

CNS: EXPERIMENT - 8

Aim:

Study of packet sniffer tools Wireshark :-

- a. Observer performance in promiscuous as well as non-promiscuous mode.
- b. Show the packets can be traced based on different filters
Port Filters, Address Filters, Protocol Filters, String Filters

Theory:

Wireshark is a network packet analyzer. A network packet analyzer presents captured packet data in as much detail as possible.

You could think of a network packet analyzer as a measuring device for examining what's happening inside a network cable, just like an electrician uses a voltmeter for examining what's happening inside an electric cable (but at a higher level, of course).

In the past, such tools were either very expensive, proprietary, or both. However, with the advent of Wireshark, that has changed. Wireshark is available for free, is open source, and is one of the best packet analyzers available today.

Applications of wireshark:-

- Network administrators use it to troubleshoot network problems
- Network security engineers use it to examine security problems
- QA engineers use it to verify network applications
- Developers use it to debug protocol implementations
- People use it to learn network protocol internals

OUTPUT

Promiscuous Mode:

Screenshot of Wireshark showing network traffic in Promiscuous Mode. The interface is set to "Capturing from Ethernet".

Summary Table:

No.	Time	Source	Destination	Protocol	Length	Info
74298	93.264120	fe80::37c4:1265:a27...	ff02::1:3	LLMNR	95	Standard query 0x21b1 AAAA desktop-13mq5is
74299	93.264120	192.168.45.164	224.0.0.252	LLMNR	75	Standard query 0x21b1 A desktop-13mq5is
74300	93.264120	192.168.45.164	224.0.0.252	LLMNR	75	Standard query 0x21b1 AAAA desktop-13mq5is
74301	93.264195	192.168.45.164	224.0.0.251	MDNS	81	Standard query 0x0000 A desktop-13mq5is.local, "QM" question
74302	93.264835	fe80::37c4:1265:a27...	ff02::fb	MDNS	101	Standard query 0x0000 A desktop-13mq5is.local, "QM" question
74303	93.264851	192.168.41.190	224.0.0.251	MDNS	60	Standard query response 0x0000
74304	93.265414	fe80::941c:c745:76b...	ff02::fb	MDNS	74	Standard query response 0x0000
74305	93.265660	192.168.45.164	224.0.0.251	MDNS	81	Standard query 0x0000 AAAA desktop-13mq5is.local, "QU" question
74306	93.265897	192.168.45.164	224.0.0.251	MDNS	81	Standard query 0x0000 A desktop-13mq5is.local, "QM" question
74307	93.266314	fe80::37c4:1265:a27...	ff02::fb	MDNS	101	Standard query 0x0000 A desktop-13mq5is.local, "QM" question
74308	93.266591	192.168.41.190	224.0.0.251	MDNS	60	Standard query response 0x0000
74309	93.266591	192.168.41.190	224.0.0.251	MDNS	60	Standard query response 0x0000
74310	93.266775	192.168.45.164	224.0.0.251	MDNS	81	Standard query 0x0000 AAAA desktop-13mq5is.local, "QU" question
74311	93.266810	fe80::941c:c745:76b...	ff02::fb	MDNS	74	Standard query response 0x0000
74312	93.267218	fe80::37c4:1265:a27...	ff02::fb	MDNS	101	Standard query 0x0000 AAAA desktop-13mq5is.local, "QU" question
74313	93.267494	192.168.41.190	224.0.0.251	MDNS	60	Standard query response 0x0000
74314	93.267670	fe80::37c4:1265:a27...	ff02::fb	MDNS	101	Standard query 0x0000 AAAA desktop-13mq5is.local, "QU" question
74315	93.267942	fe80::941c:c745:76b...	ff02::fb	MDNS	74	Standard query response 0x0000
74316	93.268220	fe80::941c:c745:76b...	ff02::fb	MDNS	74	Standard query response 0x0000
74317	93.293744	HonHaiPr_86:49:81	Broadcast	ARP	60	Who has 192.168.32.20? Tell 192.168.33.77

