Befundsdokumentation 3.2.

Übungsaufgabe 3 - A2

Team: 13
Bearbeiter: 3009728 | 3026182 | 3019335 | 3008816
Datum der Erstellung: 27.04.2025

Nicht-technische Zusammenfassung

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

Im Rahmen einer forensischen Untersuchung wurde eine Festplatte sichergestellt und dem Sachverständigen zur Analyse übergeben. Ziel war es, zentrale Fragen zu Betriebssystem, Benutzeridentität, Passwort und gespeicherten Dateien zu klären.

i) Betriebssystem:
Die Analyse des gesicherten Datenabbilds ergab, dass auf dem System das Betriebssystem `Linux` verwendet wurde. Dies konnte durch die Struktur der Partitionen sowie typische Linux-Systemordner (z. B. `/etc`, `/home`, `/var`) eindeutig festgestellt werden.

ii) Benutzername:
In der Datei `passwd`, die Informationen zu Systembenutzern enthält, wurde der Benutzername `dif` gefunden. Dieser war der einzige reguläre Benutzer mit einem eigenen Home-Verzeichnis (`/home/dif`) und ist daher mit hoher Wahrscheinlichkeit der Hauptnutzer des Systems.

iii) Passwort:
Das Passwort wurde mithilfe eines Hash-Werts aus der Datei `shadow` und anschließender Brute-Force-Analyse mit dem Programm `hashcat` erfolgreich entschlüsselt. Das Passwort des Benutzers lautet: `22dif04`.

iv) Gespeicherte Dateien und Inhalte:
Im Benutzerverzeichnis wurden im Ordner „Pictures“ zwei erstellte Bilddateien gefunden:

- **schuhschnabel.png**
- **schuhschnabel.webp**

Diese Dateien enthalten Bildmaterial eines „Schuhschnabels“ (eines exotischen Vogels).

Technischer Bericht

1. Übersicht der analysierten Daten

Datenquelle	Typ	Datentyp	Größe	Hash (SHA256)
image.zip	ZIP	-	4.7GB	33685e37574d2dfc7d88acb72d566fc085561f9
image.img	Image	RAW	21GB	9b88ff2c1688645ab9d32899fccc6e4cc073c51

2. Chronologisches Analyseprotokoll

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

[+] Command: `du –d 1 –h`

- Timestamp: `2025-04-27T12-57-42-551874+00-00`
- GPG-signature: [x] Invalid
- SHA256: `c2d8d71eed5e884d51bacef5b08ce3c17f208da84a8cd3a23137604c17ded02f`

Output:

```
[STDOUT]
4.7G    .

[STDERR]
```

Context:

Analyst: Markus Winklhofer
Timestamp: 2025-04-27T12:57:42.730245+00:00

[x] No specific explanation found.

[+] Command: `ls`

- Timestamp: `2025-04-27T12-58-36-798617+00-00`
- GPG-signature: [+] Valid
- SHA256: `36ba8fd620d465681327e464a5ef8d625298fe757f5bb9e9d2d32a2098ee28c7`

Output:

```
[STDOUT]
image.zip

[STDERR]
```

Context:

Analyst: Markus Winklhofer
Timestamp: 2025-04-27T12:58:36.963025+00:00

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

[+] Command: `shasum -a 1 image.zip`

- Timestamp: `2025-04-27T13-02-54-455155+00-00`
- GPG-signature: [+] Valid
- SHA256: `383d926453e4e338202a5c818c81f2fe879dae0d4446fa3cd9e8f350ee3cb673`

Output:

```
[STDOUT]
33685e37574d2dfc7d88acb72d566fc085561f9e  image.zip

[STDERR]
```

Context:

Analyst: Markus Winklhofer
Timestamp: 2025-04-27T13:03:07.473781+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: `unzip image.zip -d Image03`

- Timestamp: `2025-04-27T13-13-18-419573+00-00`

- GPG-signature: [+] Valid
- SHA256: `74d017da0b894e78f6929703ce0dfe1558819e7ec4c07ad6beb16514b6d7bd88`

Output:

```
[!] Command failed:
warning [image.zip]:  726422008 extra bytes at beginning or within
zipfile
  (attempting to process anyway)
error [image.zip]:  start of central directory not found;
  zipfile corrupt.
  (please check that you have transferred or created the zipfile in the
  appropriate BINARY mode and that you have compiled UnZip properly)
```

Context:

Analyst: Markus Winklhofer
Timestamp: 2025-04-27T13:13:18.564261+00:00

`unzip` extracts a ZIP archive. Since it changes data on the destination system, it should only be used in **virtual analysis environments** or on forensic clones.

The `-d` option specifies the destination directory for extracted files. Useful to keep extracted data organized.

[+] Command: `unzip image.zip -d Image03`

- Timestamp: `2025-04-27T13-31-24-768088+00-00`
- GPG-signature: [+] Valid
- SHA256: `74d017da0b894e78f6929703ce0dfe1558819e7ec4c07ad6beb16514b6d7bd88`

Output:

```
[!] Command failed:
warning [image.zip]:  726422008 extra bytes at beginning or within
zipfile
  (attempting to process anyway)
error [image.zip]:  start of central directory not found;
  zipfile corrupt.
  (please check that you have transferred or created the zipfile in the
  appropriate BINARY mode and that you have compiled UnZip properly)
```

Context:

Analyst: Markus Winklhofer
Timestamp: 2025-04-27T13:31:24.919712+00:00

`unzip` extracts a ZIP archive. Since it changes data on the destination system, it should only be used in **virtual analysis environments** or on forensic clones.

