

Projektbericht

Modul „Forensische Datenanalyse“

Der Karpfenkalender

Eingereicht am: 01.03.2022

von: Max Mustermann
geboren am 01.02.1993
in Musterstadt
Matrikelnummer 123455

von: John Doe
geboren am 06.09.1996
in Hamburg
Matrikelnummer 123456

Betreuer: Prof. Dr.-Ing. Antje Raab-Düsterhöft

Inhaltsverzeichnis

1	Aufgabenstellung	4
2	Beschreibung des Szenarios	5
3	Umsetzung des Szenarios	7
3.1	Vorbetrachtungen	7
3.2	Vorbereitung der Datenquellen	8
3.2.1	Dienstrechner der Mecklenburger Angelprofi GmbH	8
3.2.2	Nextcloud im Rechenzentrum Komet GbR	10
3.2.3	USB-Stick	13
3.2.4	Privatrechner des Tatverdächtigen	13
3.3	Durchführung des Vorfalls	14
4	Erzeugung der Images	19
4.1	PCs der betroffenen Personen	19
4.1.1	Konvertierung von QEMU-Images	19
4.1.2	Erzeugung von Images im EWF	20
4.2	USB-Stick	23
4.3	Nextcloud	26
4.4	Speicherung des Container-Snapshots	29
5	Forensisches Gutachten	31
5.1	Deckblatt	31
5.2	Auftrag und juristische Fragestellung	32
5.3	Zusammenfassung der Untersuchung	33
5.4	Untersuchungsobjekte	35
5.5	Untersuchungswerkzeuge	35
5.6	Untersuchung der Asservate	36
5.6.1	Asservat 01 – Festplattenimage des Dienstrechners	36
5.6.2	Asservat 02 – Snapshot des Nextcloud-Servers	44
5.6.3	Asservat 03 – USB-Stick	48
5.6.4	Asservat 04 – Festplattenimage des Laptops	54
6	Details zur Untersuchungstechnik	59
6.1	Festplattenimage des Dienstrechners	59
6.1.1	Nachweis einer bestehenden Verbindung zu einer Nextcloud	59

6.1.2	Löschung synchronisierter Daten	60
6.2	Snapshot des Nextcloud-Servers	62
6.2.1	Extraktion einer Datenbank aus einem Container-Snapshot . .	62
6.2.2	Einrichtung eines Containerklons aus dem Snapshot	63
6.2.3	Anmeldungsversuche	66
6.2.4	Veränderung des Datenbestands	66
6.3	USB-Stick	68
7	Zusammenfassung und Ausblick	70
7.1	Zusammenfassung	70
7.2	Ausblick	71
Anlage A	Einrichtung einer KVM mit virt-manager	73
Anlage B	Einrichtung einer KVM mit Proxmox	76
Anlage C	Verbindung des Nextcloud-Clients mit einem Server	80
Anlage D	Dateilisten der durch Guymager erzeugten Images	84
D.1	Dienstrechner des Geschädigten	84
D.2	Laptop des Tatverdächtigen	86
D.3	USB-Stick	88
Anlage E	Metadaten des LXC-Snapshots	92
Quellen		96
Bildverzeichnis		97
Tabellenverzeichnis		100
Listingverzeichnis		101
Abkürzungsverzeichnis		102
Glossar		104

1 Aufgabenstellung

Dieser Projektbericht stellt eine Prüfungsleistung im Modul „Forensische Datenanalyse“ im 2. Fachsemester des Masterstudiengangs „Angewandte Informatik“ dar. Es sollen anhand eines erdachten Vorfalls IT-forensische Methoden demonstriert werden. Folgende Schwerpunkte sind zu bearbeiten und zu präsentieren:

- Realisierung eines Vorfalls, für den mindestens zwei Geräte relevant sind, sowie eine SQL-Datenbank
- Erzeugung der Datenträger-Images für die Untersuchung
- Bearbeitung des Falls mit gängiger IT-Forensik-Software
- Erstellung eines IT-forensischen Gutachtens zum Vorfall
- technische Details der Untersuchung

Hinweis zum forensischen Gutachten

Im Allgemeinen soll das forensische Gutachten natürlich ein selbstständiges Dokument darstellen. Da die Erstellung des Gutachtens eine Teilaufgabe dieser Arbeit ist, werden alle seine Abschnitte als Unterabschnitte des Kapitels 5 in diesen Projektbericht mit einem eigenen Deckblatt eingegliedert.

2 Beschreibung des Szenarios

Disclaimer

Das folgende Szenario, alle Namen, Personen und Geschehnisse sind fiktiv. Ähnlichkeiten mit realen Personen, Orten oder Produkten sind rein zufällig und nicht beabsichtigt.

Die Mecklenburger Angelprofi GmbH mit Sitz in der Hansestadt Wismar versorgt Angler im Landkreis Nordwestmecklenburg mit dem nötigen Equipment für die Sport- und Freizeitfischerei. Das Unternehmen veröffentlicht jährlich zu Beginn der Weihnachtszeit einen „Karpfenkalender“ für das darauffolgende Jahr. Dabei handelt es sich um einen Wandkalender mit zwölf hochqualitativen fischereibezogenen Motiven und Fotomodellen aus der Region.

Am 17. Dezember 2021 sind die für den „Karpfenkalender 2022“ bestimmten Fotos öffentlich zugänglich in voller Druckqualität im Internet aufgetaucht, sodass eine unautorisierte Anfertigung und Vervielfältigung des Kalenders durch Dritte möglich ist. Die Fotos seien außerdem aus dem Cloudspeicher der Firma entfernt worden. Den Hinweis über das Auftauchen der Bilder im Netz erhielt das Unternehmen von einem anonymen Stammkunden per Telefon am 18. Dezember 2021 gegen 15:45 Uhr. Daraufhin kontaktierte der Geschäftsführer, Jörg Klabauter-Mann, die Polizeiinspektion Wismar und erstattete Anzeige. Nach Aussagen des Geschäftsführers rechnet das Unternehmen mit hohen finanziellen Einbußen für Q4 2021 beziehungsweise Q1 2022, da in den Wintermonaten seltener Fischereiausrüstung verkauft wird als im Rest des Jahres und der Kalender besonders unter Angelenthusiasten ein beliebtes Weihnachtsgeschenk darstellt.

Tatverdächtiger ist der 26-jährige Phillip Jansen, der zum Zeitpunkt des Vorfalls Angestellter in der Mecklenburger Angelprofi GmbH war. Eine Kündigung seines Beschäftigungsverhältnisses zum 1. Januar 2022 lag bereits vor. Zum Kündigungsgrund wollten sich weder Jansen noch sein Vorgesetzter äußern. Jansen wird vorgeworfen, zwischen dem 13. und 18. Dezember 2021 unbefugt das Büro des Geschäftsführers betreten, Kopien der Fotos aus dem Cloudspeicher gemacht, sie gelöscht und anschließend auf der Image-Sharing-Plattform *Imgur* verbreitet zu haben. Damit liege sowohl ein Gesetzesverstoß gemäß § 202a (Ausspähen von Daten), Strafgesetzbuch (StGB), als auch § 106 (Unerlaubte Verwertung urheberrechtlich geschützter Werke) nach dem Urheberrechtsgesetz (UrhG) vor. Mitarbeiter des Fischbrötchenkutters „Backfisch Maike“ bezeugten, dass sich Herr Klabauter-Mann zum Tatzeitpunkt am Stadthafen befand.

Das Unternehmen mietet für die sichere Speicherung wichtiger firmeninterner Dokumente, darunter auch die Fotos für den Kalender, einen Cloudspeicher beim regionalen IT-Dienstleister Komet GbR, Inh. Claus Stoertebéker. Dabei handelt es sich um eine Instanz der Cloud-Software Nextcloud auf einem virtuellen Server (vServer). Auf den Speicher kann über ein passwortgeschütztes Web-Portal oder die direkte Kopplung mit einem Dienstrechner über eine spezielle Software zugegriffen werden. Aufgrund der Sensibilität der dort gespeicherten Dokumente verfügt nur der Geschäftsführer über die Zugangsdaten.

Im Rahmen der Ermittlungen wurden der Desktop PC (Dienstrechner) von Herrn Klabauter-Mann sowie ein Laptop PC und ein USB-Stick (Privatbesitz) von Herrn Jansen beschlagnahmt. Ebenfalls gelang es der Polizei, in Kooperation mit dem Rechenzentrum der Komet GbR, eine Kopie des vServers des Geschädigten zu beschaffen.

Die Staatsanwaltschaft übergibt nun die beschlagnahmten Speichermedien an das Dezernat 5 des Kriminalamtes Friedenshof zur IT-forensischen Untersuchung.

3 Umsetzung des Szenarios

In diesem Kapitel wird die Umsetzung des Szenarios beschrieben. Zuerst wird in Abschnitt 3.1 der Vorfall an sich grob skizziert. Abschnitt 3.2 schildert, wie die für den Vorfall relevanten Datenquellen vorbereitet bzw. präpariert wurden. In Abschnitt 3.3 werden anschließend die Schritte genannt, die für den Vorfall und die in den Kapiteln 5 und 6 zu untersuchenden Daten von Bedeutung sind.

3.1 Vorbetrachtungen

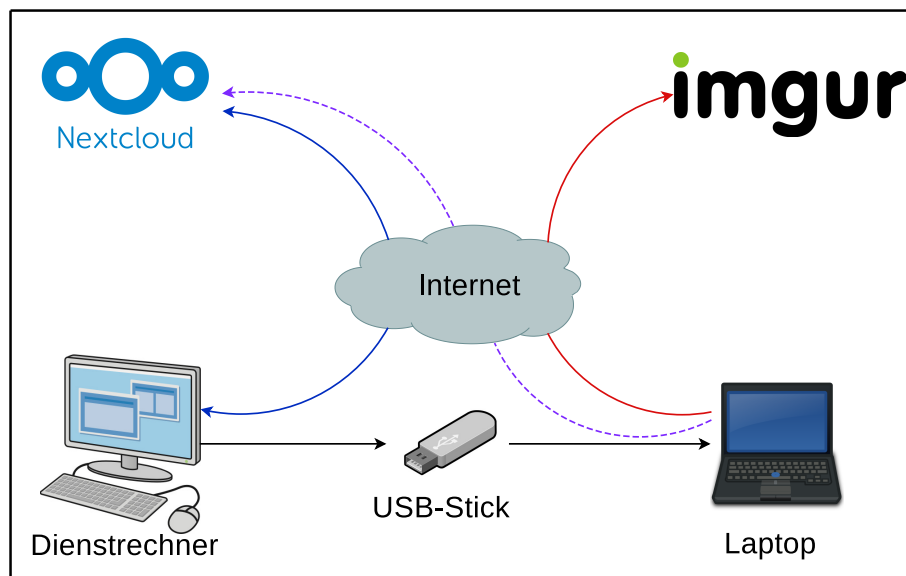


Bild 1: Schematische Beziehung zwischen den Geräten bezüglich des Vorfalls

Das Szenario umfasst vier Geräte:

1. den Dienstrechner der „Mecklenburger Angelpflicht GmbH“,
2. die Nextcloud derselben,
3. den Privatrechner des TV sowie
4. den USB-Stick, den er für den Datentransport nutzt.

Die gestohlenen Daten liegen anfänglich in einem Verzeichnis im Cloudspeicher der Firma, der mit dem Dienstrechner über eine Client-Software verbunden ist. Der TV soll zuerst versuchen, die Daten über das Webinterface der Cloud abzurufen, woran er allerdings aufgrund des mangelnden Passworts scheitern wird. In einem zweiten

Versuch verschafft er sich Zugang zum Dienstrechner (welcher nicht gesperrt ist) und kann somit auf die Cloud zugreifen. Er kopiert die nun zugänglichen Daten auf einen eigenen USB-Stick, löscht sie vom Dienstrechner und aufgrund der Synchronisation auch aus der Cloud. Anschließend kopiert er die Daten vom USB-Stick auf seinen Privatrechner, von dem aus er die Bilder auf der Image-Sharing-Plattform *Imgur*¹ veröffentlicht. In Bild 1 ist die Beziehung der Geräte untereinander schematisch dargestellt.

3.2 Vorbereitung der Datenquellen

Das Szenario wurde, mit Ausnahme des USB-Datenträgers, komplett virtualisiert durchgeführt. In diesem Abschnitt werden die verwendeten Virtualisierungstechniken und ihre Anwendung zur Vorbereitung des Vorfalls beschrieben.

3.2.1 Dienstrechner der Mecklenburger Angelprofi GmbH

Als Dienstrechner wurde eine virtuelle Maschine mit dem Betriebssystem „Windows 10“ eingerichtet. Die Schritte zur Einrichtung der VM sind in Anhang A abgebildet. Damit die VM die Internetverbindung ihres Hypervisors nutzen kann, muss zusätzlich ein virtuelles Netzwerk (Bild 2) einrichtet und aktiv sein.

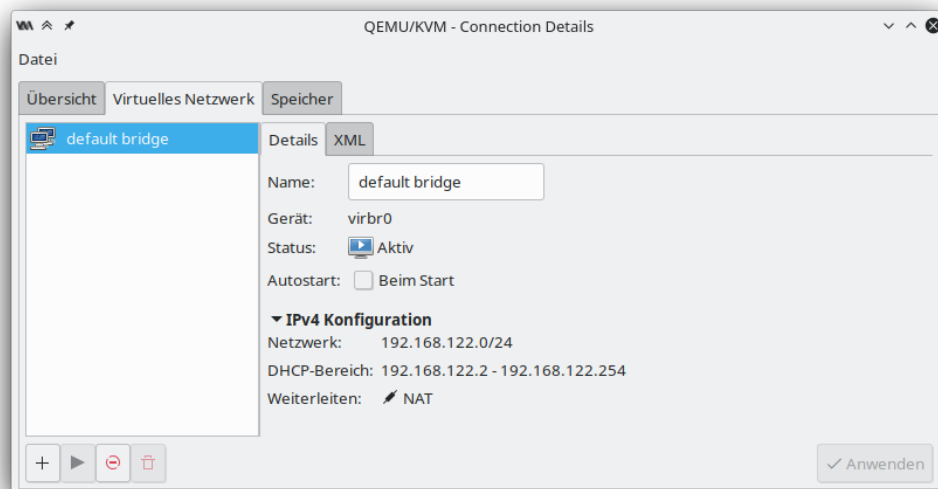


Bild 2: Virtuelles Netzwerk im virt-manager

¹<https://imgur.com/>

Für die Verwaltung der VM wurde der **virt-manager**² verwendet. Dieses Programm ist eine grafische Benutzerschnittstelle für **libvirt**, mit der unter anderem virtuelle Maschinen unter Einsatz von KVM erzeugt werden können. Bild 3 zeigt den virtualisierten Dienstrechner in der Hauptansicht des **virt-managers**.

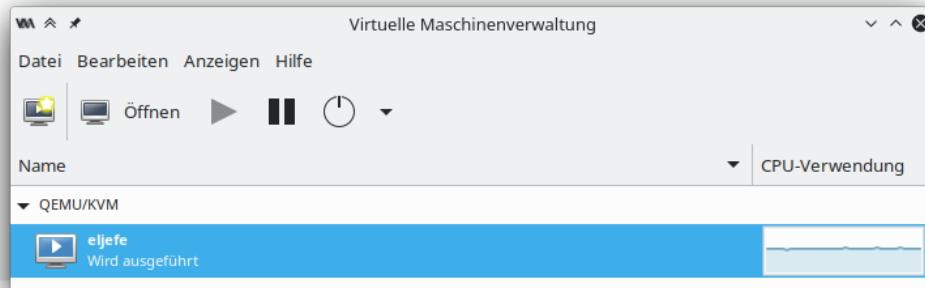


Bild 3: Hauptansicht des **virt-managers** mit laufender VM

Nach Erstellung der VM wurde die Verbindung mit dem Nextcloud-Server eingerichtet. Dazu wurde zuerst die Installationsdatei für den Nextcloud Desktop Client³ heruntergeladen, gestartet und dem Installationsassistenten gefolgt. Als nächstes musste die Verbindung zur Cloud (Abschnitt 3.2.2) hergestellt werden. Die dafür durchgeführten Schritte sind in Anhang C aufgeführt. In Bild 4 ist der geöffnete Desktop der VM zu sehen.

²<https://virt-manager.org/>

³<https://nextcloud.com/install/#install-clients>

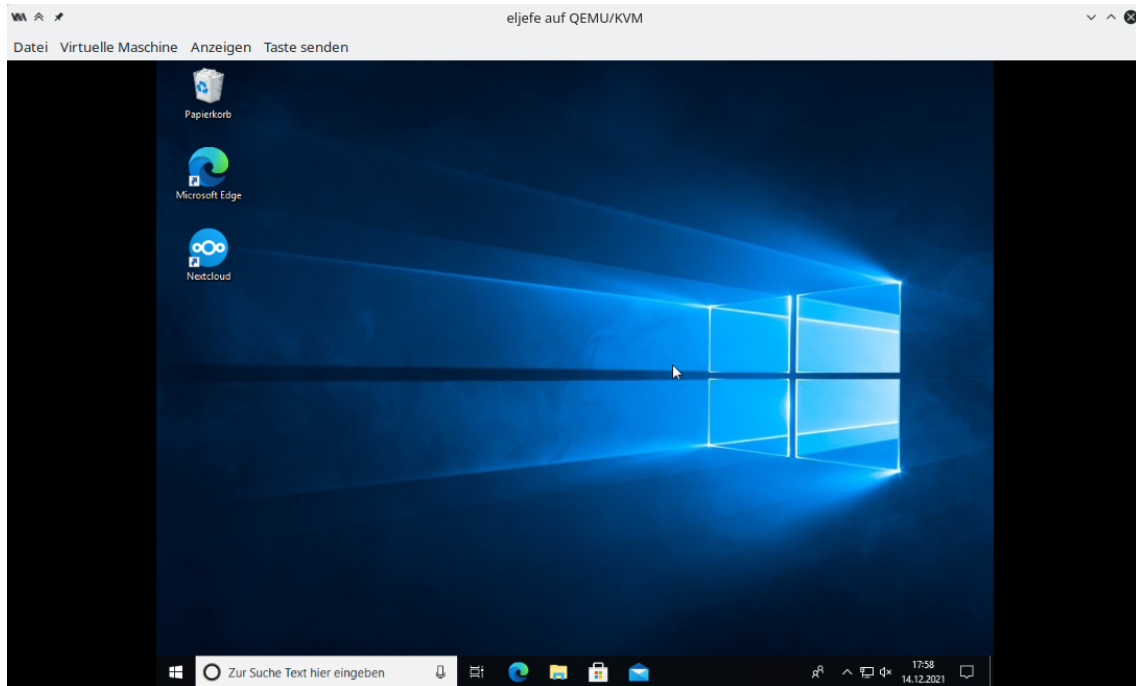


Bild 4: Virtualisierter Desktop des Dienstrechners

Unter dem Systempfad `C:/Users/el jefe/Nextcloud` befindet sich nun der Ordner, dessen Inhalte mit denen des Nextcloud-Servers abgeglichen werden, sobald eine Änderung am Datenbestand entdeckt wird.

3.2.2 Nextcloud im Rechenzentrum Komet GbR

Zur Realisierung der Nextcloud-Umgebung wurde Proxmox VE verwendet. Proxmox VE ist eine Open-Source-Virtualisierungsplattform zur Verwaltung virtueller Maschinen und Container auf Basis des Betriebssystems Debian und den Virtualisierungstechniken KVM und LXC. LXC-Container zeichnen sich dadurch aus, dass sie lediglich aus einem Dateisystem und Prozessen bestehen, die durch Kernelfunktionen vom Rest des Betriebssystems isoliert werden. Dies hat zur Folge, dass Container sehr leicht zu portieren sind. Proxmox VE ist eine der marktführenden Virtualisierungsplattformen und wurde deshalb auch für das Rechenzentrum der fiktiven Komet GbR genutzt.

Die Nextcloud-Instanz für das Szenario wurde in einem auf Debian basierenden LXC-Container betrieben und nach der empfohlenen Installation für GNU/Linux-Systeme der Entwickler entworfen [1]. Diese beinhaltet:

1. Webserver Apache2 zur Auslieferung der Inhalte

2. Datenbankplattform MariaDB (abgesichert über `mysql_secure_installation`)
3. PHP für den Betrieb des Nextcloud-Servers.

Die Nextcloud-Umgebung wurde mithilfe des Apache2 in der Version 2.4.52 sowie PHP in der Version 8.0 und dessen Modulen betrieben. Diese wurden direkt über die Debian-Paketverwaltung bezogen, verfügten deshalb über die aktuellen Sicherheitsupdates.

Die Daten der Nextcloud liegen im Systempfad `/var/www/nextcloud` und werden über den Webserver Apache2 ausgeliefert. Zusätzlich wurde der Webserver so konfiguriert, dass dieser nur auf Anfragen über den Port 80 hört und ausschließlich über diesen kommuniziert. Apache2 arbeitet dabei unter dem System-Nutzer `www-data`. Dieser hat Zugriff auf alle Daten der Nextcloud, kann aber ansonsten nicht auf Daten außerhalb von `/var/www/nextcloud` zugreifen. Um die Nutzung der Nextcloud-Umgebung zu vereinfachen, wurde für Apache2 die Funktion *pretty URLs* aktiviert. Diese überschreibt die tatsächliche URL der aktuellen Seite mit einer leichter lesbaren Adresse. So wird aus `https://fda.stoertebeker.dev/nextcloud/index.php` die URL `https://fda.stoertebeker.dev`.

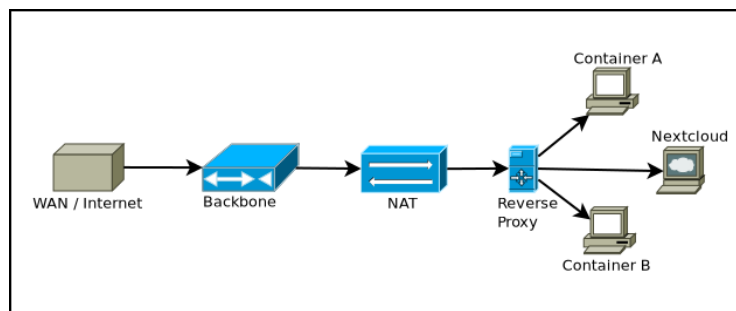


Bild 5: Netzwerkdiagramm des Rechenzentrums

Als Datenbankplattform für das Backend der Cloud wurde MariaDB verwendet. Abgesichert wurde die Datenbank mit dem von MariaDB bereitgestellten Skript `mysql_secure_installation`. Dieses Skript setzt gängige Sicherheitskonfigurationen für neu angelegte Datenbanken um, um diese schnell und einfach abzusichern [2]. Darunter zählen:

1. Passwort für den Admin-Nutzer
2. Deaktivierung anonymer Nutzer
3. Löschen der Beispieldatenbank

Die Auslieferung der Inhalte in das Internet wird über einen Reverse-Proxy geregelt. Der Reverse-Proxy wurde mithilfe der *request rerouting* Funktion des Web-servers Nginx umgesetzt. Dieser hat zwei Funktionen: Grundlegend übernimmt er die gesamte Kommunikation zwischen externen und internen Clients, die über die Ports 80 und 443 kommunizieren wollen. Alle Anfragen, die auf diesen Ports gestellt werden, werden immer zuerst an den Reverse-Proxy umgeleitet. Der Reverse-Proxy wird netzintern unter der IP-Adresse 192.168.1.11 betrieben. Innerhalb des Proxy-servers ist fest konfiguriert, welche Domainanfrage unter welchem Port an welchen internen Server und Port weitergeleitet werden soll. Im Falle der Nextcloud lautet die Domain `fda.stoertebeker.dev`. Hierbei zeigt allerdings der Nameserver-Eintrag der Domain auf die IP-Adresse des Reverse-Proxy, welcher so konfiguriert ist, dass er alle Anfragen der Domain `fda.stoertebeker.dev` unter den Ports 80 und 443 an die interne Adresse der Nextcloud-Umgebung auf den Port 80 weiterleitet. Somit wird erreicht, dass nur ein Host über Internet erreichbar ist, hinter dem sich jedoch viele weitere Server verbergen; ebenso kommuniziert die Nextcloud nur mit dem Reverse-Proxy und nie mit einem externen Client.

Die zweite Funktion des Reverse-Proxy ist die Absicherung der Kommunikation. Hierbei wird die interne Kommunikation immer als sicher angesehen und deshalb nur über HTTP kommuniziert. Dies erleichtert die Konfiguration der internen Clients erheblich. Dabei ist der Proxyserver so konfiguriert, dass alle Anfragen von außen an den Port 80 als Anfragen auf dem Port 443 angesehen werden, eine Kommunikation über HTTP deshalb unmöglich ist und immer HTTPS erzwungen wird. Die Kommunikation über HTTPS wird mithilfe von speziell ausgestellten Zertifikaten abgesichert. Die Zertifikate müssen vom Webserver selbst ausgeliefert werden. Zur Generierung der Zertifikate wurde die Zertifizierungsstelle „Let’s Encrypt“⁴ verwendet. Diese Zertifizierungsstelle stellt kostenfreie, aber gleichzeitig vertrauenswürdige SSL-Zertifikate aus, welche drei Monate gültig sind. Der Reverse-Proxy übernimmt die Funktion der regelmäßigen Aktualisierung der Zertifikate, sodass den einzelnen Servern im Netz die Aufgabe der Kommunikationsabsicherung abgenommen wird.

Die Konfiguration des Nextcloud-Servers wird in der Datei `nextcloud.conf` umgesetzt. Damit die Cloud auf die definierte Domain korrekt reagiert, muss diese noch in die Liste der „trusted domains“ aufgenommen werden. Nextcloud reagiert nur auf Anfragen, die als Ziel diese Adressen beinhalten. So wird beispielsweise das Aufrufen der Cloud über die IP-Adresse des Containers verhindert, was das Angriffsrisiko minimiert.

⁴<https://letsencrypt.org/>

Es ist zu beachten, dass standardmäßig nur eine Minimalinstallation von Nextcloud bereitgestellt wird. Es werden keinerlei zusätzliche Pakete oder Sicherheitskonfigurationen mitgeliefert.

3.2.3 USB-Stick

Der Täter verwendet einen 128 MB USB-Speicherstick, um die gestohlenen Daten vom Dienstrechner des Geschädigten auf seinen eigenen zu übertragen und sie letztendlich im Internet zu veröffentlichen. Der USB-Stick der Marke *Hama* wurde wie in Listing 1 in Vorbereitung auf das Szenario vollständig mit Zufallsdaten überschrieben, um Datenartefakte aus vorheriger Nutzung zu vermeiden, und danach als FAT32-Dateisystem mit der Bezeichnung „FLASHPEN128“ formatiert:

```
$ dd if=/dev/urandom of=/dev/sde          # /dev/sde ist der USB-Stick  
$ mkdosfs -F 32 -n "FLASHPEN128" -I /dev/sde # Alias für mkfs.vfat ...
```

Listing 1: Formatierung des USB-Sticks

3.2.4 Privatrechner des Tatverdächtigen

Auf dem Privatrechner des TV ist das Betriebssystem Windows 10 mit den zur Zeit der Durchführung aktuellen Patches installiert. Der Rechner verfügt über eine Internetanbindung und wurde durch eine auf KVM-basierende VM in Proxmox VE erzeugt. Die Schritte zur Einrichtung dieser VM sind im Anhang B genauer dokumentiert. Auf dem System befindet sich der Webbrowser Firefox, über welchen auf das Internet zugegriffen wird. Zusätzlich besitzt diese VM eine USB-Schnittstelle, welche für externe Geräte genutzt werden kann.

Es gilt zu beachten, dass sich der Privatrechner und der Nextcloud-Server für dieses Szenario auf demselben Virtualisierungsserver befinden. Das bedeutet, dass sich „Angreifer“ und „Opfer“ im gleichen Netzwerk befinden und in den Log-Dateien beider Systeme nur lokale IP-Adressen auftreten.

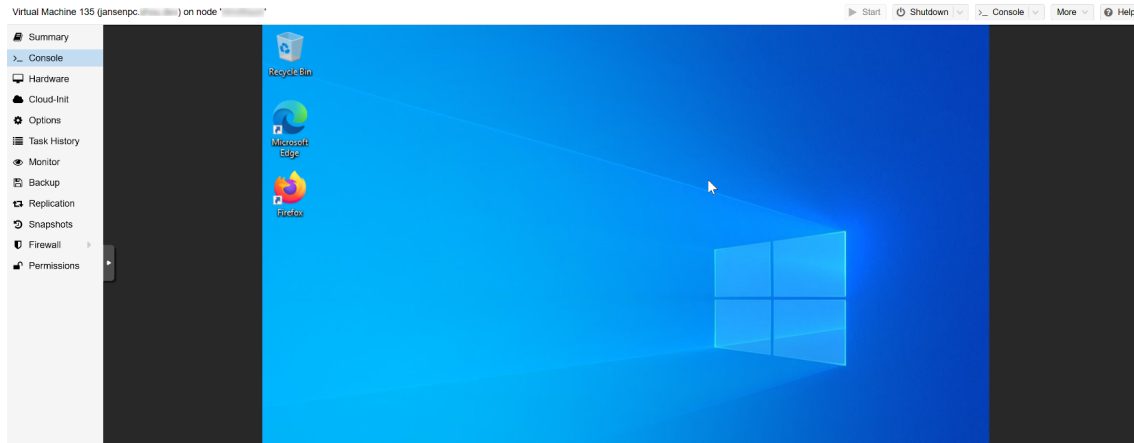


Bild 6: Virtualisierter Desktop des Privatrechners

3.3 Durchführung des Vorfalles

Hinweis zu verwendetem Bildmaterial

Innerhalb dieser Arbeit wurde ggf. urheberrechtlich geschütztes Bildmaterial unklaren Ursprungs verwendet. Diese Inhalte dienen ausschließlich zu Bildungszwecken im Rahmen dieses Projekts und sind nicht für die Vervielfältigung gedacht.

Zuerst mussten die relevanten Bilddateien in die Cloud übertragen werden. Das Verzeichnis mit den Bilddateien für den Kalender wurde der Einfachheit halber vom Hypervisor aus über das Webinterface hochgeladen (Bild 7), da auf diese Weise kein Dateiaustausch zwischen der VM und ihrem Hypervisor eingerichtet werden musste. Somit befanden sich nun die relevanten Dateien im Cloudspeicher, welcher mit dem Dienstrechner der fiktiven Firma synchronisiert wurde.

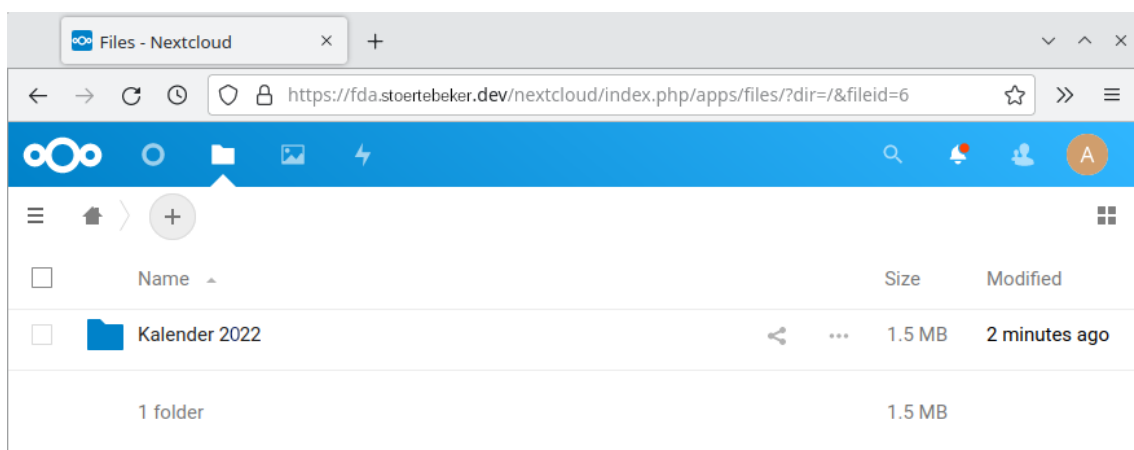


Bild 7: Hochgeladener Ordner in der Cloud

Als nächstes wurde der Eingriff des TV am Dienstrechner der Firma simuliert, beginnend mit dem Anschließen seines USB-Sticks, auf den die Bilder später übertragen werden sollen. Damit die VM auf den USB-Stick zugreifen kann, musste dieser zuerst vom Host an den virtuellen Computer durchgereicht werden. Der `virt-manager` hat eine eingebaute Funktion, über die beliebige an den Host angeschlossene Peripheriegeräte für das Gastsystem sichtbar gemacht werden können (Bild 8).

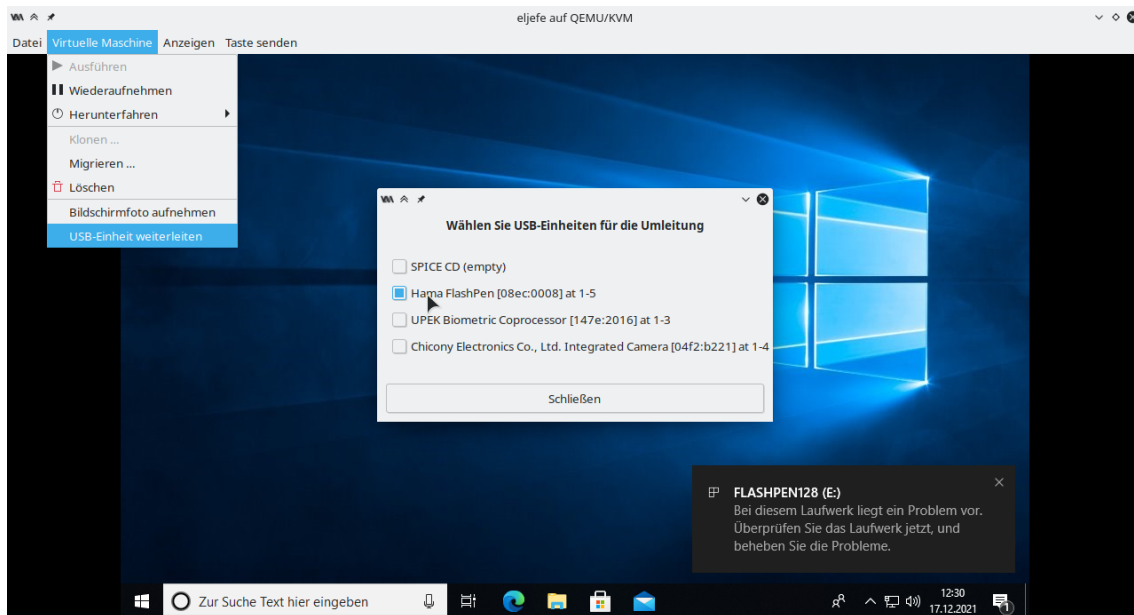


Bild 8: Durchreichen des USB-Sticks in die VM

Nachdem der USB-Stick in der VM erkannt und eingehängt wurde, konnte der Ordner „Kalender 2022“ auf den USB-Stick kopiert werden (Bild 9). Im Anschluss wurde der betroffene Ordner vom Rechner gelöscht, was durch die Synchronisation ebenfalls die Löschung in der Cloud zur Folge hatte. Der USB-Stick wurde ausgeworfen und vom System entfernt.

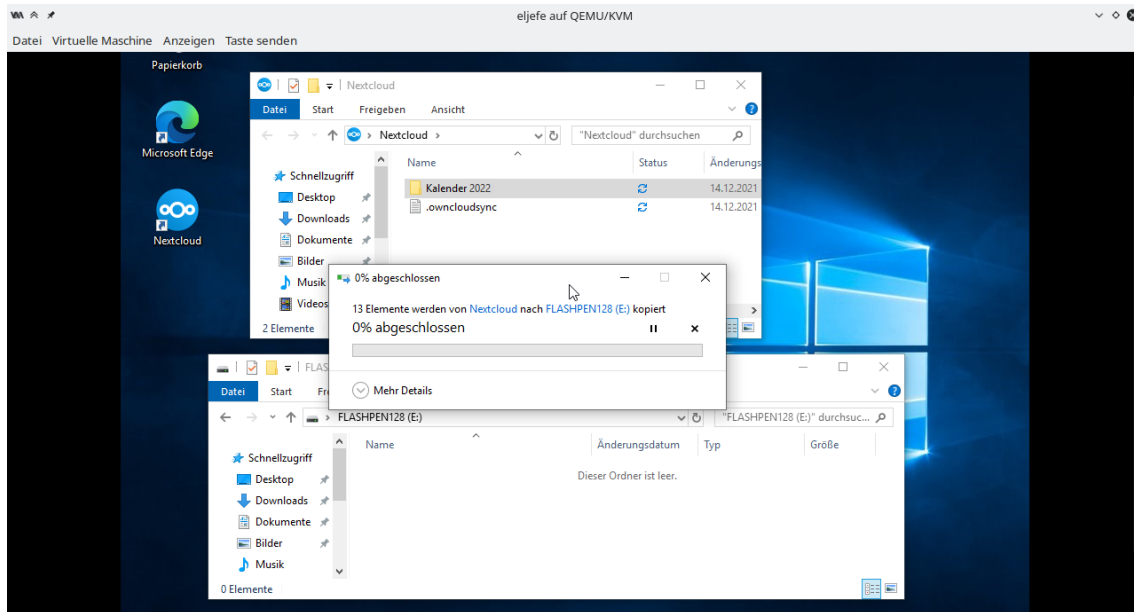


Bild 9: Daten werden auf den USB-Stick kopiert

Hinweis

Aufgrund der räumlichen Trennung der Bearbeiter dieser Aufgabe wurden für den Vorfall zwei verschiedene USB-Speichermedien verwendet. Innerhalb dieser Betrachtungen werden deshalb die Datenträger mit den Seriennummern 0E1145514041D91B und 0901B3C4FF44A-B3395C04A36911997795F91BD0B1CAE6F8078417994CBF03F2524220000000000000000-0000C2BA95F0FF8D2D2081558107312A754E als identisch betrachtet.

Nachdem die Dateien auf den USB-Stick übertragen wurden, wurde dieser mit dem Rechner des TV verbunden. Wegen der Virtualisierung des Rechners musste das USB-Speichermedium auch hier an das Gastsystem durchgereicht werden. Da der Rechner des TV innerhalb einer Proxmox VE-Umgebung virtualisiert wurde, funktioniert das Durchreichen anders als im vorherigen Beispiel. Bild 10 zeigt den Prozess für die VM in Proxmox VE.

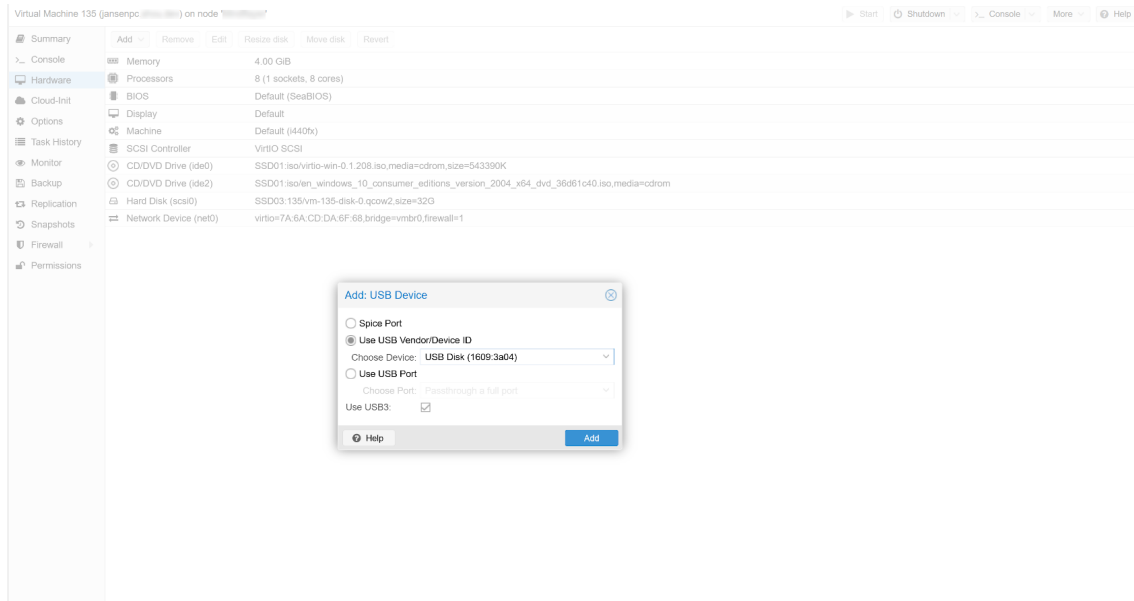


Bild 10: Durchreichen des USB-Sticks in die Maschine des TV

Nachdem das USB-Speichermedium für die VM des TV verfügbar gemacht wurde, wurden die betroffenen Daten von dem USB-Stick auf den Desktop des Rechners kopiert und die Daten anschließend vom USB-Stick gelöscht.

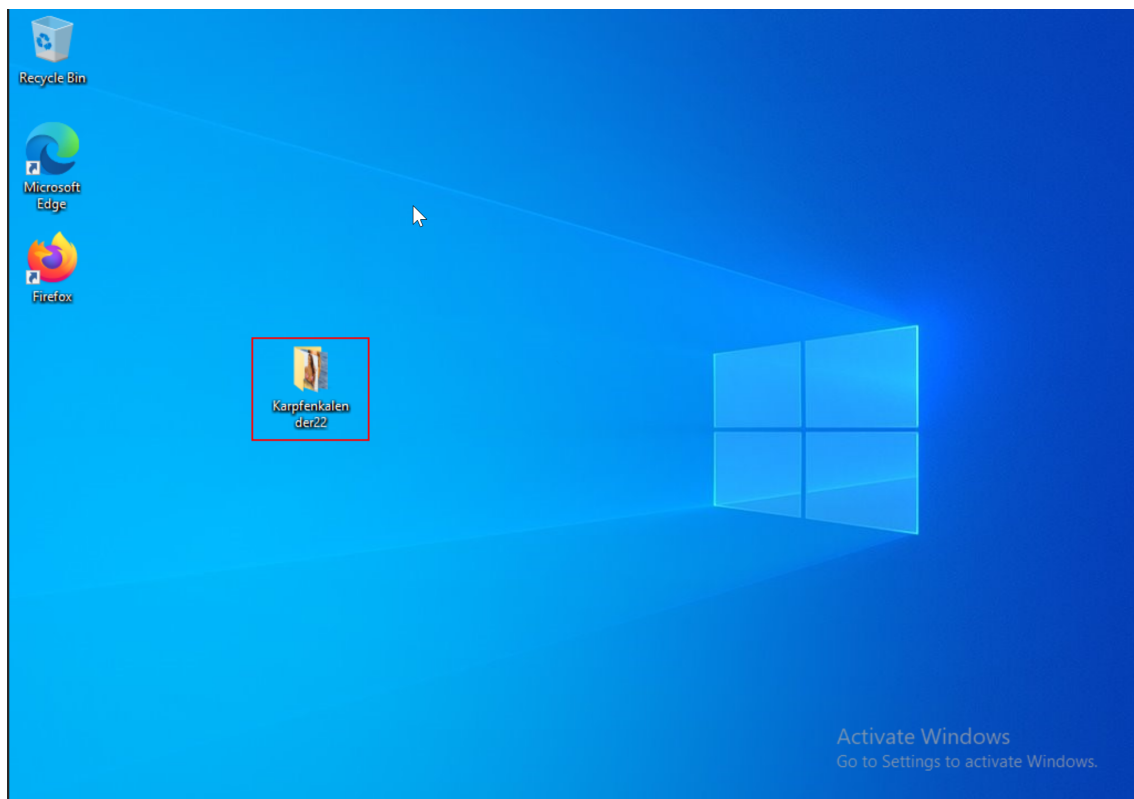


Bild 11: Relevante Dateien in der VM

Abschließend wurde das Upload-Portal der Image-Sharing-Plattform Imgur aufgerufen, um das Hochladen der Bilder zu simulieren (Bild 12). Auf ein tatsächliches Hochladen wurde an dieser Stelle verzichtet, um mögliche Urheberrechtsverletzungen zu vermeiden. Die Daten wurden als hochgeladen und die Durchführung des Vorfalls somit als abgeschlossen betrachtet.

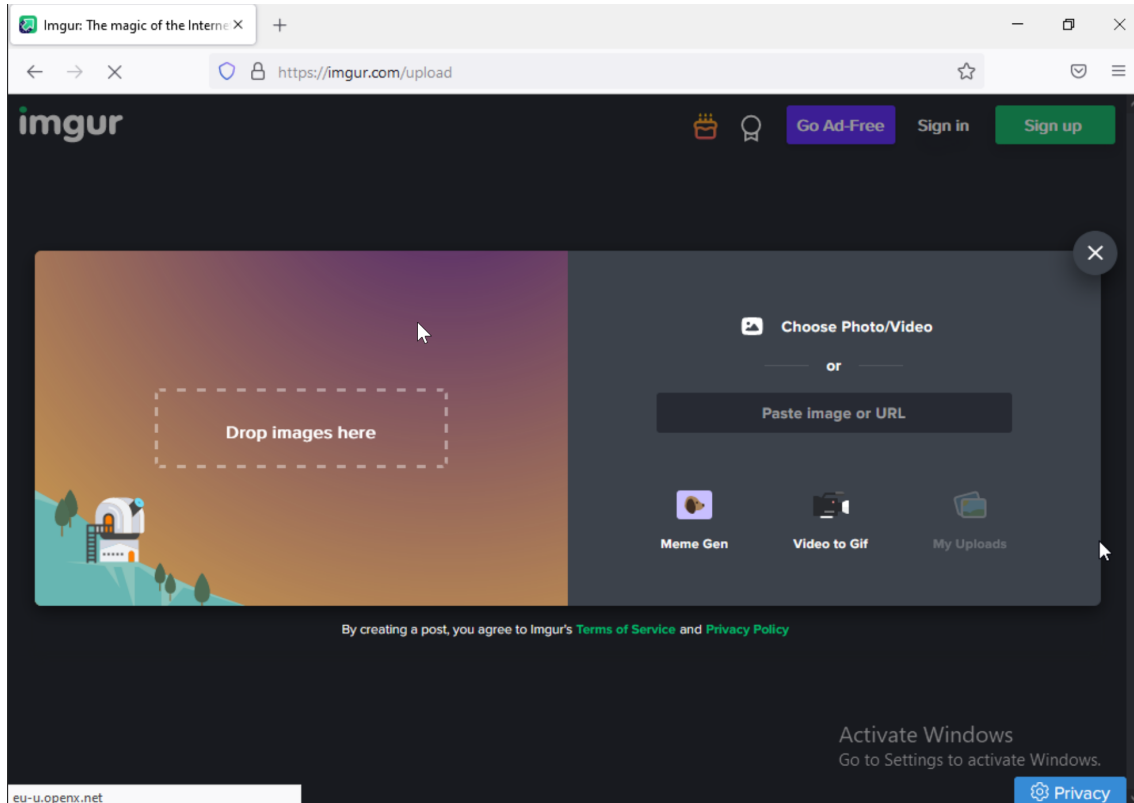


Bild 12: Upload der Dateien auf der Image-Sharing-Plattform Imgur

4 Erzeugung der Images

Um das erdachte Szenario untersuchen und auswerten zu können, mussten nach den in Abschnitt 3.3 beschriebenen Durchführungsschritten die betroffenen Datenträger gesichert, beziehungsweise unverfälschte Abbilder (Images) von ihnen zur Untersuchung erzeugt werden. In diesem Kapitel werden die Schritte zum Erzeugen der Images und die dabei eingesetzten Verfahren mit der entsprechenden Software erläutert.

Hinweis zum Realitätsbezug

Bei realen Vorfällen müssen selbstverständlich die physischen Datenträger über einen Write-Blocker angeschlossen und ausgelesen werden, beziehungsweise wendet ein Ermittler je nach Gerät unterschiedliche Extraktionsmethoden an, um das Speichermedium zu bergen oder zu sichern. Da es sich hier um ein simuliertes Szenario handelt, weicht der Umgang mit Datenträgern leicht von der Praxis ab. Es wird dennoch versucht, so realitätsnah wie möglich zu arbeiten.

4.1 PCs der betroffenen Personen

Da sowohl der Privatrechner des TV als auch der Dienstrechner des Geschädigten mit der gleichen Virtualisierungstechnik simuliert wurden, sind die Schritte zur Erzeugung der Images derer identisch.

4.1.1 Konvertierung von QEMU-Images

Beide virtuellen Maschinen wurden mit einer virtuellen Festplatte im `qcow2` Format erstellt. Dieses Format entspricht bereits einem unkomprimierten Datenstrom ähnlich zu dem eines beispielsweise mittels `dd` erzeugten Datenträgerabbildes. Auf diese Weise erzeugte virtuelle Festplatten befinden sich häufig in einem Standardverzeichnis wie `/var/lib/libvirt/images`, sofern nicht anders vom Nutzer konfiguriert. Gängige ITFS beherrscht mitunter den Umgang mit solchen Dateien. Weil die virtuellen Datenträger für das untersuchte Szenario allerdings als Images realer Festplatten behandelt werden sollen, müssen diese zuerst in ein Rohdatenformat umgewandelt werden. QEMU stellt das Kommando `qemu-img` für die Verwaltung der virtuellen Festplatten zur Verfügung. Damit kann, wie in Listing 2 dargestellt, eine

qcow2 Datei in das **raw** Format konvertiert werden. Auf diese Weise wurden auch die Rohformate der beiden relevanten virtuellen Festplatten erzeugt.

```
$ cd /var/lib/libvirt/images
$ qemu-img convert eljefe.qcow2 eljefe.raw
$ qemu-img convert sus.qcow2 sus.raw
```

Listing 2: Umwandlung von virtuellen QEMU-Festplatten in ein Rohformat

4.1.2 Erzeugung von Images im EWF

Im nächsten Schritt mussten die Rohdaten in ein Format übersetzt werden, das auch von gängiger ITFS unterstützt wird, wie zum Beispiel das Expert Witness Format (EWF). Für die Erzeugung dieser Daten wurde das freie Programm Guymager¹ genutzt. Damit können in erster Linie Images physischer Geräte in einem forensischen Datenformat erzeugt, gehasht und verifiziert werden. Das Programm ermöglicht es außerdem, Rohdatenabbilder wie einen gewöhnlichen Datenträger zu betrachten und ein Image davon anzulegen. Im Folgenden wird die Erstellung des Images für den Dienstrechner des Geschädigten beschrieben. Für den Laptop des TV ist das Vorgehen in diesem Fall identisch.

In Bild 13 ist das Hauptfenster des Guymagers zu sehen. Es werden alle Datenträger aufgelistet, die an die Forensik-Workstation zum aktuellen Zeitpunkt angeschlossen sind (auch virtuelle Laufwerke). Unter dem Menüeintrag *Devices* gibt es den Unterpunkt *Add special device*, über den ein Image aus dem Dateisystem als Datenträger eingehängt werden kann.

¹<https://guymager.sourceforge.io/>

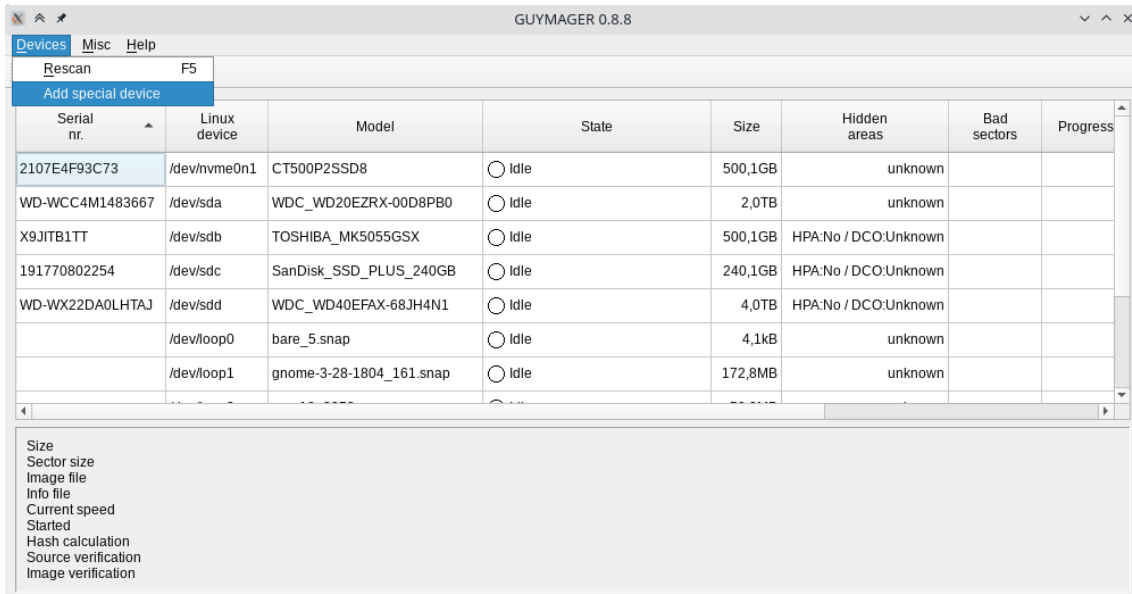


Bild 13: Einhängen eines „Spezialgeräts“ im Guymager

Anschließend wird das Datenträgerabbild als verfügbares Gerät aufgelistet, wie es in Bild 14 zu sehen ist.

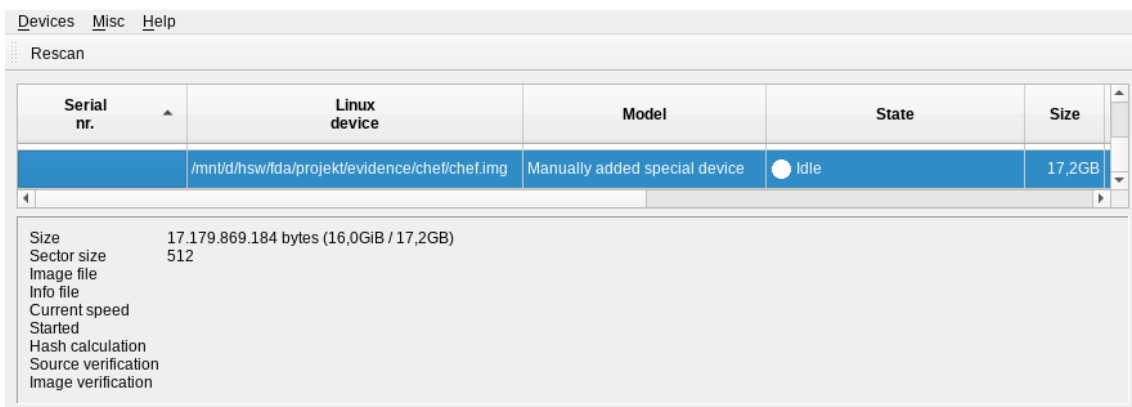


Bild 14: Datenträgerabbild in der Liste verfügbarer Geräte im Guymager

Aus dem Kontextmenü (über einen Rechtsklick auf den entsprechenden Listeneintrag hervorgerufen) wird die Aktion *Acquire image* ausgewählt. Es erscheint daraufhin ein neues Unterfenster (siehe Bild 15), in dem die Optionen für die Imageerzeugung eingestellt werden. Für dieses Szenario wurde das **EXX** Format² mit einer maximalen Größe von 2047 MiB für die Zielformate gewählt³. Neben allgemeinen Metadaten zur Untersuchung (Bearbeiter, Asservatsnummer, Zielformat etc.) wurde eingestellt,

²EXX steht hierbei für eine EWF Datei, wobei XX die Laufvariable ist, die die Reihenfolge der Image-Segmente angibt.

³Teil der Untersuchung wurde in entfernten virtuellen Maschinen durchgeführt, welche einen Datei-Upload von maximal 2 GB pro Datei erlauben.

dass für das Image MD5-, SHA-1- und SHA-256-Hashwerte erzeugt und anschließend mit den Hashwerten des Datenträgers abgeglichen werden sollen. Nach erfolgreicher Erzeugung und Verifizierung (Bild 16) befanden sich die E01 bis E04 Dateien in den Zielverzeichnissen für die untersuchten Datenträger sowie Textdateien mit Informationen über die Erzeugung (Anhang D).

File format

☐ Linux dd raw image (file extension .dd or .xxx) | ☒ Split image files

☒ Expert Witness Format, sub-format Guymager (file extension .Exx) | Split size 2047 MiB

Case number 1

Evidence number 1

Examiner John Doe

Description Festplatte aus dem Desktop-Computer des Geschädigten

Notes

Destination

Image directory ... /mnt/d/hsw/fda/projekt/evidence/chef/exx/

Image filename (without extension) chef

Info filename (without extension) chef

Hash calculation / verification

☒ Calculate MD5 ☒ Calculate SHA-1 ☒ Calculate SHA-256

☒ Re-read source after acquisition for verification (takes twice as long)

☒ Verify image after acquisition (takes twice as long)

Cancel Duplicate image... Start

Bild 15: Einstellungen für die Imageerzeugung

Devices Misc Help				
Rescan				
Serial nr.	Linux device	Model	State	Size
	/mnt/d/hsw/fda/projekt/evidence/chef/chef.img	Manually added special device	Finished - Verified & ok	17,2GB
Size 17.179.869.184 bytes (16,0GiB / 17,2GB) Sector size 512 Image file /mnt/d/hsw/fda/projekt/evidence/chef/exx/chef.Exx Info file /mnt/d/hsw/fda/projekt/evidence/chef/exx/chef.info Current speed Started 19. Januar 17:04:55 (00:05:48) Hash calculation MD5, SHA-1 and SHA-256 Source verification on Image verification on				

Bild 16: Erfolgreiche Verifizierung des Images

4.2 USB-Stick

Auch dieses Image wurde mit Guymager erzeugt. Der USB-Stick des TV ist das einzige physisch existente Asservat in diesem Szenario. Deshalb konnte der im Abschnitt 4.1.2 genannte Schritt zum Einhängen virtueller Festplatten übersprungen werden.

Der USB-Stick wurde an die Forensik-Workstation über einen USB-2-Port angeschlossen und nicht eingehängt, um die darauf gespeicherten Daten unberührt zu lassen. Danach konnte Guymager gestartet und das Image erzeugt werden. In den Bildern 17, 18 und 19 sind die Arbeitsschritte zu sehen. Die erzeugten Dateien sind in Anhang D aufgelistet.

Devices Misc Help					
Rescan					
Serial nr. ^	Linux device	Model	State	Size	Hidden areas
2107E4F93C73	/dev/nvme0n1	CT500P2SSD8	○ Idle	500,1GB	unknown
WD-WCC4M1483667	/dev/sda	WDC_WD20EZR-00D8PB0	○ Idle	2,0TB	unknown
X9JTB1TT	/dev/sdb	TOSHIBA_MK5055GSX	○ Idle	500,1GB	HPA:No / DCO:Unknown
191770802254	/dev/sdc	SanDisk_SSD_PLUS_240GB	○ Idle	240,1GB	HPA:No / DCO:Unknown
WD-WX22DA0LHTAJ	/dev/sdd	WDC_WD40EFAX-68JH4N1	○ Idle	4,0TB	HPA:No / DCO:Unknown
0E1145514041D91B	/dev/sde	Hama FlashPen	● Idle	129,0MB	unknown
	/dev/loop0	bare_5.snap	○ Idle	4,1kB	unknown
	/dev/loop1	gnome-3-28-1804_161.snap	○ Idle	172,8MB	unknown
	/dev/loop2	core18_2253.snap	○ Idle	58,2MB	unknown
	/dev/loop3	gtk-common-themes_1519.snap	○ Idle	68,4MB	unknown
	/dev/loop4	core18_2284.snap	○ Idle	58,2MB	unknown
	/dev/loop5	snapt_14295.snap	○ Idle	45,4MB	unknown
<div> <div>Size</div> <div>Sector size</div> <div>Image file</div> <div>Info file</div> <div>Current speed</div> <div>Started</div> <div>Hash calculation</div> <div>Source verification</div> <div>Image verification</div> </div> <div> 128.974.848 bytes (123MiB / 129MB) 512 </div>					

Bild 17: USB-Stick in der Guymager Geräteliste

File format

☐ Linux dd raw image (file extension .dd or .xxx)
 ☒ Split image files

☒ Expert Witness Format, sub-format Guymager (file extension .Exx)
 Split size MiB

Case number

Evidence number

Examiner

Description

Notes

Destination

Image directory

Image filename (without extension)

Info filename (without extension)

Hash calculation / verification

☒ Calculate MD5
 ☒ Calculate SHA-1
 ☒ Calculate SHA-256

☒ Re-read source after acquisition for verification (takes twice as long)

☒ Verify image after acquisition (takes twice as long)

Bild 18: Einstellungen für die Imageerzeugung des USB-Stick

Devices Misc Help				
Rescan				
Serial nr.	Linux device	Model	State	Size
0E1145514041D91B	/dev/sde	Hama FlashPen	Finished - Verified & ok	129,0MB
Size 128.974.848 bytes (123MiB / 129MB) Sector size 512 Image file /mnt/d/hsw/fda/projekt/evidence/stick/exx/stick.Exx Info file /mnt/d/hsw/fda/projekt/evidence/stick/exx/stick.info Current speed Started 19. Januar 15:20:18 (00:00:28) Hash calculation MD5, SHA-1 and SHA-256 Source verification on Image verification on				

Bild 19: Erfolgreiche Verifizierung der USB-Stick-Images

4.3 Nextcloud

Der Prozess der Vorbereitung für die forensische Analyse weicht stark aufgrund der zugrundeliegenden Technologien, im Vergleich zu Bare-Metal-Systemen oder virtuellen Maschinen, ab. Wie bereits im Kapitel 3.2.2 beschrieben besteht ein LXC-Container lediglich aus einem isolierten Prozess sowie einem isolierten Bereich innerhalb des Host-Dateisystems. Diese Architektur hat mehrere Implikationen zur Folge. Es lässt sich aus einem Container kein herkömmliches forensisches Image bilden. Es kann lediglich ein Abbild des Dateisystems erstellt werden, was einen gewissen Informationsverlust mit sich bringt. Hardware-Level-Analysesoftware wie X-Ways Forensics kann hier nur spärlich eingesetzt werden, da sich die Analyseschritte in erster Linie auf die Inhalte von existierenden Dateien beschränkt, wozu in der Regel keine Spezialsoftware nötig ist. Wurde ein Snapshot generiert, kann er auf einem anderen System direkt entpackt und auf das gesamte Dateisystem des Containers zugegriffen werden. Es kann direkt auf alle Dateien des geklonten Systems zugegriffen werden.

LXC besitzt eine native Snapshot-Funktion, die ein Abbild des aktuellen Dateisystems sowie der Containerkonfiguration, welche im TAR-Format vorliegt und dann beispielsweise in anderen LXC-Anwendungen genutzt werden kann, um diesen Container wiederherzustellen. Des Weiteren kann das Archiv komprimiert werden, beispielsweise mit dem GZ- oder Zstandard (ZSTD) Algorithmus. Dieses Archiv beinhaltet ein vollständiges Abbild des Containers und kann daher für die forensische Analyse herangezogen werden. Diese Snapshot-Funktion ist in die Management-Oberfläche von Proxmox VE integriert.

Die Technik des Container-Snapshots impliziert, dass keine tiefgehende forensische Analyse von Datenartefakten durchgeführt werden kann. Durch das Kopieren des Dateisystems im Snapshot-Prozess werden eventuelle Fragmente von gelöschten Dateien nicht berücksichtigt. Es existieren Techniken, um dies trotzdem zu ermöglichen, zum Beispiel das Nutzen von speziellen Dateisystemen, allerdings müssen diese explizit im Voraus eingerichtet werden.

Theoretisch ist es auch möglich, den gesamten Hypervisor oder den zentralen Speicher (falls die virtuellen Maschinen nicht lokal gelagert werden) zu klonen, um eine exakte Kopie des Dateisystems zu erhalten. Ein solches Vorgehen ist allerdings nicht zu empfehlen, weil dies Downtime von nicht beteiligten Systemen bedeuten könnten, was wiederum zu finanziellen Einbußen bei Betreiber und Kunden führen kann.

Zuzüglich werden eventuell Daten von Kunden erhoben, welche nicht im Zusammenhang mit der Untersuchung stehen und somit nicht erhoben werden dürfen.

Zur Generierung des Snapshots wurde die in Proxmox VE eingebaute Snapshot-Funktion verwendet (Bild 20). Diese ist über das *Snapshot*-Menü erreichbar und kann ausgeführt werden, ohne die Verfügbarkeit des Containers zu beeinträchtigen. Abgelegt wird das gepackte Archiv im Anschluss in ein zentrales Snapshot-Verzeichnis. Beim Start der Snapshot-Funktion wird grundsätzlich ein Ziel für diesen ausgewählt (Bild 21). Die möglichen Ziele der Snapshots müssen vorab innerhalb von Proxmox VE definiert werden. Diese Pfade entsprechen grundsätzlich der Struktur `SPEICHERMEDIUM/dump/Snapshot.tar.gz` oder `snapshot.vma.gz`. Hierbei ist es nicht von Bedeutung, ob es sich um einen Container oder um eine vollwertige VM handelt. Innerhalb des Snapshot-Prozesses wird die Integritätsprüfung durchgeführt, um zu gewährleisten, dass ein originalgetreues Abbild erstellt wird.

