Batch: SYIT A4 **Experiment Number: 3**

Roll Number: 16010423099 **Name: Suryanshu Banerjee**

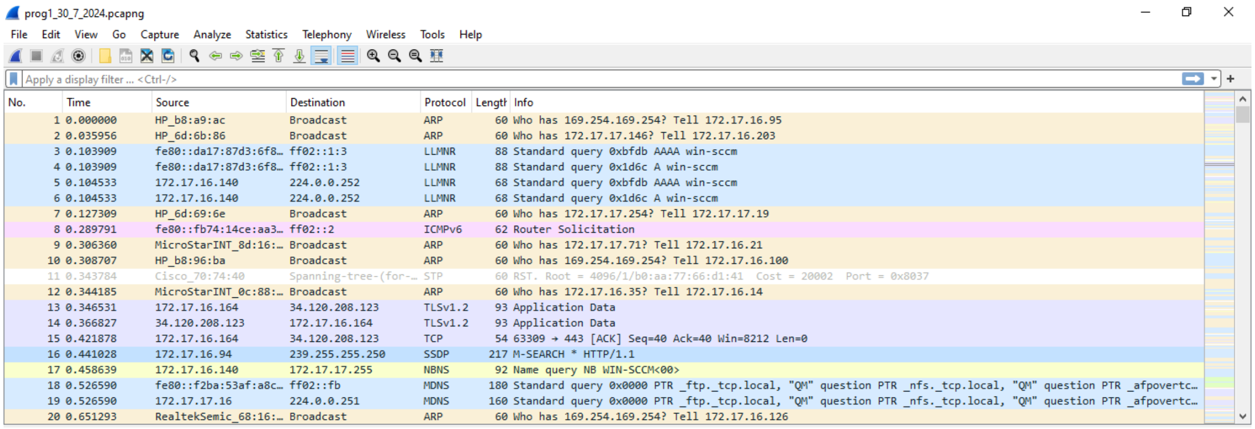
Aim of the Experiment: To explore application layer protocols with packet analysis using Wireshark.

Program/ Steps:

As instructed by the document, taken screenshots for
1. Capturing a packet.
2. Color coding of different protocols.
3. Statistics for the application layer protocol chosen.

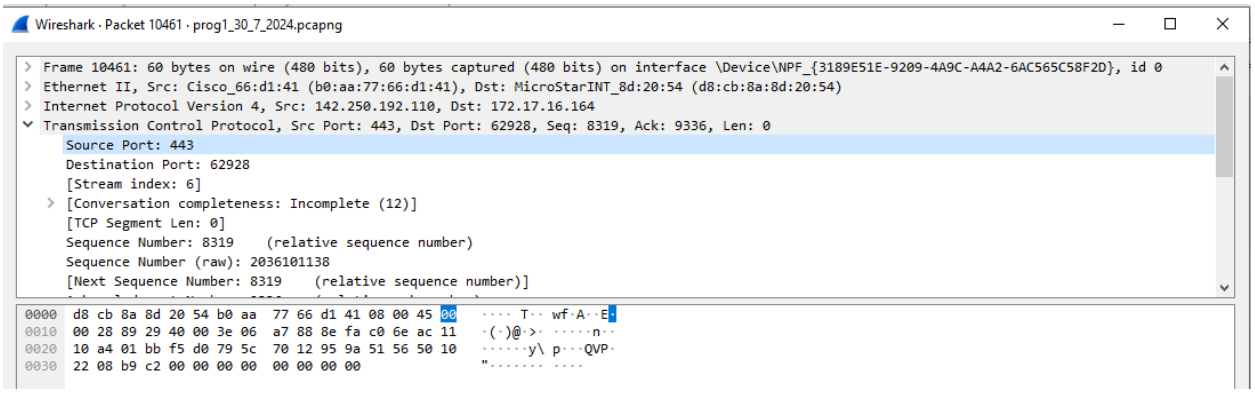
Output/Result:

Capturing a Packet



prog1_30_7_2024.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>

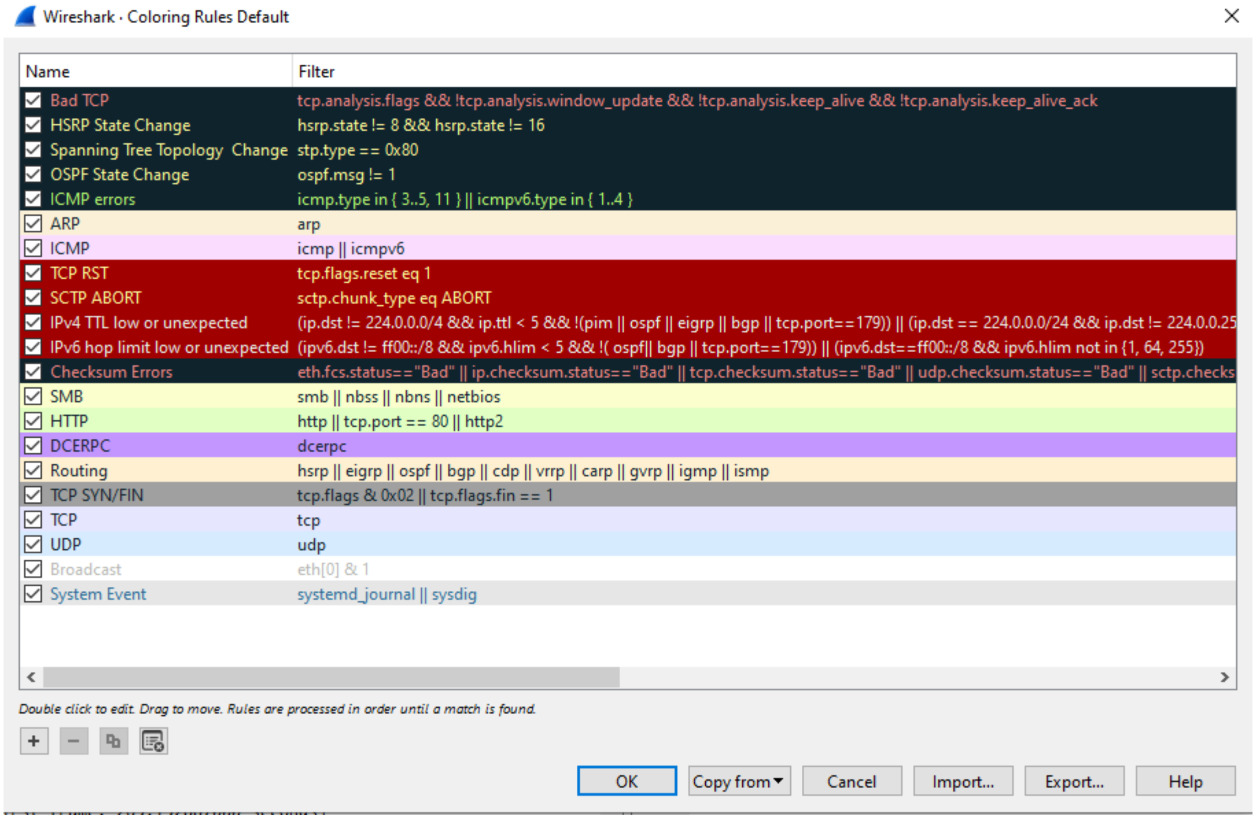
No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	HP_b8:a9:ac	Broadcast	ARP	60	Who has 169.254.169.254? Tell 172.17.16.95
2	0.035956	HP_6d:6b:86	Broadcast	ARP	60	Who has 172.17.17.146? Tell 172.17.16.203
3	0.103909	fe80::da17:87d3:6f8…	ff02::1:3	LLMNR	88	Standard query 0xbfdb AAAA win-sccm
4	0.103909	fe80::da17:87d3:6f8…	ff02::1:3	LLMNR	88	Standard query 0x1d6c A win-sccm
5	0.104533	172.17.16.140	224.0.0.252	LLMNR	68	Standard query 0xbfdb AAAA win-sccm
6	0.104533	172.17.16.140	224.0.0.252	LLMNR	68	Standard query 0x1d6c A win-sccm
7	0.127309	HP_6d:69:6e	Broadcast	ARP	60	Who has 172.17.17.254? Tell 172.17.17.19
8	0.289791	fe80::fb74:14ce:aa3…	ff02::2	ICMPv6	62	Router Solicitation
9	0.306360	MicroStarINT_8d:16:…	Broadcast	ARP	60	Who has 172.17.17.71? Tell 172.17.16.21
10	0.308707	HP_b8:96:ba	Broadcast	ARP	60	Who has 169.254.169.254? Tell 172.17.16.100
11	0.343784	Cisco_70:74:40	Spanning-tree-(for-…	STP	60	RST. Root = 4096/1/b0:aa:77:66:d1:41 Cost = 20002 Port = 0x8037
12	0.344185	MicroStarINT_0c:88:…	Broadcast	ARP	60	Who has 172.17.16.35? Tell 172.17.16.14
13	0.346531	172.17.16.164	34.120.208.123	TLSv1.2	93	Application Data
14	0.366827	34.120.208.123	172.17.16.164	TLSv1.2	93	Application Data
15	0.421878	172.17.16.164	34.120.208.123	TCP	54	63309 → 443 [ACK] Seq=40 Ack=40 Win=8212 Len=0
16	0.441028	172.17.16.94	239.255.255.250	SSDP	217	M-SEARCH * HTTP/1.1
