Hochschule Wismar
Studiengang Master „IT-Sicherheit und Forensik“
Modul „Forensik in Betriebssystemen und Anwendungen“

Praktikumsbericht

Gruppennummer: HH-03

Tim Kläs
Jens Knispel
Samuel Philipp

31. Juli 2019

Inhaltsverzeichnis

1 Einleitung **1**

2 Vorbereitung und Durchführung des Szenarios **2**
2.1 Einrichtung der virtuellen Maschine . . . 2
2.1.1 Betriebssysteminstallation . . . 2
2.1.2 Installation und Konfiguration der Software . . . 3
2.2 Erzeugung der Fall-Daten . . . 6
2.3 Ablauf des Szenarios . . . 7

3 Erzeugen der forensischen Abbilder **9**
3.1 Vorbereitung . . . 9
3.2 Datensammlung . . . 9
3.2.1 Hauptspeicherabbild . . . 9
3.2.2 Festplattenabbild . . . 10

4 Forensische Analyse **13**
4.1 Anlegen des Falles mit Axiom Process . . . 13
4.2 Einlesen der Beweisquellen . . . 14
4.2.1 Hauptspeicherabbild . . . 14
4.2.2 Windows-Festplattenabbild . . . 14
4.3 Verarbeitungsoptionen . . . 15
4.4 Auswahl der Artefakte . . . 15
4.5 Beweisanalyse . . . 15
4.6 Auswertung des Falles mit Axiom Examine . . . 16
4.6.1 Untersuchung der Microsoft Registry . . . 16
4.6.2 Installierte Software . . . 17
4.6.3 Medien und Dokumente . . . 18
4.6.4 Versteckte Ordner . . . 21
4.6.5 Gelöschte Dateien . . . 21
4.6.6 E-Mail . . . 22
4.6.7 FTP-Client . . . 23
4.7 Rekonstruierte Zeitachse . . . 25

5 Fazit **26**
5.1 Beweisanalyse . . . 26
5.2 Gesamtprojekt . . . 26

Abbildungsverzeichnis

1 Konfiguration der Festplattengröße der VM . . . 2
2 Zusammenfassung der Konfiguration der VM . . . 3
3 Auswahl der Festplatte für die Betriebssysteminstallation . . . 3
4 Anlegen des System Administrators Teutates . . . 4
5 Installation des FileZilla Servers . . . 5
6 Konfiguration des FileZilla Servers . . . 5
7 FileZilla Client . . . 7
8 Konfiguration des Hauptspeicherabbilds . . . 9
9 Fortschritt der Erzeugung des Hauptspeicherabbilds . . . 10
10 Auswahl der Festplatte zur Erzeugung des Abbilds . . . 10
11 Auswahl des Abbild-Typs . . . 11
12 Konfiguration des Festplattenabbilds . . . 11
13 Fortschritt der Erzeugung des Festplattenabbilds . . . 12
14 Schritte der Image Erstellung . . . 13
15 Auswahl der Beweisquellen unter Windows . . . 14
16 Image E01 Speicherbereiche . . . 14
17 Auswahl von Keywords . . . 15
18 Artefakte: Dokumente . . . 15
19 Durchführung der Beweisanalyse . . . 16
20 Übereinstimmungen des Keywords . . . 16
21 Angelegte Benutzer . . . 17
22 Auszug: Registrierte USB-Sticks MS Registry . . . 17
23 Installierte Programme . . . 18
24 Abgelegte Dokumente . . . 19
25 Übereinstimmungen mit Keyword *FTP* . . . 19
26 Modifiziertes Dokument . . . 20
27 Veränderte Zaubertrankformel . . . 20
28 Hash des des Original-Dokuments . . . 21
29 Dateien innerhalb des Papierkorbs . . . 22
30 Übersicht des Mailverlaufs . . . 22
31 Auszug: Detail-Ansicht E-Mail . . . 22
32 E-Mail: Von Idefix an Caesar . . . 23
33 Durchführung der Beweisanalyse . . . 23
34 Auszug: Registrierte Benutzer des FTP Servers . . . 23
35 Auszug: Log-File - Herunterladen und Löschen von Dateien . . . 24
36 Ausschnitt: Download der Zaubertrankformel . . . 24
37 Troubadix: Upload der Maildaten . . . 24
38 Dokumente der Zeitachse . . . 25
39 Eigene Darstellung: Rekonstruierte Zeitachse . . . 25

1 Einleitung

Für die vorliegende Praktikumsarbeit wird ein Szenario erstellt, dass im späteren Verlauf forensisch untersucht und bewertet wird. Der folgende Fall bildet das entwickelte Szenario.

Ein interner Server der gallischen Provinz „Das Dorf“ wird, auf Grund eines Tipps von *Troubadix*, einem Mitarbeiter der Dorfverwaltung, untersucht. Auf diesem Server arbeiten einige Bewohner des Dorfes. Auf dem Server liegen die verschiedensten Daten der Dorfverwaltung. In sämtlichen Dateiformaten werden geheime und interne Daten abgelegt.

Der Tippgeber gibt an, einen Teil von einer E-Mail Konversation gefunden und anschließend auf den Server hochgeladen zu haben. Das Hochladen der E-Mails geschah am 09.07.2019. Der Tipp selber wurde am 10.07.2019 gegeben. Dieser Ausschnitt des E-Mail Verkehrs belastet einen weiteren Mitarbeiter *Idefix* der Stadtverwaltung. Dieser soll intere Dokumente heruntergeladen und anschließend an die Römer weitergeben haben. Darüber hinaus wurden Dokumente manipuliert und gelöscht, so auch das schützendswerteste Geheimnis, die Zaubertrankformel. Direkt am 11.07.2019 wird die Ermittlung aufgenommen und die forensische Untersuchung eingeleitet.

In der folgenden Arbeit wird dieses Szenario in einer virtuellen Maschine (VM) erzeugt. Anschließend wird mit dem FTK-Imager Tool ein Abbild des Server-Datenträgers erstellt. Danach wird das Abbild mit Hilfe von der Forensik-Software *MAGNET AXIOM* untersucht. Darauf folgt eine detaillierte Dokumentation der einzelnen Schritte der Untersuchung und Präsentation der Ergebnisse.

2 Vorbereitung und Durchführung des Szenarios

Die erforderlichen Vorbereitungen zur Durchführung des Szenarios umfassen das Bereitstellen des Systems auf dem sich das Szenario abspielt und die Erzeugung der verschiedenen Fall-Daten, die auf dem System abgelegt werden sollen.

2.1 Einrichtung der virtuellen Maschine

Für die Umsetzung des Szenarios ist es notwendig eine VM bereitzustellen. Als Hypervisor (Typ-2, hosted) wird ein *VMware Workstation Player* eingesetzt. Auf der VM wird im Folgenden ein Windows 10 Betriebssystem aufgesetzt, sowie die notwendige Software zur Durchführung der Aufgabenstellung installiert.

2.1.1 Betriebssysteminstallation

Um das Betriebssystem in einer VM zu installieren muss zunächst die VM selbst erstellt werden. Hierfür wird im *VMware Player* die Option *Create a New Virtual Machine* genutzt und die entsprechende ISO Datei ausgewählt. Im nächsten Schritt muss die Größe der Festplatte festgelegt werden. Der *VMware Player* empfiehlt eine Größe von 60 Giga Byte für Windows Maschinen. Wie Abbildung 1 zeigt wurde für dieses Szenario eine Größe von 13 Giga Byte festgelegt, um das zu analysierende Abbild so klein wie möglich zu halten. So können die Übertragungs- und Analysezeiten etwas minimiert werden.

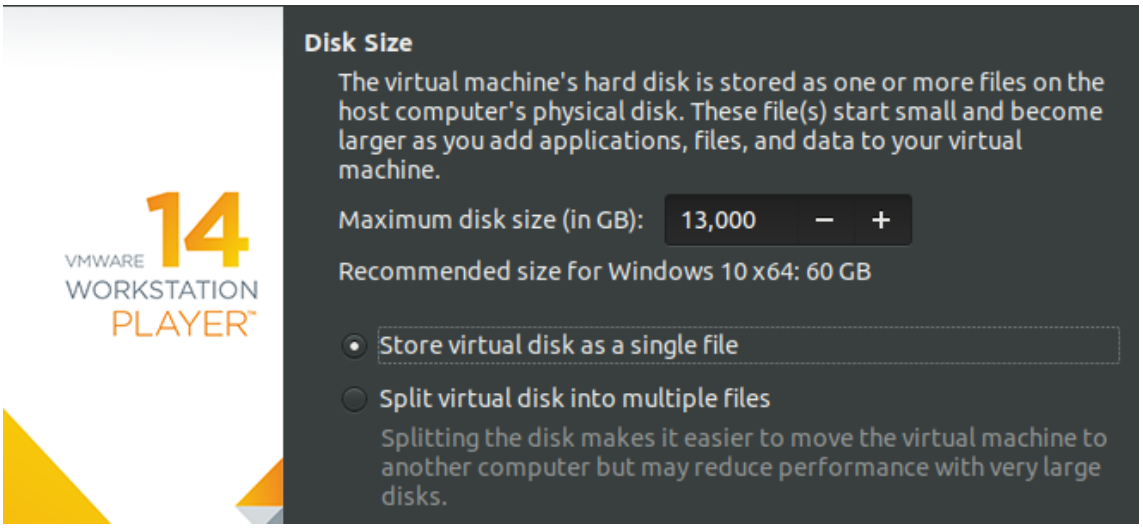

Abbildung 1: Konfiguration der Festplattengröße der VM

Nachdem die Festplattengröße definiert ist zeigt der *VMware Player* eine Zusammenfassung der konfigurierten Parameter für die zu erstellende VM an. Diese ist in Abbildung 2 dargestellt. In der Ansicht können die Parameter noch einmal verändert werden. Für die VM dieses Berichts wurde ein Giga Byte Arbeitsspeicher festgelegt, um auch hier die Analysezeit möglichst gering zu halten.

Der *VMware Player* startet abschließend die VM in der nun das entsprechende Betriebssystem installiert werden kann. Dafür wird die VM zunächst vom virtuellen CD Laufwerk gestartet, in dem die ausgewählte ISO Datei für die Installation bereitgestellt wird. Nun folgt die Installation von Windows 10, wie sie auch auf einem handelsüblichen Rechner durchgeführt werden könnte.

