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	Aufg	gabenstellung	4
2	Besc	hreibung des Falls	5
3	Dok	umentation der Umsetzung	7
	3.1	Dienstrechner	7
	3.2	Smartphone B	9
4	Fore	nsisches Gutachten	10
	4.1	Deckblatt	10
	4.2	Auftragsspezifikation	11
	4.3	Zusammenfassung der Ermittlungsergebnisse	12
		4.3.1 Fragestellungen	12
		4.3.2 Zeitliche Einordnung	13
	4.4	Untersuchungsobjekte	14
	4.5	Untersuchungswerkzeuge	14
	4.6	Untersuchung der Asservate	15
		4.6.1 Asservat 01 & 02	15
		4.6.2 Asservat 03	19
5	Dok	umentation der Erstellung der Images	22
	5.1	Dienstrechner: Hauptspeicher / RAM	22
	5.2	Dienstrechner: Sekundärspeicher / SSD	22
	5.3	Smartphone: Datenpartition (Interner Speicher)	23
6	Dok	umentation der Details zur forensischen Analyse	25
	6.1	Dienstrechner: Hauptspeicher / RAM	25
	6.2	Dienstrechner: Sekundärspeicher / SSD	26
	6.3	Smartphone: Datenpartition (Interner Speicher)	27
7	Zusa	mmenfassung und kritisches Review	28
Ar	nhang	A Volatility-Profilerstellung	30
Ar	nhang	B Autopsy Screenshots	31
Ar	nhang	C WhatsApp Verlauf	35
Ar	nhang	D Autopsy Installation Linux	36
Ar	nhang	E IPED Installation und Einrichtung	37

Anhang F Notenverwaltung	38
Abbildungsverzeichnis	40
Tabellenverzeichnis	41
Quellcodeverzeichnis	42

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.

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

 Tabelle 1: Zur Umsetzung verwendete Geräte

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 PDO¹ 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.

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



Abbildung 2: ER-Diagramm der Notendatenbank

	۵	owx GN	4X: E- M	🖌 Ostsee-W	🕒 Wie die K	Klasse 8	×	+	~			
\leftarrow	\rightarrow	С	08	noten-manage	r.internal /stude	nts.php: 🖍	3	\bigtriangledown	۲	பி	O	≡

Schüler der Klasse 8

Name	
Avery Hall	<u>verwalten</u>
David Lee	<u>verwalten</u>
Evelyn Adams	<u>verwalten</u>
James Nelson	<u>verwalten</u>
Jane Smith	<u>verwalten</u>
John Doe	<u>verwalten</u>
Logan Perez	<u>verwalten</u>
Matthew Martinez	<u>verwalten</u>
Mia Baker	<u>verwalten</u>
Sophia Moore	<u>verwalten</u>
Till Bauer	<u>verwalten</u>
William Garcia	<u>verwalten</u>

