INPT

# FORENSICS

CIT

MADE BY:

FATIMA EZZAHRA ACHAIT

MOHAMMED KHALDOUNE

# PLAN

1. INTRODUCTION - DEMO
2. FILE SIGNATURE
2.1 HEXEDIT
2.2 CHANGE MAGIC BYTES - DEMO
3. FILE EXTENTION
4. INTRO TO WIRESHARK
4.1 FILTERING PACKETS
4.2 EXTACTING FILES
5. CAPTURE PACKETS OF A HTTP/HTTPS WEBSITE - DEMO
6. RECOVERY DATA FROM DISK IMAGES - DEMO
7. EXTRACTING DATA FROM MEMORY CAPTURE - DEMO

# 1. INTRODUCTION

- Cyber forensics in the simplest words means **investigating**, **gathering**, and **analyzing** information from a computer device which can then be transformed into hardware proof to be presented in the court regarding the crime in question.
- The goal of computer forensics is to perform a structured investigation and maintain a documented chain of evidence to find out exactly **what happened** on a computing device and **who was responsible** for it.

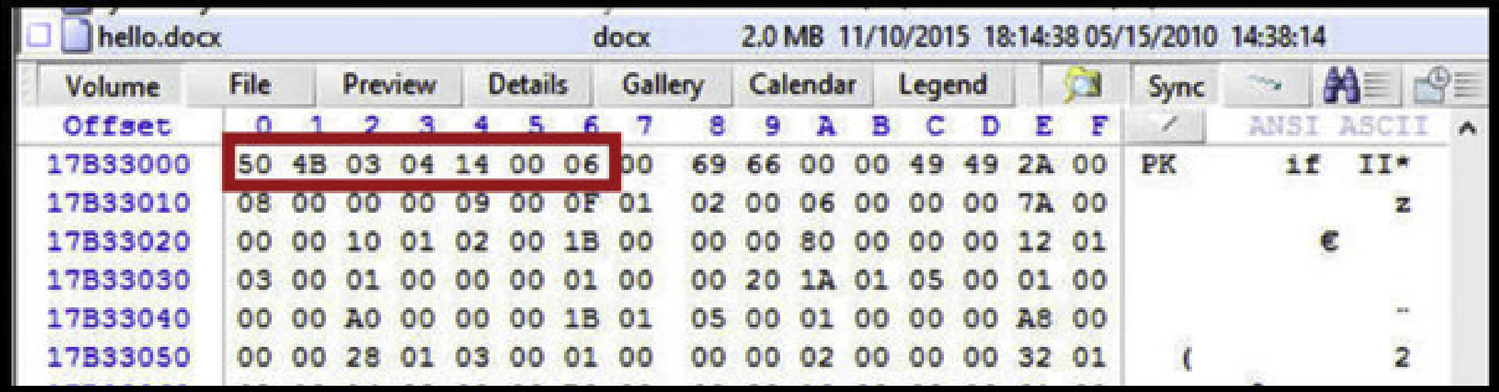
Note : OSINT & Steganography are part of forensics

# 1.INTRODUCTION- DEMO

our client bank is under attack, may the logs will help to find the name of the malware the attacker used

# 2. FILE SIGNATURE

- File Signature or Magic Number is a protocol set of constant numerical and text values used to identify file format.
- In other words, every file type requires a unique signature in order for an operating system to recognize it, classify it and show it to a user.
- A file signature is a unique sequence of identifying bytes written to a file's header.
- Itis a data used to identify or verify the contents of a file.




