ZUR VERÖFFENTLICHUNG IM INTERNET

Gutachten „Verdacht auf Datendiebstahl“ im Rahmen der Hausarbeit der Vorlesung „Forensik in Betriebs- und Anwendungssystemen“ im Sommersemester 2022.

Version: 1.0

Status: vorgelegt

Ersteller:

- Kurt Degenhart
- G.H.
- Tobias Reich

Verteiler:

- Ersteller
- Frau Prof. Dr.-Ing. Antje Raab-Düsterhöft

Inhalt

Abbildungs- und Tabellenverzeichnis

Auftragsspezifikation

Aufgabe

Basierend auf dem im Anhang beschriebenen Szenario wurde folgender Sachverhalt und Auftrag vom Firmenbesitzer an uns herangetragen:

Hr. Meyer hat am 12.05.2022 um 16:30 laut einem Augenzeugen in einem XLS-Dokument Daten bearbeitet, die dem Augenzeugen für die Tätigkeit von Hrn. Meyer unüblich vorgekommen sind. Kurz vorher fand ein Streitgespräch zwischen dem Firmeninhaber und Hrn. Meyer statt. Hr. Meyer hat danach einem Kollegen gegenüber geäußert, dass er vermutet, dass sein Arbeitsvertrag nicht verlängert wird.

Nach Rücksprache mit Betriebsrat und Personalabteilung wird entschieden, zu analysieren, welche Daten Hr. Meyer zu dem erwähnten Zeitraum bearbeitet hat und wie er damit weiter verfuhr. Diese Informationen müssen in Form eines Berichtes vorgelegt werden.

Insbesondere ist dabei auf mögliche Verbindung zu externen Stellen und Speicherung von Daten auf Datenzuträgern zu achten. Nicht Teil des Gutachtens sollen organisatorische Absicherung der Firma sein, da der Gesamtkontext durch den Sicherheitsbeauftragten der Firma, in Zusammenarbeit mit dem Informationssicherheitsbeauftragen und Datenschutzbeauftragten festgestellt wird.

1. Welche Daten hat Herr Meyer am 12.05.2022 bearbeitet?
2. Welche Verarbeitungsvorgänge hat Herr Meyer mit den unter 1. identifizierten Daten durchgeführt?

Situation nach Eintreffen am Arbeitsplatz und erste Maßnahmen

- Windows-Surface GO (‚Tablet') liegt am Arbeitsplatz und ist nicht gesperrt. Weiterhin ist keine nutzerbezogene Anwendung aktiv.
- Firmeneigener USB-Stick liegt neben dem Rechner
- Werkschutz und Firmeninhaber sind gegenwärtig, die ‚Genehmigung' für die Untersuchung liegt schriftlich vor.
- Fotos vom Rechner und den elektronischen Geräten wurden erstellt.
- Erdung wurde bewusst nicht durchgeführt, da der Rechner nicht geöffnet wird.
- Netzwerkverbindungen wurden getrennt, WLAN und Bluetooth deaktiviert. Ein Netzteil wurde vorbeugend als Stromversorgung angeschlossen.
- Bildschirmsperre deaktiviert.

Als Vorgehensmodell wurde im weiteren Verlauf SAP (Secure – Analyse – Present) gewählt.

Untersuchungszeitraum

Der zeitliche Verlauf der Untersuchung stellt sich folgendermaßen dar:

Auftragsvergabe und Annahme	12.05.2022
Analyse der Aufgabenstellung im persönlichen Gespräch – keine weiteren Informationen benötigt.	12.05.2022

Sichern der Beweismittel und erstellen der Images mit der Software FTK Imager	13.05.2022
Analyse der Sachverhalte	14.05.2022 – 24.05.2022
Dokumentation der Ergebnisse und Erstellen des Gutachtens	30.05.2022 – 11.07.2022

Tabelle 1: Ablauf der Beauftragung

Untersuchte Objekte

Es wurden 2 Objekte gefunden, von denen insgesamt 3 Images, nachfolgend ‚Asservate' genannt, gesichert und analysiert worden sind.

Objekt-Nr.	Name des Objektes	Eindeutige ID, Seriennummer, Hashwert
Asservat 01	RAM des Surface-Go	MD5 checksum: 287ded16c81b4a54d2b322ee9419fd0f SHA1 checksum: 8de50a917916eef27874faaa3b1ac06bac2ba4cb
Asservat 02	Festplatte im Surface-Go	MD5 checksum: c6694c1956158c1f20113f2b54309467 SHA1 checksum: 8504507b2612ed21ba7b36a3e124b15dfb17f43d
Asservat 03	USB-Stick: ‚WSD TC108 32GByte' blau – 2-fach-USB anschließbar: USB-A und USB-C	MD5 checksum: 10af3edbc2fd90e6aecef3fb8bcafde8 SHA1 checksum: 969d906f7e872b38c73c9041697fc9c5f0565700

Tabelle 2: Übersicht der Asservate

Arbeitsmittel, Tools und Methodik

Folgende Arbeitsmittel wurden verwendet:

Name	Version	Funktion
Desktop-PC	Mainboard: Micro-Star, B450-A PRO MAX (MS-7B86), AMI-Bios M.70	Hardware zum Betrieb der Forensischen Tools
Betriebssystem Windows	10 - Professional, Patch-Level 21H2, build 19044.1766	OS unter dem die erwähnten weiteren Tools ausgeführt worden sind.
FTK-Imager	4.7.1.2	Sichern digitaler Asservate
Magnet AXIOM Examine	6.1.0.31400	Analyse der Daten
Magnet AXIOM Process	6.1.0.31400	Einspielen der Daten
Microsoft Word	Cloud-Version 2022	Dokumentation der Ergebnisse und Erstellen des Gutachtens

Microsoft Teams	Cloud-Version 2022	Online-Konferenz-Tool und Fileablageort

Tabelle 3: Liste der verwendeten Arbeitsmittel

Bei FTK-Imager handelt es sich um ein kostenfreies und bewährtes Tool zur Erstellung von forensischen Abbildern, es ist fachlich anerkannt. Es wird von der Firma ‚AccessData' angeboten und erstellt je nach Einstellungen physische Abbilder von Datenträgern. Eine portable Version ist ebenfalls verfügbar, um von einem externen Speichermedium gestartet zu werden.[1]

Die Software ‚Magnet Axiom Process' und ‚Examine' der Firma ‚Magnet Forensics' ist eine bewährte und am Markt etablierte Spezialsoftware für die Computerforensische Beweisaufnahme (Process) sowie für die Auswertung (Examine). Die Programme werden im Geschäftsumfeld, Öffentlichen Dienst und Militär eingesetzt. Die zwei Programme sind eng miteinander verbunden und können nur im Verbund zweckdienlich eingesetzt werden.[2]

Microsoft Word und Microsoft Teams wurden zum Austausch der Arbeitsgruppe und zu Dokumentationszwecken genutzt. Bei beiden Programmen handelt es sich um am Markt etablierte und verlässliche Office Anwendungen.

Der PC mit dem Betriebssystem ‚Win10 Professional: entspricht einem am Markt verfügbaren und etablierten Gerät. Sowohl die Software als auch das Betriebssystem wurden stets aktuell gehalten.

SAP-Phase ‚Secure'

Vor Ort wurden zwei Geräte vorgefunden, ein nicht gesperrter laufender PC „Surface GO" von Microsoft und ein daneben liegender USB Stick. Der PC war über WLAN mit einem Netzwerk verbunden, der USB Stick war nicht angeschlossen. Eine bildliche Dokumentation der Geräte wurde vorgenommen und befindet sich im Anhang.

Das Surface GO verfügt genau über einen USB-C Anschluss. An diesen war ein USB-HUB angeschlossen.

Um zu verhindern, dass sich der zu analysierende und der analysierende Computer zur Laufzeit in den Standby-Modus, bzw. in den ‚Sperr-Modus' versetzt, wurden bei beiden zu Beginn die Stromspar- und Bildschirmschoner-Tasks deaktiviert und alle Netzwerkverbindungen (WLAN, Bluetooth) deaktiviert. Ein Netzwerkkabel war nicht angeschlossen. Da die Untersuchenden bei der Sicherung permanent anwesend waren und Bildschirmsperren deaktiviert hatten, war ein MouseJiggler nicht erforderlich.

Bei der Sicherung wurde die Flüchtigkeit der Daten berücksichtigt und es wurde daher folgendermaßen vorgegangen[3]:

1. Sicherung der Hauptspeichers
2. Sicherung der Festplatte
3. Sicherung des USB-Sticks

[1] https://www.exterro.com/ftk-imager
[2] https://www.magnetforensics.com/
[3] Laut RFC 3227

Die Datensicherung und -Validierung erfolgte mit dem Tool ‚FTK-Imager'. Es wurde auf einen USB-Stick installiert, für das Speichern der Daten wurde eine externe Festplatte verwendet, die vorher mit Windows-Mitteln formatiert worden war und als Laufwerk ‚G' im Analyse-Rechner angesprochen werden konnte.

Sicherung Asservat 01 - RAM des Surface-Go

Ein USB Stick mit einer portablen Version von FTK Imager wurde über den HUB an das Surface GO angeschlossen, ebenso eine Datenfestplatte zum Speichern des Images. Durch die Deaktivierung der Online-Verbindungen war eine externe Manipulation der Daten ausgeschlossen worden.

Im ‚FTK-Imager' wurde die Option ‚capture Memory' und das Ziellaufwerk ‚G' ausgewählt.

Es wurde damit begonnen, einen Dump des Hauptspeichers zu erstellen, der in Summe 10 GByte an Speicherplatz belegt hat und im File ‚memdump.mem' abgelegt worden ist.

Anschließend wurde noch die Datei ‚pagefile.sys' (1,3 GByte) kopiert, da sich dort vor allem in Windows-Systemen oft Speicherrelevante Informationen befinden.

Die Datei „memcapture.ad1" wurde ebenfalls als Image-Datei angelegt. Es handelt sich um eine komprimierte Dateiform welche die Dateien „memdump.mem" und „pagefile.sys" enthält. In der Datei „memcapture.ad1.txt" wird dabei auch ein Protokoll der Sicherung inkl. Verifikation und Einstellungen angelegt.

Folgende Abbildung zeigt die gespeicherten Dateien, die Datums- und Uhrzeitangaben und die Größe.

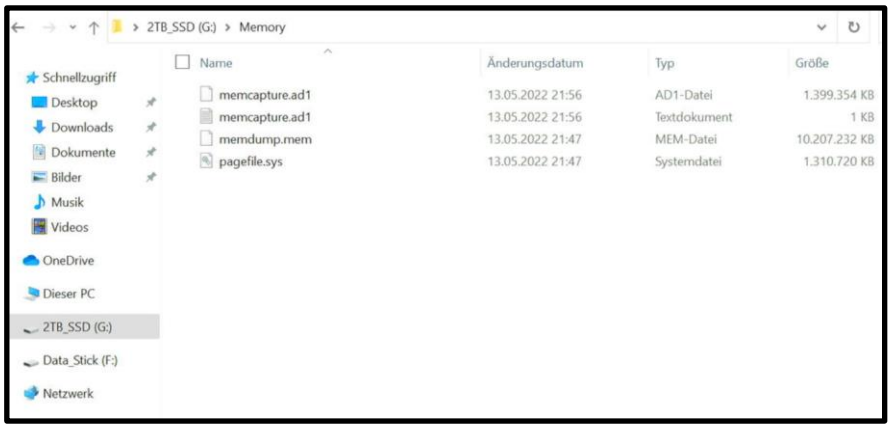


Abbildung 1: Files des gesicherten Hauptspeichers

Sicherung Asservat 02 – Festplatte im Surface-Go

Nach dem Sichern des Hauptspeichers wurde ein Image der Festplatte erzeugt.

