



# Digital Forensic

---

By Ravel



01

---

**File Format**

02

---

**Steganography**

03

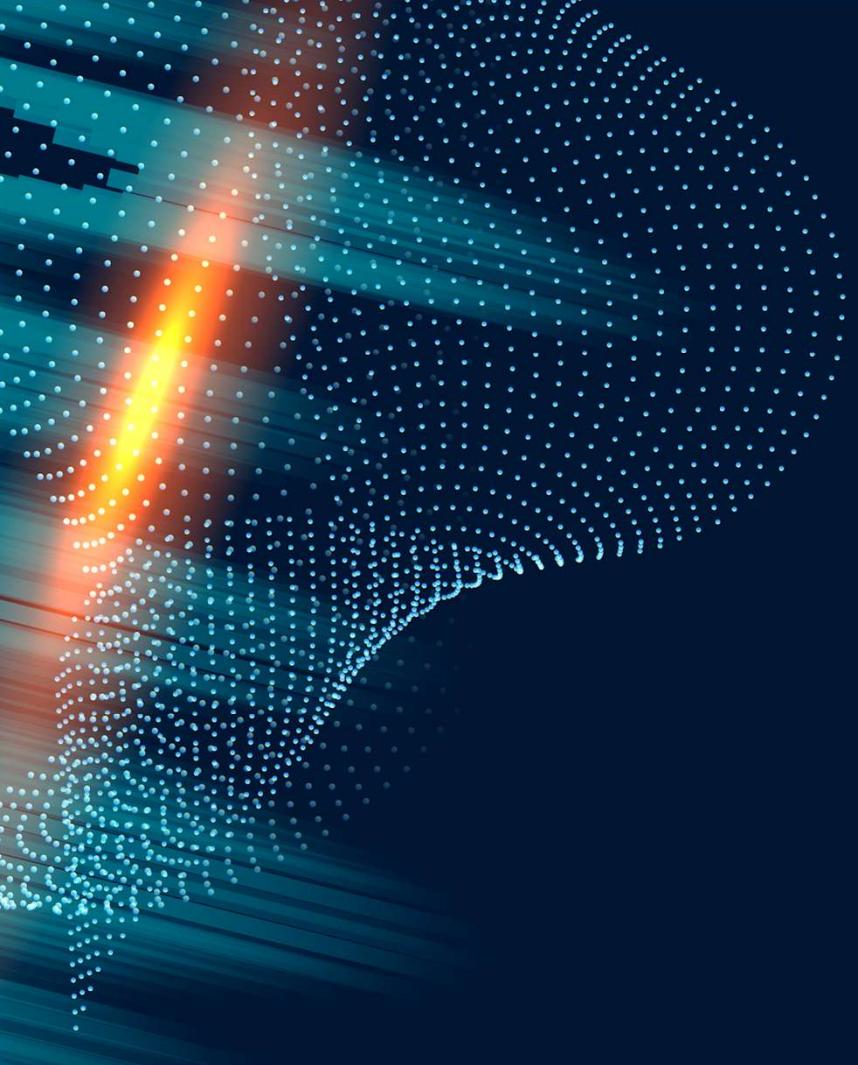
---

**Network Traffic**

04

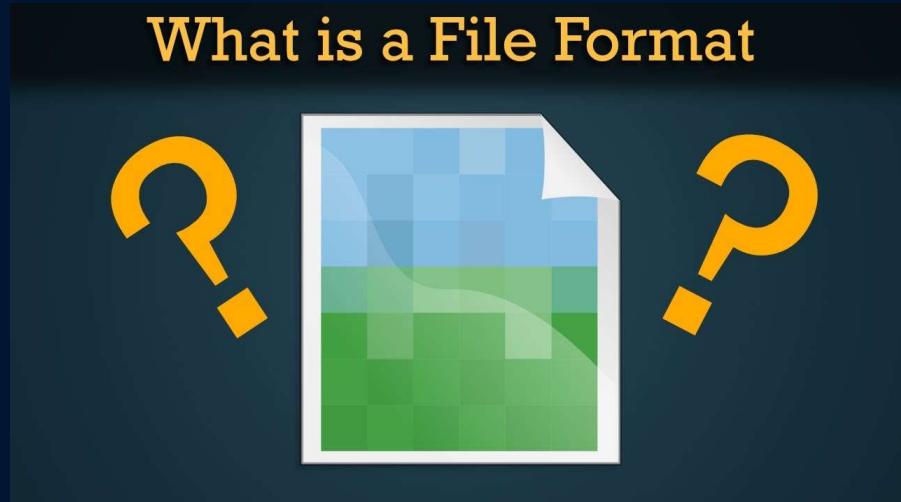
---

**Memory dump**



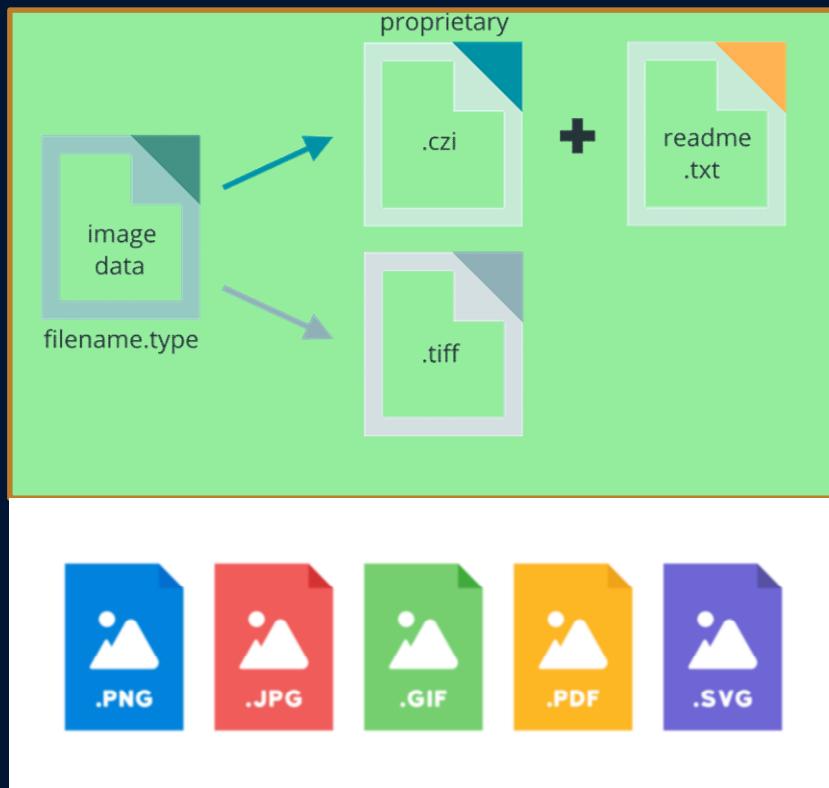
# File Format

What is a File Format

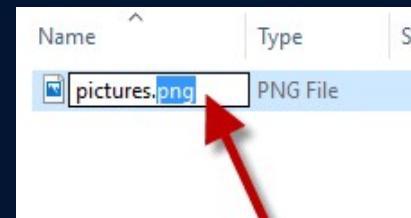


How does a computer know what  
is the type of the file?

# File extension?



**File Extensions** are not the sole way to identify the type of a file, files have certain leading bytes called **file signatures** which allow programs to parse the data in a consistent manner. Files can also contain additional "hidden" data called **metadata** which can be useful in finding out information about the context of a file's data.



**File signatures** which allow programs to parse the data in a consistent manner.  
Files can also contain additional "hidden" data called **metadata**



## “file” command in Linux

```
(raviel㉿kali)-[~/Desktop]
$ file Random_pic.jpg
Random_pic.jpg: JPEG image data, JFIF standard 1.01, aspect ratio, density 72x7
3x2048, components 3

(raviel㉿kali)-[~/Desktop]
$ file Random_pic
Random_pic: JPEG image data, JFIF standard 1.01, aspect ratio, density 72x72, s
48, components 3

(raviel㉿kali)-[~/Desktop]
$ file pwn_cheatsheet.txt
pwn_cheatsheet.txt: Python script, ASCII text executable

(raviel㉿kali)-[~/Desktop]
$ file -h
Usage: file [-bcCdEhikLlNnprsSvZZ0] [--apple] [--extension] [--mime-encoding]
           [--mime-type] [-e <testname>] [-F <separator>] [-f <namefile>]
           [-m <magicfiles>] [-P <parameter=value>] [--exclude-quiet]
           <file> ...
       file -C [-m <magicfiles>]
       file [--help]
```



pwn\_cheatsheet.txt



Random\_pic



Random\_pic.jpg

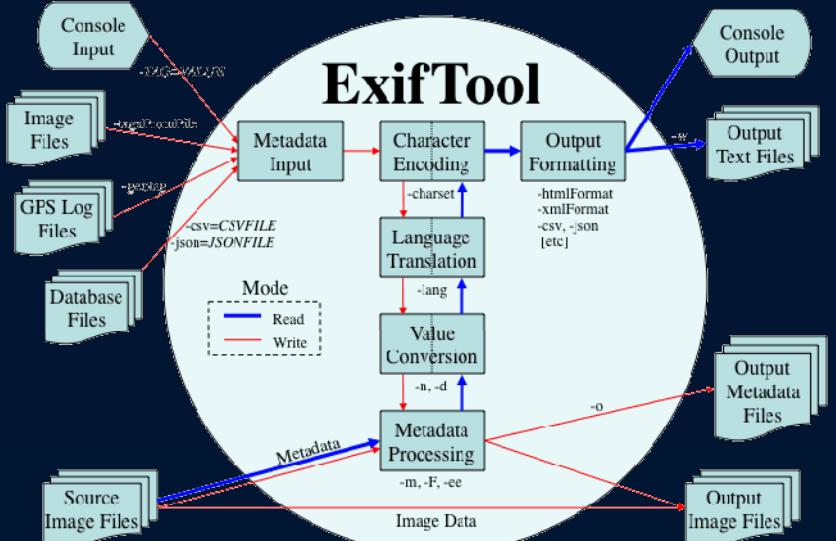
# Metadata

Metadata is data about data.  
Different types of files have  
different metadata. The  
metadata on a photo could  
include **dates, camera  
information, GPS location,  
comments, etc.**



```
File Name : C7qraX0.png
Directory :
File Size : 1014 kB
File Modification Date/Time : 2014:07:04 12:40:58-04:00
File Access Date/Time : 2015:07:11 21:38:58-04:00
File Creation Date/Time : 2015:07:11 21:38:58-04:00
File Permissions : rW-rW-rW-
File Type : PNG
File Type Extension : png
MIME Type : image/png
Image Width : 1920
Image Height : 1080
Bit Depth : 8
Color Type : RGB with Alpha
Compression : Deflate/Inflate
Filter : Adaptive
Interlace : Noninterlaced
Pixels Per Unit X : 2835
Pixels Per Unit Y : 2835
Pixel Units : meters
Profile Name : Photoshop ICC profile
Profile CMH Type : appl
Profile Version : 2.1.0
Profile Class : Display Device Profile
Color Space Data : RGB
Profile Connection Space : XYZ
Profile Date Time : 2014:06:08 20:13:16
Profile File Signature : acsp
Primary Platform : Apple Computer Inc.
CMH Flags : Not Embedded, Independent
Device Manufacturer :
Device Model :
Device Attributes : Reflective, Glossy, Positive, Color
Rendering Intent : Media-Relative Colorimetric
Connection Space Illuminant : 0.9642 1 0.62491
Profile Creator : appl
Profile ID : 0
Profile Description : Display
Profile Description ML (hr-HR) : LCD u boji
Profile Description ML (ko-KR) : 모니터 LCD
Profile Description ML (nb-NO) : Farge-LCD
Profile Description ML (hu-HU) : Színes LCD
Profile Description ML (cs-CZ) : Barevný LCD
Profile Description ML (da-DK) : LCD-farveSkærm
Profile Description ML (uk-UA) : Цвітний LCD
Profile Description ML (it-IT) : LCD colori
```

## How exiftool work?



[Click here](#)

## **Exiftool -a <add/file>**

```
[raveli@kali:~/Desktop]$ exiftool -a 115194173_p0_master1200.jpg
ExifTool Version Number : 12.76
File Name : 115194173_p0_master1200.jpg
Directory : .
File Size : 1334 kB
File Modification Date/Time : 2024:06:04 04:28:27-04:00
File Access Date/Time : 2024:06:04 04:28:39-04:00
File Inode Change Date/Time : 2024:06:04 04:28:38-04:00
File Permissions : -rw-
File Type : JPEG
File Type Extension : jpg
MIME Type : image/jpeg
JFIF Version : 1.01
Resolution Unit : None
X Resolution : 1
Y Resolution : 1
Profile CMM Type : Linotronic
Profile Version : 2.1.0
Profile Class : Display Device Profile
Color Space Data : RGB
Profile Connection Space : XYZ
Profile Date Time : 1998:02:09 06:49:00
Profile File Signature : acsp
Primary Platform : Microsoft Corporation
CMM Flags : Not Embedded, Independent
Device Manufacturer : Hewlett-Packard
Device Model : sRGB
Device Attributes : Reflective, Glossy, Positive, Color
Rendering Intent : perceptual
Connection Space Illuminant : 0.9642 1 0.82491
Profile Creator : Hewlett-Packard
Profile ID : 0
Profile Copyright : Copyright (c) 1998 Hewlett-Packard Company
Profile Description : sRGB IEC61966-2.1
Media White Point : 0.95045 1 1.08905
Media Black Point : 0 0 0
```

# File signatures

(magic numbers or Magic Bytes)

**file signatures** are  
datas used to  
identify or verify  
the content of a file

Random\_pic.jpg x

Address	Hex	ASCII	Description
00000000	FF D8 FF E0 00 10 4A 46 49 46	...JFIF....H	Header
00000010	00 48 00 00 FF DB 00 43 00 04 04 04 04 04 04 07	H...C...	
00000020	04 04 07 0A 07 07 07 0A 0D 0A 0A 0A 0A 0D 10 0D	.....	
00000030	0D 0D 0D 0D 10 14 10 10 10 10 10 10 14 14 14 14	.....	
00000040	14 14 14 14 18 18 18 18 18 18 18 18 1C 1C 1C 1C 1F	.....	
00000050	1F 1F 1F 1F 1F 1F 1F 1F 1F FF DB 00 43 01 05 05	.....C...	
00000060	05 08 07 08 0E 07 07 0E 20 16 12 16 20 20 20 20 20	.....	
00000070	20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20	.....	
00000080	20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20	.....	
00000090	20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20	.....	
000000A0	00 11 08 08 00 06 11 03 01 22 00 02 11 01 03 11	....."	
000000B0	01 FF C4 00 1C 00 00 01 05 01 01 01 00 00 00 00	.....	
000000C0	00 00 00 00 00 00 01 00 02 03 04 05 06 07 08 FF	.....	
000000D0	C4 00 1B 01 00 02 03 01 01 01 00 00 00 00 00 00	.....	
000000E0	00 00 00 00 00 01 02 03 04 05 06 07 FF DA 00 0C	.....F...	
000000F0	03 01 00 02 10 03 10 00 00 01 F2 30 87 47 1D 34	.....@0cG.4	
00000100	85 16 A4 90 14 8B 41 02 32 43 9A 8C 15 16 D2 88	...nE.iA.2C0i..T	
00000110	24 88 02 8B 48 38 02 41 01 08 02 49 31 24 41 38	\$e.iH8.A...I1\$A8	
00000120	38 17 45 CF EE 6A CB EA 5C 7F 61 C0 76 3C 9E 9D	8.E <i>eiw2\oalv&lt;P\$</i>	
00000130	FF D9	+	Header & Footer

## Image Files

File type	Typical extension	Hex digits xx = variable	Ascii digits . = not an ascii char
Bitmap format	.bmp	42 4d	BM
FITS format	.fits	53 49 4d 50 4c 45	SIMPLE
GIF format	.gif	47 49 46 38	GIF8
Graphics Kernel System	.gks	47 4b 53 4d	GKSM
IRIS rgb format	.rgb	01 da	..
ITC (CMU WM) format	.itc	f1 00 40 bb	...
JPEG File Interchange Format	.jpg	ff d8 ff e0	...
NIFF (Navy TIFF)	.nif	49 49 4e 31	IIN1
PM format	.pm	56 49 45 57	VIEW
PNG format	.png	89 50 4e 47	.PNG
Postscript format	.[e]ps	25 21	%!
Sun Rasterfile	.ras	59 a6 6a 95	Yj.
Targa format	.tga	xx xx xx	...
TIFF format (Motorola - big endian)	.tif	4d 4d 00 2a	MM.*
TIFF format (Intel - little endian)	.tif	49 49 2a 00	II*.
X11 Bitmap format	.xbm	xx xx	
XCF Gimp file structure	.xcf	67 69 6d 70 20 78 63 66 20 76	gimp xcf
Xfig format	.fig	23 46 49 47	#FIG
XPM format	.xpm	2f 2a 20 58 50 4d 20 2a 2f	/* XPM */

## Compressed files

File type	Typical extension	Hex digits xx = variable	Ascii digits . = not an ascii char
Bzip	.bz	42 5a	BZ
Compress	.Z	1f 9d	..
gzip format	.gz	1f 8b	..
pkzip format	.zip	50 4b 03 04	PK..

