Forensische Untersuchung des Datenträgers mit Asservatennummer 35/17/2015

Julian Kotzur

1.05.2021

Inhaltsverzeichnis

1 Prolog **1**
1.1 Auftrag . . . 1
1.2 Arbeitsumgebung . . . 1
1.2.1 Verwendete Software . . . 1
1.2.2 Verwendete Hardware . . . 1
1.3 Sicherstellung der Integrität des Datenträgers . . . 2

2 Zusammenfassung **3**

3 Technische Analyse **4**
3.1 Partiontabelle . . . 4
3.2 Analyse der Partition in Slot 002 . . . 4
3.2.1 Grundlegende Analyse der Partition in Slot 002 . . . 4
3.2.2 Weitere Analyse der Partition in Slot 002 mittels testdisk . . . 5
3.3 Analyse der Partition in Slot 001 . . . 5
3.4 Zusätzliche Analyse mit scalpel . . . 5
3.5 Abschluss der Analyse . . . 6

4 Anhang **7**
4.1 Konsolenausgaben . . . 7
4.2 Bilder . . . 12

1 Prolog

1.1 Auftrag

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. Er habe den Datenträger vor 3 Jahren gebraucht im Internet erworben.
Durch eine Überlastung der Kriminalinspektion 5 (Cybercrime und digitale Spuren) war eine zeitnahe Auswertung in der polizeilichen Forensik nicht möglich, weswegen ich von der Staatsanwaltschaft als externer Gutachter zur Analyse des beschlagnahmten Datenträgers bestellt wurde.
Die Untersuchung soll zum Einen zeigen ob Bilddateien mit potentiell rhinographischer Natur sich auf dem Datenträger befinden. Des Weiteren soll klargestellt werden bei wie vielen der Bilder ein Grund zur Annahme besteht, dass der Beschuldigte von ihrer Existenz weiß.

1.2 Arbeitsumgebung

Als Betriebssystem wurde Kali Linux in der Version 2021.1 innerhalb der Virtuellen Maschine VMware Workstation 16 auf Ubuntu 20.04.2 LTS verwendet.

1.2.1 Verwendete Software

Hardware	Modell
GNU coreutils	8.32
The Sleuth Kit	4.10.1
Hexdump	2.36.1
Photorec	7.1
file	5.39
GNOME Image Viewer	3.38.1
testdisk	7.1
GNU nano	5.4
Scalpel	1.60

1.2.2 Verwendete Hardware

Zur Analys des Datenträgers wurde ein XMG Fusion 15 Laptop mit folgender Konfiguration verwendet:

Hardware	Modell
CPU	Intel Core i7-9750H
GPU	Nvidia GeForce RTX 2070 Max-Q | 8 GB GDDR6
RAM	1x 16 GB DDR4-2666 Samsung
SSD	SanDisk Extreme PRO M.2 NVMe 3D SSD 500GB

1.3 Sicherstellung der Integrität des Datenträgers

Die Kopie des Abbilds des Datenträgers wurde mit mitsamt der Hash256-Prüfsumme von der Staatsanwaltschaft ausgehändigt. Das Asservat und dessen Hashsumme wurde vorher durch Sicherheitsdienste vor Manipulation geschützt. Dafür wurde zudem eine gedruckte Version der Prüfsumme sicher verwart.
Anschließend habe ich die Integrität des Asservates vor und nach der Analyse nachgewiesen. Dafür habe ich folgenden Command im Terminal verwendet:

```
sha256sum -c exercise_1.img exercise_1.img.sha25
```

Der Befehl **sha256sum** ist Teil der GNU coreutils. Damit wurde gezeigt, dass der Datenträger unverändert ist. Abschließend konnte die Prüfsumme nocheinmal mit der gedruckten Version verglichen werden um jegliche Manipulation auszuschließen.
Zudem kannd er Computer, welcher zur Analyse verwendet werden, als sicher eingestuft werden. Zu diesem habe nur ich Zugriff, die Datenträger sind AES 256 mit CBC-Modus verschlüsselt und das ganze System ist Passwortgeschützt.

2 Zusammenfassung

Die forensische Analyse des Datenträgers mit der Asservatennummer 35/17/2015 ergab, dass sich auf diesem vier Bilder mit potentieller Rhinographie befinden. Zwei der Bilder (Bild 1, Bild 2) waren leicht auffindbar. Ein Bild (Bild 3) war in gewisser Weise „versteckt “. Das letzte Bild (siehe Bild 4) war gelöscht, aber konnte unter zu Hilfename forensischer Software rekonstruiert werden.

