Aufgabe 1 (Imageerzeugung)

Hashwert nach der Abbilderzeugung:

```
$ md5sum /run/media/xe/TOSHIBA\ EXT/ForImage5.img
6eb8d7ab10e54706d0ccb3966e041f7e /run/media/xe/TOSHIBA EXT/ForImage5.img

$ sha1sum /run/media/xe/TOSHIBA\ EXT/ForImage5.img
a25ab111c649c8f904e4804c2a62dc277b026ab9 /run/media/xe/TOSHIBA EXT/ForImage5.img
```

Aufgabe 2 (Artefakte)

#	Dateiname	Speicherort (Pfad)	Hashwert
1	Passwörter.kdbx	/home/olaf/Passwörter.kdbx	8796e44f9a67308f5 feab3c1b80eb46b (md5)
2	formhistory.sqlite	/home/olaf/snap/firefox/common/ .mozilla/firefox/b7q08ugf.default/ formhistory.sqlite	548c0f1bf5833a67c 5b3e69306d1398d (md5)
3	places.sqlite	/home/olaf/snap/firefox/common/ .mozilla/firefox/b7q08ugf.default/ places.sqlite	851295f11c4e4b91 d003b6bb4d1d8798 (md5)
4	recently-used.xbel	/home/olaf/.local/share/recently-used.xbel	1457ed4766ec65f aafa30459ebf8b5d4 (md5)
5	maxresdefault.jpg	/home/olaf/Downloads/ maxresdefault.jpg	cf3139dda8e3d25f 5c8a64289b0c3b6d (md5)
6	XXX	/media/olaf/028AA54C0562CCCE/ porn/newStuff/XXX	80c42f0bfaf08194a 109ff5566693be4 (md5)
7	Ordner mit Vorschaubilder	/mnt/linux/home/olaf/.cache/ thumbnails	Siehe Befund 4.3.3

Aufgabe 3 (Gutachten)

Gutachten nach §161StPO
Ermittlungsverfahren Peukert

Gutachter:
Sachverständigenbüro Findet die Wahrheit
Team 9
Erkenntnisplatz 42
D-83093 Antwort

Gutachtenempfänger:
Oberstaatsanwältin Blitzgescheit
Hochschule Mannheim, Forensiklabor CSB/IMB/IB
D-420815 Forum

Betreff:
Ermittlungsverfahren gegen Abram Peukert, geb. 19.07.1994, wohnhaft Lilli-Henck-Straße 51, 44257 Gräfenhainichen, wegen Stalking

31.07.2022

Inhaltsverzeichnis

Abbildungsverzeichnis

Tabellenverzeichnis

1. Untersuchungsauftrag

Team 9 vom Sachverständigenbüro Findet die Wahrheit wurde durch Frau Oberstaatsanwältin Blitzgescheit mit der forensischen Auswertung einer sichergestellten Festplatte und der Erstellung eines Gutachtens über die Inhalte besagter Festplatte. Die Festplatte wurde im Zusammenhang mit dem Ermittlungsverfahren gegen Abram Peukert, geb. 19.07.1994, wohnhaft Lilli-Henck-Straße 51, 44257 Gräfenhainichen, wegen Stalking sichergestellt. Die Auswertung soll insbesondere umfassen:

a) Feststellung von Dateien (Bilder, Video) zum Ermittlungsverfahren wegen Stalking

b) Nachweis der Nutzung/Verbreitung

c) Extrahierung der elektronischen Kommunikation (E-Mail, Chat)

Zusätzlich zu dem in Abschnitt 2 aufgeführten Asservaten wurde an das Sachverständigenbüro Findet die Wahrheit die Datei *wordlist.txt* übergeben. Diese enthält eine Liste von Passwörtern welche eventuell vom Beschuldigten verwendet wurden.

2. Asservate

Es wurde eine Festplatte vom Hersteller Toshiba mit einer Gesamtkapazität von 500GB nach Herstellerangaben für die Untersuchung bereitgestellt. Auf der Vorderseite der Festplatte befand sich ein Aufkleber mit der Nummer „9“ und auf der Rückseite ein Aufkleber mit dem Schriftzug „qcow2“ (siehe Abbildung 1).
Die Festplatte enthielt nur eine Datei mit dem Dateinamen *ForImage5.img*. Diese Datei wurde zur weiteren Untersuchung kopiert und mitgenommen. Um sicherzustellen das Kopie und Orginal übereinstimmen wurden beide Dateien sowohl mit dem *MD5*-, als auch mit dem *SHA1*-Hashverfahren gehashed und die entstandenen Hashwerte auf Gleichheit überprüft.

	Hashwert	
Hashverfahren	Orginal	Kopie
MD5	6eb8d7ab10e54706d0 ccb3966e041f7e	6eb8d7ab10e54706d0 ccb3966e041f7e
SHA1	a25ab111c649c8f904e48 04c2a62dc277b026ab9	a25ab111c649c8f904e48 04c2a62dc277b026ab9

Tabelle 1: Hashwerte des Dateiabbildes

Abbildung 1: HDD Vorderseite und Rückseite

3. Ergebniszusammenfassung

Das zur Untersuchung stehende Asservat enthielt ein Festplattenabbild mit vier Partitionen. Davon waren Partition 3 und 4 für die Untersuchung von Interesse (siehe **??**). Die beiden anderen Partitionen existierten aus technischen Gründen und enthalten keine Nutzerdaten. Bei Partition 3 handelt es sich um ein Ubuntu Linux System, bei Partition 4 handelt es sich höchstwahrscheinlich um die Kopie eines USB-Sticks welcher indem für Windows typischen NTFS-Format formatiert ist.

#	Partition	Dateisystemtyp	Größe	Hashwert (MD5)
1	BIOS	mbr	1MiB	
2	EFI	fat32	513MiB	
3	Linux	ext4	21.5GiB	6a0f7a571bdc1c115438d74618d31795
4	Windows	NTFS	9.3GiB	06eb47519040dac1a411d7b0297911e6

Tabelle 2: Dateisystempartitionen

Auf dem Linux System wurden die Heimverzeichnisse für drei Nutzer gefunden:

- olaf
- pascal
- pc

Die Staatsanwaltschaft ist mit drei Anforderungen an die Gutachter herangetreten auf welche besonderen Augenmerk bei dieser Untersuchung gelegt werden sollte:

a) **Feststellung von Dateien (Bilder, Video) zum Ermittlungsverfahren wegen Stalking**
Im Heimverzeichnis des Nutzers *olaf* konnten Hinweise auf mehrere Fotos von einer Frau festgestellt werden. Die Frau hat dunkle Haare, trägt einen schwarzen Schall und eine schwarze Handtasche. Sie ist mit einer roten Hose und einem grauen Mantel bekleidet. Die Bilder sind dem Eindruck der Gutachter nach ohne das Wissen der Frau aufgenommen worden. Die auf die Fotos weißen Vorschaubilder hin, welche Automatisch erzeugt werden wenn mit dem Dateimanager ein Verzeichnis geöffnet wird welches die Fotos enthält. Eine Liste mit den Dateinamen aller Vorschaubilder ist in Unterunterabschnitt 4.3.2 zu finden. Beispiele zu diesen Vorschaubildern sind in Abbildung 2 zu sehen. Die Original Fotos konnten nicht auf dem Linux-System aufgefunden werden. Es ist zu vermuten das sich die Bilder in einem Verschlüsselten *Veracrypt*-Container auf Partition 4 befinden. Auf diesen konnte im Rahmen des Gutachtens nicht Zugegriffen werden da das passende Passwort für den Container nicht gefunden werden konnte und es auch zum aktuellen Zeitpunkt keine praktikable Lösung gibt das Passwort des Containers zu umgehen.
Außerdem befindet sich im Download-Ordner des Nutzers *olaf* auch das Bild *maxresdefault.jpg*, dieses zeigt eine Frau welche von einem Unbekannten Mann verfolgt

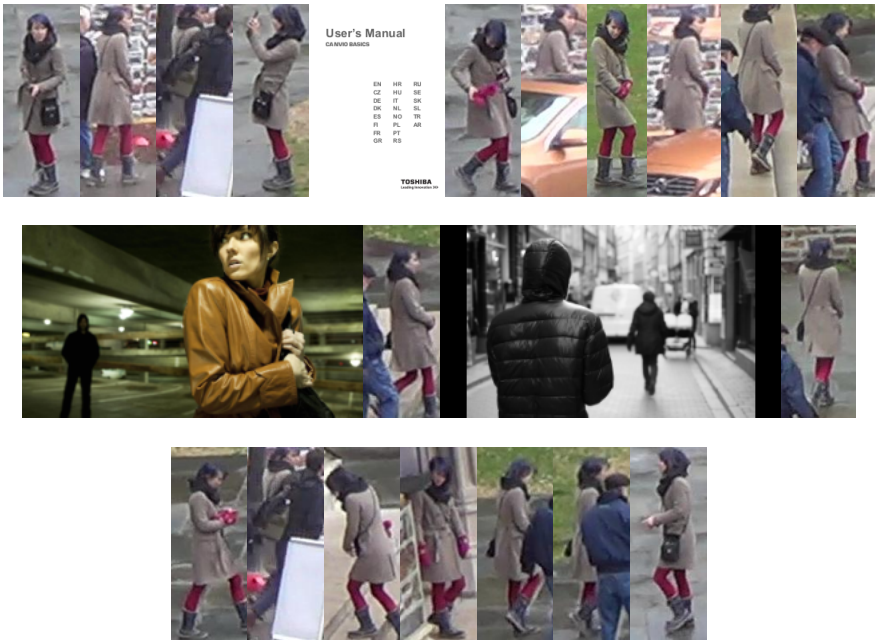

Abbildung 2: Examplarisch einige Vorschaubilder welche beim Nutzer *olaf* gefunden wurden

wird. Durch die Analyse der Internethistorie des Nutzers kann geschlussfolgert werden das dieses Bild aus dem Internet heruntergeladen wurde, es finden sich einige Bilder mit ähnlichen Motiven im Internetverlauf des Nutzers (Details dazu in Unterunterabschnitt 4.3.1).

b) **Nachweis der Nutzung/Verbreitung**
Die Historie der geöffneten Programme des Users *olaf* legt nahe das die Bilder *Stalking.jpg*, *maxresdefault.jpg* und *anti- stalking-gesetz-500x334.webp* geöffnet wurden. Auch das der Veracrypt-Container, in dem weitere Bilder vermutet werden, geöffnet durch den Nutzer *olaf* wurde ist in dem Protokoll festgehalten (vergleiche Unterunterabschnitt 4.3.3).
In der Internet Historie von Nutzer *olaf* findet sich eine Suche nach „picture upload“, aufgrund dessen lässt sich vermuten das der Nutzer eine Möglichkeit gesucht hat Bilder im Internet zu speichern oder über das Internet dritten zur Verfügung zu stellen. Es finden sich aber keine weiteren Hinweise zu einem solchen Versuch Bilder zu verbreiten.

c) **Extrahierung der elektronischen Kommunikation (E-Mail, Chat)**
Es konnte keine elektronischen Kommunikation auf dem System festgestellt werden.
Mit dem Nutzer *olaf* wurde die Socialmedia Plattform Facebook besucht aber ob der Nutzer einen Account bei dieser Seite besitzt konnte nicht festgestellt wer-

den. Ein solcher Account ist notwendig um mit anderen Mitgliedern von Facebook in Kontakt treten zu können. Der Nutzer *pc* hatte eine SSH mit der IP-Adresse *192.168.122.1*. Der Inhalt dieser Kommunikation konnte allerdings nicht rekonstruiert werden.

4. Befund

Im folgenden sind alle aussagekräftigen Rechnernutzungsspuren aufgeführt welche aus dem Festplattenabbild extrahiert werden konnten. Die Befunde sind untergliedert nach Nutzern. Es gab drei Nutzer auf dem System welche sich einloggen konnten, *olaf*, *pascal* und *pc*. Die meisten Nutzungsspuren finden sich beim Nutzer *olaf*, der Nutzer *pascal* wurde nur genutzt um die Programme *keepassxc* und *veracrypt* zu installieren. Der Nutzer *pc* wurde angelegt aber es wurde sich nie über die Benutzeroberfläche eingeloggt. In Abschnitt 4 findet man eine Liste aller Nutzer mit ihrem Heimverzeichnis und ihrem Passwort.

#	Nutzer	Passwort	Heimverzeichnis MD5
1	olaf	EiShaev2	/home/olaf
2	pascal	Ekee5Eng	/home/pascal
3	pc		/home/pc

Tabelle 3: Vorgefundene Benutzer

4.1. Dateisystem

Bei der Analyse des Systems (siehe Unterunterabschnitt 5.1.2) wurden folgende Partitionen gefunden:

#	Partition	Dateisystemtyp	Größe	Hashwert
1	BIOS	mbr	1MiB	
2	EFI	fat32	513MiB	
3	Linux	ext4	21.5GiB	6a0f7a571bdc1c115438d74618d31795
4	Windows	NTFS	9.3GiB	06eb47519040dac1a411d7b0297911e6

Tabelle 4: Dateisystempartitionen

4.2. Nutzer *pc*

4.2.1. Befehls Historie

Die Historie der in die Kommandozeile eingegebenen Befehle des Nutzers *pc*. Extrahiert aus der Datei */home/pc/.bash_history*.

```
sudo add-apt-repository ppa:unit193/encryption --yes
sudo apt-get install veracrypt
sudo apt-get install keepassxc
cd ~
ls
```

4.3. Nutzer *olaf*

4.3.1. Internet Historie

Internet Historie aus dem Firefox Webbrowsers des Nutzers *olaf*. Extrahiert aus der Datei */home/olaf/snap/firefox/common/.mozilla/firefox/b7q08ugf.default/places.sqlite*.

URL	Title	Zugriffsdatum
`https://www.mozilla.org/privacy/firefox/`		04.07.2022 20:54:49 GMT+0200
`https://www.mozilla.org/de/privacy/firefox/`	Firefox Datenschutzhinweis — Mozilla	04.07.2022 20:54:49 GMT+0200
`https://www.google.com/search?channel=fs&client=ubuntu&q=picture+upload`	picture upload - Google Suche	04.07.2022 20:58:47 GMT+0200
`https://www.google.com/search?q=picture+upload&client=ubuntu&hs=iup&channel=fs&source=lnms&tbm=isch&sa=X&ved=2ahUKEwiakLqb9d_4AhWLhP0HHTL2A3QQ_AUoAXoECAEQAw&biw=950&bih=656`	picture upload – Google Suche	04.07.2022 20:58:52 GMT+0200
`https://www.google.com/search?channel=fs&client=ubuntu&q=People+search+engine%22`	People search engine Google Suche	04.07.2022 20:59:27 GMT+0200
`https://www.lifewire.com/search-engines-that-top-the-web-3482269`	8 Best People Search Engines You Can Use to Find Anyone	04.07.2022 20:59:35 GMT+0200
`https://www.facebook.com/`	Facebook - Anmelden oder Registrieren	04.07.2022 20:59:48 GMT+0200
`https://www.google.com/search?channel=fs&client=ubuntu&q=Stalking+pictures`	Stalking pictures - Google Suche	04.07.2022 20:59:35 GMT+0200

https://www.google.com/search?q=Stalking+pictures&client=ubuntu&hs=2vp&channel=fs&source=lnms&tbm=isch&sa=X&ved=2ahUKEwib6sLC9d_4AhXV7rsIHfZ2AmwQ_AUoAXoECAEQAw&biw=950&bih=656&dpr=1	Stalking pictures – Google Suche	04.07.2022 21:00:12 GMT+0200
https://www.google.com/imgres?imgurl=https%3A%2F%2Fwww.polizei-beratung.de%2Ffileadmin%2FBilder%2FOpferinformationen%2Fstalking-nachstellung-opfer-infos-hilfe-2.jpg&imgrefurl=https%3A%2F%2Fwww.polizei-beratung.de%2Fopferinformationen%2Fstalking%2F&tbnid=1VJ4FsHfLPBBaM&vet=12ahUKEwiYndjD9d_4AhUNWxoKHUj3DOAQMygAegUIARDUAQ..i&docid=bn-ggSaPcymaWM&w=591&h=372&q=Stalking%20pictures&client=ubuntu&ved=2ahUKEwiYndjD9d_4AhUNWxoKHUj3DOAQMygAegUIARDUAQ	Stalking pictures - Google Suche	04.07.2022 21:00:17 GMT+0200

https://www.google.com/imgres?imgurl=https%3A%2F%2F378636.smushcdn.com%2F2450221%2Fwp-content%2Fuploads%2F2021%2F09%2Fanti-stalking-gesetz-500x334.jpg%3Flossy%3D1%26strip%3D1%26webp%3D1&imgrefurl=https%3A%2F%2Fwww.strafrechtsiegen.de%2Fverschaerfung-des-anti-stalking-tatbestandes%2F&tbnid=APvw4TruAs_JOM&vet=12ahUKEwiYndjD9d_4AhUNWxoKHUj3DOAQMygDegUIARDaAQ..i&docid=bepYDAWoQjFzfM&w=500&h=334&q=Stalking%20pictures&client=ubuntu&ved=2ahUKEwiYndjD9d_4AhUNWxoKHUj3DOAQMygDegUIARDaAQ	Stalking pictures - Google Suche	04.07.2022 21:00:22 GMT+0200
https://www.google.com/imgres?imgurl=https%3A%2F%2Fi.ytimg.com%2Fvi%2F92ItpmV_Rt4%2Fmaxresdefault.jpg&imgrefurl=https%3A%2F%2Fwww.youtube.com%2Fwatch%3Fv%3D92ItpmV_Rt4&tbnid=IU45j9vwCIDKsM&vet=12ahUKEwiYndjD9d_4AhUNWxoKHUj3DOAQMygEegUIARDcAQ..i&docid=fV9OObxYfQLzPM&w=1280&h=720&q=Stalking%20pictures&client=ubuntu&ved=2ahUKEwiYndjD9d_4AhUNWxoKHUj3DOAQMygEegUIARDcAQ	Stalking pictures - Google Suche	04.07.2022 21:00:24 GMT+0200

https://www.google.com/imgres?imgurl=https%3A%2F%2Fimg.welt.de%2Fimg%2Fwissenschaft%2Fmobile142393936%2F2981357647-ci16x9-w1200%2FStalking.jpg&imgrefurl=https%3A%2F%2Fwww.welt.de%2Fwissenschaft%2Farticle142393938%2FWen-sich-Stalker-besonders-oft-als-Opfer-aussuchen.html&tbnid=20W6qa8IoD5v2M&vet=12ahUKEwiYndjD9d_4AhUNWxoKHUj3DOAQMygFegUIARDfAQ..i&docid=GahHUF_hgIiAkM&w=1200&h=675&q=Stalking%20pictures&client=ubuntu&ved=2ahUKEwiYndjD9d_4AhUNWxoKHUj3DOAQMygFegUIARDfAQ	Stalking pictures - Google Suche	04.07.2022 21:00:27 GMT+0200
https://img.welt.de/img/wissenschaft/mobile142393936/2981357647-ci16x9-w1200/Stalking.jpg	Stalking.jpg	04.07.2022 21:00:39 GMT+0200
https://i.ytimg.com/vi/92ItpmV_Rt4/maxresdefault.jpg	maxresdefault.jpg	04.07.2022 21:00:46 GMT+0200
https://378636.smushcdn.com/2450221/wp-content/uploads/2021/09/anti-stalking-gesetz-500x334.jpg?lossy=1&strip=1&webp=1	anti-stalking-gesetz-500x334.webp	04.07.2022 21:00:59 GMT+0200

4.3.2. Vorschaubilder

Liste aller Vorschaubilder des Nutzer *olaf* im Verzeichnis */home/olaf/.cache/thumbnails/large/*. Diese Vorschaubilder werden beim Öffnen des Verzeichnisses, das diese Bilder enthält, vom Datei-Manager (Nautilus) erzeugt.

#	Dateiname	Hashwert (md5)
1	0094a4b74ed34d78cb5d5f00314b5d2d.png	53ee5adb4eaa7a592cd897083f966046
2	0106e31c70f6b9de2c4799ffda30bb4d.png	a99c34b314621af363541a6306a23956
3	02bd16d2344c9f487faef0307d33ceae.png	2977554313d9f5271d07a2481ab7e4b2
4	02f20ddeed282eb100be9c9dd67ebc63.png	e4fc0d226b0c162003ef3c1d865210cd
5	04c44fd862f5e549cd07b500c0905daf.png	c9022e7a2b42bcdbb5222b0fad1c4926

6	069d72d1481020f4c074ec2d7a7ac917.png	065f3e68e825cf3892f914dba6c48683
7	06cb468a77b541acae822d9302d92670.png	878dc0f435a4f38fa0d9f7492fe0c7ce
8	08924052760a89d0bec48da2ebce817f.png	aeaacdff349ddaca1037a1de57079bca
9	0ed76b47cf31b14d2b4f05527a15478c.png	b8014ccabc8497dcadb0757349dcd231
10	10e5a7e70a91f8115a1ae8985c6fdb1f.png	b4f595e593490007bd24568979cf4e10
11	118c34eb2ecb31a7905ea7628ae44303.png	89845ec3006bd05d86d8c664568d7aa6
12	11d19b274daeeb282bb3f8df2332cb3d.png	8346b5a1dec688031b6a1bd0a1519fa2
13	13d1475d3ca1052238816e811a8388a5.png	cafbd7b16ae44d605ed18f26d8c35b39
14	16dd145492e21569dce86953a31fb0aa.png	f517258521c1cc1f6f281915326eea1a
15	1895698c570a89cfc17cc5e745e346db.png	eed24182c26606bf01b5cf6fae8c2dac
16	18f4e1a56e9037a80a630ead24d66406.png	721b24dd73fc3bf4ed8eaa077c972a8a
17	1a703ce854335fe8ccd8b08f463824f5.png	737e6b533302fb663bc31e57c770691d
18	1fa3eb0bd0a47ecf098884bafa54d40c.png	70309fedd60cbcf52287cf0ee951a084
19	2185d774891a67b25a9886ac8fd21e5e.png	86fc0a68d903e55bcc9030322fa7f9cf
20	22f995ba88f3f041524d527ec3ceb15c.png	32afcf58399eb993c9884f41982f264b
21	2502a254e235d5b47ba1e58d48fa6f8c.png	e9d680b7b1e32c72a8b49810af277bd2
22	28cf86e094576accc11848638ec59b29.png	af61d66bc7c79b29f7fd54cf0b89f977
23	298fb7e13e667a5e7187aeede5f0264f.png	a9855d0a1c21e24cb6b6e6013f8aafd0
24	2a2f2254e1b9ba624ea9a4e6fb15c55b.png	3d3d8ed3565028ee82c62bac481d5382
25	2a4c73997d7d4a106bbdbaff075a4ffa.png	617f7caa11b51fd11495b016be0db4e2
26	2dde2bda1e693b202bb2438f8f3ad9f6.png	304e3f2f3eaae265217537f9f053ce6e
27	2e1ff5d4636e7fb9e7c7a408937a4ae4.png	0233688f61af3d62f488cee598c3ad7f
28	301dd3879075b46660f4b8b5dcf46d29.png	9dcc44b000bb53dfd81e67d672db39ce
29	308b5035c3c6b2bb2a053d3c6e67e811.png	0b85c00266ef8ac3f2501a3ca8132621
30	332f2774500099c31c2ca737f8c2d799.png	c1f6192b14a34e6570ec0e10d6b0c315
31	355f50dcb3dbacb5276a943dcca3c1b3.png	c5cb22db945246aa97b71e3a697d61a9
32	358eacd4db6fcdc14c8986601d1def91.png	83da1686361cc64ce98cf77e73769b40
33	360f28ce83c4ba72d3be15003f088fab.png	9da724df0e9353afe201aba5a918dd7c
34	37c7034bad5f06138fa72d11c7890f25.png	3352cb0eeafa8a8cb37036d3aca7d516
35	3a4cbbd06146f6e44665497a6ed31cb4.png	8da128c0489789db9a18a5bd2e842522
36	3aad25e29eeaa3ba555278dc722127ca.png	014cea3da0ffefc982c7c64750a65020
37	3b8541b53886f537d3fc56af7d8bb52b.png	15d1621a0e0380f0885715b1fcb44e92
38	3bff7f08ad5d29f82be80e10637c3cb9.png	5c33bb66d59746b73e99e8e20a04374f
39	3db9276fb19402dd8d3885bbb932274e.png	7ef92b4bdf0245162ebfca2ddc1d48f1
40	3eae9b804d8607b04b23cc25ccc9a547.png	7f7ff4b8a78ba0761955018cdf956146
41	3f0947fdb6851e432f3b32bdf6050067.png	e867b5c0b4ac744f3a5c963d0e9bf22a
42	3f38a85fe8410b5f3911bd56bda3924e.png	8cbba981c966733cdc5b09fd3c37358e
43	3f3df9c84092cdccd9b9e365d9869ad8.png	f7810fbb3841ec2e27eb503f546f6ae2
44	4114f03b3f916479431df18f0d3be139.png	e71fd26f5c42cd68e9ad92b492c7ed57
45	429055223d13819a7f3504d71754a42b.png	ebf530c7e9d447042b59318e631466a4
46	43907d5648a359597e0ac258196575f2.png	9d3e8311181da8bcd033d84d3a90b5ce
47	4501f4335c8bf718e47a6b81eea3dffe.png	31121bfaba355763b0059d3b5efb048c
48	455648512573db351eed96663dbb0e1e.png	5b8ec5024eec977d2b6188d534b0b91b
49	4b6c9d6516afaf34dd5dcb9596465101.png	ccebb1fb1f67a6c6bac0c68875b581d7

50	50482b3c5a39608609eec1e08966e6fc.png	e901e7597258b7b3132e3d1e5f156c2c
51	547aa01766b74b09336aedab547b1215.png	f20d231dadb00d8ac6f99a1f603c0e8f
52	5694e186d9bf4da415a82ec911250060.png	e425c6c6bf66170785db56c2c4f0028e
53	58556becb3ef05b1fe5d8f3fce8907cf.png	e722b99cd4dd9e775cc1b5c59a7d4d7e
54	5b98889bf75ba016387d425aa38f51fb.png	b65a64eeeb9801495e6fc1fb58479502
55	5d6363255e5218725f3407cf327aa0f1.png	4d38497f04f7a0659fc6d38bfda71d8a
56	5e6205d42e724cd5aab85678883111ce.png	6d01a903024797042980c332bdc0f861
57	61ab7df059f9927e89950f5d944ec681.png	cb8e4873cf9c0d9c17b542d9e48127cb
58	637c40d8864d1aac51dafdd990a9e550.png	c3b60c41f801b7fdb075d4921b9a65bd
59	6461fca17a0b8cb7100dcb9ad223b0a7.png	b4ca63a64a346ab3eb6970174380b003
60	64d284a3ec75a4eb35d22d5f20a95b11.png	7ed59fdd0f5002988bdf7272580a18c2
61	64eceaf4a67f6785e5fe7a4e4258aa78.png	664ab5491cfb6a2eb97ae9329ab17e4d
62	654300da6cfff727c884ace3dade7003.png	dcaa427a3627289fb0429ef4ec377d26
63	66675bd5a2581b190940c4ade2d20364.png	4a8cef2fe80093356f83d8dac2f7d93e
64	68c0a6c338e12c4724e2bd10a89ee3d3.png	b7c1656c67127f7d93dde91c8acc03f5
65	6a4d147c5167fd74bc3b7cce557c5925.png	800b55c16c99022de2aba0c5c25105fa
66	6a665aa007d0265a3d188fa474ce243c.png	8abef8c13577c236f593ec013b49a89f
67	6c3d18fa8becd74dbba124f2c45293b3.png	0ee2d480cc446dd1778099c1740d8b2d
68	6e5e7fca52bf24a787167bfe9dc86901.png	f10d7bc4b862e441615d3a24443594cb
69	6f70cfc46918825dfa5f114960159c5b.png	5f3279e450c4752fd1941ba5394a58f0
70	6fd0a7846d766b3c790c49a62a4fe9f3.png	776c2f47d2307960133f94d74293f6ec
71	710531bb719d369e647da1a67f82e6f1.png	6a53e2cadb00ef04acb03cf357ef3d9f
72	712af6eddad5a9950126cd29a27fd923.png	7c1b186630afa93a6cf5af9527d1de95
73	71400d0a86ba11c26b9d2eef864c2625.png	fb6ab922244d038f7ebec77f992d6936
74	7170719ab7c3de0732390d5c7e10a401.png	50ab62dc4571b2bf4e092190ba50ea28
75	71e1ed2abbdd8480842d0146d40618f7.png	c969a11b1f9bc89e041c89048578fcc0
76	79b9d537e2063082e8249c4b7a4b14a2.png	a1b8bd3d80e165f77d47704c46c66c97
77	7f63401bf5c2cc0ed5e47ce028cf4bdb.png	5a9ec8b45275d5c6405475fab1e3b23f
78	80b362f3cea9fc080b7dd3fa7f3c4498.png	e8ccae4bab2b24b682b4c0a9f32ec4b8
79	826255cdf80eb8d4455c2149f578bb56.png	eca4fba898cef0a4fcebc2164da146c0
80	82e55ba364d2f511383fe6f2d7a71abf.png	d35c5417f9b27fc1db250ee91733b7bd
81	8484b2f45da86504bfe9ced7be8d4e40.png	b9fdfea63bd560c4025c95af4f12b940
82	889677202e67cb3dc45d7e0d1d2f04b9.png	1506f4aed1b4277df36de87fb2e45e8f
83	8a0447cc662f6599c78eda833cabc274.png	b12fd44fddf0b046388027408a002f8f
84	8bcb18ab9b2c8018591a856739324738.png	b4c37271d8bbf02b4b4a6a45d23a71aa
85	8be06fd642b1fcb8d2e5c03f47bdbd7a.png	8c2aa77350454bca0885265e09e547b4
86	8d522e4195c20831ab8badb78cbe1a83.png	75106e9ff52b1a93d189a31058bae312
87	9429336d57786abb9983cf61f0d54973.png	497e5c323368f9e5d4b9a87d7d08db47
88	95d711aa9d13aa561ce8a6f167be9ad0.png	fd8163a42fe7888543cbb8b5e9865f2a
89	9663125741cbfbbd286726b00cd3f241.png	f0ae0f47573840775db82668949806c6
90	96ba941af1fd655a5e7b0dd3d6ed846c.png	23dee9f57f3a3a9e09fc847798f40a4a
91	9effe3603a352fb932a23e65ed030da8.png	07aca92954a8c7ba3429f0e8716c375d
92	9f59a34208a949af8618c3e4f259b25f.png	b99b645a75c4f36778e379a6072939dc
93	a4ed887e2824f71511045825728d697f.png	3924e006c8ede679bd3447bfbd34548c

94	a7ccece387ac9c3c55ba940aeb6cea17.png	10682beb2b1fa8f2c99990df97e49af5
95	a80d43ab0dd88c9cff11eccd951d20f9.png	39138c1451cd943f3fb727770b8d6811
96	aca8e3593a32274604e8e543d362bb0f.png	204e5928ea40432b8cc417f80f9d29ab
97	ad9c31d0f9e874adf2d54037eb2638cc.png	74fd1feca119fd345191a830fe89e49d
98	af4ab3e0a04d85fcfa1d5716e4e3b12e.png	173d618c57ca70f9e4e7562553e5fcd3
99	b075fec4cff11c4292c73ed797140972.png	a87b8df47d0d38a7a1094c1a266e6aad
100	b141c22bc5141c331f99b96218cb7c46.png	e97e37f0b2cb7955679b3cc24796c316
101	b2478e59528f2771ba35c12a6fe0afd0.png	63fac43db706495d7a23380090b668f3
102	b89c3a07489449ed2634312a2a02fb82.png	a97661ea906d2e1fe5e497773c7be381
103	baff90c7de109e29f21686370903c80f.png	02d984f96e53979853e74295da902c59
104	bb8bb510181801f19014f9bc0fd78132.png	18d39070e1af4b07431838180d617a93
105	bd700ac1d25198cb583de8c1b891fa61.png	6add0a143dade240a9e2c1487588d10d
106	c0ac8ff827e68d1ab78f65fa91c00988.png	6002513ad10825e6cc9b15506117ec3a
107	c2d4b723031c13b01bc75477b6bb8093.png	11d0cdf96bb2ab3b85b30eaee751a0a0
108	c5fae6405f94fa53ecd30d898eb6e42f.png	9162e50b00081ce69366676c66f6cdd0
109	c73e21a11c8dc3bba5ae549c3a38dc90.png	94393604a09a7de6b9b1f9c03ff06314
110	c949fe531fa66c81d219290ac957ba82.png	05cc545230b30d1f2ae4f56326fa5cf1
111	ccf14e81491c817e8ff585782464197d.png	fa9a994812c98628dc9756c1ab67c2d1
112	cd9ec964e18023a97f953a054e792314.png	b0a369f96caade28c034a9a6191fb4b6
113	ce73b65efadda14715936098768bc747.png	c4641998502881547019dab68d45dfaf
114	d02746e20cacf4e3236088e33f61784c.png	b77790a70158be526048e967ac28ac57
115	d26dba9609829209ac5f01358bf4727e.png	dcc0f4f4584a930e447a0d6d9cbdcf38
116	d2b6a014c20117a78daac610d095da88.png	c18bc4ec6d1c1f7aca5842860ee69b4a
117	d43295d4cd8e8ec08a741dff0115e2e8.png	15ef0acc8d07856065204846faf666b3
118	d9477fcecd35426c593e736a5b22433e.png	bdd5787547a346d0f58eea726d9cc13e
119	d94bfebe5c528be69d631dbf0ff7771f.png	59c8d1beb5a4b3ce44d1a2e6d49ce339
120	d95d3d170b14ad25c04ebb0f6bb5300f.png	b12d43b024a7533c8b2f6fedd2478513
121	d9a45079bacb0813e8a786d636d3df16.png	4e2bee9532dedb9ac0f49f918e959c38
122	d9ef4d2eb1c4f7ac87ad7aae713ed095.png	8b9e1fafbb036f622622acaca3875501
123	da1299152955a3e714300f19d3241d98.png	6b5b9002a16b2549a8c601750deed4a6
124	dd5d25693279c10dad327b541b7f5d88.png	58fee2cdb005fc8bbcd9c129e8cc8a1a
125	e2180707cf3770acdcfbb2e1df568065.png	bc628e8d24db439dca7468273fdd4194
126	e2720c20b69cd99c0441f482529f8589.png	c92cd1359e40c69e7b70f48a2f139d86
127	e31245758a04a2a2376ffc39114e52d8.png	6ce5b0335d6a32eb75b581d5a82ddb3c
128	e37e819bf4f8a163c526f46efc3e46ef.png	8a3960a618a90fb8d7db38446bb4e2f0
129	e505ef912f71a4306e830b032189d6a6.png	424c0bb276fbc10de0f08619f610acbd
130	e5954dc9fee0ac1ce9014206c0527aa0.png	5e77e4a0fbc84cec28d271ae807ea154
131	e59ac6cbe82c2ceba7ce36bc36b23a13.png	711ac4e720684d19a0f74a167439adf9
132	e65cb5b38bf05134f838298c0d51cb09.png	d39849a93bc66f40e85c5cce213a40ad
133	e69e8dd80091be540a9e64d4b7019244.png	e18c2138e551523fe1965758bd5c8173
134	e7a227bc4428345ba8d360f970afdf99.png	19ff82c2567dcf8daaaf4f89a68b1013
135	e8466162462c83ce0909bf1bf5b75b3c.png	16a63606813e5d494fcdad2b5d6b6359
136	e852032a961bba2ba6391be8e05aa6fa.png	41170145679403c14de109df4a7b940e
137	eb0d21492d8db5c4c2d253efa2bb9742.png	2c0321785403e44815f50281dece2c7e

138	eb3ce5b9082e075f4fa46bfa9fa629fc.png	4d2a2bfe229823e9191b78bb053f1ffe
139	ed49fcc6ba1ddf4e96c1afd1218705d3.png	eebde8e39d69bd191df6e91611f842c9
140	f0b2c280a4e030f17640ac6bf6261931.png	35234bf7ff3a69dd517031cba116ca34
141	f0f2e4af30faf9768b449944b1624d84.png	60cc7fc441a228296fded091af5eb642
142	f1318696b01db18d91c5cf9be0f08a11.png	82a611b13d8f8ae30431a2c9b51e653f
143	f2d5a8639f52a98b53849edf4c129c78.png	44905edf9a1a9a9afde1f77f0ef3965f
144	f2d7633da25b75ecbdef63cc8c488bfd.png	582f5f15977c6ec439e88c23b6ba3aa8
145	f2f67317e479f5556b0392acf7c4aa5b.png	59c9d0d01d3e808e8c6f8563b07ec253
146	f40e6ccf669df4fcc47a9c6a382226a9.png	fdb1c166848a090935f1b28f5c7a1187
147	f5bfd2d43e713a89ecc4983bc331eab1.png	89e5a9e147ce1766ef5964101f54f2ab
148	f5f82f9d7aba54ccf37214eaeb356f17.png	08a4e69604eb176cf3e14b98a80935e7
149	f64480439eea12f523a2ac5367253355.png	f8d7db1751b35e0c54002608ef3939e8
150	faa826ed3d34aae8316331588db74112.png	01c5fa91e797612ef9c6a891e02d804b
151	fc2c421153fd160c72ebdd6d3138c2bd.png	ffa1bb223377f748c4fc809626dbd499
152	fc5d5307374c3ce99fc1fc9d0445c4fc.png	d73027d9f382c4e57b80de1490a81438
153	fcb3a73f60a266831ef2bc6a1a669917.png	125d4eadccb6dae1f56a5a2610842499
154	fdb5d71798a660d487fa70896f0d8e22.png	6016dd0efa0632a61aacaddaa86d1867
155	fec29173bd89a86aa780e8310dc45ab7.png	ab47ff476dc38668766bf7352992faa3

Tabelle 6: Olafs Vorschaubilder

4.3.3. Nutzungshistorie

Der Verlauf der vom Nutzer *olaf* geöffneten Programme. Extrahiert aus der Datei */home/olaf/.local/share/recently-used.xbel*.

Dateipfad	Dateityp	Zeitstempel	Programmname
/home/olaf/Passwörter.kdbx	keepass database	04.07.2022 18:53:55 GMT+0000	keepassxc
/media/olaf/028AA54C0562CCCE/porn/newStuff/XXX	varacrypt container	04.07.2022 18:55:44 GMT+0000	veracrypt
/home/olaf/Downloads/Stalking.jpg	image jpg	04.07.2022 19:00:38 GMT+0000	firefox
/home/olaf/Downloads/maxresdefault.jpg	image jpg	04.07.2022 19:00:46 GMT+0000	
/home/olaf/Downloads/anti-stalking-gesetz-500x334.webp	image webp	04.07.2022 19:00:58 GMT+0000	
/media/veracrypt5/neu	veracrypt decrypted container	04.07.2022 19:01:48 GMT+0000	nautilus

Tabelle 7: Verlauf der aufgerufenen Programme durch den Nutzer *olaf*

4.3.4. Websuchen

Die Eingaben in die Suchmaske der Google Websuche durch den Nutzer *olaf*. Extrahiert aus der Datei */home/olaf/snap/firefox/common/.mozilla/firefox/b7q08ugf.default/formhistory.sqlite*.

Wert	Zeitstempel
picture upload	04.07.2022 20:58:47 GMT+0200
People search engine	04.07.2022 20:59:27 GMT+0200
Stalking pictures	04.07.2022 21:00:09 GMT+0200

Tabelle 8: Eingaben in der Websuche durch den User *olaf*

4.4. Nutzer *pascal*

Für den Nutzer *pascal* wurden keine relevanten Rechnernutzungsspuren gefunden.

