Computer Forensic Investigative Analysis Report (CFIAR)

|  |  |
| --- | --- |
| **Incident Report Number** | **[2017,09,29,II,1]** |
| **Reported Incident Date** | **2017-09-29** |
|  |  |
| **Examiner(s)** | **Forensic Analysis Team (FAT)**  **Group 14: Wisam Faik, Md Piar Hossain, Cecilia To** |
| **Requester(s)** | **Police Investigator Jesper Bergman** |
| **Suspected Offence** | **”unknown”** |
| **Investigation hours** | **72 hours** |

# Case *Christopher Hemsworth*

Police investigator Jesper Bergman 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 the Forensics Analysis team (FAT). He suspected this virtual hard disk image might contain evidences to support his investigation of money laundering. He has requested the FAT to perform several forensic operations such as Windows File System Reconstruction and analysis of the Windows Operating System on the artifacts (Windows registry keys information) including any relevant data information that might lead to money laundering activities by the SUBJECT.

**Objective**: Search for evidence of performed or planned criminal activities of the SUBJECT or other parties who would have access via File System Reconstruction and analysis of the Windows Operating System artifacts.

-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 forensic tools: FTK Imager v3.4.2.6, EnCase v8.04, md5deep64.exe v 4.4,

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

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

**Offense**: not specified

**Case agent**: Police Investigator Jesper Bergman

**Chain of Custody**: see Apendix A.

**Evidence number**: #1234567

**Where examination took place**: DSV Forensics Security Lab at Stockholm University, Department of Computer Science,

Borgarfjordsgatan 12, Kista, Sweden.

**Tools used**: Access Data FTK Imager version 3.4.2.6, EnCase version 8.04, Oracle Virtual Box version 5.1.26r Manager (vboxmanager.exe), md5deep64.exe version 4.4, sha1deep64.exe version 4.4 and Foremost from Kali,

## Processing

**Identification:**

1. An Oracle virtual hard disk image, ‘*winxp.vdi’*, was provided to Forensics Analysis Lab team (FAT) on 2017-09-28 16:00PM by police investigator Johnson.
2. Police Investigator Jesper Bergman works at the San Francisco Mission police department and is authorized to submit digital evidence to FAT team.
3. Hash values of ‘*winxp.vdi’* were provided to FAT team. They were:
   1. Md5 hash sum: *c965a5e2236d60624c07c8233ed0aeb3*
   2. SHA1 hash sum: *a8d7b2a8ebffc3905ab8b04edfe7e6fa92076fce*
4. No further case details were provided to FAT team.

**Acquisition**:

1. FAT team used multiple tools in order to perform the acquisition steps. These tools led the team to discover several types of information from the SUBJECT’s system.
2. SUBJECT’s system was provided to the FAT team in the form of Oracle virtual hard disk image.
3. FAT team didn’t receive the actual hardware of the SUBJECT’s system, thus the team would only be able to state the facts discovered and found from SUBJECT’s evidence.
4. FAT team could not confirm the origin or the evidence’s attribution to the SUBJECT and could not ensure that the evidence would represent the original state of the SUBJECT’s data.
5. Chain of custody:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Chain of Custody** | | | | |
| **Item #** | **Date/Time** | **Released by** (Signature & ID#) | **Received by** (Signature & ID#) | **Comments/Location** |
| 1 | 2017-09-28 16:00PM | Police Investigator Jesper Bergman | Forensics Analysis Lab Chief: Oliver | Evidence was in the form of Oracle virtual hard disk image ‘*winxp.vdi’* |
| 1 | 2017-09-29 09:00AM | Forensics Analysis Lab Chief: Oliver B. Popov | FAT team: MD Piar Hossain | Evidence was transferred to FAT database (ilearn2.dsv.sus.se) |
| 1 | 2017-09-29 09:05AM | FAT team | FAT team | Evidence obtained by the FAT team. |
| 1 | 2017-09-29 09:15AM | FAT team | FAT team | Evidence processed and investigation started |
| 1 | 2017-09-30 18:00PM | FAT team | FAT team | Evidence hashes verification after investigation and case closed. |

1. Due to receiving the evidence from police investigator Jesper Bergman, FAT team would assume the acquisition and the attribution of the evidence to the SUBJECT.
2. FAT team would perform these acquisition step:
   1. identification of the evidence and establishment of the case file and chain of custody,
   2. examination using forensic investigative analysis, recording, documenting and photographing of the SUBJECT’s evidence,
   3. file carving as digital extraction in order for examination and storage of the SUBJECT’s evidence,
   4. extraction process will be documented to include the programs used, hash values and the configuration of the SUBJECT’s evidence.
3. For forensic investigation to start, a digital copy will be made and the original SUBJECT’s evidence will be stored in vault for preservation. All work will be performed on the digital copy.

I) Starting the first process of acquisition on the digital copy of the SUBJECT’s evidence by using:

* Initially, FAT team used two strategies to process the *winxp.vdi* evidence file.

