

Experiment No. 1

Aim: Monitoring the network traffic using Wireshark

2. Objectives: To observe the performance in promiscuous & non-promiscuous mode & to find the packets based on different filters.

3. Outcomes: The learner will be able to:-

Identify different packets moving in/out of network using packet sniffer for network analysis.

Understand professional, ethical, legal, security and social issues and responsibilities. Also will be able to analyze the local and global impact of computing on individuals, organizations, and society.

Match the industry requirements in the domains of Database management, Programming and Networking with the required management skills.

4. Hardware / Software Required: Wireshark, Ethereal and tcpdump.

5. 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.

Applications:

Network administrators use it to troubleshoot network problems

Network security engineers use it to examine security problems

Developers use it to debug protocol implementations

People use it to learn network protocol internals beside these examples can be helpful in many other situations too. **Features:**

The following are some of the many features wireshark provides:

Available for UNIX and Windows.

Capture live packet data from a network interface.

Open files containing packet data captured with tcpdump/WinDump, Wireshark, and a number of other packet capture programs.

Import packets from text files containing hex dumps of packet data.

Display packets with very detailed protocol information.

Export some or all packets in a number of capture file formats.

Filter packets on many criteria.

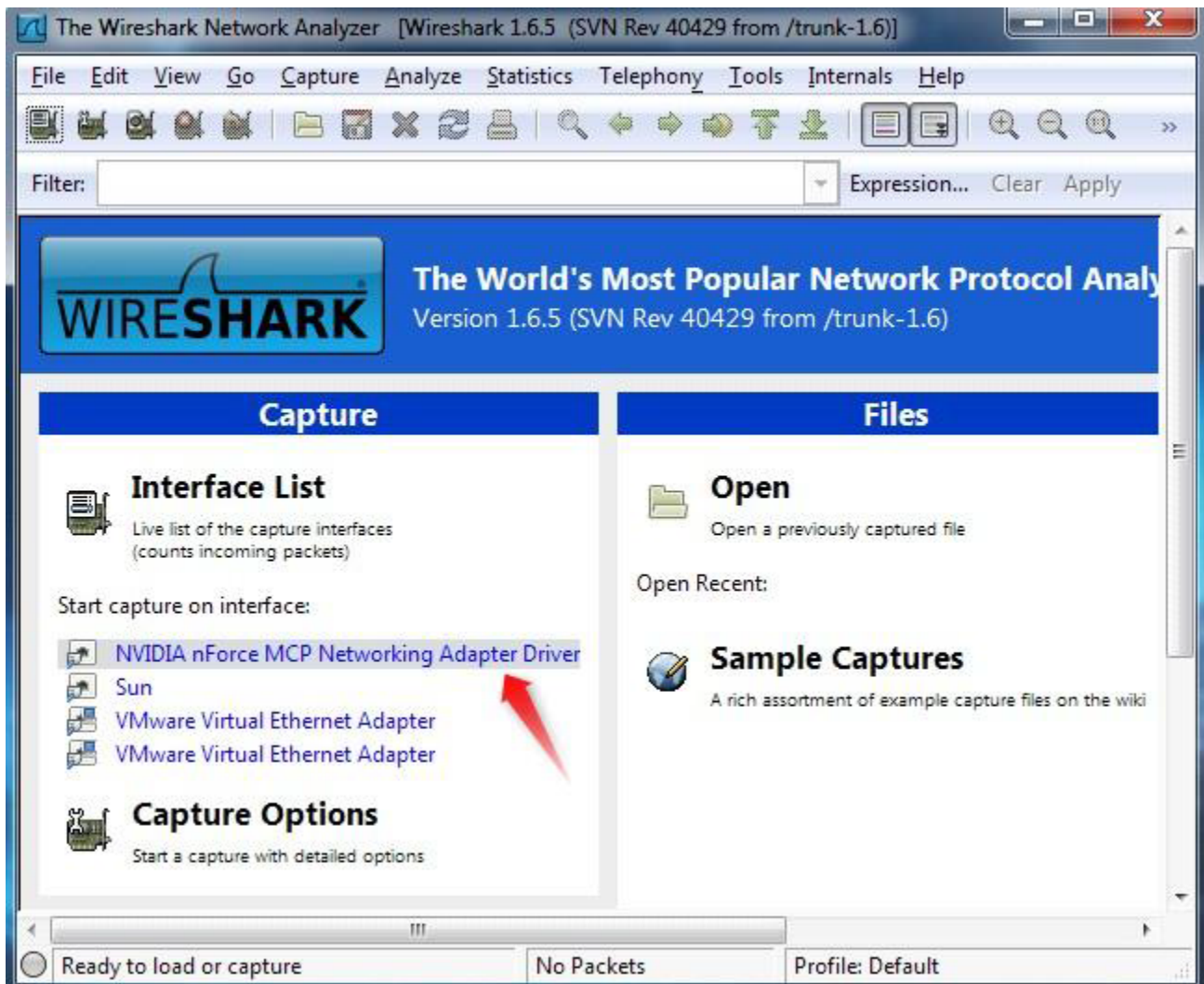
Search for packets on many criteria.

Colorize packet display based on filters.

Create various statistics.

Capturing Packets

After downloading and installing wireshark, you can launch it and click the name of an interface under Interface List to start capturing packets on that interface. For example, if you want to capture traffic on the wireless network, click your wireless interface. You can configure advanced features by clicking Capture Options.



As soon as you click the interface's name, you'll see the packets start to appear in real time. Wireshark captures each packet sent to or from your system. If you're capturing on a wireless interface and have promiscuous mode enabled in your capture options, you'll also see other the other packets on the network

Capturing from NVIDIA nForce MCP Networking Adapter Driver [Wireshark 1.6.5 (SVN Rev ...]

File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help

Filter: Expression... Clear Apply

No.	Time	Source	Destination	Protocol	Length
1038	40.422312	192.168.1.77	173.194.33.1	TCP	54
1039	40.659611	fe80::bdca:e67b:5eb7::1	ff02::c	SSDP	200
1040	41.550320	192.168.1.77	207.8.65.23	HTTP	51
1041	41.580992	207.8.65.23	192.168.1.77	TCP	60
1042	42.051665	192.168.1.76	239.255.255.250	UDP	50
1043	42.104199	Actionte_d8:a3:88	Msi_74:82:e6	ARP	60
1044	42.104226	Msi_74:82:e6	Actionte_d8:a3:88	ARP	42
1045	42.119803	192.168.1.74	239.255.255.250	UDP	56
1046	42.910321	192.168.1.77	74.125.53.125	Jabber/	51
1047	42.929318	74.125.53.125	192.168.1.77	TCP	60
1048	43.659423	fe80::bdca:e67b:5eb7::1	ff02::c	SSDP	200
1049	45.052365	192.168.1.76	239.255.255.250	UDP	50
1050	45.121318	192.168.1.74	239.255.255.250	UDP	56
1051	45.418680	192.168.1.77	72.165.61.176	UDP	120
1052	46.659410	fe80::bdca:e67b:5eb7::1	ff02::c	SSDP	200

Frame 924: 60 bytes on wire (480 bits), 60 bytes captured (480 bits)

