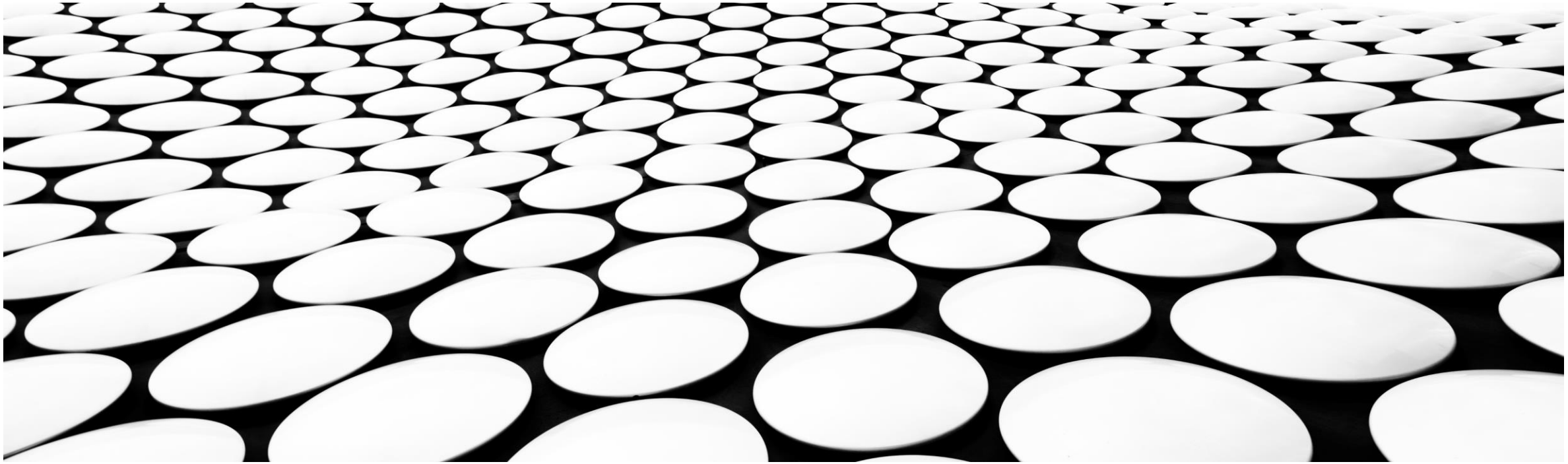
SKILLSBUILD FOR COLLEGES

EDUNET FOUNDATION



Edunet Foundation

Registered Trust

Recognized under sections 12AA and 80G of Income Tax Act.