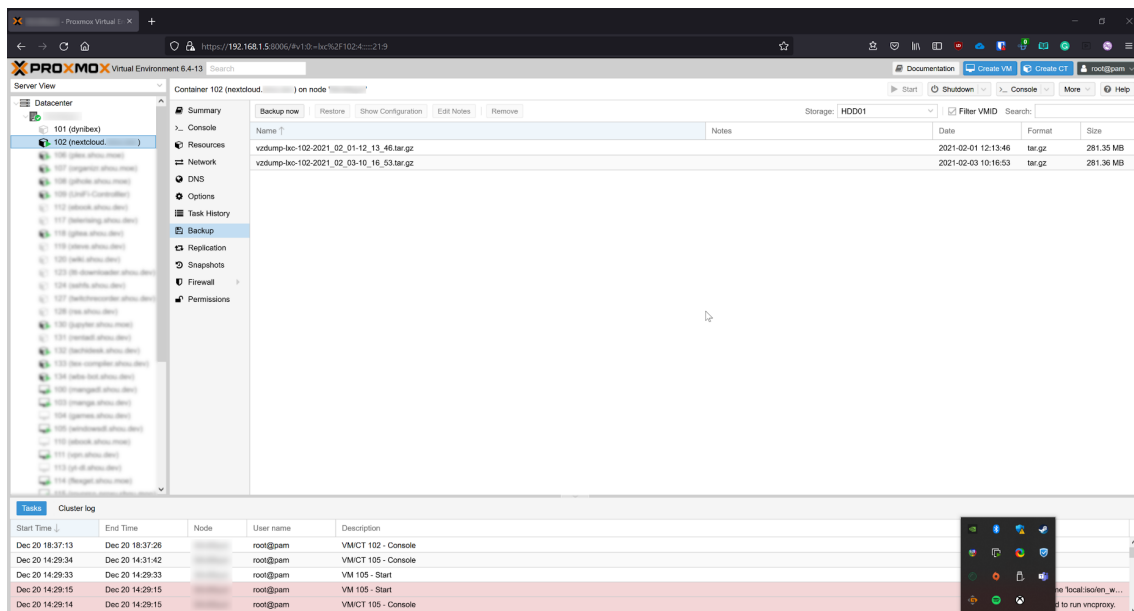


Bild 20: Starten der Snapshot-Erstellung über den Backup-Reiter in Proxmox

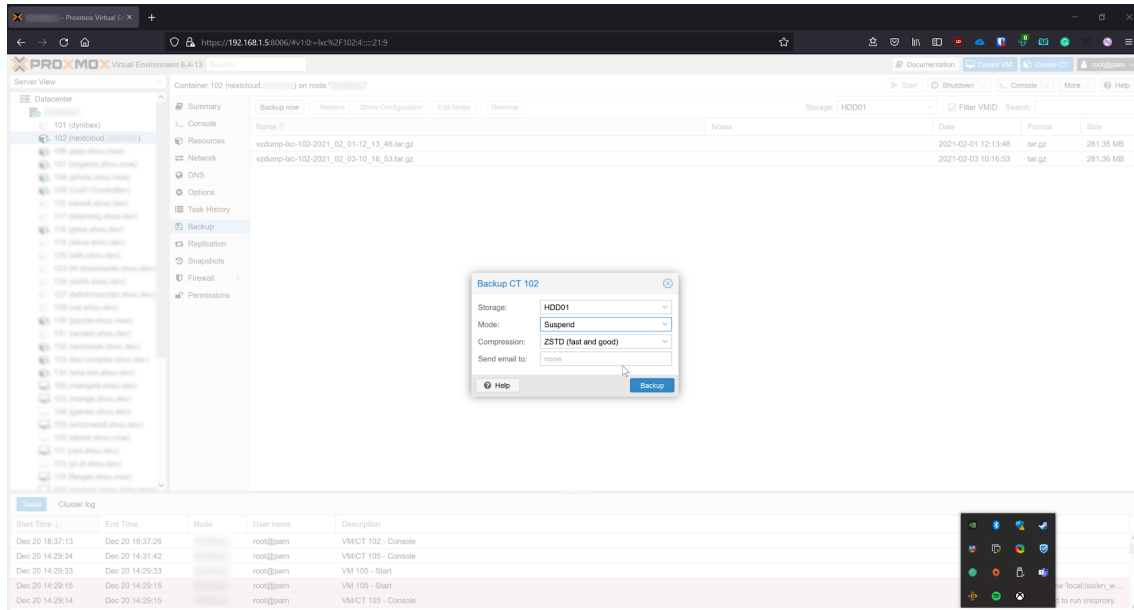


Bild 21: Auswahl des Zielspeichers und der Kompressionsart

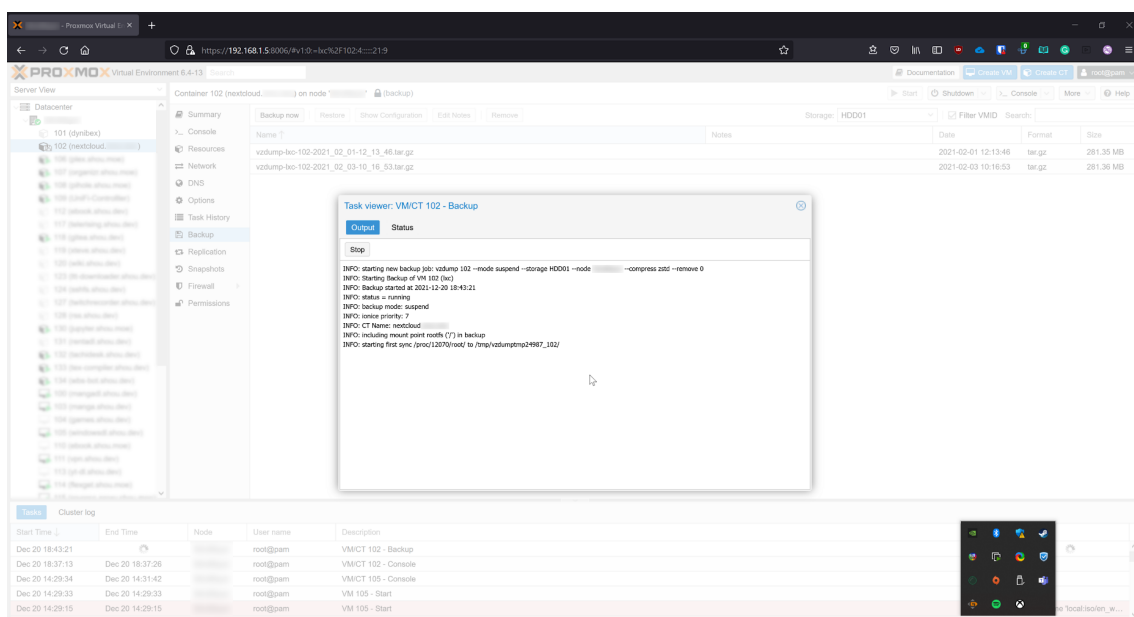


Bild 22: Log-Ausgabe während der Snapshot-Erstellung (1)

Ein Snapshot kann theoretisch auch manuell erstellt werden. Dies ist möglich, indem die virtuelle Festplatte, die im Rohdatenformat unter `SPEICHERMEDIUM/image/containerid/vm-containerid-disk0.raw` abgelegt ist, dupliziert wird. Diese virtuelle Festplatte kann dann in ein Archiv überführt, oder direkt weiterverwendet werden. Zusätzlich muss die Containerkonfiguration noch in die Metadaten des Archivs geschrieben werden. Allerdings handelt es sich auch hierbei nur um ein Abbild des Dateisystems und nicht um ein vollwertiges Image.

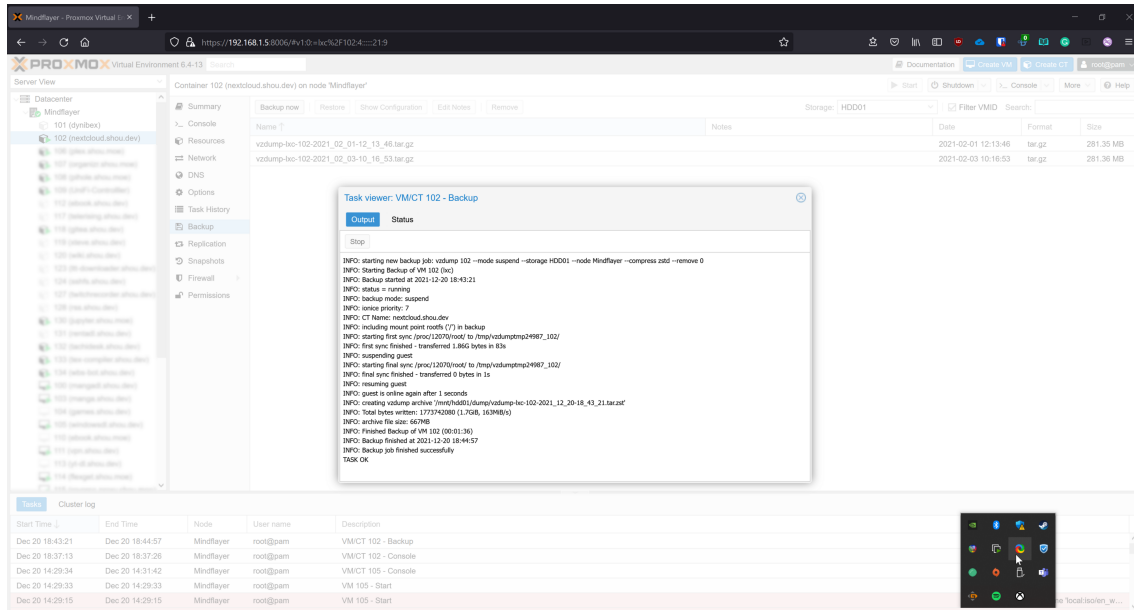


Bild 23: Log-Ausgabe während der Snapshot-Erstellung (2)

4.4 Speicherung des Container-Snapshots

In diesem fiktiven Vorfall wurde der Snapshot des relevanten Containers in Kooperation mit dem IT-Dienstleister erzeugt. Hierbei muss allerdings besonders auf die Integritätserhaltung des Snapshots geachtet werden, weil das erzeugte Archiv ohne großen Aufwand mit einem Archivverwaltungsprogramm manipuliert werden könnte. Deshalb sind zwei Hashes nötig: ein oder mehrere Prüfsummen des Snapshots selbst und der Hash des Datenträgers, auf dem sich Snapshot und Prüfsummen befinden. Als Datenträger zum Transport des Snapshots eignen sich am besten einmal beschreibbare optische Datenträger, also CDs, DVDs oder BDs.

Für dieses Projekt wurden der Snapshot und die Textdateien mit dessen MD5-, SHA-1- und SHA-256-Hashes mit dem Brennprogramm K3b⁴ auf eine CD-R geschrieben. Listing 3 zeigt ein mögliches Vorgehen zum Erzeugen der Hashwerte einer Daten-CD.

```
$ isoinfo dev=/dev/sr0 -d
CD-ROM is in ISO 9660 format
System id: LINUX
Volume id: vzdump-lxc-102-2021_12_20-18_43_
# ...
Application id: K3B THE CD KREATOR (C) 1998-2018 SEBASTIAN TRUEG, MICHAL MALEK AND
LESLIE ZHAI
# ...
Volume set size is: 1
Volume set sequence number is: 1
Logical block size is: 2048
```

⁴<https://userbase.kde.org/K3b/>

```
$ dd if=/dev/sr0 bs=2048 count=341969 \  
> | tee >(md5sum) >(sha1sum) >(sha256sum) >/dev/null \  
> | cat  
47406+0 records in  
47406+0 records out  
97087488 bytes (97 MB, 93 MiB) copied, 133,159 s, 729 kB/s  
69dbc13c9f0a7fb266e0c106db0b191fc2433b14471e8c1fec2a0b8d4ef40f -  
54bbf3d70d05a38762e93993affea04ba61553e7 -  
fd2b71868b45bf0a9777a625ad4d7592 -
```

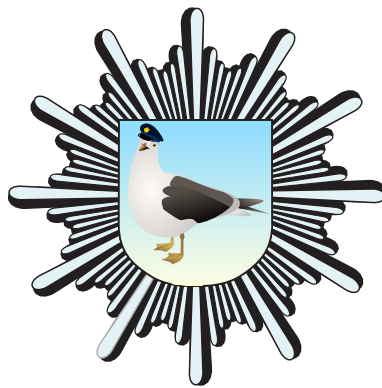
Listing 3: Prüfsummenerzeugung einer CD-ROM

5 Forensisches Gutachten

5.1 Deckblatt

Gutachten der IT-Forensik

Kriminalamt Friedenshof



Auftraggeber

Staatsanwaltschaft Schwerin

Aktenzeichen

0001/1337/2022

Sachverständige: Max Mustermann (B. Sc.)
John Doe (B. Sc.)

Abschluss: 20.01.2022

5.2 Auftrag und juristische Fragestellung

Die Staatsanwaltschaft Schwerin beauftragt im Rahmen eines Datendiebstahlsfalles die Auswertung unten aufgelisteter Asservate und das Verfassen eines IT-forensischen Gutachtens für den Zeitraum vom 20.12.2021 bis zum 21.01.2022. Zusätzlich zu den übergebenen Datenträgern liegen Arbeitskopien und deren Hashwerte vor, die von der Polizeiinspektion Wismar im Vorfeld angefertigt wurden.

Folgende Fragestellungen gilt es zu beantworten:

Asservat 01

- Frage 1) Welches Betriebssystem befindet sich auf dem Gerät?
- Frage 2) Bestand eine aktive Verbindung zu einem Nextcloud-Server?
- Frage 3) Wurden Daten im Cloudspeicher von diesem Gerät aus verändert?
- Frage 4) Welche USB-Datenträger wurden an dieses Gerät angeschlossen?

Asservat 02

- Frage 1) Gab es unerlaubte Versuche, auf den Cloudspeicher zuzugreifen?
- Frage 2) Wurde zum Tatzeitpunkt der Datenbestand in der Cloud verändert?
- Frage 3) Welche Zugänge zu den Daten der Cloud existieren?

Asservat 03

- Frage 1) Befinden sich gelöschte Daten auf diesem Datenträger?
- Frage 2) Wurde dieses Speichermedium mit dem Asservat 01 verbunden?

Asservat 04

- Frage 1) Welches Betriebssystem befindet sich auf dem Gerät und welche Nutzerkonten sind hinterlegt?
- Frage 2) Welche USB-Datenträger wurden an dieses Gerät angeschlossen?
- Frage 3) Befinden sich Bilder auf diesem Gerät, die inhaltlich den vermissten Daten gleichen?
- Frage 4) Wurden Bilder von diesem Gerät aus im Internet veröffentlicht?

5.3 Zusammenfassung der Untersuchung

Asservat – Festplatte des Dienstrechners

Auf der Festplatte befindet sich das Betriebssystem **Windows 10 Home N**. Es wurde eine kürzlich genutzte Instanz des **Nextcloud-Clients** gefunden, die unter dem **Nutzernamen „admin“** in Verbindung mit einem **Nextcloud-Server** unter der Adresse **<https://fda.stoertebeker.dev/nextcloud/>** stand. Die Löschung des Ordners „Kalender 2022“ und aller 12 darin enthaltenen Bilddateien im lokalen Verzeichnis der Cloud wurde bestätigt. Der Löschvorgang wurde an die Cloud übermittelt. Ein USB-Speichermedium mit der **Seriennummer 0E1145514041D91B** und der Bezeichnung „**FLASHPEN128**“ wurde mit dem Gerät verbunden.

Asservat 02 – Nextcloud

In der Benutzerdatenbank des Nextcloud-Servers existiert ein **einzigter Nutzer mit dem Namen „admin“**. **Keine der Daten** dieses Nutzers wurden für einen externen Zugriff **freigeben**. In den Logdateien der Cloud wurden **fünf gescheiterte Anmelungsversuche** von einem Computer mit dem Betriebssystem „Windows 10“ und dem Internet-Browser „Mozilla Firefox 95“ identifiziert. Der Ordner „**Kalender 2022**“ wurde zur **Löschung vorgesehen** und in den „Papierkorb“ verschoben.

Asservat 03 – USB-Stick

Von dem USB-Stick mit der Bezeichnung „**FLASHPEN128**“ konnte ein **gelöschter Ordner „Kalender 2022“** mit 12 JPEG-Dateien geborgen werden. Ein USB-Speichermedium gleicher Marke und Bezeichnung wurde nachweislich an das Asservat 01 angeschlossen.

Asservat 04 – Laptop

Auf dem Gerät mit dem Betriebssystem „**Windows 10**“ existiert der Benutzer „**jansen**“. Es wurde eine Installation des Internetbrowsers „**Mozilla Firefox**“ in der **Version 95.0.1** gefunden. Mit diesem Browser fanden **mehrere Anmelungsversuche** unter der Adresse **<https://fda.stoertebeker.dev/>** statt. Es wurde ebenfalls das Upload-Portal der Image-Sharing-Plattform **Imgur mit der Adresse <https://imgur.com/>** besucht. Es wurde ein USB-Speicherstick mit der **Seriennummer 0E1145514041D91B** an das Gerät angeschlossen. Im Verzeichnis des Nutzers „**jansen**“ befinden sich **12 JPEG-Dateien**, deren Inhalte **identisch mit den Dateien aus den Papierkörben von Asservat 01 und Asservat 02 und den aus Asservat 03 geborgenen Daten** sind.

Timeline

Asservat	Zeitstempel	Event	Beschreibung
2	12.12.21 15:53:43	E	Ordner „Kalender 2022“ wird in der Nextcloud angelegt
1	17.12.21 11:59:40	O	Anmeldung des Windows-Nutzers „el jefe“
1	17.12.21 12:00:05	O	Nextcloud-Client gestartet
4	17.12.21 12:17:04	O	Erster Aufruf Webinterface der Cloud
2	17.12.21 12:17:05	O	Erster gescheiterter Anmeldeversuch
2	17.12.21 12:17:17	O	Zweiter gescheiterter Anmeldeversuch
2	17.12.21 12:17:38	O	Dritter gescheiterter Anmeldeversuch
2	17.12.21 12:17:03	O	Vierter gescheiterter Anmeldeversuch
2	17.12.21 12:17:17	O	Fünfter gescheiterter Anmeldeversuch
4	17.12.21 12:18:13	O	Letzter Aufruf Webinterface der Cloud
1	17.12.21 12:30:09	O	USB-Speichermedium mit der Serien-Nr. 0E1145514041D91B verbunden
3	17.12.21 12:30:23	E	Erzeugung de Ordners „Kalender 2022“ mit 12 JPEG-Datien
2	17.12.21 12:31:03	M	Verschiebung des Ordners „Kalender 2022“ in den Papierkorb
1	17.12.21 12:31:07	M	Verschiebung des Ordners „Kalender 2022“ in den Papierkorb
1	17.12.21 12:31:38	M	Änderung der lokalen Synchronisationsdatenbank
4	17.12.21 12:48:33	O	USB-Speichermedium mit der Serien-Nr. 0E1145514041D91B verbunden
4	17.12.21 12:49:06	E	Kopieren der Bilder auf den Desktop
3	17.12.21 12:49:25	L	Löschung des Ordners „Kalender 2022“ aus dem Dateisystem
4	17.12.21 12:50:00	O	Hochladen der Bilder auf imgur.com

Legende

E Erzeugung von Daten

L Löschung von Daten

M Modifizierung von Daten

O Operationen (Ausführung, Funktion, Handlung)

Alle Zeitstempel sind in MEZ angegeben.

5.4 Untersuchungsobjekte

Tabelle 1: Untersuchungsobjekte

Objekt	Dateiname(n)	MD5-Hashwert
Asservat 01	chef.E01	dc4108c131215806e6875d1a23bc9174
	chef.E02	0d118af12fe6be02e173571b2bb0d783
	chef.E03	3a0806a94c4bb2589c6aca6a4b9a0de0
	chef.E04 (HDD Dienstrechner)	32f82efa52c4e59dd30478bbf618c0bd
Asservat 02	vzdumplx-102-2021_12_20-18_43_21.tar.iso	4f96c5ceb4ea8452fbcf3b3ba9ca696f
	vzdumplx-102-2021_12_20-18_43_21.tar.zst (Sicherung Nextcloud)	245f199a24008aaf317338b98e7483f6
Asservat 03	stick.E01 (USB-Stick)	e635a29d107bbb994d12083bc4608cf7
Asservat 04	sus.E01	c054128195fd5b74915c560ef1295eaf
	sus.E02	b3f474e629aa8f1eba05d3d1e812aa83
	sus.E03	f79b4238f56dc1287133eea2def1a949
	sus.E04	43479d118b6aa7cd25b5ae8774acd31f
	sus.E05	35e9a4f822b76f174f6a5b3d8cce8410
	sus.E06 (HDD Laptop)	f81743c4b784f662b898c26a3da5ff5b

5.5 Untersuchungswerkzeuge

Tabelle 2: Untersuchungswerkzeuge

Name	Version	Funktion
X-Ways Forensics	19.5	Umfangreiche Datenforensik-Software mit integriertem Hex-Editor.
The Sleuth Kit (TSK)	4.11.1	Sammlung von Kommandozeilenprogrammen für die Image-Analyse.
Autopsy	4.19.2	Grafisches Programm zur Nutzung der Werkzeugsammlung TSK, inklusive Plugins für zusätzliche Funktionen.
RegRipper	3.0	Sammlung von Perl-Skripten zum Auslesen des Windows-Registry.
MariaDB Server	10.4	Serveranwendung für die relationale Datenbank MariaDB.

5.6 Untersuchung der Asservate

5.6.1 Asservat 01 – Festplattenimage des Dienstrechners



Bild 24: Asservat 01

Integritätsprüfung

```

root@forensik-pc:/mnt/evidence/2021/0001/1$ tail chef.md5sum
dc4108c131215806e6875d1a23bc9174 chef.E01
0d118af12fe6be02e173571b2bb0d783 chef.E02
3a0806a94c4bb2589c6aca6a4b9a0de0 chef.E03
32f82efa52c4e59dd30478bbf618c0bd chef.E04
root@forensik-pc:/mnt/evidence/2021/0001/1$ md5sum chef.E*
dc4108c131215806e6875d1a23bc9174 chef.E01
0d118af12fe6be02e173571b2bb0d783 chef.E02
3a0806a94c4bb2589c6aca6a4b9a0de0 chef.E03
32f82efa52c4e59dd30478bbf618c0bd chef.E04
root@forensik-pc:/mnt/evidence/2021/0001/1$ md5sum --check chef.md5sum
chef.E01: OK
chef.E02: OK
chef.E03: OK
chef.E04: OK

```

Bild 25: Integritätsprüfung des Images des Dienstrechners

Die übermittelten Hashwerte stimmen mit den lokal erzeugten Hashwerten überein. Die Images weisen somit keine Veränderung auf.

Betriebssystem

Das Festplattenimage wurde mit der IT-Forensik-Software Autopsy eingelesen. Aufgrund des Vorkommens charakteristischer Verzeichnisstrukturen, Dateien und deren Inhalte konnte das Programm darauf eine 64-Bit-Installation des Betriebssystems „Windows 10 Home N“ identifizieren (Bild 26). Es handelt sich dabei um das einzige installierte Betriebssystem auf diesem Computer.

Source Name	Name	Version	Processor Architecture	Data Source	Program Name	Date/Time	Product ID	Owner	Temporary Files Directory	Path
SYSTEM	DESKTOP-HDQKONQ	Windows_NT	AMD64	chef.E01					%SystemRoot%\TEMP	
SOFTWARE				chef.E01	Windows 10 Home N	2021-12-12 18:52:07 MEZ	00327-00000-00000-AA533	el jefe		C:\Windows

Bild 26: Betriebssystem auf dem Festplattenimage

Verbindung zum Cloudspeicher

Durch die Suche nach bestimmten Dateien wurde zuerst die Installation der Nextcloud-Client Software überprüft. Unter Verwendung von Autopsy konnte im Downloadverlauf des Internetbrowsers Microsoft Edge die Installationsdatei `Nextcloud-3.3.6-x64.msi` im Verzeichnis `C:/Users/el jefe/Downloads` gefunden werden (Bild 27). Die Datei stammt aus den offiziellen Download-Quellen der Nextcloud GmbH. Am 16.12.2021 um 22:24:49 Uhr wurde zuletzt auf die Datei zugegriffen.

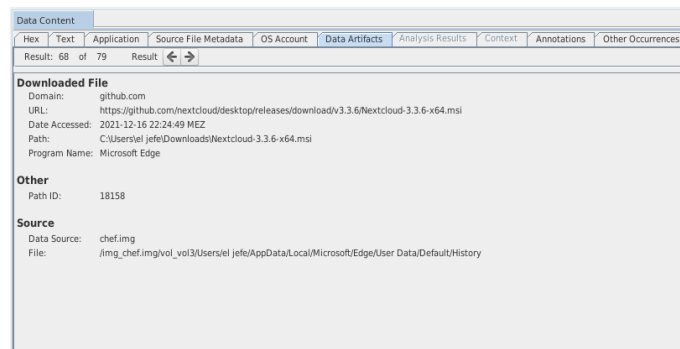


Bild 27: Installationsdatei Nextcloud-Client

Die Suche nach dem Schlüsselwort „Nextcloud“ zeigte, dass sich ein installierter Nextcloud-Client im Pfad `C:/Program Files/Nextcloud` befindet. Das sich darin befindliche Programm `nextcloud.exe` wurde zuletzt am 17.12.2021 um 12:00:05 Uhr gestartet (Bild 28).

Source Name	Program Name	Date/Time
SLUI.EXE-724E99D9.pf	SLUI.EXE	2021-12-17 11:59:58 MEZ
BACKGROUNDTASKHOST.EXE-AC1DA110.pf	BACKGROUNDTASKHOST.EXE	2021-12-17 12:00:03 MEZ
NEXTCLOUD.EXE-4D64E8F2.pf	NEXTCLOUD.EXE	2021-12-17 12:00:05 MEZ
SMARTSCREEN.EXE-9B5E4173.pf	SMARTSCREEN.EXE	2021-12-17 12:00:05 MEZ
WEVTUTIL.EXE-EF5861C4.pf	WEVTUTIL.EXE	2021-12-17 12:00:06 MEZ
SECURITYHEALTHSYSTRAY.EXE-41AD6DE1.pf	SECURITYHEALTHSYSTRAY.EXE	2021-12-17 12:00:08 MEZ
MSEDGE.EXE-78F1488A.pf	MSEDGE.EXE	2021-12-17 12:00:09 MEZ

Type	
Program Name	NEXTCLOUD.EXE
Path	/PROGRAM FILES/NEXTCLOUD
Date/Time	2021-12-17 12:00:05 MEZ
Count	6
Comment	Prefetch File
Source File Path	/img_chef.img/vol3/Windows/Prefetch/NEXTCLOUD.EXE-4D64E8F2.pf
Artifact ID	-9223372036854771826

Bild 28: Letzte Ausführung des Nextcloud-Clients

Aus der Konfigurationsdatei `C:/Users/el_jefe/AppData/Roaming/Nextcloud/nextcloud.cfg` geht hervor, dass der Client mit einem Server unter der Web-Adresse `https://fda.stoertebeker.dev/nextcloud` verbunden und für den Nutzer „admin“ authentifiziert wurde. Das zu synchronisierende Verzeichnis befindet sich unter `C:/Users/el_jefe/Nextcloud`. Eine dort befindliche Datenbank für das Aufzeichnen aller Aktivitäten bestätigt eine Synchronisation mit dem Server am 17.12.2021 um 12:31:38 Uhr. Aufgrund der erfolgreichen Authentifizierung ist es möglich, ohne weiteren Identitätsnachweis vom untersuchten Computer auf die Daten im Cloudspeicher zuzugreifen. Da das Benutzerkonto, für das der Nextcloud-Client installiert wurde, kein Passwort benötigt (Bild 30, letzter Login am 17.12.2021 um 11:59:40 Uhr), sind die synchronisierten Daten vor Zugriffen durch Dritte ungeschützt, sobald physischer Zugang zum Gerät besteht.

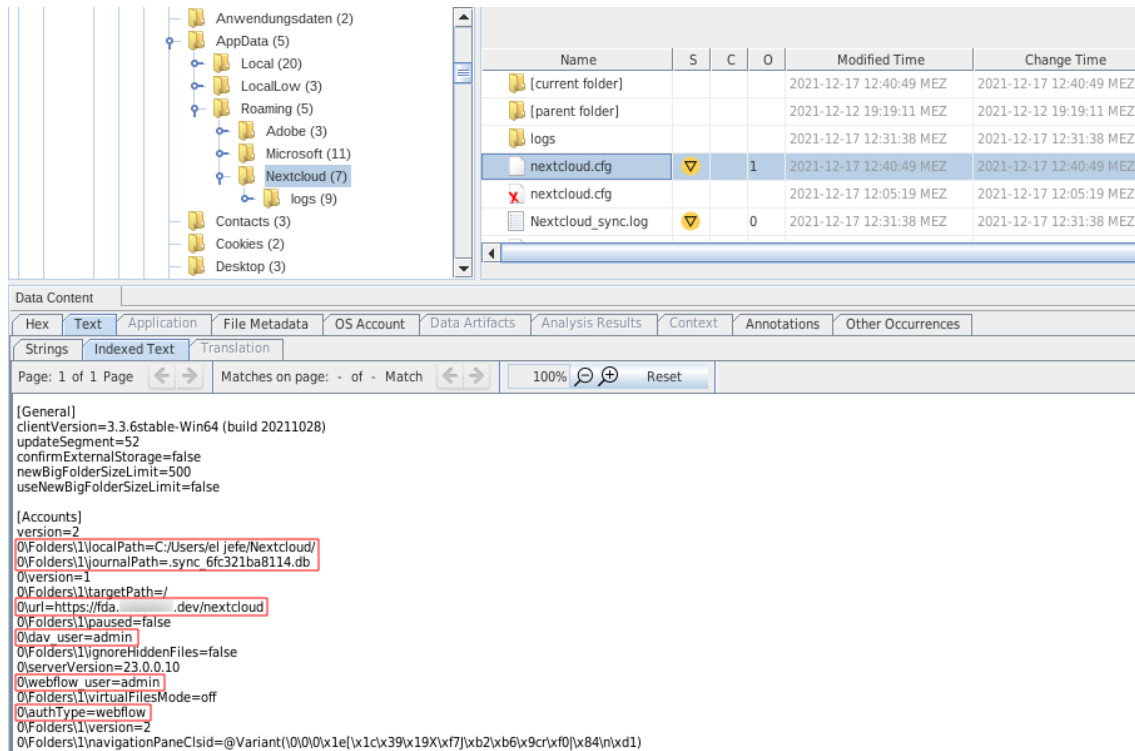


Bild 29: Konfigurationsdatei des Nextcloud-Clients



Bild 30: Benutzerinformationen auf dem Dienstrechner

Veränderung der Clouddaten

Das Image wurde mit X-Ways Forensics nach Nutzungsartefakten und Konfigurationsdateien des Nextcloud-Clients durchsucht. Alle Aktivitäten des Nextcloud-Clients wurden in der Log-Datei `C:/Users/el jefe/AppData/Roaming/Nextcloud/`

hinweist:

Tabelle 3: Dateinamen aus der Datenbank des Nextcloud-Clients

Dateiname
Kalender 2022
Kalender 2022/DSC_012.jpeg
Kalender 2022/DSC_011.jpeg
Kalender 2022/DSC_010.jpeg
Kalender 2022/DSC_009.jpeg
Kalender 2022/DSC_006.jpeg
Kalender 2022/DSC_008.jpeg
Kalender 2022/DSC_007.jpeg
Kalender 2022/DSC_005.jpeg
Kalender 2022/DSC_003.jpeg
Kalender 2022/DSC_002.jpeg
Kalender 2022/DSC_004.jpeg
Kalender 2022/DSC_001.jpeg

Mit Autopsy können Dateien aufgelistet werden, die vom Nutzer in den „Papierkorb“ verschoben wurden. Dabei wurde zusätzlich der Eintrag „Kalender 2022“ gefunden (Bild 33).

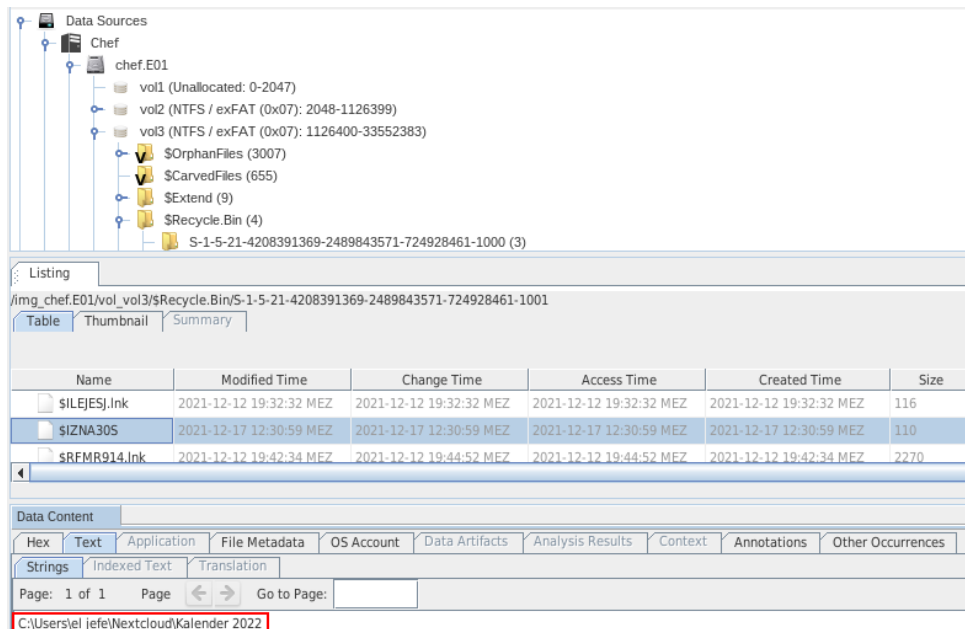


Bild 33: „Kalender 2022“ im Papierkorb

Daraus wird geschlossen, dass sich das Verzeichnis „Kalender 2022“ mit 12 untergeordneten JPEG-Dateien im Nextcloud-Ordner des Benutzers befand, am 17.12.2021 um 12:31 Uhr gelöscht und die Löschung anschließend an den Nextcloud-Server übermittelt wurde.

