


# wireshark101






[← Back to all walkthroughs](#)



## Wireshark 101

**Premium room**

Learn the basics of Wireshark and how to analyze various protocols and PCAPs

   60 min  95,481 

[Share your achievement](#) [Start AttackBox](#) [Badge](#) [Save Room](#) [2843 Recommend](#) [Options](#)

Room completed ( 100% )

**ARP or Address Resolution Protocol is a Layer 2 protocol that is used to connect IP Addresses with MAC Addresses. They will contain REQUEST messages and RESPONSE messages. To identify packets the message header will contain one of two operation codes:**

- ## What is the Opcode for Packet 6? Request (1)

[illegible]

What is the source MAC Address of Packet 19? 80:fb:06:f0:45:d7

Apply a display filter ... <Ctrl-/>						
No.	Time	Source	Destination	Protocol	Length	Info
6	23.595917	HuaweiTechno_f0:45:...	Sfr_e3:c3:31	ARP	60	Who has 10.251.196.22
7	23.595953	HuaweiTechno_f0:45:...	Sfr_60:2d:11	ARP	60	Who has 10.194.144.14
8	24.651131	Sfr_18:c2:73	Broadcast	PPPoED	82	Active Discovery Init
9	29.254270	0.0.0.0	255.255.255.255	DHCP	445	DHCP Discover - Trans
10	29.811743	Sfr_18:c2:73	Broadcast	PPPoED	82	Active Discovery Init
11	32.257198	0.0.0.0	255.255.255.255	DHCP	445	DHCP Discover - Trans
12	32.771702	HuaweiTechno_f0:45:...	Sfr_49:6d:f9	ARP	60	Who has 10.194.144.84
13	32.772685	HuaweiTechno_f0:45:...	MS-NLB-PhysServer-3...	ARP	60	Who has 10.194.144.14
14	32.774163	HuaweiTechno_f0:45:...	SagemcomBroa_17:e0:...	ARP	60	Who has 10.251.196.16
15	34.816127	Sfr_18:c2:73	Broadcast	PPPoED	82	Active Discovery Init
16	35.260227	0.0.0.0	255.255.255.255	DHCP	445	DHCP Discover - Trans
17	37.765789	HuaweiTechno_f0:45:...	Sfr_72:0a:d9	ARP	60	Who has 10.251.196.13
18	37.767245	HuaweiTechno_f0:45:...	Sfr_97:24:91	ARP	60	Who has 10.251.196.10
19	37.768724	HuaweiTechno_f0:45:...	Sfr_88:e7:a1	ARP	60	Who has 10.251.196.74
20	39.821132	Sfr_18:c2:73	Broadcast	PPPoED	82	Active Discovery Init
21	39.874293	Sfr_61:00:00	Sfr_18:c2:73	PPPoED	64	Active Discovery Offe
22	39.874692	Sfr_18:c2:73	Sfr_61:00:00	PPPoED	82	Active Discovery Requ
23	39.875775	Ericsson_03:a4:3b	Sfr_18:c2:73	PPPoED	64	Active Discovery Offe
24	40.024585	Sfr_61:00:00	Sfr_18:c2:73	PPPoED	64	Active Discovery Sess
25	40.048828	Sfr_18:c2:73	Sfr_61:00:00	PPP LCP	36	Configuration Request
26	40.071921	Sfr_61:00:00	Sfr_18:c2:73	PPP LCP	60	Configuration Request
27	40.071953	Sfr_61:00:00	Sfr_18:c2:73	PPP LCP	60	Configuration Ack
28	40.072258	Sfr_18:c2:73	Sfr_61:00:00	PPP LCP	41	Configuration Ack
29	40.072421	Sfr_18:c2:73	Sfr_61:00:00	PPP LCP	30	Echo Request
30	40.094086	Sfr_61:00:00	Sfr_18:c2:73	PPP CH...	60	Challenge (NAME='SE16
31	40.094268	Sfr_18:c2:73	Sfr_61:00:00	PPP CH...	63	Response (NAME='E0A1C
32	40.096058	Sfr_61:00:00	Sfr_18:c2:73	PPP LCP	60	Echo Reply
33	40.165272	Sfr_61:00:00	Sfr_18:c2:73	PPP CH...	64	Success (MESSAGE='CHA
34	40.165299	Sfr_61:00:00	Sfr_18:c2:73	PPP IP...	60	Configuration Request
35	40.165849	Sfr_18:c2:73	Sfr_61:00:00	PPP IP...	44	Configuration Request

Ethernet (1)  
IPv4 (0x0800)  
6  
4  
: (1)  
ress: HuaweiTechno\_f0:45:d7 (80:fb:06:f0:45:d7)  
ress: 10.251.196.1  
ress: 00:00:00\_00:00:00 (00:00:00:00:00:00)  
ress: 10.251.196.74

0000 30 7e cb 88 e7 a1 80 fb 06 f0 45 d7 08 06 00  
0010 08 00 06 04 00 01 80 fb 06 f0 45 d7 0a fb c4  
0020 00 00 00 00 00 00 0a fb c4 4a 01 49 ff ff ff  
0030 e9 20 24 37 07 de 01 02 00 00 00 3c

## What 4 packets are Reply packets? 76,400,459,520

nb6-startup\_1602384431514.pcap

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

arp.opcode==2

No.	Time	Source	Destination	Protocol	Length	Info
76	61.879014	HuaweiTechno_f0:45:...	Sfr_18:c2:72	ARP	60	10.251.23.1 is at 80:fb:06:f0:45:d7
400	1388651131.6...	HuaweiTechno_f0:45:...	Sfr_18:c2:72	ARP	60	10.251.23.1 is at 80:fb:06:f0:45:d7
459	1388651198.7...	HuaweiTechno_f0:45:...	Sfr_18:c2:72	ARP	60	10.251.23.1 is at 80:fb:06:f0:45:d7
520	1388651266.9...	HuaweiTechno_f0:45:...	Sfr_18:c2:72	ARP	60	10.251.23.1 is at 80:fb:06:f0:45:d7

## What IP Address is at 80:fb:06:f0:45:d7? 10.251.23.1

eth.addr == 80:fb:06:f0:45:d7

No.	Time	Source	Destination	Protocol	Length	Info
13	32.772685	HuaweiTechno_f0:45:...	MS-NLB-PhysServer-3...	ARP	60	Who has 10.194.144.14
14	32.774163	HuaweiTechno_f0:45:...	SagemcomBroa_17:e0:...	ARP	60	Who has 10.251.196.16
17	37.765789	HuaweiTechno_f0:45:...	Sfr_72:0a:d9	ARP	60	Who has 10.251.196.13
18	37.767245	HuaweiTechno_f0:45:...	Sfr_97:24:91	ARP	60	Who has 10.251.196.16
19	37.768724	HuaweiTechno_f0:45:...	Sfr_88:e7:a1	ARP	60	Who has 10.251.196.74
42	47.800605	HuaweiTechno_f0:45:...	MS-NLB-PhysServer-3...	ARP	60	Who has 10.194.144.16
43	47.800641	HuaweiTechno_f0:45:...	MS-NLB-PhysServer-3...	ARP	60	Who has 10.194.144.17
44	47.800663	HuaweiTechno_f0:45:...	SagemcomBroa_2d:55:...	ARP	60	Who has 10.251.196.18
45	52.775929	HuaweiTechno_f0:45:...	Sfr_ef:4c:11	ARP	60	Who has 10.251.196.15
46	52.777863	HuaweiTechno_f0:45:...	MS-NLB-PhysServer-3...	ARP	60	Who has 10.194.144.19
47	52.779336	HuaweiTechno_f0:45:...	Sfr_ae:e6:55	ARP	60	Who has 10.251.196.16
48	52.780310	HuaweiTechno_f0:45:...	SagemcomBroa_f5:28:...	ARP	60	Who has 10.251.196.53
49	52.781789	HuaweiTechno_f0:45:...	SagemcomBroa_1c:f2:...	ARP	60	Who has 10.251.196.17
58	58.449505	HuaweiTechno_f0:45:...	Broadcast	ARP	60	Who has 10.251.23.139
59	58.455650	10.194.143.1	10.251.23.139	DHCP	389	DHCP Offer - Trans
61	58.515752	10.194.143.1	10.251.23.139	DHCP	389	DHCP ACK - Trans
62	58.524464	10.194.143.1	10.251.23.139	DHCP	389	DHCP Offer - Trans
75	61.879584	86.64.145.29	10.251.23.139	ICMP	98	Echo (ping) request
76	61.879614	HuaweiTechno_f0:45:...	Sfr_18:c2:72	ARP	60	10.251.23.1 is at 80:fb:06:f0:45:d7
77	61.879898	10.251.23.139	86.66.0.227	TCP	74	35383 → 80 [SYN] Seq=
78	61.879932	10.251.23.139	86.64.145.29	ICMP	98	Echo (ping) reply
79	61.901780	86.66.0.227	10.251.23.139	TCP	74	80 → 35383 [SYN, ACK]
80	61.902071	10.251.23.139	86.66.0.227	TCP	66	35383 → 80 [ACK] Seq=
81	61.902421	10.251.23.139	86.66.0.227	TCP	71	35383 → 80 [PSH, ACK]
82	61.925158	86.66.0.227	10.251.23.139	TCP	66	80 → 35383 [ACK] Seq=
83	61.925376	10.251.23.139	86.66.0.227	HTTP	351	GET /cfgnb6dslgeneral
84	61.950288	86.66.0.227	10.251.23.139	TCP	66	80 → 35383 [ACK] Seq=
85	62.047389	86.66.0.227	10.251.23.139	TCP	1510	80 → 35383 [ACK] Seq=
86	62.047583	10.251.23.139	86.66.0.227	TCP	66	35383 → 80 [ACK] Seq=

