Digital Forensic Report
Exhibit No. 45/28/2015

Max Muster

May 13th 2022

Contents

1 Prolog

1.1 Summary of Case and Tasking

The public prosecutor's office has initiated preliminary investigation against Mr. Jürgen S. He is suspected of possessing illegal rhinoceros images (illegal rhinography) according to § 184m StGB (German Criminal Code). According to § 184m StGB it is illegal to knowingly possess more than 3 images of rhinoceroses

During a house search in the apartment of Mr. S. on 25.10.2016, an external USB thumb drive (brand Oceangateway, evidence number 45/28/2015, year of manufacture 2007) was seized. The defendant admitted to being the owner of the drive, which he had purchased second-hand on the Internet three years before the seizure.

The author of this report was appointed as digital forensics expert to analyze the seized USB drive.

The prosecution requests answers to the following questions:

1. Are there image files on the disk that are potentially of rhinographic nature?
2. For how many of the images is there reason to believe that the defendant knew of their existence?

1.2 Proof of the integrity of the exhibit

To ensure the Chain of Custody various measures were implemented.

1.2.1 Tamper-proofing of the Analysis

Initially, the prosecutor's office called, giving instructions on the analysis and information on a courier that would soon be sent over. The courier arrived within hours, delivering two letters, with their seals still intact, and the exhibit. The letters contained the analysis task and the exhibit's hash sum respectively. The exhibit seemed untampered with upon visual inspection. By showing an ID, the courier could identify himself as being sent by the prosecutor's office. As shown in section 1.2.2, the hash sum was then immediately calculated on the analysis computer. After the successful comparison to the hash sum from the letter, a working copy of the exhibit was created and the original and its hash sum securely locked into separate safes. From this moment on, both items were only taken out of their safe on two occasions: For the final integrity check and when handing the exhibit back to the courier.

Both the safes as well as the forensic workstation are located in a forensic laboratory. This laboratory is structurally modified to render undetected entering impossible. It has no windows and the doors are locked by a state-of-the-art locking system. If any door stays open for more than ten seconds, an alarm will sound and the security service will be immediately notified. For each room only the analysts currently working in it have the keys. The whole laboratory is being camera surveilled around the clock by a remote security service. Any access to doors or working devices as well as all system anomalies are being logged.

Each analysis room contains three safes and a digital forensic workstation. The three safes are used to separately store exhibits, hash sums and the workstation, when they are not in use. The access codes are only known to the persons working on the analysis task the room is assigned to. The work environment consists of a computer (see Section 1.3 for specifics) and necessary equipment to work on exhibits. The computer is air gapped from any network at all times, updates are being

deployed by portable devices. Before connecting any portable device to the workstation, it is ensured that no malware is present on the portable device. The hash sums of any software or software update brought to the workstation are compared with the one published by the software manufacturer before installation. On the computer there is only software which is necessary for digital forensic analyses. Each separate analysis is being conducted on a fresh live system. If during an analysis the necessity for any research should arise, a separate computer system specifically for this task is used. Since this separate computer system is never used to handle evidence, there is no problem with it being connected to the Internet.

1.2.2 Checking the Hash Sums

Upon receipt of the disk image, the following *SHA256* sum was handed over:

```
a27ae11f02b661a14b546e93b7df92c6c78b4392296d59fc892b97358d63aafc
```

Immediately after receipt of the exhibit, the hash sum was caluclated on the evidence and successfully compared to the one delivered by the courier (see Figure 6). Any time a working copy of the exhibit was created, the hash sum was also checked and proved to be correct everytime.

For each file or any data that were extracted from the exhibit a hash sum was immediately created and subsequently both manually and digitally documented. All hash sums were checked again at the end of the analysis: None of the sums diverted from their documented counterpart (see Figure 11).

1.3 Working Environment

1.3.1 Used Hardware

The work environment consisted of a workstation of type *Leneu IdeenPad 5 15ARE05* from 2020. It contains the following components:

- Processor: ADM Risen 5 4600U (6 Core, 12 threads, 8MB Cache, up to 4.00 GHz)
- Memory: 16 GB DDR4 3200 MHz
- First Hard Drive: 1 TB, 5400 Rpm HDD
- 128 GB SSD, M.2 2242, PCIe, NVMe, TLC
- Monitor: 15.6" FHD, IPS, 300 cd/m^2
- Graphics: integrated in CPU
- Peripheral: 2x USB-A 3.1 Gen 1, 1x USB-C Gen 1

Since the computer was aquired, no changes were made to any of the systems' components. It remains the way it was manufatcured.

1.3.2 Used Software

The analysis system is running *Kali GNU/Linux Rolling (64-bit)* with version *Debian 5.10.28-1kali1 (2021-04-12)*.

Apart from the operating system and its standard tools, the following software was used in the analysis:

Name	Version	Note
Sleuthkit	4.11.1	
Testdisk	7.1	
Photorec	7.1	
ClamAV	0.103.5/65537	with virus database from May 11th 2022
Exiftool	12.41	
hexedit	1.5-5	
xxd	2:8.2.3995-1+b3	

2 Analysis Summary

As requested by the prosecutor's office, I examined the evidence provided to me according to the investigation order. Regarding the first question the analysis found three distinct pictures we believe, based on their content, could be of interest:

1. First picture: A nameless image showing a rhinoceros standing on green grass and in front of green bushes (see Figure 1)
2. Second picture: An image named "riNoHorn.jpg" which depicts a presumably young rhinoceros walking towards the camera and away from wooden barricades in the back (see Figure 2)
3. Third picture: An image named "rhino.jpg", showing a figurine shaped like a rhinoceros, made from a golden material (see Figure 4)

For the second and third picture, we also found thumbnails (small preview images) which can be seen in Figures 3 and 5. Analyzing the metadata of the image files produced possible information on the origin of these pictures. The nameless image's Owner is listed as "John Mountjoy", the picture may have been shared using the platform "Flickr" and created on 2010:05:09 13:14:04 CEST. "riNoHorn.jpg" had tags indicating the picture was taken with a "CANON EOS-1D Mark III" camera on 2013:07:06 16:29:43 CEST by a person named "Holly Occhipinti". The image "rhino.jpg" was at some point downloaded from "wikimedia", the owner is named as "Sian Tiley-Nel" and the files creation date is 2012:05:09 12:44:35 CEST. The name Jürgen S. appeared nowhere on the exhibit, even when explicitly searching for it. For the second picture there also was metadata describing the pictures content as "Cute baby white rhino with large feet" and "Baby Rhinoceros". The tags for "rhino.jpg" had the original file name as "/File:UP_rhino.JPG".

To determine whether or not Jürgen S. knew of theses pictures several aspects are important. One of these is the location where the pictures were found on the exhibit. Storage devices, such as the provided evidence, can be logically divided into multiple parts. That means, while the disk stays physically intact and whole, computers recognize multiple storage areas on it. Also, these areas do not have to cover the whole disk at all times. It is not only possible but common for some part of disks to stay unused for various reasons, for example not needing the whole storage space or saving it for later. The free, unused parts are called unpartitioned, while the divided and used areas are called partitions. On the exhibit there is roughly 10% unpartitioned disk space, while the remaining 90% are used in a normal partition. When connecting the disk to a normal personal computer, the files stored in that partition are visible to and modifiable by the user. The unpartitioned space however can only be read and modified with additional tools and computer knowledge beyond that of a normal user.

We found the first picture in this unpartitioned storage space. To give an indication about Jürgen S.'s knowledge about this picture, we tried to find clues of how and when the picture was stored there and if it had been viewed. Apart from the metadata timestamp above, this proved difficult. It is the nature of unpartitioned space to have no documentation of usage, therefore no additional usage data could be found. Note that the date provided above only tells the time the picture was created. It cannot be used to say with certainty that it was placed on this disk at the time, though it could be possbile. But it could also have been transferred from a computer or other storage medium to this disk at another, undocumented time. If Jürgen S. evidently does not posses advanced skills with computers, it would be highly unlikely for him to have placed or used this picture. In this case him knowing about the picture or its content would also be highly unlikely. If, on the other hand, he does have such knowledge, we believe it to be likely he knew about this picture, based on unpartitoned areas being typical hiding places.

The other two pictures were found on the file system in the partitioned area. In contrast to the unpartitioned space, file systems document the last usage of files. The second picture had been deleted by the user but could be recovered during the analysis. The exhibit must not have been used much since the deletion, else the picture would have been overwritten and would not have been recoverable. The third picture still existed on the file system. Both pictures were intially placed in the root directory of the file system, meaning they would be directly visible when opening the disk on a computer. However, the deletion of the second pictured changed that. From the moment of its deletion the second picture would have been invisible to a normal user. The time stamp of last usage for both these pictures are 2015:09:23 16:49:36 CEST. This is also the timestamp for the deletion of the second picture. The disk's owner at the time, Jürgen S., will have not only viewed the picture "rhino.jpg" but also deleted the picture "riNoHorn.jpg". We therefore conclude that he had knowledge of these two pictures. According to the file systems meta data this was also the last time the disk was used.

The metadata on the disk is generally consistent, making it highly unlikely the evidence was manipulated before or after it was seized. It seems however likely that the last usage of the disk was also the time the second and third picture were copied onto the disk, right after their file system was created. This means the picture "riNoHorn.jpg" was deleted right after it was copied to the disk. Also, all timestamps we found were set by the computer the disk was used with. If at that time this computer's clock was not set correctly or even manipulated, it would not be evident on the disk. Based on the exhibit it cannot be ruled out, that any or all timestamps could therefore be incorrect.

Routinely, the exhibit was checked for malware, none could be found.

If further investigation is necessary, we would suggest analyses of the computers Jürgen S. could have used that disk with. Even though malware could be most definitely ruled out as source of traces or evidence, further malware analysis on these computers could further affirm the absence of malware. Also the uncertainty regarding the timestamps could be significantly reduced by examining the clock of the computers the disk was used with. We believe it also possible to find further evidence on these computers to prove or disprove whether Jürgen S. knew about the first picture we found.

3 Technical Details

This section presents the exact procedure of the exhibits analysis. It documents the analysis approach, the use of the forensic tools and discusses the results. In general the same tools are used for the same tasks, therefore forensic tools are only explicitly named at the first use or when it could be ambiguous which tool was used.

The analysis was conducted on May 11th 2022.

3.1 Preservation

Upon receiving the exhibit and its hash sum, the exhibit was immediately loaded onto the analysis computer and its was hash sum calculated by using the tool *sha256sum*. The calculated hash sum was identical to the one handed over by the courier (see Figure 6).

For keeping the original image as a backup, with help of *dd* a working copy of the exhibit was created, as seen in Figure 6. The exhibits size is *20971520 Bytes* or roughly *20 MB*. Any and all analysis work was done on this copy. The only exception to this is the malware analysis, for which a separate copy was created (see Figure 7). For both these copies, the hash sum was immediately created and successfully compared to the one of the original image.

This procedure was kept up for any data extracted or generated by the forensic tools: The resulting files' hash sums are immediately calculated. The resulting hash sums were subsequently both digitally and by hand secured in writing. This is implicitly done and will usually not be mentioned in the further course of this section.

After finishing the analysis, all recorded hash sums were recalculated and compared to the saved original ones. Figure 11 is proof that none of the hash sums differed.

Therefore the analysis integrity is ensured.

3.2 Recovery

3.2.1 Disk Structure

The exhibits working copy is present as raw data, the file ending on *.img* indicating it to be a disk image. *file* seems to confirm this assumption, reporting the file to host a *DOS/MBR* partition scheme (see Figure 13). As seen above, the exhibit's size is roughly *20 MB* and therefore relatively small for a hard drive disk.

According to *fsstat* the image contains high entropy, though this could be a false-positive caused by the unusually small image size and its therefore relatively high amount of data entropy (see Figure 13).

Using *TheSleuthKit's* tools *mmstat* and *mmls*, we find further indication of a *DOS/MBR* partition scheme. The sector size of units is usual *512 Byte*. *mmls* also shows the partition table according to its analysis of the *MBR*. It identifies only one partition that comprises nearly the whole disk. The partition type is set as *Linux*. The only other sections on the disk are the *MBR* and some (roughly 10% of the whole disk) unallocated space 13 between the *MBR* and the partition. So far, the partition layout seems normal.

The previous findings were confirmed by manually looking at the *MBR* with *hexedit*, as seen in Figure 14. The *MBR* structure appears to be in order, no abnormalities were found. The *bootloader* is zeroed, the disk image therefore is non-bootable. This fits the exhibit's usage as external hard drive disk which normally do not contain bootable systems. No further information regarding the partition structure could be found.

It is not uncommon for the partition and file system structure to change over time. By using *testdisk* we try to find traces of such previous structures. Matching previous findings, it automatically identifies the exhibits file size as *20 MB*. The partition table type was unsurprisingly automatically identified as *Intel* and therefore chosen as analysis option, before running *testdisk* (see Figure 15). A *HPFS - NTFS* file system could be found that can, by its geometry, be identified as the *Linux* partition that was previously found, as seen in Figure 16. Conversion from CHS to LBA was done with `https://chstolba.org/` (last retrieved on May 11th 2022). Using the *Deeper Search*, no other file systems or their remainings could be found 17.

3.2.2 File Systems and Files

Testdisk was also used to list the content of the *NTFS* file system it found. As can be seen in Figure 18, it identifies a single file with filename "rhino.jpg". Using *testdisk's* file extraction functionality, the picture was cut from the exhibit's image. Subsequently, its hash sum was computed 8.

When extracting files with *testdisk*, the *modifyied*-timestamp is set accordingly, therefore *stat* was used to on the extracted picture obtain this timestamp (see Figure 19). Also, the *exif* meta data was extracted by using *exiftool*, the results can be seen in Listing 1.