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

```
sudo htpasswd -b -c /etc/apache2/.htpasswd schmidt n0t3nl0g1n
1
2
3 sudo sed -i -f - /etc/apache2/sites-enabled/000-default.conf <<-EOF</pre>
4 /<VirtualHost \*:80>/a \\
     <Directory /var/www/html/> \\
\mathbf{5}
       AuthName "Dialog prompt" \\
6
       AuthType Basic \\
7
       AuthUserFile /etc/apache2/.htpasswd \\
8
       Require valid-user \\
9
     </Directory> \\
10
11 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 LineageOS² bzw. eine angepasste Variante³ neu aufgesetzt. Zusätzlich war TWRP⁴ 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 Anleitungen⁵, deren Effekt äquivalent sein sollte. Die Telefonnummer des Smartphone C wurde als Kontakt "Till" eingespeichert.

²https://lineageos.org/

³https://xdaforums.com/t/exp-lineageos-13-ufofficial-cve-2019-april.3621221/

⁴https://twrp.me/lg/lgoptimus4xhd.html

⁵https://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 xxxxxxx), 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:

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 Bildschirmsper-
		re 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	Offnen 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 ange-
		schlossen
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

Tabelle 2: Zeitliche Einordnung der Untersuchungsergebnisse

4.4 Untersuchungsobjekte

Objekt	Dateinamen	Hashwerte (MD5)
Asservat 01	ram.lime	ecd58bd396991f62878f819f580e588b
(Hauptspeicher des		
Dienstrechners)		
Asservat 02	ssd (EWF)	a645b43cadd1e7fd056cf6cfbbde0832
(SDD des Dienst-	ssd.E01	bfbd591643d5e86e766a1428a810ae4e
rechners)	ssd.E02	b6a7222ed7aeb5f6351f119803536799
	ssd.E03	794370272c949732579109420601a68c
Asservat 03	phone.dd	651cab7fa906e8e34272a7a617d8fa7a
(Interner Speicher		
Smartphone LG		
P880)		

Tabelle 3: Liste der Asservate

4.5 Untersuchungswerkzeuge

	_		
Tabelle 4: Die	verwendeten	Untersuchungswerkzeu	ıge

Name	Version	Funktion					
Tsurugi Acquire	2021.1	Live-Boot System mit Datenträger Schreib-					
		schutz und Werkzeugen zur Abbilderstellung					
Guymager	0.8.12	Erstellung von verifizierten Festplatten-					
		images 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 ei-					
		ner Rekonstruktion von WhatsApp Chats					
GNU strings	2.40	Extraktion von Zeichenketten aus Binärda-					
		ten					
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.





(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).

							5ave	Table as
⇔ Name	5	С	0	Modified Time	Change Time	Access Time	Created Time	Size
[current folder]				2024-03-11 11:59:50 CET	2024-03-11 11:59:50 CET	2024-03-11 12:04:55 CET	2024-03-01 14:20:59 CET	4096
[parent folder]				2024-03-01 14:40:46 CET	2024-03-01 14:40:46 CET	2024-03-06 15:22:07 CET	2024-03-01 14:19:55 CET	4096
alternatives.log				2024-03-01 14:41:12 CET	2024-03-01 14:41:12 CET	2021-09-15 22:25:48 CEST	2024-03-01 14:21:13 CET	45078
apache2				2024-03-11 11:59:50 CET	2024-03-11 11:59:50 CET	2024-03-11 12:04:55 CET	2024-03-01 14:40:46 CET	4096
apt				2024-03-08 12:02:51 CET	2024-03-08 12:02:51 CET	2021-09-15 22:30:10 CEST	2024-03-01 14:21:13 CET	4096
auth.log				2024-03-11 13:08:35 CET	2024-03-11 13:08:35 CET	2024-03-11 11:59:50 CET	2024-03-11 11:59:50 CET	3031
auth.log.1				2024-03-09 14:17:01 CET	2024-03-11 11:59:50 CET	2024-03-08 11:59:27 CET	2024-03-08 11:59:27 CET	3039
auth.log.1				2024-03-11 11:58:29 CET	2024-03-11 11:59:50 CET	2024-03-08 11:59:27 CET	2024-03-08 11:59:27 CET	68011
boot.log				2024-03-08 11:59:47 CET	2024-03-08 11:59:47 CET	2024-03-08 11:59:27 CET	2024-03-08 11:59:27 CET	7423
boot.log				2024-03-08 11:59:47 CET	2024-03-08 11:59:47 CET	2024-03-08 11:59:29 CET	2024-03-08 11:59:29 CET	326
btmp				2021-09-15 22:17:18 CEST	2024-03-01 14:21:13 CET	2021-09-15 22:17:18 CEST	2024-03-01 14:21:13 CET	0
cups				2024-03-11 11:59:50 CET	2024-03-11 11:59:50 CET	2024-03-11 12:04:55 CET	2024-03-01 14:21:13 CET	4096
Text Applicatio	n File f	Aetada	ita	05 Account Data Artifact	Analysis Results Co	Intext Annotations Oth	er Occurrences	
gs Extracted Text	Transla	ition		af Matala (Taut Fauren File Taut	
1 1 7 7 7 . 0 1	RON 7218 RON 7290]: pam]: pam	_unix _unix _unix	(cron:session): session closed (cron:session): session opener (cronsession): session closed	for user root d for user root by (uid=0) for user root			



