



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*),
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 den oben genannten Bildern inhaltlich entspricht.
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.

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.

6.7 Einschränkungen

- **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.

7. Gesicherte Dateien

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 betreffenden 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 identifiziert 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

```
1 PS D:\> dir
2     Verzeichnis: D:\
3 Mode                               LastWriteTime         Length Name
4 ----
5 -a-----      01.07.2025      22:12      12748128256 ForImage9.img
6
7 PS D:\> Get-FileHash .\ForImage9.img -Algorithm MD5
8 Algorithm      Hash
9 -----
10 MD5            9C9570F6F648BA1D0FF14F8CD6AACF39
    D:\ForImage9.img
```

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

PowerShell

```
1 PS D:\> Copy-Item .\ForImage9.img C:\Users\Vik\Desktop\ForImage9.img
2 PS D:\> Get-FileHash 'C:\Users\Vik\Desktop\ForImage9.img' -Algorithm MD5
3
4 Algorithm      Hash
5 -----
6 MD5            9C9570F6F648BA1D0FF14F8CD6AACF39
    C:\Users\Vik\Desktop\ForImage...
```

7.2 Zugriff auf das Image

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

Bash

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

7.3 Passwort-Extraktion

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

Shell

```
1  sudo cat ./etc/shadow
2
3  pc:$y$j9T$grah6StsN64vZy4TX6DL01$jFAPKwPTtCP25YeK6fiAicbse.xZb3XaFXnIuwfaej4:19175:0:99999:
  7:::
4  niels:$6$mysalt$XV5j4lT9Ut5S96EU11gyef6DVRi4Gj0k7QCVMXDiGDkw.0vBPQcvRqgj iadq22fLuTMwT92GhAv
  MMg074L07w.:19177:0:99999:7:::
5  barney:$6$mysalt$9SMwo3IGWSIppwbVACGblzrNYJtxG8pjChCdVKmiFCoGm075DAiKAIDooGtETCV5vruzdJeqwb
  3nYIjw7KtUv0:19177:0:99999:7:::
```

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

Plain text

```
1  pc:$y$j9T$grah6StsN64vZy4TX6DL01$jFAPKwPTtCP25YeK6fiAicbse.xZb3XaFXnIuwfaej4
2  niels:$6$mysalt$XV5j4lT9Ut5S96EU11gyef6DVRi4Gj0k7QCVMXDiGDkw.0vBPQcvRqgj iadq22fLuTMwT92GhAv
  MMg074L07w
3  barney:$6$mysalt$9SMwo3IGWSIppwbVACGblzrNYJtxG8pjChCdVKmiFCoGm075DAiKAIDooGtETCV5vruzdJeqwb
  3nYIjw7KtUv0
```

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

```
1  curl -b "MoodleSessionmoodlehsma=016e963ec86fc2134833450bbebb24e0" https://moodle.hs-  
    mannheim.de/pluginfile.php/479555/mod_resource/content/1/wordlist.txt -L > wordlist.txt  
2  
3  hashcat --user passwd.txt wordlist.txt
```

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

Plain text

```
1  niels:xaiCh7fi  
2  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

```
1  find . -type f -name "places.sqlite"  
2  
3  
4  ./barney/snap/firefox/common/.mozilla/firefox/sn0kzhia.default/places.sqlite  
5  ./pc/snap/firefox/common/.mozilla/firefox/hsn68zcyj.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

1 SELECT * FROM moz_places
2
3 1|https://www.mozilla.org/privacy/firefox/|gro.allizom.www.|1|1|0|24|1656953208163056|A5Sq
  0lBd6fKM|0|47356411089529|||1
4 2|https://www.mozilla.org/de/privacy/firefox/|Firefox Datenschutzhinweis –
  Mozilla|gro.allizom.www.|1|0|0|98|1656953208364479|FfSBQlDTyqs0|0|47360031482596|
5   Our Privacy Notices describe the data our products and services receive, share, and use,
  as well as choices available to you.
6 |https://www.mozilla.org/media/img/mozorg/mozilla-256.4720741d4108.jpg||1
7 3|https://support.mozilla.org/products/firefox|gro.allizom.troppus.|0|0|0|137||yJd1Viv0pI_
  p|1|47358327123126|||2
8 [...]
```

Die vollständige Browser-History ist in Anlage 1 enthalten.

Die neunte Spalte enthält 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/share/recently-used.xbel`:

```
</> XML

1 <?xml version="1.0" encoding="UTF-8"?>
2 <xbel version="1.0"
3   xmlns:bookmark="http://www.freedesktop.org/standards/desktop-bookmarks"
4   xmlns:mime="http://www.freedesktop.org/standards/shared-mime-info"
5 >
6   <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">
7     <info>
8       <metadata owner="http://freedesktop.org">
9         <mime:mime-type type="inode/directory"/>
10        <bookmark:applications>
11          <bookmark:application name="org.gnome.Nautilus" exec="&apos;org.gnome.Nautilus
  %u&apos;" modified="2022-07-04T16:30:33.590045Z" count="1"/>
12        </bookmark:applications>
13      </metadata>
14    </info>
```

```

15     </bookmark>
16     <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">
17         <info>
18             <metadata owner="http://freedesktop.org">
19                 <mime:mime-type type="application/octet-stream"/>
20                 <bookmark:applications>
21                     <bookmark:application name="veracrypt" exec="&apos;veracrypt %u&apos;"
modified="2022-07-04T20:11:09.132405Z" count="3"/>
22                 </bookmark:applications>
23             </metadata>
24         </info>
25     </bookmark>
26     <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">
27         <info>
28             <metadata owner="http://freedesktop.org">
29                 <mime:mime-type type="application/x-keepass2"/>
30                 <bookmark:applications>
31                     <bookmark:application name="keepassxc" exec="&apos;keepassxc %u&apos;"
modified="2022-07-04T20:10:16.757845Z" count="1"/>
32                 </bookmark:applications>
33             </metadata>
34         </info>
35     </bookmark>
36     [...]

```

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 Users `barney` wurde eine passwortgeschützte KeePass-Datenbank gefunden:

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

Die Datenbank ließ sich mit dem zuvor wiederhergestellten Passwort `ahM4Hood` öffnen. In der Datenbank war ein einziges Passwort im Verzeichnis "Root" hinterlegt. Der Titel des Eintrags lautete „VeraCrypt“.

Das Passwort lautet „littleGirls“. **Der Inhalt des Passworts könnte auf eine bewusste Themenwahl hindeuten; eine rechtliche Bewertung dieser Tatsache erfolgt durch das Gericht.**

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

7.8 Korrrpute 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
1  xxd c1.jpeg | head -n 20
2  00000000: ddd8 ffe0 0010 4a46 4946 0001 0100 0001  ....JFIF.....
3  00000010: 0001 0000 ffdb 0084 0009 0607 1210 1215  ....
4  00000020: 0f10 1216 1015 0f10 1010 0f15 1015 150f  ....
5  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

```
1 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 unbedeckten 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.

8. Anlagen

Anlage 1: Vollständige Browser-History des users barney



Plain text

```
1 1|https://www.mozilla.org/privacy/firefox/|gro.allizom.www.|1|1|0|24|1656953208163056|A5Sq
0lBd6fKM|0|47356411089529|1|1
2 2|https://www.mozilla.org/de/privacy/firefox/|Firefox Datenschutzhinweis –
Mozilla|gro.allizom.www.|1|0|0|98|1656953208364479|FfSBQLDTyqs0|0|47360031482596|
3 Our Privacy Notices describe the data our products and services receive, share, and use,
as well as choices available to you.
4 |https://www.mozilla.org/media/img/mozorg/mozilla-256.4720741d4108.jpg|1
5 3|https://support.mozilla.org/products/firefox|gro.allizom.troppus.|0|0|0|137|yJd1VIvOpI_
p|1|47358327123126|1|2
6 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|4735995645
0016|1|2
7 5|https://www.mozilla.org/contribute/|gro.allizom.www.|0|0|0|137|ZUp2Xs0my0fc|1|473573642
18428|1|1
8 6|https://www.mozilla.org/about/|gro.allizom.www.|0|0|0|137|PxGc7HWdpK3u|1|47357608426557
|1|1
9 7|https://www.mozilla.org/firefox/central/|gro.allizom.www.|0|0|0|137|SmvTP_gRfA1X|1|4735
9969280417|1|1
10 8|https://www.google.com/search?channel=fs&client=ubuntu&q=hot+cheerleader|hot cheerleader
– Google
Suche|moc.elgoog.www.|1|0|1|1950|1656953228105571|5k6iUfwoYDt_|0|47359856985002|1|3
11 10|https://www.google.com/search?
q=hot+cheerleader+pics&client=ubuntu&hs=Urn&channel=fs&source=lnms&tbm=isch&sa=X&ved=2ahUKE
wjpo6Tq19_4AhUz57sIHUuNAVoQ_AUoAXoECAEQAw&biw=950&bih=656&dpr=1|hot cheerleader pics –
Google Suche|moc.elgoog.www.|1|0|0|98|1656953247155094|WjfpN6MdgTYb|0|47357695506675|1|3
12 11|https://www.google.com/|Google|moc.elgoog.www.|1|0|1|2000|1751399635782628|V09fMBiQ_Qe3|
0|47357433249528|1|3
13 12|https://www.google.com/search?
q=sexy+girls+cheerleader&sca_esv=b5d146501cb8d5e6&source=hp&ei=0zxkaKD3KtqUxc8Pldb3oA8&ifls
ig=A0w8s4IAAAAAaGRK4zXwm–
Q5v50hRxjl8e7RuEd90d6H&ved=0ahUKEwjgrJWJuJy0AxVaSvEDHRXrHfQQ4dUDCA4&uact=5&oq=sexy+girls+ch
earleader&gs_lp=Egdnd3Mtd2l6IHZzZXh5IGdpcmxzIGNoZWYybGVlZGVyS0FEUK8GWIdCcAF4AJABAjgBW6ABkg2
qAQIyMrgBA8gBAPgBAZgCBKACiwOoAgrCAgoQABgDGOoCGI8BwgIKEC4YAxjqAhiPacICBBAAGAPCAGsQABiABBixAx
iDacICERAUgIAEGLEDGNGEDGIMBGMcBwgIOEC4YgAQYsQMY0QMYxwHCAhQQLhiABBixAxjRaxiDARjHARiKBcICERAUg
IAEGLEDGIMBGNQCGIoFwgIOEAAYgAQYsQMYgweYigXCAGsQLhiABBjRaxjHAcICBRAAGIAEwgIFEC4YgATCaggQABiA
BBixA8ICCBauGIAEGLEDwgILEC4YgAQYsQMY1AKYA0vxBS4Z00fBhgVBkgcDMY4xoAf60rIHazIuMbgHwALCBwczLTE
uMi4xyAeJAQ&sclient=gws-wiz|Google
Search|moc.elgoog.www.|1|0|0|100|1751399650395128|VwD1rG0Id0VP|0|47358104091540|1|3
14 13|https://www.google.com/search?
q=sexy+girls+cheerleader&sca_esv=b5d146501cb8d5e6&source=hp&ei=0zxkaKD3KtqUxc8Pldb3oA8&ifls
ig=A0w8s4IAAAAAaGRK4zXwm–
Q5v50hRxjl8e7RuEd90d6H&ved=0ahUKEwjgrJWJuJy0AxVaSvEDHRXrHfQQ4dUDCA4&uact=5&oq=sexy+girls+ch
earleader&gs_lp=Egdnd3Mtd2l6IHZzZXh5IGdpcmxzIGNoZWYybGVlZGVyS0FEUK8GWIdCcAF4AJABAjgBW6ABkg2
qAQIyMrgBA8gBAPgBAZgCBKACiwOoAgrCAgoQABgDGOoCGI8BwgIKEC4YAxjqAhiPacICBBAAGAPCAGsQABiABBixAx
iDacICERAUgIAEGLEDGNGEDGIMBGMcBwgIOEC4YgAQYsQMY0QMYxwHCAhQQLhiABBixAxjRaxiDARjHARiKBcICERAUg
IAEGLEDGIMBGNQCGIoFwgIOEAAYgAQYsQMYgweYigXCAGsQLhiABBjRaxjHAcICBRAAGIAEwgIFEC4YgATCaggQABiA
BBixA8ICCBauGIAEGLEDwgILEC4YgAQYsQMY1AKYA0vxBS4Z00fBhgVBkgcDMY4xoAf60rIHazIuMbgHwALCBwczLTE
```

