# Task 3: Network Packet Sniffing and Analysis

Any action intended to safeguard the integrity and usefulness of your data and network is known as network security. Network security is the practice of protecting a computer network from unauthorized access, misuse, or attacks. It involves using tools, technologies, policies and procedures to ensure the confidentiality, integrity, and availability of systems and data within the network to ensure that data traveling over the network is safe and secure, keeping sensitive information away from hackers and other threats.

## How Does Network Security Work?

Network security uses several layers of protection, both at the edge of the network and within it. Each layer has rules and controls that determine who can access network resources. People who are allowed access can use the network safely, but those who try to harm it with attacks or other threats are stopped from doing so.

The basic principle of network security is protecting huge stored data and networks in layers that ensure the enforcement of rules and regulations that have to be acknowledged before performing any activity on the data. These levels are:

- **Physical Network Security:** This is the most basic level that includes protecting the data and network through unauthorized personnel from acquiring control over the confidentiality of the network. The same can be achieved by using devices like biometric systems.
- **Technical Network Security:** It primarily focuses on protecting the data stored in the network or data involved in transitions through the network. This type serves two purposes. One is protected from unauthorized users, and the other is protected from malicious activities.
- **Administrative Network Security:** This level of network security protects user behavior like how the permission has been granted and how the authorization process takes place. This also ensures the level of sophistication the network might need for protecting it through all the attacks. This level also suggests necessary amendments that have to be done to the infrastructure.

## 1.NETWORK THREATS:

**Network threats** are any malicious activities or events that target the integrity, confidentiality, or availability of data on a computer network. They can come from external attackers or internal users and can cause serious damage or data breaches.

## 1. Malware (Malicious Software)

Malware spreads through networks and can damage or steal data.

- **Types:**
  - **Virus** – Attaches to legitimate files and spreads.
  - **Worm** – Self-replicating and spreads without user interaction.
  - **Trojan Horse** – Disguises itself as a legitimate program.
  - **Ransomware** – Locks data until a ransom is paid.
  - **Spyware** – Monitors user activity and steals sensitive info.

## 2. Phishing Attacks

- Fake emails or websites trick users into revealing sensitive information like login credentials or credit card numbers.
- Often used to initiate **identity theft** or unauthorized access.

## 3. Denial of Service (DoS) & Distributed DoS (DDoS)

- Floods the network or servers with traffic, making them unavailable to legitimate users.
- DDoS uses multiple compromised systems (botnets) to launch the attack.

## 4. Man-in-the-Middle (MitM) Attacks

- The attacker secretly intercepts and possibly alters communication between two parties.
- Common in unsecured public Wi-Fi environments.

### 5. Packet Sniffing / Eavesdropping

- Attackers capture network traffic to read sensitive data in transit.
- Especially dangerous on unencrypted networks.

### 6. Unauthorized Access / Hacking

- Gaining access to network resources without permission.
- Can be done through password guessing, exploiting software vulnerabilities, etc.

### 7. SQL Injection

- Inserting malicious SQL queries into input fields to gain unauthorized access to a database.

### 8. Insider Threats

- Employees or trusted users misuse access to cause damage or steal data.

### 9. Zero-Day Exploits

- Attacks that exploit unknown or unpatched software vulnerabilities.

### 10. DNS Spoofing / Poisoning

- Redirects traffic from legitimate websites to fake ones by corrupting DNS data.

**How to Prevent Network Threats:**

- Use **firewalls and intrusion detection/prevention systems (IDS/IPS)**
- Keep software and systems **updated and patched**
- Use **strong encryption** for data transmission (e.g., HTTPS, VPN)
- Educate users on **phishing and social engineering**
- Implement **access control** and **multi-factor authentication**
- Regularly **monitor and audit** network activity.

## 2. SECURITY MEASURES AND WHY?

## 1. Firewalls:

***What it does:***

- Monitors and filters incoming/outgoing network traffic based on rules.

***Why it's used:***

- Blocks unauthorized access and malicious traffic.
- Acts as a first line of defense against hackers.

## 2. Intrusion Detection & Prevention Systems (IDS/IPS):

***What it does:***

- **IDS**: Monitors network for suspicious activity.
- **IPS**: Blocks threats in real time.

***Why it's used:***

- Detects hacking attempts, malware, and abnormal behavior.
- Prevents breaches before damage is done.

