CCSC
BOOTCAMP TRAINING

Day 4 : Forensics/Osint

~ [CCSC] CIT Cyber Security Cell ~
OUSSAMA RAHALI
OMAR AOUAJ

CLUB INFORMATIQUE & TÉLÉCOM

cat README.md

1. Digital Forensics :
   1.1o Networking Forensics
2. OSINT

Warning !

As we head through this meeting, we're gonna have some challenges for you to answer.. If you were able to solve one, please write DONE in the chat without writing the solution.

Don't spoil solutions on your friends :) !

1. Digital forensics

1.10- Networking

`what is that`

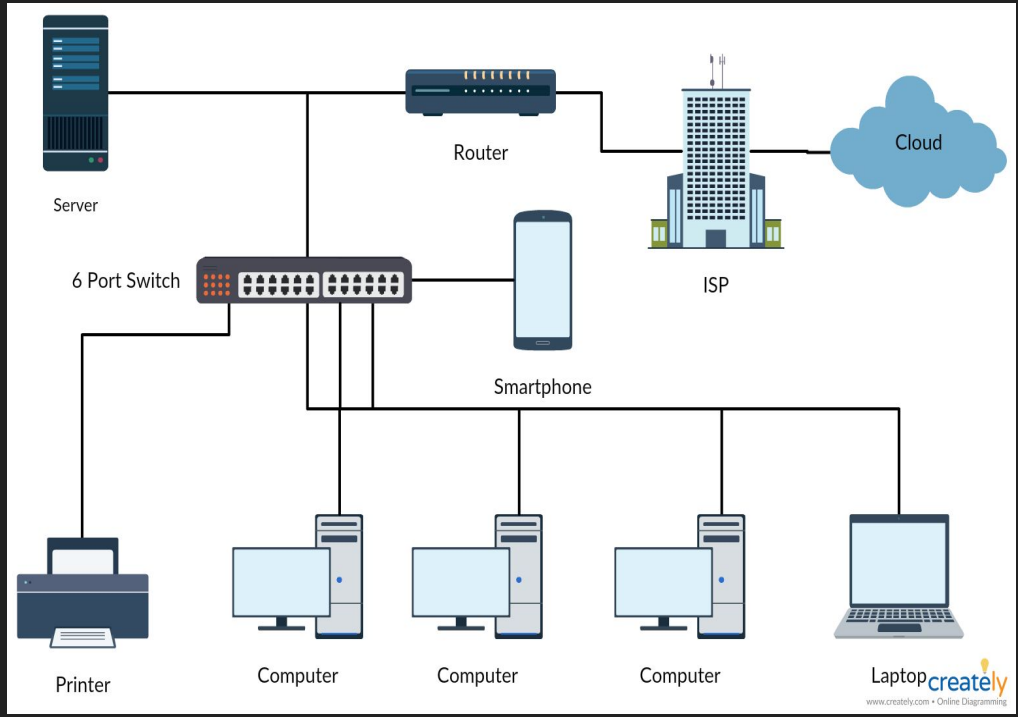
ideas

Familiarity with networking (1-10) ?

`Whatis Network`

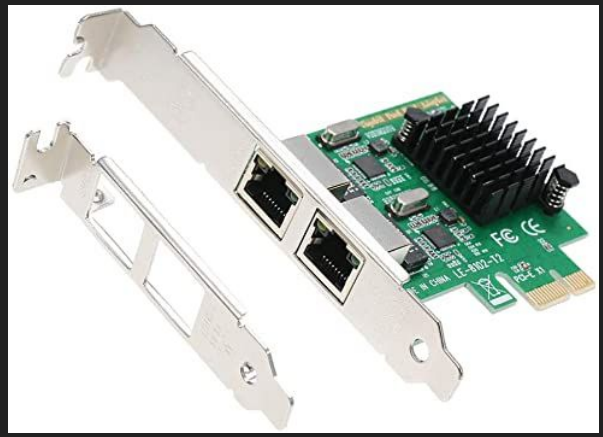
Network: nothing appropriate.

It’s a collection of devices (computers, phones, routers, switches, …) that are linked in order to exchange data (messages, files), or ressources like printers and so on.



MAC & IP

Each device within the network contains network cards (mostly just one).
This card is one responsible for sending data and it’s identified by a physical address called MAC.
MAC is physical so it cannot be modified.



