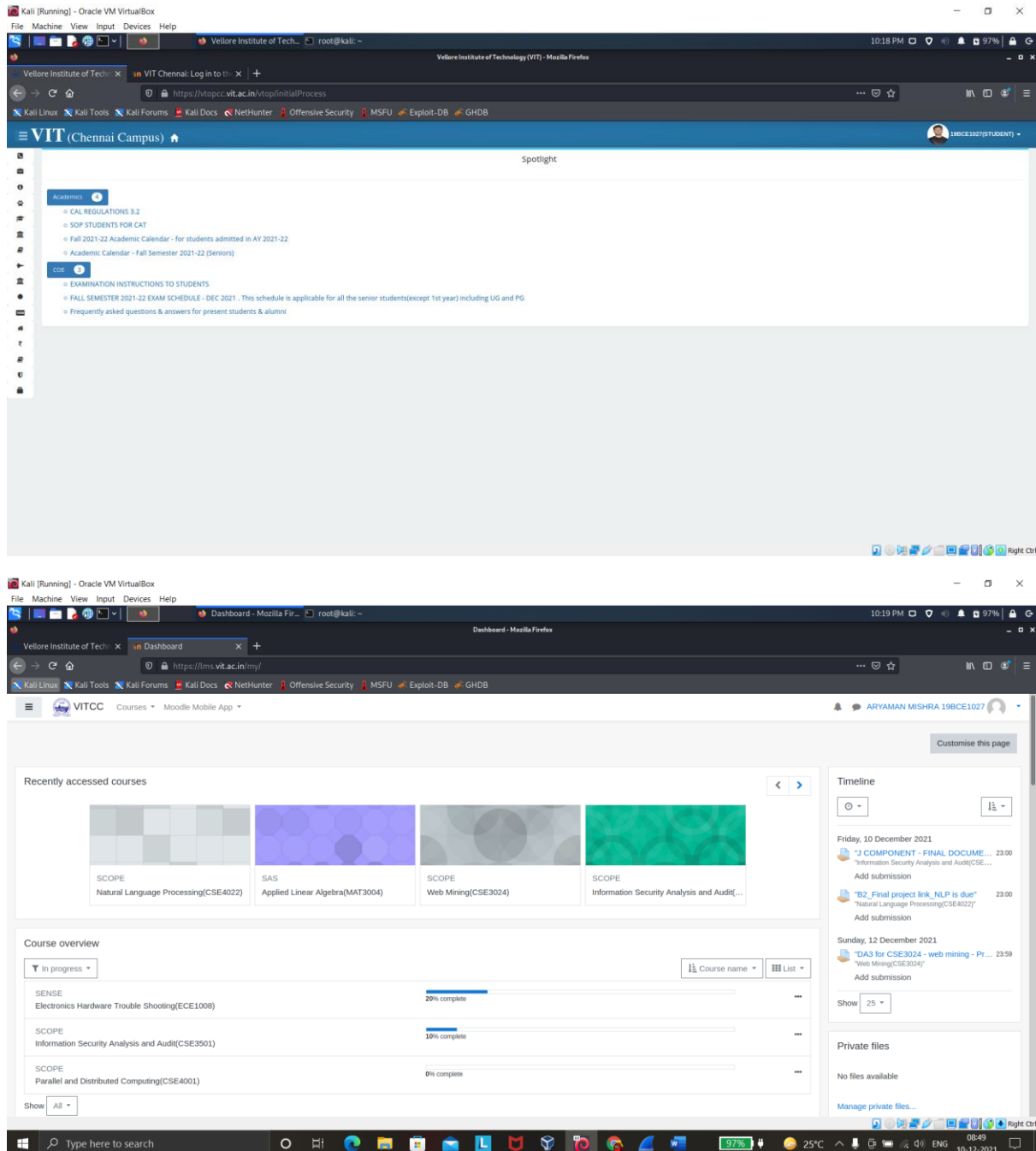


ARYAMAN MISHRA

19BCE1027

Enter into MOODLE and VTOP applications using the necessary login credentials and identify the user names and passwords of the two applications in the trace files of Wireshark. Display the screenshots that are showing the usernames and passwords in the trace and the respective ASCII codes as well.



Wi-Fi

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

tcp contains time

No.	Time	Source	Destination	Protocol	Length	Info
2912	7.028371	115.240.194.17	192.168.29.120	TCP	1514	443 → 50195 [ACK] Seq=236590 Ack=4856 Win=39296 Len=1460 [TCP segment of a reassembled PDU]
7776	23.066695	192.168.29.111	115.240.194.4	TLSv1.2	571	Client Hello
7875	23.330900	192.168.29.111	115.240.194.4	TLSv1.2	594	Client Hello
7896	23.341777	192.168.29.111	115.240.194.4	TLSv1.2	594	Client Hello
7897	23.343711	192.168.29.111	115.240.194.4	TLSv1.2	594	Client Hello
7902	23.347971	192.168.29.111	115.240.194.4	TLSv1.2	594	Client Hello
7903	23.350016	192.168.29.111	115.240.194.4	TLSv1.2	594	Client Hello
12306	31.255528	192.168.29.120	115.240.194.4	TLSv1.2	571	Client Hello
12373	31.492481	192.168.29.120	115.240.194.4	TLSv1.2	571	Client Hello
12376	31.495430	192.168.29.120	115.240.194.4	TLSv1.2	571	Client Hello
12386	31.498953	192.168.29.120	115.240.194.4	TLSv1.2	571	Client Hello
12391	31.501813	192.168.29.120	115.240.194.4	TLSv1.2	571	Client Hello
12394	31.511501	192.168.29.120	115.240.194.4	TLSv1.2	571	Client Hello
17260	49.347336	192.168.29.120	115.240.194.4	TLSv1.2	571	Client Hello
17264	49.360312	192.168.29.120	115.240.194.4	TLSv1.2	571	Client Hello
17282	49.372109	192.168.29.120	115.240.194.4	TLSv1.2	571	Client Hello
17285	49.373975	192.168.29.120	115.240.194.4	TLSv1.2	571	Client Hello
17489	49.463301	192.168.29.120	115.240.194.4	TLSv1.2	571	Client Hello

▼ Frame 2912: 1514 bytes on wire (12112 bits), 1514 bytes captured (12112 bits) on interface \Device\NPF_{9A26F4A2-063C-4748-B045-13109A0D0842E}, id 0

- Interface id: 0 (\Device\NPF_{9A26F4A2-063C-4748-B045-13109A0D0842E})
- Encapsulation type: Ethernet (1)
- Arrival Time: Dec 10, 2021 08:50:31.538957000 India Standard Time
- [Time shift for this packet: 0.000000000 seconds]
- Epoch Time: 1639106431.538957000 seconds
- [Time delta from previous captured frame: 0.000000000 seconds]
- [Time delta from previous displayed frame: 0.000000000 seconds]
- [Time since reference or first frame: 7.020371000 seconds]
- Frame Number: 2912
- Frame Length: 1514 bytes (12112 bits)
- Capture Length: 1514 bytes (12112 bits)
- [Frame is marked: False]
- [Frame is ignored: False]
- [Protocols in frame: eth:ethertype:ip:tcp]
- [Coloring Rule Name: TCP]
- [Coloring Rule String: tcp]

▼ Ethernet II, Src: Sercomm_0e:aa:33 (30:49:50:2e:aa:33), Dst: IntelCor_a5:13:ba (50:e0:85:a5:13:ba)

- Destination: IntelCor_a5:13:ba (50:e0:85:a5:13:ba)
- Source: Sercomm_0e:aa:33 (30:49:50:2e:aa:33)

The frame matched this coloring rule string (frame.coloring_rule.string)

Packets: 20265 · Displayed: 18 (0.1%) · Dropped: 0 (0.0%) Profile: Default

Wi-Fi

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

tcp contains vstop

No.	Time	Source	Destination	Protocol	Length	Info
1429	6.851108	192.168.29.120	115.240.194.17	TLSv1.2	571	Client Hello
1535	6.328403	192.168.29.120	115.240.194.17	TLSv1.2	571	Client Hello
1539	6.331095	192.168.29.120	115.240.194.17	TLSv1.2	571	Client Hello
1542	6.332301	192.168.29.120	115.240.194.17	TLSv1.2	571	Client Hello
1545	6.333316	192.168.29.120	115.240.194.17	TLSv1.2	571	Client Hello
1549	6.340305	192.168.29.120	115.240.194.17	TLSv1.2	571	Client Hello

▼ Frame 1549: 571 bytes on wire (4568 bits), 571 bytes captured (4568 bits) on interface \Device\NPF_{9A26F4A2-063C-4748-B045-13109A0D0842E}, id 0

