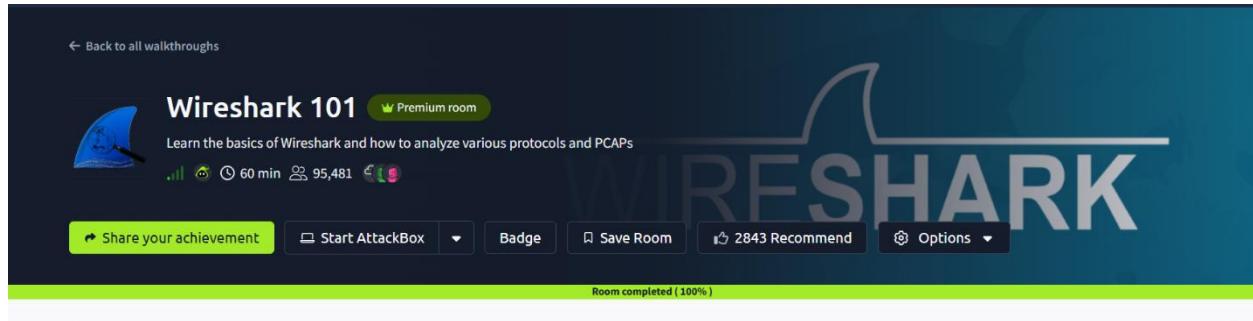


wireshark101



ARP Overview

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:

- Request (1)
 - Reply (2)

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

No.	Time	Source	Destination	Protocol	Length Info
1	0.000000	0.0.0.0	255.255.255.255	DHCP	445 DHCP Discover - Transaction ID 0x6f5114eb
2	0.03255	0.0.0.0	255.255.255.255	DHCP	445 DHCP Discover - Transaction ID 0x6f5114eb
3	0.06239	0.0.0.0	255.255.255.255	DHCP	445 DHCP Discover - Transaction ID 0x6f5114eb
4	14.601385	Sfr_18:c2:73	Broadcast	PPPoED	82 Active Discovery Initiation (PADT)
5	14.60175	Sfr_18:c2:73	Broadcast	PPPoED	82 Active Discovery Initiation (PADT)
6	23.595917	HuaweiTechno_f0:45.. Sfr_e3:c3:31	ARP	60 Who has 10.251.196.227? Tell 10.251.196.1	
7	23.595953	HuaweiTechno_f0:45.. Sfr_60:d2:11	ARP	60 Who has 10.194.144.144? Tell 10.194.144.1	
8	24.651131	Sfr_18:c2:73	Broadcast	PPPoED	82 Active Discovery Initiation (PADT)
9	29.254207	0.0.0.0	255.255.255.255	DHCP	445 DHCP Discover - Transaction ID 0x656db7d
10	29.811743	Sfr_18:c2:73	Broadcast	PPPoED	82 Active Discovery Initiation (PADT)
11	32.257198	0.0.0.0	255.255.255.255	DHCP	445 DHCP Discover - Transaction ID 0x656db7d
12	32.771702	HuaweiTechno_f0:45.. Sfr_49:6d:f9	ARP	60 Who has 10.194.144.84? Tell 10.194.144.1	
13	32.772685	HuaweiTechno_f0:45.. MS-NLB-PhyServer-3.. ARP	ARP	60 Who has 10.194.144.147? Tell 10.194.144.1	
14	32.774163	HuaweiTechno_f0:45.. SagemcomBrosa_17:e0.. ARP	ARP	60 Who has 10.251.196.162? Tell 10.251.196.1	
15	34.816127	Sfr_18:c2:73	Broadcast	PPPoED	82 Active Discovery Initiation (PADT)
16	35.260227	0.0.0.0	255.255.255.255	DHCP	445 DHCP Discover - Transaction ID 0x656db7d
17	37.765789	HuaweiTechno_f0:45.. Sfr_72:0a:d9	ARP	60 Who has 10.251.196.132? Tell 10.251.196.1	
18	37.767245	HuaweiTechno_f0:45.. Sfr_97:24:91	ARP	60 Who has 10.251.196.106? Tell 10.251.196.1	
19	37.768724	HuaweiTechno_f0:45.. Sfr_88:e7:a1	ARP	60 Who has 10.251.196.74? Tell 10.251.196.1	
20	39.821132	Sfr_18:c2:73	Broadcast	PPPoED	82 Active Discovery Initiation (PADT)
21	39.874293	Sfr_61:00:00	Sfr_18:c2:73	PPPoED	64 Active Discovery Offer (PAOD) AC-Name='SE100-CRL1-1'
22	39.874692	Sfr_18:c2:73	Sfr_61:00:00	PPPoED	64 Active Discovery Request (PAOR)
23	39.875775	Ericsson_03:a4:3b	Sfr_18:c2:73	PPPoED	64 Active Discovery Offer (PAOD) AC-Name='SE100-CRL1-1'
24	40.024585	Sfr_61:00:00	Sfr_18:c2:73	PPPoED	64 Active Discovery Session-confirmation (PADS) AC-Name='SE100-CRL1-1'
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	36 Echo Request
30	40.094086	Sfr_61:00:00	Sfr_18:c2:73	PPP CH..	60 Challenge (NAME='SE100-CRL1-1', VALUE=0xb4e9e3423c7f0ff2a055b7519ab8c242)
31	40.094166	Sfr_18:c2:73	Sfr_61:00:00	PPP CH..	60 Challenge (NAME='SE100-CRL1-1', VALUE=0xb4e9e3423c7f0ff2a055b7519ab8c242)
Padding: 000000					
Trailer: 01bbae00000000000000000000000000c					
Address Resolution Protocol (request)					
Hardware type: Ethernet (1)					
Protocol type: IPv4 (0x0800)					
Hardware size: 6					
Protocol size: 4					
Opcode: request (1)					
Sender MAC address: HuaweiTechno_f0:45:d7 (80:fb:06:f0:45:d7)					
Sender IP address: 10.251.196.1					