Die letzten beiden Bilder waren nicht einfach zugänglich, wodurch man nicht eindeutig sagen kann, dass der Beschuldigte von ihrer Existenz wusste. Das gelöschte Bild hätte von der Person gelöscht sein können, aber es ließen sich keine Beweise dafür finden. Das bedeutet, dass die gelöschte Datei bereits beim Erwerb auf dem Datenträger gewesen sein könnte. Auch für die versteckte Datei gilt, dass man dem Beschuldigten nicht eindeutig nachweisen kann, dass er von ihrer Existenz wusste.
Jedoch ließen sich für die ersten beiden Bilder Hinweise finden, dass der Beschuldigte wahrscheinlich von ihrer Existenz wusste. Die Zeitstempel dieser Dateien besagen, dass am 23.09.2015 um 10:49 EDT mit diesen Dateien gearbeitet wurde. Dies entspricht dem Zeitraum, indem der Datenträger im Besitz des Angeklagten war. Die Daten könnten natürlich auch von Drittem oder einer Schadsoftware auf den Datenträger gelangt sein, weshalb nur die starke Vermutung des Wissens zur Existenz der Bilder vorliegt, aber kein eindeutiger Beweis.

Da der Strafbestand erst für den wissentlichen Besitz von drei Nashornbildern in Kraft tritt, ingesamt nur vier auf dem Datenträger enthalten sind, bei denen es nur für zwei Bilder verstärkte Evidenzen gibt, kann festgehalten werden, dass der Angeklagte mit sehr hoher Wahrscheinlichkeit noch keine Straftat begannen hat.

3 Technische Analyse

3.1 Partiontabelle

Das zugrundeliegende Datenträgerbild exercise_1.img hat eine Größe von 20MiB. Wie bereits beschrieben wurde zuerst die Prüfsumme ermittelt und verifiziert. Der nächste Schritt bestand darin mit Hilfe von **mmstat**, welches Teil von „The Sleuth Kit“ ist, die Partitionsart zu ermitteln. Das Ergebnis war, dass es sich um einer DOS Partitionierung handelt. Anschließend wurde mittels **mmls**, welches auch Teil von „The Sleuth Kit“ ist, die folgende Partitionstabelle erzeugt:

Listing 1: Partitionstabelle

```
0       Slot    Start        End          Length       Description
1  000: Meta    0000000000   0000000000   0000000001   Primary Table (#0)
2  001: -------  0000000000   0000003455   0000003456   Unallocated
3  002: 000:000  0000003456   0000040959   0000037504   Linux (0x83)
```

Als Ergebnis kann man festhalten, dass der Datenträger in zwei Partitionen unterteilt ist. Die Partition in Slot 001 ist ein nicht zugewiesener Speicherbereich mit der Länge 3456 Sektoren. Die Partition in Slot 002 ist eine Linux Partition mit der Länge 37504 Sektoren. Um mit den beiden Partitionen arbeiten zu können werden diese mit **mmcat**, welches Teil von „The Sleuth Kit“ ist, seperat kopiert und abgespeichert. Für die beiden enstandenen Dateien wurden nun Prüfsummen gebildet, welche am Ende der Analyse erneut verifizert wurden. Im Folgenden wird zuerst die Partition 002 betrachtet, da angenommen wird, dass man auf dieser mit höhrerer Wahrscheinlichkeit verwertbare Spuren findet. Anschließend wird zur Vervollständigung der Analyse auch die Partition 001 genauer untersucht.

