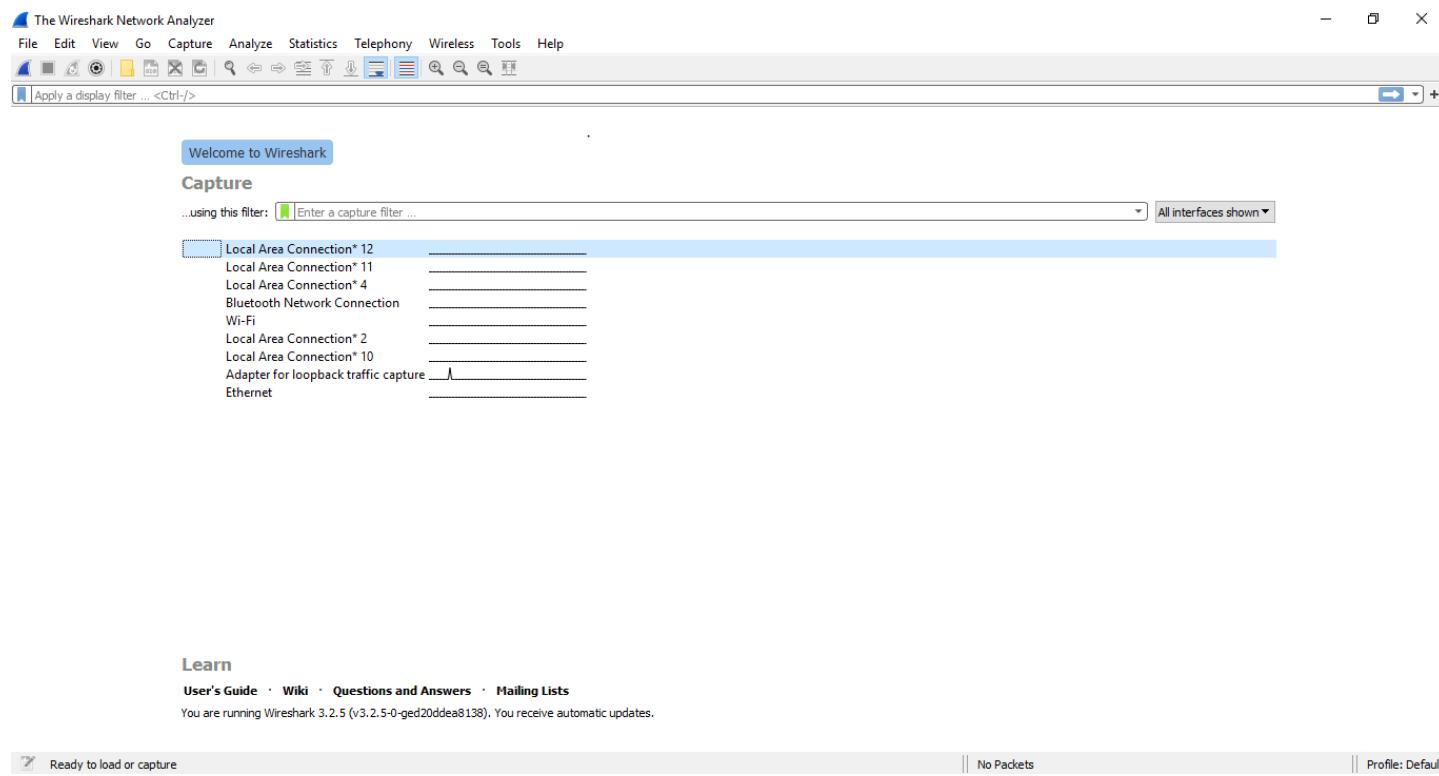


Name : Md. Sohag Hossain
ID : IT-17060
Lab report no : 2
Name of the lab report : Wireshark display
Objectives : To learn basic packet analysis using Wireshark

Theory:

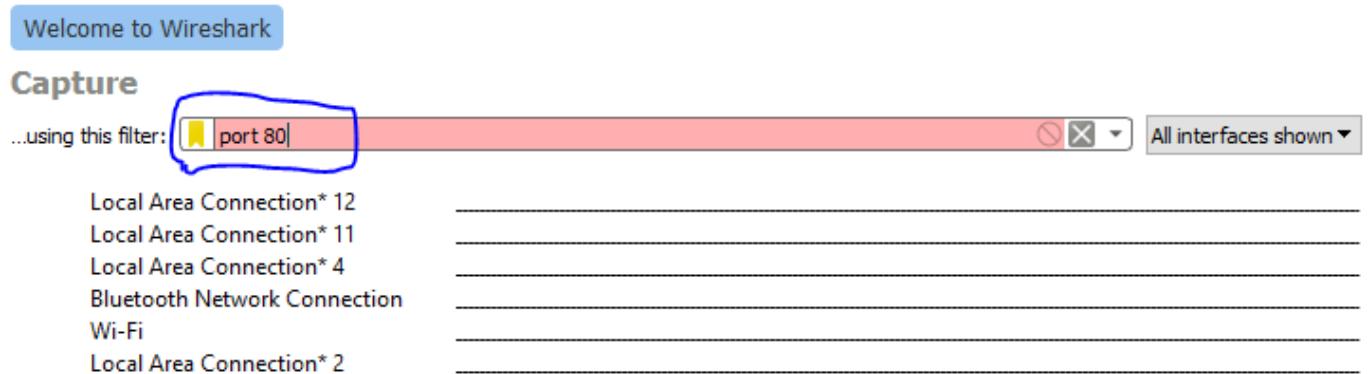
Wireshark is the world's leading network traffic analyzer, and an essential tool for any security professional or systems administrator. This free software lets you analyze network traffic in real time, and is often the best tool for troubleshooting issues on your network.

Opening display of Wireshark:

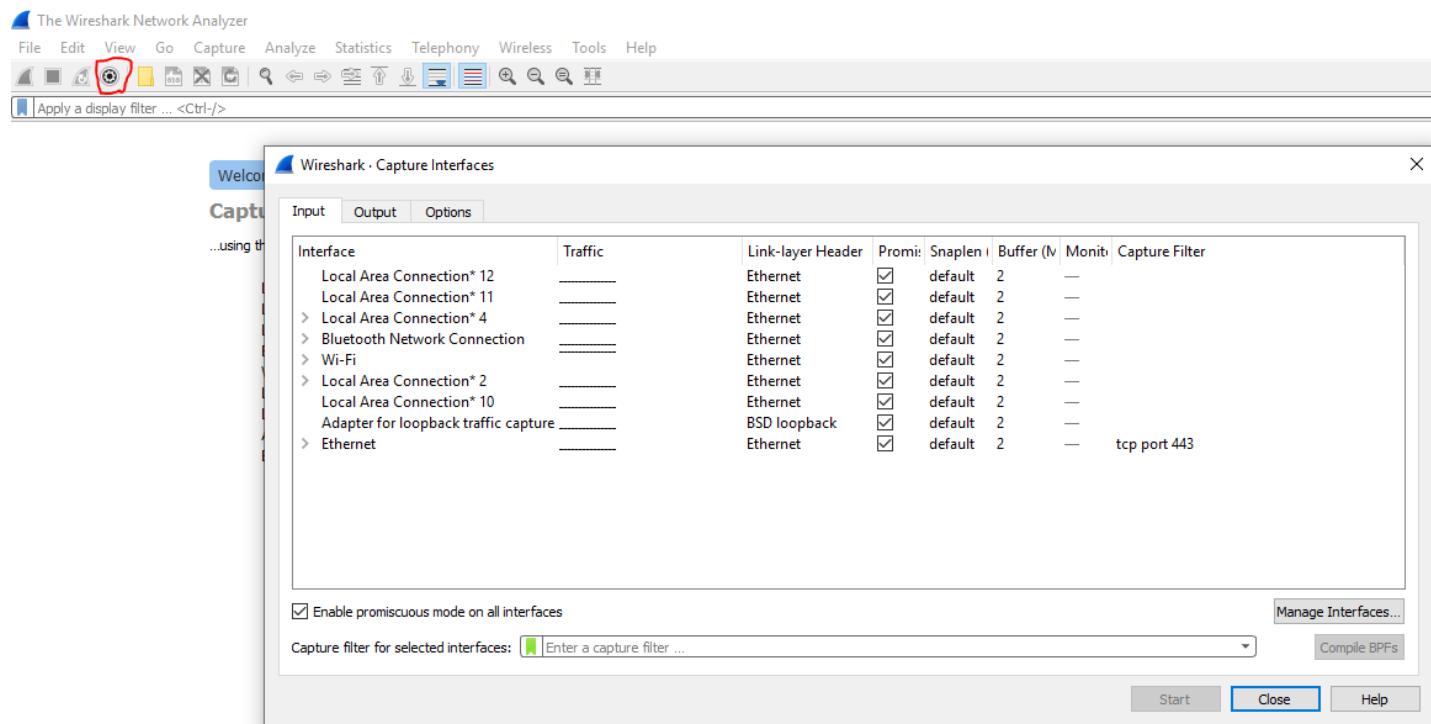


Packet Capturing:

In order to packet capturing we need click capture bar and write any packet name such as port 80, tcp port 443, tcp port http and many others.



If we click the red marked option we will see the Capture Interface



Learn

[User's Guide](#) · [Wiki](#) · [Questions and Answers](#) · [Mailing Lists](#)

You are running Wireshark 3.2.5 (v3.2.5-0-ged20ddea8138). You receive automatic updates.

Activate V
Go to Setting

Welcome to Wireshark

Capture

...using this filter:	<input type="text"/> Enter a capture filter ...
Local Area Connection* 12	_____
Local Area Connection* 11	_____
Local Area Connection* 4	_____
Bluetooth Network Connection	_____
Wi-Fi	_____
Local Area Connection* 2	_____
Local Area Connection* 10	_____
Adapter for loopback traffic capture	_____
Ethernet	_____

If we click the yellow highlighted portion(Wi-Fi) then we will see the below figure.

The screenshot shows the Wireshark interface with the title bar "*Wi-Fi". The menu bar includes File, Edit, View, Go, Capture, Analyze, Statistics, Telephony, Wireless, Tools, and Help. The toolbar includes icons for opening files, saving, zooming, and filtering. A display filter bar at the top says "Apply a display filter ... <ctrl>/>". The main window displays a list of network packets. The first few packets are highlighted in yellow. The details pane shows the following information for the first packet:

No.	Time	Source	Destination	Protocol	Length	Info
110	4.573919	192.168.43.78	192.168.43.255	NBNS	92	Name query NB WORKGROUP<1>
111	4.642189	192.168.43.1	192.168.43.78	DNS	184	Standard query response 0x9e60 A client.wns.windows.com CNAME wns.notify.windows.com.akadns.n...
112	4.642827	192.168.43.78	40.119.211.203	TCP	66	50192 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
113	4.645622	192.168.43.1	192.168.43.78	DNS	122	Standard query response 0xb604 A arc.msn.com CNAME arc.msn.com.nsatc.net A 20.189.123.78
114	4.646864	192.168.43.78	20.189.123.78	TCP	66	50192 → 443 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM=1
115	4.921264	192.168.43.1	192.168.43.78	DNS	119	Standard query response 0xa020 A clients4.google.com CNAME clients.l.google.com A 172.217.166...
116	4.921779	192.168.43.78	172.217.166.110	TCP	66	50193 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1

The details pane also contains expanded information about the source address:

- Address: Broadcast (ff:ff:ff:ff:ff:ff)
-1. = LG bit: Locally administered address (this is NOT the factory default)
-1 = IG bit: Group address (multicast/broadcast)

Source: IntelCor_9a:5a:2e (30:e3:7a:9a:5a:2e)

- Address: IntelCor_9a:5a:2e (30:e3:7a:9a:5a:2e)
-0. = LG bit: Globally unique address (factory default)
-0. = IG bit: Individual address (unicast)

Type: IPv4 (0x0800)

The bytes pane shows the raw hex and ASCII data for the selected packet.

*Wi-Fi

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Apply a display filter ... <Ctrl-/>

No.	Time	Source	Destination	Protocol	Length	Info
206	68.196155	192.168.43.78	151.101.9.132	TCP	55	[TCP Keep-Alive] 49783 → 443 [ACK] Seq=1 Ack=1 Win=259 Len=1
207	68.198390	192.168.43.78	74.125.24.189	TCP	55	[TCP Keep-Alive] 49775 → 443 [ACK] Seq=1 Ack=1 Win=260 Len=1
208	68.375130	151.101.9.132	192.168.43.78	TCP	66	[TCP Keep-Alive ACK] 443 → 49783 [ACK] Seq=1 Ack=2 Win=60 Len=0 SLE=1 SRE=2
209	68.382308	74.125.24.189	192.168.43.78	TCP	66	[TCP Keep-Alive ACK] 443 → 49775 [ACK] Seq=1 Ack=2 Win=281 Len=0 SLE=1 SRE=2
210	68.658020	192.168.43.78	151.101.9.132	TCP	55	[TCP Keep-Alive] 49782 → 443 [ACK] Seq=1 Ack=1 Win=255 Len=1
211	68.817013	151.101.9.132	192.168.43.78	TCP	66	[TCP Keep-Alive ACK] 443 → 49782 [ACK] Seq=1 Ack=2 Win=62 Len=0 SLE=1 SRE=2

```
> Frame 1: 75 bytes on wire (600 bits), 75 bytes captured (600 bits) on interface \Device\NPF_{4CC6E86C-C9F3-4D79-B8F7-DC6DD308F6BD}, id 0
> Ethernet II, Src: IntelCor_9a:5a:2e (30:e3:7a:9a:5a:2e), Dst: XiaomiCo_bd:05:78 (4c:49:e3:bd:05:78)
> Internet Protocol Version 4, Src: 192.168.43.78, Dst: 74.125.24.189
> User Datagram Protocol, Src Port: 59036, Dst Port: 443
> Data (33 bytes)

0000  4c 49 e3 bd 05 78 30 e3 7a 9a 5a 2e 08 00 45 00  LI...x0 z-Z..E-
0010  00 3d 59 a3 40 00 80 11 51 dc c0 a8 2b 4e 4a 7d  .=Y@... 0...+N}
0020  18 bd e6 9c 01 bb 00 29 b0 31 54 11 a5 ca 14 9e  .... ) 1T.....
0030  a4 3d 9c 98 0c e0 3e f8 b1 66 23 0e 64 83 6b 09  =....> f#-d-k-
0040  03 da 51 01 d8 00 e1 81 05 59 c5  ..Q.....Y.
```

_packets: 211 |Displayed: 211 (100.0%) | Profile: Default

Here the total number of packets is 211.

List of Captured packet:

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Apply a display filter ... <Ctrl-/>

No.	Time	Source	Destination	Protocol	Length	Info
3	15.001026	192.168.43.78	74.125.24.189	UDP	75	59036 → 443 Len=33
4	15.230616	74.125.24.189	192.168.43.78	UDP	68	443 → 59036 Len=26
5	24.316006	192.168.43.78	74.125.130.188	TLSv1...	80	Application Data
6	24.477114	74.125.130.188	192.168.43.78	TCP	54	5228 → 49719 [ACK] Seq=1 Ack=27 Win=265 Len=0
7	24.477114	74.125.130.188	192.168.43.78	TLSv1...	80	Application Data
8	24.517085	192.168.43.78	74.125.130.188	TCP	54	49719 → 5228 [ACK] Seq=27 Ack=27 Win=260 Len=0

```
> Frame 1: 86 bytes on wire (688 bits), 86 bytes captured (688 bits) on interface \Device\NPF_{4CC6E86C-C9F3-4D79-B8F7-DC6DD308F6BD}, id 0
> Ethernet II, Src: XiaomiCo_bd:05:78 (4c:49:e3:bd:05:78), Dst: IntelCor_9a:5a:2e (30:e3:7a:9a:5a:2e)
> Internet Protocol Version 4, Src: 74.125.24.189, Dst: 192.168.43.78
> User Datagram Protocol, Src Port: 443, Dst Port: 59036
> Data (44 bytes)
```

```
0000  30 e3 7a 9a 5a 2e 4c 49  e3 bd 05 78 08 00 45 08  0-z.Z.LI ...x..E-
0010  00 48 00 00 40 00 36 11  f5 6c 4a 7d 18 bd c0 a8  .H...@6..1J}....
0020  2b 4e 01 bb e6 9c 00 34  f2 f1 4d 71 9d 66 a6 55  +N.....4 ..Mq.f.U
0030  9e d1 5d ca 5b 2b f3 12  c9 88 00 84 c5 f5 f8 e5  ...].+[... .....
0040  cd bb cf 96 1a c0 52 d0  ab 6b ff eb 37 b8 46 9c  .....R..k..7.F.
0050  52 42 1a 1f cf 2a  RB...*
```

TCP packet capture:

*Wi-Fi

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

tcp

No.	Time	Source	Destination	Protocol	Length	Info
115	156.989805	192.168.43.78	74.125.130.188	TCP	55	[TCP Keep-Alive] 49719 → 5228 [ACK] Seq=1 Ack=1 Win=260 Len=1
116	157.240083	74.125.130.188	192.168.43.78	TCP	66	[TCP Keep-Alive ACK] 5228 → 49719 [ACK] Seq=1 Ack=2 Win=265 Len=0 SLE=1 SRE=2
123	182.635888	192.168.43.78	172.217.163.206	TCP	55	[TCP Keep-Alive] 49806 → 443 [ACK] Seq=1 Ack=58 Win=260 Len=1
124	182.831507	172.217.163.206	192.168.43.78	TCP	54	443 → 49806 [RST] Seq=58 Win=0 Len=0
133	202.243637	192.168.43.78	74.125.130.188	TCP	55	[TCP Keep-Alive] 49719 → 5228 [ACK] Seq=1 Ack=1 Win=260 Len=1
134	202.406402	74.125.130.188	192.168.43.78	TCP	66	[TCP Keep-Alive ACK] 5228 → 49719 [ACK] Seq=1 Ack=2 Win=265 Len=0 SLE=1 SRE=2
183	247.406371	192.168.43.78	74.125.130.188	TCP	55	[TCP Keep-Alive] 49719 → 5228 [ACK] Seq=1 Ack=1 Win=260 Len=1

```
> Frame 60: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface \Device\NPF_{4CC6E86C-C9F3-4D79-B8F7-DC6DD308F6BD}, id 0
> Ethernet II, Src: XiaomiCo_bd:05:78 (4c:49:e3:bd:05:78), Dst: IntelCor_9a:5a:2e (30:e3:7a:9a:5a:2e)
> Internet Protocol Version 4, Src: 74.125.130.188, Dst: 192.168.43.78
> Transmission Control Protocol, Src Port: 5228, Dst Port: 49719, Seq: 1, Ack: 2, Len: 0
```

0000	30 e3 7a 9a 5a 2e 4c 49	e3 bd 05 78 08 00 45 08	0·z·Z.LI ···x··E·
0010	00 34 06 3c 00 00 36 06	c5 50 4a 7d 82 bc c0 a8	·4<··6· ·P]···
0020	2b 4e 14 6c c2 37 75 56	22 d2 4e 5e 50 7c 80 10	+N·1·7uV "·N^P ··
0030	01 09 74 29 00 00 01 01	05 0a 4e 5e 50 7b 4e 5e	·t)···· ·N^P[N^
0040	50 7c		P

Transmission Control Protocol: Protocol

|| Packets: 192 · Displayed: 34 (17.7%) · Dropped: 0 (0.0%)

SSDP packet capture:

ssdp

No.	Time	Source	Destination	Protocol	Length	Info
61	70.225266	192.168.43.78	239.255.255.250	SSDP	216	M-SEARCH * HTTP/1.1
62	71.226029	192.168.43.78	239.255.255.250	SSDP	216	M-SEARCH * HTTP/1.1
65	72.226590	192.168.43.78	239.255.255.250	SSDP	216	M-SEARCH * HTTP/1.1
66	73.227890	192.168.43.78	239.255.255.250	SSDP	216	M-SEARCH * HTTP/1.1
126	190.237657	192.168.43.78	239.255.255.250	SSDP	216	M-SEARCH * HTTP/1.1
128	191.238100	192.168.43.78	239.255.255.250	SSDP	216	M-SEARCH * HTTP/1.1
129	192.239185	192.168.43.78	239.255.255.250	SSDP	216	M-SEARCH * HTTP/1.1

> Frame 61: 216 bytes on wire (1728 bits), 216 bytes captured (1728 bits) on interface \De
 > Ethernet II, Src: IntelCor_9a:5a:2e (30:e3:7a:9a:5a:2e), Dst: IPv4mcast_7f:ff:fa (01:00:
 > Internet Protocol Version 4, Src: 192.168.43.78, Dst: 239.255.255.250
 > User Datagram Protocol, Src Port: 62112, Dst Port: 1900
 ▼ Simple Service Discovery Protocol
 > M-SEARCH * HTTP/1.1\r\n
 HOST: 239.255.255.250:1900\r\n
 MAN: "ssdp:discover"\r\n

0000	01 00 5e 7f ff fa 30 e3	7a 9a 5a 2e 08 00 45 00	..^...0. z.Z..E.
0010	00 ca 34 c8 00 00 01 11	a8 6a c0 a8 2b 4e ef ff	.4..... j...+N..
0020	ff fa f2 a0 07 6c 00 b6	2a d0 4d 2d 53 45 41 521.. *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 47 6f 6f 67 6c 65 20	43 68 72 6f 6d 65 2f 38	Google Chrome/8
00c0	34 2e 30 2e 34 31 34 37	2e 31 30 35 20 57 69 6e	4.0.4147 .105 Win
00d0	64 6f 77 73 0d 0a 0d 0a		dows....

UDP packet capture:

*Wi-Fi

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

udp

No.	Time	Source	Destination	Protocol	Length	Info
49	56.915468	74.125.24.189	192.168.43.78	UDP	68	443 → 59036 Len=26
50	56.961919	172.217.163.78	192.168.43.78	UDP	67	443 → 62111 Len=25
51	57.041848	172.217.163.78	192.168.43.78	UDP	67	443 → 62111 Len=25
52	57.057638	172.217.163.78	192.168.43.78	UDP	571	443 → 62111 Len=529
53	57.057638	172.217.163.78	192.168.43.78	UDP	277	443 → 62111 Len=235
54	57.058698	192.168.43.78	172.217.163.78	UDP	75	62111 → 443 Len=33
58	66.758219	74.125.24.189	192.168.43.78	UDP	86	443 → 59036 Len=44

> Frame 61: 216 bytes on wire (1728 bits), 216 bytes captured (1728 bits) on interface \Device\NPF_{...}

> Ethernet II, Src: IntelCor_9a:5a:2e (30:e3:7a:9a:5a:2e), Dst: IPv4mcast_7f:ff:fa (01:00:00:00:00:00)

> Internet Protocol Version 4, Src: 192.168.43.78, Dst: 239.255.255.250

> User Datagram Protocol, Src Port: 62112, Dst Port: 1900

Simple Service Discovery Protocol

M-SEARCH * HTTP/1.1\r\n

HOST: 239.255.255.250:1900\r\n

MAN: "ssdp:discover"\r\n

0000	01 00 5e 7f ff fa 30 e3 7a 9a 5a 2e 08 00 45 00	..^...0. z-Z...E.
0010	00 ca 34 c8 00 00 01 11 a8 6a c0 a8 2b 4e ef ff	.4..... j...+N..
0020	ff fa f2 a0 07 6c 00 b6 2a d0 4d 2d 53 45 41 521.. *-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:discover".
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	1:1.. USE R-AGENT:
00b0	20 47 6f 6f 67 6c 65 20 43 68 72 6f 6d 65 2f 38	Google Chrome/8
00c0	34 2e 30 2e 34 31 34 37 2e 31 30 35 20 57 69 6e	4.0.4147 .105 Win
00d0	64 6f 77 73 0d 0a 0d 0a	dows... .

