Experiment - 25

network layer Protocol header Analysis using wire shark - ARP & HTTP.

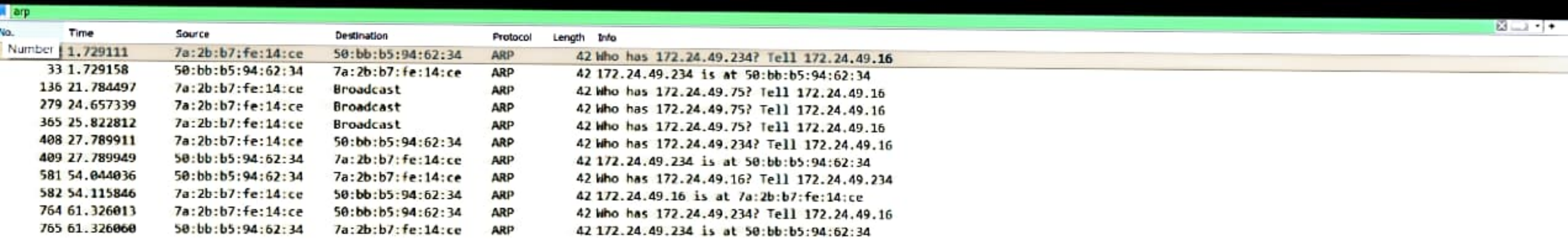
Aim To analyse the capturing of transport layer & Protocol header analysis using wire-shark ARP & HTTP.

Software: wireshark network analyzer.

Procedure

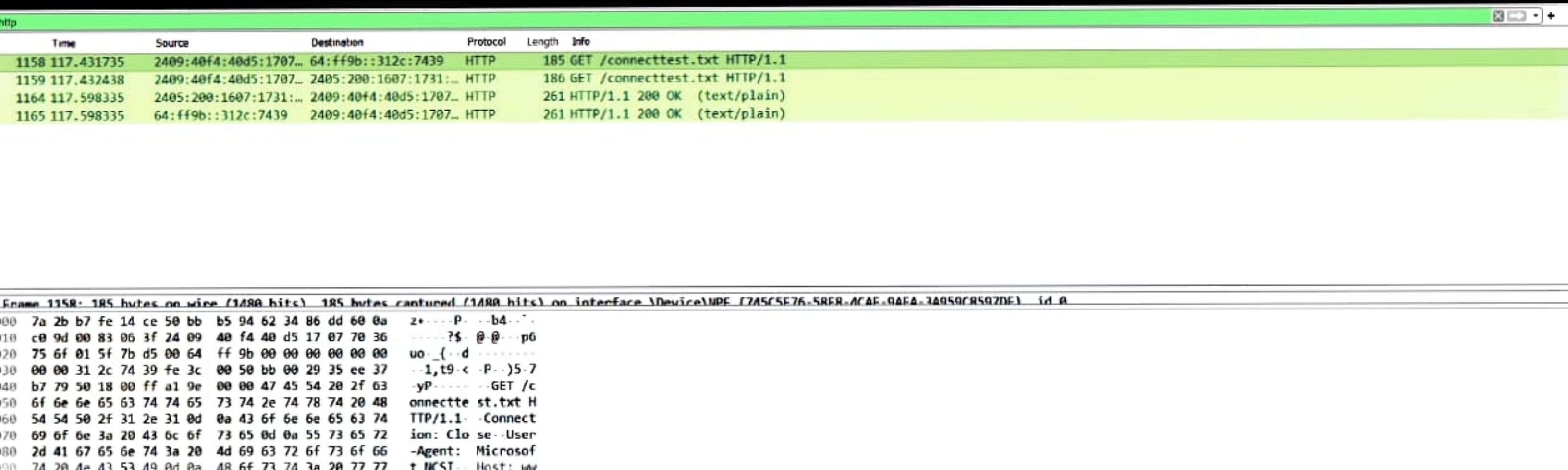
1. open wire shark
2. Click on available interface
3. Choose the LAN interface
4. Click on start button.
5. Active packets will be displayed.
6. Capture the packets & select IP addresses
7. click on IPv4 -> IP address.
8. select the double equals (==)
9. Click on apply button
10. All the packets will be filtered using source address

Result: Hence the capturing of packets using wire shark network analyser was analysed for ARP & HTTP



arp

```
No.      Time          Source               Destination          Protocol  Length  Info
Number   1.729111      7a:2b:b7:fe:14:ce    50:bb:b5:94:62:34    ARP           42 Who has 172.24.49.234? Tell 172.24.49.16
     33  1.729158      50:bb:b5:94:62:34    7a:2b:b7:fe:14:ce    ARP           42 172.24.49.234 is at 50:bb:b5:94:62:34
    136  21.784497     7a:2b:b7:fe:14:ce    Broadcast            ARP           42 Who has 172.24.49.75? Tell 172.24.49.16
    279  24.657339     7a:2b:b7:fe:14:ce    Broadcast            ARP           42 Who has 172.24.49.75? Tell 172.24.49.16
    365  25.822812     7a:2b:b7:fe:14:ce    Broadcast            ARP           42 Who has 172.24.49.75? Tell 172.24.49.16
    408  27.789911     7a:2b:b7:fe:14:ce    50:bb:b5:94:62:34    ARP           42 Who has 172.24.49.234? Tell 172.24.49.16
    409  27.789949     50:bb:b5:94:62:34    7a:2b:b7:fe:14:ce    ARP           42 172.24.49.234 is at 50:bb:b5:94:62:34
    581  54.044036     50:bb:b5:94:62:34    7a:2b:b7:fe:14:ce    ARP           42 Who has 172.24.49.16? Tell 172.24.49.234
    582  54.115846     7a:2b:b7:fe:14:ce    50:bb:b5:94:62:34    ARP           42 172.24.49.16 is at 7a:2b:b7:fe:14:ce
    764  61.326013     7a:2b:b7:fe:14:ce    50:bb:b5:94:62:34    ARP           42 Who has 172.24.49.234? Tell 172.24.49.16
    765  61.326060     50:bb:b5:94:62:34    7a:2b:b7:fe:14:ce    ARP           42 172.24.49.234 is at 50:bb:b5:94:62:34
```



```
       Time        Source                    Destination               Protocol  Length Info
1158 117.431735  2409:40f4:40d5:1707…  64:ff9b::312c:7439        HTTP       185 GET /connecttest.txt HTTP/1.1
1159 117.432438  2409:40f4:40d5:1707…  2405:200:1607:1731:…      HTTP       186 GET /connecttest.txt HTTP/1.1
1164 117.598335  2405:200:1607:1731:…  2409:40f4:40d5:1707…      HTTP       261 HTTP/1.1 200 OK  (text/plain)
1165 117.598335  64:ff9b::312c:7439    2409:40f4:40d5:1707…      HTTP       261 HTTP/1.1 200 OK  (text/plain)
```

```
Frame 1158: 185 bytes on wire (1480 bits), 185 bytes captured (1480 bits) on interface \Device\NPF_{745C5E76-58E8-4CAE-9AEA-3A959C8597DE}, id 0
000  7a 2b b7 fe 14 ce 50 bb  b5 94 62 34 86 dd 60 0a   z+····P· ··b4··`·
010  c0 9d 00 83 06 3f 24 09  40 f4 40 d5 17 07 70 36   ·····?$· @·@···p6
020  75 6f 01 5f 7b d5 00 64  ff 9b 00 00 00 00 00 00   uo·_{··d ········
030  00 00 31 2c 74 39 fe 3c  00 50 bb 00 29 35 ee 37   ··1,t9·< ·P··)5·7
040  b7 79 50 18 00 ff a1 9e  00 00 47 45 54 20 2f 63   ·yP····· ··GET /c
050  6f 6e 6e 65 63 74 74 65  73 74 2e 74 78 74 20 48   onnectte st.txt H
060  54 54 50 2f 31 2e 31 0d  0a 43 6f 6e 6e 65 63 74   TTP/1.1· ·Connect
070  69 6f 6e 3a 20 43 6c 6f  73 65 0d 0a 55 73 65 72   ion: Clo se··User
080  2d 41 67 65 6e 74 3a 20  4d 69 63 72 6f 73 6f 66   -Agent:  Microsof
090  74 20 4e 43 53 49 0d 0a  48 6f 73 74 3a 20 77 77   t NCSI·· Host: ww
```