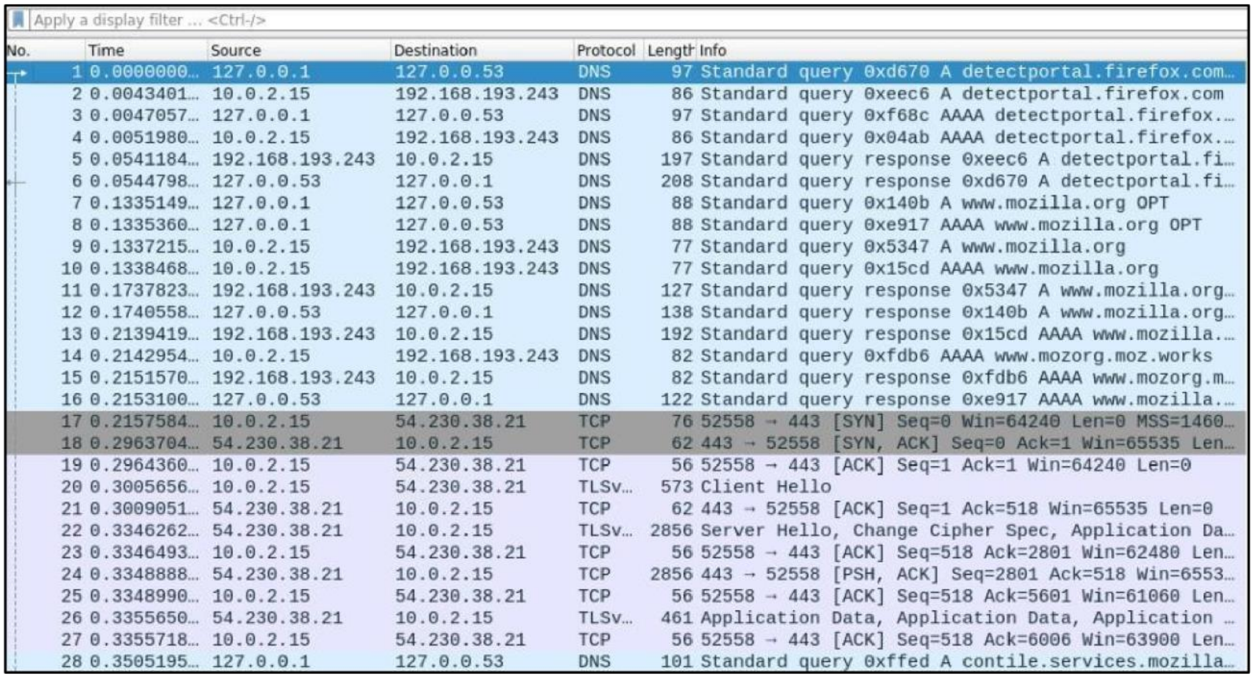
Assignment 6

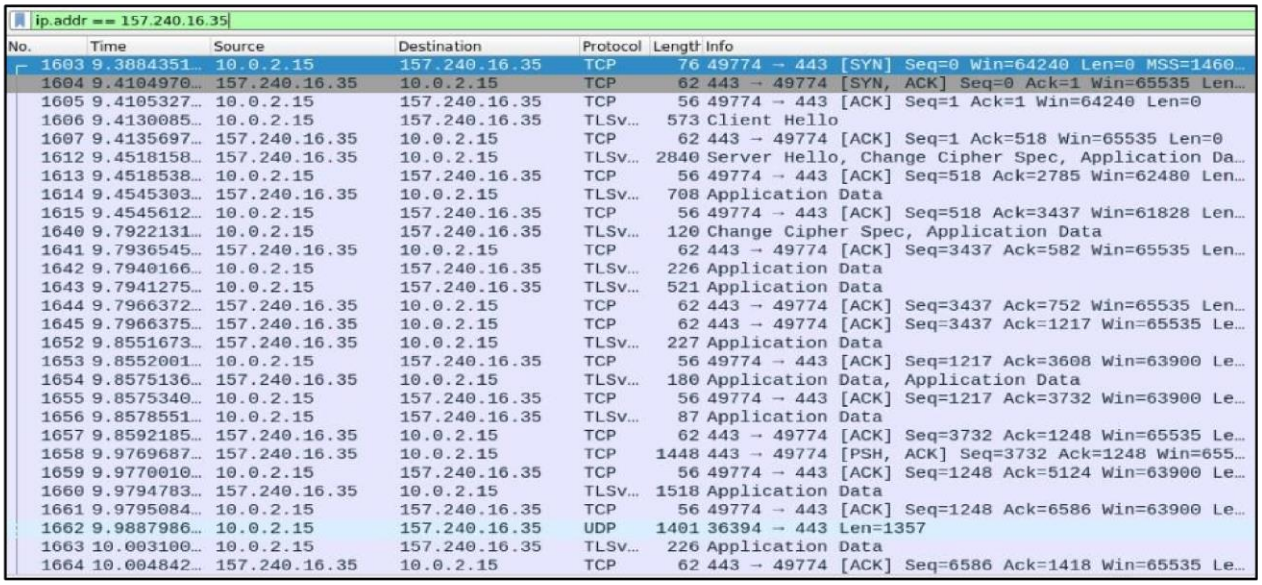
Problem Statement: Configure and demonstrate use of vulnerability assessment tool like Wireshark or SNORT.



