Network Security Report

This report documents the findings from analyzing network security threats, implementing basic security measures, and monitoring network traffic using Wireshark. It also includes security best practices and recommendations.

1. Summary of Network Threats.

Network Threats	Description	Potential impact	Examples
Viruses	Malicious programs that spread by attaching to files	Data corruption, slow system performance	**YahLover (Love Bug) Virus (2002)** In the early 2000s, the YahLover virus spread through infected email attachments in India. It corrupted files and slowed down system performance in various government and corporate networks.
Worms	Self-replicating malware that spreads without user action	Network congestion, resource exhaustion	**WannaCry Ransomware Attack (2017)** Although WannaCry is primarily ransomware, it spread like a worm by exploiting vulnerabilities in outdated Windows systems. Many computers in India's banking sector, including ATMs, were infected, causing widespread disruption.
Trojans	Disguised as legitimate software to gain unauthorized access.	Data theft, system compromise.	**Android Banking Trojan (EventBot, 2020)** EventBot targeted Indian users by disguising itself as a legitimate financial app. It stole banking credentials and intercepted SMS-based two-factor authentication (2FA) codes, leading

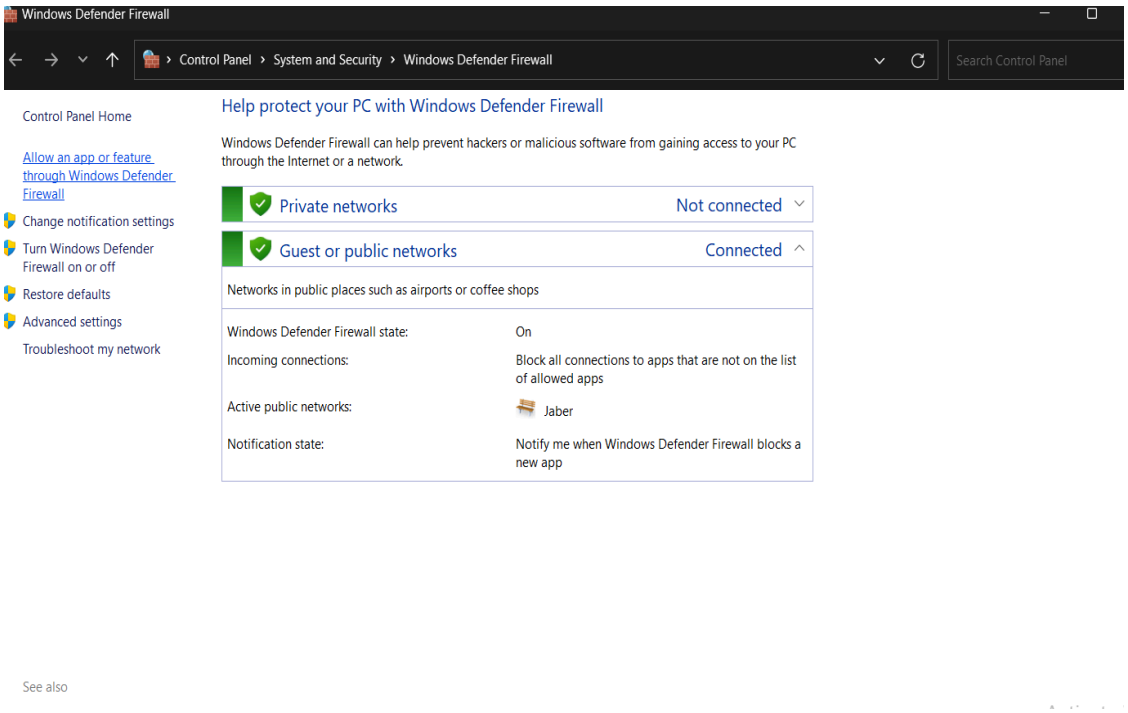
			to unauthorized fund transfers.
Phishing	Deceptive techniques to trick users into revealing sensitive information.	Credential theft, financial fraud.	**State Bank of India (SBI) Phishing Scam (2020)** Attackers sent fake SMS messages, pretending to be from SBI, urging users to update their KYC details. Victims who click on the fraudulent links unknowingly enter sensitive banking information, leading to financial fraud.
MITM Attacks	Interception of communications to manipulate or steal data.	Confidentiality breaches.	**Aadhaar Data Interception (2018)** Hackers allegedly intercepted Aadhaar (India's biometric ID system) data during transmission, exploiting vulnerabilities in government portals. This raised concerns about privacy breaches and misuse of personal data.
DDoS Attacks	Overloading a network/server to disrupt availability	Service downtime, Financial losses.	**ICICI Bank DDoS Attack (2012)** ICICI Bank's online banking services were hit by a massive DDoS attack, slowing down services and causing temporary disruptions to customer transactions.

Ransomware	Encrypts user files and demands payment for decryption.	Data loss, financial extortion.	**Petyas Ransomware (2021, Maharashtra Police Case)** The Maharashtra Police Department was hit by a ransomware attack, encrypting critical data and demanding a ransom. Though the government did not pay, the attack disrupted official operations.

