

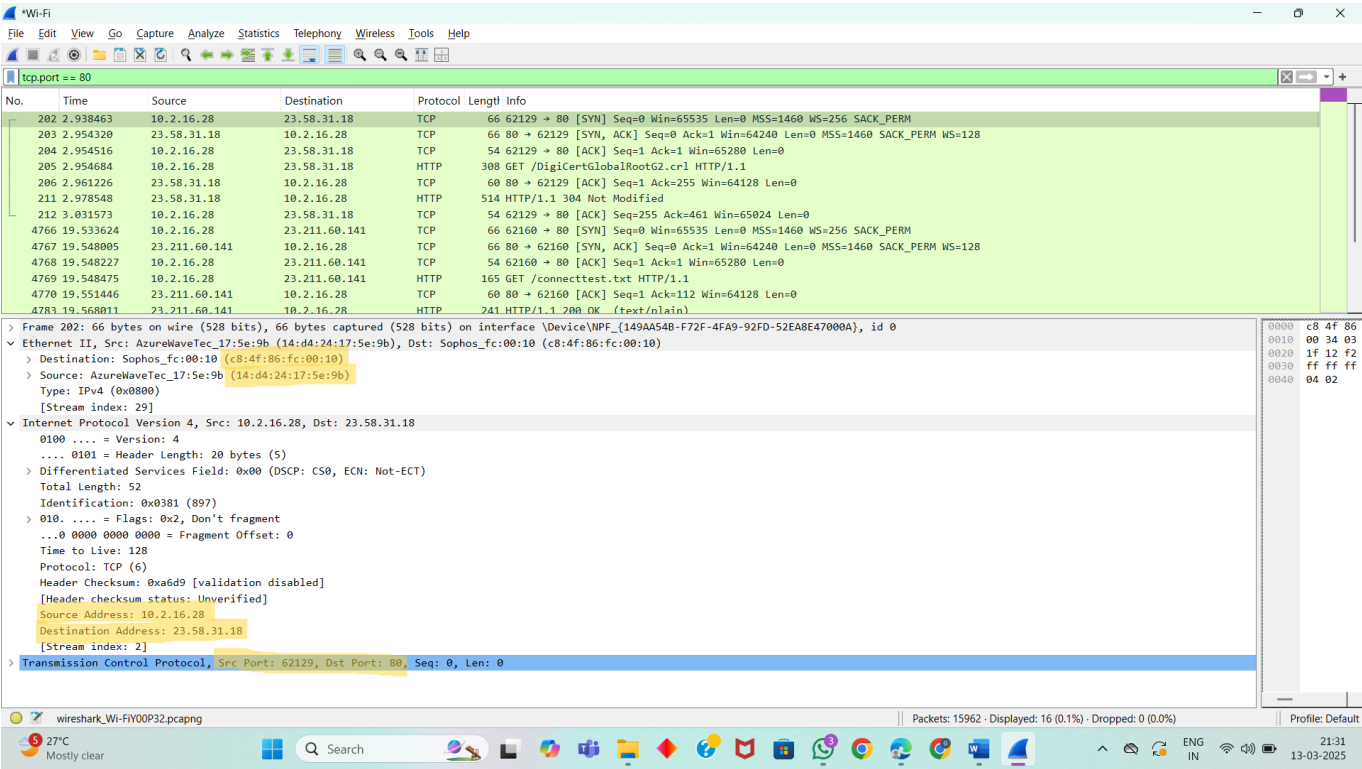
Register No:	99220040570
Name:	K.Hanumaan
Class/Section:	8501 A/S06
Ex.No:	11
Name of the Experiment	Capture and Analyzing TCP 3 way handshake
Google Drive link of the packet tracer file (give view permission):	https://drive.google.com/drive/folders/1bPielwY257DVwUtO2qz_DVoPJ4_fk_R?usp=drive_link

