EXPERIMENT NO. : 04

Aim: Using wireshark understand the operations of TCP/IP layers:

- Ethernet Layer: Frame header, frame size tec.
- Data Link Layer: MAC address, ARP.
- Network Layer: IP packet(Header, fragmentation, ICMP).
- Transport Layer: TCP Ports, TCP handshake.
- Application Layer: FTP header format.

Theory: Wireshark, a network analysis tool formerly known as Ethereal, captures packets in real time and display them in human-readable format. Wireshark includes filters, color coding, and other features that let you dig deep into network traffic and inspect individual packets. Wireshark can be downloaded from their official website (https://www.wireshark.org/). For the linux users wireshark can be installed from package repositories.

Color Coding: The packets are highlighted in a variety of different colors. Wireshark uses colors to identify the types of traffic at a glance. By default, light purple is TCP traffic, light blue is UDP traffic, and black identifies packets with errors, for example, packets delivered out of order. To view exactly what the color codes mean, click View > Coloring Rules. We can also customize and modify the coloring rules.

Filtering Packets:The most basic way to apply a filter is by typing it into the filter box at the top of the window and clicking Apply (or pressing Enter). For example, type "dns" and you'll see only DNS packets. When you start typing, Wireshark will help you auto complete your filter.

Ethernet Layer: In computer networking, an Ethernet frame is a data link layer protocol data unit and uses the underlying Ethernet physical layer transport mechanisms. In other words, a data unit on an Ethernet link transports an Ethernet frame as its payload.An Ethernet frame is preceded by a preamble and start frame delimiter (SFD), which are both part of the Ethernet packet at the physical layer. Each Ethernet frame starts with an Ethernet header, which contains destination and source MAC addresses as its first two fields. The middle section of the frame is payload data including any headers for other protocols (for example, Internet Protocol) carried in the frame. The frame ends with a frame check sequence (FCS), which is a 32-bit cyclic redundancy check used to detect any in-transit corruption of data.

MAC Addresses are unique 48-bits hardware number of a computer, which is embedded into network card (known as Network Interface Card) during the time of

manufacturing. MAC Address is also known as Physical Address of a network device. In IEEE 802 standard, Data Link Layer is divided into two sublayers -

1. Logical Link Control(LLC) Sublayer
2. Media Access Control(MAC) Sublayer

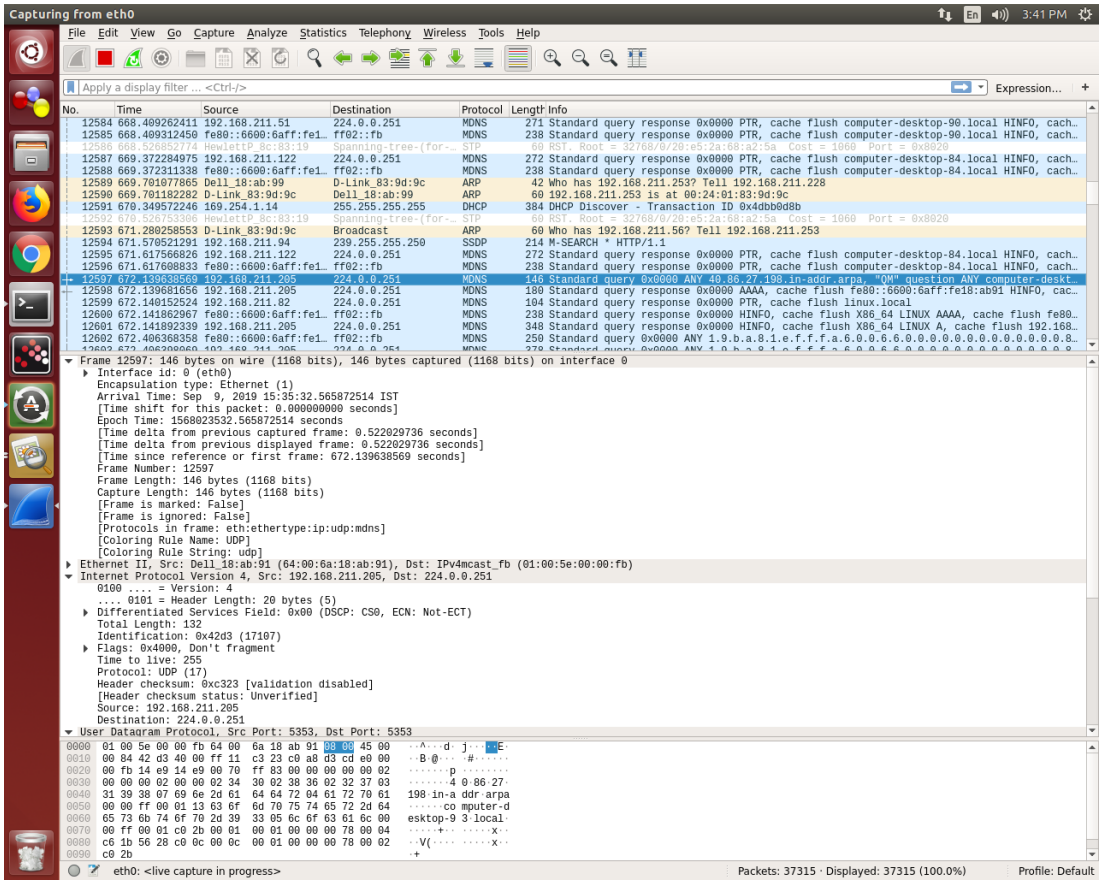
MAC address is used by Media Access Control (MAC) sublayer of Data-Link Layer. MAC Address is word wide unique, since millions of network devices exists and we need to uniquely identify each.

