Hochschule Wismar
Fakultät für Ingenieurwissenschaften
Bereich Elektrotechnik und Informatik

Praktikumsaufgabe Sommersemester 2022

Forensik in Betriebs- und Anwendungssysteme

„Erstellen eines Images und Nutzung der Windows Forensik Software X-Ways, Axiom, FTK, Encase zur Auswertung des Images“

eingereicht von: HRS Forensics GmbH

Betreuer: Prof. Dr.-Ing. Antje Raab-Düsterhöft

Abgabedatum: 17. Juli 2022

Inhaltsverzeichnis

1 Beschreibung des Szenarios

Am 01.06.2022 meldete sich eine Zeugin namens Katja Scherer auf der Polizeidienststelle Heppenheim und berichtete, dass ein Bekannter Heinz Werner in einem Gespräch andeutete, er habe sich einer Gruppe angeschlossen, um das System zustürzen.

Aussage Zeugin

„*Vorgestern, am 30.05.2022, habe ich mich mit meinem guten Bekannten Heinz Werner zu einem Grillabend getroffen. Natürlich sind wir im Laufe des Abends auf die Corona Pandemie und die ganzen Maßnahmen zu sprechen gekommen. Ich sehe auch manches kritisch, aber Heinz hat sich immer mehr reingesteigert und auf die Politik geschimpft, die seiner Meinung nach die ganze Pandemie geplant hat, um uns Bürger zu unterdrücken. Je später der Abend wurde und je mehr Alkohol getrunken wurde, desto ausfälliger ist Heinz geworden. So kannte ich ihn bis dahin gar nicht. Ich wusste auch nicht, ob das nur eine Laune ist oder nicht.*

Irgendwann hat er mir dann auch erzählt, dass er sich mit jemandem zusammengetan hat um es "denen da oben" zu zeigen und für eine neue Regierung zu sorgen.

Ich habe auch länger darüber nachgedacht, ob ich überhaupt zur Polizei gehen soll oder nicht. Aber das was Heinz erzählt hat war teilweise für mich schon sehr konkret, weil auch der Monat Juli fiel und ich will nicht, dass er irgendwas blödes unternimmt. Und mir hat das einfach keine Ruhe gelassen."

Maßnahmen der Polizei

Die Hinweise der Zeugin waren konkret und glaubwürdig.

Die Polizei hat daraufhin Untersuchungen zu Heinz Werner angestellt und ist dabei auf eine Teilnahme an einer Demonstration der Leerdenker 4711 gestoßen, bei der die Personalien des Hr. Werner aufgenommen wurden, weil dieser gegen die Corona-Auflagen verstoßen hat.

Im Anschluss wurde Heinz Werner von der Polizei beobachtet und es wurde festgestellt, dass sich Heinz Werner mit weiteren Spitzen der Leerdenker 4711 getroffen hat.

Das führte dazu, dass die Polizei am 07.07.2022 eine Hausdurchsuchung an der Wohnanschrift des Herrn Werner - Musterstr. 75 in 01234 Musterstadt - vornahm. Dabei wurden ein Laptop und ein USB-Stick beschlagnahmt.

Herr Werner wurde festgenommen und machte von seinem Aussageverweigerungsrecht gebraucht.

Hintergrund

Heinz Werner hat sich im Laufe der Corona-Pandemie radikalisiert und sich einer Gruppierung angeschlossen, die einen Anschlag auf ein Umspannwerk plant. Die Gruppe hofft, damit einen größeren Blackout zu provozieren der zu Unruhen in der Bevölkerung und schließlich zu einem Systemsturz führt.

Die Gruppe hat Anfang 2022 mit den Planungen begonnen und sich in mehreren konspirativen Treffen mit ihrem Vorhaben beschäftigt. Heinz Werner ist in die Ausführung und die Planung eingebunden. Das heißt, er hat verschiedene Bestandteile der geplanten Bomben bestellt, das Hotel auf der Fluchtroute gebucht und auch Informationen zum Umspannwerk Lampertheim gesammelt.

Die Gefahren eines Blackouts ist immer gegeben und der Roman “Blackout” von Marc Elsberg (natürlich zugespitzt) und auch Experten wie Herbert Saurugg beschreiben ganz gut, dass die Bevölkerung nicht gut auf ein solches Ereignis vorbereitet ist und es tatsächlich zu Problemen mit der Versorgung und auch Unruhen kommen kann.

Auch in der Realität haben sich einige Kritiker der Corona-Maßnahmen und sogenannte Reichsbürger auf den “Tag X” vorbereitet.

Das Unternehmen HRS Forensics wurde beauftragt, den Rechner und den beschlagnahmten USB-Stick forensisch min. auf die nach folgende Zielstellungen zu untersuchen.

- Hinweise auf die Pläne und Vorgehensweise der Gruppe
- Hinweise zu den konkreten Anschlagszielen
- Hinweise auf Komplizen

2 Umsetzung des Szenarios und Erstellung eines Images

In diesem Kapitel wird die Umsetzung des beschriebenen Szenarios und Erstellung der individuellen Images für den USB-Stick und den Täter-Rechner beschrieben. Dabei wird beschrieben, wie die Artefakte auf den Systemen hinterlegt und manipuliert werden.

2.1 Vorbereitungen zur Softwarewahl für die forensische Auswertung

Aus den Vorüberlegungen zum Szenario wurden anhand von Dokumentationen und Handbüchern geprüft, mit welcher Forensik Software das Szenario gerichtsfest, benutzerfreundlich umsetzbar ist. Leider standen VMs der Wings nach einem Sicherheitsvorfall nicht mehr zur Verfügung, sodass nur die Forensik Software FTK Imager und Magnet Axiom für die Imageerstellung getestet wurden. Grundsätzlich kann mit beiden Anwendungen Images von einem USB-Stick und einem Rechner erstellt werden, jedoch ist Magnet Axiom für Einsteiger etwas benutzerfreundlicher.

2.2 Vorbereitung der Infrastruktur

Für die Umsetzung des Szenarios werden nicht nur die Systeme (USB-Stick und Täte-Rechner) vorbereitet, sondern ebenfalls eine entsprechende Infrastruktur. Der Täter-Rechner wird durch die Virtualisierungssoftware „VM VirtualBox“ von Oracle implementiert.

Um den Täter-Rechner beliebig nutzen zu können, wurde er als VirtualBox Virtuelle Maschine installiert. In einem realen Fall würde man aber eine Festplatte vorliegen haben, von der ein Image erstellt wird. Um das nachstellen zu können, muss die (virtuelle) Festplatte der Virtuellen Maschine als Laufwerk im Hostsystem eingebunden werden.

Die virtuellen Festplatten liegen als Datei vom Dateityp `vdi` vor. Zum Einbinden als Festplatte nutzen wir das Tool ImDisk [4]. Nach dem Download und der Installation von ImDisk kann die virtuelle Festplatte eingebunden werden.

Über das Startmenü des Arbeitsrechners kann das Tool gestartet werden:

Bild 2: VDI Tool starten

Im anschließend geöffneten Fenster kann die vdi-Datei ausgewählt und einem Laufwerksbuchstaben zugeordnet werden. Um Probleme mit der Virtuellen Maschine zu vermeiden, binden wir das Laufwerk "schreibgeschützt" ein.

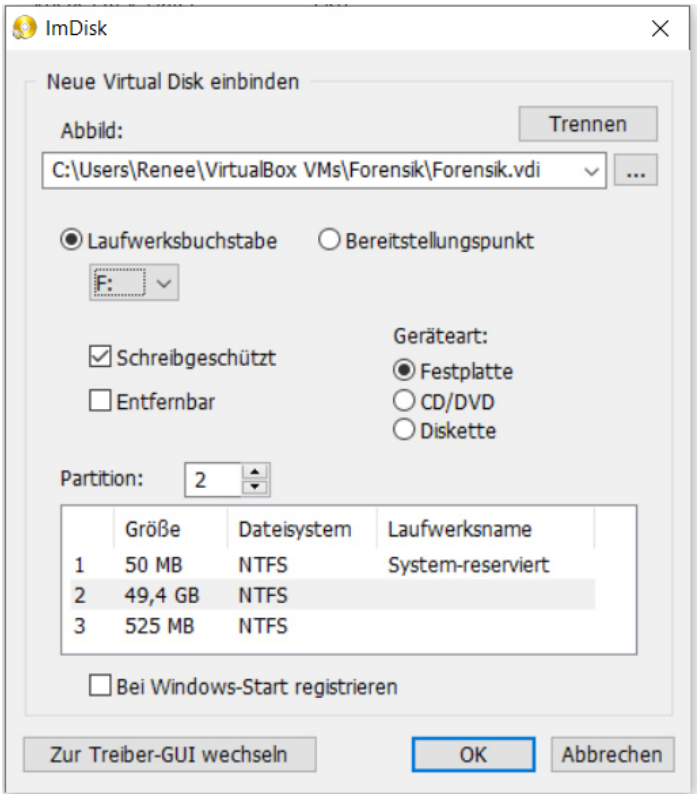


Bild 1: VDI Datei einbinden

Nachdem ImDisk die virtuelle Festplatte eingebunden hat, steht diese als neues Laufwerk zur Verfügung und anschließend kann in Axiom ein Abbild dieses Laufwerks erstellt werden.

2.3 Vorbereitung des Täter-Rechner

Als Täter-Rechner wird eine virtuelle Maschine mit dem Betriebssystem Windows genutzt. Mit Hilfe des Wings Zugangs zu Microsoft Azure Education war es möglich ein Windows 10 Education Image mit gültigen Lizenzschlüssel für den Täter-Rechner zu verwenden. Dies wurde wie bereits erwähnt in Dies Auf diesem Rechner sind die standardmäßig installierte Software sowie folgende Anwendungen zu finden:

- Google Chrome (Version 103.0.5060.114)
- Messenger von Meta (Version 153.0.0.18.110)
- Adobe Acrobat Reader DC (Version 22.256)

Auf dem Täter-Rechner sollen dem Szenario entsprechende Spuren zu finden sein:

- Browser-Historie
- Chat-Nachrichten
- Events für das Verbinden mit dem USB-Stick (Asservat 2)

Im Kapitel 2.3.1 wird beschrieben, wie die Browser-Historie und in Kapitel 2.3.2 wie die Chat-Nachrichten vorbereitet werden.

Wenn alle Vorbereitungen abgeschlossen sind, wurden die manipulierte Browser-Historie und Chat-Nachrichten über einen gemeinsamen Ordner in die VM kopiert.

Ebenfalls soll in dem Event Log des Täter-Rechner ein Logeintrag existieren, wenn der USB-Stick, der von der Polizei beschlagnahmt wurde, an den Täter-Rechner angeschlossen wurde. Dabei ist zu beachten, dass man im Vorfeld die Uhrzeit des Rechners manuell anpassen muss.

2.3.1 Vorbereiten der Chrome Historie

Das Szenario sieht vor, dass die Terrorgruppe einen Anschlag plant. In der Vorbereitung des Vorhabens haben die Beteiligten über das Internet nach möglichen Anschlagszielen gesucht und sich Informationen über den Bombenbau, die Fluchtroute und Unterkünfte verschafft.

An diese Informationen gelangen sie mit Hilfe von Suchen mit der Suchmaschine Google, Google Maps und den Besuch der gefundenen Seiten. Dazu wird der Browser Chrome genutzt.

Um die Forensik nicht zu einfach zu machen, werden noch weitere Suchanfragen und Besuche weiterer Webseiten eingestreut.

Alle Vorgänge händisch zu machen ist zu aufwändig. Außerdem erlaubt der Browser es nicht Webseiten mit HTTPS zu besuchen, wenn die Zeit des Rechners manuell in die Vergangenheit gesetzt wird und das SSL-Zertifikat zu dem Zeitpunkt nicht gültig war (siehe Bild 3).

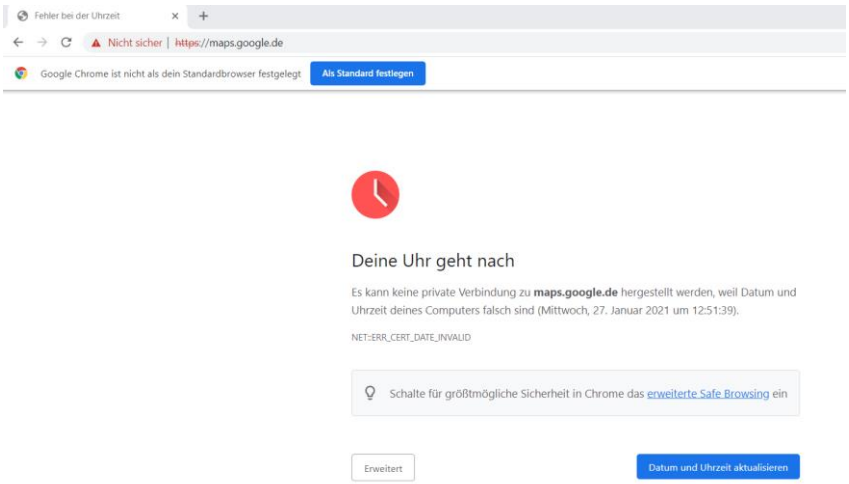


Bild 3: Manipulierte Uhrzeit Browser Verlauf

Aus diesem Grund soll die Historie des Browsers selbst manipuliert und auf dem zu untersuchenden System wieder eingespielt werden. Die Historie des Browsers Chrome wird in einer SQLite-Datenbank namens `HISTORY` gespeichert. Man findet sie in dem Verzeichnis *`C:\Users\[Username]\AppData\Local\Google\Chrome`* . Die Datenbank enthält folgende Tabellen, die für das Szenario interessant sind:

Tabellenname	Zweck
`downloads / downloads_url_chains`	Heruntergeladene Dateien
`keyword_search_terms`	Suchbegriffe
`urls`	Aufgerufene URLs
`visits`	Tatsächliche Webseitenbesuche inkl. Zeitstempel und Besuchszeit

Tabelle 1: relevante SQLite Datenbank Tabellen

Generell ist noch wichtig zu sagen, dass Chrome unter Windows die Zeitstempel in der Datenbank als Nanosekunden seit 01.01.1601 speichert.

2.3.1.1 Downloads

Die Informationen zu den Downloads sind in den Tabellen `downloads` und `downloads_url_chains` gespeichert.

In `downloads` sind die Zeitstempel, Größe und Pfad der heruntergeladenen Datei zu finden. In `downloads_url_chains` ist zu finden, von welcher URL die Datei heruntergeladen wird und unter welcher URL die Datei schlussendlich zu finden war.

In dem Szenario sollen Dateien auf einem USB-Stick gefunden werden, die über einen Browser aus dem Internet heruntergeladen wurden. Diese Downloads müssen auch in der Browserhistorie/Downloadhistorie wieder zu finden sein.

2.3.1.2 Suchbegriffe

Sobald ein Nutzer in Chrome im Internet nach einem Begriff sucht, wird dieser Begriff in der Tabelle `keyword_search_terms` gespeichert. Das bedeutet, dass für das Szenario Begriffe wie "Bombe", "Trafo" und "Umspannwerk" darin zu finden sein sollen.