Ethernet II, Src: CiscoSpv_4a:df:be (60:2a:d0:4a:df:be), Dst: IPv4mcast_6f:00

Internet Protocol Version 4, Src: 192.168.1.76 (192.168.1.76), Dst: 232.239.0

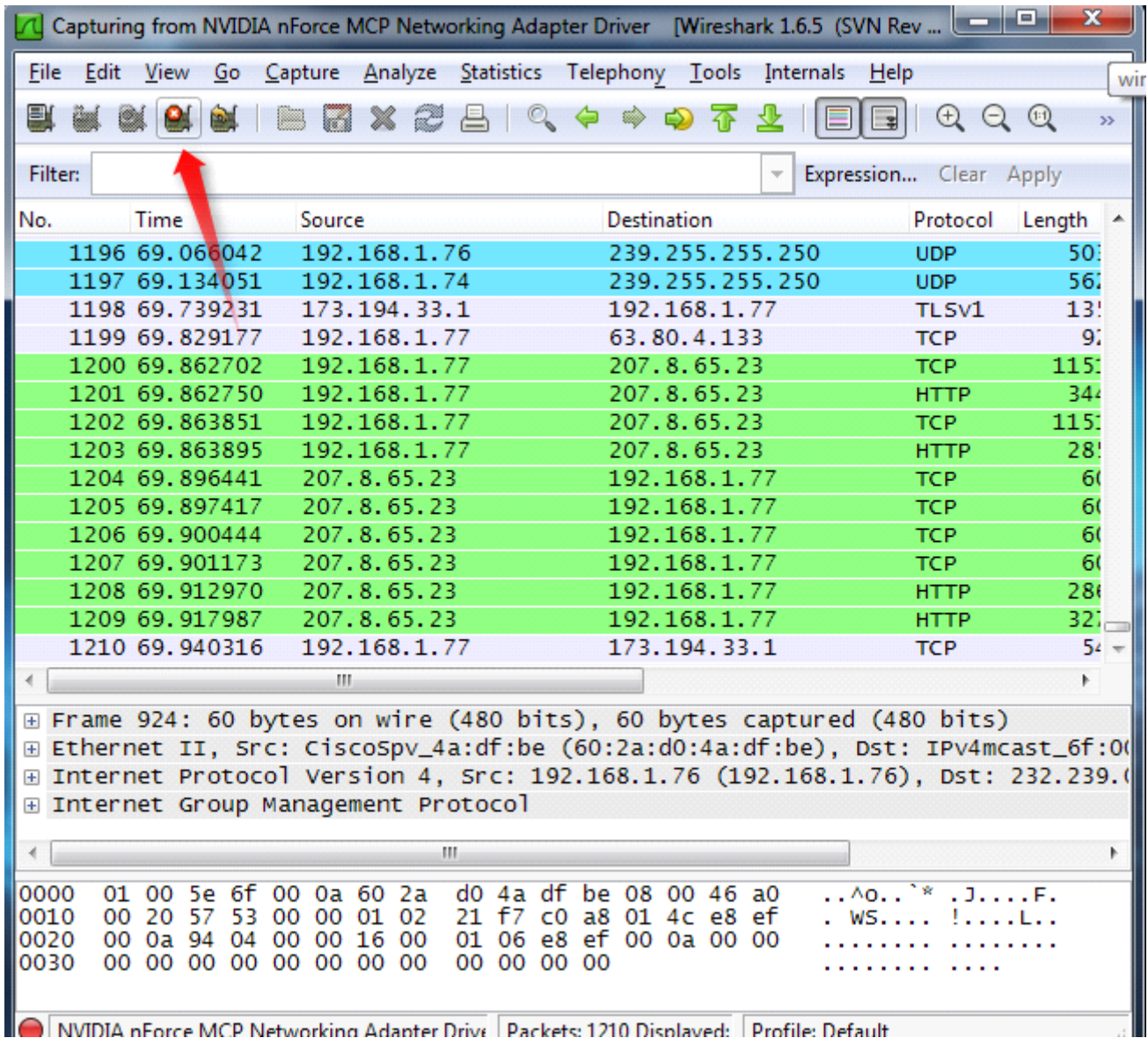
Internet Group Management Protocol

```

0000  01 00 5e 6f 00 0a 60 2a d0 4a df be 08 00 46 a0  ..^O..`* .J....F.
0010  00 20 57 53 00 00 01 02 21 f7 c0 a8 01 4c e8 ef  . WS.... !....L..
0020  00 0a 94 04 00 00 16 00 01 06 e8 ef 00 0a 00 00  .....
0030  00 00 00 00 00 00 00 00 00 00 00 00  .....

```

Click the stop capture button near the top left corner of the window when you want to stop capturing traffic.



Wireshark 1.6.5 (SVN Rev ...)

File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help

Filter: Expression... Clear Apply

No.	Time	Source	Destination	Protocol	Length
1196	69.066042	192.168.1.76	239.255.255.250	UDP	50
1197	69.134051	192.168.1.74	239.255.255.250	UDP	56
1198	69.739231	173.194.33.1	192.168.1.77	TLSv1	13
1199	69.829177	192.168.1.77	63.80.4.133	TCP	9
1200	69.862702	192.168.1.77	207.8.65.23	TCP	115
1201	69.862750	192.168.1.77	207.8.65.23	HTTP	344
1202	69.863851	192.168.1.77	207.8.65.23	TCP	115
1203	69.863895	192.168.1.77	207.8.65.23	HTTP	28
1204	69.896441	207.8.65.23	192.168.1.77	TCP	60
1205	69.897417	207.8.65.23	192.168.1.77	TCP	60
1206	69.900444	207.8.65.23	192.168.1.77	TCP	60
1207	69.901173	207.8.65.23	192.168.1.77	TCP	60
1208	69.912970	207.8.65.23	192.168.1.77	HTTP	28
1209	69.917987	207.8.65.23	192.168.1.77	HTTP	32
1210	69.940316	192.168.1.77	173.194.33.1	TCP	54

Frame 924: 60 bytes on wire (480 bits), 60 bytes captured (480 bits)

