

Task-1

Drives and Partition in Linux

First, we are going to analyze and gather information about our disk

Using command “**sudo fdisk -l**”

```
(kali㉿kali)-[~]
$ sudo fdisk -l
Disk /dev/sda: 80 GiB, 85899345920 bytes, 167772160 sectors
Disk model: VBOX HARDDISK
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: 0xea9da5e6

Device Boot      Start         End      Sectors  Size Id Type
/dev/sda1 *        2048     165771263  165769216    79G 83 Linux
/dev/sda2          165773310  167770111    1996802    975M  5 Extended
/dev/sda5          165773312  167770111    1996800    975M 82 Linux swap / Solaris

Disk /dev/sdb: 14.91 GiB, 16008609792 bytes, 31266816 sectors
Disk model: Cruzer Blade
Units: sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes
```

Getting information about the list devices and drives recognized by our machine

Analyzing **/dev** directory

```
(kali㉿kali)-[~]
$ cd ../../dev
(kali㉿kali)-[/dev]
$ ls
autofs      mqueue      stdout      tty31       tty56       vcs6
block       net          tty         tty32       tty57       vcs7
bsg         null        tty0        tty33       tty58       vcs8
btrfs-control nvram       tty1        tty34       tty59       vcsa
bus         port        tty10       tty35       tty6        vcsa1
cdrom       ppp         tty11       tty36       tty60       vcsa2
char        psaux       tty12       tty37       tty61       vcsa3
console     ptmx        tty13       tty38       tty62       vcsa4
core        pts         tty14       tty39       tty63       vcsa5
cpu_dma_latency random      tty15       tty4        tty7        vcsa6
cuse        rfkill      tty16       tty40       tty8        vcsa7
disk        rtc         tty17       tty41       tty9        vcsa8
dri         rtc0        tty18       tty42       ttyS0       vcsu
fb0         sda         tty19       tty43       ttyS1       vcsu1
fd          sda1        tty2         tty44       ttyS2       vcsu2
full        sda2        tty20       tty45       ttyS3       vcsu3
fuse        sda5        tty21       tty46       uhid        vcsu4
hidraw0     sdb         tty22       tty47       uinput      vcsu5
hpet        sg0         tty23       tty48       urandom     vcsu6
hugepages   sg1         tty24       tty49       vboxguest   vcsu7
initctl     sg2         tty25       tty5        vboxuser    vcsu8
```

Hardware Disk information

```
(kali㉿kali)-[/dev]
$ sudo lshw -class disk -short
```

H/W path	Device	Class	Description
/0/100/1.1/0.0.0	/dev/cdrom	disk	CD-ROM
/0/100/6/1/2/0.0.0	/dev/sdb	disk	16GB Cruzer Blade
/0/100/6/1/2/0.0.0/0	/dev/sdb	disk	16GB
/0/100/d/0.0.0	/dev/sda	disk	85GB VBOX HARDDISK

Hardware Volume information

```
(kali㉿kali)-[/dev]
$ sudo lshw -class volume -short
```

H/W path	Device	Class	Description
/0/100/d/0.0.0/1	/dev/sda1	volume	79GiB EXT4 volume
/0/100/d/0.0.0/2	/dev/sda2	volume	975MiB Extended par
/0/100/d/0.0.0/2/5	/dev/sda5	volume	975MiB Linux swap v

Task-2

Linux Hashing Commands

Learning about hashing commands

```
(kali㉿kali)-[~/Desktop/Digital-Forensics]
$ printf cs362 | sha1sum
ee337f581bdf94a9270c7d6ac33acb58659d40a2 -

(kali㉿kali)-[~/Desktop/Digital-Forensics]
$ printf cs362 | md5sum
21e807599f8ec807297d3f9d9bcbb635 -

(kali㉿kali)-[~/Desktop/Digital-Forensics]
$ printf cs362 | sha512sum
be47fe03860b2c7330b2d15bb7911fbd4b5e73327b35d1a1857537948f92f92f3aaf28fb56bc595d5d8f0a9fdf580fb294840
f33a2df3c4fd46f07cc2cfefbd97 -

(kali㉿kali)-[~/Desktop/Digital-Forensics]
$ #HASHING A FILE

(kali㉿kali)-[~/Desktop/Digital-Forensics]
$ echo "I am Junead" > file1.txt

(kali㉿kali)-[~/Desktop/Digital-Forensics]
$ md5sum file1.txt
90e0189980ab80205d10254a2be0c302 file1.txt
```