3.2 Analyse der Partition in Slot 002

3.2.1 Grundlegende Analyse der Partition in Slot 002

Die Analyse dieser Partition wurde begonnen, indem mittels **fls**, welches Teil von „The Sleuth Kit“ ist, das Dateisystem genauer betrachtet wurde (siehe Ergebnis von **fls -r part002**). Daraus lässt sich vermuten, dass es sich um ein NTFS Dateisystem handelt, welches meist zu den Betriebssystemen von Microsoft gehört.
Anschließend wurde mit Hilfe des Befehls **istat**, welches Teil von „The Sleuth Kit“ ist, die einzelnen Dateie der Partition genauer untersucht. Auf Grund der verdächtigen Namenbenennung wurde mit der Datei mit der Inode Nummer 65-128-2 begonnen (siehe Ergebnis von **istat part002 65**). Daraufhin wurde die Datei mit **icat**, welches Teil von „The Sleuth Kit“ ist, herausgeschnitten. Anschließend wurde mittels des Befehls **file**, welcher zu den Standard Linux Befehlen gehört, die herausgeschnittene Datei genauer überprüft (siehe Ergebnis von **file nashorncut.jpg**). Dabei wurde die Vermutung bestätigt, dass es sich um eine JPEG-Datei handelt. Daraufhin wurde die Datei mit dem GNOME Image Viewer betrachtet. Bei dem zu Sehenden Bild handelt es sich demnach um potentielle Rhinographie (siehe Bild 1).
Der selbe Vorgang wurde bei der Datei mit der Inode Numme 64-128-2 wiederholt. Das dabei gefundene Bild enthält auch potentielle Rhinographie (siehe Bild 2).
Alle weiteren Dateien der Partition wurden schließlich auch mit **istat** untersucht. Das einzige was auffiel ist, dass alle Dateien, bis auf die vorher betrachteten Dateien den gleichen Zeitstempel besitzen. Auch mit der Betrachtung mittels **hexdump**, welches zum Standardpaket util-Linux gehört, konnten keine weiteren Spuren identifiziert werden.
Fazit: Es wurden zwei Dateien von potentiell rhinographischer Natur gefunden. Aufgrund

der leichten Zugänglichkeit zu den Daten und den Zeitstempeln, welche sich von allen anderen Dateien unterscheiden, kann angenommen werden, dass der Beschuldigte Kenntnis von den Bildern hatte.

3.2.2 Weitere Analyse der Partition in Slot 002 mittels testdisk

Mittels des Programmes **testdisk** kann nun zur vollständigen Durchsuchung noch nach weiteren Partitionen mit dem Partitionstyp „None“ gesucht werden. Als Ergebnis wurden drei Partitionen gefunden (siehe Ergebnispartitionen von **testdisk part002**). Die erste, welche 37504 Sektoren groß ist, entspricht der bereits analysierten Partition. Auf die zweite Partition kann nicht zugegriffen werden, da diese anscheinend beschädigt ist. Es kann sich dabei auch um ein fehlerhaftes Ergebnis handeln. Die dritte gefundene Partition hingegen scheint bisher unendeckte Daten zu enthalten (siehe Analyse der Rhino NTFS Partition).
Diese Partition enthält augenscheinlich eine verdächtige Datei mit dem Namen remaining.jpg. Die Datei wurde wie oben genauer beschrieben herauskopiert, analyisiert und anschließend mit einem Bildbetrachter geöffnet (siehe Bild 3). Die Vermutung, dass es sich um potentielles rhinographische Material handelt, wurde dadurch bestätigt.
Fazit: Es kann nicht mit Sicherheit gesagt werden, ob der Angeklagte von dieser Datei wusste, da der Zugriff auf diese Daten im Allgemeinen nicht trivial ist.

3.3 Analyse der Partition in Slot 001

Das Problem bei dieser Partition ist, dass der Speicherplatz nicht zugewiesen ist. Das bedeutet, dass man nicht mit herkömmlichen Methoden auf die möglicherweise enthaltene Dateien zugreifen kann. Um dennoch herauszufinden, ob innerhalb des Speicherplatzes versteckte Spuren enthalten sind, wurde mittels **hexdump** der Speicherbereich manuell analysiert. Dafür wurde folgender Befehl verwendet:

```
hexdump -Cv part001 | less
```

Mit „partu“ wurde die Kopie der Slot 001 Partition bezeichnet. Dabei wurde festgestellt, dass wertvolle Spuren in Form eines Bildes enthalten sein könnten. Im Anhang (siehe Ergebnis von **hexdump -Cv part001 | less**) kann mittels einem ausgewählter Bereich des Hexdumps, welcher zu der Annahme führte, dieser Schritt nachvollzogen werden.
Aufgrund der Annahme wurde mittels **photorec** die Partition analysisert. Damit wurde aus dem nicht zugewiesenem Speicherbereich eine JPEG-Datei extrahiert. Diese enthält augenscheinlich rhinografisches Materiall (siehe Bild 4).
Fazit: Es kann nicht mit Sicherheit gesagt werden, ob der Angeklagte von dieser Datei wusste. Es ist wahrscheinlicher, dass diese Datei bereits bei Kauf des Datenträgers enthalten und nicht einfach zugänglich war. Das Datum aus dem hexdump an stelle 00000280 untermauert diese These.