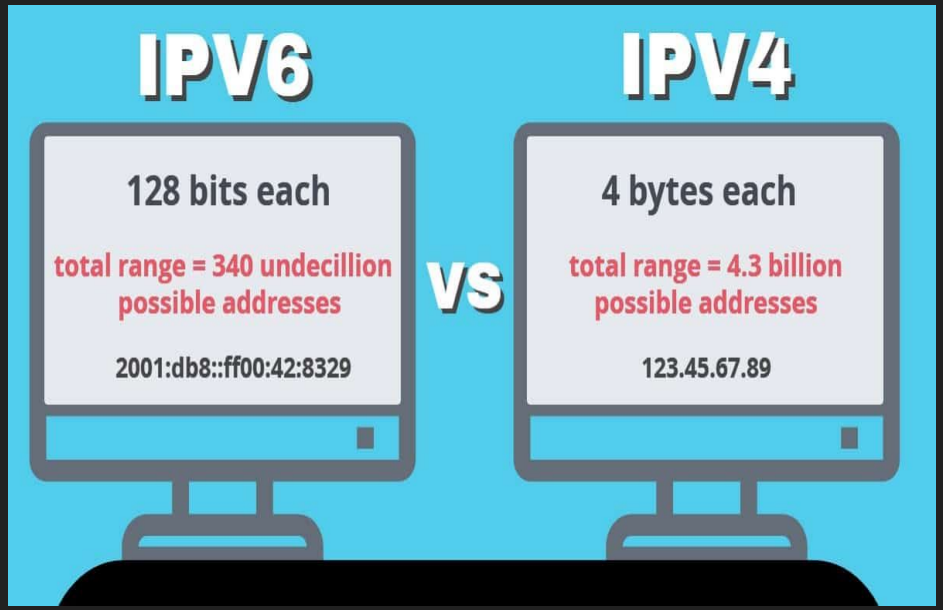
`00:1C:A2:01:A3:45`

It’s encoded on 48 bits.

MAC & IP

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

Given the syntax:

a.b.c.d 0<=(a,b,c,d)<=255

We have 5 classes depending on “a” value:

1<=a<=126: Class A (syntax of a network **a.0.0.0/8**)

128<=a<=191: Class B (syntax of a network **a.b.0.0/16**)

192<=a<=223: Class C (syntax of a network **a.b.c.0/24**)

224<=a<=239: Class D (multicast or groups in a network)

240<=a<=254: Class E (reserved for research and development)

IP types

Public IPs: Used for the global communication, and it’s unique.

All the ranges we’ve seen are public excluding **10.0.0.0/8**, **172.16.0.0--->172.31.255.255 and 192.168.0.0--->192.168.255.255**.

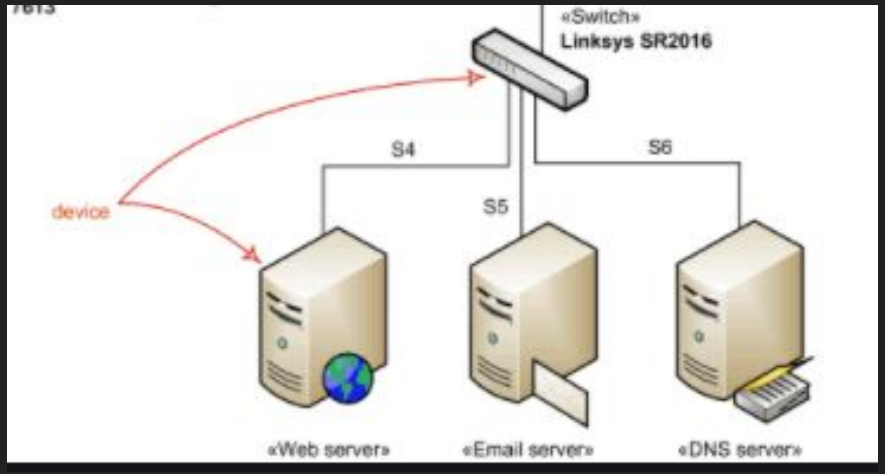
Private IPs: Used for the local communication (inside a company, inside a house,...), 2 different devices in 2 different local networks can have the same local address.

Now, you must know what are private IPs exactly :D

Ah yes, we didn’t talk about **127.0.0.0/8**, it’s used for localhost or for communications inside the machine itself.

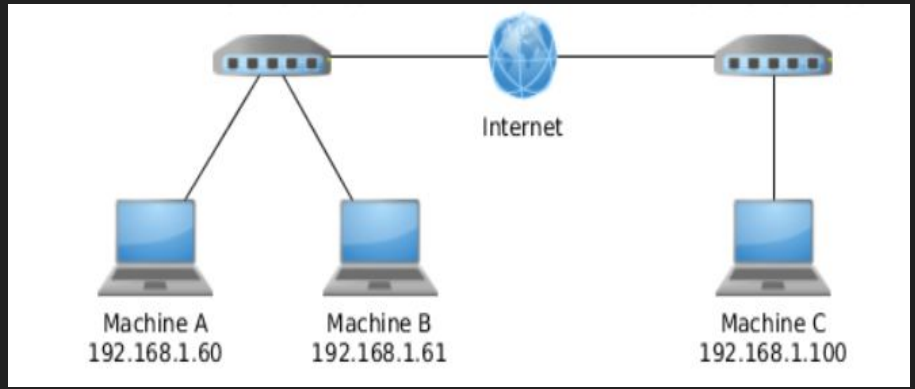
`whatis Switch`

Switch: It’s just a device (without MAC or IP addresses) which ease communication between multiple computers for instance. If we have n>2 computers, we can’t connect each one to all the others directly, so we use switches for this purpose.