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

No.   Time          Source            Destination       Protocol Length Info
    1 0.0000000…   127.0.0.1         127.0.0.53        DNS        97 Standard query 0xd670 A detectportal.firefox.com…
    2 0.0043401…   10.0.2.15         192.168.193.243   DNS        86 Standard query 0xeec6 A detectportal.firefox.com
    3 0.0047057…   127.0.0.1         127.0.0.53        DNS        97 Standard query 0xf68c AAAA detectportal.firefox.…
    4 0.0051980…   10.0.2.15         192.168.193.243   DNS        86 Standard query 0x04ab AAAA detectportal.firefox.…
    5 0.0541184…   192.168.193.243   10.0.2.15         DNS       197 Standard query response 0xeec6 A detectportal.fi…
    6 0.0544798…   127.0.0.53        127.0.0.1         DNS       208 Standard query response 0xd670 A detectportal.fi…
    7 0.1335149…   127.0.0.1         127.0.0.53        DNS        88 Standard query 0x140b A www.mozilla.org OPT
    8 0.1335360…   127.0.0.1         127.0.0.53        DNS        88 Standard query 0xe917 AAAA www.mozilla.org OPT
    9 0.1337215…   10.0.2.15         192.168.193.243   DNS        77 Standard query 0x5347 A www.mozilla.org
   10 0.1338468…   10.0.2.15         192.168.193.243   DNS        77 Standard query 0x15cd AAAA www.mozilla.org
   11 0.1737823…   192.168.193.243   10.0.2.15         DNS       127 Standard query response 0x5347 A www.mozilla.org…
   12 0.1740558…   127.0.0.53        127.0.0.1         DNS       138 Standard query response 0x140b A www.mozilla.org…
   13 0.2139419…   192.168.193.243   10.0.2.15         DNS       192 Standard query response 0x15cd AAAA www.mozilla.…
   14 0.2142954…   10.0.2.15         192.168.193.243   DNS        82 Standard query 0xfdb6 AAAA www.mozorg.moz.works
   15 0.2151570…   192.168.193.243   10.0.2.15         DNS        82 Standard query response 0xfdb6 AAAA www.mozorg.m…
   16 0.2153100…   127.0.0.53        127.0.0.1         DNS       122 Standard query response 0xe917 AAAA www.mozilla.…
   17 0.2157584…   10.0.2.15         54.230.38.21      TCP        76 52558 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460…
   18 0.2963704…   54.230.38.21      10.0.2.15         TCP        62 443 → 52558 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len…
   19 0.2964360…   10.0.2.15         54.230.38.21      TCP        56 52558 → 443 [ACK] Seq=1 Ack=1 Win=64240 Len=0
   20 0.3005656…   10.0.2.15         54.230.38.21      TLSv…     573 Client Hello
   21 0.3009051…   54.230.38.21      10.0.2.15         TCP        62 443 → 52558 [ACK] Seq=1 Ack=518 Win=65535 Len=0
   22 0.3346262…   54.230.38.21      10.0.2.15         TLSv…    2856 Server Hello, Change Cipher Spec, Application Da…
   23 0.3346493…   10.0.2.15         54.230.38.21      TCP        56 52558 → 443 [ACK] Seq=518 Ack=2801 Win=62480 Len…
   24 0.3348888…   54.230.38.21      10.0.2.15         TCP      2856 443 → 52558 [PSH, ACK] Seq=2801 Ack=518 Win=6553…
   25 0.3348990…   10.0.2.15         54.230.38.21      TCP        56 52558 → 443 [ACK] Seq=518 Ack=5601 Win=61060 Len…
   26 0.3355650…   54.230.38.21      10.0.2.15         TLSv…     461 Application Data, Application Data, Application …
   27 0.3355718…   10.0.2.15         54.230.38.21      TCP        56 52558 → 443 [ACK] Seq=518 Ack=6006 Win=63900 Len…
   28 0.3505195…   127.0.0.1         127.0.0.53        DNS       101 Standard query 0xffed A contile.services.mozilla…
```

All Packets that were captured

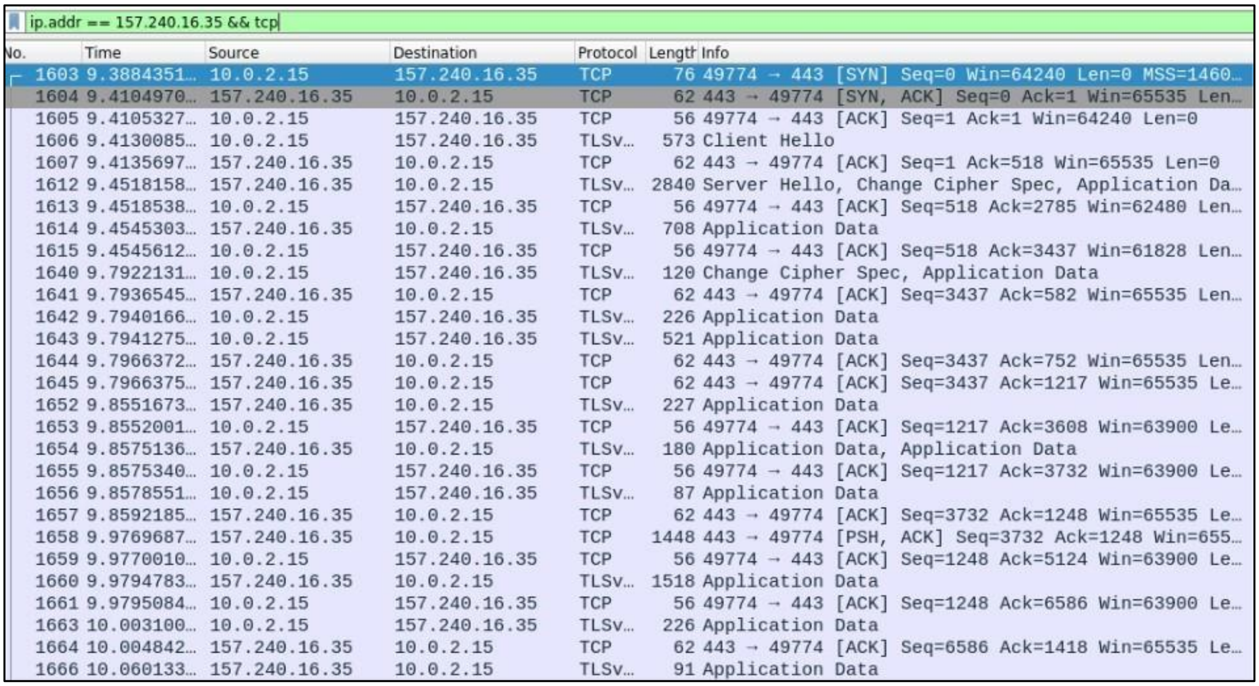


```
ip.addr == 157.240.16.35

No.   Time          Source            Destination       Protocol Length Info
 1603 9.3884351…   10.0.2.15         157.240.16.35     TCP        76 49774 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460…
 1604 9.4104970…   157.240.16.35     10.0.2.15         TCP        62 443 → 49774 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len…
 1605 9.4105327…   10.0.2.15         157.240.16.35     TCP        56 49774 → 443 [ACK] Seq=1 Ack=1 Win=64240 Len=0
 1606 9.4130085…   10.0.2.15         157.240.16.35     TLSv…     573 Client Hello
 1607 9.4135697…   157.240.16.35     10.0.2.15         TCP        62 443 → 49774 [ACK] Seq=1 Ack=518 Win=65535 Len=0
 1612 9.4518158…   157.240.16.35     10.0.2.15         TLSv…    2840 Server Hello, Change Cipher Spec, Application Da…
 1613 9.4518538…   10.0.2.15         157.240.16.35     TCP        56 49774 → 443 [ACK] Seq=518 Ack=2785 Win=62480 Len…
 1614 9.4545303…   157.240.16.35     10.0.2.15         TLSv…     708 Application Data
 1615 9.4545612…   10.0.2.15         157.240.16.35     TCP        56 49774 → 443 [ACK] Seq=518 Ack=3437 Win=61828 Len…
 1640 9.7922131…   10.0.2.15         157.240.16.35     TLSv…     120 Change Cipher Spec, Application Data
 1641 9.7936545…   157.240.16.35     10.0.2.15         TCP        62 443 → 49774 [ACK] Seq=3437 Ack=582 Win=65535 Len…
 1642 9.7940166…   10.0.2.15         157.240.16.35     TLSv…     226 Application Data
