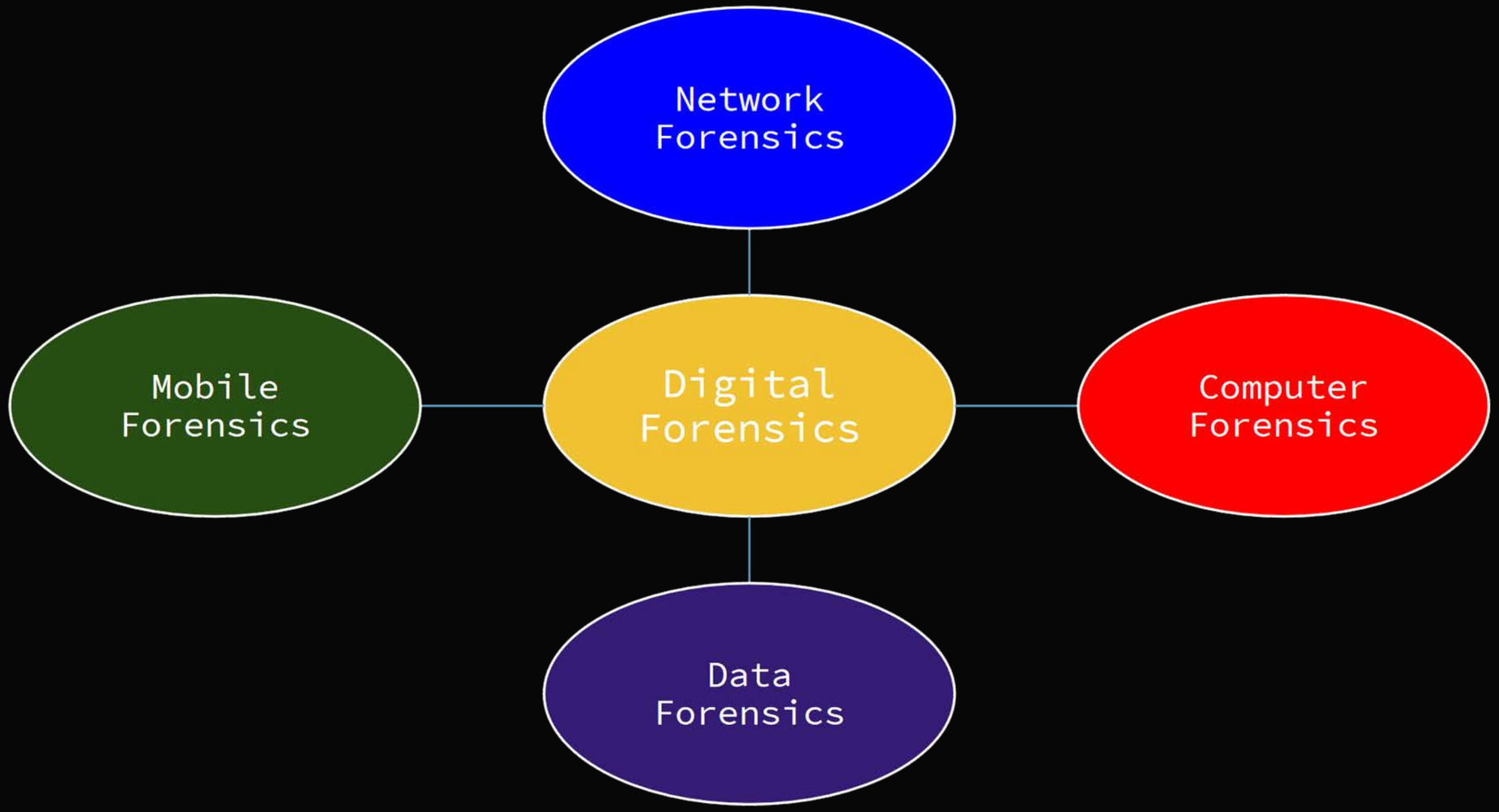
# EIT TRAINING

# TRAINING PLAN

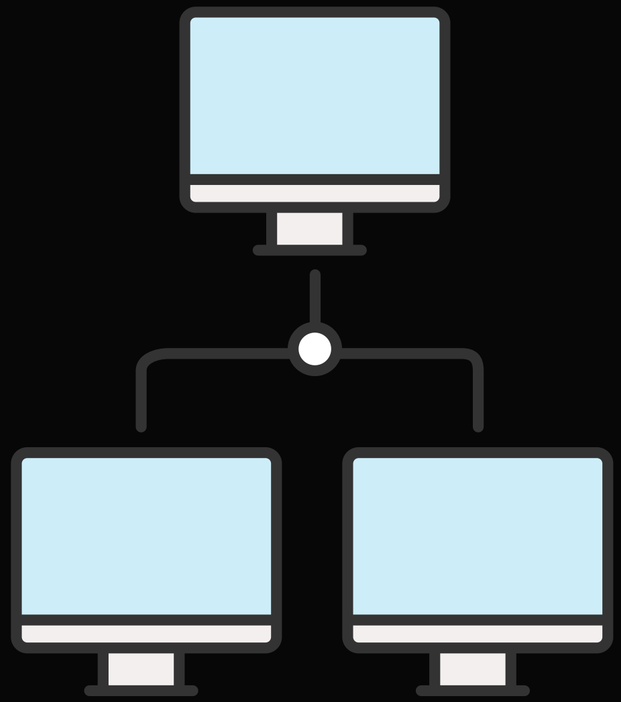
- INTRODUCTION TO LINUX
- **FORENSICS AND OSINT**
- CRYPTOGRAPHY
- WEB EXPLOITATION
- REVERSE ENGINEERING
- BINARY EXPLOITATION

