Academic Year: 2022-2023

Name:	Prerna Sunil Jadhav
Sap Id:	60004220127
Class:	S. Y. B.Tech (Computer Engineering)
Course:	Computer Networks (DJ12CEL405)
Date of Performance:	
Date of Submission:	
Experiment No.:	09
Aim:	Packet Capturing In Wireshark

AIM: **TO IMPLEMENT AND SIMULATE PACKET CAPTURING IN WIRESHARK.**

THEORY:

- ✓ A packet is a unit of data which is transmitted over a network between the origin and the destination.
- ✓ Network packets are small, i.e., maximum 1.5 Kilobytes for Ethernet packets and 64 Kilobytes for IP packets. The data packets in the Wireshark can be viewed online and can be analyzed offline.
- ✓ Packet capturing and analyzing are essential tasks in computer networking, especially in troubleshooting network problems and securing the network from malicious attacks. Here are some notes on packet capturing and analyzing in computer networking:
  - Packet capturing: Packet capturing is the process of intercepting and collecting network traffic data packets for analysis. Packet capturing tools are used to capture packets passing through a specific network interface. Some popular packet capturing tools include Wireshark, tcpdump, and Microsoft Network Monitor.
  - Packet analysis: Packet analysis involves examining the captured packets to understand the network traffic patterns, identify issues, and pinpoint the source of problems. Packet analysis tools are used to analyze the captured packets to gain insight into the network traffic, identify performance issues, and detect potential security threats. Some popular packet analysis tools include Wireshark, Microsoft Message Analyzer, and Network Miner.
  - Protocols: Network traffic consists of packets of data that are exchanged between different devices using different protocols. Popular protocols include TCP, UDP, HTTP, DNS, SMTP, FTP, and ICMP. Understanding the protocols used in network traffic is essential to perform effective packet analysis.
  - Filters: Packet filtering is the process of selecting and analyzing packets based on specific criteria. Packet filtering tools allow users to filter packets based on protocols, source and destination addresses, port numbers, and other parameters. This helps in isolating specific packets for analysis and improving the efficiency of packet analysis.
  - Security: Packet capturing and analysing can also be used for security purposes, such as detecting and preventing cyber-attacks. Network administrators can use packet

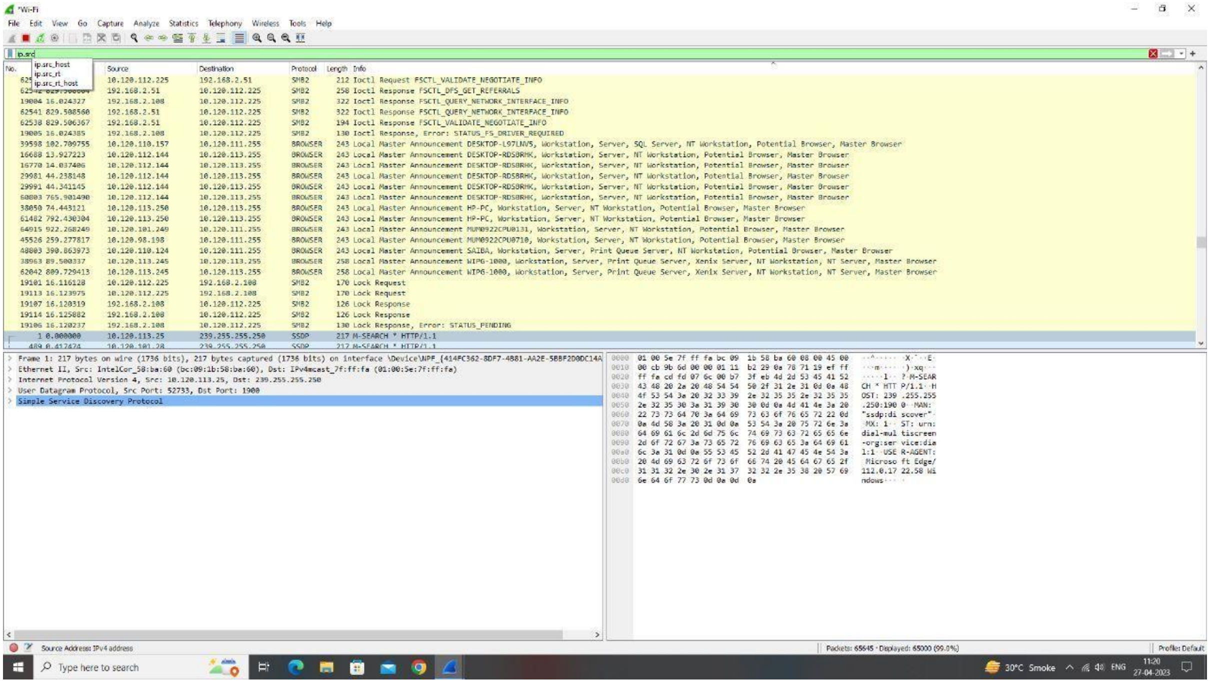
analysis to identify and block malicious traffic, analyse security threats, and detect intrusions.

- ✓ Wireshark is an open-source packet analyzer, which is used for education, analysis, software development, communication protocol development, and network troubleshooting.
- ✓ It is used to track the packets so that each one is filtered to meet our specific needs. It is commonly called as a sniffer, network protocol analyzer, and network analyzer. It is also used by network security engineers to examine security problems.
- ✓ Wireshark is a free to use application which is used to apprehend the data back and forth. It is often called as a free packet sniffer computer application. It puts the network card into an unselective mode, i.e., to accept all the packets which it receives.
- ✓ Uses of Wireshark:
  1. It is used by network security engineers to examine security problems.
  2. It allows the users to watch all the traffic being passed over the network.
  3. It is used by network engineers to troubleshoot network issues.
  4. It also helps to troubleshoot latency issues and malicious activities on your network.
  5. It can also analyze dropped packets.
  6. It helps us to know how all the devices like laptop, mobile phones, desktop, switch, routers, etc., communicate in a local network or the rest of the world.

Filters in Wireshark

1. Ip:

   a. Src


*Wi-Fi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
ip.src
ip.src_host
ip.src_rt
ip.src_rt_host
Type here to search
30°C Smoke ENG 11:20 27-04-2023

```
No.    Time        Source           Destination      Protocol Length Info
625                10.120.112.225   192.168.2.51     SMB2     212 Ioctl Request FSCTL_VALIDATE_NEGOTIATE_INFO
625                192.168.2.51     10.120.112.225   SMB2     258 Ioctl Response FSCTL_DFS_GET_REFERRALS
19004 16.024327    192.168.2.108    10.120.112.225   SMB2     322 Ioctl Response FSCTL_QUERY_NETWORK_INTERFACE_INFO
62541 829.508560   192.168.2.51     10.120.112.225   SMB2     322 Ioctl Response FSCTL_QUERY_NETWORK_INTERFACE_INFO
62538 829.506367   192.168.2.51     10.120.112.225   SMB2     194 Ioctl Response FSCTL_VALIDATE_NEGOTIATE_INFO
19005 16.024385    192.168.2.108    10.120.112.225   SMB2     130 Ioctl Response, Error: STATUS_FS_DRIVER_REQUIRED
39598 102.709755   10.120.110.157   10.120.111.255   BROWSER  243 Local Master Announcement DESKTOP-L97LNV5, Workstation, Server, SQL Server, NT Workstation, Potential Browser, Master Browser
16688 13.927223    10.120.112.144   10.120.113.255   BROWSER  243 Local Master Announcement DESKTOP-RDSBRHK, Workstation, Server, NT Workstation, Potential Browser, Master Browser
16770 14.037406    10.120.112.144   10.120.113.255   BROWSER  243 Local Master Announcement DESKTOP-RDSBRHK, Workstation, Server, NT Workstation, Potential Browser, Master Browser
29981 44.238148    10.120.112.144   10.120.113.255   BROWSER  243 Local Master Announcement DESKTOP-RDSBRHK, Workstation, Server, NT Workstation, Potential Browser, Master Browser
29991 44.341145    10.120.112.144   10.120.113.255   BROWSER  243 Local Master Announcement DESKTOP-RDSBRHK, Workstation, Server, NT Workstation, Potential Browser, Master Browser
60803 765.901490   10.120.112.144   10.120.113.255   BROWSER  243 Local Master Announcement DESKTOP-RDSBRHK, Workstation, Server, NT Workstation, Potential Browser, Master Browser
38050 74.443121    10.120.113.250   10.120.113.255   BROWSER  243 Local Master Announcement HP-PC, Workstation, Server, NT Workstation, Potential Browser, Master Browser
61482 792.430304   10.120.113.250   10.120.113.255   BROWSER  243 Local Master Announcement HP-PC, Workstation, Server, NT Workstation, Potential Browser, Master Browser
64915 922.268249   10.120.101.249   10.120.111.255   BROWSER  243 Local Master Announcement MUM0922CPU0131, Workstation, Server, NT Workstation, Potential Browser, Master Browser
45526 259.277817   10.120.98.198    10.120.111.255   BROWSER  243 Local Master Announcement MUM0922CPU0710, Workstation, Server, NT Workstation, Potential Browser, Master Browser
48803 390.863973   10.120.110.124   10.120.111.255   BROWSER  243 Local Master Announcement SAIBA, Workstation, Server, Print Queue Server, NT Workstation, Potential Browser, Master Browser
38963 89.500337    10.120.113.245   10.120.113.255   BROWSER  258 Local Master Announcement WIPG-1000, Workstation, Server, Print Queue Server, Xenix Server, NT Workstation, NT Server, Master Browser
62042 809.729413   10.120.113.245   10.120.113.255   BROWSER  258 Local Master Announcement WIPG-1000, Workstation, Server, Print Queue Server, Xenix Server, NT Workstation, NT Server, Master Browser
19101 16.116128    10.120.112.225   192.168.2.108    SMB2     170 Lock Request
19113 16.123975    10.120.112.225   192.168.2.108    SMB2     170 Lock Request
19107 16.120319    192.168.2.108    10.120.112.225   SMB2     126 Lock Response
19114 16.125882    192.168.2.108    10.120.112.225   SMB2     126 Lock Response
19106 16.120237    192.168.2.108    10.120.112.225   SMB2     130 Lock Response, Error: STATUS_PENDING
    1 0.000000     10.120.113.25    239.255.255.250  SSDP     217 M-SEARCH * HTTP/1.1
  489 0.417474     10.120.101.28    239.255.255.250  SSDP     217 M-SEARCH * HTTP/1.1
```

```
> Frame 1: 217 bytes on wire (1736 bits), 217 bytes captured (1736 bits) on interface \Device\NPF_{414FC362-8DF7-4881-AA2E-5BBF2D0DC14A
> Ethernet II, Src: IntelCor_58:ba:60 (bc:09:1b:58:ba:60), Dst: IPv4mcast_7f:ff:fa (01:00:5e:7f:ff:fa)
> Internet Protocol Version 4, Src: 10.120.113.25, Dst: 239.255.255.250
> User Datagram Protocol, Src Port: 52733, Dst Port: 1900
> Simple Service Discovery Protocol
```

