

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							
2	Bes	chreibu	ing des Szenarios	5				
3	Umsetzung des Szenarios							
	3.1	Vorbe	trachtungen	7				
	3.2	Vorbe	reitung der Datenquellen	8				
		3.2.1	Dienstrechner der Mecklenburger Angelprofi GmbH	8				
		3.2.2	Next cloud im Rechenzentrum Komet GbR	10				
		3.2.3	USB-Stick	13				
		3.2.4	Privatrechner des Tatverdächtigen	13				
	3.3	Durch	führung des Vorfalls	14				
4	Erze	eugung	der Images	19				
	4.1	PCs d	er betroffenen Personen	19				
		4.1.1	Konvertierung von QEMU-Images	19				
		4.1.2	Erzeugung von Images im EWF	20				
	4.2	USB-S	Stick	23				
	4.3	Nextc	loud	26				
	4.4	Speich	nerung des Container-Snapshots	29				
5	Fore	ensisch	es Gutachten	31				
	5.1	Deckb	latt	31				
	5.2	Auftra	ag und juristische Fragestellung	32				
	5.3	Zusan	ımenfassung der Untersuchung	33				
	5.4	Unters	suchungsobjekte	35				
	5.5	Unters	suchungswerkzeuge	35				
	5.6	Unters	suchung der Asservate	36				
		5.6.1	Asservat 01 – Fest plattenimage des Dienstrechners $\ .\ .\ .$.	36				
		5.6.2	Asservat 02 – Snapshot des Next cloud-Servers \hdots	44				
		5.6.3	Asservat $03 - USB$ -Stick	48				
		5.6.4	Asservat 04 – Festplattenimage des Laptops	54				
6	Det	ails zur	r Untersuchungstechnik	59				
	6.1	Festpl	attenimage des Dienstrechners	59				
		6.1.1	Nachweis einer bestehenden Verbindung zu einer Next cloud $\ $.	59				

		6.1.2	Löschung synchronisierter Daten	. 60
	6.2	Snapsl	not 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-S	tick	. 68
7	Zusa	mmen	fassung und Ausblick	70
	7.1	Zusam	menfassung	. 70
	7.2	Ausbli	ck	. 71
Ar	lage	A Ein	richtung einer KVM mit virt-manager	73
Ar	lage	B Ein	richtung einer KVM mit Proxmox	76
Ar	lage	C Ver	bindung des Nextcloud-Clients mit einem Server	80
Ar	lage	D Dat	eilisten der durch Guymager erzeugten Images	84
	D.1	Dienst	rechner des Geschädigten	. 84
	D.2	Laptop	e des Tatverdächtigen	. 86
	D.3	USB-S	tick	. 88
Ar	امرم			
	nage	E Me	tadaten des LXC-Snapshots	92
Qu	ıellen	E Me	tadaten des LXC-Snapshots	92 96
Qu Bil	iellen Idverz	E Me zeichni	tadaten des LXC-Snapshots	92 96 97
Qu Bil Ta	iellen Idverz bellei	E Me zeichni nverzei	tadaten des LXC-Snapshots s chnis	92 96 97 100
Qu Bil Ta Lis	iellen Idverz bellei stingv	E Me zeichni nverzei verzeich	tadaten des LXC-Snapshots s chnis mis	92 96 97 100 101
Qu Bil Ta Lis Ab	iellen Idverz bellei stingv	E Me zeichni nverzei verzeich ungsve	tadaten des LXC-Snapshots s chnis nnis rzeichnis	 92 96 97 100 101 102

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 Angelprofi 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) einreichtet und aktiv sein.



Bild 2: Virtuelles Netzwerk im virt-manager

¹https://imgur.com/

Für die Verwaltung der VM wurde der virt-manager² 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.

²https://virt-manager.org/

³https://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 Webservers 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 Proxyservers 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 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.

⁴https://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:

<pre>\$ dd if=/dev/urandom of=/dev/sde</pre>	<pre># /dev/sde ist der USB-Stick</pre>
<pre>\$ mkdosfs -F 32 -n "FLASHPEN128" -I /dev/sde</pre>	# 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 Vorfalls

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.

MA ♠ ★ eljefe auf QEMU/KVM	$\vee \diamond \otimes$
Datei Virtuelle Maschine Anzeigen Taste senden	
Papierkorb	
💿 🖓 📙 = Nextcloud — 🗆 🗙	
Datei Start Freigeben Ansicht 🗸 🕡	
$\langle \leftrightarrow \rangle \rightarrow \uparrow \diamond$ Nextcloud $\rangle \rightarrow \lor \Diamond$ "Nextcloud" durchsuchen	
Microsoft Edge	
★ Schnellzugriff Verne Scatus Anderungs	
■ Desktop Kalender 2022 Control 14.12.2021 Langer and and and a second and a sec	
Upownloads at Downloads at Downloads	
Nextcloud 🔮 Dokumente 🖈	
■ Bilder	
🖒 Musik 🐂 0% abgeschlossen — — — 🗙	
I Stemente werden von Nextcloud nach FLASHPENI28 (E) kopiert >	
2 Elemente 0% abgeschlossen II × E	
Datei Start Fr 🕑 Mehr Details 🗸 🗸 🚱	
← → < ↑ → FLASHPEN128 (E)	
A Name Anderungsdatum Typ Große	
★ Schnellzugriff	
Desktop * Dieser Ordner ist leer.	
Downloads *	
😫 Dokumente 🖈	
🖬 Bilder 🖈	
Musik 🗸	
0 Elemente	

Bild 9: Daten werden auf den USB-Stick kopiert

Hinweis

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.

Virtual Machine 135	(jansenpc) on node '					Þ	Start 🕐 Shutdown 🗸	>_ Console V	More 🗸 👩 Help
Summary	Add V Remove Edit								
>_ Console	Memory	4.00 GiB							
Hardware	Processors	8 (1 sockets, 8 core	38)						
Cloud-Init	BIOS	Default (SeaBIOS)							
 Ontions 	🖵 Display	Default							
we options	Oo Machine	Default (i440fx)							
I Task History	SCSI Controller	VirtIO SCSI							
Monitor	 CD/DVD Drive (ide0) 	SSD01:iso/virtio-wi	n-0.1.208.iso,media=cdrom,size=543390K						
🖺 Backup	 CD/DVD Drive (ide2) 	SSD01:iso/en_wind	lows_10_consumer_editions_version_2004_x64_	dvd_36d61c40.iso,med	ia=cdrom				
13 Replication	A Hard Disk (scsi0)	SSD03:135/vm-135	5-disk-0.qcow2,size=32G						
3 Snapshots		virtio=7A:6A:CD:D/	A:6F:68,bridge=vmbr0,firewall=1						
C Firewall									
Dermissions									
			Add: USB Device	\otimes					
			Spice Port Use USB Vendor/Device ID						
			Choose Device: USB Disk (1609:3a04)	v					
			O Use USB Port						
				~					
			Use USB3:						
			@ Help	Add					

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 eingesetzen 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.

¹https://guymager.sourceforge.io/

X & *			GUYMAGER 0.8.8				~ ^ ×
Devices Misc Help							
<u>R</u> escan	F5						
Add special device		1					
Serial nr.	Linux device	Model	State	Size	Hidden areas	Bad sectors	Progress
2107E4F93C73	/dev/nvme0n1	CT500P2SSD8	Oldle	500,1GB	unknown		
WD-WCC4M1483667	/dev/sda	WDC_WD20EZRX-00D8PB0	Oldle	2,0TB	unknown		
X9JITB1TT	/dev/sdb	TOSHIBA_MK5055GSX	Oldle	500,1GB	HPA:No / DCO:Unknown		
191770802254	/dev/sdc	SanDisk_SSD_PLUS_240GB	Oldle	240,1GB	HPA:No / DCO:Unknown		
WD-WX22DA0LHTAJ	/dev/sdd	WDC_WD40EFAX-68JH4N1	Oldle	4,0TB	HPA:No / DCO:Unknown		
	/dev/loop0	bare_5.snap	Oldle	4,1kB	unknown		
	/dev/loop1	gnome-3-28-1804_161.snap	Oldle	172,8MB	unknown		
4			A		· · · ·		• •
Size Sector size Inage file Current speed Started Hash calculation Source verification Image verification							

Bild 13: Einhängen eines "Spezialgeräts" im Guymager

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

<u>D</u> evices <u>M</u> isc <u>H</u> e Rescan	lp					
Serial nr.	•	Linux device	Model	State Size		
		/mnt/d/hsw/fda/projekt/evidence/chef/chef.img	Manually added special device	🔵 ldle	17,2GB	
Size Sector size Image file Info file Current speed Started Hash calculation Source verification Image verification	17. 512	179.869.184 bytes (16,0GiB / 17,2GB) 2				

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 Zieldateien gewählt³. Neben allgemeinen Metadaten zur Untersuchung (Bearbeiter, Asservatsnummer, Zieldateipfad etc.) wurde eingestellt,

 $^{^2\}mathsf{EXX}$ 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							
○ <u>L</u> inux dd raw ir	nage (file extensi	on .dd or .xxx)	✓ Split image files				
Expert Witness	Format, sub-form	nat Guymager (file extension .Exx)	Split size 2047 MiB 💌				
Case number	1						
Evidence number	1						
Examiner	John Doe						
Description	Festplatte aus de	em Desktop-Computer des Geschäd	ligten				
Notes							
Destination							
Image directory		/mnt/d/hsw/fda/projekt/evidence/ch	ef/exx/				
lmage filename (w	ithout extension)	chef					
Info filename (with	out extension)	chef					
Hash calculation / ve	rification						
✓ Calculate MD5		✓ Calculate SHA-1	✓ Calculate SHA-256				
✓ Re-read source after acquisition for verification (takes twice as long)							
✓ Verify image af	ter acquisition (tal	kes twice as long)					
Cancel		Duplicate image	Start				

Bild 15: Einstellungen für die Imageerzeugung

Devices Misc He	elp					
Rescan						
Serial nr.	•	Linux device	Model	State	Size	•
	/mnt/d/hsw/fo	la/projekt/evidence/chef/chef.img	Manually added special device	Finished - Verified & ok	17,2GB	•
•					•	
Size Sector size Image file Info file Current speed Started Hash calculation Source verification Image verification	17.179.869.184 512 /mnt/d/hsw/fda/p /mnt/d/hsw/fda/p 19. Januar 17:0 MD5, SHA-1 an on on	bytes (16,0GiB / 17,2GB) rojekt/evidence/chef/exx/chef.Exx rojekt/evidence/chef/exx/chef.info 4:55 (00:05:48) 1 SHA-256				

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.

Serial nr.	Linux device	Model	State	Size	Hidden areas
107E4F93C73	/dev/nvme0n1	CT500P2SSD8	Oldle	500,1GB	unknow
D-WCC4M1483667	/dev/sda	WDC_WD20EZRX-00D8PB0	Oldle	2,0TB	unknow
X9JITB1TT /dev/sdb		TOSHIBA_MK5055GSX	Oldle	500,1GB	HPA:No / DCO:Unknow
91770802254	/dev/sdc	SanDisk_SSD_PLUS_240GB	Oldle	240,1GB	HPA:No / DCO:Unknow
/D-WX22DA0LHTAJ	/dev/sdd	WDC_WD40EFAX-68JH4N1	Oldle	4,0TB	HPA:No / DCO:Unknow
E1145514041D91B	/dev/sde	Hama FlashPen	🔵 ldle	129,0MB	unknow
	/dev/loop0	bare_5.snap	🔿 Idle	4,1kB	unknow
	/dev/loop1	gnome-3-28-1804_161.snap	Oldle	172,8MB	unknow
	/dev/loop2	core18_2253.snap	Oldle	58,2MB	unknow
	/dev/loop3	gtk-common-themes_1519.snap	Oldle	68,4MB	unknow
	/dev/loop4	core18_2284.snap	Oldle	58,2MB	unknow
	/dev/loop5	snapd_14295.snap	Oldle	45,4MB	unknow

Sector size Image file Info file Current speed Started Hash calculation Source verification Image verification

Bild 17: USB-Stick in der Guymager Geräteliste

File format					
○ <u>L</u> inux dd raw ir	nage (file extensi	on .dd or .xxx)	✓ Split image files		
Expert Witness	Format, sub-form	at Guymager (file extension .Exx)	Split size 2047 MiB 👻		
Case number	1				
Evidence number	3				
Examiner	John Doe				
Description	USB-Speicherm	edium aus dem Haushalt des Tatve	rdächtigen		
Notes	0E11455140410	091B			
Destination					
Image directory		/mnt/d/hsw/fda/projekt/evidence/st	stick/exx/		
lmage filename (w	ithout extension)	stick			
Info filename (with	out extension)	stick			
Hash calculation / ve	rification				
✓ Calculate MD5		✓ Calculate SHA-1	✓ Calculate SHA-256		
✔ Re-read source	e after acquisition	for verification (takes twice as long)		
✔ Verify image af	ter acquisition (tal	kes twice as long)			
Cancel		Duplicate image	Start		

Bild 18: Einstellungen für die Imageerzeugung des USB-Stick

<u>D</u> evices <u>M</u> isc <u>H</u> Rescan	lelp					
Serial nr.	*	Linux device	Model		State	Size
0E1145514041D9	1B	/dev/sde	Hama FlashPen	Finished	- Verified & ok	129,0MB
 ▲ Size 	12	8.974.848 bytes	(123MiB / 129MB)			•
Sector size Image file Info file	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					
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 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 forensischen 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 bedeuteten könnten, was wiederum zu finanzellen 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.

× - Proxmox Virt														
< → C ŵ		A https://192.1	68.1.5:8006/#v1:0:=bcc%					ය <u>එ</u>			. 🚺		<u>e</u> e e	
× PRO×MO>	Virtual Environment	6.4-13 Search							@ Docu	mentation 🗔	create VM	Creat	CT 占 root@	am v
Server View	× c	ontainer 102 (nexto	loud.) on node '						▶ Start	() Shutdown	~ >_ c	console ~	More V	Help
Datacenter	^ <i>e</i>	Summary	Backup now Rest	ore Show Configuration Edit	Notes Remove			Storage: HDD01		V Filter V	MID Se	arch:		
101 (dynibex)	>	Console	Name 1				Notes			Date		Format	Size	_
102 (nextcloud.	L) 😮	Resources	vzdump-lxc-102-2021	02 01-12 13 46.tar.oz						2021-02-01	12:13:46	tar.gz	281.35	мв
106 (plex should be a should be should be should be a should be a should be a should be		Network	vzdump-bxc-102-2021	02_03-10_16_53.tar.gz						2021-02-03	10:16:53	tar.gz	281.36	мв
 TOP (organize or		DNS												
109 (JHF) Con	and	Options												
112 (abook.aho)	nudev)	Task History												
10 117 (belierbeing a	atura dev)	Backup												
E) 115 (deve abox	a devi	Regisation												
E) 120 (whi should be a straight of the st	(inv)	Conceptor												
(c) 123 (8 downlos)	ader shouldes)	Circumit in the												
124 (salids also)	u.dev)	Firewall >												
(c) 127 percention	And	Permissions												
130 (Lapyler alle	(au.most)						3							
(c) 131 (rented also	was.dev)													
132 (tachideak)	abou.dev)													
133 (tex-compil	for shou dev)													
134 (abs-bot.at	Prou.dev)													
too prangad a	article (dev)													
104 (parties also	was dev)													
📮 105 (windowed	f. shou dev)													
💭 110 (abook aho	nu mont													
🕞 111 (spn.ahou.)	dev.)													
113 (st di abou	(dev)													
2 114 passpar. an	~													
Tasks Cluster log														
Start Time \downarrow	End Time	Node	User name	Description						-		۰ 👔		
Dec 20 18:37:13	Dec 20 18:37:26		root@pam	VM/CT 102 - Console								•		^
Dec 20 14:29:34	Dec 20 14:31:42		root@pam	VM/CT 105 - Console						×		• •		
Dec 20 14:29:33	Dec 20 14:29:33		root@pam	VM 105 - Start						0		B 🤹		
Dec 20 14:29:15	Dec 20 14:29:15		root@pam	VM 105 - Start								~	ne 'local:iso/en_v	f
Dec 20 14:29:14	Dec 20 14:29:15		root@pam	VM/CT 105 - Console							•	•	d to run vncproxy	

