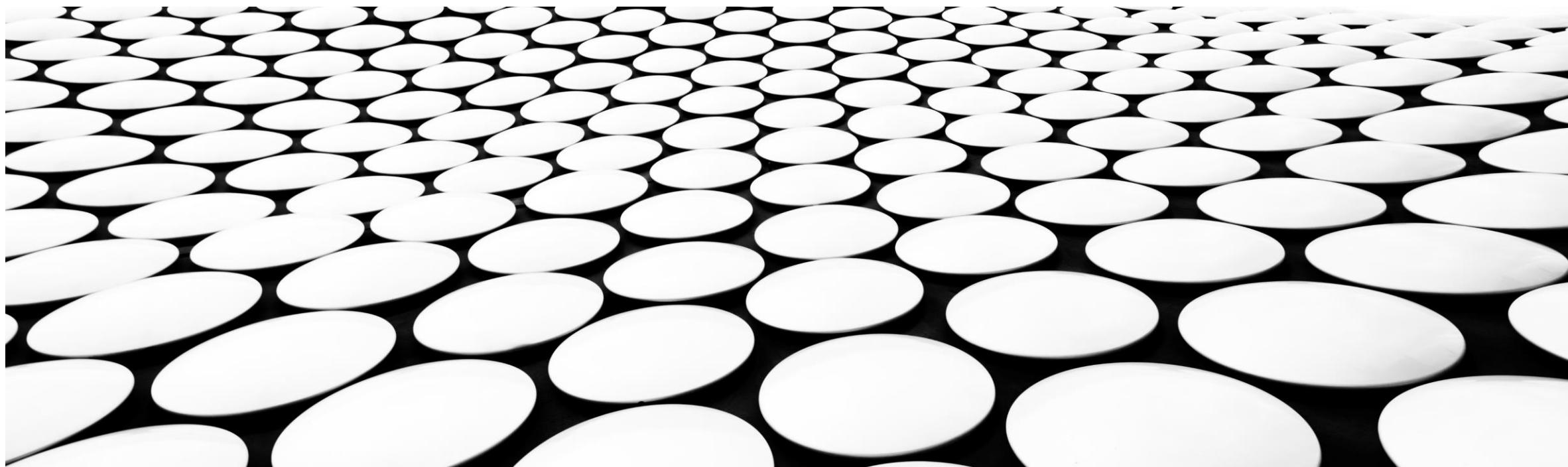


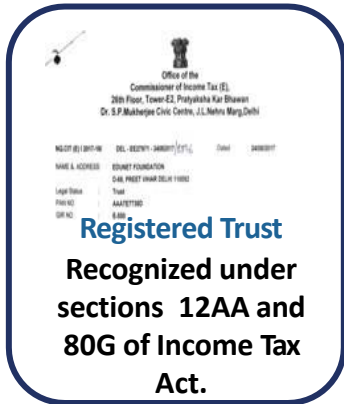
---

# SKILLSBUILD FOR COLLEGES

EDUNET FOUNDATION



# Edunet Foundation



# Goal

## Creation of educational networks and sustainable communities

## Focus

## 4<sup>th</sup> & 5<sup>th</sup> Industrial Revolution

focused Employability and Entrepreneurship

# Audience

**150,000+** learners in past 12 months from K-12 schools, ITIs and colleges

More than **300,000+** Higher Education learners

## National Footprint

Large pool of technical manpower on the ground:  
70+ technical and soft-skills trainers

Over 250 active institution partnerships and access to tens of thousands of students

