Befundsdokumentation 4.2.

Übungsaufgabe 4 - A2

Team: 13
Bearbeiter: 3009728 | 3026182 | 3019335 | 3008816
Datum der Erstellung: 04.05.2025

Nicht-technische Zusammenfassung

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

Im Rahmen dieser Untersuchung wurde ein forensisches Abbild („Image“) eines USB-Sticks erstellt, um dessen Inhalt vollständig und unverändert zu erfassen. Ziel war es, alle auf dem Stick vorhandenen Dateien sicher zu extrahieren, ihre Echtheit zu prüfen und nach versteckten oder manipulierten Daten zu suchen .

Vorgehensweise und technische Schritte

- Zuerst wurde das gelieferte Archiv entpackt und das enthaltene Abbild (`vUSB.img` , ca. 3,1 GB) via SHA-256-Prüfsumme auf Unversehrtheit verifiziert .
- Anschließend wurde dieses Image als virtuelles Laufwerk eingebunden, um das Dateisystem dort eingehend zu untersuchen .

Dateisystem und gefundene Dateien

- Auf dem Stick liegt ein standardmäßiges FAT32-Dateisystem vor, wie es bei USB-Sticks häufig verwendet wird (mit Boot-Bereich, zwei FAT-Tabellen und Datenbereich) .
- Insgesamt konnten drei Bilddateien gefunden werden:
  1. **Bild1_extr.jpg** (ca. 193 KB, 1 536 × 1 152 Pixel): Zeigt einen Greifvogel, wurde zuletzt am 9. Mai 2022 erstellt. Alle sichtbaren und unsichtbaren Metadaten sind unauffällig .
  2. **Bild2_extr.jpeg** (ca. 2,1 MB, 1 600 × 1 600 Pixel): Ebenfalls eine Greifvogelaufnahme, mit üblicher JPEG-Kodierung und unveränderten Metadaten vom Mai 2022.
  3. **blue_extr.png** (ca. 16 KB, 1 920 × 1 080 Pixel): Ein komplett blaues Bild, in GIMP erstellt, letzte Änderung am 9. Mai 2022, enthält zusätzliche Information über einen PIN, der in einem nahezu identischen Blauton im Bild hinterlegt ist.

Prüfung auf Manipulation und Vollständigkeit

- Die drei Dateien wurden sowohl direkt aus dem USB-Abbild als auch nach Entpacken aus einem SquashFS-Container extrahiert. Dabei ergaben sich jeweils identische SHA-256-Hashes, was eine unveränderte Übertragung bestätigt.
- Zusätzlich wurde das Anlegen des Abbilds mit verschiedenen Tools (z. B. `dd`, `dcfldd`) wiederholt und jedes Mal durch Hash-Vergleiche bestätigt, dass keine Änderungen auftraten.

Ergebnis und Schlussfolgerung
Die Untersuchung ergab keinerlei Auffälligkeiten: Das Dateisystem enthält ausschließlich die drei genannten Bilder und die üblichen FAT-Metadaten, ohne versteckte Dateien oder unübliche Datenstrukturen. Eines der Bilder (Blue.png) enthält jedoch einen PIN, welcher lautet: 5713

Technischer Bericht

1. Übersicht der analysierten Daten

Datenquelle	Typ	Datentyp	Größe	Hash (SHA256)
vUSB	Disk Image	.img	3.1 GB	2c9c0f5117cdc3e8f3b9156bb5eef7d95 63f46b
Bild1.jpg		.jpg		d2cc34b1613360da8fe39bd9f95e0749f0d48ac
Bild2.jpeg		.jpeg		01b8a6d33ba74fec3a5e04fdd3d52f9738bd97c
Blue.png		.png		efc4cbf142fdfe55d5695fe02240cd1f0782e086

2. Chronologisches Analyseprotokoll

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

[++] Timeline of Commands and Comments

[+] Command: `7z x vUSB.zip`

- Timestamp: `2025-05-04T19-35-59-312959+00-00`
- GPG-signature: [+] Valid
- SHA256: `9c4434d8acac9975e5f754a99116962b73611ce965e200470a5503db92a0a9ed`

Output:

```
[STDOUT]

7-Zip 24.09 (arm64) : Copyright (c) 1999-2024 Igor Pavlov : 2024-11-29
 64-bit arm_v:8-A locale=en_US.UTF-8 Threads:4 OPEN_MAX:1024, ASM

Scanning the drive for archives:
1 file, 5484894 bytes (5357 KiB)

Extracting archive: vUSB.zip
--
Path = vUSB.zip
Type = zip
Physical Size = 5484894

Everything is Ok

Size:       3221225472
Compressed: 5484894

[STDERR]
```

Context:

Analyst: Markus Winklhofer
Timestamp: 2025-05-04T19:36:05.796143+00:00

[x] No specific explanation found.

[+] Command: `shasum -a 256 vUSB.img`

- Timestamp: `2025-05-04T19-39-04-287395+00-00`
- GPG-signature: [+] Valid
- SHA256: `a469ae61a6fe06fca24355b0515d0c6a258a776ea3772913a0f0ccd20b9bcba9`

Output:

```
[STDOUT]
2c9c0f5117cdc3e8f3b9156bb5eef7d9563f46b4e0e4e51123711d828c89e8a2
vUSB.img

[STDERR]
```

Context:

Analyst: Markus Winklhofer
Timestamp: 2025-05-04T19:39:15.051747+00:00

`shasum` generates SHA hash values (SHA-1 by default unless specified). It is used to verify file integrity. In forensic contexts, it is recommended to specify stronger hashes like SHA-256.

The `-a` option allows selection of the SHA variant (e.g., 1, 256, 512). Always use SHA-256 or higher for forensics.

[+] Command: `stat vUSB.img`

- Timestamp: `2025-05-04T19-41-46-086245+00-00`
- GPG-signature: [+] Valid
- SHA256: `b805cdc33a46ce035cbe758e05a8ac868036862012b7debe41c7377a15b99044`

Output:

Shell

```
[STDOUT]
  File: vUSB.img
  Size: 3221225472  Blocks: 6291464    IO Block: 4096   regular file
Device: 254,3   Inode: 3146325     Links: 1
Access: (0664/-rw-rw-r--)  Uid: ( 1000/  forick)   Gid: ( 1000/
forick)
Access: 2025-05-04 21:39:04.468824256 +0200
Modify: 2022-05-09 17:57:52.000000000 +0200
Change: 2025-05-04 21:36:05.775712707 +0200
 Birth: 2025-05-04 21:35:59.487683570 +0200

[STDERR]
```

Context:

Analyst: Markus Winklhofer
Timestamp: 2025-05-04T19:41:46.246873+00:00

[x] No specific explanation found.

[+] Command: `stat vUSB.img`

- Timestamp: `2025-05-04T19-42-37-005956+00-00`
- GPG-signature: [+] Valid
- SHA256: `b805cdc33a46ce035cbe758e05a8ac868036862012b7debe41c7377a15b99044`

Output:

```shell
[STDOUT]
  File: vUSB.img
  Size: 3221225472  Blocks: 6291464    IO Block: 4096   regular file
Device: 254,3   Inode: 3146325     Links: 1
Access: (0664/-rw-rw-r--)  Uid: ( 1000/  forick)   Gid: ( 1000/
forick)
Access: 2025-05-04 21:39:04.468824256 +0200
Modify: 2022-05-09 17:57:52.000000000 +0200
Change: 2025-05-04 21:36:05.775712707 +0200
 Birth: 2025-05-04 21:35:59.487683570 +0200

[STDERR]
```

Context:

Analyst: Markus Winklhofer
Timestamp: 2025-05-04T19:42:37.154709+00:00

[x] No specific explanation found.

[+] Command: `du -sh vUSB.img`

- Timestamp: `2025-05-04T19-42-44-193759+00-00`
- GPG-signature: [+] Valid
- SHA256: `0d228b622abd82c10e83d6c98003334db1525da41ea5ab1e7ab480f104066226`

Output:

```shell
[STDOUT]
3.1G    vUSB.img

[STDERR]
```

Context:

Analyst: Markus Winklhofer
Timestamp: 2025-05-04T19:42:44.339881+00:00

[x] No specific explanation found.

[+] Timestamp: `2025-05-04T19-44-08-064203+00-00`

[+] Comment from analyst: Markus Winklhofer

[+] Content:

Image ist 3.1GB groß

[+] Command: `mount: /home/forick/mnt/evidence: /home/forick/Desktop/DIF/Aufgaben/U4/vUSB.img is already mounted.`

- Timestamp: `2025-05-04T20-16-58-133190+00-00`
- GPG-signature: [+] Valid
- SHA256: `a6355b48267a03eba8a30570661ddd0df52521b570fff1fda2a028f385df76a5`

Output:

Shell

```
[!] Command failed:
mount: /home/forick/mnt/evidence:
/home/forick/Desktop/DIF/Aufgaben/U4/vUSB.img is already mounted.
```

Context:

Analyst: Markus Winklhofer
Timestamp: 2025-05-04T20:16:58.282721+00:00

[x] No specific explanation found.

[+] Command: `umount: /home/forick/mnt/evidence: target is busy.`

- Timestamp: `2025-05-04T20-18-22-680700+00-00`
- GPG-signature: [+] Valid
- SHA256: `2e06b49c6ef0f26d27d4deeb285cf2d2728d48fca869e93db7b716a380ba1470`

Output:

```shell
[!] Command failed:
umount: /home/forick/mnt/evidence: target is busy.
```

Context:

Analyst: Markus Winklhofer
Timestamp: 2025-05-04T20:18:22.832922+00:00

[x] No specific explanation found.

[+] Command: `sudo umount ~/mnt/evidence`

- Timestamp: `2025-05-04T20-18-30-808467+00-00`
- GPG-signature: [+] Valid
- SHA256: `aec4dbdae6db78716bf86b6c6d3a9f3327d00c39a9d0715fb7ff7b953c1c499f`

Output:

```shell
[STDOUT]

[STDERR]
```

Context:

Analyst: Markus Winklhofer
Timestamp: 2025-05-04T20:18:30.959767+00:00

[x] No specific explanation found.

[+] Timestamp: `2025-05-04T20-19-12-733468+00-00`

[+] Comment from analyst: Markus Winklhofer

[+] Content:

[+] Timestamp: `2025-05-04T20-19-50-713285+00-00`

[+] Comment from analyst: Markus Winklhofer

[+] Content:

Wenn Image gemountet wird, sind nur drei Bilder zu sehen. Statdessen wird ein virtual Device erstellt.

[+] Command: `fdisk -l vUSB.img`

- Timestamp: `2025-05-04T20-22-08-048592+00-00`
- GPG-signature: [+] Valid
- SHA256: `680da9bf4bf739f6123e19e17f59af0c7d6673d3587ff8f3d43fbb0471875c98`

Output:

Shell

```
[STDOUT]
Disk vUSB.img: 3 GiB, 3221225472 bytes, 6291456 sectors
Units: sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes
Disklabel type: dos
Disk identifier: 0x00000000

[STDERR]
```

Context:

Analyst: Markus Winklhofer
Timestamp: 2025-05-04T20:22:08.209658+00:00

[x] No specific explanation found.

[+] Command: `sudo losetup -fP vUSB.img`

- Timestamp: `2025-05-05T19-41-16-581160+00-00`
- GPG-signature: [+] Valid
- SHA256: `aec4dbdae6db78716bf86b6c6d3a9f3327d00c39a9d0715fb7ff7b953c1c499f`

Output:

```shell
[STDOUT]

[STDERR]
```

Context:

Analyst: Markus Winklhofer
Timestamp: 2025-05-05T19:41:18.565789+00:00

[x] No specific explanation found.

[+] Command: `sudo losetup -a`

- Timestamp: `2025-05-05T19-44-16-851861+00-00`
- GPG-signature: [+] Valid
- SHA256: `2f9729cd850118a9b1e48e7f782e9b98ac68af06e0c9dd365e1a1afc1005c486`

Output:

```shell
[STDOUT]
/dev/loop0: [65027]:3146325
(/home/forick/Desktop/DIF/Aufgaben/U4/vUSB.img)

[STDERR]
```

Context:

Analyst: Markus Winklhofer
Timestamp: 2025-05-05T19:44:17.016506+00:00

[x] No specific explanation found.

[+] Command: `sudo fdisk -l /dev/loop0`

- Timestamp: `2025-05-05T19-46-38-586341+00-00`
- GPG-signature: [+] Valid
- SHA256: `64001cc384704369cabcd7599b44dc117a801feefba09d333852b72e16d5ad53`

Output:

Shell

```
[STDOUT]
Disk /dev/loop0: 3 GiB, 3221225472 bytes, 6291456 sectors
Units: sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes
Disklabel type: dos
Disk identifier: 0x00000000

[STDERR]
```

Context:

Analyst: Markus Winklhofer
Timestamp: 2025-05-05T19:46:38.751851+00:00

[x] No specific explanation found.

[+] Command: `sudo dd if=/dev/loop0 of=usb_dd.img bs=4M conv=noerror,sync status=progress`

- Timestamp: `2025-05-07T11-14-19-699665+00-00`
- GPG-signature: [+] Valid
- SHA256: `3b30680df7e4a62152b8c332ccf48e44114812b382d83cb4c54ddd6d9161e4eb`

Output:

Shell

```
[STDOUT]

[STDERR]

473956352 bytes (474 MB, 452 MiB) copied, 1 s, 472 MB/s
977272832 bytes (977 MB, 932 MiB) copied, 2 s, 487 MB/s
1799356416 bytes (1.8 GB, 1.7 GiB) copied, 3 s, 599 MB/s
```

```
2663383040 bytes (2.7 GB, 2.5 GiB) copied, 4 s, 666 MB/s
768+0 records in
768+0 records out
3221225472 bytes (3.2 GB, 3.0 GiB) copied, 4.74357 s, 679 MB/s
```

Context:

Analyst: Markus Winklhofer
Timestamp: 2025-05-07T11:14:26.354296+00:00

[x] No specific explanation found.

[+] Command: `sudo: dc3dd: command not found`

- Timestamp: `2025-05-07T11-14-58-759504+00-00`
- GPG-signature: [+] Valid
- SHA256: `257141031ebe2c0b96cdfdf26d52a8d6a7aa43aac73c829f5115c7e536fc155c`

Output:

Shell

```
[!] Command failed:
sudo: dc3dd: command not found
```

Context:

Analyst: Markus Winklhofer
Timestamp: 2025-05-07T11:14:58.918539+00:00

[x] No specific explanation found.