The `-d` option specifies the destination directory for extracted files. Useful to keep extracted data organized.

[+] Command: `wxHexEditor image.zip`

- Timestamp: `2025-04-27T13-32-45-780363+00-00`
- GPG-signature: [+] Valid
- SHA256: `77081e37ddf65ddbbd36aea4d13736b26dff6421f5ce8f68b9cc575d6e0db80d`

Output:

```
[STDOUT]
5021389400

[STDERR]
03:39:02 PM: 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: 2025-04-27T13:39:02.368557+00:00

[x] No specific explanation found.

[+] Command: `unzip -l image.zip`

- Timestamp: `2025-04-27T13-39-32-949730+00-00`
- GPG-signature: [+] Valid
- SHA256: `74d017da0b894e78f6929703ce0dfe1558819e7ec4c07ad6beb16514b6d7bd88`

Output:

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

```
warning [image.zip]:  726422008 extra bytes at beginning or within zipfile
  (attempting to process anyway)
error [image.zip]:  start of central directory not found;
  zipfile corrupt.
  (please check that you have transferred or created the zipfile in the
  appropriate BINARY mode and that you have compiled UnZip properly)
```

Context:

Analyst: Markus Winklhofer
Timestamp: 2025-04-27T13:39:33.107427+00:00

`unzip` extracts a ZIP archive. Since it changes data on the destination system, it should only be used in **virtual analysis environments** or on forensic clones.

> ⓘ **Done**
>
> Datei kann nicht entpackt werden, da die Sektoren in der Datenstruktur verschoben sind

---

[+] Command: `zip -FFv image.zip --out fixed.zip`

- Timestamp: `2025-04-27T13-42-43-344908+00-00`
- GPG-signature: [+] Valid
- SHA256: `f418a1458b0f8324431b4795a1163f930fafeae6e9411b1ee1dfcf67b64c861e`

Output:

```
[STDOUT]
Fix archive (-FF) - salvage what can
 Found end record (EOCDR) - says expect single disk archive
Scanning for entries...
 Local ( 1      0): copying: image.img
.....................................................................
(5021389168 bytes)
Central Directory found...
 Cen   ( 1 5021389227): updating: image.img
    zip warning: needs unzip 4.5 on system type 0: image.img
Zip64 EOCDR found ( 1 5021389302)...
Zip64 EOCDL found ( 1 5021389358)...
EOCDR found ( 1 5021389378)...

[STDERR]
```

Context:

Analyst: Markus Winklhofer
Timestamp: 2025-04-27T13:43:01.089982+00:00

[x] No specific explanation found.

> **Done**
>
> Erneut entpackt im `-FF` (Fix Fix) Mode um, die beschädigte Datei zu reparieren und anschließend als neue .zip zu speichern

---

[+] Command: `unzip image.zip -d Image03`

- Timestamp: `2025-04-27T14-38-01-852893+00-00`
- GPG-signature: [+] Valid
- SHA256: `b931a45956fc067a64fc82e56e6e227e6e1d6e7bf339667f92fec475e865e785`

Output:

```
[STDOUT]
Archive:  image.zip
  inflating: Image03/image.img

[STDERR]
```

Context:

Analyst: Markus Winklhofer
Timestamp: 2025-04-27T14:40:05.454851+00:00

`unzip` extracts a ZIP archive. Since it changes data on the destination system, it should only be used in **virtual analysis environments** or on forensic clones.

The `-d` option specifies the destination directory for extracted files. Useful to keep extracted data organized.

[+] Command: `shasum -a 1 image.img`

- Timestamp: `2025-04-27T14-53-54-042697+00-00`
- GPG-signature: [+] Valid
- SHA256: `06050e7cf0cad444b74773cd4e09f6768647cd9821efce758af6ae513489af87`

Output:

```
[STDOUT]
9b88ff2c1688645ab9d32899fccc6e4cc073c51a  image.img

[STDERR]
```

Context:

Analyst: Markus Winklhofer
Timestamp: 2025-04-27T14:54:39.399601+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: `du -d 1 -h`

- Timestamp: `2025-04-27T14-56-06-667293+00-00`
- GPG-signature: [+] Valid
- SHA256: `f47272ad30bf8ef63ad6251f4181212dc84ea09332823a34a45009ab46771585`

Output:

```
[STDOUT]
21G .

[STDERR]
```

Context:

Analyst: Markus Winklhofer
Timestamp: 2025-04-27T14:56:06.816818+00:00

[x] No specific explanation found.

[+] Command: `echo 21474836480 / 1073741824 | bc -l`

- Timestamp: `2025-04-27T15-07-27-915919+00-00`
- GPG-signature: [+] Valid
- SHA256: `5ea97da6611d9fed2dff172f107b9527a57db9ad432faa2b25e73b2a897b2429`

Output:

```
[STDOUT]
20.00000000000000000000

[STDERR]
```

Context:

Analyst: Markus Winklhofer
Timestamp: 2025-04-27T15:07:28.072329+00:00

[x] No specific explanation found.

> **Done**
>
> Datei größe genau 20GB. Extrem selten, wsl mit `dd` eine Datei mit exakt 20 gb erstellt.

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

- Timestamp: `2025-04-27T15-10-40-428394+00-00`
- GPG-signature: [+] Valid
- SHA256: `ec6cba379190daec7a598fbdebd1091b460908aaafe956172bb81f422f59aa84`

Output:

```
[STDOUT]
Disk image.img: 20 GiB, 21474836480 bytes, 41943040 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: gpt
Disk identifier: C9C91594-26B4-4241-A6AC-99ED6689E164

Device       Start      End  Sectors  Size Type
image.img1    2048     4095     2048    1M BIOS boot
image.img2    4096  1054719  1050624  513M EFI System
image.img3 1054720 41940991 40886272 19.5G Linux filesystem

[STDERR]
```

Context:

Analyst: Markus Winklhofer
Timestamp: 2025-04-27T15:10:40.601681+00:00

[x] No specific explanation found.

> ⓘ **Done**
>
> Betriebssystem ist Linux

[+] Command: `mv image.img ~/Desktop/DIF/Aufgabe_2/U3`

- Timestamp: `2025-04-27T15-37-41-642525+00-00`
- GPG-signature: [+] Valid
- SHA256: `aec4dbdae6db78716bf86b6c6d3a9f3327d00c39a9d0715fb7ff7b953c1c499f`

Output:

```
[STDOUT]

[STDERR]
```

Context:

Analyst: Markus Winklhofer
Timestamp: 2025-04-27T15:37:41.793646+00:00

[x] No specific explanation found.

[+] Command: `sudo mount -o ro,loop image.img ~/mnt/evidence`

- Timestamp: `2025-04-27T15-42-06-376077+00-00`
- GPG-signature: [+] Valid
- SHA256: `587e9bc972f5a1098ce162b310de91f114b997d13f6d1bed2cea53ab74e2388f`

Output:

```
[!] Command failed:
mount: /home/forick/mnt/evidence: wrong fs type, bad option, bad superblock on /dev/loop0, missing codepage or helper program, or other error.
       dmesg(1) may have more information after failed mount system call.
```

Context:

Analyst: Markus Winklhofer
Timestamp: 2025-04-27T15:42:09.060834+00:00

[x] No specific explanation found.

> ⓘ **Done**
>
> image kann nicht gemaountet werder wegen fehlendem offst. Offset berechnet sich aus `offset=start*512`. 512 gibt dabei die standart Byte-Sektorgröße an.

[+] Command: `sudo dd if=image.img of=extraxtion.img bs=512 skip=1054720 count=40886272 conv=notrunc,sync,noerror`

- Timestamp: `2025-04-27T19-30-59-062689+00-00`
- GPG-signature: [+] Valid
- SHA256: `8f8f88b05e058bc7db97d6b2325cb3dcea2c648945bc11dd42a660e0e459d266`

Output:

```
[STDOUT]

[STDERR]
40886272+0 records in
40886272+0 records out
20933771264 bytes (21 GB, 19 GiB) copied, 97.6704 s, 214 MB/s
```

Context:

Analyst: Markus Winklhofer
Timestamp: 2025-04-27T19:32:39.096573+00:00

[x] No specific explanation found.

[+] Command: `sudo mount -o ro,loop,offset=540016640 extraxtion.img ~/mnt/evidence`

- Timestamp: `2025-04-27T19-34-17-668459+00-00`
- GPG-signature: [+] Valid
- SHA256: `587e9bc972f5a1098ce162b310de91f114b997d13f6d1bed2cea53ab74e2388f`

Output:

```
[!] Command failed:
mount: /home/forick/mnt/evidence: wrong fs type, bad option, bad superblock on /dev/loop0, missing codepage or helper program, or other error.
       dmesg(1) may have more information after failed mount system call.
```

Context:

Analyst: Markus Winklhofer
Timestamp: 2025-04-27T19:34:17.867913+00:00

[x] No specific explanation found.

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

- Timestamp: `2025-04-27T19-35-52-560841+00-00`

- GPG-signature: [+] Valid
- SHA256: `8a0ebe3fb7957b6ed5ec4204651f516f22fd16fd0241c4021a13fb3340218e7c`

Output:

```
[STDOUT]
Disk extraxtion.img: 19.5 GiB, 20933771264 bytes, 40886272 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

[STDERR]
```

Context:

Analyst: Markus Winklhofer
Timestamp: 2025-04-27T19:35:52.729939+00:00

[x] No specific explanation found.

[+] Command: `sudo mount -o ro,loop extraxtion.img ~/mnt/evidence`

- Timestamp: `2025-04-27T19-36-57-750133+00-00`
- GPG-signature: [+] Valid
- SHA256: `aec4dbdae6db78716bf86b6c6d3a9f3327d00c39a9d0715fb7ff7b953c1c499f`

Output:

```
[STDOUT]

