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	**20 hours**

CFIAR [insert number]

Case “Assigment 4”

<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.

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 (TEAM)
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, Bless 0.6.0, Oracle VirtualBox Version 5.1.28 r117968 (Qt5.6.2)

Processing

Identification:

CFIAR [insert number]

1. winxp.vdi was downloaded from the DIFO lab files on Thursday 28th of September
2. No case details were provided by the Lab assistant to the TEAM

Acquisition:

1. 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

2. 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.
   This tool was selected due to it being readily available within kali linux, the platform of choice for the investigation. The tools provided to us by the lab assistant (EnCase, FTK) did not function as expected. Therefore, to make progress, we used the tools available to us within Kali Linux.

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

   - if= is the input device, in this case winxp.vdi.
   - hash=md5 tells the command to calculate an MD5 hash of the image that we can use to assure the image integrity.
   - of=/root/Desktop/Lab1/image.dd is the file that the disk image with go, in this case on an external device mounted at /media.

- bs=512 tells the command we want to transfer the image 512 bytes at a time.
- conv=noerror tells the command that in the case of error continue to do the data transfer, but write zeros where the error occur.

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

3074048+0 records in
3074048+0 records out

3. The resulting file called image.dd is of the file type Raw Image Format, which is a bit for bit copy of the raw data of the virtual drive.

4. This copy was then checked again using md5sum and sha1sum to make sure the copy was identical.

   Command:
   root@kali:~/Desktop/Lab1/Exercise4_Acquisition# md5sum *

CFIAR [insert number]

Result:
c965a5e2236d60624c07c8233ed0aeb3 image.dd
c965a5e2236d60624c07c8233ed0aeb3 winxp.vdi

Command
root@kali:~/Desktop/Lab1/Exercise4_Acquisition# sha1sum *

Result:
a8d7b2a8ebffc3905ab8b04edfe7e6fa92076fce image.dd
a8d7b2a8ebffc3905ab8b04edfe7e6fa92076fce winxp.vdi

5. This confirms that the copy is indeed identical to the original.

6. When opened in the hex editor Bless, the file was identified as a 'Oracle VM Virtual Disk Image' indicating that the disk image was created by the program Virtual Box as a virtual drive image.

7. The file image.dd was mounted within Virtual Box and started, but crashes as soon as the OS (Windows XP) was booting.

Examination:

1. Examination was started on 2017-09-29 10:30 am.

2. Using Foremost, the copy was extracted using the command:

   Command:
   foremost image.dd

3. The following directory structure was found within:

```
output/
├── avi
├── bmp
├── dll
├── exe
├── gif
├── htm
├── jar
├── jpg
├── ole
├── png
├── wav
├── wmv
└── zip
    ├── 01675711
    └── 01676159
```

   15 directories and 4213 files

4. The files were scanned using the antivirus program ‘ClamScan’ from the program suite ‘ClamAV 0.99.3-beta1’ but no files were reported as being infected or reported as malicious.

5. Visual examination of the image files, and video files contained within, showed nothing suspicious or malicious. The files seem to be regular Windows XP operating system files.

6. Within the extracted folder, a manual search for keywords were performed using the linux tools ‘grep’ and ‘find’. The keywords that were searched for was “explosives”, “bomb”, “porn”, “terror”. These searches found nothing out of the ordinary.

Documentation and reporting:

During the investigation, the TEAM worked collaboratively with the investigation and documentation. Every step was documented by either of the team members and any findings were brought to the attention of the other team members.

Investigation was finished and closed on 2017-10-02 12:15 a.m.