DFAa Report

xmikul69
Brno University of Technology
Brno, Česká republika

1. Introduction

The city of New Orleans passed a law in 2004 making possession of nine or more unique rhinoceros images a serious crime. The network administrator at the University of New Orleans recently alerted police when his instance of RHINOVORE flagged illegal rhino traffic. Evidence in the case includes a computer and USB key seized from one of the University's labs. Unfortunately, the computer had no hard drive.

2. Evidence Files

Files gathered for the investigation:

- RHINOUSB.dd
  - 248 MiB
  - MD5: 80348c58eec4c328ef1f7709adc56a54
- rhino.log
  - 3,1 MiB
  - MD5: c0d0093eb1664cd7b73f3a5225ae3f30
- rhino2.log
  - 286 kiB
  - MD5: cd21eaf4acfb50f71ffff857d7968341
- rhino3.log
  - 221 kiB
  - MD5: 7e29f9d67346df25faaf18efcd95fc30

3. Tools and Techniques

- data carving:
  - photorec 7.1
  - foremost 1.5.7
- packet papture analysis and data extraction from packet capture:
  - Wireshark 4.0.4
- file metadata analysis:
  - exiftool
- zip analysis:
  - UnZip 6.00
- zip password recovery:
  - bkcrack 1.5.0
  - John the Ripper 1.9.0
- steganography analysis:
  - steghide 0.5.1

4. Findings and Evidence

The suspects' computer seems to appear in capture files with IP addresses 137.30.120.39 and 137.30.123.234 and MAC address 00:03:93:CC:57:92.

It was attempted to recover encrypted contents of “contraband.zip” using tools bkcrack and John the Ripper, result being bkcrack unable to succeed with headers of image “f0106409.jpg” used as plaintext and John the Ripper did not recover passowrd of the archive in running time of two hours.

4.1. Disclosed Persons

- “*bighonkingrhino@hotmail.com*”, email address of suspect,
- “Jeremy”, from diary, not specified further,
- “John”
  - email address: “*hugerhinolover@hotmail.com*”
  - email display name: “Huge Lover”
- “George” / “Georgia”, signed below note left on server.
  - logged in as “gnome” from 137.30.120.40.

5. Timeline Reconstruction

Times of packet captures are in UTC, times within them as offset from beginning of capture.

- 26/04/2004 16:42:04 Packet capture rhino.log begins.
  - 6 s suspect logs in to webmail client on “hotmail.com” as “hugerhinolover@hotmail.com” from 137.30.122.253,
  - 1 min 28 s IMAP client received “*BYE Lost mailbox lock*” and after that reauthenticated with username “golden” and password “kinky!tang” and issued a “fetch” command for all messages in inbox,
  - 1 min 42 s log in as “gnome” with password “gnome123” to 137.30.120.40 via telnet, listing files and unsuccessfully attempting to change password,
  - 2 min 59 s log in FTP server on address 137.30.120.40 with username “gnome” and password “gnome123” from IP 137.30.122.253 and upload of file “rhino1.jpg”,
  - 3 min 15 s same log in as one above and upload of file “rhino3.jpg”,
  - 3 min 46 s periodic check of messages over IMAP,
  - 4 min 40 s 1st email sent from 137.30.122.253 via webmail client,
  - 4 min 51 s manually logged out of webmail,
  - 5 min 19 s log into hotmail web client as “hugerhinolover@hotmail.com” from 137.30.122.253,
  - 7 min 34 s 2nd email sent,
  - 7 min 59 s log in FTP server on address 137.30.120.40 with username “gnome” and password “gnome123” from IP 137.30.122.253 and upload of file “contraband.zip”,
  - 8 min 13 s attempt from 137.30.122.253 to guess telnet password for user “golden”
  - 8 min 51 s logged in as “gnome” and wrote note about attempted password guessing, signed at first “George” and changed to “Georgia”,
  - 12 min 30 s Packet capture rhino.log ends.
- 28/04/2004 15:50:22 Packet capture rhino2.log begins.
  - 7 s suspect visits “http://www.cs.uno.edu/~gnome”, “http://www.cs.uno.edu/~gnome/”,and downloads “rhino4.jpg” and (in 14th second) “rhino5.gif” from 137.30.123.234,
  - 18 s periodic check of messages over IMAP,
  - 43 s suspect visits “http://www.cs.uno.edu/~venkata/” and “/~venkata/2025/index.html” from 137.30.123.234. This does not seem to be connected to investigated activity,
  - 1 min 39 s Packet capture rhino2.log ends.
- 28/04/2004 15:50:26 Packet capture rhino3.log begins.
  - 0 s search query for “rhino.exe” on google.com from 137.30.123.234,

- 42 s downloaded “rhino.exe” from “www.cs.uno.edu/~gnome/rhino.exe”,
- 67 s periodic check of messages over IMAP,
- 1 min 6 s Packet capture rhino2.log ends.

5.1. Investigation Conclusions

5.1.1. Who provided the accused with a telnet/ftp account?

Jeremy, according to “f0335017_She_died_in_February_at_the_age_of_74.doc”:

“I need to change the password on the gnome account that Jeremy gave me”

5.1.2. What is the username/password associated with the account?

- Telnet/FTP:
  - cook.cs.uno.edu:
    - gnome / gnome123
- IMAP:
  - golden / kinky!tang

5.1.3. Which file transfers in the network traces are relevant to the case?

- rhino.log
  - TCP stream 60:
    - telnet
    - Source Address: 137.30.122.253
    - Destination Address: 137.30.120.40
    - commands issued:
      - logged in as gnome / gnome123
      - “ls -l”
      - “du -k”
      - attempt to change password to “gnome1234” and “gnome12345”, did fail with “Permission denied”
      - “logout”, which was not found, then “exit”
  - TCP stream 69:
    - FTP
    - Source Address: 137.30.122.253
    - Destination Address: 137.30.120.40
    - commands issued:
      - logged in as gnome / gnome123,
      - **uploaded “rhino1.jpg”**
  - TCP stream 72:
    - FTP
    - Source Address: 137.30.122.253
    - Destination Address: 137.30.120.40
    - commands issued:
      - logged in as gnome / gnome123,
      - **uploaded “rhino3.jpg”**
  - TCP stream 109:
    - HTTP
    - Source Address: 137.30.122.253

    - Destination Address: 64.4.43.250
    - POST to webmail client (only entries of relevance listed):
        - to: "*bighonkingrhino@hotmail.com*"
        - login: "*hugerhinolover*"
        - subject: "*New rhino pics*"
        - body:
          "*I just checked a few things on the gnome account on cook.cs.uno.edu. I'm about to upload some new rhino stuff.*

          Check it out.

          –John"
- TCP stream 286:
    - HTTP
    - Source Address: 137.30.122.253
    - Destination Address: 65.54.244.250
    - POST to webmail client (only entries of relevance listed):
        - to: "*hugerhinolover@hotmail.com*"
        - login: "*bighonkingrhino*"
        - subject: "*RE: New rhino pics*"
        - body:
          "*Dear John,*

          I'll check the account later for the rhino stuff. I'm tied up for the moment working on something in the lab.

          What's your social security number? I want to sign you up for a few Rhino Lovers magaz"
- TCP stream 305:
    - FTP
    - Source Address: 137.30.122.253
    - Destination Address: 137.30.120.40
    - commands issued:
        - logged in as gnome / gnome123,
        - **uploaded "contraband.zip"**
- TCP stream 318:
    - telnet
    - Source Address: 137.30.122.253
    - Destination Address: 137.30.120.40
    - commands issued:
        - logged in as gnome / gnome123
        - "cat > JOHNREADME", written "I tried to hack Golden's account u. .but the password was wrong. –George. .ia"
        - "ls -l"
        - "logout", which was not found, then "exit"
- rhino2.log
    - TCP stream 1:
        - HTTP

    - Source Address: 137.30.120.37
    - Destination Address: 137.30.123.234 (www.cs.uno.edu)
    - requests:
      - GET /~gnome
      - GET /~gnome/
      - GET /icons/blank.gif
      - **GET /~gnome/rhino4.jpg**
  - TCP stream 2:
    - HTTP
    - Source Address: 137.30.120.37
    - Destination Address: 137.30.123.234 (www.cs.uno.edu)
    - requests:
      - GET /icons/back.gif
      - **GET /~gnome/rhino5.gif**
- rhino3.log
  - TCP stream 3:
    - HTTP
    - Source Address: 137.30.120.37
    - Destination Address: 137.30.123.234 (www.cs.uno.edu)
    - request: GET /~gnome/rhino.exe

5.1.4. What was the fate of the hard drive in the computer, and where is it currently located?

Quote from file "f0335017_She_died_in_February_at_the_age_of_74.doc", which seems to be suspects diary, date not stated:

"OK. Things are getting a little weird. I zapped the hard drive and then threw it into the Mississippi River. I'm gonna reformat my USB key after this entry, but try not to destroy the good stuff. I need to change the password on the gnome account that Jeremy gave me. I can probably just do that at Radio Shack."

