THE NORTHCAP UNIVERSITY

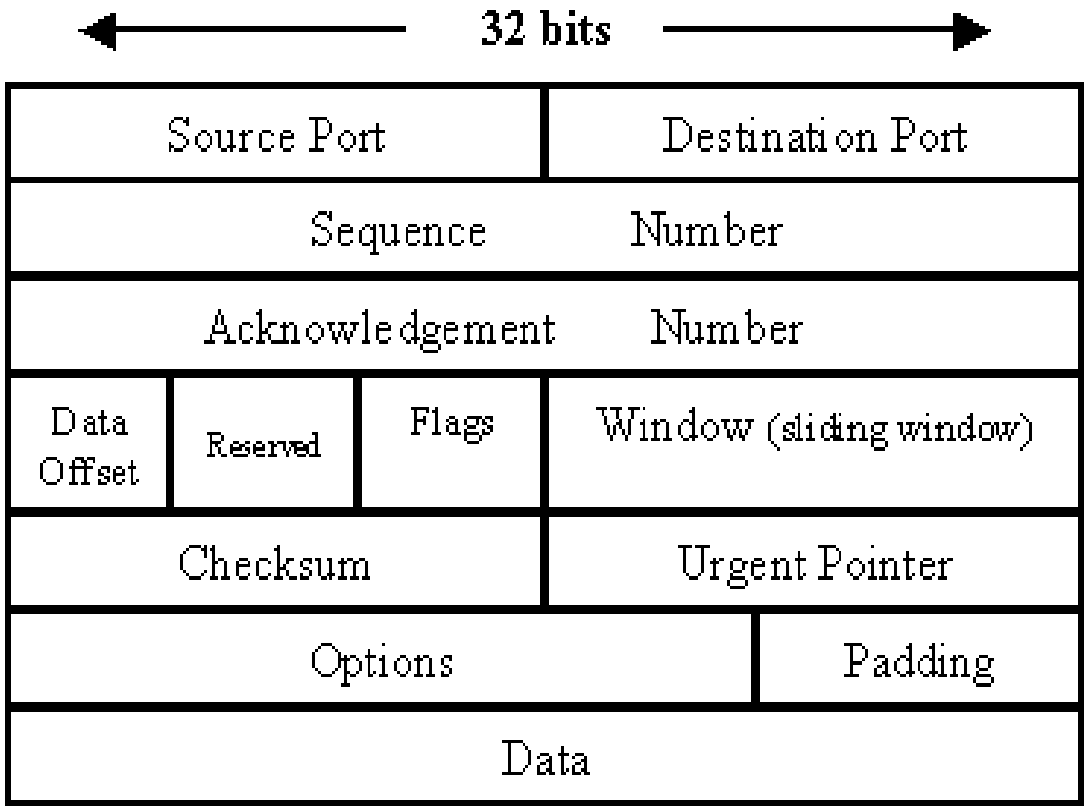
Network Scanning/Sniffing

30 YEARS OF EXCELLENCE

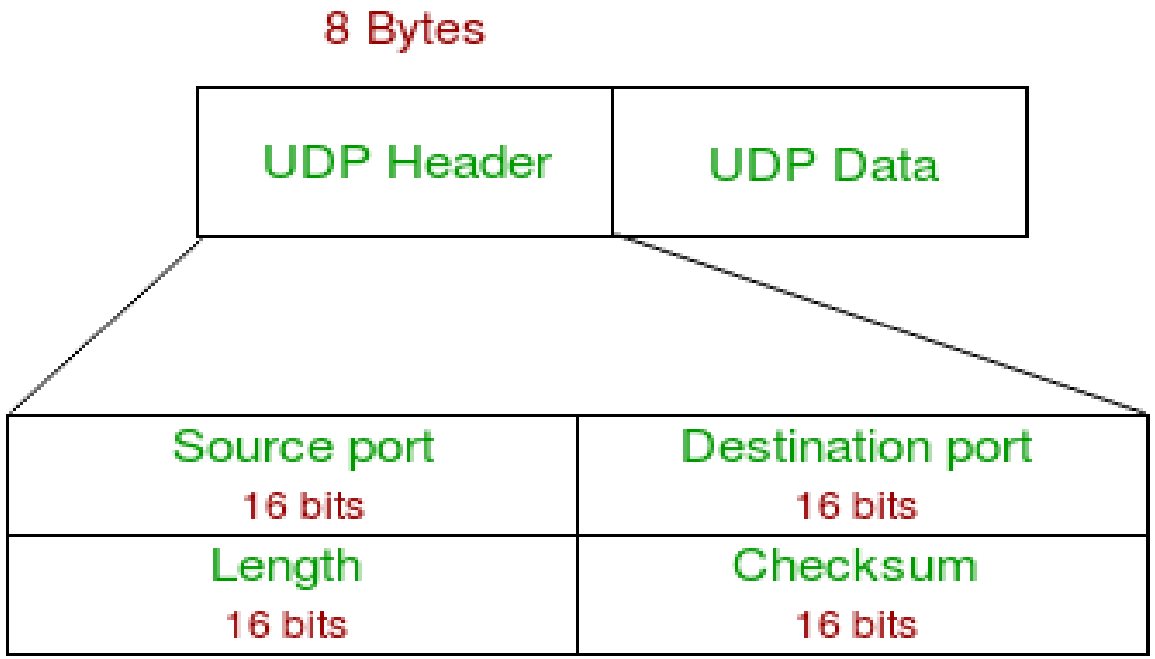
NAAC Accredited

2 Protocols- TCP and UDP

- TCP header



UDP Header



Inclass Question

Q. Suppose Sender is sending packets to the receiver.

- If suppose last 5 packets are lost?
- How does receiver know how many packets are there?
- What is the last packet?

Ans:

Therefore, in TCP there is a **index packet** which sends **total no. of packets** before sending all the packets

And connection is **not disconnected till sender does not receive acknowledgement** for it.