`whatis Router`

Router: It’s a device (with MAC and IP addresses) which is the elementary composant of that cloud which we call the INTERNET. It also links local networks to that INTERNET.



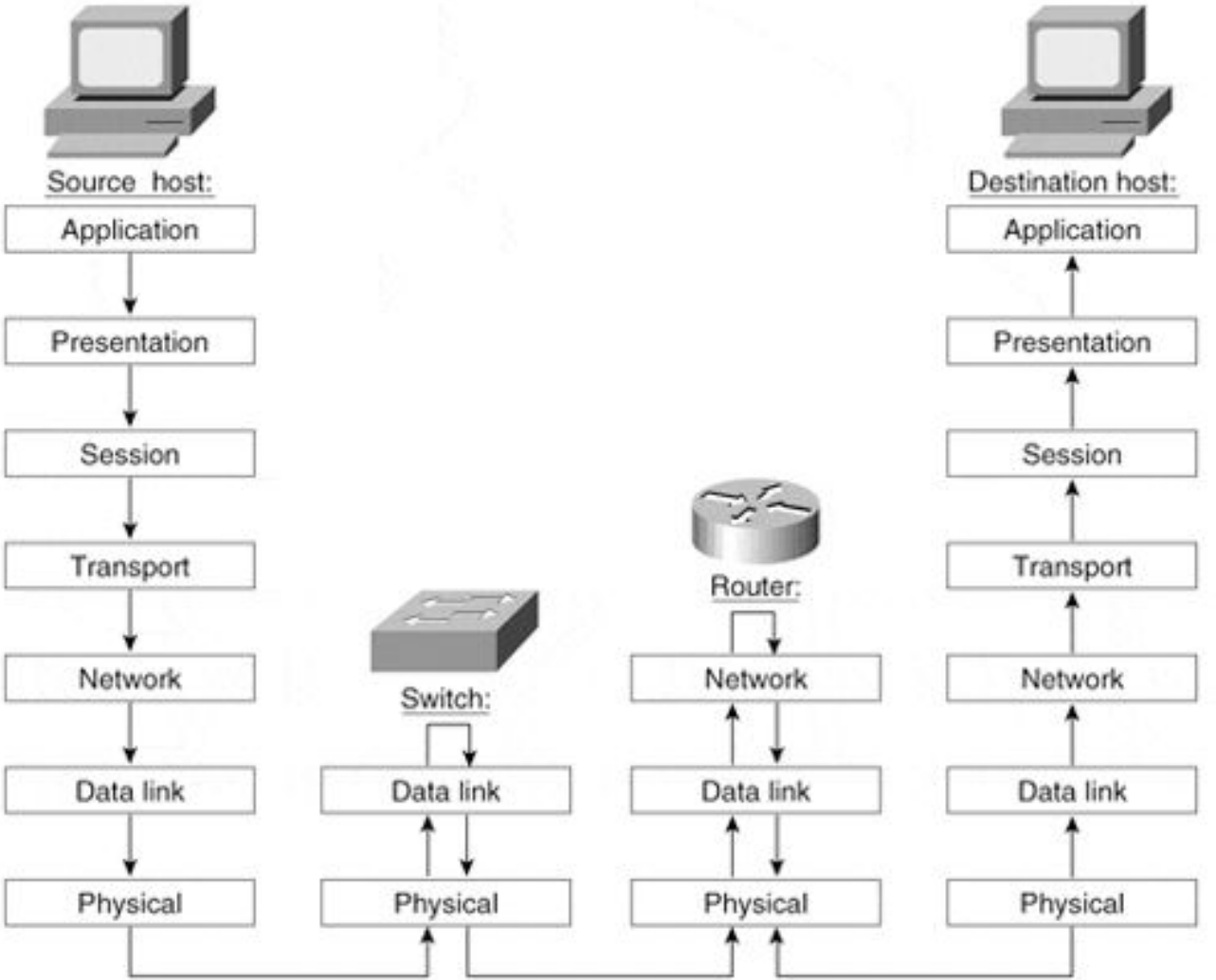
OSI model

In order to simplify networking (maybe it complicated it idk), ISO, not us, presented the OSI model which abstracts the concept of communication and devices.