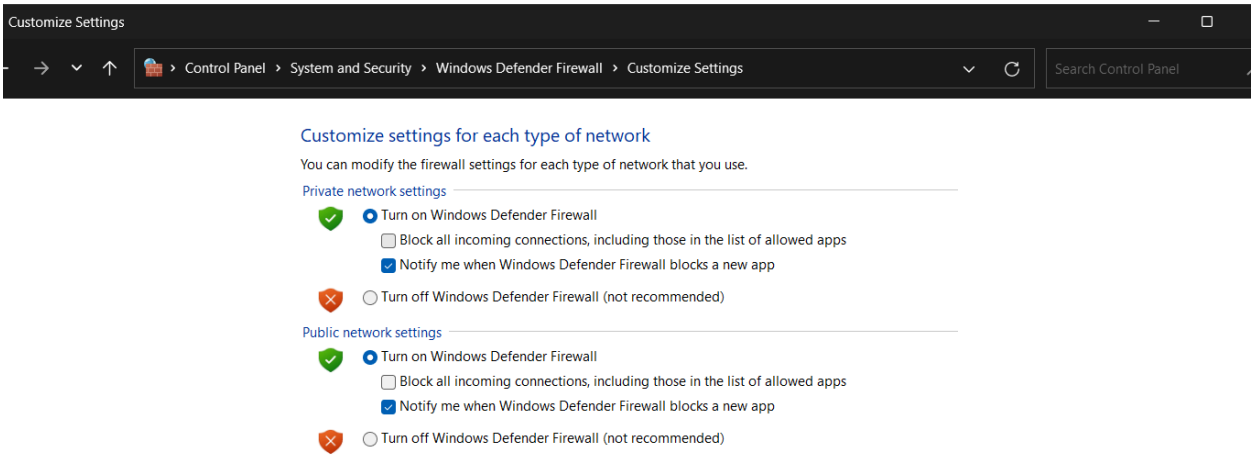
2. Implemented security measures

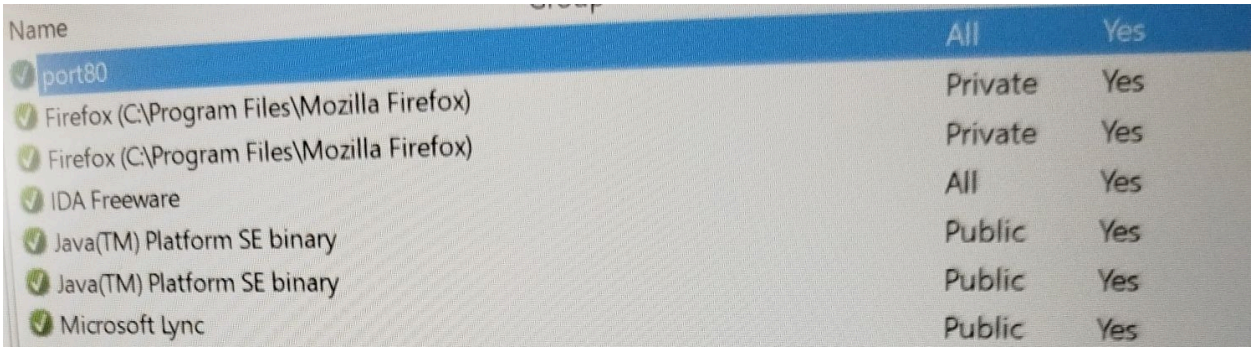
a. Firewall configuration

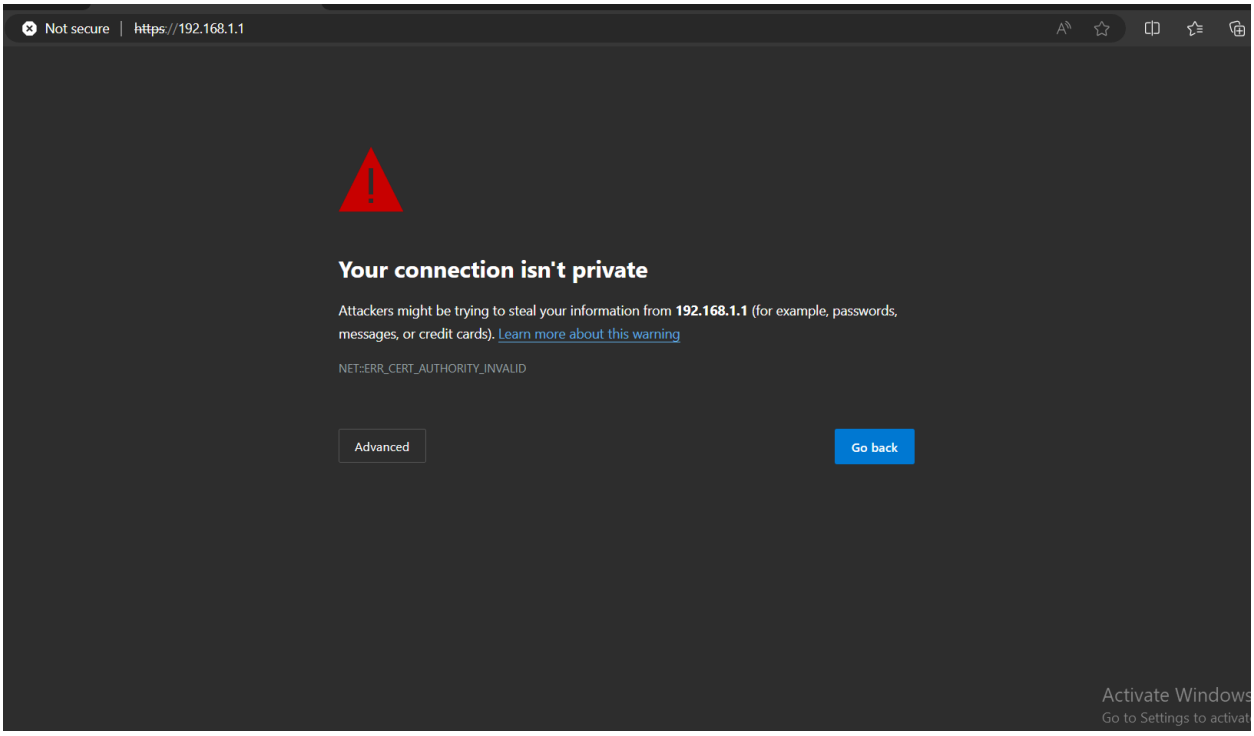
- Configured Windows Defender Firewall to block unauthorized access.