- Interface id: 0 (\Device\NPF_{9A26F4A2-063C-4748-B045-13109A0D0842E})
- Encapsulation type: Ethernet (1)
- Arrival Time: Dec 10, 2021 08:50:30.858891000 India Standard Time
- [Time shift for this packet: 0.000000000 seconds]
- Epoch Time: 1639106430.858891000 seconds
- [Time delta from previous captured frame: 0.000274000 seconds]
- [Time delta from previous displayed frame: 0.0006989000 seconds]
- [Time since reference or first frame: 6.340305000 seconds]
- Frame Number: 1549
- Frame Length: 571 bytes (4568 bits)
- Capture Length: 571 bytes (4568 bits)
- [Frame is marked: False]
- [Frame is ignored: False]
- [Protocols in frame: eth:ethertype:ip:tcp:tls]
- [Coloring Rule Name: TCP]
- [Coloring Rule String: tcp]

▼ Ethernet II, Src: IntelCor_a5:13:ba (50:e0:85:a5:13:ba), Dst: Sercomm_0e:aa:33 (30:49:50:2e:aa:33)

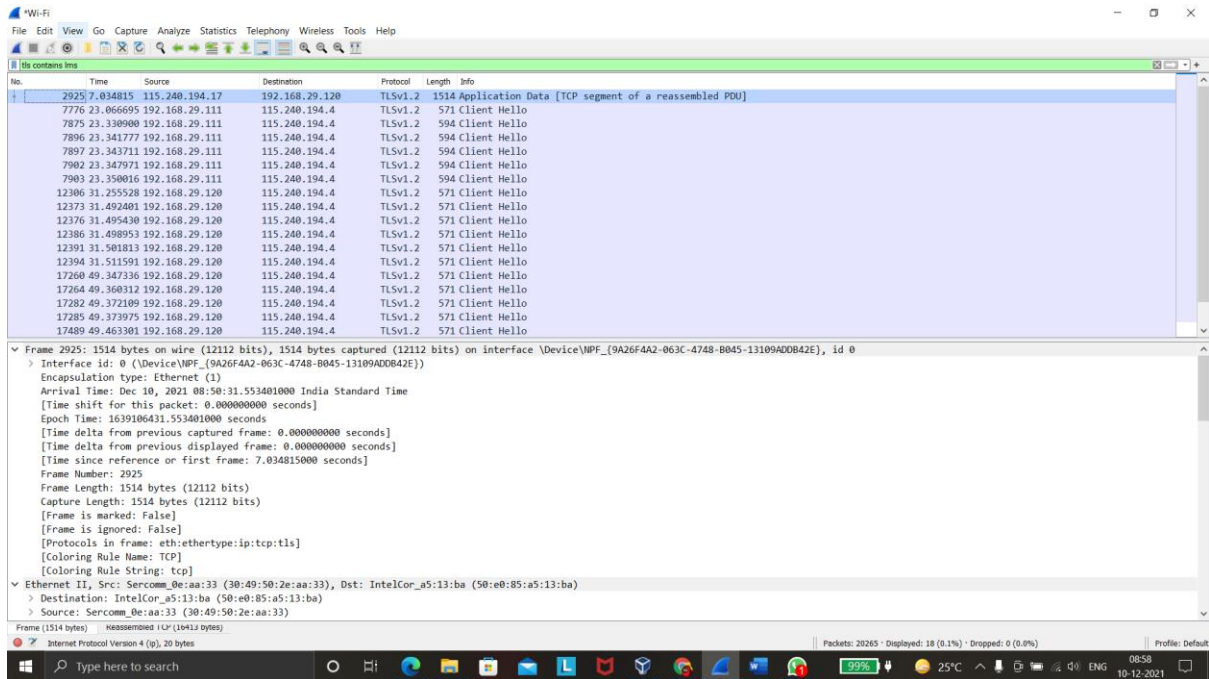
- Destination: Sercomm_0e:aa:33 (30:49:50:2e:aa:33)
- Source: IntelCor_a5:13:ba (50:e0:85:a5:13:ba)
- Type: IPv4 (0x0800)

▼ Internet Protocol Version 4, Src: 192.168.29.120, Dst: 115.240.194.17

- 0100 = Version: 4
- 0101 = Header Length: 20 bytes (5)
- ▼ Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
- 0000 00.. = Differentiated Services Codepoint: Default (0)
-00 = Explicit Congestion Notification: Not ECN-Capable Transport (0)
- Total Length: 557
- Identification: 0x51ca (37322)
- ▼ Flags: 0x00, Don't Fragment
- 0... = Reserved bit: Not set
- = Don't Fragment: Set

Internet Protocol Version 4 (ip), 20 bytes

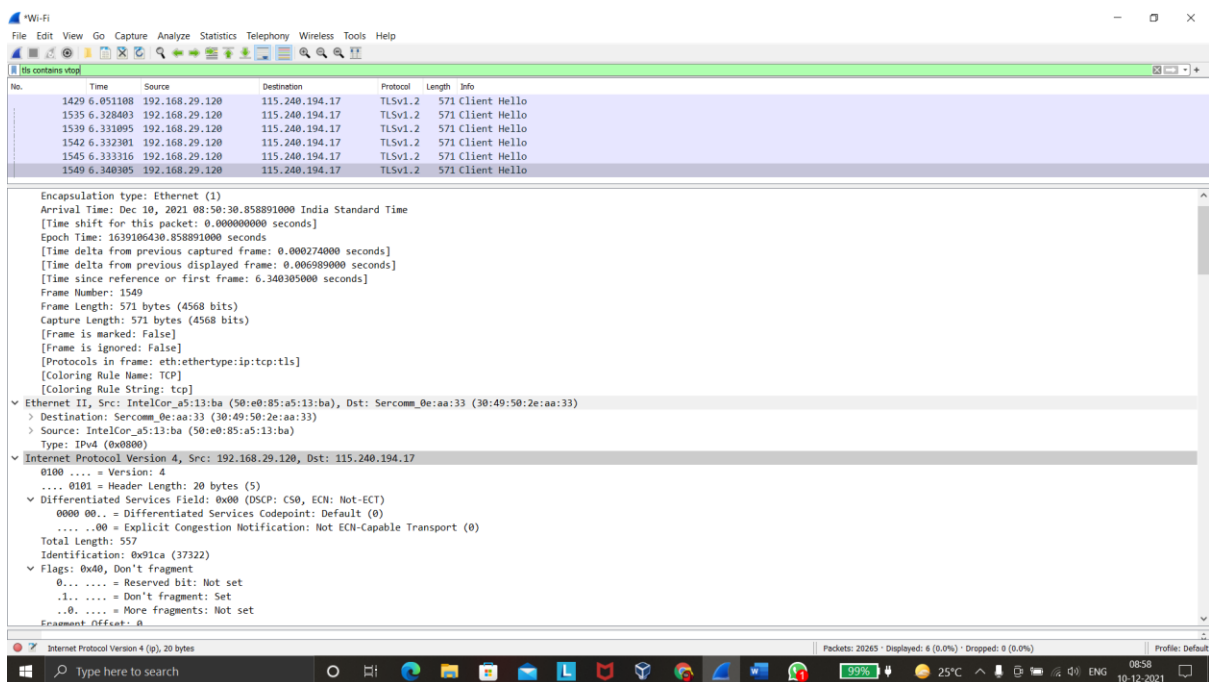
Packets: 20265 · Displayed: 6 (0.0%) · Dropped: 0 (0.0%) Profile: Default



Open **Wireshark-tutorial-on-decrypting-HTTPS-SSL-TLS-traffic.pcap** in Wireshark. Use a basic web filter as described in this previous [tutorial about Wireshark filters](#). Our basic filter for Wireshark 3.x is:

(http.request or tls.handshake.type eq 1) and !(ssdp)

Open **Wireshark-tutorial-on-decrypting-HTTPS-SSL-TLS-traffic.pcap** in Wireshark. Then use the menu path **Edit --> Preferences** to bring up the Preferences Menu



The image shows a Wireshark packet capture window titled "Wireshark - Packet 2647 - Wi-Fi". The packet list on the left shows a single packet (2647) of type "TLSv1.2" with a length of 1000 bytes. The packet details pane on the right shows the following structure:

- Cipher Suites Length: 32
 - > Cipher Suites (16 suites)
- Compression Methods Length: 1
 - > Compression Methods (1 method)
- Extensions Length: 403
 - > Extension: Reserved (GREASE) (len=0)
 - > Extension: server_name (len=21)
 - Type: server_name (0)
 - Length: 21
 - > Server Name Indication extension
 - Server Name list length: 19
 - Server Name Type: host_name (0)
 - Server Name length: 16
 - Server Name: vtopcc.vit.ac.in
 - > Extension: extended_master_secret (len=0)