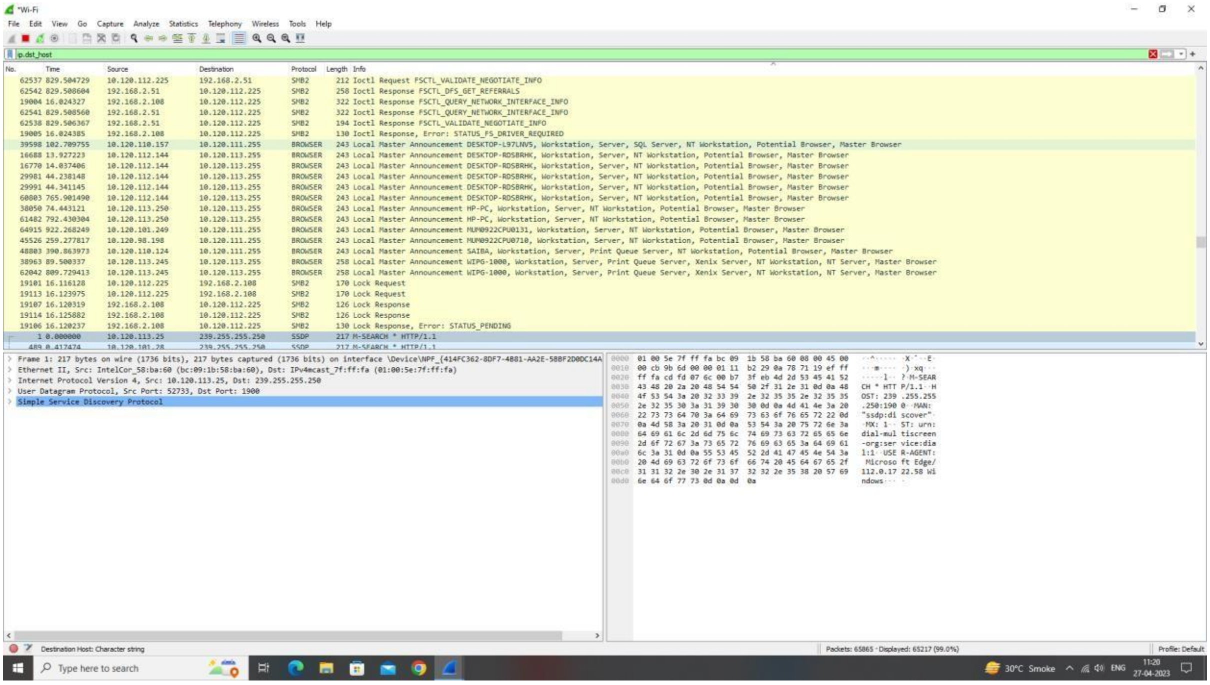
```
0000  01 00 5e 7f ff fa bc 09  1b 58 ba 60 08 00 45 00   ··^·····X·`··E·
0010  00 cb 9b 6d 00 00 01 11  b2 29 0a 78 71 19 ef ff   ···m·····)·xq···
0020  ff fa cd fd 07 6c 00 b7  3f eb 4d 2d 53 45 41 52   ·····l··?·M-SEAR
0030  43 48 20 2a 20 48 54 54  50 2f 31 2e 31 0d 0a 48   CH * HTT P/1.1··H
0040  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 31 32 2e 30 2e 31 37  32 32 2e 35 38 20 57 69   112.0.17 22.58 Wi
00d0  6e 64 6f 77 73 0d 0a 0d  0a                        ndows····
```

Source Address: IPv4 address

Packets: 65645 · Displayed: 65000 (99.0%)

Profile: Default

   b. Dst


*Wi-Fi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Type here to search
30°C Smoke ENG 11:20 27-04-2023

ip.dst_host

```
No.    Time        Source           Destination      Protocol Length Info
62537 829.504729   10.120.112.225   192.168.2.51     SMB2     212 Ioctl Request FSCTL_VALIDATE_NEGOTIATE_INFO
62542 829.508604   192.168.2.51     10.120.112.225   SMB2     258 Ioctl Response FSCTL_DFS_GET_REFERRALS
19004 16.024327    192.168.2.108    10.120.112.225   SMB2     322 Ioctl Response FSCTL_QUERY_NETWORK_INTERFACE_INFO
62541 829.508560   192.168.2.51     10.120.112.225   SMB2     322 Ioctl Response FSCTL_QUERY_NETWORK_INTERFACE_INFO
62538 829.506367   192.168.2.51     10.120.112.225   SMB2     194 Ioctl Response FSCTL_VALIDATE_NEGOTIATE_INFO
19005 16.024385    192.168.2.108    10.120.112.225   SMB2     130 Ioctl Response, Error: STATUS_FS_DRIVER_REQUIRED
39598 102.709755   10.120.110.157   10.120.111.255   BROWSER  243 Local Master Announcement DESKTOP-L97LNV5, Workstation, Server, SQL Server, NT Workstation, Potential Browser, Master Browser
16688 13.927223    10.120.112.144   10.120.113.255   BROWSER  243 Local Master Announcement DESKTOP-RDSBRHK, Workstation, Server, NT Workstation, Potential Browser, Master Browser
16770 14.037406    10.120.112.144   10.120.113.255   BROWSER  243 Local Master Announcement DESKTOP-RDSBRHK, Workstation, Server, NT Workstation, Potential Browser, Master Browser
29981 44.238148    10.120.112.144   10.120.113.255   BROWSER  243 Local Master Announcement DESKTOP-RDSBRHK, Workstation, Server, NT Workstation, Potential Browser, Master Browser
29991 44.341145    10.120.112.144   10.120.113.255   BROWSER  243 Local Master Announcement DESKTOP-RDSBRHK, Workstation, Server, NT Workstation, Potential Browser, Master Browser
60803 765.901490   10.120.112.144   10.120.113.255   BROWSER  243 Local Master Announcement DESKTOP-RDSBRHK, Workstation, Server, NT Workstation, Potential Browser, Master Browser
38050 74.443121    10.120.113.250   10.120.113.255   BROWSER  243 Local Master Announcement HP-PC, Workstation, Server, NT Workstation, Potential Browser, Master Browser
61482 792.430304   10.120.113.250   10.120.113.255   BROWSER  243 Local Master Announcement HP-PC, Workstation, Server, NT Workstation, Potential Browser, Master Browser
64915 922.268249   10.120.101.249   10.120.111.255   BROWSER  243 Local Master Announcement MUM0922CPU0131, Workstation, Server, NT Workstation, Potential Browser, Master Browser
45526 259.277817   10.120.98.198    10.120.111.255   BROWSER  243 Local Master Announcement MUM0922CPU0710, Workstation, Server, NT Workstation, Potential Browser, Master Browser
48803 390.863973   10.120.110.124   10.120.111.255   BROWSER  243 Local Master Announcement SAIBA, Workstation, Server, Print Queue Server, NT Workstation, Potential Browser, Master Browser
38963 89.500337    10.120.113.245   10.120.113.255   BROWSER  258 Local Master Announcement WIPG-1000, Workstation, Server, Print Queue Server, Xenix Server, NT Workstation, NT Server, Master Browser
62042 809.729413   10.120.113.245   10.120.113.255   BROWSER  258 Local Master Announcement WIPG-1000, Workstation, Server, Print Queue Server, Xenix Server, NT Workstation, NT Server, Master Browser
19101 16.116128    10.120.112.225   192.168.2.108    SMB2     170 Lock Request
19113 16.123975    10.120.112.225   192.168.2.108    SMB2     170 Lock Request
19107 16.120319    192.168.2.108    10.120.112.225   SMB2     126 Lock Response
19114 16.125882    192.168.2.108    10.120.112.225   SMB2     126 Lock Response
19106 16.120237    192.168.2.108    10.120.112.225   SMB2     130 Lock Response, Error: STATUS_PENDING
    1 0.000000     10.120.113.25    239.255.255.250  SSDP     217 M-SEARCH * HTTP/1.1
  489 0.417474     10.120.101.28    239.255.255.250  SSDP     217 M-SEARCH * HTTP/1.1
```

```
> Frame 1: 217 bytes on wire (1736 bits), 217 bytes captured (1736 bits) on interface \Device\NPF_{414FC362-8DF7-4881-AA2E-5BBF2D0DC14A
> Ethernet II, Src: IntelCor_58:ba:60 (bc:09:1b:58:ba:60), Dst: IPv4mcast_7f:ff:fa (01:00:5e:7f:ff:fa)
> Internet Protocol Version 4, Src: 10.120.113.25, Dst: 239.255.255.250
> User Datagram Protocol, Src Port: 52733, Dst Port: 1900
> Simple Service Discovery Protocol
```

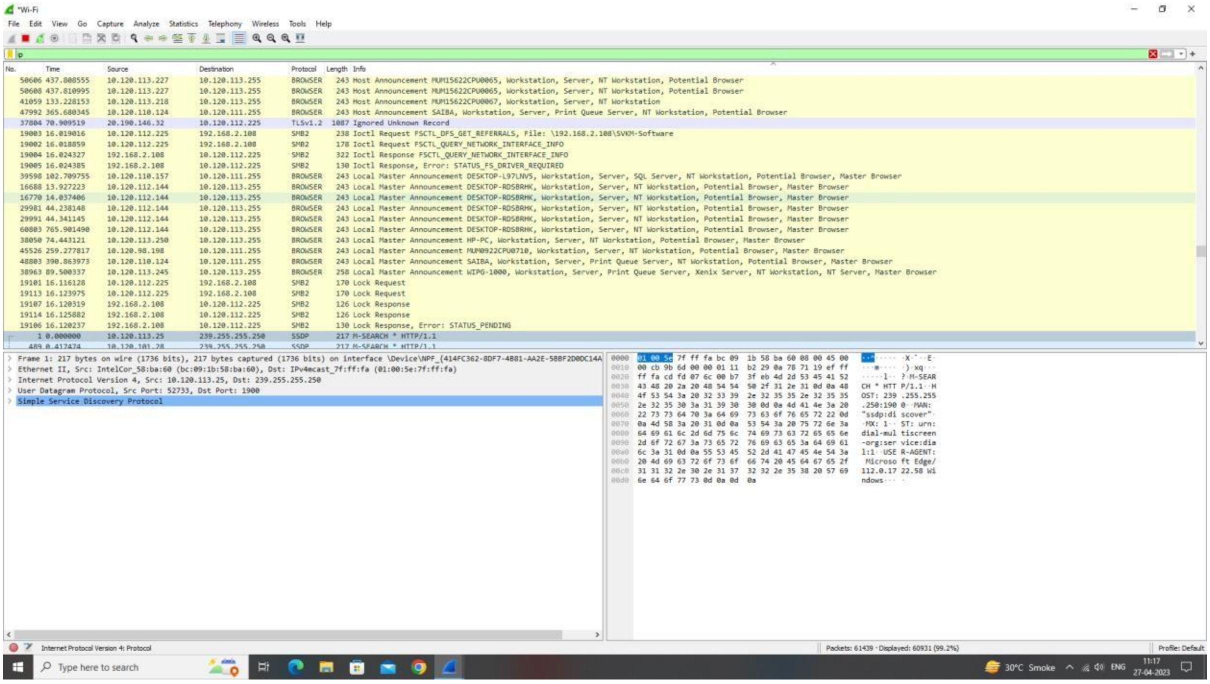
```
0000  01 00 5e 7f ff fa bc 09  1b 58 ba 60 08 00 45 00   ··^·····X·`··E·
0010  00 cb 9b 6d 00 00 01 11  b2 29 0a 78 71 19 ef ff   ···m·····)·xq···
0020  ff fa cd fd 07 6c 00 b7  3f eb 4d 2d 53 45 41 52   ·····l··?·M-SEAR
0030  43 48 20 2a 20 48 54 54  50 2f 31 2e 31 0d 0a 48   CH * HTT P/1.1··H
0040  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 31 32 2e 30 2e 31 37  32 32 2e 35 38 20 57 69   112.0.17 22.58 Wi
00d0  6e 64 6f 77 73 0d 0a 0d  0a                        ndows····
```

Destination Host: Character string

Packets: 65865 · Displayed: 65217 (99.0%)

Profile: Default

c. Addr


*Wi-Fi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
ip
Internet Protocol Version 4: Protocol
Packets: 61439 · Displayed: 60931 (99.2%)
Profile: Default
Type here to search
30°C Smoke ENG 11:17 27-04-2023