Ethernet II, Src: CiscoSpv_4a:df:be (60:2a:d0:4a:df:be), Dst: IPv4mcast_6f:00

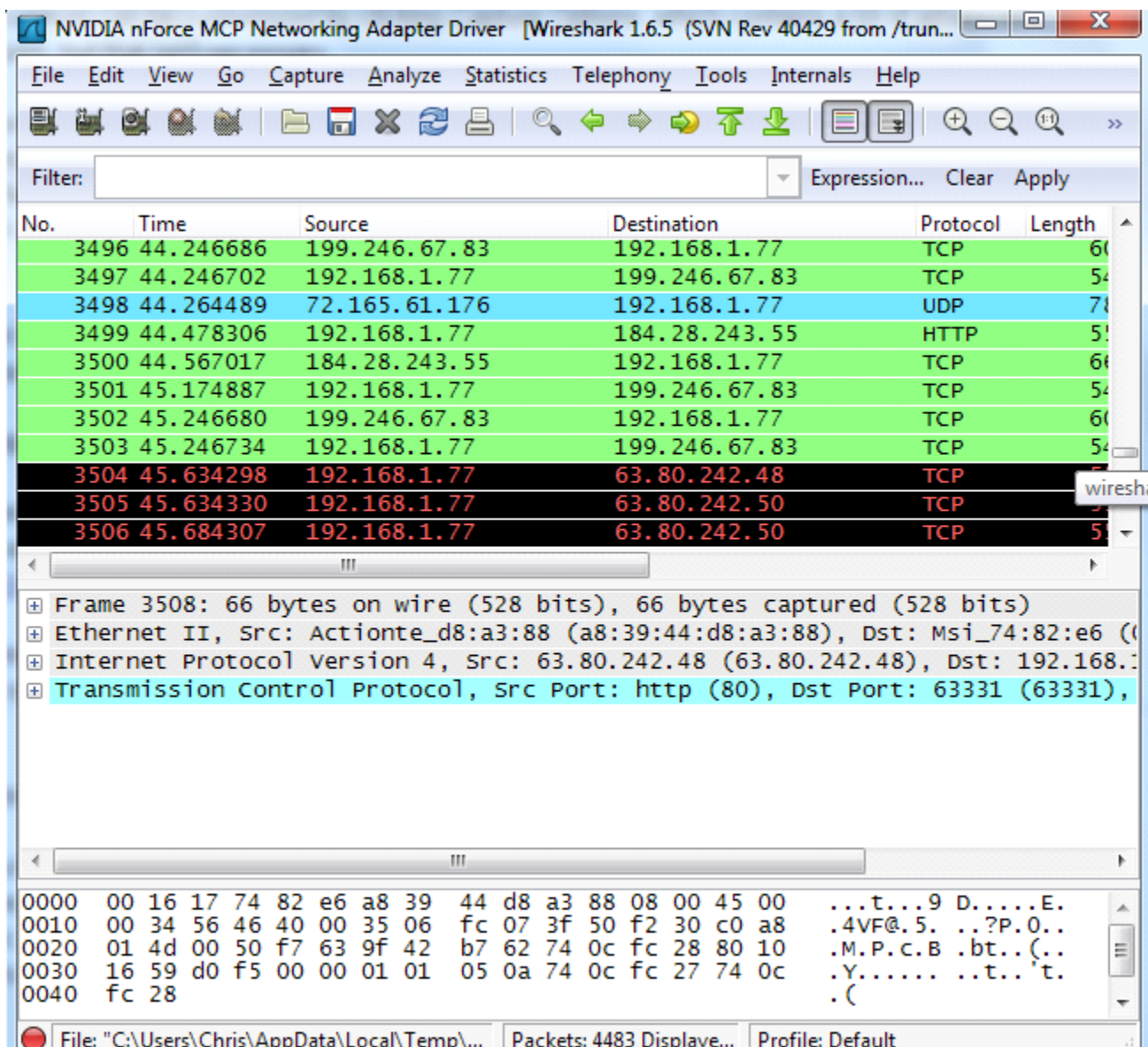
Internet Protocol Version 4, Src: 192.168.1.76 (192.168.1.76), Dst: 232.239.0

Internet Group Management Protocol

0000 01 00 5e 6f 00 0a 60 2a d0 4a df be 08 00 46 a0 ..^O..`* .J....F.
0010 00 20 57 53 00 00 01 02 21 f7 c0 a8 01 4c e8 ef . WS.... !....L..
0020 00 0a 94 04 00 00 16 00 01 06 e8 ef 00 0a 00 00
0030 00 00 00 00 00 00 00 00 00 00 00 00

NVIDIA nForce MCP Networking Adapter Driver Packets: 1210 Displayed: Profile: Default

Wireshark uses colors to help you identify the types of traffic at a glance. By default, green is TCP traffic, dark blue is DNS traffic, light blue is UDP traffic, and black identifies TCP packets with problems – for example, they could have been delivered out-of-order.



Filtering Packets

If you're trying to inspect something specific, such as the traffic a program sends when phoning home, it helps to close down all other applications using the network so you can narrow down the traffic. Still, you'll likely have a large amount of packets to sift through. That's where Wireshark's filters come in.