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.

Directory Tree	Listing								
 ♦ 	/img_ssd.E01/val_val2/ha	me/emma/D	okume	ente/Schule/Klasse 7					5 Results
9 🗐 Data Sources		Summary	1					Emu	Table as CEV
P ssd.E01_1 Host				1	1		1	Dave	Table as CSV
vol1 (Upallocated: 0-2047)	∧ Name	5 C	0	Modified Time	Change Time	Access Time	Created Time	5ize	Flags(Dir)
vol2 (Unanocated: 0-2047)	Deutsch			2024-03-08 12:06:02 CET	2024-03-08 12:06:02 CET	2024-03-11 12:47:15 CET	2024-03-08 12:04:34 CET	4096	Allocated
CombanElles (0)	🗙 Klasse7.zip		1	2024-03-11 12:49:55 CET	2024-03-11 12:49:55 CET	2024-03-11 12:49:55 CET	2024-03-11 12:49:55 CET	32768	Unallocated
SUnalloc (11)	📕 Mathematik			2024-02-28 18:56:29 CET	2024-03-01 14:33:09 CET	2024-03-11 12:47:15 CET	2024-03-01 14:33:09 CET	4096	Allocated
🗢] bin (201)	[current folder]			2024-03-11 12:48:53 CET	2024-03-11 12:48:53 CET	2024-03-11 12:42:33 CET	2024-03-01 14:33:09 CET	4096	Allocated
🕶 退 boot (15)	[parent folder]			2024-02-16 14:35:50 CET	2024-03-01 14:33:09 CET	2024-03-11 12:42:32 CET	2024-03-01 14:33:09 CET	4096	Allocated
🕶 📜 cdrom (41)									
• J dev (15)									•
etc (300)									
• in nome (3)	Data Content								
• .cache (15)	Hex Text Applic	ation Fil	e Meta	data 05 Account Dat	Artifacts Analysis Result	ts Context Annotation	15 Other Occurrences		
- 📙 . config (17)	Metadata								^
🗢 📙 . gnupg (7)	Name:	/img_ssd.E	01/vol_	vol2/home/emma/Dokumen	e/Schule/Klasse 7/Klasse7.zip	1			
🗢 📜 . local (3)	Type:	File System	n –						
🗢 📜 . mozilla (5)	MIME Type:	application	/octet-	stream					
— 📜 .ssh (2)	Size:	32768							
🗢 📜 Bilder (5)	File Name Allocation:	Unallocate	d						
🛛 🔔 Dokumente (3)	Metadata Allocation:	Allocated							
🕈 📙 Schule (4)	Modified:	2024-03-13	12:49:	:55 CET					
9- 🔔 Klasse 7 (5)	Accessed:	2024-03-13	12:49:	:55 CET					
— 📙 Deutsch (4)	Created:	2024-03-13	12:49:	SS CET					
🔶 📙 Mathematik (3)	Changed:	2024-03-13	12:49:	:55 CET					
🛉 📜 Klasse 8 (3)	MD5:	b873f70922	216912	c646cba13cafc5668					
🗢 📙 Mathematik (4) 🦷	5HA-256:	c41625447	1483a3	aZab70ebaedb39f08c7c9334	8b776cd9394defa421aaa5a2	7			-



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).

ng_ssd.E01/vol_vol2/var/log/apac	he2											8 Result
	y I										5ar	ve Table as CSV
△ Name	5	С	0	Modified Time	Change Time	Access Time	Created Time	Size	Flags(Dir)	Flags(Meta)	Known	
📙 (current folder)				2024-03-11 11:59:50 CET	2024-03-11 11:59:50 CET	2024-03-11 12:04:55 CET	2024-03-01 14:40:46 CET	4096	Allocated	Allocated	unknown	/img_ssd.E01/vi
📙 (parent folder)				2024-03-11 11:59:50 CET	2024-03-11 11:59:50 CET	2024-03-11 12:04:55 CET	2024-03-01 14:20:59 CET	4096	Allocated	Allocated	unknown	/img_ssd.E01/v
access.log			0	2024-03-11 12:38:51 CET	2024-03-11 12:38:51 CET	2024-03-08 11:59:28 CET	2024-03-08 11:59:28 CET	2353	Allocated	Allocated	unknown	/img_ssd.E01/vi
error.log			0	2024-03-11 13:08:36 CET	2024-03-11 13:08:36 CET	2024-03-11 11:59:50 CET	2024-03-11 11:59:50 CET	464	Allocated	Allocated	unknown	/img_ssd.E01/vr
error.log.1			0	2024-03-11 11:59:50 CET	2024-03-11 11:59:50 CET	2024-03-08 11:59:28 CET	2024-03-08 11:59:28 CET	526	Allocated	Allocated	unknown	/img_ssd.E01/v/
🗙 error.log.1.gz			1	2024-03-06 14:44:46 CET	2024-03-11 11:59:50 CET	2024-03-06 14:39:46 CET	2024-03-11 11:59:50 CET	335	Unallocated	Allocated	unknown	/img_ssd.E01/vi
💼 error.log.2.gz			1	2024-03-06 14:44:46 CET	2024-03-11 11:59:50 CET	2024-03-06 14:39:46 CET	2024-03-11 11:59:50 CET	335	Allocated	Allocated	unknown	/img_ssd.E01/vi
other_vhosts_access.log				2024-03-08 11:59:28 CET	2024-03-08 11:59:28 CET	2024-03-08 11:59:28 CET	2024-03-08 11:59:28 CET	0	Allocated	Allocated	unknown	/img_ssd.E01/vr
Data Content Hex Text Application Strings Extracted Text Tr	File Me anslatic	tadat	a 1	05 Account 🍸 Data Artifacts	s Analysis Results Co	ntext Annotations Ot	her Occurrences					
Page: 1 of 1 Page 🛛 🗧 🔶 🛛	Matches	sonp	age:	- of - Match < ->	100% ⊖ 🕀 Reset					Text Source:	File Text	•
Construction Construction<												

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-

<pre>dfir@dfir-vm:~\$</pre>	strings	/media/dfir/evidence_stick/ram.lime	grep	n0t3nl0g1n
n0t3nl0g1n				
hpschmidt:n0t3n]	l0g1n			
schmidt:n0t3nl0g	g1n			
hpschmidt:n0t3n]	l0g1n			
hpschmidt:n0t3n]	l0g1n			

Abbildung 8: Arbeitsspeicherabbild enthält Zugangsdaten der Notenverwaltung