Now, the *SleuthKit's* Tools were used to examine the only found partition. To address the partition, its offset (3456 sectors) was given together with the *-o* flag as argument to all tools. With the help of *fsstat*, the metadata of the partition's file system was extracted. As can be seen in Figure 20, the file system type was identified as *NTFS* being created by Software originating from *Windows XP*. This seems contrary to the partition type being *Linux*. Listing the file systems content with the help of *fls -r* confirmed the type to be *NTFS*, because it only contained the meta files that fit an *NTFS* file system. The listing with the file systems content can be found in Listing 4. This listing also shows the file system metadata of the content according to the *-l* flag.

Three entries have names that could indicate content relevant to this analysis: "rhino.jpg" (inode 65) and two copies of "rhiNoHorn.jpg" (inodes 0/64). Apart from some OrphanFiles, these three entries seem to be the only files apart from meta files on the file system. The entry of file "rhino.jpg" is inconspicuous apart from its name, while the two entries of "rhiNoHorn.jpg" indicate that the file is no longer regularly existent on the file system. The matching name and absence of other artifacts of recent deletion suggest the name "rhiNoHorn.jpg" formerly belonged together. The linking of file metadata and content seems to be broken, indicating the file was deleted, but neither its *MFT* entry nor its data blocks were overwritten yet. A probable reason for this is that the deletion resulted from recent usage, meaning there has not yet been enough further use of the file system to overwrite the data.

There are also eight "OrphanFiles" listed, but using *istat* to look at their metadata and size, all of their data blocks or original names are not recoverable.

The files "rhino.jpg" and "rhiNoHorn.jpg" were extracted into files using *icat*, as can be seen in Figure 21. Both files were immediately hashed and their *exif* data was extracted. For each file the meta data was further examined using *istat* 24 25.

To further investigate file deletion, both the meta file *$MFT* and its mirror *$MFTmirr* were extracted together with their meta data, visible in Figures 22 and 26. They were subsequently compared to each other with the help of the tools *diff* and *xxd* (see Figure 32). Also, the *$LogFile* was extracted, but *hd* shows it to be completely filled with ones and therefore void of information, as can be seen in Figure 23.

3.2.3 Carving

To find any data structure that might be a picture, the exhibits image was then carved using *photorec*. Analogous to *testdisk*, *photorec* identified the disk's structure and size matching previous findings. The carving tool was instructed on searching the image assuming there to be no partitions and no file systems present on the disk. *Photorec* reports finding three images, as can be seen in Figure 27. The target directory additionally contains two files with filenames leading with a "t", indicating matching thumbnails for two of the images. All resulting files were hashed (see Figure 9).

As with *testdisk*, *photorec* also sets the *modified*-timestamp. It was extracted for all five pictures analogously (see Figures 28 and 29). Also, for all pictures any available *exif* metadata was extracted (see Figure 2).

3.2.4 Malware analysis

Routinely, the exhibit was checked for signs of malware. First, the malware database was updated, using *freshclam*. Then, the separate image copy created at the beginning of the analysis was searched for traces of malware with *clamscan*. Figure 31 shows that no malware or traces of it could be found.

3.3 Analysis

Based on the examination described above, this subsection presents the evidence found and possible explanations for these.

3.3.1 Findings

All analysis methods were in agreement that the disk's size is *20 MB* and was partitioned with a *DOS/MBR* partitioning scheme. The disk was not bootable and has only one valid partition which comprises roughly 90% of the exhibit's overall storage space. The partition's type was given as *Linux* while its file system is of type *NTFS*. While this is not typical, it is not uncommon to (re-)format partitions with new file systems, which seems likely to be the reason here. Between the *MBR* and the partition the disk is unpartitioned. There were no traces of previous file systems or partitions. *fsstat* identified the disk to have high entropy, possibly indicating encryption. However, analysis did not substantiate this. A more likely explanation for this would be that, due to the high disk usage found during the analysis, the images data appeared highly entropic.

Reading the contents of the partition's file system, *testdisk* only found a single file named "rhino.jpg" which contains a picture and can be seen in Figure 4. The image shows a figure which depicts a golden rhinoceros. Analysis (with tools from *TheSleuthKit* toolkit suite) of the *NTFS* file system produced a picture with identical name and appearance. Additionally, another picture named "riNoHorn.jpg" was found. It had been deleted from the file system, however this seems to have happened recently as all data and meta data were still present. The image shows a young rhinoceros walking towards the camera and away from wooden barricades. The picture is shown in Figure 2. With *photorec*, three pictures could be recovered. Two of those show the same motives as previously found, the third one shows the side view of a rhinoceros, standing surrounded by green nature (see Figure 1). According to the disk sector, *photorec* found this picture in, it is stored in the unpartitioned disk space. Comparing the pictures that show the same motives, we found the files' hash sums to be identical, meaning the pictures are identical (see Figure 11). The pictures named "rhino.jpg" by *testdisk* and *TheSleuthKit* were found to be identical. Also the picture "rhino.jpg" is identical to "f0026472.jpg" and "riNoHorn.jpg" identical to "f0026304.jpg".

Photorec also found two thumbnails that matched storage address and content of the images recovered from the *NTFS* file system. These can be seen in Figures 3 and 5. Extraction of the *exif* data produced the same thumbnails from the pictures found through *TheSleuthKit* and *testdisk*.

Overall three unique pictures and two unique thumbnails were found on the exhibit that we believe could possibly depict rhinographic content.

Further analysis of the *exif* data (see Listings 1, 2 and 3) resulted in information that may possibly increase the likelihood that the pictures contain rhinographic content. The *exif* tags for "riNoHorn.jpg" describe its content as "Cute baby white rhino with large feet" or "Baby Rhinoceros", while the tags for "rhino.jpg" had the pictures original file name as "/File:UP_rhino.JPG".

There were also tags on possible origins of the images: The image found in the unpartitioned storage space named the owner as "John Mountjoy" and there is a tag indicating it was shared using "Flickr". "riNoHorn.jpg" had tags indicating the picture was taken with a "CANON EOS-1D Mark III" camera by a person named"Holly Occhipinti". According to two of the *exif* tags, the origin for "rhino.jpg" is "wikimedia" and the owner is "Sian Tiley-Nel".

Lastly, the *exif* data shows the pictures to have been created at the following times: 2010:05:09 13:14:04+02:00 (picture in unpartitioned space), 2013:07:06 16:29:43+02:00 ("rhiNoHorn.jpg") and 2012:05:09 12:44:35+02:00 ("rhino.jpg"). Together with the file system meta data which shows nearly all timestamps as 2015:09:23 16:49:36+02:00, the timestamps seem consistent at first glance. There are however four timestamps that are different: The timestamps stored in *$STANDARD_INFORMATION* for *$MFT* show a date in *2076* which obviously cannot be the time the file was created. Also, it seems remarkable for all file system timestamps to share exactly the same date and time. The comparison of both *$MFT* files showed no unusual differences in their content, with *$MFTmirr* missing only the newest entries from *$MFT*. This means, that in *$MFT* and *$MFTmirr* *$STANDARD_INFORMATION* stores *2076* as timestamp for *$MFT*. The analysis of *$LogFile* did not help resolve any of these problems since it was empty. Section 3.3.2 further covers these abnormalities.

The malware analysis was inconspicuous. With no evidence of malware, it can be assumed that all traces and findings did not result from malware activities. However, an infection of the computer the disk was used on could not be ruled out. If this was the case, data on the exhibit could have originated from that malware.

3.3.2 Conspicuities

After discovering the presented abnormalities, the *created* timestamp from the *$MFT* was further investigated. Looking at the entries in *hexedit*, it becomes clear that the field which stores this timestamp is simply zeroed in *$STANDARD_INFORMATION* in *$MFT* and *$MFTmirr*, while it is intact in *$FILE_NAME* (see Figure 5). It seems that *TheSleuthKit* simply misrepresented the Bytes if the timestamps was zero. As to why the field is zeroed at all, no indications could be found. Manipulation could be a possibile explanation, but we cannot envision a reason to modify a single metafile timestamp. This appears especially futile since the timestamps of *$FILE_NAME* do not differ. Missing the duality of timestamp management in *NTFS* file systems seems not fitting for a highly skilled amnipulator. Therefore, we believe it is very unlikely this type of manipulation happened.

Alternatively, this could be the overlooked residue of a more extensive manipulation. In this case all timestamps had been perfectly manipulated, except for those in *$STANDARD_INFORMATION* in both *$MFT* and *$MFTmirr*. Since no other traces of manipulation were found, it seems highly unlikely a manipulator achieved hiding any or even all traces of their work but overlooked something so obvious. We therefore believe this manipulation scenario very unlikely as well. Even though there also is no proof or further indication for that, these timestamps are in our opinion far more likely

to be the result of an unknown software error.

The reason for all meta data timestamps being identical to the second could also be manipulation. However, a manipulation of that scale would, in our professional experience, require extensive effort. Far more likely, because it is less cumbersome, is a second possibility that the file system was very recently formatted and all the files were created at the same time. This could for instance have been done by a tool that creates storage mediums to automatically copy files there. Given such a tool, a normal user should be able to use it. This theory would also match the differences between *$MFT* and *$MFTmirr* and explain the "empty" *$LogFile*. In that case, the *$LogFile* was not overwritten but simply has not been filled yet.

4 Appendix

The following sections present the findings and provide proofs to support claims made in Section 3.

4.1 Found Images

This section lists all images found on the exhibit during the analysis that may be relevant to the case.

For some pictures the quality may seem unsatisfactory. The reason for this is the low file size and therefore low quality of the pictures themselves. Especially thumbnails are naturally smaller and of lower quality than the original image.

Figure 1: Image found at the beginning of the hard drive disk, outside of any file system. It shows the side view of an rhinoceros in nature.

Figure 2: Deleted image that once resided on the hard disk drives file system that could be recovered. It was not visible to the normal user. It shows a presumably young rhinoceros from the front, walking away from a wooden barrier.

Figure 3: Thumbnail of the image 2.

Figure 4: Image found on the hard disk drives file systems on top of the directory structure, making it directly visible to any user of the disk. It shows an artistic representation of a rhinoceros made of presumably gold.

Figure 5: Thumbnail of the image 4.

4.2 Proof of Integrity

This section presents proof that the exhibit and all extracted data were rigorously and regularly checked for integrity.

For the immediate creation of hash sums when extracting data also take a look at Subsection 4.3.

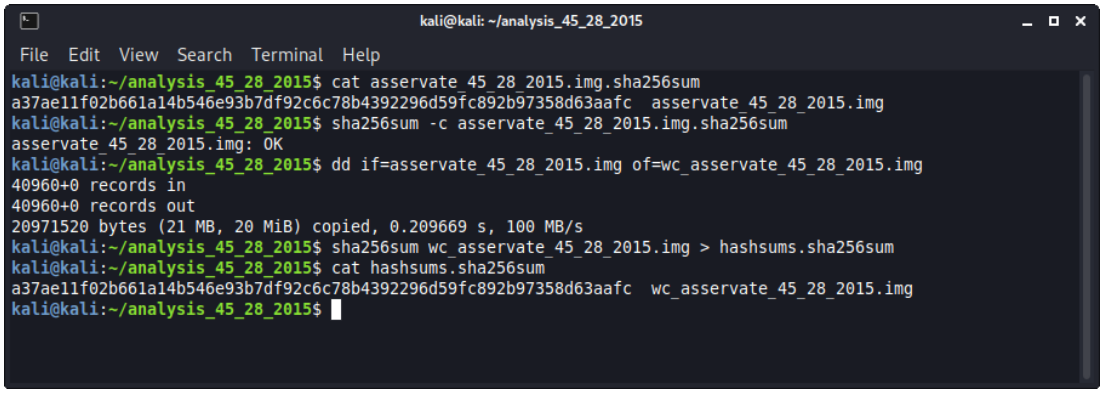

Figure 6: Initial successful calculation and verification of the exhibits hash sum. Also shows the creation of a working copy.

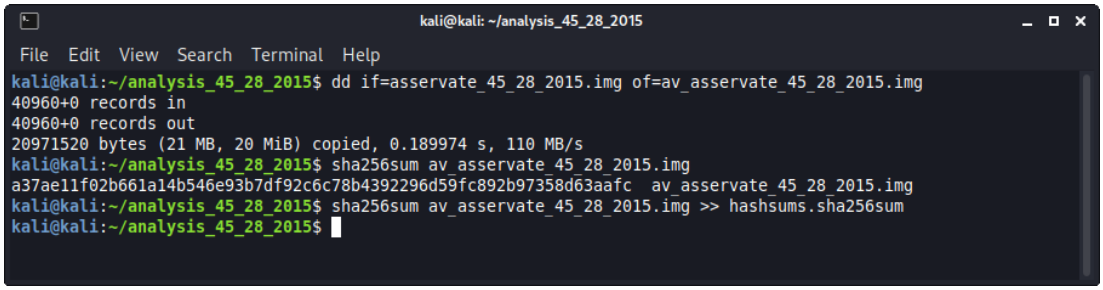

Figure 7: Creation of a working copy for the malware analysis and initial successfully calculation and verification of its hash sum.

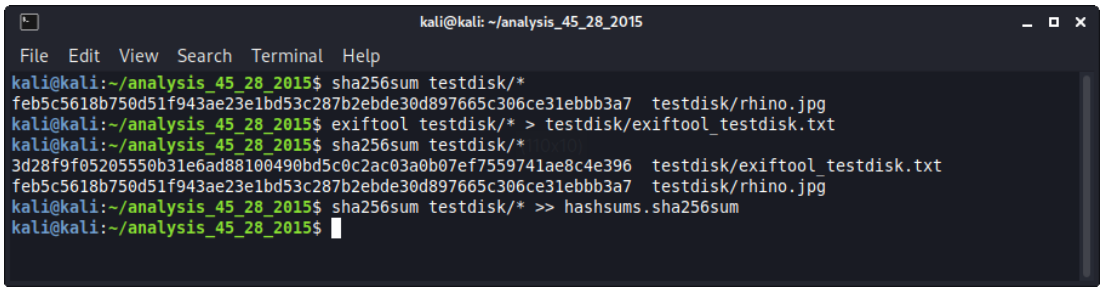

Figure 8: Creation of hash sums for the files *testdisk* returned.

