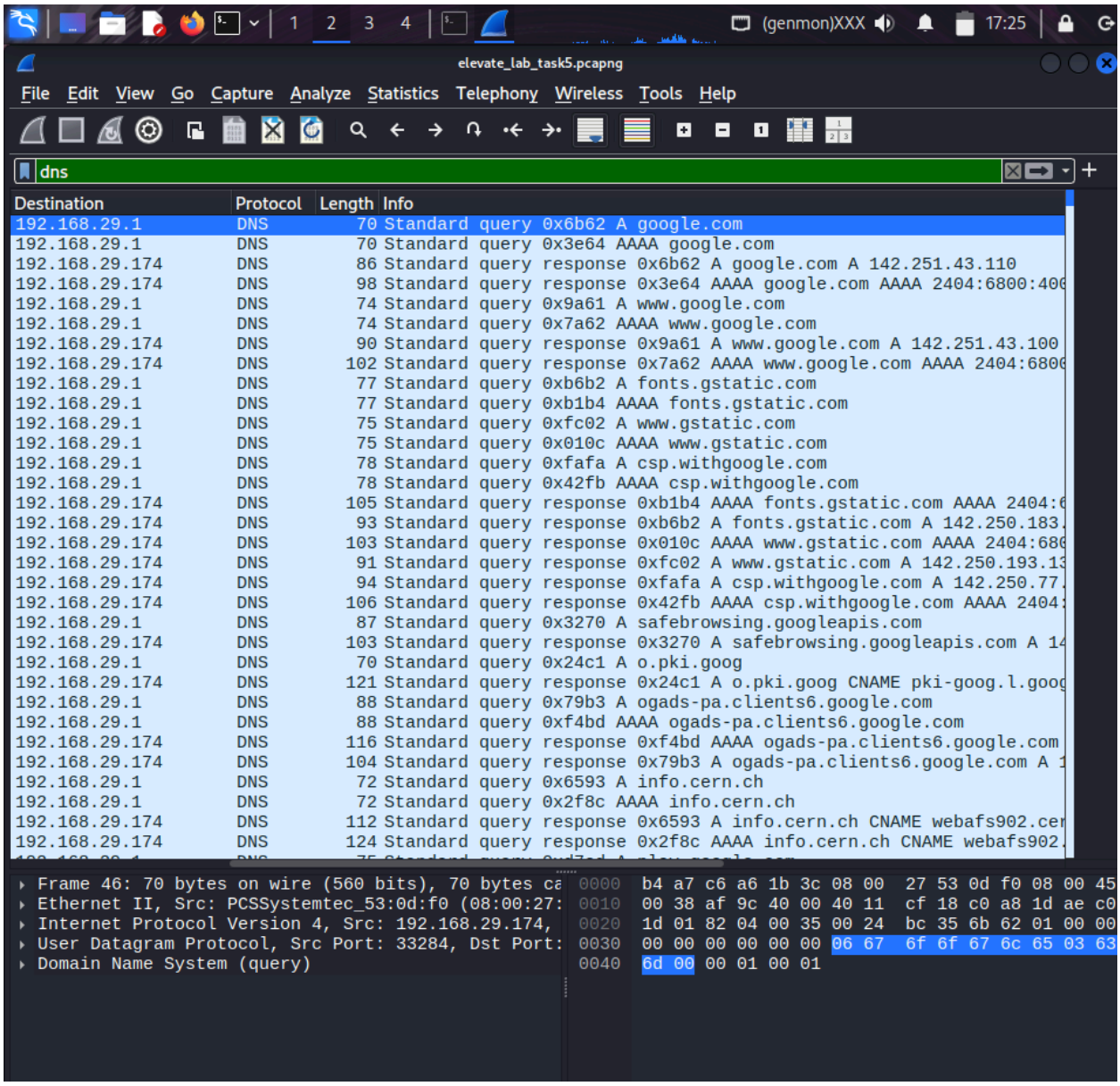