In der Tabelle wird auf die `urls`-Tabelle verwiesen, in der die komplette URL mit dem Suchbegriff zu finden ist.

2.3.1.3 Webseitenbesuche

Die besuchten URLs werden in der `urls`-Tabelle gespeichert. Hier werden außerdem der Titel der Seite, die Anzahl der Besuche und der Zeitpunkt des letzten Besuchs gespeichert.

Die Besuche an sich werden in der Tabelle `visits` gespeichert. Neben der Referenz auf die URL sind diese Informationen in der Tabelle zu finden:

- Zeitpunkt des Besuchs
- Dauer des Besuchs

Interessant ist auch noch die Spalte `transition`, da diese anzeigt, ob die URL z.B. direkt in der Adressleiste des Browsers eingegeben wurde oder ein Link angeklickt

wurde. Der Wert in der Spalte ist aber wenig aussagekräftig, da es nur Integer-Werte sind. Die möglichen Werte sind unter `https://chromium.googlesource.com/chromium/chromium/+/142dbc0336a678cde9069b7da4e4808e0c4b2da1/chrome/common/page_transition_types.h` einzusehen.

Die anderen Tabellen sind für unsere forensische Auswertung uninteressant und bleiben leer.

2.3.1.4 Programm zur Erstellung einer Chrome Historie

Um die Chrome-Historie für das Szenario zu erstellen, wurde ein Perl-Programm geschrieben, das in Github [5] zu finden ist.

Neben den für das Szenario wichtigen Webseiten sollen noch weitere Webseiten besucht werden. Die URLs dafür kommen von der Webseite [6] und werden in einer extra Datei abgelegt.

Dort kann eine Liste mit URLs hinterlegt werden, die auf jeden Fall gefunden werden sollen. Man kann dabei auch einen Zeitpunkt angeben, zu dem die URL in der Historie auftauchen soll. Die Daten können als JSON-Datenstruktur definiert werden:

```
{
    "URLs" : [
        {
             "URL" : "https://beispiel.domain",
             "Date": "2022-01-15 ..."
         },
         {
             "URL" : "https://beispiel.domain",
             "Date": "2022-01-15 ...",
             "Download": "file.txt",
             "Bytes": 13841
        },
    ]
}
```

Tabelle 2: Beispiel URL zur Erstellung einer Chrome Historie

2.3.2 Vorbereitung der Chat-Nachrichten

Mittlerweile wird viel Kommunikation über Chats bzw. Messenger-Dienste betrieben. Aus diesem Grund wurde bei dem Szenario davon ausgegangen, dass auch die Gruppierung um Hr. Werner sich über Chats austauscht. Laut dem Axiom-Blog [2] kann die Software mit der Desktopanwendung zum Facebook Messenger umgehen. Um einen Chatverlauf

passend zum Szenario zu bekommen, wurden zwei Accounts bei Facebook angelegt. Dazu muss ein neues Konto erstellt werden (siehe Bild 4) und die Registrierung vervollständigt werden (siehe Bild 5.

Dazu musste natürlich auch eine gültige E-Mailadresse anlegt und verifiziert werden.

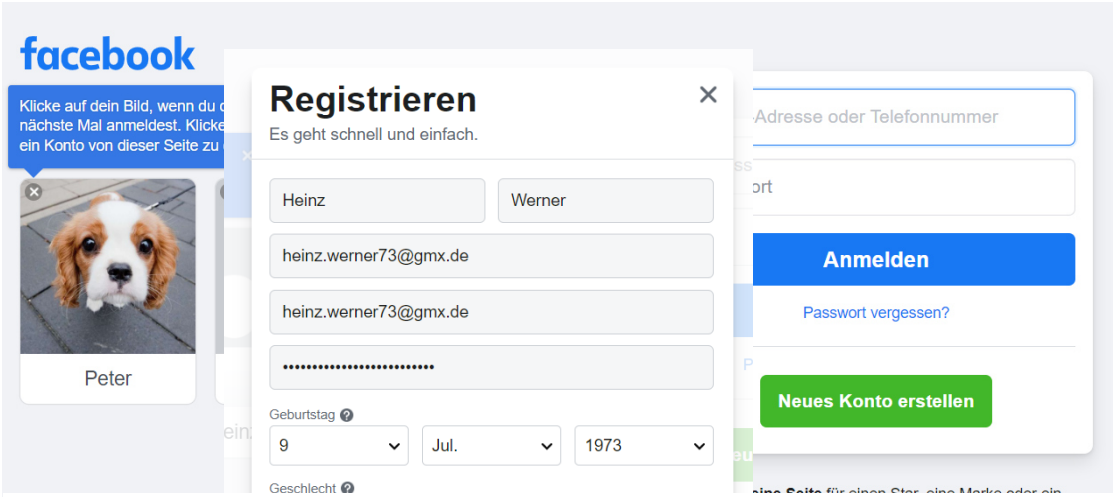


Bild 4: Erstellung der Facebook Accounts

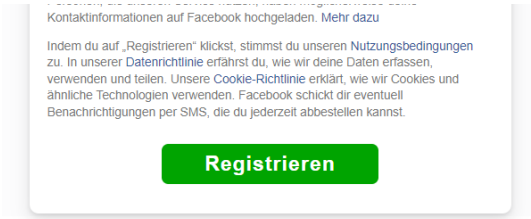


Bild 5: Registrierung Facebook

Sind beide Accounts (Peter Herbert und Heinz Werner) angelegt, kann die „Freundschaft“ hergestellt werden, indem eine Freundschaftsanfrage gesendet (siehe Bild 6) und jeweils bestätigt wird (siehe Bild 7).

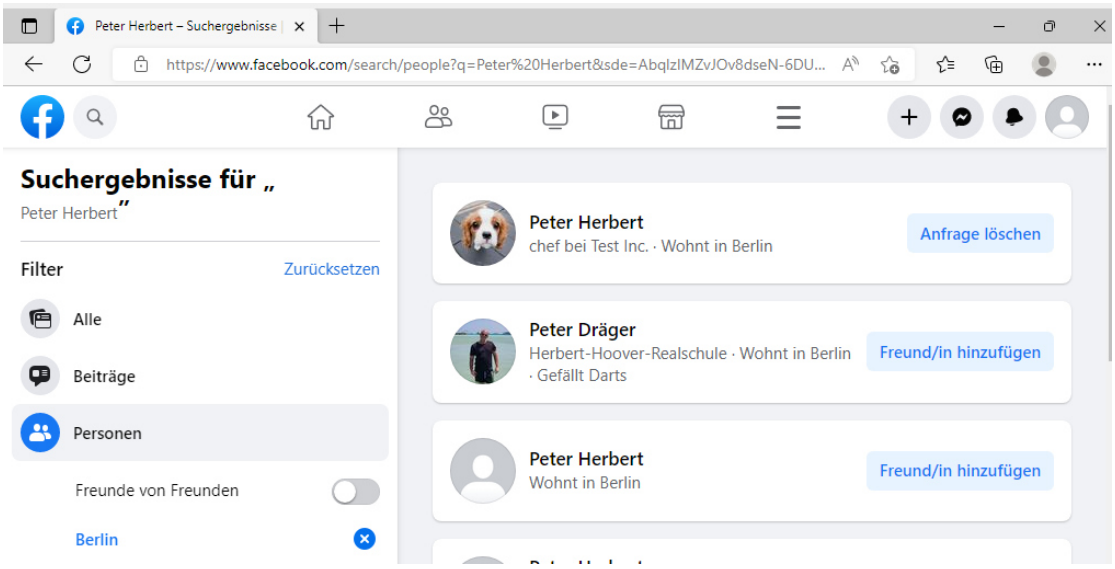


Bild 6: Freundschaftsanfragen senden

In der heutigen Zeit kann ein Facebook-Nutzer nicht nur über die Webanwendung mit anderen Leuten kommunizieren, sondern Facebook hat zum Chatten eine Desktopanwendung namens „Messenger“ entwickelt, die auf der Webseite [3] herunterzuladen ist.

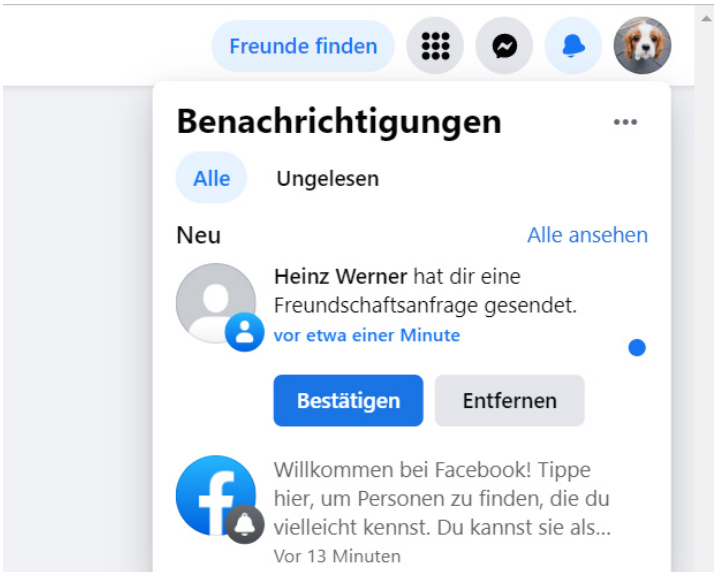


Bild 7: Freundschaftsanfrage bestätigen

Im Rahmen dieser Hausarbeit wurde die Desktop-App auf dem Täter-Rechner installiert und der Facebook-Nutzer Peter Herbert angemeldet. Auf dem nachfolgenden Bild ist die Kommunikation zwischen Heinz Werner und Peter Herbert zu erkennen, die dem Szenario entspricht.

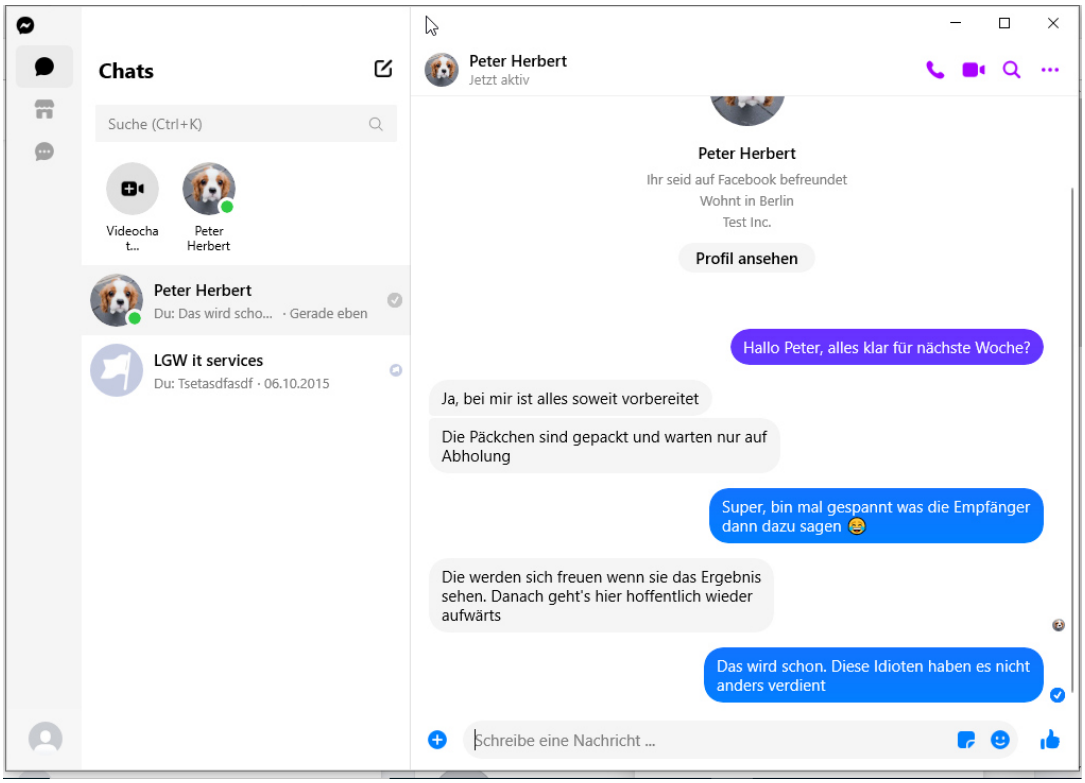


Bild 9: Messenger Desktop App Kommunikation

Der andere Facebook-Nutzer Heinz Werner kann ebenfalls über die Desktopanwendung von seinem Rechner schreiben oder aber die Web-GUI von Facebook nutzen (siehe Bild 8).

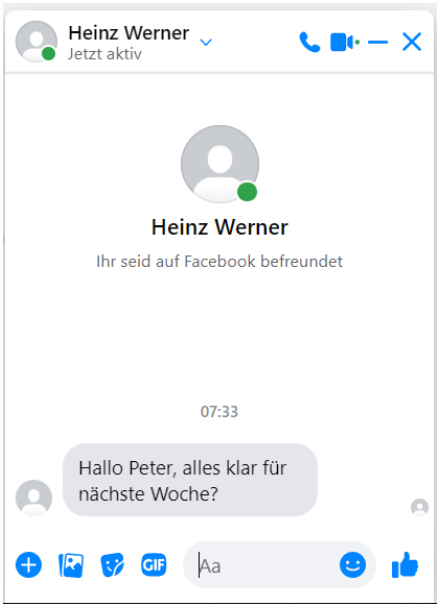
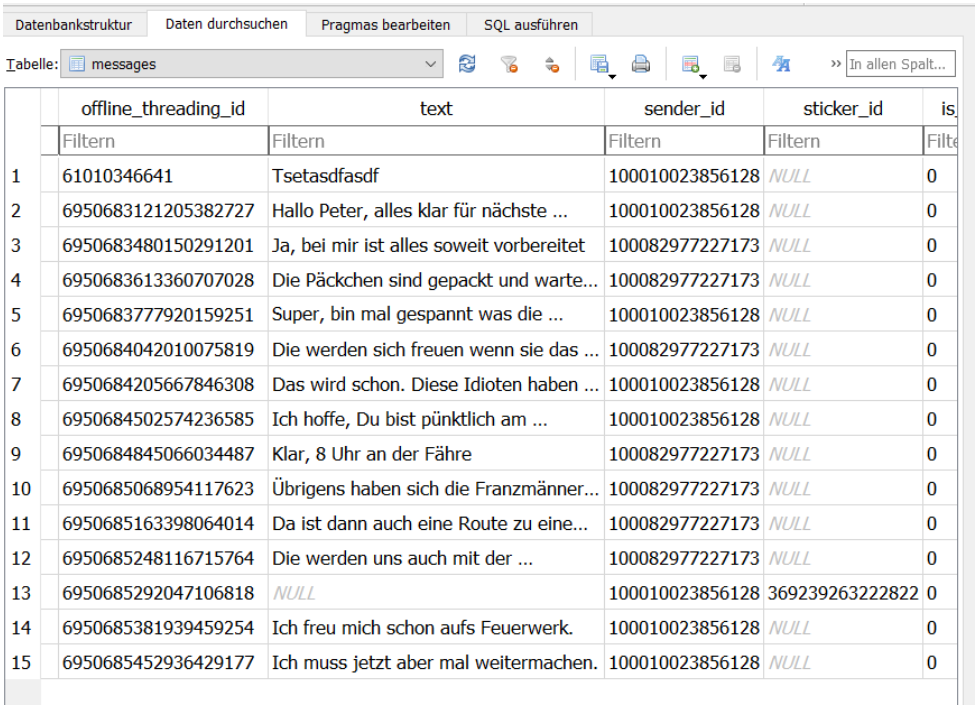


Bild 8: Web-GUI Facebook Messenger

In den ersten Tests mit Axiom wurden die Messenger-Chats nicht gefunden. Eine Ursache könnte gewesen sein, dass die virtuelle Festplatte der Virtuellen Maschine direkt mit Axiom ausgewertet wurde. Deshalb wurde die virtuelle Festplatte im Hostsystem eingebunden (siehe Kapitel 2.2), davon ein Image erstellt und dieses dann ausgewertet. Dabei wurden die Messenger-Nachrichten gefunden wie das nachfolgende Bild zeigt.

