SACHVERSTÄNDIGENBÜRO

FINDE DIE WAHRHEIT

DIGITALE FORENSISCHE UNTERSUCHUNGEN

Technische Hochschule Mannheim Forensiklabor · CSB/IMB/IB · D-420815 Forum

Sachverständige/r

Team 16

Datum	**20.07.2025**
Büro	**Finde die Wahrheit**
Name	**Team 16**
Durchwahl	**0621 / 292 - 8745**
LVN	**0621-2025-4832**
Aktenzeichen	**S-125 Js 938/25**
	(Bitte bei Antwort angeben)

Beschuldigt: Deborah FLIEGNER, geb. 18.10.1949, wegen 184d StGB
wohnhaft Müllerweg 37, 25325 Luckau

1. Auftrag

Die Auftraggeberin, die Generalstaatsanwaltschaft (Frau Oberstaatsanwältin Blitzgescheit), beauftragte mit dem Auftrag vom 26.06.2025 das Team 16 des Sachverständigenbüro "Finde die Wahrheit" mit der forensischen Auswertung von sichergestellten Beweismitteln. Insbesondere war zu prüfen, ob sich anhand der Beweismittel Dateien mit kinderpornographischen Inhalten feststellen lassen. Hierzu sollte geprüft werden, ob sich gegebenenfalls Nutzung und/oder Verbreitung besagter Inhalte durch die Beschuldigte nachweisen lasse. Desweiteren waren elektronische Kommunikationen wie E-Mails oder Chats aus dem Beweismittel zu extrahieren. Die vollständige Dokumentation des Auftrags finden Sie im Anschluss.

---

2. Anlagen

- 1x USB-Festplatte mit Markierung "qcow2": Toshiba v63700 - A 500GB HDD-Festplatte - **Ass. Lfd.-Nr. 0.1** - **Intakt**

3. Ergebniszusammenfassung

Es wurde festgestellt:

1. dass in der Browser-History auf dem Datenträger mit der Lfd.-Nr. 1 der Beschuldigten FLIEGNER Google-Suchanfragen dokumentiert sind, die auf ein Interesse an Darstellungen von minderjährigen Personen in sexualisiertem Kontext hindeuten (*Anlage 1*),
2. dass auf dem entschlüsselten Container-Image auf dem Datenträger mit der Lfd.-Nr. 1 im Verzeichnis `/media/barney/067E7AF632AA2E11/xxx` Bilddateien enthalten sind, die Personen mit kindlichem Erscheinungsbild in suggestiven Posen zeigen (*Anlage 2*),
3. dass sich auf dem Datenträger mit der Lfd.-Nr. 1 gelöschte Bilddateien befanden, die durch Wiederherstellung zugänglich gemacht werden konnten und vergleichbare Inhalte aufweisen (*Anlage 3*),
4. dass Einträge in der Datei `/home/barney/.local/share/recently-used.xbel` Hinweise auf eine Nutzung des verschlüsselten Containers sowie der zugehörigen Keepass-Datenbank enthalten (*Anlage 4*). Die forensische Entschlüsselung des Containers bestätigte, dass dieser die in Anlage 2 beschriebenen Bilddateien enthielt,
5. dass sich auf dem Datenträger mit der Lfd.-Nr. 1 eine beschädigte JPEG-Datei befand, die nach Reparatur geöffnet werden konnte und eine Darstellung enthielt, die hinsichtlich des abgebildeten kindlichen Erscheinungsbilds und der Pose mit den in Anlage 2 dokumentierten Dateien vergleichbar ist,
6. dass der Container mit VeraCrypt verschlüsselt war und durch ein Passwort gesichert war, das durch Analyse einer auf dem System befindlichen KeePass-Datenbank ermittelt werden konnte (*Anlage 4*),
7. dass die betreffenden Bilddateien sich in einem Verzeichnis mit der Bezeichnung „/xxx/“ befanden, was auf eine gezielte Benennung oder Verschleierung hindeuten könnte,
8. dass das zur Entschlüsselung des Containers verwendete Passwort den Begriff „littleGirls“ enthielt. Dieser Begriff steht in engem thematischen Zusammenhang mit dem Inhalt des Containers. Die gewählte Bezeichnung könnte daher auf eine bewusste Themenwahl schließen lassen. Eine abschließende rechtliche Bewertung dieses Umstands erfolgt durch das Gericht,
9. dass in einem wiederhergestellten Logfragment (vermutlich aus /var/log/auth.log) ein einmaliger erfolgreicher SSH-Zugriff am 2. Juli 2025 um 22:57 Uhr dokumentiert ist,
   - mit dem Benutzerkonto pc über die lokale IP-Adresse 192.168.122.1,
   - mit einer Verbindungsdauer von unter zwei Minuten,
   - ohne Hinweise auf Internetzugriff oder externe Fremdeinwirkung (*Anlage 5*).

Darüber hinaus konnten keine Hinweise auf eine Verbreitung der sichergestellten Dateien festgestellt werden.

Weder Upload-Vorgänge noch versendete Anhänge oder Einbindungen in E-Mails oder andere Kommunikationskanäle waren nachweisbar.

Ebenso wurden keine gespeicherten E-Mails oder Chatverläufe aufgefunden. Hinweise auf elektronische Kommunikation mit Bezug zum Asservat lagen nicht vor.

Marwe Saai

Viktor Linner

Niclas Frey

4. Sicherung der Datenträger

Von dem Asservat werden forensische 1:1 Abbilder erstellt.

Diese sog. Images werden für die Untersuchung verwendet. Die schreibgeschützten Originaldatenträger werden nicht weiter herangezogen. Bei dem in Asservat 0.1 USB-Gerät handelt es sich um einen Datenträger.

Das gefertigte Abbild ist nach HASH-Abgleich identisch mit dem Originalasservat. Die Dokumentation der Sicherung ist in digitaler Form hinterlegt.

---

5. Betriebssystem, Benutzerkonten

5.1 Kerndaten zu dem Betriebssystem (OS)

Auf dem Asservat 0.1 ist Ubuntu-OS installiert:

Feld	**Wert**
Computer Name	pc-Standard-PC-Q35-ICH9-2009
Owner	*(leer)*
Version	Ubuntu 22.04 LTS
Time zone	Europe/Berlin
Installation	2022-07-01 14:30:12.123456789 +0000
Upgrade	2025-07-01 21:42:35.123456789 +0000
Last shutdown	2025-07-04 22:11:46.123456789 +0000

6. Methodik

Die nachfolgende Methodik beschreibt das übergreifende Vorgehen des Sachverständigenteams bei der Begutachtung. Sie umfasst die eingesetzten Werkzeuge, Sicherheitsvorkehrungen, forensischen Prinzipien sowie technische Maßnahmen zur Wahrung der Integrität und Nachvollziehbarkeit.

6.1 Arbeitsumgebung und Grundprinzipien

Die Auswertung erfolgte ausschließlich auf einer abgesicherten Linux-Umgebung (Kali Linux 2025.2). Der originale Datenträger wurde niemals schreibend eingebunden. Alle Arbeitsschritte wurden auf forensischen 1:1-Abbildern durchgeführt, deren Integrität über Prüfsummenverfahren sichergestellt wurde.