-a) from Kali, FAT team used ‘dd’ command to do bit by bit copy of the *winxp.vdi* to *winxp.dd.*

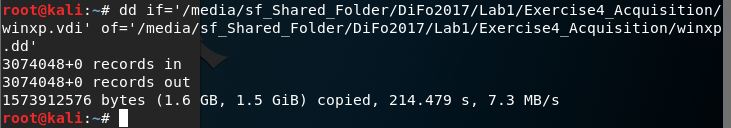


Figure-1: dd command.

-b) from Windows 7, FAT team used FTK Imager to create a new case. After adding a new case, FAT team started with creating a disk image of ‘*winxp.vdi’,* then they added this *created image* as evidence.

Since both Kali with dd image and the image created by the FTK Imager revealed the same *‘unrecognized file system[unknown type]’* when FAT team opened both images from FTK imager. This first method was not helpful for FAT team since they were not able to process further. So FAT team decided to persuade two methods (II and III) below.

II) Starting the second process of acquisition on the digital copy of the SUBJECT’s evidence by using::

In order to start the acquisition process of ‘*winxp.vdi’* for evidence, FAT team initially had to convert the evidence file from Oracle virtual hard disk ‘*vdi’* format to ‘*raw’* format.

* From the DOS command prompt, FAT team used Oracle VBoxManager.exe by converting the Oracle virtual hard disk image to a 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 step was to duplicate the virtual hard disk image in the matter that protected and preserved the evidence.

* Hash values was performed by using md5deep64 and sha1deep64:

Md5 algorithm:

SUBJECT’s original image hash: *c965a5e2236d60624c07c8233ed0aeb3*

Acquired raw image hash value: *a8d0e8ea3dc646e190cda809fbfa325f*

Sha1 algorithm:

SUBJECT’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.

The acquired raw image looked like this from FTK Imager:

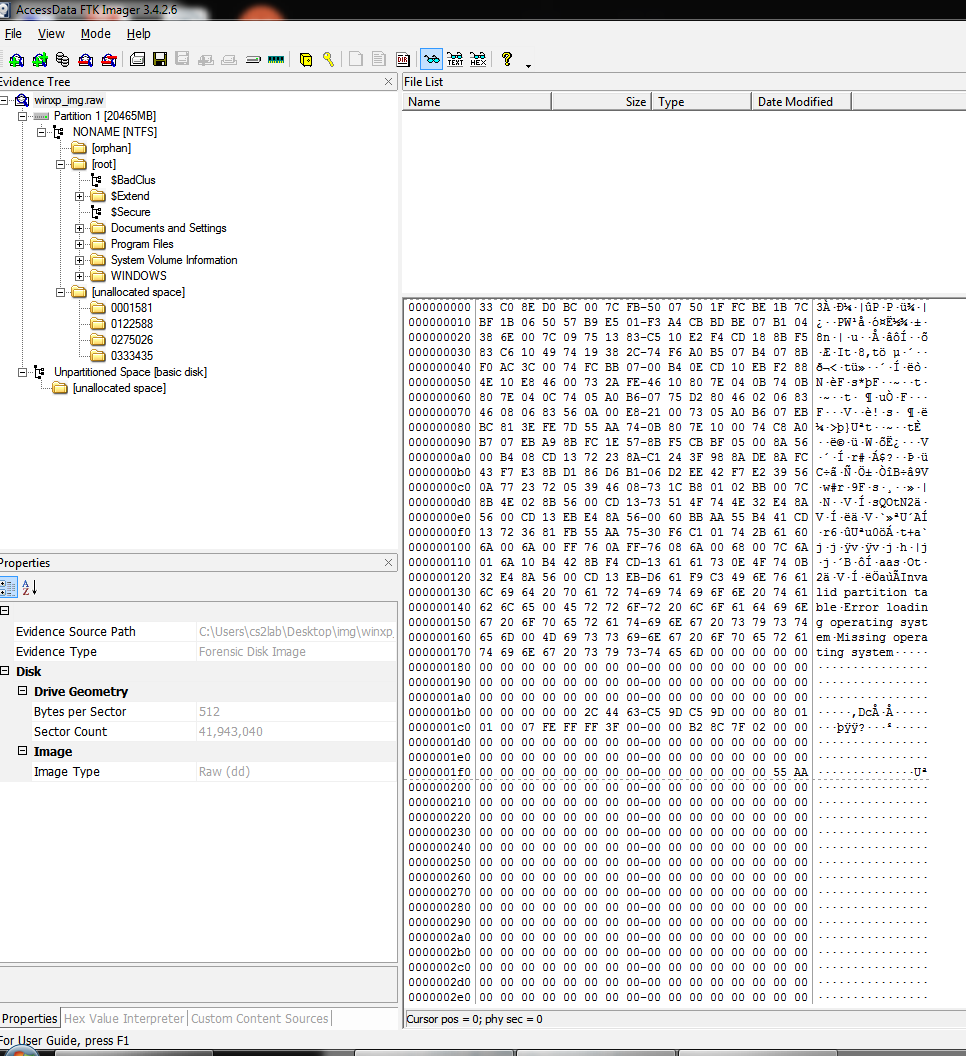


Figure-2: Initial step of FTK Imager.

