

Q1. What is the IP address and TCP port number used by the client computer?

A: client computer IP: 192.168.0.167 Port: 4368

```

1295 26.397693 192.168.0.167 128.119.245.12 HTTP 560 GET /wireshark-lab
<
> Frame 1295: 560 bytes on wire (4480 bits), 560 bytes captured (4480 bits) on
> Ethernet II, Src: WistronI_64:ed:a8 (98:ee:cb:64:ed:a8), Dst: HitronTe_19:32:
> Internet Protocol Version 4, Src: 192.168.0.167, Dst: 128.119.245.12
> Transmission Control Protocol, Src Port: 4368, Dst Port: 80, Seq: 1, Ack: 1,
  Source Port: 4368
  Destination Port: 80
  [Stream index: 15]
  [Conversation completeness: Incomplete, DATA (15)]
  [TCP Segment Len: 506]
  Sequence Number: 1 (relative sequence number)

```

Q2. What is the sequence number of the TCP SYN segment that is used to initiate the TCP connection between the client computer and server? What is the value in the segment that identifies the segment as a SYN segment?

A: Sequence number: 0, SYN segment value: Syn: Set (1)

```

1290 26.177669 192.168.0.167 128.119.245.12 TCP 66 4368 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
1293 26.397422 128.119.245.12 192.168.0.167 TCP 66 80 → 4368 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1460 SACK_
1294 26.397466 192.168.0.167 128.119.245.12 TCP 54 4368 → 80 [ACK] Seq=1 Ack=1 Win=131328 Len=0
1295 26.397693 192.168.0.167 128.119.245.12 HTTP 560 GET /wireshark-labs/INTRO-wireshark-file1.html HTTP/1.1
<
> Frame 1290: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on in
> Ethernet II, Src: WistronI_64:ed:a8 (98:ee:cb:64:ed:a8), Dst: HitronTe_19:3
> Internet Protocol Version 4, Src: 192.168.0.167, Dst: 128.119.245.12
> Transmission Control Protocol, Src Port: 4368, Dst Port: 80, Seq: 0, Len: 0
  Source Port: 4368
  Destination Port: 80
  [Stream index: 15]
  [Conversation completeness: Incomplete, DATA (15)]
  [TCP Segment Len: 0]
  Sequence Number: 0 (relative sequence number)
  Sequence Number (raw): 3174586830
  [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 .... = Accurate ECN: Not set
    ....0... = Congestion Window Reduced: 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

```

Q3. What is the value of the ACKnowledgement field in the SYNACK segment? How did server determine that value?

A: ACKnowledgement value: 1, ACKnowledgement value = Sequence number + 1 = 0 + 1 = 1

1290	26.177669	192.168.0.167	128.119.245.12	TCP	66	4368 → 80	[SYN]	Seq=0	Win=64240	Len=0	MSS=1460	WS=256	SACK_PER
1293	26.397422	128.119.245.12	192.168.0.167	TCP	66	80 → 4368	[SYN, ACK]	Seq=0	Ack=1	Win=29200	Len=0	MSS=1460	SACK
1294	26.397466	192.168.0.167	128.119.245.12	TCP	54	4368 → 80	[ACK]	Seq=1	Ack=1	Win=131328	Len=0		
1295	26.397693	192.168.0.167	128.119.245.12	HTTP	560	GET /wireshark-labs/INTRO-wireshark-file1.html HTTP/1.1							

Protocol: TCP (6)
Header Checksum: 0x1af1 [validation disabled]
[Header checksum status: Unverified]
Source Address: 128.119.245.12
Destination Address: 192.168.0.167

Transmission Control Protocol, Src Port: 80, Dst Port: 4368, Seq: 0, Ack: 1
Source Port: 80
Destination Port: 4368
[Stream index: 15]
[Conversation completeness: Incomplete, DATA (15)]
[TCP Segment Len: 0]
Sequence Number: 0 (relative sequence number)
Sequence Number (raw): 3817696098
[Next Sequence Number: 1 (relative sequence number)]
Acknowledgment Number: 1 (relative ack number)
Acknowledgment number (raw): 3174586831
1000 = Header Length: 32 bytes (8)

0000 98 ee cb 64 ed a8 60 6c 63 19 32 72 0
0010 00 34 00 00 40 00 29 06 1a f1 80 77 f
0020 00 a7 00 50 11 10 e3 8d 6b 62 bd 38 5
0030 72 10 4e c5 00 00 02 04 05 b4 01 01 0
0040 03 07

Q4. What is the amount of available buffer space advertised at the web server for the connection?

A: 29200

1290	26.177669	192.168.0.167	128.119.245.12	TCP	66	4368 → 80	[SYN]	Seq=0	Win=64240	Len=0	MSS=1460	WS=256	SACK_PERM
1293	26.397422	128.119.245.12	192.168.0.167	TCP	66	80 → 4368	[SYN, ACK]	Seq=0	Ack=1	Win=29200	Len=0	MSS=1460	SACK_PER
1294	26.397466	192.168.0.167	128.119.245.12	TCP	54	4368 → 80	[ACK]	Seq=1	Ack=1	Win=131328	Len=0		
1295	26.397693	192.168.0.167	128.119.245.12	HTTP	560	GET /wireshark-labs/INTRO-wireshark-file1.html HTTP/1.1							

> Frame 1293: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface
> Ethernet II, Src: HitronTe_19:32:72 (60:6c:63:19:32:72), Dst: WistronI_64:ed:
> Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192.168.0.167

Transmission Control Protocol, Src Port: 80, Dst Port: 4368, Seq: 0, Ack: 1,
Source Port: 80
Destination Port: 4368
[Stream index: 15]
[Conversation completeness: Incomplete, DATA (15)]
[TCP Segment Len: 0]
Sequence Number: 0 (relative sequence number)
Sequence Number (raw): 3817696098
[Next Sequence Number: 1 (relative sequence number)]
Acknowledgment Number: 1 (relative ack number)
Acknowledgment number (raw): 3174586831
1000 = Header Length: 32 bytes (8)

> Flags: 0x012 (SYN, ACK)
Window: 29200
[Calculated window size: 29200]
Checksum: 0x4ec5 [unverified]
[Checksum Status: Unverified]
Urgent Pointer: 0

> Options: (12 bytes), Maximum segment size, No-Operation (NOP), No-Operation
> [Timestamps]
> [SEQ/ACK analysis]

0000 98 ee cb 64 ed a8 60 6c 63 19 32 72 08 0
0010 00 34 00 00 40 00 29 06 1a f1 80 77 f5 0
0020 00 a7 00 50 11 10 e3 8d 6b 62 bd 38 59 c
0030 72 10 4e c5 00 00 02 04 05 b4 01 01 04 0
0040 03 07