- Set up firewall rules to allow only trusted applications and services.







b. Secure Network Configurations

- **Changed Default Router Passwords:** Default router passwords are often weak and publicly known, making them a prime target for attackers. Changing these to strong, unique passwords enhances security.
- **Enabled WPA2/WPA3 Encryption:** WPA3 provides stronger security for wireless networks compared to WPA/WEP, protecting against brute-force attacks and improving encryption strength.
- **Disabled Unnecessary Network Services:** Many routers and devices come with default services enabled (such as remote management, UPnP, and Telnet), which can introduce vulnerabilities. Disabling unnecessary services minimizes attack surfaces.

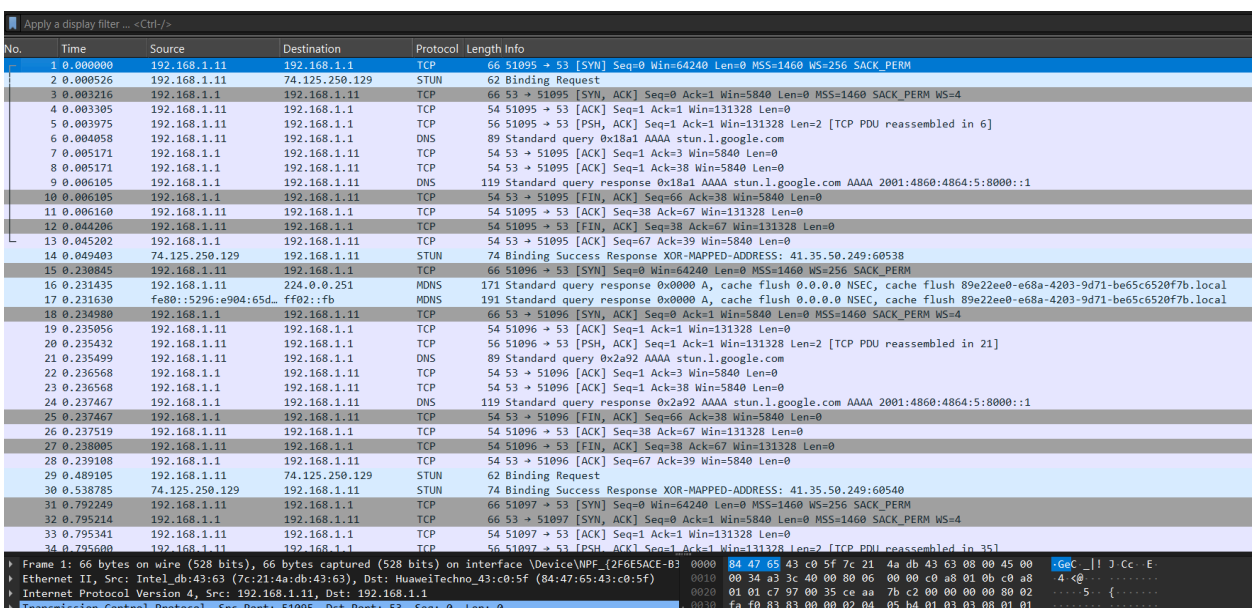
- **Implemented MAC Address Filtering:** Restricting network access to known MAC addresses helps prevent unauthorized devices from connecting to the network.
- **Enabled Network Segmentation:** Dividing the network into segments using VLANs reduces the impact of a security breach, preventing unauthorized lateral movement between different network areas.
- **Deployed Network Address Translation (NAT):** NAT hides internal IP addresses, making it more difficult for attackers to target specific devices within the network.
- **Configured DNS Security Features:** Using secure DNS providers and enabling DNS filtering helps prevent access to malicious websites and phishing domains.
- **Regular Security Audits and Updates:** Periodically reviewing network configurations and applying firmware updates ensures protection against newly discovered vulnerabilities.

c. Access Control and Authentication

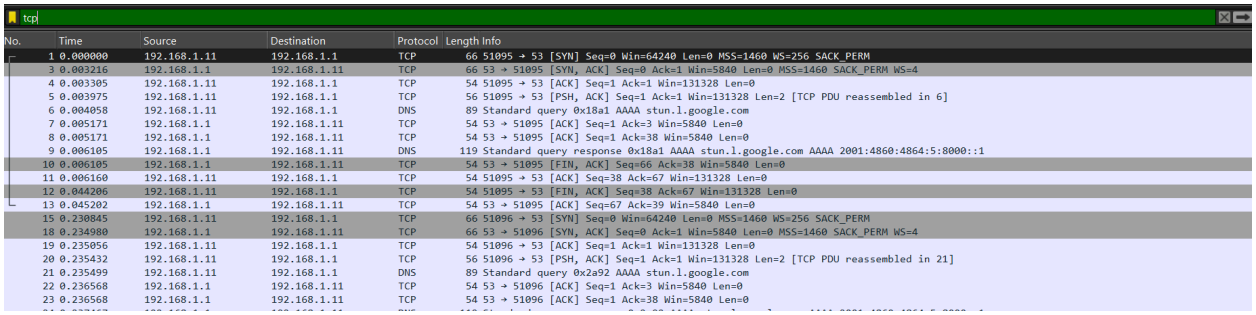
- Enabled **Multi-Factor Authentication (MFA)** for sensitive logins.
- Implemented **strong password policies**.

3. Wireshark Analysis

Analysis of Network Traffic of my Network .

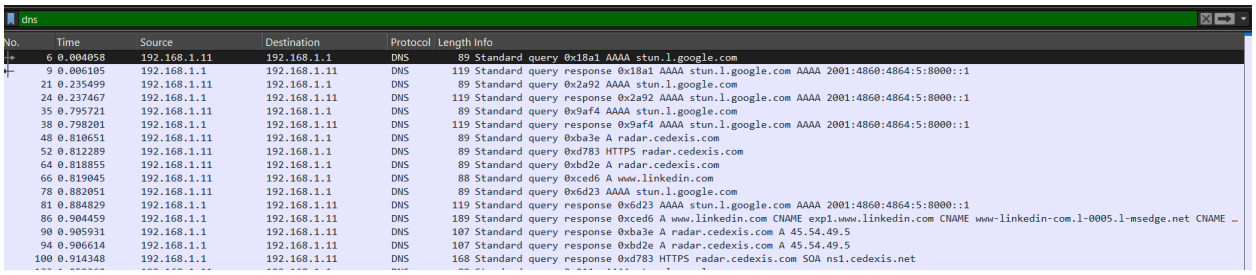


TCP(Transfer control protocol) - Filter the TCP in filter section



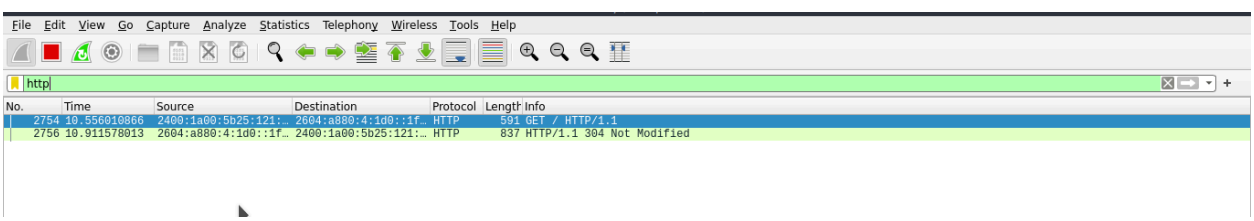
No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	192.168.1.11	192.168.1.1	TCP	66	51095 → 53 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
3	0.003216	192.168.1.1	192.168.1.11	TCP	66	53 → 51095 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1460 SACK_PERM WS=4
4	0.003305	192.168.1.11	192.168.1.1	TCP	54	51095 → 53 [ACK] Seq=1 Ack=1 Win=131328 Len=0
5	0.003975	192.168.1.11	192.168.1.1	TCP	56	51095 → 53 [PSH, ACK] Seq=1 Ack=1 Win=131328 Len=2 [TCP PDU reassembled in 6]
6	0.004058	192.168.1.11	192.168.1.1	DNS	89	Standard query 0x18a1 AAAA stun.l.google.com
7	0.005171	192.168.1.1	192.168.1.11	TCP	54	53 → 51095 [ACK] Seq=1 Ack=3 Win=5840 Len=0
8	0.005171	192.168.1.1	192.168.1.11	TCP	54	53 → 51095 [ACK] Seq=1 Ack=38 Win=5840 Len=0
9	0.006105	192.168.1.1	192.168.1.11	DNS	119	Standard query response 0x18a1 AAAA stun.l.google.com AAAA 2001:4860:4864:5:8000::1
10	0.006105	192.168.1.1	192.168.1.11	TCP	54	53 → 51095 [FIN, ACK] Seq=66 Ack=38 Win=5840 Len=0
11	0.006160	192.168.1.11	192.168.1.1	TCP	54	51095 → 53 [ACK] Seq=38 Ack=67 Win=131328 Len=0
12	0.044206	192.168.1.11	192.168.1.1	TCP	54	51095 → 53 [FIN, ACK] Seq=38 Ack=67 Win=131328 Len=0
13	0.045202	192.168.1.1	192.168.1.11	TCP	54	53 → 51095 [ACK] Seq=67 Ack=39 Win=5840 Len=0
15	0.230845	192.168.1.11	192.168.1.1	TCP	66	51096 → 53 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
18	0.234980	192.168.1.1	192.168.1.11	TCP	66	53 → 51096 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1460 SACK_PERM WS=4
19	0.235056	192.168.1.11	192.168.1.1	TCP	54	51096 → 53 [ACK] Seq=1 Ack=1 Win=131328 Len=0
20	0.235432	192.168.1.11	192.168.1.1	TCP	56	51096 → 53 [PSH, ACK] Seq=1 Ack=1 Win=131328 Len=2 [TCP PDU reassembled in 21]
21	0.235499	192.168.1.11	192.168.1.1	DNS	89	Standard query 0x2a92 AAAA stun.l.google.com
22	0.236568	192.168.1.1	192.168.1.11	TCP	54	53 → 51096 [ACK] Seq=1 Ack=3 Win=5840 Len=0
23	0.236568	192.168.1.1	192.168.1.11	TCP	54	53 → 51096 [ACK] Seq=1 Ack=38 Win=5840 Len=0

DNS (Domain Name system)