Abbildung 2: Zusammenfassung der Konfiguration der VM

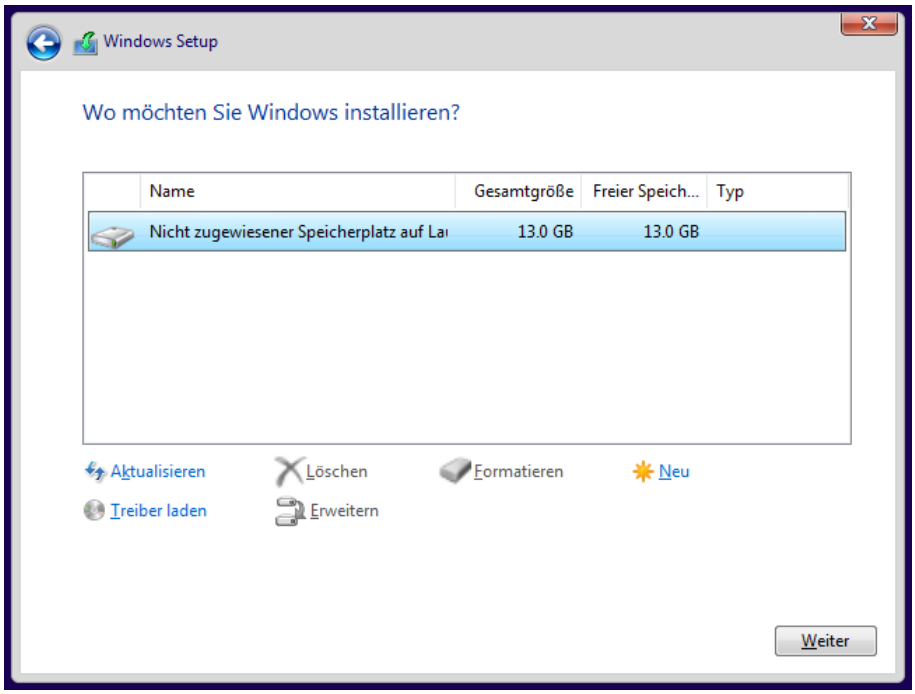

Abbildung 3: Auswahl der Festplatte für die Betriebssysteminstallation

Nach dem Start der Installation, der Auswahl von *Windows 10 Home* als Betriebssystem und des Akzeptierens der Datenschutzbestimmungen muss die Festplatte ausgewahlt werden auf der das System installiert wird. Hier wird, wie Abbildung 3 zeigt, die im voraus für die VM erstellte 13 Giga Byte große Festplatte ausgewählt. Anschließend wird *Windows 10* in der VM installiert. Die Installation wird mit dem Anlegen des Administrator-Benutzers abgeschlossen.

Auf dem neuen System wird ein Offlinekonto für den Benutzer *Teutates* mit dem Passwort *teutates* angelegt. Abbildung 4 zeigt diesen Vorgang. Dieser verwaltet das System und unter seinem Namen wird im Folgenden die notwendige Software installiert.

2.1.2 Installation und Konfiguration der Software

Nachdem *Windows 10* erfolgreich installiert ist wird nun ein File Transfer Protocol (FTP) Server installiert, über den die Nutzer Daten mit dem Rechner austauschen können. Hierfür wird der In-

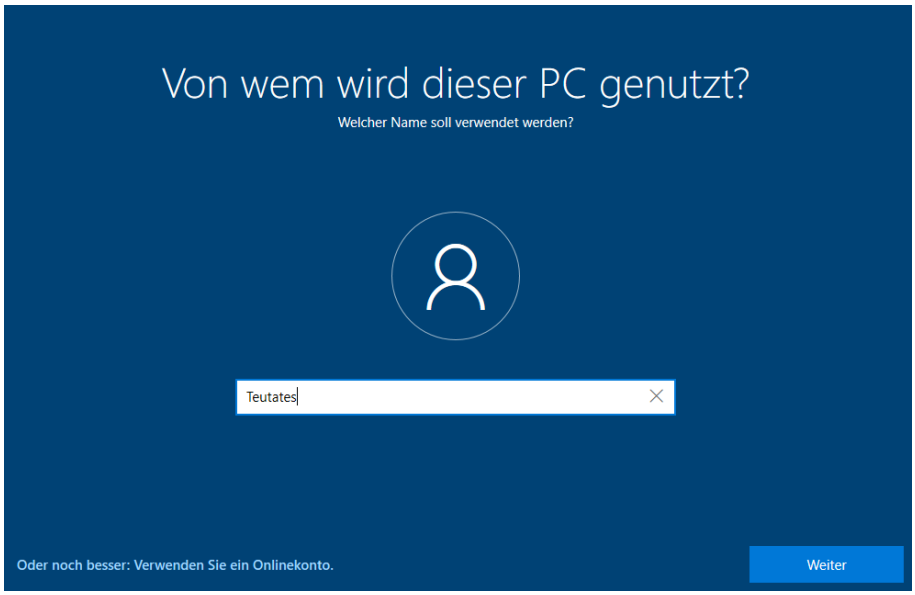

Abbildung 4: Anlegen des System Administrators Teutates

staller von der offiziellen Webseite (`https://filezilla-project.org/download.php?type=server`) herunter geladen und gestartet. Für die Installation des FTP-Servers können verschiedene Module ausgewählt werden, wie Abbildung 5 zeigt. Für dieses Szenario wurde der Server selbst, das Administrator interface, die Shortcuts und das Desktop Icon installiert.

Nachdem die Installation abgeschlossen ist wird der FTP-Server automatisch gestartet und kann konfiguriert werden. Für dieses Szenario werden sechs Benutzer zur Nutzung des FTP-Servers angelegt:

- majestix
- asterix
- obelix
- idefix
- miraculix
- troubadix

Für jeden Nutzer wird ein entsprechendes Passwort festlelegt. Abbildung 6 zeigt die Konfiguration für den Nutzer `miraculix`.

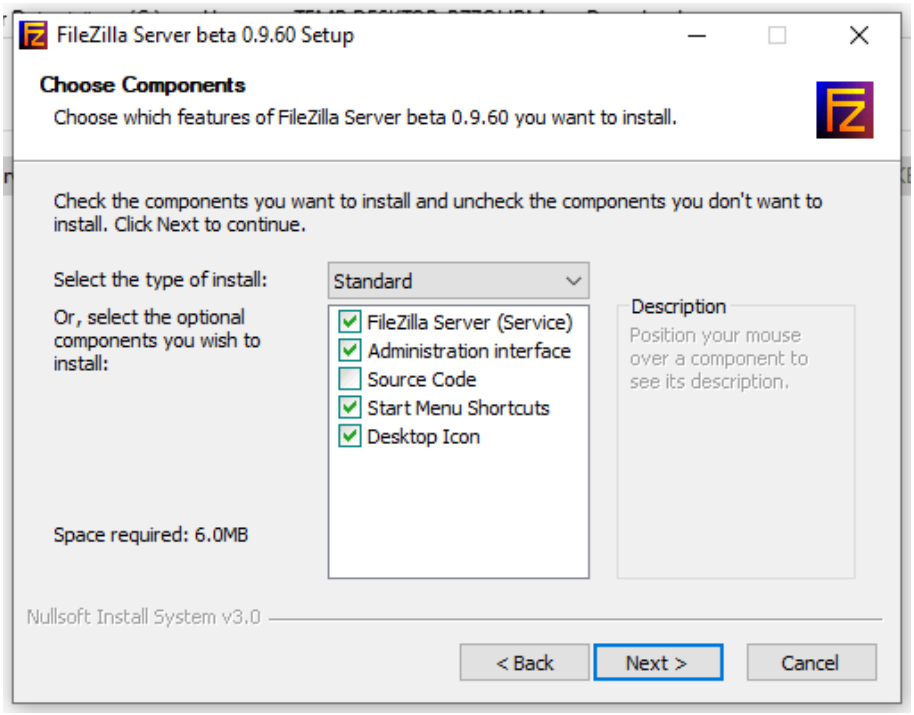

Abbildung 5: Installation des FileZilla Servers

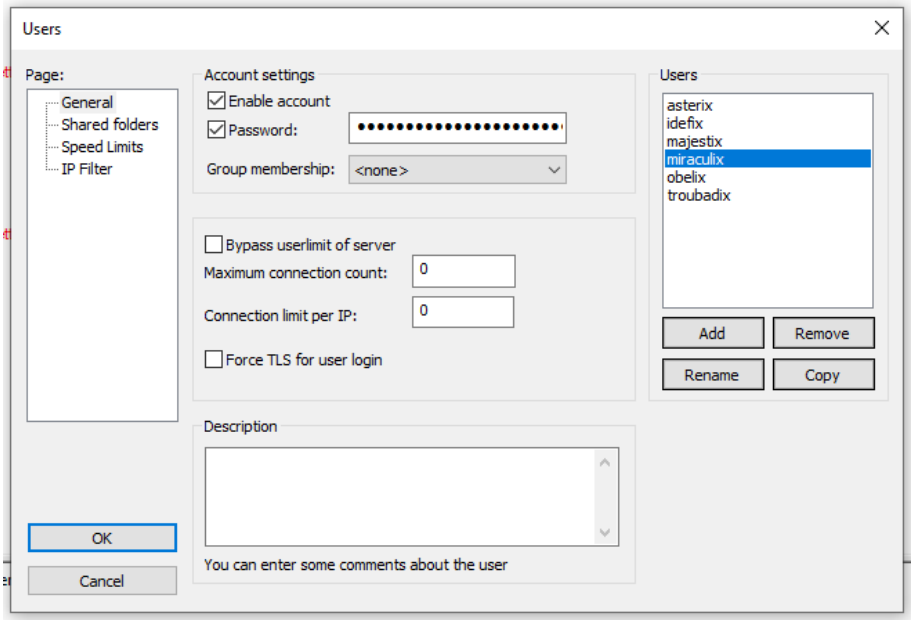

Abbildung 6: Konfiguration des FileZilla Servers

Außerdem wird für jeden Nutzer ein Basis-Verzeichnis angegeben. Für dieses Szenario haben alle Nutzer das selbe Verzeichnis um einen Dateiaustausch einfach möglich zu machen. Das Verzeichnis ist `C:\Users\Teutates\FTP`. Jeder Nutzer hat zusätzlich alle Berechtigungen (Dateien lesen und schreiben, sowie Verzeichnisse erstellen, löschen oder Inhalte auflisten) um Dateien hochladen und herunterladen zu können.