1. Visit any one website by opening a browser fill your machine details.

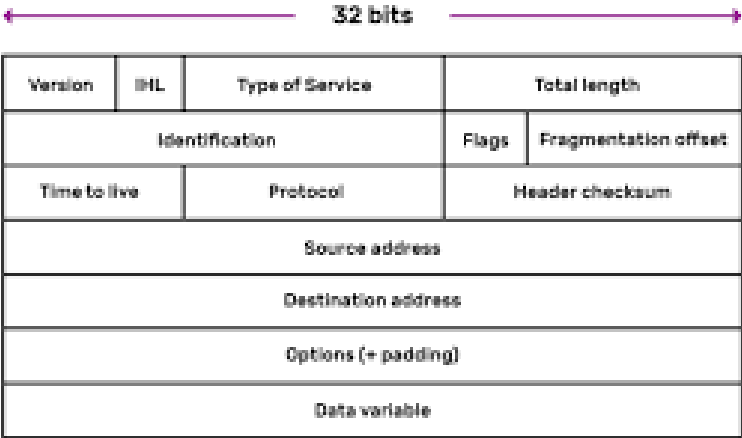
Parameter	Value
Your Machine IP Address.	10.2.16.28
Your Machine MAC Address	14:d4:24:17:5e:9b
Default Gateway address	10.2.0.1
Website URL	www.amazon.in
Website IP Address	23.58.31.18

2. Fill the following details:

Field Name	Field Length (no of bits)	Field value
Destination MAC address	48 bits	c8:4f:86:fc:00:10
Source MAC address	48 bits	14:d4:24:17:5e:9b
Destination IP address	32 bits	23.58.31.18
Source IP Address	32 bits	10.2.16.28
Destination TCP port	16 bits	80
Source TCP port	16 bits	62129



3. Fill the details as per the IP frame format .(highlight the details for each of the output and paste screenshot)



4	20 bytes	DSCP:CS0	52	
0x0381 (897)			0x2	0
128		TCP (6)	0xa6d9	
10.2.16.28				
23.58.31.18				
None				
None				

Wi-Fi

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

tcp.port == 80

No.	Time	Source	Destination	Protocol	Length	Info
202	2.938463	10.2.16.28	23.58.31.18	TCP	66	62129 → 80 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM
203	2.954320	23.58.31.18	10.2.16.28	TCP	66	80 → 62129 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460 SACK_PERM WS=128
204	2.954516	10.2.16.28	23.58.31.18	TCP	54	62129 → 80 [ACK] Seq=1 Ack=1 Win=65280 Len=0
205	2.954684	10.2.16.28	23.58.31.18	HTTP	308	GET /DigiCertGlobalRootG2.crl HTTP/1.1
206	2.961226	23.58.31.18	10.2.16.28	TCP	60	80 → 62129 [ACK] Seq=1 Ack=255 Win=64128 Len=0
211	2.978548	23.58.31.18	10.2.16.28	HTTP	514	HTTP/1.1 304 Not Modified
212	3.031573	10.2.16.28	23.58.31.18	TCP	54	62129 → 80 [ACK] Seq=255 Ack=461 Win=65024 Len=0
4766	19.533624	10.2.16.28	23.211.60.141	TCP	66	62160 → 80 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM
4767	19.548005	23.211.60.141	10.2.16.28	TCP	66	80 → 62160 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460 SACK_PERM WS=128
4768	19.548227	10.2.16.28	23.211.60.141	TCP	54	62160 → 80 [ACK] Seq=1 Ack=1 Win=65280 Len=0
4769	19.548475	10.2.16.28	23.211.60.141	HTTP	165	GET /connecttest.txt HTTP/1.1
4770	19.551446	23.211.60.141	10.2.16.28	TCP	60	80 → 62160 [ACK] Seq=1 Ack=112 Win=64128 Len=0
4783	19.568011	23.211.60.141	10.2.16.28	HTTP	241	HTTP/1.1 200 OK (text/plain)

> Frame 202: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface \Device\NPF_{149AA548-F72F-4FA9-92FD-52EA8E47000A}, id 0

> Ethernet II, Src: AzureWaveTec_17:5e:9b (14:d4:24:17:5e:9b), Dst: Sophos_fc:00:10 (c8:4f:86:fc:00:10)

> Destination: Sophos_fc:00:10 (c8:4f:86:fc:00:10)

> Source: AzureWaveTec_17:5e:9b (14:d4:24:17:5e:9b)

Type: IPv4 (0x0800)

[Stream index: 29]

