

ITW 7

1a. Youtube.com Ip address 142.250.9.132

1b. Source:172.16.2.195 Source Port:53644 Destination: 142.250.9.132 Destination Port: 443
Header Checksum: Unverified

1c.

No.	Time	Source	Destination	Protocol	Length	Info
1068	12.362807	173.194.24.202	172.16.2.195	TCP	66	443 → 53632 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1408 SACK_PERM WS=256
1074	12.363237	173.194.24.202	172.16.2.195	TCP	66	443 → 53631 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1408 SACK_PERM WS=256
1366	12.960146	172.16.0.1	172.16.2.195	TCP	66	53 → 53637 [SYN, ACK] Seq=0 Ack=1 Win=60000 Len=0 MSS=1376 SACK_PERM WS=1
1367	12.960146	172.16.0.1	172.16.2.195	TCP	66	53 → 53638 [SYN, ACK] Seq=0 Ack=1 Win=60000 Len=0 MSS=1376 SACK_PERM WS=1
1380	12.962365	172.16.0.1	172.16.2.195	TCP	66	53 → 53639 [SYN, ACK] Seq=0 Ack=1 Win=60000 Len=0 MSS=1376 SACK_PERM WS=1
1381	12.962365	172.16.0.1	172.16.2.195	TCP	66	53 → 53640 [SYN, ACK] Seq=0 Ack=1 Win=60000 Len=0 MSS=1376 SACK_PERM WS=1
1468	13.387747	172.16.0.1	172.16.2.195	TCP	66	53 → 53642 [SYN, ACK] Seq=0 Ack=1 Win=60000 Len=0 MSS=1376 SACK_PERM WS=1
1469	13.387747	172.16.0.1	172.16.2.195	TCP	66	53 → 53643 [SYN, ACK] Seq=0 Ack=1 Win=60000 Len=0 MSS=1376 SACK_PERM WS=1
1609	13.461498	142.250.9.132	172.16.2.195	TCP	66	443 → 53644 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1412 SACK_PERM WS=256
1723	13.750355	172.16.0.1	172.16.2.195	TCP	66	53 → 53646 [SYN, ACK] Seq=0 Ack=1 Win=60000 Len=0 MSS=1376 SACK_PERM WS=1
1724	13.750355	172.16.0.1	172.16.2.195	TCP	66	53 → 53647 [SYN, ACK] Seq=0 Ack=1 Win=60000 Len=0 MSS=1376 SACK_PERM WS=1
1775	13.957493	172.16.0.1	172.16.2.195	TCP	66	53 → 53648 [SYN, ACK] Seq=0 Ack=1 Win=60000 Len=0 MSS=1376 SACK_PERM WS=1
1776	13.957493	172.16.0.1	172.16.2.195	TCP	66	53 → 53649 [SYN, ACK] Seq=0 Ack=1 Win=60000 Len=0 MSS=1376 SACK_PERM WS=1
1885	14.341435	137.221.105.232	172.16.2.195	TCP	62	443 → 53653 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460 SACK_PERM
1905	14.509309	34.110.236.123	172.16.2.195	TCP	66	443 → 53655 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1412 SACK_PERM WS=256
1907	14.570599	34.110.236.123	172.16.2.195	TCP	66	443 → 53658 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1412 SACK_PERM WS=256
2201	15.966828	172.16.0.1	172.16.2.195	TCP	66	53 → 53662 [SYN, ACK] Seq=0 Ack=1 Win=60000 Len=0 MSS=1376 SACK_PERM WS=1
2202	15.966828	172.16.0.1	172.16.2.195	TCP	66	53 → 53663 [SYN, ACK] Seq=0 Ack=1 Win=60000 Len=0 MSS=1376 SACK_PERM WS=1
2335	16.052730	172.253.124.149	172.16.2.195	TCP	66	443 → 53665 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1412 SACK_PERM WS=256

Transmission Control Protocol, Src Port: 443, Dst Port: 53644, Seq: 0, Ack: 1, Len: 0

Source Port: 443

Destination Port: 53644

[Stream index: 35]

[Stream Packet Number: 2]

[Conversation completeness: Complete, WITH_DATA (31)]

[TCP Segment Len: 0]

Sequence Number: 0 (relative sequence number)

Sequence Number (raw): 2572509964

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

Acknowledgment Number: 1 (relative ack number)

Acknowledgment number (raw): 3429943908

1000 = Header Length: 32 bytes (0)

Flags: 0x012 [SYN, ACK]

Window: 65535

[Calculated window size: 65535]

Checksum: 0xc15f [unverified]

[Checksum Status: Unverified]

Urgent Pointer: 0

Options: (12 bytes), Maximum segment size, No-Operation (NOP), No-Operation (NOP), SACK permitted,

0000 14 5a 64 04 b7 db 00 50 e8 0a 7d b3 08 00 45 00 72 . . P . . . E .
0010 00 34 00 00 40 00 76 06 bd 72 fe fa 09 04 ac 10 4 . @ v
0020 02 c3 01 bb d1 8c 99 55 63 0c cc 70 ca 64 80 12 U c . p d .
0030 ff ff c1 5f 00 00 02 04 05 84 01 01 04 02 01 03
0040 03 08

1d.

No.	Time	Source	Destination	Protocol	Length	Info
1446	13.069757	172.16.2.195	142.250.9.132	QUIC	77	Protected Payload (KP0), DCID=F39bae61129939ee
1452	13.083183	142.250.9.132	172.16.2.195	QUIC	162	Protected Payload (KP0)
1453	13.083467	172.16.2.195	142.250.9.132	QUIC	73	Protected Payload (KP0), DCID=F39bae61129939ee
1457	13.097398	142.250.9.132	172.16.2.195	QUIC	67	Protected Payload (KP0)
1532	13.428795	172.16.2.195	142.250.9.132	TCP	66	53644 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
1609	13.461498	142.250.9.132	172.16.2.195	TCP	66	443 → 53644 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1412 SACK_PERM WS=256
1611	13.461957	172.16.2.195	142.250.9.132	TCP	54	53644 → 443 [ACK] Seq=1 Ack=1 Win=131072 Len=0
1616	13.463533	172.16.2.195	142.250.9.132	TCP	1466	53644 → 443 [ACK] Seq=1 Ack=1 Win=131072 Len=1412 [TCP PDU reassembled in 1616]
1616	13.463538	172.16.2.195	142.250.9.132	TLSv1.3	409	Client Hello (SNI=1h6.googleusercontent.com)
1624	13.493976	142.250.9.132	172.16.2.195	TCP	60	443 → 53644 [ACK] Seq=1 Ack=1413 Win=268288 Len=0
1625	13.493976	142.250.9.132	172.16.2.195	TCP	60	443 → 53644 [ACK] Seq=1 Ack=1768 Win=268032 Len=0
1626	13.507829	142.250.9.132	172.16.2.195	TLSv1.3	1466	Server Hello, Change Cipher Spec
1627	13.507829	142.250.9.132	172.16.2.195	TCP	1466	443 → 53644 [PSH, ACK] Seq=1413 Ack=1768 Win=268032 Len=1412 [TCP PDU reassembled in 1633]
1628	13.507829	142.250.9.132	172.16.2.195	TCP	1466	443 → 53644 [ACK] Seq=2825 Ack=1768 Win=268032 Len=1412 [TCP PDU reassembled in 1633]
1629	13.507829	142.250.9.132	172.16.2.195	TCP	1466	443 → 53644 [PSH, ACK] Seq=4237 Ack=1768 Win=268032 Len=1412 [TCP PDU reassembled in 1633]
1630	13.507829	142.250.9.132	172.16.2.195	TCP	1466	443 → 53644 [ACK] Seq=5649 Ack=1768 Win=268032 Len=1412 [TCP PDU reassembled in 1633]
1631	13.507829	142.250.9.132	172.16.2.195	TCP	1466	443 → 53644 [PSH, ACK] Seq=7061 Ack=1768 Win=268032 Len=1412 [TCP PDU reassembled in 1633]
1632	13.507829	142.250.9.132	172.16.2.195	TCP	1466	443 → 53644 [ACK] Seq=8473 Ack=1768 Win=268032 Len=1412 [TCP PDU reassembled in 1633]
1633	13.507829	142.250.9.132	172.16.2.195	TLSv1.3	628	Application Data
1634	13.507233	172.16.2.195	142.250.9.132	TCP	54	53644 → 443 [ACK] Seq=1768 Ack=10459 Win=131072 Len=0

Internet Protocol Version 4, Src: 172.16.2.195, Dst: 142.250.9.132

Transmission Control Protocol, Src Port: 53644, Dst Port: 443, Seq: 1, Ack: 1, Len: 1412

Source Port: 53644

Destination Port: 443

[Stream index: 35]

[Stream Packet Number: 4]

[Conversation completeness: Complete, WITH_DATA (31)]

[TCP Segment Len: 1412]

Sequence Number: 1 (relative sequence number)

Sequence Number (raw): 3429943908

[Next Sequence Number: 1413 (relative sequence number)]

Acknowledgment Number: 1 (relative ack number)

Acknowledgment number (raw): 2572509965

0101 = Header Length: 20 bytes (5)

Flags: 0x010 [ACK]

Window: 512

[Calculated window size: 131072]

[Window size scaling factor: 256]

Checksum: 0x2cdb [unverified]

[Checksum Status: Unverified]

0020 09 84 d1 8c 01 bb cc 70 ca 64 99 55 63 0d 50 10 p d U c P .
0030 02 00 2c db 00 00 16 03 01 06 e2 01 00 06 de 03
0040 03 d0 02 d6 08 54 a0 30 ea 8b a3 3b 1d 14 36 c8 T G .
0050 a0 6f 17 0b 97 3f 9b 40 cf c6 e7 da 0f a0 52 e9
0060 b5 20 44 78 54 b0 2e e9 d1 e4 e5 e5 7f 05 05 d4
0070 e6 24 e1 65 0a d9 0c 71 78 f9 e1 36 48 cd 81 c1
0080 49 08 00 20 ea 13 01 13 02 13 03 c0 2b c0 2f
0090 c0 2c c0 30 cc a9 cc a8 c0 13 c0 14 00 9c 00 9d
00a0 00 2f 00 35 01 00 06 75 5a 5a 00 00 23 00 00
00b0 00 1b 00 03 02 00 02 00 0d 00 12 00 10 04 03 08
00c0 04 04 01 05 03 08 05 01 08 06 06 01 00 12 00
00d0 00 44 69 00 05 00 03 02 68 32 00 10 00 00 0c
00e0 02 68 12 08 68 74 74 70 2f 21 2e 31 00 00 02
00f0 01 00 00 00 1e 00 1c 00 00 19 6c 68 36 2e 67
0100 6f 6f 6f 6c 65 75 73 65 72 63 6f 6e 74 65 6e 74
0110 2e 63 6f 6d 00 2b 00 07 06 8a 8a 03 04 03 03 00
0120 33 04 ef 04 ed ca ca 00 01 00 63 99 04 c0 88 bd 3
0130 5a 6e 52 57 97 0d 9d 31 a6 93 06 14 51 ca eb 93
0140 0f 3b 1e 9c 2b 22 03 92 55 c2 0e 4a 20 58 24
0150 3c 92 59 83 76 2a 2b 04 bc 0e af 54 bc e7 31 7d
0160 c9 07 16 20 58 0b 99 81 64 52 b9 35 6e 85
0170 50 44 0c 14 26 05 50 19 c6 c9 33 5d a7 3c 92

Packets: 2638, Discarded: 102 (4.1%) - Dropped: 0 (0.0%)