Hochschule Wismar
Studiengang Master „IT-Sicherheit und Forensik“

PRAKTIKUMSBERICHT

Gruppe 01 FFM

Modul „Forensik in Betriebs- und Anwendungssystemen“

Eingereicht am: 24. Juli 2020
von: Ulrich Bielenstein
Tommy Neubert
Christian Frenzel

Inhaltsverzeichnis

Abbildungsverzeichnis

1 Aufgabenstellung

Das Ziel der Praktikumsaufgabe besteht darin, bez. eines Computers oder eines mobilen Gerätes ein Festplatten- oder Daten-Image zu erzeugen und dieses Image unter Nutzung einer speziellen Forensik-Software zeitbasiert auszulesen und zu analysieren.

2 Szenario und Vorbereitung

Das diesem Praktikum zugrundeliegende Szenario spielt mit dem klassischen Motiv des betrogenen Betrügers, nur dass es sich hier um einen ausspionierten Spion handelt.

Ausgangspunkt ist eine Erkundungsmission, auf die ein bundesdeutscher Agent namens Manuel Opfermann in den Kaukasus gesandt wird.
Opfermann tarnt sich als Reporter, der an einer Dokumentation über die Gebirge des Nahen Ostens arbeitet. Seine geheime Mission besteht jedoch darin, vor Ort etwaige Raketenstellungen der im dortigen Gebiet operierenden Rebellen zu erkunden und zu fotografieren. Die Aufnahmen will Opfermann mittels Steganografie in seinen unverfänglichen Berichten verbergen (Datenverschleierung im herkömmlichen Sinne).

Auf seiner Mission trifft der Agent Opfermann auf ortskundige Einheimische und freundet sich mit einem von ihnen an. Der Einheimische, der nur seinen ungewöhnlichen Kampfnamen A. N. Greifer nennt, berichtet Opfermann ausführlich über verschiedene Gebirge und insbesondere über den Kaukasus. Tatsächlich ist A. N. Greifer ein Mitglied der im Kaukasus operierenden Rebellenorganisation, die auf Opfermanns Aktivitäten aufmerksam geworden ist.

Unter dem Vorwand, ihm schriftliche Informationen geben zu wollen, sendet A. N. Greifer an den scheinbaren Journalist Opfermann eine selbstextrahierende Archivdatei, die nicht nur die versprochene PDF-Datei, sondern auch Schadcode enthält. Bei diesem Schadcode handelt es sich um eine „Reverse Shell“, die eine Verbindung zum angreifenden Rechner im nahegelegenen Rebellenstützpunkt aufbaut.

Opfermann öffnet arglos die Datei und aktiviert damit die verborgene Malware. Die Rebellen können jetzt auf seinen kompromittierten Rechner zugreifen und weitere Daten und Informationen über den Reporter erlangen. Abschließend versuchen die Angreifer ihre Spuren auf dem angegriffenen Rechner Opfermanns zu verwischen (Datenverschleierung im Sinne der Anti-Forensik).

Nach seiner Rückkehr nach Deutschland wird Opfermanns Laptop routinemäßig forensisch untersucht. Diese Untersuchung wird in diesem Praktikum durchgeführt und im vorliegenden Praktikumsbericht beschrieben.

2.1 Definition Datenverschleierung

Die Datenverschleierung auch bekannt als Steganografie ist die Kunst oder Wissenschaft der verborgenen Speicherung oder Übermittlung von Informationen in einem Trägermedium.
Der Einsatz durch Steganografie hat das Ziel der Geheimhaltung und die Vertraulichkeit zu wahren. **Informationen werden so verborgen,** dass ein Dritter bei Betrachtung des Trägermediums keinen Verdacht schöpft. Damit ist zugleich erreicht, dass die verborgenen Informationen
nicht Dritten bekannt werden, d.h. die Geheimhaltung ist (wie bei der Kryptographie) gewährleistet.

Datenverschleierung oder auch Steganografie ist ein Oberbegriff.
Dieser kann unter anderem in folgende Bereiche unterteilt werden:

- Semagramme: Nachrichten, die in Details von Schriften oder Bildern verborgen sind
- Anamorphose: Betrachtung einer Information im Bild aus einem bestimmten Blickwinkel
- Maskierung: Open Code, wie Nicetext z.B. Spammimic
- Jargon, Milieu Code: Sondersprachen, wie „Schnee“ für Kokain
- Unsichtbarer Klartext: Text mit Tintenlöscher oder Zitronensaft verfassen
- Wasserzeichen
- Steghide: Trägerdatei .bmp, .jpg, .wav, und .au

Darüber hinaus hat der Begriff Datenverschleierung im Kontext der IT-Forensik, genauer: in der Anti-Forensik, noch eine weitere Bedeutung. Angreifer bemühen sich oftmals die Spuren ihrer Angriffe zu verwischen, zu löschen oder falsche Fährten zu legen. Auf diese Weise werden forensische Untersuchungen erschwert, fehlgeleitet oder komplett verunmöglicht. Die Zielsetzung der Angreifer kann dabei unterschiedlich sein. Denkbar ist zunächst, dass verborgen werden soll, dass überhaupt ein Angriff stattfand bzw. welchem Ziel der Angriff galt bzw. wie erfolgreich er war. Eine weitere Möglichkeit stellt die Absicht dar, dass etwaige Hinweise auf die eigene Täterschaft verwischt werden sollen. Weiterhin ist denkbar, dass gezielte Hinweise platziert werden, die unbeteiligte Dritte des Angriffs verdächtig machen sollen.

Die Methoden der Datenverschleierung sind vielfältig. Eine Variante ist die Manipulation bzw. Löschung von Logfiles.

Im Rahmen dieses Praktikums werden beide Varianten der Datenverschleierung, also die Steganografie als auch die antiforensische Datenverschleierung, angewendet.

2.2 Informationen zur Datenverschleierung

Um das Szenario in Kapitel 2 realisieren zu können, sind entsprechende Vorbereitungen durchzuführen. Diese bestehen aus den zwei Komponenten:

- Informationszusammenstellung der Materialien und
- E-Mail-Versand an die Person in der BRD

2.2.1 Informationszusammenstellung der Materialien

Für den Dokumentationsbericht über die schönen Gebirge des Nahen Ostens sind folgende Dateien zur Verfügung gestellt worden:

- Dokumentation_Kaukasus.pdf
- Pflanze.png
- Tiger.png

Die Abbildung 1 listet den Ordnerinhalt „Dokumentation Kaukasus“ auf.

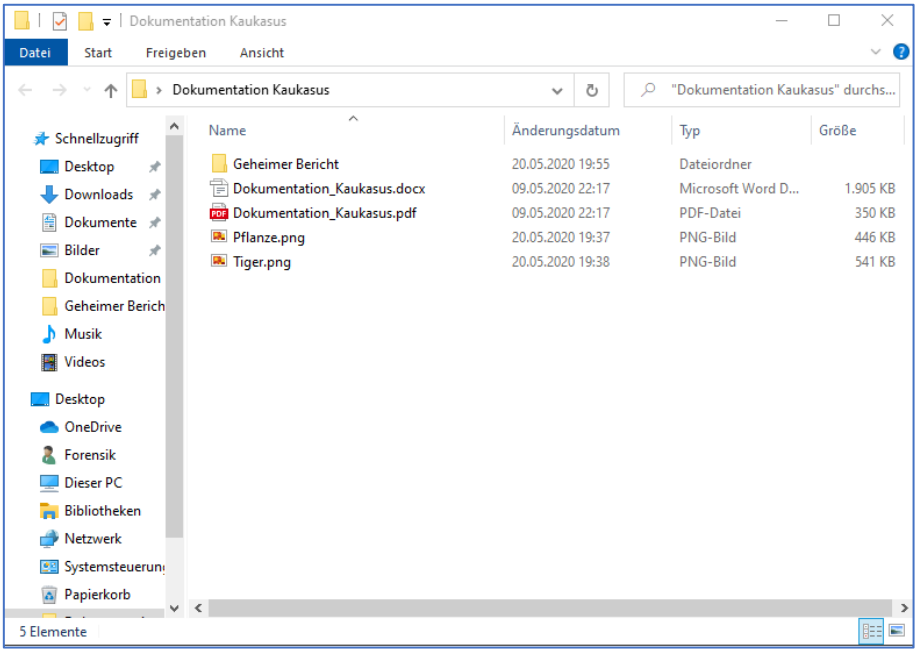


Abbildung 1: Ordnerinhalt „Dokumentation Kaukasus"

Die geheimen Informationen, die der Agent an die BRD verschleiert versenden soll, befinden sich im Unterordner „Geheimer Bericht“ im gleichen Ordner.

Dieser beinhaltet die Dateien:

- Katjuscha BM-13.png
- Katjuscha BM-21.png
- Katjuscha BM-27.png
- RSD-10.png
- Raketenstellungen.txt

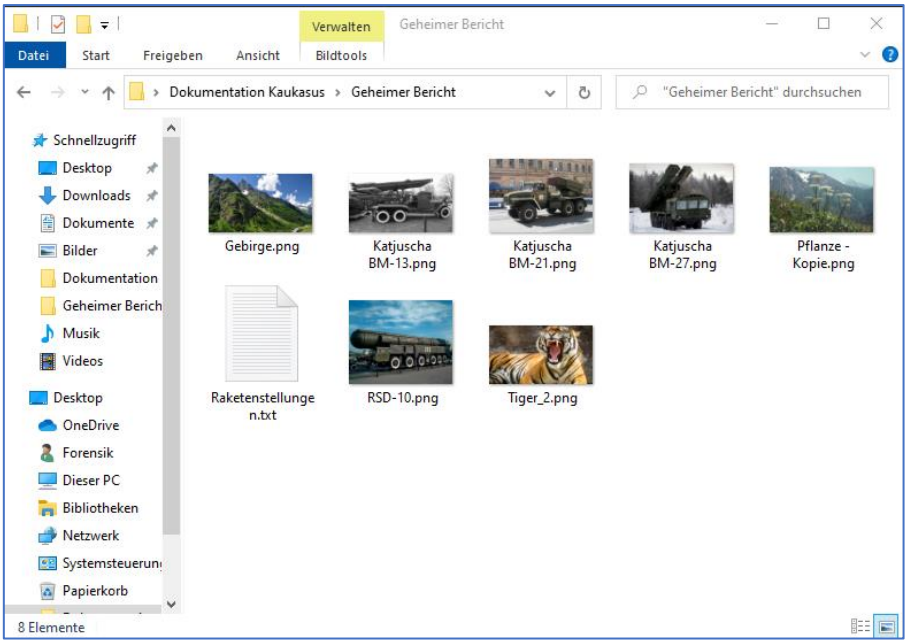


Abbildung 2: Ordnerinhalt „Geheimer Bericht"

Die Bilddateien sollen für unser Praxisbeispiel die Bilder darstellen, die der Agent im Kaukasus geschossen hat sowie seine Notizen mit den genauen Google-Koordinaten der Raketenstellungen in Verbindung mit dem Typ der Rakete in Form einer Textdatei.

Abbildung 3: Google-Koordinaten der Raketenstellungen und Typ der Rakete

Um die Datenverschleierung erfolgreich durchführen zu können, ist unter Zuhilfenahme die Software Stegano.Net eingesetzt worden. Die Software Stegano.Net ist von Herrn Sven Aßmann (Freiberuflicher Software Ingenieur Dipl. Inf. (FH)) entwickelt worden und ist ein Steghide-Tool. Unter Verwendung des Steghide-Tools in Verbindung mit der Bilddatei „Tiger_beladen“ sind die Bilddateien (Katjuscha BM-13.png, Katjuscha BM-21.png, Katjuscha BM-27.png und RSD-10.png) erfolgreich integriert worden.
Die Abbildung 4 zeigt die erfolgreiche Implementierung der Bilddateien in das „Tiger_beladen“ Bild.

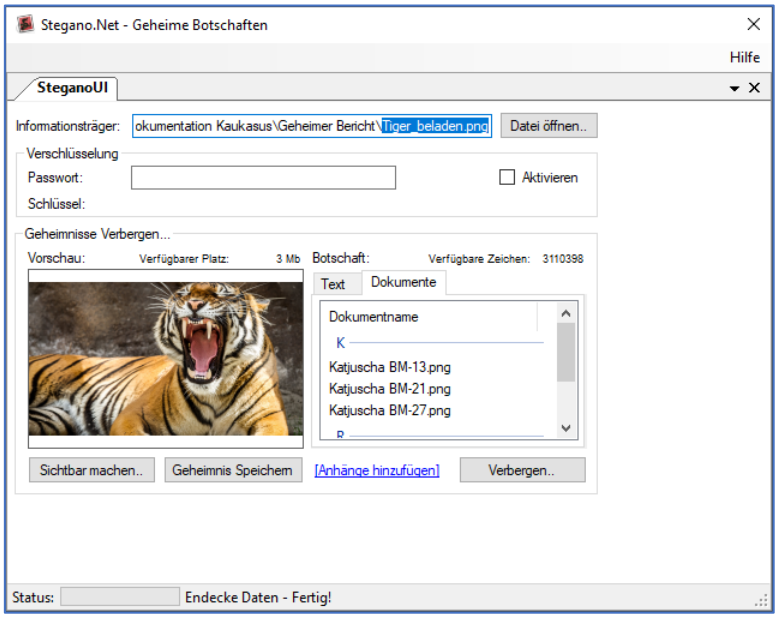


Abbildung 4: Bild „Tiger_beladen“ mit zusätzlichen Bilddateien

Nach erfolgreicher Datenverschleierung, indem die zusätzlichen Materialien in das Bild eingebettet worden sind, ist die Speicherkapazität des Bildes größer geworden. Dies veranschaulicht die Abbildung 5.

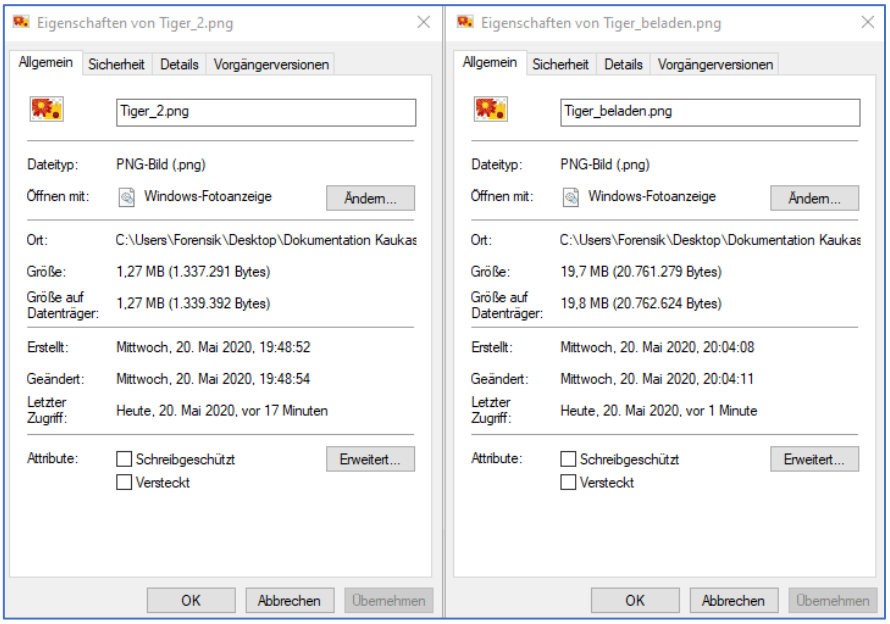


Abbildung 5: Vergleich der Änderungen bez. Speichergröße der Bilder

Das Bild links zeigt das Tiger Bild ohne zusätzliche Informationen und rechts mit den zusätzlichen Informationen.

Des Weiteren beinhaltet das Bild „Pflanze_beladen.png“ die Notizen des Agenten in Form einer Textdatei mit den Google-Koordinaten und den Typ der Rakete.

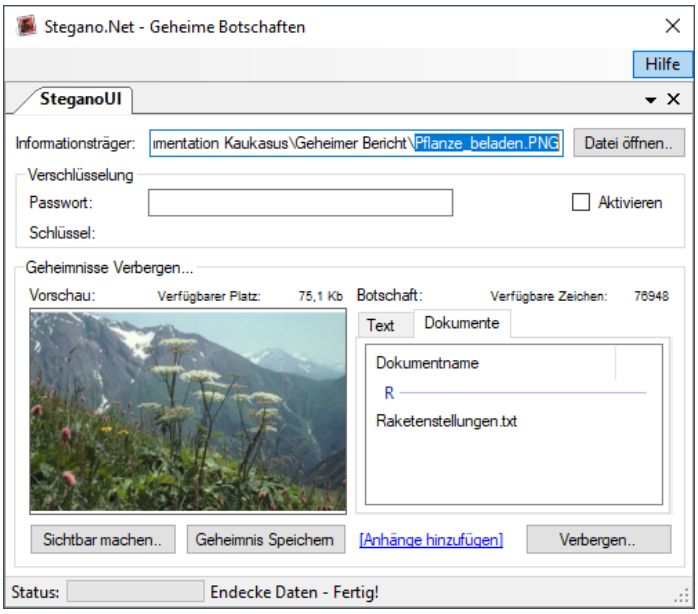


Abbildung 6: Bild “Pfanze_beladen“ mit der Zusatzinfo "Raketenstellungen.txt"

2.2.2 E-Mail-Versand

Nach erfolgreicher Datenverschleierung der Informationen in die beiden Bilddateien “Tiger_beladen.png“ und “Pflanze_beladen.png“ sind die Informationen an die BRD versendet worden. Hierzu wurde ein spezieller Text an die BRD mit den Hinweisen von Zusatzinformationen formuliert. Als möglicher Empfänger wurde die E-Mail an unser Gruppen-Mitglied Herr Tommy Neubert gesendet. Die Abbildung 7 zeigt die erfolgreiche Versendung der E-Mail mit dem Dokumentationsbericht sowie der Bilddateien.