5.1.5. What happened to the USB key?

Files have been deteled (by removing entry from FAT) and it has been overwritten with files containing lines "SORRY" and "CHARLIE". Later it was reformatted to new FAT16 partition, which contains two files, gumbo1.txt and gumbo2.txt, text files with cooking recipes.

5.1.6. What data can be retrieved from the dd image of the USB key?

- 2 text files with recipes:
  - gumbo1.txt
  - gumbo2.txt
- 4 images of rhinoceros, filename could not be recovered by used tools:
  - f0106393.jpg
  - f0106409.jpg
  - f0106865.gif
  - f0106889.gif
- 5 images of crocodiles, also without filename:
  - f0104057.jpg
  - f0104249.jpg
  - f0105065.jpg

- f0105873.jpg
- f0335081.jpg
- According to steghide, each of those images contain 5 - 23,1 kB of capacity to hide data, which might have been used. However, deeper analysis was not conducted.

- document f0335017_She_died_in_February_at_the_age_of_74.doc

5.1.7. Is there any indication of a connection between the USB key and the network traces in the evidence? If so, what evidence supports this?

Yes, in the capture file rhino.log appears a zip file contraband.zip, uploaded by FTP from 137.30.122.253 to 137.30.120.40. Althouh the file in archive, named “rhino2.jpg”, is encrypted and a password was not obtained, the file has identical file size and CRC checksum as “f0106409.jpg” obtained from the USB key, which suggests the files are identical.

6. Disclosed Evidence

- f0335017_She_died_in_February_at_the_age_of_74.doc
  - 30 kiB
  - MD5: 68059d3355f0138c9fdd7eaa75e7bc16
  - metadata:
    - Os: Windows, Version 5.1,
    - Code page: 1252,
    - Title: She died in February at the age of 74,
    - Author: NO WAY MAN NO WAY MAN NOWAY.
    - Last Saved By: NOWAY MAN NO WAY MAN NO WAY.,
    - Revision Number: 9,
    - Name of Creating Application: Microsoft Office Word,
    - Total Editing Time: 19:00,
    - Create Time/Date: Tue Aug 9 03:17:00 2005,
    - Last Saved Time/Date: Tue Aug 9 03:40:00 2005,
    - Number of Pages: 3,
    - Number of Words: 1022,
    - Number of Characters: 5832
- contraband.zip
  - 266 kiB
  - MD5: 2eef3f61f6cf90b2fbb724c9bfaec88e
  - contains one encrypted file, rhino2.jpg
    - CRC: 936EBE65
    - uncompressed size: 225.3 kiB

6.1. Possible Evidence Files

- rhino.exe
  - 142.5 kiB
  - MD5: d62d9989535c4c8db14e50b58c9f25a0
  - is a Windows executable of “Microsoft DiskPart version 1.0”, according to its help
  - due to its filename and origin, it might contain evidence or a tool to manipluate / hide evidence, althouh this has not been proved.

Crocodile images:

- f0104057.jpg
  - 93.6 kiB

    - MD5: ee67d8bef72f9b63fa93dc9ea1bb833a
- f0104249.jpg
    - 405.8 kiB
    - MD5: 4d37a1033450b8cc96ffd1564829d321
- f0105065.jpg
    - 401.7 kiB
    - MD5: 6bd0e9bd4fb4a738f9ca4c351a853281
- f0105873.jpg
    - 258.4 kiB
    - MD5: f1bbcd31cd33badc65ca3d1d781f57fa
- f0335081.jpg
    - 258.4 kiB
    - MD5: f1bbcd31cd33badc65ca3d1d781f57fa
    - is the same file as f0105873.jpg

Recpies:

- gumbo1.txt
    - 2.7 kiB
    - d3fc014d86a03730b707ad4205dbc63e
- gumbo2.txt
    - 1.3 kiB
    - 24695a1699fa85ea5553b49d62fd46c2

6.2. Rhinoceros Images

Figure 1: rhino1.jpg,
MD5: d5a83cde0131c3a034e5a0d3bd94b3c9

Figure 2: rhino3.jpg,
MD5: b058218ea0060092d4e01ef3d7a3b815

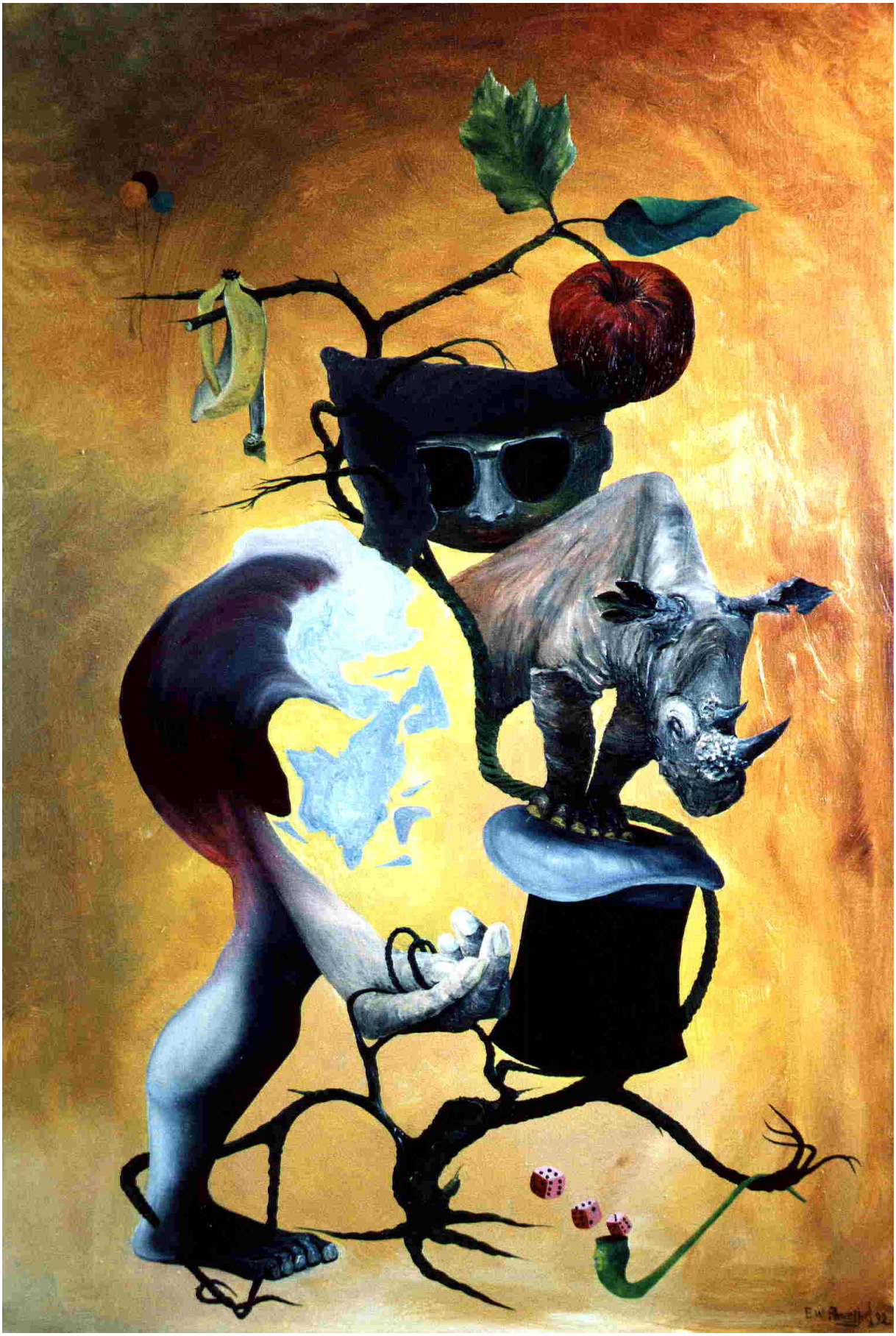

Figure 3: rhino4.jpg,
MD5: aa64102afff71b93ed61fb100af8d52a

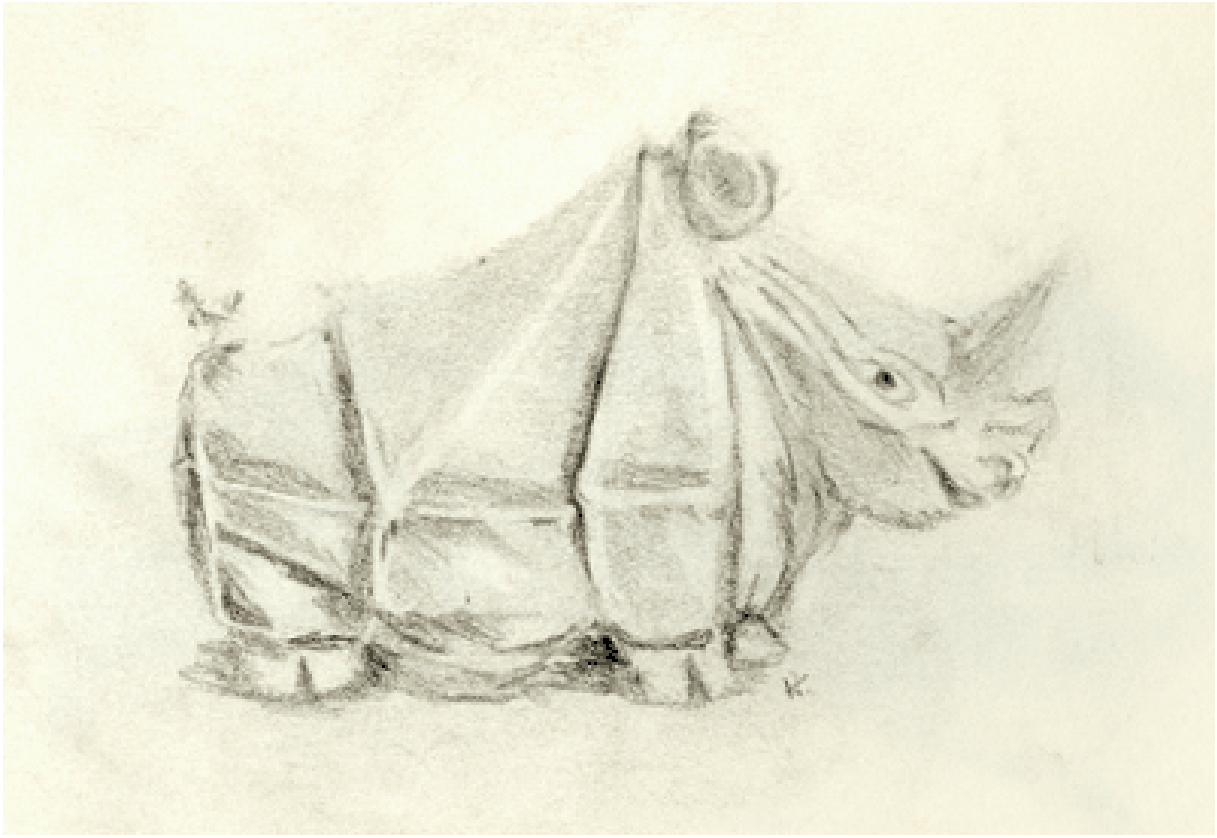

Figure 4: rhino5.gif,
MD5: 1e90b7f70b2ecb605898524a88269029

Figure 5: f0106393.jpg,
MD5: ca03f2eed3db06a82a8a31b3a3defa24

Figure 6: f0106409.jpg,
MD5: ed870202082ea4fd8f5488533a561b35

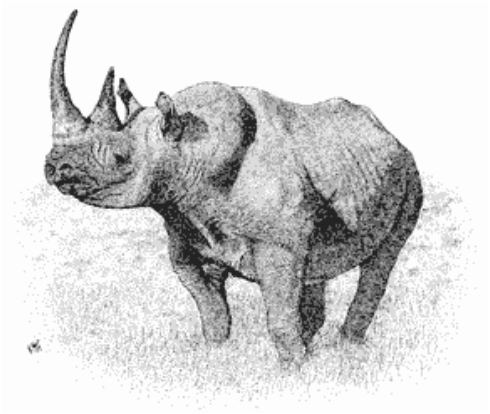

Figure 7: f0106865.gif,
MD5: 76610b7bdb85e5f65e96df3f7e417a74

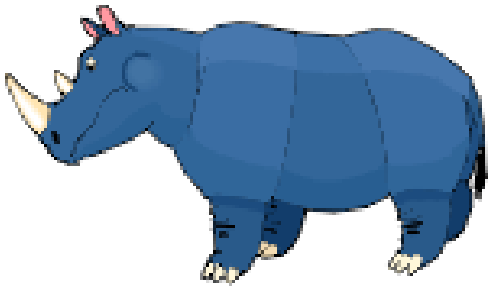

Figure 8: f0106889.gif,
MD5: d03dc23d4ec39e4d16da3c46d2932d62

7. Conclusion

This investigation found 8 unique images of rhinoceros held by investigated suspect, therefore not serving as a witness to law violation. However, more rhinoceros images might exist in investigated evidence, which were not revealed. These include primarily images of crocodiles found on suspects USB key and the file rhino.exe which may serve as a tool to hide the illegal images. The entry from suspects diary:

"Rhino pictures illegal? Makes me sick. I "hid" the photos...hehehehe. Apparently, if there are less than 10 photos, it's no big deal."

suggests the suspect was aware of violating the law and took measures to hide the evidence.