GuideStar Verified

for transparency

Great Place To Work Certified

Special Consultative Status

with the United Nations

Goal

Creation of educational networks and sustainable communities

Focus

4th & 5th 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

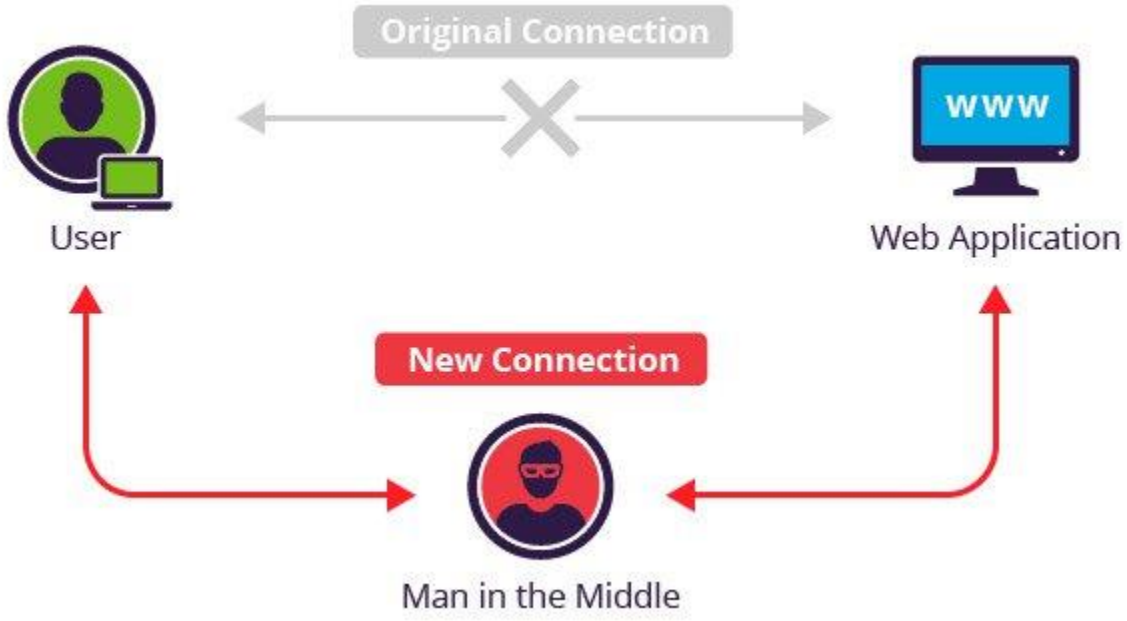
MITM

MITM ATTACK & ARP SPOOFING

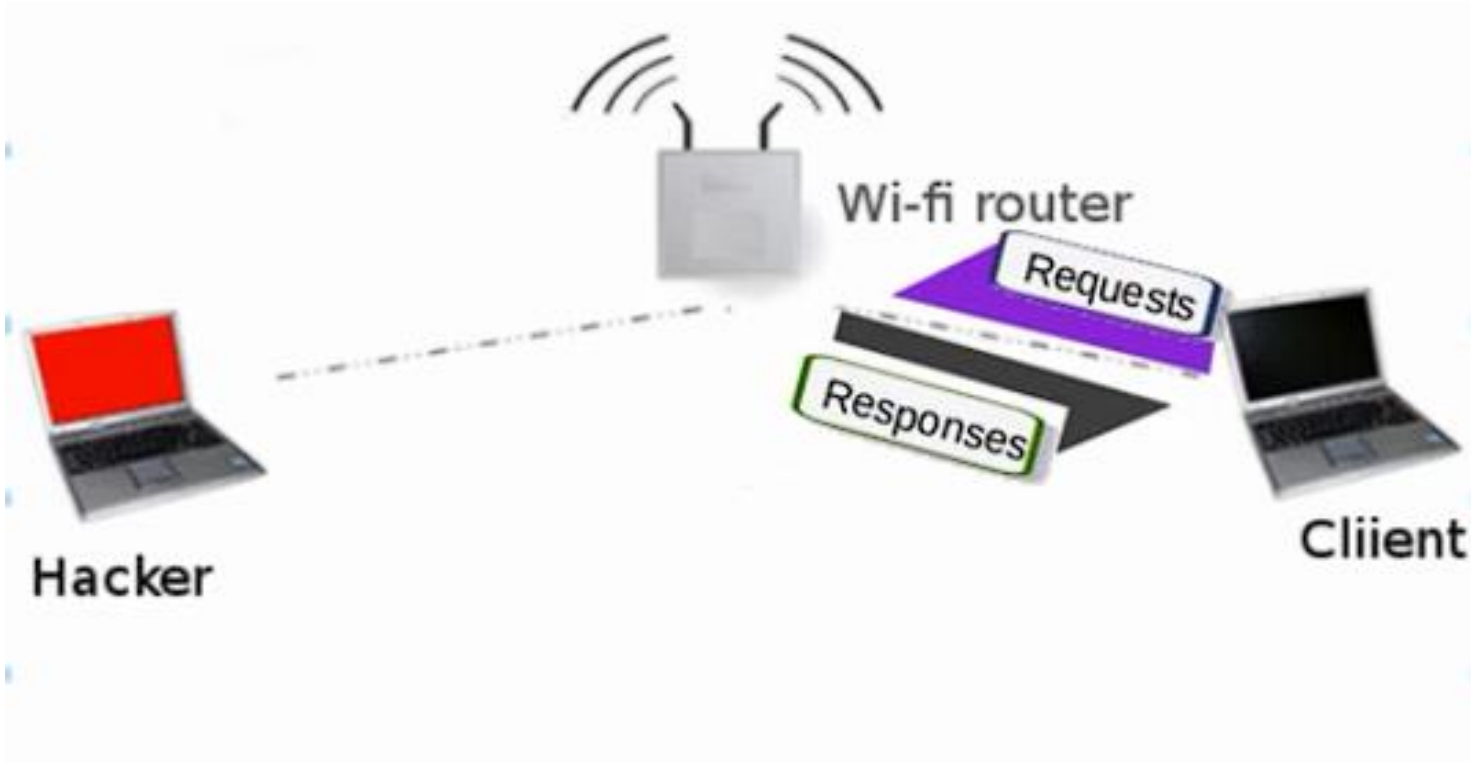
This is one of the most dangerous and effective attacks that can be used, it is used to redirect packets to and from any client to our device, and since we have the network key, we can read/modify/drop these packets. This allows us to launch very powerful attacks.

