Hochschule Wismar
University of Applied Sciences
Technology, Business and Design
Fakultät für Ingenieurwissenschaften

Modularbeit

Forensische Datenanalyse: Untersuchung eines fiktiven Vorfalls

Eingereicht am: 19. März 2024

von: Autor 1
geboren am 01.01.1970
in Wismar
Matrikelnummer 12345

Autor 2
geboren am 01.01.1970
in Wismar
Matrikelnummer 12345

Autor 3
geboren am 01.01.1970
in Wismar
Matrikelnummer 12345

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

Inhaltsverzeichnis

1 Aufgabenstellung

Diese Hausarbeit ist die Prüfungsleistung für das Modul „Forensische Datenanalyse“ im Studiengang „Angewandte Informatik“ der Hochschule Wismar. Es soll ein fiktives Szenario ausgedacht und dokumentiert werden, welches zu einer forensischen Analyse führt. Für die geforderte Analyse des Szenarios müssen zu Beginn Daten erzeugt werden. Dafür wird das gesamte Szenario unter Verwendung mehrerer Geräte durchgeführt und der Prozess dokumentiert. Für die spätere Analyse wird von jedem Gerät ein Image erzeugt. Dieser Schritt ist ebenfalls zu dokumentieren. Die Analyse erfordert den Einsatz verschiedener Computerforensik-Software. Schritte, welche erweiterte Kenntnisse voraussetzen, sollen dokumentiert und begründet werden. Schließlich ist ein forensisches Gutachten zum beschriebenen Szenario zu erstellen. Die Randbedingungen des Szenarios und der Durchführung sind:

- Mindestens fünf Aktionen (z. B. E-Mail schreiben, Löschen von Daten, …) auf mindestens drei Geräten
- Davon eine Aktion, bei der eine RAM-Analyse benötigt wird
- Eine zusätzliche Aktion mit Datenbankzugriff

2 Beschreibung des Szenarios

Ein internationales Forschungsteam arbeitet fieberhaft an der Entwicklung eines Fusionsreaktors und steht kurz vor dem Durchbruch. Es fehlen lediglich einige Verbesserungen, bevor der Reaktor die Marktreife erreicht. Die gesamte Forschung findet unter strengster Geheimhaltung statt. Die Idee dahinter ist folgende: Der Reaktor soll zunächst entwickelt werden, dann wird das Ergebnis mit einem Patent versehen und anschließend der gesamten Welt kostenlos zur Verfügung gestellt. Dadurch soll verhindert werden, dass ein einziges Unternehmen in den Genuss dieser Technologie kommt und sich dadurch eine Monopolstellung sichern kann. Während einer längeren Krankheitsperiode, schreitet die Entwicklung nur langsam voran, als plötzlich eine Pressemitteilung die Aufmerksamkeit der gesamten Welt auf sich zieht: Der Energieriese *ERWEE* hat es geschafft, einen Fusionsreaktor zu entwickeln und in Betrieb zu nehmen. Die Forschenden erkennen anhand der Fotos aus der Zeitung, dass der Reaktor, dem von ihnen entwickelten sehr ähnlich ist. Der Verdacht erhärtet sich, dass jemand aus dem Team die Ergebnisse an den Konzern verkauft hat. Eine Untersuchung wird gestartet. Das gesamte Team ist verpflichtet auf Dienstnotebooks zu arbeiten und sämtliche private Technik muss mit Betreten der Arbeitsstelle abgegeben und eingeschlossen werden. Deshalb nimmt sich das Untersuchungsteam zunächst die Dienstgeräte der Forscherinnen und Forscher vor. Das Gerät von Herrn Kurz ist dabei besonders auffällig. Er hat sämtliche Forschungsdaten von dem Fileserver heruntergeladen und auf seinem Notebook gespeichert. Als er darauf angesprochen wird, ist er selber verwundert und behauptet, dass es sich dabei um eine automatische Synchronisation der Daten handeln muss, anders könne er sich das nicht erklären. Das Untersuchungsteam lässt sich davon jedoch nicht überzeugen, stellt sein Gerät sofort im laufenden Betrieb sicher und startet zusammen mit der Polizei weitere Ermittlungen gegen Herrn Kurz. Was sie zu diesem Zeitpunkt noch nicht wissen: Herr Kurz hatte nur wenige Tage zuvor ein mysteriöses Treffen mit Herrn Lange, einem Vertreter von *ERWEE*.

3 Umsetzung des Szenarios

In diesem Kapitel wird die Durchführung des Szenarios beschrieben. In Abschnitt 3.1 wird zunächst der Ablauf des Vorfalls grafisch dargestellt und die verwendeten Geräte aufgezeigt. Das darauffolgende Kapitel 3.2 beschreibt, wie die verwendeten Geräte und Technologien vorbereitet wurden, um dieses Szenario umzusetzen. Abschließend wird in Kapitel 3.3 die tatsächliche Umsetzung aufgezeigt.

3.1 Vorbetrachtungen

Das geschilderte Szenario beschreibt den Vorfall der Industriespionage. In den Vorfall sind fünf Geräte involviert:

- das Dienstnotebook von Herrn Kurz
- das private Notebook von Herrn Kurz
- das private Handy von Herrn Kurz
- ein USB-Stick
- eine Nextcloud des Unternehmens *ERWEE* mit Zugriff von Herrn Lange

Die Abbildung 1 zeigt den schematischen Zusammenhang der Geräte untereinander. Die Daten befinden sich zunächst auf einem Netzlaufwerk und werden dann auf das Dienstnotebook von Herrn Kurz kopiert. Anschließend wird der USB-Stick an dieses Notebook angeschlossen und die Daten darauf übertragen. Der USB-Stick wird dann mit dem privaten Notebook von Herrn Kurz verbunden, auf welches die Daten kopiert werden. Zum Abschluss wurden die Daten von dem privaten Notebook in die Nextcloud von *ERWEE* hochgeladen. Der Link dazu wurde in den Nachrichten auf dem Handy ausgetauscht, die parallel zum Ablauf verfasst wurden.

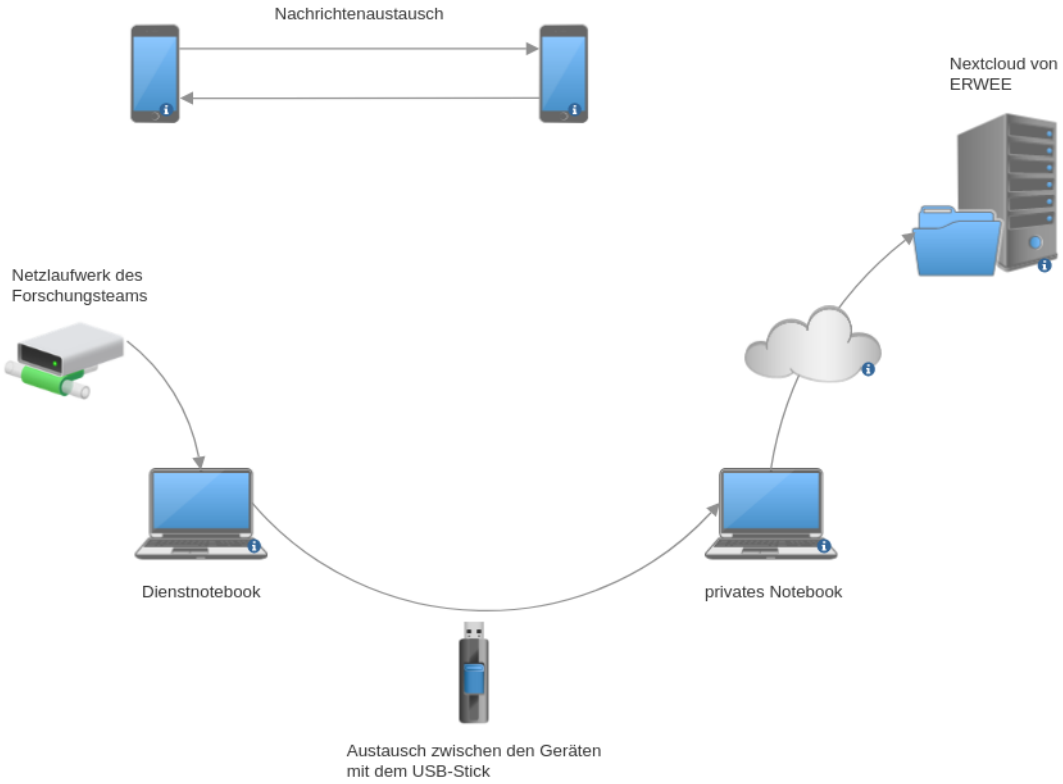


Abbildung 1: Zusammenhang zwischen den einzelnen Geräten

3.2 Vorbereitung der Datenquellen

Alle Aktionen wurden auf physischen Geräten ausgeführt. Es existieren zwei Notebooks, auf denen die Daten mithilfe des USB-Sticks ausgetauscht wurden. Die Nextcloud von *ERWEE* ist mithilfe eines Docker-Containers gehostet. Für die E-Mail-Konten wurden Dienste von Drittanbietern genutzt. Die Nachrichten wurden an das Telefon eines Gruppenmitglieds gesendet, wobei das Telefon, welches später untersucht wurde, gerootet war.

3.2.1 Erstellung der E-Mail-Konten

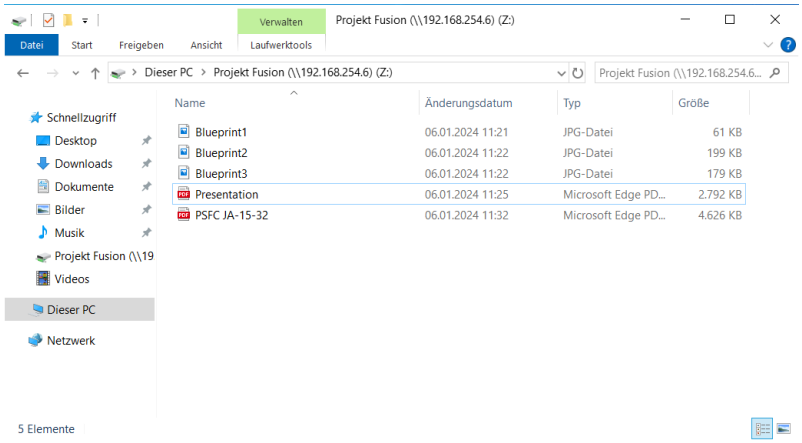
Für den Austausch von Nachrichten wurden zwei E-Mail-Konten erstellt. Zum einen ein E-Mail-Account für Herrn Kurz und zum anderen ein Account für Herrn Lange von *ERWEE*.
Der private Account von Herrn Kurz wurde bei dem Google-Mail (Gmail) Service erstellt. Die zugrundeliegenden persönlichen Daten sind ausgedacht. Lediglich die

verwendete Telefonnummer ist echt und dieselbe, wie in Kapitel 3.2.4. Mit der E-Mail-Adresse von Herrn Kurz wurden schließlich Newsletter abonniert, um das Postfach mit E-Mails zu füllen und so den Eindruck eines aktiven Kontos zu erwecken. Die E-Mail-Adresse lautet: *heinrich4575@gmail.com*.
Der zugrundeliegende E-Mail-Service des E-Mail-Kontos von *ERWEE* ist ProtonMail. Hier wurde lediglich ein E-Mail-Konto eingerichtet und das Postfach nicht mit E-Mails gefüllt. Begründet ist diese Entscheidung darin, dass Herr L. von *ERWEE* dieses E-Mail-Konto im Verlauf der Geschichte ausschließlich angelegt hat, um mit Herrn K. zu kommunizieren. Die E-Mail-Adresse lautet: *erweeunternehmen@protonmail.com*.

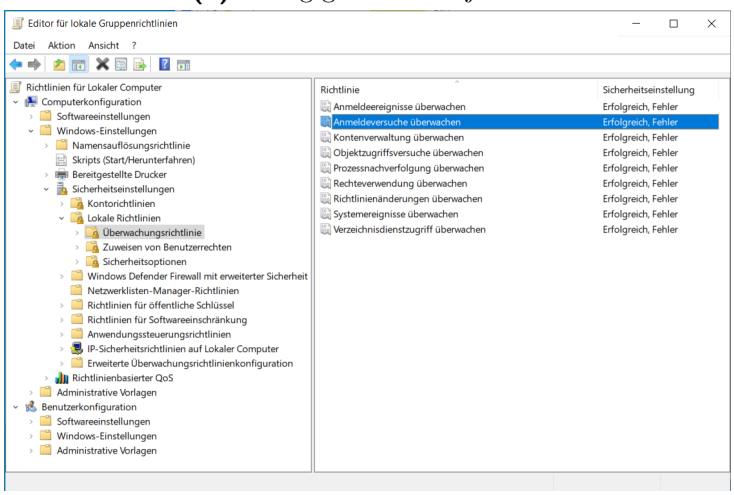
3.2.2 Dienstnotebook

Als Dienstnotebook von Herrn dient ein P650SE des Herstellers Clevo. In dieses wurde ein 2 TB fassende SSD eingebaut und auf dieser Windows 10 Pro 22H2 installiert. Während der Ersteinrichtung wurde ein Offline-Konto mit dem Namen „Heinrich Kurz“ und Passwort „H3inrich“ angelegt und das Notebook mit dem WLAN-Netzwerk „Stark Industries“ verbunden. Nach Abschluss des Einrichtungsassistenten wurden sämtliche verfügbaren Windows Updates installiert. Zum Zeitpunkt der Anfertigung der Arbeit befand sich somit die Build-Version 19045.3803 auf dem Gerät. Der Gerätename wurde in „NB-003-HK“ geändert. Um bei der späteren Sicherung nicht zu viel Speicher zu benötigen, wurde die C-Partition mithilfe der Windows Datenträgerverwaltung auf 59 GB verkleinert. Mit dem Laufwerkbuchstaben Z wurde ein Netzlaufwerk zum Pfad `\\192.168.254.6\Projekt Fusion` verbunden. In diesem befinden sich die streng geheimen Projektdaten, welche Herr Kurz mit dem Dienstnotebook auf einen USB-Stick kopieren und mit dem privaten Notebook in Nextcloud von Herrn Lange hochladen wird (Abb. 2a).