Die Festplatte ist bei Asservat 02 verlötet und im Rahmen der Studienarbeit nicht ausbaubar. Das Gerät wurde entsperrt und im Betrieb angefunden. Aus diesem Grund wurde entschieden ein Image der Festplatte im laufenden Betrieb zu erzeugen (Online-Sicherung). Dies bedingte auch, dass KEIN Writeblocker verwendet worden ist, da sonst das auch die systemseitig notwendigen Schreibversuche blockiert und das System damit voraussichtlich instabil geworden wäre. Eine Prüfung mit der Windows-Datenträgerverwaltung ergab, dass nur eine Festplatte vorhanden ist. Diese ist die Quelle der Sicherung.

Als Tool der Wahl wurde hier wieder der FTK-Imager eingesetzt. Dort wurde die Festplatte durch das Anlegen eines neuen Evidence-Items angebunden und das Image mit folgenden Parametern gesichert:

- Case-Number: 001
- Evidence-Numer: E001
- Unique Description:Surface_Go_Meyer_Systempartition
- Examiner: AG_01
- Notes: image 13.05.22 – 22:00
- ImageDestination-File: Festplatte auf extra-2TB-Festplatte
- Filename: 001_E001, 1500 MB Fragment-Size, fastest
- Format: E01

Die Sicherung wurde am 13.05.22 um 22:02:13 Uhr gestartet und dauerte bis 22:26:56.

Der anschließende Verifikationsprozess, der am 13.05.22 von 22:26:57 – 22:45:32 dauerte, ergab nach einem Vergleich der Hashwerte, dass das Image identisch gewesen ist (siehe folgenden Screenshot).

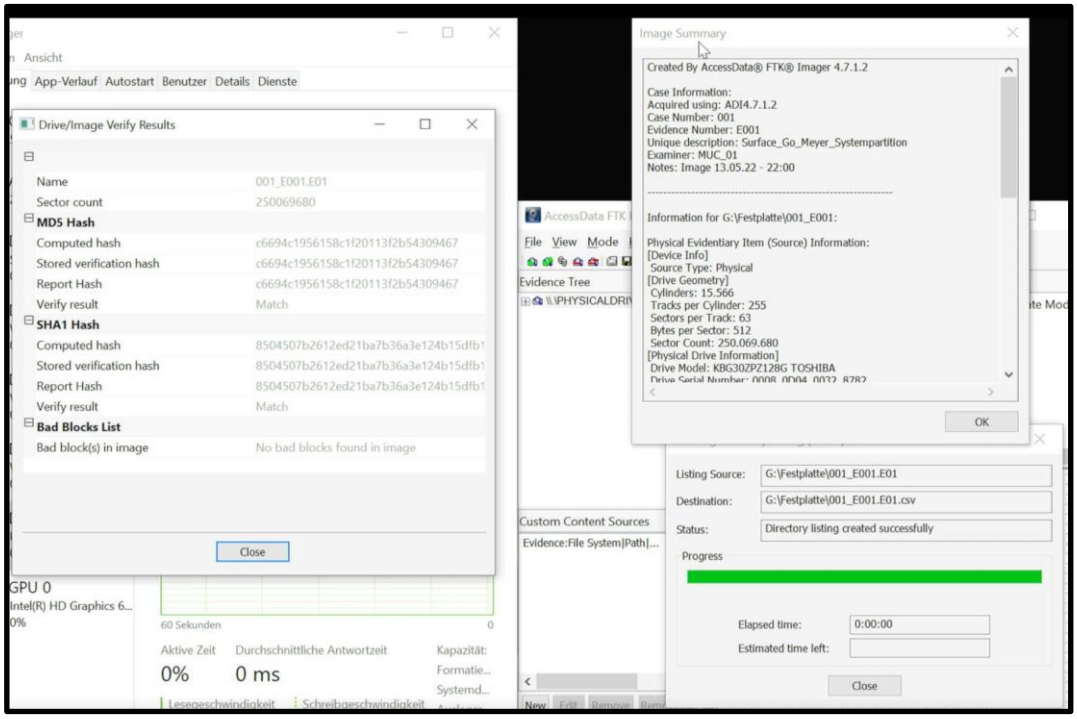
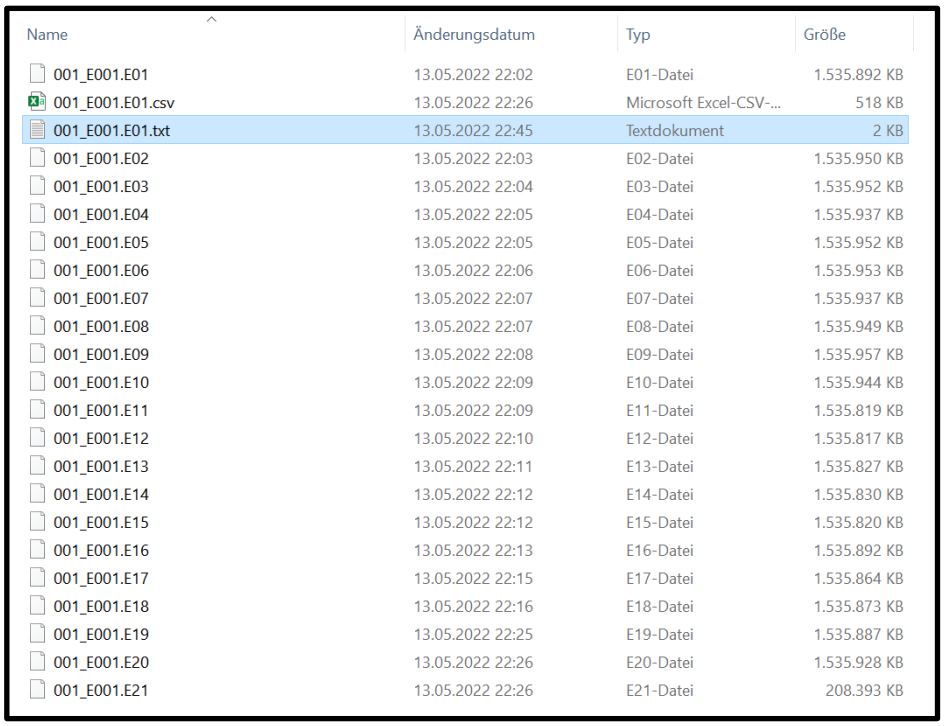


Abbildung 2: Vergleich der Hashwerte nach dem Sichern der Festplatte

Das Image wurde in folgenden Dateien gespeichert:



Name	Änderungsdatum	Typ	Größe
001_E001.E01	13.05.2022 22:02	E01-Datei	1.535.892 KB
001_E001.E01.csv	13.05.2022 22:26	Microsoft Excel-CSV-...	518 KB
001_E001.E01.txt	13.05.2022 22:45	Textdokument	2 KB
001_E001.E02	13.05.2022 22:03	E02-Datei	1.535.950 KB
001_E001.E03	13.05.2022 22:04	E03-Datei	1.535.952 KB
001_E001.E04	13.05.2022 22:05	E04-Datei	1.535.937 KB
001_E001.E05	13.05.2022 22:05	E05-Datei	1.535.952 KB
001_E001.E06	13.05.2022 22:06	E06-Datei	1.535.953 KB
001_E001.E07	13.05.2022 22:07	E07-Datei	1.535.937 KB
001_E001.E08	13.05.2022 22:07	E08-Datei	1.535.949 KB
001_E001.E09	13.05.2022 22:08	E09-Datei	1.535.957 KB
001_E001.E10	13.05.2022 22:09	E10-Datei	1.535.944 KB
001_E001.E11	13.05.2022 22:09	E11-Datei	1.535.819 KB
001_E001.E12	13.05.2022 22:10	E12-Datei	1.535.817 KB
001_E001.E13	13.05.2022 22:11	E13-Datei	1.535.827 KB
001_E001.E14	13.05.2022 22:12	E14-Datei	1.535.830 KB
001_E001.E15	13.05.2022 22:12	E15-Datei	1.535.820 KB
001_E001.E16	13.05.2022 22:13	E16-Datei	1.535.892 KB
001_E001.E17	13.05.2022 22:15	E17-Datei	1.535.864 KB
001_E001.E18	13.05.2022 22:16	E18-Datei	1.535.873 KB
001_E001.E19	13.05.2022 22:25	E19-Datei	1.535.887 KB
001_E001.E20	13.05.2022 22:26	E20-Datei	1.535.928 KB
001_E001.E21	13.05.2022 22:26	E21-Datei	208.393 KB

Abbildung 3: Gespeicherte Files der Festplatte

Die Datei „001_E001.E01.txt“ enthält dabei ein Protokoll der Sicherung inkl. Verifikation und Einstellungen.

Sicherung Asservat 03 – USB-Stick

Datensicherung

Für den USB-Stick wurde ebenfalls im FTK-Imager ein eigenes Evidence-Item angelegt. Das Image wurde auf die bereits erwähnte externe Festplatte in einem eigenen Verzeichnis gespeichert.

(Anmerkung zur Studienarbeit: Ein WriteBlocker wurde im Rahmen der Studienarbeit aus Kostengründen nicht eingesetzt, würde aber in der Praxis eingesetzt werden.)

Dabei wurden folgende Attribute verwendet:

- Case-Number: 001
- Evidence-Numer: E002
- Unique Description: USB_Meyer_blau_32GB
- Examiner: MUC_01
- Notes: image 13.05.22 – 22:32
- ImageDestination-File: Festplatte auf extra-2TB-Festplatte
- Filename: E002, 1500 MB Fragment-Size, fastest
- Fileformat: E01

Nach der Sicherung, die 3 Minuten,42 Sekunden dauerte erfolgte eine Verifikation, die weitere 79 Sekunden in Anspruch nahm. Hier ergaben sich keine Abweichungen der Hashwerte, so dass Ursprung und Image-Copy identisch sind.

Name	Änderungsdatum	Typ	Größe
E002.E01	13.05.2022 22:36	E01-Datei	160.348 KB
E002.E01.csv	13.05.2022 22:36	Microsoft Excel-CSV-...	50 KB
E002.E01.txt	13.05.2022 22:38	Textdokument	2 KB

Abbildung 4: Gespeicherte Daten des USB-Sticks.

Die Datei „E002.E01.txt“ enthält dabei ein Protokoll der Sicherung inkl. Verifikation und Einstellungen.

SAP-Phase ‚Analyse‘

Vorbereitende Tätigkeiten

Als Auswertetool wurde das bereits beschriebene Axiom Process und Examine Version 6.1.0.31400 gewählt.

Mittels Axiom Process wurde der Fall 001 angelegt, die Falldateien wurden im Ordner Axiom_Case und die Beweise, welche von Axiom hinterlegt werden, sind im Ordner Axiom_Beweise gespeichert. Originaldateien wurden im Ordner Images gespeichert.

