

Ermittlungsverfahren gegen Alexander Adler wegen des Besitzes von illegaler Nashornographie

Aneta Větrovská
aneta.vetrovska@fau.de

Asservatennummer : Asservat_23948-24.zip

30. 6. 2024

Inhaltsverzeichnis

1 Prolog	3
1.1 Untersuchungsauftrag	3
1.2 Nachweis über Integrität der Asservate	4
1.3 Arbeitsumgebung	4
1.4 verwendete Werkzeuge	5
2 Ergebniszusammenfassung	6
3 Technische Analyse	7
3.1 Überprüfung der Integrität vor der Analyse	7
3.2 Analyse des Partitionsschemas	7
3.2.1 part0	8
3.2.2 part1	8
3.2.3 part2	8
3.2.4 part3	8
3.2.5 part4	8
3.2.6 part5	8
3.2.7 part6	9
3.2.7.1 Browser-History	9
3.2.7.2 E-Mail Kommunikation	9
3.2.7.3 Bash_history	9
3.2.7.4 Verzeichnisse	9
3.2.8 part7	9
3.2.9 part8	10
3.3 Auffinden und Wiederherstellung gelöschter Dateien	10
3.4 Analyse von Logs und Cronjobs	10
3.4 Analyse von Logs	10
3.4 Analyse von Cronjobs	11
3.5 Suche nach Schadsoftware	11
3.6 Überprüfung der Integrität nach der Analyse	11
4 Anhang	12

1 Prolog

1.1 Untersuchungsauftrag

Die Staatsanwaltschaft Nürnberg-Fürth hat ein Ermittlungsverfahren gegen Alexander Adler, geb. am 13.10.1989 in Erlangen, wegen des Besitzes illegaler Nashornographie gemäß §184n StGB eingeleitet.

Die NSA überwachte ein Untergrundforum für illegale Nashornbilder auf <https://www.reddit.com/r/rhino/>. Deutsche IP-Adressen wurden an Europol und dann an das BKA weitergeleitet. Eine IP-Adresse vom 9.5.2024 wurde Adlers Hausanschluss zugeordnet. Am 14.05.2024 wurde ein Dell XPS-PC bei ihm sichergestellt. Die IP-Adresse eines Zugriffs vom 9.5.2024 konnte dem Hausanschluss des Beschuldigten zugewiesen werden. Im Rahmen einer Hausdurchsuchung am 14.05.2024 wurde in der Wohnung des Beschuldigten ein PC der Marke Dell XPS sichergestellt. Der PC wurde im ausgeschalteten Zustand angetroffen.

Die Staatsanwaltschaft erbittet Antwort auf folgende Fragen in Form eines Gutachtens bis zum 9. 7. 2024 :

1. Befinden sich auf dem Datenträger Bild- oder Videodateien, in denen unbekleidete Nashörner abgebildet sind? Falls ja, gibt es Hinweise auf den Ursprung dieser Daten, und gibt es Hinweise darauf, dass diese Bilder vom Nutzer aufgerufen, geöffnet, umbenannt, oder in sonstiger Art und Weise „genutzt“ wurden?
2. Gibt es Hinweise darauf, dass der Nutzer des Laptops der Beschuldigte ist? Gibt es Hinweise darauf, dass auch andere Personen den Laptop genutzt haben oder Zugriff darauf hatten? Wenn ja, welche Personen waren das?
3. Enthält der Datenträger Hinweise auf die Verbreitung o.g. Nashorndateien? Falls ja, über welche Kanäle wurden welche Nashorndateien verbreitet und in welchem Zeitraum fand die Verbreitung statt?
4. Finden sich auf dem Datenträger Hinweise auf Kommunikationsbeziehungen mit der E-Mail-Adresse rhinobroker@reddit.com? Falls ja, erbitten wir eine vollständige Auflistung des Kommunikationsverlaufs und der Kommunikationsinhalte.

Auszug aus dem Sicherungsbericht der Kriminalinspektion 5 vom 14.05.2024 :

Im Rahmen der Durchsuchung am 14.05.2024 wurde gegen 8:00 Uhr ein PC Marke Dell XPS (Asservatennummer 23948-24) beschlagnahmt und in die Asservatenkammer des Polizeipräsidiums verbracht. Der Rechner wurde im ausgeschalteten Zustand angetroffen. Um 10:45 Uhr des selben Tages wurde die Festplatte des Laptops ausgebaut und im Forensik-Labor der Kriminalinspektion 5 eine forensische 1:1-Kopie mit gleichzeitiger Hashwertberechnung (SHA256) unter Verwendung eines Hardware-Write-Blocker Marke WiebkeTech SAS angefertigt. Die Arbeiten wurden fachgerecht von Herrn KHK Müller durchgeführt. SHA256-Hashsumme der entpackten Datei:

02779dd1ee62c0c3823eb0f7810670dcc8d5ce46c8568a358a53b1124ea49298

Die angefertigte Image-Datei wurde auf einen externen Datenträger kopiert und am 14.05.2024 an die Staatsanwaltschaft übergeben. Nach Wiedereinbau der Festplatte wurde Asservat 34-787 am 14.05.2024, 16:30 Uhr, wieder in die Asservatenkammer des Polizeipräsidiums verbracht.

