

Name :

Abubaker Attique

Roll no :

P20-0560

Section :

5-A

Lab 09

Lab Task:

1. What is the source and destination port numbers?

Answer :

Source port :60643

Destination port: 80

```
1 0.000000 192.168.1.122 64.238.147.113 TCP 78 60643 → 80 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=8 TSval=256679793 TSecr=0 SACK_PE
```

.....

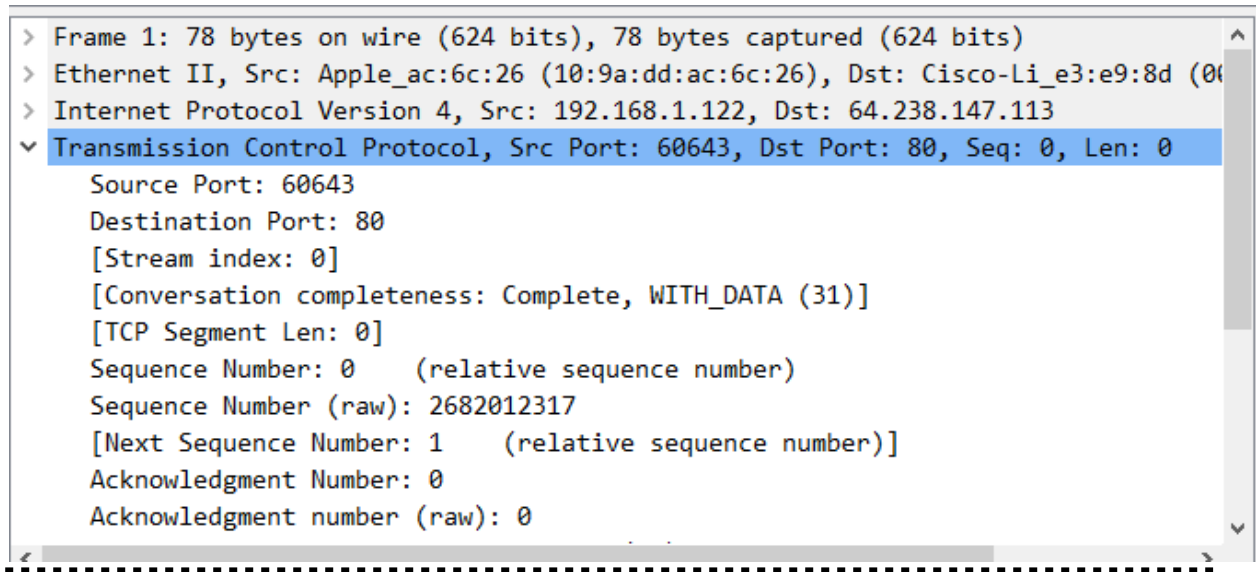
2. What is the sequence number of the TCP SYN segment that is used to initiate the TCP connection? What is it in the segment that identifies the segment as a SYN segment?

Answer :

Sequence Number: 0

TCP Segment Len: 0

The value is 0 in this trace. The SYN flag is set to 1 and it indicates that this segment is a SYN,ACK segment.



The image shows a Wireshark packet capture window. The packet list on the left shows 'Frame 1: 78 bytes on wire (624 bits), 78 bytes captured (624 bits)'. The packet details pane on the right shows the following information:

- Ethernet II, Src: Apple_ac:6c:26 (10:9a:dd:ac:6c:26), Dst: Cisco-Li_e3:e9:8d (08:00:0c:2c:3e:00)
- Internet Protocol Version 4, Src: 192.168.1.122, Dst: 64.238.147.113
- Transmission Control Protocol, Src Port: 60643, Dst Port: 80, Seq: 0, Len: 0

The TCP details pane shows the following information:

- Source Port: 60643
- Destination Port: 80
- [Stream index: 0]
- [Conversation completeness: Complete, WITH_DATA (31)]
- [TCP Segment Len: 0]
- Sequence Number: 0 (relative sequence number)
- Sequence Number (raw): 2682012317
- [Next Sequence Number: 1 (relative sequence number)]
- Acknowledgment Number: 0
- Acknowledgment number (raw): 0

3. What is the sequence number of the SYNACK segment sent by the server to the client computer in reply to the SYN? What is the value of the Acknowledgement field in the SYNACK segment? How did server determine that value? What is it in the segment that identifies the segment as a SYNACK segment?