## Archive files

File type	Typical extension	Hex digits xx = variable	Ascii digits . = not an ascii char
TAR (pre-POSIX)	.tar	xx xx	(a filename)
TAR (POSIX)	.tar	75 73 74 61 72	ustar (offset by 257 bytes)

## Executable files

File type	Typical extension	Hex digits xx = variable	Ascii digits . = not an ascii char
MS-DOS, OS/2 or MS Windows		4d 5a	MZ
Unix elf		7f 45 4c 46	.ELF

# Corrupted File?

```
corrupted.jpg x
00000000 DC 00 FE E1 20 10 4A 47 50 16 00 01 01 00 00 48
00000010 00 48 00 00 FF DB 00 43 00 04 04 04 04 04 04 04 07
00000020 04 04 07 0A 07 07 07 0A 0D 0A 0A 0A 0A 0A 0D 10 0D
00000030 0D 0D 0D 0D 10 14 10 10 10 10 10 10 10 14 14 14
00000040 14 14 14 14 18 18 18 18 18 18 1C 1C 1C 1C 1C 1F
00000050 1F 1F 1F 1F 1F 1F 1F 1F 1F FF DB 00 43 01 05 05
00000060 05 08 07 08 0E 07 07 0E 20 16 12 16 20 20 20 20
00000070 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20
00000080 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20
...
(ravie@kali)-[~/Desktop]
$ file corrupted.jpg
corrupted.jpg: data
```

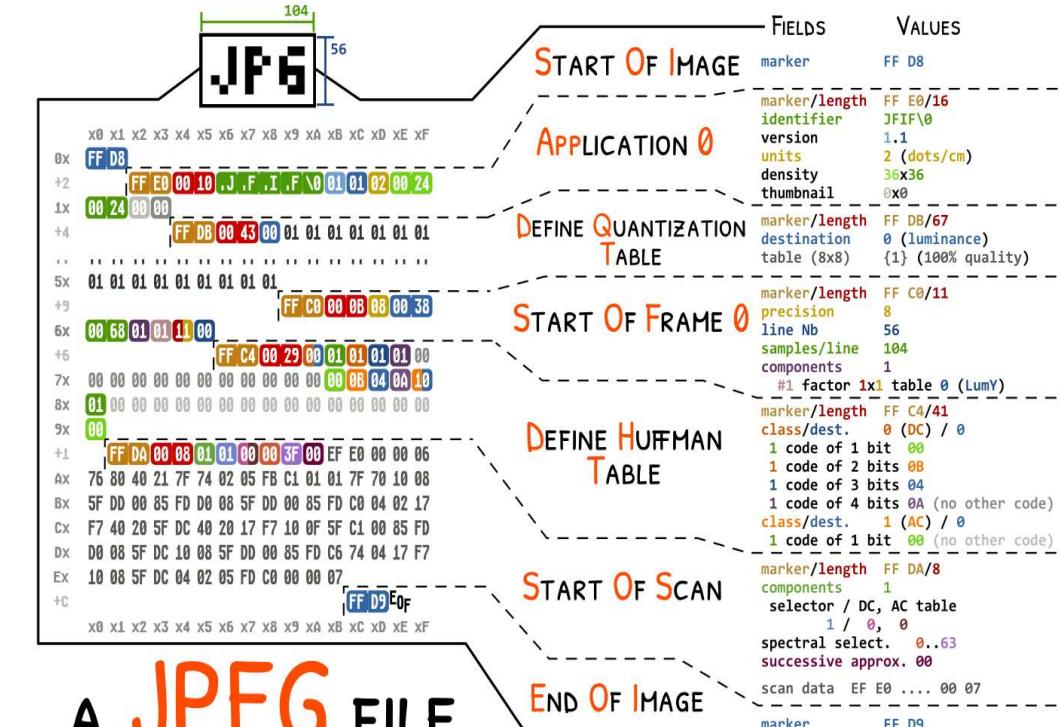


corrupted.jpg



corrupted.jpg

It looks like we don't support this file format.



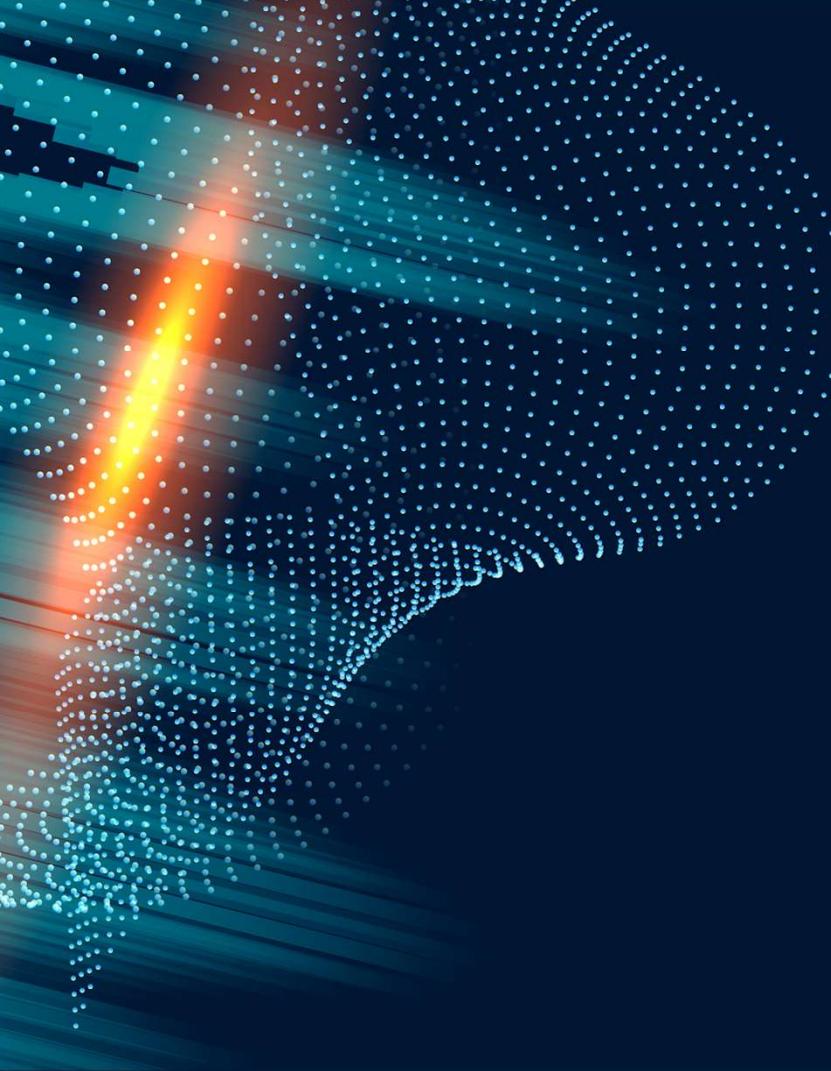
A **JPEG** FILE

ANGE ALBERTINI 2022 (CC BY 4.0)

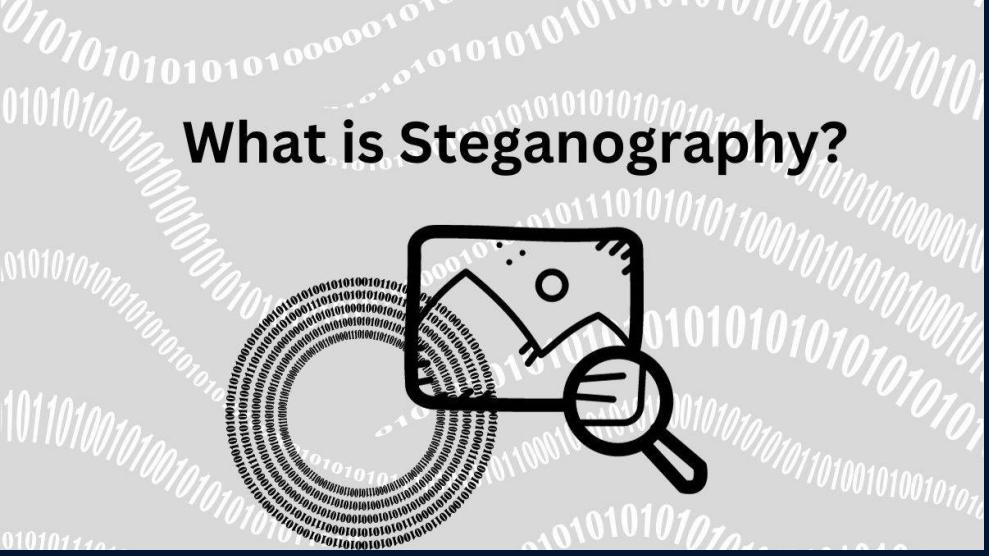
# steganography

---





# steganography

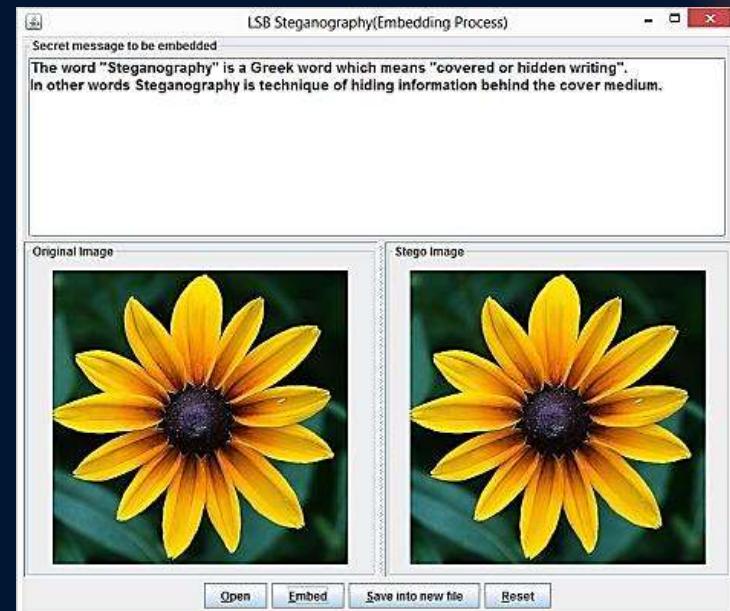
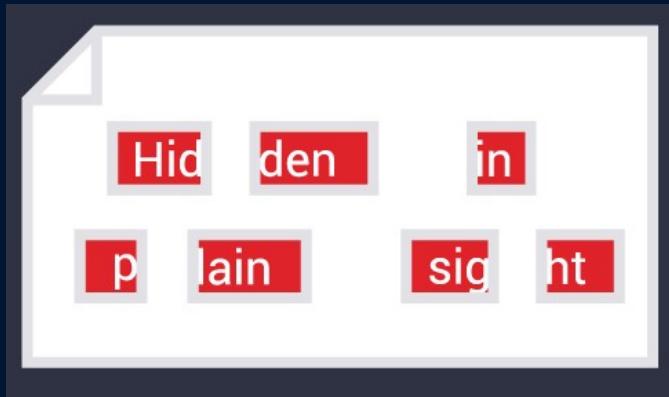


What is Steganography?



# Image Steganography

Based on what we have learnt so far, can you give me an idea how to hide a “data” inside an image



# Strings Command

We can use Strings to crawl all the printable ascii-letters in a file's data

## Manual

Strings <add/name>

```
(raviel㉿kali)-[~/Desktop]
└─$ strings chall
/lib64/ld-linux-x86-64.so.2
__libc_start_main
__gmon_start_
_ITM_deregisterTMClockTable
_ITM_registerTMClockTable
__cxa_finalize
__edata
__bss_start
__end
printf
_isoc99_scanf
libc.so.6
GLIBC_2.2.5
GLIBC_2.7
GLIBC_2.34
libc++.so.1
libc++abi.so.1
libunwind.so.1
libstdc++.so.6
libm.so.6
libgcc_s.so.1
```

```
(raviel㉿kali)-[~/Desktop]
└─$ echo "this is some printable ascii-letters" > flag

(raviel㉿kali)-[~/Desktop]
└─$ strings flag
this is some printable ascii-letters

(raviel㉿kali)-[~/Desktop]
└─$ strings flag > output.txt

(raviel㉿kali)-[~/Desktop]
└─$ cat output.txt
this is some printable ascii-letters
```

You can also use ">" <name>.<ext> to print the output to a file

# Dimensional Hidden text

How can you determine  
the image's size?  
Open properties?

Image	—
Image ID	
Dimensions	1553 x 2048
Width	1553 pixels
Height	2048 pixels



Raviel{ n0w\_u\_Kn0W\_d0m41n\_3xp4ns10n }

# JPG image height

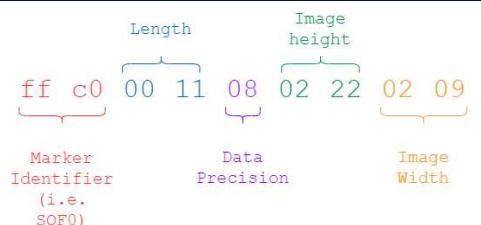


spot the difference yet?



