimmermann

Versuchsreihe: AKAT001_AMZ

Protokoll

Versuchstierart:	Katze
Kennungsnummer Tier:	KA33T
Blutgruppe:	AB+
Datum Versuchsbeginn:	01.05.2020
Gesundheitszustand Versuchsbeginn:	Alzheimererkrankung wurde bereits festgestellt

Versuchsdaten

Medikamenteninformationen

Name:	AZAWAY
Datum der Verabreichung:	01.05.2020
Dosis der Verabreichung:	3 Ampullen

Beobachtungen

Nach 12 Stunden	Das Medikament ruft keine Änderungen im Blutbild hervor
Nach 24 Stunden	Weiterhin keine Änderungen
Nach 48 Stunden	KA33T kann wieder allein laufen
Nach 72 Stunden	KA33T hat Anzeichen einer Alzheimererkrankung

Ergebnis

Der Zustand verbesserte sich stetig. KA33T konnte wieder allein Laufen, weitere Änderungen wurden jedoch nicht verzeichnet.

Dieser Versuch war ein teilweiser Erfolg. Bei einer Längeren Studie könnte das Medikament eventuell weitere Besserungen hervorrufen.

Kaufvertrag

Auftraggeber:

FabLabZentrum

Industriestrasse 96

79108 Freiburg

Auftragnehmer:

Tierheim Glückes Baare

Industriestrasse 1a

79108 Freiburg

Inhalt des Vertrags:

Die Auftragnehmerin verpflichtet sich zu einer monatlichen Lieferung von Katzen, die folgenden Kriterien entsprechen:

- Jungen Alters, maximal 1.5 jährig
- Ohne Vorerkrankung
- Ohne aktuelle Erkrankung

Die Bedingungen des Kaufvertrages hinsichtlich Qualität, Lieferfristen, Verschwiegenheit und sonstige Bedingungen, befinden sich in der separaten Anlage [Ref.01].

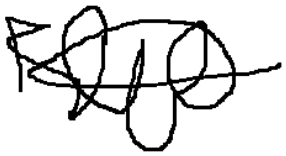
Die Auftraggeberin zahlt innert 30-tägiger Frist pro übermitteltem Tier, den vereinbarten Wert von 2’000 (Zwei-Tausend) Euro.

Das Retournieren von Tieren (lebend, verstorben) ist ausgeschlossen.

Bei Verzug einer Lieferung greifen die in [Ref.01] hinterlegten Bedingungen.

Der Vertrag ist gültig ab 19.02.2020 und endet per 31.12.2021 automatisch.

Auftraggeber
Dr. O. Taylor
FabLab Zentrum



Auftragnehmer
B. Ludwig
Tierheim Glückes Baare

Betreff: AW: Vergangenes Wochenend
Von: Frida Zimmermann <fridazimmermann@fablab-zentrum.de>
Datum: 23.03.2020, 09:19
An: thorbennowak@fablab-zentrum.de

Thorben, mit ging es wie dir am Sonntag 🙂

Und ich finde es super mutig, dass du mich gefragt hast. Auch wenn wir uns noch nicht lange kennen, freue ich auf die nächste Gelegenheit, wenn wir uns außerhalb der Arbeit sehen werden.

Bis gleich beim Essen,
F.

PS: Hast du mitbekommen, was bei den Tierversuchen los ist?

Betreff: Experimente mit Versuchstieren
Von: Thorben Nowak <thorbennowak@fablab-zentrum.de>
Datum: 30.03.2020, 10:20
An: fridazimmermann@fablab-zentrum.de

Hey Frieda,

ich habe mich, aufgrund deiner Anmerkung der Versuchstiere, beim Rauchen mit einem Laborassi unterhalten. Dieser gab mir den Tip mir die Dokumente der Aufsichtsbehörde anzuschauen bezüglich der bewilligten Tierarten. Ich weiß nicht ob du das gemeint hast, aber wir haben für die Katzen gar keine Genehmigung! Ob das mit Olivias Einwilligung geschieht?! Anders kann ich mir das nicht erklären.

