

Who Are You?

Forensisches Fallbeispiel

Praktische Arbeit

zu Modul 116 - Unix-Forensik



vorgelegt von: Michael Koll

Matrikelnummer:

Prüfer:

© 2019

Inhaltsverzeichnis

| | |
|--|-----------|
| 1. Einleitung | 3 |
| 1.1. Asservate | 3 |
| 1.2. Vorgehen | 4 |
| 2. Befunde | 6 |
| 2.1. Zuordnungen | 6 |
| 2.2. Container | 7 |
| 2.3. User-Verzeichnisse | 9 |
| 2.4. Gelöschte Dateien | 12 |
| 2.5. E-Mail-Konten | 12 |
| 2.6. E-Mail-Verkehr | 13 |
| 2.7. Browser | 18 |
| 2.8. HTTP-Server | 18 |
| 2.9. MySQL-Server | 19 |
| 2.10. USB-Sticks | 20 |
| 2.11. Konten und Anmeldungen | 23 |
| 2.12. Bild- und Videodateien | 24 |
| 2.12.1. Timeline USB-Sticks | 25 |
| 2.12.2. Timeline Virtuelle Maschinen | 26 |
| 3. Zusammenfassung | 28 |
| 3.1. Beteiligte und Rollen | 28 |
| 3.2. Timeline | 29 |
| 3.3. Illegaler Bild- und Videobesitz | 31 |
| 3.4. Herkunft USB-Sticks | 31 |
| 3.5. Kundendaten | 31 |
| 3.6. Offene Fragen und Anmerkungen | 32 |
| Eidesstattliche Erklärung | 33 |
| Verzeichnis der Listings | 34 |
| Abbildungsverzeichnis | 35 |
| Tabellenverzeichnis | 37 |

| | |
|--------------------------|-----------|
| A. Anhang | 38 |
| A.1. Skripte | 39 |
| A.2. Konten | 45 |
| A.3. E-Mails | 48 |
| A.4. Zeitgeist | 56 |
| A.5. Medien | 57 |

1. Einleitung

1.1. Asservate

Bei vorangegangenen Untersuchungen wurden dreivirtuelle Maschinen in Form von OVA-Dateien, Arbeitsspeicher-Dumps und HDD-Dumps, sowie vier USB-Sticks sichergestellt (siehe Tabelle 1.1):

| ID | Name | Datei | MD5 |
|----|--------|------------------|----------------------------------|
| 1 | Stick1 | stick1.dd | 0047551735d73c94304e80b73c18a72a |
| 2 | Stick2 | stick2.dd | 14749008f93808ca6140f030d79d86a2 |
| 3 | Stick3 | stick3.dd | e47e70d2a70a5e5258f283c4acdf93b |
| 4 | Stick4 | stick4.dd | 569d95ca3fc957bf9dcdb92521499712 |
| 5 | VM1mem | memdump_vm1.lime | a874d64cb8a28e1d9262f7cb6776fee1 |
| 6 | VM1ova | vm1.ova | ac8aaf5a75ccda58b283fcd81c3f4b02 |
| 7 | VM1dd | vm1_dd | d5bdb02e13a75504a23b7bfd35b5bbe |
| 8 | VM2mem | memdump_vm2.lime | ece046c70a309d2c5c011cab80c88655 |
| 9 | VM2ova | vm2.ova | dd5209639ea3ae6c60652b238b0c82ed |
| 10 | VM2dd | vm2_dd | c840b5932059e762b78716e40f22cc14 |
| 11 | VM3mem | memdump_vm3.lime | 621dbaab6472708ce2520406f185cae8 |
| 12 | VM3ova | vm3.ova | 09bb97d2e1687027d1bccd52f22aa34d |
| 13 | VM3dd | vm3_dd | e1a97a9bfe51ccef923925006965b4 |

Tabelle 1.1.: Untersuchte Asservate

Weiterhin wurde ein Notizzettelsichergestellt, der die in Tabelle 1.2 aufgeführten Informationen enthält, bei denen es sich vermutlich um Zugangsdaten handelt:

| Typ | Wert |
|--------------|---------------|
| Benutzername | Nitro |
| Benutzername | Niko Nerd |
| Benutzername | user |
| Benutzername | Muti |
| Benutzername | Mathias Mutig |
| Benutzername | Pepp |

| | |
|--------------|----------------|
| Benutzername | Peter Pepper |
| Benutzername | root |
| E-Mail-Konto | nitro94@gmx.de |
| E-Mail-Konto | muti97@gmx.de |
| E-Mail-Konto | pepp87@gmx.net |
| Passwort | 12345678 |
| Passwort | 123456 |
| Passwort | abcd1234 |

Tabelle 1.2.: Notizzettel

1.2. Vorgehen

In den folgenden Abschnitten wird das Vorgehen zur Analyse der Asservate grob beschrieben, inklusive der verwendeten Software.

Arbeitsspeicheranalyse

Die Arbeitsspeicheranalyse wurde auf einer virtuellen Maschine mit dem Betriebssystem Remnux durchgeführt. Die Analyse der Arbeitsspeicherdumps erfolgte mit dem Tool Volatility in der Version 2.5.

Aufgrund der unterschiedlichen Betriebssystemversionen der virtuellen Maschinen wurden folgende Volatility-Profile verwendet:

| VM | Profil |
|-----|---------------------------------|
| VM1 | LinuxUbuntu4_2_0-27-genericx64 |
| VM2 | LinuxUbuntu4_2_0-16-genericx64 |
| VM3 | LinuxUbuntu3_19_0-15-genericx64 |

Tabelle 1.3.: Verwendete Volatility-Profile

Für alle drei virtuelle Maschinen wurden zu Beginn vordefinierte Plugins ausgeführt und die Ergebnisse in Textdateien gespeichert. Die ausgeführten Plugins sind in A.1 aufgeführt, die Ergebnisdateien liegen vollständig auf dem Datenträger bei (`results/volatilityplugins/`).

Dateianalyse

Zur Analyse der Dateien in Form der Festplattendumps, USB-Sticks und weiterer Outputs wurde Autopsy in der Version 4.13 auf einer virtuellen Windows-Maschine verwendet. Dazu wurden alle Festplattenabbilder, USB-Stick-Abbilder und weitere Dateien wie die Volatility-Ausgaben in einen Case importiert.












| Data Source Name | Type | Files | Results | Tags |
|--|--|--------|---------|------|
|  stick1.dd | Flash Drive | 2916 | 209 | 8 |
|  Stick2.dd | Flash Drive | 8827 | 1138 | 6 |
|  Stick3.dd | Flash Drive | 481 | 112 | 5 |
|  Stick4.dd | Flash Drive | 28 | 19 | 14 |
|  volatilityoutput | | 49 | 14 | 0 |
|  vm1_dd.001 | OS Drive (Linux Debian), OS Drive (Linu... | 427062 | 172068 | 125 |
|  vm2_dd.001 | OS Drive (Linux Debian), OS Drive (Linu... | 495700 | 117307 | 79 |
|  vm3_dd.001 | | 643 | 63 | 0 |
|  vm3_luks_decr.dd | OS Drive (Linux Debian), OS Drive (Linu... | 474311 | 188518 | 37 |
|  Container VM1 | | 39 | 19 | 19 |
|  Container VM2 | | 2 | 0 | 0 |

Abbildung 1.1.: Datenquellen Autopsy

Der vollständige Autopsy Ergebnis-Report ist unter **results/autopsy** angefügt.

Relevante Informationen, wie gefundene Benutzernamen, IP-Adressen o.ä. wurden in Suchsets eingetragen, um Vorkommnisse auf den untersuchten Datenträgern und Dateien zu finden.

Relevante Dateien (Medien, Vertriebspläne), die während der Analyse gefunden wurden, wurden in ein Hash-Set eingetragen um alle Vorkommnisse auf den untersuchten Datenträgern zu finden.

Virtuelle Maschinen

Die virtuellen Maschinen wurden zur Verifizierung gewisser Annahmen gestartet und diese überprüft. Alle in diesem Bericht dargestellten Befunde können ohne den Start der virtuellen Maschinen extrahiert werden.

2. Befunde

2.1. Zuordnungen

Tabellen 2.1 und 2.2 stellen eine Zusammenfassung der Zuordnungen dar, die während der Analyse ermittelt werden konnten.

| VM Name | | Username | Mail | IP |
|---------|---------------|----------|----------------|----------------|
| vm1 | Niko Nerd | user | nitro94@gmx.de | 192.168.178.31 |
| vm2 | Mathias Mutig | user | muti97@gmx.de | 192.168.178.47 |
| vm3 | Peter Pepper | user | pepp87@gmx.de | 192.168.178.23 |

Tabelle 2.1.: Zuordnungen Übersicht

| Passwort | Verwendung |
|-----------|-------------------------------------|
| abcd1234 | LUKS-Partition VM3 |
| 123456 | Benutzer user VM1 |
| 123456 | Benutzer user VM2 |
| 123456 | Benutzer user VM3 |
| 12345678 | E-Mail nitro95@gmx.de |
| 12345678 | E-Mail muti97@gmx.de |
| 12345678 | E-Mail pepp87@gmx.net |
| abcd1234 | Container VM1 |
| abcd1234 | Container VM2 (TrueCrypt) |
| geheim321 | Bilder.zip (Stick 4) |
| geheim123 | Kundendaten_Sicherung.zip (Stick 4) |

Tabelle 2.2.: Zuordnungen Passwörter

2.2. Container

Auf den Asservaten konnten diverse verschlüsselte Container gefunden werden, deren Entschlüsselung und Inhalt in den folgenden Abschnitten beschrieben wird.

Export LUKS-Partition VM3

Der Festplattendump der VM3 enthält eine LUKS-Partition, die verschlüsselt ist. Zum Entschlüsseln wurde die Partition aus Autopsy exportiert. Anschließend wurde die Partition mittels `cryptsetup` und dem Passwort `abcd1234` entschlüsselt und eine Kopie mittels `dd` erzeugt (siehe Abbildung 2.1).

```
mkoll@mkoll:~$ sudo cryptsetup luksOpen /home/mkoll/Studium/M116/PA/Exports/luks/vm3_dd.001-Unalloc-1223194-1223820.dat vm3_luks
Geben Sie die Passphrase für »/home/mkoll/Studium/M116/PA/Exports/luks/vm3_dd.001-Unalloc-1223194-1223820.dat« ein:
mkoll@mkoll:~$ sudo mount /dev/mapper/vm3_luks /media/vm3_luks
mkoll@mkoll:~$ dd if=/dev/mapper/vm3_luks of=/home/mkoll/Studium/M116/PA/Exports/luks/vm3_luks_decr.dd
dd: konnte '/dev/mapper/vm3_luks' nicht öffnen: Keine Berechtigung
mkoll@mkoll:~$ sudo !!
sudo dd if=/dev/mapper/vm3_luks of=/home/mkoll/Studium/M116/PA/Exports/luks/vm3_luks_decr.dd
29876224+0 Datensätze ein
29876224+0 Datensätze aus
15296626688 Bytes (15 GB, 14 GiB) kopiert, 135,776 s, 113 MB/s
mkoll@mkoll:~$ md5sum /home/mkoll/Studium/M116/PA/Exports/luks/vm3_luks_decr.dd
597cfe9f1d7b970e9255a5fed4e5fe /home/mkoll/Studium/M116/PA/Exports/luks/vm3_luks_decr.dd
mkoll@mkoll:~$
```

Abbildung 2.1.: LUKS-Partition entschlüsseln und kopieren

Die extrahierte entschlüsselte Partition wurde anschließend wie oben beschrieben mit Autopsy untersucht.

Entschlüsselung Veracrypt-Container

Auf VM1 und VM2 wurden im Pfad `/home/user/Container` eine Datei `Container` gefunden und ebenfalls durch Autopsy als möglicher verschlüsselter Container erkannt.

Beide Container konnten mittels Veracrypt und den auf dem Notizzettel gefundenen Passwort `abcd1234` entschlüsselt werden. Die benötigten Einstellungen sind in den Abbildungen 2.2 und 2.3 abgebildet.

Beide Container wurden anschließend in Autopsy als Data Source hinzugefügt und im Rahmen der weiteren Analyse betrachtet.

WHO ARE YOU?

Forensisches Fallbeispiel

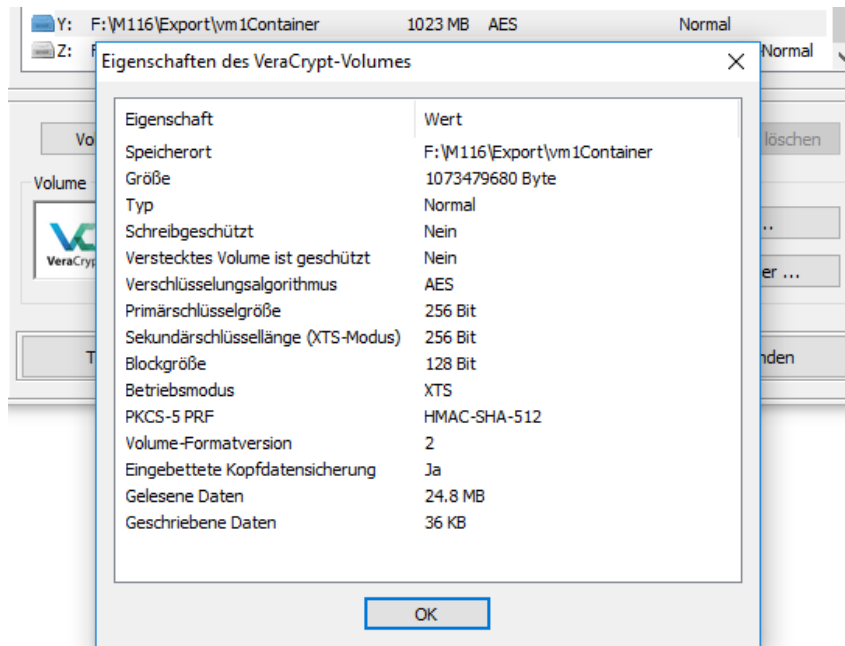


Abbildung 2.2.: Veracrypt Eigenschaften Container VM1

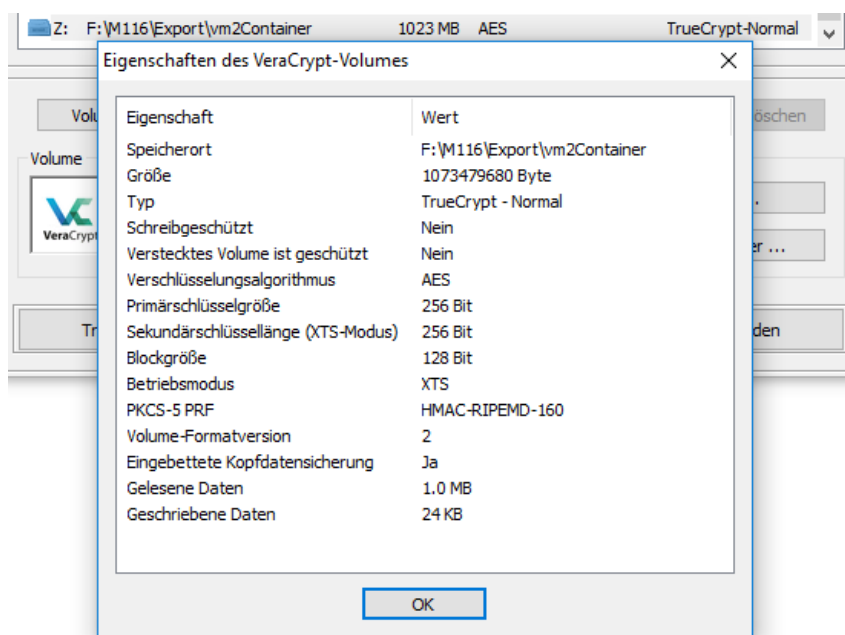


Abbildung 2.3.: Veracrypt Eigenschaften Container VM2

2.3. User-Verzeichnisse

Mittels Autopsy wurden auf allen Datenträgern das Nutzerverzeichnis des Nutzers **user** ausgewertet. Auffällige Mediendateien wurden in das Hashset aufgenommen und markiert (siehe 2.12).

In den folgenden Abschnitten werden Besonderheiten aufgeführt, die auf den Datenträgern in den Nutzerverzeichnissen gefunden wurden.

VM1

Bash-History

In der Bash-History von VM1 wurden folgende relevanten Aktionen gefunden (siehe `/results/.bash_history_vm1`):

- Installation Apache
- Installation VeraCrypt
- Diverse Kopier- und Verschiebevorgänge der Daten `neue_ware.tar.gz`
- SSH-Session zu 192.168.178.47 (VM2)
- MySQL-Login zu 192.168.178.23 (VM3)

Die Einträge der Bash-History konnten über die Analyse des Arbeitsspeichers verifiziert werden (siehe `results/volatilityplugins/vm1/linux_bash.vol`).

Zeitgeist

Die Analyse der Zeitgeistaktivitäten der SQLite-Datenbank `/home/user/.local/share/zeitgeist/activity.sqlite` (siehe `/results/zeitgeist/activity.sqlite_vm1`) erfolgte mittels SQLiteBrowser und der in Listing A.4 dargestellten Abfrage. Die vollständigen Ergebnisse der Abfrage sind in der Datei `results/zeitgeist/activity_vm1.csv` gespeichert, folgende Tabelle stellt die wichtigsten Ergebnisse interpretiert mit der Bash-History dar:

| Zeitstempel (UTC+2) | Objekt | Aktion |
|------------------------|------------|--|
| 2016-04-16 10:12:37 | VeraCrypt | Installation |
| ab 2016-07-18 10:31:15 | USB-Sticks | Zugriff auf USB6, USB2, USB5, USB1, USB4, USB3, USB7, USB9, USB8 |

| | | |
|-------------------------|-----------------|--|
| 2016-07-19 13:25:44 | Thunderbird | Start |
| 2016-07-29 11:33:06 | Thunderbird | Start (Mail 003 gelesen) |
| 2016-07-29 11:54:02 | Mediendateien | Erstellt in Desktop |
| 2016-07-29 11:59:35 | Archive Manager | Erstellt neue_ware.tar.gz |
| ca. 2016-07-29 12:01:39 | Archive Manager | neue_ware.tar.gz verschieben nach /var/www |
| 2016-07-31 12:06:57 | Thunderbird | Versand Mail 004 |
| 2016-08-10 12:42:47 | Thunderbird | Start (Mail 005 gelesen) |
| 2016-08-10 12:43:11 | Terminal | SSH-Session 192.168.178.47 (Vertriebsplan nach Desktop kopiert mittels GEdit) |
| 2016-08-16 13:21:08 | Text Editor | Vertriebsplan.txt öffnen |
| 2016-08-16 13:24:18 | Archive Manager | Kopie neue_ware.tar.gz nach Downloads und entpacken |
| ab 2016-08-16 13:25:29 | Mediendateien | Erstellen von Verzeichnis Mark_Quark und kopieren der Mediendateien (15 Bilder / 1 Video) |
| ab 2016-08-16 13:26:29 | Mediendateien | Erstellen von Verzeichnis Bart_Simpson und kopieren der Mediendateien (7 Bilder / 3 Videos) |
| ab 2016-08-16 13:26:56 | Mediendateien | Erstellen von Verzeichnis Pumuckel und kopieren der Mediendateien (2 Bilder) |
| ab 2016-08-16 13:34:22 | VeraCrypt | Starten von Veracrypt und Kopie Mediendateien in Container |
| ab 2016-08-16 13:41:52 | Mediendateien | Verschieben von Mediendateien in Container in Textdateien (Urlaub*.txt) |

Tabelle 2.3.: Zeitgeist-Events VM1

VM2

Bash-History

In der Bash-History von VM2 wurden folgende relevanten Aktionen gefunden (siehe `/results/.bash_history_vm2`):

- Installation OpenSSH-Server
- Installation TrueCrypt
- Bearbeitung Vertriebsplan

Die Einträge der Bash-History konnten über die Analyse des Arbeitsspeichers verifiziert werden (siehe `results/volatilityplugins/vm2/linux_bash.vol`).

Zeitgeist

Die Analyse der Zeitgeistaktivitäten der SQLite-Datenbank `/home/user/.local/share/zeitgeist/activity.sqlite` (siehe `/results/zeitgeist/activity.sqlite.vm2`) erfolgte mittels SQLiteBrowser und der in Listing A.4 dargestellten Abfrage. Die vollständigen Ergebnisse der Abfrage sind in der Datei `results/zeitgeist/activity.vm2.csv` gespeichert, folgende Tabelle stellt die wichtigsten Ergebnisse interpretiert mit der Bash-History dar:

| Zeitstempel (UTC+2) | Objekt | Aktion |
|------------------------|-----------------|---|
| 2016-05-09 11:29:11 | TrueCrypt | Installation |
| ab 2016-07-18 10:43:18 | USB-Sticks | Zugriff auf USB5, USB6, USB2, USB1, USB4. USB9 |
| 2016-07-18 13:37:47 | Thunderbird | Start (Mail 001 gelesen) und Speichern <code>IMAGE_121.JPG</code> |
| ab 2016-07-23 14:11:19 | Text Editor | Erstellen <code>Desktop/Vertriebsplan.txt</code> |
| 2016-07-20 11:37:47 | Thunderbird | Start (Versand Mail 002) |
| 2016-07-29 11:34:33 | Thunderbird | Start (Versand Mail 003) |
| 2016-08-02 12:22:36 | Thunderbird | Start (Mail 004 gelesen) |
| 2016-08-02 12:23:27 | FireFox | Download <code>neue_ware.tar.gz</code> |
| 2016-08-06 12:32:18 | Thunderbird | Start (Versand Mail 005) |
| 2016-08-16 14:07:54 | Archive Manager | Entpacken <code>neue_ware.tar.gz</code> |
| ab 2016-08-16 14:09:17 | Mediendateien | Erstellen von Verzeichnis <code>DieMaus</code> und kopieren der Mediendateien (15 Bilder) |
| ab 2016-08-16 14:09:50 | Mediendateien | Erstellen von Verzeichnis <code>BerndDasBrot</code> und kopieren der Mediendateien (2 Bilder / 1 Video) |
| ab 2016-08-16 14:10:17 | Mediendateien | Erstellen von Verzeichnis <code>AeffleundPferde</code> und kopieren der Mediendateien (10 Bilder / 4 Video) |
| ab 2016-08-16 14:10:48 | Mediendateien | Verschieben aller Kundenordner (Ziel unklar) |

Tabelle 2.4.: Zeitgeist-Events VM2

VM3

Bash-History

In der Bash-History von VM3 wurden folgende relevanten Aktionen gefunden (siehe `/results/.bash_history_vm3`):

- Nutzung des lokalen MySQL-Servers
- Installation VeraCrypt
- Kopieren der Inhalte des Ordners `/home/user/Downloads/Pinocchio/*`

Die Einträge der Bash-History konnten über die Analyse des Arbeitsspeichers verifiziert werden (siehe `results/volatilityplugins/vm3/linux_bash.vol`).

