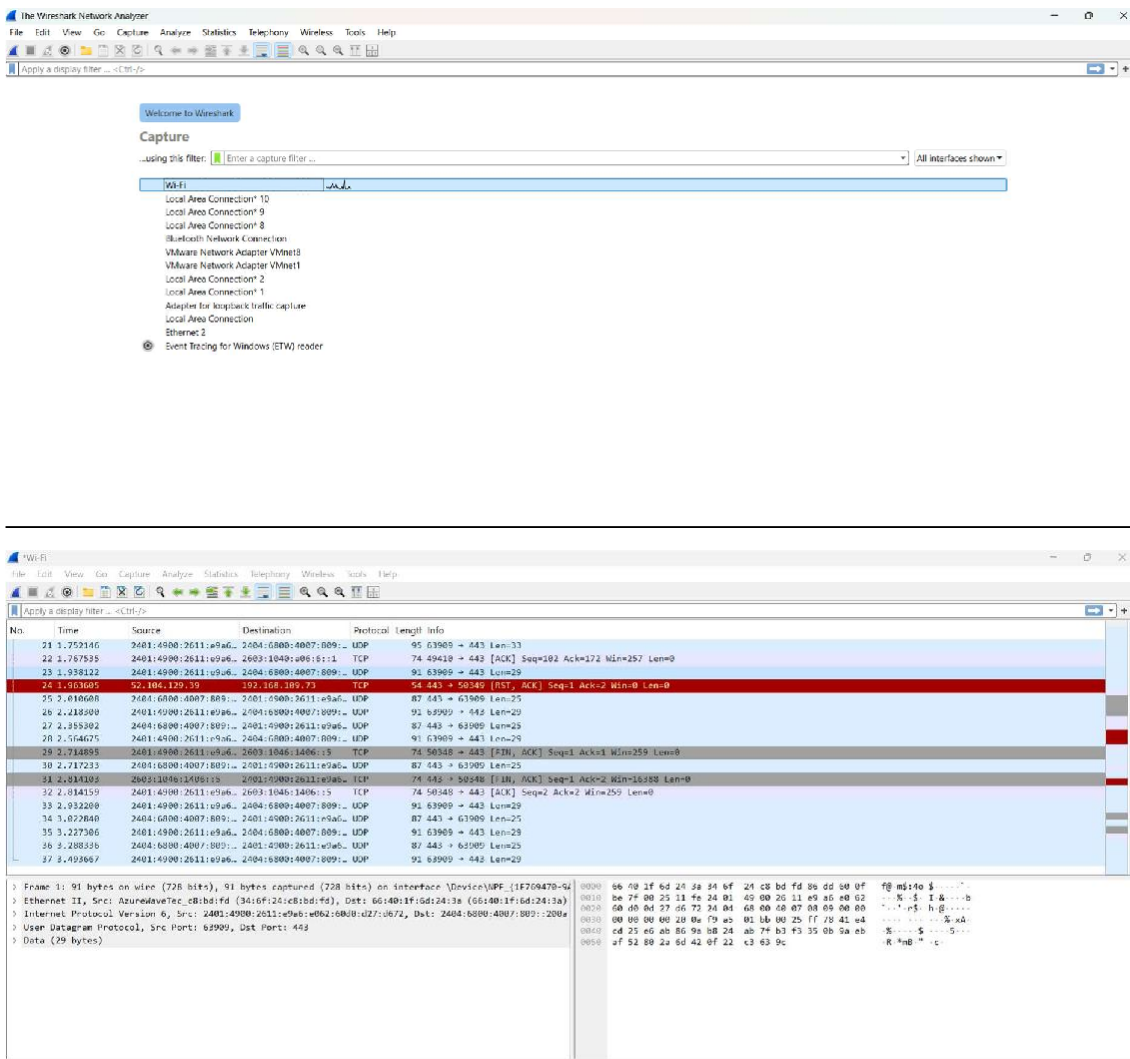


Practical 5

Aim:

Experiments on Packet capture tool: Wireshark

Capturing Packets:



Color Coding:

The 'Wireshark - Coloring Rules Default' dialog box is open, showing a list of rules with checkboxes and filters. The rules include:

- Bad TCP: tcp.analysis.flags && !tcp.analysis.window_update &&
- HSRP State Change: hsrp.state != 8 && hsrp.state != 16
- Spanning Tree Topology Change: stp.type == 0x80
- OSPF State Change: ospfmsg != 1
- ICMP errors: icmp.type in {3,5,11} || icmpv6.type in {1,4}
- ARP: arp
- ICMP: icmp || icmpv6
- TCP RST: tcp.flags.reset eq 1
- SCTP ABORT: sctp.chunk_type eq ABORT
- IPv4 TTL low or unexpected: (ip.ttl < 224 || 0.0.0.4 && ip.ttl < 5 && !ipim || ospf || bop) && ip.v4hop limit low or unexpected
- IPv6 hop limit low or unexpected: (ipv6.hop limit < 5 && !ipsec || ospf || bop) && ip.v6hop limit low or unexpected
- Checksum Errors: eth.fcs.status == "Bad" || ip.checksum.status == "Bad" ||
- SMB: smb || nbss || nbns || netbios
- HTTP: http || tcp.port == 80 || http2
- DCE/RPC: dcerpc
- Routing: arp || eigrp || ospf || bgp || cdp || vrrp || carp || uwp ||
- TCP SYN/FIN: tcp.flags & 0x02 || tcp.flags.fin == 1
- TCP: tcp
- UDP: udp
- Broadcast: eth[0] & 1
- System Event: systemd_journal || sysdig

The main packet list on the right shows packets with color-coded backgrounds (e.g., red for RST, green for ACK). The packet list includes:

- 21 1.752146
- 22 1.767535
- 23 1.938123
- 24 1.963660
- 25 2.010698
- 26 2.218360
- 27 2.355302
- 28 2.564675
- 29 2.714895
- 30 2.717233
- 31 2.814103
- 32 2.814159
- 33 2.932260
- 34 3.022840
- 35 3.227306
- 36 3.288336
- 37 3.493667

Filtering Packets:

The 'tcp' filter is applied to the packet list. The packet list shows only TCP packets, with the filter expression 'tcp' visible in the filter bar. The packet list includes:

- 11 1.552539
- 12 1.61714
- 13 1.618305
- 14 1.619935
- 15 1.723680
- 16 1.723680
- 17 1.723680
- 18 1.723680
- 19 1.723680
- 20 1.723680
- 21 1.767535
- 22 1.963660
- 23 2.010698
- 24 2.218360
- 25 2.355302
- 26 2.564675
- 27 2.714895
- 28 2.717233
- 29 2.814103
- 30 2.814159

Display Filters:

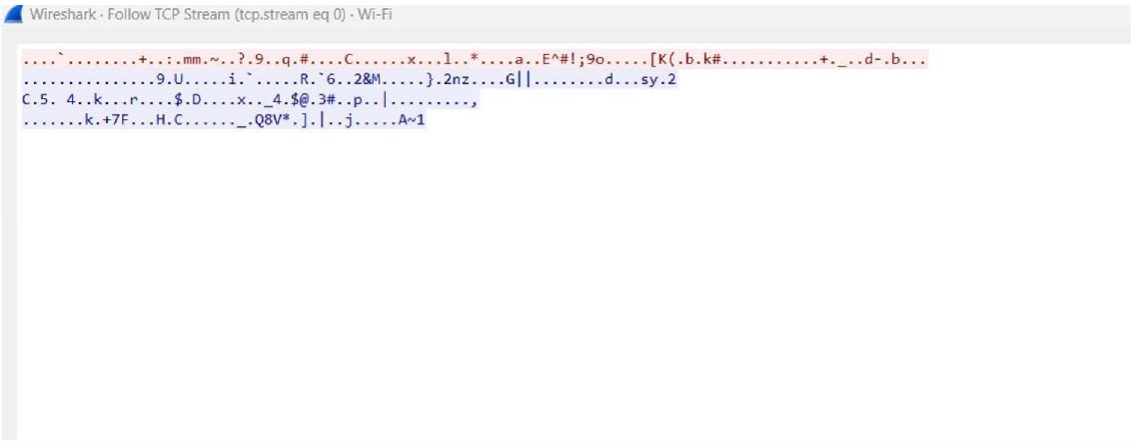
The 'Wireshark - Display Filters' dialog box is open, showing a list of filters with checkboxes and expressions. The filters include:

- Ethernet address 00:00:5e:00:53:00: eth.addr == 00:00:5e:00:53:00
- Ethernet type 0x0806 (ARP): eth.type == 0x0806
- Ethernet broadcast: eth.addr == ff:ff:ff:ff:ff:ff
- No ARP: not arp
- IPv4 only: ip
- IPv4 address 192.0.2.1: ip.addr == 192.0.2.1
- IPv4 address isn't 192.0.2.1: ip.addr != 192.0.2.1
- IPv6 only: ipv6
- IPv6 address 2001:db8::1: ipv6.addr == 2001:db8::1
- TCP only: tcp
- UDP only: udp
- Non-DNS port: !udp.port == 53 || tcp.port == 53
- TCP or UDP port is 80 (HTTP): tcp.port == 80 || udp.port == 80
- HTTP: http
- No ARP and no DNS: not arp and not dns
- Non-HTTP and non-SMTP to/from 192.0.2.1: ip.addr == 192.0.2.1 and tcp.port not in ...