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:...	SagemcomBrod..._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 10.251.196.16
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 Offer
22	39.874692	Sfr_18:c2:73	Sfr_61:00:00	PPPoED	82	Active Discovery Request
23	39.875775	Ericsson_03:a4:3b	Sfr_18:c2:73	PPPoED	64	Active Discovery Offer
24	40.024585	Sfr_61:00:00	Sfr_18:c2:73	PPPoED	64	Active Discovery Session
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='SE10')
31	40.094268	Sfr_18:c2:73	Sfr_61:00:00	PPP CH...	63	Response (NAME='E0A1D')
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)
:ess: HuaweiTechno_f0:45:d7 (80:fb:06:f0:45:d7)
:ess: 10.251.196.1
:ess: 00:00:00_00:00:00 (00:00:00:00:00:00)
:ess: 10.251.196.74

```

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

nb6-startup_1602384431514.pcap

No.	Time	Source	Destination	Protocol	Length	Info
76	61.8...2014	HuaweiTechno_f0:45:...	Sfr_18:c2:72	ARP	60	10.251.23.1 is at 80:fb:0
400	1388651131.6...	HuaweiTechno_f0:45:...	Sfr_18:c2:72	ARP	60	10.251.23.1 is at 80:fb:0
459	1388651198.7...	HuaweiTechno_f0:45:...	Sfr_18:c2:72	ARP	60	10.251.23.1 is at 80:fb:0
520	1388651266.9...	HuaweiTechno_f0:45:...	Sfr_18:c2:72	ARP	60	10.251.23.1 is at 80:fb:0

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:...	SagemcomBrod...	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 10.251.196.18
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:...	SagemcomBrod...	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:...	SagemcomBrod...	ARP	60	Who has 10.251.196.53
49	52.781789	HuaweiTechno_f0:45:...	SagemcomBrod...	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:
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 /cfgnb6dsgeneral
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?

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: 8.8.8.8 (08:00:22:08:00:45)
Internet Protocol Version 4, Src: 192.168.43.9, Dst: 8.8.8.8
Internet Control Message Protocol
Type: Echo (ping) request (8)
Code: 0
Checksum: 0xbbbb [correct]
[Checksum Status: Good]
Identifier (BE): 55099 (0xd73b)
Identifier (LE): 15319 (0x3bd7)

```

0000 02 1a 11 f0 c8 3b 60 33 4b 13 c5 58 08 00 45
0010 00 54 26 ef 00 00 40 01 57 f9 c0 a8 2b 09 08
0020 08 08 08 00 bb b3 d7 3b 00 00 51 a7 d6 7d 00
0030 51 e4 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 type for packet 5?