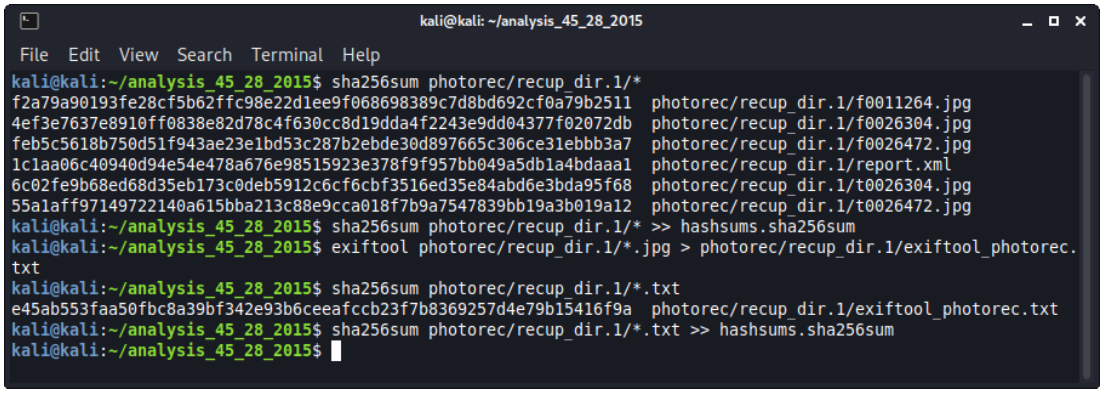

Figure 9: Creation of hash sums for the files *photorec* returned.

Figure 10: Creation of hash sums for the files that could be extracted from the disks file system.

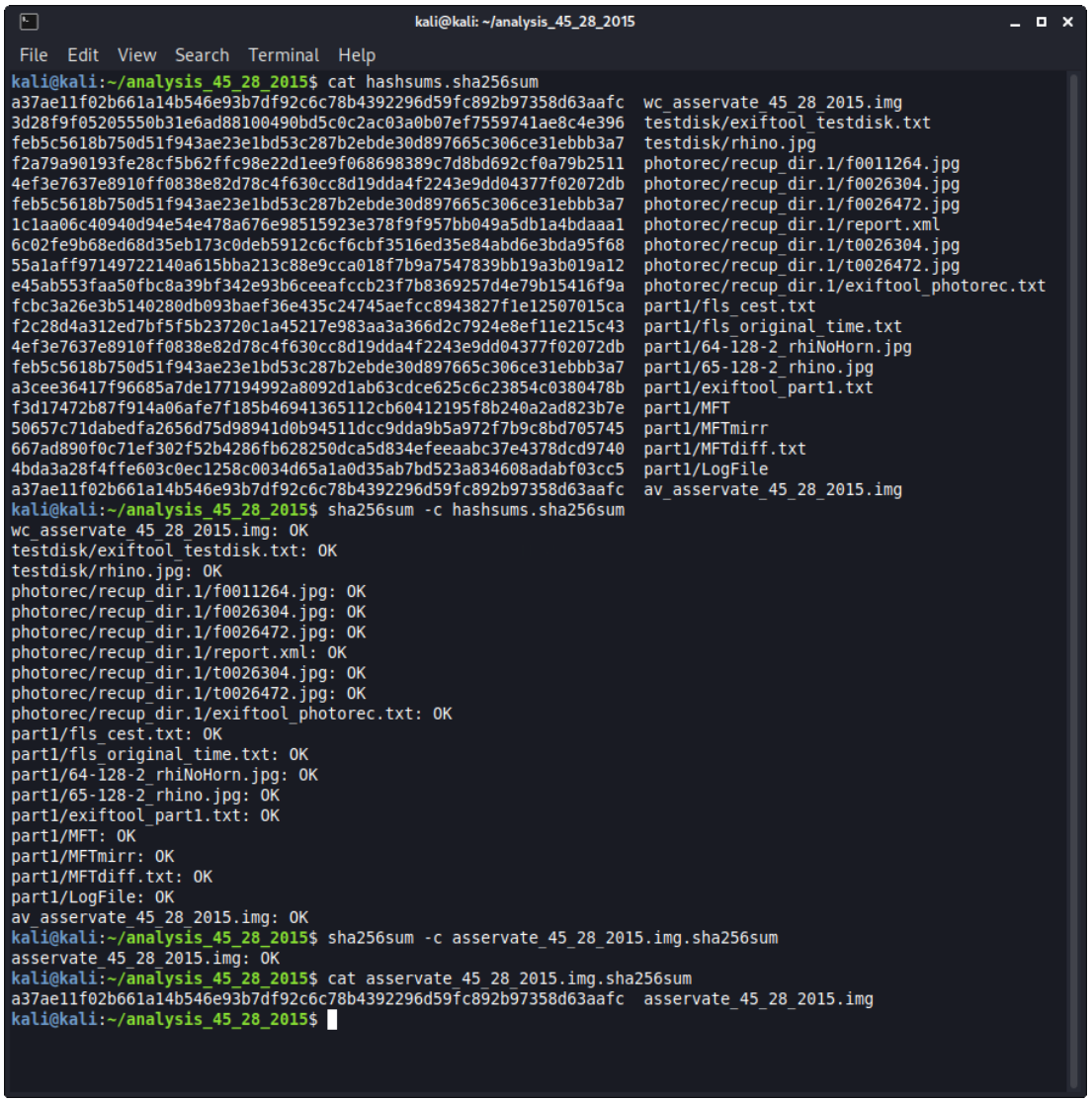

Figure 11: Final, successful calculation and verification of the exhibits and all datas' hash sums.

4.3 Console and Program Outputs

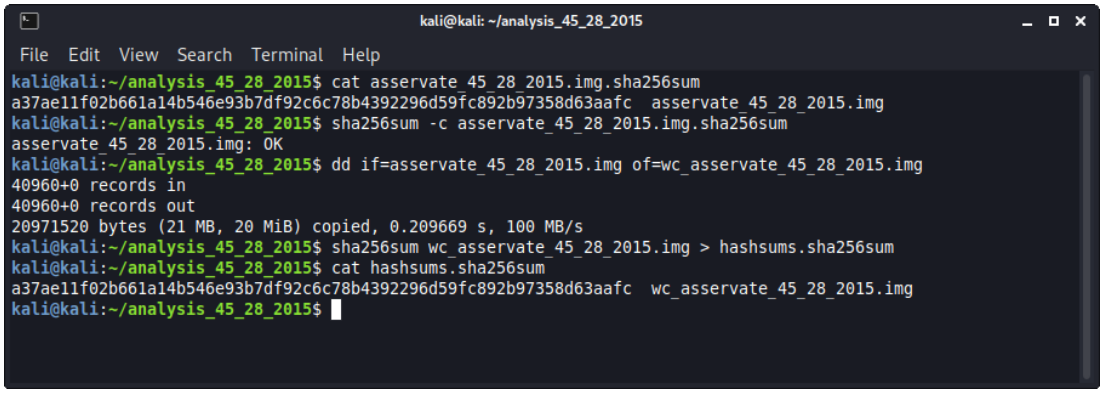

Figure 12: Initial preparation of the exhibit for the analysis.

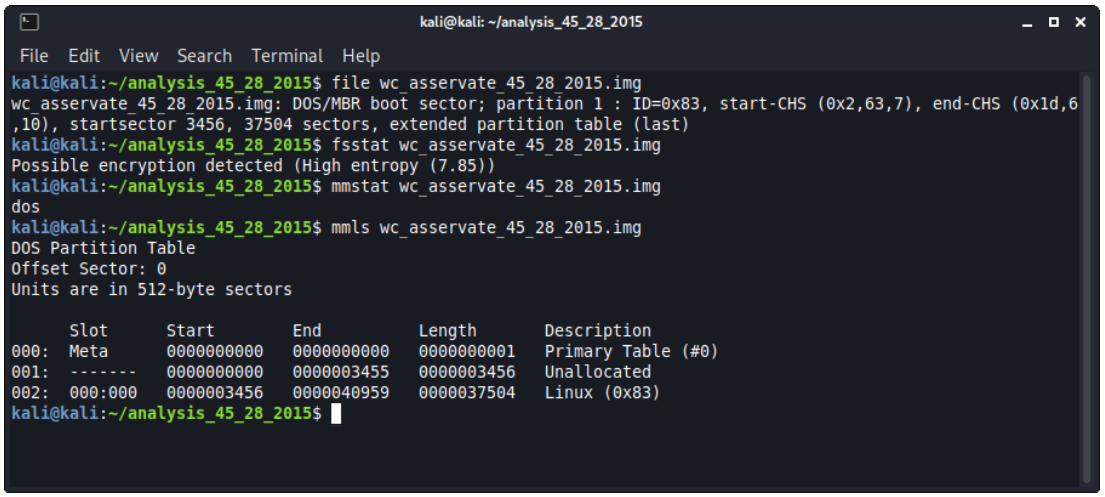

Figure 13: Analysis of exhibits file type and partition table.

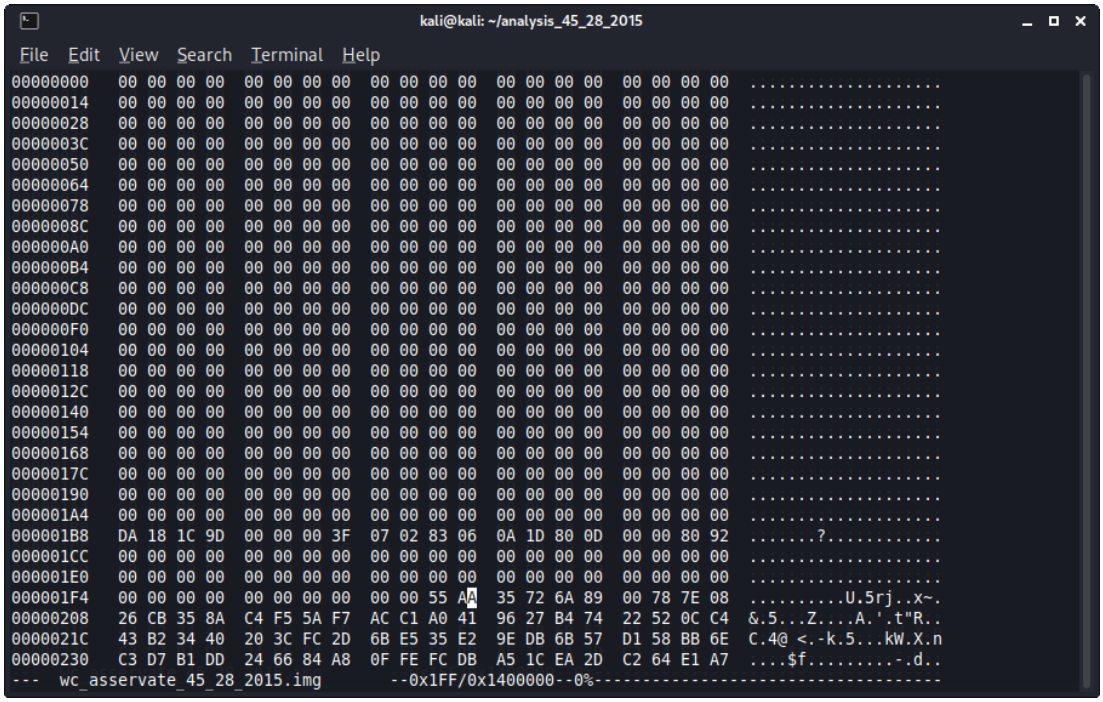

Figure 14: *MBR* area of the exhibit.

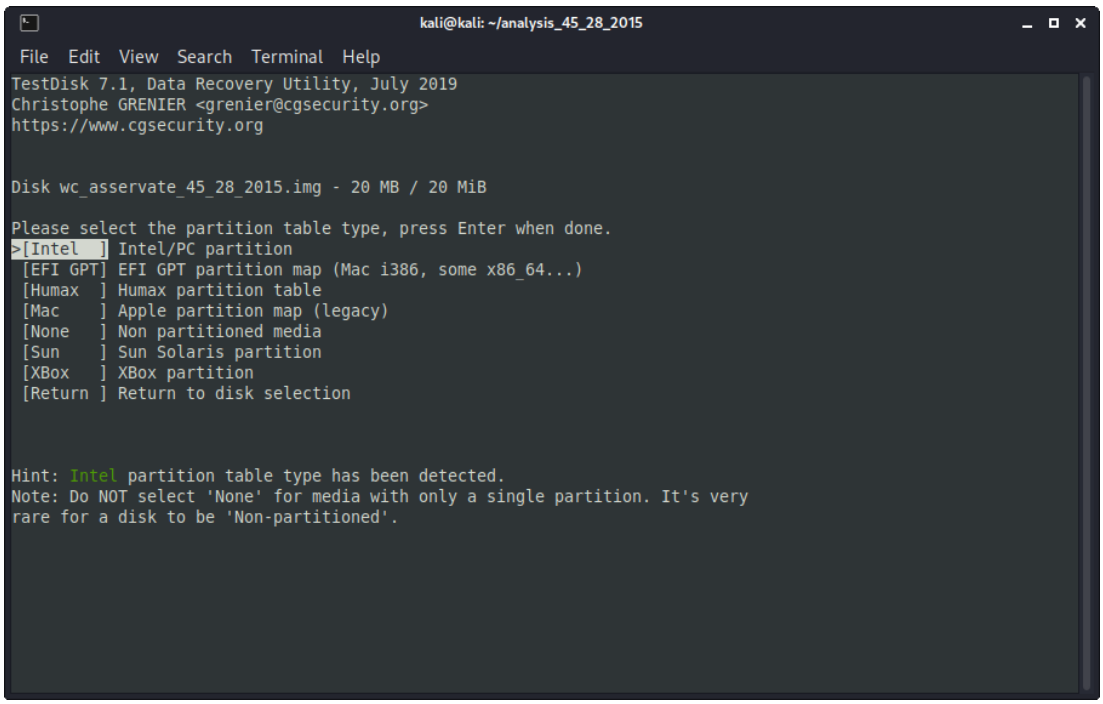

Figure 15: *Testdisk* automatically identifies the partition table type as *Intel*.