Raveli{n0w\_u\_Kn0W\_d0m41n\_3xp4ns10n}

```
test.jpg x Random_pic.jpg x
FF D8 FF E0 00 10 4A 46 49 46 00 01 01 01 00 60
00 60 00 00 FF E1 00 22 45 78 69 66 00 00 4D 4D
00 2A 00 00 00 08 00 01 01 12 00 03 00 00 00 00 01
00 01 00 00 00 00 00 00 FF DB 00 43 00 02 01 01
02 01 01 02 02 02 02 02 02 02 03 05 03 03 03
03 03 06 04 04 03 05 07 06 07 07 06 07 07 08
09 0B 09 08 08 0A 08 07 07 0A 0D 0A 0A 0B 0C 0C
0C 0C 07 09 0E 0F 0D 0C 0E 0B 0C 0C 0C FF DB 00
43 01 02 02 02 03 03 03 06 03 03 06 0C 08 07 08
0C 0C
0C 0C 0C 0C 0C 0C 0C 0C 0C 0C 0C 0C 0C 0C 0C 0C
0C 0C 0C 0C 0C 0C 0C 0C 0C 0C 0C 0C 0C 0C 0C 0C
0C 0C FF C0 00 11 08 07 C0 06 10 03 01 22 00 02
11 01 03 11 01 FF C4 00 1F 00 00 01 05 01 01 01
01 01 01 00 00 00 00 00 00 00 01 02 03 04 05
06 07 08 09 0A 0B FF C4 00 B5 10 00 02 01 03 03
02 04 02 05 05 04 04 00 00 01 02 03 02 03 02 04
```



```
test.jpg x Random_pic.jpg x
FF D8 FF E0 00 10 4A 46 49 46 00 01 01 01 00 60
00 60 00 00 FF E1 00 22 45 78 69 66 00 00 4D 4D
00 2A 00 00 00 08 00 01 01 12 00 03 00 00 00 00 01
00 01 00 00 00 00 00 00 FF DB 00 43 00 02 01 01
02 01 01 02 02 02 02 02 02 02 03 05 03 03 03
03 03 06 04 04 03 05 07 06 07 07 06 07 07 08
09 0B 09 08 08 0A 08 07 07 0A 0D 0A 0A 0B 0C 0C
0C 0C 07 09 0E 0F 0D 0C 0E 0B 0C 0C 0C FF DB 00
43 01 02 02 02 03 03 03 06 03 03 06 0C 08 07 08
0C 0C
0C 0C 0C 0C 0C 0C 0C 0C 0C 0C 0C 0C 0C 0C 0C 0C
0C 0C 0C 0C 0C 0C 0C 0C 0C 0C 0C 0C 0C 0C 0C 0C
0C 0C FF C0 00 11 08 08 C0 06 10 03 01 22 00 02
11 01 03 11 01 FF C4 00 1F 00 00 01 05 01 01 01
01 01 01 00 00 00 00 00 00 00 01 02 03 04 05
06 07 08 09 0A 0B FF C4 00 B5 10 00 02 01 03 03
02 04 02 05 05 04 04 00 00 01 02 03 02 03 02 04
```

# PNG image height



spot the difference yet?



Ravel{4n0th3r\_Fl4g}

changed.png × png\_pic.png ×

```
89 50 4E 47 0D 0A 1A 0A 00 00 00 00 0D 49 48 44 52  
00 00 03 A0 00 00 05 10 08 06 00 00 00 09 A7 88  
2D 00 00 00 01 73 52 47 42 00 AE CE 1C E9 00 00  
00 04 67 41 4D 41 00 00 B1 8F 0B FC 61 05 00 00  
00 09 70 48 59 73 00 00 0E F2 00 00 0E F2 01 CE  
14 7B DE 00 00 00 11 74 45 58 74 54 69 74 6C 65
```

changed.png × png\_pic.png ×

```
89 50 4E 47 0D 0A 1A 0A 00 00 00 00 0D  
00 00 03 A0 00 00 05 92 08 06 00 00  
2D 00 00 00 01 73 52 47 42 00 AE CE  
00 04 67 41 4D 41 00 00 B1 8F 0B FC  
00 09 70 48 59 73 00 00 0E F2 00 00  
14 7B DE 00 00 00 11 74 45 58 74 54
```

# Extract hidden file from image

## Manual

**steghide extract -sf <add\name> (jpg,bmp only)**

```
(raviel㉿kali)-[~/Desktop]
$ steghide extract -sf Random_pic.jpg
Enter passphrase: ←
wrote extracted data to "flag".
```

they do require a password  
but you can find it by using  
other methods or just press  
Enter

**binwalk --dd='.\*' <add/name>**

```
(raviel㉿kali)-[~/Desktop]
$ binwalk --dd='.*' Random_pic.jpg

DECIMAL      HEXADECIMAL      DESCRIPTION
-----      -----      -----
0            0x0            JPEG image data, JFIF standard 1.01
```

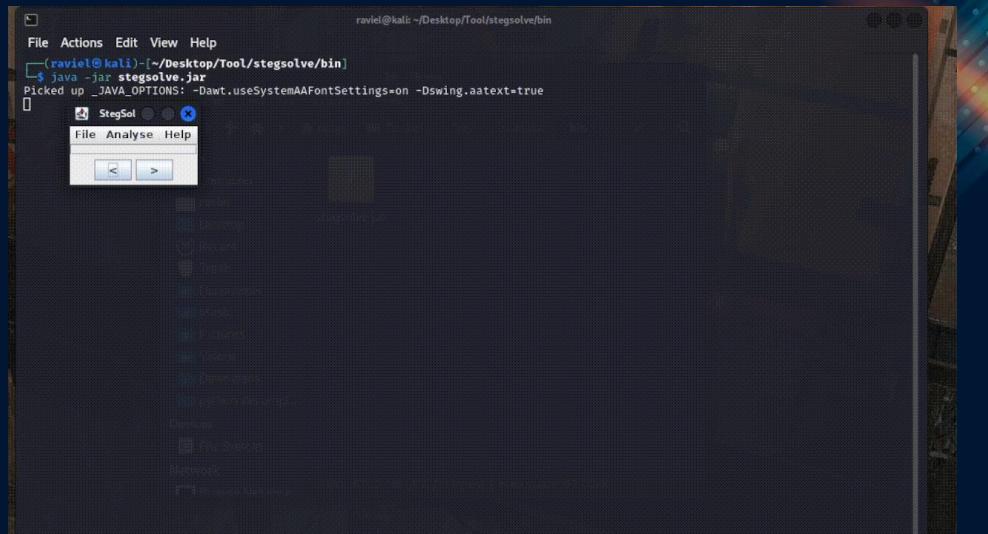
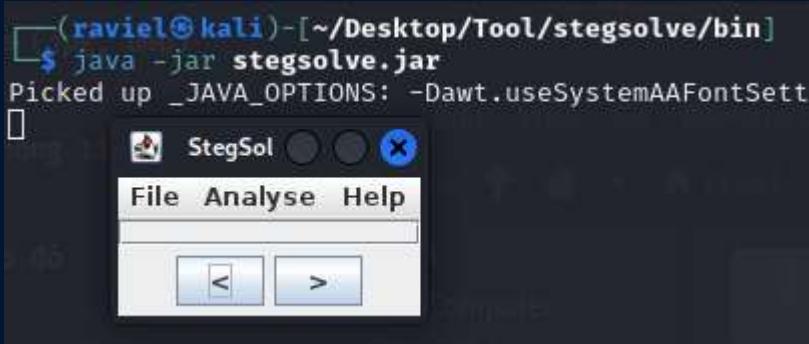
# Extract hidden text in plain colour

## Install stegsolve.jar

```
wget http://www.caesum.com/handbook/Stegsolve.jar -O stegsolve.jar  
chmod +x stegsolve.jar
```

## Run stegsolve.jar

```
java -jar stegsolve.jar
```



(Gif Example)

# LSB/MSB (sigbits)

## Install:

pip install Pillow

git clone https://github.com/Pulho/sigBits

## Manual:

\*python sigBits.py --type=LSB + <add/name> (if the picture look completely normal)

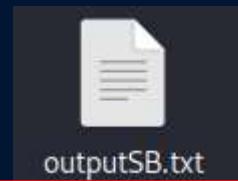
\*python sigBits.py --type=MSB + <add/name> (if the picture's colour is corrupted)



This is an  
example of MSB

```
(raviel㉿kali)-[~/Desktop/Tool/sigBits]  
└─$ python sigBits.py --type=MSB MSB.png  
Done, check the output file!
```

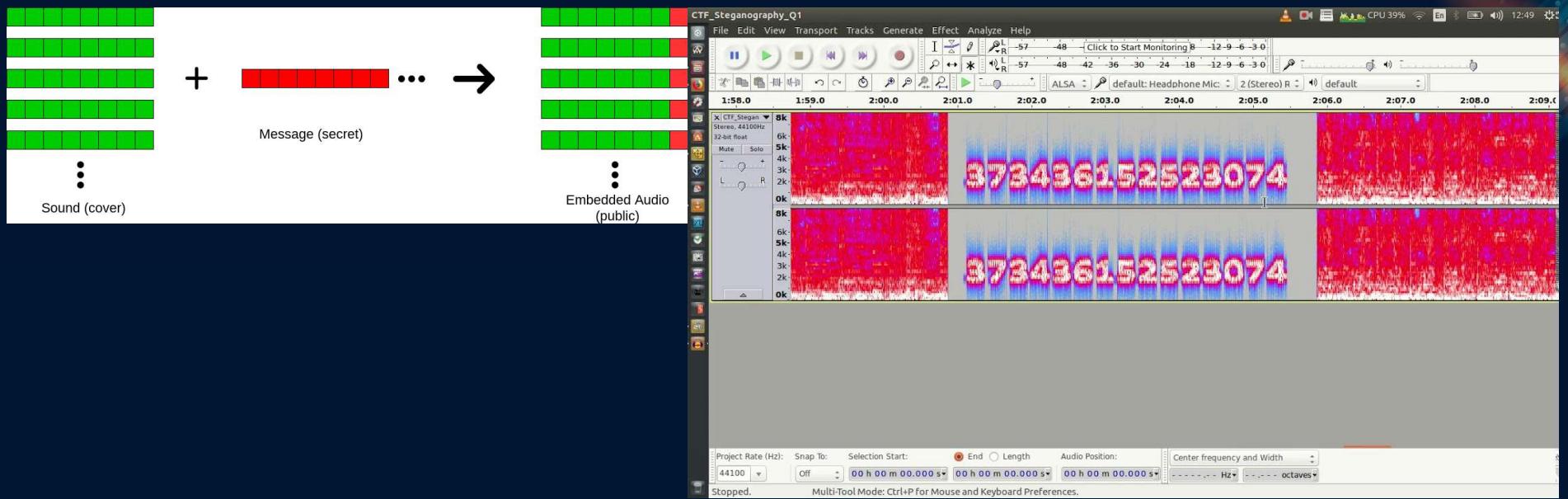
After using the command there will be an output file named outputSB.txt



Since the file contain enormous amount of letters its may crash or froze your VM, it should be opened on your real machine!!!

# Audio Steganography

**Audio Steganography is a technique used to transmit hidden information by modifying an audio signal in an imperceptible manner.**



# **Slow down/speed up/revert Audio**

**One of the most common  
task in audio steganography**



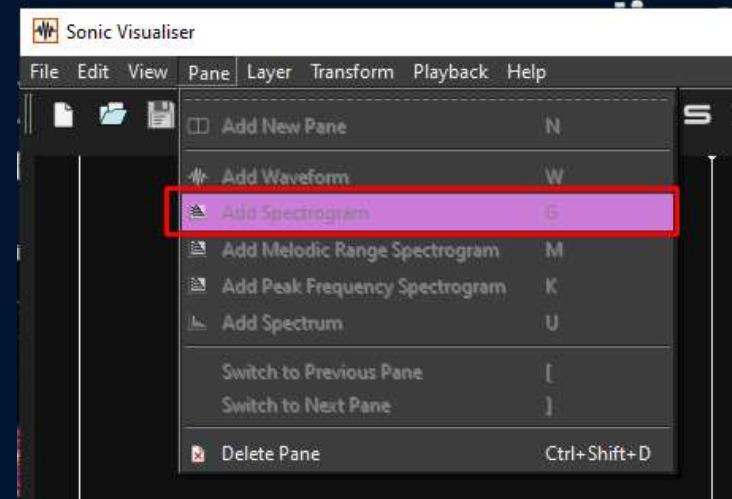
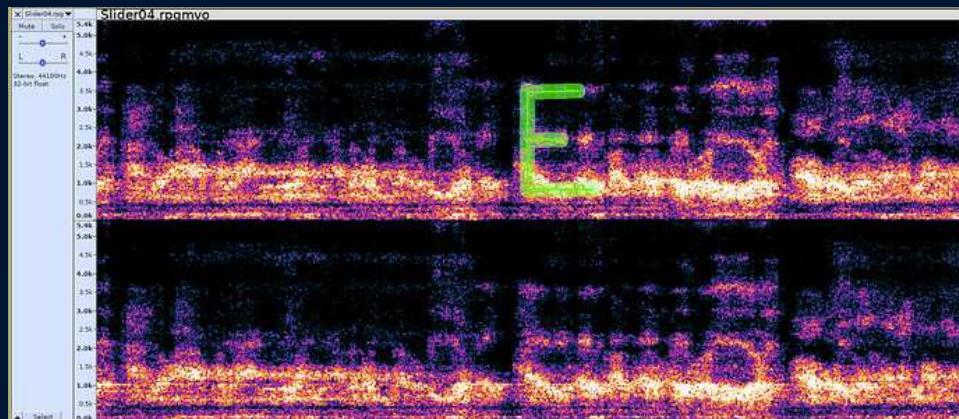
**Original Audio**

**After repairing  
The audio**



# Spectrogram

Sometime time they may hid word in spectrogram, you can use some application such as audacity, sonic visualizer, then show spectrogram to observe



## Encoded Audio

Sometime audio steganography  
can be really guessy



Do you know what type  
of encoding this is?

