

HỌ TÊN : NGUYỄN XUÂN TRỰC

MSSV : 1513804

=====o0o=====

LAB_3A

1) Select one UDP packet from your trace. From this packet, determine how many fields there are in the UDP header. (You shouldn't look in the textbook! Answer these questions directly from what you observe in the packet trace.) Name these fields.

SOLUTION

UDP header contains 4 fields:

- Source Port
- Destination Port
- Length
- Checksum

No.	Time	Source	Destination	Protocol	Length	Info
1	07:14:27.484641	172.17.4.110	239.255.255.250	SSDP	167	M-SEARCH * HTTP/1.1
4	07:14:27.548137	172.217.194.189	172.17.0.120	UDP	82	443 → 58831 Len=40
5	07:14:27.557537	172.17.0.120	172.217.194.189	UDP	70	58831 → 443 Len=28
6	07:14:27.588989	172.17.4.110	239.255.255.250	SSDP	167	M-SEARCH * HTTP/1.1
8	07:14:27.694695	172.17.4.110	239.255.255.250	SSDP	167	M-SEARCH * HTTP/1.1
15	07:14:27.998182	172.17.1.223	172.17.31.255	UDP	305	54915 → 54915 Len=263

> Frame 1: 167 bytes on wire (1336 bits), 167 bytes captured (1336 bits) on interface \Device\NPF_{AE991849-34A6-43D8-8EB0-5442C1293884}, id 0
> Ethernet II, Src: Apple_be:2a:6f (f4:0f:24:be:2a:6f), Dst: IPv4mcast_7f:ff:fa (01:00:5e:7f:ff:fa)
> Internet Protocol Version 4, Src: 172.17.4.110, Dst: 239.255.255.250
▼ User Datagram Protocol, Src Port: 53554, Dst Port: 1900
Source Port: 53554
Destination Port: 1900
Length: 133
Checksum: 0x5842 [unverified]
[Checksum Status: Unverified]
[Stream index: 0]
> [Timestamps]
> Simple Service Discovery Protocol

2) By consulting the displayed information in Wireshark's packet content field for this packet, determine the length (in bytes) of each of the UDP header fields.

SOLUTION

The UDP header has a fixed length of 8 bytes. Each of these 4 header fields is 2 bytes long.

No.	Time	Source	Destination	Protocol	Length	Info
1	07:14:27.484641	172.17.4.110	239.255.255.250	SSDP	167	M-SEARCH * HTTP/1.1
4	07:14:27.548137	172.217.194.189	172.17.0.120	UDP	82	443 → 58831 Len=40
5	07:14:27.557537	172.17.0.120	172.217.194.189	UDP	70	58831 → 443 Len=28
6	07:14:27.588989	172.17.4.110	239.255.255.250	SSDP	167	M-SEARCH * HTTP/1.1
8	07:14:27.694695	172.17.4.110	239.255.255.250	SSDP	167	M-SEARCH * HTTP/1.1
15	07:14:27.998182	172.17.1.223	172.17.31.255	UDP	305	54915 → 54915 Len=263

> Frame 1: 167 bytes on wire (1336 bits), 167 bytes captured (1336 bits) on interface \Device\NPF_{AE991849-34A6-43D8-8EB0-5442C1293B84}, id 0

> Ethernet II, Src: Apple_be:2a:6f (f4:0f:24:be:2a:6f), Dst: IPv4mcast_7f:ff:fa (01:00:5e:7f:ff:fa)

> Internet Protocol Version 4, Src: 172.17.4.110, Dst: 239.255.255.250

▼ User Datagram Protocol, Src Port: 53554, Dst Port: 1900

Source Port: 53554
Destination Port: 1900
Length: 133
Checksum: 0x5842 [unverified]
[Checksum Status: Unverified]
[Stream index: 0]
> [Timestamps]

> Simple Service Discovery Protocol


```

0000  01 00 5e 7f ff fa f4 0f 24 be 2a 6f 08 00 45 00  ..^....$.*o..E.
0010  00 90 01 00 00 00 01 01 56 c2 c1 04 6e ef ff  ....V.....n..
0020  ff f1 d1 32 07 6c 00 85 58 42 4d 2d 53 45 41 52  ..2.1..XM-SEAR
0030  43 48 20 20 20 20 20 20 20 20 20 20 20 20 20 20  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 0d 0a 1:1....