 1643 9.7941275…   10.0.2.15         157.240.16.35     TLSv…     521 Application Data
 1644 9.7966372…   157.240.16.35     10.0.2.15         TCP        62 443 → 49774 [ACK] Seq=3437 Ack=752 Win=65535 Len…
 1645 9.7966375…   157.240.16.35     10.0.2.15         TCP        62 443 → 49774 [ACK] Seq=3437 Ack=1217 Win=65535 Le…
 1652 9.8551673…   157.240.16.35     10.0.2.15         TLSv…     227 Application Data
 1653 9.8552001…   10.0.2.15         157.240.16.35     TCP        56 49774 → 443 [ACK] Seq=1217 Ack=3608 Win=63900 Le…
 1654 9.8575136…   157.240.16.35     10.0.2.15         TLSv…     180 Application Data, Application Data
 1655 9.8575340…   10.0.2.15         157.240.16.35     TCP        56 49774 → 443 [ACK] Seq=1217 Ack=3732 Win=63900 Le…
 1656 9.8578551…   10.0.2.15         157.240.16.35     TLSv…      87 Application Data
 1657 9.8592185…   157.240.16.35     10.0.2.15         TCP        62 443 → 49774 [ACK] Seq=3732 Ack=1248 Win=65535 Le…
 1658 9.9769687…   157.240.16.35     10.0.2.15         TCP      1448 443 → 49774 [PSH, ACK] Seq=3732 Ack=1248 Win=655…
 1659 9.9770010…   10.0.2.15         157.240.16.35     TCP        56 49774 → 443 [ACK] Seq=1248 Ack=5124 Win=63900 Le…
 1660 9.9794783…   157.240.16.35     10.0.2.15         TLSv…    1518 Application Data
 1661 9.9795084…   10.0.2.15         157.240.16.35     TCP        56 49774 → 443 [ACK] Seq=1248 Ack=6586 Win=63900 Le…
 1662 9.9887986…   10.0.2.15         157.240.16.35     UDP      1401 36394 → 443 Len=1357
 1663 10.003100…   10.0.2.15         157.240.16.35     TLSv…     226 Application Data
 1664 10.004842…   157.240.16.35     10.0.2.15         TCP        62 443 → 49774 [ACK] Seq=6586 Ack=1418 Win=65535 Le…
```

Packets from Facebook (IP = 157.240.16.35)

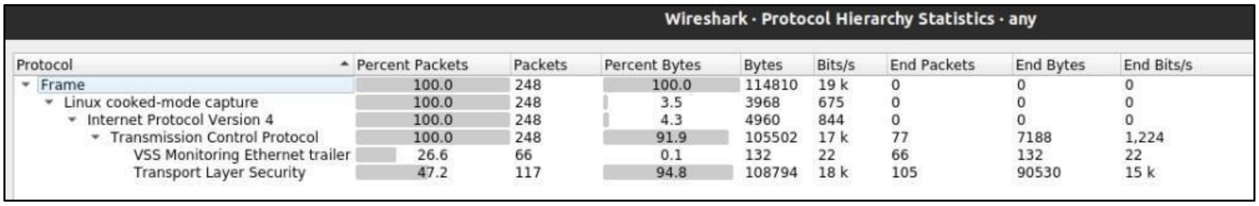
Assignment 6



ip.addr == 157.240.16.35 && tcp

No.	Time	Source	Destination	Protocol	Length	Info
1603	9.3884351…	10.0.2.15	157.240.16.35	TCP	76	49774 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460…
1604	9.4104970…	157.240.16.35	10.0.2.15	TCP	62	443 → 49774 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len…
1605	9.4105327…	10.0.2.15	157.240.16.35	TCP	56	49774 → 443 [ACK] Seq=1 Ack=1 Win=64240 Len=0
1606	9.4130085…	10.0.2.15	157.240.16.35	TLSv…	573	Client Hello
1607	9.4135697…	157.240.16.35	10.0.2.15	TCP	62	443 → 49774 [ACK] Seq=1 Ack=518 Win=65535 Len=0
1612	9.4518158…	157.240.16.35	10.0.2.15	TLSv…	2840	Server Hello, Change Cipher Spec, Application Da…