3.4 Zusätzliche Analyse mit scalpel

Abschließend wurde der komplette Datenträger noch mit dem Programm **scalpel** analysiert. Dieses Programm sucht nach ausgewählten Dateitypen auf allokiertem und nicht allokiertem Speicher und erstellt zu gefundenen Dateien eine Kopie. In der dazugehörigen Konfigurationsdatei wurden GIF-, JPG-, PNG-, DOC-, HTML- und PDF-Dateien ausgewählt (siehe Ergebnis von **scalpel**).
Neben ein paar Dateien welche fehlerhaft waren, wurden nur die Bilder gefunden, welche bereits nach obrigen Verfahren entdeckt wurden. Es konnten keine zusätzlichen relevaten Dateien gefunden werden. Dies untermauert die Vermutung, dass alle Dateien von potentiell rhinographischer Natur ermittelt wurden.

3.5 Abschluss der Analyse

4 Anhang

4.1 Konsolenausgaben

Listing 2: Ergebnis von **fls -r part002**

```
 0  r/r 4-128-1:     $AttrDef
 1  r/r 8-128-2:     $BadClus
 2  r/r 8-128-1:     $BadClus:$Bad
 3  r/r 6-128-1:     $Bitmap
 4  r/r 7-128-1:     $Boot
 5  d/d 11-144-2:    $Extend
 6  + r/r 25-144-2:  $ObjId:$O
 7  + r/r 24-144-3:  $Quota:$O
 8  + r/r 24-144-2:  $Quota:$Q
 9  + r/r 26-144-2:  $Reparse:$R
10  r/r 2-128-1:     $LogFile
11  r/r 0-128-1:     $MFT
12  r/r 1-128-1:     $MFTMirr
13  r/r 9-128-2:     $Secure:$SDS
14  r/r 9-144-3:     $Secure:$SDH
15  r/r 9-144-4:     $Secure:$SII
16  r/r 10-128-1:    $UpCase
17  r/r 10-128-2:    $UpCase:$Info
18  r/r 3-128-3:     $Volume
19  r/r 65-128-2:    nashorn.jpg
20  r/- * 0:         nasohnehorn.jpg
21  -/r * 64-128-2:  nasohnehorn.jpg
22  V/V 66:  $OrphanFiles
23  + -/r * 16:      OrphanFile-16
24  + -/r * 17:      OrphanFile-17
25  + -/r * 18:      OrphanFile-18
26  + -/r * 19:      OrphanFile-19
27  + -/r * 20:      OrphanFile-20
28  + -/r * 21:      OrphanFile-21
29  + -/r * 22:      OrphanFile-22
30  + -/r * 23:      OrphanFile-23
```

Listing 3: Ergebnis von **istat part002 65**

```
 0  MFT Entry Header Values:
 1  Entry: 65        Sequence: 1
 2  $LogFile Sequence Number: 0
 3  Allocated File
 4  Links: 1
 5
 6  $STANDARD_INFORMATION Attribute Values:
 7  Flags: Archive
 8  Owner ID: 0
 9  Security ID: 0  ()
10  Created:         2015-09-23 10:49:36.187708300 (EDT)
11  File Modified:   2015-09-23 10:49:36.188246300 (EDT)
12  MFT Modified:    2015-09-23 10:49:36.188246300 (EDT)
13  Accessed:        2015-09-23 10:49:36.187708300 (EDT)
14
15  $FILE_NAME Attribute Values:
16  Flags: Archive
17  Name: nashorn.jpg
18  Parent MFT Entry: 5     Sequence: 5
19  Allocated Size: 57344           Actual Size: 0
20  Created:         2015-09-23 10:49:36.187708300 (EDT)
21  File Modified:   2015-09-23 10:49:36.187708300 (EDT)
22  MFT Modified:    2015-09-23 10:49:36.187708300 (EDT)
```

```
23  Accessed:       2015-09-23 10:49:36.187708300 (EDT)
24
25  Attributes:
26  Type: $STANDARD_INFORMATION (16-0)   Name: N/A   Resident   size: 48
27  Type: $FILE_NAME (48-3)   Name: N/A   Resident   size: 88
28  Type: $SECURITY_DESCRIPTOR (80-1)   Name: N/A   Resident   size: 80
29  Type: $DATA (128-2)   Name: N/A   Non-Resident   size: 57242   init_size: 57242
30  2877 2878 2879 2880 2881 2882 2883 2884
31  2885 2886 2887 2888 2889 2890
```

