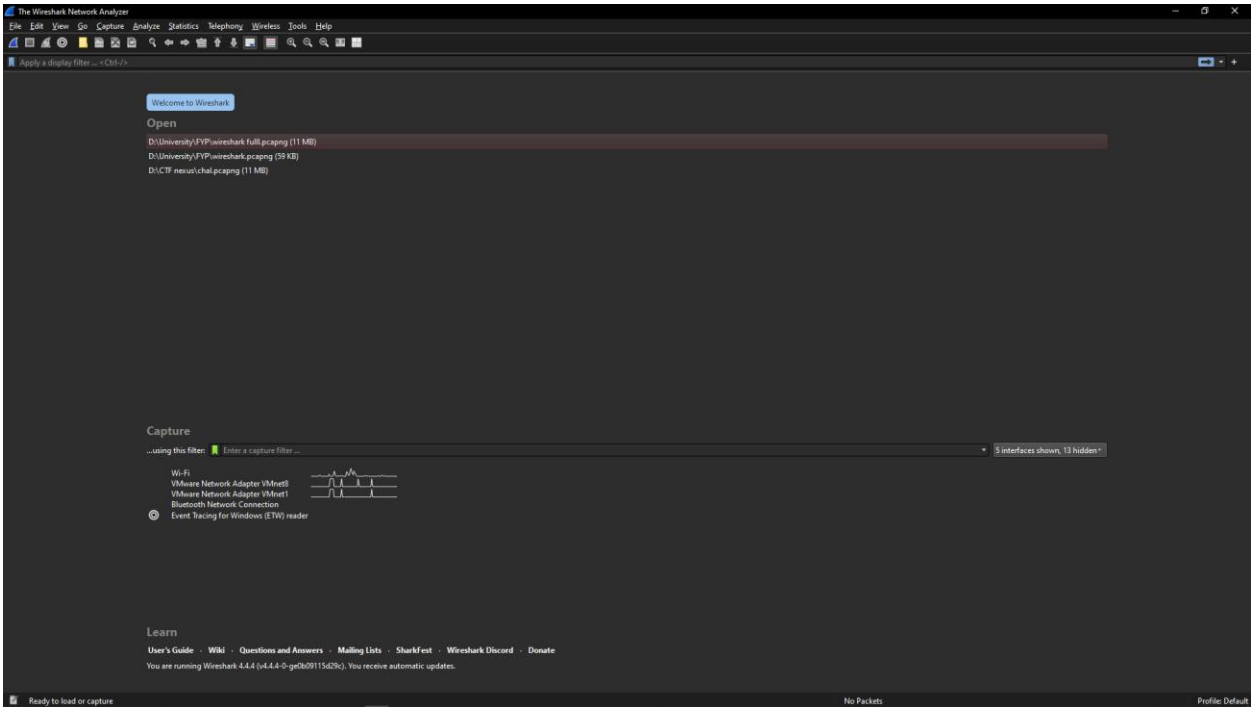
Task 1: Analyze Network Traffic

Monitor and analyze network traffic using a tool like Wireshark.