Flags

Syn: Synchronise Flag

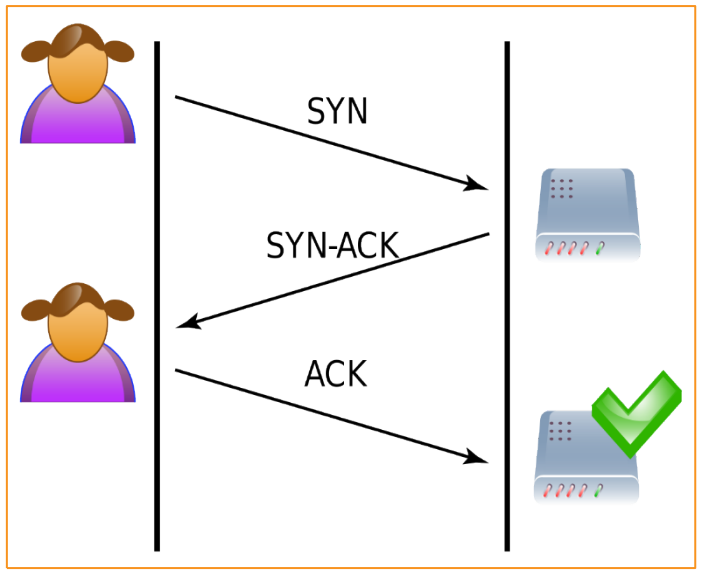
Ack: Acknowledgment Flag

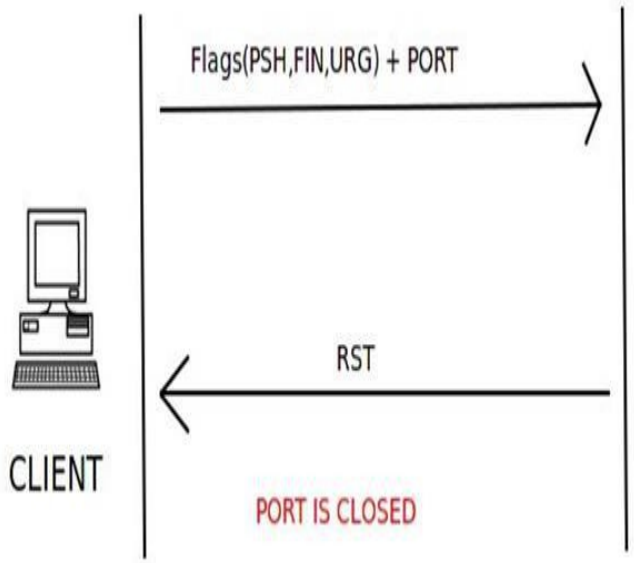
- 3 way handshaking

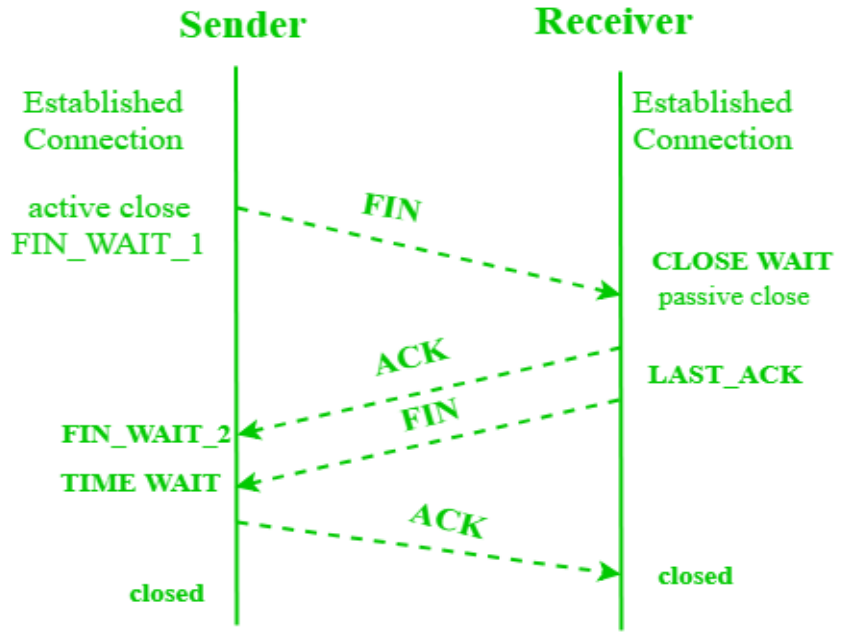
RST: Reset Flag

FIN: Finish Flag

Forced Stop







- https://cybersecuritynews.com/syn-attack/?fbclid=IwAR0CSGi3D-pb5LE1V1-cPVdIKeIhpZ5Lpm9qbATVjd7m6fQSMXELIaIoAXA

Network Scanning

THE NORTHCAP UNIVERSITY

Another type of scanning

Scan network to **extract information**

- **Web link**
- **Source IP**
- **Destination IP**
- **Usernames**
- **Passwords**
- **Cookies**

If Using Same credentials for other sites like LinkedIn, Twitter, etc

Can be done by sniffing packets

30 YEARS OF EXCELLENCE

NAAC Accredited

What is a Packet Sniffer

THE NORTHCAP UNIVERSITY

- To **monitor the data transmitted** over a network
- Used **for diagnostic or troubleshooting** purposes To
- **steal data** transmitted over the network.
- **Applicable to both wired and wireless networks**
- Can be **passive or active**

30 YEARS OF EXCELLENCE

NAAC Accredited

What information can be retrieved from a sniffer?

THE NORTHCAP UNIVERSITY

If an **end user sends credit card/password information over an insecure protocol.**

If the attacker manages to **steal the private** cryptographic **key, then it can be directly provided to sniffer to decrypt all the communication.**

Examples

Use of **weak standards like WEP** are vulnerable to sniffing.