* The date and time information when the SUBJECT’s system of the acquired raw image was last accessed by a user.

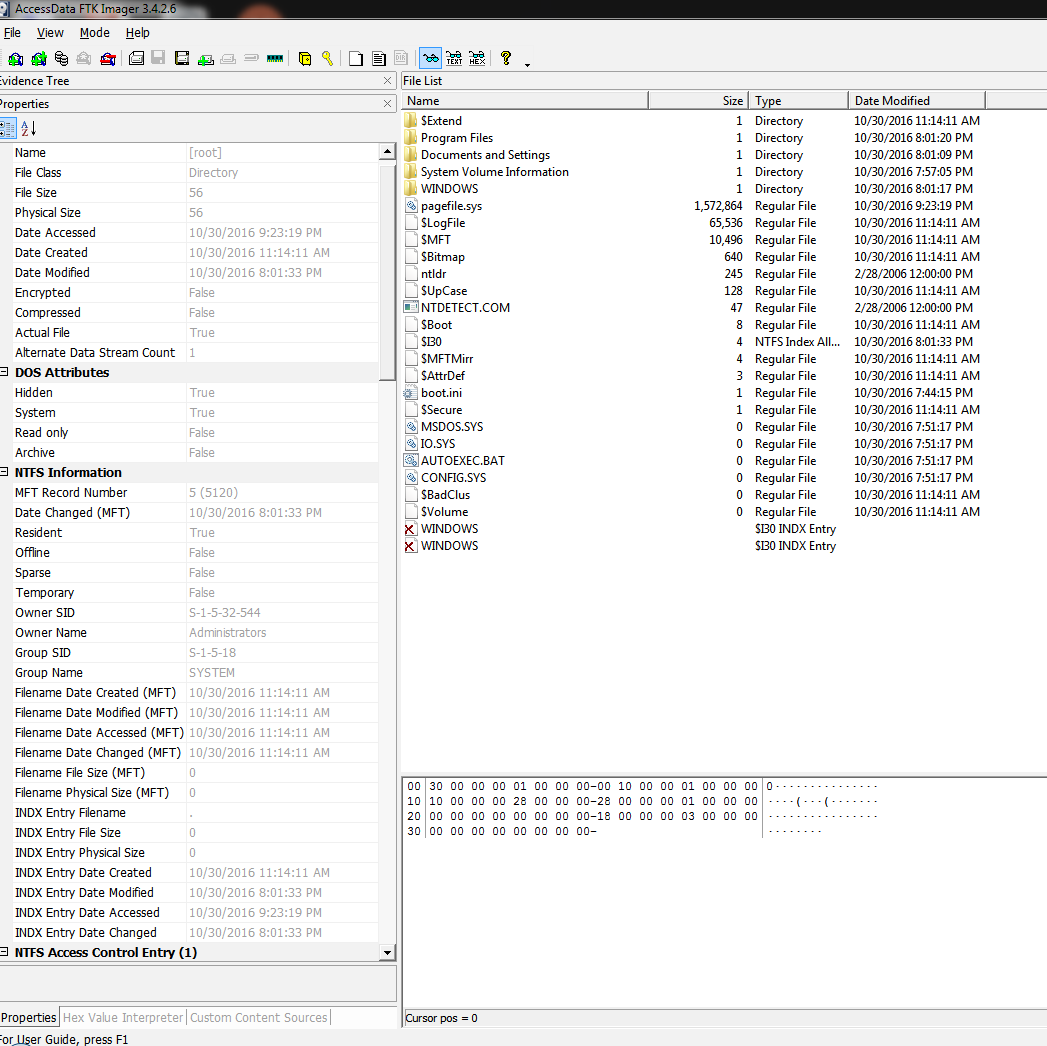


Figure-3: Time and date when SUBJECT’s system was accessed last.

By using this 2nd acquisition method, the FAT team was able to gather the SUBJECT’s system information from the ‘*winxp.vdi’* image file such as:

* SUBJECT’s hardware computer information: an Intel 32 bit processor,
* *Windows XP(NTFS 3.1)* as SUBJECT’s operating system,
* Serial number of the SUBJECT’s operation system: *9CBD-AFA8*
* *RegisterOwner* information of the SUBJECT’s system: *Christopher Hemsworth*
* several user accounts on the SUBJECT’s system,
* files (mainly empty files) discovered in the SUBJECT’s unallocated space,
* *2016-10-31 09:23:19PM* the last time the SUBJECT had accessed the SUBJECT’s system,

III) Starting the third process of acquisition on the digital copy of the SUBJECT’s evidence by using:

This third method of acquiring the *winxp.vdi* was to use Foremost tool from Kali to perform file carving of the SUBJECT’s virtual hard disk image.