[+] Command: `sudo dc3dd if=/dev/loop0 of=usb_dc3dd.img hash=sha256 log=dc3dd_log.txt`

- Timestamp: `2025-05-07T11-15-34-930965+00-00`
- GPG-signature: [+] Valid
- SHA256: `cb55295ff6f4e606a459657eceb0ee54c2953cfbddced8d6ec3670a737b5d676`

Output:

Shell

```
[STDOUT]

[STDERR]

dc3dd 7.2.646 started at 2025-05-07 13:15:35 +0200
compiled options:
command line dc3dd if=/dev/loop0 of=usb_dc3dd.img hash=sha256
log=dc3dd_log.txt
device size: 6291456 sectors (probed),    3,221,225,472 bytes
sector size: 512 bytes (probed)

    28442624 bytes ( 27 M ) copied (  1% ),    0 s, 270 M/s

    56590336 bytes ( 54 M ) copied (  2% ),    0 s, 269 M/s

    85360640 bytes ( 81 M ) copied (  3% ),    0 s, 271 M/s

   114393088 bytes ( 109 M ) copied (  4% ),    0 s, 272 M/s

   144375808 bytes ( 138 M ) copied (  4% ),    1 s, 275 M/s

   174489600 bytes ( 166 M ) copied (  5% ),    1 s, 277 M/s

   203948032 bytes ( 194 M ) copied (  6% ),    1 s, 277 M/s

   234160128 bytes ( 223 M ) copied (  7% ),    1 s, 279 M/s

   261521408 bytes ( 249 M ) copied (  8% ),    1 s, 277 M/s

   288587776 bytes ( 275 M ) copied (  9% ),    1 s, 275 M/s

   318767104 bytes ( 304 M ) copied ( 10% ),    1 s, 276 M/s

   348225536 bytes ( 332 M ) copied ( 11% ),    1 s, 276 M/s

   376668160 bytes ( 359 M ) copied ( 12% ),    1 s, 276 M/s

   403767296 bytes ( 385 M ) copied ( 13% ),    1 s, 274 M/s

   433651712 bytes ( 414 M ) copied ( 13% ),    2 s, 275 M/s

   464191488 bytes ( 443 M ) copied ( 14% ),    2 s, 276 M/s

   493486080 bytes ( 471 M ) copied ( 15% ),    2 s, 276 M/s

   524320768 bytes ( 500 M ) copied ( 16% ),    2 s, 277 M/s

   553975808 bytes ( 528 M ) copied ( 17% ),    2 s, 277 M/s

```

```
 583598080 bytes ( 557 M ) copied ( 18% ),    2 s, 278 M/s

 614563840 bytes ( 586 M ) copied ( 19% ),    2 s, 278 M/s

 642973696 bytes ( 613 M ) copied ( 20% ),    2 s, 278 M/s

 673742848 bytes ( 643 M ) copied ( 21% ),    2 s, 279 M/s

 701759488 bytes ( 669 M ) copied ( 22% ),    2 s, 278 M/s

 730005504 bytes ( 696 M ) copied ( 23% ),    3 s, 278 M/s

 761987072 bytes ( 727 M ) copied ( 24% ),    3 s, 279 M/s

 790560768 bytes ( 754 M ) copied ( 25% ),    3 s, 279 M/s

 818905088 bytes ( 781 M ) copied ( 25% ),    3 s, 278 M/s

 849543168 bytes ( 810 M ) copied ( 26% ),    3 s, 279 M/s

 878411776 bytes ( 838 M ) copied ( 27% ),    3 s, 279 M/s

 907345920 bytes ( 865 M ) copied ( 28% ),    3 s, 279 M/s

 937197568 bytes ( 894 M ) copied ( 29% ),    3 s, 279 M/s

 963248128 bytes ( 919 M ) copied ( 30% ),    3 s, 278 M/s

 994541568 bytes ( 948 M ) copied ( 31% ),    3 s, 278 M/s

1023311872 bytes ( 976 M ) copied ( 32% ),    4 s, 278 M/s

1051164672 bytes ( 1002 M ) copied ( 33% ),    4 s, 278 M/s

1081737216 bytes ( 1 G ) copied ( 34% ),    4 s, 278 M/s

1110966272 bytes ( 1 G ) copied ( 34% ),    4 s, 278 M/s

1139834880 bytes ( 1.1 G ) copied ( 35% ),    4 s, 278 M/s

1170341888 bytes ( 1.1 G ) copied ( 36% ),    4 s, 279 M/s

1198751744 bytes ( 1.1 G ) copied ( 37% ),    4 s, 278 M/s

1228406784 bytes ( 1.1 G ) copied ( 38% ),    4 s, 278 M/s

1258422272 bytes ( 1.2 G ) copied ( 39% ),    4 s, 279 M/s

1286176768 bytes ( 1.2 G ) copied ( 40% ),    4 s, 278 M/s

```

```
 99     1317076992 bytes ( 1.2 G ) copied ( 41% ),    5 s, 279 M/s
100
101     1345781760 bytes ( 1.3 G ) copied ( 42% ),    5 s, 279 M/s
102
103     1374486528 bytes ( 1.3 G ) copied ( 43% ),    5 s, 278 M/s
104
105     1404403712 bytes ( 1.3 G ) copied ( 44% ),    5 s, 279 M/s
106
107     1434681344 bytes ( 1.3 G ) copied ( 45% ),    5 s, 279 M/s
108
109     1463746560 bytes ( 1.4 G ) copied ( 45% ),    5 s, 279 M/s
110
111     1494155264 bytes ( 1.4 G ) copied ( 46% ),    5 s, 279 M/s
112
113     1521549312 bytes ( 1.4 G ) copied ( 47% ),    5 s, 279 M/s
114
115     1552220160 bytes ( 1.4 G ) copied ( 48% ),    5 s, 279 M/s
116
117     1581645824 bytes ( 1.5 G ) copied ( 49% ),    5 s, 279 M/s
118
119     1612513280 bytes ( 1.5 G ) copied ( 50% ),    6 s, 279 M/s
120
121     1642233856 bytes ( 1.5 G ) copied ( 51% ),    6 s, 279 M/s
122
123     1671266304 bytes ( 1.6 G ) copied ( 52% ),    6 s, 279 M/s
124
125     1689616384 bytes ( 1.6 G ) copied ( 52% ),    6 s, 277 M/s
126
127     1722253312 bytes ( 1.6 G ) copied ( 53% ),    6 s, 278 M/s
128
129     1750695936 bytes ( 1.6 G ) copied ( 54% ),    6 s, 278 M/s
130
131     1778319360 bytes ( 1.7 G ) copied ( 55% ),    6 s, 278 M/s
132
133     1808039936 bytes ( 1.7 G ) copied ( 56% ),    6 s, 278 M/s
134
135     1837531136 bytes ( 1.7 G ) copied ( 57% ),    6 s, 278 M/s
136
137     1866629120 bytes ( 1.7 G ) copied ( 58% ),    6 s, 278 M/s
138
139     1895104512 bytes ( 1.8 G ) copied ( 59% ),    7 s, 278 M/s
140
141     1922203648 bytes ( 1.8 G ) copied ( 60% ),    7 s, 277 M/s
142
143     1952088064 bytes ( 1.8 G ) copied ( 61% ),    7 s, 277 M/s
144
145     1981874176 bytes ( 1.8 G ) copied ( 62% ),    7 s, 278 M/s
146
147     2010349568 bytes ( 1.9 G ) copied ( 62% ),    7 s, 277 M/s
148
```

```
2040954880 bytes ( 1.9 G ) copied ( 63% ),    7 s, 278 M/s

2072510464 bytes ( 1.9 G ) copied ( 64% ),    7 s, 278 M/s

2099970048 bytes ( 2 G ) copied ( 65% ),    7 s, 278 M/s

2129526784 bytes ( 2 G ) copied ( 66% ),    7 s, 278 M/s

2157805568 bytes ( 2 G ) copied ( 67% ),    7 s, 278 M/s

2190573568 bytes ( 2 G ) copied ( 68% ),    8 s, 278 M/s

2221408256 bytes ( 2.1 G ) copied ( 69% ),    8 s, 278 M/s

2251423744 bytes ( 2.1 G ) copied ( 70% ),    8 s, 278 M/s

2279702528 bytes ( 2.1 G ) copied ( 71% ),    8 s, 278 M/s

2310438912 bytes ( 2.2 G ) copied ( 72% ),    8 s, 278 M/s

2338553856 bytes ( 2.2 G ) copied ( 73% ),    8 s, 278 M/s

2368438272 bytes ( 2.2 G ) copied ( 74% ),    8 s, 278 M/s

2397569024 bytes ( 2.2 G ) copied ( 74% ),    8 s, 278 M/s

2429059072 bytes ( 2.3 G ) copied ( 75% ),    8 s, 279 M/s

2458943488 bytes ( 2.3 G ) copied ( 76% ),    8 s, 279 M/s

2486992896 bytes ( 2.3 G ) copied ( 77% ),    9 s, 278 M/s

2520055808 bytes ( 2.3 G ) copied ( 78% ),    9 s, 279 M/s

2549448704 bytes ( 2.4 G ) copied ( 79% ),    9 s, 279 M/s

2578022400 bytes ( 2.4 G ) copied ( 80% ),    9 s, 279 M/s

2607972352 bytes ( 2.4 G ) copied ( 81% ),    9 s, 279 M/s

2634874880 bytes ( 2.5 G ) copied ( 82% ),    9 s, 279 M/s

2666528768 bytes ( 2.5 G ) copied ( 83% ),    9 s, 279 M/s

2697003008 bytes ( 2.5 G ) copied ( 84% ),    9 s, 279 M/s

2726363136 bytes ( 2.5 G ) copied ( 85% ),    9 s, 279 M/s

2755854336 bytes ( 2.6 G ) copied ( 86% ),    9 s, 279 M/s

```

```
  2784755712 bytes ( 2.6 G ) copied ( 86% ),   10 s, 279 M/s

  2813132800 bytes ( 2.6 G ) copied ( 87% ),   10 s, 279 M/s

  2844950528 bytes ( 2.6 G ) copied ( 88% ),   10 s, 279 M/s

  2872934400 bytes ( 2.7 G ) copied ( 89% ),   10 s, 279 M/s

  2902949888 bytes ( 2.7 G ) copied ( 90% ),   10 s, 279 M/s

  2932178944 bytes ( 2.7 G ) copied ( 91% ),   10 s, 279 M/s

  2959769600 bytes ( 2.8 G ) copied ( 92% ),   10 s, 279 M/s

  2989031424 bytes ( 2.8 G ) copied ( 93% ),   10 s, 279 M/s

  3017703424 bytes ( 2.8 G ) copied ( 94% ),   10 s, 279 M/s

  3046768640 bytes ( 2.8 G ) copied ( 95% ),   10 s, 279 M/s

  3075342336 bytes ( 2.9 G ) copied ( 95% ),   11 s, 279 M/s

  3104604160 bytes ( 2.9 G ) copied ( 96% ),   11 s, 279 M/s

  3135078400 bytes ( 2.9 G ) copied ( 97% ),   11 s, 279 M/s

  3166699520 bytes ( 2.9 G ) copied ( 98% ),   11 s, 279 M/s

  3195994112 bytes ( 3 G ) copied ( 99% ),   11 s, 279 M/s

  3221225472 bytes ( 3 G ) copied ( 100% ),   11 s, 279 M/s

  3221225472 bytes ( 3 G ) copied ( 100% ),   11 s, 279 M/s

input results for device `/dev/loop0':
   6291456 sectors in
   0 bad sectors replaced by zeros
   2c9c0f5117cdc3e8f3b9156bb5eef7d9563f46b4e0e4e51123711d828c89e8a2
(sha256)

output results for file `usb_dc3dd.img':
   6291456 sectors out

dc3dd completed at 2025-05-07 13:15:46 +0200
```

Context:

Analyst: Markus Winklhofer
Timestamp: 2025-05-07T11:15:46.118650+00:00

[x] No specific explanation found.

[+] Command: `sudo dcfldd if=/dev/loop0 of=usb_dcfldd.img hash=sha256 hashlog=dcfldd_hashes.txt`

- Timestamp: `2025-05-07T11-16-27-993126+00-00`
- GPG-signature: [+] Valid
- SHA256: `1374dd6d0390e65da9cf0fa2f36c796c948bb1784f9dd33b35ab5650db6f27f4`

Output:

Shell

```
[STDOUT]

[STDERR]

256 blocks (8Mb) written.
512 blocks (16Mb) written.
768 blocks (24Mb) written.
1024 blocks (32Mb) written.
1280 blocks (40Mb) written.
1536 blocks (48Mb) written.
1792 blocks (56Mb) written.
2048 blocks (64Mb) written.
2304 blocks (72Mb) written.
2560 blocks (80Mb) written.
2816 blocks (88Mb) written.
3072 blocks (96Mb) written.
3328 blocks (104Mb) written.
3584 blocks (112Mb) written.
3840 blocks (120Mb) written.
4096 blocks (128Mb) written.
4352 blocks (136Mb) written.
4608 blocks (144Mb) written.
4864 blocks (152Mb) written.
5120 blocks (160Mb) written.
5376 blocks (168Mb) written.
5632 blocks (176Mb) written.
5888 blocks (184Mb) written.
6144 blocks (192Mb) written.
6400 blocks (200Mb) written.
6656 blocks (208Mb) written.
6912 blocks (216Mb) written.
7168 blocks (224Mb) written.
7424 blocks (232Mb) written.
```

```
  7680 blocks (240Mb) written.
  7936 blocks (248Mb) written.
  8192 blocks (256Mb) written.
  8448 blocks (264Mb) written.
  8704 blocks (272Mb) written.
  8960 blocks (280Mb) written.
  9216 blocks (288Mb) written.
  9472 blocks (296Mb) written.
  9728 blocks (304Mb) written.
  9984 blocks (312Mb) written.
  10240 blocks (320Mb) written.
  10496 blocks (328Mb) written.
  10752 blocks (336Mb) written.
  11008 blocks (344Mb) written.
  11264 blocks (352Mb) written.
  11520 blocks (360Mb) written.
  11776 blocks (368Mb) written.
  12032 blocks (376Mb) written.
  12288 blocks (384Mb) written.
  12544 blocks (392Mb) written.
  12800 blocks (400Mb) written.
  13056 blocks (408Mb) written.
  13312 blocks (416Mb) written.
  13568 blocks (424Mb) written.
  13824 blocks (432Mb) written.
  14080 blocks (440Mb) written.
  14336 blocks (448Mb) written.
  14592 blocks (456Mb) written.
  14848 blocks (464Mb) written.
  15104 blocks (472Mb) written.
  15360 blocks (480Mb) written.
  15616 blocks (488Mb) written.
  15872 blocks (496Mb) written.
  16128 blocks (504Mb) written.
  16384 blocks (512Mb) written.
  16640 blocks (520Mb) written.
  16896 blocks (528Mb) written.
  17152 blocks (536Mb) written.
  17408 blocks (544Mb) written.
  17664 blocks (552Mb) written.
  17920 blocks (560Mb) written.
  18176 blocks (568Mb) written.
  18432 blocks (576Mb) written.
  18688 blocks (584Mb) written.
  18944 blocks (592Mb) written.
  19200 blocks (600Mb) written.
  19456 blocks (608Mb) written.
  19712 blocks (616Mb) written.
  19968 blocks (624Mb) written.
  20224 blocks (632Mb) written.
```

```
20480 blocks (640Mb) written.
20736 blocks (648Mb) written.
20992 blocks (656Mb) written.
21248 blocks (664Mb) written.
21504 blocks (672Mb) written.
21760 blocks (680Mb) written.
22016 blocks (688Mb) written.
22272 blocks (696Mb) written.
22528 blocks (704Mb) written.
22784 blocks (712Mb) written.
23040 blocks (720Mb) written.
23296 blocks (728Mb) written.
23552 blocks (736Mb) written.
23808 blocks (744Mb) written.
24064 blocks (752Mb) written.
24320 blocks (760Mb) written.
24576 blocks (768Mb) written.
24832 blocks (776Mb) written.
25088 blocks (784Mb) written.
25344 blocks (792Mb) written.
25600 blocks (800Mb) written.
25856 blocks (808Mb) written.
26112 blocks (816Mb) written.
26368 blocks (824Mb) written.
26624 blocks (832Mb) written.
26880 blocks (840Mb) written.
27136 blocks (848Mb) written.
27392 blocks (856Mb) written.
27648 blocks (864Mb) written.
27904 blocks (872Mb) written.
28160 blocks (880Mb) written.
28416 blocks (888Mb) written.
28672 blocks (896Mb) written.
28928 blocks (904Mb) written.
29184 blocks (912Mb) written.
29440 blocks (920Mb) written.
29696 blocks (928Mb) written.
29952 blocks (936Mb) written.
30208 blocks (944Mb) written.
30464 blocks (952Mb) written.
30720 blocks (960Mb) written.
30976 blocks (968Mb) written.
31232 blocks (976Mb) written.
31488 blocks (984Mb) written.
31744 blocks (992Mb) written.
32000 blocks (1000Mb) written.
32256 blocks (1008Mb) written.
32512 blocks (1016Mb) written.
32768 blocks (1024Mb) written.
33024 blocks (1032Mb) written.
```

```
  33280 blocks (1040Mb) written.
  33536 blocks (1048Mb) written.
  33792 blocks (1056Mb) written.
  34048 blocks (1064Mb) written.
  34304 blocks (1072Mb) written.
  34560 blocks (1080Mb) written.
  34816 blocks (1088Mb) written.
  35072 blocks (1096Mb) written.
  35328 blocks (1104Mb) written.
  35584 blocks (1112Mb) written.
  35840 blocks (1120Mb) written.
  36096 blocks (1128Mb) written.
  36352 blocks (1136Mb) written.
  36608 blocks (1144Mb) written.
  36864 blocks (1152Mb) written.
  37120 blocks (1160Mb) written.
  37376 blocks (1168Mb) written.
  37632 blocks (1176Mb) written.
  37888 blocks (1184Mb) written.
  38144 blocks (1192Mb) written.
  38400 blocks (1200Mb) written.
  38656 blocks (1208Mb) written.
  38912 blocks (1216Mb) written.
  39168 blocks (1224Mb) written.
  39424 blocks (1232Mb) written.
  39680 blocks (1240Mb) written.
  39936 blocks (1248Mb) written.
  40192 blocks (1256Mb) written.
  40448 blocks (1264Mb) written.
  40704 blocks (1272Mb) written.
  40960 blocks (1280Mb) written.
  41216 blocks (1288Mb) written.
  41472 blocks (1296Mb) written.
  41728 blocks (1304Mb) written.
  41984 blocks (1312Mb) written.
  42240 blocks (1320Mb) written.
  42496 blocks (1328Mb) written.
  42752 blocks (1336Mb) written.
  43008 blocks (1344Mb) written.
  43264 blocks (1352Mb) written.
  43520 blocks (1360Mb) written.
  43776 blocks (1368Mb) written.
  44032 blocks (1376Mb) written.
  44288 blocks (1384Mb) written.
  44544 blocks (1392Mb) written.
  44800 blocks (1400Mb) written.
  45056 blocks (1408Mb) written.
  45312 blocks (1416Mb) written.
  45568 blocks (1424Mb) written.
  45824 blocks (1432Mb) written.
```

```
  46080 blocks (1440Mb) written.
  46336 blocks (1448Mb) written.
  46592 blocks (1456Mb) written.
  46848 blocks (1464Mb) written.
  47104 blocks (1472Mb) written.
  47360 blocks (1480Mb) written.
  47616 blocks (1488Mb) written.
  47872 blocks (1496Mb) written.
  48128 blocks (1504Mb) written.
  48384 blocks (1512Mb) written.
  48640 blocks (1520Mb) written.
  48896 blocks (1528Mb) written.
  49152 blocks (1536Mb) written.
  49408 blocks (1544Mb) written.
  49664 blocks (1552Mb) written.
  49920 blocks (1560Mb) written.
  50176 blocks (1568Mb) written.
  50432 blocks (1576Mb) written.
  50688 blocks (1584Mb) written.
  50944 blocks (1592Mb) written.
  51200 blocks (1600Mb) written.
  51456 blocks (1608Mb) written.
  51712 blocks (1616Mb) written.
  51968 blocks (1624Mb) written.
  52224 blocks (1632Mb) written.
  52480 blocks (1640Mb) written.
  52736 blocks (1648Mb) written.
  52992 blocks (1656Mb) written.
  53248 blocks (1664Mb) written.
  53504 blocks (1672Mb) written.
  53760 blocks (1680Mb) written.
  54016 blocks (1688Mb) written.
  54272 blocks (1696Mb) written.
  54528 blocks (1704Mb) written.
  54784 blocks (1712Mb) written.
  55040 blocks (1720Mb) written.
  55296 blocks (1728Mb) written.
  55552 blocks (1736Mb) written.
  55808 blocks (1744Mb) written.
  56064 blocks (1752Mb) written.
  56320 blocks (1760Mb) written.
  56576 blocks (1768Mb) written.
  56832 blocks (1776Mb) written.
  57088 blocks (1784Mb) written.
  57344 blocks (1792Mb) written.
  57600 blocks (1800Mb) written.
  57856 blocks (1808Mb) written.
  58112 blocks (1816Mb) written.
  58368 blocks (1824Mb) written.
  58624 blocks (1832Mb) written.
```

```
  58880 blocks (1840Mb) written.
  59136 blocks (1848Mb) written.
  59392 blocks (1856Mb) written.
  59648 blocks (1864Mb) written.
  59904 blocks (1872Mb) written.
  60160 blocks (1880Mb) written.
  60416 blocks (1888Mb) written.
  60672 blocks (1896Mb) written.
  60928 blocks (1904Mb) written.
  61184 blocks (1912Mb) written.
  61440 blocks (1920Mb) written.
  61696 blocks (1928Mb) written.
  61952 blocks (1936Mb) written.
  62208 blocks (1944Mb) written.
  62464 blocks (1952Mb) written.
  62720 blocks (1960Mb) written.
  62976 blocks (1968Mb) written.
  63232 blocks (1976Mb) written.
  63488 blocks (1984Mb) written.
  63744 blocks (1992Mb) written.
  64000 blocks (2000Mb) written.
  64256 blocks (2008Mb) written.
  64512 blocks (2016Mb) written.
  64768 blocks (2024Mb) written.
  65024 blocks (2032Mb) written.
  65280 blocks (2040Mb) written.
  65536 blocks (2048Mb) written.
  65792 blocks (2056Mb) written.
  66048 blocks (2064Mb) written.
  66304 blocks (2072Mb) written.
  66560 blocks (2080Mb) written.
  66816 blocks (2088Mb) written.
  67072 blocks (2096Mb) written.
  67328 blocks (2104Mb) written.
  67584 blocks (2112Mb) written.
  67840 blocks (2120Mb) written.
  68096 blocks (2128Mb) written.
  68352 blocks (2136Mb) written.
  68608 blocks (2144Mb) written.
  68864 blocks (2152Mb) written.
  69120 blocks (2160Mb) written.
  69376 blocks (2168Mb) written.
  69632 blocks (2176Mb) written.
  69888 blocks (2184Mb) written.
  70144 blocks (2192Mb) written.
  70400 blocks (2200Mb) written.
  70656 blocks (2208Mb) written.
  70912 blocks (2216Mb) written.
  71168 blocks (2224Mb) written.
  71424 blocks (2232Mb) written.
```

```
  71680 blocks (2240Mb) written.
  71936 blocks (2248Mb) written.
  72192 blocks (2256Mb) written.
  72448 blocks (2264Mb) written.
  72704 blocks (2272Mb) written.
  72960 blocks (2280Mb) written.
  73216 blocks (2288Mb) written.
  73472 blocks (2296Mb) written.
  73728 blocks (2304Mb) written.
  73984 blocks (2312Mb) written.
  74240 blocks (2320Mb) written.
  74496 blocks (2328Mb) written.
  74752 blocks (2336Mb) written.
  75008 blocks (2344Mb) written.
  75264 blocks (2352Mb) written.
  75520 blocks (2360Mb) written.
  75776 blocks (2368Mb) written.
  76032 blocks (2376Mb) written.
  76288 blocks (2384Mb) written.
  76544 blocks (2392Mb) written.
  76800 blocks (2400Mb) written.
  77056 blocks (2408Mb) written.
  77312 blocks (2416Mb) written.
  77568 blocks (2424Mb) written.
  77824 blocks (2432Mb) written.
  78080 blocks (2440Mb) written.
  78336 blocks (2448Mb) written.
  78592 blocks (2456Mb) written.
  78848 blocks (2464Mb) written.
  79104 blocks (2472Mb) written.
  79360 blocks (2480Mb) written.
  79616 blocks (2488Mb) written.
  79872 blocks (2496Mb) written.
  80128 blocks (2504Mb) written.
  80384 blocks (2512Mb) written.
  80640 blocks (2520Mb) written.
  80896 blocks (2528Mb) written.
  81152 blocks (2536Mb) written.
  81408 blocks (2544Mb) written.
  81664 blocks (2552Mb) written.
  81920 blocks (2560Mb) written.
  82176 blocks (2568Mb) written.
  82432 blocks (2576Mb) written.
  82688 blocks (2584Mb) written.
  82944 blocks (2592Mb) written.
  83200 blocks (2600Mb) written.
  83456 blocks (2608Mb) written.
  83712 blocks (2616Mb) written.
  83968 blocks (2624Mb) written.
  84224 blocks (2632Mb) written.
```

```
  84480 blocks (2640Mb) written.
  84736 blocks (2648Mb) written.
  84992 blocks (2656Mb) written.
  85248 blocks (2664Mb) written.
  85504 blocks (2672Mb) written.
  85760 blocks (2680Mb) written.
  86016 blocks (2688Mb) written.
  86272 blocks (2696Mb) written.
  86528 blocks (2704Mb) written.
  86784 blocks (2712Mb) written.
  87040 blocks (2720Mb) written.
  87296 blocks (2728Mb) written.
  87552 blocks (2736Mb) written.
  87808 blocks (2744Mb) written.
  88064 blocks (2752Mb) written.
  88320 blocks (2760Mb) written.
  88576 blocks (2768Mb) written.
  88832 blocks (2776Mb) written.
  89088 blocks (2784Mb) written.
  89344 blocks (2792Mb) written.
  89600 blocks (2800Mb) written.
  89856 blocks (2808Mb) written.
  90112 blocks (2816Mb) written.
  90368 blocks (2824Mb) written.
  90624 blocks (2832Mb) written.
  90880 blocks (2840Mb) written.
  91136 blocks (2848Mb) written.
  91392 blocks (2856Mb) written.
  91648 blocks (2864Mb) written.
  91904 blocks (2872Mb) written.
  92160 blocks (2880Mb) written.
  92416 blocks (2888Mb) written.
  92672 blocks (2896Mb) written.
  92928 blocks (2904Mb) written.
  93184 blocks (2912Mb) written.
  93440 blocks (2920Mb) written.
  93696 blocks (2928Mb) written.
  93952 blocks (2936Mb) written.
  94208 blocks (2944Mb) written.
  94464 blocks (2952Mb) written.
  94720 blocks (2960Mb) written.
  94976 blocks (2968Mb) written.
  95232 blocks (2976Mb) written.
  95488 blocks (2984Mb) written.
  95744 blocks (2992Mb) written.
  96000 blocks (3000Mb) written.
  96256 blocks (3008Mb) written.
  96512 blocks (3016Mb) written.
  96768 blocks (3024Mb) written.
  97024 blocks (3032Mb) written.
```

```
384   97280 blocks (3040Mb) written.
385   97536 blocks (3048Mb) written.
386   97792 blocks (3056Mb) written.
387   98048 blocks (3064Mb) written.
388   98304 blocks (3072Mb) written.
389   98304+0 records in
390   98304+0 records out
```

Context:

Analyst: Markus Winklhofer
Timestamp: 2025-05-07T11:16:44.570319+00:00

[x] No specific explanation found.

[+] Command: `sudo mksquashfs usb_dd.img usb_dd_container.sqsh -noappend -comp xz`

- Timestamp: `2025-05-07T11-27-52-851087+00-00`
- GPG-signature: [+] Valid
- SHA256: `7e23ea8a518b663f9fab17861ee866c20ec10f1109837704b77d8b57e4f02ba2`

Output:

Shell

```
1   [STDOUT]
2   Parallel mksquashfs: Using 4 processors
3   Creating 4.0 filesystem on usb_dd_container.sqsh, block size 131072.
4
5   [============================================================/]
    24576/24576 100%
6
7   Exportable Squashfs 4.0 filesystem, xz compressed, data block size
    131072
8       compressed data, compressed metadata, compressed fragments,
9       compressed xattrs, compressed ids
10      duplicates are removed
11  Filesystem size 2300.38 Kbytes (2.25 Mbytes)
12      0.07% of uncompressed filesystem size (3145824.25 Kbytes)
13  Inode table size 1386 bytes (1.35 Kbytes)
14      1.41% of uncompressed inode table size (98394 bytes)
15  Directory table size 32 bytes (0.03 Kbytes)
16      100.00% of uncompressed directory table size (32 bytes)
17  Number of duplicate files found 0
18  Number of inodes 2
```

```
Number of files 1
Number of fragments 0
Number of symbolic links 0
Number of device nodes 0
Number of fifo nodes 0
Number of socket nodes 0
Number of directories 1
Number of hard-links 0
Number of ids (unique uids + gids) 1
Number of uids 1
    root (0)
Number of gids 1
    root (0)

[STDERR]
```

Context:

Analyst: Markus Winklhofer
Timestamp: 2025-05-07T11:27:56.331597+00:00

[x] No specific explanation found.

[+] Timestamp: `2025-05-07T11-31-38-594273+00-00`

[+] Comment from analyst: Markus Winklhofer

[+] Content:

Zu Aufgabe 2.3. Am besten wäre das Tool dcfldd, da dieses eine parallele Erstellung von Hashwerten während der Sicherung ermöglicht. Es ist speziell für die digitale Forensik ausgelegt und bietet sich so optimal an.

[+] Command: `fdisk -l usb_dd.img`

- Timestamp: `2025-05-07T13-18-32-957527+00-00`
- GPG-signature: [+] Valid
- SHA256: `2d5c86671e1427523fa54e7d41b6c99e007b3ee9d25db194ce5a3559f9b45b16`

Output:

Shell

```
[STDOUT]
Disk usb_dd.img: 3 GiB, 3221225472 bytes, 6291456 sectors
Units: sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes
Disklabel type: dos
Disk identifier: 0x00000000

[STDERR]
```

Context:

Analyst: Markus Winklhofer
Timestamp: 2025-05-07T13:18:33.108155+00:00

[x] No specific explanation found.

[+] Command: `sudo file -s /dev/loop0`

- Timestamp: `2025-05-07T13-25-09-964949+00-00`
- GPG-signature: [+] Valid
- SHA256: `c2744d25e209982b538cfe6902d3b94197c89f0815dbb2d68ee83eb0f382ec3c`

Output:

Shell

```
[STDOUT]
/dev/loop0: DOS/MBR boot sector, code offset 0x58+2, OEM-ID "mkfs.fat",
sectors/cluster 8, Media descriptor 0xf8, sectors/track 63, heads 255,
sectors 6291456 (volumes > 32 MB), FAT (32 bit), sectors/FAT 6136,
serial number 0x3700c1ae, unlabeled

[STDERR]
```

Context:

Analyst: Markus Winklhofer
Timestamp: 2025-05-07T13:25:11.947800+00:00

[x] No specific explanation found.

[+] Command: `sudo: fstat: command not found`

- Timestamp: `2025-05-07T13-26-06-683988+00-00`
- GPG-signature: [+] Valid
- SHA256: `ce488342cd482b5ed8c2f245caf8424222132748209229 2dddb97b490b1ed3e1`

Output:

```shell
[!] Command failed:
sudo: fstat: command not found
```

Context:

Analyst: Markus Winklhofer
Timestamp: 2025-05-07T13:26:06.837146+00:00

[x] No specific explanation found.

[+] Command: `sudo fsstat /dev/loop0`

- Timestamp: `2025-05-07T13-26-15-130476+00-00`
- GPG-signature: [+] Valid
- SHA256: `377bc3ffe4760f092973bb1a77d97c33b11307bb392768fdcc6dd1a63fe91332`

Output:

```shell
[STDOUT]
FILE SYSTEM INFORMATION
--------------------------------------------
File System Type: FAT32

OEM Name: mkfs.fat
Volume ID: 0x3700c1ae
Volume Label (Boot Sector): NO NAME
Volume Label (Root Directory):
File System Type Label: FAT32
Next Free Sector (FS Info): 16920
Free Sector Count (FS Info): 6274528

Sectors before file system: 0

File System Layout (in sectors)
Total Range: 0 - 6291455
```

```
* Reserved: 0 - 31
** Boot Sector: 0
** FS Info Sector: 1
** Backup Boot Sector: 6
* FAT 0: 32 - 6167
* FAT 1: 6168 - 12303
* Data Area: 12304 - 6291455
** Cluster Area: 12304 - 6291455
*** Root Directory: 12304 - 12311

METADATA INFORMATION
--------------------------------------------
Range: 2 - 100466438
Root Directory: 2

CONTENT INFORMATION
--------------------------------------------
Sector Size: 512
Cluster Size: 4096
Total Cluster Range: 2 - 784895

FAT CONTENTS (in sectors)
--------------------------------------------
12304-12311 (8) -> EOF
12312-12695 (384) -> EOF
12696-16895 (4200) -> EOF
16896-16927 (32) -> EOF

[STDERR]
```

Context:

Analyst: Markus Winklhofer
Timestamp: 2025-05-07T13:26:15.334583+00:00

[x] No specific explanation found.

[+] Timestamp: `2025-05-07T13-33-30-823688+00-00`

[+] Comment from analyst: Markus Winklhofer

[+] Content:

Dateisystem ist FAT32, dieses wird oft verwendet bei USB-Sticks/SD-Karten oder ähnlichen Datenträgern.

[+] Timestamp: `2025-05-07T13-35-25-978428+00-00`

[+] Comment from analyst: Markus Winklhofer

[+] Content:

Nun erneute Sicherung der vUSB.img Datei mittels dcfldd mit Hashwerten jeden 1M Chunk und SHA1 Alghorithmus.

[+] Command: ``

- Timestamp: `2025-05-07T13-42-08-455473+00-00`
- GPG-signature: [+] Valid
- SHA256: `a483c327cd24c752285cb9206f37f5ce23dd88d3bb2cd18023d60c4b8c43ea1b`

Output:

Shell

```
[!] Command failed:
dcfldd: unrecognized option progress=onTry `dcfldd --help' for more information.
```

Context:

Analyst: Markus Winklhofer
Timestamp: 2025-05-07T13:42:08.611667+00:00

[x] No specific explanation found.

[+] Command: `dcfldd:/dev/loop0: Permission denied`

- Timestamp: `2025-05-07T13-42-21-452184+00-00`
- GPG-signature: [+] Valid
- SHA256: `c81795248530cbfa686dff21906a57d4e7bd77d4434286692ac85ed4b7f1ce41`

Output:

Shell

```
[!] Command failed:
dcfldd:/dev/loop0: Permission denied
```

Context:

Analyst: Markus Winklhofer
Timestamp: 2025-05-07T13:42:21.601120+00:00

[x] No specific explanation found.

[+] Command: `sudo dcfldd if=/dev/loop0 of=usb_dcfldd_2.img hash=sha1 hashwindow=1M hashlog=hashes_usb_dcfldd.txt`

- Timestamp: `2025-05-07T13-42-36-126479+00-00`
- GPG-signature: [+] Valid
- SHA256: `1374dd6d0390e65da9cf0fa2f36c796c948bb1784f9dd33b35ab5650db6f27f4`

Output:

Shell

```
[STDOUT]

[STDERR]

256 blocks (8Mb) written.
512 blocks (16Mb) written.
768 blocks (24Mb) written.
1024 blocks (32Mb) written.
1280 blocks (40Mb) written.
1536 blocks (48Mb) written.
1792 blocks (56Mb) written.
2048 blocks (64Mb) written.
2304 blocks (72Mb) written.
2560 blocks (80Mb) written.
2816 blocks (88Mb) written.
3072 blocks (96Mb) written.
3328 blocks (104Mb) written.
3584 blocks (112Mb) written.
3840 blocks (120Mb) written.
4096 blocks (128Mb) written.
4352 blocks (136Mb) written.
4608 blocks (144Mb) written.
4864 blocks (152Mb) written.
5120 blocks (160Mb) written.
5376 blocks (168Mb) written.
5632 blocks (176Mb) written.
```

```
  5888 blocks (184Mb) written.
  6144 blocks (192Mb) written.
  6400 blocks (200Mb) written.
  6656 blocks (208Mb) written.
  6912 blocks (216Mb) written.
  7168 blocks (224Mb) written.
  7424 blocks (232Mb) written.
  7680 blocks (240Mb) written.
  7936 blocks (248Mb) written.
  8192 blocks (256Mb) written.
  8448 blocks (264Mb) written.
  8704 blocks (272Mb) written.
  8960 blocks (280Mb) written.
  9216 blocks (288Mb) written.
  9472 blocks (296Mb) written.
  9728 blocks (304Mb) written.
  9984 blocks (312Mb) written.
  10240 blocks (320Mb) written.
  10496 blocks (328Mb) written.
  10752 blocks (336Mb) written.
  11008 blocks (344Mb) written.
  11264 blocks (352Mb) written.
  11520 blocks (360Mb) written.
  11776 blocks (368Mb) written.
  12032 blocks (376Mb) written.
  12288 blocks (384Mb) written.
  12544 blocks (392Mb) written.
  12800 blocks (400Mb) written.
  13056 blocks (408Mb) written.
  13312 blocks (416Mb) written.
  13568 blocks (424Mb) written.
  13824 blocks (432Mb) written.
  14080 blocks (440Mb) written.
  14336 blocks (448Mb) written.
  14592 blocks (456Mb) written.
  14848 blocks (464Mb) written.
  15104 blocks (472Mb) written.
  15360 blocks (480Mb) written.
  15616 blocks (488Mb) written.
  15872 blocks (496Mb) written.
  16128 blocks (504Mb) written.
  16384 blocks (512Mb) written.
  16640 blocks (520Mb) written.
  16896 blocks (528Mb) written.
  17152 blocks (536Mb) written.
  17408 blocks (544Mb) written.
  17664 blocks (552Mb) written.
  17920 blocks (560Mb) written.
  18176 blocks (568Mb) written.
  18432 blocks (576Mb) written.
```

```
 18688 blocks (584Mb) written.
 18944 blocks (592Mb) written.
 19200 blocks (600Mb) written.
 19456 blocks (608Mb) written.
 19712 blocks (616Mb) written.
 19968 blocks (624Mb) written.
 20224 blocks (632Mb) written.
 20480 blocks (640Mb) written.
 20736 blocks (648Mb) written.
 20992 blocks (656Mb) written.
 21248 blocks (664Mb) written.
 21504 blocks (672Mb) written.
 21760 blocks (680Mb) written.
 22016 blocks (688Mb) written.
 22272 blocks (696Mb) written.
 22528 blocks (704Mb) written.
 22784 blocks (712Mb) written.
 23040 blocks (720Mb) written.
 23296 blocks (728Mb) written.
 23552 blocks (736Mb) written.
 23808 blocks (744Mb) written.
 24064 blocks (752Mb) written.
 24320 blocks (760Mb) written.
 24576 blocks (768Mb) written.
 24832 blocks (776Mb) written.
 25088 blocks (784Mb) written.
 25344 blocks (792Mb) written.
 25600 blocks (800Mb) written.
 25856 blocks (808Mb) written.
 26112 blocks (816Mb) written.
 26368 blocks (824Mb) written.
 26624 blocks (832Mb) written.
 26880 blocks (840Mb) written.
 27136 blocks (848Mb) written.
 27392 blocks (856Mb) written.
 27648 blocks (864Mb) written.
 27904 blocks (872Mb) written.
 28160 blocks (880Mb) written.
 28416 blocks (888Mb) written.
 28672 blocks (896Mb) written.
 28928 blocks (904Mb) written.
 29184 blocks (912Mb) written.
 29440 blocks (920Mb) written.
 29696 blocks (928Mb) written.
 29952 blocks (936Mb) written.
 30208 blocks (944Mb) written.
 30464 blocks (952Mb) written.
 30720 blocks (960Mb) written.
 30976 blocks (968Mb) written.
 31232 blocks (976Mb) written.
```

```
31488 blocks (984Mb) written.
31744 blocks (992Mb) written.
32000 blocks (1000Mb) written.
32256 blocks (1008Mb) written.
32512 blocks (1016Mb) written.
32768 blocks (1024Mb) written.
33024 blocks (1032Mb) written.
33280 blocks (1040Mb) written.
33536 blocks (1048Mb) written.
33792 blocks (1056Mb) written.
34048 blocks (1064Mb) written.
34304 blocks (1072Mb) written.
34560 blocks (1080Mb) written.
34816 blocks (1088Mb) written.
35072 blocks (1096Mb) written.
35328 blocks (1104Mb) written.
35584 blocks (1112Mb) written.
35840 blocks (1120Mb) written.
36096 blocks (1128Mb) written.
36352 blocks (1136Mb) written.
36608 blocks (1144Mb) written.
36864 blocks (1152Mb) written.
37120 blocks (1160Mb) written.
37376 blocks (1168Mb) written.
37632 blocks (1176Mb) written.
37888 blocks (1184Mb) written.
38144 blocks (1192Mb) written.
38400 blocks (1200Mb) written.
38656 blocks (1208Mb) written.
38912 blocks (1216Mb) written.
39168 blocks (1224Mb) written.
39424 blocks (1232Mb) written.
39680 blocks (1240Mb) written.
39936 blocks (1248Mb) written.
40192 blocks (1256Mb) written.
40448 blocks (1264Mb) written.
40704 blocks (1272Mb) written.
40960 blocks (1280Mb) written.
41216 blocks (1288Mb) written.
41472 blocks (1296Mb) written.
41728 blocks (1304Mb) written.
41984 blocks (1312Mb) written.
42240 blocks (1320Mb) written.
42496 blocks (1328Mb) written.
42752 blocks (1336Mb) written.
43008 blocks (1344Mb) written.
43264 blocks (1352Mb) written.
43520 blocks (1360Mb) written.
43776 blocks (1368Mb) written.
44032 blocks (1376Mb) written.
```

```
  44288 blocks (1384Mb) written.
  44544 blocks (1392Mb) written.
  44800 blocks (1400Mb) written.
  45056 blocks (1408Mb) written.
  45312 blocks (1416Mb) written.
  45568 blocks (1424Mb) written.
  45824 blocks (1432Mb) written.
  46080 blocks (1440Mb) written.
  46336 blocks (1448Mb) written.
  46592 blocks (1456Mb) written.
  46848 blocks (1464Mb) written.
  47104 blocks (1472Mb) written.
  47360 blocks (1480Mb) written.
  47616 blocks (1488Mb) written.
  47872 blocks (1496Mb) written.
  48128 blocks (1504Mb) written.
  48384 blocks (1512Mb) written.
  48640 blocks (1520Mb) written.
  48896 blocks (1528Mb) written.
  49152 blocks (1536Mb) written.
  49408 blocks (1544Mb) written.
  49664 blocks (1552Mb) written.
  49920 blocks (1560Mb) written.
  50176 blocks (1568Mb) written.
  50432 blocks (1576Mb) written.
  50688 blocks (1584Mb) written.
  50944 blocks (1592Mb) written.
  51200 blocks (1600Mb) written.
  51456 blocks (1608Mb) written.
  51712 blocks (1616Mb) written.
  51968 blocks (1624Mb) written.
  52224 blocks (1632Mb) written.
  52480 blocks (1640Mb) written.
  52736 blocks (1648Mb) written.
  52992 blocks (1656Mb) written.
  53248 blocks (1664Mb) written.
  53504 blocks (1672Mb) written.
  53760 blocks (1680Mb) written.
  54016 blocks (1688Mb) written.
  54272 blocks (1696Mb) written.
  54528 blocks (1704Mb) written.
  54784 blocks (1712Mb) written.
  55040 blocks (1720Mb) written.
  55296 blocks (1728Mb) written.
  55552 blocks (1736Mb) written.
  55808 blocks (1744Mb) written.
  56064 blocks (1752Mb) written.
  56320 blocks (1760Mb) written.
  56576 blocks (1768Mb) written.
  56832 blocks (1776Mb) written.
```

```
  57088 blocks (1784Mb) written.
  57344 blocks (1792Mb) written.
  57600 blocks (1800Mb) written.
  57856 blocks (1808Mb) written.
  58112 blocks (1816Mb) written.
  58368 blocks (1824Mb) written.
  58624 blocks (1832Mb) written.
  58880 blocks (1840Mb) written.
  59136 blocks (1848Mb) written.
  59392 blocks (1856Mb) written.
  59648 blocks (1864Mb) written.
  59904 blocks (1872Mb) written.
  60160 blocks (1880Mb) written.
  60416 blocks (1888Mb) written.
  60672 blocks (1896Mb) written.
  60928 blocks (1904Mb) written.
  61184 blocks (1912Mb) written.
  61440 blocks (1920Mb) written.
  61696 blocks (1928Mb) written.
  61952 blocks (1936Mb) written.
  62208 blocks (1944Mb) written.
  62464 blocks (1952Mb) written.
  62720 blocks (1960Mb) written.
  62976 blocks (1968Mb) written.
  63232 blocks (1976Mb) written.
  63488 blocks (1984Mb) written.
  63744 blocks (1992Mb) written.
  64000 blocks (2000Mb) written.
  64256 blocks (2008Mb) written.
  64512 blocks (2016Mb) written.
  64768 blocks (2024Mb) written.
  65024 blocks (2032Mb) written.
  65280 blocks (2040Mb) written.
  65536 blocks (2048Mb) written.
  65792 blocks (2056Mb) written.
  66048 blocks (2064Mb) written.
  66304 blocks (2072Mb) written.
  66560 blocks (2080Mb) written.
  66816 blocks (2088Mb) written.
  67072 blocks (2096Mb) written.
  67328 blocks (2104Mb) written.
  67584 blocks (2112Mb) written.
  67840 blocks (2120Mb) written.
  68096 blocks (2128Mb) written.
  68352 blocks (2136Mb) written.
  68608 blocks (2144Mb) written.
  68864 blocks (2152Mb) written.
  69120 blocks (2160Mb) written.
  69376 blocks (2168Mb) written.
  69632 blocks (2176Mb) written.
```

```
69888 blocks (2184Mb) written.
70144 blocks (2192Mb) written.
70400 blocks (2200Mb) written.
70656 blocks (2208Mb) written.
70912 blocks (2216Mb) written.
71168 blocks (2224Mb) written.
71424 blocks (2232Mb) written.
71680 blocks (2240Mb) written.
71936 blocks (2248Mb) written.
72192 blocks (2256Mb) written.
72448 blocks (2264Mb) written.
72704 blocks (2272Mb) written.
72960 blocks (2280Mb) written.
73216 blocks (2288Mb) written.
73472 blocks (2296Mb) written.
73728 blocks (2304Mb) written.
73984 blocks (2312Mb) written.
74240 blocks (2320Mb) written.
74496 blocks (2328Mb) written.
74752 blocks (2336Mb) written.
75008 blocks (2344Mb) written.
75264 blocks (2352Mb) written.
75520 blocks (2360Mb) written.
75776 blocks (2368Mb) written.
76032 blocks (2376Mb) written.
76288 blocks (2384Mb) written.
76544 blocks (2392Mb) written.
76800 blocks (2400Mb) written.
77056 blocks (2408Mb) written.
77312 blocks (2416Mb) written.
77568 blocks (2424Mb) written.
77824 blocks (2432Mb) written.
78080 blocks (2440Mb) written.
78336 blocks (2448Mb) written.
78592 blocks (2456Mb) written.
78848 blocks (2464Mb) written.
79104 blocks (2472Mb) written.
79360 blocks (2480Mb) written.
79616 blocks (2488Mb) written.
79872 blocks (2496Mb) written.
80128 blocks (2504Mb) written.
80384 blocks (2512Mb) written.
80640 blocks (2520Mb) written.
80896 blocks (2528Mb) written.
81152 blocks (2536Mb) written.
81408 blocks (2544Mb) written.
81664 blocks (2552Mb) written.
81920 blocks (2560Mb) written.
82176 blocks (2568Mb) written.
82432 blocks (2576Mb) written.
```

```
  82688 blocks (2584Mb) written.
  82944 blocks (2592Mb) written.
  83200 blocks (2600Mb) written.
  83456 blocks (2608Mb) written.
  83712 blocks (2616Mb) written.
  83968 blocks (2624Mb) written.
  84224 blocks (2632Mb) written.
  84480 blocks (2640Mb) written.
  84736 blocks (2648Mb) written.
  84992 blocks (2656Mb) written.
  85248 blocks (2664Mb) written.
  85504 blocks (2672Mb) written.
  85760 blocks (2680Mb) written.
  86016 blocks (2688Mb) written.
  86272 blocks (2696Mb) written.
  86528 blocks (2704Mb) written.
  86784 blocks (2712Mb) written.
  87040 blocks (2720Mb) written.
  87296 blocks (2728Mb) written.
  87552 blocks (2736Mb) written.
  87808 blocks (2744Mb) written.
  88064 blocks (2752Mb) written.
  88320 blocks (2760Mb) written.
  88576 blocks (2768Mb) written.
  88832 blocks (2776Mb) written.
  89088 blocks (2784Mb) written.
  89344 blocks (2792Mb) written.
  89600 blocks (2800Mb) written.
  89856 blocks (2808Mb) written.
  90112 blocks (2816Mb) written.
  90368 blocks (2824Mb) written.
  90624 blocks (2832Mb) written.
  90880 blocks (2840Mb) written.
  91136 blocks (2848Mb) written.
  91392 blocks (2856Mb) written.
  91648 blocks (2864Mb) written.
  91904 blocks (2872Mb) written.
  92160 blocks (2880Mb) written.
  92416 blocks (2888Mb) written.
  92672 blocks (2896Mb) written.
  92928 blocks (2904Mb) written.
  93184 blocks (2912Mb) written.
  93440 blocks (2920Mb) written.
  93696 blocks (2928Mb) written.
  93952 blocks (2936Mb) written.
  94208 blocks (2944Mb) written.
  94464 blocks (2952Mb) written.
  94720 blocks (2960Mb) written.
  94976 blocks (2968Mb) written.
  95232 blocks (2976Mb) written.
```

```
 95488 blocks (2984Mb) written.
 95744 blocks (2992Mb) written.
 96000 blocks (3000Mb) written.
 96256 blocks (3008Mb) written.
 96512 blocks (3016Mb) written.
 96768 blocks (3024Mb) written.
 97024 blocks (3032Mb) written.
 97280 blocks (3040Mb) written.
 97536 blocks (3048Mb) written.
 97792 blocks (3056Mb) written.
 98048 blocks (3064Mb) written.
 98304 blocks (3072Mb) written.
 98304+0 records in
 98304+0 records out
```

