

# CS19541-COMPUTER NETWORKS-LAB MANUAL

## CAPTURING AND ANALYSING PACKETS USING WIRESHARK TOOL

To filter, capture, view, packets in Wireshark Tool.

Capture 100 packets from the Ethernet: IEEE 802.3 LAN Interface and save it.

### Procedure

- ☐ Select Local Area Connection in Wireshark.
- ☐ Go to capture ☐ option
- ☐ Select stop capture automatically after 100 packets.
- ☐ Then click Start capture.
- ☐ Save the packets.

### Output

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	Pegatron_e0:87:9e	Broadcast	ARP	60	Who has 172.16.9.94? Tell 172.16.9.138
2	0.000180	RealtekS_55:2c:b8	Broadcast	ARP	60	Who has 172.16.10.36? Tell 172.16.10.50
3	0.000294	RealtekS_55:2c:b8	Broadcast	ARP	60	Who has 172.16.11.36? Tell 172.16.10.50
4	0.000295	RealtekS_55:2c:b8	Broadcast	ARP	60	Who has 172.16.8.37? Tell 172.16.10.50
5	0.000296	RealtekS_55:2c:b8	Broadcast	ARP	60	Who has 172.16.9.37? Tell 172.16.10.50
6	0.000296	RealtekS_55:2c:b8	Broadcast	ARP	60	Who has 172.16.11.37? Tell 172.16.10.50
7	0.001460	fe80::4968:12a7:5e3...	ff02::1:3	LLMNR	95	Standard query 0xae2b A TLFL3-HDC101701
8	0.001622	172.16.8.95	224.0.0.252	LLMNR	75	Standard query 0xae2b A TLFL3-HDC101701
9	0.001623	172.16.8.95	224.0.0.252	LLMNR	75	Standard query 0x28c0 AAAA TLFL3-HDC101701
10	0.001625	fe80::4968:12a7:5e3...	ff02::1:3	LLMNR	95	Standard query 0x28c0 AAAA TLFL3-HDC101701
11	0.045051	fe80::4968:12a7:5e3...	ff02::1:3	LLMNR	95	Standard query 0xae2b A TLFL3-HDC101701

▶ Frame 7: 95 bytes on wire (760 bits), 95 bytes captured (760 bits) on interface 0

▶ Ethernet II, Src: Dell\_35:10:a8 (50:9a:4c:35:10:a8), Dst: IPv6mcast\_01:00:03 (33:33:00:01:00:03)

▶ Internet Protocol Version 6, Src: fe80::4968:12a7:5e36:523e, Dst: ff02::1:3

▲ User Datagram Protocol, Src Port: 62374, Dst Port: 5355

Source Port: 62374

Destination Port: 5355

Length: 41

Checksum: 0x90e0 [unverified]

[Checksum Status: Unverified]

[Stream index: 0]

▶ Link-local Multicast Name Resolution (query)

0000	33 33 00 01 00 03 50 9a	4c 35 10 a8 86 dd 60 00	33...P- L5....
0010	00 00 00 29 11 01 fe 80	00 00 00 00 00 00 49 68	....)....Ih
0020	12 a7 5e 36 52 3e ff 02	00 00 00 00 00 00 00 00	..^6R>....
0030	00 00 00 01 00 03 f3 a6	14 eb 00 29 90 e0 ae 2b	.....)....+
0040	00 00 00 01 00 00 00 00	00 00 0f 54 4c 46 4c 33	.....-TLFL3
0050	2d 48 44 43 31 30 31 37	30 31 00 00 01 00 01	-HDC1017 01....

1. Create a Filter to display only TCP/UDP packets, inspect the packets and provide the flow graph

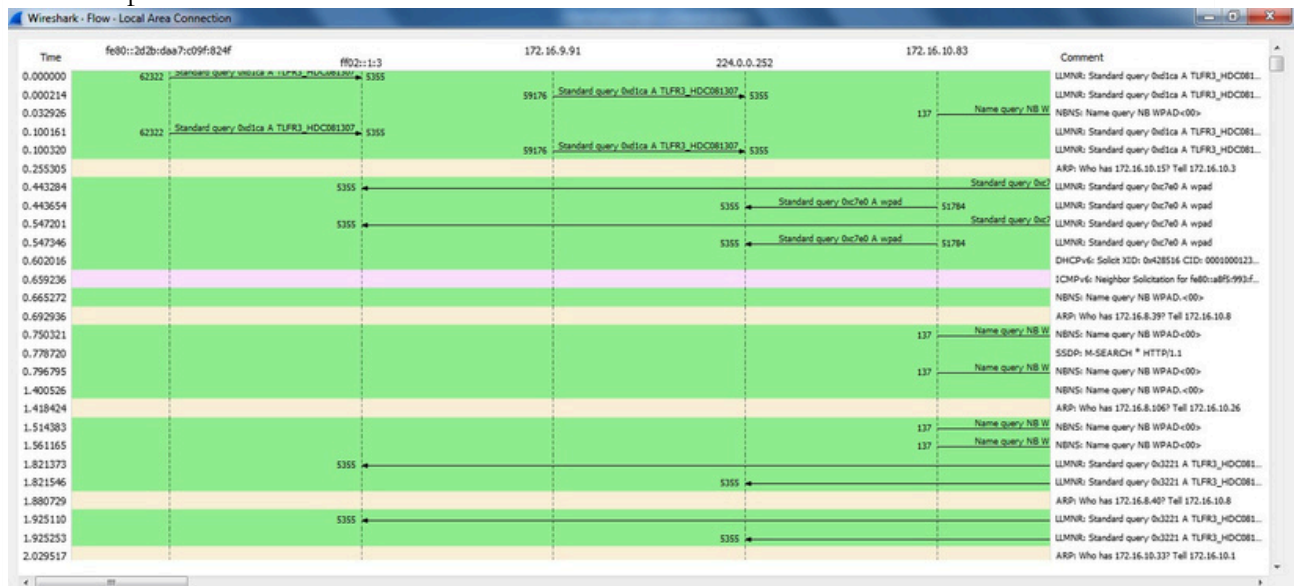
### Procedure

- ☐ Select Local Area Connection in Wireshark.
- ☐ Go to capture ☐ option
- ☐ Select stop capture automatically after 100 packets.
- ☐ Then click Start capture.
- ☐ Search TCP packets in search bar.
- ☐ To see flow graph click Statistics ☐ Flow graph.
- ☐ Save the packets.

# CS19541-COMPUTER NETWORKS-LAB MANUAL

No.	Time	Source	Destination	Protocol	Length	Info
123	4.557832	fe80::8532:3a9f:aff...	fe80::5c2b:19eb:d33...	TCP	74	1509 → 2869 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
126	4.557993	172.16.9.106	172.16.9.96	TCP	60	1506 → 2869 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
1095	30.718732	172.16.8.83	172.16.9.96	TCP	66	51526 → 2869 [SYN, ECH, CLR] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
1096	30.718794	172.16.9.96	172.16.8.83	TCP	66	2869 → 51526 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
1097	30.719129	172.16.8.83	172.16.9.96	TCP	60	51526 → 2869 [ACK] Seq=1 Ack=1 Win=65536 Len=0
1099	30.719919	172.16.9.96	172.16.8.83	TCP	278	2869 → 51526 [PSH, ACK] Seq=1 Ack=133 Win=65536 Len=224 [TCP segment of a reassembled PDU]
1100	30.719986	172.16.9.96	172.16.8.83	TCP	1514	2869 → 51526 [ACK] Seq=225 Ack=133 Win=65536 Len=1460 [TCP segment of a reassembled PDU]
1101	30.720279	172.16.8.83	172.16.9.96	TCP	60	51526 → 2869 [ACK] Seq=133 Ack=1685 Win=65536 Len=0
Frame 123: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface 0 Ethernet II, Src: Realtek5_b2:60:90 (00:e0:4c:b2:60:90), Dst: IntelCor_13:ed:7c (00:27:0e:13:ed:7c) Internet Protocol Version 6, Src: fe80::8532:3a9f:aff1:b3ca, Dst: fe80::5c2b:19eb:d33d:a1cd Transmission Control Protocol, Src Port: 1509, Dst Port: 2869, Seq: 1, Ack: 1, Len: 0						
0000	00 27 0e 13 ed 7c 00 e0	4c b2 60 90 86 dd 60 00	.....L.....			
0010	00 00 00 14 06 80 fe 80	00 00 00 00 00 85 32	.....2			
0020	3a 9f af f1 b3 ca fe 80	00 00 00 00 00 5c 2b	:.....\+			
0030	19 eb d3 3d a1 cd 05 e5	0b 35 3b ef f1 2f bd	.....5;./..			
0040	67 35 50 14 00 00 3e de	00 00	gSP > ..			

## Flow Graph



2. Create a Filter to display only ARP packets and inspect the packets.

### Procedure

- ☐ Go to capture ☐ option
- ☐ Select stop capture automatically after 100 packets.
- ☐ Then click Start capture.
- ☐ Search ARP packets in search bar.
- ☐ Save the packets.

# CS19541-COMPUTER NETWORKS-LAB MANUAL

## Output

arp						
No.	Time	Source	Destination	Protocol	Length	Info
6	0.255305	Foxconn_c9:c5:f0	Broadcast	ARP	60	Who has 172.16.10.15? Tell 172.16.10.3
14	0.692936	Foxconn_d0:ac:46	Broadcast	ARP	60	Who has 172.16.8.39? Tell 172.16.10.8
19	1.418424	Foxconn_c9:c9:91	Broadcast	ARP	60	Who has 172.16.8.106? Tell 172.16.10.26
24	1.880729	Foxconn_d0:ac:46	Broadcast	ARP	60	Who has 172.16.8.40? Tell 172.16.10.8
27	2.029517	Giga-Byt_92:d2:ef	Broadcast	ARP	60	Who has 172.16.10.33? Tell 172.16.10.1
41	2.509905	Giga-Byt_7c:c5:34	Broadcast	ARP	60	Who has 172.16.9.82? Tell 172.16.9.111
44	2.602358	Foxconn_c9:c8:24	Broadcast	ARP	60	Who has 172.16.8.139? Tell 172.16.10.22
46	2.743021	Dell_35:11:11	Broadcast	ARP	60	Who has 172.16.8.118? Tell 172.16.10.195
56	3.201822	Giga-Byt_92:d2:ef	Broadcast	ARP	60	Who has 172.16.10.34? Tell 172.16.10.1
60	3.237061	Giga-Byt_7c:c5:34	Broadcast	ARP	60	Who has 172.16.9.82? Tell 172.16.9.111
71	3.439062	Dell_35:11:11	Broadcast	ARP	60	Who has 172.16.8.118? Tell 172.16.10.195

▶ Frame 119: 42 bytes on wire (336 bits), 42 bytes captured (336 bits) on interface 0

▶ Ethernet II, Src: IntelCor\_13:ed:7c (00:27:0e:13:ed:7c), Dst: RealtekS\_b2:60:90 (00:e0:4c:b2:60:90)

▶ Address Resolution Protocol (reply)

0000	00 e0 4c b2 60 90 00 27 0e 13 ed 7c 08 06 00 01	..L.....
0010	08 00 06 04 00 02 00 27 0e 13 ed 7c ac 10 09 60	.....[...]
0020	00 e0 4c b2 60 90 ac 10 09 6a	..L.....

3. Create a Filter to display only DNS packets and provide the flow graph.

### Procedure

- ☐ Go to capture ☐ option
- ☐ Select stop capture automatically after 100 packets.
- ☐ Then click Start capture.
- ☐ Search DNS packets in search bar
- ☐ To see flow graph click Statistics ☐ Flow graph.
- ☐ Save the packets.

*Local Area Connection						
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help						
Filter						
No.	Time	Source	Destination	Protocol	Length	Info
989	32.977988	172.16.9.96	172.16.8.1	DNS	74	Standard query 0xe40 A www.google.com
990	32.978738	172.16.8.1	172.16.9.96	DNS	90	Standard query response 0xe40 A www.google.com A 172.217.163.132
1199	37.273599	172.16.9.96	172.16.8.1	DNS	79	Standard query 0xb50b A accounts.google.com
1200	37.273822	172.16.9.96	172.16.8.1	DNS	75	Standard query 0x6af4 A ssl.gstatic.com
1201	37.273837	172.16.8.1	172.16.9.96	DNS	95	Standard query response 0xb50b A accounts.google.com A 172.217.163.141
1202	37.273978	172.16.8.1	172.16.9.96	DNS	91	Standard query response 0x6af4 A ssl.gstatic.com A 172.217.26.163
1203	37.274368	172.16.9.96	172.16.8.1	DNS	77	Standard query 0xe76d A fonts.gstatic.com
1204	37.274541	172.16.8.1	172.16.9.96	DNS	129	Standard query response 0xe76d A fonts.gstatic.com CNAME.gstaticadssl.google.com A 172.217.160.131
1738	38.875803	172.16.9.96	172.16.8.1	DNS	80	Standard query 0x7a60 A accounts.youtube.com
1739	38.875294	172.16.8.1	172.16.9.96	DNS	124	Standard query response 0x7a60 A accounts.youtube.com CNAME www3.l.google.com A 172.217.167.142

▶ Frame 989: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface 0

▶ Ethernet II, Src: IntelCor\_13:ed:7c (00:27:0e:13:ed:7c), Dst: Caswell\_f2:b4:a1 (00:15:71:f2:b4:a1)

▶ Internet Protocol Version 4, Src: 172.16.9.96, Dst: 172.16.8.1

▶ User Datagram Protocol, Src Port: 62278, Dst Port: 53

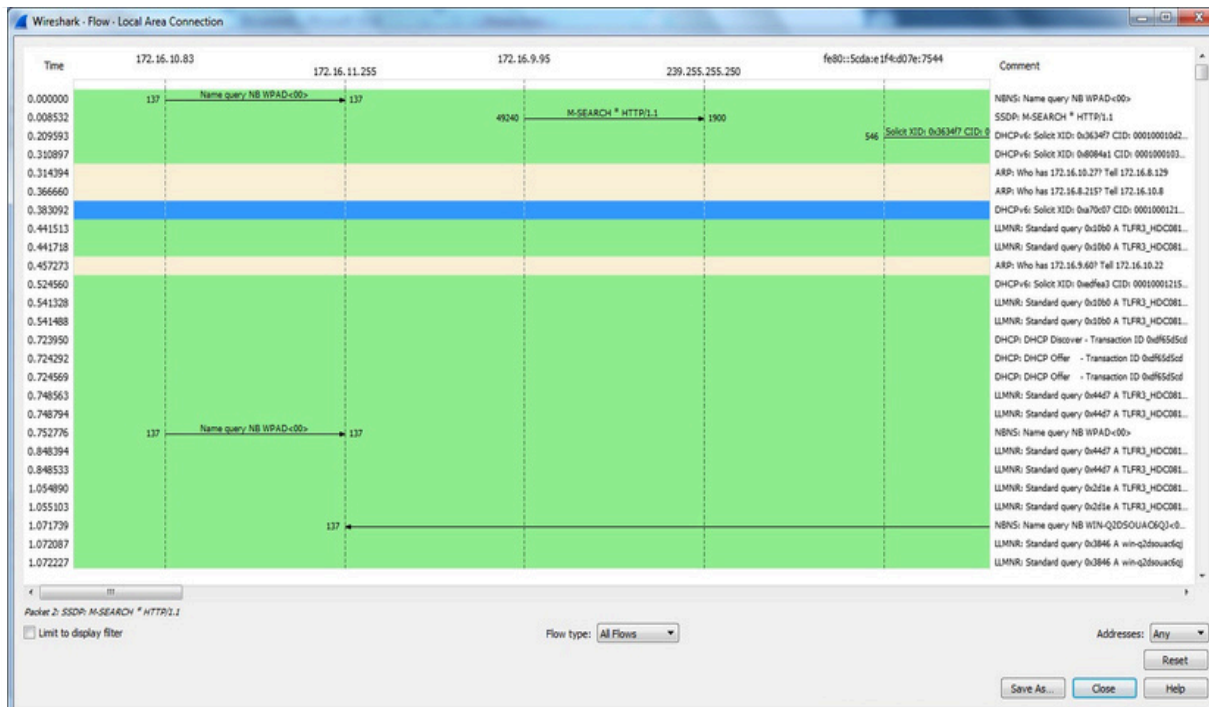
▶ Domain Name System (query)

0000	00 35 71 f2 b4 a1 00 27 0e 13 ed 7c 00 00 45 00	5g.....E
0010	00 3c 37 bb 00 00 00 11 00 00 ac 10 09 60 ac 10	<7.....
0020	00 01 f3 46 00 35 00 28 69 bb 9e 40 01 00 00 01	...FSLI@...
0030	00 00 00 00 00 00 00 63 77 77 00 67 6f 67 6c	...wwwgoogl
0040	65 03 63 6f 6d 00 00 01 00 01	e.com.....



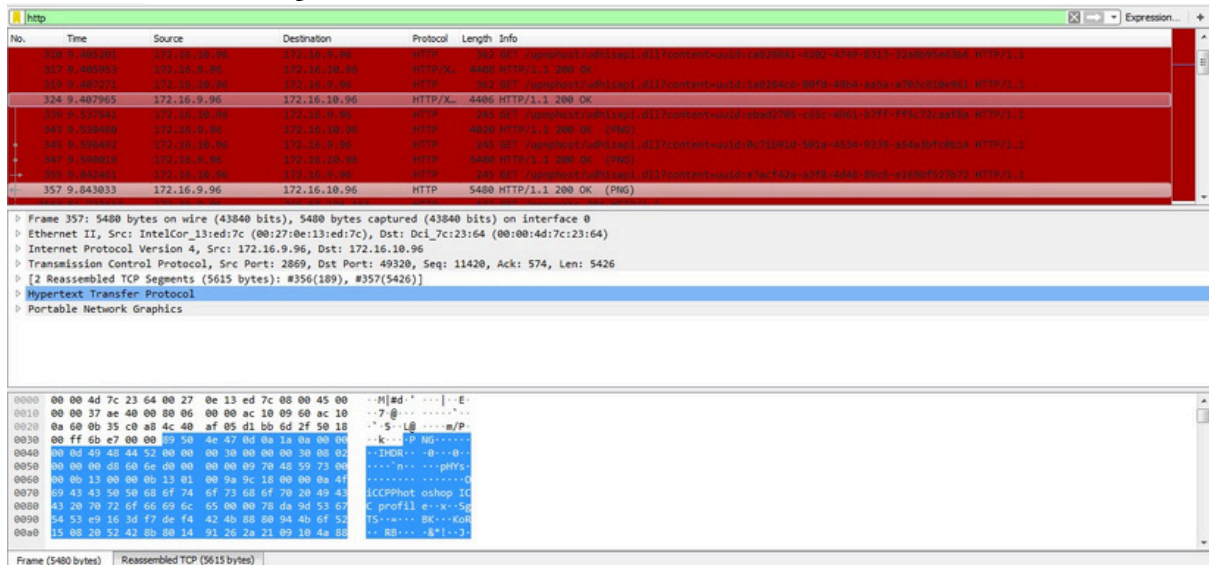
# CS19541-COMPUTER NETWORKS-LAB MANUAL



4. Create a Filter to display only HTTP packets and inspect the packets

## Procedure

- ☐ Select Local Area Connection in Wireshark.
- ☐ Go to capture ☐ option
- ☐ Select stop capture automatically after 100 packets.
- ☐ Then click Start capture.
- ☐ Search HTTP packets in search bar.
- ☐ Save the packets.

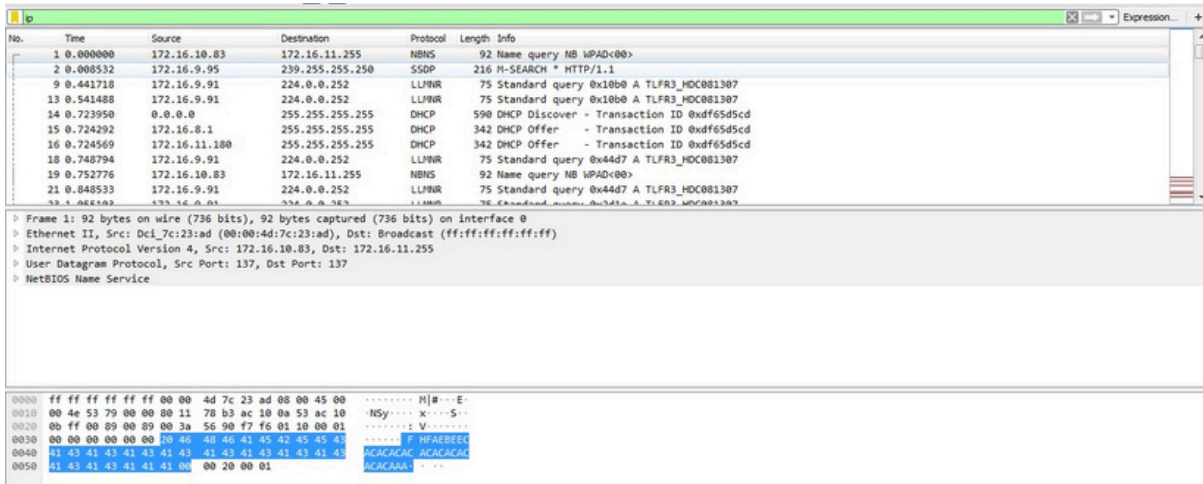


# CS19541-COMPUTER NETWORKS-LAB MANUAL

5. Create a Filter to display only IP/ICMP packets and inspect the packets.

Procedure

- ☐ Select Local Area Connection in Wireshark.
- ☐ Go to capture ☐ option
- ☐ Select stop capture automatically after 100 packets.
- ☐ Then click Start capture.
- ☐ Search ICMP/IP packets in search bar.
- ☐ Save the packets



6. Create a Filter to display only DHCP packets and inspect the packets.

Procedure

- ☐ Select Local Area Connection in Wireshark.
- ☐ Go to capture ☐ option
- ☐ Select stop capture automatically after 100 packets.
- ☐ Then click Start capture.
- ☐ Search DHCP packets in search bar.
- ☐ Save the packets

Output