Um möglichst viele Log-Daten zu erzeugen wurde per Gruppenrichtlinien sämtliche verfügbaren Überwachungsrichtlinien aktiviert (Abb. 2b und 2c)



(a) streng geheime Projektdaten auf dem Netzlaufwerk



(b) Entsperrbefehl am Rechner **(c)** Anmeldeversuche überwachen

Abbildung 2: Vorbereitung des Dienstnotebooks

3.2.3 Privatnotebook

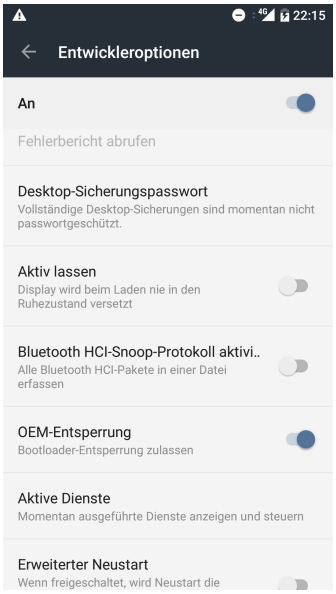
Herr K. besitzt einen privaten Rechner in Form eines Lenovo Yoga 920. Auf diesem Notebook ist Windows 10 Home in dem Build 19045.3758 installiert. Die Installation ist mit lediglich einer vom Standard abweichenden Einstellung vonstattengegangen: Es wurde keine Internetverbindung während der Installation bereitgestellt. Dadurch ist sichergestellt, dass es sich um eine lokale Installation handelt, bei welcher kein Microsoft-Konto notwendig ist. Erst nach Abschluss der Windows Installation durfte sich das Gerät mit dem Internet verbinden.
Bei dem verwendeten E-Mailprogramm fiel die Wahl auf *Thunderbird*, wo das private E-Mail-Konto von Herrn K. hinterlegt wurde.
Damit das später erzeugte Image nicht verschlüsselt vorliegt, galt es abschließend noch die *BitLocker*-Verschlüsselung der Festplatte zu deaktivieren. Außerdem wurde

die C-Partition mithilfe der Windows Datenträgerverwaltung auf 80 GB verkleinert, um das später erzeugte Image kleinzuhalten.

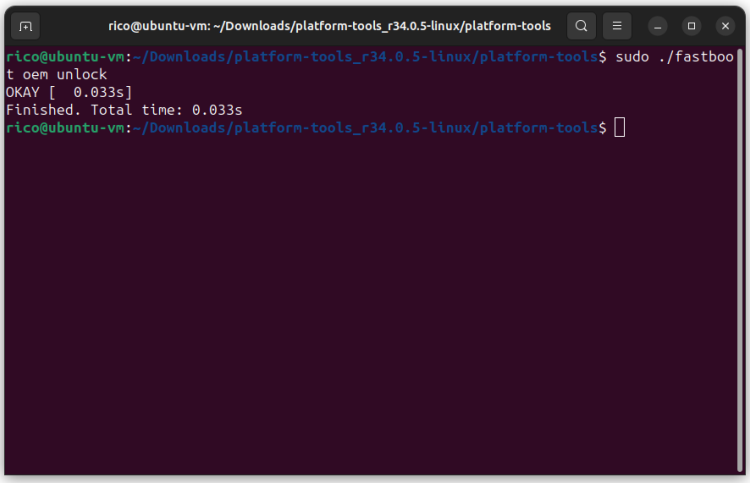
3.2.4 Handy

Als Telefon von Herrn Kurz wurde ein schon etwas älteres Oneplus 2 genutzt. Auf diesem befindet sich die aktuellste Originalfirmware (Android 6.0.1) des Herstellers. Da sich die Sicherung von Smartphones ohne teure Spezialhardware als außerordentlich schwierig erweisen kann, wurden einige Vorarbeiten vorgenommen. Im ersten Schritt wurde der Bootloader entsperrt. Hierdurch ist es möglich, vom Hersteller nicht signierte Software, wie z. B. TWRP[1], auf das Telefon aufzuspielen und über diese letztlich Root-Zugriff auf das zu erhalten. Dazu ist unter `Einstellungen/Über das Telefon` fünf Mal der Eintrag Build-Nummer anzutippen, um den Menüpunkt `Entwicklereinstellungen` freizuschalten. In diesem kann daraufhin die OEM–Entsperrung aktiviert werden (Abb. 3a). Anders als der Eintrag vielleicht vermuten lässt, ist der Bootloader nun noch nicht entsperrt, sondern zur Entsperrung freigegeben. Um diese tatsächlich durchzuführen, ist das Telefon im sogenannten Fastboot-Modus zu starten. Dazu müssen im ausgeschalteten Zustand gleichzeitig die Power- und Lauter-Tast gedrückt gehalten werden. Im Fastboot-Modus ist das Telefon per USB an einen Computer anzuschließen und mittels des Programms *fastboot* aus der Android Debug Bridge Toolsammlung[2] zu entsperren. Der ensprechende Befehl lautet `sudo fastboot unlock oem` (Abb. 3b). Auf dem Telefon erscheint nun noch ein chinesischsprachiger Warnhinweis, dass alle auf dem Telefon befindlichen Daten gelöscht werden (Abb. 3c). Spätestens hier wird ersichtlich, dass ohne diese Vorbereitungen eine spätere Sicherung der Daten im Rahmen dieser Arbeit nicht möglich gewesen wäre.

[1] `https://twrp.me/`
[2] `https://developer.android.com/tools/adb`



(a) Aktivierung unter Android



(b) Entsperrbefehl am Rechner

(c) Bestätigen des Warnhinweises

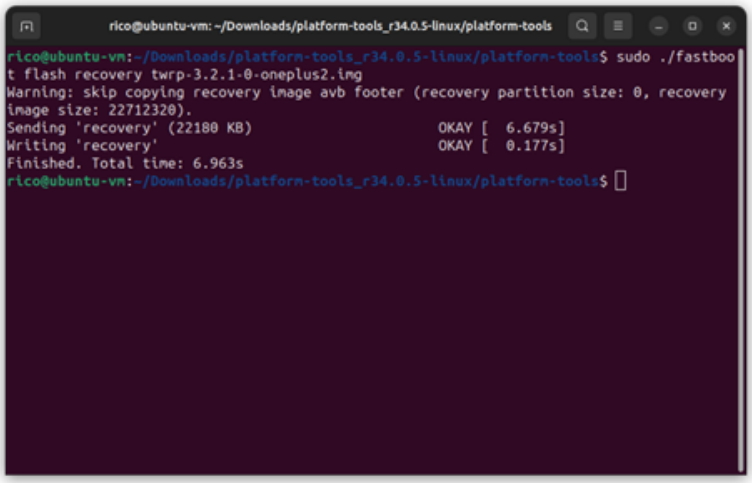
Abbildung 3: Entsperrung des Bootloaders, um Custom Recovery ROM aufspielen zu können

Danach wurde das Custom Recovery System TWRP in der Version 3.2.1.0[3] aufgespielt. Dies geschieht durch den Befehl `sudo fastboot flash recovery twrp-3.2.1-0-oneplus2.img` (Abb. 4a). Das Telefon muss sich hierzu wieder im Fastboot-Modus befinden und per USB angeschlossen sein. Nachdem der Vorgang erfolgreich abgeschlossen ist, kann durch gleichzeitiges Gedrückthalten der Power- und Leiser-

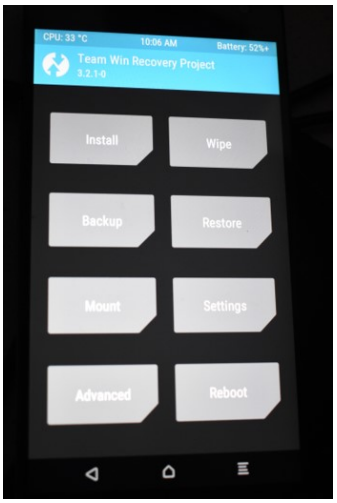
[3] `https://eu.dl.twrp.me/oneplus2/`

Taste das aufgespielte TWRP System gestartet werden (Abb. 4c). Am PC, an den das Telefon angeschlossen ist, kann nun mit dem Programm *adb* aus der ADB-Toolsammlung eine Root-Shell gestartet werden: `sudo adb shell`

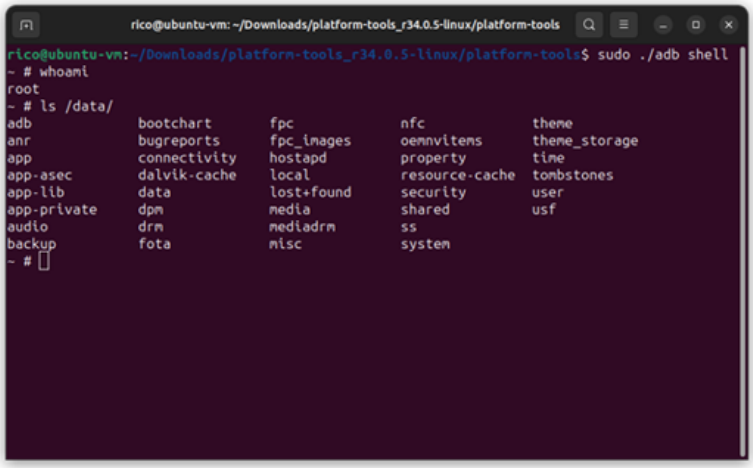
Somit ist nun die Erstellung eines physischen oder logischen Datenträgerabbilds und folglich auch eine forensische Untersuchung möglich. Auf die Erstellung des Abbilds wird im Abschnitt 5.2 näher eingegangen.



(a) TWRP flashen



(b) TWRP Oberfläche



(c) ADB Root-Shell

Abbildung 4: Flashen von TWRP und starten einer Root-Shell mit ADB

Im letzten Schritt wurde das Handy final eingerichtet. Es wurde zunächst eine SIM-Karte mit der Telefonnummer +49179******** eingelegt. Nun wurde das Android System gebootet. Da das Telefon durch die Entsperrung des Bootloaders auf Werkseinstellungen zurückgesetzt wurde, erfolgte anschließend die Ersteinrichtung

des Android Systems. Hierbei wurde eine Verbindung mit dem WLAN-Netz „Stark-Industries“ hergestellt und eine Anmeldung am Google-Account *heinrichk4575* vorgenommen. Über den Play-Store wurde WhatsApp installiert und ein Account mit der genannten Telefonnummer angelegt.

3.2.5 USB-Stick

Der USB-Stick wurde verwendet, um die Daten von dem Dienstlaptop auf das private Notebook zu transferieren. Aufgrund von räumlicher Trennung wurden zwei USB-Sticks verwendet, die in der folgenden Arbeit als einer behandelt werden.
Um die USB-Sticks für den Fall vorzubereiten, sind sie zunächst formatiert worden. Dabei wurde auf „Schnellformatierung“ verzichtet, um so viele Fragmente zu entfernen wie möglich. Als Erstes hat man die Daten auf den Dienstrechner von Herrn K. heruntergeladen und auf den ersten USB-Stick kopiert. Dadurch erscheint die Verwendung des Sticks in den Logfiles. Danach wurden die Daten auf einen vom Fall unabhängigen Rechner geladen und auf den zweiten USB-Stick kopiert. Abschließend wurde der zweite Stick an den privaten Rechner angeschlossen und die Daten darauf kopiert, um sie dann im späteren Verlauf in die Nextcloud von *ERWEE* hochzuladen.

3.2.6 Nextcloud

Für die Erstellung der Nextcloud Umgebung von *ERWEE* wurde die Container-Technologie Docker zusammen mit *Docker-Compose* verwendet. Docker bietet eine einfache Konsolenumgebung zur Verwaltung von Containern. Es ist entwickelt worden, um Anwendungen schnell und einfach in isolierten Umgebungen ausführen zu können. Mit Docker können Images erstellt, verwaltet und veröffentlicht werden. Es wurde im März 2013 veröffentlicht und bekommt immer mehr Aufmerksamkeit [3]. Es gibt ein großes Repository, den Docker Hub, welches viele Images verwaltet, ähnlich wie in .NET NuGet oder in Java das MvnRepository [2, 3].

Nach der Einführung von Docker hat sich der Bedarf ergeben, Container zu erstellen, die von anderen Container abhängen. Die meisten Anwendungen benötigen eine Datenbank, welche ebenfalls in einem Container laufen kann. Bei *ERWEE* ist dies ebenfalls der Fall, da hier eine *MariaDB* zusätzlich zur Nextcloud Instanz benötigt wird. Es müssen somit zwei Container parallel gestartet werden, wobei der eine vom anderen abhängig ist. *Docker-Compose* löst das Problem, mehrere abhängige Container auf einer Maschine zu verwalten. Anstatt mehrere einzelne Startargumente

für alle Container zu definieren, gibt es eine zentrale Konfiguration in YAML, die beschreibt, welche Container wie gestartet werden müssen. Durch diese Konfiguration ist es möglich, mehrere Container durch einen einzigen Befehl zu starten. In der Konfiguration können auch die allgemeinen Docker Einstellungen vorgenommen werden, wie beispielsweise das Definieren von *Ports* oder *bind mounts*. Die *Ports* dienen dazu, die Services im Container verfügbar zu machen, indem sie Anfragen an gewisse Ports des Host Systems an den Container weiterleiten [4].

Die Nextcloud für das Szenario wird mittels eines Apache Images, welches von den Entwicklern vorkonfiguriert ist und auf Docker Hub veröffentlicht wird, aufgesetzt. Außerdem wird eine MariaDB Datenbank, ebenfalls aus dem Docker Hub, verwendet. Die Installation erfolgte über die offizielle Anleitung von Nextcloud [5]. Für den Zugriff von außerhalb durch Herrn Lange und Herrn Kurz wurde zusätzlich die Tunnel Lösung von Cloudflare verwendet. Über diese Funktion wurde eine SSL-Verschlüsselung sichergestellt. Für die Einrichtung existiert ebenfalls ein Docker Image, welches mithilfe der offiziellen Anleitung in Betrieb genommen wurde [1]. Die gesamte *Docker-Compose* Konfiguration ist im Anhang eingefügt (Quellcode 1). In den Zeilen 9 und 23 sind jeweils die *bind mounts* definiert, in denen die Daten der jeweiligen Container gespeichert werden. Diese werden im Abschnitt 5.4 verwendet, um die Images zu erzeugen. Sie werden benötigt, da innerhalb von Containern keine persistenten Daten gespeichert werden sollten, da Sie im Update-Prozess zusammen mit den Containern gelöscht werden.

Beim erstmaligen Starten der Container über den Befehl `docker compose up`, werden verschiedene Daten innerhalb des *mounts* erstellt. In dem Fall von Nextcloud wird ein `config` Ordner erzeugt, in der die Konfigurationen von Nextcloud gespeichert werden. In diesem Ordner befindet sich unter anderem eine `config.php` in dem die vertrauenswürdigen Domains definiert werden. Es ist wichtig, dass die über Cloudflare verwendete Domain hier hinterlegt wird, damit die Nextcloud Instanz auch über diese Domain erreichbar ist. Andernfalls wird eine Nachricht angezeigt, dass der Zugriff über eine nicht vertrauenswürdige Domain erfolgt ist, woraufhin der Zugriff blockiert wird.

Nachdem die *ERWEE* Nextcloud Instanz vollständig eingerichtet ist, wird ein Benutzeraccount für Herrn Lange erstellt. Für die Einrichtung wird die zuvor erstellte Proton Mail Adresse von *ERWEE* verwendet. Die Erstellung des Benutzers ist in Abbildung 5 dargestellt.

