

Practical - 4

Aim: - Packet capturing and network scanning using Wireshark.

Wireshark: -

- Wireshark is a free and open source packet analyzer.
- It is used for network troubleshooting, analysis, software and communications protocol development, and education.
- Wireshark is cross-platform, using the Qt widget toolkit in current releases to implement its user interface, and using pcap to capture packets; it runs on Linux, macOS, BSD, Solaris, some other Unix-like operating systems, and Microsoft Windows.
- There is also a terminal-based (non-GUI) version called TShark. Wireshark, and the other programs distributed with it such as TShark, are free software, released under the terms of the GNU General Public License.

Capturing Packets: -

Wireshark 1.12.1 (v1.12.1-0-g01b65bf from master-1.12)

File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help

Filter: Expression... Clear Apply Save

No.	Time	Source	Destination	Protocol	Length	Info
75	10.5269260	151.101.2.49	192.168.0.102	TCP	1494	[TCP segment of a reassembled PDU]
76	10.5277800	151.101.2.49	192.168.0.102	TLSv1.2	1494	Application Data
77	10.5281620	192.168.0.102	151.101.2.49	TCP	54	1885-443 [ACK] Seq=247 Ack=28827 win=2835 Len=0
78	10.5374530	151.101.2.49	192.168.0.102	TCP	1494	[TCP segment of a reassembled PDU]
79	10.5399700	151.101.2.49	192.168.0.102	TLSv1.2	1494	Application Data
80	10.5403860	192.168.0.102	151.101.2.49	TCP	54	1885-443 [ACK] Seq=247 Ack=31707 win=2835 Len=0
81	10.5572590	151.101.2.49	192.168.0.102	TCP	1494	[TCP segment of a reassembled PDU]
82	10.5603200	151.101.2.49	192.168.0.102	TLSv1.2	1494	Application Data
83	10.5607660	192.168.0.102	151.101.2.49	TCP	54	1885-443 [ACK] Seq=247 Ack=34587 win=2835 Len=0
84	10.5747750	151.101.2.49	192.168.0.102	TCP	1494	[TCP segment of a reassembled PDU]
85	10.5771780	151.101.2.49	192.168.0.102	TLSv1.2	1494	Application Data
86	10.5774660	192.168.0.102	151.101.2.49	TCP	54	1885-443 [ACK] Seq=247 Ack=37467 win=2835 Len=0
87	10.5952300	151.101.2.49	192.168.0.102	TLSv1.2	1494	Application Data
88	10.5966340	151.101.2.49	192.168.0.102	TLSv1.2	1222	Application Data
89	10.5970080	192.168.0.102	151.101.2.49	TCP	54	1885-443 [ACK] Seq=247 Ack=40075 win=2835 Len=0
90	10.6127940	192.168.0.102	151.101.2.49	TLSv1.2	177	Application Data
91	10.7713920	151.101.2.49	192.168.0.102	TLSv1.2	234	Application Data
92	10.8216400	192.168.0.102	151.101.2.49	TCP	54	1885-443 [ACK] Seq=370 Ack=40255 win=2834 Len=0

Frame 1: 571 bytes on wire (4568 bits), 571 bytes captured (4568 bits) on interface 0

Ethernet II, Src: HonHaiPR_9e:a1:39 (9c:ad:97:9e:a1:39), Dst: TendaTec_5d:29:b0 (c8:3a:35:5d:29:b0)

Internet Protocol Version 4, Src: 192.168.0.102 (192.168.0.102), Dst: 104.27.189.128 (104.27.189.128)

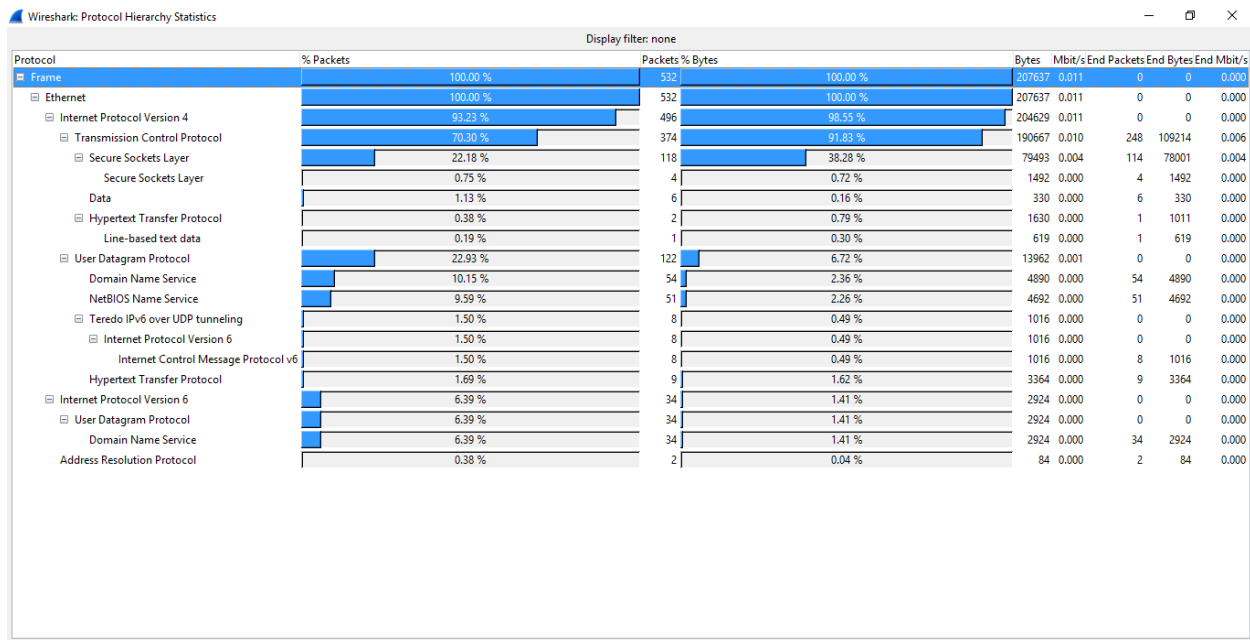
Transmission Control Protocol, Src Port: 1941 (1941), Dst Port: 443 (443), Seq: 1, Ack: 1, Len: 517