* From the Kali command prompt, command used was:

*>foremost –i /…input path…/winxp.vdi –o /…output path…/foremost\_carving/*

Total files carved were 4085 files and from the results, there were ‘jpg’, ‘bmp’, ‘png’, ‘gif’, ‘.exe’, ‘zip’, ‘ole’, ‘htm’, ‘rif’, and ‘wmv’, see figure-4.

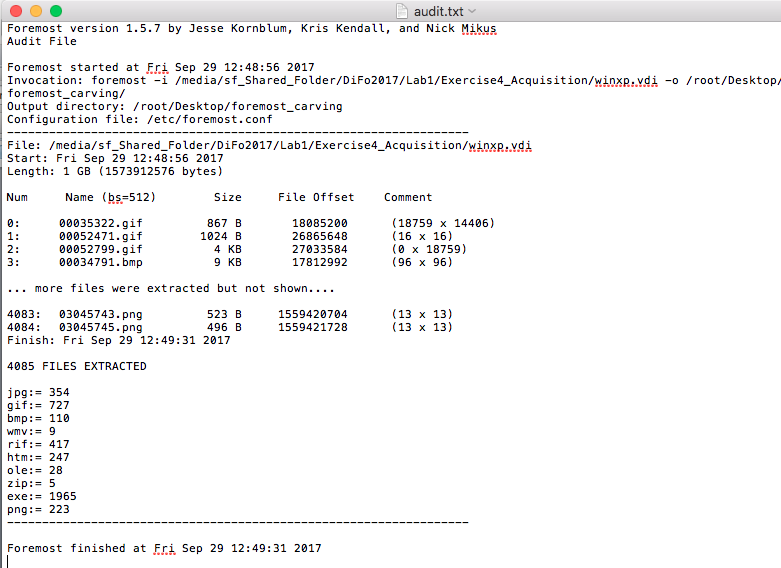
****

Figure-4: Foremost file carving results

**Examination**:

1. The examination started on 2017-09-29 at 09:00AM by the FAT team to acquire the SUBJECT’s system as raw format image, ‘*winxp\_img.raw*’.
2. FAT team was able to view the SUBJECT’s evidence.
3. The computer used to acquire the SUBJECT’s 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.
4. The sector information of the SUBJECT’s acquired evidence was:
5. - SUBJECT’s system sector count from FTK Imager was: *41943040* and bytes per sector was: *512*
6. - FAT team calculated the SUBJECT’s system sector:

41943040 \* 512 per sector = 2.147484e10 bytes

2.147484e10 bytes / 1024 bytes = 20971523.4 kilobytes  
20971523.4 kilobytes / 1024 kilobytes = 20480.0033metabytes

1. which confirmed the same as what FTK imager had provided: 20480MB (see figure-4) of the SUBJECT’s system.