Zeitgeist

Die Analyse der Zeitgeistaktivitäten der SQLite-Datenbank `/home/user/.local/share/zeitgeist/activity.sqlite` (siehe `/results/zeitgeist/activity.sqlite.vm2`) erfolgte mittels SQLiteBrowser und der in Listing A.4 dargestellten Abfrage. Die vollständigen Ergebnisse der Abfrage sind in der Datei `results/zeitgeist/activity.vm2.csv` gespeichert.

Das Logging über Zeitgeist wurde auf VM3 deaktiviert. Dies geschah vermutlich am 25.05.19 11:56:32, welches den letzten Logeintrag von Zeitgeist darstellt.

2.4. Gelöschte Dateien

2.5. E-Mail-Konten

Bei der Analyse der Festplatten wurden drei E-Mail-Konten in dem E-Mailprogramm Thunderbird gefunden. Bei allen drei Accounts handelt es sich um GMX-Accounts (siehe Tabelle 2.5), durch einen Login im GMX-Accounts unter <https://www.gmx.de> konnten die zugehörigen hinterlegten Adressen extrahiert werden (siehe Bilder A.1, A.2 und A.3).

| ID | Mail | Name | Kundennummer |
|------|----------------|--------------|--------------|
| EMK1 | nitro94@gmx.de | Niko Nerd | 278927850 |
| EMK2 | muti97@gmx.de | Markus Mutig | 278927594 |

| | | | |
|------|----------------|--------------|-----------|
| EMK3 | pepp87@gmx.net | Peter Pepper | 278928295 |
|------|----------------|--------------|-----------|

Tabelle 2.5.: Übersicht E-Mail-Konten

2.6. E-Mail-Verkehr

Unter Verwendung von Autopsy konnten die in Tabelle 2.6 aufgelisteten E-Mails sichergestellt werden. Mails, die eindeutig nicht relevant für den Fall sind (z.B. Werbemails von GMX) wurden vernachlässigt. Die Auswertung wurde mit Hilfe von Autopsy und den gesicherten virtuellen Maschinen bzw. dem dort installierten E-Mail-Programm **Thunderbird** durchgeführt. Die E-Mail-Header wurden auf Auffälligkeiten wie auffällige IP-Adressen oder E-Mail-Server untersucht, es konnten keine Auffälligkeiten festgestellt werden, die dem unten dargestellten Ablauf widersprechen.

Alle E-Mails wurden als EML-Dateien unter **results/emails** abgelegt. Die Inhalte der Postfächer wie sie zum Start der jeweiligen VMs vorgefunden wurden sind in Abschnitt A.3 aufgeführt. Tabelle 2.6 stellt eine Zusammenfassung aller relevanten E-Mails dar. Die Zeitstempel wurden den E-Mail-Headern der EML-Dateien entnommen, wobei **Received** den Zeitstempel der GMX-Email-Server beschreibt und **Date** das Date-Feld des E-Mail-Headers. In den anschließend folgenden Abbildungen (2.5 bis 2.9) ist der jeweilige Textinhalte der E-Mail dargestellt.

| ID | Received | Date | Von | An | Betreff | Link |
|-----|--------------|---------------|---------|---------|--------------------|------|
| 001 | 18.07. 13:30 | 18.07. 13:30 | pepp87 | muti97 | Neue Aufträge | 2.5 |
| 002 | 18.07. 13:42 | nicht bekannt | muti97 | niko94 | neue Aufträge | 2.6 |
| 002 | 18.07. 13:42 | 20.07. 13:45 | muti97 | pepp87 | neue Aufträge | 2.6 |
| 003 | 19.07. 11:33 | 29.07. 11:36 | muti97 | nitro94 | Fwd: neue Aufträge | 2.7 |
| 004 | 19.07. 12:07 | 31.07. 12:10 | nitro94 | muti97 | Ware ist da | 2.8 |
| 004 | 19.07. 12:07 | 31.07. 12:10 | nitro94 | pepp87 | Ware ist da | 2.8 |
| 005 | 19.07. 12:32 | 06.08. 12:35 | muti97 | nitro94 | Vertriebsplan | 2.9 |
| 005 | 19.07. 12:32 | 06.08. 12:35 | muti97 | pepp87 | Vertriebsplan | 2.9 |

Tabelle 2.6.: Übersicht E-Mails

Für den E-Mailempfänger der Nachricht 002 ~~niko94@gmx.de~~ konnten keine weiteren Spuren gefunden werden, weshalb beim weiteren Verlauf der Untersuchungen davon ausgegangen wird, dass dies ein Tippfehler war und keine vierte beteiligte Person.

WHO ARE YOU?

Forensisches Fallbeispiel

Zusammenfassend ergibt sich für die E-Mail-Kommunikation die in Abbildung 2.4 dargestellte Timeline, basierend auf dem Date-Feld der E-Mail-Header¹.

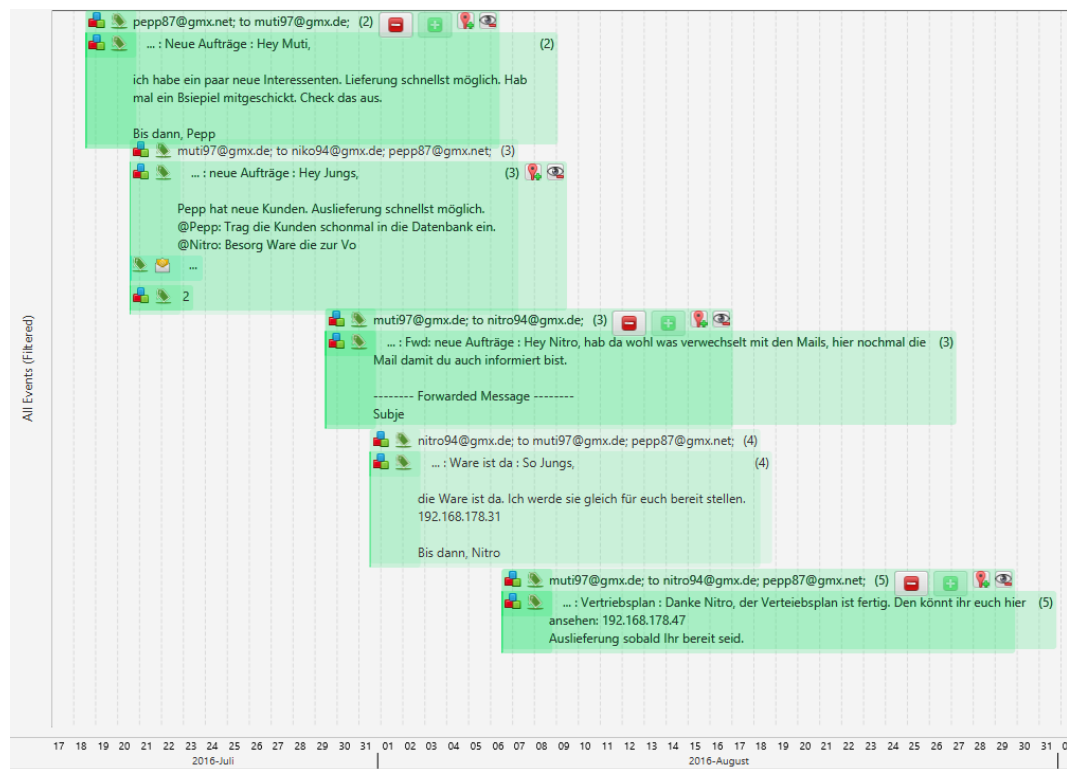


Abbildung 2.4.: Timeline der E-Mail-Kommunikation

¹Die MTA-Daten scheinen nicht plausibel zu sein und werden als Übungskünstlichkeit betrachtet.

WHO ARE YOU?

Forensisches Fallbeispiel

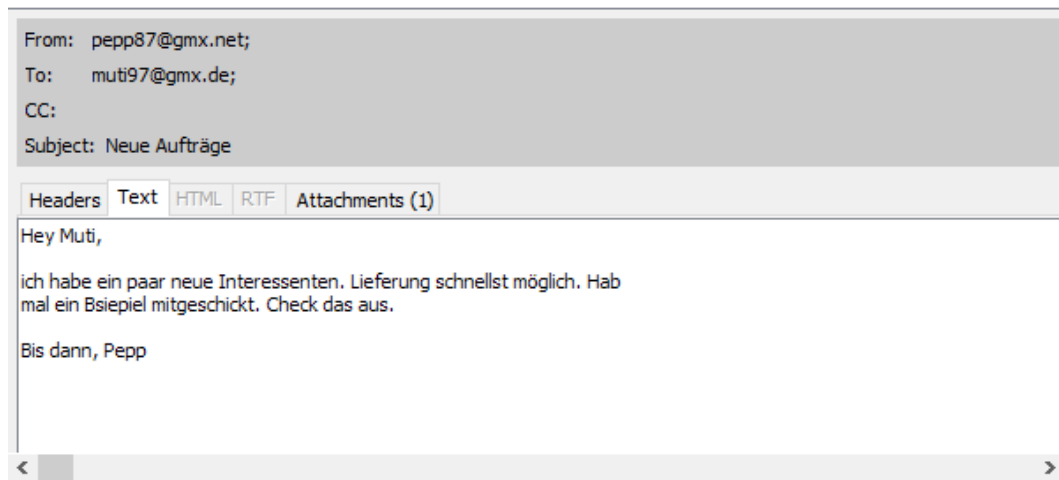


Abbildung 2.5.: Email 001 - Neue Aufträge



Abbildung 2.6.: Email 002 - neue Aufträge

WHO ARE YOU?

Forensisches Fallbeispiel



Abbildung 2.7.: Email 003 - Fwd: neue Aufträge



Abbildung 2.8.: Email 004 - Ware ist da

WHO ARE YOU?

Forensisches Fallbeispiel



Abbildung 2.9.: Email 005 - Vertriebsplan

2.7. Browser

In diesem Abschnitt werden die relevanten Spuren der Browser-History dargestellt. Diese basieren auf den durch Autopsy extrahierten Artefakten.

Wie in Abbildung 2.10 zu sehen wird am 02.08.16 um 12:23:06 die Datei `neue_ware.tar.gz` von dem Webserver auf VM1 auf VM2 heruntergeladen. Dies bestätigt ebenfalls die Ergebnisse der Zeitgeist-Analyse (siehe Tabelle 2.4).

| | | |
|---------------------|---------------|---|
| 2016-05-09 11:28:46 | Web History | https://download.truecrypt.ch/older/truecrypt-6.3a-ubuntu-x64.tar.gz |
| 2016-05-09 11:28:48 | Web History | https://download.truecrypt.ch/older/truecrypt-6.3a-ubuntu-x64.tar.gz |
| 2016-05-09 11:28:48 | Web Downl... | https://download.truecrypt.ch/older/truecrypt-6.3a-ubuntu-x64.tar.gz |
| 2016-05-09 11:29:53 | Web Cookies | .google.de |
| 2016-05-09 11:29:55 | Web Search... | www.google.de |
| 2016-05-09 11:29:55 | Web History | https://www.google.de/search?client=ubuntu&channel=fs&q=truecrypt+older&ie=utf-8&oe=utf-8&gfe_rd=cr&ei=FFgwV5OvJaSI8Qfr3KWIDQ |
| 2016-05-09 11:29:55 | Web Cookies | .google.de |
| 2016-05-09 11:29:57 | Web Cookies | www.google.de |
| 2016-05-09 11:29:57 | Web Cookies | .google.de |
| 2016-05-09 11:30:03 | Web History | https://download.truecrypt.ch/older/ |
| 2016-08-02 12:23:35 | Web Cookies | .google.com |
| 2016-08-02 12:23:36 | Web History | http://192.168.178.31/ |
| 2016-08-02 12:24:01 | Web History | http://192.168.178.31/neue_ware.tar.gz |
| 2016-08-02 12:24:06 | Web History | http://192.168.178.31/neue_ware.tar.gz |
| 2016-08-02 12:24:06 | Web Downl... | http://192.168.178.31/neue_ware.tar.gz |

Abbildung 2.10.: Browserverlauf VM2

In der Web-History von VM3 kann der Download der Datei `neue_ware.tar.gz` am 02.08.16 um 12:28:00 bestätigt werden (siehe 2.11)

| | | |
|---------------------|---------------|---|
| 2016-05-09 11:28:46 | Web History | https://download.truecrypt.ch/older/truecrypt-6.3a-ubuntu-x64.tar.gz |
| 2016-05-09 11:28:48 | Web History | https://download.truecrypt.ch/older/truecrypt-6.3a-ubuntu-x64.tar.gz |
| 2016-05-09 11:28:48 | Web Downl... | https://download.truecrypt.ch/older/truecrypt-6.3a-ubuntu-x64.tar.gz |
| 2016-05-09 11:29:53 | Web Cookies | .google.de |
| 2016-05-09 11:29:55 | Web Search... | www.google.de |
| 2016-05-09 11:29:55 | Web History | https://www.google.de/search?client=ubuntu&channel=fs&q=truecrypt+older&ie=utf-8&oe=utf-8&gfe_rd=cr&ei=FFgwV5OvJaSI8Qfr3KWIDQ |
| 2016-05-09 11:29:55 | Web Cookies | .google.de |
| 2016-05-09 11:29:57 | Web Cookies | www.google.de |
| 2016-05-09 11:29:57 | Web Cookies | .google.de |
| 2016-05-09 11:30:03 | Web History | https://download.truecrypt.ch/older/ |
| 2016-08-02 12:23:35 | Web Cookies | .google.com |
| 2016-08-02 12:23:36 | Web History | http://192.168.178.31/ |
| 2016-08-02 12:24:01 | Web History | http://192.168.178.31/neue_ware.tar.gz |
| 2016-08-02 12:24:06 | Web History | http://192.168.178.31/neue_ware.tar.gz |
| 2016-08-02 12:24:06 | Web Downl... | http://192.168.178.31/neue_ware.tar.gz |

Abbildung 2.11.: Browserverlauf VM3

2.8. HTTP-Server

Auf VM1 wird eine Apache-Webserver betrieben, über den die Datei `neue_ware.tar.gz` bereitgestellt wird. Die bereits durch die Zeitgeist-Analyse und die Web-

History bestätigten Downloads von VM2 und VM3 können in der Protokollierung des Apache-Webserver bestätigt werden(/var/log/apache2/access.log.1).

```
192.168.178.47 - - [02/Aug/2016:12:23:28 +0200] "GET / HTTP/1.1" 200 3594 "-" "Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:41.0) Gecko/20100101 Firefox/41.0"
192.168.178.47 - - [02/Aug/2016:12:23:28 +0200] "GET /icons/ubuntu-logo.png HTTP/1.1" 200 3688 "http://192.168.178.21/" "Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:41.0) Gecko/20100101 Firefox/41.0"
192.168.178.47 - - [02/Aug/2016:12:23:28 +0200] "GET /favicon.ico HTTP/1.1" 404 508 "-" "Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:41.0) Gecko/20100101 Firefox/41.0"
192.168.178.47 - - [02/Aug/2016:12:24:03 +0200] "GET /neue_ware.tar.gz HTTP/1.1" 200 24138289 "-" "Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:41.0) Gecko/20100101 Firefox/41.0"
192.168.178.23 - - [02/Aug/2016:12:27:55 +0200] "GET /neue_ware.tar.gz HTTP/1.1" 200 24138289 "-" "Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:37.0) Gecko/20100101 Firefox/37.0"
```

Abbildung 2.12.: Apache Zugriffsprotokoll VM1

2.9. MySQL-Server

Auf VM3 wird ein MySQL-Server betrieben, der zur Verwaltung von Kundendaten dient. Das Logfile (/var/log/mysql/mysql.log) ermöglicht es alle Aktionen nachzuvollziehen, die auf dem SQL-Server durchgeführt wurden (siehe `results/mysql/mysql.log.vm2`).

Am 21.07.16 um 13:59 Uhr wird die Kundentabelle angelegt und befüllt. Hierzu werden "Pseudonamen", Adressen und die Anzahl der *bestellten* Bilder eingetragen (siehe Abbildung 2.13).

```
160721 13:51:31      2 Connect          root@localhost on
160721 13:52:25      2 Query select @@version_comment limit 1
160721 13:52:25      2 Query create database if not exists kunden
160721 13:54:29      2 Query SHOW DATABASES
160721 13:56:26      2 Query SELECT DATABASE()
160721 14:01:39      2 Init DB          kunden
160721 14:02:06      2 Query show databases
160721 14:02:06      2 Query show tables
160721 13:59:01      2 Query CREATE TABLE kunden( name varchar(50), addr varchar(200), daten varchar(500), verantw varchar(50) )
160721 13:59:11      2 Query SHOW TABLES
160721 13:59:25      2 Query SHOW FIELDS FROM kunden
160721 14:01:32      2 Query INSERT INTO kunden VALUES("Mark Quark", "Magdeburgerstr. 1, Magdeburg", "15Bilder, 1Video", "")
160721 14:01:39      2 Query SHOW TABLES
160721 14:01:44      2 Query SHOW FIELDS FROM kunden
160721 14:02:06      2 Query SELECT * from kunden
160721 14:02:55      2 Query INSERT INTO kunden VALUES("Bart Simpson", "742 Evergreen Terrace, Springfield", "7Bilder, 3Video", "")
160721 14:03:26      2 Query INSERT INTO kunden VALUES("Fumuckel", "Widenmayerstrasse 1, Muenchen", "2Bilder, 0Video", "")
160721 14:03:58      2 Query INSERT INTO kunden VALUES("Die Maus", "Appelholtsplatz 1, Koeln", "15Bilder, 0Video", "")
160721 14:04:31      2 Query INSERT INTO kunden VALUES("Bernd Das Brot", "Fischmarkt in Erfurt, Erfurt", "2Bilder, 1Video", "")
160721 14:05:17      2 Query INSERT INTO kunden VALUES("Aeffle und Pferdle", "Thomasstr. 43, Stuttgart", "10Bilder, 4Video", "")
160721 14:05:54      2 Query INSERT INTO kunden VALUES("Paul Panzer", "Bachemerstr. 88, Koeln", "2Bilder, 3Videos", "")
160721 14:06:32      2 Query INSERT INTO kunden VALUES("Agent Ranjid", "Alabadstr. 1, Bremen", "0Bilder, 4Videos", "")
160721 14:06:58      2 Query INSERT INTO kunden VALUES("Pinocchio", "Holzmarkt 2, Freiburg", "2Bilder, 0Videos", "")
160721 14:07:04      2 Query SELECT * from kunden
160721 14:07:21      2 Quit
```

Abbildung 2.13.: MySQL-Log 001 - Anlage Kundendaten

Anschließend erfolgen zwei Lesezugriffe von VM2 am 23.07. um 14:15 Uhr (siehe Abbildung 2.14) und VM1 am 16.08. um 13:54 (siehe Abbildung 2.15). Bei beiden Zugriffen wird über das Statement `Query select * from kunden` der vollständige Inhalt der Kundentabelle aufgerufen.

```
160723 14:15:39      12 Connect          root@vm2.fritz.box on
160723 14:15:43      12 Query select @@version_comment limit 1
160723 14:15:43      12 Query SELECT DATABASE()
160723 14:15:43      12 Init DB           kunden
160723 14:15:43      12 Query show databases
160723 14:15:43      12 Query show tables
160723 14:15:43      12 Field List        kunden
160723 14:15:50      12 Query select * from kunden
```

Abbildung 2.14.: MySQL-Log 002 - Lesezugriff von root@vm2.fritz.box

```
160816 13:54:15      2 Connect          root@vm1.fritz.box on
160816 13:54:16      2 Query select @@version_comment limit 1
160816 13:54:19      2 Query SELECT DATABASE()
160816 13:54:19      2 Init DB           kunden
160816 13:54:19      2 Query show databases
160816 13:54:19      2 Query show tables
160816 13:54:19      2 Field List        kunden
160816 13:54:25      2 Query select * from kunden
160816 13:54:39      2 Quit
```

Abbildung 2.15.: MySQL-Log 003 - Lesezugriff von root@vm1.fritz.box

2.10. USB-Sticks

Als erstes wurden die auf den virtuellen Maschinen gemounteten USB-Sticks ausgewertet. Die Timeline in Abbildung 2.17 basiert auf den Seriennummern der USB-Sticks, dem Label des USB-Sticks und den zugehörigen Logeinträgen in den Syslog-Protokollierungen der virtuellen Maschinen. Die Auswertung der Syslog-Daten erfolgte mit dem Skript A.3, der vollständige Output ist in als CSV-Datei unter `results/syslog/output.csv` hinterlegt.

Für Abbildungen 2.17 und 2.16 gelten folgende Legendendefinitionen:

- Jede Seriennummer ist mit einer eindeutigen Hintergrundfarbe gekennzeichnet
- Die Beschriftung gibt den Mountpoint bzw. das verwendete Label an
- Die Textfarbe gibt die virtuelle Maschine an
 - weiß entspricht VM1
 - schwarz entspricht VM2
 - gelb entspricht VM3

In Abbildung 2.17 ist zu sehen, dass insgesamt 10 USB-Sticks am 18.07.2016 auf den drei virtuellen Maschinen gemountet wurden. Dabei ist auffällig, dass jeder USB-Stick auf mehreren virtuellen Maschinen gemountet und das Label bei den meisten USB-Sticks geändert wurde.

Eine gefilterte Sicht auf die drei USB-Sticks, die auch am 29.07.2016 gemountet wurden (siehe Abbildung 2.16) zeigt eindeutig, dass diese Mounts dieser drei USB-Sticks nur auf VM1 durchgeführt wurden.