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 autocomplete your filter.

NVIDIA nForce MCP Networking Adapter Driver [Wireshark 1.6.5 (SVN Rev 40429 from /trun...]

File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help

Filter: dns Expression... Clear Apply

No.	Time	Source	Destination	Protocol	Length
1020	9.161988	192.168.1.77	8.8.8.8	DNS	80
1021	9.164656	192.168.1.77	8.8.8.8	DNS	76
1029	9.181951	8.8.8.8	192.168.1.77	DNS	100
1031	9.191415	8.8.8.8	192.168.1.77	DNS	100
1032	9.204042	192.168.1.77	8.8.8.8	DNS	79
1034	9.224022	8.8.8.8	192.168.1.77	DNS	284
1035	9.239748	192.168.1.77	8.8.8.8	DNS	80
1050	9.260332	8.8.8.8	192.168.1.77	DNS	274
1296	21.095831	192.168.1.77	8.8.8.8	DNS	80
1297	21.115981	8.8.8.8	192.168.1.77	DNS	99
1222	22.244702	192.168.1.75	224.0.0.251	MDNS	204

Frame 1021: 76 bytes on wire (608 bits), 76 bytes captured (608 bits)

Ethernet II, Src: Msi_74:82:e6 (00:16:17:74:82:e6), Dst: Actionte_d8:a3:88 (00:16:17:74:82:e6)

Internet Protocol Version 4, Src: 192.168.1.77 (192.168.1.77), Dst: 8.8.8.8 (8.8.8.8)

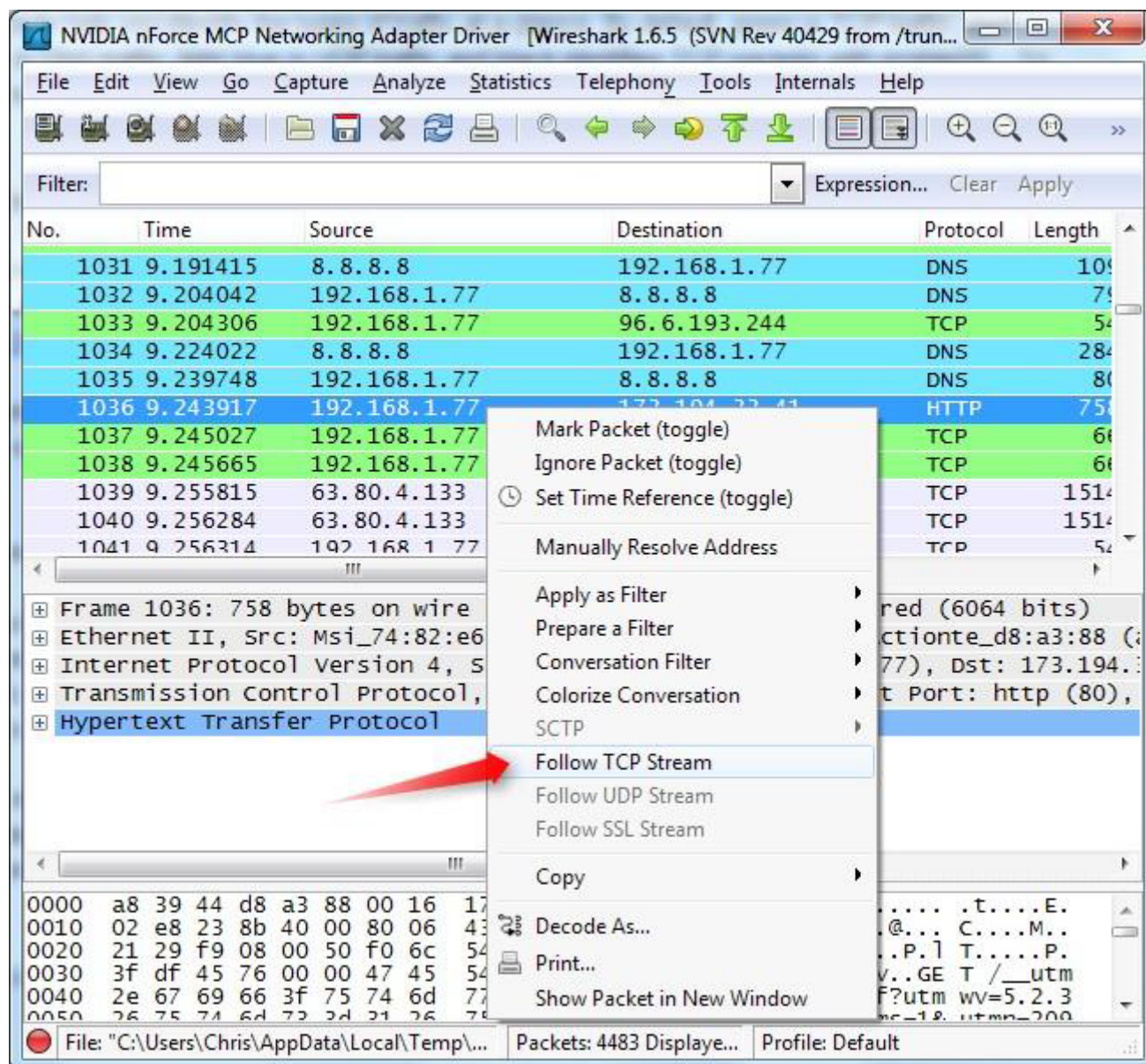
User Datagram Protocol, Src Port: 58168 (58168), Dst Port: domain (53)

Domain Name System (query)

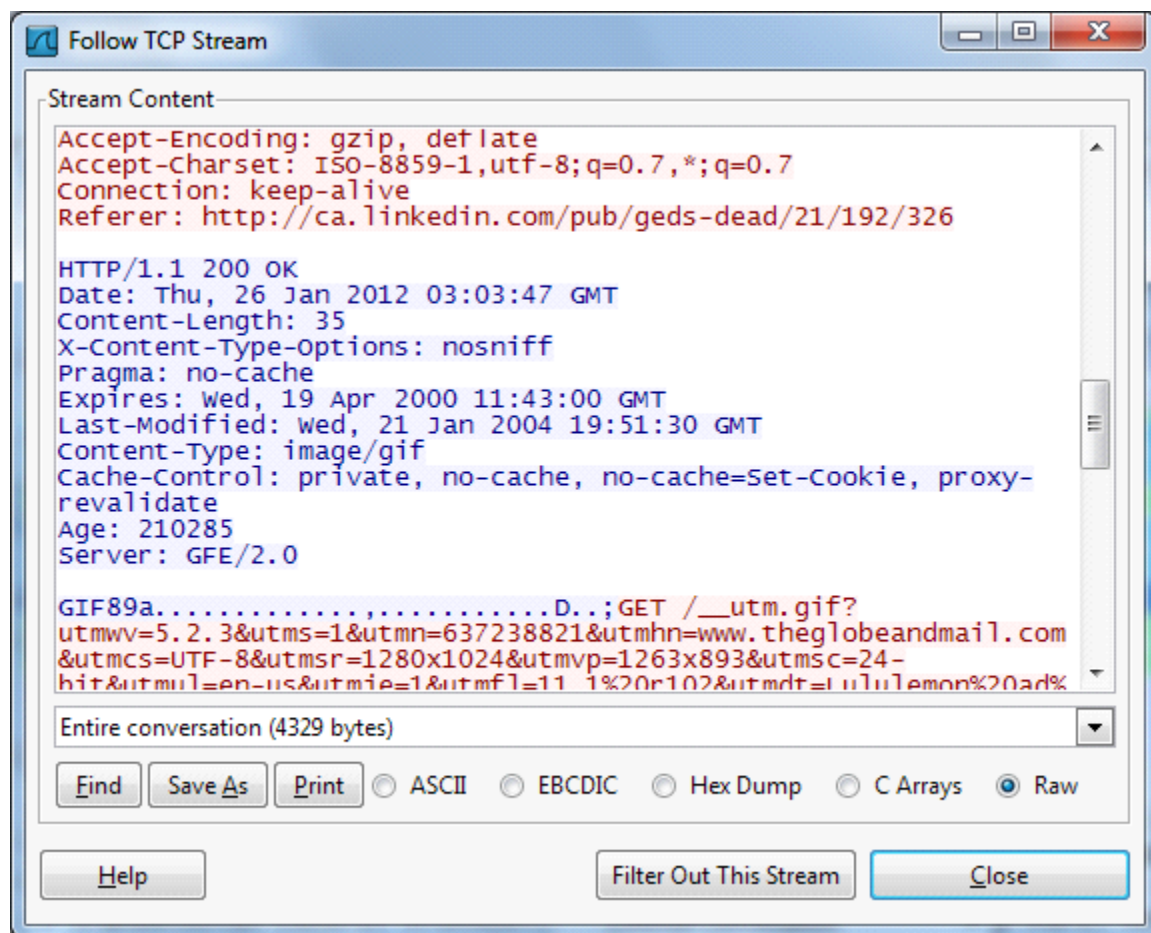
0000 a8 39 44 d8 a3 88 00 16 17 74 82 e6 08 00 45 00 .9D..... .t....E.
 0010 00 3e 23 85 00 00 80 11 45 25 c0 a8 01 4d 08 08 .>#..... E%...M..
 0020 08 08 e3 38 00 35 00 2a 3f f6 0e 23 01 00 00 01 ...8.5.*?...#....
 0030 00 00 00 00 00 00 03 77 77 77 08 6c 69 6e 6b 65w ww.linke
 0040 64 69 6e 03 63 6f 6d 00 00 01 00 01 din.com.

File: "C:\Users\Chris\AppData\Local\Temp\... Packets: 4483 Displave... Profile: Default

Another interesting thing you can do is right-click a packet and select Follow TCP Stream



You'll see the full conversation between the client and the server.



Close the window and you'll find a filter has been applied automatically — Wireshark is showing you the packets that make up the conversation.

NVIDIA nForce MCP Networking Adapter Driver [Wireshark 1.6.5 (SVN Rev 40429 from /trun...]

File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help

Filter: tcp.stream eq 67 Expression... Clear Apply

No.	Time	Source	Destination	Protocol	Length	Info
1036	9.243917	192.168.1.77	173.194.33.41	HTTP	758	G
1046	9.258497	173.194.33.41	192.168.1.77	HTTP	430	H
1048	9.258920	192.168.1.77	173.194.33.41	HTTP	1120	G
1059	9.273910	173.194.33.41	192.168.1.77	HTTP	430	H
1096	9.473301	192.168.1.77	173.194.33.41	TCP	54	6
2307	29.191953	192.168.1.77	173.194.33.41	TCP	1484	[
2308	29.191961	192.168.1.77	173.194.33.41	HTTP	55	G
2309	29.210835	173.194.33.41	192.168.1.77	TCP	60	h
2310	29.211104	173.194.33.41	192.168.1.77	HTTP	430	H
2374	29.411299	192.168.1.77	173.194.33.41	TCP	54	6

Frame 1036: 758 bytes on wire (6064 bits), 758 bytes captured (6064 bits)

Ethernet II, Src: Msi_74:82:e6 (00:16:17:74:82:e6), Dst: Actionte_d8:a3:88 (00:16:17:74:82:e6)

Internet Protocol Version 4, Src: 192.168.1.77 (192.168.1.77), Dst: 173.194.33.41 (173.194.33.41)

Transmission Control Protocol, Src Port: 63752 (63752), Dst Port: http (80), Seq: 300000000, Win: 65535, Len: 0

Hypertext Transfer Protocol

File: "C:\Users\Chris\AppData\Local\Temp\..." Packets: 4483 Displayed Profile: Default

Inspecting Packets
Click a packet to select it and you can dig down to view its details.

NVIDIA nForce MCP Networking Adapter Driver [Wireshark 1.6.5 (SVN Rev 40429 from /trun...]

File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help

Filter: Expression... Clear Apply

No.	Time	Source	Destination	Protocol	Length
2198	27.504985	12.129.210.71	192.168.1.77	TCP	1514
2199	27.505467	12.129.210.71	192.168.1.77	TCP	1514
2200	27.505504	192.168.1.77	12.129.210.71	TCP	54
2201	27.590919	12.129.210.71	192.168.1.77	HTTP	69
2202	27.590986	192.168.1.77	12.129.210.71	TCP	54
2203	27.591228	192.168.1.77	12.129.210.71	TCP	54
2204	27.594178	192.168.1.77	8.8.8.8	DNS	78
2205	27.623129	8.8.8.8	192.168.1.77	DNS	237
2206	27.667342	173.194.33.27	192.168.1.77	TCP	60
2207	27.667406	192.168.1.77	173.194.33.27	TCP	54
2208	27.677887	12.129.210.71	192.168.1.77	TCP	60