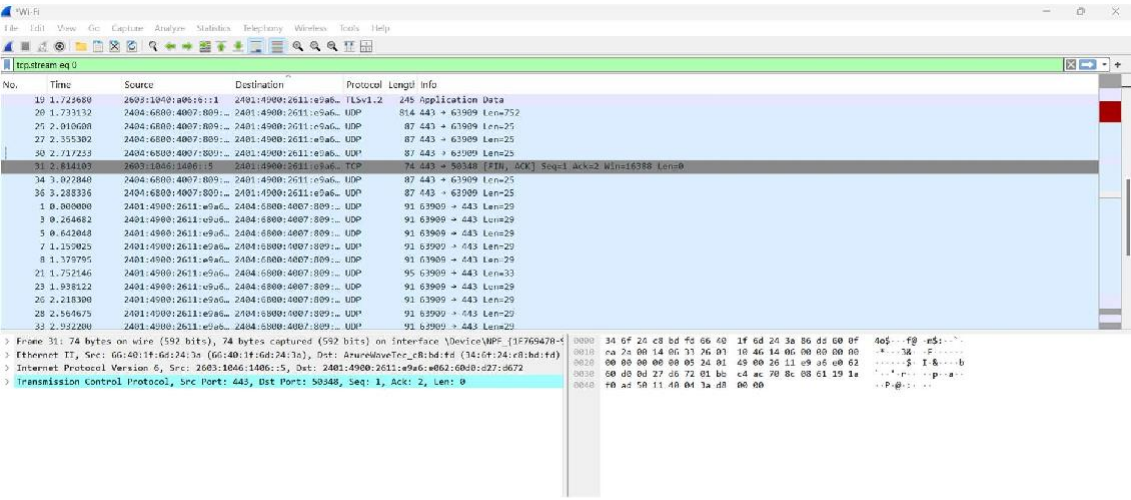
The main packet list on the right shows packets with color-coded backgrounds (e.g., red for RST, green for ACK). The packet list includes:

- 11 1.552539
- 12 1.61714
- 13 1.618305
- 14 1.619935
- 15 1.723680
- 16 1.723680
- 17 1.723680
- 18 1.723680
- 19 1.723680
- 20 1.723680
- 21 1.767535
- 22 1.963660
- 23 2.010698
- 24 2.218360
- 25 2.355302
- 26 2.564675
- 27 2.714895
- 28 2.717233
- 29 2.814103
- 30 2.814159

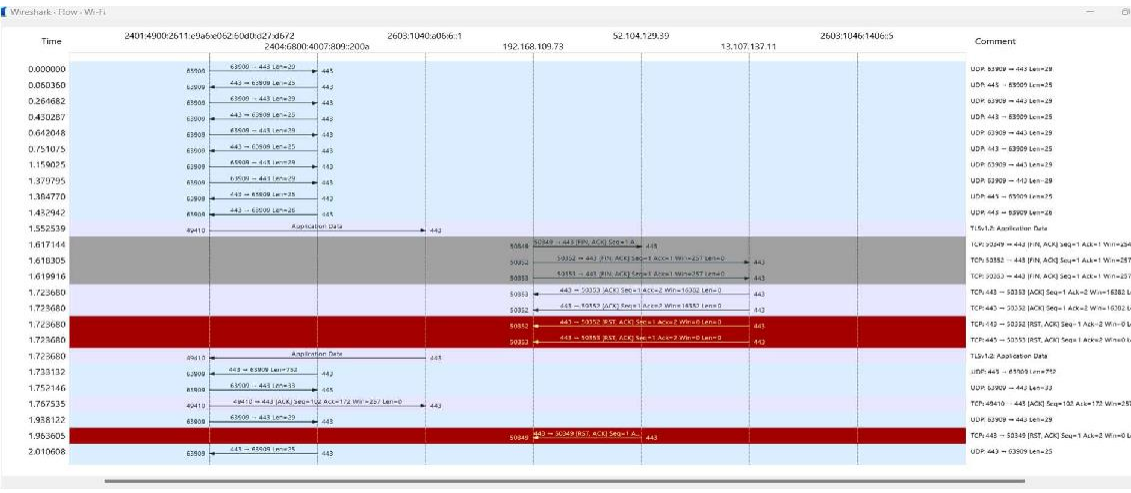
Tcp Stream:



Inspecting Packets:



Flow Graph:



1. Create a Filter to display only TCP/UDP packets, inspect the packets and provide the flow graph

Procedure

Select Local Area Connection in Wireshark.