17	0.458639	172.17.16.140	172.17.17.255	NBNS	92	Name query NB WIN-SCCM<00>
18	0.526590	fe80::f2ba:53af:a8c…	ff02::fb	MDNS	180	Standard query 0x0000 PTR _ftp._tcp.local, "QM" question PTR _nfs._tcp.local, "QM" question PTR _afpovertc…
19	0.526590	172.17.17.16	224.0.0.251	MDNS	160	Standard query 0x0000 PTR _ftp._tcp.local, "QM" question PTR _nfs._tcp.local, "QM" question PTR _afpovertc…
20	0.651293	RealtekSemic_68:16:…	Broadcast	ARP	60	Who has 169.254.169.254? Tell 172.17.16.126



```
> Frame 10461: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface \Device\NPF_{3189E51E-9209-4A9C-A4A2-6AC565C58F2D}, id 0
> Ethernet II, Src: Cisco_66:d1:41 (b0:aa:77:66:d1:41), Dst: MicroStarINT_8d:20:54 (d8:cb:8a:8d:20:54)
> Internet Protocol Version 4, Src: 142.250.192.110, Dst: 172.17.16.164
v Transmission Control Protocol, Src Port: 443, Dst Port: 62928, Seq: 8319, Ack: 9336, Len: 0
    Source Port: 443
    Destination Port: 62928
    [Stream index: 6]
  > [Conversation completeness: Incomplete (12)]
    [TCP Segment Len: 0]
    Sequence Number: 8319    (relative sequence number)
    Sequence Number (raw): 2036101138
    [Next Sequence Number: 8319    (relative sequence number)]

0000  d8 cb 8a 8d 20 54 b0 aa  77 66 d1 41 08 00 45 00   ···· T·· wf·A··E·
0010  00 28 89 29 40 00 3e 06  a7 88 8e fa c0 6e ac 11   ·(·)@·>· ·····n··
0020  10 a4 01 bb f5 d0 79 5c  70 12 95 9a 51 56 50 10   ······y\ p···QVP·
0030  22 08 b9 c2 00 00 00 00  00 00 00 00              "······· ····
```