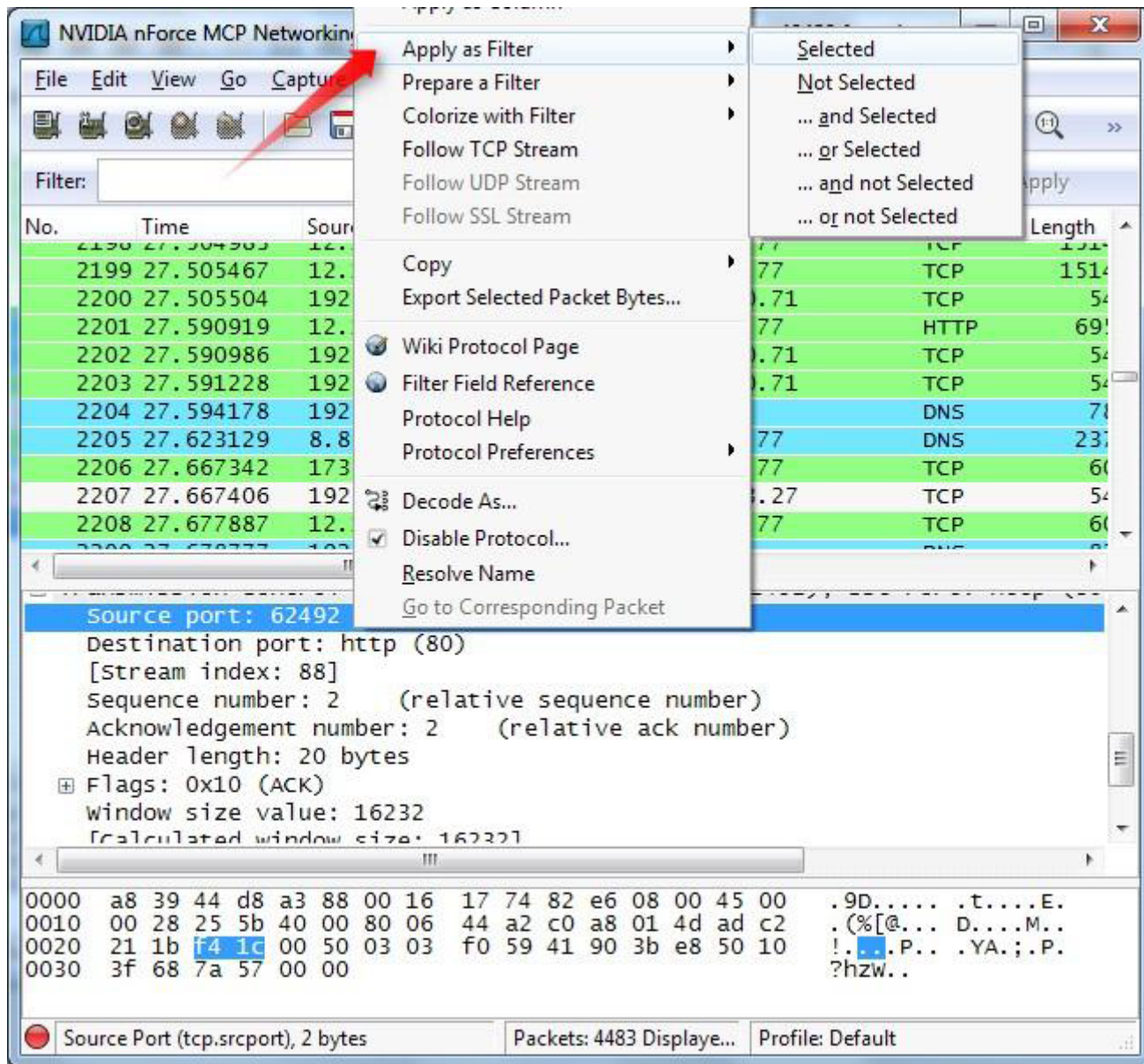
Frame 2207: 54 bytes on wire (432 bits), 54 bytes captured (432 bits)

Arrival Time: Jan 28, 2012 05:28:58.189043000 Pacific Standard Time
Epoch Time: 1327757338.189043000 seconds
[Time delta from previous captured frame: 0.000064000 seconds]
[Time delta from previous displayed frame: 0.000064000 seconds]
[Time since reference or first frame: 27.667406000 seconds]
Frame Number: 2207
Frame Length: 54 bytes (432 bits)
Capture Length: 54 bytes (432 bits)

0000	a8 39 44 d8 a3 88 00 16 17 74 82 e6 08 00 45 00	.9D.....t...E.
0010	00 28 25 5b 40 00 80 06 44 a2 c0 a8 01 4d ad c2	. (%[@... D...M..
0020	21 1b f4 1c 00 50 03 03 f0 59 41 90 3b e8 50 10	!....P.. .YA.;.P.
0030	3f 68 7a 57 00 00	?hzw..

Frame (frame), 54 bytes Packets: 4483 Displaye... Profile: Default

You can also create filters from here — just right-click one of the details and use the Apply as Filter submenu to create a filter based on it.



Wireshark is an extremely powerful tool, and this tutorial is just scratching the surface of what you can do with it. Professionals use it to debug network protocol implementations, examine security problems and inspect network protocol internals.

6. Conclusion:

In this experiment we analyze various packet sniffing tools that monitor network traffic transmitted between legitimate users or in the network. The packet sniffer is network monitoring tool. It is opted for network monitoring, traffic analysis, troubleshooting, Packet grapping, message, protocol analysis, penetration testing and many other purposes.