Abschließend wurde die Firewall des Systems soweit eigeschränkt um externe Verbindungen zum FTP-Server zuzulassen. Dadurch können die Nutzer ihren jeweiligen FTP-Client nutzen um mit dem Server zu interagieren.

2.2 Erzeugung der Fall-Daten

Es werden Ordnerstrukturen und Daten für die Verwaltung einer gallischen Provinz angelegt. Zusätzlich zu den öffentlichen Ordnern werden versteckte Verzeichnisse angelegt, auf denen im geheimen Daten ausgetauscht werden. Die folgenden Ordner sind angelegt, zusätzlich werden die jeweilig zuständigen Mitarbeiter aufgeführt:

Öffentlich:

- Bildung - Troubadix & Miraculix
- Buchhaltung - Majestix & Asterix
- Exportwaren - Asterix & Miraculix
- Gallierverzeichnis - Majestix & Miraculix
- Importwaren - Troubadix & Obelix
- Kundgebungen - Asterix & Majestix
- Versammlungsprotokolle - Idefix, Obelix & Troubadix
- Verteidigungsstrategien - Obelix, Asterix, Miraculix

Geheim:

- .Bilder - Asterix, Obelix, Idefix
- .Daten - Asterix, Obelix, Idefix
- .Musik - Asterix, Obelix, Idefix

Es werden Dateien die zur Verwaltung notwendig sind exemplarisch für das Szenario angelegt. Dabei handelt es sich um Dokumente die während des Falls verschoben, modifiziert oder gelöscht werden und die den folgenden Formaten entsprechen:

- Microsoft Word (*.docx)
- Microsoft PowerPoint (*.pptx)
- Mirosoft Excel (*.xlsx)
- Libre Office Writer (*.odt)
- Libre Office Impress (*.odp)
- Libre Office Calc (*.ods)
- PDF Dokumente (*.pdf)

Es werden ebenfalls speziellere Dateien angelegt, die in den Ordnern liegen und teilweise eine große Bedeutung bei der Analyse der Falldaten haben werden.

- MP3 Dateien (*.mp3)
- E-Mail Dateien (*.eml)

2.3 Ablauf des Szenarios

Zunächst verbinden sich die einzelnen Benutzer des FTP-Servers von einem lokalen Rechner ihrer Wahl mit dem Server um im Folgenden Daten mit dem Server und dadurch auch mit den anderen Benutzern austauschen zu können. Abbildung 7 zeigt den FTP-Client FileZilla, mit dem die Benutzer auf die Daten des Servers zugreifen.

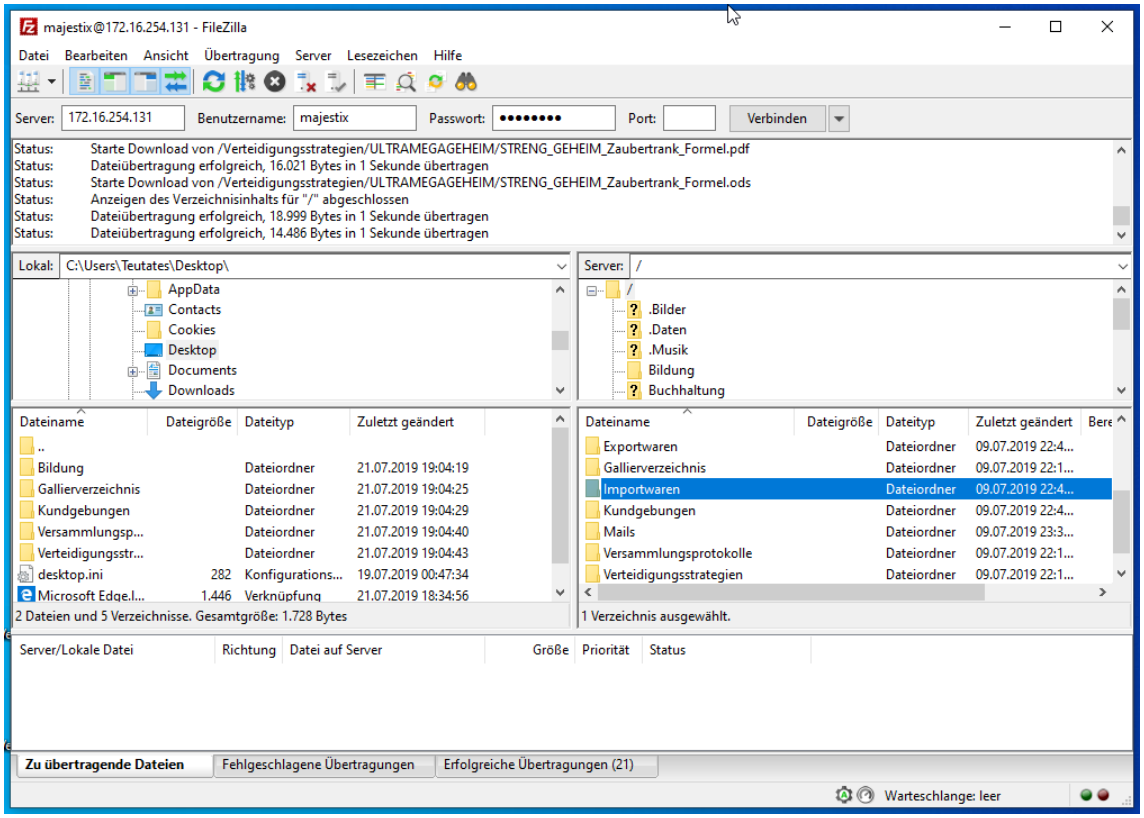

Abbildung 7: FileZilla Client

Als erstes wird die vollständige Ordnerstruktur von Majestix angelegt. Anschließend können die einzelnen Nutzer ihre Dateien in die dafür vorgesehenen Ordner hochladen, wieder löschen oder herunterladen. Es ist auch möglich die einzelnen Dateien durch Herunterladen, Bearbeiten und erneutem Hochladen zu modifizieren und so auf dem aktuellen Stand zu halten.

Der Ordner `Bildung` wird von Troubadix und Mirakulix gepflegt. Asterix und und Majestix sind die Hauptnutzer des Ordners `Buchhaltung` und allen Unterordnern. Asterix und Mirakulix sind außerdem für den Ordner `Exportwaren` verantwortlich. Den Ordner `Gallierverzeichnis` halten Majestix und Miraculix aktuell. Troubadix und Obelix verwalten den Ordner `Importwaren`. Um den Ordner `Kundgebungen` kümmern sich Asterix und Majestix. Die Dateien im Ordner `Versammlungsprotokolle`

pflegen Idefix, Obelix und Troubadix. Den Ordner `Verteidigungsstrategien` betreuen Obelix, Asterix und Miraculix.

Die geheimen Ordner `.Bilder`, `.Daten` und `.Musik` legt Idefix an. An deren Inhalt beteiligen sich außer Idefix noch Asterix und Obelix.

Zu Beginn des eigentlichen Vorfalls meldet sich Idefix am FTP-Server an und läd alle Ordner inklusive deren Inhalt herunter. Anschließend löscht er einige relevante Dateien und meldet sich wieder ab. Einige Zeit später läd Troubadix drei Mails auf den Server hoch, welche eine Absprache zwischen Idefix und Caesar belegen. Im Zuge dessen wird eine forensische Untersuchung angestellt, die diesen Vorfall rekonstruieren soll.

3 Erzeugen der forensischen Abbilder

Um eine forensische Analyse durchführen zu können müssen zunächst einige Vorbereitungen getroffen, sowie einige Abbilder des Systems erstellt werden.

3.1 Vorbereitung

Zum Erstellen der Abbilder wird im Folgenden der *FTK-Imager* auf dem Server installiert. Mit dessen Hilfe werden anschließend die notwendigen Abbilder erzeugt. Für die Installation wird der FTK-Imager zunächst von der offiziellen Webseite[1] heruntergeladen. Nachdem die Lizenzvereinbarungen bestätigt und das Installationsverzeichnis ausgewählt wurde wird die Software automatisch installiert und das Programm gestartet. Nun kann mit der Option *Capture Memory...* ein Abbild des Arbeitsspeichers und mit der Option *Create Disk Image...* ein Abbild der Festplatte erzeugt werden.

3.2 Datensammlung

Nachdem die Vorbereitungen abgeschlossen sind kann mit dem erstellen der Images begonnen werden. Im Folgenden wird nun ein Abbild des Hauptspeichers, sowie ein Abbild des Festplattenspeichers erzeugt.

3.2.1 Hauptspeicherabbild

Mit der Option *Capture Memory...* wird mit dem FTK-Imager ein Haupspeicherabbild erstellt. Hierfür muss das zu erstellende Abbild zunächst konfiguriert werden. Abbildung 8 zeigt die Einstellungen für das Abbild.

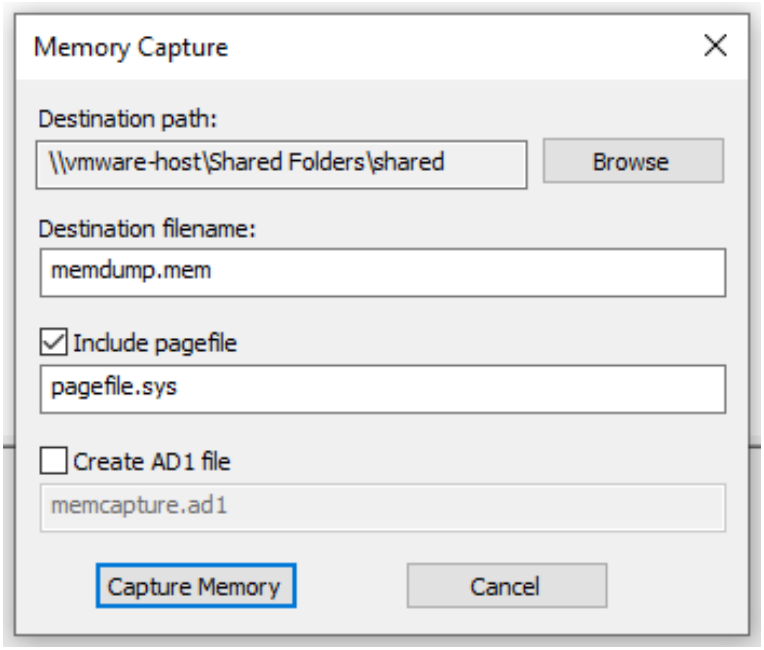

Abbildung 8: Konfiguration des Hauptspeicherabbilds

[1] https://accessdata.com/product-download/ftk-imager-version-4.2.1

In diesem Schritt muss der Dateipfad, sowie der Dateiname angegeben werden und es können weitere Optionen ausgewählt werden. Wenn die Konfiguration abgeschlossen ist werden die Images erzeugt. Abbildung 9 zeigt den Status des Fortschitts während der Erzeugung des Hauptspeicherabbilds. Für diese Arbeit wurde sowohl ein `memdump.mem` als auch ein `pagefile.sys` erstellt.