Bild 10: Test der Messenger Nachrichten

Bei der Ursachensuche wurden aber die SQLite-Datenbanken des Messengers manuell gefunden (diese sind unter *<USERHOME>/AppData/Local/Messenger/msys_*.db* gespeichert). Es wurde aus Zeitgründen hier kein Versuch unternommen Chatnachrichten von anderen Zeitpunkten direkt in der Datenbank zu erstellen. Das nachfolgende Bild zeigt ein Ausschnitt aus der messages-Tabelle mit dem SQLite-Browser.



	offline_threading_id	text	sender_id	sticker_id	is
	Filtern	Filtern	Filtern	Filtern	Filte
1	61010346641	Tsetasdfasdf	100010023856128	NULL	0
2	6950683121205382727	Hallo Peter, alles klar für nächste ...	100010023856128	NULL	0
3	6950683480150291201	Ja, bei mir ist alles soweit vorbereitet	100082977227173	NULL	0
4	6950683613360707028	Die Päckchen sind gepackt und warte...	100082977227173	NULL	0
5	6950683779201592 51	Super, bin mal gespannt was die ...	100010023856128	NULL	0
6	6950684042010075819	Die werden sich freuen wenn sie das ...	100082977227173	NULL	0
7	6950684205667846308	Das wird schon. Diese Idioten haben ...	100010023856128	NULL	0
8	6950684502574236585	Ich hoffe, Du bist pünktlich am ...	100010023856128	NULL	0
9	6950684845066034487	Klar, 8 Uhr an der Fähre	100082977227173	NULL	0
10	6950685068954117623	Übrigens haben sich die Franzmänner...	100082977227173	NULL	0
11	6950685163398064014	Da ist dann auch eine Route zu eine...	100082977227173	NULL	0
12	6950685248116715764	Die werden uns auch mit der ...	100082977227173	NULL	0
13	6950685292047106818	NULL	100010023856128	369239263222822	0
14	6950685381939459254	Ich freu mich schon aufs Feuerwerk.	100010023856128	NULL	0
15	6950685452936429177	Ich muss jetzt aber mal weitermachen.	100010023856128	NULL	0

Bild 11: Chat-Nachrichten SQLite-Browser

Wenn ein Emoticon verschickt wird, erscheint dieses nur als Sticker (siehe Zeile 13 im Bild 11). Da Billigung und Zustimmung ggf. durch solche Emoticons ausgedrückt werden, könnte das unter Umständen strafrechtlich relevant werden. In solchen Fällen müsste die `sticker_ids` ebenfalls untersucht werden.

2.4 Vorbereitung des USB-Images

Für das der Hausarbeit zu Grunde liegende Szenario sieht vor, dass die Polizeibehörden bei dem Verdächtigen einen USB-Stick beschlagnahmen, der forensisch untersucht werden soll. Für die Hausarbeit gehen wir davon aus, dass darauf einige für das Szenario relevante Artefakte zu finden sind.

2.4.1 Überlegungen zu den Artefakten

In dem Szenario wird davon ausgegangen, dass die Gruppierung einen Anschlag auf ein Umspannwerk plant und von dort aus flüchtet.

Die erste Überlegung ist also, wie eine solche Gruppe Informationen zu dem Ziel findet. Das einfachste ist erstmal über Google Maps. Dort gibt es Satellitenbilder, man kann sich die Zu- und Abfahrtwege anschauen und bekommt einen Überblick über die Umgebung.

Der nächste Schritt wäre, vor Ort ein paar Fotos zu machen. Die Fotos haben in der Regel Geodaten in den EXIF-Daten. Das erlaubt es, eine Beziehung zwischen der Google-Maps-Suche und Fotos herzustellen.

Vor einem Anschlag müssen Materialien besorgt und gelagert werden. Aus diesem Grund wird eine Lagerhalle benötigt und von der Lieferung gibt es einen Lieferschein.

Die Planungen werden kurz in einem Dokument zusammengefasst, damit die Gruppe intern weiß, wann was passieren soll.

Für die Flucht wird eine Unterkunft benötigt. Wenn eine Unterkunft gebucht wird, gibt es in der Regel eine Buchungsbestätigung.

Was die Zeiten für die Artefakte angeht, war die Überlegung, dass die Gruppe zuerst ein Ziel bestimmt, dann auf die Suche nach den Materialien geht und anschließend die Flucht plant.

2.4.2 Erstellen der Artefakte

Beim Erstellen der Artefakte kommt es darauf an, dass diese zu dem geplanten Szenario passen. Die Vorüberlegungen haben ergeben, welche Artefakte benötigt werden:

- Screenshots von Google Maps

Fotos, die am Umspannwerk gemacht sein könnten

- Lieferschein für die Materialien
- Buchungsbestätigung des Hotels
- Datei mit dem groben Zeitplan

Beim Erstellen der Artefakte kommt es auch darauf an, dass die verschiedenen Zeiten mit dem Szenario bzw. den Vorüberlegungen zu den Artefakten zusammenpassen. Bei Dateien gibt es mehrere Zeiten, die beachtet werden müssen:

- Zeitpunkt der Dateierstellung
- Zeitpunkt der letzten Änderung
- ggf. Zeitpunkt des letzten Zugriffs

Der Zeitpunkt der Dateierstellung darf nicht nach dem Zeitpunkt der letzten Änderung liegen.

Eine weitere Überlegung war, dass die Artefakte "versteckt" werden sollten. Das ist zwar kein richtiger Schutz, da es nur eine "Anzeigeeigenschaft" ist, aber das war auch im Hinblick auf die Übung mit der Forensik-Software eine gute Option.

2.4.3 Umstellen der Zeiten

Für die Erstellung der Artefakte wurde ein Windows-System genutzt. Im ersten Schritt wurde beim Kopieren der Dateien auf den USB-Stick die Systemzeit wie folgt umgesetzt:

Zuerst nach den Einstellungen suchen

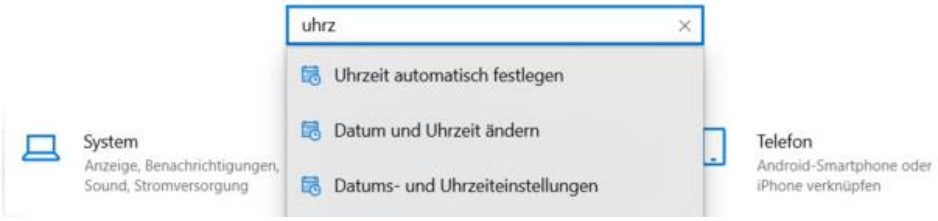


Bild 12: Windows Einstellungen Uhrzeit suchen

Danach das automatische Festlegen der Uhrzeit deaktivieren und die Uhrzeit manuell festlegen

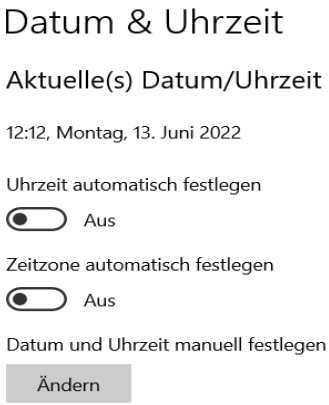


Bild 13: Deaktivierung der automatischen Uhrzeit

Anschließend kann die gewünschte Uhrzeit einstellen.

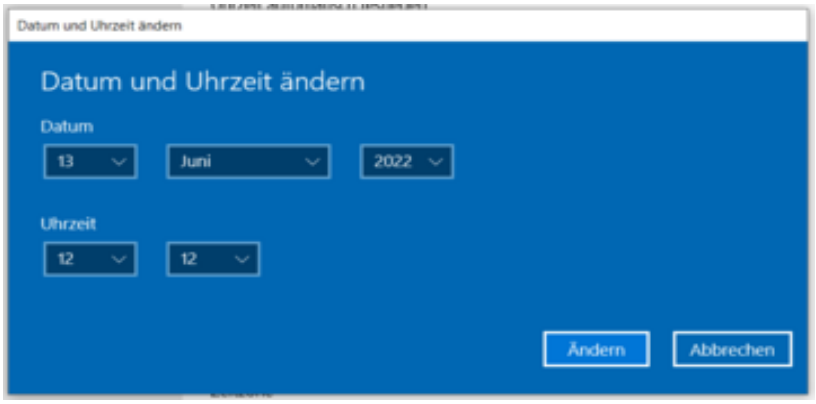


Bild 14: Änderung der Windows Uhrzeit

Das war aber noch nicht ausreichend (siehe "Test des USB-Sticks"), so dass noch die Erstellzeit geändert werden musste. Es gibt verschiedene Tools, die das können, oder bei wenigen Dateien kann auch PowerShell genutzt werden:

```
PS E:\dayx> Get-ChildItem -Force .\Lieferschein.pdf | foreach { $_.CreationTime = Get-Date -Year 2022 -Month 3 -Day 4 -Hour 8 -Minute 33 }
PS E:\dayx> Get-ChildItem -Force .\Hotel.pdf | foreach { $_.CreationTime = Get-Date -Year 2022 -Month 4 -Day 20 -Hour 14 -Minute 25 }
PS E:\dayx> Get-ChildItem -Force .\ablauf.txt | foreach { $_.CreationTime = Get-Date -Year 2022 -Month 1 -Day 15 -Hour 23 -Minute 25 }
PS E:\dayx> Get-ChildItem -Force .\mitarbeiter\th-3438313806 | foreach { $_.CreationTime = Get-Date -Year 2022 -Month 5 -Day 25 -Hour 18 -Minute 59 }
PS E:\dayx> Get-ChildItem -Force .\paeckchen\71-119384666--null--12-07-2017-19-03-27-261-.jpg | foreach { $_.CreationTime = Get-Date -Year 2022 -Month 1 -
PS E:\dayx> Get-ChildItem -Force .\paeckchen\12665138_shift-644x0_1wmQwp_tLlC7Z.jpg| foreach { $_.CreationTime = Get-Date -Year 2022 -Month 1 -Day 21 -Hou
PS E:\dayx> Get-ChildItem -Force .\paeckchen\28861375-ein-countdown-zaehler-der-wie-eine-bombenattrappe-aussieht-4ea.jpg | foreach { $_.CreationTime = Get
PS E:\dayx> Get-ChildItem -Force .\paeckchen\A1Cw96Gc07L._AC_SL1500_.jpg | foreach { $_.CreationTime = Get-Date -Year 2022 -Month 1 -Day 20 -Hour 16 -Minu
PS E:\dayx> Get-ChildItem -Force .\paeckchen\e6ba0152b9f085e54ca35b1e4298ddd5--post-apocalyptique-airsoft.jpg | foreach { $_.CreationTime = Get-Date -Year
PS E:\dayx> Get-ChildItem -Force .\paeckchen\Pipe_bomb_02.jpg | foreach { $_.CreationTime = Get-Date -Year 2022 -Month 1 -Day 20 -Hour 15 -Minute 34 }
PS E:\dayx> Get-ChildItem -Force .\paeckchen\Schema-Timer.gif | foreach { $_.CreationTime = Get-Date -Year 2022 -Month 1 -Day 20 -Hour 15 -Minute 34 }
PS E:\dayx> Get-ChildItem -Force .\umspannwerk\3DSchnittTrafo20kV.jpg | foreach { $_.CreationTime = Get-Date -Year 2022 -Month 5 -Day 20 -Hour 18 -Minute
```

Bild 15: Änderung der Erstellzeit mittels Powershell

Das `-Force` war hier notwendig, da die Dateien "versteckt" waren und das Kommando `Get-ChildItem` diese Dateien sonst nicht gefunden hätte.

2.4.4 Ändern der Geoinformationen in den Fotos

Ein Teil der Artefakte sollten Fotos vom potenziellen Anschlagsziel sein. Viele Digitalkameras (auch die in den Smartphones) speichern dabei sogenannte Geoinformationen in den Metadaten (hier: EXIF-Daten). Dabei werden die Koordinaten und ihre Ausrichtung (Nord/Süd, West/Ost) einer Bildaufnahme gespeichert.

In den heruntergeladenen Fotos waren keine Geoinformationen gespeichert, weshalb diese manuell eingefügt werden mussten. Mit der freien Bildbearbeitungssoftware GIMP konnte man nach dem Öffnen des Bildes kann unter dem Reiter `Bild` und dem Menüpunkt `Metadaten` die Option `Metadaten bearbeiten` auswählen, was ein Dialog zum Bearbeiten der Geoinformationen erlaubte.

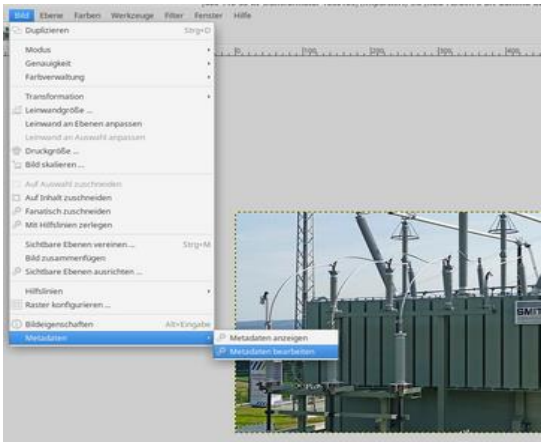


Bild 16: Bearbeitung der Metadateneines Bildes mit GIMP

Im Tab GPS des Dialogs können die gewünschten Koordinaten eingegeben und gespeichert werden.

Bild 17: Manipulation der Geoinformationen eines Bildes

2.4.5 Verstecken von Dateien

Die zum Szenario gehörenden Artefakte sollen in einem versteckten Ordner gespeichert werden, so dass dieser Ordner standardmäßig nicht angezeigt wird.