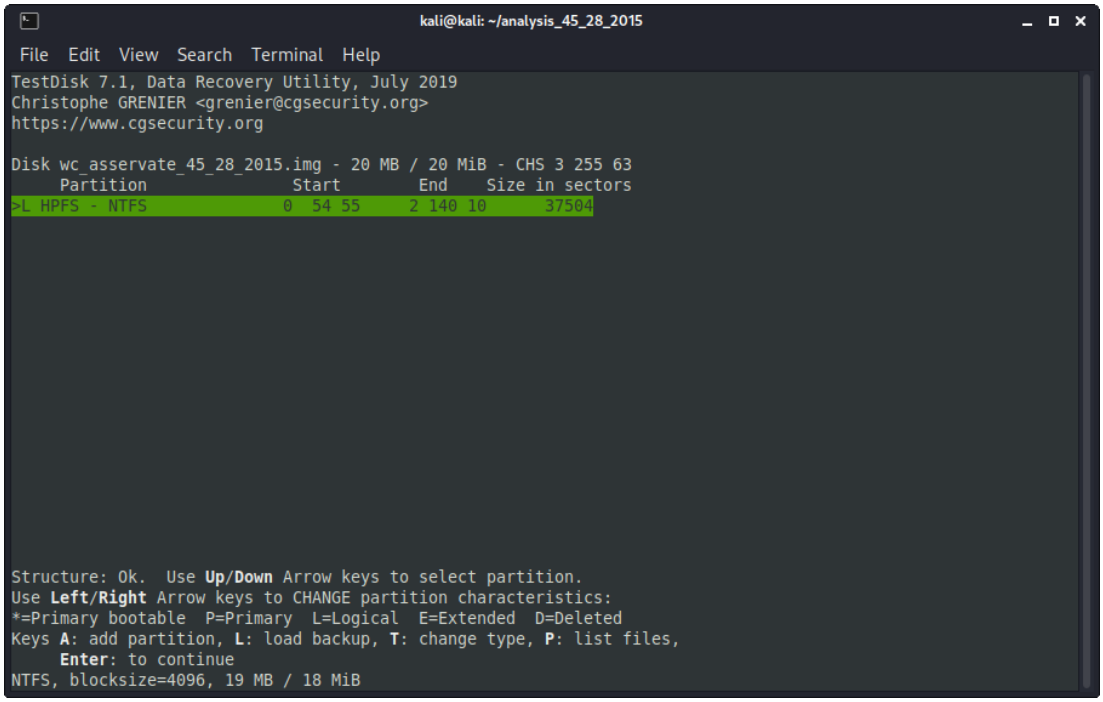

Figure 16: *Testdisk's Quicksearch* only finds one *NTFS* file system.

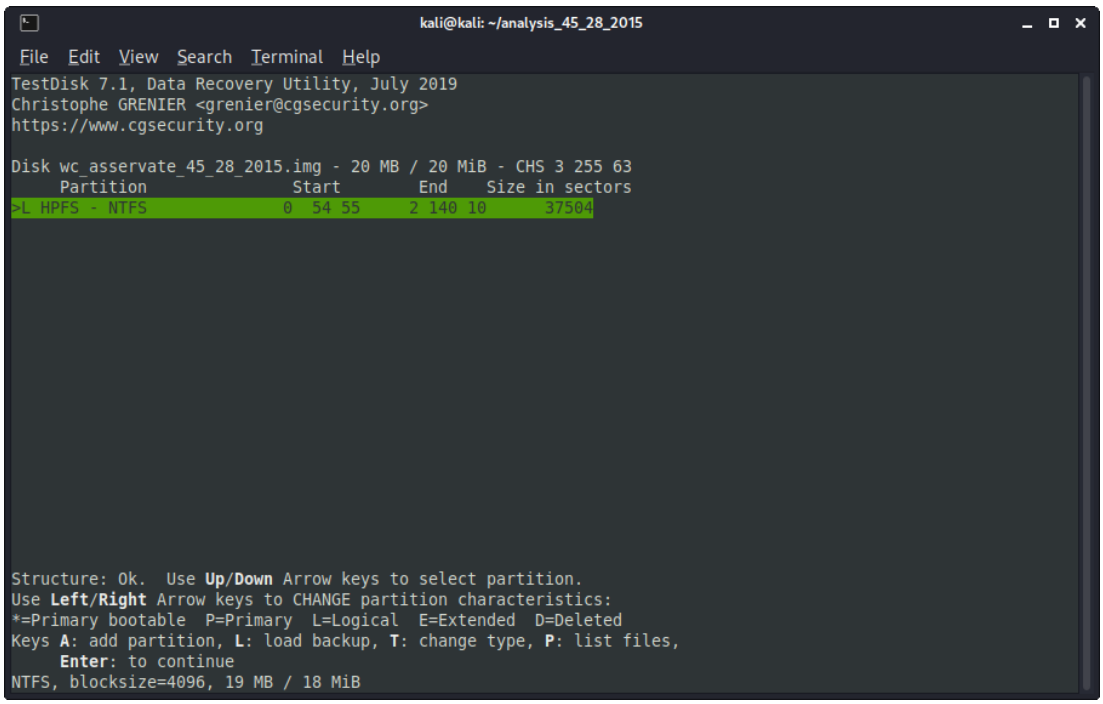

Figure 17: *Testdisk's Deeper Search* only finds one *NTFS* file system.

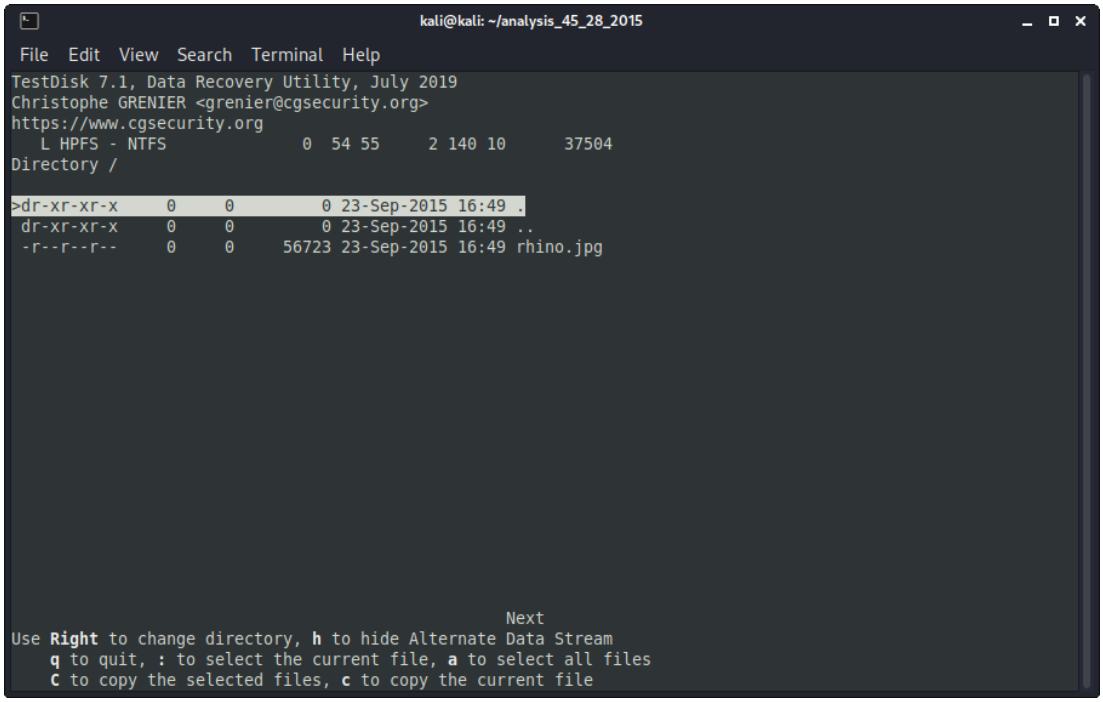

Figure 18: Content of the file system *testdisk* found. A single file named "rhino.jpg" can be seen.

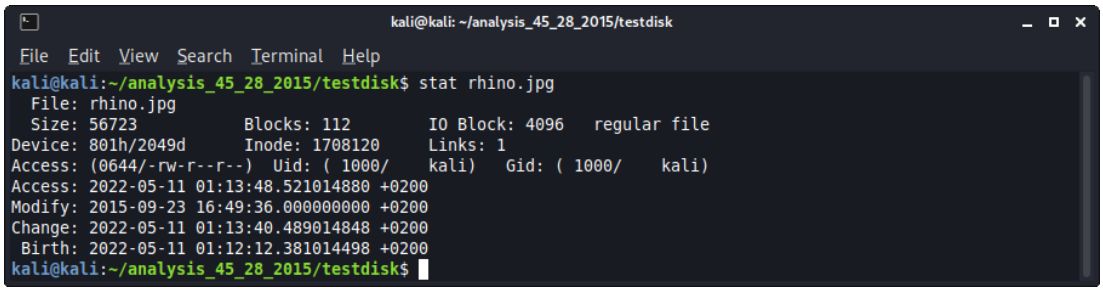

Figure 19: Result of using *stat* on the picture extracted by *testdisk*.

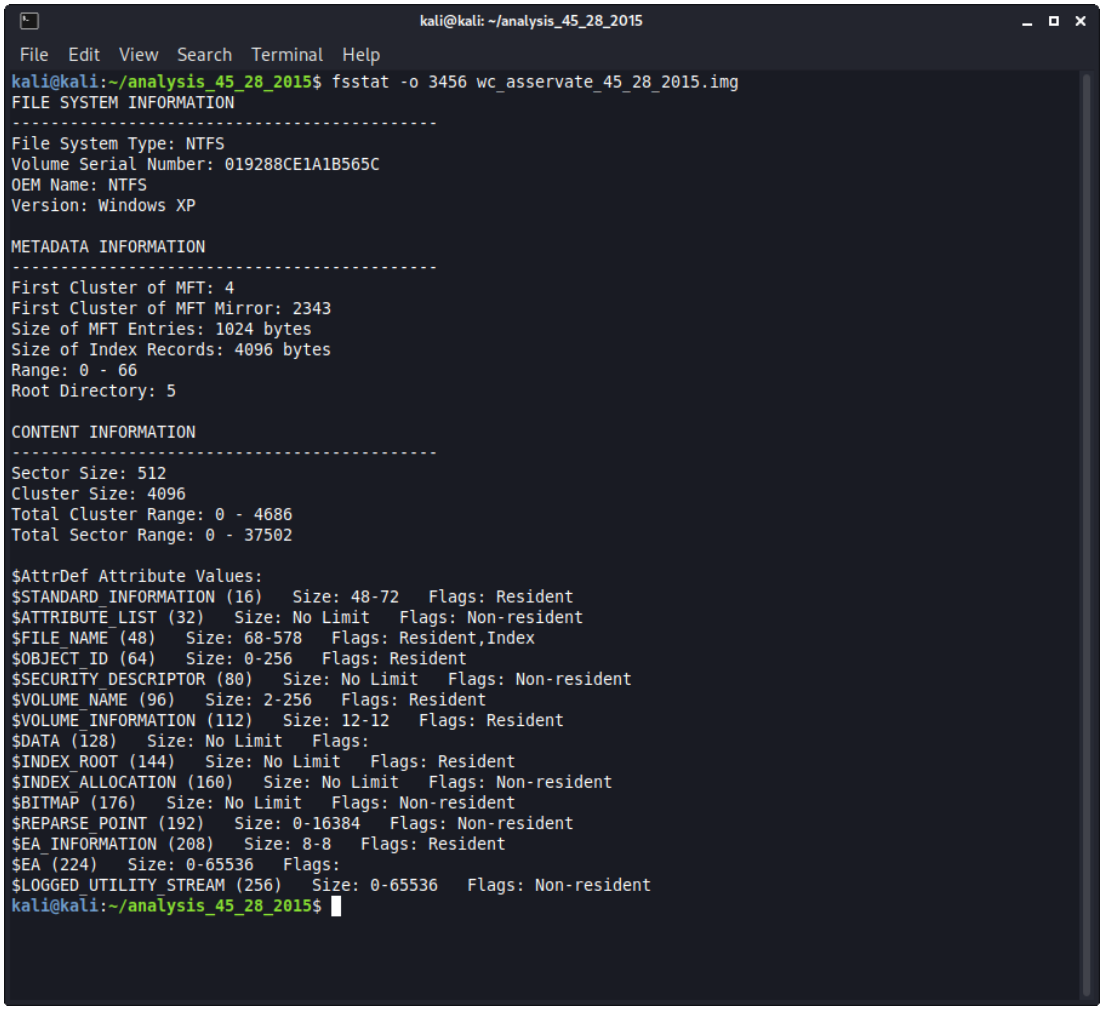

Figure 20: Result of using *fsstat* on the only partition's file system.

