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.

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[1] 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:
    a. Md5 hash sum: *c965a5e2236d60624c07c8233ed0aeb3*
    b. 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.

[1] **http://md5deep.sourceforge.net/**

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 B. Popov	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.

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

I) Starting the first process of acquisition on the digital copy of the SUBJECT's evidence:

- 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.*

```
root@kali:~# dd if='/media/sf_Shared_Folder/DiFo2017/Lab1/Exercise4_Acquisition/
winxp.vdi' of='/media/sf_Shared_Folder/DiFo2017/Lab1/Exercise4_Acquisition/winxp
.dd'
3074048+0 records in
3074048+0 records out
1573912576 bytes (1.6 GB, 1.5 GiB) copied, 214.479 s, 7.3 MB/s
root@kali:~#
```

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]'* message when FAT team opened both images from FTK imager. This first method was not helpful for FAT team since they were not able to proceed further. So FAT team decided to persuade two other methods. See (II and III) below.

II) Starting the second process of acquisition on the digital copy of the SUBJECT's evidence:

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.exe and sha1deep64.exe:
  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:

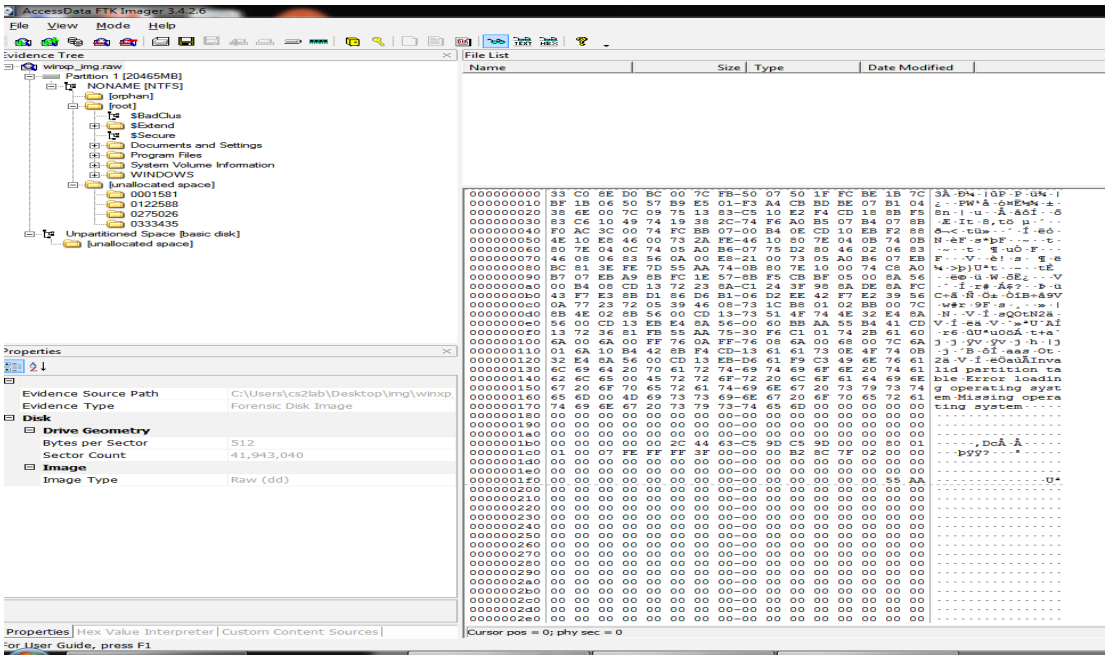


Figure-2: Initial step of FTK Imager.

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

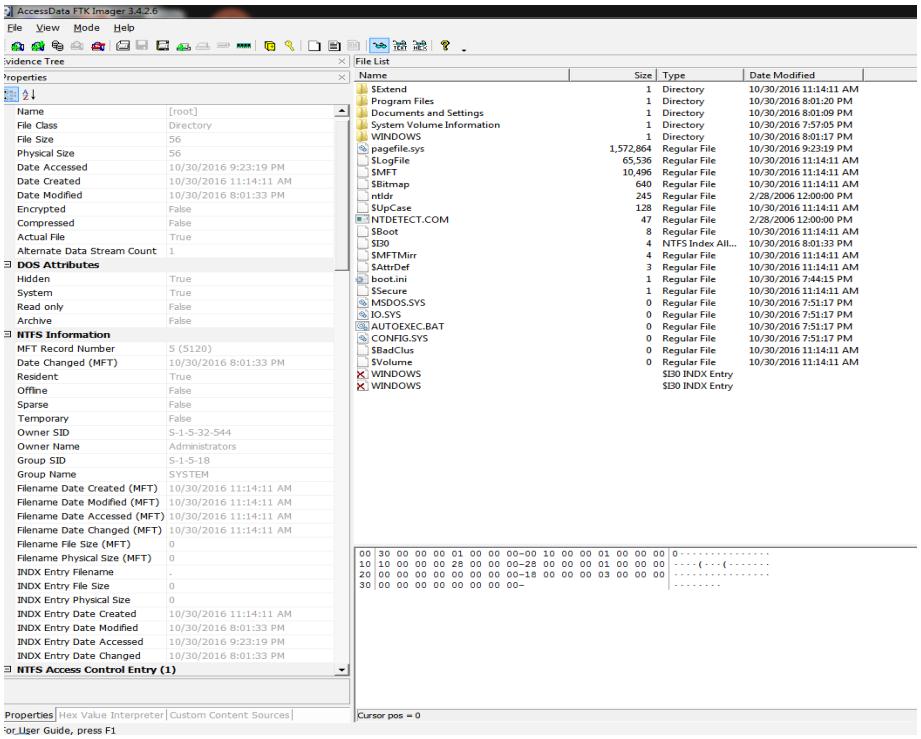


Figure-3: Time and date when SUBJECT's system was accessed last.

By using this 2nd acquisition method, the FAT team was able to gather the SUBJECT's system information from the acquired raw image evidende 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,
- 25 files were discovered in the SUBJECT's unallocated space,
- *2016-10-31 09:23:19PM* was the last time the SUBJECT had accessed on the SUBJECT's system,

III) Starting the third process of acquisition on the digital copy of the SUBJECT's evidence:
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' files, see figure-4.

audit.txt

```
Foremost version 1.5.7 by Jesse Kornblum, Kris Kendall, and Nick Mikus
Audit File

Foremost started at Fri Sep 29 12:48:56 2017
Invocation: foremost -i /media/sf_Shared_Folder/DiFo2017/Lab1/Exercise4_Acquisition/winxp.vdi -o /root/Desktop/
foremost_carving/
Output directory: /root/Desktop/foremost_carving
Configuration file: /etc/foremost.conf
------------------------------------------------------------------
File: /media/sf_Shared_Folder/DiFo2017/Lab1/Exercise4_Acquisition/winxp.vdi
Start: Fri Sep 29 12:48:56 2017
Length: 1 GB (1573912576 bytes)

Num      Name (bs=512)        Size     File Offset    Comment

0:      00035322.gif         867 B       18085200      (18759 x 14406)
1:      00052471.gif        1024 B       26865648      (16 x 16)
2:      00052799.gif          4 KB       27033584      (0 x 18759)
3:      00034791.bmp          9 KB       17812992      (96 x 96)

... more files were extracted but not shown....

4083:   03045743.png         523 B     1559420704      (13 x 13)
4084:   03045745.png         496 B     1559421728      (13 x 13)
Finish: Fri Sep 29 12:49:31 2017

4085 FILES EXTRACTED

jpg:= 354
gif:= 727
bmp:= 110
wmv:= 9
rif:= 417
htm:= 247
ole:= 28
zip:= 5
exe:= 1965
png:= 223
------------------------------------------------------------------

Foremost finished at Fri Sep 29 12:49:31 2017
```

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 of 16GB, for 64 bit operating system. The operating system was Windows 7.

4) The sector information of the SUBJECT's acquired evidence was:

   a. SUBJECT's system sector count from FTK Imager was: *41943040* and bytes per sector was: *512*

   b. 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

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

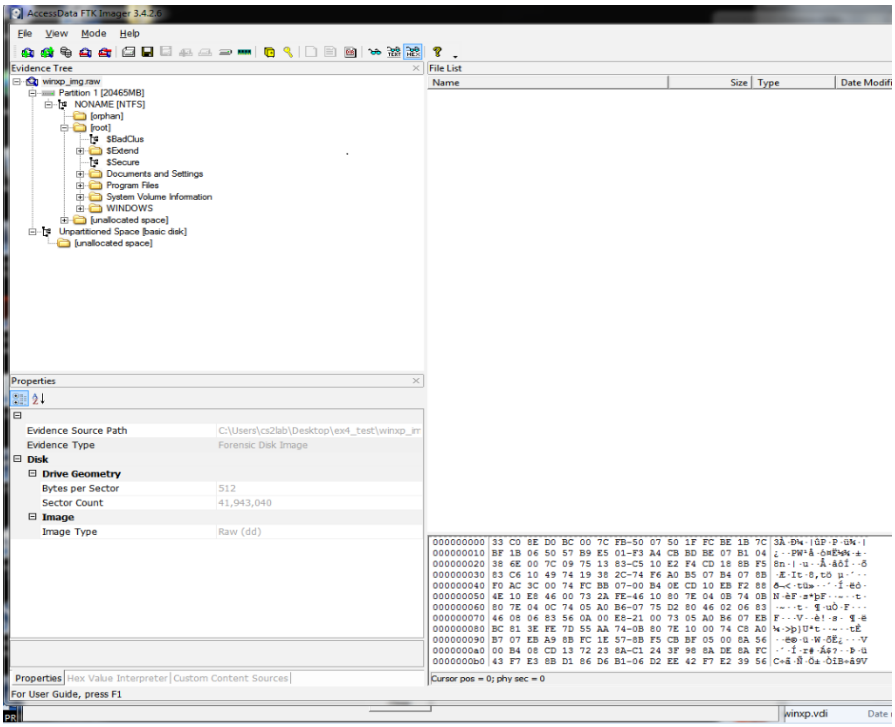


Figure-4: sector information from FTK Imager.

5) 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. From this FTK report, hash values were verified as matched. See figure-5 below.

```
Created By AccessData® FTK® Imager 3.4.2.6

Case Information:
Acquired using: ADI3.4.2.6
Case Number: Group 14
Evidence Number: #1234567
Unique Description:
Examiner:  DSV forensics team
Notes:

---------------------------------------------------------------

Information for C:\Users\cs2lab\Desktop\ex4_test\acquired_evidence:

Physical Evidentiary Item (Source) Information:
[Device Info]
 Source Type: Physical
[Drive Geometry]
 Bytes per Sector: 512
 Sector Count: 41,943,040
[Image]
 Image Type: Raw (dd)
 Source data size: 20480 MB
 Sector count:   41943040
[Computed Hashes]
 MD5 checksum:   a8d0e8ea3dc646e190cda809fbfa325f
 SHA1 checksum:  ec1e66120b45522ae8cc49d4158aaeb6fea883dc

Image Information:
 Acquisition started:  Thu Sep 29 14:10:40 2017
 Acquisition finished: Thu Sep 29 14:22:18 2017
 Segment list:
  C:\Users\cs2lab\Desktop\ex4_test\acquired_evidence.E01

Image Verification Results:
 Verification started:  Thu Sep 29 14:22:23 2017
 Verification finished: Thu Sep 29 14:27:09 2017
 MD5 checksum:   a8d0e8ea3dc646e190cda809fbfa325f : verified
 SHA1 checksum:  ec1e66120b45522ae8cc49d4158aaeb6fea883dc : verified
```

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

6) Using EnCase, we added the '*acquired_evidence.EO1'* and it generated a summary report which matched the same hash values verified by FTK Imager. See figure-6 below.

Name	acquired_evidence.E01
Primary Path	C:\Users\cs2lab\Desktop \ex4_test\acquired_evidence.E01 Evidence
Paths	•
GUID	a8d0e8ea3dc646c190cda809fbfa325f
Index File	C:\Users\cs2lab\AppData\Local\Temp\case4\EvidenceCache\A8D0E8EA3DC646C190CDA80 9FBFA325F\DeviceIndex.L01
Actual Date	09/29/17 12:10:40 PM
Target Date	09/29/17 12:10:40 PM
File Integrity	Completely Verified, 0 Errors Acquisition
MD5	a8d0e8ea3dc646e190cda809fbfa325f
Verification MD5	a8d0e8ea3dc646e190cda809fbfa325f
Acquisition SHA1	ec1e66120b45522ae8cc49d4158aaeb6fea883dc
Verification SHA1	ec1e66120b45522ae8cc49d4158aaeb6fea883dc
EnCase Version	ADI3.4.2.6
Error Granularity	0
Read Errors	0
Missing Sectors	0
CRC Errors	0
Compression	None
Source Type	Evidence File
Case Number	Group 14
Examiner Name	DSV Forensic Analysis team

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

7) 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' registry key files.

   a. FAT team was able to discover the SUBJECT's system hardware information from the *MatchingDEviceID* of the 'Windows/System32/Config/System' registry key file, see figure 7. It indicated it was an Intel 32bit processor.

Name	Type	Data
InfPath	REG_SZ	cpu.inf
InfSection	REG_SZ	IntelPPM_Inst
InfSectionExt	REG_SZ	.NT
ProviderName	REG_SZ	Microsoft
DriverDateData	REG_BINARY	00 40 89 46 7C 17 C4 01
DriverDate	REG_SZ	4-1-2004
DriverVersion	REG_SZ	5.1.2600.0
MatchingDeviceId	REG_SZ	acpi\genuineintel_-_x86
DriverDesc	REG_SZ	Intel Processor

Figure-7: Subject's hardware system information.

   b. From the Software registry 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 registry key file, see See figure-8.