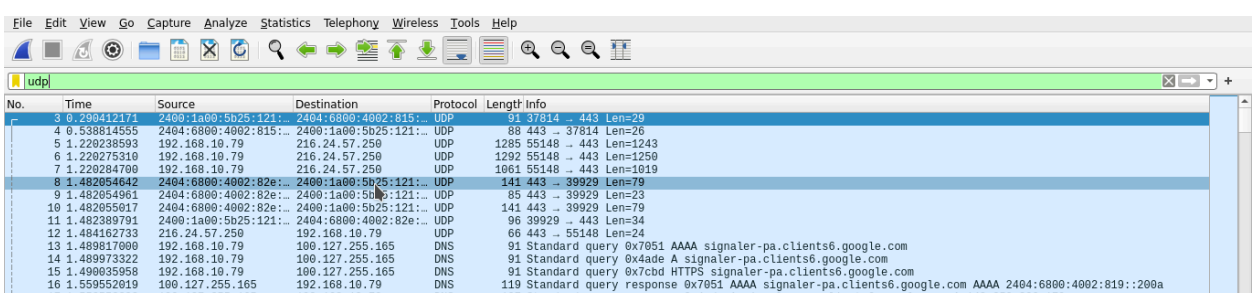
No.	Time	Source	Destination	Protocol	Length	Info
6	0.004058	192.168.1.11	192.168.1.1	DNS	89	Standard query 0x18a1 AAAA stun.l.google.com
9	0.006105	192.168.1.1	192.168.1.11	DNS	119	Standard query response 0x18a1 AAAA stun.l.google.com AAAA 2001:4860:4864:5:8000::1
21	0.235499	192.168.1.11	192.168.1.1	DNS	89	Standard query 0x2a92 AAAA stun.l.google.com
24	0.237467	192.168.1.1	192.168.1.11	DNS	119	Standard query response 0x2a92 AAAA stun.l.google.com AAAA 2001:4860:4864:5:8000::1
35	0.795721	192.168.1.11	192.168.1.1	DNS	89	Standard query 0x9af4 AAAA stun.l.google.com
38	0.798201	192.168.1.1	192.168.1.11	DNS	119	Standard query response 0x9af4 AAAA stun.l.google.com AAAA 2001:4860:4864:5:8000::1
48	0.810651	192.168.1.11	192.168.1.1	DNS	89	Standard query 0xba3e A radar.cedexis.com
52	0.812289	192.168.1.11	192.168.1.1	DNS	89	Standard query 0xd783 HTTPS radar.cedexis.com
64	0.818855	192.168.1.11	192.168.1.1	DNS	89	Standard query 0xbd2e A radar.cedexis.com
66	0.819045	192.168.1.11	192.168.1.1	DNS	88	Standard query 0xced6 A www.linkedin.com
78	0.882051	192.168.1.11	192.168.1.1	DNS	89	Standard query 0x6d23 AAAA stun.l.google.com
81	0.884829	192.168.1.1	192.168.1.11	DNS	119	Standard query response 0x6d23 AAAA stun.l.google.com AAAA 2001:4860:4864:5:8000::1
86	0.904459	192.168.1.1	192.168.1.11	DNS	189	Standard query response 0xced6 A www.linkedin.com CNAME exp1.www.linkedin.com CNAME www-linkedin-com.l-0005.l-msedge.net CNAME …
90	0.905931	192.168.1.1	192.168.1.11	DNS	107	Standard query response 0xba3e A radar.cedexis.com A 45.54.49.5
94	0.906614	192.168.1.1	192.168.1.11	DNS	107	Standard query response 0xbd2e A radar.cedexis.com A 45.54.49.5
100	0.914348	192.168.1.1	192.168.1.11	DNS	168	Standard query response 0xd783 HTTPS radar.cedexis.com SOA ns1.cedexis.net

HTTP (HyperText Transfer Protocol)



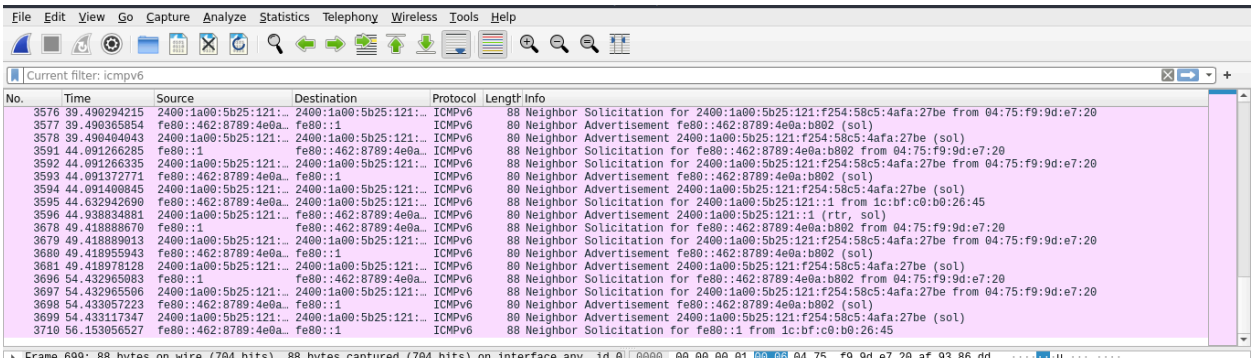
No.	Time	Source	Destination	Protocol	Length	Info
2754	10.556010866	2400:1a00:5b25:121:…	2604:a880:4:1d0::1f…	HTTP	591	GET / HTTP/1.1
2756	10.911578013	2604:a880:4:1d0::1f…	2400:1a00:5b25:121:…	HTTP	837	HTTP/1.1 304 Not Modified

UDP (User Datagram Protocol)



No.	Time	Source	Destination	Protocol	Length	Info
3	0.290412171	2400:1a00:5b25:121:…	2404:6800:4002:815:…	UDP	91	37814 → 443 Len=29
4	0.538814555	2404:6800:4002:815:…	2400:1a00:5b25:121:…	UDP	88	443 → 37814 Len=26
5	1.220238593	192.168.10.79	216.24.57.250	UDP	1285	55148 → 443 Len=1243
6	1.220275310	192.168.10.79	216.24.57.250	UDP	1292	55148 → 443 Len=1250
7	1.220284700	192.168.10.79	216.24.57.250	UDP	1061	55148 → 443 Len=1019
8	1.482054642	2404:6800:4002:82e:…	2400:1a00:5b25:121:…	UDP	141	443 → 39929 Len=79
9	1.482054961	2404:6800:4002:82e:…	2400:1a00:5b25:121:…	UDP	85	443 → 39929 Len=23
10	1.482055017	2404:6800:4002:82e:…	2400:1a00:5b25:121:…	UDP	141	443 → 39929 Len=79
11	1.482389791	2400:1a00:5b25:121:…	2404:6800:4002:82e:…	UDP	96	39929 → 443 Len=34
12	1.484162733	216.24.57.250	192.168.10.79	UDP	66	443 → 55148 Len=24
13	1.489817000	192.168.10.79	100.127.255.165	DNS	91	Standard query 0x7051 AAAA signaler-pa.clients6.google.com
14	1.489973322	192.168.10.79	100.127.255.165	DNS	91	Standard query 0x4ade A signaler-pa.clients6.google.com
15	1.490035958	192.168.10.79	100.127.255.165	DNS	91	Standard query 0x7cbd HTTPS signaler-pa.clients6.google.com
16	1.559552019	100.127.255.165	192.168.10.79	DNS	119	Standard query response 0x7051 AAAA signaler-pa.clients6.google.com AAAA 2404:6800:4002:819::200a

ICMP (Internet control message protocol)



Short description about these Network Traffic

- **HTTP (Hypertext Transfer Protocol)** – Used for web browsing; transmits data in plaintext, making it vulnerable to interception.
- **HTTPS (Secure HTTP)** – Encrypted version of HTTP that ensures secure communication between the browser and website.
- **DNS (Domain Name System)** – Resolves domain names into IP addresses; suspicious DNS requests can indicate malware activity.
- **TCP (Transmission Control Protocol** – Ensures reliable, ordered, and error-checked data transmission between devices.
- **UDP (User Datagram Protocol)** – A faster but less reliable protocol than TCP, commonly used for real-time applications like video calls and gaming.
- **ICMP (Internet Control Message Protocol)** – Used for diagnostics and error reporting (e.g., ping requests); excessive ICMP traffic can indicate a DDoS attack.

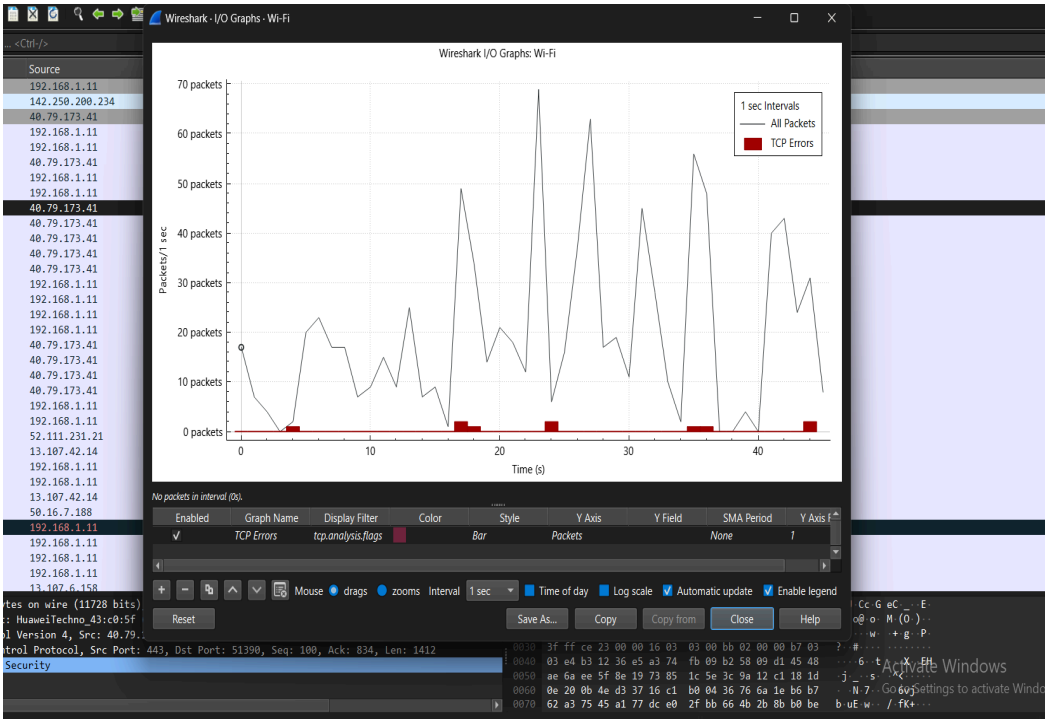
4. Detecting Suspicious Network Traffic

1. **Suspicious Protocol Usage:**
    - **Unencrypted HTTP:** Sensitive data may be exposed if sent over HTTP (port 80) instead of HTTPS (port 443).
    - **Unusual Ports:** Malware may use uncommon ports for communication.
    - **DNS Exfiltration:** Large or strange DNS requests may indicate data theft.
2. **Large Packet Volumes:**
    - **DoS Attack:** High TCP SYN traffic can signal a SYN flood attack.
    - **Unusual DNS Traffic:** Excessive DNS requests to unknown domains may indicate malware.
3. **Scanning Activity:**
    - Many SYN packets sent to different ports could mean an attacker is scanning for vulnerabilities.
4. **Unusual IP Addresses:**
    - Unexpected external connections, especially from unfamiliar regions, may indicate unauthorized access.