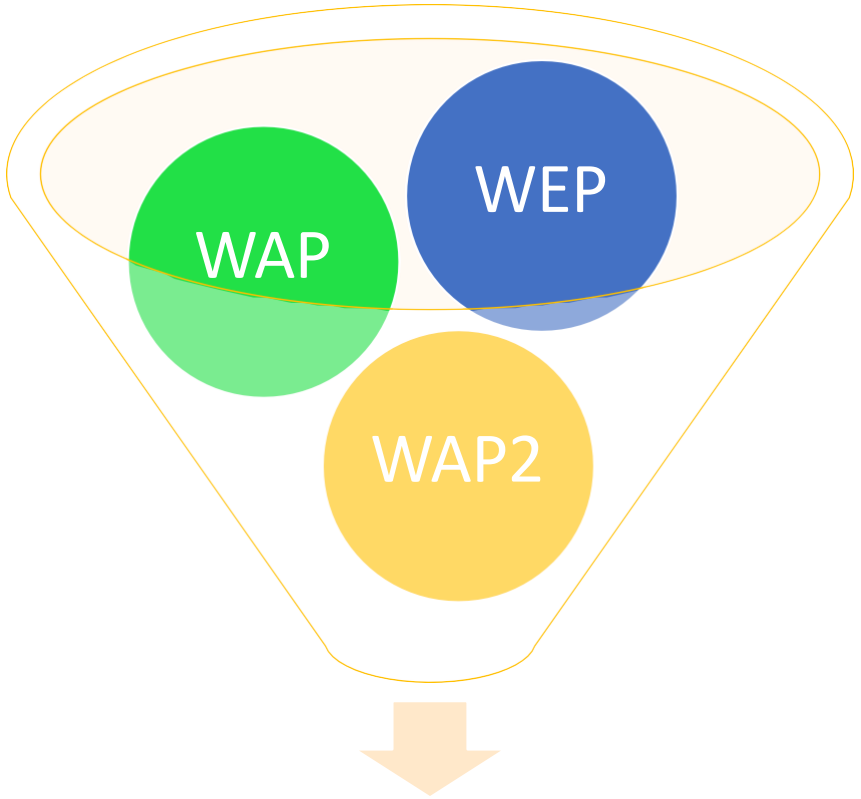
?

30 YEARS OF EXCELLENCE

NAAC Accredited

Class Task

What does WIFI at your home uses?



??

Check and take screenshot with your admin name in it so to identify that it is your system only.

Top Sniffing Tools list

Wireshark

THE NORTHCAP UNIVERSITY

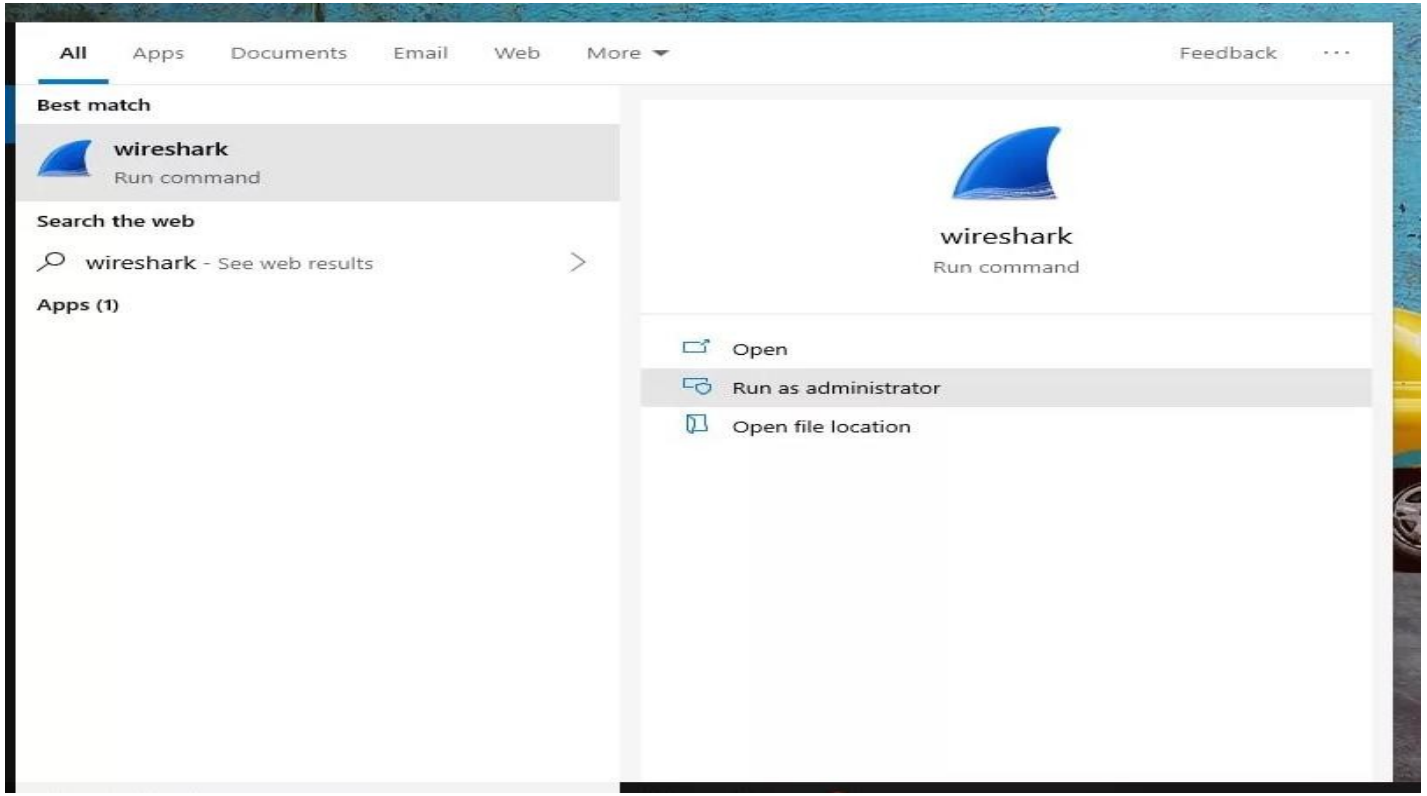
- World's foremost and **widely-used network protocol analyzer**.
- Tells **what's happening** on your network **at a microscopic level**
- **Standard across** many commercial and non-profit enterprises**,** government agencies, and educational institutions.
- **Got famous in black hat**.
- **Observes the messages exchanged.**
- **Passive and Preinstalled in Kali Linux,** for **windows** http://www.wireshark.org.