Ich bin höchst besorgt, denn dafür bin ich nicht in die Forschung gegangen!

Sehen wir uns später?

In Liebe,

Thorben

Betreff: Vertragsdokument "vertrag_gl_flzentrum_20200219.pdf" auf Gruppenlaufwerk
Von: Thorben Nowak <thorbennowak@fablab-zentrum.de>
Datum: 27.04.2020, 12:52
An: fridazimmermann@fablab-zentrum.de

Frieda,

ich habe den Beweis gefunden! Im Gruppenlaufwerk liegt ein Vertrag, den FLZ mit dem lokalem Tierheim „Glückes Baare“ unterzeichnet hat.

Der Pfad lautet X:_extern_2020\vertraege_gb\vertrag_gl_flzentrum_20200219.pdf

Ich habe mir die Datei aber auch lokal gesichert und werde sie mir später nochmal ausdrucken.

Ich bin gespannt was du dazu sagst!

Dein Thorben

Betreff: WG: Resultat der Begehung am 29. April 2020
Von: Olivia Taylor <oliviataylor@fablab-zentrum.de>
Datum: 29.04.2020, 18:40
An: thorbennowak@fablab-zentrum.de

Datum: 29.04.2020 18:40
Von: oliviataylor@fablab-zentrum.de
An: thorbennowak@fablab-zentrum.de
Betreff: WG: Resultat der Begehung am 29. April 2020

Liebe Mitarbeiter,

wie nicht anders zu erwarten war, haben wir die behördlichen Anforderungen an die Tierversuche in unserer Abteilung erfüllt und können mit diesen weitere drei Jahre fortfahren.

Ich danke allen für Ihre Mitarbeit.

Mit besten Grüße,

Olivia Taylot

-------- Weitergeleitete Nachricht --------
Datum: 29.04.2020 17:29
Von: referatsleitung_ref35@rps.bwl.de
An: oliviataylor@fablab-zentrum.de
Betreff: Resultat der Begehung am 29. April 2020

Sehr geehrte Frau Taylor,

in Anbetracht des Eindruckes, den wir auf der heute Besichtigung hinsichtlich des Umgangs mit Versuchstieren und deren Haltungsbedingungen erhalten haben,
freue ich mich Ihnen die Genehmigung, nach § 8 TierSchG, seiten des Regierungspräsidium Stuttgarts, erteilen zu dürfen.

Mit besten Grüßen,

Magnus Wienfried

Referatsleiter
Referat 35 - Veterinärwesen, Lebensmittelüberwachung
https://rp.baden-wuerttemberg.de/rps/Abt3/Ref35

Betreff: Begehung unseres Referats durch das Regierungspräsidium Stuttgart
Von: Thorben Nowak <thorbennowak@fablab-zentrum.de>
Datum: 30.04.2020, 12:51
An: fridazimmermann@fablab-zentrum.de

Meine Frida,

das ganze kommt mir mittlerweile vor wie eine Farce?

Wie du ja sicher mitbekommen hast, hat uns das das entsprechende Referat des Regierungspräsidium Stuttgarts geprüft und keine(!!!) Unregelmäßigkeiten festellen können.

Ich weiß du wolltest heute Hbend mit Maja zum Sport, aber bitte können wir uns heute Abend sehen?

Hoffentlich bis später,

Thorben

Betreff: Tierversuche im Referat Alzheimerforschung 1
Von: Thorben Nowak <thorbennowak@fablab-zentrum.de>
Datum: 04.05.2020, 20:30
An: oliviataylor@fablab-zentrum.de

Frau Taylor

Über die letzten Monate habe ich stets weg geschaut und meine Arbeit nach Vorschrift gemacht.