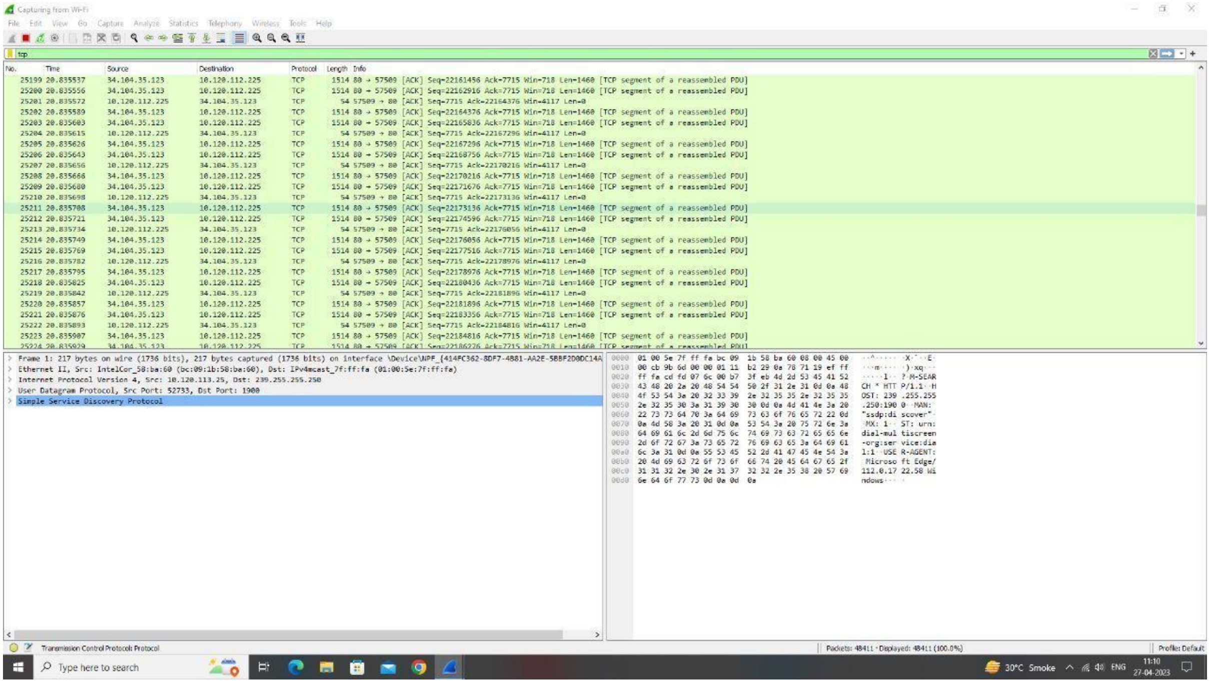
```
No.    Time        Source          Destination      Protocol Length Info
 50606 437.808555  10.120.113.227  10.120.113.255   BROWSER   243 Host Announcement MUM15622CPU0065, Workstation, Server, NT Workstation, Potential Browser
 50608 437.810995  10.120.113.227  10.120.113.255   BROWSER   243 Host Announcement MUM15622CPU0065, Workstation, Server, NT Workstation, Potential Browser
 41059 133.228153  10.120.113.218  10.120.113.255   BROWSER   243 Host Announcement MUM15622CPU0067, Workstation, Server, NT Workstation
 47992 365.680345  10.120.110.124  10.120.111.255   BROWSER   243 Host Announcement SAIBA, Workstation, Server, Print Queue Server, NT Workstation, Potential Browser
 37804 70.909519   20.190.146.32   10.120.112.225   TLSv1.2  1087 Ignored Unknown Record
 19003 16.019016   10.120.112.225  192.168.2.108    SMB2      238 Ioctl Request FSCTL_DFS_GET_REFERRALS, File: \192.168.2.108\SVKM-Software
 19002 16.018859   10.120.112.225  192.168.2.108    SMB2      178 Ioctl Request FSCTL_QUERY_NETWORK_INTERFACE_INFO
 19004 16.024327   192.168.2.108   10.120.112.225   SMB2      322 Ioctl Response FSCTL_QUERY_NETWORK_INTERFACE_INFO
 19005 16.024385   192.168.2.108   10.120.112.225   SMB2      130 Ioctl Response, Error: STATUS_FS_DRIVER_REQUIRED
 39598 102.709755  10.120.110.157  10.120.111.255   BROWSER   243 Local Master Announcement DESKTOP-L97LNV5, Workstation, Server, SQL Server, NT Workstation, Potential Browser, Master Browser
 16688 13.927223   10.120.112.144  10.120.113.255   BROWSER   243 Local Master Announcement DESKTOP-RDSBRHK, Workstation, Server, NT Workstation, Potential Browser, Master Browser
 16770 14.037406   10.120.112.144  10.120.113.255   BROWSER   243 Local Master Announcement DESKTOP-RDSBRHK, Workstation, Server, NT Workstation, Potential Browser, Master Browser
 29981 44.238148   10.120.112.144  10.120.113.255   BROWSER   243 Local Master Announcement DESKTOP-RDSBRHK, Workstation, Server, NT Workstation, Potential Browser, Master Browser
 29991 44.341145   10.120.112.144  10.120.113.255   BROWSER   243 Local Master Announcement DESKTOP-RDSBRHK, Workstation, Server, NT Workstation, Potential Browser, Master Browser
 60803 765.901490  10.120.112.144  10.120.113.255   BROWSER   243 Local Master Announcement DESKTOP-RDSBRHK, Workstation, Server, NT Workstation, Potential Browser, Master Browser
 38050 74.443121   10.120.113.250  10.120.113.255   BROWSER   243 Local Master Announcement HP-PC, Workstation, Server, NT Workstation, Potential Browser, Master Browser
 45526 259.277817  10.120.98.198   10.120.111.255   BROWSER   243 Local Master Announcement MUM0922CPU0710, Workstation, Server, NT Workstation, Potential Browser, Master Browser
 48803 390.863973  10.120.110.124  10.120.111.255   BROWSER   243 Local Master Announcement SAIBA, Workstation, Server, Print Queue Server, NT Workstation, Potential Browser, Master Browser
 38963 89.500337   10.120.113.245  10.120.113.255   BROWSER   258 Local Master Announcement WIPG-1000, Workstation, Server, Print Queue Server, Xenix Server, NT Workstation, NT Server, Master Browser
 19101 16.116128   10.120.112.225  192.168.2.108    SMB2      170 Lock Request
 19113 16.123975   10.120.112.225  192.168.2.108    SMB2      170 Lock Request
 19107 16.120319   192.168.2.108   10.120.112.225   SMB2      126 Lock Response
 19114 16.125882   192.168.2.108   10.120.112.225   SMB2      126 Lock Response
 19106 16.120237   192.168.2.108   10.120.112.225   SMB2      130 Lock Response, Error: STATUS_PENDING
     1 0.000000    10.120.113.25   239.255.255.250  SSDP      217 M-SEARCH * HTTP/1.1
   489 0.417474    10.120.101.28   239.255.255.250  SSDP      217 M-SEARCH * HTTP/1.1
```

```
> Frame 1: 217 bytes on wire (1736 bits), 217 bytes captured (1736 bits) on interface \Device\NPF_{414FC362-8DF7-4B81-AA2E-5BBF2D0DC14A
> Ethernet II, Src: IntelCor_58:ba:60 (bc:09:1b:58:ba:60), Dst: IPv4mcast_7f:ff:fa (01:00:5e:7f:ff:fa)
> Internet Protocol Version 4, Src: 10.120.113.25, Dst: 239.255.255.250
> User Datagram Protocol, Src Port: 52733, Dst Port: 1900
> Simple Service Discovery Protocol
```

```
0000  01 00 5e 7f ff fa bc 09  1b 58 ba 60 08 00 45 00   ··^····· ·X·`··E·
0010  00 cb 9b 6d 00 00 01 11  b2 29 0a 78 71 19 ef ff   ···m···· ·)·xq···
0020  ff fa cd fd 07 6c 00 b7  3f eb 4d 2d 53 45 41 52   ·····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 31 32 2e 30 2e 31 37  32 32 2e 35 38 20 57 69   112.0.17 22.58 Wi
00d0  6e 64 6f 77 73 0d 0a 0d  0a                        ndows····
```