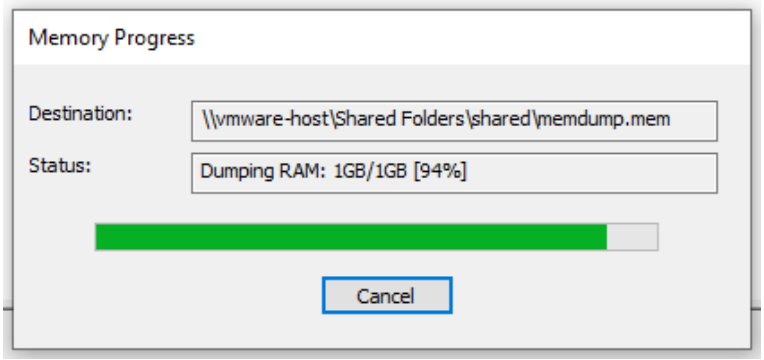

Abbildung 9: Fortschritt der Erzeugung des Hauptspeicherabbilds

In den folgenden Kapiteln wird die Analyse der erzeugten Images beschrieben. Im nächsten Abschnitt wird die Erzeugung des Festplattenabbilds dargestellt, welches ebenfalls für die Analyse des Szenarios notwendig ist.

3.2.2 Festplattenabbild

Um ein Abbild der Festplatte der VM zu erstellen muss die Option *Create Disk Image...* im FTK-Imager verwendet werden. Im ersten Schritt muss, wie in Abbildung 10 dargestellt, die Quelle für das zu Erstellende Abbild gewählt werden. Im Falle dieses Szenarios wird *Physical Drive* ausgewählt.

Im nächsten Schritt muss das eigentliche Laufwerk der Festplatte gewählt werden. Da die VM dieses Szenarios nur eine Festplatte enthält, kann auch nur diese verwendet werden.

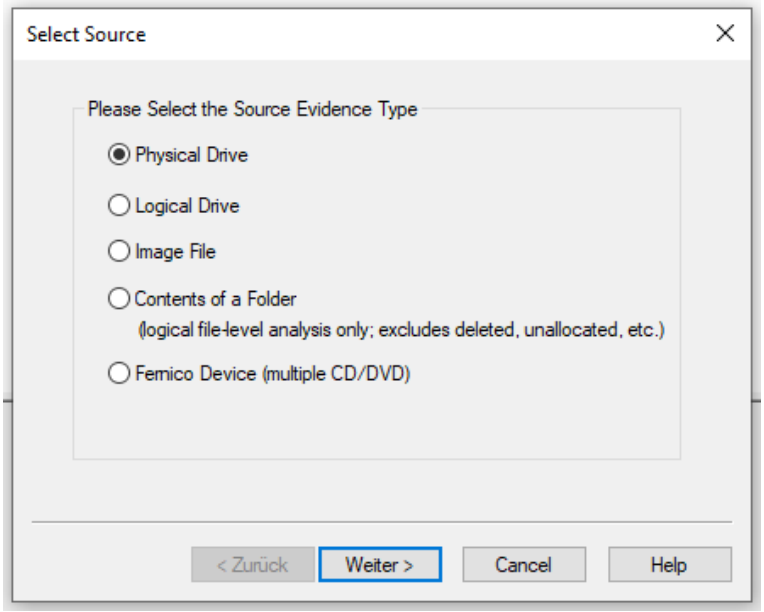

Abbildung 10: Auswahl der Festplatte zur Erzeugung des Abbilds

Zum Erstellen des Abbilds wird im Folgenden der Dateityp des Images festgelegt. Abbildung 11 zeigt die unterschiedlichen Auswahlmöglichkeiten. FTK-Imager kann Abbilder im *Raw*, *SMART*, *E01* und *AFF* Format erzeugen. Für diese Arbeit wurde *E01* gewählt.

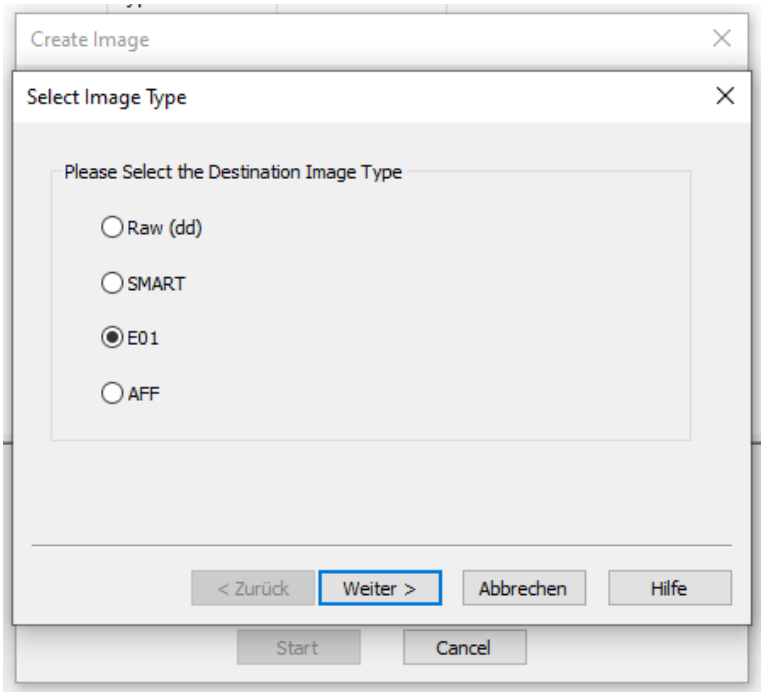

Abbildung 11: Auswahl des Abbild-Typs

Im letzten Schritt vor dem Erstellen des Images muss dieses noch konfiguriert werden. Abbildung 12 zeigt die Konfiguration fur das Festplattenabbild.

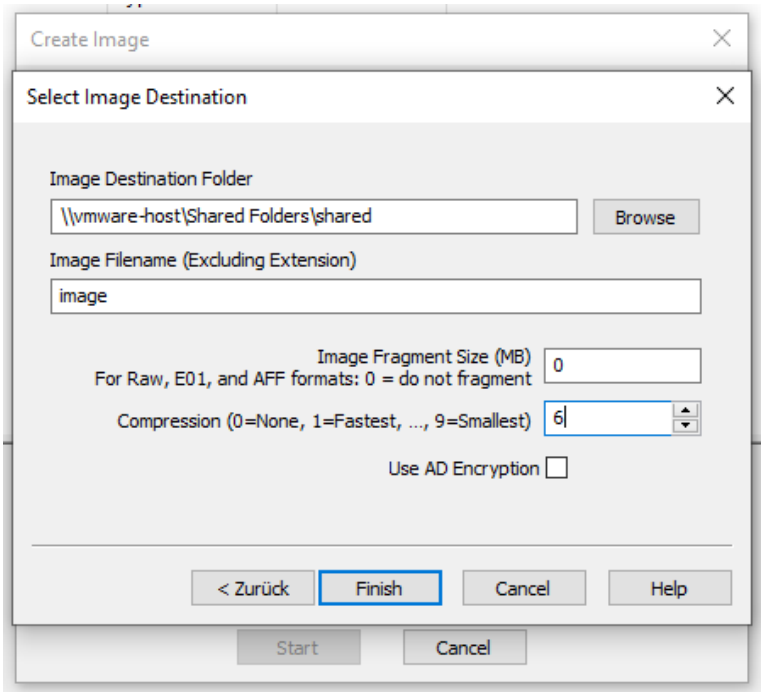

Abbildung 12: Konfiguration des Festplattenabbilds

Wie beim Erstellen des Haupspeicherabbilds müssen auch hier Dateipfad und Dateiname festgelegt werden. Außerdem kann eine Fragment-Größe und eine Kompressionsrate angegeben werden. Für *E01* Abbilder soll die Fragment-Größe auf null gesetzt werden, die Kompressionsgröße wird auf dem Standardwert sechs belassen.

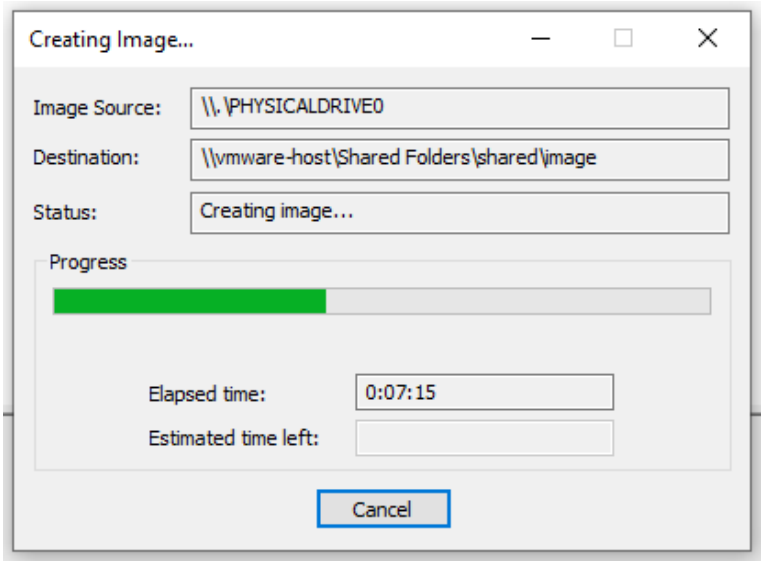

Abbildung 13: Fortschritt der Erzeugung des Festplattenabbilds

Nachdem alle Vorbereitungen abgeschlossen sind, wird das Image mit den eingestellten Bedingungen erzeugt. Abbildung 13 zeigt den Status des Exportprozesses. Wenn dieser erfolgreich abgeschlossen ist, kann die Analyse der in diesem Kapitel erzeugten Abbilder durchgeführt und damit das Szenario rekonstruiert werden.

4 Forensische Analyse

Die forensische Analyse soll mit Hilfe der Software *MAGNET Forensics AXIOM* unter *Windows 10* erfolgen. Das Forensik-Werkzeug Axiom besteht aus zwei Programmen, eins zum erstellen eines Falls und das andere zum Auswerten von diesem:

AXIOM Process
: Es dient zum Suchen von Beweismaterial in Abbildern, auf Laufwerken, in Dateien und Ordnern sowie in weiteren Quellen. Es lassen sich spezielle vorgefertigte Artefakte für verschiedene Anwendungsgebiete auswählen. Zudem können Suchbegriffe und viele weitere Dinge (Hashwerte bilden, Archive durchsuchen, Cyber-Grooming rausfiltern, ...) zum optimieren der Ergebnisfindung gewählt werden.

AXIOM Examine
: Nach dem Erstellen eines Falls mit Axiom Process werden die Ergebnisse in diesem Tool in benutzerfreundlicher Form dargestellt. Neben einer allgemeinen Übersicht über die gewählten Artefakte, lassen sich noch weitere Daten anzeigen. Beziehungen zwischen Dateien, Einblicke in die Registry und in das Dateisystem sind möglich. Es ist insbesondere Interessant das eine Zeitachse erstellt werden kann, die einzelne Dateien in einen zeitlichen Zusammenhang bringt.

Mit Hilfe dieser Tools lässt sich das zuvor erstellte Image automatisch anhand der gewählten Vorgaben analysieren. Die Ergebnisse der Analyse lassen sich im Anschluss daran auswerten und in einen Zusammenhang bringen.

4.1 Anlegen des Falles mit Axiom Process

Mit dem Tool Axiom Process kann, nach dem Abschalten der Antivirensoftware, ein Fall zu der Analyse von verschiedenen IT-Forensichen-Beweisquellen erstellt werden.

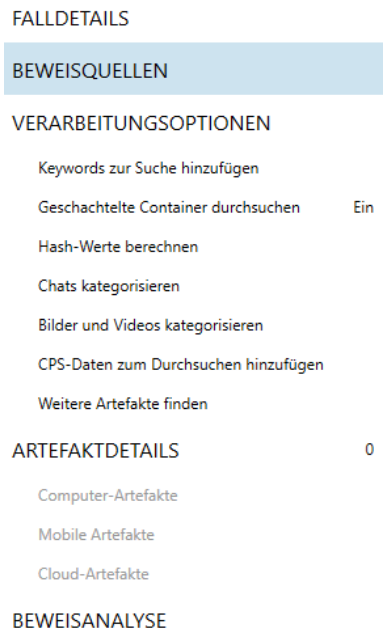

Abbildung 14: Schritte der Image Erstellung

Das Anlegen des Falls ist in fünf verschiedene Überpunkte unterteilt. Bei diesen handelt es sich um Falldetails, Beweisquellen, Verarbeitungsoptionen, Artefaktdetails und die Beweisanalyse. In jeder Kategorie muss anhand verschiedener Vorschläge eine Auswahl relevanter Informationen getroffen werden.

Unter dem Reiter Falldetails werden allgemeine Informationen zu dem Fall wie Fallnummer, Fallbezeichnung, Fallart, Speicherort der Analysedatei und einige weitere gewählt.

4.2 Einlesen der Beweisquellen

Im zweiten Reiter Beweisquellen lassen sich verschiedene Datenquellen für die Analyse wählen. An dieser Stelle werden die in Kapitel 3 erstellten forensichen Abbilder geprüft und zur Analyse ausgewählt. Zunächst muss ein Betriebssystem gewählt werden, da die Artefakte anhand dieser Wahl vorgeschlagen werden.

Abbildung 15: Auswahl der Beweisquellen unter Windows

Danach kann, hier beispielsweise unter Windows, eine der vorgeschlagenen Beweisquellen gewählt und eine dazu passende Datei rausgesucht werden. Diese Datei wird dann im nachhinein von der Analyse-Software untersucht.

4.2.1 Hauptspeicherabbild

Zum Einlesen des Hauptspeicherabbildes wird über Beweisquellen - Beweisquelle auswählen - Arbeitsspeicher - Speicherabbilddatei die mit dem FTK Imager erstellte Datei `memdump.mem` ausgewählt. Anschließend muss ein Profil, auf Basis des aktuell vorliegenden Betriebsystems, angegeben werden. Die Analyse des Arbeitsspeicherabbilds lässt sich zudem noch durch weitere Kriterien einschränken.

4.2.2 Windows-Festplattenabbild

Das erstelle Festplattenabbild kann ebenfalls wie das Arbeitsspeicherabbild über Beweisquellen - Beweisquelle auswählen - Abbild ausgewählt werden. In diesem Fall wird die Datei `image.E01` selektiert und in Axiom Process geöffnet.

Abbildung 16: Image E01 Speicherbereiche

Anschließend werden die Inhalte des logischen Laufwerks aufgelistet, für die jeweils eine Suchart festgelegt werden muss. In diesem Fall sind die vom System vorgeschlagenen Suchtypen Vollständig und Sektorebene für die jeweiligen Speicherbereiche gewählt worden. Dies bedeutet das alle möglichen Bereiche anhand der eingestellten Verarbeitungsoptionen und Artefakten durchsucht werden.

4.3 Verarbeitungsoptionen

Über die Verarbeitungsoption lässt sich in *AXIOM Process* die Suche in den Beweismitteln optimieren. Es lassen sich beispielsweise bestimmte Schlagwörter festlegen oder Bilder kategorisieren

Unter den Verarbeitungsoptionen lässt sich die Suche in den Beweismitteln optimieren. Es kann nach vielen verschiedenen Kriterien, von dem durchsuchen von Archiven, dem bilden von Hash Werten über alle Dateien bis hin zu speziellen Suchbegriffen für unter anderem Cyber-Grooming in Chats gesucht werden.

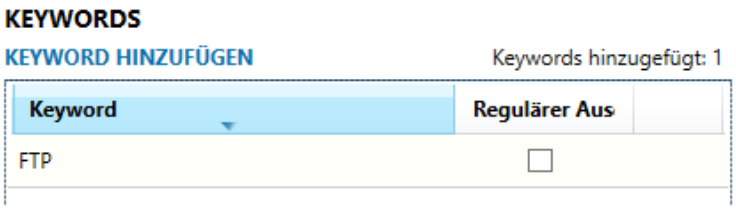

Abbildung 17: Auswahl von Keywords

Im Bereich der Keywords wurde für die Analyse der Begriff *FTP* eingetragen, damit im speziellen nach diesem gesucht wird und die Ergebnisse im nachhinein entsprechend eingeschränkt werden können.

4.4 Auswahl der Artefakte

Es werden gezielt Artefakte gewählt, bei denen vermutet wird, dass wichtige Informationen und Daten in den Anwendungs- und Nutzungsdaten gewonnen werden können.

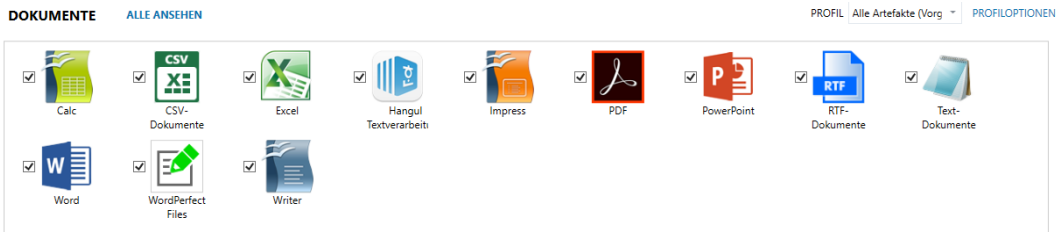

Abbildung 18: Artefakte: Dokumente

Anhand des vorliegenden Falls und dem ersten Überblick über die Daten wurden insbesondere Artefakte aus dem Bereich des Betriebssystems, der Dokumente und Mails gewählt.

4.5 Beweisanalyse

Nach der Wahl der Kritierien für die Suchoptimierung kann die Beweisanalyse gestartet werden.

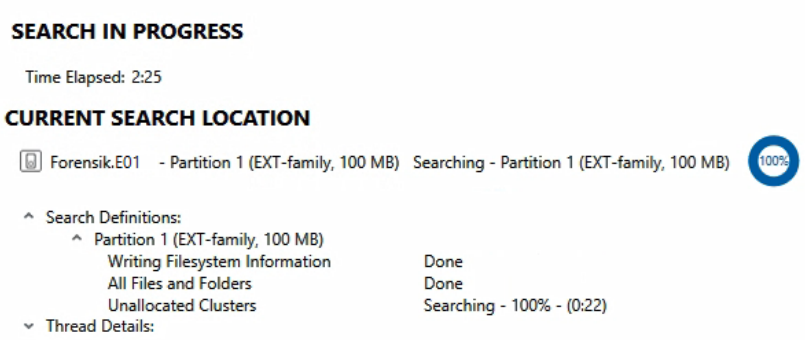

Abbildung 19: Durchführung der Beweisanalyse

Es werden zehn einzelne Schritte durchlaufen in denen das Festplatten- und das Hauptspeicherabbild durch die Sotware analysiert werden. Da das Festplattenimage bereits die Auslagerungsdatei des Arbeitsspeichers beinhaltete, konnte durch die separate Analyse des Arbeitsspeicherabbilds keine weiteren nennenswerten Erkenntnisse gewonnen werden.

4.6 Auswertung des Falles mit Axiom Examine

Zur Auswertung des Falles wird die Software *Axiom Examine* gestartet und der vorher, durch Axiom Process, erstellte Fall in die Software geladen. In der folgenden Abbildung 20 ist die Gesamtheit der gefunden Artefakte auf dem Datenträger-Abbild aufgezeigt. Zur Auswertung werden alle Beweisquellen ausgewählt und vorerst keine feinere Auswahl getroffen.