3 5.006792	192.168.43.1	192.168.43.9	DNS	124 Standard query respon	
→ 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 respon	
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 respon	
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 respon	
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 respon	
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 c0
└─ Internet Control Message Protocol
    Type: Echo (ping) reply (0)
    Code: 0
    Checksum: 0xc3b3 [correct]
    [Checksum Status: Good]
    Identifier (BE): 55099 (0xd73b)
    Identifier (LE): 15319 (0x3bd7)
    0020 2b 09 00 00 c3 b3 d7 3b 00 00 51 a7 d6 7d 00
    0030 51 e4 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 timestamp for packet 12, only including month day and year? May 30, 2013

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

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 ms]

Data (48 bytes)

What is the full data string for packet 18?

08090a0b0c0d0e0f101112131415161718191a1b1c1d1e1f202122232425262728

292a2b2c2d2e2f3031323334353637

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	124 Standard query response 0x528e PTR 8.8.8.8.in-addr.arpa PTR google-public-dns-a.google.com
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=40 (request in 4)
6	6.012920	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=40 (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=40 (request in 8)
10	7.791410	192.168.43.9	192.168.43.1	DNS	80 Standard query 0x695d PTR 4.4.8.8.in-addr.arpa
11	7.979359	192.168.43.1	192.168.43.9	DNS	124 Standard query response 0x695d 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=0xd3b, 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=0xd3b, seq=1/256, ttl=40 (reply in 14)
14	9.323049	8.8.4.4	192.168.43.9	ICMP	98 Echo (ping) reply id=0xd3b, seq=1/256, ttl=40 (request in 13)
15	9.985425	192.168.43.9	8.8.4.4	ICMP	98 Echo (ping) request id=0xd3b, 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	12.078588	192.168.43.9	4.2.2.2	ICMP	98 Echo (ping) request id=0xd3b, seq=0/0, ttl=64 (reply in 19)
→	19	12.148722	4.2.2.2	ICMP	98 Echo (ping) reply id=0xd3b, seq=0/0, ttl=50 (request in 18)
20	13.079308	192.168.43.9	4.2.2.2	ICMP	98 Echo (ping) request id=0xd3b, 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=0xd3b, seq=1/256, ttl=50 (request in 20)
22	14.079860	192.168.43.9	4.2.2.2	ICMP	98 Echo (ping) request id=0xd3b, seq=2/512, ttl=64 (reply in 23)
23	15.208499	4.2.2.2	192.168.43.9	ICMP	98 Echo (ping) reply id=0xd3b, seq=2/512, ttl=50 (request in 22)
24	15.289472	192.168.43.9	192.168.43.1	DNS	77 Standard query 0x121 A www.wireshark.org
25	15.703377	192.168.43.1	192.168.43.9	DNS	93 Standard query response 0x121 A www.wireshark.org A 174.137.42.65
26	15.722009	192.168.43.9	192.168.43.1	DNS	77 Standard query 0x2c50 A www.wireshark.org
27	15.865643	192.168.43.1	192.168.43.9	DNS	93 Standard query response 0x2c50 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	17.040000	174.137.42.65	192.168.43.9	ICMP	98 Echo (ping) reply id=0xe03b, seq=1/256, ttl=48 (request in 30)

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.in-addr.arpa

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

Transaction ID: 0x528e

Flags: 0x0100 Standard query

Questions: 1

Answer RRs: 0

Authority RRs: 0

Additional RRs: 0

Queries

- 8.8.8.in-addr.arpa: type PTR, class IN

Name: 8.8.8.in-addr.arpa

```

0000 02 1a 11 f0 c8 3b 60 33 4b 13 c5 58 08 00 45
0010 00 42 81 bf 00 00 40 11 21 91 c0 a8 2b 09 c0
0020 2b 01 c9 dd 00 35 00 2e f2 68 52 8e 01 00 00
0030 00 00 00 00 00 01 38 01 38 01 38 01 38 07
0040 6e 2d 61 64 64 72 04 61 72 70 61 00 00 0c 00

```

What site is being queried in packet 26? www.wireshark.org

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

```

Transaction ID: 0x2c58
Flags: 0x0100 Standard query
Questions: 1
Answer RRs: 0
Authority RRs: 0
Additional RRs: 0
Queries
  www.wireshark.org: type A, class IN
    Name: www.wireshark.org
  
```

0000	02	1a	11	f0	c8	3b	60	33	4b	13	c5	58	08	00	45
0010	00	3f	64	e7	00	00	ff	11	7f	6b	c0	a8	2b	09	c0
0020	2b	01	d5	63	00	35	00	2b	7f	5c	2c	58	01	00	00
0030	00	00	00	00	00	00	03	77	77	77	09	77	69	72	65
0040	68	61	72	6b	03	6f	72	67	00	00	01	00	01	00	01

What is the Transaction ID for packet 26? 0x2c58

NetworkMiner Screenshot showing network traffic analysis.