Viewing the Color Codes for Different Protocols

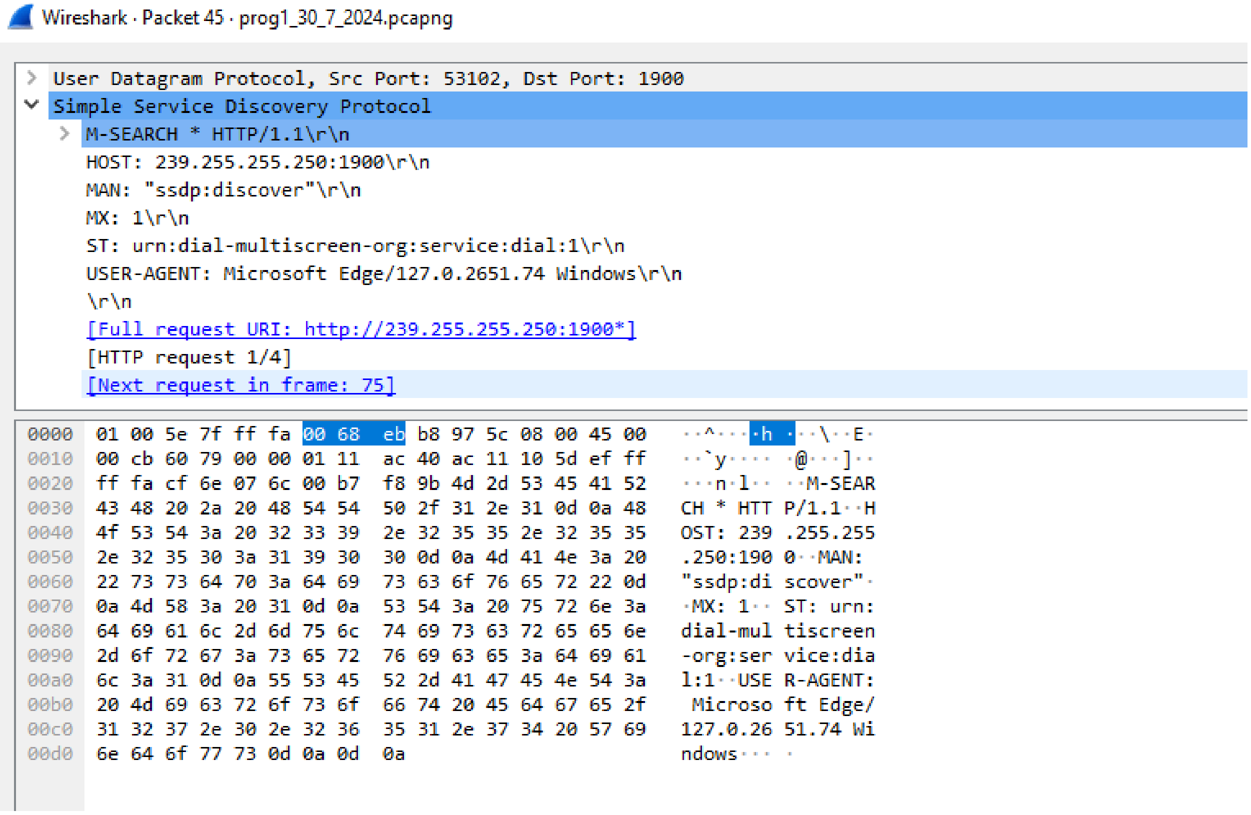


Wireshark · Coloring Rules Default

<table>
<tr><th>Name</th><th>Filter</th></tr>
<tr><td>☑ Bad TCP</td><td>tcp.analysis.flags && !tcp.analysis.window_update && !tcp.analysis.keep_alive && !tcp.analysis.keep_alive_ack</td></tr>
<tr><td>☑ HSRP State Change</td><td>hsrp.state != 8 && hsrp.state != 16</td></tr>
<tr><td>☑ Spanning Tree Topology Change</td><td>stp.type == 0x80</td></tr>
<tr><td>☑ OSPF State Change</td><td>ospf.msg != 1</td></tr>
<tr><td>☑ ICMP errors</td><td>icmp.type in { 3..5, 11 } || icmpv6.type in { 1..4 }</td></tr>
<tr><td>☑ ARP</td><td>arp</td></tr>
<tr><td>☑ ICMP</td><td>icmp || icmpv6</td></tr>
<tr><td>☑ TCP RST</td><td>tcp.flags.reset eq 1</td></tr>
<tr><td>☑ SCTP ABORT</td><td>sctp.chunk_type eq ABORT</td></tr>
<tr><td>☑ IPv4 TTL low or unexpected</td><td>(ip.dst != 224.0.0.0/4 && ip.ttl < 5 && !(pim || ospf || eigrp || bgp || tcp.port==179)) || (ip.dst == 224.0.0.0/24 && ip.dst != 224.0.0.25</td></tr>