Go to capture → option

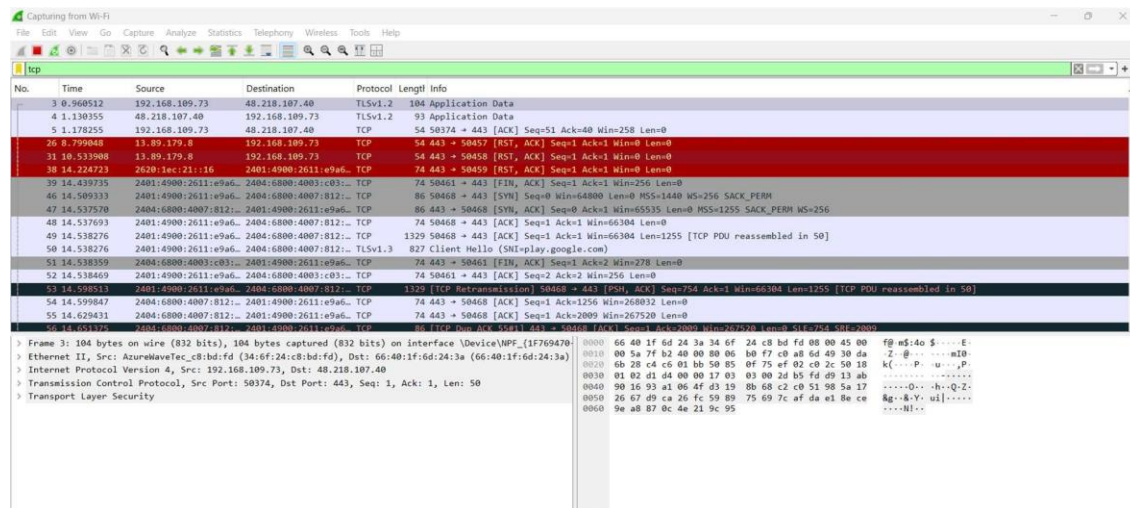
Select stop capture automatically after 100 packets.

Then click Start capture.

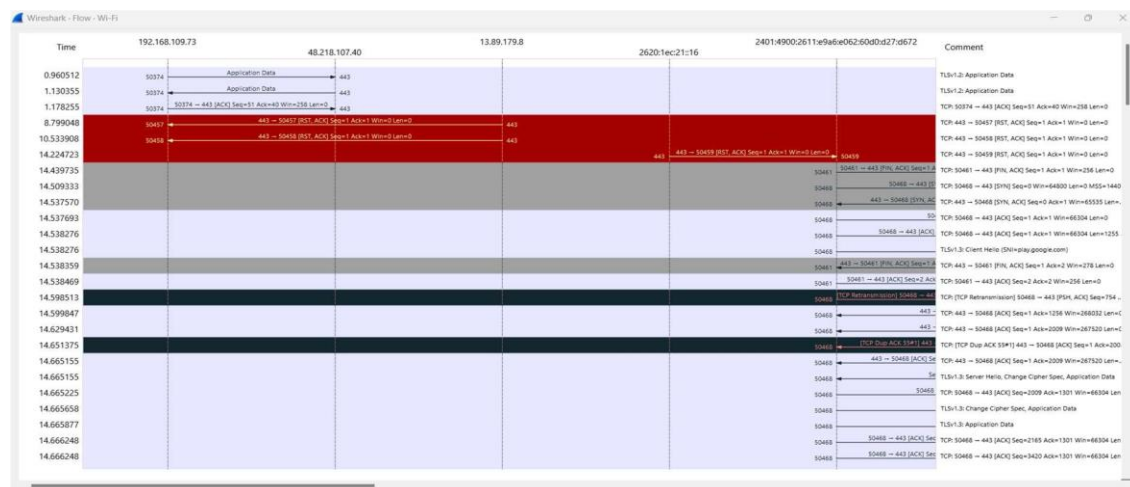
Search TCP packets in search bar.