## **ICMP Traffic Overview**

### **ICMP request:**

**Below we see packet details for a ping request packet. There are a few important things within the packet details that we can take note of first being the type and code of the packet. A type that equals 8 means that it is a request packet, if it is equal to 0 it is a reply packet. When these codes are altered or do not seem correct that is typically a sign of suspicious activity.**

**There are two other details within the packet that are useful to analyze: timestamp and data. The timestamp can be useful for identifying the time the ping was requested it can also be useful to identify suspicious activity in some cases. We can also look at the data string which will typically just be a random data string.**

## What is the type for packet 4?8

Apply a display filter ... <Ctrl-/>						
No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	192.168.43.9	192.168.43.1	DNS	80	Standard query 0x528e
2	5.001009	192.168.43.9	192.168.43.1	DNS	80	Standard query 0x528e
3	5.006792	192.168.43.1	192.168.43.9	DNS	124	Standard query response
→ 4	5.013334	192.168.43.9	8.8.8.8	ICMP	98	Echo (ping) request
← 5	5.505538	8.8.8.8	192.168.43.9	ICMP	98	Echo (ping) reply
6	6.019290	192.168.43.9	8.8.8.8	ICMP	98	Echo (ping) request
7	6.153653	8.8.8.8	192.168.43.9	ICMP	98	Echo (ping) reply
8	7.015108	192.168.43.9	8.8.8.8	ICMP	98	Echo (ping) request
9	7.781987	8.8.8.8	192.168.43.9	ICMP	98	Echo (ping) reply
10	7.791410	192.168.43.9	192.168.43.1	DNS	80	Standard query 0x695c
11	7.979359	192.168.43.1	192.168.43.9	DNS	124	Standard query response
12	7.983593	192.168.43.9	8.8.4.4	ICMP	98	Echo (ping) request
13	8.984437	192.168.43.9	8.8.4.4	ICMP	98	Echo (ping) request
14	9.323049	8.8.4.4	192.168.43.9	ICMP	98	Echo (ping) reply
15	9.985425	192.168.43.9	8.8.4.4	ICMP	98	Echo (ping) request
16	11.999365	192.168.43.9	192.168.43.1	DNS	80	Standard query 0x833a
17	12.073341	192.168.43.1	192.168.43.9	DNS	116	Standard query response
18	12.078588	192.168.43.9	4.2.2.2	ICMP	98	Echo (ping) request
19	12.148722	4.2.2.2	192.168.43.9	ICMP	98	Echo (ping) reply
20	13.079308	192.168.43.9	4.2.2.2	ICMP	98	Echo (ping) request
21	13.383662	4.2.2.2	192.168.43.9	ICMP	98	Echo (ping) reply
22	14.079860	192.168.43.9	4.2.2.2	ICMP	98	Echo (ping) request
23	15.280499	4.2.2.2	192.168.43.9	ICMP	98	Echo (ping) reply
24	15.289472	192.168.43.9	192.168.43.1	DNS	77	Standard query 0x2121
25	15.703377	192.168.43.1	192.168.43.9	DNS	93	Standard query response
26	15.722009	192.168.43.9	192.168.43.1	DNS	77	Standard query 0x2c58
27	15.865643	192.168.43.1	192.168.43.9	DNS	93	Standard query response
28	15.866126	192.168.43.9	174.137.42.65	ICMP	98	Echo (ping) request
29	16.636590	174.137.42.65	192.168.43.9	ICMP	98	Echo (ping) reply
30	16.867268	192.168.43.9	174.137.42.65	ICMP	98	Echo (ping) request

▶ Ethernet II, Src: Apple_13:c5:58 (60:33:4b:13:c5:58), Dst: 08:00:5e:00:00:00	0000	02 1a 11 f0 c8 3b 60 33 4b 13 c5 58 08 00 45
▶ Internet Protocol Version 4, Src: 192.168.43.9, Dst: 8.8.8.8	0010	00 54 26 ef 00 00 40 01 57 f9 c0 a8 2b 09 08
▼ Internet Control Message Protocol	0020	08 08 08 00 bb b3 d7 3b 00 00 51 a7 d6 7d 00
Type: Echo (ping) request (8)	0030	51 e4 08 09 0a 0b 0c 0d 0e 0f 10 11 12 13 14
Code: 0	0040	16 17 18 19 1a 1b 1c 1d 1e 1f 20 21 22 23 24
Checksum: 0xbbb3 [correct]	0050	26 27 28 29 2a 2b 2c 2d 2e 2f 30 31 32 33 34
[Checksum Status: Good]	0060	36 37
Identifier (BE): 55099 (0xd73b)		
Identifier (LE): 15319 (0x3bd7)		

## What is the type for packet 5?0

3	5.006792	192.168.43.1	192.168.43.9	DNS	124 Standard query response
→ 4	5.013334	192.168.43.9	8.8.8.8	ICMP	98 Echo (ping) request
← 5	5.505538	8.8.8.8	192.168.43.9	ICMP	98 Echo (ping) reply
6	6.019290	192.168.43.9	8.8.8.8	ICMP	98 Echo (ping) request
7	6.153653	8.8.8.8	192.168.43.9	ICMP	98 Echo (ping) reply
8	7.015108	192.168.43.9	8.8.8.8	ICMP	98 Echo (ping) request
9	7.781987	8.8.8.8	192.168.43.9	ICMP	98 Echo (ping) reply
10	7.791410	192.168.43.9	192.168.43.1	DNS	80 Standard query 0x695c
11	7.979359	192.168.43.1	192.168.43.9	DNS	124 Standard query response
12	7.983593	192.168.43.9	8.8.4.4	ICMP	98 Echo (ping) request
13	8.984437	192.168.43.9	8.8.4.4	ICMP	98 Echo (ping) request
14	9.323049	8.8.4.4	192.168.43.9	ICMP	98 Echo (ping) reply
15	9.985425	192.168.43.9	8.8.4.4	ICMP	98 Echo (ping) request
16	11.999365	192.168.43.9	192.168.43.1	DNS	80 Standard query 0x833a
17	12.073341	192.168.43.1	192.168.43.9	DNS	116 Standard query response
18	12.078588	192.168.43.9	4.2.2.2	ICMP	98 Echo (ping) request
19	12.148722	4.2.2.2	192.168.43.9	ICMP	98 Echo (ping) reply
20	13.079308	192.168.43.9	4.2.2.2	ICMP	98 Echo (ping) request
21	13.383662	4.2.2.2	192.168.43.9	ICMP	98 Echo (ping) reply
22	14.079860	192.168.43.9	4.2.2.2	ICMP	98 Echo (ping) request
23	15.280499	4.2.2.2	192.168.43.9	ICMP	98 Echo (ping) reply
24	15.289472	192.168.43.9	192.168.43.1	DNS	77 Standard query 0x2121
25	15.703377	192.168.43.1	192.168.43.9	DNS	93 Standard query response
26	15.722009	192.168.43.9	192.168.43.1	DNS	77 Standard query 0x2c58
27	15.865643	192.168.43.1	192.168.43.9	DNS	93 Standard query response
28	15.866126	192.168.43.9	174.137.42.65	ICMP	98 Echo (ping) request
29	16.636590	174.137.42.65	192.168.43.9	ICMP	98 Echo (ping) reply
30	16.867268	192.168.43.9	174.137.42.65	ICMP	98 Echo (ping) request

▶ Ethernet II, Src: MS-NLB-PhysServer-26_11:f0:c8:	0000	60 33 4b 13 c5 58 02 1a 11 f0 c8 3b 08 00 45
▶ Internet Protocol Version 4, Src: 8.8.8.8, Dst:	0010	00 54 00 00 00 00 28 01 96 e8 08 08 08 08 c0
▼ Internet Control Message Protocol	0020	2b 09 00 00 c3 b3 d7 3b 00 00 51 a7 d6 7d 00
Type: Echo (ping) reply (0)	0030	51 e4 08 09 0a 0b 0c 0d 0e 0f 10 11 12 13 14
Code: 0	0040	16 17 18 19 1a 1b 1c 1d 1e 1f 20 21 22 23 24
Checksum: 0xc3b3 [correct]	0050	26 27 28 29 2a 2b 2c 2d 2e 2f 30 31 32 33 34
[Checksum Status: Good]	0060	36 37
Identifier (BE): 55099 (0xd73b)		
Identifier (LE): 15319 (0x3bd7)		



What is the timestamp for packet 12, only including month day and year? May 30, 2013