Selected Frame (Frame 1):

```
> Frame 1: 93 bytes on wire (744 bits), 93 bytes captured (744 bits) on interface \Device\NPF_{...}
> Ethernet II, Src: HonHaiPr_86:20:d7 (f4:6b:8c:8d:20:d7), Dst: IPv4mcast_fb (01:00:00:00:00:00)
> Internet Protocol Version 4, Src: 10.3.3.1, Dst: 224.0.0.251
> User Datagram Protocol, Src Port: 5353, Dst Port: 5353
> Multicast Domain Name System (query)
```

Hex Dump:

```
0000  01 00 5e 00 00 fb f4 6b 8c 8d 20 d7 08 00 45 00 ..^....k ...-E-
0010  00 4f 46 07 00 00 01 11 85 98 0a 03 01 e0 00 .OF.....
0020  00 fb 14 e9 14 e9 00 3b ff e9 00 00 00 00 00 01 .....; .....
0030  00 00 00 00 00 00 ff 44 45 53 4b 54 4f 50 2d 51 .....D E5KTOP-Q
0040  53 37 47 47 56 45 06 5f 64 6f 73 76 63 04 5f 74 S7GGVE_-dosvc_-t
0050  63 70 05 6c ff 63 61 6c 00 00 ff 00 01 cp-local .....
```

Ethernet: <live capture in progress> | Packets: 74317 - Displayed: 74317 (100.0%) | Profile: Default

Non Promiscuous Mode:

Screenshot of Wireshark showing network traffic in Non Promiscuous Mode. The interface is set to "Capturing from Ethernet".

Summary Table:

No.	Time	Source	Destination	Protocol	Length	Info
1622	7.842564	192.168.41.190	224.0.0.251	MDNS	60	Standard query response 0x0000
1623	7.843254	192.168.45.164	224.0.0.251	MDNS	81	Standard query 0x0000 A desktop-13mq5is.local, "QM" question
1624	7.843974	192.168.41.190	224.0.0.251	MDNS	60	Standard query response 0x0000
1625	7.851087	HonHaiPr_8d:20:83	Broadcast	ARP	60	Who has 192.168.32.20? Tell 192.168.47.5
1626	7.851280	192.168.42.71	224.0.0.252	LLMNR	69	Standard query 0x606d AAAA extc410-1
1627	7.851280	192.168.42.71	224.0.0.252	LLMNR	69	Standard query 0xeax30 A extc410-1
1628	7.853902	192.168.45.208	224.0.0.251	MDNS	429	Standard query response 0x0000 PTR DESKTOP-8DHG11A._dosvc._tcp.local SRV 0 0 7680 DESKTO...
1629	7.854307	192.168.45.208	224.0.0.251	MDNS	365	Standard query response 0x0000 SRV 0 0 7680 DESKTOP-8DHG11A.local TXT A 192.168.45.208 ...
1630	7.862083	192.168.32.193	224.0.0.251	MDNS	298	Standard query response 0x0000 PTR DESKTOP-DNDJS02._dosvc._tcp.local SRV 0 0 7680 DESKTO...
1631	7.862651	192.168.32.193	224.0.0.251	MDNS	93	Standard query 0x0000 ANY DESKTOP-DNDJS02._dosvc._tcp.local, "QM" question
1632	7.863501	192.168.41.190	224.0.0.251	MDNS	60	Standard query response 0x0000
1633	7.868593	HonHaiPr_86:45:64	Broadcast	ARP	60	Who has 192.168.37.218? Tell 192.168.44.72
1634	7.872433	HonHaiPr_86:4d:06	Broadcast	ARP	60	Who has 192.168.37.143? Tell 192.168.46.119
1635	7.882212	HonHaiPr_8b:3a:ab	Broadcast	ARP	60	Who has 192.168.32.170? Tell 192.168.42.71
1636	7.882312	HonHaiPr_8b:3a:ab	Broadcast	ARP	60	Who has 192.168.33.107? Tell 192.168.42.71
1637	7.883058	HonHaiPr_8b:3a:ab	Broadcast	ARP	60	Who has 192.168.46.244? Tell 192.168.42.71
1638	7.896158	Dell_22:8:e0	Broadcast	ARP	60	Who has 192.168.32.20? Tell 192.168.47.169
1639	7.899630	Sophos_fc:00:05	Broadcast	ARP	60	Who has 192.168.32.71? Tell 192.168.32.1
1640	7.904592	HonHaiPr_86:4d:08	Broadcast	ARP	60	Who has 192.168.32.20? Tell 192.168.33.136
1641	7.935144	HonHaiPr_86:49:50	Broadcast	ARP	60	Who has 192.168.38.93? Tell 192.168.46.218
1642	7.943504	HonHaiPr_86:4d:09	Broadcast	ARP	60	Who has 192.168.32.20? Tell 192.168.44.102