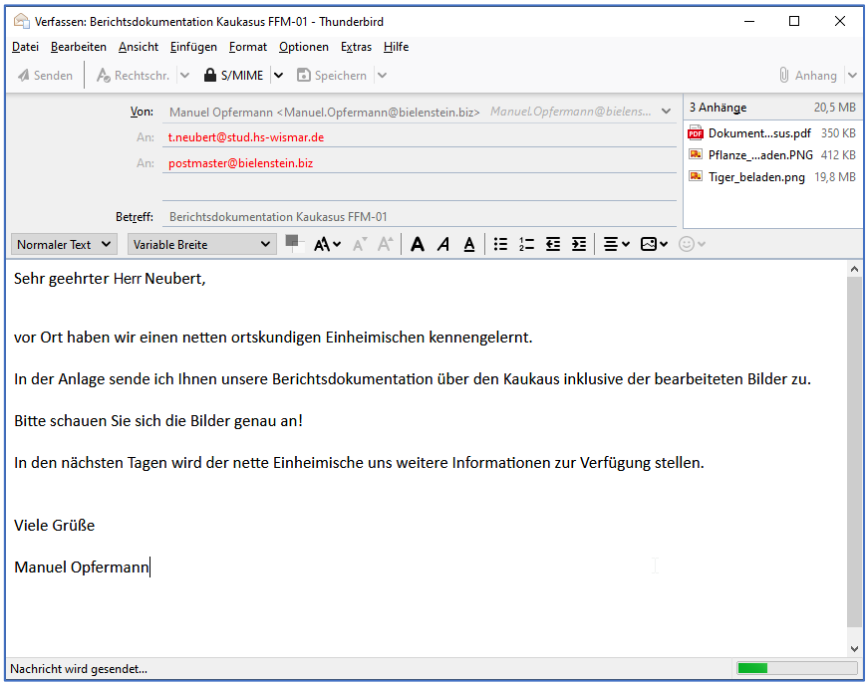


Abbildung 7: Versendung der E-Mail an die BRD mit den verschleierten

3 Vorbereitung und Durchführung des Angriffs

In diesem Abschnitt werden die Vorbereitung sowie die Durchführung des Angriffs beschrieben. Es wird mittels Metasploit, einem Bordmittel von Kali-Linux, die Malware erstellt. Anschließend wird die Malware zu einem Trojaner verpackt und an das Opfer gesendet.

3.1 Beschreibung des Trojaners

In dem diesem Praktikum zugrundeliegenden Szenario beabsichtigt der Angreifer („A.N.Greifer“) danach, den Computer des Opfers („Opfermann“) auszuspionieren.
Es handelt sich dabei also um eine Form des Advanced Persistent Threats (APT), und es kommt ein Remote Access Trojaner (RAT) zum Einsatz:

> *Bei Remote Access Trojanern (Abk. RAT) handelt es sich um eine spezielle Form von Trojanern. Der Einsatz erfolgt dabei i.d.R. gezielt, z.B. bei Advanced Persistent Threats (APTs) oder aber auch in breiteren allgemeinen Angriffen.*
>
> *Wie für Trojaner oftmals typisch, wird dem Opfer ein scheinbar nützliches Programm bereitgestellt, in dem sich tatsächlich jedoch eine getarnte Malware mit bösartiger Absicht und Zugriff aus der Ferne ("Fernadministration") verbirgt.*
>
> *Die Möglichkeiten, welche sich für den entfernten Angreifer bieten, können vielseitig sein, sind jedoch davon abhängig, mit welchen Rechten der eingeschleuste Schadcode ausgeführt wird. Denkbar ist beispielsweise, dass neben Anzeige des Bildschirminhaltes und Aufzeichnung der Tastatureingaben auch verwendete Peripheriegeräte, wie Webcams oder Mikrofone abgehört werden können. Durch Nachlässigkeit, Unachtsamkeit oder Unwissenheit führt ein Benutzer das scheinbare nützliche Programm mit administrativen Rechten aus. Durch dieses wird dann der entsprechende Schadcode nachgeladen und ausgeführt.*
>
> *Durch den Einsatz von Remote-Access-Trojanern (RATs), als Untergruppe der klassischen Trojaner, wird durch den Angreifer primär das Ziel verfolgt, eine Hintertür ("Backdoor") auf dem System des Opfers einzurichten. Über diese Hintertür strebt ein Angreifer die Fernsteuerung ("Remote-Access and Administration") des Opfersystems ohne Kenntnis des Eigentümers/Betreibers an. Es wird besonderer Wert daraufgelegt, hierbei möglichst lange oder im besten Falle für immer unerkannt zu bleiben. Sind die Ziele des Angreifers erreicht, so werden oftmals im Anschluss sämtliche Spuren entfernt oder verwischt, damit die verwendete Technik zukünftig nicht durch Heuristiken oder Signaturen erkannt wird.*[1]

Konkret kommt in diesem Fall eine selbstentpackende Archivdatei zum Einsatz, die neben der Malware auch eine Nutzlast, hier eine Dokumentation über den Kaukasus, enthält.

[1] https://it-forensik.fiw.hs-wismar.de/index.php/Remote_Access_Trojaner_(RAT)

3.2 Erstellung der Malware

Zunächst ist unter Kali Linux mithilfe von Metasploit, genauer: mit msfvenom, die Malware als unter Windows lauffähige *.exe-Datei erstellt worden.

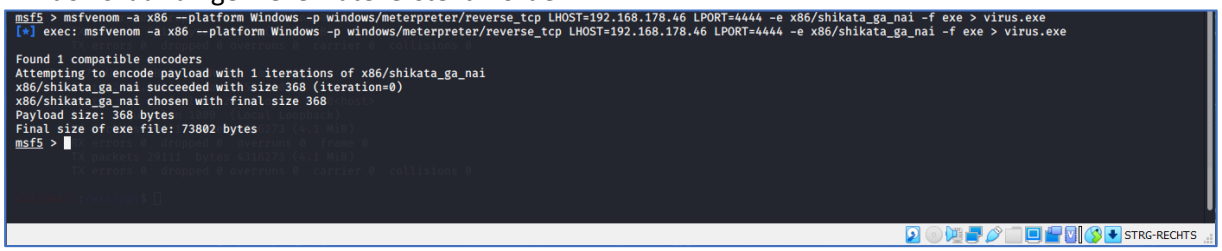


Abbildung 8: msfvenom erstellt die Malware

3.3 Erstellung und Versand des Trojaners

Der Virus wird unter Windows mit Hilfe des Programmes „WinRAR“ in ein selbstentpackendes Archiv (SFX-Datei) komprimiert. In SFX-Dateien gepackte Daten kann der Empfänger entpacken, ohne dass er eine Software für die Komprimierung installiert hat.
Die SFX-Datei wird so konfiguriert, dass die Datei „virus.exe“ sofort nach dem Entpacken ausgeführt wird, wohingegen die Dokumentation über den Kaukasus normal entpackt wird. Der Empfänger merkt so kaum, dass er soeben einen Trojaner ausgeführt hat.

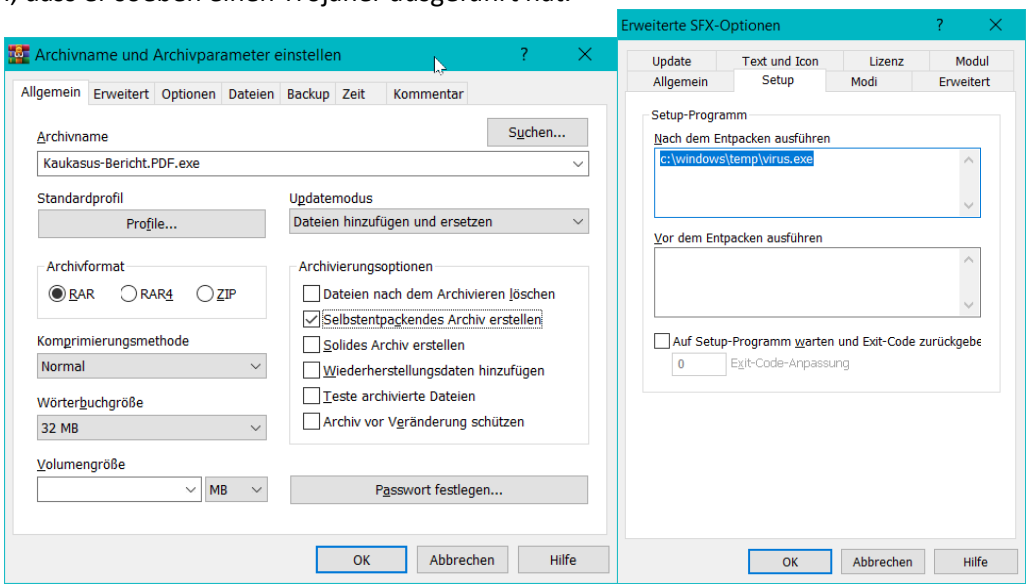


Abbildung 9 Erstellung des Trojaners

Wenn zusätzlich das Archiv mit einem Passwort verschlüsselt wird, dann hat der Virenscanner auf der Empfängerseite keine Chance den Virus rechtzeitig zu erkennen.

3.4 Durchführung des Angriffs zur Kompromittierung des IT-Systems

Um das Laptop des Agenten erfolgreich zu kompromittieren, hat der Angreifer (der nette und freundliche Einheimische) einen Trojaner gebaut und den Trojaner mit zusätzlichen Materialien (einer weiteren PDF-Datei) in ein selbstentpackendes Archiv erstellt. Die genaue Beschreibung zur Erstellung des Trojaners ist in Kapitel 3.2 erläutert.
Damit ein Hacking-Angriff erfolgreich ist, besteht dieser aus vier essentiellen Phasen, diese sind:

1. Aufklärung
2. Scan
3. Eindringen
4. Nachbereitung und Erhaltung des Zugriffs

Die Phasen Aufklärung und Scan werden für das Praxisprojekt nicht weiter betrachtet, da diese im Vorfeld in Form des Kommunikationsaustausches zwischen dem Reporter (Agent) und dem netten freundlichen Einheimischen (Angreifer) passiert ist.

3.4.1 Eindringen

In dieser Phase ist das Eindringen der Vorgang, die Kontrolle über ein System zu gewinnen. Diese Phase wird auch als Exploitation bezeichnet, weil eine Schwachstelle erfolgreich ausgenutzt wird. In unserer Fallkonstellation ist die Schwachstelle der Mensch, konkret der Reporter (Agent), indem er auf die E-Mail des netten Einheimischen (Angreifer) geklickt hat und den Anhang heruntergeladen sowie das selbstentpackende Archiv ausgeführt hat.
Bei der Ausführung des selbstentpackenden Archives wurde im Hintergrund eine „Reverse Shell“ gestartet. Das besondere bei einer „Reverse Shell“ ist, dass das Opfer IT-System eine Verbindung zu der Angreifer-Maschine aufbaut und somit mögliche Firewall-Regeln umgeht, da von einem internen IT-System eine Verbindung zu einem externen IT-System aufgebaut wird.
Die Abbildung 10 veranschaulicht grafisch das Konzept einer „Reverse Shell“.

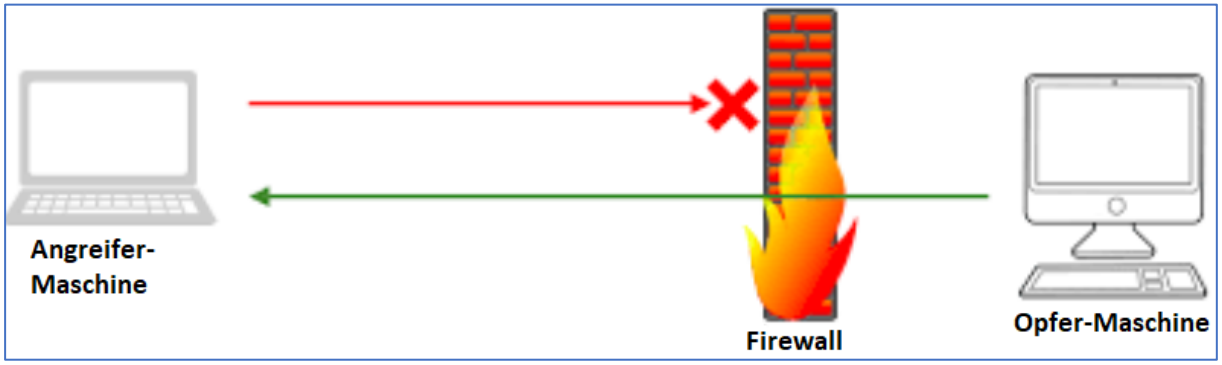


Abbildung 10: Konstrukt einer „Reverse Shell“

Nach erfolgreichem Starten der „Reverse Shell“ hat der Angreifer Zugriff auf das Opfer IT-System, dies veranschaulicht Abbildung 11.

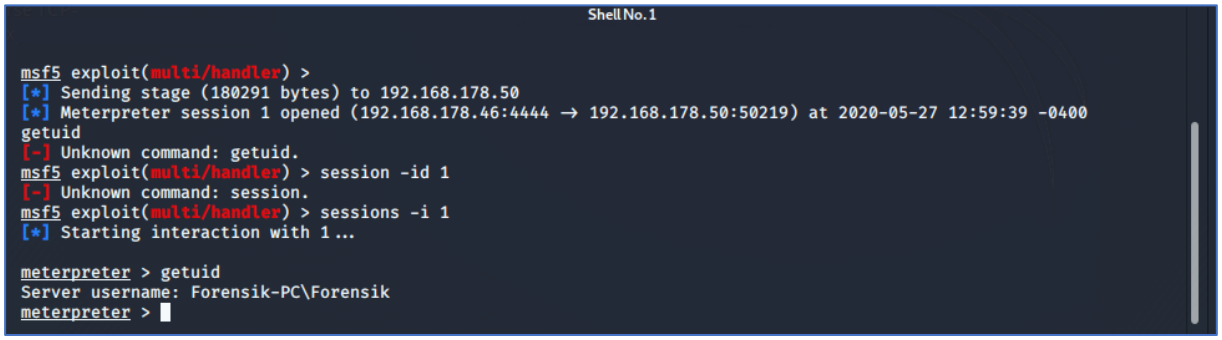


Abbildung 11: Zugriff auf das Opfer IT-System via Reverse Shell

Hierbei sind vom Angreifer verschiedene Shell- und Windows-Befehle durchgeführt worden, um mehr Informationen über das Opfer IT-System des Reporters (Agenten) zu erhalten.

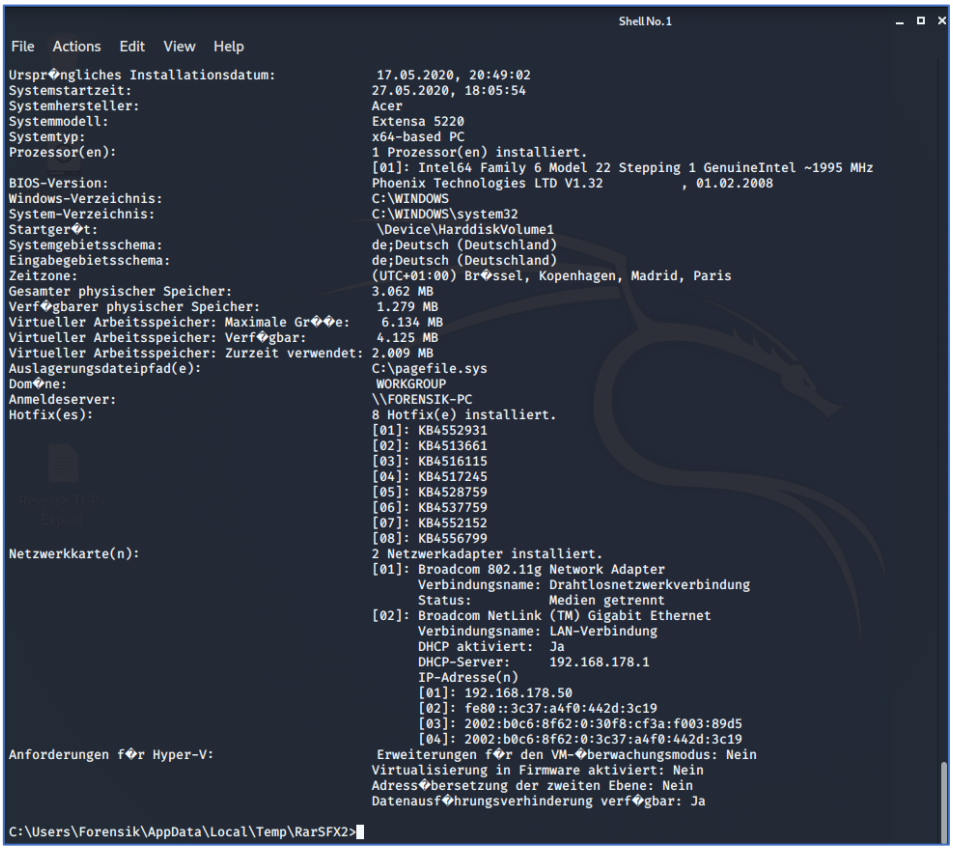


Abbildung 12: Befehl „sysinfo“ gibt Informationen über den Ziel-Host an.