---

# MAN-IN-THE-MIDDLE ATTACK

MITM

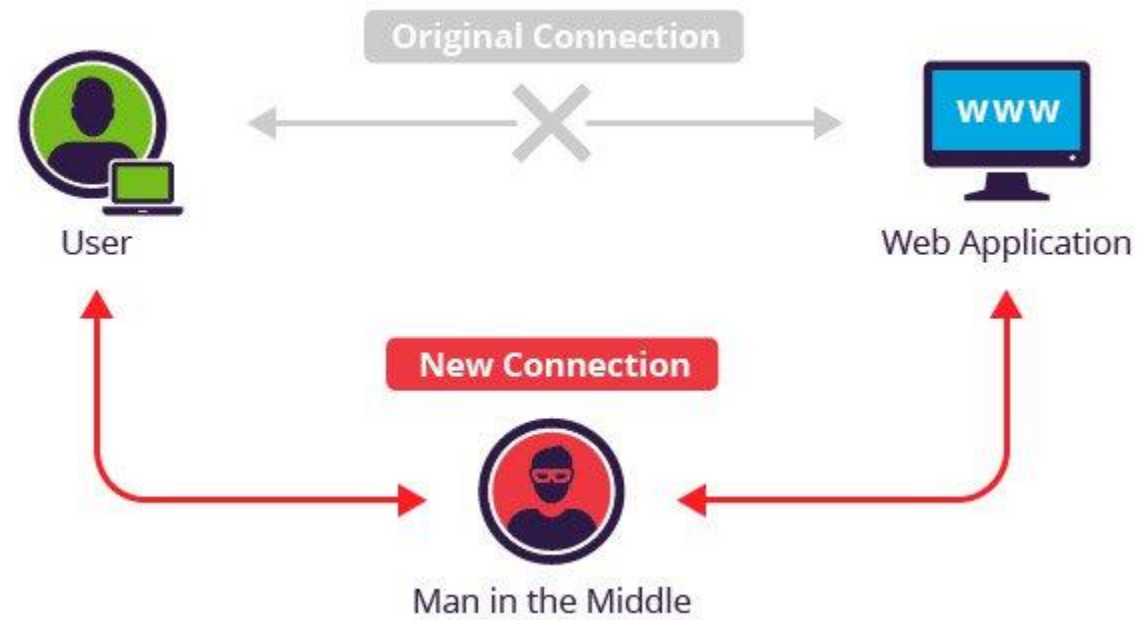


## MITM ATTACK & ARP SPOOFING

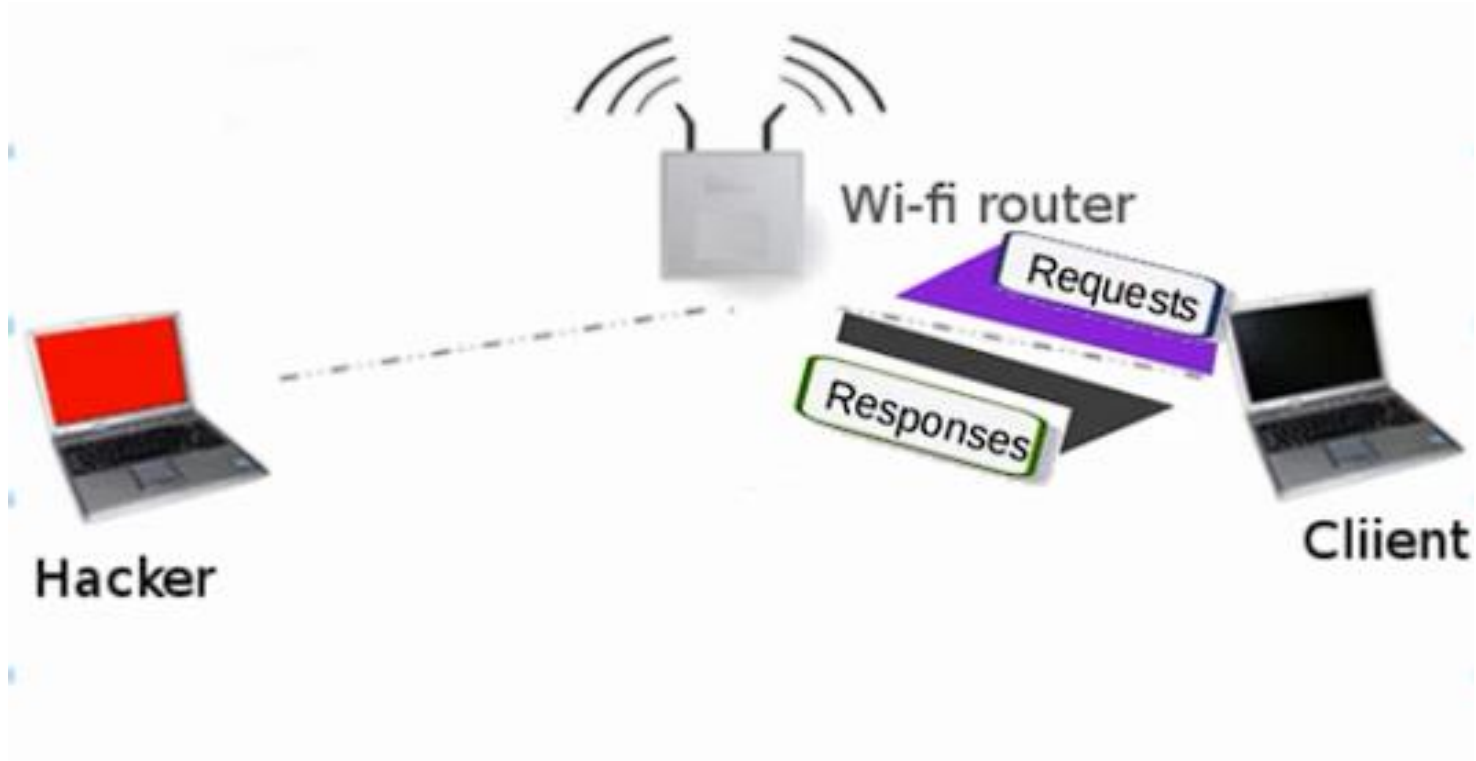
This is one of the most dangerous and effective attacks that can be used, it is used to **redirect packets to and from any client to our device**, and since we have the network key, we can read/modify/drop these packets. This allows us to launch very powerful attacks.