**HINT:** How did pictures from  
the moon landing get sent  
back to Earth?

ANS

SOLUTION

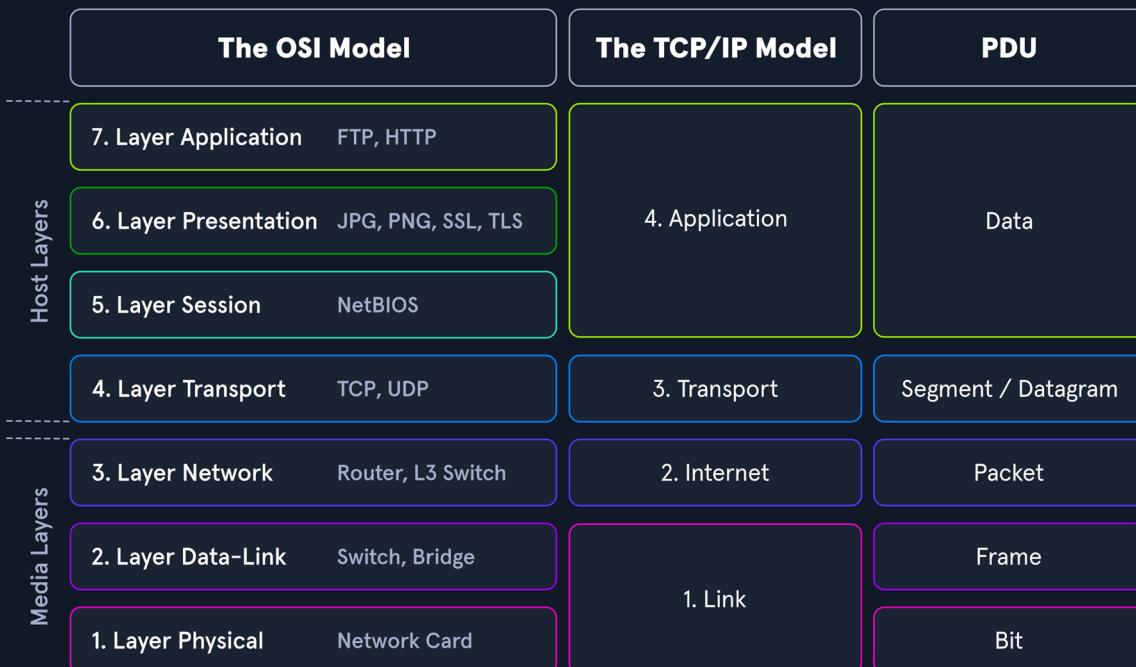


# Network Traffic

---

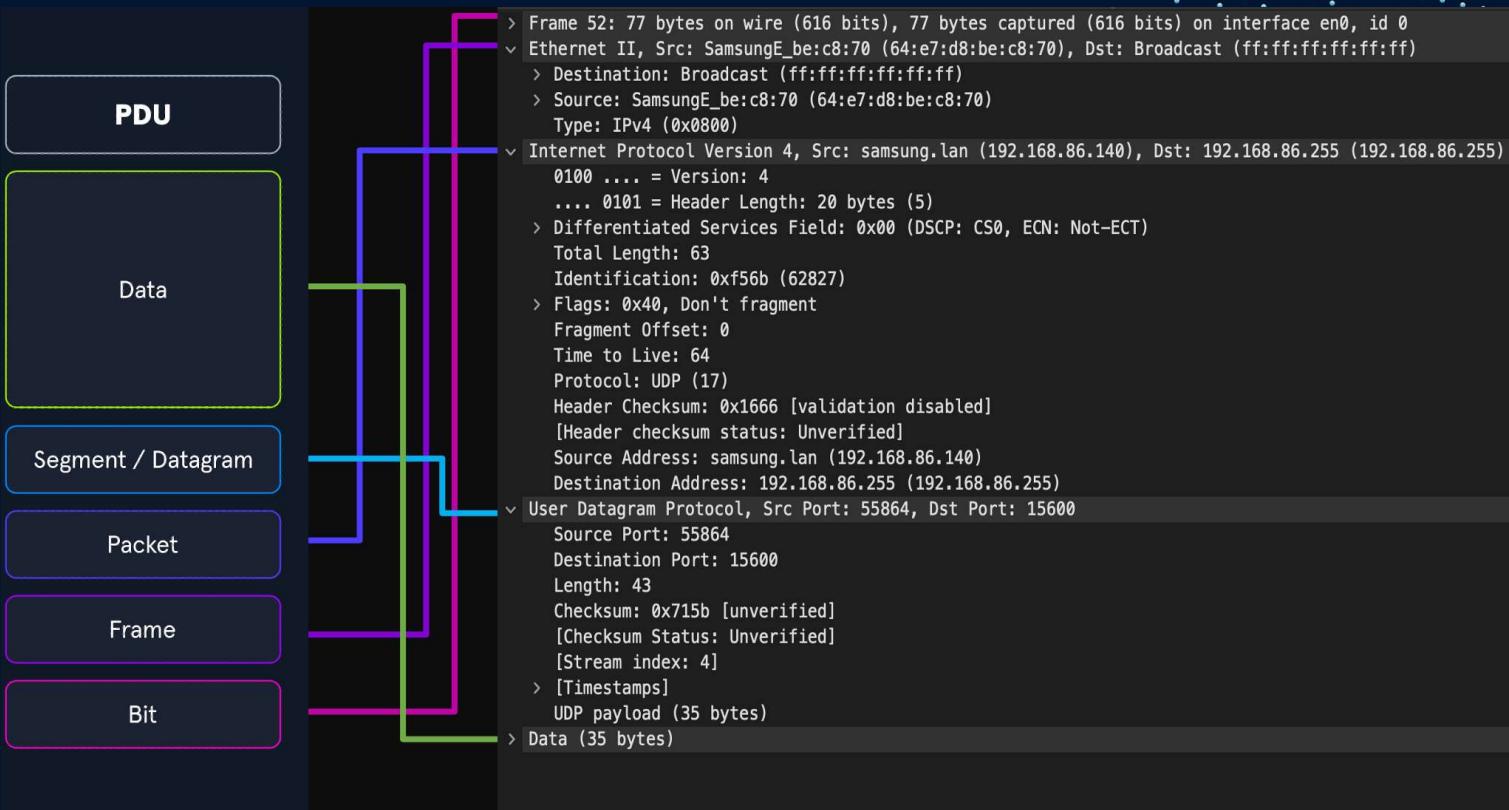
# Review

**Before going into Network traffic,  
we need some revision**



**OSI model?  
UDP, TCP?  
IP, Port?**

# PDU Packet Breakdown



## IPv4/IPv6/Mac

Which is IPv4, IPv6 and Mac address?

IPv4:

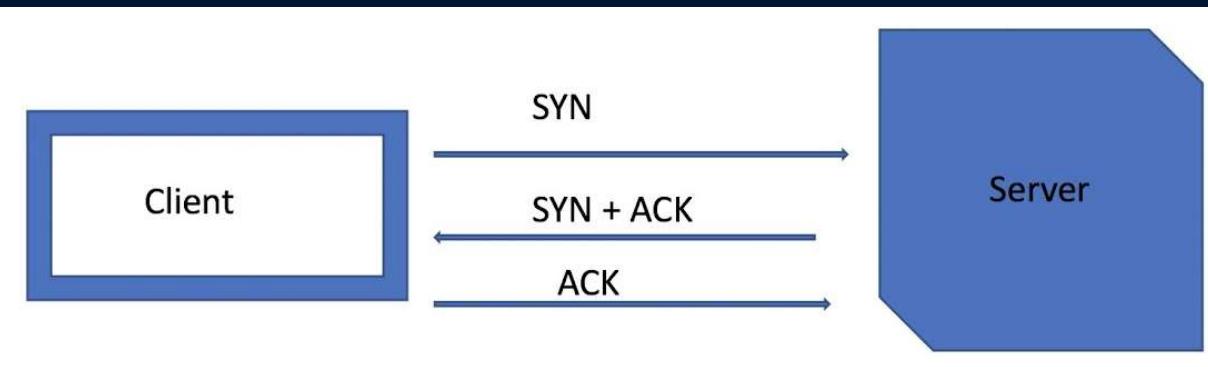
ANS

IPv6:

MAC:

```
en0: flags=8863<UP,BROADCAST,SMART,RUNNING,SIMPLEX,MULTICAST> mtu 1500
      options=400<CHANNEL_IO>
      ether 88:66:5a:11:bb:36
      inet6 fe80::49f:e3c:bf36:9bb1%en0 prefixlen 64 secured scopeid 0x6
      inet 192.168.86.243 netmask 0xffffffff broadcast 192.168.86.255
        nd6 options=201<PERFORMNUD,DAD>
        media: autoselect
        status: active
```

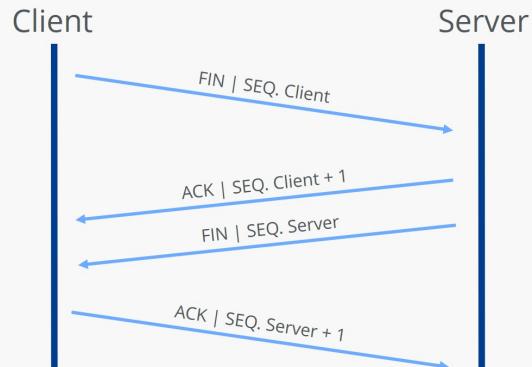
# TCP Three-way Handshake



Source	Destination	Protocol	Length	Info
192.168.1.140	174.143.213.184	TCP	74	57678 → 80 [SYN] Seq=0 Win=5840 Len=0 MSS=
174.143.213.184	192.168.1.140	TCP	74	80 → 57678 [SYN, ACK] Seq=0 Ack=1 Win=5792
192.168.1.140	174.143.213.184	TCP	66	57678 → 80 [ACK] Seq=1 Ack=1 Win=888 Len=
192.168.1.140	174.143.213.184	HTTP	200	GET /images/Layout/logo.png HTTP/1.0
174.143.213.184	192.168.1.140	TCP	66	80 → 57678 [ACK] Seq=1 Ack=135 Win=6912 Len=
174.143.213.184	192.168.1.140	TCP	1514	80 → 57678 [ACK] Seq=1 Ack=135 Win=6912 Len=
192.168.1.140	174.143.213.184	TCP	66	57678 → 80 [ACK] Seq=135 Ack=1449 Win=8832
174.143.213.184	192.168.1.140	TCP	1514	80 → 57678 [ACK] Seq=1449 Ack=135 Win=6912
192.168.1.140	174.143.213.184	TCP	66	57678 → 80 [ACK] Seq=135 Ack=2897 Win=1164
174.143.213.184	192.168.1.140	TCP	1514	80 → 57678 [ACK] Seq=2897 Ack=135 Win=6912
192.168.1.140	174.143.213.184	TCP	66	57678 → 80 [ACK] Seq=135 Ack=4345 Win=1459
174.143.213.184	192.168.1.140	TCP	1514	80 → 57678 [ACK] Seq=4345 Ack=135 Win=6912
192.168.1.140	174.143.213.184	TCP	66	57678 → 80 [ACK] Seq=135 Ack=5793 Win=1753
174.143.213.184	192.168.1.140	TCP	1514	80 → 57678 [ACK] Seq=5793 Ack=135 Win=6912

# TCP Session Teardown

## TCP connection termination (TCP Teardown)



174.143.213.184	192.168.1.140	TCP	1514 80 → 57678 [ACK] Seq=15929 Ack=135
192.168.1.140	174.143.213.184	TCP	66 57678 → 80 [ACK] Seq=135 Ack=17377
174.143.213.184	192.168.1.140	TCP	1514 80 → 57678 [ACK] Seq=17377 Ack=135
192.168.1.140	174.143.213.184	TCP	66 57678 → 80 [ACK] Seq=135 Ack=18825
174.143.213.184	192.168.1.140	TCP	1514 80 → 57678 [ACK] Seq=18825 Ack=135
192.168.1.140	174.143.213.184	TCP	66 57678 → 80 [ACK] Seq=135 Ack=20273
174.143.213.184	192.168.1.140	TCP	1514 80 → 57678 [ACK] Seq=20273 Ack=135
192.168.1.140	174.143.213.184	TCP	66 57678 → 80 [ACK] Seq=135 Ack=21721
174.143.213.184	192.168.1.140	HTTP	391 HTTP/1.1 200 OK (PNG)
192.168.1.140	174.143.213.184	TCP	66 57678 → 80 [ACK] Seq=135 Ack=22046
192.168.1.140	174.143.213.184	TCP	66 57678 → 80 [FIN, ACK] Seq=135 Ack=22046
174.143.213.184	192.168.1.140	TCP	66 80 → 57678 [FIN, ACK] Seq=22046 Ack=22047
192.168.1.140	174.143.213.184	TCP	66 57678 → 80 [ACK] Seq=136 Ack=22047

# Wireshark



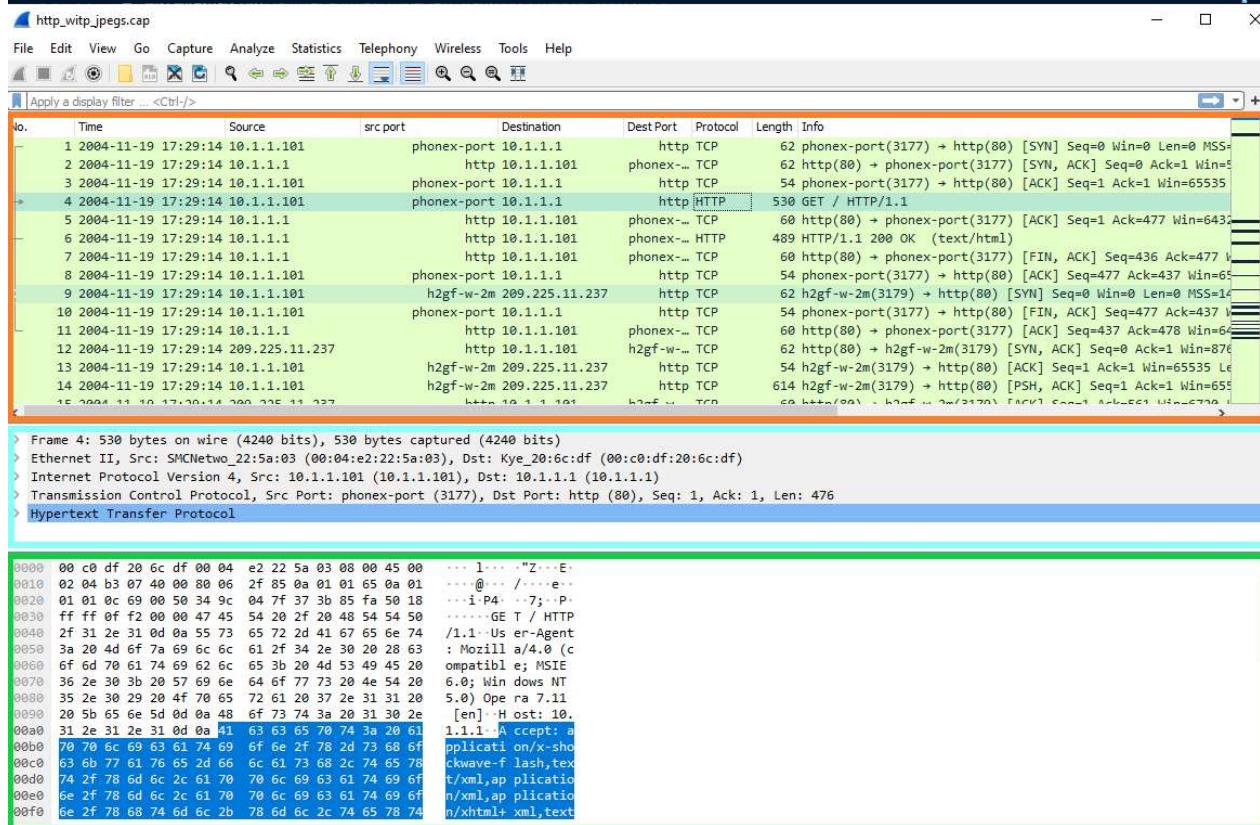
**Install (linux)**

**\$ sudo apt install wireshark**

**Install (windows)**

**<https://www.wireshark.org/download.html>**

# Wireshark GUI



## Packet List

## Packet Details

## Packet Bytes

# Packet List

No.	Time	Source	src port	Destination	Dest Port	Protocol	Length	Info
1	2004-11-19 17:29:14	10.1.1.101		phonex-port 10.1.1.1	http TCP	62	phonex-port(3177) → http(80) [SYN] Seq=0 Win=0 Len=0 MSS=1460	
2	2004-11-19 17:29:14	10.1.1.1		http 10.1.1.101	phonex... TCP	62	http(80) → phonex-port(3177) [SYN, ACK] Seq=0 Ack=1 Win=512	
3	2004-11-19 17:29:14	10.1.1.101		phonex-port 10.1.1.1	http TCP	54	phonex-port(3177) → http(80) [ACK] Seq=1 Ack=1 Win=65535	
4	2004-11-19 17:29:14	10.1.1.101		phonex-port 10.1.1.1	http HTTP	530	GET / HTTP/1.1	
5	2004-11-19 17:29:14	10.1.1.1		http 10.1.1.101	phonex... TCP	60	http(80) + phonex-port(3177) [ACK] Seq=1 Ack=477 Win=6432	
6	2004-11-19 17:29:14	10.1.1.1		http 10.1.1.101	phonex... HTTP	489	HTTP/1.1 200 OK (text/html)	
7	2004-11-19 17:29:14	10.1.1.1		http 10.1.1.101	phonex... TCP	60	http(80) → phonex-port(3177) [FIN, ACK] Seq=436 Ack=477 Win=6432	
8	2004-11-19 17:29:14	10.1.1.101		phonex-port 10.1.1.1	http TCP	54	phonex-port(3177) → http(80) [ACK] Seq=477 Ack=437 Win=65535	
9	2004-11-19 17:29:14	10.1.1.101		h2gf-w-2m 209.225.11.237	http TCP	62	h2gf-w-2m(3179) → http(80) [SYN] Seq=0 Win=0 Len=0 MSS=1460	
10	2004-11-19 17:29:14	10.1.1.101		phonex-port 10.1.1.1	http TCP	54	phonex-port(3177) → http(80) [FIN, ACK] Seq=477 Ack=437 Win=6432	
11	2004-11-19 17:29:14	10.1.1.1		http 10.1.1.101	phonex... TCP	60	http(80) + phonex-port(3177) [ACK] Seq=437 Ack=478 Win=6432	
12	2004-11-19 17:29:14	209.225.11.237		h2gf-w-2m 209.225.11.237	http TCP	62	http(80) → h2gf-w-2m(3179) [SYN, ACK] Seq=0 Ack=1 Win=876	
13	2004-11-19 17:29:14	10.1.1.101		h2gf-w-2m 209.225.11.237	http TCP	54	h2gf-w-2m(3179) → http(80) [ACK] Seq=1 Ack=1 Win=65535	
14	2004-11-19 17:29:14	10.1.1.101		h2gf-w-2m 209.225.11.237	http TCP	614	h2gf-w-2m(3179) → http(80) [PSH, ACK] Seq=1 Ack=1 Win=65535	
15	2004-11-19 17:29:14	209.225.11.237		http 10.1.1.101	h2gf-w... TCP	60	http(80) → h2gf-w-2m(3179) [ACK] Seq=1 Ack=65535 Win=6700	

In this window, we see a summary line of each packet that includes the fields listed below by default. We can add or remove columns to change what information is presented.