Using openssl to use hashing command sha3

```
(kali㉿kali)-[~/Desktop/Digital-Forensics]
$ printf cs362 | openssl dgst -sha3-256
(stdin)= e4ca8e0e958b39280f5ba86cd8864b194645c37ac1b89a778416a1bf23e4ef0a

(kali㉿kali)-[~/Desktop/Digital-Forensics]
$ openssl dgst -sha3-256 ./*
SHA3-256(./file1.txt)= e5a28afe5da4e4906c92e6e36a09fd76e76d0745f057c034b882b0a0f9ad6dfa
```

Task-3

Acquisition using dc3dd and dd Commands

Creating raw-image of USB

```
(kali㉿kali)-[~/Desktop/Digital-Forensics]
$ sudo dc3dd if=/dev/sdb hash=sha1 log=usb_forensics.log of=usb_image.dd

[sudo] password for kali:

dc3dd 7.2.646 started at 2022-02-06 03:39:08 -0500
compiled options:
command line: dc3dd if=/dev/sdb hash=sha1 log=usb_forensics.log of=usb_image.dd
device size: 31266816 sectors (probed), 16,008,609,792 bytes
sector size: 512 bytes (probed)
16008609792 bytes (15 G) copied (100%), 1426 s, 11 M/s

input results for device `/dev/sdb':
31266816 sectors in
0 bad sectors replaced by zeros
18a088e7823b420963569339990623c344d59a3c (sha1)

output results for file `usb_image.dd':
31266816 sectors out

dc3dd completed at 2022-02-06 04:02:54 -0500
```

Splitting the files of the created image

```
(kali㉿kali)-[~/Desktop/Digital-Forensics]
$ sudo dc3dd if=/dev/sdb hash=sha1 log=usb_forensics.log ofsz=550M ofs=usb_forensics.000
[sudo] password for kali:

dc3dd 7.2.646 started at 2022-02-06 04:05:09 -0500
compiled options:
command line: dc3dd if=/dev/sdb hash=sha1 log=usb_forensics.log ofsz=550M ofs=usb_forensics.000
device size: 31266816 sectors (probed), 16,008,609,792 bytes
sector size: 512 bytes (probed)
16008609792 bytes (15 G) copied (100%), 1425 s, 11 M/s

input results for device `/dev/sdb':
31266816 sectors in
0 bad sectors replaced by zeros
18a088e7823b420963569339990623c344d59a3c (sha1)

output results for files `usb_forensics.000':
31266816 sectors out

dc3dd completed at 2022-02-06 04:28:54 -0500

(kali㉿kali)-[~/Desktop/Digital-Forensics]
$ ls
file1.txt          usb_forensics.006  usb_forensics.013  usb_forensics.020  usb_forensics.027
usb_forensics.000  usb_forensics.007  usb_forensics.014  usb_forensics.021  usb_forensics.log
usb_forensics.001  usb_forensics.008  usb_forensics.015  usb_forensics.022  usb_image.dd
usb_forensics.002  usb_forensics.009  usb_forensics.016  usb_forensics.023
usb_forensics.003  usb_forensics.010  usb_forensics.017  usb_forensics.024
usb_forensics.004  usb_forensics.011  usb_forensics.018  usb_forensics.025
usb_forensics.005  usb_forensics.012  usb_forensics.019  usb_forensics.026
```


Computing hash function

```
(kali㉿kali)-[~/Desktop/Digital-Forensics]
$ cat usb_forensics.000 | sha1sum
80d359c83a856e00c7a0297cab5fe46db7f9d5c7  -
```