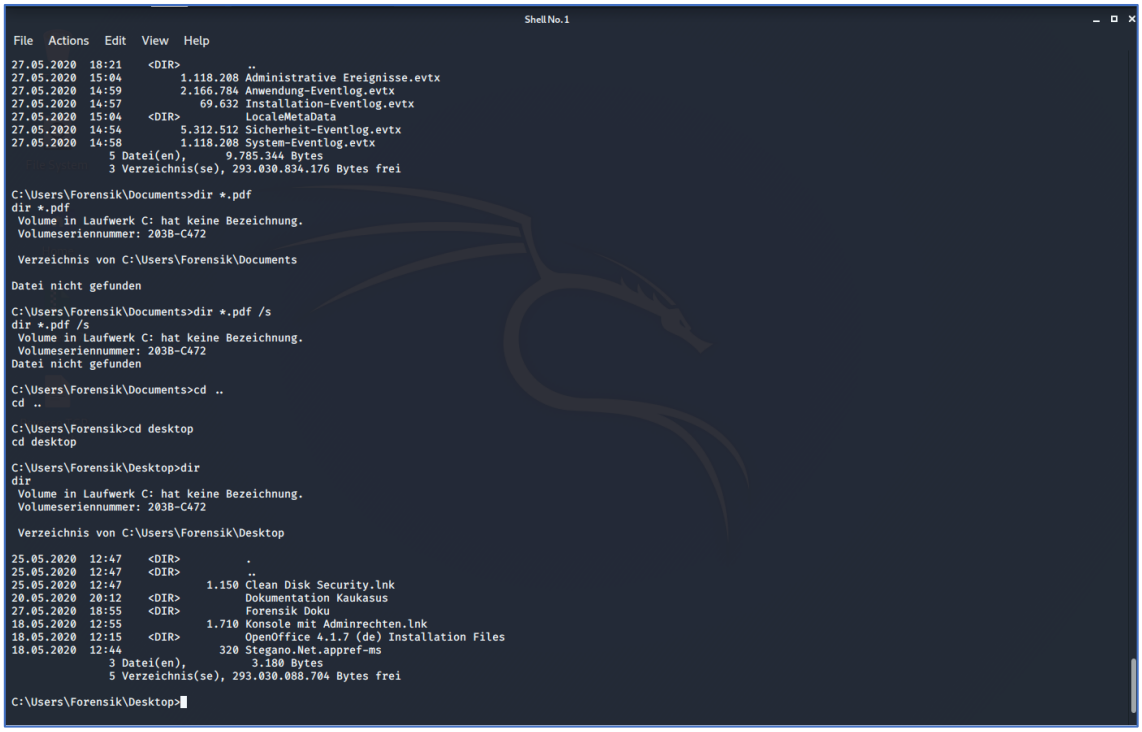


Abbildung 13: Ordnerauflistung im Verzeichnis „Desktop“ via Shell- und Windows-Kommandos

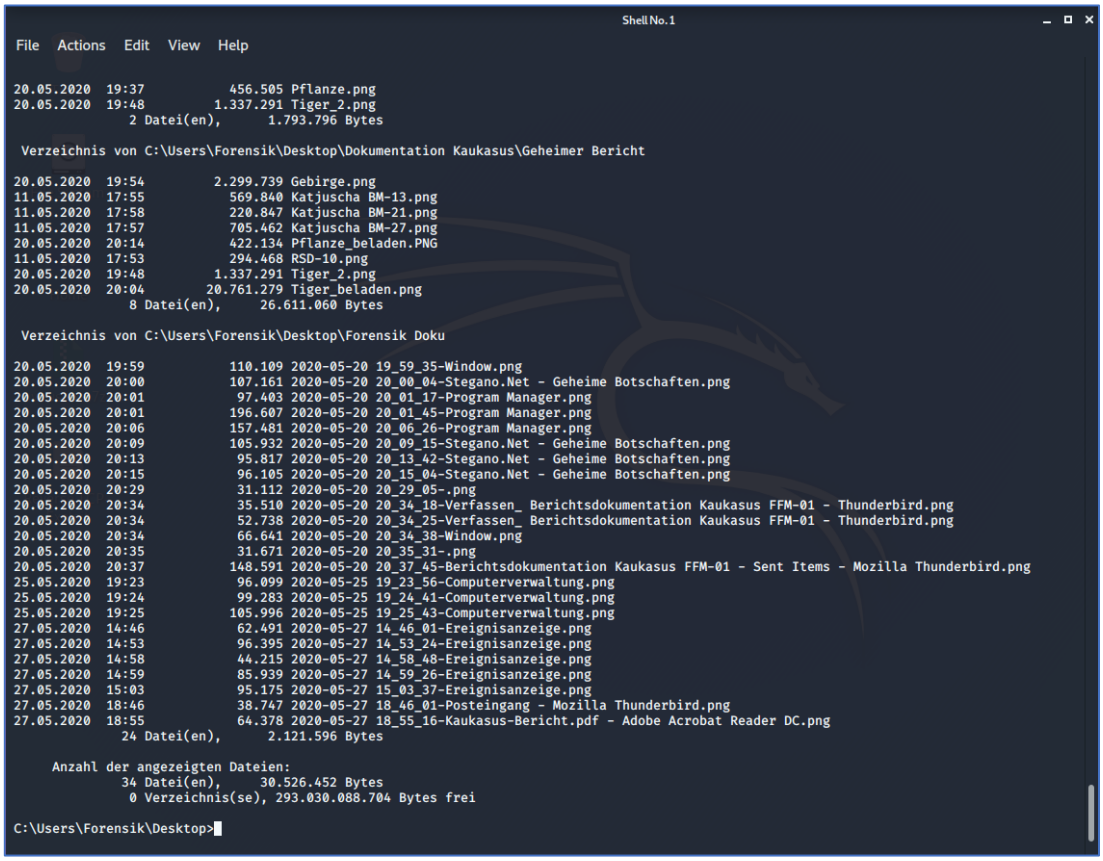


Abbildung 14: Routing in das Zielverzeichnis „Forensik Doku“

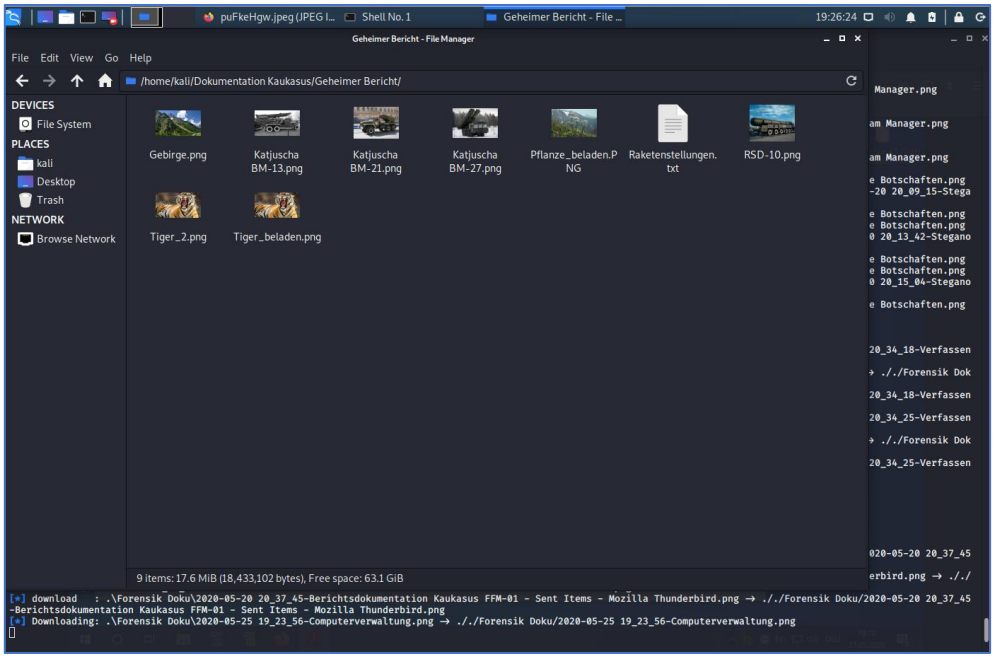


Abbildung 15: Befehl „screenshot“

3.4.2 Nachbereitung und Erhaltung des Zugriffs

Damit der Hacking-Angriff auf dem Opfer IT-System des Reporters (Agenten) unbemerkt bleibt, wurde hier wieder das Prinzip der Datenverschleierung angewendet. Hierbei werden alle Log-Einträge des Windows-Clients gelöscht.

Damit die Log-Einträge erfolgreich mit dem Befehl „clearev“ gelöscht werden können, sind erhöhte Rechte bzw. privilegierte Rechte notwendig, die das Ausführen des Befehls erlauben.

Um die erhöhten Rechte zu umgehen, wurde „Authentication Bypass“ betrieben. Dabei verschafft sich ein Angreifer mit den Privilegien eines autorisierten oder privilegierten Benutzers Zugang zu Anwendung, Dienst oder Gerät, indem er einen Authentifizierungsmechanismus umgeht. Der Angreifer ist daher in der Lage, auf geschützte Daten zuzugreifen, ohne dass jemals eine Authentifizierung stattgefunden hat.

Für die erfolgreiche Durchführung des „Authentication Bypasses“ ist unter Zuhilfenahme von Metasploit das Modul „comhijack“ ausgeführt worden. Dies erlaubt Dienste ohne erhöhte Rechte, die im Normalfall notwendig sind zu umgehen.

Die Abbildung 16 zeigt die erfolgreiche Ausführung des Moduls „comhijack“ mithilfe von Metasploit zur erfolgreichen Löschung der Windows Log-Einträgen.

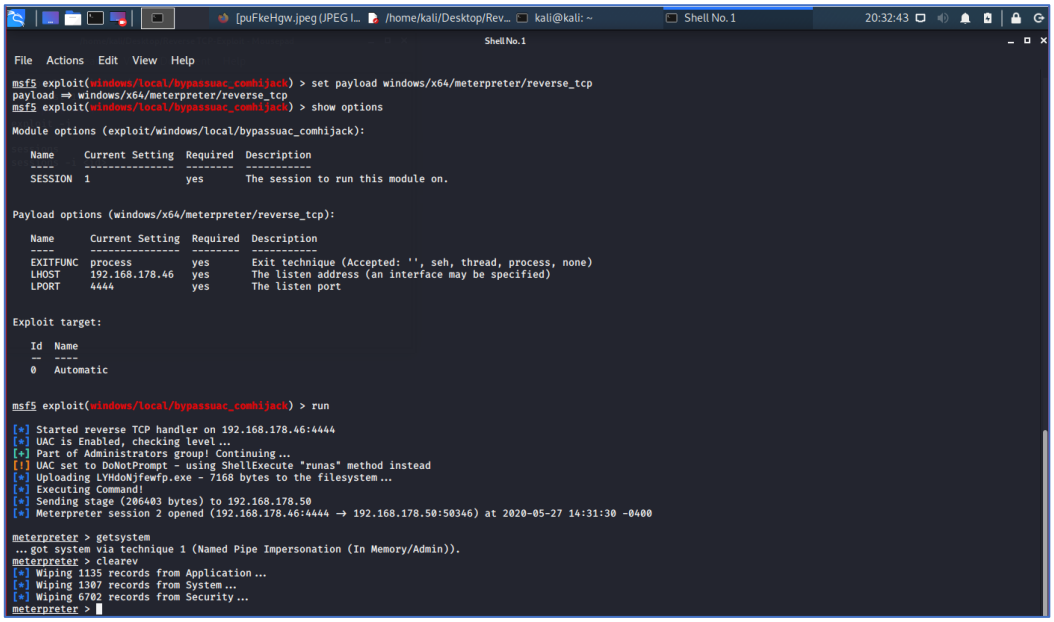


Abbildung 16: Erfolgreiche Durchführung von „Authentication Bypass“

Nach erfolgreichem Löschen der Windows Log-Einträge ist die Verbindung zum Opfer IT-System getrennt worden, weil unsere Einbruchspuren erfolgreich verschleiert haben.

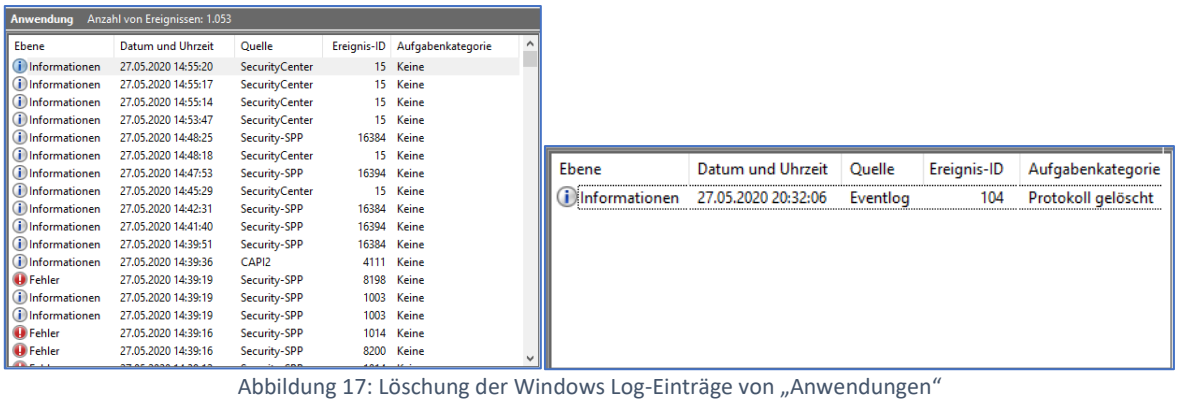
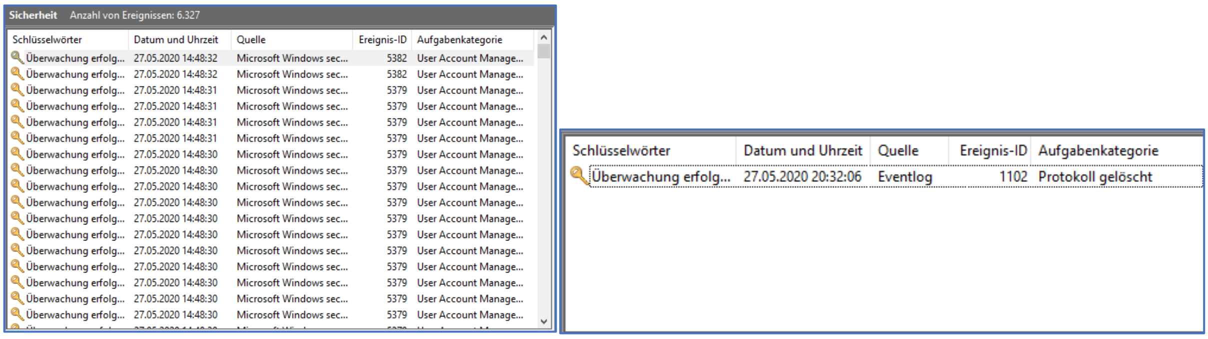


Abbildung 17: Löschung der Windows Log-Einträge von „Anwendungen“

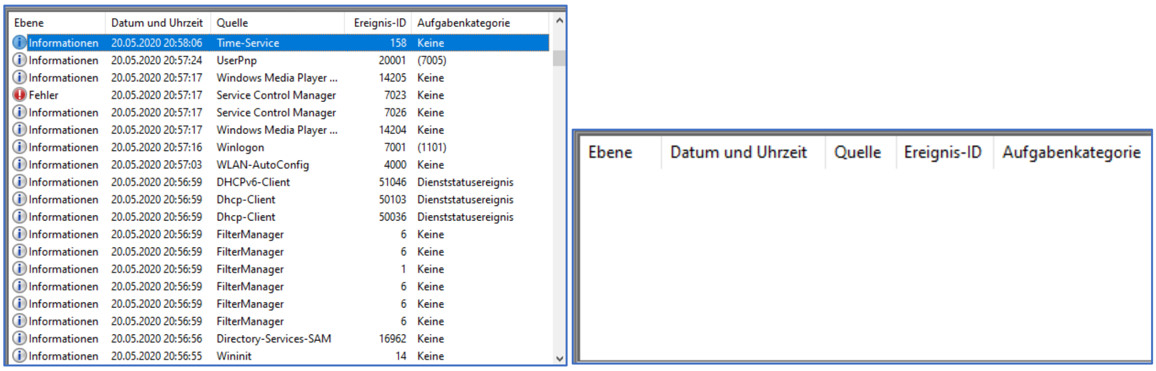


Sicherheit Anzahl von Ereignissen: 6.327

Schlüsselwörter	Datum und Uhrzeit	Quelle	Ereignis-ID	Aufgabenkategorie
Überwachung erfolg...	27.05.2020 14:48:32	Microsoft Windows sec...	5382	User Account Manage...
Überwachung erfolg...	27.05.2020 14:48:32	Microsoft Windows sec...	5382	User Account Manage...
Überwachung erfolg...	27.05.2020 14:48:31	Microsoft Windows sec...	5379	User Account Manage...
Überwachung erfolg...	27.05.2020 14:48:31	Microsoft Windows sec...	5379	User Account Manage...
Überwachung erfolg...	27.05.2020 14:48:31	Microsoft Windows sec...	5379	User Account Manage...
Überwachung erfolg...	27.05.2020 14:48:31	Microsoft Windows sec...	5379	User Account Manage...
Überwachung erfolg...	27.05.2020 14:48:30	Microsoft Windows sec...	5379	User Account Manage...
Überwachung erfolg...	27.05.2020 14:48:30	Microsoft Windows sec...	5379	User Account Manage...
Überwachung erfolg...	27.05.2020 14:48:30	Microsoft Windows sec...	5379	User Account Manage...
Überwachung erfolg...	27.05.2020 14:48:30	Microsoft Windows sec...	5379	User Account Manage...
Überwachung erfolg...	27.05.2020 14:48:30	Microsoft Windows sec...	5379	User Account Manage...
Überwachung erfolg...	27.05.2020 14:48:30	Microsoft Windows sec...	5379	User Account Manage...
Überwachung erfolg...	27.05.2020 14:48:30	Microsoft Windows sec...	5379	User Account Manage...
Überwachung erfolg...	27.05.2020 14:48:30	Microsoft Windows sec...	5379	User Account Manage...
Überwachung erfolg...	27.05.2020 14:48:30	Microsoft Windows sec...	5379	User Account Manage...
Überwachung erfolg...	27.05.2020 14:48:30	Microsoft Windows sec...	5379	User Account Manage...
Überwachung erfolg...	27.05.2020 14:48:30	Microsoft Windows sec...	5379	User Account Manage...