> Internet Protocol Version 4, Src: 10.2.16.28, Dst: 23.58.31.18

0100 = Version: 4

.... 0101 = Header Length: 20 bytes (5)

> Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)

Total Length: 52

Identification: 0x0381 (897)

> 010. = Flags: 0x2, Don't fragment

...0 0000 0000 0000 = Fragment Offset: 0

Time to Live: 128

Protocol: TCP (6)

Header Checksum: 0xa6d9 [validation disabled]

[Header checksum status: Unverified]

Source Address: 10.2.16.28

Destination Address: 23.58.31.18

[Stream index: 2]

> Transmission Control Protocol, Src Port: 62129, Dst Port: 80, Seq: 0, Len: 0

wireshark_Wi-Fi00P32.pcapng

Packets: 15962 · Displayed: 16 (0.1%) · Dropped: 0 (0.0%)

Profile: Default

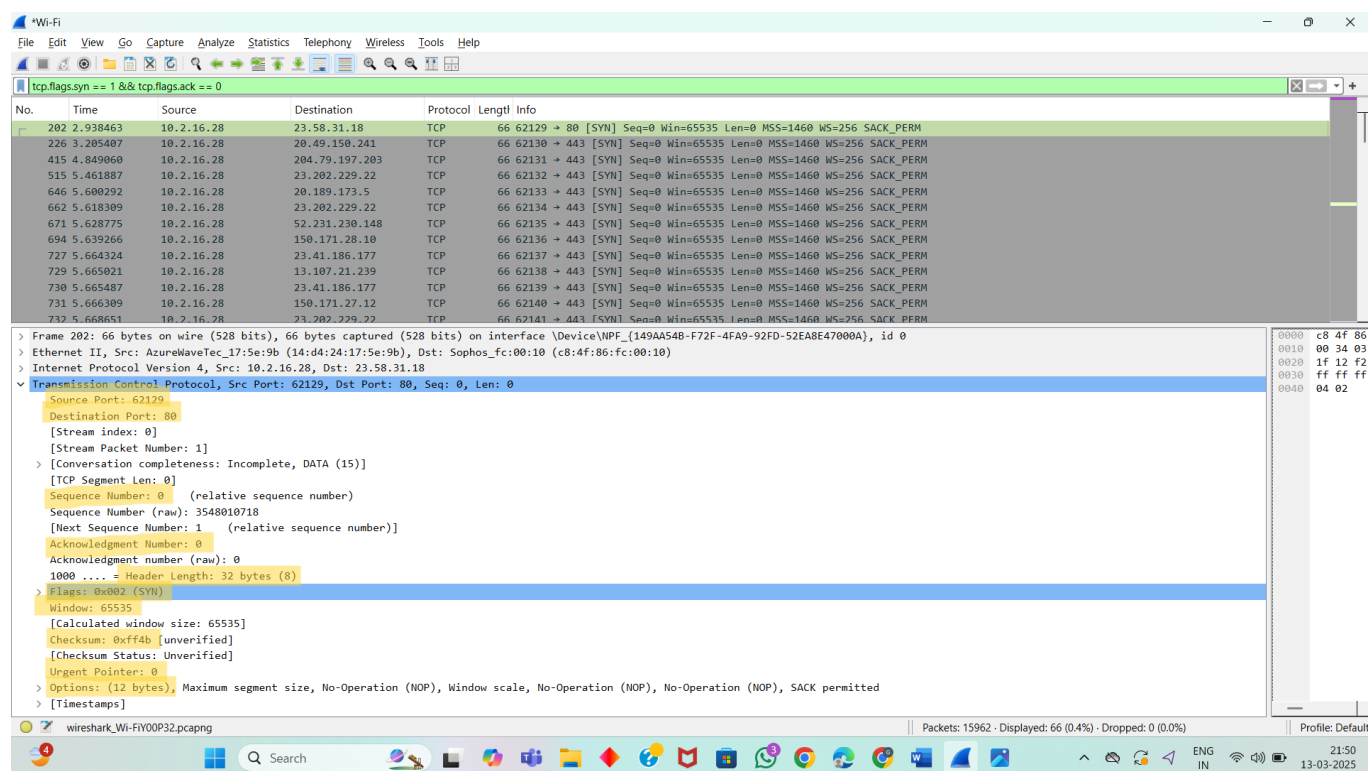
27°C Mostly clear

Search

ENG IN

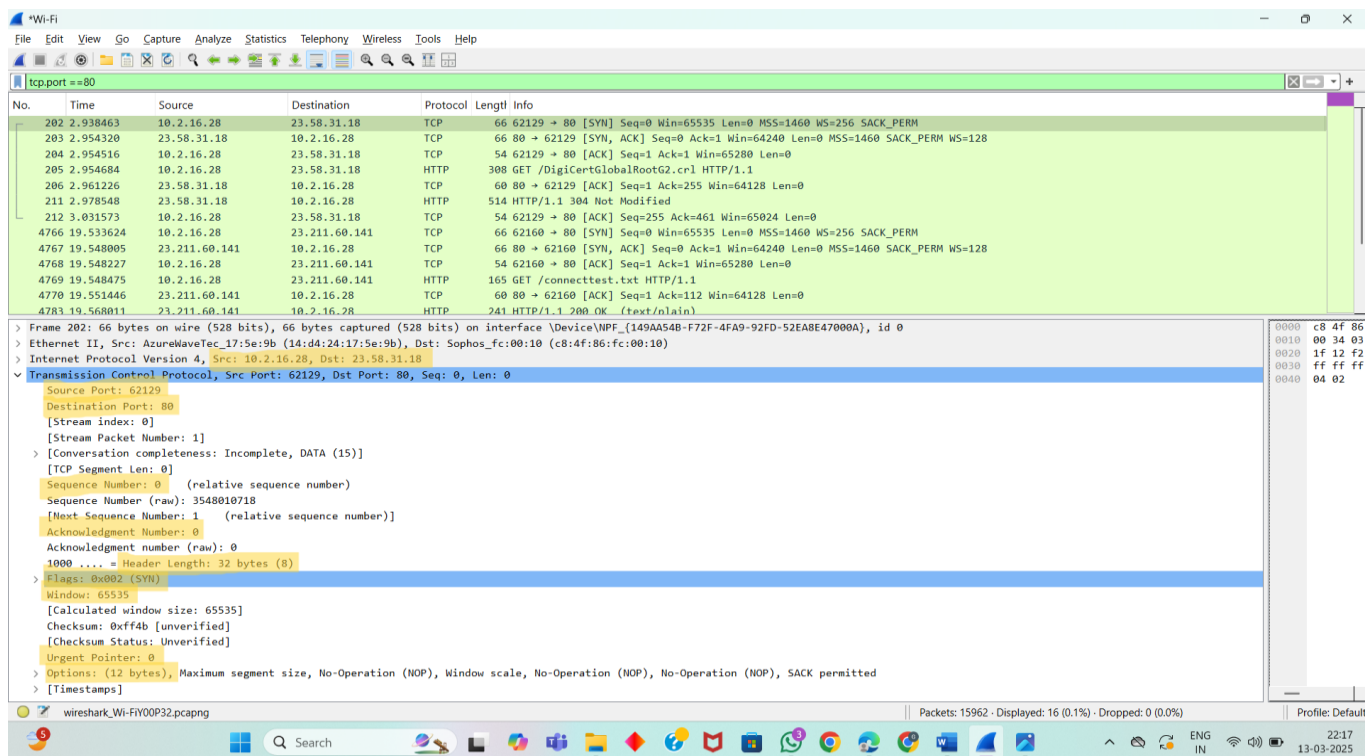
21:41 13-03-2025

4. Using the Wireshark capture of the first TCP session startup (SYN bit set to 1), fill in information about the TCP header. (paste screenshot for each of the output). Capture the packet and analyze it.



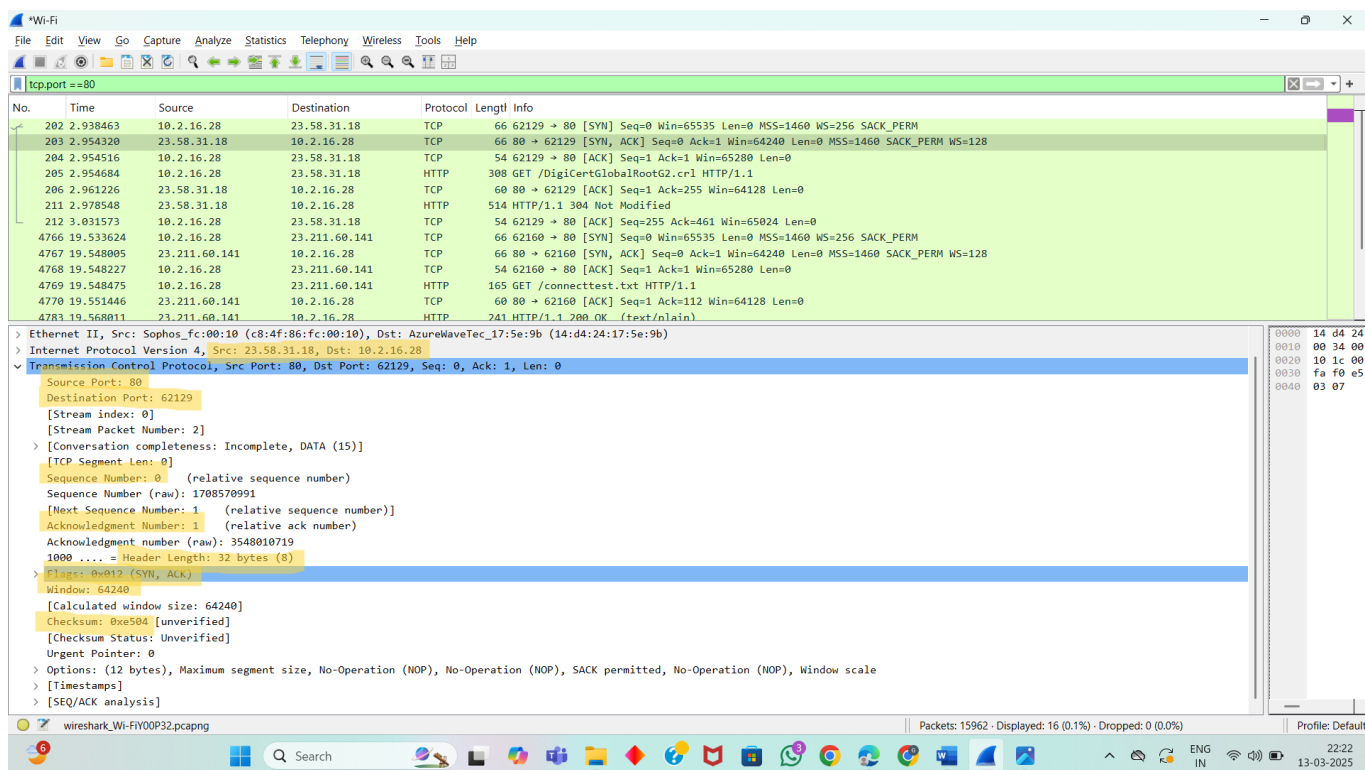
5. Fill in the following information regarding the SYN message. (highlight the details for each of the output and paste screenshot)

Source IP address	10.2.16.28
Destination IP address	23.58.31.18
Source port number	62129
Destination port number	80
Sequence number	0
Acknowledgement number	0
Flags	0x002 (SYN)
Header length	32 bytes (8)
Window size	65535
Checksum	0xff4b