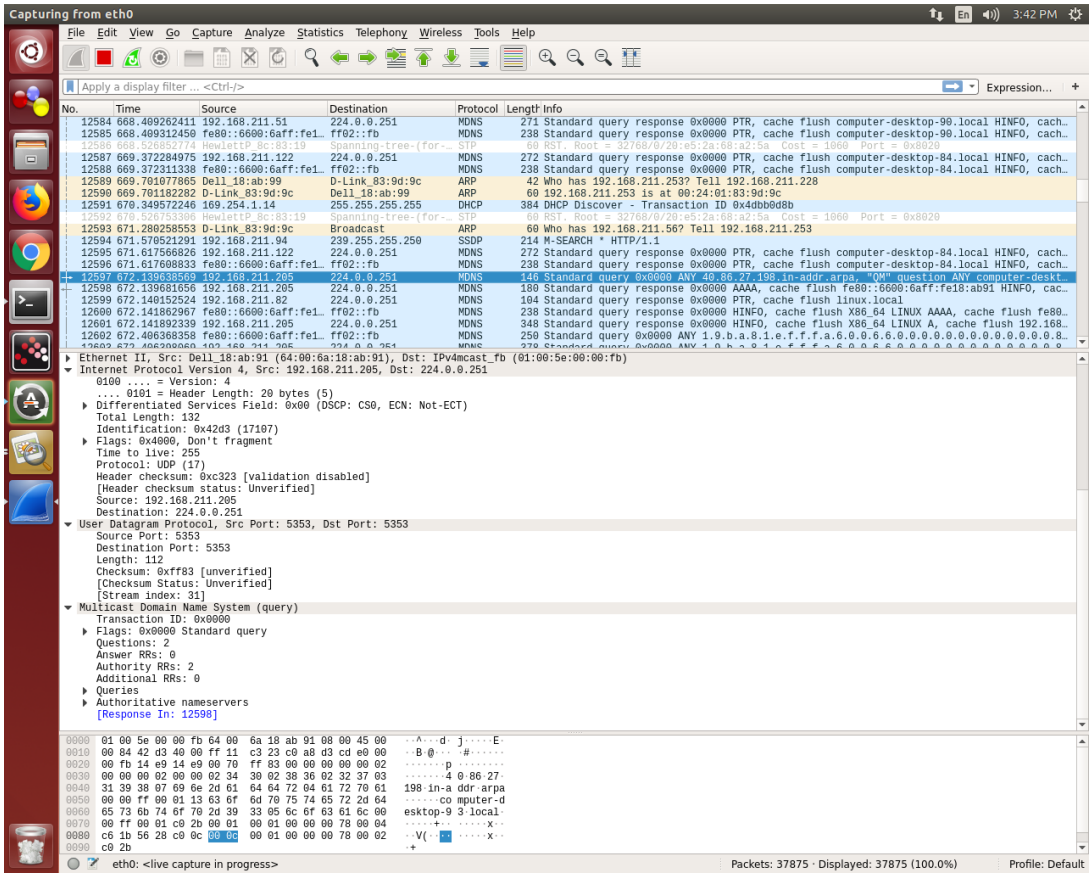
Network Layer :The Ethernet layer is concerned with node to node. The IP layer is concerned with moving between networks, hence the original meaning of the term internetwork, from whence Internet was derived. Highlighting the network layer shows more details. From Figure C, we can see the source and destination IP addresses as well as the IP header length (20 bytes in this case). We can also see the Differentiated Services (DiffServ) area. This would be where extra information relating to the packet's type of service goes. For most packets on a LAN this is set to zero, which means best effort.