Schlüsselwörter	Datum und Uhrzeit	Quelle	Ereignis-ID	Aufgabenkategorie
Überwachung erfolg...	27.05.2020 20:32:06	Eventlog	1102	Protokoll gelöscht

Abbildung 18: Löschvorgang der Windows Log-Einträge „Sicherheit“



Ebene	Datum und Uhrzeit	Quelle	Ereignis-ID	Aufgabenkategorie
Informationen	20.05.2020 20:58:06	Time-Service	158	Keine
Informationen	20.05.2020 20:57:24	UserPnp	20001	(7005)
Informationen	20.05.2020 20:57:17	Windows Media Player ...	14205	Keine
Fehler	20.05.2020 20:57:17	Service Control Manager	7023	Keine
Informationen	20.05.2020 20:57:17	Service Control Manager	7026	Keine
Informationen	20.05.2020 20:57:17	Windows Media Player ...	14204	Keine
Informationen	20.05.2020 20:57:16	Winlogon	7001	(1101)
Informationen	20.05.2020 20:57:03	WLAN-AutoConfig	4000	Keine
Informationen	20.05.2020 20:56:59	DHCPv6-Client	51046	Dienststatusereignis
Informationen	20.05.2020 20:56:59	Dhcp-Client	50103	Dienststatusereignis
Informationen	20.05.2020 20:56:59	Dhcp-Client	50036	Dienststatusereignis
Informationen	20.05.2020 20:56:59	FilterManager	6	Keine
Informationen	20.05.2020 20:56:59	FilterManager	6	Keine
Informationen	20.05.2020 20:56:59	FilterManager	1	Keine
Informationen	20.05.2020 20:56:59	FilterManager	6	Keine
Informationen	20.05.2020 20:56:59	FilterManager	6	Keine
Informationen	20.05.2020 20:56:59	FilterManager	6	Keine
Informationen	20.05.2020 20:56:56	Directory-Services-SAM	16962	Keine
Informationen	20.05.2020 20:56:55	Wininit	14	Keine

Ebene	Datum und Uhrzeit	Quelle	Ereignis-ID	Aufgabenkategorie

Abbildung 19: Löschung der Windows Log-Einträge von „System“

4 Vorbereitung der forensischen Untersuchung

Dieses Kapitel beschreibt die analytische Vorgehensweise zur erfolgreichen Untersuchung des beschriebenen Fallszenarios.

4.1 Vorgehensmodell

Nach dem Secure-Analyse-Present (S-A-P) Modell werden IT-forensische Untersuchung in drei Phasen eingeteilt. Gemein ist allen drei Phasen, dass die Abläufe höchstgenau dokumentiert werden, damit die Prozessschritte im Nachhinein von einem unbeteiligten Dritten nachvollzogen werden können.

Secure
In der Secure-Phase geschehen die Identifikation, Sicherstellung und Aufbereitung potentiell relevanter Artefakte. Insbesondere werden hierbei Daten auf Datenträgern gesichert, und es werden Master- und Arbeitskopien davon angefertigt.

Analyse
Die gesicherten Daten werden in dieser Phase analysiert, interpretiert und bewertet. Die Wahl der Methode und der Werkzeuge hängen dabei stets von den Gegebenheiten des konkreten Falles ab.

Present
Die Ergebnisse der Analysephase werden nun miteinander und zueinander in Bezug gesetzt. Das sich ergebende Gesamtbild wird gemäß der Zielgruppe aufbereitet und verständlich dokumentiert.

4.2 Auswahlkriterien für den Einsatz der IT-Forensik-Tools

Grundsätzlich sind die allgemeinen Grundsätze für die Auswahl von Werkzeugen und Methoden in der IT-Forensik zu beachten. Die folgenden Auswahlkriterien wurden zugrunde gelegt und beachtet.

- **Akzeptanz:** Die im Prozess angewandten Methoden und benutzten Werkzeuge müssen von der Fachwelt beschrieben und akzeptiert sein.

  ➔ Die hier ausgewählten Tools sind in der Fachwelt bekannt und allgemein anerkannt.

- **Glaubwürdigkeit**: Die Funktionalität und Robustheit der Ermittlungsmethode sollen im Bedarfsfall nachgewiesen werden können.

  ➔ Die Einhaltung der Ermittlungsmethodik wird im vorliegenden Fall durch das 6-Augen-Prinzip sichergestellt.

- **Wiederholbarkeit**: Eine dritte Person, welche die gleichen Methoden und Hilfsmittel nutzt, soll nach Durchführung der gleichen Schritte dieselben Ergebnisse erhalten.

  ➔ Die Korrektheit der Ergebnisse der Zwischenschritte wurde unter Beachtung des 6-Augen-Prinzips stichprobenweise überprüft.

- **Ursache und Auswirkung**: Die gewählten Methoden müssen es ermöglichen, zwischen Personen, Ereignissen und Beweisspuren logisch nachvollziehbare Verbindungen zu finden.

  ➔ Das eingesetzte Werkzeug AXIOM® stellt die Erfüllung dieser Anforderung sicher.

- **Authentizität**: Auf die Echtheit/Originalität der erhobenen Daten ist Wert zu legen.

  ➔ Der Zugriff auf das Untersuchungsobjekt war auf die Teammitglieder wirksam beschränkt.

- **Integrität**: Sichergestellte Spuren dürfen nicht unbemerkt verändert werden können.

➔ Zu Beginn wurde eine Masterkopie der zu untersuchenden Festplatte erstellt, von der wiederum eine Arbeitskopie angefertigt wurde. Die Übereinstimmung der Hashwerte wurde überprüft.

- **Dokumentation**: Jeder Schritt des Prozesses soll angemessen dokumentiert werden.

Weitere spezielle Entscheidungskriterien sind die Bedienbarkeit und Handhabbarkeit der Werkzeuge sowie die Verfügbarkeit von Online-Tutorials und weiteren Informationsquellen.
Nach umfangreichen Recherchen kommt das Team zur Entscheidung als Softwarewerkzeuge

- FTK-Imager® (Version 4.3.0.18) des Herstellers AccessData® und
- Magnet Axiom (Version 3.11.0.19007) des Herstellers Magnet Forensics, Inc.

zu wählen.

Zur Auswahl standen die Softwaretools X-Ways und AXIOM.
AXIOM bietet für folgende Vorteile:

- GUI ist einfach und intuitiv verständlich zu bedienen.
- Die Einarbeitungszeit ist geringer.

X-Ways deckt den Bereich der Analyse auch ab, jedoch sind folgende Nachteile (für diesen Fall) zu groß:

- Die GUI ist sehr komplex.
- Die notwendigen Konfigurationen sind komplex durchzuführen und entsprechend zeitlich aufwändig.

Anhand von Screenshots wurden alle Schritte der Untersuchung nachvollziehbar dokumentiert.

5 Durchführung der Beweissicherung

Dies ist die Secure-Phase nach dem S-A-P-Modell.

5.1 Erstellung des Festplatten-Images

Zunächst wird die Festplatte aus dem kompromittierten Rechner ausgebaut und über eine SATA Docking Station über USB an den Untersuchungsrechner angeschlossen.

Zur Erstellung eines Abbilds der Festplatte des zu untersuchenden Laptops wird die Anwendung FTK-Imager in der Version 4.3.0.18 eingesetzt.

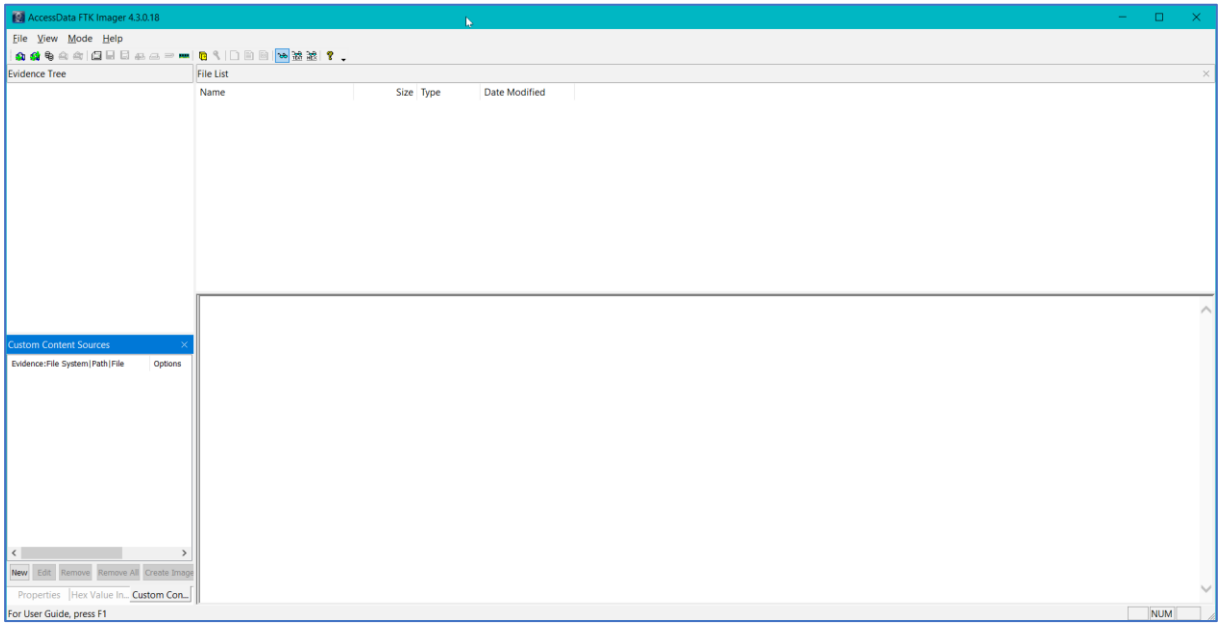


Abbildung 20: Initialbildschirm des FTK-Imagers

Durch Klick auf den Button „Create Disk Image“ wird der Prozess gestartet.

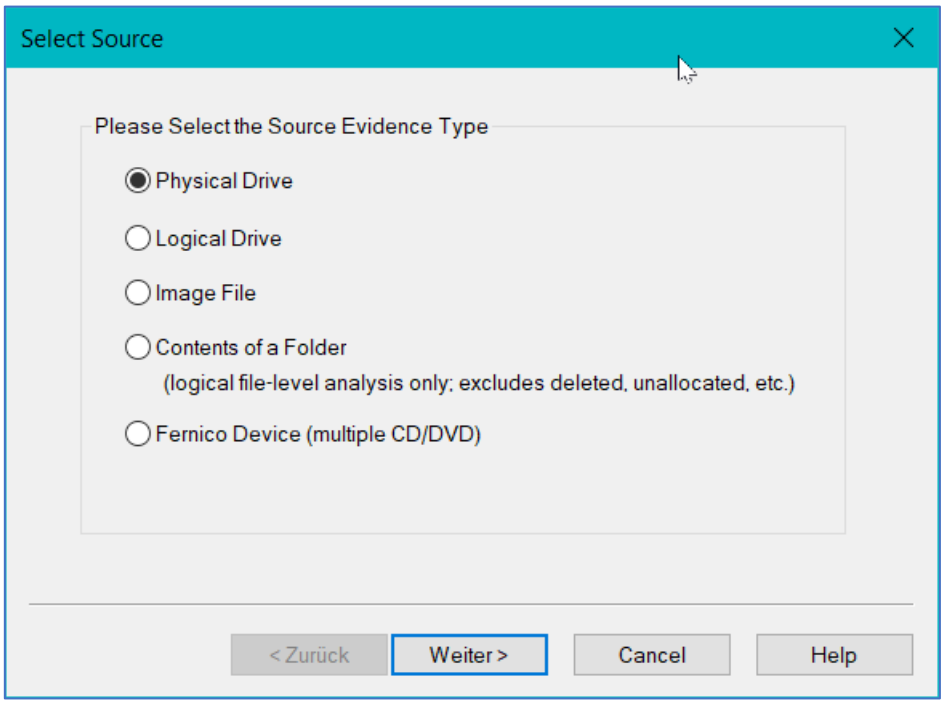


Abbildung 21: Auswahl der Ressource

Die richtige Auswahl „Physical Drive“ ist bereits vorausgewählt. Es geht weiter mit der Auswahl der angeschlossenen Festplatte.

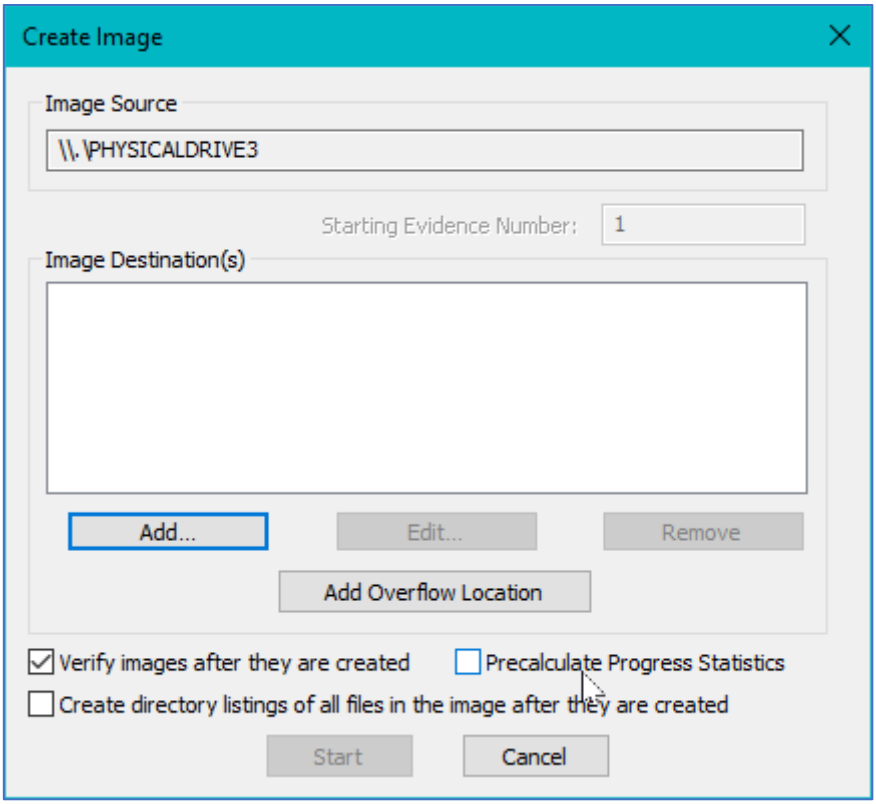


Abbildung 22: Festlegung der Parameter zur Imageerstellung

Typ und Zielverzeichnis des Images werden festgelegt.

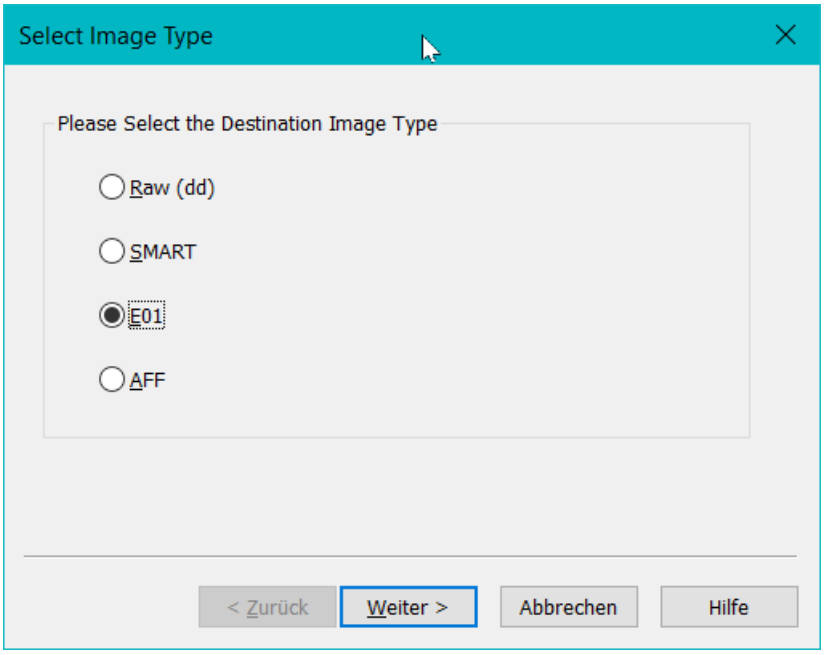


Abbildung 23: Definieren des Imagetyps

Das Format „E01“ hat die Vorteile, dass es von Axiom verarbeitet werden kann und vergleichsweise kompakt ist. Dann wird das Beweisstück mit einigen Informationen versehen.