It is very effective and dangerous because it's very hard to protect against it as it exploits the insecure way that ARP works.

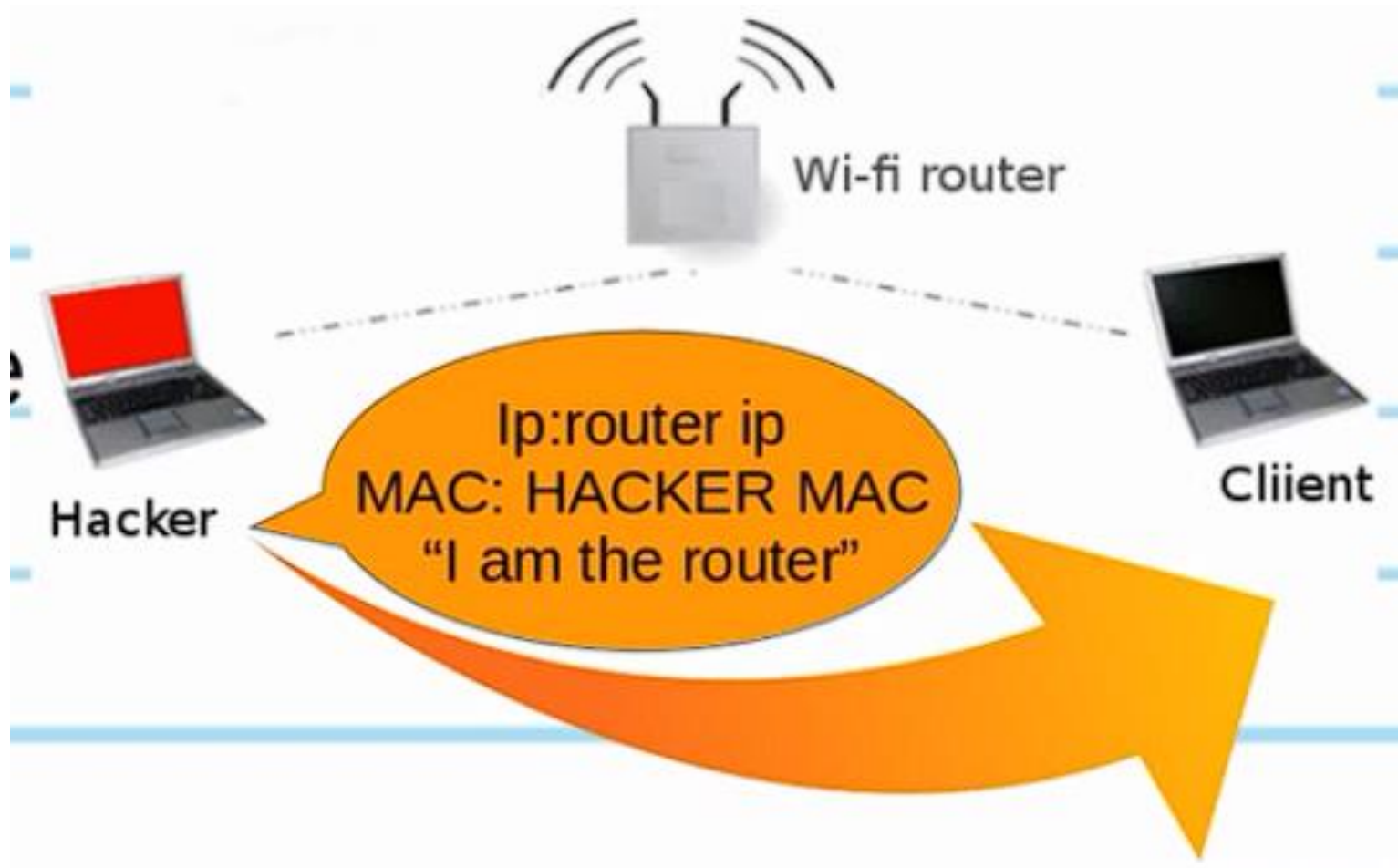
# MAN-IN-THE-MIDDLE ATTACK



# MAN IN THE MIDDLE ATTACKS ARP POISONING



# MAN IN THE MIDDLE ATTACKS ARP POISONING



## OVERVIEW OF MITM ATTACKS

1. Interception in MITM Attacks
2. Eavesdropping in MITM Attacks
3. Data Modification in MITM Attacks
4. Spoofing and Identity Impersonation in MITM Attacks



# DNS-SERVER



# DNS (DOMAIN NAME SYSTEM)

- DNS is kind of directory service.
- It provides mapping between host name and its numerical address
- Numerical Address is nothing else but the IP address of any resource which is stored on server
- Example of IP address : 172.16.16.21
  
- Why DNS is required
- Difficult to remember numerical address of different resources



# **WIRESHARK-PACKET ANALYZER**

# WHAT IS WIRESHARK

1. Wireshark is the widely-used network protocol analyzer
2. It is an application that captures packets from a network connection
3. It is commonly called as a sniffer, network protocol analyzer, and network analyzer



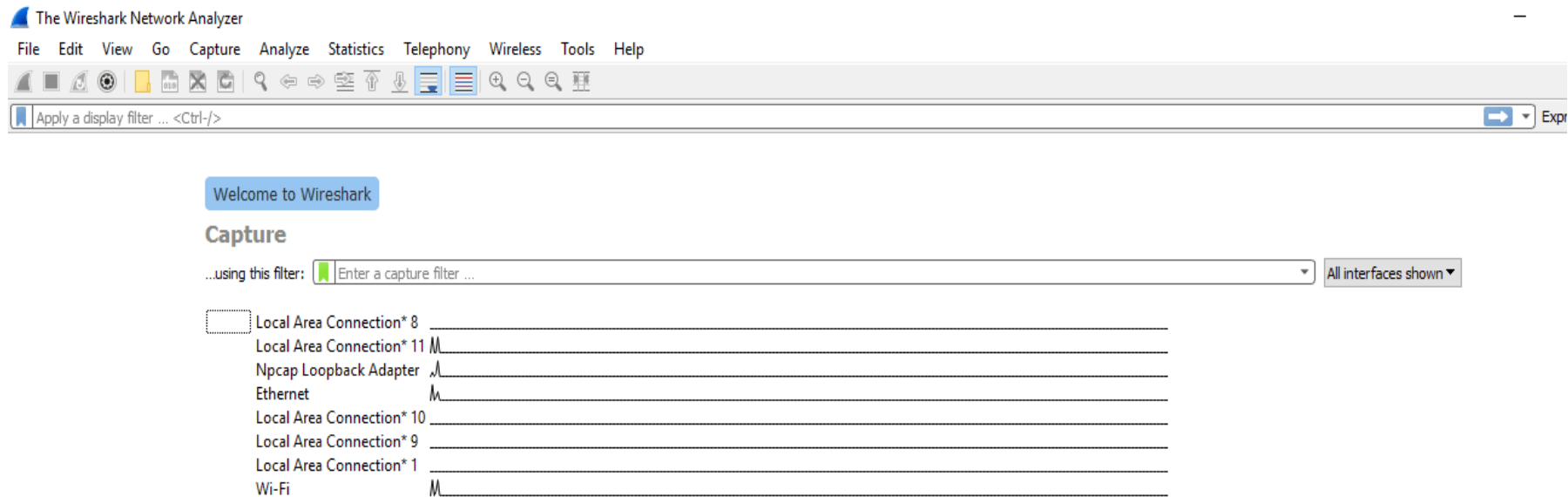
## USES OF WIRESHARK

1. Network engineers use it to troubleshoot network issues.
2. Network security engineers use it to investigate security issues.
3. It allows users to view every traffic passing via the network.
4. It also aids in the diagnosis of latency issues and malicious network activity.
5. It can also examine packets that have been dropped.



Open Wireshark and select NIC(Network Interface) .

