Forensischer Untersuchungbericht

name

13. Mai 2021

Inhaltsverzeichnis

Teil I

Untersuchungsbericht

Kapitel 1

Prolog

1.1 Beweismittel

1.1.1 Identifikation

Das Beweismittel ein Datenträger mit der SHA256-Summe 1f23fcf72f931e14a2762b3014b97f51e5031c045129d044287457a996b0c4cc wurde von der Staatsanwaltschaft ausgehändigt, mit der von der Spurensicherung erstellten Hash-Summe zur Überprüfung der Echtheit des Datenträgers. Die Echtheit des Datenträgers konnte somit erfolgreich verifiziert werden. Daraufhin wurde eine 1 zu 1 Kopie des Datenträgers angefertigt, welche für die folgende Analyse verwendet wurde. Der orginale Datenträger wurde bis auf die Kopie für nichts anderes benutzt.

1.1.2 Verlauf

Der Ermittlungsverlauf des Falles sah wie folgt aus:

- Nachweis der Integrität des Asservats
- Anfertigung einer Kopie
- Analyse des Datenträgers und Suche nach rhinographischem Material
- Mögliche Strafbarkeit von Jürgen S. aufgrund gefundener Bilder

1.2 Auftrag

Untersuchungsauftrag: Verdacht auf Besitz illegaler Nashornographie gemäß § 184k StGBVorbemerkung: § 184k ist ein hypothetischer Straftatbestand, der die Umständevon § 184b übungsfreundlich nachbildet. Der neue Straftatbestand verbietet denBesitz und die Weitergabe von Nashornbildern. In der Rechtspraxis wird man be-straft, wenn manmindestens dreiNashornbilder wissentlich besitzt. Die Aufgaben-stellung geht auf den DFRWS Forensic Rodeo Challenge 2005 zurück, vgl. http://www.cfreds.nist.gov/dfrws/Rhino_Hunt.html
Die Staatsanwaltschaft hat ein Ermittlungsverfahren gegen Herrn Jürgen S. ein-geleitet. Es besteht der Verdacht auf Besitz illegaler Nashornbilder (Nashornographie) gemäß § 184k StGB.
Im Rahmen einer Hausdurchsuchung am 25.10.2016 wurde in der Wohnung von Herrn S. ein Datenträger (externe USB-Festplatte Marke Seetor, Asservatennummer 35/17/2015, Baujahr 2007) beschlagnahmt. Der Beschuldigte hat zugegeben,der Besitzer des Datenträgers zu sein, welchen er 3 Jahre vor der Beschlagnahmung gebraucht im Internet erworben hatte.
Durch die aktuelle Überlastung der Kriminalinspektion 5 (Cybercrime und digitaleSpuren) ist eine zeitnahe Auswertung in der polizeilichen Forensik nicht möglich. Deshalb bestellt die Staatsanwaltschaft Sie als externen Gutachter/externe Gut-achterin zur Analyse des beschlagnahmten Datenträgers.
Die Staatsanwaltschaft erbittet Antworten auf folgende Fragen:
1. Befinden sich auf dem Datenträger Bilddateien, die potentiell rhinographi-scher Natur sind?
2. Bei wievielen der Bilder besteht Grund zur Annahme, der Beschuldigte wissevon ihrer Existenz?
Die Staatsanwaltschaft händigt Ihnen das Abbild des Datenträgers aus. Die SHA256-Summe lautet:

1f23fcf72f931e14a2762b3014b97f51e5031c045129d044287457a996b0c4cc
Die Staatsanwaltschaft erwartet Ihre Ergebnisse in Form eines Untersuchungsbe-richts bis zum13.05.2021 (23:59 Uhr).

