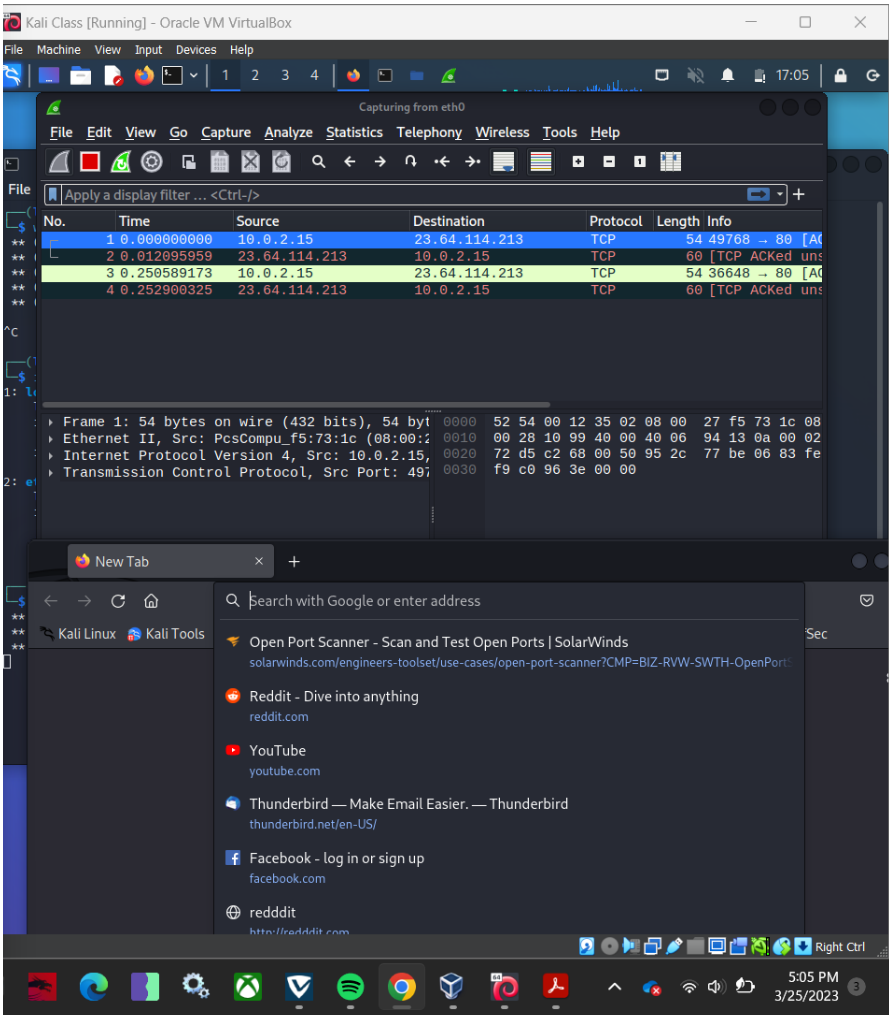
ITT-307 -Wireshark

Professor:	Ingrid Gaviria
Course:	ITT-307 Cybersecurity Foundations
Student:	Liela Pressley
Date:	3/25/2023
Title:	**Wireshark**

Overview:Wireshark allows users to see all the network activities happening on their device and on wireless networks their device could be connected to. In this analysis I used wireshark to view the activities on my VM Kali Linux, I then connected to the Firefox browser and went to the GCU website where I was able to see the packets and UDP/TCP protocols in order to retrieve the website information to my computer. This basic steps will show some of the data you can access and how they can present information about unwanted hosts or devices within a network.

1. Once I opened Wireshark I couldn't see any traffic, so I decided to open my browser to create some network movement.


Kali Class [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
17:05
Capturing from eth0
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter … <Ctrl-/>
New Tab
Search with Google or enter address
Kali Linux
Kali Tools
Right Ctrl
5:05 PM
3/25/2023

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	10.0.2.15	23.64.114.213	TCP	54	49768 → 80 [AC
2	0.012095959	23.64.114.213	10.0.2.15	TCP	60	[TCP ACKed uns
3	0.250589173	10.0.2.15	23.64.114.213	TCP	54	36648 → 80 [AC
4	0.252900325	23.64.114.213	10.0.2.15	TCP	60	[TCP ACKed uns

```
› Frame 1: 54 bytes on wire (432 bits), 54 byt   0000  52 54 00 12 35 02 08 00  27 f5 73 1c 08
› Ethernet II, Src: PcsCompu_f5:73:1c (08:00:2   0010  00 28 10 99 40 00 40 06  94 13 0a 00 02
› Internet Protocol Version 4, Src: 10.0.2.15,   0020  72 d5 c2 68 00 50 95 2c  77 be 06 83 fe
› Transmission Control Protocol, Src Port: 497   0030  f9 c0 96 3e 00 00
```