5. Methodik

5.1. Festplattenabbild

5.1.1. Herstellung der Kopie

Berechnung der Hashwerte des original Abbildes.

```
$ sha1sum /run/media/xe/TOSHIBA\ EXT/ForImage5.img
a25ab111c649c8f904e4804c2a62dc277b026ab9 /run/media/xe/TOSHIBA EXT/ForImage5.img
```

```
$ md5sum /run/media/xe/TOSHIBA\ EXT/ForImage5.img
6eb8d7ab10e54706d0ccb3966e041f7e /run/media/xe/TOSHIBA EXT/ForImage5.img
```

Anschließend wurde mit dem Programm *dd* eine Kopie des Abbildes erstellt.

```
$ sudo dc3dd if=/run/media/xe/TOSHIBA\ EXT/ForImage5.img of=/home/xe/ForImage5.img
dc3dd 7.2.646 started at 2022-07-06 13:18:43 +0200
compiled options:
command line: dc3dd if=/run/media/xe/TOSHIBA EXT/ForImage5.img of=/home/xe/ForImage5.img
sector size: 512 bytes (assumed)
 10944249856 bytes ( 10 G ) copied ( 100% ), 86 s, 121 M/s

input results for file ‘/run/media/xe/TOSHIBA EXT/ForImage5.img’:
   21375488 sectors in

output results for file ‘/home/xe/ForImage5.img’:
   21375488 sectors out‘

dc3dd completed at 2022-07-06 13:20:09 +0200
```

Berechnung des Hashwerts der neu erstellten Kopien, um die Gleichheit von Original und Kopie sicherzustellen.

```
$ sha1sum /home/xe/ForImage5.img
a25ab111c649c8f904e4804c2a62dc277b026ab9 /home/xe/ForImage5.img
```

```
$ md5sum /home/xe/ForImage5.img
6eb8d7ab10e54706d0ccb3966e041f7e /home/xe/ForImage5.img
```

5.1.2. Analyse der Festplattenpartitionen

Aus der *Magic Number* (*5146 49fb*) von *ForImage5.img* kann man erkennen, dass es sich bei dem Image um eine *.qcow2*-Datei handeln muss.

```
$ xxd ForImage5.img | head -10
00000000: 5146 49fb 0000 0003 0000 0000 0000 0000 QFI.............
00000010: 0000 0000 0000 0010 0000 0008 4000 0000 ............@...
00000020: 0000 0000 0000 0042 0000 0000 0003 0000 .......B........
00000030: 0000 0000 0001 0000 0000 0001 0000 0000 ................
00000040: 0000 0000 0000 0000 0000 0000 0000 0000 ................
00000050: 0000 0000 0000 0001 0000 0000 0000 0000 ................
00000060: 0000 0004 0000 0070 0000 0000 0000 0000 .......p........
00000070: 6803 f857 0000 0180 0000 6469 7274 7920 h..W......dirty
00000080: 6269 7400 0000 0000 0000 0000 0000 0000 bit.............
00000090: 0000 0000 0000 0000 0000 0000 0000 0000 ................
```

Das *.qcow2* Format wird für die virtuellen Maschinenvolumen des QEMU-Emulators verwendet. Das *.qcow2* Format kann mit dem Befehl qemu-img in ein *.raw*-Abbild umgewandelt werden.

```
$ mv ForImage5.img image.qcow2
$ qemu-img convert -p -O raw image.qcow2 image.raw
```

Mit den Werkzeugen *fdisk* und *parted* kann man feststellen, welche Partitionen im Dateisystem von *image.raw* vorhanden sind.

```
$ fdisk -l image.raw
Disk image.raw: 33 GiB, 35433480192 bytes, 69206016 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: 7AB35F56-8FB0-407B-AC62-FD7C3E10AB6A

Device       Start     End  Sectors Size Type
image.raw1    2048    4095    2048   1M BIOS boot
image.raw2    4096 1054719 1050624 513M EFI System
image.raw3 1054720 46135295 45080576 21.5G Linux filesystem
image.raw4 47851520 67383295 19531776 9.3G Microsoft basic data
```

```
$ parted image.raw print
WARNING: You are not superuser. Watch out for permissions.
Model: (file)
Disk /home/xe/image.raw: 35.4GB
Sector size (logical/physical): 512B/512B
Partition Table: gpt
Disk Flags:

Number  Start   End     Size    File system  Name                  Flags
 1      1049kB  2097kB  1049kB                                     bios_grub
 2      2097kB  540MB   538MB   fat32        EFI System Partition  boot, esp
 3      540MB   23.6GB  23.1GB  ext4
 4      24.5GB  34.5GB  10.0GB  ntfs         NTFS                  msftdata
```

Es wurden Kopien von Partition 3 und 4 angefertigt da die Partitionen 1 und 2 nur BIOS und EFI enthalten und deshalb für die Untersuchung nicht von Interesse sind.

```
$ dd if=image.raw of=linux.ext4 skip=1054720 count=$[46135295-1054720+1] conv=notrunc,
    sync,noerror
45080576+0 records in
45080576+0 records out
23081254912 bytes (23 GB, 21 GiB) copied, 104.566 s, 221 MB/s
```

```
$ dd if=image.raw of=usb.ntfs skip=47851520 count=$[67383295-47851520+1] conv=notrunc,
    sync,noerror
19531776+0 records in
19531776+0 records out
10000269312 bytes (10 GB, 9.3 GiB) copied, 38.715 s, 258 MB/s
```

Berechnung der Hashwerte der zwei extrahierten Partitionen

```
$ md5sum linux.ext4
6a0f7a571bdc1c115438d74618d31795 linux.ext4
```

```
$ md5sum usb.ntfs
06eb47519040dac1a411d7b0297911e6 usb.ntfs
```

5.2. Ermittlung von Passwörtern

#	Nutzer	Hash Funktion	Passwort-Hash
1	olaf	SHA-512	6mysalt$a9KjYIIO12xnzJdf5nnqUcsgvMZNreLZLyGgL9vPzlYKKNRkQT53cWCSPqIZGcgkdtCr8/m19HCSjQI4GsjV.0
2	pascal	SHA-512	6mysalt$pSsKOuVGAuqXvu3CaIy5uK97KiBjz/N1rDzOq4/waPCfr0SS76VLL2AgzS5gne7RhzYjFxQfndu3.SSO1YU2a.
3	pc	yescrypt	yj9T$graH6StsN64vZy4TX6DLO1$jFAPKwPTtCP25YeK6fiAIcbse.xZb3XaFXnIuwfaej4

Tabelle 9: Benutzer Passwörter Hashwerte

5.2.1. Ermittlung der Passwörter der Nutzer *olaf* und *pascal* mit dem Werkzeug john

Zunächst werden die Nutzernamen und Passwort-Hashes zusammengeführt mit dem Werkzeug *unshadow*.

```
$ sudo unshadow /mnt/linux/etc/passwd /mnt/linux/etc/shadow > ~/unshadow.txt
```

Dann kann damit begonnen werden die Kennwörter mit einer Wörterbuchattacke zu ermitteln. Dazu wird die mit dem Asservat übergebene Passwortliste *wordlist.txt* verwendet.

```
$ sudo john unshadow.txt --wordlist=wordlist.txt
Using default input encoding: UTF-8
Loaded 2 password hashes with no different salts (sha512crypt, crypt(3) $6$ [SHA512
    128/128 SSE2 2x])
Cost 1 (iteration count) is 5000 for all loaded hashes
Will run 4 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
0g 0:00:00:16 0.14% (ETA: 19:53:10) 0g/s 521.4p/s 521.4c/s 1042C/s see7Thu9..iemoo6Do
0g 0:00:04:11 2.11% (ETA: 20:00:23) 0g/s 522.4p/s 522.4c/s 1044C/s hohx6Cai..Ahn5oi5u
0g 0:00:04:47 2.40% (ETA: 20:00:37) 0g/s 522.4p/s 522.4c/s 1044C/s oVeh1ib6..nai0Je9o
0g 0:00:04:48 2.41% (ETA: 20:00:38) 0g/s 522.4p/s 522.4c/s 1044C/s Quuoz1mo..AhKah4mi
EiShaev2       (olaf)
Ekee5Eng       (pascal)
2g 0:03:59:25 DONE (2022-07-24 20:41) 0.000139g/s 274.4p/s 274.4c/s 548.8C/s paigai0I..
    ieruJ6Ue
Use the "--show" option to display all of the cracked passwords reliably
Session completed.
```

Das Kennwort des Benutzers *pascal* lautet: Ekee5Eng
Das Kennwort des Benutzer *olaf* lautet: EiShaev2

5.2.2. Ermitteln des Passwortes von *pc* mit dem Werkzeug john

Da für das Passwort von *pc* ein anderes Hashverfahren verwendet wurde als für die restlichen Nutzer, wird dieser Hash gesondert behandelt. Zunächst wurde es versucht mit der gleichen Angriffmethode wie bei den anderen Nutzern versucht.

```
$ john --wordlist=~/wordlist.txt ~/user_pc.txt -format=crypt
Using default input encoding: UTF-8
Loaded 1 password hash (crypt, generic crypt(3) [?/64])
Cost 1 (algorithm [1:descrypt 2:md5crypt 3:sunmd5 4:bcrypt 5:sha256crypt 6:sha512crypt])
     is 0 for all loaded hashes
Cost 2 (algorithm specific iterations) is 1 for all loaded hashes
Will run 20 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
0g 0:00:00:44 0.27% (ETA: 11:22:06) 0g/s 377.2p/s 377.2c/s 377.2C/s eeBee8ji..eef4Goec
0g 0:01:21:47 29.11% (ETA: 11:28:41) 0g/s 370.7p/s 370.7c/s 370.7C/s ubah3OoW..thaiK3fe
0g 0:03:33:15 75.30% (ETA: 11:30:55) 0g/s 367.8p/s 367.8c/s 367.8C/s rei4eeLa..iPh7phai
Warning: Only 40 candidates left, minimum 96 needed for performance.
0g 0:04:41:48 DONE (2022-07-21 11:29) 0g/s 369.6p/s 369.6c/s 369.6C/s yuenai5A..Uu5achah
Session completed

$ john --show ~/user_pc.txt
0 password hashes cracked, 0 left
```