Die Verarbeitung erfolgte ausschließlich im Terminal bzw. mit minimalistischen Tools ohne Automatisierung. Sensible Operationen (z. B. Passwortextraktion, Dateiwiederherstellung, Containeröffnung) wurden manuell protokolliert. Die verwendete Umgebung war physisch vom Internet getrennt.

Forensische Grundprinzipien:

- Keine Änderungen am Originaldatenträger
- Arbeiten ausschließlich auf Kopien
- Lückenlose Hash-basierte Integritätsprüfung
- Nachvollziehbare und dokumentierte Befundpfade
- Verwendung gerichtlich anerkannter oder in der Praxis etablierter Tools

---

6.2 Versionierte Werkzeuge

Die nachfolgend aufgeführten Werkzeuge wurden zur Analyse verwendet. Alle wurden entweder aus offiziellen Paketquellen installiert oder über offizielle Quellen heruntergeladen. Die jeweilige Version zum Zeitpunkt der Untersuchung ist dokumentiert:

Tool	Version
qemu-nbd (qemu-utils)	9.2.92 (Debian 1:10.0.0~rc2+ds-2)
PhotoRec	7.2 (February 2024)
hashcat	v6.2.6
VeraCrypt	1.26.24
xxd	2024-12-07
wxHexEditor	0.24
sqlite3 (SQLite-Tools)	3.46.1
find (GNU findutils)	4.10.0
curl	8.12.1
KeePassXC	2.7.10
PowerShell	5.1.19041.6093

6.3 Verwendete Analysewerkzeuge und Einsatzkontext

Werkzeug	Zweck
qemu-nbd	Einbinden von QCOW2-Containern im Read-Only-Modus über /dev/nbdX
hashcat	Wiederherstellung von Benutzerpasswörtern aus /etc/shadow mittels Wörterbuchangriff
PhotoRec	Wiederherstellung gelöschter Dateien ohne Rückgriff auf Dateisystemstruktur
VeraCrypt	Öffnung verschlüsselter Container mit aus KeePassXC extrahierten Passwörtern
xxd + wxHexEditor	Untersuchung beschädigter Bilddateien und Korrektur fehlerhafter Magic Bytes
sqlite3	Manuelles Auslesen und Filtern der places.sqlite (Firefox History)
find	Lokalisierung relevanter Dateien und Browserdaten
KeePassXC	Öffnung und Sichtung verschlüsselter Passwort-Datenbank (Pass.kdbx)
curl	Download verifizierter Wortlisten für Passwortanalyse
PowerShell	Berechnung von Hashwerten und Dateiverwaltung unter Windows (siehe Abschnitt 7.1)

6.4 Integritätsprüfung und Hash-Strategie

Zur Gewährleistung der Datenintegrität wurde nach Erstellung des forensischen Abbilds ein **MD5-Hash** gebildet. Obwohl **MD5 kryptographisch als unsicher gilt**, ist es in der Praxis der digitalen Forensik weiterhin **üblich und ausreichend**, um die **Bitidentität von Arbeitskopien zu verifizieren**.

Vorgehen:

- Initialer Hash vor erster Nutzung (`Get-FileHash` , PowerShell)
- Kopie auf Arbeitsgerät
- Erneute Hashbildung nach Kopiervorgang
- Vergleich mit dem Ursprungshash

6.5 Reproduzierbarkeit

Alle durchgeführten Schritte wurden mittels standardisierter Befehle protokolliert. Es wurden keine kommerziellen, proprietären oder intransparenten Analyseumgebungen verwendet. Alle eingesetzten Tools sind **frei verfügbar** oder Bestandteil gängiger Linux-Distributionen.

Die Wiederholung der Arbeitsschritte mit denselben Werkzeugen unter den dokumentierten Bedingungen führt erwartungsgemäß zu denselben Ergebnissen.

6.6 Kommunikationsanalyse

Im Rahmen der forensischen Untersuchung wurde gezielt nach E-Mail-Archiven, Chatverläufen sowie Spuren aktiver Kommunikationssoftware (z. B. Thunderbird, Outlook, Webmail, WhatsApp, Signal, Skype, Telegram) gesucht. Hierzu wurden typische Konfigurationsverzeichnisse, lokale Speicherpfade und Browserverläufe systematisch überprüft. Auch .mbox-Archive, PST-Dateien und Anwendungscaches wurden berücksichtigt.
Die Überprüfung erfolgte durch manuelle Sichtung auffälliger Verzeichnisse.

7. Befund und Untersuchungsgang

7.1 Datensicherung

Am 02.07.2025 um 11:20 besuchten die Sachverständigen des Sachverständigenbüro "Finde die Wahrheit" Niclas Frey und Viktor Linner das Büro von Frau Oberstaatsanwältin Blitzgescheit zur Sicherung der zur Begutachtung relevanten Daten von allen betrefflichen Asservaten im Fall FLIEGNER. Das Asservat wurde als `img` -Datei auf einer `Toshiba v63700 – A 500GB` HDD-Festplatte bereitgestellt. Um sicherzustellen, dass die Daten auf dem Asservat nicht durch die Sachverständigen versehentlich oder absichtlich verändert werden können, wurde ein Write Blocker der Firma "**Logicube**" des Typs **WriteProtect USB wpu 201018 59°** genutzt, der es unmöglich machte, die Toshiba-Festplatte zu beschreiben.
Das für die begutachtung relevante Image wurde identifiert als Date `ForImage9.img` . Vor der Kopie des Images auf einen Datenträger der Sachverständigen wurde ein MD5-Hash des Images erstellt, um nach dem Kopiervorgang feststellen zu können, dass die Kopie identisch zum Original ist.

PowerShell

```
PS D:\> dir
    Verzeichnis: D:\
Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
-a----         01.07.2025     22:12    12748128256 ForImage9.img

PS D:\> Get-FileHash .\ForImage9.img -Algorithm MD5
Algorithm       Hash                                                                   Path
---------       ----                                                                   ----
MD5             9C9570F6F648BA1D0FF14F8CD6AACF39
D:\ForImage9.img
```

Danach wurde das Image kopiert, und von der Kopie wurde ein MD5-Hash erstellt.

PowerShell

```
PS D:\> Copy-Item .\ForImage9.img C:\Users\Vik\Desktop\ForImage9.img
PS D:\> Get-FileHash 'C:\Users\Vik\Desktop\ForImage9.img' -Algorithm MD5

Algorithm       Hash                                                                   Path
---------       ----                                                                   ----
MD5             9C9570F6F648BA1D0FF14F8CD6AACF39
C:\Users\Vik\Desktop\ForImage...
```

7.2 Zugriff auf das Image

Um auf das Image zugreifen zu können, nutzten die Sachverständigen `quemu-utils` :

Bash

```
sudo apt install qemu-utils
sudo modprobe nbd max_part=8
sudo qemu-nbd --connect=/dev/nbd0 ForImage9.img --read-only
lsblk /dev/nbd0
```

7.3 Passwort-Extraktion

Die Sachverständigen extrahierten zunächst die Passwörter aller Nutzer aus der Datei `/etc/shadow` :