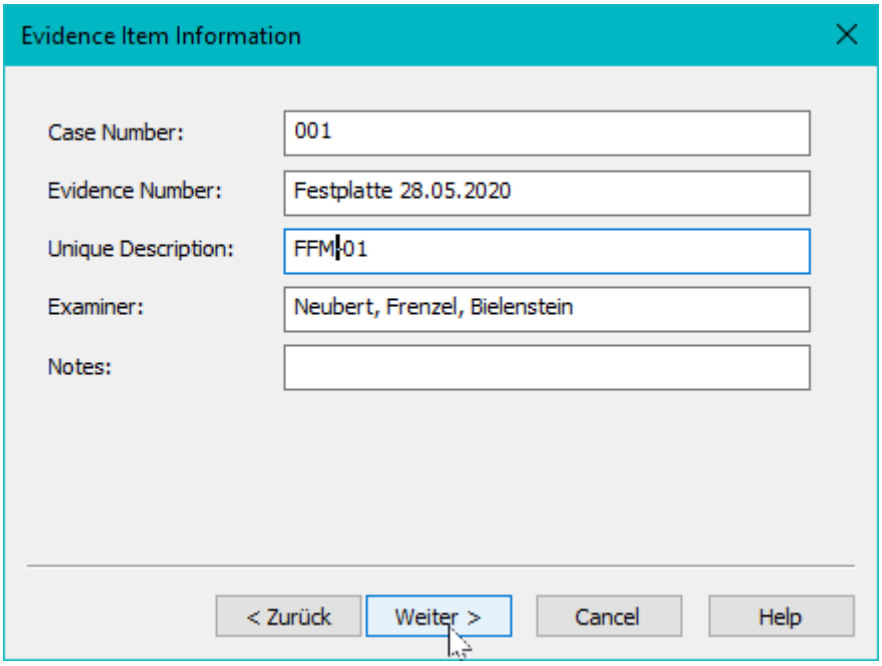


Abbildung 24: Definieren von Metadaten

Nach dem Klick auf „Weiter“ wird das Zielverzeichnis festgelegt.

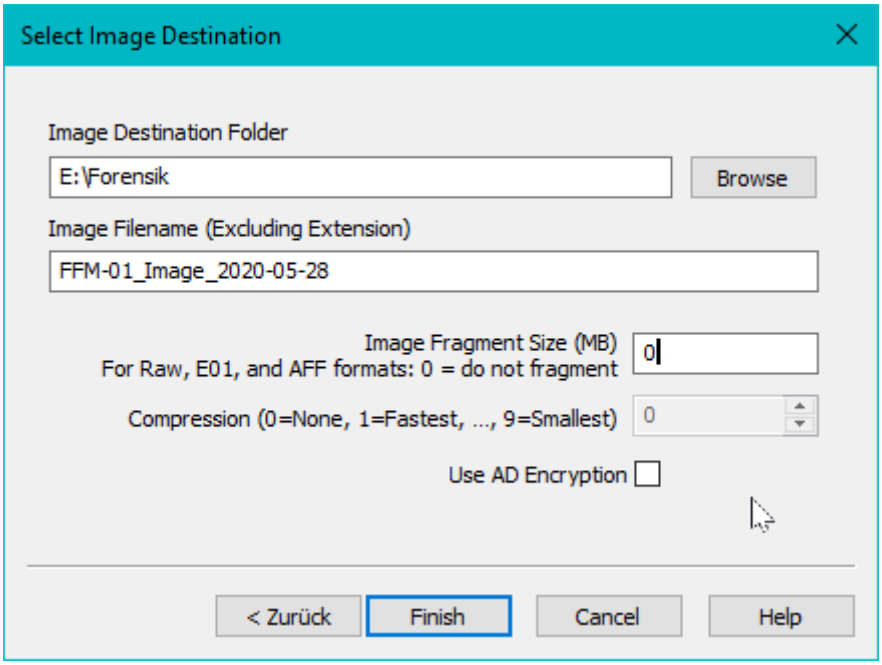


Abbildung 25: Definieren des Zielordners

Klick auf den Button „Finish“ startet nun die Imageerzeugung.

Da die Option *Verify images after they are created* zuvor aktiviert wurde, beginnt die Software direkt den Hash-Wert des Images zu berechnen und mit dem Hash der Quelle zu vergleichen, wenn der Image-Vorgang erfolgreich abgeschlossen ist. Dieser Vorgang hat in diesem Fall ca. 100 Minuten gedauert.

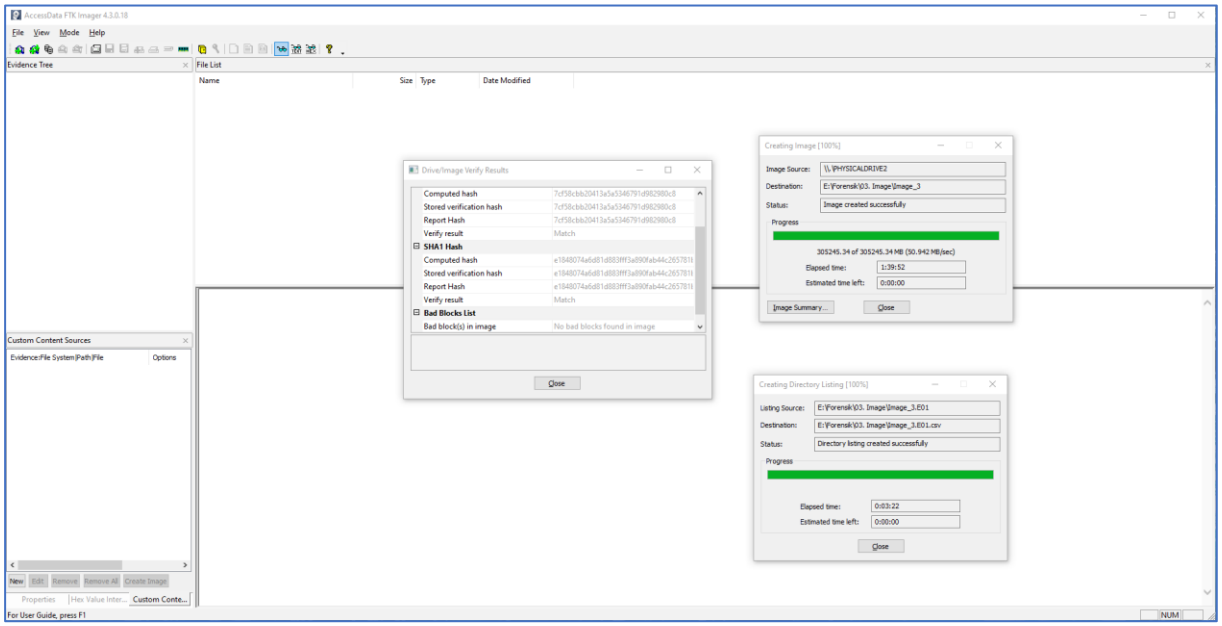


Abbildung 26: Vergleich der Hashwerte

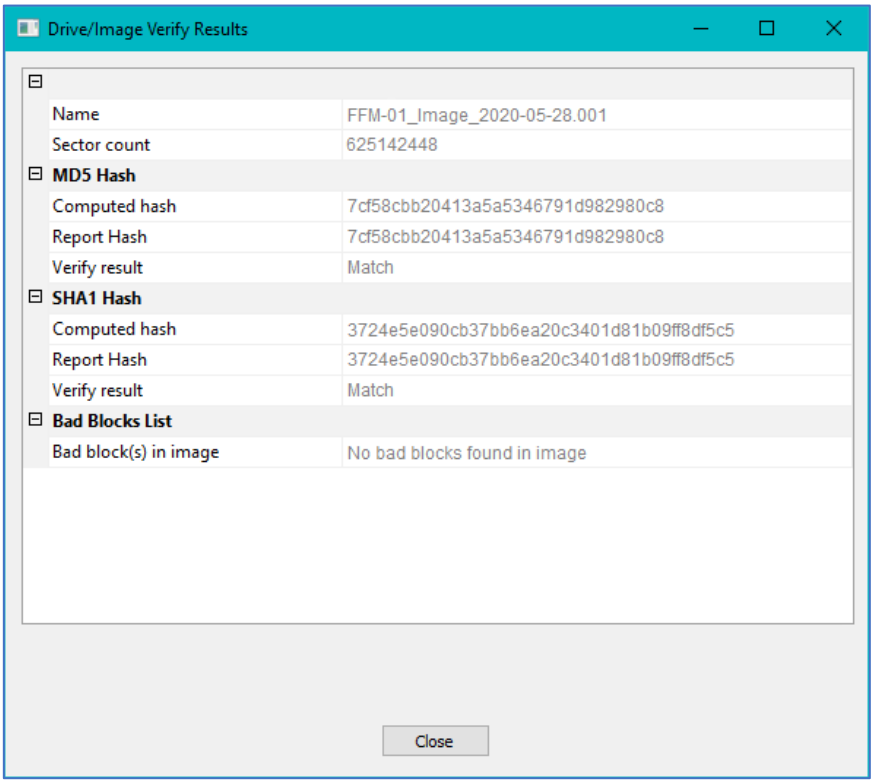


Abbildung 27: Ergebnisse der Verifizierung

6 Analyse des vorbereiteten Images

Dies ist die Analyse-Phase nach dem S-A-P-Modell.

6.1 Erstellung eines neuen Falls

Um eine Analyse zu starten, muss im ersten Schritt ein Fall erstellt werden. Dabei sind essentielle Angaben notwendig, wie Fallinformation, Speicherort der Falldaten, Speicherort für die gesicherten Beweise und die Scaninformationen.

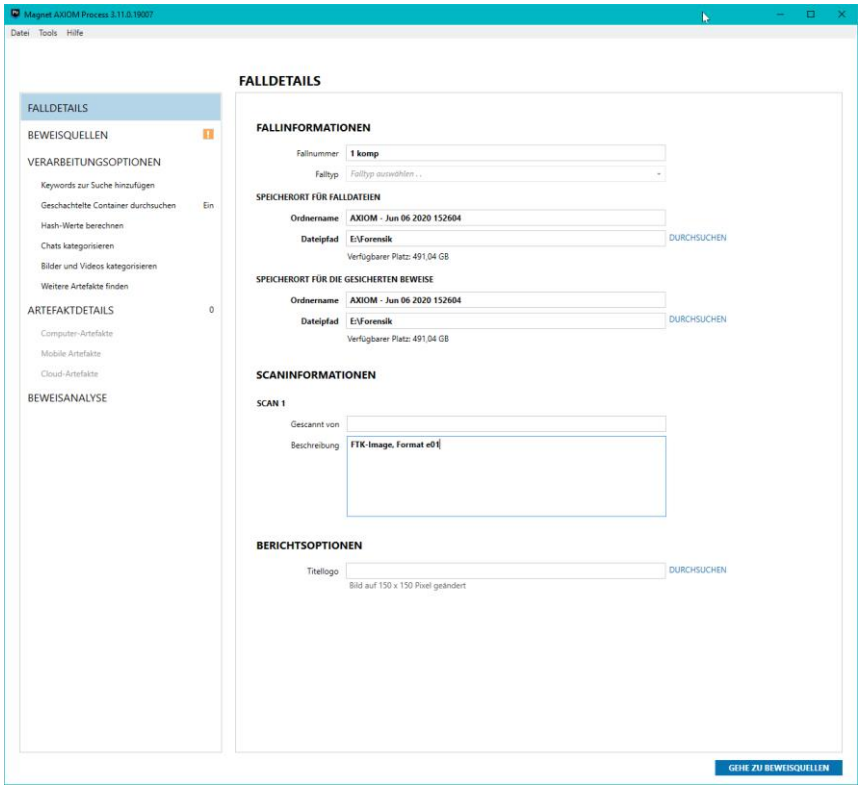


Abbildung 28: Erstellung eines Falls

6.2 Einlesen der Image-Datei

Als Beweisquelle ist die Kopie des erstellten Images verwendet worden. Nachdem das Image als Quelle hinzugefügt worden ist, hat die Software vier Bereiche der Festplatte detektiert.

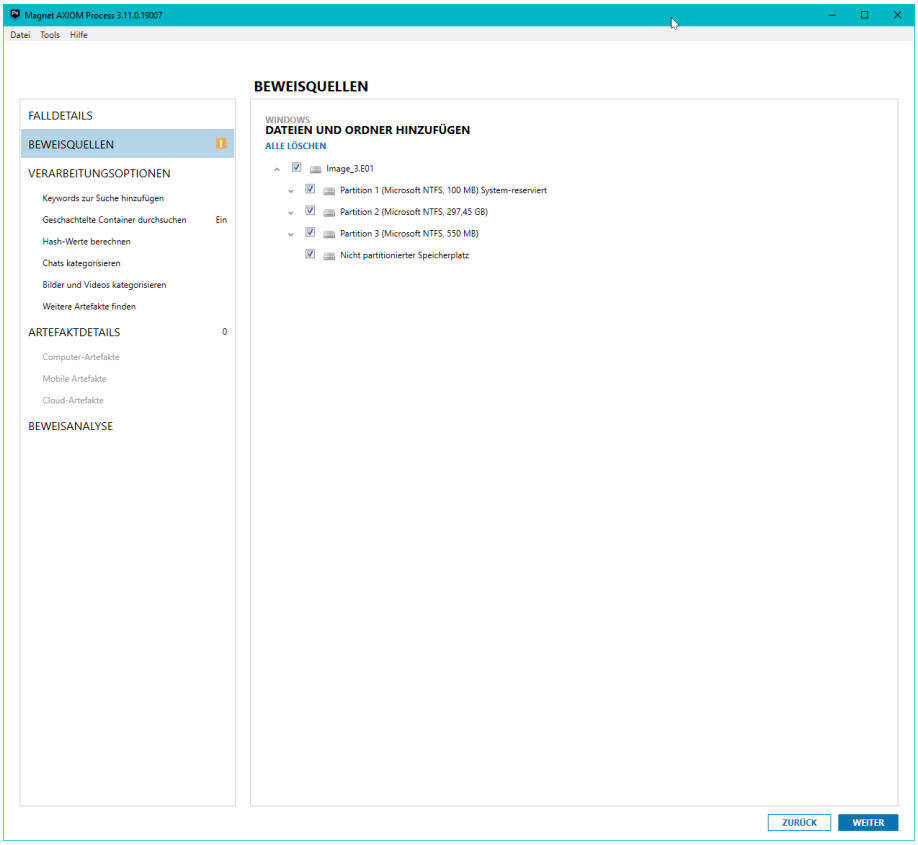


Abbildung 29: Auswahl der Partitionen

Für die jeweiligen einzelnen Partitionen 1 bis 3 wird der Suchtyp „Vollständig“ sowie der nicht partitionierte Speicherplatz auf den Suchtyp „nicht partitionierter Speicherplatz“ ausgewählt, damit alle verfügbaren Bereiche eingebunden werden.

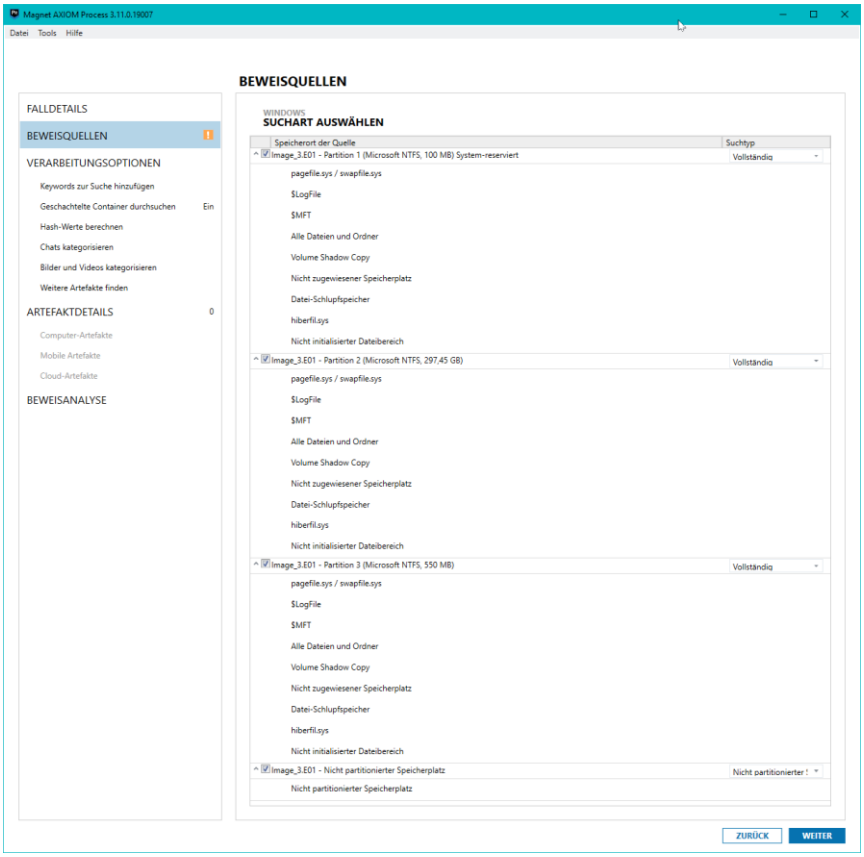


Abbildung 30: Auswahl des Suchtyps

Anschließend sind die ausgewählten Partitionen, die für die Analyse betrachtet werden sollen, zur Beweisquelle „Computer“ hinzugefügt worden.