Answer :

Acknowledgment Number = 1 (relative ack number)

Sequence Number (raw) = 349487776

The server adds 1 to the initial sequence number of SYN segment from the client computer because window size is 1. 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.

Window = 5792

4	0.088579	192.168.1.122	64.238.147.113	HTTP	257 GET /si
5	0.177819	64.238.147.113	192.168.1.122	TCP	66 80 → 60
6	0.178321	64.238.147.113	192.168.1.122	TCP	311 80 → 60
7	0.178388	192.168.1.122	64.238.147.113	TCP	66 60643 →
8	0.189114	64.238.147.113	192.168.1.122	TCP	1434 80 → 60
9	0.266705	64.238.147.113	192.168.1.122	TCP	1434 80 → 60
10	0.266787	192.168.1.122	64.238.147.113	TCP	66 60643 →
11	0.267657	64.238.147.113	192.168.1.122	TCP	1434 80 → 60
12	0.354612	64.238.147.113	192.168.1.122	TCP	1434 80 → 60
13	0.354647	192.168.1.122	64.238.147.113	TCP	66 60643 →

[Conversation completeness: Complete, WITH_DATA (31)]
[TCP Segment Len: 0]
Sequence Number: 0 (relative sequence number)
Sequence Number (raw): 349487776
[Next Sequence Number: 1 (relative sequence number)]
Acknowledgment Number: 1 (relative ack number)
Acknowledgment number (raw): 2682012318
1010 = Header Length: 40 bytes (10)
> **Flags: 0x012 (SYN, ACK)**
Window: 5792
[Calculated window size: 5792]
Checksum: 0x67d7 [unverified]
[Checksum Status: Unverified]
Urgent Pointer: 0

.....

4. What is the length of each of the first six TCP segments?

Answer :

1:

Apply a display filter ... <Ctrl-/>						
No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	192.168.1.122	64.238.147.113	TCP	78	60643 → 80 [
2	0.088010	64.238.147.113	192.168.1.122	TCP	74	80 → 60643 [
3	0.088080	192.168.1.122	64.238.147.113	TCP	66	60643 → 80 [
4	0.088579	192.168.1.122	64.238.147.113	HTTP	257	GET /sigcomm
5	0.177819	64.238.147.113	192.168.1.122	TCP	66	80 → 60643 [
6	0.178321	64.238.147.113	192.168.1.122	TCP	311	80 → 60643 [
7	0.178388	192.168.1.122	64.238.147.113	TCP	66	60643 → 80 [
8	0.189114	64.238.147.113	192.168.1.122	TCP	1434	80 → 60643 [
9	0.266705	64.238.147.113	192.168.1.122	TCP	1434	80 → 60643 [
10	0.266787	192.168.1.122	64.238.147.113	TCP	66	60643 → 80 [
11	0.267657	64.238.147.113	192.168.1.122	TCP	1434	80 → 60643 [
12	0.354612	64.238.147.113	192.168.1.122	TCP	1434	80 → 60643 [
13	0.354647	192.168.1.122	64.238.147.113	TCP	66	60643 → 80 [

> Frame 4: 257 bytes on wire (2056 bits), 257 bytes captured (2056 bits)	0000
> Ethernet II, Src: Apple_ac:6c:26 (10:9a:dd:ac:6c:26), Dst: Cisco-Li_e3:e9:8d (08:00:0c:08:00:08)	0010
> Internet Protocol Version 4, Src: 192.168.1.122, Dst: 64.238.147.113	0020
▼ Transmission Control Protocol, Src Port: 60643, Dst Port: 80, Seq: 1, Ack: 1, Len: 257	0030
Source Port: 60643	0040
Destination Port: 80	0050
[Stream index: 0]	0060
[Conversation completeness: Complete, WITH_DATA (31)]	0070
[TCP Segment Len: 191]	0080
Sequence Number: 1 (relative sequence number)	0090
Sequence Number (raw): 2682012318	00a0
[Next Sequence Number: 192 (relative sequence number)]	00b0
Acknowledgment Number: 1 (relative ack number)	00c0
Acknowledgment number (raw): 349487777	00d0