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

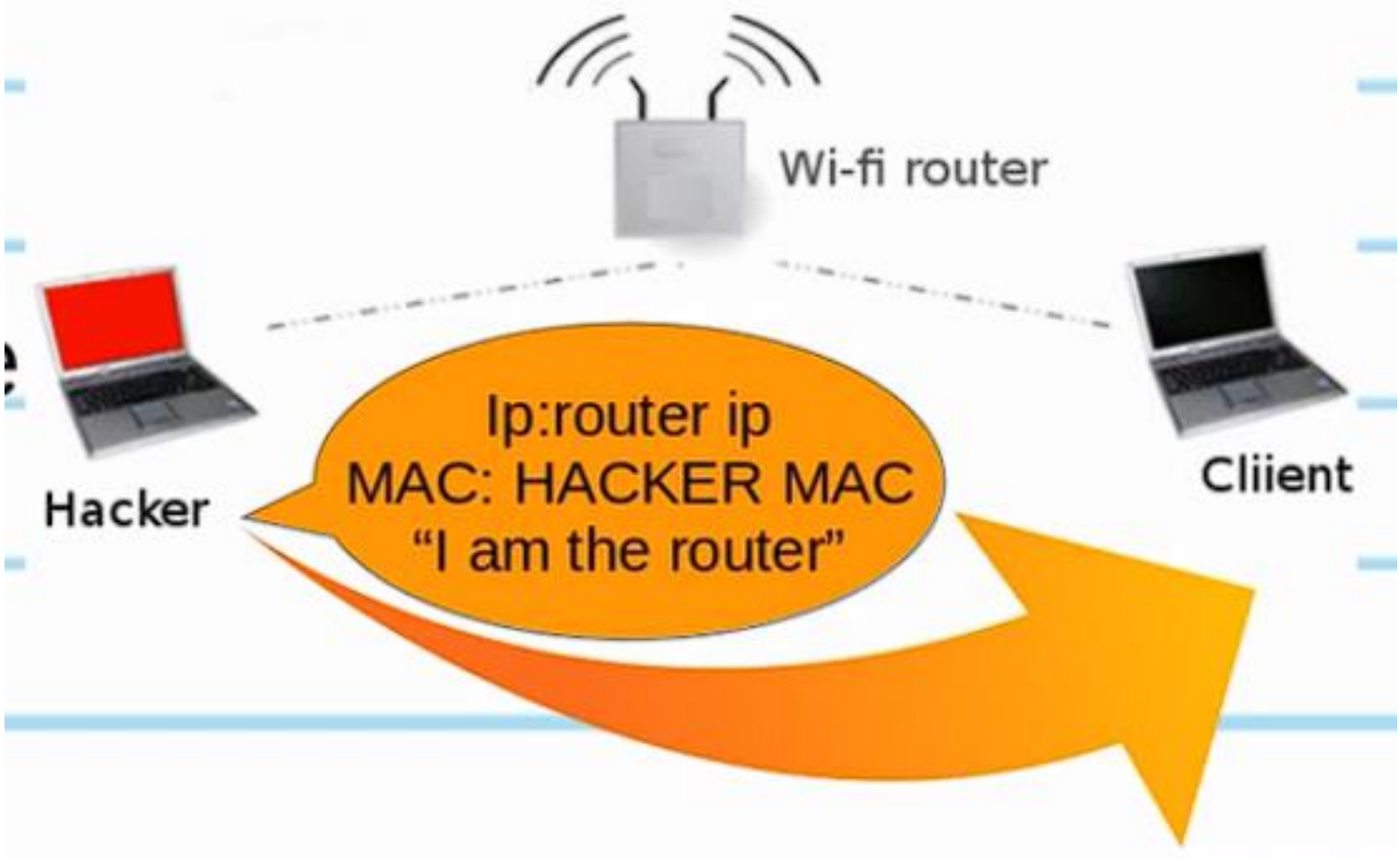
MAN-IN-THE-MIDDLE ATTACK



MAN IN THE MIDDLE ATTACKS ARP POISONING



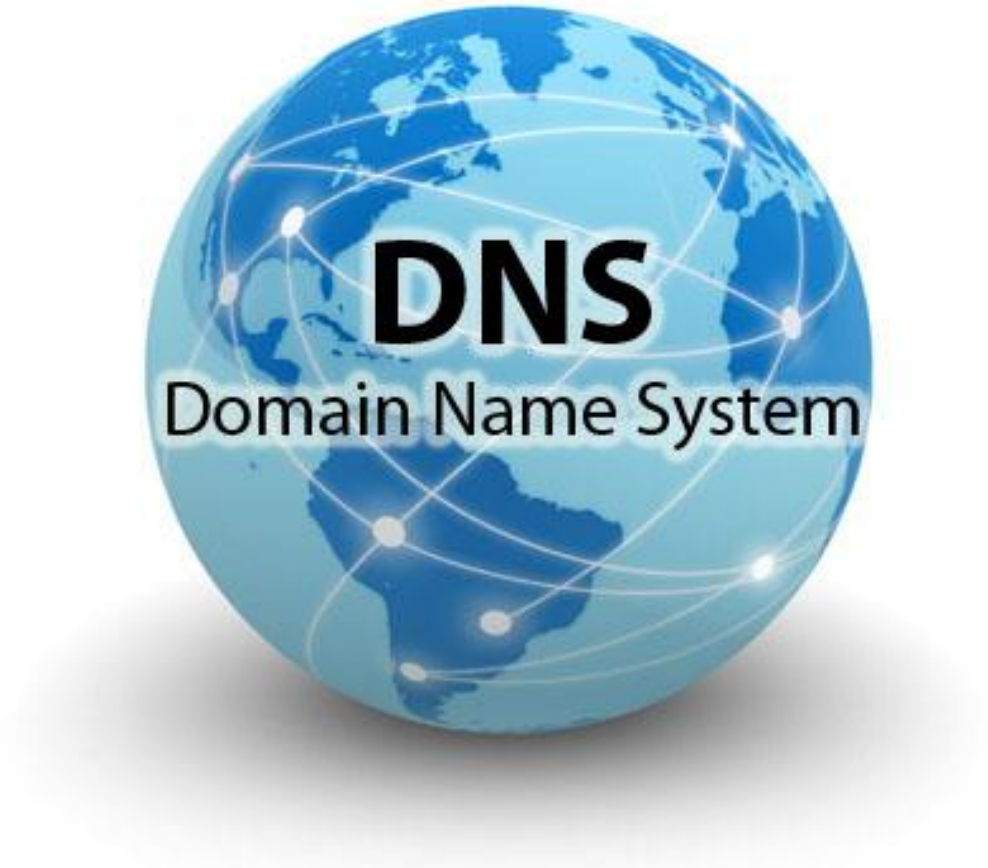
MAN IN THE MIDDLE ATTACKS ARP POISONING



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

