

Befundsdokumentation 3.1.

Übungsaufgabe 3 - A1

Team: 13

Bearbeiter: 3009728 | 3026182 | 3019335 | 3008816

Datum der Erstellung: 25.04.2025

Nicht-technische Zusammenfassung

Eine für Laien verständliche Zusammenfassung der Untersuchung und der wichtigsten Erkenntnisse.

In der Untersuchung wurden zwei beschädigte Dateien (RecoverMe01.raw und RecoverMe02.raw) analysiert. Zunächst wurden beide Dateien in ein bearbeitbares Format umbenannt. Bei der Datei RecoverMe02.raw wurde mit einem Hex-Editor der Header repariert, indem ein fehlerhaftes "Magic Byte" angepasst wurde. Danach konnte die Datei erfolgreich als .png -Bild geöffnet werden.

Anschließend wurde RecoverMe01.raw untersucht. Mittels exiftool wurden Metadaten ausgelesen, die auf ein Bild einer Canon EOS 1000D hinwiesen. Auch hier wurde der fehlerhafte Dateikopf im Hex-Editor korrigiert. Danach wurde die Datei zu RecoverMe01.jpeg umbenannt und konnte ebenfalls geöffnet werden.

Technischer Bericht

1. Übersicht der analysierten Daten

Datenquelle	Typ	Datentyp	Größe	Hash (SHA256)
~/Desktop/DIF/Aufgabe2/Image/U2.img	Disk-image	RAW	8.4GB	ea49596c6ae0700ccab0978d0d84c94ad472e6ae
~/mnt/evidence/RecoverMe01	-	-	1.6MB	
~/mnt/evidence/RecoverMe02	-	-	20KB	

2. Chronologisches Analyseprotokoll

Jede Terminal-Eingabe mit zugehörigem Befehl, Zeitstempel, GPG-Signatur, Hash-Wert, Ausgabe, Kontext und (falls vorhanden) rechtlicher Erklärung .

[++] Executed commands & logs

Info

Beide RecoverMe Dateien wurde mittels `cp` Command in `.raw` Dateien umbenannt und anschließend analysiert

[+] Command: `wxHexEditor RecoverMe02.raw`

- Timestamp: `2025-04-24T08-45-46-502978+00-00`
- GPG-signature: [+] Valid
- SHA256: `fd919e45a98f1ae9c0947eed0f758c5cc388ed705627f6eb2e150686d70814bc`

Output:

```
1  [!] Command failed:
```

Context:

Analyst: Markus Winklhofer

Timestamp: 2025-04-24T08:46:36.320943+00:00

[x] No specific explanation found.

[+] Command: `ls`

- Timestamp: `2025-04-24T08-46-55-025730+00-00`
- GPG-signature: [+] Valid
- SHA256: `784735f4a3dc1bba66ee16678f0d70e78913288472f2e9c9514b3599233545f7`

Output:

```
1  [STDOUT]
2  Image
3  RecoverMe01
4  RecoverMe01.jpeg
5  RecoverMe02
6  RecoverMe02.raw
7  U2.zip
8  U2.zip.md5
```

```
9    U2.zip.sha1
10   vUSB.zip
11
12   [STDERR]
```

Context:

Analyst: Markus Winklhofer

Timestamp: 2025-04-24T08:46:55.171977+00:00

`ls` lists files in a directory. It is used to gain an overview and does not modify data.

[+] Command: wxHexEditor RecoverMe02.raw

- Timestamp: 2025-04-24T08-51-44-569895+00-00
- GPG-signature: [+] Valid
- SHA256: f26b5791b1a7401af6ad61ad94be8c7c57ef4fa7db9b4b6e85ee7495eefc26a1

Output:

```
1   [STDOUT]
2
3   [STDERR]
4   10:53:24 AM: Debug: In file ./src/unix/threadpsx.cpp at line 293:
    'pthread_mutex_destroy()' failed with error 0x00000010 (Device or
    resource busy).
```

Context:

Analyst: Markus Winklhofer

Timestamp: 2025-04-24T08:53:24.233705+00:00

[x] No specific explanation found.

Done

Header wurde analysiert und mit funktionsfähigem verglichen [1].

Magic Byte wurde anschließend im Header in der ersten Zeile, viertem Paar, von 77 auf 47 geändert.