- List_of_file_signatures

# 2.1 HEXEDIT

--$ hexedit begin.jpg

```
kali@kali: ~/Downloads
kali@kali: ~/Downloads 105x29
00000000   FF D8 FF E0  00 10 4A 46  49 46 00 01  01 00 00 48  00 48 00 00  ......JFIF.....H.H..
00000014   FF E1 00 B4  45 78 69 66  00 00 4D 4D  00 2A 00 00  00 08 00 04  ....Exif..MM.*......
00000028   01 1A 00 05  00 00 00 01  00 00 00 3E  01 1B 00 05  00 00 00 01  ...........>........
0000003C   00 00 00 46  01 28 00 03  00 00 00 01  00 02 00 00  87 69 00 04  ...F.(...........i..
00000050   00 00 00 01  00 00 00 4E  00 00 00 00  00 00 00 48  00 00 00 01  .......N.......H....
00000064   00 00 00 48  00 00 00 01  00 06 A0 01  00 03 00 00  00 01 00 01  ...H................
00000078   00 00 A0 02  00 04 00 00  00 01 00 00  01 40 A0 03  00 04 00 00  ............@......
0000008C   00 01 00 00  01 C0 A2 0E  00 05 00 00  00 01 00 00  00 9C A2 0F  ....................
000000A0   00 05 00 00  00 01 00 00  00 A4 A2 10  00 03 00 00  00 01 00 01  ....................
000000B4   00 00 00 00  00 00 00 00  00 48 00 00  00 01 00 00  00 48 00 00  .........H.......H..
000000C8   00 01 FF ED  00 38 50 68  6F 74 6F 73  68 6F 70 20  33 2E 30 00  .....8Photoshop 3.0.
000000DC   38 42 49 4D  04 04 00 00  00 00 00 00  38 42 49 4D  04 25 00 00  8BIM........8BIM.%..
000000F0   00 00 00 10  D4 1D 8C D9  8F 00 B2 04  E9 80 09 98  EC F8 42 7E  ..................B~
00000104   FF C2 00 11  08 01 C0 01  40 03 01 22  00 02 11 01  03 11 01 FF  ........@.."........
00000118   C4 00 1F 00  00 01 05 01  01 01 01 01  01 00 00 00  00 00 00 00  ....................
0000012C   03 02 04 01  05 00 06 07  08 09 0A 0B  FF C4 00 C3  10 00 01 03  ....................
00000140   03 02 04 03  04 06 04 07  06 04 08 06  73 01 02 00  03 11 04 12  ............s.......
00000154   21 05 31 13  22 10 06 41  51 32 14 61  71 23 07 81  20 91 42 15  !.1."..AQ2.aq#.. .B.
00000168   A1 52 33 B1  24 62 30 16  C1 72 D1 43  92 34 82 08  E1 53 40 25  .R3.$b0..r.C.4...S@%
0000017C   63 17 35 F0  93 73 A2 50  44 B2 83 F1  26 54 36 64  94 74 C2 60  c.5..s.PD...&T6d.t.`
00000190   D2 84 A3 18  70 E2 27 45  37 65 B3 55  75 A4 95 C3  85 F2 D3 46  ....p.'E7e.Uu......F
000001A4   76 80 E3 47  56 66 B4 09  0A 19 1A 28  29 2A 38 39  3A 48 49 4A  v..GVf.....()*89:HIJ
000001B8   57 58 59 5A  67 68 69 6A  77 78 79 7A  86 87 88 89  8A 90 96 97  WXYZghijwxyz........
000001CC   98 99 9A A0  A5 A6 A7 A8  A9 AA B0 B5  B6 B7 B8 B9  BA C0 C4 C5  ....................
000001E0   C6 C7 C8 C9  CA D0 D4 D5  D6 D7 D8 D9  DA E0 E4 E5  E6 E7 E8 E9  ....................
000001F4   EA F3 F4 F5  F6 F7 F8 F9  FA FF C4 00  1F 01 00 03  01 01 01 01  ....................
00000208   01 01 01 01  01 00 00 00  00 00 01 02  00 03 04 05  06 07 08 09  ....................
0000021C   0A 0B FF C4  00 C3 11 00  02 02 01 03  03 03 02 03  05 02 05 02  ....................
---  begin.jpg       --0x0/0x5560--0%-----------------------------------------------------------
```

