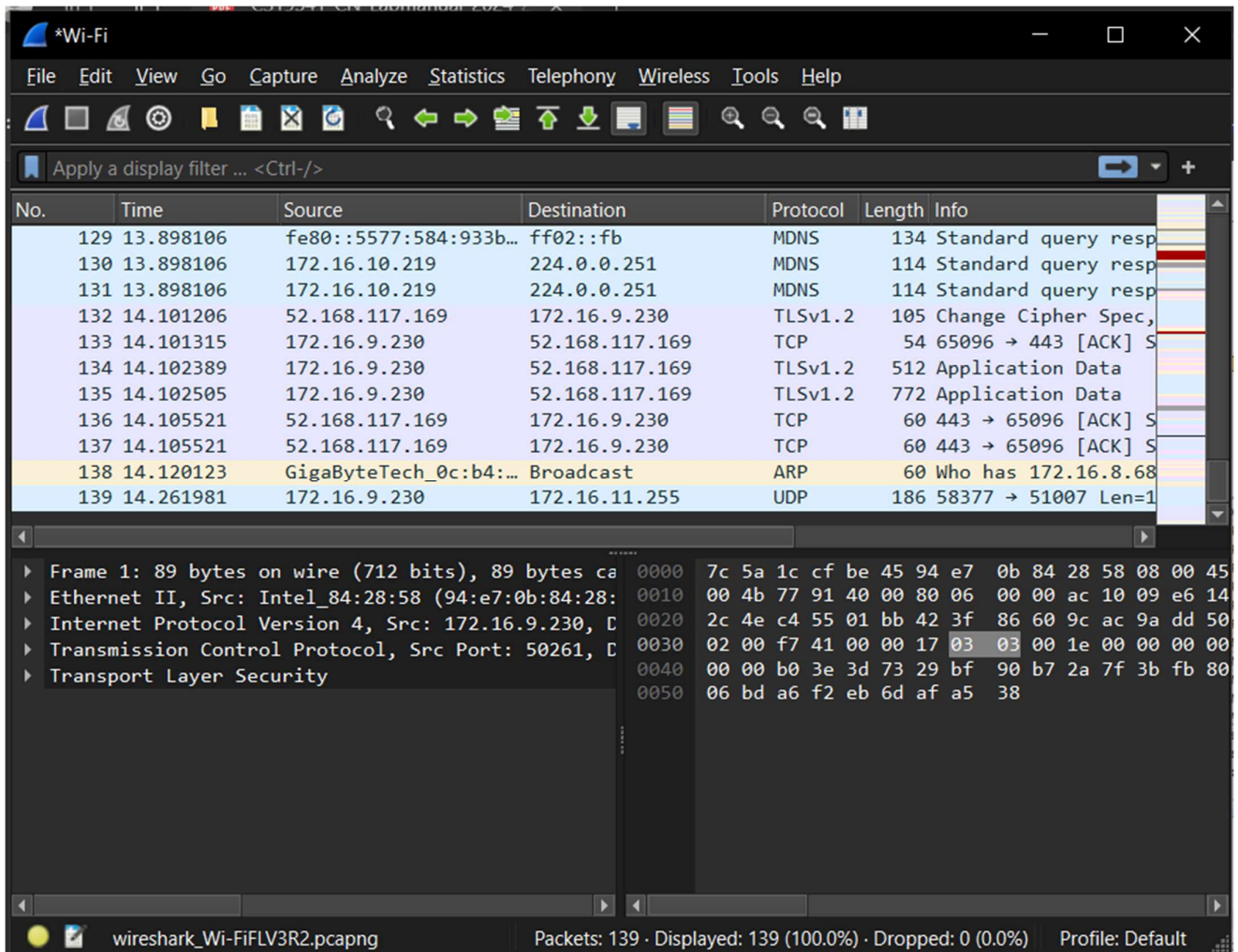


CAPTURING AND ANALYSING PACKETS USING WIRESHARK TOOL



The image shows the Wireshark network protocol analyzer interface. The top menu bar includes File, Edit, View, Go, Capture, Analyze, Statistics, Telephony, Wireless, Tools, and Help. Below the menu is a toolbar with various icons for file operations, capture control, and analysis. A display filter bar is present above the packet list.

The packet list table shows the following data:

No.	Time	Source	Destination	Protocol	Length	Info
129	13.898106	fe80::5577:584:933b...	ff02::fb	MDNS	134	Standard query resp
130	13.898106	172.16.10.219	224.0.0.251	MDNS	114	Standard query resp
131	13.898106	172.16.10.219	224.0.0.251	MDNS	114	Standard query resp
132	14.101206	52.168.117.169	172.16.9.230	TLSv1.2	105	Change Cipher Spec,
133	14.101315	172.16.9.230	52.168.117.169	TCP	54	65096 → 443 [ACK] S
134	14.102389	172.16.9.230	52.168.117.169	TLSv1.2	512	Application Data
135	14.102505	172.16.9.230	52.168.117.169	TLSv1.2	772	Application Data
136	14.105521	52.168.117.169	172.16.9.230	TCP	60	443 → 65096 [ACK] S
137	14.105521	52.168.117.169	172.16.9.230	TCP	60	443 → 65096 [ACK] S
138	14.120123	GigaByteTech_0c:b4:...	Broadcast	ARP	60	Who has 172.16.8.68
139	14.261981	172.16.9.230	172.16.11.255	UDP	186	58377 → 51007 Len=1

The detailed view of Frame 138 shows the following structure:

- Frame 1: 89 bytes on wire (712 bits), 89 bytes captured on interface
- Ethernet II, Src: Intel_84:28:58 (94:e7:0b:84:28:58), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
- Internet Protocol Version 4, Src: 172.16.9.230, Dst: 255.255.255.255
- Transmission Control Protocol, Src Port: 50261, Dst Port: 51007
- Transport Layer Security

The packet bytes are displayed in hexadecimal and ASCII format. The status bar at the bottom indicates: Packets: 139 · Displayed: 139 (100.0%) · Dropped: 0 (0.0%) · Profile: Default.

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

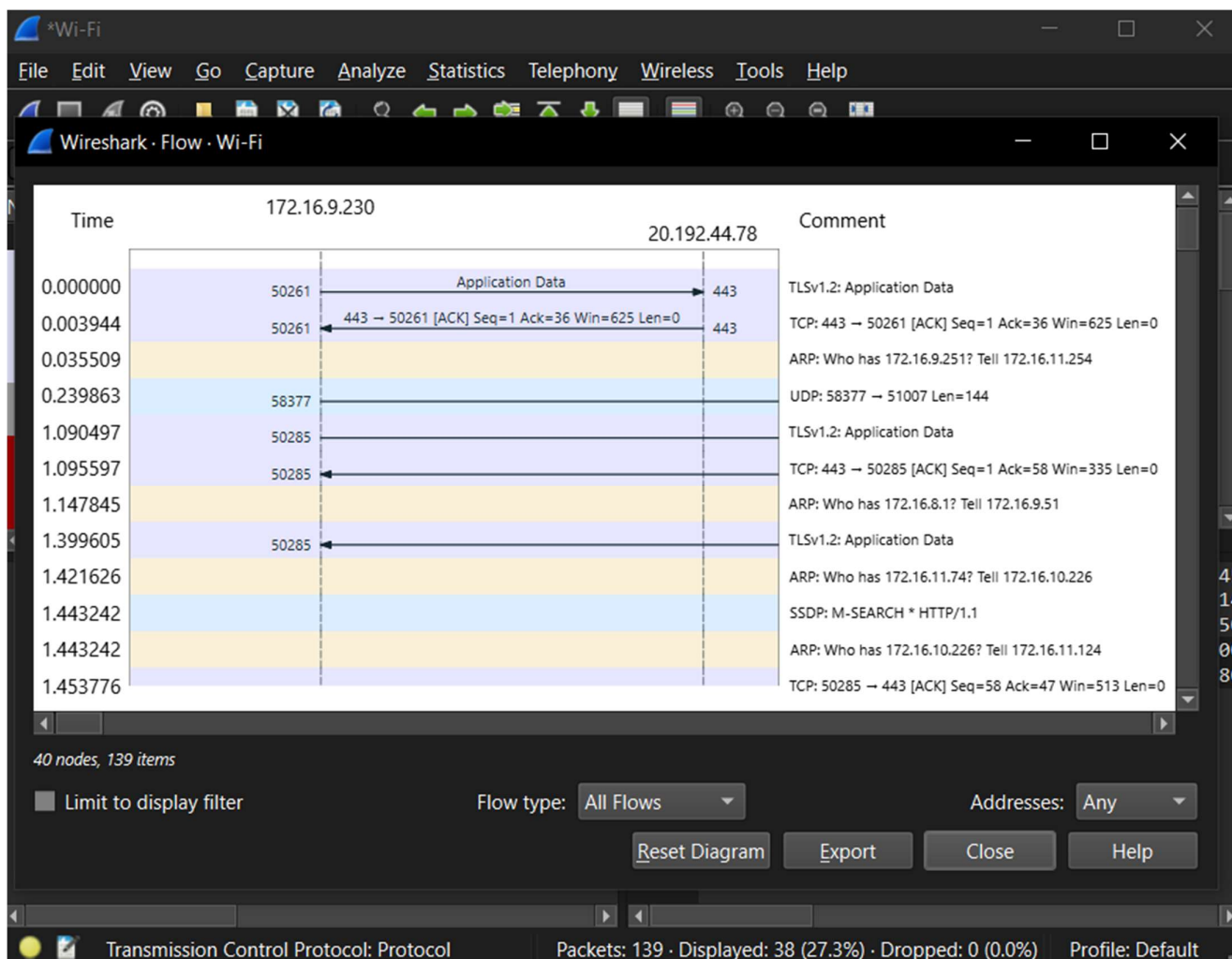
The image shows the Wireshark network protocol analyzer interface. The title bar indicates the capture is on a Wi-Fi interface. The menu bar includes File, Edit, View, Go, Capture, Analyze, Statistics, Telephony, Wireless, Tools, and Help. The toolbar contains icons for various functions like opening files, saving, and analyzing. A filter bar at the top shows the filter 'tcp' applied. The packet list pane displays a table of captured packets, with the first 28 packets shown. The packet details pane on the right shows the structure of the selected packet (No. 1), including Ethernet II, Internet Protocol Version 4, and Transport Layer Security. The packet bytes pane at the bottom shows the raw data in hexadecimal and ASCII.

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	172.16.9.230	20.192.44.78	TLSv1.2	89	Application Data
2	0.003944	20.192.44.78	172.16.9.230	TCP	60	443 → 50261 [ACK] S
5	1.090497	172.16.9.230	4.195.14.14	TLSv1.2	111	Application Data
6	1.095597	4.195.14.14	172.16.9.230	TCP	60	443 → 50285 [ACK] S
8	1.399605	4.195.14.14	172.16.9.230	TLSv1.2	100	Application Data
12	1.453776	172.16.9.230	4.195.14.14	TCP	54	50285 → 443 [ACK] S
16	3.381788	172.16.9.230	40.99.9.34	TCP	54	50536 → 443 [FIN, A
22	5.044442	172.16.9.230	23.223.244.137	TCP	54	50523 → 443 [FIN, A
25	5.299095	172.16.9.230	23.223.244.137	TCP	54	50531 → 443 [RST, A
26	5.299112	172.16.9.230	13.107.6.254	TCP	54	50540 → 443 [RST, A
27	5.299112	172.16.9.230	204.79.197.254	TCP	54	50541 → 443 [RST, A
28	5.299231	172.16.9.230	23.223.244.137	TCP	54	50534 → 443 [RST, A

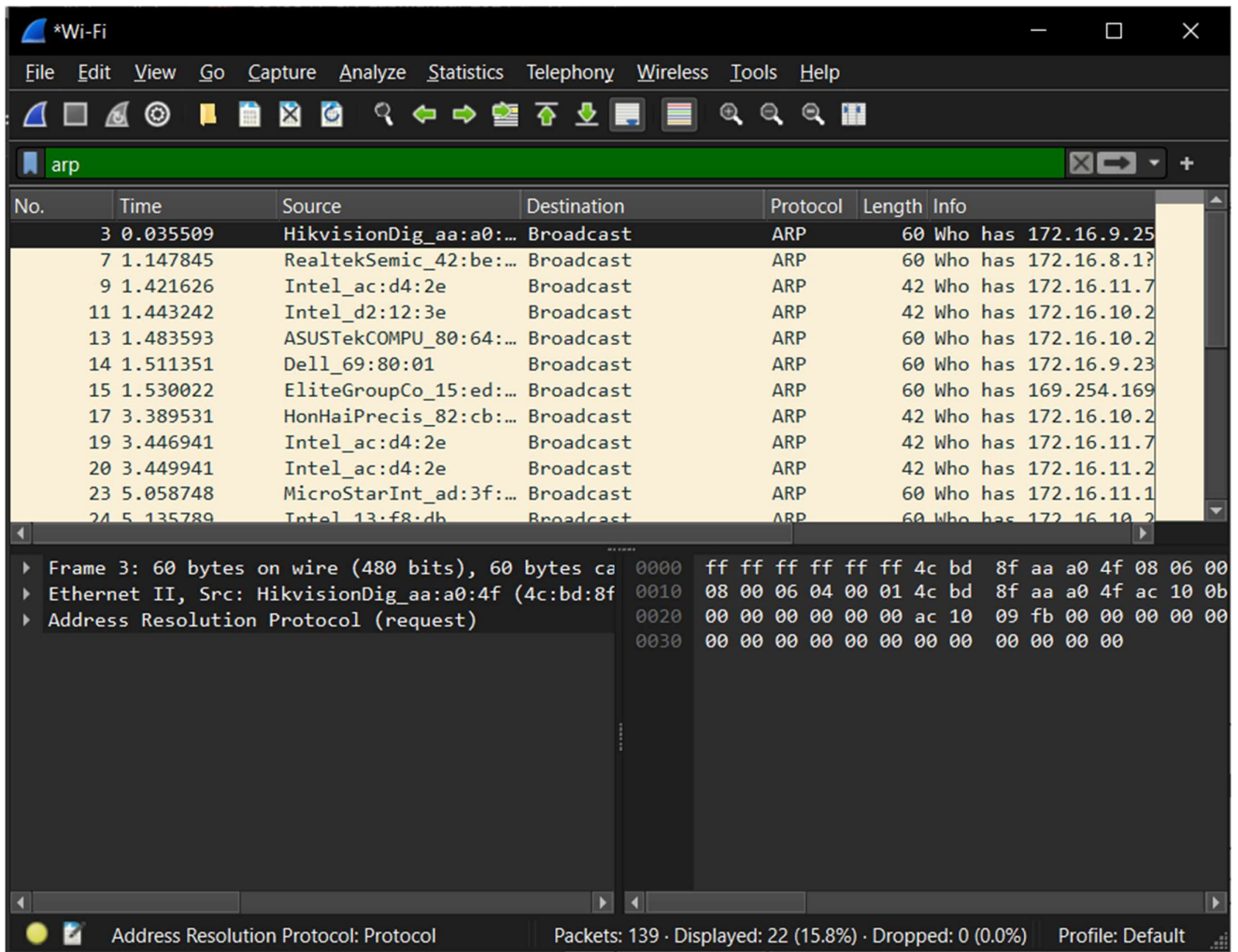
Frame 1: 89 bytes on wire (712 bits), 89 bytes captured (712 bits) on interface 0
Ethernet II, Src: Intel_84:28:58 (94:e7:0b:84:28:58), Dst: 08:00:27:00:00:00
Internet Protocol Version 4, Src: 172.16.9.230, Dst: 20.192.44.78
Transmission Control Protocol, Src Port: 50261, Dst Port: 443
Transport Layer Security

0000 7c 5a 1c cf be 45 94 e7 0b 84 28 58 08 00 45
0010 00 4b 77 91 40 00 80 06 00 00 ac 10 09 e6 14
0020 2c 4e c4 55 01 bb 42 3f 86 60 9c ac 9a dd 50
0030 02 00 f7 41 00 00 17 03 03 00 1e 00 00 00 00
0040 00 00 b0 3e 3d 73 29 bf 90 b7 2a 7f 3b fb 80
0050 06 bd a6 f2 eb 6d af a5 38

Transmission Control Protocol: Protocol Packets: 139 · Displayed: 38 (27.3%) · Dropped: 0 (0.0%) Profile: Default



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



The image shows the Wireshark network protocol analyzer interface. The title bar indicates the capture is on the *Wi-Fi interface. The menu bar includes File, Edit, View, Go, Capture, Analyze, Statistics, Telephony, Wireless, Tools, and Help. The toolbar contains various icons for file operations, capture control, and analysis. A green filter bar at the top displays the filter 'arp'. The packet list pane shows a list of captured packets, with the first three highlighted in yellow. The packet details pane shows the structure of the selected packet (Frame 3), including Ethernet II and Address Resolution Protocol (request). The packet bytes pane shows the raw data in hexadecimal and ASCII.

No.	Time	Source	Destination	Protocol	Length	Info
3	0.035509	HikvisionDig_aa:a0:...	Broadcast	ARP	60	Who has 172.16.9.25
7	1.147845	RealtekSemic_42:be:...	Broadcast	ARP	60	Who has 172.16.8.1?
9	1.421626	Intel_ac:d4:2e	Broadcast	ARP	42	Who has 172.16.11.7
11	1.443242	Intel_d2:12:3e	Broadcast	ARP	42	Who has 172.16.10.2
13	1.483593	ASUSTekCOMPU_80:64:...	Broadcast	ARP	60	Who has 172.16.10.2
14	1.511351	Dell_69:80:01	Broadcast	ARP	60	Who has 172.16.9.23
15	1.530022	EliteGroupCo_15:ed:...	Broadcast	ARP	60	Who has 169.254.169
17	3.389531	HonHaiPrecis_82:cb:...	Broadcast	ARP	42	Who has 172.16.10.2
19	3.446941	Intel_ac:d4:2e	Broadcast	ARP	42	Who has 172.16.11.7
20	3.449941	Intel_ac:d4:2e	Broadcast	ARP	42	Who has 172.16.11.2
23	5.058748	MicroStarInt_ad:3f:...	Broadcast	ARP	60	Who has 172.16.11.1
24	5.135789	Intel_13:f8:db	Broadcast	ARP	60	Who has 172.16.10.2

Frame 3: 60 bytes on wire (480 bits), 60 bytes captured on interface (480 bits) on Wi-Fi
Ethernet II, Src: HikvisionDig_aa:a0:4f (4c:bd:8f), Dst: ff:ff:ff:ff:ff:ff
Address Resolution Protocol (request)

Address Resolution Protocol: Protocol

Packets: 139 · Displayed: 22 (15.8%) · Dropped: 0 (0.0%) Profile: Default

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

The image shows the Wireshark network protocol analyzer interface. The top menu bar includes File, Edit, View, Go, Capture, Analyze, Statistics, Telephony, Wireless, Tools, and Help. The toolbar contains various icons for packet capture and analysis. The packet list pane shows a list of captured packets, with packet 62 selected. The packet details pane shows the structure of the selected packet, including Ethernet II, Internet Protocol Version 4, and Hypertext Transfer Protocol. The packet bytes pane shows the raw data of the selected packet in hexadecimal and ASCII.

No.	Time	Source	Destination	Protocol	Length	Info
62	1.333759	172.16.9.230	34.104.35.123	HTTP	520	GET /edgedl/diffgen
85	1.587342	34.104.35.123	172.16.9.230	HTTP	692	HTTP/1.1 416 Reques
89	1.589990	172.16.9.230	34.104.35.123	HTTP	500	HEAD /edgedl/diffge
103	1.681359	34.104.35.123	172.16.9.230	HTTP	707	HTTP/1.1 200 OK
115	1.735861	172.16.9.230	34.104.35.123	HTTP	520	GET /edgedl/diffgen
146	2.610929	34.104.35.123	172.16.9.230	HTTP	692	HTTP/1.1 416 Reques
155	2.613199	172.16.9.230	34.104.35.123	HTTP	500	HEAD /edgedl/diffge
166	2.928873	34.104.35.123	172.16.9.230	HTTP	707	HTTP/1.1 200 OK
184	2.992602	172.16.9.230	34.104.35.123	HTTP	520	GET /edgedl/diffgen
208	4.051452	34.104.35.123	172.16.9.230	HTTP	692	HTTP/1.1 416 Reques
212	4.053466	172.16.9.230	34.104.35.123	HTTP	500	HEAD /edgedl/diffge
217	4.252037	34.104.35.123	172.16.9.230	HTTP	668	HTTP/1.1 200 OK

Frame 62: 520 bytes on wire (4160 bits), 520 byte captured (4160 bits) on interface 0
 Ethernet II, Src: Intel_84:28:58 (94:e7:0b:84:28:58), Dst: 34:104:35:123:00:00
 Internet Protocol Version 4, Src: 172.16.9.230, Dst: 34.104.35.123
 Transmission Control Protocol, Src Port: 65107, Dst Port: 80
 Hypertext Transfer Protocol

0000 7c 5a 1c cf be 45 94 e7 0b 84 28 58 08 00
 0010 01 fa 90 bb 40 00 80 06 00 00 ac 10 09 e6
 0020 23 7b fe 53 00 50 cf 42 57 fe 87 35 12 eb
 0030 01 fe fd c5 00 00 47 45 54 20 2f 65 64 67
 0040 6c 2f 64 69 66 66 67 65 6e 2d 70 75 66 66
 0050 2f 68 66 6e 6b 70 69 6d 6c 68 68 67 69 65
 0060 64 67 66 65 6d 6a 68 6f 66 6d 66 62 6c 6d
 0070 62 2f 31 2e 62 31 37 36 61 30 63 33 61 31
 0080 64 62 63 30 62 34 63 38 65 33 38 34 64 66
 0090 38 31 33 36 63 32 39 32 65 63 38 61 38 63
 00a0 35 38 30 31 34 61 38 32 62 37 39 37 64 30
 00b0 39 38 33 38 2f 31 2e 64 36 38 66 31 66 64
 00c0 30 65 64 32 64 66 37 34 61 64 31 33 30 37
 00d0 65 39 64 34 36 35 30 37 35 62 65 33 38 65

Hypertext Transfer Protocol: Protocol
 Packets: 791 · Displayed: 24 (3.0%) · Dropped: 0 (0.0%) Profile: Default

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

The image shows the Wireshark network protocol analyzer interface. The top menu bar includes File, Edit, View, Go, Capture, Analyze, Statistics, Telephony, Wireless, Tools, and Help. Below the menu is a toolbar with various icons for packet capture and analysis. The main display area is divided into three panes:

- Packet List Pane:** Displays a list of captured packets. The selected packet is number 62, which is an HTTP GET request to /edgedl/diffgen.
- Packet Details Pane:** Shows the hierarchical structure of the selected packet. It includes Ethernet II, Internet Protocol Version 4, Transmission Control Protocol, and Hypertext Transfer Protocol.
- Packet Bytes Pane:** Displays the raw bytes of the selected packet in hexadecimal and ASCII format.

The status bar at the bottom indicates that 791 packets were captured, 591 were displayed (74.7%), and 0 were dropped (0.0%). The profile is set to Default.