30 YEARS OF EXCELLENCE

NAAC Accredited

1. Open the Wireshark

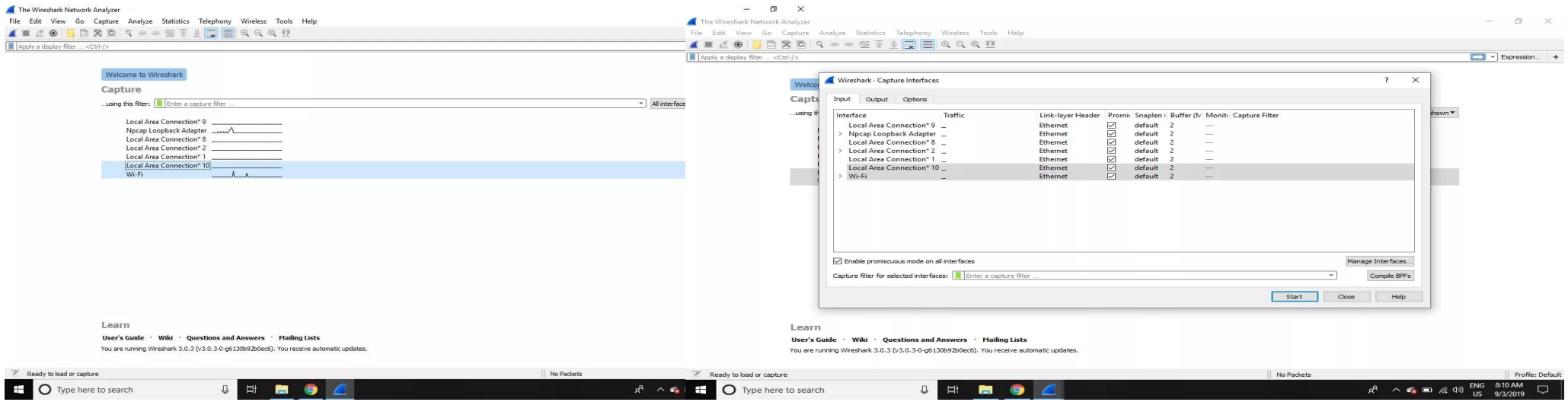
- Run as admin



2. Select the network/interface

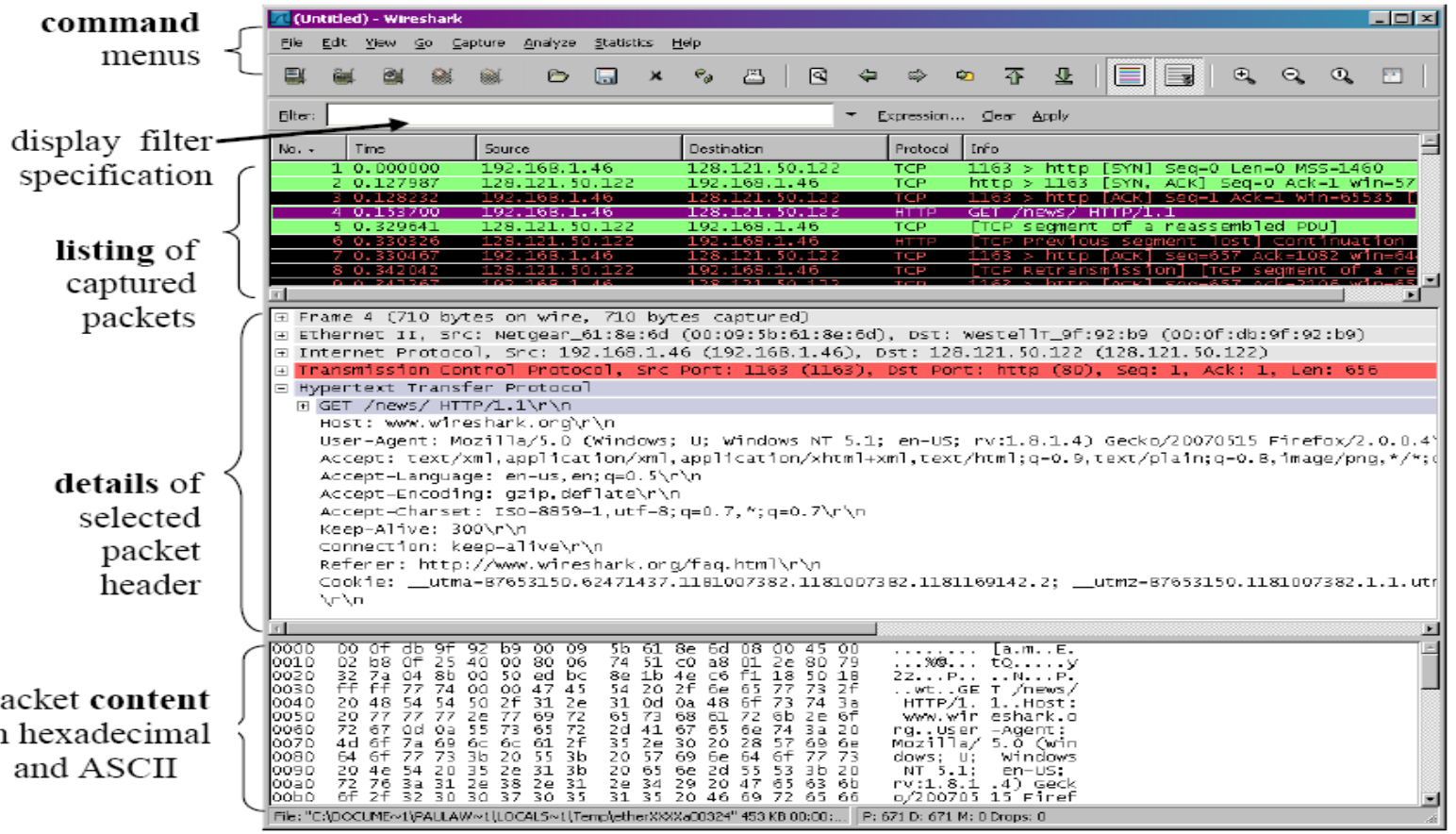
Select one or more of networks, go to the menu bar, then select **Capture**.

- Promiscuous mode (Capture > Options)
  - On – record all packets reaching the interface
  - Off – record only those packets directed to the host.



