```
CCF Lab Assignment:
  Data Acquisition
```

# 1 Imaging

1. Form a group of two and discuss how you can retrieve an image from an, currently off-line, hard disk in a forensically sound manner. Create and describe this method.

**Answer:**

As Peter mentioned in his wiki page about the principal of creating an image in forensically sound manner, so I will start immediately with the procedure.

We are not going to use Guymager because it gonna takes a lot of time in order to acquire full disk image.

We will use Dcfldd because it satisfies the forensically sound manner and based its documentation. This tool will:

- hash the transmitted data On-the-fly.
- Verification that the image is identical to the original drive, bit-for-bit.
- Simultaneous output to more than one file/disk is possible.
- The output can be split into multiple files.
- Logs and data can be piped into external applications.

For copy:

```
dcfldd if=/dev/sdb1 of=/media/disk/test_image.dd hash=md5,sha1
hashlog=/media/disk/hashlog.txt
```

For verification:

```
dcfldd if=/dev/sdb1 vf=/media/disk/test_image.dd
verifylog=/media/disk/verifylog.txt
```

Finally, we are going to use dc3dd. Because dcfldd used old version of dd command. However, dc3dd will be updated every time GNU dd is updated und is therefore not affected by any bugs of an old dd version.

dc3dd parameters used:

```
dc3dd if=/dev/sdb hof=sdb_image.img hash=sha256 log=lab1.log cnt=39843750
```

if = read input from FILE hof = Write output to a file or device, hash the output bytes, and verify by comparing the output hash(es) to the input hash(es) hash = Compute an ALGORITHM hash of the input and also of any outputs log = Log I/O statistcs, diagnostics, and total hashes of input and output

to FILE cnt = Read only SECTORS input sectors.

*Sources:*

1- https://wiki.bitcurator.net/index.php?title=Creating_a_Disk_Image_Using_Guymager

2- http://forensicswiki.org/wiki/Dcfldd

3- http://www.cyber-forensics.ch/acquiring-data-with-dd-dcfldd-dc3dd/

2. Write a one-line description, or note a useful feature for the following tools included in CAINE: Guymager, Disk Image Mounter, dcfldd, kpartx

**Answer:**

- Guymager: GUI based free forensic imager for media acquisition
- Disk Image Mounter: used to mount the disk image
- dcfldd: is an enhanced version of dd with features: Hashing on-the-fly, Status output, Flexible disk wipes, Image/wipe Verify, Multiple outputs, Split output, Piped output and logs
- kpartx: Create device maps from partition tables

3. Retrieve one of the evidence harddisks and SATA-to-USB interfaces from the lab teachers. Take extra care to check and maintain the chain of custody!

**Answer:**

Arno gave us a harddisk and SATA-to-USB interface with writeblocker.

4. Follow your method to retrieve the image. Please use timestamps, explain every tool and note down the version. For the purpose of speed, you can assume that the disk is empty after the first 19 GiB 1. If you don’t trust this, go ahead, but take into account that a full dump can take hours. Make sure both team members have access to the retrieved image. You can use your servers as an evidence sharing platform. 2.

**Answer:**

15:35 → disk mounted at /dev/sdb 15:53 → disk copy started

```
root@caine:/local/home/os3# dc3dd if=/dev/sdb hof=sdb_image.img hash=sha256
log=lab1.log cnt=39843750

dc3dd 7.2.646 started at 2018-02-08 15:53:33 +0100
compiled options:
command line: dc3dd if=/dev/sdb hof=sdb_image.img hash=sha256 log=lab1.log
cnt=39843750
device size: 490234752 sectors (probed),   251,000,193,024 bytes
sector size: 512 bytes (probed)
 20400000000 bytes ( 19 G ) copied ( 100% ),  434 s, 45 M/s
 20400000000 bytes ( 19 G ) hashed ( 100% ),  101 s, 193 M/s

input results for device `/dev/sdb':
   39843750 sectors in
   0 bad sectors replaced by zeros
   b63062cb3d3b05f650ef6cc855cc81a70f8ff7081ebcfcc606e835597d93aa77 (sha256)

output results for file `sdb_image.img':
   39843750 sectors out
   [ok] b63062cb3d3b05f650ef6cc855cc81a70f8ff7081ebcfcc606e835597d93aa77
(sha256)

dc3dd completed at 2018-02-08 16:00:47 +0100

root@caine:/local/home/os3# ls
examples.desktop  lab1.log  sdb_image.img
```

Default block size is used, which is 512 bytes. 19GiB = 39843750 * 512 bytes.

5. Read about CAINE Linux and its features while waiting on the dump to finish.

(a) Why would you use a Forensic distribution and what are the main differences between a regular distribution?

**Answer:**

many tools provided, made by professional people, they are at hand in the distro. support is available and bugs are filled quickly. In addition to that, they keep update it. In addition for that in our Caine based on ubuntu distribution. However, it contains a lot of forensic tools and software. So on normal distribution you won't have these tools already installed and verified automatically.

(b) When would you use a live environment and when would you use an installed environment?

**Answer:**

Live environments are really helpful in situations where fornicator has access on that environment and has immediately to gather evidence.

In addition to that, the live environment will always boot up with the same set of tools containing all the needed and verified configurations. So it will eliminate the wrong configuration which leads to incorrect evidence. furthermore, Live environment is used when the situation needs to be like that. Example: Taking image of the memory before it cleaned in order to retrieve the keys and passwords “for encrypted hard disk”. In situations where you want to analyze evidence of a large scale it's better to work with an installed environment and it also depends on the situation.

© What are the policies of CAINE?

**Answer:**

You can find it on manual but I will list some. Mount the storage device manually. ( default either not mounted or if its mounted it is in read-only format). GUI, user friendly and open source tools. provide complete inventory for the investigation process in its four phases.

**Manual and Policies of CAINE: https://www.caine-live.net/page8/page8.htm**

6. As soon as your dump finishes, start a tool to create a timeline on the image. This can take a long time, so either (1) tune the tool to do less work, or (2) go for the full scan and use the time to discuss project ideas with your planned project partner. You will need this timeline later in the assignment. Hints: log2timeline.py,pinfo.py, psort.py, XLSX

**Answer:**

```
root@caine:/local/home/os3# log2timeline.py PeterParker.plaso sdb_image.img

plaso - log2timeline version 20171020

Source path : /local/home/os3/sdb_image.img
Source type : storage media image

Tasks:          Queued  Processing      To merge        Abandoned
```

```
Total
                1       0               1702            0
17181

Identifier      PID     Status          Memory          Sources
Events          File
Main            28685   running         600.3 MiB       122979 (0)
61908 (12)
Worker_00       28708   idle            297.6 MiB       38116 (0)
23371 (4)       TSK:/usr/share/help/bg/ubuntu-help/color-
notspecifiededid.page
Worker_01       28712   idle            259.5 MiB       46495 (0)
22062 (4)       TSK:/usr/share/help/bg/ubuntu-help/color-missingvcgt.page
Worker_02       28716   idle            276.0 MiB       38440 (0)
23304 (4)       TSK:/usr/share/help/bg/ubuntu-help/color-notifications.page
```

# 2 Verification

7. Create and describe a method that enables the verification of your method. Write this down in steps that the other team can follow.

+

8. Exchange HDDs and images with another team. Verify the procedure that they used and the resulting image. Write a small paragraph of max 200 words. Write as if you were verifying the evidence gathering procedure for a court case.

**Answer:**

Ivo, In order to verify this, use the following command and verify that the resulting hash matches our hash in question 5 above.

In order to ensure the chain of custody. Verify the make, model and serial number of the drive by checking the following output:

```
[ 3886.444522] usb 1-1.1.4: Product: CSR8510 A10
[ 5151.401040] usb 4-1: new SuperSpeed USB device number 2 using xhci_hcd
[ 5151.418250] usb 4-1: New USB device found, idVendor=152d, idProduct=9561
[ 5151.418255] usb 4-1: New USB device strings: Mfr=1, Product=2,
SerialNumber=3
[ 5151.418257] usb 4-1: Product: QuickPort XT USB3.0
[ 5151.418259] usb 4-1: Manufacturer: Sharkoon
[ 5151.418261] usb 4-1: SerialNumber: 000000778899
[ 5151.993451] usbcore: registered new interface driver usb-storage
```

```
[ 5151.996522] scsi host6: uas
[ 5151.996614] usbcore: registered new interface driver uas
[ 5151.997298] scsi 6:0:0:0: Direct-Access     WDC WD25 00YD-01NVB1
8201 PQ: 0 ANSI: 6
```

```
 dc3dd if=/dev/sdb hof=sdb_image.img hash=sha256 log=lab1.log cnt=39843750
```