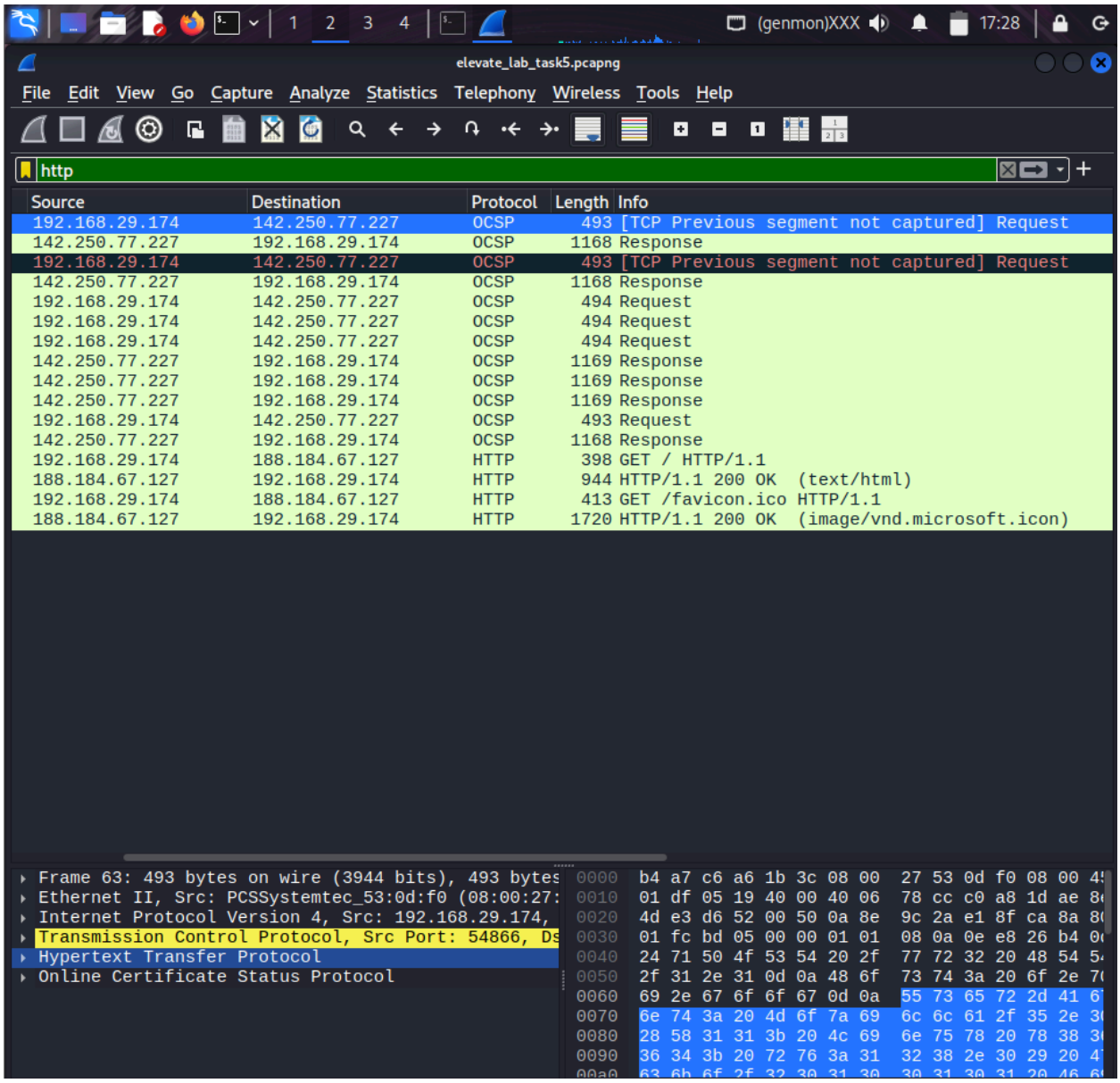