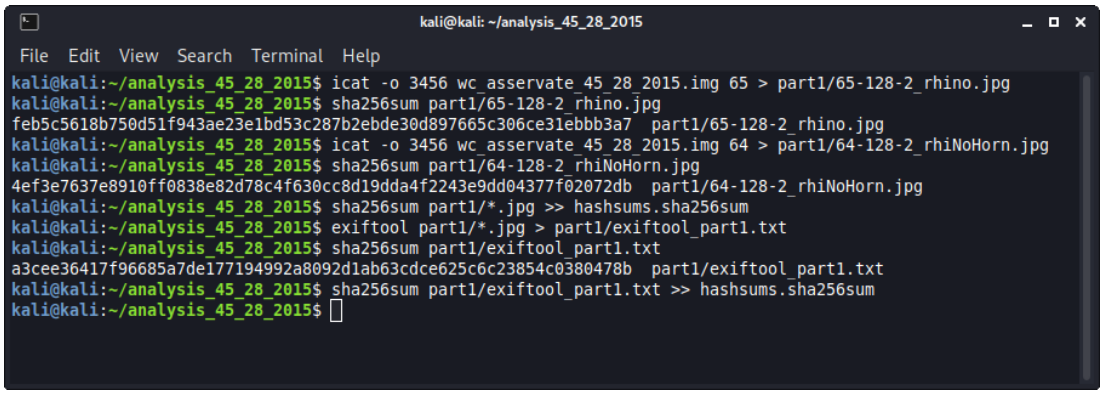

Figure 21: Cutting the two regular files from the *NTFS* file system and extracting their *exif* data.

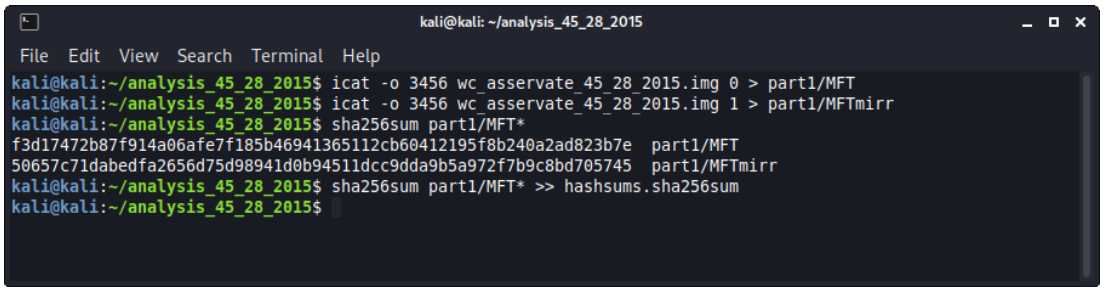

Figure 22: Cutting *MFT* meta file and its mirror from the image.

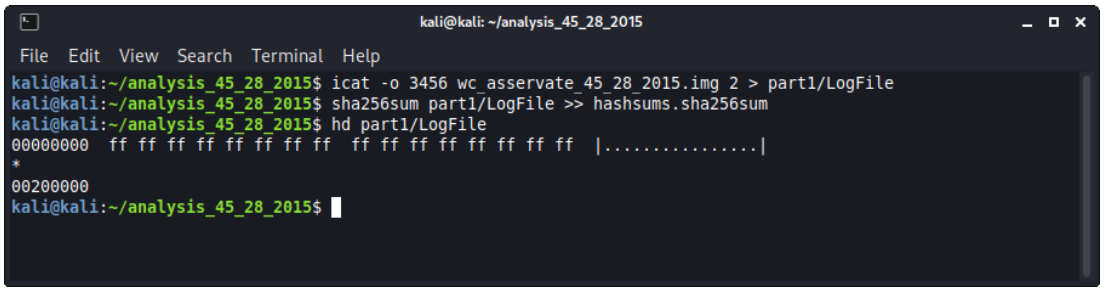

Figure 23: Extraction and analysis of the *LogFile*.

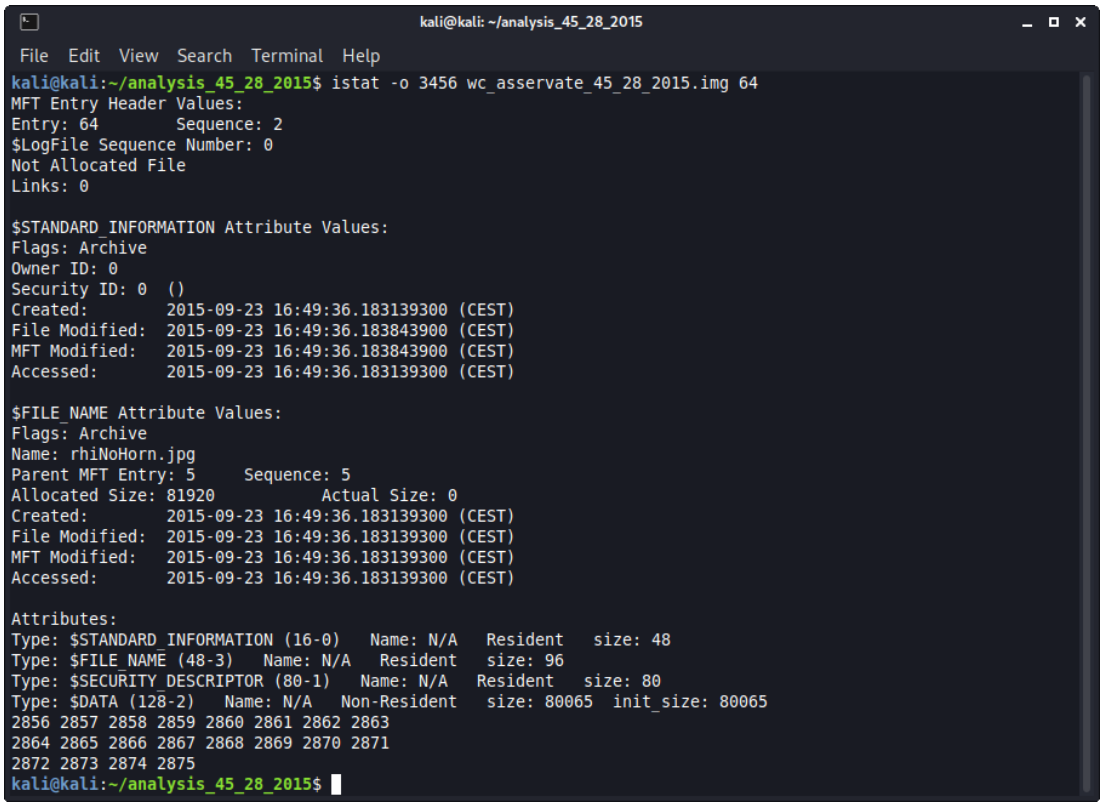

Figure 24: Metadata of file with INode 64.

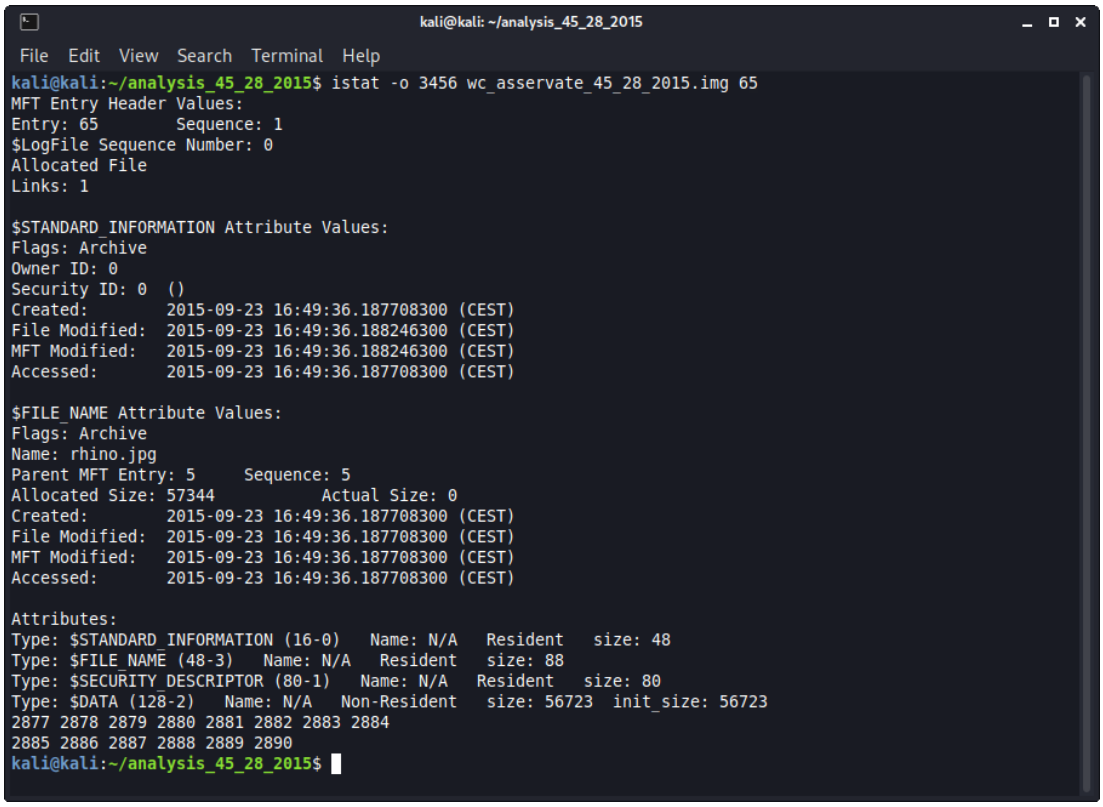

Figure 25: Metadata of file with INode 65.

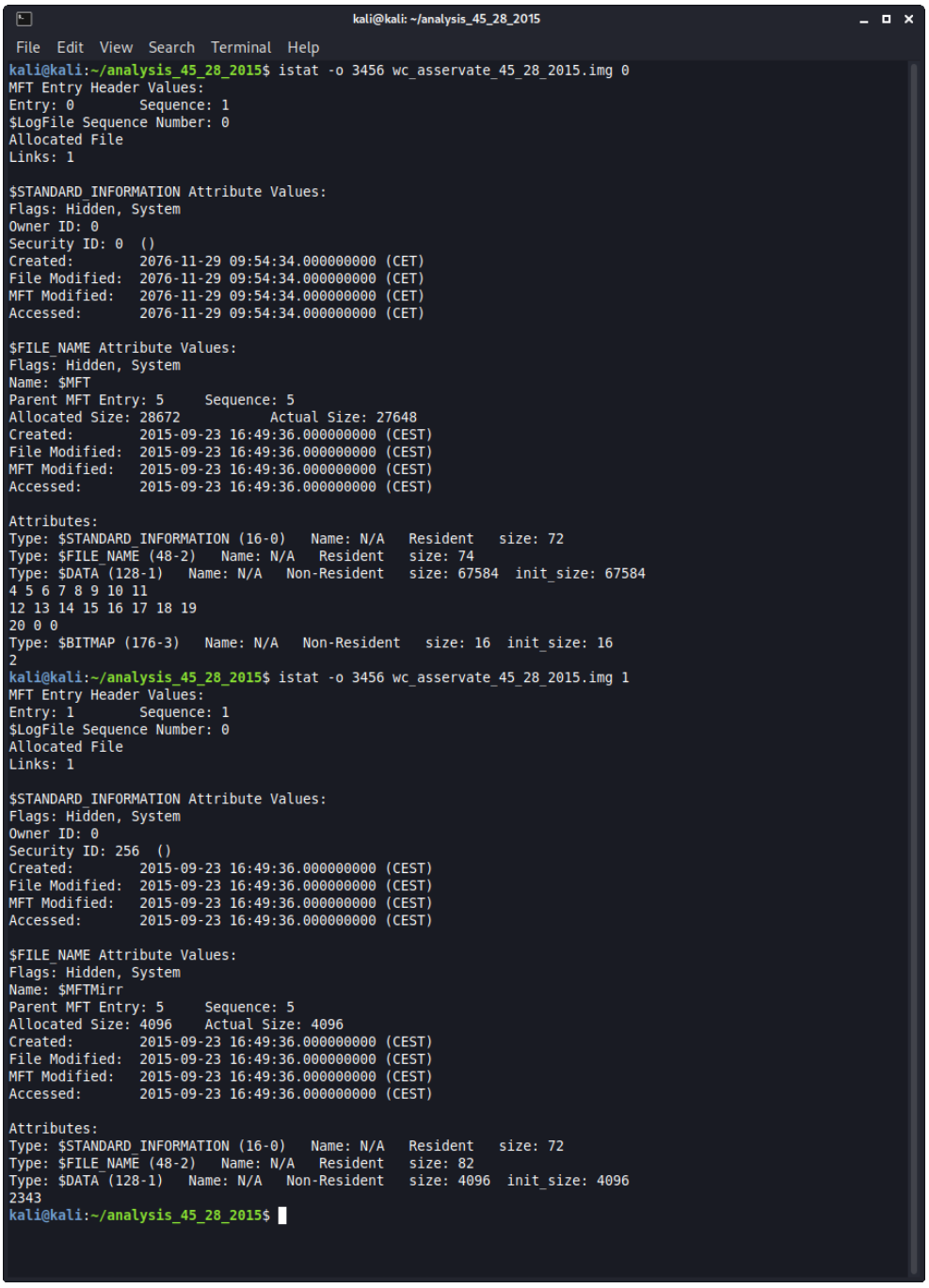

Figure 26: Metadata of bot *MFT* files.