## 3. Authentication and Access Control:

***What it does:***

- Requires users to prove identity (e.g., passwords, biometrics, MFA).
- Controls who can access what on the network.

***Why it's used:***

- Prevents unauthorized users from accessing sensitive systems or data.
- Limits internal risks and enforces role-based access.

## 4. Encryption (SSL/TLS, VPN, etc.):

***What it does:***

- Scrambles data so only authorized parties can read it.
- Used in emails, files, web traffic (HTTPS), etc.

***Why it's used:***

- Protects data confidentiality during transmission.
- Prevents eavesdropping and data theft.

## 5. Regular Updates and Patch Management:

***What it does:***

- Keeps operating systems, software, and hardware up to date.

***Why it's used:***

- Fixes security vulnerabilities that hackers could exploit.
- Closes known loopholes.

## 6. Network Monitoring:

***What it does:***

- Continuously checks traffic, logs, and system behavior.

***Why it's used:***

- Detects abnormal activities quickly.
- Helps in identifying and responding to threats early.

## 7. Security Policies and Training:

***What it does:***

- Teaches users how to behave safely online.
- Sets rules for passwords, data use, email, etc.

***Why it's used:***

- Reduces human error and insider threats.
- Builds a security-aware culture.

## 8. Antivirus and Anti-malware Tools:

*What it does:*

- Scans systems for known malware and removes it.

***Why it's used:***

- Prevents damage from viruses, worms, ransomware, etc.
- Essential for endpoint protection.

## 9. Physical Security:

***What it does:***

- Protects servers, routers, and network hardware with locks, cameras, etc.

***Why it's used:***

- Prevents physical tampering or theft that could lead to a security breach.

## 10. Backup and Disaster Recovery Plans:

***What it does:***

- Regularly saves copies of data and system configurations.

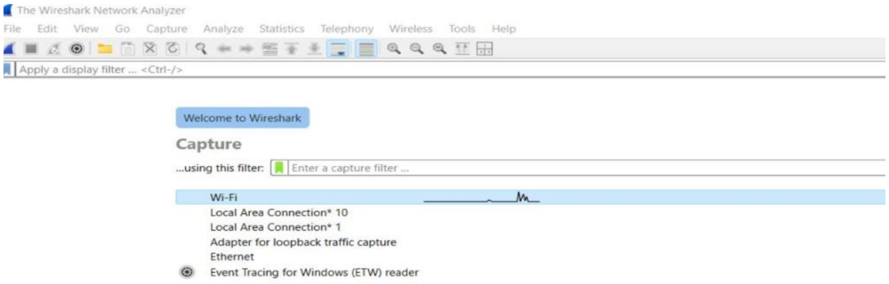
***Why it's used:***

- Ensures quick recovery after ransomware attacks, data loss, or system failures.

## 3. Descriptions of the Traffic captured with Wireshark:

### Step 1: Install and Open Wireshark

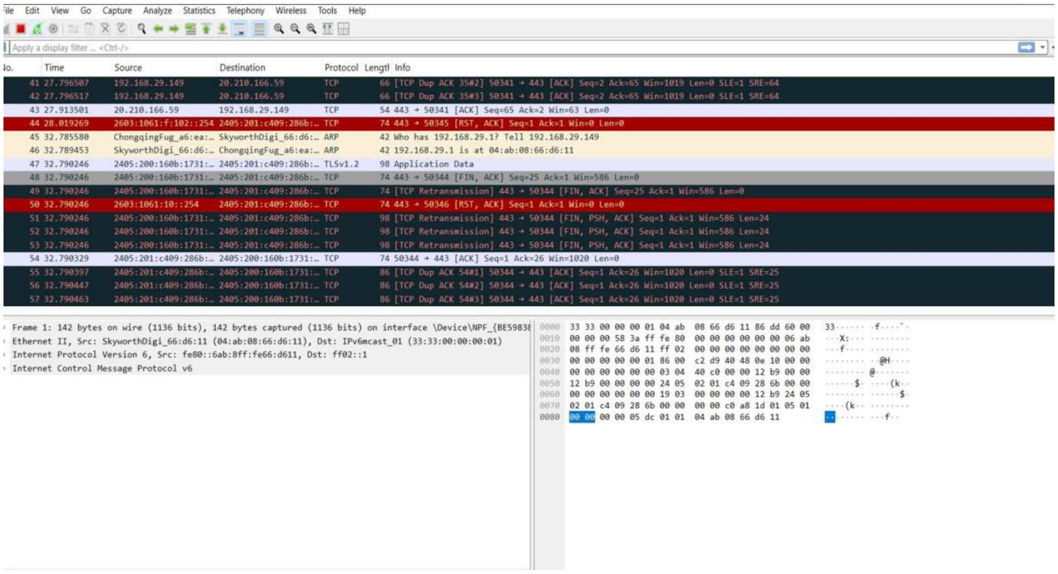
1. Download from https://www.wireshark.org.
2. Install and run it **as Administrator** (important for full access).
3. You’ll see a list of available **network interfaces** (e.g., Wi-Fi, Ethernet).