Wireshark is opened



Lets start network traffic capture of Wi-Fi

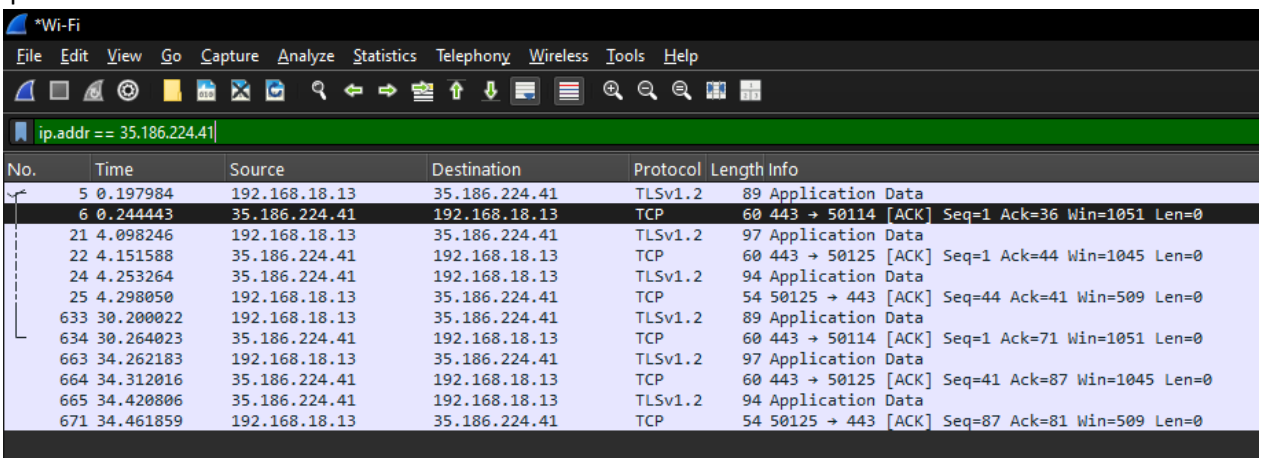
Captured 1061 packets

1049	51.161080	3e:52:a1:07:ef:72	Broadcast	AR
1050	51.161080	3e:52:a1:07:ef:72	Broadcast	AR
1051	51.161080	3e:52:a1:07:ef:72	Broadcast	AR
1052	51.161376	192.168.18.13	192.168.243.130	TC
1053	51.698524	52.34.114.27	192.168.18.13	TL
1054	51.698524	20.207.73.82	192.168.18.13	TL
1055	51.698524	20.207.73.82	192.168.18.13	TL
1056	51.698524	20.207.73.82	192.168.18.13	TC
1057	51.698524	204.79.197.222	192.168.18.13	TC
1058	51.698585	192.168.18.13	52.34.114.27	TC
1059	51.698641	192.168.18.13	20.207.73.82	TC
1060	51.698781	192.168.18.13	20.207.73.82	TC
1061	52.009608	192.168.18.13	20.207.73.82	TC

Now lets analyze it by applying filters

1. **Filter by IP Address:**

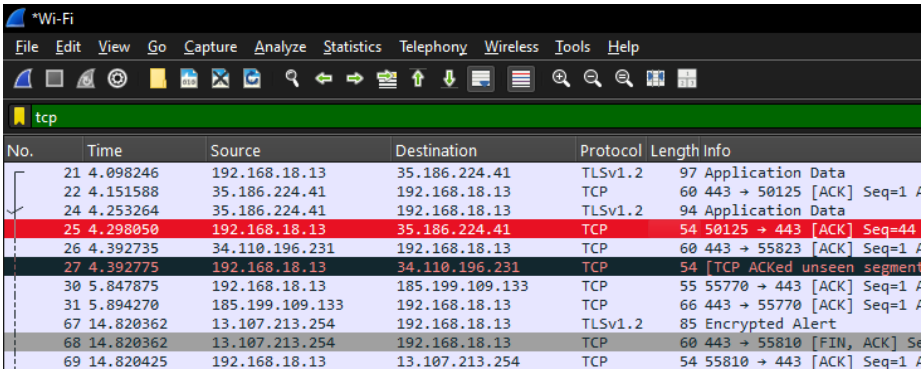
   ip.addr == 35.186.224.41



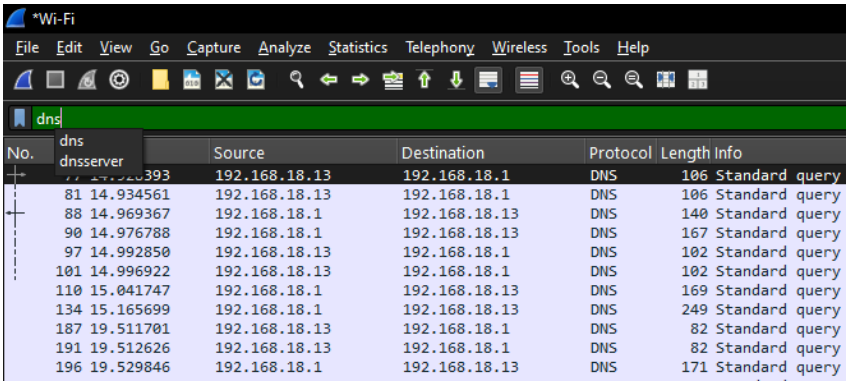
   Using this filter we can see traffic of a specific ip address