Verbundene USB-Speichermedien

Informationen über verbundene USB-Speichermedien wurden mittels Sleuthkit und RegRipper aus dem Festplattenimage extrahiert. Zuerst wurde die Position der Systempartition bestimmt und daraus ein Auszug der Registry-Daten erzeugt. Das Registry ist eine Datenbank in Betriebssystemen der Windows-NT-Familie, in der systemspezifische Konfigurationen und Ereignisse gespeichert werden. Mit dem Plugin `usbstor` für RegRipper wurde der Registry-Auszug nach Informationen über verbundene USB-Speichermedien untersucht (Bild 34):

```
root@forensik-pc:/mnt/evidence/2021/0001/1$ mmls chef.E0?
DOS Partition Table
Offset Sector: 0
Units are in 512-byte sectors
```

	Slot	Start	End	Length	Description
000:	Meta	0000000000	0000000000	0000000001	Primary Table (#0)
001:	-----	0000000000	0000002047	0000002048	Unallocated
002:	000:000	0000002048	0001126399	0001124352	NTFS / exFAT (0x07)
003:	000:001	0001126400	0033552383	0032425984	NTFS / exFAT (0x07)
004:	-----	0033552384	0033554431	0000002048	Unallocated

```
root@forensik-pc:/mnt/evidence/2021/0001/1$ fls -r -o 1126400 chef.E0? | grep "SYSTEM$"
+++ r/r 78080-128-4:  SYSTEM
root@forensik-pc:/mnt/evidence/2021/0001/1$ icat -o 1126400 chef.E0? 78080-128-4 > SYSTEM
root@forensik-pc:/mnt/evidence/2021/0001/1$ rip.pl -r SYSTEM -p usbstor
Launching usbstor v.20200515
usbstor v.20200515
(System) Get USBStor key info

USBStor
ControlSet001\Enum\USBStor

Disk&Ven_Generic&Prod_Flash_Disk&Rev_8.07 [2021-12-17 11:09:38]
S/N: 9209FB34&0 [2021-12-17 11:09:39Z]
Device Parameters LastWrite: [2021-12-17 11:09:39Z]
Properties LastWrite : [2021-12-17 11:09:39Z]
  FriendlyName      : Generic Flash Disk USB Device
  First InstallDate  : 2021-12-17 11:09:39Z
  InstallDate       : 2021-12-17 11:09:39Z
  Last Arrival      : 2021-12-17 11:09:38Z
  Last Removal      : 2021-12-17 11:10:16Z

Disk&Ven_Hama&Prod_FlashPen&Rev_1.02 [2021-12-17 11:30:09]
S/N: 0E1145514041D91B&0 [2021-12-17 11:30:09Z]
Device Parameters LastWrite: [2021-12-17 11:30:09Z]
Properties LastWrite : [2021-12-17 11:30:09Z]
  FriendlyName      : Hama FlashPen USB Device
  First InstallDate  : 2021-12-17 11:30:09Z
  InstallDate       : 2021-12-17 11:30:09Z
  Last Arrival      : 2021-12-17 11:30:09Z
  Last Removal      : 2021-12-17 11:31:20Z
```

Bild 34: Per RegRipper ermittelte angeschlossene USB-Geräte

An das Gerät wurden folgende USB-Speichermedien angeschlossen:

Tabelle 4: Verbundene Speichermedien (Asservat 01)

Zeitstempel	Serien-Nr.	Bezeichnung
17.12.2021 12:09:39	9209FB34	Generic Flash Disk USB Device
17.12.2021 12:30:09	0E1145514041D91B	Hama FlashPen USB Device

5.6.2 Asservat 02 – Snapshot des Nextcloud-Servers



Bild 35: Asservat 02

Integritätsprüfung

```
root@forensik-pc:/mnt/evidence/2021/0001/2$ tail lxc-102.md5sum
4f96c5ceb4ea8452fbcf3b3ba9ca696f vzdump-lxc-102-2021_12_20-18_43_21.tar.iso
root@forensik-pc:/mnt/evidence/2021/0001/2$ md5sum vzdump-lxc-102-2021_12_20-18_43_21.tar.iso
4f96c5ceb4ea8452fbcf3b3ba9ca696f vzdump-lxc-102-2021_12_20-18_43_21.tar.iso
root@forensik-pc:/mnt/evidence/2021/0001/2$ md5sum --check lxc-102.md5sum
vzdump-lxc-102-2021_12_20-18_43_21.tar.iso: OK
```

Bild 36: Integritätsprüfung des Snapshot-Datenträgers

Der Snapshot des Nextcloud-Servers aus dem Rechenzentrum der Komet GbR ist auf einer CD-R mit 700 MB Speicherkapazität gesichert. Auf dem Datenträger befindet sich der Snapshot als komprimiertes Archiv sowie dessen MD5-, SHA-1- und SHA-256-Hashwerte.

```
root@forensik-pc:/mnt/evidence/2021/0001/2$ tail md5sum
245f199a24008aaf317338b98e7483f6 vzdump-lxc-102-2021_12_20-18_43_21.tar.zst
root@forensik-pc:/mnt/evidence/2021/0001/2$ md5sum vzdump-lxc-102-2021_12_20-18_43_21.tar.zst
245f199a24008aaf317338b98e7483f6 vzdump-lxc-102-2021_12_20-18_43_21.tar.zst
root@forensik-pc:/mnt/evidence/2021/0001/2$ md5sum --check md5sum
vzdump-lxc-102-2021_12_20-18_43_21.tar.zst: OK
```

Bild 37: Integritätsprüfung des Nextcloud-Snapshots

Der übermittelte Hashwert stimmt mit dem lokal erzeugten Hashwert überein. Das Image weist somit keine Veränderung auf.

Gescheiterte Anmeldeversuche

Für die Untersuchung der Anmeldeversuche wurde die Log-Datei des Nextcloud-Servers betrachtet. Standardmäßig befindet sich diese unter `/var/www/html/nextcloud/data/nextcloud.log`. Da die vorliegende Installation nicht anders konfiguriert wurde, konnte die Log-Datei in ihrem Standardverzeichnis gefunden werden. Darin befinden sich 5 Meldungen über gescheiterte Anmeldeversuche (Bild 38). Zeits-

«nextcloud.log»	/LogicalFileSet1/www/html/nextcloud/data/nextcloud.log	0000-00-00 00:00:00
rtrim(\$dataDir, '/') . '«nextcloud.log»'; \$output->...	/LogicalFileSet1/www/html/nextcloud/core/Command/Log...	0000-00-00 00:00:00
. 'logfile (data/«nextcloud.log»). If you want to re-run	/LogicalFileSet1/root/latest.zip/nextcloud/core/Command/...	2021-11-26 21:51:45 MEZ
directory nextcloud/data/nextcloud.log. PHP version and	/LogicalFileSet1/root/latest.zip/nextcloud/core/doc/admin/...	2021-11-26 21:53:54 MEZ

Zeitsstempel	IP-Adresse	Browser	Betriebssystem
17.12.2021 12:17:05	192.168.1.11	Firefox 95.0	Windows 10
17.12.2021 12:17:17	192.168.1.11	Firefox 95.0	Windows 10
17.12.2021 12:17:38	192.168.1.11	Firefox 95.0	Windows 10
17.12.2021 12:18:03	192.168.1.11	Firefox 95.0	Windows 10
17.12.2021 12:18:17	192.168.1.11	Firefox 95.0	Windows 10

Bild 38: Auszug aus dem Nextcloud-Log

temple der Anmeldeversuche aus dem Nextcloud-Log: Alle Anmeldeversuche

Tabelle 5: Anmeldeversuche

Zeitstempel	IP-Adresse	Browser	Betriebssystem
17.12.2021 12:17:05	192.168.1.11	Firefox 95.0	Windows 10
17.12.2021 12:17:17	192.168.1.11	Firefox 95.0	Windows 10
17.12.2021 12:17:38	192.168.1.11	Firefox 95.0	Windows 10
17.12.2021 12:18:03	192.168.1.11	Firefox 95.0	Windows 10
17.12.2021 12:18:17	192.168.1.11	Firefox 95.0	Windows 10

stammen von der gleichen IP-Adresse und identischen Browser- und Betriebssysteminformationen.

Des Weiteren speichert der Nextcloud-Server Brute-force-Angriffe in seiner Datenbank¹. Darin sind 5 Anmeldeversuche im Zeitraum vom 17.12.2021 zwischen 12:17:05 Uhr und 12:18:17 Uhr von einem Computer mit der IP-Adresse 192.168.1.11 aus vermerkt. Die Daten sind identisch zu denen in der Log-Datei.

¹Bei einem Brute-force-Angriff testet ein Angreifer verschiedene Passwörter, bis eventuell eines davon den Zugriff auf ein System ermöglicht.

Veränderung des Datenbestands

Aktivitäten bezüglich des Datenbestands werden in der Datenbank gespeichert. Unter den letzten Aktivitäten in der Cloud vor der Erstellung des Snapshots befindet sich die Löschung des Eintrags „Kalender 2022“. Aus einer separaten Tabelle konnte der Systempfad `files_trashbin/files/Kalender 2022.d1639740663` als neuer Speicherort der Dateien ermittelt werden. Tabelle 6 zeigt alle darin befindlichen Dateien.

Tabelle 6: Gelöschte Dateien in der Cloud

Letzter Zugriff	Dateiname	MD5-Hashwert
20.12.2021 18:44:43	DSC_012.jpeg	f8f3f3159eee154a14f609d51e751159
20.12.2021 18:44:43	DSC_003.jpeg	246c853ca7034eb7f4070763c4fa6ba6
20.12.2021 18:44:43	DSC_008.jpeg	554b287e802e1eae97b1f656e8b85607
20.12.2021 18:44:43	DSC_004.jpeg	83b407c98a8ee7608a944213a08dc697
20.12.2021 18:44:43	DSC_002.jpeg	074b919c71571fdd42169f07e673b089
20.12.2021 18:44:43	DSC_010.jpeg	367e011e99c8610b8b153d00b6789bfd
20.12.2021 18:44:43	DSC_011.jpeg	892a4c27c5b7fe1809ef1fb80a696e06
20.12.2021 18:44:43	DSC_006.jpeg	e130ffd91d97fbaf3e82e14b1009d8ac
20.12.2021 18:44:43	DSC_007.jpeg	d1b8136d8d009153acc5800ae41fc579
20.12.2021 18:44:43	DSC_009.jpeg	9229dc847d984bdbc5fe81ac6804e794
20.12.2021 18:44:43	DSC_005.jpeg	dbf2ee178c353702a8a13631aca223f8
20.12.2021 18:44:43	DSC_001.jpeg	9da5b7202f87b81be324f0f89c760b7b

Das Verzeichnis „Kalender 2022“ und die 12 darin enthaltenen JPEG-Dateien wurden demnach am 17.12.2021 um 12:31:03 Uhr zur Löschung markiert.

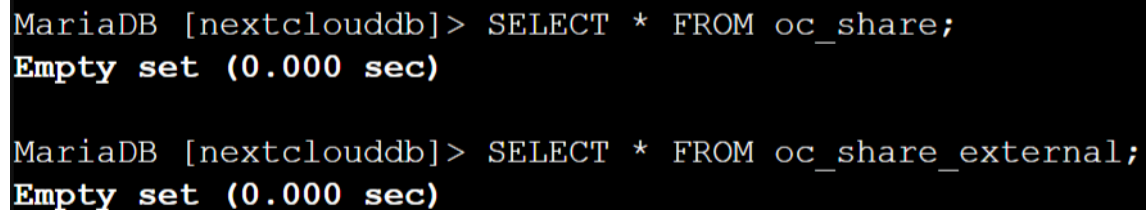
Zugang zu den Daten

Aufgrund der Mehrbenutzerarchitektur von Nextcloud besteht die Möglichkeit, dass es abgesehen vom Besitzer einer Datenmenge noch andere Nutzer mit Zugriff auf die relevanten Daten gibt. Zur Analyse wurde die Datenbank des Nextcloud-Servers über das MariaDB-Kommandozeilenprogramm ausgelesen. Im System wurde nur ein einziger Nutzer mit Administrationsprivilegien gefunden:

Tabelle 7: Nutzer der Cloud

Nutzername	Gruppe
Admin	admin

Nextcloud stellt darüber hinaus eine Funktion zum Teilen von Dateien über einen Zugangslink bereit. Das bedeutet, dass ausgewählte Dateien nicht nur von Nutzern der Cloud, sondern auch über einen privaten Link abgerufen werden können. Mit den Informationen aus der Datenbank wurde überprüft, ob solche Zugänge existieren (Bild 39).



```
MariaDB [nextcloudodb]> SELECT * FROM oc_share;  
Empty set (0.000 sec)  
  
MariaDB [nextcloudodb]> SELECT * FROM oc_share_external;  
Empty set (0.000 sec)
```

Bild 39: Auflistung der Freigaben über MariaDB

Es zeigte sich, dass es keine Freigaben innerhalb der Cloud gab, weshalb ein Zugriff auf die Daten durch einen anderen Nutzer oder Dritte ausgeschlossen werden kann.

5.6.3 Asservat 03 – USB-Stick

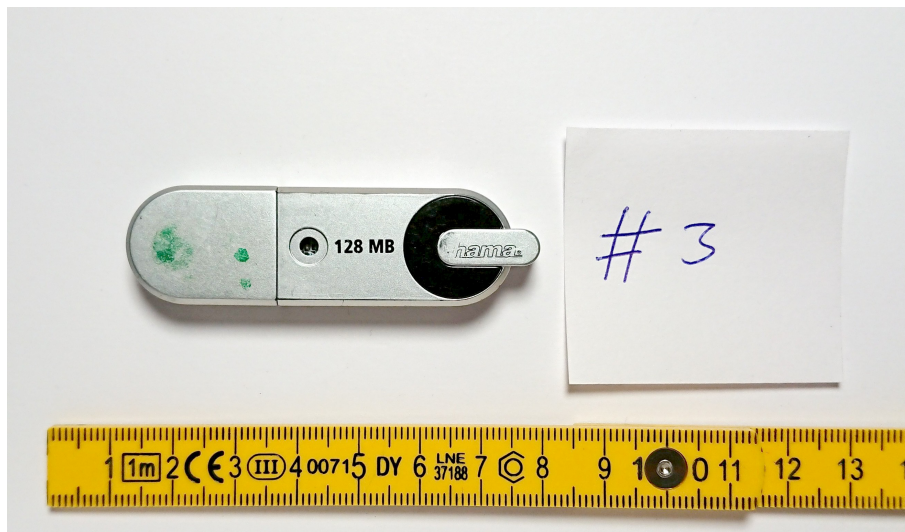


Bild 40: Asservat 03

Integritätsprüfung

```
root@forensik-pc:/mnt/evidence/2021/0001/3$ tail stick.md5sum
e635a29d107bbb994d12083bc4608cf7 stick.E01
root@forensik-pc:/mnt/evidence/2021/0001/3$ md5sum stick.E01
e635a29d107bbb994d12083bc4608cf7 stick.E01
root@forensik-pc:/mnt/evidence/2021/0001/3$ md5sum --check stick.md5sum
stick.E01: OK
```

Bild 41: Integritätsprüfung des USB-Stick-Images

Der übermittelte Hashwert stimmt mit dem lokal erzeugten Hashwert überein. Das Image weist somit keine Veränderung auf.

Gelöschte Daten

Für die Suche nach gelöschten Daten wurde zuerst die Datenpartition auf dem Speichermedium mittels Sleuthkit lokalisiert. An Position 2048 befindet sich ein FAT-Dateisystem mit der Bezeichnung „FLASHPEN128“. Darin liegt ein gelöscht Verzeichnis mit dem Namen „Kalender 2022“ (Bild 42).

```

root@forensik-pc:/mnt/evidence/2021/0001/3$ mmls stick.E0?
DOS Partition Table
Offset Sector: 0
Units are in 512-byte sectors

    Slot      Start      End      Length    Description
000:  Meta      0000000000  0000000000  0000000001  Primary Table (#0)
001:  -----  0000000000  00000002047  00000002048  Unallocated
002:  000:000  00000002048  00000239615  00000237568  Win95 FAT32 (0x0c)
003:  -----  00000239616  00000251903  00000012288  Unallocated
root@forensik-pc:/mnt/evidence/2021/0001/3$ fls -o 2048 stick.E01
r/r 3:  FLASHPEN128 (Volume Label Entry)
d/d 6:  System Volume Information
d/d * 8:  Kalender 2022
d/d 10:  .Trash-1000
v/v 3741379:  $MBR
v/v 3741380:  $FAT1
v/v 3741381:  $FAT2
V/V 3741382:  $OrphanFiles

```

Bild 42: Dateisysteminformationen über das USB-Stick-Image

Im Hex-Editor des Programms X-Ways Forensics ist das gelöschte Datenfragment „Kalender 2022“ auf der Datenpartition des USB-Sticks (Bild 43) sichtbar.

Partition	File		Preview			Details			Gallery			Calendar			Legend			Sync	
Offset	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	ANSI	ASCII	
00000000	46	4C	41	53	48	50	45	4E	31	32	38	08	00	00	17	8E	FLASHPEN128	ž	
00000010	3F	54	3F	54	00	00	17	8E	3F	54	00	00	00	00	00	00	?T?T	ž?T	
00000020	42	20	00	49	00	6E	00	66	00	6F	00	0F	00	72	72	00	B I n f o	rr	
00000030	6D	00	61	00	74	00	69	00	6F	00	00	00	6E	00	00	00	m a t i o n		
00000040	01	53	00	79	00	73	00	74	00	65	00	0F	00	72	6D	00	S y s t e m		
00000050	20	00	56	00	6F	00	6C	00	75	00	00	00	6D	00	65	00	V o l u m e		
00000060	53	59	53	54	45	4D	7E	31	20	20	20	16	00	55	BC	65	SYSTEM~1	U4e	
00000070	91	53	91	53	00	00	BD	65	91	53	03	00	00	00	00	00	'S'S	4e'S	
00000080	E5	4B	00	61	00	6C	00	65	00	6E	00	0F	00	E9	64	00	ãK a l e n	éd	
00000090	65	00	72	00	20	00	32	00	30	00	00	00	32	00	32	00	e r 2 0	2 2	
000000A0	E5	41	4C	45	4E	44	7E	31	20	20	20	10	00	92	C1	65	ãALEND~1	'Áe	
000000B0	91	53	91	53	00	00	49	58	8E	53	06	00	00	04	00	00	'S'S	IXžS	
000000C0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00			

Bild 43: Artefakte eines Dateiordners

Im darauffolgenden Speicherbereich befinden sich sieben gelöschte Bilder im JPEG-Format (Bild 44).

vzdump-lxc-102-2021_12_2...										chef, P2	chef	stick	stick, Volume	
\Kalender 2022														
	Name	Description	Size	Created	Modified	Record changed	Attr.	1st sector						
	.. = (Root directory)	existing	124 MB							3.908				
	. = Kalender 2022 (7)	prev. existing, data not necessarily intact	1,1 MB	17.12.2021 12:46:03	14.12.2021 11:02:18					3.912				
	DSC_001.jpeg	prev. existing, data not necessarily intact	144 KB	17.12.2021 12:30:23	12.12.2021 13:55:46				A	3.913				
	DSC_002.jpeg	prev. existing, data not necessarily intact	48,4 KB	17.12.2021 12:30:23	12.12.2021 14:23:38				A	4.202				
	DSC_003.jpeg	prev. existing, data not necessarily intact	154 KB	17.12.2021 12:30:23	12.12.2021 14:07:44				A	4.299				
	DSC_004.jpeg	prev. existing, data not necessarily intact	207 KB	17.12.2021 12:30:23	12.12.2021 14:26:14				A	4.608				
	DSC_005.jpeg	prev. existing, data not necessarily intact	169 KB	17.12.2021 12:30:23	12.12.2021 14:24:08				A	5.022				
	DSC_006.jpeg	prev. existing, data not necessarily intact	309 KB	17.12.2021 12:30:23	12.12.2021 14:09:34				A	5.360				
	DSC_007.jpeg	prev. existing, data not necessarily intact	92,8 KB	17.12.2021 12:30:24	12.12.2021 14:23:22				A	5.979				

Bild 44: Liste gefundener gelöschter Dateien aus X-Ways Forensics

Bei der Suche nach Bilddateien mit dem Programm Autopsy wurden fünf weitere

Bilder im JPEG-Format gefunden (Bild 45). Diese Dateien konnten nur durch File-Carving² erkannt werden.

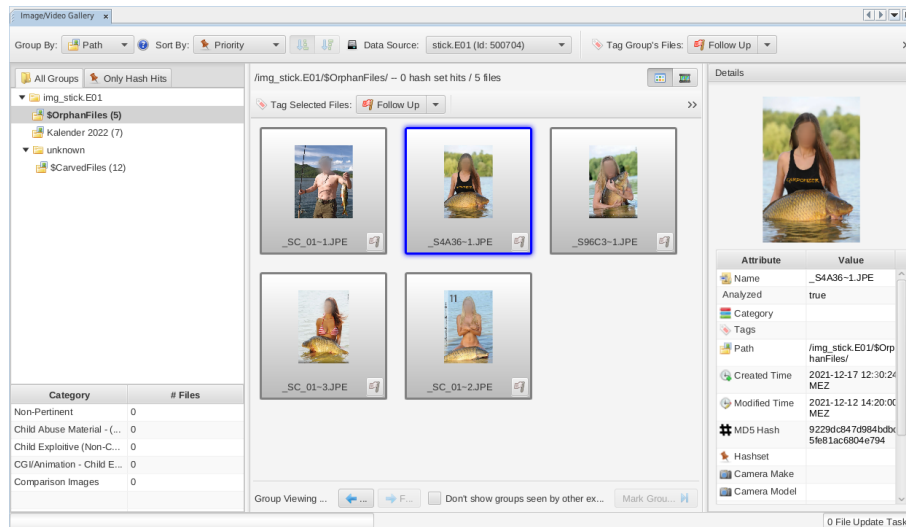


Bild 45: Gefundene Bilddateien (Autopsy)

Insgesamt wurden auf dem Datenträger 13 gelöschte Dateien gefunden:

Tabelle 8: Alle vom USB-Stick geborgenen Dateien

Erzeugung	Dateiname	Typ	MD5-Hashwert
17.12.2021 12:30:23	Kalender 2022	Ordner	-
17.12.2021 12:30:23	DSC_001.jpeg	Bild	9da5b7202f87b81be324f0f89c760b7b
17.12.2021 12:30:23	DSC_002.jpeg	Bild	074b919c71571fdd42169f07e673b089
17.12.2021 12:30:23	DSC_003.jpeg	Bild	246c853ca7034eb7f4070763c4fa6ba6
17.12.2021 12:30:23	DSC_004.jpeg	Bild	83b407c98a8ee7608a944213a08dc697
17.12.2021 12:30:23	DSC_005.jpeg	Bild	dbf2ee178c353702a8a13631aca223f8
17.12.2021 12:30:23	DSC_006.jpeg	Bild	e130ffd91d97fbaf3e82e14b1009d8ac
17.12.2021 12:30:24	DSC_007.jpeg	Bild	d1b8136d8d009153acc5800ae41fc579
17.12.2021 12:30:24	_SC_01~1.JPE	Bild	367e011e99c8610b8b153d00b6789bfd
17.12.2021 12:30:24	_SA36~1.JPE	Bild	9229dc847d984bdbc5fe81ac6804e794
17.12.2021 12:30:24	_S96C3~1.JPE	Bild	554b287e802e1eae97b1f656e8b85607
17.12.2021 12:30:24	_SC_01~3.JPE	Bild	f8f3f3159eee154a14f609d51e751159
17.12.2021 12:30:24	_SC_01~2.JPE	Bild	892a4c27c5b7fe1809ef1fb80a696e06

Da im Dateisystem des USB-Sticks nicht mehr auf diese Dateien verwiesen wird, werden diese Daten als gelöscht betrachtet.

²Im Dateisystem gibt es keine Verweise auf diese Dateien. Sie wurden über die Suche nach charakteristischen Byte-Sequenzen, in diesem Fall JPEG-Datei-Header, identifiziert.

Verbindung zu Asservat 01

Auf dem Datenträger befindet sich das Verzeichnis „System Volume Information“. Dies deutet darauf hin, dass der Datenträger in der Vergangenheit mit einem Windows-System verbunden wurde. Die letzte Änderung in diesem Verzeichnis geschah, wie in Bild 46 zu sehen, am 17.12.2021 um 12:48:33 Uhr.

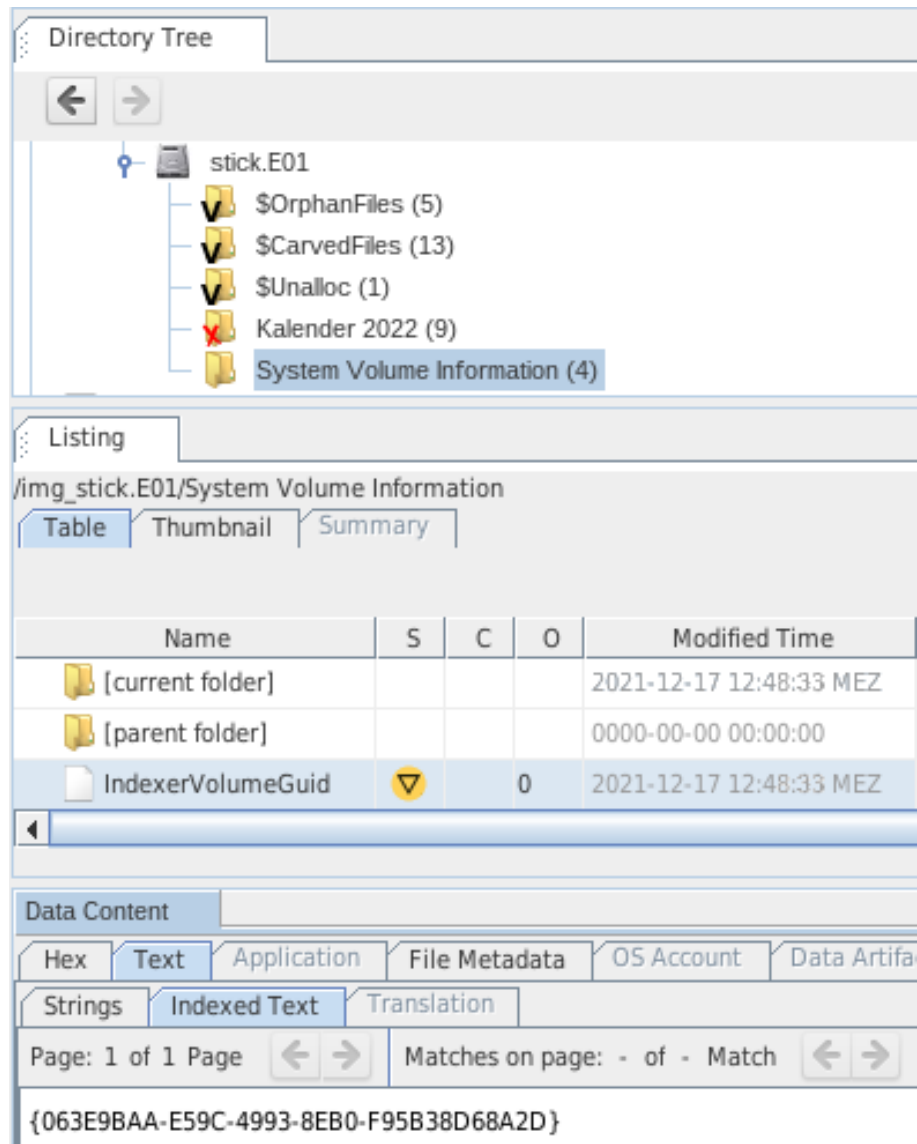


Bild 46: „System Volume Information“ des USB-Datenträgers

In den vorangegangenen Untersuchungsschritten (S. 48) wurde die Bezeichnung des Dateisystems auf dem Datenträger, „FLASHPEN128“, ermittelt. Die Festplattenimages des Asservats 01 wurden mit Autopsy nach Vorkommen dieser Bezeichnung durchsucht. Aus den Registry-Einträgen ist ersichtlich, dass eine Festplatte mit der Bezeichnung „FLASHPEN128“ unter dem Laufwerksbuchstaben „E“ in das System

eingehängt wurde. Unter den jüngsten Aktivitäten im Dateisystem des Asservats 01 ist ein Eintrag eines Ordners „Kalender 2022“ auf dem Laufwerk „E“ gelistet. Der letzte Schreibvorgang auf diesen Datenträger geschah am 17.12.2021 um 12:30:10 Uhr (Bilder 47, 48, 49, 50 und 51).