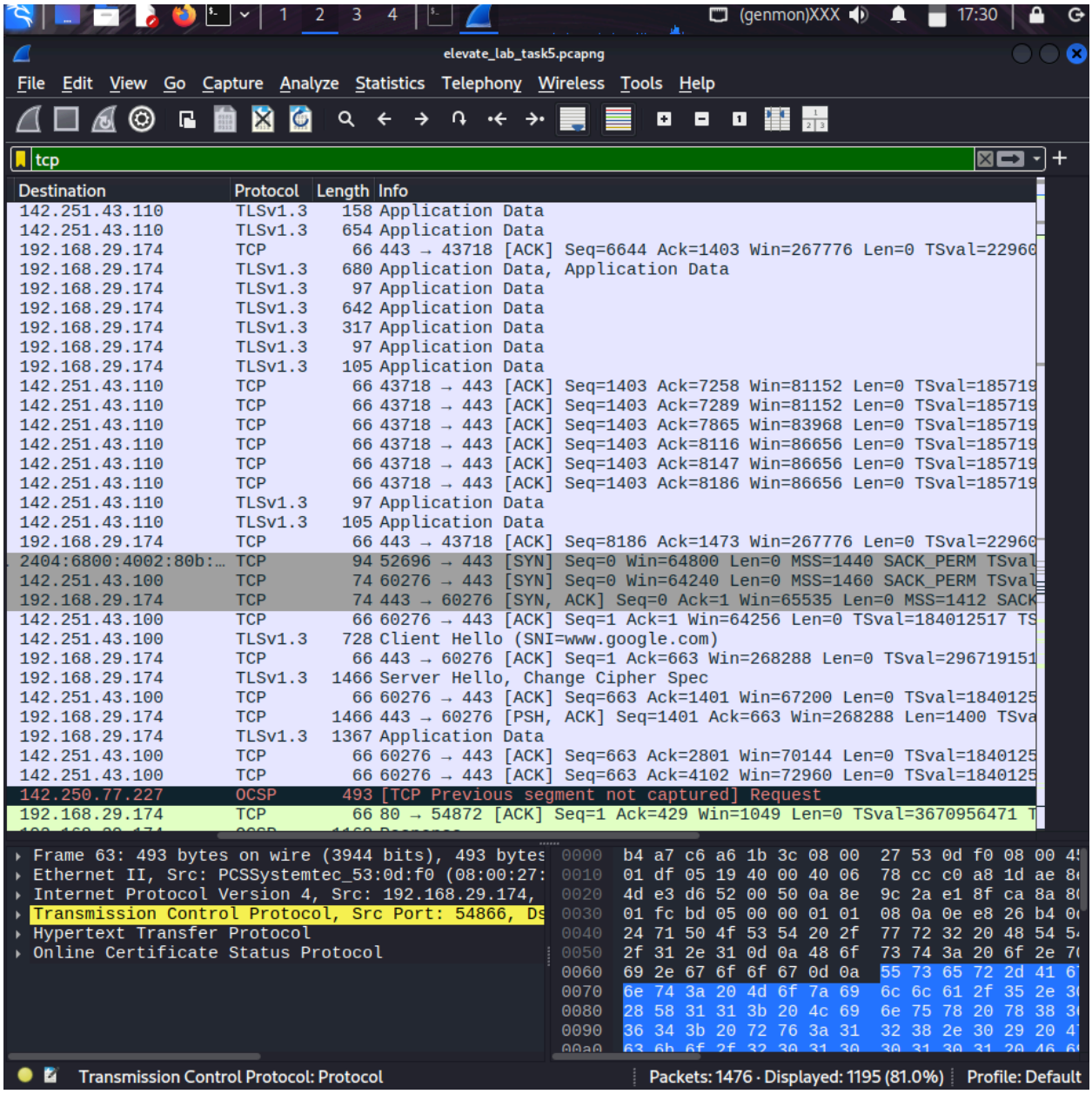
1. Dns filter