Selected Frame (Frame 1):

```
> Frame 1: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface \Device\NPF_{...}
> Ethernet II, Src: HonHaiPr_86:45:2d (f4:6b:8c:8d:45:2d), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
> Address Resolution Protocol (request)
```

Hex Dump:

```
0000  ff ff ff ff ff ff 44 6b 8c 8d 20 08 00 00 01 .....k .E...
0010  00 08 06 04 00 01 4f 6b 8c 8d c0 a8 2c aa .....k ..E...
0020  00 00 00 00 00 00 c0 a8 20 14 00 00 00 00 00 ..... .
0030  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
```

Ethernet: <live capture in progress> | Packets: 1737 - Displayed: 1737 (100.0%) | Profile: Default

Port Filters:

tcp.port ≥ 1024 & tcp.port ≤ 65535

This Wireshark capture shows a list of TCP packets. The table includes columns for No., Time, Source, Destination, Protocol, Length, and Info. The Info column provides detailed packet analysis, such as sequence numbers, ACKs, and window sizes. A large portion of the captured data is highlighted in light purple, indicating the scope of the port filter applied.

No.	Time	Source	Destination	Protocol	Length	Info
2479	8.068214	192.168.36.7	142.251.222.78	TCP	55	50875 → 443 [ACK] Seq=1 Ack=1 Win=8211 Len=1 [TCP segment of a reassembled PDU]
2480	8.069204	142.251.222.78	192.168.36.7	TCP	66	443 → 50875 [ACK] Seq=1 Ack=2 Win=320 Len=0 SLE=1 SRE=2
2540	8.336472	192.168.36.7	172.64.155.209	TLSv1.2	318	Ignored Unknown Record
2541	8.336507	192.168.36.7	172.64.155.209	TLSv1.2	93	Application Data
2542	8.336564	192.168.36.7	172.64.155.209	TLSv1.2	316	Application Data
2543	8.336763	172.64.155.209	192.168.36.7	TCP	60	443 → 50929 [ACK] Seq=1 Ack=266 Win=1502 Len=0
2544	8.336763	172.64.155.209	192.168.36.7	TCP	60	443 → 50929 [ACK] Seq=1 Ack=305 Win=1502 Len=0
2545	8.337062	172.64.155.209	192.168.36.7	TCP	60	443 → 50929 [ACK] Seq=1 Ack=567 Win=1502 Len=0
2546	8.339062	172.64.155.209	192.168.36.7	TLSv1.2	93	Application Data
2560	8.380713	192.168.36.7	172.64.155.209	TCP	54	50929 → 443 [ACK] Seq=567 Ack=40 Win=8206 Len=0
2608	8.629484	172.64.155.209	192.168.36.7	TLSv1.2	432	Application Data, Application Data, Application Data
2609	8.631470	192.168.36.7	172.64.155.209	TLSv1.2	89	Application Data
2651	8.858420	172.64.155.209	192.168.36.7	TCP	432	[TCP Spurious Retransmission] 443 → 50929 [PSH, ACK] Seq=40 Ack=567 Win=1502 Len=378
2652	8.858485	192.168.36.7	172.64.155.209	TCP	66	[TCP Dup ACK 2609#1] 50929 → 443 [ACK] Seq=602 Ack=418 Win=8212 Len=0 SLE=40 SRE=418
2679	8.943069	192.168.36.7	172.64.155.209	TCP	89	[TCP Retransmission] 50929 → 443 [PSH, ACK] Seq=567 Ack=418 Win=8212 Len=35
2682	8.976964	204.79.197.222	192.168.36.7	TCP	60	443 → 50924 [FIN, ACK] Seq=1 Ack=1 Win=280 Len=0
2683	8.977053	192.168.36.7	204.79.197.222	TCP	54	50924 → 443 [ACK] Seq=1 Ack=2 Win=1823 Len=0
2685	8.990528	172.64.155.209	192.168.36.7	TCP	60	443 → 50929 [ACK] Seq=418 Ack=602 Win=1502 Len=0
2738	9.255157	192.168.36.7	142.251.222.78	TCP	55	50860 → 443 [ACK] Seq=1 Ack=1 Win=8212 Len=1 [TCP segment of a reassembled PDU]
2739	9.255610	142.251.222.78	192.168.36.7	TCP	66	443 → 50860 [ACK] Seq=1 Ack=2 Win=670 Len=0 SLE=1 SRE=2

