ANALYZE YOUR FIRST PACKET WITH WIRESHARK

Pedro Osorio Lopez.

1. High-Level Project Description:

*In this lab activity, we'll learn how to open and analyze a packet capture file using Wireshark.

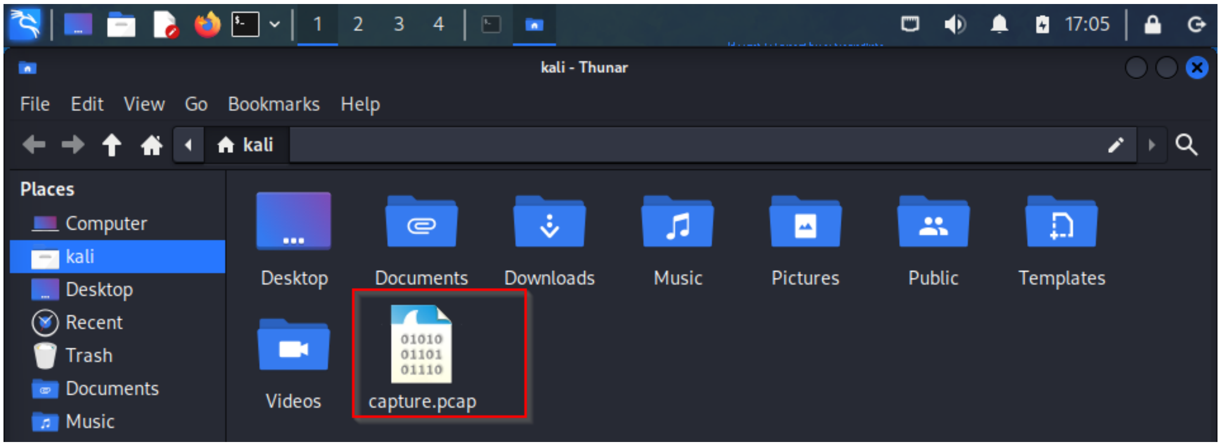
2. Project Setup and Required Tools:

*Either a Linux, Mac, or Windows Machine can be used to perform this task. The tool Wireshark was already provided to us; however, it can be downloaded from https://www.wireshark.org/download.html if necessary.

