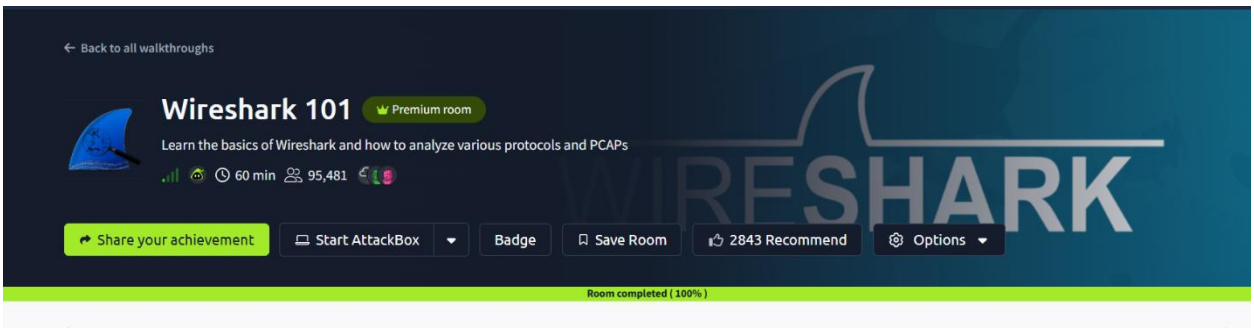
wireshark101

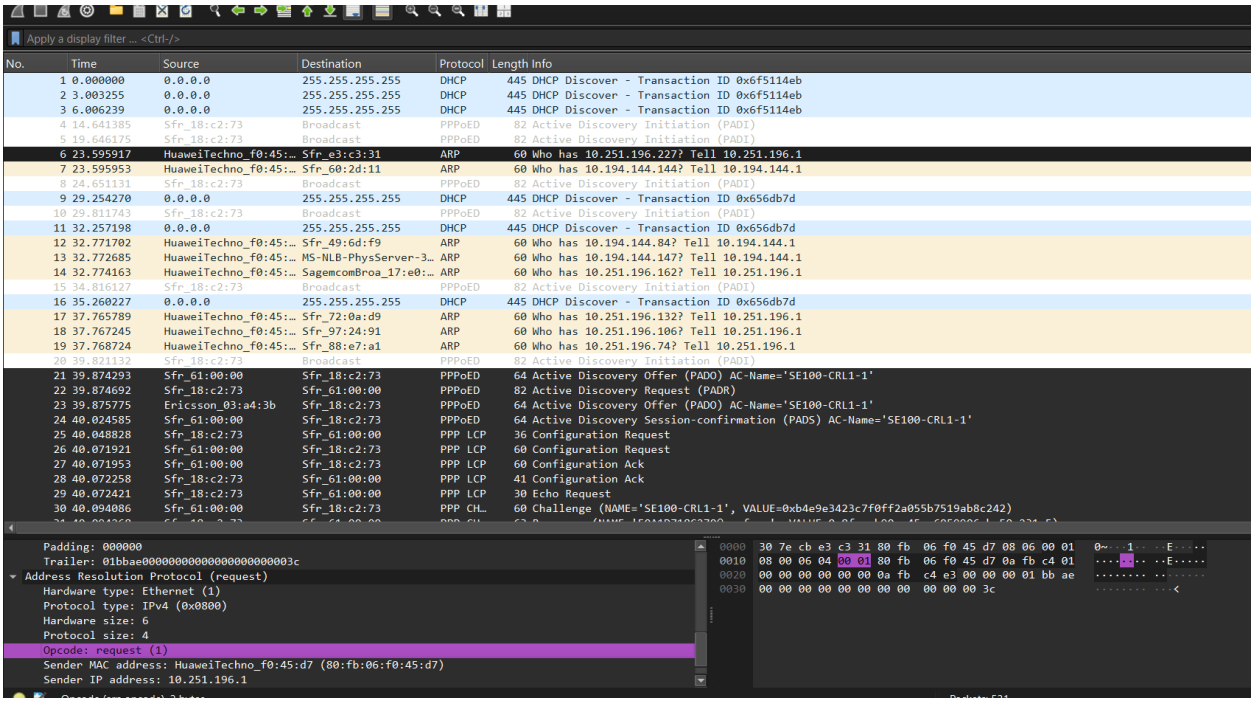


ARP Overview

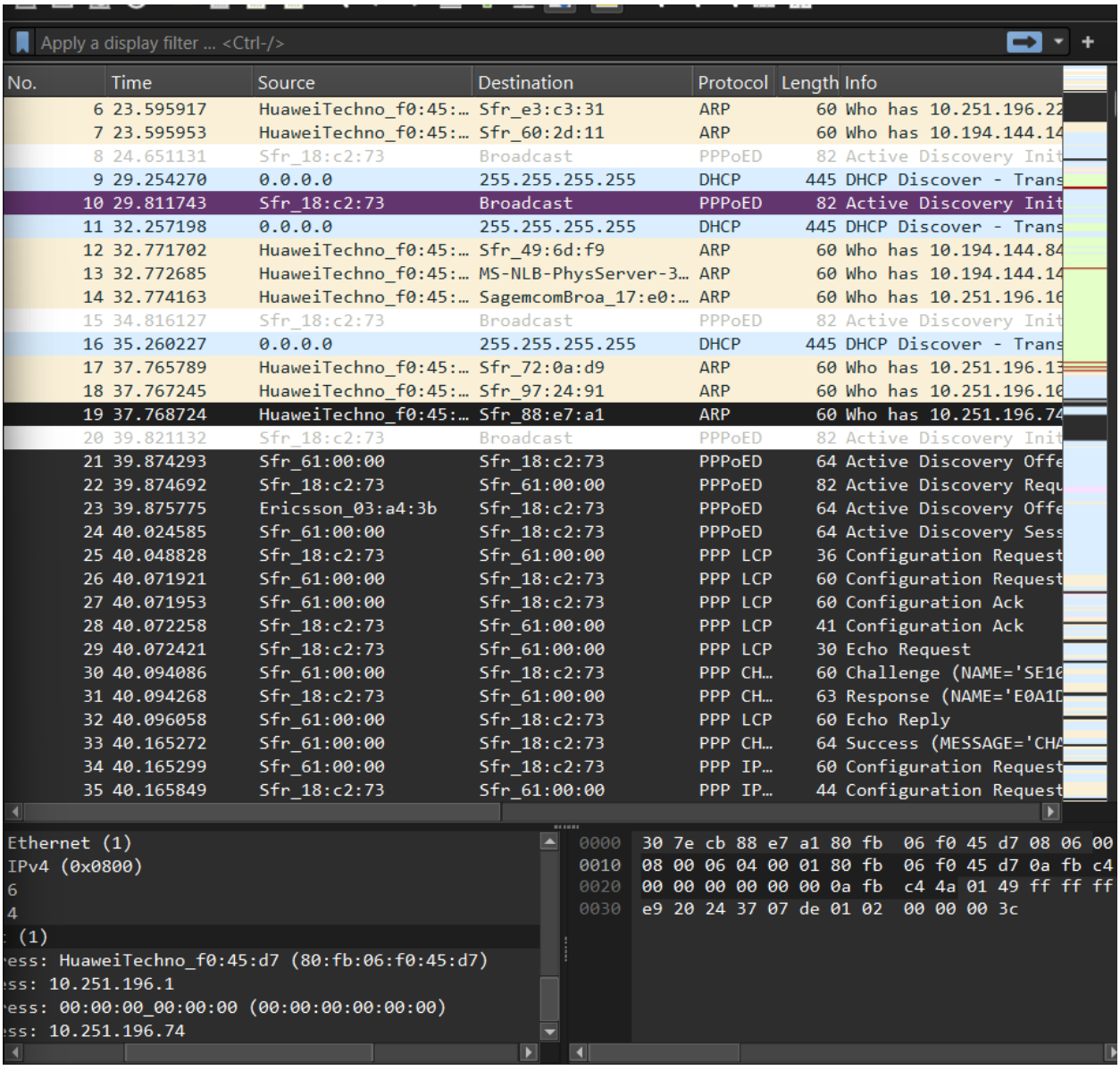
ARP or Address Resolution Protocol is a Layer 2 protocol that is used to connect IP Addresses with MAC Addresses. They will contain REQUEST messages and RESPONSE messages. To identify packets the message header will contain one of two operation codes:

- **Request (1)**
- **Reply (2)**

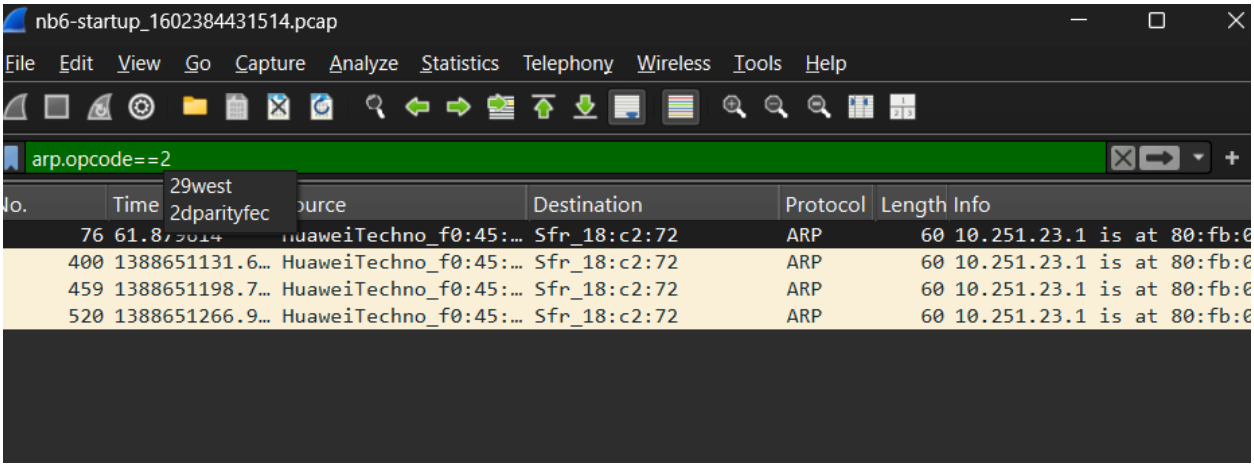
What is the Opcode for Packet 6? Request (1)



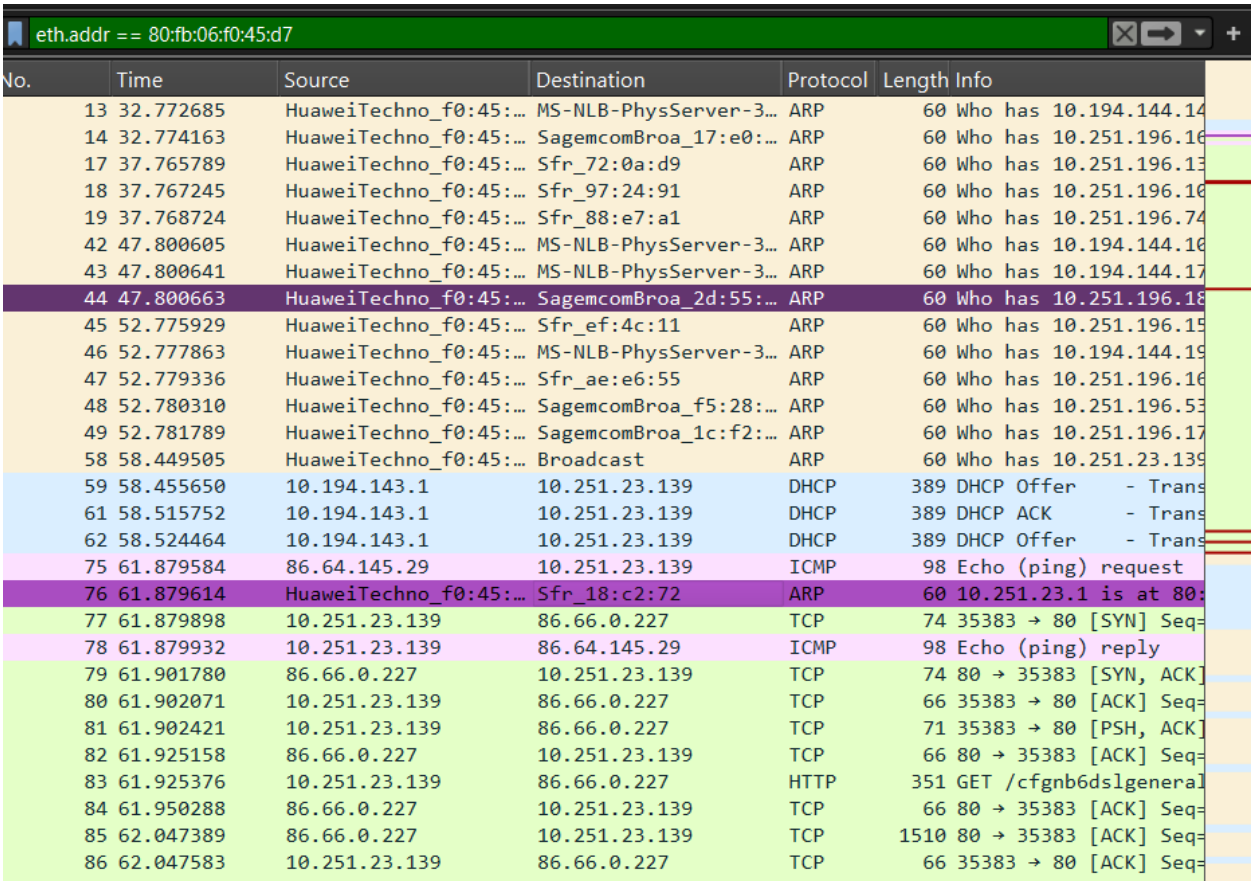
What is the source MAC Address of Packet 19? 80:fb:06:f0:45:d7



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



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



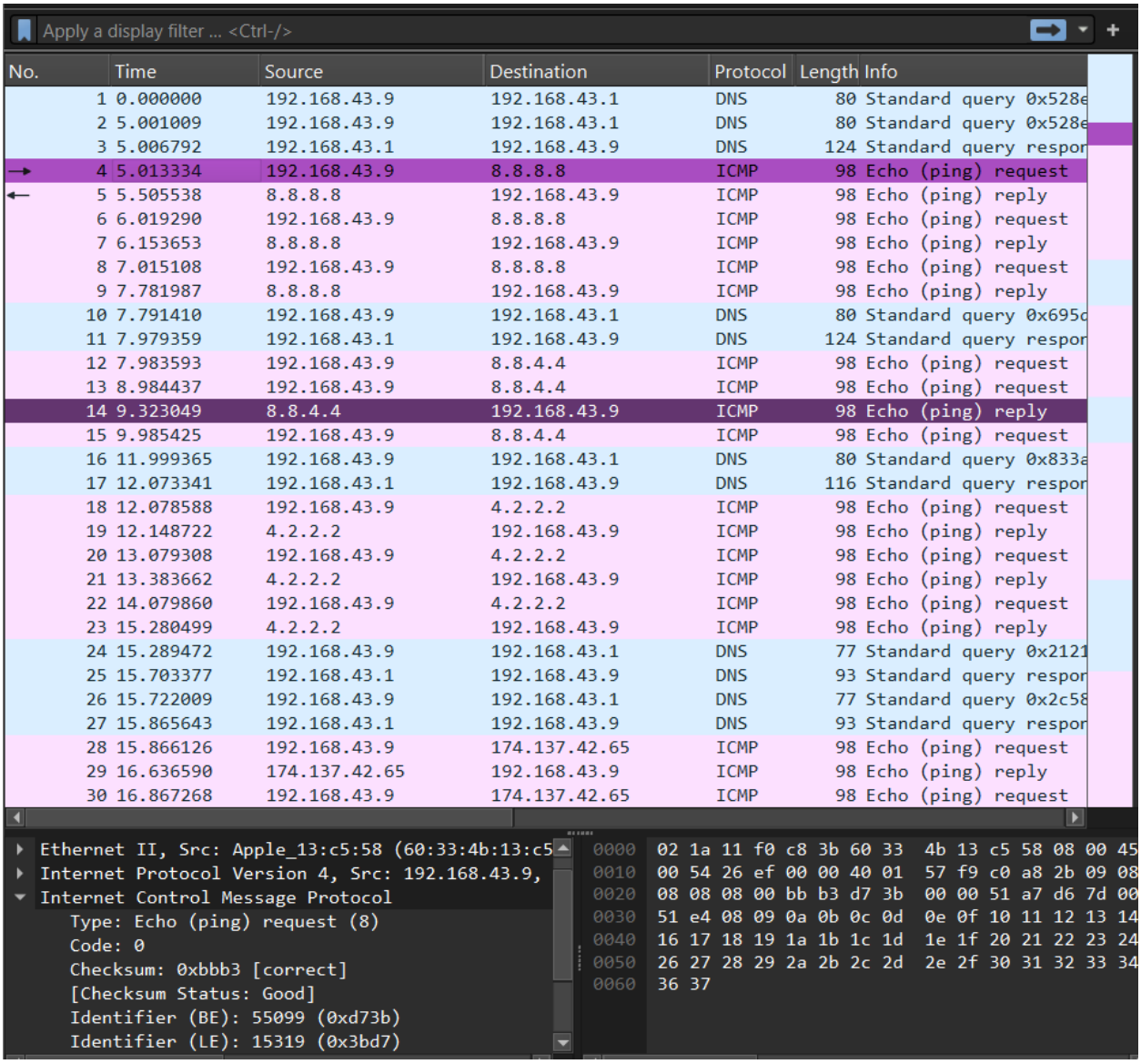
ICMP Traffic Overview

ICMP request:

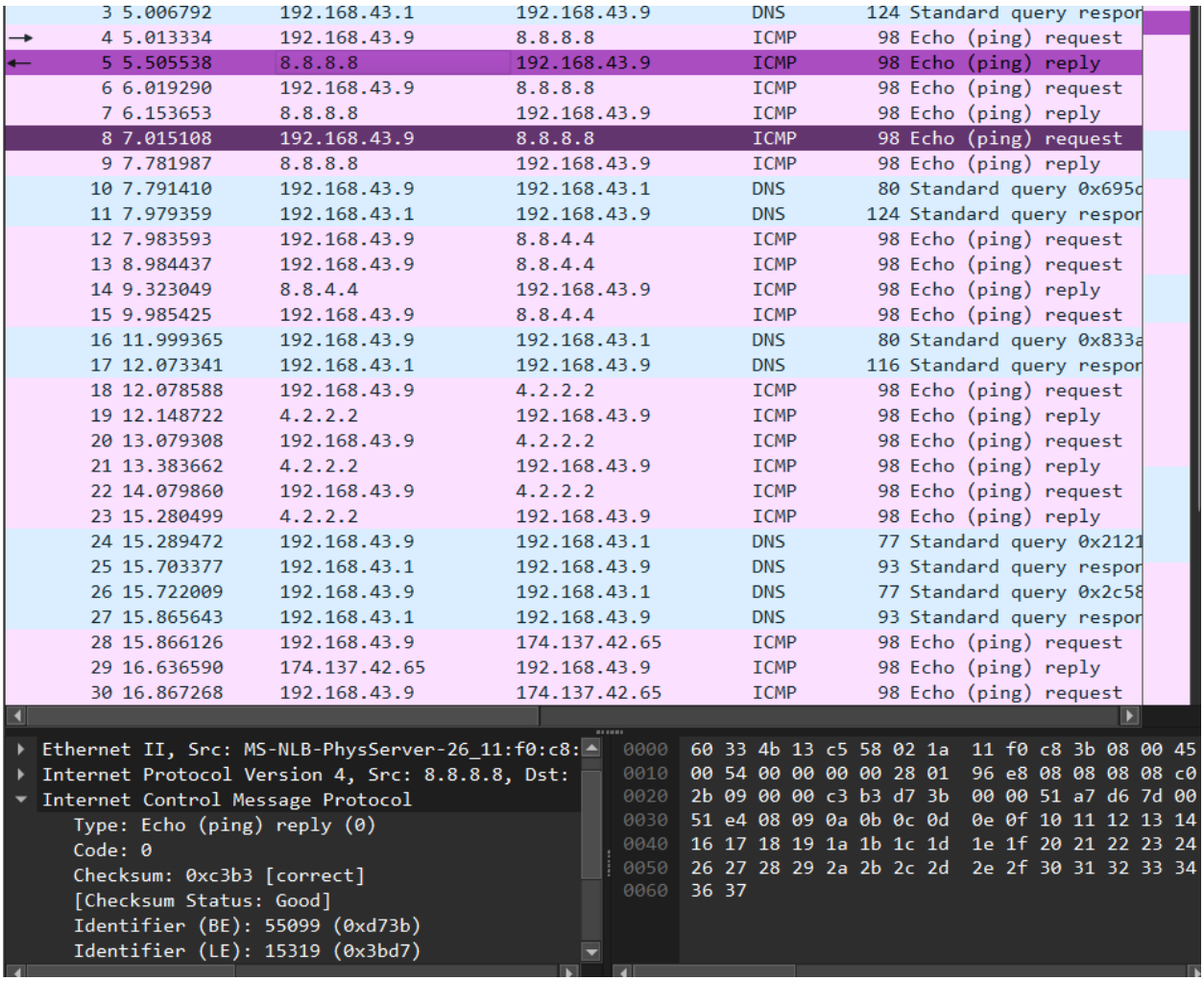
Below we see packet details for a ping request packet. There are a few important things within the packet details that we can take note of first being the type and code of the packet. A type that equals 8 means that it is a request packet, if it is equal to 0 it is a reply packet. When these codes are 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.

