

UK Statutes and Guidelines Followed:
Criminal Procedure Rules, r 27.1 (1)
Criminal Justice Act 1967, s. 9
Magistrates' Court Act 1980, s.5B
ACPO Digital Evidence Guidelines

EXPERT WITNESS REPORT

IN RELATION TO

ILLEGAL RHINOCEROS IMAGES

BY REQUEST OF: MR. GARETH DAVIES

NAME OF EXPERT: DAVIDE PERON

CASE NAME: RHINO-1151910

This statement (consisting of 10 pages each signed by myself) is true to the best of my knowledge and belief and I make it knowing that, if tendered in evidence, I shall be liable to prosecution if I have wilfully stated in it anything which I know to be false or do not believe to be true.

Signature:

Date:

Contents

Curriculum Vitae	3
Instruction/Objectives	3
Abstract of the case	3
Statement of Instructions	3
Received Evidence Items	3
Analysis of the evidence items	4
rhino.log analysis	4
rhino2.log analysis	5
rhino3.log analysis	6
f0334472.doc analysis	6
Search for images in img_RHINOUSB.dd	7
Expert Witness Opinion	9
Non-Availability of Expert Witness	9
Contact Information	9
Appendix 1 - Software used	10
Autopsy	10
S-Tools	10

Curriculum Vitae

I am Davide Peron and I am a student in MSc Telecommunications Engineering in University of Padova. I have a Bachelor Degree in Information Engineering. I have matured my skills in digital devices and networks analysis during my academic career and now I can analyse in depth some devices like smartphones, hard disks, live computers or computer networks.

Name	Davide Peron
Enrolment Number	1151910
Institutional E-mail	davide.peron.2@studenti.unipd.it
Occupation	Student in first year of Telecommunications Engineering

Instruction/Objectives

Abstract of the case

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 some illegal rhino traffic was flagged by his network monitoring software. The suspect is a research student and is the primary user of a University computer. The computer hard drive was missing at the time of the alleged offence.

Police have taken a forensically image of USB flash drive seized from one of the University's computer. Network administrator has recovered three network traces involve the machine with the missing hard drive.

Statement of Instructions

The police has requested that I Davide Peron carry out an investigation on the following evidence items:

- *RHINOUSB.dd* USB Image
- Three network traces

The purpose of this report is to outline the result of the investigation in order to answer to the question *Is there any evidence to show that the suspect did store illegal images on the University computer?*

Received Evidence Items

For each evidence item received, the correspondent MD5 hash checksum was provided. This checksum has been recalculated at the end of the investigation to ensure the integrity of evidence items.

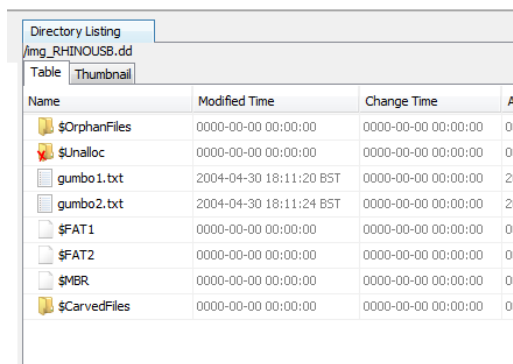
The provided MD5 checksums are shown in Table 1

Evidence Item	MD5 checksum
RHINOUSB.dd	80348c58eec4c328ef1f7709adc56a54
rhino.log	c0d0093eb1664cd7b73f3a5225ac3f30
rhino2.log	cd21eaf4acfb50f71ffff857d7968341
rhino3.log	7e29f9d67346df25faaf18efcd95fc30

Table 1: Evidence Items's MD5 checksums

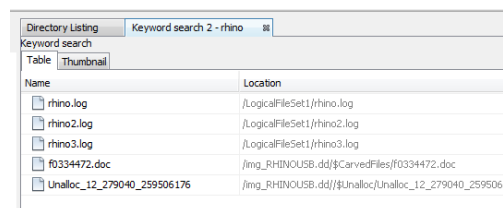
Analysis of the evidence items

A new case in Autopsy¹ has been created, including in it the evidence items. Figure 1 shows the root folder of *RHINOUSB.dd* USB image. Searching for the keyword *rhino* in Autopsy, I have obtained files that contains this word (as shown in Figure 2). We can see at them one by one.