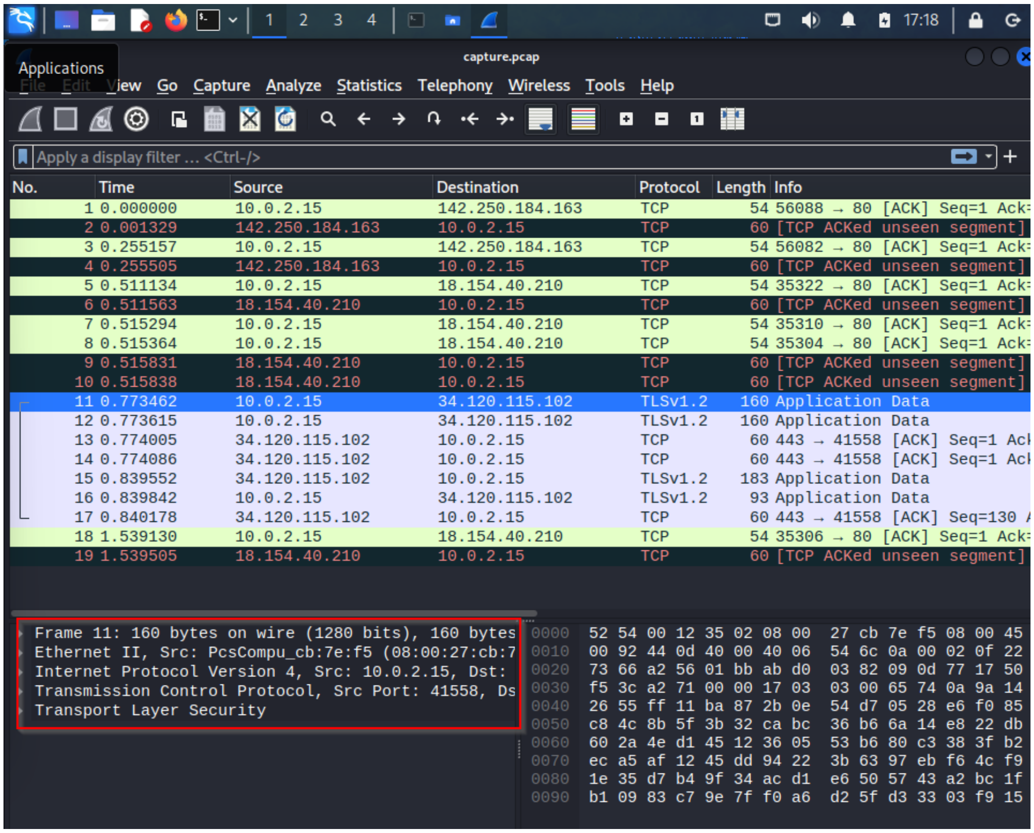
3. Step by Step Project Walkthrough

*We have a few tasks in this lab: Open a packet capture file using Wireshark, examine packet information, and apply display filters

*We will start by opening the packet capture we previously saved using tcpdump (note that Wireshark can also be used to capture packets). We simply clicked on the saved capture to start.



*Once opened the file, we can see that several rows of information are displayed, each corresponding to a packet. Click on one packet and you will be able to see the information it contains, including the MAC addresses (Data Link layer/OSI layer 2), IP addresses (Internet layer/OSI layer 3), TCP (Transport layer/OSI layer 4), etc.