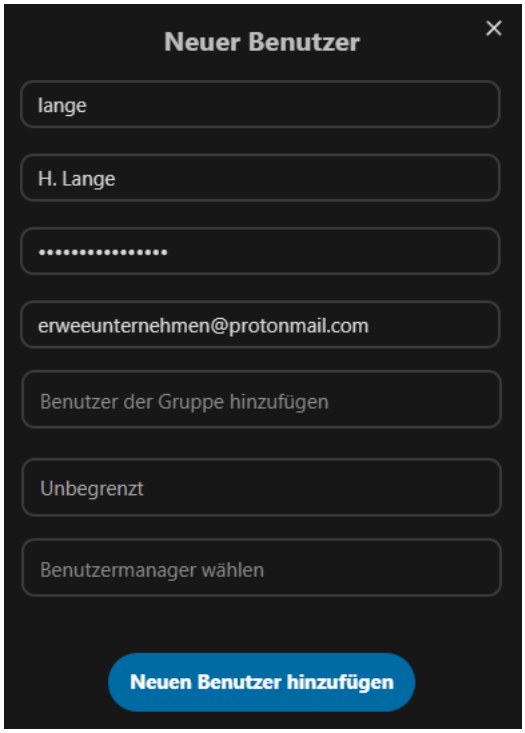


Abbildung 5: Nextcloud Benutzer von Herrn Lange erstellen

3.3 Durchführung des Vorfalls

In dem geschilderten Szenario treffen sich Herr Kurz und Herr Lange im Vorfeld an einem öffentlichen Ort und führen ein persönliches Gespräch. Dabei tauschen sie Kontaktinformationen aus. Herr Kurz sendet Herrn Lange über den erhaltenen Kontakt eine E-Mail, in der er vermittelt, dass er an dem Angebot interessiert ist (Abb. 6). Dafür wurde das zuvor installierte Programm *Thunderbird* verwendet. Anschließend bittet Herr Lange um die Kontaktaufnahme per WhatsApp, um die weitere Vorgehensweise zu besprechen.

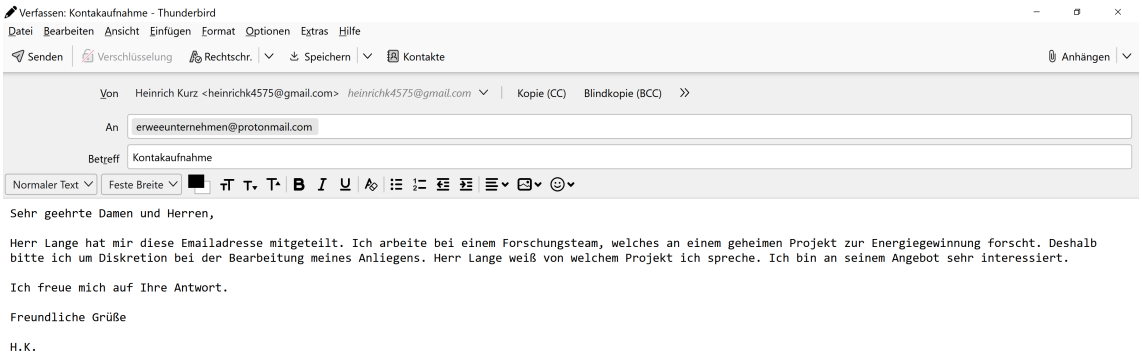


Abbildung 6: E-Mail Entwurf von Herrn Kurz an *ERWEE*

Parallel zur weiteren Durchführung des Vorfalls wurde ein fiktiver Chatverlauf zwischen Herrn Kurz und dem *ERWEE* Mitarbeiter Herrn Lange geführt (Abb. 7). Da für die Durchführung die privaten WhatsApp Accounts mehrerer Autoren dieser Arbeit genutzt wurden, wird deren Telefonnummer in den folgenden Betrachtungen ab der Vorwahl unkenntlich gemacht.

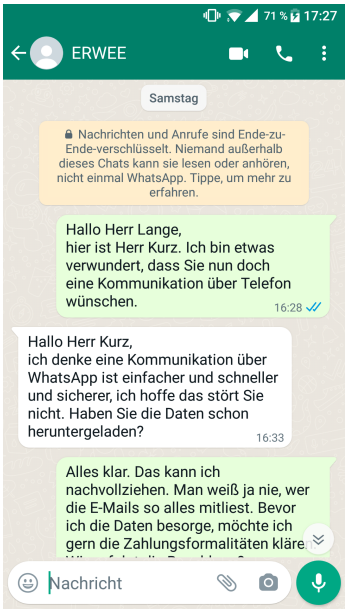


Abbildung 7: Chatverlauf

Nach den ersten Nachrichten über WhatsApp, in denen es unter anderem um die Bezahlung geht, wurden an dem Dienstnotebook von Herrn Kurz die Daten von dem verbundenen Netzwerklaufwerk auf die lokale Festplatte kopiert. Anschließend wurden die Daten verschlüsselt in einem ZIP-Archiv abgelegt und dieses auf den USB-Stick kopiert (Abb. 8).

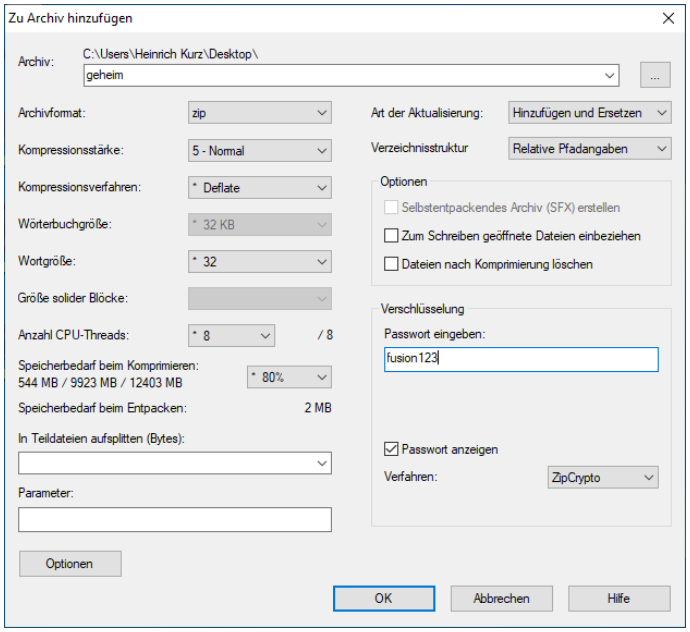


Abbildung 8: ZIP-Archiv erstellen

Parallel zur Beschaffung der Daten wurde der Freigabeordner über den Account von Herrn Lange in der Nextcloud von *ERWEE* erstellt. Dabei ist zu beachten, dass das Hochladen von Daten in den Freigabeordner erlaubt wird (Abb. 9). Anschließend sendete man den Link zu dem Freigabeordner über WhatsApp an Herrn Kurz.

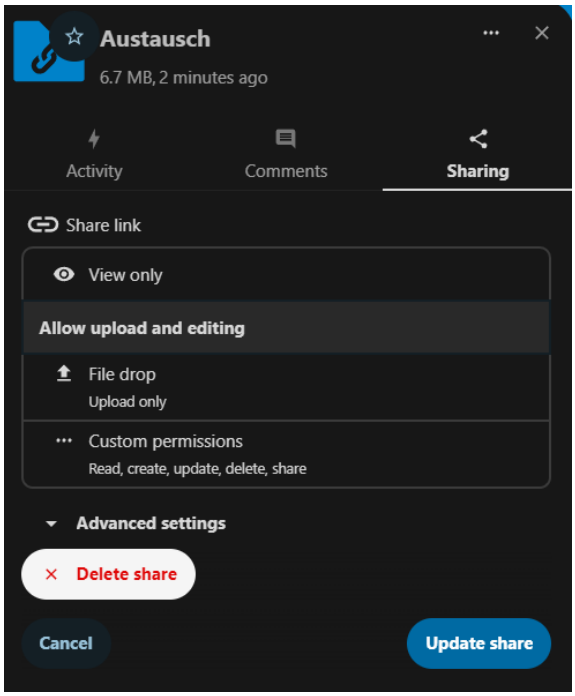


Abbildung 9: Freigabeordner erstellen

Der USB-Stick, welcher zuvor an dem Dienstnotebook angeschlossen war, wurde mit dem privaten Notebook von Herrn Kurz verbunden und die darauf enthaltene *geheim.zip* Datei auf das Notebook kopiert. Mit dem privaten Notebook wurde anschließend der Link zur Nextcloud von *ERWEE* geöffnet und die Datei in den Freigabeordner hochgeladen (Abb. 10). Dadurch, dass der Freigabeordner über einen Link geteilt wurde, war eine Anmeldung an der Nextcloud nicht notwendig.

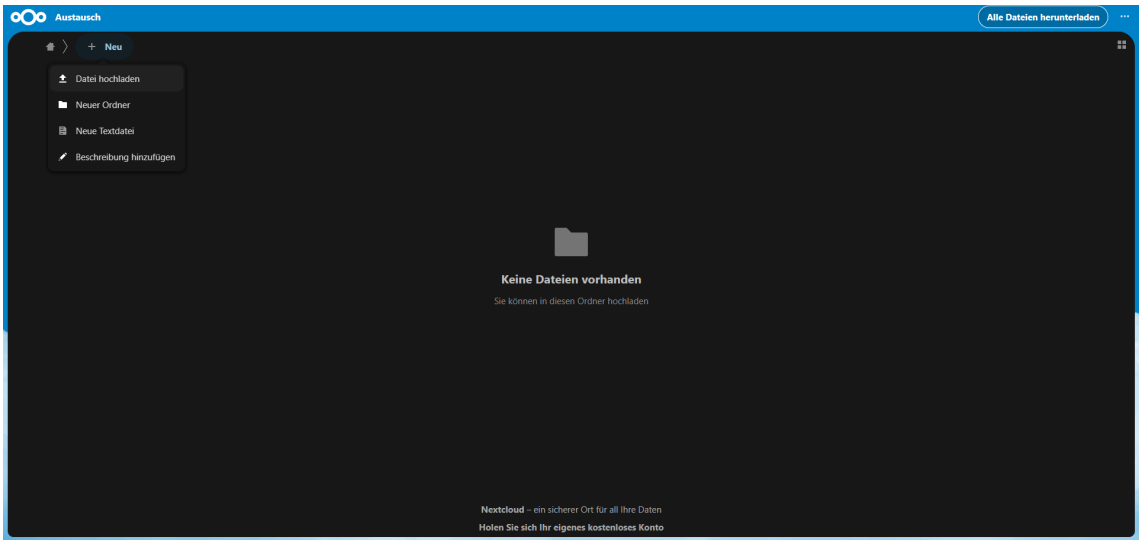


Abbildung 10: ZIP-Archiv hochladen

Anschließend endete das Gespräch über WhatsApp, nachdem Herr Lange Herrn Kurz darüber informiert hatte, dass er die Daten erhalten hat. Daraufhin wurden die Daten von dem USB-Stick, welcher am Notebook von Herrn Kurz angeschlossen war, gelöscht. Dies schließt die Durchführung des Vorfalls ab.

4 Forensisches Gutachten

4.1 Deckblatt

Gutachten

der IT-Forensik

Kriminalamt Friedenshof

Auftraggeber

Staatsanwaltschaft Hochschule Wismar

Aktenzeichen

1234/5678/2024

Sachverständige: Max Mustermann
Erika Mustermann

Abschluss: 19. März 2024

Kriminalamt Friedenshof • Musterstraße 1 • 23966 Wismar • Tel: +49 123 456789

4.2 Auftrag und juristische Fragestellung

Die Staatsanwaltschaft *Hochschule Wismar* beauftragt im Rahmen des Verdachtes der Industriespionage die Auswertung der unten aufgelisteten Asservate. Diese sollen forensisch untersucht und die Ergebnisse in einem forensischen Gutachten festgehalten werden.

Im Gutachten sollen folgende Fragestellungen beantwortet werden:

Asservat 01 (Dienstnotebook)

1. Welches Betriebssystem befindet sich auf dem Gerät und wann wurde es installiert?
2. Wann hat sich Herr Kurz zuletzt am System angemeldet?
3. Wie lauten die Zugangsdaten zum Benutzerkonto?
4. Hatte Herr Kurz mit dem Notebook Zugriff auf die Projektdateien?
5. Befinden sich Projektdateien auf dem Notebook?
6. Wurde Asservat 04 (USB-Stick) an das Gerät angeschlossen?
7. Wurden Daten von diesem Gerät aus auf Asservat 04 (USB-Stick) kopiert?

Asservat 02 (Privates Notebook)

1. Welches Betriebssystem befindet sich auf dem Gerät und wann wurde es installiert?
2. Wann hat sich Herr Kurz zuletzt am System angemeldet?
3. Wie lauten die Zugangsdaten zum Benutzerkonto?
4. Fand mithilfe von Asservat 02 (privates Notebook) für den Fall relevante Kommunikation statt?
5. Befanden sich für den Fall relevante Daten auf dem Gerät?
6. Wurde Asservat 04 (USB-Stick) an das Gerät angeschlossen?
7. Steht das Gerät in einer Verbindung zu Asservat 05 (Nextcloud)?

Asservat 03 (Telefon)

1. Fand eine Kommunikation zwischen Herrn Kurz und Herrn Lange statt?
2. Falls ja, was war Inhalt dieser Konversation?
3. In welchem Zeitraum fand die Konversation statt?

Asservat 04 (USB-Stick)

1. Befinden sich auf dem USB-Stick sachverhaltsrelevante Daten?

2. Falls ja, welche sind das und wann wurden sie auf den USB-Stick kopiert?

Asservat 05 (Nextcloud)

1. Welche Zugänge zur Nextcloud existieren?
2. Befinden sich Projektdateien in der Nextcloud?
3. Wurden Daten von Herrn Kurz auf die Nextcloud hochgeladen?
4. Wurden Daten von Herrn Lange von der Nextcloud heruntergeladen?

4.3 Zusammenfassung der Ermittlungsergebnisse

Asservat 01 (Dienstnotebook)

Das Dienstnotebook von Herrn Kurz konnte im eingeschalteten und entsperrten Zustand sichergestellt werden. Auf dem Gerät befindet sich das Betriebssystem Windows 10 Pro in der Version 22H2, welches am 06.01.2024 um 12:50 Uhr (GMT+1) installiert wurde. Aus dem RAM konnte zu dem Anmeldenamen „Heinrich Kurz“ das Anmeldepasswort „H3inrich“ ausgelesen werden. Unter dem Laufwerkbuchstaben Z: ist ein Netzlaufwerk zum Pfad `\\192.168.254.6\Projekt Fusion` eingebunden. Unter dieser Adresse sind im internen Netzwerk der Mitarbeiter die Projektdateien auf dem Server abgelegt. Es konnten ein ZIP-Archiv festgestellt werden, welches ebenfalls auf Asservat 04 und 05 aufgefunden wurde. An dem Computer wurde am 06.01.2024 um 16:30 Uhr ein USB-Gerät mit der Seriennummer 12082385003071, also derselben Seriennummer wie Asservat 04, angeschlossen. Aus den Logdateien der kürzlichen Aktivität geht hervor, dass eine Datei mit dem Namen *geheim.zip* auf einem unter dem Laufwerkbuchstaben E: eingebundenen Datenträger vorhanden war, auf welche um 16:58 Uhr zuletzt zugegriffen wurde. Artefakte, die ein Kopieren der ZIP-Datei mit den Projektdaten auf Asservat 04 belegen, konnten nicht gefunden werden.