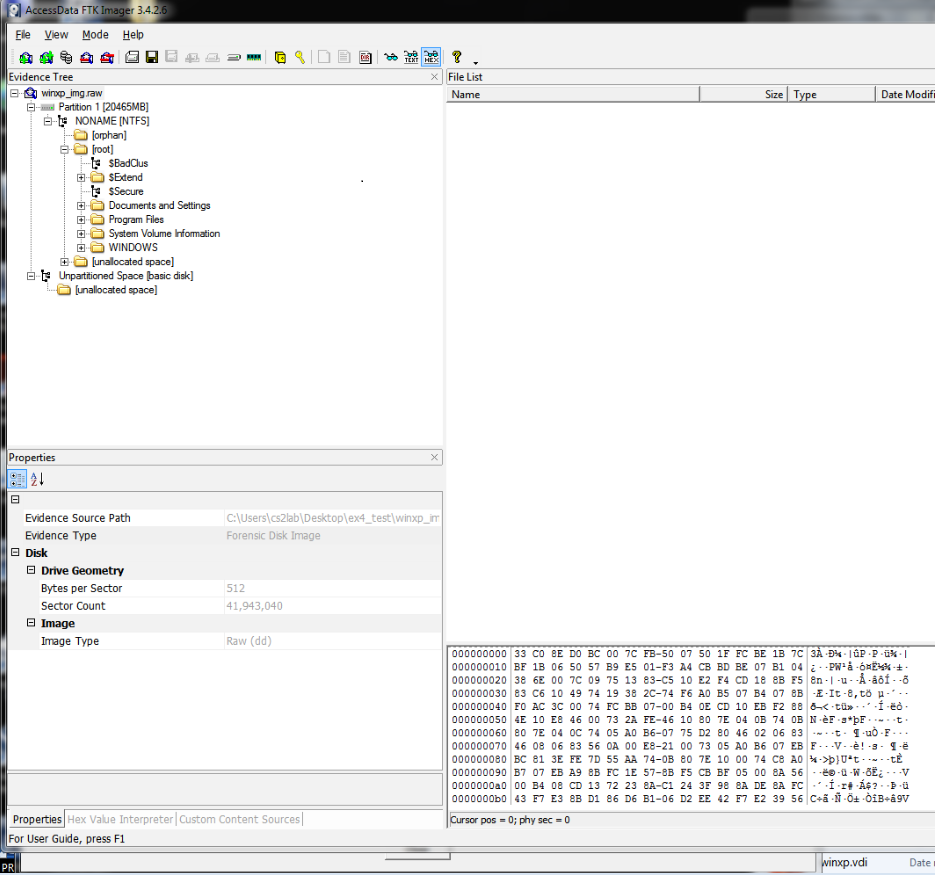


Figure-4: sector information from FTK Imager.

1. 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\_evidence.EO1’*. FTK Imager automatically generated the summary report of hash verification for us. From this FTK report, hash values were verified as matched.

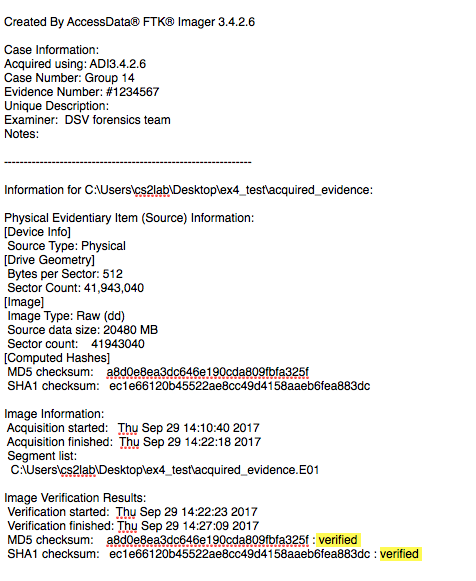


Figure-5: Verified hash values by FTK Imager summary report.

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

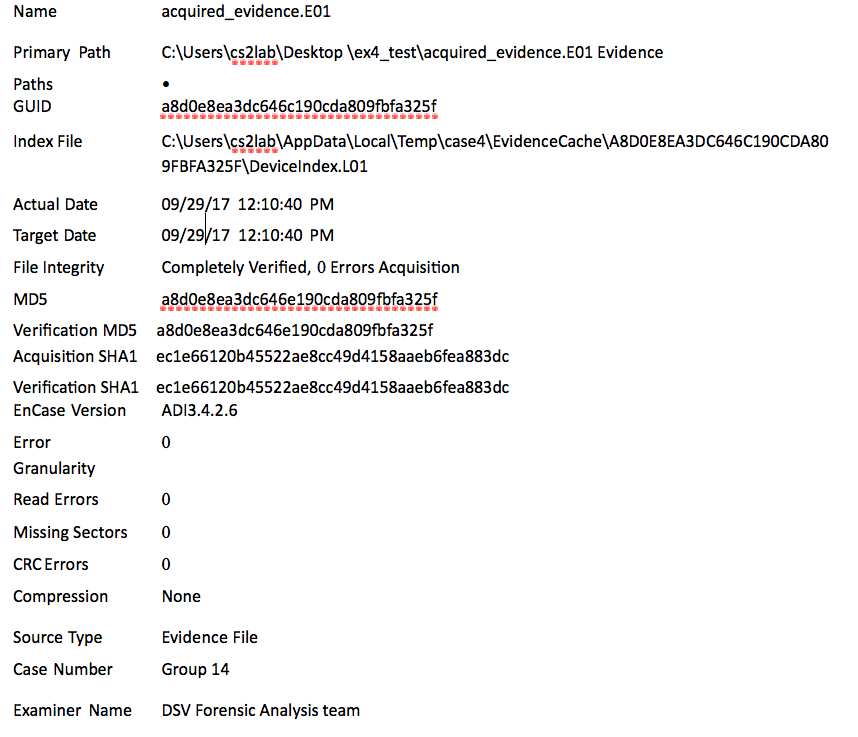


Figure-6: Verified hash values by EnCase summary report.

1. Extra evidence files were discovered during the examination phase. These extra evidence files were obtained from the FTK Imager by exporting ‘/root/Documents and Settings/Cookies’ directory, ‘Windows/System32/Config/SAM’, ‘Windows/System32/Config/Software’, and ‘Windows/System32/Config/System’ key files.
2. FAT team was able to discover the SUBJECT’s system hardware information from the *MatchingDEviceID* of the ‘Windows/System32/Config/System’ key file, see figure 7. It indicated it was an Intel 32bit processor.