Context:

Analyst: Markus Winklhofer
Timestamp: 2025-05-07T13:43:06.450544+00:00

[x] No specific explanation found.

[+] Command: `ls`

- Timestamp: `2025-05-07T13-51-22-544555+00-00`
- GPG-signature: [+] Valid
- SHA256: `5e338c03513c205b84b57e33e36b81ad5de1b2ecd6505442fdf27f2552593a49`

Output:

Shell

```
[STDOUT]
dc3dd_log.txt
dcfldd_hashes.txt
hashes_usb_dcfldd.txt
usb_dc3dd.img
usb_dcfldd_2.img
usb_dcfldd.img
usb_dd_container.sqsh
usb_dd.img
vUSB.img
vUSB.zip

[STDERR]
```

Context:

Analyst: Markus Winklhofer
Timestamp: 2025-05-07T13:51:22.703075+00:00

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

[+] Command: `cat hashes_usb_dcfldd.txt`

- Timestamp: `2025-05-07T13-52-37-792981+00-00`
- GPG-signature: [+] Valid
- SHA256: `97f6f96e741357eba25a92c43f50d762c2d549eebc3e52434f09f83351a7e477`

Output:

Shell

```
[STDOUT]
0 - 1048576: a253aa45f32e482664f24084758393209cfe31fd
1048576 - 2097152: 3b71f43ff30f4b15b5cd85dd9e95ebc7e84eb5a3
2097152 - 3145728: 3b71f43ff30f4b15b5cd85dd9e95ebc7e84eb5a3
3145728 - 4194304: 302f8a09309ffe605c547e1a11a99018c635cd6e
...
3219128320 - 3220176896: 3b71f43ff30f4b15b5cd85dd9e95ebc7e84eb5a3
3220176896 - 3221225472: 3b71f43ff30f4b15b5cd85dd9e95ebc7e84eb5a3

Total (sha1): 1f5dd4cd5f9209f11bdaef31bd88d2c011244581

[STDERR]
```

Context:

Analyst: Markus Winklhofer
Timestamp: 2025-05-07T13:52:37.941195+00:00

[x] No specific explanation found.

[+] Command: `Error opening image file (raw_open: file "/dev/loop0" - Permission denied)`

- Timestamp: `2025-05-07T13-57-35-656056+00-00`
- GPG-signature: [+] Valid

- SHA256: `407e394195219f9b58cd231749b151d846ee45f8fcbe28187c285823f2058936`

Output:

```Shell
[!] Command failed:
Error opening image file (raw_open: file "/dev/loop0" - Permission denied)
```

Context:

Analyst: Markus Winklhofer
Timestamp: 2025-05-07T13:57:35.830256+00:00

[x] No specific explanation found.

[+] Command: `sudo fls -r -p -f fat /dev/loop0`

- Timestamp: `2025-05-07T13-57-45-107636+00-00`
- GPG-signature: [+] Valid
- SHA256: `0996062a042501ca75685983bcf354607efa0e572a2a39b211707f3736bb32b3`

Output:

```Shell
[STDOUT]
r/r 4:  Bild1.jpg
r/r 6:  Bild2.jpeg
r/r 8:  Blue.png
v/v 100466435:  $MBR
v/v 100466436:  $FAT1
v/v 100466437:  $FAT2
V/V 100466438:  $OrphanFiles

[STDERR]
```

Context:

Analyst: Markus Winklhofer
Timestamp: 2025-05-07T13:57:53.428896+00:00

[x] No specific explanation found.

[+] Timestamp: `2025-05-07T14-13-13-750620+00-00`

[+] Comment from analyst: Markus Winklhofer

[+] Content:

Drei Dateien auf dem Dateisystem hinterlegt. Nun extrahieren mit icat

---

[+] Command: `Invalid magic value (Not a FATFS file system (magic))`

- Timestamp: `2025-05-07T14-18-31-796087+00-00`
- GPG-signature: [+] Valid
- SHA256: `7c83cf10ad069a737a0219111616e0bba00b580b5b715a624145942aace36fb6`

Output:

```shell
[!] Command failed:
Invalid magic value (Not a FATFS file system (magic))
```

Context:

Analyst: Markus Winklhofer
Timestamp: 2025-05-07T14:18:31.965958+00:00

[x] No specific explanation found.

[+] Command: `sudo icat -f fat /dev/loop0 4 > Bild1_extr.jpg`

- Timestamp: `2025-05-07T14-24-18-329747+00-00`
- GPG-signature: [+] Valid
- SHA256: `aec4dbdae6db78716bf86b6c6d3a9f3327d00c39a9d0715fb7ff7b953c1c499f`

Output:

```shell
[STDOUT]

```

```
3  [STDERR]
```

Context:

Analyst: Markus Winklhofer
Timestamp: 2025-05-07T14:24:18.524139+00:00

[x] No specific explanation found.

[+] Command: `sudo icat -f fat /dev/loop0 6 > Bild1_extr.jpg`

- Timestamp: `2025-05-07T14-24-26-980018+00-00`
- GPG-signature: [+] Valid
- SHA256: `aec4dbdae6db78716bf86b6c6d3a9f3327d00c39a9d0715fb7ff7b953c1c499f`

Output:

Shell

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

Context:

Analyst: Markus Winklhofer
Timestamp: 2025-05-07T14:24:27.148421+00:00

[x] No specific explanation found.

[+] Command: `sudo icat -f fat /dev/loop0 6 > Bild2_extr.jpg`

- Timestamp: `2025-05-07T14-24-41-948872+00-00`
- GPG-signature: [+] Valid
- SHA256: `aec4dbdae6db78716bf86b6c6d3a9f3327d00c39a9d0715fb7ff7b953c1c499f`

Output:

Shell

```
[STDOUT]

[STDERR]
```

Context:

Analyst: Markus Winklhofer
Timestamp: 2025-05-07T14:24:42.111336+00:00

[x] No specific explanation found.

[+] Command: `sudo icat -f fat /dev/loop0 6 > Bild2_extr.jpeg`

- Timestamp: `2025-05-07T14-24-58-160563+00-00`
- GPG-signature: [+] Valid
- SHA256: `aec4dbdae6db78716bf86b6c6d3a9f3327d00c39a9d0715fb7ff7b953c1c499f`

Output:

Shell

```
[STDOUT]

[STDERR]
```

Context:

Analyst: Markus Winklhofer
Timestamp: 2025-05-07T14:24:58.319960+00:00

[x] No specific explanation found.

[+] Command: `sudo icat -f fat /dev/loop0 8 > blue_extr.png`

- Timestamp: `2025-05-07T14-25-37-843658+00-00`
- GPG-signature: [+] Valid
- SHA256: `aec4dbdae6db78716bf86b6c6d3a9f3327d00c39a9d0715fb7ff7b953c1c499f`

Output:

```
Shell
[STDOUT]

[STDERR]
```

Context:

Analyst: Markus Winklhofer
Timestamp: 2025-05-07T14:25:38.002383+00:00

[x] No specific explanation found.

[+] Command: `ls`

- Timestamp: `2025-05-07T14-25-50-994388+00-00`
- GPG-signature: [+] Valid
- SHA256: `7d94b1225b2b60c140c3ea0b1a770293128e234e01ef824ba06075a1cc8b5503`

Output:

```
Shell
[STDOUT]
Bild1_extr.jpg
Bild2_extr.jpeg
blue_extr.png
dc3dd_log.txt
dcfldd_hashes.txt
hashes_usb_dcfldd.txt
usb_dc3dd.img
usb_dcfldd_2.img
usb_dcfldd.img
usb_dd_container.sqsh
usb_dd.img
vUSB.img
vUSB.zip

[STDERR]
```

Context:

Analyst: Markus Winklhofer
Timestamp: 2025-05-07T14:25:51.140965+00:00

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

[+] Command: `sudo icat -f fat /dev/loop0 4 > Bild1_extr.jpg`

- Timestamp: `2025-05-07T14-28-00-726114+00-00`
- GPG-signature: [+] Valid
- SHA256: `aec4dbdae6db78716bf86b6c6d3a9f3327d00c39a9d0715fb7ff7b953c1c499f`

Output:

```shell
[STDOUT]

[STDERR]
```

Context:

Analyst: Markus Winklhofer
Timestamp: 2025-05-07T14:28:00.894601+00:00

[x] No specific explanation found.