2. **Filter by Protocol:**

   tcp

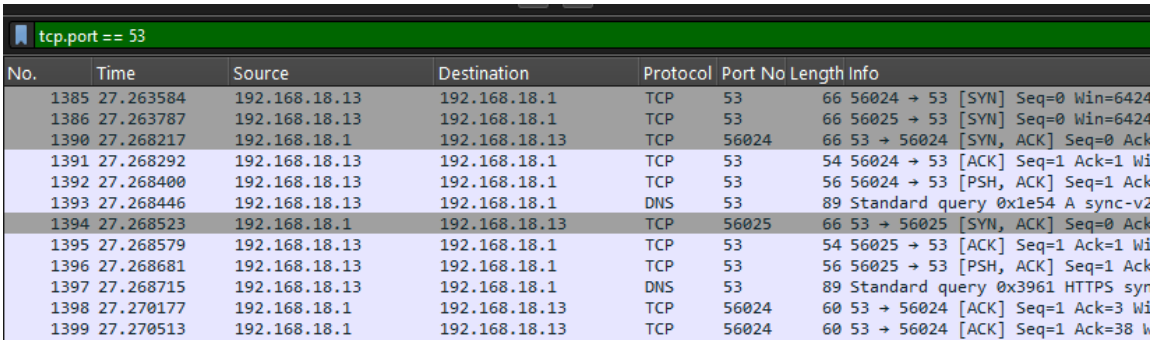


   Dns



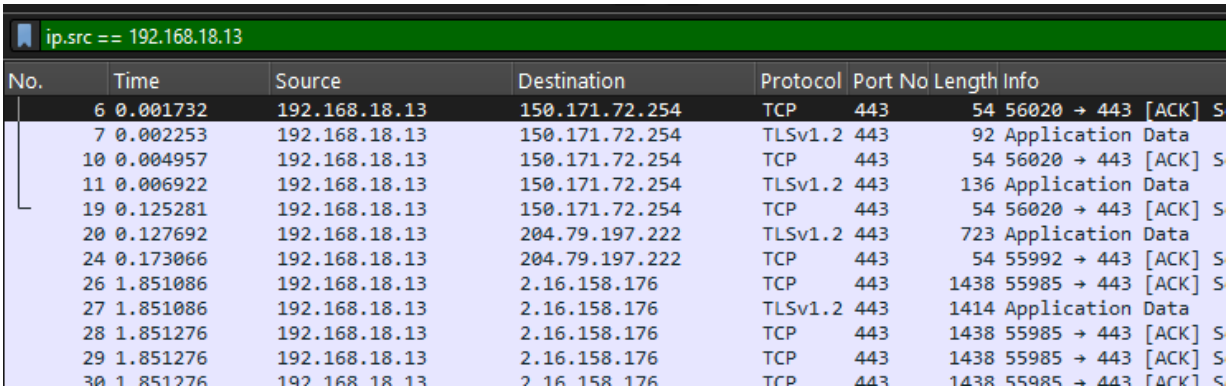
3. **Filter by Port Number:**

   tcp.port == 53

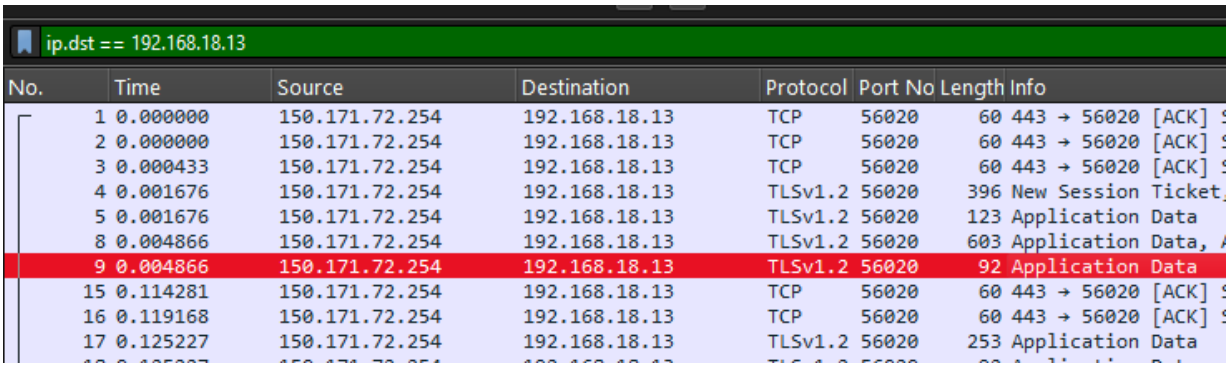


4. **Filter by Source or Destination:**

ip.src == 192.168.18.13



ip.dst == 192.168.18.13



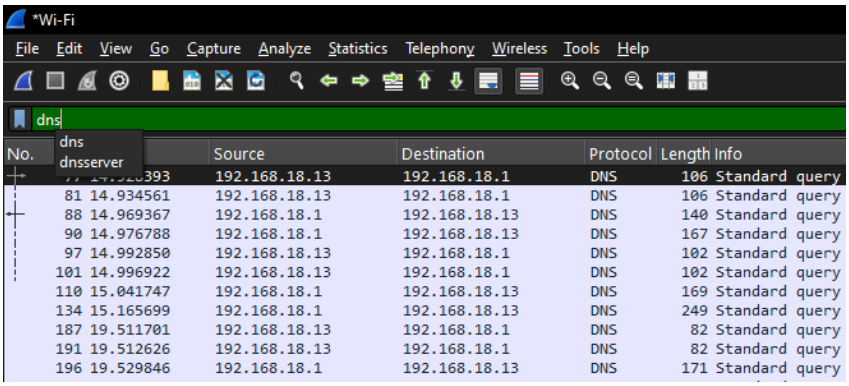
These are some common filters that are used in industry

Identify common network protocols and traffic patterns.

1. DNS (Domain Name System) – Port 53

Function:

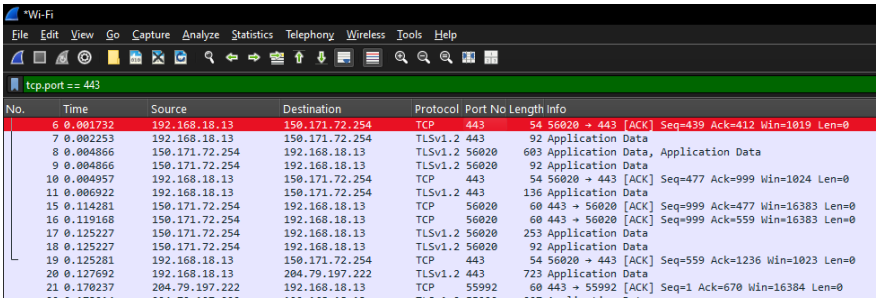
- DNS translates human-readable domain names (e.g., www.google.com) into IP addresses (e.g., 142.250.190.14).
- Without DNS, users would need to remember IP addresses instead of domain names.



2. HTTP & HTTPS – Ports 80 & 443

HTTP (Hypertext Transfer Protocol) – Port 80

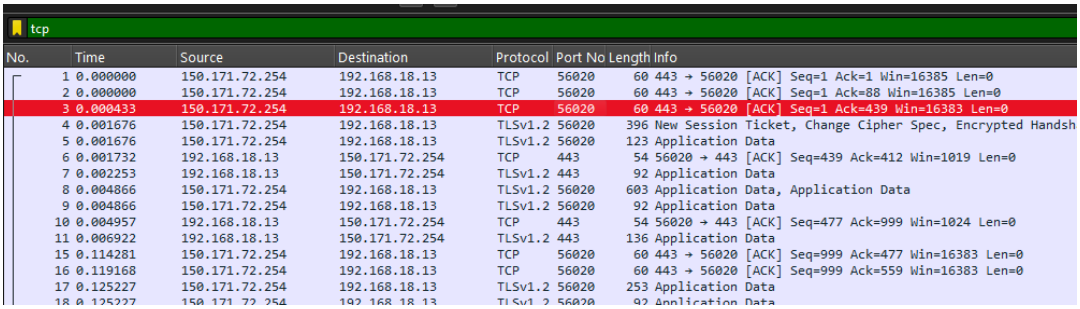
- Used for communication between web browsers and servers.
- Sends and receives web pages, images, and other resources.
- **Not encrypted**, making it vulnerable to interception (e.g., MITM attacks).