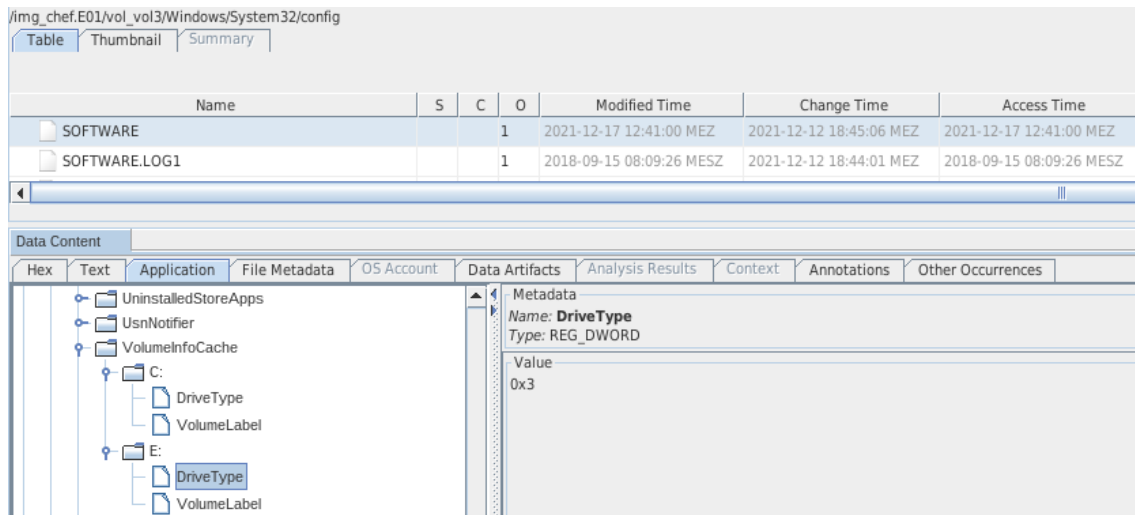


Bild 47: Vermerk Laufwerk „E“ im Registry

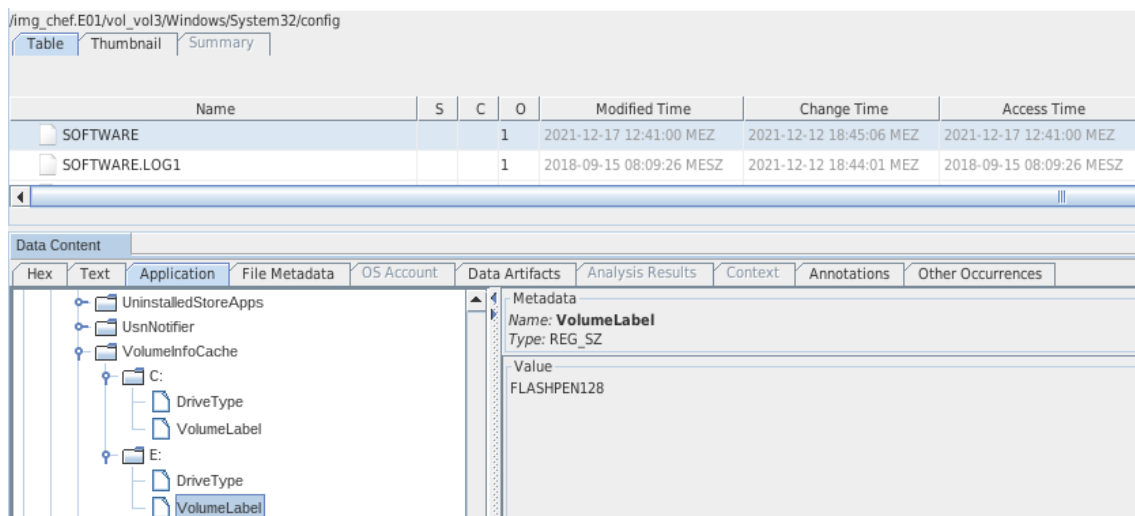


Bild 48: Bezeichnung „FLASHPEN128“ für Laufwerk „E“ im Registry

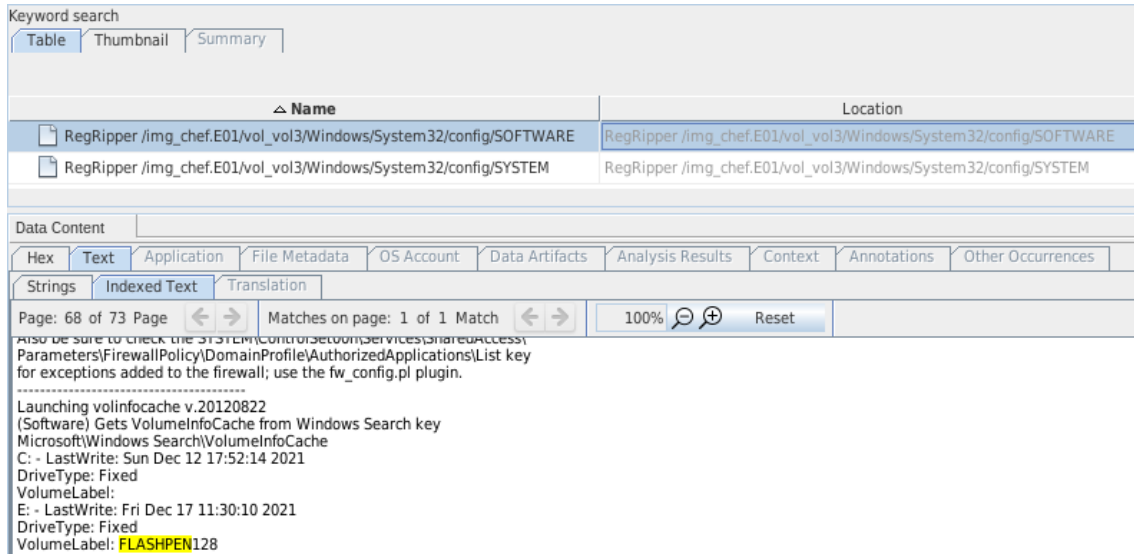


Bild 49: Auftreten der Dateisystembezeichnung „FLASHPEN128“ im Registry

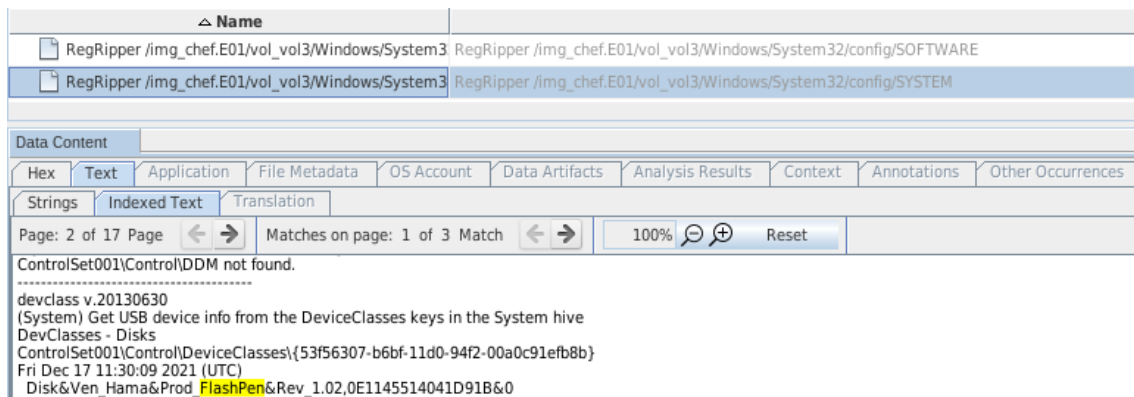


Bild 50: USB-Stick-Modell „FlashPen“ des Herstellers „Hama“ im Registry des Asservats 01

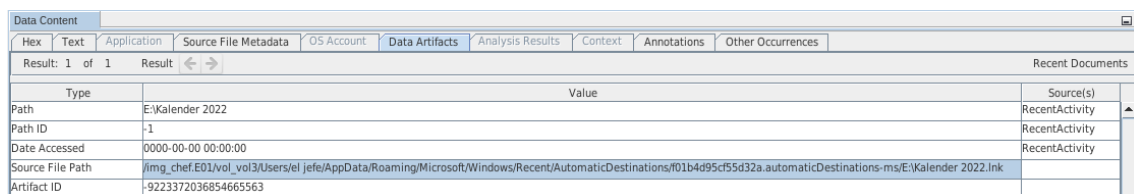


Bild 51: Ordner „Kalender 2022“ auf dem kürzlich verwendeten Laufwerk „E“

5.6.4 Asservat 04 – Festplattenimage des Laptops



Bild 52: Asservat 04

Integritätsprüfung

```

root@forensik-pc:/mnt/evidence/2021/0001/4$ tail sus.md5sum
c054128195fd5b74915c560ef1295eaf    sus.E01
b3f474e629aa8f1eba05d3d1e812aa83    sus.E02
f79b4238f56dc1287133eea2def1a949    sus.E03
43479d118b6aa7cd25b5ae8774acd31f    sus.E04
35e9a4f822b76f174f6a5b3d8cce8410    sus.E05
f81743c4b784f662b898c26a3dafff5b    sus.E06
root@forensik-pc:/mnt/evidence/2021/0001/4$ md5sum sus.E*
c054128195fd5b74915c560ef1295eaf    sus.E01
b3f474e629aa8f1eba05d3d1e812aa83    sus.E02
f79b4238f56dc1287133eea2def1a949    sus.E03
43479d118b6aa7cd25b5ae8774acd31f    sus.E04
35e9a4f822b76f174f6a5b3d8cce8410    sus.E05
f81743c4b784f662b898c26a3dafff5b    sus.E06
root@forensik-pc:/mnt/evidence/2021/0001/4$ md5sum --check sus.md5sum
sus.E01: OK
sus.E02: OK
sus.E03: OK
sus.E04: OK
sus.E05: OK
sus.E06: OK

```

Bild 53: Integritätsprüfung des Laptop-Images

Die übermittelten Hashwerte stimmen mit den lokal erzeugten Hashwerten überein. Die Images weisen somit keine Veränderung auf.

Nutzerdaten des Laptops

Program Name	Windows 10 Home
Date/Time	2021-12-12 20:35:02 CET
Path	C:\Windows
Product ID	00326-10000-00000-AA247
Owner	jansen

Bild 54: Betriebssystem und Nutzer des Laptop-Images

Name	DESKTOP-37E56OH
Domain	
Version	Windows_NT
Processor Architecture	AMD64
Temporary Files Directory	%SystemRoot%\TEMP

Bild 55: Zugrundeliegende Architektur des Laptop-Images

Bei dem betrachteten Laptop-Image handelt es sich um ein „Windows 10“ System (Bild 54), welches auf einem 64-Bit-Prozessor betrieben wird. Der Gerätenamen ist „DESKTOP-37E56OH“ (Bild 55) mit dem Administrationsnutzer „jansen“ (Bild 54).

Internetaktivitäten des Laptops

SOFTWARE		2	Mozilla Maintenance Service v.95.0.1	2021-12-17 11:09:26 CET	sus.E01
SOFTWARE		2	Mozilla Firefox (x64 de) v.95.0.1	2021-12-17 11:09:25 CET	sus.E01

Bild 56: Installierte Software auf dem Laptop

/img_sus.E01/vol3/Users/jansen/Downloads											
Table Thumbnail Summary											
Name	S	C	O	Modified Time	Change Time	Access Time	Created Time	Size	Flags(Dir)	Flags(Meta)	Known
[current folder]				2021-12-17 12:09:04 CET	2021-12-17 12:09:04 CET	2021-12-17 11:48:49 CET	2021-12-12 22:09:43 CET	392	Allocated	Allocated	unknown
[parent folder]				2021-12-12 22:12:23 CET	2021-12-12 22:12:23 CET	2021-12-17 11:50:23 CET	2021-12-12 22:09:43 CET	256	Allocated	Allocated	unknown
desktop.ini			2	2021-12-12 22:10:16 CET	2021-12-12 22:10:16 CET	2021-12-17 11:50:20 CET	2021-12-12 22:10:16 CET	282	Allocated	Allocated	unknown
Firefox Installer.exe			3	2021-12-17 12:09:04 CET	2021-12-17 12:09:06 CET	2021-12-17 11:48:49 CET	2021-12-17 12:09:03 CET	333944	Allocated	Allocated	unknown
Firefox Installer.exe:SmartScreen			2	2021-12-17 12:09:04 CET	2021-12-17 12:09:06 CET	2021-12-17 11:48:49 CET	2021-12-17 12:09:03 CET	7	Allocated	Allocated	unknown

Bild 57: Inhalt des Download-Verzeichnisses

Es ist davon auszugehen, dass kürzlich der Webbrowser Mozilla Firefox verwendet wurde. Diese Aussage ist zu treffen, da Firefox das einzige nicht vorinstallierte Programm auf dem System ist (Bild 56) und die Installationsdatei **Firefox Installer.exe** im Download-Verzeichnis gefunden wurde (Bild 57). Mit Autopsy wurde ebenfalls der Browserverlauf von Firefox gefunden (Datei **C:/Users/jansen/AppData/Roaming/Mozilla/Firefox/Profiles/5zcbi6rg.default-release/places.sqlite**).

Durch die Analyse des Browserverlaufs wird ersichtlich, dass es mehrfache Versuche gab, über das Webinterface auf die Cloud zuzugreifen (Bilder 58 und 59). Allerdings fehlt im Browserverlauf ein Eintrag der Zielseite der Cloud, weshalb die Anmeldeversuche als gescheitert betrachtet werden.

places.sqlite	https://fda. .dev/index.php/login	2021-12-17 12:12:06 CET	https://fda. .dev/	Nextcloud	Firefox
places.sqlite	https://fda. .dev/index.php/login?user=admin&direct=1	2021-12-17 12:17:04 CET	https://fda. .dev/index.php/login	Nextcloud	Firefox

Bild 58: Auszug aus dem Browserverlauf

id	fieldname	value	timesUsed	firstUsed	lastUsed	guid
1	user	admin	5	1639739823545000	1639739893978000	zsOPreNQRJIT7IO9
2	searchbar-history	imgut	1	1639738185304000	1639738185304000	mf/Fq8f/RGuZFIUJ

Bild 59: Mehrfache Anmeldeversuche mit dem Nutzernamen „admin“

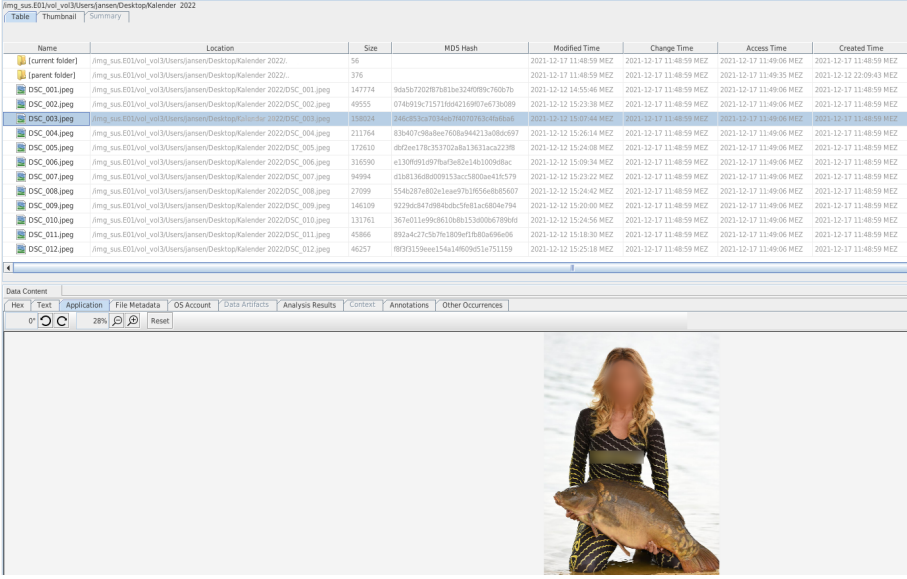
Verbundene USB-Geräte

Aus der Untersuchung mit Autopsy wird ersichtlich, dass ein USB-Speichermedium mit der Seriennummer 0E1145514041D91B am 17.12.2021 um 12:48:33 angeschlossen wurde.

SYSTEM	2021-12-17 12:48:33 CET		ROOT_HUB	4&2e134bf2&0	sus.E01
SYSTEM	2021-12-17 12:48:30 CET		ROOT_HUB30	5&1673f047&0&0	sus.E01
SYSTEM	2021-12-17 12:48:33 CET	Adomax Technology Co., Ltd	Product: 0001	28754-0000:00:01.2-1	sus.E01
SYSTEM	2021-12-17 12:48:33 CET	M-Systems Flash Disk Pioneers	TravelDrive 2C	0E1145514041D91B	sus.E01

Bild 60: Übersicht über die angeschlossenen USB-Geräte

Bilddateien auf dem Laptop



Name	Location	Size	MD5 Hash	Modified Time	Change Time	Access Time	Created Time
(current folder)	/img_sus_E01/vel_vol3/Users/jansen/Desktop/Kalender 2022	56		2021-12-17 11:48:59 MEZ	2021-12-17 11:48:59 MEZ	2021-12-17 11:49:06 MEZ	2021-12-17 11:48:59 MEZ
(parent folder)	/img_sus_E01/vel_vol3/Users/jansen/Desktop/Kalender 2022	376		2021-12-17 11:48:59 MEZ	2021-12-17 11:48:59 MEZ	2021-12-17 11:49:35 MEZ	2021-12-17 11:48:59 MEZ
DSC_001.jpeg	/img_sus_E01/vel_vol3/Users/jansen/Desktop/Kalender 2022/DSC_001.jpeg	147774	9da5b7202f87b81be324f0f89c760b7b	2021-12-12 14:55:46 MEZ	2021-12-17 11:48:59 MEZ	2021-12-17 11:49:06 MEZ	2021-12-17 11:48:59 MEZ
DSC_002.jpeg	/img_sus_E01/vel_vol3/Users/jansen/Desktop/Kalender 2022/DSC_002.jpeg	49255	074b919c71571fdd42169f07e673b089	2021-12-12 15:23:38 MEZ	2021-12-17 11:48:59 MEZ	2021-12-17 11:49:06 MEZ	2021-12-17 11:48:59 MEZ
DSC_003.jpeg	/img_sus_E01/vel_vol3/Users/jansen/Desktop/Kalender 2022/DSC_003.jpeg	159255	246c853ca7034eb7f4070763c4fa6ba6	2021-12-12 15:07:48 MEZ	2021-12-17 11:48:59 MEZ	2021-12-17 11:49:06 MEZ	2021-12-17 11:48:59 MEZ
DSC_004.jpeg	/img_sus_E01/vel_vol3/Users/jansen/Desktop/Kalender 2022/DSC_004.jpeg	213764	83b407c98a8ee7608a944213a08dc697	2021-12-12 15:28:14 MEZ	2021-12-17 11:48:59 MEZ	2021-12-17 11:49:06 MEZ	2021-12-17 11:48:59 MEZ
DSC_005.jpeg	/img_sus_E01/vel_vol3/Users/jansen/Desktop/Kalender 2022/DSC_005.jpeg	173635	dbf2ee178c353702a8a13631aca223f8	2021-12-12 15:24:08 MEZ	2021-12-17 11:48:59 MEZ	2021-12-17 11:49:06 MEZ	2021-12-17 11:48:59 MEZ
DSC_006.jpeg	/img_sus_E01/vel_vol3/Users/jansen/Desktop/Kalender 2022/DSC_006.jpeg	336590	e130ffd91d97fbaf3e82e14b1009d8ac	2021-12-12 15:09:34 MEZ	2021-12-17 11:48:59 MEZ	2021-12-17 11:49:06 MEZ	2021-12-17 11:48:59 MEZ
DSC_007.jpeg	/img_sus_E01/vel_vol3/Users/jansen/Desktop/Kalender 2022/DSC_007.jpeg	94994	d1b8136d8d009153acc5800ae41fc579	2021-12-12 15:23:22 MEZ	2021-12-17 11:48:59 MEZ	2021-12-17 11:49:06 MEZ	2021-12-17 11:48:59 MEZ
DSC_008.jpeg	/img_sus_E01/vel_vol3/Users/jansen/Desktop/Kalender 2022/DSC_008.jpeg	27099	554b287e802e1eae97b1f656e8b85607	2021-12-12 15:24:42 MEZ	2021-12-17 11:48:59 MEZ	2021-12-17 11:49:06 MEZ	2021-12-17 11:48:59 MEZ
DSC_009.jpeg	/img_sus_E01/vel_vol3/Users/jansen/Desktop/Kalender 2022/DSC_009.jpeg	148309	9229dc847d984bdbc5fe81ac6804e794	2021-12-12 15:20:00 MEZ	2021-12-17 11:48:59 MEZ	2021-12-17 11:49:06 MEZ	2021-12-17 11:48:59 MEZ
DSC_010.jpeg	/img_sus_E01/vel_vol3/Users/jansen/Desktop/Kalender 2022/DSC_010.jpeg	131761	367e011e99c8610b8b153d00b6789bfd	2021-12-12 15:24:56 MEZ	2021-12-17 11:48:59 MEZ	2021-12-17 11:49:06 MEZ	2021-12-17 11:48:59 MEZ
DSC_011.jpeg	/img_sus_E01/vel_vol3/Users/jansen/Desktop/Kalender 2022/DSC_011.jpeg	45866	892a4c27c5b7fe1809ef1fb80a696e06	2021-12-12 15:18:30 MEZ	2021-12-17 11:48:59 MEZ	2021-12-17 11:49:06 MEZ	2021-12-17 11:48:59 MEZ
DSC_012.jpeg	/img_sus_E01/vel_vol3/Users/jansen/Desktop/Kalender 2022/DSC_012.jpeg	46257	f8f3f3159eee154a14f609d51e751159	2021-12-12 15:25:18 MEZ	2021-12-17 11:48:59 MEZ	2021-12-17 11:49:06 MEZ	2021-12-17 11:48:59 MEZ

Bild 61: Bilddaten auf dem Laptop

Unter Verwendung der Suchfunktion von Autopsy nach Bilddateien konnten 12 Bilder im Ordner `C:/Users/jansen/Desktop/Kalender 2022` gefunden werden (Bild 61). Die Dateinamen und MD5-Hashes der Dateien sind in Tabelle 9 aufgelistet.

Tabelle 9: Bilddateien und ihre MD5-Hashes

Dateiname	MD5-Hashwert	Letzter Zugriff
DSC_001.jpeg	9da5b7202f87b81be324f0f89c760b7b	17.12.2021 12:49:06
DSC_002.jpeg	074b919c71571fdd42169f07e673b089	17.12.2021 12:49:06
DSC_003.jpeg	246c853ca7034eb7f4070763c4fa6ba6	17.12.2021 12:49:06
DSC_004.jpeg	83b407c98a8ee7608a944213a08dc697	17.12.2021 12:49:06
DSC_005.jpeg	dbf2ee178c353702a8a13631aca223f8	17.12.2021 12:49:06
DSC_006.jpeg	e130ffd91d97fbaf3e82e14b1009d8ac	17.12.2021 12:49:06
DSC_007.jpeg	d1b8136d8d009153acc5800ae41fc579	17.12.2021 12:49:06
DSC_008.jpeg	554b287e802e1eae97b1f656e8b85607	17.12.2021 12:49:06
DSC_009.jpeg	9229dc847d984bdbc5fe81ac6804e794	17.12.2021 12:49:06
DSC_010.jpeg	367e011e99c8610b8b153d00b6789bfd	17.12.2021 12:49:06
DSC_011.jpeg	892a4c27c5b7fe1809ef1fb80a696e06	17.12.2021 12:49:06
DSC_012.jpeg	f8f3f3159eee154a14f609d51e751159	17.12.2021 12:49:06

Um einen möglichen Zusammenhang zu dem gefundenen Bildmaterial in den zuvor untersuchten Asservaten zu prüfen, wurde in Autopsy ein Hashset aus den MD5-

Prüfsummen der auf diesem Datenträger gefundenen Dateien erstellt und auf den restlichen Datenträgern nach diesem gesucht. Es gab in allen Asservaten Übereinstimmungen mit dem Hashset (Bild 62). Das bedeutet, dass sich Dateien mit identischen Inhalten auf allen untersuchten Asservaten befanden.

File	File Path	Size	MD5 Hash	Modified Time	Changed Time	Accessed Time
DSC_002.jpeg	/LogicalFileSet1/www/html/nextcloud/data/admin/files_tra...	49555	074b919c71571fdd4216907e673b089	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00
DSC_002.jpeg	/img_stick.E01/Kalender 2022/DSC_002.jpeg	49555	074b919c71571fdd4216907e673b089	2021-12-12 14:23:38 MEZ	0000-00-00 00:00:00	2021-12-17 00:00:00 MEZ
DSC_002.jpeg	/img_chef.E01/vol_vol3/\$Recycle.Bin/S-1-5-21-4208391369...	49555	074b919c71571fdd4216907e673b089	2021-12-12 15:23:39 MEZ	2021-12-17 12:30:59 MEZ	2021-12-17 12:30:43 MEZ
DSC_002.jpeg	/img_sus.E01/vol_vol3/Users/jansen/Desktop/Karpenkalen...	49555	074b919c71571fdd4216907e673b089	2021-12-12 15:23:38 MEZ	2021-12-17 11:48:59 MEZ	2021-12-17 11:49:06 MEZ
DSC_003.jpeg	/img_stick.E01/Kalender 2022/DSC_003.jpeg	158024	246c853ca7034eb7f4070763c4fa6ba6	2021-12-12 14:07:44 MEZ	0000-00-00 00:00:00	2021-12-17 00:00:00 MEZ
DSC_003.jpeg	/LogicalFileSet1/www/html/nextcloud/data/admin/files_tra...	158024	246c853ca7034eb7f4070763c4fa6ba6	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00
DSC_003.jpeg	/img_sus.E01/vol_vol3/Users/jansen/Desktop/Karpenkalen...	158024	246c853ca7034eb7f4070763c4fa6ba6	2021-12-12 15:07:44 MEZ	2021-12-17 11:48:59 MEZ	2021-12-17 11:49:06 MEZ
DSC_003.jpeg	/img_chef.E01/vol_vol3/\$Recycle.Bin/S-1-5-21-4208391369...	158024	246c853ca7034eb7f4070763c4fa6ba6	2021-12-12 15:07:45 MEZ	2021-12-17 12:30:59 MEZ	2021-12-17 12:30:44 MEZ
DSC_010.jpeg	/img_chef.E01/vol_vol3/\$Recycle.Bin/S-1-5-21-4208391369...	131761	367e011e99c8610b8b153d00b6789bdf	2021-12-12 15:24:57 MEZ	2021-12-17 12:30:59 MEZ	2021-12-17 12:30:44 MEZ
_SC_01-1.JPG	/img_stick.E01/\$OrphanFiles/_SC_01-1.JPG	131761	367e011e99c8610b8b153d00b6789bdf	2021-12-12 14:24:56 MEZ	0000-00-00 00:00:00	2021-12-17 00:00:00 MEZ
DSC_010.jpeg	/LogicalFileSet1/www/html/nextcloud/data/admin/files_tra...	131761	367e011e99c8610b8b153d00b6789bdf	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00
DSC_010.jpeg	/img_sus.E01/vol_vol3/Users/jansen/Desktop/Karpenkalen...	131761	367e011e99c8610b8b153d00b6789bdf	2021-12-12 15:24:56 MEZ	2021-12-17 11:48:59 MEZ	2021-12-17 11:49:06 MEZ
DSC_008.jpeg	/img_sus.E01/vol_vol3/Users/jansen/Desktop/Karpenkalen...	27099	554b287e802e1eae97b1f656e8b85607	2021-12-12 15:24:42 MEZ	2021-12-17 11:48:59 MEZ	2021-12-17 11:49:06 MEZ
DSC_008.jpeg	/LogicalFileSet1/www/html/nextcloud/data/admin/files_tra...	27099	554b287e802e1eae97b1f656e8b85607	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00
_S96C3-1.JPG	/img_stick.E01/\$OrphanFiles/_S96C3-1.JPG	27099	554b287e802e1eae97b1f656e8b85607	2021-12-12 14:24:42 MEZ	0000-00-00 00:00:00	2021-12-17 00:00:00 MEZ
DSC_008.jpeg	/img_chef.E01/vol_vol3/\$Recycle.Bin/S-1-5-21-4208391369...	27099	554b287e802e1eae97b1f656e8b85607	2021-12-12 15:24:42 MEZ	2021-12-17 12:30:59 MEZ	2021-12-17 12:30:44 MEZ
DSC_004.jpeg	/img_chef.E01/vol_vol3/\$Recycle.Bin/S-1-5-21-4208391369...	211764	83b407c98a8ee7608a944213a08dc697	2021-12-12 15:26:14 MEZ	2021-12-17 12:30:59 MEZ	2021-12-17 12:30:44 MEZ
DSC_004.jpeg	/LogicalFileSet1/www/html/nextcloud/data/admin/files_tra...	211764	83b407c98a8ee7608a944213a08dc697	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00
DSC_004.jpeg	/img_stick.E01/Kalender 2022/DSC_004.jpeg	211764	83b407c98a8ee7608a944213a08dc697	2021-12-12 14:26:14 MEZ	0000-00-00 00:00:00	2021-12-17 00:00:00 MEZ
DSC_004.jpeg	/img_sus.E01/vol_vol3/Users/jansen/Desktop/Karpenkalen...	211764	83b407c98a8ee7608a944213a08dc697	2021-12-12 15:26:14 MEZ	2021-12-17 11:48:59 MEZ	2021-12-17 11:49:06 MEZ
DSC_011.jpeg	/img_sus.E01/vol_vol3/Users/jansen/Desktop/Karpenkalen...	45866	892a4c27c5b7e1809ef1fb80a696e06	2021-12-12 15:18:30 MEZ	2021-12-17 11:48:59 MEZ	2021-12-17 11:49:06 MEZ
DSC_011.jpeg	/LogicalFileSet1/www/html/nextcloud/data/admin/files_tra...	45866	892a4c27c5b7e1809ef1fb80a696e06	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00
_SC_01-2.JPG	/img_stick.E01/\$OrphanFiles/_SC_01-2.JPG	45866	892a4c27c5b7e1809ef1fb80a696e06	2021-12-12 14:18:30 MEZ	0000-00-00 00:00:00	2021-12-17 00:00:00 MEZ
DSC_011.jpeg	/img_chef.E01/vol_vol3/\$Recycle.Bin/S-1-5-21-4208391369...	45866	892a4c27c5b7e1809ef1fb80a696e06	2021-12-12 15:18:30 MEZ	2021-12-17 12:30:59 MEZ	2021-12-17 12:30:44 MEZ
DSC_009.jpeg	/img_chef.E01/vol_vol3/\$Recycle.Bin/S-1-5-21-4208391369...	146109	9229dc847d984dbdc5fe81ac6804e794	2021-12-12 15:20:01 MEZ	2021-12-17 12:30:59 MEZ	2021-12-17 12:30:44 MEZ
DSC_009.jpeg	/LogicalFileSet1/www/html/nextcloud/data/admin/files_tra...	146109	9229dc847d984dbdc5fe81ac6804e794	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00
DSC_009.jpeg	/img_sus.E01/vol_vol3/Users/jansen/Desktop/Karpenkalen...	146109	9229dc847d984dbdc5fe81ac6804e794	2021-12-12 15:20:00 MEZ	2021-12-17 11:48:59 MEZ	2021-12-17 11:49:06 MEZ
_S4A36-1.JPG	/img_stick.E01/\$OrphanFiles/_S4A36-1.JPG	146109	9229dc847d984dbdc5fe81ac6804e794	2021-12-12 14:20:00 MEZ	0000-00-00 00:00:00	2021-12-17 00:00:00 MEZ
DSC_001.jpeg	/img_chef.E01/vol_vol3/\$Recycle.Bin/S-1-5-21-4208391369...	147774	9da5b7202f87b81be324f0f9c760b7b	2021-12-12 14:55:46 MEZ	2021-12-17 12:30:59 MEZ	2021-12-17 12:30:43 MEZ
DSC_001.jpeg	/LogicalFileSet1/www/html/nextcloud/data/admin/files_tra...	147774	9da5b7202f87b81be324f0f9c760b7b	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00
DSC_001.jpeg	/img_stick.E01/Kalender 2022/DSC_001.jpeg	147774	9da5b7202f87b81be324f0f9c760b7b	2021-12-12 13:55:46 MEZ	0000-00-00 00:00:00	2021-12-17 00:00:00 MEZ
DSC_001.jpeg	/img_sus.E01/vol_vol3/Users/jansen/Desktop/Karpenkalen...	147774	9da5b7202f87b81be324f0f9c760b7b	2021-12-12 14:55:46 MEZ	2021-12-17 11:48:59 MEZ	2021-12-17 11:49:06 MEZ
DSC_001.jpeg	/img_chef.E01/vol_vol3/\$Recycle.Bin/S-1-5-21-4208391369...	94994	d1b81368d009153acc5800ae41fc579	2021-12-12 15:23:23 MEZ	2021-12-17 12:30:59 MEZ	2021-12-17 12:30:44 MEZ
DSC_007.jpeg	/img_stick.E01/Kalender 2022/DSC_007.jpeg	94994	d1b81368d009153acc5800ae41fc579	2021-12-12 14:23:22 MEZ	0000-00-00 00:00:00	2021-12-17 00:00:00 MEZ
DSC_007.jpeg	/LogicalFileSet1/www/html/nextcloud/data/admin/files_tra...	94994	d1b81368d009153acc5800ae41fc579	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00
DSC_007.jpeg	/img_sus.E01/vol_vol3/Users/jansen/Desktop/Karpenkalen...	94994	d1b81368d009153acc5800ae41fc579	2021-12-12 15:23:22 MEZ	2021-12-17 11:48:59 MEZ	2021-12-17 11:49:06 MEZ
DSC_005.jpeg	/img_sus.E01/vol_vol3/Users/jansen/Desktop/Karpenkalen...	172610	dbf2ee178c353702a8a13631aca223f8	2021-12-12 15:24:08 MEZ	2021-12-17 11:48:59 MEZ	2021-12-17 11:49:06 MEZ
DSC_005.jpeg	/LogicalFileSet1/www/html/nextcloud/data/admin/files_tra...	172610	dbf2ee178c353702a8a13631aca223f8	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00
DSC_005.jpeg	/img_stick.E01/Kalender 2022/DSC_005.jpeg	172610	dbf2ee178c353702a8a13631aca223f8	2021-12-12 14:24:08 MEZ	0000-00-00 00:00:00	2021-12-17 00:00:00 MEZ
DSC_005.jpeg	/img_chef.E01/vol_vol3/\$Recycle.Bin/S-1-5-21-4208391369...	172610	dbf2ee178c353702a8a13631aca223f8	2021-12-12 15:24:08 MEZ	2021-12-17 12:30:59 MEZ	2021-12-17 12:30:44 MEZ
DSC_006.jpeg	/LogicalFileSet1/www/html/nextcloud/data/admin/files_tra...	316590	e130ff9d1d97fba7e3e82e14b1009d8ac	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00
DSC_006.jpeg	/img_stick.E01/Kalender 2022/DSC_006.jpeg	316590	e130ff9d1d97fba7e3e82e14b1009d8ac	2021-12-12 14:09:34 MEZ	0000-00-00 00:00:00	2021-12-17 00:00:00 MEZ
DSC_006.jpeg	/img_sus.E01/vol_vol3/Users/jansen/Desktop/Karpenkalen...	316590	e130ff9d1d97fba7e3e82e14b1009d8ac	2021-12-12 15:09:34 MEZ	2021-12-17 11:48:59 MEZ	2021-12-17 11:49:06 MEZ
DSC_006.jpeg	/img_chef.E01/vol_vol3/\$Recycle.Bin/S-1-5-21-4208391369...	316590	e130ff9d1d97fba7e3e82e14b1009d8ac	2021-12-12 15:09:34 MEZ	2021-12-17 12:30:59 MEZ	2021-12-17 12:30:44 MEZ
_SC_01-3.JPG	/img_stick.E01/\$OrphanFiles/_SC_01-3.JPG	46257	fbf3f3159eee154a14f609d51e751159	2021-12-12 14:25:18 MEZ	0000-00-00 00:00:00	2021-12-17 00:00:00 MEZ
DSC_012.jpeg	/img_chef.E01/vol_vol3/\$Recycle.Bin/S-1-5-21-4208391369...	46257	fbf3f3159eee154a14f609d51e751159	2021-12-12 15:25:18 MEZ	2021-12-17 12:30:59 MEZ	2021-12-17 12:30:45 MEZ
DSC_012.jpeg	/img_sus.E01/vol_vol3/Users/jansen/Desktop/Karpenkalen...	46257	fbf3f3159eee154a14f609d51e751159	2021-12-12 15:25:18 MEZ	2021-12-17 11:48:59 MEZ	2021-12-17 11:49:06 MEZ
DSC_012.jpeg	/LogicalFileSet1/www/html/nextcloud/data/admin/files_tra...	46257	fbf3f3159eee154a14f609d51e751159	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00

Bild 62: Auflistung aller Übereinstimmungen mit dem Hashset

Veröffentlichung von Daten im Internet

Im Browserverlauf des Firefox ist der Aufruf der Image-Sharing-Plattform „Imgur“ (<https://imgur.com/>) zu finden. Des Weiteren sind Artefakte zu sehen (Bild 63), die auf das Hochladen von mehreren Bildern hinweisen.


	places.sqlite	https://imgur.com/	Imgur: The magic of the Internet	FireFox	imgur.com
	places.sqlite	https://imgur.com/upload	Imgur: The magic of the Internet	FireFox	imgur.com

Bild 63: Aufruf des Upload-Portals von Imgur im Browserverlauf

6 Details zur Untersuchungstechnik

In diesem Kapitel werden Untersuchungsschritte im Detail erläutert, die den Rahmen eines Gutachten sprengen würden und gegebenenfalls zu technisch für ein allgemein verständliches Dokument wie dieses ausfallen. Ein Großteil der Untersuchung konnte in den Programmen X-Ways und Autopsy durchgeführt werden. Allerdings verfügen diese Programme im Bezug auf Datenbanken nur stark beschränkte Funktionen, sodass an der Stelle andere Untersuchungsmethoden zum Einsatz kamen.