uMi4xyAeJAQ&scient=gws-wiz&sei=4jxkaILdFq3Xxc8PkYvV0Q0|sexy girls chearleader - Google
Suche|moc.elgoog.www. |1|0|0|100|1751399650869426|oD-XfeUoeZN9|0|47357505484614| |||3
15 14|https://www.google.com/search?
sca_esv=b5d146501cb8d5e6&q=sexy+girls+cheerleader&udm=2&fbs=AIiJpHw2KGh6wpocn18KLjPMw8n5Yp8
-1M0n6BD6JoVBP_K3fXXvA3S3XGyupmJLMg20um-
mJAe036stiqcDeSp1syInrodDcdKxMuB2TiCVf45CLzCoNRKRBZlvU8DUj0lI7KC-ZRxx-
gxikqc1yM1oJcoJGNUwir8qlkx4kLIK4GELCJ58DYXpqPW_aK1GFeloqICCzjL7&sa=X&ved=2ahUKEwjkhRGQuJy0A
xVsSfEDHWfWK1sQtKgLKAF6BAgTEAE&biw=950&bih=656&dpr=1|sexy girls cheerleader - Google
Suche|moc.elgoog.www. |2|0|0|200|1751399794152616|84PG8mjR9eFS|0|47359998535018| |||3
16 15|https://www.google.com/search?
sca_esv=b5d146501cb8d5e6&q=sexy+girls+cheerleader&udm=2&fbs=AIiJpHw2KGh6wpocn18KLjPMw8n5Yp8
-1M0n6BD6JoVBP_K3fXXvA3S3XGyupmJLMg20um-
mJAe036stiqcDeSp1syInrodDcdKxMuB2TiCVf45CLzCoNRKRBZlvU8DUj0lI7KC-ZRxx-
gxikqc1yM1oJcoJGNUwir8qlkx4kLIK4GELCJ58DYXpqPW_aK1GFeloqICCzjL7&sa=X&ved=2ahUKEwjkhRGQuJy0A
xVsSfEDHWfWK1sQtKgLKAF6BAgTEAE&biw=950&bih=656&dpr=1#vhid=cxWEukMoNf2AeM&vssid=mosaic|sexy
girls cheerleader - Google
Suche|moc.elgoog.www. |1|0|0|100|1751399681729745|oK9M9ukKGCqYk|0|47359365193005| |||3
17 16|https://www.google.com/search?
sca_esv=b5d146501cb8d5e6&q=sexy+girls+cheerleader&udm=2&fbs=AIiJpHw2KGh6wpocn18KLjPMw8n5Yp8
-1M0n6BD6JoVBP_K3fXXvA3S3XGyupmJLMg20um-
mJAe036stiqcDeSp1syInrodDcdKxMuB2TiCVf45CLzCoNRKRBZlvU8DUj0lI7KC-ZRxx-
gxikqc1yM1oJcoJGNUwir8qlkx4kLIK4GELCJ58DYXpqPW_aK1GFeloqICCzjL7&sa=X&ved=2ahUKEwjkhRGQuJy0A
xVsSfEDHWfWK1sQtKgLKAF6BAgTEAE&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 18|https://www.google.com/url?
sa=i&url=https%3A%2F%2Fwww.shutterstock.com%2Fde%2Fsearch%2Fhot-
cheerleader&psig=A0vVaw1jVI9MPGMcs8DtCnFhnfLL&ust=1751486058108000&source=images&cd=vfe&opi
=89978449&ved=0CBQQjRxqFwoTCNjdLZ-
4nI4DFQAAAAAABAS| |moc.elgoog.www. |1|1|0|25|1751399857179623|-
VXB1m6v3hA9|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

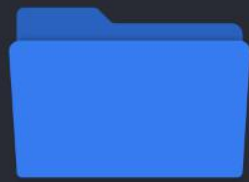


c4.jpeg

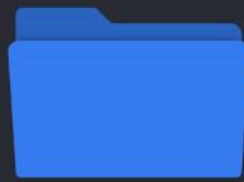
Anlage 3: Gelöschtes Bildmaterial



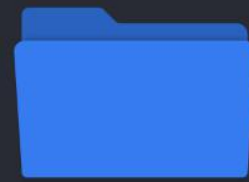
recovered_data



jpg



png



webp



f1431560.jpg



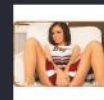
f1437928.jpg



f1438152.jpg



f1461800.jpg



f1461928.jpg



f1462024.jpg



f1462048.jpg



f1462192.jpg



f1464376.jpg



f1464768.jpg



f1470136.jpg



f1507000.jpg



f1520680.jpg



f1520728.jpg



f1531280.jpg



f1536672.jpg



f1537056.jpg



f1552456.jpg



f1560008.jpg



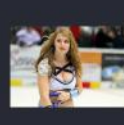
f1560040.jpg



f1563976.jpg



f1564032.jpg



f1565320.jpg



f1565408.jpg



317 files: 4.7 MiB (4,892,798 bytes) | Free space: 180.1 GiB



f13548312.png



f13548408.png



f13946368.png



f13947392.png



f13948672.png



f19438328.png



f29890880.png



f29896824.png

8 files: 3.8 MiB (3,987,776 bytes) | Free space: 180.1 GiB



f1569440.webp



f4272024.webp



f4272104.webp



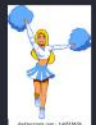
f4272144.webp



f4276640.webp



f10094248.webp



f10094296.webp



f10214664.webp



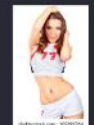
f10247384.webp



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

```
1 <?xml version="1.0" encoding="UTF-8"?>
2 <xbel version="1.0"
3     xmlns:bookmark="http://www.freedesktop.org/standards/desktop-bookmarks"
4     xmlns:mime="http://www.freedesktop.org/standards/shared-mime-info"
5 >
6     <bookmark href="file:///media/barney/067E7AF632AA2E11/Bilder" added="2022-07-
7         04T16:30:33.590042Z" modified="2022-07-04T16:30:33.590048Z" visited="2022-07-
8         04T16:30:33.590043Z">
9         <info>
10             <metadata owner="http://freedesktop.org">
11                 <mime:mime-type type="inode/directory"/>
12                 <bookmark:applications>
13                     <bookmark:application name="org.gnome.Nautilus" exec="&apos;org.gnome.Nautilus
14 %u&apos;" modified="2022-07-04T16:30:33.590045Z" count="1"/>
15                 </bookmark:applications>
16             </metadata>
17         </info>
18     </bookmark>
19     <bookmark href="file:///media/barney/067E7AF632AA2E11/xxx" added="2022-07-
20         04T16:34:14.977136Z" modified="2022-07-04T20:11:09.132408Z" visited="2022-07-
21         04T16:34:14.977137Z">
22         <info>
23             <metadata owner="http://freedesktop.org">
24                 <mime:mime-type type="application/octet-stream"/>
25                 <bookmark:applications>
26                     <bookmark:application name="veracrypt" exec="&apos;veracrypt %u&apos;"
27 modified="2022-07-04T20:11:09.132405Z" count="3"/>
28                 </bookmark:applications>
29             </metadata>
30         </info>
31     </bookmark>
32     <bookmark href="file:///home/barney/Pass.kdbx" added="2022-07-04T20:10:16.757839Z"
33 modified="2022-07-04T20:10:16.757851Z" visited="2022-07-04T20:10:16.757841Z">
34         <info>
35             <metadata owner="http://freedesktop.org">
36                 <mime:mime-type type="application/x-keepass2"/>
37                 <bookmark:applications>
38                     <bookmark:application name="keepassxc" exec="&apos;keepassxc %u&apos;"
39 modified="2022-07-04T20:10:16.757845Z" count="1"/>
40                 </bookmark:applications>
41             </metadata>
42         </info>
43     </bookmark>
44     <bookmark href="file:///home/barney/Dokumente/Annual_Report.odp" added="2025-07-
45         01T20:06:39.710911Z" modified="2025-07-01T20:06:39.710943Z" visited="2025-07-
46         01T20:06:39.710925Z">
47         <info>
48             <metadata owner="http://freedesktop.org">
49                 <mime:mime-type type="application/vnd.oasis.opendocument.presentation"/>
50                 <bookmark:applications>
```


9. 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.