2. Tcp:

a. Tcp

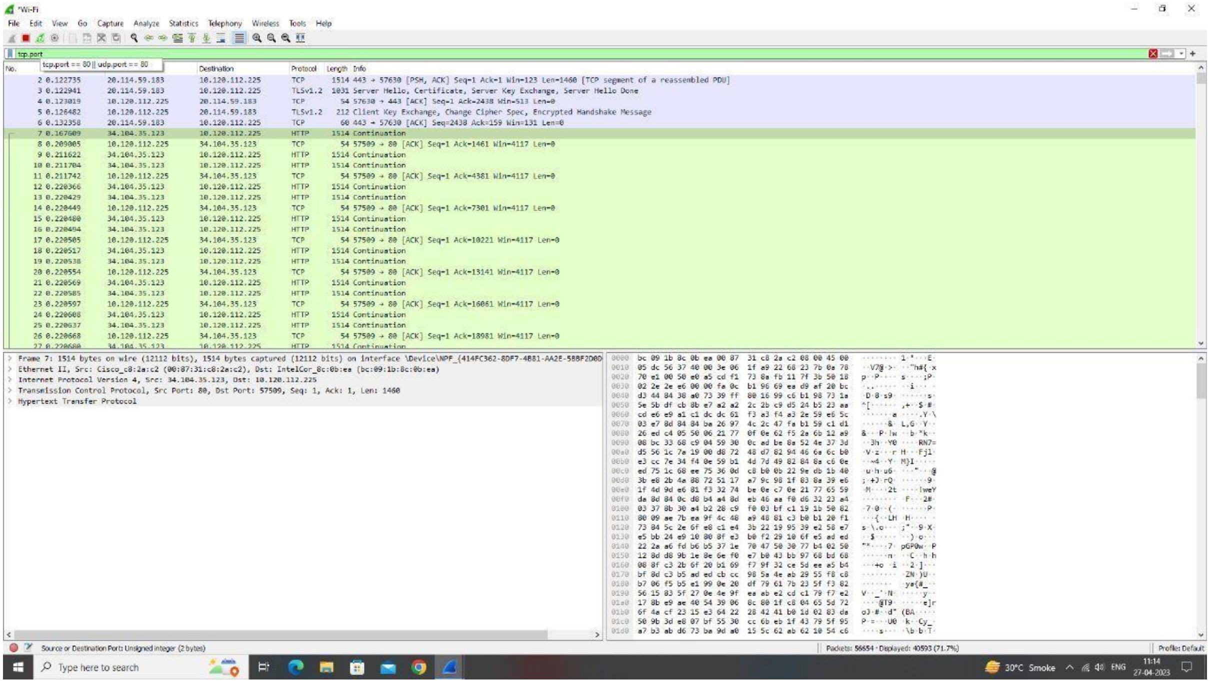

Capturing from Wi-Fi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
tcp
Transmission Control Protocol: Protocol
Packets: 48411 · Displayed: 48411 (100.0%)
Profile: Default
Type here to search
30°C Smoke ENG 11:10 27-04-2023

```
No.    Time        Source          Destination      Protocol Length Info
 25199 20.835537   34.104.35.123   10.120.112.225   TCP      1514 80 → 57509 [ACK] Seq=22161456 Ack=7715 Win=718 Len=1460 [TCP segment of a reassembled PDU]
 25200 20.835556   34.104.35.123   10.120.112.225   TCP      1514 80 → 57509 [ACK] Seq=22162916 Ack=7715 Win=718 Len=1460 [TCP segment of a reassembled PDU]
 25201 20.835572   10.120.112.225  34.104.35.123    TCP        54 57509 → 80 [ACK] Seq=7715 Ack=22164376 Win=4117 Len=0
 25202 20.835589   34.104.35.123   10.120.112.225   TCP      1514 80 → 57509 [ACK] Seq=22164376 Ack=7715 Win=718 Len=1460 [TCP segment of a reassembled PDU]
 25203 20.835603   34.104.35.123   10.120.112.225   TCP      1514 80 → 57509 [ACK] Seq=22165836 Ack=7715 Win=718 Len=1460 [TCP segment of a reassembled PDU]
 25204 20.835615   10.120.112.225  34.104.35.123    TCP        54 57509 → 80 [ACK] Seq=7715 Ack=22167296 Win=4117 Len=0
 25205 20.835626   34.104.35.123   10.120.112.225   TCP      1514 80 → 57509 [ACK] Seq=22167296 Ack=7715 Win=718 Len=1460 [TCP segment of a reassembled PDU]
 25206 20.835643   34.104.35.123   10.120.112.225   TCP      1514 80 → 57509 [ACK] Seq=22168756 Ack=7715 Win=718 Len=1460 [TCP segment of a reassembled PDU]
 25207 20.835656   10.120.112.225  34.104.35.123    TCP        54 57509 → 80 [ACK] Seq=7715 Ack=22170216 Win=4117 Len=0
 25208 20.835666   34.104.35.123   10.120.112.225   TCP      1514 80 → 57509 [ACK] Seq=22170216 Ack=7715 Win=718 Len=1460 [TCP segment of a reassembled PDU]
 25209 20.835680   34.104.35.123   10.120.112.225   TCP      1514 80 → 57509 [ACK] Seq=22171676 Ack=7715 Win=718 Len=1460 [TCP segment of a reassembled PDU]
 25210 20.835698   10.120.112.225  34.104.35.123    TCP        54 57509 → 80 [ACK] Seq=7715 Ack=22173136 Win=4117 Len=0
 25211 20.835708   34.104.35.123   10.120.112.225   TCP      1514 80 → 57509 [ACK] Seq=22173136 Ack=7715 Win=718 Len=1460 [TCP segment of a reassembled PDU]
 25212 20.835721   34.104.35.123   10.120.112.225   TCP      1514 80 → 57509 [ACK] Seq=22174596 Ack=7715 Win=718 Len=1460 [TCP segment of a reassembled PDU]
 25213 20.835734   10.120.112.225  34.104.35.123    TCP        54 57509 → 80 [ACK] Seq=7715 Ack=22176056 Win=4117 Len=0
 25214 20.835749   34.104.35.123   10.120.112.225   TCP      1514 80 → 57509 [ACK] Seq=22176056 Ack=7715 Win=718 Len=1460 [TCP segment of a reassembled PDU]
 25215 20.835769   34.104.35.123   10.120.112.225   TCP      1514 80 → 57509 [ACK] Seq=22177516 Ack=7715 Win=718 Len=1460 [TCP segment of a reassembled PDU]
 25216 20.835782   10.120.112.225  34.104.35.123    TCP        54 57509 → 80 [ACK] Seq=7715 Ack=22178976 Win=4117 Len=0
 25217 20.835795   34.104.35.123   10.120.112.225   TCP      1514 80 → 57509 [ACK] Seq=22178976 Ack=7715 Win=718 Len=1460 [TCP segment of a reassembled PDU]
 25218 20.835825   34.104.35.123   10.120.112.225   TCP      1514 80 → 57509 [ACK] Seq=22180436 Ack=7715 Win=718 Len=1460 [TCP segment of a reassembled PDU]
 25219 20.835842   10.120.112.225  34.104.35.123    TCP        54 57509 → 80 [ACK] Seq=7715 Ack=22181896 Win=4117 Len=0
 25220 20.835857   34.104.35.123   10.120.112.225   TCP      1514 80 → 57509 [ACK] Seq=22181896 Ack=7715 Win=718 Len=1460 [TCP segment of a reassembled PDU]
 25221 20.835876   34.104.35.123   10.120.112.225   TCP      1514 80 → 57509 [ACK] Seq=22183356 Ack=7715 Win=718 Len=1460 [TCP segment of a reassembled PDU]
 25222 20.835893   10.120.112.225  34.104.35.123    TCP        54 57509 → 80 [ACK] Seq=7715 Ack=22184816 Win=4117 Len=0
 25223 20.835907   34.104.35.123   10.120.112.225   TCP      1514 80 → 57509 [ACK] Seq=22184816 Ack=7715 Win=718 Len=1460 [TCP segment of a reassembled PDU]
 25224 20.835929   34.104.35.123   10.120.112.225   TCP      1514 80 → 57509 [ACK] Seq=22186276 Ack=7715 Win=718 Len=1460 [TCP segment of a reassembled PDU]
```

```
> Frame 1: 217 bytes on wire (1736 bits), 217 bytes captured (1736 bits) on interface \Device\NPF_{414FC362-8DF7-4B81-AA2E-5BBF2D0DC14A
> Ethernet II, Src: IntelCor_58:ba:60 (bc:09:1b:58:ba:60), Dst: IPv4mcast_7f:ff:fa (01:00:5e:7f:ff:fa)
> Internet Protocol Version 4, Src: 10.120.113.25, Dst: 239.255.255.250
> User Datagram Protocol, Src Port: 52733, Dst Port: 1900
> Simple Service Discovery Protocol
```

```
0000  01 00 5e 7f ff fa bc 09  1b 58 ba 60 08 00 45 00   ··^····· ·X·`··E·
0010  00 cb 9b 6d 00 00 01 11  b2 29 0a 78 71 19 ef ff   ···m···· ·)·xq···
0020  ff fa cd fd 07 6c 00 b7  3f eb 4d 2d 53 45 41 52   ·····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 31 32 2e 30 2e 31 37  32 32 2e 35 38 20 57 69   112.0.17 22.58 Wi
00d0  6e 64 6f 77 73 0d 0a 0d  0a                        ndows····
```

b. Port


*Wi-Fi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

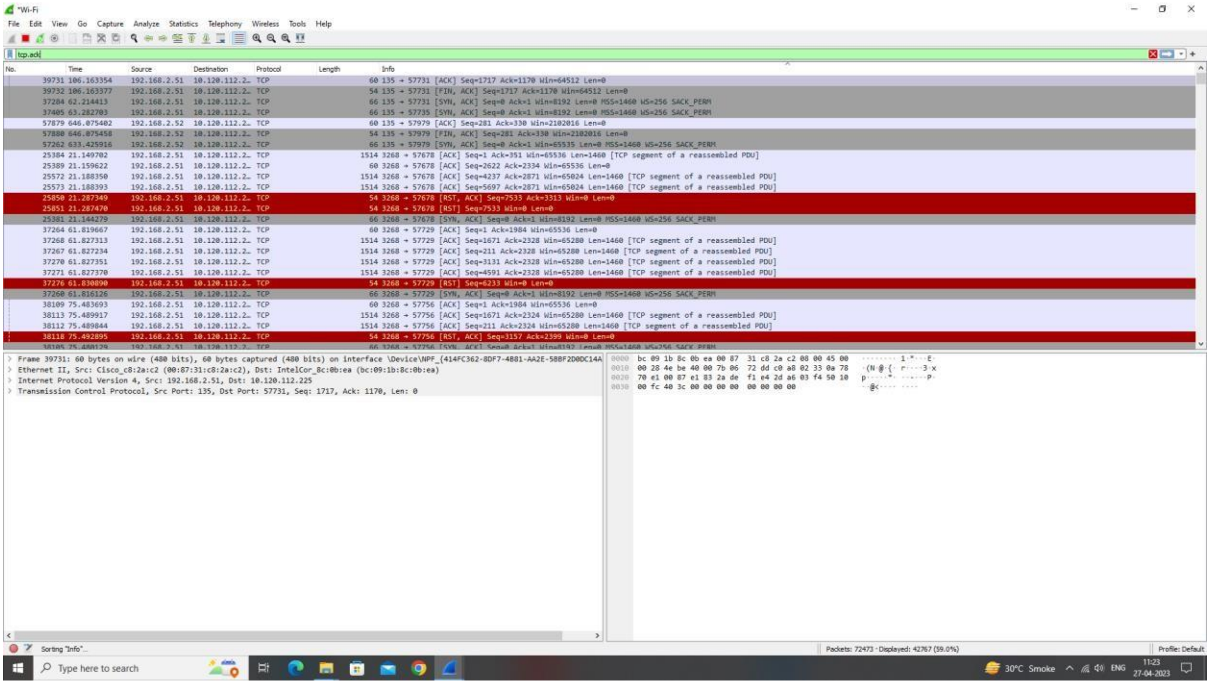
```
tcp.port
tcp.port == 80 || udp.port == 80
No.  Destination  Protocol  Length  Info
 2 0.122735  20.114.59.183   10.120.112.225  TCP      1514 443 → 57630 [PSH, ACK] Seq=1 Ack=1 Win=123 Len=1460 [TCP segment of a reassembled PDU]
 3 0.122941  20.114.59.183   10.120.112.225  TLSv1.2  1031 Server Hello, Certificate, Server Key Exchange, Server Hello Done
 4 0.123019  10.120.112.225  20.114.59.183   TCP        54 57630 → 443 [ACK] Seq=1 Ack=2438 Win=513 Len=0
 5 0.126482  10.120.112.225  20.114.59.183   TLSv1.2   212 Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
 6 0.132358  20.114.59.183   10.120.112.225  TCP        60 443 → 57630 [ACK] Seq=2438 Ack=159 Win=131 Len=0
 7 0.167609  34.104.35.123   10.120.112.225  HTTP     1514 Continuation
 8 0.209005  10.120.112.225  34.104.35.123   TCP        54 57509 → 80 [ACK] Seq=1 Ack=1461 Win=4117 Len=0
 9 0.211622  34.104.35.123   10.120.112.225  HTTP     1514 Continuation
10 0.211704  34.104.35.123   10.120.112.225  HTTP     1514 Continuation
11 0.211742  10.120.112.225  34.104.35.123   TCP        54 57509 → 80 [ACK] Seq=1 Ack=4381 Win=4117 Len=0
12 0.220366  34.104.35.123   10.120.112.225  HTTP     1514 Continuation
13 0.220429  34.104.35.123   10.120.112.225  HTTP     1514 Continuation
14 0.220449  10.120.112.225  34.104.35.123   TCP        54 57509 → 80 [ACK] Seq=1 Ack=7301 Win=4117 Len=0
15 0.220480  34.104.35.123   10.120.112.225  HTTP     1514 Continuation
16 0.220494  34.104.35.123   10.120.112.225  HTTP     1514 Continuation
17 0.220505  10.120.112.225  34.104.35.123   TCP        54 57509 → 80 [ACK] Seq=1 Ack=10221 Win=4117 Len=0
18 0.220517  34.104.35.123   10.120.112.225  HTTP     1514 Continuation
19 0.220538  34.104.35.123   10.120.112.225  HTTP     1514 Continuation
20 0.220554  10.120.112.225  34.104.35.123   TCP        54 57509 → 80 [ACK] Seq=1 Ack=13141 Win=4117 Len=0
21 0.220569  34.104.35.123   10.120.112.225  HTTP     1514 Continuation
22 0.220585  34.104.35.123   10.120.112.225  HTTP     1514 Continuation
23 0.220597  10.120.112.225  34.104.35.123   TCP        54 57509 → 80 [ACK] Seq=1 Ack=16061 Win=4117 Len=0
24 0.220608  34.104.35.123   10.120.112.225  HTTP     1514 Continuation
25 0.220637  34.104.35.123   10.120.112.225  HTTP     1514 Continuation
26 0.220668  10.120.112.225  34.104.35.123   TCP        54 57509 → 80 [ACK] Seq=1 Ack=18981 Win=4117 Len=0
27 0.220680  34.104.35.123   10.120.112.225  HTTP     1514 Continuation

> Frame 7: 1514 bytes on wire (12112 bits), 1514 bytes captured (12112 bits) on interface \Device\NPF_{414FC362-8DF7-4B81-AA2E-5BBF2D0D
> Ethernet II, Src: Cisco_c8:2a:c2 (00:87:31:c8:2a:c2), Dst: IntelCor_8c:0b:ea (bc:09:1b:8c:0b:ea)
> Internet Protocol Version 4, Src: 34.104.35.123, Dst: 10.120.112.225
> Transmission Control Protocol, Src Port: 80, Dst Port: 57509, Seq: 1, Ack: 1, Len: 1460
> Hypertext Transfer Protocol

0000  bc 09 1b 8c 0b ea 00 87  31 c8 2a c2 08 00 45 00
0010  05 dc 56 37 40 00 3e 06  1f a9 22 68 23 7b 0a 78
0020  70 e1 00 50 e0 a5 cd f1  73 8a fb 11 7f 3b 50 18
0030  02 2e 2e e6 00 00 fa 0c  b1 96 69 ea d9 af 20 bc
0040  d3 44 84 38 a0 73 39 ff  80 16 99 c6 b1 98 73 1a
0050  5e 5b df cb 8b e7 a2 a2  2c 2b c9 d5 24 b5 23 aa
0060  cd e6 e9 a1 c1 dc dc 61  f3 a3 f4 a3 2e 59 e6 5c
0070  03 e7 8d 84 84 ba 26 97  4c 2c 47 fa b1 59 c1 d1
0080  26 ed c4 05 50 06 21 77  0f 0e 62 f5 2a 6b 12 a9
0090  08 bc 33 68 c9 04 59 30  0c ad be 8a 52 4e 37 3d
00a0  d5 56 1c 7a 19 00 d8 72  48 d7 82 94 46 6a 6c b0
00b0  e3 cc 7e 34 f4 0e 59 b1  4d 7d 49 82 84 8a c6 0e
00c0  ed 75 1c 68 ee 75 36 0d  c8 b0 0b 22 9e db 1b 40
00d0  3b e8 2b 4a 88 72 51 17  a7 9c 98 1f 83 8a 39 e6
00e0  1f 4d 9d e6 81 f3 32 74  be 0e c7 0e 21 77 65 59
00f0  da 8d 84 0c d8 b4 a4 8d  eb 46 aa f0 d6 32 23 a4
0100  03 37 8b 30 a4 b2 28 c9  f0 03 bf c1 19 1b 50 82
0110  80 09 ae 7b ea 9f 4c 48  a9 48 81 c3 b0 b1 20 f1
0120  73 84 5c 2e 6f e8 c1 e4  3b 22 19 95 39 e2 58 e7
0130  e5 bb 24 e9 10 80 8f e3  b0 f2 29 10 6f e5 ad ed
0140  22 2a a6 fd b6 b5 37 1e  70 47 50 30 77 b4 02 50
0150  12 8d d8 9b 1e 8e 6e f0  e7 b0 43 bb 97 68 bd 68
0160  08 8f c3 2b 6f 20 b1 69  f7 9f 32 ce 5d ee a5 b4
0170  bf 8d c3 b5 ad ed cb cc  98 5a 4e ab 29 55 f8 c8
0180  b7 06 f5 b5 e1 99 0e 20  df 79 61 7b 23 5f f3 82
0190  56 15 83 5f 27 0e 4e 9f  ea ab e2 cd c1 79 f7 e2
01a0  17 8b e9 ae 40 54 39 06  8c 80 1f c8 04 65 5d 72
01b0  6f 4a cf 23 15 e3 64 22  28 42 41 b0 1d 02 83 da
01c0  50 9b 3d e8 07 bf 55 30  cc 6b eb 1f 43 79 5f 95
01d0  a7 b3 ab d6 73 ba 9d a0  15 5c 62 ab 62 10 54 c6

Source or Destination Port: Unsigned integer (2 bytes)    Packets: 56654 · Displayed: 40593 (71.7%)    Profile: Default
Type here to search    30°C Smoke  ENG  11:14 27-04-2023
```