Shell

```
sudo cat ./etc/shadow

pc:$y$j9T$graH6StsN64vZy4TX6DLO1$jFAPKwPTtCP25YeK6fiAIcbse.xZb3XaFXnIuwfaej4:19175:0:99999:7:::
niels:$6$mysalt$XV5j4lT9Ut5S96EU11gyef6DVRi4GjOk7QCVMXDiGDkw.OvBPQcvRqgjiadq22fLuTMwT92GhAvMMg074LO7w.:19177:0:99999:7:::
barney:$6$mysalt$9SMwo3IGWSIppwbVACGblzrNYJtxG8pjChCdVKmiFCoGm075DAiKAIDooGtETCV5vruzdJeqwb3nYIjw7KtUv0:19177:0:99999:7:::
```

Die Hashes wurden in folgendem Format in einer Datei `passwd.txt` abgelegt:

Plain text

```
pc:$y$j9T$graH6StsN64vZy4TX6DLO1$jFAPKwPTtCP25YeK6fiAIcbse.xZb3XaFXnIuwfaej4
niels:$6$mysalt$XV5j4lT9Ut5S96EU11gyef6DVRi4GjOk7QCVMXDiGDkw.OvBPQcvRqgjiadq22fLuTMwT92GhAvMMg074LO7w
barney:$6$mysalt$9SMwo3IGWSIppwbVACGblzrNYJtxG8pjChCdVKmiFCoGm075DAiKAIDooGtETCV5vruzdJeqwb3nYIjw7KtUv0
```

Das Format dient dazu, die Passwörter nach dem Cracken der jeweiligen Nutzer*in zuordnen zukönnen.

Danach wurde begonnen, die Passwörter mittels Wörterbuchangriff zu cracken.

Shell

```
curl -b "MoodleSessionmoodlehsma=016e963ec86fc2134833450bbebb24e0" https://moodle.hs-mannheim.de/pluginfile.php/479555/mod_resource/content/1/wordlist.txt -L > wordlist.txt

hashcat --user passwd.txt wordlist.txt
```

Nach circa zwei Stunden konnten zwei der drei Passwörter wiederhergestellt werden:

Plain text

```
niels:xaiCh7fi
barney:ahM4Hood
```

Das Passwort des Nutzers `pc` konnte nach ausgiebigen Versuchen vom Sachverständigenbüro nicht wiederhergestellt werden. Allerdings ist auch anzumerken, dass bis auf eine passwortgeschützte KeePass-Datei keine weitere Stelle im Asservat gefunden wurde, bei der die Verwendung eines Passworts notwendig gewesen wäre.

7.4 Browser-History

Der Kommandozeilenbefehl `find` wurde genutzt, um Browser-Histories des Browsers "Firefox" ausfindig zu machen:

Shell

```
find . -type f -name "places.sqlite"


./barney/snap/firefox/common/.mozilla/firefox/sn0kzhia.default/places.sqlite
./pc/snap/firefox/common/.mozilla/firefox/hsn68zcj.default/places.sqlite
```

In Folge dessen wurden alle Einträge der Datenbank nach Inhalten durchsucht. Die Tabelle `moz_places` enthielt die zuletzt besuchten Seiten des users `barney`:
Auszug aus der Tabelle moz_places:

SQL

```sql
SELECT * FROM moz_places

1|https://www.mozilla.org/privacy/firefox/||gro.allizom.www.|1|1|0|24|1656953208163056|A5SqOlBd6fKM|0|47356411089529||||1
2|https://www.mozilla.org/de/privacy/firefox/|Firefox Datenschutzhinweis — Mozilla|gro.allizom.www.|1|0|0|98|1656953208364479|FfSBQlDTyqsO|0|47360031482596|
  Our Privacy Notices describe the data our products and services receive, share, and use, as well as choices available to you.
|https://www.mozilla.org/media/img/mozorg/mozilla-256.4720741d4108.jpg||1
3|https://support.mozilla.org/products/firefox||gro.allizom.troppus.|0|0|0|137||yJd1VIvOpI_p|1|47358327123126||||2
[...]
```

Die vollständige Browser-History ist in Anlage 1 enthalten.

Die neunte Spalte enhält Zahlen im Format `1656953208163056` (Beispiel aus der ersten Zeile der Ausgabe). Dies sind sogenannte 'Unix-Timestamps' - Zeitstempel in einem bestimmten Format. Diese Zeitstempel erlaubten es den Sachverständigen, die Browserdaten zeitlich einzuordnen.

7.5 Kürzlich genutzte Dateien

Die Datei `/home/barney/.local/share/recently-used.xbel` gibt Auskunft über kürzlich genutzte Dateien des Users `barney`:

Auszug aus /home/barney/.local/sharerecently-used.xbel:

XML

```xml
<?xml version="1.0" encoding="UTF-8"?>
<xbel version="1.0"
      xmlns:bookmark="http://www.freedesktop.org/standards/desktop-bookmarks"
      xmlns:mime="http://www.freedesktop.org/standards/shared-mime-info"
>
  <bookmark href="file:///media/barney/067E7AF632AA2E11/Bilder" added="2022-07-04T16:30:33.590042Z" modified="2022-07-04T16:30:33.590048Z" visited="2022-07-04T16:30:33.590043Z">
    <info>
      <metadata owner="http://freedesktop.org">
        <mime:mime-type type="inode/directory"/>
        <bookmark:applications>
          <bookmark:application name="org.gnome.Nautilus" exec="&amp;apos;org.gnome.Nautilus %u&amp;apos;" modified="2022-07-04T16:30:33.590045Z" count="1"/>
        </bookmark:applications>
      </metadata>
    </info>
```

```
    </bookmark>
    <bookmark href="file:///media/barney/067E7AF632AA2E11/xxx" added="2022-07-04T16:34:14.977136Z" modified="2022-07-04T20:11:09.132408Z" visited="2022-07-04T16:34:14.977137Z">
      <info>
        <metadata owner="http://freedesktop.org">
          <mime:mime-type type="application/octet-stream"/>
          <bookmark:applications>
            <bookmark:application name="veracrypt" exec="&amp;apos;veracrypt %u&amp;apos;" modified="2022-07-04T20:11:09.132405Z" count="3"/>
          </bookmark:applications>
        </metadata>
      </info>
    </bookmark>
    <bookmark href="file:///home/barney/Pass.kdbx" added="2022-07-04T20:10:16.757839Z" modified="2022-07-04T20:10:16.757851Z" visited="2022-07-04T20:10:16.757841Z">
      <info>
        <metadata owner="http://freedesktop.org">
          <mime:mime-type type="application/x-keepass2"/>
          <bookmark:applications>
            <bookmark:application name="keepassxc" exec="&amp;apos;keepassxc %u&amp;apos;" modified="2022-07-04T20:10:16.757845Z" count="1"/>
          </bookmark:applications>
        </metadata>
      </info>
    </bookmark>
[...]
```

Für die Begutachtung waren hierbei folgende Erkenntnisse zu gewinnen:

1. Die Datei `/media/barney/067E7AF632AA2E11/xxx`, deren Dateityp vorher nicht näher zu bestimmen war, wurde mit `veracrypt` bedient. Veracrypt ist ein Programm, welches zur Ver- oder Entschlüsselung von Dateien, Verzeichnissen oder ganzer Dateisysteme die
2. Nach Zugriff auf die Veracrypt-Datei wurde auf `/home/barney/Pass.kdbx` zugegriffen. Es stellte sich später heraus (siehe Abschnitt Keepass-Datenbank), dass diese Datei eine KeePass-Datenbank ist. Die Zeitliche Abfolge der Zugriffe auf diese beiden Dateien legte nahe, dass das Passwort, was zur Entschlüsselung der Veracrypt-Datei benötigt ist, in der KeePass-Datenbank hinterlegt ist.