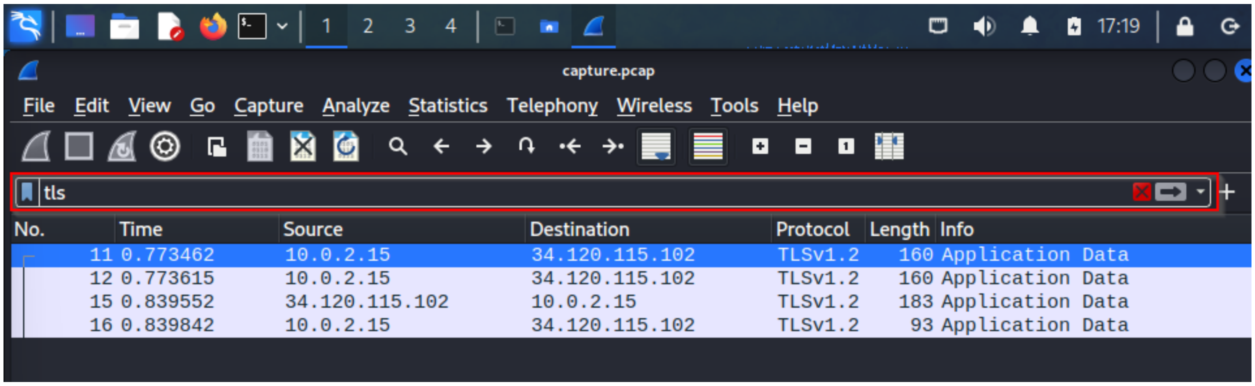

Applications
capture.pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter … <Ctrl-/>
17:18

```
No.    Time       Source            Destination       Protocol  Length Info
     1 0.000000   10.0.2.15         142.250.184.163   TCP          54 56088 → 80 [ACK] Seq=1 Ack=
     2 0.001329   142.250.184.163   10.0.2.15         TCP          60 [TCP ACKed unseen segment]
     3 0.255157   10.0.2.15         142.250.184.163   TCP          54 56082 → 80 [ACK] Seq=1 Ack=
     4 0.255505   142.250.184.163   10.0.2.15         TCP          60 [TCP ACKed unseen segment]
     5 0.511134   10.0.2.15         18.154.40.210     TCP          54 35322 → 80 [ACK] Seq=1 Ack=
     6 0.511563   18.154.40.210     10.0.2.15         TCP          60 [TCP ACKed unseen segment]
     7 0.515294   10.0.2.15         18.154.40.210     TCP          54 35310 → 80 [ACK] Seq=1 Ack=
     8 0.515364   10.0.2.15         18.154.40.210     TCP          54 35304 → 80 [ACK] Seq=1 Ack=
     9 0.515831   18.154.40.210     10.0.2.15         TCP          60 [TCP ACKed unseen segment]
    10 0.515838   18.154.40.210     10.0.2.15         TCP          60 [TCP ACKed unseen segment]
    11 0.773462   10.0.2.15         34.120.115.102    TLSv1.2     160 Application Data
    12 0.773615   10.0.2.15         34.120.115.102    TLSv1.2     160 Application Data
    13 0.774005   34.120.115.102    10.0.2.15         TCP          60 443 → 41558 [ACK] Seq=1 Ack
    14 0.774086   34.120.115.102    10.0.2.15         TCP          60 443 → 41558 [ACK] Seq=1 Ack
    15 0.839552   34.120.115.102    10.0.2.15         TLSv1.2     183 Application Data
    16 0.839842   10.0.2.15         34.120.115.102    TLSv1.2      93 Application Data
    17 0.840178   34.120.115.102    10.0.2.15         TCP          60 443 → 41558 [ACK] Seq=130 A
    18 1.539130   10.0.2.15         18.154.40.210     TCP          54 35306 → 80 [ACK] Seq=1 Ack=
    19 1.539505   18.154.40.210     10.0.2.15         TCP          60 [TCP ACKed unseen segment]
```

```
Frame 11: 160 bytes on wire (1280 bits), 160 bytes
Ethernet II, Src: PcsCompu_cb:7e:f5 (08:00:27:cb:7
Internet Protocol Version 4, Src: 10.0.2.15, Dst:
Transmission Control Protocol, Src Port: 41558, Ds
Transport Layer Security
```

```
0000  52 54 00 12 35 02 08 00  27 cb 7e f5 08 00 45
0010  00 92 44 0d 40 00 40 06  54 6c 0a 00 02 0f 22
0020  73 66 a2 56 01 bb ab d0  03 82 09 0d 77 17 50
0030  f5 3c a2 71 00 00 17 03  03 00 65 74 0a 9a 14
0040  26 55 ff 11 ba 87 2b 0e  54 d7 05 28 e6 f0 85
0050  c8 4c 8b 5f 3b 32 ca bc  36 b6 6a 14 e8 22 db
0060  60 2a 4e d1 45 12 36 05  53 b6 80 c3 38 3f b2
0070  ec a5 af 12 45 dd 94 22  3b 63 97 eb f6 4c f9
0080  1e 35 d7 b4 9f 34 ac d1  e6 50 57 43 a2 bc 1f
0090  b1 09 83 c7 9e 7f f0 a6  d2 5f d3 33 03 f9 15
```

*Lastly, in order to apply a display filter, simple look for the search tab and apply any filters you would need (such as a specific MAC or IP, packets using a given protocol, etc).


capture.pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
17:19

```
tls
```

```
No.    Time       Source            Destination       Protocol  Length Info
    11 0.773462   10.0.2.15         34.120.115.102    TLSv1.2     160 Application Data
    12 0.773615   10.0.2.15         34.120.115.102    TLSv1.2     160 Application Data
    15 0.839552   34.120.115.102    10.0.2.15         TLSv1.2     183 Application Data
    16 0.839842   10.0.2.15         34.120.115.102    TLSv1.2      93 Application Data
```

4. Summary and/or Recommendations:

*In this activity, we learned how to use Wireshark, arguably the most utilized tool for analyzing packet captures, by opening a packet capture, examining the contents of packets, and applying filters.