The Wireshark Network Analyzer
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
Welcome to Wireshark
Capture
...using this filter:
Enter a capture filter ...

Wi-Fi
Local Area Connection* 10
Local Area Connection* 1
Adapter for loopback traffic capture
Ethernet
Event Tracing for Windows (ETW) reader

### Step 2: Start Packet Capture

1. Select your **active interface** (the one with live traffic — usually Wi-Fi or Ethernet).
2. Click the **blue shark fin icon**  at the top-left to start capturing.
3. Wireshark starts showing live packet data in real time.


File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>

```
No.   Time       Source                Destination           Protocol Length Info
 41 27.796507  192.168.29.149        20.210.166.59         TCP      66 [TCP Dup ACK 35#2] 50341 → 443 [ACK] Seq=2 Ack=65 Win=1019 Len=0 SLE=1 SRE=64
 42 27.796517  192.168.29.149        20.210.166.59         TCP      66 [TCP Dup ACK 35#3] 50341 → 443 [ACK] Seq=2 Ack=65 Win=1019 Len=0 SLE=1 SRE=64
 43 27.913501  20.210.166.59         192.168.29.149        TCP      54 443 → 50341 [ACK] Seq=65 Ack=2 Win=63 Len=0
 44 28.019269  2603:1061:f:102::254  2405:201:c409:286b:…  TCP      74 443 → 50345 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
 45 32.785580  ChongqingFug_a6:ea:…  SkyworthDigi_66:d6:…  ARP      42 Who has 192.168.29.1? Tell 192.168.29.149
 46 32.789453  SkyworthDigi_66:d6:…  ChongqingFug_a6:ea:…  ARP      42 192.168.29.1 is at 04:ab:08:66:d6:11
 47 32.790246  2405:200:160b:1731:…  2405:201:c409:286b:…  TLSv1.2  98 Application Data
 48 32.790246  2405:200:160b:1731:…  2405:201:c409:286b:…  TCP      74 443 → 50344 [FIN, ACK] Seq=25 Ack=1 Win=586 Len=0
 49 32.790246  2405:200:160b:1731:…  2405:201:c409:286b:…  TCP      74 [TCP Retransmission] 443 → 50344 [FIN, ACK] Seq=25 Ack=1 Win=586 Len=0
 50 32.790246  2603:1061:10::254     2405:201:c409:286b:…  TCP      74 443 → 50346 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
 51 32.790246  2405:200:160b:1731:…  2405:201:c409:286b:…  TCP      98 [TCP Retransmission] 443 → 50344 [FIN, PSH, ACK] Seq=1 Ack=1 Win=586 Len=24
 52 32.790246  2405:200:160b:1731:…  2405:201:c409:286b:…  TCP      98 [TCP Retransmission] 443 → 50344 [FIN, PSH, ACK] Seq=1 Ack=1 Win=586 Len=24
 53 32.790246  2405:200:160b:1731:…  2405:201:c409:286b:…  TCP      98 [TCP Retransmission] 443 → 50344 [FIN, PSH, ACK] Seq=1 Ack=1 Win=586 Len=24
 54 32.790329  2405:201:c409:286b:…  2405:200:160b:1731:…  TCP      74 50344 → 443 [ACK] Seq=1 Ack=26 Win=1020 Len=0
 55 32.790397  2405:201:c409:286b:…  2405:200:160b:1731:…  TCP      86 [TCP Dup ACK 54#1] 50344 → 443 [ACK] Seq=1 Ack=26 Win=1020 Len=0 SLE=1 SRE=25
 56 32.790447  2405:201:c409:286b:…  2405:200:160b:1731:…  TCP      86 [TCP Dup ACK 54#2] 50344 → 443 [ACK] Seq=1 Ack=26 Win=1020 Len=0 SLE=1 SRE=25
 57 32.790463  2405:201:c409:286b:…  2405:200:160b:1731:…  TCP      86 [TCP Dup ACK 54#3] 50344 → 443 [ACK] Seq=1 Ack=26 Win=1020 Len=0 SLE=1 SRE=25
```

```
Frame 1: 142 bytes on wire (1136 bits), 142 bytes captured (1136 bits) on interface \Device\NPF_{BE5983
Ethernet II, Src: SkyworthDigi_66:d6:11 (04:ab:08:66:d6:11), Dst: IPv6mcast_01 (33:33:00:00:00:01)
Internet Protocol Version 6, Src: fe80::6ab:8ff:fe66:d611, Dst: ff02::1
Internet Control Message Protocol v6
```

```
0000  33 33 00 00 00 01 04 ab  08 66 d6 11 86 dd 60 00   33······ ·f····`·
0010  00 00 00 58 3a ff fe 80  00 00 00 00 00 00 06 ab   ···X:··· ········
0020  08 ff fe 66 d6 11 ff 02  00 00 00 00 00 00 00 00   ···f···· ········
0030  00 00 00 00 00 01 86 00  c2 d9 40 48 0e 10 00 00   ········ ··@H····
0040  00 00 00 00 00 00 03 04  40 c0 00 00 12 b9 00 00   ········ @·······
0050  12 b9 00 00 00 00 24 05  02 01 c4 09 28 6b 00 00   ······$· ····(k··
0060  00 00 00 00 00 00 19 03  00 00 00 00 12 b9 24 05   ········ ······$·
0070  02 01 c4 09 28 6b 00 00  00 00 c0 a8 1d 01 05 01   ····(k·· ········
0080  00 00 00 00 05 dc 01 01  04 ab 08 66 d6 11         ········ ···f··
```