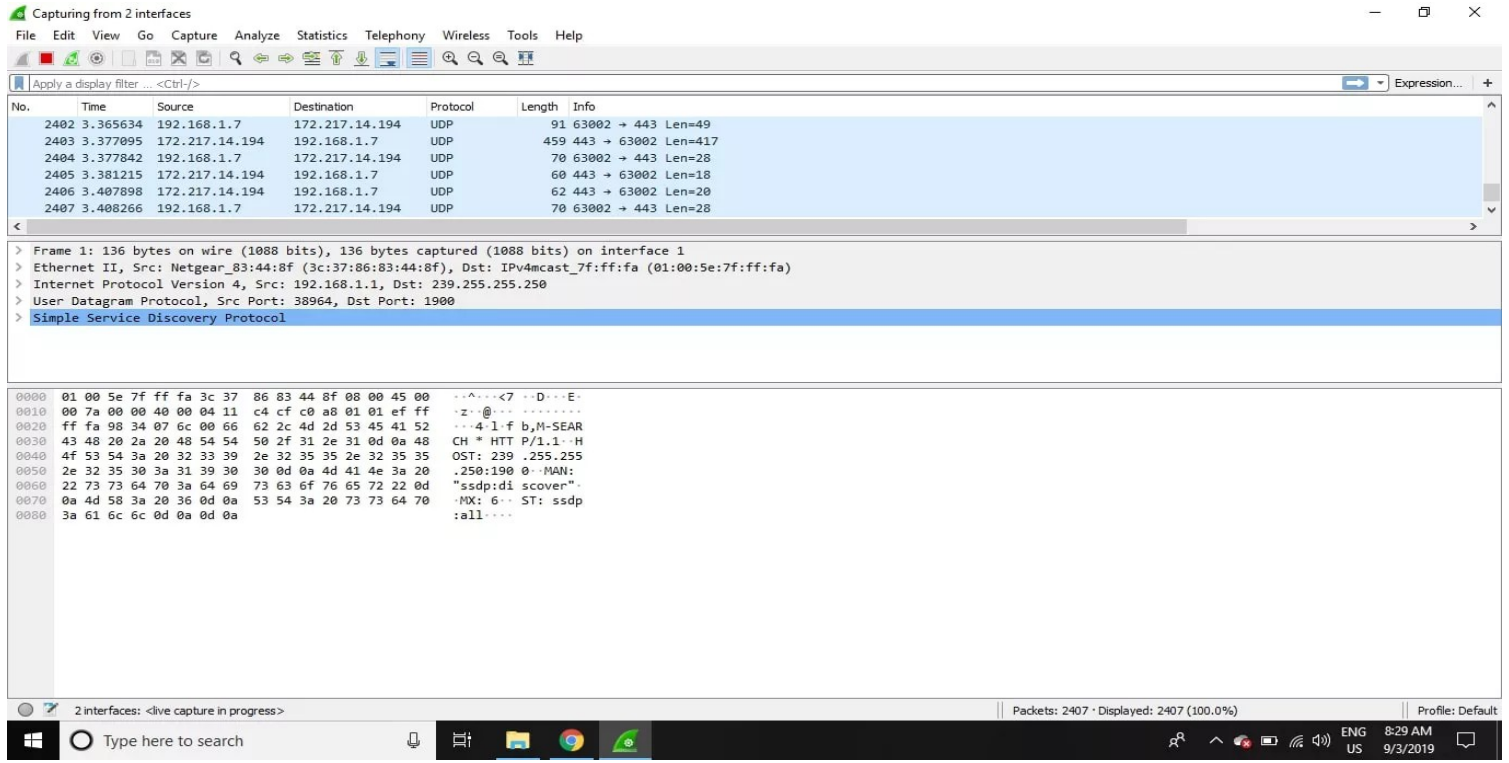
4. Shows all the traffic

- It will show all the traffic in the network



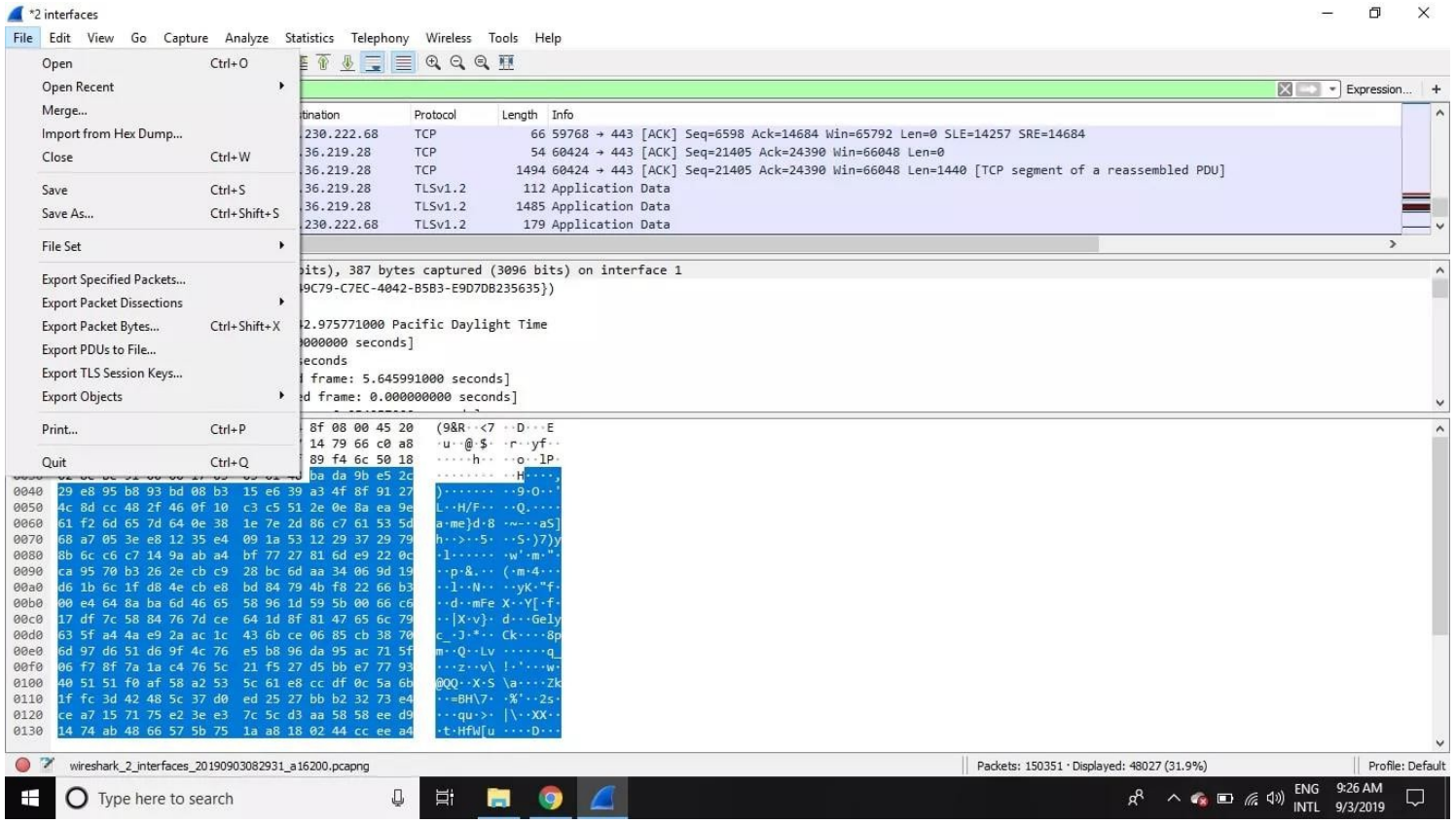
5. Stop Capturing

- To stop capturing, press **Ctrl+E**. Or, go to the