

SECCIÓN TCP:

1. Captura de paquetes

Capturando desde Adapter for loopback traffic capture

ArchivoEdiciónVisualizaciónIr aCapturaAnalizarEstadísticasTelefoníaWirelessHerramientasAyuda

tcp.port==3000

No.	Time	Source	Destination	Protocol	Length	Info
48	12.457009	127.0.0.1	127.0.0.1	TCP	56	14997 → 3000 [SYN] Seq=0 Win=65535 Len=0 MSS=65495 WS=256 SACK_PERM
49	12.457074	127.0.0.1	127.0.0.1	TCP	56	3000 → 14997 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=65495 WS=256 SACK_PERM
50	12.457102	127.0.0.1	127.0.0.1	TCP	44	14997 → 3000 [ACK] Seq=1 Ack=1 Win=2619648 Len=0
156	38.962269	127.0.0.1	127.0.0.1	TCP	72	14997 → 3000 [PSH, ACK] Seq=1 Ack=1 Win=2619648 Len=28
157	38.962297	127.0.0.1	127.0.0.1	TCP	44	3000 → 14997 [ACK] Seq=1 Ack=29 Win=2619648 Len=0
158	38.990496	127.0.0.1	127.0.0.1	TCP	68	3000 → 14997 [PSH, ACK] Seq=1 Ack=29 Win=2619648 Len=24
159	38.990519	127.0.0.1	127.0.0.1	TCP	44	14997 → 3000 [ACK] Seq=29 Ack=25 Win=2619648 Len=0
182	45.208994	127.0.0.1	127.0.0.1	TCP	50	14997 → 3000 [PSH, ACK] Seq=29 Ack=25 Win=2619648 Len=6
183	45.209021	127.0.0.1	127.0.0.1	TCP	44	3000 → 14997 [ACK] Seq=25 Ack=35 Win=2619648 Len=0
184	45.209435	127.0.0.1	127.0.0.1	TCP	50	3000 → 14997 [PSH, ACK] Seq=25 Ack=35 Win=2619648 Len=6
185	45.209454	127.0.0.1	127.0.0.1	TCP	44	14997 → 3000 [ACK] Seq=35 Ack=31 Win=2619648 Len=0
186	45.210457	127.0.0.1	127.0.0.1	TCP	44	14997 → 3000 [FIN, ACK] Seq=35 Ack=31 Win=2619648 Len=0
187	45.210476	127.0.0.1	127.0.0.1	TCP	44	3000 → 14997 [ACK] Seq=31 Ack=36 Win=2619648 Len=0
188	45.210686	127.0.0.1	127.0.0.1	TCP	44	3000 → 14997 [FIN, ACK] Seq=31 Ack=36 Win=2619648 Len=0
189	45.210701	127.0.0.1	127.0.0.1	TCP	44	14997 → 3000 [ACK] Seq=36 Ack=32 Win=2619648 Len=0

Arrival Time: Aug 7, 2024 15:26:07.421892000 Hora estándar, América Central
UTC Arrival Times Aug 7, 2024 21:26:07.421892000 UTC
Epoch Arrival Time: 1723065967.421892000
[Time shift for this packet: 0.000000000 seconds]
[Time delta from previous captured frame: 0.163943000 seconds]
[Time delta from previous displayed frame: 0.000000000 seconds]
[Time since reference or first frame: 12.457009000 seconds]
Frame Number: 48
Frame Length: 56 bytes (448 bits)
Capture Length: 56 bytes (448 bits)
[Frame is marked: False]
[Frame is ignored: False]
[Protocols in frame: null:ip:tcp]
[Coloring Rule Name: TCP SYN/FIN]
[Coloring Rule String: tcp.flags & 0x02 || tcp.flags.fin == 1]
▼ Null/Loopback
Family: IP (2)
▼ Internet Protocol Version 4, Src: 127.0.0.1, Dst: 127.0.0.1
0100 = Version: 4
... 0101 = Header Length: 20 bytes (5)
► Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
Total Length: 52
Identification: 0xbdc7 (48583)
► 010. = Flags: 0x2, Don't fragment
...0 0000 0000 0000 = Fragment Offset: 0
Time to Live: 128
Protocol: TCP (6)
Header Checksum: 0x0000 [validation disabled]

0000 02 00 00 00 45 00 00 34 bd c7 40 00 00 06 80 80 ...E...4 ..@...
0010 7f 00 00 01 7f 00 00 01 3a 95 0b b8 c7 7d fd 65:..} e
0020 00 00 00 00 80 02 ff ff 6b b9 00 00 02 04 ff d7k
0030 01 03 03 08 01 01 04 02

Paquetes: 209 - Mostrador: 15 (7.2%)