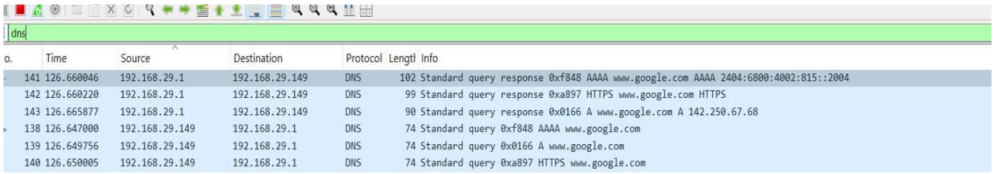
### Step 3: Generate Traffic

To capture meaningful data:

- Open a browser and visit websites like http://example.com, https://google.com.
- Use ping or nslookup in the command prompt:
- ping google.com
- nslookup example.com

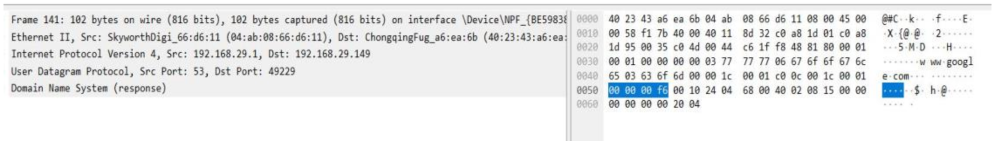
### Step 4: Apply Display Filters to Identify Traffic Types

| Protocol | Filter | What It Shows |
|---|---|---|
| **HTTP** | http | Web requests (GET/POST), unencrypted data |
| **DNS** | dns | Domain-to-IP lookups |
| **TCP** | tcp | Reliable transport layer traffic |
| **UDP** | udp | Lightweight, fast connections (e.g., DNS) |
| **ICMP** | icmp | Ping and diagnostic packets |
| **ARP** | arp | Local IP-to-MAC mapping |