[+] Command: `sha256sum Bild1_extr.jpg > extraction_hashes.txt`

- Timestamp: `2025-05-07T14-31-49-802270+00-00`
- GPG-signature: [+] Valid
- SHA256: `aec4dbdae6db78716bf86b6c6d3a9f3327d00c39a9d0715fb7ff7b953c1c499f`

Output:

```shell
[STDOUT]

[STDERR]
```

Context:

Analyst: Markus Winklhofer
Timestamp: 2025-05-07T14:31:49.973934+00:00

[x] No specific explanation found.

[+] Command: `sha256sum Bild2_extr.jpeg > extraction_hashes.txt`

- Timestamp: `2025-05-07T14-32-17-786561+00-00`
- GPG-signature: [+] Valid
- SHA256: `aec4dbdae6db78716bf86b6c6d3a9f3327d00c39a9d0715fb7ff7b953c1c499f`

Output:

```Shell
[STDOUT]

[STDERR]
```

Context:

Analyst: Markus Winklhofer
Timestamp: 2025-05-07T14:32:17.945147+00:00

[x] No specific explanation found.

[+] Command: `sha256sum Bild1_extr.jpg > extraction_hashes.txt`

- Timestamp: `2025-05-07T14-34-13-758067+00-00`
- GPG-signature: [+] Valid
- SHA256: `aec4dbdae6db78716bf86b6c6d3a9f3327d00c39a9d0715fb7ff7b953c1c499f`

Output:

```Shell
[STDOUT]

[STDERR]
```

Context:

Analyst: Markus Winklhofer
Timestamp: 2025-05-07T14:34:13.930916+00:00

[x] No specific explanation found.

[+] Command: `sha256sum Bild2_extr.jpeg > extraction_hashes.txt`

- Timestamp: `2025-05-07T14-38-18-768003+00-00`
- GPG-signature: [+] Valid
- SHA256: `aec4dbdae6db78716bf86b6c6d3a9f3327d00c39a9d0715fb7ff7b953c1c499f`

Output:

```shell
[STDOUT]

[STDERR]
```

Context:

Analyst: Markus Winklhofer
Timestamp: 2025-05-07T14:38:18.934267+00:00

[x] No specific explanation found.

[+] Command: `sha256sum blue_extr.png > extraction_hashes.txt`

- Timestamp: `2025-05-07T14-38-33-660223+00-00`
- GPG-signature: [+] Valid
- SHA256: `aec4dbdae6db78716bf86b6c6d3a9f3327d00c39a9d0715fb7ff7b953c1c499f`

Output:

```shell
[STDOUT]

[STDERR]
```

Context:

Analyst: Markus Winklhofer
Timestamp: 2025-05-07T14:38:33.812957+00:00

[x] No specific explanation found.

[+] Command: `sha256sum Bild1_extr.jpg >> extraction_hashes.txt`

- Timestamp: `2025-05-07T14-38-51-355821+00-00`
- GPG-signature: [+] Valid
- SHA256: `aec4dbdae6db78716bf86b6c6d3a9f3327d00c39a9d0715fb7ff7b953c1c499f`

Output:

```Shell
[STDOUT]

[STDERR]
```

Context:

Analyst: Markus Winklhofer
Timestamp: 2025-05-07T14:38:51.506103+00:00

[x] No specific explanation found.

[+] Command: `sha256sum Bild2_extr.jpeg >> extraction_hashes.txt`

- Timestamp: `2025-05-07T14-38-59-289718+00-00`
- GPG-signature: [+] Valid
- SHA256: `aec4dbdae6db78716bf86b6c6d3a9f3327d00c39a9d0715fb7ff7b953c1c499f`

Output:

```Shell
[STDOUT]

```

```
3  [STDERR]
```

Context:

Analyst: Markus Winklhofer
Timestamp: 2025-05-07T14:38:59.439431+00:00

[x] No specific explanation found.

[+] Command: `sha256sum blue_extr.png >> extraction_hashes.txt`

- Timestamp: `2025-05-07T14-39-05-922173+00-00`
- GPG-signature: [+] Valid
- SHA256: `aec4dbdae6db78716bf86b6c6d3a9f3327d00c39a9d0715fb7ff7b953c1c499f`

Output:

Shell

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

Context:

Analyst: Markus Winklhofer
Timestamp: 2025-05-07T14:39:06.071652+00:00

[x] No specific explanation found.

[+] Command: `sudo istat -f fat /dev/loop0 4`

- Timestamp: `2025-05-07T14-40-52-882602+00-00`
- GPG-signature: [+] Valid
- SHA256: `c7040961be05a1900cdff509043022dc485ac3cd2f5a765fe26ad05b6797dd5c`

Output:

Shell

```
1  [STDOUT]
```

```
Directory Entry: 4
Allocated
File Attributes: File, Archive
Size: 192827
Name: BILD1.JPG

Directory Entry Times:
Written:    2022-05-09 15:22:28 (CEST)
Accessed:   2022-05-09 00:00:00 (CEST)
Created:    2022-05-09 15:22:29 (CEST)

Sectors:
12312 12313 12314 12315 12316 12317 12318 12319
12320 12321 12322 12323 12324 12325 12326 12327
12328 12329 12330 12331 12332 12333 12334 12335
12336 12337 12338 12339 12340 12341 12342 12343
12344 12345 12346 12347 12348 12349 12350 12351
12352 12353 12354 12355 12356 12357 12358 12359
12360 12361 12362 12363 12364 12365 12366 12367
12368 12369 12370 12371 12372 12373 12374 12375
12376 12377 12378 12379 12380 12381 12382 12383
12384 12385 12386 12387 12388 12389 12390 12391
12392 12393 12394 12395 12396 12397 12398 12399
12400 12401 12402 12403 12404 12405 12406 12407
12408 12409 12410 12411 12412 12413 12414 12415
12416 12417 12418 12419 12420 12421 12422 12423
12424 12425 12426 12427 12428 12429 12430 12431
12432 12433 12434 12435 12436 12437 12438 12439
12440 12441 12442 12443 12444 12445 12446 12447
12448 12449 12450 12451 12452 12453 12454 12455
12456 12457 12458 12459 12460 12461 12462 12463
12464 12465 12466 12467 12468 12469 12470 12471
12472 12473 12474 12475 12476 12477 12478 12479
12480 12481 12482 12483 12484 12485 12486 12487
12488 12489 12490 12491 12492 12493 12494 12495
12496 12497 12498 12499 12500 12501 12502 12503
12504 12505 12506 12507 12508 12509 12510 12511
12512 12513 12514 12515 12516 12517 12518 12519
12520 12521 12522 12523 12524 12525 12526 12527
12528 12529 12530 12531 12532 12533 12534 12535
12536 12537 12538 12539 12540 12541 12542 12543
12544 12545 12546 12547 12548 12549 12550 12551
12552 12553 12554 12555 12556 12557 12558 12559
12560 12561 12562 12563 12564 12565 12566 12567
12568 12569 12570 12571 12572 12573 12574 12575
12576 12577 12578 12579 12580 12581 12582 12583
12584 12585 12586 12587 12588 12589 12590 12591
12592 12593 12594 12595 12596 12597 12598 12599
12600 12601 12602 12603 12604 12605 12606 12607
12608 12609 12610 12611 12612 12613 12614 12615
```

```
12616 12617 12618 12619 12620 12621 12622 12623
12624 12625 12626 12627 12628 12629 12630 12631
12632 12633 12634 12635 12636 12637 12638 12639
12640 12641 12642 12643 12644 12645 12646 12647
12648 12649 12650 12651 12652 12653 12654 12655
12656 12657 12658 12659 12660 12661 12662 12663
12664 12665 12666 12667 12668 12669 12670 12671
12672 12673 12674 12675 12676 12677 12678 12679
12680 12681 12682 12683 12684 12685 12686 12687
12688 0 0 0 0 0 0 0

[STDERR]
```

Context:

Analyst: Markus Winklhofer
Timestamp: 2025-05-07T14:40:53.053441+00:00

[x] No specific explanation found.

[+] Command: `sudo istat -f fat /dev/loop0 6`

- Timestamp: `2025-05-07T14-41-27-760152+00-00`
- GPG-signature: [+] Valid
- SHA256: `da52b421630b861f3c63ae7cea5068eedade839e64a991bbb9a8a39229cbe924`

Output:

Shell

```
[STDOUT]
Directory Entry: 6
Allocated
File Attributes: File, Archive
Size: 2148214
Name: BILD2~1.JPE

Directory Entry Times:
Written:    2022-05-09 15:22:40 (CEST)
Accessed:   2022-05-09 00:00:00 (CEST)
Created:    2022-05-09 15:22:41 (CEST)

Sectors:
12696 12697 12698 12699 12700 12701 12702 12703
12704 12705 12706 12707 12708 12709 12710 12711
12712 12713 12714 12715 12716 12717 12718 12719
```

```
12720 12721 12722 12723 12724 12725 12726 12727
12728 12729 12730 12731 12732 12733 12734 12735
...
16864 16865 16866 16867 16868 16869 16870 16871
16872 16873 16874 16875 16876 16877 16878 16879
16880 16881 16882 16883 16884 16885 16886 16887
16888 16889 16890 16891 0 0 0 0

[STDERR]
```

Context:

Analyst: Markus Winklhofer
Timestamp: 2025-05-07T14:41:27.921673+00:00

[x] No specific explanation found.

[+] Command: `sudo istat -f fat /dev/loop0 8`

- Timestamp: `2025-05-07T14-43-01-005589+00-00`
- GPG-signature: [+] Valid
- SHA256: `84519aec0b31b0079085a8099047530dbfcb1f6be5c4f6f55ec219013d254a92`

Output:

Shell

```
[STDOUT]
Directory Entry: 8
Allocated
File Attributes: File, Archive
Size: 15540
Name: BLUE.PNG

Directory Entry Times:
Written:    2022-05-09 15:52:12 (CEST)
Accessed:   2022-05-09 00:00:00 (CEST)
Created:    2022-05-09 15:52:13 (CEST)

Sectors:
16896 16897 16898 16899 16900 16901 16902 16903
16904 16905 16906 16907 16908 16909 16910 16911
16912 16913 16914 16915 16916 16917 16918 16919
16920 16921 16922 16923 16924 16925 16926 0

[STDERR]
```

Context:

Analyst: Markus Winklhofer
Timestamp: 2025-05-07T14:43:01.162098+00:00

[x] No specific explanation found.

[+] Timestamp: `2025-05-07T14-46-30-814507+00-00`

[+] Comment from analyst: Markus Winklhofer

[+] Content:

Analyse der gefundenen Dateien: Visuell betrachtet sind auf zwei Bildern jeweils ein Greifvogel zu sehen. Da letzte bild blue.png ist nur ein Bild mit der Farbe Blau. Anlschießend werden die Dateien noch genauer analysiert, um zu prüfen, ob die Daten noch weitere Infos enthalten.

[+] Timestamp: `2025-05-07T15-20-24-100735+00-00`

[+] Comment from analyst: Markus Winklhofer

[+] Content:

Analyse der Datei Bild1_extr.jpg

[+] Command: `exiftool Bild1_extr.jpg`

- Timestamp: `2025-05-07T15-20-45-395031+00-00`
- GPG-signature: [+] Valid
- SHA256: `8390dff1d5d5a7e94f0fe4d5d786cc743853bb6c6c5f73e2f9a2a92bb879fe72`

Output:

Shell

```
[STDOUT]
ExifTool Version Number         : 13.10
File Name                       : Bild1_extr.jpg
Directory                       : .
```

```
File Size                       : 193 kB
File Modification Date/Time     : 2025:05:07 16:28:00+02:00
File Access Date/Time           : 2025:05:07 16:28:07+02:00
File Inode Change Date/Time     : 2025:05:07 16:28:00+02:00
File Permissions                : -rw-rw-r--
File Type                       : JPEG
File Type Extension             : jpg
MIME Type                       : image/jpeg
JFIF Version                    : 1.02
Resolution Unit                 : None
X Resolution                    : 1
Y Resolution                    : 1
Image Width                     : 1536
Image Height                    : 1152
Encoding Process                : Baseline DCT, Huffman coding
Bits Per Sample                 : 8
Color Components                : 3
Y Cb Cr Sub Sampling            : YCbCr4:2:0 (2 2)
Image Size                      : 1536x1152
Megapixels                      : 1.8

[STDERR]
```

Context:

Analyst: Markus Winklhofer
Timestamp: 2025-05-07T15:20:45.604985+00:00

[x] No specific explanation found.

[+] Command: `file Bild1_extr.jpg`

- Timestamp: `2025-05-07T15-21-26-661321+00-00`
- GPG-signature: [+] Valid
- SHA256: `b9c5f6d025487efba2f6fec70c54b026f630b231d96ae509138e26b4872168ab`

Output:

Shell

```
[STDOUT]
Bild1_extr.jpg: JPEG image data, JFIF standard 1.02, aspect ratio,
density 1x1, segment length 16, baseline, precision 8, 1536x1152,
components 3

[STDERR]
```

Context:

Analyst: Markus Winklhofer
Timestamp: 2025-05-07T15:21:26.815132+00:00

[x] No specific explanation found.

[+] Timestamp: `2025-05-07T15-23-06-299926+00-00`

[+] Comment from analyst: Markus Winklhofer

[+] Content:

Analyse der Datei Bild2_extr.jpeg

[+] Command: `exiftool Bild2_extr.jpeg`

- Timestamp: `2025-05-07T15-23-16-395050+00-00`
- GPG-signature: [+] Valid
- SHA256: `0e7e96be61ab897d545d541c773d0b6df23d82cc79cd22341c0d5900b7fc7ad9`

Output:

Shell

```
[STDOUT]
ExifTool Version Number         : 13.10
File Name                       : Bild2_extr.jpeg
Directory                       : .
File Size                       : 2.1 MB
File Modification Date/Time     : 2025:05:07 16:24:58+02:00
File Access Date/Time           : 2025:05:07 16:27:03+02:00
File Inode Change Date/Time     : 2025:05:07 16:24:58+02:00
File Permissions                : -rw-rw-r--
File Type                       : JPEG
File Type Extension             : jpg
MIME Type                       : image/jpeg
JFIF Version                    : 1.01
Resolution Unit                 : None
X Resolution                    : 1
Y Resolution                    : 1
Image Width                     : 1600
Image Height                    : 1600
```

```
Encoding Process                : Baseline DCT, Huffman coding
Bits Per Sample                 : 8
Color Components                : 3
Y Cb Cr Sub Sampling            : YCbCr4:4:4 (1 1)
Image Size                      : 1600x1600
Megapixels                      : 2.6

[STDERR]
```

Context:

Analyst: Markus Winklhofer
Timestamp: 2025-05-07T15:23:16.603158+00:00

[x] No specific explanation found.