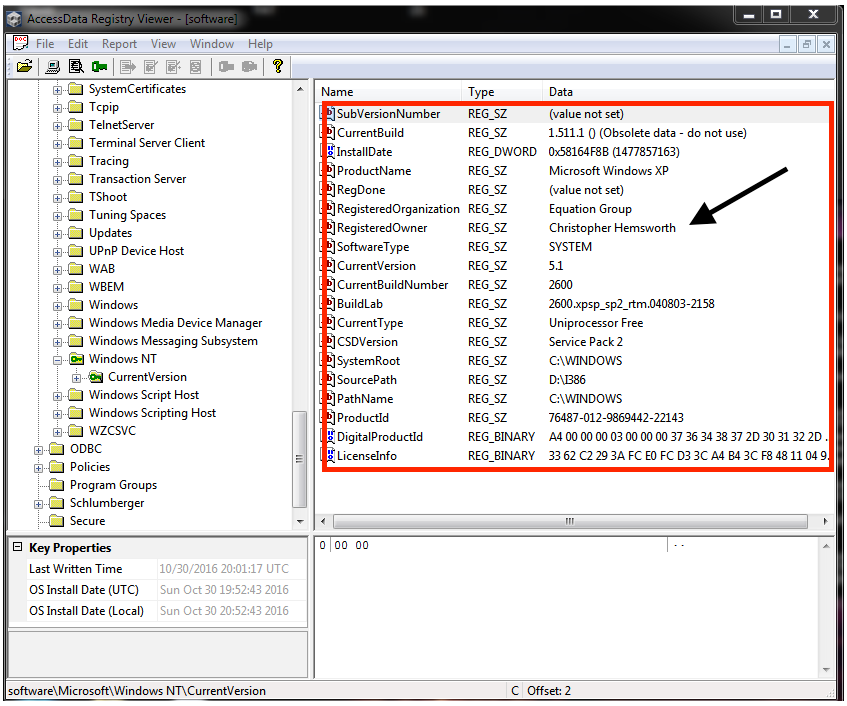
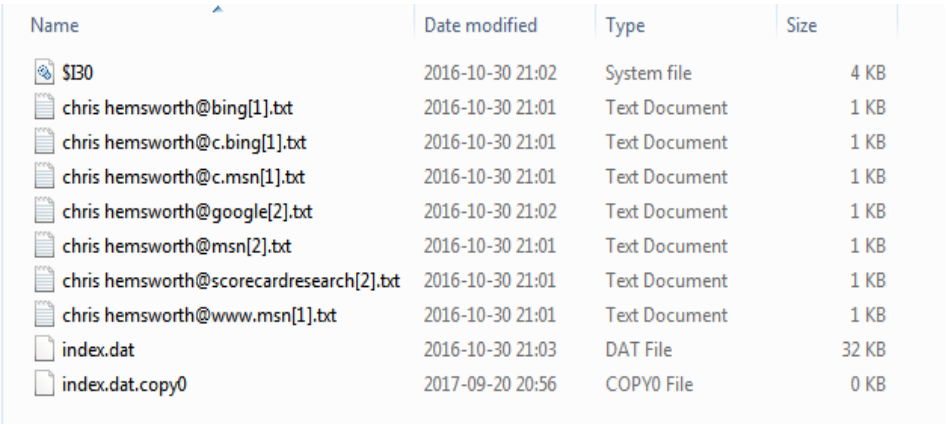


Figure-8: Subject's registered owner name.

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 drive found which was the drive D and it contained the source of I386.

c. From the Cookies registry key file, a user account of '*Chris Hemsworth'* was found. Within this Cookies' user account registry 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.



Name	Date modified	Type	Size
$I30	2016-10-30 21:02	System file	4 KB
chris hemsworth@bing[1].txt	2016-10-30 21:01	Text Document	1 KB
chris hemsworth@c.bing[1].txt	2016-10-30 21:01	Text Document	1 KB
chris hemsworth@c.msn[1].txt	2016-10-30 21:01	Text Document	1 KB
chris hemsworth@google[2].txt	2016-10-30 21:02	Text Document	1 KB
chris hemsworth@msn[2].txt	2016-10-30 21:01	Text Document	1 KB
chris hemsworth@scorecardresearch[2].txt	2016-10-30 21:01	Text Document	1 KB
chris hemsworth@www.msn[1].txt	2016-10-30 21:01	Text Document	1 KB
index.dat	2016-10-30 21:03	DAT File	32 KB
index.dat.copy0	2017-09-20 20:56	COPY0 File	0 KB

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

d. 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:

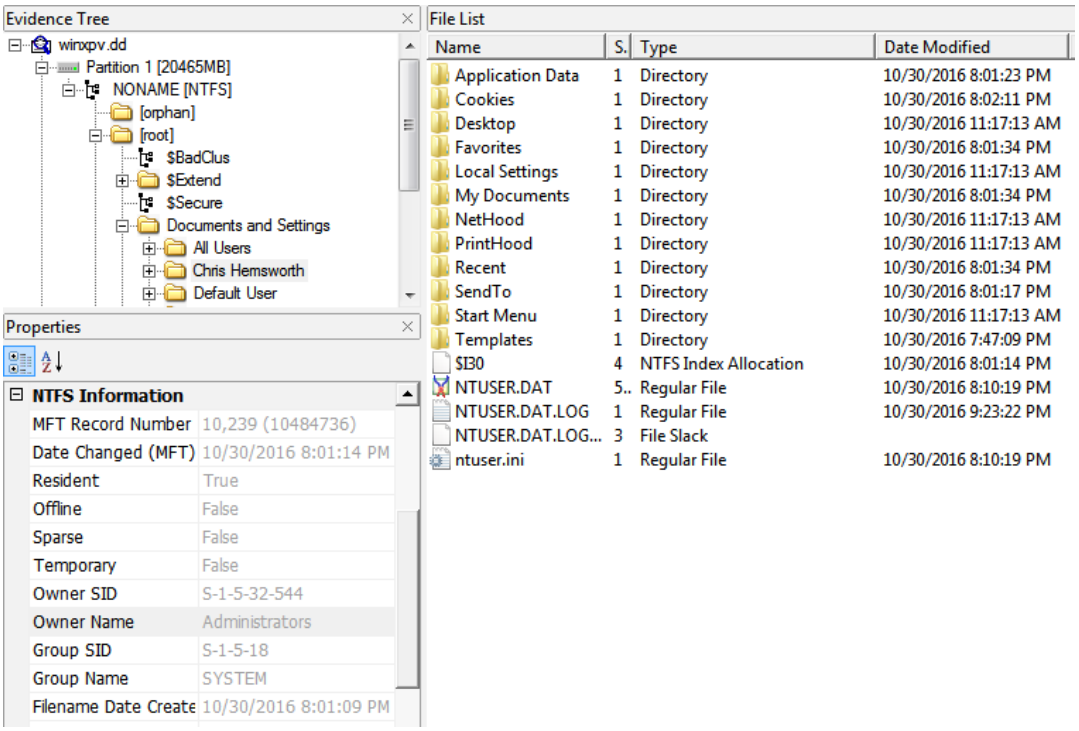


Figure-10: SUBJECT's as administrator.