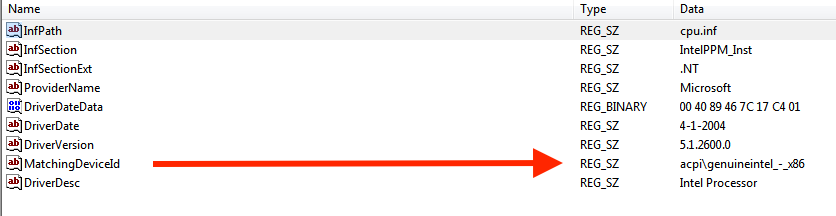


Figure-7: Subject’s hardware system information.

1. From the Software key file by using the AccessData Registory Viewer, FAT team discovered the SUBJECT’s registered owner name of the acquired image. The owner was ‘Christopher Hemsworth’ by inspecting the *RegisteredOwner* field from the Software key file, see See figure-8.

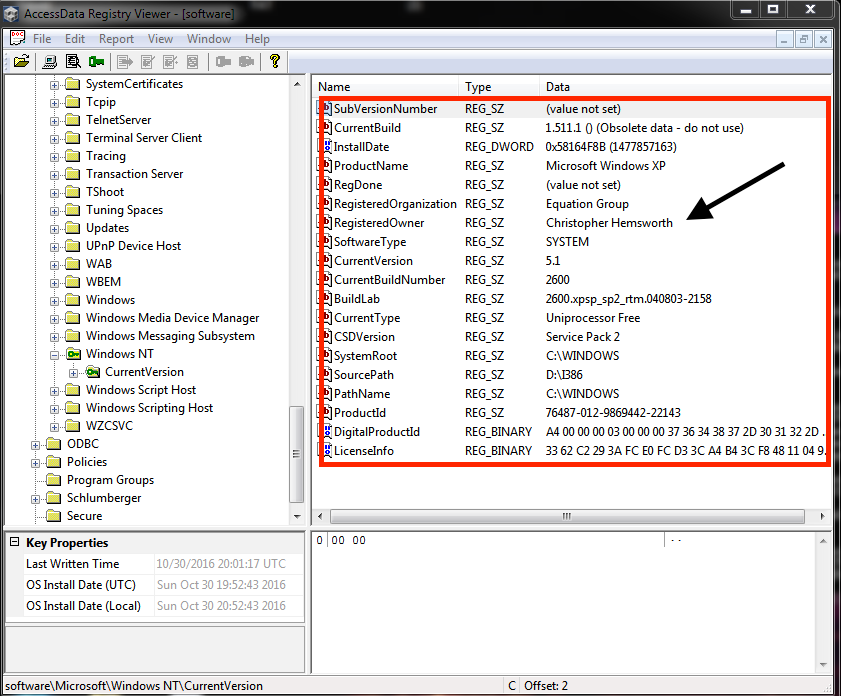


Figure-8: Subject’s registered owner name.

Additionally, FAT team found out what type of system the acquired image was. It was a Windows XP with Service Pack 2 installed onto the C drive. Also, there was another partition found which was the drive D and it contained the source of I386.

1. From the Cookies key file, a user account of ‘*Chris Hemsworth’* was found. Within this Cookies’ user account key file, there were directories with files that were inside ‘*Chris Hemsworth’* directory and the files were protected. FAT team was not able to open these files. These files were last accessed on 2016-10-30 at 21:03 PM. See figure-9 below.

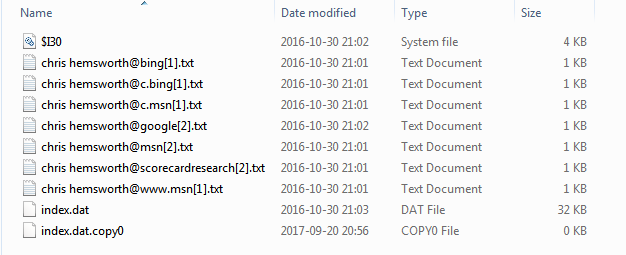


Figure-9: Cookies key file of ‘*Chris Hemsworth’* information.

1. From FTK Imager property tab of the SUBJECT’s evidence image of ‘*Chris Hemsworth’,* indicated that the SUBJECT had administrator’s privileges. See figure-10 below:

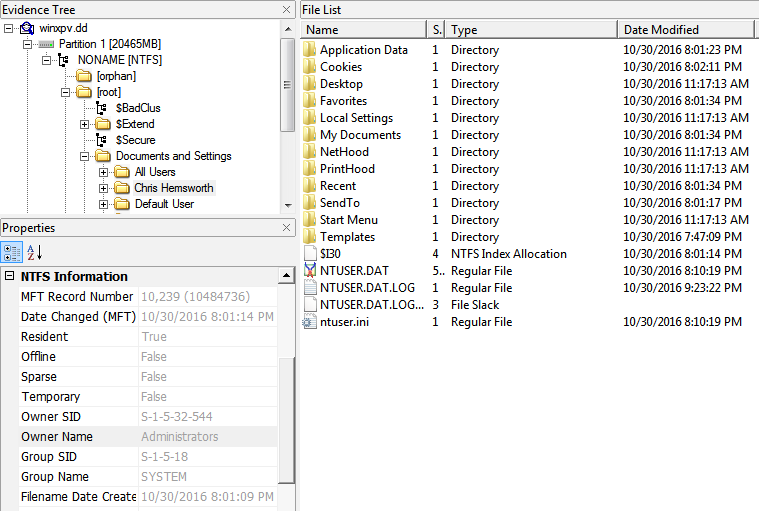


Figure-10: SUBJECT’s as administrator.