<tr><td>☑ IPv6 hop limit low or unexpected</td><td>(ipv6.dst != ff00::/8 && ipv6.hlim < 5 && !(ospf|| bgp || tcp.port==179)) || (ipv6.dst==ff00::/8 && ipv6.hlim not in {1, 64, 255})</td></tr>
<tr><td>☑ Checksum Errors</td><td>eth.fcs.status=="Bad" || ip.checksum.status=="Bad" || tcp.checksum.status=="Bad" || udp.checksum.status=="Bad" || sctp.checks</td></tr>
<tr><td>☑ SMB</td><td>smb || nbss || nbns || netbios</td></tr>
<tr><td>☑ HTTP</td><td>http || tcp.port == 80 || http2</td></tr>
<tr><td>☑ DCERPC</td><td>dcerpc</td></tr>
<tr><td>☑ Routing</td><td>hsrp || eigrp || ospf || bgp || cdp || vrrp || carp || gvrp || igmp || ismp</td></tr>
<tr><td>☑ TCP SYN/FIN</td><td>tcp.flags & 0x02 || tcp.flags.fin == 1</td></tr>
<tr><td>☑ TCP</td><td>tcp</td></tr>
<tr><td>☑ UDP</td><td>udp</td></tr>
<tr><td>☑ Broadcast</td><td>eth[0] & 1</td></tr>
<tr><td>☑ System Event</td><td>systemd_journal || sysdig</td></tr>
</table>

Double click to edit. Drag to move. Rules are processed in order until a match is found.

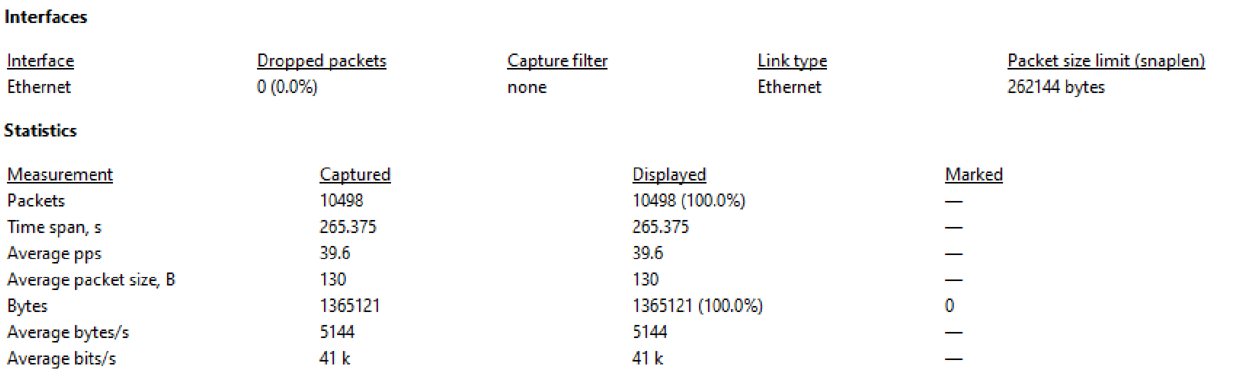
Viewing the Statistics of the Application Layer Protocol Chosen (SSDP)