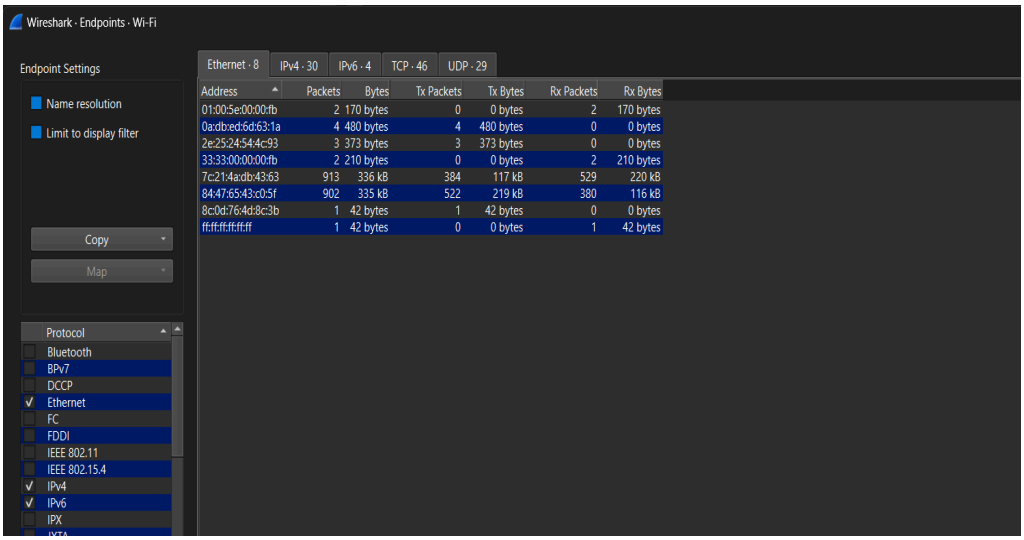
5. **Malformed Packets:**
    - TCP retransmissions and checksum errors can suggest attackers trying to bypass security measures.

5. Network Traffic Analysis & Security Measures

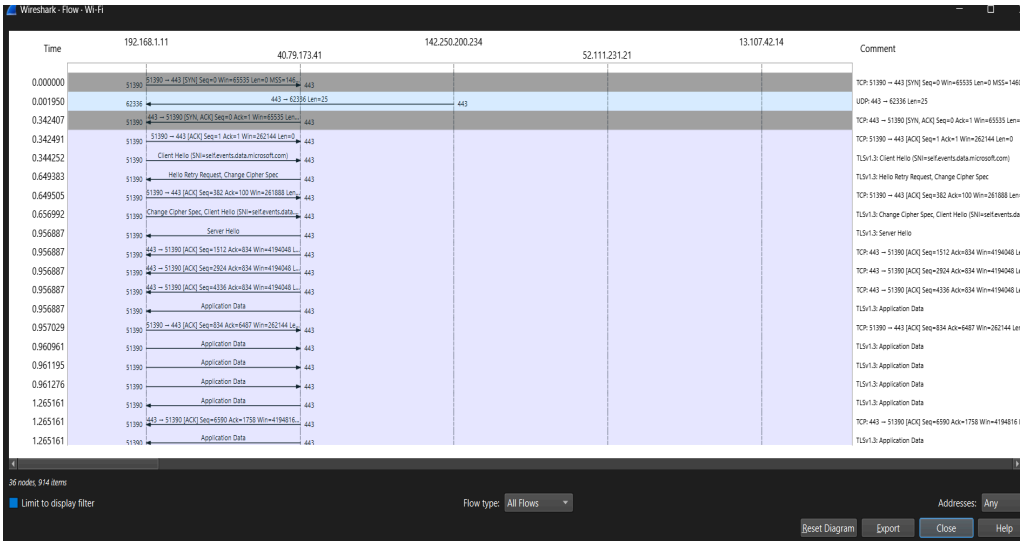
1. **Traffic Monitoring Tools:**
    - **Statistical I/O Graphs:** Detect traffic spikes that may indicate DoS attacks or large file transfers.



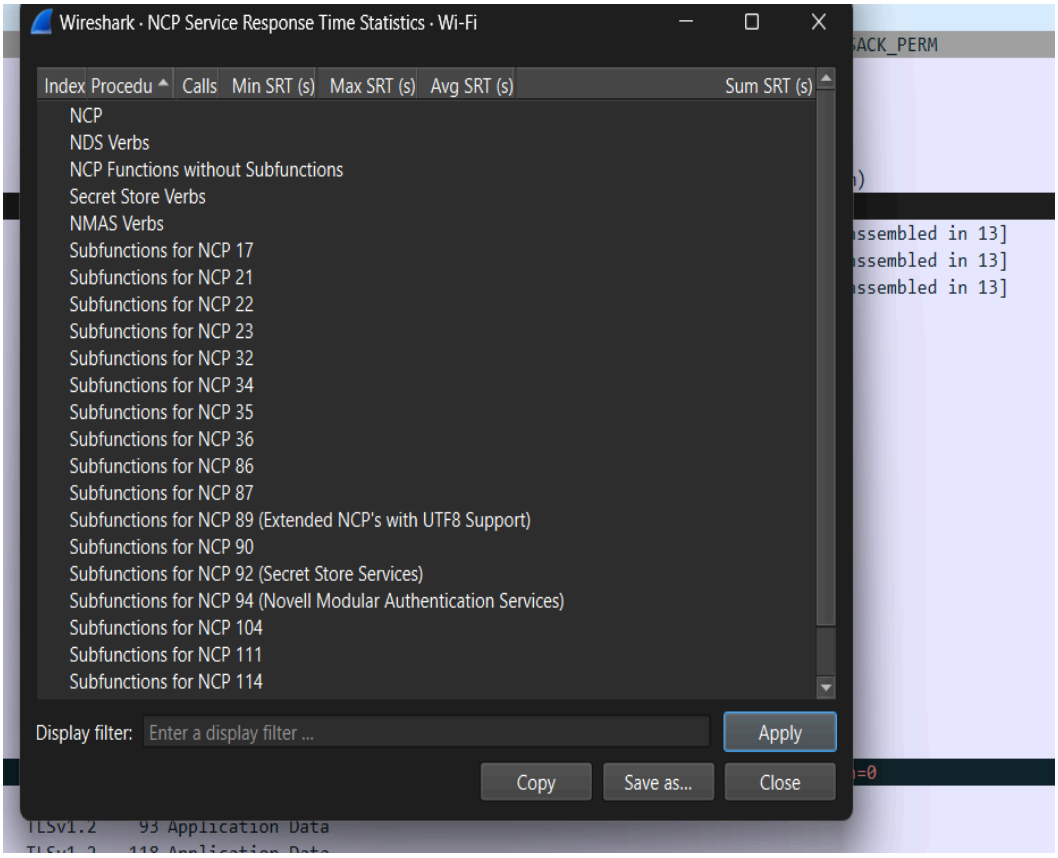
    - **Endpoints:** Identify active devices and detect unknown or unauthorized ones.