The table displays network traffic details:

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

Selected packet details:

- 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

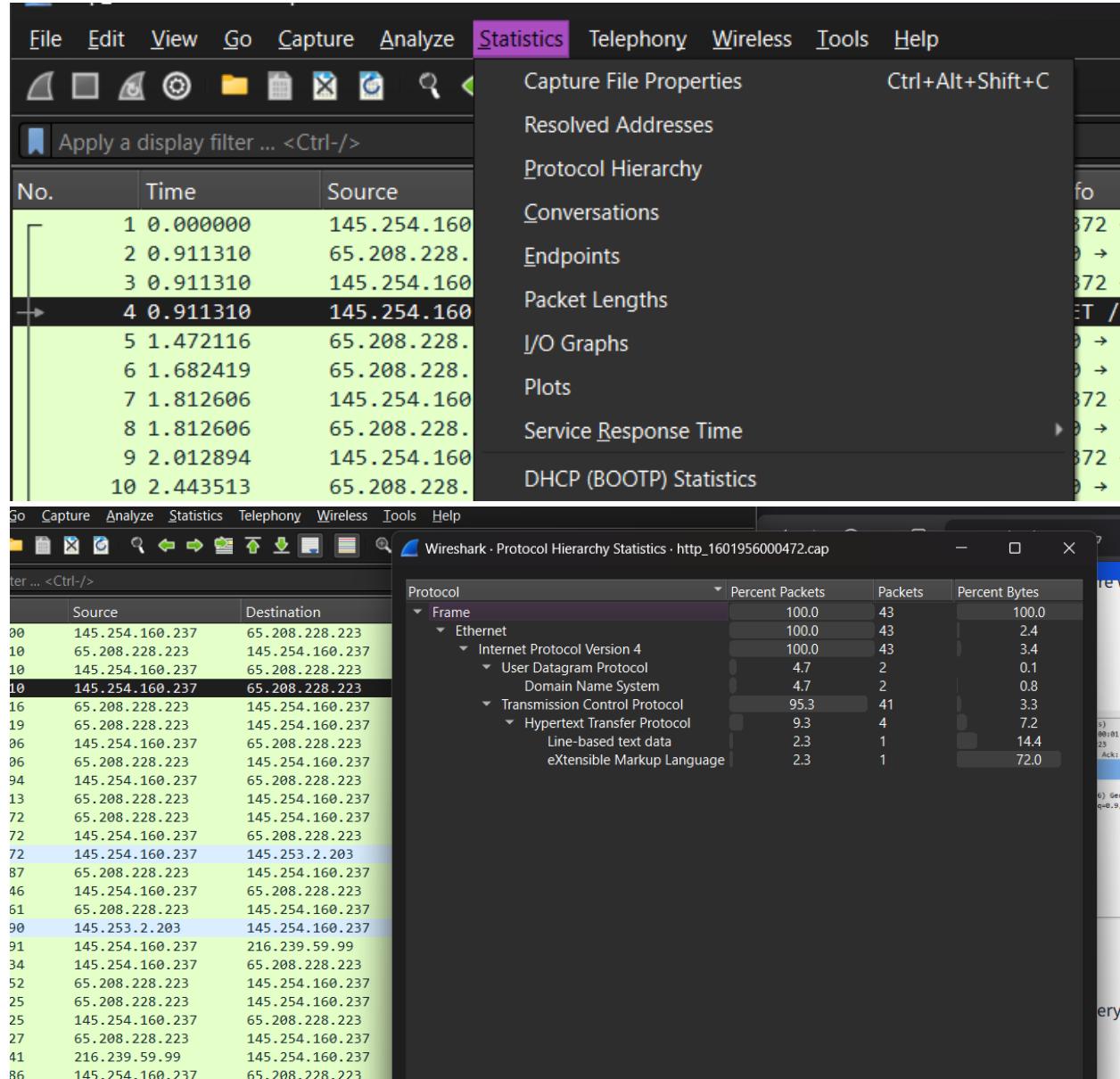
Hex dump of the selected DNS packet:

0000	02 1a 11 f0 c8 3b 60 33 4b 13 c5 58 08 00 40
0010	00 3f 64 e7 00 00 ff 11 7f 6b c0 a8 2b 09 d0
0020	2b 01 d5 63 00 35 00 2b 7f 5c 2c 58 01 00 00
0030	00 00 00 00 00 00 03 77 77 77 09 77 69 72 60
0040	68 61 72 6b 03 6f 72 67 00 00 01 00 01 00 01

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



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&lmt=1082467020&format=468x60_as&output=html&url=http://www.ether.eal.com/.download.html&.color_bg=F_FFFF&color_tx=t=333333&color_li=nk=000000&color_u=rl=666633&color_border=666633

No.	Time	Source	Destination	Protocol	Length Info
1	0.000000	145.254.160.237	65.208.228.223	TCP	62 3372 → 88 [SYN] Seq=0 Win=8760 Len=0 MSS=1460 SACK_PERM
2	0.911310	65.208.228.223	145.254.160.237	TCP	62 88 → 3372 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1380 SACK_PERM
3	0.911310	145.254.160.237	65.208.228.223	TCP	54 3372 → 88 [ACK] Seq=1 Ack=1 Win=9660 Len=0
4	0.911310	145.254.160.237	65.208.228.223	HTTP	533 GET /download.html HTTP/1.1
5	1.472116	65.208.228.223	145.254.160.237	TCP	54 88 → 3372 [ACK] Seq=1 Ack=480 Win=6432 Len=1380
6	1.682419	65.208.228.223	145.254.160.237	TCP	1434 88 → 3372 [ACK] Seq=1 Ack=480 Win=6432 Len=1380 [TCP PDU reassembled in 38]
7	1.812606	145.254.160.237	65.208.228.223	TCP	54 3372 → 88 [ACK] Seq=480 Ack=1381 Win=9660 Len=0
8	1.812606	65.208.228.223	145.254.160.237	TCP	1434 88 → 3372 [ACK] Seq=1381 Ack=480 Win=6432 Len=1380 [TCP PDU reassembled in 38]
9	2.012894	145.254.160.237	65.208.228.223	TCP	54 3372 → 88 [ACK] Seq=480 Ack=2761 Win=9660 Len=0
10	2.012894	65.208.228.223	145.254.160.237	TCP	1434 88 → 3372 [ACK] Seq=2761 Ack=480 Win=6432 Len=1380 [TCP PDU reassembled in 38]
12	2.553672	145.254.160.237	65.208.228.223	TCP	54 3372 → 88 [ACK] Seq=480 Ack=5521 Win=9660 Len=0
13	2.553672	145.254.160.237	145.254.160.237	DNS	89 Standard query response 0x0023 A pagead2.googlesyndication.com
14	2.633787	65.208.228.223	145.254.160.237	TCP	1434 88 → 3372 [ACK] Seq=5521 Ack=480 Win=6432 Len=1380 [TCP PDU reassembled in 38]
15	2.814046	145.254.160.237	65.208.228.223	TCP	54 3372 → 88 [ACK] Seq=480 Ack=6901 Win=9660 Len=0
16	2.894161	65.208.228.223	145.254.160.237	TCP	1434 88 → 3372 [ACK] Seq=6901 Ack=480 Win=6432 Len=1380 [TCP PDU reassembled in 38]
17	2.914194	145.254.160.237	145.254.160.237	DNS	188 Standard query response 0x0023 A pagead2.googlesyndication.com CNAME pagead2.google.akadns.net A 216.239.59.99
18	2.984291	145.254.160.237	216.239.59.99	HTTP	775 GET /pagead/ads?client=ca-pub-2309191948673629&random=1084443430285&lmt=1082467020&format=468x60_as&output=html&url=http%3A%2F%2Fpagead2.googlesyndication.com%2Fpagead%2Fads%3Fclient%3Dca-pub-2309191948673629%26random%3D1084443430285%26lmt%3D1082467020%26format%3D468x60_as%26output%3Dhtml%26url%3Dhttp%3A%2F%2Fwww.ether.eal.com%2F%2Fdownload.html
19	3.014334	145.254.160.237	65.208.228.223	TCP	54 3372 → 88 [ACK] Seq=480 Ack=8281 Win=9660 Len=0
20	3.374852	65.208.228.223	145.254.160.237	TCP	1434 88 → 3372 [ACK] Seq=8281 Ack=480 Win=6432 Len=1380 [TCP PDU reassembled in 38]
21	3.495025	65.208.228.223	145.254.160.237	TCP	1434 88 → 3372 [PSH, ACK] Seq=9661 Ack=480 Win=6432 Len=1380 [TCP PDU reassembled in 38]