dns

```
o.    Time        Source          Destination     Protocol Lengtl Info
  141 126.660046  192.168.29.1    192.168.29.149  DNS       102 Standard query response 0xf848 AAAA www.google.com AAAA 2404:6800:4002:815::2004
  142 126.660220  192.168.29.1    192.168.29.149  DNS        99 Standard query response 0xa897 HTTPS www.google.com HTTPS
  143 126.665877  192.168.29.1    192.168.29.149  DNS        90 Standard query response 0x0166 A www.google.com A 142.250.67.68
  138 126.647000  192.168.29.149  192.168.29.1    DNS        74 Standard query 0xf848 AAAA www.google.com
  139 126.649756  192.168.29.149  192.168.29.1    DNS        74 Standard query 0x0166 A www.google.com
  140 126.650005  192.168.29.149  192.168.29.1    DNS        74 Standard query 0xa897 HTTPS www.google.com
```



```
Frame 141: 102 bytes on wire (816 bits), 102 bytes captured (816 bits) on interface \Device\NPF_{BE5983
Ethernet II, Src: SkyworthDigi_66:d6:11 (04:ab:08:66:d6:11), Dst: ChongqingFug_a6:ea:6b (40:23:43:a6:ea:
Internet Protocol Version 4, Src: 192.168.29.1, Dst: 192.168.29.149
User Datagram Protocol, Src Port: 53, Dst Port: 49229
Domain Name System (response)
```

```
0000  40 23 43 a6 ea 6b 04 ab  08 66 d6 11 08 00 45 00   @#C··k·· ·f····E·
0010  00 58 f1 7b 40 00 40 11  8d 32 c0 a8 1d 01 c0 a8   ·X·{@·@· ·2······
0020  1d 95 00 35 c0 4d 00 44  c6 1f f8 48 81 80 00 01   ···5·M·D ···H····
0030  00 01 00 00 00 00 03 77  77 77 06 67 6f 6f 67 6c   ·······w ww·googl
0040  65 03 63 6f 6d 00 00 1c  00 01 c0 0c 00 1c 00 01   e·com··· ········
0050  00 00 00 f6 00 10 24 04  68 00 40 02 08 15 00 00   ······$· h·@·····
0060  00 00 00 00 20 04                                  ···· ·
```

**Step 5: Analyze Packets**

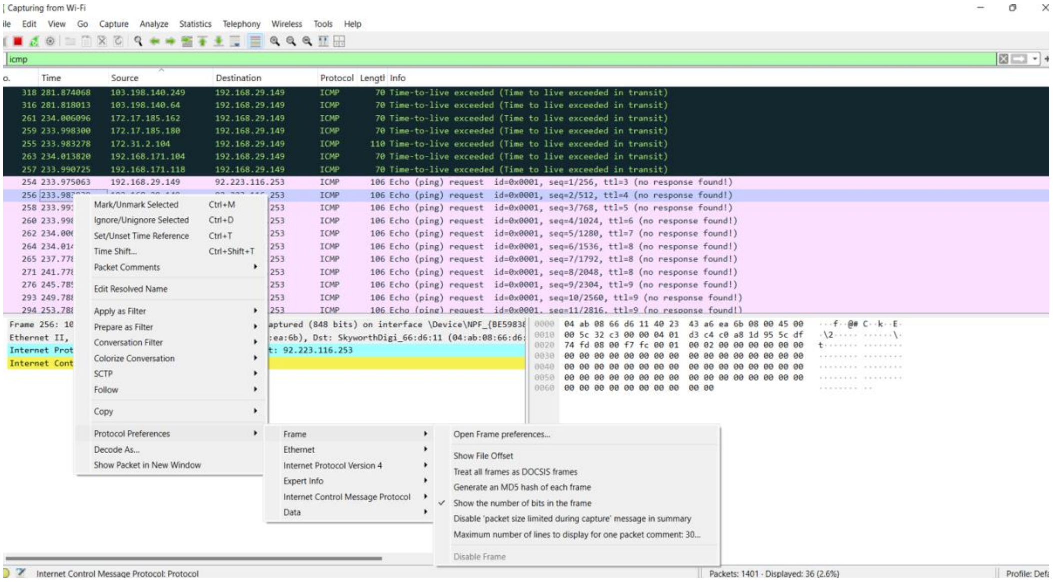
Click any packet to view details in the lower panel:

- **Frame**: Packet size, time
- **Ethernet / IP**: Source and destination IP addresses
- **Protocol** (TCP/UDP/ICMP)
- **Payload**: Application data (like URLs, hostnames, certificates, etc.)