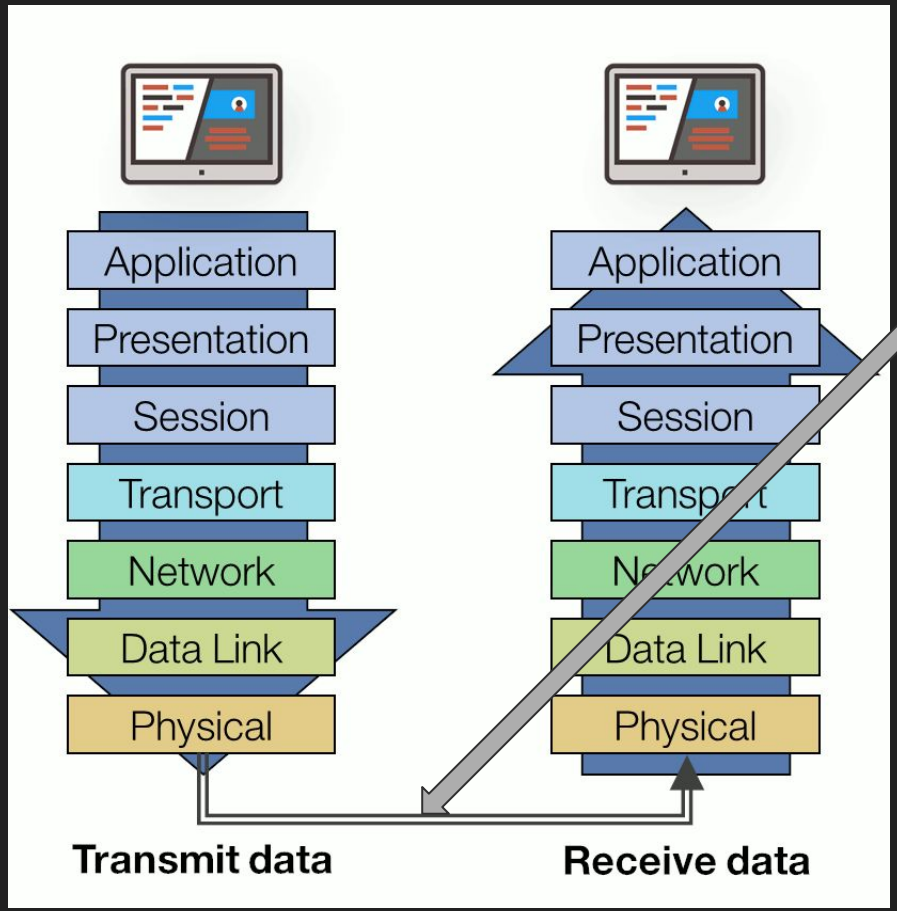
OSI model is a layer model (like that delicious burrito). It decorticates each device to many levels.

7 Layers of the OSI Model

Application	• End User layer • HTTP, FTP, IRC, SSH, DNS
Presentation	• Syntax layer • SSL, SSH, IMAP, FTP, MPEG, JPEG
Session	• Synch & send to port • API's, Sockets, WinSock
Transport	• End-to-end connections • TCP, UDP
Network	• Packets • IP, ICMP, IPSec, IGMP
Data Link	• Frames • Ethernet, PPP, Switch, Bridge
Physical	• Physical structure • Coax, Fiber, Wireless, Hubs, Repeaters


Source host:
Application
Presentation
Session
Transport
Network
Data link
Physical
Switch:
Data link
Physical
Router:
Network
Data link
Physical
Destination host:
Application
Presentation
Session
Transport
Network
Data link
Physical

Where all the magic happens



The OSI model is an abstraction, so we can't practically see the packet while it's travelling inside the device, yet, with a suitable software (like Wireshark or Ettercap), we can identify each packet sent in the network.

Let’s capture the packets together !

demo wireshark

Just before we begin

When the packet arrives to the physical layer of the sender machine, it has many encapsulations (headers and suffixes) which helps all the network devices in knowing who are the sender and the receiver, what are the protocols used by this packet (TCP or UDP in the transport layer, HTTP or HTTPS or FTP or SSH or … in the application layer).

Since we are listening to the network communication from the physical side, we must know that the packet we see are encapsulated by many headers representing the layers that the packet came across.

Just before we begin

Another thing is that after an attack or a security incident in a company via the company's network itself, it's always useful to analyze the traffic when it was under attack.

The purpose of this analysis is to answer many questions:

Who did the attack? (identify MAC, IP of the attacker)

When did the attack happen?

Who were the victims of the attack?

Which vulnerability did the attacker exploit?

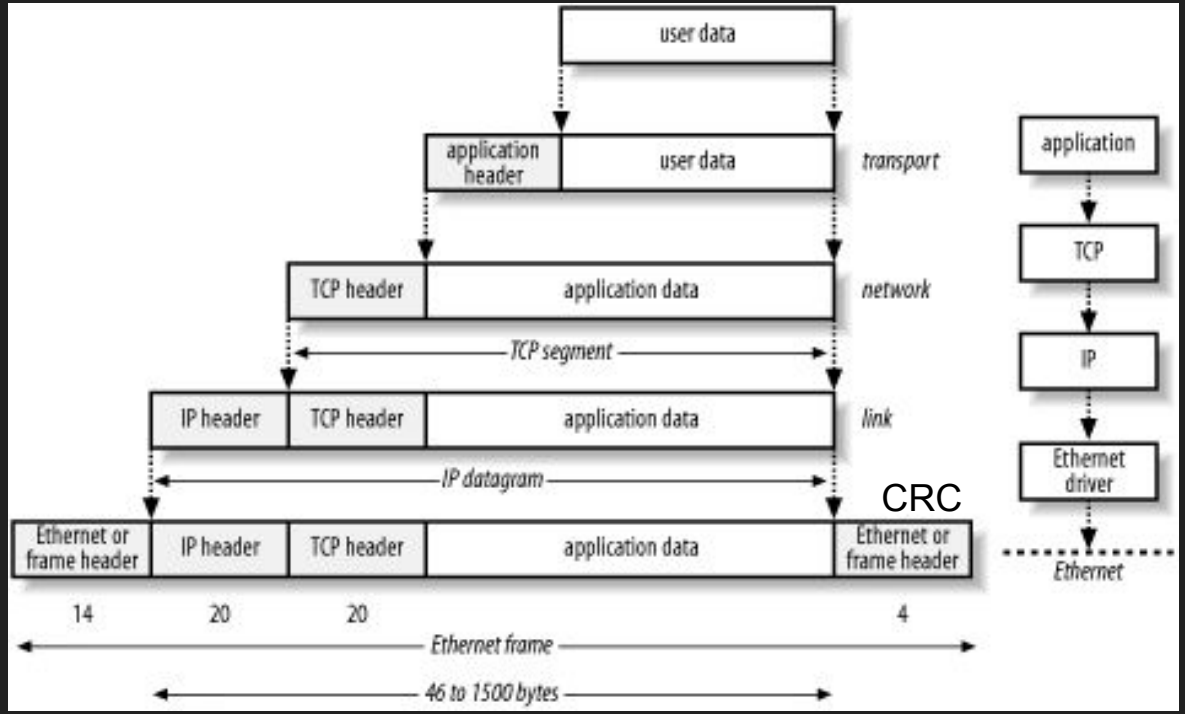
What did the attacker steal or deploy in the company's devices?

.

.

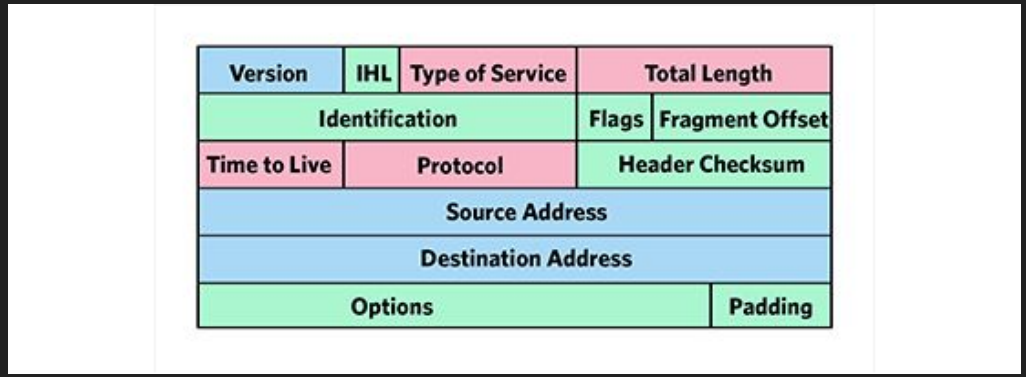
Just before we begin

In order to do all this investigation, we must firstly decorticate the packet (identify all its components) and understand its structure.

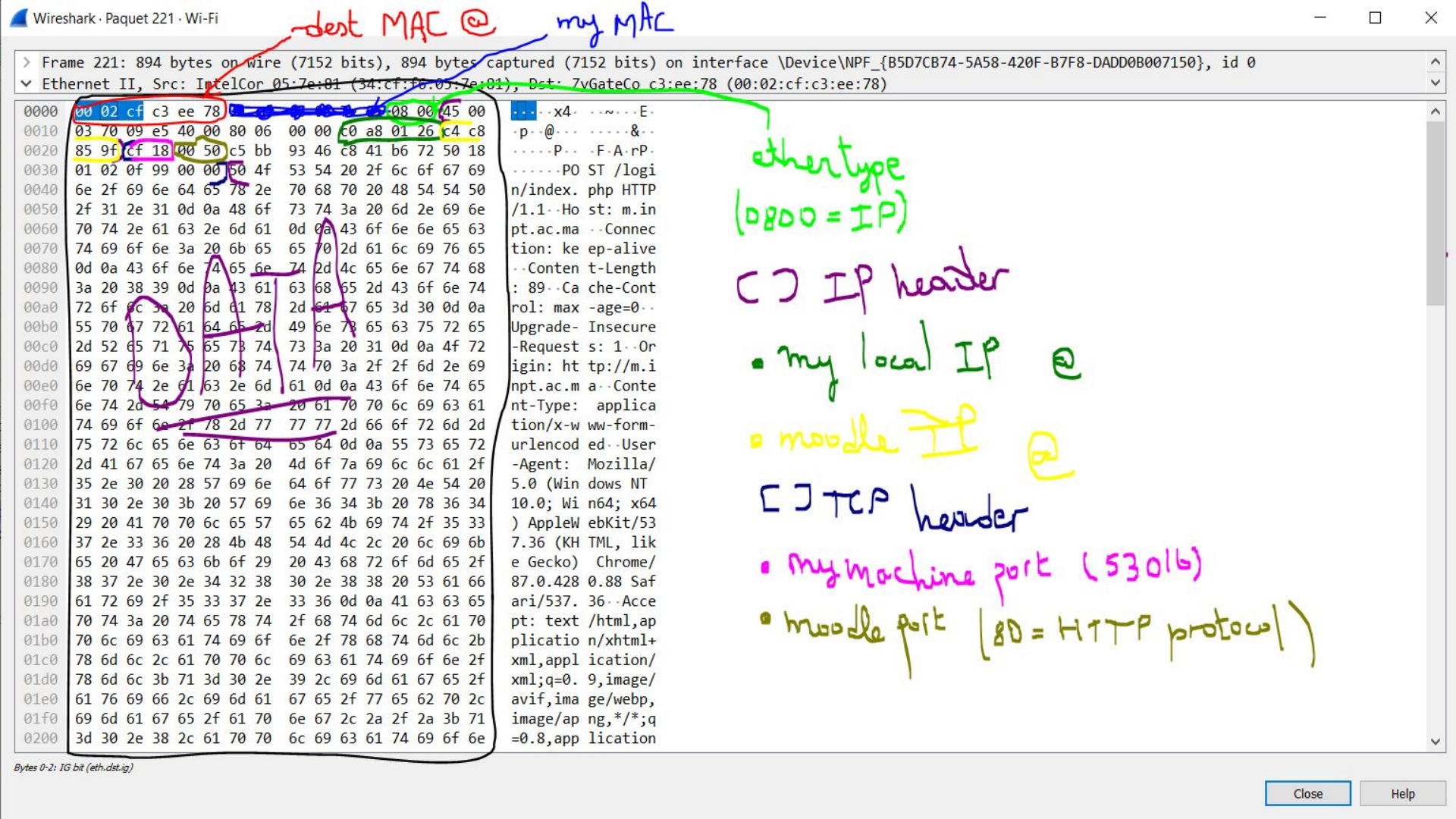


Ethernet header

IP header (much more complicated)



For example, if I want to login into moodle platform, my device will send the following packet:


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:f0:05:7e:81), Dst: ZyGateCo_c3:ee:78 (00:02:cf:c3:ee:78)
0000 00 02 cf c3 ee 78 34 cf f0 05 7e 81 08 00 45 00 ·····x4· ··~···E·
0010 03 70 09 e5 40 00 80 06 00 00 c0 a8 01 26 c4 c8 ·p··@··· ·····&··
0020 85 9f cf 18 00 50 c5 bb 93 46 c8 41 b6 72 50 18 ·····P·· ·F·A·rP·
0030 01 02 0f 99 00 00 50 4f 53 54 20 2f 6c 6f 67 69 ·····PO ST /logi
0040 6e 2f 69 6e 64 65 78 2e 70 68 70 20 48 54 54 50 n/index. php HTTP
0050 2f 31 2e 31 0d 0a 48 6f 73 74 3a 20 6d 2e 69 6e /1.1··Ho st: m.in
0060 70 74 2e 61 63 2e 6d 61 0d 0a 43 6f 6e 6e 65 63 pt.ac.ma ··Connec
0070 74 69 6f 6e 3a 20 6b 65 65 70 2d 61 6c 69 76 65 tion: ke ep-alive
0080 0d 0a 43 6f 6e 74 65 6e 74 2d 4c 65 6e 67 74 68 ··Conten t-Length
0090 3a 20 38 39 0d 0a 43 61 63 68 65 2d 43 6f 6e 74 : 89··Ca che-Cont
00a0 72 6f 6c 3a 20 6d 61 78 2d 61 67 65 3d 30 0d 0a rol: max -age=0··
00b0 55 70 67 72 61 64 65 2d 49 6e 73 65 63 75 72 65 Upgrade- Insecure
00c0 2d 52 65 71 75 65 73 74 73 3a 20 31 0d 0a 4f 72 -Request s: 1··Or
00d0 69 67 69 6e 3a 20 68 74 74 70 3a 2f 2f 6d 2e 69 igin: ht tp://m.i
00e0 6e 70 74 2e 61 63 2e 6d 61 0d 0a 43 6f 6e 74 65 npt.ac.m a··Conte
00f0 6e 74 2d 54 79 70 65 3a 20 61 70 70 6c 69 63 61 nt-Type: applica
0100 74 69 6f 6e 2f 78 2d 77 77 77 2d 66 6f 72 6d 2d tion/x-w ww-form-
0110 75 72 6c 65 6e 63 6f 64 65 64 0d 0a 55 73 65 72 urlencod ed··User
0120 2d 41 67 65 6e 74 3a 20 4d 6f 7a 69 6c 6c 61 2f -Agent: Mozilla/
0130 35 2e 30 20 28 57 69 6e 64 6f 77 73 20 4e 54 20 5.0 (Win dows NT
0140 31 30 2e 30 3b 20 57 69 6e 36 34 3b 20 78 36 34 10.0; Wi n64; x64
0150 29 20 41 70 70 6c 65 57 65 62 4b 69 74 2f 35 33) AppleW ebKit/53
0160 37 2e 33 36 20 28 4b 48 54 4d 4c 2c 20 6c 69 6b 7.36 (KH TML, lik
0170 65 20 47 65 63 6b 6f 29 20 43 68 72 6f 6d 65 2f e Gecko) Chrome/
0180 38 37 2e 30 2e 34 32 38 30 2e 38 38 20 53 61 66 87.0.428 0.88 Saf
0190 61 72 69 2f 35 33 37 2e 33 36 0d 0a 41 63 63 65 ari/537. 36··Acce
01a0 70 74 3a 20 74 65 78 74 2f 68 74 6d 6c 2c 61 70 pt: text /html,ap
01b0 70 6c 69 63 61 74 69 6f 6e 2f 78 68 74 6d 6c 2b plicatio n/xhtml+
01c0 78 6d 6c 2c 61 70 70 6c 69 63 61 74 69 6f 6e 2f xml,appl ication/
01d0 78 6d 6c 3b 71 3d 30 2e 39 2c 69 6d 61 67 65 2f xml;q=0. 9,image/
01e0 61 76 69 66 2c 69 6d 61 67 65 2f 77 65 62 70 2c avif,ima ge/webp,
01f0 69 6d 61 67 65 2f 61 70 6e 67 2c 2a 2f 2a 3b 71 image/ap ng,*/*;q
0200 3d 30 2e 38 2c 61 70 70 6c 69 63 61 74 69 6f 6e =0.8,app lication
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

The example we've shown you is for a live capture, but what if an attack happened yesterday, we won't be able to track every packet every day (there isn't a job for that!!).

So in companies, we mostly save a capture with thousands of packets every day or hour (depending on how big is the traffic inside the company) in a file with the extension *.pcap* or *.pcapng*. You can open this kind of files with wireshark or any other packets capture software.

Here comes the forensics engineer role after or during an attack (sometimes on a daily basis), he needs to take each saved pcap file into consideration, analyze its packets and infiltrate what he does really need (since he can't analyze thousands of packets every day, he isn't a robot!!).

Get your hands dirty

Challenge 1 :

>> we captured some network traffic from a website that we believe has a flag on it. The data has already been filtered to eliminate any unnecessary packets. Can you analyze the capture file using wireshark and do these two tasks?

1st task: what protocol was the flag transferred with?

2nd task: what is the flag?

CRC

Flag syntax: ctfa{}

Get your hands dirty

Challenge 2 :

>> This time, we have captured some network traffic from a website that we think has two flags on it. However, we were not able to filter out unnecessary packets, so you will have to sift through them to find the HTTP packets containing the flags. Good luck!

1st task: Gimme the flags nooow!

CRC

2nd task: if we suppose that the capture began at `21:12:43`, when was the 2nd flag sent exactly (`hh:mm:ss`)?