To see flow graph click Statistics→Flow graph.

Save the packets.



Flowgraph:



2. Create a Filter to display only ARP packets and inspect the packets.

Procedure

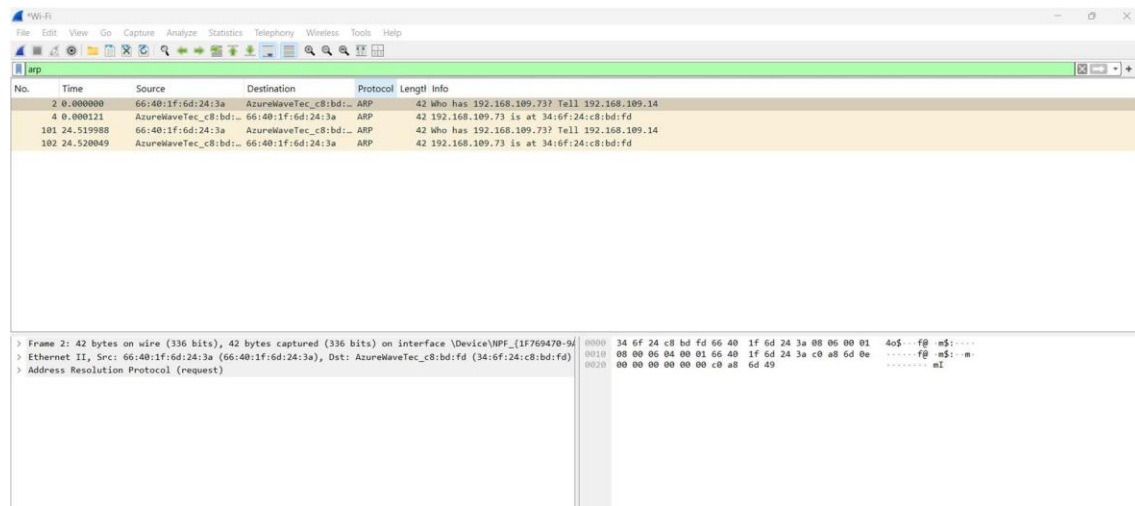
Go to capture → option

Select stop capture automatically after 100 packets.

Then click Start capture.

Search ARP packets in search bar.

Save the packets.



3. Create a Filter to display only DNS packets and provide the flow graph.

Procedure

Go to capture → option

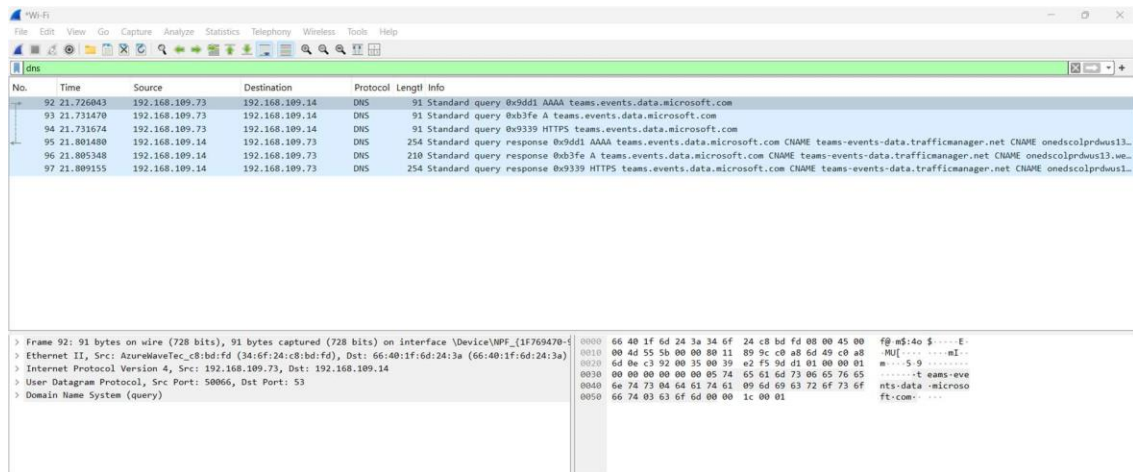
Select stop capture automatically after 100 packets.

Then click Start capture.