- Number- Order the packet arrived in Wireshark
- Time- Unix time format
- Source- Source IP
- Destination- Destination IP
- Protocol- The protocol used (TCP, UDP, DNS, ETC.)
- Information- Information about the packet. This field can vary based on the type of protocol used within. It will show, for example, what type of query it is for a DNS packet.

## Packet Details

```
> Frame 4: 530 bytes on wire (4240 bits), 530 bytes captured (4240 bits)
> Ethernet II, Src: SMCNetwo_22:5a:03 (00:04:e2:22:5a:03), Dst: Kye_20:6c:df (00:c0:df:20:6c:df)
> Internet Protocol Version 4, Src: 10.1.1.101 (10.1.1.101), Dst: 10.1.1.1 (10.1.1.1)
> Transmission Control Protocol, Src Port: phonex-port (3177), Dst Port: http (80), Seq: 1, Ack: 1, Len: 476
> Hypertext Transfer Protocol
```

The Packet Details window allows us to drill down into the packet to inspect the protocols with greater detail. It will break it down into chunks that we would expect following the typical OSI Model reference. The packet is dissected into different encapsulation layers for inspection.

Keep in mind, Wireshark will show this encapsulation in reverse order with lower layer encapsulation at the top of the window and higher levels at the bottom.

## Packet Bytes

```
0000  00 c0 df 20 6c df 00 04 e2 22 5a 03 08 00 45 00 ... l... "Z...E
0010  02 04 b3 07 40 00 80 06 2f 85 0a 01 01 65 0a 01 .....@... /....e...
0020  01 01 0c 69 00 50 34 9c 04 7f 37 3b 85 fa 50 18 ...i·P4. ·7;·P·
0030  ff ff 0f f2 00 00 47 45 54 20 2f 20 48 54 54 50 .....GE T / HTTP
0040  2f 31 2e 31 0d 0a 55 73 65 72 2d 41 67 65 6e 74 /1.1·Us er-Agent
0050  3a 20 4d 6f 7a 69 6c 6c 61 2f 34 2e 30 20 28 63 : Mozill a/4.0 (c
0060  6f 6d 70 61 74 69 62 6c 65 3b 20 4d 53 49 45 20 ompatibl e; MSIE
0070  36 2e 30 3b 20 57 69 6e 64 6f 77 73 20 4e 54 20 6.0; Win dows NT
0080  35 2e 30 29 20 4f 70 65 72 61 20 37 2e 31 31 20 5.0) Ope ra 7.11
0090  20 5b 65 6e 5d 0d 0a 48 6f 73 74 3a 20 31 30 2e [en]·H ost: 10.
00a0  31 2e 31 2e 31 0d 0a 41 63 63 65 70 74 3a 20 61 1.1.1·A ccept: a
00b0  70 70 6c 69 63 61 74 69 6f 6e 2f 78 2d 73 68 6f pplicati on/x-sho
00c0  63 6b 77 61 76 65 2d 66 6c 61 73 68 2c 74 65 78 ckwave-f lash,tx
00d0  74 2f 78 6d 6c 2c 61 70 70 6c 69 63 61 74 69 6f t/xml,ap plicatio
00e0  6e 2f 78 6d 6c 2c 61 70 70 6c 69 63 61 74 69 6f n/xml,ap plicatio
00f0  6e 2f 78 68 74 6d 6c 2b 78 6d 6c 2c 74 65 78 74 n/xhtml+xml,txt
```

The Packet Bytes window allows us to look at the packet contents in ASCII or hex output. As we select a field from the windows above, it will be highlighted in the Packet Bytes window and show us where that bit or byte falls within the overall packet.

This is a great way to validate that what we see in the Details pane is accurate and the interpretation Wireshark made matches the packet output.

Each line in the output contains the data offset, sixteen hexadecimal bytes, and sixteen ASCII bytes. Non-printable bytes are replaced with a period in the ASCII format.

# Wireshark Menu

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help



Apply a display filter ... <Ctrl-/>

## Display Filter Command Table

Display Filters	Result
ip.addr == x.x.x.x	Capture only traffic pertaining to a certain host. This is an OR statement.
ip.addr == x.x.x.x/24	Capture traffic pertaining to a specific network. This is an OR statement.
ip.src/dst == x.x.x.x	Capture traffic to or from a specific host
dns / tcp / ftp / arp / ip	filter traffic by a specific protocol. There are many more options.
tcp.port == x	filter by a specific tcp port.
tcp.port / udp.port != x	will capture everything except the port specified
and / or / not	AND will concatenate, OR will find either of two options, NOT will exclude your input option.

# Wireshark Menu

## The Statistics Tab

The screenshot shows the Wireshark interface with the Statistics tab selected. It displays several windows:

- Statistics - All Addresses - Wi-Fi**: Shows a table of all addresses with columns: Topic / Item, Count, Average, Min Val, Max Val, Rate (ms), Percent, Burst Rate, and Burst Start.
- Statistics - Conversations - Wi-Fi**: Shows a table of network conversations with columns: Address A, Address B, Packets, Bytes, Packets A → B, Bytes A → B, Packets B → A, Bytes B → A, Rel Start, Duration, Bits/s A → B, and Bits/s B → A.
- Statistics - Protocol Hierarchy Statistics - Wi-Fi**: Shows a hierarchical breakdown of protocols with columns: Protocol, Percent Packets, Packets, Percent Bytes, Bytes, Bits/s, End Packets, End Bytes, and End Bits/s.
- Protocol Details**: A detailed view of a specific protocol entry, likely Ethernet, showing its statistics.
- Frame Details**: A detailed view of a specific frame entry, showing its bytes and hex dump.

The Statistics Tab give us detailed reports about the network traffic being utilized. It can show us everything from the top talkers in our environment to specific conversations and even breakdown by IP and protocol.

# Following a packet (tcp.stream eq X)

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Apply a display filter ... <Ctrl-/>

No.	Time	Source	Destination	Protocol	Length	Info
37 2.075124089	192.168.159.128	128.136.252.75	TCP	54	45084 → 443 [ACK] Seq=514 Ack=2921 Win=62780 Len=0	
38 2.075169889	128.136.252.75	192.168.159.128	TLSv1.2	1514	Certificate [TCP segment of a reassembled PDU]	
39 2.075236688	192.168.159.128	128.136.252.75	TCP	54	45084 → 443 [ACK] Seq=514 Ack=4381 Win=61320 Len=0	
40 2.075296388	128.136.252.75	192.168.159.128	TLSv1.2	73	Server Key Exchange, Server Hello Done	
41 2.075336688	192.168.159.128	128.136.252.75	TCP	54	45084 → 443 [ACK] Seq=514 Ack=4400 Win=61320 Len=0	
42 2.088688659	192.168.159.128	128.136.252.75	TLSv1.2	180	Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message	
43 2.089171749	128.136.252.75	192.168.159.128	TCP	60	443 → 45084 [ACK] Seq=4400 Ack=640 Win=64240 Len=0	
44 2.091832741	192.168.159.128	192.168.159.2	DNS	77	Standard query 0x2444 A ocs.digicert.com	
45 2.117518667	128.136.252.75	192.168.159.128	TLSv1.2	296	New Session Ticket, Change Cipher Spec, Encrypted Handshake Message	
46 2.117574167	192.168.159.128	128.136.252.75	TCP	54	45084 → 443 [ACK] Seq=640 Ack=4642 Win=62780 Len=0	
47 2.121171257	192.168.159.2	192.168.159.128	DNS	125	Standard query response 0x2444 A ocs.digicert.com CNAME cs9.wac.phicdn.net A 72.21.91.29	
48 2.122315754	192.168.159.128	72.21.91.29	TCP	74	51696 → 80 [SYN] Seq=0 Win=64240 MSS=1460 SACK_PERM=1 TSeqval=247263667 TSeqr=0 WS=128	
49 2.143878093	72.21.91.29	192.168.159.128	TCP	60	80 → 51696 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460	
50 2.144170592	192.168.159.128	72.21.91.29	TCP	54	51696 → 80 [ACK] Seq=1 Ack=1 Win=64240 Len=0	
51 2.148263981	192.168.159.128	72.21.91.29	OCSP	425	Request	
52 2.149391977	72.21.91.29	192.168.159.128	TCP	60	80 → 51696 [ACK] Seq=1 Ack=372 Win=64240 Len=0	
53 2.287330884	72.21.91.29	192.168.159.128	OCSP	819	Response	
54 2.287374284	192.168.159.128	72.21.91.29	TCP	54	51696 → 80 [ACK] Seq=372 Ack=766 Win=63495 Len=0	
55 2.291426272	192.168.159.128	128.136.252.75	TCP	60	80 → 407 Application Data	

Frame 51: 425 bytes on wire (3400 bits), 425 bytes captured (3400 bits) on interface eth0, id 0

Ethernet II, Src: VMware\_38:b3:d0 (00:0c:29:38:b3:d0), Dst: VMware\_f7:fc:70 (00:50:56:f7:fc:70)

Internet Protocol Version 4, Src: 192.168.159.128, Dst: 72.21.91.29

Transmission Control Protocol, Src Port: 51696, Dst Port: 80, Seq: 1, Ack: 1, Len: 371

Hypertext Transfer Protocol

Online Certificate Status Protocol

Packets: 10788 · Displayed: 10788 (100.0%) · Dropped: 0 (0.0%)

Profile: Default

Num Lock Off

wireshark\_eth0\_20210209210759\_xfAmk5.pcapng

# Extract Files From The GUI

http\_with\_jpegs.cap

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

http

No.	Time	Source	Destination	Protocol	Length	Info
46	01:36:69	10.1.1.101	10.1.1.1	HTTP	599	GET / HTTP/1.1
60	03:22:89	10.1.1.1	10.1.1.101	HTTP	489	HTTP/1.1 200 OK (text/html)
160	04:49:49	10.1.1.101	209.225.11.237	HTTP	487	POST /scripts/cms/xcms.asp HTTP/1.1 (application/vnd.xacp)
190	05:46:40	209.225.11.237	10.1.1.101	HTTP	68	[TCP Previous segment not captured] Continuation
311	1:28:39:85	10.1.1.101	10.1.1.1	HTTP	628	GET /websidan/index.html HTTP/1.1
381	1:29:23:67	10.1.1.1	10.1.1.101	HTTP	275	HTTP/1.1 200 OK (text/html)
481	1:40:36:83	10.1.1.101	10.1.1.1	HTTP	651	GET /websidan/images/bg.jpg HTTP/1.1
+ 501	1:40:49:38	10.1.1.101	10.1.1.1	HTTP	654	GET /websidan/images/sydney.jpg HTTP/1.1
611	1:41:03:60	10.1.1.1	10.1.1.101	HTTP	1320	HTTP/1.1 200 OK (JPEG JFIF image)
721	1:42:45:18	10.1.1.1	10.1.1.101	HTTP	624	HTTP/1.1 200 OK (JPEG JFIF image)
821	1:50:17:85	10.1.1.101	209.225.0.6	HTTP	1211	GET /site=126885/bnum=opera1/bins=1/opid=10030285/ver=711/dst=Win_700 HTTP/1.1
841	1:50:21:33	10.1.1.101	209.225.0.6	HTTP	1211	GET /site=126885/bnum=opera2/bins=1/opid=10030867/ver=711/dst=Win_700 HTTP/1.1
861	1:50:24:07	10.1.1.101	209.225.0.6	HTTP	1211	GET /site=126885/bnum=opera3/bins=1/opid=10032112/ver=711/dst=Win_700 HTTP/1.1
901	1:50:59:70	10.1.1.101	209.225.0.6	HTTP	1211	GET /site=126885/bnum=opera4/bins=1/opid=10003005/ver=711/dst=Win_700 HTTP/1.1
1001	1:59:45:17	209.225.0.6	10.1.1.101	HTTP	1301	[TCP Previous segment not captured] Continuation
1099	2:18:07:30	209.225.0.6	10.1.1.101	HTTP	1301	[TCP Previous segment not captured] Continuation
1202	2:57:27:73	209.225.0.6	10.1.1.101	HTTP	1301	[TCP Previous segment not captured] Continuation
1282	2:58:05:36	10.1.1.101	209.225.0.6	HTTP	1267	GET /site=0000127709/nnum=0000162763/genr=1/logs=0/mdtm=1077726643/bins=1 HTTP/1.1
1322	2:58:41:52	10.1.1.101	209.225.0.6	HTTP	1267	GET /site=0000127709/nnum=0000162763/genr=1/logs=0/mdtm=1077726643/bins=1 HTTP/1.1

Frame 72: 624 bytes on wire (4992 bits), 624 bytes captured (4992 bits)  
Ethernet II, Src: Kye-20:6c:df (00:00:00:20:6c:df), Dst: SMCNetwo\_22:5a:03 (00:04:e2:22:5a:03)  
Internet Protocol Version 4, Src: 10.1.1.1, Dst: 10.1.1.101  
Transmission Control Protocol, Src Port: 80, Dst Port: 3199, Seq: 8761, Ack: 601, Len: 570  
[7 Reassembled TCP Segments (9330 bytes): #55(1460), #63(1460), #65(1460), #67(1460), #68(1460), #70(1460), #72(570)]  
HyperText Transfer Protocol  
HTTP/1.1 200 OK  
Date: Sat, 20 Nov 2004 10:21:07 GMT\r\nServer: Apache/2.0.40 (Red Hat Linux)\r\nLast-Modified: Tue, 16 Jan 2001 05:00:00 GMT\r\nETag: "46a51-2355-d5a3f400"\r\nAccept-Ranges: bytes\r\nContent-Length: 9045\r\nConnection: close\r\nContent-Type: image/jpeg\r\nX-Pad: avoid browser bug\r\n\r\n[HTTP response 1/1]  
[Time since request: 0.019580000 seconds]  
[Request in frame: 50]

0000 00 e4 22 5a 03 00 c0 df 20 6c df 08 00 45 00 ... "Z... 1.. E:  
0010 02 62 b4 d0 40 00 40 06 6d 5e 0a 01 01 01 0a 01 b @ @ m^.....  
0020 01 65 00 50 00 76 37 ea 15 84 34 a7 0b 8a 50 19 e P V7.. 4 ..P.  
0030 19 c8 eb 50 00 3d b2 d6 01 21 54 4d e9 88 a9 ..P. = ..ITM..  
0040 82 e1 2a a8 8a 1b 79 b9 41 41 75 31 ba ee 2b de ..\*.. y AAU1 ..+.  
0050 58 c5 94 cf 89 64 73 67 03 14 d2 7a 41 bb c9 e6 X...dsg ..ZA...  
0060 18 56 ab f5 32 65 06 0d b1 11 77 73 63 c4 aa ab V 2e .. wsc...  
0070 a6 4d b0 14 ec 17 44 20 55 f7 51 10 3c 8b cd M .. D UoW <..  
0080 24 7d 20 b3 36 2e 35 63 1e f0 63 0e 48 e4 bc 1f \$} 6.5c c H..  
0090 a4 5c 75 d2 54 8e 98 f8 2d 79 73 98 2f 50 1b \u T .. -ys /P.  
00a0 e7 b9 46 db 00 25 52 61 a9 af 27 ee 10 ac 52 84 F %R .. R.  
00b0 b7 16 ba 6b 51 c8 32 bb 82 e5 45 3d e1 8d 50 9d KQ 2 E= P.  
00c0 b2 dc 46 4c 5c 79 4e 3f 31 a1 07 a7 66 04 1c KeLyN 71 ..  
00d0 63 4e db e5 a3 1e 41 0f e2 04 16 23 43 3f f9 50 cN .. A .. #C P.  
00e0 53 0d f7 65 2a 92 7c 5e 59 e5 3c 00 42 fb d4 69 S .. e\* | ^ P < B .. i.  
00f0 4f d4 3a 97 d0 65 40 7e bc fe 65 38 05 6f 1b 3e O : e@~ .. e8 o >  
0100 21 53 59 e5 92 2c 09 cb 57 d4 45 c8 25 b7 89 e3 ISY .. W E % ..  
0110 cc c5 88 b3 71 5b af ac 10 40 72 3c fd c8 ae db ..q[ .. @r< ..