1.2 Nachweis über Integrität der Asservate

Am 19. Juni 2024 um 11:00 (CEST) Uhr habe ich das Festplattenabbild von der offiziellen Website der Staatsanwaltschaft heruntergeladen, deren Authentizität verifiziert wurde. Die SHA256-Summe des Abbilds wurde mir auf sicherem Weg durch einen verifizierten Kurier in schriftlicher Form zugestellt, dessen Identität und Berechtigung zuvor durch die Staatsanwaltschaft bestätigt worden waren. Direkt danach fuhr ich in mein Büro und kopierte das Beweismaterial (die Imagedatei Asservat_23948.img) dort um 11:30 (CEST) Uhr auf eine eigens dafür erstellte virtuelle Maschine (VM) auf meinem Arbeitsrechner. Die schriftliche SHA256-Summe sicherte ich anschließend in einem Tresor. Sowohl auf den Arbeitsrechner mit der erstellten VM als auch auf den Tresor habe nur ich allein Zugriff. Beide befinden sich in einem alarmgesicherten Raum, zu dem niemand sonst Zugang hat.

Zunächst überprüfte ich, ob die auf meinem Computer berechnete SHA256-Summe des Abbilds mit der mir in Papierform übergebenen übereinstimmte. Dies war der Fall (**Bild 4.1.1 und 4.1.2**). Den Hash des Abbilds speicherte ich in der Datei *hashes*.

Das Asservat wurde im Zeitraum vom 19. 6. 2024 bis zum 9. 7. 2024 untersucht. Während dieser Zeit führte ich regelmäßig SHA256-Prüfungen durch, um eine nachträgliche Verfälschung der Daten auszuschließen. Die Prüfsummen der Images sowie aller daraus extrahierten Partitionsabbilder und Dateien sind als Bildschirmfoto der Datei *hashes* im Anhang zu finden (**Bild 4.1.4**).

1.3 Arbeitsumgebung

Die Untersuchung wurde auf meinem ausschließlich von mir genutzten Arbeitsrechner durchgeführt. Dieser ist mit einem langen und somit sicheren Passwort geschützt, das nur mir bekannt ist und wöchentlich geändert wird. Vor Beginn der Arbeit wurde sichergestellt, dass das System virenfrei und stabil ist. Zum Einsatz kam ein Lenovo ThinkPad T14 Gen1 mit einem Intel(R) Core(TM) i7-10510U @ 1.80GHz Prozessor mit 8 Kernen, einer Mesa Intel(R) UHD Graphics (CometLake-U GT2) Grafikkarte und 32 GB RAM zur Verfügung. Auf dem Rechner läuft eine 64-Bit-Version von Ubuntu 22.04.4 LTS.

Zur Durchführung der Analyse wurde eine virtuelle Maschine mit 64-Bit Kali Linux 2024.2 verwendet, betrieben mit Oracle VirtualBox, die speziell für forensische Untersuchungen eingerichtet wurde. Sämtliche Einstellungen der VM sind in der beigefügten Abbildung dokumentiert (**Bild 4.1.5**).

1.4 verwendete Werkzeuge

- *clamscan* (Version 1.2.1)
- *hexdump* (from util-linux Version 2.40)
- *gunzip* (Version 1.12)
- *photorec* (Version 7.1)
- *sha256sum* (Version 9.4)
- tools for forensics analysis on volume and filesystem data *Sleuthkit* (Version 4.12.1)
- DB Browser for SQLite *sqlitebrowser* (Version 3.12.2)
- *testdisk* (Version 7.1)
- *vim* (Version 9.1) zum Betrachten von Skripten

2 Ergebniszusammenfassung

- 2.1 Befinden sich auf dem Datenträger Bild- oder Videodateien mit Nashörner ?
- 2.2 Gibt es Hinweise darauf, dass der Nutzer des Laptops der Beschuldigte ist?
- 2.3 Enthält der Datenträger Hinweise auf die Verbreitung o.g. Nashorndateien?
- 2.4 Finden sich auf dem Datenträger Hinweise auf Kommunikationsbeziehungen mit der E-Mail-Adresse rhinobroker@reddit.com?

3 Technische Analyse

Im Rahmen meiner forensischen Untersuchung habe ich das Asservat chronologisch bearbeitet und dabei jeden Schritt sorgfältig dokumentiert. Jede Untersuchung wurde durch Fotos sowie detaillierte Notizen festgehalten. Zusätzlich habe ich für jede neu gefundene Datei mittels des SHA256-Hashwerts eine Prüfsumme erzeugt und diese in einer Datei namens *hashes* gespeichert (**Bild 4.1.4**). Diese systematische Vorgehensweise gewährleistet die Integrität und Nachvollziehbarkeit aller untersuchten Daten.

3.1 Überprüfung der Integrität vor der Analyse

Zur Überprüfung der Integrität vor der Analyse habe ich zunächst den SHA-256-Hash des Asservats generiert (**Bild 4.1.2**) und diesen mit dem vom Kurier gelieferten SHA-256-Hash verglichen (**Bild 4.1.1**). Beide Hashwerte stimmten überein. Anschließend habe ich die schriftliche Version im Tresor gesichert, auf den nur ich Zugriff habe. Den generierten SHA-256-Hash des Asservats habe ich als ersten Eintrag in der *hashes* Datei gespeichert, um die Integrität auch zukünftig nachvollziehen und bewahren zu können.

3.2 Analyse des Partitionsschemas

Um mehr über das Partitionsschema herauszufinden, habe ich zunächst mit den SleuthKit-Befehlen und dem Tool *mmstat* ermittelt, dass es sich um eine GPT-Standard handelt (**Bild 4.2.1**). Anschließend habe ich den Befehl *mmls* verwendet, um das Partitionslayout zu erstellen (**Bild 4.2.2**).