The packet bytes pane at the bottom shows the raw data in hexadecimal and ASCII. The ASCII column contains the following text:

```
.....U...|B-V-J.  
...q...p...8yQ..  
K...g...B...Q...  
...\JJ...+++/..  
...0...  
.../5...  
.....vto pcc.vit.  
ac.in...  
...zz...  
...h2..  
http/1.1...  
.....  
)zz...|Pf..  
...9WAV...fq...  
...R...0...j...  
...+...zz..  
.....Di...h2..
```

No.	Time	Source	Destination	Protocol	Length	Server Name	Info
357	2.498881	2405:201:6008:30c8::	2404:6800:4002:82d::	QUIC		1292 client65.google.com	Initial, OCID=3df88a1eb959ecab, PKN: 1, PADDING, PING, PADDING, PING, CRYPTO, PING, PADDING,
875	7.731410	2405:201:6008:30c8::	2404:6800:4002:80c::	TLSv1.3		591 beacons.gcp.gvt2.com	Client Hello
828	7.732596	2405:201:6008:30c8::	2404:6800:4002:80c::	TLSv1.3		591 beacons.gcp.gvt2.com	Client Hello
1875	9.727572	192.168.1.210	130.211.16.53	TLSv1.3		644 .joinhoney.com	Client Hello
2015	9.464364	192.168.1.210	130.211.16.229	TLSv1.3		644 .joinhoney.com	Client Hello
2044	9.459463	192.168.1.210	13.107.22.200	TLSv1.2		628 bat.bing.com	Client Hello
2300	10.647081	192.168.1.210	52.114.33.123	TLSv1.2		571 api-apac.flightproxy.te.	Client Hello
2465	11.811860	2405:201:6008:30c8::	2404:6800:4009:82f::	QUIC		1292 www.google.com	Initial, OCID=ec0cb88ee1e728, PKN: 1, PADDING, CRYPTO, CRYPTO, CRYPTO, PADDING, PING,
2647	12.568370	192.168.1.210	115.240.194.17	TLSv1.2		571 vtopcc.vit.ac.in	Client Hello
2651	12.577580	192.168.1.210	115.240.194.17	TLSv1.2		571 vtopcc.vit.ac.in	Client Hello
3514	13.038667	192.168.1.210	54.160.135.242	TLSv1.2		571 mip.api.mcafeebeadvviso.	Client Hello
4076	13.113552	192.168.1.210	115.240.194.17	TLSv1.2		571 vtopcc.vit.ac.in	Client Hello
4077	13.113740	192.168.1.210	115.240.194.17	TLSv1.2		571 vtopcc.vit.ac.in	Client Hello
4078	13.113955	192.168.1.210	115.240.194.17	TLSv1.2		571 vtopcc.vit.ac.in	Client Hello
4079	13.114125	192.168.1.210	115.240.194.17	TLSv1.2		571 vtopcc.vit.ac.in	Client Hello
4539	13.204134	192.168.1.210	54.160.135.242	TLSv1.2		571 mip.api.mcafeebeadvviso.	Client Hello
4882	14.664823	2405:201:6008:30c8::	2404:6800:4009:82f::	QUIC		1292 www.google.com	Initial, OCID=527f23a1391b204, PKN: 1, CRYPTO, PADDING, CRYPTO, CRYPTO, PING, PADDING,
7702	13.370187	192.168.1.210	54.160.135.242	TLSv1.2		571 mip.api.mcafeebeadvviso.	Client Hello
7706	13.388870	192.168.1.210	54.160.135.242	TLSv1.2		571 mip.api.mcafeebeadvviso.	Client Hello
7701	13.846621	192.168.1.210	54.160.135.242	TLSv1.2		571 mip.api.mcafeebeadvviso.	Client Hello
8141	14.016935	2405:201:6008:30c8::	2404:6800:4002:80c::	TLSv1.3		591 beacons.gcp.gvt2.com	Client Hello
8145	14.018024	2405:201:6008:30c8::	2404:6800:4002:80c::	TLSv1.3		591 beacons.gcp.gvt2.com	Client Hello
8164	14.057234	2405:201:6008:30c8::	2404:6800:4009:813::	TLSv1.3		591 google.co.in	Client Hello
8316	14.326130	192.168.1.210	35.206.197.100	TLSv1.3		571 e2c31.gcp.gvt2.com	Client Hello
8338	14.410346	192.168.1.210	35.216.18.75	TLSv1.3		571 e2c34.gcp.gvt2.com	Client Hello
8396	14.655255	192.168.1.210	35.216.18.75	TLSv1.3		571 e2c34.gcp.gvt2.com	Client Hello
8493	15.059232	2405:201:6008:30c8::	2404:6800:4002:80b::	TLSv1.3		591 beacons.gcp.gvt2.com	Client Hello
8535	15.254901	2405:201:6008:30c8::	2404:6800:4002:80b::	TLSv1.3		591 beacons.gcp.gvt2.com	Client Hello
11884	14.506400	192.168.1.210	35.227.159.135	TLSv1.3		571 e2c27.gcp.gvt2.com	Client Hello
12817	16.849767	2405:201:6008:30c8::	2404:6800:4009:82f::	QUIC		1292 www.google.com	Initial, OCID=eab6f34f6cd0740, PKN: 1, CRYPTO, PADDING, PING, PADDING, CRYPTO, PADDING, PING,
13112	17.125418	2405:201:6008:30c8::	2404:6800:4009:82b::	QUIC		1292	Initial, OCID=4ea03ddaf32262f, PKN: 4, CRYPTO, CRYPTO, PADDING, CRYPTO, PADDING, CRYPTO, C
13155	17.288028	2405:201:6008:30c8::	2404:6800:4002:81d::	QUIC		1292 play.google.com	Initial, OCID=b8d2b891e09638a, PKN: 1, PADDING, CRYPTO, PADDING, CRYPTO, PADDING, CRYPTO, C
13160	17.366515	2405:201:6008:30c8::	2404:6800:4009:82f::	QUIC		1292 www.google.com	Initial, OCID=f7d048d2f1acfb2a, PKN: 1, CRYPTO, CRYPTO, PING, PING, PADDING, PADDING, CRYPTO,
13421	19.736682	2405:201:6008:30c8::	2404:6800:4009:829::	QUIC		1292 safebrowsing.google.com	Initial, OCID=f752521f1ef8feab, PKN: 1, PING, PADDING, CRYPTO, PADDING, PING, PADDING, CRYPTO,