```

3) The value in the Length field is the length of what? (You can consult the text for this answer). Verify your claim with your captured UDP packet.

SOLUTION

The length field specifies the number of bytes in the UDP segment (header plus data). An explicit length value is needed since the size of the data field may differ from one UDP segment to the next.

The length of UDP payload for selected packet is 125 bytes. (133 bytes - 8 bytes = 125 bytes).

No.	Time	Source	Destination	Protocol	Length	Info
1	07:14:27.484641	172.17.4.110	239.255.255.250	SSDP	167	M-SEARCH * HTTP/1.1
4	07:14:27.548137	172.217.194.189	172.17.0.120	UDP	82	443 → 58831 Len=40
5	07:14:27.557537	172.17.0.120	172.217.194.189	UDP	70	58831 → 443 Len=28
6	07:14:27.588989	172.17.4.110	239.255.255.250	SSDP	167	M-SEARCH * HTTP/1.1
8	07:14:27.694695	172.17.4.110	239.255.255.250	SSDP	167	M-SEARCH * HTTP/1.1
15	07:14:27.998182	172.17.1.223	172.17.31.255	UDP	305	54915 → 54915 Len=263

> Frame 1: 167 bytes on wire (1336 bits), 167 bytes captured (1336 bits) on interface \Device\NPF_{AE991849-34A6-43D8-8EB0-5442C1293B84}, id 0

> Ethernet II, Src: Apple_be:2a:6f (f4:0f:24:be:2a:6f), Dst: IPv4mcast_7f:ff:fa (01:00:5e:7f:ff:fa)

> Internet Protocol Version 4, Src: 172.17.4.110, Dst: 239.255.255.250

▼ User Datagram Protocol, Src Port: 53554, Dst Port: 1900

Source Port: 53554
Destination Port: 1900
Length: 133
Checksum: 0x5842 [unverified]
[Checksum Status: Unverified]
[Stream index: 0]
> [Timestamps]

> Simple Service Discovery Protocol

4) What is the maximum number of bytes that can be included in a UDP payload?

SOLUTION

The maximum number of bytes that can be included in a UDP payload is $(2^{16} - 1)$ bytes plus the header bytes. This gives 65535 bytes – 8 bytes = 65527 bytes.

5) What is the largest possible source port number?

SOLUTION

The largest possible source port number is $(2^{16} - 1) = 65535$.

6) What is the protocol number for UDP? Give your answer in both hexadecimal and decimal notation.

SOLUTION

The IP protocol number for UDP is 0x11 hex, which is 17 in decimal value.

No.	Time	Source	Destination	Protocol	Length	Info
1	07:14:27.484641	172.17.4.110	239.255.255.250	SSDP	167	M-SEARCH * HTTP/1.1
4	07:14:27.548137	172.217.194.189	172.17.0.120	UDP	82	443 → 58831 Len=40
5	07:14:27.557537	172.17.0.120	172.217.194.189	UDP	70	58831 → 443 Len=28
6	07:14:27.588989	172.17.4.110	239.255.255.250	SSDP	167	M-SEARCH * HTTP/1.1
8	07:14:27.694695	172.17.4.110	239.255.255.250	SSDP	167	M-SEARCH * HTTP/1.1
15	07:14:27.998182	172.17.1.223	172.17.31.255	UDP	305	54915 → 54915 Len=263

>	Frame 1: 167 bytes on wire (1336 bits), 167 bytes captured (1336 bits) on interface \Device\NPF_{AE991849-34A6-43D8-8EB0-5442C1293B84}, id 0
>	Ethernet II, Src: Apple_be:2a:6f (f4:0f:24:be:2a:6f), Dst: IPv4mcast_7f:ff:fa (01:00:5e:7f:ff:fa)
▼	Internet Protocol Version 4, Src: 172.17.4.110, Dst: 239.255.255.250
	0100 = Version: 4
 0101 = Header Length: 20 bytes (5)
>	Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
	Total Length: 153
	Identification: 0xc1f8 (49656)
>	Flags: 0x0000
	Fragment offset: 0
	Time to live: 1
	Protocol: UDP (17)
	Header checksum: 0x56e2 [validation disabled]
	[Header checksum status: Unverified]
	Source: 172.17.4.110
	Destination: 239.255.255.250
>	User Datagram Protocol, Src Port: 53554, Dst Port: 1900
>	Simple Service Discovery Protocol