Flags syntax: ctfa{}

2- OSINT

`whatis 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 the 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, ...)

`whatis 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 infos about someone, (a hacker if you’re an IT security pro, employees of a company if you’re a hacker).

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.

No tools? Just research?

Firstly, we should know that there aren’t some specific tools to do OSINT. 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).

One important thing is that:

YANDEX >>>>>>>>>>>>>>>>>>>>>>>>> GOOGLE

For example, if you’re given an image, the first reflex is to upload it to google images to find its context, yet, yandex images can give you much more precise information.

Get your hands dirty

Challenge 3 :

>> we're following lately a suspect called James, we recently found his twitter yet we have to know which US political party does he support ?

here's his twitter account:

https://twitter.com/jammymarkson

CRC

Get your hands dirty

Challenge 4 :

>> we're suspecting that James is hiding something in his house, we need to break into it but we have to be sure he's at work.
Can you please tell me in what city does he work ?

here's his twitter account:
https://twitter.com/jammymarkson

CRC

Get your hands dirty

Challenge 5 :

>> we're suspecting that a website has some illegal activities but when we try to access it, the server is not responding.
our sources suggest that this server was active 4 years ago but we don't know what to do with this information!! I think you'll find a flag there!
Flag syntax: IceCTF{}

CRC

here's the website address:

http://time-traveler.icec.tf/

Get your hands dirty

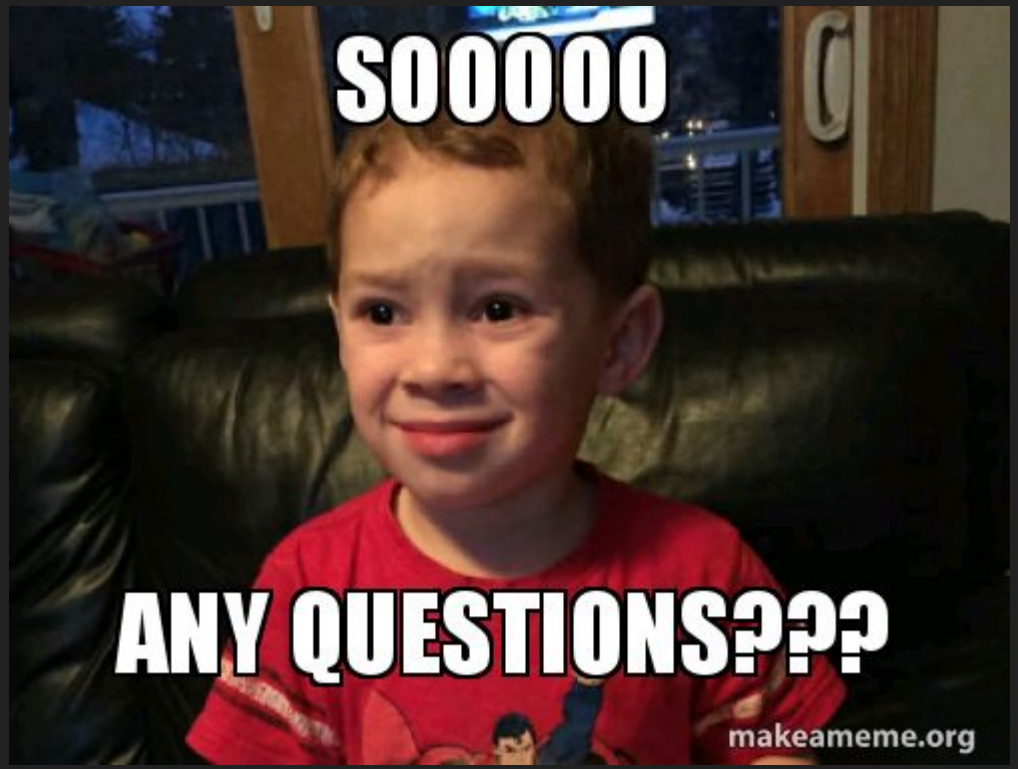
Challenge 6 :

>> A suspect was running away in the airport when he dropped this boarding pass, it's clear that he erased some pieces of information there, can you recover it and give us the number his seat number in the plane?

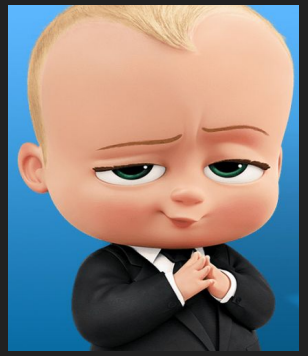
CRC

shutdown

tfi dak lmch9of



ls -al .Contact_us



OUSSAMA RAHALI

Facebook : /oussama.rahali.925

OMAR AOUAJ

Facebook : /omar.aouaj.77