Secure Sockets Layer

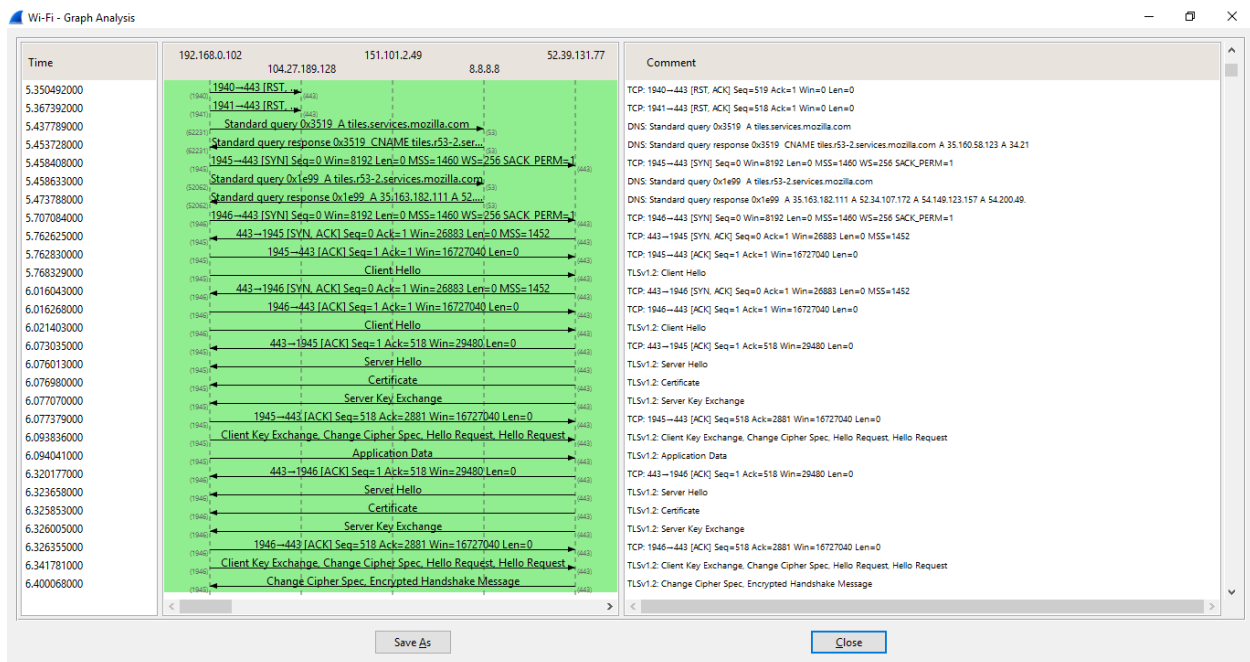
0000 c8 3a 35 5d 29 b0 9c ad 97 9e a1 39 08 00 45 00 :5]}... ..9..E.
 0010 02 2d 44 12 40 00 80 06 ce 0e c0 a8 00 66 68 1b :-D.@... ..fh.
 0020 bd 80 07 95 01 bb 09 96 0b ed 53 1f 36 79 50 18 :.....S.6yp.
 0030 01 04 d9 47 00 00 16 03 01 02 00 01 00 01 fc 03 :.G.....
 0040 03 81 c7 6a 6d 02 2f 95 b3 54 4c 92 84 06 f3 a8 :...jm./..TL.....
 0050 f0 03 54 c5 f0 c1 6c 40 2d 2d 2d 2d 2d 2d 2d 2d :.....
 0060 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 :.....

Wi-Fi: <live capture in progress> File: C:\Use... | Packets: 160 | Displayed: 160 (100.0%) | Profile: Default

Protocol Hierarchy: -



Flow Graph: -



TCP Handshaking: -

Capturing from Wi-Fi [Wireshark 1.12.1 (v1.12.1-0-g01b65bf from master-1.12)]

File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help

Filter: tcp Expression... Clear Apply Save

No.	Time	Source	Destination	Protocol	Length	Info
19	5.45840800	192.168.0.102	52.39.131.77	TCP	66	1945-443 [SYN] Seq=0 win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
22	5.70708400	192.168.0.102	52.39.131.77	TCP	66	1946-443 [SYN] Seq=0 win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
23	5.76262500	192.168.0.102	52.39.131.77	TCP	58	443-1945 [SYN, ACK] Seq=0 Ack=1 win=26883 Len=0 MSS=1452
24	5.76283000	192.168.0.102	52.39.131.77	TCP	54	1945-443 [ACK] Seq=1 Ack=1 win=16727040 Len=0
25	5.76832900	192.168.0.102	52.39.131.77	SSL	571	Client Hello
26	6.01604300	52.39.131.77	192.168.0.102	TCP	58	443-1946 [SYN, ACK] Seq=0 Ack=1 win=26883 Len=0 MSS=1452
27	6.01626800	192.168.0.102	52.39.131.77	TCP	54	1946-443 [ACK] Seq=1 Ack=1 win=16727040 Len=0
28	6.02140300	192.168.0.102	52.39.131.77	TLSv1.2	571	Client Hello
29	6.07303500	52.39.131.77	192.168.0.102	TCP	54	443-1945 [ACK] Seq=1 Ack=518 win=29480 Len=0
30	6.07561300	52.39.131.77	192.168.0.102	TLSv1.2	1404	Server Hello

Follow TCP Stream: -

Follow TCP Stream (tcp.stream eq 4)

Stream Content

```
X...{.....}X...8...aj...X&...
a...]u$...+.../...0.
...3.9.../S...
...tiles.services.mozilla.com...
...#...h2.http/1.1...3.k.i...1...>...#9s.a...@...q...q...A...I\...Cs...V...M.f...4FU...j<...-#.1.AT...j...Q...[C...gb
\...F...O...+...
@...
+u...f...76...;...4...Y...jE...3)rh...3.u...T.n...=tj...d.../...
...
...c0...0...G...-E...PS.P...0
...M...
...OM1.0...U...US1.0...U...
...Digicert Incl'0%.U...Digicert SHA2 Secure Server CA0..
171003000000Z.
200108120000Z.1.0...U...US1.0...U...
California1.0...U...
Mountain View1.0...U...
..Mozilla Corporation1.0...U...Cloud Services1.0...U...*.services.mozilla.com0.."0
...H...
...0...
...(*.a1...-nb...o...u...>...h...V...ja...5*...7AH...D.../d~f.0q...o...b...\n.st6...XY...M...p.qj...t.X...#...#.C...d...Z.D-M
(d-g...-3...R...2...(.f...h...>N...n...!...x]...P?F...A.q.w.w.k...al...)-X?...6.(W.K...0...0...U...#...0...a...ia.../
(.F&...0...U...e.S...A.p...U...#107...U...00...*.services.mozilla.com...services.mozilla.com0...U...0...U...0...+...0k...U...dob0/-
+.)http://cr13.digicert.com/ssca-sha2-g1.cr10/-,+.)http://cr14.digicert.com/ssca-sha2-g1.cr10L...U...E0C07...H...1.0*0(+...https://www.digicert.com/
CPS0...g...0l...+...d0n05...+...0...http://ocsp.digicert.com0F...+...0...http://cacerts.digicert.com/digicertSHA2SecureServerCA.crt0...U...0.0
...H...
.../ng8y...:u.&N...L...KK5@.4...T.R.h...[.o...H...>[Y.B.Yk...%H.'~(r.K...IA.G...t5.../R.d...R9...;...a...!...D...t...%
NA...%\...%.UEE...D...b...:7.&...3Q.&IpFV\G...6
...Tj...l.I.m...h...#...y...0...0...0...n...u...C.PK...0
...H...
...0a1.0...U...US1.0...U...
...Digicert Incl.0...U...www.digicert.com1.0...U...Digicert Global Root CA0..
130308120000Z.
230308120000ZOM1.0...U...US1.0...U...
...Digicert Incl'0%.U...Digicert SHA2 Secure Server CA0.."0
...H...
...0...
...X.M...0...5[n<...qC.d&...M.F...
sn...6.d.7...A...sm3...S...+UH-V7[.12...][K.GF...y...j...eN...z...~U1.9.../...j...WTS5...D...k)...D.KX.m.K...s...H...Eu...71...T
j...79A...%\...A...Efg...e...N...N...P...0...w...[(W...EX...Z0.V0...U...0...0...0...0...0...04...+...0...0...0...http://ocsp.digicert.com0
```

Entire conversation (3770 bytes)

Find Save As Print ASCII EBCDIC Hex Dump C Arrays Raw

Help Filter Out This Stream Close