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

- Proximox Virtual Er × +					
← → C @ ○ A https://19	2:168.1.5:8006/#v1:0:=lxc%2F102:4:::::21:9		☆ 호 ♡	in ED 🔍 🗠 🖪 🐺 🖽 🥥	
XPROXMOX Virtual Environment 6.4-13 Search			2	Documentation	🛔 root@pam 🗸
Server View Container 102 (ne	xtcloud.) on node '			art 🕐 Shutdown 🖂 > Console 🖂 More	V @ Help
Datacenter	Backup now Restore Show Configuration Edit Notes		Storage: HDD01	V Filter VMID Search:	
101 (dynibex) >_ Console					
102 (nextcloud.)	vzdumo-lac-102-2021 02 01-12 13 46 tar.oz			2021-02-01 12-13:46 tar.oz	281.35 MB
Retwork	vzdump-bxc-102-2021 02 03-10 16 53.tar.gz			2021-02-03 10:16:53 tar.gz	281.36 MB
Ø DNS					
Options					
Task History					
D Rankup					
12 Replication					
Snanshote					
D Errowall					
Pirewaii O Demoissione	Ba	Sackup CT 102 🛞			
" Permissions	St	Storage: HDD01			
(3) 132 (paper along mont)	M	Aode: Suspend V			
	Co	Compression: ZSTD (fast and good)			
 Controllege attended atten	54	Send email to: none			
134 (also but also data)					
😱 100 (mangatil alrea. dev.)		Help Backup			
103 (manga alina dav)					
105 (animpress) about the l					
110 (shock shoc rost)					
111 (specialized day)					
· · · · · · · · · · · · · · · · · · ·					
Tasks Cluster log					
Start Time 🧼 End Time Node				······································	
Dec 20 18:37:13 Dec 20 18:37:26	root@pam VM/CT 102 - Console				
Dec 20 14:29:34 Dec 20 14:31:42	root@pam VM/CT 105 - Console				
Dec 20 14:29:33 Dec 20 14:29:33	root@pam VM 105 - Start			 O D W 	
				🤹 😑 🐼 he focal:	liso/en_w

Bild 21: Auswahl des Zielspeichers und der Kompressionsart

× - Prosmox Virtual									a ×
< → C @		A https://192.16	58.1.5:8006/#v1:0:=bc:%a			2 2	🗢 lin 🗉 😐 💁 🚺	e 🛛 📀	. ⊗ ≡
× PROXMOX	firtual Environment 6	6.4-13 Search					Documentation Create VM	Create CT	🛔 root@pam 🗸
Server View	° Co	ontainer 102 (nextolo	oud.) on node '	' 🚨 (backup)			▶ Start 🖉 Shutdown 🗸 > Co	nsole 🖂 More	e V 🔞 Help
Datacenter	^ <i>e</i>	Summary	Backup now Rest			Storage: HDD01	V Filter VMID Sea		
101 (dynibex)		Console							
102 (nextcloud.) ©	Resources	vzdump-bxc-102-2021_0	02_01-12_13_46.tar.gz			2021-02-01 12:13:46	tar.gz	281.35 MB
117 (requestor also	=	: Network	vzdump-bxc-102-2021_0	02_03-10_16_53.tar.gz			2021-02-03 10:16:53	tar.gz	281.36 MB
C 100 photo atour	0	DNS							
6 100 (Louis Control	0	Options		Task viewer: VM/CT 102 - Backup		8			
		Task History				Ŭ			
E 112 julias altera de	8	Backup		Output Status					
() 110 prevalation in		Replication		Stop					
	3	Snapshots		INFO: starting new backup job: vzdump 102mode suspendstorage HDD01node	compress 2stdremove 0				
	0	Firewall >		INFO: Starting Backup of VM 102 (bx) INFO: Backup started at 2021-12-20 18:43:21					
	-	Permissions		INFO: status = running					
				INFO: backup mode: suspend INFO: ionice priority: 7					
🚯 132 (capter about				INFO: CT Name: nextcloud INFO: including mount point rooth (77) in backup					
				INFO: starting first sync /proc/12070/root/ to /tmp/vzdumptmp24987_102/					
E 111 des constitut									
134 (who but also					-				
🖵 100 (mangadi aho									
🙀 103 (manga ahou									
111 Information of the									
111 (specialized dev									
114 (Beoget about									
Tasks Cluster log									
	d Time	Node					a 8 (
Dec 20 18:43:21	0		root@pam	VM/CT 102 - Backup					
Dec 20 18:37:13 De	c 20 18:37:26		root@pam	VM/CT 102 - Console			• • • •		
Dec 20 14:29:34 De	c 20 14:31:42		root@pam	VM/CT 105 - Console			 O E 	1 🧃	
Dec 20 14:29:33 De	c 20 14:29:33		root@pam	VM 105 - Start			÷ • •		
Dec 20 14:29:15 De	c 20 14:29:15		root@pam	VM 105 - Start				ne loca	il:iso/en_w 🗸