Frame 91: 164 bytes on wire (1312 bits), 164 bytes captured (1312 bits) on interface **Ethernet II, Src: Dell_a9:99:88 (e4:54:e8:a9:99:88)**, Dst: 58:41:46:94:c7:3d (58:41:46:94:c7:3d) [ethernet header], [IP header], [TCP header].
Internet Protocol Version 4, Src: 192.168.36.7, Dst: 192.168.47.220
Transmission Control Protocol, Src Port: 50755, Dst Port: 8009, Seq: 1, Ack: 1, Len: 164
TCP Segment of a reassembled PDU (Seq=1 Ack=1 Win=280 Len=0).
Data bytes (hex): 0000 58 41 46 94 c7 3d e4 54 e8 a9 99 88 00 45 00 XAF--T-----E-
0010 00 96 e9 f2 40 00 86 00 00 c0 a8 24 07 c0 a8 ...@...\$...
0020 2f dc d6 43 1f 49 25 6b 51 47 51 b6 a5 20 50 18 /..C-I%k QGQ-P.
0030 04 01 d5 bc 00 00 17 03 03 00 69 f7 ff d4 6b 5a-i--kZ
0040 71 53 c3 fc 93 ba 64 8a 45 bd f9 78 28 da 94 e6 qS---d-E-(...
0050 05 9e f1 6d 43 59 5d 6b 05 c1 3f 89 d0 07 23 1f ..mCY]k ..?..#.
0060 7c 4a 58 37 fe 1d 6d 4f 76 a1 c6 a6 25 9a e3 74]JX7--m0 v-%..t
0070 fb 14 33 4e 1d 1e 4e e5 4a 5e eb fa d7 78 a8 1e ..3N-N- J^--x..
Data bytes (text):
Packets: 2765 - Displayed: 42 (1.5%) | Profile: Default

Address Filter:

ip.addr = 142.251.42.68

This Wireshark capture shows a list of IP packets from the source IP 142.251.42.68. The table includes columns for No., Time, Source, Destination, Protocol, Length, and Info. The Info column provides detailed packet analysis, including sequence numbers and TTL values. A large portion of the captured data is highlighted in light purple, indicating the scope of the address filter applied.

No.	Time	Source	Destination	Protocol	Length	Info
1655	154.011522	142.251.42.68	192.168.37.241	TCP	60	443 → 49988 [ACK] Seq=10195 Ack=8093 Win=44800 Len=0
1657	154.138203	142.251.42.68	192.168.37.241	TLSv1.3	1514	Application Data
1657	154.138203	142.251.42.68	192.168.37.241	TLSv1.3	749	Application Data
1657	154.138203	142.251.42.68	192.168.37.241	TLSv1.3	158	Application Data, Application Data
1657	154.138203	142.251.42.68	192.168.37.241	TLSv1.3	93	Application Data
1657	154.185832	142.251.42.68	192.168.37.241	TCP	60	443 → 49988 [ACK] Seq=12493 Ack=8132 Win=44800 Len=0
1966	175.229105	192.168.36.7	142.251.42.68	ICMP	74	Echo (ping) request id=0x0001, seq=1/256, ttl=128 (reply in 196640)
1966	175.229105	142.251.42.68	192.168.36.7	ICMP	74	Echo (ping) reply id=0x0001, seq=1/256, ttl=119 (request in 196621)
2019	176.240043	192.168.36.7	142.251.42.68	ICMP	74	Echo (ping) request id=0x0001, seq=2/512, ttl=128 (reply in 201967)
2019	176.249571	142.251.42.68	192.168.36.7	ICMP	74	Echo (ping) reply id=0x0001, seq=2/512, ttl=119 (request in 201944)
2051	177.256231	192.168.36.7	142.251.42.68	ICMP	74	Echo (ping) request id=0x0001, seq=3/768, ttl=128 (reply in 205119)
2051	177.259796	142.251.42.68	192.168.36.7	ICMP	74	Echo (ping) reply id=0x0001, seq=3/768, ttl=119 (request in 205112)
2089	179.649988	142.251.42.68	192.168.36.7	ICMP	74	Echo (ping) request id=0x0001, seq=4/1024, ttl=128 (reply in 208916)
2089	179.649977	192.168.36.7	142.251.42.68	ICMP	74	Echo (ping) request id=0x0001, seq=4/1024, ttl=119 (request in 208912)
2260	194.907576	142.251.42.68	192.168.37.241	TCP	66	[TCP Dup ACK 161364#1] 443 → 49951 [ACK] Seq=352248 Ack=110486 Win=224256 Len=0 SLE=110..
2273	197.587584	142.251.42.68	192.168.37.241	TCP	66	[TCP Dup ACK 164147#1] 443 → 49971 [ACK] Seq=7021 Ack=2303 Win=35712 Len=0 SLE=2302 SRE=2302
2287	199.186652	142.251.42.68	192.168.37.241	TCP	66	[TCP Dup ACK 165722#1] 443 → 49988 [ACK] Seq=12493 Ack=8132 Win=44800 Len=0 SLE=8131 SR=8131
2384	210.721672	142.251.42.68	192.168.37.241	TCP	60	443 → 49971 [FIN, ACK] Seq=7021 Ack=2304 Win=35712 Len=0
2384	210.722499	142.251.42.68	192.168.37.241	TCP	60	443 → 49951 [FIN, ACK] Seq=352248 Ack=110487 Win=224256 Len=0
2384	210.723221	142.251.42.68	192.168.37.241	TCP	60	443 → 49988 [FIN, ACK] Seq=12493 Ack=8133 Win=44800 Len=0

Frame 17434: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface **Ethernet II, Src: Sophos_fc:00:05 (c8:4f:86:fc:00:05)**, Dst: Dell_ad:1b:fd (8c:ec:4f)

Internet Protocol Version 4, Src: 142.251.42.68, Dst: 192.168.37.241
Transmission Control Protocol, Src Port: 443, Dst Port: 49737, Seq: 1, Ack: 1, Len: 66

Data bytes (hex): 0000 8c ec 4b ad 1b fd c8 4f 86 fc 00 05 08 00 45 00 ..K---0-----E-
0010 00 34 3f 4b 40 00 40 06 5a f0 8e fb 2a 44 c0 a8 .4?@. Z-*D..
0020 25 f1 01 bb c2 49 bc 92 f4 d2 71 8f 7e 93 80 10 %---I--q~...
0030 01 18 92 fa 00 00 01 01 05 0a 71 8f 7e 92 71 8f-q~.q~.
0040 7e 93 ..

Packets: 269223 - Displayed: 424 (0.2%) | Profile: Default

Protocol Filters:

udp

The screenshot shows a Wireshark capture of a single UDP frame. The packet details pane shows the following information:

No.	Time	Source	Destination	Protocol	Length	Info
4205..	364.272211	fe80::941c:c745:76b.. ff02::fb		MDNS	74	Standard query response 0x0000
4205..	364.272623	192.168.41.190	224.0.0.251	MDNS	60	Standard query response 0x0000
4205..	364.272623	fe80::941c:c745:76b.. ff02::fb		MDNS	74	Standard query response 0x0000
4205..	364.272807	192.168.41.213	224.0.0.251	MDNS	60	Standard query response 0x0000
4205..	364.272807	fe80::a0ba:bdd6:f36.. ff02::fb		MDNS	74	Standard query response 0x0000
4205..	364.301097	192.168.46.179	192.168.47.255	BROWSER	243	Host Announcement AIDS211-7, Workstation, Server, SQL Server, NT Workstation
4205..	364.302916	192.168.34.145	224.0.0.251	MDNS	81	Standard query 0x0000 A desktop-d3eggf6.local, "QM" question
4205..	364.303068	192.168.46.151	224.0.0.251	MDNS	60	Standard query response 0x0000
4205..	364.303068	192.168.41.213	224.0.0.251	MDNS	60	Standard query response 0x0000
4205..	364.303564	fe80::d3ef:a563:fec.. ff02::fb		MDNS	101	Standard query 0x0000 A desktop-d3eggf6.local, "QM" question
4205..	364.303564	192.168.41.190	224.0.0.251	MDNS	60	Standard query response 0x0000
4205..	364.303855	fe80::941c:c745:76b.. ff02::fb		MDNS	74	Standard query response 0x0000
4205..	364.303864	fe80::a0ba:bdd6:f36.. ff02::fb		MDNS	74	Standard query response 0x0000
4205..	364.304190	192.168.34.145	224.0.0.251	MDNS	81	Standard query 0x0000 AAAA desktop-d3eggf6.local, "QM" question
4205..	364.304247	192.168.46.151	224.0.0.251	MDNS	60	Standard query response 0x0000
4205..	364.304531	192.168.41.190	224.0.0.251	MDNS	60	Standard query response 0x0000
4205..	364.304552	fe80::d3ef:a563:fec.. ff02::fb		MDNS	101	Standard query 0x0000 AAAA desktop-d3eggf6.local, "QM" question
4205..	364.304873	192.168.41.213	224.0.0.251	MDNS	60	Standard query response 0x0000
4205..	364.304991	fe80::941c:c745:76b.. ff02::fb		MDNS	74	Standard query response 0x0000
4205..	364.306028	fe80::a0ba:bdd6:f36.. ff02::fb		MDNS	74	Standard query response 0x0000

The bytes pane shows the captured frame content:

```

> Frame 17408: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface
> Ethernet II, Src: Dell_a9:98:af (e4:54:e8:a9:98:af), Dst: IPv6mcast_fb (33:33:00:0
> Internet Protocol Version 6, Src: fe80::6585:946d:ab35:54a4, Dst: ff02::fb
> User Datagram Protocol, Src Port: 5353, Dst Port: 5353
> Multicast Domain Name System (response)

```

```

0000  33 33 00 00 00 fb e4 54 e8 a9 98 af 86 dd 60 00 33....T ....`.
0010  00 00 00 14 11 01 fe 80 00 00 00 00 00 65 85 .....e....
0020  94 6d ab 35 54 a4 ff 02 00 00 00 00 00 00 00 ..m-5T.....
0030  00 00 00 00 00 fb 14 e9 14 e9 00 14 59 a8 00 .....Y....
0040  84 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....`...

```

String Filter:

tcp contains "HTTP"

The screenshot shows a Wireshark interface with the following details:

- File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help**
- tcp contains "HTTP"** is selected in the search bar.
- No. Time Source Destination Protocol Length Info** are the columns in the packet list.
- 13953 19.056568 202.94.162.202 192.168.37.241 TCP 1514 80 → 49874 [ACK] Seq=1 Ack=1 Win=254 Len=1460 [TCP segment of a reassembled PDU]** is the first visible packet.
- 18009 11.320875 202.94.162.202 192.168.37.241 TCP 1514 80 → 49874 [ACK] Seq=6016 Ack=2074 Win=287 Len=1460 [TCP segment of a reassembled PDU]** is the second visible packet.
- 202.94.162.202 192.168.37.241 TCP 1514 80 → 49874 [ACK] Seq=108850 Ack=2594 Win=296 Len=1460 [TCP segment of a reassembled PDU]** is the third visible packet.
- 21343 13.573140 202.94.162.202 192.168.37.241 TCP 1514 80 → 49874 [ACK] Seq=191324 Ack=3114 Win=304 Len=1460 [TCP segment of a reassembled PDU]** is the fourth visible packet.
- 21977 6.639590 202.94.162.202 192.168.37.241 TCP 1514 80 → 49874 [ACK] Seq=336862 Ack=3634 Win=312 Len=1460 [TCP segment of a reassembled PDU]** is the fifth visible packet.
- 22721 15.819029 202.94.162.202 192.168.37.241 TCP 1514 80 → 49874 [ACK] Seq=682947 Ack=4155 Win=321 Len=1460 [TCP segment of a reassembled PDU]** is the sixth visible packet.
- 23932 16.931075 202.94.162.202 192.168.37.241 TCP 1514 80 → 49874 [ACK] Seq=1443491 Ack=4677 Win=329 Len=1460 [TCP segment of a reassembled PDU]** is the seventh visible packet.
- 26285 18.055327 202.94.162.202 192.168.37.241 TCP 1514 80 → 49874 [ACK] Seq=2948407 Ack=5199 Win=337 Len=1460 [TCP segment of a reassembled PDU]** is the eighth visible packet.
- 27837 19.182113 202.94.162.202 192.168.37.241 TCP 1514 80 → 49874 [ACK] Seq=5895636 Ack=5722 Win=336 Len=1460 [TCP segment of a reassembled PDU]** is the ninth visible packet.
- 30092 20.313126 202.94.162.202 192.168.37.241 TCP 1514 80 → 49874 [ACK] Seq=11776420 Ack=6246 Win=354 Len=1460 [TCP segment of a reassembled PDU]** is the tenth visible packet.
- 31391 20.933166 34.104.35.123 192.168.37.241 TCP 743 80 → 49785 [PSH, ACK] Seq=1 Ack=1 Win=329 Len=689 [TCP segment of a reassembled PDU]** is the eleventh visible packet.
- 31608 21.347981 199.232.46.172 192.168.37.241 HTTP 486 HTTP/1.1 304 Not Modified** is the twelfth visible packet.
- 31729 21.437197 199.232.46.172 192.168.37.241 TCP 1514 80 → 49886 [ACK] Seq=433 Ack=479 Win=31360 Len=1460 [TCP segment of a reassembled PDU]** is the thirteenth visible packet.
- 35052 25.010482 34.104.35.123 192.168.37.241 TCP 1514 80 → 49785 [ACK] Seq=690 Ack=333 Win=337 Len=1460 [TCP segment of a reassembled PDU]** is the fourteenth visible packet.
- 38303 28.649387 199.232.46.172 192.168.37.241 TCP 1514 80 → 49893 [ACK] Seq=1 Ack=197 Win=30336 Len=1460 [TCP segment of a reassembled PDU]** is the fifteenth visible packet.
- 38469 29.071176 34.104.35.123 192.168.37.241 TCP 1514 80 → 49785 [ACK] Seq=7145 Ack=669 Win=346 Len=1460 [TCP segment of a reassembled PDU]** is the sixteenth visible packet.
- 40208 31.116660 34.104.35.123 192.168.37.241 TCP 1514 80 → 49785 [ACK] Seq=16980 Ack=1006 Win=354 Len=1460 [TCP segment of a reassembled PDU]** is the seventeenth visible packet.
- 41004 32.142654 34.104.35.123 192.168.37.241 TCP 1514 80 → 49785 [ACK] Seq=17622 Ack=1324 Win=203 Len=1460 [TCP segment of a reassembled PDU]** is the eighteenth visible packet.

Details pane:

- Frame 13953: 1514 bytes on wire (12112 bits), 1514 bytes captured (12112 bits) on
- Ethernet II, Src: Sophos_fc_00:05 (c8:4f:86:f0:00:05), Dst: Dell_ad:1b:fd (8c:ec:4
- Internet Protocol Version 4, Src: 202.94.162.202, Dst: 192.168.37.241
- Transmission Control Protocol, Src Port: 80, Dst Port: 49874, Seq: 39091, Ack: 155

Bytes pane:

0000	8c 4c 4b ad 1b fd c8 4f 8c 00 05 08 00 45 00	-K- .O.....E-
0010	05 dc ce 91 4b 00 08 06 12 ca 5e a2 ca c9 a8@.~.^.~..
0020	25 f1 00 50 c2 d2 82 51 df bf 3e d8 d2 dd 50 10	%..P..Q..>..P..
0030	01 17 b5 20 00 00 48 54 54 50 2f 31 2e 31 20 32	...%.HT TP/1.1 2
0040	30 36 20 50 61 72 74 69 61 6c 20 43 6f 74 65	06 Part al Conte
0050	6e 74 0d 0a 53 65 72 76 65 72 3a 20 6e 67 69 6e	nt-Serv er: nginx
0060	78 0d 0a 44 61 74 65 3a 20 57 65 64 2c 20 30 31	x-Date: Wed, 01
0070	20 4f 63 74 20 32 30 32 35 20 30 33 3a 35 35 3a	Oct 202 5 03:55: