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

Projektbericht

Modul “Forensische Datenanalyse”

Tills Notenspiegel

Eingereicht am: 21. Mai 2024

von: Emma Schmidt
111111

von: Harry Schmidt
222222

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

Inhaltsverzeichnis

1 Aufgabenstellung

Im Rahmen einer alternativen Prüfungsleistung soll ein digital nachvollziehbarer Vorfall entworfen werden, der mindestens sechs Aktionen auf mindestens zwei Geräten beinhaltet. Bei einer der Aktionen sollte auf eine Datenbank zugegriffen werden. Eines der Geräte muss ein Smartphone sein.

Dieser Vorfall soll von den Bearbeitern nachgespielt und anschließend durch eine forensische Datenanalyse nachgewiesen werden. Es ist erforderlich, dass eine der Aktionen durch eine RAM-Analyse aufgedeckt wird.

Die Abgabe erfolgt in Form einer schriftlichen Dokumentation, dessen Inhalt durch die folgende Gliederung vorgegeben ist:

Inhalt der Hausarbeit (PDF):

1. Deckblatt mit Namen und Matrikelnummer
2. Inhaltsverzeichnis
3. Aufgabenstellung
4. Beschreibung des Falles/ der Story/ des Szenarios
5. Dokumentation der Umsetzung des Szenarios und der dabei ausgeführten Aktionen
6. Forensisches Gutachten zur Auswertung des Falles
7. Dokumentation der Erstellung des Images
8. Dokumentation der Details zur forensischen Analyse
9. Zusammenfassung und kritisches Review
10. Anlagen

2 Beschreibung des Falls

In dem nachfolgend beschriebenen Fall treten die vier fiktiven Personen Emma, Harry und Bruno Schmidt sowie Till Bauer auf. H ist Polizist und Ehemann von E. E ist Lehrerin am St. Ursula Gymnasium und Mutter von B. Schüler T wird von E unterrichtet und ist mit B bekannt. Die Schule nutzt einen Datenbankserver zur Verwaltung der Noten ihrer Schüler. Die Zutrittserlaubnis erfolgt über eine Anmeldung (HTTP Basic Auth).

T tritt am 11.03.2024 über WhatsApp an B heran und bittet ihn darum heimlich die Noten im Fach Mathematik zu ändern. B errät das Passwort des Dienstrechners (Laptop) seiner Mutter, während sie ein Mittagessen zubereitet. Dort öffnet er in Firefox die Weboberfläche der Notendatenbank in einem privaten Fenster. Nach fehlgeschlagener Anmeldung mit den Zugangsdaten des Laptops, findet er nach einer kurzen Suche einen Zettel unterhalb des Laptops, welchem er die korrekten Zugangsdaten entnimmt. Er navigiert zur Seite von T und ändert drei Noten. Die erfolgreiche Änderung teilt B über WhatsApp mit. Anschließend sucht er nach Tills kommender Prüfung und fotografiert diese ab. B sendet die Fotos an T über WhatsApp. Die eigenen bevorstehenden Prüfungen verpackt er in eine .zip Datei und überträgt sie über die USB Schnittstelle auf sein angeschlossenes Handy.

Als E wieder ihr Arbeitszimmer betritt, entdeckt sie ihren Passwortmerkzettel für die Notenverwaltung auf dem Fußboden. Beim Aufklappen ihres Laptops bemerkt sie, dass die Sitzung bereits entsperrt ist. Sie realisiert, dass in ihrer Abwesenheit jemand an ihrem Rechner gewesen sein muss. Sie holt H hinzu, welcher als Forensiker arbeitet. Zusammen analysieren sie die digitalen Spuren und erstellen ein forensisches Gutachten, um ihren Sohn deutlich auf die offenen Spuren seines Eingriffs hinzuweisen.

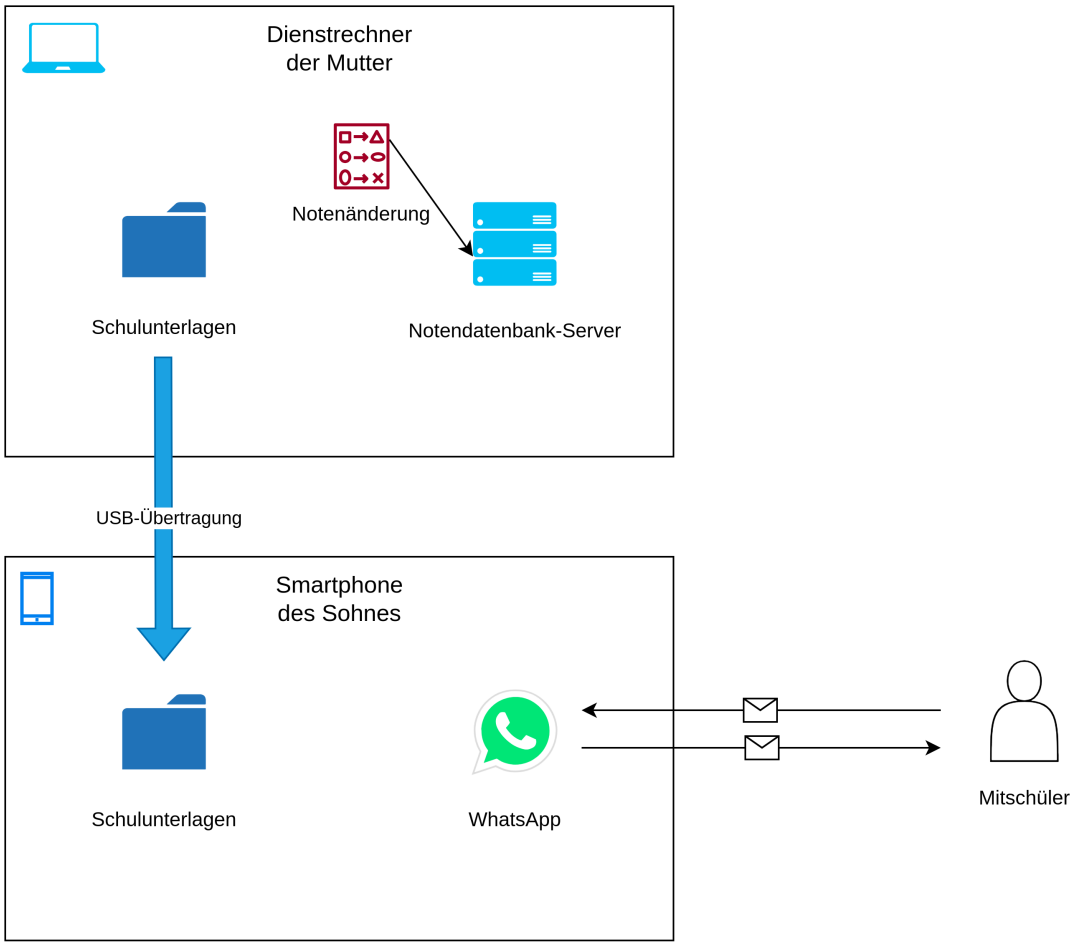


Abbildung 1: Abstrahierte Darstellung des Szenarios

3 Dokumentation der Umsetzung

Die Geräte, auf denen die Tat nachgespielt wurde, sind ein Smartphone und ein Dienstrechner. Der Dienstrechner wird hierbei durch eine virtuelle Maschine der Einfachheit halber simuliert. Um B einen Gesprächspartner zu geben, wurde ein zweites Telefon mit Whatsapp verwendet, welches nicht weiter von Relevanz ist. Zur forensischen Datenerfassung wurde ein USB-Stick hinzugezogen. Die untenstehende Tabelle enthält weitere Informationen.

Tabelle 1: Zur Umsetzung verwendete Geräte

Typ	**Gerät**	**Details**
Smartphone B	LG P880 Optimus 4X HD	Android: 6.0.1 (Custom LineageOS 13) Bootloader unlocked
Smartphone C	-	-
Dienstrechner	VirtualBox 7 VM	Ubuntu 18.04
USB-Stick	Corsair Voyager GS 64GB	Dateisystem: NTFS

3.1 Dienstrechner

In der Virtuellen Maschine ist das Betriebssystem „Ubuntu 18.04“ installiert. Die Notenverwaltung wird als simple Webseite mit PHP (s. Listing 5) unter dem Apache HTTP Server realisiert. Über PHP PDO[1] findet die Kommunikation mit der PostgreSQL-Datenbank (s. Abb. 2) statt. Sowohl der Apache Server als auch die Datenbank wird auf dem Dienstrechner selbst unter der Domain `noten-manager.internal` bereitgestellt (Abb. 3).

Die Domain verweist durch einen Eintrag in der `/etc/hosts` Datei auf `localhost`. Da alle Änderungen an der Datenbank nachvollziehbar sein sollten, ist die Protokollierung aktiviert worden. Dazu wurde in der Datei `/etc/postgresql/10/main/postgresql.conf` die Zeile `log_statement = "all"` ergänzt. Die Passwortabfrage der Notenverwaltung wurde in der Konfiguration des Webservers aktiviert.

[1] `https://www.php.net/manual/de/ref.pdo-pgsql.php`

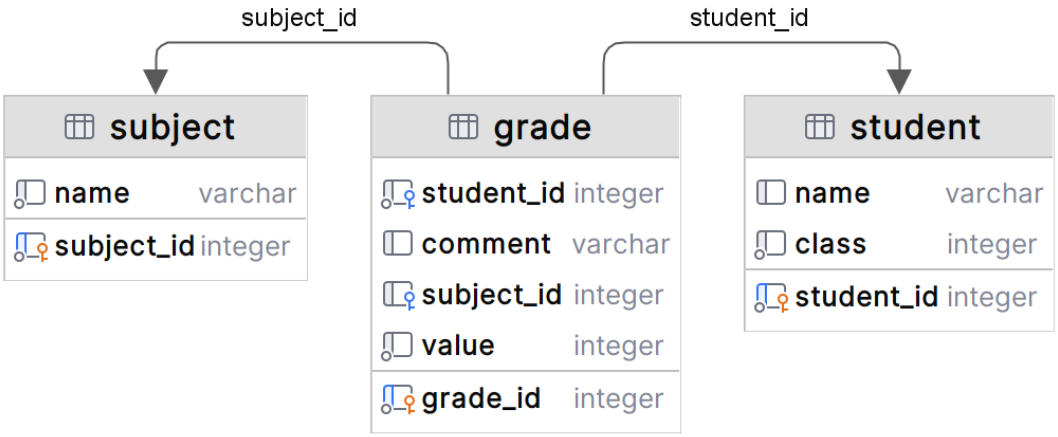


Abbildung 2: ER-Diagramm der Notendatenbank

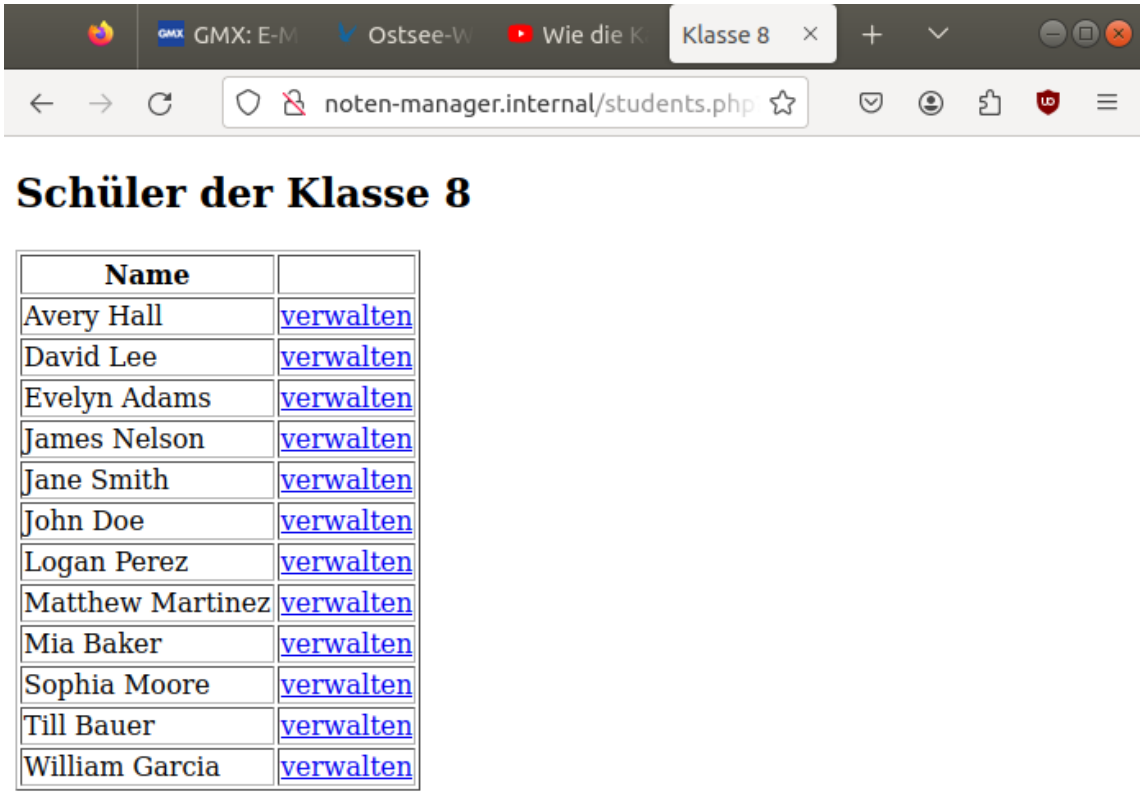


Abbildung 3: Die Übersicht über die Schüler der 8. Klasse auf der Notenverwaltungsseite

```
sudo htpasswd -b -c /etc/apache2/.htpasswd schmidt n0t3nl0g1n

sudo sed -i -f - /etc/apache2/sites-enabled/000-default.conf <<-EOF
/<VirtualHost \*:80>/a \\
  <Directory /var/www/html/> \\
    AuthName "Dialog prompt" \\
    AuthType Basic \\
    AuthUserFile /etc/apache2/.htpasswd \\
    Require valid-user \\
  </Directory> \\
EOF
```

Listing 1: Konfiguration der Passwortabfrage

Außerdem wurden einige Ordner und PDFs von Klassenarbeiten im Dateisystem angelegt.