3. TCP & UDP – Transport Layer Protocols

TCP (Transmission Control Protocol) – Connection-Oriented

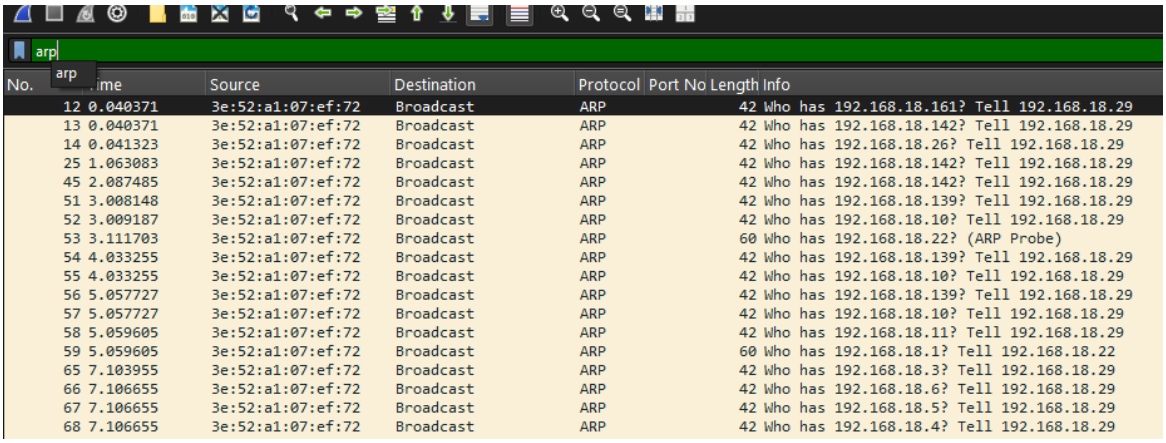
- Reliable data transfer with **error checking and retransmission**.
- Uses a **three-way handshake** before data is sent:
    1. SYN (Client → Server)
    2. SYN-ACK (Server → Client)
    3. ACK (Client → Server)
- Used by **HTTP, HTTPS, FTP, SSH, and email protocols (SMTP, IMAP, POP3).**



4. ARP (Address Resolution Protocol)

Function:

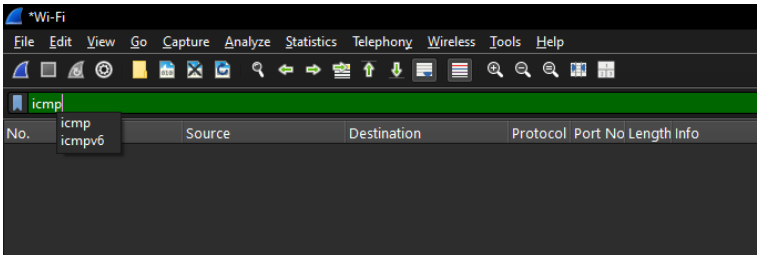
- Maps **IP addresses to MAC addresses** on a local network.
- Used in LAN communication when a device wants to send data but doesn't know the destination MAC address.



5. ICMP (Internet Control Message Protocol) – Ping & Network Diagnostics

Function:

- Used for **network troubleshooting, testing connectivity, and error reporting**.
- Works at the **Network Layer (Layer 3 of the OSI Model)**.



Protocol	*Port*	*Function*	*Security Risks*	*Wireshark Filter*
DNS	53	Resolves domain names to IP addresses	DNS spoofing, cache poisoning	`dns`
HTTP	80	Transfers web pages (unencrypted)	MITM attacks, data interception	`http`
HTTPS	443	Secure web browsing (encrypted)	SSL/TLS vulnerabilities	`tcp.port == 443`
TCP	Various	Reliable, connection-based transport	SYN floods, session hijacking	`tcp`
UDP	Various	Fast, connectionless transport	Packet loss, DDoS attacks	`udp`
ARP	No port (Layer 2)	Maps IP addresses to MAC addresses	ARP spoofing, MITM attacks	`arp`
ICMP	No port (Layer 3)	Network diagnostics, pings	Ping floods, ICMP tunneling	`icmp`