[STDERR]
```

Context:

Analyst: Markus Winklhofer
Timestamp: 2025-04-27T19:36:57.946019+00:00

[x] No specific explanation found.

[+] Command: `ls`

- Timestamp: `2025-04-27T19-38-24-591841+00-00`
- GPG-signature: [+] Valid
- SHA256: `394993d14590b6369ea62d8fc1f4ae9b6af79975eb46de8c6ea1c9a197072eb6`

Output:

```
[STDOUT]
bin
boot
cdrom
dev
etc
home
lib
lib32
lib64
libx32
lost+found
media
mnt
opt
proc
root
run
sbin
snap
srv
swapfile
sys
tmp
usr
var

[STDERR]
```

Context:

Analyst: Markus Winklhofer
Timestamp: 2025-04-27T19:38:24.741281+00:00

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

[+] Command: `ls`

- Timestamp: `2025-04-27T19-40-31-232999+00-00`

- GPG-signature: [+] Valid
- SHA256: `63670117ec2d5cafcce1ef5866aead3aedd18011264c679abc91dbf957c02932`

Output:

```
[STDOUT]
dif

[STDERR]
```

Context:

Analyst: Markus Winklhofer
Timestamp: 2025-04-27T19:40:31.382965+00:00

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

> **Done**
>
> Extraktionsbereich gemountet und Benutzernamen analysiert. Benutzername lautet `dif`

[+] Command: `cd etc`

- Timestamp: `2025-04-27T19-42-32-281861+00-00`
- GPG-signature: [+] Valid
- SHA256: `aec4dbdae6db78716bf86b6c6d3a9f3327d00c39a9d0715fb7ff7b953c1c499f`

Output:

```
[STDOUT]

[STDERR]
```

Context:

Analyst: Markus Winklhofer
Timestamp: 2025-04-27T19:42:32.442699+00:00

`cd` is used to change directories. It does not modify data and is forensically harmless.

[+] Command: `ls`

- Timestamp: `2025-04-27T19-42-38-484730+00-00`
- GPG-signature: [+] Valid
- SHA256: `394993d14590b6369ea62d8fc1f4ae9b6af79975eb46de8c6ea1c9a197072eb6`

Output:

```
[STDOUT]
bin
boot
cdrom
dev
etc
home
lib
lib32
lib64
libx32
lost+found
media
mnt
opt
proc
root
run
sbin
snap
srv
swapfile
sys
tmp
usr
var

[STDERR]
```

Context:

Analyst: Markus Winklhofer
Timestamp: 2025-04-27T19:42:38.634062+00:00

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

[+] Command: `ls`

- Timestamp: `2025-04-27T19-43-06-686654+00-00`
- GPG-signature: [+] Valid
- SHA256: `7e79deeb013f477c70b296296ce22342bf81683c02f7fd7d37f027454648ac5a`

Output:

```
[STDOUT]
acpi
adduser.conf
alsa
alternatives
anacrontab
apg.conf
apm
apparmor
apparmor.d
apport
appstream.conf
apt
avahi
bash.bashrc
bash_completion
bash_completion.d
bindresvport.blacklist
binfmt.d
bluetooth
brlapi.key
brltty
brltty.conf
ca-certificates
ca-certificates.conf
chatscripts
console-setup
cracklib
cron.d
cron.daily
cron.hourly
cron.monthly
crontab
cron.weekly
cups
cupshelpers
dbus-1
dconf
debconf.conf
debian_version
default
deluser.conf
```

```
depmod.d
dhcp
dictionaries-common
dpkg
e2scrub.conf
emacs
environment
environment.d
ethertypes
firefox
fonts
fprintd.conf
fstab
fuse.conf
fwupd
gai.conf
gdb
gdm3
geoclue
ghostscript
glvnd
gnome
groff
group
group-
grub.d
gshadow
gshadow-
gss
gtk-2.0
gtk-3.0
hdparm.conf
host.conf
hostid
hostname
hosts
hosts.allow
hosts.deny
hp
ifplugd
init
init.d
initramfs-tools
inputrc
insserv.conf.d
ipp-usb
iproute2
issue
issue.net
kernel
```

```
kernel-img.conf
kerneloops.conf
ldap
ld.so.cache
ld.so.conf
ld.so.conf.d
legal
libao.conf
libaudit.conf
libblockdev
libnl-3
libpaper.d
libreoffice
locale.alias
locale.gen
localtime
logcheck
login.defs
logrotate.conf
logrotate.d
lsb-release
ltrace.conf
machine-id
magic
magic.mime
mailcap
mailcap.order
manpath.config
mime.types
mke2fs.conf
modprobe.d
modules
modules-load.d
mtab
nanorc
netconfig
netplan
network
networkd-dispatcher
NetworkManager
networks
newt
nsswitch.conf
openvpn
opt
os-release
PackageKit
pam.conf
pam.d
papersize
```

```
passwd
passwd-
pcmcia
perl
pki
pm
pnm2ppa.conf
polkit-1
ppp
profile
profile.d
protocols
pulse
python3
python3.9
rc0.d
rc1.d
rc2.d
rc3.d
rc4.d
rc5.d
rc6.d
rc.local
rcS.d
resolv.conf
rmt
rpc
rsyslog.conf
rsyslog.d
rygel.conf
sane.d
security
selinux
sensors3.conf
sensors.d
services
sgml
shadow
shadow-
shells
skel
snmp
speech-dispatcher
ssh
ssl
subgid
subgid-
subuid
subuid-
sudo.conf
```