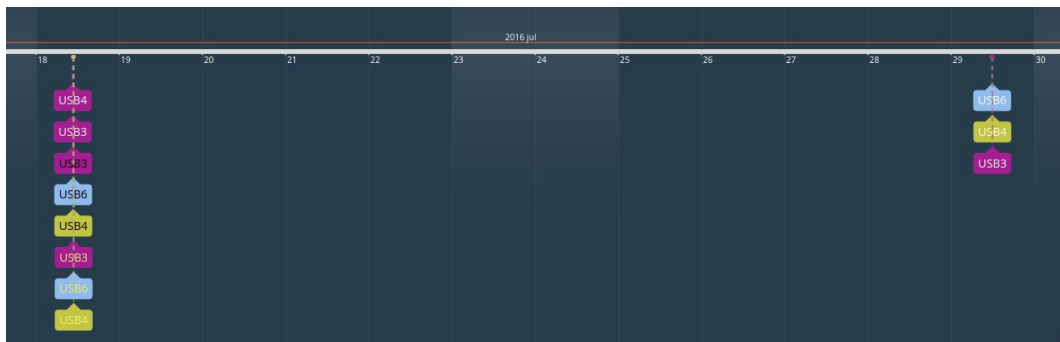


Abbildung 2.16.: Mounts USB 3, 4 und 6 Timeline

Diese drei Mounts der USB-Sticks erlauben die eindeutige Zuordnung zu den sicher-gestellten Images zum Sicherungszeitpunkt, wie es in Tabelle 2.7 dargestellt ist:

| Label | Image | Serial |
|-------|-----------|------------------|
| USB3 | stick1.dd | 07A30A003C48F199 |
| USB4 | stick2.dd | 07A30A003C48F29A |
| USB6 | stick3.dd | 07A30A00655B2CB1 |
| USB6 | stick4.dd | 07A30A00655B2CCF |

Tabelle 2.7.: USB Zuordnungen

WHO ARE YOU?

Forensisches Fallbeispiel

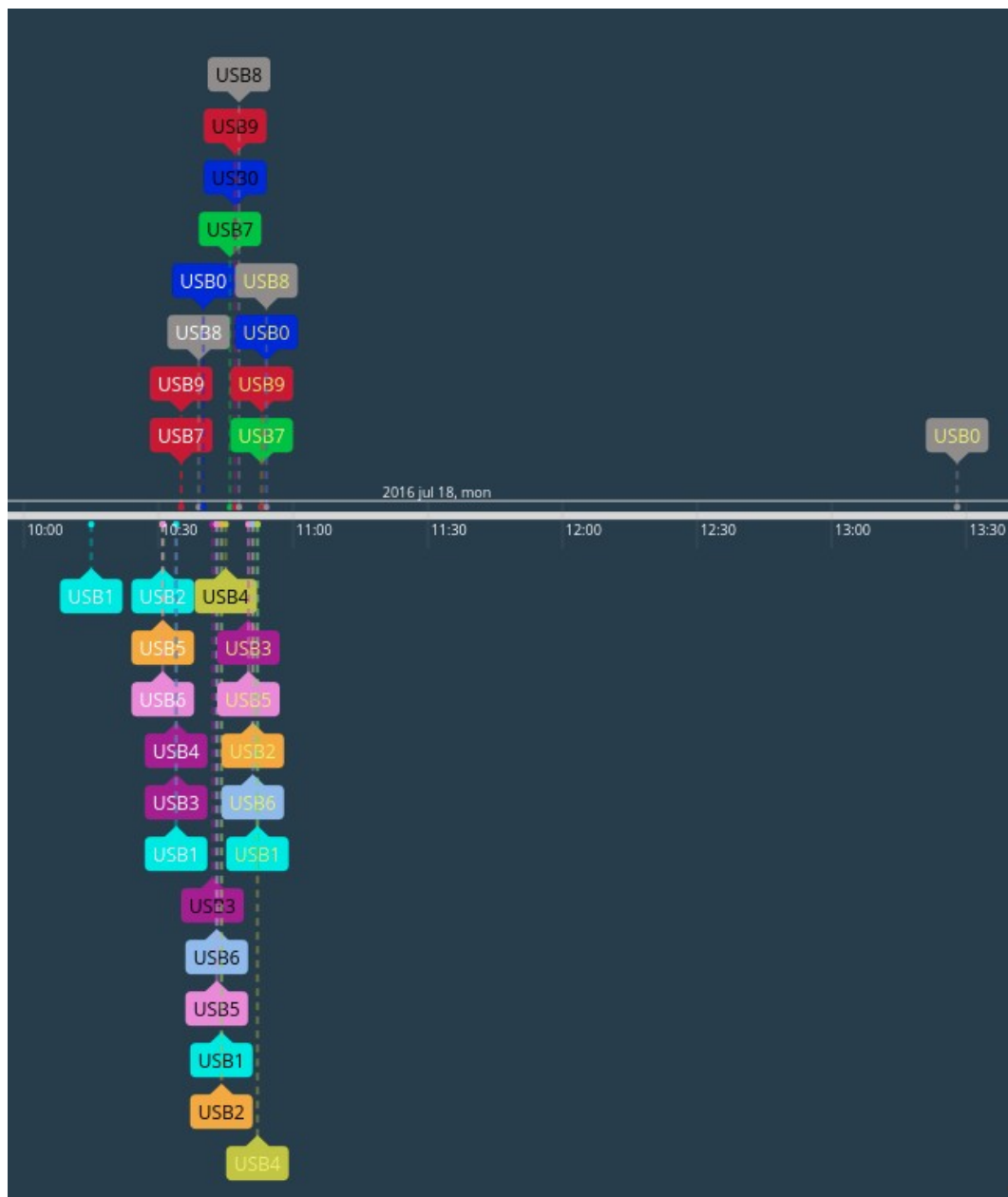


Abbildung 2.17.: Mounts USB Timeline 18.07.

Stick4

Auf dem USB-Stick wurden zwei verschlüsselte und passwortgeschützte ZIP-Archive sowie zwei PNG-Dateien mit einem Hinweis auf versteckte Passwörter (siehe Abbildung 2.18). Weiterhin wurde ein Python-Skript `showMessage.py` auf dem Stick gefunden (siehe Listing A.2).

| Name | S | C | MD5 Hash | Location |
|---|---|---|----------------------------------|---|
| [current folder] | | | | /img_Stick4.dd/Daten/. |
| [parent folder] | | | | /img_Stick4.dd/Daten/.. |
| Anderes | | | | /img_Stick4.dd/Daten/Anderes |
| Bilder.zip | | ! | ff719c1060f77d803a8f9e4639671384 | /img_Stick4.dd/Daten/Bilder.zip |
| Kundendaten_Sicherung.zip | | ! | 5e8eef60d618880e89322c16a9294cc3 | /img_Stick4.dd/Daten/Kundendaten_Sicherung.zip |
| passwort_zu_Bilder.zip.png | | ! | b2dc47a7199e789ec9e7af6d0b378ee8 | /img_Stick4.dd/Daten/passwort_zu_Bilder.zip.png |
| passwort_zu_Kundendaten_Sicherung.zip.png | | ! | 342820c5a7f2318e30c29ed476e2a9d7 | /img_Stick4.dd/Daten/passwort_zu_Kundendaten_Sicheru... |

Abbildung 2.18.: Stick 4 - verschlüsselte ZIP-Dateien

Mit Hilfe des Skripts konnten die Passwörter der beiden ZIP-Dateien ermittelt werden (siehe Abbildung 2.19). Die Passwörter konnten anschließend in Autopsy zur Entschlüsselung genutzt werden. Eine Anwendung des Skripts auf andere gefundene Mediendateien wurde ebenfalls getestet, es konnten allerdings keine weiteren Passwörter auf diesem Weg ermittelt werden.

```
mkoll@mkoll:~/Studium/M116/PA/Exports/temp$ python3 showMessage.py --mode show --input=passwort_zu_Bilder.zip.png
Nachricht:
Passwort der Datei Bilder.zip ist geheim321
mkoll@mkoll:~/Studium/M116/PA/Exports/temp$ python3 showMessage.py --mode show --input=passwort_zu_Kundendaten_Sicherung.zip.png
Nachricht:
Passwort der Datei Kundendaten_Sicherung.zip ist geheim123
mkoll@mkoll:~/Studium/M116/PA/Exports/temp$
```

Abbildung 2.19.: Entschlüsselung ZIP-Dateien Stick 4

Wie in Abschnitt 2.12 erläutert liegen alle Zeitstempel auf diesem USB-Stick in der Zeitlinie deutlich hinter dem relevanten Zeitraum. Ebenfalls ist auf dem Stick kein `Testfile` zu finden, was daraufhin deutet, dass dieser Stick nicht am 18.07.19, wie in den Zeitgeistanalysen erläutert, gemountet und vorbereitet wurde.

2.11. Konten und Anmeldungen

SSH-Logins

Auf VM2 wird ein OpenSSH-Server betrieben, der einen Remote-Zugriff ermöglicht. Die Logdateien `/var/log/auth.log` zeigen zwei Zugriffe von den anderen Maschinen

(siehe Abbildungen 2.21 und 2.20). Von VM3 wird am 10.08. um 12:49 Uhr zugegriffen, von VM1 am 10.08. um 12:43 Uhr (dies deckt sich mit der Zeitgeistauswertung in Tabelle 2.3).

```
Aug 10 12:49:54 vm2 sshd[2153]: Accepted password for user from 192.168.178.23 port 35916 ssh2
Aug 10 12:49:54 vm2 sshd[2153]: pam_unix(sshd:session): session opened for user user by (uid=0)
Aug 10 12:49:54 vm2 systemd-logind[543]: New session 2 of user user.
Aug 10 12:50:14 vm2 sshd[2190]: Received disconnect from 192.168.178.23: 11: disconnected by user
Aug 10 12:50:14 vm2 sshd[2190]: Disconnected from 192.168.178.23
Aug 10 12:50:14 vm2 sshd[2153]: pam_unix(sshd:session): session closed for user user
Aug 10 12:50:14 vm2 systemd-logind[543]: Removed session 2.
```

Abbildung 2.20.: VM2 SSH - Zugriff von VM3

```
Aug 10 12:43:42 vm2 sshd[1858]: Accepted password for user from 192.168.178.31 port 43056 ssh2
Aug 10 12:43:42 vm2 sshd[1858]: pam_unix(sshd:session): session opened for user user by (uid=0)
Aug 10 12:43:42 vm2 systemd-logind[543]: New session 1 of user user.
Aug 10 12:44:21 vm2 systemd-logind[543]: Removed session cl.
Aug 10 12:44:35 vm2 sshd[1936]: Received disconnect from 192.168.178.31: 11: disconnected by user
Aug 10 12:44:35 vm2 sshd[1936]: Disconnected from 192.168.178.31
Aug 10 12:44:35 vm2 sshd[1858]: pam_unix(sshd:session): session closed for user user
Aug 10 12:44:35 vm2 systemd-logind[543]: Removed session 1.
```

Abbildung 2.21.: VM2 SSH - Zugriff von VM1

2.12. Bild- und Videodateien

Alle als illegal eingestuft gefundenen Bilder und deren Vorkommnisse sind in A.1 aufgeführt und als Datei in **results/media** abgelegt. In Tabelle 2.8 sind alle gefundenen Bilder (identifiziert an der MD5-Hashsumme) nach deren Vorkommen auf den USB-Sticks und virtuellen Maschinen aufgeführt. Alle relevanten Dateien wurden auf allen drei virtuellen Maschinen gefunden. Bei den USB-Sticks 1-3 gibt es keine Überschneidungen. USB-Stick 4 enthält dieselben Dateien wie USB-Stick 3, wie in Abschnitt 2.10 gezeigt jedoch in verschlüsselter Form. Das Archiv **neue_ware.tar.gz** ist nur auf den virtuellen Maschinen zu finden und dient offensichtlich der internen Verteilung der Mediendateien.

Die in Tabelle 2.8 verwendeten Bezeichnungen bedeuten:

- **U1-4** - USB-Stick 1-4
- **V1-3** - VM 1-3

| Name | MD5 | U1 | U2 | U3 | U4 | V1 | V2 | V3 |
|---------------|----------------------------------|----|----|----|----|----|----|----|
| IMAGE_121.JPG | 3f5f0a4b9c8d774f0242c84d1fda2577 | X | | | | X | X | X |
| IMAGE_122.JPG | e2485f5650a48af631cf79c937a741ca | X | | | | X | X | X |
| IMAGE_123.JPG | ecdfe5ee600db53b4fd6f63bba296dfb | X | | | | X | X | X |

| | | | | | | |
|------------------|-----------------------------------|---|---|---|---|---|
| IMAGE_124.JPG | 2ec96ec2ddbe8699fa1e24324efbdbb00 | X | | X | X | X |
| IMAGE_125.JPG | 44849ef3351b81145366ff3908a1987e | X | | X | X | X |
| IMAGE_126.JPG | 028905b8afffeacfb7aca2b5975fc21d | X | | X | X | X |
| IMAGE_127.JPG | fc08ecc7da1287bc7e824c61ec3cd3fa | X | | X | X | X |
| IMAGE_128.JPG | 969f0f1eb4d10659f2bb35cb579e67d3 | X | | X | X | X |
| IMAGE_129.JPG | 8977a3717bcdbc68dc9d4adb24c66b3f8 | | X | X | X | X |
| IMAGE_130.JPG | 43f7b0bff9aa8433f722912785538ea2 | | X | X | X | X |
| IMAGE_131.JPG | ecc04f2b32e56a7fc28c2677f26fd6c6 | | X | X | X | X |
| IMAGE_132.JPG | 5383de1960832d5c3d356b9cc41e48b8 | | X | X | X | X |
| IMAGE_133.JPG | ac311d5b2027be1e45228a7473960682 | | X | X | X | X |
| IMAGE_134.JPG | dc55c4560205eb9e0bd773cd69f05774 | X | | X | X | X |
| IMAGE_135.JPG | 44f0786ba69c50db7a8f978889f7c6cf | X | | X | X | X |
| MOVIE_1.mpg | 6396875c8619361cd4271f7cd7dfec3c | X | | X | X | X |
| MOVIE_2.mpg | 4b579dda2fad59d4ee983361feb70261 | X | | X | X | X |
| MOVIE_3.mpg | 8af5a5e8a2190a7be1a0b072544bcd9f | X | | X | X | X |
| MOVIE_4.mpg | 4ba983ab9b083549c123c603c8d93f39 | X | | X | X | X |
| neue_ware.tar.gz | 4bec7618bdaebbb449485254ad0ab5c0 | | | X | X | X |

Tabelle 2.8.: Mediendateien Verteilung

2.12.1. Timeline USB-Sticks

Um die Dateitransfers nachzuvollziehen können die Events in vier verschiedene Abschnitte zerlegt werden und anhand der Zeitstempel gruppiert. Die Filterungen wurden mit Hilfe von Autopsy und einem geeigneten Tagging durchgeführt und anschließend in eine Timeline gebracht.

Der erste Abschnitt sind die Zeitstempel der auffälligen Dateien auf den USB-Sticks. Wie in Tabelle A.2 zu sehen ist, können vier Cluster gebildet werden:

| Zeitstempel | Beschreibung |
|---------------------------|---|
| 18.07.16 12:07 (Modified) | Alle Mediendaten auf den USB-Sticks 1-4 wurden zu diesem Zeitpunkt das letzte Mal geändert (inhaltlich) |
| 24.07.16 11:29 (Created) | Die Dateien wurden auf den USB-Sticks 1-3 erstellt |
| 29.07.16 (Accessed) | Letzter Zugriff auf die Dateien auf den USB-Sticks 1-3 |

| | |
|--------------------|---|
| 18.09.17 (Created) | Auf USB-Stick 4 wurde die Datei Bilder.zip angelegt und 5 Mediendateien archiviert |
|--------------------|---|

Tabelle 2.9.: Cluster Mediendateien USB-Sticks

Die Interpretation der Daten bis zu diesem Zeitpunkt weist daraufhin, dass die USB-Sticks 1-3 am 18.07. auf den unterschiedlichen virtuellen Maschinen vorbereitet wurden (siehe Zeitgeistanalysen). Anschließend wurden am 24.07. die Mediendateien auf die Sticks kopiert.

USB-Stick 4 enthielt nach den auswertbaren Spuren keine Mediendateien vor dem 18.09.2017, was daraufhin deutet, dass dieser Stick erst zu einem späteren Zeitpunkt zum Einsatz kam.

2.12.2. Timeline Virtuelle Maschinen

Die weiteren drei Abschnitte beziehen sich auf die Dateiübertragungen und -events der relevanten Mediendateien auf den drei virtuellen Maschinen. In den Abbildungen 2.22 bis 2.24 sind die relevanten Zeitstempel der Dateien dargestellt. Die Rohdaten liegen in `results/media/timelinevm[1-3].csv` vor.

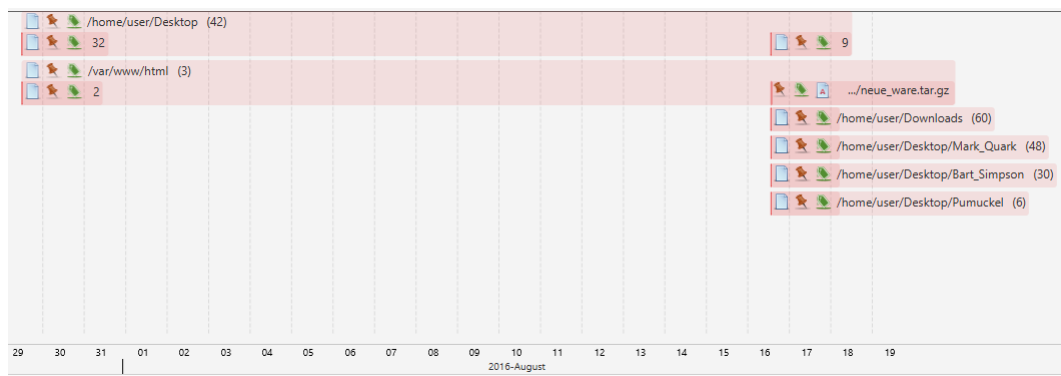


Abbildung 2.22.: Mediendateien VM1 Timeline

WHO ARE YOU?

Forensisches Fallbeispiel

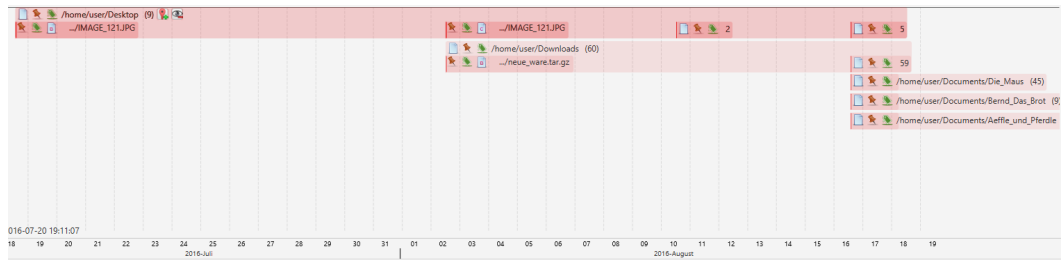


Abbildung 2.23.: Mediendateien VM2 Timeline

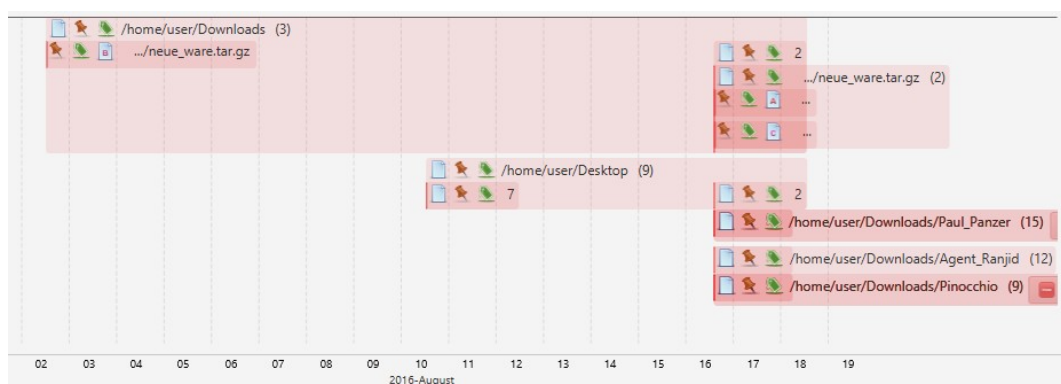


Abbildung 2.24.: Mediendateien VM3 Timeline

3. Zusammenfassung

Die in Kapitel 2 gesicherten Spuren werden in den folgenden Abschnitten zusammengeführt und zur Beantwortung Fragen zur Ermittlung ausgewertet. Im Abschnitt 3.6 werden einige offene Fragen und Anmerkungen aufgeführt.

3.1. Beteiligte und Rollen

Tabelle 3.1 stellt die Zuordnungen der Beteiligten zu den E-Mail-Konten, den virtuellen Maschinen und deren Rolle in dem Prozess dar.

Die Rolleninterpretation beruht hauptsächlich auf der Verteilung der durchgeführten Aktionen wie sie vor allem in der Timeline in Abschnitt 3.2 deutlich werden.

- *Herr Mutig* nimmt die Rolle als Chef und Koordinator wahr und verteilt Anweisungen zur Erstellung der Kundendatenbank und zur Beschaffung von Ware. Er ist weiterhin für die Koordination der Warenlieferung zuständig.
- *Herr Nerd* beschafft die benötigte Ware und verteilt diese an die anderen Beteiligten.
- *Herr Pepper* ist zuständig für den Vertrieb, indem er neue Kunden akquiriert und die Kundendatenbank pflegt.
- Alle drei Beteiligten sind bei der Auslieferung beteiligt, indem sie die geforderten Kundenpakete erstellen.