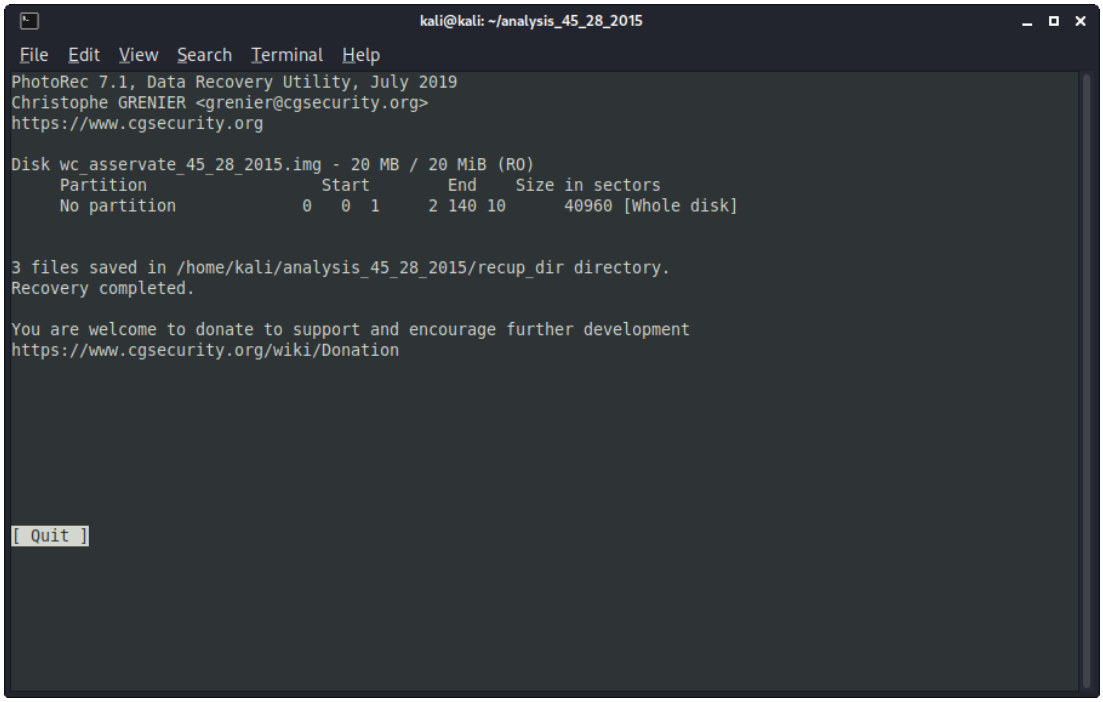

Figure 27: *Photorec* finds three images when carving the exhibit.

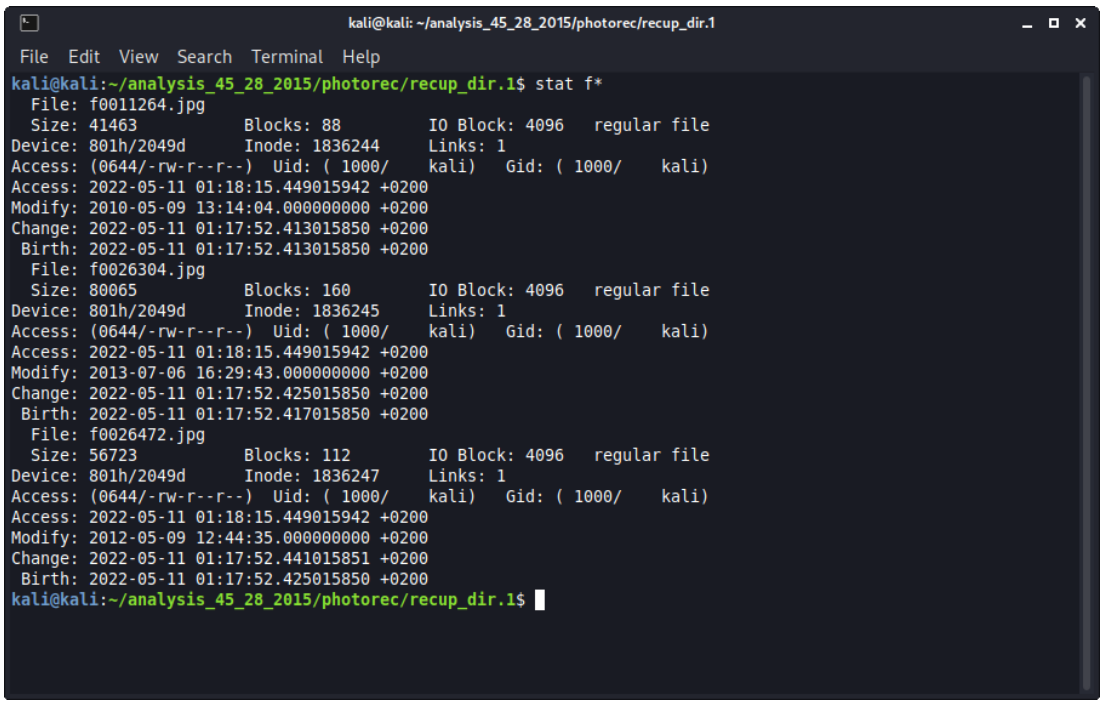

Figure 28: Result of using *stat* on the pictures extracted by *photorec*.

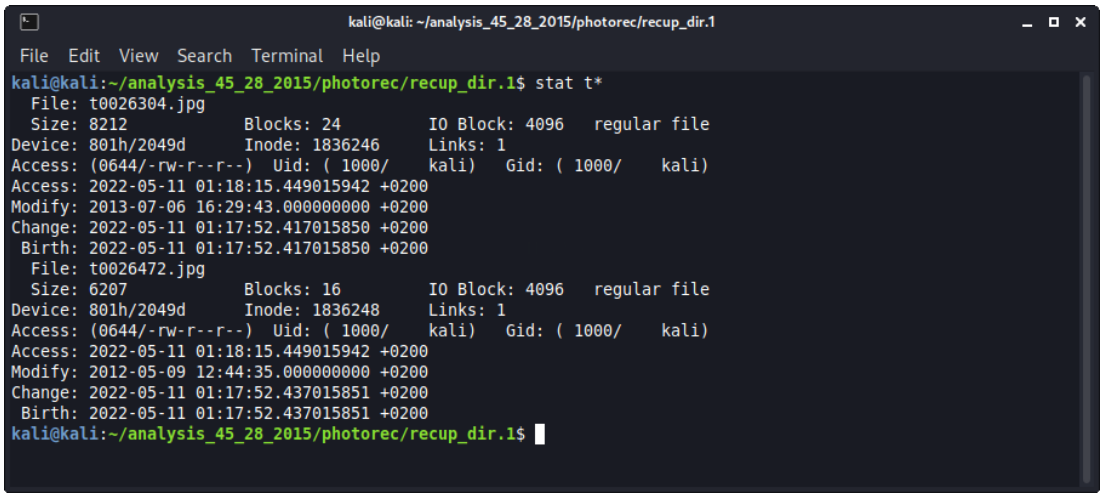

Figure 29: Result of using *stat* on the thumbnails extracted by *photorec*.

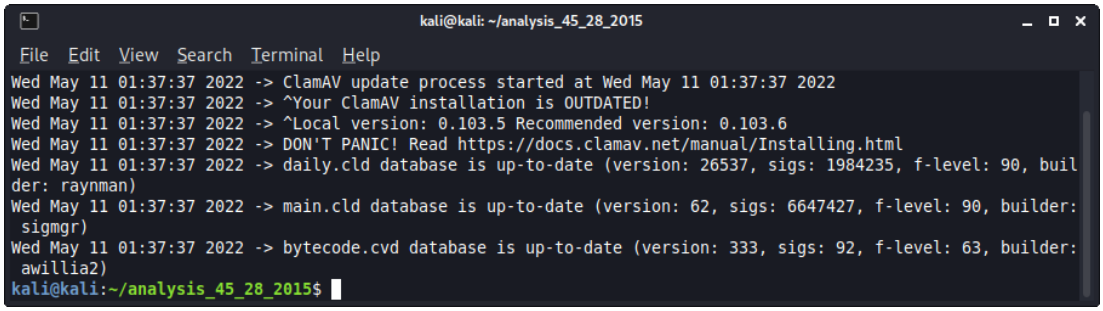

Figure 30: Update of antivirus database.

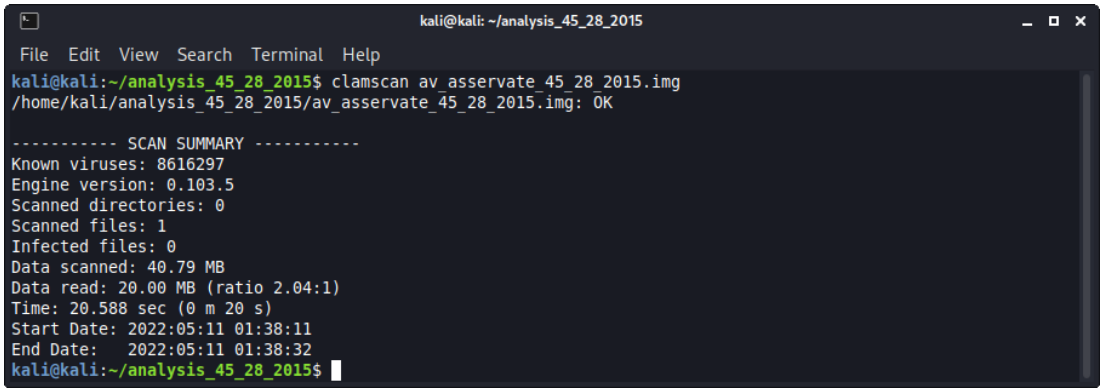

Figure 31: Scan of the exhibit for malware.

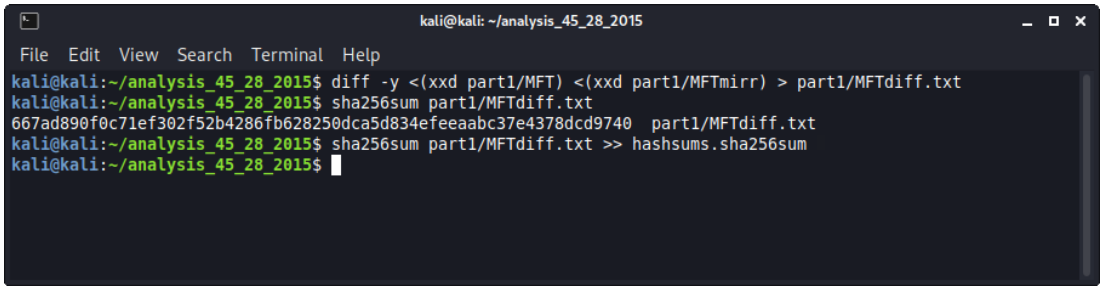

Figure 32: Comparing *MFT* and its mirror file.

4.4 Logfiles

Listing 1: Output of *exiftool* when analyzing the image recovered through *testdisk*.

```
1  ExifTool Version Number          : 12.41
2  File Name                        : rhino.jpg
3  Directory                        : testdisk
4  File Size                        : 55 KiB
5  File Modification Date/Time      : 2015:09:23 16:49:36+02:00
6  File Access Date/Time            : 2022:05:11 01:13:48+02:00
7  File Inode Change Date/Time      : 2022:05:11 01:13:40+02:00
8  File Permissions                 : -rw-r--r--
9  File Type                        : JPEG
10 File Type Extension              : jpg
11 MIME Type                        : image/jpeg
12 Exif Byte Order                  : Big-endian (Motorola, MM)
13 Subfile Type                     : Reduced-resolution image
14 Compression                      : JPEG (old-style)
15 Photometric Interpretation       : YCbCr
16 Orientation                      : Horizontal (normal)
17 Samples Per Pixel                : 3
18 X Resolution                     : 72
19 Y Resolution                     : 72
20 Resolution Unit                  : inches
21 Modify Date                      : 2012:03:30 12:44:35
22 Y Cb Cr Positioning              : Centered
23 Exif Version                     : 0232
24 Date/Time Original               : 2012:05:09 12:44:35
25 Components Configuration         : Y, Cb, Cr, -
26 Flashpix Version                 : 0100
27 Color Space                      : sRGB
28 Thumbnail Offset                 : 422
29 Thumbnail Length                 : 6207
30 Current IPTC Digest              : 0d21c8be1360931d84647ac8e4ff3d0e
31 Date Created                     : 2012:03:30
32 Time Created                     : 12:44:35-12:44
33 Application Record Version       : 4
34 XMP Toolkit                      : Image::ExifTool 12.41
35 Owner                            : Sian Tiley-Nel
36 Comment                          : File source: https://commons.wikimedia.org/wiki/
       File:UP_rhino.JPG
37 Image Width                      : 640
38 Image Height                     : 457
39 Encoding Process                 : Progressive DCT, Huffman coding
40 Bits Per Sample                  : 8
41 Color Components                 : 3
42 Y Cb Cr Sub Sampling             : YCbCr4:4:4 (1 1)
43 Image Size                       : 640x457
44 Megapixels                       : 0.292
45 Thumbnail Image                  : (Binary data 6207 bytes, use -b option to extract)
46 Date/Time Created                : 2012:03:30 12:44:35-12:44
```

Listing 2: Output of *exiftool* when analyzing the image recovered through *photorec*.

```
1  ======== photorec/recup_dir.1/f0011264.jpg
2  ExifTool Version Number          : 12.41
3  File Name                        : f0011264.jpg
4  Directory                        : photorec/recup_dir.1
5  File Size                        : 40 KiB
6  File Modification Date/Time      : 2010:05:09 13:14:04+02:00
```

```
File Access Date/Time           : 2022:05:11 01:18:15+02:00
File Inode Change Date/Time     : 2022:05:11 01:17:52+02:00
File Permissions                : -rw-r--r--
File Type                       : JPEG
File Type Extension             : jpg
MIME Type                       : image/jpeg
Exif Byte Order                 : Big-endian (Motorola, MM)
X Resolution                    : 1
Y Resolution                    : 1
Resolution Unit                 : None
Modify Date                     : 2010:05:09 13:14:04
Y Cb Cr Positioning             : Centered
Profile Copyright               : Copyright (c) 1998 Hewlett-Packard Company
Current IPTC Digest             : 2fa2203a6b34e28e14f3f53187a402de
Envelope Record Version         : 4
Coded Character Set             : UTF8
Application Record Version      : 4
Credit                          : Flickr - CC BY 2.0
Copyright Notice                : Flickr - CC BY 2.0
XMP Toolkit                     : Image::ExifTool 12.41
Owner                           : John Mountjoy
Image Width                     : 400
Image Height                    : 267
Encoding Process                : Baseline DCT, Huffman coding
Bits Per Sample                 : 8
Color Components                : 3
Y Cb Cr Sub Sampling            : YCbCr4:2:0 (2 2)
Image Size                      : 400x267
Megapixels                      : 0.107
======== photorec/recup_dir.1/f0026304.jpg
ExifTool Version Number         : 12.41
File Name                       : f0026304.jpg
Directory                       : photorec/recup_dir.1
File Size                       : 78 KiB
File Modification Date/Time     : 2013:07:06 16:29:43+02:00
File Access Date/Time           : 2022:05:11 01:18:15+02:00
File Inode Change Date/Time     : 2022:05:11 01:17:52+02:00
File Permissions                : -rw-r--r--
File Type                       : JPEG
File Type Extension             : jpg
MIME Type                       : image/jpeg
Exif Byte Order                 : Big-endian (Motorola, MM)
Subfile Type                    : Reduced-resolution image
Compression                     : JPEG (old-style)
Make                            : Canon
Camera Model Name               : CANON EOS-1D Mark III
Orientation                     : Horizontal (normal)
X Resolution                    : 300
Y Resolution                    : 300
Resolution Unit                 : inches
Modify Date                     : 2013:07:06 16:29:43
Y Cb Cr Positioning             : Centered
Exposure Time                   : 1/640
F Number                        : 5.6
Exposure Program                : Aperture-priority AE
ISO                             : 800
Exif Version                    : 0221
Date/Time Original              : 2013:07:06 16:29:43
Create Date                     : 2013:07:06 16:29:43
Components Configuration        : Y, Cb, Cr, -
```

```
Shutter Speed Value             : 1/664
Aperture Value                  : 5.7
Exposure Compensation           : 0
Focal Length                    : 300.0 mm
User Comment                    :
Sub Sec Time                    : 00
Sub Sec Time Original           : 00
Sub Sec Time Digitized          : 00
Flashpix Version                : 0100
Color Space                     : sRGB
Exif Image Width                : 4527
Exif Image Height               : 3018
Focal Plane X Resolution        : 3512.195122
Focal Plane Y Resolution        : 3521.73913
Focal Plane Resolution Unit     : inches
Custom Rendered                 : Normal
Exposure Mode                   : Auto
White Balance                   : Auto
Scene Capture Type              : Standard
Contrast                        : Normal
Saturation                      : Normal
Sharpness                       : Hard
Owner Name                      : Holly Occhipinti
Serial Number                   : 527065
Lens Model                      : EF100-400mm f/4.5-5.6L IS USM
GPS Version ID                  : 2.2.0.0
Thumbnail Offset                : 940
Thumbnail Length                : 8212
Current IPTC Digest             : 5d2e2a771f9e439b0608f1c728753acb
Application Record Version      : 2
Object Name                     : Baby Rhinoceros
Keywords                        : baby, rhino, rhinoceros, animal, africa, wildlife,
    mammal, park, calf, wild, safari, big, endangered, reserve, young, african, south
    , tourism, herbivore, nature, dangerous, five, grass, big5, savanna, white,
    strong, bush, large, face, watchful, massive, lip, hide, ears, eyes, small, game,
     national, conservation, grassland, fauna, cute, feet, baby, rhino, rhinoceros,
    animal, africa, wildlife, mammal, park, calf, wild, safari, big, endangered,
    reserve, young, african, south, tourism, herbivore, nature, dangerous, five,
    grass, big5, savanna, white, strong, bush, large, face, watchful, massive, lip,
    hide, ears, eyes, small, game, national, conservation, grassland, fauna, cute,
    feet
Country-Primary Location Name   : South Africa
Credit                          : Holly Occhipinti - Flickr
Copyright Notice                : Holly Occhipinti - Flickr
Caption-Abstract                : Cute baby white rhino with large feet
XMP Toolkit                     : Image::ExifTool 7.30
Description                     : Cute baby white rhino with large feet
Subject                         : baby, rhino, rhinoceros, animal, africa, wildlife,
    mammal, park, calf, wild, safari, big, endangered, reserve, young, african, south
    , tourism, herbivore, nature, dangerous, five, grass, big5, savanna, white,
    strong, bush, large, face, watchful, massive, lip, hide, ears, eyes, small, game,
     national, conservation, grassland, fauna, baby, rhino, rhinoceros, animal,
    africa, wildlife, mammal, park, calf, wild, safari, big, endangered, reserve,
    young, african, south, tourism, herbivore, nature, dangerous, five, grass, big5,
    savanna, white, strong, bush, large, face, watchful, massive, lip, hide, ears,
    eyes, small, game, national, conservation, grassland, fauna, cute, feet
Title                           : Baby Rhinoceros
Flash Fired                     : True
Flash Function                  : False
Flash Mode                      : On
```

```
Flash Red Eye Mode                : False
Flash Return                      : No return detection
Sequence Number                   : 0
Color Temperature                 : 5200
Tone Curve                        : Standard
Image Width                       : 650
Image Height                      : 434
Encoding Process                  : Progressive DCT, Huffman coding
Bits Per Sample                   : 8
Color Components                  : 3
Y Cb Cr Sub Sampling              : YCbCr4:4:4 (1 1)
Aperture                          : 5.6
Image Size                        : 650x434
Megapixels                        : 0.282
Scale Factor To 35 mm Equivalent: 1.1
Shutter Speed                     : 1/640
Create Date                       : 2013:07:06 16:29:43.00
Date/Time Original                : 2013:07:06 16:29:43.00
Modify Date                       : 2013:07:06 16:29:43.00
Thumbnail Image                   : (Binary data 8212 bytes, use -b option to extract)
Flash                             : On, Fired
Circle Of Confusion               : 0.027 mm
Field Of View                     : 6.2 deg
Focal Length                      : 300.0 mm (35 mm equivalent: 330.2 mm)
Hyperfocal Distance               : 588.66 m
Light Value                       : 11.3
Lens ID                           : EF100-400mm f/4.5-5.6L IS USM
======== photorec/recup_dir.1/f0026472.jpg
ExifTool Version Number           : 12.41
File Name                         : f0026472.jpg
Directory                         : photorec/recup_dir.1
File Size                         : 55 KiB
File Modification Date/Time       : 2012:05:09 12:44:35+02:00
File Access Date/Time             : 2022:05:11 01:18:15+02:00
File Inode Change Date/Time       : 2022:05:11 01:17:52+02:00
File Permissions                  : -rw-r--r--
File Type                         : JPEG
File Type Extension               : jpg
MIME Type                         : image/jpeg
Exif Byte Order                   : Big-endian (Motorola, MM)
Subfile Type                      : Reduced-resolution image
Compression                       : JPEG (old-style)
Photometric Interpretation        : YCbCr
Orientation                       : Horizontal (normal)
Samples Per Pixel                 : 3
X Resolution                      : 72
Y Resolution                      : 72
Resolution Unit                   : inches
Modify Date                       : 2012:03:30 12:44:35
Y Cb Cr Positioning               : Centered
Exif Version                      : 0232
Date/Time Original                : 2012:05:09 12:44:35
Components Configuration          : Y, Cb, Cr, -
Flashpix Version                  : 0100
Color Space                       : sRGB
Thumbnail Offset                  : 422
Thumbnail Length                  : 6207
Current IPTC Digest               : 0d21c8be1360931d84647ac8e4ff3d0e
Date Created                      : 2012:03:30
Time Created                      : 12:44:35-12:44
```

```
Application Record Version      : 4
XMP Toolkit                     : Image::ExifTool 12.41
Owner                           : Sian Tiley-Nel
Comment                         : File source: https://commons.wikimedia.org/wiki/
    File:UP_rhino.JPG
Image Width                     : 640
Image Height                    : 457
Encoding Process                : Progressive DCT, Huffman coding
Bits Per Sample                 : 8
Color Components                : 3
Y Cb Cr Sub Sampling            : YCbCr4:4:4 (1 1)
Image Size                      : 640x457
Megapixels                      : 0.292
Thumbnail Image                 : (Binary data 6207 bytes, use -b option to extract)
Date/Time Created               : 2012:03:30 12:44:35-12:44
======== photorec/recup_dir.1/t0026304.jpg
ExifTool Version Number         : 12.41
File Name                       : t0026304.jpg
Directory                       : photorec/recup_dir.1
File Size                       : 8.0 KiB
File Modification Date/Time     : 2013:07:06 16:29:43+02:00
File Access Date/Time           : 2022:05:11 01:18:15+02:00
File Inode Change Date/Time     : 2022:05:11 01:17:52+02:00
File Permissions                : -rw-r--r--
File Type                       : JPEG
File Type Extension             : jpg
MIME Type                       : image/jpeg
JFIF Version                    : 1.01
Resolution Unit                 : None
X Resolution                    : 1
Y Resolution                    : 1
Image Width                     : 256
Image Height                    : 170
Encoding Process                : Baseline DCT, Huffman coding
Bits Per Sample                 : 8
Color Components                : 3
Y Cb Cr Sub Sampling            : YCbCr4:2:0 (2 2)
Image Size                      : 256x170
Megapixels                      : 0.044
======== photorec/recup_dir.1/t0026472.jpg
ExifTool Version Number         : 12.41
File Name                       : t0026472.jpg
Directory                       : photorec/recup_dir.1
File Size                       : 6.1 KiB
File Modification Date/Time     : 2012:05:09 12:44:35+02:00
File Access Date/Time           : 2022:05:11 01:18:15+02:00
File Inode Change Date/Time     : 2022:05:11 01:17:52+02:00
File Permissions                : -rw-r--r--
File Type                       : JPEG
File Type Extension             : jpg
MIME Type                       : image/jpeg
JFIF Version                    : 1.01
Resolution Unit                 : None
X Resolution                    : 1
Y Resolution                    : 1
Image Width                     : 256
Image Height                    : 182
Encoding Process                : Baseline DCT, Huffman coding
Bits Per Sample                 : 8
Color Components                : 3
```

```
Y Cb Cr Sub Sampling            : YCbCr4:2:0 (2 2)
Image Size                      : 256x182
Megapixels                      : 0.047
    5 image files read
```

Listing 3: Output of *exiftool* when analyzing the image recovered from the hard drive disks file system.

```
======== part1/64-128-2_rhiNoHorn.jpg
ExifTool Version Number         : 12.41
File Name                       : 64-128-2_rhiNoHorn.jpg
Directory                       : part1
File Size                       : 78 KiB
File Modification Date/Time     : 2022:05:11 01:31:37+02:00
File Access Date/Time           : 2022:05:11 01:31:40+02:00
File Inode Change Date/Time     : 2022:05:11 01:31:37+02:00
File Permissions                : -rw-r--r--
File Type                       : JPEG
File Type Extension             : jpg
MIME Type                       : image/jpeg
Exif Byte Order                 : Big-endian (Motorola, MM)
Subfile Type                    : Reduced-resolution image
Compression                     : JPEG (old-style)
Make                            : Canon
Camera Model Name               : CANON EOS-1D Mark III
Orientation                     : Horizontal (normal)
X Resolution                    : 300
Y Resolution                    : 300
Resolution Unit                 : inches
Modify Date                     : 2013:07:06 16:29:43
Y Cb Cr Positioning             : Centered
Exposure Time                   : 1/640
F Number                        : 5.6
Exposure Program                : Aperture-priority AE
ISO                             : 800
Exif Version                    : 0221
Date/Time Original              : 2013:07:06 16:29:43
Create Date                     : 2013:07:06 16:29:43
Components Configuration        : Y, Cb, Cr, -
Shutter Speed Value             : 1/664
Aperture Value                  : 5.7
Exposure Compensation           : 0
Focal Length                    : 300.0 mm
User Comment                    :
Sub Sec Time                    : 00
Sub Sec Time Original           : 00
Sub Sec Time Digitized          : 00
Flashpix Version                : 0100
Color Space                     : sRGB
Exif Image Width                : 4527
Exif Image Height               : 3018
Focal Plane X Resolution        : 3512.195122
Focal Plane Y Resolution        : 3521.73913
Focal Plane Resolution Unit     : inches
Custom Rendered                 : Normal
Exposure Mode                   : Auto
White Balance                   : Auto
Scene Capture Type              : Standard
Contrast                        : Normal
Saturation                      : Normal
```

```
53 Sharpness                       : Hard
54 Owner Name                      : Holly Occhipinti
55 Serial Number                   : 527065
56 Lens Model                      : EF100-400mm f/4.5-5.6L IS USM
57 GPS Version ID                  : 2.2.0.0
58 Thumbnail Offset                : 940
59 Thumbnail Length                : 8212
60 Current IPTC Digest             : 5d2e2a771f9e439b0608f1c728753acb
61 Application Record Version      : 2
62 Object Name                     : Baby Rhinoceros
63 Keywords                        : baby, rhino, rhinoceros, animal, africa, wildlife,
       mammal, park, calf, wild, safari, big, endangered, reserve, young, african, south
       , tourism, herbivore, nature, dangerous, five, grass, big5, savanna, white,
       strong, bush, large, face, watchful, massive, lip, hide, ears, eyes, small, game,
        national, conservation, grassland, fauna, cute, feet, baby, rhino, rhinoceros,
       animal, africa, wildlife, mammal, park, calf, wild, safari, big, endangered,
       reserve, young, african, south, tourism, herbivore, nature, dangerous, five,
       grass, big5, savanna, white, strong, bush, large, face, watchful, massive, lip,
       hide, ears, eyes, small, game, national, conservation, grassland, fauna, cute,
       feet
64 Country-Primary Location Name   : South Africa
65 Credit                          : Holly Occhipinti - Flickr
66 Copyright Notice                : Holly Occhipinti - Flickr
67 Caption-Abstract                : Cute baby white rhino with large feet
68 XMP Toolkit                     : Image::ExifTool 7.30
69 Description                     : Cute baby white rhino with large feet
70 Subject                         : baby, rhino, rhinoceros, animal, africa, wildlife,
       mammal, park, calf, wild, safari, big, endangered, reserve, young, african, south
       , tourism, herbivore, nature, dangerous, five, grass, big5, savanna, white,
       strong, bush, large, face, watchful, massive, lip, hide, ears, eyes, small, game,
        national, conservation, grassland, fauna, baby, rhino, rhinoceros, animal,
       africa, wildlife, mammal, park, calf, wild, safari, big, endangered, reserve,
       young, african, south, tourism, herbivore, nature, dangerous, five, grass, big5,
       savanna, white, strong, bush, large, face, watchful, massive, lip, hide, ears,
       eyes, small, game, national, conservation, grassland, fauna, cute, feet
71 Title                           : Baby Rhinoceros
72 Flash Fired                     : True
73 Flash Function                  : False
74 Flash Mode                      : On
75 Flash Red Eye Mode              : False
76 Flash Return                    : No return detection
77 Sequence Number                 : 0
78 Color Temperature               : 5200
79 Tone Curve                      : Standard
80 Image Width                     : 650
81 Image Height                    : 434
82 Encoding Process                : Progressive DCT, Huffman coding
83 Bits Per Sample                 : 8
84 Color Components                : 3
85 Y Cb Cr Sub Sampling            : YCbCr4:4:4 (1 1)
86 Aperture                        : 5.6
87 Image Size                      : 650x434
88 Megapixels                      : 0.282
89 Scale Factor To 35 mm Equivalent: 1.1
90 Shutter Speed                   : 1/640
91 Create Date                     : 2013:07:06 16:29:43.00
92 Date/Time Original              : 2013:07:06 16:29:43.00
93 Modify Date                     : 2013:07:06 16:29:43.00
94 Thumbnail Image                 : (Binary data 8212 bytes, use -b option to extract)
95 Flash                           : On, Fired
```

```
Circle Of Confusion             : 0.027 mm
Field Of View                   : 6.2 deg
Focal Length                    : 300.0 mm (35 mm equivalent: 330.2 mm)
Hyperfocal Distance             : 588.66 m
Light Value                     : 11.3
Lens ID                         : EF100-400mm f/4.5-5.6L IS USM
======== part1/65-128-2_rhino.jpg
ExifTool Version Number         : 12.41
File Name                       : 65-128-2_rhino.jpg
Directory                       : part1
File Size                       : 55 KiB
File Modification Date/Time     : 2022:05:11 01:31:34+02:00
File Access Date/Time           : 2022:05:11 01:31:35+02:00
File Inode Change Date/Time     : 2022:05:11 01:31:34+02:00
File Permissions                : -rw-r--r--
File Type                       : JPEG
File Type Extension             : jpg
MIME Type                       : image/jpeg
Exif Byte Order                 : Big-endian (Motorola, MM)
Subfile Type                    : Reduced-resolution image
Compression                     : JPEG (old-style)
Photometric Interpretation      : YCbCr
Orientation                     : Horizontal (normal)
Samples Per Pixel               : 3
X Resolution                    : 72
Y Resolution                    : 72
Resolution Unit                 : inches
Modify Date                     : 2012:03:30 12:44:35
Y Cb Cr Positioning             : Centered
Exif Version                    : 0232
Date/Time Original              : 2012:05:09 12:44:35
Components Configuration        : Y, Cb, Cr, -
Flashpix Version                : 0100
Color Space                     : sRGB
Thumbnail Offset                : 422
Thumbnail Length                : 6207
Current IPTC Digest             : 0d21c8be1360931d84647ac8e4ff3d0e
Date Created                    : 2012:03:30
Time Created                    : 12:44:35-12:44
Application Record Version      : 4
XMP Toolkit                     : Image::ExifTool 12.41
Owner                           : Sian Tiley-Nel
Comment                         : File source: https://commons.wikimedia.org/wiki/
    File:UP_rhino.JPG
Image Width                     : 640
Image Height                    : 457
Encoding Process                : Progressive DCT, Huffman coding
Bits Per Sample                 : 8
Color Components                : 3
Y Cb Cr Sub Sampling            : YCbCr4:4:4 (1 1)
Image Size                      : 640x457
Megapixels                      : 0.292
Thumbnail Image                 : (Binary data 6207 bytes, use -b option to extract)
Date/Time Created               : 2012:03:30 12:44:35-12:44
    2 image files read
```

Listing 4: Listing of all files on the file system with their respective metadata. Timestamp in CEST. The metadata is in the following order: file_type inode file_name mod_time acc_time chg_time

cre_time size uid gid.

```
1  r/r 4-128-1:     $AttrDef         2015-09-23 16:49:36 (CEST)       2015-09-23 16:49:36 (
       CEST)       2015-09-23 16:49:36 (CEST)       2015-09-23 16:49:36 (CEST)       2560
            0        48
2  r/r 8-128-2:     $BadClus         2015-09-23 16:49:36 (CEST)       2015-09-23 16:49:36 (
       CEST)       2015-09-23 16:49:36 (CEST)       2015-09-23 16:49:36 (CEST)       0
              0        0
3  r/r 8-128-1:     $BadClus:$Bad    2015-09-23 16:49:36 (CEST)       2015-09-23 16:49:36 (
       CEST)       2015-09-23 16:49:36 (CEST)       2015-09-23 16:49:36 (CEST)
       19197952         0        0
4  r/r 6-128-1:     $Bitmap 2015-09-23 16:49:36 (CEST)       2015-09-23 16:49:36 (CEST)
            2015-09-23 16:49:36 (CEST)       2015-09-23 16:49:36 (CEST)       592      0
             0
5  r/r 7-128-1:     $Boot    2015-09-23 16:49:36 (CEST)       2015-09-23 16:49:36 (CEST)
            2015-09-23 16:49:36 (CEST)       2015-09-23 16:49:36 (CEST)       8192     0
             48
6  d/d 11-144-2:    $Extend 2015-09-23 16:49:36 (CEST)       2015-09-23 16:49:36 (CEST)
            2015-09-23 16:49:36 (CEST)       2015-09-23 16:49:36 (CEST)       344      0
             0
7  + r/r 25-144-2: $ObjId:$O        2015-09-23 16:49:36 (CEST)       2015-09-23 16:49:36 (
       CEST)       2015-09-23 16:49:36 (CEST)       2015-09-23 16:49:36 (CEST)       48
              0        0
8  + r/r 24-144-3: $Quota:$O        2015-09-23 16:49:36 (CEST)       2015-09-23 16:49:36 (
       CEST)       2015-09-23 16:49:36 (CEST)       2015-09-23 16:49:36 (CEST)       88
              0        0
9  + r/r 24-144-2: $Quota:$Q        2015-09-23 16:49:36 (CEST)       2015-09-23 16:49:36 (
       CEST)       2015-09-23 16:49:36 (CEST)       2015-09-23 16:49:36 (CEST)       208
            0        0
10 + r/r 26-144-2: $Reparse:$R      2015-09-23 16:49:36 (CEST)       2015-09-23 16:49:36 (
       CEST)       2015-09-23 16:49:36 (CEST)       2015-09-23 16:49:36 (CEST)       48
              0        0
11 r/r 2-128-1:     $LogFile         2015-09-23 16:49:36 (CEST)       2015-09-23 16:49:36 (
       CEST)       2015-09-23 16:49:36 (CEST)       2015-09-23 16:49:36 (CEST)
       2097152 0        0
12 r/r 0-128-1:     $MFT     2076-11-29 09:54:34 (CET)        2076-11-29 09:54:34 (CET)
            2076-11-29 09:54:34 (CET)        2076-11-29 09:54:34 (CET)        67584    0
             0
13 r/r 1-128-1:     $MFTMirr         2015-09-23 16:49:36 (CEST)       2015-09-23 16:49:36 (
       CEST)       2015-09-23 16:49:36 (CEST)       2015-09-23 16:49:36 (CEST)       4096
            0        0
14 r/r 9-128-2:     $Secure:$SDS     2015-09-23 16:49:36 (CEST)       2015-09-23 16:49:36 (
       CEST)       2015-09-23 16:49:36 (CEST)       2015-09-23 16:49:36 (CEST)       262396
          0        0
15 r/r 9-144-3:     $Secure:$SDH     2015-09-23 16:49:36 (CEST)       2015-09-23 16:49:36 (
       CEST)       2015-09-23 16:49:36 (CEST)       2015-09-23 16:49:36 (CEST)       144
              0        0
16 r/r 9-144-4:     $Secure:$SII     2015-09-23 16:49:36 (CEST)       2015-09-23 16:49:36 (
       CEST)       2015-09-23 16:49:36 (CEST)       2015-09-23 16:49:36 (CEST)       128
              0        0
17 r/r 10-128-1:    $UpCase 2015-09-23 16:49:36 (CEST)       2015-09-23 16:49:36 (CEST)
            2015-09-23 16:49:36 (CEST)       2015-09-23 16:49:36 (CEST)       131072   0
             0
18 r/r 10-128-2:    $UpCase:$Info    2015-09-23 16:49:36 (CEST)       2015-09-23 16:49:36 (
       CEST)       2015-09-23 16:49:36 (CEST)       2015-09-23 16:49:36 (CEST)       32
              0        0
19 r/r 3-128-3:     $Volume 2015-09-23 16:49:36 (CEST)       2015-09-23 16:49:36 (CEST)
            2015-09-23 16:49:36 (CEST)       2015-09-23 16:49:36 (CEST)       0        0
             48
20 r/r 65-128-2:    rhino.jpg        2015-09-23 16:49:36 (CEST)       2015-09-23 16:49:36 (
       CEST)       2015-09-23 16:49:36 (CEST)       2015-09-23 16:49:36 (CEST)       56723
```

```
          0        48
21  r/- * 0:          rhiNoHorn.jpg    0000-00-00 00:00:00 (UTC)        0000-00-00 00:00:00 (
        UTC)        0000-00-00 00:00:00 (UTC)        0000-00-00 00:00:00 (UTC)        0
                0        0
22  -/r * 64-128-2: rhiNoHorn.jpg    2015-09-23 16:49:36 (CEST)       2015-09-23 16:49:36 (
        CEST)       2015-09-23 16:49:36 (CEST)       2015-09-23 16:49:36 (CEST)       80065
          0        48
23  V/V 66: $OrphanFiles     0000-00-00 00:00:00 (UTC)        0000-00-00 00:00:00 (UTC)
                0000-00-00 00:00:00 (UTC)        0000-00-00 00:00:00 (UTC)        0        0
                0
24  + -/r * 16:       OrphanFile-16    2015-09-23 16:49:36 (CEST)       2015-09-23 16:49:36 (
        CEST)       2015-09-23 16:49:36 (CEST)       2015-09-23 16:49:36 (CEST)       0
                0        4294967295
25  + -/r * 17:       OrphanFile-17    2015-09-23 16:49:36 (CEST)       2015-09-23 16:49:36 (
        CEST)       2015-09-23 16:49:36 (CEST)       2015-09-23 16:49:36 (CEST)       0
                0        4294967295
26  + -/r * 18:       OrphanFile-18    2015-09-23 16:49:36 (CEST)       2015-09-23 16:49:36 (
        CEST)       2015-09-23 16:49:36 (CEST)       2015-09-23 16:49:36 (CEST)       0
                0        4294967295
27  + -/r * 19:       OrphanFile-19    2015-09-23 16:49:36 (CEST)       2015-09-23 16:49:36 (
        CEST)       2015-09-23 16:49:36 (CEST)       2015-09-23 16:49:36 (CEST)       0
                0        4294967295
28  + -/r * 20:       OrphanFile-20    2015-09-23 16:49:36 (CEST)       2015-09-23 16:49:36 (
        CEST)       2015-09-23 16:49:36 (CEST)       2015-09-23 16:49:36 (CEST)       0
                0        4294967295
29  + -/r * 21:       OrphanFile-21    2015-09-23 16:49:36 (CEST)       2015-09-23 16:49:36 (
        CEST)       2015-09-23 16:49:36 (CEST)       2015-09-23 16:49:36 (CEST)       0
                0        4294967295
30  + -/r * 22:       OrphanFile-22    2015-09-23 16:49:36 (CEST)       2015-09-23 16:49:36 (
        CEST)       2015-09-23 16:49:36 (CEST)       2015-09-23 16:49:36 (CEST)       0
                0        4294967295
31  + -/r * 23:       OrphanFile-23    2015-09-23 16:49:36 (CEST)       2015-09-23 16:49:36 (
        CEST)       2015-09-23 16:49:36 (CEST)       2015-09-23 16:49:36 (CEST)       0
                0        4294967295
```

Listing 5: Comparison of the file system's *MFT* and *MFTmirr*.

```
1  The size of this file is too large for this apendix. If necessary it can be supplied
       later.
```