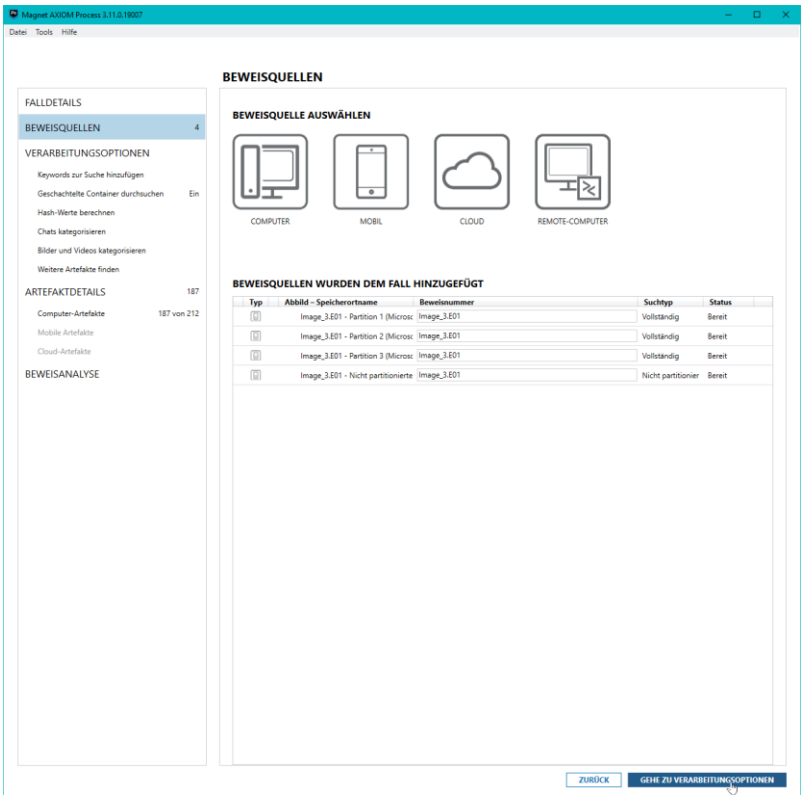


Abbildung 31: Auswahl der Beweisquelle

6.3 Aufbereitung der Daten

Bei den „Verarbeitungsoptionen“ sind die Standardeinstellungen übernommen worden.

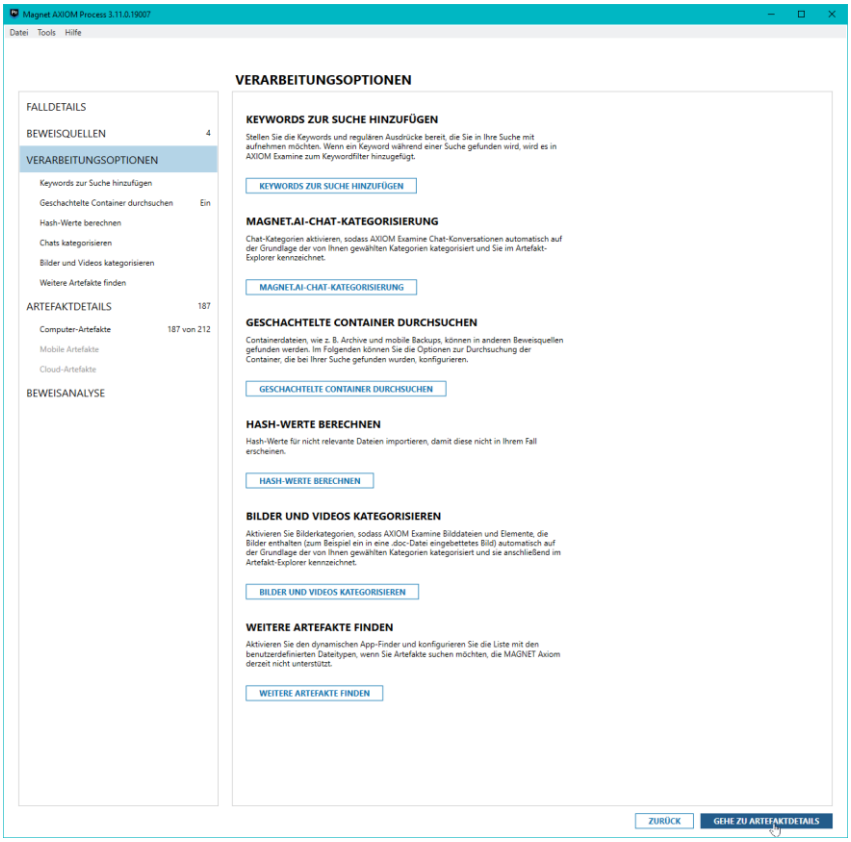


Abbildung 32: Auswahl der Verarbeitungsoption

Im Anschluss werden die „Artefaktdetails“ angezeigt, die in der Standardeinstellung übernommen worden sind.

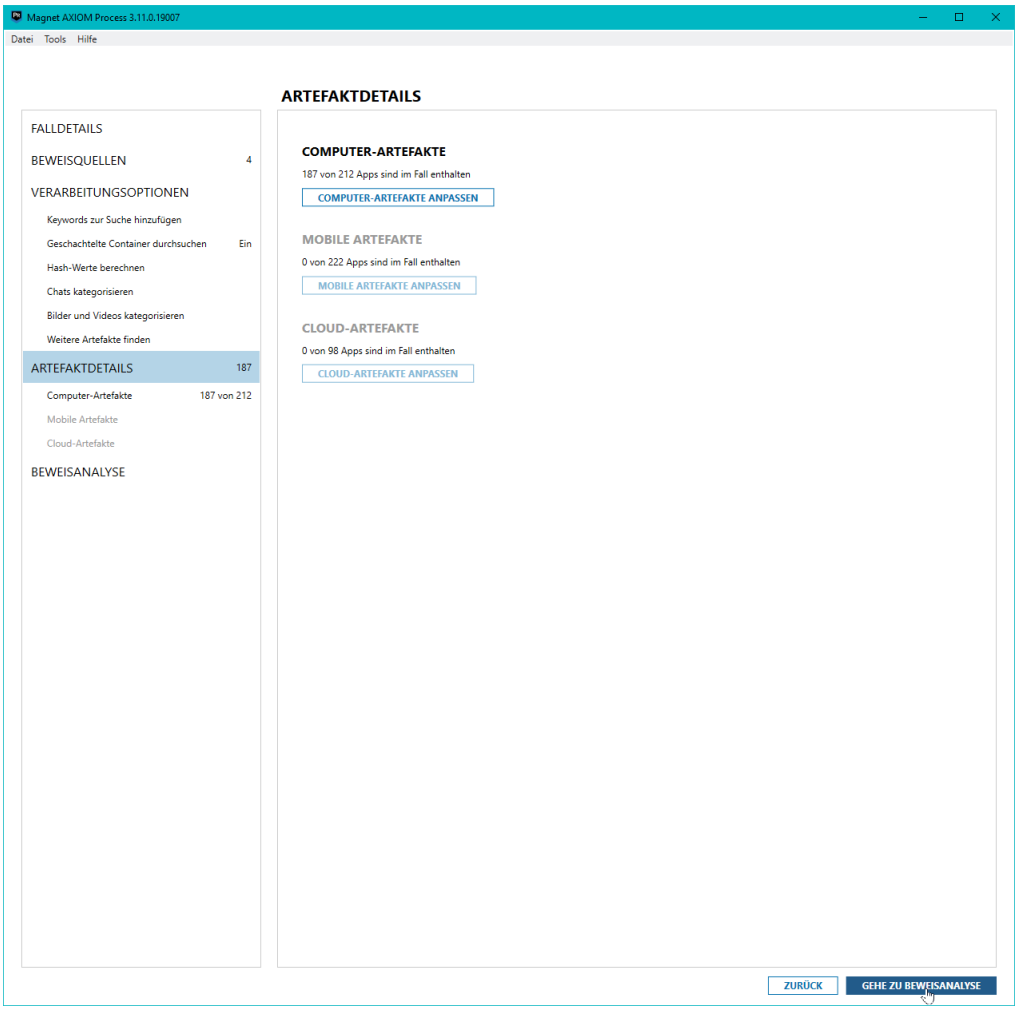


Abbildung 33: Anpassung der Computer-Artefakte

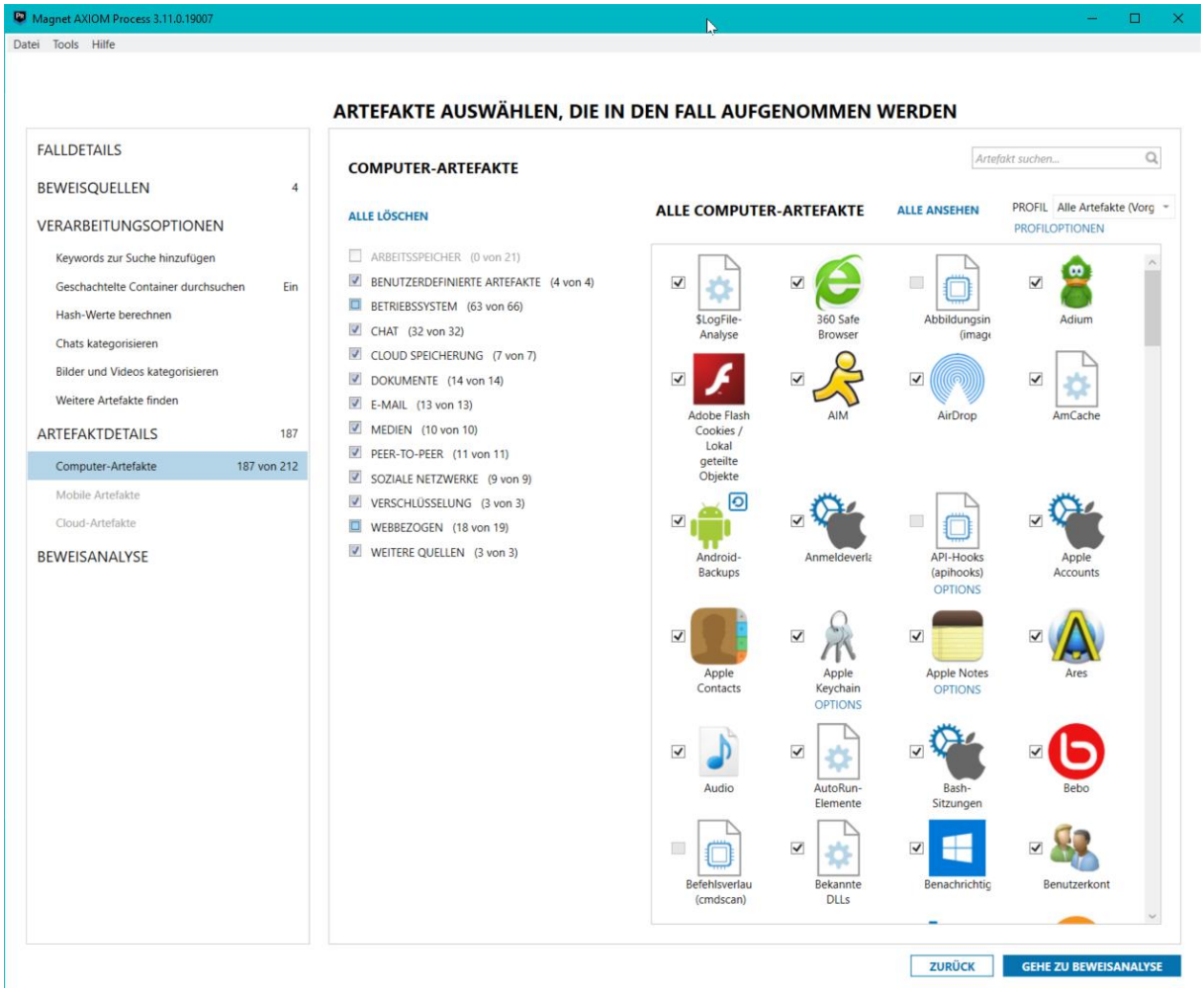


Abbildung 34: Ausgewählte Computer-Artefakte

Die für den IT-forensischen Fall bevorzugten Artefakte sind kategorisiert mit den wichtigen Attributen dargestellt. Damit wird ersichtlich, auf welche Detailebene Magnet Axiom analysiert und die weitere forensische Untersuchung fortgeführt werden muss, sind detailliert in der offiziellen *Artifact Reference*[2] die Attribute zu den wichtigen Artefakten betrachtet.

[2] https://www.magnetforensics.com/docs/artifacts/html-axiom/Content/Resources/PDFs/Artifact%20Reference.pdf

Bevor die Analyse gestartet wird, wurde nochmals eine Auflistung der dann bearbeiteten Quellen angezeigt.

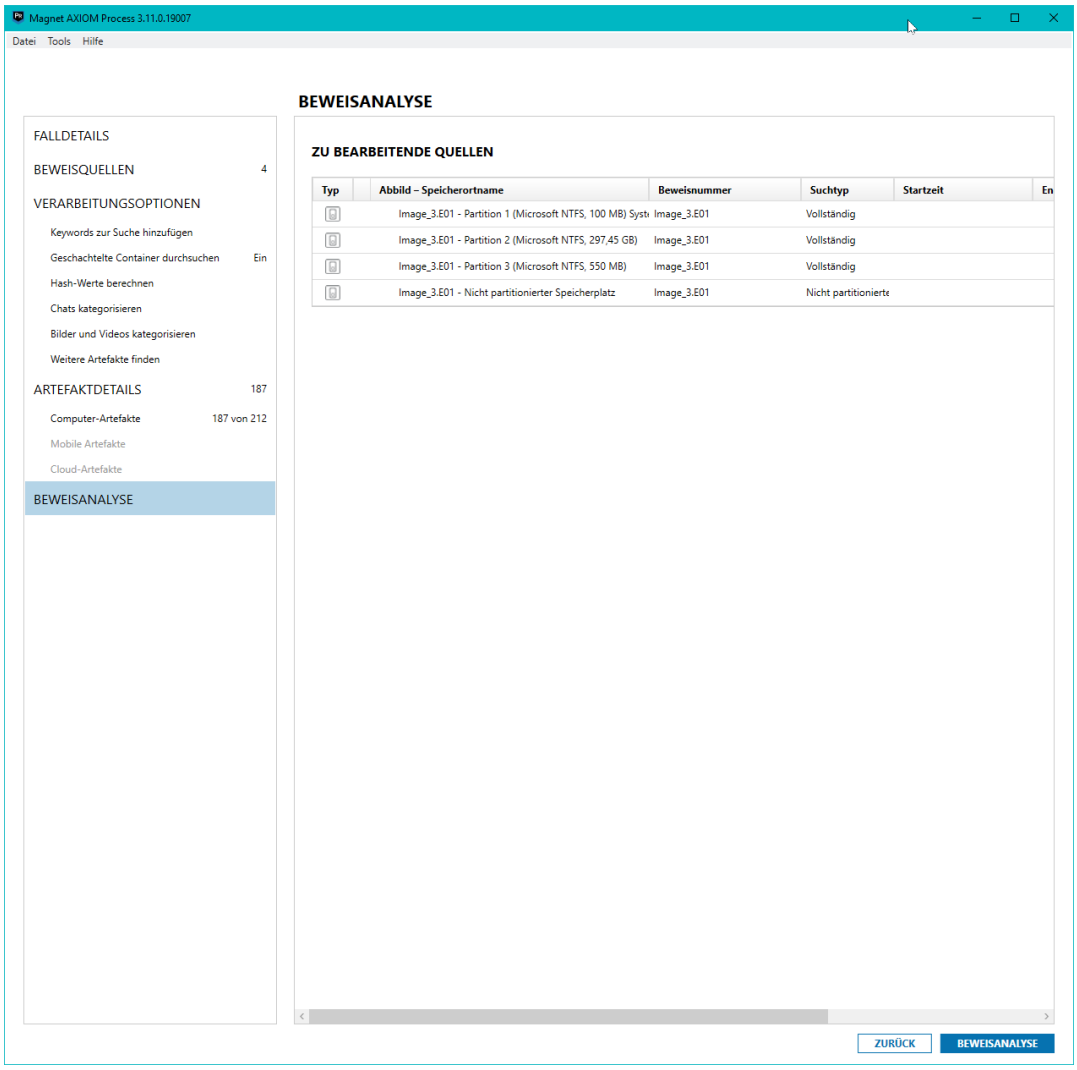


Abbildung 35: Anzeige der zu bearbeitenden Quellen

6.4 Durchführung der Aufbereitung

Nach dem Klick auf „Beweisanalyse“ ist die Analyse gestartet worden.