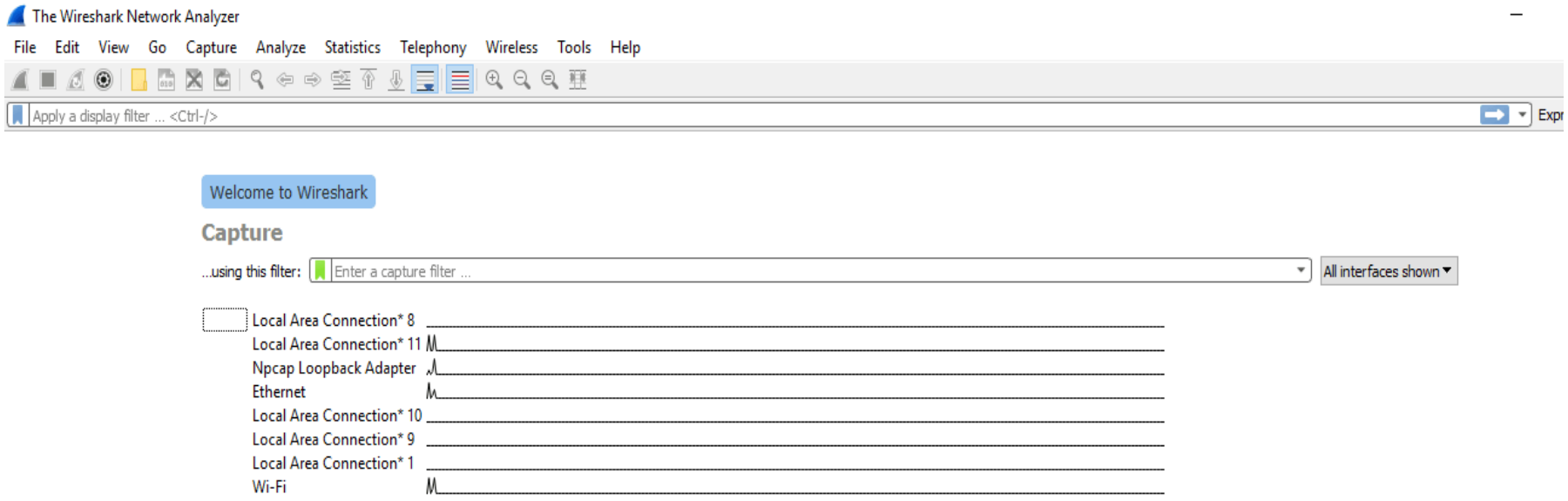
1. Wireshark is the widely-used network protocol analyzer
2. It is an application that captures packets from a network connection
3. It is commonly called as a sniffer, network protocol analyzer, and network analyzer

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) .