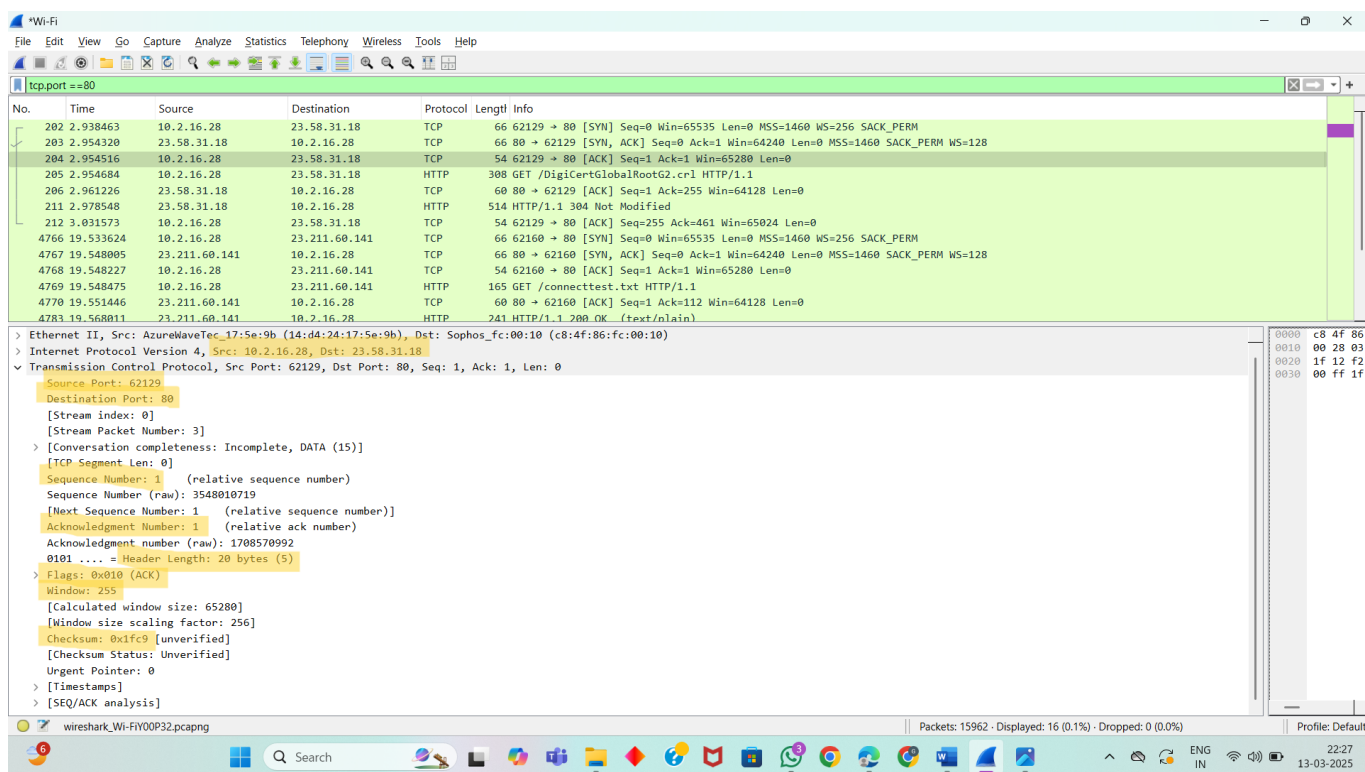
6. Fill in the following information regarding the SYN-ACK message .(highlight the details for each of the output and paste screenshot)

Source IP address	23.58.31.18
Destination IP address	10.2.16.28
Source port number	80
Destination port number	62129
Sequence number	0
Acknowledgement number	1
Header length	32 bytes (8)
Window size	64240
Flags	0x012 (SYN, ACK)
Checksum	0xe504



7. Fill in the following information regarding the ACK message. (highlight the details for each of the output and paste screenshot)

Source IP address	10.20.16.28
Destination IP address	23.58.31.18
Source port number	62129
Destination port number	80
Sequence number	1
Acknowledgement number	1
Header length	20 bytes (5)
Window size	255
Flags	0x010 (ACK)
Checksum	0x1fc9



Rubrics for Wireshark labs: (To be Filled by the Class Teacher)

Rubrics	Excellent	Fair	Poor	Marks
Understanding (2)	Understand the Concept very well. (2)	Understand the Concept (1)	Poor Understand the Concept (0)	
Usage of filters (3)	Identified and applied the filter correctly (3)	Identified the filter, but not applied correctly (2-1)	Couldn't identify and apply the filter. Just captured the packets (1)	
Attach relevant Screenshots (3)	clearly Highlighted the answers and attached the screenshots (3)	attached the screenshots, but not highlighted. (2-1)	Did not attach the screenshots (0)	
On time Submission (2)	Early or on time submission (2)	Submitted after deadline (1)	Did not Submit (0)	
Total				

Result: Thus the Capture and Analyzing TCP 3 way handshake has been implemented and successfully verified.