Für alle Images wurden vorab unter Verarbeitungsoptionen Voreinstellungen vorgenommen. Im Einzelnen wurde der Suchbegriffe „Kunde“ als Keyword hinzugefügt. Von einer Texterkennung in Bildern (OCR Extrahierung) wurde vorab abgesehen, sollte sich im weiteren Verlauf der Analyse ein Bedarf ergeben besteht die Möglichkeit diese durchzuführen. Da kein Verdacht auf Straftaten gegen die sexuelle Selbstbestimmung existiert wurden keine Chats im Zusammenhang mit Sex und Kindern kategorisiert, ebenso wurden Bilder und Videos nicht kategorisiert. CPS Daten wurden ebenfalls nicht angegeben.

Es ist unbekannt welche Tätigkeiten Hr. Meyer zuletzt ausgeführt hat, in der Kategorie Artefakte wurden daher alle auf dem System möglichen Artefakte aktiviert um eine umfassende Übersicht zu erhalten.

Im Folgenden wurden die Asservate als Beweisquellen hinzugefügt und die Beweisanalyse gestartet. Die ist in den folgenden Abschnitten detailliert beschrieben.

Nach Abschluss des Hinzufügens der Beweise sortiert Axiom die Artefakte und Dateien automatisch nach Dateitypen, Zeiten und kann auch Zusammenhänge darstellen. Um dies zu erleichtern wurde die Berechnung der Zusammenhänge und die Berechnung der Zeitleiste veranlasst und durch Axiom durchgeführt.

Analyse Asservat 01 - RAM des Surface-Go

Einstellungen Analyse Asservat 01 – RAM des Surface-Go

Mittels FTK Imager wurde der Hashwert des Hauptspeichers unter „Images\E001\Memory\memcapture.ad1“ erfolgreich verifiziert. Dazu wurde das Asservat in FTK Imager eingebunden und mittels der Funktion „Verify Drive/Image“ geprüft. Das Ergebnis der Prüfung wird graphisch angezeigt und in der begleitenden Protokolldatei „memcapture.ad1.txt“ durch FTK abgespeichert. Ein manueller Vergleich mit den Hash-Werten der Chain of Custody Bögen ist ebenfalls erfolgreich. Die Integrität des Asservats ist erhalten.

Die Datei wurde in den in den angelegten Fall 001 von AxiomProcess übernommen, dazu wurde unter Beweisquellen folgende Auswahl getroffen „Computer“, „Windows“, „Beweise laden“, „Abbild“ und die verifizierte Datei „memcapture.ad1“ ausgewählt. Sie setzt sich aus „memdump.mem“ und „pagefile.sys“ zusammen.

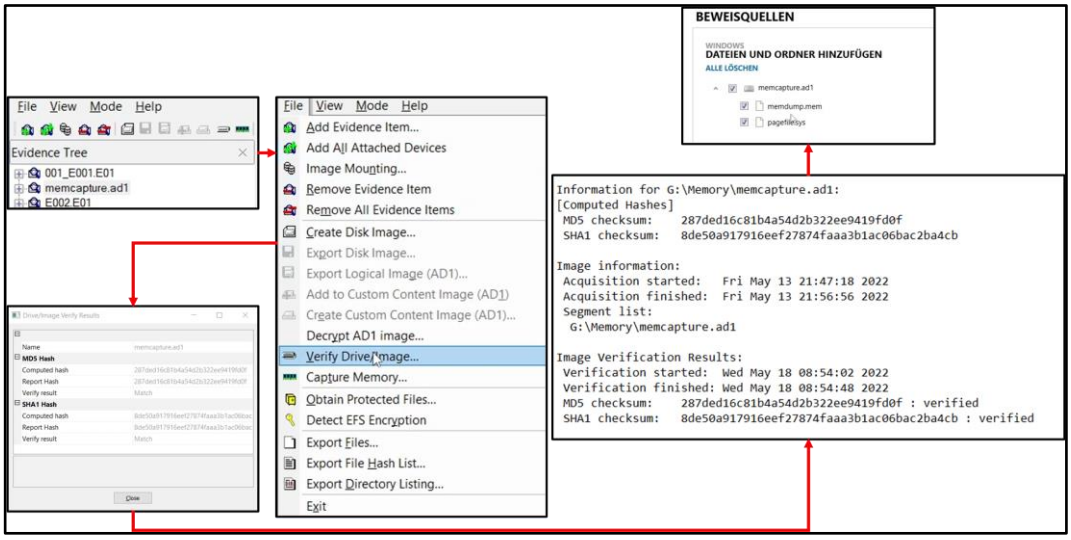


Abbildung 5 Einstellungen Import Asservat 1

Artefakte Analyse Asservat 01 – RAM des Surface-Go

Nachdem alle Asservate in Axiom eingebunden waren wurde die rechenintensive Analyse gestartet. Die Beweise können für jedes Asservat einzeln dargestellt werden und sind hier für Asservat 1 dargestellt.

Im Asservat 1 findet sich auf der Zeitachse in Axiom Examine mit einem Suchfilter Datum 13.05.22 19:35 (UTC) +- 20 Minuten drei (3) Axiom-Kategorien Benutzerkommunikation in Form von E-Mails. Betreff ist „Re: Kundendaten, wie versprochen.“ Gesendet von [E-Mail 1] (stellt Hr. Müller dar) an [E-Mail 2] (stellt Hr. Meyer dar) um 19:37:35 UTC. Der Speicherort im memdump.mem lautet Offset 8349737993. Die Ortszeit lautet UTC + 2. Damit wurde die Mail am 13.05.22 um 21:37 von Hr. Müller an Hr. Meyer gesendet. Inhalt der Mail ist eine Danksagung an Herr Meyer bezüglich einer Vereinbarung. Aus der noch angehängten ursprünglichen Mail geht hervor, dass es sich um nicht weiter spezifizierte Daten handelt.

Abbildung 6: Antwortmail von Hrn. Müller an Hrn. Meyer

Analyse Asservat 02 – Festplatte im Surface-Go

Einstellungen Analyse Asservat 02 – Festplatte des Surface-Go

Mittels FTK Imager wurde der Hashwert der Festplatte unter „Images\E001\Festplatte\ 001_E001.E01“ erfolgreich verifiziert. Dazu wurde das Asservat in FTK Imager eingebunden und mittels der Funktion „Verfify Drive/Image“ geprüft, bei der Generierung wurden 21 Teildateien gebildet, die Verifizierung wurde über alle Dateien durchgeführt. Das Ergebnis der Prüfung wird graphisch angezeigt und in der begleitenden Protokolldatei „001_E001.E01.txt“ durch FTK abgespeichert. Ein manueller Vergleich mit den Hash-Werten der Chain of Custody Bögen ist ebenfalls erfolgreich. Die Integrität des Asservats ist erhalten.

Die Datei wurde in den angelegten Fall 001 von AxiomProcess übernommen, dazu wurde unter Beweisquellen folgende Auswahl getroffen „Computer“, „Windows“, „Beweise laden“, „Abbild“ und die verifizierte Datei „001_E001.E01“ ausgewählt. Sie setzt sich aus 21 fortlaufend nummerierten Dateien zusammen und enthält vier Partitionen und den nicht partitionierten Speicherplatz.

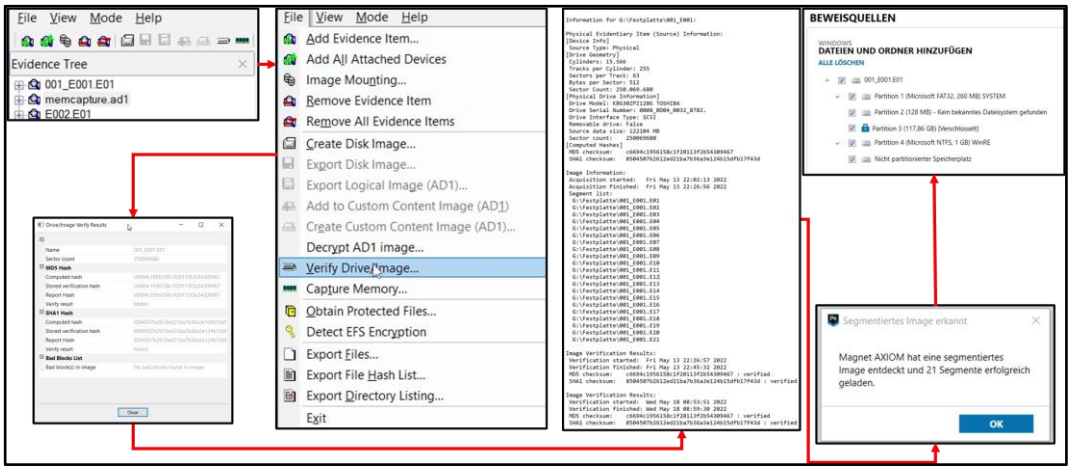


Abbildung 7 Einstellungen Import Asservat 2

Nach Beginn dem Einbinden aller Asservate wurde die rechenintensive Analyse gestartet, dabei wurde die Partition 3, welche mit BitLocker verschlüsselt ist, durch Axiom automatisch entschlüsselt wurde und unter „…\001_Axiom_Evidence\001_E001.E01 - Partition 3 (117,86 GB)_decrypted.img“ gespeichert. Axiom arbeitet bezüglich der Partition 3 von nun an mit dem entschlüsselten Image und fügt dies im Beweisordner von Axiom als eigenen Beweis an.

Abbildung 8 Entschlüsselte BitLocker Partition

Artefakte Analyse Asservat 02 – Festplatte des Surface-Go

Die Beweise können für jedes Asservat einzeln dargestellt werden und sich hier für Asservat 2 dargestellt.

Der Account von Herr Mayer lautet WINGS_AG_01 und wird über die eindeutige Nutzer-SID S-1-5-21-1729541559-3972090306-2745686515-1001 identifiziert, der Account ist mit einem Passwort geschützt. Es handelt sich um den einzigen Nutzeraccount auf dem Gerät.

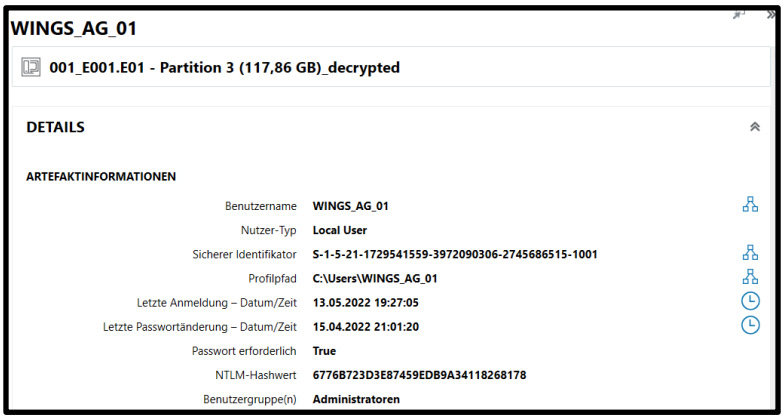


Abbildung 9 Eindeutiger Nutzer Asservat 2

Am 13.05.22 um 19:27:18 UTC authentifiziert sich der User WINGS_AG_01 mit der Benutzer-SID S-1-5-21 unter Verwendung seines Passwort am System.

Am 13.05.22.19:31:54 UTC wurden zuletzt auf die Dateien Namenliste.xlsx und Namensliste.csv zugegriffen, die Hashwerte stimmen mit den obigen Hashwerten überein. Die den Dateien anhängige SicherheitsID in der jeweiligen Masterfiletable (MFT) S-1-5-21-1729541559-3972090306-2745686515-1001 ist eindeutig dem Nutzer WINGS_AG_01 zuzuordnen. Die Hashwerte der Anlagen befinden sich in der nachfolgenden Tabelle. Die Dateien enthalten fünf (5) Spalten mit Vor-, Nachnamen, zugehörigen E-Mailadressen, Geburtsdatum und Telefonnummern.