Hinweis:

Die Zuordnung der natürlichen Personen zu den virtuellen Maschinen und Konten kann nur über die GMX-Email-Accounts erfolgen (siehe Abschnitt 2.5). Ob diese Accounts tatsächlich von den beschuldigten Personen angelegt und genutzt werden kann durch das Gutachten nicht geklärt werden.

| Name | Kurzname | VM Rolle |
|------|----------|----------|
|------|----------|----------|

| | | | |
|---------------|---------|-----|--------------------------------------|
| Niko Nerd | nitro94 | vm1 | Beschaffung, Verteilung, Mitarbeiter |
| Mathias Mutig | muti97 | vm2 | Verteilung, Chef |
| Peter Pepper | pepp87 | vm3 | Vertrieb, Verteilung, Mitarbeiter |

Tabelle 3.1.: Zusammenfassung: Beteiligte, Rollen und Zuordnungen

3.2. Timeline

Alle relevanten gefundenen Events wurden interpretiert und in eine Timeline (Abbildung 3.1) zusammengefasst. Die graphische Darstellung ermöglicht die Erkennung der verschiedenen Phasen und Verantwortlichkeiten, die in der folgenden Auflistung näher erläutert werden:

Kundenakquise Verantwortlich: Herr Pepper - Herr Pepper verteilt die Information über neue Kunden und versendet ein Beispielfeld an Herr Mutig und Herr Nerd.

Vorbereitung Verantwortlich: Herr Mutig - Herr Mutig weist Herr Pepper an eine Kundendatenbank anzulegen und Herr Nerd neue Ware zu beschaffen. Beide erfüllen ihre Aufgaben.

Ware intern verteilen Verantwortlich: Herr Nerd - Die Ware wird unter den Beteiligten über einen Webserver verteilt.

Planung Auslieferung Verantwortlich: Herr Mutig - Herr Mutig erstellt einen Vertriebsplan und legt für jeden Kunden einen Verantwortlichen fest.

Auslieferung Verantwortlich: Alle - Alle erstellen die jeweiligen Kundenpakete.

In der Timeline sind alle Events bezogen auf E-Mail unterhalb der Zeitachse angebracht, oberhalb der Zeitachse sind alle Ereignisse die Dateiübertragungen, Kundendatenbanken oder ähnliches beinhalten.

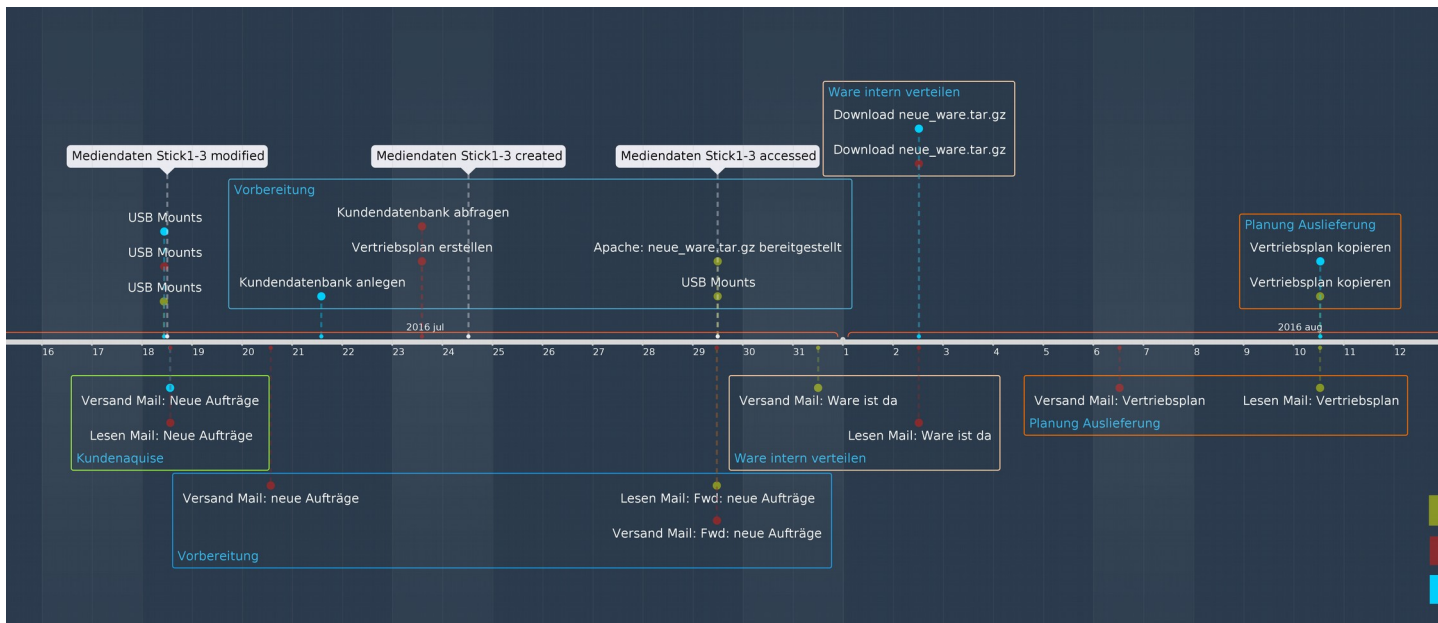


Abbildung 3.1.: Zusammenfassung: Timeline

3.3. Illegaler Bild- und Videobesitz

Während der Analyse konnten eine Vielzahl an Bild- und Videodateien sichergestellt werden, die als illegal einzustufen sind.

Die vollständige Auflistung der gefundenen eindeutigen Dateien (siehe Tabelle 2.8) und aller Vorkommnisse A.1 basierend auf den überlassenen Asservaten ist hinreichend als Beweis für den Besitz der Bilder zu deuten.

Die Quelle der Mediendateien konnte nicht festgestellt werden. Die Mediendateien wurden über die Sticks 1-3 geliefert, woher diese Sticks stammen kann nur anhand der vorhandenen Daten auf diesen Sticks vermutet werden. Ob die vorhandenen Hinweise auf natürliche Personen, die auf den Sticks in den älteren Dateien gefunden wurden, ausreichend sind kann bezweifelt werden. Die Quelle ist demnach als unbekannt anzusehen.

Der technische Weg der Auslieferung konnte ebenfalls nicht vollständig nachvollzogen werden. Die Erstellung der Kundenpakete durch die Beteiligten zugeordnet zu dem Vertriebsplan ist eindeutig. Wie die Mediendateien an die Kunden ausgeliefert werden konnte nicht nachgewiesen werden.

Nachgewiesen werden konnte dementsprechend nur die Planung des Vertriebs der Besitz der Mediendateien und die Verteilung innerhalb der drei Beteiligten.

3.4. Herkunft USB-Sticks

Alle vier USB-Sticks wurden auf den virtuellen Maschinen am 18.07.2016 zum ersten Mal eingebunden. Auf den Sticks 1-3 wurden Spuren von anderen Personen bzw. Accounts und E-Mail-Adressen gefunden. Ob diese Personen an der Tat beteiligt konnte in dieser Auswertung nicht ermittelt werden.

3.5. Kundendaten

Während der Untersuchung konnten zwei Versionen des Vertriebsplans sichergestellt werden. In diesen änderten sich die Anschriften einiger Kunden. Welche Anschriften korrekt sind muss weiter ermittelt werden. Die Zuordnung der Anzahl der Bilder zu den erstellten Kundenpakete der Beteiligten konnte verifiziert werden und stimmt überein.

WHO ARE YOU?

Forensisches Fallbeispiel

| Customer Name | Address | Video Files |
|--------------------|------------------------------------|-----------------------------------|
| Mark Quark | Magdeburgerstr. 1, Magdeburg | 10x Bild1, 5x Bild2, 1x Video VM1 |
| Bart Simpson | 742 Evergreen Terrace, Springfield | 5x Bild1, 2x Bild2, 3x Video VM1 |
| Pumuckl | Widenmayerstraße 1, München | 1x Bild1, 1x Bild2, 0x Video VM1 |
| Die Maus | Appellhofplatz 1 Köln | 5x Bild1, 10x Bild2, 0x Video VM2 |
| Bernd Das Brot | Fischmarkt in Erfurt, Erfurt | 1x Bild1, 1x Bild2, 1x Video VM2 |
| Aeffle und Pferdle | Thomastr. 43 Stuttgart | 5x Bild1, 5x Bild2, 0x Video VM2 |
| Paul Panzer | Bachemer Straße 88 Köln | 0x Bild1, 2x Bild2, 3x Video VM3 |
| Agent Ranjid | Alabadstr. 1, Bremen | 0x Bild1, 0x Bild2, 5x Video VM3 |
| Pinocchio | Holzmarkt 2, Freiburg | 2x Bild1, 0x Bild2, 0x Video VM3 |

Abbildung 3.2.: Kundendaten Stand 18.09.2017

| name | addr | daten | verantw |
|--------------------|------------------------------------|------------------|---------|
| Mark Quark | Magdeburgerstr. 1, Magdeburg | 15Bilder, 1Video | Nitro |
| Bart Simpson | 742 Evergreen Terrace, Springfield | 7Bilder, 3Video | Nitro |
| Pumuckl | Widenmayerstrasse 1, Muenchen | 2Bilder, 0Video | Nitro |
| Die Maus | Appelhofplatz 1, Koeln | 15Bilder, 0Video | Muti |
| Bernd Das Brot | Fischmarkt in Erfurt, Erfurt | 2Bilder, 1Video | Muti |
| Aeffle und Pferdle | Thomastr. 43, Stuttgart | 10Bilder, 4Video | Muti |
| Paul Panzer | Bachemerstr. 88, Koeln | 2Bilder, 3Videos | Pepp |
| Agent Ranjid | Alabadstr. 1, Bremen | 0Bilder, 4Videos | Pepp |
| Pinocchio | Holzmarkt 2, Freiburg | 2Bilder, 0Videos | Pepp |

Abbildung 3.3.: Kundendaten Stand 16.08.2016

3.6. Offene Fragen und Anmerkungen

- Auf VM1 wurden zwei SMTP-Server eingetragen, neben dem zu erwartenden nitro94@gmx.de auch muti97@gmx.de. Es konnte allerdings kein Versand über die Absenderadresse muti97@gmx.de auf VM1 festgestellt werden. Warum ist der zweite SMTP-Server hinterlegt? Wurde dieser benutzt?
- Es wird angenommen, dass der E-Mail-Empfänger miko94@gmx.de keine weitere beteiligte Person ist, sondern lediglich durch einen Tippfehler von Herrn Mutig in die E-Mail-Kommunikation einbezogen wurde.

Verzeichnis der Listings

| | |
|-------------------------------------|----|
| A.1. Volatility Plugins | 39 |
| A.2. showMessage.py | 41 |
| A.3. readUSBMounts.py | 43 |
| A.4. zeitgeistanalyse.sql | 56 |

Abbildungsverzeichnis

| | |
|---|----|
| 1.1. Datenquellen Autopsy | 5 |
| 2.1. LUKS-Partition entschlüsseln und kopieren | 7 |
| 2.2. Veracrypt Eigenschaften Container VM1 | 8 |
| 2.3. Veracrypt Eigenschaften Container VM2 | 8 |
| 2.4. Timeline der E-Mail-Kommunikation | 14 |
| 2.5. Email 001 - Neue Aufträge | 15 |
| 2.6. Email 002 - neue Aufträge | 15 |
| 2.7. Email 003 - Fwd: neue Aufträge | 16 |
| 2.8. Email 004 - Ware ist da | 16 |
| 2.9. Email 005 - Vertriebsplan | 17 |
| 2.10. Browserverlauf VM2. | 18 |
| 2.11. Browserverlauf VM3. | 18 |
| 2.12. Apache Zugriffsprotokoll VM1 | 19 |
| 2.13. MySQL-Log 001 - Anlage Kundendaten. | 19 |
| 2.14. MySQL-Log 002 - Lesezugriff von root@vm2.fritz.box. | 20 |
| 2.15. MySQL-Log 003 - Lesezugriff von root@vm1.fritz.box. | 20 |
| 2.16. Mounts USB 3, 4 und 6 Timeline | 21 |
| 2.17. Mounts USB Timeline 18.07. | 22 |
| 2.18. Stick 4 - verschlüsselte ZIP-Dateien | 23 |
| 2.19. Entschlüsselung ZIP-Dateien Stick 4. | 23 |
| 2.20. VM2 SSH - Zugriff von VM3 | 24 |
| 2.21. VM2 SSH - Zugriff von VM1 | 24 |
| 2.22. Mediendateien VM1 Timeline | 26 |
| 2.23. Mediendateien VM2 Timeline | 27 |
| 2.24. Mediendateien VM3 Timeline | 27 |
| 3.1. Zusammenfassung: Timeline | 30 |
| 3.2. Kundendaten Stand 18.09.2017 | 32 |
| 3.3. Kundendaten Stand 16.08.2016 | 32 |
| A.1. GMX Account nitro94@gmx.de. | 45 |
| A.2. GMX Account muti97@gmx.de | 46 |
| A.3. GMX Account pepp87@gmx.net | 47 |

| | |
|--|----|
| A.4. Inbox muti97@gmx.de | 48 |
| A.5. Sent muti97@gmx.de | 49 |
| A.6. Inbox nitro94@gmx.de | 50 |
| A.7. Sent nitro94@gmx.de | 51 |
| A.8. Inbox pepp87@gmx.net | 52 |
| A.9. Sent pepp87@gmx.net | 53 |
| A.10.Email 001 - Neue Aufträge (Anhang) .. | 54 |
| A.11.Email 002 - neue Aufträge (Anhang). | 54 |
| A.12.Email 003 - Fwd: neue Aufträge (Anhang) .. | 55 |

Tabellenverzeichnis

| | |
|--|----|
| 1.1. Untersuchte Asservate | 3 |
| 1.2. Notizzettel | 4 |
| 1.3. Verwendete Volatility-Profile | 4 |
| 2.1. Zuordnungen Übersicht | 6 |
| 2.2. Zuordnungen Passwörter | 6 |
| 2.3. Zeitgeist-Events VM1 | 10 |
| 2.4. Zeitgeist-Events VM2 | 11 |
| 2.5. Übersicht E-Mail-Konten | 13 |
| 2.6. Übersicht E-Mails | 13 |
| 2.7. USB Zuordnungen | 21 |
| 2.8. Mediendateien Verteilung | 25 |
| 2.9. Cluster Mediendateien USB-Sticks | 26 |
| 3.1. Zusammenfassung: Beteiligte, Rollen und Zuordnungen | 29 |
| A.1. Mediendateien Gesamt | 70 |
| A.2. Mediendateien USB-Sticks Timestamps | 71 |

A. Anhang

A.1. Skripte

Listing A.1: Volatility Plugins

```
1 vol.py -f memdump_vm1.lime --profile=LinuxUbuntu4_2_0-27-genericx64 linux_arp > ←
→ vm1/linux_arp.vol
2 vol.py -f memdump_vm1.lime --profile=LinuxUbuntu4_2_0-27-genericx64 linux_banner > ←
→ vm1/linux_banner.vol
3 vol.py -f memdump_vm1.lime --profile=LinuxUbuntu4_2_0-27-genericx64 linux_bash > ←
→ vm1/linux_bash.vol
4 vol.py -f memdump_vm1.lime --profile=LinuxUbuntu4_2_0-27-genericx64 linux_bash_env ←
→ > vm1/linux_bash_env.vol
5 vol.py -f memdump_vm1.lime --profile=LinuxUbuntu4_2_0-27-genericx64 linux_bash_hash ←
→ > vm1/linux_bash_hash.vol
6 vol.py -f memdump_vm1.lime --profile=LinuxUbuntu4_2_0-27-genericx64 linux_cpuinfo > ←
→ vm1/linux_cpuinfo.vol
7 vol.py -f memdump_vm1.lime --profile=LinuxUbuntu4_2_0-27-genericx64 linux_dmesg > ←
→ vm1/linux_dmesg.vol
8 vol.py -f memdump_vm1.lime --profile=LinuxUbuntu4_2_0-27-genericx64 linux_ifconfig ←
→ > vm1/linux_ifconfig.vol
9 vol.py -f memdump_vm1.lime --profile=LinuxUbuntu4_2_0-27-genericx64 linux_lsmod > ←
→ vm1/linux_lsmod.vol
10 vol.py -f memdump_vm1.lime --profile=LinuxUbuntu4_2_0-27-genericx64 linux_lsof > ←
→ vm1/linux_lsof.vol
11 vol.py -f memdump_vm1.lime --profile=LinuxUbuntu4_2_0-27-genericx64 linux_mount > ←
→ vm1/linux_mount.vol
12 vol.py -f memdump_vm1.lime --profile=LinuxUbuntu4_2_0-27-genericx64 linux_netfilter ←
→ > vm1/linux_netfilter.vol
13 vol.py -f memdump_vm1.lime --profile=LinuxUbuntu4_2_0-27-genericx64 linux_netscan > ←
→ vm1/linux_netscan.vol
14 vol.py -f memdump_vm1.lime --profile=LinuxUbuntu4_2_0-27-genericx64 linux_netstat > ←
→ vm1/linux_netstat.vol
15 vol.py -f memdump_vm1.lime --profile=LinuxUbuntu4_2_0-27-genericx64 linux_pslist > ←
→ vm1/linux_pslist.vol
16 vol.py -f memdump_vm1.lime --profile=LinuxUbuntu4_2_0-27-genericx64 linux_pstree > ←
→ vm1/linux_pstree.vol
17 vol.py -f memdump_vm1.lime --profile=LinuxUbuntu4_2_0-27-genericx64 linux_ssh_keys ←
→ > vm1/linux_ssh_keys.vol
18
19 vol.py -f memdump_vm2.lime --profile=LinuxUbuntu4_2_0-16-genericx64 linux_arp > ←
→ vm2/linux_arp.vol
20 vol.py -f memdump_vm2.lime --profile=LinuxUbuntu4_2_0-16-genericx64 linux_banner > ←
→ vm2/linux_banner.vol
21 vol.py -f memdump_vm2.lime --profile=LinuxUbuntu4_2_0-16-genericx64 linux_bash > ←
→ vm2/linux_bash.vol
22 vol.py -f memdump_vm2.lime --profile=LinuxUbuntu4_2_0-16-genericx64 linux_bash_env ←
→ > vm2/linux_bash_env.vol
23 vol.py -f memdump_vm2.lime --profile=LinuxUbuntu4_2_0-16-genericx64 linux_bash_hash ←
→ > vm2/linux_bash_hash.vol
```

WHO ARE YOU?

Forensisches Fallbeispiel

```
24 vol.py -f memdump_vm2.lime --profile=LinuxUbuntu4_2_0-16-genericx64 linux_cpuinfo > ←
   ↳ vm2/linux_cpuinfo.vol
25 vol.py -f memdump_vm2.lime --profile=LinuxUbuntu4_2_0-16-genericx64 linux_dmesg > ←
   ↳ vm2/linux_dmesg.vol
26 vol.py -f memdump_vm2.lime --profile=LinuxUbuntu4_2_0-16-genericx64 linux_ifconfig ←
   ↳ > vm2/linux_ifconfig.vol
27 vol.py -f memdump_vm2.lime --profile=LinuxUbuntu4_2_0-16-genericx64 linux_lsmod > ←
   ↳ vm2/linux_lsmod.vol
28 vol.py -f memdump_vm2.lime --profile=LinuxUbuntu4_2_0-16-genericx64 linux_lsof > ←
   ↳ vm2/linux_lsof.vol
29 vol.py -f memdump_vm2.lime --profile=LinuxUbuntu4_2_0-16-genericx64 linux_mount > ←
   ↳ vm2/linux_mount.vol
30 vol.py -f memdump_vm2.lime --profile=LinuxUbuntu4_2_0-16-genericx64 linux_netfilter ←
   ↳ > vm2/linux_netfilter.vol
31 vol.py -f memdump_vm2.lime --profile=LinuxUbuntu4_2_0-16-genericx64 linux_netscan > ←
   ↳ vm2/linux_netscan.vol
32 vol.py -f memdump_vm2.lime --profile=LinuxUbuntu4_2_0-16-genericx64 linux_netstat > ←
   ↳ vm2/linux_netstat.vol
33 vol.py -f memdump_vm2.lime --profile=LinuxUbuntu4_2_0-16-genericx64 linux_pslist > ←
   ↳ vm2/linux_pslist.vol
34 vol.py -f memdump_vm2.lime --profile=LinuxUbuntu4_2_0-16-genericx64 linux_pstree > ←
   ↳ vm2/linux_pstree.vol
35 vol.py -f memdump_vm2.lime --profile=LinuxUbuntu4_2_0-16-genericx64 linux_ssh_keys ←
   ↳ > vm2/linux_ssh_keys.vol
36
37 vol.py -f memdump_vm3.lime --profile=LinuxUbuntu3_19_0-15-genericx64 linux_arp > ←
   ↳ vm3/linux_arp.vol
38 vol.py -f memdump_vm3.lime --profile=LinuxUbuntu3_19_0-15-genericx64 linux_banner > ←
   ↳ vm3/linux_banner.vol
39 vol.py -f memdump_vm3.lime --profile=LinuxUbuntu3_19_0-15-genericx64 linux_bash > ←
   ↳ vm3/linux_bash.vol
40 vol.py -f memdump_vm3.lime --profile=LinuxUbuntu3_19_0-15-genericx64 linux_bash_env ←
   ↳ > vm3/linux_bash_env.vol
41 vol.py -f memdump_vm3.lime --profile=LinuxUbuntu3_19_0-15-genericx64 ←
   ↳ linux_bash_hash > vm3/linux_bash_hash.vol
42 vol.py -f memdump_vm3.lime --profile=LinuxUbuntu3_19_0-15-genericx64 linux_cpuinfo ←
   ↳ > vm3/linux_cpuinfo.vol
43 vol.py -f memdump_vm3.lime --profile=LinuxUbuntu3_19_0-15-genericx64 linux_dmesg > ←
   ↳ vm3/linux_dmesg.vol
44 vol.py -f memdump_vm3.lime --profile=LinuxUbuntu3_19_0-15-genericx64 linux_ifconfig ←
   ↳ > vm3/linux_ifconfig.vol
45 vol.py -f memdump_vm3.lime --profile=LinuxUbuntu3_19_0-15-genericx64 linux_lsmod > ←
   ↳ vm3/linux_lsmod.vol
46 vol.py -f memdump_vm3.lime --profile=LinuxUbuntu3_19_0-15-genericx64 linux_lsof > ←
   ↳ vm3/linux_lsof.vol
47 vol.py -f memdump_vm3.lime --profile=LinuxUbuntu3_19_0-15-genericx64 linux_mount > ←
   ↳ vm3/linux_mount.vol
48 vol.py -f memdump_vm3.lime --profile=LinuxUbuntu3_19_0-15-genericx64 ←
   ↳ linux_netfilter > vm3/linux_netfilter.vol
```


WHO ARE YOU?