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 size is: 1
Logical block size is: 2048
```

⁴https://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
69dbcbc13c9f0a7fb266e0c106db0b191fc2433b14471e8c1fec2a0b8d4ef40f 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

Kriminalamt Friedenshof = Talstraße 3-5 = 23966 Wismar = Tel: 03841123456

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 **einziger Nutzer mit** dem Namen "admin". Keine der Daten dieses Nutzers wurden für einen externen Zugriff freigeben. In den Logdateien der Cloud wurden fünf gescheiterte Anmeldungsversuche 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 Anmeldungsversuche 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.

Asservat	Zeitstempel	Event	Beschreibung
2	12.12.21 15:53:43	E	Ordner "Kalender 2022" wird in der Next-
			cloud angelegt
1	17.12.21 11:59:40	0	Anmeldung des Windows-Nutzers "el jefe"
1	17.12.21 12:00:05	0	Nextcloud-Client gestartet
4	17.12.21 12:17:04	0	Erster Aufruf Webinterface der Cloud
2	17.12.21 12:17:05	0	Erster gescheiterter Anmeldungsversuch
2	17.12.21 12:17:17	0	Zweiter gescheiterter Anmeldungsversuch
2	17.12.21 12:17:38	0	Dritter gescheiterter Anmeldungsversuch
2	17.12.21 12:17:03	0	Vierter gescheiterter Anmeldungsversuch
2	17.12.21 12:17:17	0	Fünfter gescheiterter Anmeldungsversuch
4	17.12.21 12:18:13	0	Letzter Aufruf Webinterface der Cloud
1	17.12.21 12:30:09	0	USB-Speichermedium mit der Serien-Nr.
			0E1145514041D91B verbunden
3	17.12.21 12:30:23	Е	Erzeugung de Ordners "Kalender 2022" mit
			12 JPEG-Datien
2	17.12.21 12:31:03	М	Verschiebung des Ordners "Kalender 2022"
			in den Papierkorb
1	17.12.21 12:31:07	М	Verschiebung des Ordners "Kalender 2022"
			in den Papierkorb
1	17.12.21 12:31:38	М	Änderung der lokalen Synchronisationsda-
			tenbank
4	17.12.21 12:48:33	0	USB-Speichermedium mit der Serien-Nr.
			0E1145514041D91B verbunden
4	17.12.21 12:49:06	Е	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	0	Hochladen der Bilder auf imgur.com

Timeline

Legende

E Erzeugung von Daten

- L Löschung von Daten
- ${\bf M} \quad {\rm Modifizierung \ von \ Daten}$
- **O** Operationen (Ausführung, Funktion, Handlung)

Alle Zeitstempel sind in MEZ angegeben.

5.4 Untersuchungsobjekte

Objekt	Dateiname(n)	MD5-Hashwert		
	chef.E01	dc4108c131215806e6875d1a23bc9174		
	chef.E02	0d118af12fe6be02e173571b2bb0d783		
Asservat 01	chef.E03	3a0806a94c4bb2589c6aca6a4b9a0de0		
	chef.E04	32f82efa52c4e59dd30478bbf618c0bd		
	(HDD Dienstrechner)			
	vzdumplxc-102-2021_12_20-	4f96c5ceb4ea8452fbcf3b3ba9ca696f		
	18_43_21.tar.iso			
Asservat 02	vzdumplxc-102-2021_12_20-	245f199a24008aaf317338b98e7483f6		
	18_43_21.tar.zst			
	(Sicherung Nextcloud)			
Accompation	stick.E01	e635a29d107bbb994d12083bc4608cf7		
Asservat 05	(USB-Stick)			
	sus.E01	c054128195fd5b74915c560ef1295eaf		
	sus.E02	b3f474e629aa8f1eba05d3d1e812aa8		
	sus.E03	f79b4238f56dc1287133eea2def1a949		
Asservat 04	sus.E04	43479d118b6aa7cd25b5ae8774acd31f		
	sus.E05	35e9a4f822b76f174f6a5b3d8cce8410		
	sus.E06	f81743c4b784f662b898c26a3dafff5b		
	(HDD Laptop)			

 Tabelle 1:
 Untersuchungsobjekte

5.5 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 Kommandozeilenprogrammer				
		für die Image-Analyse.				
		Grafisches Programm zur Nutzung der Werk-				
Autopsy	4.19.2	zeugsammlung TSK, inklusive Plugins für zu-				
		sätzliche Funktionen.				
DegDinnen	2.0	Sammlung von Perl-Skripten zum Auslese				
Regripper	3.0	des Windows-Registry.				
Maria DD Convon	10.4	Serveranwendung für die relationale Daten-				
ManaDD Server	10.4	bank MariaDB.				

5.6 Untersuchung der Asservate



5.6.1 Asservat 01 – Festplattenimage des Dienstrechners

Bild 24: Asservat 01

Integritätsprüfung

root@forensik-pc:/mnt/evidence/202	21/0001/1\$	tail c	nef.md5su	um
dc4108c131215806e6875d1a23bc9174	chef.E01			
0d118af12fe6be02e173571b2bb0d783	chef.E02			
3a0806a94c4bb2589c6aca6a4b9a0de0	chef.E03			
32f82efa52c4e59dd30478bbf618c0bd	chef.E04			
root@forensik-pc:/mnt/evidence/202	21/0001/1\$	md5sum	chef.E*	
dc4108c131215806e6875d1a23bc9174	chef.E01			
0d118af12fe6be02e173571b2bb0d783	chef.E02			
3a0806a94c4bb2589c6aca6a4b9a0de0	chef.E03			
32f82efa52c4e59dd30478bbf618c0bd	chef.E04			
root@forensik-pc:/mnt/evidence/202	21/0001/1\$	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.

Data Content	
Hex Text	Application Source File Metadata OS Account Data Artifacts Analysis Results Context Annotations Other Occurrences
Result: 68 of	79 Result 🗲 🗲
Downloaded F	ile
Domain:	github.com
URL:	https://github.com/nextcloud/desktop/releases/download/v3.3.6/Nextcloud-3.3.6-x64.msi
Date Accessed:	2021-12-16 22:24:49 MEZ
Path:	C:\Users\el jefe\Downloads\Nextcloud-3.3.6-x64.msi
Program Name:	Microsoft Edge
Other	
Path ID:	19169
Facility.	10130
Source	
Data Source:	chef.img
File:	/img_chef.img/vol_vol3/Users/el jefe/AppData/Local/Microsoft/Edge/User Data/Default/History
1	

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).

Data Artifacte	Source	Name	Program Name	△ Date/Time
Communication Accounts (6)	対 SLUI.EXE-724E99D9.	pf	SLUI.EXE	2021-12-17 11:59:58 MEZ
- Service (4)	M BACKGROUNDTASK	HOST.EXE-AC1DA110.pf	BACKGROUNDTASKHOST.EXE	2021-12-17 12:00:03 MEZ
— 😼 Installed Programs (26)	MEXTCLOUD.EXE-4D	64E8F2.pf	NEXTCLOUD.EXE	2021-12-17 12:00:05 MEZ
— > Metadata (117)	MARTSCREEN.EXE-	9B5E4173.pf	SMARTSCREEN.EXE	2021-12-17 12:00:05 MEZ
Operating System Information (3)	V WEVTUTIL.EXE-EF58	61C4.pf	WEVTUTIL.EXE	2021-12-17 12:00:06 MEZ
Recent Documents (17)	SECURITYHEALTHSY	STRAY.EXE-41AD6DE1.pf	SECURITYHEALTHSYSTRAY.EXE	2021-12-17 12:00:08 MEZ
- M Run Programs (667)	MSEDGE.EXE-78F14	B8A.pf	MSEDGE.EXE	2021-12-17 12:00:09 MEZ
- 🧍 Shell Bags (22) 💌				
Data Content				
Hex Text Application Source File Meta	idata OS Account Data	Artifacts Analysis Res	ults Context Annotations Oth	er Occurrences
Hex Text Application Source File Meta Result: 2 of 6 Result	idata OS Account Data	Artifacts Analysis Res	ults Context Annotations Oth	er Occurrences
Hex Text Application Source File Meta Result: 2 of 6 Result +	idata OS Account Data	Artifacts Analysis Res	ults Context Annotations Oth	er Occurrences
Hex Text Application Source File Meta Result: 2 of 6 Result 🗲 🍝 Type	idata 🖌 OS Account 🍸 Data	Artifacts Analysis Res	ults Context Annotations Oth	er Occurrences
Hex Text Application Source File Meta Result: 2 of 6 Result + Type Program Name	idata 🍸 OS Account 🤺 Data	Artifacts Analysis Res	ults Context Annotations Oth	er Occurrences
Hex Text Application Source File Meta Result: 2 of 6 Result Program Name Type Path	idata 🍸 OS Account 🍸 Data	Artifacts Analysis Res	ults Y Context Y Annotations Y Oth	er Occurrences
Hex Text Application Source File Meta Result: 2 of 6 Result • Program Name Type Path Date/Time	idata 🍸 OS Account 🍸 Data	Artifacts Analysis Res	ults / Context / Annotations / Oth	er Occurrences
Hex Text Application Source File Meta Result: 2 of 6 Result ▲ Program Name Type Path Date/Time Count	data Y OS Account Y Data	Artifacts Analysis Res NEXTCLOUD.EXE /PROGRAM FILES/NEXTCI 2021-12-17 12:00:05 MEZ 6	ults Context Annotations Oth	er Occurrences
Hex Text Application Source File Meta Result: 2 of 6 Result Program Name Type Path Date/Time Count Comment	idata 🍸 OS Account 🤺 Data	Artifacts Analysis Res NEXTCLOUD.EXE /PROGRAM FILES/NEXTCI 2021-12-17 12:00:05 MEZ 6 Prefetch File	ults Y Context Y Annotations Y Oth	er Occurrences
Hex Text Application Source File Meta Result: 2 of 6 Result ● Program Name Type Path Date/Time Count Comment Source File Path	data Y OS Account Y Data	Artifacts Analysis Res NEXTCLOUD.EXE /PROGRAM FILES/NEXTCI 2021-12-17 12:00:05 MEZ 6 Prefetch File /img_chef.img/vol_vol3/W	ults / Context / Annotations / Oth	er Occurrences

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

Basic Properties	
Login:	el jefe
Full Name:	
Address:	S-1-5-21-4208391369-2489843571-724928461-1001
Type:	
Creation Date:	2021-12-12 19:08:20 MEZ
Chef Details	
Last Login:	2021-12-17 11:59:40 MEZ
Login Count:	7
Password Settings:	Password does not expire, Password not required
Flag:	Normal user account
Home Directory:	C:/Users/el jefe
Last Login:	2021-12-17 11:59:40 MEZ
Login Count:	7
Password Settings:	Password does not expire, Password not required
Flag:	Normal user account
Home Directory:	C:/Users/el jefe

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/ Nextcloud_sync.log gespeichert. In dieser Datei wurde am 17.12.2021 um 12:31:07 Uhr die Löschung eines Ordners mit dem Namen "Kalender 2022" registriert (Bild 31).

C:/Users/el jefe/Nextcloud/
timestamp duration file instruction dir modtime etag size file!d 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 00000259ocmrorx1f0j5 4 0 0 0
11:05:25 Kalender 2022/DSC_001.jpeg 8 2 1639317346 64cbddf749b15479f277c03b86d3eed9 147774 00000317ocmrorx1f0j5 4 200 0 0 a60161d9-b603-4b41-be1d-9d84f1542301
11:05:26 Kalender 2022/DSC_004.jpeg 8 2 1639319174 ec838365ebe717a8aa352e87c649123f 211764 00000269ocmrorx1f0j5 4 200 0 0 cca1d849-1a5c-4da7-9003-12facadfb5f9
11:05:26 Kalender 2022/DSC_002.jpeg 8 2 1639319019 104a145d0d261c99b704f0ba55eadc41 49555 00000276ocmrorx1f0j5 4 200 0 0 a127e9b6-d09e-4db3-ac82-c055cc8cd22c
11:05:26 Kalender 2022/DSC_003.jpeg 8 2 1639318065 a395f9e4af4f08998c0b3b92476a49aa 158024 00000267ocmrorx1f0j5 4 200 0 0 38397ce0-a1a7-4f46-92e9-585232566090
11:05:27 Kalender 2022/DSC_005.jpeg 8 2 1639319048 b2ef2fe7e71a603e302614df5cbf3f42 172610 00000316ocmrorx1f0j5 4 200 0 0 8a500fa5-34ef-4467-8a7d-5b69f5e47aa8
11:05:28 Kalender 2022/DSC_007.jpeg 8 2 1639319003 39339372613e3535faa0f58cc270f6045 94994 00000296ocmrorx1f0j5 4 200 0 0 7b176c9e-c9c0-4136-a055-0c7a41c175e7
11:05:28 Kalender 2022/DSC_008.jpeg 8 2 1639319082 7fe7daa76d0e9c1d8466363697919256 27099 00000268ocmrorx1f0j5 4 200 0 0 a29fc20d-da6b-4347-b75e-10182740a959
11:05:28 Kalender 2022/DSC_006.jpeg 8 2 1639318174 591e2132215272f168f1fc022a15ba97 316590 00000282ocmrorx1f0j5 4 200 0 0 c668f751-1324-4a27-a019-fd39bd67ebbb
11:05:28 Kalender 2022/DSC_009.jpeg 8 2 1639318801 05529a18875d378a47ea9821ad57f63c 146109 00000305ocmrorx1f0j5 4 200 0 0 b1d659c7-0b6f-4742-b99f-4e8b671cbb3a
11:05:29 Kalender 2022/DSC_010.jpeg 8 2 1639319097 8b0acea6a3f81112ed87b1d634e01619 131761 00000279ocmrorx1f0j5 4 200 0 0 f268a375-8a72-4740-8636-0c1867915557
11:05:30 Kalender 2022/DSC_011.jpeg 8 2 1639318710 351b6ba7e857af1e87e5ee18df668f57 45866 00000280ocmrorx1f0j5 4 200 0 0 9a0ed03f-83f5-4216-8cc6-a774f17d63ec
11:05:30 Kalender 2022/DSC_012.jpeg 8 2 1639319118 7ce063f69535c5b031caaf82258fe5f4 46257 00000265ocmrorx1f0j5 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 639320839 61b60d0920b8b 0 00000259ocmrorx1f0j5 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)

Bild 31: Log-Datei der Client-Software

Der Client führt eine lokale Datenbank aller relevanter Dateien im synchronisierten Verzeichnis in der Datenbankdatei C:/Users/el jefe/Nextcloud/.sync_6fc321ba-8114.db. Bei der Betrachtung mit dem X-Ways Hex-Editor zeigt diese Artefakte gelöschter Einträge (Bild 32).

Name A	Description	Y Size Y Created	Modified	TRecord changed	Y Attr.	Ist sector	Analysis	
. = eljefe (4.998)	existing, already viewed	890 MB 12.12.2021 19:08:24	17.12.2021 12:05:18	17.12.2021 12:05:18		1.017.912		
. = Nextcloud (4)	existing, already viewed		3 17.12.2021 12:40:49	17.12.2021 12:40:49		26.363.840		
.owncloudsync.log	existing, already viewed	0 B 17.12.2021 12:05:20	0 17.12.2021 12:05:20	17.12.2021 12:05:20	Α	6.482.794		
sync_6fc321ba8114.db	existing, file contents unknown (partially),	112 KB 17.12.2021 12:05:19	9 17.12.2021 12:40:49	17.12.2021 12:40:49	HA	26.363.864		
sync_6fc321ba8114.db-wal	prev. existing, data not necessarily intact, a	773 KB 17.12.2021 12:05:19	0 17.12.2021 12:31:38	17.12.2021 12:31:38	HA	26.364.016		
Desktop.ini	existing	76 B 17.12.2021 12:05:13	3 17.12.2021 12:05:18	17.12.2021 12:05:18	SH	6.465.938		
Partition File Preview	Details Gallery Calendar Legend toindex_key_value_store_1key_value_store0_0	Raw Sync 🛰 🎢 a70 0 f		ON metadata(inod	e)	- Loindexr	metadata file	
emetadatametadata CREATE T tadata(fileid)/ 0.0 C 0 indexsqlit 0.0 00 00 00 00 00 00 00 00 00 00 00	ABLE metadata(pP0000) 0 iindexmetadata_in e_autoindex_metadata_1metadata00 0000 •2000000000000000000000000000000	odemetadatal CREATE INL	CX metadata_mode		0,00 0 0	e onidexi	netadata_me	_idmetadatall CREA
r(key))-0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0	ABLE metadata(pP0 00) 0 indexmetadata_in e_autoindex_metadata_1metadata0 0 00 µ ¥20 10 0 0 0 0 50 0 0	odemetadatal CREATE INL	JEX meradara_inode			2 Ondexa	netauata_ne	_idmetadatal CREA
(Trey),	ABLE_metadata[pP0 ID] 0 indexmetadata_in autoindex_metadata_tmetadata1 (10)6DNVCKR0 0 ID A0 0 0 0 0 MSI 0 0] 12,pepd], 0 affU N7ce063f69535c5b031caaf825 11)pegd], 0 affU N7ce063f69535c5b031caaf825 11)pegd], 0 affU N7ce063f69535c5b031caaf825 9)pegd - CaffU 0 0 552918875d378a47e82821a 000, jepg 1 yaf1 2591e37247816875d378a47e8821a 000, jepg 1 yaf1 7/Fo7daa75040527814875d378a47e8821a 000, jepg 1 yaf1 00, jepg 1 yaf1 10 b2e7247816750235faa6766c270 5) pegd 1 CaffU 0 b2e72167716050235faa6766c270 5) pegd 1 CaffU 0 b2e7216771a603e302614df5cbf	odemetadatali CREATE INL 8fe54400000265ocmronx1f0j 66885700000280ocmronx1f0 44016190000279ocmronx 45763200000305ocmronx1f 50430700002880cmronx1f 6045000002860cmronx1f0j 3442000003160cmronx1f0j51	5WDNVR*±1a042a3 5WDNVR*±35588e8 10j5WDNVR ±b0 0j5WDNVR ±b0 j5WDNVR1*2635a 95WDNVR10265a WDNVR1 sl 928a60 NDNVR sl 928a60	36e6c5784bda669d c86b9467c7509462 222d3ca3dd87508a acbb5ba3467e561 8843de258b0d54a 4af104da0951530d 4893afa50039b240 3e829dc784deaa8d	0defbc4 e8a384 454b4c2 ab0745b 2774b2c 48fa516 691adf9 e5da90fr	7e72e69de5 19f9727502f ff518ffea31c 049e2779ef ca22da31ce 1a41f13f393 082a87cbfbo c10a6295eb	0 a0 0 A0 0 0 0 %0 0 A0 0 0 0 %0 0 A0 0 0 rec 0 0 0 A0 7700 0 0 0 A0 10 .0 0 A0 0 0 .0 0 A0 0 3 æ0 0 A0 0	idmetadatai/ CREA 0 0 0 M50 0 0] 0 0 0 0 M50 0 0] 0 0 0 0 M50 0 0] 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0
((key),-1 0 C4P intersequite au mentadatametadata CREATE T adata[fileid) 0 0 0 0 0 0 0 0 0 0 0 0 10 0 0 0 0 0 0	ABLE_metadata[pP0 ID] 0 indexmetadata_in autoindex_metadata_tmetadata1 10 p 20 10 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0	odemetadatali CREATE INL 8fe5f400000265ocmrorx1f0j 568/8700000280ocmrorx1f0 462/16300000279ocmrorx 462/16320000279ocmrorx 163/2630000288ocmrorx1f0 91925600000268ocmrorx1f0j 3f4200000316ocmrorx1f0j5 000267ocmrorx1f0j5WDNV	5WDNVR ±18042a3 5WDNVR ±18042a3 5WDNVR *5356868 105WDNVR ±5656868 105WDNVR ±565 5WDNVR ±565 5WDNVR ±585 WDNVR ±585 WDNVR ±585 800NVR ±585	36e6c5784bda669d c86b9467c750946 212df3ca3dd87508 aachb5b31667e56 8843de258bd54a 24104da0951530d 1469afa5b0939b240 3e829dc784deaa8d 18ca946de9df07c3	0defbc4 e8a384 454b4c2 ab0745b 774b2c 48fa516 691adf9 e5da90fi 04123c7	7e72e69de5i 19f9727502fi ff518ffea310 049e2779ef ca22da31ce 1a41f13f393 082a87cbfbc c10a6295eb e97320 0 =0	0 a0 0 A0 0 0 0 ½0 A0 0 0 1½0 A0 0 0 b710 0 A0 0 b710 0 0 A0 0 b71d 0 0 0 50 0 A0 0 3 æ0 0 A0 0 0 A0 0 0 0 0	dmetadatal CREA
(Treey),	ABLE metadata[pP0 ID] D indexmetadata_in a utoindex. metadata[pP0 ID] D indexmetadata_in 0 p 420 10 0 10 0 0 0 0 0 0 0 0 0 0 0 0 0 xtt0j6DNVCKR0 D D AD 0 0 0 0 0 0 0 0 11 jpegi J affD IVCe06365953655031caaf8253 11 jpegi J affD IVCe06365953655031caaf8253 19 jpegi J affD IVCe0637695365784788022 10 jpegi J affD IVCe063763784788022 10 jpegi J affD IVCe05378183753784788022 10 jpegi J affD IVCe05378183753784788022 10 jpegi J affD IVCe3528183753784788022 10 jpegi J affD IVCe3528183753784788022 10 jpegi J affD IVCe3528183753784788022 10 jpegi J affD IVCe37818355784788022 10 jpegi J affD IVCe37818355784788022 10 aff 1a395f9e484f08998c0b3b924768498a00 pl zyaffD e104a145d0d261c9b704f0ba55eadc4 104.jpegi [affD 1+c838365ebe71788a35287c6	odemetadatali CREATE INL 8fe55400000265ocmrorx1f0ji 66885700000280ocmrorx1f0 440161900002760ocmrorx1 15ba37000002780ocmrorx1 19125600000286ocmrorx1f0 19125600000286ocmrorx1f0 3420000316ocmrorx1f0ji 000267ocmrorx1f0jiSWDL 100000276ocmrorx1f0jiSWDL 19123f00000269ocmrorx1f1	SWDNVR ±104203 SWDNVR ±104203 SWDNVR ±06424 SWDNVR ±06444 SWDNVR ±06444 WDNVR ±06244 WDNVR ±082450 WDNVR ±08250 R iH825150be428a R iH825150be428a	36e6c5784bda669d c86b9467c7509462 22d3c3a3dd7508a acbb5b3167c266 8843de28bd64aa 41104da9515300 4499afa5b033b240 3e829dc784deaa8d 18ca946de9df07c30 520d433816ddc7 411e6d509a38164	0defbc4 e8a384 454b4c2 ab0745b 2774b2c 48fa516 691adf9 e5da90fi 04123c7 5c5cd32 510a23fc	7e72e69de5 ff510ffea31c 049e2779ef ca22da31ce 1a41f13730 82a87cbfb c10a6295eb e97320 0 =0 4164400 10 0b15d8825e	0 a0 0 A0 0 0 1 %0 0 A0 0 0 1 %0 0 A0 0 700 u0 A0 5714 0 0 0 0 A0 0 20 \$0 0 A0 0 0 A0 0 0 0 0 0 A0 0 0 0 A0 0 0 0 0 A0 0	dmetadatal CREA

\chef, P2\Users\el jefe\Nextcloud\.sync_6fc321ba8114.db

Bild 32: Datenartefakte aus der SQLite-Datenbank des Nextcloud-Clients

Der Verzeichnisname "Kalender 2022" des laut Log-Datei gelöschten Verzeichnisses tritt hier ebenfalls auf. Es befinden sich insgesamt folgende 13 einzigartige Dateinamen im nicht zugewiesenen Bereich der Datenbankdatei, was auf deren Entfernung

hinweist:

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					

 Tabelle 3: Dateinamen aus der Datenbank des Nextcloud-Clients

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

Chef Chef.EO Chef.E	L (Unallocated: 0-2047) (NTFS / exFAT (0x07): 2048-: (NTFS / exFAT (0x07): 11264 \$CorphanFiles (3007) \$CarvedFiles (655) \$Extend (9) \$Recycle.Bin (4) \$S-1-5-21-4208391369-244 Recycle.Bin/S-1-5-21-4208391 \$Summary	1126399) 00-33552383) 39843571-724928461-1000 (3 369-2489843571-724928461-) 1001		
Name	Modified Time	Change Time	Access Time	Created Time	Size
\$ILEJESJ.Ink	2021-12-12 19:32:32 MEZ	2021-12-12 19:32:32 MEZ	2021-12-12 19:32:32 MEZ	2021-12-12 19:32:32 MEZ	116
\$IZNA305	2021-12-17 12:30:59 MEZ	2021-12-17 12:30:59 MEZ	2021-12-17 12:30:59 MEZ	2021-12-17 12:30:59 MEZ	110
\$RFMR914.lnk	2021-12-12 19:42:34 MEZ	2021-12-12 19:44:52 MEZ	2021-12-12 19:44:52 MEZ	2021-12-12 19:42:34 MEZ	2270

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
                   Start
0000000000
                                                    Length
0000000001
       Slot
                                                                    Description
                                    End
                                    0000000000
                                                                    Primary Table (#0)
000:
       Meta
                                                                    Unallocated
                    0000000000
                                                    0000002048
001:
                                    0000002047
                                                                    NTFS / exFAT (0x07)
NTFS / exFAT (0x07)
002:
      000:000
                    0000002048
                                    0001126399
                                                    0001124352
003:
       000:001
                    0001126400
                                    0033552383
                                                    0032425984
004:
                    0033552384
                                    0033554431
                                                    0000002048
                                                                    Unallocated
root@forensik-pc:/mnt/evidence/2021/0001/1$ fls -r -o
                                                                   1126400 chef.E0? | grep "SYSTEM$"
 -++ r/r 78080-128-4:
root@forensik-pc:/mnt/evidence/2021/0001/1$ 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]
                                : Generic Flash Disk USB Device
: 2021-12-17 11:09:39Z
     FriendlyName
     First InstallDate
     InstallDate
                                  2021-12-17
                                                11:09:39Z
                                  2021-12-17
     Last Arrival
                                                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
        11:30:092]

        Properties LastWrite
        :
        [2021-12-17
        11:30:092]

     .
FriendlyName
                                  Hama FlashPen USB Device
     First InstallDate
                                : 2021-12-17 11:30:09Z
                                  2021-12-17
                                                11:30:097
     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:

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

 Tabelle 4:
 Verbundene Speichermedien (Asservat 01)



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\$ md5sumcheck lxc-102.md5sum
vzdump-lxc-102-2021_12_20-18_43_21.tar.iso: 0K

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.



Bild 37: Integritätsprüfung des Nextcloud-Snapshots

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

Gescheiterte Anmeldungsversuche

Für die Untersuchung der Anmeldungsversuche 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 Anmeldungsversuche (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 peytcloud/data/«peytcloud lon« PHP version and	/LogicalFileSet1/root/latest zip/nextcloud/core/doc/admin/i	2021-11-26 21:53:54 ME7
tions Other Occurrences		
app::://noex-,*metnod:::"GET*,*url":*/favicon.ico*,*message t '/nextcloud/index.php')","Code":0,"Trace":[{"file":*//var/wwv	:"The requested uni(mavicon.ico) cannot be processed by the //html/nextcloud/lib/base.php","line":944,"function":"getRawP	script='/nextciouq/index.pnp")" athInfo","class":"OC\\AppFran
p/Request.php", "Line":770, "CustomMessage":"	/login" "message":"Login failed: admin (Remote IP: 192.168.1 login", "message":"Login failed: admin (Remote IP: 192.168.1 p/login", "message":"Login failed: admin (Remote IP: 192.168. o/login", "message":"Login failed: admin (Remote IP: 192.168. /login", "message":"Login failed: admin (Remote IP: 192.168.1).	I.11)", "userAgent": "Mozilla/5.0 11)", "userAgent": "Mozilla/5.0 .1.11)", "userAgent": "Mozilla/5 1.11)", "userAgent": "Mozilla/5. .11)", userAgent": "Mozilla/5.0

Bild 38: Auszug aus dem Nextcloud-Log

tempel der Anmeldungsversuche aus dem Nextcloud-Log: Alle Anmeldungsversuche

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

 Tabelle 5:
 Anmeldungsversuche

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

Des Weiteren speichert der Nextcloud-Server Bruteforce-Attacken in seiner Datenbank¹. Darin sind 5 Anmeldungsversuche 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 Bruteforce-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.

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

Tabelle 6: Gelöschte Dateien in der Cloud

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



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 gelöschtes Verzeichnis mit dem Namen "Kalender 2022" (Bild 42).

root	oot@forensik-pc:/mnt/evidence/2021/0001/3\$ mmls stick.E0?								
DOS	DOS Partition Table								
0ffs	set Sector:	0							
Unit	s are in 5	12-byte sector	^S						
	Slot	Start	End	Length	Description				
000:	Meta	0000000000	00000000000	0000000001	Primary Table (#0)				
001:		00000000000	0000002047	0000002048	Unallocated				
002:	000:000	0000002048	0000239615	0000237568	Win95 FAT32 (0x0c)				
003:		0000239616	0000251903	0000012288	Unallocated				
root	@forensik-	pc:/mnt/evide	nce/2021/0001,	/3\$ fls -o 204	8 stick.E01				
r/r	3: FLASHPE	EN128 (Volume	Label Entry)						
d/d	6: System	Volume Inform	nation						
d/d	* 8:	Kalender 202	22						
d/d	10: .Trash	-1000							
v/v	3741379:	\$MBR							
v/v	3741380:	\$FAT1							
v/v	3741381:	\$FAT2							
V/V	3741382:	\$0rphanFiles	5						

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	F	ile		Prev	iew		Deta	ils	Ga	llery		Cale	ndar	1	Leg	end	Sync	• A1≡
Offset	0	1	2	3	4	5	6	7	8	9	Α	В	С	D	Е	F	ANSI ASC	II 🔺
00000000	46	4C	41	53	48	50	45	4E	31	32	38	08	00	00	17	8E	FLASHPEN128	Ž
00000010	ЗF	54	3F	54	00	00	17	8E	ЗF	54	00	00	00	00	00	00	?T?T Ž?T	
00000020	42	20	00	49	00	6E	00	66	00	6F	00	OF	00	72	72	00	B Infor	r
0000030	6D	00	61	00	74	00	69	00	6F	00	00	00	6E	00	00	00	matio n	
00000040	01	53	00	79	00	73	00	74	00	65	00	OF	00	72	6D	00	Syste n	n
00000050	20	00	56	00	6F	00	6C	00	75	00	00	00	6D	00	65	00	Volu m	e
00000060	53	59	53	54	45	4D	7E	31	20	20	20	16	00	55	BC	65	SYSTEM~1 U	ke 🛛
00000070	91	53	91	53	00	00	BD	65	91	53	03	00	00	00	00	00	`S`S ¾e`S	
08000000	E5	4B	00	61	00	6C	00	65	00	6E	00	OF	00	E9	64	00	åKalen é	d
00000090	65	00	72	00	20	00	32	00	30	00	00	00	32	00	32	00	er 202	2
0A000000	E5	41	4C	45	4E	44	7E	31	20	20	20	10	00	92	C1	65	åALEND~1 '	Áe
000000B0	91	53	91	53	00	00	49	58	8E	53	06	00	00	04	00	00	'S'S IXŽS	
00000000	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 ch	nef stick stick, Volume						
\Kalender 2022							
□ ▼Name▲	Description	Y Size	Created	Modified	TRecord changed	Attr.	Ist sector
(Root directory)	existing						3.908
🗆 😰 . = Kalender 2022 (7)	prev. existing, data not necessarily intact		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		Α	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		Α	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		Α	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		Α	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		Α	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		Α	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		Α	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:

Erzeugung	Dateiname	Тур	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

 Tabelle 8: Alle vom USB-Stick geborgenen Dateien

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.

Directory Tree								
€ →								
	sk.E01 \$OrphanFiles (5) \$CarvedFiles (13) \$Unalloc (1) Kalender 2022 (9) System Volume Information (4)							
Listing								
/img_stick.E01/Syste	/img_stick.E01/System Volume Information							
Table Thumbn	ail Sum	mary						
Name		S	С	0	Modified Time			
退 (current fold	er]				2021-12-17 12:48:33 MEZ			
退 (parent folde	r]				0000-00-00 00:00:00			
IndexerVolu	neGuid	▽		0	2021-12-17 12:48:33 MEZ			
•								
Data Content								
Hex Text A	pplication	File	e Meta	data	OS Account Data Artifa			
Strings Indexe	d Text	Fransla	ation]	· · ·			
Page: 1 of 1 Page (<> Matches on page: - of - Match								
{063E9BAA-E59C-4	993-8EB0-F	95B3	8D68A	2D}				

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

/img_chef.E01/vol_vol3/Windows/System32/config							
Name	S	C	0	Modified Time	Change Time	Access Time	
SOFTWARE			1	2021-12-17 12:41:00 MEZ	2021-12-12 18:45:06 MEZ	2021-12-17 12:41:00 MEZ	
SOFTWARE.LOG1			1	2018-09-15 08:09:26 MESZ	2021-12-12 18:44:01 MEZ	2018-09-15 08:09:26 MESZ	
Data Content Hex Text Application File Metadata OS Acco	Data Content Image: Context Co						
Call VolumeInfoCache		Ē	Nan Type	e: VolumeLabel e: REG_SZ			
			- Val FLA	ue SHPEN128			

Bild 48: Bezeichnung "FLASHPEN128" für Laufwerk "E" im Registry

Keyword search						
△ Name	Location					
RegRipper /img_chef.E01/vol_vol3/Windows/System32/config/SOFTWARE	RegRipper /img_chef.E01/vol_vol3/Windows/System32/config/SOFTWARE					
RegRipper /img_chef.E01/vol_vol3/Windows/System32/config/SYSTEM	RegRipper /img_chef.E01/vol_vol3/Windows/System32/config/SYSTEM					
Data Content Hex Text Application File Metadata OS Account Data Artifacts Analysis Results Context Annotations Other Occurrences Strings Indexed Text Translation Page: 68 of 73 Page Matcher on page: 1 of 1 Match 100% P Reset						
Parameters/FirewallPolicy/DomainProfile/AuthorizedApplications/List key for exceptions added to the firewall; use the fw_config.pl plugin. Launching volinfocache v.20120822 (Software) Gets VolumeInfoCache from Windows Search key Microsoft/Windows Search/VolumeInfoCache C: - LastWrite: Sun Dec 12 17:52:14 2021 DriveType: Fixed VolumeLabel: E: - LastWrite: Fri Dec 17 11:30:10 2021 DriveType: Fixed VolumeLabel: FLASHPEN128						

Bild 49: Auftreten der Dateisystembezeichnung "FLASHPEN128" im Registry



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

Data Content			-			
Hex Text Applic	ation Source File Metadata OS Account Data Artifacts Analysis Results Context Annotations Other Occurrences					
Result: 1 of 1	Result <	Recent Documen	ts			
Туре	Value	Source(s)				
Path	E:\Kalender 2022	RecentActivity				
Path ID	h ID -1 RecentActivity					
Date Accessed	0000-00-00 00:00	RecentActivity	1			
Source File Path	/img_chef.E01/vol_vol3/Users/el jefe/AppData/Roaming/Microsoft/Windows/Recent/AutomaticDestinations/f01b4d95cf55d32a.automaticDestinations-ms/E:\Kalender 2022.Ink		1			
Artifact ID	9223372036854665563					

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



5.6.4 Asservat 04 – Festplattenimage des Laptops

Bild 52: Asservat 04

Integritätsprüfung

<pre>root@forensik-pc:/mnt/evidence/20</pre>	21/0001/4\$	tail s	us.md5sur	n
c054128195fd5b74915c560ef1295eaf	sus.E01			
b3f474e629aa8f1eba05d3d1e812aa83	sus.E02			
f79b4238f56dc1287133eea2def1a949	sus.E03			
43479d118b6aa7cd25b5ae8774acd31f	sus.E04			
35e9a4f822b76f174f6a5b3d8cce8410	sus.E05			
f81743c4b784f662b898c26a3dafff5b	sus.E06			
root@forensik-pc:/mnt/evidence/20	21/0001/4\$	md5sum	n 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/20	21/0001/4\$	md5sum	ıcheck	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 Gerätename ist "DESKTOP-37E56OH" (Bild 55) mit dem Administrationsnutzer "jansen" (Bild 54).

Internetaktivitäten des Laptops

対 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/vol_vol3/Users/jansen/Downlo Table Thumbnail Summary	ads										
Name	s	с	0	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 Anmeldungsversuche 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.	l.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	zsOPreNQRJiT7lO9
2	searchbar-history	imgut	1	1639738185304000	1639738185304000	mf/Fq8f/RGuZFlUJ

Bild 59: Mehrfache Anmeldungsversuche 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	482e134bf280	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

Lineret teiler Immunities Lineret teiler Immunities Lineret teiler Lineret teiler<	Name		Location	Size	MD5 Hash	Modified Time	Change Time	Access Time	Created Time
Insert Column Insert Links Starting visibles/second-basity/clinks/second-basity/second-basity/clinks/second-basity/second-	[current folder]	/img_sus.E01/vol_vol3/Users/janser	/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 ME
0 = 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0,	[parent folder]	/img_sus.E01/vol_vol3/Users/janser	/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	2021-12-12 22:09:43 ME
0.00000000000000000000000000000000000	DSC_001.jpeg	/img_sus.E01/vol_vol3/Users/janser	/Desktop/Kalender 2022/DSC_I	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 ME
D E 05 00 Jung mg un 10 E300 v v 40 Management/bitating to use 242010; 20 mg 1800 M 6623b 023 Med 100 V 1	DSC_002.jpeg	/img_sus.E01/vol_vol3/Users/janser	/Desktop/Kalender 2022/DSC_I	002.jpeg 49555	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 ME
0.00000000000000000000000000000000000	DSC_003.jpeg			003.jpeg 158024	246c853ca7034eb7f4070763c4fa6ba6		2021-12-17 11:48:59 MEZ	2021-12-17 11:49:06 MEZ	
0 00 00 00 00 00 00 00 00 00 00 00 00 0	DSC_004.jpeg	/img_sus.E01/vol_vol3/Users/janser	/Desktop/Kalender 2022/DSC_(004.jpeg 211764	83b407c98a8ee7608a944213a08dc697	2021-12-12 15:26:14 MEZ	2021-12-17 11:48:59 MEZ	2021-12-17 11:49:06 MEZ	2021-12-17 11:48:59 ME
0.00000000000000000000000000000000000	DSC_005.jpeg	/img_sus.E01/vol_vol3/Users/janser	/Desktop/Kalender 2022/DSC_I	005.jpeg 172610	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 M
0 00 00 /00 /00 /00 /00 /00 /00 /00 /00	DSC_006.jpeg	/img_sus.E01/vol_vol3/Users/janser	/Desktop/Kalender 2022/DSC_(006.jpeg 316590	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 MI
0.00 CORR mm xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx	DSC_007.jpeg	/img_sus.E01/vol_vol3/Users/janser	/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 M
0 00 CONTRACT 0 00 CO	DSC_008.jpeg	/img_sus.E01/vol_vol3/Users/janser	/Desktop/Kalender 2022/DSC_(008.jpeg 27099	554b287e802e1eae97b1/656e8b85607	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 MI
DBC_000pp mp_1xx820vd_vd_vdXxxes/beexep0edstagte/beexe	DSC 009.ipeg	/img_sus.E01/vol_vol3/Users/janser	/Desktop/Kalender 2022/DSC_(009.jpeg 146109	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 M
0.00_011_ppg /mgsub_302.04_01_wid3.0em/genum0-destragationeder 2022/05[_011_ppg 4666 802.4271/05/818/09/16880468600 2021.15.13.13.8.102 2021.15.13.11.46.591									
050_012/pege //mg_sus_802/vel_yel/30/kers/seven0-bettags/kalender/2022/052_012_peg 48237 8007139eet154.19609516751159 2021-12-17.11-48-59 MEZ	DSC_010.jpeg	/img_sus.E01/vol_vol3/Users/janser	/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 MI
Commer I Then: Application: File Metadata: OS Account: Data Antifacts: Analysis Results: Control: Annotations: Other Occurrences: Image: Control: Annotations: Control: Annotations: Control: Annotations: Control: Contro: Contro: Contro	DSC_010.jpeg DSC_011.jpeg	/img_sus.E01/vol_vol3/Users/janser /img_sus.E01/vol_vol3/Users/janser	/Desktop/Kalender 2022/DSC_/ /Desktop/Kalender 2022/DSC_/	010.jpeg 131761 011.jpeg 45866	367e011e99c8610b8b153d00b6789bfd 892a4c27c5b7fe1809ef1fb80a696e06	2021-12-12 15:24:56 MEZ 2021-12-12 15:18:30 MEZ	2021-12-17 11:48:59 MEZ 2021-12-17 11:48:59 MEZ	2021-12-17 11:49:06 MEZ 2021-12-17 11:49:06 MEZ	2021-12-17 11:48:59 M 2021-12-17 11:48:59 M
	DSC_010.jpeg DSC_011.jpeg DSC_012.jpeg DSC_012.jpeg	img_sus.E01/vol_vol3/Users/janser img_sus.E01/vol_vol3/Users/janser img_sus.E01/vol_vol3/Users/janser	i/Desktopi/Kalender 2022/DSC_ I/Desktopi/Kalender 2022/DSC_ I/Desktopi/Kalender 2022/DSC_ I/Desktopi/Kalender 2022/DSC_ I/Desktopi/Kalender 2022/DSC_	010.jpeg 131761 011.jpeg 45866 012.jpeg 46257 sis Results Y Context	367e011e99c810b8b153a00b6789cH 892a4c27c5a7fe1809ef1fb80a69fe66 (8/3/3159eee154a14609d51e751159	2021-12-12 15:24:56 MEZ 2021-12-12 15:18:30 MEZ 2021-12-12 15:25:18 MEZ	2021-12-17 11:48:59 MEZ 2021-12-17 11:48:59 MEZ 2021-12-17 11:48:59 MEZ	2021-12-17 11:49:06 MEZ 2021-12-17 11:49:06 MEZ 2021-12-17 11:49:06 MEZ	2021-12-17 11:48:59 N 2021-12-17 11:48:59 N 2021-12-17 11:48:59 N
	DSC_010.jpeg DSC_011.jpeg DSC_012.jpeg Content Text Appli	img_sus.E01/vol_vol3/Users/janser img_sus.E01/vol_vol3/Users/janser img_sus.E01/vol_vol3/Users/janser cation File Metadata OS Accou	i/Desktopi/Kalender 2022/DSC_ I/Desktopi/Kalender 2022/DSC_ I/D esktopi/Kalender 2022/DSC_ I/D esktopi/Kalender 2022/DSC_ I/D esktopi/Kalender 2022/DSC_	010.jpeg 131761 011.jpeg 45866 012.jpeg 46257 sis Results / Context	367e011e99c810b80153d00b6789cld 992a4c27c557b1809e11b80a696c66 (8783159eee154a14659d51e751159 Annotations Other Occurrences	2021-12-12 15:24:56 MEZ 2021-12-12 15:18:30 MEZ 2021-12-12 15:25:18 MEZ #	2021-12-17 11-48-59 MEZ 2021-12-17 11-48-59 MEZ 2021-12-17 11-48-59 MEZ	2021-12-17 11-49:06 MEZ 2021-12-17 11-49:06 MEZ 2021-12-17 11-49:06 MEZ	2021-12-17 11:48:59 2021-12-17 11:48:59 2021-12-17 11:48:59
	DSC_010,jpeg DSC_011,jpeg DSC_012,jpeg DSC_012,jpeg	Img_sus_EDUvol_vol3Usersjanset Img_sus_EDUvol_vol3Usersjanset Img_sus_EDUvol_vol3Usersjanset Cation File Metadata OS Accou 28% O O Reset	Desktop/Kalender 2022DSC (Desktop/Kalender 2022DSC Desktop/Kalender 2022DSC N ← Costs Artifacts ← Analyg	010.jpeg 131761 011.jpeg 45866 012.jpeg 46257	367-011-05/0610080153800679806 929-427-267-067041080069060 929-427-267-067041080069060 929-1427-267-067041080069060 9291359eee154a146009051a751159 * Annotations * Other Occurrences	2021-12-12 15:24:56 MEZ 2021-12-12 15:18:30 MEZ 2021-12-12 15:18:30 MEZ	2021-12-17 11-48-59 MEZ 2021-12-17 11-48-59 MEZ 2021-12-17 11-48-59 MEZ	2021-12-17 11-19-06 MEZ 2021-12-17 11-49-06 MEZ 2021-12-17 11-49-06 MEZ	2021-12-17 11-48:59 M 2021-12-17 11-48:59 M 2021-12-17 11-48:59 M
	DSC_010,jpeg DSC_011,jpeg DSC_012,jpeg DSC_012,jpeg Content Text Appli 0* O C	イmg, sa 601/vel, vel 30.ben/jene /mg, sa 601/vel, vel 30.ben/je	UPEAKopKalender 2022DSC UPEAKopKalender 2022DSC DreaktopKalender 2022DSC UPEAKopKalender 2022DSC Not PData Artifacts Analys	010.jpg 131761 011.jpg 4566 012.jpg 46257 sis Results Context	37-011-894801.0888.153.0007-78966 9924.427-058-1940-1880-054600 9730139vee134a14609631a751159 *#netablos: Other Occurrences	2021-12-12 152455 MEZ 2021-12-12 153518 MEZ 2021-12-12 153518 MEZ	2021-12-17 11-48-59 MEZ 2021-12-17 11-48-59 MEZ 2021-12-17 11-48-59 MEZ	2021-12-77 11-49-06 MEZ 2021-12-17 11-49-06 MEZ 2021-12-17 11-49-06 MEZ	2021-12-17 11-48-59 M
	DSC_010,jpeg DSC_011,jpeg DSC_012,jpeg DSC_012,jpeg	السرية مع الكانية بالالكانية المنافعة المنافعة المنافعة المنافعة المنافعة المنافعة المنافعة المنافعة المنافعة ا السري بعد 2012 من الألكانية المنافعة المنافعة المنافعة المنافعة المنافعة المنافعة المنافعة المنافعة المنافعة ال منافعة المنافعة المنافعة منافعة المنافعة من منافعة المنافعة ال منافعة المنافعة المنافعة منافعة المنافعة من منافعة المنافعة المنافعة المنافعة من المنافعة المنافعة منافعة منافعة من من منافعة المنافعة المنافعة المنافعة المنافعة المنافعة المنافعة منافعة منافعة منافعة منافعة منافعة منافعة منافعة من منافعة منافعة من منافعة من منافعة من منافعة منافعة منافعة من منافعة منافعة من منافعة من من	DesktopKalender 2022DSC iDesktopKalender 2022DSC DesktopKalender 2022DSC N [™] Data Antifacts [™] Analys	010.jpeg 231761 011.jpeg 45866 012.jpeg 46257 sis Results / Context	13F011E90601088135300578966 2023427205F1040180805400 40701590ee0154a146009051e751159 Constations ' Other Occurrences	2021-12-12 15 25 456 MEZ 2021-12-12 15 24 56 MEZ 2021-12-12 15 25 51 B MEZ	2021-12-17 11-48-59 MEZ 2021-12-17 11-48-59 MEZ 2021-12-17 11-48-59 MEZ	2021-12-17 11-49-06 MEZ 2021-12-17 11-49-06 MEZ 2021-12-17 11-49-06 MEZ	2021-12-17 11-48-59 M
	DSC_010.jpeg DSC_011.jpeg DSC_012.jpeg DSC_012.jpeg ontent Text Appli 0 O	Img us BDIvel vel3berdjoner Img us BDIvel vel3berdjoner Im	MesktopKinklender 2022DSC (DesktopKinender 2022DSC (DesktopKinender 2022DSC (DesktopKinender 2022DSC (DesktopKinender 2022DSC)	010 (peg) 133761 011 (peg) 4586 012 (peg) 46257 sis Results Context	3470-011494063038-83.53000679900 2002-021-0219-0210-01149-01490 002159xee-154a.14609401e731159 74900401497 006er 0400471e7455	2021-12-12 15 25 456 MEZ 2021-12-12 15 25 456 MEZ 2021-12-12 15 25 18 MEZ	2021-12-17 11-48-59 MEZ 2021-12-17 11-48-59 MEZ 2021-12-17 11-48-59 MEZ	2021-12-17 11-49-06 MEZ 2021-12-17 11-49-06 MEZ 2021-12-17 11-49-06 MEZ	2021-12-17 11-48-59 N 2022-12-17 11-48-59 N 2021-12-17 11-48-59 N
	DSC_010.jpeg DSC_011.jpeg DSC_012.jpeg DSC_012.jpeg	Amg tao 2012vity vel33berdyman Amg, tao 2012vity vel33berdyman Amg, tao 2012vity vel33berdyman ag, tao 2512vity vel33berdyma	Desktopfkelender 2020/05, (Desktopfkelender 2020/05, (Desktopfkelender 2020/05, (R * 164a Artifister 7 Anslyt	010.jpeg 231761 01.jpeg 45866 012.jpeg 45257 sis Results Context	34701104960301883.53000679900 200242-25981104014084960 (8701359eet154814609511c51159 (Annotations) Other Occurrences	2011-12 15 5455 MFZ 2011-12 15 5455 MFZ 2011-12 15 15 18 MFZ 2011-12 15 15 18 MFZ 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0	2011-11 11-489 MEZ 2011-12 11 14-499 MEZ 2021-12 11 14-499 MEZ	2021-12-17 11-496 MEZ 2021-12-17 11-496 MEZ 2021-12-17 11-496 MEZ	2021-12-17 11-48-59 M
	DSC_010,jpeg DSC_011,jpeg DSC_012,jpeg DSC_012,jpeg Text Appli or OC	img μα 620-να γκ3/bandpane mg μα 620-να γκ3/bandpane Amg μα 620-να γκ3/bandpane Amg μα 620-να γκ3/bandpane (mg μα 620-να γκ3/bandpane (mg μα 620-να γκ3/bandpane) (mg μα	Desktopfischerder 2020/05/ Umstragfischerder 2020/05/ Desktopfischerder 2020/ Desktopfischerder 2020/ Desktopfischerd	010 (peg) 333761 011 (peg) 45866 012 (peg) 46257 als Results Context	3470-011494063038-83.53000679900 2002-02398-12408-14900-01499-0149-01499-0149-01399-0149-01499-0149-013199 002159ee-124ea146094014-013199 Annotations 000er0400-0149-0149-0149-0149-0149-0149-0149-	2011-12 15 2545 MEZ 2011-12 15 2545 MEZ 2011-12 15 15 18 MEZ 2011-12 12 15 25 18 MEZ 7	2011-111.469 MIZ 2011-1211.469 MIZ 2011-1211.469 MIZ	2021-12-17 11-060 MIZ 2021-12-17 11-060 MIZ 2021-12-17 11-060 MIZ	2021-12-17 11-48-59 M
	DSC_010,jpeg DSC_011,jpeg DSC_012,jpeg DSC_012,jpeg	Amg yaa SOUvet yed Xaberdyaana Amg yaa Souvet yed Yaberdyaana Amg yaa Souvet yed Yaberdyaanaa	Destanguisedere 2020.05. Constanguisedere 2020.05. Destroyklander 2020.05. Nestroyklander 202	010 (peg) 433761 011 (peg) 43666 012 (peg) 40567 sis Results Context	3470-011494060.0188-5330006-79900 2002-02-2015-010240-014030-9606 (070159eert 548146096516751159 (Annotations)) Other Occurreces	2011-12 15 5245 MEZ 2011-12 15 15 45 MEZ 2011-12 12 15 55 18 MEZ 2011-12 12 15 55 18 MEZ 9 9 9 9 9 9 9 9 9 9 9 9 9 9 9 9 9 9 9	2011-21711-469 MEZ 2011-21711-469 MEZ 2021-23711-4699 MEZ	2021-12-17 11-060 MEZ 2021-12-17 11-060 MEZ 2021-12-17 11-060 MEZ	2021-12-17 11-06-59 M 2021-12-17 11-06-59 M 2021-12-17 11-06-59 M
	DSC_010,jpeg DSC_011,jpeg DSC_012,jpeg DSC_012,jpeg Text Appli	img μα 620-να γα3/barnforms mg μα 620-να γα3/barnforms Amg μα 620-να γα3/barnforms A	Destanguisender 2020/06. Understagnistender 2020/06. Desktagnistender 2020/06. Desktagnistender 2020/06. Desktagnistender 2020/06. Desktagnistender 2020/06.	010 (peg) 233761 011 (peg) 45866 012 (peg) 46257 sis Results Y Context	3470110496030188353000679900 200242-2208170200618089606 0021559ee1254a14009611e731159 7 Annotations Other Oscurrences	2011-12 15 5245 MEZ 2011-12 15 15 545 MEZ 2011-12 12 15 25 18 MEZ 2011-12 12 15 25 18 MEZ 7	2011-111.469.MEZ 2011-121.11.469.MEZ 2011-121.11.469.MEZ	2021-12-17 11-069 MEZ 2021-12-17 11-069 MEZ 2021-12-17 11-069 MEZ	2021-12-17 11-48-59 M
	DSC_010.jpeg DSC_012.jpeg DSC_012.jpeg ontent Text Appli 0* O C	Amg yaa SOUvel yed Xaberdyaana Amg yaa SOUvel yed Xaberdyaana Amg yaa SOUvel yed Xaberdyaana Amg yaa SOUvel yed Xaberdyaana Amg yaa Sou yaa yaa yaa yaa yaa yaa yaa yaa yaa ya	Destanguisedere 2020.05. Constanguisedere 2020.05. Destroyklander 2020.05. Nestroyklander 2020.05. R * Dista Antilasta * Analyz	010 (peg) 133761 011 (peg) 43865 102 (peg) 45557 sis Results Context	347011049601018533000679000 200242-213961104030906 (RODISSeet 154140096516751159 (Annotations) Other Occurreces	2011-12 15 5456 MEZ 2011-12 15 5456 MEZ 2011-12 12 15 55 18 MEZ 2011-12 12 15 55 18 MEZ 9 9 9 9 9 9 9 9 9 9 9 9 9 9 9 9 9 9 9	2011-21711.469482 2011-2171.469482 2011-21711-469482 2011-21711-469482	2021-12-17 11-060 MEZ 2021-12-17 11-060 MEZ 2021-12-17 11-060 MEZ	2021-12-17 11-06-59 N 2021-12-17 11-06-59 N 2021-12-17 11-06-59 N 2021-12-17 11-06-59 N
	DSC_010,peg DSC_011,peg DSC_012,peg DSC_012,peg ontent Text Appli or O	img μα 602vet vel3kbendjøren mag μα 6202vet vel3kbendjøren Amg μα 6202vet vel3kbendjøren Amg μα 6204vet vel3kbendjøren 20% ββββββββββββ βøset	Destanguisender 2020/06. Destanguisender Analysis R. [Data Attifacts.] Analysis (Data Attifacts.] Analysis	010 (peg 433761 011 (peg 4566 012 (peg 4657 4657 4657 4657 4657	3470110496030188353000679900 200242-220817050040849660 0021559ee1254a14009611e731159 74000401097 00167050011731159	2011-13 15 3545 MFZ 2011-12 15 15 345 MFZ 2011-12 15 15 35 MFZ 2011-12 12 15 35 18 MFZ 2011-12 12 15 35 18 MFZ	2011-21711.469482 2011-21711.469482 2011-21711.469482 2011-21711.4699482	2021-12-77 11-060 MEZ 2021-12-77 11-060 MEZ 2021-12-77 11-060 MEZ	2021-2-7 11:48:59 2021-2-7 11:48:59 2021-2-7 11:48:59 2022-12-17 11:48:59

Bilddateien auf dem Laptop

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.

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

Tabelle 9: Bilddateien und ihre MD5-Hashes

Um einen möglichen Zusammenhang zu dem gefundenen Bildmaterial in den zuvor untersuchten Asservaten zu prüfen, wurde in Autopsy ein Hashset aus den MD5Prüfsummen 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
NSC_002.jpeg	/LogicalFileSet1/www/html/nextcloud/data/admin/files_tra	49555	074b919c71571fdd42169f07e673b089	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00
NSC_002.jpeg	/img_stick.E01/Kalender 2022/DSC_002.jpeg	49555	074b919c71571fdd42169f07e673b089	2021-12-12 14:23:38 MEZ	0000-00-00 00:00:00	2021-12-17 00:00:00 MEZ
NSC_002.jpeg	/img_chef.E01/vol_vol3/\$Recycle.Bin/S-1-5-21-4208391369	49555	074b919c71571fdd42169f07e673b089	2021-12-12 15:23:39 MEZ	2021-12-17 12:30:59 MEZ	2021-12-17 12:30:43 MEZ
NSC_002.jpeg	/img_sus.E01/vol_vol3/Users/jansen/Desktop/Karpfenkalen	49555	074b919c71571fdd42169f07e673b089	2021-12-12 15:23:38 MEZ	2021-12-17 11:48:59 MEZ	2021-12-17 11:49:06 MEZ
NSC_003.jpeg	/img_stick.E01/Kalender 2022/DSC_003.jpeg	158024	246c853ca7034eb7f4070763c4fa6ba6	2021-12-12 14:07:44 MEZ	00:00-00-00 00:00:00	2021-12-17 00:00:00 MEZ
NSC_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
NSC_003.jpeg	/img_sus.E01/vol_vol3/Users/jansen/Desktop/Karpfenkalen	158024	246c853ca7034eb7f4070763c4fa6ba6	2021-12-12 15:07:44 MEZ	2021-12-17 11:48:59 MEZ	2021-12-17 11:49:06 MEZ
NSC_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
NSC_010.jpeg 🌺	/img_chef.E01/vol_vol3/\$Recycle.Bin/S-1-5-21-4208391369	131761	367e011e99c8610b8b153d00b6789bfd	2021-12-12 15:24:57 MEZ	2021-12-17 12:30:59 MEZ	2021-12-17 12:30:44 MEZ
NSC_01~1.JPE	/img_stick.E01/\$OrphanFiles/_SC_01~1.JPE	131761	367e011e99c8610b8b153d00b6789bfd	2021-12-12 14:24:56 MEZ	0000-00-00 00:00:00	2021-12-17 00:00:00 MEZ
NSC_010.jpeg 🌺	/LogicalFileSet1/www/html/nextcloud/data/admin/files_tra	131761	367e011e99c8610b8b153d00b6789bfd	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00
NSC_010.jpeg 🌺	/img_sus.E01/vol_vol3/Users/jansen/Desktop/Karpfenkalen	131761	367e011e99c8610b8b153d00b6789bfd	2021-12-12 15:24:56 MEZ	2021-12-17 11:48:59 MEZ	2021-12-17 11:49:06 MEZ
NSC_008.jpeg 🌺	/img_sus.E01/vol_vol3/Users/jansen/Desktop/Karpfenkalen	27099	554b287e802e1eae97b1f656e8b85607	2021-12-12 15:24:42 MEZ	2021-12-17 11:48:59 MEZ	2021-12-17 11:49:06 MEZ
NSC_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
NGC3~1.JPE	/img_stick.E01/\$OrphanFiles/_S96C3~1.JPE	27099	554b287e802e1eae97b1f656e8b85607	2021-12-12 14:24:42 MEZ	0000-00-00 00:00:00	2021-12-17 00:00:00 MEZ
NSC_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
NSC_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
NSC_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
NSC_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
NSC_004.jpeg	/img_sus.E01/vol_vol3/Users/jansen/Desktop/Karpfenkalen	211764	83b407c98a8ee7608a944213a08dc697	2021-12-12 15:26:14 MEZ	2021-12-17 11:48:59 MEZ	2021-12-17 11:49:06 MEZ
NSC_011.jpeg	/img_sus.E01/vol_vol3/Users/jansen/Desktop/Karpfenkalen	45866	892a4c27c5b7fe1809ef1fb80a696e06	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	892a4c27c5b7fe1809ef1fb80a696e06	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00
_SC_01~2.JPE	/img_stick.E01/\$OrphanFiles/_SC_01~2.JPE	45866	892a4c27c5b7fe1809ef1fb80a696e06	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	892a4c27c5b7fe1809ef1fb80a696e06	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	9229dc847d984bdbc5fe81ac6804e794	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	9229dc847d984bdbc5fe81ac6804e794	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/Karpfenkalen	146109	9229dc847d984bdbc5fe81ac6804e794	2021-12-12 15:20:00 MEZ	2021-12-17 11:48:59 MEZ	2021-12-17 11:49:06 MEZ
_S4A36~1.JPE	/img_stick.E01/\$OrphanFiles/_S4A36~1.JPE	146109	9229dc847d984bdbc5fe81ac6804e794	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/5-1-5-21-4208391369	147774	9da5b7202f87b81be324f0f89c760b7b	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	9da5b7202f87b81be324f0f89c760b7b	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	9da5b7202f87b81be324f0f89c760b7b	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/Karpfenkalen	147774	9da5b7202f87b81be324f0f89c760b7b	2021-12-12 14:55:46 MEZ	2021-12-17 11:48:59 MEZ	2021-12-17 11:49:06 MEZ
DSC_007.jpeg	/img_chef.E01/vol_vol3/\$Recycle.Bin/5-1-5-21-4208391369	94994	d1b8136d8d009153acc5800ae41fc579	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	d1b8136d8d009153acc5800ae41tc579	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	d1b8136d8d009153acc5800ae41fc579	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/Karpfenkalen	94994	d1b8136d8d009153acc5800ae41fc579	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/Karptenkalen	172610	dbf2ee1/8c353/02a8a13631aca223f8	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	1/2610	dbf2ee1/8c353/02a8a13631aca223f8	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.EU1/vol_vol3/\$Recycle.Bin/5-1-5-21-4208391369	1/2610	dbf2ee1/8c353/02a8a13631aca223f8	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	e130m091d97fbaf3e82e14b1009d8ac	0000-00-00 00:00:00	0000-00-00 00:00:00	00:00:00:00:00
DSC_006.jpeg	/img_stick.Eu1/Kalender 2022/DSC_006.jpeg	316590	e130ffe01403fbaf3e82e14b1009d8ac	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.cu1/v01/v013/Users/Jansen/Desktop/Karpfenkalen	216200	e1300091097087568261401009088C	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_cnei.cot/voi_voi3/\$kecycle.Bin/5-1-5-21-4208391369	210220	e150109109708768261401009088C	2021-12-12 15:09:34 MEZ	2021-12-17 12:30:59 MEZ	2021-12-17 12:30:44 MEZ
_SC_01~3.JPE	/img_suck.cou/\$UrpnanHies/_SU_U1~3.JPE	40257	101313139969615481476090516751159	2021-12-12 14:25:18 MEZ	2021 12 17 12 20 50 1157	2021-12-17 00:00:00 MEZ
DSC_012.jpeg	/img_cnet.cut/voi_vois/skecycle.BIN/S-1-5-21-4208391369	40207	1015151559eee154d1476090510751159	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.cu.rvoi_vois/users/jansen/uesk.up/Karptenkalen	40207	101515155666615481410090516751159	2021-12-12 13:23:16 MEZ	2021-12-17 11:40:39 MEZ	2021-12-17 11:49:00 MEZ
DSC_015'lbeg	/cogicali nesect/www.incmi/nextcloud/data/admin/files_tra	40207	10121272566612491410030216121123	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":"
        yKTVA4zgxjfivy52WqD8kW3M2pKGQr6srmUXMipRdunxjPFripJn0GMfmtN0q0olYSuJ6sCN"
}
```

```
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.

Keyword search			
Table Thumbnail Summary			
△ Name	Location	Modified Time	
C 20211217 1200 owncloud log 0			0000-
	mg_chel.mg/vol_vols/osels/el_elexppb.aca/coaming/wextclobul/dgs/zoz1121/_1200_ownclobul/dg.og2/zoz1121/_1200_ownclobul/dg.o		
4	II		
Data Content			
Her Text Application File Metadata 05 Acc	ount / Data Artifacts / Analysis Results / Context / Annotations / Other Occurrences		
The recorded of the recorded of the			
Strings Indexed Text Translation			
Paren 2 of 16 Paren 4 A Matabas on anno 1 of			
Page: 2 of 16 Page	i Malchi V 100% O D Reset		
20211217_1200_owncloud.log.0 domain=fdadev;	path=/nextcloud"), QNetworkCookie("nc_sameSiteCookiestrict=true; secure; HttpOnly; expires=Fri, 31-Dec-2100 23:59:59 GMT; domain=fd	adev; path=/nextclo	ud"))
2021-12-17 12:04:28:619 [info nextcloud.sync.networkjob	: OCC::SimpleNetworkJob created for "https://fda.dev/nextcloud" + "" ="		
2021-12-17 12:04:29:068 [info nextcloud.sync.credentials.	low2auth]: Success getting the appPassword for user: "admin", server: "https://fda		

Bild 64: Abruf eines Nextcloud-Client-Passwortes

Anmeldeinformationsverwaltung		- 🗆 X
← → × ↑ 🧧 « Benutzerkor	nten > Anmeldeinformationsverwaltung	✓ ひ Systemsteuerung durchsuchen ク
	Sie kännen gemeicherte Anmeldeinformationen	für Websiter verbundene Anwendungen und Networke
Startseite der Systemsteuerung	anzeigen und löschen.	für websites, verbundene Anwendungen und Netzwerke
	Webanmeldeinformationen	Windows-Anmeldeinformationen
	<	>
	Anmeldedaten sichern Anmeldedaten wiederh	rerstellen
	Windows-Anmeldeinformationen	Windows-Anmeldeinformationen hinzufügen
	Es sind keine Windows-Anmeldeinformationen	vorhanden.
	Zertifikatbasierte Anmeldeinformationen	Zertifikatbasierte Anmeldeinformationen hinzufügen
	Es sind keine Zertifikate vorhanden.	
	Generische Anmeldeinformationen	Generische Anmeldeinformationen hinzufügen
	Nextcloud_admin:https://fdadev/next	tcloud/:0 Geändert: 17.12.2021
	Internet- oder Netzwerkadresse: Nextcloud_admin:https://fdadev/	/nextcloud/:0
	Benutzername:	
Siehe auch	Kennwort: ••••••	
Benutzerkonten	Dauerhaftigkeit: Unternehmen	
	Bearbeiten Entfernen	~

Bild 65: "AppPassword" im Windows Credential Manager

6.1.2 Löschung synchronisierter Daten

(Bezug S. 39)

Die Datei Nextcloud_sync.log im Anwendungsdatenverzeichnis C:/Users/<user>/ AppData/Roaming/Nextcloud speichert alle Datei-Operationen in synchronisierten Verzeichnissen. Listing 5 zeigt die Log-Datei aus dem Image. Jede Operation, hier "Instruction", ist in der aktuellen Version mit einem numerischen Code versehen¹. Im hier gezeigten Log treten die Codes 8 und 2 auf. Diese Codes sind jedoch nicht in den Nutzerhandbüchern für Server und Client dokumentiert.

C:/Users/el jefe/Nextcloud/

¹In älteren Versionen des Nextcloud-Clients wird die Operation noch als String angegeben, wodurch Aktionen leichter nachvollziehbar sind