Insgesamt wurden acht Partitionen gemäß den GPT-Standards (Safety Table, GPT Header, Partition Table, Partitionen -> Vergleich mit Wikipedia : https://en.wikipedia.org/wiki/GUID_Partition_Table#/media/File:GUID_Partition_Table_Scheme.svg) erkannt. Ich habe alle Partitionen mit Hilfe des Tools *mmcatt* in Dateien *partX*, wobei *X* der entsprechenden Nummer ist, gespeichert (**Bild 4.2.3**). Außerdem habe ich SHA-256-Hashes für jede *partX*-Datei generiert und in der *hashes*-Datei gesichert. Anschließend habe ich das Tool *testdisk* verwendet, um versteckte oder verlorene Partitionen zu finden. *testdisk* identifizierte drei Partitionen - FAT32, ext4, ext4 - (**Bild 4.2.4**), deren Dateisystemtypen und Größen mit den Ergebnissen der Verwendung des Tools *fsstat* auf den Dateien *part4*, *part5* und *part6* größtenteils übereinstimmten. Es gab eine kleine Abweichung in der Größe der FAT32-Partition, die wahrscheinlich darauf zurückzuführen ist, wie die Tools Sektoren zählen oder Partitionsmetadaten handhaben. Diese geringe Differenz deutet nicht zwangsläufig auf eine versteckte Partition hin, daher habe ich diese Spur nicht weiter verfolgt und die Untersuchung der gespeicherten Partitionen in den Dateien *part4*, *part5* und *part6* fortgesetzt.

Eine Partition, die als Linux LUKS identifiziert wurde, konnte nicht wiederhergestellt werden, da die Festplatte zu klein zu sein schien (**Bild 4.2.5**). Dies könnte daran liegen, dass die Partition verschlüsselt ist und man ein Passwort benötigt, um darauf zugreifen zu können.

3.2.1 *part0*

Hierbei handelt es sich um die Safety Table. Sie wurde mit dem Befehl *hexdump* analysiert und es wurden keine Auffälligkeiten gefunden.

3.2.2 *part1*

Diese Partition ist unalloziert und überschneidet sich mit den Partitionen 0, 2 und 3. Sie wurde mit *hexdump* untersucht und es wurden keine Unstimmigkeiten gefunden.

3.2.3 *part2*

Hierbei handelt es sich um den GPT-Header. Dieser wurde mit dem Befehl *hexdump* analysiert und es wurden keine Auffälligkeiten gefunden.

3.2.4 *part3*

Hierbei handelt es sich um die Partitionstabelle. Diese wurde mit dem Befehl *hexdump* analysiert und es wurden keine Auffälligkeiten gefunden.

3.2.5 *part4*

Die untersuchte Partition ist eine EFI-Systempartition, die als Boot-Partition funktioniert. Sie ist im FAT32-Dateisystem formatiert und enthält wichtige Dateien wie *BOOTX64.CSV*, die ihre Funktion bestätigen. Diese Dateien zeigen, dass die Partition für das Starten eines Betriebssystems konfiguriert ist. Die EFI-Systempartition enthält die notwendigen Bootloader- und Konfigurationsdateien, die vom EFI-Firmware während des Bootvorgangs geladen werden.

3.2.6 *part5*

Diese Partition hat das Dateisystem vom Typ ext4 und es ist Ubuntu 22.04 darauf installiert. Die Dateien *lsb-release* (**Bild 4.2.6**), *passwd* (**Bild 4.2.7**) und *shadow* (**Bild 4.2.8**) wurden extrahiert, und es wurde nur der Benutzer *alex:Alex Adler* gefunden. Aufgrund dieses virtuellen Nutzernamens könnte eine Verbindung zur physischen Person von Alex Adler bestehen.

Die Partition wurde mit den Schlüsselwörtern *nashorn* und *rhino* durchsucht, wobei für letzteres zwei Rhino-Bilder aus dem Katalog (wahrscheinlich Ikonen) gefunden wurden (eins 48x48 und eins 64x64) (**Bild 4.2.9**). Außerdem wurde ein Compiler namens *rhino.vim* gefunden, aber ich denke nicht, dass dieser Funde für den Fall relevant ist. Abgesehen davon wurde nichts Weiteres auf der Partition gefunden.

3.2.7 part6

Diese Partition hat ebenfalls das Dateisystem vom Typ ext4.

3.2.7.1 Browser-History

Ich habe herausgefunden, dass der Browser Mozilla Firefox installiert ist. Daher habe ich die Datei *places.sqlite* extrahiert, um den Verlauf anzuschauen.

Ich habe die Datei mit dem Befehl *sqlite3* durchsucht und zunächst *moz_places* überprüft, um nach Einträgen zu suchen, die mit den Schlüsselwörtern *rhino*, *nashorn* und *reddit* in Verbindung stehen könnten. Es gab einige Zugriffe auf Reddit, aber nichts Relevantes wurde gefunden (**Bild 4.2.10**). Auch andere Tabellen wurden durchsucht, aber ich konnte nichts finden, was von Bedeutung wäre.

3.2.7.2 E-Mail Kommunikation

Es wurde auch eine Thunderbird-Mail gefunden. Es konnte lediglich das Posteingangsverzeichnis im Pfad *alex/.thunderbird/6golie1p.default-release/ImapMail/imap.gmx.net/INBOX* extrahiert werden. Die E-Mail-Adresse des Benutzers Alex Adler wurde identifiziert *alex.adler1@gmx.de* (**Bild 4.2.11**) aber es wurden jedoch keine E-Mails im Zusammenhang mit der Adresse *rhinobroker@reddit.com* gefunden (**Bild 4.2.12**).