Frame (624 bytes) Reassembled TCP (9330 bytes)

http\_with\_jpegs.cap

Packets: 483 · Displayed: 38 (7.9%)

Tuesday February 9, 2021

# Application layer(5-7)

## HTTP Methods(port 80 / 8000)

To perform operations such as **fetching webpages**, **requesting items for download**, or **posting** your most recent tweet all require the use of specific methods. These methods define the actions taken when requesting a URI

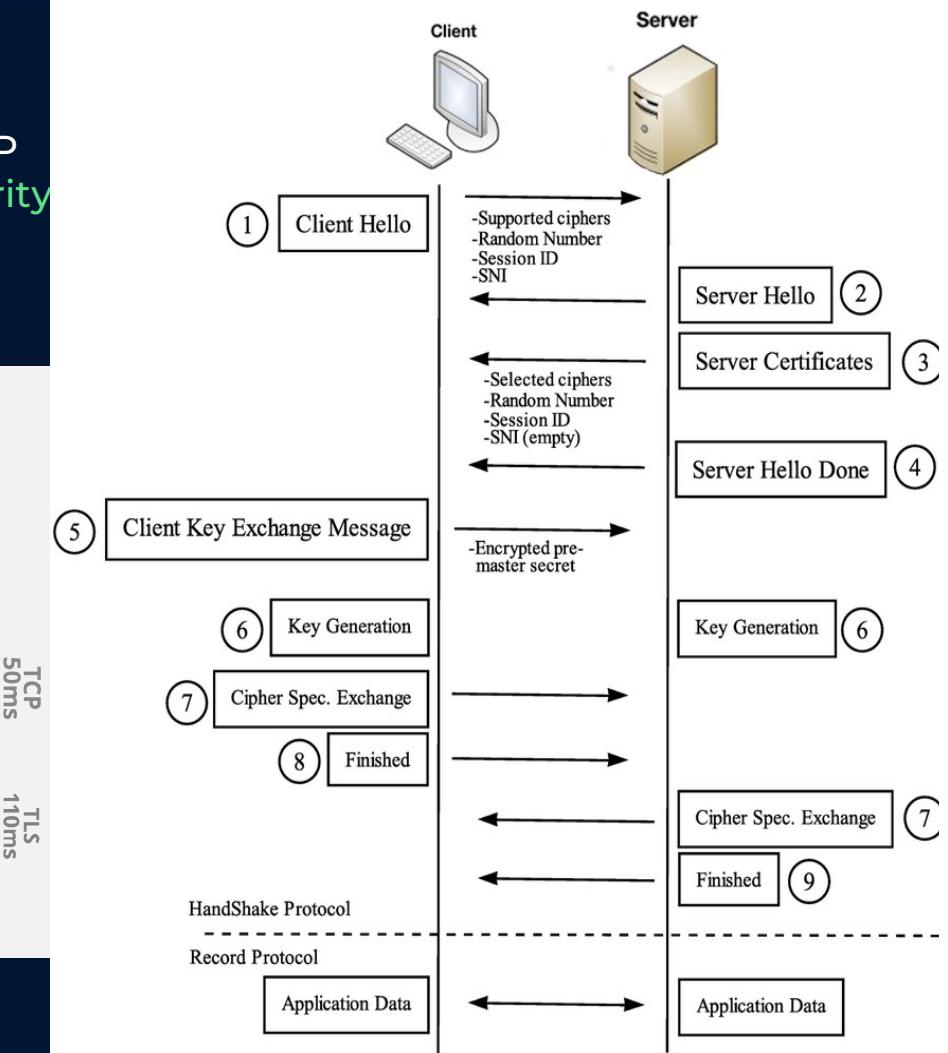
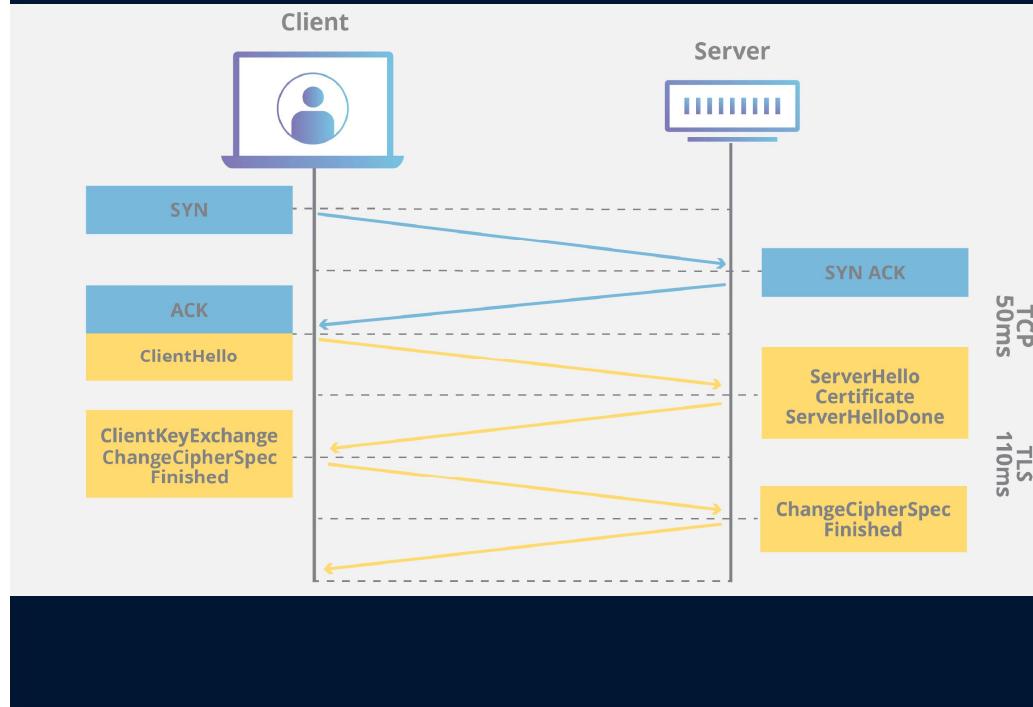


Method	Description
HEAD	<b>required</b> is a safe method that requests a response from the server similar to a Get request except that the message body is not included. It is a great way to acquire more information about the server and its operational status.
GET	<b>required</b> Get is the most common method used. It requests information and content from the server. For example, GET http://10.1.1.1/Webserver/index.html requests the index.html page from the server based on our supplied URI.
POST	<b>optional</b> Post is a way to submit information to a server based on the fields in the request. For example, submitting a message to a Facebook post or website forum is a POST action. The actual action taken can vary based on the server, and we should pay attention to the response codes sent back to validate the action.
PUT	<b>optional</b> Put will take the data appended to the message and place it under the requested URI. If an item does not exist there already, it will create one with the supplied data. If an object already exists, the new PUT will be considered the most up-to-date, and the object will be modified to match. The easiest way to visualize the differences between PUT and POST is to think of it like this; PUT will create or update an object at the URI supplied, while POST will create child entities at the provided URI. The action taken can be compared with the difference between creating a new file vs. writing comments about that file on the same page.
DELETE	<b>optional</b> Delete does as the name implies. It will remove the object at the given URI.
TRACE	<b>optional</b> Allows for remote server diagnosis. The remote server will echo the same request that was sent in its response if the TRACE method is enabled.
OPTIONS	<b>optional</b> The Options method can gather information on the supported HTTP methods the server recognizes. This way, we can determine the requirements for interacting with a specific resource or server without actually requesting data or objects from it.
CONNECT	<b>optional</b> Connect is reserved for use with Proxies or other security devices like firewalls. Connect allows for tunneling over HTTP. (SSL tunnels)

# HTTPS(port 433 / 8433)

HTTP Secure (HTTPS) is a modification of the HTTP protocol designed to utilize Transport Layer Security (TLS) or Secure Sockets Layer (SSL)

## TLS Handshake Via HTTPS



## TLS Handshake Via HTTPS

Source	Destination	Protocol	Length	Info
192.168.86.243	104.20.55.68	TCP	78	60201 → 443 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=64
104.20.55.68	192.168.86.243	TCP	66	443 → 60201 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=
192.168.86.243	104.20.55.68	TCP	54	60201 → 443 [ACK] Seq=1 Ack=1 Win=262144 Len=0
192.168.86.243	104.20.55.68	TLSv1.3	607	Client Hello
104.20.55.68	192.168.86.243	TCP	54	443 → 60201 [ACK] Seq=1 Ack=554 Win=67584 Len=0
104.20.55.68	192.168.86.243	TLSv1.3	266	Server Hello, Change Cipher Spec, Application Data
192.168.86.243	104.20.55.68	TCP	54	60201 → 443 [ACK] Seq=554 Ack=213 Win=261888 Len=0
192.168.86.243	104.20.55.68	TLSv1.3	118	Change Cipher Spec, Application Data
192.168.86.243	104.20.55.68	TLSv1.3	146	Application Data
192.168.86.243	104.20.55.68	TLSv1.3	1270	Application Data
192.168.86.243	104.20.55.68	TLSv1.3	107	Application Data
104.20.55.68	192.168.86.243	TCP	60	443 → 60201 [ACK] Seq=213 Ack=618 Win=67584 Len=0
104.20.55.68	192.168.86.243	TCP	60	443 → 60201 [ACK] Seq=213 Ack=710 Win=67584 Len=0
104.20.55.68	192.168.86.243	TLSv1.3	575	Application Data, Application Data
192.168.86.243	104.20.55.68	TCP	54	60201 → 443 [ACK] Seq=1979 Ack=734 Win=261568 Len=0
192.168.86.243	104.20.55.68	TLSv1.3	85	Application Data
104.20.55.68	192.168.86.243	TCP	60	443 → 60201 [ACK] Seq=734 Ack=1926 Win=69632 Len=0

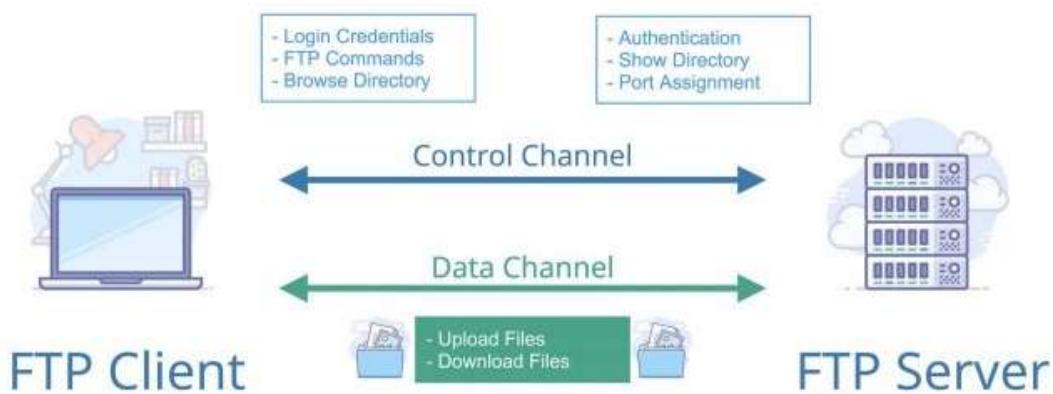
In the first few packets, we can see that the client establishes a session to the server using port 443 boxed in blue. This signals the server that it wishes to use **HTTPS** as the **application communication protocol**.

Once the session is established, all data and methods will be sent through the **TLS** connection and appear as **TLS Application Data** as seen in the red box. **TLS** is still using TCP as its **transport protocol**, so we will still see acknowledgment packets from the stream coming over port 443.

# FTP(port 20 / 21)

Port 20 is used for data transfer, while port 21 is utilized for issuing commands controlling the FTP session

**File Transfer Protocol (FTP) is an Application Layer protocol that enables quick data transfer between computing devices.**



# FTP Command & Response

**Active mode** is the default, with the server listening for a **PORT command** from the client to determine the data transfer port.

**Passive mode**, used for accessing servers behind firewalls or NAT, involves the client sending a **PASV** command to receive the IP and port details from the server for data transfer.

Protocol	src.p	dest.p	Length	Info
FTP	21	49767	97	Response: 200 Switching to Binary mode.
FTP	49767	21	73	Request: CWD /
FTP	21	49767	103	Response: 250 Directory successfully changed.
FTP	49767	21	72	Request: PASV
FTP	21	49767	116	Response: 227 Entering Passive Mode (172,16,146,2,207,99).
FTP	49767	21	84	Request: RETR secrets.txt
FTP	21	49767	135	Response: 150 Opening BINARY mode data connection for secrets.txt (46 bytes).
FTP	21	49767	90	Response: 226 Transfer complete.
FTP	21	49762	103	Response: 425 Failed to establish connection.
FTP	49769	21	82	Request: USER anonymous
FTP	21	49769	142	Response: 220 Welcome to the PowerBroker FTP service. Grab or leave juicy info here.
FTP	21	49769	100	Response: 331 Please specify the password.
FTP	49769	21	92	Request: PASS cfnetwork@apple.com
FTP	21	49769	89	Response: 230 Login successful.
FTP	49769	21	72	Request: SYST
FTP	21	49769	85	Response: 215 UNIX Type: L8
FTP	49769	21	71	Request: PWD
FTP	21	49769	100	Response: 257 "/" is the current directory
FTP	49769	21	74	Request: TYPE I
FTP	21	49769	97	Response: 200 Switching to Binary mode.
FTP	49769	21	73	Request: CWD /
FTP	21	49769	103	Response: 250 Directory successfully changed.
FTP	49769	21	72	Request: PASV
FTP	21	49769	115	Response: 227 Entering Passive Mode (172,16,146,2,95,17).
FTP	49769	21	95	Request: RETR Shield-prototype-plans
FTP	21	49769	146	Response: 150 Opening BINARY mode data connection for Shield-prototype-plans (72 bytes).
FTP	21	49769	90	Response: 226 Transfer complete.

Client Request

FTP server response

# FTP Commands Table

Command	Description
<b>USER</b>	specifies the user to log in as.
<b>PASS</b>	sends the password for the user attempting to log in.
<b>PORT</b>	when in active mode, this will change the data port used.
<b>PASV</b>	switches the connection to the server from active mode to passive.
<b>LIST</b>	displays a list of the files in the current directory.
<b>CWD</b>	will change the current working directory to one specified.
<b>PWD</b>	prints out the directory you are currently working in.
<b>SIZE</b>	will return the size of a file specified.
<b>RETR</b>	retrieves the file from the FTP server.
<b>QUIT</b>	ends the session.