Listing 4: Ergebnis von **file nashorncut.jpg**

```
0  i65-128-2: JPEG image data, JFIF standard 1.01, resolution (DPI),
1  density 72x72, segment length 16, Exif Standard: [TIFF image data,
2  big-endian, direntries=10, description=Rhino Warning Sign With Glossy Effect,
3  orientation=upper-left, xresolution=172, yresolution=180, resolutionunit=2,
4  software=Adobe Photoshop CS3 Windows, datetime=2009:02:20 14:17:44],
5  baseline, precision 8, 346x346, components 3
```

Listing 5: Ergebnispartitionen von **testdisk part002**

```
0  Disk partL - 19 MB / 18 MiB - CHS 3 255 63
1  Partition               Start         End     Size in sectors
2  P NTFS                  0   0  1       2  85 19      37504
3  P NTFS                  1 137 24       1 238 53       6393
4  P NTFS                  1 238 53       2  85 19       6393 [RHINO]
```

Listing 6: Analyse der Rhino NTFS Partition

```
0  dr-xr-xr-x     0     0          0 23-Sep-2015 10:49 .
1  dr-xr-xr-x     0     0          0 23-Sep-2015 10:49 ..
2  -r--r--r--     0     0      57242 23-Sep-2015 10:49 nashorn.jpg
```

