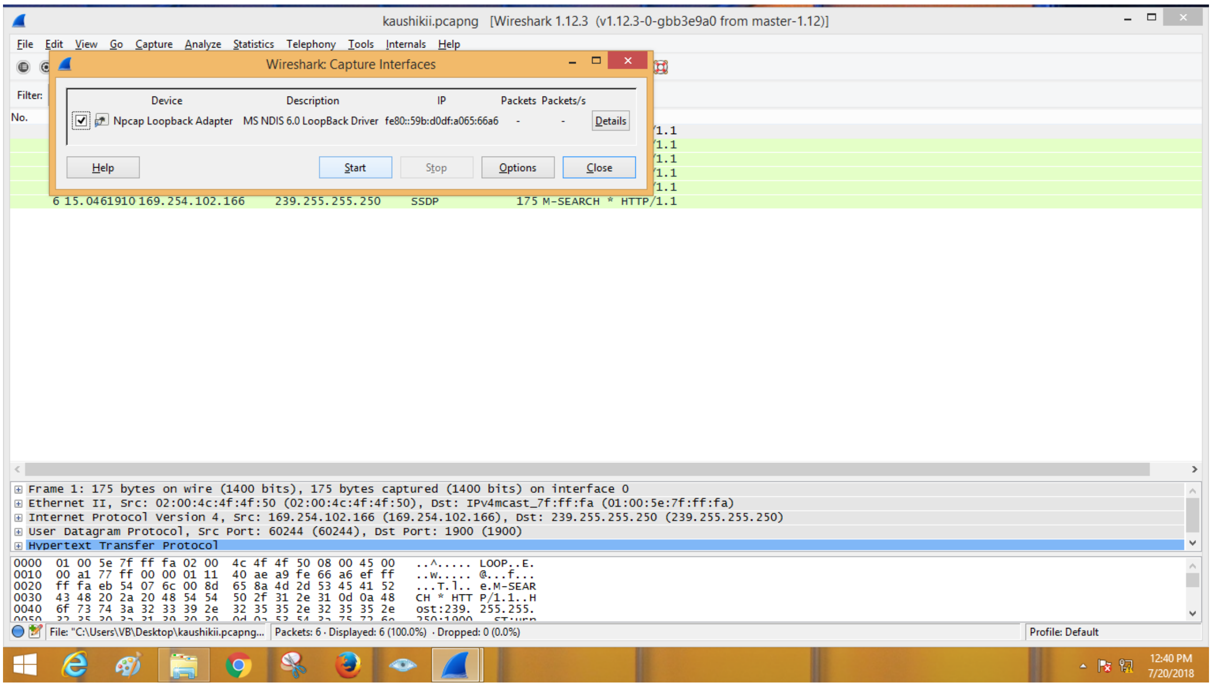
Practical 4

Aim: network vulnerability using Wireshark..

Open windows system and go to Wireshark application.

Use different functions like capture, filter and inspection of packets.

1. Capture


kaushikii.pcapng [Wireshark 1.12.3 (v1.12.3-0-gbb3e9a0 from master-1.12)]
File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help
Filter:
No.
Wireshark: Capture Interfaces
Help
Start
Stop
Options
Close
Details
Profile: Default
12:40 PM
7/20/2018