Dadurch wird sich nicht auf den erwarteten Vorfall beschränkt, sondern auch weitere mögliche Beweise gesammelt. Insgesamt werden *71.172 Artefakte* gefunden. Diese unterteilen sich hauptsächich in die Kategorien Betriebssystem, Medien, Webbezogen, Dokumente und E-Mail.

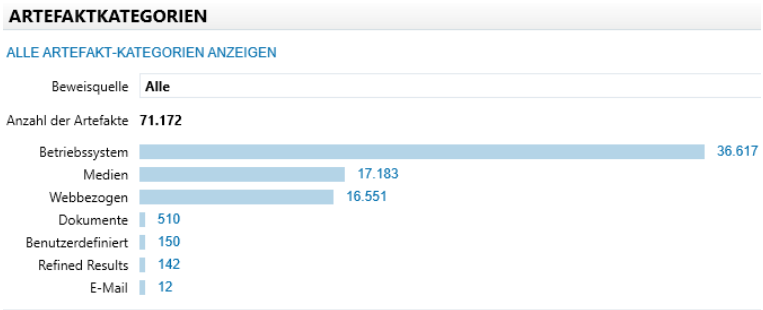

Abbildung 20: Übereinstimmungen des Keywords

4.6.1 Untersuchung der Microsoft Registry

Registrierte Benutzer

Im ersten Schritt der Auswertung wird das Benutzerverzeichnis aus der Registry ausgewertet. In Abbildung 21 sind einige Standard-Benutzer und -Dienste aufgeführt. Das Benutzerverzeichnis zeigt, dass neben den Standard-Benutzern und -Diensten, nur ein weiterer Benutzer-Account *Teutates* auf

der Maschine registriert ist. Damit ist bestätigt, dass zum Zeitpunkt des untersuchten Vorfalles nur der Administrator *Teutates* und kein anderer Mitarbeiter der Dorfverwaltung, administrativen Zugang zu dem Server hat.

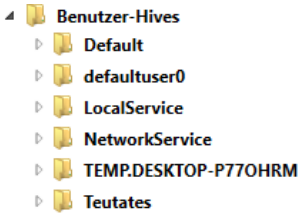

Abbildung 21: Angelegte Benutzer

Registrierte USB-Sticks

Bei der Untersuchung der Registry, auf verwendete USB-Sticks, wurden zwei verschiedene USB-Sticks gefunden. Ein Auszug aus der Registry ist in der folgenden Abbildung 22 dargestellt.

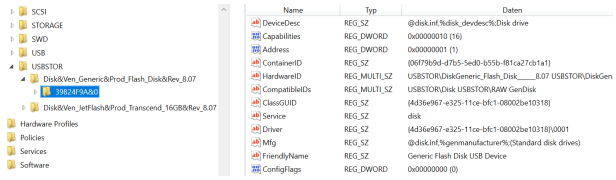

Abbildung 22: Auszug: Registrierte USB-Sticks MS Registry

Eine weitere Untersuchung der zwei USB-Sticks ergab keine weiteren Erkenntnisse für diesen Fall. Auf den USB-Sticks liegen lediglich Daten des Administrators für seine tägliche Arbeit.

4.6.2 Installierte Software

Damit ein erster Eindruck über den Umfang der intallierten Software gewonnen werden kann, wird das Standard-Verzeichnis von *Windows 10* für installierte Software ausgewertet.

In der folgenden Abbildung 23 ist ein Ausschnitt dieses Standard-Verzeichnisses zudargstellt. In diesem Verzeichnis ist zusätzlich zu den Standard-Programmen von *Windows 10* ein *FileZilla Server* installiert. Diese wird in der gesamten Untersuchung im Mittelpunkt stehen.

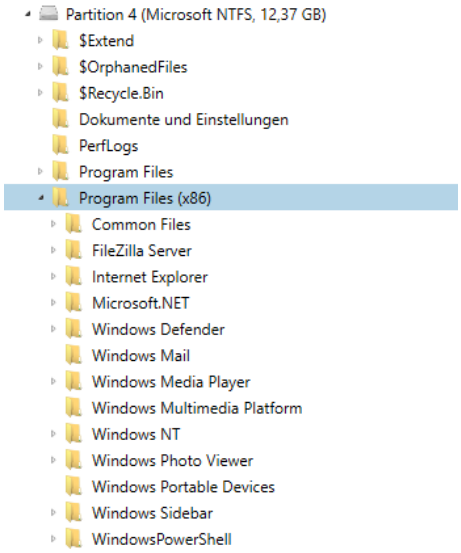

Abbildung 23: Installierte Programme

In den weiteren Programm-Verzeichnissen der Betriebssystem-Partition konnten keine weiteren nachinstallierten Programme gefunden werden.

4.6.3 Medien und Dokumente

Im nächsten Schritt werden die Ordnerstrukturen der Standard-Benutzer untersucht. Diese Untersuchung zeigt keine Auffälligkeiten, sodass mit der Untersuchung der Ordnerstruktur des Administrators *Teutates* begonnen wird. In der Ordnerstruktur des Administrators ist, neben den von *Microsoft Windows 10* standardmäßig erstellten Ordnern, ein weitere Ordner *FTP* anlegt. Dies ist der Standard-Ordner von der Software *FileZilla Server*.

Aufgeklappt zeigt der Ordner *FTP* weitere Unterordner. Dies ist die Ordnerstruktur auf dem FTP-Server der Dorfverwaltung.

Eine besondere Auffälligkeit sind die mit dem „ . “ vor dem Namen gekennzeichneten Ordnern, zu erkennen in Abbildung 24. Dies sind verstecke Ordnern, die ohne weiteres Wissen nicht öffentlich erreichbar sind. Auf diese Ordner wird im späteren Verlauf der Untersuchung eingegangen.

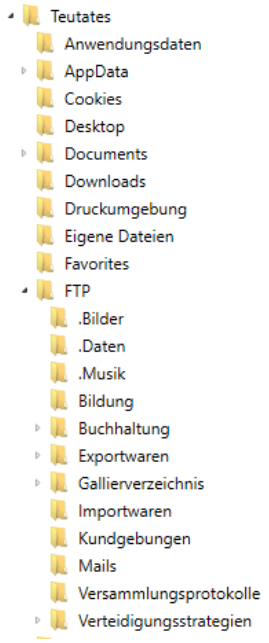

Abbildung 24: Abgelegte Dokumente

Eine erste grobe Verfeinerung des Falls wird mit der Betrachtung des FTP-Clients erstellt. Dieser wird in der forensischen Untersuchung im Vordergrund stehen. Wie in der unten stehenden Abbildung 25 dokumentiert ist, grenzt das Keyword *FTP* die Übereinstimmungen auf eine Anzahl von 45 Dateien und Ordner ein. Ein Ausschnitt der mit diesem Keyword aufgefundenen Daten wird ebenfalls aufgezeigt.

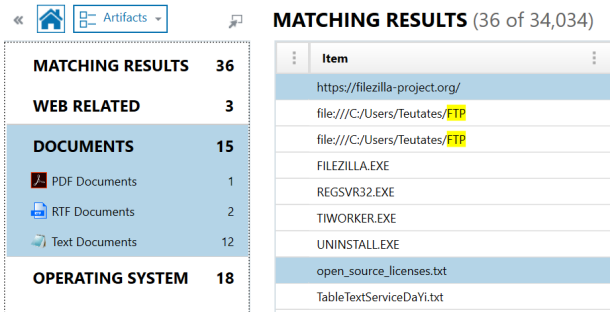

Abbildung 25: Übereinstimmungen mit Keyword *FTP*

Außen vor gelassen werden zu diesem Zeitpunkt der Untersuchung die Daten in den versteckten Ordnern. Bei der Untersuchung der einzelnen Dokumente auf dem Server werden einige Auffälligkeiten entdeckt. Einige der Dokumente wurden, zum Zeitpunkt der Vorfalls, verändert.

Innerhalb der Software *Axiom Examine* werden die Dokumente auf dem FTP-Server auf Auffälligkeiten untersucht. Durch den Abgleich des Zeitstempels der Erstellung mit dem Zeitstempel der letzten Modifikation bzw. des letzten Zugriffs, konnte eine modifizierte Datei entdeckt werden.
Die folgende Abbildung 26 zeigt einen Ausschnitt des Abgleichs der verschiedenen Zeitstempel.

09.07.2019 20:34:51	File System Last Modifi...	File/folder opening	Documents	PDF Documents	Filename	Liste der Gottheiten in den Asterix-Comics –
09.07.2019 20:35:39	File System Last Modifi...	File/folder opening	Documents	Calc Documents	File Name	STRENG_GEHEIM_Zaubertrank_Formel.ods

Abbildung 26: Modifiziertes Dokument

Diese Datei wird folgend genau analysiert. Genutzt wird dafür weiterhin die Software Axiom Examine. Die Datei ist mit der Bemerkung *STRENG_ GEHEIM_* versehen und trägt den Namen *Zaubertrank_ Formel*. Die Dateiendung *.ods* lässt auf ein LibreOffice Tabellendokument schließen.

Weitere Informationen der Datei werden den Details, erstellt durch *Axiom Examine*, entnommen. Diese sind in Abbildung 27 dargestellt.

Die modifizierte Datei liegt in dem Ordnerpfad `image.E01 - Partition 4 (Microsoft NTFS, 12,37 GB)\Teutates\FTP\Verteidigungsstrategien\ULTRAMEGAGEHEIM\`. Diesem ist zu entnehmen, dass hier sehr brisante Daten abgelegt werden.

Weiterhin werden die verschiedenen Zeitstempel, die Größe der Datei, Passwortschutz, Anzahl der Editierungen, die MD5 Hash-Summe und die SHA1 Hash-Summe aufgeführt. Weiterhin ist ein visueller Einblick in die modifizierte Datei dargestellt.