3.2 Smartphone B

Am Smartphone B sind einige Schritte der Vorbereitung notwendig. Der Bootloader muss entsperrt und eine Custom-Recovery installiert sein. In diesem Fall wurde auch das Betriebssystem LineageOS[2] bzw. eine angepasste Variante[3] neu aufgesetzt. Zusätzlich war TWRP[4] als Custom-Recovery installiert. Da auf dem für diesen Fall genutzten Gerät dies bereits seit längerem der Fall war, lässt sich das genaue Vorgehen für die Durchführung des Projekts nicht mehr nachvollziehen. Im Internet gibt es jedoch eine Vielzahl von Anleitungen[5], deren Effekt äquivalent sein sollte. Die Telefonnummer des Smartphone C wurde als Kontakt „Till“ eingespeichert.

[2] https://lineageos.org/
[3] https://xdaforums.com/t/exp-lineageos-13-ufofficial-cve-2019-april.3621221/
[4] https://twrp.me/lg/lgoptimus4xhd.html
[5] https://xdaforums.com/f/lg-optimus-4x-hd.1649/

4 Forensisches Gutachten

4.1 Deckblatt

Gutachten

der IT-Forensik

Auftrag: St. Ursula Gymnasium

Aktenzeichen

123/221/400

Sachverständige

Harry Schmidt

Emma Schmidt

Abschluss:

15. März 2024

4.2 Auftragsspezifikation

Die Schulleitung des St. Ursula Gymnasiums beauftragt im Rahmen der Fälschung von schulischen Leistungen am 01.03.2024 zwischen 15:30 Uhr und 16:30 Uhr die Untersuchung der unten aufgeführten Asservate und die Erstellung eines IT-forensischen Gutachtens. Folgende Fragestellungen sind darin zu beantworten:

Asservat 01 - Hauptspeicher des Dienstrechners des Opfers
und
Asservat 02 - Festspeicher des Dienstrechners des Opfers

- F1.1 Fand eine unautorisierte Anmeldung auf dem Rechner zwischen 12:30 und 13:00 Uhr statt?
- F1.2 Wurden schulische Daten entwendet?
- F1.3 Wurden schulische Daten manipuliert?
- F1.4 Wurden Maßnahmen zur Vertuschung der Tat unternommen?

Asservat 03 - Festspeicher des Mobiltelefons des Tatverdächtigen

- F2.1 Befinden sich Hinweise auf das Motiv des Tatverdächtigen auf dem Mobilgerät?
- F2.2 Befinden sich geheime schulische Informationen auf dem Gerät?
- F2.3 Wurden Schulgeheimnisse von dem Gerät aus verbreitet?

4.3 Zusammenfassung der Ermittlungsergebnisse

4.3.1 Fragestellungen

Asservat 01
und
Asservat 02
Innerhalb des Tatzeitfensters und somit in Abwesenheit autorisierter Nutzer fanden einige Aktionen auf dem Dienstrechner statt. Dazu zählt eine Anmeldung mit zwei vorhergehend fehlgeschlagenen Anmeldeversuchen. Außerdem wurde die im Mathekurs der 8. Klasse bevorstehende Klassenarbeit mit dem PDF-Viewer Evince geöffnet und auf die Mathe-Klassenarbeit sowie das Deutsch-Diktat der 7. Klasse zugegriffen.

Im Protokoll der Notendatenbank sind Änderungen innerhalb des Tatzeitfensters an Till Bauers Noten verzeichnet. Darüber hinaus protokollierte der Notenverwaltungsserver einen Akteur, dessen IP-Adresse mit der des Dienstrechners übereinstimmt. Im Browserverlauf war der Zugriff auf die Notendatenbank jedoch nicht auffindbar.

Außerdem befanden sich die Anmeldedaten zur Notenverwaltungsseite im RAM des Dienstrechners, obwohl Emma Schmidt diese nach eigener Aussage seit dem letzten Neustart weder benutzt und noch eingespeichert hat. Ebenfalls wurde ein innerhalb des Tatzeitfensters erstelltes Archiv, welches die Unterlagen der 7. Klasse enthielt gelöscht. Im relevanten Zeitraum wurde der Browser neu gestartet, wie man der Prozesslaufzeit und Zeugenaussagen der Frau S. entnehmen kann. Im Systemprotokoll ist nachvollziehbar, dass das Smartphone des Tatverdächtigen Bruno S über eine USB-Schnittstelle an den Rechner angeschlossen wurde.

Asservat 03
Auf dem Telefon des Tatverdächtigen befindet sich ein WhatsApp-Chatverlauf mit dem Kontakt „Till“ (+49 xxxxxxxxx), in dem Bruno S. dazu aufgefordert wird, für eine Gegenleistung die Noten desselben Kontakts in der Datenbank zu verbessern. Später im selben Chat befinden sich vom Asservat aus versendete Fotografien der verfälschten Noten von Till Bauer und den Lösungen der bevorstehenden Klassenarbeit seiner Schulklasse. Zusätzlich zu den genannten Fotografien befindet sich noch ein Archiv, dessen Inhalt dem Ordner der Schulunterlagen zur Klasse 7 und dem gelöschten Archiv auf dem Dienstrechner entspricht. Höchstwahrscheinlich wurde der Ordner vom Dienstrechner komprimiert und auf das Smartphone kopiert.

4.3.2 Zeitliche Einordnung

Die Untersuchungsergebnisse lassen sich im folgendem Zeitlichen Verlauf (Tabelle 2) zusammenfassen:

Tabelle 2: Zeitliche Einordnung der Untersuchungsergebnisse

Asservat	**Zeitpunkt (CET)**	**Aktionen**
03	12:06	Bruno wird zur Tat aufgefordert durch Kontakt „Till“
03	12:11	Antwort über WhatsApp an „Till“
03	12:35	Bruno gibt den Start der Aktion über WhatsApp bekannt
02	12:35	Zwei Fehlgeschlagene Passworteingaben bei Bildschirmsperre des Dienstrechners
02	12:36	Erfolgreiche Anmeldung am Dienstrechner
02	12:36	Dienstrechner besucht die Notenverwaltung
02	12:36	Authentifizierung als „emma“ bei der Notenverwaltung schlägt fehl
01, 02	12:38	Authentifizierung bei der Notenverwaltung erfolgreich
02	12:38	Navigation durch die Notenverwaltung bis zur Seite von Till Bauer
02	12:38	Änderung Tills Noten in Mathematik: • Leistungskontrolle (Geometrie): 1 • Mitarbeit: 2 • Leistungskontrolle (Ungleichungen): 1
03	12:40	Versendung einer Fotografie der geöffneten Notenübersicht über WhatsApp von Brunos Smartphone an Till
02	12:41	Schließen aller Firefox-Fenster
01, 02	12:41	Öffnen von Firefox
03	12:41	„Till“ äußert Interesse an potentiellen Musterlösungen
03	12:41	Bruno antwortet
02	12:42	Bruno öffnet den Dateimanager
02	12:42	Bruno öffnet Klassenarbeit PDF (Mathematik Klasse 8)
03	12:44	Bruno fotografiert Lösungen (3 Seiten)
03	12:45	Schickt die 3 Fotos an „Till“ über WhatsApp
03	12:46	„Till“ bedankt sich
02	12:47	Täter erstellt ZIP-Archiv von dem Ordner „Klasse 7“
02	12:48	Brunos Smartphone wird an den Laptop per USB angeschlossen
03	12:49	„Klasse7.zip“ Archiv entsteht auf dem Smartphone
02	12:49	Löscht das Archiv auf dem Laptop
02	12:49	Trennung der USB-Verbindung
03	12:53	Bruno teilt „Till“ mit, dass seine Mutter nun wieder ins Zimmer gegangen ist

4.4 Untersuchungsobjekte

Tabelle 3: Liste der Asservate

Objekt	Dateinamen	Hashwerte (MD5)
Asservat 01 (Hauptspeicher des Dienstrechners)	ram.lime	`ecd58bd396991f62878f819f580e588b`

Asservat 02 (SDD des Dienstrechners)	ssd (EWF)
	ssd.E01
	ssd.E02
	ssd.E03
		`a645b43cadd1e7fd056cf6cfbbde0832`
		`bfbd591643d5e86e766a1428a810ae4e`
		`b6a7222ed7aeb5f6351f119803536799`
		`794370272c949732579109420601a68c`

Asservat 03 (Interner Speicher Smartphone LG P880)	phone.dd	`651cab7fa906e8e34272a7a617d8fa7a`

4.5 Untersuchungswerkzeuge

Tabelle 4: Die verwendeten Untersuchungswerkzeuge

Name	Version	Funktion
Tsurugi Acquire	2021.1	Live-Boot System mit Datenträger Schreibschutz und Werkzeugen zur Abbilderstellung
Guymager	0.8.12	Erstellung von verifizierten Festplattenimages im EWF oder dd Format
The Sleuthkit	4.12.1	Gesammelte Kommandozeilenprogramme zur Analyse von Festplattenimages
Autopsy	4.21.0	Grafische Oberfläche zur Nutzung von The Sleuthkit
AVML	0.13.0	Erstellung von Ram-Images unabhängig von der Architektur des Zielsystems
volatility	2.6.1	Analyse von Ram-Images
IPED	4.1.5	Analyse von Speicherabbildern inklusive einer Rekonstruktion von WhatsApp Chats
GNU strings	2.40	Extraktion von Zeichenketten aus Binärdaten
GNU grep	3.8	Mustersuche in Zeichenketten
Android Debug Bridge	1.0.41	Programm zur Ausführung von Befehle auf einem Android-Gerät oder deren Sicherung
ext4magic	0.3.2	File-Carver für das EXT4-Dateisystem

4.6 Untersuchung der Asservate

4.6.1 Asservat 01 & 02

Um möglichst alle relevanten Daten aus dem Hauptspeicher aufzufangen, wurde als erstes und schnellstmöglich das RAM-Image erstellt. So wurde die Veränderung des Speicherinhaltes durch laufende Prozesse minimal gehalten. Das Programm zur Abbilderstellung wurde von einem USB-Stick ausgeführt.
Durch das Herunterfahren direkt nach der RAM-Extraktion wurden Veränderungen am Festspeicher vorgebeugt. Des Weiteren stellte Tsurugi Acquire sicher, dass während der Imageerstellung keine Schreibaktionen die Originaldaten der Festplatte veränderten. Das Programm Guymager erstellte die Speicherabbilder und verifizierte sie durch ihren Hashwert. Anschließend wurde das Image von Autopsy analysiert und die Ergebnisse menschenlesbar präsentiert.

Abbildung 4: Bilder vom Dienstrechner

(a) Oberseite

(b) Unterseite

F1.1 Fand eine unautorisierte Anmeldung auf dem Rechner zwischen 12:30 und 13:00 Uhr statt?

In den Systemdateien (auth.log vgl. Abb. 5) ist sichtbar, dass sich ein Nutzer mit zwei fehlgeschlagenen Anmeldeversuchen an den Dienstrechner angemeldet hat. Die zwei fehlgeschlagenen Anmeldeversuche deuten eine unautorisierte Anmeldung an. Das erraten des schwachen Passworts mit persönlichem Bezug wäre für den Tatverdächtigen durch seine Beziehung zum Opfer in einigen wenigen Anmeldeversuchen möglich gewesen. Des Weiteren festigen alle nachfolgenden Untersuchungsergebnisse die Beobachtung, dass eine Anmeldung im Untersuchungszeitraum stattfand. So zeigt z.B. Volatility, dass die aktuell laufende Browser-Instanz innerhalb des Tatzeitraums gestartet wurde (vgl. Abb. 17).

