

# Laboratorio 05 – 21000492

## SECCIÓN TCP:

### 1. Captura de paquetes

Capturando desde Adapter for loopback traffic capture

Archivo Edición Visualización Ir Captura Analizar Estadísticas Telefonía Wireless Herramientas Ayuda

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	45.210680	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 Time: 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 80 06 00 00 .....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 d7 .....k.....  
0030 01 03 03 08 01 01 04 02 .....

Header Checksum (ip.checksum), 2 byte(s)

Paquetes: 209 - Mostrados: 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?*

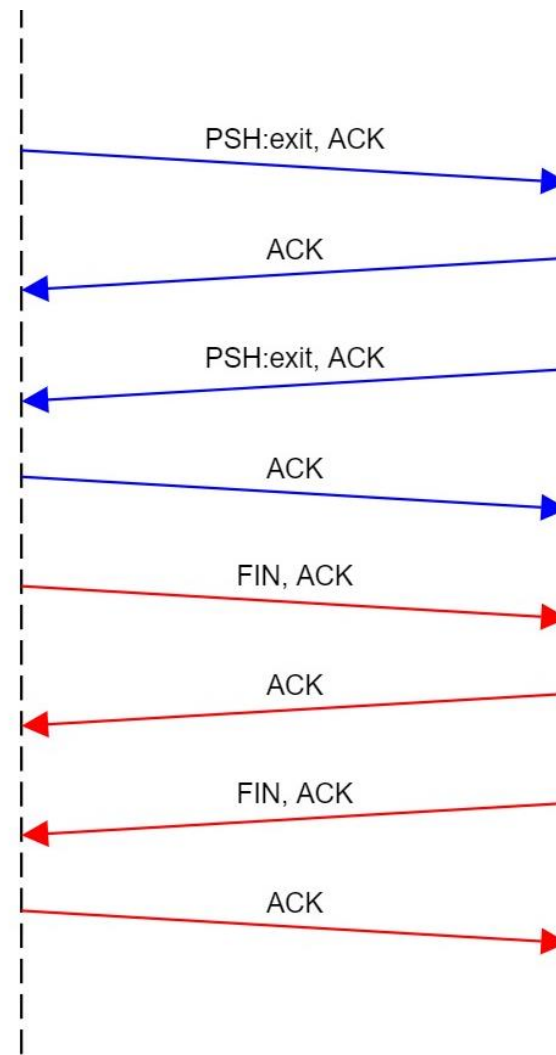
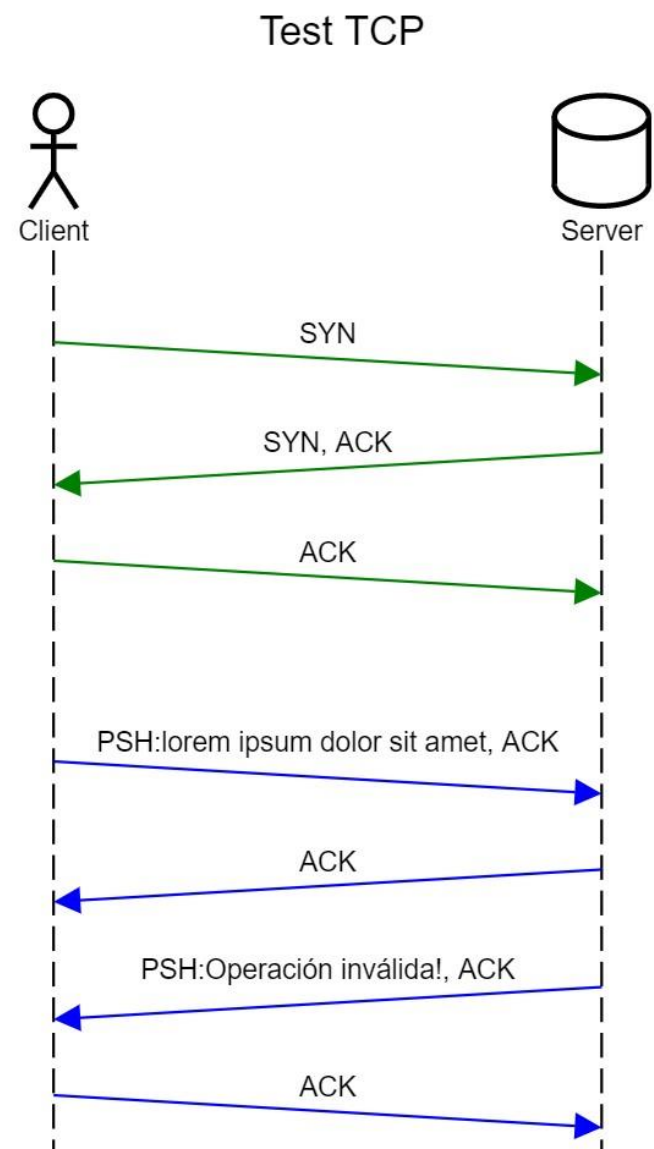
Seq inicial es 0. Seq final es 36 (31 para Server).