2:

Trace tcp (1).pcap

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Apply a display filter ... <Ctrl-/>

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	192.168.1.122	64.238.147.113	TCP	78	6064
2	0.088010	64.238.147.113	192.168.1.122	TCP	74	80 -
3	0.088080	192.168.1.122	64.238.147.113	TCP	66	6064
4	0.088579	192.168.1.122	64.238.147.113	HTTP	257	GET
5	0.177819	64.238.147.113	192.168.1.122	TCP	66	80 -
6	0.178321	64.238.147.113	192.168.1.122	TCP	311	80 -
7	0.178388	192.168.1.122	64.238.147.113	TCP	66	6064
8	0.189114	64.238.147.113	192.168.1.122	TCP	1434	80 -
9	0.266705	64.238.147.113	192.168.1.122	TCP	1434	80 -
10	0.266787	192.168.1.122	64.238.147.113	TCP	66	6064
11	0.267657	64.238.147.113	192.168.1.122	TCP	1434	80 -
12	0.354612	64.238.147.113	192.168.1.122	TCP	1434	80 -
13	0.354647	192.168.1.122	64.238.147.113	TCP	66	6064

<

> Frame 5: 66 bytes on wire (528 bits), 66 bytes captured (528 bits)

> Ethernet II, Src: Cisco-Li_e3:e9:8d (00:16:b6:e3:e9:8d), Dst: Apple_ac:6c:26 (10:00:00:00:00:00)

> Internet Protocol Version 4, Src: 64.238.147.113, Dst: 192.168.1.122

▼ Transmission Control Protocol, Src Port: 80, Dst Port: 60643, Seq: 1, Ack: 192, Window: 0

Source Port: 80

Destination Port: 60643

[Stream index: 0]

[Conversation completeness: Complete, WITH_DATA (31)]

[TCP Segment Len: 0]

Sequence Number: 1 (relative sequence number)

Sequence Number (raw): 349487777

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

Acknowledgment Number: 192 (relative ack number)

Acknowledgment number (raw): 2682012509

<

3:

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Apply a display filter ... <Ctrl-/>

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	192.168.1.122	64.238.147.113	TCP	78	60643 -
2	0.088010	64.238.147.113	192.168.1.122	TCP	74	80 → 60
3	0.088080	192.168.1.122	64.238.147.113	TCP	66	60643 -
4	0.088579	192.168.1.122	64.238.147.113	HTTP	257	GET /si
5	0.177819	64.238.147.113	192.168.1.122	TCP	66	80 → 60
6	0.178321	64.238.147.113	192.168.1.122	TCP	311	80 → 60
7	0.178388	192.168.1.122	64.238.147.113	TCP	66	60643 -
8	0.189114	64.238.147.113	192.168.1.122	TCP	1434	80 → 60
9	0.266705	64.238.147.113	192.168.1.122	TCP	1434	80 → 60
10	0.266787	192.168.1.122	64.238.147.113	TCP	66	60643 -
11	0.267657	64.238.147.113	192.168.1.122	TCP	1434	80 → 60
12	0.354612	64.238.147.113	192.168.1.122	TCP	1434	80 → 60
13	0.354647	192.168.1.122	64.238.147.113	TCP	66	60643 -

<

> Frame 6: 311 bytes on wire (2488 bits), 311 bytes captured (2488 bits)

> Ethernet II, Src: Cisco-Li_e3:e9:8d (00:16:b6:e3:e9:8d), Dst: Apple_ac:6c:26 (10:00:00:00:00:00)

> Internet Protocol Version 4, Src: 64.238.147.113, Dst: 192.168.1.122

✓ Transmission Control Protocol, Src Port: 80, Dst Port: 60643, Seq: 1, Ack: 192, Window: 0

Source Port: 80

Destination Port: 60643

[Stream index: 0]

[Conversation completeness: Complete, WITH_DATA (31)]

[TCP Segment Len: 245]