Wireshark · Follow TCP Stream (tcp.stream eq 105) · Wi-Fi

.....xG...16..U.m...y...uv.....wD.....:f..#70.....o.....V[.....**.....+./..0...../5...jj.....
lms.vit.ac.in.....
.....
.....#..{.....2!>@WH..h.W..Ep
.....4..~.G*..&/&...?..8}.....e./:..c..Qro!-^..s...c..j..(..8y...I.z...:..?.....G..=..4%.P"...
4..L
...W,.....2.Z.T>w...Gn..fy-&.....w.....n....M.....h2.http/1.1.....
.....3+.).....\$.u..cD.d;.....RDP4.....90..-.....+..
.....Di.....h2.....\.....xn.....C...n.....}.<Dk...f..#70....o.....V[.....
0.....http/1.1.....(z'...Z..%.....').....]+.tK.\Z#^.....(.....V...A..C..".....;I...e3....'8C
..i.....T(1CC.r.-ja%~N.....i.l.....0.aU]%ea.....x.Ta.C./..LG.Y^..\...J.d..U.m.....w]*.....z..Cf.....Gi..z_aE=-.X.....`.e(t.
...L.R..A..A...\$.S..1...u.....c.w..e..UL..N..'
...Y[...kH&.)\$.0..j...Z...gS<....!K....*.....3..c+..l.A.V.L&H&.M.|.....OB.WU.9.....B..R.../[=.....I..d...8...D.....".u.!x.A.~.)
S..&
.8.....Co#1.*...B4.|m1..'@[0.txS...\$o<...~..
...T.....":Nz..7!..T..4..E..(d..j|.C..?..-...p....wL.;T...W.{b...*06..uEW5\$....\$.Sx.
(.....T.<.....F..E.w).~.....z..e..j|.V.....F.....;L...~.....V>..P.....!M).<-.....|.q.....(.....?..)/...\$.KXU...p.../]..a.)...
gs.b...r+...K..9%.a.....wX[J.....>...P..8T?.m(.....3.K.8j.
...L.R..A..A...\$.S..1...u.....c.w..e..UL..N..'
D.xFn.7(.3Ka.ki..S.....c^..0....Aw.W..VR....R....NZ%.\?..w....la....3..R9..TS..{.1.|ch\$..T.%..O..?5}#T...
..G.....
.....S...[o..o...(\w..B....xj)..=...I..R..z.....a.X.Q...
...3..
...9.p.(...9.R:..%..0..\$.....|.g>.f.T..Vg4.p.|g0hF.....kU.8nH.1./!I...Yw.;_)...f..&6..11.....\;:.....x.0..~.4...2..}
Fd<U..I..\$Y..>.....jhSw.y..e.....
p.Ec%/j.....j...17..b..i..
..F..^..H....j..@.....;...uO..L'/.{nc.^..Kuk..%.3..6Z....
.t.m.ab1...w^..yw.....s..jhdNR.....o.)..m.Y.z2...T.oMF...>.G.oQ....1..S..
..>.K|.<%).\$.p.....S.E.....z'...Z..2q....8u....*f....".{v.1..K..S(q..W.c..n...fL.Q..(.....N>..7.7..2.....i..c.....=Q...c.).....
...BRR*.V."5..N...0...r.....IX#c3..0.....R..
.....]'.~'.n...!F.d.....=...pz.....&C.n.....0h.....'.....k.Y...f..Z..sM..r...J..O./?Y.L...vBv&..A...L.....7...u.K.+.
2...y.V3.....?..?..B.Ig...j.h'G..."%H...
(S...S:..x8..~..oV...3..n.....h.....0...t...}|...w|...a.....z'..Z...|7%.....P...qH