3.2.7.3 Bash_history

Ein weiteres extrahiertes Datei war die *bash_history* (**Bild 4.2.13**). Darin öffnete der Benutzer *alex* zuerst eine interaktive Root-Shell mit allen administrativen Privilegien und änderte dann die Eigentümerschaft von Dateien und Verzeichnissen auf den Benutzer Alex und die Gruppe Alex. Er bearbeitete auch eine Liste namens *passwortListe.txt*, in der vermutlich einige seiner Passwörter gespeichert sind. Diese Datei konnte jedoch nicht gefunden werden. Das Ändern der Dateiberechtigungen könnte in diesem Fall auf Versuche hinweisen, Dateien zu verbergen oder zu übertragen.

3.2.7.4 Verzeichnisse

Nachdem ich Verzeichnisse *Bilder*, *Dokumente*, *Downloads*, *Musik*, *Öffentlich*, *Schreibtisch*, *Videos*, *Papierkorb* und *Vorlagen* analysiert habe, fand ich unter *Bilder* drei Bildschirmfotos. In einem dieser Fotos entdeckte ich eine Datei mit Passwörtern für die verschlüsselte Partition (*part7*) sowie das E-Mail-Passwort (**Bild 4.2.14**). Andere Bilder und Dokumente wurden ebenfalls gefunden, jedoch als nicht relevant eingestuft.

3.2.8 part7

Diese Partition war verschlüsselt, aber wie in Abschnitt 3.2.7.4 erwähnt, habe ich ein Bildschirmfoto des Passworts gefunden. Ich habe versucht, das Passwort nach Ausführung

des Befehls *cryptsetup* einzugeben, aber nach vielen Versuchen erhielt ich immer noch die Meldung "No key available with this passphrase".

3.2.9 *part8*

Diese Partition ist unalloziert, sie wurde mit *hexdump* untersucht und es wurden keine Unstimmigkeiten gefunden.

3.3 Auffinden und Wiederherstellung gelöschter Dateien

Um Daten zu finden und wiederherzustellen, die bereits gelöscht wurden, habe ich das Tool *photorec* verwendet und nach den Schlüsselwörtern *rhino* und *nashorn* gesucht. Dabei kamen einige Funde zutage (**Bild 4.2.15**):

- zwei .mov-Videos, die nicht abgespielt werden konnten
- ein .jpg-Bild
- eine _chrome.zip-Datei

Nach dem Öffnen des jpg-Bildes und der Betrachtung des Inhalts habe ich ein Nashorn-Bild gefunden. Zusätzlich habe ich fünf weitere Nashorn-Bilder gefunden (**Bilder 4.3**). Eine ZIP-Datei wurde ebenfalls gefunden, aber nach gründlicher Untersuchung bin ich zu dem Schluss gekommen, dass es sich um die Google Chrome-Erweiterung für ein Wörterbuch handelte, und habe daher die Durchsuchung dieser Datei nicht fortgesetzt.

3.4 Analyse von Logs und Cronjobs

3.4.1 Analyse von Logs

Schließlich habe ich die Logs überprüft, um herauszufinden, was passiert ist. Zuerst habe ich die Datei *auth.log* extrahiert. Diese beginnt am 7. Mai und geht bis zum 13. Mai, dem Tag der Beschlagnahme. Ich habe ein paar interessante Dinge gefunden. Der Benutzer *alex* versuchte mehrmals, den Benutzer *vboxadd* hinzuzufügen, was darauf hindeuten könnte, dass er versuchte, eine virtuelle Maschine zu starten, es aber nicht schaffte. Er versuchte auch, Bluetooth zu nutzen (**Bild 4.2.16**), scheiterte jedoch ebenfalls. Am interessantesten waren die gefundenen Cron-Jobs, die ich später noch überprüfen wollte (**Bild 4.2.17**).

Eine weitere interessante Entdeckung war, dass der Name in den Logs *adlerhorst* war. Adler ist Alex' Nachname und Horst könnte entweder sein zweiter Vorname oder ein anderer Benutzer sein. Da es das erste Mal war, dass ich diesen Namen gesehen habe und er keine Befehle ausführte oder irgendetwas tat, habe ich dies vorerst unbeachtet gelassen.

Dann habe ich die Dateien *auth.log.1* und *auth.log.2.gz* extrahiert, die ich anschließend mit *gunzip* entpackt habe. Die Struktur der Loge war überraschend ähnlich zu *auth.log*; es schien mir, als hätte er jeden Tag genau dasselbe getan: Sitzungen der Benutzer *gmd*, *alex* und *root* wurden geöffnet, *alex* führte *sudo upgrade* aus und dann wurden das System und die Repositorys aktualisiert und aufgefrischt. In *auth.log.2* habe ich herausgefunden, dass *alex VBoxGuestAdditions* in den Ordner *home/alex* installiert hat. Anschließend gelang es

ihm, eine VM zu starten. Ich habe alle generierten SHA256-Checksummen in meiner *hashes*-Datei gespeichert und weiter überprüft, welche Cron-Jobs auf dem System geplant waren.

3.4.2 Analyse von Cronjobs

Ich fand heraus, dass die Cron-Jobs immer 17 Minuten nach einer vollen Stunde ausgeführt werden und die nächste Sitzung dann immer um 30 Minuten nach einer vollen Stunde beginnt. Daher habe ich zuerst *cron.hourly* (**Bild 4.2.18**) angesehen, da es angeblich 17 Minuten nach jeder vollen Stunde ausgeführt werden soll. Leider war nichts darin, und nachdem ich alle anderen *cron.** überprüft hatte, kam ich zu dem Schluss, dass alles leer war.

3.5 Suche nach Schadsoftware

Bevor ich meine Suche abgeschlossen habe, habe ich das Tool *clamscan* benutzt, um herauszufinden, ob Schadsoftware vorhanden ist. Es wurde keine Schadsoftware gefunden, und alle meine Datenbanken waren up-to-date (**Bild 4.2.19**).

3.6 Überprüfung der Integrität nach der Analyse

Schließlich habe ich den Befehl *sha256sum -c hashes* ausgeführt, um zu überprüfen, ob die Integrität beibehalten wurde (**Bild 4.1.3**).

4 Anhang

4.1 Prüfsummen

4.1.1 sha256-Summe im Papierformat

02779dd1ee62c0c3823eb0f7810670dcc8d5ce46c8568a358a53b1124ea49298

4.1.2 berechnete *sha256sum* von *Asservat_23948.img*

```
(kali-user㉿kali-user)-[~/Documents]
$ sha256sum Asservat_23948-24.img
02779dd1ee62c0c3823eb0f7810670dcc8d5ce46c8568a358a53b1124ea49298 Asservat_23948-24.img
```

4.1.3 Prüfung der Hashsummen am Ende

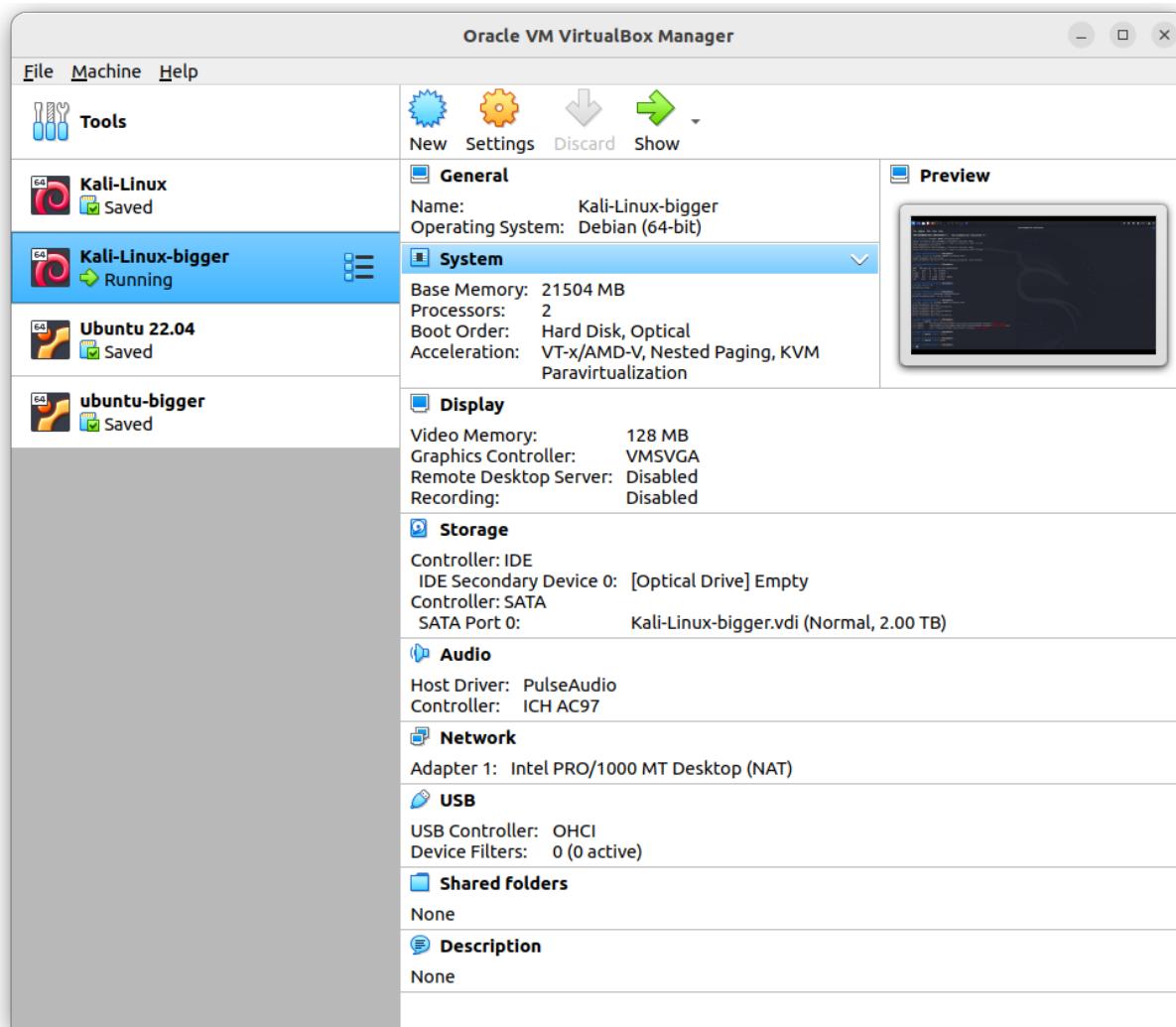
```
(kali-user㉿kali-user)-[~/Documents]
$ sha256sum -c hashes
Asservat_23948-24.img: OK
part0: OK
part1: OK
part2: OK
part3: OK
part4: OK
part5: OK
part6: OK
part7: OK
part8: OK
rhino_1: OK
f68098048.jpg: OK
f68100288.jpg: OK
f68104640.jpg: OK
f68109184.jpg: OK
f68109312.jpg: OK
f71245208.jpg: OK
auth.log: OK
auth.log.1: OK
auth.log.2: OK
places.sqlite_mozilla: OK
inbox: OK
bash_history: OK
Bildschirmfotos_2: OK
crontab: OK
passwd_part5: OK
lsb-release_part5: OK
shadow_part5: OK
```