Das Verstecken von Ordnern funktioniert unter Windows folgendermaßen: Zuerst muss man die Eigenschaften des Ordners öffnen (Linksklick bei der Maus → Eigenschaften) und dann den Haken bei der Checkbox `Versteckt` setzen:

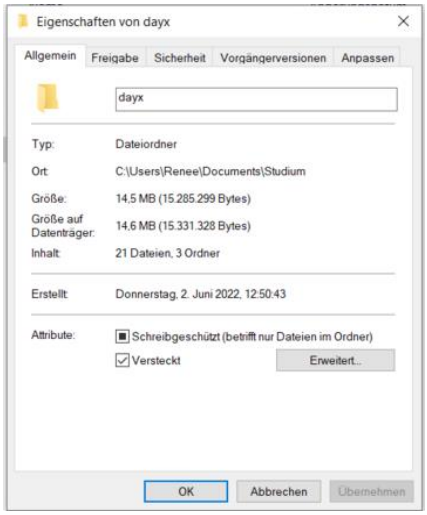


Bild 18: Ordner verstecken

Anschließend ist beim Bestätigen der Änderungen noch auszuwählen, dass alle enthaltenen Elemente (Ordner/Dateien) ebenfalls versteckt werden sollen.

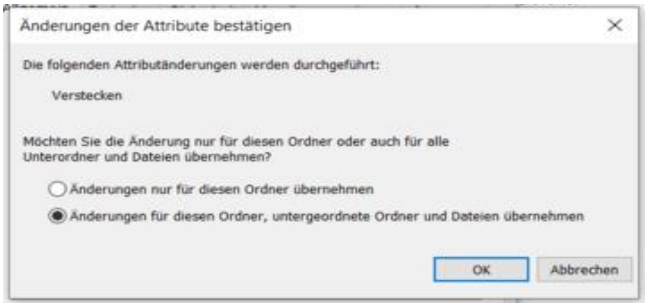


Bild 19: Untergeordnete Ordner und Dateien verstecken

2.4.6 Weitere Dateien

Auf dem USB-Stick sollen nicht nur die Artefakte für das Szenario zu finden sein, sondern auch weitere Dateien. Dazu wurden einige Bauanleitungen für Lego und Informationen aus dem Internet heruntergeladen und auf dem USB-Stick gespeichert.

2.4.7 Test des USB-Sticks

Nach der Sammlung der Artefakte wurde testweise ein Image sowohl mit Axiom als auch mit der Forensik-Software FTK-Imager erstellt, um zum einen die beiden Produkte auf ihre Anwendbarkeit zu prüfen und zum anderen die Funktionalität der Auswertung zu testen.

Beim ersten Test hat sich herausgestellt, dass die Zeiten an den Artefakten bzw. die Zeitleiste in Magnet Axiom nicht zum erdachten Szenario passten, da die Bilder aus dem Internet und auch die Google-Maps-Screenshots mit einem "neueren" Datum erstellt wurden als durch die Umstellung der Zeit "manipulierte" Änderungsdatum. Also mussten die Erstellzeiten geändert werden.

Diese Tests wurden mehrmals durchgeführt, bis die Zeiten logisch zum Szenario gepasst haben.

Bei einigen Kleinigkeiten haben wir auf die Bereinigung von Inkonsistenzen verzichtet, so ist in der Auswertung der Forensik-Software zu sehen sein wird, wenn ein Bild mit GIMP manipuliert, statt von einer Kamera aufgenommen wurde

2.4.8 Bildnachweise

Zur Vorbereitung des Täter Rechners sind Google-Maps-Screenshots erstellt worden,

die das Anschlagsziel der Gruppierung darstellen.

2.5 Forensische Datensicherung

Nachdem die Systeme vorbereiten wurden, müssen aus diesen Systemen forensische Images erzeugt werden. Dazu wird Axiom Process gestartet und ein Neuer Fall angelegt. Für die Fallnummer wurde StA-FFM-2022-06-15 verwendet und als Falltyp entsprechend unserem Szenario Terrorbekämpfung gewählt. Als Beweisquelle wird für den Täter-Rechner Windows und für den USB-Stick Removeable Media gewählt und bei den Artefakten, die in den Fall aufgenommen werden, wurden zunächst keine grundsätzlich ausgeschlossen.

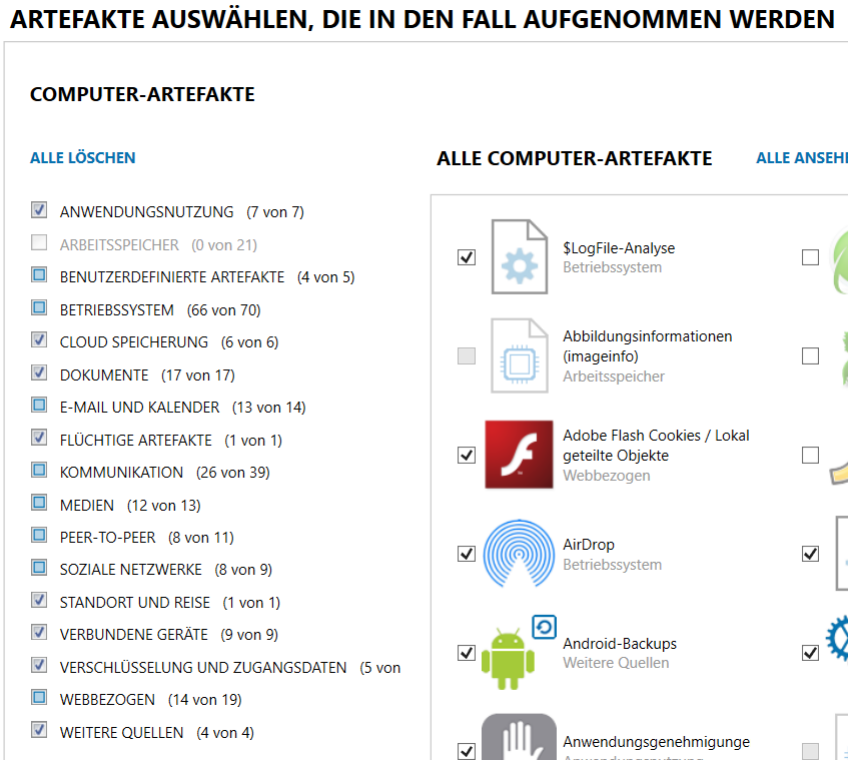


Bild 20: Artefakteauswahl für die Imageerstellung

Bei der Auswahl der Laufwerke wurde der USB-Stick und das VDI Laufwerk verwendet. Zudem wird mit dem Abbildtyp E01 die Images erstellt.

Ebenfalls wurde das Hashing für die Images aktiviert, was bedeutet, dass man die Integrität der Images nun sicherstellt. Als Hashverfahren wurde zum einen MD5 und SHA-1 gewählt.

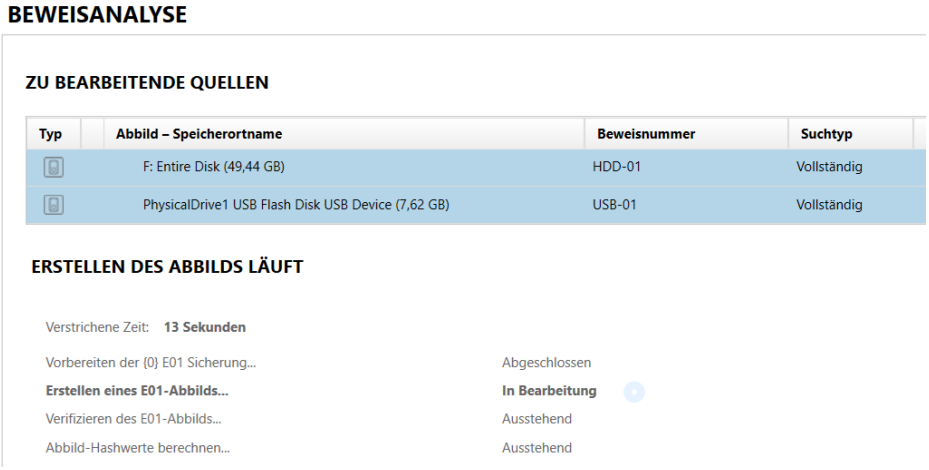


Bild 21: Imaging der beiden Systeme

Zur Absicherung des Erfolgs der Imageerstellung wurde nach dieser Magnet Axiom Examiner automatisch geöffnet und die Fallübersicht der Images dargestellt, was das nachfolgende Bild zeigt.

Abschließend liegen nun vier Images vor, zwei Sicherheitskopien und zwei Arbeitskopien, mit denen nun das Gutachten erstellt werden kann.

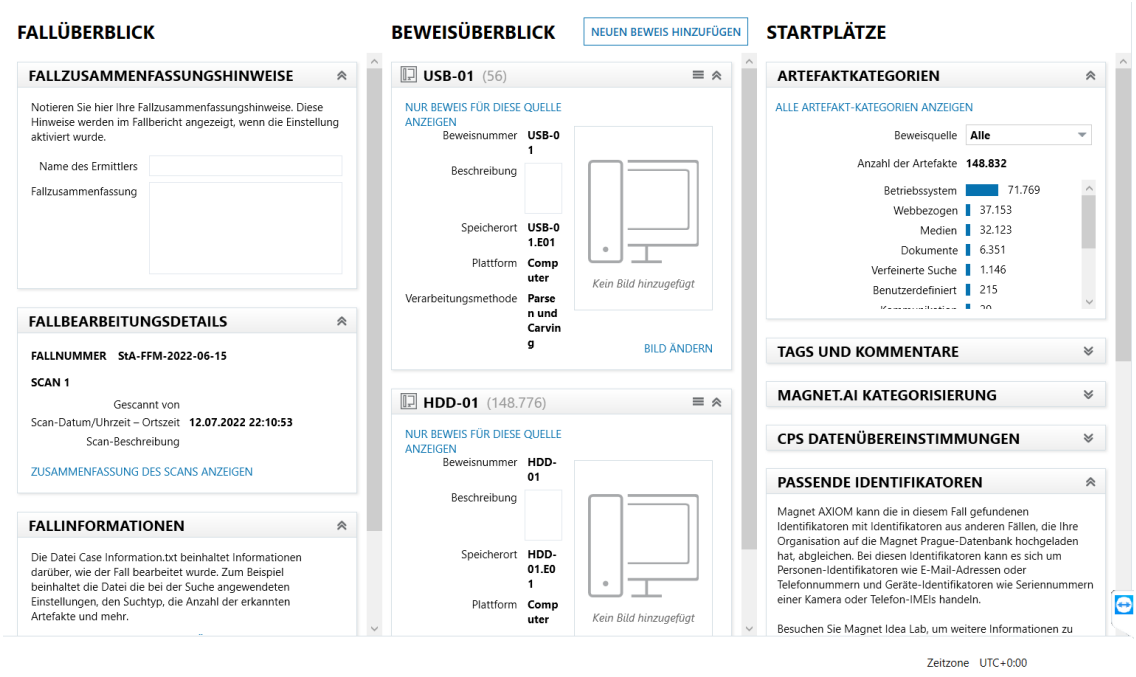


Bild 22: Fallübersicht nach Imageerstellung

3 Literaturverzeichnis

[1] DIRK LABUDDE / MICHAEL SPRANGER: „Forensik in der digitalen Welt“, 2017, Springer Verlag

[2] MAGNET FORENSICS: „New in Magnet AXIOM 5.8: Map Details Card, More Crypto Artifacts, and Magnet.AI Hate Symbol Update - Magnet Forensics“, https://www.magnetforensics.com/blog/new-in-magnet-axiom-5-8-map-details-card-more-cyprto-artifacts-and-magnet-ai-hate-symbol-update/, 14.12.2021, Zugriff: 04.07.2022

[3] FACEBOOK – MESSENGER: https://messenger.com, Zugriff 04.07.2022

[4] W77: „INDISK-TOOLKIT“, https://sourceforge.net/projects/imdisk-toolkit/, 01.03.2021, Zugriff 05.07.2022

[5] RENEEB: „Fake Chrome History“, https://github.com/reneeb/super-duper-guacamole, 14.07.2022, Zugriff: 14.07.2022

[6] JENS SCHRÖDER: „Top 100: die populärsten Websites in Deutschland“, Marktdaten Media, https://meedia.de/2014/12/10/top-100-die-populaersten-websites-in-deutschland/,10.12.2014, Zugriff: 06.07.2022

4 Tabellenverzeichnis

5 Bilderverzeichnis

Gutachten

im Auftrag der Staatsanwaltschaft Frankfurt

Herr Staatsanwalt Mustermann

Aktenzeichen Staatsanwaltschaft:

0472-745/MS/2022/01

Aktenzeichen Polizei

0472/FFM/2022/01

erstellt vom: HRS Forensics GmbH

Abschluss: 17. Juli 2022

HRS Forensics GmbH
Musterstraße 1
65931 Frankfurt

Tel.: 069 123 456 0
Email: info@hrs-forensics.de
Web: https://www.hrs-forensics.de

IBAN: DE12 3456 0000 1234 5678 90

Inhaltsverzeichnis

1. Auftragsspezifikation

Die Staatsanwaltschaft Frankfurt hat HRS Forensics mit der Auswertung einer Festplatte und eines USB-Sticks beauftragt sowie die Erstellung eines Gutachtens bis zum 17.07.2022.

Grund des Auftrags sind konkrete Hinweise auf einen möglichen Terroranschlag in Deutschland, weshalb die Polizei Heppenheim bei einer Hausdurchsuchung Asservate wie ein USB-Stick und ein möglichen Beschuldigten-Rechner sichergestellt hat.

Da der Verdächtige bereits seit Anfang 2022 in einer Gruppe aktiv ist, ist der relevante Zeitraum für die Artefakten-Analyse auf den 01.01.2022 bis zum 11.07.2022 einzugrenzen.

In diesem Zeitraum sollen alle Informationen gefunden werden,

- um dem vorliegenden Rechner mit dem Verdächtigen in Verbindung zu setzen,
- die darauf schließen lassen, dass der gefundene USB-Stick an dem gefundenen Rechner angeschlossen war,
- die Terrorverdächtige Inhalte aufzeigen,
- die ein potenzielles Anschlagsziel der Gruppe darstellen,
- die Hinweise auf Komplizen des Verdächtigen geben.

2. Zusammenfassung der Ermittlungsergebnisse

In diesem Kapitel werden die Ermittlungsergebnisse zusammengefasst. Zuerst nach Asservaten aufgeteilt und abschließend eine Gesamtbetrachtung.

2.1. Asservat 1- USB-01

Auf dem USB-Stick war besonders ein versteckter Ordner von Interesse. Darin wurde eine Hotelbuchung in Frankreich gefunden. Außerdem ein Lieferschein aus einem Baumarkt für Materialien, die für einen Bombenbau genutzt werden können. In dem Ordner `mitarbeiter` wurde eine Bilddatei entdeckt, die nicht eingeordnet werden kann, da diese ohne weitere Kommentare eine männliche Person zeigt. Im Verzeichnis `paeckchen` wurden Bilddateien gefunden, die Timer für Bomben und den grundsätzlichen Aufbau einer Rohrbombe zeigen. Der Ordner `umspannwerk` enthält Dateien zum Umspannwerk Lampertheim und das ehemalige Kernkraftwerk Biblis. Weiterhin wurden hier Fotos gefunden, die beim ehemaligen AKW Biblis aufgenommen wurden, wie die EXIF-Daten der Fotos gezeigt haben.

2.2. Asservat 2 - HDD-01

Die Analyse der Festplatte hat ergeben, dass neben den Systembenutzern nur der Benutzer „Heinz Werner“ angelegt war. In den Ereignislogs wurden auch nur Anmeldungen dieses Benutzers festgestellt. Die Prüfung der Historie des Webbrowsers Chrome hat ergeben, dass einige Suchbegriffe im Zusammenhang mit dem Thema „Bombe“ genutzt wurden (siehe Kapitel 5.2.23). Weiterhin wurden einige Dateien aus dem Forum `12chan.io` heruntergeladen, das von Behörden als Rechtsextremistisch eingestuft wird. Die Untersuchung der Festplatte hat eine Konversation mit Peter Herbert über den Facebook Messenger hervorgebracht.

2.3. Gesamtbetrachtung

Auf dem USB-Stick wurden Dateien gefunden, deren Namen mit denen aus der Download-Historie des Laptops übereinstimmen. Da zum Erstellungszeitpunkt dieser USB-Stick mit dem asservierten Laptop verbunden war, ist davon auszugehen, dass die Dateien von dem Laptop auf den USB-Stick übertragen wurden.

3. Untersuchungsobjekte

In dem Zeitraum vom 11.07.2022 bis zum 17.07.2022 fand die Untersuchung statt. Die folgenden Datenträger wurden als Untersuchungsobjekte an das Team zur Untersuchung übergeben und entsprechend auf dem Chain-of-Custody-Formular dokumentiert (siehe Anhang 1).

Asservat-Nr.	Art des Asservates	Seriennummer	Name des Asservates
Asservat-01	USB-Stick	8623C082	USB-01
Asservat-02	HDD	9A79546D	HDD-01

Tabelle 1: Übersicht der Asservate

Das nachfolgende Bild zeigt den übergebenen USB-Stick und das Bild 1 verdeutlicht die übergebene Festplatte.

Bild 2: Asservat-01 USB-01

Bild 1: Asservat-02 HDD-01

4. Untersuchungswerkzeuge, -ablauf und -methodik

Dieses Kapitel zeigt die verwendeten Forensik-Werkzeuge sowie den Untersuchungszeitraum und die angewendete Untersuchungsmethodik.

4.1. Untersuchungswerkzeuge

Das Forensik Team hat die übergebenen Asservate und Artefakte mit der folgenden Software untersucht.

Name	Hersteller	Version	Funktion
Google Earth Pro (Desktop)	Google LLC	7.3.4.8642	Darstellung der Orte, die aus EXIF-Daten gewonnen wurden
Magnet AXIOM	Magnet Forensics, Inc.	6.3.0.32040	Forensische Datenanalyse der Image Asservate
PowerShell	Microsoft	5.1.19041.1682	Prüfen der MD5 Hashes

Tabelle 2: Untersuchungswerkzeuge

Grundsätzlich ist Magnet Axiom dafür geeignet, die übergebenen Asservate gerichtsfest zu verarbeiten und auszuwerten.

4.2. Untersuchungszeitraum

Datum der Auftragserteilung.	11.07.2022
Untersuchungszeitraum	11.07.2022 – 17.07.2022
Zeitsynchronisation	Zeitzone UTC + 1:00

Tabelle 3: Untersuchungszeitraum

4.3. Untersuchungsmethodik

Bei der Untersuchungsmethodik wurde eine gewählt, die gerichtsfest also glaubwürdigen, objektiven, nachvollziehbaren sowie reproduzierbaren Untersuchung dargestellt. Um dies zu erfüllen, wurde nach dem SAP-Modell (Secure-Analyse-Present-Modell) gearbeitet:

Secure:

Das Forensik Team hat die Asservate übergeben bekommen, was entsprechend im dem Chain-of-Custody-Formular dokumentiert ist.

Von den übergebenen Asservaten wurden Sicherheitskopien erstellt, die den unveränderten Stand der Systeme darstellen. Von den Sicherheitskopien wurden Arbeitskopien erstellt, mit denen die Untersuchungen durchgeführt werden. Für die Sicherheitskopien sowie für die Arbeitskopien wurden Hashsummen gebildet und miteinander vergleichen, um die Integrität der Daten für den Untersuchungszeitraum zu wahren. Anhand der folgenden Tabelle wird deutlich, dass die Checksummen der Sicherheits- und Arbeitskopien übereinstimmen, sodass die Kopien zur Untersuchung verwendet werden können.

Image	Hashwert (Sicherheitskopie)	Hashwert (Arbeitskopie)
USB-01	MD5 checksum: d55c440f06d80ec0616bedb599b6f56b	MD5 checksum: d55c440f06d80ec0616bedb599b6f56b
HDD-01	MD5 checksum: 841c257473ede001d3af6eec3292214c	MD5 checksum: 841c257473ede001d3af6eec3292214c

Tabelle 4: Vergleich der Image-Checksummen

Analyse:

Die übergebenen Images wurden mit der Software Magnet AXIOM analysiert. Dabei wurde zunächst eine zeitliche Datenreduktion durchgeführt, sodass nur Daten betrachtet wurden, die sich in der möglichen Vorbereitungszeit des Beschuldigten befinden. Es wurden Datenkategorien zunächst nicht prinzipiell ausgeschlossen.

Present:

Eine detaillierte Vorgehensweise bei der Analyse und die resultierenden Untersuchungsergebnisse der Images werden unter dem Kapitel „Untersuchungsergebnisse“ aufgelistet. Die Ergebnisse werden mit Screenshots untermauert, die im Anhang zu finden sind. Darüber hinaus wird anhand einer Timeline die Vorbereitung des potenziellen Attentats rekonstruiert. Ergänzt wird die Timeline mit allen relevanten Artefakten und verbundenen, relevanten Aktionen aus beiden Asservaten.

5. Untersuchung der Asservate

In dem Kapitel 4.2 wurde der zu untersuchende Zeitraum auf den 01.01.2022 bis zum 11.07.2022 festgelegt. Eine Zeugin hatte eine Aussage bei der Polizei zu einem potenziellen Anschlag in Deutschland gemacht. Seit Anfang des Jahres ist der Verdächtige in der Gruppe Mitglied, sodass der untersuchende Zeitraum bis zum Untersuchungstag ausgedehnt wird.

5.1. Forensische Datenaufbereitung

Damit die Daten forensisch analysiert werden können, müssen diese zunächst aufbereitet werden. Das Forensik Team nutzt zum Extrahieren der relevanten digitalen Artefakte die Software Magnet AXIOM.

Im ersten Schritt wird ein neuer Fall in Magnet AXIOM angelegt und als Beweisquelle die Arbeitskopien der HDD und des USB-Sticks importiert (siehe Anhang 2). Bei der Datenaufbereitung wurde im Rahmen der Datenaufbereitung keine Artefakte von der Analyse ausgeschlossen (siehe Anhang 3).

Nachdem die Images als Beweisquellen ergänzt wurden, erfolgten die detaillierten Untersuchungen mit Hilfe des Moduls Magnet AXIOM Examine.

5.2. Forensische Datenanalyse

Dieses Kapitel stellt die forensische Datenanalyse der beiden Asservate dar. Hierbei wird jeweils zwischen der physischen Medienanalyse, Laufwerksanalyse und der Dateisystemanalyse unterschieden.

5.2.1. Asservat 1 – USB-Stick

Nach dem Vier-Augen-Prinzip erfolgte die Übergabe des Asservats 1, was entsprechend in dem Chain-of-custody-Formular dokumentiert ist.

Das USB-Stick-Image sollte auf Informationen untersucht werden, die potenziell vom Beschuldigten-Rechner auf den USB-Stick gespeichert wurden.

5.2.1.1. Physische Medienanalyse

Die Seriennummer des Asservates 1 (8623C082) wurde bereits im Kapitel 3 notiert zur weiteren Verwendung. Im Rahmen der Medienanalyse wurden außerdem folgende Datenträgerinformationen festgestellt (siehe Anlage 5).

Information	Wert
Gesamtkapazität (Bytes)	8162086912
Zugeteilter Bereich (Bytes)	43515904
Nicht zugeteilter Bereich (Bytes)	8118571008
Speichermediums-Offset (Bytes)	28672
Cluster gesamt	1992697
Freie Cluster	1982073
Sektoren gesamt	15974344
Startsektor	56
Endsektor	15974400
Bytes je Sektor	8
Sektoren je Cluster	512

Tabelle 5: Asservat 1 - Daten aus der physischen Medienanalyse

5.2.1.2. Laufwerksanalyse

Bei der Laufwerksanalyse wird der logische Aufbau des Datenträgers analysiert. Hierbei wurden die folgenden Partitionen identifiziert (siehe Anhang 10).

Name der Partition	Größe	Partitionstyp
Partition 1	8 GB	FAT32

Tabelle 6: Asservat 1 - Daten aus der Laufwerksanalyse

Die relevante Partition ist die Partition 1, denn da befinden sich die Dateien.

5.2.1.3. Dateisystemanalyse

Auf dem USB-01 befinden sich Dateien, die kategorisiert und hinsichtlich ihrer Relevanz für die aktuelle Untersuchung bewertet wurden.

Die Klassifizierung der gefundenen Ordner (siehe Anhang 4) wurden in Magnet AXIOM Examine mit dem Tag „von Interesse“ gekennzeichnet.

Kategorie	Datenmenge	Relevanzbewertung	Begründung
Ordner (versteckt)	4	Von Interesse	Planungsordner
Ordner	2	Nicht relevant	Keine verdächtigen Merkmale

Tabelle 7: Asservat 1 – Dateisystemanalyse - Ordner

Um sicherzustellen, dass die PDF-Dateien in den Nicht relevanten Ordnern keine versteckten Informationen enthalten, wurden die Dateien mit den URLs aus der Chrome-Historie der Festplatte aus dem Internet heruntergeladen und die MD5-Prüfsummen berechnet. Diese wurden mit den Ergebnissen der Forensik-Software für die gefundenen Dateien verglichen (siehe Anhang 6 und Anhang 7).

Die Prüfsummen waren alle gleich, so dass davon auszugehen ist, dass diese Dateien nicht manipuliert wurden und keine Geheiminformationen beinhalten.

Für die Prüfsummenberechnung der heruntergeladenen Dateien wurde Powershell mit folgendem Befehl genutzt:

```
Get-ChildItem -recurse | foreach-object { Get-FileHash $_.FullName -
Algorithm MD5 }
```

Zum einfacheren Vergleich wurden die MD5-Summen der Artefakte als Excel-Datei aus Axiom exportiert.

In den gekennzeichneten Ordnern sind insgesamt 21 Dateien identifiziert worden.

Diese 21 Dateien wurden unter der Dateierweiterung und auf Schlagwörtern zugewiesenen Artefakten-Kategorien hinsichtlich ihrer Relevanz für die aktuelle Untersuchung bewertet.

Kategorie	Anzahl Dateien	Relevanzbewertung	Begründung
PDF	2	Von Interesse	Verdächtige Dateinamen
Textdateien	1	Von Interesse	Verdächtige Dateinamen
Bilder / GIF	17	Von Interesse	Verdächtige Dateinamen
unbekannt	1	prüfen	Potenzielles Komplizenbild

Tabelle 8: Asservat 1 – Dateisystemanalyse - Dateien

Es wurden 21 Dateien mit dem Kennzeichen „von Interesse“ versehen. Diese Dateien wurden der folgenden inhaltlichen Untersuchung unterzogen.

5.2.1.4. Dateianalyse

Datei ablauf.txt

Datei Name	ablauf.txt
Datei Größe	177 Bytes
Angelegt	07.07.2022
Letzter Zugriff	07.07.2022
Dateiinhalt	15.07.2022 - Treffpunkt Zur Rheinfähre Nordhelm 8 Uhr Detonation 23:59 Uhr Notfalltreffpunkt WaldCamp Warndt AP: Herr Fuchs Nachtreffen McDonalds Morsbach 16.07.2022 22Uhr
Bewertung	Es könnte sich hierbei um den Ablaufplan des Anschlags handeln

Tabelle 9: Asservat 1 – Dateianalyse – ablauf

Datei Hotel.pdf

Datei Name	Hotel.pdf
Datei Größe	98,5 KB
Angelegt	07.07.2022
Letzter Zugriff	07.07.2022
Dateiinhalt	Hotelbuchungsbestätigung - Siehe Anhang 7: Hotelbuchung
Bewertung	Es könnte sich hierbei um ein Hotel auf der Fluchtroute sein.

Tabelle 10: Asservat 1 – Dateianalyse - Hotel

Datei Lieferschein.pdf

Datei Name	Lieferschein.pdf
Datei Größe	72,7 KB
Angelegt	07.07.2022
Letzter Zugriff	07.07.2022
Dateiinhalt	Lieferschein von Dünger, Fässer, Draht zu einem Zentrallager in Worms
Bewertung	Es könnte sich hierbei um eine Bestellung für eine Bombe handeln.

Tabelle 11: Asservat 1 – Dateianalyse – lieferschein

Datei UebersichtLampertheim.png

Datei Name	UebersichtLampertheim.png
Datei Größe	1,44 MB
Angelegt	07.07.2022
Letzter Zugriff	07.07.2022
Dateiinhalt	Übersicht eines Umspannwerkes bei Lampertheim
Bewertung	Potenzielles Anschlagsziel

Tabelle 12: Asservat 1 – Dateianalyse – Uebersicht Lampertheim

Über Axiom wurden die in Fotos gefundenen Geoinformationen exportiert und die daraus resultierende KML-Datei wurde in Google Earth Pro geladen, um herauszufinden, an welchen Orten diese Fotos aufgenommen wurden. Diese Prüfung hat ergeben, dass die Fotos alle im Umfeld des ehemaligen AKWs Biblis aufgenommen wurden (siehe Anhang 8 bis 10).

5.2.2. Asservat 2 – HDD vom Beschuldigten-Rechner

Nach dem Vier-Augen-Prinzip erfolgte die Übergabe des Asservats 2, was entsprechend in dem Chain-of-custody-Formular dokumentiert ist.

Das Rechner-Image sollte auf Informationen untersucht werden, die Hinweise auf Informationen auf einen potenziellen Anschlag hinweisen und darüber hinaus sollte festgestellt werden, ob der Verdächtige weitere Komplizen hat.

Beim Einlesen des Images wurden alle Artefakt-Kategorien in AXIOM Process berücksichtigt.

5.2.2.1. Physische Medienanalyse

Die Seriennummer des Asservates 2 (9A79546D) wurde bereits im Kapitel 3 notiert zur weiteren Verwendung. Im Rahmen der Medienanalyse wurden außerdem folgende Datenträgerinformationen festgestellt (siehe Anlage 4).

Information	Wert
Gesamtkapazität (Bytes)	53080678400
Zugeteilter Bereich (Bytes)	21777960960
Nicht zugeteilter Bereich (Bytes)	31302717440
Speichermediums-Offset (Bytes)	0
Cluster gesamt	21959150
Freie Cluster	7642265
Sektoren gesamt	103673200
Startsektor	0
Endsektor	103673200
Bytes je Sektor	512
Sektoren je Cluster	8

Tabelle 13: Asservat 2 - Daten aus der physischen Medienanalyse

5.2.2.2. Laufwerksanalyse

Bei der Laufwerksanalyse wird der logische Aufbau des Datenträgers analysiert. Hierbei wurde die folgende Partition identifiziert (siehe Anhang 11).

Information	Größe	Partitionstyp	Bedeutung
Partition 1	49,44 GB	Microsoft NTFS	Betriebssystem und Nutzerdaten

Tabelle 14: Asservat 2 - Daten aus der Laufwerksanalyse

5.2.2.3. Dateisystemanalyse

Auf der einen Partition befinden sich Daten eines zu analysierenden Windows 10 Education Betriebssystems mit dem Dateiformat NTFS. Jede Datei hat einen Zeitstempel und eine physikalische Adresse.

Die Dateisystemanalyse dient dem Rekonstruieren der Vorgänge ohne Zugriff auf das eigentliche Betriebssystem.

Um die Planung des potenziellen Anschlags zu identifizieren, wird zunächst nach Daten des Dateisystems gesucht, die zeitlich für die Untersuchung relevant sind.

Dazu wird im Axiom Examine die Zeitleiste für den Zeitraum vom 01.01.2022 bis 11.07.2022 dargestellt. Als Beweise enthalten ist das Image des Beschuldigten-Rechners Asservat 2 und zur Ergänzung das Image des Asservats 1 (USB-Stick), wobei in diesem Abschnitt nur die Untersuchung des Asservats 2 beschrieben wird. Es werden alle Artefakte ausgewählt.

Fragestellung 1: Welchem Benutzer gehört dieser Rechner?

Da es sich um die Festplatte des Laptops handelt, sind in dem Image auch Informationen zu Benutzerkonten zu finden. Dabei ist zu sehen, dass das einzige Benutzerkonto, das nicht vom System angelegt wird, das Konto „Heinz Werner“ ist.

Ergebnisse:

Es konnte nachgewiesen werden, dass der Rechner zu dem Benutzer Heinz Werner gehört (siehe Anhang 12).

Fragestellung 2:

Wurde der USB-Stick an diesem Rechner angeschlossen?

Bekannt ist aus der Analyse des Asservats 1, dass sich auf dem USB-Stick, Dateien befinden, die das potenzielle Anschlagsziel enthält. Deshalb wird geprüft, ob der USB-Stick mit dem Beschuldigen Rechner verbunden war und ob dabei Dateien übertragen wurden.

Ergebnis:

Es konnte nachgewiesen werden, dass der USB-Stick (Asservat 1) mit dem Beschuldigten-Rechner verbunden war (Anhang 13).

USB-Gerät	Anzahl der Zeitstempel	Zeitstempel
Zu findende Seriennummer: SCY0000000053715 Seriennummer: 8623C082	5	Installationszeitraum: 07.07.2022 04:42:44 Zuletzt verbunden: 09.07.2022 00:08:09 Datum der ersten Installation: 07.07.2022 04:42:44 Zuletzt eingefügt: 09.07.2022 00:08:09 Zuletzt gelöscht: 09.07.2022 00:08:29

Tabelle 15: Asservat 2 - Zeitstempel USB-Stick

Fragestellung 3:

Welche Terrorverdächtigen Inhalte sind auf dem Beschuldigten-Rechner zu finden?

Ergebnis:

In dem Image waren die Browser-Historien von zwei verschiedenen Browsern zu finden. Zum einen des vorinstallierten Browsers Microsoft Edge und weiterhin von Google Chrome.

In der Historie des Microsoft Edge sind Webseitenbesuche bei Google, Facebook, Discord sowie Bing zu finden. Bei Facebook wurde mehrfach nach einem „Peter Herbert“ gesucht. Weitere Personensuchen fanden nicht statt.

In den Downloads des Microsoft Edge sind nur zwei Einträge zu finden: Es wurden der Browser Google Chrome und die Chatanwendung Messenger (von Facebook) heruntergeladen.

Die weiteren Webaktivitäten wurden über den Google Chrome erledigt. Hervorzuheben sind die Besuche der Webseiten booking.com, facebook.com und 12chan.io, die jeweils sehr häufig besucht wurden.

In der Historie des Chrome Download-Manager sind heruntergeladene Dateien der 12chan.io Webseite zur Herstellung von Bomben gefunden worden (siehe Anhang 14). Diese sind nun auf dem USB-Stick zu finden.

Darüber hinaus wurde in der Chrome Historie über die Google Suche verschiedene Begriffe zu dem Thema „Bombe“ gefunden (siehe Anhang 17).

Fragestellung 4:

Welches Ziel könnte von dem Terroranschlag betroffen sein?

Ergebnis:

Das potenzielle Anschlagsziel kann mit der Datenanalyse des USB-Stick vermutet werden. Dazu kann zum einen die Datei UebersichtLampertheim.png und zum anderen zeigen die weiteren Geolocations der anderen Bilder dieselbe Gegend – Lampertheim (siehe Anhang 8-10).

Fragestellung 5:

Gibt es Hinweise darauf, dass der Terrorverdächtige Komplizen hat?

Ergebnis:

Über die Forensik-Software wurden Chatnachrichten gefunden, die über den Facebook Messenger verschickt wurden. Teilnehmer der Konversation waren „Heinz Werner“ (UID: 100010023856128) und „Peter Herbert“ (UID: 100082977227173). In dieser Konversation wurde am 07.07.2022 über „die nächste Woche“ gesprochen. Der Chat-verlauf ist im Anhang 15 zu finden.

6. Untersuchungsergebnisse

Die Untersuchungsergebnisse werden in diesem Kapitel zusammengefasst, die in den vorhergehenden Kapiteln detailliert beschrieben wurden.

6.1. Untersuchungsergebnisse – Timeline

Die identifizierten Artefakte und daraus resultierenden Vorbereitungen auf einen Terroranschlag werden im Folgenden chronologisch aufsteigend geordnet dargestellt.

Darüber hinaus kann zeigt der Anhang 16 die entsprechende graphische Timeline an.

Zeitpunkt	Asservat	Artefakt Bezeichner	Festgestellte Aktion	Kommentar
05.01.2022 10:21:07 Uhr	Asservat 1	Koordinaten.biblis.png lampertheim.png uebersichtakwbiblis.png	Datei angelegt	
15.01.2022 10:34:04 Uhr	Asservat 1	Ablauf.txt	Datei angelegt	
18.01.2022 18:54:04 Uhr	Asservat 2	schema-timer.gif	Datei download	Nun auf Asservat 1 zu finden
25.01.2022 17:25:07 Uhr	Asservat 1	400-110-30-kv-transformator-1030105.jpg GRKRT_110-20_neuer_Trafo_eqos-Lieferwagen.jpg	Datei angelegt	
04.03.2022 12:33:07 Uhr	Asservat 1	Lieferschein.pdf	Datei angelegt	

25.05.2022	Asservat 2	28861375-ein-countdown-zaehler-der-wie-eine-bombenattrappe-aussieht-4ea.jpg	Datei download	Nun auf Asservat 1 zu finden
07.07.2022 04:42:44 Uhr	Asservat 2	USB-Stick an Beschuldigten-Rechner	Device angeschlossen	Anhang 13
07.07.2022 05:33:17 Uhr	Asservat 2	Facebook Messenger Chat	Kommunikation	Anhang 15

Tabelle 16: Timeline 1

6.2. Untersuchungsergebnisse – inhaltliche Feststellungen

In diesem Kapitel werden die Untersuchungsergebnisse mit den inhaltlichen Feststellungen dargestellt.

6.2.1. Asservat 1 – USB-Stick-01

Auf dem USB-Stick war besonders ein versteckter Ordner von Interesse. Darin wurde eine Hotelbuchung in Frankreich gefunden. Außerdem ein Lieferschein aus einem Baumarkt für Materialien, die für einen Bombenbau genutzt werden können. In dem Ordner `mitarbeiter` wurde eine Bilddatei entdeckt, die nicht eingeordnet werden kann, da diese ohne weitere Kommentare eine männliche Person zeigt. Im Verzeichnis `paeckchen` wurden Bilddateien gefunden, die Timer für Bomben und den grundsätzlichen Aufbau einer Rohrbombe zeigen. Der Ordner `umspannwerk` enthält Dateien zum Umspannwerk Lampertheim und das ehemalige Kernkraftwerk Biblis. Weiterhin wurden hier Fotos gefunden, die beim ehemaligen AKW Biblis aufgenommen wurden, wie die EXIF-Daten der Fotos gezeigt haben.

6.2.1.1. Asservat 2 – HDD-01

Die Analyse der Festplatte hat ergeben, dass neben den Systembenutzern nur der Benutzer „Heinz Werner“ angelegt war. In den Ereignislogs wurden auch nur Anmeldungen dieses Benutzers festgestellt. Die Prüfung der Historie des Webbrowsers Chrome hat ergeben, dass einige Suchbegriffe im Zusammenhang mit dem Thema

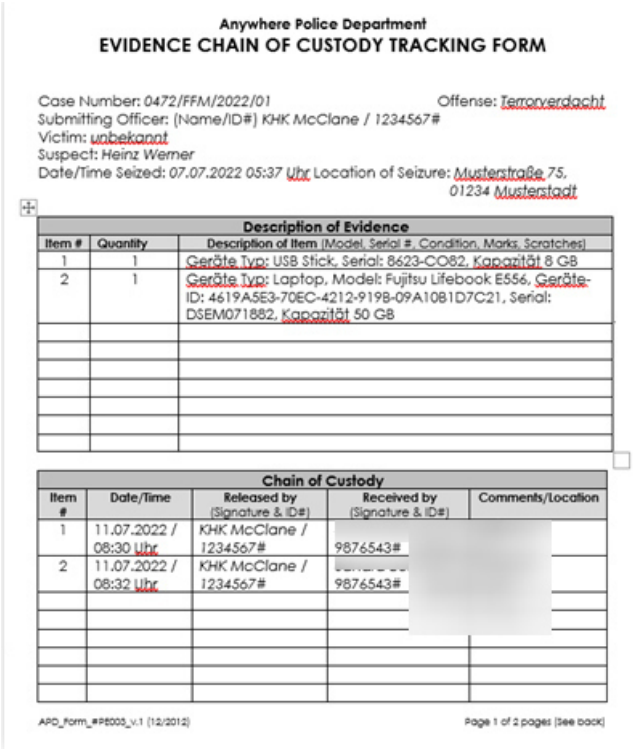
„Bombe“ genutzt wurden (siehe Kapitel 5.2.2.3). Weiterhin wurden einige Dateien aus dem Forum `12chan.io` heruntergeladen, das von Behörden als Rechtsextremistisch eingestuft wird. Die Untersuchung der Festplatte hat eine Konversation mit Peter Herbert über den Facebook Messenger hervorgebracht.

7. Tabellenverzeichnis

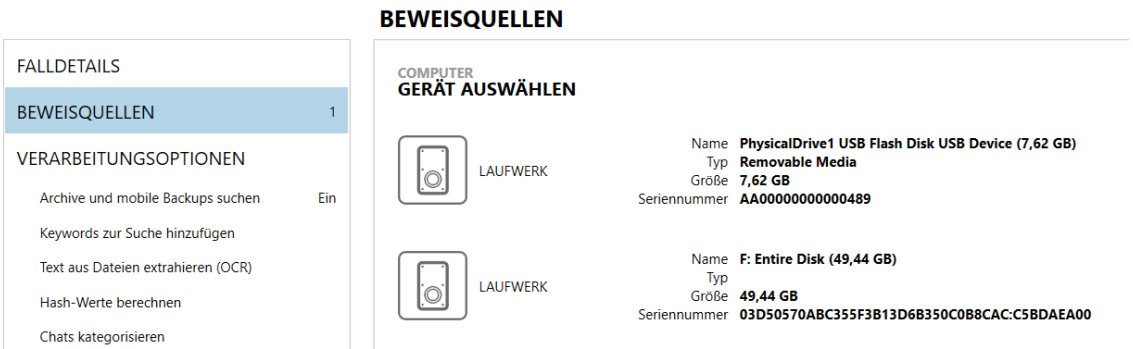
8. Bilderverzeichnis

9. Anlagenverzeichnis

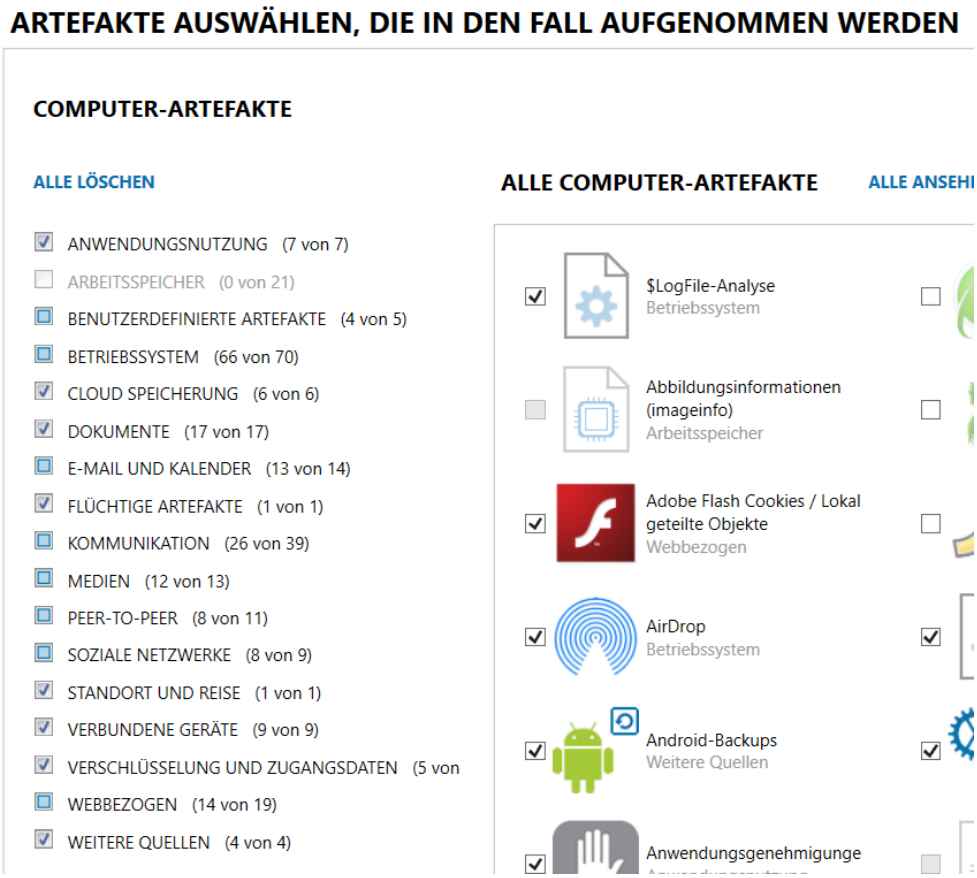
Anhang 1: Chain-of.custody Formulare



Anhang 2: Beweisquellen

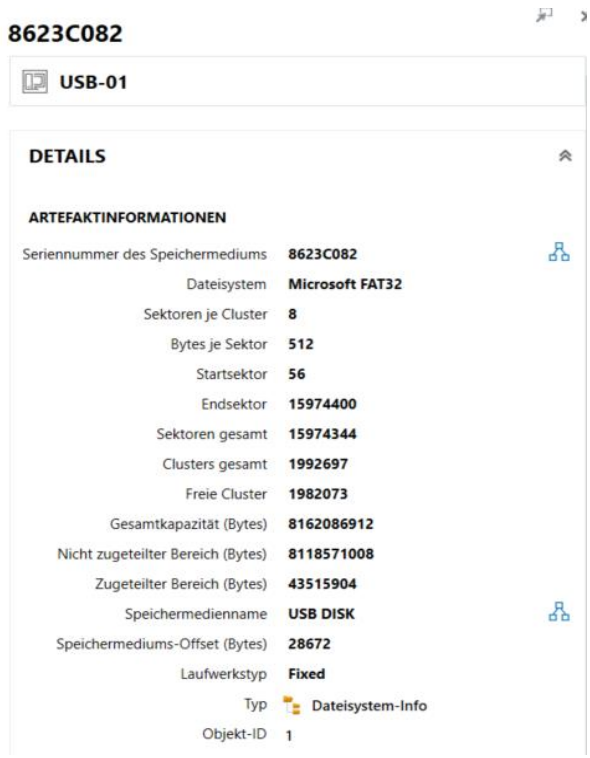


Anhang 3: Artefaktenauswahl

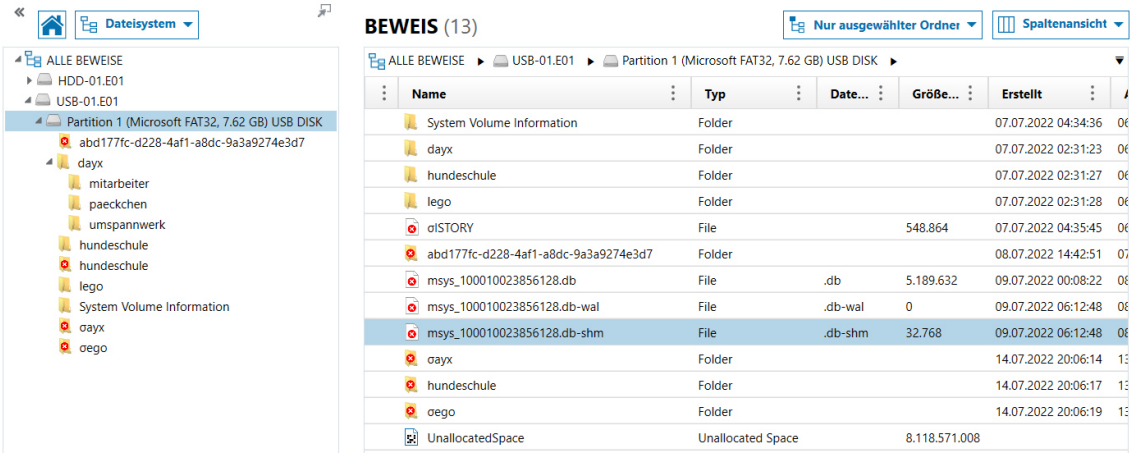


Anhang 4: Informationen zu der HDD

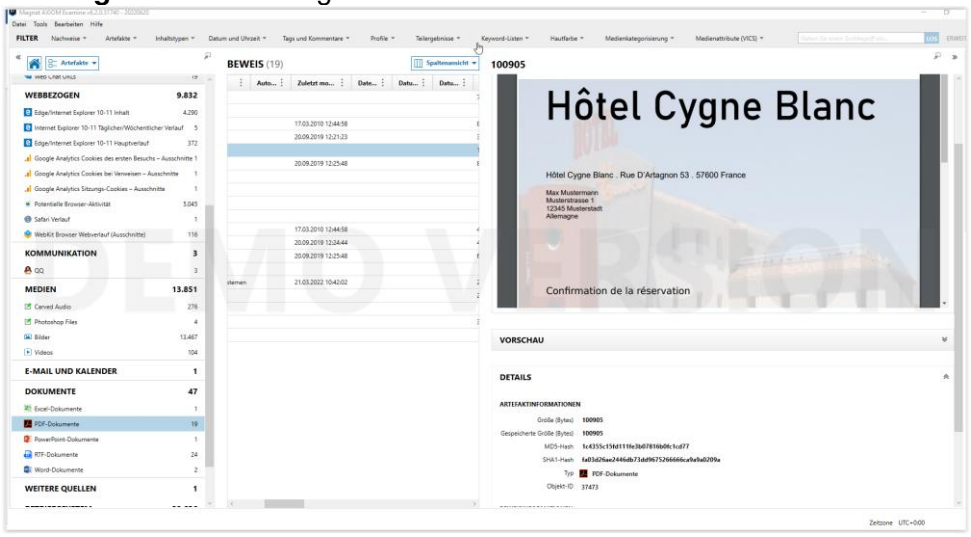
Anhang 5: Informationen zu der USB-Stick0