Listing 7: Ergebnis von **hexdump -Cv part001 | less**

```
0   00000200  ff d8 ff e0 00 10 4a 46  49 46 00 01 01 01 00 48  |......JFIF.....H|
1   00000210  00 48 00 00 ff e1 00 d0  45 78 69 66 00 00 49 49  |.H......Exif..II|
2   00000220  2a 00 08 00 00 00 06 00  1a 01 05 00 01 00 00 00  |*...............|
3   00000230  56 00 00 00 1b 01 05 00  01 00 00 00 5e 00 00 00  |V...........^...|
4   00000240  28 01 03 00 01 00 00 00  02 00 00 00 32 01 02 00  |(...........2...|
5   00000250  14 00 00 00 66 00 00 00  13 02 03 00 01 00 00 00  |....f...........|
6   00000260  01 00 00 00 69 87 04 00  01 00 00 00 7a 00 00 00  |....i.......z...|
7   00000270  00 00 00 00 48 00 00 00  01 00 00 00 48 00 00 00  |....H.......H...|
8   00000280  01 00 00 00 32 30 30 38  3a 30 34 3a 32 32 20 31  |....2008:04:22 1|
9   00000290  33 3a 34 39 3a 34 38 00  06 00 00 90 07 00 04 00  |3:49:48.........|
10  000002a0  00 00 30 32 32 30 01 91  07 00 04 00 00 00 01 02  |..0220..........|
11  000002b0  03 00 00 a0 07 00 04 00  00 00 30 31 30 30 01 a0  |..........0100..|
12  000002c0  03 00 01 00 00 00 ff ff  00 00 02 a0 03 00 01 00  |................|
13  000002d0  00 00 e5 07 00 00 03 a0  03 00 01 00 00 00 04 0a  |................|
14  000002e0  00 00 00 00 00 00 ff ed  02 d2 50 68 6f 74 6f 73  |..........Photos|
15  000002f0  68 6f 70 20 33 2e 30 00  38 42 49 4d 04 04 00 00  |hop 3.0.8BIM....|
16  00000300  00 00 02 b5 1c 02 00 00  02 00 02 1c 02 05 00 14  |................|
17  00000310  57 68 69 74 65 20 52 68  69 6e 6f 20 49 73 6f 6c  |White Rhino Isol|
18  00000320  61 74 65 64 1c 02 19 00  05 72 68 69 6e 6f 1c 02  |ated.....rhino..|
19  00000330  19 00 05 77 68 69 74 65  1c 02 19 00 06 61 66 72  |...white.....afr|
20  00000340  69 63 61 1c 02 19 00 06  61 6e 69 6d 61 6c 1c 02  |ica.....animal..|
21  00000350  19 00 07 61 6e 69 6d 61  6c 73 1c 02 19 00 03 62  |...animals.....b|
22  00000360  69 67 1c 02 19 00 09 64  61 6e 67 65 72 6f 75 73  |ig.....dangerous|
23  00000370  1c 02 19 00 0a 65 6e 64  61 6e 67 65 72 65 64 1c  |.....endangered.|
24  00000380  02 19 00 0a 65 78 70 65  64 69 74 69 6f 6e 1c 02  |....expedition..|
25  00000390  19 00 09 68 65 72 62 69  76 6f 72 65 1c 02 19 00  |...herbivore....|
26  000003a0  04 68 6f 72 6e 1c 02 19  00 04 68 75 67 65 1c 02  |.horn.....huge..|
```

```
000003b0  19 00 05 6c 61 72 67 65  1c 02 19 00 06 6d 61 6d  |...large.....mam|
000003c0  6d 61 6c 1c 02 19 00 06  6e 61 74 75 72 65 1c 02  |mal.....nature..|
000003d0  19 00 0a 72 68 69 6e 6f  63 65 72 6f 73 1c 02 19  |...rhinoceros...|
000003e0  00 06 73 61 66 61 72 69  1c 02 19 00 06 74 72 61  |..safari.....tra|
000003f0  76 65 6c 1c 02 19 00 04  77 69 6c 64 1c 02 19 00  |vel.....wild....|
00000400  08 77 69 6c 64 6c 69 66  65 1c 02 19 00 04 65 61  |.wildlife.....ea|
00000410  72 73 1c 02 19 00 08 69  73 6f 6c 61 74 65 64 1c  |rs.....isolated.|
00000420  02 19 00 05 77 68 69 74  65 1c 02 19 00 05 72 68  |....white.....rh|
00000430  69 6e 6f 1c 02 19 00 05  77 68 69 74 65 1c 02 19  |ino.....white...|
00000440  00 06 61 66 72 69 63 61  1c 02 19 00 06 61 6e 69  |..africa.....ani|
00000450  6d 61 6c 1c 02 19 00 07  61 6e 69 6d 61 6c 73 1c  |mal.....animals.|
00000460  02 19 00 03 62 69 67 1c  02 19 00 09 64 61 6e 67  |....big.....dang|
00000470  65 72 6f 75 73 1c 02 19  00 0a 65 6e 64 61 6e 67  |erous.....endang|
00000480  65 72 65 64 1c 02 19 00  0a 65 78 70 65 64 69 74  |ered.....expedit|
00000490  69 6f 6e 1c 02 19 00 09  68 65 72 62 69 76 6f 72  |ion.....herbivor|
000004a0  65 1c 02 19 00 04 68 6f  72 6e 1c 02 19 00 04 68  |e.....horn.....h|
000004b0  75 67 65 1c 02 19 00 05  6c 61 72 67 65 1c 02 19  |uge.....large...|
000004c0  00 06 6d 61 6d 6d 61 6c  1c 02 19 00 06 6e 61 74  |..mammal.....nat|
000004d0  75 72 65 1c 02 19 00 0a  72 68 69 6e 6f 63 65 72  |ure.....rhinocer|
000004e0  6f 73 1c 02 19 00 06 73  61 66 61 72 69 1c 02 19  |os.....safari...|
000004f0  00 06 74 72 61 76 65 6c  1c 02 19 00 04 77 69 6c  |..travel.....wil|
00000500  64 1c 02 19 00 08 77 69  6c 64 6c 69 66 65 1c 02  |d.....wildlife..|
00000510  19 00 04 65 61 72 73 1c  02 19 00 08 69 73 6f 6c  |...ears.....isol|
00000520  61 74 65 64 1c 02 65 00  0c 53 6f 75 74 68 20 41  |ated..e..South A|
00000530  66 72 69 63 61 1c 02 6e  00 17 44 75 6e 63 61 6e  |frica..n..Duncan|
00000540  20 4e 6f 61 6b 65 73 20  2d 20 46 6f 74 6f 6c 69  | Noakes - Fotoli|
00000550  61 1c 02 73 00 07 37 32  38 35 37 34 36 1c 02 74  |a..s..7285746..t|
00000560  00 17 44 75 6e 63 61 6e  20 4e 6f 61 6b 65 73 20  |..Duncan Noakes |
```