Avoid recovery of deleted files

```
(kali㉿kali)-[~/Desktop/Digital-Forensics]
$ sudo dc3dd wipe=/dev/sdb

dc3dd 7.2.646 started at 2022-02-06 05:34:35 -0500
compiled options:
command line: dc3dd wipe=/dev/sdb
device size: 31266816 sectors (probed), 16,008,609,792 bytes
sector size: 512 bytes (probed)
16008609792 bytes (15 G) copied (100%), 2776 s, 5.5 M/s

input results for pattern `00':
31266816 sectors in

output results for device `/dev/sdb':
31266816 sectors out

dc3dd completed at 2022-02-06 06:20:52 -0500
```

```
(kali㉿kali)-[~/Desktop/Digital-Forensics]
$ sudo dc3dd wipe=/dev/sdb tpat=happyholiday
[sudo] password for kali:

dc3dd 7.2.646 started at 2022-02-06 06:26:35 -0500
compiled options:
command line: dc3dd wipe=/dev/sdb tpat=happyholiday
device size: 31266816 sectors (probed), 16,008,609,792 bytes
sector size: 512 bytes (probed)
16008609792 bytes (15 G) copied (100%), 2763 s, 5.5 M/s

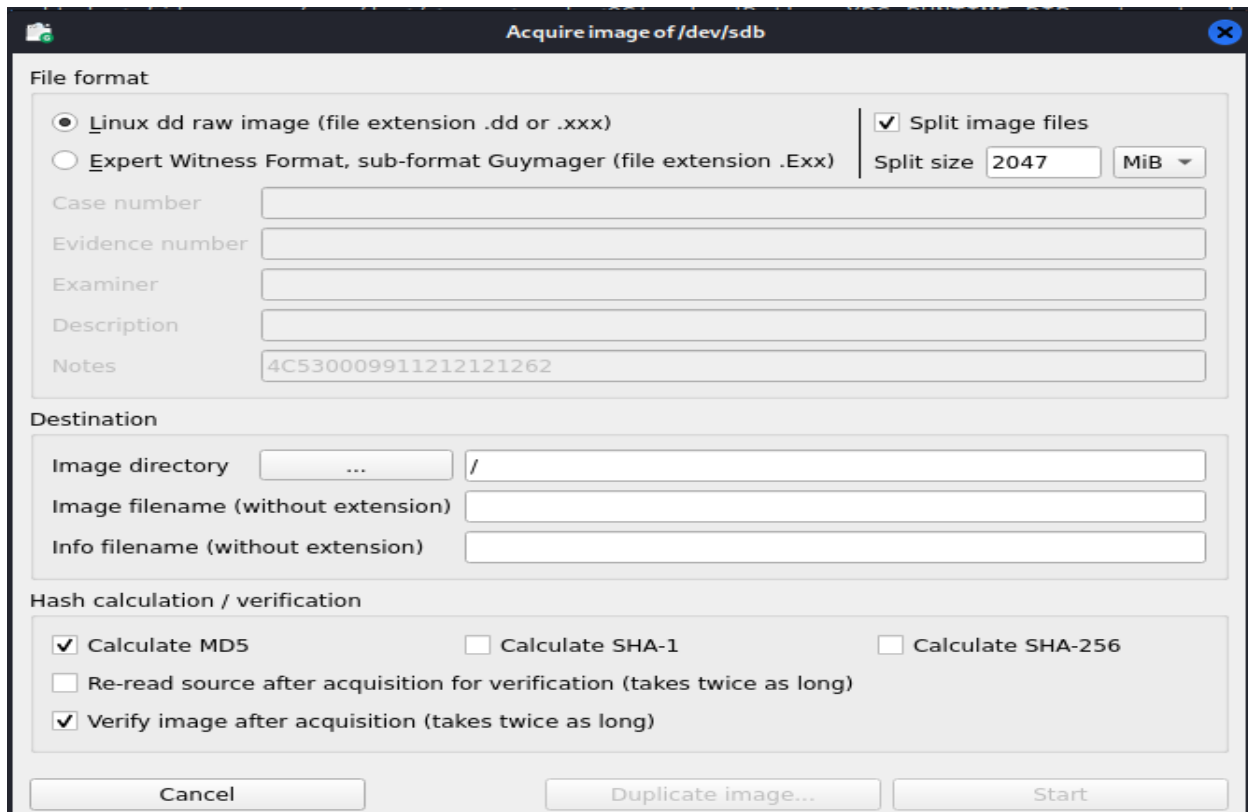
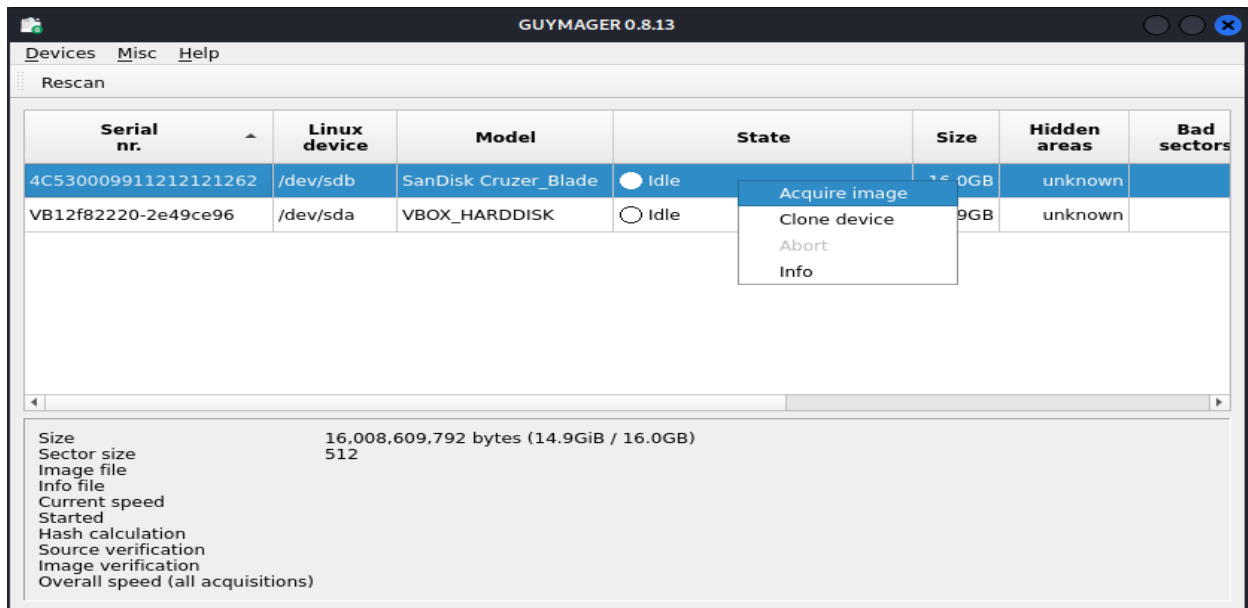
input results for pattern `happyholiday':
31266816 sectors in

output results for device `/dev/sdb':
31266816 sectors out

dc3dd completed at 2022-02-06 07:12:37 -0500
```