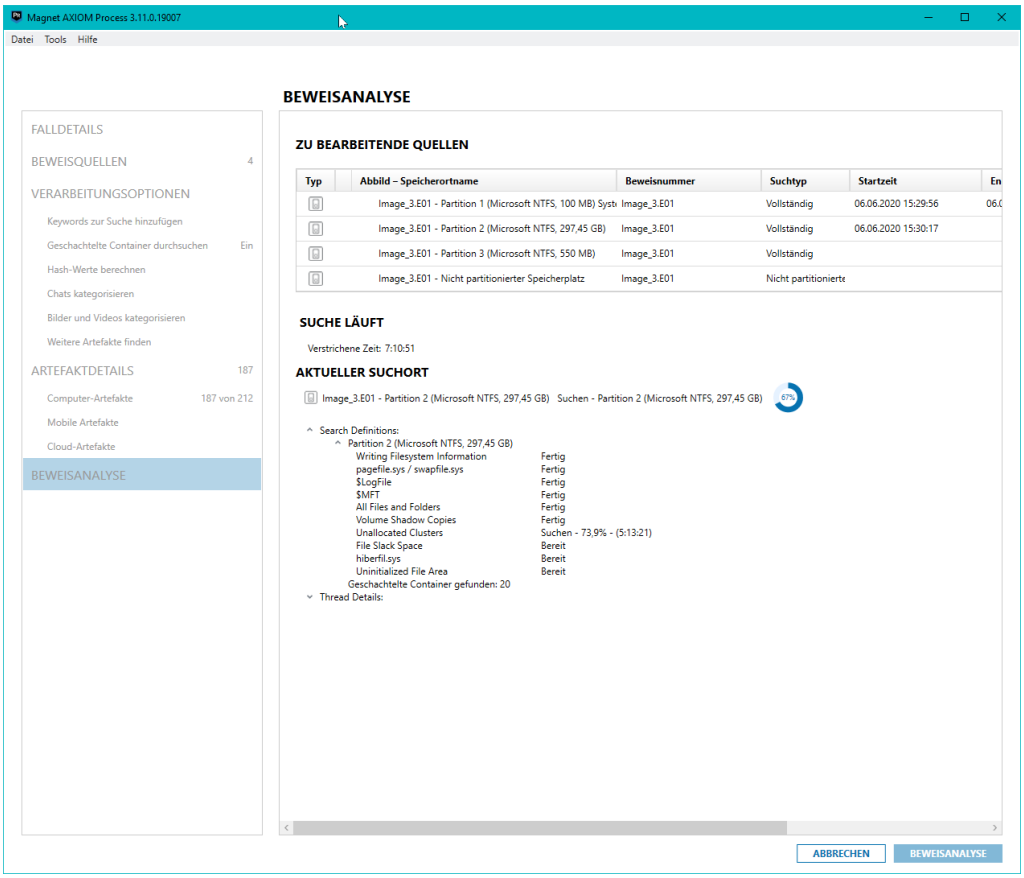


Abbildung 36: Analysevorgang

Nachdem der Vorgang nach 09:17:18 h abgeschlossen war, konnte man folgendes Ergebnis erkennen:

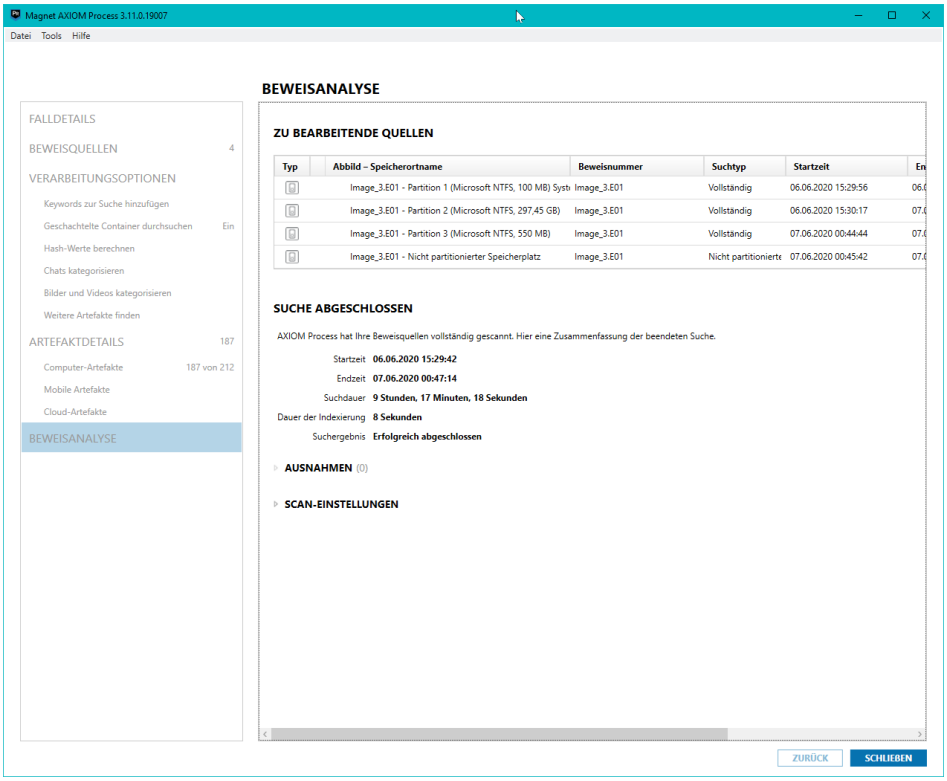


Abbildung 37: Zusammenfassung des Scans

6.5 Überprüfung der Integrität durch einen MD5-Hash

Damit die Integrität des kopierten Images sichergestellt werden kann, wurde über die Option Abbildung 38 eine erneute Hash-Wert-Berechnung in AXIOM durchgeführt.

```
Verified Images:
================
Image_3.E01
-----------
Verification Started: Jul 11, 2020 19:45:29
Verification Finished: Jul 11, 2020 20:07:44
MD5 Image Hash: 7cf58cbb20413a5a5346791d982980c8
MD5 Verification Hash: 7cf58cbb20413a5a5346791d982980c8
Outcome: MATCH
```

Abbildung 38: Ausgabe des berechneten MD5 Hash-Wertes in AXIOM

Durch den Vergleich mit Abbildung 27 zeigt sich, dass AXIOM mit dem korrekten Image gearbeitet hat und keine Änderung an dem Image vorgenommen wurde.

7 Ergebnisse der IT-forensischen Untersuchung

In diesem Abschnitt werden die Ergebnisse der IT-forensischen Untersuchung präsentiert. Dies stellt die Presentation-Phase nach dem S-A-P-Modell dar. Dabei ist die Analyse mithilfe der Software AXIOM durchgeführt worden. Hierbei liegt der Fokus auf den Ereignissen, die auf dem IT-System stattgefunden haben.

7.1 Timeline des IT-Systems

20.05.2020 @ 20:34:10 (MESZ):

Der Reporter hat die geheimen Dokumente erfolgreich an Herrn Neubert in die BRD versendet. Die E-Mail beinhaltet Text mit speziellen Hinweisen bez. der Bilder im Anhang, die mit gesendet worden sind. Ebenso ist im Anhang der Dokumentationsbericht über die schönen Gebirge des Nahen Ostens enthalten.

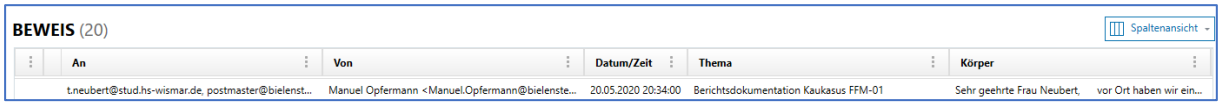


Abbildung 39: Versand der E-Mail mit Anhang an Herr Neubert

27.05.2020 @ 18:45Uhr (MESZ):

Der Reporter erhält eine E-Mail vom netten und freundlichen Einheimischen (Angreifer) mit Anhang. Der Anhang ist ein selbstentpackendes Archiv, das eine PDF-Datei mit dem Namen „Kaukasus-Bericht.pdf.rar“ enthält sowie eine ausführbare Windows Exe-Datei mit dem Namen „virus2.exe“.

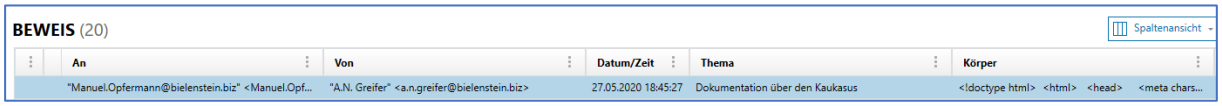


Abbildung 40: Empfang der E-Mail vom Einheimischen (Angreifer) mit Schadhaften Anhang

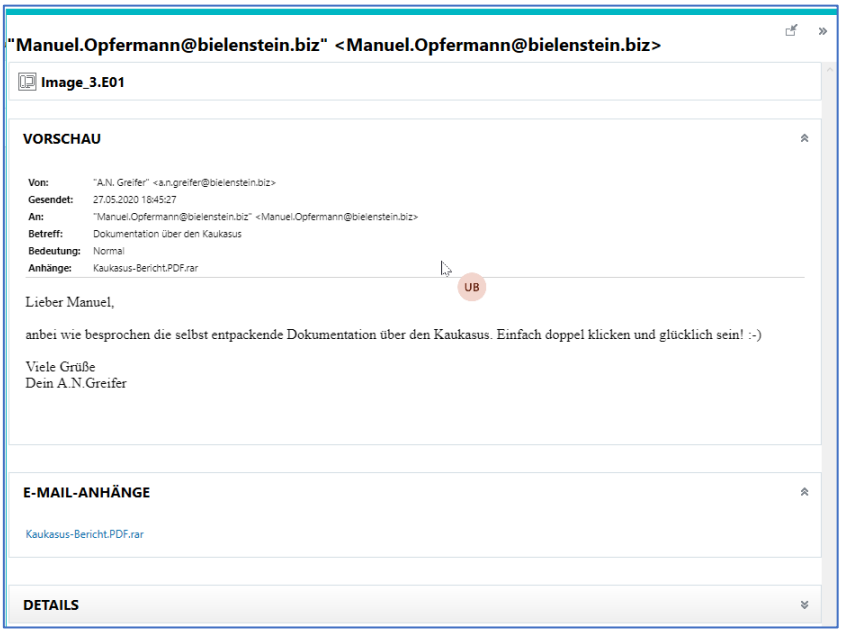


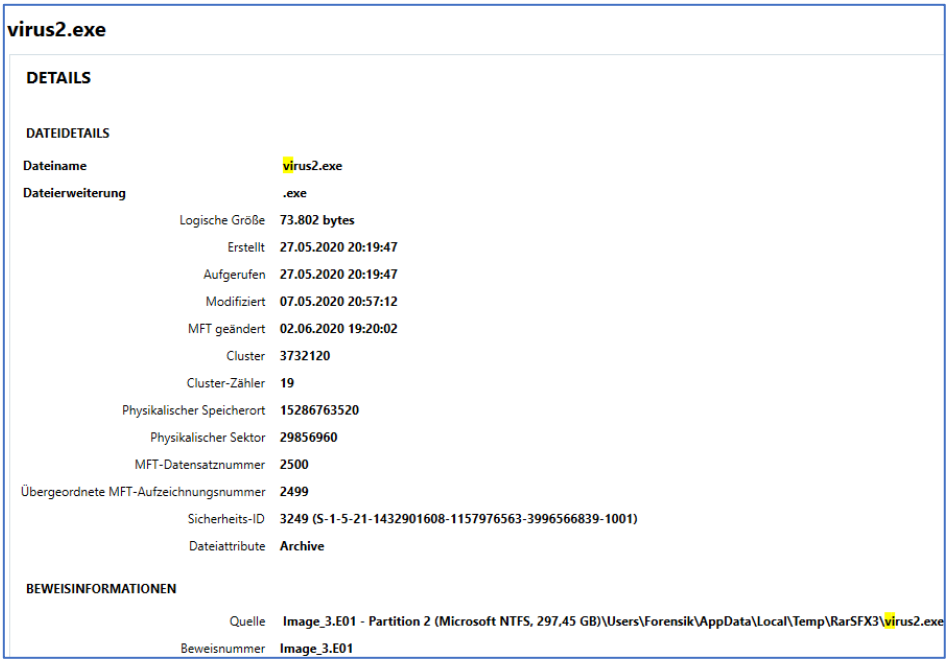
Abbildung 41: Übersicht der E-Mail vom Angreifer in AXIOM

27.05.2020 @ 20:19Uhr (MESZ):

Der Reporter hat den E-Mail-Anhang vom Angreifer heruntergeladen und das selbstentpackende Archiv ausgeführt.

Der Speicherort des „virus2.exe“ ist im Pfad „C:\Users\Forensik\AppData\Local\Temp\RarSFX3\virus2.exe“ abgespeichert worden.

„Virus2.exe“ konnte leider nicht intensiver untersucht werden, weil im Hex-Editor nichts Auffälliges zu sehen war und das technische „Know-how“ für eine tiefgründige Untersuchung mittels Reverse-Engineerings nicht gegeben war.



virus2.exe

DETAILS

DATEIDETAILS

Dateiname	**virus2.exe**
Dateierweiterung	**.exe**
Logische Größe	**73.802 bytes**
Erstellt	**27.05.2020 20:19:47**
Aufgerufen	**27.05.2020 20:19:47**
Modifiziert	**07.05.2020 20:57:12**
MFT geändert	**02.06.2020 19:20:02**
Cluster	**3732120**
Cluster-Zähler	**19**
Physikalischer Speicherort	**15286763520**
Physikalischer Sektor	**29856960**
MFT-Datensatznummer	**2500**
Übergeordnete MFT-Aufzeichnungsnummer	**2499**
Sicherheits-ID	**3249 (S-1-5-21-1432901608-1157976563-3996566839-1001)**
Dateiattribute	**Archive**

BEWEISINFORMATIONEN

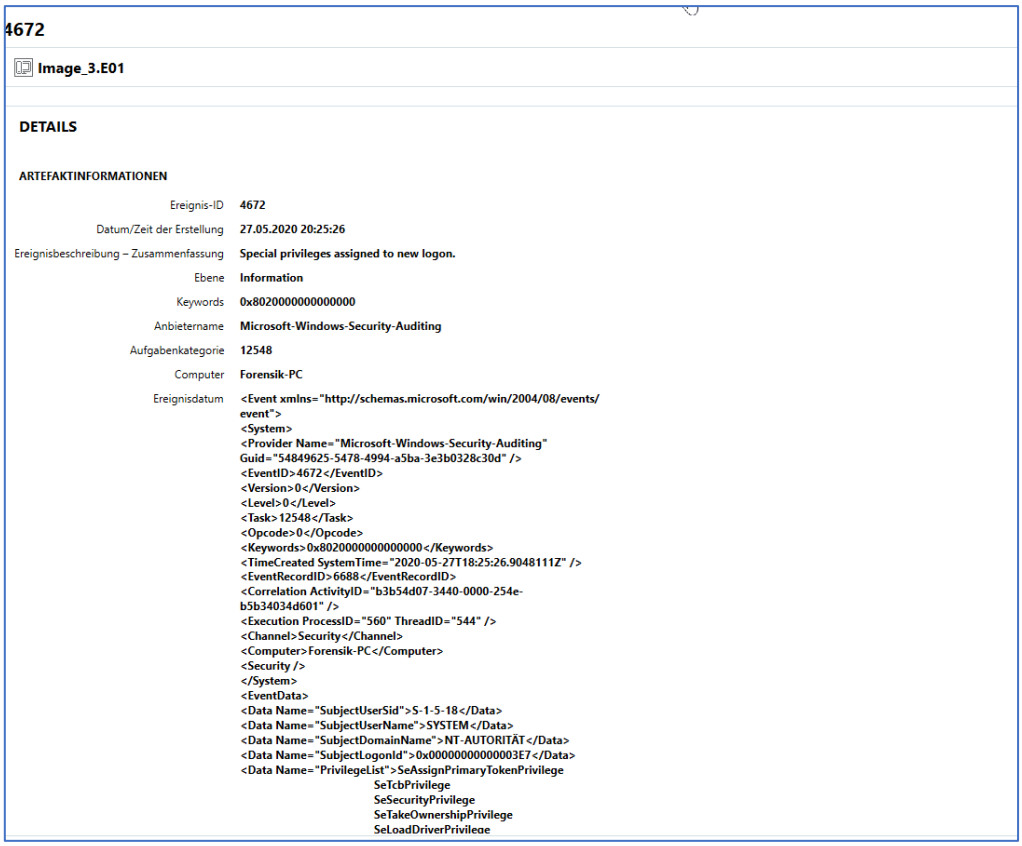
Quelle	**Image_3.E01 - Partition 2 (Microsoft NTFS, 297,45 GB)\Users\Forensik\AppData\Local\Temp\RarSFX3\virus2.exe**
Beweisnummer	**Image_3.E01**

Abbildung 42: Name und Speicherort des „virus2.exe“

<u>27.05.2020 @ 20:20Uhr – 20:24Uhr (MESZ):</u>

Zwischen dieser Uhrzeit sind verschiedene Aktivitäten wohlmöglich vom Angreifer auf dem Opfer IT-System durchgeführt worden. Die forensische Analyse hat zu diesem Zeitraum keine genauen Ergebnisse geliefert.

Hierbei wurden alle Log- und die MRU-Einträge erfolglos untersucht.