For example, with http, you can see the full request:

GET /index.html HTTP/1.1

Host: example.com

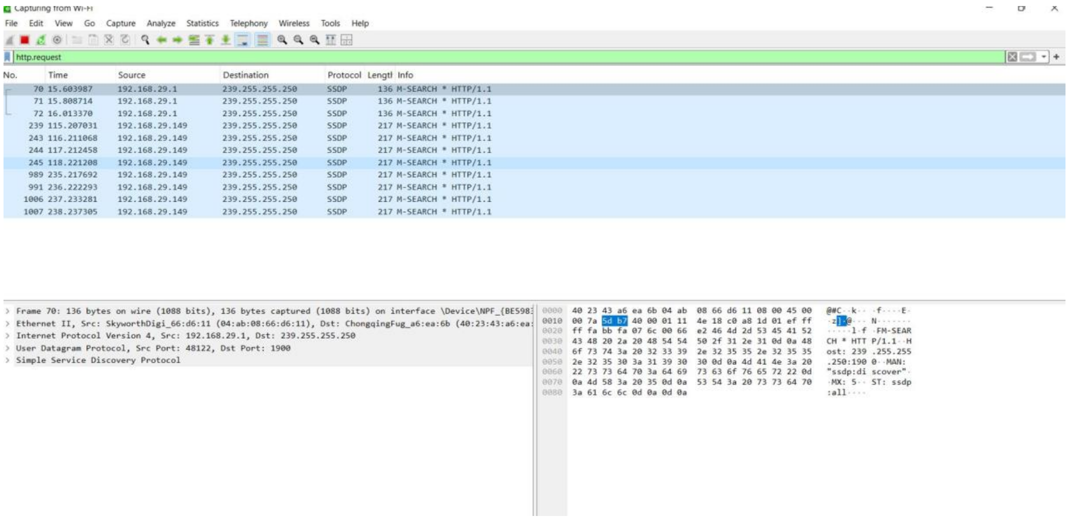

Capturing from Wi-Fi
ile Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Mark/Unmark Selected Ctrl+M
Ignore/Unignore Selected Ctrl+D
Set/Unset Time Reference Ctrl+T
Time Shift... Ctrl+Shift+T
Packet Comments
Edit Resolved Name
Apply as Filter
Prepare as Filter
Conversation Filter
Colorize Conversation
SCTP
Follow
Copy
Protocol Preferences
Decode As...
Show Packet in New Window
Frame
Ethernet
Internet Protocol Version 4
Expert Info
Internet Control Message Protocol
Data
Open Frame preferences...
Show File Offset
Treat all frames as DOCSIS frames
Generate an MD5 hash of each frame
✓ Show the number of bits in the frame
Disable 'packet size limited during capture' message in summary
Maximum number of lines to display for one packet comment: 30...
Disable Frame
Profile: Defa

```
icmp

o.   Time        Source           Destination      Protocol Lengtl Info
 318 281.874068  103.198.140.249  192.168.29.149   ICMP      70 Time-to-live exceeded (Time to live exceeded in transit)
 316 281.818013  103.198.140.64   192.168.29.149   ICMP      70 Time-to-live exceeded (Time to live exceeded in transit)
 261 234.006096  172.17.185.162   192.168.29.149   ICMP      70 Time-to-live exceeded (Time to live exceeded in transit)
 259 233.998300  172.17.185.180   192.168.29.149   ICMP      70 Time-to-live exceeded (Time to live exceeded in transit)
 255 233.983278  172.31.2.104     192.168.29.149   ICMP     110 Time-to-live exceeded (Time to live exceeded in transit)
 263 234.013820  192.168.171.104  192.168.29.149   ICMP      70 Time-to-live exceeded (Time to live exceeded in transit)
 257 233.990725  192.168.171.118  192.168.29.149   ICMP      70 Time-to-live exceeded (Time to live exceeded in transit)
 254 233.975063  192.168.29.149   92.223.116.253   ICMP     106 Echo (ping) request  id=0x0001, seq=1/256, ttl=3 (no response found!)
 256 233.98                                  253   ICMP     106 Echo (ping) request  id=0x0001, seq=2/512, ttl=4 (no response found!)
 258 233.99                                  253   ICMP     106 Echo (ping) request  id=0x0001, seq=3/768, ttl=5 (no response found!)
 260 233.99                                  253   ICMP     106 Echo (ping) request  id=0x0001, seq=4/1024, ttl=6 (no response found!)
 262 234.00                                  253   ICMP     106 Echo (ping) request  id=0x0001, seq=5/1280, ttl=7 (no response found!)
 264 234.01                                  253   ICMP     106 Echo (ping) request  id=0x0001, seq=6/1536, ttl=8 (no response found!)
 265 237.77                                  253   ICMP     106 Echo (ping) request  id=0x0001, seq=7/1792, ttl=8 (no response found!)
 271 241.77                                  253   ICMP     106 Echo (ping) request  id=0x0001, seq=8/2048, ttl=8 (no response found!)
 276 245.78                                  253   ICMP     106 Echo (ping) request  id=0x0001, seq=9/2304, ttl=9 (no response found!)
 293 249.78                                  253   ICMP     106 Echo (ping) request  id=0x0001, seq=10/2560, ttl=9 (no response found!)
 294 253.78                                  253   ICMP     106 Echo (ping) request  id=0x0001, seq=11/2816, ttl=9 (no response found!)

Frame 256: 10                aptured (848 bits) on interface \Device\NPF_{BE5983
Ethernet II,                 :ea:6b), Dst: SkyworthDigi_66:d6:11 (04:ab:08:66:d6:
Internet Prot                t: 92.223.116.253
Internet Cont

0000  04 ab 08 66 d6 11 40 23  43 a6 ea 6b 08 00 45 00   ···f··@# C··k··E·
0010  00 5c 32 c3 00 00 04 01  d3 c4 c0 a8 1d 95 5c df   ·\2····· ······\·
0020  74 fd 08 00 f7 fc 00 01  00 02 00 00 00 00 00 00   t······· ········
0030  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ········ ········
0040  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ········ ········
0050  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ········ ········
0060  00 00 00 00 00 00 00 00  00 00                     ········ ··

Internet Control Message Protocol: Protocol        Packets: 1401 · Displayed: 36 (2.6%)
```

**Step 6: Identify Suspicious or Malicious Traffic**

| **Behavior** | **How to Detect** | **What It Might Indicate** |
|---|---|---|
| □ Repeated SYN packets | Filter: tcp.flags.syn == 1 && tcp.flags.ack == 0 | Port scanning |
| □ High ICMP volume | Filter: icmp | Ping flood or network scan |
| □ Unknown domain queries | Filter: dns | Suspicious DNS tunneling |
| □ Fake ARP responses | Filter: arp | ARP spoofing (MITM attack) |

| Behavior | How to Detect | What It Might Indicate |
|---|---|---|
| □ Data to port 4444, 6667, etc. | Filter: tcp.port == 4444 | Malware connection / backdoor |


Capturing from Wi-Fi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

http.request

```
No.   Time        Source          Destination      Protocol Lengtl Info
   70 15.603987   192.168.29.1    239.255.255.250  SSDP     136 M-SEARCH * HTTP/1.1
   71 15.808714   192.168.29.1    239.255.255.250  SSDP     136 M-SEARCH * HTTP/1.1
   72 16.013370   192.168.29.1    239.255.255.250  SSDP     136 M-SEARCH * HTTP/1.1
  239 115.207031  192.168.29.149  239.255.255.250  SSDP     217 M-SEARCH * HTTP/1.1
  243 116.211068  192.168.29.149  239.255.255.250  SSDP     217 M-SEARCH * HTTP/1.1
  244 117.212458  192.168.29.149  239.255.255.250  SSDP     217 M-SEARCH * HTTP/1.1
  245 118.221208  192.168.29.149  239.255.255.250  SSDP     217 M-SEARCH * HTTP/1.1
  989 235.217692  192.168.29.149  239.255.255.250  SSDP     217 M-SEARCH * HTTP/1.1
  991 236.222293  192.168.29.149  239.255.255.250  SSDP     217 M-SEARCH * HTTP/1.1
 1006 237.233281  192.168.29.149  239.255.255.250  SSDP     217 M-SEARCH * HTTP/1.1
 1007 238.237305  192.168.29.149  239.255.255.250  SSDP     217 M-SEARCH * HTTP/1.1
```

```
> Frame 70: 136 bytes on wire (1088 bits), 136 bytes captured (1088 bits) on interface \Device\NPF_{BE598:
> Ethernet II, Src: SkyworthDigi_66:d6:11 (04:ab:08:66:d6:11), Dst: ChongqingFug_a6:ea:6b (40:23:43:a6:ea:
> Internet Protocol Version 4, Src: 192.168.29.1, Dst: 239.255.255.250
> User Datagram Protocol, Src Port: 48122, Dst Port: 1900
> Simple Service Discovery Protocol
```

```
0000  40 23 43 a6 ea 6b 04 ab  08 66 d6 11 08 00 45 00   @#C··k·· ·f····E·
0010  00 7a 5d b7 40 00 01 11  4e 18 c0 a8 1d 01 ef ff   ·z]·@··· N·······
0020  ff fa bb fa 07 6c 00 66  e2 46 4d 2d 53 45 41 52   ·····l·f ·FM-SEAR
0030  43 48 20 2a 20 48 54 54  50 2f 31 2e 31 0d 0a 48   CH * HTT P/1.1··H
0040  6f 73 74 3a 20 32 33 39  2e 32 35 35 2e 32 35 35   ost: 239 .255.255
0050  2e 32 35 30 3a 31 39 30  30 0d 0a 4d 41 4e 3a 20   .250:190 0··MAN: 
0060  22 73 73 64 70 3a 64 69  73 63 6f 76 65 72 22 0d   "ssdp:di scover"·
0070  0a 4d 58 3a 20 35 0d 0a  53 54 3a 20 73 73 64 70   ·MX: 5·· ST: ssdp
0080  3a 61 6c 6c 0d 0a 0d 0a                            :all····
```

**Step 7: Save and Export**

- **Save Capture**: File → Save As → .pcapng for future analysis
- **Export Summary**: File → Export Packet Dissections → As CSV or plain text

**Step 8: Stop Capture**

Click the **red square (■)** at the top to stop capturing when done.

## 4.How Basic Security Measures Protect the Network

**Basic security measures are the** first line of defense **in network protection. Though they may seem simple, they play a crucial role in** preventing unauthorized access**,** detecting threats early**, and** maintaining data integrity and confidentiality**.**

### *1. Firewalls*

- **Function:** Block or allow traffic based on predefined rules.
- **Protection:** Prevents **unauthorized access** to or from private networks.
- **Example:** A firewall can block incoming traffic from a suspicious IP address trying to access your system.

### *2. Changing Default Passwords*

- **Function:** Replaces easily guessable manufacturer-set credentials.
- **Protection:** Prevents attackers from using known default logins to access routers, IoT devices, or admin panels.
- **Example:** Changing the default router password can stop an intruder from logging in and changing network settings.

### *3. Enabling WPA2/WPA3 Encryption*

- **Function:** Encrypts wireless communication between devices and access points.
- **Protection:** Prevents attackers from intercepting or modifying data on Wi-Fi networks.
- **Example:** WPA3 makes it harder for hackers to crack Wi-Fi passwords using brute-force attacks.

### *4. Regular Software Updates*

- **Function:** Patches security vulnerabilities in systems and applications.
- **Protection:** Prevents exploitation of known bugs or backdoors by attackers.
- **Example:** Updating your OS can fix a flaw that hackers use for remote access.

### *5. Antivirus and Anti-Malware Tools*

- **Function:** Scans for, detects, and removes malicious software.
- **Protection:** Helps stop malware that could steal data, spy on users, or corrupt systems.
- **Example:** A good antivirus can block ransomware before it encrypts your files.

### *6. Network Segmentation*

- **Function:** Divides the network into smaller parts (subnets).
- **Protection:** Limits the spread of threats and restricts access based on role.
- **Example:** If a virus infects a guest network, it won't affect internal business systems.

## 5.Consider what additional security measures could be implemented in a larger, more complex network.

In a larger, more complex network, additional security measures are essential to protect against advanced threats and ensure smooth operations. These may include implementing **intrusion detection and prevention systems (IDPS)** to monitor and block malicious activity in real-time, and **network segmentation** to limit access between different parts of the network, reducing the impact of a potential breach. **Multi-factor authentication (MFA)** should be enforced for all users, especially those with administrative access. **Regular vulnerability assessments and penetration testing** can help identify and fix security gaps. Additionally, **security information and event management (SIEM)** systems can provide centralized logging, monitoring, and threat analysis to detect suspicious patterns. Finally, **employee training programs** and **incident response plans** ensure that both technology and people are prepared to defend the network effectively.

## Write a short paragraph on how you would educate others about the importance of network security in everyday use.

To educate others about the importance of network security in everyday use, I would start by explaining how much of our daily lives rely on the internet—from online banking and shopping to social media and communication. I would use real-life examples of cyber threats like phishing, malware, and identity theft to show how easily personal information can be stolen if proper security measures aren't taken. By highlighting simple practices such as using strong passwords, avoiding suspicious links, updating software regularly, and enabling firewalls, I would emphasize how small steps can greatly reduce the risk of cyberattacks. The goal would be to make network security feel practical, relevant, and essential for everyone.