Wireshark · Packet 45 · prog1_30_7_2024.pcapng

```
> User Datagram Protocol, Src Port: 53102, Dst Port: 1900
v Simple Service Discovery Protocol
  > M-SEARCH * HTTP/1.1\r\n
    HOST: 239.255.255.250:1900\r\n
    MAN: "ssdp:discover"\r\n
    MX: 1\r\n
    ST: urn:dial-multiscreen-org:service:dial:1\r\n
    USER-AGENT: Microsoft Edge/127.0.2651.74 Windows\r\n
    \r\n
    [Full request URI: http://239.255.255.250:1900*]
    [HTTP request 1/4]
    [Next request in frame: 75]
```

```
0000  01 00 5e 7f ff fa 00 68  eb b8 97 5c 08 00 45 00   ··^····h ···\··E·
0010  00 cb 60 79 00 00 01 11  ac 40 ac 11 10 5d ef ff   ··`y···· ·@···]··
0020  ff fa cf 6e 07 6c 00 b7  f8 9b 4d 2d 53 45 41 52   ···n·l·· ··M-SEAR
0030  43 48 20 2a 20 48 54 54  50 2f 31 2e 31 0d 0a 48   CH * HTT P/1.1··H
0040  4f 53 54 3a 20 32 33 39  2e 32 35 35 2e 32 35 35   OST: 239 .255.255
0050  2e 32 35 30 3a 31 39 30  30 0d 0a 4d 41 4e 3a 20   .250:190 0··MAN: 
0060  22 73 73 64 70 3a 64 69  73 63 6f 76 65 72 22 0d   "ssdp:di scover"·
0070  0a 4d 58 3a 20 31 0d 0a  53 54 3a 20 75 72 6e 3a   ·MX: 1·· ST: urn:
0080  64 69 61 6c 2d 6d 75 6c  74 69 73 63 72 65 65 6e   dial-mul tiscreen
0090  2d 6f 72 67 3a 73 65 72  76 69 63 65 3a 64 69 61   -org:ser vice:dia
00a0  6c 3a 31 0d 0a 55 53 45  52 2d 41 47 45 4e 54 3a   l:1··USE R-AGENT:
00b0  20 4d 69 63 72 6f 73 6f  66 74 20 45 64 67 65 2f    Microso ft Edge/
00c0  31 32 37 2e 30 2e 32 36  35 31 2e 37 34 20 57 69   127.0.26 51.74 Wi
00d0  6e 64 6f 77 73 0d 0a 0d  0a                        ndows··· ·
```



Interfaces

Interface	Dropped packets	Capture filter	Link type	Packet size limit (snaplen)
Ethernet	0 (0.0%)	none	Ethernet	262144 bytes

Statistics

Measurement	Captured	Displayed	Marked
Packets	10498	10498 (100.0%)	—
Time span, s	265.375	265.375	—
Average pps	39.6	39.6	—
Average packet size, B	130	130	—
Bytes	1365121	1365121 (100.0%)	0
Average bytes/s	5144	5144	—
Average bits/s	41 k	41 k	—

Post Lab Question-Answers:

1. What is the difference between Wireshark software and NMAP software?

Answer: Nmap primarily focuses on scanning and discovering network hosts and services. Wireshark specializes in deep packet analysis.

2. At which of the OSI layer Wireshark runs?

Answer: Gives you output on Application layer but captures data in Data Link Layer

3. Just write down the names of the softwares which have similar functionality as Wireshark. (open source or proprietary)

Answer: tcpdump, etherape

Outcomes:

CO2: Enumerate the layers of the OSI model and TCP/IP model, their functions and Protocols

Conclusion (based on the Results and outcomes achieved):

Wireshark helped understand the role of packet inspection in understanding and troubleshooting network communication.

References:

- Behrouz A Forouzan, “Data Communication and networking”, Tata McGraw hill, India, 4th Edition
- http://www.wireshark.org
- Wireshark user manual.