Magic Bytes: 89 50 4E 47 0D 0A 1A 0A

[+] Command: `ls`

- Timestamp: 2025-04-24T08:56:18-852794+00-00
- GPG-signature:`` [+] Valid
- SHA256: 784735f4a3dc1bba66ee16678f0d70e78913288472f2e9c9514b3599233545f7

Output:

```
1  [STDOUT]
2  Image
3  RecoverMe01
4  RecoverMe01.jpeg
5  RecoverMe02
6  RecoverMe02.raw
7  U2.zip
8  U2.zip.md5
9  U2.zip.sha1
10 vUSB.zip
11
12 [STDERR]
```

Context:

Analyst: Markus Winklhofer

Timestamp: 2025-04-24T08:56:19.001523+00:00

`ls` lists files in a directory. It is used to gain an overview and does not modify data.

[+] Command: `cp RecoverMe02.raw RecoverMe02.png`

- Timestamp: 2025-04-24T08:57-07-003230+00-00
- GPG-signature: [+] Valid
- SHA256: aec4dbdae6db78716bf86b6c6d3a9f3327d00c39a9d0715fb7ff7b953c1c499f

Output:

```
1  [STDOUT]
2
3  [STDERR]
```

Context:

Analyst: Markus Winklhofer

Timestamp: 2025-04-24T08:57:07.149380+00:00

[x] No specific explanation found.

Done

Die reparierte Datei wurde per `cp` Command von `.raw` zu `.png` geändert. Anschließend kann diese normal geöffnet werden.

[+] Command: `ls`

- Timestamp: 2025-04-24T08-57-17-302116+00-00
- GPG-signature: [+] Valid
- SHA256: a2ac54cf01253b71879739100b49898287236b68054245c736a634dae82260bc

Output:

```
1  [STDOUT]
2  Image
3  RecoverMe01
4  RecoverMe01.jpeg
5  RecoverMe02
6  RecoverMe02.png
7  RecoverMe02.raw
8  U2.zip
9  U2.zip.md5
10 U2.zip.sha1
11 vUSB.zip
12
13 [STDERR]
```

Context:

Analyst: Markus Winklhofer

Timestamp: 2025-04-24T08:57:17.448549+00:00

`ls` lists files in a directory. It is used to gain an overview and does not modify data.

[+] Command: `open RecoverMe02.png`

- Timestamp: 2025-04-24T08-57-38-196020+00-00
- GPG-signature: [+] Valid
- SHA256: aec4bdbae6db78716bf86b6c6d3a9f3327d00c39a9d0715fb7ff7b953c1c499f

Output:

```
1 [STDOUT]
2
3 [STDERR]
```

Context:

Analyst: Markus Winklhofer

Timestamp: 2025-04-24T08:58:26.154584+00:00

[x] No specific explanation found.

Info

Weiterführend wird die Datei `RecoverMe01.raw` analysiert.

[+] Command: `ls`

- Timestamp: 2025-04-24T09-04-05-315311+00-00
- GPG-signature: [+] Valid
- SHA256: d18189002ac39e8ec0b2c63726835eb0324d128ae9231fe473685c1dc0f35581

Output:

```
1 [STDOUT]
2 Image
3 RecoverMe01
4 RecoverMe02
5 RecoverMe02.png
6 RecoverMe02.raw
7 U2.zip
8 U2.zip.md5
9 U2.zip.sha1
10 vUSB.zip
11
12 [STDERR]
```

Context:

Analyst: Markus Winklhofer

Timestamp: 2025-04-24T09:04:05.465531+00:00

`ls` lists files in a directory. It is used to gain an overview and does not modify data.

[+] Command: `ls`

- Timestamp: 2025-04-24T09-04-39-168818+00-00
- GPG-signature: [+] Valid
- SHA256: 300e0424c989a3775dcf116c405d19fbe316420fa1e515fd8837200c0d056de7

Output:

```
1  [STDOUT]
2  Image
3  RecoverMe01
4  RecoverMe01.raw
5  RecoverMe02
6  RecoverMe02.png
7  RecoverMe02.raw
8  U2.zip
9  U2.zip.md5
10 U2.zip.sha1
11 vUSB.zip
12
13 [STDERR]
```

Context:

Analyst: Markus Winklhofer

Timestamp: 2025-04-24T09:04:39.316116+00:00

`ls` lists files in a directory. It is used to gain an overview and does not modify data.

[+] Command: `wxHexEditor RecoverMe01.raw`

- Timestamp: 2025-04-24T09-04-59-125448+00-00
- GPG-signature: [+] Valid
- SHA256: bdd61ac5c1e3d6fab5d64f4b7a13c4cbd21e40ef912b0ffd5932ca04cd588073

Output:

```
1 [STDOUT]
2
3 [STDERR]
4 11:05:36 AM: Debug: In file ./src/unix/threadpsx.cpp at line 293:
  'pthread_mutex_destroy()' failed with error 0x00000010 (Device or
  resource busy).
```

Context:

Analyst: Markus Winklhofer

Timestamp: 2025-04-24T09:05:36.856869+00:00

[x] No specific explanation found.

Done

Datei wird im Hex-Editor wxHexEditor geöffnet und analysiert. Der Hexcode gibt Hinweise auf EXIF Daten einer JPEG Datei.

[+] Command: `exiftool RecoverMe01.raw`

- Timestamp: 2025-04-24T09-06-43-565174+00-00
- GPG-signature: [+] Valid
- SHA256: d70088202929df56b649dd823b8f66a82e43c9e083b002e8dee1552d86499d9f

Output:

```
1 [STDOUT]
2 ExifTool Version Number      : 13.10
3 File Name                    : RecoverMe01.raw
4 Directory                    : .
5 File Size                    : 1580 kB
6 File Modification Date/Time  : 2025:04:24 11:04:35+02:00
7 File Access Date/Time       : 2025:04:24 11:04:59+02:00
8 File Inode Change Date/Time  : 2025:04:24 11:04:35+02:00
9 File Permissions             : -rwxr-xr-x
10 Warning                     : Processing TIFF-like data after
  unknown 12-byte header
11 Exif Byte Order              : Little-endian (Intel, II)
12 Image Width                  : 1851
13 Image Height                 : 2453
14 Bits Per Sample              : 8 8 8
15 Photometric Interpretation   : RGB
16 Make                         : Canon
```

17	Camera Model Name	: Canon EOS 1000D
18	Orientation	: Horizontal (normal)
19	Samples Per Pixel	: 3
20	X Resolution	: 240
21	Y Resolution	: 240
22	Resolution Unit	: inches
23	Software	: Adobe Photoshop CS5 Windows
24	Modify Date	: 2010:09:17 14:44:37
25	Artist	: Rudolf Stricker
26	Exposure Time	: 1/100
27	F Number	: 11.0
28	Exposure Program	: Aperture-priority AE
29	ISO	: 200
30	Sensitivity Type	: Unknown
31	Exif Version	: 0221
32	Date/Time Original	: 2010:09:17 09:37:05
33	Create Date	: 2010:09:17 09:37:05
34	Shutter Speed Value	: 1/100
35	Aperture Value	: 11.0
36	Exposure Compensation	: 0
37	Max Aperture Value	: 2.7
38	Subject Distance	: 6.88 m
39	Metering Mode	: Center-weighted average
40	Flash	: Off, Did not fire
41	Focal Length	: 23.0 mm
42	Sub Sec Time	: 94
43	Sub Sec Time Original	: 94
44	Sub Sec Time Digitized	: 94
45	Color Space	: sRGB
46	Exif Image Width	: 1641
47	Exif Image Height	: 2182
48	Focal Plane X Resolution	: 4438.356164
49	Focal Plane Y Resolution	: 4445.969125
50	Focal Plane Resolution Unit	: inches
51	Custom Rendered	: Normal
52	Exposure Mode	: Auto
53	White Balance	: Auto
54	Scene Capture Type	: Standard
55	Owner Name	: Rudolf Stricker
56	Serial Number	: 2350566822
57	Lens Info	: 17-50mm f/?
58	Lens Model	: 17-50mm
59	GPS Version ID	: 2.2.0.0
60	GPS Latitude Ref	: North
61	GPS Longitude Ref	: East
62	GPS Altitude Ref	: Above Sea Level
63	GPS Time Stamp	: 09:37:05
64	GPS Satellites	: 0
65	GPS Map Datum	: WGS-84
66	GPS Date Stamp	: 2010:09:17

```
67  Compression                : JPEG (old-style)
68  Thumbnail Offset            : 1250
69  Thumbnail Length            : 8817
70  Aperture                    : 11.0
71  Image Size                  : 1851x2453
72  Megapixels                   : 4.5
73  Scale Factor To 35 mm Equivalent: 1.6
74  Shutter Speed                : 1/100
75  Create Date                  : 2010:09:17 09:37:05.94
76  Date/Time Original           : 2010:09:17 09:37:05.94
77  Modify Date                  : 2010:09:17 14:44:37.94
78  Thumbnail Image              : (Binary data 8817 bytes, use -b option
    to extract)
79  GPS Altitude                  : 99 m Above Sea Level
80  GPS Date/Time                 : 2010:09:17 09:37:05Z
81  GPS Latitude                  : 49 deg 28' 10.56" N
82  GPS Longitude                 : 8 deg 28' 56.32" E
83  Circle Of Confusion           : 0.019 mm
84  Depth Of Field                : inf (1.89 m - inf)
85  Field Of View                 : 51.6 deg
86  Focal Length                  : 23.0 mm (35 mm equivalent: 37.2 mm)
87  GPS Position                  : 49 deg 28' 10.56" N, 8 deg 28' 56.32"
    E
88  Hyperfocal Distance           : 2.59 m
89  Light Value                   : 12.6
90  Lens ID                       : 17-50mm
91
92  [STDERR]
```

Context:

Analyst: Markus Winklhofer

Timestamp: 2025-04-24T09:06:43.785800+00:00

[x] No specific explanation found.

Done

Exif Daten werden mittels exiftool eingelesen und analysiert. Aus den Exif-Daten ist unter:

```
Warning : Processing TIFF-like data after unknown 12-byte header
```

herauszulesen, dass der 12-Byte header nicht richtig eingelesen werden kann.

[+] Command: wxHexEditor RecoverMe01.raw

- Timestamp: 2025-04-24T09-08-43-172860+00-00
- GPG-signature: [+] Valid
- SHA256: 665e81bace22968926d83714eb3baa5199337aefaa4ffa59441034ee96bb1005

Output:

```
1 [STDOUT]
2
3 [STDERR]
4 11:09:12 AM: Debug: In file ./src/unix/threadpsx.cpp at line 293:
  'pthread_mutex_destroy()' failed with error 0x00000010 (Device or
  resource busy).
```

Context:

Analyst: Markus Winklhofer

Timestamp: 2025-04-24T09:09:12.199523+00:00

[x] No specific explanation found.

 **Done**

MagicBytes der Datei wurden abgeglichen und entsprechend angepasst:

F8 D8 FF E1 -> FF D8 FF E1

[+] Command: mv RecoverMe01.raw RecoverMe01.jpeg

- Timestamp: 2025-04-24T09-10-20-477711+00-00
- GPG-signature: [+] Valid
- SHA256: aec4dbdae6db78716bf86b6c6d3a9f3327d00c39a9d0715fb7ff7b953c1c499f

Output:

```
1 [STDOUT]
2
3 [STDERR]
```

Context:

Analyst: Markus Winklhofer

Timestamp: 2025-04-24T09:10:20.625945+00:00

[x] No specific explanation found.

 **Done**

RecoverMe01.raw Datei wurde zu RecoverMe01.jpeg umgeändert.

[+] Command: `ls`

- Timestamp: 2025-04-24T09-10-29-714525+00-00
- GPG-signature: [+] Valid
- SHA256: a2ac54cf01253b71879739100b49898287236b68054245c736a634dae82260bc

Output:

```
1  [STDOUT]
2  Image
3  RecoverMe01
4  RecoverMe01.jpeg
5  RecoverMe02
6  RecoverMe02.png
7  RecoverMe02.raw
8  U2.zip
9  U2.zip.md5
10 U2.zip.sha1
11 vUSB.zip
12
13 [STDERR]
```

Context:

Analyst: Markus Winklhofer

Timestamp: 2025-04-24T09:10:29.860714+00:00

`ls` lists files in a directory. It is used to gain an overview and does not modify data.

[+] Command: `open RecoverMe01.jpeg`

- Timestamp: 2025-04-24T09-10-45-533002+00-00

- GPG-signature: [+] Valid
- SHA256: aec4dbdae6db78716bf86b6c6d3a9f3327d00c39a9d0715fb7ff7b953c1c499f

Output:

```
1 [STDOUT]
2
3 [STDERR]
```

Context:

Analyst: Markus Winklhofer

Timestamp: 2025-04-24T09:10:52.565202+00:00

[x] No specific explanation found.

[+] GPG-Overview

Each .log -file was digitally signed with GPG.

The signature status is documented per command.

3. Ergebnisse

[RecoverMe01.jpeg](#)

[RecoverMe02.png](#)

4. Verwendete Quellen

[1] https://en.wikipedia.org/wiki/List_of_file_signatures