Task-4

Image Acquisition using Guymager



This is a graphical method of acquiring an image

```
<usb_forensics.info>
File Edit Search Options Help
DMA: not supported
PIO: pio0

Command executed: bash -c "CIDFILE=/sys/block/$(basename /dev/sdb)/device/cid; echo -n "CID: " ; if [ -e $CIDFILE ] ; then cat $CID
Information returned:
-----
CID: not available
-----
Hidden areas: unknown
|
Acquisition
=====
Linux device      : /dev/sdb
Device size       : 16008609792 (16.0GB)
Format            : Linux split dd raw image - file extension is .xxx
Image path and file name: /home/power/Desktop/disk-forensics/usb_forensics.xxx
Info path and file name: /home/power/Desktop/disk-forensics/usb_forensics.info
Hash calculation  : SHA-1
Source verification : off
Image verification : off

No bad sectors encountered during acquisition.
State: Finished successfully

MD5 hash
MD5 hash verified source : --
MD5 hash verified image  : --
SHA1 hash                 : ab603232611e6083eeac8cf0c9a293fb7e87f731
SHA1 hash verified source : --
SHA1 hash verified image  : --
SHA256 hash               : --
SHA256 hash verified source: --
SHA256 hash verified image: --

Acquisition started: 2022-02-05 20:16:17 (ISO format YYYY-MM-DD HH:MM:SS)
Ended               : 2022-02-05 20:28:47 (0 hours, 12 minutes and 30 seconds)
Acquisition speed  : 20.36 MByte/s (0 hours, 12 minutes and 30 seconds)
```

Task-5

Retrieve the Master Boot Record (MBR) using the dd Command

```
└─$ sudo dd if=/dev/sda bs=512 of=mbr.image count=1
[sudo] password for kali:
1+0 records in
1+0 records out
512 bytes copied, 0.000144197 s, 3.6 MB/s
```