Das war erfolglos, das Passwort des Benutzers *pc* ist nicht in der *wordlist.txt* enthalten. Deshalb wurde versucht das Passwort mit einer Bruteforce-Attacke heraus zu finden.

```
$sudo john pc_hash.txt -format=crypt
Using default input encoding: UTF-8
Loaded 1 password hash (crypt, generic crypt(3) [?/64])
Cost 1 (algorithm [1:descrypt 2:md5crypt 3:sunmd5 4:bcrypt 5:sha256crypt 6:sha512crypt])
     is 0 for all loaded hashes
Cost 2 (algorithm specific iterations) is 1 for all loaded hashes
Will run 4 OpenMP threads
Proceeding with single, rules:Single
Press 'q' or Ctrl-C to abort, almost any other key for status
Warning: Only 90 candidates buffered for the current salt, minimum 96 needed for
    performance.
0g 0:00:00:12 76.77% 1/3 (ETA: 13:58:18) 0g/s 37.12p/s 37.12c/s 37.12C/s PcK..Pc69
0g 0:00:00:14 85.19% 1/3 (ETA: 13:58:19) 0g/s 37.60p/s 37.60c/s 37.60C/s Pc30..Pc77777
Almost done: Processing the remaining buffered candidate passwords, if any.
Warning: Only 58 candidates left, minimum 96 needed for performance.
Proceeding with wordlist:/usr/share/john/password.lst
0g 0:00:00:35 0.32% 2/3 (ETA: 16:57:36) 0g/s 37.63p/s 37.63c/s 37.63C/s brenda..keith
0g 0:00:22:49 31.81% 2/3 (ETA: 15:09:46) 0g/s 38.97p/s 38.97c/s 38.97C/s psycho6..koala6
0g 0:00:47:47 70.41% 2/3 (ETA: 15:05:54) 0g/s 39.00p/s 39.00c/s 39.00C/s Sierra8..Nancy8
Proceeding with incremental:ASCII
0g 0:01:12:17 3/3 0g/s 38.94p/s 38.94c/s 38.94C/s 083223..098616
0g 0:01:12:25 3/3 0g/s 38.94p/s 38.94c/s 38.94C/s annang..anitch
0g 0:01:12:35 3/3 0g/s 38.94p/s 38.94c/s 38.94C/s alinca..allina
0g 0:05:12:05 3/3 0g/s 38.63p/s 38.63c/s 38.63C/s 252435..252100
```

```
0g 0:22:35:42 3/3 0g/s 38.58p/s 38.58c/s 38.58C/s ljbjjs..ljbosi
0g 0:22:35:54 3/3 0g/s 38.58p/s 38.58c/s 38.58C/s ljb401..ljbloo
0g 0:22:35:57 3/3 0g/s 38.58p/s 38.58c/s 38.58C/s ljblom..ljbldi
0g 0:22:46:49 3/3 0g/s 38.58p/s 38.58c/s 38.58C/s bumsm..bln29
0g 0:23:09:29 3/3 0g/s 38.58p/s 38.58c/s 38.58C/s ceesin1..ceesoff
0g 1:00:30:10 3/3 0g/s 38.55p/s 38.55c/s 38.55C/s studgins..studguri
0g 1:01:42:44 3/3 0g/s 38.54p/s 38.54c/s 38.54C/s cmar24..cmal10
Session aborted
```

Nach über einem Tag Rechenzeit wurde der Angriff ohne Erfolg abgebrochen.

5.3. Ermitteln des Passwortes zu *Passwörter.kdbx*

Es wurde versucht den Passwort-Hash des Masterpasswortes des Passwortsafes *Passwörter.kdbx* zu extrahieren.

```
$ keepass2john Passwoerter.kdbx > ~/keepass.hash
! Passwoerter.kdbx : File version '40000' is currently not supported!
```

Das schlug fehl, es konnte auch keine alternative Methode gefunden werden.

5.4. Ermitteln des Passwortes des Veracrypt Containers

5.4.1. Extraktion des Veracrypt-Containerschlüssels

Zunächst musste der Hash zu dem Passwort des Containers Extrahiert werden, dazu werden die ersten 512Byte aus dem Container mit dem Werkzeug *dd* heraus kopiert.

```
$ sudo dd if=XXX of=vera_key.hash bs=512 count=1
1+0 records in
1+0 records out
512 bytes copied, 4.2123e-05 s, 12.2 MB/s
```

5.4.2. Ermitteln des Veracrypt-Containerschlüssels mit hashcat

Der extrahierte Hash wurde dann mit einer Wörterbuchattacke mit dem Werkzeug hashcat angegriffen.

```
$ hashcat -a 3 -m 13721 vera_key.hash wordlist.txt
hashcat (v6.2.5) starting

* Device #1: WARNING! Kernel exec timeout is not disabled.
             This may cause "CL_OUT_OF_RESOURCES" or related errors.
             To disable the timeout, see: https://hashcat.net/q/timeoutpatch
* Device #2: WARNING! Kernel exec timeout is not disabled.
             This may cause "CL_OUT_OF_RESOURCES" or related errors.
             To disable the timeout, see: https://hashcat.net/q/timeoutpatch
CUDA API (CUDA 11.7)
====================
* Device #1: NVIDIA GeForce GTX 960, 1497/1993 MB, 8MCU

OpenCL API (OpenCL 3.0 CUDA 11.7.99) - Platform #1 [NVIDIA Corporation]
=======================================================================
```

```
* Device #2: NVIDIA GeForce GTX 960, skipped

Minimum password length supported by kernel: 0
Maximum password length supported by kernel: 128

Hashes: 1 digests; 1 unique digests, 1 unique salts
Bitmaps: 16 bits, 65536 entries, 0x0000ffff mask, 262144 bytes, 5/13 rotates

Optimizers applied:
* Zero-Byte
* Single-Hash
* Single-Salt
* Brute-Force
* Slow-Hash-SIMD-LOOP
* Uses-64-Bit

Session..........: hashcat
Status...........: Exhausted
Hash.Mode........: 13721 (VeraCrypt SHA512 + XTS 512 bit)
Hash.Target......: vera_key.hash
Time.Started.....: Fri Jul 29 14:42:09 2022 (11 secs)
Time.Estimated...: Fri Jul 29 14:42:20 2022 (0 secs)
Kernel.Feature...: Pure Kernel
Guess.Mask.......: eenuzo3N [8]
Guess.Queue......: 2314/6250025 (0.04%)
Speed.#1.........:      0 H/s (1.27ms) @ Accel:16 Loops:125 Thr:512 Vec:1
Recovered........: 0/1 (0.00%) Digests
Progress.........: 1/1 (100.00%)
Rejected.........: 0/1 (0.00%)
Restore.Point....: 1/1 (100.00%)
Restore.Sub.#1...: Salt:0 Amplifier:0-1 Iteration:499875-499999
Candidate.Engine.: Device Generator
Candidates.#1....: eenuzo3N -> eenuzo3N
Hardware.Mon.#1..: Temp: 63c Fan: 28% Util: 94% Core:1252MHz Mem:3004MHz Bus:16
```

Da der Angriff kein Ergebnis in akzeptabler Zeit hervorbrachte wurde er abgebrochen.

5.5. Benutzer-Administratoren

Kontrolle der Benutzer mit Administrationsrechten

```
$ grep '^sudo:.*$' /mnt/linux/etc/group | cut -d: -f4
pc,pascal,olaf
```