c. Ack


*Wi-Fi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

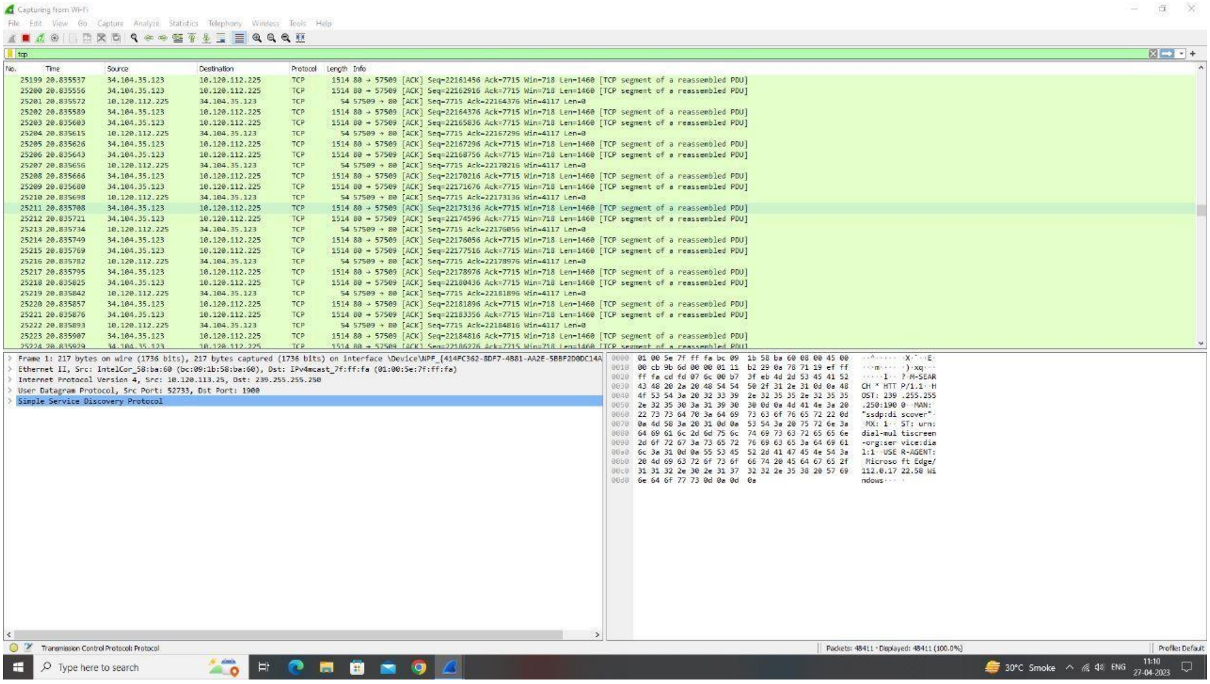
```
tcp.ack
No.   Time        Source        Destination     Protocol  Length  Info
39731 106.163354  192.168.2.51  10.120.112.2…  TCP    60 135 → 57731 [ACK] Seq=1717 Ack=1170 Win=64512 Len=0
39732 106.163377  192.168.2.51  10.120.112.2…  TCP    54 135 → 57731 [FIN, ACK] Seq=1717 Ack=1170 Win=64512 Len=0
37284 62.214413   192.168.2.51  10.120.112.2…  TCP    66 135 → 57731 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM
37405 63.282703   192.168.2.51  10.120.112.2…  TCP    66 135 → 57735 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM
57879 646.075402  192.168.2.52  10.120.112.2…  TCP    60 135 → 57979 [ACK] Seq=281 Ack=330 Win=2102016 Len=0
57880 646.075458  192.168.2.52  10.120.112.2…  TCP    54 135 → 57979 [FIN, ACK] Seq=281 Ack=330 Win=2102016 Len=0
57262 633.425916  192.168.2.52  10.120.112.2…  TCP    66 135 → 57979 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM
25384 21.149702   192.168.2.51  10.120.112.2…  TCP  1514 3268 → 57678 [ACK] Seq=1 Ack=351 Win=65536 Len=1460 [TCP segment of a reassembled PDU]
25389 21.159622   192.168.2.51  10.120.112.2…  TCP    60 3268 → 57678 [ACK] Seq=2622 Ack=2334 Win=65536 Len=0
25572 21.188350   192.168.2.51  10.120.112.2…  TCP  1514 3268 → 57678 [ACK] Seq=4237 Ack=2871 Win=65024 Len=1460 [TCP segment of a reassembled PDU]
25573 21.188393   192.168.2.51  10.120.112.2…  TCP  1514 3268 → 57678 [ACK] Seq=5697 Ack=2871 Win=65024 Len=1460 [TCP segment of a reassembled PDU]
25850 21.287349   192.168.2.51  10.120.112.2…  TCP    54 3268 → 57678 [RST, ACK] Seq=7533 Ack=3313 Win=0 Len=0
25851 21.287470   192.168.2.51  10.120.112.2…  TCP    54 3268 → 57678 [RST] Seq=7533 Win=0 Len=0
25381 21.144279   192.168.2.51  10.120.112.2…  TCP    66 3268 → 57678 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM
37264 61.819667   192.168.2.51  10.120.112.2…  TCP    60 3268 → 57729 [ACK] Seq=1 Ack=1984 Win=65536 Len=0
37268 61.827313   192.168.2.51  10.120.112.2…  TCP  1514 3268 → 57729 [ACK] Seq=1671 Ack=2328 Win=65280 Len=1460 [TCP segment of a reassembled PDU]
37267 61.827234   192.168.2.51  10.120.112.2…  TCP  1514 3268 → 57729 [ACK] Seq=211 Ack=2328 Win=65280 Len=1460 [TCP segment of a reassembled PDU]
37270 61.827351   192.168.2.51  10.120.112.2…  TCP  1514 3268 → 57729 [ACK] Seq=3131 Ack=2328 Win=65280 Len=1460 [TCP segment of a reassembled PDU]
37271 61.827370   192.168.2.51  10.120.112.2…  TCP  1514 3268 → 57729 [ACK] Seq=4591 Ack=2328 Win=65280 Len=1460 [TCP segment of a reassembled PDU]
37276 61.830890   192.168.2.51  10.120.112.2…  TCP    54 3268 → 57729 [RST] Seq=6233 Win=0 Len=0
37260 61.816126   192.168.2.51  10.120.112.2…  TCP    66 3268 → 57729 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM
38109 75.483693   192.168.2.51  10.120.112.2…  TCP    60 3268 → 57756 [ACK] Seq=1 Ack=1984 Win=65536 Len=0
38113 75.489917   192.168.2.51  10.120.112.2…  TCP  1514 3268 → 57756 [ACK] Seq=1671 Ack=2324 Win=65280 Len=1460 [TCP segment of a reassembled PDU]
38112 75.489844   192.168.2.51  10.120.112.2…  TCP  1514 3268 → 57756 [ACK] Seq=211 Ack=2324 Win=65280 Len=1460 [TCP segment of a reassembled PDU]
38118 75.492895   192.168.2.51  10.120.112.2…  TCP    54 3268 → 57756 [RST, ACK] Seq=3157 Ack=2399 Win=0 Len=0
38105 75.480129   192.168.2.51  10.120.112.2…  TCP    66 3268 → 57756 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM

> Frame 39731: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface \Device\NPF_{414FC362-8DF7-4B81-AA2E-5BBF2D0DC14A
> Ethernet II, Src: Cisco_c8:2a:c2 (00:87:31:c8:2a:c2), Dst: IntelCor_8c:0b:ea (bc:09:1b:8c:0b:ea)
> Internet Protocol Version 4, Src: 192.168.2.51, Dst: 10.120.112.225
> Transmission Control Protocol, Src Port: 135, Dst Port: 57731, Seq: 1717, Ack: 1170, Len: 0

0000  bc 09 1b 8c 0b ea 00 87  31 c8 2a c2 08 00 45 00
0010  00 28 4e be 40 00 7b 06  72 dd c0 a8 02 33 0a 78
0020  70 e1 00 87 e1 83 2a de  f1 e4 2d a6 03 f4 50 10
0030  00 fc 40 3c 00 00 00 00  00 00 00 00

Sorting "Info"...    Packets: 72473 · Displayed: 42767 (59.0%)    Profile: Default
Type here to search    30°C Smoke  ENG  11:23 27-04-2023
```