Packet 13994. 3 client pkts, 3 server pkts. 3 turns. Click to select.

Entire conversation (2371 bytes) Show data as ASCII Stream 105

Find: Find Next

Filter Out This Stream Print Save as... Back Close Help

Wi-Fi

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

tcp.stream eq 105

No.	Time	Source	Destination	Protocol	Length	Server Name	Info
13981	61.566128	192.168.29.120	115.240.194.4	TCP	66		50430 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
13992	61.686560	115.240.194.4	192.168.29.120	TCP	66		443 → 50430 [SYN, ACK] Seq=0 Ack=1 Win=16860 Len=0 MSS=1460 SACK_PERM=1 WS=2
13993	61.686601	192.168.29.120	115.240.194.4	TCP	54		50430 → 443 [ACK] Seq=1 Ack=1 Win=13128 Len=0
13994	61.686871	192.168.29.120	115.240.194.4	TLShv1.2	571	lms.vit.ac.in	Client Hello
14006	61.647384	115.240.194.4	192.168.29.120	TCP	54		443 → 50430 [ACK] Seq=1 Ack=518 Win=16060 Len=0
14007	61.647384	115.240.194.4	192.168.29.120	TLShv1.2	286		Server Hello, Change Cipher Spec, Encrypted Handshake Message
14008	61.647591	192.168.29.120	115.240.194.4	TLShv1.2	105		Change Cipher Spec, Encrypted Handshake Message
14009	61.647732	192.168.29.120	115.240.194.4	TLShv1.2	1259		Application Data
14016	61.691888	115.240.194.4	192.168.29.120	TCP	54		443 → 50430 [ACK] Seq=153 Ack=1774 Win=18470 Len=0
14410	62.798163	115.240.194.4	192.168.29.120	TLShv1.2	469		Application Data
14439	62.846159	192.168.29.120	115.240.194.4	TCP	54		50430 → 443 [ACK] Seq=1774 Ack=568 Win=130816 Len=0
15174	67.802031	115.240.194.4	192.168.29.120	TLShv1.2	85		Encrypted Alert
15175	67.802031	115.240.194.4	192.168.29.120	TCP	54		443 → 50430 [FIN, ACK] Seq=599 Ack=1774 Win=18470 Len=0
15176	67.802207	192.168.29.120	115.240.194.4	TCP	54		50430 → 443 [ACK] Seq=1774 Ack=600 Win=130560 Len=0
15644	72.746845	192.168.29.120	115.240.194.4	TCP	54		50430 → 443 [FIN, ACK] Seq=1774 Ack=600 Win=130560 Len=0
15645	72.746872	192.168.29.120	115.240.194.4	TCP	54		50430 → 443 [RST, ACK] Seq=1775 Ack=600 Win=0 Len=0