elevate_lab_task5.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
dns
Destination Protocol Length Info
192.168.29.1 DNS 70 Standard query 0x6b62 A google.com
192.168.29.1 DNS 70 Standard query 0x3e64 AAAA google.com
192.168.29.174 DNS 86 Standard query response 0x6b62 A google.com A 142.251.43.110
192.168.29.174 DNS 98 Standard query response 0x3e64 AAAA google.com AAAA 2404:6800:406
192.168.29.1 DNS 74 Standard query 0x9a61 A www.google.com
192.168.29.1 DNS 74 Standard query 0x7a62 AAAA www.google.com
192.168.29.174 DNS 90 Standard query response 0x9a61 A www.google.com A 142.251.43.100
192.168.29.174 DNS 102 Standard query response 0x7a62 AAAA www.google.com AAAA 2404:6806
192.168.29.1 DNS 77 Standard query 0xb6b2 A fonts.gstatic.com
192.168.29.1 DNS 77 Standard query 0xb1b4 AAAA fonts.gstatic.com
192.168.29.1 DNS 75 Standard query 0xfc02 A www.gstatic.com
192.168.29.1 DNS 75 Standard query 0x010c AAAA www.gstatic.com
192.168.29.1 DNS 78 Standard query 0xfafa A csp.withgoogle.com
192.168.29.1 DNS 78 Standard query 0x42fb AAAA csp.withgoogle.com
192.168.29.174 DNS 105 Standard query response 0xb1b4 AAAA fonts.gstatic.com AAAA 2404:6
192.168.29.174 DNS 93 Standard query response 0xb6b2 A fonts.gstatic.com A 142.250.183.
192.168.29.174 DNS 103 Standard query response 0x010c AAAA www.gstatic.com AAAA 2404:680
192.168.29.174 DNS 91 Standard query response 0xfc02 A www.gstatic.com A 142.250.193.13
192.168.29.174 DNS 94 Standard query response 0xfafa A csp.withgoogle.com A 142.250.77.
192.168.29.174 DNS 106 Standard query response 0x42fb AAAA csp.withgoogle.com AAAA 2404:
192.168.29.1 DNS 87 Standard query 0x3270 A safebrowsing.googleapis.com
192.168.29.174 DNS 103 Standard query response 0x3270 A safebrowsing.googleapis.com A 14
192.168.29.1 DNS 70 Standard query 0x24c1 A o.pki.goog
192.168.29.174 DNS 121 Standard query response 0x24c1 A o.pki.goog CNAME pki-goog.l.goog
192.168.29.1 DNS 88 Standard query 0x79b3 A ogads-pa.clients6.google.com
192.168.29.1 DNS 88 Standard query 0xf4bd AAAA ogads-pa.clients6.google.com
192.168.29.174 DNS 116 Standard query response 0xf4bd AAAA ogads-pa.clients6.google.com
192.168.29.174 DNS 104 Standard query response 0x79b3 A ogads-pa.clients6.google.com A 1
192.168.29.1 DNS 72 Standard query 0x6593 A info.cern.ch
192.168.29.1 DNS 72 Standard query 0x2f8c AAAA info.cern.ch
192.168.29.174 DNS 112 Standard query response 0x6593 A info.cern.ch CNAME webafs902.cer
192.168.29.174 DNS 124 Standard query response 0x2f8c AAAA info.cern.ch CNAME webafs902.
Frame 46: 70 bytes on wire (560 bits), 70 bytes ca
Ethernet II, Src: PCSSystemtec_53:0d:f0 (08:00:27:
Internet Protocol Version 4, Src: 192.168.29.174,
User Datagram Protocol, Src Port: 33284, Dst Port:
Domain Name System (query)
0000 b4 a7 c6 a6 1b 3c 08 00 27 53 0d f0 08 00 45
0010 00 38 af 9c 40 00 40 11 cf 18 c0 a8 1d ae c0
0020 1d 01 82 04 00 35 00 24 bc 35 6b 62 01 00 00
0030 00 00 00 00 00 00 06 67 6f 6f 67 6c 65 03 63
0040 6d 00 00 01 00 01

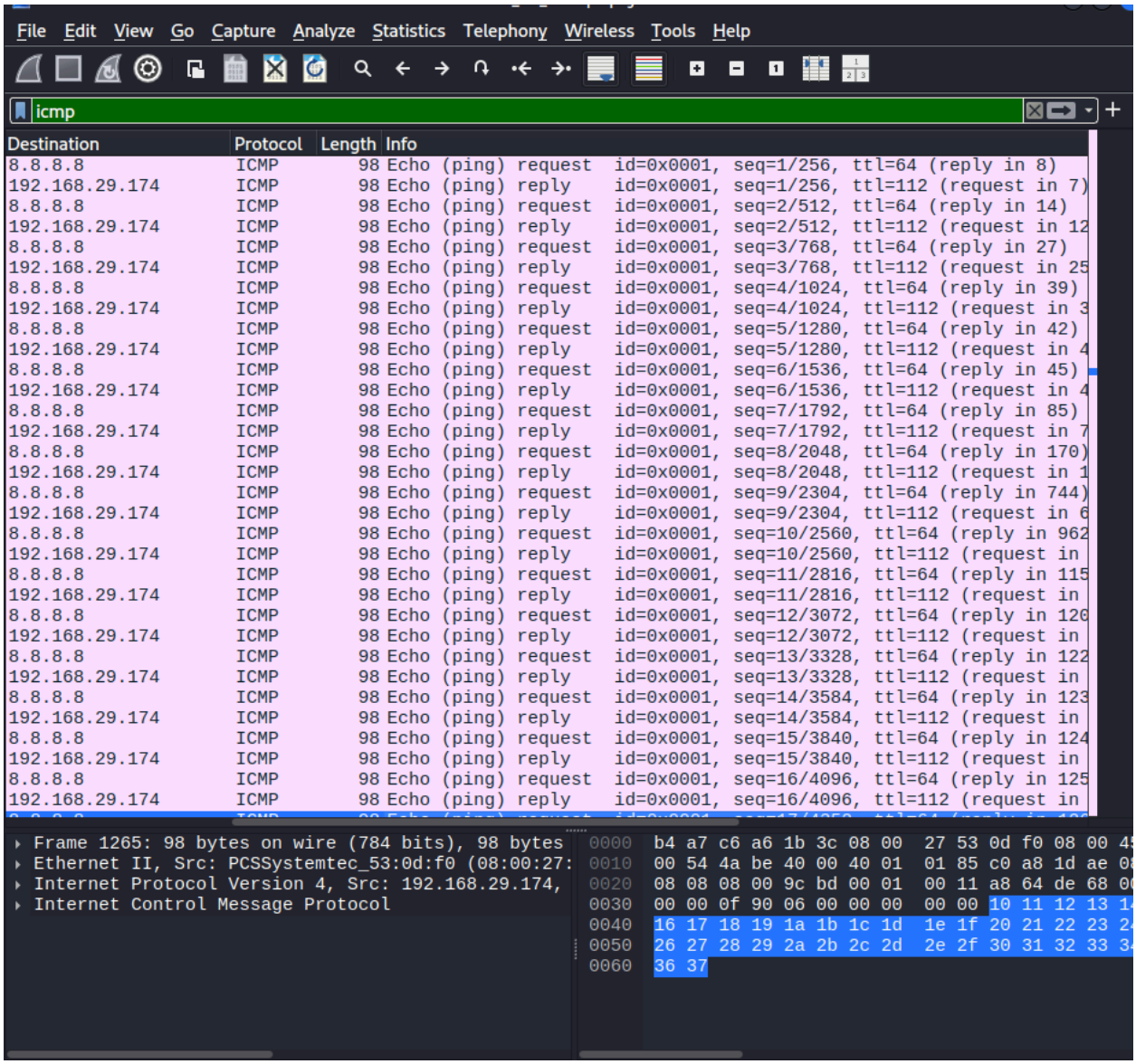
2. Http


elevate_lab_task5.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
http
Source Destination Protocol Length Info
192.168.29.174 142.250.77.227 OCSP 493 [TCP Previous segment not captured] Request
142.250.77.227 192.168.29.174 OCSP 1168 Response
192.168.29.174 142.250.77.227 OCSP 493 [TCP Previous segment not captured] Request
142.250.77.227 192.168.29.174 OCSP 1168 Response
192.168.29.174 142.250.77.227 OCSP 494 Request
192.168.29.174 142.250.77.227 OCSP 494 Request
192.168.29.174 142.250.77.227 OCSP 494 Request
142.250.77.227 192.168.29.174 OCSP 1169 Response
142.250.77.227 192.168.29.174 OCSP 1169 Response
142.250.77.227 192.168.29.174 OCSP 1169 Response
192.168.29.174 142.250.77.227 OCSP 493 Request
142.250.77.227 192.168.29.174 OCSP 1168 Response
192.168.29.174 188.184.67.127 HTTP 398 GET / HTTP/1.1
188.184.67.127 192.168.29.174 HTTP 944 HTTP/1.1 200 OK (text/html)
192.168.29.174 188.184.67.127 HTTP 413 GET /favicon.ico HTTP/1.1
188.184.67.127 192.168.29.174 HTTP 1720 HTTP/1.1 200 OK (image/vnd.microsoft.icon)
Frame 63: 493 bytes on wire (3944 bits), 493 bytes
Ethernet II, Src: PCSSystemtec_53:0d:f0 (08:00:27:
Internet Protocol Version 4, Src: 192.168.29.174,
Transmission Control Protocol, Src Port: 54866, Ds
Hypertext Transfer Protocol
Online Certificate Status Protocol
0000 b4 a7 c6 a6 1b 3c 08 00 27 53 0d f0 08 00 45
0010 01 df 05 19 40 00 40 06 78 cc c0 a8 1d ae 8
0020 4d e3 d6 52 00 50 0a 8e 9c 2a e1 8f ca 8a 8
0030 01 fc bd 05 00 00 01 01 08 0a 0e e8 26 b4 0
0040 24 71 50 4f 53 54 20 2f 77 72 32 20 48 54 5
0050 2f 31 2e 31 0d 0a 48 6f 73 74 3a 20 6f 2e 7
0060 69 2e 67 6f 6f 67 0d 0a 55 73 65 72 2d 41 6
0070 6e 74 3a 20 4d 6f 7a 69 6c 6c 61 2f 35 2e 3
0080 28 58 31 31 3b 20 4c 69 6e 75 78 20 78 38 3
0090 36 34 3b 20 72 76 3a 31 32 38 2e 30 29 20 4

3. Tcp


elevate_lab_task5.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
tcp
Destination Protocol Length Info
142.251.43.110 TLSv1.3 158 Application Data
142.251.43.110 TLSv1.3 654 Application Data
192.168.29.174 TCP 66 443 → 43718 [ACK] Seq=6644 Ack=1403 Win=267776 Len=0 TSval=22960
192.168.29.174 TLSv1.3 680 Application Data, Application Data
192.168.29.174 TLSv1.3 97 Application Data
192.168.29.174 TLSv1.3 642 Application Data
192.168.29.174 TLSv1.3 317 Application Data
192.168.29.174 TLSv1.3 97 Application Data
192.168.29.174 TLSv1.3 105 Application Data
142.251.43.110 TCP 66 43718 → 443 [ACK] Seq=1403 Ack=7258 Win=81152 Len=0 TSval=185719
142.251.43.110 TCP 66 43718 → 443 [ACK] Seq=1403 Ack=7289 Win=81152 Len=0 TSval=185719
142.251.43.110 TCP 66 43718 → 443 [ACK] Seq=1403 Ack=7865 Win=83968 Len=0 TSval=185719
142.251.43.110 TCP 66 43718 → 443 [ACK] Seq=1403 Ack=8116 Win=86656 Len=0 TSval=185719
142.251.43.110 TCP 66 43718 → 443 [ACK] Seq=1403 Ack=8147 Win=86656 Len=0 TSval=185719
142.251.43.110 TCP 66 43718 → 443 [ACK] Seq=1403 Ack=8186 Win=86656 Len=0 TSval=185719
142.251.43.110 TLSv1.3 97 Application Data
142.251.43.110 TLSv1.3 105 Application Data
192.168.29.174 TCP 66 443 → 43718 [ACK] Seq=8186 Ack=1473 Win=267776 Len=0 TSval=22960
2404:6800:4002:80b:… TCP 94 52696 → 443 [SYN] Seq=0 Win=64800 Len=0 MSS=1440 SACK_PERM TSval
142.251.43.100 TCP 74 60276 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval
192.168.29.174 TCP 74 443 → 60276 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1412 SACK
142.251.43.100 TCP 66 60276 → 443 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=184012517 TS
142.251.43.100 TLSv1.3 728 Client Hello (SNI=www.google.com)
192.168.29.174 TCP 66 443 → 60276 [ACK] Seq=1 Ack=663 Win=268288 Len=0 TSval=296719151
192.168.29.174 TLSv1.3 1466 Server Hello, Change Cipher Spec
142.251.43.100 TCP 66 60276 → 443 [ACK] Seq=663 Ack=1401 Win=67200 Len=0 TSval=1840125
192.168.29.174 TCP 1466 443 → 60276 [PSH, ACK] Seq=1401 Ack=663 Win=268288 Len=1400 TSva
192.168.29.174 TLSv1.3 1367 Application Data
142.251.43.100 TCP 66 60276 → 443 [ACK] Seq=663 Ack=2801 Win=70144 Len=0 TSval=1840125
142.251.43.100 TCP 66 60276 → 443 [ACK] Seq=663 Ack=4102 Win=72960 Len=0 TSval=1840125
142.250.77.227 OCSP 493 [TCP Previous segment not captured] Request
192.168.29.174 TCP 66 80 → 54872 [ACK] Seq=1 Ack=429 Win=1049 Len=0 TSval=3670956471
Frame 63: 493 bytes on wire (3944 bits), 493 bytes
Ethernet II, Src: PCSSystemtec_53:0d:f0 (08:00:27:
Internet Protocol Version 4, Src: 192.168.29.174,
Transmission Control Protocol, Src Port: 54866, Ds
Hypertext Transfer Protocol
Online Certificate Status Protocol
0000 b4 a7 c6 a6 1b 3c 08 00 27 53 0d f0 08 00
0010 01 df 05 19 40 00 40 06 78 cc c0 a8 1d ae
0020 4d e3 d6 52 00 50 0a 8e 9c 2a e1 8f ca 8a
0030 01 fc bd 05 00 00 01 01 08 0a 0e e8 26 b4
0040 24 71 50 4f 53 54 20 2f 77 72 32 20 48 54
0050 2f 31 2e 31 0d 0a 48 6f 73 74 3a 20 6f 2e
0060 69 2e 67 6f 6f 67 0d 0a 55 73 65 72 2d 41
0070 6e 74 3a 20 4d 6f 7a 69 6c 6c 61 2f 35 2e
0080 28 58 31 31 3b 20 4c 69 6e 75 78 20 78 38
0090 36 34 3b 20 72 76 3a 31 32 38 2e 30 29 20
Transmission Control Protocol: Protocol
Packets: 1476 · Displayed: 1195 (81.0%)
Profile: Default

4. Icmp


File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
icmp
Destination Protocol Length Info
8.8.8.8 ICMP 98 Echo (ping) request id=0x0001, seq=1/256, ttl=64 (reply in 8)
192.168.29.174 ICMP 98 Echo (ping) reply id=0x0001, seq=1/256, ttl=112 (request in 7)
8.8.8.8 ICMP 98 Echo (ping) request id=0x0001, seq=2/512, ttl=64 (reply in 14)
192.168.29.174 ICMP 98 Echo (ping) reply id=0x0001, seq=2/512, ttl=112 (request in 12
8.8.8.8 ICMP 98 Echo (ping) request id=0x0001, seq=3/768, ttl=64 (reply in 27)
192.168.29.174 ICMP 98 Echo (ping) reply id=0x0001, seq=3/768, ttl=112 (request in 25
8.8.8.8 ICMP 98 Echo (ping) request id=0x0001, seq=4/1024, ttl=64 (reply in 39)
192.168.29.174 ICMP 98 Echo (ping) reply id=0x0001, seq=4/1024, ttl=112 (request in 3
8.8.8.8 ICMP 98 Echo (ping) request id=0x0001, seq=5/1280, ttl=64 (reply in 42)
192.168.29.174 ICMP 98 Echo (ping) reply id=0x0001, seq=5/1280, ttl=112 (request in 4
8.8.8.8 ICMP 98 Echo (ping) request id=0x0001, seq=6/1536, ttl=64 (reply in 45)
192.168.29.174 ICMP 98 Echo (ping) reply id=0x0001, seq=6/1536, ttl=112 (request in 4
8.8.8.8 ICMP 98 Echo (ping) request id=0x0001, seq=7/1792, ttl=64 (reply in 85)
192.168.29.174 ICMP 98 Echo (ping) reply id=0x0001, seq=7/1792, ttl=112 (request in 7
8.8.8.8 ICMP 98 Echo (ping) request id=0x0001, seq=8/2048, ttl=64 (reply in 170)
192.168.29.174 ICMP 98 Echo (ping) reply id=0x0001, seq=8/2048, ttl=112 (request in 1
8.8.8.8 ICMP 98 Echo (ping) request id=0x0001, seq=9/2304, ttl=64 (reply in 744)
192.168.29.174 ICMP 98 Echo (ping) reply id=0x0001, seq=9/2304, ttl=112 (request in 6
8.8.8.8 ICMP 98 Echo (ping) request id=0x0001, seq=10/2560, ttl=64 (reply in 962
192.168.29.174 ICMP 98 Echo (ping) reply id=0x0001, seq=10/2560, ttl=112 (request in
8.8.8.8 ICMP 98 Echo (ping) request id=0x0001, seq=11/2816, ttl=64 (reply in 115
192.168.29.174 ICMP 98 Echo (ping) reply id=0x0001, seq=11/2816, ttl=112 (request in
8.8.8.8 ICMP 98 Echo (ping) request id=0x0001, seq=12/3072, ttl=64 (reply in 120
192.168.29.174 ICMP 98 Echo (ping) reply id=0x0001, seq=12/3072, ttl=112 (request in
8.8.8.8 ICMP 98 Echo (ping) request id=0x0001, seq=13/3328, ttl=64 (reply in 122
192.168.29.174 ICMP 98 Echo (ping) reply id=0x0001, seq=13/3328, ttl=112 (request in
8.8.8.8 ICMP 98 Echo (ping) request id=0x0001, seq=14/3584, ttl=64 (reply in 123
192.168.29.174 ICMP 98 Echo (ping) reply id=0x0001, seq=14/3584, ttl=112 (request in
8.8.8.8 ICMP 98 Echo (ping) request id=0x0001, seq=15/3840, ttl=64 (reply in 124
192.168.29.174 ICMP 98 Echo (ping) reply id=0x0001, seq=15/3840, ttl=112 (request in
8.8.8.8 ICMP 98 Echo (ping) request id=0x0001, seq=16/4096, ttl=64 (reply in 125
192.168.29.174 ICMP 98 Echo (ping) reply id=0x0001, seq=16/4096, ttl=112 (request in
Frame 1265: 98 bytes on wire (784 bits), 98 bytes
Ethernet II, Src: PCSSystemtec_53:0d:f0 (08:00:27:
Internet Protocol Version 4, Src: 192.168.29.174,
Internet Control Message Protocol
0000 b4 a7 c6 a6 1b 3c 08 00 27 53 0d f0 08 00 4
0010 00 54 4a be 40 00 40 01 01 85 c0 a8 1d ae 0
0020 08 08 08 00 9c bd 00 01 00 11 a8 64 de 68 0
0030 00 00 0f 90 06 00 00 00 00 00 10 11 12 13 1
0040 16 17 18 19 1a 1b 1c 1d 1e 1f 20 21 22 23 2
0050 26 27 28 29 2a 2b 2c 2d 2e 2f 30 31 32 33 3
0060 36 37