Reading mbr.image file in hex format

```
(kali㉿kali)-[~/Desktop/Digital-Forensics]
└─$ xxd mbr.image
00000000: eb63 9010 8ed0 bc00 b0b8 0000 8ed8 8ec0  .c.....
00000010: fbbe 007c bf00 06b9 0002 f3a4 ea21 0600  ...|.....!..
00000020: 00be be07 3804 750b 83c6 1081 fefe 0775  ...8.u.....u
00000030: f3eb 16b4 02b0 01bb 007c b280 8a74 018b  .....|...t..
00000040: 4c02 cd13 ea00 7c00 00eb fe00 0000 0000  L.....|.....
00000050: 0000 0000 0000 0000 0000 0080 0100 0000  .....
00000060: 0000 0000 fffa 9090 f6c2 8074 05f6 c270  .....t...p
00000070: 7402 b280 ea79 7c00 0031 c08e d88e d0bc  t...y|..1.....
00000080: 0020 fba0 647c 3cff 7402 88c2 52be 807d  . ..d|<.t...R..}
00000090: e817 01be 057c b441 bbba 55cd 135a 5272  ....|..A..U..ZRR
000000a0: 3d81 fb55 aa75 3783 e101 7432 31c0 8944  =..U.u7...t21..D
000000b0: 0440 8844 ff89 4402 c704 1000 668b 1e5c  .@.D..D.....f.. \
000000c0: 7c66 895c 0866 8b1e 607c 6689 5c0c c744  |f.\.f..`|f.\..D
000000d0: 0600 70b4 42cd 1372 05bb 0070 eb76 b408  ..p.B...r...p.v..
000000e0: cd13 730d 5a84 d20f 83d8 00be 8b7d e982  ..s.Z.....}...
000000f0: 0066 0fb6 c688 64ff 0466 8944 040f b6d1  .f....d.@f..D...
00000100: c1e2 0288 e888 f440 8944 080f b6c2 c0e8  .....@.D.....
00000110: 0266 8904 66a1 607c 6609 c075 4e66 a15c  .f..f..`|f..uNf.\
00000120: 7c66 31d2 66f7 3488 d131 d266 f774 043b  |f1.f.4...1.f.t.;
00000130: 4408 7d37 fec1 88c5 30c0 c1e8 0208 c188  D.}7....0.....
00000140: d05a 88c6 bb00 708e c331 dbb8 0102 cd13  .Z....p...1....
00000150: 721e 8cc3 601e b900 018e db31 f6bf 0080  r...`.....1....
00000160: 8ec6 fcf3 a51f 61ff 265a 7cbe 867d eb03  ....a.8Z|..}..
00000170: be95 7de8 3400 be9a 7de8 2e00 cd18 ebfe  ..}.4...}.....
00000180: 4752 5542 2000 4765 6f6d 0048 6172 6420  GRUB .Geom.Hard
00000190: 4469 736b 0052 6561 6400 2045 7272 6f72  Disk.Read. Error
000001a0: 0d0a 00bb 0100 b40e cd10 ac3c 0075 f4c3  .....<.u...
000001b0: 0000 0000 0000 0000 e6a5 9dea 0000 8004  .....
000001c0: 0104 83fe c2ff 0008 0000 0070 e109 00fe  .....p.....
000001d0: c2ff 05fe c2ff fe7f e109 0278 1e00 0000  .....x.....
000001e0: 0000 0000 0000 0000 0000 0000 0000 0000  .....
000001f0: 0000 0000 0000 0000 0000 0000 55aa  .....U..
```