5.6. SSH Verbindungen

Überprüfung der von Benutzern hergestellten SSH-Verbindungen. Man kann sehen, dass es Verbindungen von einem anderen Computer aus dem logischen Netzwerk gab (IP: *192.168.122.1*)

```
$ cat var/log/auth.log | grep -E "sshd.+from\s"
Jul  2 17:00:27 pc-Standard-PC-Q35-ICH9-2009 sshd[3820]: Accepted password for pc from
    127.0.0.1 port 44030 ssh2
```

```
Jul  2 17:00:30 pc-Standard-PC-Q35-ICH9-2009 sshd[3883]: Received disconnect from
    127.0.0.1 port 44030:11: disconnected by user
Jul  2 17:00:30 pc-Standard-PC-Q35-ICH9-2009 sshd[3883]: Disconnected from user pc
    127.0.0.1 port 44030
Jul  2 17:31:57 pc-Standard-PC-Q35-ICH9-2009 sshd[2197]: Accepted password for pc from
    192.168.122.1 port 44702 ssh2
Jul  2 17:32:05 pc-Standard-PC-Q35-ICH9-2009 sshd[2255]: Received disconnect from
    192.168.122.1 port 44702:11: disconnected by user
Jul  2 17:32:05 pc-Standard-PC-Q35-ICH9-2009 sshd[2255]: Disconnected from user pc
    192.168.122.1 port 44702
Jul  2 17:42:46 pc-Standard-PC-Q35-ICH9-2009 sshd[2288]: Accepted password for pc from
    192.168.122.1 port 44706 ssh2
Jul  2 17:43:46 pc-Standard-PC-Q35-ICH9-2009 sshd[2324]: Received disconnect from
    192.168.122.1 port 44706:11: disconnected by user
Jul  2 17:43:46 pc-Standard-PC-Q35-ICH9-2009 sshd[2324]: Disconnected from user pc
    192.168.122.1 port 44706
Jul  2 17:46:28 pc-Standard-PC-Q35-ICH9-2009 sshd[2369]: Accepted password for pc from
    192.168.122.1 port 44708 ssh2
Jul  2 17:47:39 pc-Standard-PC-Q35-ICH9-2009 sshd[2405]: Received disconnect from
    192.168.122.1 port 44708:11: disconnected by user
Jul  2 17:47:39 pc-Standard-PC-Q35-ICH9-2009 sshd[2405]: Disconnected from user pc
    192.168.122.1 port 44708
Jul  2 17:49:48 pc-Standard-PC-Q35-ICH9-2009 sshd[2445]: Accepted password for pc from
    192.168.122.1 port 44710 ssh2
Jul  2 17:51:38 pc-Standard-PC-Q35-ICH9-2009 sshd[2481]: Received disconnect from
    192.168.122.1 port 44710:11: disconnected by user
Jul  2 17:51:38 pc-Standard-PC-Q35-ICH9-2009 sshd[2481]: Disconnected from user pc
    192.168.122.1 port 44710
Jul  2 17:59:11 pc-Standard-PC-Q35-ICH9-2009 sshd[2580]: Accepted password for pc from
    192.168.122.1 port 44712 ssh2
Jul  2 18:02:18 pc-Standard-PC-Q35-ICH9-2009 sshd[2616]: Received disconnect from
    192.168.122.1 port 44712:11: disconnected by user
Jul  2 18:02:18 pc-Standard-PC-Q35-ICH9-2009 sshd[2616]: Disconnected from user pc
    192.168.122.1 port 44712
Jul  2 18:02:35 pc-Standard-PC-Q35-ICH9-2009 sshd[2728]: Accepted password for pc from
    192.168.122.1 port 44714 ssh2
Jul  2 18:03:36 pc-Standard-PC-Q35-ICH9-2009 sshd[2764]: Received disconnect from
    192.168.122.1 port 44714:11: disconnected by user
Jul  2 18:03:36 pc-Standard-PC-Q35-ICH9-2009 sshd[2764]: Disconnected from user pc
    192.168.122.1 port 44714
Jul  2 22:22:35 pc-Standard-PC-Q35-ICH9-2009 sshd[3316]: Accepted password for pc from
    192.168.122.1 port 44718 ssh2
Jul  2 22:23:35 pc-Standard-PC-Q35-ICH9-2009 sshd[3374]: Received disconnect from
    192.168.122.1 port 44718:11: disconnected by user
Jul  2 22:23:35 pc-Standard-PC-Q35-ICH9-2009 sshd[3374]: Disconnected from user pc
    192.168.122.1 port 44718
Jul  2 22:57:01 pc-Standard-PC-Q35-ICH9-2009 sshd[2190]: Accepted password for pc from
    192.168.122.1 port 44720 ssh2
Jul  2 22:58:56 pc-Standard-PC-Q35-ICH9-2009 sshd[2248]: Received disconnect from
    192.168.122.1 port 44720:11: disconnected by user
Jul  2 22:58:56 pc-Standard-PC-Q35-ICH9-2009 sshd[2248]: Disconnected from user pc
    192.168.122.1 port 44720
Jul  2 23:34:20 pc-Standard-PC-Q35-ICH9-2009 sshd[2431]: Accepted password for pc from
    192.168.122.1 port 44722 ssh2
```

```
Jul  3 14:15:41 pc-Standard-PC-Q35-ICH9-2009 sshd[2467]: Received disconnect from
    192.168.122.1 port 44722:11: disconnected by user
Jul  3 14:15:41 pc-Standard-PC-Q35-ICH9-2009 sshd[2467]: Disconnected from user pc
    192.168.122.1 port 44722
Jul  4 11:09:34 pc-Standard-PC-Q35-ICH9-2009 sshd[2772]: Accepted password for pc from
    192.168.122.1 port 56916 ssh2
Jul  4 11:09:36 pc-Standard-PC-Q35-ICH9-2009 sshd[2881]: Received disconnect from
    192.168.122.1 port 56916:11: disconnected by user
Jul  4 11:09:36 pc-Standard-PC-Q35-ICH9-2009 sshd[2881]: Disconnected from user pc
    192.168.122.1 port 56916
Jul  4 11:48:17 pc-Standard-PC-Q35-ICH9-2009 sshd[3851]: Accepted password for pc from
    192.168.122.1 port 56918 ssh2
Jul  4 11:49:20 pc-Standard-PC-Q35-ICH9-2009 sshd[3887]: Received disconnect from
    192.168.122.1 port 56918:11: disconnected by user
Jul  4 11:49:20 pc-Standard-PC-Q35-ICH9-2009 sshd[3887]: Disconnected from user pc
    192.168.122.1 port 56918
Jul  4 12:34:41 pc-Standard-PC-Q35-ICH9-2009 sshd[4136]: Accepted password for pc from
    192.168.122.1 port 56920 ssh2
Jul  4 12:35:23 pc-Standard-PC-Q35-ICH9-2009 sshd[4328]: Accepted password for olaf from
    192.168.122.1 port 56922 ssh2
Jul  4 12:35:25 pc-Standard-PC-Q35-ICH9-2009 sshd[4390]: Received disconnect from
    192.168.122.1 port 56922:11: disconnected by user
Jul  4 12:35:25 pc-Standard-PC-Q35-ICH9-2009 sshd[4390]: Disconnected from user olaf
    192.168.122.1 port 56922
Jul  4 12:35:43 pc-Standard-PC-Q35-ICH9-2009 sshd[4194]: Received disconnect from
    192.168.122.1 port 56920:11: disconnected by user
Jul  4 12:35:43 pc-Standard-PC-Q35-ICH9-2009 sshd[4194]: Disconnected from user pc
    192.168.122.1 port 56920
```

6. Untersuchungsgang

Nach Erhalt des Asservats sicherten wir die Hashwerte des Datenträgers und erstellten eine genaue Kopie des Datenträgers mit Hilfe des Foresischentools *dd* (siehe Unterunterabschnitt 5.1.1). Sobald wir im Besitz der Datenträgerkopie waren, begannen wir mit der Analyse des Dateiformats, um herauszufinden, wie wir vorgehen sollten. Nach einer Analyse des Imageheaders wurde festgestellt, dass es sich um ein von QEMU verwendetes Volume im .qcow2 Format handelt. Ein Programm welches zur Virtualisierung von Betriebssystemen verwendet wird. Diese .qcow2 Datei konnte in QEMU gemountet und gestartet werden, aber man stößt auf einen Login Screen des Ubuntu Betriebssystems. Dieser Anmeldebildschirm zeigt drei Benutzer an: *olaf*, *pascal*, *pc*; alle drei sind passwortgeschützt. Da die Passwörter der drei Benutzer nicht bekannt waren, wurde beschlossen, die Datei in das *.raw* Format zu konvertieren und ein Image des Betriebssystems zu erstellen (siehe Listing 5.1.2).

Die QEMU Tools bieten ein Werkzeug um *.qcow2* in .qcow2 Dateien zu konvertieren. Wenn nun die Imagedatei im *.raw* Format vorliegt, kann man mit Hilfe von *fdisk* und *parted* das Betriebssystem untersuchen und feststellen, aus welchen Partitionen es besteht (siehe Unterunterabschnitt 5.1.2). Wenn man sich einen Überblick über die Zusammensetzung des Betriebssystems verschafft, kann man sehen, dass es sich um eine Linux Distribution handelt, an der wahrscheinlich ein 10 GByte USB-Stick angeschlossen war. Um fortzufahren, wurden Kopien der wichtigsten Partitionen erstellt: die Linux-Hauptpartition (ext4) und die USB-Partition (NTFS). Nachdem die Kopien erstellt wurden, konnte man beiden Partitionen ohne Schreibrechte einhängen, um das Betriebssystem und die darin enthaltenen Informationen nicht zu kompromittieren.

Auf der USB-Partition gibt es nur eine Datei mit dem Namen *XXX* und dem Pfad */porn/newStuff/XXX*; es handelt sich um eine verschlüsselte Datei, die nicht geöffnet werden kann.

In der Linux-Partition sind die üblichen Verzeichnisse eines Linux-basierten Betriebssystems zu finden. Als Erstes wurde geprüft, welche Benutzer registriert waren, und nach deren Kennwörter gesucht. Nach einer Durchsuchung der Systemkonfigurationsdateien wurde bestätigt, dass drei Benutzer auf dem System registriert waren: *olaf*, *pascal* und *pc*. Die Passwörter der Benutzer *olaf* und *pascal* waren mit dem sha-512-Algorithmus verschlüsselt; mit einem Bruteforce-Angriff unter Verwendung einer Wordlist war es möglich, die Passwörter für diese beiden Konten zu erlangen (siehe Unterunterabschnitt 5.2.1). Nur das Konto *pc*, dessen Kennwort mit einem anderen Algorithmus verschlüsselt war (yescrypt), blieb übrig. Mit demselben Bruteforce Angriff unter Verwendung des Wordlist ließen sich das Kennwort nicht herausfinden. Die Passwörter der Benutzer *olaf* und *pascal* reichten jedoch aus, um Administratorrechte auf dem System zu erlangen, da beide über die notwendigen Privilegien verfügen (siehe Unterabschnitt 5.5). Bei der Analyse der Hauptordner der Benutzer wurde festgestellt, dass der Benutzer *pascal* zwar angelegt worden war, sich aber nie über die Desktop-Umgebung, sondern wahrscheinlich nur über die Kommandozeile angemeldet hatte; dies war daran zu erkennen, dass er über keinen der Ordner verfügte, die die Desktopumgebung nach der ersten Anmeldung anlegt; Ordner, welche *olaf* und *pc* besitzen. Zu beachten ist die Chronologie der vom Nutzer

pc ausgeführten Befehle, die Befehle zur Installation von zwei Programmen zeigt: *KeePassXC* und *Veracrypt* (siehe Unterunterabschnitt 4.2.1), aber abgesehen davon gab es keine weiteren Unregelmäßigkeiten. Der Nutzer *olaf* ist der welcher wahrscheinlich am meisten genutzt wurde. Dieser Benutzer hatte auch eine Passwortdatenbank in seinem Hauptordner (*Passwörter.kdbx*). Diese Datenbank kann mit dem Programm KeePassXC geöffnet werden. Es wurde versucht, die Datenbank mit KeePassXC unter Verwendung des Passworts des Benutzers olaf und *pascal* zu öffnen, aber keines dieser Passwörter war das richtige.
Im Pfad */home/olaf/.local/share/* wurde die Datei *recently-used.xbel* gefunden, die anzeigt welche Programme vom Benutzer *olaf* geöffnet wurden und wann sie geöffnet wurden. Anhand dieser Datei konnte festgestellt werden, dass der Benutzer die Datei *Passwörter.kdbx* mit dem Programm KeePassXC öffnete, dann die Datei */porn/newStuff/XXX* mit Veracrypt mountete und anschließend mit dem Firefox-Browser drei Bilder aus dem Internet heruntergeladen hat (siehe Unterunterabschnitt 4.3.3). Nur eines dieser drei Bilder ist auffindbar; es befindet sich in */home/olaf/Download/*. Es wurde versucht die fehlenden Bilder im Papierkorb zu finden (Pfad */home/olaf/.local/share/Trash/*) aber es befanden sich keine Dateien im Papierkorb. Weiter ging es mit der Überprüfung der vom FileManager des Systems erstellten Vorschaubilder, im Ordner */home/olaf/.cache/thumbnails/large/* fanden wir insgesamt 155 Vorschaubilder (siehe Unterunterabschnitt 4.3.2). Diese Images wurden wahrscheinlich von *Nautilus*, dem Ubuntu FileManager, erstellt. Bei diesen Bildern handelte es sich eindeutig um Bilder, die mit einer Kamera aus der Ferne gemacht worden waren und ein Mädchen zeigten; unter diesen Vorschaubildern befanden sich auch die Bilder, die der Benutzer von Firefox heruntergeladen hatte, sowie ein Vorschaubild eines USB-Stick-Handbuchs der Firma TOSHIBA.