d. Payload


Capturing from Wi-Fi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

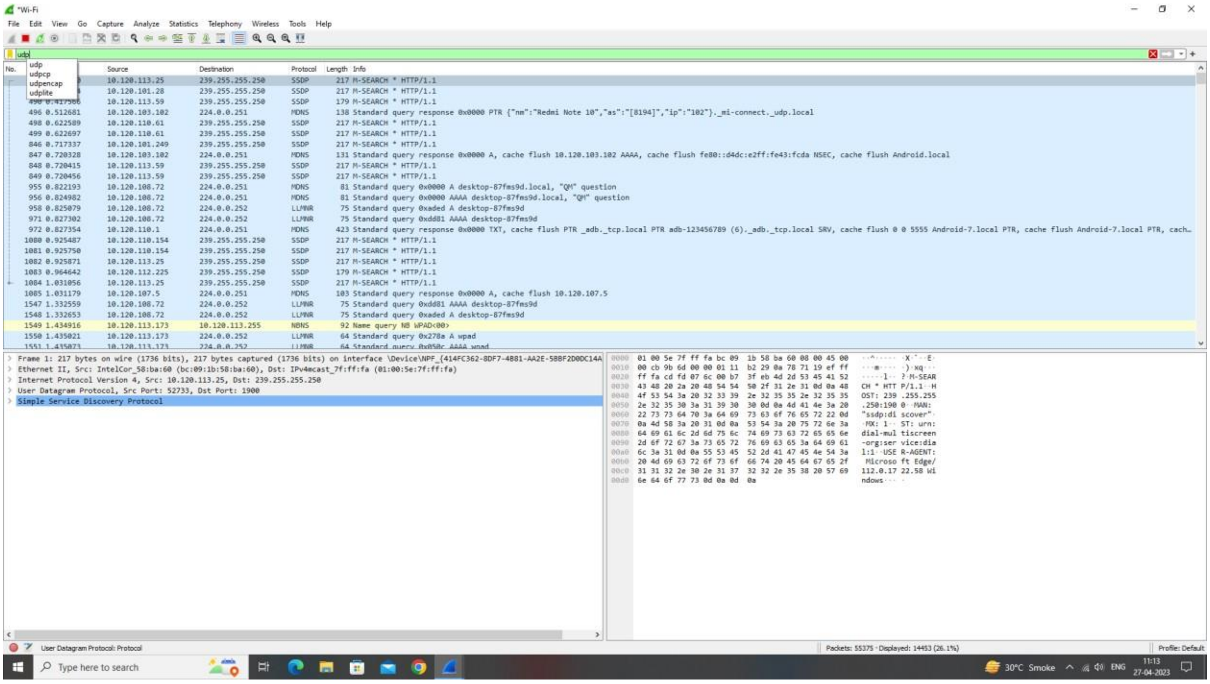
```
tcp
No.   Time       Source          Destination     Protocol Length Info
25199 20.835537  34.104.35.123   10.120.112.225  TCP   1514 80 → 57509 [ACK] Seq=22161456 Ack=7715 Win=718 Len=1460 [TCP segment of a reassembled PDU]
25200 20.835556  34.104.35.123   10.120.112.225  TCP   1514 80 → 57509 [ACK] Seq=22162916 Ack=7715 Win=718 Len=1460 [TCP segment of a reassembled PDU]
25201 20.835572  10.120.112.225  34.104.35.123   TCP     54 57509 → 80 [ACK] Seq=7715 Ack=22164376 Win=4117 Len=0
25202 20.835589  34.104.35.123   10.120.112.225  TCP   1514 80 → 57509 [ACK] Seq=22164376 Ack=7715 Win=718 Len=1460 [TCP segment of a reassembled PDU]
25203 20.835603  34.104.35.123   10.120.112.225  TCP   1514 80 → 57509 [ACK] Seq=22165836 Ack=7715 Win=718 Len=1460 [TCP segment of a reassembled PDU]
25204 20.835615  10.120.112.225  34.104.35.123   TCP     54 57509 → 80 [ACK] Seq=7715 Ack=22167296 Win=4117 Len=0
25205 20.835626  34.104.35.123   10.120.112.225  TCP   1514 80 → 57509 [ACK] Seq=22167296 Ack=7715 Win=718 Len=1460 [TCP segment of a reassembled PDU]
25206 20.835643  34.104.35.123   10.120.112.225  TCP   1514 80 → 57509 [ACK] Seq=22168756 Ack=7715 Win=718 Len=1460 [TCP segment of a reassembled PDU]
25207 20.835656  10.120.112.225  34.104.35.123   TCP     54 57509 → 80 [ACK] Seq=7715 Ack=22170216 Win=4117 Len=0
25208 20.835666  34.104.35.123   10.120.112.225  TCP   1514 80 → 57509 [ACK] Seq=22170216 Ack=7715 Win=718 Len=1460 [TCP segment of a reassembled PDU]
25209 20.835680  34.104.35.123   10.120.112.225  TCP   1514 80 → 57509 [ACK] Seq=22171676 Ack=7715 Win=718 Len=1460 [TCP segment of a reassembled PDU]
25210 20.835698  10.120.112.225  34.104.35.123   TCP     54 57509 → 80 [ACK] Seq=7715 Ack=22173136 Win=4117 Len=0
25211 20.835708  34.104.35.123   10.120.112.225  TCP   1514 80 → 57509 [ACK] Seq=22173136 Ack=7715 Win=718 Len=1460 [TCP segment of a reassembled PDU]
25212 20.835721  34.104.35.123   10.120.112.225  TCP   1514 80 → 57509 [ACK] Seq=22174596 Ack=7715 Win=718 Len=1460 [TCP segment of a reassembled PDU]
25213 20.835734  10.120.112.225  34.104.35.123   TCP     54 57509 → 80 [ACK] Seq=7715 Ack=22176056 Win=4117 Len=0
25214 20.835749  34.104.35.123   10.120.112.225  TCP   1514 80 → 57509 [ACK] Seq=22176056 Ack=7715 Win=718 Len=1460 [TCP segment of a reassembled PDU]
25215 20.835769  34.104.35.123   10.120.112.225  TCP   1514 80 → 57509 [ACK] Seq=22177516 Ack=7715 Win=718 Len=1460 [TCP segment of a reassembled PDU]
25216 20.835782  10.120.112.225  34.104.35.123   TCP     54 57509 → 80 [ACK] Seq=7715 Ack=22178976 Win=4117 Len=0
25217 20.835795  34.104.35.123   10.120.112.225  TCP   1514 80 → 57509 [ACK] Seq=22178976 Ack=7715 Win=718 Len=1460 [TCP segment of a reassembled PDU]
25218 20.835825  34.104.35.123   10.120.112.225  TCP   1514 80 → 57509 [ACK] Seq=22180436 Ack=7715 Win=718 Len=1460 [TCP segment of a reassembled PDU]
25219 20.835842  10.120.112.225  34.104.35.123   TCP     54 57509 → 80 [ACK] Seq=7715 Ack=22181896 Win=4117 Len=0
25220 20.835857  34.104.35.123   10.120.112.225  TCP   1514 80 → 57509 [ACK] Seq=22181896 Ack=7715 Win=718 Len=1460 [TCP segment of a reassembled PDU]
25221 20.835876  34.104.35.123   10.120.112.225  TCP   1514 80 → 57509 [ACK] Seq=22183356 Ack=7715 Win=718 Len=1460 [TCP segment of a reassembled PDU]
25222 20.835893  10.120.112.225  34.104.35.123   TCP     54 57509 → 80 [ACK] Seq=7715 Ack=22184816 Win=4117 Len=0
25223 20.835907  34.104.35.123   10.120.112.225  TCP   1514 80 → 57509 [ACK] Seq=22184816 Ack=7715 Win=718 Len=1460 [TCP segment of a reassembled PDU]
25224 20.835929  34.104.35.123   10.120.112.225  TCP   1514 80 → 57509 [ACK] Seq=22186276 Ack=7715 Win=718 Len=1460 [TCP segment of a reassembled PDU]

> Frame 1: 217 bytes on wire (1736 bits), 217 bytes captured (1736 bits) on interface \Device\NPF_{414FC362-8DF7-4881-AA2E-5BBF2D0DC14A
> Ethernet II, Src: IntelCor_58:ba:60 (bc:09:1b:58:ba:60), Dst: IPv4mcast_7f:ff:fa (01:00:5e:7f:ff:fa)
> Internet Protocol Version 4, Src: 10.120.113.25, Dst: 239.255.255.250
> User Datagram Protocol, Src Port: 52733, Dst Port: 1900
> Simple Service Discovery Protocol

0000  01 00 5e 7f ff fa bc 09  1b 58 ba 60 08 00 45 00   ··^·····  ·X·`··E·
0010  00 cb 9b 6d 00 00 01 11  b2 29 0a 78 71 19 ef ff   ···m····  ·)·xq···
0020  ff fa cd fd 07 6c 00 b7  3f eb 4d 2d 53 45 41 52   ·····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 31 32 2e 30 2e 31 37  32 32 2e 35 38 20 57 69   112.0.17  22.58 Wi
00d0  6e 64 6f 77 73 0d 0a 0d  0a                        ndows····

Transmission Control Protocol: Protocol        Packets: 48411 · Displayed: 48411 (100.0%)        Profile: Default
```

3. Arp:


*Wi-Fi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
udp
udpcp
udpencap
udplite

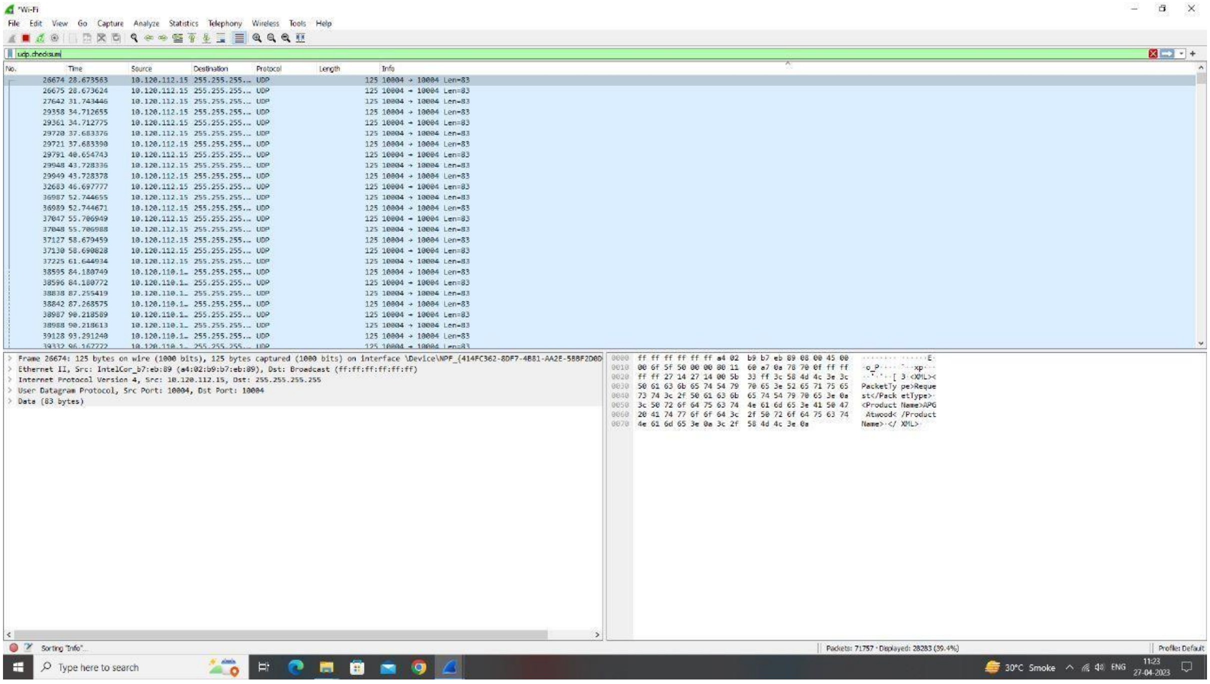
```
udp
No.   Time       Source          Destination      Protocol Length Info
                 10.120.113.25   239.255.255.250  SSDP   217 M-SEARCH * HTTP/1.1
                 10.120.101.28   239.255.255.250  SSDP   217 M-SEARCH * HTTP/1.1
  490 0.417566   10.120.113.59   239.255.255.250  SSDP   179 M-SEARCH * HTTP/1.1
  496 0.512681   10.120.103.102  224.0.0.251      MDNS   138 Standard query response 0x0000 PTR {"nm":"Redmi Note 10","as":"[8194]","ip":"102"}._mi-connect._udp.local
  498 0.622589   10.120.110.61   239.255.255.250  SSDP   217 M-SEARCH * HTTP/1.1
  499 0.622697   10.120.110.61   239.255.255.250  SSDP   217 M-SEARCH * HTTP/1.1
  846 0.717337   10.120.101.249  239.255.255.250  SSDP   217 M-SEARCH * HTTP/1.1
  847 0.720328   10.120.103.102  224.0.0.251      MDNS   131 Standard query response 0x0000 A, cache flush 10.120.103.102 AAAA, cache flush fe80::d4dc:e2ff:fe43:fcda NSEC, cache flush Android.local
  848 0.720415   10.120.113.59   239.255.255.250  SSDP   217 M-SEARCH * HTTP/1.1
  849 0.720456   10.120.113.59   239.255.255.250  SSDP   217 M-SEARCH * HTTP/1.1
  955 0.822193   10.120.108.72   224.0.0.251      MDNS    81 Standard query 0x0000 A desktop-87fms9d.local, "QM" question
  956 0.824982   10.120.108.72   224.0.0.251      MDNS    81 Standard query 0x0000 AAAA desktop-87fms9d.local, "QM" question
  958 0.825079   10.120.108.72   224.0.0.252      LLMNR   75 Standard query 0xaded A desktop-87fms9d
  971 0.827302   10.120.108.72   224.0.0.252      LLMNR   75 Standard query 0xdd81 AAAA desktop-87fms9d
  972 0.827354   10.120.110.1    224.0.0.251      MDNS   423 Standard query response 0x0000 TXT, cache flush PTR _adb._tcp.local PTR adb-123456789 (6)._adb._tcp.local SRV, cache flush 0 0 5555 Android-7.local PTR, cache flush Android-7.local PTR, cach…
 1080 0.925487   10.120.110.154  239.255.255.250  SSDP   217 M-SEARCH * HTTP/1.1
 1081 0.925750   10.120.110.154  239.255.255.250  SSDP   217 M-SEARCH * HTTP/1.1
 1082 0.925871   10.120.113.25   239.255.255.250  SSDP   217 M-SEARCH * HTTP/1.1
 1083 0.964642   10.120.112.225  239.255.255.250  SSDP   179 M-SEARCH * HTTP/1.1
 1084 1.031056   10.120.113.25   239.255.255.250  SSDP   217 M-SEARCH * HTTP/1.1
 1085 1.031179   10.120.107.5    224.0.0.251      MDNS   103 Standard query response 0x0000 A, cache flush 10.120.107.5
 1547 1.332559   10.120.108.72   224.0.0.252      LLMNR   75 Standard query 0xdd81 AAAA desktop-87fms9d
 1548 1.332653   10.120.108.72   224.0.0.252      LLMNR   75 Standard query 0xaded A desktop-87fms9d
 1549 1.434916   10.120.113.173  10.120.113.255   NBNS    92 Name query NB WPAD<00>
 1550 1.435021   10.120.113.173  224.0.0.252      LLMNR   64 Standard query 0x278a A wpad
 1551 1.435073   10.120.113.173  224.0.0.252      LLMNR   64 Standard query 0x050c AAAA wpad

> Frame 1: 217 bytes on wire (1736 bits), 217 bytes captured (1736 bits) on interface \Device\NPF_{414FC362-8DF7-4881-AA2E-5BBF2D0DC14A
> Ethernet II, Src: IntelCor_58:ba:60 (bc:09:1b:58:ba:60), Dst: IPv4mcast_7f:ff:fa (01:00:5e:7f:ff:fa)
> Internet Protocol Version 4, Src: 10.120.113.25, Dst: 239.255.255.250
> User Datagram Protocol, Src Port: 52733, Dst Port: 1900
> Simple Service Discovery Protocol

0000  01 00 5e 7f ff fa bc 09  1b 58 ba 60 08 00 45 00   ··^·····  ·X·`··E·
0010  00 cb 9b 6d 00 00 01 11  b2 29 0a 78 71 19 ef ff   ···m····  ·)·xq···
0020  ff fa cd fd 07 6c 00 b7  3f eb 4d 2d 53 45 41 52   ·····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 31 32 2e 30 2e 31 37  32 32 2e 35 38 20 57 69   112.0.17  22.58 Wi
00d0  6e 64 6f 77 73 0d 0a 0d  0a                        ndows····

User Datagram Protocol: Protocol        Packets: 55375 · Displayed: 14453 (26.1%)        Profile: Default
```

4. Udp:



*Wi-Fi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

udp.checksum

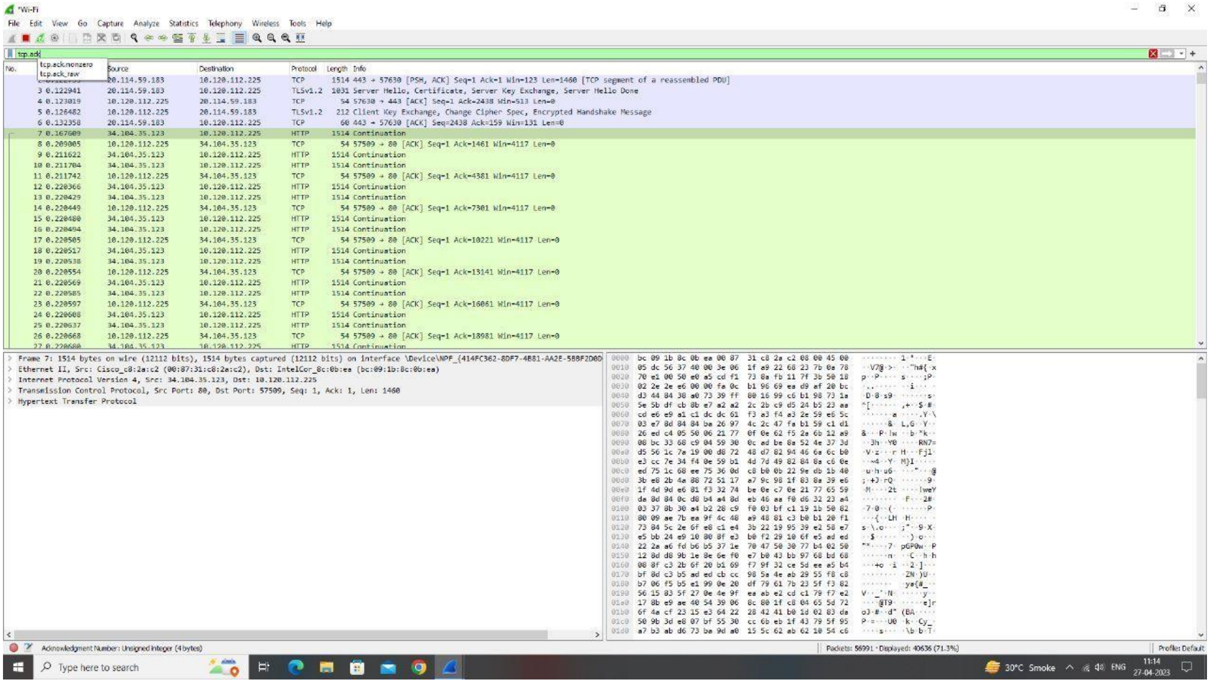
```
No.          Time       Source         Destination       Protocol  Length  Info
      26674 28.673563  10.120.112.15  255.255.255...  UDP              125 10004 → 10004 Len=83
      26675 28.673624  10.120.112.15  255.255.255...  UDP              125 10004 → 10004 Len=83
      27642 31.743446  10.120.112.15  255.255.255...  UDP              125 10004 → 10004 Len=83
      29358 34.712655  10.120.112.15  255.255.255...  UDP              125 10004 → 10004 Len=83
      29361 34.712775  10.120.112.15  255.255.255...  UDP              125 10004 → 10004 Len=83
      29720 37.683376  10.120.112.15  255.255.255...  UDP              125 10004 → 10004 Len=83
      29721 37.683390  10.120.112.15  255.255.255...  UDP              125 10004 → 10004 Len=83
      29791 40.654743  10.120.112.15  255.255.255...  UDP              125 10004 → 10004 Len=83
      29948 43.728336  10.120.112.15  255.255.255...  UDP              125 10004 → 10004 Len=83
      29949 43.728378  10.120.112.15  255.255.255...  UDP              125 10004 → 10004 Len=83
      32683 46.697777  10.120.112.15  255.255.255...  UDP              125 10004 → 10004 Len=83
      36987 52.744655  10.120.112.15  255.255.255...  UDP              125 10004 → 10004 Len=83
      36989 52.744671  10.120.112.15  255.255.255...  UDP              125 10004 → 10004 Len=83
      37047 55.706949  10.120.112.15  255.255.255...  UDP              125 10004 → 10004 Len=83
      37048 55.706988  10.120.112.15  255.255.255...  UDP              125 10004 → 10004 Len=83
      37127 58.679459  10.120.112.15  255.255.255...  UDP              125 10004 → 10004 Len=83
      37130 58.690828  10.120.112.15  255.255.255...  UDP              125 10004 → 10004 Len=83
      37225 61.644934  10.120.112.15  255.255.255...  UDP              125 10004 → 10004 Len=83
      38595 84.180749  10.120.110.1…  255.255.255...  UDP              125 10004 → 10004 Len=83
      38596 84.180772  10.120.110.1…  255.255.255...  UDP              125 10004 → 10004 Len=83
      38838 87.255419  10.120.110.1…  255.255.255...  UDP              125 10004 → 10004 Len=83
      38842 87.268575  10.120.110.1…  255.255.255...  UDP              125 10004 → 10004 Len=83
      38987 90.218589  10.120.110.1…  255.255.255...  UDP              125 10004 → 10004 Len=83
      38988 90.218613  10.120.110.1…  255.255.255...  UDP              125 10004 → 10004 Len=83
      39128 93.291240  10.120.110.1…  255.255.255...  UDP              125 10004 → 10004 Len=83
      39332 96.167772  10.120.110.1…  255.255.255...  UDP              125 10004 → 10004 Len=83
```

```
> Frame 26674: 125 bytes on wire (1000 bits), 125 bytes captured (1000 bits) on interface \Device\NPF_{414FC362-8DF7-4B81-AA2E-588F2D0D
> Ethernet II, Src: IntelCor_b7:eb:89 (a4:02:b9:b7:eb:89), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
> Internet Protocol Version 4, Src: 10.120.112.15, Dst: 255.255.255.255
> User Datagram Protocol, Src Port: 10004, Dst Port: 10004
> Data (83 bytes)
```

```
0000  ff ff ff ff ff ff a4 02  b9 b7 eb 89 08 00 45 00   ········ ······E·
0010  00 6f 5f 50 00 00 80 11  60 a7 0a 78 70 0f ff ff   ·o_P···· `··xp···
0020  ff ff 27 14 27 14 00 5b  33 ff 3c 58 4d 4c 3e 3c   ··'·'··[ 3·<XML><
0030  50 61 63 6b 65 74 54 79  70 65 3e 52 65 71 75 65   PacketTy pe>Reque
0040  73 74 3c 2f 50 61 63 6b  65 74 54 79 70 65 3e 0a   st</Pack etType>·
0050  3c 50 72 6f 64 75 63 74  4e 61 6d 65 3e 41 50 47   <Product Name>APG
0060  20 41 74 77 6f 6f 64 3c  2f 50 72 6f 64 75 63 74    Atwood< /Product
0070  4e 61 6d 65 3e 0a 3c 2f  58 4d 4c 3e 0a            Name>·</ XML>·
```

Sorting "Info"... | Packets: 71757 · Displayed: 28283 (39.4%) | Profile: Default

5. Http:



*Wi-Fi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
tcp.ack.nonzero
tcp.ack_raw

tcp.ack

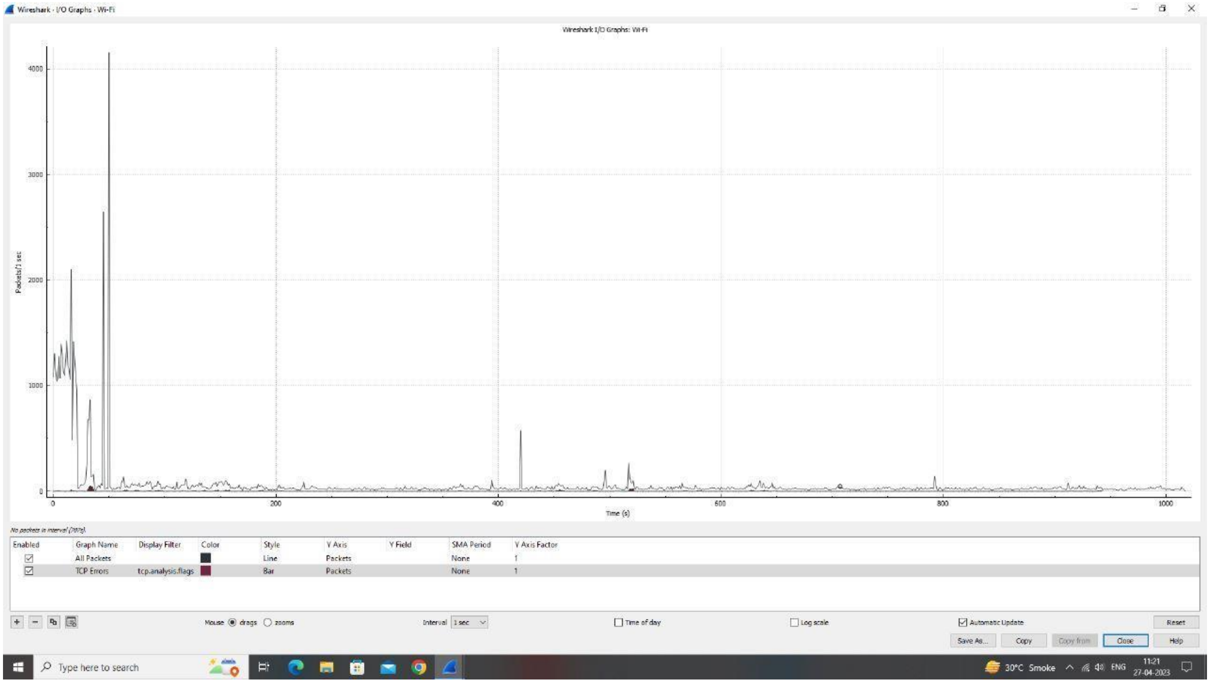
```
No.     Time       Source           Destination      Protocol  Length Info
                   20.114.59.183    10.120.112.225   TCP       1514 443 → 57630 [PSH, ACK] Seq=1 Ack=1 Win=123 Len=1460 [TCP segment of a reassembled PDU]
      3 0.122941   20.114.59.183    10.120.112.225   TLSv1.2   1031 Server Hello, Certificate, Server Key Exchange, Server Hello Done
      4 0.123019   10.120.112.225   20.114.59.183    TCP         54 57630 → 443 [ACK] Seq=1 Ack=2438 Win=513 Len=0
      5 0.126482   10.120.112.225   20.114.59.183    TLSv1.2    212 Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
      6 0.132358   20.114.59.183    10.120.112.225   TCP         60 443 → 57630 [ACK] Seq=2438 Ack=159 Win=131 Len=0
      7 0.167609   34.104.35.123    10.120.112.225   HTTP      1514 Continuation
      8 0.209005   10.120.112.225   34.104.35.123    TCP         54 57509 → 80 [ACK] Seq=1 Ack=1461 Win=4117 Len=0
      9 0.211622   34.104.35.123    10.120.112.225   HTTP      1514 Continuation
     10 0.211704   34.104.35.123    10.120.112.225   HTTP      1514 Continuation
     11 0.211742   10.120.112.225   34.104.35.123    TCP         54 57509 → 80 [ACK] Seq=1 Ack=4381 Win=4117 Len=0
     12 0.220366   34.104.35.123    10.120.112.225   HTTP      1514 Continuation
     13 0.220429   34.104.35.123    10.120.112.225   HTTP      1514 Continuation
     14 0.220449   10.120.112.225   34.104.35.123    TCP         54 57509 → 80 [ACK] Seq=1 Ack=7301 Win=4117 Len=0
     15 0.220480   34.104.35.123    10.120.112.225   HTTP      1514 Continuation
     16 0.220494   34.104.35.123    10.120.112.225   HTTP      1514 Continuation
     17 0.220505   10.120.112.225   34.104.35.123    TCP         54 57509 → 80 [ACK] Seq=1 Ack=10221 Win=4117 Len=0
     18 0.220517   34.104.35.123    10.120.112.225   HTTP      1514 Continuation
     19 0.220538   34.104.35.123    10.120.112.225   HTTP      1514 Continuation
     20 0.220554   10.120.112.225   34.104.35.123    TCP         54 57509 → 80 [ACK] Seq=1 Ack=13141 Win=4117 Len=0
     21 0.220569   34.104.35.123    10.120.112.225   HTTP      1514 Continuation
     22 0.220585   34.104.35.123    10.120.112.225   HTTP      1514 Continuation
     23 0.220597   10.120.112.225   34.104.35.123    TCP         54 57509 → 80 [ACK] Seq=1 Ack=16061 Win=4117 Len=0
     24 0.220608   34.104.35.123    10.120.112.225   HTTP      1514 Continuation
     25 0.220637   34.104.35.123    10.120.112.225   HTTP      1514 Continuation
     26 0.220668   10.120.112.225   34.104.35.123    TCP         54 57509 → 80 [ACK] Seq=1 Ack=18981 Win=4117 Len=0
     27 0.220680   34.104.35.123    10.120.112.225   HTTP      1514 Continuation
```

```
> Frame 7: 1514 bytes on wire (12112 bits), 1514 bytes captured (12112 bits) on interface \Device\NPF_{414FC362-8DF7-4B81-AA2E-588F2D0D
> Ethernet II, Src: Cisco_c8:2a:c2 (00:87:31:c8:2a:c2), Dst: IntelCor_8c:0b:ea (bc:09:1b:8c:0b:ea)
> Internet Protocol Version 4, Src: 34.104.35.123, Dst: 10.120.112.225
> Transmission Control Protocol, Src Port: 80, Dst Port: 57509, Seq: 1, Ack: 1, Len: 1460
> Hypertext Transfer Protocol
```

```
0000  bc 09 1b 8c 0b ea 00 87  31 c8 2a c2 08 00 45 00   ········ 1·*···E·
0010  05 dc 56 37 40 00 3e 06  1f a9 22 68 23 7b 0a 78   ··V7@·>· ··"h#{·x
0020  70 e1 00 50 e0 a5 cd f1  73 8a fb 11 7f 3b 50 18   p··P···· s····;P·
0030  02 2e 2e e6 00 00 fa 0c  b1 96 69 ea d9 af 20 bc   ·..····· ··i··· ·
0040  d3 44 84 38 a0 73 39 ff  80 16 99 c6 b1 98 73 1a   ·D·8·s9· ······s·
0050  5e 5b df cb 8b e7 a2 a2  2c 2b c9 d5 24 b5 23 aa   ^[······ ,+··$·#·
0060  cd e6 e9 a1 c1 dc dc 61  f3 a3 f4 a3 2e 59 e6 5c   ·······a ····.Y·\
0070  03 e7 8d 84 84 ba 26 97  4c 2c 47 fa b1 59 c1 d1   ······&· L,G··Y··
0080  26 ed c4 05 50 06 21 77  0f 0e 62 f5 2a 6b 12 a9   &···P·!w ··b·*k··
0090  08 bc 33 68 c9 04 59 30  0c ad be 8a 52 4e 37 3d   ··3h··Y0 ····RN7=
00a0  d5 56 1c 7a 19 00 d8 72  48 d7 82 94 46 6a 6c b0   ·V·z···r H···Fjl·
00b0  e3 cc 7e 34 f4 0e 59 b1  4d 7d 49 82 84 8a c6 0e   ··~4··Y· M}I·····
00c0  ed 75 1c 68 ee 75 36 0d  c8 b0 0b 22 9e db 1b 40   ·u·h·u6· ···"···@
00d0  3b e8 2b 4a 88 72 51 17  a7 9c 98 1f 83 8a 39 e6   ;·+J·rQ· ······9·
00e0  1f 4d 9d e6 81 f3 32 74  be 0e c7 0e 21 77 65 59   ·M····2t ····!weY
00f0  da 8d 84 0c d8 b4 a4 8d  eb 46 aa f0 d6 32 23 a4   ········ ·F···2#·
0100  03 37 8b 30 a4 b2 28 c9  f0 03 bf c1 19 1b 50 82   ·7·0··(· ······P·
0110  80 09 ae 7b ea 9f 4c 48  a9 48 81 c3 b0 b1 20 f1   ···{··LH ·H···· ·
0120  73 84 5c 2e 6f e8 c1 e4  3b 22 19 95 39 e2 58 e7   s·\.o··· ;"··9·X·
0130  e5 bb 24 e9 10 80 8f e3  b0 f2 29 10 6f e5 ad ed   ··$····· ··)·o···
0140  22 2a a6 fd b6 b5 37 1e  70 47 50 30 77 b4 02 50   "*····7· pGP0w··P
0150  12 8d d8 9b 1e 8e 6e f0  e7 b0 43 bb 97 68 bd 68   ······n· ··C··h·h
0160  08 8f c3 2b 6f 20 b1 69  f7 9f 32 ce 5d ee a5 b4   ···+o ·i ··2·]···
0170  bf 8d c3 b5 ad ed cb cc  98 5a 4e ab 29 55 f8 c8   ········ ·ZN·)U··
0180  b7 06 f5 b5 e1 99 0e 20  df 79 61 7b 23 5f f3 82   ·······  ·ya{#_··
0190  56 15 83 5f 27 0e 4e 9f  ea ab e2 cd c1 79 f7 e2   V··_'·N· ·····y··
01a0  17 8b e9 ae 40 54 39 06  8c 80 1f c8 04 65 5d 72   ····@T9· ·····e]r
01b0  6f 4a cf 23 15 e3 64 22  28 42 41 b0 1d 02 83 da   oJ·#··d" (BA·····
01c0  50 9b 3d e8 07 bf 55 30  cc 6b eb 1f 43 79 5f 95   P·=···U0 ·k··Cy_·
01d0  a7 b3 ab d6 73 ba 9d a0  15 5c 62 ab 62 10 54 c6   ····s··· ·\b·b·T·
```

Acknowledgment Number: Unsigned integer (4 bytes) | Packets: 56991 · Displayed: 40636 (71.3%) | Profile: Default

6. I/O Graph:



No packets in interval (707s).

Enabled	Graph Name	Display Filter	Color	Style	Y Axis	Y Field	SMA Period	Y Axis Factor
☑	All Packets		■	Line	Packets		None	1
☑	TCP Errors	tcp.analysis.flags	■	Bar	Packets		None	1

Mouse ● drags ○ zooms

Interval 1 sec

□ Time of day

□ Log scale

☑ Automatic Update

Conclusion: Thus, we have simulated Packet Capturing in Wireshark.