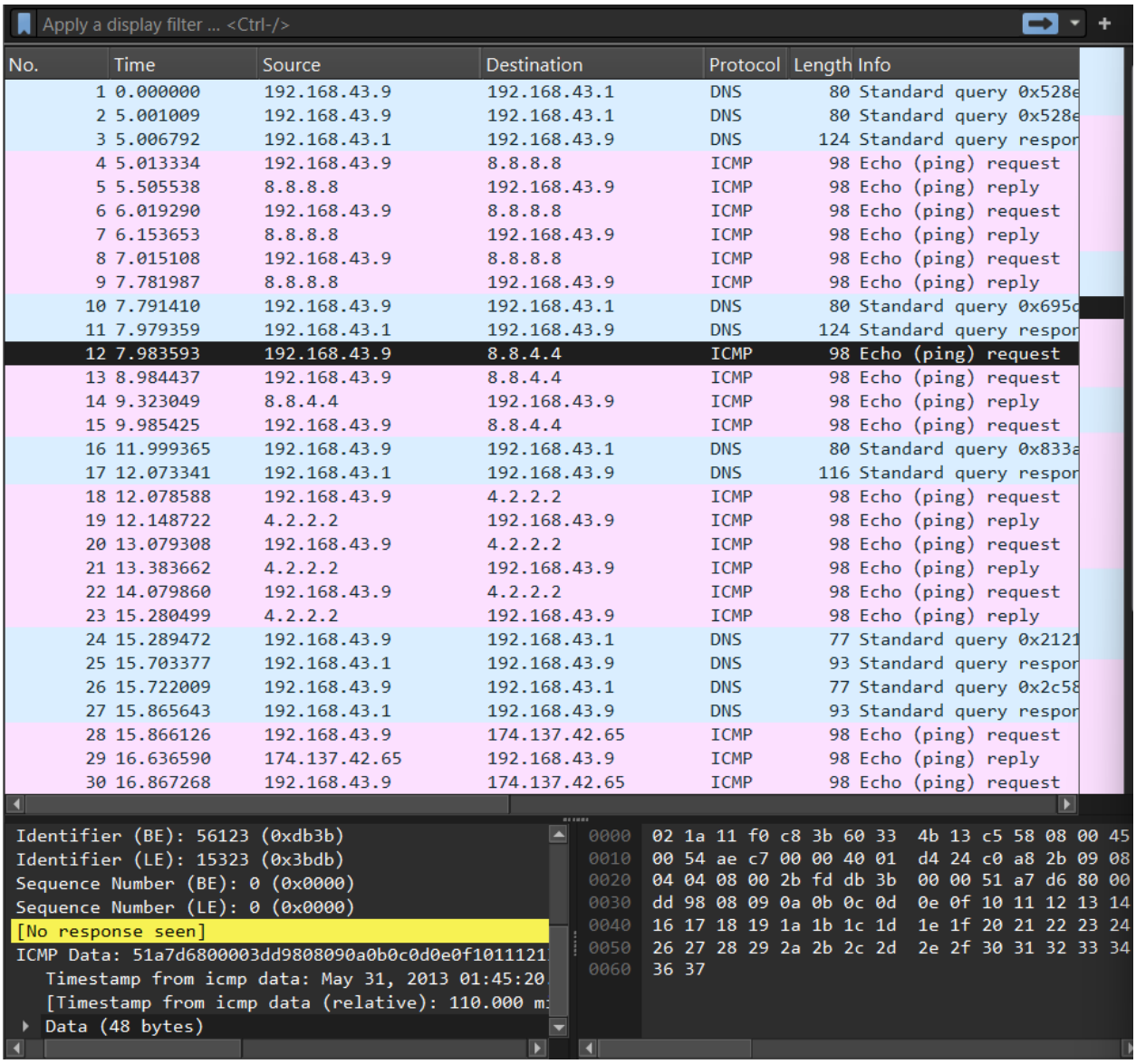
What is the type for packet 4?8



What is the type for packet 5?0

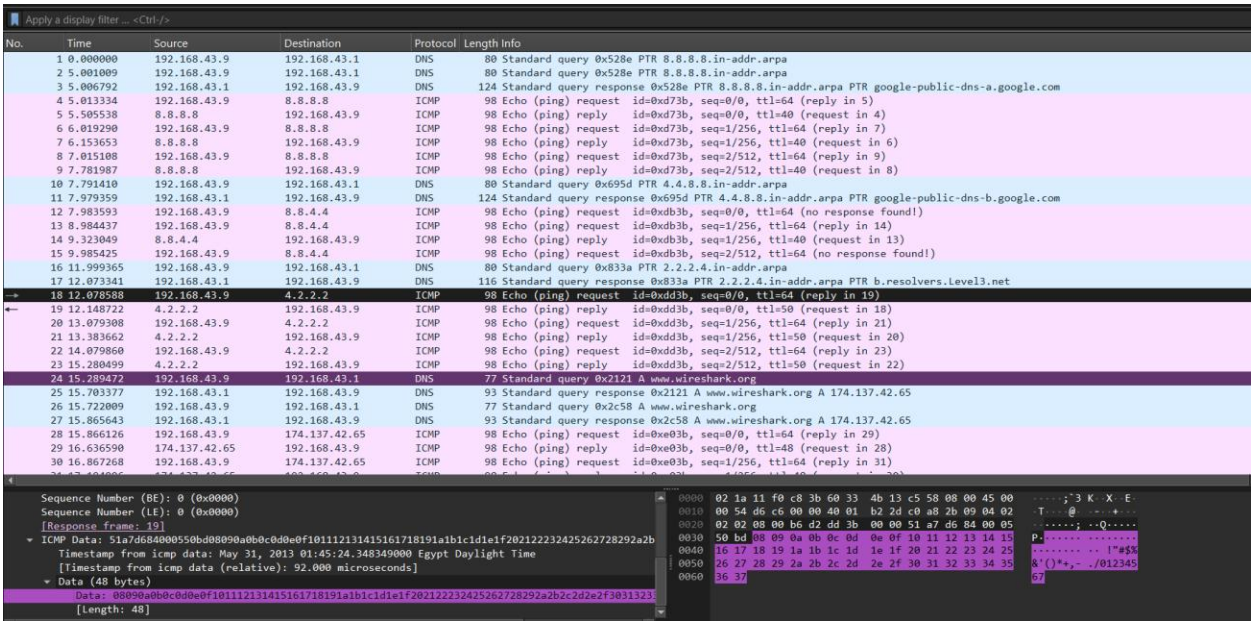


What is the timestamp for packet 12, only including month day and year? May 30, 2013



What is the full data string for packet 18?

08090a0b0c0d0e0f101112131415161718191a1b1c1d1e1f202122232425262728292a2b2c2d2e2f3031323334353637



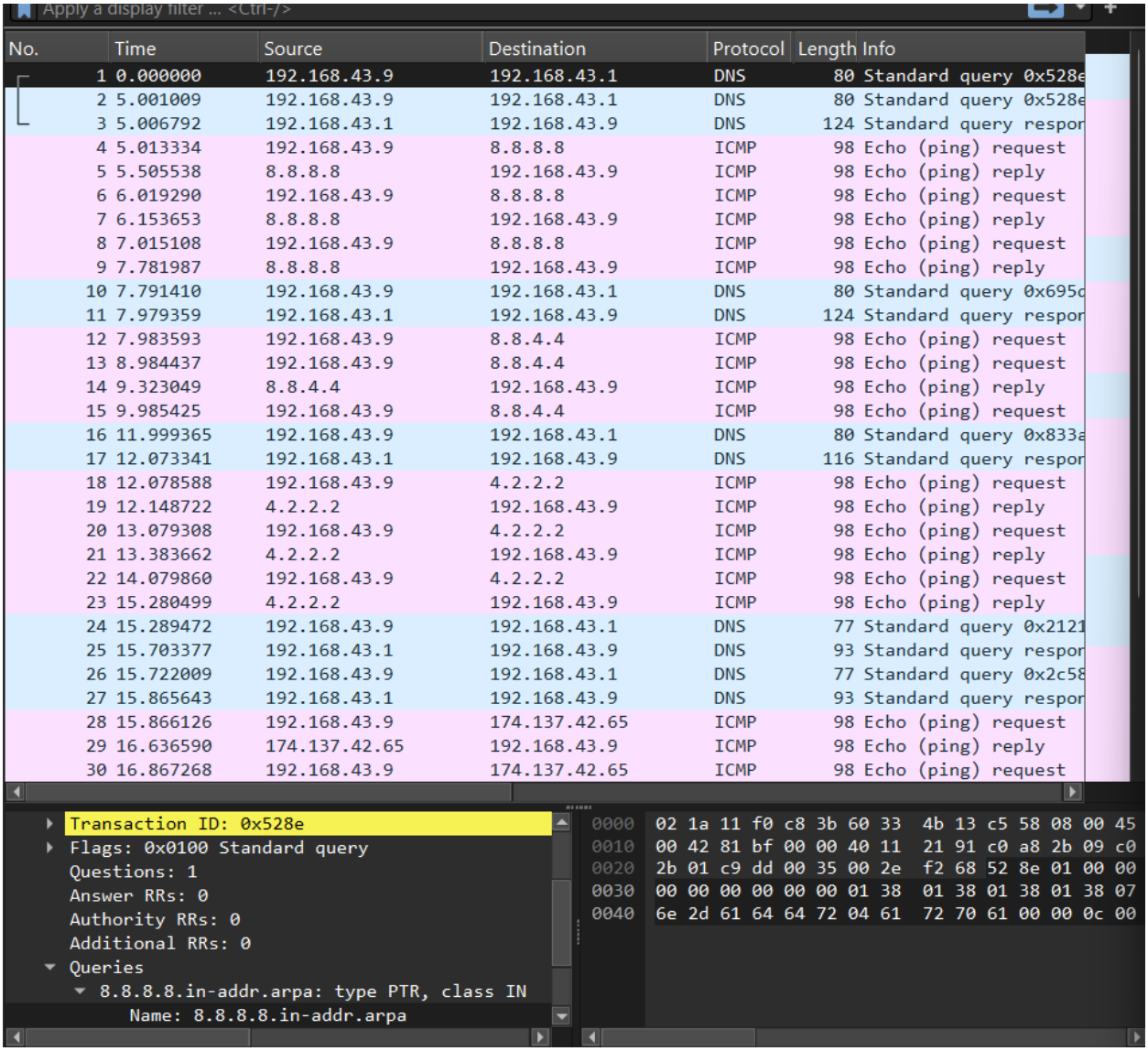
NS Overview

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].