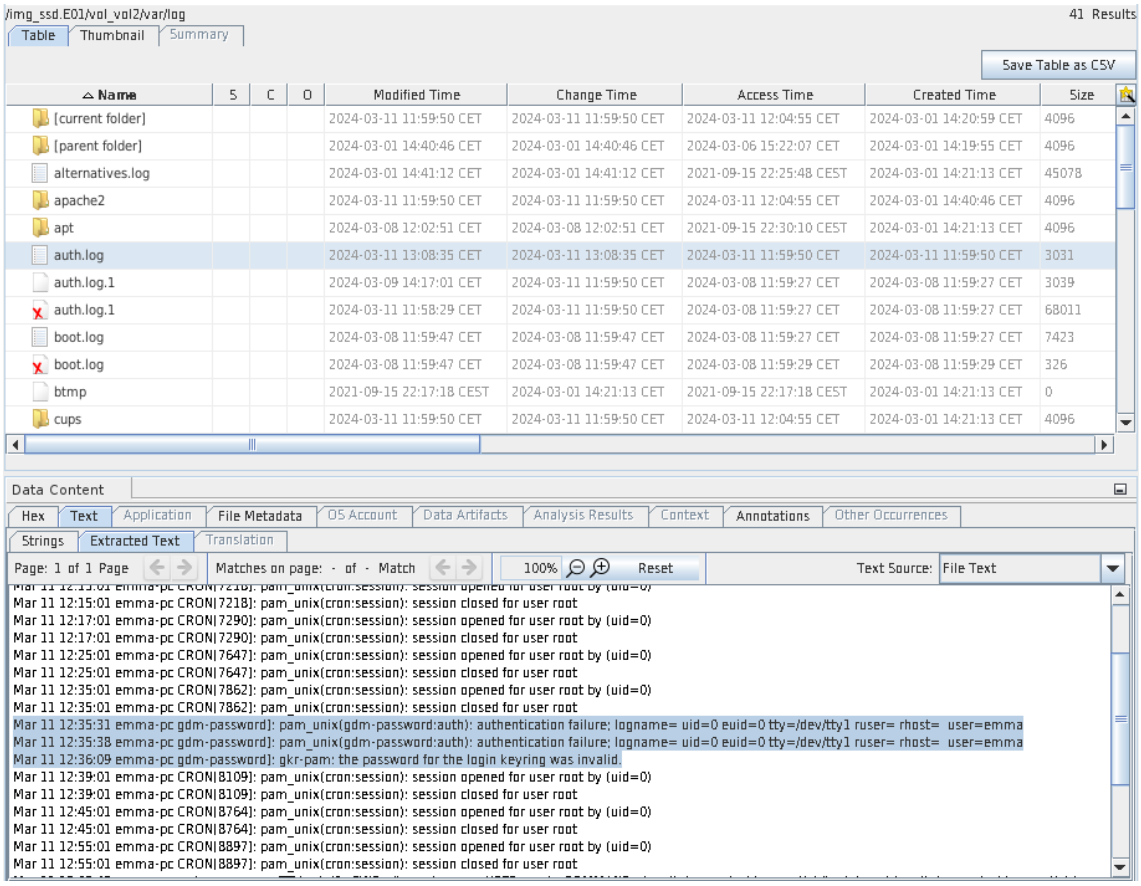


Abbildung 5: Autopsy zeigt Loginversuche aus der auth.log Datei

F1.2 Wurden schulische Daten entwendet?

Durch zielgerichtete Suche im Dateisystem konnte nachgewiesen werden, dass im Tatzeitraum Dateien der 7. und 8. Klasse aufgerufen wurden. Ebenfalls durch die Systemdateien (vgl. Abb. 25 im Anhang) wird anhand der Seriennummer ersichtlich, dass das Handy des Tatverdächtigen an den PC angeschlossen wurde. Im Festspeicherabbild befindet sich das Artefakt eines gelöschten ZIP-Archivs „Klasse7.zip“ (vgl. Abb. 6). Der Namenseintrag der gelöschten Datei verweist jedoch bereits auf die Daten einer anderen Datei. Unter den mittels ext4magic wiederhergestellten Dateien mit fehlenden Metadaten befindet sich ein ZIP-Archiv, dessen Hashwert mit dem des Archivs auf dem Smartphone übereinstimmt: `76905cac53ae58092797586f2a4cded1` (vgl. Abb. 11). Das Archiv beinhaltete die Schulunterlagen der Klasse 7.

Darüber hinaus wurde auf die Notendatenbank zugegriffen, welche geheime Schulunterlagen enthält. Details zu dieser Untersuchung folgen in Abschnitt 4.6.1 F1.3.

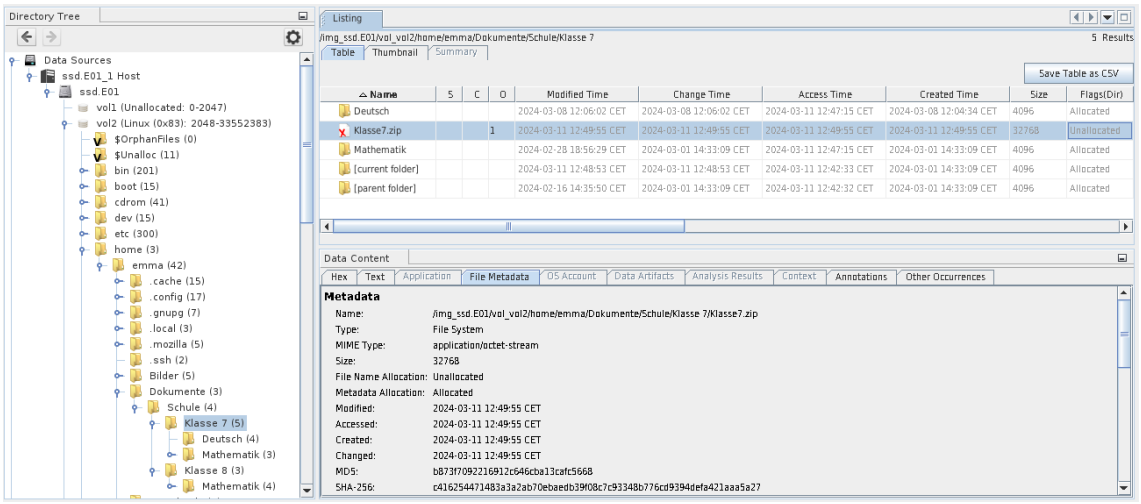


Abbildung 6: Autopsy zeigt Eintrag des gelöschten Archivs „Klasse7.zip“

F1.3 Wurden schulische Daten manipuliert?

Im Protokoll des Apache-Servers ist eindeutig nachweisbar, dass von der IP-Adresse 127.0.0.1, der lokalen Schnittstelle für Rechner-Interne Netzwerkkommunikation, auf den Notenserver zugegriffen wurde (vgl. Abb. 7).

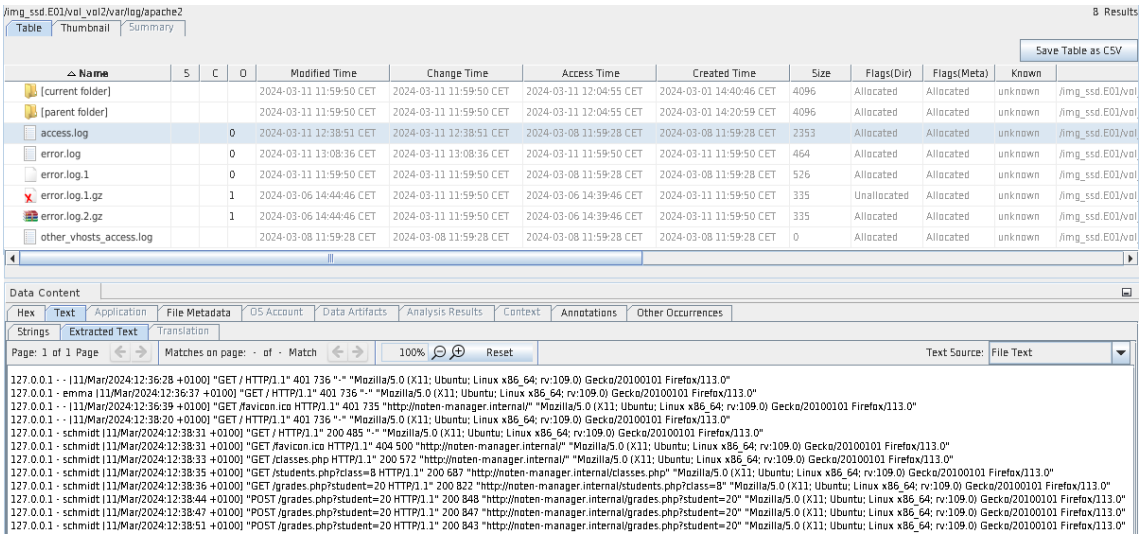


Abbildung 7: Autopsy zeigt den letzten Zugriff auf den Apache Server

Den Zugriff erhielt der Täter über Frau Schmidts Passwort, welches auf einem Zettelt nahe des Laptops notiert war. Obwohl Fr. Schmidt seit dem letzten PC-Start das Passwort nicht verwendet hat, ist dieses mit den Programmen GNU strings und GNU grep im Hauptspeicherabbild gefunden wworden (vgl. Abb. 8).

In den Dateien der PostgreSQL-Datenbank ist niedergeschrieben, dass die Noten-

```
dfir@dfir-vm:~$ strings /media/dfir/evidence_stick/ram.lime | grep n0t3nl0g1n
n0t3nl0g1n
n0t3nl0g1n
n0t3nl0g1n
n0t3nl0g1n
n0t3nl0g1n
n0t3nl0g1n
hpschmidt:n0t3nl0g1n
schmidt:n0t3nl0g1n
hpschmidt:n0t3nl0g1n
hpschmidt:n0t3nl0g1n
```

Abbildung 8: Arbeitsspeicherabbild enthält Zugangsdaten der Notenverwaltung

einträge in Till Bauers Profil verändert wurden (vgl. Abb. 9, 12).

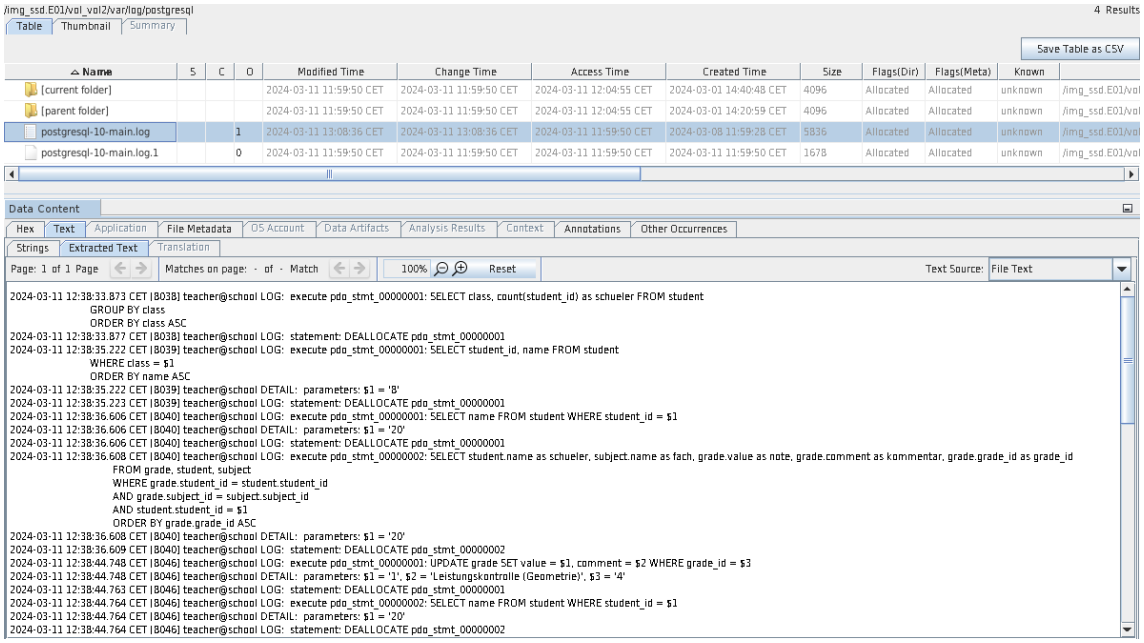


Abbildung 9: Autopsy zeigt die Aktionen an der Notendatenbank

F1.4 Wurden Maßnahmen zur Vertuschung der Tat unternommen?

Durch die Programmerweiterung „Firefox Analyzer“ konnte die Historie der mit dem Dienstrechner besuchten Webseiten wiederhergestellt werden. Die Notenverwaltungsseite war darin nicht enthalten. Da im vorangegangenen Abschnitt 4.6.1 F1.3 gezeigt wurde, dass durchaus die Website besucht wurde, und kein anderer Browser installiert ist, muss eine von zwei Maßnahmen durch den Täter vollzogen worden sein: (a) Öffnen der Seite in einem Privaten Fenster (b) Gezieltes Löschen

der Firefox-Historie. Beide Maßnahmen dienen ausschließlich der Vertuschung der Handlung.

4.6.2 Asservat 03

Abbildung 10: Bilder des Smartphones

(a) Frontseite **(b)** Rückseite **(c)** Rückseite (offen)

Das Telefon befand sich zum Zeitpunkt der Konfiskation im ausgeschalteten Zustand. Der interne Speicher des Smartphones ließ sich im Recovery-Modus über eine USB-Datenverbindung mittels ADB sichern. Anschließend ist das physische Abbild mit IPED ausgewertet worden.

F2.1 Befinden sich Hinweise auf das Motiv des Tatverächtigen auf dem Mobilgerät?

Dem Tatverdächtigen wurde für die Durchführung einer Anpassung der Noten von Till Bauer ein unter Schülern üblicher Sachwert versprochen. Im extrahierten WhatsApp-Chatverlauf mit dem Kontakt „Till“ ist dies nachzuvollziehen (vgl. Abb. 13).

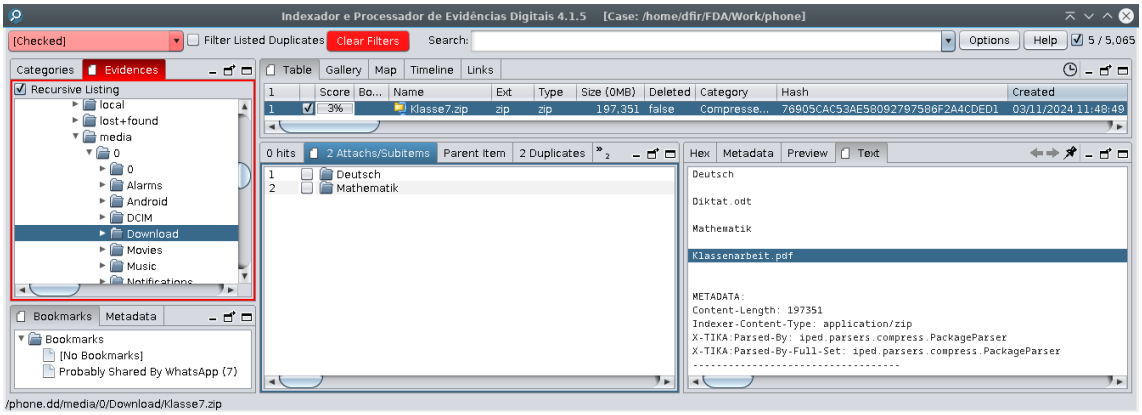


Abbildung 11: Klasse7.zip auf dem Smartphone

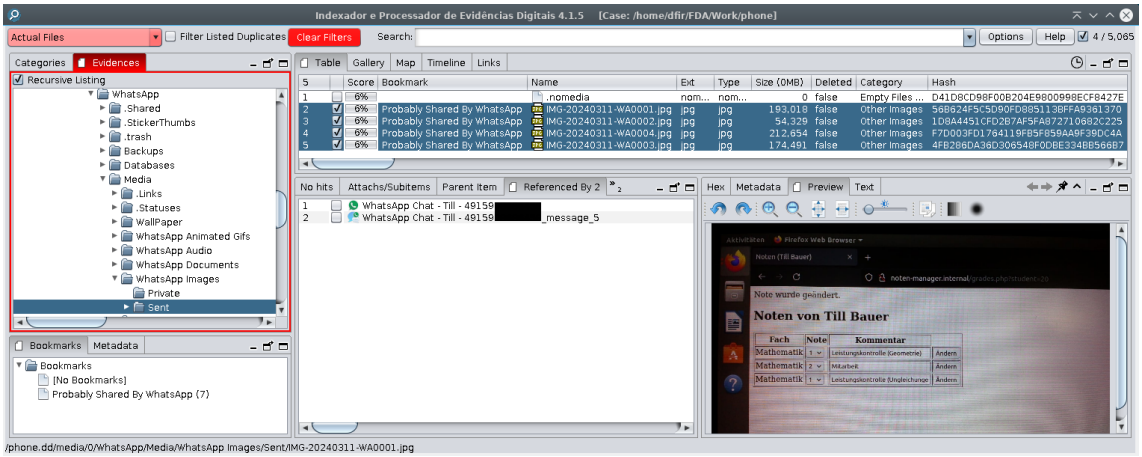


Abbildung 12: Die vom Smartphone über WhatsApp an Till versendeten Bilder

F2.2 Befinden sich geheime schulische Informationen auf dem Gerät?

Im Dateisystem befindet sich das inhaltlich zum Ordner des Dienstrechners korrespondierende ZIP-Archiv „Klasse7.zip“ (vgl. Abb. 6. 11).

F2.3 Wurden Schulgeheimnisse von dem Gerät aus verbreitet?

Der Abbildung 13 ist zu entnehmen, dass Bilder der Musterlösung einer Klassenarbeit an „Till“ versendet wurden.

Abbildung 13: Anstiftung zur Tat und Dokumentation dieser im wiederhergestellten WhatsApp Verlauf mit Kontakt „Till“

5 Dokumentation der Erstellung der Images

5.1 Dienstrechner: Hauptspeicher / RAM

Der Hauptspeicher wurde zuerst gesichert, um dem Verlust flüchtiger Daten vorzubeugen. Dazu wurde AVML[1] (Acquire Volatile Memory for Linux) von Microsoft genutzt. Da im behandelten Szenario der Opfer-PC analysiert wird, steht den Untersuchenden das Administratorpasswort zur Verfügung. Dadurch wird die Benutzung des Programms möglich. AVML speichert das Abbild standardmäßig im LIME-kompatiblen Format ab und unterstützt darüber hinaus auch Kompression sowie den Export über das Netzerk. Im Gegensatz zu LIME ist AVML statisch und portabel, wodurch kein Wissen über das Zielsystem und keine Kompilierung oder Kernelmodule auf dem Zielsystem nötig sind.

Am Terminal wurden die folgenden Befehle ausgeführt:
`sudo /media/emma/evidence_stick/tools/avml`
`/media/emma/evidence_stick/ram.lime`

Anschließend wurde der PC heruntergefahren.

5.2 Dienstrechner: Sekundärspeicher / SSD

Für die anschließende Sicherung der Festplatte wurde der PC zunächst über einen USB-Stick mit dem Linux-Live-System Tsurugi Acquire[2] hochgefahren. Dieses bindet Datenträger standardmäßig schreibgeschützt ein. Mit dem dort vorinstallierten Programm Guymager[3] wurden Images im Expert Witness Format erstellt und anschließend automatisch verifiziert (Abb. 15).

[1] `https://github.com/microsoft/avml`
[2] `https://tsurugi-linux.org/index.php`
[3] `https://github.com/cyberknightX/Guymager`

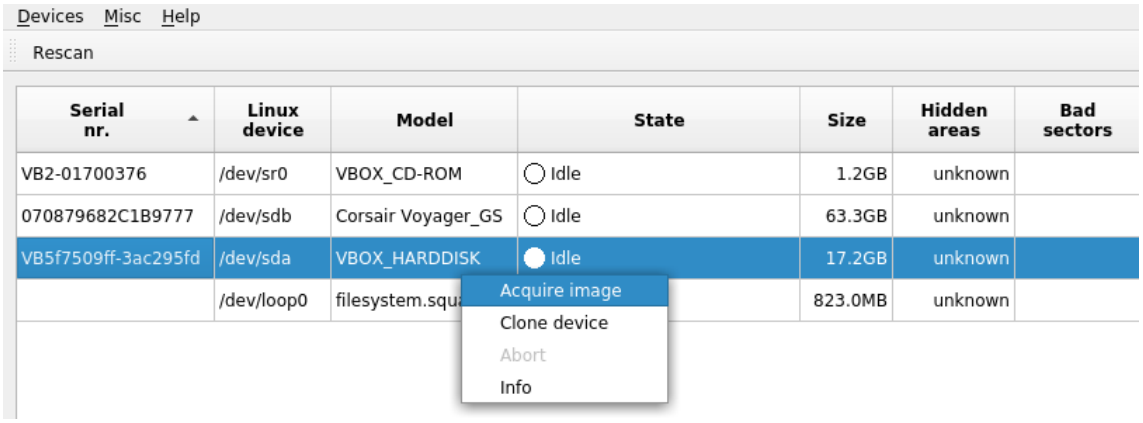


Abbildung 14: Guymager Übersicht

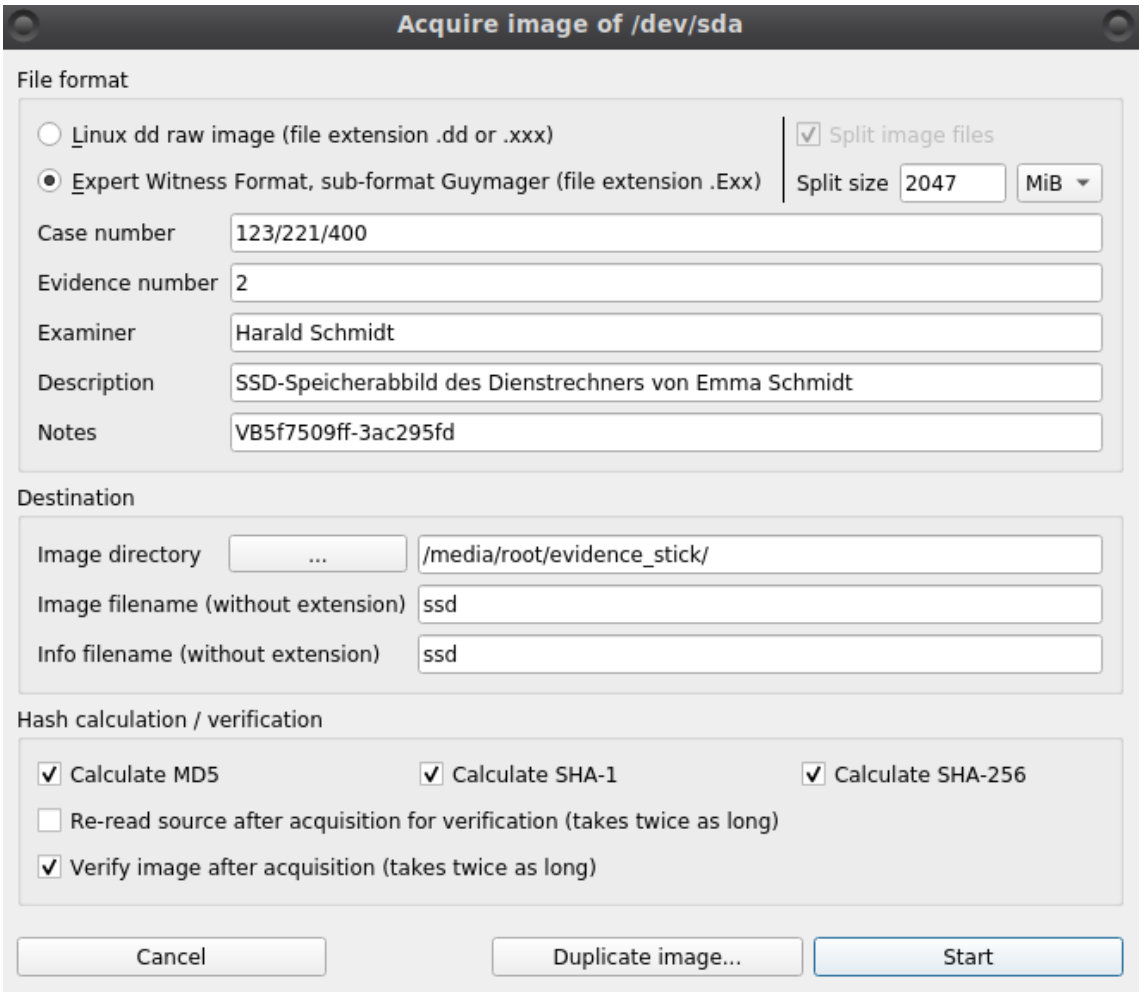


Abbildung 15: Guymager Dialog

5.3 Smartphone: Datenpartition (Interner Speicher)

Die Datenpartition lässt sich in diesem Fall über die bereits installierte Custom-Recovery TWRP sichern. Um in die Recovery zu gelangen, muss bei diesem Smartphone-

Modell beim Anschalten die “Vol-”-Taste gedrückt gehalten werden. Ein USB-Kabel sollte hierbei noch nicht angeschlossen sein, da sonst der “S/W Upgrade” Bildschirm erreicht wird. In der Recovery angelangt, kann nun ein USB-Datenkabel angeschlossen werden. Sollte das Gerät bei “adb devices” nicht aufgelistet werden, kann im Recovery Reboot-Menü das Smartphone nochmals in die Recovery neu gestartet werden, nun auch bei angeschlossenen USB-Kabel. Am Analyse-PC kann mit den folgendem Befehl ein Abbild des Speichers gezogen werden: `adb pull /dev/block/mmcblk0p8 /media/root/evidence_stick/mmcblk0p8.img` Dies ist auch in Abbildung 16 nachvollziehbar.

```
dfir@dfir-vm:~$ adb devices
List of devices attached
015d3fbaad4ffc18        device

dfir@dfir-vm:~$ adb shell mount
rootfs on / type rootfs (rw,seclabel)
tmpfs on /dev type tmpfs (rw,seclabel,nosuid,relatime,mode=755)
devpts on /dev/pts type devpts (rw,seclabel,relatime,mode=600)
proc on /proc type proc (rw,relatime)
sysfs on /sys type sysfs (rw,seclabel,relatime)
selinuxfs on /sys/fs/selinux type selinuxfs (rw,relatime)
tmpfs on /tmp type tmpfs (rw,seclabel,relatime)
/dev/block/mmcblk0p4 on /cache type ext4 (rw,seclabel,relatime,user_xattr,acl,barrier=1,data=ordered)
/dev/block/mmcblk0p8 on /data type ext4 (rw,seclabel,relatime,user_xattr,acl,barrier=1,data=ordered)
/dev/block/mmcblk0p8 on /sdcard type ext4 (rw,seclabel,relatime,user_xattr,acl,barrier=1,data=ordered)
dfir@dfir-vm:~$ adb shell md5sum /dev/block/mmcblk0p8
651cab7fa906e8e34272a7a617d8fa7a  /dev/block/mmcblk0p8
dfir@dfir-vm:~$ adb pull /dev/block/mmcblk0p8 /media/dfir/evidence_stick/phone.dd
/dev/block/mmcblk0p8: 1 file pulled, 0 skipped. 2.4 MB/s (13375635456 bytes in 5351.378s)
dfir@dfir-vm:~$ md5sum /media/dfir/evidence_stick/phone.dd
651cab7fa906e8e34272a7a617d8fa7a  /media/dfir/evidence_stick/phone.dd
```

Abbildung 16: Sicherung der Datenpartition mit ADB

6 Dokumentation der Details zur forensischen Analyse

6.1 Dienstrechner: Hauptspeicher / RAM

Die Auswertung von Hauptspeicherabbildern mit Volatility2 benötigt sogenannte Profile. Diese beinhalten Informationen über die Datenstrukturen und Debugsymbole des Kernels - sind demnach meist systemspezifisch. Steht kein zum Zielsystem passendes Profil zur Verfügung[1], muss dieses selbst erstellt werden. Aus dem mit Guymager erstellten Image sind die dafür notwendigen Informationen extrahierbar (vgl. Anhang A). Alternativ kann das Profil in einer VM mit denselben Eigenschaften wie dem Zielsystem oder auf einer Kopie des Festplattenabbilds erfolgen.

Mit passendem Profil stellt Volatility eine Liste verschiedener Plug-ins bereit, um die RAM-Daten aufzubereiten. So kann mit `linux_pslist` eine dem Programm *ps* nachempfundene Funktionalität aufgerufen werden. Dies ist in Abbildung 17 zu sehen.

```
root@66ea4bd390a8:/workspace# volatility --plugins=. --profile=LinuxUbuntu1804x64 -f /evidence/ram.lime linux_pslist 2> /dev/null
Offset             Name                 Pid             PPid            Uid             Gid    DTB                Start Time
------------------ -------------------- --------------- --------------- --------------- ------ ------------------ ----------
0xffff8e3bfc1daf00 systemd              1               0               0               0      0x00000000bba36000 2024-03-11 10:39:20 UTC+0000
0xffff8e3bfc1dc680 kthreadd             2               0               0               0      ------------------ 2024-03-11 10:39:20 UTC+0000
0xffff8e3bfc1dde00 rcu_gp               3               2               0               0      ------------------ 2024-03-11 10:39:20 UTC+0000
0xffff8e3bfc1d9780 rcu_par_gp           4               2               0               0      ------------------ 2024-03-11 10:39:20 UTC+0000
0xffff8e3bfc1f0000 kworker/0:0H         6               2               0               0      ------------------ 2024-03-11 10:39:20 UTC+0000
                                                        ••••••••••••••••••••
0xffff8e3b66338000 kworker/0:7          8164            2               0               0      ------------------ 2024-03-11 11:41:59 UTC+0000
0xffff8e3b438a1780 firefox              8185            1               1000            1000   0x0000000003868000 2024-03-11 11:42:07 UTC+0000
0xffff8e3b42f10000 Socket Process       8238            8237            1000            1000   0x00000000a632c000 2024-03-11 11:42:07 UTC+0000
0xffff8e3b66305e00 Privileged Cont      8278            8237            1000            1000   0x000000001c5f6000 2024-03-11 11:42:07 UTC+0000
0xffff8e3b5d0e8000 WebExtensions        8314            8237            1000            1000   0x0000000026318000 2024-03-11 11:42:08 UTC+0000
0xffff8e3b66339780 Isolated Web Co      8382            8237            1000            1000   0x00000000b99ec000 2024-03-11 11:42:09 UTC+0000
0xffff8e3b5c4f0000 Isolated Web Co      8386            8237            1000            1000   0x0000000052654000 2024-03-11 11:42:09 UTC+0000
0xffff8e3bcb908000 RDD Process          8494            8237            1000            1000   0x000000001c622000 2024-03-11 11:42:12 UTC+0000
0xffff8e3b66038000 Utility Process      8501            8237            1000            1000   0x000000001c070000 2024-03-11 11:42:12 UTC+0000
0xffff8e3b5e810000 Web Content          8687            8237            1000            1000   0x000000008bb5a000 2024-03-11 11:43:17 UTC+0000
0xffff8e3b42ec2f00 scsi_eh_3            9004            2               0               0      ------------------ 2024-03-11 12:03:41 UTC+0000
0xffff8e3b42ec0000 scsi_tmf_3           9005            2               0               0      ------------------ 2024-03-11 12:03:41 UTC+0000
0xffff8e3b42ec1780 usb-storage          9006            2               0               0      ------------------ 2024-03-11 12:03:41 UTC+0000
0xffff8e3b5c709780 uas                  9009            2               0               0      ------------------ 2024-03-11 12:03:41 UTC+0000
0xffff8e3b926dde00 mount.ntfs           9047            1               0               0      0x000000001c628000 2024-03-11 12:03:43 UTC+0000
0xffff8e3bb7c12f00 Web Content          9076            8237            1000            1000   0x00000000b6be2000 2024-03-11 12:03:45 UTC+0000
0xffff8e3b6633c680 seahorse             9100            2005            1000            1000   0x0000000034060000 2024-03-11 12:03:46 UTC+0000
0xffff8e3bbb3b4680 gnome-terminal-      9101            2005            1000            1000   0x000000001c248000 2024-03-11 12:03:46 UTC+0000
0xffff8e3b66345e00 bash                 9165            9101            1000            1000   0x00000000b6250000 2024-03-11 12:03:48 UTC+0000
0xffff8e3bcba9de00 kworker/1:3          9221            2               0               0      ------------------ 2024-03-11 12:04:14 UTC+0000
0xffff8e3bfc3bde00 sudo                 9222            9165            0               0      0x00000000a63de000 2024-03-11 12:04:15 UTC+0000
0xffff8e3be62b5e00 avml                 9223            9222            0               0      0x00000000b470c000 2024-03-11 12:04:17 UTC+0000
```

Abbildung 17: Gekürzte Ausgabe des Volatility-Plugins linux_pslist

[1] `https://github.com/volatilityfoundation/profiles`

6.2 Dienstrechner: Sekundärspeicher / SSD

Beim Durchsuchen des Images ist es notwendig die zu betrachtende Datenmenge zu reduzieren. Mit der von Autopsy bereitgestellten Funktion zur Erstellung einer Timeline lassen sich die erfassten relevanten Änderungen darstellen. Darüber hinaus ist die zeitliche Genauigkeit, in welcher die Ereignisse dargestellt werden sollen, konfigurierbar. So sind große Datenmengen in kleinen Schritten besser auszuwerten. Welche Dateien näher betrachtet werden, ergibt sich auch anhand der Fragestellungen des Gutachtens. Im Anhang B sind einige Erkenntnisse anhand von Screenshots dokumentiert. Wie im Gutachten bereits erwähnt, verweist der Namenseintrag der gelöschten „Klasse7.zip“ auf die Inode einer anderen Datei (s. Abb. 18). Zur Wiederherstellung der Archivdaten wurde der File-Carver ext4magic genutzt. Dieser macht vom Ext4-Journal Gebrauch um bspw. kürzlich gelöschte Dateien zu finden.[2] Erwähnenswert ist hierbei auch das korrekte, wiederhergestellte Erstelldatum des Archivs.

```
dfir@dfir-vm:~/FDA$ ifind -o 2048 -n /home/emma/Dokumente/Schule/Klasse\ 7/Klasse7.zip /media/dfir/evidence_stick/ssd.E01
809683
dfir@dfir-vm:~/FDA$ ffind -o 2048 /media/dfir/evidence_stick/ssd.E01 809683
/home/emma/.local/share/gvfs-metadata/home-2debea18.log
dfir@dfir-vm:~/FDA$ findmnt | grep /mnt/ssd
├─/mnt/ssd_ewf                                      /dev/fuse   fuse            rw,nosuid,nodev,relatime,user_id=0,group_id=0
└─/mnt/ssd                                          /dev/loop0  ext4            ro,noexec,relatime,norecovery
dfir@dfir-vm:~/FDA$ sudo ext4magic -r /dev/loop0
"RECOVERDIR"  accept for recoverdir
Filesystem in use: /dev/loop0

Using  internal Journal at Inode 8
Inode 2 is allocated
      ••••••••••••••••••••••
MAGIC-2 : start lost in journal search
      ••••••••••••••••••••••
--------        RECOVERDIR/MAGIC-2/text/xml/I_0001068287.txt
--------        RECOVERDIR/MAGIC-2/text/plain/I_0001068331.txt
--------        RECOVERDIR/MAGIC-2/text/plain/I_0001068363.txt
--------        RECOVERDIR/MAGIC-2/application/zip\012-/I_0001068483.unknown
      ••••••••••••••••••••••
ext4magic : EXIT_SUCCESS
dfir@dfir-vm:~/FDA$ sudo file RECOVERDIR/MAGIC-2/application/zip\\012-/I_0001068483.unknown
RECOVERDIR/MAGIC-2/application/zip\012-/I_0001068483.unknown: Zip archive data, at least v2.0 to extract, compression method=store
dfir@dfir-vm:~/FDA$ sudo md5sum RECOVERDIR/MAGIC-2/application/zip\\012-/I_0001068483.unknown
\76905cac53ae58092797586f2a4cded1  RECOVERDIR/MAGIC-2/application/zip\\012-/I_0001068483.unknown
dfir@dfir-vm:~/FDA$ sudo ls -l RECOVERDIR/MAGIC-2/application/zip\\012-/I_0001068483.unknown
-rw-rw-r-- 1 dfir dfir 197351 Mar 11 12:47 'RECOVERDIR/MAGIC-2/application/zip\012-/I_0001068483.unknown'
```

Abbildung 18: Carving des Archivs

[2] `https://ext4magic.sourceforge.net/journal_de.html`

6.3 Smartphone: Datenpartition (Interner Speicher)

Die verwendete IPED Version benötigt ein Java 11 JDK mit JavaFX Modulen.[3] Empfohlen wird das Full Liberica JDK von BellSoft.[4]

Anhand der von Linux protokollierten Seriennummer des Smartphones durch den Anschluss über USB, lässt sich diese mit IPEDs Volltextsuche in der Datenpartition wiederfinden. Die Seriennummer aus `kern.log` des Dienstrechners (s. Abb. 25) und der WLAN-Konfiguration `wpa_supplicant.conf` des Smartphones unterscheidet sich jedoch von der vom Aufkleber im inneren des Smartphones (s. Abb. 10c). Da die digitalen Spuren übereinstimmen ist der Aufkleber nicht weiter von Bedeutung.

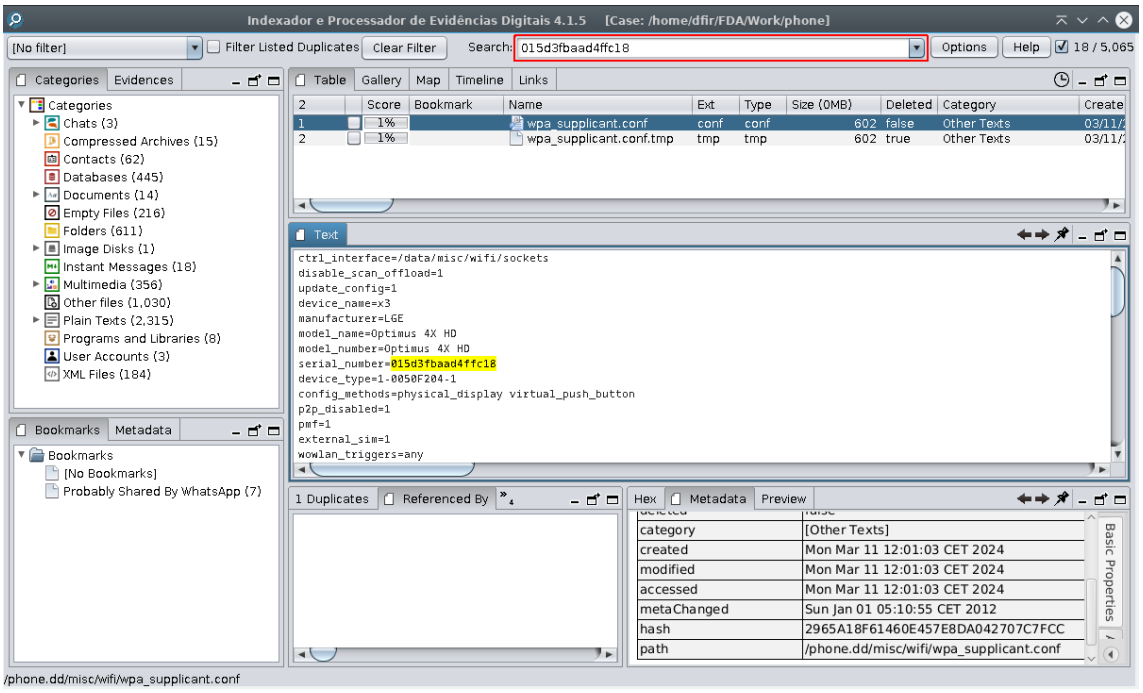


Abbildung 19: IPED Volltextsuche findet Seriennummer des Smartphones

Ebenfalls ist es nachvollziehbar, dass um 12:44 Uhr die Kamera-App geöffnet worden ist (s. Abb. 27), wie im Ablauf (vgl. Tabelle 2) verzeichnet.

[3] `https://github.com/sepinf-inc/IPED/wiki/Linux`
[4] `https://bell-sw.com/pages/downloads/#jdk-11-lts`

7 Zusammenfassung und kritisches Review

In dieser Arbeit wurde eine Misstat in einem digitalen Umfeld von zwei Geräten (Ein Linux-PC und ein Android Smartphone) erdacht und durchgeführt. Die Dokumentation dieses ersten Schrittes findet sich in Kapitel 3. Für die Anschließende Analyse wurden Speicherabbilder der Festspeicher beider Geräte und des flüchtigen Speichers des PCs genommen (Kapitel 5). Anhand der darin enthaltenen Artefakte wurde der Hergang (Kapitel 6) rekonstruiert und an ein forensisches Gutachten angelehnt präsentiert (Kapitel 4). Zu diesen Zwecken wurden übliche und auch weniger bekannte Werkzeuge exploriert und angewendet (Tabelle 4).

Das Betriebssystem Tsurugi fiel dadurch auf, dass es anders als übliche forensische Betriebssysteme eine aktuelle Version von Autopsy und auch alle anderen hier verwendeten Programme, bis auf IPED, vorinstalliert hatte. Aus Ressourcengründen wurde jedoch letztendlich eine minimale Debian-VM zur Analyse verwendet. Zur Abbilderstellung überzeugte Tsurugi Acquire, die leichtgewichtigere Ausführung von Tsurugi, mit aktuellen Programmen sowie automatischem Schreibschutz für eingebundene Datenträger.

Zwischen AVML und LiME fiel die Wahl auf AVML, da es anders als LiME keine Informationen über das Zielsystem vorraussetzt.

Der Nutzen der RAM-Analyse eines Linux-Systems mit Volatility hält sich in Grenzen. Die Auswahl der Plugins ist überschaubar und viele der extrahierbaren Informationen lassen sich auch gut im Festspeicher nachweisen. Andere potentiell relevanten Informationen konnten aufgrund des vom Kernel verwendeten Speicherallokators SLUB nicht ausgelesen werden. Obwohl Volatility-Profile für diverse Linux Versionen zur Verfügung stehen, muss realistisch gesehen ein eigenes gebaut werden. Dies kann für einen Einsteiger irreführend sein.

Wider Erwarten war es nicht möglich die Inhalte des gelöschten Archivs (vgl. Abbildung 6) in Autopsy wiederherzustellen. Dies ist jedoch durch Carving mittels ext4magic möglich gewesen. Da ext4magic mit dem Ext4-Journal arbeitet, wäre es zukünftig empfehlenswert den Journal direkt vom laufenden System zu sichern und

diesen ext4magic als Argument zu übergeben. Möglich wäre das mit dem folgenden Befehl: `sudo debugfs -R 'dump <8> journal' /dev/sdX .`

In der Praxis werden nur die wenigsten Smartphones gerooted sein oder einen offenen Bootloader haben. Moderne Androidgeräte müssen darüber hinaus verschlüsselt sein. [1]
Leider konnte das Auf- und Zuklappen des Laptops in der VM nicht nachgestellt und die Zeitpunkte somit auch nicht festgestellt werden.
Insgesamt sind wir damit zufrieden wie genau sich die Timeline des Tatvorgangs wiederherstellen lies.

[1] `https://source.android.com/docs/security/features/encryption`

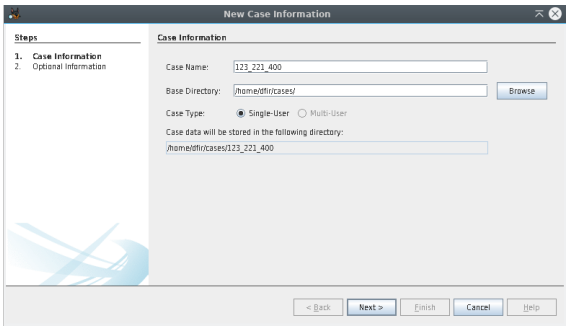
A Volatility-Profilerstellung

```
sudo apt install ewf-tools dwarfdump

sudo mkdir -p /mnt/ssd_ewf /mnt/ssd
sudo ewfmount /media/dfir/evidence_stick/ssd.E01 /mnt/ssd_ewf

sudo file /mnt/ssd_ewf/ewf1
# /mnt/ssd_ewf/ewf1: DOS/MBR boot sector


sudo mmls /mnt/ssd_ewf/ewf1
# 002:  000:000   0000002048   0033552383   0033550336   Linux (0x83)

dataoffset=`echo 2048 \* 512 | bc`
sudo mount -o ro,loop,noexec,noload,offset=$dataoffset /mnt/ssd_ewf/ewf1
↪  /mnt/ssd

file /mnt/ssd/vmlinuz
# /mnt/ssd/vmlinuz: symbolic link to boot/vmlinuz-5.4.0-150-generic


sudo cp -r /mnt/ssd/usr/src/linux-headers-5.4.0-150-generic/
↪  /mnt/ssd/usr/src/linux-hwe-5.4-headers-5.4.0-150/ /usr/src/
sudo cp -r /mnt/ssd/lib/modules/5.4.0-150-generic/ /lib/modules/

git clone https://github.com/volatilityfoundation/volatility.git
↪  ~/FDA/volatility
cd ~/FDA/volatility/tools/linux

KVER=5.4.0-150-generic CONFIG_DEBUG_INFO_DWARF4=y make
sudo zip Ubuntu1804.zip module.dwarf
↪  /mnt/ssd/boot/System.map-5.4.0-150-generic
# sudo chown $USER:$USER Ubuntu1804.zip

sudo umount /mnt/ssd
sudo umount /mnt/ssd_ewf
```

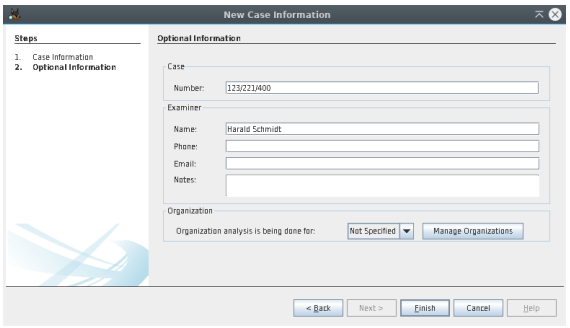
Listing 2: Erstellung eines angepassten Volatility-Profils

B Autopsy Screenshots

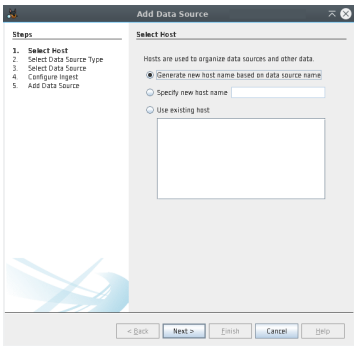
Abbildung 20: Erstellen eines Falls in Autopsy



