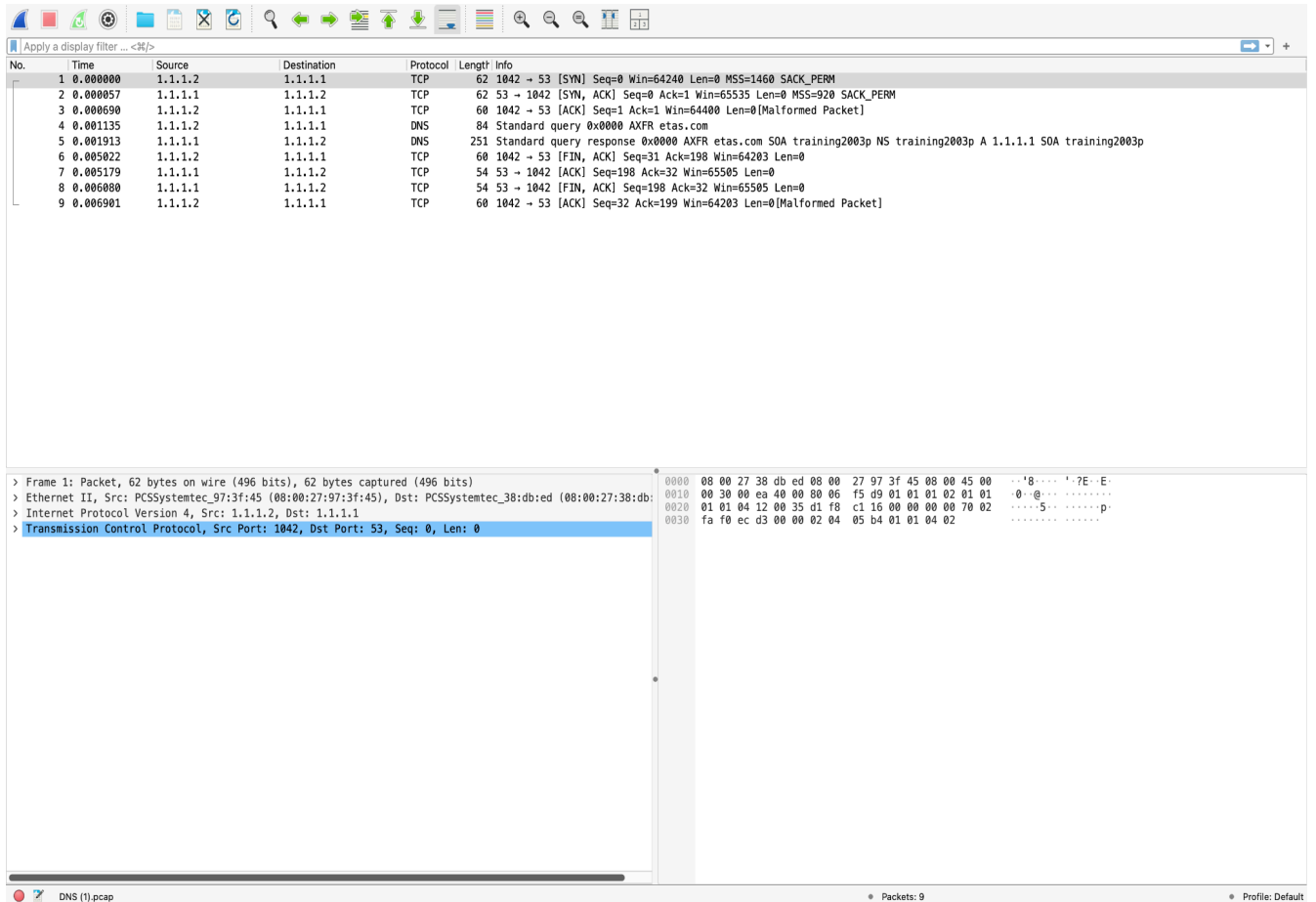


WireShark Lab 1

Lab Example used on WireShark!



The image shows the WireShark network protocol analyzer interface. The top pane displays a list of 9 captured packets. The bottom pane shows the detailed view of the selected packet (Frame 1), which is a Transmission Control Protocol (TCP) segment.

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	1.1.1.2	1.1.1.1	TCP	62	1042 → 53 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM
2	0.000057	1.1.1.1	1.1.1.2	TCP	62	53 → 1042 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=920 SACK_PERM
3	0.000690	1.1.1.2	1.1.1.1	TCP	60	1042 → 53 [ACK] Seq=1 Ack=1 Win=64400 Len=0 [Malformed Packet]
4	0.001135	1.1.1.2	1.1.1.1	DNS	84	Standard query 0x0000 AXFR etas.com
5	0.001913	1.1.1.1	1.1.1.2	DNS	251	Standard query response 0x0000 AXFR etas.com SOA training2003p NS training2003p A 1.1.1.1 SOA training2003p
6	0.005022	1.1.1.2	1.1.1.1	TCP	60	1042 → 53 [FIN, ACK] Seq=31 Ack=198 Win=64203 Len=0
7	0.005179	1.1.1.1	1.1.1.2	TCP	54	53 → 1042 [ACK] Seq=198 Ack=32 Win=65505 Len=0
8	0.006080	1.1.1.1	1.1.1.2	TCP	54	53 → 1042 [FIN, ACK] Seq=198 Ack=32 Win=65505 Len=0
9	0.006901	1.1.1.2	1.1.1.1	TCP	60	1042 → 53 [ACK] Seq=32 Ack=199 Win=64203 Len=0 [Malformed Packet]

Frame 1: Packet, 62 bytes on wire (496 bits), 62 bytes captured (496 bits) on interface 0

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

0000 08 00 27 38 db ed 08 00 27 97 3f 45 08 00 45 00 ..8... :7E:E
0010 00 30 00 ea 40 00 06 f5 d9 01 01 01 02 01 01 ..0..@...
0020 01 01 04 12 00 35 d1 f8 c1 16 00 00 00 70 025.....p
0030 fa f0 ec d3 00 00 02 04 05 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-cyb~ersecurity/networking>

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

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