Wireshark toolbar and select the red **Stop** button that's located next to the shark fin.



6. Save File

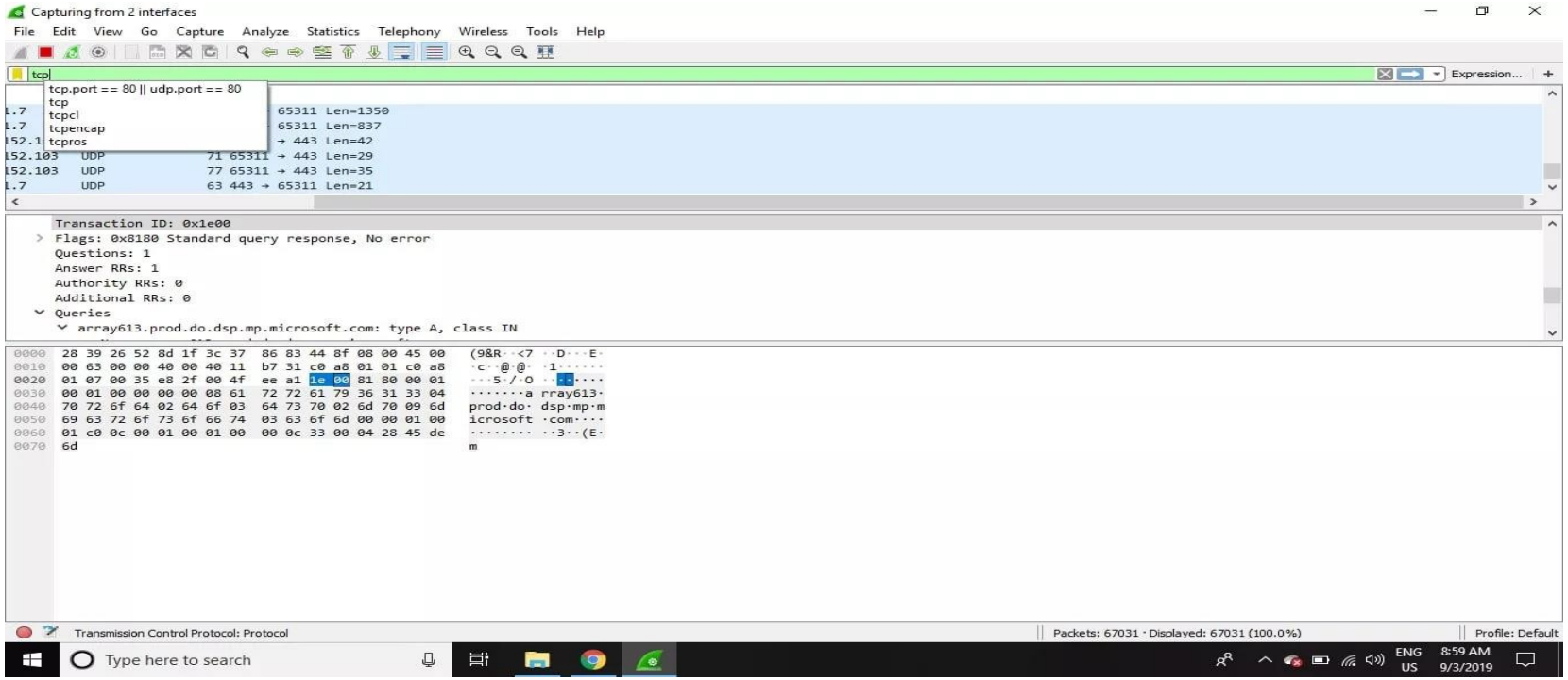
- Select **File** > **Save As** or choose an **Export** option to record the capture