Transport Layer :The transport layer is where applications communicate via the use of ports. Figure 4 will show the source port i.e 40519 and the destination port i.e 5001. The header length (32 bytes in this case) and the sequence number are displayed. The sequence number generally will change for each packet.

Application layer (FTP header) :FTP stands for File transfer protocol, which is used to transfer files from one host to other. It makes use of two separate connections (Control and Data connections) before transferring files. It uses TCP as its underlying network.Firstly, the Client (10.10.10.7) makes a request to the Server (78.47.100.174) for transferring a file. After that, 4 to 5, request and response messages are transferred between the two machines. Take a close look at Packet No. 10967, the client makes a request to the server for getting a file named "flag.rar". In the next packet, server tries to send the file to the requested machine. Finally packet no 11091 indicates the transfer of file named "flag.rar" to 10.10.10.7.

Conclusion: Wireshark is used to capture data packets and allows us to perform more precise analysis. The main focus of this tool is observing the data traffic within a network. This tool allows the user to examine their own computer, for protocol errors, problems within the network architecture, discovering and stopping hacker attacks.


Capturing from eth0
3:41 PM
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
Expression...
No. Time Source Destination Protocol Length Info
12584 668.409262411 192.168.211.51 224.0.0.251 MDNS 271 Standard query response 0x0000 PTR, cache flush computer-desktop-90.local HINFO, cach…
12585 668.409312450 fe80::6600:6aff:fe1… ff02::fb MDNS 238 Standard query response 0x0000 PTR, cache flush computer-desktop-90.local HINFO, cach…
12586 669.526852774 HewlettP_8c:83:19 Spanning-tree-(for-… STP 60 RST. Root = 32768/0/20:e5:2a:68:a2:5a Cost = 1060 Port = 0x8020
12587 669.372284975 192.168.211.122 224.0.0.251 MDNS 272 Standard query response 0x0000 PTR, cache flush computer-desktop-84.local HINFO, cach…
12588 669.372311338 fe80::6600:6aff:fe1… ff02::fb MDNS 238 Standard query response 0x0000 PTR, cache flush computer-desktop-84.local HINFO, cach…
12589 669.701077865 Dell_18:ab:99 D-Link_83:9d:9c ARP 42 Who has 192.168.211.253? Tell 192.168.211.228
12590 669.701182282 D-Link_83:9d:9c Dell_18:ab:99 ARP 60 192.168.211.253 is at 00:24:01:83:9d:9c
12591 670.349572246 169.254.1.14 255.255.255.255 DHCP 384 DHCP Discover - Transaction ID 0x4dbb0d8b
12592 670.526753306 HewlettP_8c:83:19 Spanning-tree-(for-… STP 60 RST. Root = 32768/0/20:e5:2a:68:a2:5a Cost = 1060 Port = 0x8020
12593 671.280258553 D-Link_83:9d:9c Broadcast ARP 60 Who has 192.168.211.56? Tell 192.168.211.253
12594 671.570521291 192.168.211.94 239.255.255.250 SSDP 214 M-SEARCH * HTTP/1.1
12595 671.617566826 192.168.211.122 224.0.0.251 MDNS 272 Standard query response 0x0000 PTR, cache flush computer-desktop-84.local HINFO, cach…
12596 671.617608833 fe80::6600:6aff:fe1… ff02::fb MDNS 238 Standard query response 0x0000 PTR, cache flush computer-desktop-84.local HINFO, cach…
12597 672.139638569 192.168.211.205 224.0.0.251 MDNS 146 Standard query 0x0000 ANY 40.86.27.198.in-addr.arpa, "QM" question ANY computer-deskt…
12598 672.139681656 192.168.211.205 224.0.0.251 MDNS 180 Standard query response 0x0000 AAAA, cache flush fe80::6600:6aff:fe18:ab91 HINFO, cac…
12599 672.140152524 192.168.211.82 224.0.0.251 MDNS 104 Standard query response 0x0000 PTR, cache flush linux.local
12600 672.141862967 fe80::6600:6aff:fe1… ff02::fb MDNS 238 Standard query response 0x0000 HINFO, cache flush X86_64 LINUX AAAA, cache flush fe80…
12601 672.141892339 192.168.211.205 224.0.0.251 MDNS 348 Standard query response 0x0000 HINFO, cache flush X86_64 LINUX A, cache flush 192.168…
12602 672.406368358 fe80::6600:6aff:fe1… ff02::fb MDNS 250 Standard query 0x0000 ANY 1.9.b.a.8.1.e.f.f.f.a.6.0.0.6.6.0.0.0.0.0.0.0.0.0.0.0.0.0.8…
Frame 12597: 146 bytes on wire (1168 bits), 146 bytes captured (1168 bits) on interface 0
Interface id: 0 (eth0)
Encapsulation type: Ethernet (1)
Arrival Time: Sep 9, 2019 15:35:32.565872514 IST
[Time shift for this packet: 0.000000000 seconds]
Epoch Time: 1568023532.565872514 seconds
[Time delta from previous captured frame: 0.522029736 seconds]
[Time delta from previous displayed frame: 0.522029736 seconds]
[Time since reference or first frame: 672.139638569 seconds]
Frame Number: 12597
Frame Length: 146 bytes (1168 bits)
Capture Length: 146 bytes (1168 bits)
[Frame is marked: False]
[Frame is ignored: False]
[Protocols in frame: eth:ethertype:ip:udp:mdns]
[Coloring Rule Name: UDP]
[Coloring Rule String: udp]
Ethernet II, Src: Dell_18:ab:91 (64:00:6a:18:ab:91), Dst: IPv4mcast_fb (01:00:5e:00:00:fb)
Internet Protocol Version 4, Src: 192.168.211.205, Dst: 224.0.0.251
0100 .... = Version: 4
.... 0101 = Header Length: 20 bytes (5)
Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
Total Length: 132
Identification: 0x42d3 (17107)
Flags: 0x4000, Don't fragment
Time to live: 255
Protocol: UDP (17)
Header checksum: 0xc323 [validation disabled]
[Header checksum status: Unverified]
Source: 192.168.211.205
Destination: 224.0.0.251
User Datagram Protocol, Src Port: 5353, Dst Port: 5353
0000 01 00 5e 00 00 fb 64 00 6a 18 ab 91 08 00 45 00 ··^···d· j·····E·
0010 00 84 42 d3 40 00 ff 11 c3 23 c0 a8 d3 cd e0 00 ··B·@··· ·#·····
0020 00 fb 14 e9 14 e9 00 70 ff 83 00 00 00 00 02 ·····p ·····
0030 00 00 00 02 00 00 02 34 30 02 38 36 02 32 37 03 ·····4 0·86·27·
0040 31 39 38 07 69 6e 2d 61 64 64 72 04 61 72 70 61 198·in-a ddr·arpa
0050 00 00 ff 00 01 13 63 6f 6d 70 75 74 65 72 2d 64 ·····co mputer-d
0060 65 73 6b 74 6f 70 2d 39 33 05 6c 6f 63 61 6c 00 esktop-9 3·local·
0070 00 ff 00 01 c0 2b 00 01 00 01 00 00 00 78 00 04 ·····+·· ·····x··
0080 c6 1b 56 28 c0 0c 00 0c 00 01 00 00 00 78 00 02 ··V(···· ·····x··
0090 c0 2b ·+
eth0: <live capture in progress>
Packets: 37315 · Displayed: 37315 (100.0%)
Profile: Default