Zaubertrank Formel:

Zutaten		Zutaten		Menge
Misteln			2 Bunde	
Hummer			1 stk.	
einigermaßen frischen Fisch			3 stk.	
Steinöl oder Roterrübensaft			222 ml	
Schnudelfix			1 ml	
	Druidenmix			333 ml

DETAILS

ARTIFACT INFORMATION

File Name	**STRENG_GEHEIM_Zaubertrank_Formel.ods**
File System Last Modified Date/Time	**09.07.2019 20:35:39**
File System Last Accessed Date/Time	**09.07.2019 21:36:48**
File System Created Date/Time	**09.07.2019 20:19:19**
Recovered Size (Bytes)	**14486**
Password Required	**No**
Editing Cycles	**3**
MD5 Hash	**bcd8aeed930f69ca83a71463e9c94bb4**
SHA1 Hash	**4bc2df86167bdfea854bbf6e624838bf0061fc18**

EVIDENCE INFORMATION

Source	**image.E01 - Partition 4 (Microsoft NTFS, 12,37 GB)\Users\Teutates\FTP\Verteidigungsstrategien\ULTRAMEGAGEHEIM \STRENG_GEHEIM_Zaubertrank_Formel.ods**

Abbildung 27: Veränderte Zaubertrankformel

Auch aus diesem lässt sich eine Modifikation, durch verschobene Spalten, erkennen.

Zur Bestätigung wird die MD5 Hash-Summe über die Original-Datei, bereitgestellt aus einem Backup vom 06.07.2019, gebildet. Diese wird am Terminal errechnet. Das Ergebnis ist in Abbildung 28 aufgezeigt.

Ein Vergleich der zwei MD5-Hash-Summen zeigt, dass diese nicht gleich sind und somit eine Veränderung der Datei stattgefunden haben muss.

```
droid01@debdroid:~/Downloads$ md5sum STRENG_GEHEIM_Zaubertrank_Formel.ods
d839bded95f4488137a9f89bdd021bf2  STRENG_GEHEIM_Zaubertrank_Formel.ods
```

Abbildung 28: Hash des des Original-Dokuments

4.6.4 Versteckte Ordner

Während der Untersuchung des FTP-Servers sind drei verstecke Ordner (s. 4.6.3 Medien und Dokumente Abs. 3) mit Medien-Inhalten entdeckt worden. Eine Übersicht über die versteckten Ordner und Dateien ist folgenden dargstellt.

.Bilder:

- oberlix.jpg
- gallier.jpg
- asterix.jpg
- schlacht.jpg
- troubadix.jpg

.Daten:

- Asterix - Wikipedia.pdf
- Figuren aus Asterix - Wikipedia.pdf
- Liste der Gottheiten in den Asterix-Comics - Wikipedia.pdf

.Musik:

- troubadix1.mp3
- troubadix2.mp3

Die versteckten Ordner enthalten Dateien verschiedener Medienformate. Diese dienen scheinbar als private Ablage oder als Austausch-Ordner. Abgelegt wurden JPG-, PDF- und MP3-Dateien.

4.6.5 Gelöschte Dateien

Es konnten innerhalb der Untersuchung keine gelöschten Dateien auf dem Datenträger-Abbild gefunden werden. Die Untersuchung des Papierkorbs ergab ebenfalls keine weiteren Erkenntnisse. Die im Papierkorb aufgefundenen Daten sind in Abbildung 29 zu sehen.

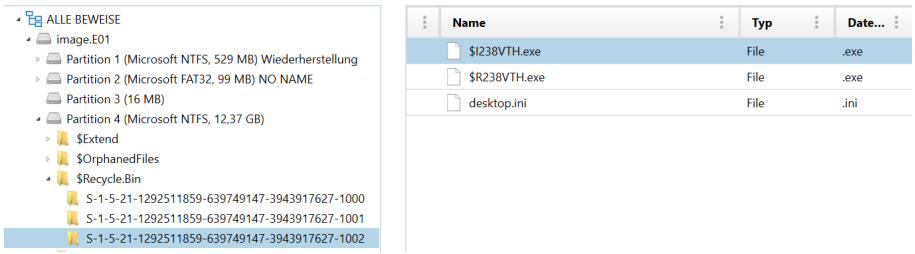

Abbildung 29: Dateien innerhalb des Papierkorbs

4.6.6 E-Mail

Unter dem Artefakt E-Mail werden genau drei E-Mails gefunden. Ein Überblick über den gesamtem E-Mail Verlauf ist in Abbildung 30 aufgezeigt.

"Ceasar" <caesar@rom.it>	Idefix <idefix@gallien.org>	Antwort Operation "Run Fast"
"Ceasar" <caesar@rom.it>	Idefix <idefix@gallien.org>	Antwort Antwort Operation "Run Fast"
"Idefix" <idefix@gallien.org>	Ceasar <caesar@rom.it>	Operation "Run Fast"

Abbildung 30: Übersicht des Mailverlaufs

Ein Auszug der Detail-Ansicht der ersten E-Mail wird in Abbildung 31 dargestellt. Aus diesem Ausschnitt ist zu Erkennen, dass der Absender der sich *Idefix* nennt, mit der E-Mail Adresse *idefix@gallien.org* eine E-Mail an *Caesar* mit der E-Mail Adresse *caesar@rom.it* gesendet hat. Weiterhin sind der empfangende Server und der sendende Server, Betreff der E-Mail und auch die Zeitstempel dargestellt.

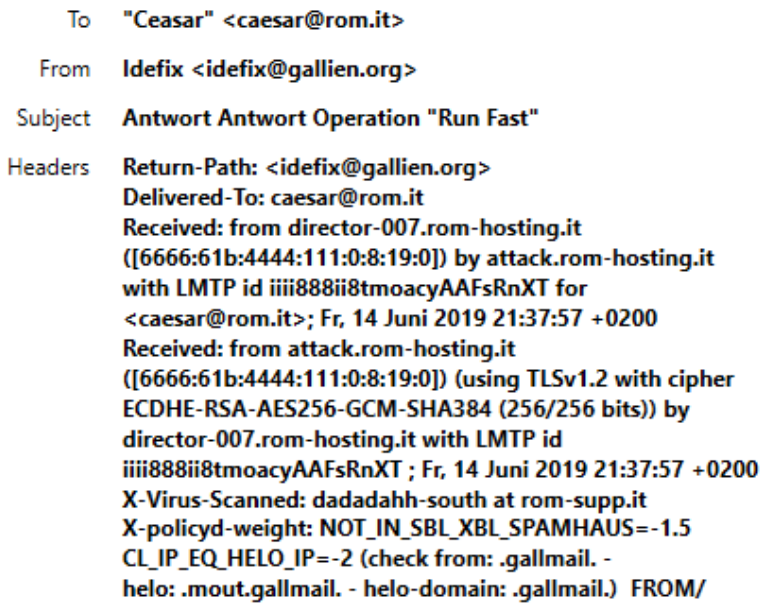

Abbildung 31: Auszug: Detail-Ansicht E-Mail

Die Abbildung 32 zeigt beispielhaft den Inhalt einer solchen E-Mail. Diese wurde aus der Software *Axiom Examine* exportiert und anschließend über den standardmäßig installierten *Editor* geöffnet. Der Inhalt der E-Mail erschwert den Vorwurf, dass Idefix Daten an die Römer und Caesar verkauft haben soll. Nach der Untersuchung des gesamten Gesprächsverlaufs, ist mit Klarheit zusagen, dass wenn nur Idefix selber Zugang zu seinem E-Mail Postfach hat, er sämtliche Daten an die Römer gegeben hat.

```
<p>Hallo Caesar,</p>
<p>kein Problem. Bin auf dem Weg, melde mich morgen <br /><strong></p>
<p>Bitte keine Mails mehr, könnten mich verraten!</p><br/><br/>
<p></p>
<p></p>
<p></p>
<p><strong>Die naechsten Schritte:</strong></p>
<ul>
<li>Ich finde dich und gebe dir saemtliche Daten.</li>
</ul>
<p> </p>  <br />
  <p>Beste Gruesse</p>
  <p>Dein Idefix</p>
```

Abbildung 32: E-Mail: Von Idefix an Caesar

4.6.7 FTP-Client

Innerhalb der forensischen Untersuchung mit *Axiom Examine* ist das Log-File `fzs-2019-07-09.log` und die Systemdatei `FileZilla.xml` des FTP-Servers gefunden worden. Der Fund des Log-Files ist in der Abbildung 33 dokumentiert. Folgend werden beide Dateien tiefergehend analysiert.

Name	Typ	Date...	Größe...	Erstellt	Aufgerufen	Modifiziert
fzs-2019-07-09.log	File	.log	288.608	09.07.2019 19:13:43	09.07.2019 21:40:00	09.07.2019 21:40:00
fzs-2019-07-10.log	File	.log	1.044	09.07.2019 22:00:02	10.07.2019 15:13:01	10.07.2019 15:13:01

Abbildung 33: Durchführung der Beweisanalyse

Registrierte Benutzer des FTP-Servers

Begonnen wird mit der Untersuchung der Systemdatei. Aus dieser können die registrierten Benutzer an dem FTP-Server ausgelesen werden. Ein Auszug eines solchen Benutzers ist in Abbildung 34 gezeigt.

```
▼<User Name="idefix">
  ▼<Option Name="Pass">
      FC57932DCDF20D0FF4552A84A5F3A094C06AD3DF11B74
    </Option>
  ▼<Option Name="Salt">
      X1!}JkE;-Lugj^O?PGGw+hfFz]&E[^%
      (CHn]1Zd^fMhBr`4,as|b%uhz)7aFF~{}
```

Abbildung 34: Auszug: Registrierte Benutzer des FTP Servers

Weitere registrierte Benutzernamen sind:

- asterix
- idefix

- majestix
- miraculix
- obelix
- troubadix

Auslesen des Log-Files

Die Forensik-Software *Axiom Examine* beitet keine Funktion zur Auswertung von Log-Files, aus diesem Grund wurde das Log-File exportiert. Anschließend wurde es in die Software *Microsoft Excel 2017* importiert. Dadurch sind einfache Filter-Funktionen gegeben, die die Auswertung deutlich beschleunigen. Dadurch kann nach Datum, Benutzer und IP-Adressen gefiltert werden.