Ich habe Ihnen und Frau Zimmermann assistiert und auch dabei unterstützt die «anderen» Tiere zu füttern und Bluttests an ihnen vorzunehmen.

Ich halte es jedoch nicht mehr aus. Sie wissen, dass dies nicht richtig und in keiner Weise ethisch vertretbar ist. Die Aufsichtsbehörde an der Nase herumzuführen ist ein weiterer Faktor, den ich nicht mit mir und meiner Wertvorstellung in Einklang bringen kann. Sie Spielen mit dem Leben, als wäre es Ihnen nichts wert. Glauben Sie wirklich daran einen Durchbruch in der Alzheimer-Forschung zu erzielen und dabei ungehindert so weiter zu machen – und glauben Sie wirklich Niemand wird diesen Betrug, diese ungeheuerliche und abstossende Tat nicht bemerken?

Mir ist durchaus bewusst, dass ich als PhD-Student in der Hackordnung sehr weit unten rangiere. Aber das hält mich nicht davon ab, auf Unrecht hinzuweisen und falls nötig die notwendigen Schritte einzuleiten.

Ich werde nicht mehr weiter zuschauen. Ich bitte, nein ich empfehle Ihnen, dass Sie diesen Taten ein Ende bereiten. Ansonsten sehe ich mich gezwungen an entsprechender Stelle auf Ihne Methoden hinzuweisen. Das FabLab Zentrum ist ein renommiertes Forschungszentrum und weltweit anerkannt. Setzen Sie diesen Ruf nicht aufs Spiel. Ich weiss durchaus, an wen ich mich in dieser Institution vertrauensvoll wenden kann, sodass diesem Spuk ein Ende gesetzt wird.

Mit freundlichen Grüssen

Thorben Novak

PhD-Student

Alzheimerforschung 1

FabLab Zentrum

Betreff: AW: Tierversuche im Referat Alzheimerforschung 1
Von: Olivia Taylor <oliviataylor@fablab-zentrum.de>
Datum: 05.05.2020, 07:25
An: thorbennowak@fablab-zentrum.de

Lieber Thorben

Vielen Dank für deine Nachricht.

Ich verstehe dich sehr gut und ich kann fühlen, dass es dich irritiert. Aber du musst es so sehen: Wir retten Leben – wir zerstören hier keine!

Denkst du, es ist ethisch vertretbarer, dass einem jungen Menschen nicht rechtzeitig, in einem frühen Stadium, eine Diagnose gestellt wird und deshalb erst viel zu spät etwas gegen den aufhaltsamen Verlauf unternommen werden kann? Der junge Mensch ist von uns und unserer Forschung abhängig, genauso wie Milliarden anderer Menschen auf dieser Welt. Sie setzen all ihre Hoffnung in uns und in unsere Arbeit, die wir stolz jeden Tag verrichten. Wir kommen dem Ziel immer näher. Möchtest du das alles aufs Spiel setzen? Möchtest du etwa nicht, dass das «dahin vegetieren» aufgehalten werden kann? Denk an die Qualen, die dein Grossvater erleben musste. Du selbst hast mir diese traurige Geschichte zu Beginn deiner Zeit hier im FabLab erzählt.

Im Grunde genommen bist du eine Enttäuschung für mich.

Ich habe so viel Zeit und Nerven, ja sogar Geld in dich und deine Ausbildung gesteckt, weil du keine Eltern mehr hast. Du könntest Grosses erreichen – und das ist der Dank dafür?

Du vergisst, was das Grosse und Ganze ist. Hier geht es nicht um dich und auch nicht um mich.

Nein, ich revidiere meine Meinung: ich verstehe dich nicht.

Solltest auch nur im Ansatz versuchen die Forschungsreihe zu sabotieren oder einen Versuch unternehmen, die Leitung des Zentrums zu informieren, wird nicht nur deine Karriere ein jähes Ende nehmen, sondern ich werde alles daran setzen, dass du nicht einmal mehr als Hausmeister einen Job bekommst. Überlege es dir also gut!!!

Solltest du wieder zur Vernunft kommen, dann steht meine Bürotür wie gewohnt für dich offen und wir vergessen deine Kinderei.

Liebe Grüsse,
Olivia

Betreff: Taten statt Worte
Von: Thorben Nowak <thorbennowak@fablab-zentrum.de>
Datum: 14.05.2020, 18:21
An: fridazimmermann@fablab-zentrum.de

Liebste Frida,

auch nachdem wir viele Abend unsere Argumente ausgetauscht haben habe das Gefühl meine Herz und mein Kopf explodieren bei dem Gedanken nichts zu tun. Nach langer Überlegung habe mich entscheiden den Tieren auf meine Art zu helfen.

Mehr musst du nicht wissen.

In Liebe,

Thorben

Betreff: Kündigungsbestätigung
Von: Geschäftsführung FabLab-Zentrum <geschaeftsfuerung@fablab-zentrum.de>
Datum: 15.05.2020, 09:03
An: thorbennowak@fablab-zentrum.de

Sehr geehrter Herr Novak

Wir haben die Bestätigung darüber erhalten, dass Ihnen die Kündigung Seitens FabLab Zentrum zugestellt wurde.

Aus diesem Grund möchten wir Sie hiermit nochmals daran erinnern folgende Tätigkeiten an Ihrem letzten Arbeitstag 22.06.2020 durchzuführen:

Abgabe des Laptops

Abgabe des Badges

Abgabe der Schlüssel zu den Medizinschränken

Räumung ihres persönlichen Schrankabteils, inklusive Reinigung dessen

Sämtliche Abgaben können über den Empfang im Gebäude A, spätestens bis 18:00 Uhr, vollzogen werden. Sollten die Gegenstände bist zu dieser Uhrzeit nicht eingetroffen und registriert sein, werden wir uns vorbehalten einen Mitarbeiter des Sicherheitsdiensts für das Herausbegleiten zu beordern.

Ich bedanke mich im Voraus und wünsche Ihnen für Ihre Zukunft alles Gute.

Mit freundlichen Grüssen

Kasimir Huber

Assistenz der Geschäftsleitung

FabLabZentrum

Betreff: Unterlagen
Von: Thorben Nowak <thorbennowak@fablab-zentrum.de>
Datum: 22.06.2020, 18:16
An: naoyamamoto85@gmail.com

Guten Tag Frau Yamamoto

Da ich heute meinen letzten Arbeitstag habe, sende ich Ihnen noch schnell die Unterlagen.

Es ist alles so, wie wir es telefonisch besprochen haben.

Sie finden hier alle wichtigen Angaben, die Sie für die Story brauchen!

Bringen Sie die Story zeitnah, dann werden Sie es zu einer richtig grossen Zeitung schaffen – versprochen.

Ich werde mich nun für eine Zeit absetzen. Versuchen Sie nicht mich zu kontaktieren.

Viel Erfolg!

Thorben

Anhänge:

Forschungsbericht_FabLab_03_Kan.docx	23,2 KB
Forschungsbericht_FabLab_04_Kan.docx	23,2 KB
Forschungsbericht_FabLab_04_Kat.docx	23,1 KB
Forschungsbericht_FabLab_05_Kan.docx	23,3 KB
Forschungsbericht_FabLab_05_Kat.docx	23,9 KB
Forschungsbericht_FabLab_06_Kan.docx	23,0 KB
Forschungsbericht_FabLab_06_Kat.docx	23,4 KB
vertrag_gl_flzentrum_20200219.pdf.pdf	104 KB
Bericht_Aufsichtsbehörde.docx	20,9 KB
Forschungsbericht_FabLab_01_Kan.docx	23,2 KB
Forschungsbericht_FabLab_02_Kan.docx	23,0 KB