0000	01 00 5e 7f ff fa 4 01 4 be 2a 6f 08 00 45 00	..^.....\$.*o..E.
0010	00 99 c1 f8 00 00 c1 11 6 e2 ac 11 04 6e ef ffV....n..
0020	ff fa d1 32 07 6c 00 85 58 42 4d 2d 53 45 41 52	...2.l..XBM-SEAR
0030	43 48 20 2a 20 48 54 54 50 2f 31 2e 31 0d 0a 48	CH * HTT P/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-mul tiscreen
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 0d 0a	l:1....

7) Examine a pair of UDP packets in which your host sends the first UDP packet and the second UDP packet is a reply to this first UDP packet.

SOLUTION

The source port of the UDP packet sent by the host is the same as the destination port of the reply packet, and conversely the destination port of the UDP packet sent by the host is the same as the source port of the reply packet.

tcp.stream eq 28						
No.	Time	Source	Destination	Protocol	Length	Info
1152	07:47:42.567943	172.17.0.120	172.217.163.238	TCP	55	62659 → 443 [ACK] Seq=1 Ack=1 Win=507 Len=1 [TCP segment
1153	07:47:42.594753	172.217.163.238	172.17.0.120	TCP	66	443 → 62659 [ACK] Seq=1 Ack=2 Win=2096 Len=0 SLE=1 SRE=2

<

> Frame 1152: 55 bytes on wire (440 bits), 55 bytes captured (440 bits) on interface \Device\NPF_{AE991849-34A6-43D8-8EB0-5442C1293B84}, id 0

> Ethernet II, Src: IntelCor_e2:6b:f2 (70:1c:e7:e2:6b:f2), Dst: Routerbo_fd:17:74 (00:0c:42:fd:17:74)

> Internet Protocol Version 4, Src: 172.17.0.120, Dst: 172.217.163.238

▼ Transmission Control Protocol, Src Port: 62659, Dst Port: 443, Seq: 1, Ack: 1, Len: 1

Source Port: 62659

Destination Port: 443

[Stream index: 28]

[TCP Segment Len: 1]

Sequence number: 1 (relative sequence number)

Sequence number (raw): 252995199

[Next sequence number: 2 (relative sequence number)]

Acknowledgment number: 1 (relative ack number)

Acknowledgment number (raw): 558856873

0101 = Header Length: 20 bytes (5)

> Flags: 0x010 (ACK)

Window size value: 507

[Calculated window size: 507]

[Window size scaling factor: -1 (unknown)]

Checksum: 0xa87c [unverified]

[Checksum Status: Unverified]

No.	Time	Source	Destination	Protocol	Length	Info
1152	07:47:42.567943	172.17.0.120	172.217.163.238	TCP	55	62659 → 443 [ACK] Seq=1 Ack=1 Win=507 Len=1 [TCP segment of a reas
1153	07:47:42.594753	172.217.163.238	172.17.0.120	TCP	66	443 → 62659 [ACK] Seq=1 Ack=2 Win=2096 Len=0 SLE=1 SRE=2

<

> Frame 1153: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface \Device\NPF_{AE991849-34A6-43D8-8EB0-5442C1293B84}, id 0

> Ethernet II, Src: Routerbo_fd:17:74 (00:0c:42:fd:17:74), Dst: IntelCor_e2:6b:f2 (70:1c:e7:e2:6b:f2)

> Internet Protocol Version 4, Src: 172.217.163.238, Dst: 172.17.0.120

▼ Transmission Control Protocol, Src Port: 443, Dst Port: 62659, Seq: 1, Ack: 2, Len: 0

Source Port: 443

Destination Port: 62659

[Stream index: 28]