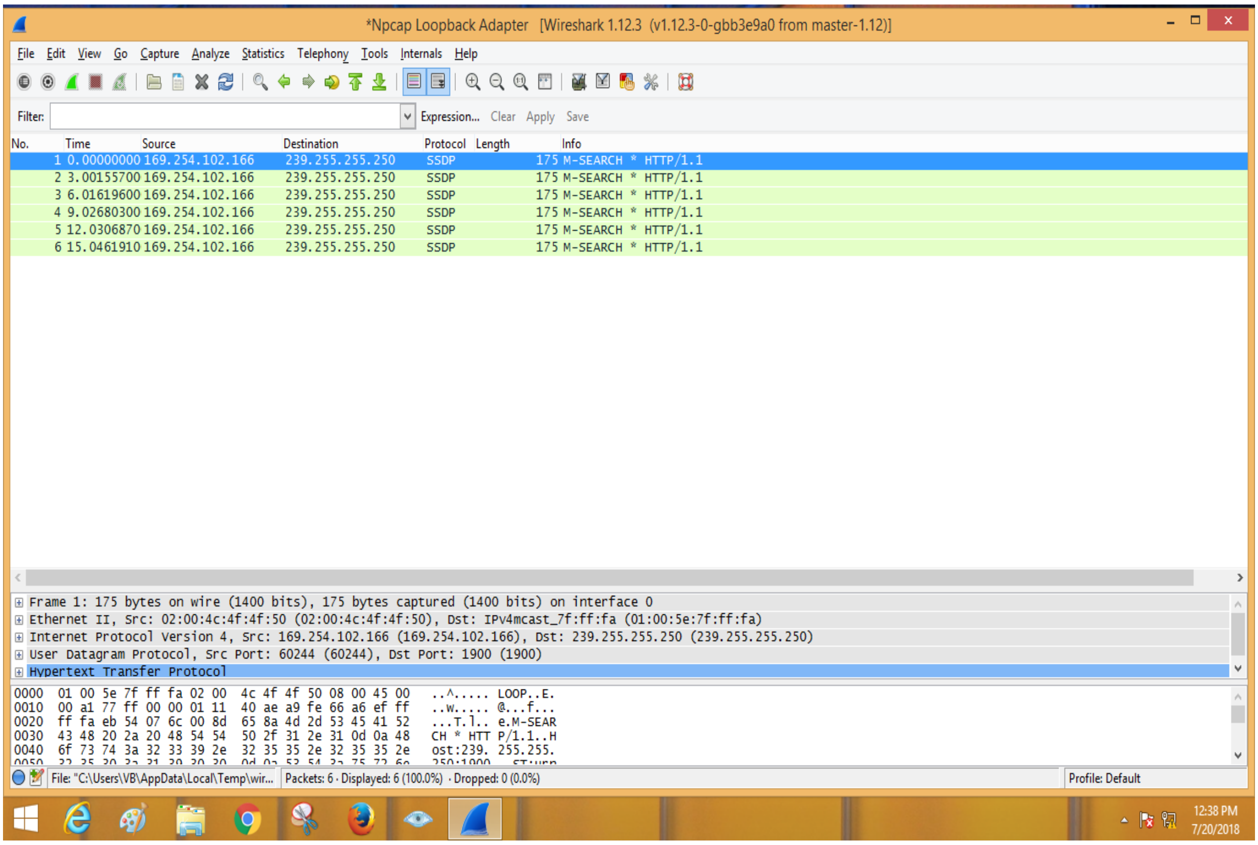
	Device	Description	IP	Packets	Packets/s
☑	Npcap Loopback Adapter	MS NDIS 6.0 LoopBack Driver	fe80::59b:d0df:a065:66a6	-	-

```
6 15.0461910 169.254.102.166    239.255.255.250    SSDP         175 M-SEARCH * HTTP/1.1
```

```
⊞ Frame 1: 175 bytes on wire (1400 bits), 175 bytes captured (1400 bits) on interface 0
⊞ Ethernet II, Src: 02:00:4c:4f:4f:50 (02:00:4c:4f:4f:50), Dst: IPv4mcast_7f:ff:fa (01:00:5e:7f:ff:fa)
⊞ Internet Protocol Version 4, Src: 169.254.102.166 (169.254.102.166), Dst: 239.255.255.250 (239.255.255.250)
⊞ User Datagram Protocol, Src Port: 60244 (60244), Dst Port: 1900 (1900)
⊞ Hypertext Transfer Protocol
```

```
0000  01 00 5e 7f ff fa 02 00  4c 4f 4f 50 08 00 45 00   ..^..... LOOP..E.
0010  00 a1 77 ff 00 00 01 11  40 ae a9 fe 66 a6 ef ff   ..w..... @...f...
0020  ff fa eb 54 07 6c 00 8d  65 8a 4d 2d 53 45 41 52   ...T.l.. e.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  6f 73 74 3a 32 33 39 2e  32 35 35 2e 32 35 35 2e   ost:239. 255.255.
```

File: "C:\Users\VB\Desktop\kaushikii.pcapng... Packets: 6 · Displayed: 6 (100.0%) · Dropped: 0 (0.0%)


*Npcap Loopback Adapter [Wireshark 1.12.3 (v1.12.3-0-gbb3e9a0 from master-1.12)]
File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help
Filter:
Expression... Clear Apply Save

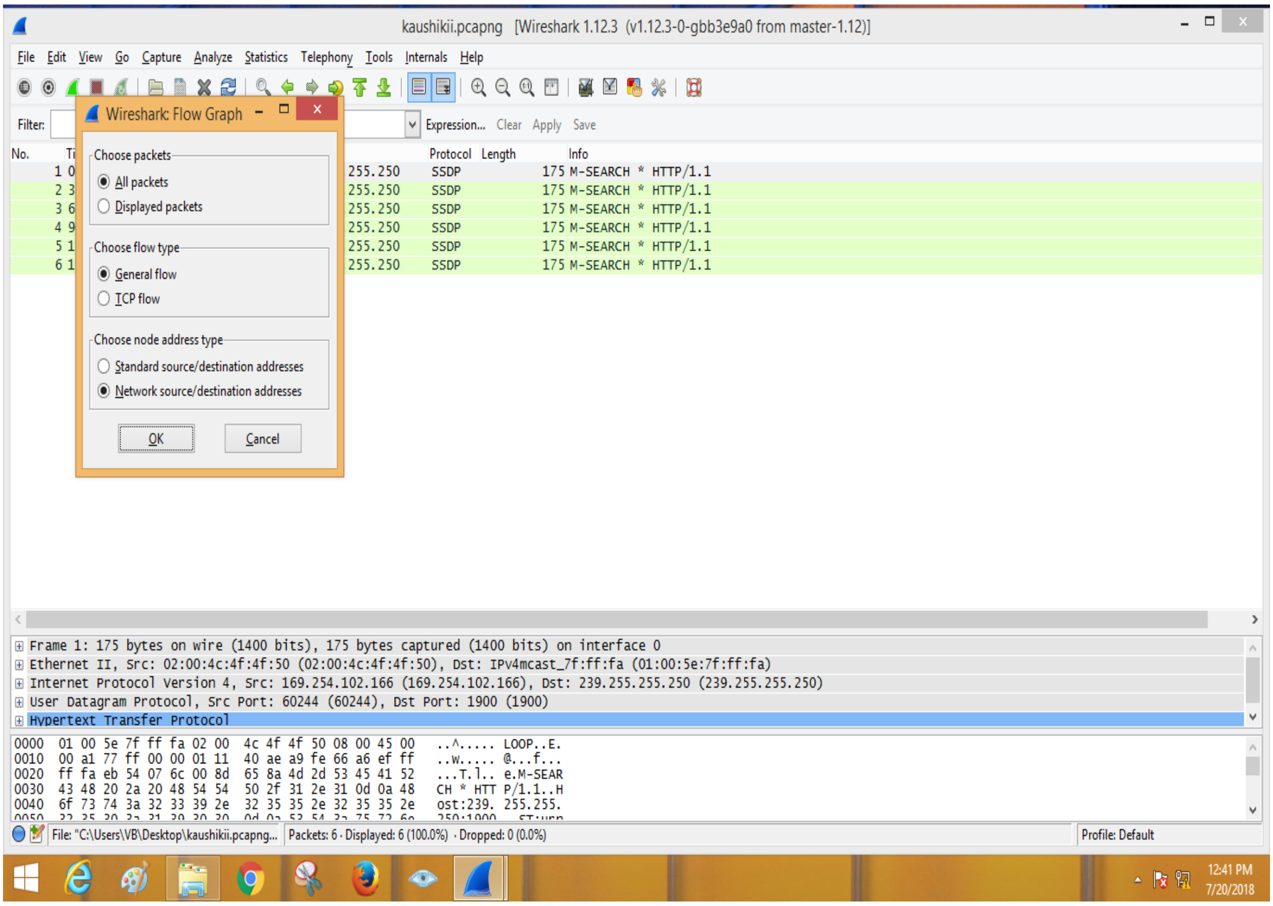
```
No.   Time       Source          Destination      Protocol  Length  Info
    1 0.00000000 169.254.102.166 239.255.255.250  SSDP         175 M-SEARCH * HTTP/1.1
    2 3.00155700 169.254.102.166 239.255.255.250  SSDP         175 M-SEARCH * HTTP/1.1
    3 6.01619600 169.254.102.166 239.255.255.250  SSDP         175 M-SEARCH * HTTP/1.1
    4 9.02680300 169.254.102.166 239.255.255.250  SSDP         175 M-SEARCH * HTTP/1.1
    5 12.0306870 169.254.102.166 239.255.255.250  SSDP         175 M-SEARCH * HTTP/1.1
    6 15.0461910 169.254.102.166 239.255.255.250  SSDP         175 M-SEARCH * HTTP/1.1
```

```
⊞ Frame 1: 175 bytes on wire (1400 bits), 175 bytes captured (1400 bits) on interface 0
⊞ Ethernet II, Src: 02:00:4c:4f:4f:50 (02:00:4c:4f:4f:50), Dst: IPv4mcast_7f:ff:fa (01:00:5e:7f:ff:fa)
⊞ Internet Protocol Version 4, Src: 169.254.102.166 (169.254.102.166), Dst: 239.255.255.250 (239.255.255.250)
⊞ User Datagram Protocol, Src Port: 60244 (60244), Dst Port: 1900 (1900)
⊞ Hypertext Transfer Protocol
```

```
0000  01 00 5e 7f ff fa 02 00  4c 4f 4f 50 08 00 45 00   ..^..... LOOP..E.
0010  00 a1 77 ff 00 00 01 11  40 ae a9 fe 66 a6 ef ff   ..w..... @...f...
0020  ff fa eb 54 07 6c 00 8d  65 8a 4d 2d 53 45 41 52   ...T.l.. e.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  6f 73 74 3a 32 33 39 2e  32 35 35 2e 32 35 35 2e   ost:239. 255.255.
0050  32 35 30 3a 31 39 30 30  0d 0a 53 54 3a 75 72 6e   250:1900 ..ST:urn
```

File: "C:\Users\VB\AppData\Local\Temp\wir... Packets: 6 · Displayed: 6 (100.0%) · Dropped: 0 (0.0%) Profile: Default

2. Satisticflowgraph


kaushikii.pcapng [Wireshark 1.12.3 (v1.12.3-0-gbb3e9a0 from master-1.12)]
File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help
Filter:
Expression... Clear Apply Save
Wireshark: Flow Graph

Choose packets
- ● All packets
- ○ Displayed packets

Choose flow type
- ● General flow
- ○ TCP flow

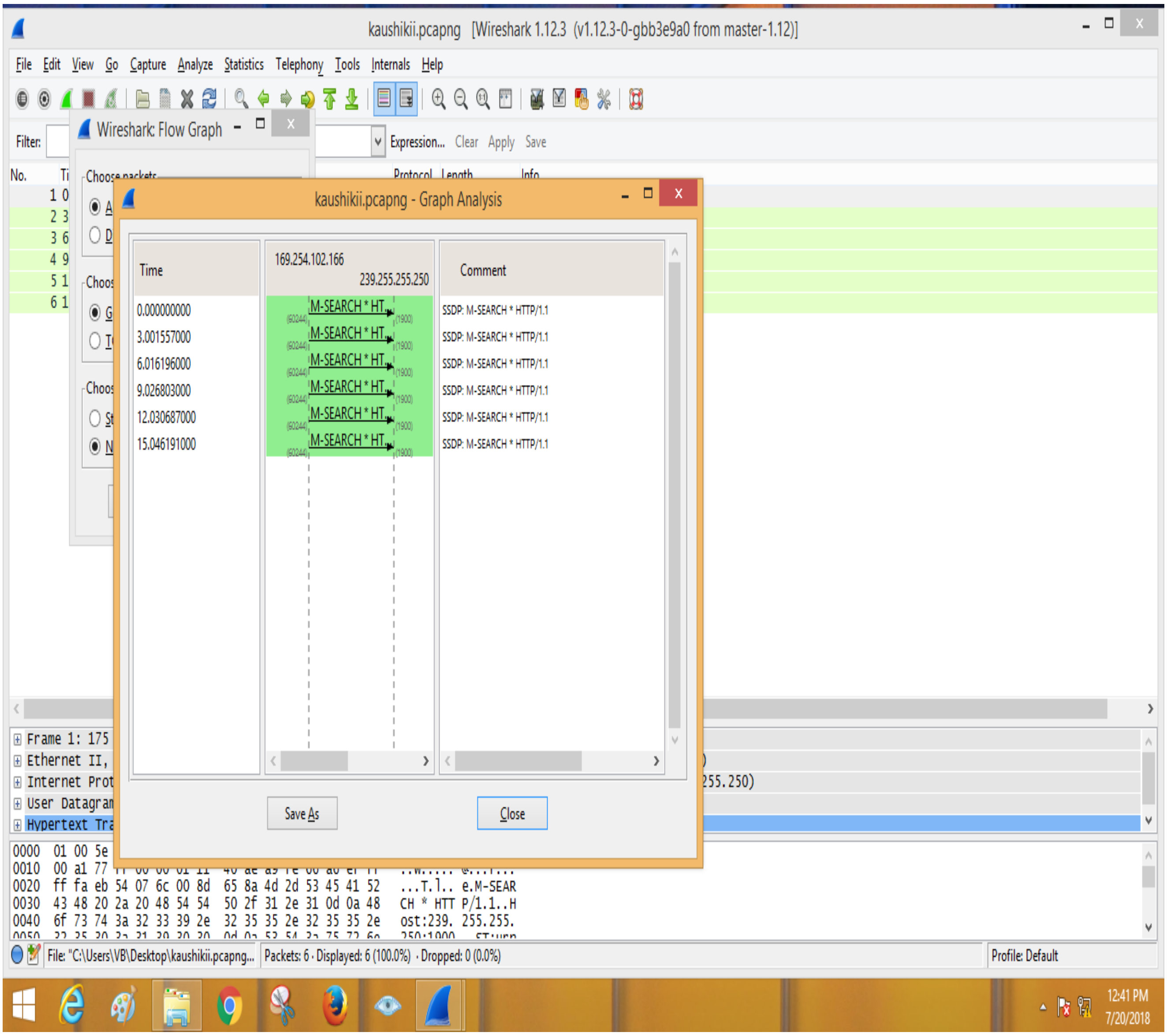
Choose node address type
- ○ Standard source/destination addresses
- ● Network source/destination addresses

```
No.   Ti   255.250  Protocol  Length  Info
    1 0    255.250  SSDP         175 M-SEARCH * HTTP/1.1
    2 3    255.250  SSDP         175 M-SEARCH * HTTP/1.1
    3 6    255.250  SSDP         175 M-SEARCH * HTTP/1.1
    4 9    255.250  SSDP         175 M-SEARCH * HTTP/1.1
    5 1    255.250  SSDP         175 M-SEARCH * HTTP/1.1
    6 1    255.250  SSDP         175 M-SEARCH * HTTP/1.1
```

```
⊞ Frame 1: 175 bytes on wire (1400 bits), 175 bytes captured (1400 bits) on interface 0
⊞ Ethernet II, Src: 02:00:4c:4f:4f:50 (02:00:4c:4f:4f:50), Dst: IPv4mcast_7f:ff:fa (01:00:5e:7f:ff:fa)
⊞ Internet Protocol Version 4, Src: 169.254.102.166 (169.254.102.166), Dst: 239.255.255.250 (239.255.255.250)
⊞ User Datagram Protocol, Src Port: 60244 (60244), Dst Port: 1900 (1900)
⊞ Hypertext Transfer Protocol
```

```
0000  01 00 5e 7f ff fa 02 00  4c 4f 4f 50 08 00 45 00   ..^..... LOOP..E.
0010  00 a1 77 ff 00 00 01 11  40 ae a9 fe 66 a6 ef ff   ..w..... @...f...
0020  ff fa eb 54 07 6c 00 8d  65 8a 4d 2d 53 45 41 52   ...T.l.. e.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  6f 73 74 3a 32 33 39 2e  32 35 35 2e 32 35 35 2e   ost:239. 255.255.
0050  32 35 30 3a 31 39 30 30  0d 0a 53 54 3a 75 72 6e   250:1900 ..ST:urn
```

File: "C:\Users\VB\Desktop\kaushikii.pcapng... Packets: 6 · Displayed: 6 (100.0%) · Dropped: 0 (0.0%) Profile: Default



kaushikii.pcapng [Wireshark 1.12.3 (v1.12.3-0-gbb3e9a0 from master-1.12)]

Wireshark: Flow Graph

kaushikii.pcapng - Graph Analysis

Time	169.254.102.166 → 239.255.255.250	Comment
0.000000000	(60244) M-SEARCH * HT... (1900)	SSDP: M-SEARCH * HTTP/1.1
3.001557000	(60244) M-SEARCH * HT... (1900)	SSDP: M-SEARCH * HTTP/1.1
6.016196000	(60244) M-SEARCH * HT... (1900)	SSDP: M-SEARCH * HTTP/1.1
9.026803000	(60244) M-SEARCH * HT... (1900)	SSDP: M-SEARCH * HTTP/1.1
12.030687000	(60244) M-SEARCH * HT... (1900)	SSDP: M-SEARCH * HTTP/1.1
15.046191000	(60244) M-SEARCH * HT... (1900)	SSDP: M-SEARCH * HTTP/1.1

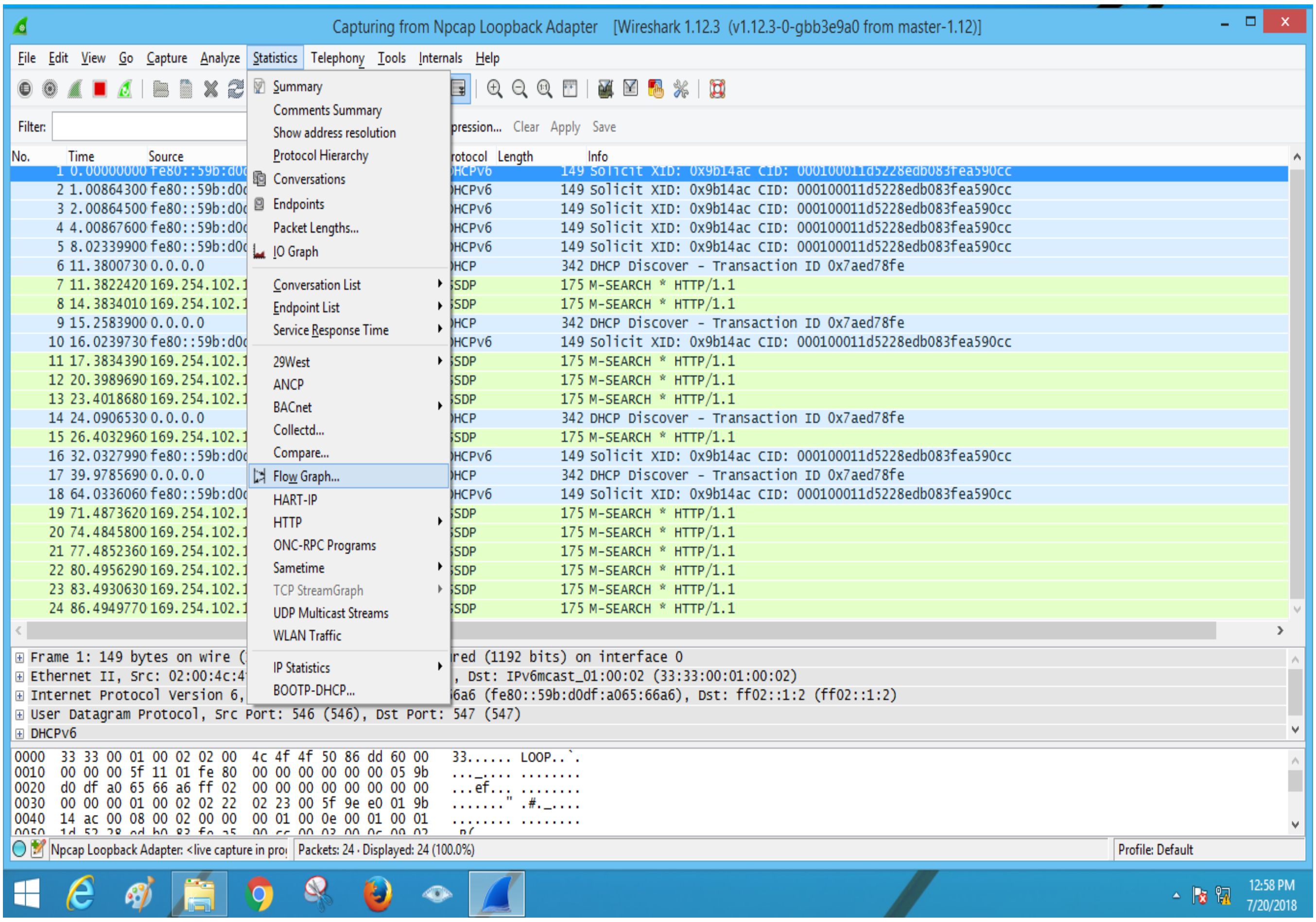
```
⊞ Frame 1: 175
⊞ Ethernet II,
⊞ Internet Prot                                        255.250)
⊞ User Datagram
⊞ Hypertext Tra
```

```
0000  01 00 5e
0010  00 a1 77
0020  ff fa eb 54 07 6c 00 8d  65 8a 4d 2d 53 45 41 52   ...T.l.. e.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  6f 73 74 3a 32 33 39 2e  32 35 35 2e 32 35 35 2e   ost:239. 255.255.
```

File: "C:\Users\VB\Desktop\kaushikii.pcapng... Packets: 6 · Displayed: 6 (100.0%) · Dropped: 0 (0.0%) Profile: Default

File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help
Filter:
Expression... Clear Apply Save
No. Ti Protocol Length Info
Choose packets
Save As
Close
12:41 PM
7/20/2018

3. Packet inspection.



```
No.    Time       Source                            rotocol  Length   Info
  1 0.00000000 fe80::59b:d0c                         HCPv6            149 Solicit XID: 0x9b14ac CID: 000100011d5228edb083fea590cc
  2 1.00864300 fe80::59b:d0c                         HCPv6            149 Solicit XID: 0x9b14ac CID: 000100011d5228edb083fea590cc
  3 2.00864500 fe80::59b:d0c                         HCPv6            149 Solicit XID: 0x9b14ac CID: 000100011d5228edb083fea590cc
  4 4.00867600 fe80::59b:d0c                         HCPv6            149 Solicit XID: 0x9b14ac CID: 000100011d5228edb083fea590cc
  5 8.02339900 fe80::59b:d0c                         HCPv6            149 Solicit XID: 0x9b14ac CID: 000100011d5228edb083fea590cc
  6 11.3800730 0.0.0.0                               HCP              342 DHCP Discover - Transaction ID 0x7aed78fe
  7 11.3822420 169.254.102.1                         SDP              175 M-SEARCH * HTTP/1.1
  8 14.3834010 169.254.102.1                         SDP              175 M-SEARCH * HTTP/1.1
  9 15.2583900 0.0.0.0                               HCP              342 DHCP Discover - Transaction ID 0x7aed78fe
 10 16.0239730 fe80::59b:d0c                         HCPv6            149 Solicit XID: 0x9b14ac CID: 000100011d5228edb083fea590cc
 11 17.3834390 169.254.102.1                         SDP              175 M-SEARCH * HTTP/1.1
 12 20.3989690 169.254.102.1                         SDP              175 M-SEARCH * HTTP/1.1
 13 23.4018680 169.254.102.1                         SDP              175 M-SEARCH * HTTP/1.1
 14 24.0906530 0.0.0.0                               HCP              342 DHCP Discover - Transaction ID 0x7aed78fe
 15 26.4032960 169.254.102.1                         SDP              175 M-SEARCH * HTTP/1.1
 16 32.0327990 fe80::59b:d0c                         HCPv6            149 Solicit XID: 0x9b14ac CID: 000100011d5228edb083fea590cc
 17 39.9785690 0.0.0.0                               HCP              342 DHCP Discover - Transaction ID 0x7aed78fe
 18 64.0336060 fe80::59b:d0c                         HCPv6            149 Solicit XID: 0x9b14ac CID: 000100011d5228edb083fea590cc
 19 71.4873620 169.254.102.1                         SDP              175 M-SEARCH * HTTP/1.1
 20 74.4845800 169.254.102.1                         SDP              175 M-SEARCH * HTTP/1.1
 21 77.4852360 169.254.102.1                         SDP              175 M-SEARCH * HTTP/1.1
 22 80.4956290 169.254.102.1                         SDP              175 M-SEARCH * HTTP/1.1
 23 83.4930630 169.254.102.1                         SDP              175 M-SEARCH * HTTP/1.1
 24 86.4949770 169.254.102.1                         SDP              175 M-SEARCH * HTTP/1.1
```

```
⊞ Frame 1: 149 bytes on wire (                     red (1192 bits) on interface 0
⊞ Ethernet II, Src: 02:00:4c:4                     , Dst: IPv6mcast_01:00:02 (33:33:00:01:00:02)
⊞ Internet Protocol Version 6,                     6a6 (fe80::59b:d0df:a065:66a6), Dst: ff02::1:2 (ff02::1:2)
⊞ User Datagram Protocol, Src Port: 546 (546), Dst Port: 547 (547)
⊞ DHCPv6
```

```
0000  33 33 00 01 00 02 02 00  4c 4f 4f 50 86 dd 60 00   33...... LOOP..`.
0010  00 00 00 5f 11 01 fe 80  00 00 00 00 00 00 05 9b   ..._.... ........
0020  d0 df a0 65 66 a6 ff 02  00 00 00 00 00 00 00 00   ...ef... ........
0030  00 00 00 01 00 02 02 22  02 23 00 5f 9e e0 01 9b   ......." .#._....
0040  14 ac 00 08 00 02 00 00  00 01 00 0e 00 01 00 01   ........ ........
```

Npcap Loopback Adapter: <live capture in pro Packets: 24 · Displayed: 24 (100.0%)