4672

Image_3.E01

DETAILS

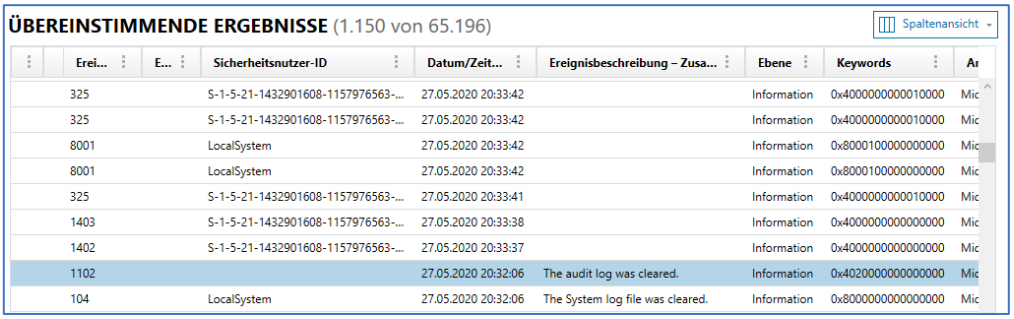
ARTEFAKTINFORMATIONEN

Ereignis-ID	**4672**
Datum/Zeit der Erstellung	**27.05.2020 20:25:26**
Ereignisbeschreibung – Zusammenfassung	**Special privileges assigned to new logon.**
Ebene	**Information**
Keywords	**0x8020000000000000**
Anbietername	**Microsoft-Windows-Security-Auditing**
Aufgabenkategorie	**12548**
Computer	**Forensik-PC**
Ereignisdatum	**<Event xmlns="http://schemas.microsoft.com/win/2004/08/events/event">** **<System>** **<Provider Name="Microsoft-Windows-Security-Auditing" Guid="54849625-5478-4994-a5ba-3e3b0328c30d" />** **<EventID>4672</EventID>** **<Version>0</Version>** **<Level>0</Level>** **<Task>12548</Task>** **<Opcode>0</Opcode>** **<Keywords>0x8020000000000000</Keywords>** **<TimeCreated SystemTime="2020-05-27T18:25:26.9048111Z" />** **<EventRecordID>6688</EventRecordID>** **<Correlation ActivityID="b3b54d07-3440-0000-254e-b5b34034d601" />** **<Execution ProcessID="560" ThreadID="544" />** **<Channel>Security</Channel>** **<Computer>Forensik-PC</Computer>** **<Security />** **</System>** **<EventData>** **<Data Name="SubjectUserSid">S-1-5-18</Data>** **<Data Name="SubjectUserName">SYSTEM</Data>** **<Data Name="SubjectDomainName">NT-AUTORITÄT</Data>** **<Data Name="SubjectLogonId">0x00000000000003E7</Data>** **<Data Name="PrivilegeList">SeAssignPrimaryTokenPrivilege** **SeTcbPrivilege** **SeSecurityPrivilege** **SeTakeOwnershipPrivilege** **SeLoadDriverPrivilege**

Abbildung 43: Zugriff auf das Opfer IT-System mit erhöhten Rechten

27.05.2020 @ 20:32Uhr (MESZ):

Der Angreifer hat auf dem Opfer IT-System die System-, Anwendungen- und Sicherheit-Log-Einträge erfolgreich gelöscht.



Erei...	E...	Sicherheitsnutzer-ID	Datum/Zeit...	Ereignisbeschreibung – Zusa...	Ebene	Keywords	Ar
325		S-1-5-21-1432901608-1157976563-...	27.05.2020 20:33:42		Information	0x4000000000010000	Mic
325		S-1-5-21-1432901608-1157976563-...	27.05.2020 20:33:42		Information	0x4000000000010000	Mic
8001		LocalSystem	27.05.2020 20:33:42		Information	0x8000100000000000	Mic
8001		LocalSystem	27.05.2020 20:33:42		Information	0x8000100000000000	Mic
325		S-1-5-21-1432901608-1157976563-...	27.05.2020 20:33:41		Information	0x4000000000010000	Mic
1403		S-1-5-21-1432901608-1157976563-...	27.05.2020 20:33:38		Information	0x4000000000000000	Mic
1402		S-1-5-21-1432901608-1157976563-...	27.05.2020 20:33:37		Information	0x4000000000000000	Mic
1102			27.05.2020 20:32:06	The audit log was cleared.	Information	0x4020000000000000	Mic
104		LocalSystem	27.05.2020 20:32:06	The System log file was cleared.	Information	0x8000000000000000	Mic

Abbildung 44: Übersicht der gefundenen Einträge in den Windows-Logs

1102

ARTEFAKTINFORMATIONEN

Ereignis-ID	**1102**
Datum/Zeit der Erstellung	**27.05.2020 20:32:06**
Ereignisbeschreibung – Zusammenfassung	**The audit log was cleared.**
Ebene	**Information**
Keywords	**0x4020000000000000**
Anbietername	**Microsoft-Windows-Eventlog**
Aufgabenkategorie	**104**
Computer	**Forensik-PC**
Ereignisdatum	**<Event xmlns="http://schemas.microsoft.com/win/2004/08/events/event"> <System> <Provider Name="Microsoft-Windows-Eventlog" Guid="{fc65ddd8-d6ef-4962-83d5-6e5cfe9ce148}" /> <EventID>1102</EventID> <Version>0</Version> <Level>4</Level> <Task>104</Task> <Opcode>0</Opcode> <Keywords>0x4020000000000000</Keywords> <TimeCreated SystemTime="2020-05-27T18:32:06.8367089Z" /> <EventRecordID>6703</EventRecordID> <Correlation /> <Execution ProcessID="312" ThreadID="1704" /> <Channel>Security</Channel> <Computer>Forensik-PC</Computer> <Security /> </System> <UserData> <LogFileCleared xmlns="http://manifests.microsoft.com/win/2004/08/windows/eventlog"> <SubjectUserSid>S-1-5-18</SubjectUserSid> <SubjectUserName>SYSTEM</SubjectUserName> <SubjectDomainName>NT-AUTORITÄT</SubjectDomainName> <SubjectLogonId>0x00000000000003E7</SubjectLogonId> </LogFileCleared> </UserData> </Event>**

Abbildung 45: Protokollierung des Löschvorganges in den Windows Anwendungen-Logs

104

Image_3.E01

DETAILS

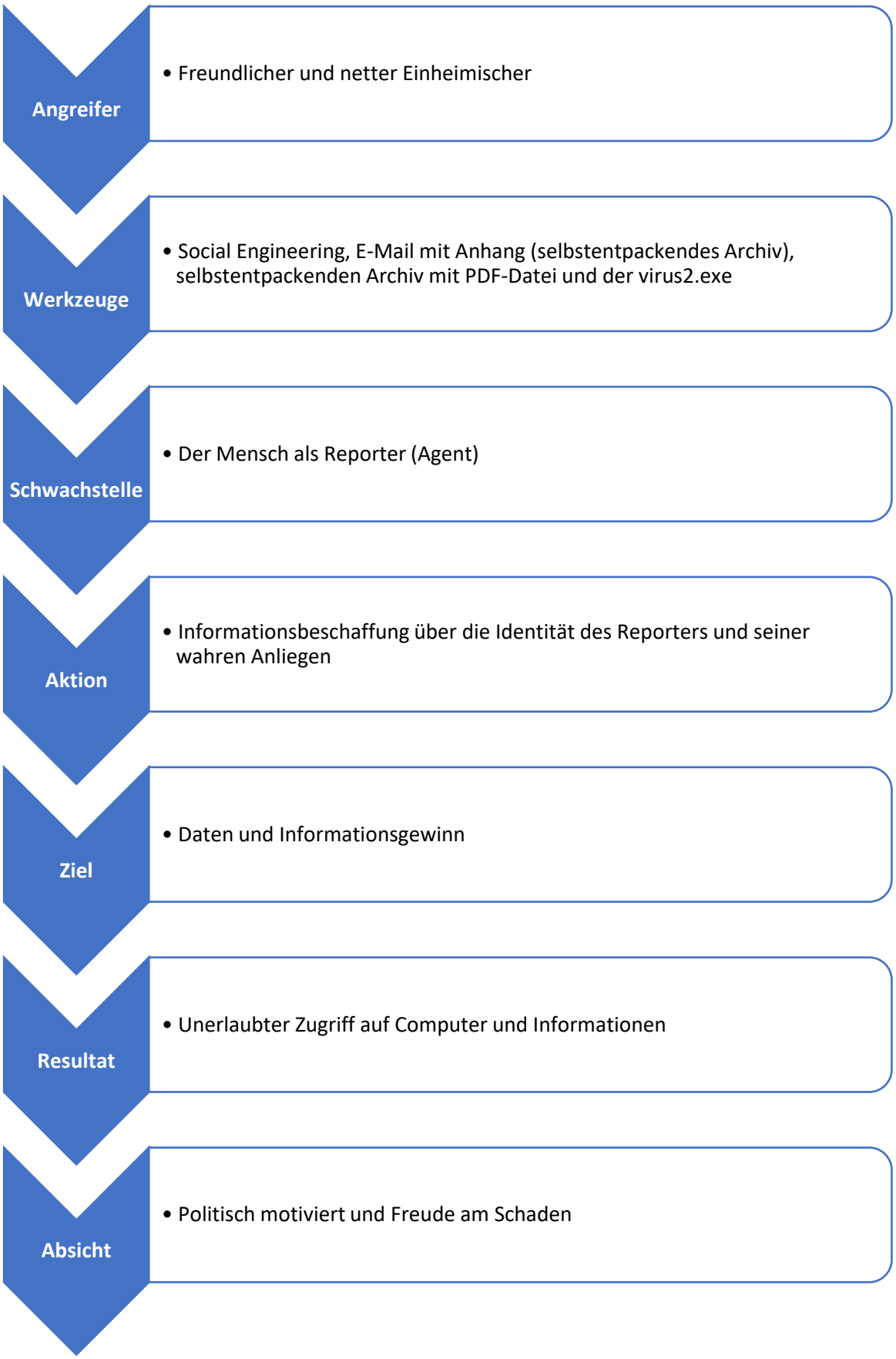
ARTEFAKTINFORMATIONEN

Ereignis-ID	**104**
Sicherheitsnutzer-ID	**LocalSystem**
Datum/Zeit der Erstellung	**27.05.2020 20:32:06**
Ereignisbeschreibung – Zusammenfassung	**The System log file was cleared.**
Ebene	**Information**
Keywords	**0x8000000000000000**
Anbietername	**Microsoft-Windows-Eventlog**
Aufgabenkategorie	**104**
Computer	**Forensik-PC**
Ereignisdatum	**<Event xmlns="http://schemas.microsoft.com/win/2004/08/events/event"> <System> <Provider Name="Microsoft-Windows-Eventlog" Guid="{fc65ddd8-d6ef-4962-83d5-6e5cfe9ce148}" /> <EventID>104</EventID> <Version>0</Version> <Level>4</Level> <Task>104</Task> <Opcode>0</Opcode> <Keywords>0x8000000000000000</Keywords> <TimeCreated SystemTime="2020-05-27T18:32:06.6147092Z" /> <EventRecordID>1308</EventRecordID> <Correlation /> <Execution ProcessID="312" ThreadID="1704" /> <Channel>System</Channel> <Computer>Forensik-PC</Computer> <Security UserID="S-1-5-18" /> </System> <UserData> <LogFileCleared xmlns="http://manifests.microsoft.com/win/2004/08/windows/eventlog"> <SubjectUserName>SYSTEM</SubjectUserName> <SubjectDomainName>NT-AUTORITÄT</SubjectDomainName> <Channel>System</Channel> <BackupPath></BackupPath> </LogFileCleared> </UserData>**

Abbildung 46: Protokollierung des Löschvorganges in den Windows Sicherheit-Logs

7.2 Bewertung des Angriffs nach der CERT-Taxonomie

Zur schematischen Darstellung des Angriffsverlaufs ist der Vorfall nach der CERT-Taxonomie klassifiziert worden.



8 Fazit und Untersuchungsergebnisse

In diesem Abschnitt des Kapitels wird die Vorgehensweise, der Einsatz der eingesetzten Werkzeuge und Tools sowie die Untersuchungsergebnisse evaluiert.

8.1 Bewertung der Ergebnisse

Die bisherigen Untersuchungsergebnisse stellen nicht das Ende der forensischen Untersuchung dar. Hierbei können weitere Aktivitäten eingeleitet werden, indem eine Anzeige gegen den netten Einheimischen (Angreifer) auf Basis seiner E-Mail-Adresse definiert wird. Darüber hinaus sollte in einer weiteren polizeilichen Untersuchung die „virus2.exe“ analysiert werden mithilfe der Methodik von Reverse-Engineering, um das Schadensausmaß besser klassifizieren zu können. Hierbei konnte bei der forensischen Untersuchung nicht identifiziert werden, welche möglichen Dateien oder Dokumente der Angreifer vom Reporter-Laptop heruntergeladen hat, da die Microsoft Windows Log-Einträge gelöscht worden sind. Des Weiteren waren keine weiteren Anzeichen, wie in den Most-Recently-Used-Einträgen in den Windows-Registry zu sehen. Darüber hinaus sollte ebenfalls untersucht werden, ob schon ähnliche Fälle mit der bekannten Absender E-Mail-Adresse existieren. Eine übergreifende polizeiliche Zusammenarbeit mit anderen Ländern wäre möglich.

8.2 Bewertung der Vorgehensweise

Das Vorgehen bei dieser forensischen Untersuchung in unserer Fallkonstellation besitzt zwei große Schwachstellen bei der Sicherung der Daten. Aus finanziellen Gründen konnte keine ordnungsgemäße und gerichtsverwertbare Beweissicherung sichergestellt werden. Hierbei ist der Einsatz eines Write-Blockers bei der Datensicherung sowie das 4-Augen-Prinzip nicht zum Einsatz gekommen. Dies hätte in einem realen Gerichtsverfahren erhebliche Einschränkungen bezüglich der Gerichtsfestigkeit, weil die Beweismittel nicht vollumfänglich dokumentiert worden sind. Darüber hinaus würde das Strafmaß gegenüber dem Beschuldigten gemindert werden aufgrund fehlerhafter Erhebung und Verarbeitung der forensischen Daten.

8.3 Bewertung der genutzten Werkzeuge und Tools

Die eingesetzten Werkzeuge und Tools haben sich bei der Falluntersuchung besonders gut bewährt. Wie im Studienbrief beschrieben, ist der Einsatz von einem universellen Schraubendreher und einer Taschenlampe bei der Sicherung von essentieller Bedeutung. Das Ansetzen des Schraubendrehers bei den kleinen Torx-Schrauben ist durch die zusätzliche Beleuchtung mit einer Tisch-/Taschenlampe erleichtert worden, um die Festplatte erfolgreich aus dem Gehäuse lösen zu können.

Der Einsatz des Tools FTK-Imager vom Hersteller AccessData hat sich für die Vorbereitung zur Image-Erstellung als gut erwiesen, um die Hashsummen für die spätere Auswertung mit dem Tool Axiom vom Hersteller Magnet Forensics Inc. bilden zu können. Des Weiteren ist die Software FTK-Imager ein bekanntes und anerkanntes Forensik Tool bei Behörden und in der freien Marktwirtschaft.

Das Tool Axiom vom Hersteller Magnet Forensics Inc. ist ebenfalls ein anerkanntes und bekanntes Forensik Tool. Die Software ist leicht zu verstehen, konfigurierbar und es existieren diverse Literaturen sowie Online-Schulungen zur erfolgreichen Abwicklung einer forensischen Untersuchung. Bei unserer Fallkonstellation hat die Software allerdings einen Nachteil aufgewiesen.

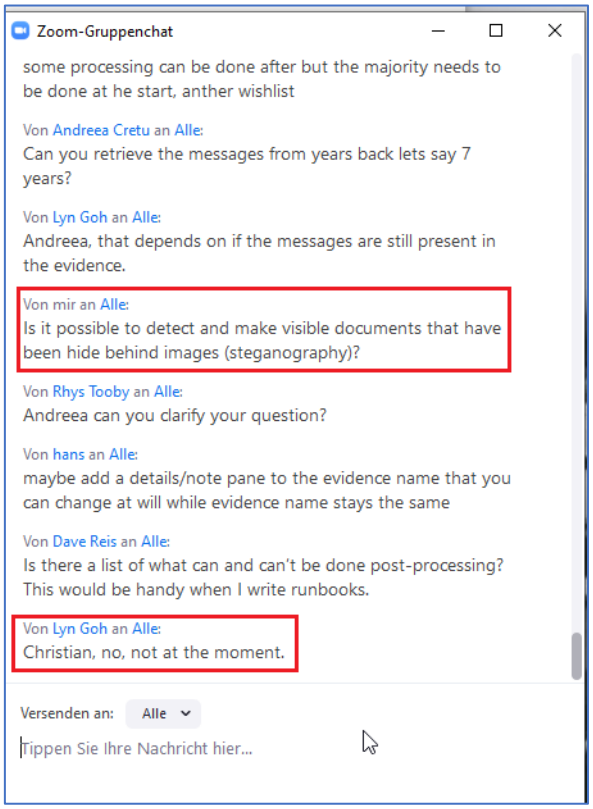


Abbildung 47: Anfrage und Antwort des Axiom-Supporters

Aktuell ist es mithilfe von Axiom nicht möglich, versteckte Bilder hinter einem anderen Bild (Steganografie) zu detektieren. Dies wurde bei einer Online-Schulung vom Axiom-Support bestätigt.