[TCP Segment Len: 0]

Sequence number: 1 (relative sequence number)

Sequence number (raw): 558856873

[Next sequence number: 1 (relative sequence number)]

Acknowledgment number: 2 (relative ack number)

Acknowledgment number (raw): 252995200

1000 = Header Length: 32 bytes (8)

> Flags: 0x010 (ACK)

Window size value: 2096

[Calculated window size: 2096]

[Window size scaling factor: -1 (unknown)]

Checksum: 0x8108 [unverified]

[Checksum Status: Unverified]

LAB_3B

1) What is the IP address and TCP port number used by the client computer (source) that is transferring the file to gaia.cs.umass.edu? To answer this question, it's probably easiest to select an HTTP message and explore the details of the TCP packet used to carry this HTTP message, using the "details of the selected packet header window" (refer to Figure 2 in the "Getting Started with Wireshark" Lab if you're uncertain about the Wireshark windows).

SOLUTION

According to above figure, the client computer (source)'s IP address is 172.17.0.120.

1011	08:12:36.415729	172.17.0.120	128.119.245.12	HTTP	602 GET /wireshark-labs/alice.txt HTTP/1.1
1231	08:12:37.376468	128.119.245.12	172.17.0.120	HTTP	1357 HTTP/1.1 200 OK (text/plain)
1847	08:13:00.174908	172.17.0.120	128.119.245.12	HTTP	451 POST /wireshark-labs/lab3-1-reply.htm HTTP/1.1 (text/plain)
1870	08:13:00.417285	128.119.245.12	172.17.0.120	HTTP	831 HTTP/1.1 200 OK (text/html)
2356	08:13:23.026807	172.17.0.120	69.195.128.18	HTTP	455 GET /multi/checkref.php HTTP/1.1
2363	08:13:23.267097	69.195.128.18	172.17.0.120	HTTP	329 HTTP/1.1 200 OK (text/html)

> Frame 1011: 602 bytes on wire (4816 bits), 602 bytes captured (4816 bits) on interface \Device\NPF_{AE991849-34A6-43D8-8EB0-5442C1293B84}, id 0
> Ethernet II, Src: IntelCor_e2:6b:f2 (70:1c:e7:e2:6b:f2), Dst: Routerbo_fd:17:74 (00:0c:42:fd:17:74)
> Internet Protocol Version 4, Src: 172.17.0.120, Dst: 128.119.245.12
▼ Transmission Control Protocol, Src Port: 63024, Dst Port: 80, Seq: 1, Ack: 1, Len: 548
Source Port: 63024
Destination Port: 80
[Stream index: 17]
[TCP Segment Len: 548]
Sequence number: 1 (relative sequence number)
Sequence number (raw): 2739044321
[Next sequence number: 549 (relative sequence number)]
Acknowledgment number: 1 (relative ack number)
Acknowledgment number (raw): 2759727347
0101 = Header Length: 20 bytes (5)

2) What is the IP address of gaia.cs.umass.edu? On what port number is it sending and receiving TCP segments for this connection?

SOLUTION

According to above figure, the IP address of gaia.cs.umass.edu is 128.119.245.12 and the TCP port number is 80.

1011	08:12:36.415729	172.17.0.120	128.119.245.12	HTTP	602 GET /wireshark-labs/alice.txt HTTP/1.1
1231	08:12:37.376468	128.119.245.12	172.17.0.120	HTTP	1357 HTTP/1.1 200 OK (text/plain)
1847	08:13:00.174908	172.17.0.120	128.119.245.12	HTTP	451 POST /wireshark-labs/lab3-1-reply.htm HTTP/1.1 (text/plain)
1870	08:13:00.417285	128.119.245.12	172.17.0.120	HTTP	831 HTTP/1.1 200 OK (text/html)
2356	08:13:23.026807	172.17.0.120	69.195.128.18	HTTP	455 GET /multi/checkref.php HTTP/1.1
2363	08:13:23.267097	69.195.128.18	172.17.0.120	HTTP	329 HTTP/1.1 200 OK (text/html)