6.1 Festplattenimage des Dienstrechners

6.1.1 Nachweis einer bestehenden Verbindung zu einer Nextcloud

(Bezug S. 37)

Durch die Suche nach bekannten Installationsdateien (.msi, .exe) und installierten Programmordnern kann leicht die Existenz eines Programms im Betriebssystem nachgewiesen werden. Im Falle des Nextcloud-Clients reicht dies jedoch noch nicht aus, eine aktive Verbindung zu einem Nextcloud-Server aufzuzeigen. Beim Hinzufügen einer neuen Verbindung ruft der Client mit einem Internetbrowser den Web-Login der Cloud auf, über den sich der Nutzer anmelden muss. Nach geglückter Anmeldung antwortet der Nextcloud-Server mit einem JSON-Objekt wie beispielsweise in Listing 4.

```
{
  "server": "https://cloud.example.com",
  "loginName": "username",
  "appPassword": "
    yKTVA4zgxfivy52WqD8kW3M2pKGQr6srmUXMipRdunxjPFripJn0GMfmtN0q0o1YSuJ6sCN"
}
```

Listing 4: Beispiel einer erfolgreichen Authentifizierung des Nextcloud-Clients [3]

Wichtig ist hierbei der Schlüssel „appPassword“. Der Client authentifiziert sich beim Server nur über dieses Token, welches je nach Betriebssystem an einem unterschiedlichen Ort gespeichert wird. Das erfolgreiche Beziehen des Passworts wird in der Logdatei des Clients vermerkt (Bild 64). Windows 10 speichert das Passwort im *Credential Manager* (Bild 65). Somit besteht nach erstmaliger Anmeldung eines Nutzers so lange eine valide Verbindung, die keines weiteren Identitätsnachweises bedarf, bis sie manuell beendet wird.


```
# timestamp | duration | file | instruction | dir | modtime | etag | size | fileId |
status | errorString | http result code | other size | other modtime | X-Request-
ID
##-##-## Syncrun started 2021-12-17T11:05:22Z
##-##-##-## Propagation starts 2021-12-17T11:05:23Z (last step: 1590 msec, total: 1590
msec)
||Kalender 2022|8|2|1639320839|61b60d0920b8b|0|00000259ocmrrox1f0j5|4||0|0|0||
11:05:25||Kalender 2022/DSC_001.jpeg|8|2|1639317346|64cbddf749b15479f277c03b86d3eed9
|147774|00000317ocmrrox1f0j5|4||200|0|0|a60161d9-b603-4b41-be1d-9d84f1542301|
11:05:26||Kalender 2022/DSC_004.jpeg|8|2|1639319174|ec838365ebe717a8aa352e87c649123f
|211764|00000269ocmrrox1f0j5|4||200|0|0|cca1d849-1a5c-4da7-9003-12facadfb5f9|
11:05:26||Kalender 2022/DSC_002.jpeg|8|2|1639319019|104a145d0d261c99b704f0ba55eadc41
|49555|00000276ocmrrox1f0j5|4||200|0|0|a127e9b6-d09e-4db3-ac82-c055cc8cd22c|
11:05:26||Kalender 2022/DSC_003.jpeg|8|2|1639318065|a395f9e4af4f08998c0b3b92476a49aa
|158024|00000267ocmrrox1f0j5|4||200|0|0|38397ce0-a1a7-4f46-92e9-585232566090|
11:05:27||Kalender 2022/DSC_005.jpeg|8|2|1639319048|b2ef2fe7e71a603e302614df5cbf3f42
|172610|00000316ocmrrox1f0j5|4||200|0|0|8a500fa5-34ef-4467-8a7d-5b69f5e47aa8|
11:05:28||Kalender 2022/DSC_007.jpeg|8|2|1639319003|3939372613e3535faa0f58cc270f6045
|94994|00000296ocmrrox1f0j5|4||200|0|0|7b176c9e-c9c0-4136-a055-0c7a41c175e7|
11:05:28||Kalender 2022/DSC_008.jpeg|8|2|1639319082|7fe7daa76d0e9c1d8466363697919256
|27099|00000268ocmrrox1f0j5|4||200|0|0|a29fc20d-da6b-4347-b75e-10182740a959|
11:05:28||Kalender 2022/DSC_006.jpeg|8|2|1639318174|591e2132215272f168f1fc022a15ba97
|316590|00000282ocmrrox1f0j5|4||200|0|0|c668f751-1324-4a27-a019-fd39bd67ebbb|
11:05:28||Kalender 2022/DSC_009.jpeg|8|2|1639318801|05529a18875d378a47ea9821ad57f63c
|146109|00000305ocmrrox1f0j5|4||200|0|0|b1d659c7-0b6f-4742-b99f-4e8b671cbb3a|
11:05:29||Kalender 2022/DSC_010.jpeg|8|2|1639319097|8b0acea6a3f81112ed87b1d634e01619
|131761|00000279ocmrrox1f0j5|4||200|0|0|f268a375-8a72-4740-8636-0c1867915557|
11:05:30||Kalender 2022/DSC_011.jpeg|8|2|1639318710|351b6ba7e857af1e87e5ee18df668f57
|45866|00000280ocmrrox1f0j5|4||200|0|0|9a0ed03f-83f5-4216-8cc6-a774f17d63ec|
11:05:30||Kalender 2022/DSC_012.jpeg|8|2|1639319118|7ce063f69535c5b031caaf82258fe5f4
|46257|00000265ocmrrox1f0j5|4||200|0|0|bff380d8-f8de-4bde-b7d1-989471bd6d4b|
##-##-## Syncrun finished 2021-12-17T11:05:32Z (last step: 8308 msec, total: 9899 msec)
##-##-## Syncrun started 2021-12-17T11:31:01Z
##-##-##-## Propagation starts 2021-12-17T11:31:02Z (last step: 455 msec, total: 455
msec)
11:31:07||Kalender 2022|2|1|1639320839|61b60d0920b8b|0|00000259ocmrrox1f0j5
|4||204|0|1639320839|aefea4e5-41e7-4c79-a8be-6f20876c3d77|
##-##-## Syncrun finished 2021-12-17T11:31:06Z (last step: 4315 msec, total: 4771 msec)
##-##-## Syncrun started 2021-12-17T11:31:38Z
##-##-##-## Propagation starts 2021-12-17T11:31:38Z (last step: 124 msec, total: 124
msec)
##-##-## Syncrun finished 2021-12-17T11:31:38Z (last step: 6 msec, total: 130 msec)
```

Listing 5: Synchronisations-Log des Nextcloud-Clients

Die Bedeutung dieser Codes geht aus dem Quelltext des Nextcloud-Clients hervor (Listing 6). Eine 8 steht für die Erzeugung einer neuen Datei, die 2 für eine Löschung.

```
$ git clone https://github.com/nextcloud/desktop && cd desktop
$ grep -r -i "instruction" ./src
./src/csync/csync.h: CSYNC_INSTRUCTION_NONE = 0, /* Nothing to do
(UPDATE|RECONCILE) */
./src/csync/csync.h: CSYNC_INSTRUCTION_EVAL = 1 << 0, /* There was
changed compared to the DB (UPDATE) */
```

```

./src/csync/csync.h:    CSYNC_INSTRUCTION_REMOVE        = 1 << 1, /* The file need
    to be removed (RECONCILE) */
./src/csync/csync.h:    CSYNC_INSTRUCTION_RENAME          = 1 << 2, /* The file need
    to be renamed (RECONCILE) */
./src/csync/csync.h:    CSYNC_INSTRUCTION_EVAL_RENAME       = 1 << 11, /* The file is
    new, it is the destination of a rename (UPDATE) */
./src/csync/csync.h:    CSYNC_INSTRUCTION_NEW            = 1 << 3, /* The file is
    new compared to the db (UPDATE) */
./src/csync/csync.h:    CSYNC_INSTRUCTION_CONFLICT        = 1 << 4, /* The file need
    to be downloaded because it is a conflict (RECONCILE) *

```

Listing 6: Erläuterung der „Instruction“-Codes

Weitere Informationen über gelöschte Dateien können aus der lokalen SQLite-DB des Nextcloud-Clients bezogen werden. Diese Datenbank befindet sich im synchronisierten Verzeichnis. Wird diese Datenbank mit einem Programm geöffnet, welches SQLite-Datenbanken einlesen kann (z. B. der SQLite-Browser oder die in Autopsy eingebaute Funktion dafür), werden die gelöschten Einträge jedoch nicht gezeigt. Sie können aber mit einem Hex-Editor in der Datenbankdatei gefunden werden.

6.2 Snapshot des Nextcloud-Servers

6.2.1 Extraktion einer Datenbank aus einem Container-Snapshot

Ein Nextcloud-Server ist eine klassische LAMP-Anwendung und baut in der Regel auf einer MariaDB- oder MySQL-Datenbank auf. Deshalb bietet sich eine Datenbank-zentrierte Untersuchung solcher Systeme an. Die Zugangsdaten zur Datenbank sind in der Konfigurationsdatei der Cloud (`config.php`) gespeichert.

Im hier betrachteten Szenario befindet sich die Datenbank in einem LXC-Container. Da ein Container-Snapshot lediglich ein komprimiertes Abbild des gesamten Dateibaums ist, kann das Datenbank-Verzeichnis (auffindbar durch Suche in der Serverkonfiguration oder nach bekannten Pfaden) aus dem Archiv extrahiert werden. Für die Untersuchung der Datenbank wurde hier die Containervirtualisierungssoftware Docker beziehungsweise das Äquivalent Podman verwendet. Durch den Einsatz eines MariaDB-Containers wird die Einrichtung eines Datenbank-Klons deutlich vereinfacht. Das vorher extrahierte Datenbankverzeichnis kann als Volume anstelle des Standardverzeichnisses in den Container einbezogen werden. Nach Erzeugung des Containers kann die Datenbank mit der MariaDB-Kommandozeilenanwendung durchsucht werden. Listing 7 zeigt diesen Prozess. Die Syntax ist für `podman` und

`docker` identisch. Auf diese Weise wurde ein Großteil der Untersuchung bezüglich der Nextcloud in dieser Arbeit durchgeführt.

```
$ tar --use-compress-program=unzstd -xvf vzdump.tar.zst ./var/lib/mysql
$ podman run --name ncdb -e MYSQL_ROOT_PASSWORD=secret -p 3307:3306 -d mariadb:10.4 -v
  ./var/lib/mysql:/var/lib/mysql
$ podman exec -it ncdb bash
# mariadb
```

Listing 7: Erzeugung eines Datenbankklons mittels Docker

Hinweis zur Extraktion des Snapshots

Unter GNU/Linux-Betriebssystemen sei darauf zu achten, möglichst nicht das gesamte Dateisystem aus dem Snapshot ins lokale Dateisystem zu extrahieren. Im Snapshot können sich Softlinks befinden, die Verknüpfungen zu Dateien im eigenen Betriebssystem herstellen. Wird der Snapshot dann in einem Programm wie Autopsy eingelesen, werden Dateien vom Untersuchungsrechner in die Untersuchung mit einbezogen, was unter allen Umständen vermieden werden muss.

6.2.2 Einrichtung eines Containerklons aus dem Snapshot

Metadaten in LXC-Containern

Es kann im Rahmen einer Untersuchung hilfreich sein, einen LXC-Snapshot in einem Hex-Editor zu öffnen, da sich im Dateiheder des Archivs die Konfiguration des Containers, Zeitstempel und weitere Metadaten befinden. Ein ausführlicher Auszug solcher Daten ist in Anhang E gelistet.

vzdump-lxc-102-2021_12_2...		chef	
Name		Description	Size
vzdump-lxc-102-2021_12_20-18_43_21.tar existing			1,7 GB
Created		20.01.2022	12:51:38
Modified		20.01.2022	12:22:26
Volume	File	Preview	Details
Offset	0 1 2 3 4 5 6 7	8 9 A B C D E F	ANSI ASCII
00000600	61 72 63 68 3A 20 61 6D	64 36 34 0A 63 6F 72 65	arch: amd64 core
00000610	73 3A 20 38 0A 66 65 61	74 75 72 65 73 3A 20 66	s: 8 features: f
00000620	75 73 65 3D 31 2C 6D 6F	75 6E 74 3D 6E 66 73 3B	use=1,mount=nfs;
00000630	63 69 66 73 2C 6E 65 73	74 69 6E 67 3D 31 0A 68	cifs,nesting=1 h
00000640	6F 73 74 6E 61 6D 65 3A	20 6E 65 78 74 63 6C 6F	ostname: nextclo
00000650	75 64 2E 73 68 6F 75 2E	64 65 76 0A 6D 65 6D 6F	ud. .dev memo
00000660	72 79 3A 20 32 30 34 38	0A 6E 65 74 30 3A 20 6E	ry: 2048 net0: n
00000670	61 6D 65 3D 65 74 68 30	2C 62 72 69 64 67 65 3D	ame=eth0,bridge=
00000680	76 6D 62 72 30 2C 66 69	72 65 77 61 6C 6C 3D 31	vmbr0,firewall=1
00000690	2C 67 77 3D 31 39 32 2E	31 36 38 2E 31 2E 31 2C	,gw=192.168.1.1,
000006A0	68 77 61 64 64 72 3D 39	45 3A 31 34 3A 38 30 3A	hwaddr=9E:14:80:
000006B0	32 44 3A 37 38 3A 46 42	2C 69 70 3D 31 39 32 2E	2D:78:FB,ip=192.
000006C0	31 36 38 2E 31 2E 35 31	2F 32 34 2C 74 79 70 65	168.1.51/24,type
000006D0	3D 76 65 74 68 0A 6F 73	74 79 70 65 3A 20 64 65	=veth ostype: de
000006E0	62 69 61 6E 0A 72 6F 6F	74 66 73 3A 20 48 44 44	bian rootfs: HDD
000006F0	30 31 3A 31 30 32 2F 76	6D 2D 31 30 32 2D 64 69	01:102/vm-102-di
00000700	73 6B 2D 30 2E 72 61 77	2C 73 69 7A 65 3D 33 32	sk-0.raw,size=32
00000710	47 0A 73 77 61 70 3A 20	32 30 34 38 0A 00 00 00	G swap: 2048

Bild 66: Metadaten eines LXC-Containers

Eine weitere Möglichkeit zur Untersuchung eines LXC-Containers ist die Erzeugung einer Kopie dessen in einer lokalen Proxmox VE-Umgebung². Um einen neuen Container aus einem Snapshot zu generieren, muss der Snapshot in das im Vorfeld konfigurierte Backup-Verzeichnis von Proxmox VE kopiert werden. Dieses liegt in der Regel unter `SPEICHERMEDIUM/dumps/`. Zur Instanziierung eines neuen Containers auf Basis eines Snapshots wird die *Restore* Funktion verwendet, indem ein Snapshot als Backup eines Containers angesehen und daraus wiederhergestellt wird. Dabei werden alle aktuellen Daten dieses Containers verworfen und die Daten des Snapshots eingelesen [4].

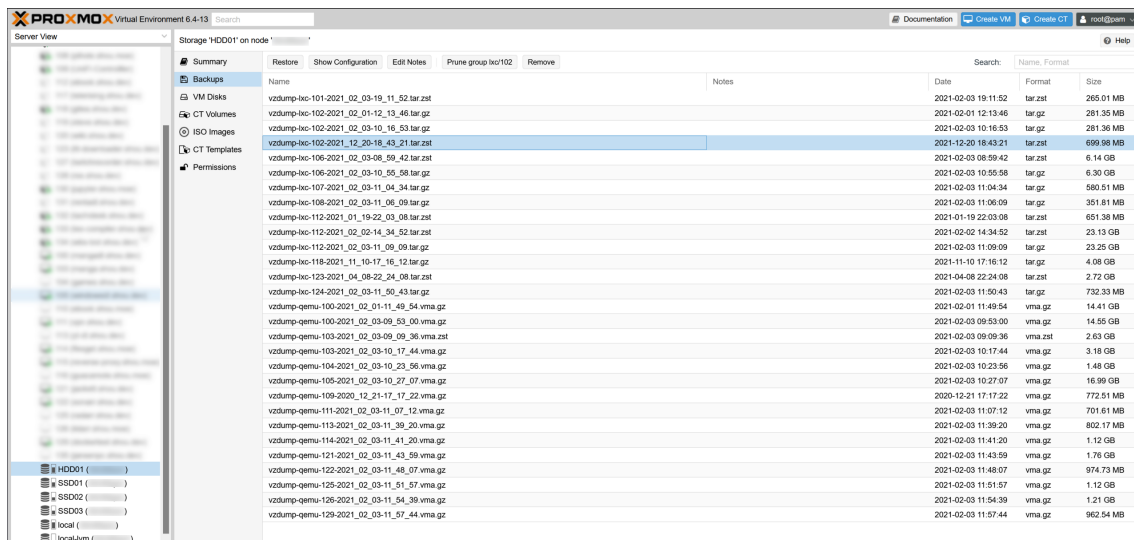


Bild 67: Einlesen des Snapshots

Innerhalb des Webinterface ist dieser Snapshot verfügbar und kann weiterverwendet werden.

²Alternativ zu einer vollständigen Proxmox VE-Umgebung kann ein LXC-Container ebenfalls mit dem `virt-manager` (siehe Kapitel 3) erzeugt werden.

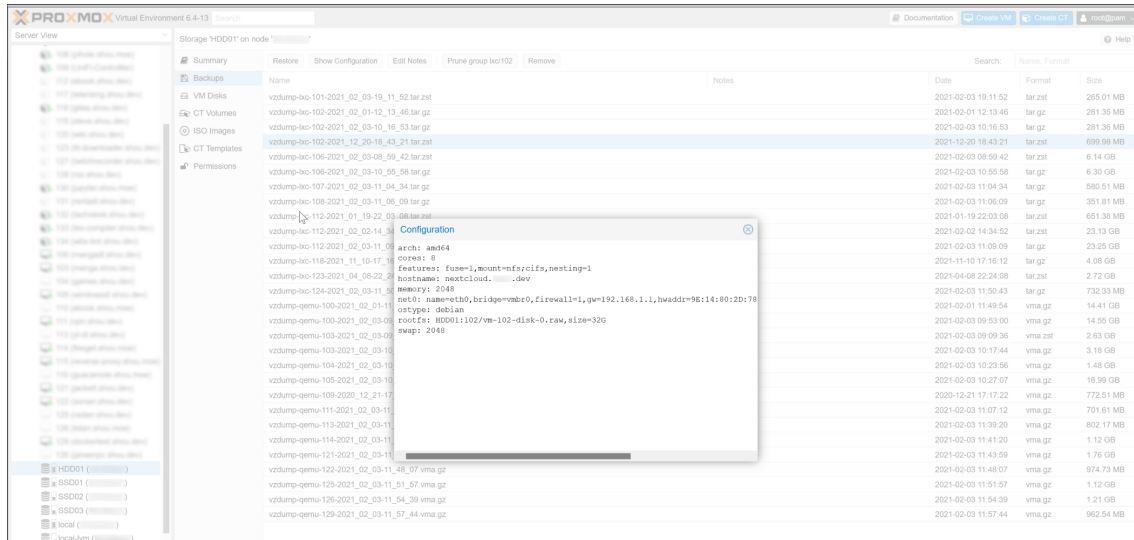


Bild 68: Konfiguration des Containers

Zur Instanziierung eines Containers wird eine Konfigurationsdatei benötigt. Während der Instanziierung des Snapshots wird die letzte mit dem Snapshot in Verbindung gebrachte Konfiguration genutzt. Der Snapshot wird über die in den Archivmetadaten gespeicherten Containerkonfiguration identifiziert. Sollte bereits eine Konfiguration vorhanden sein, liegt diese unter `/etc/pve/lxc` und kann auf Wunsch angepasst werden.

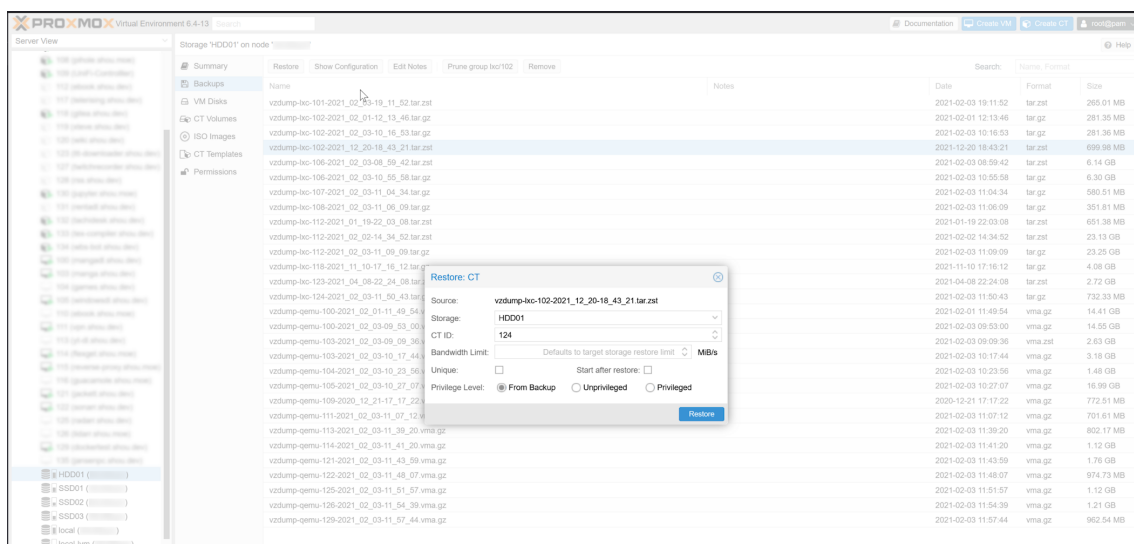


Bild 69: Instanziierung eines neuen Containers

Für die Instanziierung eines neuen Containers muss eine freie Container-ID, sowie ein Speicherort für den Container vergeben werden. Sofern dies geschehen ist, kann der Container verwendet werden. Es ist zu beachten, dass ein Container bei der

Wiederherstellung in den Zustand nach einem frischen Boot versetzt wird. Das bedeutet, dass lediglich Prozesse aktiv sind, die mit für den *Autostart* gekennzeichnet sind.

6.2.3 Anmeldeversuche

(Bezug S. 45)

Gescheiterte oder verdächtige Anmeldeversuche in einer Nextcloud können direkt aus ihrer Datenbank abgelesen werden. Die Tabelle `oc_bruteforce_attempts` speichert alle fehlgeschlagenen Anmeldeversuche (Bild 70).

```
> select * from oc_bruteforce_attempts;
```

id	action	occurred	ip	subnet	metadata
1	login	1639739825	192.168.1.11	192.168.1.11/32	{"user":"admin"}
2	login	1639739837	192.168.1.11	192.168.1.11/32	{"user":"admin"}
3	login	1639739858	192.168.1.11	192.168.1.11/32	{"user":"admin"}
4	login	1639739884	192.168.1.11	192.168.1.11/32	{"user":"admin"}
5	login	1639739899	192.168.1.11	192.168.1.11/32	{"user":"admin"}

Bild 70: Bruteforce-Versuche in der Nextcloud-Datenbank

6.2.4 Veränderung des Datenbestands

(Bezug S. 46)

Nextcloud verfügt über ein eigenes Plugin-System, in diesem Kontext „Apps“ genannt. Zu den standardmäßig installierten Apps einer Nextcloud gehört auch der „Papierkorb“ [5]. Diese App verhindert, dass Daten sofort gelöscht werden. Sobald eine Datei gelöscht wird, verschwindet sie zwar aus dem Datenbestand des Nutzers, existiert aber dennoch im Dateisystem. Gelöschte Daten werden, sofern nicht anders konfiguriert, bis zu 30 Tage nach der Löschung vorbehalten und in der Datenbanktabelle `oc_files_trash` vermerkt (Bild 71).

```
> SELECT * FROM oc_files_trash;
```

auto_id	id	user	timestamp	location	type	mime
1	Nextcloud.png	admin	1639320509	.	NULL	NULL
2	Photos	admin	1639320509	.	NULL	NULL
3	Nextcloud intro.mp4	admin	1639320510	.	NULL	NULL
4	Documents	admin	1639320510	.	NULL	NULL
5	Templates	admin	1639320509	.	NULL	NULL
6	Nextcloud Manual.pdf	admin	1639320514	.	NULL	NULL
7	Reasons to use Nextcloud.pdf	admin	1639320515	.	NULL	NULL
8	Kalender 2022	admin	1639740663	.	NULL	NULL

Bild 71: Gelöschte Dateien in der Nextcloud-Datenbank

Zusätzlich gibt es die Tabelle `oc_filecache` (Bild 72), in der die vollständigen Dateipfade zuletzt verwendeter Dateien aufgelistet werden. Daraus ist der Speicherort vermeindlich gelöschter Dateien abzulesen.

```
> SELECT fileid, path, name FROM oc_filecache;
```

fileid	path	name
259	files_trashbin/files/Kalender 2022.d1639740663	Kalender 2022.d1639740663
265	files_trashbin/files/Kalender 2022.d1639740663/DSC_012.jpeg	DSC_012.jpeg
267	files_trashbin/files/Kalender 2022.d1639740663/DSC_003.jpeg	DSC_003.jpeg
268	files_trashbin/files/Kalender 2022.d1639740663/DSC_008.jpeg	DSC_008.jpeg
269	files_trashbin/files/Kalender 2022.d1639740663/DSC_004.jpeg	DSC_004.jpeg
276	files_trashbin/files/Kalender 2022.d1639740663/DSC_002.jpeg	DSC_002.jpeg
279	files_trashbin/files/Kalender 2022.d1639740663/DSC_010.jpeg	DSC_010.jpeg
280	files_trashbin/files/Kalender 2022.d1639740663/DSC_011.jpeg	DSC_011.jpeg
282	files_trashbin/files/Kalender 2022.d1639740663/DSC_006.jpeg	DSC_006.jpeg
296	files_trashbin/files/Kalender 2022.d1639740663/DSC_007.jpeg	DSC_007.jpeg
305	files_trashbin/files/Kalender 2022.d1639740663/DSC_009.jpeg	DSC_009.jpeg
316	files_trashbin/files/Kalender 2022.d1639740663/DSC_005.jpeg	DSC_005.jpeg
317	files_trashbin/files/Kalender 2022.d1639740663/DSC_001.jpeg	DSC_001.jpeg

Bild 72: Datei-Cache in der Nextcloud-Datenbank

Dateilöschungen sind aus den Inhalten der Tabelle `oc_activity` ersichtlich.

```
> SELECT activity_id, timestamp, type, subject, file FROM oc_activity WHERE timestamp > 1639320514;
```

activity_id	timestamp	type	subject	file
41	1639320823	file_created	created_self	/bilder
42	1639320829	file_created	created_self	/bilder/DSC_012.jpeg
43	1639320830	file_created	created_self	/bilder/DSC_008.jpeg
44	1639320830	file_created	created_self	/bilder/DSC_003.jpeg
45	1639320830	file_created	created_self	/bilder/DSC_004.jpeg
46	1639320835	file_created	created_self	/bilder/DSC_002.jpeg
47	1639320835	file_created	created_self	/bilder/DSC_010.jpeg
48	1639320836	file_created	created_self	/bilder/DSC_011.jpeg
49	1639320836	file_created	created_self	/bilder/DSC_006.jpeg
50	1639320840	file_created	created_self	/bilder/DSC_007.jpeg
51	1639320841	file_created	created_self	/bilder/DSC_009.jpeg
52	1639320841	file_created	created_self	/bilder/DSC_005.jpeg
53	1639320841	file_created	created_self	/bilder/DSC_001.jpeg
54	1639320858	file_changed	renamed_self	//Kalender 2022
55	1639740663	file_deleted	deleted_self	/Kalender 2022

Bild 73: Aktivitäten in der Nextcloud-Datenbank

Nutzerkonten in der Cloud

(Bezug S. 46)

Mithilfe der *Restore*-Funktion von Proxmox VE wurde aus dem Snapshot des Containers eine neue Containerinstanz der Nextcloud erstellt. Zur Analyse der Nextcloud-Umgebung wurde die bereits extrahierte Datenbank verwendet (siehe Abschnitt 6.2.1). Zur Einsicht aller auf der Cloud verfügbaren Nutzer wird die Tabelle `oc_users` aus der Datenbank `nextcloudb` untersucht. Mit einer einfachen `SELECT`-Anfrage wird ersichtlich, dass es nur einen Nutzer names „admin“ der Gruppe „admin“ gibt (siehe Bild 74).


```

MariaDB [nextclouddb]> SELECT * FROM oc_users;
+-----+-----+-----+-----+
| uid | displayname | password | uid_lower |
+-----+-----+-----+-----+
| admin | NULL | 3|Sargon2id$v=19$m=65536,t=4,p=1$M2ltS003NkdDam14U1VYbg$Mf+T7Bue2HkfcIBozlo1vHr3XgWBgfk1Of+7cGIFNPM | admin |
+-----+-----+-----+-----+
1 row in set (0.000 sec)

```

Bild 74: Auslesen der Tabelle oc_users

Daraus lässt sich schließen, dass es keine weiteren Nutzer in der Cloud-Umgebung gibt, die auf die gestohlenen Daten hätten Zugriff haben können.

Analyse geteilter Daten

(Bezug S. 46)

Um zu untersuchen, welche Daten entweder mit einem anderen Nutzer der Cloud geteilt oder über einen privaten Zugriffslink zugänglich gemacht wurden, konnte ebenfalls die Datenbank in Betracht gezogen werden. Alle geteilten Daten sind ersichtlich, indem man die Tabellen `oc_share` und `oc_share_external` auswertet. Werden beide Tabellen mithilfe des `SELECT`-Befehls ausgelesen (Bild 75), wird ersichtlich, dass es keine Einträge diesbezüglich gibt. Hieraus ist zu erkennen, dass es keine geteilten Daten auf der Cloud-Umgebung gibt und somit auch kein externer Zugriff auf die Daten erfolgen konnte.

```

MariaDB [nextclouddb]> SELECT * FROM oc_share;
Empty set (0.000 sec)

MariaDB [nextclouddb]> SELECT * FROM oc_share_external;
Empty set (0.000 sec)

```

Bild 75: Auslesen der Tabellen oc_share und oc_share_external

6.3 USB-Stick

(Bezug S. 48)

Für die Untersuchung des USB-Sticks und ob dieser mit dem Asservat 01 verbunden war, wurden unter anderem Programme aus TSK verwendet. Auf dem Analyse-PC (Ubuntu 20.04) wurde ebenfalls mit Autopsy gearbeitet, was hier zu Problemen führte. Autopsy benötigt seine eigene Version von TSK, `sleuthkit-java`, die nicht parallel zur TSK-Installation aus den offiziellen Paketquellen existieren kann (Bild 76).


```

root@forensik-pc:/mnt/evidence/2021/0001/3$ apt install sleuthkit
Paketlisten werden gelesen... Fertig
Abhängigkeitsbaum wird aufgebaut.
Statusinformationen werden eingelesen.... Fertig
Starting pkgProblemResolver with broken count: 1
Starting 2 pkgProblemResolver with broken count: 1
Investigating (0) sleuthkit-java:amd64 < 4.11.1-1 @ii mK Ib >
Broken sleuthkit-java:amd64 Kollidiert mit on libtsk13:amd64 < none -> 4.6.7-1build1 @un uN >
  Considering libtsk13:amd64 -1 as a solution to sleuthkit-java:amd64 -2
  Removing sleuthkit-java:amd64 rather than change libtsk13:amd64
Done
Die folgenden zusätzlichen Pakete werden installiert:
  libdate-manip-perl libtsk13
Vorgeschlagene Pakete:
  autopsy mac-robber
Die folgenden Pakete werden ENTFERNT:
  sleuthkit-java
Die folgenden NEUEN Pakete werden installiert:
  libdate-manip-perl libtsk13 sleuthkit

```

Bild 76: Paketkonflikt zwischen verschiedenen TSK-Versionen

Um trotzdem beide Werkzeuge nutzen zu können, wurde auf Distrobox³ zurückgegriffen. Diese Docker-basierte Umgebung ermöglicht es, den Userspace einer anderen GNU/Linux-Installation innerhalb des aktuellen Betriebs- und Dateisystems zu verwenden. Die Einrichtung einer neuen Forensik-Distrobox zeigt Listing 8. Dadurch wurde die Nutzung der TSK-Werkzeuge für kleinere Untersuchungsschritte trotz vorhandener Autopsy-Installation realisiert.

```

$ sudo distrobox-create -n tsx -i docker.io/kalilinux/kali-rolling:latest
$ sudo distrobox-enter -n tsx
# apt install -y sleuthkit

```

Listing 8: Benutzung von Distrobox

³<https://distrobox.privatedns.org/>

7 Zusammenfassung und Ausblick

7.1 Zusammenfassung

In diesem Projekt wurde ein Datendiebstahlsfall inszeniert (Kapitel 2, 4 und 3) und die daran beteiligten Geräte einer IT-forensischen Analyse unterzogen (Kapitel 5). Informationen zu den genutzten Untersuchungstechniken wurden in Kapitel 6 gegeben. Dabei kamen verschiedene Ermittlungsmethoden zum Einsatz. Es wurden Spuren auf Kommandozeilenebene durch die Werkzeuge aus TSK aus den Images extrahiert, welche eine granuläre Kontrolle über den Arbeitsablauf erlauben. Mit dem grafischen Frontend Autopsy für diese Programmsammlung konnte ein größerer Pool möglicher Spuren deutlich schneller zu Verfügung gestellt werden, weil spezielle Artefakte nicht erst manuell ausfindig gemacht werden mussten, sondern automatisch vom Programm bereitgestellt wurden. Ein weiteres grafisches Forensik-Programm, X-Ways Forensics, ließ sich im Rahmen dieser Arbeit nur schwer einsetzen. Während X-Ways Forensics besonders für Untersuchungen auf Byte-Ebene geeignet ist, lag der Hauptschwerpunkt dieser Arbeit auf der Suche nach bekannten Dateien und deren Analyse. Aus diesem Grund konnte das volle Potenzial von X-Ways Forensics nicht ausgeschöpft werden und Autopsy lieferte in kürzerer Zeit verwertbarere Ergebnisse, wenn auch dessen Hex-Editor qualitativ nicht auf dem Niveau von Win-Hex ist. Außerdem wurde zur Auswertung der relationalen Datenbank in dem hier betrachteten Szenario ein Rekonstruktionsprozess mittels Docker vorgestellt.

Einen wichtigen Teil des Geschehens stellten die Aktivitäten innerhalb eines Servers dar, der als LXC-Container virtualisiert wurde. Während der Bearbeitung des Vorfalls stellte sich heraus, dass zwar der Umgang mit Containern mit volatilem Dateisystem (z. B. Docker) hinreichend dokumentiert ist, die forensische Analyse von Containern mit persistentem Dateisystem hingegen in der Fachliteratur bisher stark vernachlässigt wurde und dementsprechend Grundlagen zur Handhabung solcher Spureenträger fehlen.

Die Signifikanz korrekter Zeitzoneneinordnungen sei an dieser Stelle abschließend hervorgehoben. Im Image des untersuchten Laptops trat – obwohl die virtuelle Maschine richtig konfiguriert wurde – eine inkorrekte Zeitverschiebung auf. Manche Zeitstempel waren um eine Stunde nach hinten verschoben, andere wiederum stimmten mit den Uhren der anderen Geräte überein. Dieses Problem konnte in Autopsy nicht korrigiert werden, weshalb einigen Spuren angepasst werden mussten, um die

Kontinuität der Untersuchung aufrecht zu erhalten. In der Praxis wird davon dringend abgeraten; stattdessen sollten Spurenträger und Analysesoftware noch einmal genauestens überprüft werden.

Während der Untersuchung stellte sich heraus, dass Nachweise für Kopiervorgänge zwischen einem Computer und einem USB-Stick nicht wirklich offensichtlich sind, wenn diese Arten von Ereignissen nicht im Vorfeld ausdrücklich mitgeschnitten werden. Zwar bietet sich alternativ der Vergleich von Seriennummern an, um ein USB-Speichermedium trotzdem mit einem Computer in einen Zusammenhang zu bringen, allerdings ist dabei zumindest der echte Datenträger für die Untersuchung nötig, da dessen Seriennummer für gewöhnlich nicht in ein Image eingebettet wird. Eine Information, die meist sowohl auf dem Speichermedium als auch auf dem Computer zu finden ist, ist die Dateisystembezeichnung („Label“). Diese Spur sollte allerdings mit Vorsicht betrachtet werden, weil die Bezeichnung eines Datenträgers leicht geändert werden kann. Besonders aufschlussreich waren die Informationen, die aus der Laufzeitumgebung des Nextcloud-Clients und der Datenbank des Nextcloud-Servers gewonnen werden konnten, auch ohne nennenswerte strategische Vorbereitung. Dagegen zeigte sich aber, dass wegen der Netzwerkarchitektur des imaginären Rechenzentrums, in dem sich der Server befand, kein Bezug zwischen Angreifer und Cloud auf Grundlage der IP-Adressen hergestellt werden konnte. Aus dem Image des Angreifers konnte lediglich die IP-Adresse aus dem Heimnetz entnommen werden, die in einem solchen Fall nicht von Bedeutung ist, und der Reverse-Proxy im Rechenzentrum verschleierte sämtliche Zugriffe von außerhalb hinter seiner eigenen netzinternen Adresse. Abhilfe in solchen Fällen schafft nur die zusätzliche Untersuchung der Infrastruktur des IT-Dienstleisters, was die Komplexität der Analyse deutlich erhöht.

Insgesamt konnten dennoch aus vielen anderen Spuren nützliche Erkenntnisse gezogen werden, um den Tathergang zu rekonstruieren. Alle Fragestellungen des Gutachtens konnten eingehend beantwortet werden, weshalb die Untersuchung als Erfolg betrachtet wird.

7.2 Ausblick

Die stetig wachsende Landschaft der Containervirtualisierung wurde in der IT-Forensik noch nicht ausreichend betrachtet. Während Container mit volatilem Speicher vermehrt für die Containerisierung von Anwendungen eingesetzt werden, werden Container mit persistentem Dateisystem mit steigender Beliebtheit oft als Ersatz

für vollwertige virtuelle Maschinen eingesetzt. Allerdings fehlt es an umfangreichen Betrachtungen der Container im Rahmen von forensischen Analysen. Deshalb wird eine umfangreiche Untersuchung von LXC beziehungsweise LXD sowie weiteren Containervirtualisierungslösungen unter dem Aspekt des Mehrwerts für die IT-Forensik empfohlen.

A Einrichtung einer KVM mit virt-manager

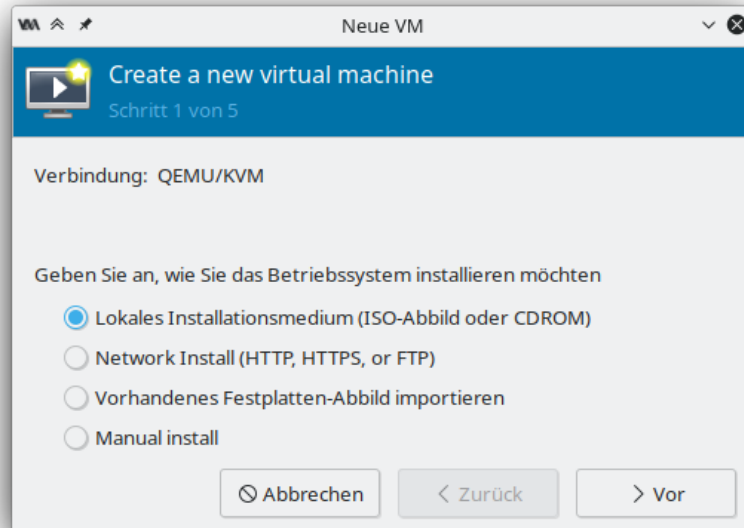


Bild 77: Erzeugung einer neuen VM

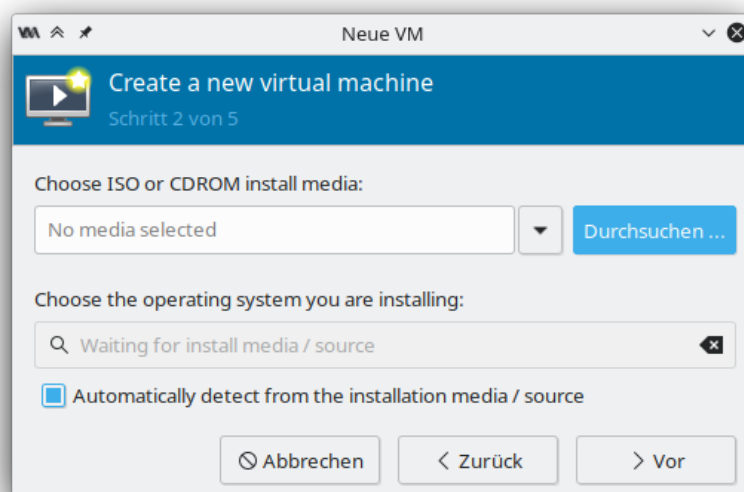


Bild 78: Auswahl einer Betriebssystem-ISO (1)

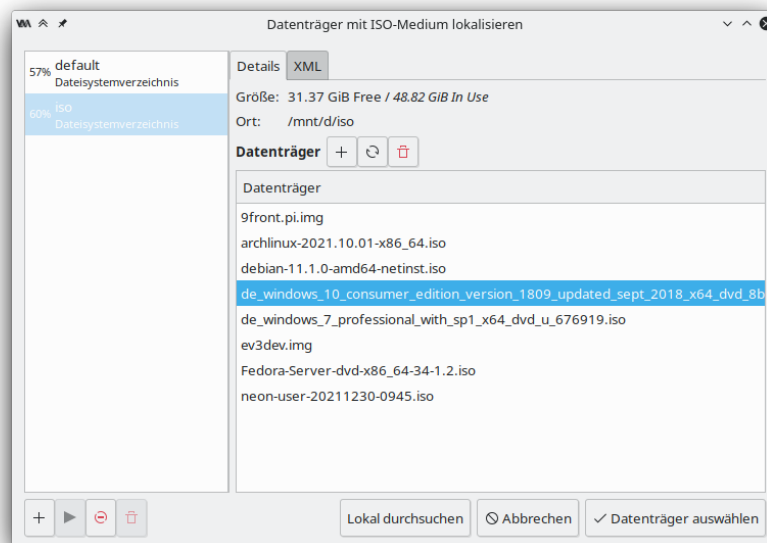


Bild 79: Auswahl einer Betriebssystem-ISO (2)

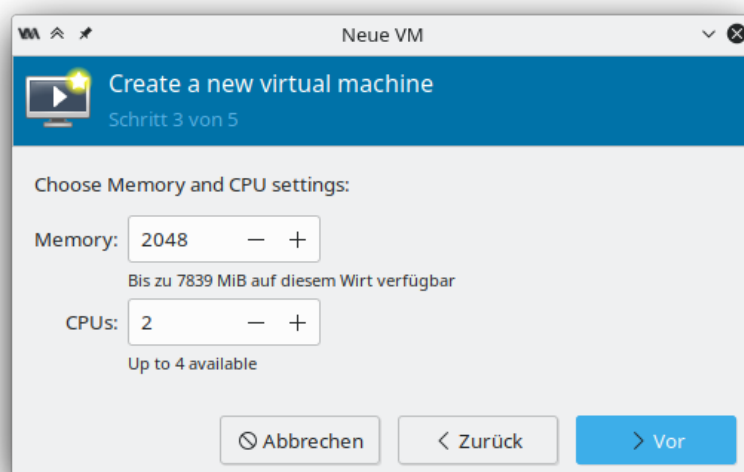


Bild 80: Hardwarespezifikation der VM

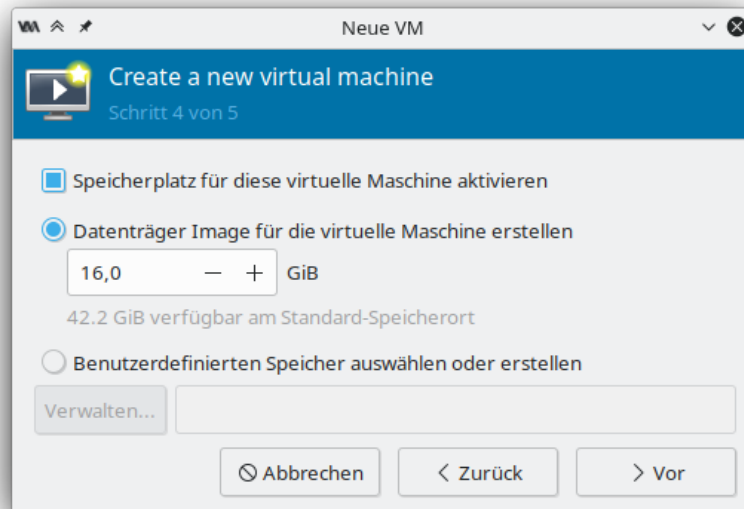


Bild 81: Virtuelle Festplatte der VM anlegen

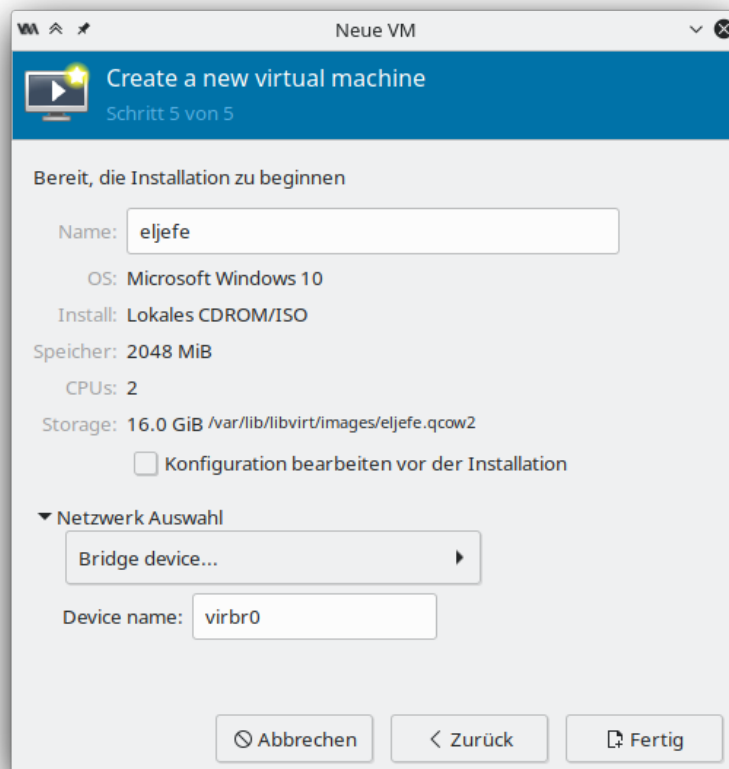


Bild 82: Einrichtung abschließen und Netzwerkkonfiguration wählen

B Einrichtung einer KVM mit Proxmox

The screenshot shows the 'Create: Virtual Machine' dialog box in Proxmox, with the 'General' tab selected. The dialog has a title bar with a close button. Below the title bar are tabs: 'General', 'OS', 'System', 'Hard Disk', 'CPU', 'Memory', 'Network', and 'Confirm'. The 'General' tab contains the following fields:

- Node:** A dropdown menu showing 'Mindflayer'.
- VM ID:** A dropdown menu showing '135'.
- Name:** A text input field containing 'jansenpc'.
- Resource Pool:** A dropdown menu.
- Start at boot:** A checkbox that is currently unchecked.
- Start/Shutdown order:** A dropdown menu showing 'any'.
- Startup delay:** A dropdown menu showing 'default'.
- Shutdown timeout:** A dropdown menu showing 'default'.

At the bottom of the dialog, there is a 'Help' button with a question mark icon, an 'Advanced' checkbox which is checked, and 'Back' and 'Next' buttons.

Bild 83: Erzeugung einer neuen VM

The screenshot shows the 'Create: Virtual Machine' dialog box in Proxmox, with the 'OS' tab selected. The dialog has the same title bar and tabs as the previous image. The 'OS' tab contains the following fields:

- Use CD/DVD disc image file (iso):** A radio button that is selected.
- Storage:** A dropdown menu showing 'SSD01'.
- ISO image:** A dropdown menu showing '1_2004_x64_dvd_36d61c40.iso'.
- Guest OS:** A dropdown menu showing 'Linux'.
- Type:** A dropdown menu showing 'Linux'.
- Version:** A dropdown menu showing '5.x - 2.6 Kernel'.
- Use physical CD/DVD Drive:** A radio button that is unselected.
- Do not use any media:** A radio button that is unselected.

At the bottom of the dialog, there is an 'Advanced' checkbox which is checked, and 'Back' and 'Next' buttons.

Bild 84: Auswahl einer Betriebssystem-ISO

The screenshot shows the 'Create: Virtual Machine' dialog box with the 'System' tab selected. The 'General' tab is also visible. The 'System' tab contains the following settings:

- Graphic card: Default
- SCSI Controller: VirtIO SCSI
- Qemu Agent: ☐
- BIOS: Default (SeaBIOS)
- Machine: Default (i440fx)

At the bottom, there is a 'Help' button, an 'Advanced' checkbox (checked), and 'Back' and 'Next' buttons.

Bild 85: Auswahl der Systemarchitektur

The screenshot shows the 'Create: Virtual Machine' dialog box with the 'Hard Disk' tab selected. The 'General' and 'System' tabs are also visible. The 'Hard Disk' tab contains the following settings:

- Bus/Device: SCSI
- Cache: Default (No cache)
- SCSI Controller: VirtIO SCSI
- Discard: ☐
- Storage: HDD01
- Disk size (GiB): 32
- Format: QEMU image format (qcow2)

Below these settings, there are checkboxes for 'SSD emulation' and 'IO thread', both of which are unchecked. There are also checkboxes for 'Backup' and 'Skip replication', both of which are checked. Below these are several input fields for read and write limits and bursts, all of which are set to 'default' or 'unlimited'.

At the bottom, there is a 'Help' button, an 'Advanced' checkbox (checked), and 'Back' and 'Next' buttons.

Bild 86: Virtuelle Festplatte der VM anlegen

Create: Virtual Machine

General OS System Hard Disk **CPU** Memory Network Confirm

Sockets: 1 Type: Default (kvm64)

Cores: 4 Total cores: 4

VCPUs: 4 CPU units: 1024

CPU limit: unlimited Enable NUMA: ☐

Extra CPU Flags:

Default	-	<input type="radio"/>	+	md-clear	Required to let the guest OS know if MDS is mitigated correctly
Default	-	<input type="radio"/>	+	pcid	Meltdown fix cost reduction on Westmere, Sandy-, and IvyBridge Intel CPUs
Default	-	<input type="radio"/>	+	spec-ctrl	Allows improved Spectre mitigation with Intel CPUs
Default	-	<input type="radio"/>	+	ssbd	Protection for "Speculative Store Bypass" for Intel models
Default	-	<input type="radio"/>	+	ibpb	Allows improved Spectre mitigation with AMD CPUs
Default	-	<input type="radio"/>	+	virt-ssbd	Basis for "Speculative Store Bypass" protection for AMD models

Help Advanced ☒ Back Next

Bild 87: Hardwarespezifikation der VM (1)

Create: Virtual Machine

General OS System Hard Disk CPU **Memory** Network Confirm

Memory (MiB): 2048

Minimum memory (MiB): 2048

Shares: Default (1000)

Ballooning Device: ☒

Help Advanced ☒ Back Next

Bild 88: Hardwarespezifikation der VM (2)

Create: Virtual Machine

General OS System Hard Disk CPU Memory **Network** Confirm

☐ No network device

Bridge: Model:
VLAN Tag: MAC address:
Firewall: ☒

Disconnect: ☐ Rate limit (MB/s):
Multiqueue:

[? Help](#) Advanced ☒ [Back](#) [Next](#)

Bild 89: Netzwerkkonfiguration wählen

C Verbindung des Nextcloud-Clients mit einem Server

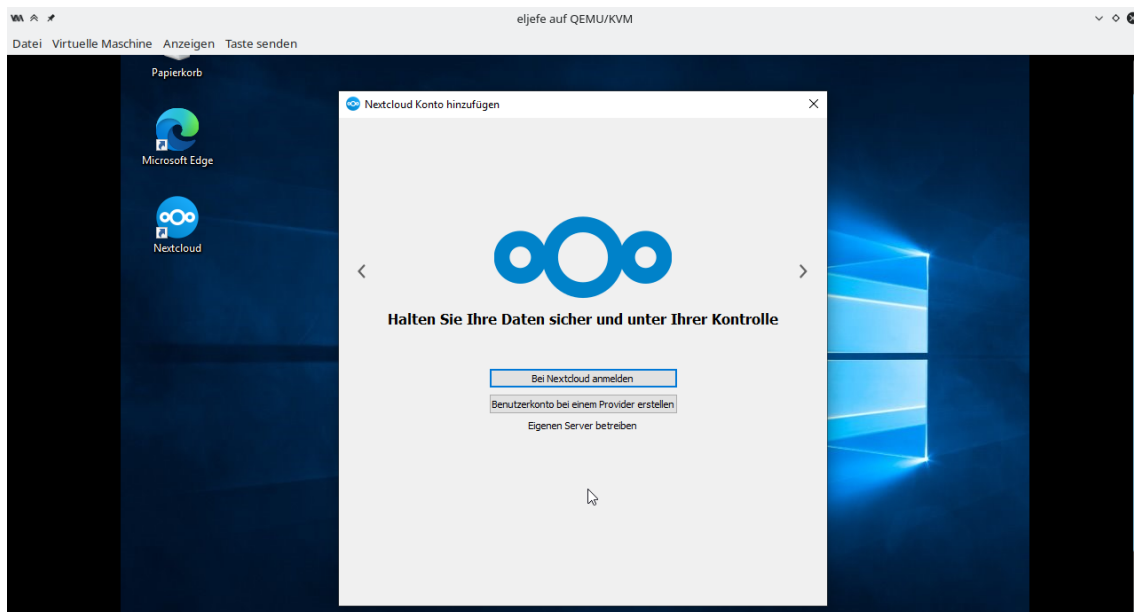


Bild 90: Neues Benutzerkonto zum Nextcloud-Client hinzufügen

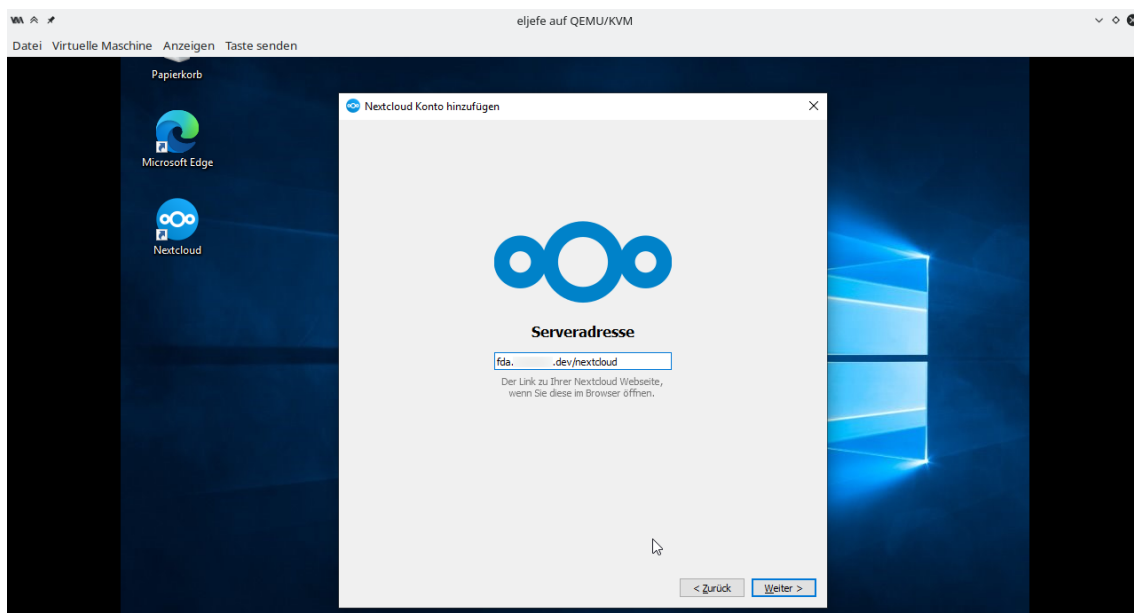


Bild 91: Adresse des Nextcloud-Servers angeben

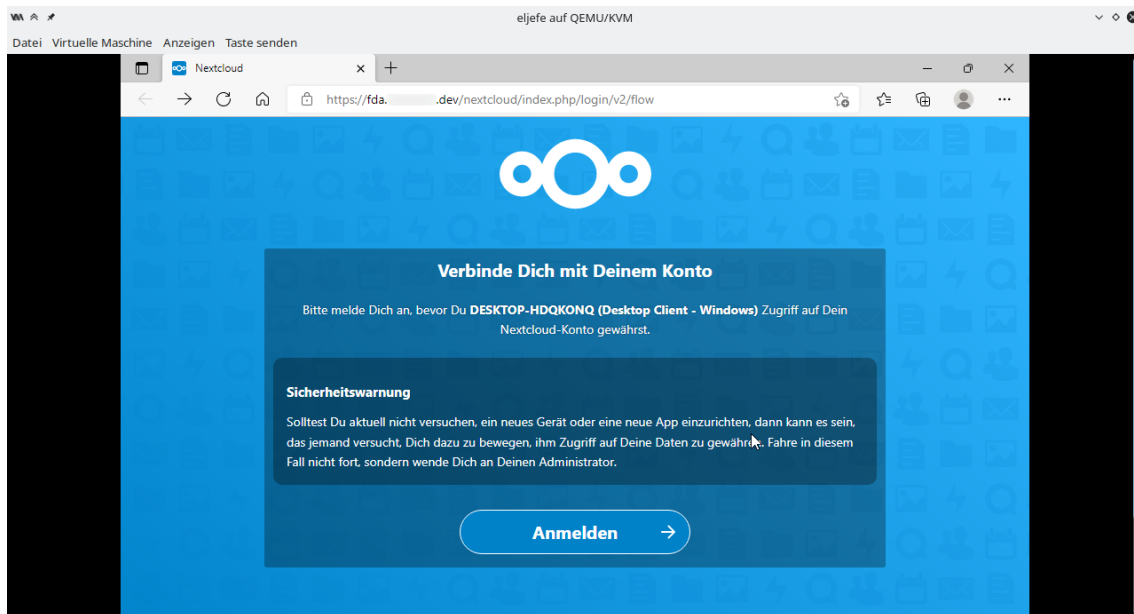


Bild 92: Web-Interface der Cloud zur Identitätsbestätigung öffnen

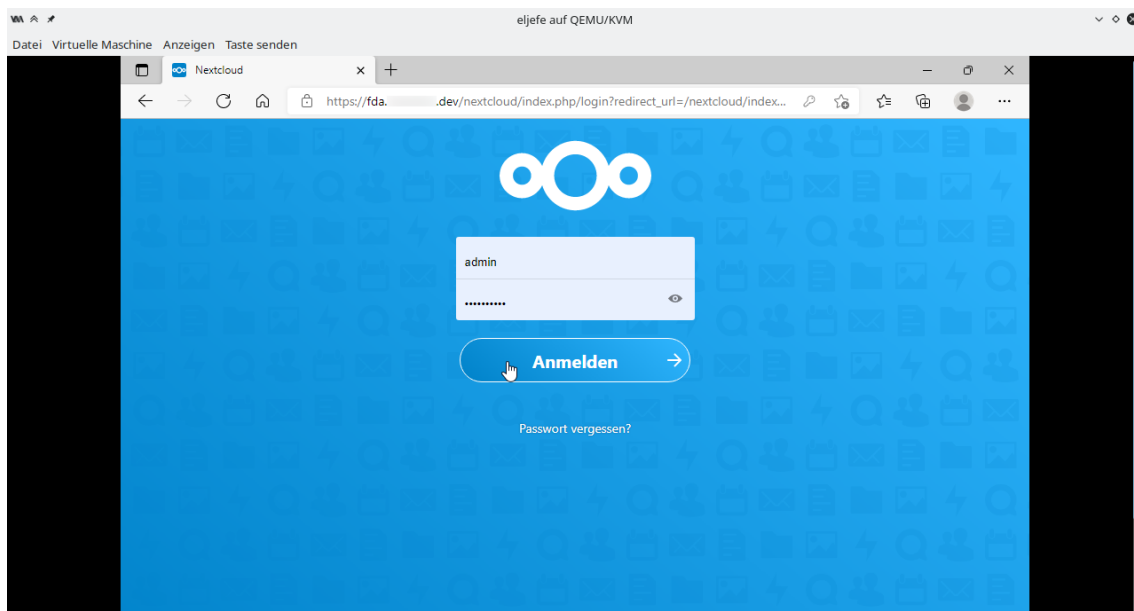


Bild 93: Benutzernamen und Passwort eintragen

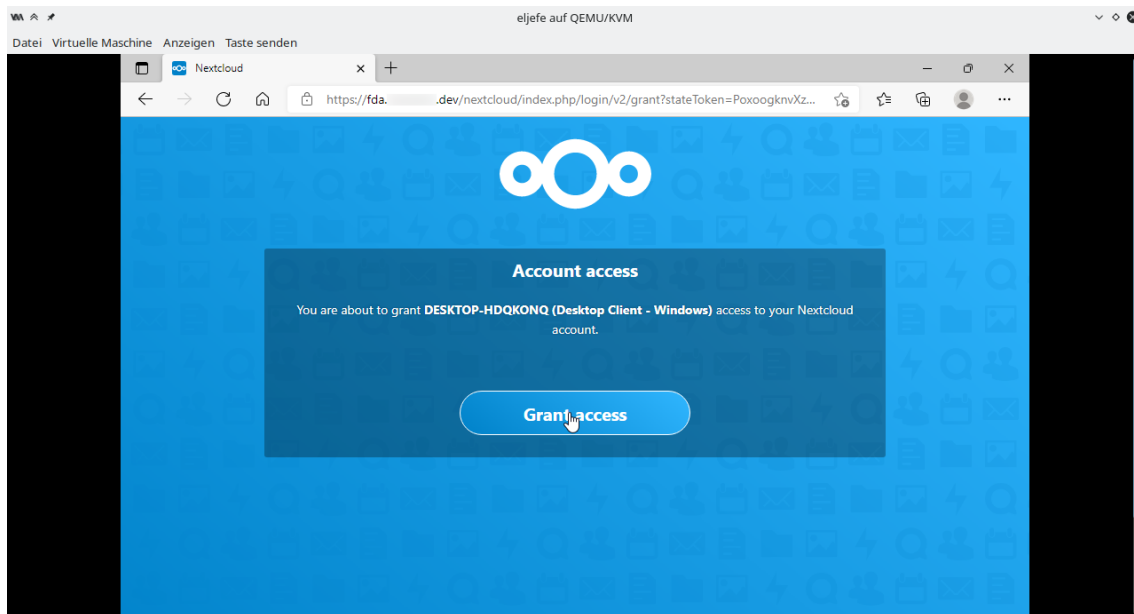


Bild 94: Zugriff des Desktop-Clients genehmigen

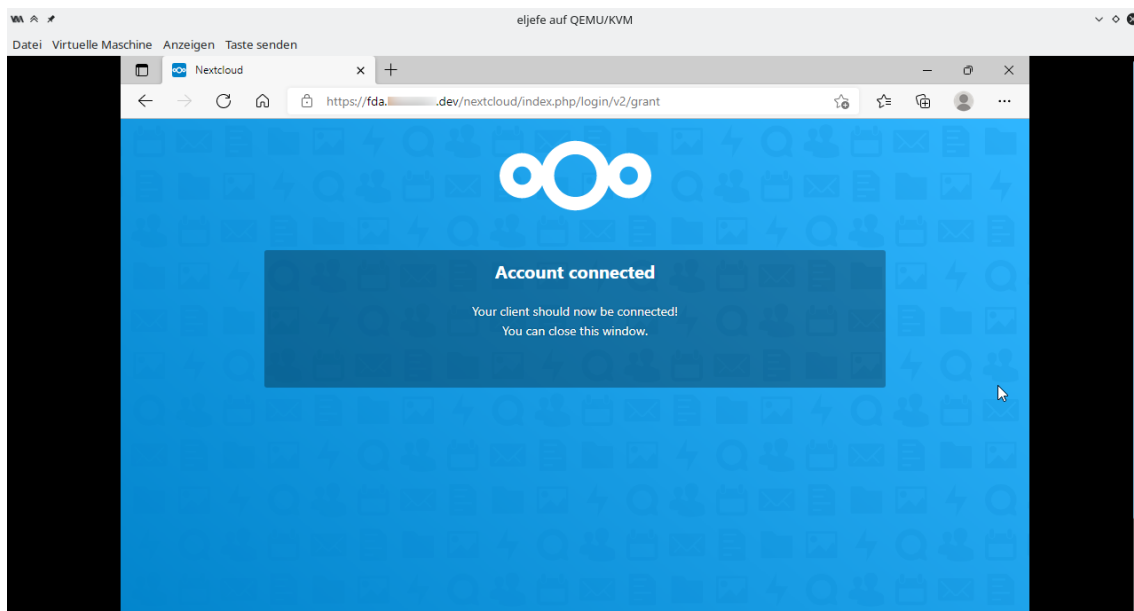


Bild 95: Bestätigung der Autorisierung

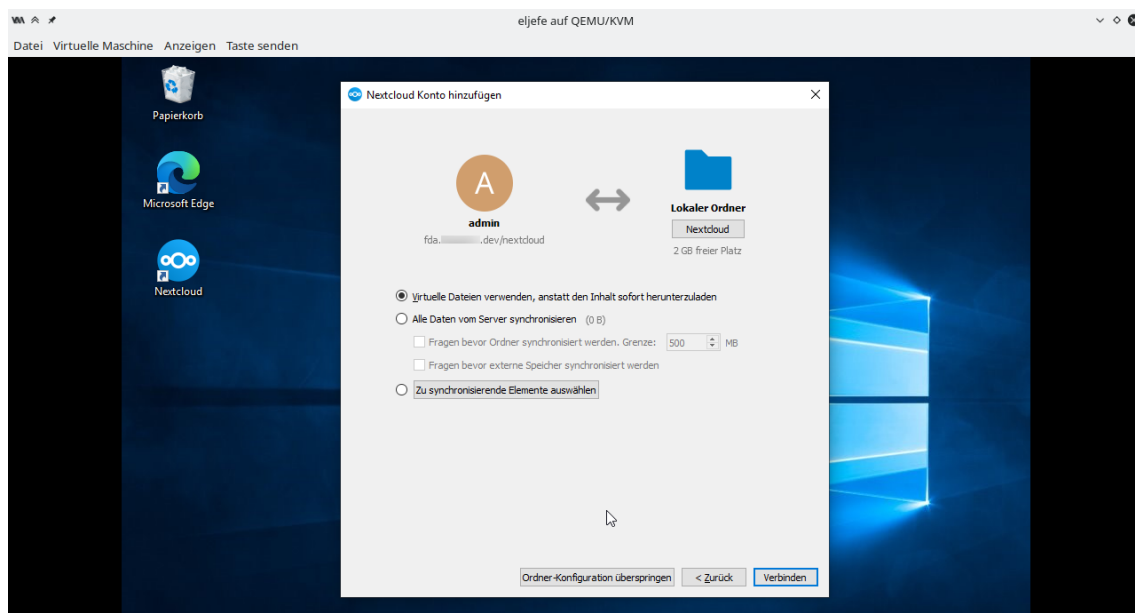


Bild 96: Lokalen Ordner zur Synchronisation wählen und Einrichtung abschließen

D Dateilisten der durch Guymager erzeugten Images

D.1 Dienstrechner des Geschädigten

```
chef/
├── chef.E01 ..... 2,0 GiB
├── chef.E02 ..... 2,0 GiB
├── chef.E03 ..... 2,0 GiB
├── chef.E04 ..... 1,9 GiB
├── chef.info ..... 5,9 KiB
└── chef.md5sum ..... 172 B
```

GUYMAGER ACQUISITION INFO FILE

=====

Guymager

=====

```
Version           : 0.8.8-3
Compilation timestamp: 2019-02-20-15.50.35
Compiled with      : gcc 8.2.0
libewf version     : 20140807 (not used as Guymager is configured to use its own EWF
                        module)
libguytools version : 2.0.5
Host name          : faust
Domain name        : (none)
System             : Linux faust 5.13.0-25-generic #26~20.04.1-Ubuntu SMP Fri Jan 7
                    16:27:40 UTC 2022 x86_64
```

Device information

=====

```
Command executed: bash -c "search=`basename /mnt/d/hsw/fda/projekt/evidence/chef/chef
                        .img`: H..t P.....d A..a de.....d" && dmesg | grep -A3 "$search" || echo "No
                        kernel HPA messages for /mnt/d/hsw/fda/projekt/evidence/chef/chef.img"
```

Information returned:

No kernel HPA messages for /mnt/d/hsw/fda/projekt/evidence/chef/chef.img

```
Command executed: bash -c "smartctl -s on /mnt/d/hsw/fda/projekt/evidence/chef/chef.
                        img ; smartctl -a /mnt/d/hsw/fda/projekt/evidence/chef/chef.img"
```

Information returned:

```
smartctl 7.1 2019-12-30 r5022 [x86_64-linux-5.13.0-25-generic] (local build)
Copyright (C) 2002-19, Bruce Allen, Christian Franke, www.smartmontools.org
```

```
/mnt/d/hsw/fda/projekt/evidence/chef/chef.img: Unable to detect device type
Please specify device type with the -d option.
```

```
Use smartctl -h to get a usage summary
```



```

smartctl 7.1 2019-12-30 r5022 [x86_64-linux-5.13.0-25-generic] (local build)
Copyright (C) 2002-19, Bruce Allen, Christian Franke, www.smartmontools.org

/mnt/d/hsw/fda/projekt/evidence/chef/chef.img: Unable to detect device type
Please specify device type with the -d option.

Use smartctl -h to get a usage summary

Command executed: bash -c "hdparm -I /mnt/d/hsw/fda/projekt/evidence/chef/chef.img"
Information returned:
-----
      HDIO_DRIVE_CMD(identify) failed: Inappropriate ioctl for device

/mnt/d/hsw/fda/projekt/evidence/chef/chef.img:

Hidden areas: unknown

Acquisition
=====

Linux device           : /mnt/d/hsw/fda/projekt/evidence/chef/chef.img
Device size            : 17179869184 (17,2GB)
Format                 : Expert Witness Format, sub-format Guymager - file extension
                        is .Exx
Image meta data
  Case number          : 1
  Evidence number      : 1
  Examiner             : John Doe
  Description           : Festplatte aus dem Desktop-Computer des Geschädigten
  Notes                :
Image path and file name: /mnt/d/hsw/fda/projekt/evidence/chef/exx/chef.Exx
Info path and file name: /mnt/d/hsw/fda/projekt/evidence/chef/exx/chef.info
Hash calculation       : MD5, SHA-1 and SHA-256
Source verification    : on
Image verification     : on

No bad sectors encountered during acquisition.
No bad sectors encountered during verification.
State: Finished successfully

MD5 hash                : 252e76445da4a962828cc1fb660b7d03
MD5 hash verified source : 252e76445da4a962828cc1fb660b7d03
MD5 hash verified image  : 252e76445da4a962828cc1fb660b7d03
SHA1 hash               : 04d32827545545513e257f7990a05eda9450045e
SHA1 hash verified source : 04d32827545545513e257f7990a05eda9450045e
SHA1 hash verified image  : 04d32827545545513e257f7990a05eda9450045e
SHA256 hash             :
                        a45886cfbc245ff7ef71290cb55f3786f1593c1a42dce9b3f7c0b8d8d11487b6
SHA256 hash verified source:
                        a45886cfbc245ff7ef71290cb55f3786f1593c1a42dce9b3f7c0b8d8d11487b6
SHA256 hash verified image :
                        a45886cfbc245ff7ef71290cb55f3786f1593c1a42dce9b3f7c0b8d8d11487b6
Source verification OK. The device delivered the same data during acquisition and
verification.
Image verification OK. The image contains exactly the data that was written.

```

```
Acquisition started : 2022-01-19 17:04:55 (ISO format YYYY-MM-DD HH:MM:SS)
Verification started: 2022-01-19 17:07:21
Ended               : 2022-01-19 17:10:44 (0 hours, 5 minutes and 48 seconds)
Acquisition speed   : 112.99 MByte/s (0 hours, 2 minutes and 25 seconds)
Verification speed   : 81.11 MByte/s (0 hours, 3 minutes and 22 seconds)
```

Generated image files and their MD5 hashes

=====

MD5	Image file
dc4108c131215806e6875d1a23bc9174	chef.E01
0d118af12fe6be02e173571b2bb0d783	chef.E02
3a0806a94c4bb2589c6aca6a4b9a0de0	chef.E03
32f82efa52c4e59dd30478bbf618c0bd	chef.E04

D.2 Laptop des Tatverdächtigen

```
sus/
├── sus.E01.....2,0 GiB
├── sus.E02.....2,0 GiB
├── sus.E03.....2,0 GiB
├── sus.E04.....2,0 GiB
├── sus.E05.....2,0 GiB
├── sus.E06 .....215,9 MiB
├── sus.info .....5,9 KiB
└── sus.md5sum .....252 B
```

GUYMAGER ACQUISITION INFO FILE

=====

Guymager

=====

```
Version           : 0.8.13-1
Version timestamp : 2021-08-13-12.57.42 UTC
Compiled with     : gcc 10.2.1 20210110
libewf version    : 20140807 (not used as Guymager is configured to use its own EWF
                        module)
libguytools version: 2.1.0
Host name         : kalilinux
Domain name      : (none)
System           : Linux kalilinux 5.10.0-kali6-amd64 #1 SMP Debian 5.10.26-1kali2
                  (2021-04-01) x86_64
```

Device information

=====

```

Command executed: bash -c "search=`basename /home/shou/Documents/sus.img`: H..t P
.....d A..a de.....d" && dmesg | grep -A3 "$search" || echo "No kernel HPA
messages for /home/shou/Documents/sus.img"
Information returned:
-----
No kernel HPA messages for /home/shou/Documents/sus.img

Command executed: bash -c "smartctl -s on /home/shou/Documents/sus.img ; smartctl -a /
home/shou/Documents/sus.img"
Information returned:
-----
smartctl 7.2 2020-12-30 r5155 [x86_64-linux-5.10.0-kali6-amd64] (local build)
Copyright (C) 2002-20, Bruce Allen, Christian Franke, www.smartmontools.org

/home/shou/Documents/sus.img: Unable to detect device type
Please specify device type with the -d option.

Use smartctl -h to get a usage summary

smartctl 7.2 2020-12-30 r5155 [x86_64-linux-5.10.0-kali6-amd64] (local build)
Copyright (C) 2002-20, Bruce Allen, Christian Franke, www.smartmontools.org

/home/shou/Documents/sus.img: Unable to detect device type
Please specify device type with the -d option.

Use smartctl -h to get a usage summary

Command executed: bash -c "hdparm -I /home/shou/Documents/sus.img"
Information returned:
-----
/home/shou/Documents/sus.img:

Command executed: bash -c "CIDFILE=/sys/block/$(basename /home/shou/Documents/sus.img)
/device/cid; echo -n "CID: " ; if [ -e $CIDFILE ] ; then cat $CIDFILE ; else echo
"not available" ; fi "
Information returned:
-----
CID: not available

Hidden areas: unknown

Acquisition
=====

Linux device          : /home/shou/Documents/sus.img
Device size           : 34359738368 (34.4GB)
Format                : Expert Witness Format, sub-format Guymager - file extension
                       is .Exx
Image meta data
  Case number          : 1
  Evidence number       : 4
  Examiner             : Max Mustermann
  Description           :
  Notes                :
Image path and file name: /mnt/storage/SWAP/fda/sus.Exx

```

```

Info path and file name: /mnt/storage/SWAP/fda/sus.info
Hash calculation       : MD5, SHA-1 and SHA-256
Source verification    : on
Image verification     : on

No bad sectors encountered during acquisition.
No bad sectors encountered during verification.
State: Finished successfully

MD5 hash               : 39398e27d33c2a0ceea66258f5586eaa
MD5 hash verified source : 39398e27d33c2a0ceea66258f5586eaa
MD5 hash verified image  : 39398e27d33c2a0ceea66258f5586eaa
SHA1 hash              : c1cd93570db9847f835c41e1f79c9322a9c273e2
SHA1 hash verified source : c1cd93570db9847f835c41e1f79c9322a9c273e2
SHA1 hash verified image  : c1cd93570db9847f835c41e1f79c9322a9c273e2
SHA256 hash            :
                        ec15eb61e642089bae4731a5ee09bdaff3c36511a6670d97add5af9323d45672
SHA256 hash verified source:
                        ec15eb61e642089bae4731a5ee09bdaff3c36511a6670d97add5af9323d45672
SHA256 hash verified image :
                        ec15eb61e642089bae4731a5ee09bdaff3c36511a6670d97add5af9323d45672
Source verification OK. The device delivered the same data during acquisition and
verification.
Image verification OK. The image contains exactly the data that was written.

Acquisition started : 2022-02-12 21:51:48 (ISO format YYYY-MM-DD HH:MM:SS)
Verification started: 2022-02-12 21:56:03
Ended               : 2022-02-12 22:00:59 (0 hours, 9 minutes and 10 seconds)
Acquisition speed   : 129.01 MByte/s (0 hours, 4 minutes and 14 seconds)
Verification speed   : 111.08 MByte/s (0 hours, 4 minutes and 55 seconds)

Generated image files and their MD5 hashes
=====

MD5                               Image file
c054128195fd5b74915c560ef1295eaf sus.E01
b3f474e629aa8f1eba05d3d1e812aa83 sus.E02
f79b4238f56dc1287133eea2def1a949 sus.E03
43479d118b6aa7cd25b5ae8774acd31f  sus.E04
35e9a4f822b76f174f6a5b3d8cce8410  sus.E05
f81743c4b784f662b898c26a3dafff5b  sus.E06

```

D.3 USB-Stick

```

stick/
├─ stick.E01..... 121,3 MiB
├─ stick.info..... 6,1 KiB
└─ stick.md5sum..... 44 B

```

```

GUYMAGER ACQUISITION INFO FILE
=====

```

```

Guymager
=====

Version           : 0.8.8-3
Compilation timestamp: 2019-02-20-15.50.35
Compiled with      : gcc 8.2.0
libewf version     : 20140807 (not used as Guymager is configured to use its own EWF
                    module)
libguytools version : 2.0.5
Host name          : faust
Domain name        : (none)
System             : Linux faust 5.13.0-25-generic #26~20.04.1-Ubuntu SMP Fri Jan 7
                    16:27:40 UTC 2022 x86_64

Device information
=====
Command executed: bash -c "search=`basename /dev/sde`: H..t P.....d A..a de.....d"
                  && dmesg | grep -A3 "$search" || echo "No kernel HPA messages for /dev/sde"
Information returned:
-----
    No kernel HPA messages for /dev/sde

Command executed: bash -c "smartctl -s on /dev/sde ; smartctl -a /dev/sde"
Information returned:
-----
    smartctl 7.1 2019-12-30 r5022 [x86_64-linux-5.13.0-25-generic] (local build)
    Copyright (C) 2002-19, Bruce Allen, Christian Franke, www.smartmontools.org

    /dev/sde: Unknown USB bridge [0x08ec:0x0008 (0x100)]
    Please specify device type with the -d option.

    Use smartctl -h to get a usage summary

    smartctl 7.1 2019-12-30 r5022 [x86_64-linux-5.13.0-25-generic] (local build)
    Copyright (C) 2002-19, Bruce Allen, Christian Franke, www.smartmontools.org

    /dev/sde: Unknown USB bridge [0x08ec:0x0008 (0x100)]
    Please specify device type with the -d option.

    Use smartctl -h to get a usage summary

Command executed: bash -c "hdparm -I /dev/sde"
Information returned:
-----
    SG_IO: bad/missing sense data, sb[]:  70 00 05 00 00 00 00 0a 00 00 00 00 20 00 00
        00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

    /dev/sde:

    ATA device, with non-removable media
    Standards:
    Likely used: 1
    Configuration:
    Logical      max current
    cylinders    0    0

```

```

heads          0    0
sectors/track  0    0
--
Logical/Physical Sector size:          512 bytes
device size with M = 1024*1024:        0 MBytes
device size with M = 1000*1000:        0 MBytes
cache/buffer size = unknown
Capabilities:
IORDY not likely
Cannot perform double-word IO
R/W multiple sector transfer: not supported
DMA: not supported
PIO: pio0

Hidden areas: unknown

Acquisition
=====

Linux device      : /dev/sde
Device size       : 128974848 (129,0MB)
Format            : Expert Witness Format, sub-format Guymager - file extension
                   is .Exx
Image meta data
  Case number      : 1
  Evidence number  : 3
  Examiner        : John Doe
  Description      : USB-Speichermedium aus dem Haushalt des Tatverdächtigen
  Notes           : 0E1145514041D91B
Image path and file name: /mnt/d/hsw/fda/projekt/evidence/stick/exx/stick.Exx
Info path and file name: /mnt/d/hsw/fda/projekt/evidence/stick/exx/stick.info
Hash calculation  : MD5, SHA-1 and SHA-256
Source verification : on
Image verification : on

No bad sectors encountered during acquisition.
No bad sectors encountered during verification.
State: Finished successfully

MD5 hash          : ac59d47ead9c5196d624a8b148c0ac44
MD5 hash verified source : ac59d47ead9c5196d624a8b148c0ac44
MD5 hash verified image  : ac59d47ead9c5196d624a8b148c0ac44
SHA1 hash         : 8fc4c85475337f510591cd1c596b360e0cbd50ee
SHA1 hash verified source : 8fc4c85475337f510591cd1c596b360e0cbd50ee
SHA1 hash verified image  : 8fc4c85475337f510591cd1c596b360e0cbd50ee
SHA256 hash       :
                   bcc15b86549da6b525e29fa5ed9b1dc5b03927352ac2c86d884fe2d3951b8221
SHA256 hash verified source:
                   bcc15b86549da6b525e29fa5ed9b1dc5b03927352ac2c86d884fe2d3951b8221
SHA256 hash verified image :
                   bcc15b86549da6b525e29fa5ed9b1dc5b03927352ac2c86d884fe2d3951b8221
Source verification OK. The device delivered the same data during acquisition and
verification.
Image verification OK. The image contains exactly the data that was written.

```

```
Acquisition started : 2022-01-19 15:20:18 (ISO format YYYY-MM-DD HH:MM:SS)
Verification started: 2022-01-19 15:20:33
Ended               : 2022-01-19 15:20:47 (0 hours, 0 minutes and 28 seconds)
Acquisition speed   : 8.79 MByte/s (0 hours, 0 minutes and 14 seconds)
Verification speed   : 8.79 MByte/s (0 hours, 0 minutes and 14 seconds)
```

Generated image files and their MD5 hashes

=====

MD5	Image file
e635a29d107bbb994d12083bc4608cf7	stick.E01

E Metadaten des LXC-Snapshots

```

./etc/vzdump/PaxHeaders.26036/pct.conf
0000644□□□□□□□□□□
002
14160140415
014501
ustar
30 mtime=1640022285.843129093
30 atime=1640022285.843129093
30 ctime=1640022285.843129093
./etc/vzdump/pct.conf
0000644□□□□□□□□□□
005
14160140415
013134
ustar
0000000□□□□

arch: amd64
cores: 8
features: fuse=1,mount=nfs;cifs,nesting=1
hostname: nextcloud.stoertebeker.dev
memory: 2048
net0: name=eth0,bridge=vbr0,firewall=1,gw=192.168.1.1,hwaddr=9E:14:80:2D:78:FB,ip
      =192.168.1.51/24,type=veth
ostype: debian
rootfs: HDD01:102/vm-102-disk-0.raw,size=32G
swap: 2048
./etc/vzdump/PaxHeaders.26036/pct.fw
0000644□□□□□□□□□□
002
14160140415
014170
ustar
30 mtime=1640022285.843129093
30 atime=1640022285.843129093
30 ctime=1640022285.843129093
./etc/vzdump/pct.fw
0000644□□□□□□□□□□
000
14160140415
012607
ustar
0000000□□□□

./PaxHeaders.26036/.
0000644□□□□□□□□□□
001
14155401350
011025
ustar
30 mtime=1639318248.883421385
29 atime=1640022284.84312614

```



```
30 ctime=1640022201.946880926
00007550000000000000
000
14155401350
007377
ustar
000000000000

./PaxHeaders.26036/root
00006440000000000000
002
14155402675
011667
ustar
30 mtime=1639318973.858323678
30 atime=1640022284.875126234
30 ctime=1640022206.102893243
./root/0000000000000000
0000
14155402675
010363
ustar
000000000000

./root/PaxHeaders.26036/.mysql_history
00006440000000000000
002
14155402446
014667
ustar
30 mtime=1639318822.293831995
30 atime=1640022204.574888714
30 ctime=1640022204.574888714
./root/.mysql_history000000000000
000
14155402446
013310
ustar
000000000000

CREATE DATABASE nextclouddb;
CREATE USER 'nextclouduser'@'localhost' IDENTIFIED BY 'password';
GRANT ALL ON nextclouddb.* TO 'nextclouduser'@'localhost';
FLUSH PRIVILEGES;
EXIT;
./root/PaxHeaders.26036/.bash_history
00006440000000000000
002
14160133376
014436
ustar
30 mtime=1640019710.203844178
30 atime=1640022204.574888714
30 ctime=1640022204.574888714
./root/.bash_history000000000000
000
```

```

01313
14160133376
013055
ustar
0000000000000000

passwd root
apt update
apt upgrade
nano /etc/php/7.3/apache2/php.ini
systemctl start apache2
systemctl start mariadb
systemctl enable apache2
systemctl enable mariadb
mysql -u root -p
wget
wget https://download.nextcloud.com/server/releases/latest.zip
unzip latest.zip
mv nextcloud /var/www/html/
chown -R www-data:www-data /var/www/html/nextcloud/
chmod -R 755 /var/www/html/nextcloud/
nano /etc/apache2/sites-available/nextcloud.conf
a2ensite nextcloud.conf
a2enmod rewrite
a2enmod headers
a2enmod env
a2enmod dir
a2enmod mime
systemctl restart apache2
service apache2 status
nano /etc/apache2/sites-available/nextcloud.conf
systemctl restart apache2
cd /var/www/html/
rm index.html
ping vpn.stoertebeker.dev
./root/PaxHeaders.26036/.wget-hsts
000064400000000000000000
002
14155402607
013665
ustar
30 mtime=1639318919.034150155
30 atime=1640022204.574888714
30 ctime=1640022204.574888714
./root/.wget-hsts
000064400000000000000000

14155402607
012315
ustar
0000000000000000

# HSTS 1.0 Known Hosts database for GNU Wget.
# Edit at your own risk.
# <hostname>    <port>    <incl. subdomains>    <created>    <max-age>
download.nextcloud.com 0    1    1639318891    63072000

```

```
./root/PaxHeaders.26036/.profile
00006440000000000000000000000000

12564377031
013411
ustar
30 atime=1640022204.574888714
30 ctime=1640022204.574888714
./root/.profile
00006440000000000000000000000000
004
564377031
012033
ustar
00000000000000000000000000000000

# ~/.profile: executed by Bourne-compatible login shells.
if [ "$BASH" ]; then
  if [ -f ~/.bashrc ]; then
    . ~/.bashrc
  fi
fi
mesg n || true
./root/PaxHeaders.26036/.local
00006440000000000000000000000000
001
14155401537
013032
ustar
29 mtime=1639318367.52802407
30 atime=1640022284.875126234
30 ctime=1640022206.102893243
```

Quellen

- [1] *Nextcloud Installation on linux*. Nextcloud GmbH. URL: https://docs.nextcloud.com/server/latest/admin_manual/installation/source_installation.html.
- [2] O. A. *Mysql_Secure_Installation*. URL: https://mariadb.com/kb/en/mysql_secure_installation/.
- [3] *Login Flow*. Nextcloud GmbH. URL: https://docs.nextcloud.com/server/latest/developer_manual/client_apis/LoginFlow/index.html.
- [4] O. A. *Hunting for Nextcloud Cloud Storage Forensic Artifacts on Endpoints*. URL: https://pve.proxmox.com/wiki/Linux_Container#_backup_and_restore.
- [5] *Nextcloud Server Administration Guide*. Nextcloud GmbH. 2022.
- [6] *Nextcloud User Manual*. Nextcloud GmbH. 2022.
- [7] *Nextcloud Client Manual*. Nextcloud GmbH. URL: <https://docs.nextcloud.com/desktop>.
- [8] Oleg Skulkin. *Hunting for Nextcloud Cloud Storage Forensic Artifacts on Endpoints*. 2020. URL: <https://blog.group-ib.com/nextcloud>.
- [9] Major Hayden. *Securing Linux Containers*. SANS Institute. 2021.

Bildverzeichnis

1	Schematische Beziehung zwischen den Geräten bezüglich des Vorfalls	7
2	Virtuelles Netzwerk im virt-manager	8
3	Hauptansicht des virt-managers mit laufender VM	9
4	Virtualisierter Desktop des Dienstrechners	10
5	Netzwerkdiagramm des Rechenzentrums	11
6	Virtualisierter Desktop des Privatrechners	14
7	Hochgeladener Ordner in der Cloud	14
8	Durchreichen des USB-Sticks in die VM	15
9	Daten werden auf den USB-Stick kopiert	16
10	Durchreichen des USB-Sticks in die Maschine des TV	17
11	Relevante Dateien in der VM	17
12	Upload der Dateien auf der Image-Sharing-Plattform Imgur	18
13	Einhängen eines „Spezialgeräts“ im Guymager	21
14	Datenträgerabbild in der Liste verfügbarer Geräte im Guymager	21
15	Einstellungen für die Imageerzeugung	22
16	Erfolgreiche Verifizierung des Images	23
17	USB-Stick in der Guymager Geräteliste	24
18	Einstellungen für die Imageerzeugung des USB-Stick	25
19	Erfolgreiche Verifizierung der USB-Stick-Images	25
20	Starten der Snapshot-Erstellung über den Backup-Reiter in Proxmox	27
21	Auswahl des Zielspeichers und der Kompressionsart	28
22	Log-Ausgabe während der Snapshot-Erstellung (1)	28
23	Log-Ausgabe während der Snapshot-Erstellung (2)	29
24	Asservat 01	36
25	Integritätsprüfung des Images des Dienstrechners	36
26	Betriebssystem auf dem Festplattenimage	37
27	Installationsdatei Nextcloud-Client	37
28	Letzte Ausführung des Nextcloud-Clients	38
29	Konfigurationsdatei des Nextcloud-Clients	39
30	Benutzerinformationen auf dem Dienstrechner	39
31	Log-Datei der Client-Software	40
32	Datenartefakte aus der SQLite-Datenbank des Nextcloud-Clients	40
33	„Kalender 2022“ im Papierkorb	41
34	Per RegRipper ermittelte angeschlossene USB-Geräte	42
35	Asservat 02	44
36	Integritätsprüfung des Snapshot-Datenträgers	44
37	Integritätsprüfung des Nextcloud-Snapshots	44
38	Auszug aus dem Nextcloud-Log	45
39	Auflistung der Freigaben über MariaDB	47
40	Asservat 03	48

41	Integritätsprüfung des USB-Stick-Images	48
42	Dateisysteminformationen über das USB-Stick-Image	49
43	Artefakte eines Dateiordners	49
44	Liste gefundener gelöschter Dateien aus X-Ways Forensics	49
45	Gefundene Bilddateien (Autopsy)	50
46	„System Volume Information“ des USB-Datenträgers	51
47	Vermerk Laufwerk „E“ im Registry	52
48	Bezeichnung „FLASHPEN128“ für Laufwerk „E“ im Registry	52
49	Auftreten der Dateisystembezeichnung „FLASHPEN128“ im Registry	53
50	USB-Stick-Modell „FlashPen“ des Herstellers „Hama“ im Registry des Asservats 01	53
51	Ordner „Kalender 2022“ auf dem kürzlich verwendeten Laufwerk „E“	53
52	Asservat 04	54
53	Integritätsprüfung des Laptop-Images	54
54	Betriebssystem und Nutzer des Laptop-Images	55
55	Zugrundeliegende Architektur des Laptop-Images	55
56	Installierte Software auf dem Laptop	55
57	Inhalt des Download-Verzeichnisses	55
58	Auszug aus dem Browserverlauf	56
59	Mehrfache Anmeldeversuche mit dem Nutzernamen „admin“	56
60	Übersicht über die angeschlossenen USB-Geräte	56
61	Bilddaten auf dem Laptop	57
62	Auflistung aller Übereinstimmungen mit dem Hashset	58
63	Aufruf des Upload-Portals von Imgur im Browserverlauf	58
64	Abruf eines Nextcloud-Client-Passwortes	60
65	„AppPassword“ im <i>Windows Credential Manager</i>	60
66	Metadaten eines LXC-Containers	63
67	Einlesen des Snapshots	64
68	Konfiguration des Containers	65
69	Instanziierung eines neuen Containers	65
70	Bruteforce-Versuche in der Nextcloud-Datenbank	66
71	Gelöschte Dateien in der Nextcloud-Datenbank	66
72	Datei-Cache in der Nextcloud-Datenbank	67
73	Aktivitäten in der Nextcloud-Datenbank	67
74	Auslesen der Tabelle <code>oc_users</code>	68
75	Auslesen der Tabellen <code>oc_share</code> und <code>oc_share_external</code>	68
76	Paketkonflikt zwischen verschiedenen TSK-Versionen	69
77	Erzeugung einer neuen VM	73
78	Auswahl einer Betriebssystem-ISO (1)	73
79	Auswahl einer Betriebssystem-ISO (2)	74
80	Hardwarespezifikation der VM	74
81	Virtuelle Festplatte der VM anlegen	75
82	Einrichtung abschließen und Netzwerkkonfiguration wählen	75
83	Erzeugung einer neuen VM	76

84	Auswahl einer Betriebssystem-ISO	76
85	Auswahl der Systemarchitektur	77
86	Virtuelle Festplatte der VM anlegen	77
87	Hardwarespezifikation der VM (1)	78
88	Hardwarespezifikation der VM (2)	78
89	Netzwerkkonfiguration wählen	79
90	Neues Benutzerkonto zum Nextcloud-Client hinzufügen	80
91	Adresse des Nextcloud-Servers angeben	80
92	Web-Interface der Cloud zur Identitätsbestätigung öffnen	81
93	Benutzernamen und Passwort eintragen	81
94	Zugriff des Desktop-Clients genehmigen	82
95	Bestätigung der Autorisierung	82
96	Lokalen Ordner zur Synchronisation wählen und Einrichtung abschließen	83

Tabellenverzeichnis

1	Untersuchungsobjekte	35
2	Untersuchungswerkzeuge	35
3	Dateinamen aus der Datenbank des Nextcloud-Clients	41
4	Verbundene Speichermedien (Asservat 01)	43
5	Anmeldungsversuche	45
6	Gelöschte Dateien in der Cloud	46
7	Nutzer der Cloud	46
8	Alle vom USB-Stick geborgenen Dateien	50
9	Bilddateien und ihre MD5-Hashes	57

Listingverzeichnis

1	Formatierung des USB-Sticks	13
2	Umwandlung von virtuellen QEMU-Festplatten in ein Rohformat . .	20
3	Prüfsummenerzeugung einer CD-ROM	29
4	Beispiel einer erfolgreichen Authentifizierung des Nextcloud-Clients [3]	59
5	Synchronisations-Log des Nextcloud-Clients	60
6	Erläuterung der „Instruction“-Codes	61
7	Erzeugung eines Datenbankklons mittels Docker	63
8	Benutzung von Distrobox	69

Abkürzungsverzeichnis

BD	Blu-ray Disc. 29
CD	Compact Disc. 29
CD-R	Compact Disc Recordable. 29, 44
DB	Datenbank, Database. 62
DVD	Digital Video Disc. 29
EWf	Expert Witness Format. 20, 21
FAT	File Allocation Table. 48
GbR	Gesellschaft bürgerlichen Rechts. 6, 10
GmbH	Gesellschaft mit beschränkter Haftung. 5, 7, 37
GNU	GNU's not UNIX. 10, 63, 69, 102
GZ	GNU-Zip. 26
HTTP	Hypertext Transfer Protocol. 12
HTTPS	Hypertext Transfer Protocol Secure. 12
ID	Identifikator. 65
IP	Internet Protocol. 12, 13, 45, 71
IT	Informationstechnologie. 4, 6, 29, 31, 32, 37, 70–72, 102
ITFS	IT-Forensik-Software. 4, 19, 20, 37
JPEG	Joint Photographic Experts Group. 33, 34, 42, 46, 49, 50
JSON	JavaScript Object Notation. 59
KVM	Kernel-basierte virtuelle Maschine. 9, 10, 13
LAMP	Linux Apache MySQL PHP. 62
LXC	Linux Containers. 10, 26, 62–64, 70, 72, 98
LXD	Linux Container Daemon. 72
MD5	Message-Digest Algorithm 5. 22, 29, 35, 44, 46, 50, 57, 100
MEZ	Mitteleuropäische Zeit. 34

PC	Personal Computer. 6, 68
PHP	PHP: Hypertext Preprocessor. 11, 102, 103
QEMU	Quick Emulator. 19, 20, 101
SHA	Secure Hash Algorithm. 22, 29, 44
SQL	Structured Query Language. 102
SSL	Secure Sockets Layer. 12
StGB	Strafgesetzbuch. 5
TAR	Tape Archiver. 26
TSK	The Sleuth Kit. 35, 68–70, 98
TV	Tatverdächtiger. 7, 13, 15–17, 19, 20, 23, 97
UrhG	Urheberrechtsgesetz. 5
URL	Uniform Resource Locator. 11
USB	Universal Serial Bus. 6–8, 13, 15–17, 23–25, 32–35, 42, 48–51, 53, 56, 68, 71, 97, 98, 100, 101
VE	Virtual Environment. 10, 13, 16, 26, 27, 64, 67, 104
VM	Virtuelle Maschine. 8, 9, 13–17, 27, 73–78, 97–99
ZSTD	Zstandard. 26

Glossar

Hypervisor	Host oder Umgebung, die ein virtualisiertes Betriebssystem beherbergt. 8, 14, 26
Proxmox VE	Proxmox VE ist eine auf Debian basierende Open-Source-Virtualisierungsplattform zum Betrieb von virtuellen Maschinen mit einem Webinterface. 10, 13, 16, 26, 27, 64, 67
Reverse-Proxy	Ein Reverse-Proxy ist ein Proxyserver in einem Rechnernetz, der die Kommunikation zwischen einem externen Client und einem oder mehreren internen Servern regelt, ohne dass diese direkt mit externen Clients kommunizieren müssen. 12, 71
vServer	Virtualisierter Server, im Gegensatz zum Bare-Metal-Server. 6