How to Use Wireshark Filters

Provides a predefined filters by default (**Apply a display filter)**

If you want to display TCP packets, type **tcp**



How to Use Wireshark Filters

a. it can specify an address

- e.g
- ip.addr==192.168.0.1
- ip.src==10.1.11.0

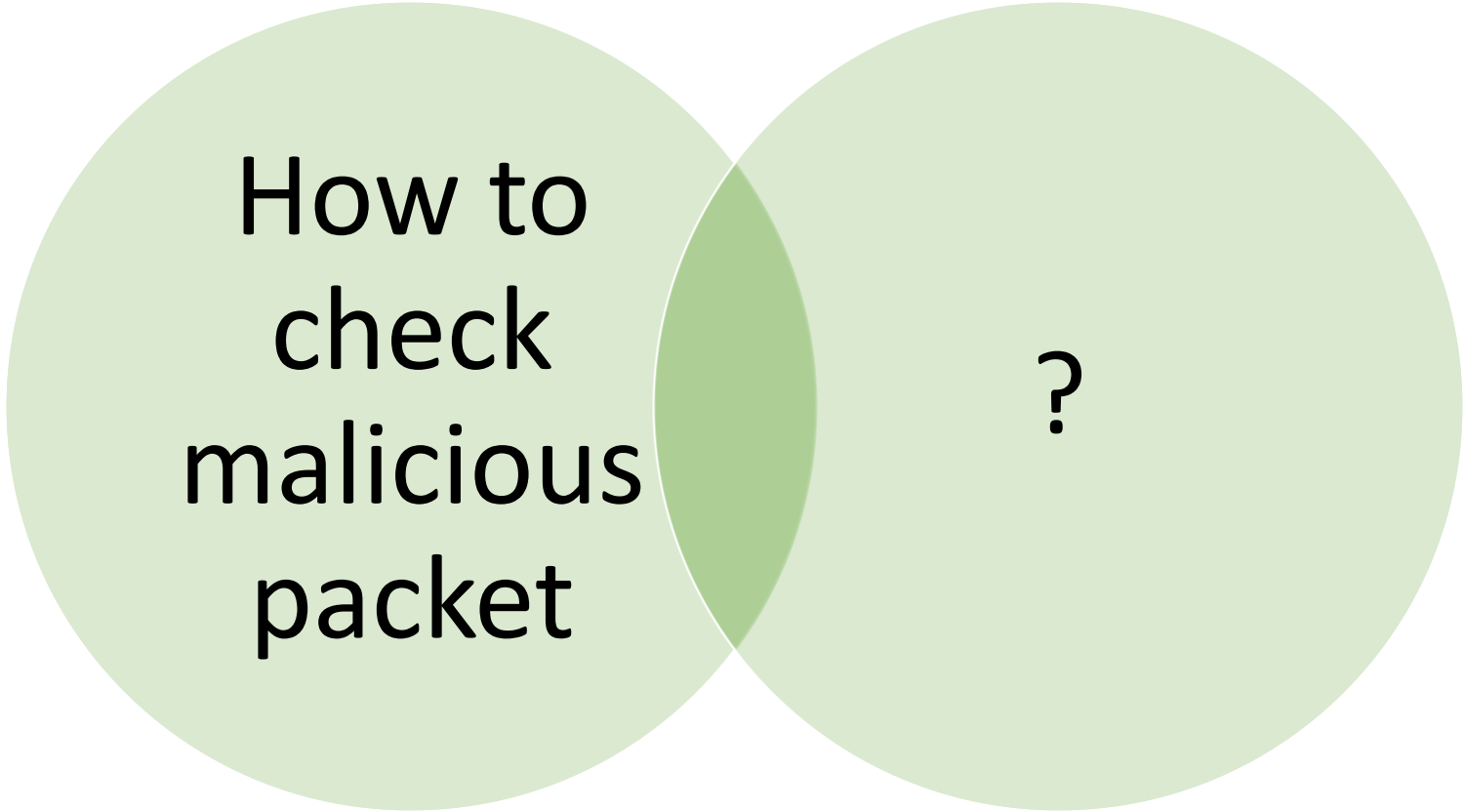
b. it can also specify a protocol

- e.g.
- tcp.port==80||tcp.port==3338
- tcp.port==80&&tcp.port==3338

e.g. Combine filters: the traffic from a particular IP and for http

- HTTP && IP.src=12:234:56:67:67:12

In class Exercise



To check victim's using http-GET request

THE NORTHCAP UNIVERSITY

Start Wireshark to capture packets

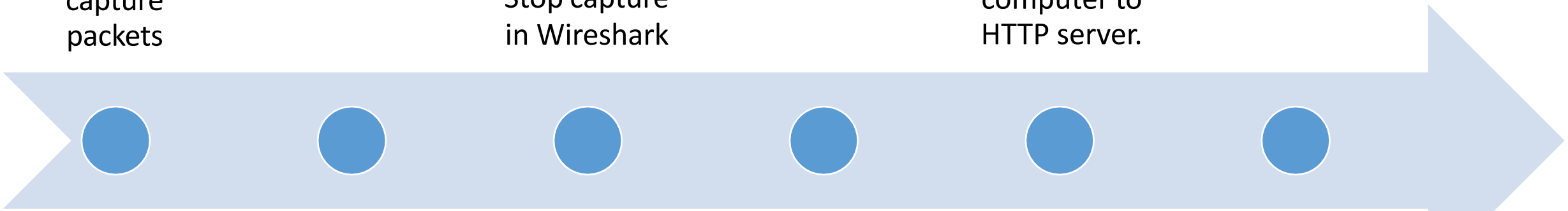
Go to web browser, **open some image**

Stop capture in Wireshark

You will see an get line and then a **HTTP1.1 get request line**

It is HTTP GET message sent from your computer to HTTP server.

And next http line shows response from web server (handshaking)



30 YEARS OF EXCELLENCE

NAAC Accredited

To check victim's using http-Get Request

Select it, you will see a JPEG or PNG key depending on which format of image you have opened

Select and right click.

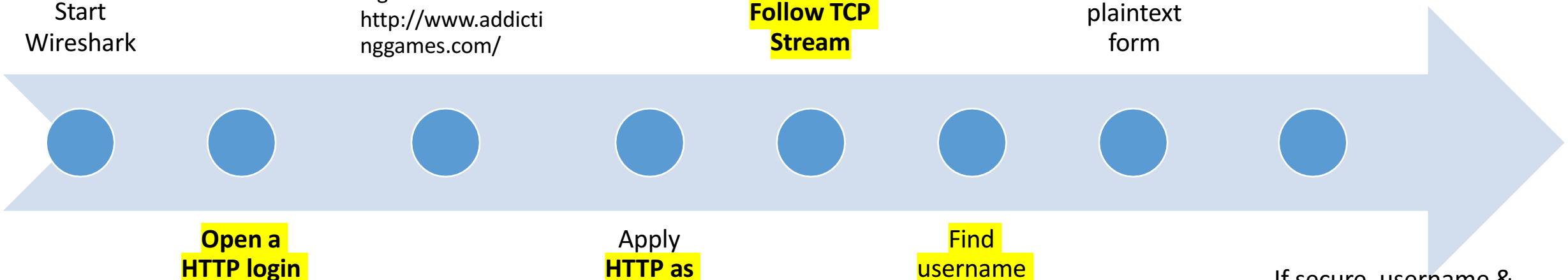
Select option **Export Selected Packet Bytes :** Save file/ open