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

/img_ssd.E01/vol_vol2/var/log/postg Table Thumbnail Summar	ng_ssd.E01/vol_vol2/var/log/postgresql 4 Results Table Thumbnail Summary														
														5a	ve Table as CSV
⇔ Name	5	C	0	Modified	Time	Change	Time	Access Time	Creater	d Time	5ize	Flags(Dir)	Flags(Meta)	Known	
📜 (current folder)				2024-03-11 11:	:59:50 CET	2024-03-11 11:	59:50 CET	2024-03-11 12:04:55	ET 2024-03-01 14	:40:48 CET	4096	Allocated	Allocated	unknown	/img_ssd.E01/val
[parent folder]				2024-03-11 11:	59:50 CET	2024-03-11 11:	59:50 CET	2024-03-11 12:04:55	ET 2024-03-01 14	:20:59 CET	4096	Allocated	Allocated	unknown	/img_ssd.E01/val
postgresql-10-main.log			1	2024-03-11 13:	:08:36 CET	2024-03-11 13:	08:36 CET	2024-03-11 11:59:50 (EET 2024-03-08 11	:59:28 CET	5836	Allocated	Allocated	unknown	/img_ssd.E01/val
postgresql-10-main.log.1			0	2024-03-11 11:	:59:50 CET	2024-03-11 11:	59:50 CET	2024-03-11 11:59:50	ET 2024-03-11 11	:59:50 CET	1678	Allocated	Allocated	unknown	/img_ssd.E01/val
1															•
Data Content															
Hex Text Application F	ile Me	tadata	3 O	5 Account Da	ita Artifacts	Analysis Resu	ilts Cont	ext Annotations	Other Occurrences						
Strings Extracted Text Tra	Inslatio	п						_							
Page: 1 of 1 Page 🔶 🛚 M	latches	ап ра	age: -	of - Match	€⇒ L	100% ⊖ 🗩	Reset						Text Source:	File Text	-
2024-03-11 12:38:38.37 CET 1803 2024-03-11 12:38:38.37 CET 1803 2024-03-11 12:38:35.22 CET 1803 WHERE dass = 5 ORDER BY name 2024-03-11 12:38:35.22 CET 1803 2024-03-11 12:38:36.606 CET 1804	ASC 9] teac 9] teac 1 ASC 9] teac 9] teac 0] teac 0] teac	ther@: ther@: ther@: ther@: ther@:	school school school school school	LOG: statement LOG: execute p DETAIL: parami LOG: statement LOG: execute p DETAIL: parami	t: DEALLOC do_stmt_00 eters: \$1 = t: DEALLOC do_stmt_00	ATE pda_stmt_00 0000001: SELECT : 'B' ATE pda_stmt_00 0000001: SELECT r 200	000001 tudent_id, n 000001 iame FROM	ame FROM student student WHERE studen	t_id = \$1						=
2024-03-11 12:38:36 665 CEF 1804 2024-03-11 12:38:36 665 CEF 1804 2024-03-11 12:38:36 665 CEF 1804 WHERE grad WHERE grad AND studen ORDER 8Y g 2024-03-11 12:38:36 669 CEF 1804 2024-03-11 12:38:36 669 CEF 1804 2024-03-11 12:38:36 467 EEF 1804 2024-03-11 12:38:44,748 CEF 1804 2024-03-11 12:38:44,748 CEF 1804 2024-03-11 12:38:44,748 CEF 1804 2024-03-11 22:38:44,748 CEF 1804	0) teac 0) teac 0) teac , stude e.stude ubject .stude rade.gi 0) teac 0) teac 6) teac 6) teac 6) teac	ther@s ther@s ther@s nt, sul ent_id id = s it_id = rade_i ther@s ther@s ther@s	school school bject = stur subject = \$1 d ASC school school school school	DETAIL: parami LOG: statemeni LOG: execute p dent.student_id t.subject_id DETAIL: parami LOG: statemeni LOG: execute p DETAIL: parami	eters: \$1 = t: DEALLOC do_stmt_0C eters: \$1 = t: DEALLOC do_stmt_0C eters: \$1 =	20' ATE pda_stmt_00 000002: SELECT : '20' ATE pda_stmt_00 000001: UPDATE '1', \$2 = 'Leistung	000001 tudent.nam 000002 grade SET v: skontrolle (1	e as schueler, subject.n alue = \$1, comment =	ame as fach, grade.va 52 WHERE grade_id =	slue as note \$3	grade.comn	nent as komme	ntar, grade.gra	de_id as gra	de_id

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

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).

<u> </u>	Indexador e Processador de Evidências Digitais 4.1.5 🛛 [Case: /home/dfir/FDA/Work/phone] 🛛 🗖 🗸 🗸 🔗
[Checked] Filter Lis	ted Duplicates Clear Filters Search:
Categories 📕 Evidences 📃 🗖 🗖	🖸 Table Gallery Map Timeline Links 🕓 🕒
Recursive Listing	1 Score Bo Name Ext Type Size (0MB) Deleted Category Hash Created
► local	1 🗹 🧐 😼 Klasse7.zip zip zip 197,351 false Compresse 76905CAC53AE58092797586F2A4CDED1 03/11/2024 11:48:49
V media	
V 🚔 0	0 hits 🚺 2 Attachs/Subitems Parent Item 2 Duplicates 🎽 🗗 🗖 Hex Metadata Preview 🗋 Text 🔶 🔶 + 📌 _ 🗗 🗖
► <u></u> 0	1 Deutsch
► 📄 Alarms	2 🗌 🕋 Mathematik
Android	Ulktat.oot
Download	Mathematik
Movies	
🕨 📄 Music	NJASSENITOET. DOI
► Notifications	
	METADATA: Contact Length: 197551
🗌 Bookmarks Metadata 📃 📑 🗖	1 Indexer-Content-Type: application/zip
🔻 🚔 Bookmarks	X-TIKA:Parsed-By: iped.parsers.compress.PackageParser
[No Bookmarks]	X-TIKA:Parsed-By-Full-Set: iped.parsers.compress.PackageParser
Probably Shared By WhatsApp (7)	1 - <u>7</u> - 7

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 AVML¹ (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 Acquire² hochgefahren. Dieses bindet Datenträger standardmäßig schreibgeschützt ein. Mit dem dort vorinstallierten Programm Guymager³ wurden Images im Expert Witness Format erstellt und anschließend automatisch verifiziert (Abb. 15).

 $^{{}^{1} \}tt{https://github.com/microsoft/avml}$

²https://tsurugi-linux.org/index.php

³https://github.com/cyberknightX/Guymager

Serial nr.	Linux device	Model	State	•	Size	Hidden areas	Bad sectors
VB2-01700376	/dev/sr0	VBOX_CD-ROM	🔿 Idle		1.2GB	unknown	
070879682C1B9777	/dev/sdb	Corsair Voyager_GS	🔿 Idle		63.3GB	unknown	
VB5f7509ff-3ac295fd	/dev/sda	VBOX_HARDDISK	🔵 Idle		17.2GB	unknown	
	/dev/loop0	filesystem.squ: A	cquire image		823.0MB	unknown	

Abbildung 14: Guymager Übersicht

0	A	cquire image (of /dev/sda		0							
File format												
O Linux dd raw ir	nage (file extensio	on .dd or .xxx)		✓ Split image files								
• Expert Witness	Format, sub-form	at Guymager (file	extension .Exx)	Split size 2047	MiB 🔻							
Case number	123/221/400											
Evidence number	2											
Examiner	Harald Schmidt	larald Schmidt										
Description	SSD-Speicherabb	SD-Speicherabbild des Dienstrechners von Emma Schmidt										
Notes	/B5f7509ff-3ac295fd											
Destination												
Image directory		/media/root/evide	ence_stick/									
Image filename (w	vithout extension)	ssd										
Info filename (with	nout extension)	ssd										
Hash calculation / ve	erification											
✓ Calculate MD5		✓ Calculate SHA	-1	✔ Calculate SHA-2	56							
Re-read source	after acquisition f	for verification (tak	es twice as long)									
✓ Verify image af	ter acquisition (ta	kes twice as long)										
Cancel		Dupl	icate image	Start								

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 SmartphoneModell 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 Verfügung¹, 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# volatilit	yplugins=µ	profile=LinuxUbu	ntu1804x64 -f /ev	/idence/	'ram.lime linux_psl:	ist 2> /dev.	/null	
Offset	Name	Pid	PPid	Uid	Gid	DTB	Start Time		
0xffff8e3bfc1daf00	systemd					0x000000000bba36000	2024-03-11	10:39:20	UTC+0000
0xffff8e3bfc1dc680	kthreadd						2024-03-11	10:39:20	UTC+0000
0xffff8e3bfc1dde00	rcu_qp						2024-03-11	10:39:20	UTC+0000
0xffff8e3bfc1d9780	rcu_par_gp						2024-03-11	10:39:20	UTC+0000
0xffff8e3bfc1f0000	kworker/0:0H						2024-03-11	10:39:20	UTC+0000
		• •			•				
0xffff8e3b66338000	kworker/0:7	8164					2024-03-11	11:41:59	UTC+0000
0xffff8e3b438a1780	firefox	8185		1000	1000	0x000000003868000	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					2024-03-11	12:03:41	UTC+0000
0xffff8e3b42ec0000	scsi_tmf_3	9005					2024-03-11	12:03:41	UTC+0000
0xffff8e3b42ec1780	usb-storage	9006					2024-03-11	12:03:41	UTC+0000
0xffff8e3b5c709780	uas	9009					2024-03-11	12:03:41	UTC+0000
0xffff8e3b926dde00	mount.ntfs	9047				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					2024-03-11	12:04:14	UTC+0000
0xffff8e3bfc3bde00	sudo	9222	9165			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

¹https://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.



Abbildung 18: Carving des Archivs

 $^{^{2} \}tt https://ext4magic.sourceforge.net/journal_de.html$

6.3 Smartphone: Datenpartition (Interner Speicher)

Die verwendete IPED Version benötigt ein Java 11 JDK mit Java
FX 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.

👂 Indexador e Processador de Evidências Digitais 4.1.5 [Case: /home/dfir/FDA/Work/phone] 🦷 🗸 🗸	^ 🛞
[No filter] Filter Listed Duplicates Clear Filter Search: 015d3fbaad4ffc18 Options Help 🗹 18	/ 5,065
Categories Evidences Categories Evidences Categories	₫ □
Categories Evidences Table Gallery Map Timeline Links Categories Categories Categories Chats (3) Compressed Archives (15) Contracts (62) Databases (445) Documents (14) Empty Files (216) Folders (611) Image Disks (1) Image D	Treate 3/11// Basic Pro
accessed Mon Mar 11 12:01:03 CET 2024 meta Changed Sun Jan 01 05:10:55 CET 2012	perties
hash 2965A18F61460E457E8DA042707C7FCC	

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.

³https://github.com/sepinf-inc/IPED/wiki/Linux

⁴https://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.

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

A Volatility-Profilerstellung

```
1 sudo apt install ewf-tools dwarfdump
2
3 sudo mkdir -p /mnt/ssd_ewf /mnt/ssd
4 sudo ewfmount /media/dfir/evidence_stick/ssd.E01 /mnt/ssd_ewf
5
6 sudo file /mnt/ssd_ewf/ewf1
7 # /mnt/ssd_ewf/ewf1: DOS/MBR boot sector
8
9
10 sudo mmls /mnt/ssd_ewf/ewf1
  # 002: 000:000
                     0000002048
                                   0033552383
                                                 0033550336
                                                             Linux (0x83)
11
12
13 dataoffset=`echo 2048 \* 512 | bc`
14 sudo mount -o ro,loop,noexec,noload,offset=$dataoffset /mnt/ssd_ewf/ewf1
   \rightarrow /mnt/ssd
15
16 file /mnt/ssd/vmlinuz
17 # /mnt/ssd/vmlinuz: symbolic link to boot/vmlinuz-5.4.0-150-generic
18
19
20 sudo cp -r /mnt/ssd/usr/src/linux-headers-5.4.0-150-generic/
   \rightarrow /mnt/ssd/usr/src/linux-hwe-5.4-headers-5.4.0-150/ /usr/src/
21 sudo cp -r /mnt/ssd/lib/modules/5.4.0-150-generic/ /lib/modules/
22
23 git clone https://github.com/volatilityfoundation/volatility.git
   → ~/FDA/volatility
24 cd ~/FDA/volatility/tools/linux
25
26 KVER=5.4.0-150-generic CONFIG_DEBUG_INFO_DWARF4=y make
  sudo zip Ubuntu1804.zip module.dwarf
27
   \rightarrow /mnt/ssd/boot/System.map-5.4.0-150-generic
28 # sudo chown $USER:$USER Ubuntu1804.zip
29
30 sudo umount /mnt/ssd
31 sudo umount /mnt/ssd_ewf
```

Listing 2: Erstellung eines angepassten Volatility-Profils

 \otimes

New Ca

B Autopsy Screenshots

Abbildung 20: Erstellen eines Falls in Autopsy



- (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

△ Name									Save T	able as C
	5	С	0	Modified Time	Change Time	Access Time	Created Time	5ize	Flags(Dir)	Flags(I
gnome-shell				2024-03-11 12:52:09 CET	2024-03-11 12:52:09 CET	2024-03-01 14:27:27 CET	2024-03-01 14:27:27 CET	4096	Allocated	Allocate
gvfs-metadata				2024-03-11 13:02:20 CET	2024-03-11 13:02:20 CET	2024-03-01 14:27:34 CET	2024-03-01 14:27:34 CET	4096	Allocated	Allocate
ibus-table				2024-03-01 14:27:29 CET	2024-03-01 14:27:29 CET	2024-03-01 14:27:29 CET	2024-03-01 14:27:29 CET	4096	Allocated	Allocate
icc				2024-03-01 14:27:31 CET	2024-03-01 14:27:31 CET	2024-03-08 11:59:56 CET	2024-03-01 14:27:31 CET	4096	Allocated	Allocat
keyrings				2024-03-01 15:02:51 CET	2024-03-01 15:02:51 CET	2024-03-08 11:59:50 CET	2024-03-01 14:27:27 CET	4096	Allocated	Allocat
nautilus				2024-03-01 14:27:35 CET	2024-03-01 14:27:35 CET	2024-03-01 14:27:35 CET	2024-03-01 14:27:35 CET	4096	Allocated	Allocati
recently-used.xbel		1		2024-03-11 13:03:31 CET	2024-03-11 13:03:31 CET	2024-03-11 13:03:31 CET	2024-03-11 13:03:31 CET		Allocated	Allocat
Text Application File	e Metada slation	ata	057	Account Data Artifacts	Analysis Results Conte	xt Annotations Other	Occurrences			
ngs Extracted Text Trans		-			100M O D Drust			avt Source:	File Text	
ngs Extracted Text Trans : 1 of 1 Page 🗲 🔶 Mat ookmark>	tches on	page:	- 0	af - Match 🧲 🔶	100% Reset		1	EAL SUBILE.		

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

							Save Table as 0
⇔ Name	5	C	0	Modified Time	Change Time	Access Time	Created Time
b hp				2021-09-15 22:20:54 CEST	2024-03-01 14:21:14 CET	2021-09-15 22:20:54 CEST	2024-03-01 14:21:13 CET
installer				2024-03-01 14:25:29 CET	2024-03-01 14:25:29 CET	2024-03-01 14:25:29 CET	2024-03-01 14:25:29 CET
journal				2024-03-01 14:27:23 CET	2024-03-01 14:27:23 CET	2024-03-11 11:59:50 CET	2024-03-01 14:21:13 CET
kern.log				2024-03-11 13:08:34 CET	2024-03-11 13:08:34 CET	2024-03-11 11:59:50 CET	2024-03-11 11:59:50 CET
kern.log.1				2024-03-11 11:58:29 CET	2024-03-11 11:59:50 CET	2024-03-08 11:59:27 CET	2024-03-08 11:59:27 CET
kern.log.1				2024-03-11 11:59:01 CET	2024-03-11 11:59:01 CET	2024-03-11 11:59:01 CET	2024-03-11 11:59:01 CET
lastlog				2024-03-01 14:40:51 CET	2024-03-01 14:40:51 CET	2021-09-15 22:24:29 CEST	2024-03-01 14:21:13 CET
				2024 02 22 22 50 50 557	2024 02 22 23 00 00 00 000	2024 02 22 22 04 FF CFT	
Content	V						
Content Text Application	File I	Metada Ition	ata	05 Account Y Data Artifact	s Analysis Results Co	ntext Annotations Oth	er Occurrences
a Content x Text Application ings Extracted Text e: 1 of 1 Page	File Match	Metada ition hes on	ata page:	O5 Account Y Data Artifact	s Y Analysis Results Y Co 100% ⊙ ⊕ Reset	ntext Annotations Oth Text Source:	er Occurrences

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

C WhatsApp Verlauf



Abbildung 26: IPED: WhatsApp Verlauf

Q			Indexador	e Processador de	Evidênci	as Digit	ais 4.1.5 [Ca	se: /home	/dfir/FDA/Work/phone]	1			⊼ ∨ ^ ⊗
[No filter]	uplicates	Clear Filter	Search:									Options He	lp 🗹 18 / 5.065
	Table	Gallony	Mon Timeline Lin	10									0 -
Vil Requires Listing	al	Gallery	Map Innenne un			Trees	01 (01-02)	Deleted	Cotores.	Lower and	a a sa al de sa al	A	
h incoursive disting	21	score	Bookmark Name		EXI	Type	SIZE (UMB)	Deleted	Category	created	Modified	Accessed	Metachangi
security	5		14_ta	skarni	xml	xml	89	7 false	XML Files	12/13/2023 15:48:40	12/13/2023 15:48:40	12/13/2023 15:48:40	12/13/2023
*	6		24_ta	sk.aml	imi	×ml	/9-	1 faise	XML Files	12/15/2023 14:37:55	12/15/2023 14:37:55	12/15/2023 14:37:55	12/15/2023
🕨 🔤 ssh	2	370	31_ta	sk.xumi	ann	sini	84	false	XML FIES	02/16/2024 12:21:56	02/16/2024 12:21:56	02/16/2024 12:21:56	02/16/2024
🔻 🚞 system	ŝ	3%		sk.adrii sk.adrii	2010	- International	0.0	5 Taise 2 foloe	XML Files	02/16/2024 12:24:43	02/16/2024 12:24:43	02/16/2024 12:24:45	02/16/2024
ache 📄	10	206	30_La	skuuni skuuni	urol.	surol	70	2 folce	XML Files	02/10/2024 15:41:19	02/10/2024 15:41:19	02/10/2024 13:41:19	02/10/2024
► Code cache	11	3%	42_10	sk vrol	wrol	am	70.	falce	YML Files	02/00/2024 13:36:54	02/00/2024 13:35:54	02/00/2024 13:55:59	02/10/2024
▶ m heapdump	12	3%	- 66 ta	skaml	arrol	xml	82) false	XML Files	03/09/2024 11:06:32	03/09/2024 11:06:32	03/09/2024 11:06:32	03/09/2024
► C ify	13	3%	🧧 72 ta	sk.xml	aml	xml	75	2 false	XML Files	03/09/2024 11:16:07	03/09/2024 11:16:07	03/09/2024 11:16:07	03/09/2024
b 🗁 investored	14	3%	🧧 78 ta	sk.xml	aml	xml	75	a false	XML Files	03/09/2024 14:12:38	03/09/2024 14:12:38	03/09/2024 14:12:38	03/09/2024
P i inputitetriod	15	3%	🧧 86 ta	sk.xml	aml	xml	81	3 false	XML Files	03/11/2024 11:02:01	03/11/2024 11:02:01	03/11/2024 11:02:01	03/11/2024
▶	16	3%	🧧 87 ta	sk.xml	aml	xml	85	7 false	XML Files	03/11/2024 11:02:58	03/11/2024 11:02:58	03/11/2024 11:02:58	03/11/2024
iap jop	17	3%	🤗 90 ta	skaani	xml	×ml	96	l false	XML Files	03/11/2024 11:44:14	03/11/2024 11:44:14	03/11/2024 11:44:14	03/11/2024
Iocksettings.db	18	3%	🤷 92 ta	skaml	xml	xml	89	5 false	XML Files	03/11/2024 11:50:40	03/11/2024 11:50:40	03/11/2024 11:50:40	03/11/2024
notification log.db	19	3%	🧧 93 ta	skaml	xml	xml	78	7 false	XML Files	03/11/2024 11:53:37	03/11/2024 11:53:37	03/11/2024 11:53:37	03/11/2024
arecent images	20	3%	🧧 93 ta	skaml	xml	×ml	90:	3 true	XML Files	03/11/2024 12:34:32	03/11/2024 12:34:32	03/11/2024 12:34:32	03/11/2024 *
In recent tasks													7.6
b C oborod profe	0.0												
- instated_piers	Paren	nt items	- C H6	x i lext Meta	adata Pri	eview						-	- <u></u>
sync	1) 📄 recent	tasks 🛛 🖓	xml version='1.0	' encodin	q='utf-l	3' standalone='	yes' ?>					
			- <t< td=""><td>ask task_id="90"</td><td>real_act</td><td>ivity="</td><td>on.android.cam</td><td>era2/con.</td><td>android.camera.Camera</td><td>Activity' orig_activit</td><td>y="com.android.camera2.</td><td>com.android.camera.Cam</td><td>neraLauncher 📉</td></t<>	ask task_id="90"	real_act	ivity="	on.android.cam	era2/con.	android.camera.Camera	Activity' orig_activit	y="com.android.camera2.	com.android.camera.Cam	neraLauncher 📉
🗇 Bookmarks Metadata 🛛 🗖 🗖			· · ·	affinity="con.an	droid.cam	era.Can	eraActivity* ro	ot_has_re	set="true" auto_remov	e_recents="false" aske	d l		
			-	ompat_mode="fals	e' user_i	d="0" e	ffective_uid="1	0043° tas	k_type="0" first_acti	ve_time=*1710157378638			
🔻 🚞 Bookmarks				last_active_time	=*1710157	458254*	last_time_move	d="171015	7454025" never_reling	uish_identity="true" t	ask		
[No Bookmarks]				escription_color	-***21212	1° task	_affiliation_co	lor="-146	06047" task_affiliati	on="90" prev_affiliati	on		
Probably Shared By WhatsApp (7)				.1" next_affilia	tion="-1"	callin	g_uid="10027" o	alling_pa	ickage="con.cyanogenno	d.trebuchet" resizeabl	=		
				false" privilege	d="false"	>							
			4	ntent action="an	droid.int	ent.act:	Lon.MAIN" Compo	nent="com	.android.cawera2/cow.	android.cawera.CameraA	tivity" flags="102000	10">	
			<0	ategories catego	ry="andro	id.inter	nt.categozy.LAU	INCHER" />					
			4	intent>									-
			4	task>									¥.
			7.6										7.6
/phone.dd/system/recent_tasks/90_task.xml													

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
  \rightarrow /autopsy-4.21.0.zip
4 unzip autopsy-4.21.0.zip autopsy-4.21.0/linux_macos_install_scripts/*
\mathbf{5}
6 sudo bash
  7 sudo bash
  { \rightarrow } ./autopsy-4.21.0/linux_macos_install_scripts/install_tsk_from_src.sh -p \\
  \rightarrow ./sleuthkit -b sleuthkit-4.12.1
8 sudo bash
  \hookrightarrow 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

```
wget https://download.bell-sw.com/java/11.0.22+12

→ /bellsoft-jdk11.0.22+12-linux-amd64-full.deb -0

→ ~/Downloads/bellsoft-jdk11.deb

sudo apt install ~/Downloads/bellsoft-jdk11.deb

wget https://github.com/sepinf-inc/IPED/releases/download/4.1.5

→ /IPED-4.1.5_plus_java_plugins.zip -0

→ ~/Downloads/IPED.zip

sunzip ~/Downloads/IPED.zip -d ~/FDA/iped

echo "tskJarPath=/usr/local/share/java/sleuthkit-4.12.1.jar" >>

→ ~/FDA/iped/iped-4.1.5/LocalConfig.txt

java -jar ~/FDA/iped/iped-4.1.5/iped.jar -d

→ /media/dfir/evidence_stick/phone.dd -o ~/FDA/Work/phone

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



```
1 <?php
2 require_once 'db_config.php';
3 if ($_SERVER['REQUEST_METHOD'] === 'POST') {
     $stmt = $pdo->prepare("UPDATE grade SET value = ?, comment = ? WHERE grade_id = ?");
4
     $stmt->execute([$_POST['grade'], $_POST['comment'], $_POST['grade_id']]);
5
6
     echo ("Note wurde geändert.");
7 }
8 $stmt = $pdo->prepare("SELECT name FROM student WHERE student_id = ?");
9 $stmt->execute([$_GET['student']]);
10 $student = $stmt->fetch(PDO::FETCH_ASSOC);
11 $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
12
    AND grade.subject_id = subject.subject_id AND student.student_id = ?
13
14
     ORDER BY grade.grade_id ASC");
15 $stmt->execute([$_GET['student']]);
16 $grades = $stmt->fetchAll(PDO::FETCH_ASSOC);
17 ?>
18 <!DOCTYPE html>
19 <html lang="en">
20 <head>
   <meta charset="UTF-8">
21
   <title>Noten (<?= $student['name'] ?>)</title>
22
23 </head>
24
   <bodv>
    <h2>Noten von <?= $student['name'] ?></h2>
25
    <?php foreach ($grades as $grade) : ?>
26
27
     <form method="post" id="form<?= $grade['grade_id'] ?>">
      <input type="hidden" name="student_id" value="<?=$_GET['student']?>" />
28
     <input type="hidden" name="grade_id" value="<?=$grade['grade_id']?>" />
29
     </form>
30
    <?php endforeach; ?>
31
32
    FachNoteKommentar
33
      <?php foreach ($grades as $grade) : ?>
34
35
       <?=$grade['fach']?>
36
37
        <t.d>
         <select form="form<?=$grade['grade_id']?>" name="grade">
38
          <?php foreach ([1, 2, 3, 4, 5, 6] as g) : ?>
39
           <option <?= ($g == $grade['note']) ? 'selected' : '' ?> value="<?= $g ?>"><?= $g</pre>
40
           \rightarrow ?></option>
          <?php endforeach; ?>
41
         </select>
42
        43
        <t.d>
44
         <input type="text" form="form<?=$grade['grade_id']?>" name="comment"
45
         → value="<?=$grade['kommentar']?>"/>
46
        <input type="submit" form="form<?=$grade['grade_id']?>" value="Ändern" />
47
       \langle tr \rangle
48
      <?php endforeach; ?>
49
50
    51 </body>
52 </html>
```

Listing 5: Quellcodeausschnitt der Notenverwaltung

Abbildungsverzeichnis

1	Abstrahierte Darstellung des Szenarios	6
$2 \\ 3$	ER-Diagramm der Notendatenbank	8 8
$ \begin{array}{r} 4 \\ 5 \\ 6 \\ 7 \\ 8 \\ 9 \\ 10 \\ 11 \\ 12 \\ 13 \\ \end{array} $	Bilder vom Dienstrechner	15 16 17 17 18 18 19 20 20 20 21
14 15 16	Guymager Übersicht	23 23 24
17 18 19	Volatility-Plugin linux_pslist	25 26 27
20 21 22 23 24 25	Erstellen eines Falls in Autopsy	31 32 32 33 33 34
26 27	IPED: WhatsApp Verlauf	$\frac{35}{35}$
28	Seiten der Notenverwaltung	38

Tabellenverzeichnis

1	Zur Umsetzung verwendete Geräte	7
2	Zeitliche Einordnung der Untersuchungsergebnisse	13
3	Liste der Asservate	14
4	Die verwendeten Untersuchungswerkzeuge	14

Quellcodeverzeichnis

1	Konfiguration der Passwortabfrage	9
2	Erstellung eines angepassten Volatility-Profils	30
3	Autopsy Installation unter Linux	36
4	IPED Installation und Einrichtung unter Linux	37
5	Quellcodeausschnitt der Notenverwaltung	39