

WireShark Lab 1

Lab Example used on WireShark!

The screenshot shows a Wireshark interface with a list of captured network frames at the top and a detailed view of frame 1 below.

Frame 1 Details:

- Frame 1: Packet, 62 bytes on wire (496 bits), 62 bytes captured (496 bits)
- Ethernet II, Src: PCSSystemtec_97:3f:45 (08:00:27:97:3f:45), Dst: PCSSystemtec_38:db:ed (08:00:27:38:db:ed)
- Internet Protocol Version 4, Src: 1.1.1.2, Dst: 1.1.1.1
- Transmission Control Protocol, Src Port: 1042, Dst Port: 53, Seq: 0, Len: 0

Hex and ASCII Data:

Hex	ASCII
0000 08 00 27 38 db ed 08 00	8 00 27 38 db ed 08 00
0010 00 30 00 ea 40 00 80 06	0 30 00 ea 40 00 80 06
0020 f5 d9 01 01 01 02 01 01	f5 d9 01 01 01 02 01 01
0030 01 01 04 12 00 35 d1 f8	01 01 04 12 00 35 d1 f8
0040 c1 16 00 00 00 00 70 02	c1 16 00 00 00 00 70 02
0050 05 b4 01 01 04 02	5 b4 01 01 04 02

Q1

What is the type of the DNS query requested?

AXFR (zone transfer)

Q2

What domain was requested?

etas.com

Q3

How many items were in the response?

4 items

Q4

What is the TTL for all of the DNS records?

(note that this is the TTL for the DNS record, not the IP packet.)

3600 seconds (TTL)

Q5

What is the IP address for the "welcome" subdomain?

1.1.1.1

Knowledge gained from these sources:

~<https://trove.cyberskyline.com/computer-fundamentals-for-cybersecurity/networking>

~~~<https://www.cengage.com/>

~~~~~<https://www.youtube.com/>