1.3 Arbeitsumgebung

Die komplette Untersuchung wurde ausschließlich unter folgenden Arbeitsbedingungen ausgeführt, wobei eine virtuelle Maschine benutzt wurde um externe Einflüsse zu minimieren:

- Oracle VM-Virtualbox 6.0.24
- Kali-Linux-2021.1-vbox-amd64
- The Sleuth Kit ver 4.10.1
- TestDisk 7.1, Data Recovery Utility, July 2019
- PhotoRec 7.1, Data Recovery Utility, July 2019

Kapitel 2

Ergebniszusammenfassung

Auf dem Datenträger befinden sich Bilder rhinographischer Natur (Abbildung 1- 4). Ebenfalls kann davon ausgegangen werden, dass der Herr Jürgen S. von 2 von 4 Bildern wissentlich im Besitz war. Die Bilder nashorn (Abbildung 4), nasohnehorn (Abbildung 3), remaining (Abbildung 2) wurden alle am 23.09.2015 um 10:49:36 Uhr auf den Datenträger geladen. Die Metadaten dieser Bilder könnten allerdings manipuliert sein, somit ist dies nicht zu 100% aussagekräftig. Das Bild nashorn befindet sich als einziges offensichtlich auf dem Datenträger, womit man davon aussgehen kann, dass Jürgen S. in Kenntis davon ist. Das Bild nasohnehorn wurde von dem Datenträger gelöscht, ist aber rekonstruierbar. Auf allen Bildern ist ein Nashorn zu sehen, somit sind sie rhinographischer Natur. Zudem wurden noch 1 weiteres Bild rhinographischer Natur (Abbildung 1) gefunden, welches allerdings vor 2012 erstellt wurde, da die Metadaten zum Datenträger allerdings verloren sind und nur die Erstellungszeit des Fotos vorhanden ist, lässt sich dies nicht eindeutig Jürgen S. zuordnen. Dieser hat nämlich die Platte im Jahre 2013 gebraucht erworben. Die Festplatte wurde stark manipuliert, es ist dringend nötig zu erfahren ob Jürgen S. Kenntnisse besitzt, die den Umgang mit der manipulierten Platte ermöglichen oder ein Geständis zum vollständigen Inhalt zu erlangen.

Kapitel 3

Detailierter Ermittlungsverlauf

3.1 Zusammenfassung

Der Master Boot Record ist beschädigt, da der Datenträger mit Linux partitioniert wurde. Die Analyse mit Testdisk einer Unknown Partition mit Quick Search liefert eine NTFS Partition bei deeper Search lassen sich 3 NTFS Partitionen erschließen. Mithilfe von Photorec findet man außerhalb der Linux partition noch ein 4tes Bild von einem Nashorn.

3.2 Erzeugung einer Arbeitskopie

TODO

3.3 Auswertung des Master Boot Records

Der Master Boot Record ist beschädigt, da der Datenträger mit Linux partitioniert wurde. Es lassen sich mithilfe von Testdisk allerdings noch 2 von drei alten NTFS Dateisysteme wiederherstellen.

3.4 Auswertung der Partitionstabelle

??

3.5 Erzeugung von Partitionskopien

TODO

3.6 Untersuchung der Partitionskopien

3.6.1 Untersuchung der ersten Partition

NTFS Dateisystem mit den Bildern nashorn.jpg und nasohnehorn.jpg, welche beide am 23.09.2015 um 10:49:36 Uhr auf den Datenträger geladen wurden.

3.6.2 Untersuchung der zweiten Partition

Beschädigt und nicht wiederherstellbar.

3.6.3 Untersuchung der dritten Partition

Die Analyse mit Testdisk einer Unknown Partition mit Quick Search liefert eine NTFS Partition, auf welcher sich ein rhinographisches Bild remaining.jpg erstellt am 23.09.2015 findet.

