Computer Forensic Investigative Analysis Report (CFIAR)

|  |  |
| --- | --- |
| **Incident Report Number** | **[2017,09,22,II,version]** |
| **Reported Incident Date** | **2017-09-22** |
|  |  |
| **Examiner(s)** | **Wisam Faik, Md Piar Hossain, Cecilia To** |
| **Requester(s)** | **Investigator Johnson** |
| **Suspected Offence** | **”unknown”** |
| **Investigation hours** | **72 hours** |

# Case Group 14

Investigator Johnson contacted DSV Forensics Security Lab to analyze the virtual hard disk image. He submitted the evidence in the form of Oracle virtual hard disk image to us. He suspected this virtual hard disk image might contain evidences to support his investigation. He also hopes that we can identify the owner of this virtual hard disk image might belong to.

**Objective**:

-To acquire the evidence from virtual hard disk to ensure the integrity of evidence by using forensics tools and procedures.

-To analyze the acquired evidence by using these tools: FTK Imager. EnCase, md5deep64, sha1deep64.

**Computer type**: suspect’s computer type is a virtual machine

**Operating system**: suspect’s windows XP

**Offense**: “unknown”

**Case agent**: Investigator Johnson

**Evidence number**: #1234567

**Where examination took place**: DSV Forensics Security Lab

**Tools used**: FTK Imager, EnCase, Oracle Virtual Box Manager (vboxmanager.exe), md5deep64.exe and sha1deep64.exe

## Processing

**Identification:**

Item submitted by investigator Johnson was Oracle virtual hard disk image, ‘*winxp.vdi’.*

**Assessment**:

Reviewed the case investigator’s request for service. The search warrant provided legal authority. The investigator was interested in finding all any information that can be used and support his investigation including access dates by the owner and ownership of the computer. It was determined that the equipment needed was available in the forensic lab.

**Acquisition**:

Acquisition of evidence was done by using:

* DOS command prompt and using Oracle VBoxManager.exe by converting the Oracle virtual hard disk image to raw image.

Command used was:

*vboxmanage.exe internalcommands converttoraw C:\Users\cs2lab\Desktop\ex4\_test\winxp.vdi C:\Users\cs2lab\Desktop\ ex4\_test\winxp\_img.raw*

There were two options specified with this command: internalcommands and converttoraw.

This procedure was to duplicate of the virtual hard disk in the matter that protected and preserved the evidence. The information including the time date and ownership of the virtual hard disk were documented.

* Hash values was performed by using md5deep64 and sha1deep64:

Md5 algorithm:

Suspect’s original image hash: c965a5e2236d60624c07c8233ed0aeb3

Acquired raw image hash value: a8d0e8ea3dc646e190cda809fbfa325f

Sha1 algorithm:

Suspect’s original image hash: a8d7b2a8ebffc3905ab8b04edfe7e6fa92076fce

Acquired raw image hash value: ec1e66120b45522ae8cc49d4158aaeb6fea883dc

* From FTK Imager, the acquired raw image evidence ‘*winxp\_img.raw*’ was added to start the process of analysis.

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

* The date of acquisition was 2017-09-20 for the acquired raw image ‘*winxp\_img.raw*’.
* The computer used to acquire the raw image was performed on Intel(R) Core(TM) i7-4770 CPU @3.40Ghz RAM has 16GB for 64 bit operating system. The operating system is Windows 7.
* The sector information of the acquired evidence was:

Sector count from FTK Imager was: 41943040 and bytes per sector: 512

sector calculation:

41943040 \* 512 per sector = 2.147484e10 bytes

2. 147484e10 bytes / 1024 bytes = 20971523.4 kilobytes  
20971523.4 kilobytes / 1024 kilobytes = 20480.0033metabytes

According to FTK imager: 20480MB.

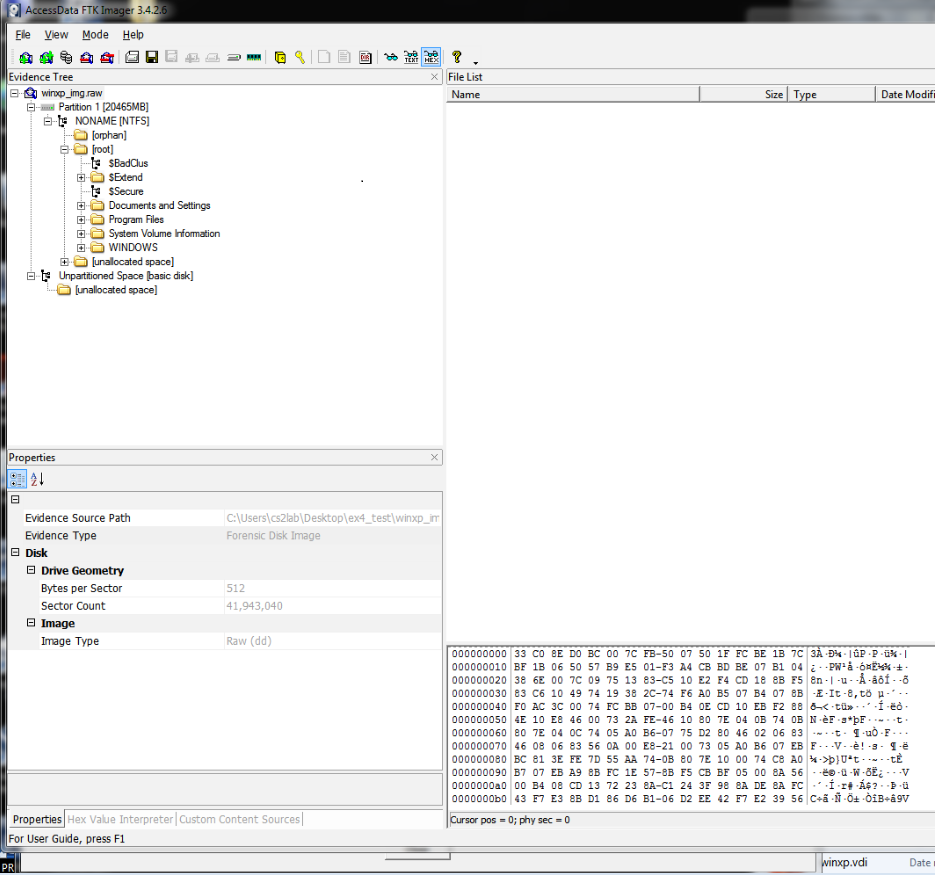


Figure 1: sector information from FTK Imager.

* In order to verify the hash values of the acquired raw image ‘*winxp\_img.raw*’, we exported the ‘*winxp\_img.raw*’ from FTK Imager to ‘*acquired\_image.EO1’*. FTK Imager automatically generated the summary report of hash verification for us. From this FTK report, hash values were verified as matched.

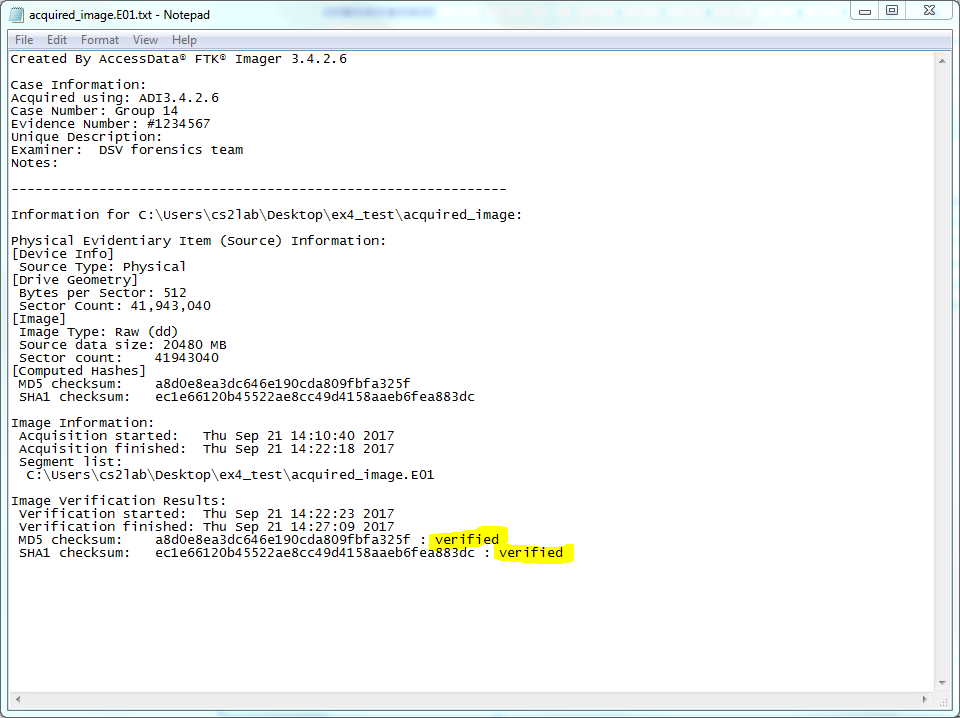


Figure 2: Verified hash values by FTK Imager summary report.

Using EnCase, we added the ‘*acquired\_image.EO1’* and it generated a summary report which matched the same hash values verified by FTK Imager.



Figure 3: Verified hash values by EnCase summary report.

* Extra evidence files were discovered during the analysis phase.

One user account was found and the name of the user account was: ‘Chris Hemsworth’.

Files that were under *Chris Hemsworth* directory were protected with user password. These files were last accessed on 2016-10-30 at 21:23:19 PM.

Cookies information were found:

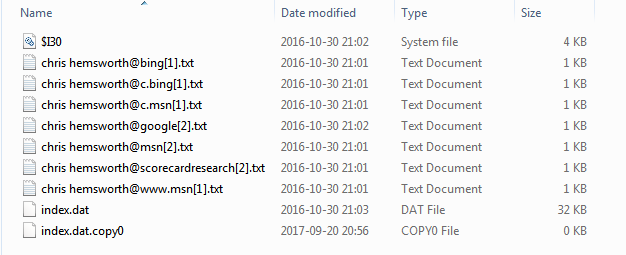


Figure 3: Cookies information.

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

This forensics report was written by DSV forensics team where the team follows this procedures from National Institute of Standards and Technology (NIST), & United States of America. (2004). Forensic Examination of Digital Evidence: A Guide for Law Enforcement. Url: <https://www.ncjrs.gov/pdffiles1/nij/199408.pdf>.

# Case Group 14 brief report

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

**MEMORANDUM FOR:** *County Sheriff’s Police of Mission District*

*Investigator Johnson*

*San Francisco, CA, USA 94110*

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

*Case Number: Group14*

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 Oracle Virtual Hard Drive, Serial # *e12F3456ABCD*

**4. Details of Findings:**

* *Findings in this paragraph related to the Oracle virtual hard disk, Model Samsung, Serial # e12F3456ABCD, recovered from Tag Number 012345.*

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

*2) The directory and file listing for the media was saved to the Microsoft® Access Database at DSV Forensics Security Lab.*

*3) The directory C:\Documment and Settings\Chris Hemsworth\, 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:\Documment and Settings\Chris Hemsworth\, 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) 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 DVD media was submitted with an electronic copy of this report. The report on DVD contains hyperlinks to the above-mentioned files and directories.*

IMA D. EXAMINER Released by**:** Faik, Hossain, To

N.N Computer Forensic Examiner