Sequence Number: 1 (relative sequence number)

Sequence Number (raw): 349487777

[Next Sequence Number: 246 (relative sequence number)]

Acknowledgment Number: 192 (relative ack number)

Acknowledgment number (raw): 2682012509

<

>

4:

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Apply a display filter ... <Ctrl-/>

No.	Time	Source	Destination	Protocol	Length
1	0.000000	192.168.1.122	64.238.147.113	TCP	78
2	0.088010	64.238.147.113	192.168.1.122	TCP	74
3	0.088080	192.168.1.122	64.238.147.113	TCP	66
4	0.088579	192.168.1.122	64.238.147.113	HTTP	257
5	0.177819	64.238.147.113	192.168.1.122	TCP	66
6	0.178321	64.238.147.113	192.168.1.122	TCP	311
7	0.178388	192.168.1.122	64.238.147.113	TCP	66
8	0.189114	64.238.147.113	192.168.1.122	TCP	1434
9	0.266705	64.238.147.113	192.168.1.122	TCP	1434
10	0.266787	192.168.1.122	64.238.147.113	TCP	66
11	0.267657	64.238.147.113	192.168.1.122	TCP	1434
12	0.354612	64.238.147.113	192.168.1.122	TCP	1434
13	0.354647	192.168.1.122	64.238.147.113	TCP	66

Frame 7: 66 bytes on wire (528 bits), 66 bytes captured (528 bits)
 Ethernet II, Src: Apple_ac:6c:26 (10:9a:dd:ac:6c:26), Dst: Cisco-Li_e3:e9:8d
 Internet Protocol Version 4, Src: 192.168.1.122, Dst: 64.238.147.113
 Transmission Control Protocol, Src Port: 60643, Dst Port: 80, Seq: 192, Ack:
 Source Port: 60643
 Destination Port: 80
 [Stream index: 0]
 [Conversation completeness: Complete, WITH_DATA (31)]
 [TCP Segment Len: 0]
 Sequence Number: 192 (relative sequence number)
 Sequence Number (raw): 2682012509
 [Next Sequence Number: 192 (relative sequence number)]
 Acknowledgment Number: 246 (relative ack number)
 Acknowledgment number (raw): 349488022

5:

trace-tcp (1).pcap

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Apply a display filter ... <Ctrl-/>

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	192.168.1.122	64.238.147.113	TCP	78	60643 →
2	0.088010	64.238.147.113	192.168.1.122	TCP	74	80 →
3	0.088080	192.168.1.122	64.238.147.113	TCP	66	60643 →
4	0.088579	192.168.1.122	64.238.147.113	HTTP	257	GET /
5	0.177819	64.238.147.113	192.168.1.122	TCP	66	80 →
6	0.178321	64.238.147.113	192.168.1.122	TCP	311	80 →
7	0.178388	192.168.1.122	64.238.147.113	TCP	66	60643 →
8	0.189114	64.238.147.113	192.168.1.122	TCP	1434	80 →
9	0.266705	64.238.147.113	192.168.1.122	TCP	1434	80 →
10	0.266787	192.168.1.122	64.238.147.113	TCP	66	60643 →
11	0.267657	64.238.147.113	192.168.1.122	TCP	1434	80 →
12	0.354612	64.238.147.113	192.168.1.122	TCP	1434	80 →
13	0.354647	192.168.1.122	64.238.147.113	TCP	66	60643 →

<

> Frame 8: 1434 bytes on wire (11472 bits), 1434 bytes captured (11472 bits)

> Ethernet II, Src: Cisco-Li_e3:e9:8d (00:16:b6:e3:e9:8d), Dst: Apple_ac:6c:26 (10:00:00:00:00:00)

> Internet Protocol Version 4, Src: 64.238.147.113, Dst: 192.168.1.122

▼ Transmission Control Protocol, Src Port: 80, Dst Port: 60643, Seq: 246, Ack: 192

Source Port: 80

Destination Port: 60643

[Stream index: 0]

[Conversation completeness: Complete, WITH_DATA (31)]

[TCP Segment Len: 1368]

Sequence Number: 246 (relative sequence number)

Sequence Number (raw): 349488022

[Next Sequence Number: 1614 (relative sequence number)]

Acknowledgment Number: 192 (relative ack number)

Acknowledgment number (raw): 2682012509

6:

trace-tcp (1).pcap

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help



Apply a display filter ... <Ctrl-/>

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	192.168.1.122	64.238.147.113	TCP	78	60643
2	0.088010	64.238.147.113	192.168.1.122	TCP	74	80 →
3	0.088080	192.168.1.122	64.238.147.113	TCP	66	60643
4	0.088579	192.168.1.122	64.238.147.113	HTTP	257	GET /
5	0.177819	64.238.147.113	192.168.1.122	TCP	66	80 →
6	0.178321	64.238.147.113	192.168.1.122	TCP	311	80 →
7	0.178388	192.168.1.122	64.238.147.113	TCP	66	60643
8	0.189114	64.238.147.113	192.168.1.122	TCP	1434	80 →
9	0.266705	64.238.147.113	192.168.1.122	TCP	1434	80 →
10	0.266787	192.168.1.122	64.238.147.113	TCP	66	60643
11	0.267657	64.238.147.113	192.168.1.122	TCP	1434	80 →
12	0.354612	64.238.147.113	192.168.1.122	TCP	1434	80 →
13	0.354647	192.168.1.122	64.238.147.113	TCP	66	60643

<

> Frame 9: 1434 bytes on wire (11472 bits), 1434 bytes captured (11472 bits)

> Ethernet II, Src: Cisco-Li_e3:e9:8d (00:16:b6:e3:e9:8d), Dst: Apple_ac:6c:26 (10:05:6c:00:06:26)

> Internet Protocol Version 4, Src: 64.238.147.113, Dst: 192.168.1.122

▼ Transmission Control Protocol, Src Port: 80, Dst Port: 60643, Seq: 1614, Ack: 192

Source Port: 80

Destination Port: 60643

[Stream index: 0]

[Conversation completeness: Complete, WITH_DATA (31)]

[TCP Segment Len: 1368]

Sequence Number: 1614 (relative sequence number)

Sequence Number (raw): 349489390

[Next Sequence Number: 2982 (relative sequence number)]

Acknowledgment Number: 192 (relative ack number)

Acknowledgment number (raw): 2682012509

>

5. Are there any retransmitted segments in the trace file? What did you check for (in the trace) in order to answer this question?

Answer :

Yes there is retransmitted in packet 7 and packet 10 because the source and destination both are same in packets and the sequence number should also be same.

Packet 7:

7	0.178388	192.168.1.122	64.238.147.113	TCP	66	60643 → 80	[ACK] Seq=192 Ack=246 Win=524280 Len=0 TSval=256679970 TSecr=4016893528
8	0.189114	64.238.147.113	192.168.1.122	TCP	1434	80 → 60643	[ACK] Seq=246 Ack=192 Win=6864 Len=1368 TSval=4016893538 TSecr=256679881
9	0.266705	64.238.147.113	192.168.1.122	TCP	1434	80 → 60643	[ACK] Seq=1614 Ack=192 Win=6864 Len=1368 TSval=4016893615 TSecr=256679970
10	0.266787	192.168.1.122	64.238.147.113	TCP	66	60643 → 80	[ACK] Seq=192 Ack=2982 Win=523944 Len=0 TSval=256680057 TSecr=4016893538
11	0.267657	64.238.147.113	192.168.1.122	TCP	1434	80 → 60643	[ACK] Seq=2982 Ack=192 Win=6864 Len=1368 TSval=4016893615 TSecr=256679970
12	0.354612	64.238.147.113	192.168.1.122	TCP	1434	80 → 60643	[ACK] Seq=4350 Ack=192 Win=6864 Len=1368 TSval=4016893703 TSecr=256680057
13	0.354647	192.168.1.122	64.238.147.113	TCP	66	60643 → 80	[ACK] Seq=192 Ack=5718 Win=523944 Len=0 TSval=256680144 TSecr=4016893615