[+] Command: `file Bild2_extr.jpeg`

- Timestamp: `2025-05-07T15-23-25-801900+00-00`
- GPG-signature: [+] Valid
- SHA256: `6a4123e57d1598a6253e7e472c55e8d4ba2a5a2d0159a71f71f331029739630a`

Output:

Shell

```
[STDOUT]
Bild2_extr.jpeg: JPEG image data, JFIF standard 1.01, aspect ratio, density 1x1, segment length 16, baseline, precision 8, 1600x1600, components 3

[STDERR]
```

Context:

Analyst: Markus Winklhofer
Timestamp: 2025-05-07T15:23:25.957644+00:00

[x] No specific explanation found.

[+] Timestamp: `2025-05-07T15-23-37-964366+00-00`

[+] Comment from analyst: Markus Winklhofer

[+] Content:

Analyse der Datei blue_extr.png

[+] Command: `exiftool blue_extr.png`

- Timestamp: `2025-05-07T15-23-55-283264+00-00`
- GPG-signature: [+] Valid
- SHA256: `e88864e7aa06774c5dfbb6e8482514b4d52250198fe443a62b14b8daf73341ee`

Output:

Shell

```
[STDOUT]
ExifTool Version Number         : 13.10
File Name                       : blue_extr.png
Directory                       : .
File Size                       : 16 kB
File Modification Date/Time     : 2025:05:07 16:25:37+02:00
File Access Date/Time           : 2025:05:07 16:27:03+02:00
File Inode Change Date/Time     : 2025:05:07 16:25:37+02:00
File Permissions                : -rw-rw-r--
File Type                       : PNG
File Type Extension             : png
MIME Type                       : image/png
Image Width                     : 1920
Image Height                    : 1080
Bit Depth                       : 8
Color Type                      : RGB
Compression                     : Deflate/Inflate
Filter                          : Adaptive
Interlace                       : Noninterlaced
Profile Name                    : ICC profile
Profile CMM Type                : Little CMS
Profile Version                 : 4.3.0
Profile Class                   : Display Device Profile
Color Space Data                : RGB
Profile Connection Space        : XYZ
Profile Date Time               : 2022:05:09 15:23:12
Profile File Signature          : acsp
Primary Platform                : Apple Computer Inc.
CMM Flags                       : Not Embedded, Independent
Device Manufacturer             :
Device Model                    :
Device Attributes               : Reflective, Glossy, Positive, Color
```

```
Rendering Intent                : Perceptual
Connection Space Illuminant     : 0.9642 1 0.82491
Profile Creator                 : Little CMS
Profile ID                      : 0
Profile Description             : GIMP built-in sRGB
Profile Copyright               : Public Domain
Media White Point               : 0.9642 1 0.82491
Chromatic Adaptation            : 1.04788 0.02292 -0.05022 0.02959
0.99048 -0.01707 -0.00925 0.01508 0.75168
Red Matrix Column               : 0.43604 0.22249 0.01392
Blue Matrix Column              : 0.14305 0.06061 0.71393
Green Matrix Column             : 0.38512 0.7169 0.09706
Red Tone Reproduction Curve     : (Binary data 32 bytes, use -b option
to extract)
Green Tone Reproduction Curve   : (Binary data 32 bytes, use -b option
to extract)
Blue Tone Reproduction Curve    : (Binary data 32 bytes, use -b option
to extract)
Chromaticity Channels           : 3
Chromaticity Colorant           : Unknown
Chromaticity Channel 1          : 0.64 0.33002
Chromaticity Channel 2          : 0.3 0.60001
Chromaticity Channel 3          : 0.15001 0.06
Device Mfg Desc                 : GIMP
Device Model Desc               : sRGB
Pixels Per Unit X               : 11811
Pixels Per Unit Y               : 11811
Pixel Units                     : meters
Modify Date                     : 2022:05:09 15:35:58
Comment                         : Created with GIMP
Image Size                      : 1920x1080
Megapixels                      : 2.1

[STDERR]
```

Context:

Analyst: Markus Winklhofer
Timestamp: 2025-05-07T15:23:55.515586+00:00

[x] No specific explanation found.

[+] Command: `file blue_extr.png`

- Timestamp: `2025-05-07T15-24-17-513631+00-00`
- GPG-signature: [+] Valid

- SHA256: `833b057483c3874807065dd25df8e6287e92dfecbd352ff1494e3cedadba43ef`

Output:

```shell
[STDOUT]
blue_extr.png: PNG image data, 1920 x 1080, 8-bit/color RGB, non-interlaced

[STDERR]
```

Context:

Analyst: Markus Winklhofer
Timestamp: 2025-05-07T15:24:17.664365+00:00

[x] No specific explanation found.

[+] Timestamp: `2025-05-07T15-32-17-211922+00-00`

[+] Comment from analyst: Markus Winklhofer

[+] Content:

Datei blue_extr.png enthält keine ungewöhnlichen Daten. Das Bild wurde in GIMP erstellt mit einer typischen Bildschirmauflösung. Die letzte Änderung hierbei war am 2022-05-09 um 15:35:58.

[+] Timestamp: `2025-05-07T15-37-03-863609+00-00`

[+] Comment from analyst: Markus Winklhofer

[+] Content:

Vergleich der Dateien mit den Dateien aus den Squash Containern.

[+] Command: `unsquash: command not found`

- Timestamp: `2025-05-07T15-37-32-283104+00-00`

- GPG-signature: [+] Valid
- SHA256: `79b6c1b50fb4a29710c687deda72a4e489b3a674e4e1ca15d0f7c4bb6ada19cc`

Output:

```shell
[!] Command failed:
unsquash: command not found
```

Context:

Analyst: Markus Winklhofer
Timestamp: 2025-05-07T15:37:32.501901+00:00

[x] No specific explanation found.

[+] Command: `unsquashfs -ll usb_dd_container.sqsh`

- Timestamp: `2025-05-07T15-37-45-307661+00-00`
- GPG-signature: [+] Valid
- SHA256: `df85b39445b3e2dc97bb63553045ef95bca9a1a02af466aaa44daaf72523156d`

Output:

```shell
[STDOUT]
drwxrwxrwx root/root               33 2025-05-07 13:27 squashfs-root
-rw-r--r-- root/root       3221225472 2025-05-07 13:14 squashfs-
root/usb_dd.img

[STDERR]
```

Context:

Analyst: Markus Winklhofer
Timestamp: 2025-05-07T15:37:45.457445+00:00

[x] No specific explanation found.

[+] Command: `unsquashfs usb_dd_container.sqsh`

- Timestamp: `2025-05-07T15-39-09-782171+00-00`
- GPG-signature: [+] Valid
- SHA256: `72f22ad69bc2d5d07d3c9f0b37db1da991fdd7f9742c3fe55766da4319aa99da`

Output:

Shell

```
[STDOUT]
Parallel unsquashfs: Using 4 processors
1 inodes (24576 blocks) to write


[=============================================================/]
24577/24577 100%
[=============================================================/]
24577/24577 100%
[=============================================================\]
24577/24577 100%
[=============================================================|]
24577/24577 100%
[=============================================================/]
24577/24577 100%
[=============================================================-]
24577/24577 100%
[=============================================================\]
24577/24577 100%
[=============================================================|]
24577/24577 100%
[=============================================================/]
24577/24577 100%
[=============================================================-]
24577/24577 100%
[=============================================================\]
24577/24577 100%
[=============================================================\]
24577/24577 100%

created 1 file
created 1 directory
created 0 symlinks
created 0 devices
created 0 fifos
created 0 sockets
created 0 hardlinks

[STDERR]
```

Context:

Analyst: Markus Winklhofer
Timestamp: 2025-05-07T15:39:12.748031+00:00

[x] No specific explanation found.

[+] Command: `sudo losetup -fP squashfs-root/usb_dd.img`

- Timestamp: `2025-05-07T15-44-03-668653+00-00`
- GPG-signature: [+] Valid
- SHA256: `aec4dbdae6db78716bf86b6c6d3a9f3327d00c39a9d0715fb7ff7b953c1c499f`

Output:

```shell
[STDOUT]

[STDERR]
```

Context:

Analyst: Markus Winklhofer
Timestamp: 2025-05-07T15:44:05.711647+00:00

[x] No specific explanation found.

[+] Command: `sudo losetup -a`

- Timestamp: `2025-05-07T15-48-03-991868+00-00`
- GPG-signature: [+] Valid
- SHA256: `ccc4b7680827bb89d884ee0f50bfef638354a6cf70ef6101c1df4e57c1084aca`

Output:

```shell
[STDOUT]
/dev/loop1: [65027]:3407874 (/home/forick/Desktop/DIF/Aufgaben/U4/squashfs-root/usb_dd.img)
/dev/loop0: [65027]:3146325 (/home/forick/Desktop/DIF/Aufgaben/U4/vUSB.img)
```

```
4
5   [STDERR]
```

Context:

Analyst: Markus Winklhofer
Timestamp: 2025-05-07T15:48:04.160431+00:00

[x] No specific explanation found.

[+] Command: `sudo fls -r -p -f fat /dev/loop1`

- Timestamp: `2025-05-07T15-51-16-528696+00-00`
- GPG-signature: [+] Valid
- SHA256: `0996062a042501ca75685983bcf354607efa0e572a2a39b211707f3736bb32b3`

Output:

Shell

```
1   [STDOUT]
2   r/r 4:  Bild1.jpg
3   r/r 6:  Bild2.jpeg
4   r/r 8:  Blue.png
5   v/v 100466435:  $MBR
6   v/v 100466436:  $FAT1
7   v/v 100466437:  $FAT2
8   V/V 100466438:  $OrphanFiles
9
10  [STDERR]
```

Context:

Analyst: Markus Winklhofer
Timestamp: 2025-05-07T15:51:22.978440+00:00

[x] No specific explanation found.

[+] Command: `sudo istat -f fat /dev/loop1 4`

- Timestamp: `2025-05-07T15-57-15-647107+00-00`
- GPG-signature: [+] Valid

- SHA256: `c7040961be05a1900cdff509043022dc485ac3cd2f5a765fe26ad05b6797dd5c`

Output:

Shell

```
[STDOUT]
Directory Entry: 4
Allocated
File Attributes: File, Archive
Size: 192827
Name: BILD1.JPG

Directory Entry Times:
Written:    2022-05-09 15:22:28 (CEST)
Accessed:   2022-05-09 00:00:00 (CEST)
Created:    2022-05-09 15:22:29 (CEST)

Sectors:
12312 12313 12314 12315 12316 12317 12318 12319
12320 12321 12322 12323 12324 12325 12326 12327
12328 12329 12330 12331 12332 12333 12334 12335
12336 12337 12338 12339 12340 12341 12342 12343
12344 12345 12346 12347 12348 12349 12350 12351
12352 12353 12354 12355 12356 12357 12358 12359
12360 12361 12362 12363 12364 12365 12366 12367
12368 12369 12370 12371 12372 12373 12374 12375
12376 12377 12378 12379 12380 12381 12382 12383
12384 12385 12386 12387 12388 12389 12390 12391
12392 12393 12394 12395 12396 12397 12398 12399
12400 12401 12402 12403 12404 12405 12406 12407
12408 12409 12410 12411 12412 12413 12414 12415
12416 12417 12418 12419 12420 12421 12422 12423
12424 12425 12426 12427 12428 12429 12430 12431
12432 12433 12434 12435 12436 12437 12438 12439
12440 12441 12442 12443 12444 12445 12446 12447
12448 12449 12450 12451 12452 12453 12454 12455
12456 12457 12458 12459 12460 12461 12462 12463
12464 12465 12466 12467 12468 12469 12470 12471
12472 12473 12474 12475 12476 12477 12478 12479
12480 12481 12482 12483 12484 12485 12486 12487
12488 12489 12490 12491 12492 12493 12494 12495
12496 12497 12498 12499 12500 12501 12502 12503
12504 12505 12506 12507 12508 12509 12510 12511
12512 12513 12514 12515 12516 12517 12518 12519
12520 12521 12522 12523 12524 12525 12526 12527
12528 12529 12530 12531 12532 12533 12534 12535
12536 12537 12538 12539 12540 12541 12542 12543
12544 12545 12546 12547 12548 12549 12550 12551
```

```
12552 12553 12554 12555 12556 12557 12558 12559
12560 12561 12562 12563 12564 12565 12566 12567
12568 12569 12570 12571 12572 12573 12574 12575
12576 12577 12578 12579 12580 12581 12582 12583
12584 12585 12586 12587 12588 12589 12590 12591
12592 12593 12594 12595 12596 12597 12598 12599
12600 12601 12602 12603 12604 12605 12606 12607
12608 12609 12610 12611 12612 12613 12614 12615
12616 12617 12618 12619 12620 12621 12622 12623
12624 12625 12626 12627 12628 12629 12630 12631
12632 12633 12634 12635 12636 12637 12638 12639
12640 12641 12642 12643 12644 12645 12646 12647
12648 12649 12650 12651 12652 12653 12654 12655
12656 12657 12658 12659 12660 12661 12662 12663
12664 12665 12666 12667 12668 12669 12670 12671
12672 12673 12674 12675 12676 12677 12678 12679
12680 12681 12682 12683 12684 12685 12686 12687
12688 0 0 0 0 0 0 0

[STDERR]
```

Context:

Analyst: Markus Winklhofer
Timestamp: 2025-05-07T15:57:15.839920+00:00

[x] No specific explanation found.

[+] Command: `sudo icat -f fat /dev/loop1 4 >Bild1_extr_sqsh.jpg`

- Timestamp: `2025-05-07T15-59-16-193817+00-00`
- GPG-signature: [+] Valid
- SHA256: `aec4dbdae6db78716bf86b6c6d3a9f3327d00c39a9d0715fb7ff7b953c1c499f`

Output:

Shell

```
[STDOUT]

[STDERR]
```

Context:

Analyst: Markus Winklhofer
Timestamp: 2025-05-07T15:59:16.354081+00:00

[x] No specific explanation found.

[+] Command: `sudo icat -f fat /dev/loop1 6 >Bild2_extr_sqsh.jpeg`

- Timestamp: `2025-05-07T15-59-32-481827+00-00`
- GPG-signature: [+] Valid
- SHA256: `aec4dbdae6db78716bf86b6c6d3a9f3327d00c39a9d0715fb7ff7b953c1c499f`

Output:

```shell
[STDOUT]

[STDERR]
```

Context:

Analyst: Markus Winklhofer
Timestamp: 2025-05-07T15:59:32.648136+00:00

[x] No specific explanation found.

[+] Command: `sudo icat -f fat /dev/loop1 8 > blue_extr_sqsh.png`

- Timestamp: `2025-05-07T15-59-47-376302+00-00`
- GPG-signature: [+] Valid
- SHA256: `aec4dbdae6db78716bf86b6c6d3a9f3327d00c39a9d0715fb7ff7b953c1c499f`

Output:

```shell
[STDOUT]

[STDERR]
```

Context:

Analyst: Markus Winklhofer
Timestamp: 2025-05-07T15:59:47.539166+00:00

[x] No specific explanation found.