Außerdem wurden bei allen drei Nutzern SSH-Keys gefunden (Pfade */home/olaf/.ssh/*, */home/pascal/.ssh/* und */home/pc/.ssh/*). Der Benutzer *pc* hatte außerdem Verbindungen zu SSH-Servern gespeichert (Dateipfad */home/pc/.ssh/know_host*), aber auch diese sind verschlüsselt. Durch Auslesen der Systemlogs (*/var/log/auth.log*) war es jedoch möglich, Verbindungen von einer lokalen IP-Adresse (*192.168.122.1*) festzustellen, wahrscheinlich einem anderen Computer aus demselben Netzwerk (siehe Unterabschnitt 5.6).

7. Auswertung und Rückgabe der Asservate, Löschen von übergebenen Sicherungskopien

Zur Erstellung des vorliegenden Gutachtens wurde eine Kopie der Inhalte des Asservates erstellt (siehe Abschnitt 2), nach der Erstellung der Kopie wurde das Asservat unverzüglich zurück an Frau Oberstaatsanwältin Blitzgescheit übergeben. Nach der Erstellung des Gutachtens wurden alle Kopien des Asservats welche sich im Besitz des Sachverständigenbüros Findet die Wahrheit befanden vernichtet. Dazu wurden Verfahren verwendet welche eine Wiederherstellung der Kopie unmöglich machen.

A. Wichtige Lesehinweise zum Gutachten

- Inhalt: Es wurden nicht alle negativen Untersuchungsergebnisse dokumentiert
- Juristische Begriffe: Falls ein juristischer Begriff Verwendet wurde, geschieht das ungewollt und in der umgangssprachlichen Bedeutung. Eine juristische Deutung obliegt der Staatsanwaltschaft und dem hohen Gericht.
- Nutzer: Als „Nutzer“ wird ein Zugang zu dem Softwaresystem bezeichnet. Es ist möglich das ein Nutzer von mehreren natürlichen Personen benutzt wird oder mehrere Nutzer von nur einer Person. Ob eine Person welche einen Nutzer verwendet der Beschuldigte ist kann meist nicht eindeutig beantwortet werden.
- Manipulation des Asservats: Das Gutachten erfolgt auf Basis des vorliegenden Asservats. Aufgrund der technischen Eigenschaften des Asservats kann eine Manipulation des Assarvats vor Übergabe an das Sachverständigenbüro Findet die Wahrheit nicht zwingend festgestellt werden. Werden während dem Gutachten Hinweise auf Manipulationen gefunden wird dies im Gutachten erwähnt.

B. Anmerkungen zur Technischen Vorgehensweise

- Veränderung des Original-Datenbestands: Für das Gutachten wurde eine Kopie des original Festplattenabbildes verwendet. So wurde verhindert dass das Beweisstück verändert wurde. Um die Integrität der Kopie sicherzustellen wurde nach dem Kopiervorgang die Kopie mit dem Original mittels Hashverfahren verglichen. Während der Arbeit an der Kopie wurde sie durch einen Software seitigen Schreibschutz vor Veränderungen geschützt.
- Verwendete Werkzeuge: Die Auswertung von Datenträgern erfolgt nach forensischen Gesichtspunkten und auf dem aktuellen Stand der Technik. An Hard- und Softwareprodukten werden von Ermittlungs-, Finanz- und Steuerbehörden weltweit genutzte und gerichtlich anerkannte Produkte unter Windows und Linux eingesetzt.

Glossar

BIOS ist eine Software auf dem Mainboard Ihres Computers. Es sorgt dafür, dass die Hardware Komponenten dessen funktionieren und fehlerfrei zusammenwirken.. 20

Browser Webbrowser, oder allgemein auch Browser , sind spezielle Computerprogramme zur Darstellung von Webseiten im World Wide Web oder allgemein von Dokumenten und Daten.. 28

Bruteforce Es handelt sich um den Versuch, ein Passwort oder einen Benutzernamen zu knacken oder eine verborgene Webseite oder den Schlüssel zu finden, mit dem eine Nachricht verschlüsselt wurde.. 22, 27

Byte Ist die kleinste Informationseinheit eines Rechners und entspricht den Zuständen "Strom an" (1) und "Strom aus" (0).. 23, 27

dd dd ist ein Befehlszeilendienstprogramm, dessen Hauptzweck das Konvertieren und Kopieren von Dateien ist.. 19, 23, 27

EFI Die EFI-Systempartition (ESP) ist eine Partition Format, mit FAT32 formatierte Partition. 20

ext4 Dateisystemen zur Speicherung und zum Lesen von Daten. 27

fdisk Ist ein Programm zur Partitionierung von Festplatten. 20, 27

FileManager Ein Dateimanager (englisch File Manager) ist ein Computerprogramm zum Verwalten von Inhalten auf Dateisystemen, die sich auf unterschiedlichen Speichermedien befinden können. 28

Hash Eine Textzeichenfolge, die eine Datei/Daten eindeutig identifiziert. Es kann nicht umgekehrt werden.. 3, 5, 9, 13, 19–23, 27, 29

hashcat Hashcat ist ein Werkzeug zur Wiederherstellung von Passwörtern.. 1, 23

HDD Ein Festplattenlaufwerk, das digitale Daten mithilfe eines magnetischen Speichers.. 2, 5

Image Ein VM-Image ist eine Datei, die eine virtuelle Festplatte enthält, auf der ein bootfähiges Betriebssystem installiert wurde.. 19

IP Eine IP-Adresse ist eine numerische Darstellung des Standortes, von dem aus ein Gerät mit dem Internet verbunden ist. So können Sie ermitteln, wo sich etwas befindet und, bis zu einem gewissen Grad, worum es sich dabei handelt.. 24

john John the Ripper ist ein Opensource Softwareprogramm zum Knacken von Passwörtern.. 1, 21, 22

kdbx Von KeePass Password Safe erstellte Datei. 28

KeePassXC KeePassXC ist ein Passwort-Manager, der komplett lokal arbeitet. 28

Linux Linux ist ein Open-Source-Betriebssystem. 6, 27

Login Als Login oder Log-in (von engl.: (to) log in = „einloggen“, „anmelden“ → „[Benutzer-]Anmeldung“, auch: Sign-in/Sign-on, Log-on usf.) wird der Vorgang bezeichnet, sich in einem Computersystem anzumelden (einzuloggen). 27

Magic Number Magic Numbers sind die ersten paar Bytes einer Datei, die für einen bestimmten Dateityp eindeutig sind. Diese Bytes können vom System zur "Unterscheidung und Erkennung verschiedener Dateien" ohne Dateierweiterung verwendet werden.. 19

MD5 Beim Message-Digest Algorithm 5 (MD5) handelt es sich um eine Hashfunktion, die aus einer bestimmten Zeichenkette oder Nachricht einen immer gleichen Hashwert erzeugt. 5, 6, 9

Nautilus Nautilus ist ein freier Dateimanager für Linux Systeme. Es ist der Standard-Dateimanager der Desktop-Umgebung Gnome und wird auch einfach Dateien genannt.. 13

NTFS Dateisystemen zur Speicherung und zum Lesen von Daten. 6, 27

parted Die kostenlose Linux-basierende Programmsammlung Parted Magic hilft beim Erstellen, Bearbeiten, Kopieren oder Löschen von Partitionen auf der Festplatte.. 20, 27

Partition Was versteht man unter einer Partition? Der Vorgang des Erstellens von Partitionen wird als Partitionieren bezeichnet. Partitionieren lassen sich externe oder interne Speichergeräte wie herkömmliche Festplatten, SSDs oder Flash-Speicher. 6, 20, 27

qcow2 qcow2 ist ein Speicherformat für virtuelle Festplatten.. 5, 19, 20, 27

QEMU QEMU ist ein Opensource Emulator, der Betriebssysteme virtualisieren und emulieren kann.. 20, 27

raw Ist das Rohdatenformat. 20, 27

Server Rechner, der für andere in einem Netzwerk mit ihm verbundene Systeme bestimmte Aufgaben übernimmt und von dem diese ganz oder teilweise abhängig sind.. 28

sha-512 Ist eine kryptologische Hashfunktion. 27

SHA1 Ist eine kryptologische Hashfunktion,dient sie dazu, digitale Dateien (z.B.: Nachrichten) mit einem Hash-Wert (digitale Signatur) zu versehen. 5

SSH SSH, auch bekannt als Secure Shell oder Secure Socket Shell, ist ein Netzwerkprotokoll, das Benutzern, insbesondere Systemadministratoren, eine sichere Möglichkeit bietet, über ein ungesichertes Netzwerk auf einen Computer zuzugreifen.. 8, 24, 28

Ubuntu Bei Ubuntu handelt es sich um ein Betriebssystem wie Windows oder Mac OS X.. 6, 28

unshadow Unter allen aktuellen Linux-Distributionen stehen Benutzernamen (/etc/passwd) und Passwörter (/etc/shadow) in unterschiedlichen Dateien. Früher standen beide Informationen in /etc/passwd. unshadow fügt beide Dateien wieder zusammen, so dass john sie analysieren kann.unter allen aktuellen Linux-Distributionen stehen Benutzernamen (/etc/passwd) und Passwörter (/etc/shadow) in unterschiedlichen Dateien. Früher standen beide Informationen in /etc/passwd. unshadow fügt beide Dateien wieder zusammen, so dass john sie analysieren kann.. 21

USB Ein USB-Stick ist ein kompaktes, transportables Speichergerät für Computer.. 6, 27, 28

Veracrypt Ist eine Software zur Datenverschlüsselung, insbesondere zur vollständigen oder partiellen Verschlüsselung von Festplatten und Wechseldatenträgern.. 1, 6, 7, 23, 28

Wordlist Ist eine Liste von Wörtern, die als Passwort probiert werden können. 27

yescrypt yescrypt ist eine passwortbasierte funktion. 27