1. From SAM key file using AccessData Registry Viewer, FAT team discovered the other users on the SUBJECT’s system. See figure 11 below.

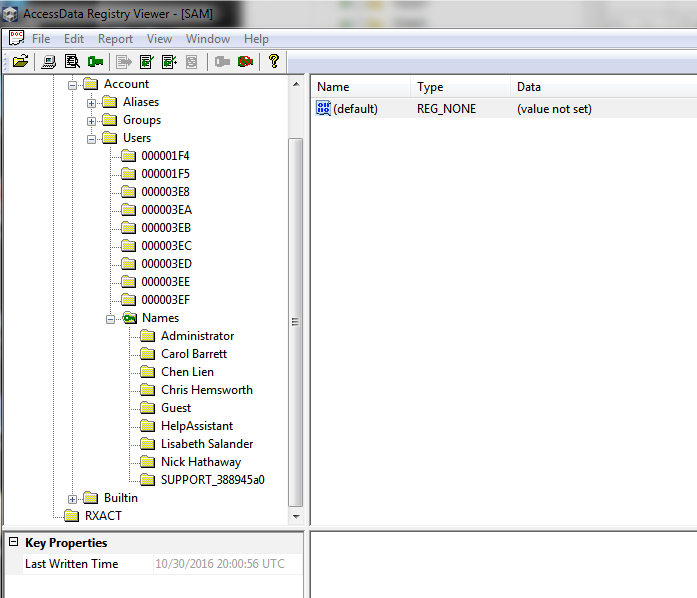


Figure-11: Other users’ accounts from SUBJECT’s system.

1. Additionally, FAT team discovered there were unallocated space from the SUBJECT’s evidence. The contents from this unallocated space were empty. See figure-12
2. FAT team was able to carve files from SUBJECT’s system using Foremost tool and discovered there were 4085 files. These 4085 files comprised of 354 jpeg files, 727 gif files, 110 bmp files,, videos, music, dynamic-link libraries (dll) and applications(.exe) from the SUBJECT’s evidence. See figure-13 from next page for more details.

There were 9 bmp files that FAT team could not access or opened them. These files might have been altered by the SUBJECT’s. Further investigation might be needed on these files.

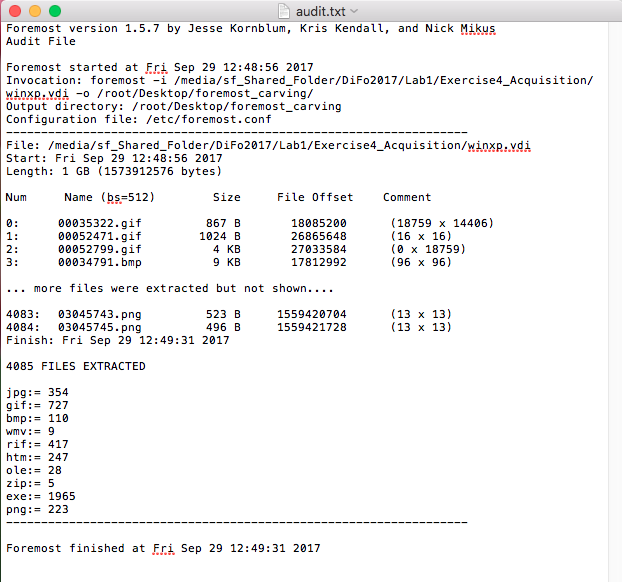


Figure-13: Foremost files carving result.

There were other bmp files which appeared to be corrupted by visual inspection such as file ‘*00578015.bmp’*, see figure-13 below.

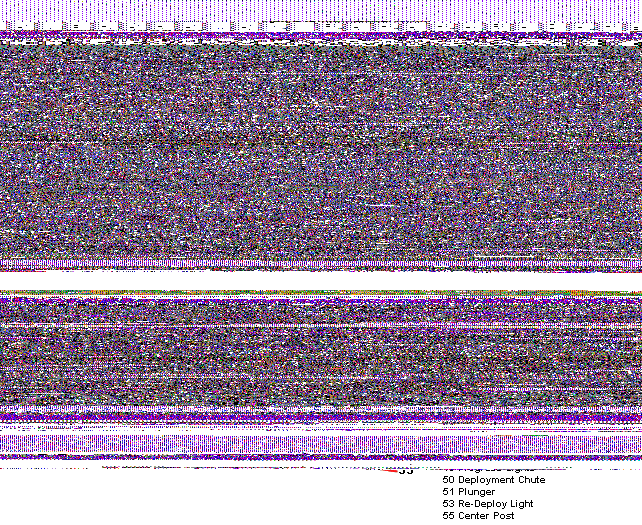


Figure-14: Corrupted bmp file.