```
sudoers
sudoers.d
sudo_logsrvd.conf
sysctl.conf
sysctl.d
systemd
terminfo
thermald
timezone
tmpfiles.d
ubuntu-advantage
ucf.conf
udev
udisks2
ufw
update-manager
update-motd.d
update-notifier
UPower
usb_modeswitch.conf
usb_modeswitch.d
vim
vmware-tools
vtrgb
vulkan
wgetrc
wpa_supplicant
X11
xattr.conf
xdg
xml
zsh_command_not_found

[STDERR]
```

Context:

Analyst: Markus Winklhofer
Timestamp: 2025-04-27T19:43:06.833796+00:00

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

[+] Command: `cat ~/mnt/evidence/etc/passwd`

- Timestamp: `2025-04-27T19-46-21-566251+00-00`
- GPG-signature: [+] Valid

- SHA256: `d8006459429689b6c96d249af55a268e1688afcd086f59b057f8a03cb85616d6`

Output:

```
[STDOUT]
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/run/ircd:/usr/sbin/nologin
gnats:x:41:41:Gnats Bug-Reporting System
(admin):/var/lib/gnats:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
systemd-network:x:100:102:systemd Network
Management,,,:/run/systemd:/usr/sbin/nologin
systemd-resolve:x:101:103:systemd
Resolver,,,:/run/systemd:/usr/sbin/nologin
systemd-timesync:x:102:104:systemd Time
Synchronization,,,:/run/systemd:/usr/sbin/nologin
messagebus:x:103:106::/nonexistent:/usr/sbin/nologin
syslog:x:104:111::/home/syslog:/usr/sbin/nologin
_apt:x:105:65534::/nonexistent:/usr/sbin/nologin
tss:x:106:112:TPM software stack,,,:/var/lib/tpm:/bin/false
uuidd:x:107:115::/run/uuidd:/usr/sbin/nologin
tcpdump:x:108:116::/nonexistent:/usr/sbin/nologin
avahi-autoipd:x:109:118:Avahi autoip daemon,,,:/var/lib/avahi-
autoipd:/usr/sbin/nologin
usbmux:x:110:46:usbmux daemon,,,:/var/lib/usbmux:/usr/sbin/nologin
rtkit:x:111:119:RealtimeKit,,,:/proc:/usr/sbin/nologin
dnsmasq:x:112:65534:dnsmasq,,,:/var/lib/misc:/usr/sbin/nologin
kernoops:x:113:65534:Kernel Oops Tracking Daemon,,,:/:/usr/sbin/nologin
avahi:x:114:121:Avahi mDNS daemon,,,:/run/avahi-daemon:/usr/sbin/nologin
cups-pk-helper:x:115:122:user for cups-pk-helper service,,,:/home/cups-
pk-helper:/usr/sbin/nologin
whoopsie:x:116:123::/nonexistent:/bin/false
sssd:x:117:124:SSSD system user,,,:/var/lib/sss:/usr/sbin/nologin
speech-dispatcher:x:118:29:Speech Dispatcher,,,:/run/speech-
dispatcher:/bin/false
```

```
nm-openvpn:x:119:125:NetworkManager
OpenVPN,,,:/var/lib/openvpn/chroot:/usr/sbin/nologin
saned:x:120:127::/var/lib/saned:/usr/sbin/nologin
colord:x:121:128:colord colour management
daemon,,,:/var/lib/colord:/usr/sbin/nologin
geoclue:x:122:129::/var/lib/geoclue:/usr/sbin/nologin
pulse:x:123:130:PulseAudio daemon,,,:/run/pulse:/usr/sbin/nologin
gnome-initial-setup:x:124:65534::/run/gnome-initial-setup/:/bin/false
hplip:x:125:7:HPLIP system user,,,:/run/hplip:/bin/false
gdm:x:126:132:Gnome Display Manager:/var/lib/gdm3:/bin/false
dif:x:1000:1000:DIF,,,:/home/dif:/bin/bash
systemd-coredump:x:999:999:systemd Core Dumper:/:/usr/sbin/nologin

[STDERR]
```

Context:

Analyst: Markus Winklhofer
Timestamp: 2025-04-27T19:46:21.721863+00:00

[x] No specific explanation found.

[+] Command: `sudo cat ~/mnt/evidence/etc/shadow`

- Timestamp: `2025-04-27T19-46-38-089865+00-00`
- GPG-signature: [+] Valid
- SHA256: `d95258b1e9cdccca9c14c7fc1be0ac3f5d88e6ac9cd90e7925dca8747a523fa8`

Output:

```
[STDOUT]
root:!:19105:0:99999:7:::
daemon:*:18912:0:99999:7:::
bin:*:18912:0:99999:7:::
sys:*:18912:0:99999:7:::
sync:*:18912:0:99999:7:::
games:*:18912:0:99999:7:::
man:*:18912:0:99999:7:::
lp:*:18912:0:99999:7:::
mail:*:18912:0:99999:7:::
news:*:18912:0:99999:7:::
uucp:*:18912:0:99999:7:::
proxy:*:18912:0:99999:7:::
www-data:*:18912:0:99999:7:::
backup:*:18912:0:99999:7:::
list:*:18912:0:99999:7:::
```