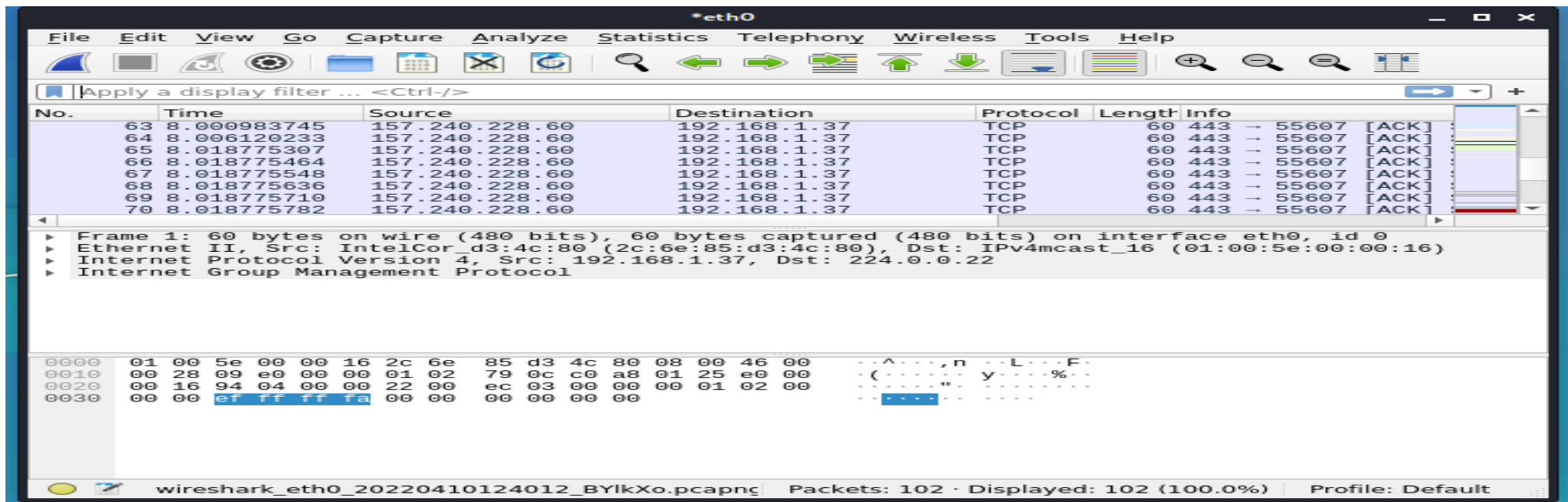
## STARTING WIRESHARK



# CAPTURE PACKETS IN WIRESHARK

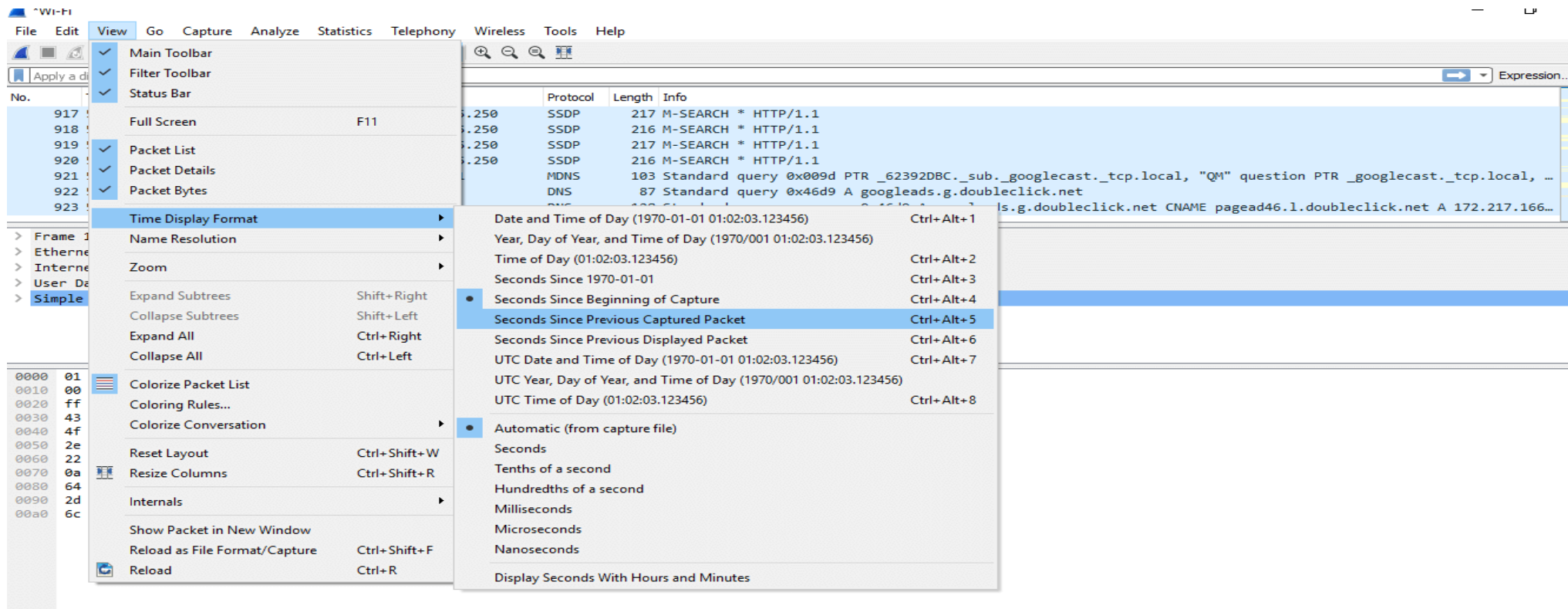
Open Wireshark and select NIC(Network Interface) .

Click on start button



We may also modify the interface view using the view option on the menu bar. The number of items in the view menu can be changed. You can also enable and disable any option based on your needs.