3.6.4 Untersuchung der dritten Partition

Teil II

Anhang

Kapitel 4

Beweismittel

4.1 Bild des Beweismittels

Kapitel 5

Arbeitsumgebung

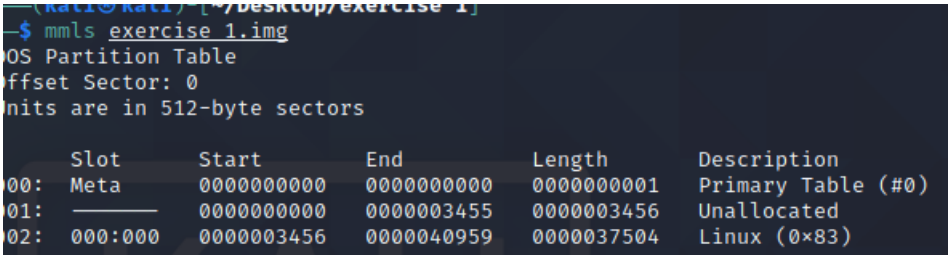
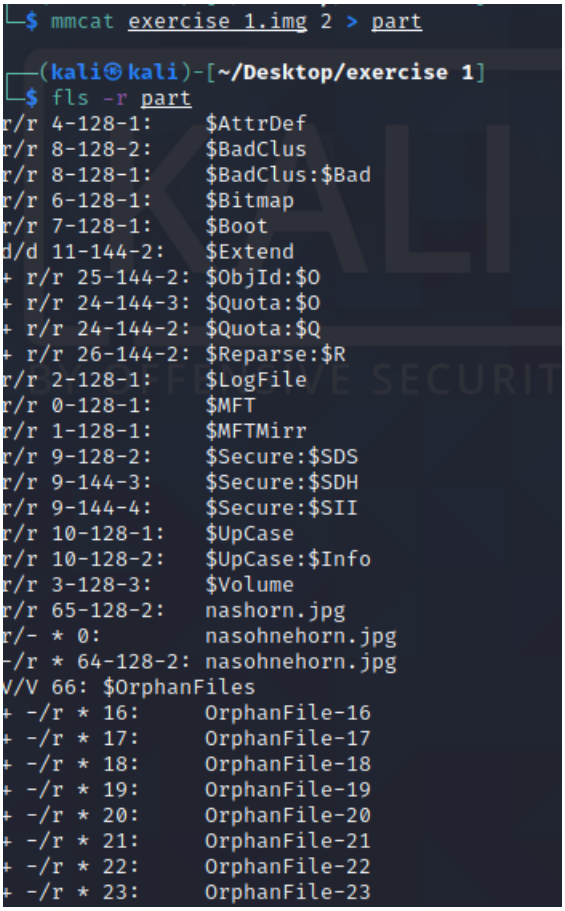
5.1 Verwendete Werkzeuge

Kapitel 6

Konsolenausgaben

6.1 Master Boot Record

6.1.1 Sleutkit

- 
```
$ mmls exercise_1.img
OS Partition Table
ffset Sector: 0
nits are in 512-byte sectors

     Slot      Start        End          Length       Description
00:  Meta      0000000000   0000000000   0000000001   Primary Table (#0)
01:  ------    0000000000   0000003455   0000003456   Unallocated
02:  000:000   0000003456   0000040959   0000037504   Linux (0x83)
```
- 
```
$ mmcat exercise_1.img 2 > part

(kali㉿kali)-[~/Desktop/exercise 1]
$ fls -r part
r/r 4-128-1:    $AttrDef
r/r 8-128-2:    $BadClus
r/r 8-128-1:    $BadClus:$Bad
r/r 6-128-1:    $Bitmap
r/r 7-128-1:    $Boot
d/d 11-144-2:   $Extend
+ r/r 25-144-2: $ObjId:$O
+ r/r 24-144-3: $Quota:$O
+ r/r 24-144-2: $Quota:$Q
+ r/r 26-144-2: $Reparse:$R
r/r 2-128-1:    $LogFile
r/r 0-128-1:    $MFT
r/r 1-128-1:    $MFTMirr
r/r 9-128-2:    $Secure:$SDS
r/r 9-144-3:    $Secure:$SDH
r/r 9-144-4:    $Secure:$SII
r/r 10-128-1:   $UpCase
r/r 10-128-2:   $UpCase:$Info
r/r 3-128-3:    $Volume
r/r 65-128-2:   nashorn.jpg
r/- * 0:        nasohnehorn.jpg
-/r * 64-128-2: nasohnehorn.jpg
V/V 66: $OrphanFiles
+ -/r * 16:     OrphanFile-16
+ -/r * 17:     OrphanFile-17
+ -/r * 18:     OrphanFile-18
+ -/r * 19:     OrphanFile-19
+ -/r * 20:     OrphanFile-20
+ -/r * 21:     OrphanFile-21
+ -/r * 22:     OrphanFile-22
+ -/r * 23:     OrphanFile-23
```

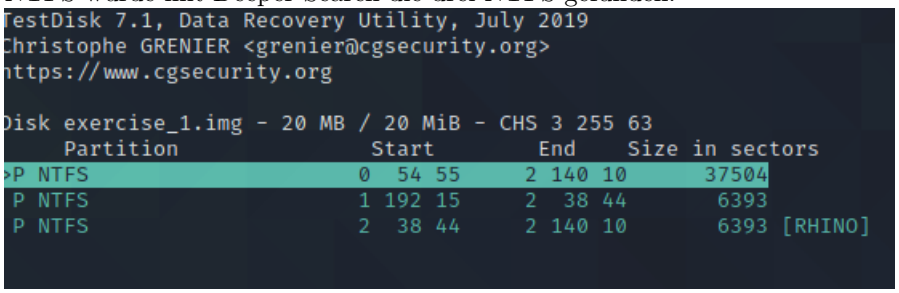
```
└─$ istat part 64-128-2
MFT Entry Header Values:
Entry: 64        Sequence: 2
$LogFile Sequence Number: 0
Not Allocated File
Links: 0

$STANDARD_INFORMATION Attribute Values:
Flags: Archive
Owner ID: 0
Security ID: 0  ()
Created:        2015-09-23 10:49:36.183139300 (EDT)
File Modified:  2015-09-23 10:49:36.183843900 (EDT)
MFT Modified:   2015-09-23 10:49:36.183843900 (EDT)
Accessed:       2015-09-23 10:49:36.183139300 (EDT)

$FILE_NAME Attribute Values:
Flags: Archive
Name: nasohnehorn.jpg
Parent MFT Entry: 5     Sequence: 5
Allocated Size: 86016           Actual Size: 0
Created:        2015-09-23 10:49:36.183139300 (EDT)
File Modified:  2015-09-23 10:49:36.183139300 (EDT)
MFT Modified:   2015-09-23 10:49:36.183139300 (EDT)
Accessed:       2015-09-23 10:49:36.183139300 (EDT)

Attributes:
Type: $STANDARD_INFORMATION (16-0)   Name: N/A   Resident   size: 48
Type: $FILE_NAME (48-3)   Name: N/A   Resident   size: 96
Type: $SECURITY_DESCRIPTOR (80-1)   Name: N/A   Resident   size: 80
Type: $DATA (128-2)   Name: N/A   Non-Resident   size: 82020  init_size: 82020
2856 2857 2858 2859 2860 2861 2862 2863
2864 2865 2866 2867 2868 2869 2870 2871
2872 2873 2874 2875 2876
```

```
└─$ istat part 65
MFT Entry Header Values:
Entry: 65        Sequence: 1
$LogFile Sequence Number: 0
Allocated File
Links: 1

$STANDARD_INFORMATION Attribute Values:
Flags: Archive
Owner ID: 0
Security ID: 0  ()
Created:        2015-09-23 10:49:36.187708300 (EDT)
File Modified:  2015-09-23 10:49:36.188246300 (EDT)
MFT Modified:   2015-09-23 10:49:36.188246300 (EDT)
Accessed:       2015-09-23 10:49:36.187708300 (EDT)

$FILE_NAME Attribute Values:
Flags: Archive
Name: nashorn.jpg
Parent MFT Entry: 5     Sequence: 5
Allocated Size: 57344           Actual Size: 0
Created:        2015-09-23 10:49:36.187708300 (EDT)
File Modified:  2015-09-23 10:49:36.187708300 (EDT)
MFT Modified:   2015-09-23 10:49:36.187708300 (EDT)
Accessed:       2015-09-23 10:49:36.187708300 (EDT)

Attributes:
Type: $STANDARD_INFORMATION (16-0)   Name: N/A   Resident   size: 48
Type: $FILE_NAME (48-3)   Name: N/A   Resident   size: 88
Type: $SECURITY_DESCRIPTOR (80-1)   Name: N/A   Resident   size: 80
Type: $DATA (128-2)   Name: N/A   Non-Resident   size: 57242  init_size: 57242
2877 2878 2879 2880 2881 2882 2883 2884
2885 2886 2887 2888 2889 2890
```