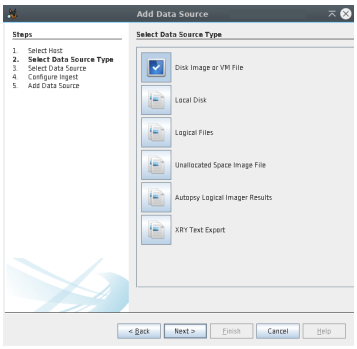
(a) Fallinformation



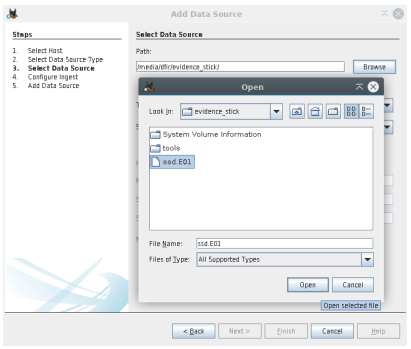
(b) Optionale Angaben



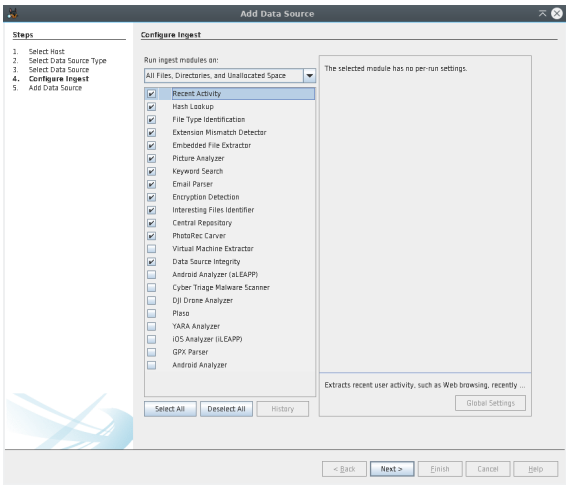
(c) Neue Datenquelle



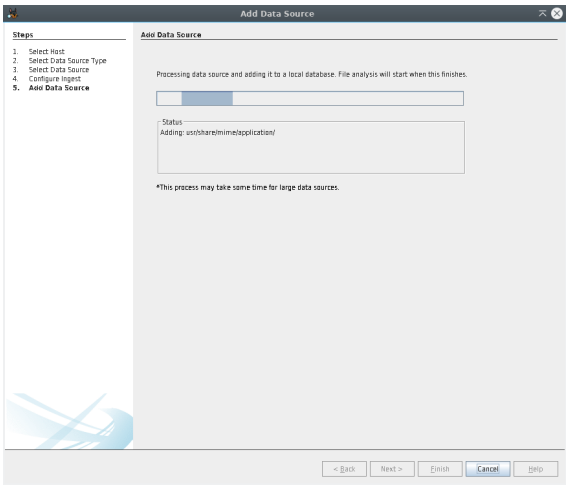
(d) Typ der Datenquelle



(e) Auswahl der Quelle



(f) Auswahl von Analyse-Modulen



(g) Verarbeitung der Datenquelle

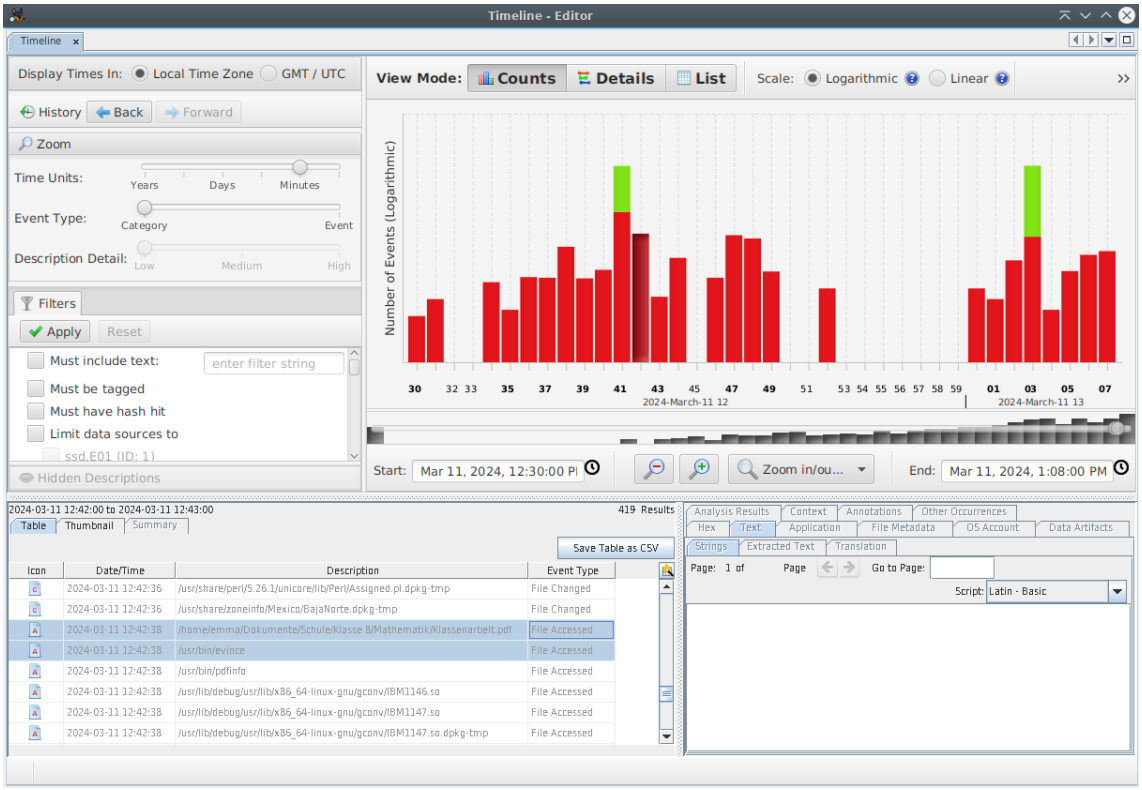


Abbildung 21: Autopsy zeigt eine Timeline mit allen registrierten Dateiänderungen im Tatzeitraum. Man erkennt, dass der Zugriff auf das Klassenarbeits-PDF und den PDF-Viewer Evince sehr nah beieinander liegen.

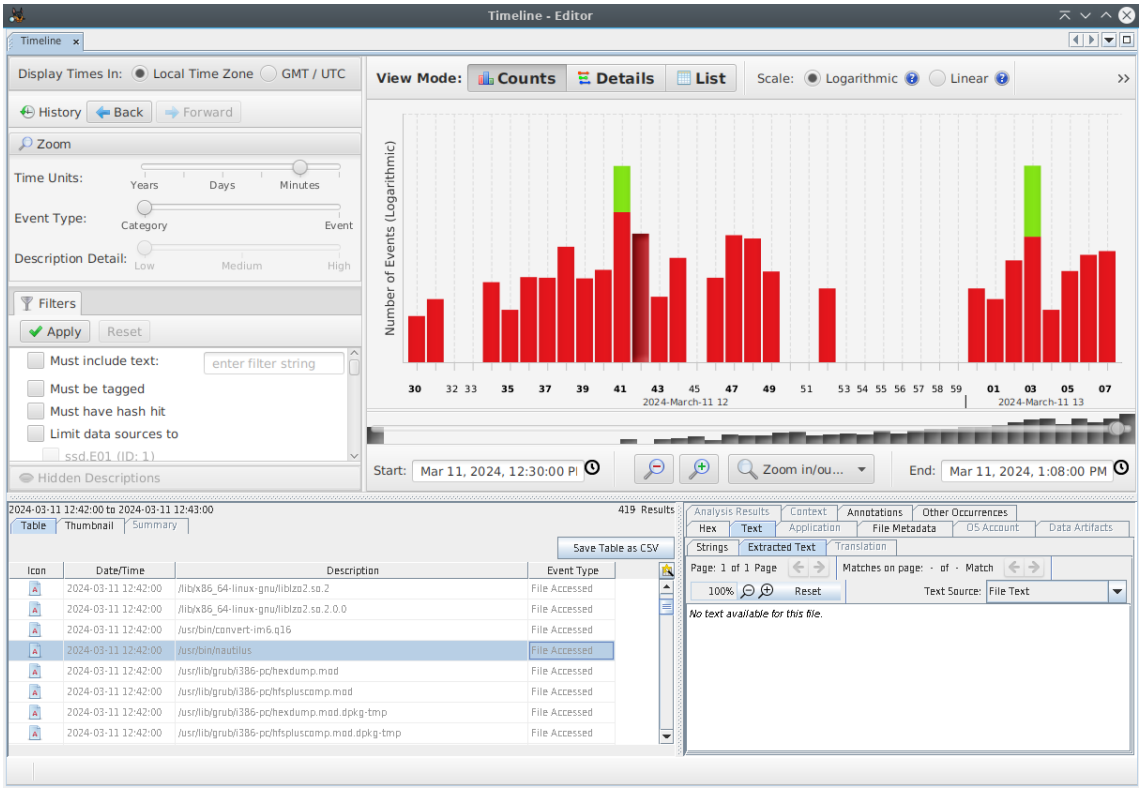


Abbildung 22: Autopsy Timeline: Aufruf des Dateimanagers Nautilus

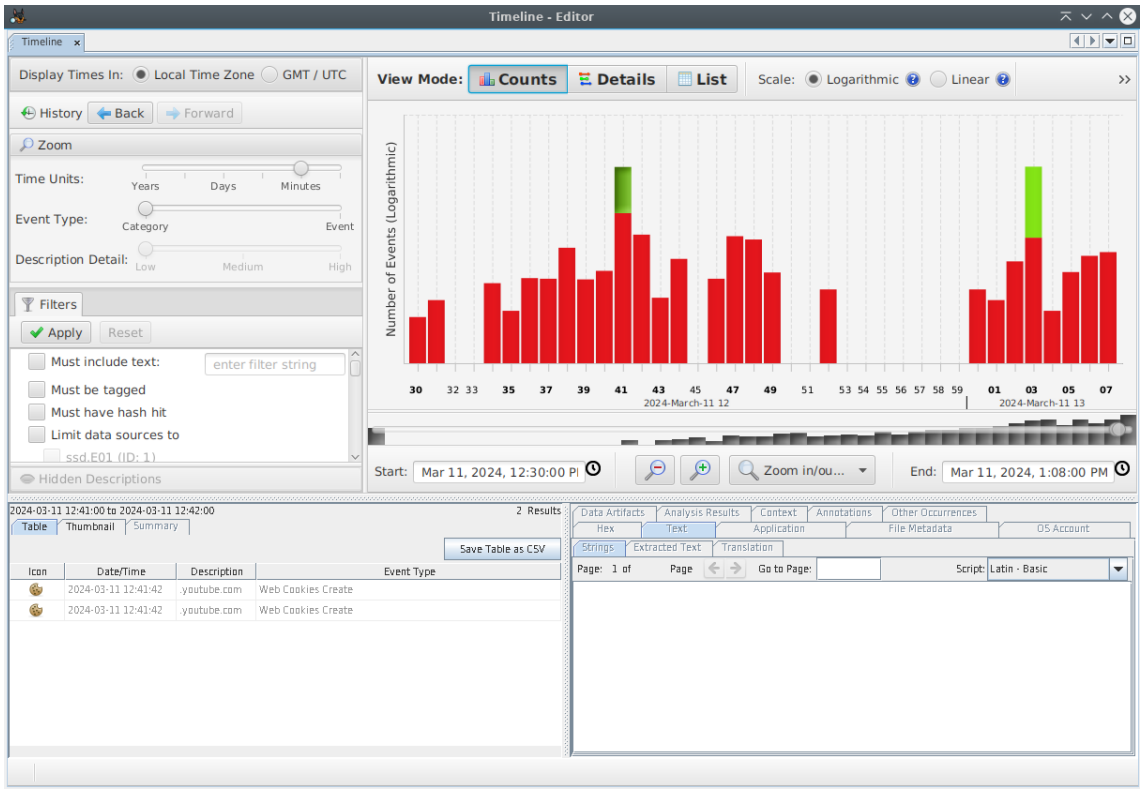


Abbildung 23: Autopsy Timeline: Firefox Cookies

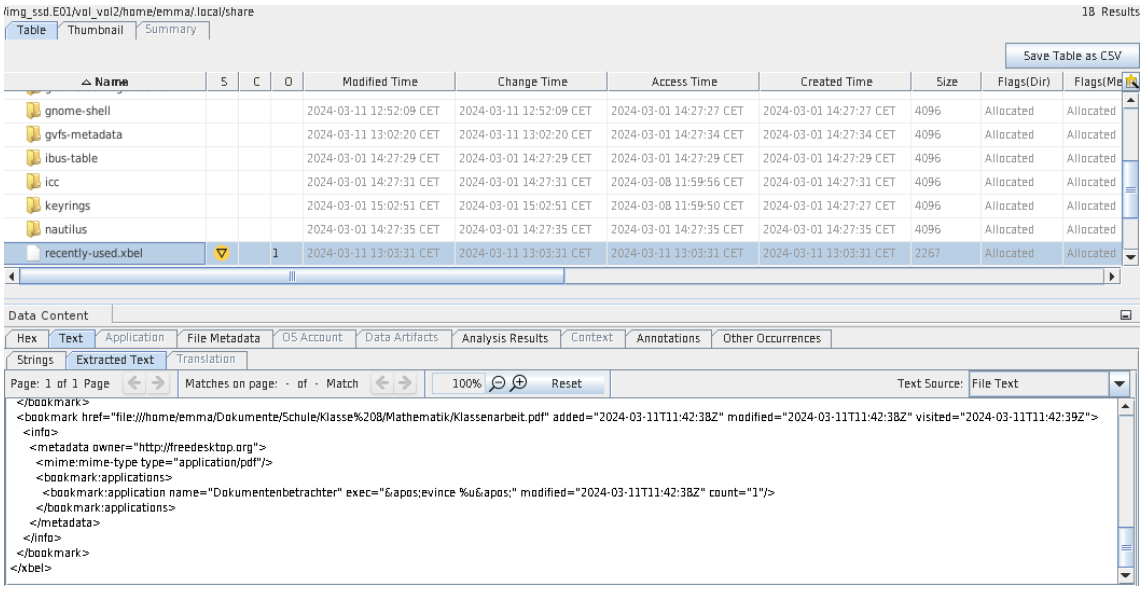


Abbildung 24: Autopsy: Liste kürzlich verwendeter Dateien („recently-used.xbel“)

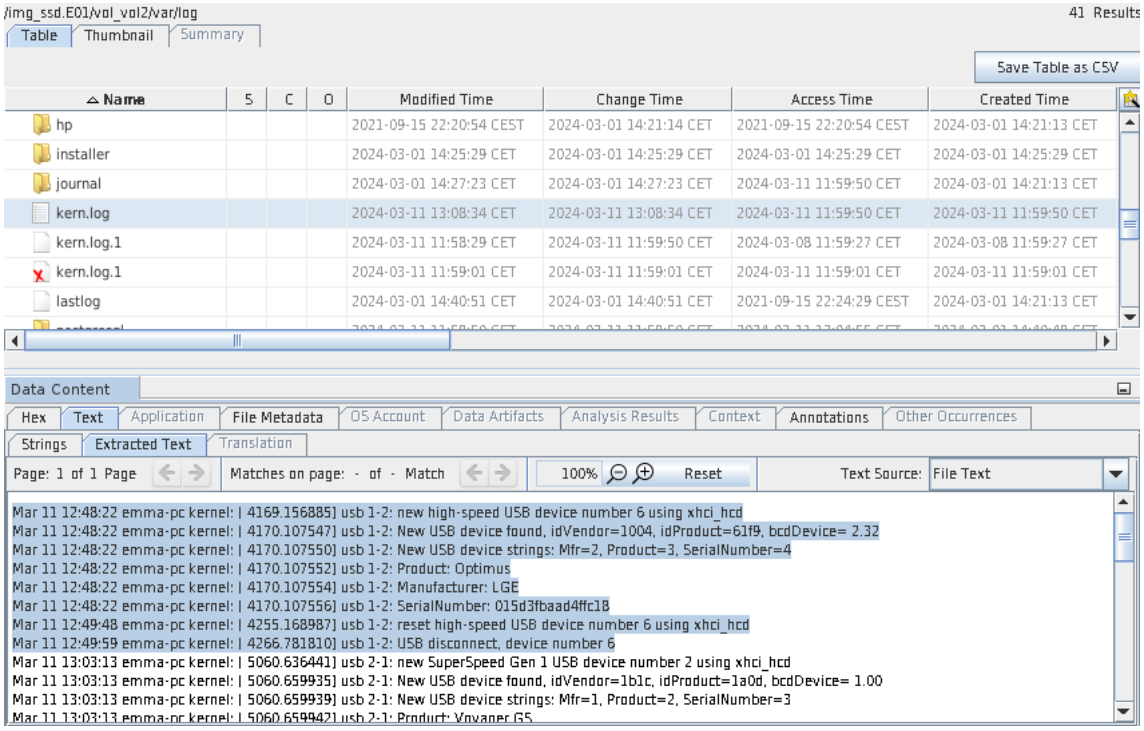


Abbildung 25: Autopsy: Historie der USB-Geräte aus „kern.log“

C WhatsApp Verlauf

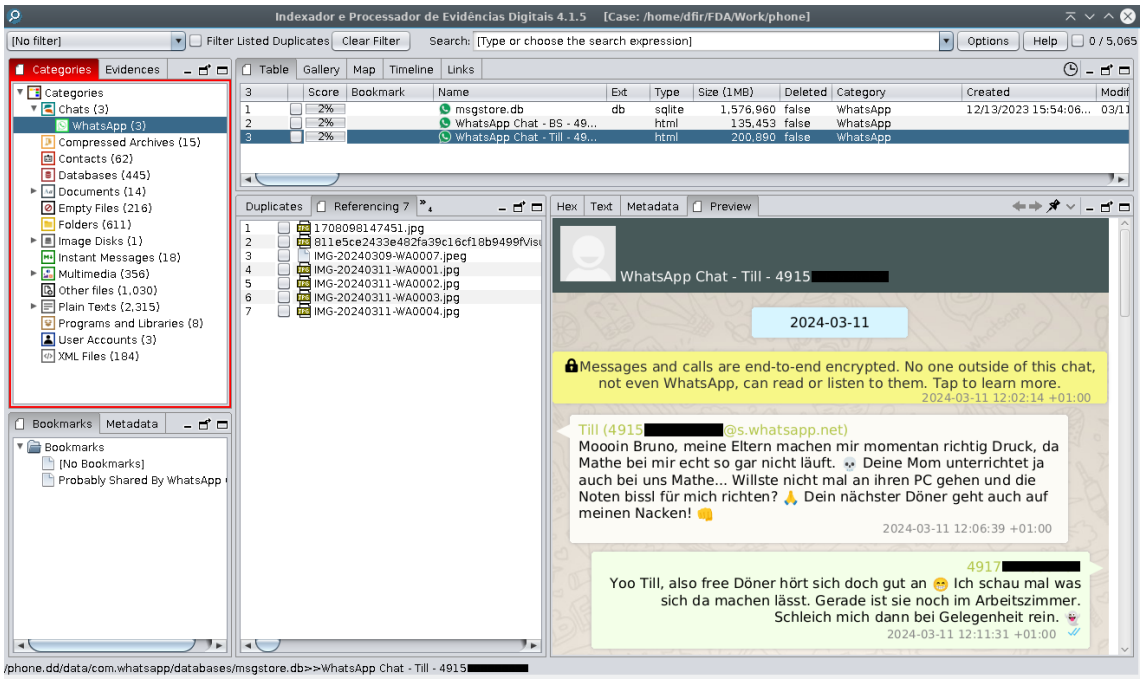


Abbildung 26: IPED: WhatsApp Verlauf

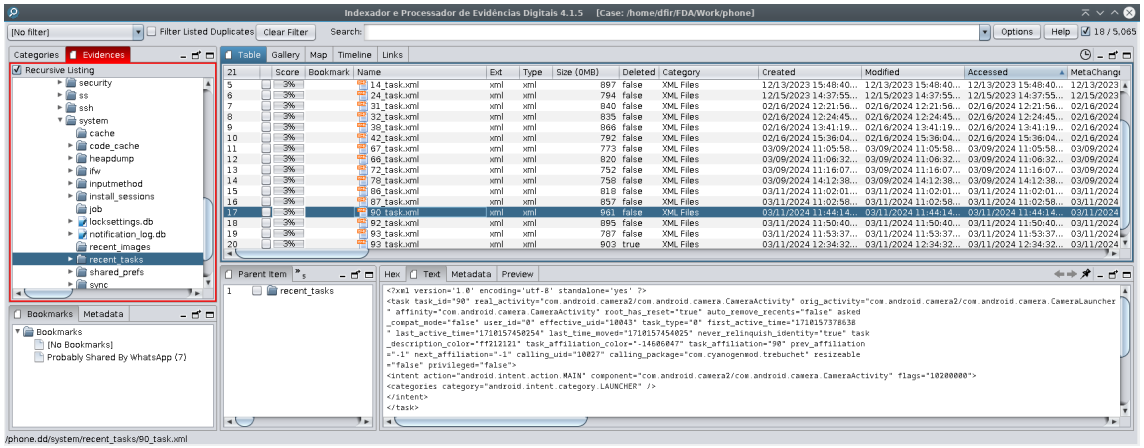


Abbildung 27: IPED: Öffnen der Kamera-App nachvollziehbar

D Autopsy Installation Linux

```
1  mkdir ~/FDA && cd ~/FDA
2
3  wget https://github.com/sleuthkit/autopsy/releases/download/autopsy-4.21.0
   ↪  /autopsy-4.21.0.zip
4  unzip autopsy-4.21.0.zip autopsy-4.21.0/linux_macos_install_scripts/*
5
6  sudo bash
   ↪  ./autopsy-4.21.0/linux_macos_install_scripts/install_prereqs_ubuntu.sh
7  sudo bash
   ↪  ./autopsy-4.21.0/linux_macos_install_scripts/install_tsk_from_src.sh -p
   ↪  ./sleuthkit -b sleuthkit-4.12.1
8  sudo bash
   ↪  ./autopsy-4.21.0/linux_macos_install_scripts/install_application.sh -z
   ↪  autopsy-4.21.0.zip -i ~/autopsy -j
   ↪  /usr/lib/jvm/java-1.17.0-openjdk-amd64
9
10 ~/autopsy/autopsy-4.21.0/bin/autopsy --nosplash
```

Listing 3: Autopsy Installation unter Linux

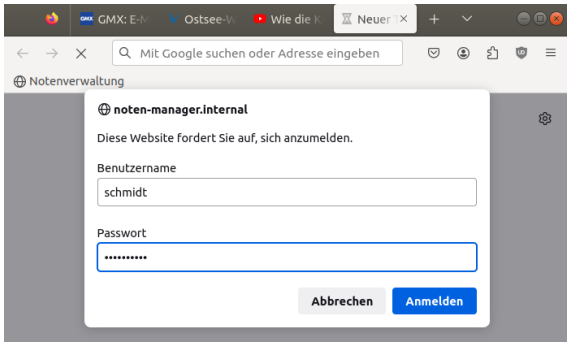
E IPED Installation und Einrichtung

```
1 wget https://download.bell-sw.com/java/11.0.22+12
  ↪ /bellsoft-jdk11.0.22+12-linux-amd64-full.deb -O
  ↪ ~/Downloads/bellsoft-jdk11.deb
2 sudo apt install ~/Downloads/bellsoft-jdk11.deb
3
4 wget https://github.com/sepinf-inc/IPED/releases/download/4.1.5
  ↪ /IPED-4.1.5_plus_java_plugins.zip -O
  ↪ ~/Downloads/IPED.zip
5 unzip ~/Downloads/IPED.zip -d ~/FDA/iped
6 echo "tskJarPath=/usr/local/share/java/sleuthkit-4.12.1.jar" >>
  ↪ ~/FDA/iped/iped-4.1.5/LocalConfig.txt
7 java -jar ~/FDA/iped/iped-4.1.5/iped.jar -d
  ↪ /media/dfir/evidence_stick/phone.dd -o ~/FDA/Work/phone
8 java -jar ~/FDA/Work/phone/iped/lib/iped-search-app.jar
```

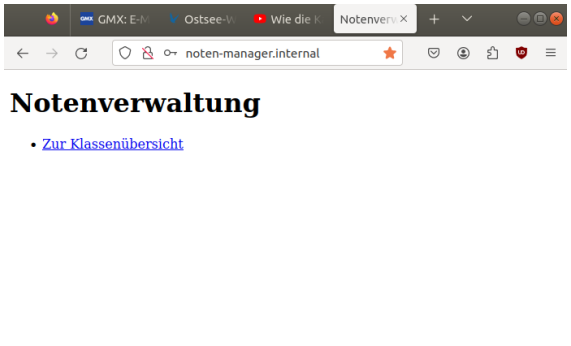
Listing 4: IPED Installation und Einrichtung unter Linux

F Notenverwaltung

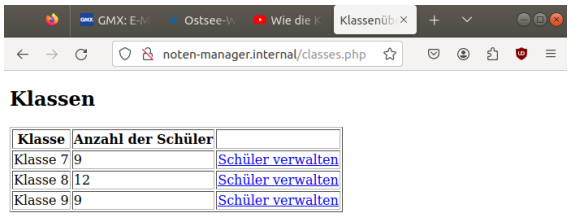
Abbildung 28: Seiten der Notenverwaltung



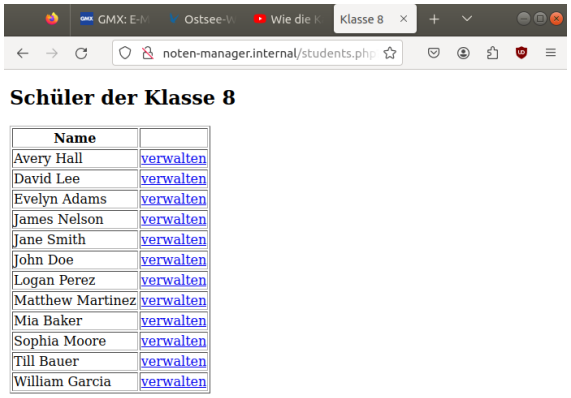
(a) Login (Basic Auth Prompt)



(b) Startseite



(c) Klassenübersicht



(d) Übersicht der Schüler einer Klasse

```php
<?php
require_once 'db_config.php';
if ($_SERVER['REQUEST_METHOD'] === 'POST') {
  $stmt = $pdo->prepare("UPDATE grade SET value = ?, comment = ? WHERE grade_id = ?");
  $stmt->execute([$_POST['grade'], $_POST['comment'], $_POST['grade_id']]);
  echo ("Note wurde geändert.");
}
$stmt = $pdo->prepare("SELECT name FROM student WHERE student_id = ?");
$stmt->execute([$_GET['student']]);
$student = $stmt->fetch(PDO::FETCH_ASSOC);
$stmt = $pdo->prepare("SELECT student.name as schueler, subject.name as fach, grade.value as note, grade.comment as kommentar, grade.grade_id as grade_id
  FROM grade, student, subject WHERE grade.student_id = student.student_id
  AND grade.subject_id = subject.subject_id AND student.student_id = ?
  ORDER BY grade.grade_id ASC");
$stmt->execute([$_GET['student']]);
$grades = $stmt->fetchAll(PDO::FETCH_ASSOC);
?>
<!DOCTYPE html>
<html lang="en">
<head>
 <meta charset="UTF-8">
 <title>Noten (<?= $student['name'] ?>)</title>
</head>
<body>
 <h2>Noten von <?= $student['name'] ?></h2>
 <?php foreach ($grades as $grade) : ?>
  <form method="post" id="form<?= $grade['grade_id'] ?>">
   <input type="hidden" name="student_id" value="<?=$_GET['student']?>" />
   <input type="hidden" name="grade_id" value="<?=$grade['grade_id']?>" />
  </form>
 <?php endforeach; ?>
 <table border="1">
  <tr><th>Fach</th><th>Note</th><th>Kommentar</th></tr>
   <?php foreach ($grades as $grade) : ?>
    <tr>
     <td><?=$grade['fach']?></td>
     <td>
      <select form="form<?=$grade['grade_id']?>" name="grade">
       <?php foreach ([1, 2, 3, 4, 5, 6] as $g) : ?>
        <option <?= ($g == $grade['note']) ? 'selected' : '' ?> value="<?= $g ?>"><?= $g ?></option>
       <?php endforeach; ?>
      </select>
     </td>
     <td>
      <input type="text" form="form<?=$grade['grade_id']?>" name="comment" value="<?=$grade['kommentar']?>"/>
     </td>
     <td><input type="submit" form="form<?=$grade['grade_id']?>" value="Ändern" /></td>
    </tr>
   <?php endforeach; ?>
 </table>
</body>
</html>
```

Listing 5: Quellcodeausschnitt der Notenverwaltung

Abbildungsverzeichnis

Tabellenverzeichnis

Quellcodeverzeichnis