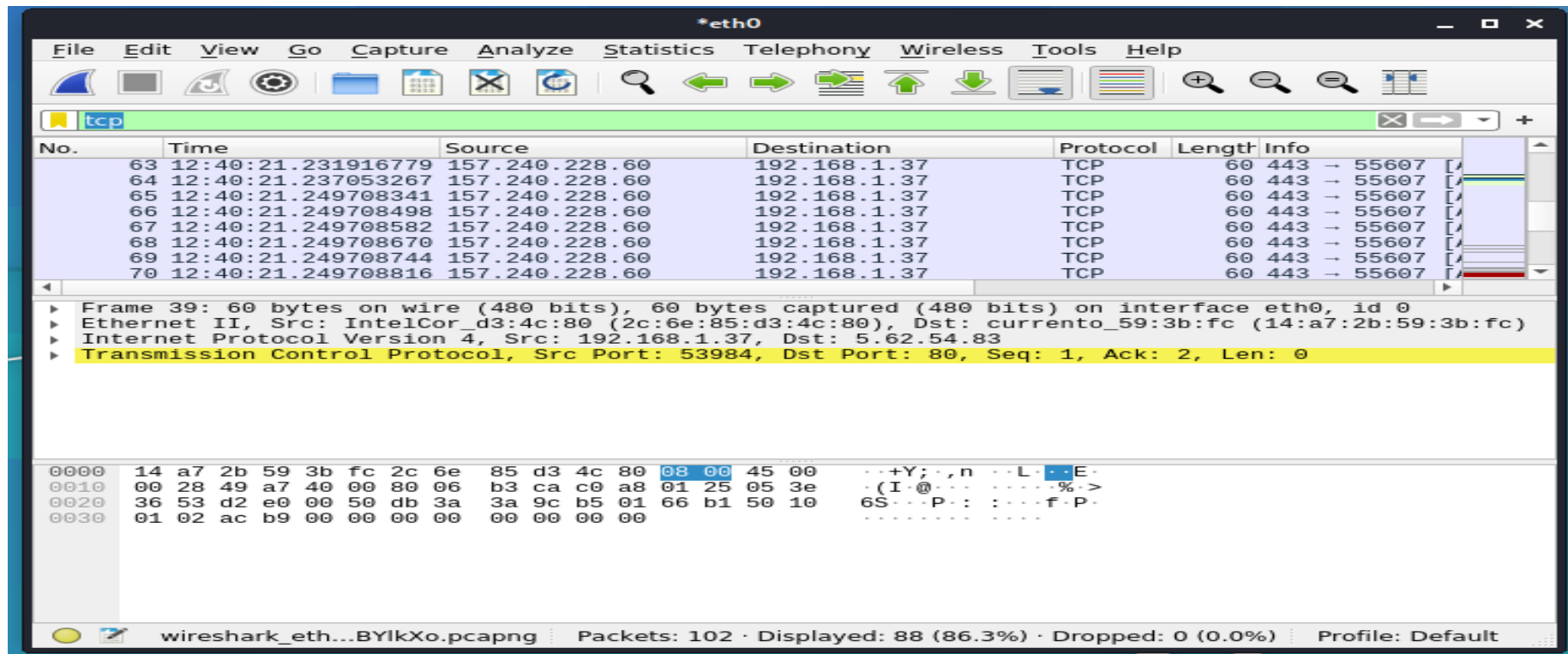
## WIRESHARK VIEW





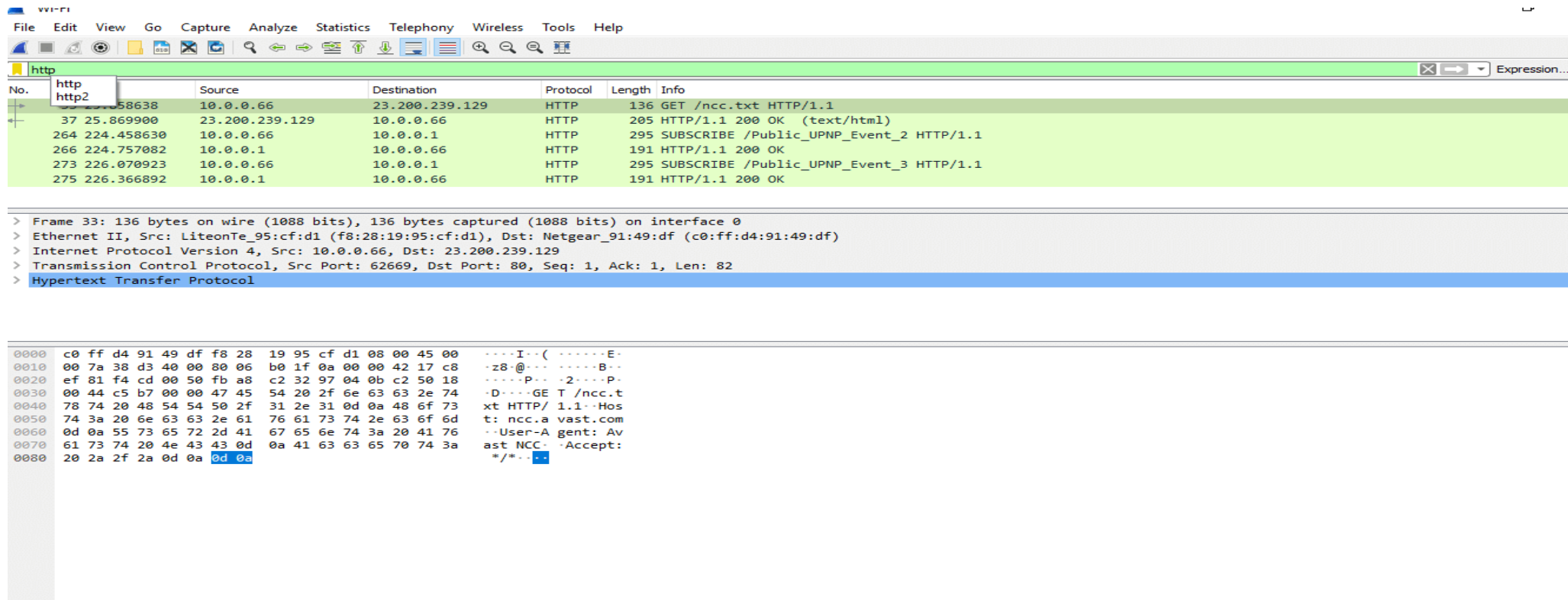
To filter packets, we need to apply some filtering commands in filter area. Following shows all packets with protocol TCP