Transmission Control Protocol, Src Port: 60643, Dst Port: 80, Seq: 192, Ack: 246	0000	00 16 b6 e3 e9 8d 10 9a dd ac 6c 26 08 00 45 00:1&..E
Source Port: 60643	0010	00 34 5f be 40 00 40 06 44 84 c0 a8 01 7a 40 ee	..4_@.@.D...z@.
Destination Port: 80	0020	93 71 ec e3 00 50 9f dc 43 5d 14 d4 c3 96 80 10	..q...P...C].....
[Stream index: 0]	0030	ff ff aa 2e 00 00 01 01 08 0a 0f 4c a0 22 ef 6cL...".
[Conversation completeness: Complete, WITH_DATA (31)]	0040	ee 58	X
[TCP Segment Len: 0]			
Sequence Number: 192 (relative sequence number)			
Sequence Number (raw): 2682012509			
[Next Sequence Number: 192 (relative sequence number)]			
Acknowledgment Number: 246 (relative ack number)			
Acknowledgment number (raw): 349488022			
1000 = Header Length: 32 bytes (8)			
Flags: 0x010 (ACK)			
Window: 65535			

Packet 10

5	0.177819	64.238.147.113	192.168.1.122	TCP	66	80 → 60643	[ACK] Seq=1 Ack=192 Win=6864 Len=0 TSval=4016893527 TSecr=256679881
6	0.178321	64.238.147.113	192.168.1.122	TCP	311	80 → 60643	[PSH, ACK] Seq=1 Ack=192 Win=6864 Len=245 TSval=4016893528 TSecr=25667988
7	0.178388	192.168.1.122	64.238.147.113	TCP	66	60643 → 80	[ACK] Seq=192 Ack=246 Win=524280 Len=0 TSval=256679970 TSecr=4016893528
8	0.189114	64.238.147.113	192.168.1.122	TCP	1434	80 → 60643	[ACK] Seq=246 Ack=192 Win=6864 Len=1368 TSval=4016893538 TSecr=256679881
9	0.266705	64.238.147.113	192.168.1.122	TCP	1434	80 → 60643	[ACK] Seq=1614 Ack=192 Win=6864 Len=1368 TSval=4016893615 TSecr=256679970
10	0.266787	192.168.1.122	64.238.147.113	TCP	66	60643 → 80	[ACK] Seq=192 Ack=2982 Win=523944 Len=0 TSval=256680057 TSecr=4016893538
11	0.267657	64.238.147.113	192.168.1.122	TCP	1434	80 → 60643	[ACK] Seq=2982 Ack=192 Win=6864 Len=1368 TSval=4016893615 TSecr=256679970
12	0.354612	64.238.147.113	192.168.1.122	TCP	1434	80 → 60643	[ACK] Seq=4350 Ack=192 Win=6864 Len=1368 TSval=4016893703 TSecr=256680057
13	0.354647	192.168.1.122	64.238.147.113	TCP	66	60643 → 80	[ACK] Seq=192 Ack=5718 Win=523944 Len=0 TSval=256680144 TSecr=4016893615

Transmission Control Protocol, Src Port: 60643, Dst Port: 80, Seq: 192, Ack: 2982	0000	00 16 b6 e3 e9 8d 10 9a dd ac 6c 26 08 00 45 00:1&..E
Source Port: 60643	0010	00 34 76 e5 40 00 40 06 2d 5d c0 a8 01 7a 40 ee	..4v_@.@.-]...z@.
Destination Port: 80	0020	93 71 ec e3 00 50 9f dc 43 5d 14 d4 c6 4e 80 10	..q...P...C]...F..
[Stream index: 0]	0030	ff d5 9f 47 00 00 01 01 08 0a 0f 4c a0 79 ef 6c	...G.....L..y.1
[Conversation completeness: Complete, WITH_DATA (31)]	0040	ee 62	-b
[TCP Segment Len: 0]			
Sequence Number: 192 (relative sequence number)			
Sequence Number (raw): 2682012509			
[Next Sequence Number: 192 (relative sequence number)]			
Acknowledgment Number: 2982 (relative ack number)			
Acknowledgment number (raw): 349490758			
1000 = Header Length: 32 bytes (8)			
Flags: 0x010 (ACK)			
Window: 65493			