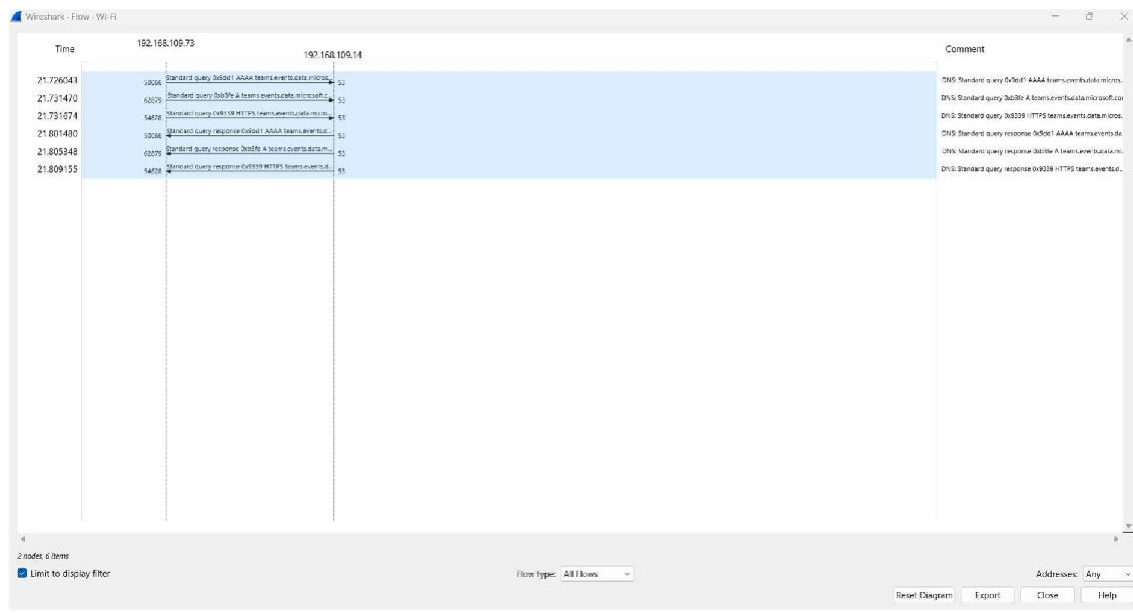
Search DNS packets in search bar.

To see flow graph click Statistics → Flow graph.

Save the packets.



Flowgraph:



4. Create a Filter to display only DHCP packets and inspect the packets.

Procedure

Select Local Area Connection in Wireshark.

Go to capture → option

Select stop capture automatically after 100 packets.

Then click Start capture.

Search DHCP packets in search bar.

Save the packets

The image shows a Wireshark packet capture of a DHCP transaction. The packet list pane at the top shows two packets: a DHCP Request (No. 573) and a DHCP ACK (No. 574). The packet details pane for the ACK shows the IP address 192.168.109.14 assigned to the client. The packet bytes pane at the bottom shows the raw data in hexadecimal and ASCII.

No.	Time	Source	Destination	Protocol	Length	Info
573	85.896500	192.168.109.73	192.168.109.14	DHCP	348	DHCP Request - Transaction ID 0x5b154d7
574	85.849742	192.168.109.14	192.168.109.73	DHCP	352	DHCP ACK - Transaction ID 0x5b154d7

Packet 574 details:

- Ethernet II, Src: AsustekE100-c8:b1:d4 (34:5f:24:c8:b1:d4), Dst: 08:00:1f:6d:24:3a (08:00:1f:6d:24:3a)
- Internet Protocol Version 4, Src: 192.168.109.73, Dst: 192.168.109.14
- User Datagram Protocol, Src Port: 68, Dst Port: 67
- Dynamic Host Configuration Protocol (Request)

Packet 574 bytes:

```

0000  66 40 1f 6d 24 3a 34 d7 24 c8 b1 d4 00 00 45 00  f6 nd 50 5... E
0010  01 4e 55 70 00 00 00 11 88 06 c0 a8 6d 40 c0 a8  8p...m...l...
0020  6d 0e 00 44 00 43 01 2a 01 c1 01 06 00 53 b1  m...C...m...S
0030  54 47 00 00 00 c0 a8 6d 49 00 00 00 00 60 00  T...n...f...
0040  00 00 00 00 00 00 24 d7 24 c8 b1 d4 00 00 00  4...d...f...
0050  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  0...0...0...
0060  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  0...0...0...
0070  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  0...0...0...
0080  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  0...0...0...
0090  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  0...0...0...
00a0  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  0...0...0...
00b0  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  0...0...0...
00c0  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  0...0...0...
00d0  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  0...0...0...
00e0  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  0...0...0...
00f0  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  0...0...0...
0100  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  0...0...0...

```