```
# timestamp | duration | file | instruction | dir | modtime | etag | size | fileId |
    status | errorString | http result code | other size | other modtime | X-Request-
    TD
#=#=## 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|00000259ocmrorx1f0j5|4||0|0|0||
11:05:25||Kalender 2022/DSC_001.jpeg|8|2|1639317346|64cbddf749b15479f277c03b86d3eed9
    |147774|00000317ocmrorx1f0j5|4||200|0|0|a60161d9-b603-4b41-be1d-9d84f1542301|
11:05:26||Kalender 2022/DSC_004.jpeg|8|2|1639319174|ec838365ebe717a8aa352e87c649123f
    |211764|00000269ocmrorx1f0j5|4||200|0|0|cca1d849-1a5c-4da7-9003-12facadfb5f9|
11:05:26||Kalender 2022/DSC_002.jpeg|8|2|1639319019|104a145d0d261c99b704f0ba55eadc41
    |49555|00000276ocmrorx1f0j5|4||200|0|0|a127e9b6-d09e-4db3-ac82-c055cc8cd22c|
11:05:26||Kalender 2022/DSC_003.jpeg|8|2|1639318065|a395f9e4af4f08998c0b3b92476a49aa
    |158024|00000267ocmrorx1f0j5|4||200|0|0|38397ce0-a1a7-4f46-92e9-585232566090|
11:05:27||Kalender 2022/DSC_005.jpeg|8|2|1639319048|b2ef2fe7e71a603e302614df5cbf3f42
    |172610|00000316ocmrorx1f0j5|4||200|0|0|8a500fa5-34ef-4467-8a7d-5b69f5e47aa8|
11:05:28||Kalender 2022/DSC 007.jpeq|8|2|1639319003|3939372613e3535faa0f58cc270f6045
    |94994|00000296ocmrorx1f0j5|4||200|0|0|7b176c9e-c9c0-4136-a055-0c7a41c175e7|
11:05:28||Kalender 2022/DSC 008.jpeg|8|2|1639319082|7fe7daa76d0e9c1d8466363697919256
    |27099|00000268ocmrorx1f0j5|4||200|0|0|a29fc20d-da6b-4347-b75e-10182740a959|
11:05:28||Kalender 2022/DSC_006.jpeg|8|2|1639318174|591e2132215272f168f1fc022a15ba97
    |316590|00000282ocmrorx1f0j5|4||200|0|0|c668f751-1324-4a27-a019-fd39bd67ebbb|
11:05:28||Kalender 2022/DSC_009.jpeg|8|2|1639318801|05529a18875d378a47ea9821ad57f63c
    |146109|00000305ocmrorx1f0j5|4||200|0|0|b1d659c7-0b6f-4742-b99f-4e8b671cbb3a|
11:05:29||Kalender 2022/DSC_010.jpeg|8|2|1639319097|8b0acea6a3f81112ed87b1d634e01619
    |131761|00000279ocmrorx1f0j5|4||200|0|0|f268a375-8a72-4740-8636-0c1867915557|
11:05:30||Kalender 2022/DSC_011.jpeg|8|2|1639318710|351b6ba7e857af1e87e5ee18df668f57
    |45866|00000280ocmrorx1f0j5|4||200|0|0|9a0ed03f-83f5-4216-8cc6-a774f17d63ec|
11:05:30||Kalender 2022/DSC_012.jpeg|8|2|1639319118|7ce063f69535c5b031caaf82258fe5f4
    |46257|00000265ocmrorx1f0j5|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|00000259ocmrorx1f0j5
    |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.



