Practical 9 : Capture ARP & ICMP Protocol Traffic using Wireshark.

Software & Hardwere Requirements:
Wireshark

Knowledge requirements: basic knowledge of wireshark softwere…

Question:

Q-1. What are the features in Wireshark ?

Answer :
The following are some of the many features Wireshark provides:

- Available for UNIX and Windows.
- Capture live packet data from a network interface.
- Open files containing packet data captured with tcpdump/WinDump, Wireshark, and many other packet capture programs.
- Import packets from text files containing hex dumps of packet data.
- Display packets with very detailed protocol information.
- Save packet data captured.
- Export some or all packets in a number of capture file formats.
- Filter packets on many criteria.
- Search for packets on many criteria.
- Colorize packet display based on filters.
- Create various statistics.

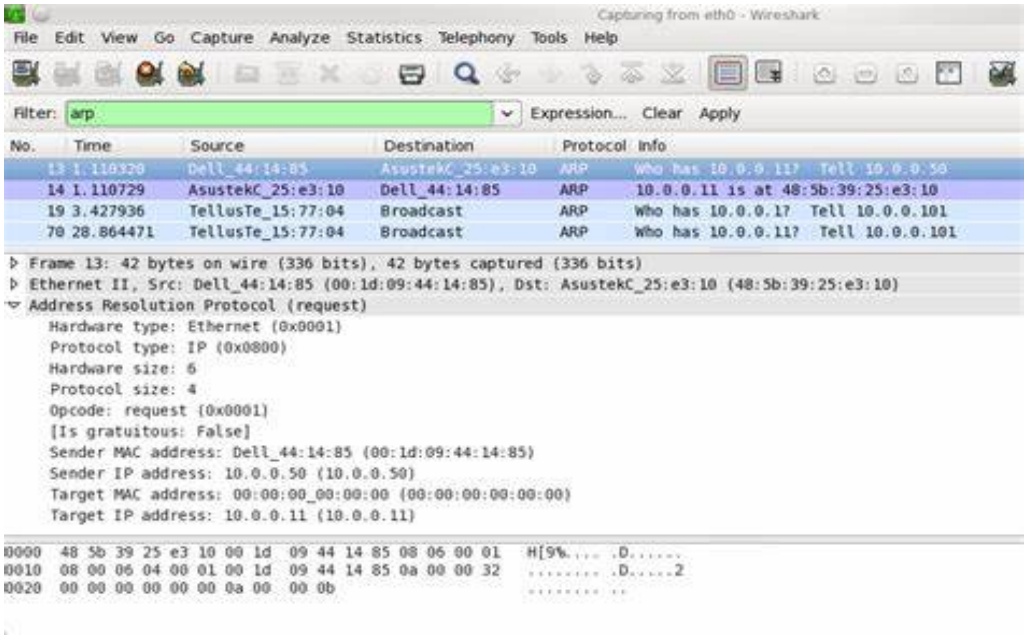
Theory:

To capture ARP traffic:

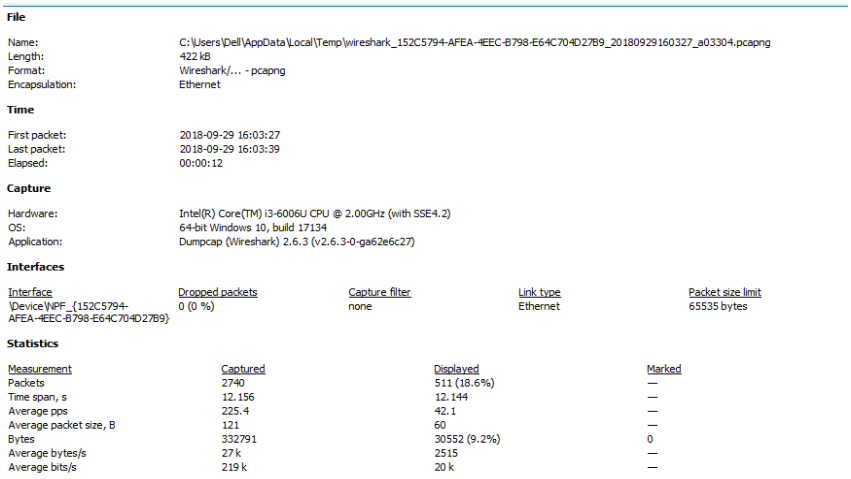
- Start Wireshark, but do not yet start a capture.
- Open an elevated/administrator command prompt.
- Use ipconfig to display the default gateway address. Note the Default Gateway displayed.
- Start a Wireshark capture.
- Use arp -d to clear the ARP cache.
- Use ping <default gateway address> to ping the default gateway address.
- Use arp -a to view the ARP cache and confirm an entry has been added for the default gateway address.
- Close the command prompt.
- Stop the Wireshark capture.

Start a Wireshark capture. Open a Windows console window, and generate some ICMP traffic by using the Ping command line tool to check the connectivity of a neighboring machine (or your home router).

Stop the capture and Wireshark should now look something like Figure 10. The Address Resolution Protocol (ARP) and ICMP packets are difficult to pick out, create a display filter to only show ARP or ICMP packets.



Now, we can find out statics of that particular frame contains each and every information of that particular frame as follows :



File

Name:	C:\Users\Dell\AppData\Local\Temp\wireshark_152C5794-AFEA-4EEC-B798-E64C704D27B9_20180929160327_a03304.pcapng
Length:	422 kB
Format:	Wireshark/... - pcapng
Encapsulation:	Ethernet

Time

First packet:	2018-09-29 16:03:27
Last packet:	2018-09-29 16:03:39
Elapsed:	00:00:12

Capture

Hardware:	Intel(R) Core(TM) i3-6006U CPU @ 2.00GHz (with SSE4.2)
OS:	64-bit Windows 10, build 17134
Application:	Dumpcap (Wireshark) 2.6.3 (v2.6.3-0-ga62e6c27)

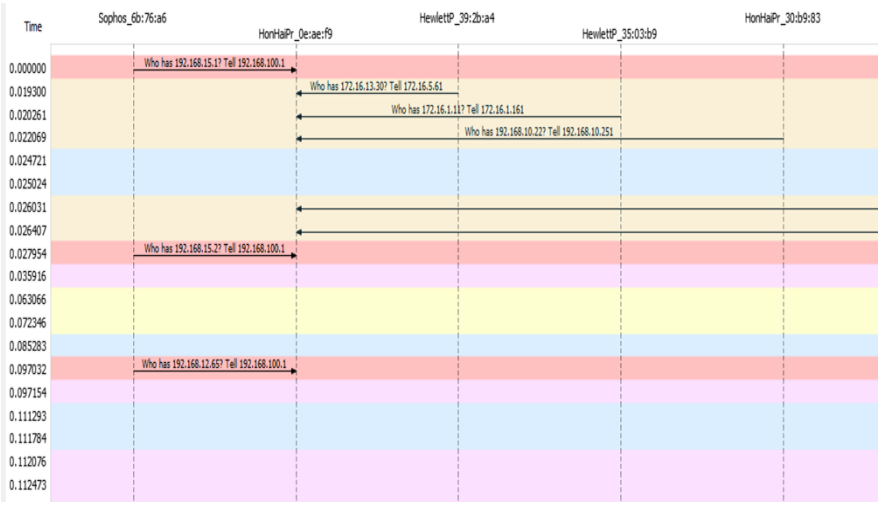
Interfaces

Interface	Dropped packets	Capture filter	Link type	Packet size limit
\Device\NPF_{152C5794-AFEA-4EEC-B798-E64C704D27B9}	0 (0 %)	none	Ethernet	65535 bytes

Statistics

Measurement	Captured	Displayed	Marked
Packets	2740	511 (18.6%)	—
Time span, s	12.156	12.144	—
Average pps	225.4	42.1	—
Average packet size, B	121	60	—
Bytes	332791	30552 (9.2%)	0
Average bytes/s	27 k	2515	—
Average bits/s	219 k	20 k	—

Now, we have flow graph of that frame means how frame passes through each and every component from sender to receiver.

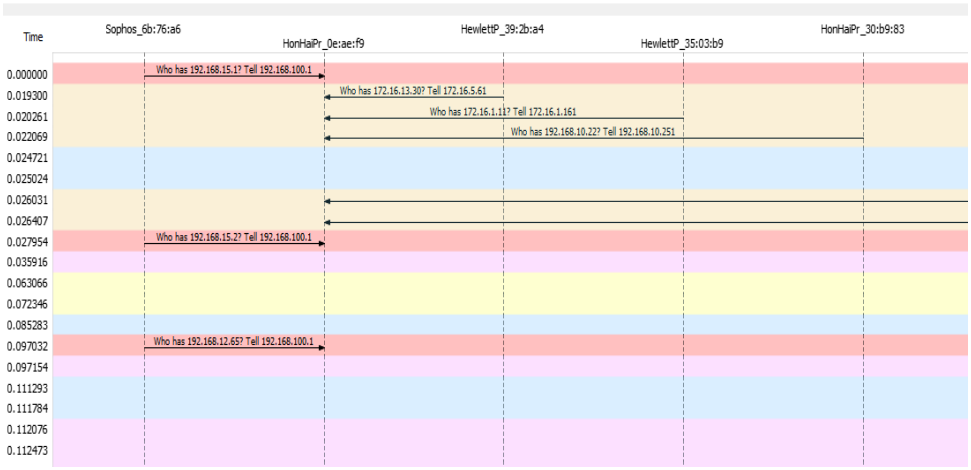


Now , similar things as ARP but now for ICMP:::

```
> Frame 275: 90 bytes on wire (720 bits), 90 bytes captured (720 bits) on interface 0
v Ethernet II, Src: IntelCor_c5:fc:a1 (2c:6e:85:c5:fc:a1), Dst: HonHaiPr_0e:ae:f9 (28:56:5a:0e:ae:f9)
  v Destination: HonHaiPr_0e:ae:f9 (28:56:5a:0e:ae:f9)
      Address: HonHaiPr_0e:ae:f9 (28:56:5a:0e:ae:f9)
      .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
      .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
  v Source: IntelCor_c5:fc:a1 (2c:6e:85:c5:fc:a1)
      Address: IntelCor_c5:fc:a1 (2c:6e:85:c5:fc:a1)
      .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
      .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
    Type: IPv6 (0x86dd)
```

```
v Internet Protocol Version 6, Src: fe80::f9cb:816f:d578:59e3, Dst: ff02::16
    0110 .... = Version: 6
  v .... 0000 0000 .... .... .... .... .... = Traffic Class: 0x00 (DSCP: CS0, ECN: Not-ECT)
      .... 0000 00.. .... .... .... .... .... = Differentiated Services Codepoint: Default (0)
      .... .... ..00 .... .... .... .... .... = Explicit Congestion Notification: Not ECN-Capable Transport (0)
    .... .... .... 0000 0000 0000 0000 0000 = Flow Label: 0x00000
    Payload Length: 36
    Next Header: IPv6 Hop-by-Hop Option (0)
    Hop Limit: 1
    Source: fe80::f9cb:816f:d578:59e3
    Destination: ff02::16
  v IPv6 Hop-by-Hop Option
      Next Header: ICMPv6 (58)
      Length: 0
      [Length: 8 bytes]
    > Router Alert
    > PadN
```

Flow Graph for ICMP frame :



CONCLUSION:

In this practical we study and perform about arp and icmp protocol traffic using wireshark.