## FF D8 FF E0

this is magic bytes or file signature for JPG file

# 2.2 CHANGE MAGIC BYTES - DEMO

**SCENARIO:**

- We have a website where we can upload only images ( jpg, png, gif )
- we want to upload a malicious script in php to the server instead of an image
- but there is a filtering that does not allow anything to be uploaded to the backend except images
- we changed the extention of the php script to .png and .jpg but none of them succeeded

## DEMO

# 3. FILE EXTENTION

Unlike Windows, Linux does not care about the extension of your files. It looks into the file contents and will figure it out by its own. In other words, Linux is extension agnostic. If you are interested to test it for yourself, use file command and give it your file name as an argument.

```
└─$ file begin.docx
begin.docx: JPEG image data, JFIF standard 1.01, aspect ratio, density 72x72, se
gment length 16, Exif Standard: [TIFF image data, big-endian, direntries=4, xres
olution=62, yresolution=70, resolutionunit=2], progressive, precision 8, 320x448
, components 3

┌──(kali㉿kali)-[~]
└─$ file data.png
data.png: ASCII text

┌──(kali㉿kali)-[~]
└─$ file DNS.txt
DNS.txt: PDF document, version 1.4
```

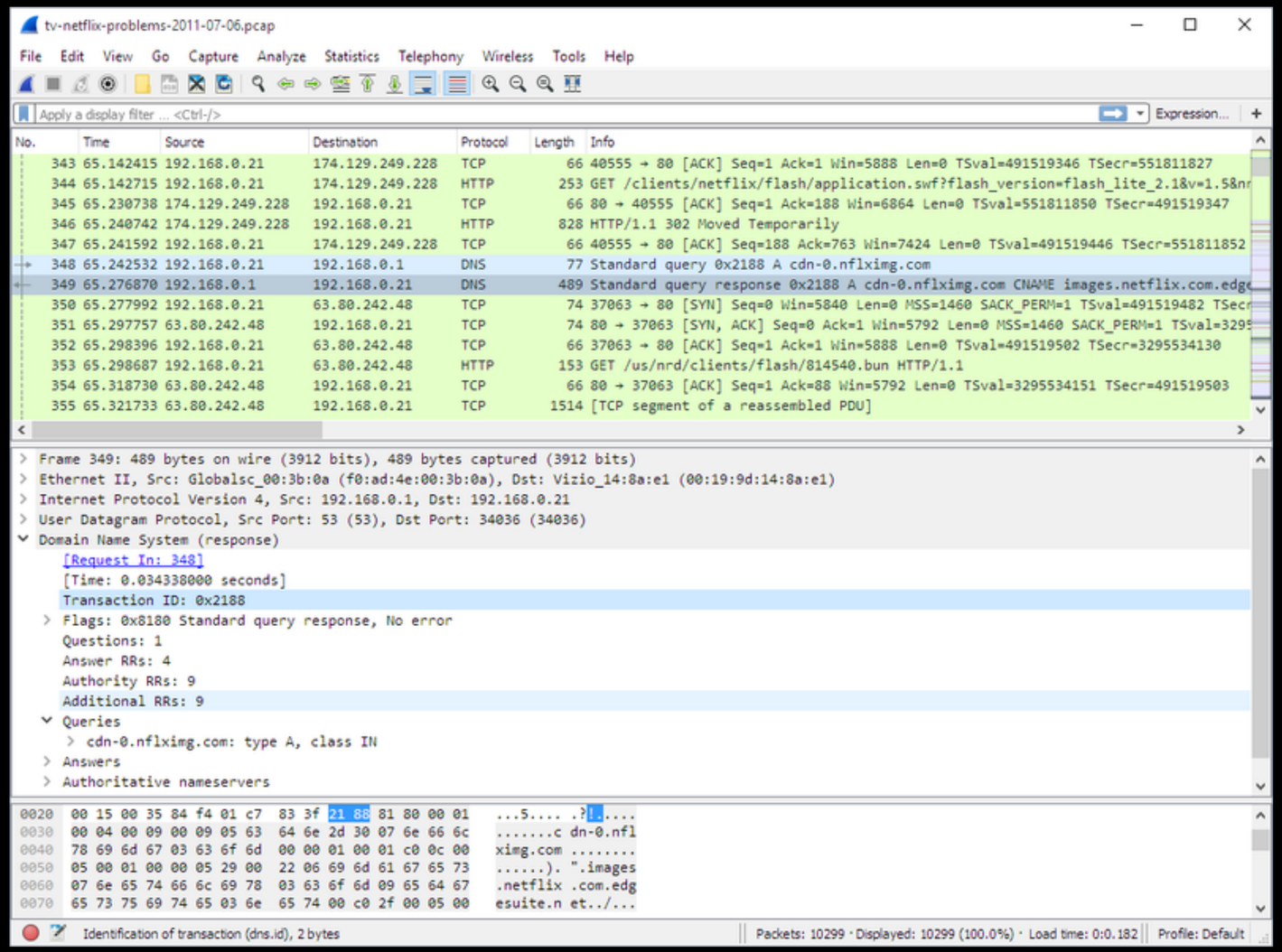
# 3. FILE EXTENTION

if a file is provided in a challenge, we can proceed as the following:

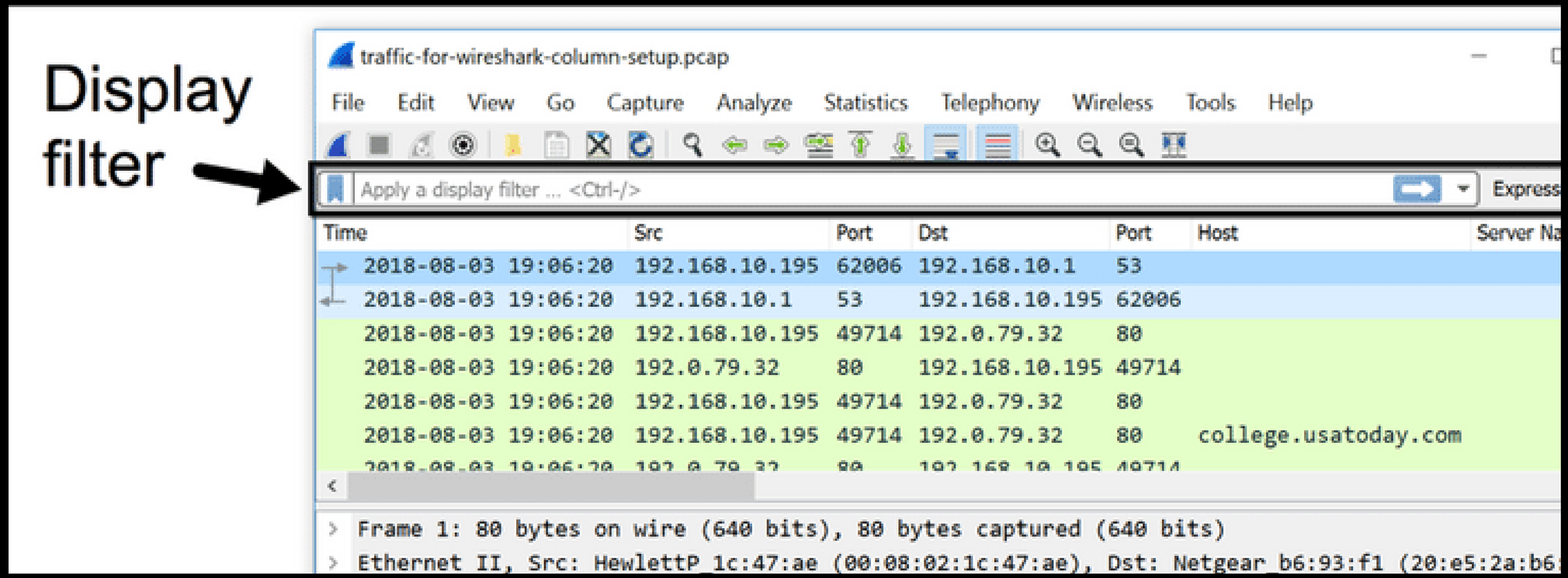
- Open the file with a normal text editor (it can be human-readable) .
- Don't forget to use **strings** command, it can reveal helpful info.
- Identify the file (google the extension and how to open that kind of files).
- Sometimes file extensions are tricky or the file is provided without extension, so try to use its magic bytes or its signature to identify it.
- Don't forget also to see the file's description ('**exiftool**' in linux).
- See if the file contains another file ('**binwalk**' in linux).
- See if the file has a password.