We ensured the chain of custody with them. We checked their manufacturer, serial number and etc. and it matched with their wiki:

```
[ 8354.274707] usb 4-1: new SuperSpeed USB device number 3 using xhci_hcd
[ 8354.291998] usb 4-1: New USB device found, idVendor=152d, idProduct=9561
[ 8354.292003] usb 4-1: New USB device strings: Mfr=1, Product=2,
SerialNumber=3
[ 8354.292005] usb 4-1: Product: QuickPort XT USB3.0
[ 8354.292007] usb 4-1: Manufacturer: Sharkoon
[ 8354.292009] usb 4-1: SerialNumber: 000000778899
[ 8354.293936] scsi host7: uas
[ 8354.306351] scsi 7:0:0:0: Direct-Access     WDC WD25 00YD-01NVB1
8201 PQ: 0 ANSI: 6
```

Now, Our turn to verify their hash:

This is their image hash:

```
0 - 10737418240:
a6d6aa4fb7b17a01972c5301e2a8e806d3d641e4d6425ac3de2156f389a0d893
10737418240 - 21474836480:
e988e707b305b1edf178f2de6b9975bd6b5cd7f6db7b36b47882f7230eb5ab46
Total (sha256):
5c85301460e9f71ccc7debcf0ba556bb3728152f37989b0e8fa3cf0f50bfe2c0
```

The contents of md5.txt should be:

```
0 - 10737418240:            5a5987622f9864ef74ac515df894e8b7
10737418240 - 21474836480:  ab06545d6d204c11f0cd9ec612cb20b3
Total (md5):                9bfaf000971609e273142abf4642
```

So in order to verify it, we will do the exact same procedure:

```
sudo dcfldd if=<device node of evidence disk> hash=md5,sha256 hashwindow=10G
md5log=md5.txt sha256log=sha256.txt hashconv=after bs=1M conv=noerror,sync
of=/dev/null count=20480
```

```
root@caine:/local/home/os3# cat md5.txt
0 - 10737418240: 5a5987622f9864ef74ac515df894e8b7
10737418240 - 21474836480: ab06545d6d204c11f0cd9ec612cb20b3
Total (md5): 9bfaf000971609e273142abf4642f15b
```

```
root@caine:/local/home/os3# cat sha256.txt
```

```
0 - 10737418240:
a6d6aa4fb7b17a01972c5301e2a8e806d3d641e4d6425ac3de2156f389a0d893
10737418240 - 21474836480:
e988e707b305b1edf178f2de6b9975bd6b5cd7f6db7b36b47882f7230eb5ab46
Total (sha256):
5c85301460e9f71ccc7debcf0ba556bb3728152f37989b0e8fa3cf0f50bfe2c0
```

As we see above, we verified their image hashes. So thumb up for them.

# 3 Live Forensics

9. What kind of things would be less important during live acquisition?

**Answer:**

Check whether the device has been tampered with. If it's already running we can start the process of gathering evidence. In addition, memory would also be less important because its volatile, so all information will disappear after the device losses power.

10. What would be different in your method?

**Answer:**

In our method we needs to include a where we got our forensic tools on to the live environment. We should also kept the gathered evidence from the live environment onto a storage that can be used further in the investigation. So a USB flash drive would be useful for that.

I would first dump the memory so as not to overwrite it for live acquisition in that way pollute the evidence.

11. Describe the new method that you would use to gather data during live forensics. Make sure to categorize by priority.

**Answer:**

According to SANS institution ( https://digital-forensics.sans.org/blog/2009/09/12/best-practices-in-digital-evidence-collection/ ) I would follow the following steps:

1. Photograph the computer and scene
2. If the computer is off do not turn it on
3. If the computer is on photograph the screen
4. Collect live data - start with RAM image (Live Response locally or remotely via F-Response) and then collect other live data “as required” such as network connection state, logged on users, currently executing processes etc.
5. If hard disk encryption detected (using a tool like Zero-View) such as full disk encryption i.e. PGP Disk — collect “logical image” of hard disk using dd.exe, Helix - locally or remotely via F-Response
6. Unplug the power cord from the back of the tower - If the computer is a laptop and does not shut down when the cord is removed then remove the battery
7. Diagram and label all cords
8. Document all device model numbers and serial numbers
9. Disconnect all cords and devices
10. Check for HPA then image hard drives using a write blocker, Helix or a hardware imager
11. Package all components (using anti-static evidence bags)
12. Seize all additional storage media (create respective images and place original devices in anti-static evidence bags)
13. Keep all media away from magnets, radio transmitters and other potentially damaging elements
14. Collect instruction manuals, documentation and notes
15. Document all steps used in the seizure

# 4 Technical analysis

12. Mount your image and make sure that it is mounted as read-only.

**Answer:**

We used Disk Image Mounter software. Disk image will be mounted as read-only.