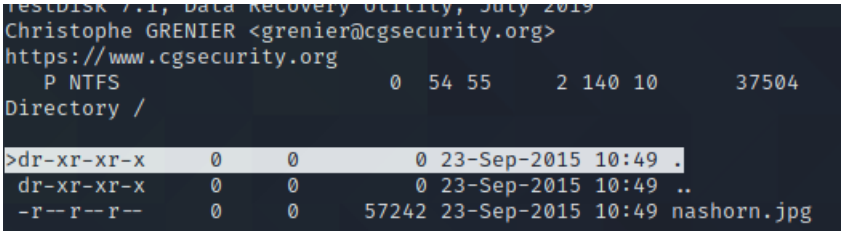
- TODO HASHES

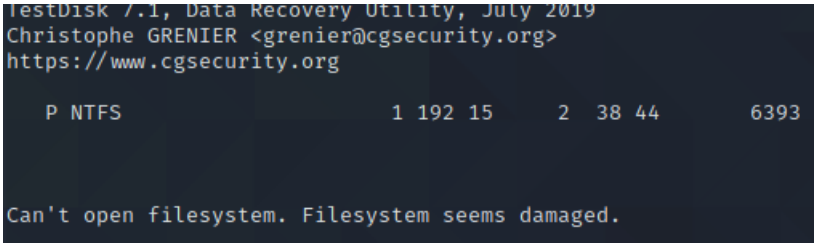
6.1.2 Testdisk

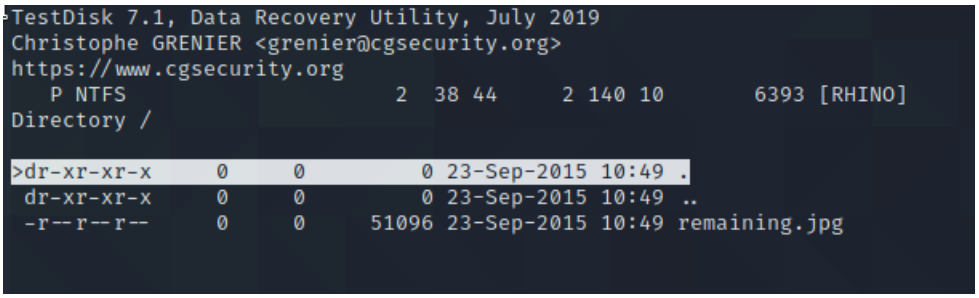
Testdisk wurde mit No Partition und unkown Filesystem verwendet und nach Funde des ersten NTFS wurde mit Deeper Search die drei NTFS gefunden.



Auflisten der Dateien:

- 

- 

- 

6.1.3 File Carving

Photorec wurde mit den Standardeinstellungen mit auf No Partition mit Other filesystem types als ext2/ext3/ext4 verwendet.