> Frame 1231: 1357 bytes on wire (10856 bits), 1357 bytes captured (10856 bits) on interface \Device\NPF_{AE991849-34A6-43D8-8EB0-5442C1293B84}, id 0
> Ethernet II, Src: Routerbo_fd:17:74 (00:0c:42:fd:17:74), Dst: IntelCor_e2:6b:f2 (70:1c:e7:e2:6b:f2)
> Internet Protocol Version 4, Src: 128.119.245.12, Dst: 172.17.0.120
▼ Transmission Control Protocol, Src Port: 80, Dst Port: 63024, Seq: 151201, Ack: 549, Len: 1303
Source Port: 80
Destination Port: 63024
[Stream index: 17]
[TCP Segment Len: 1303]
Sequence number: 151201 (relative sequence number)
Sequence number (raw): 2759878547
[Next sequence number: 152504 (relative sequence number)]
Acknowledgment number: 549 (relative ack number)
Acknowledgment number (raw): 2739044869
0101 = Header Length: 20 bytes (5)

3) What is the IP address and TCP port number used by your client computer (source) to transfer the file to gaia.cs.umass.edu?

SOLUTION

According to above figure, my client computer's IP address is 172.17.0.120 and the TCP port is 63026.

1011	08:12:36.415729	172.17.0.120	128.119.245.12	HTTP	602 GET /wireshark-labs/alice.txt HTTP/1.1
1231	08:12:37.376468	128.119.245.12	172.17.0.120	HTTP	1357 HTTP/1.1 200 OK (text/plain)
1847	08:13:00.174908	172.17.0.120	128.119.245.12	HTTP	451 POST /wireshark-labs/lab3-1-reply.htm HTTP/1.1 (text/plain)
1870	08:13:00.417285	128.119.245.12	172.17.0.120	HTTP	831 HTTP/1.1 200 OK (text/html)
2356	08:13:23.026807	172.17.0.120	69.195.128.18	HTTP	455 GET /multi/checkref.php HTTP/1.1
2363	08:13:23.267097	69.195.128.18	172.17.0.120	HTTP	329 HTTP/1.1 200 OK (text/html)

> Frame 1847: 451 bytes on wire (3608 bits), 451 bytes captured (3608 bits) on interface \Device\NPF_{AE991849-34A6-43D8-8EB0-5442C1293B84}, id 0
> Ethernet II, Src: IntelCor_e2:6b:f2 (70:1c:e7:e2:6b:f2), Dst: Routerbo_fd:17:74 (00:0c:42:fd:17:74)
> Internet Protocol Version 4, Src: 172.17.0.120, Dst: 128.119.245.12
▼ Transmission Control Protocol, Src Port: 63026, Dst Port: 80, Seq: 152649, Ack: 1, Len: 397
Source Port: 63026
Destination Port: 80
[Stream index: 16]
[TCP Segment Len: 397]
Sequence number: 152649 (relative sequence number)
Sequence number (raw): 3306529301
[Next sequence number: 153046 (relative sequence number)]
Acknowledgment number: 1 (relative ack number)
Acknowledgment number (raw): 1001211006
0101 = Header Length: 20 bytes (5)

4) What is the sequence number of the TCP SYN segment that is used to initiate the TCP connection between the client computer and gaia.cs.umass.edu? What is it in the segment that identifies the segment as a SYN segment?

SOLUTION

The sequence number of the TCP SYN segment is 0 since it is used to imitate the TCP connection between the client computer and gaia.cs.umass.edu.

According to above figure, in the Flags section, the Syn flag is set to 1 which indicates that this segment is a SYN segment.

No.	Time	Source	Destination	Protocol	Length	Info
1000	08:12:35.623491	49.213.114.176	172.17.0.120	TCP	54	443 → 62754 [ACK] Seq=352 Ack=1185 Win=212 Len=0
1009	08:12:36.409039	172.17.0.120	128.119.245.12	TCP	54	63025 → 80 [FIN, ACK] Seq=1 Ack=1 Win=516 Len=0
1010	08:12:36.409397	172.17.0.120	128.119.245.12	TCP	66	63026 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
1011	08:12:36.415729	172.17.0.120	128.119.245.12	TCP	602	63024 → 80 [PSH, ACK] Seq=1 Ack=1 Win=517 Len=548
1014	08:12:36.421978	172.17.0.120	52.163.89.138	TCP	66	63027 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
1016	08:12:36.442938	52.163.89.138	172.17.0.120	TCP	66	443 → 63027 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0 MSS=1440 WS=256 SACK_PERM=1
1017	08:12:36.443017	172.17.0.120	52.163.89.138	TCP	54	63027 → 443 [ACK] Seq=1 Ack=1 Win=132352 Len=0