## FILTER PACKETS IN WIRESHARK



Following shows all packets with http protocol

## FILTER PACKETS IN WIRESHARK



The image shows the Wireshark network protocol analyzer interface. The top menu bar includes File, Edit, View, Go, Capture, Analyze, Statistics, Telephony, Wireless, Tools, and Help. Below the menu is a toolbar with various icons. A filter bar at the top of the packet list shows the filter 'http'. The packet list displays several packets, with the first one selected. The details pane on the right shows the structure of the selected packet, including Ethernet II, Internet Protocol Version 4, Transmission Control Protocol, and Hypertext Transfer Protocol. The packet bytes pane at the bottom shows the raw data in hexadecimal and ASCII.

No.	Time	Source	Destination	Protocol	Length	Info
37	25.869900	10.0.0.66	23.200.239.129	HTTP	136	GET /ncc.txt HTTP/1.1
264	224.458630	10.0.0.66	10.0.0.1	HTTP	205	HTTP/1.1 200 OK (text/html)
266	224.757082	10.0.0.1	10.0.0.66	HTTP	295	SUBSCRIBE /Public_UPNP_Event_2 HTTP/1.1
273	226.070923	10.0.0.66	10.0.0.1	HTTP	191	HTTP/1.1 200 OK
275	226.366892	10.0.0.1	10.0.0.66	HTTP	295	SUBSCRIBE /Public_UPNP_Event_3 HTTP/1.1
				HTTP	191	HTTP/1.1 200 OK

Frame 33: 136 bytes on wire (1088 bits), 136 bytes captured (1088 bits) on interface 0  
> Ethernet II, Src: LiteonTe\_95:cf:d1 (f8:28:19:95:cf:d1), Dst: Netgear\_91:49:df (c0:ff:d4:91:49:df)  
> Internet Protocol Version 4, Src: 10.0.0.66, Dst: 23.200.239.129  
> Transmission Control Protocol, Src Port: 62669, Dst Port: 80, Seq: 1, Ack: 1, Len: 82  
> Hypertext Transfer Protocol

```
0000  c0 ff d4 91 49 df f8 28 19 95 cf d1 08 00 45 00  ....I..( .....E..
0010  00 7a 38 d3 40 00 80 06 b0 1f 0a 00 00 42 17 c8  -z8.@... ..B..
0020  ef 81 f4 cd 00 50 fb a8 c2 32 97 04 0b c2 50 18  ....P...2...P..
0030  00 44 c5 b7 00 00 47 45 54 20 2f 6e 63 63 2e 74  -D....GE T /ncc.t
0040  78 74 20 48 54 54 50 2f 31 2e 31 0d 0a 48 6f 73  xt HTTP/ 1.1..Hos
0050  74 3a 20 6e 63 63 2e 61 76 61 73 74 2e 63 6f 6d  t: ncc.a vast.com
0060  0d 0a 55 73 65 72 2d 41 67 65 6e 74 3a 20 41 76  ..User-A gent: Av
0070  61 73 74 20 4e 43 43 0d 0a 41 63 63 65 70 74 3a  ast NCC- -Accept:
0080  20 2a 2f 2a 0d 0a 0d 0a  /*/*...-..
```

## LIST OF FILTERS USED IN WIRESHARK

Filter command	Example	Description
ip.addr	ip.addr==192.168.0.12	It is used to specify the IP address as the source or the destination in the packet
protocol	http	This command filters based on the protocol
tcp.port	tcp.port==443	Filtering based on the port number
tcp contains the filter	tcp contains google	It is used to display the packets which contain such words.

# HOW TO PREVENT MITM

- 1. MITM Attack Prevention Measures
- 2. Encryption and MITM Defense
- 3. Secure Communication Protocols
- 4. Network Monitoring for MITM Detection
- 5. Two-Factor Authentication and MITM Resilience



Thank  
you