Forensisches Fallbeispiel

```
49 vol.py -f memdump_vm3.lime --profile=LinuxUbuntu3_19_0-15-genericx64 linux_netscan ←-
→ > vm3/linux_netscan.vol
50 vol.py -f memdump_vm3.lime --profile=LinuxUbuntu3_19_0-15-genericx64 linux_netstat ←-
→ > vm3/linux_netstat.vol
51 vol.py -f memdump_vm3.lime --profile=LinuxUbuntu3_19_0-15-genericx64 linux_pslint > ←-
→ vm3/linux_pslint.vol
52 vol.py -f memdump_vm3.lime --profile=LinuxUbuntu3_19_0-15-genericx64 linux_pstree > ←-
→ vm3/linux_pstree.vol
53 vol.py -f memdump_vm3.lime --profile=LinuxUbuntu3_19_0-15-genericx64 linux_ssh_keys ←-
→ > vm3/linux_ssh_keys.vol
```

Listing A.2: showMessage.py

```
1 import argparse
2 from PIL import Image
3 import numpy
4 from bitstring import BitArray
5
6 def getBitsFromString(s):
7     bytes = numpy.fromstring(s, dtype="uint8")
8     return [b for b in numpy.unpackbits(bytes)]
9
10 def binaryToString(arr):
11     return str(numpy.packbits(arr).tobytes(), 'utf-8')
12
13 def getBitsFromInt(value):
14     bits = [int(x) for x in list('{0:0b}'.format(value))]
15     return [0] * (32 - len(bits)) + bits
16
17 def binaryToInt(arr):
18     return BitArray(arr).uint
19
20 def openImage(name):
21     in_image = Image.open(name)
22     return in_image, in_image.size[0], in_image.size[1]
23
24 def Hide_message(in_imagefile, message, out_imagefile):
25     in_image, width, height = openImage(in_imagefile)
26     out_image = Image.new('RGB', in_image.size)
27     new_array = []
28     print("Nachricht:", message)
29     print("Laenge der Nachricht in Byte:", len(message))
30     n = 0
31     allBits = getBitsFromInt(len(message) * 8) + getBitsFromString(message)
32     for h in range(height):
33         for w in range(width):
34             pixel = in_image.getpixel((w, h))
35             temp = [pixel[0], pixel[1], pixel[2]]
36             for i in range(0, 3):
37                 if n < len(allBits):
```

WHO ARE YOU?

Forensisches Fallbeispiel

```
38         bit = allBits[n]
39         temp[i] = temp[i] & 254 if bit == 0 else temp[i] | 1
40         n += 1
41         new_array.append((temp[0], temp[1], temp[2]))
42     out_image.putdata(new_array)
43     out_image.save(out_imagefile)
44
45 def ExtractMessage(in_imagefile):
46     in_image, width, height = openImage(in_imagefile)
47     new_array = []
48     n = 0
49     lenComplete = False
50     stopAt = 32
51     for h in range(height):
52         for w in range(width):
53             pixel = in_image.getpixel((w, h))
54             for i in range(0, 3):
55                 if n == stopAt:
56                     if lenComplete:
57                         return stopAt // 8, binaryToString(new_array)
58                     else:
59                         messageLen = binaryToInt(new_array)
60                         new_array = []
61                         n = 0
62                         stopAt = messageLen
63                         lenComplete = True
64                 new_array.append(0 if pixel[i] & 1 == 0 else 1)
65                 n += 1
66
67 parser = argparse.ArgumentParser()
68 parser.add_argument('--mode', choices=('show', 'hide'), required=True)
69 parser.add_argument("--input", type=str, help="Eingabebild", required=False)
70 parser.add_argument("--msg", type=str, help="Nachricht", required=False)
71 parser.add_argument("--output", type=str, help="Ausgabebild (Endung =.png)",
72 → required=False)
73 args = parser.parse_args()
74 if args.mode == "show":
75     if args.input is None:
76         print("Beispiel: --mode=show --input=<Pfad.*>")
77     else:
78         length, msg = ExtractMessage(args.input)
79         print("Nachricht:")
80         print(msg)
81 elif args.mode == "hide":
82     if args.input is None\
83         or args.msg is None\
84         or args.output is None:
85         print("Beispiel: --mode=hide --input=<Pfad.*> --input=<Text>
86 → --output=<Pfad.png>")
```

WHO ARE YOU?

Forensisches Fallbeispiel

```
85     else:
86         Hide_message(args.input, args.msg, args.output)
87 else:
88     parser.print_help()
```

Listing A.3: readUSBMounts.py

```
1  import glob
2  import os
3  import re
4
5  path = '/home/mkoll/Studium/M116/Abgabe/results/syslog/'
6
7  files = [f for f in glob.glob(path + "**/syslog*", recursive=True)]
8  output = '/home/mkoll/Studium/M116/Abgabe/results/syslog/output.txt'
9  outputTime = '/home/mkoll/Studium/M116/Abgabe/results/syslog/outputTime.txt'
10
11 with open(output, 'w') as foutput:
12     with open(outputTime, 'w') as foutputTime:
13         header =
14         → ';'.join(["Detected", "VM", "ProductID", "VendorID", "Manufacturer", "Serial", "Mounted", "Name"])
15         → + os.linesep
16         foutput.write(header)
17         for file in files:
18             lineNew = ''
19             lineManu = ''
20             lineSerial = ''
21             with open(file) as origin_file:
22
23                 for line in origin_file:
24                     if 'New USB device found' in line:
25                         lineNew = line
26                         lineNewList = lineNew.split(' ')
27                     if 'Manufacturer: ' in line:
28                         lineManu = line
29                         lineManuList = lineManu.split(' ')
30                     if 'SerialNumber: ' in line:
31                         lineSerial = line
32                         lineSerialList = lineSerial.split(' ')
33                     if 'at /media/user/USB' in line:
34                         lineList = line.split(' ')
35                         result = ';'.join([lineNewList[0] + ' ' + lineNewList[1] +
36                         → ' ' +
37                         → lineNewList[2], lineNewList[3], lineNewList[-2].rsplit('=', 1)[-1].rstrip(','), lineNewList[-1].rsplit('=', 1)[-1]]
38                         manu = re.findall(r'Manufacturer: (.*)', lineManu)
39                         serial = re.findall(r'SerialNumber: (.*)', lineSerial)
40                         result = ';'.join([result.rstrip(), manu[0], serial[0]])
41                         result = ';'.join([result.rstrip(), lineList[0] + ' ' +
42                         → lineList[1] + ' ' + lineList[2], lineList[8].rsplit('/', 1)[-1]])
43                         result = result + os.linesep
```

WHO ARE YOU?

Forensisches Fallbeispiel

```
39         detTime = lineNewList[2].split(':')
40         timeline = ';'.join(["2016 7 " + lineNewList[1] + ' ' + ←-
→ detTime[0] + ' ' + detTime[1], '', lineList[8].rsplit('/', ←-
→ 1)[-1], re.findall(r'SerialNumber: (.*)', lineSerial)[0] + ',' + lineNewList[3]])
41         print(result)
42         foutput.write(result)
43         foutputTime.write(timeline + os.linesep)
```

A.2. Konten

Persönliche Daten

Zur Person

Kundennummer: **278927850**

Anrede: **Herr**

Firma/Verein:

Vorname: **Niko**

Nachname: **Nerd**

Geburtstag: ****.**.******

[Daten ändern](#)

Adresse

Straße & Hausnr.: **Münchnerstraße 1**

PLZ: **03947**

Ort: **München**

Land: **Deutschland**

[Daten ändern](#)

Abbildung A.1.: GMX Account nitro94@gmx.de

Persönliche Daten

Zur Person

Kundennummer: **278927594**

Anrede: **Herr**

Firma/Verein:

Vorname: **Markus**

Nachname: **Mutig**

Geburtstag: **** ** ******

[Daten ändern](#)

Adresse

Straße & Hausnr.: **Berlinerstraße 1**

PLZ: **72431**

Ort: **Berlin**

Land: **Deutschland**

[Daten ändern](#)

Abbildung A.2.: GMX Account muti97@gmx.de

Persönliche Daten

Zur Person

Kundennummer: **278928295**

Anrede: **Herr**

Firma/Verein:

Vorname: **Peter**

Nachname: **Pepper**

Geburtstag: ****.**.******

[Daten ändern](#)

Adresse

Straße & Hausnr.: **Bremerstraße 1**

PLZ: **92814**

Ort: **Bremen**

Land: **Deutschland**

[Daten ändern](#)

Abbildung A.3.: GMX Account pepp87@gmx.net

WHO ARE YOU?

Forensisches Fallbeispiel

A.3. E-Mails

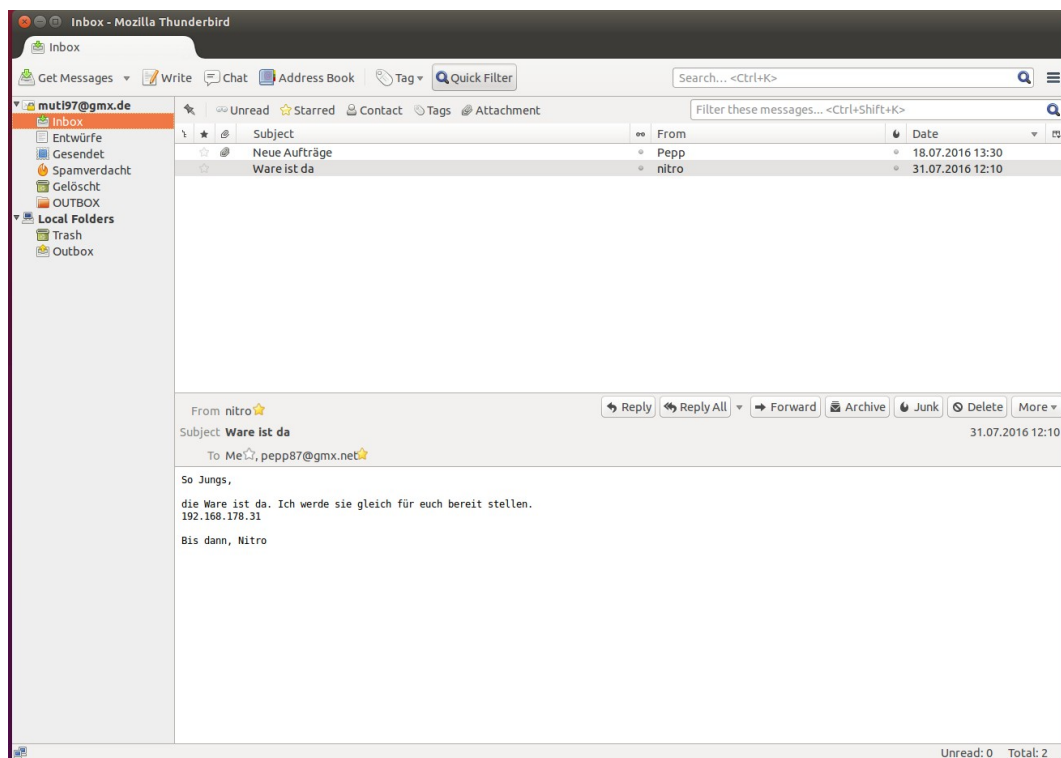


Abbildung A.4.: Inbox muti97@gmx.de

WHO ARE YOU?

Forensisches Fallbeispiel

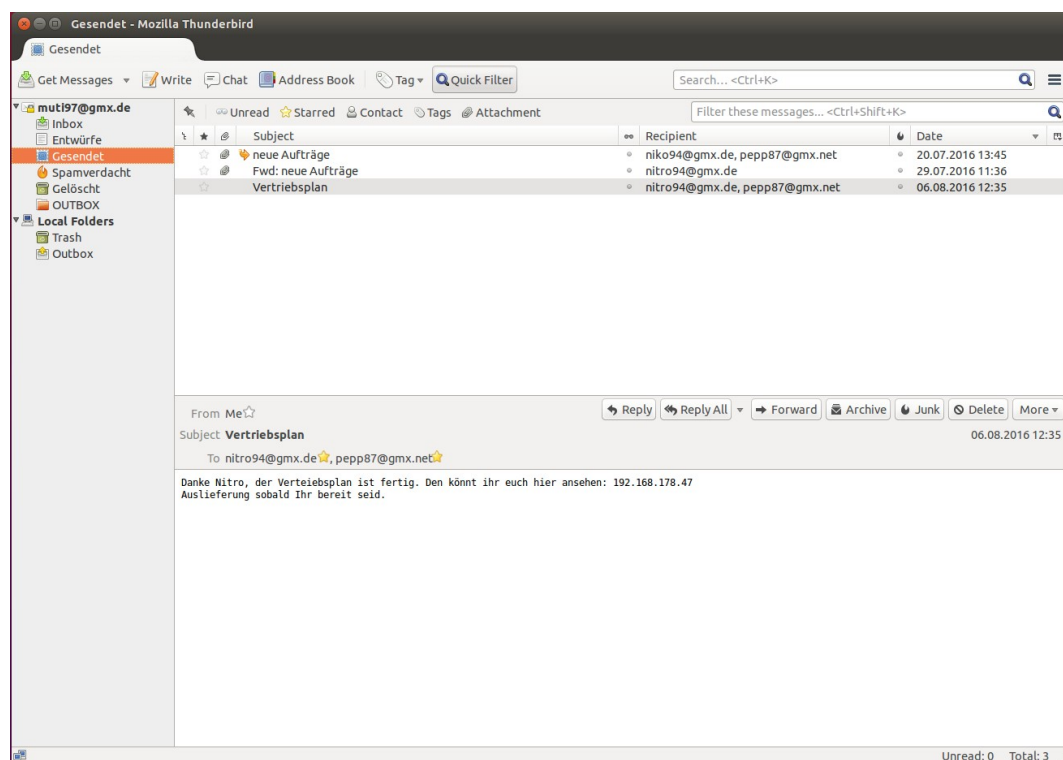


Abbildung A.5.: Sent muti97@gmx.de

WHO ARE YOU?

Forensisches Fallbeispiel

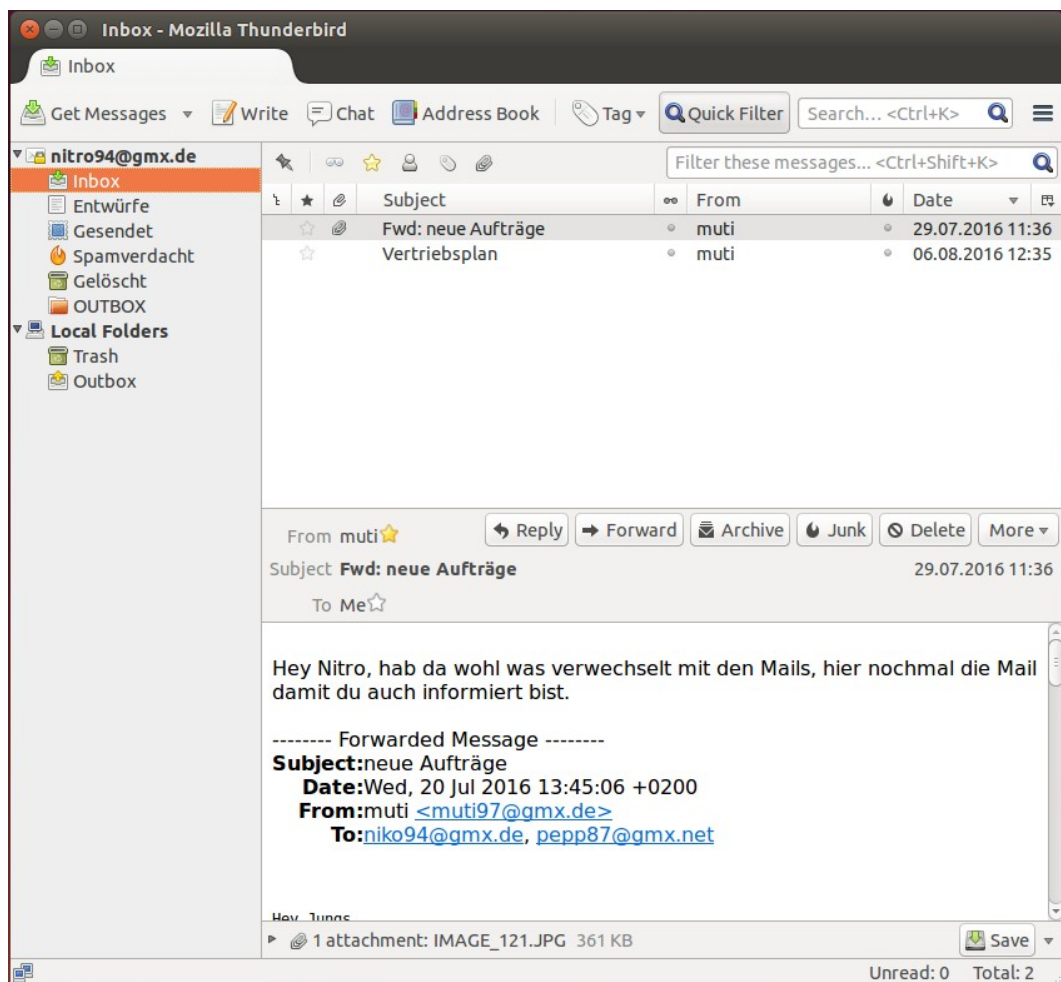


Abbildung A.6.: Inbox nitro94@gmx.de

WHO ARE YOU?

Forensisches Fallbeispiel

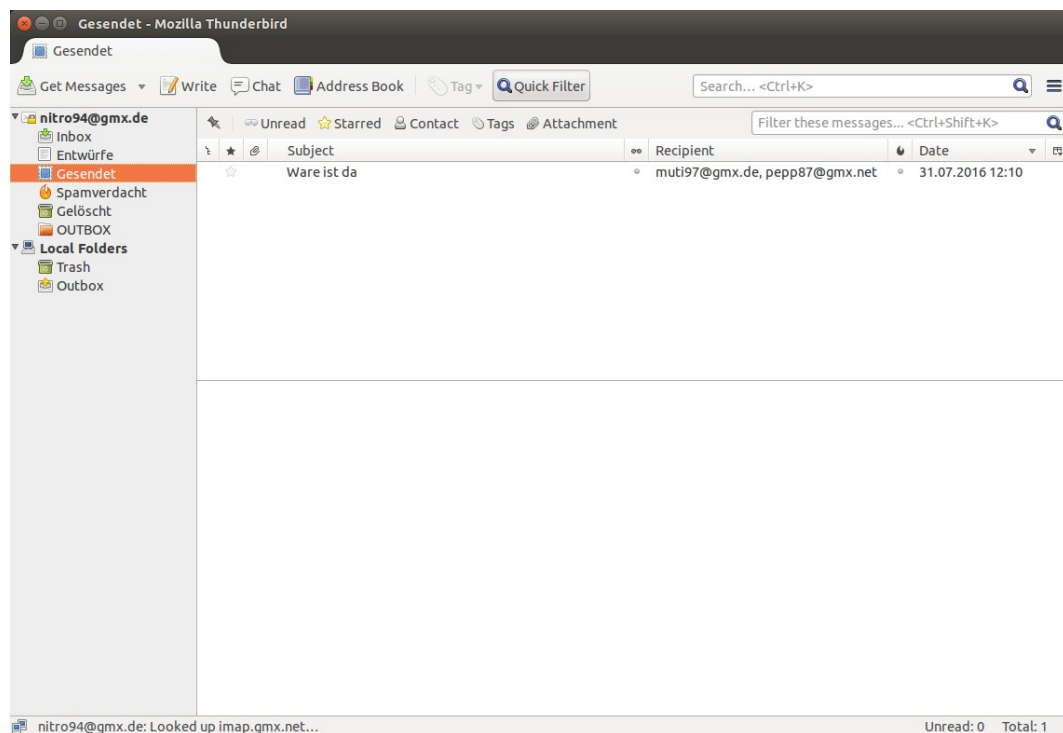


Abbildung A.7.: Sent nitro94@gmx.de

WHO ARE YOU?

Forensisches Fallbeispiel

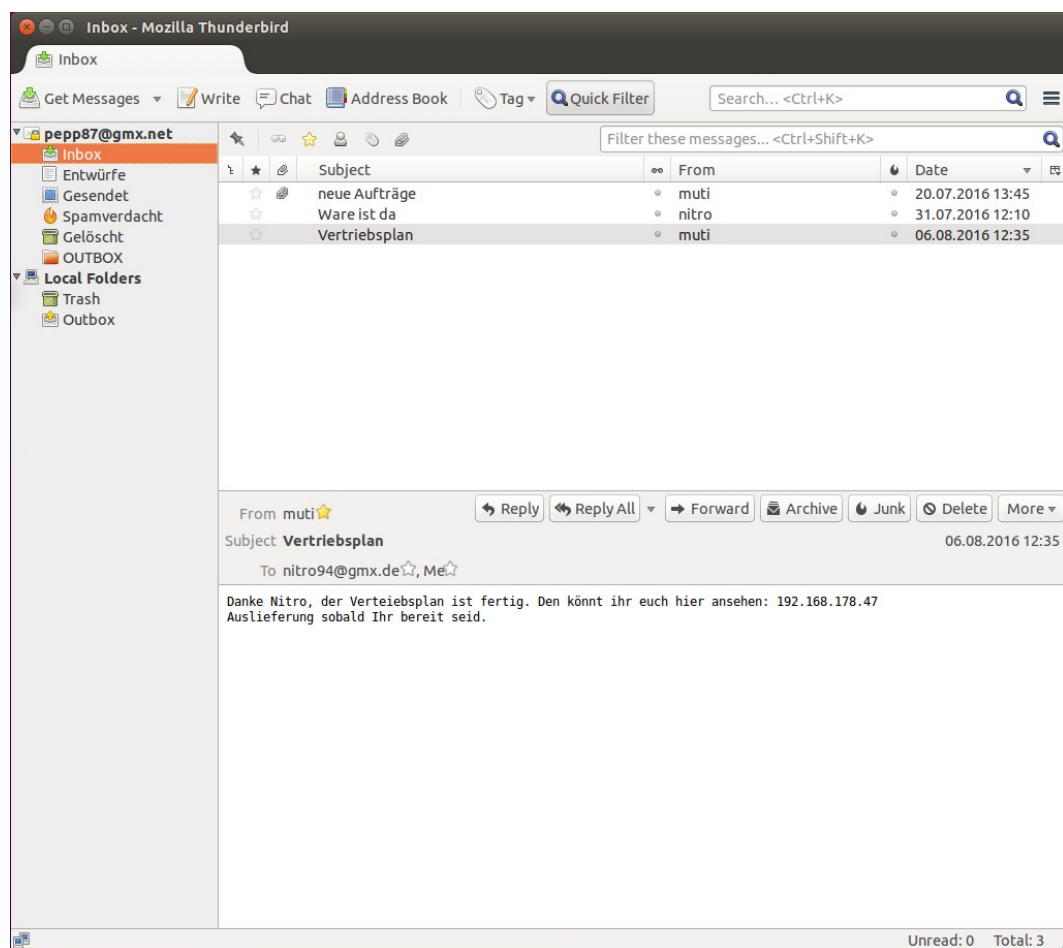


Abbildung A.8.: Inbox pepp87@gmx.net

WHO ARE YOU?

Forensisches Fallbeispiel

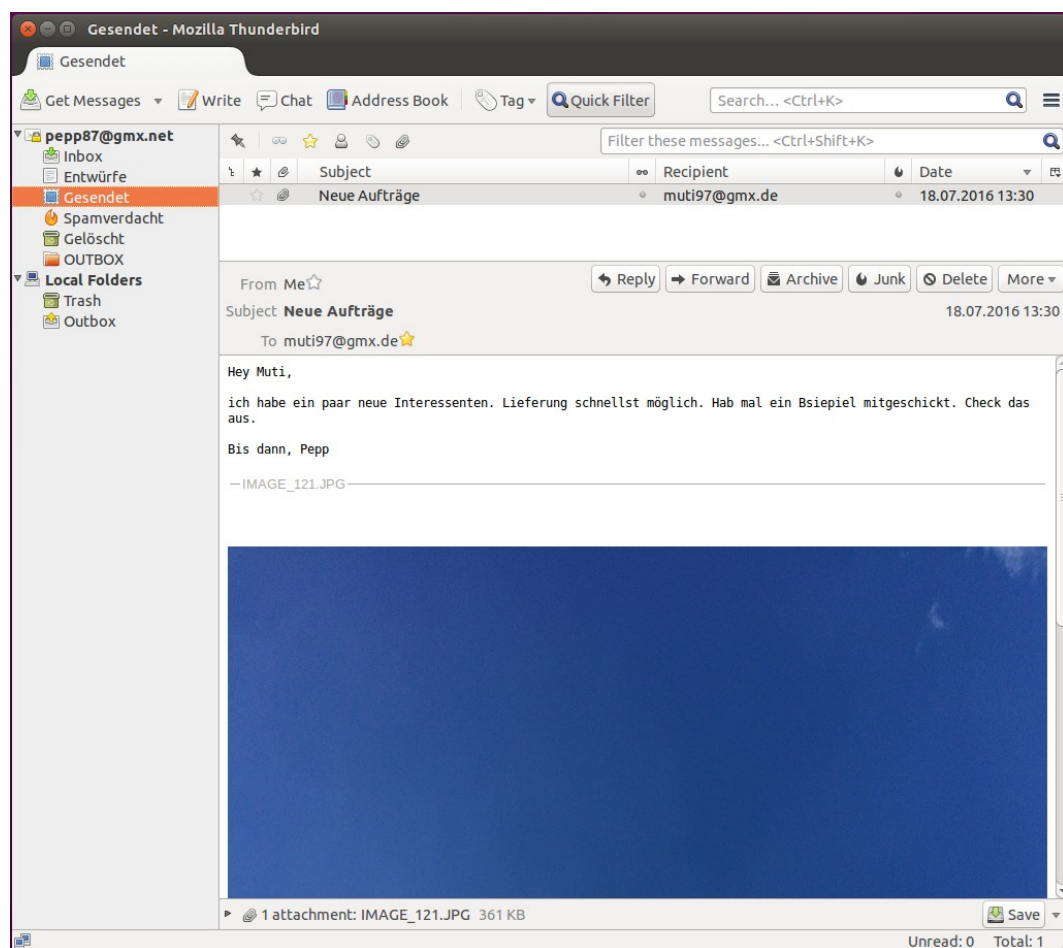


Abbildung A.9.: Sent pepp87@gmx.net

WHO ARE YOU?

Forensisches Fallbeispiel

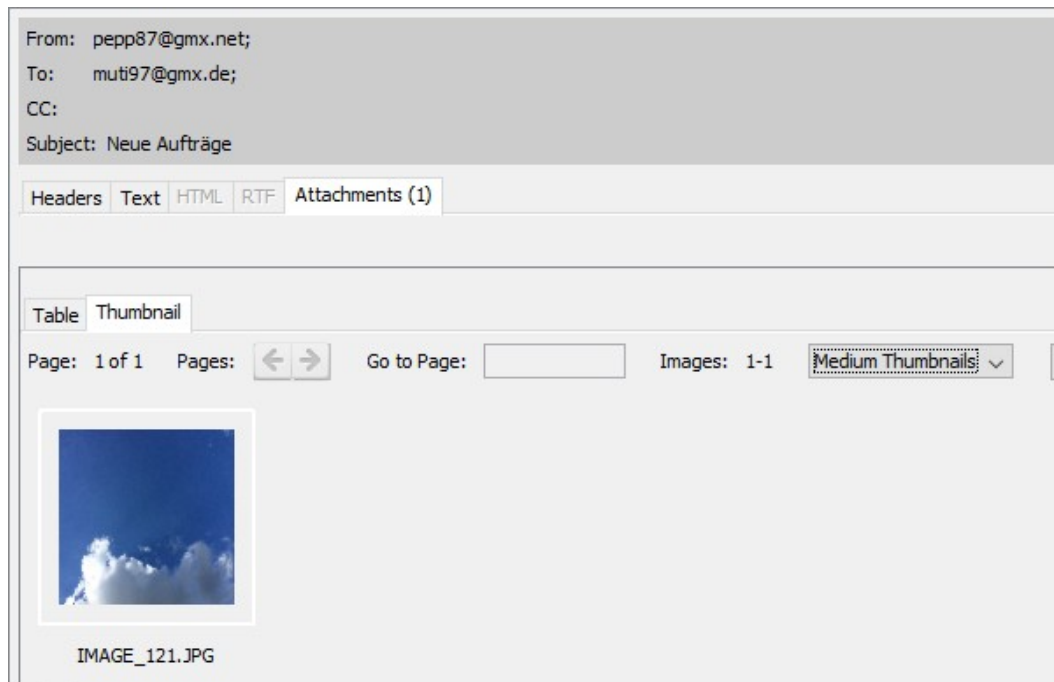


Abbildung A.10.: Email 001 - Neue Aufträge (Anhang)

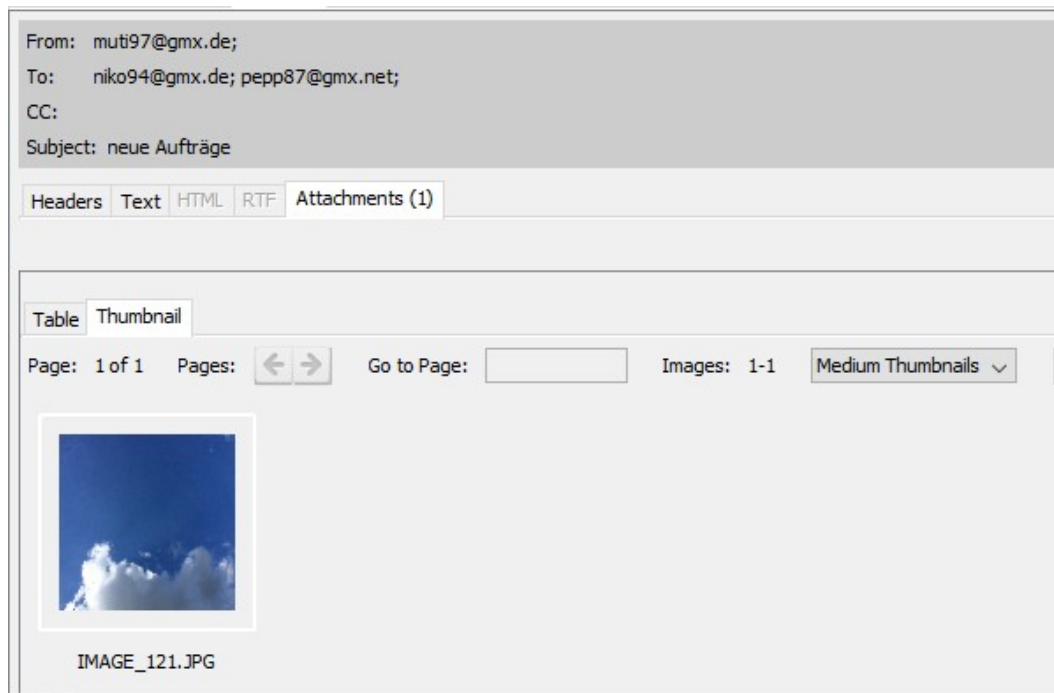


Abbildung A.11.: Email 002 - neue Aufträge (Anhang)

WHO ARE YOU?

Forensisches Fallbeispiel

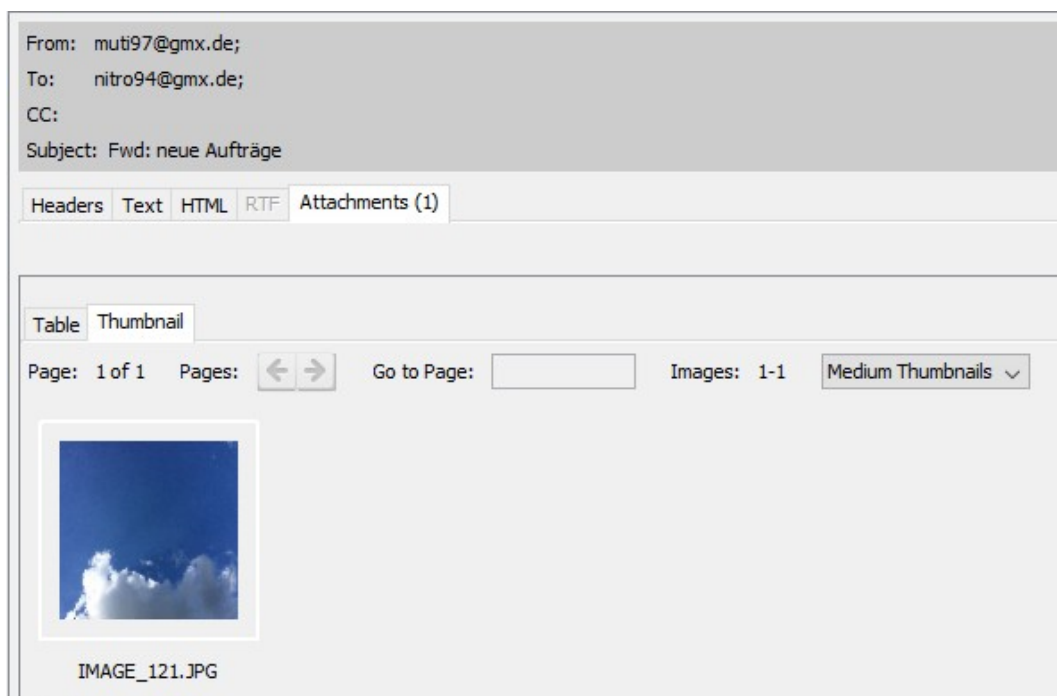


Abbildung A.12.: Email 003 - Fwd: neue Aufträge (Anhang)

A.4. Zeitgeist

Listing A.4: zeitgeistanalyse.sql

```
1 SELECT DATETIME(ROUND(timestamp / 1000), 'unixepoch') as Timestamp,
2     ev.subj_text as Subject,
3     ev.subj_uri as 'Subject Path',
4     substr(jintSubj.value, instr(jintSubj.value, '#') + 1) as 'Subject
,→ Interpretation',
5     substr(manifSubj.value, instr(manifSubj.value, '#') + 1) as 'Subject
,→ Manifestation',
6     substr(jint.value, instr(jint.value, '#') + 1) as 'Action',
7     substr(manif.value, instr(manif.value, '#') + 1 ) as 'Action Manifestation'
8 FROM event_view as ev
9 INNER JOIN interpretation as jint on jint.id = ev.interpretation
10 INNER JOIN interpretation as jintSubj on jintSubj.id = ev.subj_interpretation
11 INNER JOIN manifestation as manif on manif.id = ev.manifestation
12 INNER JOIN manifestation as manifSubj on manifSubj.id = ev.subj_manifestation
```


A.5. Medien

File Path

```
/img_Stick2.dd/vol_vol4/MOVIE_4.mpg
/ContainerVM1/.Trash-1000/files/IMAGE_132.JPG
/img_Stick4.dd/Daten/Bilder.zip/IMAGE_132.JPG
/img_Stick2.dd/vol_vol4/MOVIE_1.mpg
/ContainerVM1/.Trash-1000/files/IMAGE_135.JPG
/img_Stick3.dd/IMAGE_129.JPG
/img_stick1.dd/vol_vol4/IMAGE_128.JPG
/ContainerVM1/.Trash-1000/files/IMAGE_124.JPG
/img_Stick3.dd/IMAGE_132.JPG
/ContainerVM1/Urlaub4.txt
/ContainerVM1/.Trash-1000/files/IMAGE_127.JPG
/ContainerVM1/Urlaub5.txt
/img_stick1.dd/vol_vol4/IMAGE_125.JPG
/ContainerVM1/.Trash-1000/files/IMAGE_130.JPG
/ContainerVM1/.Trash-1000/files/IMAGE_133.JPG
/img_Stick4.dd/Daten/Bilder.zip/IMAGE_129.JPG
/img_stick1.dd/vol_vol4/IMAGE_121.JPG
/img_Stick2.dd/vol_vol4/MOVIE_3.mpg
/ContainerVM1/.Trash-1000/files/IMAGE_125.JPG
/img_Stick3.dd/IMAGE_133.JPG
/img_Stick2.dd/vol_vol4/IMAGE_135.JPG
/img_stick1.dd/vol_vol4/IMAGE_126.JPG
/ContainerVM1/Urlaub3.txt
/ContainerVM1/.Trash-1000/files/IMAGE_128.JPG
/img_Stick3.dd/IMAGE_130.JPG
/ContainerVM1/Urlaub6.txt
/ContainerVM1/.Trash-1000/files/IMAGE_131.JPG
/img_Stick4.dd/Daten/Bilder.zip/IMAGE_131.JPG
/img_stick1.dd/vol_vol4/IMAGE_122.JPG
/img_stick1.dd/vol_vol4/IMAGE_123.JPG
/ContainerVM1/.Trash-1000/files/IMAGE_134.JPG
/img_Stick4.dd/Daten/Bilder.zip
/img_Stick4.dd/Daten/Bilder.zip/IMAGE_130.JPG
/ContainerVM1/.Trash-1000/files/IMAGE_123.JPG
/img_Stick2.dd/vol_vol4/MOVIE_2.mpg
/ContainerVM1/Urlaub2.txt
/img_stick1.dd/vol_vol4/IMAGE_127.JPG
```

MD5 Hash

```
4ba983ab9b083549c123c603c8d93f39
5383de1960832d5c3d356b9cc41e48b8
5383de1960832d5c3d356b9cc41e48b8
6396875c8619361cd4271f7cd7dfec3c
44f0786ba69c50db7a8f978889f7c6cf
8977a3717bcd68dc9d4adb24c66b3f8
969f0f1eb4d10659f2bb35cb579e67d3
2ec96ec2ddbe8699fa1e24324efbdb00
5383de1960832d5c3d356b9cc41e48b8
4b579dda2fad59d4ee983361feb70261
fc08ecc7da1287bc7e824c61ec3cd3fa
8af5a5e8a2190a7be1a0b072544bcdff9
44849ef3351b81145366ff3908a1987e
43f7b0bff9aa8433f722912785538ea2
ac311d5b2027be1e45228a7473960682
8977a3717bcd68dc9d4adb24c66b3f8
3f5f0a4b9c8d774f0242c84d1fda2577
8af5a5e8a2190a7be1a0b072544bcdff9
44849ef3351b81145366ff3908a1987e
ac311d5b2027be1e45228a7473960682
44f0786ba69c50db7a8f978889f7c6cf
028905b8afffecfb7aca2b5975fc21d
6396875c8619361cd4271f7cd7dfec3c
969f0f1eb4d10659f2bb35cb579e67d3
43f7b0bff9aa8433f722912785538ea2
4ba983ab9b083549c123c603c8d93f39
ecc04f2b32e56a7fc28c2677f26fd6c6
ecc04f2b32e56a7fc28c2677f26fd6c6
e2485f5650a48af631cf79c937a741ca
ecdfc5ee600db53b4fd6f63bba296dfb
dc55c4560205eb9e0bd773cd69f05774
ff719c1060f77d803a8f9e4639671384
43f7b0bff9aa8433f722912785538ea2
ecdfc5ee600db53b4fd6f63bba296dfb
4b579dda2fad59d4ee983361feb70261
3f5f0a4b9c8d774f0242c84d1fda2577
fc08ecc7da1287bc7e824c61ec3cd3fa
```

WHO ARE YOU?

Forensisches Fallbeispiel

| | |
|--|-----------------------------------|
| /ContainerVM1/.Trash-1000/files/IMAGE_126.JPG | 028905b8afffeacfb7aca2b5975fc21d |
| /img_Stick2.dd/vol_vol4/IMAGE_134.JPG | dc55c4560205eb9e0bd773cd69f05774 |
| /ContainerVM1/.Trash-1000/files/IMAGE_129.JPG | 8977a3717bcd6c68dc9d4adb24c66b3f8 |
| /img_Stick3.dd/IMAGE_131.JPG | ecc04f2b32e56a7fc28c2677f26fd6c6 |
| /img_Stick4.dd/Daten/Bilder.zip/IMAGE_133.JPG | ac311d5b2027be1e45228a7473960682 |
| /img_stick1.dd/vol_vol4/IMAGE_124.JPG | 2ec96ec2ddbe8699fa1e24324efbdb00 |
| /ContainerVM1/Urlaub1.txt | e2485f5650a48af631cf79c937a741ca |
| \path{/img_vm1_dd.001/vol_vol2/home/user/Desktop/ Mark_Quark/IMAGE_135.JPG} | 44f0786ba69c50db7a8f978889f7c6cf |
| /img_vm1_dd.001/vol_vol2/home/user/Desktop/Bart_ Simpson/MOVIE_2.mpg | 4b579dda2fad59d4ee983361feb70261 |
| /img_vm1_dd.001/vol_vol2/home/user/Desktop/Mark_ Quark/IMAGE_121.JPG | 3f5f0a4b9c8d774f0242c84d1fda2577 |
| /img_vm1_dd.001/vol_vol2/home/user/Desktop/IMAGE_ 123.JPG | ecdfc5ee600db53b4fd6f63bba296dfb |
| /img_vm1_dd.001/vol_vol2/home/user/Desktop/Mark_ Quark/IMAGE_128.JPG | 969f0f1eb4d10659f2bb35cb579e67d3 |
| /img_vm1_dd.001/vol_vol2/home/user/Desktop/Bart_ Simpson/IMAGE_128.JPG | 969f0f1eb4d10659f2bb35cb579e67d3 |
| /img_vm1_dd.001/vol_vol2/home/user/Desktop/Mark_ Quark/IMAGE_125.JPG | 44849ef3351b81145366ff3908a1987e |
| /img_vm1_dd.001/vol_vol2/home/user/Desktop/Mark_ Quark/IMAGE_132.JPG | 5383de1960832d5c3d356b9cc41e48b8 |
| /img_vm1_dd.001/vol_vol2/home/user/Desktop/Mark_ Quark/IMAGE_127.JPG | fc08ecc7da1287bc7e824c61ec3cd3fa |
| /img_vm1_dd.001/vol_vol2/home/user/Desktop/Mark_ Quark/IMAGE_134.JPG | dc55c4560205eb9e0bd773cd69f05774 |
| /img_vm1_dd.001/vol_vol2/home/user/Desktop/Bart_ Simpson/IMAGE_127.JPG | fc08ecc7da1287bc7e824c61ec3cd3fa |
| /img_vm1_dd.001/vol_vol2/home/user/Desktop/Mark_ Quark/MOVIE_1.mpg | 6396875c8619361cd4271f7cd7dfec3c |
| /img_vm1_dd.001/vol_vol2/home/user/Desktop/IMAGE_ 124.JPG | 2ec96ec2ddbe8699fa1e24324efbdb00 |
| /img_vm1_dd.001/vol_vol2/home/user/Desktop/Mark_ Quark/IMAGE_131.JPG | ecc04f2b32e56a7fc28c2677f26fd6c6 |
| /img_vm1_dd.001/vol_vol2/home/user/Desktop/Bart_ Simpson/IMAGE_131.JPG | ecc04f2b32e56a7fc28c2677f26fd6c6 |
| /img_vm1_dd.001/vol_vol2/home/user/Desktop/IMAGE_ 127.JPG | fc08ecc7da1287bc7e824c61ec3cd3fa |

WHO ARE YOU?