[+] Command: `sha256sum Bild1_extr_sqsh.jpg >> extraction_hashes.txt`

- Timestamp: `2025-05-07T16-01-26-515694+00-00`
- GPG-signature: [+] Valid
- SHA256: `aec4dbdae6db78716bf86b6c6d3a9f3327d00c39a9d0715fb7ff7b953c1c499f`

Output:

```Shell
[STDOUT]

[STDERR]
```

Context:

Analyst: Markus Winklhofer
Timestamp: 2025-05-07T16:01:26.675735+00:00

[x] No specific explanation found.

[+] Command: `sha256sum Bild2_extr_sqsh.jpeg >> extraction_hashes.txt`

- Timestamp: `2025-05-07T16-01-36-772077+00-00`
- GPG-signature: [+] Valid
- SHA256: `aec4dbdae6db78716bf86b6c6d3a9f3327d00c39a9d0715fb7ff7b953c1c499f`

Output:

```Shell
[STDOUT]

```

```
3  [STDERR]
```

Context:

Analyst: Markus Winklhofer
Timestamp: 2025-05-07T16:01:36.926284+00:00

[x] No specific explanation found.

[+] Command: `sha256sum blue_extr_sqsh.png >> extraction_hashes.txt`

- Timestamp: `2025-05-07T16-01-48-662062+00-00`
- GPG-signature: [+] Valid
- SHA256: `aec4dbdae6db78716bf86b6c6d3a9f3327d00c39a9d0715fb7ff7b953c1c499f`

Output:

Shell

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

Context:

Analyst: Markus Winklhofer
Timestamp: 2025-05-07T16:01:48.811388+00:00

[x] No specific explanation found.

[+] Command: `ls`

- Timestamp: `2025-05-07T16-02-06-081396+00-00`
- GPG-signature: [+] Valid
- SHA256: `a84212798f6c9b36c3d79b0e69025ba4e4eea611bb78e1bd3ae34c2bebb974f4`

Output:

Shell

```
1  [STDOUT]
```

```
Bild1_extr.jpg
Bild1_extr_sqsh.jpg
Bild2_extr.jpeg
Bild2_extr_sqsh.jpeg
blue_extr.png
blue_extr_sqsh.png
dc3dd_log.txt
dcfldd_hashes.txt
extraction_hashes.txt
hashes_usb_dcfldd.txt
squashfs-root
usb_dc3dd.img
usb_dcfldd_2.img
usb_dcfldd.img
usb_dd_container.sqsh
usb_dd.img
vUSB.img
vUSB.zip

[STDERR]
```

Context:

Analyst: Markus Winklhofer
Timestamp: 2025-05-07T16:02:06.227808+00:00

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

[+] Command: `cat extraction_hashes.txt`

- Timestamp: `2025-05-07T16-02-25-883108+00-00`
- GPG-signature: [+] Valid
- SHA256: `02f67ab44a442f08f1ca74f59732cdfa7c9437ec2e56e29a01c21ef16d2656d5`

Output:

Shell

```
[STDOUT]
d2cc34b1613360da8fe39bd9f95e0749f0d48acc9396d37139b5624ab7655363  Bild1_extr.jpg - Offset: 12312
01b8a6d33ba74fec3a5e04fdd3d52f9738bd97d9d3c97c043955e1bd6bc39a92  Bild2_extr.jpeg - Offset: 12696
efc4cbf142fdfe55d5695fe02240cd1f0782e086ce5490f1b65e398c3279b375  blue_extr.png - Offset: 16896
```

```
d2cc34b1613360da8fe39bd9f95e0749f0d48acc9396d37139b5624ab7655363
Bild1_extr_sqsh.jpg
01b8a6d33ba74fec3a5e04fdd3d52f9738bd97d9d3c97c043955e1bd6bc39a92
Bild2_extr_sqsh.jpeg
efc4cbf142fdfe55d5695fe02240cd1f0782e086ce5490f1b65e398c3279b375
blue_extr_sqsh.png

[STDERR]
```

Context:

Analyst: Markus Winklhofer
Timestamp: 2025-05-07T16:02:26.030864+00:00

[x] No specific explanation found.

[+] Command: `sudo istat -f fat /dev/loop1 6`

- Timestamp: `2025-05-07T16-05-44-806619+00-00`
- GPG-signature: [+] Valid
- SHA256: `da52b421630b861f3c63ae7cea5068eedade839e64a991bbb9a8a39229cbe924`

Output:

Shell

```
[STDOUT]
Directory Entry: 6
Allocated
File Attributes: File, Archive
Size: 2148214
Name: BILD2~1.JPE

Directory Entry Times:
Written:    2022-05-09 15:22:40 (CEST)
Accessed:   2022-05-09 00:00:00 (CEST)
Created:    2022-05-09 15:22:41 (CEST)

Sectors:
12696 12697 12698 12699 12700 12701 12702 12703
12704 12705 12706 12707 12708 12709 12710 12711
12712 12713 12714 12715 12716 12717 12718 12719
12720 12721 12722 12723 12724 12725 12726 12727
...
16872 16873 16874 16875 16876 16877 16878 16879
16880 16881 16882 16883 16884 16885 16886 16887
```

```
16888 16889 16890 16891 0 0 0 0

[STDERR]
```

Context:

Analyst: Markus Winklhofer
Timestamp: 2025-05-07T16:05:44.968386+00:00

[x] No specific explanation found.

[+] Command: `sudo istat -f fat /dev/loop1 8`

- Timestamp: `2025-05-07T16-07-01-235192+00-00`
- GPG-signature: [+] Valid
- SHA256: `84519aec0b31b0079085a8099047530dbfcb1f6be5c4f6f55ec219013d254a92`

Output:

Shell

```
[STDOUT]
Directory Entry: 8
Allocated
File Attributes: File, Archive
Size: 15540
Name: BLUE.PNG

Directory Entry Times:
Written:    2022-05-09 15:52:12 (CEST)
Accessed:   2022-05-09 00:00:00 (CEST)
Created:    2022-05-09 15:52:13 (CEST)

Sectors:
16896 16897 16898 16899 16900 16901 16902 16903
16904 16905 16906 16907 16908 16909 16910 16911
16912 16913 16914 16915 16916 16917 16918 16919
16920 16921 16922 16923 16924 16925 16926 0

[STDERR]
```

Context:

Analyst: Markus Winklhofer
Timestamp: 2025-05-07T16:07:01.392116+00:00

[x] No specific explanation found.

[+] Command: `cat extraction_hashes.txt`

- Timestamp: `2025-05-07T16-07-32-498205+00-00`
- GPG-signature: [+] Valid
- SHA256: `604834b3c9037ce8aac1ea9d9ea1c47c80dedc8077e1e5100863f8973cf12c98`

Output:

Shell

```
[STDOUT]
d2cc34b1613360da8fe39bd9f95e0749f0d48acc9396d37139b5624ab7655363  Bild1_extr.jpg - Offset: 12312
01b8a6d33ba74fec3a5e04fdd3d52f9738bd97d9d3c97c043955e1bd6bc39a92  Bild2_extr.jpeg - Offset: 12696
efc4cbf142fdfe55d5695fe02240cd1f0782e086ce5490f1b65e398c3279b375  blue_extr.png - Offset: 16896
d2cc34b1613360da8fe39bd9f95e0749f0d48acc9396d37139b5624ab7655363  Bild1_extr_sqsh.jpg - Offset: 12312
01b8a6d33ba74fec3a5e04fdd3d52f9738bd97d9d3c97c043955e1bd6bc39a92  Bild2_extr_sqsh.jpeg - Offset: 12696
efc4cbf142fdfe55d5695fe02240cd1f0782e086ce5490f1b65e398c3279b375  blue_extr_sqsh.png - Offset: 16896

[STDERR]
```

Context:

Analyst: Markus Winklhofer
Timestamp: 2025-05-07T16:07:32.650385+00:00

[x] No specific explanation found.

[+] Timestamp: `2025-05-07T16-08-26-202817+00-00`

[+] Comment from analyst: Markus Winklhofer

[+] Content:

Hashes und Offsets der Dateien verglichen. Jeweis identisch. Keine weiteren Unterschiede festgestellt?

[+] Timestamp: `2025-05-07T16-11-01-409905+00-00`

[+] Comment from analyst: Markus Winklhofer

[+] Content:

Unterschied möglicherweise, dass sie in einem extra container gespeichert werden? Bzw. Habe ich ja nur das Image usb_dd.img in meinem Container und dieses dann als virtual Device anglegt, um anschließend zu vergleichen? Eventuell habe ich dadurch gar nicht die Squash Daten verglichen, sondern nur die Dateien von der dd Kopie?

[+] Timestamp: `2025-06-02T19-49-24-204538+02-00`

> ⓘ **Comment from analyst: Markus Winklhofer**
>
> Ergänzung: Analyse des Bildes blue.png

[+] Command: `identify -verbose blue_extr.png`

- Timestamp: `2025-06-02T19-51-03-067803+02-00`
- GPG-signature: [+] Valid
- SHA256: `8686f4323097d1f7068227e5d3fe615d9329e791f1538766495bf21fd683b0a7`

Output:

Shell

```
[STDOUT]
Image:
  Filename: blue_extr.png
  Permissions: rw-rw-r--
  Format: PNG (Portable Network Graphics)
  Mime type: image/png
  Class: DirectClass
  Geometry: 1920x1080+0+0
  Resolution: 118.11x118.11
  Print size: 16.256x9.14402
  Units: PixelsPerCentimeter
  Colorspace: sRGB
  Type: Palette
```

```
  Base type: TrueColor
  Endianness: Undefined
  Depth: 8-bit
  Channels: 3.0
  Channel depth:
    Red: 1-bit
    Green: 1-bit
    Blue: 8-bit
  Channel statistics:
    Pixels: 2073600
    Red:
      min: 0  (0)
      max: 0 (0)
      mean: 0 (0)
      median: 0 (0)
      standard deviation: 0 (0)
      kurtosis: 0
      skewness: 0
      entropy: 0
    Green:
      min: 0  (0)
      max: 0 (0)
      mean: 0 (0)
      median: 0 (0)
      standard deviation: 0 (0)
      kurtosis: 0
      skewness: 0
      entropy: 0
    Blue:
      min: 244  (0.956863)
      max: 245 (0.960784)
      mean: 244.101 (0.957258)
      median: 244 (0.956863)
      standard deviation: 0.301074 (0.00118068)
      kurtosis: 5.03197
      skewness: 2.65179
      entropy: 0.471551
  Image statistics:
    Overall:
      min: 0  (0)
      max: 245 (0.960784)
      mean: 81.3669 (0.319086)
      median: 81.3333 (0.318954)
      standard deviation: 0.100358 (0.000393561)
      kurtosis: 1.67732
      skewness: 0.883929
      entropy: 0.157184
  Colors: 2
  Histogram:
       1864565: (0,0,244) #0000F4 srgb(0,0,244)
```

```
      209035: (0,0,245) #0000F5 srgb(0,0,245)
  Rendering intent: Perceptual
  Gamma: 0.454545
  Chromaticity:
    red primary: (0.64,0.33,0.03)
    green primary: (0.3,0.6,0.1)
    blue primary: (0.15,0.06,0.79)
    white point: (0.3127,0.329,0.3583)
  Matte color: grey74
  Background color: white
  Border color: srgb(223,223,223)
  Transparent color: black
  Interlace: None
  Intensity: Undefined
  Compose: Over
  Page geometry: 1920x1080+0+0
  Dispose: Undefined
  Iterations: 0
  Compression: Zip
  Orientation: Undefined
  Profiles:
    Profile-icc: 672 bytes
  Properties:
    Comment: Created with GIMP
    date:create: 2025-05-07T14:25:37+00:00
    date:modify: 2025-05-07T14:25:37+00:00
    date:timestamp: 2025-06-02T17:51:03+00:00
    icc:copyright: Public Domain
    icc:description: GIMP built-in sRGB
    icc:manufacturer: GIMP
    icc:model: sRGB
    png:iCCP: chunk was found
    png:IHDR.bit-depth-orig: 8
    png:IHDR.bit_depth: 8
    png:IHDR.color-type-orig: 2
    png:IHDR.color_type: 2 (Truecolor)
    png:IHDR.interlace_method: 0 (Not interlaced)
    png:IHDR.width,height: 1920, 1080
    png:pHYs: x_res=11811, y_res=11811, units=1
    png:text: 1 tEXt/zTXt/iTXt chunks were found
    png:tIME: 2022-05-09T15:35:58Z
    signature:
c0d39c9d8423a9acf95217f7c89fae9664f98711953559468c5d22cdb712e8b1
  Artifacts:
    verbose: true
  Tainted: False
  Filesize: 15540B
  Number pixels: 2.0736M
  Pixel cache type: Memory
  Pixels per second: 122.564MP
```

```
113     User time: 0.010u
114     Elapsed time: 0:01.016
115     Version: ImageMagick 7.1.1-43 Q16 aarch64 22550
      https://imagemagick.org
116
117   [STDERR]
```

Context:

Analyst: Markus Winklhofer
Timestamp: 2025-06-02T19:51:05.950506+02:00

[x] No specific explanation found.

[+] Timestamp: `2025-06-02T19-53-17-637134+02-00`

> ⓘ **Comment from analyst: Markus Winklhofer**
>
> Aus den Metadaten des Bildes kann unter Histogramm entnommen werden, dass es sich um zwei verschiedene Farben, genauer zwei Blautöne, handelt.

[+] Command: `convert blue_extr.png -fill transparent -opaque 'srgb(0,0,244)' blue_edited.png`

- Timestamp: `2025-06-02T19-55-15-949490+02-00`
- GPG-signature: [+] Valid
- SHA256: `aec4dbdae6db78716bf86b6c6d3a9f3327d00c39a9d0715fb7ff7b953c1c499f`

Output:

Shell

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

Context:

Analyst: Markus Winklhofer
Timestamp: 2025-06-02T19:55:16.043920+02:00

[x] No specific explanation found.

[+] Timestamp: `2025-06-02T19-58-14-354260+02-00`

> ⓘ **Comment from analyst: Markus Winklhofer**
>
> Nach entfernen eines Blautones, ist der Pin deutlich erkennbar. Dieser lautet: 5713 und ist vermutlich manuell per Bildbearbeitungsprogramm hinzugefügt worden.

[+] GPG-Overview

Each `.log`-file was digitally signed with GPG where applicable.
The signature status is documented per command.

---

3. Ergebnisse

Gesicherte Bilder:

- Bild1.jpg
- Bild2.jpeg
- Blue.png
- PIN: 5713

---

4. Verwendete Quellen

-