Perfil: Default

03:26 p.m.
7/8/2024

2. Análisis de encabezados

No.	Source	Destination	Length	Flags	Seq	Ack	Win	Len	MSS	WS	SACK_PERM
48	14997	3000	56	SYN	0		65535	0	65495	256	SACK_PERM
49	3000	14997	56	SYN, ACK	0	1	65535	0	65495	256	SACK_PERM
50	14997	3000	44	ACK	1	1	2619648	0			
156	14997	3000	72	PSH, ACK	1	1	2619648	28			
157	3000	14997	44	ACK	1	29	2619648	0			
158	3000	14997	68	PSH, ACK	1	29	2619648	24			
159	14997	3000	44	ACK	29	25	2619648	0			
182	14997	3000	50	PSH, ACK	29	25	2619648	6			
183	3000	14997	44	ACK	25	35	2619648	0			
184	3000	14997	50	PSH, ACK	25	35	2619648	6			
185	14997	3000	44	ACK	35	31	2619648	0			
186	14997	3000	44	FIN, ACK	35	31	2619648	0			
187	3000	14997	44	ACK	31	36	2619648	0			
188	3000	14997	44	FIN, ACK	31	36	2619648	0			
189	14997	3000	44	ACK	36	32	2619648	0			

14997 -> Client

3000 -> Server

3. Preguntas de análisis

¿Cuál es el número de secuencia (Sequence Number) inicial y final de la conexión? ¿Hace sentido que sean esa cantidad, por qué?

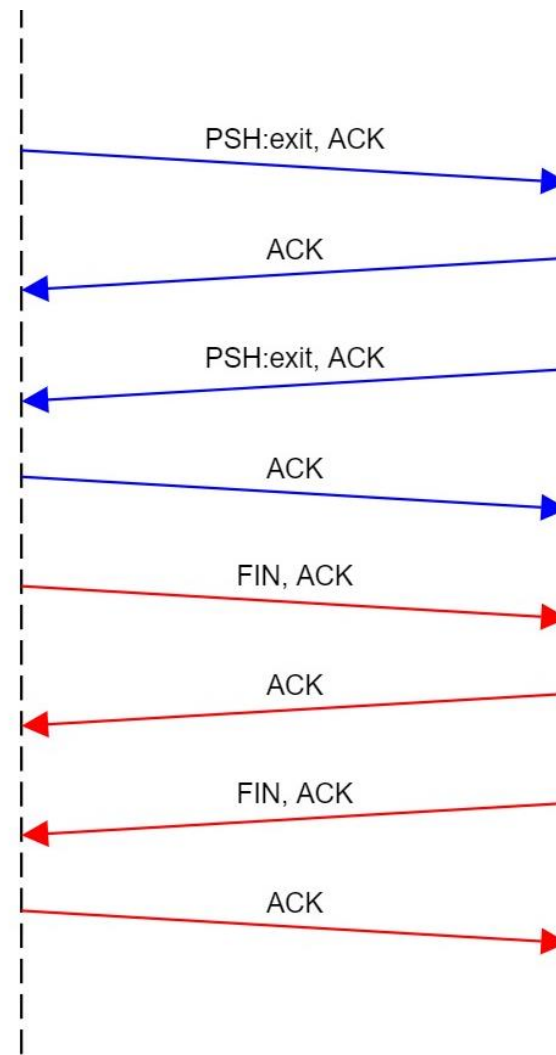
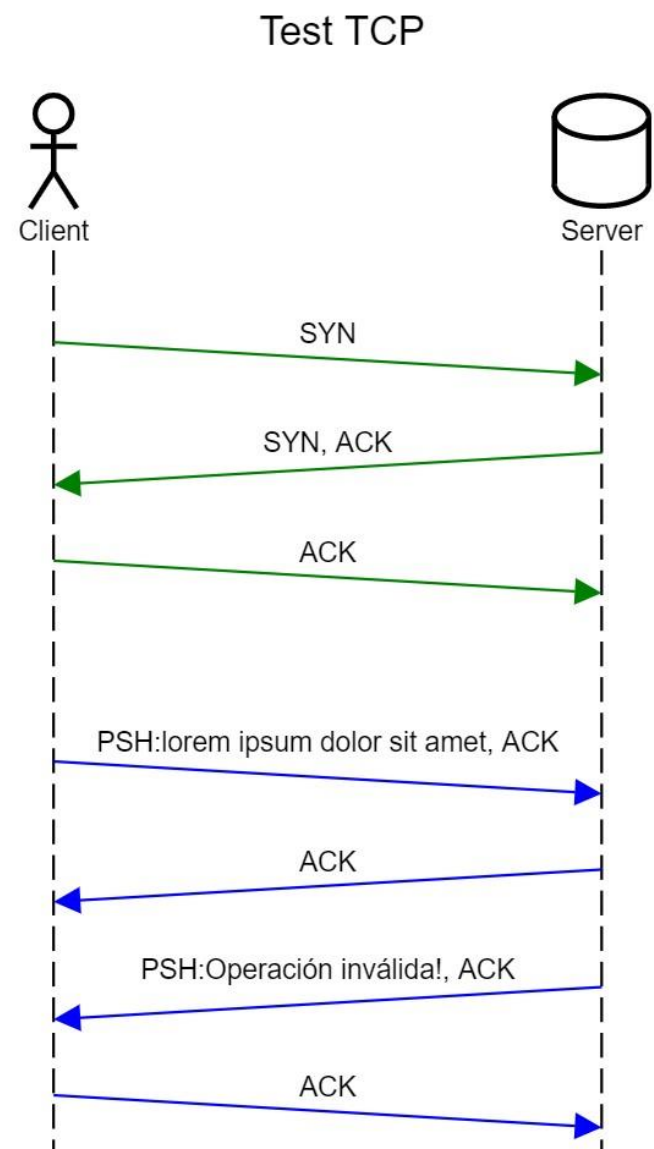
Seq inicial es 0. Seq final es 36 (31 para Server).

Sí tiene sentido, según lo que investigué, el Seq es el número de información que se ha mandado acumulado. Esta comienza en 0, vemos que con el primer mensaje aumenta a 1, cuando el cliente envía 28 el siguiente seq de cliente es 29 y el ack de server también. Y cuando el server manda length 24, el ack del cliente es 25 y el siguiente seq del server es 25. Y así continúa hasta cerrar la conexión.

¿Se enviaron 4 mensajes, por lo cual solo deben de existir 4 paquetes con DATA? ¿Es eso correcto o existen más paquetes?

Sí. Los únicos 4 paquetes con DATA deberían ser los mensajes de: Lorem Ipsum...; Operación inválida! ; exit ; exit ;

4. Diagrama Secuencial



Sección UDP:

1. Captura de paquetes

The screenshot displays the Wireshark network protocol analyzer interface. The title bar indicates the capture is on a loopback interface. The menu bar includes options like Archivo, Edición, Visualización, Ir, Captura, Analizar, Estadísticas, Telefonía, Wireless, Herramientas, and Ayuda. The toolbar contains various icons for file operations, capture control, and analysis. The packet list pane shows four captured packets, with the fourth packet (No. 60) selected. The packet details pane provides a hierarchical view of the selected packet's structure, showing the User Datagram Protocol (UDP) header and the Distributed Interactive Simulation (DIS) header. The packet bytes pane displays the raw data of the selected packet in hexadecimal and ASCII formats. The status bar at the bottom indicates that 73 packets are shown, with 4 (5.5%) displayed and 0 (0.0%) lost.

No.	Time	Source	Destination	Protocol	Length	Info
47	12.758906	127.0.0.1	127.0.0.1	DIS	58	PDUType: 114 \t Unknown
48	12.785057	127.0.0.1	127.0.0.1	DIS	54	PDUType: 101 \t Unknown
59	15.748362	127.0.0.1	127.0.0.1	UDP	36	52943 → 3000 Len=4
60	15.748790	127.0.0.1	127.0.0.1	UDP	36	3000 → 52943 Len=4

Protocol: UDP (17)
Header Checksum: 0x0000 [validation disabled]
[Header checksum status: Unverified]
Source Address: 127.0.0.1
Destination Address: 127.0.0.1

▼ User Datagram Protocol, Src Port: 52943, Dst Port: 3000
Source Port: 52943
Destination Port: 3000
Length: 34
Checksum: 0x9fb9 [unverified]
[Checksum Status: Unverified]
[Stream index: 0]
▶ [Timestamps]
UDP payload (26 bytes)

▼ Distributed Interactive Simulation
▼ Header
Proto version: Unknown (108)
Exercise ID: 111
PDU type: Unknown (114)
Proto Family: Unknown (101)
Timestamp: 25:34.592937 (relative)
PDU Length: 29557
▶ PDU Status: 0x6d

0000 02 00 00 00 45 00 00 36 1a 4b 00 00 80 11 00 00E..K.....
0010 7f 00 00 01 7f 00 00 01 ce cf 0b b8 00 22 9f b9 ".....
0020 6c 6f 72 65 6d 20 69 70 73 75 6d 20 64 6f 6c 6f lorem ip sum dolo
0030 72 20 73 69 74 20 61 6d 65 74 r sit am et

Paquetes: 73 - Mostrado: 4 (5.5%) - Perdido: 0 (0.0%) Perfil: Default

2. Análisis de encabezados

No.	Source	Destination	Length	Len	Checksum	Data
47	52943	3000	58	34	0x9fb9	lorem ipsum dolor sit amet
48	3000	52943	54	30	0x816b	Operación no válida!
59	52943	3000	36	4	0x585f	exit
60	3000	52943	36	4	0x585f	Exit

14997 -> Client

3000 -> Server

3. Preguntas de análisis

¿Se generó algún ICMP durante la transmisión? ¿Podría generarse alguno?

Se colocó el filtro “udp.port==3000 || icmp” para verificar si había algún ICMP, pero tampoco apareció ningún paquete nuevo.

Según la captura, ¿los paquetes tenían el mismo length? Si no, ¿cuál piensa que sea el motivo?

No tenían el mismo length ya que el mensaje (data) no tiene el mismo length. Pero vemos que mensajes con el mismo tamaño (exit) ambos tienen el mismo length ya que tienen el mismo contenido.

Sección ICMP

1. Captura de paquetes

Tracert google.com ----- Port Unreachable, Host unreachable, Time-to-live exceeded

The image shows a Wireshark packet capture window. The top menu bar includes Archivo, Edición, Visualización, Ir, Captura, Analizar, Estadísticas, Telefonía, Wireless, Herramientas, and Ayuda. The filter bar shows 'icmp || udp && !dns && !quic && !mdns && !mns && !lmmn'. The packet list pane displays a table of captured packets:

No.	Time	Source	Destination	Protocol	Length	Info
3586	49.596771	10.1.0.1	10.1.14.182	ICMP	134	Time-to-live exceeded (Time to live exceeded in transit)
3588	49.598101	10.1.14.182	192.178.52.142	ICMP	106	Echo (ping) request id=0x0001, seq=315/15105, ttl=1 (no response found!)
3590	49.601461	10.1.0.1	10.1.14.182	ICMP	134	Time-to-live exceeded (Time to live exceeded in transit)
3907	53.359397	0.0.0.0	255.255.255.255	DHCP	342	DHCP Request - Transaction ID 0x5653ab23
3962	53.973101	0.0.0.0	255.255.255.255	DHCP	364	DHCP Request - Transaction ID 0xc27868cf
4066	55.185629	10.1.14.182	192.178.52.142	ICMP	106	Echo (ping) request id=0x0001, seq=316/15361, ttl=2 (no response found!)
4067	55.189889	10.240.40.249	10.1.14.182	ICMP	134	Time-to-live exceeded (Time to live exceeded in transit)
4068	55.190507	10.1.14.182	192.178.52.142	ICMP	106	Echo (ping) request id=0x0001, seq=317/15617, ttl=2 (no response found!)
4069	55.195697	10.240.40.249	10.1.14.182	ICMP	134	Time-to-live exceeded (Time to live exceeded in transit)
4070	55.196249	10.1.14.182	192.178.52.142	ICMP	106	Echo (ping) request id=0x0001, seq=318/15873, ttl=2 (no response found!)
4071	55.199005	10.240.40.249	10.1.14.182	ICMP	134	Time-to-live exceeded (Time to live exceeded in transit)
4085	55.235631	10.240.40.249	10.1.14.182	ICMP	120	Destination unreachable (Port unreachable)
4123	55.720607	10.1.0.1	10.1.14.182	ICMP	94	Destination unreachable (Host unreachable)
4173	56.178909	fe80::c293:fdbb::...	ff02::1:2	DHCPv6	157	Solicit XID: 0xdfe567 CID: 0001000127b3cc8e8c04ba9a6180
4216	56.742644	10.240.40.249	10.1.14.182	ICMP	120	Destination unreachable (Port unreachable)
4332	58.249681	10.240.40.249	10.1.14.182	ICMP	120	Destination unreachable (Port unreachable)
4389	58.889037	10.1.5.240	239.255.255.250	SSDP	217	M-SEARCH * HTTP/1.1
4540	60.115863	10.1.5.240	239.255.255.250	SSDP	217	M-SEARCH * HTTP/1.1
4591	60.763079	10.1.14.182	192.178.52.142	ICMP	106	Echo (ping) request id=0x0001, seq=319/16129, ttl=3 (no response found!)
4592	60.766490	10.200.100.8	10.1.14.182	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
4593	60.767531	10.1.14.182	192.178.52.142	ICMP	106	Echo (ping) request id=0x0001, seq=320/16385, ttl=3 (no response found!)
4594	60.769542	10.200.100.8	10.1.14.182	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
4595	60.770393	10.1.14.182	192.178.52.142	ICMP	106	Echo (ping) request id=0x0001, seq=321/16641, ttl=3 (no response found!)
4597	60.772172	10.200.100.8	10.1.14.182	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
4616	61.039843	10.1.5.240	239.255.255.250	SSDP	217	M-SEARCH * HTTP/1.1

A red arrow points to the packet at time 55.235631, which is a 'Destination unreachable (Port unreachable)' message. The packet details pane shows the following information:

- Frame 610: 46 bytes on wire (368 bits), 46 bytes captured (368 bits) on interface \Device\NPF_{AF74CD52-7607-40E6-96D6-9BF8368C79CD}
- Ethernet II, Src: Intel_f2:f3:19 (7c:b2:7d:f2:f3:19), Dst: Ubiquiti_44:3c:93 (18:e8:29:44:3c:93)
- Internet Protocol Version 4, Src: 10.1.14.182, Dst: 158.120.24.222
- User Datagram Protocol, Src Port: 51978, Dst Port: 19281
- Data (4 bytes)

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

```
0000 18 e8 29 44 3c 93 7c b2 7d f2 f3 19 08 00 45 00 ..)D<.|.|.....E
0010 00 20 c8 50 00 00 40 11 00 00 0a 01 0e b6 9e 78 . P-@.....x
0020 18 de cb 0a 4b 51 00 0c d0 2a f1 d5 18 db ....KQ...*....
```

The status bar at the bottom indicates 'Paquetes: 4660 - Mostrado: 67 (1.4%)' and 'Perfil: Default'. The system clock shows '08:18 p.m. 7/8/2024'.

ping google.com ----- Echo Reply y Request

Capturando desde Wi-Fi

Archivo Edición Visualización Ir Captura Analizar Estadísticas Telefonía Wireless Herramientas Ayuda

icmp || udp && !dns && !quic && !mDNS && !nbs && !llmnr

No.	Time	Source	Destination	Protocol	Length	Info
3	0.041961	10.1.15.34	239.255.255.250	SSDP	217	M-SEARCH * HTTP/1.1
39	1.054036	10.1.15.34	239.255.255.250	SSDP	217	M-SEARCH * HTTP/1.1
52	1.225098	10.1.15.34	255.255.255.255	DB-LS...	243	Dropbox LAN sync Discovery Protocol, JSON
53	1.228940	10.1.15.34	10.1.255.255	DB-LS...	243	Dropbox LAN sync Discovery Protocol, JSON
212	5.648405	10.1.14.182	142.250.189.142	ICMP	74	Echo (ping) request id=0x0001, seq=19/4864, ttl=128 (reply in 213)
213	5.673419	142.250.189.142	10.1.14.182	ICMP	74	Echo (ping) reply id=0x0001, seq=19/4864, ttl=117 (request in 212)
243	6.666090	10.1.14.182	142.250.189.142	ICMP	74	Echo (ping) request id=0x0001, seq=20/5120, ttl=128 (reply in 245)
245	6.691015	142.250.189.142	10.1.14.182	ICMP	74	Echo (ping) reply id=0x0001, seq=20/5120, ttl=117 (request in 243)
247	6.703020	10.1.8.44	239.255.255.250	SSDP	217	M-SEARCH * HTTP/1.1
278	7.670658	10.1.14.182	142.250.189.142	ICMP	74	Echo (ping) request id=0x0001, seq=21/5376, ttl=128 (reply in 280)
280	7.695616	142.250.189.142	10.1.14.182	ICMP	74	Echo (ping) reply id=0x0001, seq=21/5376, ttl=117 (request in 278)
282	7.707402	10.1.8.44	239.255.255.250	SSDP	217	M-SEARCH * HTTP/1.1
309	8.684522	10.1.14.182	142.250.189.142	ICMP	74	Echo (ping) request id=0x0001, seq=22/5632, ttl=128 (reply in 311)
310	8.707824	10.1.8.44	239.255.255.250	SSDP	217	M-SEARCH * HTTP/1.1
311	8.709957	142.250.189.142	10.1.14.182	ICMP	74	Echo (ping) reply id=0x0001, seq=22/5632, ttl=117 (request in 309)
315	8.903749	10.1.14.182	10.1.255.255	UDP	86	57621 → 57621 Len=44
332	9.711823	10.1.8.44	239.255.255.250	SSDP	217	M-SEARCH * HTTP/1.1

Frame 3: 217 bytes on wire (1736 bits), 217 bytes captured (1736 bits) on interface \Device\NPF_{AF74CD52-7607-40E6-96D6-9BF8368C79C}

Ethernet II, Src: Dell_38:eb:32 (50:9a:4c:38:eb:32), Dst: IPv4mcast_7f:ff:fa (01:00:5e:7f:ff:fa)

Internet Protocol Version 4, Src: 10.1.15.34, Dst: 239.255.255.250

User Datagram Protocol, Src Port: 62813, Dst Port: 1900

Simple Service Discovery Protocol

0000 01 00 5e 7f ff fa 50 9a 4c 38 eb 32 08 00 45 00 ... ^...P: L8 2: E-
0010 00 cb 45 cf 00 00 01 11 6a 36 0a 01 0f 22 ef ff ... E.... j6..."
0020 ff fa f5 5d 07 6c 00 b7 71 f6 4d 2d 53 45 41 52 ...] 1... q M-SEAR
0030 43 48 20 2a 20 48 54 54 50 2f 31 2e 31 0d 0a 48 CH * HTTP/1.1. H
0040 4f 53 54 3a 20 32 33 39 2e 32 35 35 2e 32 35 35 OST: 239.255.255
0050 2e 32 35 30 3a 31 39 30 30 0d 0a 4d 41 4e 3a 20 .250:190 0- MAN:
0060 22 73 73 64 70 3a 64 69 73 63 6f 76 65 72 22 0d "ssdp:discover"
0070 0a 4d 58 3a 20 31 0d 0a 53 54 3a 20 75 72 6e 3a MX: 1- ST: urn:
0080 64 69 61 6c 2d 6d 75 6c 74 69 73 63 72 65 65 6e dial-multiscreen
0090 2d 6f 72 67 3a 73 65 72 76 69 63 65 3a 64 69 61 -org:service:dia
00a0 6c 3a 31 0d 0a 55 53 45 52 2d 41 47 45 4e 54 3a 1:1- USER-AGENT:
00b0 20 4d 69 63 72 6f 73 6f 66 74 20 45 64 67 65 2f Microso ft Edge/
00c0 31 32 37 2e 30 2e 32 36 35 31 2e 39 38 20 57 69 127.0.26 51.98 Wi
00d0 6e 64 6f 77 73 0d 0a 0d 0a ndows...

Wi-Fi: <live capture in progress>

Paquetes: 422 - Mostrado: 17 (4.0%)

Perfil: Default

09:20 p.m.
13/8/2024

Lab 01: java Client Protocol UDP server 123.123.33.55

45448	44.170779	10.1.8.44	239.255.255.250	SSDP	217 M-SEARCH * HTTP/1.1
45449	44.190310	10.1.14.182	123.123.33.55	UDP	46 64316 → 3000 Len=4
45456	44.804575	0.0.0.0	255.255.255.255	DHCP	364 DHCP Request - Transaction ID 0x6656c129
45457	44.804575	10.1.0.1	255.255.255.255	DHCP	344 DHCP ACK - Transaction ID 0x6656c129

▶ Frame 45449: 46 bytes on wire (368 bits), 46 bytes captured (368 bits) on interface \Device\NPF_{AF74CD52-7607-40E6-96D6-9BF8368C79C}

▶ Ethernet II, Src: Intel_f2:f3:19 (7c:b2:7d:f2:f3:19), Dst: Ubiquiti_44:3c:93 (18:e8:29:44:3c:93)

▶ Internet Protocol Version 4, Src: 10.1.14.182, Dst: 123.123.33.55

▶ User Datagram Protocol, Src Port: 64316, Dst Port: 3000

▼ Data (4 bytes)

Data: 61736466

[Length: 4]

0000 18 e8 29 44 3c 93 7c b2 7d f2 f3 19 08 00 45 00 ..)D<|.}....E

0010 00 20 c5 08 00 00 80 11 00 00 0a 01 0e b6 7b 7b {

0020 21 37 fb 3c 0b b8 00 0c b5 86 61 73 64 66 17 < asdf

Time-to-live exceeded:

[illegible]

Port Unreachable:

```
4071 55.199005 10.240.40.249 10.1.14.182 ICMP 134 Time-to-live exceeded (Time to live exceeded in transit)
4085 55.235631 10.240.40.249 10.1.14.182 ICMP 120 Destination unreachable (Port unreachable)
4123 55.720607 10.1.0.1 10.1.14.182 ICMP 94 Destination unreachable (Host unreachable)
4173 56.178909 fe80::c293:fdbb::... ff02::1:2 DHCPv6 157 Solicit XID: 0xdfc567 CID: 0001000127b3cc8e8c04ba9a6180
4216 56.742644 10.240.40.249 10.1.14.182 ICMP 120 Destination unreachable (Port unreachable)
4332 58.249681 10.240.40.249 10.1.14.182 ICMP 120 Destination unreachable (Port unreachable)
4389 58.889037 10.1.5.240 239.255.255.250 SSDP 217 M-SEARCH * HTTP/1.1
4540 60.115863 10.1.5.240 239.255.255.250 SSDP 217 M-SEARCH * HTTP/1.1
4591 60.763079 10.1.14.182 192.178.52.142 ICMP 106 Echo (ping) request id=0x0001, seq=319/16129, ttl=3 (no response found!)
4592 60.766490 10.200.100.8 10.1.14.182 ICMP 70 Time-to-live exceeded (Time to live exceeded in transit)

Destination Address: 10.1.14.182
Internet Control Message Protocol
Type: 3 (Destination unreachable)
Code: 3 (Port unreachable)
Checksum: 0x49e8 [correct]
[Checksum Status: Good]
Unused: 00000000
Internet Protocol Version 4, Src: 10.1.14.182, Dst: 10.240.40.249
0100 .... = Version: 4
.... 0101 = Header Length: 20 bytes (5)
Differeniated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
Total Length: 78
Identification: 0x076f (1903)
000. .... = Flags: 0x0
...0 0000 0000 0000 = Fragment Offset: 0
Time to Live: 127
Protocol: UDP (17)
Header Checksum: 0xe790 [validation disabled]
[Header checksum status: Unverified]
Source Address: 10.1.14.182
Destination Address: 10.240.40.249
User Datagram Protocol, Src Port: 137, Dst Port: 137
NetBIOS Name Service
```

Host Unreachable:

The image shows a Wireshark packet capture of an ICMP Destination unreachable (Host unreachable) message. The packet list on the left shows several ICMP messages, with the selected packet being an Echo (ping) request from 10.1.14.182 to 10.1.14.182, which resulted in a Destination unreachable (Host unreachable) response. The packet details pane on the right shows the structure of the ICMP message, including the Type (3), Code (1), and Checksum (0xc51b). The packet bytes pane on the right shows the raw data of the ICMP message, including the Type, Code, and Checksum fields.

No.	Time	Source	Destination	Protocol	Length	Info
4085	55.235631	10.240.40.249	10.1.14.182	ICMP	120	Destination unreachable (Port unreachable)
4123	55.720607	10.1.0.1	10.1.14.182	ICMP	94	Destination unreachable (Host unreachable)
4173	56.178909	fe80::c293:fdbb::	ff02::1:2	DHCPv6	157	Solicit XID: 0xdfe567 CID: 0001000127b3cc8e8c04ba9a6180
4216	56.742644	10.240.40.249	10.1.14.182	ICMP	120	Destination unreachable (Port unreachable)
4332	58.249681	10.240.40.249	10.1.14.182	ICMP	120	Destination unreachable (Port unreachable)
4389	58.889037	10.1.5.240	239.255.255.250	SSDP	217	M-SEARCH * HTTP/1.1
4540	60.115863	10.1.5.240	239.255.255.250	SSDP	217	M-SEARCH * HTTP/1.1
4591	60.763079	10.1.14.182	192.178.52.142	ICMP	106	Echo (ping) request id=0x0001, seq=319/16129, ttl=3 (no response found!)
4592	60.766490	10.200.100.8	10.1.14.182	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)

Destination Address: 10.1.14.182

Internet Control Message Protocol

- Type: 3 (Destination unreachable)
- Code: 1 (Host unreachable)
- Checksum: 0xc51b [correct]
- [Checksum Status: Good]
- Unused: 00000000

Internet Protocol Version 4, Src: 10.1.14.182, Dst: 172.16.3.47

- 0100 = Version: 4
- 0101 = Header Length: 20 bytes (5)
- Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
- Total Length: 52
- Identification: 0xaff3 (45043)
- 010. = Flags: 0x2, Don't fragment
- ... 0 0000 0000 0000 = Fragment Offset: 0
- Time to Live: 127
- Protocol: TCP (6)
- Header Checksum: 0x83da [validation disabled]
- [Header checksum status: Unverified]
- Source Address: 10.1.14.182
- Destination Address: 172.16.3.47

Transmission Control Protocol, Src Port: 10388, Dst Port: 7680, Seq: 186124094

0000 7c b2 7d f2 f3 19 18 e8 29 44 3c 93 08 00 45 c0 | } D< | } E-

0010 00 50 f8 ef 00 00 40 01 5e 45 0a 01 00 01 0a 01 | < MA.....

0020 0e b6 03 01 c5 1b 00 00 00 00 45 00 00 34 af f3 | E-4..

0030 40 00 7f 06 83 da 0a 01 0e b6 ac 10 03 2f 28 94 | @ / (..

0040 1e 00 0b 18 07 3e 00 00 00 00 80 02 fa f0 53 3f | > S?

0050 00 00 02 04 05 b4 01 03 03 08 01 01 04 02 |

Ping request:

The image shows a Wireshark packet capture of an ICMP Echo (ping) request and its response. The packet list on the left shows several ICMP messages, with the selected packet being an Echo (ping) request from 10.1.14.182 to 142.250.189.142, which resulted in an Echo (ping) reply from 142.250.189.142 to 10.1.14.182. The packet details pane on the right shows the structure of the ICMP message, including the Type (8), Code (0), and Checksum (0x4d41). The packet bytes pane on the right shows the raw data of the ICMP message, including the Type, Code, and Checksum fields.

No.	Time	Source	Destination	Protocol	Length	Info
267	10.819442	10.1.15.34	10.1.255.255	DB-LS...	243	Dropbox LAN sync Discovery Protocol, JSON
268	10.819442	10.1.15.34	10.1.255.255	DB-LS...	243	Dropbox LAN sync Discovery Protocol, JSON
279	11.509388	10.1.14.182	142.250.189.142	ICMP	74	Echo (ping) request id=0x0001, seq=26/6656, ttl=128 (reply in 280)
280	11.535026	142.250.189.142	10.1.14.182	ICMP	74	Echo (ping) reply id=0x0001, seq=26/6656, ttl=117 (request in 279)
296	12.059706	10.1.14.182	239.255.255.250	SSDP	167	M-SEARCH * HTTP/1.1

Frame 279: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface \Device\NPF{AF74CD52-7607-40E6-96D6-9BF8368C79CD}

Ethernet II, Src: Intel_f2:f3:19 (7c:b2:7d:f2:f3:19), Dst: Ubiquiti_44:3c:93 (18:e8:29:44:3c:93)

Internet Protocol Version 4, Src: 10.1.14.182, Dst: 142.250.189.142

Internet Control Message Protocol

- Type: 8 (Echo (ping) request)
- Code: 0
- Checksum: 0x4d41 [correct]
- [Checksum Status: Good]
- Identifier (BE): 1 (0x0001)
- Identifier (LE): 256 (0x0100)
- Sequence Number (BE): 26 (0x001a)
- Sequence Number (LE): 6656 (0x1a00)
- [Response frame: 280]

Data (32 bytes)

Data: 6162636465666768696a6b6c6d6e6f7071727374757677616263646566676869

[Length: 32]

0000 18 e8 29 44 3c 93 7c b2 7d f2 f3 19 08 00 45 00 | ..)D< | } E-

0010 00 3c 0d cf 00 00 80 01 00 00 0a 01 0e b6 8e fa | < MA.....

0020 bd 8e 08 00 4d 41 00 01 00 1a 61 62 63 64 65 66 | MA..... abcdef

0030 67 68 69 6a 6b 6c 6d 6e 6f 70 71 72 73 74 75 76 | ghijklmn opqrstuv

0040 77 61 62 63 64 65 66 67 68 69 | wabcdefg hi

Ping reply:

268 10.819442 10.1.15.34 10.1.255.255 DB-LS... 243 Dropbox LAN sync Discovery Protocol, JSON

279 11.509388 10.1.14.182 142.250.189.142 ICMP 74 Echo (ping) request id=0x0001, seq=26/6656, ttl=128 (reply in 280)

280 11.535026 142.250.189.142 10.1.14.182 ICMP 74 Echo (ping) reply id=0x0001, seq=26/6656, ttl=117 (request in 279)

296 12.059706 10.1.14.182 239.255.255.250 SSDP 167 M-SEARCH * HTTP/1.1

Frame 280: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface \Device\NPF_{AF74CD52-7607-40E6-96D6-9BF8368C79CD}

Ethernet II, Src: Ubiquiti_44:3c:93 (18:e8:29:44:3c:93), Dst: Intel_f2:f3:19 (7c:b2:7d:f2:f3:19)

Internet Protocol Version 4, Src: 142.250.189.142, Dst: 10.1.14.182

Internet Control Message Protocol

- Type: 0 (Echo (ping) reply)
- Code: 0
- Checksum: 0x5541 [correct]
- [Checksum Status: Good]
- Identifier (BE): 1 (0x0001)
- Identifier (LE): 256 (0x0100)
- Sequence Number (BE): 26 (0x001a)
- Sequence Number (LE): 6656 (0x1a00)
- [Request frame: 279]
- [Response time: 25.638 ms]

Data (32 bytes)

- Data: 6162636465666768696a6b6c6d6e6f7071727374757677616263646566676869
- [Length: 32]

0000 7c b2 7d f2 f3 19 18 e8 29 44 3c 93 08 00 45 00 | }) D < . . . E .

0010 00 3c 00 00 00 00 75 01 e0 81 8e fa bd 8e 0a 01 | < u

0020 0e b6 00 00 55 41 00 01 00 1a 61 62 63 64 65 66 | UA abcdef

0030 67 68 69 6a 6b 6c 6d 6e 6f 70 71 72 73 74 75 76 | ghijklmn opqrstuv

0040 77 61 62 63 64 65 66 67 68 69 | wabcdefg hi

2. Análisis de encabezados

No.	Source	Destination	Length	Type	Code	Checksum	Headers adicionales
Time-to-live exceeded							
4071	10.240.40.249	10.1.14.182	134	11	0	0xf4ff	
Port Unreachable							
4085	10.240.40.249	10.1.14.182	120	3	3	0xf4ff	
Host Unreachable							
4123	10.1.0.1	10.1.14.182	94	3	1	0xc51b	
Ping (request)							
279	10.1.14.182	142.250.189.142	74	0	0	0x4d41	id=0x0001, seq=26/6656, ttl=128 (reply in 280)
Ping (reply)							
280	142.250.189.142	10.1.14.182	74	0	0	0x5541	id=0x0001, seq=26/6656, ttl=117 (request in 279)

3. Preguntas de análisis

¿Cómo se pueden diferenciar los mensajes ICMP/IP de host y port unreachable?

Ambos son Type 3, pero el Code cambia:

- Code: 1 (Host unreachable)
- Code: 3 (Port unreachable)

¿Cuál es la respuesta al enviar un UDP/IP con IP y PORT incorrectos y por qué?

No hay respuesta. En ambos casos solo se envía por UDP, pero no se recibe respuesta. Tampoco hay mensaje de error ni nada, porque UDP solo manda y no verifica si llega.

¿Qué contiene el mensaje ICMP de Time Exceeded en su data? ¿Viene vacío?

No, sí tiene DATA: 64 bytes de 0s:

[illegible]

¿Cuál es la particularidad de los mensajes ICMP Echo y Echo Reply?

Ambos llevan 32 bits de DATA: el abecedario:

0020	bd	8e	08	00	4d	44	00	01	00	17	61	62	63	64	65	66	...	MD..	..	abcdef										
0030	67	68	69	6a	6b	6c	6d	6e	6f	70	71	72	73	74	75	76	ghijklmn				opqrstuv									
0040	77	61	62	63	64	65	66	67	68	69											w	a	b	c	d	e	f	g	h	i

Preguntas Generales

¿Qué diferencias observas en la captura de paquetes entre TCP y UDP?

En TCP vemos que hay más flags, y varios pasos previos antes de enviar el data. Vemos que siempre hay un handshake (SYN, SYN, ACK) y al finalizar hay un (FIN, ACK). En UDP no hay esto, solo se manda de una vez el paquete.

¿Qué información puedes extraer de los mensajes ICMP generados por las pruebas de UDP?

Son muy sencillos, similar a UDP. Pero llevan ciertos parámetros específicos del protocolo ICMP, que son el Type y el Code. Además del checksum que UDP ya implementa para verificaciones.

¿Cómo afectan los mensajes de control en TCP (como FIN, ACK) al cierre de la conexión?

El cliente manda un FIN para avisar que va a cerrar conexión, y luego el servidor manda su FIN, ACK. El cliente finaliza con un ACK, y ahí terminan los mensajes.

Esto afecta la conexión, ya que aunque se cierre, todavía se mandan unos últimos paquetes, asegurando que la conexión se cierre de ambos lados.

¿Qué diferencias notas en la ruta y los tiempos de respuesta entre TraceRoute y Ping?

Por observación, parece que TraceRoute busca varias rutas para llegar a un servidor, en el caso default con un máximo de 30 saltos. Vemos que hay unas rutas que tardan más en responder, unas que no responden, y unas que responden bastante rápido.

En Ping al contrario, parece que encuentra la ruta más corta y solo manda unos paquetes de verificación, por lo que la respuesta es rápida.