Forensisches Fallbeispiel

| | |
|---|-----------------------------------|
| /img_vm1_dd.001/vol_vol2/home/user/Desktop/Mark_Quark/IMAGE_124.JPG | 2ec96ec2ddbe8699fa1e24324efbdbb00 |
| /img_vm1_dd.001/vol_vol2/home/user/Desktop/MOVIE_3.mpg | 8af5a5e8a2190a7be1a0b072544bcd9f9 |
| /img_vm1_dd.001/vol_vol2/home/user/Desktop/IMAGE_125.JPG | 44849ef3351b81145366ff3908a1987e |
| /img_vm1_dd.001/vol_vol2/home/user/Desktop/Mark_Quark/IMAGE_126.JPG | 028905b8afffeacfb7aca2b5975fc21d |
| /img_vm1_dd.001/vol_vol2/home/user/Desktop/MOVIE_2.mpg | 4b579dda2fad59d4ee983361feb70261 |
| /img_vm1_dd.001/vol_vol2/home/user/Desktop/Bart_Simpson/IMAGE_126.JPG | 028905b8afffeacfb7aca2b5975fc21d |
| /img_vm1_dd.001/vol_vol2/home/user/Desktop/Mark_Quark/IMAGE_123.JPG | ecdfe5ee600db53b4fd6f63bba296dfb |
| /img_vm1_dd.001/vol_vol2/home/user/Desktop/IMAGE_121.JPG | 3f5f0a4b9c8d774f0242c84d1fda2577 |
| /img_vm1_dd.001/vol_vol2/home/user/Desktop/Mark_Quark/IMAGE_130.JPG | 43f7b0bff9aa8433f722912785538ea2 |
| /img_vm1_dd.001/vol_vol2/home/user/Desktop/Bart_Simpson/MOVIE_1.mpg | 6396875c8619361cd4271f7cd7dfec3c |
| /img_vm1_dd.001/vol_vol2/home/user/Desktop/Bart_Simpson/IMAGE_130.JPG | 43f7b0bff9aa8433f722912785538ea2 |
| /img_vm1_dd.001/vol_vol2/home/user/Desktop/IMAGE_128.JPG | 969f0f1eb4d10659f2bb35cb579e67d3 |
| /img_vm1_dd.001/vol_vol2/home/user/Desktop/Bart_Simpson/MOVIE_3.mpg | 8af5a5e8a2190a7be1a0b072544bcd9f9 |
| /img_vm1_dd.001/vol_vol2/home/user/Desktop/Bart_Simpson/IMAGE_132.JPG | 5383de1960832d5c3d356b9cc41e48b8 |
| /img_vm1_dd.001/vol_vol2/home/user/Desktop/IMAGE_126.JPG | 028905b8afffeacfb7aca2b5975fc21d |
| /img_vm1_dd.001/vol_vol2/home/user/Desktop/Mark_Quark/IMAGE_129.JPG | 8977a3717bcd68dc9d4adb24c66b3f8 |
| /img_vm1_dd.001/vol_vol2/home/user/Desktop/MOVIE_4.mpg | 4ba983ab9b083549c123c603c8d93f39 |
| /img_vm1_dd.001/vol_vol2/home/user/Desktop/Bart_Simpson/IMAGE_129.JPG | 8977a3717bcd68dc9d4adb24c66b3f8 |
| /img_vm1_dd.001/vol_vol2/home/user/Desktop/Mark_Quark/IMAGE_122.JPG | e2485f5650a48af631cf79c937a741ca |

WHO ARE YOU?

Forensisches Fallbeispiel

| | |
|---|-----------------------------------|
| /img_vm1_dd.001/vol_vol2/home/user/Desktop/IMAGE_122.JPG | e2485f5650a48af631cf79c937a741ca |
| /img_vm1_dd.001/vol_vol2/home/user/Desktop/Mark_Quark/IMAGE_133.JPG | ac311d5b2027be1e45228a7473960682 |
| /img_vm1_dd.001/vol_vol2/home/user/Downloads/IMAGE_121.JPG | 3f5f0a4b9c8d774f0242c84d1fda2577 |
| /img_vm1_dd.001/vol_vol2/home/user/Downloads/neue_ware.tar.gz/neue_ware.tar/IMAGE_121.JPG | 3f5f0a4b9c8d774f0242c84d1fda2577 |
| /img_vm1_dd.001/vol_vol2/var/www/html/neue_ware.tar.gz/neue_ware.tar/IMAGE_132.JPG | 5383de1960832d5c3d356b9cc41e48b8 |
| /img_vm1_dd.001/vol_vol2/home/user/Desktop/neue_ware.tar.gz/neue_ware.tar/IMAGE_131.JPG | ecc04f2b32e56a7fc28c2677f26fd6c6 |
| /img_vm1_dd.001/vol_vol2/home/user/Desktop/Pumuckel/IMAGE_131.JPG | ecc04f2b32e56a7fc28c2677f26fd6c6 |
| /img_vm1_dd.001/vol_vol2/home/user/Downloads/neue_ware.tar.gz/neue_ware.tar/IMAGE_131.JPG | ecc04f2b32e56a7fc28c2677f26fd6c6 |
| /img_vm1_dd.001/vol_vol2/home/user/Desktop/neue_ware.tar.gz | 4bec7618bdaebbbb449485254ad0ab5c0 |
| /img_vm1_dd.001/vol_vol2/home/user/Downloads/MOVIE_1.mpg | 6396875c8619361cd4271f7cd7dfec3c |
| /img_vm1_dd.001/vol_vol2/home/user/Downloads/neue_ware.tar.gz/neue_ware.tar/IMAGE_127.JPG | fc08ecc7da1287bc7e824c61ec3cd3fa |
| /img_vm1_dd.001/vol_vol2/var/www/html/neue_ware.tar.gz/neue_ware.tar/IMAGE_124.JPG | 2ec96ec2ddbe8699fa1e24324efbdb00 |
| /img_vm1_dd.001/vol_vol2/home/user/Downloads/IMAGE_134.JPG | dc55c4560205eb9e0bd773cd69f05774 |
| /img_vm1_dd.001/vol_vol2/home/user/Desktop/neue_ware.tar.gz/neue_ware.tar/IMAGE_128.JPG | 969f0f1eb4d10659f2bb35cb579e67d3 |
| /img_vm1_dd.001/vol_vol2/home/user/Downloads/IMAGE_122.JPG | e2485f5650a48af631cf79c937a741ca |
| /img_vm1_dd.001/vol_vol2/var/www/html/neue_ware.tar.gz/neue_ware.tar/IMAGE_135.JPG | 44f0786ba69c50db7a8f978889f7c6cf |
| /img_vm1_dd.001/vol_vol2/home/user/Desktop/neue_ware.tar.gz/neue_ware.tar/IMAGE_122.JPG | e2485f5650a48af631cf79c937a741ca |
| /img_vm1_dd.001/vol_vol2/var/www/html/neue_ware.tar.gz/neue_ware.tar/IMAGE_129.JPG | 8977a3717bcd68dc9d4adb24c66b3f8 |
| /img_vm1_dd.001/vol_vol2/var/www/html/neue_ware.tar.gz/neue_ware.tar/MOVIE_1.mpg | 6396875c8619361cd4271f7cd7dfec3c |

WHO ARE YOU?

Forensisches Fallbeispiel

| | |
|---|----------------------------------|
| /img_vm1_dd.001/vol_vol2/home/user/Downloads/ neue_ware.tar.gz/neue_ware.tar/MOVIE_4.mpg | 4ba983ab9b083549c123c603c8d93f39 |
| /img_vm1_dd.001/vol_vol2/home/user/Desktop/neue_ ware.tar.gz/neue_ware.tar/IMAGE_130.JPG | 43f7b0bff9aa8433f722912785538ea2 |
| /img_vm1_dd.001/vol_vol2/home/user/Downloads/ IMAGE_127.JPG | fc08ecc7da1287bc7e824c61ec3cd3fa |
| /img_vm1_dd.001/vol_vol2/home/user/Desktop/neue_ ware.tar.gz/neue_ware.tar | 800fbe34d1037e1a3d19afa9a7d8be75 |
| /img_vm1_dd.001/vol_vol2/var/www/html/neue_ware. tar.gz/neue_ware.tar/IMAGE_123.JPG | ecdfc5ee600db53b4fd6f63bba296dfb |
| /img_vm1_dd.001/vol_vol2/home/user/Desktop/neue_ ware.tar.gz/neue_ware.tar/IMAGE_125.JPG | 44849ef3351b81145366ff3908a1987e |
| /img_vm1_dd.001/vol_vol2/home/user/Downloads/ neue_ware.tar.gz/neue_ware.tar | 800fbe34d1037e1a3d19afa9a7d8be75 |
| /img_vm1_dd.001/vol_vol2/home/user/Downloads/ neue_ware.tar.gz/neue_ware.tar/IMAGE_126.JPG | 028905b8afffeacfb7aca2b5975fc21d |
| /img_vm1_dd.001/vol_vol2/home/user/Desktop/neue_ ware.tar.gz/neue_ware.tar/IMAGE_121.JPG | 3f5f0a4b9c8d774f0242c84d1fda2577 |
| /img_vm1_dd.001/vol_vol2/var/www/html/neue_ware. tar.gz/neue_ware.tar/IMAGE_122.JPG | e2485f5650a48af631cf79c937a741ca |
| /img_vm1_dd.001/vol_vol2/home/user/Downloads/ MOVIE_2.mpg | 4b579dda2fad59d4ee983361feb70261 |
| /img_vm1_dd.001/vol_vol2/home/user/Downloads/ neue_ware.tar.gz/neue_ware.tar/MOVIE_3.mpg | 8af5a5e8a2190a7be1a0b072544bcd9 |
| /img_vm1_dd.001/vol_vol2/home/user/Downloads/ IMAGE_128.JPG | 969f0f1eb4d10659f2bb35cb579e67d3 |
| /img_vm1_dd.001/vol_vol2/home/user/Desktop/neue_ ware.tar.gz/neue_ware.tar/IMAGE_133.JPG | ac311d5b2027be1e45228a7473960682 |
| /img_vm1_dd.001/vol_vol2/home/user/Downloads/ IMAGE_131.JPG | ecc04f2b32e56a7fc28c2677f26fd6c6 |
| /img_vm1_dd.001/vol_vol2/home/user/Downloads/ neue_ware.tar.gz/neue_ware.tar/IMAGE_134.JPG | dc55c4560205eb9e0bd773cd69f05774 |
| /img_vm1_dd.001/vol_vol2/home/user/Downloads/ neue_ware.tar.gz/neue_ware.tar/IMAGE_133.JPG | ac311d5b2027be1e45228a7473960682 |
| /img_vm1_dd.001/vol_vol2/var/www/html/neue_ware. tar.gz/neue_ware.tar/IMAGE_130.JPG | 43f7b0bff9aa8433f722912785538ea2 |
| /img_vm1_dd.001/vol_vol2/home/user/Downloads/ neue_ware.tar.gz/neue_ware.tar/IMAGE_125.JPG | 44849ef3351b81145366ff3908a1987e |

WHO ARE YOU?

Forensisches Fallbeispiel

| | |
|---|----------------------------------|
| /img_vm1_dd.001/vol_vol2/var/www/html/neue_ware. tar.gz/neue_ware.tar/IMAGE_121.JPG | 3f5f0a4b9c8d774f0242c84d1fda2577 |
| /img_vm1_dd.001/vol_vol2/home/user/Desktop/neue_ ware.tar.gz/neue_ware.tar/MOVIE_2.mpg | 4b579dda2fad59d4ee983361feb70261 |
| /img_vm1_dd.001/vol_vol2/home/user/Downloads/ IMAGE_123.JPG | ecdfc5ee600db53b4fd6f63bba296dfb |
| /img_vm1_dd.001/vol_vol2/home/user/Downloads/ neue_ware.tar.gz/neue_ware.tar/MOVIE_2.mpg | 4b579dda2fad59d4ee983361feb70261 |
| /img_vm1_dd.001/vol_vol2/var/www/html/neue_ware. tar.gz/neue_ware.tar/IMAGE_128.JPG | 969f0f1eb4d10659f2bb35cb579e67d3 |
| /img_vm1_dd.001/vol_vol2/home/user/Downloads/ IMAGE_130.JPG | 43f7b0bff9aa8433f722912785538ea2 |
| /img_vm1_dd.001/vol_vol2/home/user/Desktop/ Pumuckel/IMAGE_132.JPG | 5383de1960832d5c3d356b9cc41e48b8 |
| /img_vm1_dd.001/vol_vol2/var/www/html/neue_ware. tar.gz/neue_ware.tar/IMAGE_131.JPG | ecc04f2b32e56a7fc28c2677f26fd6c6 |
| /img_vm1_dd.001/vol_vol2/home/user/Desktop/neue_ ware.tar.gz/neue_ware.tar/IMAGE_134.JPG | dc55c4560205eb9e0bd773cd69f05774 |
| /img_vm1_dd.001/vol_vol2/home/user/Downloads/ IMAGE_129.JPG | 8977a3717bcd68dc9d4adb24c66b3f8 |
| /img_vm1_dd.001/vol_vol2/home/user/Desktop/neue_ ware.tar.gz/neue_ware.tar/IMAGE_126.JPG | 028905b8afffeacfb7aca2b5975fc21d |
| /img_vm1_dd.001/vol_vol2/home/user/Downloads/ IMAGE_124.JPG | 2ec96ec2ddbe8699fa1e24324efbdb00 |
| /img_vm1_dd.001/vol_vol2/home/user/Desktop/neue_ ware.tar.gz/neue_ware.tar/IMAGE_123.JPG | ecdfc5ee600db53b4fd6f63bba296dfb |
| /img_vm1_dd.001/vol_vol2/home/user/Downloads/ IMAGE_135.JPG | 44f0786ba69c50db7a8f978889f7c6cf |
| /img_vm1_dd.001/vol_vol2/home/user/Downloads/ neue_ware.tar.gz/neue_ware.tar/IMAGE_124.JPG | 2ec96ec2ddbe8699fa1e24324efbdb00 |
| /img_vm1_dd.001/vol_vol2/var/www/html/neue_ware. tar.gz/neue_ware.tar/IMAGE_127.JPG | fc08ecc7da1287bc7e824c61ec3cd3fa |
| /img_vm1_dd.001/vol_vol2/home/user/Desktop/neue_ ware.tar.gz/neue_ware.tar/MOVIE_3.mpg | 8af5a5e8a2190a7be1a0b072544bcd9f |
| /img_vm1_dd.001/vol_vol2/var/www/html/neue_ware. tar.gz/neue_ware.tar/MOVIE_4.mpg | 4ba983ab9b083549c123c603c8d93f39 |
| /img_vm1_dd.001/vol_vol2/home/user/Downloads/ neue_ware.tar.gz/neue_ware.tar/MOVIE_1.mpg | 6396875c8619361cd4271f7cd7dfec3c |

WHO ARE YOU?

Forensisches Fallbeispiel

| | |
|---|-----------------------------------|
| /img_vm1_dd.001/vol_vol2/home/user/Desktop/neue_ware.tar.gz/neue_ware.tar/IMAGE_135.JPG | 44f0786ba69c50db7a8f978889f7c6cf |
| /img_vm1_dd.001/vol_vol2/home/user/Downloads/MOVIE_3.mpg | 8af5a5e8a2190a7be1a0b072544bcd9f |
| /img_vm1_dd.001/vol_vol2/var/www/html/neue_ware.tar.gz/neue_ware.tar/IMAGE_126.JPG | 028905b8afffeacfb7aca2b5975fc21d |
| /img_vm1_dd.001/vol_vol2/home/user/Downloads/neue_ware.tar.gz/neue_ware.tar/IMAGE_132.JPG | 5383de1960832d5c3d356b9cc41e48b8 |
| /img_vm1_dd.001/vol_vol2/home/user/Downloads/IMAGE_132.JPG | 5383de1960832d5c3d356b9cc41e48b8 |
| /img_vm1_dd.001/vol_vol2/home/user/Downloads/neue_ware.tar.gz | 4bec7618bdaebbbb449485254ad0ab5c0 |
| /img_vm1_dd.001/vol_vol2/home/user/Downloads/neue_ware.tar.gz/neue_ware.tar/IMAGE_123.JPG | ecdfe5ee600db53b4fd6f63bba296dfb |
| /img_vm1_dd.001/vol_vol2/home/user/Desktop/neue_ware.tar.gz/neue_ware.tar/IMAGE_129.JPG | 8977a3717bcd68dc9d4adb24c66b3f8 |
| /img_vm1_dd.001/vol_vol2/home/user/Downloads/neue_ware.tar.gz/neue_ware.tar/IMAGE_129.JPG | 8977a3717bcd68dc9d4adb24c66b3f8 |
| /img_vm1_dd.001/vol_vol2/home/user/Desktop/neue_ware.tar.gz/neue_ware.tar/MOVIE_4.mpg | 4ba983ab9b083549c123c603c8d93f39 |
| /img_vm1_dd.001/vol_vol2/home/user/Downloads/MOVIE_4.mpg | 4ba983ab9b083549c123c603c8d93f39 |
| /img_vm1_dd.001/vol_vol2/var/www/html/neue_ware.tar.gz/neue_ware.tar/IMAGE_125.JPG | 44849ef3351b81145366ff3908a1987e |
| /img_vm1_dd.001/vol_vol2/home/user/Downloads/IMAGE_125.JPG | 44849ef3351b81145366ff3908a1987e |
| /img_vm1_dd.001/vol_vol2/home/user/Downloads/neue_ware.tar.gz/neue_ware.tar/IMAGE_135.JPG | 44f0786ba69c50db7a8f978889f7c6cf |
| /img_vm1_dd.001/vol_vol2/var/www/html/neue_ware.tar.gz/neue_ware.tar | 800fbe34d1037e1a3d19afa9a7d8be75 |
| /img_vm1_dd.001/vol_vol2/home/user/Desktop/neue_ware.tar.gz/neue_ware.tar/IMAGE_132.JPG | 5383de1960832d5c3d356b9cc41e48b8 |
| /img_vm1_dd.001/vol_vol2/var/www/html/neue_ware.tar.gz/neue_ware.tar/IMAGE_134.JPG | dc55c4560205eb9e0bd773cd69f05774 |
| /img_vm1_dd.001/vol_vol2/var/www/html/neue_ware.tar.gz | 4bec7618bdaebbbb449485254ad0ab5c0 |
| /img_vm1_dd.001/vol_vol2/home/user/Desktop/neue_ware.tar.gz/neue_ware.tar/IMAGE_124.JPG | 2ec96ec2ddbe8699fa1e24324efbdb00 |

WHO ARE YOU?

Forensisches Fallbeispiel

| | |
|---|----------------------------------|
| /img_vm1_dd.001/vol_vol2/var/www/html/neue_ware. tar.gz/neue_ware.tar/MOVIE_3.mpg | 8af5a5e8a2190a7be1a0b072544bcd9 |
| /img_vm1_dd.001/vol_vol2/home/user/Downloads/ neue_ware.tar.gz/neue_ware.tar/IMAGE_122.JPG | e2485f5650a48af631cf79c937a741ca |
| /img_vm1_dd.001/vol_vol2/home/user/Desktop/neue_ ware.tar.gz/neue_ware.tar/MOVIE_1.mpg | 6396875c8619361cd4271f7cd7dfec3c |
| /img_vm1_dd.001/vol_vol2/home/user/Downloads/ IMAGE_126.JPG | 028905b8afffeacfb7aca2b5975fc21d |
| /img_vm1_dd.001/vol_vol2/home/user/Downloads/ neue_ware.tar.gz/neue_ware.tar/IMAGE_130.JPG | 43f7b0bff9aa8433f722912785538ea2 |
| /img_vm1_dd.001/vol_vol2/var/www/html/neue_ware. tar.gz/neue_ware.tar/IMAGE_133.JPG | ac311d5b2027be1e45228a7473960682 |
| /img_vm1_dd.001/vol_vol2/home/user/Desktop/neue_ ware.tar.gz/neue_ware.tar/IMAGE_127.JPG | fc08ecc7da1287bc7e824c61ec3cd3fa |
| /img_vm1_dd.001/vol_vol2/home/user/Downloads/ neue_ware.tar.gz/neue_ware.tar/IMAGE_128.JPG | 969f0f1eb4d10659f2bb35cb579e67d3 |
| /img_vm1_dd.001/vol_vol2/var/www/html/neue_ware. tar.gz/neue_ware.tar/MOVIE_2.mpg | 4b579dda2fad59d4ee983361feb70261 |
| /img_vm1_dd.001/vol_vol2/home/user/Downloads/ IMAGE_133.JPG | ac311d5b2027be1e45228a7473960682 |
| /img_vm2_dd.001/vol_vol6/home/user/Downloads/ MOVIE_2.mpg | 4b579dda2fad59d4ee983361feb70261 |
| /img_vm2_dd.001/vol_vol6/home/user/Downloads/ IMAGE_132.JPG | 5383de1960832d5c3d356b9cc41e48b8 |
| /img_vm2_dd.001/vol_vol6/home/user/Downloads/ neue_ware.tar.gz/neue_ware.tar | 800fbe34d1037e1a3d19afa9a7d8be75 |
| /img_vm2_dd.001/vol_vol6/home/user/Documents/ Aeffle_und_Pferdle/MOVIE_1.mpg | 6396875c8619361cd4271f7cd7dfec3c |
| /img_vm2_dd.001/vol_vol6/home/user/Documents/ Aeffle_und_Pferdle/IMAGE_134.JPG | dc55c4560205eb9e0bd773cd69f05774 |
| /img_vm2_dd.001/vol_vol6/home/user/Downloads/ neue_ware.tar.gz/neue_ware.tar/IMAGE_126.JPG | 028905b8afffeacfb7aca2b5975fc21d |
| /img_vm2_dd.001/vol_vol6/home/user/Downloads/ neue_ware.tar.gz/neue_ware.tar/MOVIE_4.mpg | 4ba983ab9b083549c123c603c8d93f39 |
| /img_vm2_dd.001/vol_vol6/home/user/Documents/Die_ Maus/IMAGE_125.JPG | 44849ef3351b81145366ff3908a1987e |
| /img_vm2_dd.001/vol_vol6/home/user/Downloads/ IMAGE_123.JPG | ecdfc5ee600db53b4fd6f63bba296dfb |

WHO ARE YOU?