7.6 Keepass-Datenbank

Im Home-Verzeichnis des Nutzers barney wurde eine passwortgeschützte KeePass-Datenbank mit dem Namen Pass.kdbx gefunden:

Shell

```
ls
Bilder  Dokumente  Downloads  Musik  Öffentlich  Pass.kdbx  Schreibtisch  snap  Videos
Vorlagen
```

Die Datei ließ sich mit dem zuvor durch Brute-Force-Verfahren wiederhergestellten Passwort `ahM4Hood` erfolgreich öffnen.

Die geöffnete Datenbank enthielt lediglich einen einzigen Eintrag im Stammverzeichnis („Root“). Der Titel dieses Eintrags lautete **„VeraCrypt“**. Als zugehöriges Passwort war der Begriff **„littleGirls“** gespeichert.

7.7 Veracrypt-verschlüsselte Datei

Die Datei `/media/barney/067E7AF632AA2E11/xxx` konnte mit dem aus der KeePass-Datenbank gewonnenen Passwort entschlüsselt und forensisch untersucht werden:

Shell

```
sudo mkdir /mnt/veracrypt && sudo veracrypt --text --mount xxx /mnt/veracrypt
```

7.8 Korrpute Bilddatei

Die Bilddatei `Bilder/c1.jpg` wurde auf Dateikorruption untersucht, da sie die Endung einer Bilddatei besitzt, sich aber nicht als Bild öffnen ließ.
Um festzustellen, ob es sich wirklich um eine Bilddatei handelt, oder ob die Dateiendung womöglich nichts mit dem Inhalt der Datei zu tun hat (was auf Unix-Systemen durchaus sein kann), nutzten die Sachverständigen das Programm `xxd` :

Shell

```
xxd c1.jpeg | head -n 20
00000000: ddd8 ffe0 0010 4a46 4946 0001 0100 0001  ......JFIF......
00000010: 0001 0000 ffdb 0084 0009 0607 1210 1215  ................
00000020: 0f10 1216 1015 0f10 1010 0f15 1015 150f  ................
00000030: 1510 1015 1516 1615 1515 1518 1d28 2018  .............( .
```

Die ersten Bytes der Datei ähneln den bei einer jpeg-Datei erwarteten ersten Bytes `FF D8 FF E0 00` .
Um herauszufinden, ob die Datei sich bei Änderung der Bytes in die oben genannte Bytefolge als Bilddatei öffnen lässt, veränderten die Sachverständigen die Magic Bytes der Datei mit dem Hexeditor `wxhexeditor` .
Tatsächlich ließ sich nach der Änderung die Datei als Bild öffnen.

7.9 Untersuchung auf gelöschte Dateien

Das tool `photorec` wurde genutzt, um alle auf dem Image vorhandenen gelöschten Dateien wiederherzustellen:

Shell

```
photorec /home/sf_kali_share/ForImage9
```

Dabei konnte eine große Anzahl von Bilddateien wiederhergestellt werden, bei denen der Verdacht besteht, dass sie Darstellungen von teilweise unbekleideten Personen in sexualisiertem Kontext enthalten.

Eine abschließende rechtliche Bewertung dieser Inhalte ist dem Gericht vorbehalten.

Aufgrund der großen Datenmenge ist in Anlage 3 ein exemplarischer Screenshot beigefügt. Die vollständigen Inhalte wurden auf einem separaten Datenträger gesichert, der dem Gericht auf Anfrage zur Verfügung gestellt werden kann.

7.10 Kommunikation

Es wurden keine Hinweise auf gespeicherte E-Mails, lokale Chatverläufe oder sonstige elektronische Kommunikation gefunden.
Insbesondere ließen sich weder E-Mail-Clients noch Messaging-Anwendungen identifizieren, die relevante Inhalte gespeichert hätten.
Auch Browserverläufe enthielten keine Spuren von Webmail-Diensten oder Kommunikationsplattformen, die auf eine Nutzung hindeuten würden.

7.11 SSH-Zugriffsprotokolle (rekonstruiert)

Im Rahmen der Untersuchung konnten mit **PhotoRec** Logfragmente wiederhergestellt werden, die auf **eine einzelne SSH-Verbindung** hindeuten. Die betreffenden Dateien waren im aktiven Dateisystem nicht mehr vorhanden und keinem festen Pfad zuzuordnen.

Die rekonstruierten Einträge belegen **einen erfolgreichen SSH-Zugriff** am **2. Juli 2025 um 22:57 Uhr** mit dem Benutzer pc von der IP-Adresse 192.168.122.1. Die Sitzung dauerte **unter zwei Minuten**.

Die verwendete IP-Adresse gehört zum **lokalen Netzwerkbereich** und deutet auf eine virtuelle Umgebung hin. **Ein internetbasierter Fernzugriff ist nicht erkennbar.**

Weitere Logeinträge (siehe Anlage 5) zeigen, dass der SSH-Dienst bereits am **1. Juli 2025** aktiv war.

Eine detaillierte Auswertung der durchgeführten Aktivitäten ist nicht möglich. Es liegen **keine Shell-Historien oder weiteren Protokolle** vor.

Bewertung:
Die Sitzung weist **keine Anzeichen externer Fremdeinwirkung** auf. Es handelt sich um einen lokal begrenzten Zugriff innerhalb des internen Netzwerks.

8. Einschränkungen und offene Punkte

- **Passwort `pc:$y$j9T...` konnte trotz längerer Analyse nicht wiederhergestellt werden.**
- **Inhalte des gelöschten Bereichs (Photorec-Recovery) konnten nicht vollständig manuell überprüft werden**, da die Anzahl der rekonstruierten Dateien sehr groß war. Die Auswahl repräsentativer Beispiele erfolgte nach Dateigröße.

9. Anlagen

Anlage 1: Vollständige Browser-History des users `barney`

Plain text

```
1|https://www.mozilla.org/privacy/firefox/||gro.allizom.www.|1|1|0|24|1656953208163056|A5SqOlBd6fKM|0|47356411089529||||1
2|https://www.mozilla.org/de/privacy/firefox/|Firefox Datenschutzhinweis — Mozilla|gro.allizom.www.|1|0|0|98|1656953208364479|FfSBQlDTyqsO|0|47360031482596|
  Our Privacy Notices describe the data our products and services receive, share, and use, as well as choices available to you.
|https://www.mozilla.org/media/img/mozorg/mozilla-256.4720741d4108.jpg||1
3|https://support.mozilla.org/products/firefox||gro.allizom.troppus.|0|0|0|137||yJd1VIvOpI_p|1|47358327123126||||2
4|https://support.mozilla.org/kb/customize-firefox-controls-buttons-and-toolbars?utm_source=firefox-browser&utm_medium=default-bookmarks&utm_campaign=customize||gro.allizom.troppus.|0|0|0|137||fzS0A1vSmaCS|1|47359956450016||||2
5|https://www.mozilla.org/contribute/||gro.allizom.www.|0|0|0|137||ZUp2Xs0my0fc|1|47357364218428||||1
6|https://www.mozilla.org/about/||gro.allizom.www.|0|0|0|137||PxGc7HWdpK3u|1|47357608426557||||1
7|https://www.mozilla.org/firefox/central/||gro.allizom.www.|0|0|0|137||SmvTP_gRfA1X|1|47359969280417||||1
8|https://www.google.com/search?channel=fs&client=ubuntu&q=hot+chearleader|hot chearleader - Google Suche|moc.elgoog.www.|1|0|1|1950|1656953228105571|5k6iUfwoYDt_|0|47359856985002||||3
10|https://www.google.com/search?q=hot+cheerleader+pics&client=ubuntu&hs=Urn&channel=fs&source=lnms&tbm=isch&sa=X&ved=2ahUKEwjpo6Tq19_4AhUz57sIHUuNAVoQ_AUoAXoECAEQAw&biw=950&bih=656&dpr=1|hot cheerleader pics — Google Suche|moc.elgoog.www.|1|0|0|98|1656953247155094|WjfpN6MdgTYb|0|47357695506675||||3
11|https://www.google.com/|Google|moc.elgoog.www.|1|0|1|2000|1751399635782628|VO9fMBiQ_Qe3|0|47357433249528||||3
12|https://www.google.com/search?q=sexy+girls+chearleeder&sca_esv=b5d146501cb8d5e6&source=hp&ei=0zxkaKD3KtqUxc8Pldb3oA8&iflsig=AOw8s4IAAAAAaGRK4zXwm-QSv50hRxjl8e7RuEd90d6H&ved=0ahUKEwjgrJWJuJyOAxVaSvEDHRXrHfQQ4dUDCA4&uact=5&oq=sexy+girls+chearleeder&gs_lp=Egdnd3Mtd2l6IhZzZXh5IGdpcmxzIGNoZWFybGVlZGVySOFEUK8GWIdCcAF4AJABAJgBW6ABkg2qAQIyMrgBA8gBAPgBAZgCBKACiwOoAgrCAgoQABgDGOoCGI8BwgIKEC4YAxjqAhiPAcICBBAAGAPCAgsQABiABBixAxiDAcICERAuGIAEGLEDGNEDGIMBGMcBwgIOEC4YgAQYsQMY0QMYxwHCAhQQLhiABBixAxjRAxiDARjHARiKBcICERAuGIAEGLEDGIMBGNQCGIoFwgIOEAAYgAQYsQMYgwEYigXCAgsQLhiABBjRAxjHAcICBRAAGIAEwgIFEC4YgATCAggQABiABBixA8ICCBAuGIAEGLEDwgILEC4YgAQYsQMY1AKYA0vxBS4Z00fBhgVBkgcDMy4xoAf6OrIHAzIuMbgHwALCBwczLTEuMi4xyAeJAQ&sclient=gws-wiz|Google Search|moc.elgoog.www.|1|0|0|100|1751399650395128|VwD1rGOId0VP|0|47358104091540||||3
13|https://www.google.com/search?q=sexy+girls+chearleeder&sca_esv=b5d146501cb8d5e6&source=hp&ei=0zxkaKD3KtqUxc8Pldb3oA8&iflsig=AOw8s4IAAAAAaGRK4zXwm-QSv50hRxjl8e7RuEd90d6H&ved=0ahUKEwjgrJWJuJyOAxVaSvEDHRXrHfQQ4dUDCA4&uact=5&oq=sexy+girls+chearleeder&gs_lp=Egdnd3Mtd2l6IhZzZXh5IGdpcmxzIGNoZWFybGVlZGVySOFEUK8GWIdCcAF4AJABAJgBW6ABkg2qAQIyMrgBA8gBAPgBAZgCBKACiwOoAgrCAgoQABgDGOoCGI8BwgIKEC4YAxjqAhiPAcICBBAAGAPCAgsQABiABBixAxiDAcICERAuGIAEGLEDGNEDGIMBGMcBwgIOEC4YgAQYsQMY0QMYxwHCAhQQLhiABBixAxjRAxiDARjHARiKBcICERAuGIAEGLEDGNEDGIMBGMcBwgIOEAAYgAQYsQMYgwEYigXCAgsQLhiABBjRAxjHAcICBRAAGIAEwgIFEC4YgATCAggQABiABBixA8ICCBAuGIAEGLEDwgILEC4YgAQYsQMY1AKYA0vxBS4Z00fBhgVBkgcDMy4xoAf6OrIHAzIuMbgHwALCBwczLTE
```

```
uMi4xyAeJAQ&sclient=gws-wiz&sei=4jxkaILdFq3Xxc8PkYvV0Q0|sexy girls chearleeder - Google Suche|moc.elgoog.www.|1|0|0|100|1751399650869426|oD-XfeUoeZN9|0|47357505484614||||3
14|https://www.google.com/search?sca_esv=b5d146501cb8d5e6&q=sexy+girls+cheerleader&udm=2&fbs=AIIjpHw2KGh6wpocn18KLjPMw8n5Yp8-1M0n6BD6JoVBP_K3fXXvA3S3XGyupmJLMg20um-mJAeO36stiqcDeSp1syInrodDcdKxMuB2TiCVf45CLzCoNRKRBZlvU8DUj0lI7KC-ZRxX-gxikqc1yM1oJcoJGNUwir8qlkx4kLIK4GELCJ58DYXpqPW_aK1GFeloqICCzjL7&sa=X&ved=2ahUKEwjkhrGQuJyOAxVsSfEDHWfWK1sQtKgLKAF6BAgTEAE&biw=950&bih=656&dpr=1|sexy girls cheerleader - Google Suche|moc.elgoog.www.|2|0|0|200|1751399794152616|84PG8mjR9eFS|0|47359998535018||||3
15|https://www.google.com/search?sca_esv=b5d146501cb8d5e6&q=sexy+girls+cheerleader&udm=2&fbs=AIIjpHw2KGh6wpocn18KLjPMw8n5Yp8-1M0n6BD6JoVBP_K3fXXvA3S3XGyupmJLMg20um-mJAeO36stiqcDeSp1syInrodDcdKxMuB2TiCVf45CLzCoNRKRBZlvU8DUj0lI7KC-ZRxX-gxikqc1yM1oJcoJGNUwir8qlkx4kLIK4GELCJ58DYXpqPW_aK1GFeloqICCzjL7&sa=X&ved=2ahUKEwjkhrGQuJyOAxVsSfEDHWfWK1sQtKgLKAF6BAgTEAE&biw=950&bih=656&dpr=1#vhid=cxWEukMoNf2AeM&vssid=mosaic|sexy girls cheerleader - Google Suche|moc.elgoog.www.|1|0|0|100|1751399681729745|oKM9ukKGCqYk|0|47359365193005||||3
16|https://www.google.com/search?sca_esv=b5d146501cb8d5e6&q=sexy+girls+cheerleader&udm=2&fbs=AIIjpHw2KGh6wpocn18KLjPMw8n5Yp8-1M0n6BD6JoVBP_K3fXXvA3S3XGyupmJLMg20um-mJAeO36stiqcDeSp1syInrodDcdKxMuB2TiCVf45CLzCoNRKRBZlvU8DUj0lI7KC-ZRxX-gxikqc1yM1oJcoJGNUwir8qlkx4kLIK4GELCJ58DYXpqPW_aK1GFeloqICCzjL7&sa=X&ved=2ahUKEwjkhrGQuJyOAxVsSfEDHWfWK1sQtKgLKAF6BAgTEAE&biw=950&bih=656&dpr=1#vhid=PdmE7HJ-gy1JZM&vssid=mosaic|sexy girls cheerleader - Google Suche|moc.elgoog.www.|1|0|0|100|1751399736003286|mvushxzbfYqP|0|47357381351553||||3
18|https://www.google.com/url?sa=i&url=https%3A%2F%2Fwww.shutterstock.com%2Fde%2Fsearch%2Fhot-cheerleader&psig=AOvVaw1jVI9MPGMcs8DtCnFhnflL&ust=1751486058108000&source=images&cd=vfe&opi=89978449&ved=0CBQQjRxqFwoTCNjdlZ-4nI4DFQAAAAAdAAAAABAS||moc.elgoog.www.|1|1|0|25|1751399857179623|-VXBlm6v3hA9|0|47358059237094||||3
```