./src/csync/csync.h:	CSYNC_INSTRUCTION_REMOVE	=	1	<<	1,	/*	The	file	need
to be removed (RECC	DNCILE) */								
./src/csync/csync.h:	CSYNC_INSTRUCTION_RENAME		1	<<	2,	/*	The	file	need
to be renamed (RECC	DNCILE) */								
./src/csync/csync.h:	CSYNC_INSTRUCTION_EVAL_RENAME		1	<<	11,	/*	The	file	is
new, it is the dest	ination of a rename (UPDATE) */								
./src/csync/csync.h:	CSYNC_INSTRUCTION_NEW		1	<<	3,	/*	The	file	is
new compared to the	e db (UPDATE) */								
./src/csync/csync.h:	CSYNC_INSTRUCTION_CONFLICT		1	<<	4,	/*	The	file	need
to be downloaded be	ecause 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 Datenbankzentrierte 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.



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 Dateiheader des Archivs die Konfiguration des Containers, Zeitstempel und weitere Metadaten befinden. Ein ausführlicher Auszug solcher Daten ist in Anhang E gelistet.

vzdump-lxc-10	2-2021	1_12	2	ch	ef												
X.																	
🗆 🍸 Name 📥								Des	cripti	on				r	Size	ΥC	Created Modified
🗆 🛄 vzdump-l	xc-102	2-202	21_12	2_20-	18_4	3_21.	tar e	xisting	9					- 1,	7 GB	20.01	1.2022 12:51:38 20.01.2022 12:22:26
Volume	Fil	le		Previ	iew		Deta	ils	Ga	llery		Cale	nda	r	Leg	end	Sync 🐜 🎮 🔤 👘
Offset	0	1	2	3	4	5	6	7	8	9	A	в	С	D	E	F	ANSI ASCII 🔺
00000600	61	72	63	68	ЗA	20	61	6D	64	36	34	0A	63	6F	72	65	arch: amd64 core
00000610	73	ЗA	20	38	0A	66	65	61	74	75	72	65	73	ЗA	20	66	s: 8 features: f
00000620	75	73	65	ЗD	31	2C	6D	6F	75	6E	74	ЗD	6E	66	73	3B	use=1,mount=nfs;
00000630	63	69	66	73	2C	6E	65	73	74	69	6E	67	ЗD	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	uddev memo
00000660	72	79	ЗA	20	32	30	34	38	0A	6E	65	74	30	ЗA	20	6E	ry: 2048 net0: n
00000670	61	6D	65	ЗD	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	ЗD	31	<pre>vmbr0,firewall=1</pre>
00000690	2C	67	77	ЗD	31	39	32	2E	31	36	38	2E	31	2E	31	2C	,gw=192.168.1.1,
000006A0	68	77	61	64	64	72	ЗD	39	45	ЗA	31	34	ЗA	38	30	ЗA	hwaddr=9E:14:80:
000006B0	32	44	ЗA	37	38	ЗA	46	42	2C	69	70	ЗD	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	ЗD	76	65	74	68	0A	6F	73	74	79	70	65	ЗA	20	64	65	=veth ostype: de
000006E0	62	69	61	6E	0A	72	6F	6F	74	66	73	ЗA	20	48	44	44	bian rootfs: HDD
000006F0	30	31	ЗA	31	30	32	2 F	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	ЗD	33	32	<pre>sk-0.raw,size=32</pre>
00000710	47	0A	73	77	61	70	ЗA	20	32	30	34	38	0A	00	00	00	G swap: 2048
		C	2:12	16	6.	٦.4	[ot	ada	to		in	0.0	тх	\overline{C}	C	ont	ainora
			אווכ	JU	υ.	TAT	eu	aua	uer	те	111	55	\mathbf{L}	10.	-0	JIII	amers

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].