4.1.4 Datei *hashes* mit gespeicherten sha256-Summen

```
$ cat hashes
02779dd1ee62c0c3823eb0f7810670dcc8d5ce46c8568a358a53b1124ea49298 Asservat_23948-24.img
218018bdf471882d97aa86307844713e70c17e63def1f951493c7f356410bb23 part0
F473d1b6fe241c31fb91600fbac624ee47a00edb6e664c3e4f05ace1378e65 part1
763ae47f529a437fed51dc399c16161ec3993b3ca30c1c4e9be5e8fa46c0a9c5 part2
2f2bb957b5046a95d566712ae563d0a38e057b3268ca42c2e627d34491acd0e2 part3
a8263da31790f3c84b91305beec0f596768b5068b88af31bf7e885d5696c081d part4
397931dd623c3c1c48b726057e6db6b9ea4dfedcdda7a34017c35d9d617dcff3 part5
7245dae95708aa37d1b06a75e5f73b33db462a4fff9c3ff183755eb6ed59565a part6
c059b065699fdf5fa643e161543c528cf9fd542f449561132819f05e082b9704 part7
F81bbfdb1720a11ef5122fadbfbbd4368de905ba6a8e3b22d8efb3176aa0a23 part8
7d02965185d96cee3eb9be7d16a253ae4047781460e0a31da513fb28c07fb9d rhino_1
cc1f7751f1392d828304b8a065008f9ef6b4920ab2cd4e6f831f7484794f00c4 passwd
36afa676a62cf0e1443fc638d74a4034326dc2fac59cfceaf04cd7972471f7e lsb-release
c6dcdd6284ca5b845778cccd45e9af5f5115cd02a243c3e2a076b71928361af03 shadow

e3b0c44298fc1c149afbfc8996fb92427ae41e4649b934ca495991b7852b855 f68098048.jpg
e3b0c44298fc1c149afbfc8996fb92427ae41e4649b934ca495991b7852b855 f68100288.jpg
e3b0c44298fc1c149afbfc8996fb92427ae41e4649b934ca495991b7852b855 f68104640.jpg
e3b0c44298fc1c149afbfc8996fb92427ae41e4649b934ca495991b7852b855 f68109184.jpg
e3b0c44298fc1c149afbfc8996fb92427ae41e4649b934ca495991b7852b855 f68109312.jpg
e3b0c44298fc1c149afbfc8996fb92427ae41e4649b934ca495991b7852b855 f71245208.jpg
ae72053c1fe16b4ec9e82dc7270b74dab411b908a6670f6ddb4749430fdf8292 auth.log
7967db9d2caa0d382f5a5ea214f6f3e157c0c417539933e35010c664895b2f6c auth.log.1
30d78381488b7b35feb270e1c56a26f5026fe24348e82a638efe9b1b7333e183 auth.log.2
30cc756e10d9bbe514ca9e33a95b92a946538cf6f61814cf20cbc8f7610e5ffc places.sqlite_mozilla
3db65a9624d0cfe11a00849ad5a848490258a465727bc4088aec771f3aaa4c0d inbox
56a761bd503af64f29cb106db961b4a5dff9cb4130f88038e768e7db2c1c0670 bash_history
b9f36c4aa36893fb245f22ccfafaaaf629982cf47698e0cac8ccdd3d2463c743b Bildschirmfotos_2
3494e2d3ce0fb77633d00b247cad543cca29c7673da802a23bd5fe0364eb2c13 crontab
```

4.1.5 Einstellungen der VM



4.2 Analyse

4.2.1 mmstat von *Asservat_23948.img*

```
(kali-user㉿kali-user)-[~/Documents]
└─$ mmstat Asservat_23948-24.img
gpt
```

4.2.2 mmls von *Asservat_23948.img*

```
(kali-user㉿kali-user)-[~/Documents]
└─$ mmls Asservat_23948-24.img
GUID Partition Table (EFI)
Offset Sector: 0
Units are in 512-byte sectors

      Slot      Start      End      Length      Description
000: Meta 00000000000 00000000000 0000000001 Safety Table
001: _____ 00000000000 00000002047 00000002048 Unallocated
002: Meta 00000000001 00000000001 00000000001 GPT Header
003: Meta 00000000002 00000000033 00000000032 Partition Table
004: 000 00000002048 0002000895 0001998848
005: 001 0002000896 0066000895 00640000000
006: 002 0066000896 0098000895 00320000000
007: 003 0098000896 0104855551 0006854656
008: _____ 0104855552 0104857599 0000002048 Unallocated
```