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

\*Adapter for loopback traffic capture

ArchivoEdiciónVisualizaciónIrCapturaAnalizarEstadísticasTelefoníaWirelessHerramientasAyuda

udp.port==3000

⌵

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  
-----

User Datagram Protocol (udp), 8 byte(s)

000002 00 00 00 45 00 00 361a 4b 00 00 80 11 00 00.....E-6.K.....  
00107f 00 00 01 7f 00 00 01ce cf 0b b8 00 22 9f b9.....".....  
00206c 6f 72 65 6d 20 69 7073 75 6d 20 64 6f 6c 6flore ip sum dolo  
003072 20 73 69 74 20 61 6d65 74r sit am et

Paquetes: 73 · Mostrado: 4 (5.5%) · Perdido: 0 (0.0%)

Perfil: Default

07:39 p.m.  
7/8/2024

## 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 && !nbs && !lmm'. The packet list pane displays the following entries:

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 following hex data:

```
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 shows 'Paquetes: 4660 - Mostrado: 67 (1.4%)' and 'Perfil: Default'.

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

Capturando desde Wi-Fi

ArchivoEdiciónVisualizaciónIrCapturaAnalizarEstadísticasTelefoníaWirelessHerramientasAyuda

icmp || udp && !dns && !quic

No.

Time

Source

Destination

Protocol

Length

Info

376.213121192.168.92.169142.250.217.174ICMP74Echo (ping) requestid=0x0001, seq=306/12801, ttl=128 (reply in 38)

386.270473142.250.217.174192.168.92.169ICMP74Echo (ping) replyid=0x0001, seq=306/12801, ttl=116 (request in 37)

407.218038192.168.92.169142.250.217.174ICMP74Echo (ping) requestid=0x0001, seq=307/13057, ttl=128 (reply in 41)

417.271892142.250.217.174192.168.92.169ICMP74Echo (ping) replyid=0x0001, seq=307/13057, ttl=116 (request in 40)

438.232044192.168.92.169142.250.217.174ICMP74Echo (ping) requestid=0x0001, seq=308/13313, ttl=128 (reply in 45)

458.353139142.250.217.174192.168.92.169ICMP74Echo (ping) replyid=0x0001, seq=308/13313, ttl=116 (request in 43)

469.247049192.168.92.169142.250.217.174ICMP74Echo (ping) requestid=0x0001, seq=309/13569, ttl=128 (reply in 47)

479.308729142.250.217.174192.168.92.169ICMP74Echo (ping) replyid=0x0001, seq=309/13569, ttl=116 (request in 46)

11521.005240192.168.92.169239.255.255.250SSDP216M-SEARCH \* HTTP/1.1

11621.069978192.168.92.169239.255.255.250SSDP217M-SEARCH \* HTTP/1.1

11722.019116192.168.92.169239.255.255.250SSDP216M-SEARCH \* HTTP/1.1

11822.080184192.168.92.169239.255.255.250SSDP217M-SEARCH \* HTTP/1.1

13023.030109192.168.92.169239.255.255.250SSDP216M-SEARCH \* HTTP/1.1

13123.092113192.168.92.169239.255.255.250SSDP217M-SEARCH \* HTTP/1.1

13624.039122192.168.92.169239.255.255.250SSDP216M-SEARCH \* HTTP/1.1

13724.102131192.168.92.169239.255.255.250SSDP217M-SEARCH \* HTTP/1.1

Frame 37: 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: 26:e3:67:5d:84:3e (26:e3:67:5d:84:3e)

Internet Protocol Version 4, Src: 192.168.92.169, Dst: 142.250.217.174

Internet Control Message Protocol

Type: 8 (Echo (ping) request)

Code: 0

Checksum: 0x4c29 [correct]

[Checksum Status: Good]

Identifier (BE): 1 (0x0001)

Identifier (LE): 256 (0x0100)

Sequence Number (BE): 306 (0x0132)

Sequence Number (LE): 12801 (0x3201)

[Response frame: 38]

Data (32 bytes)

000026 e3 67 5d 84 3e 7c b2 7d f2 f3 19 08 00 45 00 & g]->[: }.... E

001000 3c d4 e7 00 00 80 01 00 00 c0 a8 5c a9 8e fa <..... \...

0020d9 ae 08 00 4c 29 00 01 01 32 61 62 63 64 65 66 ...L)... 2abcdef

003067 68 69 6a 6b 6c 6d 6e 6f 70 71 72 73 74 75 76 ghijklmn opqrstuv

004077 61 62 63 64 65 66 67 68 69 wabcdfgh i

Wi-Fi: <live capture in progress>

Paquetes: 316 - Mostrado: 16 (5.1%)

Perfil: Default

08:13 p.m.  
7/8/2024