# Branches of Digital Forensics

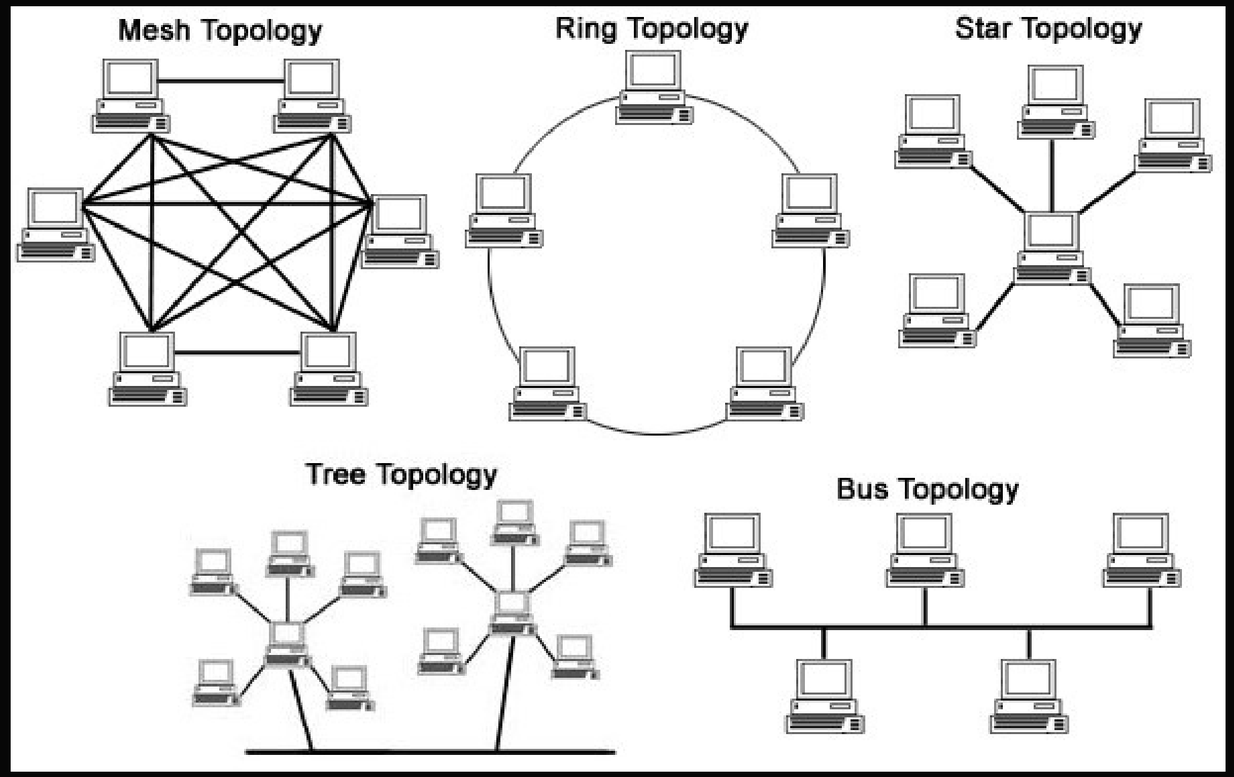


# Networking

Network: a collection of computers, servers, network devices, peripherals, or other devices connected to allow data (messages, files, resources) sharing.



# Network Topologies



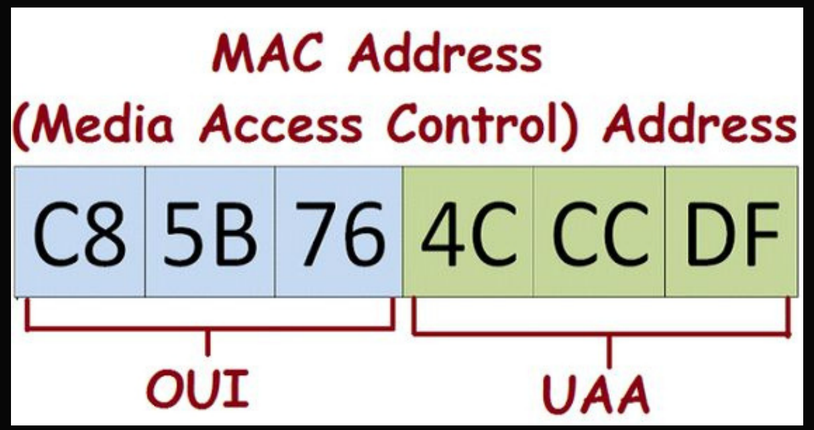

The term network topology describes the relationship of connected devices in terms of a geometric graph.

# MAC Address

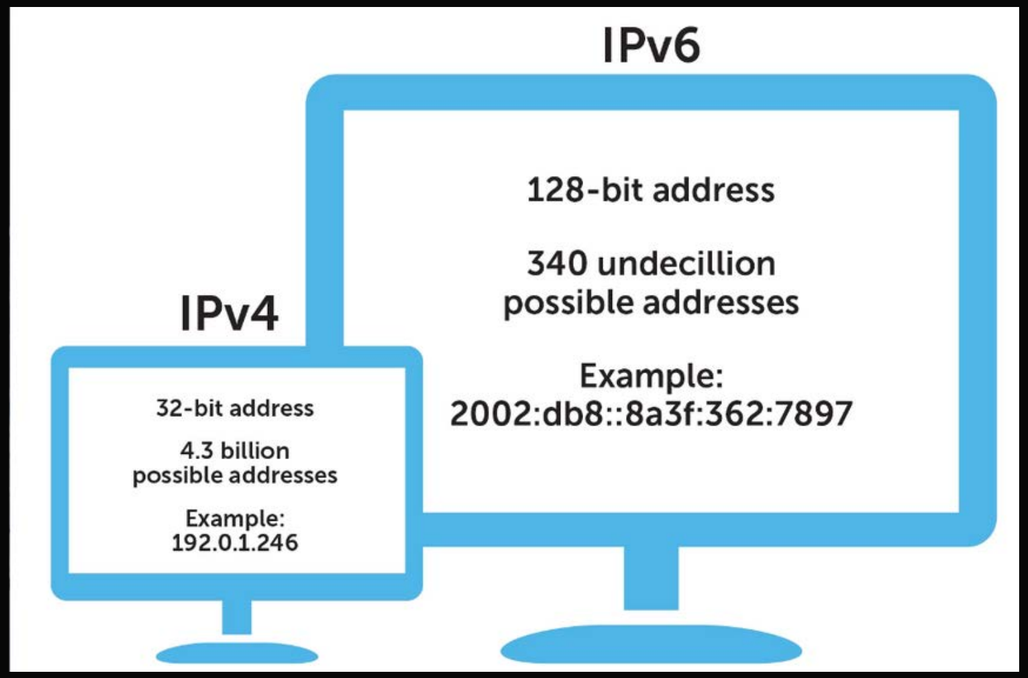
MAC Address is a unique ID assigned to network interface cards. It is also known as a physical address.

It identifies the hardware manufacturer and is used for network communication between devices in a network segment. It cannot be modified.

OUI: Organizationally Unique Identifier
UAA: Universally Administered Address



# IP Address




Another identifier of a device in a network is the IP address which ensures access to the Internet (IP protocol). It is editable, and you can configure its assignment either statically or dynamically.