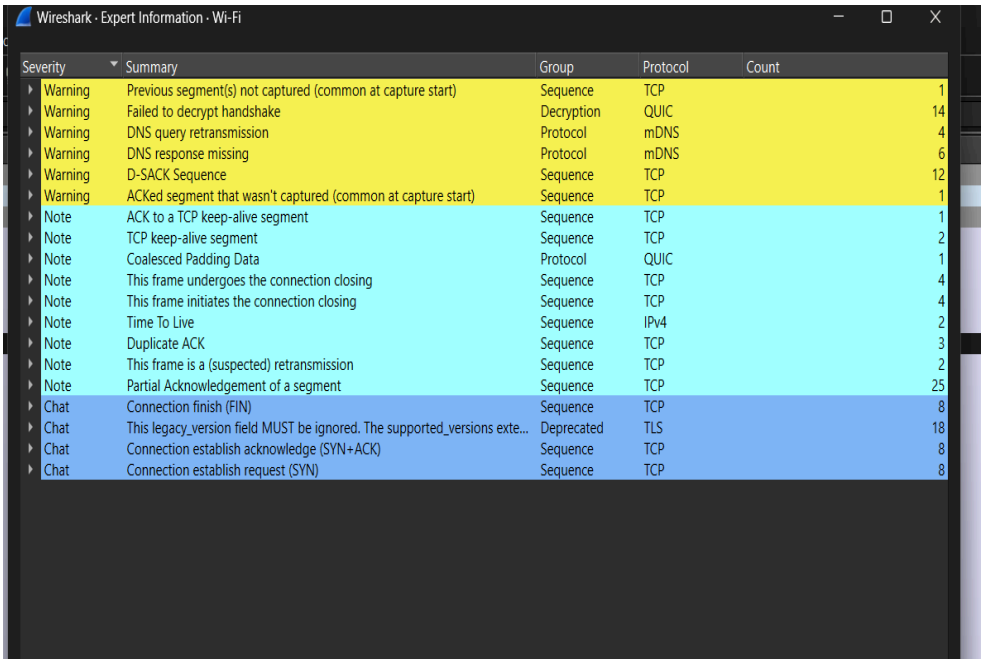
- **Flow Chart:** Troubleshoot failed connections by analyzing TCP handshakes.



- **Service Response Time:** Measure DNS and web server response speeds.



- **Expert Information:** Detect malformed packets and performance issues.



Wireshark · Expert Information · Wi-Fi

Severity	Summary	Group	Protocol	Count
Warning	Previous segment(s) not captured (common at capture start)	Sequence	TCP	1
Warning	Failed to decrypt handshake	Decryption	QUIC	14
Warning	DNS query retransmission	Protocol	mDNS	4
Warning	DNS response missing	Protocol	mDNS	6
Warning	D-SACK Sequence	Sequence	TCP	12
Warning	ACKed segment that wasn't captured (common at capture start)	Sequence	TCP	1
Note	ACK to a TCP keep-alive segment	Sequence	TCP	1
Note	TCP keep-alive segment	Sequence	TCP	2
Note	Coalesced Padding Data	Protocol	QUIC	1
Note	This frame undergoes the connection closing	Sequence	TCP	4
Note	This frame initiates the connection closing	Sequence	TCP	4
Note	Time To Live	Sequence	IPv4	2
Note	Duplicate ACK	Sequence	TCP	3
Note	This frame is a (suspected) retransmission	Sequence	TCP	2
Note	Partial Acknowledgement of a segment	Sequence	TCP	25
Chat	Connection finish (FIN)	Sequence	TCP	8
Chat	This legacy_version field MUST be ignored. The supported_versions exte...	Deprecated	TLS	18
Chat	Connection establish acknowledge (SYN+ACK)	Sequence	TCP	8
Chat	Connection establish request (SYN)	Sequence	TCP	8

2. **Larger Network Security Measures:**
   - **Intrusion Detection Systems (IDS):** Monitor for suspicious activity and potential threats.
   - **Network Segmentation:** Isolate network sections to limit attacker movement.
   - **Multi-Factor Authentication (MFA):** Adds extra security layers to prevent unauthorized access.

6. Security Best Practices and Recommendations

1 Additional Security Measures

- Implement **Intrusion Detection and Prevention Systems (IDS/IPS)**.
- Regularly **update software and apply patches** to fix known vulnerabilities.
- Use **Virtual Private Networks (VPNs)** for secure remote access.
- Enforce **least privilege access controls** to limit users' permissions.
- Conduct **regular penetration testing** to identify security weaknesses.
- Implement **endpoint protection solutions** to detect and prevent malware infections.
- Use **secure email gateways** to filter phishing attempts and spam.
- Enable **automatic security updates** for operating systems and applications.

2 User Awareness and Training

- Educate users about **phishing and social engineering attacks**.
- Promote the use of **password managers** for secure credential storage.
- Encourage **secure browsing practices**, including verifying HTTPS connections.
- Train employees on **incident response procedures** to minimize security breaches.
- Conduct **regular security awareness training** sessions.
- Establish **clear security policies** for employees and contractors.

7. Conclusion

By implementing these security measures and continuously monitoring network activity, we can enhance protection against cyber threats and ensure a secure network environment.