Apply a display filter ... <Ctrl-/>

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	192.168.43.9	192.168.43.1	DNS	80	Standard query 0x528e
2	5.001009	192.168.43.9	192.168.43.1	DNS	80	Standard query 0x528e
3	5.006792	192.168.43.1	192.168.43.9	DNS	124	Standard query response
4	5.013334	192.168.43.9	8.8.8.8	ICMP	98	Echo (ping) request
5	5.505538	8.8.8.8	192.168.43.9	ICMP	98	Echo (ping) reply
6	6.019290	192.168.43.9	8.8.8.8	ICMP	98	Echo (ping) request
7	6.153653	8.8.8.8	192.168.43.9	ICMP	98	Echo (ping) reply
8	7.015108	192.168.43.9	8.8.8.8	ICMP	98	Echo (ping) request
9	7.781987	8.8.8.8	192.168.43.9	ICMP	98	Echo (ping) reply
10	7.791410	192.168.43.9	192.168.43.1	DNS	80	Standard query 0x695d
11	7.979359	192.168.43.1	192.168.43.9	DNS	124	Standard query response
12	7.983593	192.168.43.9	8.8.4.4	ICMP	98	Echo (ping) request
13	8.984437	192.168.43.9	8.8.4.4	ICMP	98	Echo (ping) request
14	9.323049	8.8.4.4	192.168.43.9	ICMP	98	Echo (ping) reply
15	9.985425	192.168.43.9	8.8.4.4	ICMP	98	Echo (ping) request
16	11.999365	192.168.43.9	192.168.43.1	DNS	80	Standard query 0x833a
17	12.073341	192.168.43.1	192.168.43.9	DNS	116	Standard query response
18	12.078588	192.168.43.9	4.2.2.2	ICMP	98	Echo (ping) request
19	12.148722	4.2.2.2	192.168.43.9	ICMP	98	Echo (ping) reply
20	13.079308	192.168.43.9	4.2.2.2	ICMP	98	Echo (ping) request
21	13.383662	4.2.2.2	192.168.43.9	ICMP	98	Echo (ping) reply
22	14.079860	192.168.43.9	4.2.2.2	ICMP	98	Echo (ping) request
23	15.280499	4.2.2.2	192.168.43.9	ICMP	98	Echo (ping) reply
24	15.289472	192.168.43.9	192.168.43.1	DNS	77	Standard query 0x2121
25	15.703377	192.168.43.1	192.168.43.9	DNS	93	Standard query response
26	15.722009	192.168.43.9	192.168.43.1	DNS	77	Standard query 0x2c58
27	15.865643	192.168.43.1	192.168.43.9	DNS	93	Standard query response
28	15.866126	192.168.43.9	174.137.42.65	ICMP	98	Echo (ping) request
29	16.636590	174.137.42.65	192.168.43.9	ICMP	98	Echo (ping) reply
30	16.867268	192.168.43.9	174.137.42.65	ICMP	98	Echo (ping) request

Identifier (BE): 56123 (0xdb3b)  
 Identifier (LE): 15323 (0x3bdb)  
 Sequence Number (BE): 0 (0x0000)  
 Sequence Number (LE): 0 (0x0000)  
 [No response seen]  
 ICMP Data: 51a7d6800003dd9808090a0b0c0d0e0f1011121  
 Timestamp from icmp data: May 31, 2013 01:45:20  
 [Timestamp from icmp data (relative): 110.000 m:  
 Data (48 bytes)

0000 02 1a 11 f0 c8 3b 60 33 4b 13 c5 58 08 00 45  
 0010 00 54 ae c7 00 00 40 01 d4 24 c0 a8 2b 09 08  
 0020 04 04 08 00 2b fd db 3b 00 00 51 a7 d6 80 00  
 0030 dd 98 08 09 0a 0b 0c 0d 0e 0f 10 11 12 13 14  
 0040 16 17 18 19 1a 1b 1c 1d 1e 1f 20 21 22 23 24  
 0050 26 27 28 29 2a 2b 2c 2d 2e 2f 30 31 32 33 34  
 0060 36 37



What is the full data string for packet 18?

08090a0b0c0d0e0f101112131415161718191a1b1c1d1e1f202122232425262728  
292a2b2c2d2e2f3031323334353637

Apply a display filter ... <Ctrl-/>						
No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	192.168.43.9	192.168.43.1	DNS	80	Standard query 0x528e PTR 8.8.8.8.in-addr.arpa
2	5.001009	192.168.43.9	192.168.43.1	DNS	80	Standard query 0x528e PTR 8.8.8.8.in-addr.arpa
3	5.006792	192.168.43.1	192.168.43.9	DNS	124	Standard query response 0x528e PTR 8.8.8.8.in-addr.arpa PTR google-public-dns-a.google.com
4	5.013334	192.168.43.9	8.8.8.8	ICMP	98	Echo (ping) request id=0xd73b, seq=0/0, ttl=64 (reply in 5)
5	5.505538	8.8.8.8	192.168.43.9	ICMP	98	Echo (ping) reply id=0xd73b, seq=0/0, ttl=64 (request in 4)
6	6.019290	192.168.43.9	8.8.8.8	ICMP	98	Echo (ping) request id=0xd73b, seq=1/256, ttl=64 (reply in 7)
7	6.153653	8.8.8.8	192.168.43.9	ICMP	98	Echo (ping) reply id=0xd73b, seq=1/256, ttl=64 (request in 6)
8	7.015108	192.168.43.9	8.8.8.8	ICMP	98	Echo (ping) request id=0xd73b, seq=2/512, ttl=64 (reply in 9)
9	7.781987	8.8.8.8	192.168.43.9	ICMP	98	Echo (ping) reply id=0xd73b, seq=2/512, ttl=64 (request in 8)
10	7.791410	192.168.43.9	192.168.43.1	DNS	80	Standard query 0xe95d PTR 4.4.8.8.in-addr.arpa
11	7.979359	192.168.43.1	192.168.43.9	DNS	124	Standard query response 0xe95d PTR 4.4.8.8.in-addr.arpa PTR google-public-dns-b.google.com
12	7.983593	192.168.43.9	8.8.4.4	ICMP	98	Echo (ping) request id=0xdb3b, seq=0/0, ttl=64 (no response found!)
13	8.984437	192.168.43.9	8.8.4.4	ICMP	98	Echo (ping) request id=0xdb3b, seq=1/256, ttl=64 (reply in 14)
14	9.323049	8.8.4.4	192.168.43.9	ICMP	98	Echo (ping) reply id=0xdb3b, seq=1/256, ttl=64 (request in 13)
15	9.985425	192.168.43.9	8.8.4.4	ICMP	98	Echo (ping) request id=0xdb3b, seq=2/512, ttl=64 (no response found!)
16	11.999365	192.168.43.9	192.168.43.1	DNS	80	Standard query 0x833a PTR 2.2.2.4.in-addr.arpa
17	12.073341	192.168.43.1	192.168.43.9	DNS	116	Standard query response 0x833a PTR 2.2.2.4.in-addr.arpa PTR b.resolvers.level3.net
18	12.070553	192.168.43.9	4.2.2.2	ICMP	98	Echo (ping) request id=0xdd3b, seq=0/0, ttl=64 (reply in 19)
19	12.148722	4.2.2.2	192.168.43.9	ICMP	98	Echo (ping) reply id=0xdd3b, seq=0/0, ttl=64 (request in 18)
20	13.079308	192.168.43.9	4.2.2.2	ICMP	98	Echo (ping) request id=0xdd3b, seq=1/256, ttl=64 (reply in 21)
21	13.383662	4.2.2.2	192.168.43.9	ICMP	98	Echo (ping) reply id=0xdd3b, seq=1/256, ttl=64 (request in 20)
22	14.079860	192.168.43.9	4.2.2.2	ICMP	98	Echo (ping) request id=0xdd3b, seq=2/512, ttl=64 (reply in 23)
23	15.280499	4.2.2.2	192.168.43.9	ICMP	98	Echo (ping) reply id=0xdd3b, seq=2/512, ttl=64 (request in 22)
24	15.280472	192.168.43.9	192.168.43.1	DNS	77	Standard query 0x2121 A www.wireshark.org
25	15.703377	192.168.43.1	192.168.43.9	DNS	93	Standard query response 0x2121 A www.wireshark.org A 174.137.42.65
26	15.722009	192.168.43.9	192.168.43.1	DNS	77	Standard query 0xc258 A www.wireshark.org
27	15.865643	192.168.43.1	192.168.43.9	DNS	93	Standard query response 0xc258 A www.wireshark.org A 174.137.42.65
28	15.866126	192.168.43.9	174.137.42.65	ICMP	98	Echo (ping) request id=0xe03b, seq=0/0, ttl=64 (reply in 29)
29	16.636590	174.137.42.65	192.168.43.9	ICMP	98	Echo (ping) reply id=0xe03b, seq=0/0, ttl=48 (request in 28)
30	16.867268	192.168.43.9	174.137.42.65	ICMP	98	Echo (ping) request id=0xe03b, seq=1/256, ttl=64 (reply in 31)
31	16.867268	174.137.42.65	192.168.43.9	ICMP	98	Echo (ping) reply id=0xe03b, seq=1/256, ttl=64 (request in 30)

Sequence Number (BE): 0 (0x0000)  
Sequence Number (LE): 0 (0x0000)  
[Response frame: 19]  
ICMP Data: 51a7d68400050bd08090a0b0c0d0e0f101112131415161718191a1b1c1d1e1f202122232425262728292a2b2c2d2e2f3031323334353637  
Timestamp from icmp data: May 31, 2013 01:45:24.348349000 Egypt Daylight Time  
[Timestamp from icmp data (relative): 92.000 microseconds]  
Data (48 bytes)  
Data: 08090a0b0c0d0e0f101112131415161718191a1b1c1d1e1f202122232425262728292a2b2c2d2e2f3031323334353637  
[Length: 48]

0000 02 1a 11 f0 c8 3b 60 33 4b 13 c5 58 08 00 45 00 .....3 K X E  
0010 00 54 d6 c6 00 00 40 01 b2 2d c0 a8 2b 09 04 02 .....@.....  
0020 02 02 08 00 b6 d2 dd 3b 00 00 51 a7 d6 84 00 05 .....:Q.....  
0030 50 bd 08 09 0a 0b 0c 0d 0e 0f 10 11 12 13 14 15 P.....  
0040 16 17 18 19 1a 1b 1c 1d 1e 1f 20 21 22 23 24 25 .....:7453  
0050 26 27 28 29 2a 2b 2c 2d 2e 2f 30 31 32 33 34 35 8\*()\*+,-./012345  
0060 36 37 67

## NS Overview

DNS or Domain Name Service protocol is used to resolves names with IP addresses. Just like the other protocols, you should be familiar with DNS; however, if you're not you can refresh with the [IETF DNS Documentation](#).

There are a couple of things outlined below that you should keep in the back of your mind when analyzing DNS packets.

- Query-Response
- DNS-Servers Only
- UDP

## What is being queried in packet 1? 8.8.8.8.in-addr.arpa

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	192.168.43.9	192.168.43.1	DNS	80	Standard query 0x528e
2	5.001009	192.168.43.9	192.168.43.1	DNS	80	Standard query 0x528e
3	5.006792	192.168.43.1	192.168.43.9	DNS	124	Standard query response
4	5.013334	192.168.43.9	8.8.8.8	ICMP	98	Echo (ping) request
5	5.505538	8.8.8.8	192.168.43.9	ICMP	98	Echo (ping) reply
6	6.019290	192.168.43.9	8.8.8.8	ICMP	98	Echo (ping) request
7	6.153653	8.8.8.8	192.168.43.9	ICMP	98	Echo (ping) reply
8	7.015108	192.168.43.9	8.8.8.8	ICMP	98	Echo (ping) request
9	7.781987	8.8.8.8	192.168.43.9	ICMP	98	Echo (ping) reply
10	7.791410	192.168.43.9	192.168.43.1	DNS	80	Standard query 0x695c
11	7.979359	192.168.43.1	192.168.43.9	DNS	124	Standard query response
12	7.983593	192.168.43.9	8.8.4.4	ICMP	98	Echo (ping) request
13	8.984437	192.168.43.9	8.8.4.4	ICMP	98	Echo (ping) request
14	9.323049	8.8.4.4	192.168.43.9	ICMP	98	Echo (ping) reply
15	9.985425	192.168.43.9	8.8.4.4	ICMP	98	Echo (ping) request
16	11.999365	192.168.43.9	192.168.43.1	DNS	80	Standard query 0x833a
17	12.073341	192.168.43.1	192.168.43.9	DNS	116	Standard query response
18	12.078588	192.168.43.9	4.2.2.2	ICMP	98	Echo (ping) request
19	12.148722	4.2.2.2	192.168.43.9	ICMP	98	Echo (ping) reply
20	13.079308	192.168.43.9	4.2.2.2	ICMP	98	Echo (ping) request
21	13.383662	4.2.2.2	192.168.43.9	ICMP	98	Echo (ping) reply
22	14.079860	192.168.43.9	4.2.2.2	ICMP	98	Echo (ping) request
23	15.280499	4.2.2.2	192.168.43.9	ICMP	98	Echo (ping) reply
24	15.289472	192.168.43.9	192.168.43.1	DNS	77	Standard query 0x2121
25	15.703377	192.168.43.1	192.168.43.9	DNS	93	Standard query response
26	15.722009	192.168.43.9	192.168.43.1	DNS	77	Standard query 0x2c58
27	15.865643	192.168.43.1	192.168.43.9	DNS	93	Standard query response
28	15.866126	192.168.43.9	174.137.42.65	ICMP	98	Echo (ping) request
29	16.636590	174.137.42.65	192.168.43.9	ICMP	98	Echo (ping) reply
30	16.867268	192.168.43.9	174.137.42.65	ICMP	98	Echo (ping) request

Transaction ID: 0x528e	0000 02 1a 11 f0 c8 3b 60 33 4b 13 c5 58 08 00 45
Flags: 0x0100 Standard query	0010 00 42 81 bf 00 00 40 11 21 91 c0 a8 2b 09 c0
Questions: 1	0020 2b 01 c9 dd 00 35 00 2e f2 68 52 8e 01 00 00
Answer RRs: 0	0030 00 00 00 00 00 00 01 38 01 38 01 38 01 38 07
Authority RRs: 0	0040 6e 2d 61 64 64 72 04 61 72 70 61 00 00 0c 00
Additional RRs: 0	
Queries	
8.8.8.8.in-addr.arpa: type PTR, class IN	
Name: 8.8.8.8.in-addr.arpa	

What site is being queried in packet 26? [www.wireshark.org](http://www.wireshark.org)

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	192.168.43.9	192.168.43.1	DNS	80	Standard query 0x528e
2	5.001009	192.168.43.9	192.168.43.1	DNS	80	Standard query 0x528e
3	5.006792	192.168.43.1	192.168.43.9	DNS	124	Standard query response
4	5.013334	192.168.43.9	8.8.8.8	ICMP	98	Echo (ping) request
5	5.505538	8.8.8.8	192.168.43.9	ICMP	98	Echo (ping) reply
6	6.019290	192.168.43.9	8.8.8.8	ICMP	98	Echo (ping) request
7	6.153653	8.8.8.8	192.168.43.9	ICMP	98	Echo (ping) reply
8	7.015108	192.168.43.9	8.8.8.8	ICMP	98	Echo (ping) request
9	7.781987	8.8.8.8	192.168.43.9	ICMP	98	Echo (ping) reply
10	7.791410	192.168.43.9	192.168.43.1	DNS	80	Standard query 0x695c
11	7.979359	192.168.43.1	192.168.43.9	DNS	124	Standard query response
12	7.983593	192.168.43.9	8.8.4.4	ICMP	98	Echo (ping) request
13	8.984437	192.168.43.9	8.8.4.4	ICMP	98	Echo (ping) request
14	9.323049	8.8.4.4	192.168.43.9	ICMP	98	Echo (ping) reply
15	9.985425	192.168.43.9	8.8.4.4	ICMP	98	Echo (ping) request
16	11.999365	192.168.43.9	192.168.43.1	DNS	80	Standard query 0x833a
17	12.073341	192.168.43.1	192.168.43.9	DNS	116	Standard query response
18	12.078588	192.168.43.9	4.2.2.2	ICMP	98	Echo (ping) request
19	12.148722	4.2.2.2	192.168.43.9	ICMP	98	Echo (ping) reply
20	13.079308	192.168.43.9	4.2.2.2	ICMP	98	Echo (ping) request
21	13.383662	4.2.2.2	192.168.43.9	ICMP	98	Echo (ping) reply
22	14.079860	192.168.43.9	4.2.2.2	ICMP	98	Echo (ping) request
23	15.280499	4.2.2.2	192.168.43.9	ICMP	98	Echo (ping) reply
24	15.289472	192.168.43.9	192.168.43.1	DNS	77	Standard query 0x2121
25	15.703377	192.168.43.1	192.168.43.9	DNS	93	Standard query response
26	15.722009	192.168.43.9	192.168.43.1	DNS	77	Standard query 0x2c58
27	15.865643	192.168.43.1	192.168.43.9	DNS	93	Standard query response
28	15.866126	192.168.43.9	174.137.42.65	ICMP	98	Echo (ping) request
29	16.636590	174.137.42.65	192.168.43.9	ICMP	98	Echo (ping) reply
30	16.867268	192.168.43.9	174.137.42.65	ICMP	98	Echo (ping) request

Transaction ID: 0x2c58	0000	02 1a 11 f0 c8 3b 60 33 4b 13 c5 58 08 00 45
Flags: 0x0100 Standard query	0010	00 3f 64 e7 00 00 ff 11 7f 6b c0 a8 2b 09 c0
Questions: 1	0020	2b 01 d5 63 00 35 00 2b 7f 5c 2c 58 01 00 00
Answer RRs: 0	0030	00 00 00 00 00 00 03 77 77 77 09 77 69 72 65
Authority RRs: 0	0040	68 61 72 6b 03 6f 72 67 00 00 01 00 01
Additional RRs: 0		
Queries		
www.wireshark.org: type A, class IN		
Name: www.wireshark.org		

## What is the Transaction ID for packet 26? 0x2c58

The image shows a Wireshark packet capture 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. A filter bar at the top of the packet list says "Apply a display filter ... <Ctrl-/>".

The packet list table has columns: No., Time, Source, Destination, Protocol, Length, and Info. Packet 26 is highlighted in purple. It is a DNS Standard query from 192.168.43.9 to 192.168.43.1 with Transaction ID 0x2c58.

No.	Time	Source	Destination	Protocol	Length	Info
4	5.013334	192.168.43.9	8.8.8.8	ICMP	98	Echo (ping) request
5	5.505538	8.8.8.8	192.168.43.9	ICMP	98	Echo (ping) reply
6	6.019290	192.168.43.9	8.8.8.8	ICMP	98	Echo (ping) request
7	6.153653	8.8.8.8	192.168.43.9	ICMP	98	Echo (ping) reply
8	7.015108	192.168.43.9	8.8.8.8	ICMP	98	Echo (ping) request
9	7.781987	8.8.8.8	192.168.43.9	ICMP	98	Echo (ping) reply
10	7.791410	192.168.43.9	192.168.43.1	DNS	80	Standard query 0x695c
11	7.979359	192.168.43.1	192.168.43.9	DNS	124	Standard query response
12	7.983593	192.168.43.9	8.8.4.4	ICMP	98	Echo (ping) request
13	8.984437	192.168.43.9	8.8.4.4	ICMP	98	Echo (ping) request
14	9.323049	8.8.4.4	192.168.43.9	ICMP	98	Echo (ping) reply
15	9.985425	192.168.43.9	8.8.4.4	ICMP	98	Echo (ping) request
16	11.999365	192.168.43.9	192.168.43.1	DNS	80	Standard query 0x833a
17	12.073341	192.168.43.1	192.168.43.9	DNS	116	Standard query response
18	12.078588	192.168.43.9	4.2.2.2	ICMP	98	Echo (ping) request
19	12.148722	4.2.2.2	192.168.43.9	ICMP	98	Echo (ping) reply
20	13.079308	192.168.43.9	4.2.2.2	ICMP	98	Echo (ping) request
21	13.383662	4.2.2.2	192.168.43.9	ICMP	98	Echo (ping) reply
22	14.079860	192.168.43.9	4.2.2.2	ICMP	98	Echo (ping) request
23	15.280499	4.2.2.2	192.168.43.9	ICMP	98	Echo (ping) reply
24	15.289472	192.168.43.9	192.168.43.1	DNS	77	Standard query 0x2121
25	15.703377	192.168.43.1	192.168.43.9	DNS	93	Standard query response
26	15.722009	192.168.43.9	192.168.43.1	DNS	77	Standard query 0x2c58
27	15.865643	192.168.43.1	192.168.43.9	DNS	93	Standard query response
28	15.866126	192.168.43.9	174.137.42.65	ICMP	98	Echo (ping) request
29	16.636590	174.137.42.65	192.168.43.9	ICMP	98	Echo (ping) reply
30	16.867268	192.168.43.9	174.137.42.65	ICMP	98	Echo (ping) request
31	17.194006	174.137.42.65	192.168.43.9	ICMP	98	Echo (ping) reply
32	17.867597	192.168.43.9	174.137.42.65	ICMP	98	Echo (ping) request
33	18.138642	174.137.42.65	192.168.43.9	ICMP	98	Echo (ping) reply

The packet details pane for packet 26 shows:

- Internet Protocol Version 4, Src: 192.168.43.9, Dst: 192.168.43.1
- User Datagram Protocol, Src Port: 54627, Dst Port: 53
- Domain Name System (query)
  - Transaction ID: 0x2c58
  - Flags: 0x0100 Standard query
  - Questions: 1
  - Answer RRs: 0
  - Authority RRs: 0
  - Additional RRs: 0

The packet bytes pane shows the raw data of the DNS query, with the Transaction ID field (offset 0020) containing the value 0x2c58.

HTTP or Hypertext Transfer Protocol is a commonly used port for the world wide web and used by some websites, however, its encrypted counterpart: HTTPS is more common which we will discuss in the next text. HTTP is used to send GET and POST requests to a web server in order to receive things like webpages. Knowing how to analyze HTTP can be helpful to quickly spot things like SQLi, Web Shells, and other web-related attack vectors.

What percent of packets originate from Domain Name System? 4.7

The image displays the Wireshark network protocol analyzer interface. The top menu bar includes File, Edit, View, Go, Capture, Analyze, Statistics, Telephony, Wireless, Tools, and Help. The Statistics menu is open, showing options like Capture File Properties, Resolved Addresses, Protocol Hierarchy, Conversations, Endpoints, Packet Lengths, I/O Graphs, Plots, Service Response Time, and DHCP (BOOTP) Statistics. The main packet list shows 10 packets with columns for No., Time, and Source. Packet 4 is selected. Below the packet list, the 'Wireshark - Protocol Hierarchy Statistics - http\_1601956000472.cap' window is open, showing a tree view of protocols and their corresponding packet and byte counts.

Protocol	Percent Packets	Packets	Percent Bytes
Frame	100.0	43	100.0
Ethernet	100.0	43	2.4
Internet Protocol Version 4	100.0	43	3.4
User Datagram Protocol	4.7	2	0.1
Domain Name System	4.7	2	0.8
Transmission Control Protocol	95.3	41	3.3
Hypertext Transfer Protocol	9.3	4	7.2
Line-based text data	2.3	1	14.4
eXtensible Markup Language	2.3	1	72.0



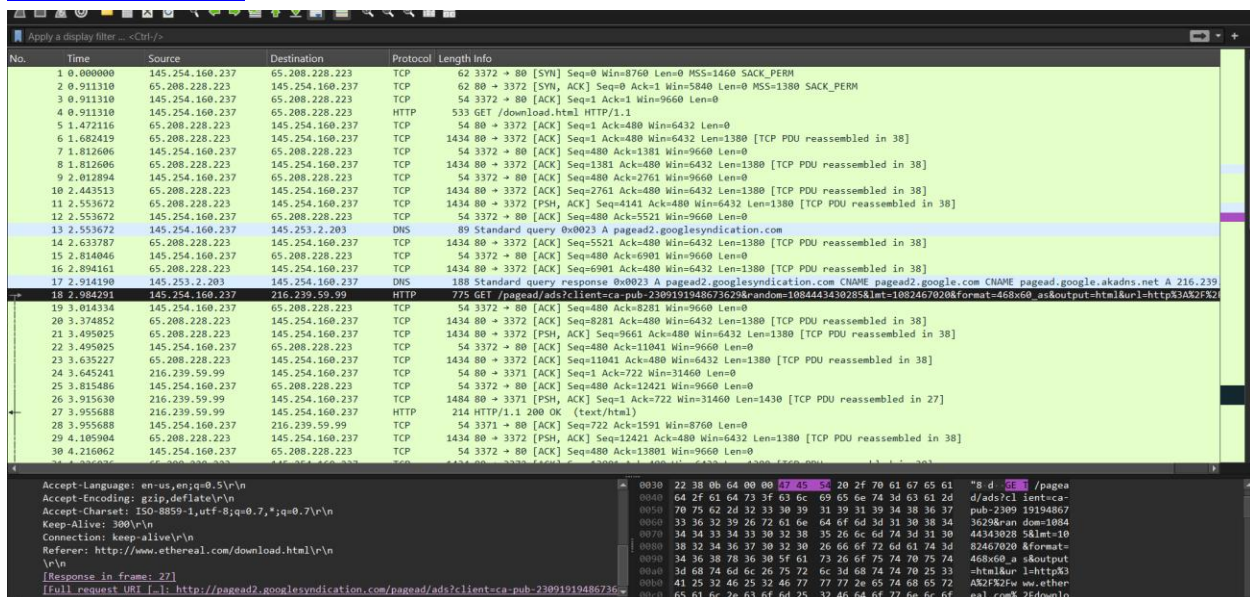
## What endpoint ends in .237? 145.254.160.237

No.	Time	Source	Destination	Protocol	Length	Info
4	0.911310	145.254.160.237	65.208.228.223	HTTP	533	GET /download.html HTTP/1.1
18	2.984291	145.254.160.237	216.239.59.99	HTTP	775	GET /pagead/ads?client=ca-p
27	3.955688	216.239.59.99	145.254.160.237	HTTP	214	HTTP/1.1 200 OK (text/html)
38	4.846969	65.208.228.223	145.254.160.237	HTTP/X...	478	HTTP/1.1 200 OK

- What is the user-agent listed in packet 4? Mozilla/5.0 (Windows; U; Windows NT 5.1; en-US; rv:1.6) Gecko/20040113\r\n

Looking at the data stream what is the full request URI from packet 18?

[http://pagead2.googlesyndication.com/pagead/ads?client=ca-pub-2309191948673629&random=1084443430285&lm=1082467020&format=468x60&as&output=html&url=http://www.ether.eal.com/.download.html&.color\\_bg=F FFFFF&color\\_text=333333&color\\_link=000000&color\\_url=666633&color\\_border=666633](http://pagead2.googlesyndication.com/pagead/ads?client=ca-pub-2309191948673629&random=1084443430285&lm=1082467020&format=468x60&as&output=html&url=http://www.ether.eal.com/.download.html&.color_bg=F FFFFF&color_text=333333&color_link=000000&color_url=666633&color_border=666633)



No.	Time	Source	Destination	Protocol	Length	Info
18	2.984291	145.254.160.237	216.239.59.99	HTTP	775	GET /pagead/ads?client=ca-pub-2309191948673629&random=1084443430285&lm=1082467020&format=468x60&as&output=html&url=http://www.ether.eal.com/.download.html&.color_bg=F FFFFF&color_text=333333&color_link=000000&color_url=666633&color_border=666633

Accept-Language: en-us,en;q=0.5\r\nAccept-Encoding: gzip,deflate\r\nAccept-Charset: ISO-8859-1,utf-8;q=0.7,\*;q=0.7\r\nKeep-Alive: 300\r\nConnection: keep-alive\r\nReferer: http://www.ether.eal.com/download.html\r\n\r\n[Response in frame: 27]

[Full request URI [..]: http://pagead2.googlesyndication.com/pagead/ads?client=ca-pub-2309191948673629&random=1084443430285&lm=1082467020&format=468x60&as&output=html&url=http://www.ether.eal.com/.download.html&.color\_bg=F FFFFF&color\_text=333333&color\_link=000000&color\_url=666633&color\_border=666633]

What domain name was requested from packet 38? [www.ethereal.com](http://www.ethereal.com)

The image shows a Wireshark packet capture 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. A display filter bar shows "Apply a display filter ... <Ctrl-/>".

The packet list pane displays the following data:

No.	Time	Source	Destination	Protocol	Length	Info
14	2.633787	65.208.228.223	145.254.160.237	TCP	1434	80 → 3372 [ACK] Seq=5
15	2.814046	145.254.160.237	65.208.228.223	TCP	54	3372 → 80 [ACK] Seq=4
16	2.894161	65.208.228.223	145.254.160.237	TCP	1434	80 → 3372 [ACK] Seq=6
17	2.914190	145.253.2.203	145.254.160.237	DNS	188	Standard query respon
18	2.984291	145.254.160.237	216.239.59.99	HTTP	775	GET /pagead/ads?clier
19	3.014334	145.254.160.237	65.208.228.223	TCP	54	3372 → 80 [ACK] Seq=4
20	3.374852	65.208.228.223	145.254.160.237	TCP	1434	80 → 3372 [ACK] Seq=8
21	3.495025	65.208.228.223	145.254.160.237	TCP	1434	80 → 3372 [PSH, ACK]
22	3.495025	145.254.160.237	65.208.228.223	TCP	54	3372 → 80 [ACK] Seq=4
23	3.635227	65.208.228.223	145.254.160.237	TCP	1434	80 → 3372 [ACK] Seq=1
24	3.645241	216.239.59.99	145.254.160.237	TCP	54	80 → 3371 [ACK] Seq=1
25	3.815486	145.254.160.237	65.208.228.223	TCP	54	3372 → 80 [ACK] Seq=4
26	3.915630	216.239.59.99	145.254.160.237	TCP	1484	80 → 3371 [PSH, ACK]
27	3.955688	216.239.59.99	145.254.160.237	HTTP	214	HTTP/1.1 200 OK (tex
28	3.955688	145.254.160.237	216.239.59.99	TCP	54	3371 → 80 [ACK] Seq=7
29	4.105904	65.208.228.223	145.254.160.237	TCP	1434	80 → 3372 [PSH, ACK]
30	4.216062	145.254.160.237	65.208.228.223	TCP	54	3372 → 80 [ACK] Seq=4
31	4.226076	65.208.228.223	145.254.160.237	TCP	1434	80 → 3372 [ACK] Seq=1
32	4.356264	65.208.228.223	145.254.160.237	TCP	1434	80 → 3372 [ACK] Seq=1
33	4.356264	145.254.160.237	65.208.228.223	TCP	54	3372 → 80 [ACK] Seq=4
34	4.496465	65.208.228.223	145.254.160.237	TCP	1434	80 → 3372 [ACK] Seq=1
35	4.496465	145.254.160.237	65.208.228.223	TCP	54	3372 → 80 [ACK] Seq=4
36	4.776868	216.239.59.99	145.254.160.237	TCP	1484	[TCP Spurious Retrans
37	4.776868	145.254.160.237	216.239.59.99	TCP	54	[TCP Dup ACK 28#1] 33
38	4.846969	65.208.228.223	145.254.160.237	HTTP/X...	478	HTTP/1.1 200 OK
39	5.017214	145.254.160.237	65.208.228.223	TCP	54	3372 → 80 [ACK] Seq=4
40	17.905747	65.208.228.223	145.254.160.237	TCP	54	80 → 3372 [FIN, ACK]
41	17.905747	145.254.160.237	65.208.228.223	TCP	54	3372 → 80 [ACK] Seq=4
42	30.063228	145.254.160.237	65.208.228.223	TCP	54	3372 → 80 [FIN, ACK]
43	30.393704	65.208.228.223	145.254.160.237	TCP	54	80 → 3372 [ACK] Seq=1

The packet details pane for packet 38 shows:

- Internet Protocol Version 4, Src: 65.208.228.223, Dst: 145.254.160.237
- Transmission Control Protocol, Seq: 3372, Len: 478, Win: 0, Len: 478
- Hypertext Transfer Protocol, 200 OK

The packet bytes pane shows the raw data of the packet, including the HTTP response status and headers.



Looking at the data stream what is the full request URI from packet 38?

<http://www.ethereal.com/download.html>

Apply a display filter ... <span>Ctrl-/</span>						
No.	Time	Source	Destination	Protocol	Length	Info
14	2.633787	65.208.228.223	145.254.160.237	TCP	1434	80 → 3372 [ACK] Seq=5
15	2.814046	145.254.160.237	65.208.228.223	TCP	54	3372 → 80 [ACK] Seq=4
16	2.894161	65.208.228.223	145.254.160.237	TCP	1434	80 → 3372 [ACK] Seq=6
17	2.914190	145.253.2.203	145.254.160.237	DNS	188	Standard query respon
18	2.984291	145.254.160.237	216.239.59.99	HTTP	775	GET /pagead/ads?clier
19	3.014334	145.254.160.237	65.208.228.223	TCP	54	3372 → 80 [ACK] Seq=4
20	3.374852	65.208.228.223	145.254.160.237	TCP	1434	80 → 3372 [ACK] Seq=8
21	3.495025	65.208.228.223	145.254.160.237	TCP	1434	80 → 3372 [PSH, ACK]
22	3.495025	145.254.160.237	65.208.228.223	TCP	54	3372 → 80 [ACK] Seq=4
23	3.635227	65.208.228.223	145.254.160.237	TCP	1434	80 → 3372 [ACK] Seq=1
24	3.645241	216.239.59.99	145.254.160.237	TCP	54	80 → 3371 [ACK] Seq=1
25	3.815486	145.254.160.237	65.208.228.223	TCP	54	3372 → 80 [ACK] Seq=4
26	3.915630	216.239.59.99	145.254.160.237	TCP	1484	80 → 3371 [PSH, ACK]
27	3.955688	216.239.59.99	145.254.160.237	HTTP	214	HTTP/1.1 200 OK (tex
28	3.955688	145.254.160.237	216.239.59.99	TCP	54	3371 → 80 [ACK] Seq=7
29	4.105904	65.208.228.223	145.254.160.237	TCP	1434	80 → 3372 [PSH, ACK]
30	4.216062	145.254.160.237	65.208.228.223	TCP	54	3372 → 80 [ACK] Seq=4
31	4.226076	65.208.228.223	145.254.160.237	TCP	1434	80 → 3372 [ACK] Seq=1
32	4.356264	65.208.228.223	145.254.160.237	TCP	1434	80 → 3372 [ACK] Seq=1
33	4.356264	145.254.160.237	65.208.228.223	TCP	54	3372 → 80 [ACK] Seq=4
34	4.496465	65.208.228.223	145.254.160.237	TCP	1434	80 → 3372 [ACK] Seq=1
35	4.496465	145.254.160.237	65.208.228.223	TCP	54	3372 → 80 [ACK] Seq=4
36	4.776868	216.239.59.99	145.254.160.237	TCP	1484	[TCP Spurious Retrans
37	4.776868	145.254.160.237	216.239.59.99	TCP	54	[TCP Dup ACK 28#1] 33
38	4.846969	65.208.228.223	145.254.160.237	HTTP/X...	478	HTTP/1.1 200 OK
39	5.017214	145.254.160.237	65.208.228.223	TCP	54	3372 → 80 [ACK] Seq=4
40	17.905747	65.208.228.223	145.254.160.237	TCP	54	80 → 3372 [FIN, ACK]
41	17.905747	145.254.160.237	65.208.228.223	TCP	54	3372 → 80 [ACK] Seq=4
42	30.063228	145.254.160.237	65.208.228.223	TCP	54	3372 → 80 [FIN, ACK]
43	30.393704	65.208.228.223	145.254.160.237	TCP	54	80 → 3372 [ACK] Seq=1

Connection: Keep-Alive\r\nContent-Type: text/html; charset=ISO-8859-1\r\n\r\n[Request in frame: 4][Time since request: 3.935659000 seconds][Request URI: /download.html][Full request URI: http://www.ethereal.com/doFile Data: 18070 byteseXtensible Markup Language

0000485454502f312e3120323030204f400100a446174653a205468752c203133200020617920323030342031303a31373a30003020474d540d0a5365727665723a20400040616368650d0a4c6173742d4d6f646000506965643a205475652c203230204170006020323030342031333a31373a30302000704d540d0a455461673a20223961303

Packet (478 bytes)Reassembled TCP (18364 bytes)Deco

## HTTPS Traffic Overview

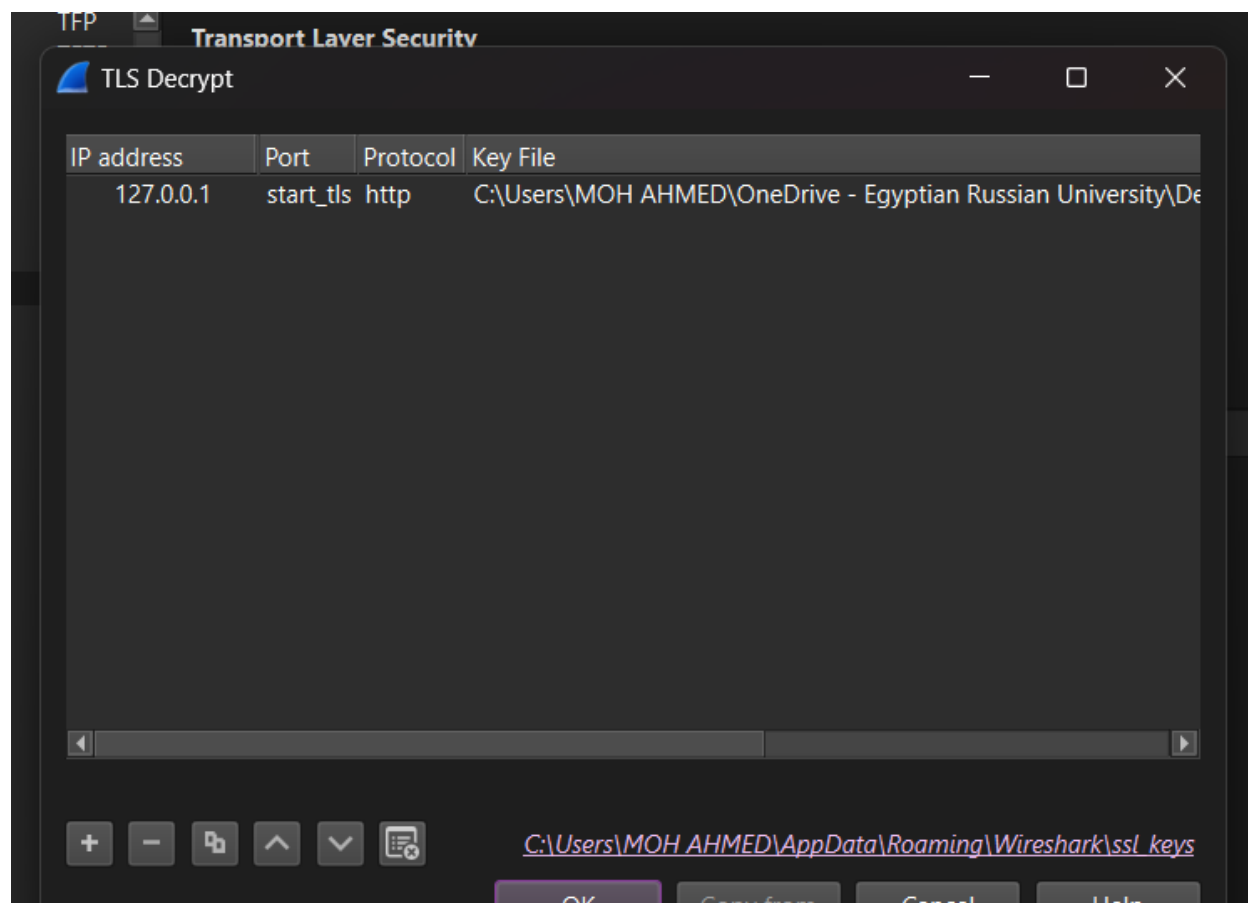
Before sending encrypted information the client and server need to agree upon various steps in order to make a secure tunnel.

1. Client and server agree on a protocol version
2. Client and server select a cryptographic algorithm
3. The client and server can authenticate to each other; this step is optional

**4. Creates a secure tunnel with a public key**

**Looking at the data stream what is the full request URI for packet 31?**

**[https://localhost/icons/apache\\_pb.png](https://localhost/icons/apache_pb.png)**



File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Apply a display filter ... <Ctrl-/>

No.	Time	Source	Destination	Protocol	Length	Info
16	2.938999	127.0.0.1	127.0.0.1	SSLv3	1073	Server Hello, Certificate, Server Hello Done
17	2.940026	127.0.0.1	127.0.0.1	SSLv3	337	Client Key Exchange, Change Cipher Spec, Finished
18	2.943406	127.0.0.1	127.0.0.1	SSLv3	172	Change Cipher Spec, Finished
19	2.944825	127.0.0.1	127.0.0.1	HTTP	5756	HTTP/1.1 200 OK (text/html)
20	2.944864	127.0.0.1	127.0.0.1	TCP	66	38713 → 443 [ACK] Seq=1143 Ack=7845 Win=32767 Len=0
21	2.964424	127.0.0.1	127.0.0.1	HTTP	471	GET /icons/jhe061.png HTTP/1.1
22	2.964572	127.0.0.1	127.0.0.1	TCP	74	38714 → 443 [SYN] Seq=0 Win=32767 Len=0 MSS=16396
23	2.964588	127.0.0.1	127.0.0.1	TCP	74	443 → 38714 [SYN, ACK] Seq=0 Ack=1 Win=32767 Len=0
24	2.964598	127.0.0.1	127.0.0.1	TCP	66	38714 → 443 [ACK] Seq=1 Ack=1 Win=32767 Len=0 TSv=0
25	2.964810	127.0.0.1	127.0.0.1	SSLv3	186	Client Hello
26	2.964819	127.0.0.1	127.0.0.1	TCP	66	443 → 38714 [ACK] Seq=1 Ack=121 Win=32767 Len=0 TSv=0
27	2.992274	127.0.0.1	127.0.0.1	SSLv3	220	Server Hello, Change Cipher Spec, Finished
28	2.992312	127.0.0.1	127.0.0.1	TCP	66	38714 → 443 [ACK] Seq=121 Ack=155 Win=32767 Len=0
29	2.992855	127.0.0.1	127.0.0.1	HTTP	562	GET /icons/debian/openlogo-25.jpg HTTP/1.1
30	2.993501	127.0.0.1	127.0.0.1	HTTP	596	HTTP/1.1 404 Not Found (text/html)
31	2.993840	127.0.0.1	127.0.0.1	HTTP	471	GET /icons/apache_pb.png HTTP/1.1
32	2.994179	127.0.0.1	127.0.0.1	HTTP	1828	HTTP/1.1 200 OK (PNG)
33	3.004256	127.0.0.1	127.0.0.1	TCP	66	443 → 38713 [ACK] Seq=7845 Ack=1548 Win=32767 Len=0
34	3.033250	127.0.0.1	127.0.0.1	TCP	66	38714 → 443 [ACK] Seq=1022 Ack=2447 Win=32767 Len=0
35	3.501643	127.0.0.1	127.0.0.1	HTTP	588	HTTP/1.1 404 Not Found (text/html)
36	3.507001	127.0.0.1	127.0.0.1	HTTP	439	GET /favicon.ico HTTP/1.1
37	3.507541	127.0.0.1	127.0.0.1	HTTP	580	HTTP/1.1 404 Not Found (text/html)
38	3.507555	127.0.0.1	127.0.0.1	TCP	66	38714 → 443 [ACK] Seq=1395 Ack=2961 Win=32767 Len=0
39	3.541174	127.0.0.1	127.0.0.1	TCP	66	38713 → 443 [ACK] Seq=1548 Ack=8367 Win=32767 Len=0
40	6.037880	127.0.0.1	127.0.0.1	HTTP	511	GET /test HTTP/1.1
41	6.037932	127.0.0.1	127.0.0.1	TCP	66	443 → 38713 [ACK] Seq=8367 Ack=1993 Win=32767 Len=0
42	6.041185	127.0.0.1	127.0.0.1	HTTP	644	HTTP/1.1 301 Moved Permanently (text/html)
43	6.041367	127.0.0.1	127.0.0.1	TCP	66	38713 → 443 [ACK] Seq=1993 Ack=8945 Win=32767 Len=0
44	6.088943	127.0.0.1	127.0.0.1	HTTP	511	GET /test/ HTTP/1.1
45	6.110160	127.0.0.1	127.0.0.1	HTTP	468	HTTP/1.1 200 OK (text/html)
46	6.110895	127.0.0.1	127.0.0.1	TCP	66	38714 → 443 [ACK] Seq=1404 Ack=3363 Win=32767 Len=0

Accept-Language: fr,fr-fr;q=0.8,en-us;q=0.5,en;q=0.3\r\n  
 Accept-Encoding: gzip,deflate\r\n  
 Accept-Charset: ISO-8859-1,utf-8;q=0.7,\*;q=0.7\r\n  
 Keep-Alive: 300\r\n  
 Connection: keep-alive\r\n  
 Referer: https://localhost/\r\n  
 \r\n  
 [Response in frame: 32]  
 [Full request URI: https://localhost/icons/apache\_pb.png]

0000 47 45 54 20 2f 6e 73 2f 62 61 63 66 72 74 3a 20 6f 63 61 6c 68 6f 73 74 0d 0a 0000 65 5f 70 62 2e 73 65 72 2d 41 67 65 66 74 3a 20 4d 6f 7a 0d 0000 73 74 3a 20 6f 63 61 6c 68 6f 73 74 0d 0a 0000 6c 61 2f 35 2e 30 20 28 5b 31 31 30 20 55 5d 0000 4c 69 6e 75 78 20 69 36 38 3e 3b 20 66 72 31 0000 72 76 3a 31 2a 38 2a 30 2e 32 29 20 47 65 66 6f 72 31 1a 1b 1c 1d 1e 1f 10 11 12 13 14 15 16 17 18 19 20 69 72 7d

Packet (474 bytes) Decoded (474 bytes) Decoded (474 bytes)

Looking at the data stream what is the full request URI for packet 50?

<https://localhost/icons/back.gif>

Apply a display filter ... <Ctrl-/>

No.	Time	Source	Destination	Protocol	Length	Info
29	2.992855	127.0.0.1	127.0.0.1	HTTP	562	GET /icons/debian/openlogo-25.jpg HTTP/1.1
30	2.993501	127.0.0.1	127.0.0.1	HTTP	596	HTTP/1.1 404 Not Found (text/html)
31	2.993840	127.0.0.1	127.0.0.1	HTTP	471	GET /icons/apache_pb.png HTTP/1.1
32	2.994179	127.0.0.1	127.0.0.1	HTTP	1828	HTTP/1.1 200 OK (PNG)
33	3.004256	127.0.0.1	127.0.0.1	TCP	66	443 → 38713 [ACK] Seq=7845 Ack=1548 Win=32767 Len=0
34	3.033250	127.0.0.1	127.0.0.1	TCP	66	38714 → 443 [ACK] Seq=1022 Ack=2447 Win=32767 Len=0
35	3.501643	127.0.0.1	127.0.0.1	HTTP	588	HTTP/1.1 404 Not Found (text/html)
36	3.507001	127.0.0.1	127.0.0.1	HTTP	439	GET /favicon.ico HTTP/1.1
37	3.507541	127.0.0.1	127.0.0.1	HTTP	580	HTTP/1.1 404 Not Found (text/html)
38	3.507555	127.0.0.1	127.0.0.1	TCP	66	38714 → 443 [ACK] Seq=1395 Ack=2961 Win=32767 Len=0
39	3.541174	127.0.0.1	127.0.0.1	TCP	66	38713 → 443 [ACK] Seq=1548 Ack=8367 Win=32767 Len=0
40	6.037880	127.0.0.1	127.0.0.1	HTTP	511	GET /test HTTP/1.1
41	6.037932	127.0.0.1	127.0.0.1	TCP	66	443 → 38713 [ACK] Seq=8367 Ack=1993 Win=32767 Len=0
42	6.041185	127.0.0.1	127.0.0.1	HTTP	644	HTTP/1.1 301 Moved Permanently (text/html)
43	6.041367	127.0.0.1	127.0.0.1	TCP	66	38713 → 443 [ACK] Seq=1993 Ack=8945 Win=32767 Len=0
44	6.088943	127.0.0.1	127.0.0.1	HTTP	511	GET /test/ HTTP/1.1
45	6.110160	127.0.0.1	127.0.0.1	HTTP	468	HTTP/1.1 200 OK (text/html)
46	6.110895	127.0.0.1	127.0.0.1	TCP	66	38714 → 443 [ACK] Seq=1404 Ack=3363 Win=32767 Len=0
47	9.232586	127.0.0.1	127.0.0.1	HTTP	511	GET /test2/ HTTP/1.1
48	9.235911	127.0.0.1	127.0.0.1	HTTP	836	HTTP/1.1 200 OK (text/html)
49	9.245287	127.0.0.1	127.0.0.1	TCP	66	38713 → 443 [ACK] Seq=8367 Ack=1993 Win=32767 Len=0
50	9.313527	127.0.0.1	127.0.0.1	HTTP	479	GET /icons/back.gif HTTP/1.1
51	9.323495	127.0.0.1	127.0.0.1	HTTP	479	GET /icons/back.gif HTTP/1.1
52	9.327622	127.0.0.1	127.0.0.1	HTTP	652	HTTP/1.1 200 OK (GIF)
53	9.337310	127.0.0.1	127.0.0.1	TCP	66	38713 → 443 [ACK] Seq=8367 Ack=1993 Win=32767 Len=0
54	9.327845	127.0.0.1	127.0.0.1	HTTP	588	HTTP/1.1 200 OK (GIF)
55	9.337410	127.0.0.1	127.0.0.1	TCP	66	38714 → 443 [ACK] Seq=1404 Ack=3363 Win=32767 Len=0
56	12.356587	127.0.0.1	127.0.0.1	HTTP	511	GET /test3/ HTTP/1.1
57	12.368244	127.0.0.1	127.0.0.1	HTTP	580	HTTP/1.1 404 Not Found (text/html)
58	12.368427	127.0.0.1	127.0.0.1	TCP	66	38713 → 443 [ACK] Seq=8367 Ack=1993 Win=32767 Len=0

Accept-Language: fr,fr-fr;q=0.8,en-us;q=0.5,en;q=0.3\r\n  
 Accept-Encoding: gzip,deflate\r\n  
 Accept-Charset: ISO-8859-1,utf-8;q=0.7,\*;q=0.7\r\n  
 Keep-Alive: 300\r\n  
 Connection: keep-alive\r\n  
 Referer: https://localhost/test2/\r\n  
 \r\n  
 [Response in frame: 52]  
 [Full request URI: https://localhost/icons/back.gif]

0000 47 45 54 20 2f 6e 73 2f 62 61 63 66 72 74 3a 20 6f 63 61 6c 68 6f 73 74 0d 0a 0000 65 5f 70 62 2e 73 65 72 2d 41 67 65 66 74 3a 20 4d 6f 7a 0d 0000 73 74 3a 20 6f 63 61 6c 68 6f 73 74 0d 0a 0000 6c 61 2f 35 2e 30 20 28 5b 31 31 30 20 55 5d 0000 4c 69 6e 75 78 20 69 36 38 3e 3b 20 66 72 31 0000 72 76 3a 31 2a 38 2a 30 2e 32 29 20 47 65 66 6f 72 31 1a 1b 1c 1d 1e 1f 10 11 12 13 14 15 16 17 18 19 20 69 72 7d

Packet (479 bytes) Decoded (479 bytes) Decoded (479 bytes)

## What is the User-Agent listed in packet 50?

No.	Time	Source	Destination	Protocol	Length	Info
29	2.992855	127.0.0.1	127.0.0.1	HTTP	562	GET /icons/debian/ope
30	2.993501	127.0.0.1	127.0.0.1	HTTP	596	HTTP/1.1 404 Not Four
31	2.993840	127.0.0.1	127.0.0.1	HTTP	471	GET /icons/apache_pb.
32	2.994179	127.0.0.1	127.0.0.1	HTTP	1828	HTTP/1.1 200 OK (PNG
33	3.004256	127.0.0.1	127.0.0.1	TCP	66	443 → 38713 [ACK] Seq
34	3.033250	127.0.0.1	127.0.0.1	TCP	66	38714 → 443 [ACK] Seq
35	3.501643	127.0.0.1	127.0.0.1	HTTP	588	HTTP/1.1 404 Not Four
36	3.507001	127.0.0.1	127.0.0.1	HTTP	439	GET /favicon.ico HTTP
37	3.507541	127.0.0.1	127.0.0.1	HTTP	580	HTTP/1.1 404 Not Four
38	3.507555	127.0.0.1	127.0.0.1	TCP	66	38714 → 443 [ACK] Seq
39	3.541174	127.0.0.1	127.0.0.1	TCP	66	38713 → 443 [ACK] Seq
40	6.037880	127.0.0.1	127.0.0.1	HTTP	511	GET /test HTTP/1.1
41	6.037932	127.0.0.1	127.0.0.1	TCP	66	443 → 38713 [ACK] Seq
42	6.041185	127.0.0.1	127.0.0.1	HTTP	644	HTTP/1.1 301 Moved Pe
43	6.041367	127.0.0.1	127.0.0.1	TCP	66	38713 → 443 [ACK] Seq
44	6.088943	127.0.0.1	127.0.0.1	HTTP	511	GET /test/ HTTP/1.1
45	6.110160	127.0.0.1	127.0.0.1	HTTP	468	HTTP/1.1 200 OK (tex
46	6.119895	127.0.0.1	127.0.0.1	TCP	66	38714 → 443 [ACK] Seq
47	9.232586	127.0.0.1	127.0.0.1	HTTP	511	GET /test2/ HTTP/1.1
48	9.235911	127.0.0.1	127.0.0.1	HTTP	836	HTTP/1.1 200 OK (tex
49	9.245287	127.0.0.1	127.0.0.1	TCP	66	38713 → 443 [ACK] Seq
50	9.318572	127.0.0.1	127.0.0.1	HTTP	479	GET /icons/back.gif H
51	9.323495	127.0.0.1	127.0.0.1	HTTP	479	GET /icons/blank.gif
52	9.327622	127.0.0.1	127.0.0.1	HTTP	652	HTTP/1.1 200 OK (GIF
53	9.337310	127.0.0.1	127.0.0.1	TCP	66	38713 → 443 [ACK] Seq
54	9.327845	127.0.0.1	127.0.0.1	HTTP	588	HTTP/1.1 200 OK (GIF
55	9.337410	127.0.0.1	127.0.0.1	TCP	66	38714 → 443 [ACK] Seq
56	12.356587	127.0.0.1	127.0.0.1	HTTP	511	GET /test3/ HTTP/1.1
57	12.368244	127.0.0.1	127.0.0.1	HTTP	580	HTTP/1.1 404 Not Four
58	12.368427	127.0.0.1	127.0.0.1	TCP	66	38713 → 443 [ACK] Seq


cept-Language: fr,fr-fr;q=0.8,en-us;q=0.5,en;q=0.3\r\n	0000	47 45 54 20 2f 69 63 6f 6e 73 2f 62 61 63 6
cept-Encoding: gzip,deflate\r\n	0010	67 69 66 20 48 54 54 50 2f 31 2e 31 0d 0a 4
cept-Charset: ISO-8859-1,utf-8;q=0.7,*;q=0.7\r\n	0020	73 74 3a 20 6c 6f 63 61 6c 68 6f 73 74 0d 0
p-Alive: 300\r\n	0030	73 65 72 2d 41 67 65 6e 74 3a 20 4d 6f 7a 6
nection: keep-alive\r\n	0040	6c 61 2f 35 2e 30 20 28 58 31 31 3b 20 55 3
erer: https://localhost/test2/\r\n	0050	4c 69 6e 75 78 20 69 36 38 36 3b 20 66 72 3
n	0060	72 76 3a 31 2e 38 2e 30 2e 32 29 20 47 65 6
sponse in frame: 52]	0070	6f 2f 32 30 30 36 30 33 30 38 20 46 69 72 6

Packet (479 bytes) Decrypted TLS (380 bytes)

final:

### Share your win with your peers

Your progress can inspire others in your community.

**Wireshark 101 completed!**

Ezz1eru completed another room on their cyber security journey.

Completed tasks

14

Points earned

160

Streak

1

Share on social media

[in LinkedIn](#) [WhatsApp](#) [Telegram](#) [Twitter / X](#) [Facebook](#) [Reddit](#)

Go to dashboard →