Name	**Hash (MD-5)**
Namensliste.xlsx	65014b891f8e75b138c436e52ca4595c
Namensliste.csv	2da86a7bd6175e9ecbf2c8d709d45bf2

Tabelle 4: Hashwerte Asservat 2

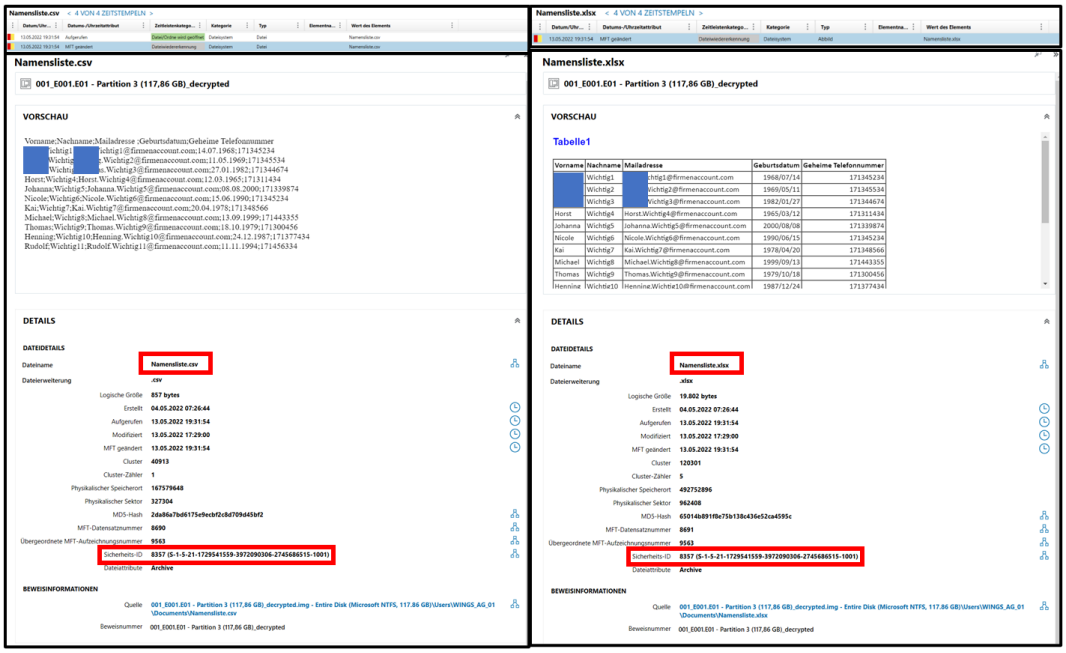


Abbildung 10: Zuordnung der Dateien zum Nutzer Meyer

Am 13.05.22 um 19:32:22 UTC öffnet Hr Meyer sein E-Mailprogramm Thunderbird.

Am 13.05.22 um 19:34:05 UTC wurden eine E-Mail an mit zwei Anlagen (Namensliste.xlsx und Namensliste.csv von [E-Mail 2] (Darstellung Herr Meyer) an [E-Mail 1] (Darstellung Herr Müller) unter Nutzung des Programmes Thunderbird Version 91.9.0 gesendet. Die Hashwerte der Dateien entsprechen den Hashwerten der obigen Tabelle

Der Betreff der Nachricht lautet „Kundendaten, wie versprochen." Der Text der Nachricht lautet: „Grüß Gott Herr Müller, wie besprochen die Daten. Mit freundlichen Grüßen Meyer". Beide Dateien enthalten offensichtlich identische personenbezogene Daten (siehe Abbildung 10: Zuordnung der Dateien zum Nutzer Meyer).

Um 19:37:24 UTC wurde ein USB-Stick erstmalig angeschlossen, installiert und um 19:37:25 UTC in das Dateisystem eingebunden.

Um 19:37:24 UTC wurde eine E-Mail von [E-Mail 1] an [E-Mail 2] empfangen. Herr Müller schickt eine Antwort-Mail für den Empfang der Daten.

Um 19:37:38 UTC wird der Ordner \Users\WINGS_AG_01\Documents geöffnet, in diesem sind die Dateien „Namensliste.xlsx" und „Namensliste.csv" gespeichert.

Um 19:37:54 UTC wurde die Verbindung zum angeschlossenen USB Stick beendet.

Analyse Asservat 03 – USB-Stick

Einstellungen Analyse Asservat 03 – USB-Stick

Mittels FTK Imager wurde der Hashwert des USB Stick unter „Images\E002\001_E002.E01" erfolgreich verifiziert. Dazu wurde das Asservat in FTK Imager eingebunden und mittels der Funktion „Verfify Drive/Image" geprüft. Das Ergebnis der Prüfung wird graphisch angezeigt und in der begleitenden Protokolldatei „E002.E01.txt" durch FTK abgespeichert. Ein manueller Vergleich mit den Hash-

Werten der Chain of Custody Bögen ist ebenfalls erfolgreich. Die Integrität des Asservats ist erhalten.

Die Datei wurde in den in den angelegten Fall 001 von AxiomProcess übernommen, dazu wurde unter Beweisquellen folgende Auswahl getroffen „Computer“, „Windows“, „Beweise laden“, „Abbild“ und die verifizierte Datei „E002.E01“ ausgewählt. Sie besteht aus einer Partition und nicht partitioniertem Speicherplatz

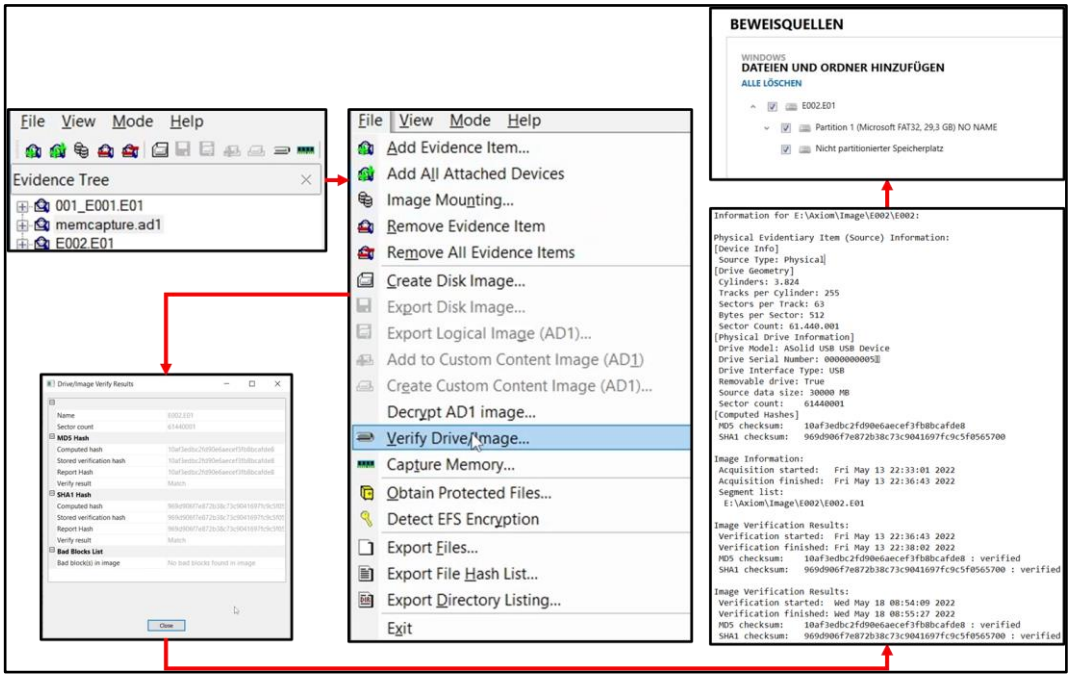


Abbildung 11 Einstellungen Import Asservat 3

Artefakte Analyse Asservat 03 – USB-Stick

Nachdem alle Asservate in Axiom eingebunden waren wurde die rechenintensive Analyse gestartet. Die Beweise können für jedes Asservat einzeln dargestellt werden und sind hier für Asservat 3 dargestellt.

Um am 13.05.2022 19:37:26 UTC wurde die System Volume Information auf dem USB Stick bearbeitet.

Auf dem USB Stick mit der Seriennummer CC316B3F sind zwei Dateien vorhanden, sie wurden am 13.05.2022 19:37:44 UTC erstellt. Die Seriennummer ist dabei den Daten aus Axiom entnommen, eine lesbare Aufschrift auf dem Stick war nicht vorhanden.

Name	**Hash (MD-5)**
Namensliste.xlsx	65014b891f8e75b138c436e52ca4595c
Namensliste.csv	2da86a7bd6175e9ecbf2c8d709d45bf2

Tabelle 5: Hashwerte Asservat 3

Um 19:37:54 UTC wurde die Verbindung zum USB Stick beendet.

Analyse der Zusammenhänge zwischen den Asservaten

Inhaltlicher Zusammenhang

Herr Mayer ist mit der User SID S-1-5-21-1729541559-3972090306-2745686515-1001 der einzige registriere Nutzer auf dem Surface Go, es wird exklusiv durch ihn genutzt.

Mittels der Beziehungsdarstellung in Axiom kann gezeigt werden, dass die Datei Namensliste.xlsx mit dem Hashwert MD-5 65014b891f8e75b138c436e52ca4595c von [E-Mail 2] (Darstellung Herr Meyer) an [E-Mail 1] gesendet wurde. Die Datei ist auf den Asservaten 2 und 3 vorhanden und wurde zuvor im Ordner \Users\Wings_AG_01\Documents gespeichert. Dieser Ordner stellt den persönlichen Dokumentenordner unter Windows von Hr. Meyer dar.

Mittels der Beziehungsdarstellung in Axiom kann gezeigt werden, dass die Datei Namensliste.csv mit dem Hashwert MD-5 2da86a7bd6175e9ecbf2c8d709d45bf2 von [E-Mail 2] (Darstellung Herr Meyer) an [E-Mail 1] gesendet wurde. Die Datei ist auf den Asservaten 2 und 3 vorhanden und wurde zuvor im Ordner \Users\Wings_AG_01\Documents gespeichert. Dieser Ordner stellt den persönlichen Dokumentenordner unter Windows von Hr. Meyer dar.

Im Detail wird die Datei Namensliste.xlsx auf Abbildung 12 mit ihren Verbindungen dargestellt. Im Erkennbar sind die MD-5 und der SHA-1 Hashwerte. Anhand des MD-5 Hashwertes kann nachgewiesen werden, dass die Identische Datei auf dem Asservat 2 und 3 gespeichert ist. Auf Asservat 2 wurde die Datei unter \Users\Wings_AG_01\Documents gespeichert. Die Namensliste wurde von [E-Mail 2] übertragen (Darstellung Hr. Meyer). Auf Abbildung 13 ist erkennbar, das von der E-Mailadresse [E-Mail 2] die Datei an [E-Mail 1] gesendet wurde und zwei Dateien (Namensliste.xlsx, Namensliste.csv) angehangen waren.

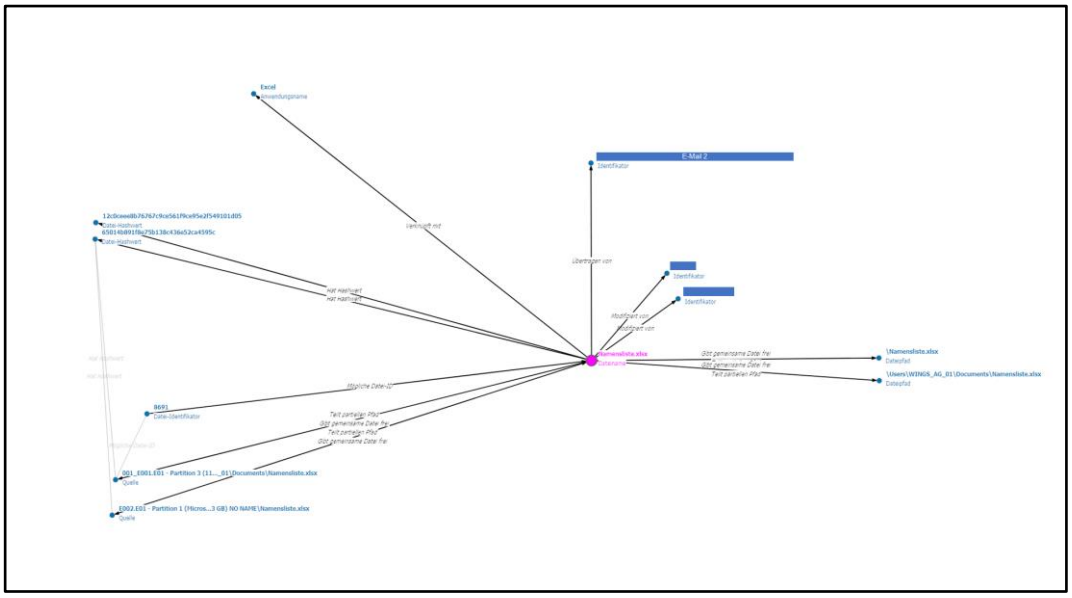


Abbildung 12: Zusammenhänge 1

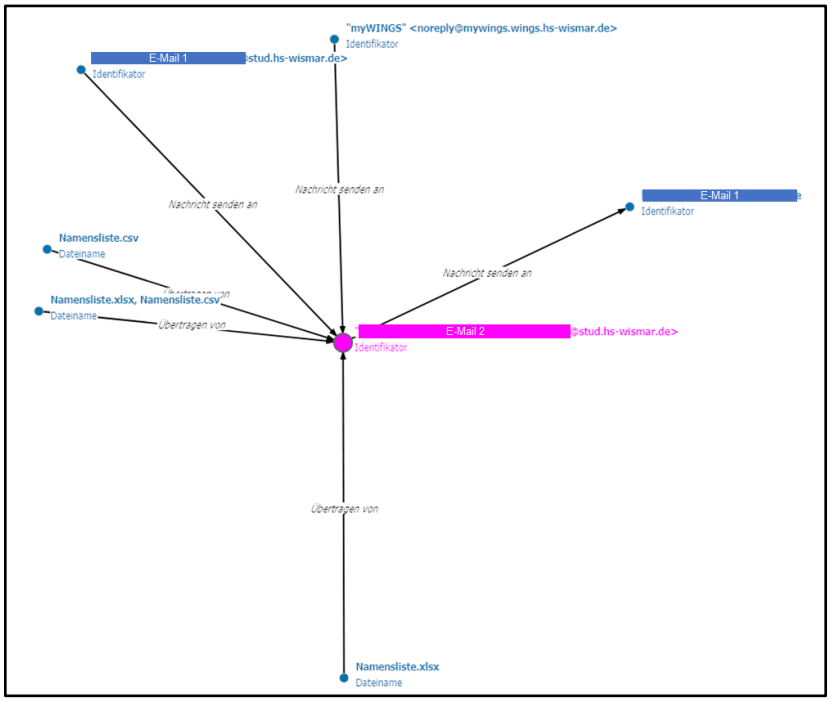


Abbildung 13 Zusammenhänge 2

Dem Pfad auf Abbildung 13 zur Namensliste.csv folgende ergibt sich, dass die Datei mit identischen MD-5 Hashwerten auf den Asservaten 2 und 3 gespeichert ist und unter \Users\Wings_AG_01\Documents auf Asservat 2 gespeichert ist. Sie wurde von [E-Mail 2] übertragen (Darstellung Hr. Meyer). Dieser Vorgang ist bereits beschrieben.

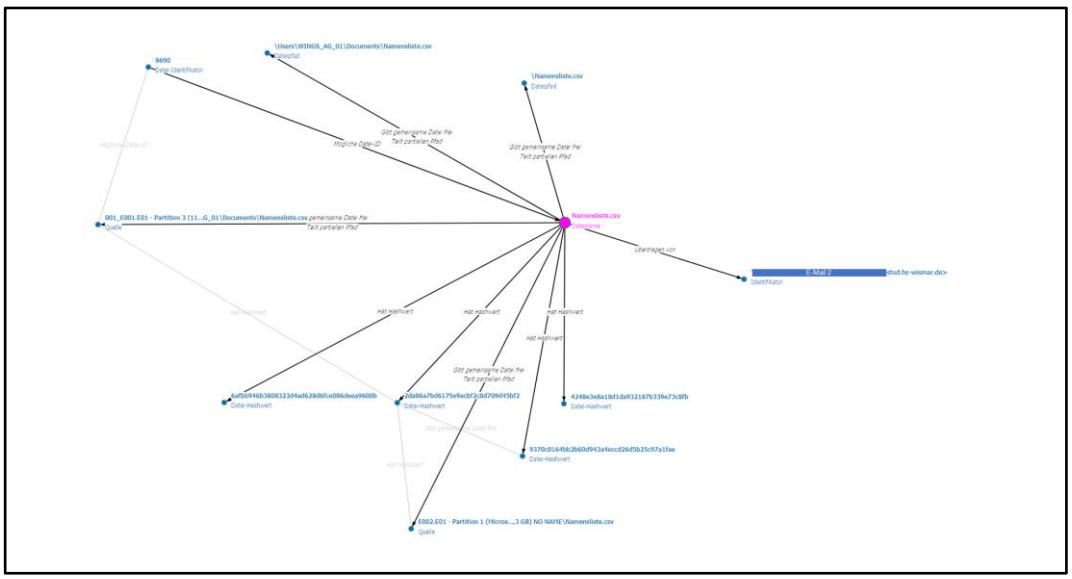


Abbildung 14 Zusammenhänge 3

Zeitlicher Ablauf

Als Darstellungszeit wurde in der Nachfolgenden Tabelle die Ortszeit gewählt (UTC + 2h), da Herr Meyer der einzige registrierte Nutzer auf dem PC ist sind die Aktivitäten auf ihn zurückzuführen.

Die in der folgenden erwähnten Dateien „Kundendaten.xlsx“ und „Kundendaten.csv“ haben identische MD-5 und SHA-1 Hashwerte und sind damit identisch.

Uhrzeit	Verhalten	Asservat Nr.
212718	Anmeldung von Hr. Meyer am PC Benutzer-SID S-1-5-21	2
213154	Bearbeitung Dateien Namensliste.xlsx, Namensliste.csv	2
213222	Öffnung Thunderbird (E-Mailprogramm)	2
213405	E-Mail mit Anlagen Namensliste.xlsx, Namensliste.csv an Hr. Müller mit Thunderbird	2
213424	Installation USB-Stick	2
213425	Einbinden USB-Stick	2
213726	System Volume Information bearbeitet	3
213735	Hr. Meyer empfängt eine Mail als Antwort auf die gesendeten Daten.	1
213738	\Users\WINGS_AG_01\Documents geöffnet	2
213744	Erstellung Namensliste.xlsx, Namensliste.csv auf Asservat 3	3
213754	Trennung Verbindung USB-Stick	2

Tabelle 6: übergreifender zeitlicher Ablauf

SAP-Phase ‚Präsentation‘

Die Ergebnisse werden abschließend zusammenfassend in der Taxonomie nach CERT beschrieben, diese ermöglicht eine Sicherheitsverletzung (Vorfall) anhand mit einer minimalen Anzahl von Begriffen zu beschreiben. Die Struktur ist in der nachfolgenden Tabelle auf der linken Seite dargestellt.

CERT				Beschreibung	Beweis-quelle
Vorfall			Angreifer	Innentäter: Hr. Müller (USER SID: S-1-5-21-1729541559-3972090306-2745686515-1001	Asservat 2
	Angriff		Werkzeuge	Standardanwendungen • E-Mail (Thunderbird) • Officeanwendung (Excel)	Asservat 2
			Schwach-stelle	Unkontrolliertes Erstellen von Dateien möglich Unkontrolliertes Senden von An-lagen möglich Anschluss USB Stick möglich.	Asservat 2
		Ereignis	Aktion	Versandt von Daten an Empfän-ger mit externen E-Mailadressen, im Folgenden Speicherung der Daten auf USB-Stick	Asservat 2,3
			Ziel	Kundendaten	Asservat 2,3
			Resultat	Beurteilungshoheit Firma X	
			Absicht	Beurteilungshoheit Firma X	

Tabelle 7: Darstellung CERT

Herr Müller hat am 13.05.22 im Zeitraum von 19:27 bis 19:38, unter Nutzung seiner bestehenden Berechtigungen, zwei Dateien mit wahrscheinlich Kundendaten (Kundendaten.xlsx und Kundendaten.csv) mittels Thunderbird an eine externe E-Mailadresse versendet und diese Dateien ebenfalls auf einen USB-Stick kopiert.

Anhang

Abgrenzung Zeitliche Einordnung ‚APL‘

Die Daten, die für die Analyse in dieser Arbeit verwendet worden sind, wurden außerhalb der normalen Arbeitszeiten erstellt. Der im Dokument skizzierte Fall fand zeitlich 29 Stunden vorher statt, um einen ‚realistischen‘ zeitlichen Verlauf anzunehmen und ist mit Realzeiten dargestellt. In der praktischen Arbeitswelt werden übliche Bürotätigkeiten nicht in der Nacht stattfinden. In der Arbeit sind die Zeiten so dargestellt wie sie in den Analyseprogrammen gespeichert waren.

Erfasste Fotos

Foto des Surface-Rechners:

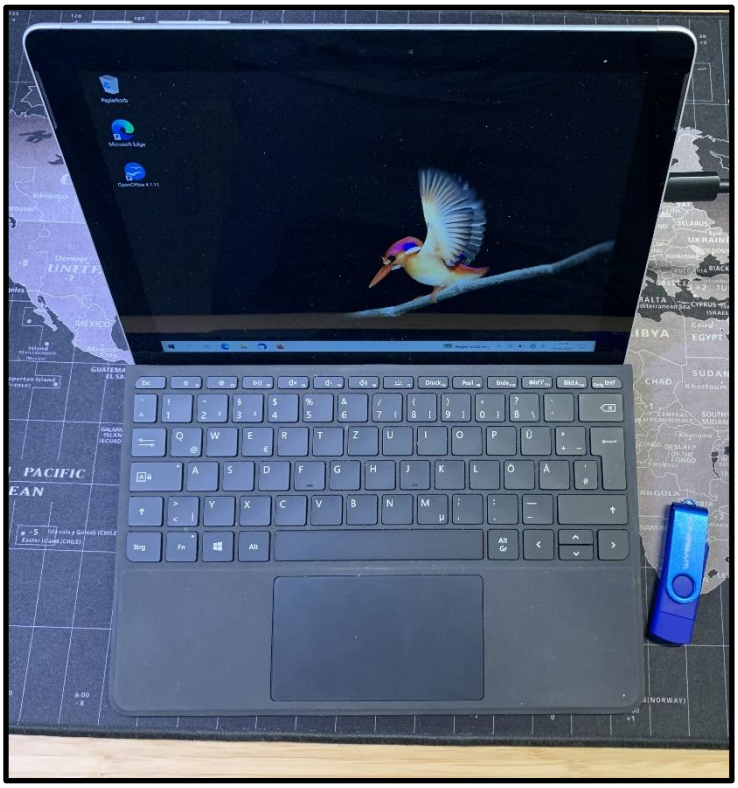


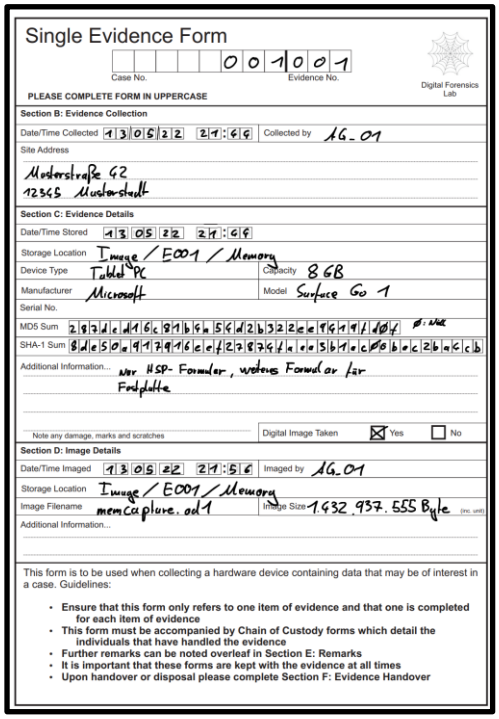
Abbildung 15: SurfaceGO

Foto des USB-Sticks:

Abbildung 16: USB-Stick

Chain of Custodies (CoCs)

COC für den Hauptspeicher:



Single Evidence Form

Case No. | Evidence No. 0 0 1 0 0 1

Digital Forensics Lab

PLEASE COMPLETE FORM IN UPPERCASE

Section B: Evidence Collection

Date/Time Collected 1 3 0 5 2 2 21:46 | Collected by AG_01

Site Address

Musterstraße 42
12345 Musterstadt

Section C: Evidence Details

Date/Time Stored 1 3 05 22 21:46

Storage Location Image / E001 / Memory

Device Type Tablet PC | Capacity 8 GB

Manufacturer Microsoft | Model Surface Go 1

Serial No.

MD5 Sum 287ded16c81b4a54d2b322ee9419fd0f

SHA-1 Sum 8de50a917916eef27874faaa3b1ac06bac2ba4cb

Additional Information... Nur HSP- Formular, weiteres Formular für Festplatte

Note any damage, marks and scratches | Digital Image Taken ☒ Yes ☐ No

Section D: Image Details

Date/Time Imaged 1 3 05 22 21:56 | Imaged by AG_01

Storage Location Image / E001 / Memory

Image Filename memcapture.ad1 | Image Size 1.932.957.555 Byte

Additional Information...

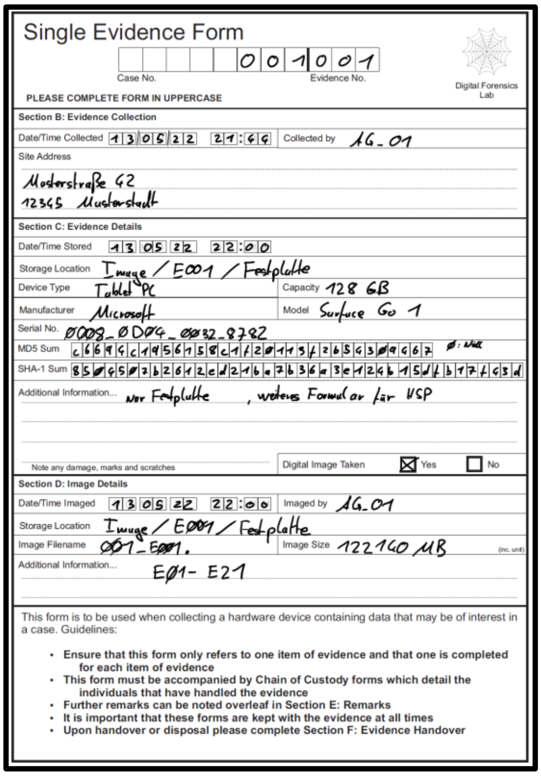
This form is to be used when collecting a hardware device containing data that may be of interest in a case. Guidelines:

- **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**

Abbildung 17: COC Hauptspeicher (Asservat 01)

```
Created By AccessData® FTK® Imager 4.7.1.2

Case Information:
Case Number:
Evidence Number:
Unique Description:
Examiner:
Notes:

---------------------------------------------------------------

Information for G:\Memory\memcapture.ad1:
[Computed Hashes]
MD5 checksum:    287ded16c81b4a54d2b322ee9419fd0f
SHA1 checksum:   8de50a917916eef27874faaa3b1ac06bac2ba4cb

Image information:
Acquisition started:   Fri May 13 21:47:18 2022
Acquisition finished:  Fri May 13 21:56:56 2022
Segment list:
  G:\Memory\memcapture.ad1

Image Verification Results:
Verification started:  Wed May 18 08:54:02 2022
Verification finished: Wed May 18 08:54:48 2022
MD5 checksum:    287ded16c81b4a54d2b322ee9419fd0f : verified
SHA1 checksum:   8de50a917916eef27874faaa3b1ac06bac2ba4cb : veri-
fied
```

COC für die Festplatte des Windows-Tablets



Single Evidence Form

Case No.	001
Evidence No.	001

Digital Forensics Lab

PLEASE COMPLETE FORM IN UPPERCASE

Section B: Evidence Collection

Date/Time Collected	13 05 22 21:44	Collected by	AG_01
Site Address	Musterstraße 42 12345 Musterstadt		

Section C: Evidence Details

Date/Time Stored	13 05 22 22:00		
Storage Location	Image / E001 / Festplatte		
Device Type	Tablet PC	Capacity	128 GB
Manufacturer	Microsoft	Model	Surface Go 1
Serial No.	0008_0D04_0032_8782		
MD5 Sum	c6694c1956158c1f20113f2b5430946 7	Ø: Null	
SHA-1 Sum	8504507b2612ed21ba7b36a3e124b15dfb17f43d		
Additional Information...	nur Festplatte, weiteres Formular für USP		
Note any damage, marks and scratches		Digital Image Taken	☒ Yes ☐ No

Section D: Image Details

Date/Time Imaged	13 05 22 22:00	Imaged by	AG_01
Storage Location	Image / E001 / Festplatte		
Image Filename	001_E001.	Image Size (inc. unit)	122160 MB
Additional Information...	E01- E21		

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

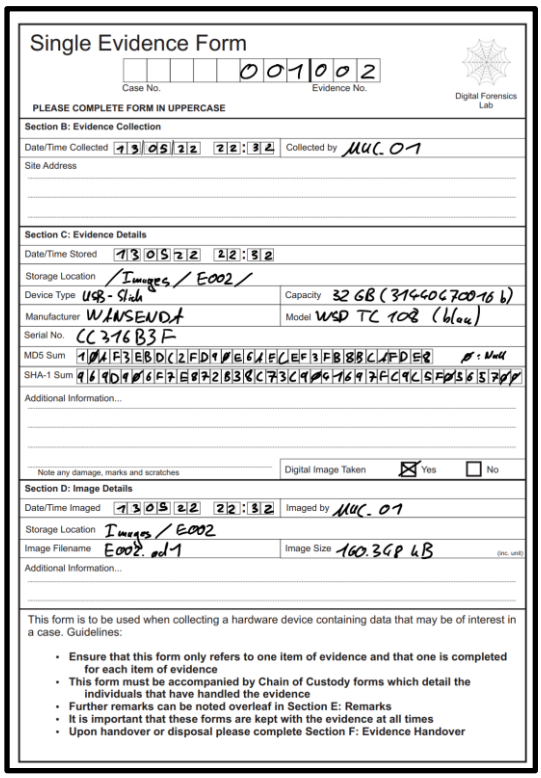
- **Ensure that this form only refers to one item of evidence and that one is completed for each item of evidence**
- **This form must be accompanied by Chain of Custody forms which detail the individuals that have handled the evidence**
- **Further remarks can be noted overleaf in Section E: Remarks**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

Abbildung 18 COC Festplatte (Asservat 02)

```
Created By AccessData® FTK® Imager 4.7.1.2

Case Information:
Acquired using: ADI4.7.1.2
Case Number: 001
Evidence Number: E001
Unique description: Surface_Go_Meyer_Systempartition
Examiner: MUC_01
Notes: Image 13.05.22 - 22:00

--------------------------------------------------------------

Information for G:\Festplatte\001_E001:

Physical Evidentiary Item (Source) Information:
[Device Info]
 Source Type: Physical
[Drive Geometry]
 Cylinders: 15.566
 Tracks per Cylinder: 255
 Sectors per Track: 63
 Bytes per Sector: 512
 Sector Count: 250.069.680
[Physical Drive Information]
 Drive Model: KBG30ZPZ128G TOSHIBA
 Drive Serial Number: 0008_0D04_0032_8782.
 Drive Interface Type: SCSI
 Removable drive: False
 Source data size: 122104 MB
 Sector count:    250069680
[Computed Hashes]
```

```
 MD5 checksum:    c6694c1956158c1f20113f2b54309467
 SHA1 checksum:   8504507b2612ed21ba7b36a3e124b15dfb17f43d

Image Information:
 Acquisition started:   Fri May 13 22:02:13 2022
 Acquisition finished:  Fri May 13 22:26:56 2022
 Segment list:
  G:\Festplatte\001_E001.E01
  G:\Festplatte\001_E001.E02
  G:\Festplatte\001_E001.E03
  G:\Festplatte\001_E001.E04
  G:\Festplatte\001_E001.E05
  G:\Festplatte\001_E001.E06
  G:\Festplatte\001_E001.E07
  G:\Festplatte\001_E001.E08
  G:\Festplatte\001_E001.E09
  G:\Festplatte\001_E001.E10
  G:\Festplatte\001_E001.E11
  G:\Festplatte\001_E001.E12
  G:\Festplatte\001_E001.E13
  G:\Festplatte\001_E001.E14
  G:\Festplatte\001_E001.E15
  G:\Festplatte\001_E001.E16
  G:\Festplatte\001_E001.E17
  G:\Festplatte\001_E001.E18
  G:\Festplatte\001_E001.E19
  G:\Festplatte\001_E001.E20
  G:\Festplatte\001_E001.E21

Image Verification Results:
 Verification started:  Fri May 13 22:26:57 2022
 Verification finished: Fri May 13 22:45:32 2022
 MD5 checksum:    c6694c1956158c1f20113f2b54309467 : verified
 SHA1 checksum:   8504507b2612ed21ba7b36a3e124b15dfb17f43d : ver-
ified

Image Verification Results:
 Verification started:  Wed May 18 08:53:51 2022
 Verification finished: Wed May 18 08:59:30 2022
 MD5 checksum:    c6694c1956158c1f20113f2b54309467 : verified
 SHA1 checksum:   8504507b2612ed21ba7b36a3e124b15dfb17f43d : ver-
ified
```

COC für den USB-Stick:



Single Evidence Form

Case No. 001 Evidence No. 002

Digital Forensics Lab

PLEASE COMPLETE FORM IN UPPERCASE

Section B: Evidence Collection

Date/Time Collected 13/05/22 22:32 Collected by MUC_01

Site Address

Section C: Evidence Details

Date/Time Stored 13/05/22 22:32

Storage Location /Images/E002/

Device Type USB-Stick Capacity 32 GB (31460670016 b)

Manufacturer WINSENDA Model WSD TC 108 (blau)

Serial No. CC316B3F

MD5 Sum 10A1F3EBDC2FD1F6G4FCEF3FB8B8C4FDE8 Ø: Null

SHA-1 Sum 16 9D1Ø6F7E8F2B3CC73C1ØG16917FC9C5FØ5657ØF

Additional Information...

Note any damage, marks and scratches

Digital Image Taken ☒ Yes ☐ No

Section D: Image Details

Date/Time Imaged 13/05/22 22:32 Imaged by MUC_01

Storage Location Images/E002

Image Filename E002.ad1 Image Size 160.368 kB (inc. unit)

Additional Information...

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**

Abbildung 19: COC USB Stick (Asservat 03)

```
Created By AccessData® FTK® Imager 4.7.1.2

Case Information:
Acquired using: ADI4.7.1.2
Case Number: 001
Evidence Number: E002
Unique description: USB_Meyer_blau_32GB
Examiner: MUC_01
Notes: 13.05.22 - 22:32

------------------------------------------------------------

Information for E:\Axiom\Image\E002\E002:

Physical Evidentiary Item (Source) Information:
[Device Info]
 Source Type: Physical
[Drive Geometry]
 Cylinders: 3.824
 Tracks per Cylinder: 255
 Sectors per Track: 63
 Bytes per Sector: 512
 Sector Count: 61.440.001
[Physical Drive Information]
 Drive Model: ASolid USB USB Device
 Drive Serial Number: 0000000005
 Drive Interface Type: USB
```

```
 Removable drive: True
 Source data size: 30000 MB
 Sector count:    61440001
[Computed Hashes]
 MD5 checksum:    10af3edbc2fd90e6aecef3fb8bcafde8
 SHA1 checksum:   969d906f7e872b38c73c9041697fc9c5f0565700

Image Information:
 Acquisition started:   Fri May 13 22:33:01 2022
 Acquisition finished:  Fri May 13 22:36:43 2022
 Segment list:
  E:\Axiom\Image\E002\E002.E01

Image Verification Results:
 Verification started:  Fri May 13 22:36:43 2022
 Verification finished: Fri May 13 22:38:02 2022
 MD5 checksum:    10af3edbc2fd90e6aecef3fb8bcafde8 : verified
 SHA1 checksum:   969d906f7e872b38c73c9041697fc9c5f0565700 : ver-
ified

Image Verification Results:
 Verification started:  Wed May 18 08:54:09 2022
 Verification finished: Wed May 18 08:55:27 2022
 MD5 checksum:    10af3edbc2fd90e6aecef3fb8bcafde8 : verified
 SHA1 checksum:   969d906f7e872b38c73c9041697fc9c5f0565700 : ver-
ified
```

Hintergrundinformationen zur Studienarbeit

Szenario:

Herr Meyer ist (noch) befristet Angestellter der Firma X. Das Arbeitsverhältnis ist seit geraumer Zeit durch Missverständnisse und Meinungsverschiedenheiten belastet. Am 12.05.2022 kommt es zwischen Herrn Meyer und seinem Chef zu einem lautstarken Streit. Herr Meyer ist sich nach dem Streit sicher, dass sein in Kürze auslaufender Arbeitsvertrag nicht verlängert werden wird. Zum einen wäre eine mündlich zugesagte Verlängerung überfällig, zum anderen hat sein Chef im Streit abermals seine subjektive Unzufriedenheit mit den Arbeitsergebnissen von Herrn Meyer kundgetan.

Aus diesem Grund fasst Herr Meyer den Entschluss, eine vertrauliche Sammlung an Kundendaten zu entwenden und einem Konkurrenten der Firma X zukommen zu lassen. Hierzu wertet er an einem seiner letzten Arbeitstage physische Ordner mit Angeboten sowie Schriftverkehr mit Kunden aus vergangenen Projekten und Kunden-Aufträgen aus und trägt diese in eine Excel-Datei ein. Ein Kollege beobachtet die Tätigkeit von Herrn Meyer und stellt diesen zur Rede – woraufhin Herr Meyer vorgibt die Unterlagen auf Versäumnisse und Lessons-Learned hin überprüfen zu wollen, um besser mit ihnen abschließen zu können. Ein kurzer Blick auf die Excel-Datei veranlasst den Kollegen jedoch dazu Herrn Meyer nicht weiter zu stören und stattdessen umgehend den Werkschutz zu informieren. Herr Meyer schöpft Verdacht und kopiert die unfertige Excel-Daten auf einen USB-Stick und versendet sie zusätzlich per Mail.

Kurze Zeit später treffen zwei Werkschutz-Mitarbeiter ein und entfernen Herr Meyer von seinem Rechner, der Rechner wurde dabei nicht gesperrt und neben seinem Rechner verbleibt auch ein firmeneigener USB-Stick zurück.

Schlüssel und Zugangskarten werden Herrn Meyer abgenommen und Herr Meyer wurde des Werksgeländes verwiesen. Im Folgenden wurde eine Ermittlung des Sachverhaltes durch die mit Sicherheit beauftragten Personen der Firma X in Auftrag gegeben, der Betriebsrat stimmt dieser zu. Für die IT-Forensik wurde ein externer Gutachter beauftragt.

Dateien

Für das Szenario waren zwei Dateien mit Kundendaten vonnöten, dies wurden vorab erstellt.

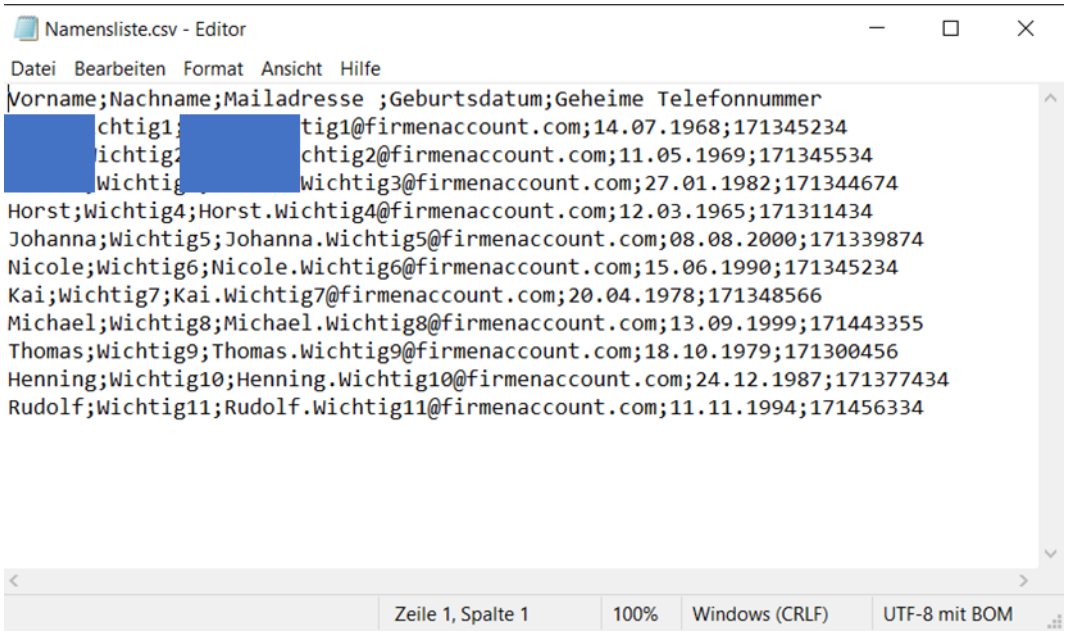


Abbildung 20: Datei Namensliste.csv

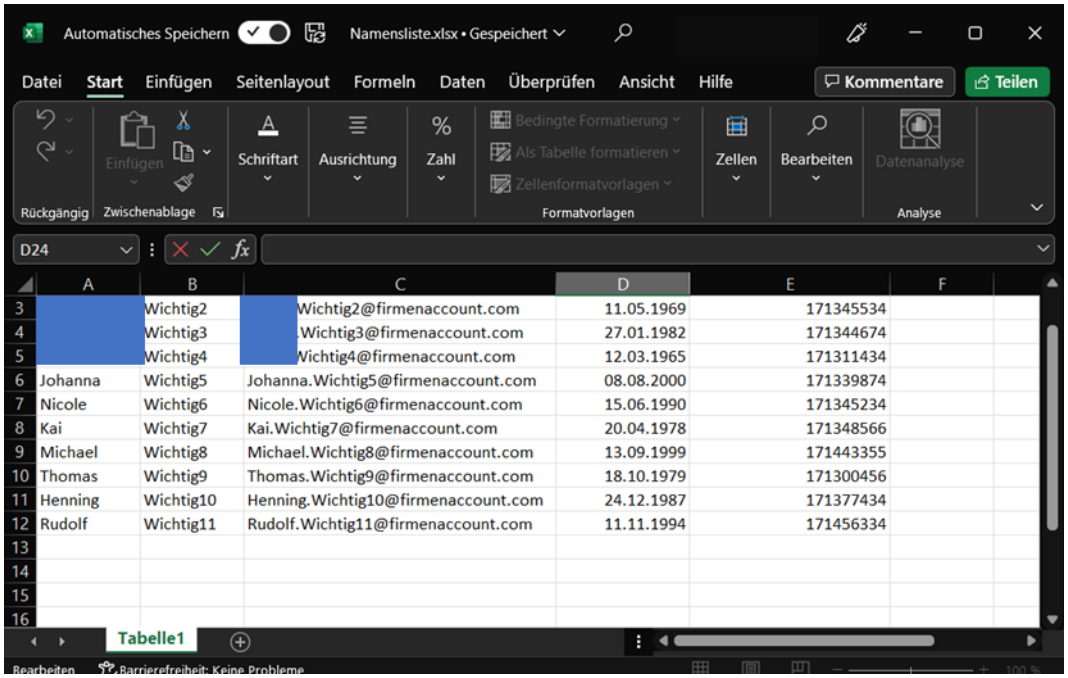


Abbildung 21 Datei Namensliste.xlsx

Vorbereitung der zu analysierenden Geräte

Ein Surface GO wurde in den Auslieferungszustand zurückgesetzt. Auf diesem wurde Windows10 installiert und mittels einem USB-Stick die im vorherigen Abschnitt dargestellten Dateien übertragen. Als Office Programm wurde OpenOffice installiert und als E-Mailprogramm wurde Thunderbird installiert. Ein studentischer Account wurde als Darstellungsaccount des Täters genutzt.

Ein bisher nicht genutzter Stick wurde für die Durchführung des Szenarios bereitgestellt.

Zur Erstellung des Images wurde FTK-Imager auf einen weiteren USB-Stick installiert und eine externe Festplatte für die Datensicherung des Images bereitgestellt.