Die folgende Abbildung 35 zeigt einen Ausschnitt des Log-Files. Dieser beweist, dass der Benutzer *idefix* einige Dateien gelöscht und heruntergeladen hat. Weitere Untersuchungen haben bestätigt, dass *idefix* alle Dateien des FTP-Servers heruntergeladen hat. Darauf folgend löschte er einige Dateien.

```
09.07.2019 22:41:29 - idefix (172.16.254.1)> 150 Opening data channel for directory listing of "/Kundgebungen"
09.07.2019 22:41:29 - idefix (172.16.254.1)> 226 Successfully transferred "/Kundgebungen"
09.07.2019 22:41:32 - idefix (172.16.254.1)> DELE Kundgebung_IV.pdf
09.07.2019 22:41:32 - idefix (172.16.254.1)> 250 File deleted successfully
```

Abbildung 35: Auszug: Log-File - Herunterladen und Löschen von Dateien

Aus der Abbildung 36 ist zu erkennen, dass *idefix* die geheime Zaubertrank-Formel heruntergeladen hat. Ein Vergleich der Zeitstempel der letzten Modifikation (s. 4.6.3 Medien und Doku- mente) und dem Zeitstempel des Log-Files zeigt außerdem, dass *idefix* das Dokument erst heruntergeladen und anschließend manipuliert und wieder hochgeladen hat.

```
09.07.2019 22:35:11 - idefix (172.16.254.1)> 150 Opening data channel for file download from server of "/Verteidigungsstrategien/ULTRAMEGAGEHEIM/STRENG_GEHEIM_Zaubertrank_Formel.ods"
09.07.2019 22:35:11 - idefix (172.16.254.1)> 226 Successfully transferred "/Verteidigungsstrategien/ULTRAMEGAGEHEIM/STRENG_GEHEIM_Zaubertrank_Formel.ods"
```

Abbildung 36: Ausschnitt: Download der Zaubertrankformel

Ein Beweis dafür, dass *Troubadix* den E-Mail Verkehr auf den Server geladen hat, ist ebenfalls dem Log-File zu entnehmen. Die nachstehende Abbildung 37 zeigt den Auszug des Log-Files, indem bestätigt wird, dass Troubadix die E-Mails hochgeladen hat.

```
09.07.2019 23:38:03 - troubadix (172.16.254.1)> 150 Opening data channel for file upload to server of "/Mails/auftrag_caesar.eml"
09.07.2019 23:38:03 - troubadix (172.16.254.1)> 226 Successfully transferred "/Mails/antwort1ZuAuftragCaesar.eml"
09.07.2019 23:38:03 - troubadix (172.16.254.1)> 150 Opening data channel for file upload to server of "/Mails/antwort2ZuAuftragCaesar .eml"
09.07.2019 23:38:03 - troubadix (172.16.254.1)> 226 Successfully transferred "/Mails/auftrag_caesar.eml"
09.07.2019 23:38:03 - troubadix (172.16.254.1)> 226 Successfully transferred "/Mails/antwort2ZuAuftragCaesar .eml"
```

Abbildung 37: Troubadix: Upload der Maildaten

4.7 Rekonstruierte Zeitachse

Die rekonstruierte Zeitachse dient einerseits für einen Überblick über das gesamte Geschehen in dem vorliegenden Fall, andererseits kann diese genutzt werden um die gesammelten Beweise und Erkenntnisse zusammen gefasst aufzutragen. Die Funktion der Zeitachse innerhalb der Forensik Software *Axiom Examine* wird für die visuelle Aufarbeitung der Zeitachse nicht verwendet, da diese das Log-File des FTP-Servers nicht lesen kann und somit auch nicht mit auf die Zeitachse aufnimmt. Jedoch werden zur Erstellung wichtige Information, wie beispielthaft die in Abbildung 38 dokumentiert sind, aus der Forensik Software *Axiom Exmine* genutzt.

Datum/Uhr...	Datums-/Uhrzeitattribut	Zeitleistenkatego...	Kategor...	Typ	Eleme...	Wert des Elements
09.07.2019 20:18:48	Dateisystem erstellt – Datum/Zeit	Dateiwiedererkennung	Dokumente	Impress-Dokumente	Dateiname	Verteidigung.odp
09.07.2019 20:19:19	Dateisystem erstellt – Datum/Zeit	Dateiwiedererkennung	Dokumente	Calc-Dokumente	Dateiname	STRENG_GEHEIM_Zaubertrank_Formel.ods
09.07.2019 20:32:30	Datum/Zeit der letzten Modifikation auf das Dateisy...	Datei/Ordne wird geöffnet	Dokumente	Impress-Dokumente	Dateiname	Verteidigung.odp
09.07.2019 20:35:39	Datum/Zeit der letzten Modifikation auf das Dateisy...	Datei/Ordne wird geöffnet	Dokumente	Calc-Dokumente	Dateiname	STRENG_GEHEIM_Zaubertrank_Formel.ods
09.07.2019 21:36:43	Datum/Zeit des letzten Zugriffs auf das Dateisystem	Datei/Ordne wird geöffnet	Dokumente	Impress-Dokumente	Dateiname	Verteidigung.odp
09.07.2019 21:36:48	Datum/Zeit des letzten Zugriffs auf das Dateisystem	Datei/Ordne wird geöffnet	Dokumente	Calc-Dokumente	Dateiname	STRENG_GEHEIM_Zaubertrank_Formel.ods

Abbildung 38: Dokumente der Zeitachse

Die folgende Abbildung 39 ist mit Hilfe der Software *Microsoft PowerPoint 2017* erstellt. Diese Abbildung spiegelt den gesamten Verlauf des Falles und somit auch des Tathergangs wieder.

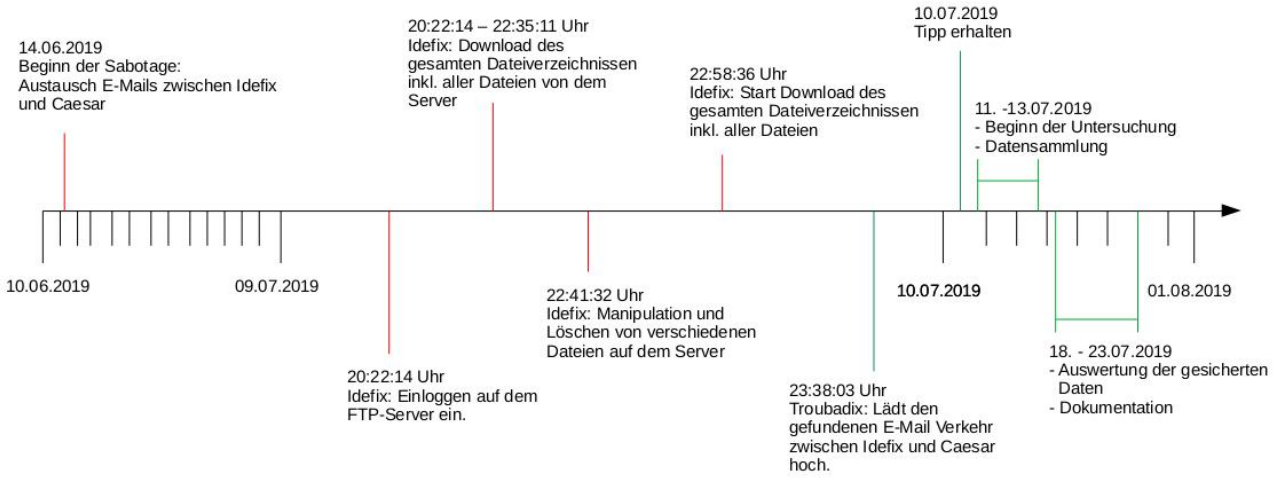

Abbildung 39: Eigene Darstellung: Rekonstruierte Zeitachse

5 Fazit

5.1 Beweisanalyse

Durch die Analyse des Datenträger-Abbildes konnte das gesamte Szenario wiederhergestellt werden. Jedoch konnten nicht alle Informationen mit Hilfe der ausgewählten Forensik-Software *MAGNET Axiom* gesammelt und ausgewertet werden. So konnten die Log-Files des FTP-Servers nicht ausgelesen werden. Ebenfalls war es nicht möglich gelöschte Dateien zu identifizieren, auch die Dateien im Papierkorb waren nicht sinnvoll nutzbar. Die Informationen aus dem Log-File wurden im Anschluss an die forensische Untersuchung mit *Axiom Examine* manuell ausgewertet.

Die durch *Axiom Examine* erstellte Zeitachse enthielt ebenfalls zu wenig Informationen, um diese sinnvoll zu nutzen. Aus diesem Grund wurde auch die Zeitachse manuell erstellt, damit die Einträge aus dem Log-File mit aufgetragen werden.

Die **.eml* - Dateien und deren Metadaten konnten direkt in *Axiom Examine* ausgelesen werden. Nur der Inhalt der E-Mail konnte nicht ausgelesen werden. Dafür wurden die **.eml* - Dateien exportiert und mit dem *Editor* geöffnet. Das Auslesen der Registry hat die erwarteten Ergebnisse erzielt.

5.2 Gesamtprojekt

Das Gesamtprojekt ist innerhalb von 7 Wochen in einer Gruppe bearbeitet worden. Nach der gemeinsamen Entscheidung für einen Fall konnten die für diesen notwendigen Dateien angelegt und mit der Erstellung eines Images begonnen werden. Aus Performance Gründen der VMs, verfügbarem Speicherplatz, sowie der Dauer von Uploads und Analysen wurde zunächst ein Linux Image erstellt, welches durch Axiom teilweise analysiert werden konnte. Nach einer Rückfrage erhielten wir den Hinweis das wir bei einer Wahl von Linux mit Punktabzügen zu rechnen hätten, daher wurde das bereits erstellte Linux Image verworfen und ein Windows System für den Fall angelegt.

Bei der Wahl einer Software zur Analyse wurden alle bereitgestellten Tools geprüft und Axiom als die beste Software für diese Analyse empfunden. Bei dem Prüfen der verschiedenen Tools in den VMs der Hochschule traten nach sehr langen Laufzeiten beim Upload oder der Analyse des Images Fehler auf.

Die Software auf den Servern der Hochschule erfüllte zudem nicht die Anforderungen, die die Softwareanbieter an Ihre Software stellen. Im laufe des Projekts wurde aus diesem Grund eine Offline Version von Axiom zur Verfügung gestellt, mit der die Analyse ohne Probleme durchgeführt werden konnte.

Der Fall konnte anhand vorgeschlagener Artefakte analysiert werden. In Teilen musste jedoch für ein brauchbares Ergebnis händisch nachgearbeitet werden.

Das Projekt konnte trotz der vielen Probleme mit Hard- und Software durch die gute Zusammenarbeit in der Gruppe erfolgreich bearbeitet werden.