Listing 8: Ergebnis von **scalpel**

```
# Scalpel configuration file
# [...]
#-----------------------------------------------------------------
# GRAPHICS FILES
#-----------------------------------------------------------------
#
#
# AOL ART files
# art y 150000  \x4a\x47\x04\x0e  \xcf\xc7\xcb
#   art y   150000  \x4a\x47\x03\x0e  \xd0\xcb\x00\x00
#
# GIF and JPG files (very common)
gif y 5000000   \x47\x49\x46\x38\x37\x61  \x00\x3b
gif y   5000000   \x47\x49\x46\x38\x39\x61  \x00\x3b
jpg y 5242880   \xff\xd8\xff???Exif   \xff\xd9  REVERSE
jpg y 5242880   \xff\xd8\xff???JFIF   \xff\xd9  REVERSE
#
#
# PNG
png y 20000000  \x50\x4e\x47? \xff\xfc\xfd\xfe
#
#
# BMP   (used by MSWindows, use only if you have reason to think there are
#       BMP files worth digging for. This often kicks back a lot of false
# positives
#
# bmp y 100000  BM??\x00\x00\x00
#
# TIFF
#   tif y 200000000 \x49\x49\x2a\x00
# TIFF
# tif y 200000000 \x4D\x4D\x00\x2A
```

```
32 #
33 #------------------------------------------------------------------
34 # ANIMATION FILES
35 #------------------------------------------------------------------
36 #
37 # AVI (Windows animation and DiVX/MPEG-4 movies)
38 #   avi y 50000000 RIFF????AVI
39 #
40 # Apple Quicktime
41 #   These needles are based on the file command's magic.  I don't
42 #   recommend uncommenting the 4th and 5th Quicktime needles unless
43 #   you're sure you need to, because they generate HUGE numbers of
44 #   false positives.
45 #
46 # mov y 10000000  ????moov
47 # mov y 10000000  ????mdat
48 # mov y 10000000  ????widev
49 # mov y 10000000  ????skip
50 # mov y 10000000  ????free
51 # mov y 10000000  ????idsc
52 # mov y 10000000  ????pckg
53 #
54 # MPEG Video
55 # mpg y 50000000  \x00\x00\x01\xba  \x00\x00\x01\xb9
56 # mpg     y    50000000  \x00\x00\x01\xb3  \x00\x00\x01\xb7
57 #
58 # Macromedia Flash
59 # fws y 4000000 FWS
60 #
61 #------------------------------------------------------------------
62 # MICROSOFT OFFICE
63 #------------------------------------------------------------------
64 #
65 # Word documents
66 #
67 #
68 doc y 10000000  \xd0\xcf\x11\xe0\xa1\xb1\x1a\xe1\x00\x00 \xd0\xcf\x11\xe0\xa1\xb1\
       x1a\xe1\x00\x00 NEXT
69 doc y 10000000  \xd0\xcf\x11\xe0\xa1\xb1
70 #
71 # Outlook files
72 # pst y 500000000 \x21\x42\x4e\xa5\x6f\xb5\xa6
73 # ost y 500000000   \x21\x42\x44\x4e
74 #
75 # Outlook Express
76 # dbx y 10000000  \xcf\xad\x12\xfe\xc5\xfd\x74\x6f
77 # idx y 10000000  \x4a\x4d\x46\x39
78 # mbx y 10000000  \x4a\x4d\x46\x36
79 #
80 #------------------------------------------------------------------
81 # WORDPERFECT
82 #------------------------------------------------------------------
83 #
84 # wpc y 1000000 ?WPC
85 #
86 #------------------------------------------------------------------
87 # HTML
88 #------------------------------------------------------------------
89 #
90 htm n 50000    <html       </html>
91 #
92 #------------------------------------------------------------------
93 # ADOBE PDF
```

```
94 #-------------------------------------------------------------------------
95 #
96 pdf y 5000000 %PDF  %EOF\x0d  REVERSE
97 pdf y 5000000 %PDF  %EOF\x0a  REVERSE
98 #
99 # [...]
```

4.2 Bilder

Abbildung 1: Bild 1

Abbildung 2: Bild 2

Abbildung 3: Bild 3

Abbildung 4: Bild 4