4.2.3 mmcatt von *Asservat_23948.img*

```
(kali-user㉿kali-user)-[~/Documents]
└─$ mmcatt Asservat_23948-24.img 0 > part0
(kali-user㉿kali-user)-[~/Documents]
└─$ mmcatt Asservat_23948-24.img 1 > part1
(kali-user㉿kali-user)-[~/Documents]
└─$ mmcatt Asservat_23948-24.img 2 > part2
(kali-user㉿kali-user)-[~/Documents]
└─$ mmcatt Asservat_23948-24.img 3 > part3
(kali-user㉿kali-user)-[~/Documents]
└─$ mmcatt Asservat_23948-24.img 4 > part4
(kali-user㉿kali-user)-[~/Documents]
└─$ mmcatt Asservat_23948-24.img 5 > part5
(kali-user㉿kali-user)-[~/Documents]
└─$ mmcatt Asservat_23948-24.img 6 > part6
(kali-user㉿kali-user)-[~/Documents]
└─$ mmcatt Asservat_23948-24.img 7 > part7
(kali-user㉿kali-user)-[~/Documents]
└─$ mmcatt Asservat_23948-24.img 7 > part7
^C
(kali-user㉿kali-user)-[~/Documents]
└─$ mmcatt Asservat_23948-24.img 8 > part8
```

4.2.4 testdisk von *Asservat_23948.img*

Disk Asservat_23948-24.img - 53 GB / 50 GiB - CHS 6528 255 63							Documents - Thunder
Partition	Start	End	Size in sectors				
P FAT32	0	32 33	124 139 32	1998801	[EFI System Partition]	[NO NAME]	
P ext4	124	140 17	4108 93 17	64000000			
>P ext4	4108	93 18	6100 69 49	32000000			

4.2.5 nicht wiederherstellbare Partition

```
The harddisk (53 GB / 50 GiB) seems too small! (< 471 GB / 438 GiB)
Check the harddisk size: HD jumper settings, BIOS detection ...
File System File Edit View Go Bookmarks Places
The following partition can't be recovered:
Partition Start End Size in sectors
> Linux LUKS 6100 69 50 57263 47 19 821932179
```

4.2.6 lsb-release part5

```
DISTRIB_ID=Ubuntu
DISTRIB_RELEASE=22.04
DISTRIB_CODENAME=jammy
DISTRIB_DESCRIPTION="Ubuntu 22.04.4 LTS"
```

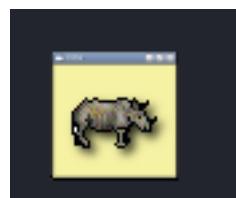
4.2.7 passwd part5

```
alex:x:1000:1000:Alex Adler,,,:/home/alex:/bin/bash
```

4.2.8 shadow part5

```
alex:$y$j9T$V4YmrzhW/WPc.tim6qwXE.$Yk2Uja.Tl8bvlQ2WWbBhm3/DGwXSc5L2N8kU6BE/i41:19838:0:99999:7:::
$boxadd:1:19838:::::
```

4.2.9 rhino-Ikone



4.2.10 Reddit Zugriffe

```
sqlite> SELECT * FROM moz_places WHERE url LIKE '%Reddit%' OR title LIKE '%Reddit%';
14:https://www.reddit.com/Mallorca verbietet offenen Alkoholkonsum am Ballermann : r/delmoc.tidder.www.|[55|0|1|5363|171544153333125|N42m5YTrzSlw|0|47359719085711|Reddit ist ein Netzwerk von Communities, in denen Menschen endlos in ihren Interessen, Hobbys und Leidenschaften eintauchen können. Auf Reddit gibt es eine Community für alles, was dich interessiert.|https://www.redditstatic.com/shreddit/assets/favicon/192x192.png||9|0||1
15:https://www.reddit.com/?rdt=65133|How Eric Dier went from Tottenham reject to Bayern Munich's rock at the back to help ignite German giants' quest for Champions League glory... and push for England recall : r/Bundesliga|moc.tidder.www.|[45|0|1|39651|171482587487239|ndc_wXlQTCs|0|47358303617636|Reddit ist ein Netzwerk von Communities, in denen Menschen endlos in ihre Interessen, Hobbys und Leidenschaften eintauchen können. Auf Reddit gibt es eine Community für alles, was dich interessiert.|https://www.redditstatic.com/shreddit/assets/favicon/192x192.png||9|0||1
16:https://www.reddit.com/r/dc/comments/1cdewv/ich_werde_nicht_noch_mit_die_polizei_holen_denn_ich_werde_nicht_noch_mal_die_Polizei_holen_| Der Virologe Christian Drosten wurde auf einem Campingplatz übel beschimpft und ersetzte Anzeige. Als Zeuge im Prozess gegen seine Beleidiger erlebt er nun eine böse Überraschung : r/delmoc.tidder.www.|[2|0|0|168|171439229745697|UAzpsdmVBOLD|0|473565802565231|||9|0||1
17:https://www.reddit.com/r/Finanzen/Comments/1cdfgv3/warum_wird_so_oft_grz%C3%A4hlt_dass_ein_firmenwagen/|Warum wird so oft erzählt, dass ein Firmenwagen günstig ist? : r/Finanzen|moc.tidder.www.|[2|0|0|168|17143926532761|ewJXHSG-o02|0|47356684631025|||9|0||1
18:https://www.reddit.com/r/pics/Comments/1cdfbux/sniper_on_the_roof_of_student_union_building_imu/|Sniper on the roof of student union building (IMU) at Indiana University : r/pics|moc.tidder.www.|[2|0|0|168|1714139417085471|I-pLOVyl0D2|0|47357285275911|||9|0||1
19:https://www.reddit.com/r/de/Comments/1cdia9e/gro%C3%9Fer_%C3%A4rger_mit_heranwachsenden_im_kreis/|Großer Ärger mit Heranwachsenden: Im Kreis Ludwigsburg wütten offenbar zwei Kindergangs : r/delmoc.tidder.www.|[2|0|0|168|1714139670020663|l99_arGbo40E|0|47357489700068|||9|0||1
20:https://www.reddit.com/r/deutschememes/Comments/1cdjzu2/schlimmste_damals/|Schlimmste damals : r/deutschememes|moc.tidder.www.|[2|0|0|168|1714139670020663|l99_arGbo40E|0|47357489700068|||9|0||1
21:https://www.reddit.com/r/ich_iel/Comments/1cdhDrv/iichel/|ich_iel : r/ich_iel|moc.tidder.www.|[2|0|0|168|1714139746987539|04KxA55y8OWC|0|473589345148951|||9|0||1
22:https://www.reddit.com/r/pcmasterrace/Comments/1cdjrj3/is_it_normal_that_the_exact_240_hz_does_not_appear/|Is it normal that the exact 240 Hz does not appear? : r/pcmasterrace|moc.tidder.www.|[2|0|0|168|1714139817013367|A9ejUU00zKKH|0|47358100831176|||9|0||1
23:https://www.reddit.com/r/de/Comments/1cdifv1/bgh_bezeichnet_korrektur_von_cannabisbeschluss/|BGH bezeichnet Korrektur von Cannabis-Beschluss als "Versehen" : r/delmoc.tidder.www.|[3|0|0|252|1714140128766628|1Yrib_tavxc_|0|7357971876442|||9|0||1
```