Directory Listing			
/img_RHINOUSB.dd			
Name	Modified Time	Change Time	A
\$OrphanFiles	0000-00-00 00:00:00	0000-00-00 00:00:00	0i
\$Unalloc	0000-00-00 00:00:00	0000-00-00 00:00:00	0i
gumbo1.txt	2004-04-30 18:11:20 BST	0000-00-00 00:00:00	2i
gumbo2.txt	2004-04-30 18:11:24 BST	0000-00-00 00:00:00	2i
\$FAT1	0000-00-00 00:00:00	0000-00-00 00:00:00	0i
\$FAT2	0000-00-00 00:00:00	0000-00-00 00:00:00	0i
\$MBR	0000-00-00 00:00:00	0000-00-00 00:00:00	0i
\$CarvedFiles	0000-00-00 00:00:00	0000-00-00 00:00:00	0i

Figure 1: Root folder of *RHINOUSB.dd* image



Directory Listing	
Keyword search 2 - rhino	
Name	Location
rhino.log	/LogicalFileSet1/rhino.log
rhino2.log	/LogicalFileSet1/rhino2.log
rhino3.log	/LogicalFileSet1/rhino3.log
f0334472.doc	/img_RHINOUSB.dd/\$CarvedFiles/f0334472.doc
Unalloc_12_279040_259506176	/img_RHINOUSB.dd/\$Unalloc/Unalloc_12_279040_259506...

Figure 2: Result of the search on *RHINOUSB.dd* image

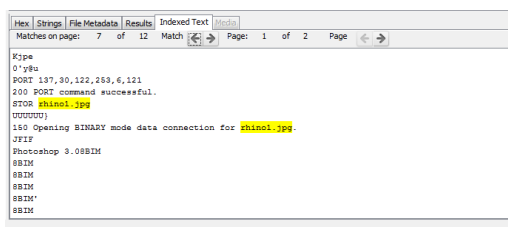
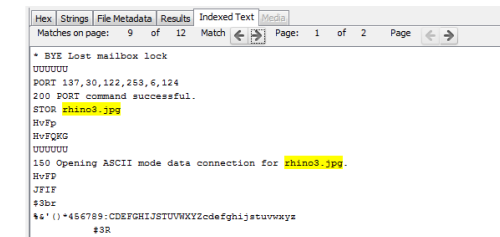
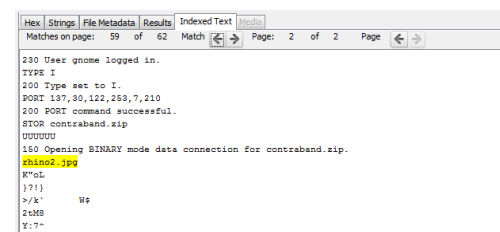
rhino.log analysis

Opening *rhino.log* I have found that several FTP file transfers have been recorded. In *rhino.log* has been recorded each FTP command, including the name of the files transferred. Through this analysis I have found some references to *rhino1.jpg* [Figure 3], *rhino3.jpg* [Figure 4] and *rhino2.jpg* [Figure 5]. This last image was contained into an archive called *contraband.zip*. In this file I have found also the name of the account from which the crime was performed and the relative password:

Account	gnome
Password	gnome123

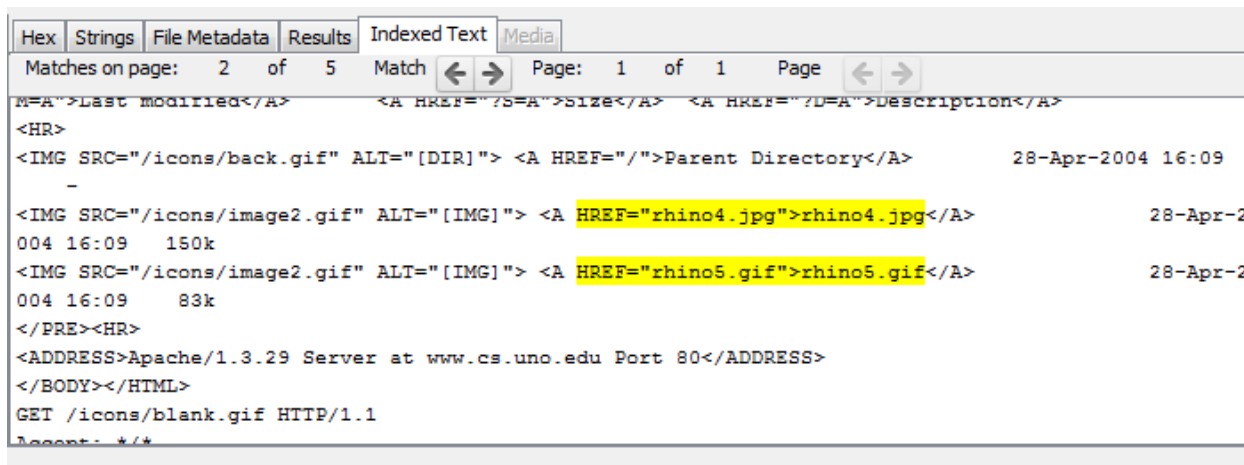
Table 2: Data of the account from which the crime was performed

¹Some more information about software used during the investigation, can be found in Appendix 1.

Figure 3: Evidence of existence of *rhino1.jpg* imageFigure 4: Evidence of existence of *rhino3.jpg* imageFigure 5: Evidence of existence of *rhino2.jpg* image inside *contraband.zip*

rhino2.log analysis

Opening *rhino2.log* in Autopsy I have found several HTTP Requests. Between them I have found references to *rhino4.jpg* and *rhino5.gif*, two fraud images (visible in Figure 6, Figure 7 and Figure 8).

Figure 6: Evidence of existence of *rhino4.jpg* and *rhino5.gif* images

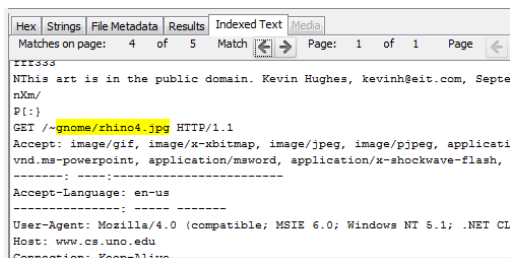


Figure 7: Evidence of existence of *rhino4.jpg* image

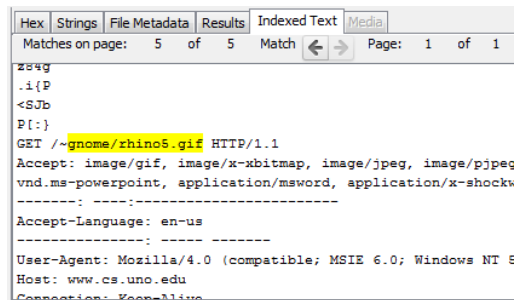


Figure 8: Evidence of existence of *rhino5.gif* image

rhino3.log analysis

Analysing this file, I have found several references to an executable file called *rhino.exe* inside an HTTP Request. One of these references is shown in Figure 9.

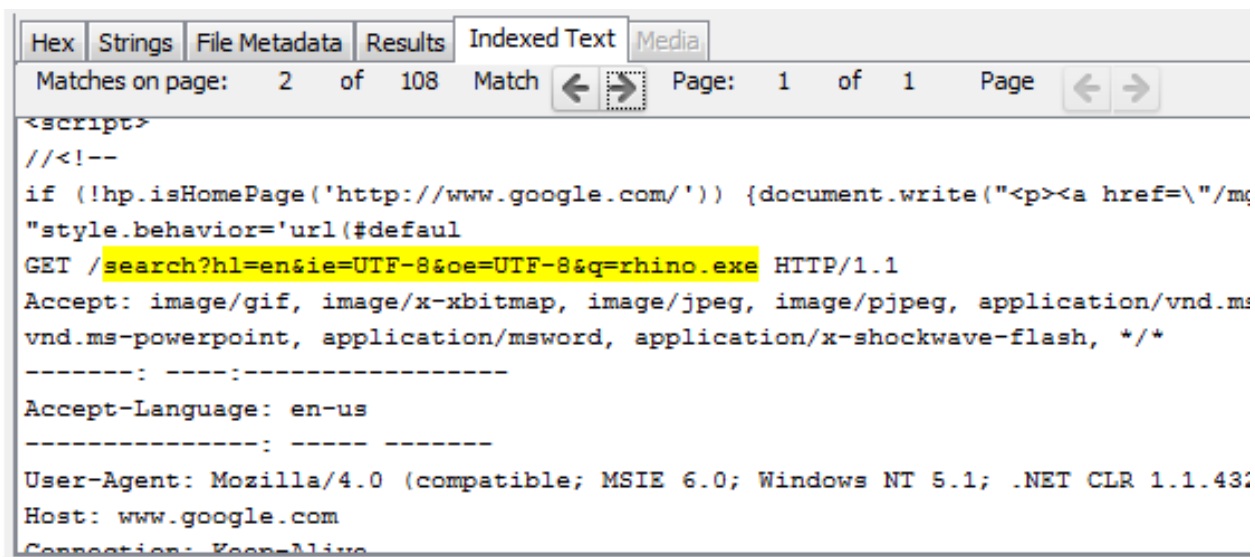


Figure 9: Evidence of existence of *rhino.exe*

f0334472.doc analysis

This is a plain text file. Here I have found a brief summary of the crime. In the last part of the text is written the following (proved by Figure 10):

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

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.

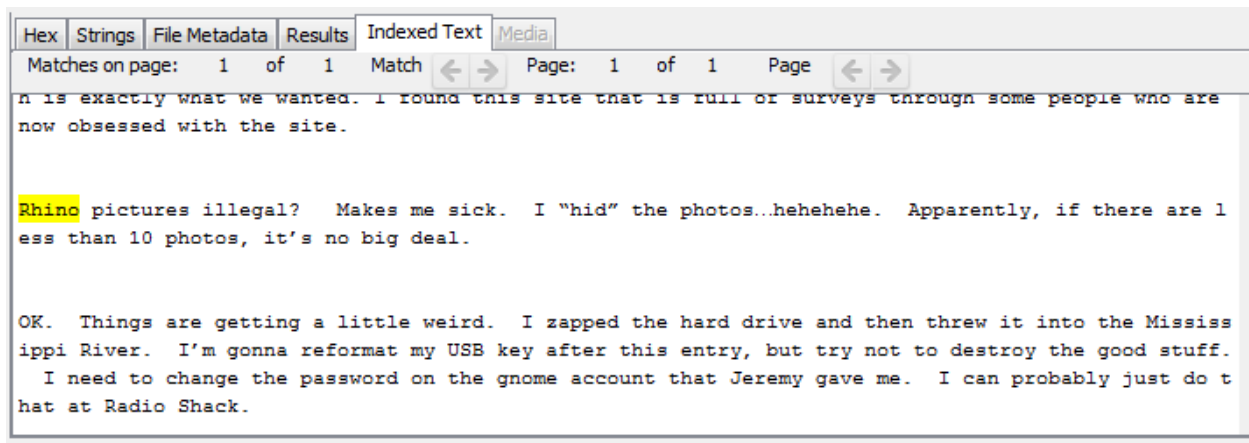


Figure 10: Text found in *f0334472.doc*

In this text there is written some information about the USB key used for the crime and about the account from which the crime was performed. In the metadata of this file I have found some other information about it.

I have found that this text is written with *Microsoft Office Word*. The metadata of this file also contain the proprietary of the PC from which this text was written, that is *University of New Orleans*. In the file *Unalloc_12_279040_259506176*, an unallocated part of the memory, there's a longer preamble text after which is appended the same text of *f0334472.doc*.

Search for images in *img_RHINOUSB.dd*

Searching in the folders of *img_RHINOUSB.dd* I have found some rhino's images. They are contained in *img_RHINOUSB.dd\$CarvedFiles* and are reported in the following.



Figure 11: Evidence in
img_RHINOUSB.dd/\$CarvedFiles/20-f0105848.jpg



Figure 12: Evidence in
img_RHINOUSB.dd/\$CarvedFiles/21-f0105864.jpg

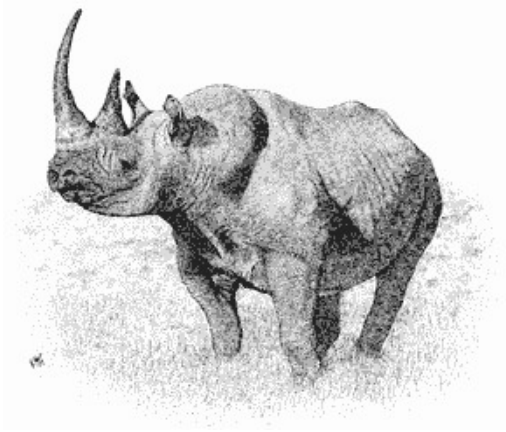


Figure 13: Evidence in
img_RHINOUSB.dd/\$CarvedFiles/22-f0106320.gif

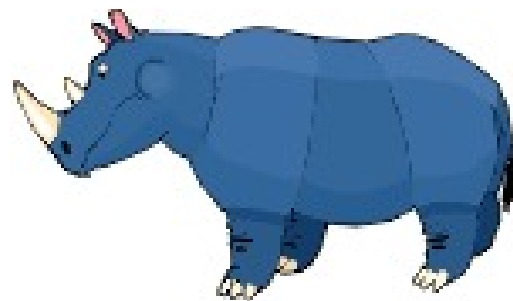


Figure 14: Evidence in
img_RHINOUSB.dd/\$CarvedFiles/23-f0106344.gif

Expert Witness Opinion

During the investigation I have found many evidence of the crime in the evidence items.

The file *f0334472.doc* demonstrate that the accused has hidden rhino pictures inside the USB key. According to this file, this USB key has been reformatted (at *Radio Shack*) hoping not to overwrite the *good* stuff, and the hard drive containing fraud images has been disposed of into the Mississippi River. This file also hints at a gnome account given to the accused by a certain Jeremy. This is a connection to *rhino.log*, since a gnome account is used to transfer some fraud images via FTP protocol. In this file there is also the password of this *gnome* account (that is *gnome123*).

In *rhino.log* and in the other two *.log* files there are several references to fraud images, in specific to *rhino1.jpg*, *rhino2.jpg*, *rhino3.jpg*, *rhino4.jpg* and *rhino5.gif*, and to an *.exe* file, all these are mentioned in FTP or HTTP Requests, this prove that these files have been in the New Orleans University's PC for a while.

Other images have been found in the *\$CarvedFiles/* folder. In conclusion, I have proved that several rhino's images have been stored in the New Orleans University's PC for a while, I have not recovered these images at all but I have found clear references to them.

Non-Availability of Expert Witness

Month of:							Month of:							Month of:						
1	2	3	4	5	6	7	1	2	3	4	5	6	7	1	2	3	4	5	6	7
8	9	10	11	12	13	14	8	9	10	11	12	13	14	8	9	10	11	12	13	14
15	16	17	18	18	20	21	15	16	17	18	19	20	21	15	16	17	18	19	20	21
22	23	24	25	26	27	28	22	23	24	25	26	27	28	22	23	24	25	26	27	28
29	30	31					29	30	31					29	30	31				
Month of:							Month of:							Month of:						
1	2	3	4	5	6	7	1	2	3	4	5	6	7	1	2	3	4	5	6	7
8	9	10	11	12	13	14	8	9	10	11	12	13	14	8	9	10	11	12	13	14
15	16	17	18	18	20	21	15	16	17	18	19	20	21	15	16	17	18	19	20	21
22	23	24	25	26	27	28	22	23	24	25	26	27	28	22	23	24	25	26	27	28
29	30	31					29	30	31					29	30	31				

Contact Information

Full name	Davide Peron
Institutional e-mail	davide.peron.2@studenti.unipd.it
Work address	Via Gradenigo 6/b 35131 - Padova Italy

Appendix 1 - Software used

For the whole investigation, I have used Autopsy and S-Tools as Forensics Software Tools and Windows 7 version 6.1 as Operating System.

Autopsy

Software name	Autopsy
Version	4.3.0

*Autopsy*TM is an open source digital forensics platform used to examine several types of items, logical or physical volumes. It is used by law enforcement, military, and corporate examiners to investigate what happened on a computer. It is based on *The Sleuth Kit*, a collection of open source programs aimed to investigate pieces of software or hardware.

S-Tools

Software name	S-Tools
Version	4.00

S-Tools is an open source software that offer several stenography tools, to create or find files with stenography in them.

I've used this program to ensure that no other rhino images are hidden into some files.