22	3.495025	145.254.160.237	65.208.228.223	TCP	54 3372 → 88 [ACK] Seq=480 Ack=118041 Win=9660 Len=0
23	3.635227	65.208.228.223	145.254.160.237	TCP	1434 88 → 3372 [ACK] Seq=118041 Ack=480 Win=6432 Len=1380 [TCP PDU reassembled in 38]
24	3.645241	216.239.59.99	145.254.160.237	TCP	54 88 → 3371 [ACK] Seq=480 Ack=722 Win=31460 Len=0
25	3.645241	145.254.160.237	65.208.228.223	TCP	1434 88 → 3371 [ACK] Seq=722 Ack=480 Win=9660 Len=0
26	3.015638	216.239.59.99	145.254.160.237	TCP	1494 89 → 3371 [PSH, ACK] Seq=15221 Ack=8760 Win=9660 Len=0
27	3.955688	216.239.59.99	145.254.160.237	HTTP	214 HTTP/1.1 200 OK (text/html)
28	3.955688	145.254.160.237	216.239.59.99	TCP	54 3371 → 88 [ACK] Seq=722 Ack=1591 Win=8760 Len=0
29	4.105904	65.208.228.223	145.254.160.237	TCP	1434 88 → 3372 [PSH, ACK] Seq=12421 Ack=480 Win=6432 Len=1380 [TCP PDU reassembled in 38]
30	4.215062	145.254.160.237	65.208.228.223	TCP	54 3372 → 88 [ACK] Seq=480 Ack=13801 Win=9660 Len=0
31	4.366705	65.208.228.223	145.254.160.237	TCP	1434 88 → 3372 [ACK] Seq=13801 Ack=480 Win=6432 Len=1380 [TCP PDU reassembled in 38]
					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=0.5\r\nKeep-Alive: 300\r\nConnection: keep-alive\r\nReferer: http://www.etherreal.com/download.html\r\n\r\n[Response in frame: 27]\n[Full request URI :]= http://pagead2.googlesyndication.com/pagead/ads?client=ca-pub-2309191948673629
					0030 22 39 00 64 00 00 47 45 52 20 2f 70 61 67 65 61 *8 d 2e /pagead/ads?client=ca-pub-2309191948673629&random=1084443430285&lmt=1082467020&format=468x60_as&output=html&url=http%3A%2F%2Fpagead2.googlesyndication.com%2Fpagead%2Fads%3Fclient%3Dca-pub-2309191948673629%26random%3D1084443430285%26lmt%3D1082467020%26format%3D468x60_as%26output%3Dhtml%26url%3Dhttp%3A%2F%2Fwww.ether.eal.com%2F%2Fdownload.html\r\n0030 22 39 00 64 73 37 45 60 65 5e 72 34 63 51 2d 1/etherreal.com\r\n0030 70 75 62 2d 32 33 30 39 31 39 11 39 34 38 36 37 pub-2309191948673629krwdom1084443430285\r\n0060 33 36 32 39 26 72 61 6e 64 6f 6d 3d 31 30 38 34 3629krwdom1084443430285\r\n0070 34 34 33 34 33 30 32 38 35 26 6c 6d 74 3d 31 30 443430285\$&lmt=10\r\n0100 38 32 34 36 37 30 32 30 26 66 6f 72 6d 71 74 3d 82467020format=\r\n0090 34 36 38 78 36 30 51 61 73 26 6f 75 74 70 75 74 468x60_a \$output=\r\n0080 3d 68 72 6d 6c 26 75 72 6c 3d 68 74 74 70 25 33 _html&ur=htt\r\n0080 41 25 32 46 25 32 45 77 77 2e 65 74 68 65 72 AX2F2F2Fw.ether\r\n0080 65 61 6c 2e 63 6f 6d 25 32 46 64 6f 77 6e 6c 6f eal.com 2Fdownlo

What domain name was requested from packet 38? www.ethereal.com

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

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

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 response
18	2.984291	145.254.160.237	216.239.59.99	HTTP	775 GET /pagead/ads?client=...
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 (text/html)
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 Retransmition]
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

Content-Type: Keep-Alive\r\nContent-Type: text/html; charset=ISO-8859-1\r\n\r\n<!-- in frame: 4 -->\r\nSince request: 3.935659000 seconds]\r\nURI: /download.html]\r\nRequest URI: http://www.ethereal.com/download.html]\r\nSize: 18070 bytes\r\nMarkup language:

0000	00 00 01 00 00 00 fe ff	20 00 01 00 08 00 4
0010	01 d0 c0 ac 40 00 2f 06	2f e0 41 d0 e4 df 9
0020	a0 ed 00 50 0d 2c 11 4c	a7 a0 38 af ff f3 5
0030	19 20 3d 97 00 00 65 6e	64 20 73 75 70 70 6
0040	74 20 71 75 65 73 74 69	6f 6e 73 20 61 62 6
0050	74 20 45 74 68 65 72 65	61 6c 20 74 6f 20 7
0060	65 0a 20 20 3c 61 20 68	72 65 66 3d 22 6d 6
0070	6c 74 6f 3a 65 74 68 65	72 65 61 6c 2d 75 7

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

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

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 response
•	18 2.984291	145.254.160.237	216.239.59.99	HTTP	775	GET /pagead/ads?client=
•	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=8
•	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 (text/html)
•	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 Retransmission]
•	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/do
File Data: 18070 bytes
eXtensible Markup Language

0000 48 54 54 50 2f 31 2e 31 20 32 30 30 20 4f 4
0010 0a 44 61 74 65 3a 20 54 68 75 2c 20 31 33 2
0020 61 79 20 32 30 30 34 20 31 30 3a 31 37 3a 3
0030 20 47 4d 54 0d 0a 53 65 72 76 65 72 3a 20 4
0040 61 63 68 65 0d 0a 4c 61 73 74 2d 4d 6f 64 6
0050 69 65 64 3a 20 54 75 65 2c 20 32 30 20 41 7
0060 20 32 30 30 34 20 31 33 3a 31 37 3a 30 30 2
0070 4d 54 0d 0a 45 54 61 67 3a 20 22 39 61 30 3

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

HTTPS Traffic Overview

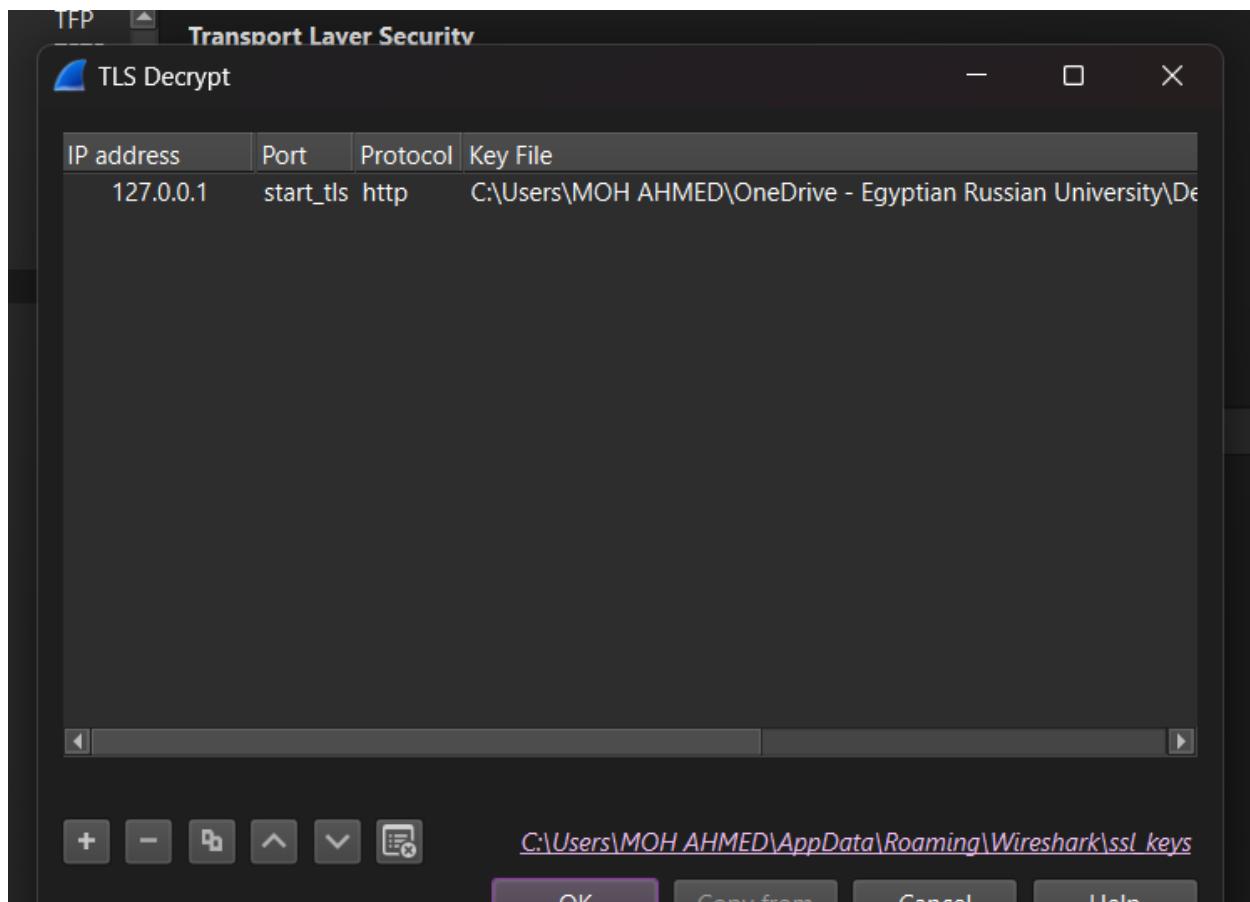
Before sending encrypted information the client and server need to agree upon various steps in order to make a secure tunnel.

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



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 38714 → 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=1
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=1
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 TSV=1
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	6.140005	127.0.0.1	127.0.0.1	TCP	66 38714 → 443 [ACK] Seq=14040 Ack=3262 Win=32767 Len=0
Accept-Language: fr,fr-fr;q=0.8,en-us;q=0.5,en;q=0.3\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: https://localhost/\r\n\r\n[Response in frame: 32]					
[Full request URI: https://localhost/icons/apache_pb.png]					

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

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

Time	Source	Destination	Protocol	Length Info
29.2.992855	127.0.0.1	127.0.0.1	HTTP	562 GET /icons.debian/opk
30.2.993501	127.0.0.1	127.0.0.1	HTTP	596 HTTP/1.1 404 Not Found
31.2.993840	127.0.0.1	127.0.0.1	HTTP	471 GET /icons/apache_pb.png
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)
46.6.140005	127.0.0.1	127.0.0.1	TCP	66 38714 → 443 [ACK] Seq=14040 Ack=3262 Win=32767 Len=0
Accept-Language: fr,fr-fr;q=0.8,en-us;q=0.5,en;q=0.3\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: https://localhost/\r\n\r\n[Response in frame: 32]				
[Full request URI: https://localhost/icons/back.gif]				

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/openbox.png
30	2.993501	127.0.0.1	127.0.0.1	HTTP	596	HTTP/1.1 404 Not Found
31	2.993840	127.0.0.1	127.0.0.1	HTTP	471	GET /icons/apache_pb.gif
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=1
34	3.033250	127.0.0.1	127.0.0.1	TCP	66	38714 → 443 [ACK] Seq=1
35	3.501643	127.0.0.1	127.0.0.1	HTTP	588	HTTP/1.1 404 Not Found
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
38	3.507555	127.0.0.1	127.0.0.1	TCP	66	38714 → 443 [ACK] Seq=1
39	3.541174	127.0.0.1	127.0.0.1	TCP	66	38713 → 443 [ACK] Seq=1
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=1
42	6.041185	127.0.0.1	127.0.0.1	HTTP	644	HTTP/1.1 301 Moved Permanently
43	6.041367	127.0.0.1	127.0.0.1	TCP	66	38713 → 443 [ACK] Seq=1
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	6.119895	127.0.0.1	127.0.0.1	TCP	66	38714 → 443 [ACK] Seq=1
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=1
50	9.318572	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/blank.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=1
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=1
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
58	12.368427	127.0.0.1	127.0.0.1	TCP	66	38713 → 443 [ACK] Seq=1

```
User-Agent: fr,fr-fr;q=0.8,en-us;q=0.5,en;q=0.3  
Accept-Encoding: gzip,deflate\r\nAccept-Charset: ISO-8859-1,utf-8;q=0.7,*;q=0.7\r\nAccept-Alive: 300\r\nConnection: keep-alive\r\nReferer: https://localhost/test2/\r\nContent-Type: application/x-www-form-urlencoded  
Content-Length: 11  
Response in frame: 52]  
Full request URI: https://localhost/icons/back.gif
```

Packet (479 bytes) Decrypted TLS (380 bytes)

final:

