

Práctica de Captura de Tramas

Equipo: 5

Profesora: Leticia Henestrosa Carrasco

Cuestión 1

Wi-Fi

Archivo Edición Visualización Ir Captura Analizar Estadísticas Telefonía Wireless Herramientas Ayuda

ip.dst==192.168.0.17

No.	Time	Source	Destination	Protocol	Length	Info
15	0.004632	192.168.0.6	192.168.0.17	ICMP	98	Destination unreachable (Port unreachable)
16	0.004632	192.168.0.1	192.168.0.17	ICMP	98	Destination unreachable (Port unreachable)
17	0.009596	192.168.0.4	192.168.0.17	ICMP	98	Destination unreachable (Port unreachable)
18	0.009718	192.168.0.3	192.168.0.17	ICMP	98	Destination unreachable (Port unreachable)
19	0.013621	192.168.0.253	192.168.0.17	ICMP	98	Destination unreachable (Port unreachable)
20	0.014129	192.168.0.14	192.168.0.17	ICMP	98	Destination unreachable (Port unreachable)
21	0.021352	192.168.0.16	192.168.0.17	ICMP	98	Destination unreachable (Port unreachable)
22	0.026225	192.168.0.105	192.168.0.17	ICMP	98	Destination unreachable (Port unreachable)
23	0.066276	192.168.0.7	192.168.0.17	ICMP	70	Destination unreachable (Port unreachable)
28	0.772510	192.168.0.4	192.168.0.17	TCP	164	8009 → 52481 [PSH, ACK] Seq=1 Ack=111 Win=497 Len=110 [TCP segment of a reassembled PDU]
31	1.169795	192.168.0.14	192.168.0.17	TCP	164	8009 → 52416 [PSH, ACK] Seq=1 Ack=111 Win=547 Len=110 [TCP segment of a reassembled PDU]

> Frame 15: 98 bytes on wire (784 bits), 98 bytes captured (784 bits) on interface \Device\NPF_{B9E11750-4B79-4741-B87C-F93A589DC400}, id 0

> Ethernet II, Src: Phillips_7f:dd:9a (00:17:88:7f:dd:9a), Dst: CyberTAN_4d:e8:87 (00:45:e2:4d:e8:87)

> Internet Protocol Version 4, Src: 192.168.0.6, Dst: 192.168.0.17

> Internet Control Message Protocol

[Community ID: 1:3aRM-1ay1z8SwD4zy64Sg+R/9UE=]

> Spirent Test Center Signature

0000 00 45 e2 4d e8 87 00 17 88 7f dd 9a 00 00 45 c0 .E.M.....E.
0010 00 54 6c 2e 00 00 40 01 8c 53 c0 a8 00 06 c0 a8 .Tl...@..S.....
0020 00 11 03 03 7e 9a 00 00 00 00 45 00 00 38 f3 8dE..B..
0030 00 00 80 11 c5 bf c0 a8 00 11 c0 a8 00 06 ce 322
0040 00 06 00 24 4d 7c 00 01 08 00 06 04 00 01 00 45 ---\$M|...E..
0050 e2 4d e8 87 c0 a8 00 11 ff ff ff ff ff c0 a8 .M.....
0060 00 06 ..

Frame 98 bytes | Spirent Test Center Signature (20 bytes)

wreshark-Wi-Fi-RHAK1.pcapng Paquetes: 11288 · Mostrado: 9177 (81.3%) · Perdido: 0 (0.0%) Perfi: Default

Wi-Fi

Archivo Edición Visualización Ir Captura Analizar Estadísticas Telefonía Wireless Herramientas Ayuda

tcp

No.	Time	Source	Destination	Protocol	Length	Info
27	0.762283	192.168.0.17	192.168.0.4	TCP	164	52481 → 8009 [PSH, ACK] Seq=1 Ack=1 Win=254 Len=110 [TCP segment of a reassembled PDU]
28	0.772510	192.168.0.4	192.168.0.17	TCP	164	8009 → 52481 [PSH, ACK] Seq=1 Ack=111 Win=497 Len=110 [TCP segment of a reassembled PDU]
29	0.824596	192.168.0.17	192.168.0.4	TCP	54	52481 → 8009 [ACK] Seq=111 Ack=111 Win=253 Len=0
30	1.166635	192.168.0.17	192.168.0.14	TCP	164	52416 → 8009 [PSH, ACK] Seq=1 Ack=1 Win=255 Len=110 [TCP segment of a reassembled PDU]
31	1.169795	192.168.0.14	192.168.0.17	TCP	164	8009 → 52416 [PSH, ACK] Seq=1 Ack=111 Win=547 Len=110 [TCP segment of a reassembled PDU]
32	1.213419	192.168.0.17	192.168.0.14	TCP	54	52416 → 8009 [ACK] Seq=111 Ack=111 Win=254 Len=0
38	2.554742	192.168.0.17	192.168.0.3	TCP	164	52484 → 8009 [PSH, ACK] Seq=1 Ack=1 Win=253 Len=110 [TCP segment of a reassembled PDU]
39	2.562327	192.168.0.3	192.168.0.17	TCP	164	8009 → 52484 [PSH, ACK] Seq=1 Ack=111 Win=660 Len=110 [TCP segment of a reassembled PDU]
40	2.613179	192.168.0.17	192.168.0.3	TCP	54	52484 → 8009 [ACK] Seq=111 Ack=111 Win=253 Len=0
41	3.089763	192.168.0.17	13.107.6.171	TLSv1.2	656	Application Data
42	3.089845	192.168.0.17	13.107.6.171	TLSv1.2	100	Application Data

> Frame 28: 164 bytes on wire (1312 bits), 164 bytes captured (1312 bits) on interface \Device\NPF_{B9E11750-4B79-4741-B87C-F93A589DC400}, id 0

> Ethernet II, Src: Google_d1:45:8a (44:07:0b:d1:45:8a), Dst: CyberTAN_4d:e8:87 (00:45:e2:4d:e8:87)

> Internet Protocol Version 4, Src: 192.168.0.4, Dst: 192.168.0.17

> Transmission Control Protocol, Src Port: 8009, Dst Port: 52481, Seq: 1, Ack: 111, Len: 110

[Community ID: 1:0/UdAUsAFFE4JTh7nmGvaB+9s8=]

0000 00 45 e2 4d e8 87 44 07 0b d1 45 8a 00 00 45 00 .E.M.D...E..
0010 00 96 50 ac 40 00 40 06 68 50 c0 a8 00 04 c0 a8 .P.@..hP.....
0020 00 11 1f 49 cd 01 29 fe 44 27 ac 5d 9d 7e 50 18 ...I.:)D']..P..
0030 01 f1 65 ac 00 00 17 03 03 00 69 da b9 e5 c5 f5 ..e.....i...
0040 b9 49 26 d8 4f 17 8b d7 25 6d 8f 3f ba fc 85 3c .I&O...%m?....
0050 8d cb 01 d1 03 91 9e 5b 48 ef 28 4c a1 39 88 2d[H(L-9-..
0060 00 a0 5e 85 30 74 0a 08 da 0d a2 ab 8f bd a2 3c ..^0t.....
0070 94 81 60 11 1a 7d 97 3a 23 a9 75 5e 09 14 de 1e .:~):#uP....
0080 b1 68 43 62 c4 f7 3f 3e 0a 1a 5a b7 7f 87 68 a6 .hCb-?>..Z...h..
0090 b0 7c ad b6 83 9b f6 52 5b 0b 9a b7 95 d7 08 2b .].....R[.....+
00a0 7c c8 6e 5d .n]

Transmission Control Protocol: Protocol Paquetes: 11288 · Mostrado: 1142 (10.1%) · Perdido: 0 (0.0%) Perfi: Default

Cuestión 3

The screenshot shows the Wireshark interface with a packet capture on the interface `\Device\NPF_{B9E11750-4B79-4741-B87C-F93A5890C40D}`. The packet list shows 16 packets. The selected packet is packet 1, which is a TLSv1.2 packet (229 bytes) from 192.168.0.17 to 192.168.0.17. The packet details pane shows the following structure:

- Frame 1: 229 bytes on wire (1832 bits), 229 bytes captured (1832 bits) on interface `\Device\NPF_{B9E11750-4B79-4741-B87C-F93A5890C40D}`, id 0
- Ethernet II, Src: ARRISGn_16:62:a4 (9c:c8:fc:16:62:a4), Dst: CyberTAN_4d:e8:87 (00:45:e2:4d:e8:87)
- Internet Protocol Version 4, Src: 192.168.0.17, Dst: 192.168.0.17
- Transmission Control Protocol, Src Port: 443, Dst Port: 56001, Seq: 1, Ack: 1, Len: 175
- Transport Layer Security
[Community ID: 1:01qfU1/0zt7KMDWIFmkBEDQ+KZQ=]

The packet bytes pane shows the raw data in hexadecimal and ASCII:

```
0000 00 45 e2 4d e8 87 9c c8 fc 16 62 a4 08 00 45 00  :E-M....b...E-
0010 00 d7 aa ef 40 00 68 06 86 b8 28 53 f7 6c c0 a8  :...@h...{S1..
0020 00 11 01 bb da c1 33 06 69 4b 27 10 bb 72 50 18  :....3 IK'..rP-
0030 1d 98 ea 9d 00 00 17 03 03 00 aa 00 00 00 00 00  :.....
0040 00 01 88 7f c8 42 9b c5 1a a2 19 eb 35 37 33 82  :....B....573-
0050 bd 05 30 6a 7a 10 0c 05 28 c6 11 e0 29 b6 45 a2  :..0jz...(-)-E-
0060 a5 35 b7 0d ac bf 8f 6b 91 cb 45 e1 a2 fe 74 18  :5....k...E...t-
0070 86 4a 3c 25 3f 48 7a 8f 49 a2 74 00 d4 a8 85 41  :Jc%Hz: I t...A
0080 d8 21 25 74 ce 6f 3c 2c b7 6b 6a d2 c2 ff 84 db  :!Xt-oc..kj.....
0090 8b 43 cb 60 f3 b2 e9 31 74 13 7e 2f da 26 44 fd  :C...1 t.../8D-
00a0 57 36 e4 a3 d6 0b d2 9a 2e 87 76 b9 79 45 5f dc  :M6.....v-yE..-
00b0 44 8a 8f 3e 74 8d 5a 42 55 a7 f7 aa 85 ae 7f 6d  :D...xt:2B U.....m
00c0 1d a1 7d c5 84 e2 48 0b 1f dd 75 b8 b0 13 e9 66  :...)..H...u....f
00d0 33 dd 12 11 de 7a e5 63 bd 63 e1 30 47 79 e8 a5  :3...z-c..c-0Gy..
00e0 60 ec 47 c6 cc
```

The screenshot shows the Wireshark interface with a packet capture on the interface `\Device\NPF_{B9E11750-4B79-4741-B87C-F93A5890C40D}`. The packet list shows 31 packets. The selected packet is packet 1, which is a TLSv1.2 packet (229 bytes) from 192.168.0.17 to 192.168.0.17. The packet details pane shows the following structure:

- Frame 1: 229 bytes on wire (1832 bits), 229 bytes captured (1832 bits) on interface `\Device\NPF_{B9E11750-4B79-4741-B87C-F93A5890C40D}`, id 0
- Ethernet II, Src: ARRISGn_16:62:a4 (9c:c8:fc:16:62:a4), Dst: CyberTAN_4d:e8:87 (00:45:e2:4d:e8:87)
- Internet Protocol Version 4, Src: 192.168.0.17, Dst: 192.168.0.17
- Transmission Control Protocol, Src Port: 443, Dst Port: 56001, Seq: 1, Ack: 1, Len: 175
- Transport Layer Security
[Community ID: 1:01qfU1/0zt7KMDWIFmkBEDQ+KZQ=]

The packet bytes pane shows the raw data in hexadecimal and ASCII:

```
0000 00 45 e2 4d e8 87 9c c8 fc 16 62 a4 08 00 45 00  :E-M....b...E-
0010 00 d7 aa ef 40 00 68 06 86 b8 28 53 f7 6c c0 a8  :...@h...{S1..
0020 00 11 01 bb da c1 33 06 69 4b 27 10 bb 72 50 18  :....3 IK'..rP-
0030 1d 98 ea 9d 00 00 17 03 03 00 aa 00 00 00 00 00  :.....
0040 00 01 88 7f c8 42 9b c5 1a a2 19 eb 35 37 33 82  :....B....573-
0050 bd 05 30 6a 7a 10 0c 05 28 c6 11 e0 29 b6 45 a2  :..0jz...(-)-E-
0060 a5 35 b7 0d ac bf 8f 6b 91 cb 45 e1 a2 fe 74 18  :5....k...E...t-
0070 86 4a 3c 25 3f 48 7a 8f 49 a2 74 00 d4 a8 85 41  :Jc%Hz: I t...A
0080 d8 21 25 74 ce 6f 3c 2c b7 6b 6a d2 c2 ff 84 db  :!Xt-oc..kj.....
0090 8b 43 cb 60 f3 b2 e9 31 74 13 7e 2f da 26 44 fd  :C...1 t.../8D-
00a0 57 36 e4 a3 d6 0b d2 9a 2e 87 76 b9 79 45 5f dc  :M6.....v-yE..-
00b0 44 8a 8f 3e 74 8d 5a 42 55 a7 f7 aa 85 ae 7f 6d  :D...xt:2B U.....m
00c0 1d a1 7d c5 84 e2 48 0b 1f dd 75 b8 b0 13 e9 66  :...)..H...u....f
00d0 33 dd 12 11 de 7a e5 63 bd 63 e1 30 47 79 e8 a5  :3...z-c..c-0Gy..
00e0 60 ec 47 c6 cc
```

Cuestión 4

Wi-Fi

Archivo Edición Visualización Ir Captura Analizar Estadísticas Telefonía Wireless Herramientas Ayuda

ip.dst==192.168.0.17

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	40.83.247.108	192.168.0.17	TLSv1.2	229	Application Data
2	0.052219	192.168.0.17	40.83.247.108	TCP	54	56001 → 443 [ACK] Seq=1 Ack=176 Win=257 Len=0
3	0.063660	192.168.0.100	224.0.0.251	MDNS	136	Standard query 0x000b PTR _X95E7C8F47989526C9BCD95D24884F6F0827C5ED._sub._googlecast._tcp.local, "QM" ques...
4	0.115894	192.168.0.17	192.168.0.3	TCP	164	52484 → 8009 [PSH, ACK] Seq=1 Ack=1 Win=254 Len=110 [TCP segment of a reassembled PDU]
6	0.188845	192.168.0.3	192.168.0.17	TCP	164	8009 → 52484 [PSH, ACK] Seq=1 Ack=111 Win=660 Len=110 [TCP segment of a reassembled PDU]
7	0.240728	192.168.0.17	192.168.0.3	TCP	54	52484 → 8009 [ACK] Seq=111 Ack=111 Win=253 Len=0
8	0.289062	192.168.0.14	224.0.0.251	MDNS	400	Standard query response 0x0000 PTR Chromecast-cc495ec4f7df32866be36c989030eac5._googlecast._tcp.local TXT, -
13	0.670761	192.168.0.3	239.255.255.250	SSDP	162	M-SEARCH * HTTP/1.1
14	0.755172	192.168.0.17	52.114.133.205	TLSv1.2	111	Application Data
15	0.763889	192.168.0.3	239.255.255.250	SSDP	162	M-SEARCH * HTTP/1.1
16	0.859993	52.114.133.205	192.168.0.17	TLSv1.2	100	Application Data

> Frame 1: 229 bytes on wire (1832 bits), 229 bytes captured (1832 bits) on interface \Device\NPF_{B9E11750-4879-4741-B87C-F93A5890C400}, id 0

> Ethernet II, Src: ARRIS6n_16:62:a4 (9c:c8:fc:16:62:a4), Dst: CyberTAN_4d:e8:87 (00:45:e2:4d:e8:87)

> Internet Protocol Version 4, Src: 40.83.247.108, Dst: 192.168.0.17

> Transmission Control Protocol, Src Port: 443, Dst Port: 56001, Seq: 1, Ack: 1, Len: 175

> Transport Layer Security
[Community ID: 1:01QFUI/0Zt7KNDWIFmk8EdQ+KZQ=]

0000 00 45 e2 4d e8 87 9c 8c fc 16 62 a4 08 00 45 00 ·E·M·····b·····E·
0010 00 d7 aa ef 40 00 68 06 86 b8 28 53 f7 6c c0 a8 ····@·h···(S·L·
0020 00 11 01 bb da c1 33 06 69 4b 27 10 bb 72 50 18 ······3·iK'···rP·
0030 1d 98 ea 9d 00 00 17 03 03 00 aa 00 00 00 00 00 ······
0040 00 01 88 7f c8 42 9b c5 1a a2 19 eb 35 37 33 82 ····B·····573·
0050 bd 05 30 6a 7a 10 0c 05 28 c5 11 e0 29 b6 45 a2 ··0jz···(···)E·
0060 a5 35 b7 0d ac bf 8f 6b 91 cb 45 e1 a2 fe 74 18 5·····k·E···t·
0070 86 4a 3c 25 3f 48 7a 8f 49 a2 74 00 4a 85 41 ·J·c%Hz·I·t·····A
0080 d8 21 25 74 ce 6f 3c 2c b7 6b 6a d2 c2 ff 84 db ·!%t·oc·,·k·j·····
0090 8b 43 cb 60 f3 b2 e9 31 74 13 7e 2f da 26 44 fd ·C'·····1·t·-/·&D·
00a0 57 36 e4 a3 d6 00 d2 9a 2e 87 76 b9 79 45 5f dc HG····· ··v·yE·
00b0 44 8a 8f 3e 7d 8d 5a 42 55 a7 f7 aa 85 ae 7f 6d D·>t·2B·U·····m
00c0 1d a1 7d c5 84 e2 48 0b 1f dd 75 b8 b0 13 e9 66 ··}···H· ·u·····f
00d0 33 dd 12 11 de 7a e5 63 bd 63 e1 30 47 79 e8 a5 3·····z·c·c·0Gy·

Internet Protocol Version 4: Protocol Paquetes: 561 · Mostrado: 553 (98.6%) · Perdido: 0 (0.0%) Perfil: Default

Wi-Fi

Archivo Edición Visualización Ir Captura Analizar Estadísticas Telefonía Wireless Herramientas Ayuda

http

No.	Time	Source	Destination	Protocol	Length	Info
6449	54.547300	192.168.0.17	72.21.91.29	HTTP	290	GET /_HFEWtZBHMEswSTA78glUrDg%KCGuABBSAUQYBhq2awm1Rh6Doh%2Fs8YgFV7gQUA95QNVbRTLtw8KP1gxvD17I98VUCEAH9o%28tuyxXIiEOl...
6456	54.669086	72.21.91.29	192.168.0.17	OCSP	853	Response

Httpertext Transfer Protocol: Protocol Paquetes: 9405 · Mostrado: 2 (0.0%) · Perdido: 0 (0.0%) Perfil: Default