Open Port Scanner - Scan and Test Open Ports | SolarWinds
solarwinds.com/engineers-toolset/use-cases/open-port-scanner?CMP=BIZ-RVW-SWTH-OpenPort

Reddit - Dive into anything
reddit.com

YouTube
youtube.com

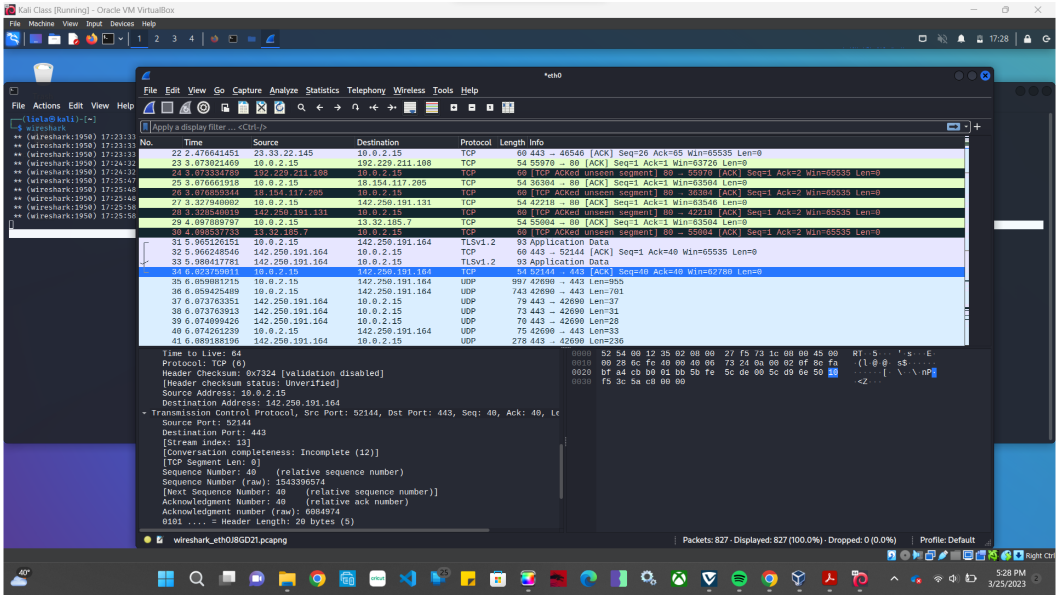
Thunderbird — Make Email Easier. — Thunderbird
thunderbird.net/en-US/

Facebook - log in or sign up
facebook.com

redddit
http://redddit.com

2. Through Wireshark you are able to see alot of key elements going on within your network traffic. This screenshot shows my ability to see the communication between my device and the servers for the Kali Linux Search Engine and then the GCU website. The GCU website communicated using TCP, transmission control protocol. Through this platform you are able to see the IP addresses of my device as well as the destination address from the web server that is providing the website to me. Here you can see where I clicked the link to the gcu website and started a new communication. You can see the source port number, the destination port number used, and the protocol switching to UDP

for faster response time from the webserver to my device.



Kali Class [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
*eth0
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter … <Ctrl-/>
17:28
Right Ctrl
40°
5:28 PM
3/25/2023

```
File  Actions  Edit  View  Help
┌──(liela㉿kali)-[~]
└─$ wireshark
** (wireshark:1950) 17:23:33
** (wireshark:1950) 17:23:33
** (wireshark:1950) 17:23:33
** (wireshark:1950) 17:24:32
** (wireshark:1950) 17:24:32
** (wireshark:1950) 17:25:47
** (wireshark:1950) 17:25:48
** (wireshark:1950) 17:25:48
** (wireshark:1950) 17:25:58
** (wireshark:1950) 17:25:58
```

```
No.   Time          Source            Destination       Protocol  Length Info
   22 2.476641451   23.33.22.145      10.0.2.15         TCP        60 443 → 46546 [ACK] Seq=26 Ack=65 Win=65535 Len=0
   23 3.073021469   10.0.2.15         192.229.211.108   TCP        54 55970 → 80 [ACK] Seq=1 Ack=1 Win=63726 Len=0
   24 3.073334789   192.229.211.108   10.0.2.15         TCP        60 [TCP ACKed unseen segment] 80 → 55970 [ACK] Seq=1 Ack=2 Win=65535 Len=0
   25 3.076661918   10.0.2.15         18.154.117.205    TCP        54 36304 → 80 [ACK] Seq=1 Ack=1 Win=63504 Len=0
   26 3.076859344   18.154.117.205    10.0.2.15         TCP        60 [TCP ACKed unseen segment] 80 → 36304 [ACK] Seq=1 Ack=2 Win=65535 Len=0
   27 3.327940002   10.0.2.15         142.250.191.131   TCP        54 42218 → 80 [ACK] Seq=1 Ack=1 Win=63546 Len=0
   28 3.328540019   142.250.191.131   10.0.2.15         TCP        60 [TCP ACKed unseen segment] 80 → 42218 [ACK] Seq=1 Ack=2 Win=65535 Len=0
   29 4.097889797   10.0.2.15         13.32.185.7       TCP        54 55004 → 80 [ACK] Seq=1 Ack=1 Win=63504 Len=0
   30 4.098537733   13.32.185.7       10.0.2.15         TCP        60 [TCP ACKed unseen segment] 80 → 55004 [ACK] Seq=1 Ack=2 Win=65535 Len=0
   31 5.965126151   10.0.2.15         142.250.191.164   TLSv1.2    93 Application Data
   32 5.966248546   142.250.191.164   10.0.2.15         TCP        60 443 → 52144 [ACK] Seq=1 Ack=40 Win=65535 Len=0
   33 5.980417781   142.250.191.164   10.0.2.15         TLSv1.2    93 Application Data
   34 6.023759011   10.0.2.15         142.250.191.164   TCP        54 52144 → 443 [ACK] Seq=40 Ack=40 Win=62780 Len=0
   35 6.059081215   10.0.2.15         142.250.191.164   UDP       997 42690 → 443 Len=955
   36 6.059425489   10.0.2.15         142.250.191.164   UDP       743 42690 → 443 Len=701
   37 6.073763351   142.250.191.164   10.0.2.15         UDP        79 443 → 42690 Len=37
   38 6.073763913   142.250.191.164   10.0.2.15         UDP        73 443 → 42690 Len=31
   39 6.074099426   142.250.191.164   10.0.2.15         UDP        70 443 → 42690 Len=28
   40 6.074261239   10.0.2.15         142.250.191.164   UDP        75 42690 → 443 Len=33
   41 6.089188196   142.250.191.164   10.0.2.15         UDP       278 443 → 42690 Len=236
```

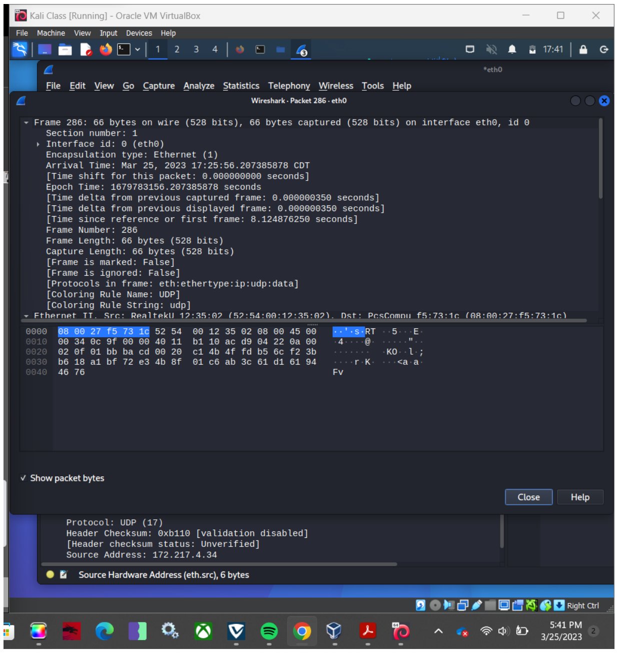
```
    Time to Live: 64
    Protocol: TCP (6)
    Header Checksum: 0x7324 [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 10.0.2.15
    Destination Address: 142.250.191.164
  Transmission Control Protocol, Src Port: 52144, Dst Port: 443, Seq: 40, Ack: 40, Le
    Source Port: 52144
    Destination Port: 443
    [Stream index: 13]
    [Conversation completeness: Incomplete (12)]
    [TCP Segment Len: 0]
    Sequence Number: 40    (relative sequence number)
    Sequence Number (raw): 1543396574
    [Next Sequence Number: 40    (relative sequence number)]
    Acknowledgment Number: 40    (relative ack number)
    Acknowledgment number (raw): 6084974
    0101 .... = Header Length: 20 bytes (5)
```

```
0000  52 54 00 12 35 02 08 00  27 f5 73 1c 08 00 45 00   RT··5···'·s···E·
0010  00 28 6c fe 40 00 40 06  73 24 0a 00 02 0f 8e fa   ·(l·@·@·s$······
0020  bf a4 cb b0 01 bb 5b fe  5c de 00 5c d9 6e 50 10   ······[·\··\·nP·
0030  f5 3c 5a c8 00 00                                  ·<Z···
```

```
wireshark_eth0J8GD21.pcapng    Packets: 827 · Displayed: 827 (100.0%) · Dropped: 0 (0.0%)    Profile: Default
```

3. Wireshark allows you to see when and what communication is happening between your device and outside servers. It shows me when my device is requesting information and receiving it and when the outside devices are requesting/recieving information
4. Once you are familiar with your device and are aware of normal functions and communications that can occur within your network, this is a great tool for monitoring your network and ensuring that there is no suspicious activity occurring within your network or trying to access your device. You can check for potential ARP spoofing by seeing if there are a suspicious amount of requests happening within a given time and you can even inspect the payloads that may cause suspicion what types of files or websites your host or other people on your network are requesting/accessing/sending. Within these

payloads you or an attacker can easily see data that has been inputted by using the filter and viewing the payload data.



Wireshark · Packet 286 · eth0

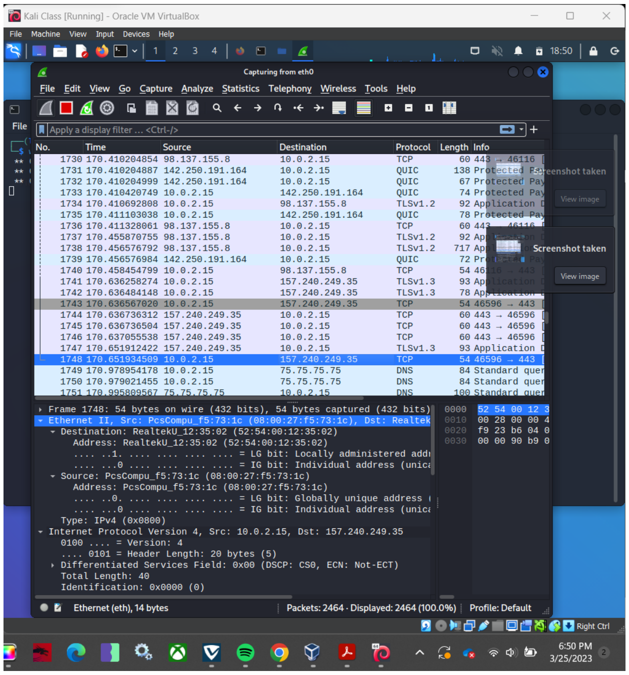
```
▾ Frame 286: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface eth0, id 0
    Section number: 1
  ▸ Interface id: 0 (eth0)
    Encapsulation type: Ethernet (1)
    Arrival Time: Mar 25, 2023 17:25:56.207385878 CDT
    [Time shift for this packet: 0.000000000 seconds]
    Epoch Time: 1679783156.207385878 seconds
    [Time delta from previous captured frame: 0.000000350 seconds]
    [Time delta from previous displayed frame: 0.000000350 seconds]
    [Time since reference or first frame: 8.124876250 seconds]
    Frame Number: 286
    Frame Length: 66 bytes (528 bits)
    Capture Length: 66 bytes (528 bits)
    [Frame is marked: False]
    [Frame is ignored: False]
    [Protocols in frame: eth:ethertype:ip:udp:data]
    [Coloring Rule Name: UDP]
    [Coloring Rule String: udp]
▾ Ethernet II, Src: RealtekU_12:35:02 (52:54:00:12:35:02), Dst: PcsCompu_f5:73:1c (08:00:27:f5:73:1c)

0000  08 00 27 f5 73 1c 52 54  00 12 35 02 08 00 45 00   ··'·s·RT ··5···E·
0010  00 34 0c 9f 00 00 40 11  b1 10 ac d9 04 22 0a 00   ·4····@· ·····"··
0020  02 0f 01 bb ba cd 00 20  c1 4b 4f fd b5 6c f2 3b   ·······  ·KO··l·;
0030  b6 18 a1 bf 72 e3 4b 8f  01 c6 ab 3c 61 d1 61 94   ····r·K· ···<a·a·
0040  46 76                                              Fv
```

```
    Protocol: UDP (17)
    Header Checksum: 0xb110 [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 172.217.4.34
```

Source Hardware Address (eth.src), 6 bytes

Kali Class [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
17:41
*eth0
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
✓ Show packet bytes
Close
Help
Right Ctrl
5:41 PM
3/25/2023

5. How can you track an attacker within your network? Wireshark allows you to see the IP addresses, MAC address, device information, and port numbers of the servers/devices that it is communicating with in order to receive or request connctions and payload information.
6. Here we can see a little more information abou the devices involved in the communication, this along with the data provided in section 5 are all great elements that we can use to identify an attacker's host or an unknown host within the network.



Capturing from eth0

```
No.  Time           Source          Destination     Protocol Length Info
1730 170.410204854  98.137.155.8    10.0.2.15       TCP      60 443 → 46116 [
1731 170.410204887  142.250.191.164 10.0.2.15       QUIC     138 Protected Pay
1732 170.410204999  142.250.191.164 10.0.2.15       QUIC     67 Protected Pay
1733 170.410420749  10.0.2.15       142.250.191.164 QUIC     74 Protected Pay
1734 170.410692808  10.0.2.15       98.137.155.8    TLSv1.2  92 Application D
1735 170.411103038  10.0.2.15       142.250.191.164 QUIC     78 Protected Pay
1736 170.411328061  98.137.155.8    10.0.2.15       TCP      60 443 → 46116 [
1737 170.455870755  98.137.155.8    10.0.2.15       TLSv1.2  92 Application D
1738 170.456576792  98.137.155.8    10.0.2.15       TLSv1.2  717 Application
1739 170.456576984  142.250.191.164 10.0.2.15       QUIC     72 Protected Pay
1740 170.458454799  10.0.2.15       98.137.155.8    TCP      54 46116 → 443 [
1741 170.636258274  10.0.2.15       157.240.249.35  TLSv1.3  93 Application D
1742 170.636484148  10.0.2.15       157.240.249.35  TLSv1.3  78 Application D
1743 170.636567020  10.0.2.15       157.240.249.35  TCP      54 46596 → 443 [
1744 170.636736312  157.240.249.35  10.0.2.15       TCP      60 443 → 46596 [
1745 170.636736504  157.240.249.35  10.0.2.15       TCP      60 443 → 46596 [
1746 170.637055538  157.240.249.35  10.0.2.15       TCP      60 443 → 46596 [
1747 170.651912422  157.240.249.35  10.0.2.15       TLSv1.3  93 Application D
1748 170.651934509  10.0.2.15       157.240.249.35  TCP      54 46596 → 443 [
1749 170.978954178  10.0.2.15       75.75.75.75     DNS      84 Standard quer
1750 170.979021455  10.0.2.15       75.75.75.75     DNS      84 Standard quer
1751 170.995809567  75.75.75.75     10.0.2.15       DNS      100 Standard quer
```

```
▸ Frame 1748: 54 bytes on wire (432 bits), 54 bytes captured (432 bits)
▾ Ethernet II, Src: PcsCompu_f5:73:1c (08:00:27:f5:73:1c), Dst: Realtek
  ▾ Destination: RealtekU_12:35:02 (52:54:00:12:35:02)
      Address: RealtekU_12:35:02 (52:54:00:12:35:02)
      .... ..1. .... .... .... .... = LG bit: Locally administered addr
      .... ...0 .... .... .... .... = IG bit: Individual address (unica
  ▾ Source: PcsCompu_f5:73:1c (08:00:27:f5:73:1c)
      Address: PcsCompu_f5:73:1c (08:00:27:f5:73:1c)
      .... ..0. .... .... .... .... = LG bit: Globally unique address (
      .... ...0 .... .... .... .... = IG bit: Individual address (unica
    Type: IPv4 (0x0800)
▾ Internet Protocol Version 4, Src: 10.0.2.15, Dst: 157.240.249.35
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  ▸ Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 40
    Identification: 0x0000 (0)

0000  52 54 00 12 3
0010  00 28 00 00 4
0020  f9 23 b6 04 0
0030  00 00 90 b9 0
```

Ethernet (eth), 14 bytes | Packets: 2464 · Displayed: 2464 (100.0%) | Profile: Default

Kali Class [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
18:50
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter … <Ctrl-/>
Screenshot taken
View image
Screenshot taken
View image
Right Ctrl
6:50 PM
3/25/2023