Virtual Environment 6.4-13	Search						Documentation Create VM	Create CT	🛓 👌 root@par
Storage *	'HDD01' on node '								© H
Sum	nmary Restore	Show Configuration	Edit Notes	Prune group ixc/102	Remove		Search:	Name, Format	
Back	kups Name					Notes	Date	Format	Size
	Disks vzdump-	Ixc-101-2021_02_03-19_	11_52.tar.zst				2021-02-03 19:11:52	tar.zst	265.01
Ge CT V	Volumes vzdump-	Ixc-102-2021_02_01-12_	13_46.tar.gz				2021-02-01 12:13:46	tar.gz	281.35
ISO	Images vzdump-	lxc-102-2021_02_03-10_	16_53.tar.gz				2021-02-03 10:16:53	tar.gz	281.36
Berti	vzdump	Ixc-102-2021_12_20-18_	43_21.tar.zst				2021-12-20 18:43:21	tar.zst	699.9
Lecin	vzdump-	lxc-106-2021_02_03-08_	59_42.tar.zst				2021-02-03 08:59:42	tar.zst	6.14
Perm	missions vzdump-	Ixc-106-2021_02_03-10_	55_58.tar.gz				2021-02-03 10:55:58	tar.gz	6.30
	vzdump-	Ixc-107-2021_02_03-11_	04_34.tar.gz				2021-02-03 11:04:34	tar.gz	580.5
	vzdump-	Ixc-108-2021_02_03-11_	06_09.tar.gz				2021-02-03 11:06:09	tar.gz	351.
	vzdump	lxc-112-2021_01_19-22_	03_08.tar.zst				2021-01-19 22:03:08	tar.zst	651.
-	vzdump	Ixc-112-2021_02_02-14_	34_52.tar.zst				2021-02-02 14:34:52	tar.zst	23.1
	vzdump	Ixc-112-2021_02_03-11_	09_09.tar.gz				2021-02-03 11:09:09	tar.gz	23.2
	vzdump-	Ixc-118-2021_11_10-17_	16_12.tar.gz				2021-11-10 17:16:12	tar.gz	4.08
	vzdump-	Ixc-123-2021_04_08-22_	24_08.tar.zst				2021-04-08 22:24:08	tar.zst	2.73
	vzdump-	Ixc-124-2021_02_03-11_	50_43.tar.gz				2021-02-03 11:50:43	tar.gz	732
	vzdump	qemu-100-2021_02_01-1	1_49_54.vma	.gz			2021-02-01 11:49:54	vma.gz	14.4
	vzdump-	qemu-100-2021_02_03-0	9_53_00.vma.	.gz			2021-02-03 09:53:00	vma.gz	14.5
	vzdump-	qemu-103-2021_02_03-0	9_09_36.vma.	zst			2021-02-03 09:09:36	vma.zst	2.63
	vzdump-	qemu-103-2021_02_03-1	0_17_44.vma.	.gz			2021-02-03 10:17:44	vma.gz	3.18
- 11 - 12	vzdump-	qemu-104-2021_02_03-1	0_23_56.vma.	.gz			2021-02-03 10:23:56	vma.gz	1.48
	vzdump-	qemu-105-2021_02_03-1	0_27_07.vma.	.gz			2021-02-03 10:27:07	vma.gz	16.9
	vzdump-	qemu-109-2020_12_21-1	7_17_22.vma.	.gz			2020-12-21 17:17:22	vma.gz	772
	vzdump-	qemu-111-2021_02_03-1	1_07_12.vma.	gz			2021-02-03 11:07:12	vma.gz	701
	vzdump	qemu-113-2021_02_03-1	1_39_20.vma.	.gz			2021-02-03 11:39:20	vma.gz	802
	vzdump	qemu-114-2021_02_03-1	1_41_20.vma.	.gz			2021-02-03 11:41:20	vma.gz	1.12
	vzdump	qemu-121-2021_02_03-1	1_43_59.vma.	.gz			2021-02-03 11:43:59	vma.gz	1.76
	vzdump-	qemu-122-2021_02_03-1	1_48_07.vma.	.gz			2021-02-03 11:48:07	vma.gz	974.
	vzdump-	qemu-125-2021_02_03-1	1_51_57.vma.	.gz			2021-02-03 11:51:57	vma.gz	1.12
	vzdump-	qemu-126-2021_02_03-1	1_54_39.vma.	.gz			2021-02-03 11:54:39	vma.gz	1.21
	vzdump-	qemu-129-2021_02_03-1	1_57_44.vma.	.gz			2021-02-03 11:57:44	vma.gz	962

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.

	ment 6.4-13 Search					Documentation Greate VM	Create CT	🔺 roct@pam 🗸
Server View	Storage 'HDD01' on no	ode'						Help
 Chi (phote shou rear) Chi (phote shou rear) 	Summary	Restore Show Configuration	Edit Notes Prune group txc/102 Remove			Search:		
() 112 (should alway day)	🖺 Backups	Name						
(c) 117 (salarising alsos day)	A VM Disks	vzdump-bxc-101-2021_02_03-19_1	1_52.tar.zst			2021-02-03 19:11:52	tar.zst	265.01 MB
E 118 (photo stress day)	Ge CT Volumes	vzdump-bxc-102-2021_02_01-12_1	3_46.tar.gz			2021-02-01 12:13:46	tar.gz	281.35 MB
 TTB (starsa atron dav) 		vzdump-bxc-102-2021_02_03-10_1	6_53.tar.gz			2021-02-03 10:16:53	tar.gz	281.36 MB
	C noo magoo	vzdump-bxc-102-2021_12_20-18_4	3_21.tar.zst			2021-12-20 18:43:21	tar.zst	699.98 MB
	Lig CT templates	vzdump-bxc-106-2021_02_03-08_5	i9_42.tar.zst			2021-02-03 08:59:42	tar.zst	6.14 GB
	Permissions	vzdump-bxc-106-2021_02_03-10_5	i5_58.tar.gz			2021-02-03 10:55:58	tar.gz	6.30 GB
Ki 100 (supplier stress result)		vzdump-bxc-107-2021_02_03-11_0	4_34.tar.gz			2021-02-03 11:04:34	tar.gz	580.51 MB
		vzdump-bxc-108-2021_02_03-11_0	6_09.tar.gz			2021-02-03 11:06:09	tar.gz	351.81 MB
112 (Includent alway dev)		vzdump->-112-2021_01_19-22_0	3 08.tar.zet			2021-01-19 22:03:08	tar.zst	651.38 MB
E 133 (too complex stress dev)		vzdump-bc-112-2021_02_02-14_3	Configuration		0	2021-02-02 14:34:52	tar.zst	23.13 GB
124 (adda had alves, dev)		vzdump-bxc-112-2021_02_03-11_0	arch: amd64			2021-02-03 11:09:09	tar.gz	23.25 GB
100 (mangadi ahnu davi)		vzdump-bx:-118-2021_11_10-17_1	cores: 8			2021-11-10 17:16:12	tar.gz	4.08 GB
tere and the second second		vzdump-bxc-123-2021 04 08-22 2	features: fuse=1,mount=nfs;cifs,nesting=1	features: fuse=1_mount=nfs;cifs,nesting=1 hostname: nextclouddev memory: 2048		2021-04-08 22:24:08	tar.zst	2.72 GB
		vzdump-bxc-124-2021 02 03-11 5	memory: 2048			2021-02-03 11:50:43	tar.gz	732.33 MB
and another states and			net0: name=eth0,bridge=vmbr0,firewall=1,gw=1	2.168.1.1,hwaddr=9E:14:80:2D:	78	2021-02-01 11:49:54	vma.gz	14.41 GB
			rootfs: HDD01:102/vm-102-disk-0.raw,size=32G			2021-02-03 09:53:00	vma.gz	14.55 GB
TTD (pt-d) show devi-			swap: 2048		_	2021-02-03 09:09:36	vma.zst	2.63 GB
114 (freeget stress reset)						2021-02-03 10:17:44	vma.gz	3.18 GB
🞑 115 (reverse prory show must)						2021-02-03 10:23:56	vma gz	1.48 GB
							vma gz	16.99 GB
121 (jackett atvou dev)							Vm9.07	772 51 MB
122 (somar show dev)							vma az	701.61 MB
		urdump demu 112 2021 02 03 11	1			2021-02-03 11:07-12	inna.gz	902.17 MD
			1				vine.gz	1.12 OB
							vine.gz	1.76 OB
			48. 07 μma στ			2021-02-03 11:43:39	vina.gz	074 72 MD
S \$\$001 ()		vzdump-gemu-122-2021_02_03-11					megz	1.12 GB
S. SSD02 ()		vacuump-quinte-120-2021_02_03-11	Lor on annual			2021-02-03 11:01:07	vina.gz	1.12 00
SSD03 (_04_38.vma.gz			2021-02-03 11:04:39	vina.gz	062 54 MR
local ()			_or_++.vina.gz			2021-02-03 11:07:44	vina.gz	992.04 MB

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.

	nent 6.4-13 Search		Documentation Create VM	Create CT	🛔 root@pam 🗸
Server View	Storage 'HDD01' on nod				Help
K) 118 (phote show must)	B Summary	Restore Show Configuration Edit Notes Prune group txc/102 Remove	Search:		
11 TTZ patronik altera dani	🖺 Backups				
	WM Disks	vzdump-txc-101-2021 02 83-19 11 62 tar.zst	2021-02-03 19:11:52	tar.zst	265.01 MB
E. 112 (phone stress day)	Fier CT Volumes	vzdump-txc-102-2021_02_01-12_13_46.tar.gz	2021-02-01 12:13:46	tar.gz	281.35 MB
 TTE (stress stress dev) 		vzdum-lxc-102-2021_02_03-10_16_63.tar.gz	2021-02-03 10:16:53	tar.gz	281.36 MB
 CO (with atom dev) 		vzdump-bxo-102-2021_12_20-18_43_21.tar.zst	2021-12-20 18:43:21	tar.zst	699.98 MB
C 107 percentation from the literation	De CT Templates	vzdump-bxc-106-2021_02_03-08_59_42.tar.zst	2021-02-03 08:59:42	tar.zst	6.14 GB
12 128 cm shouldest	Permissions	vzdump-bxc-106-2021_02_03-10_55_58.tar.gz	2021-02-03 10:55:58	tar.gz	6.30 GB
KL 100 (upplier atom must)		vzdump-bxc-107-2021_02_03-11_04_34.tar.gz	2021-02-03 11:04:34	tar.gz	580.51 MB
(c) 121 (writed about dev)		vzdump-txc-108-2021_02_03-11_06_09.tar.gz	2021-02-03 11:06:09	tar.gz	351.81 MB
E 112 (sectodesk stere dev)		vzdump-txc-112-2021_01_19-22_03_08.tar.zst	2021-01-19 22:03:08	tar.zst	651.38 MB
122 (no complex streader)		vzdump-txc-112-2021_02_02-14_34_62.tar.zst	2021-02-02 14:34:52	tar.zst	23.13 GB
E. 124 (white both stress day)		vzdump-txc-112-2021_02_03-11_09_09.tar.gz	2021-02-03 11:09:09	tar.gz	23.25 GB
the prompt store and		vzdump-txc-118-2021_11_10-17_16_12.tar.g-	2021-11-10 17:16:12	tar.gz	4.08 GB
		vzdump-txc-123-2021_04_08-22_24_08.tar: Restore: CT 🛞	2021-04-08 22:24:08	tar.zst	2.72 GB
The landstand show deal		vzdump-txc-124-2021_02_03-11_50_43.tar.; Source: vzdump-txc-102-2021_12_20-18_43_21 tar.zst	2021-02-03 11:50:43	tar.gz	732.33 MB
110 (strait, strait read)		vzdump-gemu-100-2021_02_01-11_49_54.v	2021-02-01 11:49:54	vma.gz	14.41 GB
TTT (oper phone devi)		vzdump-gemu-100-2021_02_03-09_53_00.	2021-02-03 09:53:00	vma.gz	14.55 GB
 113 (pt-distance dev) 		vzdump-qemu-103-2021_02_03-09_09_36.v	2021-02-03 09:09:36	vma.zst	2.63 GB
114 (Respectation, reset)		vzdump-gemu-103-2021_02_03-10_17_44_N Bandwidth Limit: Defaults to target storage restore limit 🗘 MiB/s	2021-02-03 10:17:44	vma.gz	3.18 GB
113 (months proxy should not)		vzdump-gemu-104-2021_02_03-10_23_56.v Unique: Start after restore:	2021-02-03 10:23:56	vma.gz	1.48 GB
 The (guardanois should not) 		vzdump-gemu-105-2021_02_03-10_27_07.v Privilege Level: From Backup Unprivileged Privileged	2021-02-03 10:27:07	vma.gz	16.99 GB
		vzdump-gemu-109-2020_12_21-17_17_22.v	2020-12-21 17:17:22	vma.gz	772.51 MB
100 context stress days		vzdump-gemu-111-2021_02_03-11_07_12.v Restore	2021-02-03 11:07:12	vma.gz	701.61 MB
C 128 (Mar alway meet)		vzdump-gemu-113-2021_02_03-11_39_20.vma.gz	2021-02-03 11:39:20	vma.gz	802.17 MB
129 (doctorheat alread dev)		vzdump-qemu-114-2021_02_03-11_41_20.vma.gz	2021-02-03 11:41:20	vma.gz	1.12 GB
 Vili prompi altos des) 		vzdump-gemu-121-2021_02_03-11_43_59.vma.gz	2021-02-03 11:43:59	vma.gz	1.76 GB
HDD01 ()		vzdump-gemu-122-2021_02_03-11_48_07.vma.gz	2021-02-03 11:48:07	vma.gz	974.73 MB
SSD01 ()		vzdump-qemu-125-2021_02_03-11_51_57.vma.gz	2021-02-03 11:51:57	vma.gz	1.12 GB
SSD02 (vzdump-qemu-126-2021_02_03-11_54_39.vma.gz	2021-02-03 11:54:39	vma.gz	1.21 GB
SSD03 ()		vzdump-gemu-129-2021_02_03-11_57_44.vma.gz	2021-02-03 11:57:44	vma.gz	962.54 MB
i local ()					

Bild 69: Instanzierung 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 Anmeldungsversuche

(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 >	<pre>select * from oc_bruteforce_attempts;</pre>										
id act	ion occurred	ip	 subnet	metadata							
1 log 2 log 3 log 4 log 5 log	in 1639739825 in 1639739837 in 1639739858 in 1639739858 in 1639739884 in 1639739899	192.168.1.11 192.168.1.11 192.168.1.11 192.168.1.11 192.168.1.11 192.168.1.11	192.168.1.11/32 192.168.1.11/32 192.168.1.11/32 192.168.1.11/32 192.168.1.11/32 192.168.1.11/32	{"user":"admin"} {"user":"admin"} {"user":"admin"} {"user":"admin"} {"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).

<pre>> SELECT * FROM oc_files_trash; +</pre>										
auto_id	lid	user	timestamp	location	type mime					
1 2 3 4 5 6 7 8	Nextcloud.png Photos Nextcloud intro.mp4 Documents Templates Nextcloud Manual.pdf Reasons to use Nextcloud.pdf Kalender 2022	admin admin admin admin admin admin admin	1639320509 1639320509 1639320510 1639320510 1639320509 1639320514 1639320515 1639740663		NULL NULL NULL NULL NULL NULL NULL NULL NULL NULL NULL NULL NULL NULL 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
259 265 267 268 269 276 279 280 282 282 296 305 316	<pre>files_trashbin/files/Kalender 2022.d1639740663 files_trashbin/files/Kalender 2022.d1639740663/DSC_012.jpeg files_trashbin/files/Kalender 2022.d1639740663/DSC_003.jpeg files_trashbin/files/Kalender 2022.d1639740663/DSC_004.jpeg files_trashbin/files/Kalender 2022.d1639740663/DSC_000.jpeg files_trashbin/files/Kalender 2022.d1639740663/DSC_010.jpeg files_trashbin/files/Kalender 2022.d1639740663/DSC_010.jpeg files_trashbin/files/Kalender 2022.d1639740663/DSC_010.jpeg files_trashbin/files/Kalender 2022.d1639740663/DSC_001.jpeg files_trashbin/files/Kalender 2022.d1639740663/DSC_001.jpeg files_trashbin/files/Kalender 2022.d1639740663/DSC_007.jpeg files_trashbin/files/Kalender 2022.d1639740663/DSC_005.jpeg files_trashbin/files/Kalender 2022.d1639740663/DSC_005_jpeg files_trashbin/files/Kalender 2022.d1639740663/DSC_005_jpeg files_trashbin/files/Kalender 2022.d1639740663/DSC_005_jpeg files_trashbin/files/Kalender 2022.d1639740663/DSC_005_jpeg</pre>	Kalender 2022.d1639740663 DSC_012.jpeg DSC_003.jpeg DSC_004.jpeg DSC_002.jpeg DSC_002.jpeg DSC_010.jpeg DSC_010.jpeg DSC_010.jpeg DSC_010.jpeg DSC_006.jpeg DSC_007.jpeg DSC_007.jpeg DSC_007.jpeg DSC_005.jpeg
+		+

Bild 72: Datei-Cache in der Nextcloud-Datenbank

Dateilöschungen sind aus den Inhalten der Tabelle oc_activity ersichtlich.

> SELECT activ	<pre>SELECT activity_id, timestamp, type, subject, file FROM oc_activity WHERE timestamp > 1639320514;</pre>										
activity_id	timestamp	type	subject	file							
41 42 43 44 45 46 46 47 47 48 49 50 51 51 52 52	1639320823 1639320829 1639320830 1639320830 1639320830 1639320835 1639320835 1639320835 1639320836 1639320840 1639320840 1639320841 1639320841	file_created file_created file_created file_created file_created file_created file_created file_created file_created file_created file_created file_created	created_self created_self created_self created_self created_self created_self created_self created_self created_self created_self created_self created_self created_self created_self	/ /bilder / /bilder/DSC_012.jpeg / /bilder/DSC_008.jpeg / /bilder/DSC_003.jpeg / /bilder/DSC_002.jpeg / /bilder/DSC_002.jpeg / /bilder/DSC_001.jpeg / /bilder/DSC_006.jpeg / /bilder/DSC_007.jpeg / /bilder/DSC_009.jpeg / /bilder/DSC_009.jpeg / /bilder/DSC_009.jpeg / /bilder/DSC_009.jpeg / /bilder/DSC_009.jpeg							
53 54 55	1639320841 1639320858 1639740663	file_changed file_changed file_deleted	reated_setf renamed_self 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 nextclouddb untersucht. Mit einer einfachen SELECT-Anfrage wird ersichtlich, dass es nur einen Nutzer names "admin" der Gruppe "admin" gibt (siehe Bild 74).



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).



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

Listing 8: Benutzung von Distrobox

³https://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 Spurenträger 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

eate a new virtual machi ritt 2 von 5	ine		
) or CDROM install media:			
selected		- Du	irchsuchen
operating system you are ins g for install media / source	talling:		Ø
atically detect from the install	ation media /	source	
⊗ Abbrechen	< Zurück	c	> Vor
o a n	O or CDROM install media: a selected e operating system you are ins ng for install media / source natically detect from the install Q Abbrechen	O or CDROM install media: a selected e operating system you are installing: ng for install media / source natically detect from the installation media /	O or CDROM install media: a selected e operating system you are installing: ng for install media / source natically detect from the installation media / source O Abbrechen < Zurück

Bild 78: Auswahl einer Betriebssystem-ISO (1)

M ☆ ⊀	Datenträger mit ISO-Medium lokalisieren v 🔨
57% default Dateisystemverzeichnis	Details XML Größe: 31.37 GiB Free / 48.82 GiB In Use Ort: /mnt/d/iso Datenträger 9front.pi.img archlinux-2021.10.01-x86_64.iso debian-11.1.0-amd64-netinst.iso de_windows_10_consumer_edition_version_1809_updated_sept_2018_x64_dvd_88 de_windows_7_professional_with_sp1_x64_dvd_u_676919.iso ev3dev.img Fedora-Server-dvd-x86_64-34-1.2.iso neon-user-20211230-0945.iso
+ > @ ī	Lokal durchsuchen

Bild 79: Auswahl einer Betriebssystem-ISO (2)

₩ ≈ ₩	Neue VM 🗸 🗸							
	Create a new virtual machine Schritt 3 von 5							
Choose M	Nemory and CPU settings:							
Memory	: 2048 - +							
	Bis zu 7839 MiB auf diesem Wirt verfügbar							
CPUs	2 - +							
	Up to 4 available							
	♦ Abbrechen							

Bild 80: Hardwarespezifikation der VM $\,$

Schr	tt 4 von 5
Speicher	platz für diese virtuelle Maschine aktivieren
🔘 Datenträ	iger Image für die virtuelle Maschine erstellen
16,0	— + GiB
42.2 GiB	verfügbar am Standard-Speicherort
🔵 Benutze	rdefinierten Speicher auswählen oder erstellen
Verwalten	

Bild 81: Virtuelle Festplatte der VM anlegen

M ≈ ★	Neue VM V
Create a Schritt 5 v	new virtual machine
Bereit, die Installa	tion zu beginnen
Name: eljefe	
OS: Microso	ft Windows 10
Install: Lokales	CDROM/ISO
Speicher: 2048 M	iB
CPUs: 2	
Storage: 16.0 Gi	3 /var/lib/libvirt/images/eljefe.qcow2
Kor	figuration bearbeiten vor der Installation
▼ Netzwerk Ausw	ahl
Bridge device	· >
Device name:	virbr0
	S Abbrechen Zurück 🗗 Fertig

Bild 82: Einrichtung abschließen und Netzwerkkonfiguration wählen

B Einrichtung einer KVM mit Proxmox

Create: Virtual	Machine						\otimes
General OS	System	Hard Disk CPU	Memory	Network	Confirm		
Node:	Mindflayer		 ✓ Resource 	Pool:			\sim
VM ID:	135		0				
Name:	jansenpc						
Start at boot:			Start/Shuto order:	down	any		
			Startup de	lay:	default		
			Shutdown	timeout:	default		
Help					Advanced 🗹	Back	Next

Bild 83: Erzeugung einer neuen VM

Create: Virtual Ma	achine				\otimes
General OS	System Hard Di	isk CPU	Memory 1	Network Confirm	
Use CD/DVD d	isc image file (iso)		Guest OS:		
Storage:	SSD01	\sim	Туре:	Linux	\sim
ISO image:	1_2004_x64_dvd_36c	161c40.iso 🗸	Version:	5.x - 2.6 Kernel	\sim
🔵 Use physical C	D/DVD Drive				
O Do not use any	media				
				Advanced 🖂	Back Next

Bild 84: Auswahl einer Betriebssystem-ISO

Create: Virtual N	Machine				\otimes
General OS	System Hard Disk	CPU	Memory Netwo	rk Confirm	
Graphic card:	Default	\sim	SCSI Controller:	VirtIO SCSI	\sim
Qemu Agent:					
BIOS:	Default (SeaBIOS)	\sim	Machine:	Default (i440fx)	\sim
Help				Advanced 🗹 🛛 Back	Next

Bild 85: Auswahl der Systemarchitektur

Create: Virtual I	Machine				\otimes
General dmS	System Hard Disk C	PU	Memory Network	c Confirm	
Bus/Device:	SCSI V 0	$\hat{}$	Cache:	Default (No cache)	~
SCSI Controller:	VirtIO SCSI		Discard:		
Storage:	HDD01	\sim			
Disk size (GiB):	32	$\hat{}$			
Format:	QEMU image format (qcow2)	\sim			
SSD emulation:			Backup:		
IO thread:			Skip replication:		
Read limit (MB/s):	unlimited	$\hat{}$	Read max burst (N	IB): default	\bigcirc
Write limit (MB/s):	unlimited	$\hat{}$	Write max burst (M	B): default	\bigcirc
Read limit (ops/s)	unlimited	$\hat{}$	Read max burst (o	ps): default	\bigcirc
Write limit (ops/s):	unlimited	$\hat{}$	Write max burst (op	os): default	\bigcirc
Help				Advanced 🕢 Back	Next

Bild 86: Virtuelle Festplatte der VM anlegen

Create: Vir	tual Machine					\otimes
General	OS Syste	m Hard Disk	CPU	Memory Netw	ork Confirm	
Sockets:	1		0	Туре:	Default (kvm64)	\sim
Cores:	4		0	Total cores:	4	
VCPUs:	4	I	$\hat{}$	CPU units:	1024	$\hat{}$
CPU limit:	unlimited	1	$\hat{}$	Enable NUMA:		
Extra CPU F	lags:					
Default	- ()) +	md-clear	Required to	o let the guest OS k	now if MDS is mitigated correctly	н.
Default	- ())+	pcid	Meltdown f Intel CPUs	ix cost reduction on	Westmere, Sandy-, and IvyBridge	
Default	- ()) +	spec-ctrl	Allows imp	roved Spectre mitig	ation with Intel CPUs	
Default	- 000 +	ssbd	Protection	for "Speculative Sto	ore Bypass" for Intel models	
Default	-) () +	ibpb	Allows imp	roved Spectre mitig	ation with AMD CPUs	
Default	-) () +	virt-ssbd	Basis for "S	Speculative Store B	ypass" protection for AMD models	
Help					Advanced 🗹 🛛 Back 🛛 Ne	ext

Bild 87: Hardwarespezifikation der VM (1)

Create: Virtual Machine	Create: Virtual Machine							
General OS Syste	em Hard Disk	CPU	Memory	Network	Confirm			
Memory (MiB):	2048	\$						
Minimum memory (MiB):	2048	0						
Ballooning Device:								
Help					Advanced 🗹	Back	Next	

Bild 88: Hardwarespezifikation der VM (2)

Create: Virtu	al Ma	chine					\otimes
General	os	System	Hard Disk	CPU	Memory Netwo	rk Confirm	
No network	devic	e					
Bridge:	VI	mbr0		\sim	Model:	VirtIO (paravirtualized)	\sim
VLAN Tag:	n	D VLAN		$\hat{}$	MAC address:	auto	
Firewall:	\checkmark						
Disconnect:					Rate limit (MB/s):	unlimited	\Diamond
					Multiqueue:		$\hat{}$
						\searrow	
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

₩4 😞 🗶	eljefe auf QEMU/KVM					~ ~ 🗞
Datei Virtuelle Maschine Anzeigen	Faste senden					
🗖 💿 Nextel	vud × +		-	- 0	×	
\leftarrow \rightarrow C	🗘 🏠 https://fda	P tê	£ €			
	36040880736040					
					4	
- 48 (**) (*					B	
					Q	
11114	Anmelden →				8	
0.42.1	Passwort vergessen?				2	
					Q	

Bild 93: Benutzernamen und Passwort eintragen



Bild 94: Zugriff des Desktop-Clients genehmigen



Bild 95: Bestätigung der Autorisierung



Bild 96: Lokalen Ordner zur Synchonisation wählen und Einrichtung abschließen

D Dateilisten der durch Guymager erzeugten Images

D.1 Dienstrechner des Geschädigten

chef/	
chef.E01	GiB
chef.E022,0	GiB
chef.E03	GiB
chef.E04	GiB
chef.info	KiB
chef.md5sum	2 B

```
GUYMAGER ACQUISITION INFO FILE
_____
Guymager
=======
                  : 0.8.8-3
Version
Compilation timestamp: 2019-02-20-15.50.35
Compiled with: gcc 8.2.0libewf 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 : Export Witness Format cub format Cubercas
Format
                      : Expert Witness Format, sub-format Guymager - file extension
   is .Exx
Image meta data
                    : 1
: 1
  Case number
   Evidence number
                      : John Doe
  Examiner
  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
                         : 04d32827545545513e257f7990a05eda9450045e
SHA1 hash
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.
```

D.2 Laptop des Tatverdächtigen

iΒ
iΒ
iΒ
iВ
iВ
ĺiΒ
iΒ
B

```
GUYMAGER ACQUISITION INFO FILE
_____
Guymager
_____
          : 0.8.13-1
Version
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
  Case number
  Examiner :
Description :
                   : Max Mustermann
  Notes
                    :
Image path and file name: /mnt/storage/SWAP/fda/sus.Exx
```

```
Info path and file name: /mnt/storage/SWAP/fda/sus.info
                 : MD5, SHA-1 and SHA-256
Hash calculation
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/	
	121,3 MiB
	6,1 KiB

GUYMAGER ACQUISITION INFO FILE

```
Guymager
=======
            : 0.8.8-3
Version
Compilation timestamp: 2019-02-20-15.50.35
Compiled with : gcc 8.2.0
libewf version : 20140807 (
                 : 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 00 00 00 00 20 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:
device size with M = 1000*1000:
                                            0 MBytes
                                            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
_____
                     : /dev/sde
Linux device
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.
```

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=vmbr0,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
000075500000000000
000
14155401350
007377
ustar
0000000
./PaxHeaders.26036/root
00006440000000000
002
14155402675
011667
ustar
30 mtime=1639318973.858323678
30 atime=1640022284.875126234
30 ctime=1640022206.102893243
0000
14155402675
010363
ustar
0000000
./root/PaxHeaders.26036/.mysql_history
0000644
002
14155402446
014667
ustar
30 mtime=1639318822.293831995
30 atime=1640022204.574888714
30 ctime=1640022204.574888714
./root/.mysql_history_____
000
14155402446
013310
ustar
0000000
CREATE DATABASE nextclouddb;
CREATE USER 'nextclouduser'@'localhost' IDENTIFIED BY 'password';
GRANT ALL ON nextclouddb.* T0 'nextclouduser'@'localhost';
FLUSH PRIVILEGES;
EXIT;
./root/PaxHeaders.26036/.bash_history
0000644
002
14160133376
014436
ustar
30 mtime=1640019710.203844178
30 atime=1640022204.574888714
30 ctime=1640022204.574888714
./root/.bash_history
000
```

14160133376 013055 ustar 0000000 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 0000644 002 14155402607 013665 ustar 30 mtime=1639318919.034150155 30 atime=1640022204.574888714 30 ctime=1640022204.574888714 ./root/.wget-hsts 0000644 14155402607 012315 ustar 0000000 # 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

01313

```
./root/PaxHeaders.26036/.profile
0000644
12564377031
013411
ustar
30 atime=1640022204.574888714
30 ctime=1640022204.574888714
./root/.profile
0000644
004
564377031
012033
ustar
0000000
# ~/.profile: executed by Bourne-compatible login shells.
if [ "$BASH" ]; then
    if [ -f ~/.bashrc ]; then
    . ~/.bashrc
  fi
mesg n || true
./root/PaxHeaders.26036/.local
0000644
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
$\overline{7}$	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 Anmeldungsversuche 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 Windows Credential Manager	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 oc_users	68
75	Auslesen der Tabellen oc_share und oc_share_external	68
76	Paketkonflikt zwischen verschiedenen TSK-Versionen	69
77	Encourance ciner neuen VM	79
11 70	$ \begin{array}{c} \text{Enzeugung einer neuen VM} \\ \text{Augusehl einer Potriebegwatern ISO} (1) \end{array} $	10 79
70	Auswahl einer Detriebssystem-ISO (1)	73
19	Auswahl ehler Dethedssystem-ISO (2)	74
0U 01	Naturalle East platte den VM auferen	(4 75
01 01	Finishtung abashlisten und Natzurschlauf zum tien zu hler	10 75
82	\square	(5)
	Emittentung abseimeben und Wetzwerkköningdration wahlen	10

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 Synchonisation 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
$2 \\ 3$	Umwandlung von virtuellen QEMU-Festplatten in ein Rohformat Prüfsummenerzeugung einer CD-ROM	20 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 CD-R	Compact Disc. 29 Compact Disc Recordable. 29, 44
DB DVD	Datenbank, Database. 62 Digital Video Disc. 29
EWF	Expert Witness Format. 20, 21
FAT	File Allocation Table. 48
GbR GmbH GNU GZ	Gesellschaft bürgerlichen Rechts. 6, 10 Gesellschaft mit beschränkter Haftung. 5, 7, 37 GNU's not UNIX. 10, 63, 69, 102 GNU-Zip. 26
HTTP HTTPS	Hypertext Transfer Protocol. 12 Hypertext Transfer Protocol Secure. 12
ID IP IT ITFS	Identifikator. 65 Internet Protocol. 12, 13, 45, 71 Informationstechnologie. 4, 6, 29, 31, 32, 37, 70–72, 102 IT-Forensik-Software. 4, 19, 20, 37
JPEG	Joint Photographic Experts Group. 33, 34, 42, 46,
JSON	49, 50 JavaScript Object Notation. 59
KVM	Kernel-basierte virtuelle Maschine. 9, 10, 13
LAMP LXC LXD	Linux Apache MySQL PHP. 62 Linux Containers. 10, 26, 62–64, 70, 72, 98 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 URL USB	Urheberrechtsgesetz. 5 Uniform Resource Locator. 11 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 Betriebs- system 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 Rech- nernetz, der die Kommunikation zwischen einem ex- ternen Client und einem oder mehreren internen Ser- vern regelt, ohne dass diese direkt mit externen Cli- ents kommunizieren müssen. 12, 71
vServer	Virtualisierter Server, im Gegensatz zum Bare-Metal-Server. 6