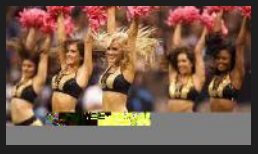
Anlage 2: Inhalt des verschlüsselten Veracrypt-Image

Nach Entschlüsselung des Containers `/media/barney/067E7AF632AA2E11/xxx` konnten folgende Bilddateien forensisch gesichert werden:

Datei	Größe	Auflösung	Datum	Beschreibung
c2.jpeg `/xxx/c2.jpeg`	7.8 KiB (7 979 Bytes)	299 × 169 px	04.07.2022	Einzelne Football-Cheerleaderin in weißem Outfit, lachend inmitten eines Stadions, offenbar beim Tanzmove.
c3.jpeg `/xxx/c3.jpeg`	6.5 KiB (6 610 Bytes)	300 × 168 px	04.07.2022	Cheerleaderinnen in weiß-blauem Uniform-Set, stehend in Studio-Pose vor weißem Hintergrund.
c4.jpeg `/xxx/c4.jpeg`	10.4 KiB (10 694 Bytes)	300 × 168 px	04.07.2022	Mehrere Cheerleaderinnen in schwarzem Top mit pinken Pom-Poms, synchron aufgereiht bei Auftritt im Freien.

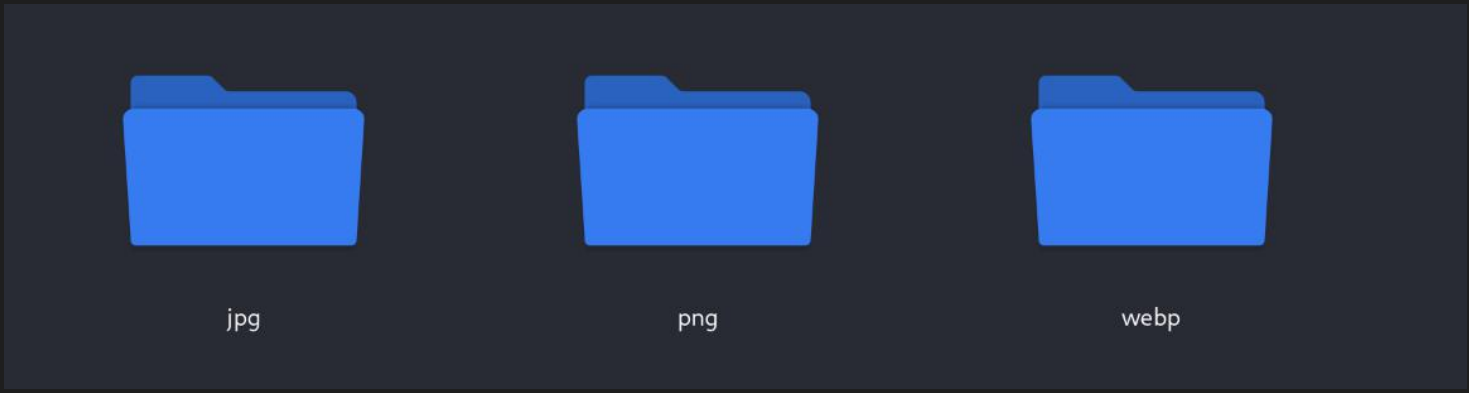
c2.jpeg

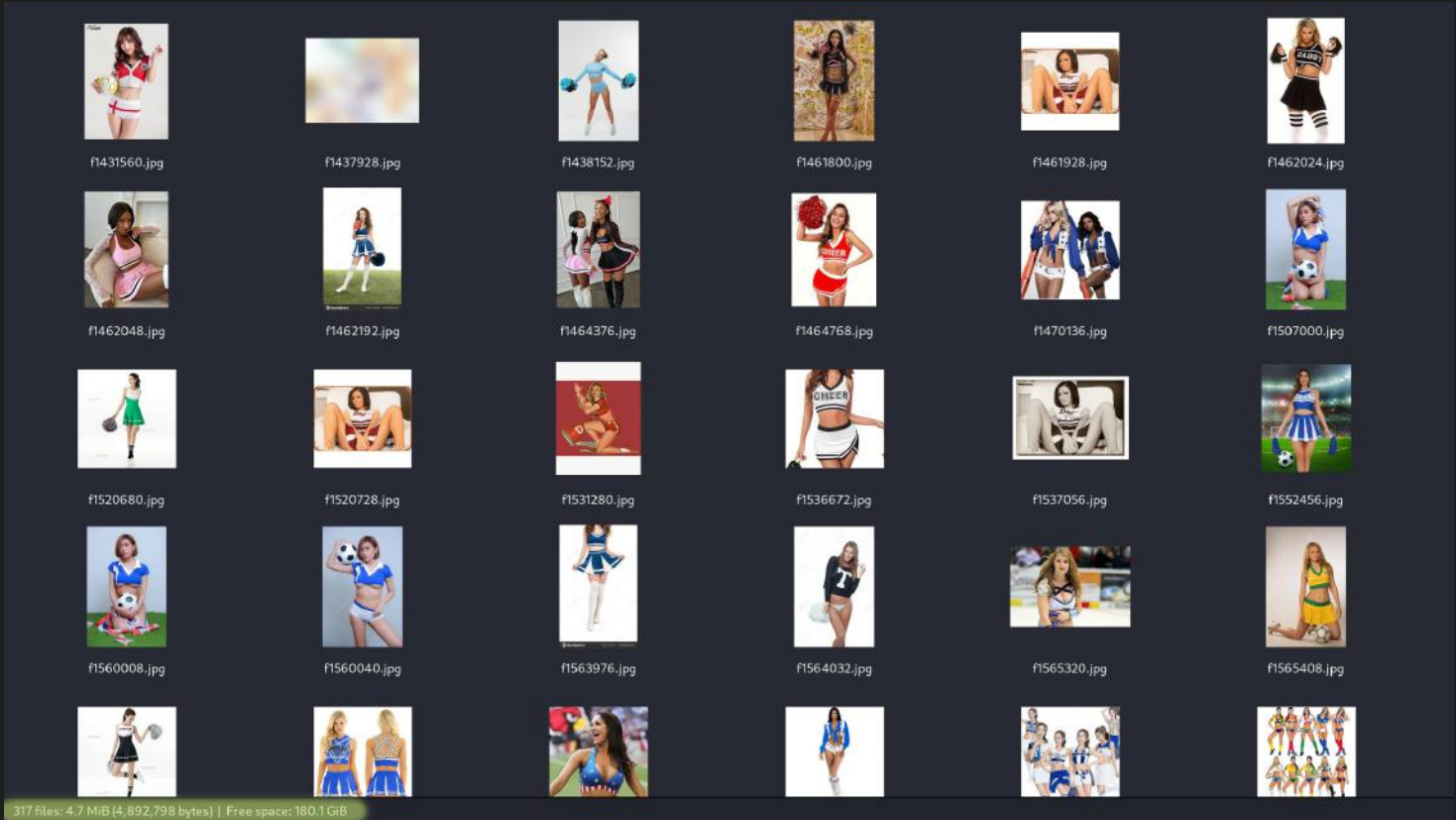
c3.jpeg



c4.jpeg

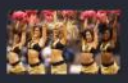
Anlage 3: Gelöschtes Bildmaterial





f13548312.png

f13548408.png



f13946368.png

f13947392.png

f13948672.png

f19438328.png

f29890880.png

f29896824.png

8 files: 3.8 MiB (3,987,778 bytes) | Free space: 180.1 GiB

f1569440.webp

f4272024.webp

f4272104.webp

f4272144.webp

f4276640.webp

f10094248.webp

f10094296.webp

f10214664.webp

f10247384.webp

f10253408.webp

f10260168.webp

f10641464.webp

f10641592.webp

f11451568.webp

f11513232.webp

f11513488.webp

f11547320.webp

f11568256.webp

f11568344.webp

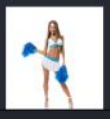
f12671464.webp

f12671568.webp

f12671800.webp

f14431808.webp

f14438336.webp



95 files: 1.2 MiB (1,274,930 bytes) | Free space: 180.1 GiB

Anlage 4: Datei `/home/barney/.local/share/recently-used.xbel`

XML

```xml
<?xml version="1.0" encoding="UTF-8"?>
<xbel version="1.0"
      xmlns:bookmark="http://www.freedesktop.org/standards/desktop-bookmarks"
      xmlns:mime="http://www.freedesktop.org/standards/shared-mime-info"
>
  <bookmark href="file:///media/barney/067E7AF632AA2E11/Bilder" added="2022-07-04T16:30:33.590042Z" modified="2022-07-04T16:30:33.590048Z" visited="2022-07-04T16:30:33.590043Z">
    <info>
      <metadata owner="http://freedesktop.org">
        <mime:mime-type type="inode/directory"/>
        <bookmark:applications>
          <bookmark:application name="org.gnome.Nautilus" exec="&amp;apos;org.gnome.Nautilus %u&amp;apos;" modified="2022-07-04T16:30:33.590045Z" count="1"/>
        </bookmark:applications>
      </metadata>
    </info>
  </bookmark>
  <bookmark href="file:///media/barney/067E7AF632AA2E11/xxx" added="2022-07-04T16:34:14.977136Z" modified="2022-07-04T20:11:09.132408Z" visited="2022-07-04T16:34:14.977137Z">
    <info>
      <metadata owner="http://freedesktop.org">
        <mime:mime-type type="application/octet-stream"/>
        <bookmark:applications>
          <bookmark:application name="veracrypt" exec="&amp;apos;veracrypt %u&amp;apos;" modified="2022-07-04T20:11:09.132405Z" count="3"/>
        </bookmark:applications>
      </metadata>
    </info>
  </bookmark>
  <bookmark href="file:///home/barney/Pass.kdbx" added="2022-07-04T20:10:16.757839Z" modified="2022-07-04T20:10:16.757851Z" visited="2022-07-04T20:10:16.757841Z">
    <info>
      <metadata owner="http://freedesktop.org">
        <mime:mime-type type="application/x-keepass2"/>
        <bookmark:applications>
          <bookmark:application name="keepassxc" exec="&amp;apos;keepassxc %u&amp;apos;" modified="2022-07-04T20:10:16.757845Z" count="1"/>
        </bookmark:applications>
      </metadata>
    </info>
  </bookmark>
  <bookmark href="file:///home/barney/Dokumente/Annual_Report.odp" added="2025-07-01T20:06:39.710911Z" modified="2025-07-01T20:06:39.710943Z" visited="2025-07-01T20:06:39.710925Z">
    <info>
      <metadata owner="http://freedesktop.org">
        <mime:mime-type type="application/vnd.oasis.opendocument.presentation"/>
        <bookmark:applications>
```

```
41            <bookmark:application name="org.gnome.Nautilus" exec="&apos;libreoffice --impress %U&apos;" modified="2025-07-01T20:06:39.710930Z" count="1"/>
42          </bookmark:applications>
43        </metadata>
44      </info>
45    </bookmark>
46    <bookmark href="file:///home/barney/Dokumente/Annual_Report_Entwurf.pptx" added="2025-07-01T20:10:06.623166Z" modified="2025-07-01T20:10:06.623196Z" visited="2025-07-01T20:10:06.623168Z">
47      <info>
48        <metadata owner="http://freedesktop.org">
49          <mime:mime-type type="application/vnd.openxmlformats-officedocument.presentationml.presentation"/>
50          <bookmark:applications>
51            <bookmark:application name="org.gnome.Nautilus" exec="&apos;libreoffice --impress %U&apos;" modified="2025-07-01T20:10:06.623178Z" count="1"/>
52          </bookmark:applications>
53        </metadata>
54      </info>
55    </bookmark>
56  </xbel>
```

Anlage 5: Wiederhergestellte SSH-Logeinträge

Log file

```
1  Jul  2 22:57:01 pc sshd[2190]: Accepted password for pc from 192.168.122.1 port 44720 ssh2
2  Jul  2 22:57:01 pc sshd[2190]: pam_unix(sshd:session): session opened for user pc(uid=1000) by (uid=0)
3  Jul  2 22:58:56 pc sshd[2248]: Received disconnect from 192.168.122.1 port 44720:11: disconnected by user
4  Jul  2 22:58:56 pc sshd[2248]: Disconnected from user pc 192.168.122.1 port 44720
5  Jul  2 22:58:56 pc sshd[2190]: pam_unix(sshd:session): session closed for user pc
```

Log file

```
1  Jul  1 21:41:48 pc sshd[619]: Server listening on 0.0.0.0 port 22.
2  Jul  1 21:41:48 pc sshd[619]: Server listening on :: port 22.
3  [...]
4  Jul  4 14:11:32 pc sshd[667]: Server listening on 0.0.0.0 port 22.
5  Jul  4 14:11:32 pc sshd[667]: Server listening on :: port 22.
```

10. Anhang

Anhang I: Grundsätzliche Vorgehensweisen

I.I. Behandlung der Asservate

I.I.1 Generelle Anmerkungen

Die Auswertung von Datenträgern erfolgt nach forensischen Gesichtspunkten und auf dem aktuellen Stand der Technik. An Hard- und Softwareprodukten werden von Ermittlungs-, Finanz- und Steuerbehörden weltweit genutzte und gerichtlich anerkannte Produkte unter Windows und LINUX eingesetzt.
Die forensische Auswertung von Datenträgern geschieht unter hohen Sicherheitsvorkehrungen ausschließlich durch forensisch geschultes Personal in abgesicherten und beaufsichtigten Räumen.
Auf veränderbare Originaldatenträger wird (soweit technisch möglich) nur mittels Spezialhardware zugegriffen, die ein Beschreiben der Originaldatenträger verhindern.
Die Auswertung geschieht mittels spezieller Software. Dabei werden – falls das durch den Auftraggeber aus Kostengründen nicht ausdrücklich ungewünscht ist – auch alle Formen von gelöschten und teilweise überschriebenen Daten sowie spezielle, mit üblichen Mitteln nicht zugängliche oder versteckte Dateien/Bereiche berücksichtigt.

I.I.2 Hardware-Write-Blocker

Für den Zugriff auf Beweisdatenträger, welche nicht auf Grund Ihrer Art selbst schreibgeschützt sind, wurden sogenannte Hardware-Write-Blocker verwendet, die durch Ihren speziellen elektronischen Aufbau den schreibenden Zugriff auf den Datenträger in jedem Fall verhindern und somit die Integrität der gesicherten Daten gewährleisten.
Hierzu fand ein Gerät der Firma "**Logicube**" des Typs **WriteProtect USB wpu 201018 59°** Verwendung.
Eine Veränderung des Original-Datenbestandes des Beweisdatenträgers durch Schreibzugriffe ist so mit ausgeschlossen.

Anhang II: Wichtige Lesehinweise zum Gutachten

Inhalt: Es werden nicht alle negativen Untersuchungen dokumentiert
Juristische Begriffe: Falls ein juristischer Begriff Verwendung findet, geschieht das ungewollt und in der umgangssprachlichen Bedeutung. Eine juristische Bewertung obliegt der Staatsanwaltschaft und dem hohen Gericht

Anhang III: Glossar

Nutzer : Der „Nutzer“ ist eine Person, die ein Gerät bedient und Daten von Speichermedien gelesen bzw. darauf geschrieben hat. Es muss sich nicht bei jeder Verwendung des Begriffs um ein und dieselbe Person handeln. Ob es sich beim Nutzer um die Beschuldigten handelt, ist aus technischer Sicht meist nicht eindeutig zu beantworten. Hinweise, die deutlich dafür oder dagegen sprechen, werden angeführt. Im Zusammenhang mit E-Mail-Empfänger- und Absender-Adressen wurden im Gutachten die zur jeweiligen Adresse gespeicherten Namen in der Dokumentation verwendet.

Browser-History: Unter dem Begriff „Browser-History“ werden die von Webbrowsern gespeicherten Nutzungsdaten verstanden. Diese beinhalten besuchte Webseiten, durchgeführte Suchanfragen sowie Zeitstempel. Je nach eingesetztem Browser und Konfiguration können auch Details wie Verweildauer oder Downloadaktionen erfasst sein.

Datenträger: Als Datenträger gelten alle elektronischen Medien, die zur Speicherung digitaler Inhalte geeignet sind. Dazu zählen unter anderem Festplatten (HDD/SSD), USB-Sticks, Speicherkarten oder optische Medien (CD/DVD). In diesem Gutachten wird der Begriff technisch und neutral verwendet.

Image: Ein Image bezeichnet eine bitweise Kopie eines Datenträgers oder eines Partitionsteils. Es handelt sich dabei um ein exaktes Abbild inklusive aller Sektoren, gelöschter Dateien, freier Bereiche sowie versteckter Partitionen.

Verschlüsselung: Datenverschlüsselung ist ein technisches Verfahren, bei dem Informationen mithilfe eines Schlüssels in eine unlesbare Form überführt werden.

Cracken von Passwörtern: Das „Cracken“ von Passwörtern bezeichnet technische Verfahren zur Wiederherstellung vergessener oder verschlüsselter Zugangsdaten. Verwendet werden dabei Methoden wie Wörterbuchangriffe, Brute-Force-Verfahren oder die Nutzung zuvor extrahierter Passwort-Hashes.

Wörterbuchangriff: Ein Wörterbuchangriff ist ein Verfahren zur Passwortwiederherstellung, bei dem eine vorbereitete Liste gängiger oder wahrscheinlich verwendeter Passwörter systematisch ausprobiert wird. Diese sogenannten „Wortlisten“ basieren häufig auf realen Datenlecks, typischen Mustern oder benutzerspezifischen Informationen (z. B. Namen, Geburtsdaten). Wörterbuchangriffe gelten als effizient, wenn schwache oder wiederverwendete Passwörter verwendet wurden.

Brute-Force-Verfahren: Das Brute-Force-Verfahren bezeichnet eine systematische und vollständige Durchprobierung aller möglichen Zeichenkombinationen eines Passworts. Es garantiert bei ausreichend Zeit und Rechenleistung die Wiederherstellung des korrekten Passworts, ist jedoch bei langen und komplexen Passwörtern rechnerisch sehr aufwendig. Brute-Force-Angriffe kommen in der forensischen Praxis meist nur in begrenzter Form oder in Kombination mit Optimierungen (z. B. Masken, Regeln) zum Einsatz.

Container-Image: Ein Container-Image ist eine verschlüsselte Datei, die mithilfe eines Programms wie VeraCrypt erstellt wurde. Sie verhält sich nach dem Mounten wie ein eigenständiger, virtuell eingebundener Datenträger. In einem Container-Image können beliebige Verzeichnisse und Dateien enthalten sein. Die Entschlüsselung ist nur mit dem korrekten Passwort möglich.

VeraCrypt: VeraCrypt ist eine Open-Source-Software zur Erstellung und Nutzung verschlüsselter Container-Dateien oder Partitionen. Sie basiert auf dem Vorgänger TrueCrypt und bietet verschiedene Verschlüsselungsalgorithmen. VeraCrypt wird in der forensischen Praxis genutzt, um verschlüsselte Datenzugriffe zu analysieren.

KeePass(-Datenbank): KeePass ist ein Open-Source-Programm zur Verwaltung von Passwörtern. Die gespeicherten Zugangsdaten werden in verschlüsselten Datenbankdateien mit der Endung `.kdbx` abgelegt. Der Zugriff auf diese Datenbanken erfolgt passwortgeschützt. In der forensischen Analyse kann eine geöffnete KeePass-Datenbank Hinweise auf weitere verwendete Passwörter oder Zugriffsgewohnheiten liefern.

Root (Eintragsverzeichnis): „Root“ bezeichnet das oberste Verzeichnis innerhalb der Datenbankstruktur, unter dem Einträge abgelegt werden können. Der Begriff ist nicht mit dem Systembenutzer „root“ zu verwechseln, sondern beschreibt hier die oberste Hierarchieebene innerhalb einer Passwortdatenbank.

recently-used.xbel: Die Datei `recently-used.xbel` ist eine XML-basierte Datei unter Linux-Desktops (z. B. GNOME), in der Verweise auf zuletzt geöffnete Dateien gespeichert werden. Sie enthält Zeitstempel, Dateipfade und Zugriffsinformationen. In der digitalen Forensik kann sie Hinweise auf die Nutzung von Dateien oder Programmen liefern.

semantische Übereinstimmung: Eine semantische Übereinstimmung liegt vor, wenn zwischen zwei Inhalten ein inhaltlicher oder thematischer Zusammenhang besteht, z. B. zwischen einem verwendeten Passwort und dem Inhalt eines Containers. In der forensischen Praxis wird eine solche Übereinstimmung als möglicher Hinweis, jedoch nicht als Beweis gewertet.