Hochschule Wismar

Studiengang Master

„IT-Sicherheit und Forensik“

Modul

„Forensik in Betriebs- und Anwendungssystemen“

Praktikumsbericht

Gruppe HH 08

<Autor A>

<Autor B>

<Autor C>

Inhalt

1. Sachverhalt (Szenario) ... 3
1.1. Einordnung des Vorfalls nach CERT Taxonomie ... 3
2. Strategische Vorbereitung ... 3
3. Operationale Vorbereitung ... 4
3.1. Identifikation und Enumeration der Datenquellen ... 4
3.2. Klärung der Ermächtigungsgrundlagen ... 4
3.3. Klärung von Einwilligungen ... 4
3.4. Identifikation & Auswahl geeigneter Werkzeuge und Verfahren ... 4
4. Dokumentation der forensischen Untersuchung ... 6
4.1. Datensicherung ... 6
4.2. Datenextraktion ... 8
4.3. Datenanalyse ... 16
4.4. Zusammenfassung der Ergebnisse ... 25
5. Nachbetrachtung der Praktikumsarbeit ... 26
5.1. Beschreibung des Laboraufbaus ... 26
5.2. Untersuchung des eingesetzten Werkzeugs ... 27
5.3. Reflexion des Auswertungsprozesses ... 28
6. Literaturverzeichnis ... 30
7. Anhang ... 31
7.1. Scan des Single Evidence Forms ... 31
7.2. Scan des Chain of Custody Forms ... 33

1. Sachverhalt (Szenario)

Der Gastronomiebetrieb „Lila's Café" bietet seinen Gästen ein kostenfreies WLAN an. In den vergangenen Wochen meldeten sich mehrere Gäste beim Betreiber, dass es im Nachgang eines Besuchs in dem Café und der Nutzung des WLANs zu Account-Einbrüchen in Online-Plattformen und Sozialen Netzwerken gekommen sei.

Nach Gesprächen des Betreibers mit seinem Servicepersonal ergab sich ein Verdacht bzgl. eines jungen Mannes, der sich in den fraglichen Zeiträumen häufig im Café aufgehalten hatte und sich nach Wahrnehmung der Angestellten „auffällig" verhielt.

Als die fragliche Person das nächste Mal das Café aussuchte, stelle der Betreiber den Gast zur Rede. Das Gespräch entwickelte sich zu einer verbalen Auseinandersetzung, in deren Verlauf das Servicepersonal die Polizei verständigte.

Die eintreffenden Beamten entschieden nach einem Gespräch mit dem Gast, den Laptop, den dieser mit sich führte, sicherzustellen.

1.1. Einordnung des Vorfalls nach CERT Taxonomie

Der Vorfall wurde zunächst gemäß der CERT-Taxonomie klassifiziert (und im Laufe der Auswertung fortgeschrieben):

Angreifer	Werkzeuge	Schwach-stelle	Aktion	Ziel	Resultat	Absicht
Mitnutzer eines öffent-lichen WLANs	WLAN-Hotspot; Sniffing-Software	Unver-schlüsselte Übertra-gungen; ignorieren von Zertifikat-fehlern durch die Nutzer (Gäste)	MITM-Angriff mittels ARP-Spoofing	Abfangen von Credential Sets (Username / Passwort)	Angreifer gelangte in den Besitz von Zugangs-daten mehrerer Nutzer / Protokolle / Dienste	Hinweise auf beabsich-tigte Folgestraf-taten inner-halb oder außerhalb des Netzes

2. Strategische Vorbereitung

Eine Einflussnahme auf die strategische Vorbereitung z.B. auf Seiten des WLAN-Betreibers war nicht möglich, da die Einbeziehung der handelnden Personen erst im Rahmen der erkannten Angriffe erfolgt ist.

3. Operationale Vorbereitung

In dieser Phase werden die erforderlichen Voraussetzungen geprüft und die weiteren Schritte definiert.

Gemäß der eingangs beschriebenen Klassifizierung werden für die forensische Analyse folgende Ziele festgelegt:

a) Nachweis der Installation von Tools, die für die Durchführung eines MITM-Angriffs mit ARP-Spoofing geeignet sind
b) Ermittlung abgefangener Zugangsdaten
c) Dokumentation der von Beschuldigten besuchten Web-Seiten, soweit dies zur Klärung der Motivation und Intention des Betroffenen fallrelevant sein könnte
d) Feststellung von Kommunikation mit möglichen Mitwissern oder Mittätern zur Klärung der Motivation und Intention des Beschuldigten

3.1. Identifikation und Enumeration der Datenquellen

Das übergebene Gerät enthält eine physische Festplatte. Von dieser Festplatte wird ein vollständiges forensisches Abbild erstellt.

Sofern sich Hinweise auf die Übertragung von Zugangsdaten in Cloud-Speicher ergeben, werden von diesen, soweit der Zugriff gelingt, ebenfalls forensische Abbilder erzeugt.

3.2. Klärung der Ermächtigungsgrundlagen

Für den Kontext dieser Praktikumsaufgabe gehen wir davon aus, dass die handelnden Personen im Auftrag von Strafverfolgungsbehörden arbeiten und eine Befugnis gem. §202a/b im Auftrag vorliegt.

3.3. Klärung von Einwilligungen

Für den Kontext dieser Praktikumsaufgabe gehen wir davon aus, dass der Beschuldigte alle Einwilligungen erteilt hat, soweit dies rechtlich erforderlich sein sollte.

3.4. Identifikation & Auswahl geeigneter Werkzeuge und Verfahren

1. Als erste Maßnahme ist der Datenträger aus dem sichergestellten Gerät zu entnehmen und ein forensisches Abbild zu erstellen. Hierfür wird das Programm FTK Imager der Firma AccessData eingesetzt. Dieses Programm ist weltweit für die Erstellung forensischer Abbilder verbreitet. Zudem sind die handelnden Personen mit diesem Programm gut vertraut. Die Einzelschritte werden im nachfolgenden Auswertungsprotokoll beschrieben.
2. Unter Berücksichtigung der zu Beginn dieses Abschnitts beschriebenen Zielsetzung der Untersuchung haben die beteiligten Personen das forensische Analyse-Programm AXIOM ausgewählt. Dieses Programm wird weltweit in der forensischen Datenanalyse eingesetzt und die handelnden Personen sind mit seiner Anwendung gut vertraut.
   Im Einzelnen werden für die Analyse des Datenträgers folgende Maßnahmen festgelegt:
   - In einem ersten Schritt wird eine Timeline erstellt, um den fallrelevanten Zeitraum genauer eingrenzen zu können.
   - Für Punkt a) wird in den Betriebssystem-Artefakten nach Hinweisen auf Programme, die üblicherweise für MITM-Angriffe eingesetzt werden (z.B. „Cain&Abel“ oder „Ettercap“), gesucht.
   - Für den Punkt b) wird eine Volltextsuche mit einer geeigneten Schlagwortliste („Passwort“, „Credential“, „Login“ etc.) durchgeführt. Zudem ist bekannt, dass eine der betroffenen Personen den Login-Namen „avictim“ nutzte, so dass auch nach dieser

Zeichenkette gezielt gesucht werden kann. Sollten sich hier Treffer ergeben, ist im unmittelbaren Umfeld nach weiteren potenziellen Zugangsdaten zu suchen.

- Für den Punkt c) wird analysiert, welche Web-Browser verwendet wurden und ob hier Seitenverläufe vorhanden oder wiederherstellbar sind. Aus diesen Seitenverläufen sollen fallrelevante Seitenzugriffe dokumentiert werden, d.h. Zugriffe auf Seiten, die Hinweise zur Planung & Durchführung sowie zu Motivation und Intention des Beschuldigten geben können
- Für den Punkt d) wird geprüft, ob Kommunikation des Beschuldigten per Mail oder Chat vorhanden oder wiederherstellbar ist. Ggf. fallrelevante Kommunikation, die Informationen zu Mittätern oder Mitwisser bzw. zu Motivation und Intention des Beschuldigten geben können, sollten dokumentiert werden.

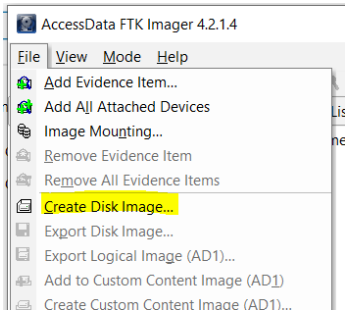
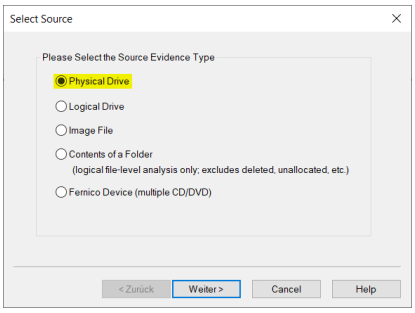
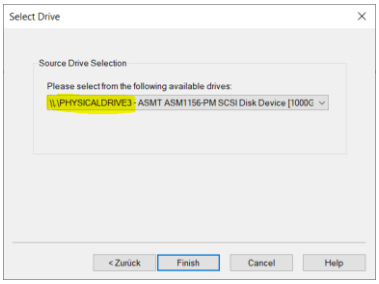
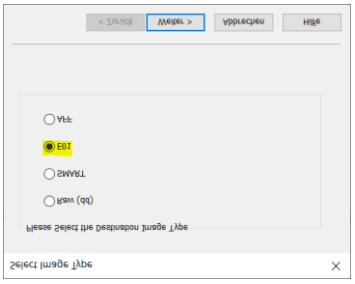
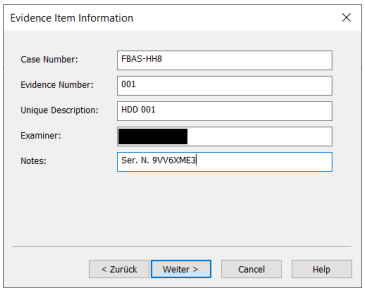
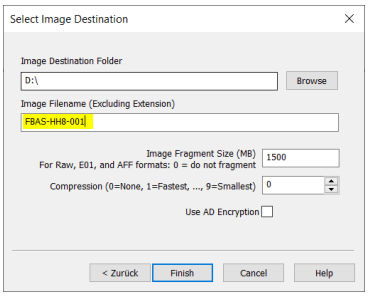
3. Sofern sich im Rahmen der Auswertung Hinweise auf weitere, potenziell fallrelevante Datenquellen (insbesondere Cloud-Speicher) ergeben, sollen auch für diese Datenquellen, soweit möglich und zulässig, die unter Punkt 2) genannten Maßnahmen ergriffen werden.

4. Dokumentation der forensischen Untersuchung

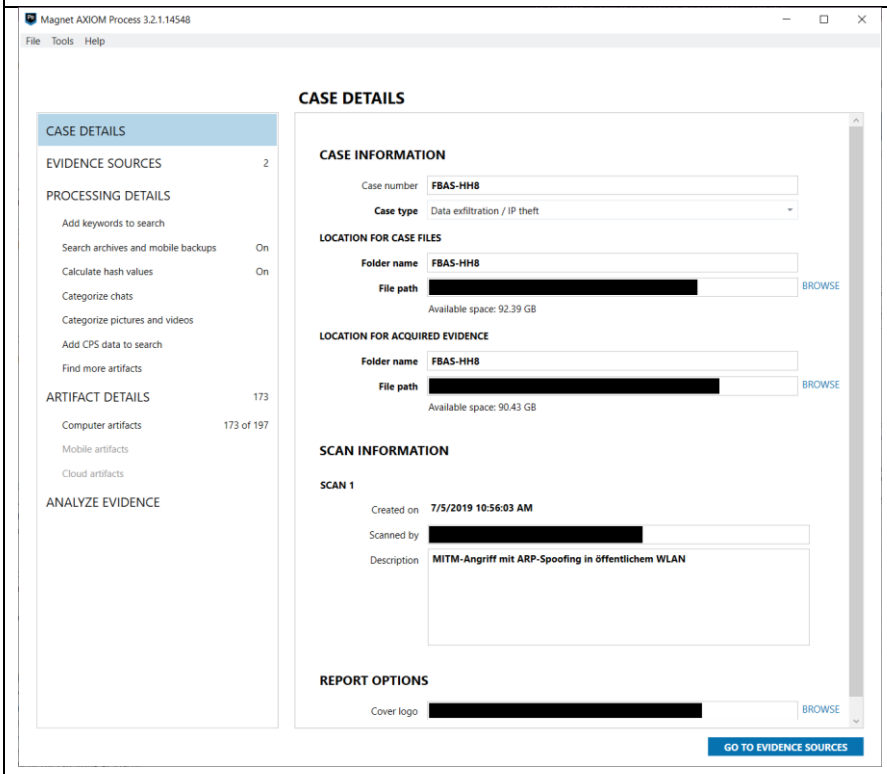
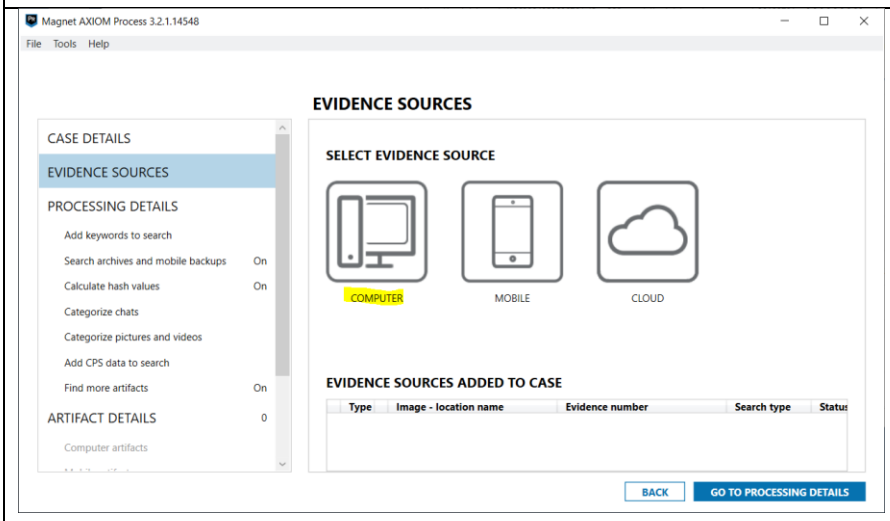
4.1. Datensicherung

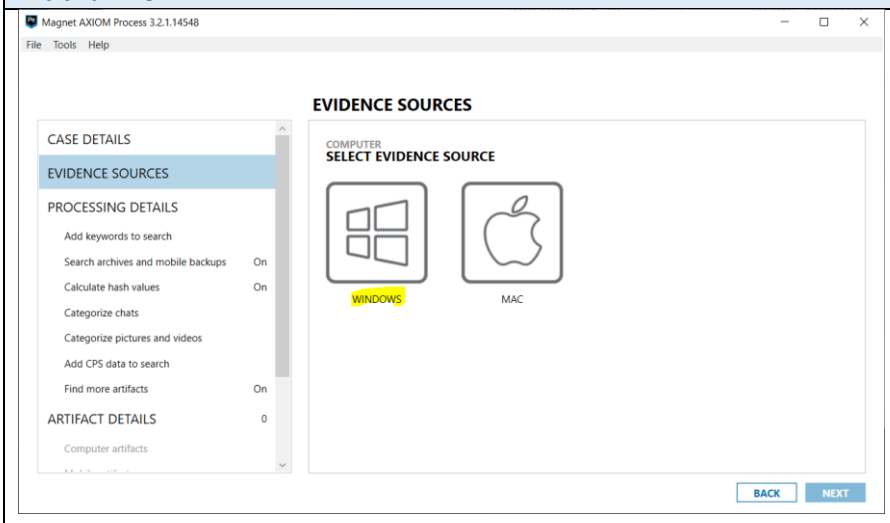
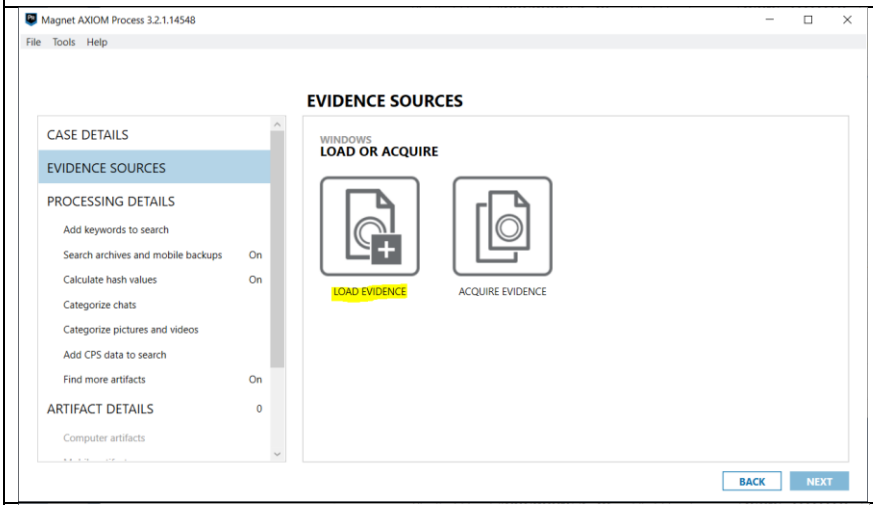
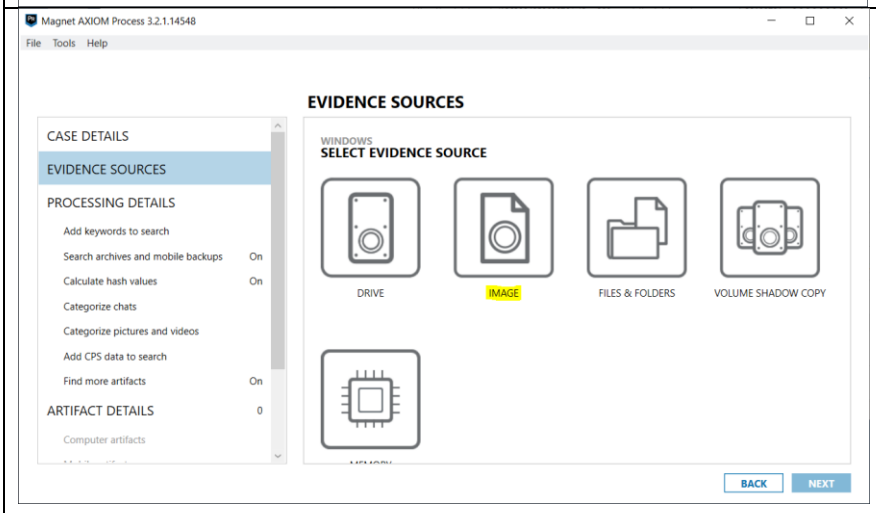
Für die Erstellung des forensischen Abbilds wird das bewährte Programm „FTK Imager“ benutzt, das bei vielen IT-forensischen Dienststellen weltweit im Einsatz ist.

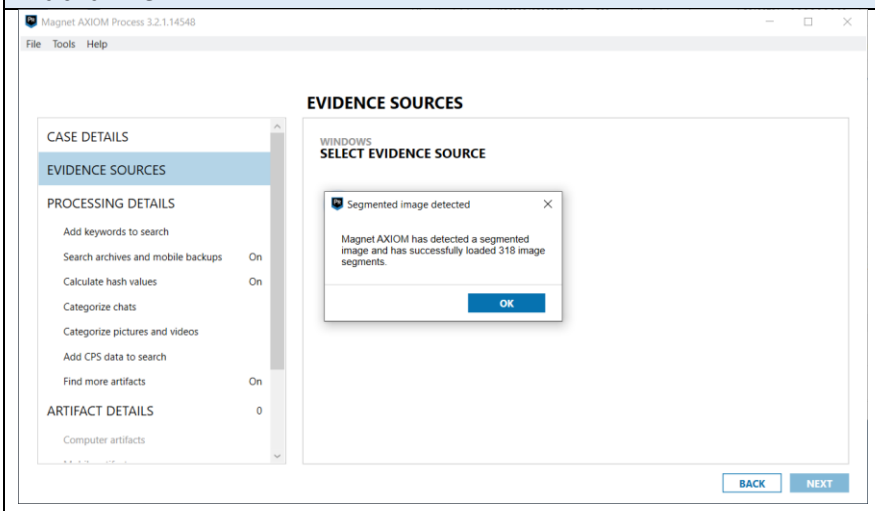
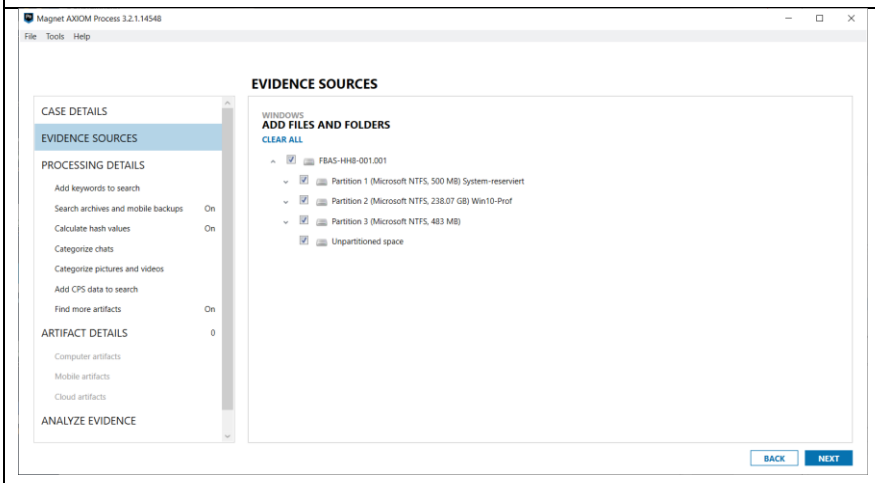
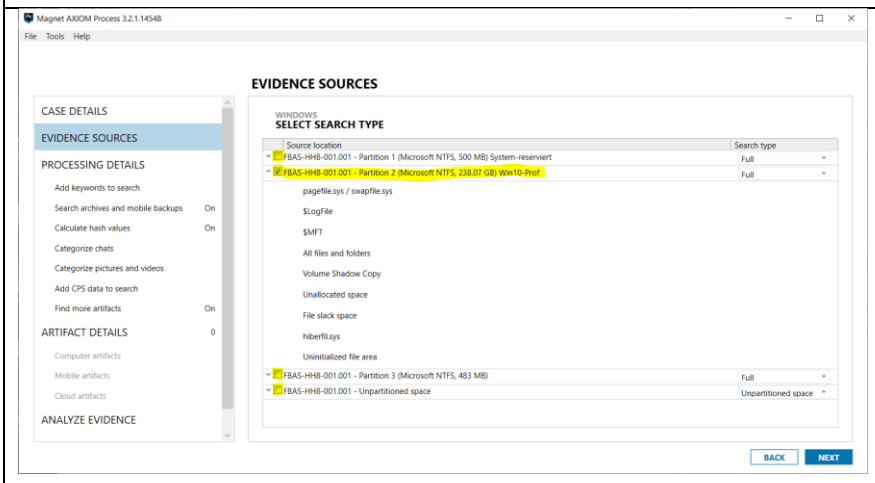
Maßnahme	Ausführung	Zeuge
Die Festplatte wurde aus dem Gerät des Beschuldigten ausgebaut. Es handelt sich um eine Festplatte Seagate Pipeline HD.2 P/N 9GW132-194 Ser.No. 9VV6XME3. 	<Autor C>	<Autor B>

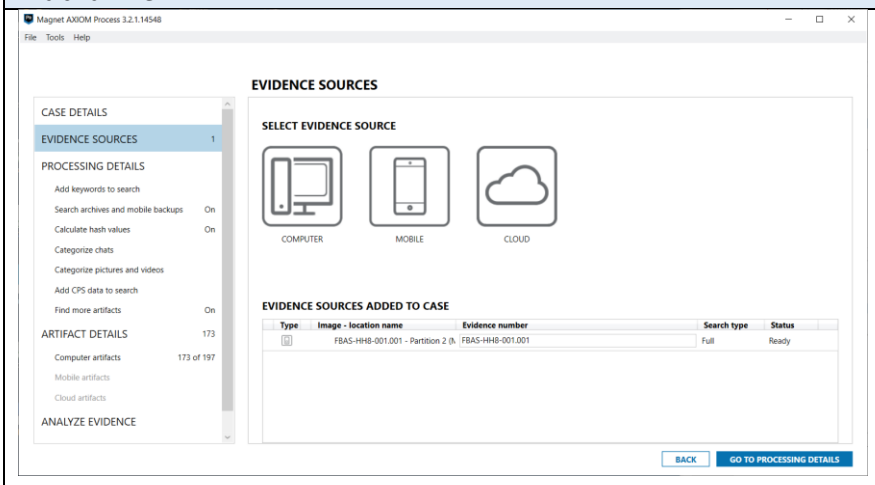
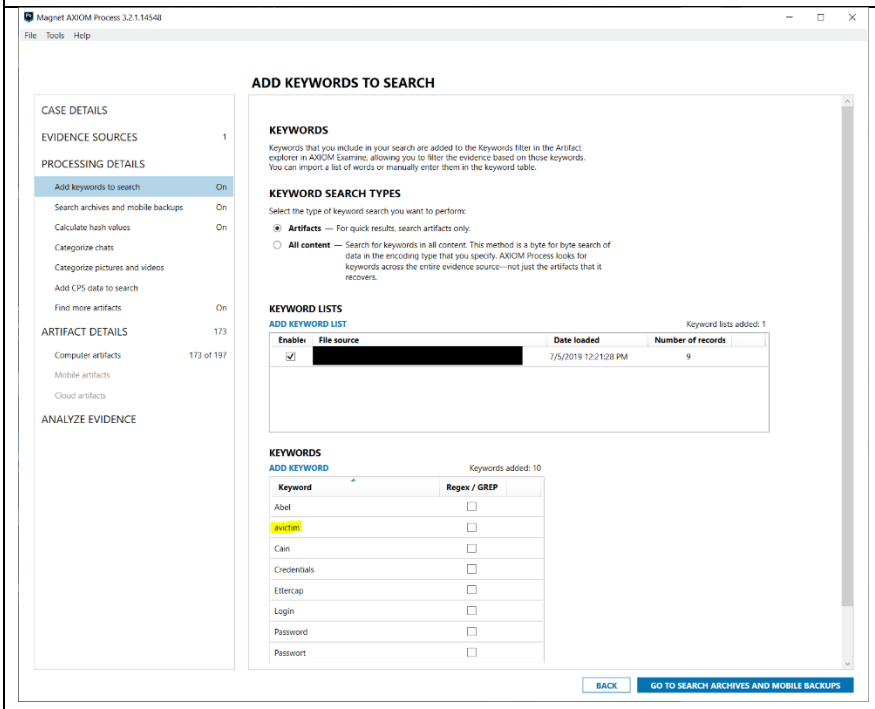
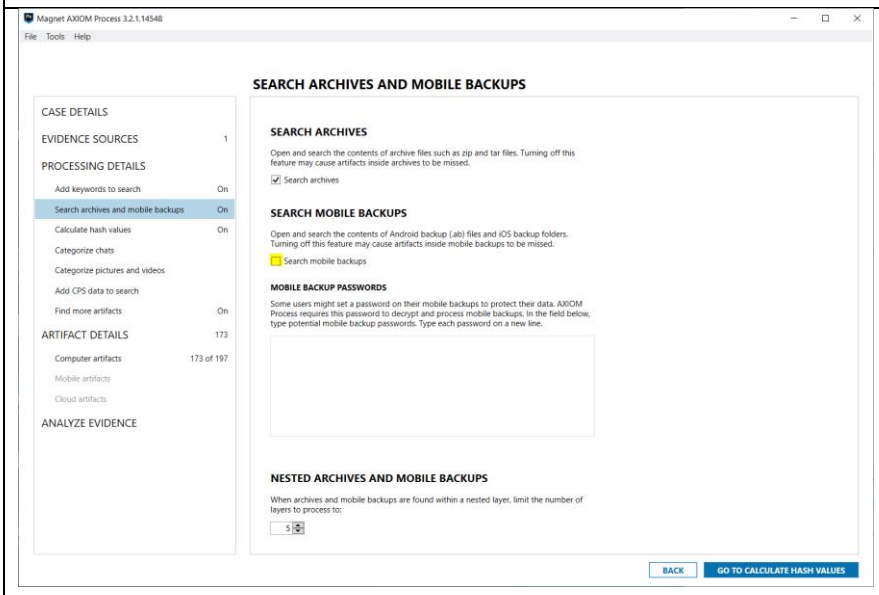
Maßnahme	Ausführung	Zeuge
Es wurde ein forensisches Abbild der Festplatte im E01-Format erstellt: Programm: AccessData FTK Imager Version: 4.2.14       Hierbei wurde eine forensische Kopierstation mit Write-Blocker verwendet: Hersteller: ACME Inc. Modell: 08/15 Inventarnummer: #463811	<Autor C>	<Autor A>
Es wurde ein „Single Evidence Form“ für das Beweismittel 001 angelegt (siehe Anhang)	<Autor C>	<Autor A>
Der Originaldatenträger wurde in einen Sealbag verpackt und im Asservaten-Tresor 3 verwahrt.	<Autor C>	<Autor A>

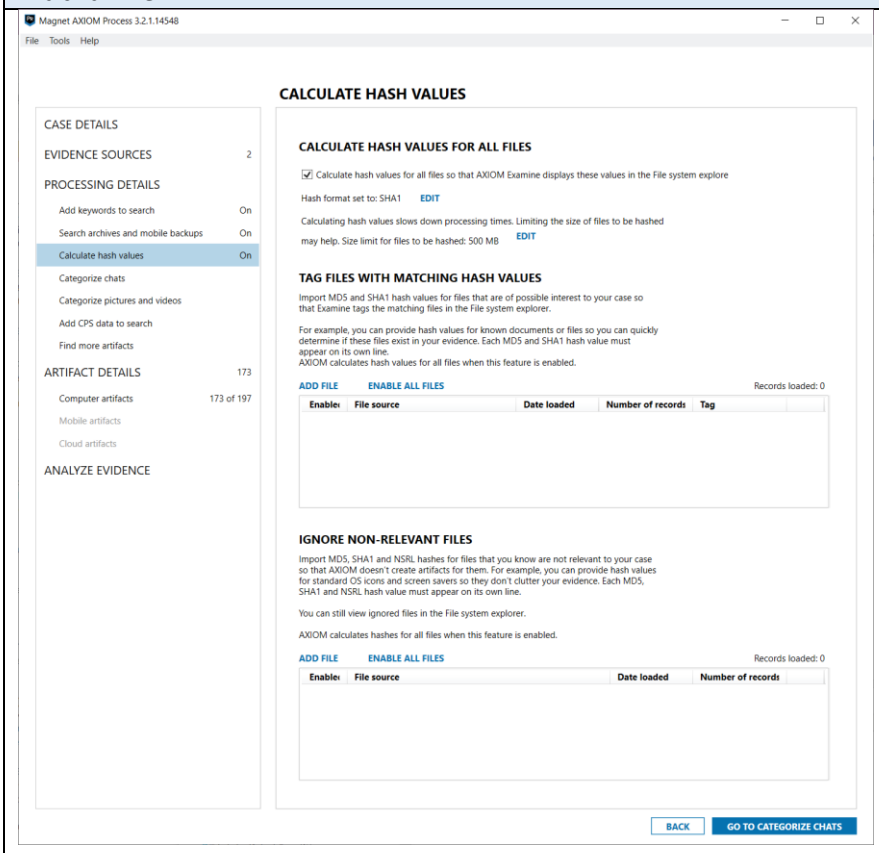
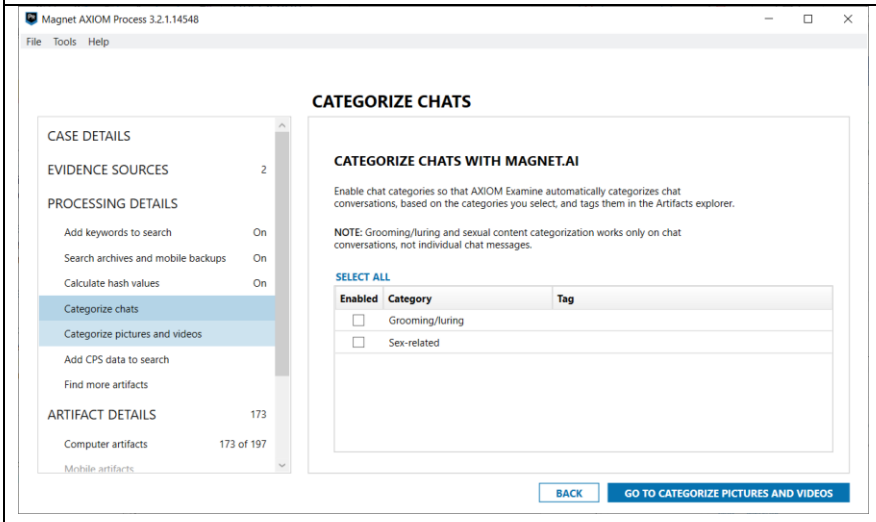
4.2. Datenextraktion

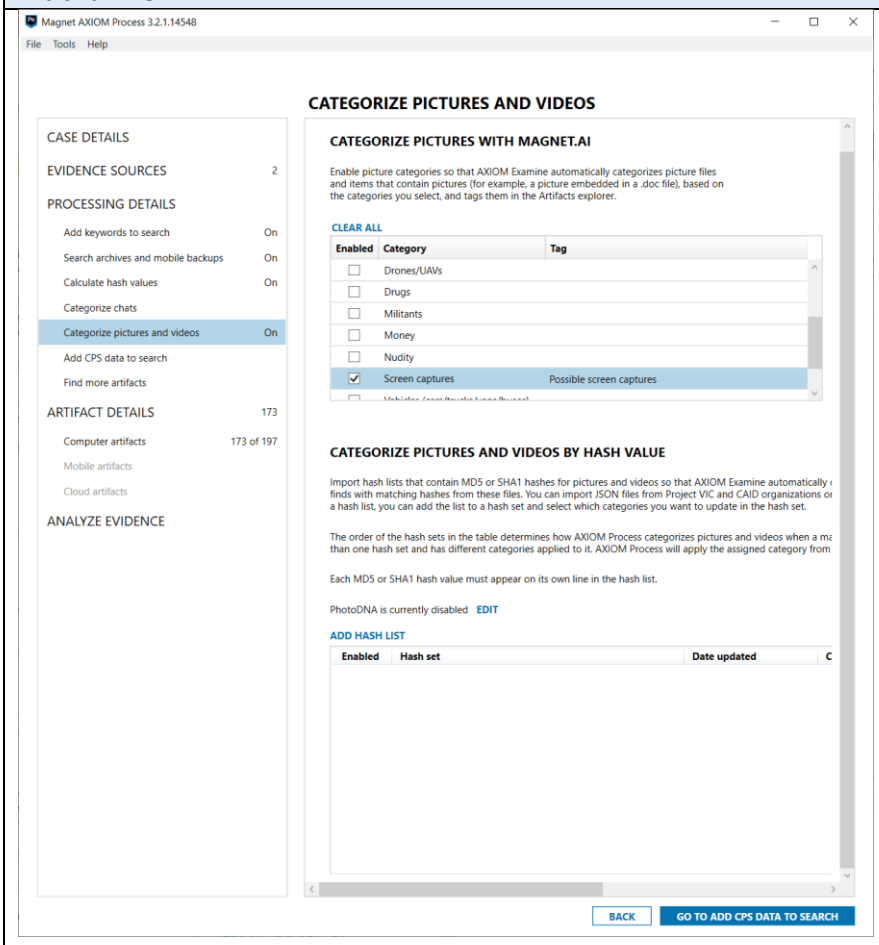
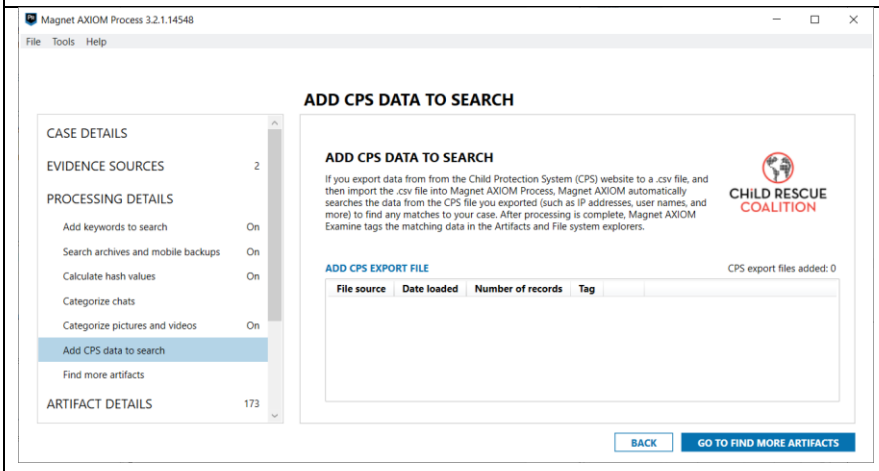
Maßnahme	Ausführung	Zeuge
Das forensische Abbild (physischer Datenträger) wurde mit dem Analyse-Arbeitsplatz verbunden.	<Autor B>	<Autor A>
Im Programm AXIOM Process wurde ein neuer Fall angelegt: Programm: Magnet AXIOM Process Version: 3.2.1.1458	<Autor B>	<Autor A>
	<Autor A>	<Autor C>
	<Autor A>	<Autor C>

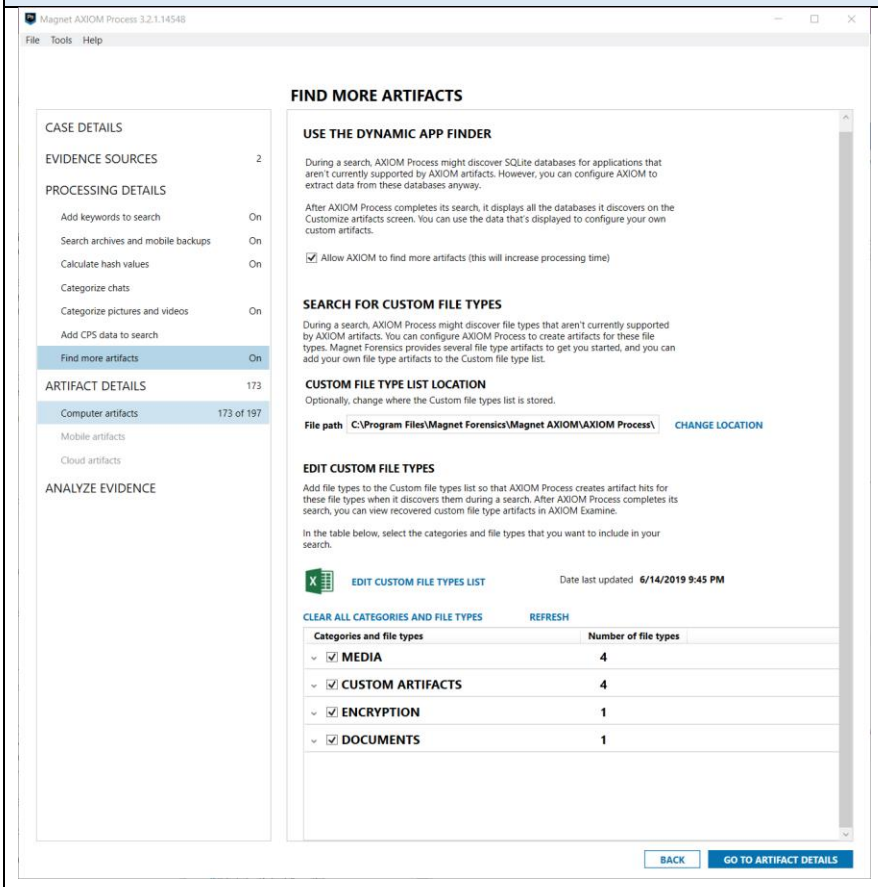
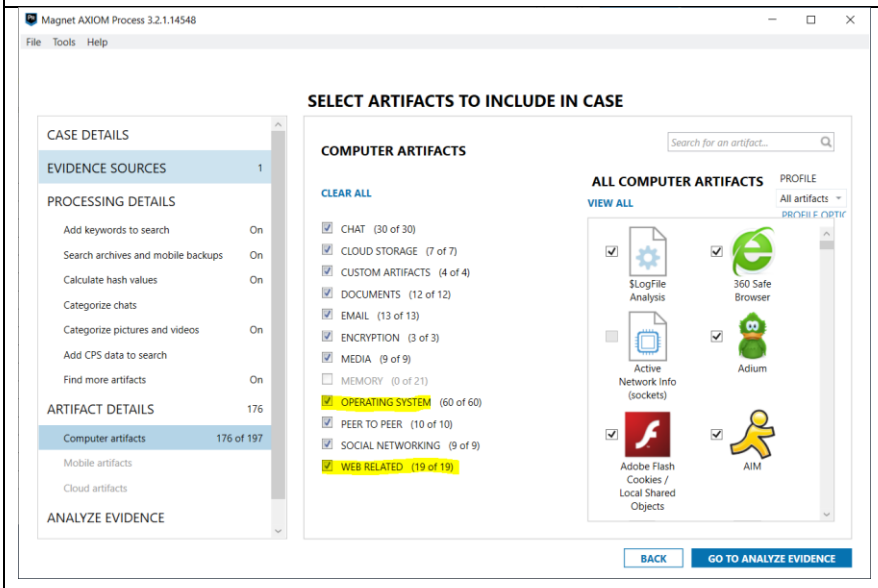
Maßnahme	Ausführung	Zeuge
	<Autor A>	<Autor C>
	<Autor A>	<Autor C>
	<Autor A>	<Autor C>

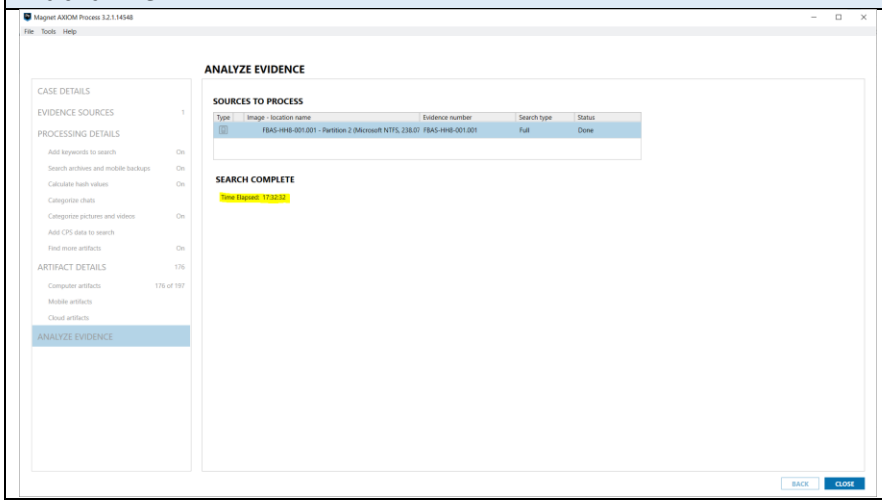
Maßnahme	Ausführung	Zeuge
	<Autor A>	<Autor C>
	<Autor A>	<Autor C>
	<Autor A>	<Autor C>

Maßnahme	Ausführung	Zeuge
	<Autor A>	<Autor C>
	<Autor A>	<Autor C>
	<Autor A>	<Autor C>

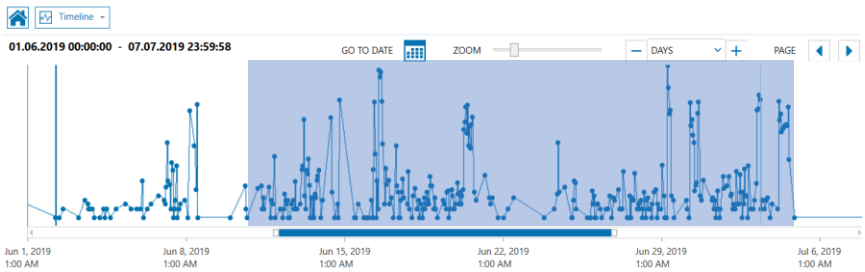
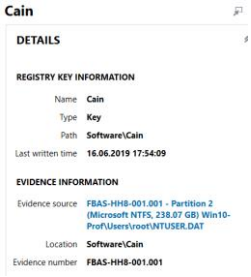
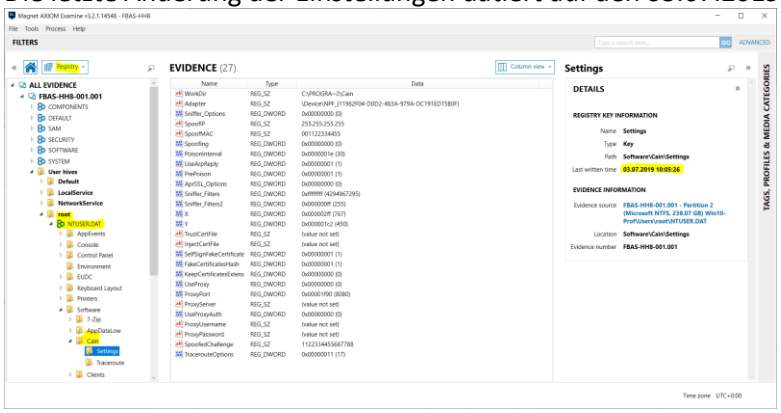
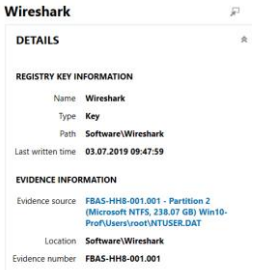
Maßnahme	Ausführung	Zeuge
	<Autor A>	<Autor C>
	<Autor A>	<Autor C>

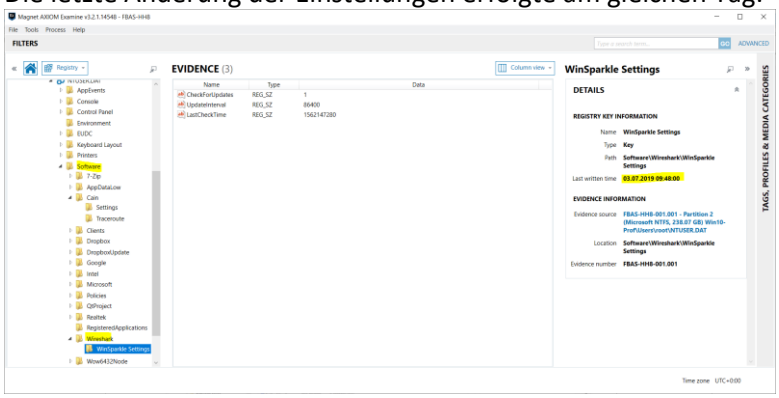
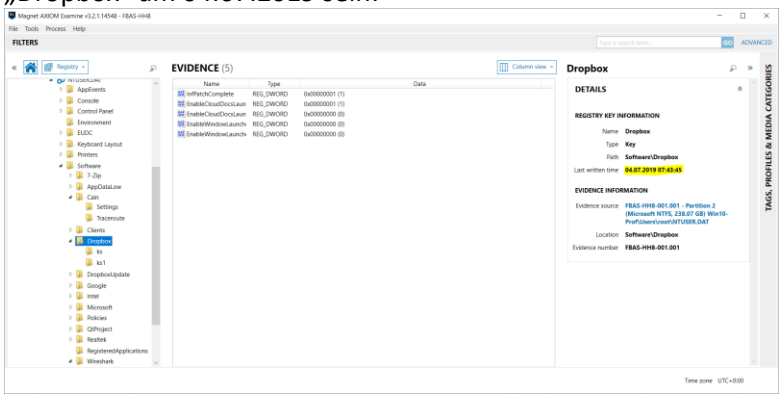
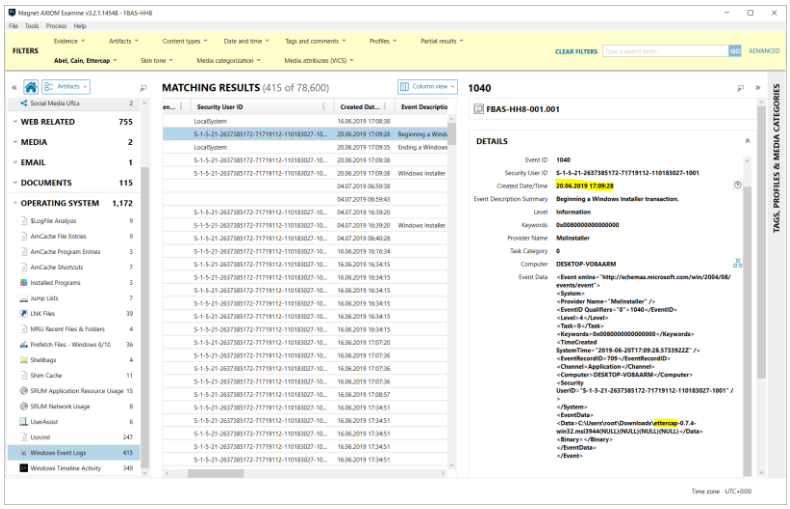
Maßnahme	Ausführung	Zeuge
	<Autor A>	<Autor C>
	<Autor A>	<Autor C>

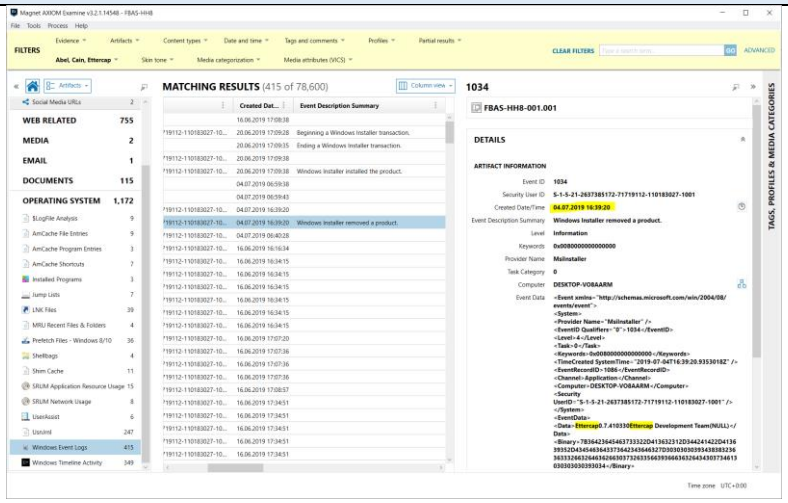
Maßnahme	Ausführung	Zeuge
	<Autor A>	<Autor C>
	<Autor A>	<Autor C>

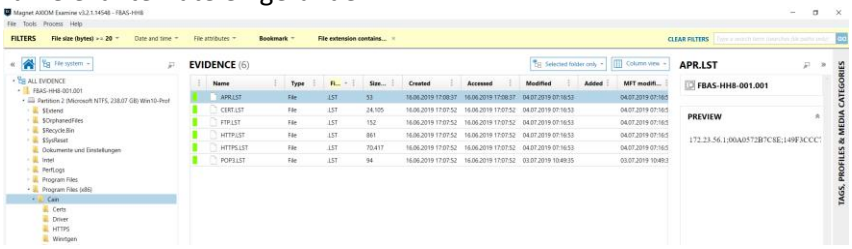
Maßnahme	Ausführung	Zeuge
	<Autor A>	<Autor C>

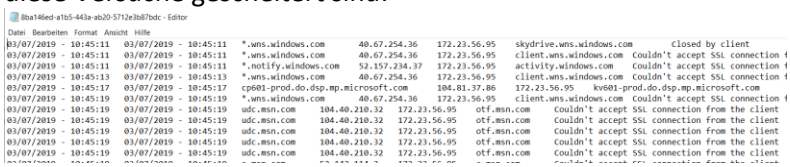
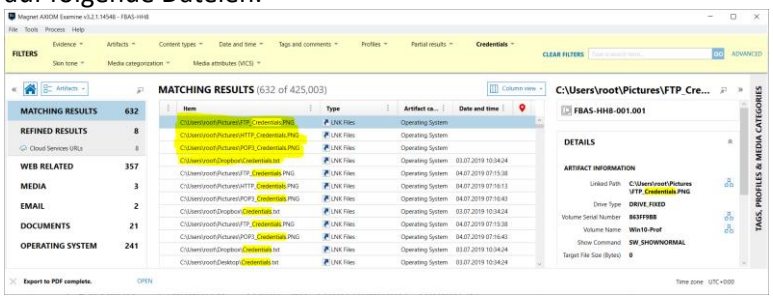
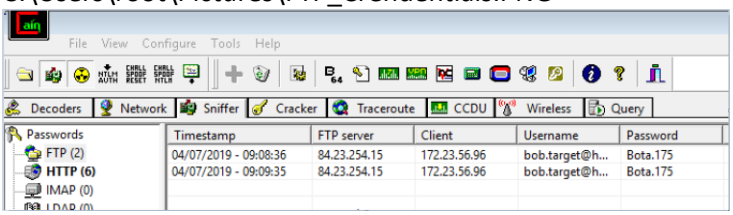
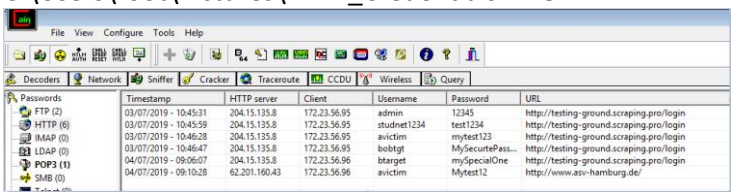
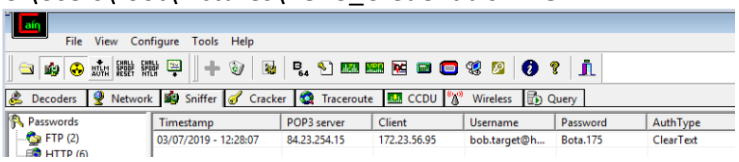
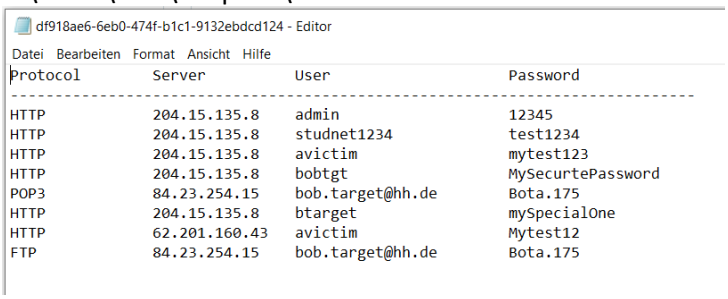
4.3. Datenanalyse

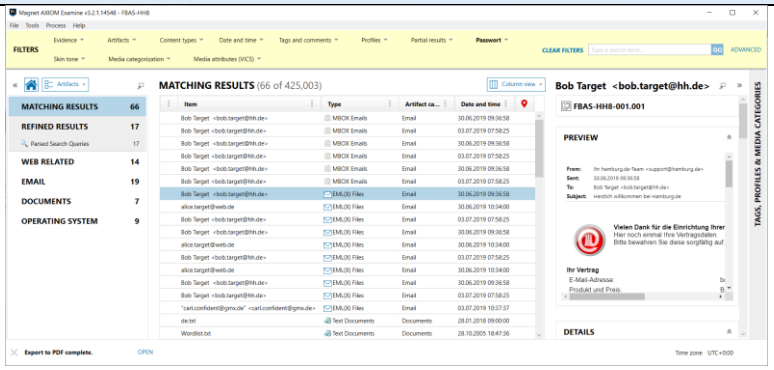
Maßnahme	Ausführung	Zeuge
Die Analyse wurde mit AXIOM Examine durchgeführt: Programm: Magnet Axiom Examine Version: 3.2.1.14548	<Autor A>	<Autor B>
<u>Erstellung und Auswertung der Timeline</u>  Die Untersuchung der Timeline ergab, dass ein Zeitfenster in etwa vom 10. Juni bis zum 4. Juli fallrelevant sein dürfte.	<Autor A>	<Autor B>
a) Nachweis der Installation von Tools, die für die Durchführung eines MITM-Angriffs mit ARP-Spoofing geeignet sind.		
<u>Prüfung der Registry-Einträge</u> • Unter der Kennung „root“ wurde die Software „Cain&Abel“ registriert; die Installation erfolgte (letztmalig) am 16.06.2019:  Die letzte Änderung der Einstellungen datiert auf den 03.07.2019:  • Unter der Kennung „root“ wurde die Software „Wireshark“ registriert; die Installation erfolgte (letztmalig) am 03.07.2019:  	<Autor B>	<Autor A>

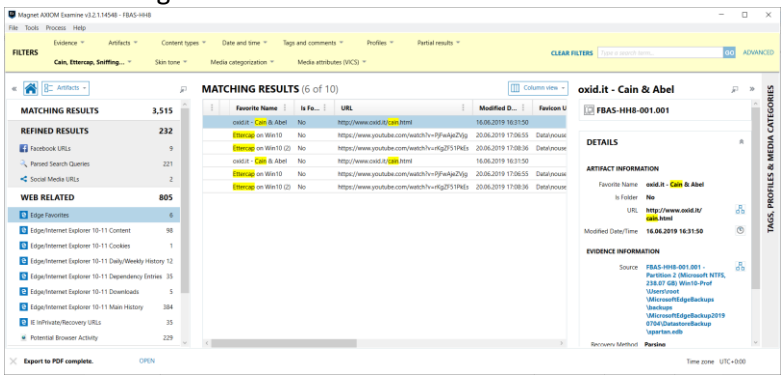
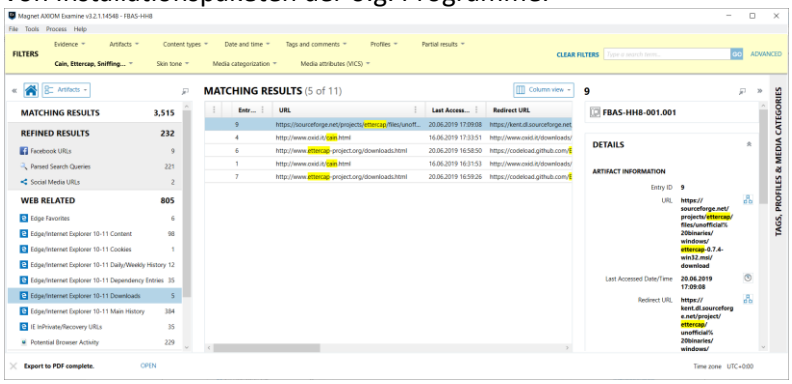
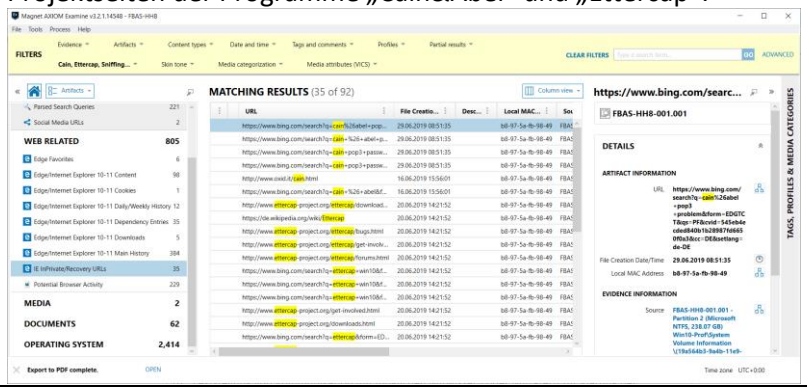
Maßnahme	Ausführung	Zeuge
Die letzte Änderung der Einstellungen erfolgte am gleichen Tag:  • Von Interesse für die weitere Untersuchung könnte auch die Installation der Client-Software des Cloud-Speicherdienstes „Dropbox“ am 04.07.2019 sein:  Es wird entschieden, nach weiteren Spuren (Zugangsdaten oder Offline-Kopien der im Cloud-Dienst gespeicherten Dateien) zu suchen.		
<u>Suche nach fallrelevanter Software im Windows Event Log:</u> • Am 20.06.2019 wurde die Software „Ettercap“ in der Version 0.7.4 installiert:  • Am 04.07.2019 wurde die vorgenannte Software „Ettercap“ wieder deinstalliert:	<Autor B>	<Autor A>

Maßnahme	Ausführung	Zeuge
		

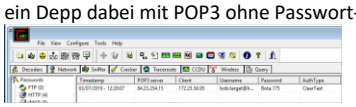
Maßnahme	Ausführung	Zeuge
b) Ermittlung abgefangener Zugangsdaten		
<u>Suche in Logfiles des Programms „Cain&Abel“</u> Nachdem die Installation des Programms „Cain&Abel“ festgestellt werden konnte - siehe Punkt a) – wurde im Installationspfad des Programms nach nicht-leeren sog. LST-Dateien gesucht, in denen dieses Programm ausgespähte Zugangsdaten protokolliert. Es wurden folgende fallrelevante Dateien gefunden:  Aus diesen Dateien lassen sich im einzelnen folgende Vorgänge nachweisen: • Aus der Datei „ARP.LST“ lässt sich ableiten, dass ein ARP-Spoofing-Angriff auf die Netzwerkverbindung zwischen den IP-Adressen 172.23.56.1 (Gateway) und 172.23.56.95 bzw. 172.23.56.96 (Angriffsziel im WLAN) erfolgte: 24e1bbad-23c3-4150-86f7-ff67ec2f9f9f - Editor Datei Bearbeiten Format Ansicht Hilfe 172.23.56.1;00A0572B7C8E;149F3CCC7852;172.23.56.96; • Aus der Datei POP3.LST ist zu entnehmen, dass die Zugangsdaten im POP3-Protokoll für ein E-Mail-Postfach abgefangen wurden: 58857696-73e2-4a0b-ba83-ecd7394f0aaf - Editor Datei Bearbeiten Format Ansicht Hilfe 03/07/2019 - 12:28:07 84.23.254.15 172.23.56.95 bob.target@hh.de Bota.175 • Die Datei FTP.LST liefert den Beleg, dass darüber hinaus ein Satz von Zugangsdaten im FTP-Protokoll abgefangen wurde: a4050830-6270-4b63-9c85-89f1c85a6150 - Editor Datei Bearbeiten Format Ansicht Hilfe 04/07/2019 - 09:08:36 84.23.254.15 172.23.56.96 bob.target@hh.de Bota.175 • Die Datei HTTP.LST belegt, dass mindestens sechs Login/Passwort-Kombinationen im http-Protokoll abgefangen wurden: e5fbf6d0-9b48-4745-8a0c-6580e6d3ef5f - Editor Datei Bearbeiten Format Ansicht Hilfe 03/07/2019 - 10:45:31 204.15.135.8 172.23.56.95 admin 12345 http://testing-gr 03/07/2019 - 10:45:59 204.15.135.8 172.23.56.95 studnet1234 test1234 h 03/07/2019 - 10:46:28 204.15.135.8 172.23.56.95 avictim mytest123 http://te 03/07/2019 - 10:46:47 204.15.135.8 172.23.56.95 bobtgt MySecurtePassword h 04/07/2019 - 09:06:07 204.15.135.8 172.23.56.96 btarget mySpecialOne http://te 04/07/2019 - 09:10:28 62.201.160.43 172.23.56.96 avictim Mytest12 http://ww • Aus der Datei CERT.LST ist zu erkennen, dass auch der Versuch unternommen wurde, HTTPS-Verbindungen mittels gefälschter Zertifikate zu brechen: 9d0d1245-9bca-4b17-97d3-9dad929e4522 - Editor Datei Bearbeiten Format Ansicht Hilfe C:\PROGRA~2\Cain\Certs\self_signed_198.199.88.104.crt;198.199.88.104;443;1.na.dl.wireshark.org; C:\PROGRA~2\Cain\Certs\self_signed_35.190.7.190.crt;35.190.7.190;443;*.lqm.io; C:\PROGRA~2\Cain\Certs\self_signed_185.33.223.197.crt;185.33.223.197;443;*.adnxs.com; C:\PROGRA~2\Cain\Certs\self_signed_216.58.206.2.crt;216.58.206.2;443;*.g.doubleclick.net; C:\PROGRA~2\Cain\Certs\self_signed_52.114.128.38.crt;52.114.128.38;443;prod.registrar.skype.com; C:\PROGRA~2\Cain\Certs\self_signed_104.25.175.13.crt;104.25.175.13;443;ssl379341.cloudflaressl.com; C:\PROGRA~2\Cain\Certs\self_signed_104.74.99.96.crt;104.74.99.96;443;cp501-prod.do.dsp.mp.microsoft.com; C:\PROGRA~2\Cain\Certs\self_signed_13.107.3.254.crt;13.107.3.254;443;*.msedge.net; C:\PROGRA~2\Cain\Certs\self_signed_185.33.223.215.crt;185.33.223.215;443;*.adnxs.com; C:\PROGRA~2\Cain\Certs\self_signed_104.74.77.232.crt;104.74.77.232;443;secure-ds.serving-sys.com; C:\PROGRA~2\Cain\Certs\self_signed_104.81.33.217.crt;104.81.33.217;443;www.norton.com;	<Autor C>	<Autor B>

Maßnahme	Ausführung	Zeuge
• Der Inhalt der Datei HTTPS.LST legen jedoch den Schluss nahe, dass diese Versuche gescheitert sind: 		
<u>Schlüsselwort-Suche in der Artefakt-Sicht:</u> • Die Suche nach dem Schlüsselwort „Credentials“ lieferte Hinweise auf folgende Dateien:  ○ C:\Users\root\Pictures\FTP_Crendentials.PNG  ○ C:\Users\root\Pictures\HTTP_Credentials.PNG  ○ C:\Users\root\Pictures\POP3_Credentials.PNG  ○ C:\Users\root\Dropbox\Credentials.txt  df918ae6-6eb0-474f-b1c1-9132ebdcd124 - Editor Datei Bearbeiten Format Ansicht Hilfe Protocol Server User Password --- HTTP 204.15.135.8 admin 12345 HTTP 204.15.135.8 studnet1234 test1234 HTTP 204.15.135.8 avictim mytest123 HTTP 204.15.135.8 bobtgt MySecurtePassword POP3 84.23.254.15 bob.target@hh.de Bota.175 HTTP 204.15.135.8 btarget mySpecialOne HTTP 62.201.160.43 avictim Mytest12 FTP 84.23.254.15 bob.target@hh.de Bota.175 • Die Suche nach dem Schlüsselwort „Passwort“ lieferte Hinweise auf eine Reihe von E-Mail-Adressen:	<Autor C>	<Autor B>

Maßnahme	Ausführung	Zeuge
 Es wird entschieden, diese E-Mail-Adressen unter Punkt d) weiter zu untersuchen. • Die Suche nach dem Schlüsselwort „avictim“ lieferte erneut einen Hinweis auf die bereits oben identifizierte, fallrelevante Datei ○ C:\Users\root\Dropbox\Credentials.txt • Die weiteren Schlagworte lieferten keine fallrelevanten Ergebnisse.		

Maßnahme	Ausführung	Zeuge
c) Dokumentation der von Beschuldigten besuchten Web-Seiten, soweit dies zur Klärung der Motivation und Intention des Betroffenen fallrelevant sein könnte		
<u>Schlüsselwort-Suche im Abschnitt „Web-Related“ der Artefakt-Sicht:</u> • Die Suche nach den Schlüsselworten „Abel“, „Ettercap“, „Sniffing“ und „WLAN“ in den Favoriten ergab mehrere Verweise auf Youtube-Videos mit Tutorials zur Anwendung der o.g. Programme zur Durchführung von MITM-Attacken:  • Die Suche nach den Schlüsselworten „Abel“, „Ettercap“, „Sniffing“ und „WLAN“ in den Downloads ergab Hinweise auf den Download von Installationspaketen der o.g. Programme:  • Die Suche nach den Schlüsselworten „Abel“, „Ettercap“, „Sniffing“ und „WLAN“ in den Browser-Historie ergab Hinweise auf die Verwendung dieser Begriffe auf Suchseiten sowie den Besuch der Projektseiten der Programme „Cain&Abel“ und „Ettercap“: 	<Autor B>	<Autor A>

Maßnahme	Ausführung	Zeuge
d) Feststellung von Kommunikation mit möglichen Mitwissern oder Mittätern zur Klärung der Motivation und Intention des Beschuldigten		
<u>Suche nach fallrelevanten Email-Kommunikationen in der Artefakt-Sicht:</u> Im Offline-Mail-Client des Beschuldigten wurde eine fallrelevante Kommunikation mit der Adresse carl.confident@gmx.de identifiziert:	<Autor A>	<Autor C>

Hallo Carl, ich habe für unser Vorhaben einen neuen Rechner aufgesetzt und ein neues E-Mail-Konto eingerichtet. Bin mal gespannt, wie das anläuft! Gruß Eve	**From:** <eve.attacker@gmx.de> **Sent:** 30.06.2019 09:00:35 **To:** <carl.confident@gmx.de> **Subject:** Neue E-Mail
From: <carl.confident@gmx.de> **Sent:** 30.06.2019 09:01:25 **To:** <eve.attacker@gmx.de> **Subject:** Neue E-Mail	Hallo Eve, Danke für die Info. Das wird bestimmt spannent. Vielleicht können wir auch ein paar Euros damit machen. Gruß Carl
Hi Carl, habe heute im LiLa Café einiges sniffen können. War sogar ein Depp dabei mit POP3 ohne Passwort-Verschlüsselung:  Da habe ich doch gleich mal sein Postfach abgegriffen ☺ Lege ich alles am bekannten Ort ab. Gruß Eve	**From:** <eve.attacker@gmx.de> **Sent:** 03.07.2019 10:37:37 **To:** <carl.confident@gmx.de> **Subject:** Ausbeute des Tages
Hi Carl, schau mal in die letzte Mail von dem Bob Target! … jetzt müssen wir nur noch herausfinden, wo er und diese Tussi, die ihm geschrieben hat, arbeiten!!! Gruß Eve	**From:** <eve.attacker@gmx.de> **Sent:** 03.07.2019 10:51:45 **To:** <carl.confident@gmx.de> **Subject:** Goldstaub!
From: <carl.confident@gmx.de> **Sent:** 03.07.2019 21:32:51 **To:** <eve.attacker@gmx.de> **Subject:** Goldstaub!	Hi Eve, schau doch mal, ob du morgen im Lila's jemanden wiedererkennst. Dann kannst du ihm ja mal nachgehen. Vielleicht arbeitet er "um die Ecke" und macht dort seine Mittagspause... Wir telefonieren morgen! Carl
Hi Carl, heute ist nicht viel los im LiLa's. Der Typ von gestern ist noch nicht wieder aufgetaucht. Hab noch ein paar Crendentials gesnifft – ist auch ein FTP-Login dabei! Gruß Eve	**From:** <eve.attacker@gmx.de> **Sent:** 04.07.2019 07:19:13 **To:** <carl.confident@gmx.de> **Subject:** Update
From: <carl.confident@gmx.de> **Sent:** 04.07.2019 16:36:05 **To:** <eve.attacker@gmx.de> **Subject:** Update	Hi Eve, alles klar – ich schau mir mal an, was wir aus den FTP-Credentials machen können. Gruß Carl
Hi Carl, alles klar! Melde mich morgen wieder… Eve	**From:** <eve.attacker@gmx.de> **Sent:** 04.07.2019 16:36:59 **To:** <carl.confident@gmx.de> **Subject:** Update

Dem Austausch zwischen dem Beschuldigten und dem mutmaßlichen Mitwisser/Mittäter ist zu entnehmen, dass die abgefangenen Informationen zur Vorbereitung weiterer strafbarer Handlungen dienten.

Maßnahme	Ausführung	Zeuge
• Zudem wurde offenbar der komplette Inhalt des WebMail-Kontos eines Betroffenen, dessen POP3-Passwort abgefangen wurde, auf die Festplatte des Betroffenen exportiert: **From:** <alice.victim@gmx.de> **Sent:** 03.07.2019 08:09:16 **To:** <bob.target@hh.de> **Subject:** Hallo Bob T Hi Bob, sehe du bist jetzt bei Hamburg.de? Gruß Alice **From:** <alice.victim@gmx.de> **Sent:** 03.07.2019 08:50:48 **To:** <bob.target@hh.de> **Subject:** Mantel mitbringen Hallo Bob, ich habe meinen Mantel im Büro vergessen. Kannst mir den bitte mitbringen? Der Türcode ist "37644#". Danke Alice Es gibt Querbeziehungen zwischen der Kommunikation in diesem Ordner und der Kommunikation zwischen dem Beschuldigten und dem mutmaßlichem Mitwisser/Mittäter carl.confident@gmx.de <u>Suche nach fallrelevanten Chat-Kommunikationen in der Artefakt-Sicht:</u> • Es wurden keine fallrelevanten Chats auf dem sichergestellten Rechner nachgewiesen. <u>Suche nach fallrelevanten Messenger-Nachrichten in der Artefakt-Sicht:</u> • Es konnten keine fallrelevanten Messenger-Nachrichten auf dem sichergestellten Rechner nachgewiesen werden.		

4.4. Zusammenfassung der Ergebnisse

Die während der Operationalen Vorbereitung festgelegten Untersuchungsziele der forensischen Analyse konnten vollumfänglich erreicht werden:

a) **Nachweis der Installation von Tools, die für die Durchführung eines MITM-Angriffs mit ARP-Spoofing geeignet sind**
Auf dem Rechner des Beschuldigten waren die Programme „Cain&Abel“ und „Wireshark“ installiert, die beide regelmäßig im Zuge von MITM-Angriffen genutzt werden. Darüber hinaus konnte anhand von Registry-Einträgen belegt werden, dass das ebenfalls für MITM-Angriffe genutzte Programm Ettercap im fallrelevanten Zeitraum auf dem Gerät installiert war, jedoch bereits vor dessen Sicherstellung wieder deinstalliert wurde.
Durch Auswertung von programmeigenen Protokolldateien der Anwendung „Cain&Abel“, die auf dem Rechner des Beschuldigten festgestellt wurden, konnte zudem eindeutig belegt werden, dass dieses Programm zum Abfangen von Zugangsdaten im HTTP-, FTP- und POP3-Protokoll genutzt wurde. Angriffe auf das HTTPS-Protokoll waren, soweit nachvollziehbar, nicht erfolgreich.

b) **Ermittlung abgefangener Zugangsdaten**
Es konnten an verschiedenen Stellen Listen von abgefangenen Zugangsdaten festgestellt werden. Hierbei handelt es sich einerseits um manuelle Aufzeichnungen des Nutzers und andererseits um Protokolldateien des eingesetzten Programms. Die Daten dieser Listen stimmen inhaltlich überein.
Bei den Zugangsdaten im POP3-Protokoll steht eine vollständige E-Mail-Adresse zur Verfügung, so dass die betroffene Person über den Vorfall informiert werden kann, um durch den Wechsel des Passworts die Sicherheit des Postfachs wiederherzustellen.
Da es sich bei den übrigen Zugangsdaten nur um einfache Login-Namen in Verbindung mit einem Passwort handelt, können die Personen nicht direkt kontaktiert werden. In diesen Fällen müssten die Kontaktdaten zunächst vom Betreiber der jeweiligen Web-Dienste (URLs sind bekannt) anhand des Login-Namens ermittelt werden.

c) **Dokumentation der vom Beschuldigten besuchten Web-Seiten, soweit dies zur Klärung der Motivation und Intention des Betroffenen fallrelevant sein könnte**
Es konnten umfassende Belege für die Suche nach Tutorials und ergänzenden Hinweisen zur Durchführung von MITM-Angriffen mit Cain&Abel oder Ettercap gefunden werden. Insbesondere hat der Beschuldigte auf verschiedene YouTube-Tutorials zu diesen Themen zugegriffen.

d) **Feststellung von Kommunikation mit möglichen Mitwissern oder Mittätern zur Klärung der Motivation und Intention des Beschuldigten**
Auf dem sichergestellten Datenträger konnte ein komplettes Offline-Postfach des Beschuldigten mit umfangreichem Email-Verkehr zu einem Mitwisser oder Mittäter (carl.confident@gmx.de) nachgewiesen werden. Diesem Mailverkehr ist zu entnehmen, dass sich die beiden beteiligten Personen für Folgestraftaten unter Verwendung der abgefangenen Zugangsdaten verabredet haben, die jedoch dank des rechtzeitigen Zugriffs unterbunden werden konnten.

5. Nachbetrachtung der Praktikumsarbeit

5.1. Beschreibung des Laboraufbaus

Für die Simulation des Vorfalls wurden die folgenden Geräte und Adressen verwendet:

Gateway:

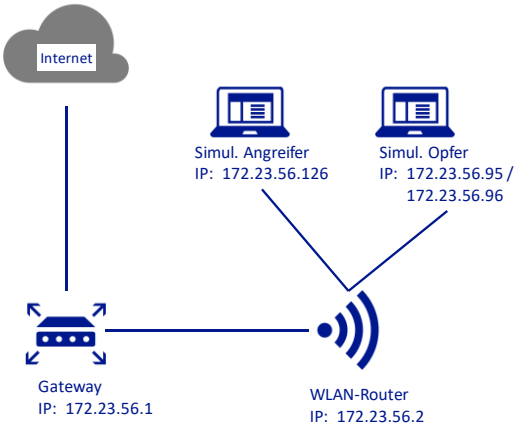
IP: 172.23.56.1
MAC: 00A0572B7C8E

Über das Gateway haben sowohl Angreifer-, als auch Opfer-Gerät den Zugang zum Internet erlangt. Die Verbindung wurde hierbei über den Standard WLAN-Adapter des jeweiligen Windows Betriebssystems hergestellt.

WLAN-Router:

Modell: LANCOM 1821+
IP: 172.23.56.2
MAC: 000B6B2CC8C1

Auf dem WLAN-Router wurde ein öffentliches Netzwerk eingerichtet, um das „Free WIFI“ des Gastronomiebetriebes zu simulieren. Um sicherzustellen, dass sich keine Dritten Zugang zum Netzwerk verschaffen und zum tatsächlichen Opfer des simulierten Angriffs werden, wurde der Zugang zum Netzwerk durch einen MAC-Adressen-Filter eingeschränkt. Lediglich die MAC-Adresse des Opfer- und Angreifer-Gerätes wurden im Filter autorisiert.



Rechner des simulierten Angreifers:

IP: 172.23.56.126
MAC: 38D5470B01E1

Über den Rechner des simulierten Angreifers wurde der MITM-Angriff auf Rechner des simulierten Opfers ausgeführt. Unter Verwendung des Tools „Cain und Abel“ hat der Angreifer das Opfer-Gerät mit manipulierten ARP-Paketen infiziert.

Rechner der simulierten Opfer:

IP: 172.23.56.95 bzw. 172.23.56.96
MAC: 148F3CCC7852

Nachdem das Gerät des simulierten Opfers mit gefälschten ARP-Paketen infiziert wurde, wurden diverse URLs über den lokalen Webbrowser aufgerufen, welche die Eingabe von Credentials erfordern. Diese wurden daraufhin vom Gerät des simulierten Angreifers mitgeschnitten.

5.2. Untersuchung des eingesetzten Werkzeugs

Für die Praktikumsaufgabe haben wir das IT-Forensik-Tool AXIOM ausgewählt. Dafür haben wir zunächst die Arbeitsweise und Leistungsmerkmale des Tools untersucht.

Das Produkt AXIOM ist unterteilt in zwei eigenständige Anwendungen:

- AXIOM Process dient der Erstellung neuer Cases und der Vorverarbeitung (Katalogisierung, Hashing und Vorfilterung, Klassifizierung und Kategorisierung)
- AXIOM Examine dient der manuellen Analyse der Ergebnisse der Vorverarbeitung

Als Gesamtpaket bieten diese beiden Anwendungen im Wesentlichen folgende Leistungsmerkmale:

- **Fall-Verwaltung**
  Für jeden Vorfall wird ein eigener Fall (engl.: Case) angelegt. Zu jedem Fall können die verfügbaren Beweismittel (engl.: Evidence Sources) hinterlegt werden. Die Quellen dieser Beweismittel können Computer, Mobiltelefone oder Cloud-Dienste sein. Für jeden Quellentyp werden wiederum verschiedene Formate in Abhängigkeit vom Akquisitionsverfahren unterstützt; für Computer z.B. physische Datenträger, forensische Abbilder oder Verzeichnisstrukturen.
- **Katalogisierung**
  Das Tool führt zunächst eine Katalogisierung aller gefundenen Dateien durch. Soweit es sich um Rohdaten-Formate handelt, wird dabei auch nach gelöschten Dateien gesucht und diese, soweit möglich wiederhergestellt.
  Zu jeder katalogisierten Datei zeigt AXIOM die genaue Fundstelle und die Metadaten an. Soweit es sich um unterstützte Text- oder Bildformate handelt, kann auch der Inhalt direkt betrachtet werden; anderenfalls wird eine Hex-Ansicht geliefert. Alle Dateien können auch in einem vom Benutzer gewählten Programm geöffnet werden.
- **Hashing und Vorfilterung**
  Es besteht die Möglichkeit, während der Katalogisierung Hashwerte für die gefundenen Dateien berechnen zu lassen und diese gegen frei konfigurierbare Hash-Listen abzugleichen. Dies dient dazu, z.B. einen Großteil der unveränderlichen Dateien von Betriebs- und Anwendungssystemen auszufiltern, sofern sie den bekannten Hashwerten entsprechen. Hierdurch kann der Umfang der katalogisierten Dateien signifikant verkleinert werden.
- **Klassifizierung und Kategorisierung**
  Die katalogisierten Dateien werden anschließend klassifiziert und kategorisiert, d.h. es wird versucht, den Dateien anhand ihrer Fundstelle und ihres Dateiformats (soweit erkannt) einem Artefakttyp zuzuordnen (-> Klassifizierung). Darüber hinaus können je nach Dateityp (Bilder, Text) noch unterschiedliche Verfahren zur Kategorisierung (Hash- bzw. Schlagwortlisten) angewendet werden.
- **Timeline**
  Die Artefakte (bzw. ausgewählte Teilmengen) können auf einer Zeitleiste geordnet werden. Diese Zeitleiste kann grafisch beschnitten und gezoomt werden, um einen fallrelevanten Ausschnitt zu betrachten.
- **Zusammenhänge**
  AXIOM versucht beim Scannen der Dateien Zusammenhänge anhand von Metadaten (Name, Nutzer etc.) herzustellen. Diese Zusammenhänge können grafisch dargestellt werden.
- **Tagging / Bookmarking**
  Jede Datei kann während der Analyse mit vom Benutzer gewählten Tags bzw. Bookmarks versehen werden. Diese Tags bzw. Bookmarks können ihrerseits wiederum zur Filterung von Ergebnismengen genutzt werden.

- **Filtern und Sortieren**
  Alle Ansichten unterstützen das Filtern und Sortieren in Trefferlisten nach einer Vielzahl von Attributen.

5.3. Reflexion des Auswertungsprozesses

Bei der Erstellung des Cases werden auch die Parameter der Vorverarbeitung (Hashing /Vorfilterung bzw. Klassifizierung/Kategorisierung) angegeben. Um einen möglichst umfassenden Eindruck von den Möglichkeiten des Tools zu erhalten, haben wir keine Vorfilterung vorgenommen. Dies führt im Ergebnis zu mehr als 400.000 Artefakten, von denen über 300.000 dem Betriebssystem zugeordnet werden. Durch die Wahl geeigneter Hashlisten für bekannte Betriebssystem- und Anwendungsdateien hätte der Katalogumfang und damit die Verarbeitungszeit signifikant reduziert werden können.

AXIOM Process fordert vor Beginn der Katalogisierung dazu auf, einen evtl. vorhandenen Virenscanner zunächst zu deaktivieren, da dieser zu einer signifikanten Verlängerung der Verarbeitungsdauer führt.

Ohne Vorfilterung und mit eingeschaltetem Virenscanner dauerte die Vorverarbeitung eines forensischen Abbilds von 500 GB bei uns mehr als 17 Stunden; dieser Zeitaufwand hätte durch entsprechende Voreinstellungen erheblich reduziert werden können.

Auch bei der weiteren Analysearbeit in AXIOM Examine stellte sich der große Umfang des Katalogs bei dem eingesetzten System (Intel i5; 8GB) bereits als hinderlich dar, d.h. die Anwendung von z.B. Filtern auf größere Treffermengen führte bereits zu Verzögerungen von mehreren Sekunden.

Generell ist zu empfehlen, dass das Auswertungssystem in Bezug auf Rechenleistung und Speicherplatz signifikant größer dimensioniert sein sollte, als die zu untersuchenden Systeme, um ein flüssiges Arbeiten zu ermöglichen.

Für die Analyse des gegebenen Szenarios haben sich insbesondere die Klassifizierung (Artefakttypen) und die die Nutzung von Schlagwort-Filtern als sehr effizient erwiesen. Die Nutzung der Timeline war im vorgegebenen Fall dagegen weniger relevant, da das zu untersuchende Zeitfenster durch das Szenario bereits recht eng eingegrenzt war. Bei langlaufenden Vorfällen/Angriffen (->APT) wird dieses Hilfsmittel nach unserer Einschätzung jedoch sehr hilfreich sein, um z.B. Muster in zeitlicher Verteilung und Reihenfolgen von Ereignissen zu erkennen.

Die „Connections“-Funktion (Darstellung von Zusammenhängen zwischen Dateien) war auch sehr hilfreich um ggf. von bereits identifizierten Indizien zu weiteren fallrelevanten Artefakten zu gelangen. Dies wird in umfangreicheren Szenarien sicher noch deutlich stärker zum Tragen kommen.

Alle Schritte der Untersuchung wurden entsprechend den Prinzipien für forensische Untersuchungen umfassend protokolliert. Dies beginnt mit der Erstellung eines „Single Evidence Forms“ und eines „Chain of Custody Forms“ für den vorgelegten Datenträger und setzt sich fort mit der Dokumentation der Datensicherung der Dokumentation der forensischen Aufbereitung sowie der Dokumentation der forensischen Analyse.

Die vollständige und umfassende Protokollierung erwies sich aufgrund der fortwährenden Wechsel der Applikationen (AXIOM, Screen-Capturer, Word) als sehr zeitaufwändig. Dies war zwar einerseits förderlich für die Wahrung einer auf Sorgfalt und Reflexion ausgerichteten Arbeitsweise, aber kann für ein beruflich-praktisches Umfeld mit wiederkehrenden/gleichartigen Aufgaben unter hohem Zeitdruck auch unkomfortabel und fehleranfällig sein. Hier wäre es aus unserer Sicht sinnvoll, den Einsatz von GUI-Testtools zu untersuchen, um die Schritte der Auswertung automatisiert

aufzuzeichnen und hieraus ebenfalls automatisiert ein gerichtsverwertbares Protokoll zu erstellen. Hierzu wären sicherlich zunächst auch rechtlich-formale Fragen zu klären.

Eine Alternative könnte eine Aufzeichnung des Screens in einem Video-Stream, kombiniert mit einer Audio-Spur zur mündlichen Kommentierung durch die Auswerter sein. Dies ist sehr leicht umsetzbar, jedoch ließe sich hieraus nicht ohne weiteres eine gerichtsverwertbare Dokumentation erstellen. Da forensische Analysen ohnehin immer nachvollziehbar sein müssen, ließe sich dies dann zwar noch „bei Bedarf“ nachholen, würde aber damit den manuellen Aufwand nur zeitlich verschieben.

Analyse der belegten Festplattenpartition

Die Festplatte, welche zur Simulation des Angriffs verwendet wurde, enthielt vier Partitionen. Von diesen vier Partitionen war zum Zeitpunkt des simulierten Angriffs lediglich eine Partition belegt. Im Rahmen der Erstellung eines RAW-Images von der Festplatte wurden folglich eine belegte und drei leere Partitionen gesichert. Zu Beginn der Analyse des Images lag der Fokus auf der belegten Festplattenpartition. Da bereits auf dieser Partition ausreichend forensische Artefakte gefunden werden konnten, um den Tathergang gerichtsfest nachzuweisen, wurde auf die Analyse der verbleibenden, unbelegten Festplattenpartitionen verzichtet.

Verzicht auf Cloud-Analyse

Das Szenario hat ursprünglich die Analyse der vom simulierten Angreifer verwendeten Cloud-Dienste vorgesehen. Dies sollte nachweisen, dass der Angreifer die während des Angriffs erzeugten Passwort-Files über Dropbox für Dritte zur Verfügung gestellt hat. Das Gerät des Angreifers verfügte jedoch über einen lokalen Dropbox-Client. Dieser wurde bei der Analyse des Festplattenimages ebenfalls überprüft und lieferte ausreichend Artefakte, um den Upload der Passwort-Files in die Cloud nachzuweisen. Daher wurde auf eine zusätzlich separierte Analyse der Cloud-Dienste verzichtet.

6. Literaturverzeichnis

Studienbrief: Forensik in Betriebs- und Anwendungssystemen

https://wingsonline.wings.hs-wismar.de/course/view.php?id=229&section=3

Praktikumsaufgabe Forensik in Betriebs- und Anwendungssystemen:

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

https://wingsonline.wings.hs-wismar.de/course/view.php?id=229&section=3

Forensik in der digitalen Welt

(Dirk Labudde, Michael Spranger; Springer-Verlag GmbH Deutschland, Auflage 2017)

Leitfaden „IT-Forensik“ des BSI (Version 1.0.1 (März 2011))

https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Cyber-Sicherheit/Themen/Leitfaden_IT-Forensik.pdf?__blob=publicationFile&v=2

FTK Imager Dokumentation

https://wingsonline.wings.hs-wismar.de/course/view.php?id=229&section=4

AXIOM Dokumentation

https://wingsonline.wings.hs-wismar.de/course/view.php?id=229&section=4

7. Anhang

7.1. Scan des Single Evidence Forms

Single Evidence Form

Case No.: FBAS-HH8 | Evidence No.: 001

Digital Forensics Lab

PLEASE COMPLETE FORM IN UPPERCASE

Section B: Evidence Collection

Date/Time Collected: 05/07/19 08:18 | Collected by: [redacted]

Site Address: Lila's Café
Elisenstr. 11
22087 Hamburg

Section C: Evidence Details

Date/Time Stored: 05 07 19 11:49

Storage Location: Asservaten-Tresor 03

Device Type: HDD | Capacity: 500GB

Manufacturer: Seagate | Model: Pipeline HD.2 9GW132-194

Serial No.: 9VV6XME3

MD5 Sum: C746001A2010649E74AAC8FD1389A76E

SHA-1 Sum: D8843AE6BDA34C0EB864C4B7DFDA709E79F58F77

Additional Information...

Forensische Kopie mit Write-Blocker Inv. No. #463811

siehe Foto
Note any damage, marks and scratches

Digital Image Taken: [X] Yes [ ] No

Section D: Image Details

Date/Time Imaged: 05 07 19 13:27 | Imaged by: [redacted]

Storage Location: Asservaten-Tresor 03

Image Filename: FBAS-HH8-001.E01 | Image Size: 465 GB (inc. unit)

Additional Information... SanDisk SSD
Modell: SDSSDA-1T00 Ser. No. 19191L453714

This form is to be used when collecting a hardware device containing data that may be of interest in a case. Guidelines:

- **Ensure that this form only refers to one item of evidence and that one is completed for each item of evidence**
- **This form must be accompanied by Chain of Custody forms which detail the individuals that have handled the evidence**
- **Further remarks can be noted overleaf in Section E: Remarks**
- **It is important that these forms are kept with the evidence at all times**
- **Upon handover or disposal please complete Section F: Evidence Handover**

Single Evidence Form

Digital Forensics Lab

Section E: Remarks

Section F: Evidence Handover / Disposal

Date/Time	05.07.19 14:29		
Submitted by	[redacted]	Signature	[redacted]
Received by	[redacted]	Signature	[redacted]
Witnessed by	[redacted]	Signature	[redacted]

7.2. Scan des Chain of Custody Forms

Chain of Custody Form

for use with a Single Evidence form

Digital Forensics Lab

F	B	A	S	-	H	H	8	0	0	1

Case No. Evidence No.

Page No. 01

This form must accompany a Single Evidence form and it's respective evidence

Chain of Custody

SUBMITTER		RECEIVER
Name: [redacted]		Name: [redacted]
Signature:		Signature:
	Evidence Modified:	
Date & Time: 05.07.19 14:29	Yes / (No)	Date & Time: 05.07.19 14:29
SUBMITTER		**RECEIVER**
Name:		Name:
Signature:		Signature:
	Evidence Modified:	
Date & Time:	Yes / No	Date & Time:
SUBMITTER		**RECEIVER**
Name:		Name:
Signature:		Signature:
	Evidence Modified:	
Date & Time:	Yes / No	Date & Time:
SUBMITTER		**RECEIVER**
Name:		Name:
Signature:		Signature:
	Evidence Modified:	
Date & Time:	Yes / No	Date & Time:
SUBMITTER		**RECEIVER**
Name:		Name:
Signature:		Signature:
	Evidence Modified:	
Date & Time:	Yes / No	Date & Time:
SUBMITTER		**RECEIVER**
Name:		Name:
Signature:		Signature:
	Evidence Modified:	
Date & Time:	Yes / No	Date & Time:
SUBMITTER		**RECEIVER**
Name:		Name:
Signature:		Signature:
	Evidence Modified:	
Date & Time:	Yes / No	Date & Time:

If this form is full please continue on another page