**Documentation and reporting:**

1. This forensics report was written by Forensics Analysis Lab 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>.
2. During the examination phase, all proceedings pertaining to this investigation were noted in an Investigation Log. All actions with this methods used and results received were documented. Relevant findings to the case were highlighted and described in details. The investigation log was stored with the detail reports within the FAL security database.
3. The examination phase finished on 2017-10-01 at 16:00 PM.
4. A Computer Forensic Investigative Analysis Report (CFIAR) was created from the content of the Investigative Log on 2017/10/02 08:00AM - 16:00PM. The investigative process and the results were described to suit the audience of the report.

# Case Group 14 brief report

**REPORT OF Requested Windows Forensic Investigation**

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

*Police Investigator Jesper Bergman*

*San Francisco, CA, USA 94110*

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

*SUBJECT: Christopher Hemsworth*

*Case Number: 012345*

1. **Status: Closed.**

2. **Summary of Findings:**

Findings in this paragraph related to the image file of Oracle virtual hard disk, Model Samsung, Serial # 0123456789, provided to FAT by the police investigator Jesper Bergman.

* ?????

**3. Items Analyzed:**

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

012345 Image file: Oracle Virtual Hard Drive, Serial # *0123456789*

**4. Details of Findings:**

|  |
| --- |
| **Summary of evidence file: (case created and verified with EnCase and FTK Imager)** |
| **Image File Name:** *acquired\_evidence.EO1*  **Image Name** (computer name): *Equation\_8FF993*  **Image MD5 File Hash**: *c965a5e2236d60624c07c8233ed0aeb3*  **Image SHA1 File Hash**: *a8d7b2a8ebffc3905ab8b04edfe7e6fa92076fce*  **Full Serial Number:** 309CBDEF9CBDAFA8  **System Time Zone**: *(UTC + 01:00)Amsterdam, Berlin, Bern, Rome, Stockholm, Vienna*  **Number of Hard Disk Partition:** 2  **Partition Information:**  System Reserved:  C: NONAME[NTFS]; Allocated: 2.7 GB; Unallocated: 17.3 GB; SIZE: 20 GB  (Windows XP Operating System) |
| **Number of Sectors on Hard Disk:** 41,913,522  **Size of Sectors on Hard Disk:** 512 bytes  **Disk Size:** 21, 459,722,240 Bytes (20 GB)  **Unallocated:** 18,611,920,896 Bytes (17.3 GB)  **Allocated:** 2,847,801,344 Bytes (2.7 GB)  **Unused Disk Space:** 4,543,926 Bytes |
| **Boot options:** There is one entry in the Windows bootloader. (look for boot.ini file, content is what we need for boot info http://best-windows.vlaurie.com/boot-ini.html)  **Path:**  **Default:**  **Timeout:** 30 seconds  **Boot Device:**  **Name:**  **Device:**  **Bootloader Path:** |

Findings in this paragraph related to the image file of Oracle virtual hard disk, Model Samsung, Serial # 0123456789, provided to FAT by the police investigator Jesper Bergman.

**System Details:**

*1) The examined hard drive was found to contain a Microsoft® Windows® XP operating system with service pack 2.*

*2) The directory and file listing for the media was saved to the Microsoft® Access Database at the Forensics Analysis security lab.*

*3) 1414 image files (jpeg, gif, bmp and png) of what appeared to money laundering’s scheme and also some phonographic pictures.*

*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.*

DSV Forensic Security Lab Released by**:** Faik, Hossain, To

FAT Computer Forensic Examiners

**Appendix A: Chain of Custody**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Chain of Custody** | | | | |
| **Item #** | **Date/Time** | **Released by** (Signature & ID#) | **Received by** (Signature & ID#) | **Comments/Location** |
| 1 | 2017-09-28 16:00PM | Police Investigator Jesper Bergman | Forensics Analysis Lab Chief: Oliver | Evidence was in the form of Oracle virtual hard disk image ‘*winxp.vdi’* |
| 1 | 2017-09-29 09:00AM | Forensics Analysis Lab Chief: Oliver B. Popov | FAT team: MD Piar Hossain | Evidence was transferred to FAT database (ilearn2.dsv.sus.se) |
| 1 | 2017-09-29 09:05AM | FAT team | FAT team | Evidence obtained by the FAT team. |
| 1 | 2017-09-29 09:15AM | FAT team | FAT team | Evidence processed and investigation started |
| 1 | 2017-09-30 18:00PM | FAT team | FAT team | Evidence hashes verification after investigation and case closed. |