Asservat 02 (Privates Notebook)

Das private Notebook von Herrn Kurz, wurde im ausgeschalteten Zustand sichergestellt. Es konnte jedoch ein Abbild des Datenträgers, welcher unverschlüsselt vorliegt, gemacht werden. Auf diesem Datenträger wurden zwei E-Mails sichergestellt, die am 06.01.2024 im Zeitraum von 16:11 Uhr und 16:27 Uhr verfasst bzw. erhalten wurden und eine Kontaktaufnahme zu Herrn Lange von *ERWEE* darstellen. Außerdem wurde das ZIP-Archiv *geheim.zip*, welches zuvor auf dem Dienstnotebook

gefunden wurde, sichergestellt. Abschließend konnte eine Verbindung von Asservat 02 (privates Notebook) an Asservat 05 (Nextcloud) am 06.01.2024 um 16:56 Uhr nachgewiesen werden.

Asservat 03 (Telefon)

Das Telefon ist mit einem Google-Account *heinrich4575@gmail.com* verknüpft. Auf dem Telefon befindet sich eine E-Mail Konversation mit *erweeunternehmen@protonmail.com*, über welche eine weitere Konversation mit der Telefonnummer +49176**** über den Messenger WhatsApp vereinbart wurde. Ein Kontakt mit der genannten Nummer ist auf dem Telefon unter dem Namen „ERWEE“ eingespeichert. Über den WhatsApp-Messenger fand mit diesem Kontakt ein Nachrichtenaustausch statt. Es wurde eine Zahlung von 25 Bitcoin von dem Kontakt „ERWEE“ an das Wallet 1EdYjbkqqPh4pdJiMwWTxyxZy9v5W4HbzW vereinbart. Im Gegenzug dazu sollten Daten unter der Adresse `https://cloud.k*****.de/s/AWd7bS5wai7RPgN` hochgeladen werden, was dem weiteren Konversationsverlauf zu Folge auch erfolgte. Weiterhin wurde ein Passwort „fusion123“ von Herrn Kurz an den Kontakt „ERWEE“ übermittelt, wobei es sich um das Verschlüsselungspasswort der übertragenen Daten handelt. Mit diesem Passwort ließ sich das in Asservat 01, 02, 04 und 05 aufgefundene ZIP-Archiv entpacken.

Asservat 04 (USB-Stick)

Es wurde ein USB-Stick mit der Seriennummer 2082385003071 sichergestellt. Auf dem Gerät wurde das Archiv *geheim.zip*, mit dem Erstellungsdatum 06.01.2024 um 16:43 Uhr (GMT+1) gefunden.

Asservat 05 (Nextcloud)

Die Nextcloud und die dazugehörige Datenbank wurden in einem Archiv gesichert. In der Benutzerdatenbank der Nextcloud existieren zwei Benutzerkonten. Zum einen der Benutzer „lange“ und zum anderen der Benutzer „admin“. Das ZIP-Archiv *geheim.zip* wurde ebenfalls auf der Nextcloud identifiziert. Dieses wurde am 06.01.2024 um 16:56:56 (GMT+1) in den zuvor durch Herrn Lange erstellten Freigabeordner hochgeladen.

Timeline

Asservat	Zeitpunkt	Aktion
02 (privates Notebook)	06.01.2024 16:11 Uhr	E-Mail von Herrn Kurz an *ERWEE* mit Bitte um Kontaktaufnahme
03 (Telefon)	06.01.2024 16:27 Uhr	E-Mail an Herrn Kurz mit Bitte um Kontakt per WhatsApp
03 (Telefon)	06.01.2024 16:27 Uhr	Kontaktaufnahme Herr Kurz → Herr Lange per WhatsApp
01 (Dienstnotebook)	06.01.2024 16:30 Uhr	Anschluss von Asservat 04 (USB-Stick) an Asservat 01 (Dienstnotebook)
03 (Telefon)	06.01.2024 16:42 Uhr	Aussage von Kurz, er werde die Daten beschaffen
01 (Dienstnotebook)	06.01.2024 16:42 Uhr	Aufruf 7-ZIP, möglicherweise Erstellen der ZIP-Datei mit Projektdaten auf USB-Stick
05 (Nextcloud)	06.01.2024 16:43 Uhr	Erstellung des Freigabeordners durch Herrn Lange
04 (USB-Stick)	06.01.2024 16:43 Uhr	Erstellung der *geheim.zip* auf dem Datenträger
02 (privates Notebook)	06.01.2024 16:51 Uhr	Erstellungszeitpunkt von *geheim.zip* auf dem Gerät
03 (Telefon)	06.01.2024 16:52 Uhr	Nachricht Kurz → Lange, er habe die Daten besorgt und mit Passwort gesichert
02 (privates Notebook)	06.01.2024 16:56 Uhr	Verbindung zu Asservat 05 (Nextcloud)
05 (Nextcloud)	06.01.2024 16:56 Uhr	Upload von *geheim.zip* auf die *ERWEE* Nextcloud
03 (Telefon)	06.01.2024 16:57 Uhr	Nachricht Kurz → Lange, dass Daten hochgeladen wurden

Tabelle 1: Timeline (Zeiten in GMT+1)

4.4 Untersuchungsobjekte

Objekt	Dateien	Hashwert (MD5)
Asservat 01	Disk_c.001 memdump.mem	fc08da503af5cceb8ab5846ca5eebc3e cdb79b8caae65bca52e94f3908eff9fb
Asservat 02	laptop_img_obl.img	86d9dcf5d96bc3c836be13f6b94a16bd
Asservat 03	OnePlus...DM-0.raw	55b4747b60b731893a7769befd261f71
Asservat 04	usb_img.img	0145b0d9b5b5abfdacd3a154176c9c7d
Asservat 05	docker-volumes.tar	cb374dacccf51e313e1cf38ea9a8de08

Tabelle 2: Untersuchungsobjekte

Die folgende Tabelle enthält die (MD5-)Hashwerte der wichtigsten Dateien der Untersuchung.

Datei/Archiv	Hashwert (MD5)
geheim.zip	acaf2ccfd6e53a18754ab693cacabe79
Blueprint1.jpg	d8bb54369bb45164b4bb74b8d6a9c498
Blueprint2.jpg	6044d36544614c371c8ef38b02216b53
Blueprint3.jpg	fde71af0f5c19279b19f4b399dc6f4db
Presentation.pdf	64723e68af7c7f9eebe670559cb1188b
PSFC JA-15-32.pdf	c7e2d1c273e2d2aea71ab49feb0ef9a1

Tabelle 3: Hashwerte

4.5 Untersuchungswerkzeuge

Name	**Version**	**Funktion**
Magnet Axiom	7.8.0.38310	All-in-One-Lösung zur forensischen Untersuchung von Computern und mobilen Geräten
FTK Imager	4.7.1.2	Programm zum Erzeugen phsyischer und logischer Datenträgerabbilder, RAM-Dumps und zur forensischen Analyse von diesen
Autopsy	4.20.0	Grafische Oberfläche der forensischen Software „The Sleuth Kit“ zur forensischen Analyse von Datenträgerabbildern.
Mimikatz	2.2.0	Tool, um unter Windows zwischengespeicherte Anmeldeinformationen auszulesen und anzuzeigen
Registry Explorer	2.0.0.0	Tool zum Auslesen und Anzeigen von Windows Dateien der Windows Registrierungsdatenbank
dd	8.32	Tool zum Kopieren einer Datei, Konvertieren und Formatieren
tar	1.34	Tool zum Archivieren von Dateien und Ordnern
Docker	25.0.3	Tool zum Verwalten von Containern
DBeaver	23.3.5	Tool zum Verwalten von Datenbanken

Tabelle 4: Untersuchungswerkzeuge

4.6 Untersuchung der Asservate

Im Folgenden werden alle Asservate untersucht und die Ergebnisse protokolliert. Ziel ist es die zuvor aufgeworfenen Fragestellungen zu beantworten und so einen möglichen Ablauf des Sachverhaltes zu rekonstruieren.

4.6.1 Asservat 01 - Dienstnotebook von Herrn Kurz

Betriebssysteminformationen

Da das Notebook zum Zeitpunkt der Durchsuchung angeschaltet und entsperrt war, wurde dieser Umstand direkt genutzt und direkt am System eine erste Untersuchung durchgeführt, bevor einige Daten (RAM-Speicher) durch das Ausschalten des Geräts unwiederbringlich verloren gehen. Es wurde ein vorbereiteter USB-Stick an das Gerät angeschlossen. Auf diesem befand sich eine Kopie der Software FTK Imager. Diese wurde direkt vom Stick gestartet und ein RAM-Dump erzeugt.

Das Erscheinungsbild des Systems ließ schon ein Windows 10 Betriebssystem vermuten. Gewissheit über diese Annahme lieferte schließlich die Analyse der Imagedateien. Aus dem Festplattenabbild wurde die Datei der Registrierungsdatenbank `C:\Windows\System32\config\SOFTWARE` exportiert und mit dem Programm *Registry Explorer* eingelesen. Innerhalb der Datenbank sind unter `Root\Microsoft\Windows NT\CurrentVersion` nähere Informationen zum Betriebssystem zu finden (Abb. 11). Darin zu finden sind auch die Zeitstempel der Installation: `InstallDate` und `InstallTime`. Beide enthalten die selben Werte, einmal als UNIX-Zeitstempel und einmal als 64 Bit Wert (Windows FILETIME). Beide Werte zeigen den 06.01.2024 12:50 lokaler Zeit (GMT+1) als Installationszeitpunkt (Abb. 12).

SystemRoot	RegSz	C:\Windows
BaseBuildRevisionNumber	RegDword	1
BuildBranch	RegSz	vb_release
BuildGUID	RegSz	ffffffff-ffff-ffff-ffff-ffffffffffff
BuildLab	RegSz	19041.vb_release.191206-1406
BuildLabEx	RegSz	19041.1.amd64fre.vb_release.191206-1406
CompositionEditionID	RegSz	Enterprise
CurrentBuild	RegSz	19045
CurrentBuildNumber	RegSz	19045
CurrentMajorVersionNumber	RegDword	10
CurrentMinorVersionNumber	RegDword	0
CurrentType	RegSz	Multiprocessor Free
CurrentVersion	RegSz	6.3
EditionID	RegSz	Professional
EditionSubManufacturer	RegSz	
EditionSubstring	RegSz	
EditionSubVersion	RegSz	
InstallationType	RegSz	Client
InstallDate	RegDword	1704541839
ProductName	RegSz	Windows 10 Pro
ReleaseId	RegSz	2009
SoftwareType	RegSz	System
UBR	RegDword	3803
PathName	RegSz	C:\Windows
ProductId	RegSz	00330-80000-00000-AA015
DigitalProductId	RegBinary	A4-00-00-00-03-00-00-00-30-30-33-33-30-2D-38-30-30-30-30-2D-30-30-30-30-30-2D-41-41-30-31-35-00-EC-0C-00-00-5B-54-48-5D-58-31-39-2D...
DigitalProductId4	RegBinary	F8-04-00-00-04-00-00-00-30-00-33-00-36-00-31-00-32-00-2D-00-30-00-33-00-33-00-30-00-38-00-2D-00-30-00-30-00-30-00-30-2D-00-30-00-30-00-...
DisplayVersion	RegSz	22H2
RegisteredOwner	RegSz	Heinrich Kurz
RegisteredOrganization	RegSz	
InstallTime	RegQword	133490154392129562

Abbildung 11: Informationen zum installierten Betriebssystem

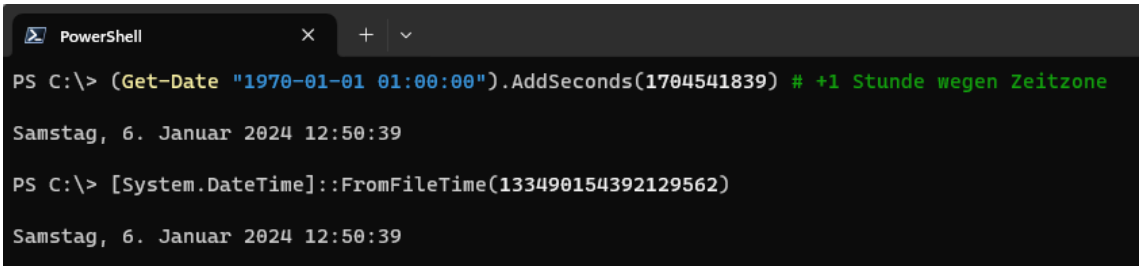


Abbildung 12: Installationszeitpunkt des Betriebssystems

Zeitpunkt der letzten Anmeldung

Analog zum Vorgehen bei der Analyse des installierten Betriebssystems wurde die Datei `C:\Windows\System32\config\SAM` exportiert. In dieser Datenbank sind unter `Root\SAM\Domains\Account\Users` Informationen über die vorhandenen Benutzerkonten zu finden. Demnach hat sich Herr Kurz zuletzt am 06.01.2024 um 17:25 Uhr (GMT+1) am System angemeldet (nach Addition einer Stunde aufgrund der lokalen Zeitzone, Abb. 13).

User Id	User N...	Invalid Lo...	Total Login Count	Last Login Time	Last Password Change	Created On	Last Incorrect Password
1001	Heinrich Kurz	0	8	2024-01-05 16:25:27	2024-01-06 11:59:23	2024-01-06 11:59:23	2024-01-06 12:04:18

Abbildung 13: Zeitpunkt der letzten Anmeldung von Herrn Kurz (MEZ)

Anmeldedaten

Zum Auslesen von Anmeldedaten wurde auch der Umstand genutzt, dass das System noch eingeschaltet war. Die ebenfalls auf dem USB-Stick abgelegte Software Mimikatz gestartet, um im Hauptspeicher vorgehaltene Passwörter auszulesen. Diese lieferte für den Benutzer „Heinrich Kurz“ das Anmeldekennwort „H3inrich“ (Abb. 14).

```
mimikatz 2.2.0 x64 (oe.eo)

  .#####.   mimikatz 2.2.0 (x64) #18362 Feb 29 2020 11:13:36
 .## ^ ##.  "A La Vie, A L'Amour" - (oe.eo)
 ## / \ ##  /*** Benjamin DELPY `gentilkiwi` ( benjamin@gentilkiwi.com )
 ## \ / ##       > http://blog.gentilkiwi.com/mimikatz
 '## v ##'       Vincent LE TOUX            ( vincent.letoux@gmail.com )
  '#####'        > http://pingcastle.com / http://mysmartlogon.com   ***/

mimikatz # log
Using 'mimikatz.log' for logfile : OK

mimikatz # privilege::debug
Privilege '20' OK

mimikatz # sekurlsa::logonpasswords

Authentication Id : 0 ; 6564944 (00000000:00642c50)
Session           : Interactive from 4
User Name         : Heinrich Kurz
Domain            : NB003-HK
Logon Server      : NB003-HK
Logon Time        : 09.02.2024 17:16:27
SID               : S-1-5-21-365240803-2440143457-561151489-1001
        msv :
         [00000003] Primary
         * Username : Heinrich Kurz
         * Domain   : NB003-HK
         * NTLM     : 1902babf328fc32939204d268640d594
         * SHA1     : 66d9e96afaaacfd41d40cc9c03466322aaab6208
         * DPAPI    : 66d9e96afaaacfd41d40cc9c03466322
        tspkg :
        wdigest :
         * Username : Heinrich Kurz
         * Domain   : NB003-HK
         * Password : H3inrich
        kerberos :
         * Username : Heinrich Kurz
         * Domain   : NB003-HK
         * Password : (null)
        ssp :   KO
        credman :
```

Abbildung 14: Anmeldepasswort für Benutzer Heinrich Kurz

Zugriff auf Projektdateien

In der Datei `NTUSER.DAT` protokolliert das Betriebssystem Windows einige Aktivitäten des Nutzers. Hierin ist auch vermerkt, dass unter dem Laufwerkbuchstaben Z: ein Netzlaufwerk zum Pfad `\\192.168.254.6\Projekt Fusion` angelegt ist. (Abb. 15)

Source Name	S	C	O	Local Path	Remote Path	Data Source
NTUSER.DAT				Network\Z	\\192.168.254.6\Projekt Fusion	Disk_c.001
NTUSER.DAT				Network\Z	\\192.168.254.6\Projekt Fusion	Disk_c.001

Abbildung 15: Eingebundenes Netzlaufwerk

Projektdaten auf dem Notebook

Mithilfe von *Autopsy* wurden in dem Image sechs Dateien gefunden (Abb. 16). Bei diesen handelt es sich exakt um die auf Asservat 02, 04 und 05 festgestellten Dateien (Hashwerte stimmen überein). Die Dateien wurden um 16:42 Uhr erstellt und der letzte Zugriff fand ebenfalls um 16:42 statt. Dieser Zeitpunkt entspricht dem Aufruf von 7-ZIP. Die Datei wurde also auf das Notebook kopiert und kurz darauf wurde das verschlüsselte *geheim.zip* Archiv erstellt.

Name	S	C	O	Modified Time	Change Time	Access Time	Created Time
Blueprint1.jpg				2024-01-06 12:21:49...	2024-01-06 15:42:59...	2024-01-06 15:42:44...	2024-01-06 15:42:09 ...
Blueprint2.jpg				2024-01-06 12:22:07...	2024-01-06 15:42:59...	2024-01-06 15:42:44...	2024-01-06 15:42:09 ...
Blueprint3.jpg				2024-01-06 12:22:21...	2024-01-06 15:42:59...	2024-01-06 15:42:44...	2024-01-06 15:42:09 ...
Presentation.pdf				2024-01-06 12:25:12...	2024-01-06 15:42:59...	2024-01-06 15:42:50...	2024-01-06 15:42:09 ...
PSFC JA-15-32.pdf				2024-01-06 12:32:11...	2024-01-06 15:42:59...	2024-01-06 15:42:50...	2024-01-06 15:42:09 ...

Abbildung 16: Projektdateien (Zeiten in MEZ)

Anschließen von USB-Stick

In der Registry-Datenbank werden an das System angeschlossene USB-Geräte aufgezeichnet. Hieraus ist ersichtlich, dass am 06.01.2024 um 15:30 Uhr (MEZ) ein Flash-Speicher mit der Seriennummer 12082385003071 angeschlossen wurde. (Abb. 17)

SYSTEM		0	2024-01-06 12:12:32 GMT	Intel Corp.	Bluetooth wireless interface	5&2ad42009&0&4	Disk_c.001
SYSTEM		0	2024-01-06 12:12:32 GMT	Intel Corp.	Integrated Rate Matching Hub	5&255532938&0&1	Disk_c.001
SYSTEM		0	2024-01-06 15:30:14 GMT	Silicon Motion, Inc. - Taiwan (formerly Feiya Technology Corp.)	Flash Drive	12082385003071	Disk_c.001
SYSTEM		0	2024-01-06 15:30:14 GMT	Silicon Motion, Inc. - Taiwan (formerly Feiya Technology Corp.)	Flash Drive	12082385003071	Disk_c.001

Abbildung 17: Eintrag eines USB-Geräts mit Seriennummer 12082385003071

Kopieren der Dateien auf USB-Stick

Ein eindeutiger Nachweis, dass die Projektdaten von diesem Notebook auf den USB-Stick kopiert wurden, ist nicht gegeben. Jedoch deuten einige Spuren darauf hin. Zum einen, dass der USB-Stick, auf welchem die Projektdateien gefunden wurden, an das Notebook angeschlossen wurden. Zum anderen ist unter dem Pfad `Users\Heinrich Kurz\AppData\Roaming\ Microsoft\Windows\Recent` eine Verknüpfung zu einer auf einem Datenträger E: gespeicherten Datei namens *geheim.zip* zu finden, auf welche am 06.01.2024 um 16:42 Uhr (GMT+1) zugegriffen wurde (Abb. 18). Dies entspricht dem Namen der auf dem USB-Stick gefundenen, die Projektdateien enthaltenen ZIP-Datei. Außerdem ist auf dem Notebook das Archivierungsprogramm 7-ZIP installiert, welches das Erstellen eines passwortgeschützten ZIP-Archivs ermöglicht. Dieses Programm wurde um 15:43 Uhr (MEZ) ausgeführt (Abb. 19).

Type	Value	Source(s)
Path	E:\geheim.zip	RecentActivity
Path ID	-1	RecentActivity
Date Accessed	2024-01-06 15:58:38 MEZ	RecentActivity
Source File Path	/img_Disk_c.001/Users/Heinrich Kurz/AppData/Roaming/Microsoft/Windows/Recent/geheim.lnk	
Artifact ID	-9223372036854775800	

Abbildung 18: Verknüpfung zur *geheim.zip* Datei

Type	Value
Program Name	7ZG.EXE
Path	/PROGRAM FILES/7-ZIP
Date/Time	2024-01-06 15:43:51 GMT
Count	4
Comment	Prefetch File
Source File Path	/img_Disk_c.001/Windows/Prefetch/7ZG.EXE-0F8C4081.pf
Artifact ID	-9223372036854770951

Abbildung 19: Ausführen von 7-ZIP

4.6.2 Asservat 02 - Privates Notebook von Herrn Kurz

Betriebssysteminformationen

Das Notebook wurde im ausgeschalteten Zustand sichergestellt. Deshalb wurde eine zuvor vorbereitete Festplatte, auf welcher Ubuntu in der Version 22.04 LTS installiert war, verwendet, um mithilfe des Commandline-Tools *dd* ein Abbild des Datenträgers des Notebooks zu erstellen. Dieses Abbild kann mit der Software *Autopsy* analysiert werden. Um die Informationen des Betriebssystems zu erlangen, kann in *Autopsy* das Image ausgewählt und der Pfad `Windows\System32\config\SOFTWARE` geöffnet werden. Innerhalb dieser Datenbank ist es möglich, ebenfalls unter Zuhilfenahme von `Autopsy`, unter `Root\Microsoft\Windows NT\CurrentVersion` die Betriebssysteminformationen, wie Name und Installationszeitpunkt, zu extrahieren (Abb. 20). Folglich handelt es sich bei dem vorliegenden Betriebssystem um Windows 10 Home in der Version 22H2, welches am 12. Dezember 2023 um 18:57 Uhr lokaler Zeit (GTM+1) installiert wurde.

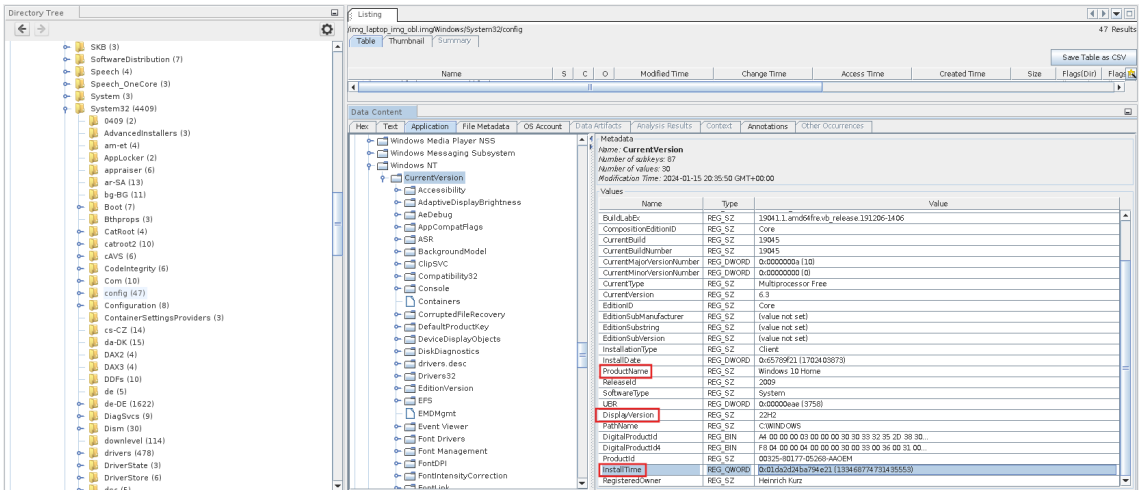


Abbildung 20: Betriebssysteminformationen des privaten Notebooks

Zeitpunkt der letzten Anmeldung

Auf Basis des vorhandenen Images kann keine Aussage über die letzte Anmeldung von Herrn K. getroffen werden. Die Anmeldeversuche an seinem privaten Laptop wurden nicht protokolliert, da dafür im Vorfeld eine Einstellung am Gerät durch Herrn Kurz hätte vorgenommen werden müssen. Es wurde jedoch auf dem PC das ZIP-Archiv *geheim.zip* gefunden, welches ebenfalls auf dem Dienstnotebook von Herrn Kurz festgestellt wurde. Anhand der letzten Bearbeitungszeit, 06.01.2024 um

17:58 Uhr (GMT+1) (Abb. 22), kann darauf geschlossen werden, dass Herr Kurz zu dieser Zeit an seinem PC angemeldet war.

Zugang zum Benutzerkonto von Herrn Kurz

Es ist möglich, mithilfe der Registry den Hashwert des Passwortes von Herrn Kurz zu extrahieren. Dieser kann dann über eine Brute-Force-Methode geknackt werden und so das Passwort darlegen. Diese Methode ist jedoch sehr aufwendig und nicht notwendig, da der Datenträger unverschlüsselt vorliegt und somit das Passwort nicht benötigt wird, um Einsicht in das Konto von Herrn Kurz zu erhalten.

Kommunikation mithilfe des Notebooks

Auf dem privaten Notebook von Herrn Kurz konnten zwei E-Mails festgestellt werden. Innerhalb der Datei `C:\Users\Heinrich Kurz\AppData\Roaming\Thunderbird\Profiles\jjl95m2o.default-release\ImapMail\imap.gmail.com\[Gmail\].sbd\Gesendet` befindet sich die E-Mail, die in Abbildung 21 dargestellt ist. In dieser, von Herrn Kurz am 06.01.2024 um 16:11 Uhr gesendeten E-Mail, bittet er darum, mit Herrn Lange in Verbindung gesetzt zu werden. Außerdem wurde die E-Mail gefunden, welche ebenfalls auf Asservat 03 (Handy) gefunden wurde und in Abbildung 25 dargestellt ist.

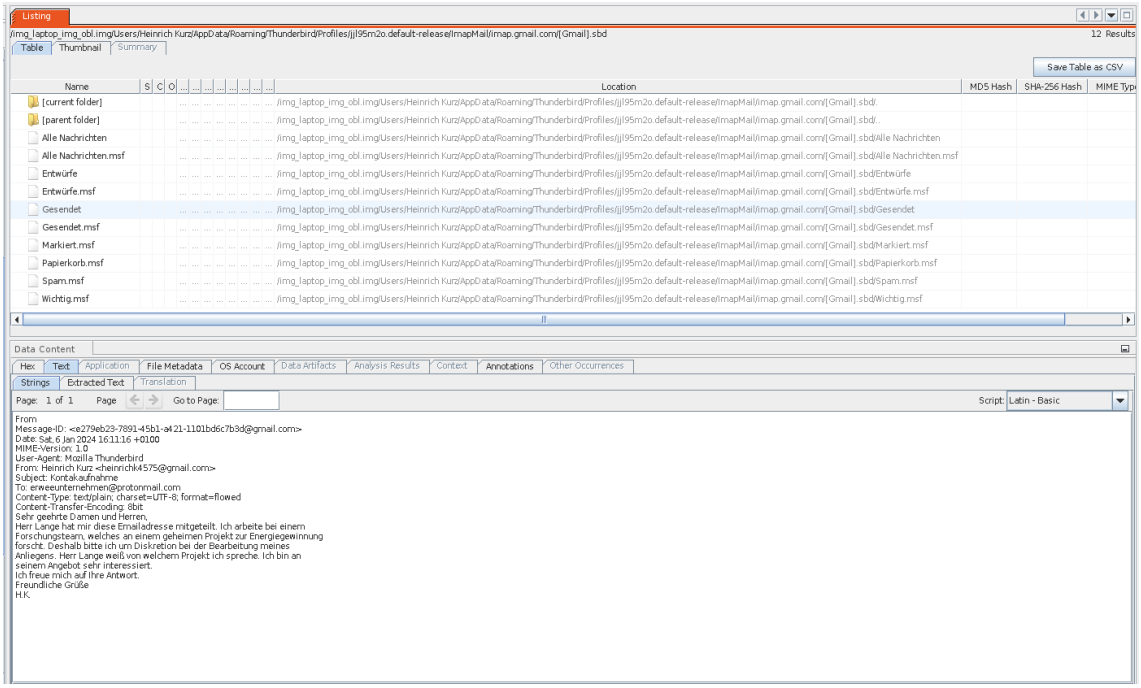


Abbildung 21: Gesendete E-Mail von Herrn Kurz an *ERWEE*

Projektdaten auf dem Notebook

Auf dem Gerät wurde das ZIP-Archiv festgestellt, welches zuvor ebenfalls auf Asservat 01 (Dienstnotebook) entdeckt wurde (Hashwerte stimmen überein). Das Archiv liegt jedoch im verschlüsselten Zustand vor. Mit dem Passwort, welches aus den Nachrichten, die auf Asservat 03 (Handy) gefunden wurden (Abb. 26), konnte es jedoch entschlüsselt werden. Das Archiv liegt unter dem Pfad `C:\Users\Heinrich Kurz\Desktop\geheim.zip` auf dem privaten Rechner. Der Erstellungs-, Bearbeitungs- und letzte Aufrufzeitpunkt sind in Abbild 22 zu sehen.

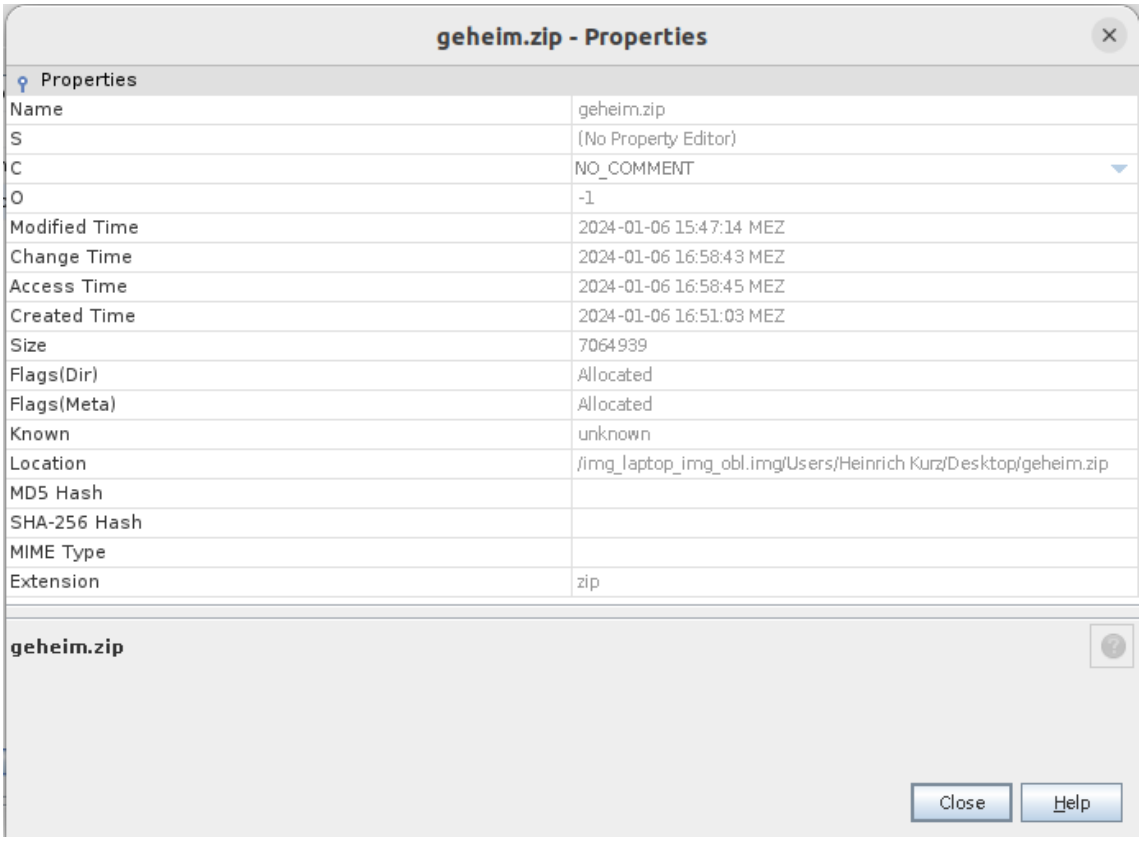


Abbildung 22: Eigenschaften von *geheim.zip*

Verbindung zwischen Asservat 02 (privates Notebook) und Asservat 04 (USB-Stick)

Es konnten auf dem System keine Spuren gefunden werden, dass Asservat 04 (USB-Stick) an dieses angeschlossen und Daten übertragen wurden.

Verbindung zwischen Asservat 02 (privates Notebook) und Asservat 05 (Nextcloud)

Auf dem privaten Notebook von Herrn Kurz konnte unter `C:\Users\Heinrich Kurz\AppD Data\Local\Microsoft\Edge\User Data\Default\History` der Verlauf des Webbrowsers von Herrn Kurz (Microsoft Edge) gesichert werden. Innerhalb des Verlaufes ist, neben für den Fall irrelevanten Einträgen, auch der Aufruf auf `https://cloud.k*****.de/s/AWd7bS5wai7RPgN` am 06.01.2024 um 16:56 Uhr (GMT+1) protokolliert. Dabei handelt es sich um dieselbe Webadresse, wie die, die in dem Nachrichtenverlauf auf Asservat 03 gefunden wurde und verwendet werden sollte, um die Dateien hochzuladen. Ein Protokoll des Hochladens konnte nicht sichergestellt werden, was aber durch eine generelle Nichtprotokollierung solcher Aktivitäten begründet ist.

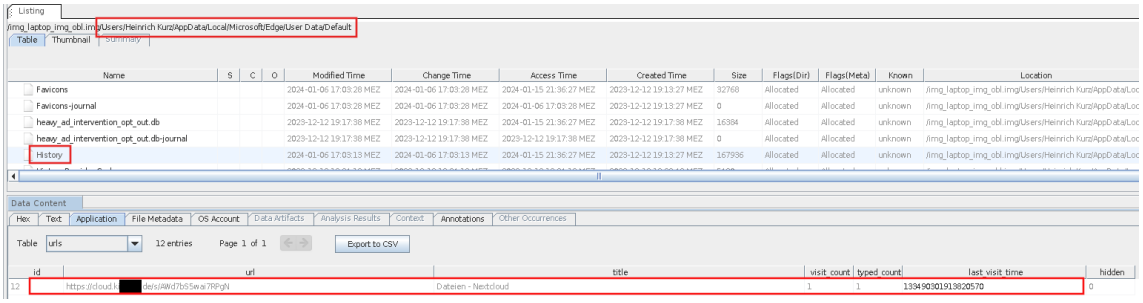
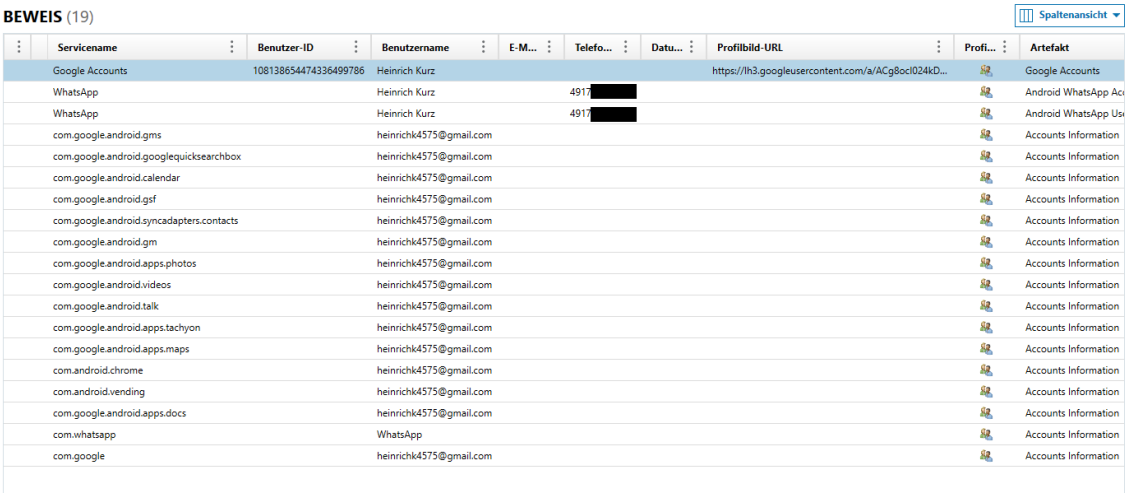


Abbildung 23: Browserverlauf (irrelevante Einträge wurden ausgeblendet)

4.6.3 Asservat 03 - Telefon von Herrn Kurz

Das Speicherabbild des Telefons von Herrn Kurz wurde mit der auf die Analyse von mobilen Geräte spezialisierte Software Magnet Axiom untersucht. Anhand mehrerer Dateien kann nachvollzogen werden, dass das Telefon an dem Google-Konto *heinrich4575@gmail.com* angemeldet und dass ein WhatsApp Account mit der Telefonnummer +49176**** vorhanden ist (Abb. 24).



BEWEIS (19) — Spaltenansicht

Servicename	Benutzer-ID	Benutzername	E-M...	Telefo...	Datu...	Profilbild-URL	Profi...	Artefakt
Google Accounts	108138654474336499786	Heinrich Kurz				https://lh3.googleusercontent.com/a/ACg8ocl024kD...		Google Accounts
WhatsApp		Heinrich Kurz		4917[redacted]				Android WhatsApp Ac
WhatsApp		Heinrich Kurz		4917[redacted]				Android WhatsApp Us
com.google.android.gms		heinrichk4575@gmail.com						Accounts Information
com.google.android.googlequicksearchbox		heinrichk4575@gmail.com						Accounts Information
com.google.android.calendar		heinrichk4575@gmail.com						Accounts Information
com.google.android.gsf		heinrichk4575@gmail.com						Accounts Information
com.google.android.syncadapters.contacts		heinrichk4575@gmail.com						Accounts Information
com.google.android.gm		heinrichk4575@gmail.com						Accounts Information
com.google.android.apps.photos		heinrichk4575@gmail.com						Accounts Information
com.google.android.videos		heinrichk4575@gmail.com						Accounts Information
com.google.android.talk		heinrichk4575@gmail.com						Accounts Information
com.google.android.apps.tachyon		heinrichk4575@gmail.com						Accounts Information
com.google.android.apps.maps		heinrichk4575@gmail.com						Accounts Information
com.android.chrome		heinrichk4575@gmail.com						Accounts Information
com.android.vending		heinrichk4575@gmail.com						Accounts Information
com.google.android.apps.docs		heinrichk4575@gmail.com						Accounts Information
com.whatsapp		WhatsApp						Accounts Information
com.google		heinrichk4575@gmail.com						Accounts Information

Abbildung 24: Google und WhatsApp Account auf Telefon

Aus der Datei `data/com.google.android.gm/databases/bigTopDataDB.-126557443` lässt sich eine um 16:27 Uhr (GMT+1) empfangene Mail von *erweeunternehmen@protonmail.com* an *heinrich4575@gmail.com* rekonstruieren (Abb. 25).

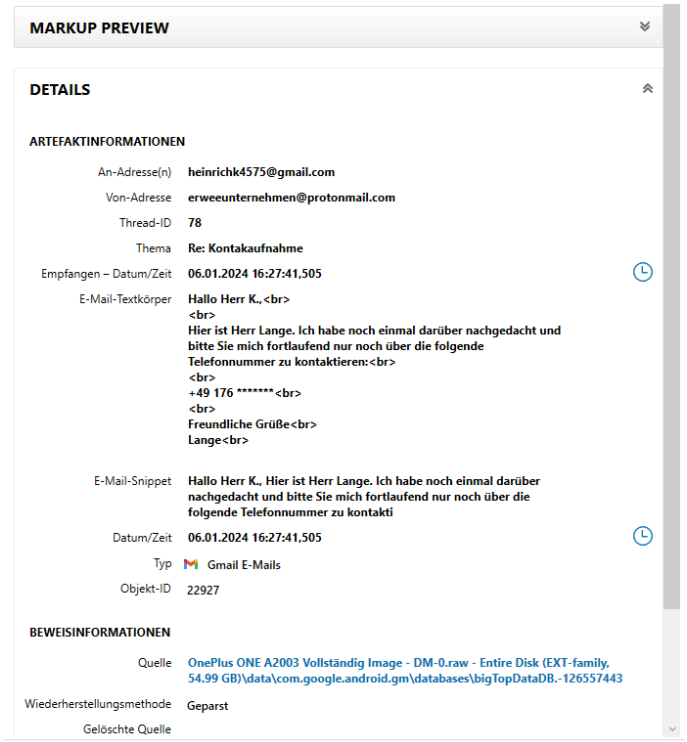


Abbildung 25: E-Mailverlauf zwischen Herrn Lange und Herrn Kurz

Der Nachrichtenverlauf innerhalb des Messengers WhatsApp wird durch Axiom automatisch aus den beiden SQLite Datenbanken `/data/com.whatsapp/databases/msgstore.db` und `/data/com.whatsapp/databases/wa.db` aufbereitet. Den Nachrichtenverlauf zeigt Abbildung 26. Die Unterhaltung in diesem Messenger fand demnach am 06.01.2024 zwischen 16:28 und 17:00 Uhr (GMT+1) statt. Der Inhalt wurde bereits in Abschnitt 4.3 zusammengefasst.

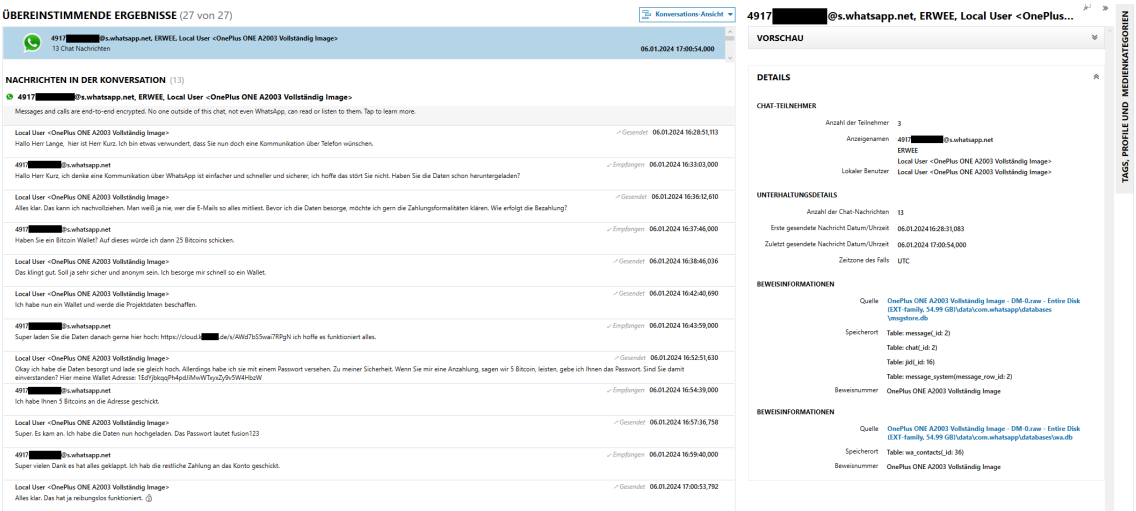


Abbildung 26: WhatsApp Chatverlauf zwischen Herrn Kurz und Herrn Lange

4.6.4 Asservat 04 - USB-Stick

Projektdaten auf dem USB-Stick

Mithilfe eines externen Notebooks und dem Commandline-Tool *dd* wurde ein Image von dem gefundenen USB-Stick mit der Seriennummer 12082385003071 erstellt. Dieses Image konnte mit der Software *Autopsy* analysiert werden. Auf dem Datenträger konnte die *geheim.zip* festegestellt werden, welche zuvor auf dem Dienstnotebook gefunden wurde (Hashwerte stimmen überein). Das ZIP-Archiv lag jedoch im gelöschten Zustand vor. Aufgrund der Eigenschaften des Archivs kann festgestellt werden, dass dieses am 06.01.2024 um 16:43 Uhr (GMT+1) erstellt, also auf den USB-Stick kopiert wurde (Abb. 27).

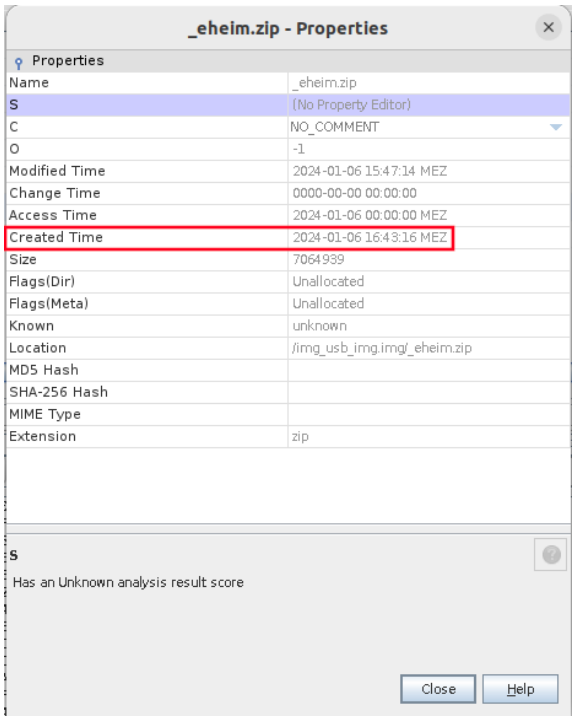


Abbildung 27: Eigenschaften der gelöschten *geheim.zip* auf Asservat 04 (USB-Stick)

4.6.5 Asservat 05 - Nextcloud

Zugänge

Für die Analyse der Datenbank wurde das Tool *DBeaver* verwendet. Die vorhandenen Zugänge zur Nextcloud konnten in der Datenbanktabelle `oc_users` gefunden werden (Abb. 28). Dabei wurde herausgefunden, dass zwei Benutzer existieren. Zum einen der Benutzer „lange“ und zum anderen der „admin“ Benutzer.

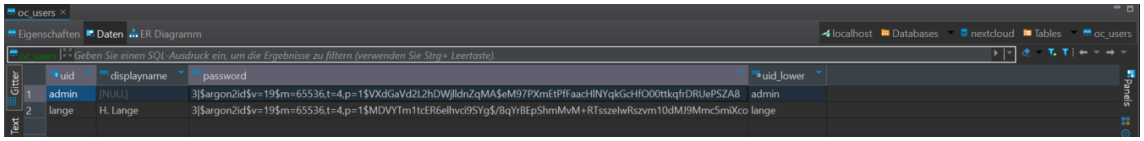


Abbildung 28: Zugänge zur Nextcloud

Projektdateien auf der Nextcloud

Mittels des Commandline-Tools *tar* wurde ein Archiv der gesamten Daten von der Nextcloud und der MariaDB erstellt. Dieses Archiv konnte neben der speziell benötigten Datenbankanalyse der MariaDB ebenfalls in *Autopsy* geladen werden. Das ZIP-Archiv *geheim.zip* konnte in dem `data` Ordner unter dem Benutzer „lange“ gefunden werden (Abb. 29). Ebenfalls stimmt der Hashwert des Archivs mit denen der Archive auf den anderen Asservaten überein und die Datei ist ebenfalls verschlüsselt. Mit dem Passwort, welches auf Asservat 03 (Handy) gefunden wurde konnte die Datei entschlüsselt werden, wie es schon der Fall bei den vorherigen Asservaten war.

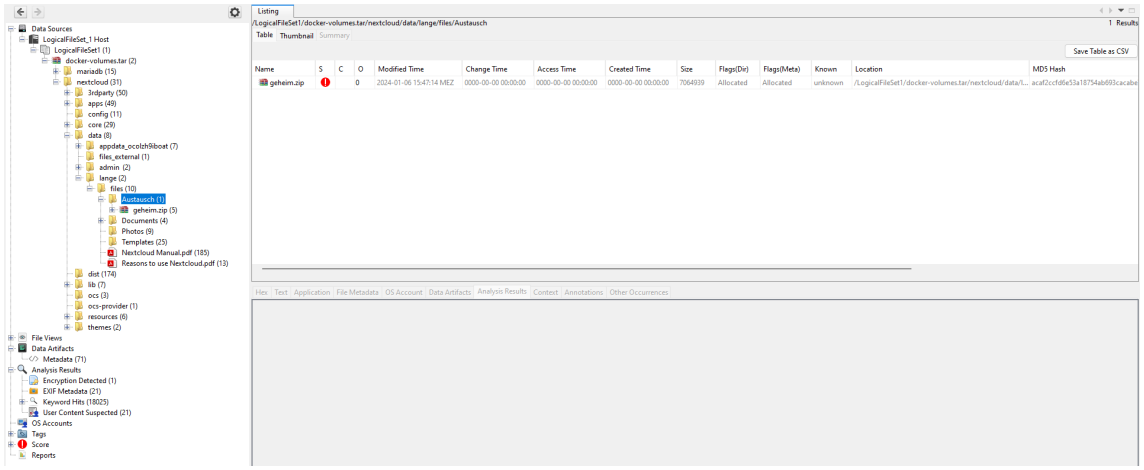


Abbildung 29: *geheim.zip* auf der Nextcloud

Upload der Projektdaten

Um zu prüfen, ob Daten in die Nextcloud hochgeladen wurden, wurde die Tabelle `oc_activity` analysiert, in der sämtliche Aktivitäten der Benutzer in der Nextcloud gespeichert werden. Dabei konnte festgestellt werden, dass die Datei *geheim.zip* am 06.01.2024 um 16:56:56 (GMT+1) hochgeladen wurde (Abb. 30). Innerhalb der Nextcloud DB werden Zeiten in der Unixzeit gespeichert. Aus diesem Grund musste der Wert 1704556616 umgerechnet werden. Auffällig ist, dass der Eintrag keinen eingetragenen Benutzer besitzt. Dies liegt daran, dass sie ohne eine Anmeldung in den Freigabeordner von Herrn Lange hochgeladen wurde. Es wurden keine weiteren Details über das verwendete Gerät oder die IP-Adresse, von der aus die Datei hochgeladen wurde, gefunden.

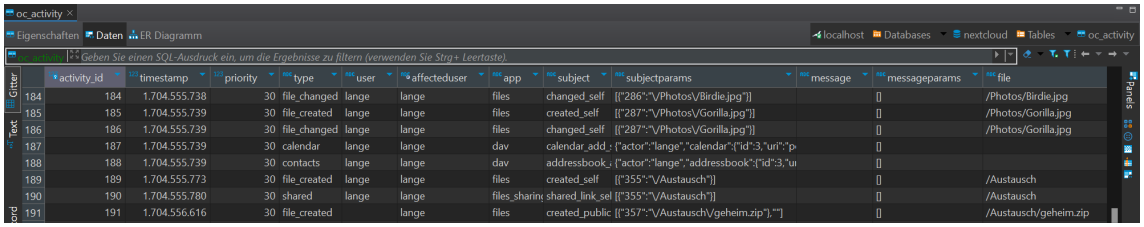


Abbildung 30: Hochladen der *geheim.zip* auf die Nextcloud

Download der Projektdaten

Es konnten auf dem System keine Spuren gefunden werden, dass die Datei *geheim.zip* von Herrn Lange heruntergeladen wurde.

5 Erzeugung der Images

Dieses Kapitel beschreibt die Erstellung der Images, welche für die forensische Analyse benötigt werden. Dazu wurden verschiedene Technologien und Werkzeuge, wie *dd*, *Magnet Axion* und *Docker* verwendet. Die resultierenden Images konnten im späteren Verlauf mithilfe von *Autopsy* analysiert und ausgewertet werden.

5.1 Notebooks

Mithilfe einer externen Festplatte, auf welcher Ubuntu in der Version 22.04 LTS installiert ist, konnte durch das Commandline-Tool *dd* sowohl ein Image des privaten als auch eines des dienstlichen Notebooks erstellt werden. Hierzu schließt man die Festplatte an das entsprechende Notebook an und bootet von dieser. Nachdem Ubuntu vollständig hochgefahren ist, öffnet man das Terminal, um die Kommandozeilen auszuführen. Hier muss als Erstes der Befehl `lsblk` ausgeführt werden. In der Ausgabe sieht man alle verfügbaren Festplattenpartitionen des Systems. Hier gilt es die gewünschte Partition herauszusuchen. Im Fall des privaten Notebooks war es beispielsweise *nvme0n1p3*, welche anhand der Größe identifiziert wurde. Mit dieser Information kann nun ein Image der Partition erstellt werden. Der Befehl hierfür lautet: `sudo dd if=/dev/nvme0n1p3 of=/var/log/laptop_image.img bs=4M status=progress`. Dabei ist hinter `if=` die zu kopierende Partition anzugeben. Hinter `of=` folgt die Datei, in welche das Ergebnis geschrieben werden soll. Hier ist darauf zu achten, dass die Datei in einem Verzeichnis auf der externen Festplatte abgelegt wird. Die beiden anderen Parameter definieren lediglich die Blocksize, die beim Kopieren verwendet werden soll und ob der Ablauf durch eine grafische Ausgabe begleitet werden soll. Abschließend kann mit `md5sum` der MD5 Hashwert der Images berechnet werden.

5.2 Handy

Nach der im Unterabschnitt 3.2.4 beschriebenen Vorarbeit kann ein physisches Image des Flash-Speichers vom Telefon recht einfach erzeugt werden. Da für die Anfer-

tigung dieser Arbeit eine Testversion der Software *Magnet Axiom* zur Verfügung stand, wurde die dort integrierte Möglichkeit zur Abbilderzeugung genutzt. Beim Anlegen eines neuen Falls mittels AXIOM Process sind Beweisquellen hinzuzufügen. Den Ablauf zeigen die Bilder a - h in Abbildung 31.

Das bzw. die erstellten Abbilder werden im zuvor festgelegten Ordner abgelegt. Durch *AXIOM* wurden zwei Abbilder erzeugt. Zum einen vom Gerät `/dev/block/mmcblk0` und zum anderen `/dev/block/dm-0`. Ersteres ist das primäre Blockgerät, also der Flash-Speicher des Telefons. dm-0 ist eine vom Linux Device Mapper[1] erzeugte Partition, welche sich auf dem Gerät mmcblk0 befindet und in diesem Fall sämtliche relevanten Daten enthält. Für die Analyse genügt hier also das Abbild von dm-0.

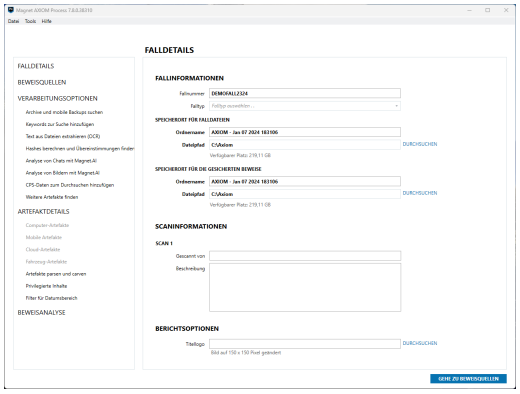
5.3 USB-Stick

Das Image des sichergestellten USB-Sticks wurde genauso erstellt, wie das der Notebooks. Jedoch kam hier keine externe Festplatte mit einem Betriebssystem zum Einsatz, sondern ein unabhängiges Notebook, auf welchem Pop!_OS installiert ist. Der USB-Stick wurde an dieses Notebook angeschlossen. Ab hier konnte genauso verfahren werden, wie in Kapitel 5.1 beschrieben. Zuerst die Feststellung der Partition mit `lsblk`, dann die Imageerzeugung mit `dd` und abschließend die Berechnung der Checksumme mit `md5sum`.

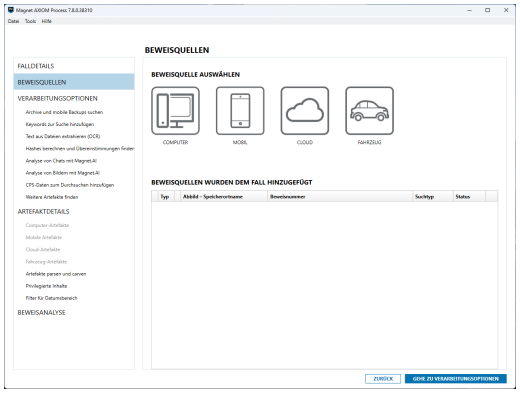
5.4 Nextcloud

Aufgrund der verwendeten Technologie der Containerisierung für die Nextcloud im Gegensatz zu den anderen verwendeten Bare-Metal-Systemen weicht die Erstellung eines Image für dieses Asservat stark ab. Wie bereits in Unterabschnitt 3.2.6 erwähnt, werden in einem Container keine Applikationsdaten wie angemeldete Benutzer gespeichert, sondern lediglich Informationen über den Container z.B. der Speicherort von Dateien über definierte *mounts*. Aus diesem Grund ist die Erstellung eines Image auf den herkömmlichen Weg einer forensischen Untersuchung nicht möglich. In dem Fall von *bind mounts* kann nur ein Abbild des dahinterliegenden Dateisystems erstellt werden. Dies wiederum führt zu einem Informationsverlust, da beispielsweise gelöschte Dateien nicht aufgeführt werden. Alternativ könnte ein Image des gesamten Servers erstellt werden, jedoch würde dies zu Ausfällen für andere Dienste auf dem Server führen und für Unternehmen somit zu finanziellen Einbußen. Ebenfalls

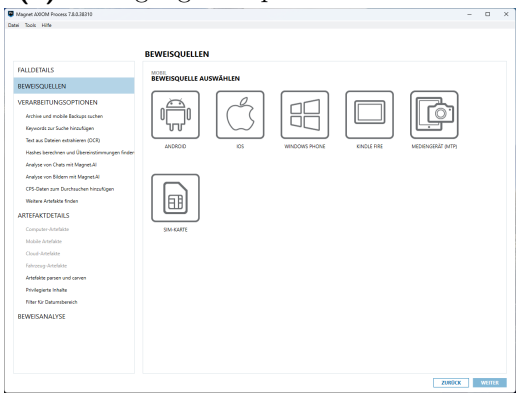
[1] `https://en.wikipedia.org/wiki/Device_mapper`



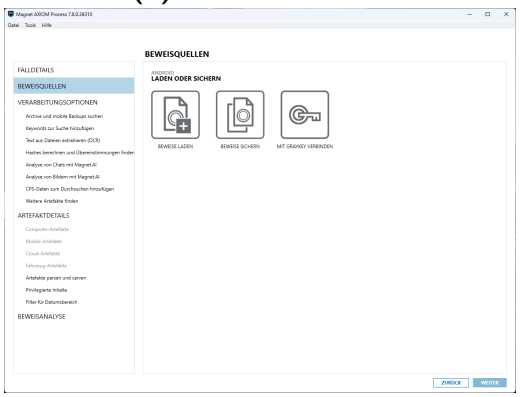
(a) Festlegung des Speicherort der Daten



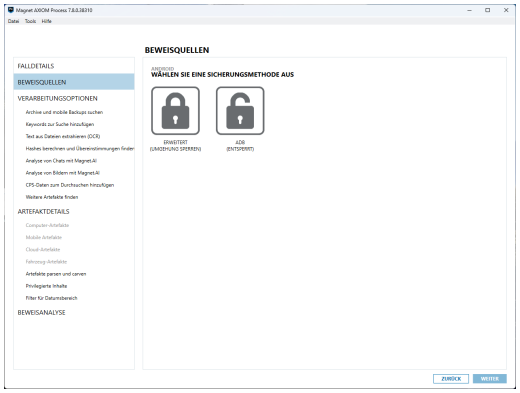
(b) Auswahl: MOBIL



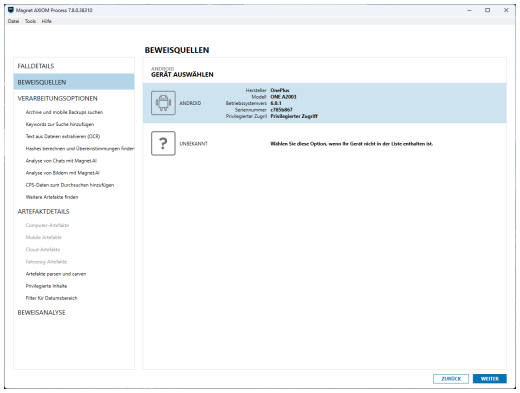
(c) Auswahl: ANDROID



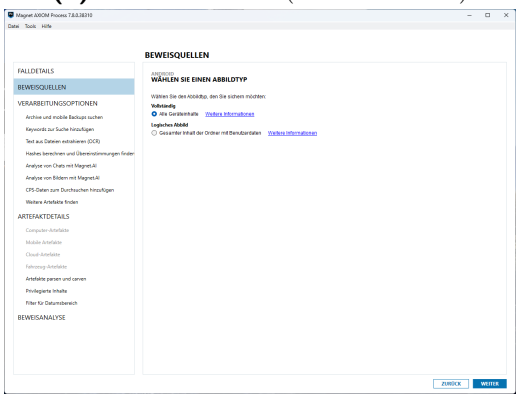
(d) Auswahl: BEWEIS SICHERN



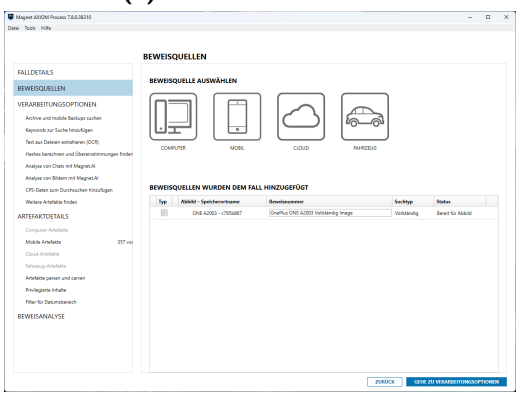
(e) Auswahl: ADB (ENTSPERRT)



(f) Auswahl des Geräts



(g) vollständige (physische) Sicherung



(h) Zusammenfassung Beweisquellen

Abbildung 31: Erzeugen eines physischen Images mit AXIOM Process

ist es möglich, dass auf dem System, auf welchem die Docker Software ausgeführt wird, weitere Daten vorhanden sind, welche nicht für den Vorfall relevant sind. Diese dürften aus diesem Grund nicht mit beschafft werden, was sich in diesem Fall aber nicht vermeiden lassen würde. Aus diesem Grund wurde sich dazu entschieden kein Image des gesamten Servers zu erstellen, sondern ausschließlich die *bind mounts* zu sichern. Ebenfalls wurde darauf verzichtet das gesamte Image über `docker image save` zu sichern, da dies über das Docker Hub öffentlich zugänglich ist.

Da in der Konfiguration der Container *bind mounts* verwendet werden, um die Daten zu speichern, müssen diese gesichert werden. Dafür wurde ein tar-Archiv erstellt, welches die *bind mounts* der Nextcloud und der MariaDB enthält. Zuerst muss in das Verzeichnis gewechselt werden, in dem die *bind mounts* liegen, da ansonsten die Verifikation bei der Erstellung des Archivs fehlschlägt. Wie in der *docker-compose* in Quellcode 1 zu sehen ist, liegen die Daten der Container in dem Verzeichnis `/etc/docker`. Anschließend kann über den Befehl `sudo tar -cWf /docker-volumes.tar mariadb nextcloud` ein Archiv erstellt werden in dem die Daten der MariaDB und der Nextcloud enthalten sind. Die Option *-c* erstellt ein neues Archiv, *-W* sorgt dafür, dass nach Abschluss der Erstellung der Datei diese verifiziert wird und *-f* gibt den Dateinamen an. Am Schluss können mehrere Ordner angegeben werden, welche in das Archiv gepackt werden sollen. Um den Hashwert erstellen zu können, welcher für die weitere Bearbeitung des Falls benötigt wird, muss zunächst in das Homeverzeichnis gewechselt werden. Anschließend kann über den Befehl `md5sum docker-volumes.tar` der MD5 Hashwert des Archivs berechnet werden.

6 Details zur Nextcloud Untersuchungstechnik

Für die Untersuchung der Nextcloud DB musste zuerst der MariaDB Ordner aus dem Archiv `docker-volumes.tar` entpackt werden. Dafür wurde ein neuer Ordner `mariadb-copy` erstellt und das Archiv in diesen entpackt. Anschließend wurde ein neuer MariaDB Container erstellt, welcher auf den entpackten Ordner zugreift. Dafür wurde der Befehl `docker run --volume /etc/docker/mariadb-copy:/var/lib/mysql --env MARIADB_USER=nextcloud --env MARIADB_PASSWORD=passwd --env MARIADB_DATABASE=nextcloud --env MARIADB_ROOT_PASSWORD=rootpwd -p 3306:3306 mariadb:latest` verwendet. Die Parameter wurden der *docker-compose* Datei in Abbildung 1 entnommen. Anschließend wurde sich mit dem Tool DBeaver mit der Datenbank verbunden und diese im Folgenden analysiert.

6.1 Zugänge

Die vorhandenen Nutzerkonten in der Cloud werden in der Tabelle `oc_users` der Datenbank `nextcloud` innerhalb der MariaDB gespeichert. Mit der einfachen Abfrage `SELECT * FROM nextcloud.oc_users` konnte ermittelt werden, welche Nutzerkonten existieren (Abb. 28). Daraus lässt sich schließen, dass zwei Nutzerkonten existieren.

6.2 Upload der Projektdateien

Die Nextcloud speichert in der Tabelle `oc_activity` sämtliche Aktivitäten der Nutzer. Hier wurde ebenfalls eine einfache SELECT Abfrage ähnlich zu der vorherigen verwendet, um herauszufinden, ob die Datei *geheim.zip* hochgeladen wurde (Abb. 30).

6.3 Download der Projektdateien

In der Tabelle `oc_activity` konnten keine Spuren gefunden werden, dass die Datei *geheim.zip* von Herrn Lange heruntergeladen wurde. Dies liegt daran, dass die Nextcloud Download-Aktivitäten standardmäßig nicht speichert. In Nextcloud gibt es jedoch die Möglichkeit Apps zu installieren. Eine dieser Apps ermöglicht es, die Downloads zu protokollieren. In der vorliegenden Nextcloud Instanz sind jedoch keine zusätzlichen Apps neben den Standard Apps installiert, wie aus der Tabelle in Abbildung 32 hervorgeht. Diese Tabelle wurde mit dem Befehl `SELECT * FROM nextcloud.oc_appconfig GROUP BY appid` erstellt. Dabei wurde die Datenbanktabelle `oc_appconfig` selektiert, in der sämtliche App Konfigurationen vorliegen. Zusätzlich musste über `appid` gruppiert werden, da in der Tabelle mehrere Einträge pro App existieren.

oc_appconfig 1 ×

SELECT * FROM nextcloud.oc_appconfig GROUP BY appid

Gitter

Text

	appid	configkey	configvalue
1	activity	enabled	yes
2	backgroundjob	lastjob	30
3	circles	enabled	yes
4	cloud_federation_api	enabled	yes
5	comments	enabled	yes
6	contactsinteraction	enabled	yes
7	core	installedat	1702319049.1344
8	dashboard	enabled	yes
9	dav	enabled	yes
10	federatedfilesharing	enabled	yes
11	federation	enabled	yes
12	files	enabled	yes
13	files_pdfviewer	enabled	yes
14	files_reminders	enabled	yes
15	files_rightclick	enabled	yes
16	files_sharing	enabled	yes
17	files_trashbin	enabled	yes
18	files_versions	enabled	yes
19	firstrunwizard	enabled	yes
20	logreader	enabled	yes
21	lookup_server_connec	enabled	yes
22	nextcloud_announcem	enabled	yes
23	notifications	enabled	yes
24	oauth2	enabled	yes
25	password_policy	enabled	yes
26	photos	enabled	yes
27	privacy	enabled	yes
28	provisioning_api	enabled	yes
29	recommendations	enabled	yes
30	related_resources	enabled	yes
31	serverinfo	cached_count_file	235
32	settings	enabled	yes
33	sharebymail	enabled	yes
34	support	enabled	yes
35	survey_client	enabled	yes
36	systemtags	enabled	yes
37	text	enabled	yes
38	theming	enabled	yes
39	twofactor_backupcod	enabled	yes
40	updatenotification	core	27.1.5.1
41	user_status	enabled	yes
42	viewer	enabled	yes
43	weather_status	enabled	yes
44	workflowengine	enabled	yes

Abbildung 32: Vorhandene Apps auf der Nextcloud

7 Zusammenfassung

In dieser Arbeit wurde ein fiktives Szenario der Betriebsspionage entwickelt und umgesetzt, um dieses dann forensisch zu untersuchen. Es erfolgte zunächst die Beschreibung der Ausgangssituation gefolgt von der Beschreibung, wie die Spuren auf den einzelnen Geräten erzeugt wurden. Auf Basis dieser Spuren wurde ein forensisches Gutachten erstellt, in welchem die erzeugten Images der Geräte analysiert und ausgewertet wurden. Daraufhin erfolgte eine Beschreibung der eigentlichen Erzeugung der Images, welche für die Untersuchungen verwendet wurden. Abschließend wurde detailliert auf die Untersuchungstechnik der Nextcloud eingegangen.
Die Arbeit wurde von drei Personen erstellt, was die unterschiedlichen Schreibstile und Wortwahl begründet. Außerdem ist kritisch anzumerken, dass alle Beteiligten der Arbeit zu jedem Zeitpunkt beigewohnt haben, wodurch bei der Analyse der Images und der Suche der Spuren jedem jederzeit das zu erreichende Ergebnis und die zu findende Spur bekannt war. Dadurch ist die Neutralität des Gutachtens und die Breite der angestellten Untersuchungen anfechtbar.
Außerdem war die zeitliche Rekonstruktion der Geschehnisse nicht zu jederzeit eindeutig anhand der Images und mithilfe von *Autopsy* möglich. Teilweise waren Zeitstempel der Datei in einer anderen Zeitzone als andere Zeitstempel derselben Datei. Das hatte zufolge, dass einige Zeiten nachträglich bearbeitet werden mussten, um die Arbeit und das Gutachten strukturiert und nachvollziehbar zu halten. Da dies das Verfälschen von Beweisen ist, sollte es so auf keinen Fall in einem realen Gutachten gehandhabt werden. Vielmehr sollte man das Problem analysieren und beheben um den Sachverhalt aufzuklären.
Abschließend ist festzuhalten, dass das Ziel dieser Arbeit, einen Sachverhalt zu konstruieren und diesen forensisch zu untersuchen und zu dokumentieren, als erfüllt betrachtet werden kann. Die Autoren konnten sich erfolgreich mit gängiger forensischer Software auseinandersetzen und Probleme, welche während einer solchen Untersuchung auftreten können, erkennen und teilweise im Vorfeld eliminieren.

A Anhang

Docker-Compose

```
version: '3.0'
services:
  db:
    image: mariadb:10.6
    ports:
      - 3306:3306
    command: --transaction-isolation=READ-COMMITTED --log-bin=binlog
  ↪ --binlog-format=ROW
    volumes:
      - /etc/docker/mariadb:/var/lib/mysql
    environment:
      - MYSQL_ROOT_PASSWORD=rootpwd
      - MYSQL_PASSWORD=passwd
      - MYSQL_DATABASE=nextcloud
      - MYSQL_USER=nextcloud

  nextcloud:
    image: nextcloud:27.1.4
    ports:
      - 8081:80
    links:
      - db
    volumes:
      - /etc/docker/nextcloud:/var/www/html
    environment:
      - MYSQL_PASSWORD=passwd
      - MYSQL_DATABASE=nextcloud
      - MYSQL_USER=nextcloud
      - MYSQL_HOST=db

  cloudflared:
    image: cloudflare/cloudflared:2023.10.0
    restart: unless-stopped
    command: tunnel run
    environment:
      - TUNNEL_TOKEN=secret
```

Listing 1: Docker-Compose.yml für Nextcloud, MariaDB und Cloudflare Tunnel

Literaturverzeichnis

[1] Cloudflare. *Set up a tunnel through the dashboard*. en. URL: https://developers.cloudflare.com/cloudflare-one/connections/connect-networks/get-started/create-remote-tunnel/ (besucht am 08. 02. 2024).

[2] Docker. *Docker Hub Container Image Library | App Containerization*. en. URL: https://hub.docker.com/ (besucht am 08. 02. 2024).

[3] Michael Eder. „Hypervisor- vs. Container-based Virtualization“. en. In: (2016). Medium: PDF Publisher: Chair for Network Architectures and Services, Department of Computer Science, Technische Universität München. DOI: 10.2313/NET-2016-07-1_01. URL: http://www.net.in.tum.de/fileadmin/TUM/NET/NET-2016-07-1/NET-2016-07-1_01.pdf (besucht am 08. 02. 2024).

[4] Ian Miell und Aidan Sayers. *Docker in Practice, Second Edition*. en. 2. Aufl. Google-Books-ID: SzgzEAAAQBAJ. Simon und Schuster, Feb. 2019. ISBN: 978-1-63835-630-1. (Besucht am 08. 02. 2024).

[5] Nextcloud. *Nextcloud Base version - apache*. en. URL: https://github.com/docker-library/docs/blob/master/nextcloud/README.md#base-version---apache (besucht am 08. 02. 2024).

Abbildungsverzeichnis

Tabellenverzeichnis

Quellcodeverzeichnis