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

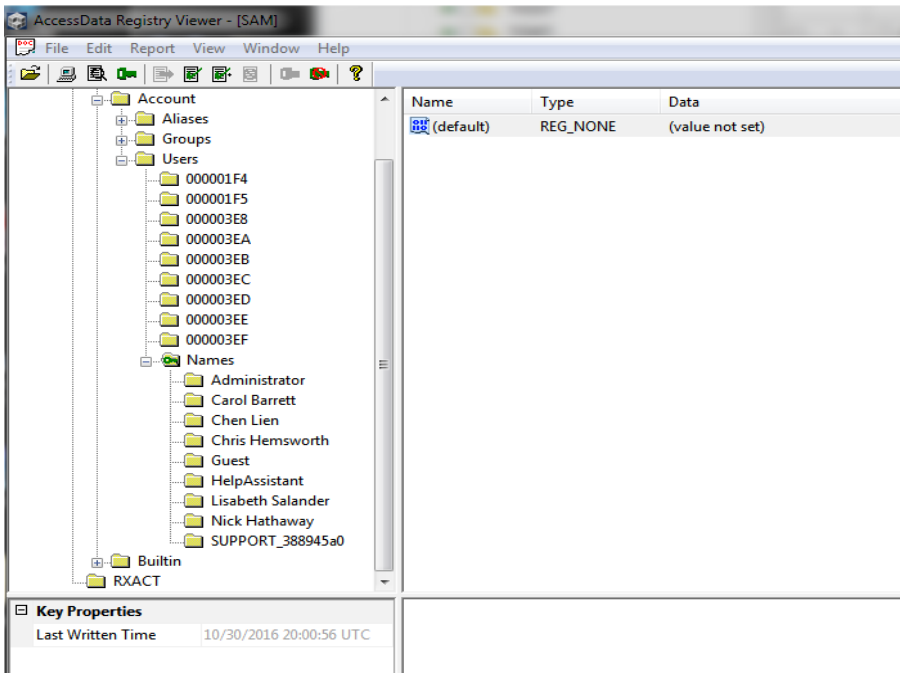


Figure-11: Other users' accounts from SUBJECT's system.

8) Additionally, FAT team discovered there was unallocated space from the SUBJECT's evidence. The contents from this unallocated space was not empty. 25 files were discovered by using recover feature from EnCase. See figure-12 on the next page.

A8D0E8EA3DC646C190CDA809FBFA325F	Folder	--
0001	Folder	--
00000001_Volume Slack_FO-559_PS-41913584+47.atn	Document	465 bytes
00000002_Volume Slack_FO-578_PS-41913584+66.ico	Windo...image	446 bytes
00000003_Volume Slack_FO-579_PS-41913584+67.aco	Document	445 bytes
00000004_Volume Slack_FO-646_PS-41913584+134.mp3	MP3 audio	378 bytes
00000005_Unallocated Clusters_FO-35782665_PS-85159+9.mp3	MP3 audio	10.5 MB
00000006_Unallocated Clusters_FO-35782686_PS-85159+30.ntf	Document	10.5 MB
00000007_Unallocated Clusters_FO-35782696_PS-85159+40.sys	Document	10.5 MB
00000008_Unallocated Clusters_FO-35782778_PS-85159+122.ico	Windo...image	10.5 MB
00000009_Unallocated Clusters_FO-35782779_PS-85159+123.aco	Document	10.5 MB
00000010_Unallocated Clusters_FO-35782780_PS-85159+124.emf	Document	10.5 MB
00000011_Unallocated Clusters_FO-35783986_PS-85161+306.sys	Document	10.5 MB
00000012_Unallocated Clusters_FO-35786746_PS-85166+506.mp3	MP3 audio	10.5 MB
00000013_Unallocated Clusters_FO-35786622_PS-85166+382.ntf	Document	10.5 MB
00000014_Unallocated Clusters_FO-35786652_PS-85166+412.sys	Document	10.5 MB
00000015_Unallocated Clusters_FO-35786762_PS-85167+10.ico	Windo...image	10.5 MB
00000016_Unallocated Clusters_FO-35786763_PS-85167+11.aco	Document	10.5 MB
00000017_Unallocated Clusters_FO-35786764_PS-85167+12.emf	Document	10.5 MB
00000018_Unallocated Clusters_FO-35784192_PS-85162+0.mui	Document	10.5 MB
00000019_Unallocated Clusters_FO-35787768_PS-85168+504.sys	Document	10.5 MB
00000020_Unallocated Clusters_FO-35790842_PS-85174+506.mp3	MP3 audio	10.5 MB
00000021_Unallocated Clusters_FO-35790718_PS-85174+382.ntf	Document	10.5 MB
00000022_Unallocated Clusters_FO-35790748_PS-85174+412.sys	Document	10.5 MB
00000023_Unallocated Clusters_FO-35790858_PS-85175+10.ico	Windo...image	10.5 MB
00000024_Unallocated Clusters_FO-35790859_PS-85175+11.aco	Document	10.5 MB
00000025_Unallocated Clusters_FO-35790860_PS-85175+12.emf	Document	10.5 MB
chris_admin.PNG	PNG image	69 KB

Figure-12: Unallocated cluster.

9) 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, 9 wmv (video), 247 html, 28 ole, 5 zip,417, 417 rif, 223 png and 1965 applications(.exe) from the SUBJECT's evidence. See figure-below for more details.

audit.txt

```
Foremost version 1.5.7 by Jesse Kornblum, Kris Kendall, and Nick Mikus
Audit File

Foremost started at Fri Sep 29 12:48:56 2017
Invocation: foremost -i /media/sf_Shared_Folder/DiFo2017/Lab1/Exercise4_Acquisition/
winxp.vdi -o /root/Desktop/foremost_carving/
Output directory: /root/Desktop/foremost_carving
Configuration file: /etc/foremost.conf
------------------------------------------------------------------
File: /media/sf_Shared_Folder/DiFo2017/Lab1/Exercise4_Acquisition/winxp.vdi
Start: Fri Sep 29 12:48:56 2017
Length: 1 GB (1573912576 bytes)

Num      Name (bs=512)         Size      File Offset     Comment

0:      00035322.gif          867 B        18085200       (18759 x 14406)
1:      00052471.gif         1024 B        26865648       (16 x 16)
2:      00052799.gif            4 KB       27033584       (0 x 18759)
3:      00034791.bmp            9 KB       17812992       (96 x 96)

... more files were extracted but not shown....

4083:   03045743.png          523 B      1559420704       (13 x 13)
4084:   03045745.png          496 B      1559421728       (13 x 13)
Finish: Fri Sep 29 12:49:31 2017

4085 FILES EXTRACTED

jpg:= 354
gif:= 727
bmp:= 110
wmv:= 9
rif:= 417
htm:= 247
ole:= 28
zip:= 5
exe:= 1965
png:= 223
------------------------------------------------------------------

Foremost finished at Fri Sep 29 12:49:31 2017
```

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.

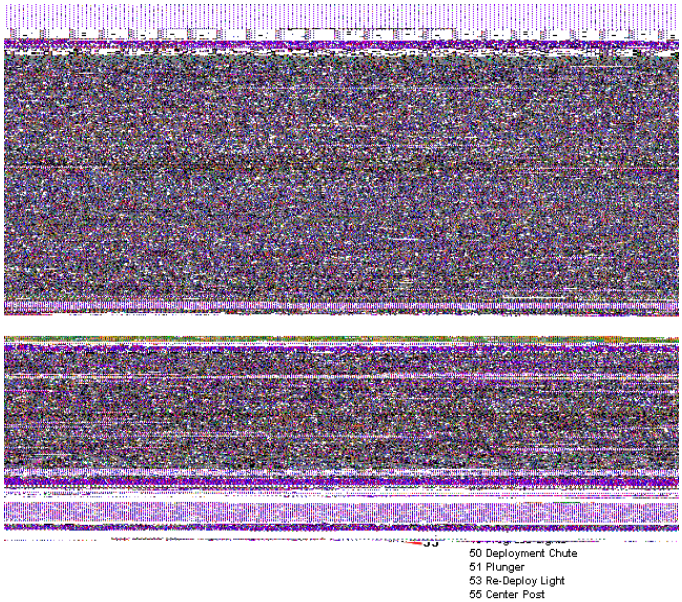


Figure-14: Corrupted bmp file.

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.

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. Also, FAT used Good_CFIAR_2015.pdf from the FAIL team for guidance to complete this forensic report.

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 report related to the image file of Oracle virtual hard disk, 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**: *Pacific Standard Time* **Number of Hard Disk Partition:** 2 **Partition Information:** 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 was one entry in the Windows bootloader. **Path:** C:\boot.ini **Default:** partition(0)\Windows [Operating System] **Timeout:** 30 seconds **Boot Device:** C drive **Name:** Microsoft Windows XP Professional **Bootloader Path:** C:\boot.ini

Findings in this report 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 acquired_evidence file contained the representation of a storage device running Windows XP Professional operation system:
   a. Program Files folder containing standard Microsoft applications.

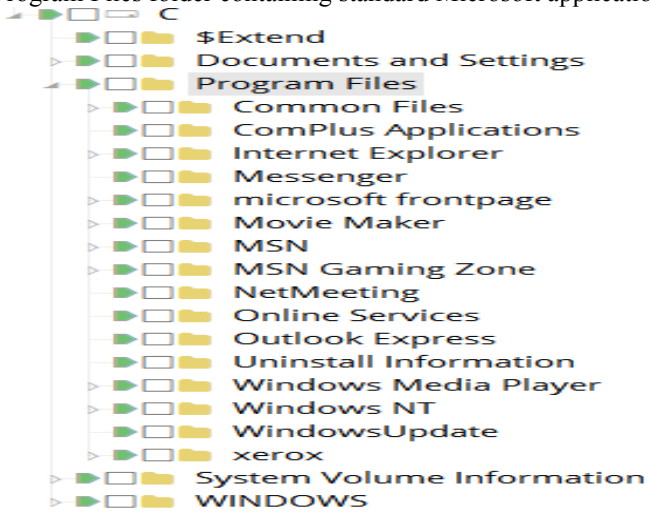


Figure-15: Microsoft applications installed.

   b. Timezone was found from 'Windows/System32/Config/System' registry key file:

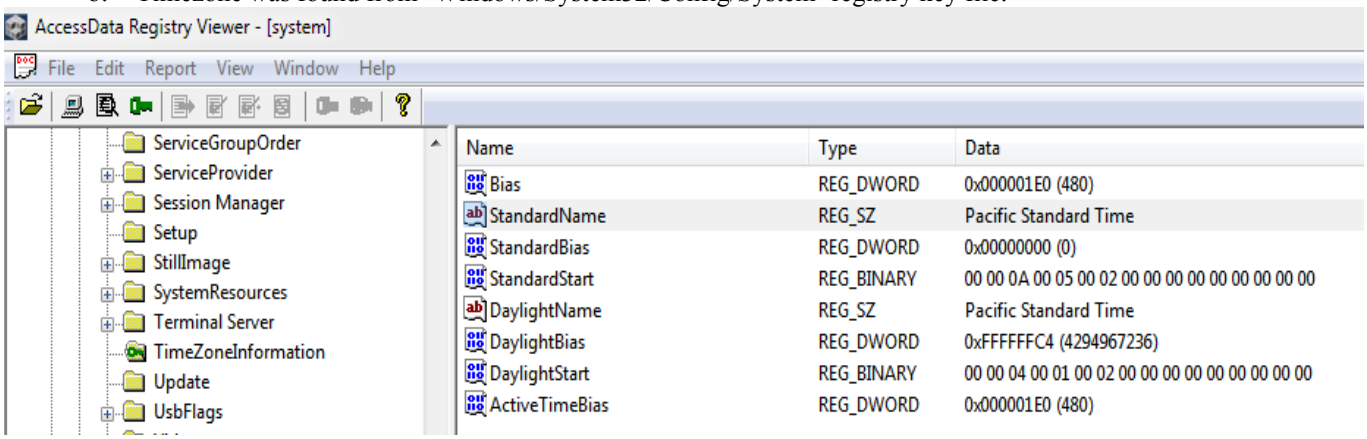


Figure-16: Timezone registry key file

   c. Windows XP was the operating system installed on the SUBJECT's machine, see figure-17 below.

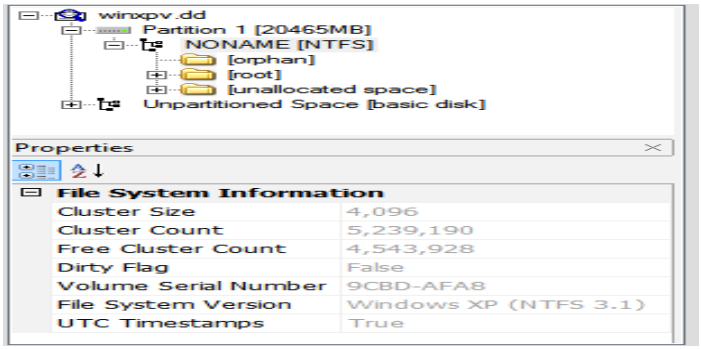


Figure-17: Windows XP

2. External devices attached to acquired_evidence file were discovered:

a. IDE and USB found from 'Windows/System32/Config/System/IDE' registry key file, see figure-18
   i. DiskQEMU_HARDDISK_____2.1.2____
   ii. USB

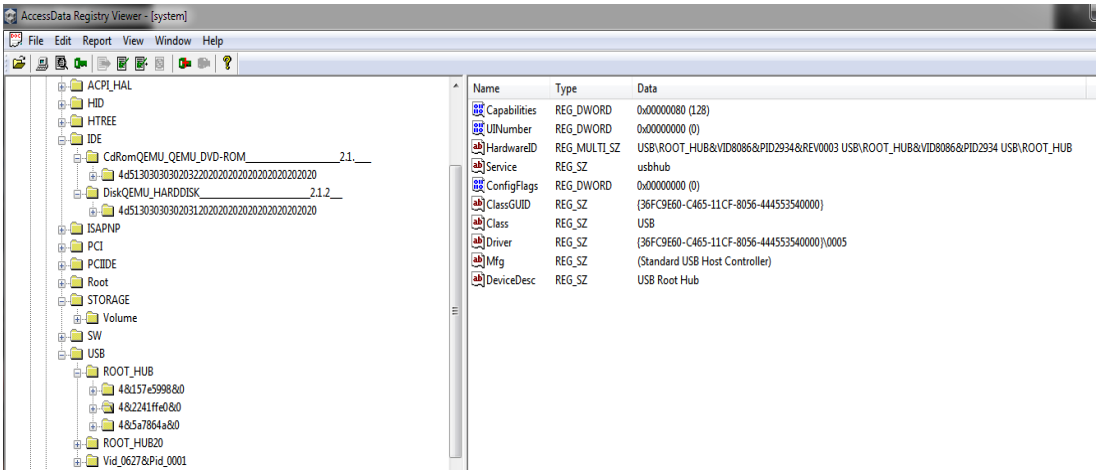


Figure-18: IDE and USB

3. DHCP service was discovered from the acquired_evidence file using 'Windows/System32/Config/System/TCPIP{77C3AEF2-0BB2-4150-9E91-9110E06472DD}' registry key file:

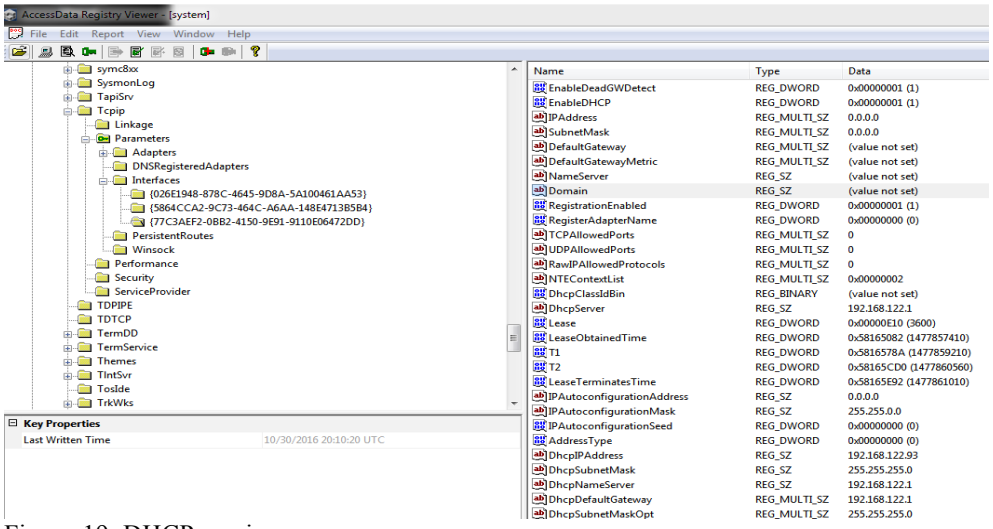


Figure-19: DHCP service

4. WIFI access using WPA service was discovered from 'Windows/System32/Config/System/WPA' registry key file:

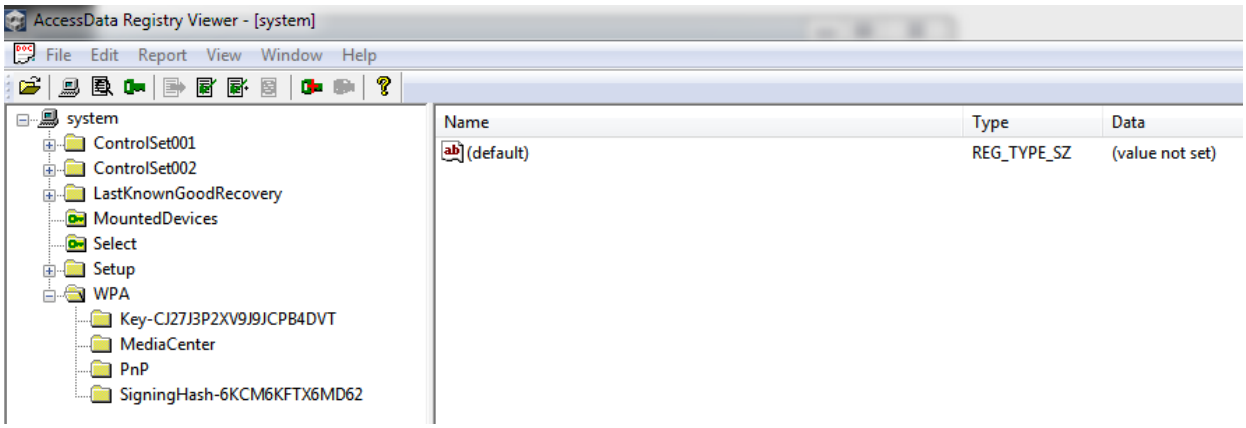


Figure-20: WIFI using WPA service

5. Last access date and time of acquired_evidence by the SUBJECT was: 2016/10/30 09:23PM from FTK Imager on the c:/root/pagefile.sys file:

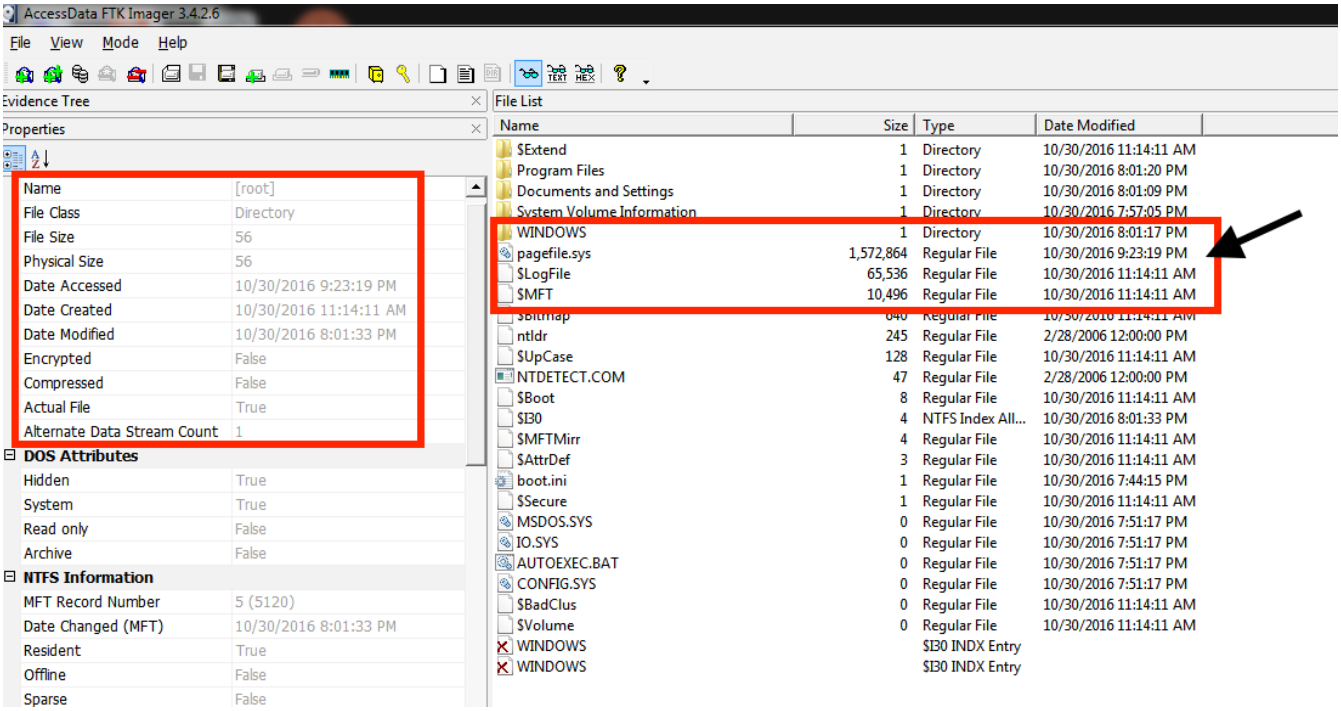


Figure-21: SUBJECT last access time.

6. Other users from the SUBJECT's acquired_evidence were found. They were:
Carol Barrett, Chen Lien, Guest, Help Assistant, Lisabeth Salander, Nick Hathaway and SUPPORT_388945a0.

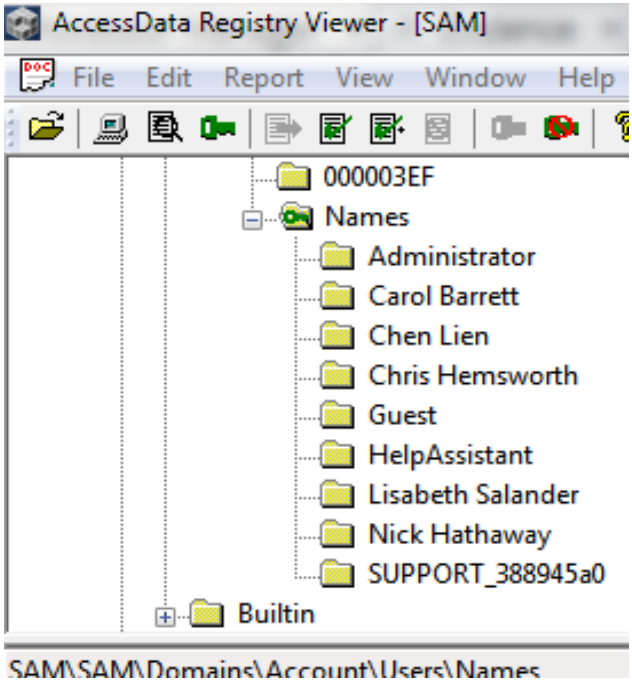


Figure-22: Other users

These other users last access time on the SUBJECT's system was the same as Chris Hemsworth 2016/10/30 20:00PM.

a) Five bmp files associated to these other five users' accounts were discovered from C:/Documents and Settings/All Users/Application Data/Microsoft/User Account Pictures/:

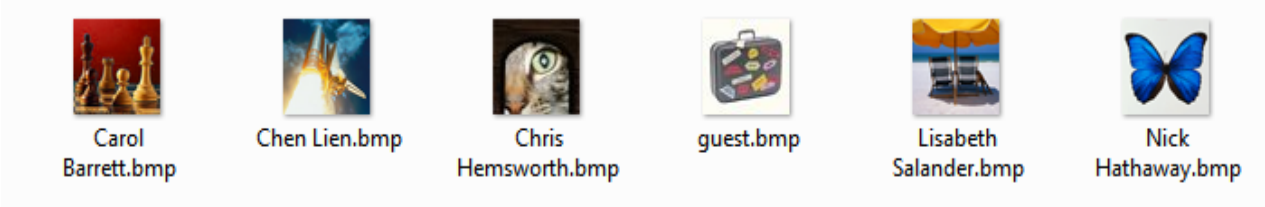


Figure-23: User Account Pictures.

7. Unallocated cluster was discovered from SUBJECT's acquired_evidence image. By using EnCase, FAT was able to recovered 210MB data comprised of 25 files found.

A8D0E8EA3DC646C190CDA809FBFA325F	Folder	--
0001	Folder	--
00000001_Volume Slack_FO-559_PS-41913584+47.atn	Document	465 bytes
00000002_Volume Slack_FO-578_PS-41913584+66.ico	Windo...image	446 bytes
00000003_Volume Slack_FO-579_PS-41913584+67.aco	Document	445 bytes
00000004_Volume Slack_FO-646_PS-41913584+134.mp3	MP3 audio	378 bytes
00000005_Unallocated Clusters_FO-35782665_PS-85159+9.mp3	MP3 audio	10.5 MB
00000006_Unallocated Clusters_FO-35782686_PS-85159+30.ntf	Document	10.5 MB
00000007_Unallocated Clusters_FO-35782696_PS-85159+40.sys	Document	10.5 MB
00000008_Unallocated Clusters_FO-35782778_PS-85159+122.ico	Windo...image	10.5 MB
00000009_Unallocated Clusters_FO-35782779_PS-85159+123.aco	Document	10.5 MB
00000010_Unallocated Clusters_FO-35782780_PS-85159+124.emf	Document	10.5 MB
00000011_Unallocated Clusters_FO-35783986_PS-85161+306.sys	Document	10.5 MB
00000012_Unallocated Clusters_FO-35786746_PS-85166+506.mp3	MP3 audio	10.5 MB
00000013_Unallocated Clusters_FO-35786622_PS-85166+382.ntf	Document	10.5 MB
00000014_Unallocated Clusters_FO-35786652_PS-85166+412.sys	Document	10.5 MB
00000015_Unallocated Clusters_FO-35786762_PS-85167+10.ico	Windo...image	10.5 MB
00000016_Unallocated Clusters_FO-35786763_PS-85167+11.aco	Document	10.5 MB
00000017_Unallocated Clusters_FO-35786764_PS-85167+12.emf	Document	10.5 MB
00000018_Unallocated Clusters_FO-35784192_PS-85162+0.mui	Document	10.5 MB
00000019_Unallocated Clusters_FO-35787768_PS-85168+504.sys	Document	10.5 MB
00000020_Unallocated Clusters_FO-35790842_PS-85174+506.mp3	MP3 audio	10.5 MB
00000021_Unallocated Clusters_FO-35790718_PS-85174+382.ntf	Document	10.5 MB
00000022_Unallocated Clusters_FO-35790748_PS-85174+412.sys	Document	10.5 MB
00000023_Unallocated Clusters_FO-35790858_PS-85175+10.ico	Windo...image	10.5 MB
00000024_Unallocated Clusters_FO-35790859_PS-85175+11.aco	Document	10.5 MB
00000025_Unallocated Clusters_FO-35790860_PS-85175+12.emf	Document	10.5 MB
chris_admin.PNG	PNG image	69 KB

Figure-23: Files discovered from unallocated cluster from SUBJECT's acquired_evidence.

By visual inspection, these files extensions were not the real file extension.

Using HexExit to inspect.mp3' file, the file header information didn't contain any ''00000005_Unallocated Clusters_F0-35782665.mp3' hexadecimal value to match a mp3 file. FAT used the Gary Kessler File Signature table [2] to verify the mp3 file header hexadecimal. Due to limited time resource, FAT was not able to analyze these files further.

Another file, '00000010_Unallocated Clusters_F0-35782780_PS-85159+124.emf' was visually inspected by trying to open it since FAT lab's system was able to associate this file to a Paint application. This error was shown *'Paint cannot read this file. This is not a valid bitmap file or its format is not currently supported'*.

Files Found Details:

1) There were 354 jpeg files discovered from SUBJECT's acquired_evidence files. These jpeg files were mainly images of Microsoft icons such as Windows setup icon, arrow icons, buildings from a city, people walking and people smiling into the camera. But there were 9 jpeg files there could have been modified or altered because by visual inspection, these files revealed missing image data. See figure-24 on the next page.

[2] **http://www.garykessler.net/library/file_sigs.html**

Figure-24: Modified jpeg file.

2) There were 110 bmp files discovered from SUBJECT's acquired_evidence file. Again these bmp files appeared to be mainly Microsoft icons such as Windows setup icon, arrow icons, and Windows display screen images. But there were 13 bmp files that there could have been modified or altered. With visual inspection, these files revealed missing image data.

3) There were 727 gif files discovered from SUBJECT's acquired_evidence file. Again these gif files appeared to be mainly Microsoft bitmap icons such as Windows icon, arrow icons and random bitmap images. But there were 75 git files that there could have been modified or altered. With visual inspection, these files revealed missing image data.

4) There were 223 png files discovered from SUBJECT's acquired_evidence file. Again these png files appeared to be mainly Microsoft bitmap icons such as Windows icon and joysticks images. But there were 41 png files that there could have been modified or altered. With visual inspection, these files revealed missing image data.

5) There were two zip files discovered from SUBJECT's acquired_evidence file. Both zip files contained bmp files that appeared to be random Microsoft icons.

6) There were 143 avi (video) files from SUBJECT's acquired_evidence file. With visual inspection by opening them, errors were found with these video files. Also there were 9 wmv (video) files.

7) There were three java jar files from SUBJECT's acquired_evidence file.

8) There were 247 html files from SUBJECT's acquired_evidence file.

9) There were 20 ole files from SUBJECT's acquired_evidence file.

10) There were 278 wav (music) files from SUBJECT's acquired_evidence file.

11) There were 25 files found from Chris Hemsworth directory. See next page for details of these file with their associated md5 hash values.

MD5	FileNames
b81a188818566fe7cae79c43eddcd753	Chris Hemsworth\Local Settings\Temporary Internet Files\Content.IE5\4JGHINMZ\AAjBqaA[1].jpg
6a42250c4a154a37409f454c9caddf3f	Chris Hemsworth\Local Settings\Temporary Internet Files\Content.IE5\4JGHINMZ\AAjC5it[1].jpg
c299d5d5d6588a125bfb698926814ac0	Chris Hemsworth\Local Settings\Temporary Internet Files\Content.IE5\4JGHINMZ\a62410[1].gif
d86e992e6f6588eb08ddfb936ada75b0	Chris Hemsworth\Local Settings\Temporary Internet Files\Content.IE5\4JGHINMZ\sv-se[1].htm
a1cdff14a788a910af867758d56ef500	Chris Hemsworth\Local Settings\Temporary Internet Files\Content.IE5\4JGHINMZ\AAjBcDY[1].jpg
4a3deb274bb5f0212c2419d3d8d08612	Chris Hemsworth\Local Settings\Temporary Internet Files\Content.IE5\4JGHINMZ\desktop.ini
6a6fba337c9d6b094f4d8f1ba7f0ac2c	Chris Hemsworth\Local Settings\Temporary Internet Files\Content.IE5\AFC5KT0B\$I30
0963ca6de36599c718a70723c4bdc4a0	Chris Hemsworth\Local Settings\Temporary Internet Files\Content.IE5\AFC5KT0B\AAi4XKG[1].png
f976e4b6b6e2b4a2c225ef8e5813952b	Chris Hemsworth\Local Settings\Temporary Internet Files\Content.IE5\AFC5KT0B\AAjAXuY[1].jpg
d9e5066d0e4e171de61b2d996f440b82	Chris Hemsworth\Local Settings\Temporary Internet Files\Content.IE5\AFC5KT0B\BBwX0ow[1].jpg
68575cc98e3eb8d10448e03589b1eb56	Chris Hemsworth\Local Settings\Temporary Internet Files\Content.IE5\AFC5KT0B\a49b8d[1].gif
4dc834d16a0d219d5c2b8a5b814569e4	Chris Hemsworth\Local Settings\Temporary Internet Files\Content.IE5\AFC5KT0B\jquery-1.11.1.min[1].js
4a3deb274bb5f0212c2419d3d8d08612	Chris Hemsworth\Local Settings\Temporary Internet Files\Content.IE5\AFC5KT0B\desktop.ini
5de85a4c25b455d48058681006e09e55	Chris Hemsworth\Local Settings\Temporary Internet Files\Content.IE5\ET8FQ7G9\$I30
97ed9ed2fb4f2067fb87e738eb37b6a8	Chris Hemsworth\Local Settings\Temporary Internet Files\Content.IE5\ET8FQ7G9\AAjBigH[1].jpg
a7694283507f9b52246839b5c5b4b3e3	Chris Hemsworth\Local Settings\Temporary Internet Files\Content.IE5\ET8FQ7G9\BBvbjgv[1].jpg
dabe16d2d7db5d9410d63763e61e6ab7	Chris Hemsworth\Local Settings\Temporary Internet Files\Content.IE5\ET8FQ7G9\AAjBITw[1].jpg
4304a19aee895422c21e5d51efacf7dc	Chris Hemsworth\Local Settings\Temporary Internet Files\Content.IE5\ET8FQ7G9\AAjC2sX[1].jpg
929b99061a2e922f2f69951dfbca504d	Chris Hemsworth\Local Settings\Temporary Internet Files\Content.IE5\ET8FQ7G9\7b-4face0-4534563a[1].css
4a3deb274bb5f0212c2419d3d8d08612	Chris Hemsworth\Local Settings\Temporary Internet Files\Content.IE5\ET8FQ7G9\desktop.ini
98a9a60168db4425b67d8ad556eaf55a	Chris Hemsworth\Local Settings\Temporary Internet Files\Content.IE5\IBA3CNIP\$I30
ccb14f5d91f91a3e2a49d0e88afc2c0e	Chris Hemsworth\Local Settings\Temporary Internet Files\Content.IE5\IBA3CNIP\AAj28ne[1].jpg
a10ebfe542b66f9715e7323735287e90	Chris Hemsworth\Local Settings\Temporary Internet Files\Content.IE5\IBA3CNIP\BBwy5Zq[1].jpg
2489ec1fa286566025dd99b201907127	Chris Hemsworth\Local Settings\Temporary Internet Files\Content.IE5\IBA3CNIP\AAjBXnl[1].jpg
08c4c554b0c4b89e2a773277794f98b5	Chris Hemsworth\Local Settings\Temporary Internet Files\Content.IE5\IBA3CNIP\c22c7d[1].gif

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.

References

1) http://md5deep.sourceforge.net/

2) http://www.garykessler.net/library/file_sigs.html