

## **EXPERIMENT-25**

### **NETWORK LAYER PROTOCOL HEADER ANALYSIS USING WIRE SHARK – ARP AND HTTP**

**AIM:** To analyze capturing of Transport layer protocol header analysis using Wire shark-ARP and

HTTP.

#### **SOFTWARE USED:**

Wire shark network  
analyzer

#### **PROCEDURE:**

1. Open wire shark.
2. Click on list the available capture interface.
3. Choose the LAN interface.
4. Click on start button.
5. Active packets will be displayed.
6. Capture the packets & select any IP address from the source.
7. Click on the expression and select IPV4 →IP addr source address in the field name.
8. Select the double equals (==) from the selection and enter the selected IP source address.
9. Click on apply button.
10. All the packets will be filtered using source address.

No.	Time	Source	Destination	Protocol	Length	Info
5910	21.341973	HikvisionDig_10:61:54	Broadcast	ARP	60	Who has 172.24.47.169? Tell 172.24.32.13
5914	21.367675	3e:9e:93:75:b4:4f	Broadcast	ARP	60	Gratuitous ARP for 172.24.33.57 (Request)
5917	21.439516	3e:9e:93:75:b4:4f	Broadcast	ARP	60	Who has 172.24.32.1? Tell 172.24.33.57
5925	21.566963	HikvisionDig_10:61:54	Broadcast	ARP	60	Who has 172.24.47.191? Tell 172.24.32.13
5955	22.093353	HikvisionDig_26:c4:f7	Broadcast	ARP	60	Who has 172.24.47.125? Tell 172.24.32.12
5971	22.243303	HikvisionDig_26:c4:f7	Broadcast	ARP	60	Who has 172.24.47.137? Tell 172.24.32.12
5974	22.296717	HikvisionDig_10:61:54	Broadcast	ARP	60	Who has 172.24.46.12? Tell 172.24.32.13
5985	22.337058	HikvisionDig_10:61:54	Broadcast	ARP	60	Who has 172.24.47.169? Tell 172.24.32.13
5996	22.400270	172.24.36.230	34.104.35.123	TCP	66	36816 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
6017	23.155299	HikvisionDig_10:61:54	Broadcast	ARP	60	Who has 172.24.47.181? Tell 172.24.32.13
6018	23.155299	HikvisionDig_10:61:54	Broadcast	ARP	60	Who has 172.24.47.194? Tell 172.24.32.13
6019	23.160517	PramaHikvisi_17:c8:a8	Broadcast	ARP	60	Who has 172.24.32.1? Tell 172.24.46.53
6024	23.184578	5e:de:09:8d:9b:c6	Broadcast	ARP	60	Who has 172.24.32.1? Tell 172.24.39.163
6029	23.199399	Cisco_4e:e7:67	Broadcast	ARP	60	Who has 172.24.47.211? Tell 172.24.32.1

  

<p>Frame 5974: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interf.</p> <p>Ethernet II, Src: HikvisionDig_10:61:54 (3c:1b:f8:10:61:54), Dst: Broadcast (ff:ff:ff:ff:ff:ff)</p> <p>Address Resolution Protocol (request)</p> <ul style="list-style-type: none"> <li>Hardware type: Ethernet (1)</li> <li>Protocol type: IPv4 (0x0800)</li> <li>Hardware size: 6</li> <li>Protocol size: 4</li> <li>Opcode: request (1)</li> <li>Sender MAC address: HikvisionDig_10:61:54 (3c:1b:f8:10:61:54)</li> <li>Sender IP address: 172.24.32.13</li> <li>Target MAC address: 00:00:00:00:00:00 (00:00:00:00:00:00)</li> <li>Target IP address: 172.24.46.12</li> </ul>	<pre> 0000  ff ff ff ff ff 3c 1b f8 10 61 54 08 00 01  .....&lt;...aT.... 0010  08 00 06 04 00 01 3c 1b f8 10 61 54 ac 18 20 0d  .....&lt;...aT.... 0020  00 00 00 00 00 00 ac 18 2e 0c 00 00 00 00 00 00  ..... 0030  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ..... </pre>
--	--

**Result:** Hence, the capturing of packets using wire shark network analyzer was analyzed for ARP and HTTP.