1613	9.4518538…	10.0.2.15	157.240.16.35	TCP	56	49774 → 443 [ACK] Seq=518 Ack=2785 Win=62480 Len…
1614	9.4545303…	157.240.16.35	10.0.2.15	TLSv…	708	Application Data
1615	9.4545612…	10.0.2.15	157.240.16.35	TCP	56	49774 → 443 [ACK] Seq=518 Ack=3437 Win=61828 Len…
1640	9.7922131…	10.0.2.15	157.240.16.35	TLSv…	120	Change Cipher Spec, Application Data
1641	9.7936545…	157.240.16.35	10.0.2.15	TCP	62	443 → 49774 [ACK] Seq=3437 Ack=582 Win=65535 Len…
1642	9.7940166…	10.0.2.15	157.240.16.35	TLSv…	226	Application Data
1643	9.7941275…	10.0.2.15	157.240.16.35	TLSv…	521	Application Data
1644	9.7966372…	157.240.16.35	10.0.2.15	TCP	62	443 → 49774 [ACK] Seq=3437 Ack=752 Win=65535 Len…
1645	9.7966375…	157.240.16.35	10.0.2.15	TCP	62	443 → 49774 [ACK] Seq=3437 Ack=1217 Win=65535 Le…
1652	9.8551673…	157.240.16.35	10.0.2.15	TLSv…	227	Application Data
1653	9.8552001…	10.0.2.15	157.240.16.35	TCP	56	49774 → 443 [ACK] Seq=1217 Ack=3608 Win=63900 Le…
1654	9.8575136…	157.240.16.35	10.0.2.15	TLSv…	180	Application Data, Application Data
1655	9.8575340…	10.0.2.15	157.240.16.35	TCP	56	49774 → 443 [ACK] Seq=1217 Ack=3732 Win=63900 Le…
1656	9.8578551…	10.0.2.15	157.240.16.35	TLSv…	87	Application Data
1657	9.8592185…	157.240.16.35	10.0.2.15	TCP	62	443 → 49774 [ACK] Seq=3732 Ack=1248 Win=65535 Le…
1658	9.9769687…	157.240.16.35	10.0.2.15	TCP	1448	443 → 49774 [PSH, ACK] Seq=3732 Ack=1248 Win=655…
1659	9.9770010…	10.0.2.15	157.240.16.35	TCP	56	49774 → 443 [ACK] Seq=1248 Ack=5124 Win=63900 Le…
1660	9.9794783…	157.240.16.35	10.0.2.15	TLSv…	1518	Application Data
1661	9.9795084…	10.0.2.15	157.240.16.35	TCP	56	49774 → 443 [ACK] Seq=1248 Ack=6586 Win=63900 Le…
1663	10.003100…	10.0.2.15	157.240.16.35	TLSv…	226	Application Data
1664	10.004842…	157.240.16.35	10.0.2.15	TCP	62	443 → 49774 [ACK] Seq=6586 Ack=1418 Win=65535 Le…
1666	10.060133…	157.240.16.35	10.0.2.15	TLSv…	91	Application Data

All TCP packets that were captured



Wireshark · Protocol Hierarchy Statistics · any

Protocol	Percent Packets	Packets	Percent Bytes	Bytes	Bits/s	End Packets	End Bytes	End Bits/s
Frame	100.0	248	100.0	114810	19 k	0	0	0
Linux cooked-mode capture	100.0	248	3.5	3968	675	0	0	0
Internet Protocol Version 4	100.0	248	4.3	4960	844	0	0	0
Transmission Control Protocol	100.0	248	91.9	105502	17 k	77	7188	1,224
VSS Monitoring Ethernet trailer	26.6	66	0.1	132	22	66	132	22
Transport Layer Security	47.2	117	94.8	108794	18 k	105	90530	15 k

Number of TCP Packets received from/sent to Facebook