# 4. INTRO TO WIRESHARK

Wireshark is a network protocol analyzer, or an application that **captures** packets from a network connection, such as from your computer to your home office or the internet. Packet is the name given to a discrete unit of data in a typical Ethernet network



# 4.1 FILTERING PACKETS




- WIRESHARK DISPLAY FILTERS

# 4.2 EXTACTING FILES

Occasionally, a PCAP file can have a transferred file (via a protocol like HTTP or SMB) from the PCAP and doing some further analysis on that file. Files transferred via HTTP can be extracted from a PCAP in Wireshark via the **File -> Export Objects -> HTTP** option. The same can be done for SMB-transferred files via the **File -> Export Objects -> SMB** option

- EXTACT THE DATA FROM THIS FILE, AND FIND THE FLAG

# 5. CAPTURE PACKETS OF A HTTP/HTTPS WEBSITE - DEMO

HTTP: stands for Hypertext Transfer Protocol. When you enter http:// in your address bar in front of the domain, it tells the browser to connect over HTTP.

HTTPS: HTTP but secure (use encryption). When you enter https:// in your address bar in front of the domain, it tells the browser to connect over HTTPS.

No encryption ==> Data transferred in clear text ==> Easy to capture with Wireshark

**Demo - Capturing HTTP/HTTPS Traffic**

# 5. CAPTURE PACKETS OF A HTTP/HTTPS WEBSITE - DEMO

The HTTP communication of a certain user was captured in a PCAP file. Can you retrieve the flag ?

# 6. RECOVER DATA FROM DISK IMAGES - DEMO

## DISK IMAGE:

A disk image is an electronic copy of a drive. It’s a bit-by-bit or bitstream file that’s an exact, unaltered copy of the media being duplicated.

Disk Images extensions: *.iso *.raw *.dmg *.mdf *.nrg *.bin *.001 *.002 *.aa *.ab *.e01 *.e02 *.vmdk *.vhd

A tool to create those disk images: AccessData FTK Imager

Tools to extract data from disk images: AutoPsy, testdisk, Sleuthkit ...

**Demo - AutoPsy**

# 7. EXTRACTING DATA FROM MEMORY CAPTURE - DEMO

## MEMORY CAPTURE:

A memory dump (also known as a core dump or system dump) is a snapshot capture of computer memory data from a specific instant.

Memory image extensions: *.raw *.mem *.vmem ...

Tools to extract data from disk images: Volatility ...

**Demo - Volatility**

# 7. EXTRACTING DATA FROM MEMORY CAPTURE - DEMO

## SOME VOLATILITY OPTIONS:

volatility -f image.raw imageinfo #get info about the capture, and get suggested profiles to use

One unique profile can be used

volatility -f image.raw --profile=Selected_Profile pslist #to list all processes

volatility -f image.raw --profile=Selected_Profile psxview #to list all processes with hidden procecces

volatility -f image.raw --profile=Selected_Profile netscan #to list all the connections

volatility -f image.raw --profile=Selected_Profile ldrmodules #full check on each process, 3 columns appear: InLoad, InInit, InMem. If anyone is false it is likely to be injected

volatility -f image.raw --profile=Selected_Profile apihooks #see processes disassembly

volatility -f image.raw --profile=Selected_Profile malfind -D directory #detect injected code and dump the files found in directory “directory”tract file in the address 0x….

# ANY QUESTIONS ?