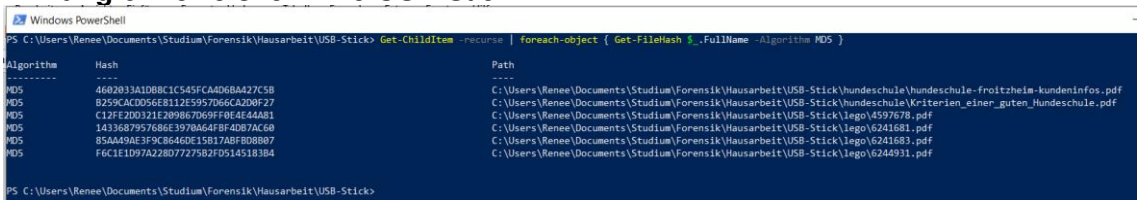
Anhang 4: USB-Stick - Ordner Struktur



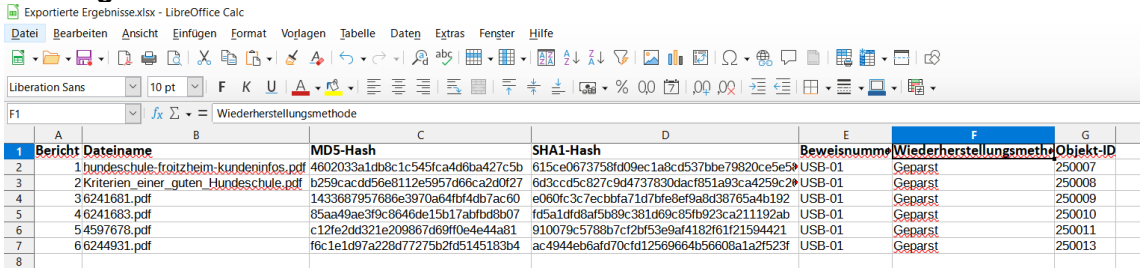
Anhang 5: Hotelbuchung



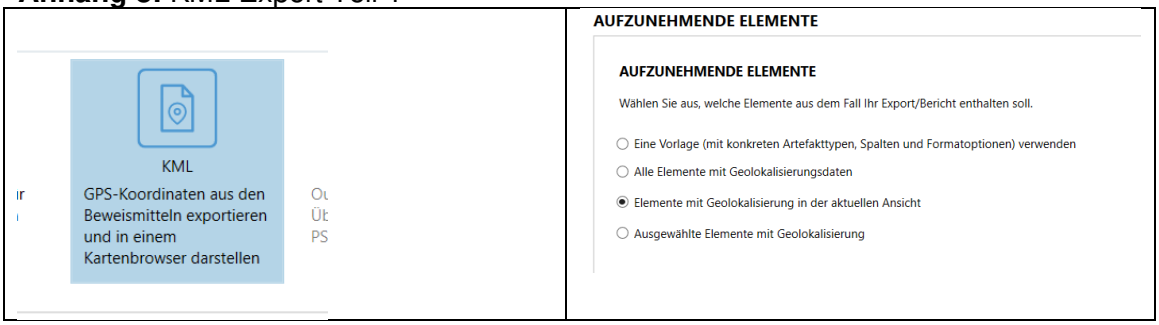
Anhang 6: Powershell MD5 USB-Stick



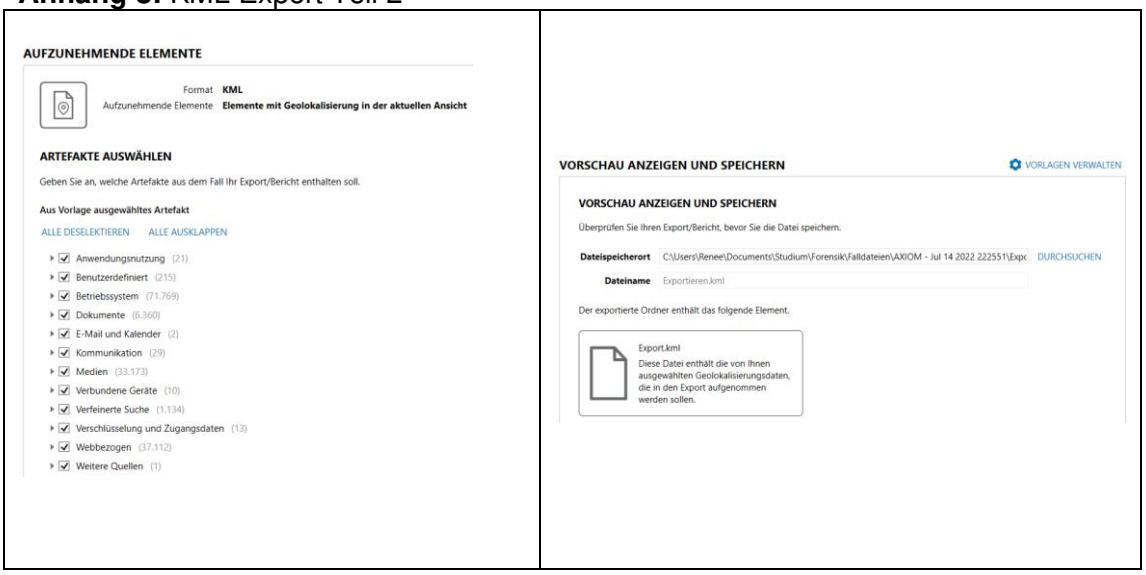
Anhang 7: Axiom MD5 USB-Stick



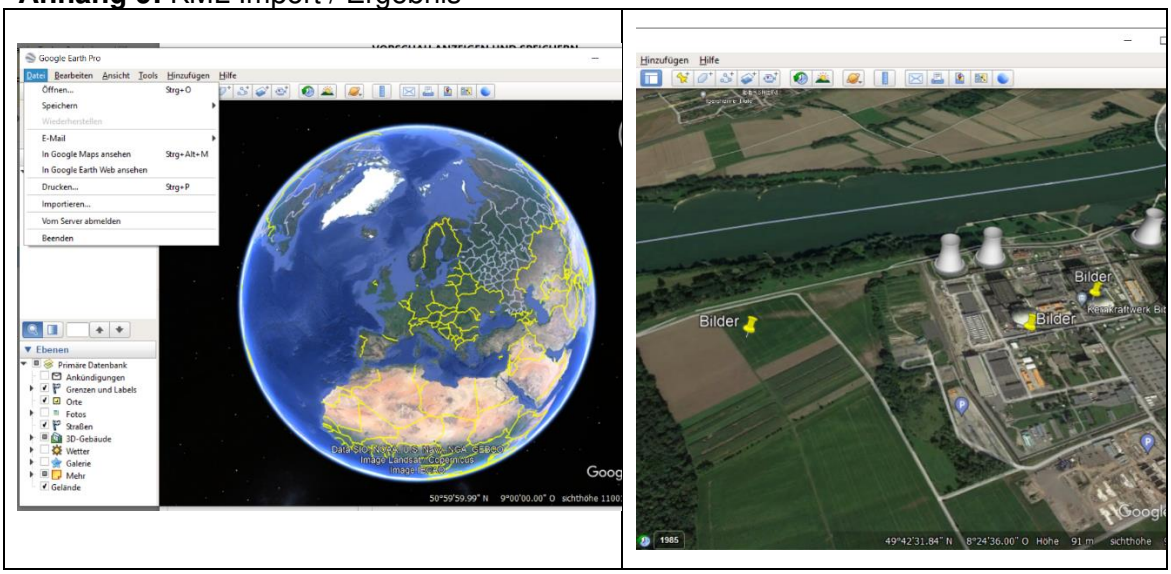
Anhang 8: KML Export Teil 1



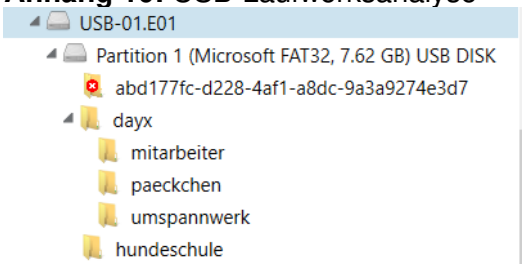
Anhang 8: KML Export Teil 2



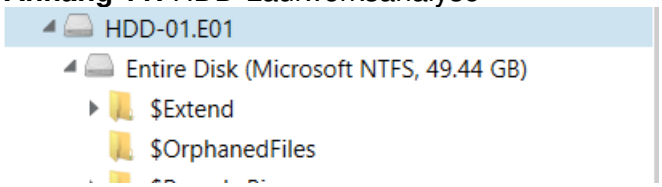
Anhang 9: KML Import / Ergebnis



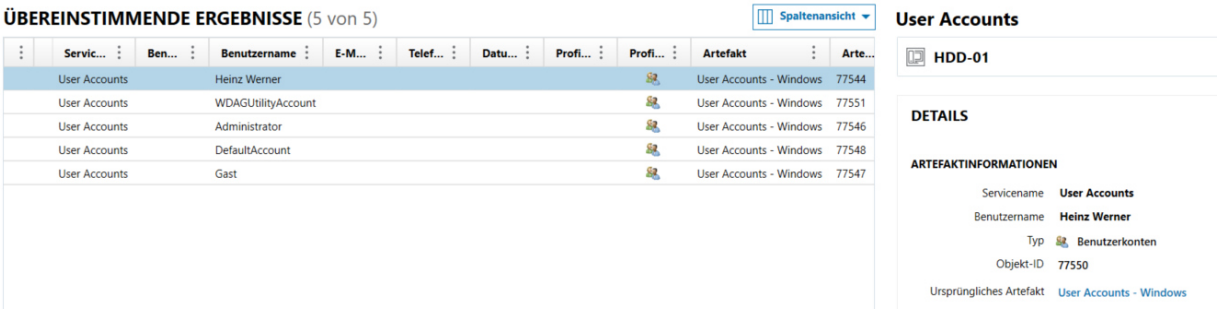
Anhang 10: USB-Laufwerksanalyse



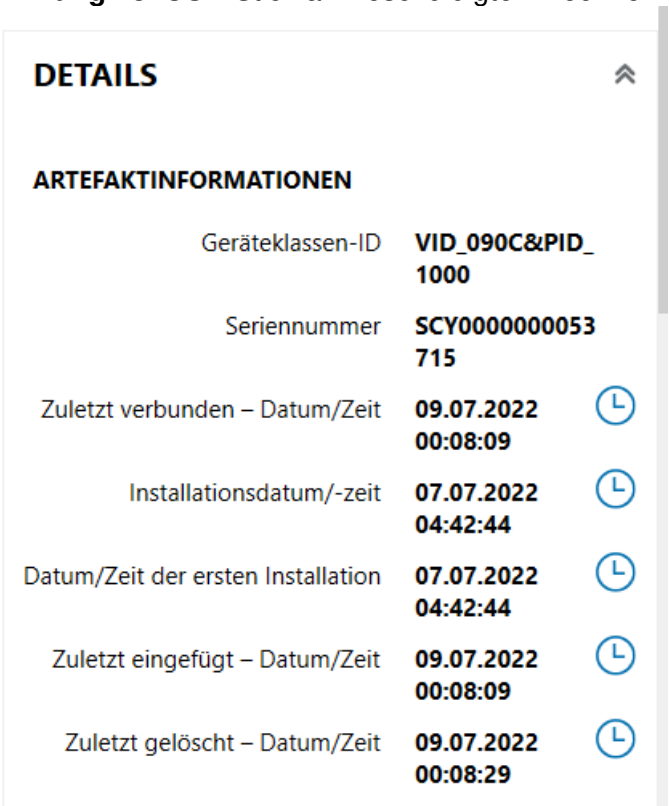
Anhang 11: HDD-Laufwerksanalyse



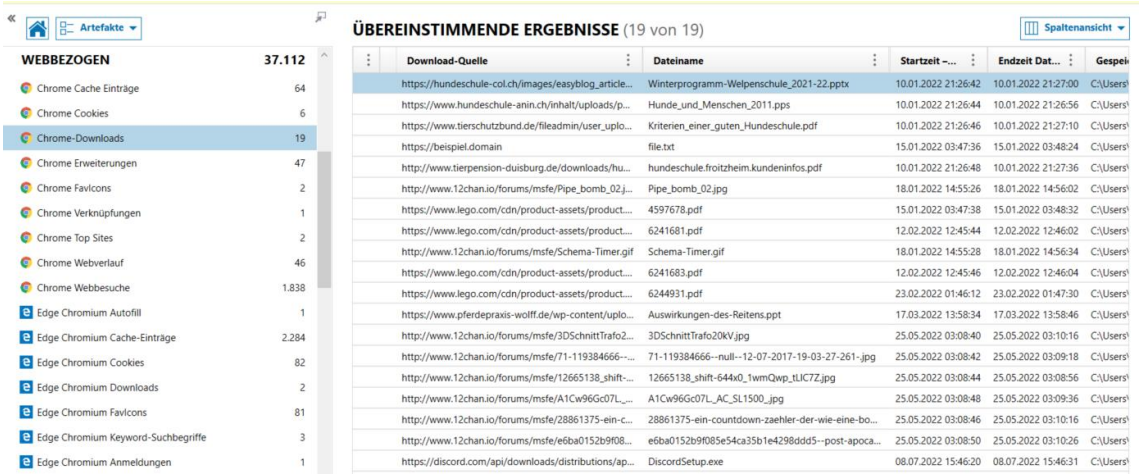
Anhang 12: Useraccount Hein Werner



Anhang 13: USB-Stick an Beschuldigten-Rechner



Anhang 14: Chrome Historie Download Manager



Artefakte

WEBBEZOGEN	37.112
Chrome Cache Einträge	64
Chrome Cookies	6
Chrome-Downloads	19
Chrome Erweiterungen	47
Chrome FavIcons	2
Chrome Verknüpfungen	1
Chrome Top Sites	2
Chrome Webverlauf	46
Chrome Webbesuche	1.838
Edge Chromium Autofill	1
Edge Chromium Cache-Einträge	2.284
Edge Chromium Cookies	82
Edge Chromium Downloads	2
Edge Chromium FavIcons	81
Edge Chromium Keyword-Suchbegriffe	3
Edge Chromium Anmeldungen	1

ÜBEREINSTIMMENDE ERGEBNISSE (19 von 19) — Spaltenansicht

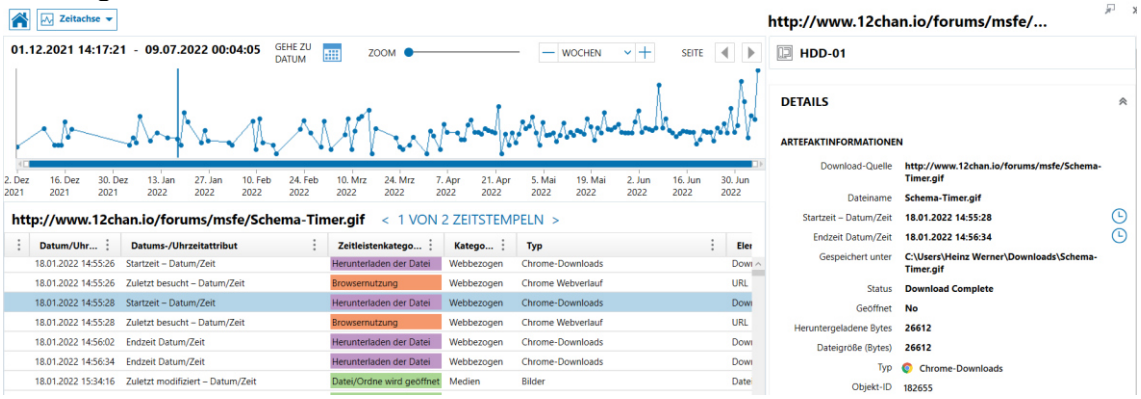
Download-Quelle	Dateiname	Startzeit –...	Endzeit Dat...	Gespei
https://hundeschule-col.ch/images/easyblog_article...	Winterprogramm-Welpenschule_2021-22.pptx	10.01.2022 21:26:42	10.01.2022 21:27:00	C:\Users\
https://www.hundeschule-anin.ch/inhalt/uploads/p...	Hunde_und_Menschen_2011.pps	10.01.2022 21:26:44	10.01.2022 21:26:56	C:\Users\
https://www.tierschutzbund.de/fileadmin/user_uplo...	Kriterien_einer_guten_Hundeschule.pdf	10.01.2022 21:26:46	10.01.2022 21:27:10	C:\Users\
https://beispiel.domain	file.txt	15.01.2022 03:47:36	15.01.2022 03:48:24	C:\Users\
http://www.tierpension-duisburg.de/downloads/hu...	hundeschule.froitzheim.kundeninfos.pdf	10.01.2022 21:26:48	10.01.2022 21:27:36	C:\Users\
http://www.12chan.io/forums/msfe/Pipe_bomb_02.j...	Pipe_bomb_02.jpg	18.01.2022 14:55:26	18.01.2022 14:56:02	C:\Users\
https://www.lego.com/cdn/product-assets/product....	4597678.pdf	15.01.2022 03:47:38	15.01.2022 03:48:32	C:\Users\
https://www.lego.com/cdn/product-assets/product....	6241681.pdf	12.02.2022 12:45:44	12.02.2022 12:46:02	C:\Users\
http://www.12chan.io/forums/msfe/Schema-Timer.gif	Schema-Timer.gif	18.01.2022 14:55:28	18.01.2022 14:56:34	C:\Users\
https://www.lego.com/cdn/product-assets/product....	6241683.pdf	12.02.2022 12:45:46	12.02.2022 12:46:04	C:\Users\
https://www.lego.com/cdn/product-assets/product....	6244931.pdf	23.02.2022 01:46:12	23.02.2022 01:47:30	C:\Users\
https://www.pferdepraxis-wolff.de/wp-content/uplo...	Auswirkungen-des-Reitens.ppt	17.03.2022 13:58:34	17.03.2022 13:58:46	C:\Users\
http://www.12chan.io/forums/msfe/3DSchnittTrafo2...	3DSchnittTrafo20kV.jpg	25.05.2022 03:08:40	25.05.2022 03:10:16	C:\Users\
http://www.12chan.io/forums/msfe/71-119384666-...	71-119384666--null--12-07-2017-19-03-27-261-.jpg	25.05.2022 03:08:42	25.05.2022 03:09:18	C:\Users\
http://www.12chan.io/forums/msfe/12665138_shift-...	12665138_shift-644x0_1wmQwp_tLIC7Z.jpg	25.05.2022 03:08:44	25.05.2022 03:08:56	C:\Users\
http://www.12chan.io/forums/msfe/A1Cw96Gc07L_...	A1Cw96Gc07L._AC_SL1500_.jpg	25.05.2022 03:08:48	25.05.2022 03:09:36	C:\Users\
http://www.12chan.io/forums/msfe/28861375-ein-c...	28861375-ein-countdown-zaehler-der-wie-eine-bo...	25.05.2022 03:08:46	25.05.2022 03:10:16	C:\Users\
http://www.12chan.io/forums/msfe/e6ba0152b9f08...	e6ba0152b9f085e54ca35b1e4298ddd5--post-apoca...	25.05.2022 03:08:50	25.05.2022 03:10:26	C:\Users\
https://discord.com/api/downloads/distributions/ap...	DiscordSetup.exe	08.07.2022 15:46:20	08.07.2022 15:46:31	C:\Users\

Anhang 15: Facebook Messenger Chat

ÜBEREINSTIMMENDE ERGEBNISSE (15 von 15)

Name...	Absender-...	Name...	Empfänge...	Datum/Zeit	Text	Nac...
Heinz Werner	100010023856128	LGW it services	406287572896644	06.10.2015 11:39:43	Tsetasdfasdf	Text
Heinz Werner	100010023856128	Peter Herbert	100082977227173	07.07.2022 05:33:17	Hallo Peter, alles klar für nächste Woche?	Text
Peter Herbert	100082977227173	Heinz Werner	100010023856128	07.07.2022 05:34:40	Ja, bei mir ist alles soweit vorbereitet	Text
Peter Herbert	100082977227173	Heinz Werner	100010023856128	07.07.2022 05:35:11	Die Päckchen sind gepackt und warten nur auf Abh...	Text
Heinz Werner	100010023856128	Peter Herbert	100082977227173	07.07.2022 05:35:52	Super, bin mal gespannt was die Empfänger dann d...	Text
Peter Herbert	100082977227173	Heinz Werner	100010023856128	07.07.2022 05:36:54	Die werden sich freuen wenn sie das Ergebnis sehen...	Text
Heinz Werner	100010023856128	Peter Herbert	100082977227173	07.07.2022 05:37:34	Das wird schon. Diese Idioten haben es nicht anders...	Text
Heinz Werner	100010023856128	Peter Herbert	100082977227173	07.07.2022 05:38:45	Ich hoffe, Du bist pünktlich am Treffpunkt	Text
Peter Herbert	100082977227173	Heinz Werner	100010023856128	07.07.2022 05:40:05	Klar, 8 Uhr an der Fähre	Text
Peter Herbert	100082977227173	Heinz Werner	100010023856128	07.07.2022 05:40:59	Übrigens haben sich die Franzmänner bei mir gemel...	Text
Peter Herbert	100082977227173	Heinz Werner	100010023856128	07.07.2022 05:41:21	Da ist dann auch eine Route zu einem sicheren Haus...	Text
Peter Herbert	100082977227173	Heinz Werner	100010023856128	07.07.2022 05:41:41	Die werden uns auch mit der Weiterreise helfen.	Text
Heinz Werner	100010023856128	Peter Herbert	100082977227173	07.07.2022 05:41:53	Sticker: 369239263222822	Sticker
Heinz Werner	100010023856128	Peter Herbert	100082977227173	07.07.2022 05:42:14	Ich freu mich schon aufs Feuerwerk.	Text
Heinz Werner	100010023856128	Peter Herbert	100082977227173	07.07.2022 05:42:31	Ich muss jetzt aber mal weitermachen.	Text

Anhang 16: Timeline



Zeitachse

01.12.2021 14:17:21 - 09.07.2022 00:04:05 — GEHE ZU DATUM — ZOOM — WOCHEN — SEITE

2. Dez 2021 · 16. Dez 2021 · 30. Dez 2021 · 13. Jan 2022 · 27. Jan 2022 · 10. Feb 2022 · 24. Feb 2022 · 10. Mrz 2022 · 24. Mrz 2022 · 7. Apr 2022 · 21. Apr 2022 · 5. Mai 2022 · 19. Mai 2022 · 2. Jun 2022 · 16. Jun 2022 · 30. Jun 2022

http://www.12chan.io/forums/msfe/Schema-Timer.gif < 1 VON 2 ZEITSTEMPELN >

Datum/Uhr...	Datums-/Uhrzeitattribut	Zeitleistenkatego...	Katego...	Typ	Ele
18.01.2022 14:55:26	Startzeit – Datum/Zeit	Herunterladen der Datei	Webbezogen	Chrome-Downloads	Dowi
18.01.2022 14:55:26	Zuletzt besucht – Datum/Zeit	Browsernutzung	Webbezogen	Chrome Webverlauf	URL
18.01.2022 14:55:28	Startzeit – Datum/Zeit	Herunterladen der Datei	Webbezogen	Chrome-Downloads	Dowi
18.01.2022 14:55:28	Zuletzt besucht – Datum/Zeit	Browsernutzung	Webbezogen	Chrome Webverlauf	URL
18.01.2022 14:56:02	Endzeit Datum/Zeit	Herunterladen der Datei	Webbezogen	Chrome-Downloads	Dowi
18.01.2022 14:56:34	Endzeit Datum/Zeit	Herunterladen der Datei	Webbezogen	Chrome-Downloads	Dowi
18.01.2022 15:34:16	Zuletzt modifiziert – Datum/Zeit	Datei/Ordne wird geöffnet	Medien	Bilder	Date

http://www.12chan.io/forums/msfe/...

HDD-01

DETAILS

ARTEFAKTINFORMATIONEN

Download-Quelle	http://www.12chan.io/forums/msfe/Schema-Timer.gif
Dateiname	Schema-Timer.gif
Startzeit – Datum/Zeit	18.01.2022 14:55:28
Endzeit Datum/Zeit	18.01.2022 14:56:34
Gespeichert unter	C:\Users\Heinz Werner\Downloads\Schema-Timer.gif
Status	Download Complete
Geöffnet	No
Heruntergeladene Bytes	26612
Dateigröße (Bytes)	26612
Typ	Chrome-Downloads
Objekt-ID	182655

Anhang 17: Google Suchbegriffe

ÜBEREINSTIMMENDE ERGEBNISSE (7 von 23)

Spaltenansicht

Suchbegriff	URL	Datum/Zeit	Datu...	Origi...	Such...
lagerhalle worms mieten	https://www.google.de/search?q=lagerhalle+worms...	02.02.2022 06:02:24			
lagerhalle lampertheim	https://www.google.de/search?q=lagerhalle+lampe...	02.02.2022 06:02:20			
bombe zünder	https://www.google.de/search?q=bombe+zünder	27.01.2022 16:31:42			
bombe dünger	https://www.google.de/search?q=bombe+dünger	27.01.2022 16:31:40			
bombe bauen	https://www.google.de/search?q=bombe+bauen	27.01.2022 16:31:38			
lagerhallen privat mieten lampertheim	https://www.google.de/search?q=lagerhallen+priva...	27.01.2022 16:31:36			
lagerhalle worms	https://www.google.de/search?q=lagerhalle+worms	02.02.2022 06:02:22			