You will get the actual file which was opened by the Victim

http://testphp.vulnweb.com/

00Ref_Wireshark_webLink&userpass.docx

To Crack Password of victim's using http-Post



Start Wireshark

Open a HTTP login website

Enter username and password credentials (e.g. game site, erp, LMS)

- E.g. http://www.addictinggames.com/

Apply **HTTP as filter** and locate a POST packet

Right click and select **Follow TCP Stream**

Find username and password there

If insecure username & password are visible in plaintext form

If secure, username & password might be available in encrypted form

00Ref_Wireshark_webLink&userpass.docx

Exercise/Assignment

THE NORTHCAP UNIVERSITY

Q1. Perform the attack to find the specific information visited by the victim

Q2. Perform the password hijacking on http website

- Find the username and password
- Write steps with screenshots

30 YEARS OF EXCELLENCE

NAAC Accredited

Cookies

An HTTP cookie is also called **web cookie, Internet cookie, browser cookie** or simply cookie

Small piece of **data sent from a website**

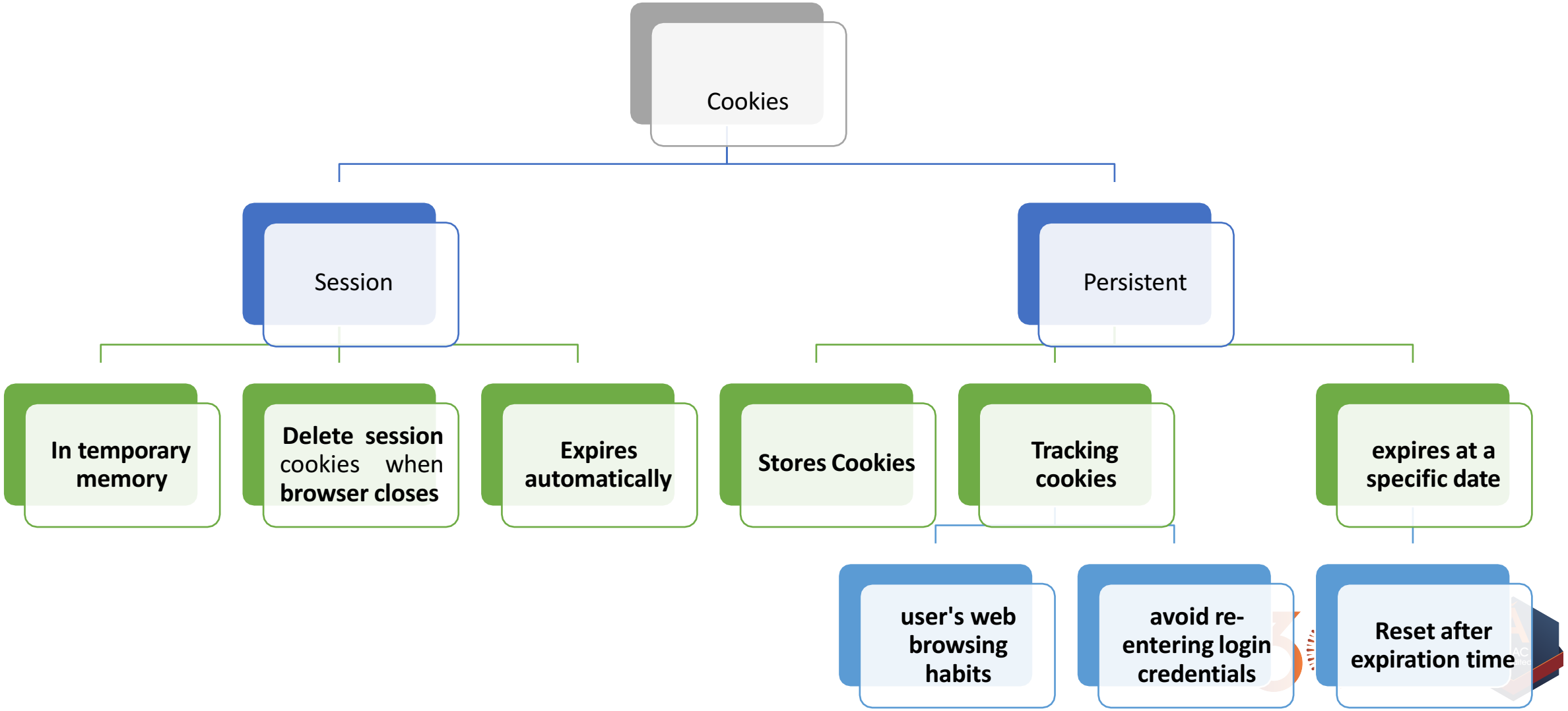
Stored in the **user's web browser** while the user is browsing.

Remember info entered in form fields **such as names, addresses, passwords, and credit card numbers**.

E.g. Remember items added in the cart in an online store

E.g. Recording which pages were visited in the past.

Types of Cookies



Session management & Personalization

THE NORTHCAP UNIVERSITY

Session management

- Server sends a cookie to the client that **contains a unique session identifier**
- Session identifier will be **sent back to the server every time the user visits** a new page on the website

Personalization

- Used to remember information about the user
- Cookie contains the username last used to login and automatically fill it next time when the user logs in
- However, the contents of shopping cart are stored in DB on server, rather than in cookie on the client

Session management & Personalization

THE NORTHCAP UNIVERSITY

Session management

- Server sends a cookie to the client that **contains a unique session identifier**
- Session identifier will be **sent back to the server every time the user visits** a new page on the website

Personalization

- Used to remember information about the user
- Cookie contains the username last used to login and automatically fill it next time when the user logs in
- However, the contents of shopping cart are stored in DB on server, rather than in cookie on the client

30 YEARS OF EXCELLENCE

NAAC Accredited

Q. Find IP address using Wireshark and tell them you know where they live?

THE NORTHCAP UNIVERSITY

In the filter bar, type UDP

You are set to troll people

Open omegle.com

Start chat by typing hey

Type ”wanna bet I can find where you live”

Start a new capture

Open ipaddress.com/search/

Type destination found above (2.88.12.41) & press lookup

This provides destination country e.g. “Saudi Arabia”, Administrative contact & other details

30 YEARS OF EXCELLENCE

NAAC Accredited