13. Identify and write a small paragraph of max 200 words about what kind of image it is. Don’t go into file specific details just yet. This includes but is not limited to:

**Answer:**

```
Show image size, partition types:

root@caine:~# fdisk -l
```

```
Disk /dev/loop2: 19 GiB, 20400000000 bytes, 39843750 sectors
Units: sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes
Disklabel type: dos
Disk identifier: 0xead2b41c

Device       Boot    Start      End  Sectors  Size Id Type
/dev/loop2p1 *        2048 29503487 29501440 14.1G 83 Linux
/dev/loop2p2      29505534 31455231  1949698  952M  5 Extended
/dev/loop2p5      29505536 31455231  1949696  952M 82 Linux swap / Solaris
```

The image is 19GiB and has 3 partitions (14.1G Linux), (952M Extended), and (952M Linux swap / Solaris).

```
caine@caine:~$ parted -l

Model: Linux device-mapper (linear) (dm)
Disk /dev/mapper/loop1p2: 1024B
Sector size (logical/physical): 512B/512B
Partition Table: msdos
Disk Flags:

Number  Start  End    Size   Type     File system  Flags
 1      1024B  998MB  998MB  primary


Model: Linux device-mapper (linear) (dm)
Disk /dev/mapper/loop1p1: 15.1GB
Sector size (logical/physical): 512B/512B
Partition Table: loop
Disk Flags:

Number  Start  End     Size    File system  Flags
 1      0.00B  15.1GB  15.1GB  ext4


Model: Linux device-mapper (linear) (dm)
Disk /dev/mapper/loop1p5: 998MB
Sector size (logical/physical): 512B/512B
Partition Table: loop
Disk Flags:

Number  Start  End    Size   File system     Flags
 1      0.00B  998MB  998MB  linux-swap(v1)
```

Based on the above output received by typing fdisk -l into terminal, it can be concluded that the image file which is 19Gb large contains 3 separate partitions. The main partition is 15.1Gb large and it is ext4 type. The remaining 2 partitions are swap partitions and the first one is said to be having an 'msdos' partition table. This suggests that an MBR partition table is used however to confirm this, the following code was run:

```
root@caine:/local/home/os3# file sdb_image.img
sdb_image.img: DOS/MBR boot sector
```

14. Using the information from the timeline you create above, write a small paragraph on what you think happened on this specific HDD device. Make it a maximum of 300 words. Please remain objective, as you would preparing evidence for a court case

**Answer:**

Outputting the contents etc/passwd:

```
dave:x:1000:1000:dave,,,:/home/dave:/bin/bash
debian-tor:x:121:129::/var/lib/tor:/bin/false
```

This means that there is a user with a username dave. The user using the username dave is also using tor. Digging into the tor state file a bit brought the following output:

```
# Tor state file last generated on 2017-02-03 12:45:13 local time
# Other times below are in UTC
# You *do not* need to edit this file.

EntryGuard PinkLine B1D81825CFD7209BD1B4520B040EF5653C204A23 DirCache
EntryGuardAddedBy B1D81825CFD7209BD1B4520B040EF5653C204A23 0.2.7.6
2017-01-19 08:57:51
EntryGuardPathBias 117.000000 116.000000 115.000000 1.000000 0.000000
2.000000
EntryGuard bugx 712E84403C2A0C03345C2E751ACE77476AA3FA90 DirCache
EntryGuardAddedBy 712E84403C2A0C03345C2E751ACE77476AA3FA90 0.2.7.6
2017-01-21 20:27:52
EntryGuard doutreval CB4EBE9C475A60A5F2CDA92C83CE093BD945D940 DirCache
EntryGuardAddedBy CB4EBE9C475A60A5F2CDA92C83CE093BD945D940 0.2.7.6
2017-01-15 11:35:28
TorVersion Tor 0.2.7.6 (git-605ae665009853bd)
LastWritten 2017-02-03 11:45:13
TotalBuildTimes 116
```

We noticed Frequent user of tor, wondering why.

In addition to that Cracklib is also installed on the system. Also cron job every minute that execute a script “init.sh”. However, we couldn't find the script in the image. XChat is also there. Finally, Dave has encrypted files in home directory. Which is suspicious.

15. What would help to investigate this evidence further?

**Answer:**

It would help to acquire the decryption keys in order to access the encrypted files inside the home directory. In addition, it would be helpful if we try to recover deleted files and files slack space in order to investigate and check them. We must also try to find the stor.enc file referenced in /root/.bash_history. also we might look at the files and directories to identify the owner of the disk. We can also try to recover some data that might interesting.