Forensisches Fallbeispiel

| | |
|---|----------------------------------|
| /img_vm2_dd.001/vol_vol6/home/user/Documents/Aeffle_und_Pferdle/IMAGE_126.JPG | 028905b8afffeacfb7aca2b5975fc21d |
| /img_vm2_dd.001/vol_vol6/home/user/Documents/Die_Maus/IMAGE_128.JPG | 969f0f1eb4d10659f2bb35cb579e67d3 |
| /img_vm2_dd.001/vol_vol6/home/user/Documents/Die_Maus/IMAGE_131.JPG | ecc04f2b32e56a7fc28c2677f26fd6c6 |
| /img_vm2_dd.001/vol_vol6/home/user/Documents/Bernd_Das_Brot/IMAGE_135.JPG | 44f0786ba69c50db7a8f978889f7c6cf |
| /img_vm2_dd.001/vol_vol6/home/user/Downloads/IMAGE_135.JPG | 44f0786ba69c50db7a8f978889f7c6cf |
| /img_vm2_dd.001/vol_vol6/home/user/Downloads/neue_ware.tar.gz/neue_ware.tar/IMAGE_131.JPG | ecc04f2b32e56a7fc28c2677f26fd6c6 |
| /img_vm2_dd.001/vol_vol6/home/user/Downloads/MOVIE_4.mpg | 4ba983ab9b083549c123c603c8d93f39 |
| /img_vm2_dd.001/vol_vol6/home/user/Downloads/neue_ware.tar.gz/neue_ware.tar/IMAGE_127.JPG | fc08ecc7da1287bc7e824c61ec3cd3fa |
| /img_vm2_dd.001/vol_vol6/home/user/Documents/Aeffle_und_Pferdle/IMAGE_129.JPG | 8977a3717bcd68dc9d4adb24c66b3f8 |
| /img_vm2_dd.001/vol_vol6/home/user/Documents/Aeffle_und_Pferdle/IMAGE_132.JPG | 5383de1960832d5c3d356b9cc41e48b8 |
| /img_vm2_dd.001/vol_vol6/home/user/Documents/Die_Maus/IMAGE_134.JPG | dc55c4560205eb9e0bd773cd69f05774 |
| /img_vm2_dd.001/vol_vol6/home/user/Documents/Die_Maus/IMAGE_123.JPG | ecdfc5ee600db53b4fd6f63bba296dfb |
| /img_vm2_dd.001/vol_vol6/home/user/Downloads/neue_ware.tar.gz/neue_ware.tar/MOVIE_2.mpg | 4b579dda2fad59d4ee983361feb70261 |
| /img_vm2_dd.001/vol_vol6/home/user/Downloads/MOVIE_3.mpg | 8af5a5e8a2190a7be1a0b072544bcd9f |
| /img_vm2_dd.001/vol_vol6/home/user/Downloads/IMAGE_129.JPG | 8977a3717bcd68dc9d4adb24c66b3f8 |
| /img_vm2_dd.001/vol_vol6/home/user/Downloads/IMAGE_126.JPG | 028905b8afffeacfb7aca2b5975fc21d |
| /img_vm2_dd.001/vol_vol6/home/user/Documents/Aeffle_und_Pferdle/MOVIE_4.mpg | 4ba983ab9b083549c123c603c8d93f39 |
| /img_vm2_dd.001/vol_vol6/home/user/Documents/Die_Maus/IMAGE_126.JPG | 028905b8afffeacfb7aca2b5975fc21d |
| /img_vm2_dd.001/vol_vol6/home/user/Downloads/neue_ware.tar.gz/neue_ware.tar/IMAGE_133.JPG | ac311d5b2027be1e45228a7473960682 |

WHO ARE YOU?

Forensisches Fallbeispiel

| | |
|---|----------------------------------|
| /img_vm2_dd.001/vol_vol6/home/user/Documents/Aeffle_und_Pferdle/MOVIE_2.mpg | 4b579dda2fad59d4ee983361feb70261 |
| /img_vm2_dd.001/vol_vol6/home/user/Downloads/neue_ware.tar.gz/neue_ware.tar/IMAGE_125.JPG | 44849ef3351b81145366ff3908a1987e |
| /img_vm2_dd.001/vol_vol6/home/user/Downloads/IMAGE_134.JPG | dc55c4560205eb9e0bd773cd69f05774 |
| /img_vm2_dd.001/vol_vol6/home/user/Downloads/neue_ware.tar.gz/neue_ware.tar/MOVIE_3.mpg | 8af5a5e8a2190a7be1a0b072544bcd9 |
| /img_vm2_dd.001/vol_vol6/home/user/Documents/Aeffle_und_Pferdle/IMAGE_127.JPG | fc08ecc7da1287bc7e824c61ec3cd3fa |
| /img_vm2_dd.001/vol_vol6/home/user/Downloads/MOVIE_1.mpg | 6396875c8619361cd4271f7cd7dfec3c |
| /img_vm2_dd.001/vol_vol6/home/user/Downloads/neue_ware.tar.gz/neue_ware.tar/IMAGE_134.JPG | dc55c4560205eb9e0bd773cd69f05774 |
| /img_vm2_dd.001/vol_vol6/home/user/Downloads/neue_ware.tar.gz/neue_ware.tar/IMAGE_129.JPG | 8977a3717bcd68dc9d4adb24c66b3f8 |
| /img_vm2_dd.001/vol_vol6/home/user/Documents/Die_Maus/IMAGE_129.JPG | 8977a3717bcd68dc9d4adb24c66b3f8 |
| /img_vm2_dd.001/vol_vol6/home/user/Downloads/neue_ware.tar.gz/neue_ware.tar/IMAGE_135.JPG | 44f0786ba69c50db7a8f978889f7c6cf |
| /img_vm2_dd.001/vol_vol6/home/user/Desktop/IMAGE_121.JPG | 3f5f0a4b9c8d774f0242c84d1fda2577 |
| /img_vm2_dd.001/vol_vol6/home/user/Documents/Bernd_Das_Brot/MOVIE_4.mpg | 4ba983ab9b083549c123c603c8d93f39 |
| /img_vm2_dd.001/vol_vol6/home/user/Downloads/IMAGE_125.JPG | 44849ef3351b81145366ff3908a1987e |
| /img_vm2_dd.001/vol_vol6/home/user/Downloads/IMAGE_133.JPG | ac311d5b2027be1e45228a7473960682 |
| /img_vm2_dd.001/vol_vol6/home/user/Downloads/IMAGE_122.JPG | e2485f5650a48af631cf79c937a741ca |
| /img_vm2_dd.001/vol_vol6/home/user/Documents/Aeffle_und_Pferdle/IMAGE_130.JPG | 43f7b0bff9aa8433f722912785538ea2 |
| /img_vm2_dd.001/vol_vol6/home/user/Documents/Die_Maus/IMAGE_132.JPG | 5383de1960832d5c3d356b9cc41e48b8 |
| /img_vm2_dd.001/vol_vol6/home/user/Downloads/neue_ware.tar.gz/neue_ware.tar/IMAGE_123.JPG | ecdfe5ee600db53b4fd6f63bba296dfb |
| /img_vm2_dd.001/vol_vol6/home/user/Documents/Die_Maus/IMAGE_135.JPG | 44f0786ba69c50db7a8f978889f7c6cf |

WHO ARE YOU?

Forensisches Fallbeispiel

| | |
|---|----------------------------------|
| /img_vm2_dd.001/vol_vol6/home/user/Downloads/ neue_ware.tar.gz/neue_ware.tar/MOVIE_1.mpg | 6396875c8619361cd4271f7cd7dfec3c |
| /img_vm2_dd.001/vol_vol6/home/user/Downloads/ IMAGE_128.JPG | 969f0f1eb4d10659f2bb35cb579e67d3 |
| /img_vm2_dd.001/vol_vol6/home/user/Documents/Die_ Maus/IMAGE_121.JPG | 3f5f0a4b9c8d774f0242c84d1fda2577 |
| /img_vm2_dd.001/vol_vol6/home/user/Downloads/ neue_ware.tar.gz/neue_ware.tar/IMAGE_132.JPG | 5383de1960832d5c3d356b9cc41e48b8 |
| /img_vm2_dd.001/vol_vol6/home/user/Documents/ Aeffle_und_Pferdle/IMAGE_133.JPG | ac311d5b2027be1e45228a7473960682 |
| /img_vm2_dd.001/vol_vol6/home/user/Downloads/ neue_ware.tar.gz/neue_ware.tar/IMAGE_124.JPG | 2ec96ec2ddbe8699fa1e24324efbdb00 |
| /img_vm2_dd.001/vol_vol6/home/user/Documents/ Aeffle_und_Pferdle/MOVIE_3.mpg | 8af5a5e8a2190a7be1a0b072544bcd9 |
| /img_vm2_dd.001/vol_vol6/home/user/Downloads/ neue_ware.tar.gz | 4bec7618bdaebbb449485254ad0ab5c0 |
| /img_vm2_dd.001/vol_vol6/home/user/Documents/Die_ Maus/IMAGE_124.JPG | 2ec96ec2ddbe8699fa1e24324efbdb00 |
| /img_vm2_dd.001/vol_vol6/home/user/Documents/Die_ Maus/IMAGE_127.JPG | fc08ecc7da1287bc7e824c61ec3cd3fa |
| /img_vm2_dd.001/vol_vol6/home/user/Downloads/ neue_ware.tar.gz/neue_ware.tar/IMAGE_121.JPG | 3f5f0a4b9c8d774f0242c84d1fda2577 |
| /img_vm2_dd.001/vol_vol6/home/user/Downloads/ IMAGE_121.JPG | 3f5f0a4b9c8d774f0242c84d1fda2577 |
| /img_vm2_dd.001/vol_vol6/home/user/Downloads/ IMAGE_130.JPG | 43f7b0bff9aa8433f722912785538ea2 |
| /img_vm2_dd.001/vol_vol6/home/user/Documents/ Aeffle_und_Pferdle/IMAGE_125.JPG | 44849ef3351b81145366ff3908a1987e |
| /img_vm2_dd.001/vol_vol6/home/user/Documents/ Aeffle_und_Pferdle/IMAGE_128.JPG | 969f0f1eb4d10659f2bb35cb579e67d3 |
| /img_vm2_dd.001/vol_vol6/home/user/Documents/Die_ Maus/IMAGE_130.JPG | 43f7b0bff9aa8433f722912785538ea2 |
| /img_vm2_dd.001/vol_vol6/home/user/Documents/ Bernd_Das_Brot/IMAGE_134.JPG | dc55c4560205eb9e0bd773cd69f05774 |
| /img_vm2_dd.001/vol_vol6/home/user/Downloads/ neue_ware.tar.gz/neue_ware.tar/IMAGE_130.JPG | 43f7b0bff9aa8433f722912785538ea2 |
| /img_vm2_dd.001/vol_vol6/home/user/Downloads/ neue_ware.tar.gz/neue_ware.tar/IMAGE_128.JPG | 969f0f1eb4d10659f2bb35cb579e67d3 |

WHO ARE YOU?

Forensisches Fallbeispiel

| | |
|---|----------------------------------|
| /img_vm2_dd.001/vol_vol6/home/user/Downloads/ neue_ware.tar.gz/neue_ware.tar/IMAGE_122.JPG | e2485f5650a48af631cf79c937a741ca |
| /img_vm2_dd.001/vol_vol6/home/user/Documents/ Aeffle_und_Pferdle/IMAGE_131.JPG | ecc04f2b32e56a7fc28c2677f26fd6c6 |
| /img_vm2_dd.001/vol_vol6/home/user/Downloads/ IMAGE_127.JPG | fc08ecc7da1287bc7e824c61ec3cd3fa |
| /img_vm2_dd.001/vol_vol6/home/user/Documents/Die_ Maus/IMAGE_122.JPG | e2485f5650a48af631cf79c937a741ca |
| /img_vm2_dd.001/vol_vol6/home/user/Documents/Die_ Maus/IMAGE_133.JPG | ac311d5b2027be1e45228a7473960682 |
| /img_vm2_dd.001/vol_vol6/home/user/Downloads/ IMAGE_131.JPG | ecc04f2b32e56a7fc28c2677f26fd6c6 |
| /img_vm2_dd.001/vol_vol6/home/user/Downloads/ IMAGE_124.JPG | 2ec96ec2ddbe8699fa1e24324efbdb00 |
| /img_vm3_luks_decr.dd/home/user/Downloads/Agent_ Ranjid/MOVIE_1.mpg | 6396875c8619361cd4271f7cd7dfec3c |
| /img_vm3_luks_decr.dd/home/user/Downloads/neue_ ware.tar.gz/neue_ware.tar/IMAGE_124.JPG | 2ec96ec2ddbe8699fa1e24324efbdb00 |
| /img_vm3_luks_decr.dd/home/user/Downloads/neue_ ware.tar.gz/neue_ware.tar/IMAGE_125.JPG | 44849ef3351b81145366ff3908a1987e |
| /img_vm3_luks_decr.dd/home/user/Downloads/ Pinocchio/IMAGE_925.JPG | 44849ef3351b81145366ff3908a1987e |
| /img_vm3_luks_decr.dd/home/user/Downloads/neue_ ware.tar.gz/neue_ware.tar/IMAGE_121.JPG | 3f5f0a4b9c8d774f0242c84d1fda2577 |
| /img_vm3_luks_decr.dd/home/user/Downloads/neue_ ware.tar.gz | 4bec7618bdaebbb449485254ad0ab5c0 |
| /img_vm3_luks_decr.dd/home/user/Downloads/neue_ ware.tar.gz/neue_ware.tar/IMAGE_130.JPG | 43f7b0bff9aa8433f722912785538ea2 |
| /img_vm3_luks_decr.dd/home/user/Downloads/Paul_ Panzer/MOVIE_1.mpg | 6396875c8619361cd4271f7cd7dfec3c |
| /img_vm3_luks_decr.dd/home/user/Downloads/Agent_ Ranjid/MOVIE_3.mpg | 8af5a5e8a2190a7be1a0b072544bcd9f |
| /img_vm3_luks_decr.dd/home/user/Downloads/neue_ ware.tar.gz/neue_ware.tar/MOVIE_1.mpg | 6396875c8619361cd4271f7cd7dfec3c |
| /img_vm3_luks_decr.dd/home/user/Downloads/neue_ ware.tar.gz/neue_ware.tar | 800fbe34d1037e1a3d19afa9a7d8be75 |
| /img_vm3_luks_decr.dd/home/user/Downloads/neue_ ware.tar.gz/neue_ware.tar/IMAGE_129.JPG | 8977a3717bcd68dc9d4adb24c66b3f8 |

WHO ARE YOU?

Forensisches Fallbeispiel

| | |
|--|----------------------------------|
| /img_vm3_luks_decr.dd/home/user/Downloads/neue_ware.tar.gz/neue_ware.tar/IMAGE_132.JPG | 5383de1960832d5c3d356b9cc41e48b8 |
| /img_vm3_luks_decr.dd/home/user/Downloads/Paul_Panzer/MOVIE_3.mpg | 8af5a5e8a2190a7be1a0b072544bcd9 |
| /img_vm3_luks_decr.dd/home/user/Downloads/neue_ware.tar.gz/neue_ware.tar/IMAGE_135.JPG | 44f0786ba69c50db7a8f978889f7c6cf |
| /img_vm3_luks_decr.dd/home/user/Downloads/neue_ware.tar.gz/neue_ware.tar/MOVIE_2.mpg | 4b579dda2fad59d4ee983361feb70261 |
| /img_vm3_luks_decr.dd/home/user/Downloads/Pinocchio/IMAGE_926.JPG | 028905b8afffeacfb7aca2b5975fc21d |
| /img_vm3_luks_decr.dd/home/user/Downloads/neue_ware.tar.gz/neue_ware.tar/IMAGE_134.JPG | dc55c4560205eb9e0bd773cd69f05774 |
| /img_vm3_luks_decr.dd/home/user/Downloads/neue_ware.tar.gz/neue_ware.tar/IMAGE_133.JPG | ac311d5b2027be1e45228a7473960682 |
| /img_vm3_luks_decr.dd/home/user/Downloads/Agent_Ranjid/MOVIE_2.mpg | 4b579dda2fad59d4ee983361feb70261 |
| /img_vm3_luks_decr.dd/home/user/Downloads/neue_ware.tar.gz/neue_ware.tar/IMAGE_126.JPG | 028905b8afffeacfb7aca2b5975fc21d |
| /img_vm3_luks_decr.dd/home/user/Downloads/Paul_Panzer/IMAGE_134.JPG | dc55c4560205eb9e0bd773cd69f05774 |
| /img_vm3_luks_decr.dd/home/user/Downloads/neue_ware.tar.gz/neue_ware.tar/IMAGE_127.JPG | fc08ecc7da1287bc7e824c61ec3cd3fa |
| /img_vm3_luks_decr.dd/home/user/Downloads/neue_ware.tar.gz/neue_ware.tar/MOVIE_4.mpg | 4ba983ab9b083549c123c603c8d93f39 |
| /img_vm3_luks_decr.dd/home/user/Downloads/neue_ware.tar.gz/neue_ware.tar/IMAGE_131.JPG | ecc04f2b32e56a7fc28c2677f26fd6c6 |
| /img_vm3_luks_decr.dd/home/user/Downloads/Pinocchio/IMAGE_126.JPG | 028905b8afffeacfb7aca2b5975fc21d |
| /img_vm3_luks_decr.dd/home/user/Downloads/neue_ware.tar.gz/neue_ware.tar/IMAGE_128.JPG | 969f0f1eb4d10659f2bb35cb579e67d3 |
| /img_vm3_luks_decr.dd/home/user/Downloads/Paul_Panzer/MOVIE_2.mpg | 4b579dda2fad59d4ee983361feb70261 |
| /img_vm3_luks_decr.dd/home/user/Downloads/neue_ware.tar.gz/neue_ware.tar/IMAGE_122.JPG | e2485f5650a48af631cf79c937a741ca |
| /img_vm3_luks_decr.dd/home/user/Downloads/Paul_Panzer/IMAGE_135.JPG | 44f0786ba69c50db7a8f978889f7c6cf |
| /img_vm3_luks_decr.dd/home/user/Downloads/neue_ware.tar.gz/neue_ware.tar/IMAGE_123.JPG | ecdfc5ee600db53b4fd6f63bba296dfb |

WHO ARE YOU?

Forensisches Fallbeispiel

```
/img_vm3_luks_decr.dd/home/user/Downloads/Agent_ 4ba983ab9b083549c123c603c8d93f39
Ranjid/MOVIE_4.mpg
/img_vm3_luks_decr.dd/home/user/Downloads/neue_ 8af5a5e8a2190a7be1a0b072544bcd9
ware.tar.gz/neue_ware.tar/MOVIE_3.mpg
```

Tabelle A.1.: Mediendateien Gesamt

| File Path | Modified Time | Accessed Time | Created Time |
|---|---------------------|---------------|---------------------|
| /img_stick1.dd/vol_vol4/ IMAGE_121.JPG | 2016-07-18 12:07:14 | 2016-07-29 | 2016-07-24 11:29:42 |
| /img_stick1.dd/vol_vol4/ IMAGE_122.JPG | 2016-07-18 12:07:16 | 2016-07-29 | 2016-07-24 11:29:43 |
| /img_stick1.dd/vol_vol4/ IMAGE_123.JPG | 2016-07-18 12:07:18 | 2016-07-29 | 2016-07-24 11:29:42 |
| /img_stick1.dd/vol_vol4/ IMAGE_124.JPG | 2016-07-18 12:07:18 | 2016-07-29 | 2016-07-24 11:29:42 |
| /img_stick1.dd/vol_vol4/ IMAGE_125.JPG | 2016-07-18 12:07:20 | 2016-07-29 | 2016-07-24 11:29:42 |
| /img_stick1.dd/vol_vol4/ IMAGE_126.JPG | 2016-07-18 12:07:22 | 2016-07-29 | 2016-07-24 11:29:42 |
| /img_stick1.dd/vol_vol4/ IMAGE_127.JPG | 2016-07-18 12:07:24 | 2016-07-29 | 2016-07-24 11:29:42 |
| /img_stick1.dd/vol_vol4/ IMAGE_128.JPG | 2016-07-18 12:07:26 | 2016-07-29 | 2016-07-24 11:29:42 |
| /img_Stick2.dd/vol_vol4/ IMAGE_134.JPG | 2016-07-18 12:07:32 | 2016-07-29 | 2016-07-24 11:30:18 |
| /img_Stick2.dd/vol_vol4/ IMAGE_135.JPG | 2016-07-18 12:07:32 | 2016-07-29 | 2016-07-24 11:30:18 |
| /img_Stick2.dd/vol_vol4/ MOVIE_1.mpg | 2016-07-18 12:25:00 | 2016-07-29 | 2016-07-24 11:30:29 |
| /img_Stick2.dd/vol_vol4/ MOVIE_2.mpg | 2016-07-18 12:24:44 | 2016-07-29 | 2016-07-24 11:30:30 |
| /img_Stick2.dd/vol_vol4/ MOVIE_3.mpg | 2016-07-18 12:25:54 | 2016-07-29 | 2016-07-24 11:30:30 |
| /img_Stick2.dd/vol_vol4/ MOVIE_4.mpg | 2016-07-18 12:28:34 | 2016-07-29 | 2016-07-24 11:30:32 |
| /img_Stick3.dd/IMAGE_ 129.JPG | 2016-07-18 12:07:26 | 2016-07-29 | 2016-07-24 11:30:03 |

| | | | |
|---|---------------------|------------|---------------------|
| /img_Stick3.dd/IMAGE_130.JPG | 2016-07-18 12:07:28 | 2016-07-29 | 2016-07-24 11:30:04 |
| /img_Stick3.dd/IMAGE_131.JPG | 2016-07-18 12:07:28 | 2016-07-29 | 2016-07-24 11:30:04 |
| /img_Stick3.dd/IMAGE_132.JPG | 2016-07-18 12:07:30 | 2016-07-29 | 2016-07-24 11:30:04 |
| /img_Stick3.dd/IMAGE_133.JPG | 2016-07-18 12:07:30 | 2016-07-29 | 2016-07-24 11:30:04 |
| /img_Stick4.dd/Daten/Bilder.zip | 2017-09-18 15:25:06 | 2017-09-18 | 2017-09-18 15:51:40 |
| /img_Stick4.dd/Daten/Bilder.zip/IMAGE_129.JPG | 2016-07-18 12:07:26 | 2017-09-18 | 2016-07-24 11:30:03 |
| /img_Stick4.dd/Daten/Bilder.zip/IMAGE_130.JPG | 2016-07-18 12:07:28 | 2017-09-18 | 2016-07-24 11:30:04 |
| /img_Stick4.dd/Daten/Bilder.zip/IMAGE_131.JPG | 2016-07-18 12:07:28 | 2017-09-18 | 2016-07-24 11:30:04 |
| /img_Stick4.dd/Daten/Bilder.zip/IMAGE_132.JPG | 2016-07-18 12:07:30 | 2017-09-18 | 2016-07-24 11:30:04 |
| /img_Stick4.dd/Daten/Bilder.zip/IMAGE_133.JPG | 2016-07-18 12:07:30 | 2017-09-18 | 2016-07-24 11:30:04 |

Tabelle A.2.: Mediendateien USB-Sticks Timestamps