Capturing from eth0
3:42 PM
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
Expression...
No. Time Source Destination Protocol Length Info
12584 668.409262411 192.168.211.51 224.0.0.251 MDNS 271 Standard query response 0x0000 PTR, cache flush computer-desktop-90.local HINFO, cach…
12585 668.409312450 fe80::6600:6aff:fe1… ff02::fb MDNS 238 Standard query response 0x0000 PTR, cache flush computer-desktop-90.local HINFO, cach…
12586 668.526852774 HewlettP_8c:83:19 Spanning-tree-(for-… STP 60 RST. Root = 32768/0/20:e5:2a:68:a2:5a Cost = 1060 Port = 0x8020
12587 669.372284975 192.168.211.122 224.0.0.251 MDNS 272 Standard query response 0x0000 PTR, cache flush computer-desktop-84.local HINFO, cach…
12588 669.372311338 fe80::6600:6aff:fe1… ff02::fb MDNS 238 Standard query response 0x0000 PTR, cache flush computer-desktop-84.local HINFO, cach…
12589 669.701077865 Dell_18:ab:99 D-Link_83:9d:9c ARP 42 Who has 192.168.211.253? Tell 192.168.211.228
12590 669.701182282 D-Link_83:9d:9c Dell_18:ab:99 ARP 60 192.168.211.253 is at 00:24:01:83:9d:9c
12591 670.349572246 169.254.1.14 255.255.255.255 DHCP 384 DHCP Discover - Transaction ID 0x4dbb0d8b
12592 670.526753306 HewlettP_8c:83:19 Spanning-tree-(for-… STP 60 RST. Root = 32768/0/20:e5:2a:68:a2:5a Cost = 1060 Port = 0x8020
12593 671.280258553 D-Link_83:9d:9c Broadcast ARP 60 Who has 192.168.211.56? Tell 192.168.211.253
12594 671.570521291 192.168.211.94 239.255.255.250 SSDP 214 M-SEARCH * HTTP/1.1
12595 671.617566826 192.168.211.122 224.0.0.251 MDNS 272 Standard query response 0x0000 PTR, cache flush computer-desktop-84.local HINFO, cach…
12596 671.617608833 fe80::6600:6aff:fe1… ff02::fb MDNS 238 Standard query response 0x0000 PTR, cache flush computer-desktop-84.local HINFO, cach…
12597 672.139638569 192.168.211.205 224.0.0.251 MDNS 146 Standard query 0x0000 ANY 40.86.27.198.in-addr.arpa, "QM" question ANY computer-deskt…
12598 672.139681656 192.168.211.205 224.0.0.251 MDNS 180 Standard query response 0x0000 AAAA, cache flush fe80::6600:6aff:fe18:ab91 HINFO, cac…
12599 672.140152524 192.168.211.82 224.0.0.251 MDNS 104 Standard query response 0x0000 PTR, cache flush linux.local
12600 672.141862967 fe80::6600:6aff:fe1… ff02::fb MDNS 238 Standard query response 0x0000 HINFO, cache flush X86_64 LINUX AAAA, cache flush fe80…
12601 672.141892339 192.168.211.205 224.0.0.251 MDNS 348 Standard query response 0x0000 HINFO, cache flush X86_64 LINUX A, cache flush 192.168…
12602 672.406368358 fe80::6600:6aff:fe1… ff02::fb MDNS 250 Standard query 0x0000 ANY 1.9.b.a.8.1.e.f.f.f.a.6.0.0.6.6.0.0.0.0.0.0.0.0.0.0.0.0.0.8…
Ethernet II, Src: Dell_18:ab:91 (64:00:6a:18:ab:91), Dst: IPv4mcast_fb (01:00:5e:00:00:fb)
Internet Protocol Version 4, Src: 192.168.211.205, Dst: 224.0.0.251
0100 .... = Version: 4
.... 0101 = Header Length: 20 bytes (5)
Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
Total Length: 132
Identification: 0x42d3 (17107)
Flags: 0x4000, Don't fragment
Time to live: 255
Protocol: UDP (17)
Header checksum: 0xc323 [validation disabled]
[Header checksum status: Unverified]
Source: 192.168.211.205
Destination: 224.0.0.251
User Datagram Protocol, Src Port: 5353, Dst Port: 5353
Source Port: 5353
Destination Port: 5353
Length: 112
Checksum: 0xff83 [unverified]
[Checksum Status: Unverified]
[Stream index: 31]
Multicast Domain Name System (query)
Transaction ID: 0x0000
Flags: 0x0000 Standard query
Questions: 2
Answer RRs: 0
Authority RRs: 2
Additional RRs: 0
Queries
Authoritative nameservers
[Response In: 12598]
0000 01 00 5e 00 00 fb 64 00 6a 18 ab 91 08 00 45 00 ··^···d· j·····E·
0010 00 84 42 d3 40 00 ff 11 c3 23 c0 a8 d3 cd e0 00 ··B·@··· ·#·····
0020 00 fb 14 e9 14 e9 00 70 ff 83 00 00 00 00 02 ·····p ·····
0030 00 00 00 02 00 00 02 34 30 02 38 36 02 32 37 03 ·····4 0·86·27·
0040 31 39 38 07 69 6e 2d 61 64 64 72 04 61 72 70 61 198·in-a ddr·arpa
0050 00 00 ff 00 01 13 63 6f 6d 70 75 74 65 72 2d 64 ·····co mputer-d
0060 65 73 6b 74 6f 70 2d 39 33 05 6c 6f 63 61 6c 00 esktop-9 3·local·
0070 00 ff 00 01 c0 2b 00 01 00 01 00 00 00 78 00 04 ·····+·· ·····x··
0080 c6 1b 56 28 c0 0c 00 0c 00 01 00 00 00 78 00 02 ··V(···· ·····x··
0090 c0 2b ·+
eth0: <live capture in progress>
Packets: 37875 · Displayed: 37875 (100.0%)
Profile: Default