Task-6

Windows Disk Investigation with PowerShell Cmdlets

Now we are using windows PowerShell to install forensics tool and look at the details of the image

```
PS C:\tools> Find-Module -name *forensic*

NuGet provider is required to continue
PowerShellGet requires NuGet provider version '2.8.5.201' or newer to interact with NuGet-based repositories. The NuGet
provider must be available in 'C:\Program Files\PackageManagement\ProviderAssemblies' or
'C:\Users\shehr\AppData\Local\PackageManagement\ProviderAssemblies'. You can also install the NuGet provider by running
'Install-PackageProvider -Name NuGet -MinimumVersion 2.8.5.201 -Force'. Do you want PowerShellGet to install and
import the NuGet provider now?
[Y] Yes [N] No [S] Suspend [?] Help (default is "Y"): Y

Version      Name                Repository      Description
-----
1.1.1        PowerForensics      PSGallery       A Digital Forensics framework for Windows PowerS...
1.1.1        PowerForensicsv2    PSGallery       A Digital Forensics framework for Windows PowerS...
1.1.1        PowerForensicsPorta PSGallery       A Digital Forensics framework for Windows PowerS...
1.0.0.0      Forensics            PSGallery       The module can be used for performing some Evide...
```

```
PS C:\tools> Get-ChildItem -Path '..\Program Files\WindowsPowerShell\Modules\'

Directory: C:\Program Files\WindowsPowerShell\Modules

Mode                LastWriteTime         Length Name
----                -
d-----         12/7/2019   1:31 AM                Microsoft.PowerShell.Operation.Validation
d-----         12/7/2019   1:31 AM                PackageManagement
d-----         12/7/2019   1:31 AM                Pester
d-----          2/5/2022   7:28 AM                PowerForensics
d-----         12/7/2019   1:31 AM                PowerShellGet
d-----         12/7/2019   1:31 AM                PSReadline
```

```
PS C:\tools> Import-Module -name PowerForensics
PS C:\tools> Get-Command -Module PowerForensics

CommandType      Name                                     Version      Source
-----
Cmdlet            ConvertFrom-BinaryData                 1.1.1        PowerForensics
Cmdlet            ConvertTo-ForensicTimeline             1.1.1        PowerForensics
Cmdlet            Copy-ForensicFile                     1.1.1        PowerForensics
Cmdlet            Get-ForensicAlternateDataStream        1.1.1        PowerForensics
Cmdlet            Get-ForensicAmcache                   1.1.1        PowerForensics
Cmdlet            Get-ForensicAttrDef                   1.1.1        PowerForensics
Cmdlet            Get-ForensicBitmap                    1.1.1        PowerForensics
Cmdlet            Get-ForensicBootSector                 1.1.1        PowerForensics
Cmdlet            Get-ForensicChildItem                 1.1.1        PowerForensics
Cmdlet            Get-ForensicContent                   1.1.1        PowerForensics
Cmdlet            Get-ForensicEventLog                  1.1.1        PowerForensics
Cmdlet            Get-ForensicExplorerTypedPath         1.1.1        PowerForensics
Cmdlet            Get-ForensicFileRecord                1.1.1        PowerForensics
Cmdlet            Get-ForensicFileRecordIndex           1.1.1        PowerForensics
```