```
irc:*:18912:0:99999:7:::
gnats:*:18912:0:99999:7:::
nobody:*:18912:0:99999:7:::
systemd-network:*:18912:0:99999:7:::
systemd-resolve:*:18912:0:99999:7:::
systemd-timesync:*:18912:0:99999:7:::
messagebus:*:18912:0:99999:7:::
syslog:*:18912:0:99999:7:::
_apt:*:18912:0:99999:7:::
tss:*:18912:0:99999:7:::
uuidd:*:18912:0:99999:7:::
tcpdump:*:18912:0:99999:7:::
avahi-autoipd:*:18912:0:99999:7:::
usbmux:*:18912:0:99999:7:::
rtkit:*:18912:0:99999:7:::
dnsmasq:*:18912:0:99999:7:::
kernoops:*:18912:0:99999:7:::
avahi:*:18912:0:99999:7:::
cups-pk-helper:*:18912:0:99999:7:::
whoopsie:*:18912:0:99999:7:::
sssd:*:18912:0:99999:7:::
speech-dispatcher:!:18912:0:99999:7:::
nm-openvpn:*:18912:0:99999:7:::
saned:*:18912:0:99999:7:::
colord:*:18912:0:99999:7:::
geoclue:*:18912:0:99999:7:::
pulse:*:18912:0:99999:7:::
gnome-initial-setup:*:18912:0:99999:7:::
hplip:*:18912:0:99999:7:::
gdm:*:18912:0:99999:7:::
dif:$1$Al1JOy/e$nSQ5CgVYrz2WTfoeXQwH11:19105:0:99999:7:::
systemd-coredump:!*:19105::::::

[STDERR]
```

Context:

Analyst: Markus Winklhofer
Timestamp: 2025-04-27T19:46:38.244990+00:00

[x] No specific explanation found.

Done

Benutzerinformationen in `passwd` und gehashtes passwort in `shadow`. Beides unter `dif:`

[+] Command: `crunch 7 7 01234defghi -t @@%%%@@@ -o cruch_pswd.txt`

- Timestamp: `2025-04-27T19-57-30-638341+00-00`
- GPG-signature: [+] Valid
- SHA256: `7ca2faf0fd9c8a52a17ab37601cb5c0e5f7744fffe706ea8c4bcb3f46848809e`

Output:

```
[!] Command failed:
The maximum and minimum length should be the same size as the pattern you specified.
min = 7  max = 7  strlen(@@%%%@@@)=8
```

Context:

Analyst: Markus Winklhofer
Timestamp: 2025-04-27T19:57:30.805097+00:00

[x] No specific explanation found.

[+] Command: `crunch 7 7 01234defghi -t @@%%%@@ -o ~/Desktop/DIF/Aufgabe_2/U3/A2/crunch_pswd.txt`

- Timestamp: `2025-04-27T20-01-25-254637+00-00`
- GPG-signature: [+] Valid
- SHA256: `dff779e931696f6600b28db04cff3efe885682e02e9214025ecf81ccf087c84e`

Output:

```
[STDOUT]

[STDERR]
Crunch will now generate the following amount of data: 117128000 bytes
111 MB
0 GB
0 TB
0 PB
Crunch will now generate the following number of lines: 14641000

crunch: 100% completed generating output
```

Context:

Analyst: Markus Winklhofer
Timestamp: 2025-04-27T20:01:29.587557+00:00

[x] No specific explanation found.

> ⓘ **Done**
>
> Mit `crunch` Passwortliste generiert. Anzahl der Einträge: `1464100`

[+] Command: `sudo grep '^dif:' ~/mnt/evidence/etc/shadow > ~/Desktop/DIF/Aufgabe_2/U3/A2/shadows_hashes.txt`

- Timestamp: `2025-04-27T20-19-00-856217+00-00`
- GPG-signature: [+] Valid
- SHA256: `aec4dbdae6db78716bf86b6c6d3a9f3327d00c39a9d0715fb7ff7b953c1c499f`

Output:

```
[STDOUT]

[STDERR]
```

Context:

Analyst: Markus Winklhofer
Timestamp: 2025-04-27T20:19:01.006712+00:00

[x] No specific explanation found.

> ⓘ **Done**
>
> Hashwert extrahiert und hinterher manuell bereinigt mit `nano`

[+] Command: `hashcat -m 500 -a 0 ~/Desktop/DIF/Aufgabe_2/U3/A2/shadows_hashes.txt ~/Desktop/DIF/Aufgabe_2/U3/A2/crunch_pswd.txt`

- Timestamp: `2025-04-27T20-32-28-598404+00-00`
- GPG-signature: [+] Valid
- SHA256: `11e0b35624b99a938ab849d71f954667f5966494c9a765ea398021ee9d73af9b`

Output:

```
[!] Command failed:
No hashes loaded.
```

Context:

Analyst: Markus Winklhofer
Timestamp: 2025-04-27T20:32:29.382178+00:00

[x] No specific explanation found.

> **Info**
>
> Passwörter evtl. falsch generiert. Anzahl der Einträge würde viel zu lange dauern mit hashcat.

[+] Command: `crunch 7 7 -o ~/Desktop/DIF/Aufgabe_2/U3/A2/crunch_pswd.txt -t @@%%%@@ -o ~/Desktop/DIF/Aufgabe_2/U3/A2/crunch_pswd.txt -f charset.lst numeric -f charset.lst lower`

- Timestamp: `2025-04-27T21-01-40-538983+00-00`
- GPG-signature: [+] Valid
- SHA256: `6c0d67c7077073215c0e74d5bb81d49371fac10418cb1b1d406f25f17f2515f4`

Output:

```
[!] Command failed:
readcharset: File charset.lst could not be opened
The problem is = No such file or directory
```

Context:

Analyst: Markus Winklhofer
Timestamp: 2025-04-27T21:01:40.704682+00:00

[x] No specific explanation found.

> **Done**
>
> cruch tool erstellt zu viele Einträge. Selbst Python script für generierung geschrieben um Prozess zu optimieren

---

[+] Command: `hashcat -m 500 -a 0 ~/Desktop/DIF/Aufgabe_2/U3/A2/shadows_hashes.txt ~/Desktop/DIF/Aufgabe_2/U3/A2/passwortliste.txt`

- Timestamp: `2025-04-27T21-21-44-881901+00-00`
- GPG-signature: [+] Valid
- SHA256: `8f0d9ce6f074beb00c6a3acb701dbafe8f2aeb1cea9591cd7c243c848f5c78b8`

Output:

```
[STDOUT]
hashcat (v6.2.6) starting

OpenCL API (OpenCL 3.0 PoCL 6.0+debian  Linux, None+Asserts, RELOC, SPIR
====================================================================
* Device #1: cpu--0x000, 1435/2935 MB (512 MB allocatable), 4MCU

Minimum password length supported by kernel: 0
Maximum password length supported by kernel: 256

Counting lines in /home/forick/Desktop/DIF/Aufgabe_2/U3/A2/shadows_hashe
/home/forick/Desktop/DIF/Aufgabe_2/U3/A2/shadows_hashes.txtParsed Hashes
patient...Sorted hashesRemoving duplicate hashes. Please be patient...Re
saltsComparing hashes with potfile entries. Please be patient...Compared
bitmap tablesHashes: 1 digests; 1 unique digests, 1 unique salts
Bitmaps: 16 bits, 65536 entries, 0x0000ffff mask, 262144 bytes, 5/13 rot
Rules: 1

Optimizers applied:
* Zero-Byte
* Single-Hash
* Single-Salt

ATTENTION! Pure (unoptimized) backend kernels selected.
Pure kernels can crack longer passwords, but drastically reduce performa
If you want to switch to optimized kernels, append -O to your commandlin
```

```
See the above message to find out about the exact limits.

Watchdog: Hardware monitoring interface not found on your system.
Watchdog: Temperature abort trigger disabled.

Initializing device kernels and memory. Please be patient...Initializing backend runtime for device #1Host memory required for this attack: 0 MB

Initialized device kernels and memoryStarting self-test. Please be patie
* Filename..: /home/forick/Desktop/DIF/Aufgabe_2/U3/A2/passwortliste.txt
* Passwords.: 135000
* Bytes.....: 1080000
* Keyspace..: 135000
* Runtime...: 0 secs

Starting autotune. Please be patient...Finished autotune

[s]tatus [p]ause [b]ypass [c]heckpoint [f]inish [q]uit =>

$1$Al1JOy/e$nSQ5CgVYrz2WTfoeXQwH11:22dif04


Session..........: hashcat
Status...........: Cracked
Hash.Mode........: 500 (md5crypt, MD5 (Unix), Cisco-IOS $1$ (MD5))
Hash.Target......: $1$Al1JOy/e$nSQ5CgVYrz2WTfoeXQwH11
Time.Started.....: Sun Apr 27 23:21:46 2025 (2 secs)
Time.Estimated...: Sun Apr 27 23:21:48 2025 (0 secs)
Kernel.Feature...: Pure Kernel
Guess.Base.......: File (/home/forick/Desktop/DIF/Aufgabe_2/U3/A2/passwo
Guess.Queue......: 1/1 (100.00%)
Speed.#1.........:    26533 H/s (9.37ms) @ Accel:64 Loops:1000 Thr:1 Vec
Recovered........: 1/1 (100.00%) Digests (total), 1/1 (100.00%) Digests
Progress.........: 65792/135000 (48.73%)
Rejected.........: 0/65792 (0.00%)
Restore.Point....: 65536/135000 (48.55%)
Restore.Sub.#1...: Salt:0 Amplifier:0-1 Iteration:0-1000
Candidate.Engine.: Device Generator
Candidates.#1....: 22dhi21 -> 22edg31

Started: Sun Apr 27 23:21:45 2025
Stopped: Sun Apr 27 23:21:50 2025

[STDERR]
```

Context:

Analyst: Markus Winklhofer
Timestamp: 2025-04-27T21:21:50.257444+00:00

[x] No specific explanation found.

> **Done**
>
> Passwort: `22dif04`
> Dauer der Suche: `5sek`

> **Info**
>
> Anschließend Analyse der erstellten Dateien

[+] Command: `ls`

- Timestamp: `2025-05-01T11-14-09-309001+00-00`
- GPG-signature: [+] Valid
- SHA256: `81c7e3f6ad2793a63fa498d258ac5fa9007643b143502d94c536e3dd05fd30d0`

Output:

```
[STDOUT]
schuhschnabel.png
schuhschnabel.webp

[STDERR]
```

Context:

Analyst: Markus Winklhofer
Timestamp: 2025-05-01T11:14:09.470580+00:00

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

> **Done**
>
> Daten manuell durchsucht. Zwei Dateien in Pictures gefunden

---

[+] Command: `stat *`

- Timestamp: `2025-05-01T11-14-57-839268+00-00`
- GPG-signature: [+] Valid
- SHA256: `254c8af3e668cc927f6aa705975bf6a895f0a60581d12aefaf4b1f3b6464aa80`

Output:

```
[STDOUT]
  File: schuhschnabel.png
  Size: 654109      Blocks: 1280       IO Block: 4096   regular file
Device: 7,0 Inode: 273060      Links: 1
Access: (0664/-rw-rw-r--)  Uid: ( 1000/  forick)   Gid: ( 1000/  forick)
Access: 2022-04-23 23:48:27.935033736 +0200
Modify: 2022-04-23 23:48:08.823039148 +0200
Change: 2022-04-23 23:48:25.187032007 +0200
 Birth: 2022-04-23 23:48:08.687039340 +0200
  File: schuhschnabel.webp
  Size: 38460       Blocks: 80         IO Block: 4096   regular file
Device: 7,0 Inode: 273052      Links: 1
Access: (0664/-rw-rw-r--)  Uid: ( 1000/  forick)   Gid: ( 1000/  forick)
Access: 2022-04-23 23:44:18.619315750 +0200
Modify: 2022-04-23 23:44:16.435243655 +0200
Change: 2022-04-23 23:44:16.463244578 +0200
 Birth: 2022-04-23 23:44:16.403242599 +0200

[STDERR]
```

Context:

Analyst: Markus Winklhofer
Timestamp: 2025-05-01T11:14:57.990912+00:00

[x] No specific explanation found.

[+] Command: `open schuhschnabel.png`

- Timestamp: `2025-05-01T11-16-56-643797+00-00`
- GPG-signature: [+] Valid
- SHA256: `aec4dbdae6db78716bf86b6c6d3a9f3327d00c39a9d0715fb7ff7b953c1c499f`

Output:

```
[STDOUT]

[STDERR]
```

Context:

Analyst: Markus Winklhofer
Timestamp: 2025-05-01T11:16:58.855509+00:00

[x] No specific explanation found.

[+] Command: `open schuhschnabel.webp`

- Timestamp: `2025-05-01T11-17-07-988556+00-00`
- GPG-signature: [+] Valid
- SHA256: `1775a049035359bec5620481ee006212d7214af1e7117a8ba772ac3488177cdf`

Output:

```
[STDOUT]

[STDERR]
** Message: 13:17:08.334: Could not open file
'file:///home/forick/mnt/evidence/home/dif/Pictures/schuhschnabel.webp':
Unsupported mime type
```

Context:

Analyst: Markus Winklhofer
Timestamp: 2025-05-01T11:17:11.036627+00:00

[x] No specific explanation found.

> ⓘ **Done**
>
> Datei `schuhschnabel.webp` kann nicht normal geöffnet werden

[+] Command: `feh schuhschnabel.webp`

- Timestamp: `2025-05-01T11-19-08-955591+00-00`
- GPG-signature: [+] Valid
- SHA256: `aec4dbdae6db78716bf86b6c6d3a9f3327d00c39a9d0715fb7ff7b953c1c499f`

Output:

```
[STDOUT]

[STDERR]
```

Context:

Analyst: Markus Winklhofer
Timestamp: 2025-05-01T11:19:11.238979+00:00

[x] No specific explanation found.

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

- Timestamp: `2025-05-01T11-22-51-183815+00-00`
- GPG-signature: [+] Valid
- SHA256: `aec4dbdae6db78716bf86b6c6d3a9f3327d00c39a9d0715fb7ff7b953c1c499f`

Output:

```
[STDOUT]

[STDERR]
```

Context:

Analyst: Markus Winklhofer
Timestamp: 2025-05-01T11:22:51.357821+00:00

[x] No specific explanation found.

[+] Command: `sha256sum image.img`

- Timestamp: `2025-05-01T11-24-45-014190+00-00`
- GPG-signature: [+] Valid
- SHA256: `05a8580462a8df9dcc0b3b85f80bfc8a63019a4c134fb2a73e85814fe495fed1`

Output:

```
[STDOUT]
dda0d1d1f8109b8096e8edb31592cb7d2e08ef007653111eead966d9da7157fa
image.img

```

```
4   [STDERR]
```

Context:

Analyst: Markus Winklhofer
Timestamp: 2025-05-01T11:25:07.961233+00:00

[x] No specific explanation found.

[+] GPG-Overview

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

---

3. Ergebnisse

Betriebssystem: `Linux`
Benutzer: `dif`
Passwort: `22dif04`
`schuhschnabel.png`
`schuhschnabel.webp`

---

4. Verwendete Quellen

/