4.2.11 E-Mail Adresse part6

```
Auto-Sabotage! auto_gen...
To: alex.adler1@gmx.de
```

4.2.12 keine Kommunikation mit rhinobroker@reddit.com

```
└──(kali-user㉿kali-user)-[~/Documents]
    $ cat inbox | grep 'info@mittelfrankenjobs.de'
From: "info@mittelfrankenjobs.de" <info@mittelfrankenjobs.de>
From: "info@mittelfrankenjobs.de" <info@mittelfrankenjobs.de>
From: "info@mittelfrankenjobs.de" <info@mittelfrankenjobs.de>
From: "info@mittelfrankenjobs.de" <info@mittelfrankenjobs.de>

└──(kali-user㉿kali-user)-[~/Documents]
    $ cat inbox | grep 'rhinobroker@reddit.com'
```

4.2.13 bash_history

```
└──(kali-user㉿kali-user)-[~/Documents]
    $ icat part6 133181 > bash_history

└──(kali-user㉿kali-user)-[~/Documents]
    $ cat bash_history
sudo apt update
sudo apt upgrade
sudo apt update
sudo apt upgrade
sudo -i
clear
sudo apt upgrade
sudo apt autoremove
sudo apt update
sudo apt upgrade
ls -lh
sudo chown alex:alex -R .
nano passwortListe.txt
sudo apt update
sudo apt upgrade
```

4.2.14 Bildchirmfoto mit Passwörter

```
(kali-user㉿kali-user)-[~/Documents]
└─$ cat Bildschirmfotos_2
PW. Verschl. Part.: RHVGaG9zRmNNITc5WUpGNA=
PW. E-Mail: NXpzVzU5cFExMg=
```

4.2.15 photorec

```
(kali-user㉿kali-user)-[~/Documents]
└─$ grep -ri "rhino" recuper_dir.*
grep: recuper_dir.2/f13856672_chrome.zip: binary file matches
grep: recuper_dir.37/f33996288_ftyp.mov: binary file matches
grep: recuper_dir.46/f41850730_mdat.mov: binary file matches

(kali-user㉿kali-user)-[~/Documents]
└─$ grep -ri "nashorn" recuper_dir.*
grep: recuper_dir.49/f68100288.jpg: binary file matches
```

4.2.16 Bluetooth-versuch

```
[system] Failed to activate service 'org.bluez': timed out (service_start_timeout=25000ms)
```

4.2.17 Cronjobs auth.log.1

```
May  4 17:17:01 adlerhorst CRON[5415]: pam_unix(cron:session): session opened for user root(uid=0) by (uid=0)
May  4 17:17:01 adlerhorst CRON[5415]: pam_unix(cron:session): session closed for user root
May  4 17:30:01 adlerhorst CRON[5718]: pam_unix(cron:session): session opened for user root(uid=0) by (uid=0)
May  4 17:30:01 adlerhorst CRON[5718]: pam_unix(cron:session): session closed for user root
```

4.2.18 cron.hourly

```
$ cat cron.hourly
#
#
# .placeholder
#
```

4.2.19 clamscan

```
(kali-user㉿kali-user)-[~/Documents]
└─$ clamscan Asservat_23948-24.img
Loading: 20s, ETA: 0s [=====] 8.70M/8.70M sigs
Compiling: 3s, ETA: 0s [=====] 41/41 tasks

/home/kali-user/Documents/Asservat_23948-24.img: OK

----- SCAN SUMMARY -----
Known viruses: 8695702
Engine version: 1.3.1
Scanned directories: 0
Scanned files: 1
Infected files: 0
Data scanned: 0.00 MB
Data read: 51200.00 MB (ratio 0.00:1)
Time: 25.246 sec (0 m 25 s)
Start Date: 2024:07:06 17:43:34
End Date: 2024:07:06 17:43:59
```

4.3 Gefundene Bilder

4.3.1 *f68098048.jpg* (von PhotoRec zugeordneter Name)



4.3.2 *f68100288.jpg* (von PhotoRec zugeordneter Name)



4.3.3 f68104640.jpg (von PhotoRec zugeordneter Name)



4.3.4 f68109184.jpg (von PhotoRec zugeordneter Name)



4.3.5 *f68109312.jpg* (von PhotoRec zugeordneter Name)



4.3.6 *f71245208.jpg* (von PhotoRec zugeordneter Name)