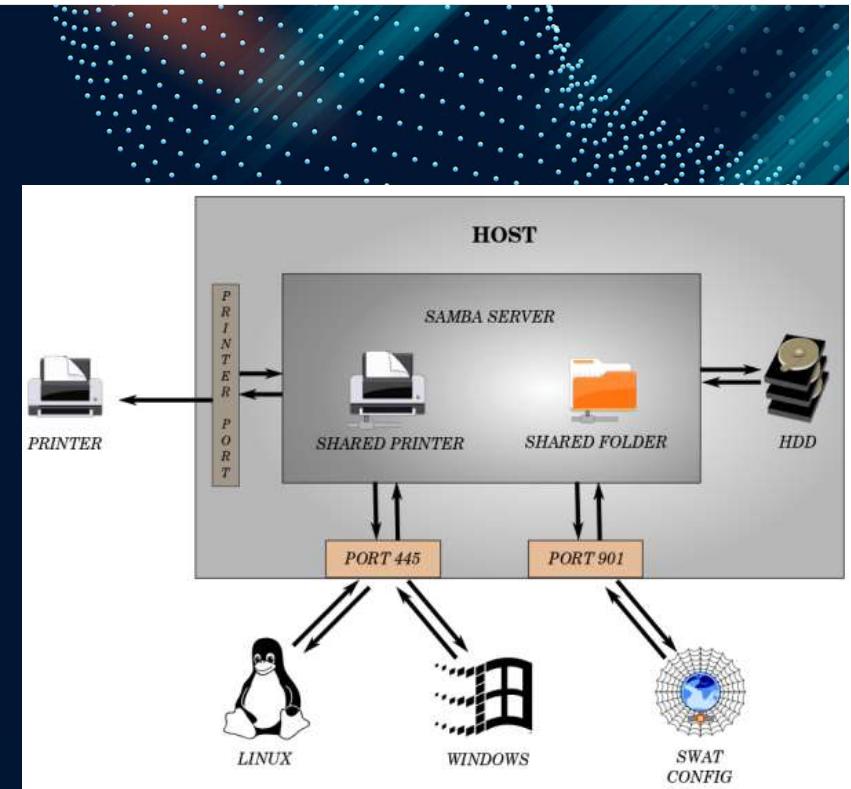
```

Info
Response: 220 Switching to Binary mode.
Request: CWD /
Response: 250 Directory successfully changed.
Request: PASV
Response: 227 Entering Passive Mode (172,16,1,10)
Request: RETR secrets.txt
Response: 150 Opening BINARY mode data connection.
Response: 226 Transfer complete.
Response: 425 Failed to establish connection.
Request: USER anonymous
Response: 220 Welcome to the PowerBroker FT
Response: 331 Please specify the password.
Request: PASS cnetwork@apple.com
Response: 230 Login successful.
Request: SYST
Response: 215 UNIX Type: L8
Request: PWD
Response: 257 "/" is the current directory.
Request: TYPE I
Response: 200 Switching to Binary mode.
Request: CWD /
Response: 250 Directory successfully changed.
Request: PASV
Response: 227 Entering Passive Mode (172,16,1,10)
Request: RETR Shield-prototype-plans
Response: 150 Opening BINARY mode data connection.
Response: 226 Transfer complete.

```

## SMB(port 137/138 [old] | port 445 (TCP) | port 139 (NetBlos) )

**Server Message Block (SMB)** is a protocol most widely seen in Windows enterprise environments that enables **sharing resources between hosts over common networking architectures.**



As a user, SMB provides us easy and convenient access to resources like printers, shared drives, authentication servers, and more. For this reason, SMB is very attractive to potential attackers as well.

Like any other application that uses TCP as its transport mechanism, it will perform standard functions like **the three-way handshake and acknowledging received packets.**

# SMB on the wire

Source	Destination	Protocol	src.p	dest.p	Length	Info
192.168.199.132	192.168.199.255	NBNS	137	137	92	Name query NB_WPAD<00>
192.168.199.132	SCV	DNS	537..	53	86	Standard query 0x142e A officeclient.microsoft.com
192.168.199.133	SCV	DNS	643..	53	92	Standard query 0xfa7d A geo-prod.do.dsp.mp.microsoft.com
VMware_61:f5:5f	SCV	ARP			42	Who has 192.168.199.1? Tell 192.168.199.133
SCV	VMware_61:f5:5f	ARP			42	192.168.199.1 is at 00:58:56:c0:00:01
192.168.199.132	192.168.199.133	TCP	496..	445	66	49670 → 445 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
192.168.199.132	192.168.199.132	TCP	445	496..	66	445 → 49670 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
192.168.199.132	192.168.199.133	TCP	496..	445	54	49670 → 445 [ACK] Seq=1 Ack=1 Win=65536 Len=0
192.168.199.132	192.168.199.133	SMB	496..	445	213	Negotiate Protocol Request
192.168.199.133	192.168.199.132	SMB2	445	496..	506	Negotiate Protocol Response
192.168.199.132	192.168.199.133	SMB2	496..	445	232	Negotiate Protocol Request
192.168.199.133	192.168.199.132	SMB2	445	496..	566	Negotiate Protocol Response
192.168.199.132	192.168.199.133	SMB2	496..	445	220	Session Setup Request, NTLMSSP_NEGOTIATE
192.168.199.133	192.168.199.132	SMB2	445	496..	401	Session Setup Response, Error: STATUS_MORE_PROCESSING_REQUIRED, NTLMSSP_CHALLENGE
192.168.199.132	192.168.199.133	SMB2	496..	445	711	Session Setup Request, NTLMSSP_AUTH, User: DESKTOP-2AEFM7G\user
192.168.199.133	192.168.199.132	SMB2	445	496..	131	Session Setup Response, Error: STATUS_LOGON_FAILURE
192.168.199.132	192.168.199.133	TCP	496..	445	54	49670 → 445 [RST, ACK] Seq=1161 Ack=1389 Win=0 Len=0
192.168.199.132	192.168.199.133	TCP	496..	445	66	49671 → 445 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
192.168.199.133	192.168.199.132	TCP	445	496..	66	445 → 49671 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
192.168.199.132	192.168.199.133	TCP	496..	445	54	49671 → 445 [ACK] Seq=1 Ack=1 Win=65536 Len=0
192.168.199.132	192.168.199.133	SMB2	496..	445	232	Negotiate Protocol Request
192.168.199.133	192.168.199.132	SMB2	445	496..	566	Negotiate Protocol Response
192.168.199.132	192.168.199.133	SMB2	496..	445	220	Session Setup Request, NTLMSSP_NEGOTIATE
192.168.199.133	192.168.199.132	SMB2	445	496..	401	Session Setup Response, Error: STATUS_MORE_PROCESSING_REQUIRED, NTLMSSP_CHALLENGE
192.168.199.132	192.168.199.133	SMB2	496..	445	711	Session Setup Request, NTLMSSP_AUTH, User: DESKTOP-2AEFM7G\user
192.168.199.133	192.168.199.132	SMB2	445	496..	131	Session Setup Response, Error: STATUS_LOGON_FAILURE
192.168.199.132	192.168.199.133	TCP	496..	445	54	49671 → 445 [RST, ACK] Seq=1002 Ack=937 Win=0 Len=0
192.168.199.132	192.168.199.133	TCP	496..	445	66	49672 → 445 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
192.168.199.133	192.168.199.132	TCP	445	496..	66	445 → 49672 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
192.168.199.132	192.168.199.133	TCP	496..	445	54	49672 → 445 [ACK] Seq=1 Ack=1 Win=65536 Len=0
192.168.199.132	192.168.199.133	SMB2	496..	445	232	Negotiate Protocol Request
192.168.199.133	192.168.199.132	SMB2	445	496..	566	Negotiate Protocol Response
192.168.199.132	192.168.199.133	SMB2	496..	445	220	Session Setup Request, NTLMSSP_NEGOTIATE

Orange box: TCP-handshake

Blue box: ports

Green box: request from user and response from SMB

Did you saw something suspicious???

# Common ports

Port Number	Protocol	Description	Port Number	Protocol	Description
20	FTP-Data	Data channel for passing FTP files.	115	SFTP	SSH File Transfer Protocol. An extension of SSH providing secure and reliable FTP services.
21	FTP-Command	Control channel for issuing commands to an FTP server.	123	NTP	Network Time Protocol. Provides timing and sync services for network devices.
22	SSH	Secure Shell Service port. Provides secure remote communications	137	Netbios-NS	Local network name resolution.
23	Telnet	Telnet service provides cleartext communications between hosts.	139	Netbios-SSN	Provides session services for data transfer. Services like SMB can utilize it.
25	SMTP	Simple Mail Transfer protocol. Utilized for email transmissions between servers.	179	BGP	Border Gateway Protocol. BGP is a protocol for exchanging routing info with autonomous systems worldwide.
53	DNS	Domain Name Services. Provides name resolution with multiple protocols	389	LDAP	Lightweight Directory Access Protocol. System agnostic authentication and authorization services.
69	TFTP	Trivial File Transfer Protocol. A lightweight, minimal-function transfer protocol.	443	HTTPS	HyperText Transfer Protocol Secure. An extension of HTTP utilizing SSL/TLS for encrypting the communications.
80	HTTP	HyperText Transfer Protocol. Provides dynamic web services	445	SMB	Server Message Block. SMB allows for the sharing of services, files, networking ports, and printers between hosts.
88	Kerberos	Providing cryptographic network authentication			
110	POP3	Mail service utilized by clients to retrieve email from a server.			
111	RPC	Remote Procedure Call. Remote service for managing network file systems.			



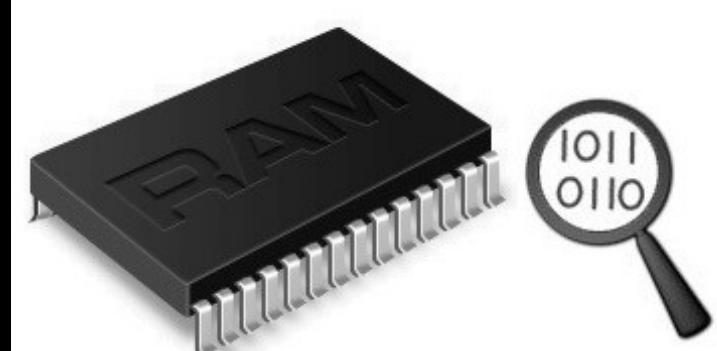
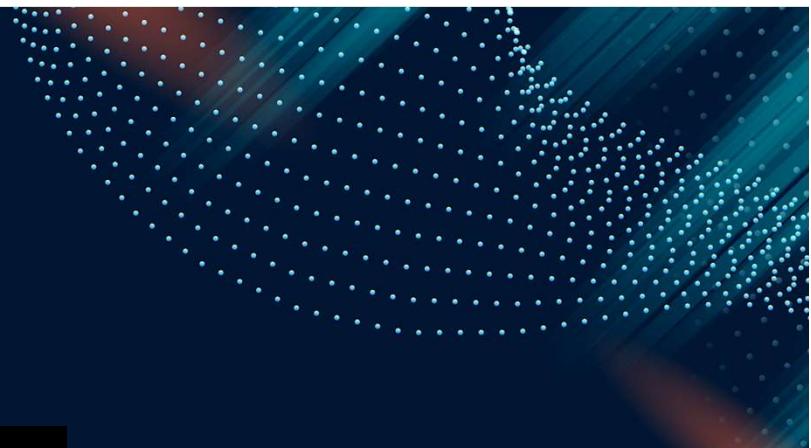
# Memory dump

---

# Memory Forensic

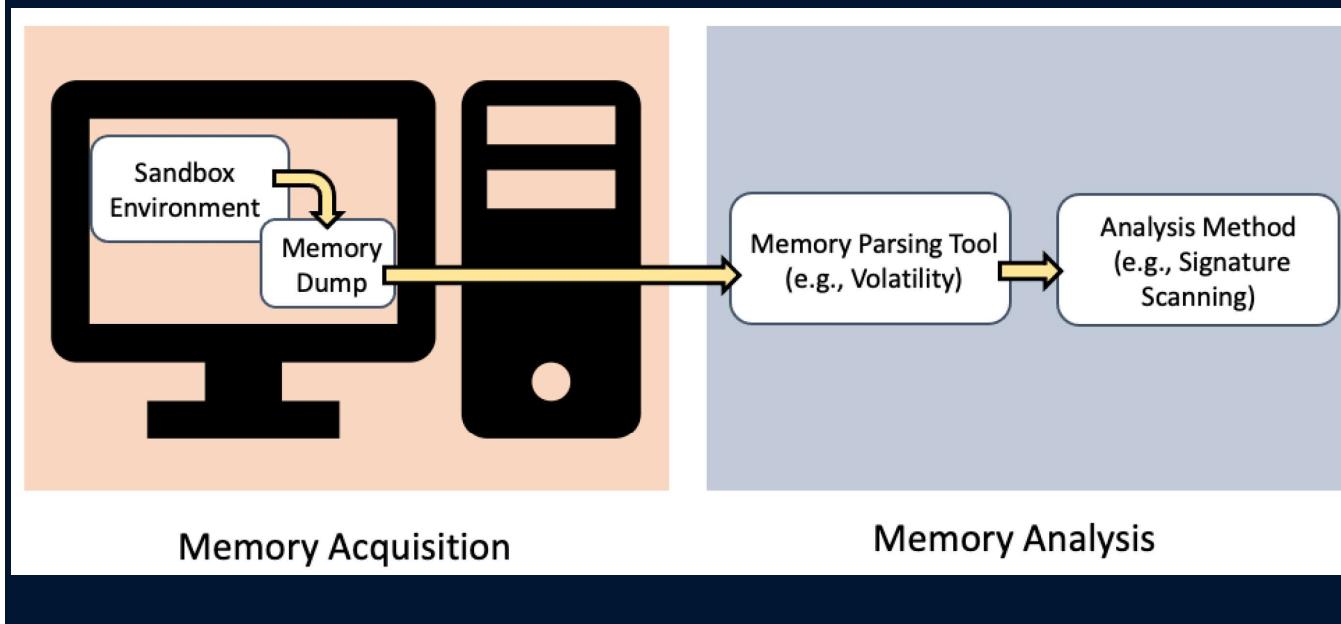
**Memory forensics**, also known as volatile memory analysis, is a specialized branch of **digital forensics** that focuses on the examination and analysis of the volatile memory (**RAM**) of a computer or digital device. Unlike traditional digital forensics, which involves analyzing data stored on non-volatile storage media like hard drives or solid-state drives, memory forensics deals with the live state of a system at a particular moment in time.

```
~/work/LZ77Huffman » vol -f Win8-d7fd4556.vmem prefetch
Volatility 3 Framework 2.0.1
Progress: 100.00          PDB scanning finished
ExecutableName  FileSize      PrefetchHash    LastExecution   ExecutionCounter
CONHOST.EXE      10648  0x3218e401  2022-07-18 12:22:04.000000  1
CONHOST.EXE      10648  0x3218e401  2022-07-18 12:22:04.000000  1
DLLHOST.EXE      18130  0x71214090  2022-07-18 12:22:14.000000  2
USERINIT.EXE     11664  0xf39ab672  2022-07-18 12:21:36.000000  1
SPPEXTCOMOBJ.EXE 17738  0xf8c1c601  2022-07-18 12:21:56.000000  1
NISSRV.EXE       30312  0x899f0efa  2022-07-18 12:21:33.000000  1
SEARCHINDEXER.EXE 100080  0x77d27bac  2022-07-18 12:21:35.000000  1
WMIPRVSE.EXE     20412  0x43972d0f  2022-07-18 12:21:48.000000  1
SEARCHFILTERHOST.EXE 15876  0xaa7a1fdd  2022-07-18 12:21:47.000000  1
SLUI.EXE         14426  0xa65918c4  2022-07-18 12:22:04.000000  1
EXPLORER.EXE     44598  0x7a3328da  2022-07-18 12:21:36.000000  1
```



## Datas that can be found in RAM

- Network connections
- File handles and open Files
- Open registry keys
- Running processes on the system
- Loaded modules
- Loaded device drivers
- Command history and console sessions
- Kernel data structures
- User and credential information
- Malware artifacts
- System configuration
- Process memory regions



# The Volatility Framework (NON-UI)

The preferred tool for conducting memory forensics is **Volatility**. **Volatility** is a leading open-source memory forensics framework.



```
BEATRIX volatility # python vol.py sockets -f /home/michael/stuxnet.vmem
Volatility Foundation Volatility Framework 2.3.1
```