Checking master boot record of the volume C disk

```
PS C:\tools> Get-ForensicVolumeBootRecord -VolumeName \\.\C: -AsBytes | Format-Hex

    00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F

00000000 EB 52 90 4E 54 46 53 20 20 20 20 00 02 08 00 00  ěRNTFS .....
00000010 00 00 00 00 00 F8 00 00 3F 00 FF 00 00 98 01 00  ....ø...?....@..
00000020 00 00 00 00 80 00 80 00 74 E0 0A 1D 00 00 00 00  ....@.@.tà.....
00000030 00 00 0C 00 00 00 00 00 02 00 00 00 00 00 00 00  .....
00000040 F6 00 00 00 01 00 00 00 FE 94 E0 AC D3 E0 AC F0  ö.....p@a-Ôà-ô
00000050 00 00 00 00 FA 33 C0 8E D0 BC 00 7C FB 68 C0 07  ....ú3Ã@Ø%,|ûhÃ.
00000060 1F 1E 68 66 00 CB 88 16 0E 00 66 81 3E 03 00 4E  ..hf.Ë@...f@>..N
00000070 54 46 53 75 15 B4 41 BB AA 55 CD 13 72 0C 81 FB  TFSu.´A»¾UÍ.r.@û
00000080 55 AA 75 06 F7 C1 01 00 75 03 E9 DD 00 1E 83 EC  U¾u.÷Ã...u.éÝ..@ì
00000090 18 68 1A 00 B4 48 8A 16 0E 00 8B F4 16 1F CD 13  .h...´H@...@ô...î.
000000A0 9F 83 C4 18 9E 58 1F 72 E1 3B 06 0B 00 75 DB A3  @@Ã.@X.rá;...uÛf
000000B0 0F 00 C1 2E 0F 00 04 1E 5A 33 DB B9 00 20 2B C8  ..Á.....Z3Û¹. +È
000000C0 66 FF 06 11 00 03 16 0F 00 8E C2 FF 06 16 00 E8  f.....@Ã....è
000000D0 4B 00 2B C8 77 EF B8 00 BB CD 1A 66 23 C0 75 2D  K.+Êwĩ.,»Í.f#Au-
000000E0 66 81 FB 54 43 50 41 75 24 81 F9 02 01 72 1E 16  f@ÛTCPAu$@ù...r..
000000F0 68 07 BB 16 68 52 11 16 68 09 00 66 53 66 53 66  h.».hR..h..fSfSf
00000100 55 16 16 16 68 B8 01 66 61 0E 07 CD 1A 33 C0 BF  U...h..fa...Í.3Ã¿
00000110 0A 13 B9 F6 0C FC F3 AA E9 FE 01 90 90 66 60 1E  ..¹ö..üó¾ép.@@f`.
00000120 06 66 A1 11 00 66 03 06 1C 00 1E 66 68 00 00 00  .f;...f.....fh...
00000130 00 66 50 06 53 68 01 00 68 10 00 B4 42 8A 16 0E  .fP.Sh..h..´B@..
00000140 00 16 1F 8B F4 CD 13 66 59 5B 5A 66 59 66 59 1F  ...@ôÍ.fY[ZfYfY.
00000150 0F 82 16 00 66 FF 06 11 00 03 16 0F 00 8E C2 FF  .@...f.....@Ã.
00000160 0E 16 00 75 BC 07 1F 66 61 C3 A1 F6 01 E8 09 00  ...u%...faÃ;ö.è..
00000170 A1 FA 01 E8 03 00 F4 EB FD 8B F0 AC 3C 00 74 09  ;ú.è...ôëý@ô~<.t.
00000180 B4 0E BB 07 00 CD 10 EB F2 C3 0D 0A 41 20 64 69  ´.»...Í.ëòÃ..A di
00000190 73 6B 20 72 65 61 64 20 65 72 72 6F 72 20 6F 63  sk read error oc
000001A0 63 75 72 72 65 64 00 0D 0A 42 4F 4F 54 4D 47 52  curred...BOOTMGR
000001B0 20 69 73 20 63 6F 6D 70 72 65 73 73 65 64 00 0D  is compressed..
000001C0 0A 50 72 65 73 73 20 43 74 72 6C 2B 41 6C 74 2B  .Press Ctrl+Alt+
000001D0 44 65 6C 20 74 6F 20 72 65 73 74 61 72 74 0D 0A  Del to restart..
000001E0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  .....
000001F0 00 00 00 00 00 00 8A 01 A7 01 BF 01 00 00 55 AA  ....@.$.¿...U¾
```

```
PS C:\tools> Get-ForensicFileRecord -Path 'C:\Users\Public\AccountPictures\S-1-5-21-3695201621-3816592265-914291048-1002\{A7FF035D-ADA2-460F-9C66-62C5CC0DBA77}-Image1080.jpg'
```

```
FullName       : C:\\Users\\Public\\AccountPictures\\S-1-5-21-3695201621-3816592265-914291048-1002\\{A7FF035D-ADA2-460F-9C66-62C5CC0DBA77}-Image1080.jpg
Name           : {A7FF035D-ADA2-460F-9C66-62C5CC0DBA77}-Image1080.jpg
SequenceNumber : 2
RecordNumber   : 86762
ParentSequenceNumber : 1
ParentRecordNumber : 86745
Directory      : False
Deleted        : False
ModifiedTime   : 9/11/2021 12:16:42 PM
AccessedTime   : 9/11/2021 12:16:42 PM
ChangedTime    : 9/11/2021 12:16:42 PM
BornTime       : 9/11/2021 12:16:42 PM
FNModifiedTime : 9/11/2021 12:16:42 PM
FNAccessedTime : 9/11/2021 12:16:42 PM
FNChangedTime  : 9/11/2021 12:16:42 PM
FNBornTime     : 9/11/2021 12:16:42 PM
```


Summary

This whole lab was about Disk Forensics. We have learned how to view information about the storage devices that are fitted in our system. We also did practical on how to use hashing commands and get hash of any text or file. Then we learned to create a raw image of a disk and also to avoid recovery of deleted files. We learned to use guymager software that is gui based software. We have also read the MBR (Master Record Boot) of our disk. At last, we have used Windows PowerShell to do Windows Disk Investigation.

←END→