Praktische Durchführung Szenario

In der Praktischen Durchführung wurde die zwei Dateien „Namensliste.xlsx“ und „Namensliste.csv“ im Nutzerordner unter Dokumente abgelegt, geöffnet und erneut gespeichert, um digitale Spuren zu erzeugen.

Unter Nutzung von Thunderbird wurde E-Mailverkehr zwischen zwei Studentischen Accounts, inklusive der Dateiübertragung der Dateien „Namensliste.xlsx“ und „Namensliste.csv“, durchgeführt.

Ein fabrikneuer USB-Stick wurde an das SurfaceGo angeschlossen und die Dateien wurden mittels ‚Kopieren und Einfügen‘ auf dem Stick gespeichert. Der Stick wurde anschließend getrennt. Ab diesem Zeitpunkt beginnt die Auswertung des SurfaceGO.

Wikipedia Artikel Cloud Log Forensik (CLF)

Definition

Mit Log-basierter Cloud Forensik – auch als "Cloud Log Forensik (CLF)" bekannt – wird die Anwendung forensischer Prozesse auf Log-Daten Cloud-basierter Systeme bezeichnet.[1]

Thematische Einordnung

Bei der CLF handelt es sich um ein Teilgebiet der Cloud-Forensik, welche wiederum ein Teilgebiet der Digitalforensik darstellt[7].

Dabei werden die üblichen Speicher- und Systemabbilder (in der Regel in Form von Snapshots) durch eine forensische Betrachtung der Logfiles ergänzt. Die Methodik berücksichtigt dabei auch Besonderheiten, die in Cloud-Umgebungen zu beachten sind (siehe auch Abschnitt 'Besondere Cloud-Charakteristika').

Die beiden maßgeblichen Ziele der CLF sind die zeitnahe Warnung beim Auftreten von Unregelmäßigkeiten sowie die Erbringung von Hinweisen (Spuren) zur vereinfachten Auswertung. Anwendung findet die CLF damit u. a. im Security Information and Event Management (SIEM), Logging as a Service (LaaS) und der Digital Forensics & Incident Response (DFIR).

Bei der CLF liegt der Fokus auf den Aspekten[1]:

- der allgemeinen "Forensicability"[2] (siehe Beweissicherung und eDiscovery) der Cloud-Umgebung,
- der erforderlichen strategischen Vorbereitung (im Rahmen des forensischen Prozesses gem. BSI-Vorgehensmodell),
- der Etablierung eines zentralen Loggings (für die verteilten Cloud-basierten sowie OnPrem-Systeme wie Firewall, Datenbanken und -speicher, VMs und Hypervisor, Anwendungen und Dienste) im Rahmen der Vorsorge für die IT-Forensik gemäß Prozessbausteins DER.2.2 des IT-Grundschutzkompendiums,
- der dadurch angestrebten beziehungsweise zusätzlich unterstützten Forensic Readiness sowie
- der Gerichtsfestigkeit der hierdurch bereitgestellten Spuren.

Besondere Cloud-Charakteristika

Cloud-Umgebungen unterscheiden sich durch ihre besonderen Charakteristiken wie Virtualisierung, Multi-Tenant-Architektur (und der damit verbundenen Orts-, Zugriffs-, Persistenz- und Skalierungs-Transparenz) sowie der Shared-Responsibility (zwischen Cloud Service Provider (CSP) und Cloud-User (CU)) sowie weiteren Aspekten wie Datenschutz[4] und grenzüberschreitende Rechtsanwendung[7] (multi-jurisdiction) maßgeblich von konventionellen (OnPrem) IT-Landschaften.

Diese Parameter beeinflussen auch die Ablage von Informationen in Log-Files, so dass eine ‚einfache', vor Gericht verwendbare Auswertung (Datensammlung und Ermittlungsarbeit) derselbigen oft nicht durchführbar ist[6]. Werden Informationen aus zentral gespeicherten Dateien extrahiert muss beispielsweise immer betrachtet werden, ob diese in der Form auch verwendbar sind, oder ob lokale Gesetze aus dem Land des Cloud-Providers oder des Cloud-Users dagegen sprechen[3].

Dieser Besonderheit soll mittels neuer Betrachtungsweisen, angepasster Werkzeuge & Methoden, Frameworks und Taxonomien sowie offener Forschungsfragen Rechnung getragen werden.[1]

Anwendung von CLF in der Praxis (Continual- und Sporadic Forensics)

CLF in der Praxis anzuwenden bedeutet, dass Parameter definiert werden müssen, die Abweichungen von regulären Verarbeitungen und damit Hinweise auf potentielle Gefährdungen erkennen lassen. Dies können beispielsweise 'Log-Einträge pro Sekunde', 'Veränderungen der Log-Datei-Größe pro Sekunde' oder auch die 'Protokollierung des Zugriffs auf geschützte Dateien' sein, jeweils unter Berücksichtigung definierter regulärer Arbeitszeiten.

Stellt das Erkennen solcher Auffälligkeiten in on-Prem-Log-Files schon eine Herausforderung dar, so vergrößert sich das Problem bei Log-Files von Cloudservices, wie im vorigen Absatz bereits beschrieben.

Generell kann CLF auf 2 Arten Anwendung finden[1]:

- im Bereich der Continual Forensics
- bei Sporadic Forensics

Bei 'Continual Forensics' werden die definierten, zu überwachenden Parameter laufend überprüft, wodurch Auffälligkeiten zeitnah erkannt werden. Diese Methode eignet sich daher auch sehr gut, um in ein Security Information and Event-Management eingebettet zu werden. Relevante Logs werden für einen bestimmten Zeitraum gespeichert.

Dauer und Umfang hängen dabei stark von folgenden Faktoren ab[4]:

- Verantwortungsbereich: bei CSP oder CU gespeichert
- rechtliche Vorgaben (Ligitation Hold)
- Datenschutzrichtlinien (Datenschutzerklärung und EU-DSGVO)
- Sicherheitskonzept und Service Level Agreements[6][7] (SLAs)
- wirtschaftliche Faktoren (Speicherplatz, Lizenz-Kosten)[4][7]

'Sporadic Forensics' bedeutet dagegen die nachträgliche Auswertung von Auffälligkeiten auf Anforderung. Hierfür sind in Abhängig vom benötigten Zugriff richterliche Erlasse nötig.

Beide Anwendungen werden von den 3 grundlegenden Cloud-Service-Modellen unterstützt, jedoch mit entsprechenden Hürden in der Auswertbarkeit. Nachfolgende Tabelle gibt eine auszugsweise Übersicht hierüber.

Infrastructure as a Service: IaaS	Da bei diesem Servicemodell der Server inkl. Betriebssystem, Middleware und Anwendungssoftware von dem Cloud-User verwaltet werden, bietet sich hier die beste Möglichkeit, eigenständig CLF einzusetzen. Sowohl Server-lastige Informationen (CPU-Verbrauch, Memory-Auslastung, Zugriff auf geschützte Dateien,...), als auch Zugriffe auf Daten (z. B. Datenbanken, Office-Dokumente) können effizient in Log-Files dokumentiert werden. Werden die Server auch noch physisch dediziert dem Cloud-User bereit gestellt, können

	Nebeneffekte anderer durch den Hypervisor bereit gestellten virtueller Umgebungen ausgeschlossen werden. Eine Manipulation dieser Log-Files kann zwar mit entsprechenden Rechten erfolgen, aber auch diese werden wiederum dokumentiert.
Platform as a Service: PaaS	Bei PaaS wird es sehr schwer, physische Parameter zu überwachen, zumal dort in der Regel mehrere virtuelle Instanzen auf den physikalischen Maschinen installiert sind und Auffälligkeiten nicht eindeutig zugewiesen werden können. Effizient können hier nur Parameter angewandt werden, die sich auf Auffälligkeiten bei den installierten Middleware- und Applikations-Lösungen beziehen.[6]
Software as a Service: SaaS	Bei diesem Modell besteht fast keine Möglichkeit für den Cloud-Kunden, individuelle Attribute zur Überwachung zu definieren, da die bereitgestellten Ressourcen und Applikationen komplett von dem Cloud-Anbieter verwaltet werden.[4] In diesem Fall ist es besonders wichtig, mit dem Cloud-Anbieter über mögliche Angriffsszenarien und vorbeugende Maßnahmen zu verhandeln.[4]

Selbstauskunft der CSP gem. BSI-C5-Katalog und Cloud Control Matrix (CCM)

Über die Analysemöglichkeiten bei ihren CSP können sich Cloud-Nutzer unter anderem auch via deren C5-Reports sowie CCM-Einträgen informieren. Die C5 Kategorien OPS 10-17 geben Auskunft über die Aspekte des "Logging and Monitoring". Insbesondere OPS-15 (Accountability) wird diesbezüglich sehr konkret: "The log data generated allows an unambiguous identification of user accesses at tenant level to support (forensic) analysis in the event of a security incident. Interfaces are available to conduct forensic analyses and perform backups of infrastructure components and their network communication."

Hinsichtlich CCM-Einträgen könnten sich folgende Katalog-Fragen aus den Bereichen Security Incident Management, E-Discovery, & Cloud Forensics (SEF) sowie Infrastructure & Virtualization Security (IVS) als relevant erweisen:

- SEF-02.2: "Do you integrate customized tenant requirements into your security incident response plans?"
- SEF-04.2: "Does your incident response capability include the use of legally admissible forensic data collection and analysis techniques?"
- IVS-01.1: "Are file integrity (host) and network intrusion detection (IDS) tools implemented to help facilitate timely detection, investigation by root cause analysis, and response to incidents?"
- IVS-01.2: "Is physical and logical user access to audit logs restricted to authorized personnel?"

Somit stellt BSI-C5 OPS-15 (Accountability) gegenüber den entsprechenden CCM-Fragen hinsichtlich der Möglichkeiten und Anwendbarkeit von CLF den aussagekräftigeren Standard dar.[5]

Quellen

1. Ghosh, A., De, D., Majumder, K. (2021)
"A Systematic Review of Log-Based Cloud Forensics."
In: Smys, S., Balas, V.E., Kamel, K.A., Lafata, P. (eds) "Inventive Computation and

Information Technologies"
Lecture Notes in Networks and Systems, vol 173. Springer, Singapore.
https://doi.org/10.1007/978-981-33-4305-4_26

2. Simou, Stavros, et al.
"A framework for designing cloud forensic forensic-enabled services (CFeS)."
Requirements Engineering 24.3 (2019): 403-430.

3. https://en.wikipedia.org/wiki/Cloud_computing_security#Legal_and_contractual_issues

4. Shaun, M. Akbar. (2020)
"A Compendium of Cloud Forensics"
http://dx.doi.org/10.4018/978-1-7998-1558-7.ch012.

5. C5:2020 Referenztabelle
Abgerufen am 10.07.2022:
https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/CloudComputing/Anforderungskatalog/2020/C5_2020_Referenztabelle.xlsx?__blob=publicationFile&v=1

6. T. Sang
"A Log Based Approach to Make Digital Forensics Easier on Cloud Computing"
In: "Third International Conference on Intelligent System Design and Engineering Applications", 2013, pp. 91-94
doi: 10.1109/ISDEA.2012.29.

7. Ruan, Keyun & Carthy, Joe & Kechadi, Tahar & Crosbie, Mark. (2011)
"Cloud forensics: An overview"