Offset(V)	PID	Port	Proto	Protocol	Address	Create Time
0x81dc2008	680	500	17	UDP	0.0.0.0	2010-10-29 17:09:05 UTC+0000
0x82061c08	4	445	6	TCP	0.0.0.0	2010-10-29 17:08:53 UTC+0000
0x82294aa8	940	135	6	TCP	0.0.0.0	2010-10-29 17:08:55 UTC+0000
0x821a5008	188	1025	6	TCP	127.0.0.1	2010-10-29 17:09:09 UTC+0000
0x81cb3d70	1080	1141	17	UDP	0.0.0.0	2010-10-31 16:36:16 UTC+0000
0x81da4d18	680	0	255	Reserved	0.0.0.0	2010-10-29 17:09:05 UTC+0000
0x81fdbbe98	1032	123	17	UDP	127.0.0.1	2011-06-03 04:25:47 UTC+0000
0x81c79778	1080	1142	17	UDP	0.0.0.0	2010-10-31 16:36:16 UTC+0000
0x81c20898	1200	1900	17	UDP	127.0.0.1	2011-06-03 04:25:47 UTC+0000
0x82060008	680	4500	17	UDP	0.0.0.0	2010-10-29 17:09:05 UTC+0000
0x81cb9e98	1580	5152	6	TCP	127.0.0.1	2010-10-29 17:09:05 UTC+0000
0x81da54b0	4	445	17	UDP	0.0.0.0	2010-10-29 17:08:53 UTC+0000

# Install (Volatility 3)

\$ git clone <https://github.com/volatilityfoundation/volatility3.git>

```
(raviel㉿kali)-[~/Tool/Volatility/Vol3/volatility3]
$ python3 vol.py -h
Volatility 3 Framework 2.5.2
usage: volatility [-h] [-c CONFIG] [--parallelism [{processes,threads,off}]] [-e EXTEND] [-p PLUGIN_DIRS]
                  [-q] [-r RENDERER] [-f FILE] [-wRITE-CONFIG] [-SAVE-CONFIG SAVE_CONFIG] [--clear]
                  [--single-location SINGLE_LOCATION] [--stackers [STACKERS ...]] [-sINGLE-SWAP-LOC
                  plugin ...

An open-source memory forensics framework

options:
  -h, --help            Show this help message and exit, for specific plugin options use 'volatility
  -c CONFIG, --config CONFIG
                        Load the configuration from a json file
  --parallelism [{processes,threads,off}]
                        Enables parallelism (defaults to off if no argument given)
  -e EXTEND, --extend EXTEND
                        Extend the configuration with a new (or changed) setting
  -p PLUGIN_DIRS, --plugin-dirs PLUGIN_DIRS
                        Semi-colon separated list of paths to find plugins
  -s SYMBOL_DIRS, --symbol-dirs SYMBOL_DIRS
                        Semi-colon separated list of paths to find symbols
  -v, --verbosity       Increase output verbosity
  -l LOG, --log LOG     Log output to a file as well as the console
  -n OUTPUT_DTR, --output-dir OUTPUT_DTR
```

```
(raviel㉿kali)-[~/Desktop/dump/vol2.6]
$ wget https://github.com/volatilityfoundation/volatility/releases/download/2.6.1/volatility_2.6_lin64_standalone.zip
--2024-06-11 06:33:06--  https://github.com/volatilityfoundation/volatility/releases/download/2.6.1/volatility_2.6_lin64_standalone
.zip
Resolving github.com (github.com) ... 20.205.243.166
Connecting to github.com (github.com)|20.205.243.166|:443 ... connected.
HTTP request sent, awaiting response ... 302 Found
Location: https://objects.githubusercontent.com/github-production-release-asset-2e65be/19114225/3488f159-fa81-4ffa-bic8-502ac0f4cba
e?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Credential=releaseassetproduction%2F20240611%2Fus-east-1%2Fs3%2Faws4_request&X-Amz-Date=20
240611T103305Z&X-Amz-Expires=3006X-Amz-Signature=0db7f58889fa1421e39d8a489b09f4f48c11b72a5bbc0d149464607eaaf935e16X-Amz-SignedHeade
rs=host&actor_id=0&key_id=0&repo_id=19114225&response-content-disposition=attachment%3B%20filename%3Dvolatility_2.6_lin64_standalon
e.zip&response-content-type=application%2Foctet-stream [following]
--2024-06-11 06:33:07--  https://objects.githubusercontent.com/github-production-release-asset-2e65be/19114225/3488f159-fa81-4ffa-b
ic8-502ac0f4cbae?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Credential=releaseassetproduction%2F20240611%2Fus-east-1%2Fs3%2Faws4_reques
t&X-Amz-Date=20240611T103305Z&X-Amz-Expires=3006X-Amz-Signature=0db7f58889fa1421e39d8a489b09f4f48c11b72a5bbc0d149464607eaaf935e16X-
Amz-SignedHeaders=host&actor_id=0&key_id=0&repo_id=19114225&response-content-disposition=attachment%3B%20filename%3Dvolatility_2.6_
lin64_standalone.zip&response-content-type=application%2Foctet-stream
Resolving objects.githubusercontent.com (objects.githubusercontent.com) ... 185.199.110.133, 185.199.109.133, 185.199.111.133, ...
Connecting to objects.githubusercontent.com (objects.githubusercontent.com)|185.199.110.133|:443 ... connected.
HTTP request sent, awaiting response ... 200 OK
Length: 14737820 (14M) [application/octet-stream]
Saving to: 'volatility_2.6_lin64_standalone.zip'

volatility_2.6_lin64_standalone. 100%[=====] 14.05M 2.45MB/s in 5.7s

2024-06-11 06:33:13 (2.47 MB/s) - 'volatility_2.6_lin64_standalone.zip' saved [14737820/14737820]
```

# Install (Volatility 2)

\$ wget  
[https://github.com/volatilityfoundation/volatility/releases/download/2.6.1/volatility\\_2.6\\_lin64\\_standalone.zip](https://github.com/volatilityfoundation/volatility/releases/download/2.6.1/volatility_2.6_lin64_standalone.zip)



```
(raviel㉿kali)-[~/Desktop/dump/vol2.6]
$ unzip volatility_2.6_lin64_standalone.zip
Archive: volatility_2.6_lin64_standalone.zip
  creating: volatility_2.6_lin64_standalone/
    inflating: volatility_2.6_lin64_standalone/AUTHORS.txt
    inflating: volatility_2.6_lin64_standalone/CREDITS.txt
    inflating: volatility_2.6_lin64_standalone/LEGAL.txt
    inflating: volatility_2.6_lin64_standalone/LICENSE.txt
    inflating: volatility_2.6_lin64_standalone/README.txt
    inflating: volatility_2.6_lin64_standalone/volatility_2.6_lin64_standalone

(raviel㉿kali)-[~/Desktop/dump/vol2.6]
$ cd volatility_2.6_lin64_standalone

(raviel㉿kali)-[~/.../Trash/files/vol2.6/volatility_2.6_lin64_standalone]
$ chmod +x volatility_2.6_lin64_standalone

(raviel㉿kali)-[~/.../Trash/files/vol2.6/volatility_2.6_lin64_standalone]
$ mv volatility_2.6_lin64_standalone vol2.6

(raviel㉿kali)-[~/.../Trash/files/vol2.6/volatility_2.6_lin64_standalone]
$ ./vol2.6 -
Volatility Foundation Volatility Framework 2.6
Usage: Volatility - A memory forensics analysis platform.
```

## **IDENTIFY OS PROFILE**

### **Volatility 2**

```
vol.py -f "/path/to/file" imageinfo
```

```
vol.py -f "/path/to/file" kdbgscan
```

### **Volatility 3**

```
vol.py -f "/path/to/file" windows.info
```

## PROCESS INFORMATION

**PSLIST** (lists the current processes running in memory)

**Volatility 2**

```
vol.py -f "/path/to/file" --profile <profile> pslist  
vol.py -f "/path/to/file" --profile <profile> psscan  
vol.py -f "/path/to/file" --profile <profile> pstree  
vol.py -f "/path/to/file" --profile <profile> psxview
```

**Volatility 3**

```
vol.py -f "/path/to/file" windows.pslist  
vol.py -f "/path/to/file" windows.psscan  
vol.py -f "/path/to/file" windows.pstree
```

## PROCESS INFORMATION

### PROCDUMP

#### Volatility 2

```
vol.py -f "/path/to/file" --profile <profile> procdump  
-p <PID> --dump-dir="/path/to/dir"
```

#### Volatility 3

```
vol.py -f "/path/to/file" -o "/path/to/dir"  
windows.dumpfiles --pid <PID>
```

## PROCESS INFORMATION

### MEMDUMP

#### Volatility 2

```
vol.py -f "/path/to/file" --profile <profile> memdump  
-p <PID> --dump-dir="/path/to/dir"
```

#### Volatility 3

```
vol.py -f "/path/to/file" -o "/path/to/dir"  
windows.memmap --dump --pid <PID>
```

## PROCESS INFORMATION

### HANDLES

**Volatility 2**

```
vol.py -f "/path/to/file" --profile <profile> handles -p <PID>
```

**Volatility 3**

```
vol.py -f "/path/to/file" windowshandles --pid <PID>
```

## PROCESS INFORMATION

### DLLS

**Volatility 2**

```
vol.py -f "/path/to/file" --profile <profile> dlllist -p <PID>
```

**Volatility 3**

```
vol.py -f "/path/to/file" windows.dlllist --pid <PID>
```

## PROCESS INFORMATION

### CMDLINES

#### Volatility 2

```
vol.py -f "/path/to/file" --profile <profile> cmdline
```

```
vol.py -f "/path/to/file" --profile <profile> cmdscan
```

```
vol.py -f "/path/to/file" --profile <profile> consoles
```

#### Volatility 3

```
vol.py -f "/path/to/file" windows.cmdline
```

## NETWORK INFORMATION

### NETSCAN

#### Volatility 2

```
vol.py -f "/path/to/file" --profile <profile> netscan
```

```
vol.py -f "/path/to/file" --profile <profile> netstat
```

#### Volatility 3

```
vol.py -f "/path/to/file" windows.netscan
```

```
vol.py -f "/path/to/file" windows.netstat
```

# REGISTRY

## HIVELIST

### Volatility 2

```
vol.py -f "/path/to/file" --profile <profile> hivescan
```

```
vol.py -f "/path/to/file" --profile <profile> hivelist
```

### Volatility 3

```
vol.py -f "/path/to/file" windows.registry.hivescan
```

```
vol.py -f "/path/to/file" windows.registry.hivelist
```

# REGISTRY

## PRINTKEY

### Volatility 2

```
vol.py -f "/path/to/file" --profile <profile> printkey  
vol.py -f "/path/to/file" --profile <profile> printkey -K "Software\Microsoft\Windows\CurrentVersion"
```

### Volatility 3

```
vol.py -f "/path/to/file" windows.registry.printkey  
vol.py -f "/path/to/file" windows.registry.printkey --key "Software\Microsoft\Windows\CurrentVersion"
```

## REGISTRY

HIVEDUMP

Volatility 2

```
vol.py -f "/path/to/file" --profile hivedump -o  
<offset>
```

Volatility 3

```
vol.py -f "/path/to/file" windows.filescan
```

# REGISTRY

## HIVELIST

### Volatility 2

```
vol.py -f "/path/to/file" --profile <profile> hivescan
```

```
vol.py -f "/path/to/file" --profile <profile> hivelist
```

### Volatility 3

```
vol.py -f "/path/to/file" windows.registry.hivescan
```

```
vol.py -f "/path/to/file" windows.registry.hivelist
```

## FILES

FILESCAN

Volatility 2

vol.py -f "/path/to/file" --profile <profile> filescan

Volatility 3

vol.py -f "/path/to/file" windows.filescan

## FILES

### FILEDUMP

#### Volatility 2

```
vol.py -f "/path/to/file" --profile <profile> dumpfiles --dump-dir="/path/to/dir"  
vol.py -f "/path/to/file" --profile <profile> dumpfiles --dump-dir="/path/to/dir" -Q <offset>  
vol.py -f "/path/to/file" --profile <profile> dumpfiles --dump-dir="/path/to/dir" -p <PID>
```

#### Volatility 3

```
vol.py -f "/path/to/file" -o "/path/to/dir" windows.dumpfiles  
vol.py -f "/path/to/file" -o "/path/to/dir" windows.dumpfiles --virtaddr <offset>  
vol.py -f "/path/to/file" -o "/path/to/dir" windows.dumpfiles --physaddr <offset>
```

## MISCELLANEOUS

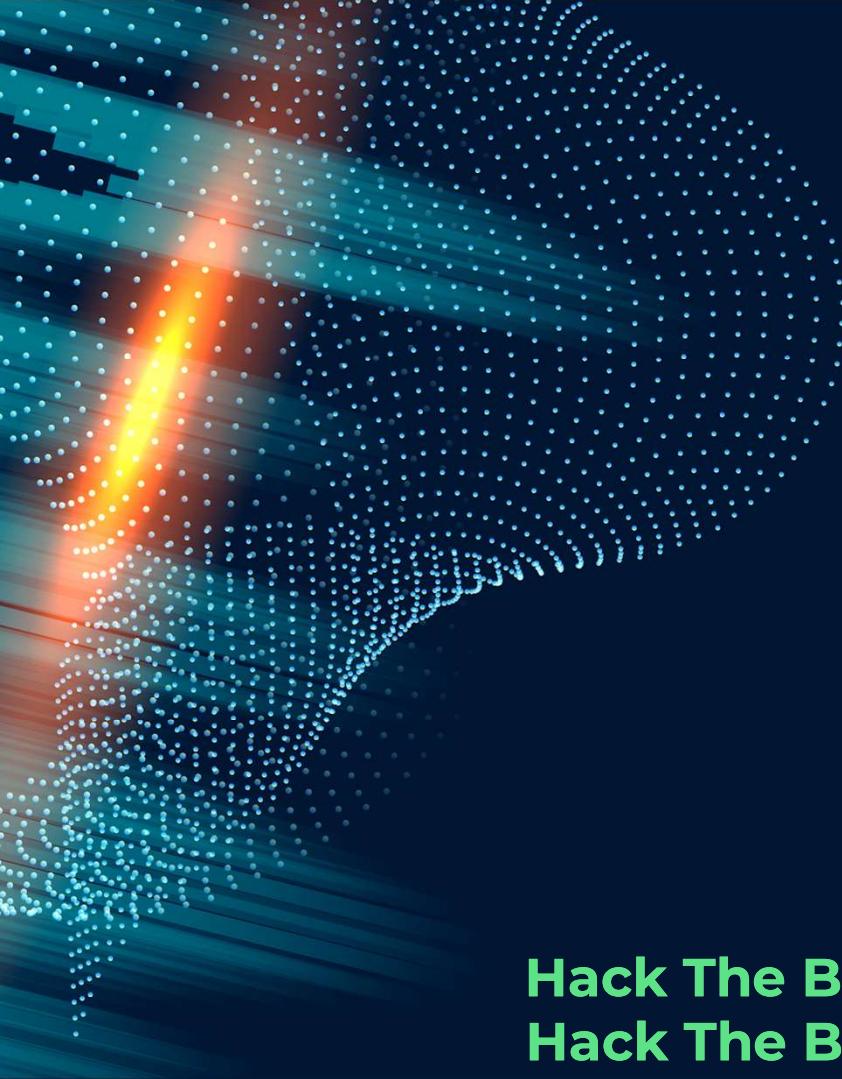
MALFIND

Volatility 2

```
vol.py -f "/path/to/file" --profile <profile> malfind
```

Volatility 3

```
vol.py -f "/path/to/file" windows.malfind
```



# THE END

**Contacts:**

Facebook:

<https://www.facebook.com/Kann.Raviel>

Discord:

raviyelna

**Reference:**

CTF101

Hack The Box Academy – Intro to Network traffic  
Hack The Box Academy – Intro to Digital forensic