There are 2 types:

- IPv4
- IPv6

# IPv4 Classes

Class A: 00000001 - 01111110 : 001-126.x.x.x : 255.255.255.0
Class B: 10000000 - 10111111 : 128-191.x.x.x : 255.255.0.0
Class C: 11000000 - 11011111 : 192-223.x.x.x : 255.255.255.0
Class D: 11100000 - 11101111 : 224-239.x.x.x -- multicast
Class E: 11110000 - 11111110 : 240-254.x.x.x -- research

## Special IP Addresses:

10.0.0.0 to 10.255.255.255
172.16.0.0 to 172.31.255.255
192.168.0.0 to 192.168.255.255
} Private IP Addresses

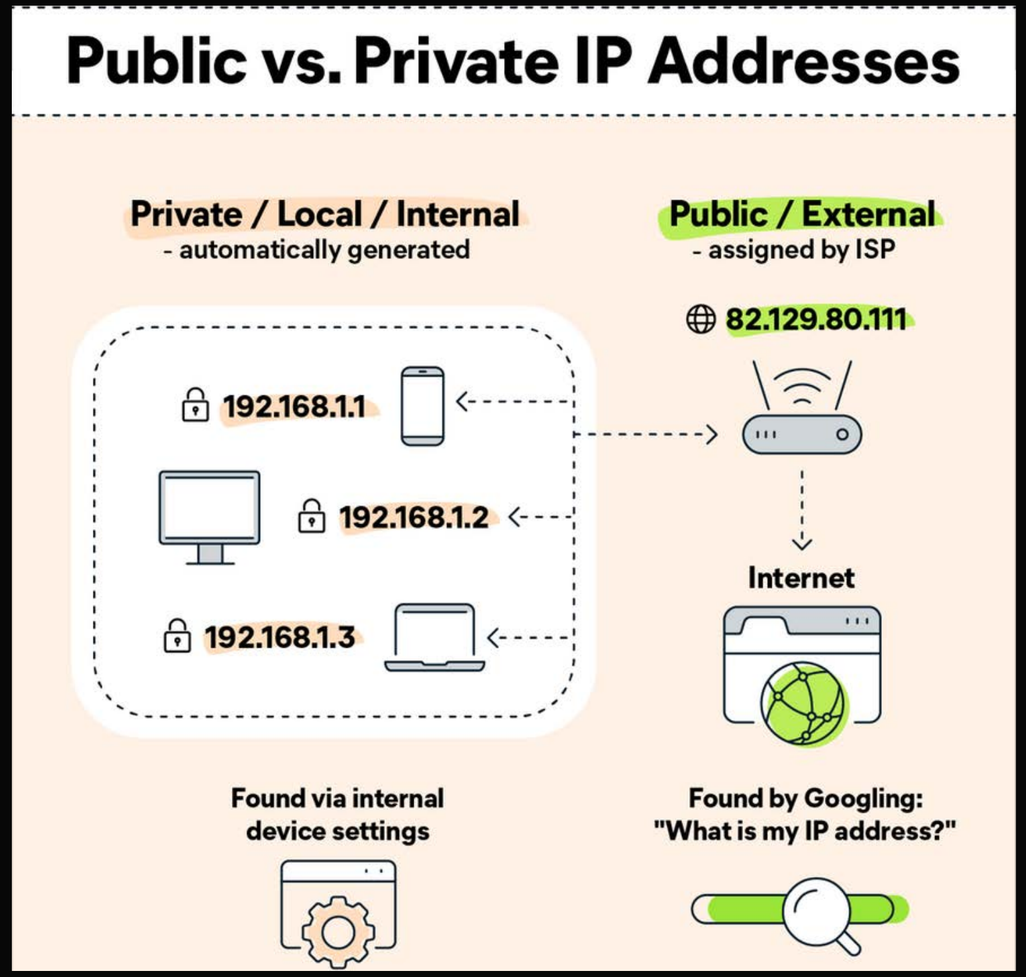
127.0.0.0 to 127.255.255.255 for communications inside the machine itself

# Public and Private IP Address

A public IP address is the IP address that can be accessed directly over the internet and is assigned to your network router by your internet service provider (ISP).

A private IP address is the address your network router assigns to your device. Each device within the same network is assigned a unique private IP address (in a company, house, ...).

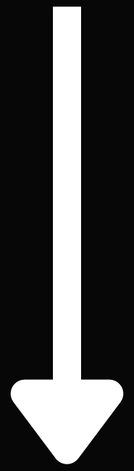
The process of converting a private IP address to a public one is done through NAT (Network Address Translation).



# IPv4

**IP Address:**

192.168.200.3/24



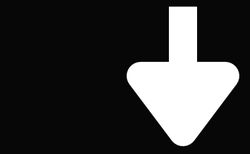
11000000.10101000.11001000.00000011

IPv4

**Net IP Address:**

192.168.1.3

& 255.255.255.0 (Netmask)



11000000.10101000.00000001.00000011

& 11111111.11111111.11111111.00000000

11000000.10101000.11001000.00000000

CIDR Notation: 192.168.1.0/24

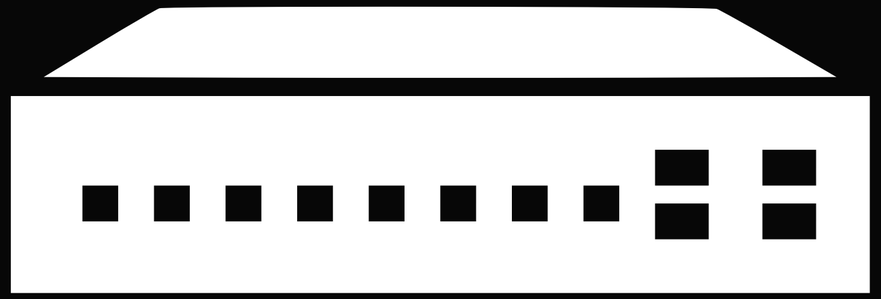
# TCP | UDP

TCP - Transmision Control Protocol
connection-oriented protocol
Uses: HTTP/HTTPS, FTP, SSH...

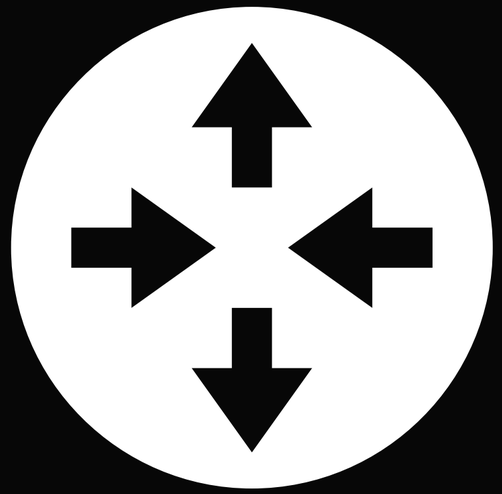
UDP - User Datagram Protocol
connectionless protocol
Uses: Streaming, VoIP...

# Switch | Router

A Switch is a device (without MAC or IP address) which eases communication between multiple computers.



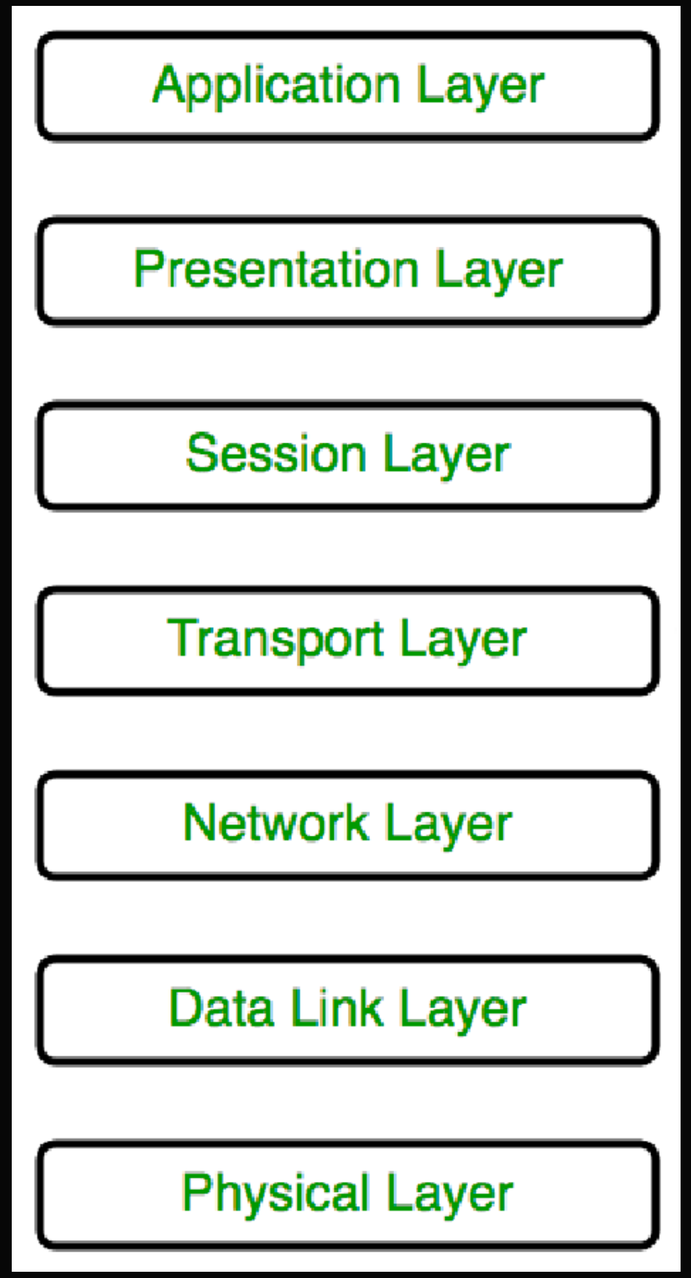
A Router is a device (with MAC and IP addresses) that connects local networks to each other. Ultimately, the internet is just another network.



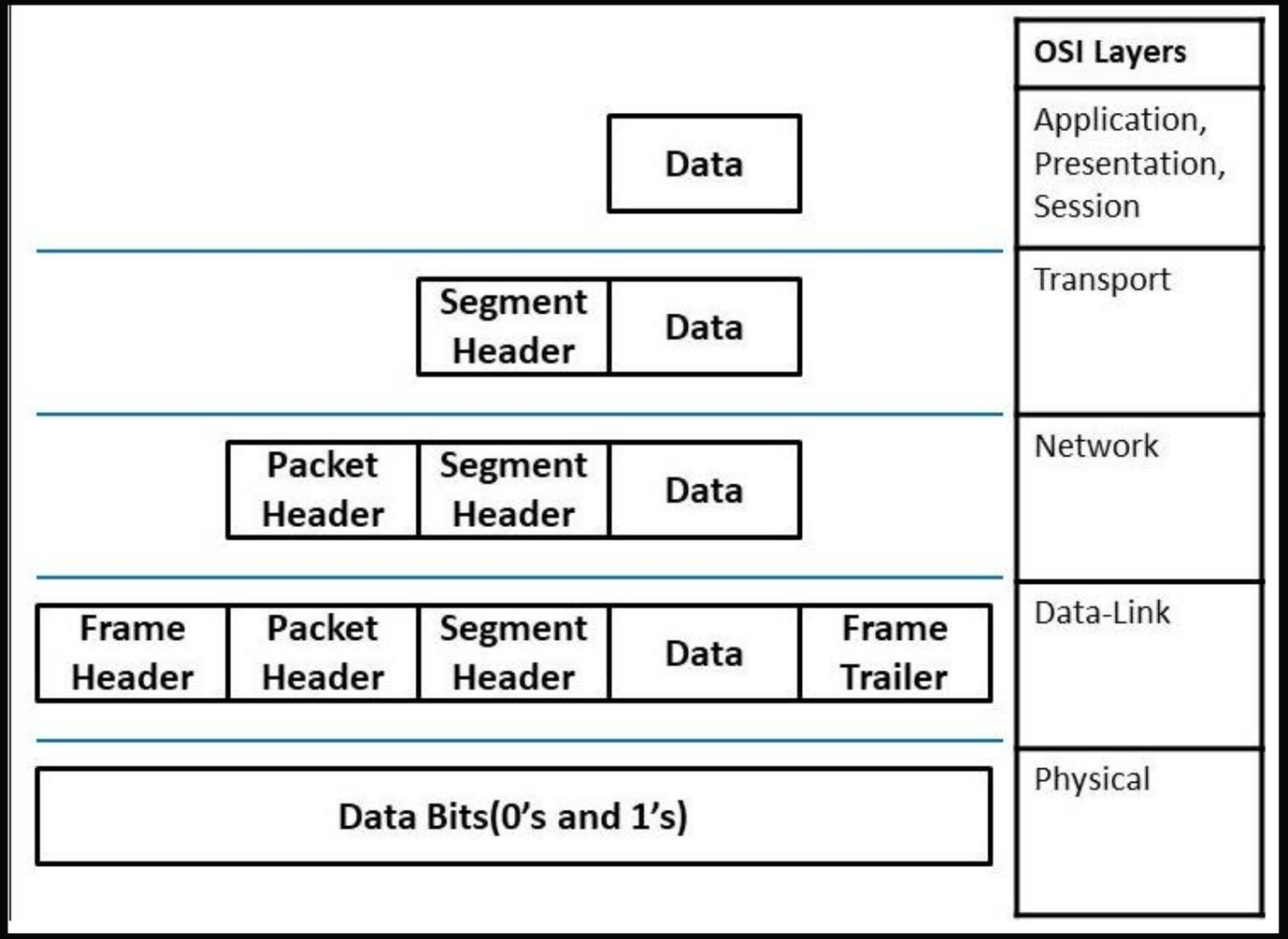
# OSI Model

In order to simplify networking, ISO presented the OSI model which abstracts the concept of communication and devices.

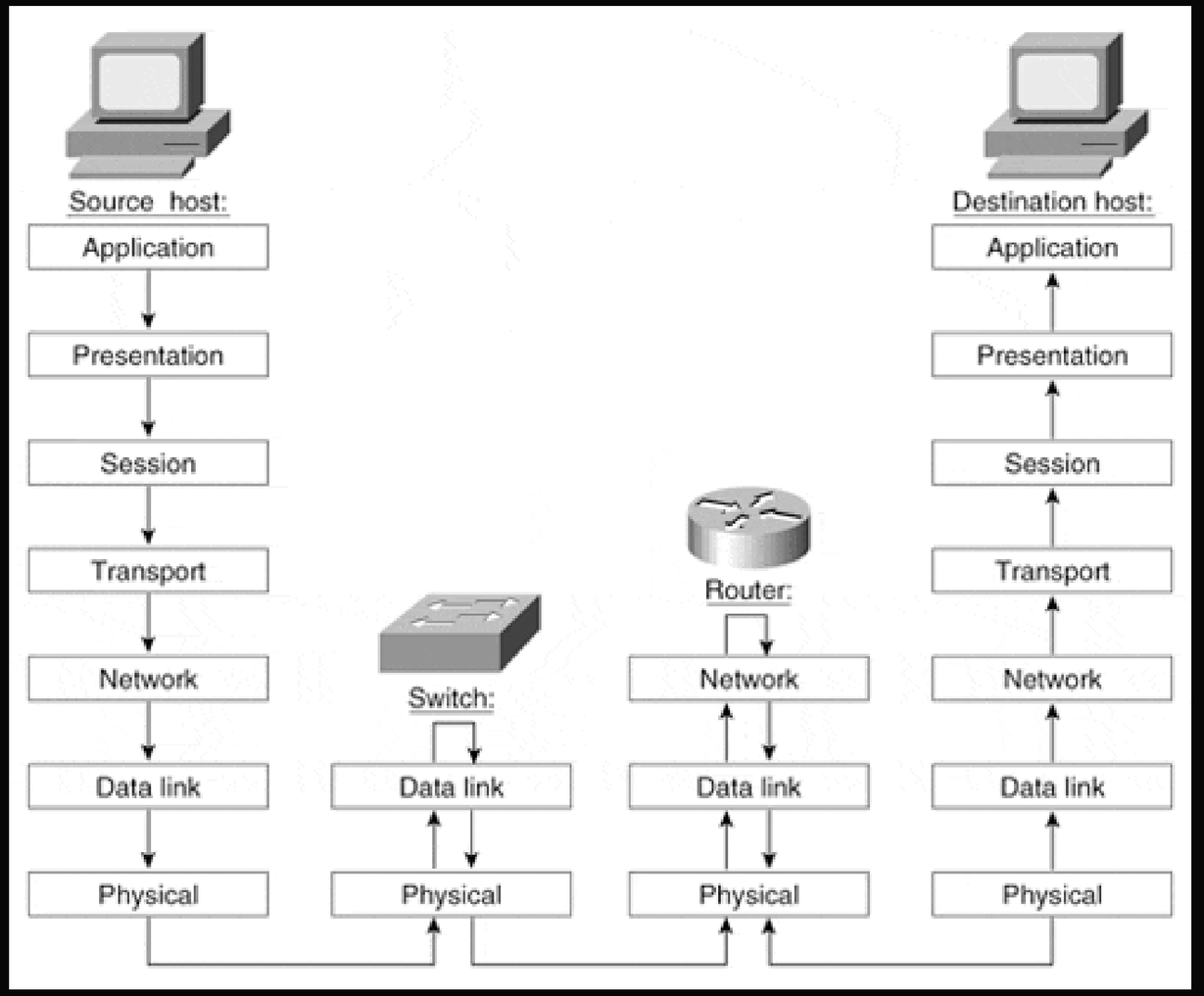
OSI model is a 7 layer model. It deconstructs each device to many levels.



# OSI Model: encapsulation



# OSI Model: inter-device comms



# TCP | UDP Header (Layer 4)

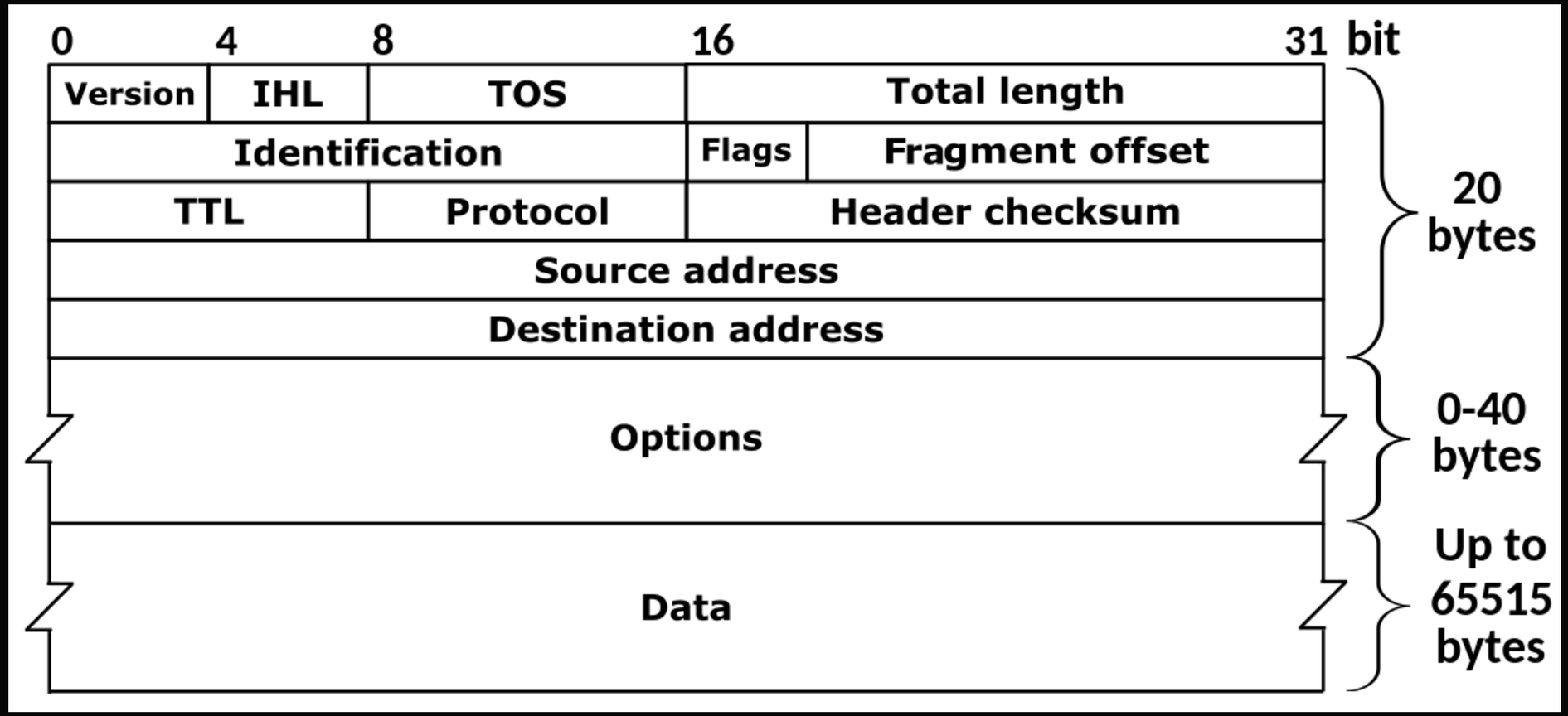
## TCP Segment Header Format

| Bit # | 0 – 7 | 8 – 15 | 16 – 23 | 24 – 31 |
|---|---|---|---|---|
| 0 | Source Port | | Destination Port | |
| 32 | Sequence Number | | | |
| 64 | Acknowledgment Number | | | |
| 96 | Data Offset | Res | Flags | Window Size |
| 128 | Header and Data Checksum | | Urgent Pointer | |
| 160... | Options | | | |

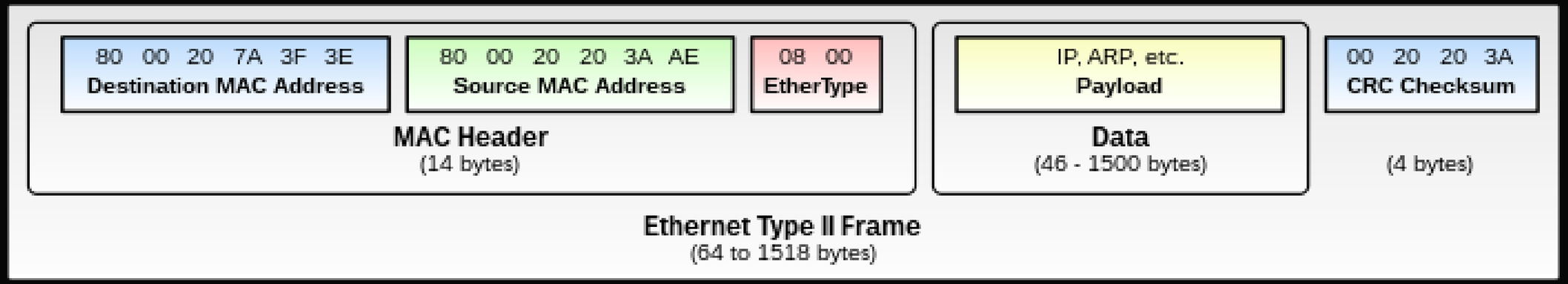
## UDP Datagram Header Format

| Bit # | 0 – 7 | 8 – 15 | 16 – 23 | 24 – 31 |
|---|---|---|---|---|
| 0 | Source Port | | Destination Port | |
| 32 | Length | | Header and Data Checksum | |

# IP Header (Layer 3)



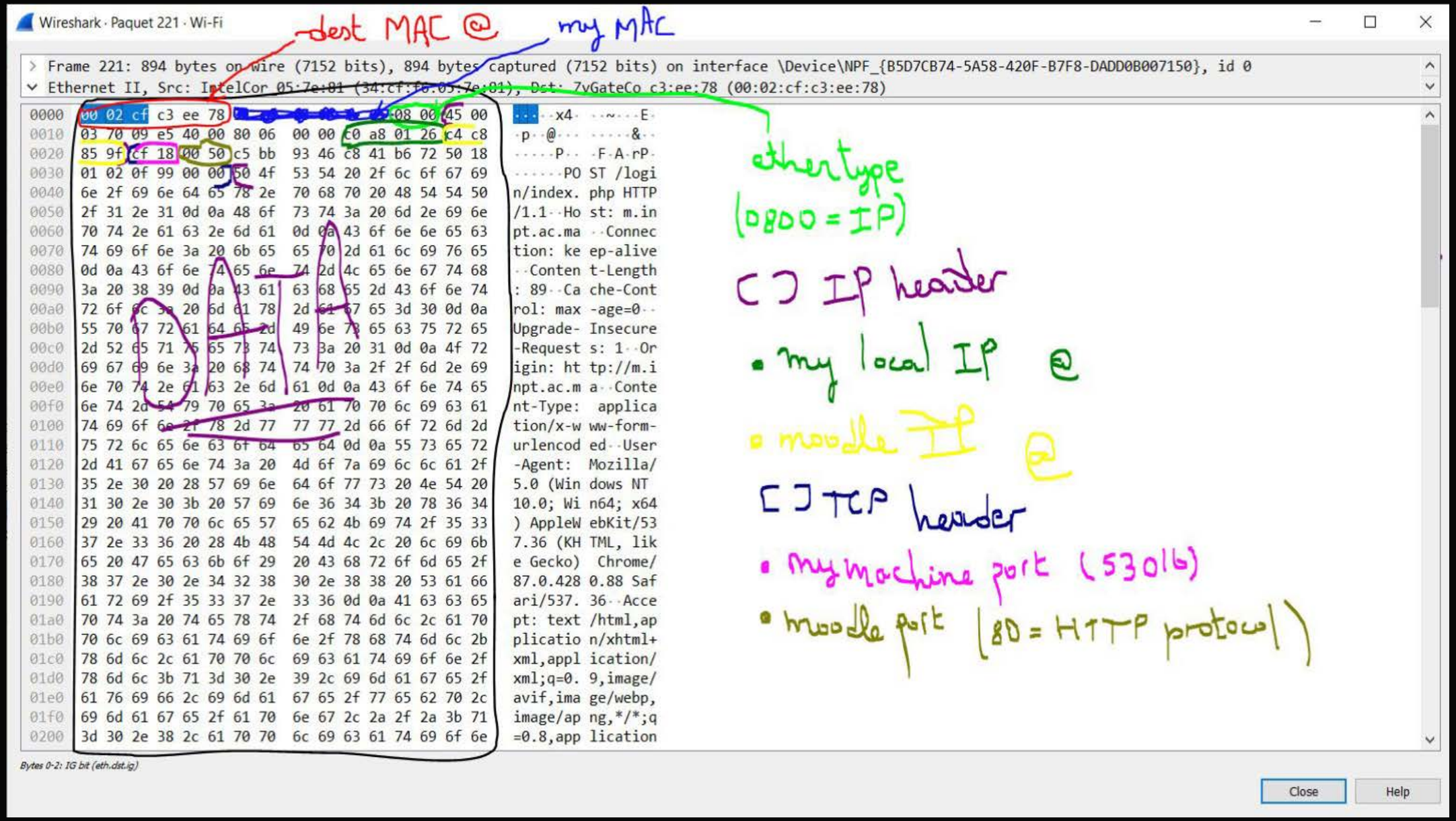
# Ethernet Header (Layer 2)



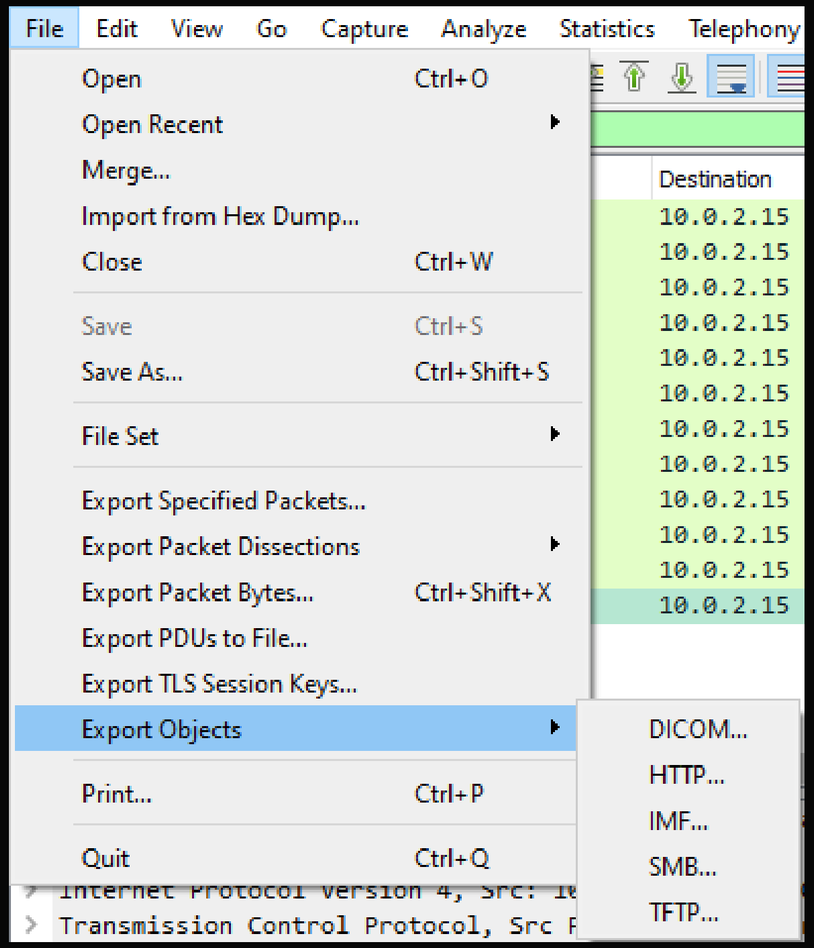
# Wireshark

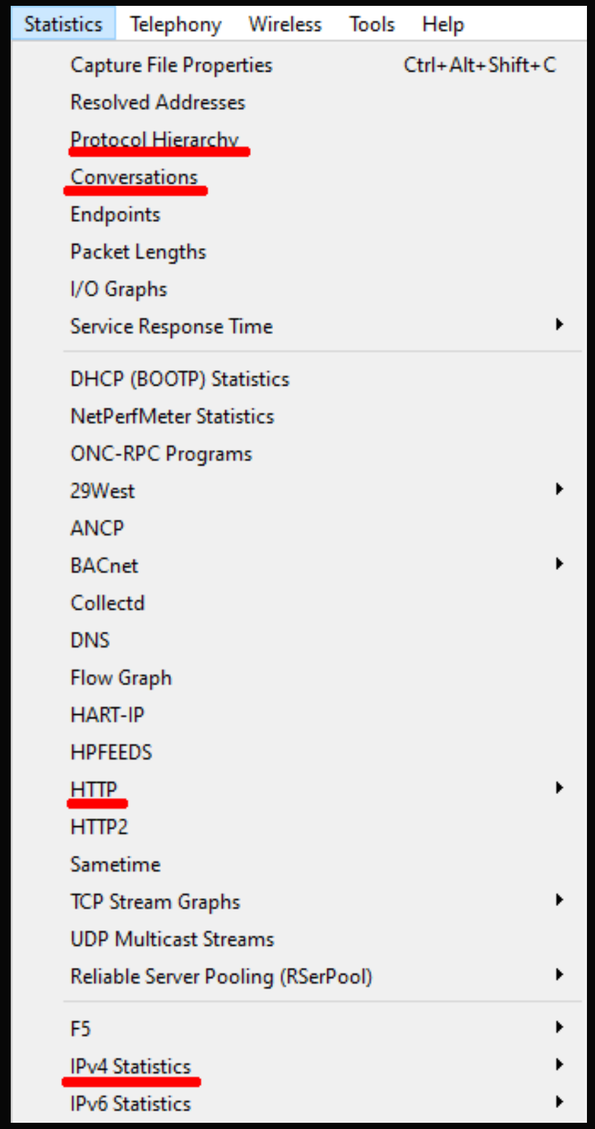
Network packet analyzer. Can be used to check all incoming and outgoing packets at the lowest layer of the OSI Model.

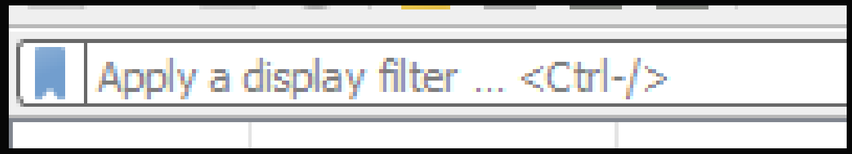
Let's use it to check what we send when attempting to login to moodle!


Wireshark · Paquet 221 · Wi-Fi
dest MAC @
my MAC
Frame 221: 894 bytes on wire (7152 bits), 894 bytes captured (7152 bits) on interface \Device\NPF_{B5D7CB74-5A58-420F-B7F8-DADD0B007150}, id 0
Ethernet II, Src: IntelCor 05:7e:81 (34:cf:f6:05:7e:81), Dst: 7vGateCo c3:ee:78 (00:02:cf:c3:ee:78)
0000 00 02 cf c3 ee 78 34 cf f6 05 7e 81 08 00 45 00
0010 03 70 09 e5 40 00 80 06 00 00 c0 a8 01 26 c4 c8
0020 85 9f cf 18 00 50 c5 bb 93 46 c8 41 b6 72 50 18
0030 01 02 0f 99 00 00 50 4f 53 54 20 2f 6c 6f 67 69
0040 6e 2f 69 6e 64 65 78 2e 70 68 70 20 48 54 54 50
0050 2f 31 2e 31 0d 0a 48 6f 73 74 3a 20 6d 2e 69 6e
0060 70 74 2e 61 63 2e 6d 61 0d 0a 43 6f 6e 6e 65 63
0070 74 69 6f 6e 3a 20 6b 65 65 70 2d 61 6c 69 76 65
0080 0d 0a 43 6f 6e 74 65 6e 74 2d 4c 65 6e 67 74 68
0090 3a 20 38 39 0d 0a 43 61 63 68 65 2d 43 6f 6e 74
00a0 72 6f 6c 3a 20 6d 61 78 2d 61 67 65 3d 30 0d 0a
00b0 55 70 67 72 61 64 65 2d 49 6e 73 65 63 75 72 65
00c0 2d 52 65 71 75 65 73 74 73 3a 20 31 0d 0a 4f 72
00d0 69 67 69 6e 3a 20 68 74 74 70 3a 2f 2f 6d 2e 69
00e0 6e 70 74 2e 61 63 2e 6d 61 0d 0a 43 6f 6e 74 65
00f0 6e 74 2d 54 79 70 65 3a 20 61 70 70 6c 69 63 61
0100 74 69 6f 6e 2f 78 2d 77 77 77 2d 66 6f 72 6d 2d
0110 75 72 6c 65 6e 63 6f 64 65 64 0d 0a 55 73 65 72
0120 2d 41 67 65 6e 74 3a 20 4d 6f 7a 69 6c 6c 61 2f
0130 35 2e 30 20 28 57 69 6e 64 6f 77 73 20 4e 54 20
0140 31 30 2e 30 3b 20 57 69 6e 36 34 3b 20 78 36 34
0150 29 20 41 70 70 6c 65 57 65 62 4b 69 74 2f 35 33
0160 37 2e 33 36 20 28 4b 48 54 4d 4c 2c 20 6c 69 6b
0170 65 20 47 65 63 6b 6f 29 20 43 68 72 6f 6d 65 2f
0180 38 37 2e 30 2e 34 32 38 30 2e 38 38 20 53 61 66
0190 61 72 69 2f 35 33 37 2e 33 36 0d 0a 41 63 63 65
01a0 70 74 3a 20 74 65 78 74 2f 68 74 6d 6c 2c 61 70
01b0 70 6c 69 63 61 74 69 6f 6e 2f 78 68 74 6d 6c 2b
01c0 78 6d 6c 2c 61 70 70 6c 69 63 61 74 69 6f 6e 2f
01d0 78 6d 6c 3b 71 3d 30 2e 39 2c 69 6d 61 67 65 2f
01e0 61 76 69 66 2c 69 6d 61 67 65 2f 77 65 62 70 2c
01f0 69 6d 61 67 65 2f 61 70 6e 67 2c 2a 2f 2a 3b 71
0200 3d 30 2e 38 2c 61 70 70 6c 69 63 61 74 69 6f 6e
ethertype
(0800 = IP)
IP header
• my local IP @
• moodle IP @
TCP header
• my machine port (53016)
• moodle port (80 = HTTP protocol)
Bytes 0-2: IG bit (eth.dst.ig)
Close
Help

# Wireshark




## List of filters:

# Common Ports and Protocols

| Port # | Application Layer Protocol | Type | Description |
|---|---|---|---|
| 20 | FTP | TCP | File Transfer Protocol - data |
| 21 | FTP | TCP | File Transfer Protocol - control |
| 22 | SSH | TCP/UDP | Secure Shell for secure login |
| 23 | Telnet | TCP | Unencrypted login |
| 25 | SMTP | TCP | Simple Mail Transfer Protocol |
| 53 | DNS | TCP/UDP | Domain Name Server |
| 67/68 | DHCP | UDP | Dynamic Host |
| 80 | HTTP | TCP | HyperText Transfer Protocol |
| 123 | NTP | UDP | Network Time Protocol |
| 161,162 | SNMP | TCP/UDP | Simple Network Management Protocol |
| 389 | LDAP | TCP/UDP | Lightweight Directory Authentication Protocol |
| 443 | HTTPS | TCP/UDP | HTTP with Secure Socket Layer |

# Challenges!

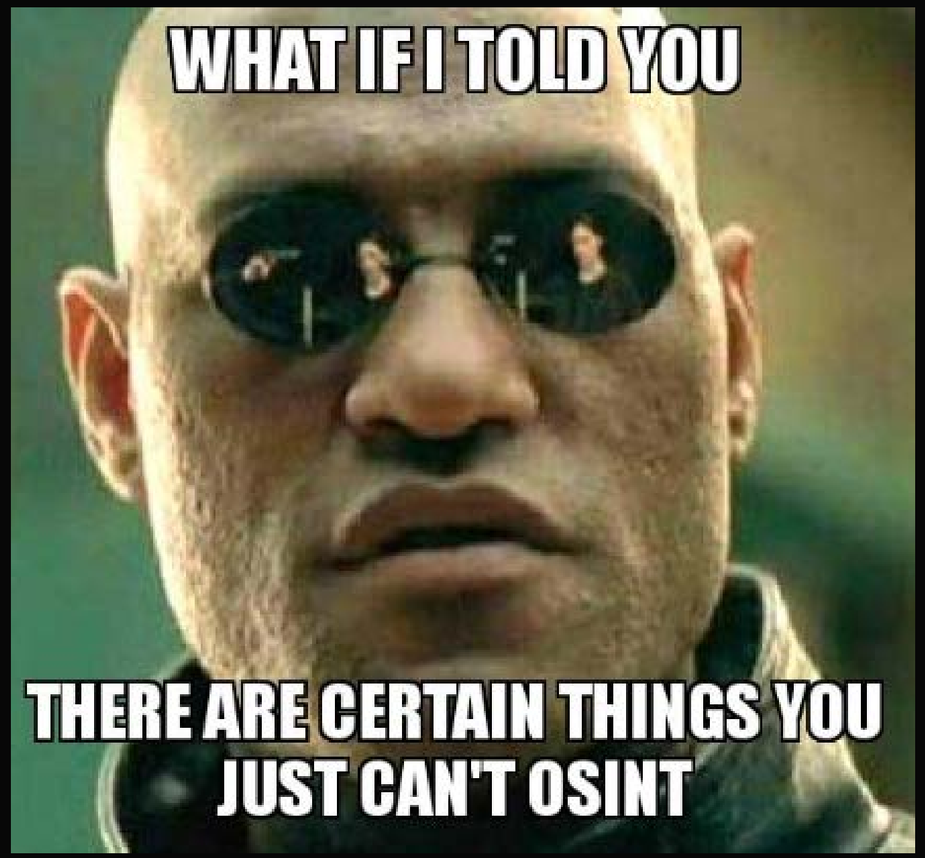
Extract the file.

Find the flag!

# OSINT

Open Source INTelligence (a.k.a OSINT), is the art of collecting information from publicly available sources.
OSINT operations, whether practiced by IT security pros or malicious hackers, use many techniques to search through a large amount of public data to find the needles/clues they're looking for to achieve their goals (important phone number, coordinates, real name of a hacker, etc.)

# OSINT




The art of OSINT resides in the fact that sometimes you can start from a small piece of data to access some very personal info about someone (an unethical hacker if you're an IT security professional, employees of a company if you're a pentester).
Sometimes, you can have as a start an image of a house, by doing OSINT you can even know the name of the dog of a neighbor's uncle, although there's always a limit to what you can reach using OSINT.

# OSINT

First, we should know that there aren’t some specific tools to do OSINT for all possible scenarios. It always depends on the context of the situation and what questions do you wanna answer. But the most important thing here is research, research and research (search engines are always helpful in this context).

# OSINT Tools

- Search using Google Dorks (search filters cheatsheet)
- HavelbeenPwned
- theHarvester, recon-ng
- Maltego
- WayBack Machine
- Page Source Code
- Reverse Image Search (Yandex, Google Lens, Tineye, etc.)
- Exiftool

Other resources