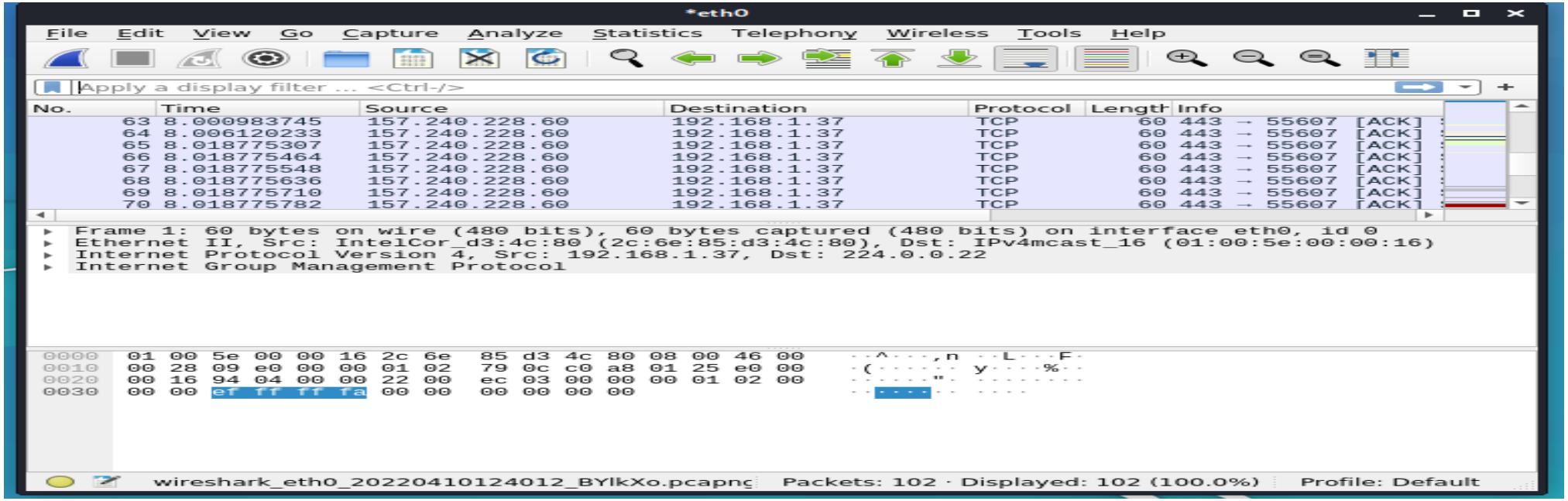
STARTING WIRESHARK



CAPTURE PACKETS IN WIRESHARK

Open Wireshark and select NIC(Network Interface) .

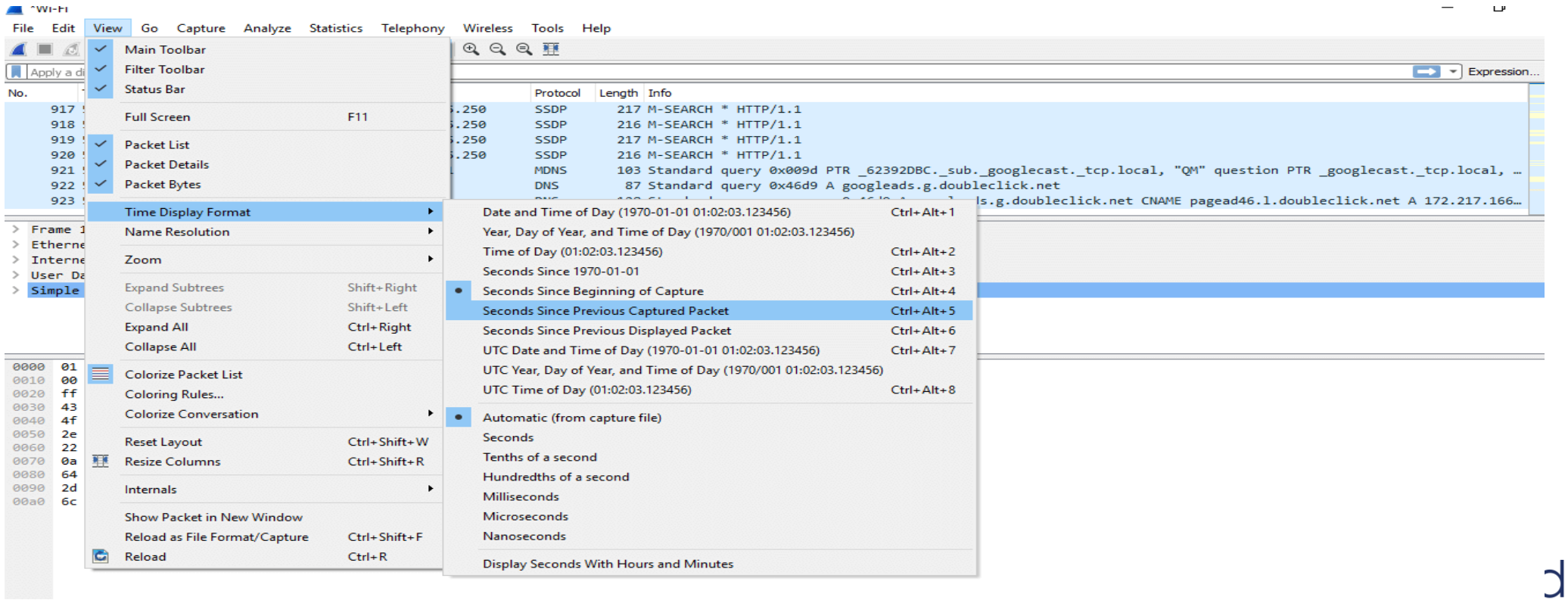
Click on start button



edunet foundation

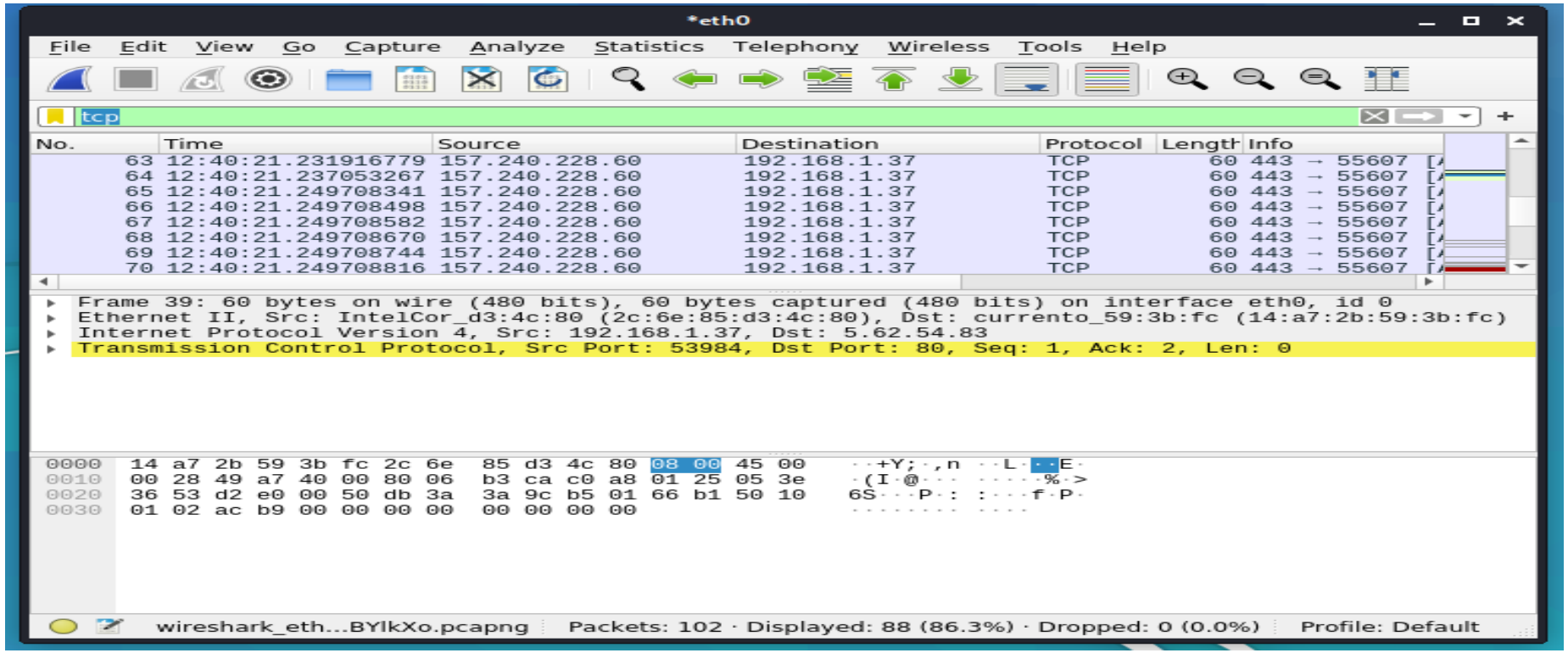
We may also modify the interface view using the view option on the menu bar. The number of items in the view menu can be changed. You can also enable and disable any option based on your needs.

WIRESHARK VIEW



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

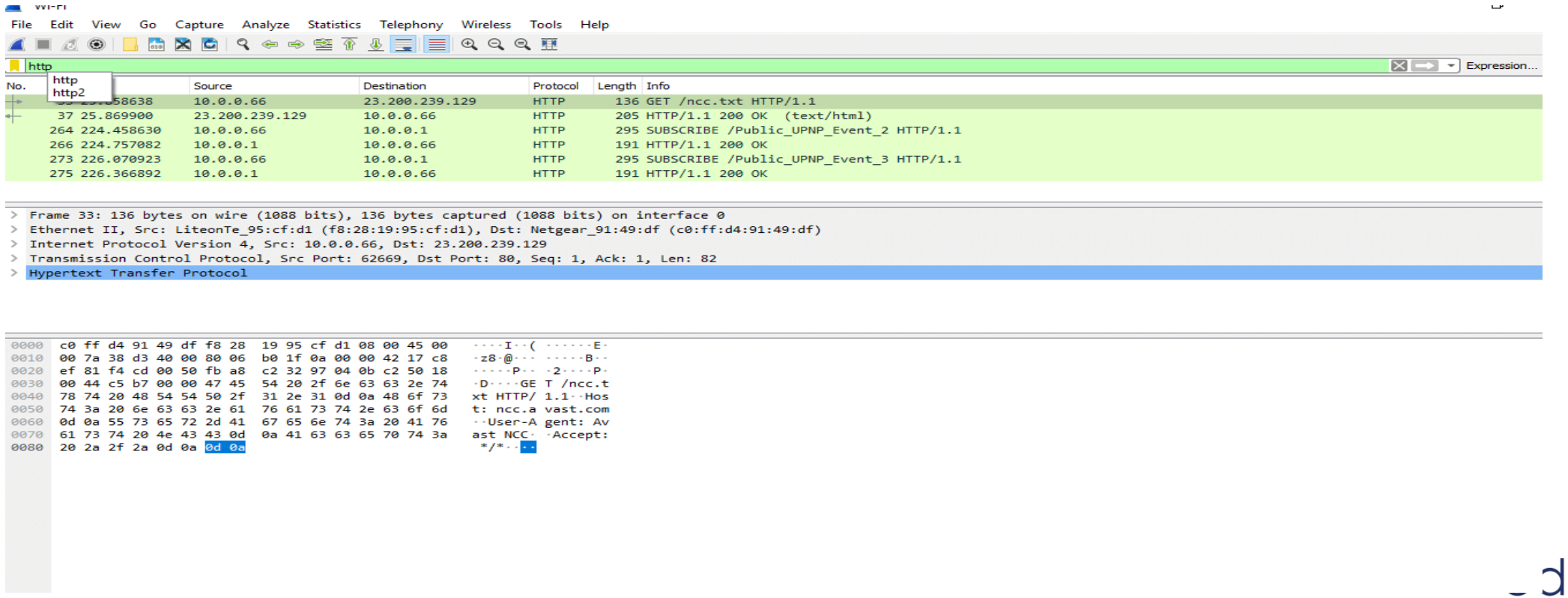
FILTER PACKETS IN WIRESHARK



edunet foundation

Following shows all packets with http protocol

FILTER PACKETS IN WIRESHARK



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