Computer Forensic Investigative Analysis Report (CFIAR)

|  |  |
| --- | --- |
| **Incident Report Number** | **[2017,09,28,II,1]** |
| **Reported Incident Date** |  |
|  |  |
| **Examiner(s)** | **DSV CS2Lab1**  **Group 29**  **Johan Bäckström**  **Anton Fluch** |
| **Requester(s)** | **DSV** |
| **Suspected Offence** | **Not known** |
| **Investigation hours** | **3-4 hours** |

# Case X

/\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\* FROM KALI

Command:

dcfldd if=winxp.vdi hash=md5 of=/root/Desktop/Lab1/ouput.dd bs=512 conv=noerror

Result:

3074048 blocks (1501Mb) written.Total (md5): c965a5e2236d60624c07c8233ed0aeb3

3074048+0 records in

3074048+0 records out

Command:

root@kali:~/Desktop/Lab1/Exercise4\_Acquisition# md5sum \*

Result:

c965a5e2236d60624c07c8233ed0aeb3 ouput.dd

c965a5e2236d60624c07c8233ed0aeb3 winxp.vdi

Command

root@kali:~/Desktop/Lab1/Exercise4\_Acquisition# sha1sum \*

Result:

a8d7b2a8ebffc3905ab8b04edfe7e6fa92076fce ouput.dd

a8d7b2a8ebffc3905ab8b04edfe7e6fa92076fce winxp.vdi

Command:

Using foremost to extract the files from the .dd copy, we got

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*/

<General description of the case and its evidence>

A digital copy of a drive (winxp.vdi) was provided to the digital forensic investigation team by the Lab instructors to be acquired in forensically sound manner. The purpose is to be acquainted with the process of acquiring evidence.

Fill in the following fields you find necessary, and/or have information about, for the case in question:

**Objective**: Acquiring evidence in a forensically sound manner

**Computer type**: x86\_64 Intel Processor Virtual System

**Operating system**: Kali-Linux-2017.1-vbox-AMD64

**Offense**: Not known

**Case agent**: Anton Fluch, Johan Bäckström

**Evidence number**: #1234567

**Where examination took place**: CS2Lab at Stockholm Universoty, Kista, Department of Computer and Systems Sciences (DSV)

**Tools used**: dcfldd 1.3.4-1, Foremost 1.5.7, grep 3.1, Eye of Gnome Image Viewer, Videos, GEdit 3.22.1, ClamAV 0.99.3-beta1,

## Processing

**Identification:**

1. WinXP.vdi was downloaded from the DIFO lab files on Thursday 28th of September
2. The disk image was checked using md5sum and sha1sum to identify the hash sums and see that the file was correct according to the lab instructions.

Results:

c965a5e2236d60624c07c8233ed0aeb3 winxp.vdi

a8d7b2a8ebffc3905ab8b04edfe7e6fa92076fce winxp.vdi

1. After making sure that the hash sums was correct a bit by bit copy of the drive image file was created with the tool dcfldd

Command:

dcfldd if=winxp.vdi hash=md5 of=/root/Desktop/Lab1/ouput.dd bs=512 conv=noerror

Result:

3074048 blocks (1501Mb) written.Total (md5): c965a5e2236d60624c07c8233ed0aeb3

3074048+0 records in

3074048+0 records out

1. This copy was then checkecd again using md5sum and sha1sum to make sure the copy was identical.

Command:

root@kali:~/Desktop/Lab1/Exercise4\_Acquisition# md5sum \*

Result:

c965a5e2236d60624c07c8233ed0aeb3 ouput.dd

c965a5e2236d60624c07c8233ed0aeb3 winxp.vdi

Command

root@kali:~/Desktop/Lab1/Exercise4\_Acquisition# sha1sum \*

Result:

a8d7b2a8ebffc3905ab8b04edfe7e6fa92076fce ouput.dd

a8d7b2a8ebffc3905ab8b04edfe7e6fa92076fce winxp.vdi

**Acquisition**: <Describe how the evidence was acquired and provide relevant hashsums for integrity purposes. Also describe how the evidence was preserved. >

Sample text:

*The hardware configuration was documented and a duplicate of the hard drive was created in a manner that protected and preserved the evidence. The CMOS information, including the time and date, was documented.*

**Examination**: <Describe how the evicedene was examined>

Sample text:

*The directory and file structures, including file dates and times, were recorded. A file header search was conducted to locate all graphic images. The image files were reviewed and those files containing images of what appeared to be children depicted in a sexually explicit manner were preserved. Shortcut files were recovered that pointed to files on floppy disks with sexually explicit file names involving children. The last accessed time and date of the files indicated the files were last accessed 10 days before the laptop was delivered to Mom & Pop’s.*

**Documentation and reporting:** <Describe how the report was written and how the case was documented in general>

Sample text:

*The investigator was given a report describing the findings of the examination. The investigator determined that he needed to conduct interviews.*

**[DELETE THIS SECTION PRIOR TO HAND-IN:]**

Well done! Now that we have the internal document in place we need to make a brief report that the attorney and other non-technical colleagues can get read through swiftly. The brief report below, is an example of a forensics investigation report which contains the essentials of a forensics investigation. This brief version of the report contains all necessary information about the case and, needless to say, it maintains the chain of custody. The italic text is sample text from the source template.

# Case X brief report

**REPORT OF \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

**MEMORANDUM FOR:** *County Sheriff’s Police*

*Investigator Johnson*

*Anytown, USA 01234*

**SUBJECT:** *Forensic Media Analysis Report*

*SUBJECT: DOE, JOHN*

*Case Number: 012345*

1. **Status: Closed.**

2. **Summary of Findings:**

* *327 files containing images of what appeared to be children depicted in a sexually explicit manner were recovered.*
* *34 shortcut files that pointed to files on floppy disks with sexually explicit file names involving children were recovered.*

**3. Items Analyzed:**

**TAG NUMBER:** **ITEM DESCRIPTION:**

012345 One Generic laptop, Serial #12345677

**4. Details of Findings:**

* *Findings in this paragraph related to the Generic Hard Drive, Model ABCDE, Serial # 3456ABCD, recovered from Tag Number 012345, One Generic laptop, Serial # 123456789.*

*1) The examined hard drive was found to contain a Microsoft® Windows® 98 operating system.*

*2) The directory and file listing for the media was saved to the Microsoft® Access Database TAG012345.MDB.*

*3) The directory C:\JOHN DOE\PERSONAL\FAV PICS\, was found to contain 327 files containing images of what appeared to be children depicted in a sexually explicit manner. The file directory for 327 files disclosed that the files’ creation date and times are 5 July 2001 between 11:33 p.m. and 11:45 p.m., and the last access date for 326 files listed is 27 December 2001. In addition, the file directory information for one file disclosed the last access date as 6 January 2002.*

*4) The directory C:\JOHN DOE\PERSONAL\FAV PICS TO DISK\ contained 34 shortcut files that pointed to files on floppy disks with sexually explicit file names involving children. The file directory information for the 34 shortcut files disclosed the files’ creation date and times are 5 July 2001 between 11:23 p.m. and 11:57 p.m., and the last access date for the 34 shortcut files was listed as 5 July 2001.*

*5) The directory C:\JOHN DOE\LEGAL\ contained five Microsoft® Word documents related to various contract relationships John Doe Roofing had with other entities.*

*6) The directory C:\JOHN DOE\JOHN DOE ROOFING\ contained files related to operation of John Doe Roofing.*

*7) No further user-created files were present on the media. 5. Glossary: Shortcut File: A file created that links to another file. 6. Items Provided: In addition to this hard copy report, one compact disk (CD) was submitted with an electronic copy of this report. The report on CD contains hyperlinks to the above-mentioned files and directories.*

IMA D. EXAMINER Released by**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

N.N Computer Forensic Examiner