> Ethernet II, Src: IntelCor_e2:6b:f2 (70:1c:e7:e2:6b:f2), Dst: Routerbo_fd:17:74 (00:0c:42:fd:17:74)
> Internet Protocol Version 4, Src: 172.17.0.120, Dst: 128.119.245.12
▼ Transmission Control Protocol, Src Port: 63026, Dst Port: 80, Seq: 0, Len: 0
Source Port: 63026
Destination Port: 80
[Stream index: 16]
[TCP Segment Len: 0]
Sequence number: 0 (relative sequence number)
Sequence number (raw): 3306376652
[Next sequence number: 1 (relative sequence number)]
Acknowledgment number: 0
Acknowledgment number (raw): 0
1000 = Header Length: 32 bytes (8)
▼ Flags: 0x002 (SYN)
000. = Reserved: Not set
...0 = Nonce: Not set
...0... = Congestion Window Reduced (CWR): Not set
....0... = ECN-Echo: Not set
....0... = Urgent: Not set
....0... = Acknowledgment: Not set
....0... = Push: Not set
....0... = Reset: Not set
>1... = Syn: Set
....0... = Fin: Not set
[TCP Flags:S.]

5) What is the sequence number of the SYNACK segment sent by gaia.cs.umass.edu to the client computer in reply to the SYN? What is the value of the Acknowledgement field in the SYNACK segment? How did gaia.cs.umass.edu determine that value? What is it in the segment that identifies the segment as a SYNACK segment?

SOLUTION

According to the above figure, the sequence number of the SYNACK segment sent by gaia.cs.umass.edu to the client computer in reply to the SYN is 0.

The value of the acknowledgement field in the SYNACK segment is 1. The value of the ACKnowledgement field in the SYNACK segment is determined by the server gaia.cs.umass.edu. The server adds 1 to the initial sequence number of SYN segment from the client computer. For this case, the initial sequence number of SYN segment from the client computer is 0, thus the value of the ACKnowledgement field in the SYNACK segment is 1.

A segment will be identified as a SYNACK segment if both SYN flag and Acknowledgement in the segment are set to 1.

No.	Time	Source	Destination	Protocol	Length	Info
1059	08:12:36.646843	128.119.245.12	172.17.0.120	TCP	66	80 → 63026 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MS
1060	08:12:36.646901	172.17.0.120	128.119.245.12	TCP	54	63026 → 80 [ACK] Seq=1 Ack=1 Win=132352 Len=0
1061	08:12:36.653781	128.119.245.12	172.17.0.120	TCP	54	80 → 63024 [ACK] Seq=1 Ack=549 Win=237 Len=0
1062	08:12:36.654459	128.119.245.12	172.17.0.120	TCP	1494	80 → 63024 [ACK] Seq=1 Ack=549 Win=237 Len=1440
1063	08:12:36.654459	128.119.245.12	172.17.0.120	TCP	1494	80 → 63024 [ACK] Seq=1441 Ack=549 Win=237 Len=1440
1064	08:12:36.654511	172.17.0.120	128.119.245.12	TCP	54	63024 → 80 [ACK] Seq=549 Ack=2881 Win=517 Len=0
1065	08:12:36.654881	128.119.245.12	172.17.0.120	TCP	1494	80 → 63024 [ACK] Seq=2881 Ack=549 Win=237 Len=1440

>	Ethernet II, Src: Routerbo_fd:17:74 (00:0c:42:fd:17:74), Dst: IntelCor_e2:6b:f2 (70:1c:e7:e2:6b:f2)
>	Internet Protocol Version 4, Src: 128.119.245.12, Dst: 172.17.0.120
▼	Transmission Control Protocol, Src Port: 80, Dst Port: 63026, Seq: 0, Ack: 1, Len: 0
	Source Port: 80
	Destination Port: 63026
	[Stream index: 16]
	[TCP Segment Len: 0]
	Sequence number: 0 (relative sequence number)
	Sequence number (raw): 1001211005
	[Next sequence number: 1 (relative sequence number)]
	Acknowledgment number: 1 (relative ack number)
	Acknowledgment number (raw): 3306376653
	1000 = Header Length: 32 bytes (8)
▼	Flags: 0x012 (SYN, ACK)
	000. = Reserved: Not set
	...0 = Nonce: Not set
	...0... = Congestion Window Reduced (CWR): Not set
0... = ECN-Echo: Not set
0 = Urgent: Not set
1 = Acknowledgment: Set
0... = Push: Not set
0... = Reset: Not set
>1 = Syn: Set
0 = Fin: Not set
	[TCP Flags:A..S.]

6) What is the sequence number of the TCP segment containing the HTTP POST command? Note that in order to find the POST command, you'll need to dig into the packet content field at the bottom of the Wireshark window, looking for a segment with a "POST" within its DATA field.

SOLUTION

1059	08:12:36.646843	128.119.245.12	172.17.0.120	TCP	66 80 → 63026	[SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1440
1060	08:12:36.646901	172.17.0.120	128.119.245.12	TCP	54 63026 → 80	[ACK] Seq=1 Ack=1 Win=132352 Len=0
1061	08:12:36.653781	128.119.245.12	172.17.0.120	TCP	54 80 → 63024	[ACK] Seq=1 Ack=549 Win=237 Len=0
1062	08:12:36.654459	128.119.245.12	172.17.0.120	TCP	1494 80 → 63024	[ACK] Seq=1 Ack=549 Win=237 Len=1440
1063	08:12:36.654459	128.119.245.12	172.17.0.120	TCP	1494 80 → 63024	[ACK] Seq=1441 Ack=549 Win=237 Len=1440
1064	08:12:36.654511	172.17.0.120	128.119.245.12	TCP	54 63024 → 80	[ACK] Seq=549 Ack=2881 Win=517 Len=0
1065	08:12:36.654881	128.119.245.12	172.17.0.120	TCP	1494 80 → 63024	[ACK] Seq=2881 Ack=549 Win=237 Len=1440

> Ethernet II, Src: IntelCor_e2:6b:f2 (70:1c:e7:e2:6b:f2), Dst: Routerbo_fd:17:74 (00:0c:42:fd:17:74)

> Internet Protocol Version 4, Src: 172.17.0.120, Dst: 128.119.245.12

▼ Transmission Control Protocol, Src Port: 63026, Dst Port: 80, Seq: 1, Ack: 1, Len: 0

Source Port: 63026

Destination Port: 80

[Stream index: 16]

[TCP Segment Len: 0]

Sequence number: 1 (relative sequence number)

Sequence number (raw): 3306376653

[Next sequence number: 1 (relative sequence number)]

Acknowledgment number: 1 (relative ack number)

Acknowledgment number (raw): 1001211006

0101 = Header length: 20 bytes (5)

▼ Flags: 0x010 (ACK)

000. = Reserved: Not set

...0 = Nonce: Not set

...0 = Congestion Window Reduced (CWR): Not set

...0 = ECN-Echo: Not set

...0 = Urgent: Not set

...1 = Acknowledgment: Set

...0 = Push: Not set

...0 = Reset: Not set

...0 = Syn: Not set

...0 = Fin: Not set

[TCP Flags:A....]

```

0000  00 0c 42 fd 17 74 70 1c e7 e2 6b f2 08 00 45 00  ..B...tp...k...E-
0010  00 28 e6 a8 40 00 80 06 f2 19 ac 11 00 78 80 77  -(...@... ..x.w
0020  f5 0c f6 32 00 50 c5 13 4d cd 3b ad 44 7e 50 10  ...2.P...M.;D~P.
0030  02 05 02 33 00 00                                ...3..

```

According to above figure, the segment No.1060 contains the HTTP POST command, the sequence number of this segment is 1.