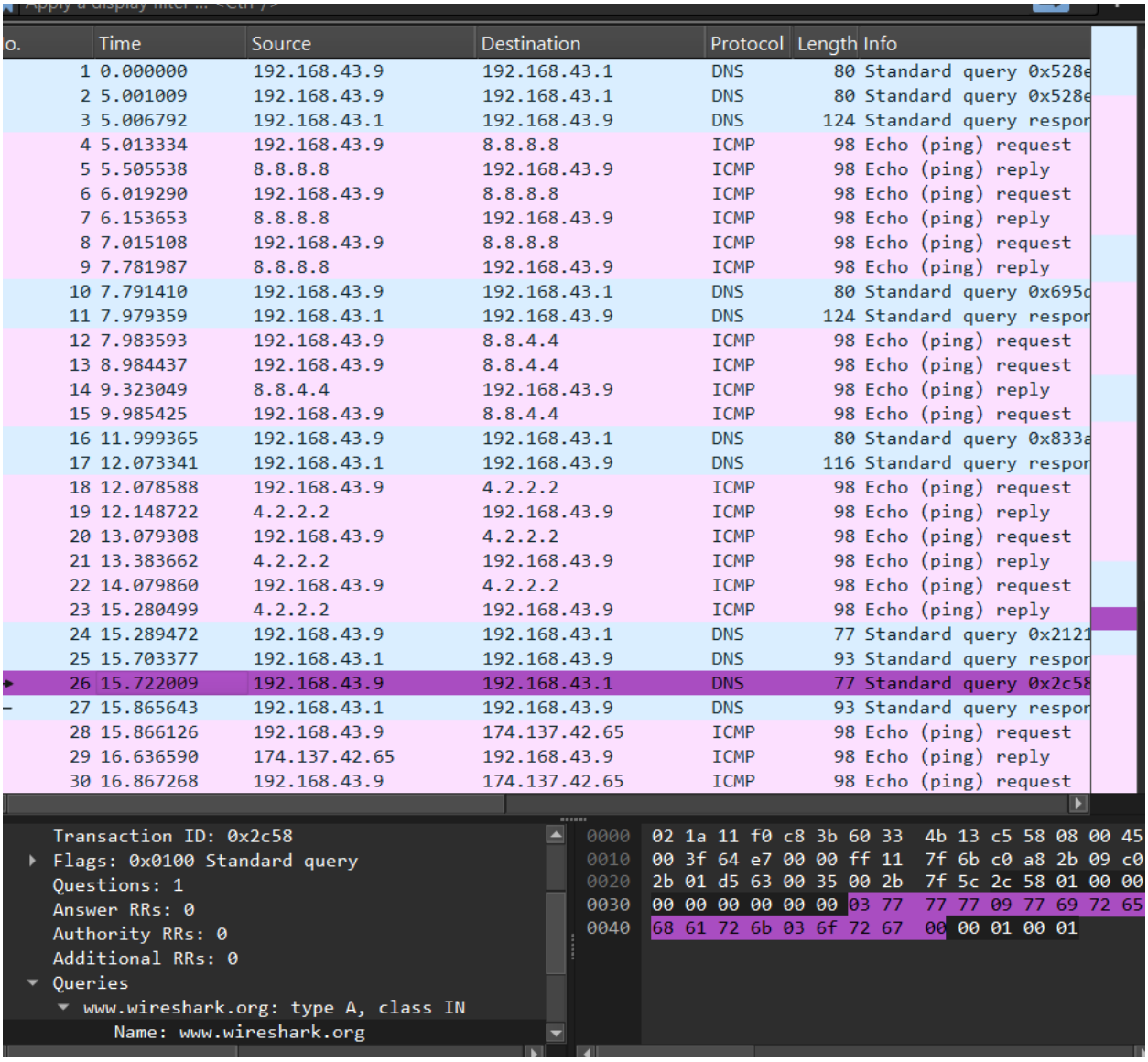
There are a couple of things outlined below that you should keep in the back of your mind when analyzing DNS packets.

- **Query-Response**
- **DNS-Servers Only**
- **UDP**

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



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

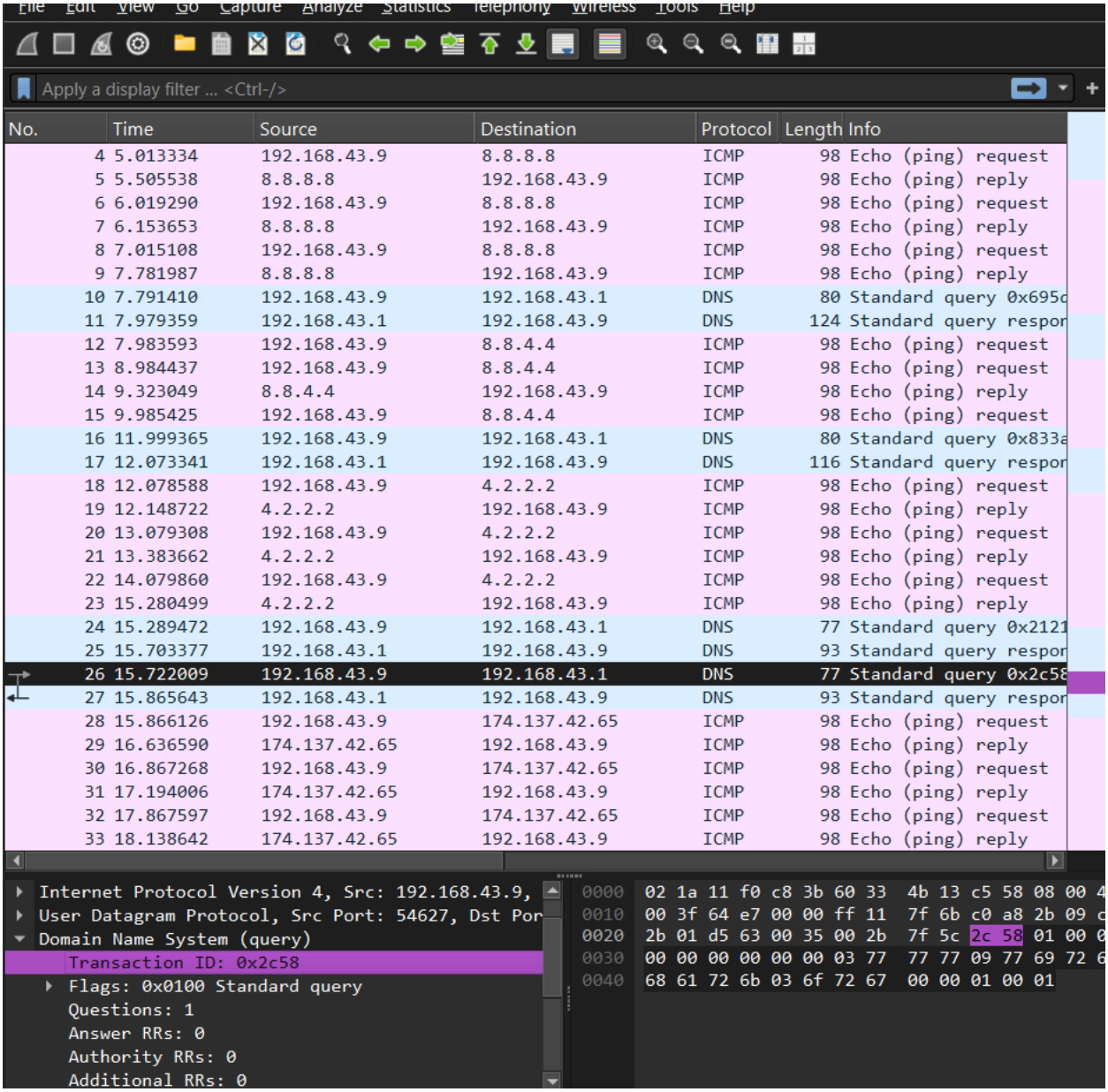


o.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	192.168.43.9	192.168.43.1	DNS	80	Standard query 0x528e
2	5.001009	192.168.43.9	192.168.43.1	DNS	80	Standard query 0x528e
3	5.006792	192.168.43.1	192.168.43.9	DNS	124	Standard query respor
4	5.013334	192.168.43.9	8.8.8.8	ICMP	98	Echo (ping) request
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 respor
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 respor
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 respor
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 respor
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
```

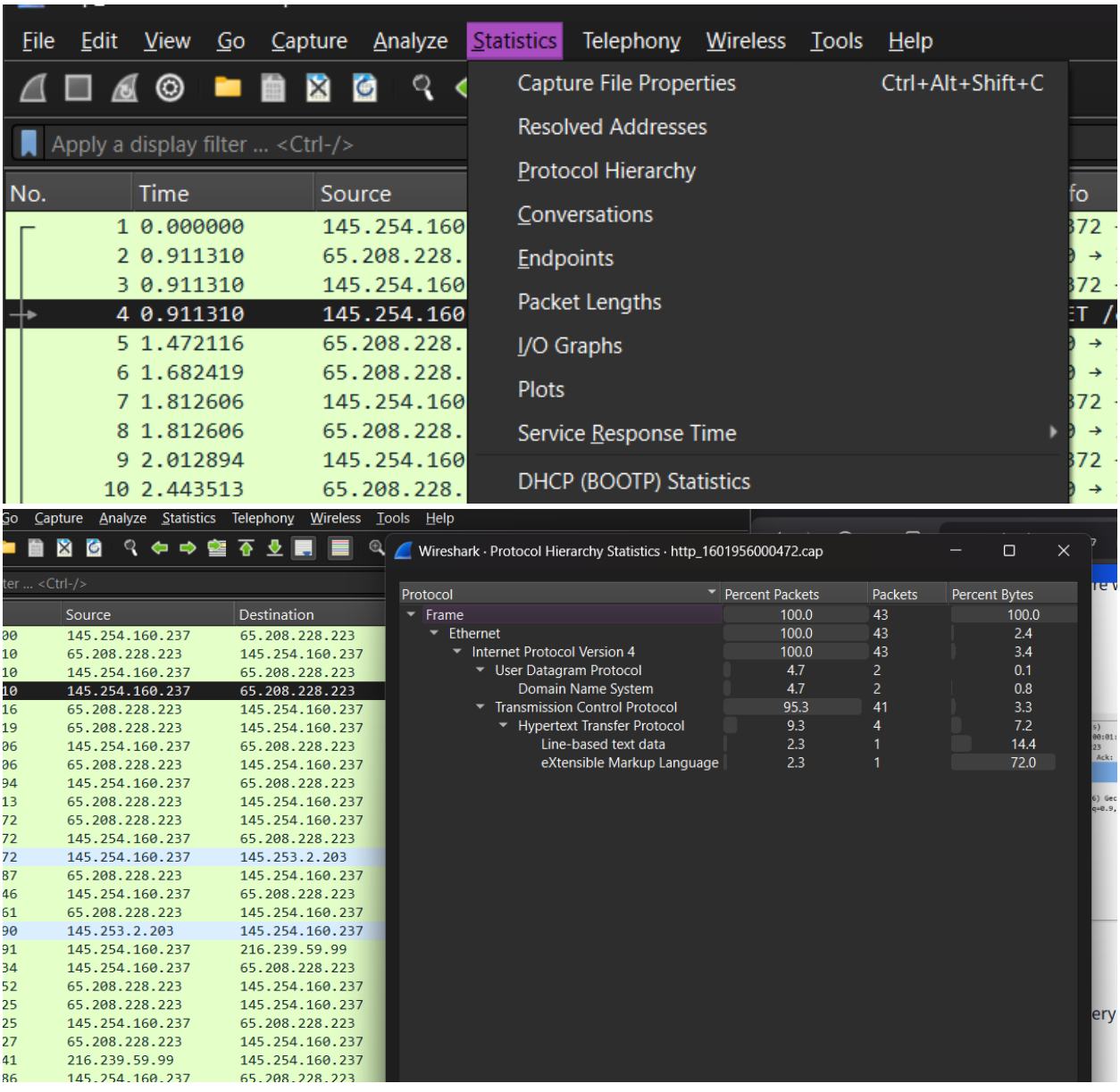
```
0000  02 1a 11 f0 c8 3b 60 33  4b 13 c5 58 08 00 45
0010  00 3f 64 e7 00 00 ff 11  7f 6b c0 a8 2b 09 c0
0020  2b 01 d5 63 00 35 00 2b  7f 5c 2c 58 01 00 00
0030  00 00 00 00 00 00 03 77  77 77 09 77 69 72 65
0040  68 61 72 6b 03 6f 72 67  00 00 01 00 01
```

What is the Transaction ID for packet 26? 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

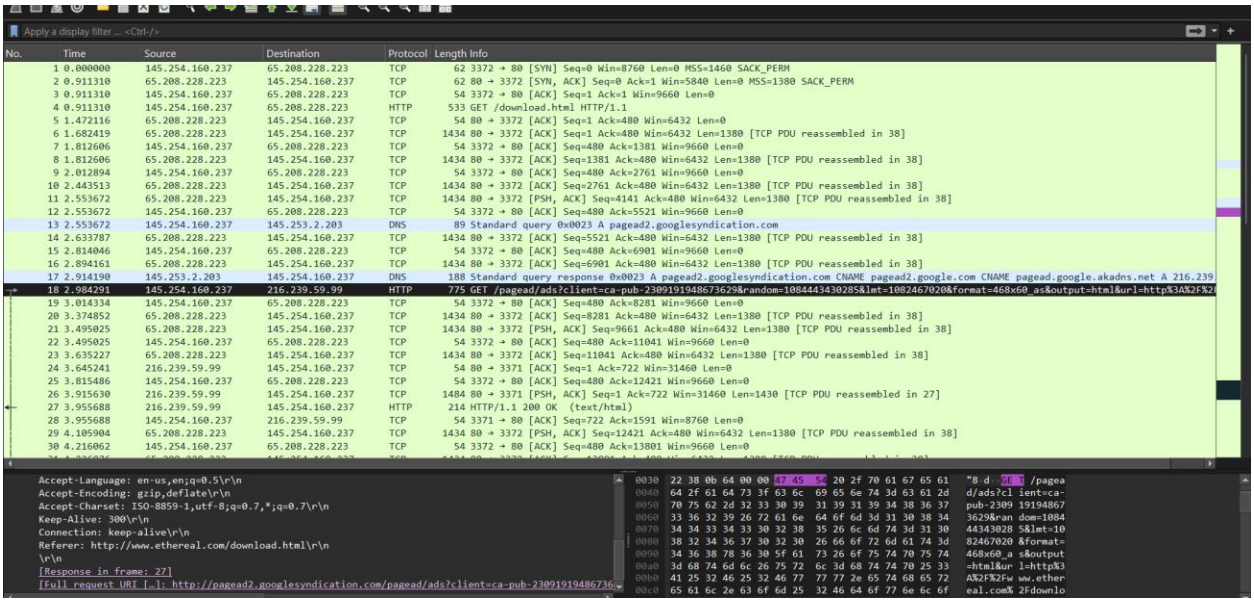


What endpoint ends in .237? 145.254.160.237

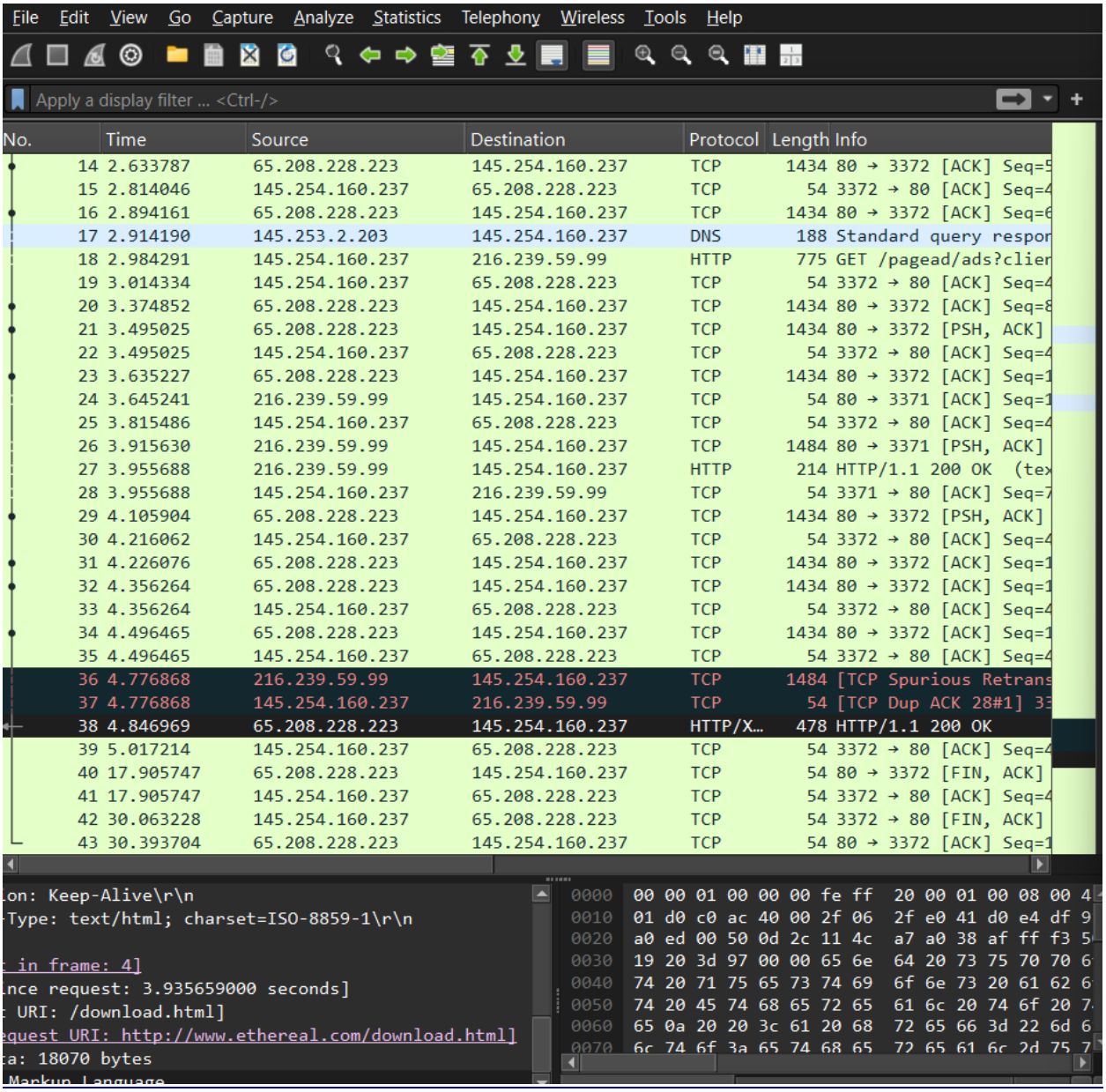
No.	Time	Source	Destination	Protocol	Length	Info
4	0.911310	145.254.160.237	65.208.228.223	HTTP	533	GET /download.html HTTP/1.1
18	2.984291	145.254.160.237	216.239.59.99	HTTP	775	GET /pagead/ads?client=ca-p
27	3.955688	216.239.59.99	145.254.160.237	HTTP	214	HTTP/1.1 200 OK (text/html
38	4.846969	65.208.228.223	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_FFFFF&color_tex_t=333333&color_li_nk=000000&color_u_rl=666633&color__border=666633

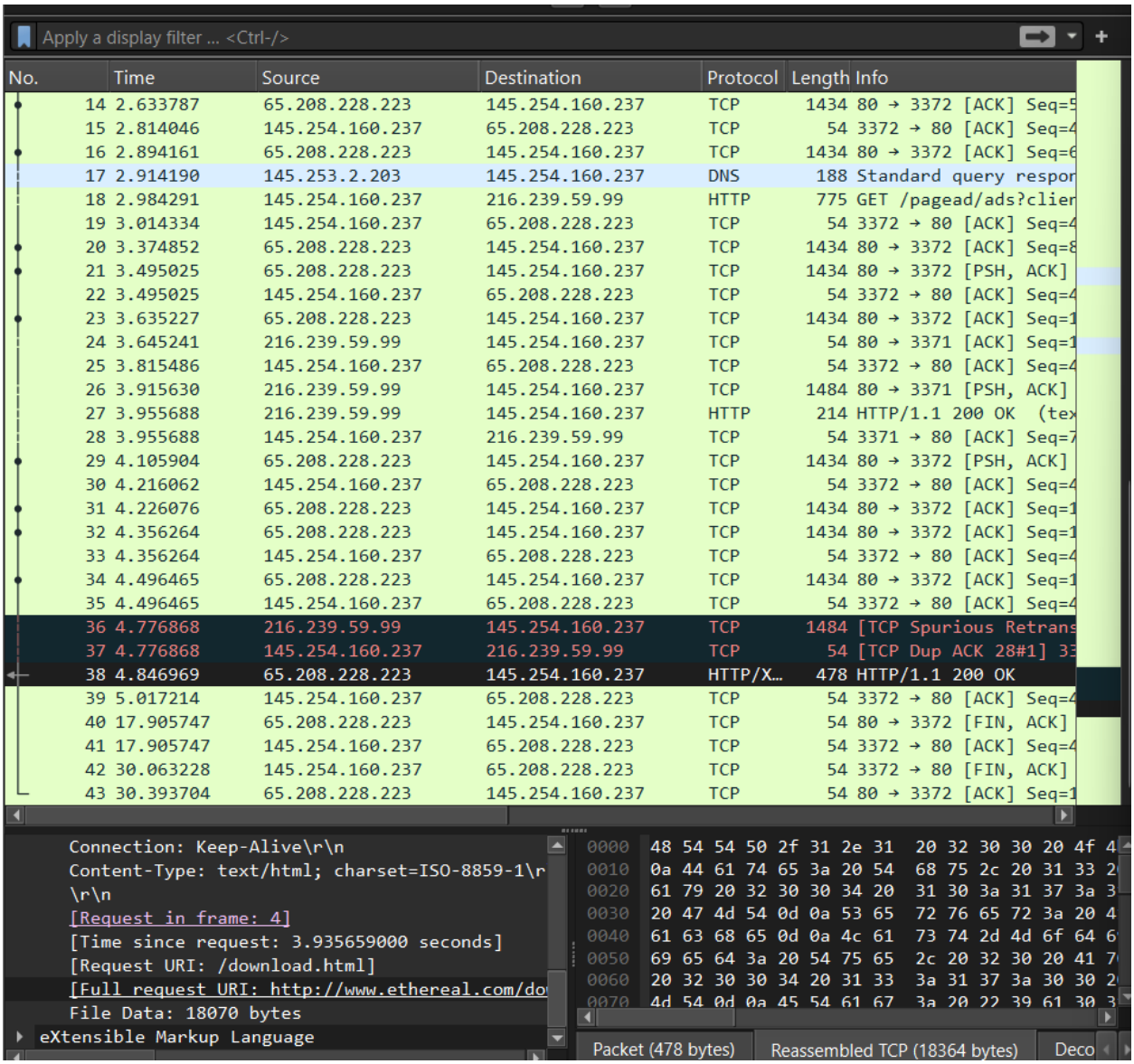


What domain name was requested from packet 38? www.ethereal.com



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

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



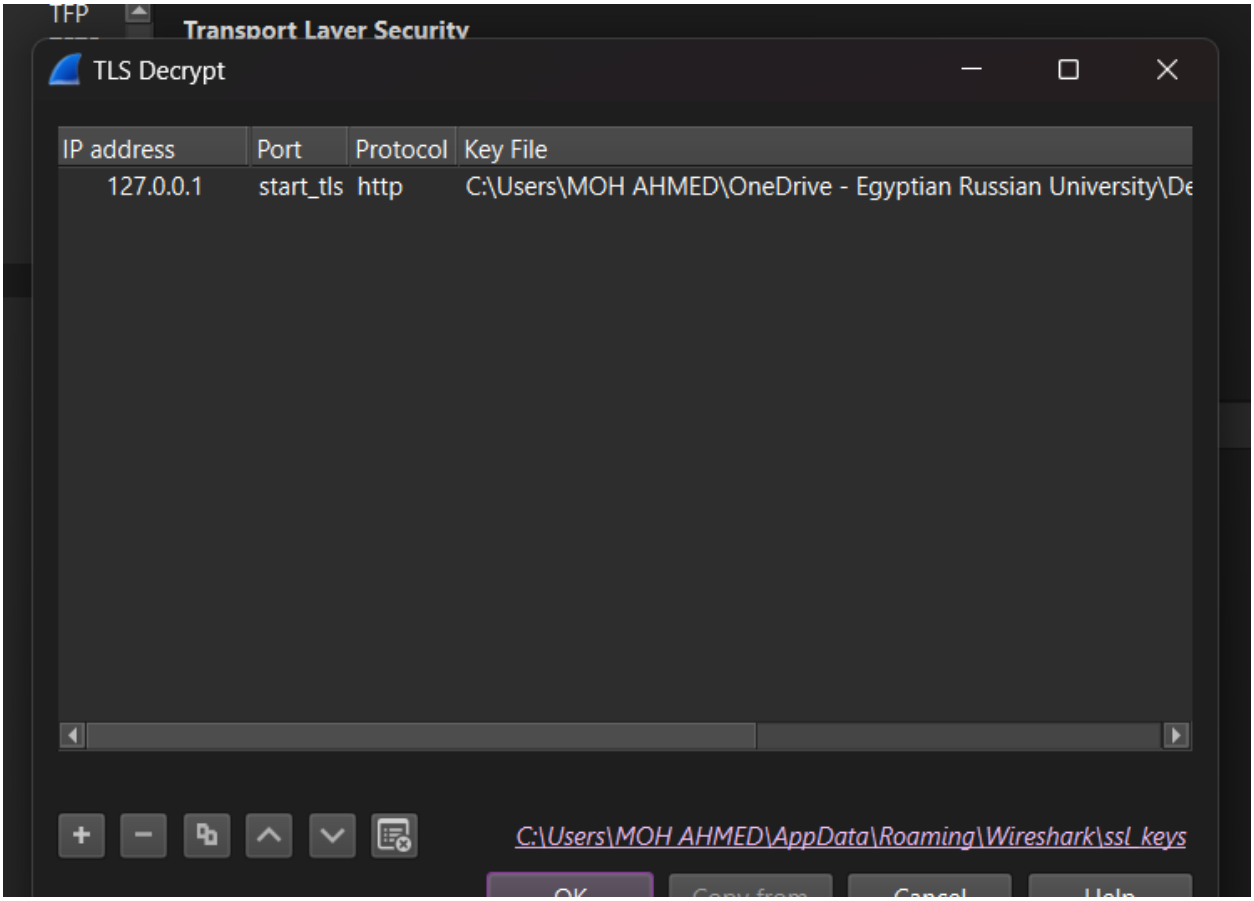
HTTPS Traffic Overview

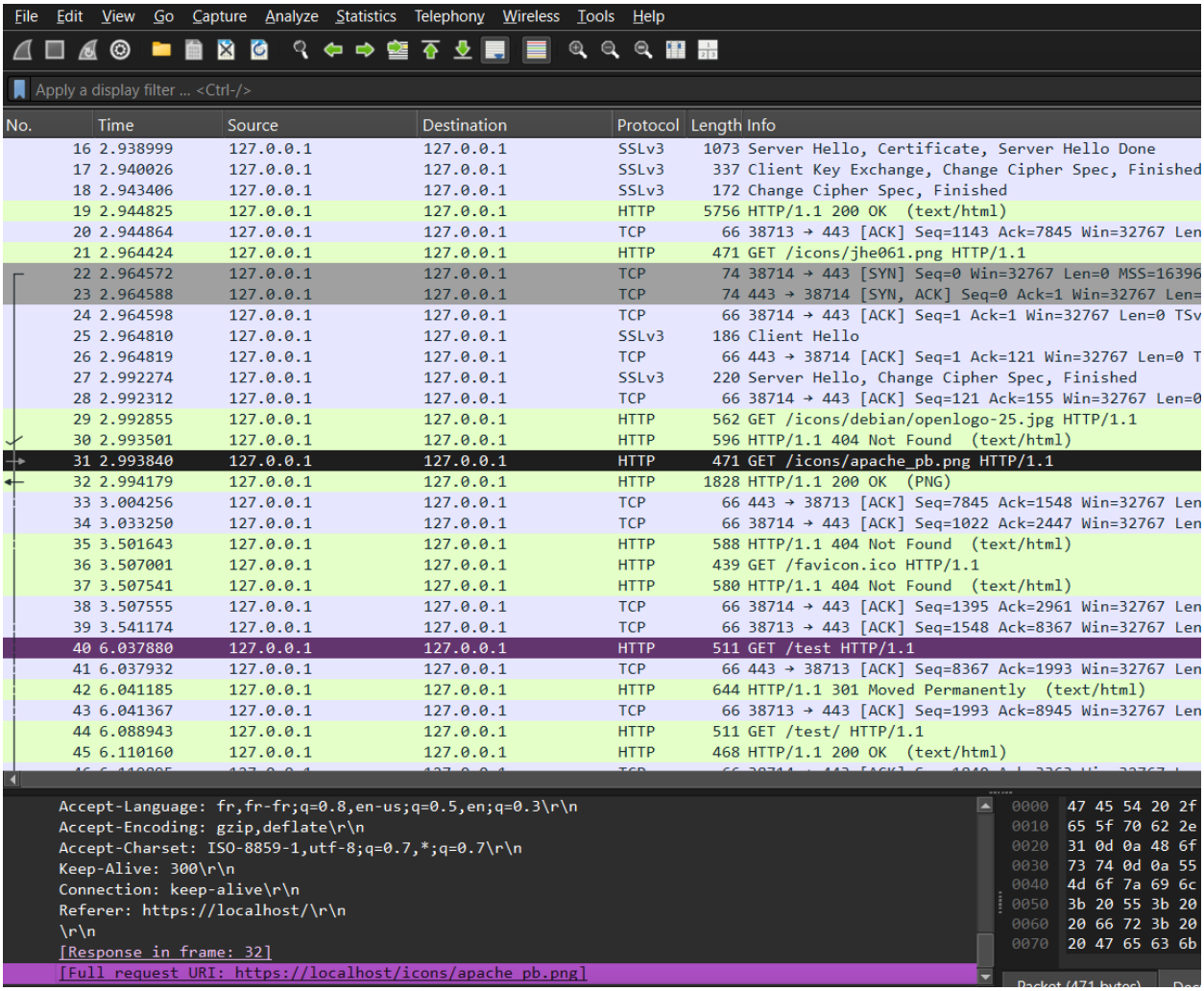
Before sending encrypted information the client and server need to agree upon various steps in order to make a secure tunnel.

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**

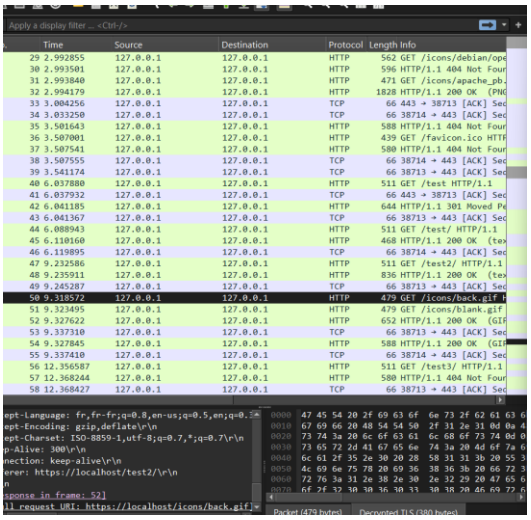
Looking at the data stream what is the full request URI for packet 31?
https://localhost/icons/apache_pb.png


TFP
Transport Layer Security
TLS Decrypt
IP address
Port
Protocol
Key File
127.0.0.1
start_tls
http
C:\Users\MOH AHMED\OneDrive - Egyptian Russian University\De
C:\Users\MOH AHMED\AppData\Roaming\Wireshark\ssl_keys

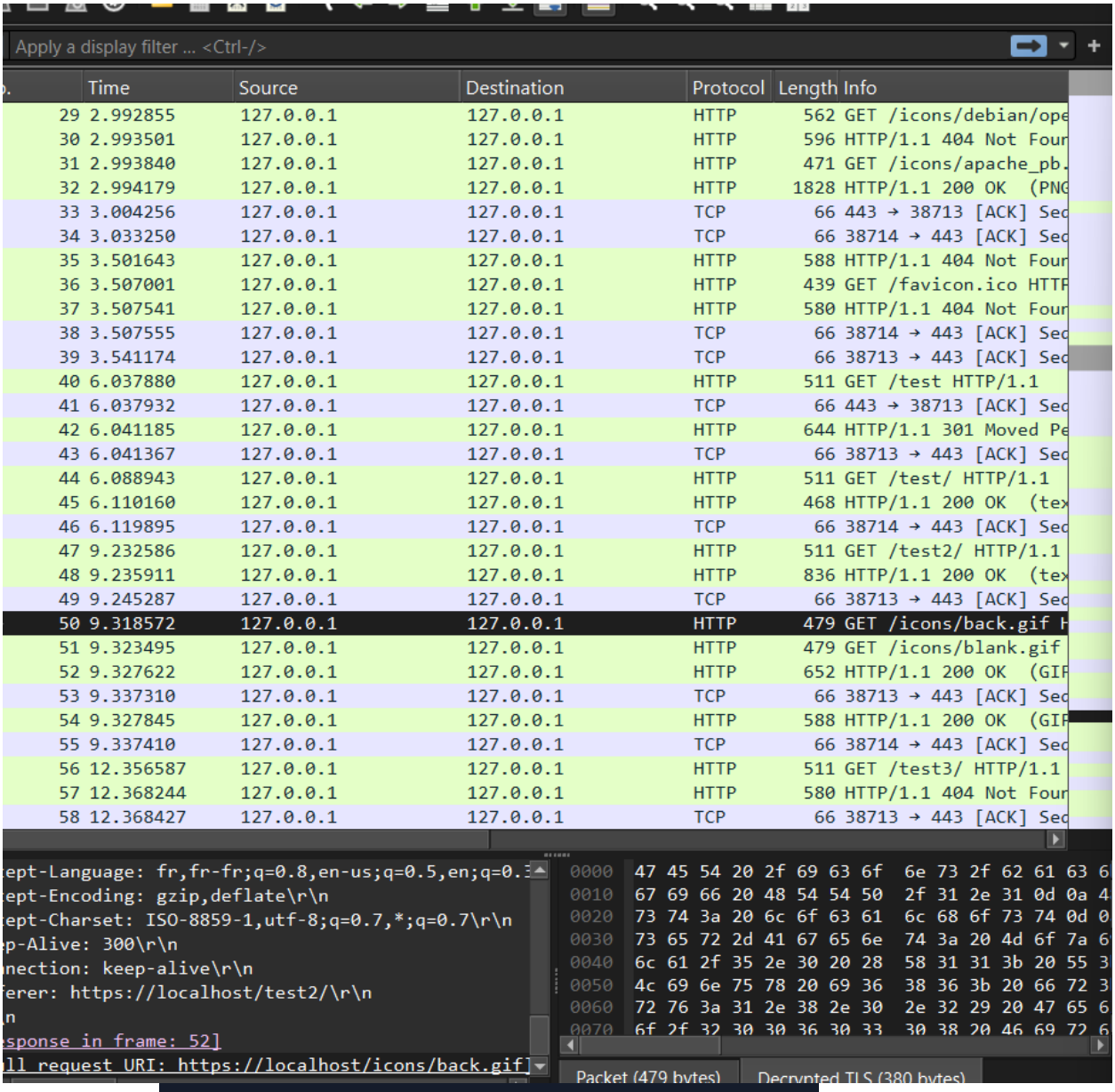


Looking at the data stream what is the full request URI for packet 50?

https://localhost/icons/back.gif



What is the User-Agent listed in packet 50?



final: