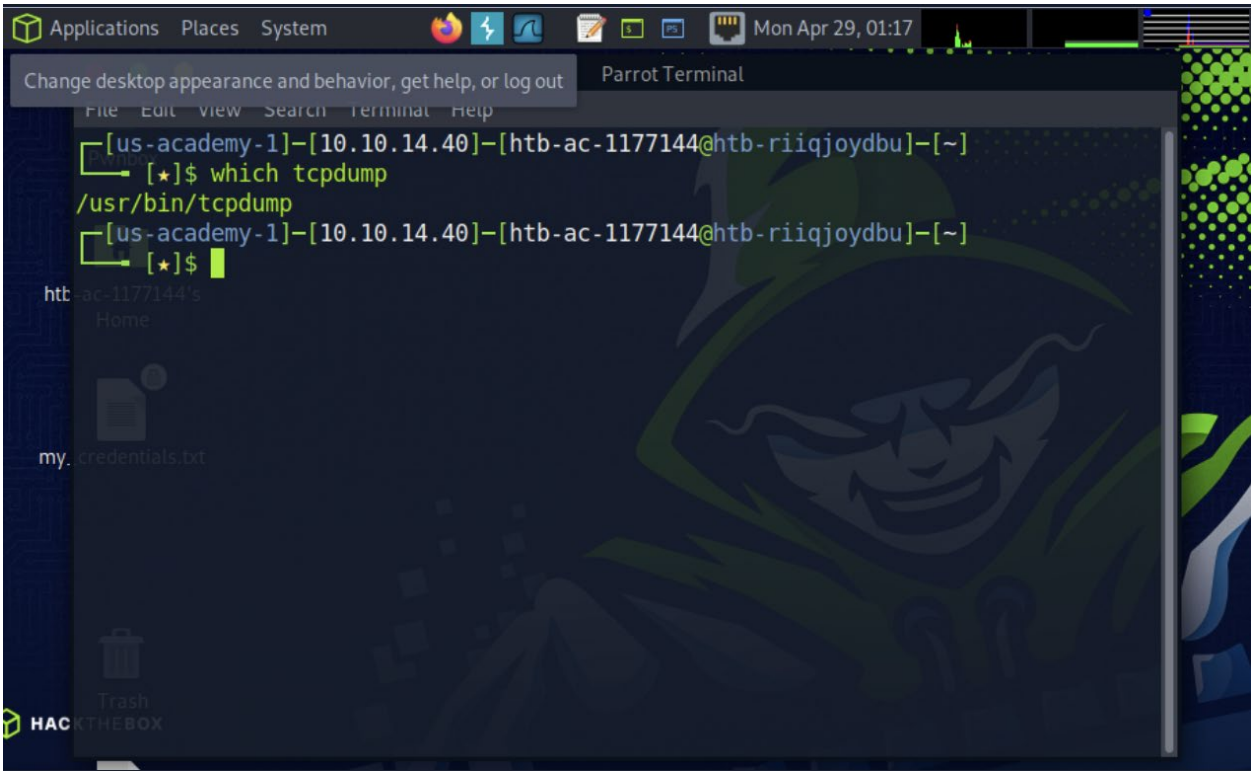
Intro to Network Traffic Analysis HackTheBox

Capturing with TCMPDUMP -Fundamentals LAB

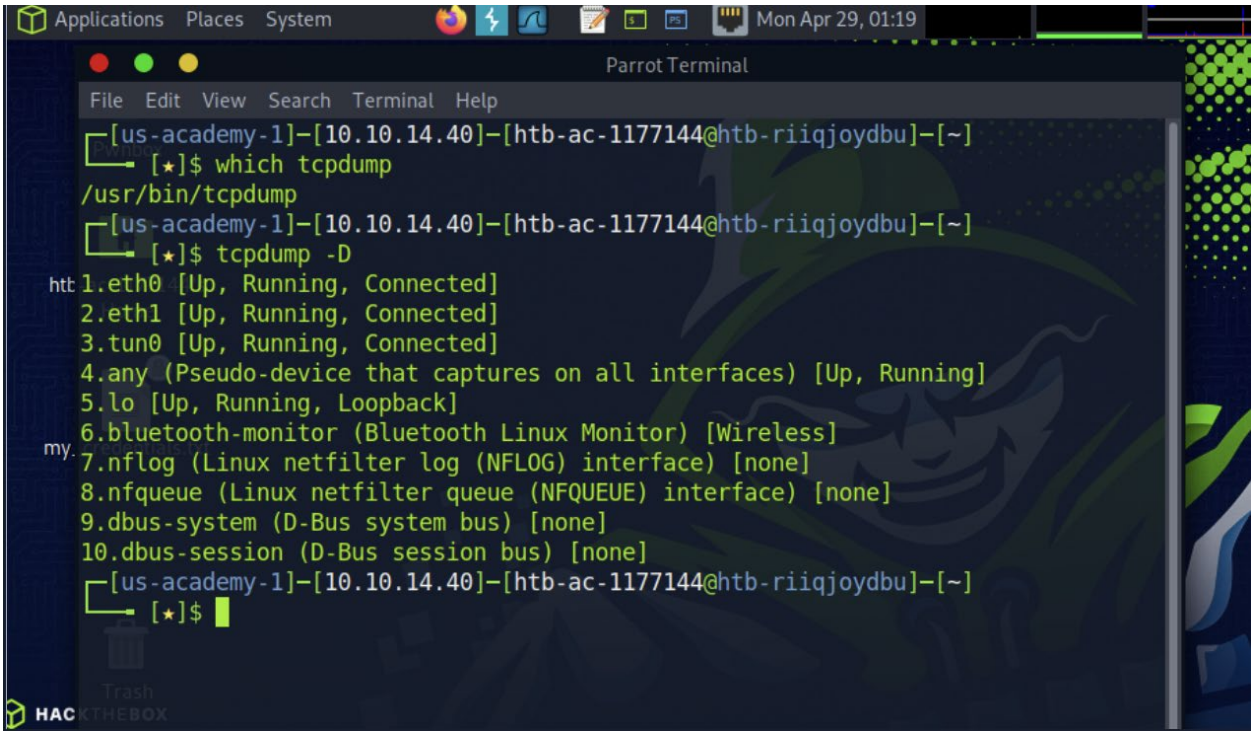
Task #1

Validate Tcpdump is installed on our machine.

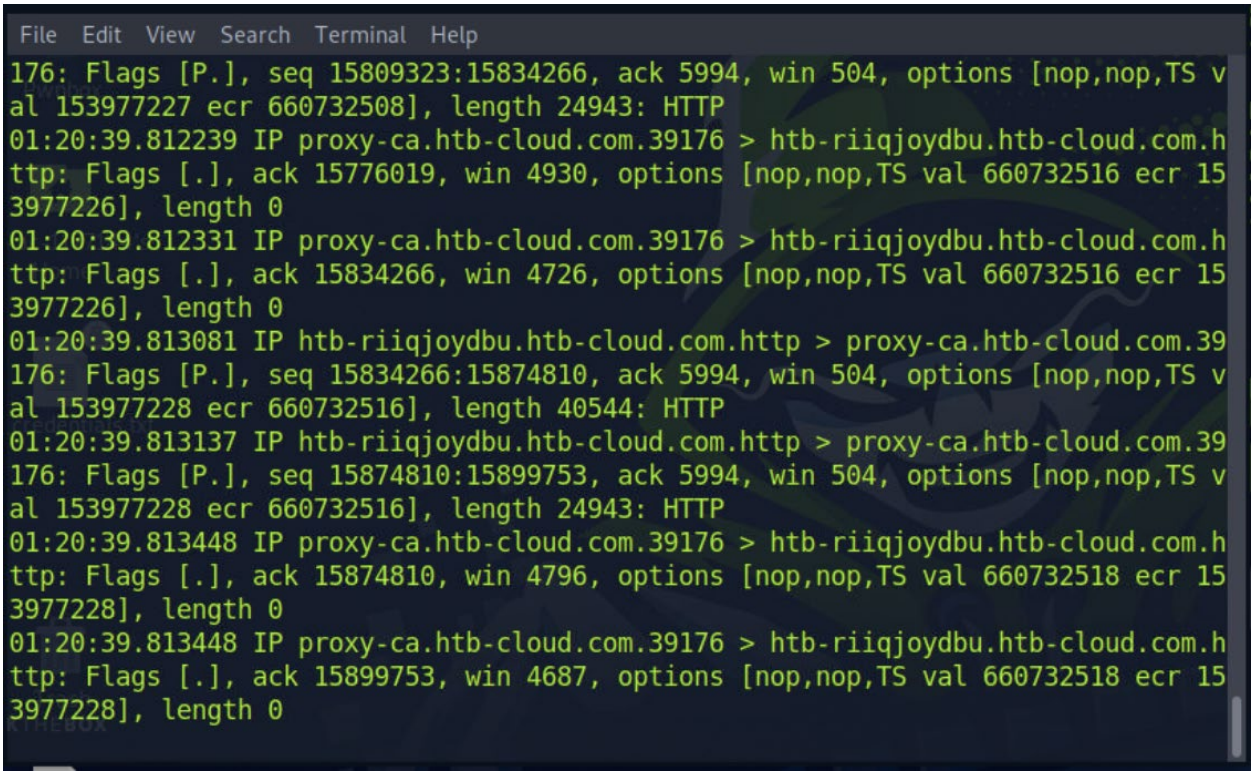


Task #2

Start a capture.

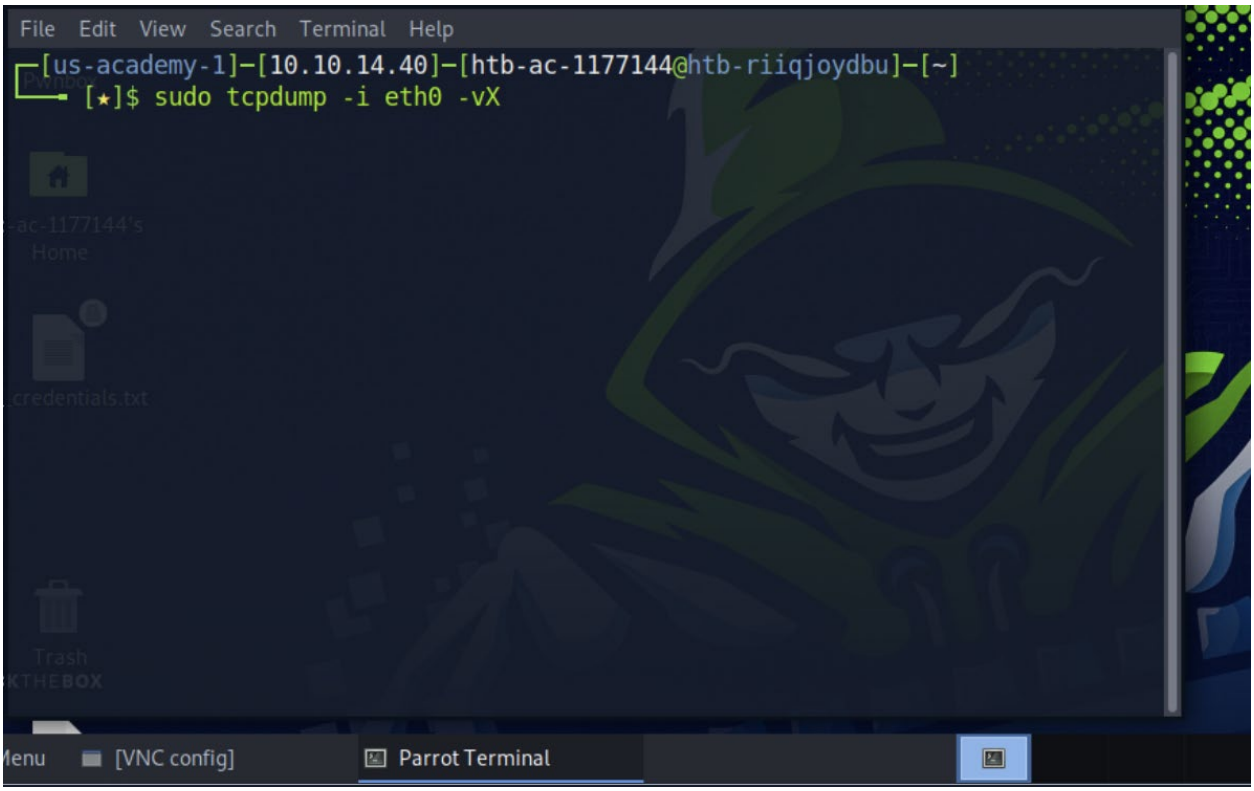


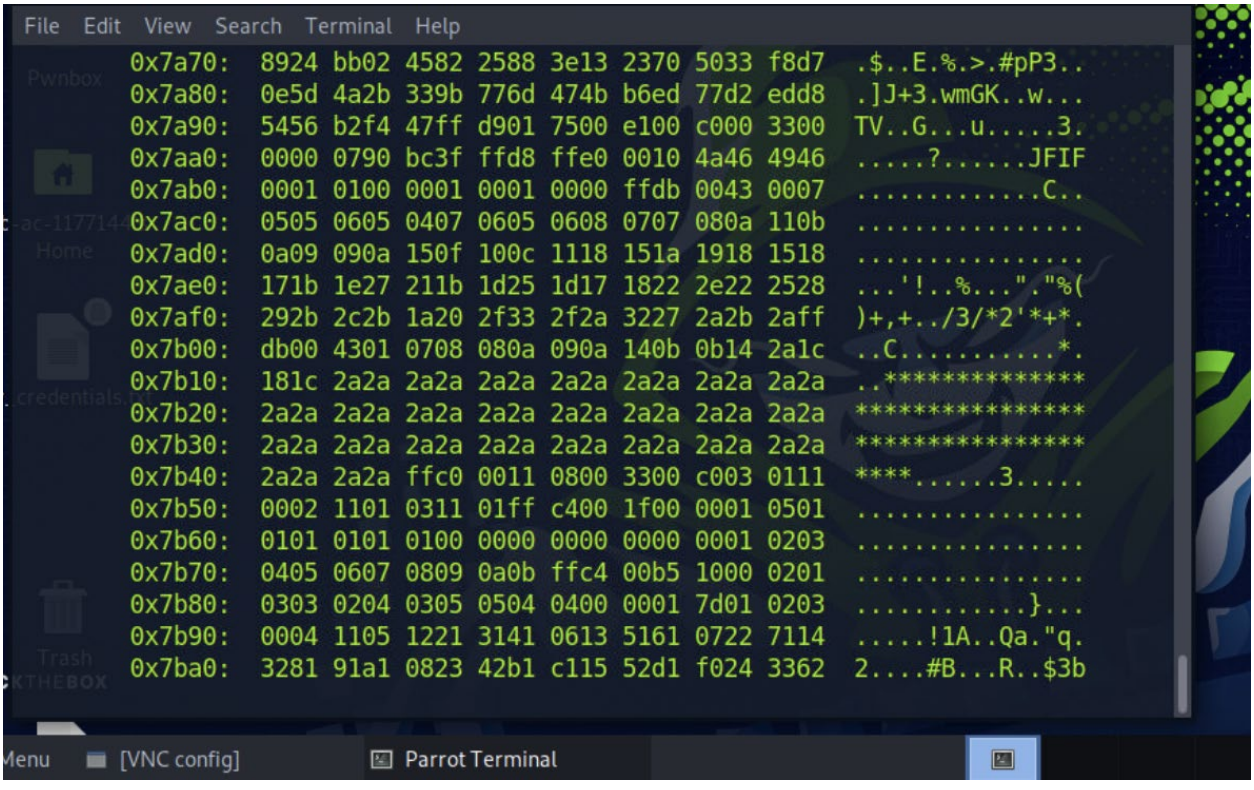

```
File  Edit  View  Search  Terminal  Help
01:20:21.035653 IP htb-riiqjoydbu.htb-cloud.com.http > proxy-ca.htb-cloud.com.39
176: Flags [P.], seq 11943433:11983977, ack 4341, win 504, options [nop,nop,TS v
al 153958450 ecr 660713731], length 40544: HTTP
01:20:21.035765 IP htb-riiqjoydbu.htb-cloud.com.http > proxy-ca.htb-cloud.com.39
176: Flags [P.], seq 11983977:12008920, ack 4341, win 504, options [nop,nop,TS v
al 153958450 ecr 660713731], length 24943: HTTP
01:20:21.036336 IP proxy-ca.htb-cloud.com.39176 > htb-riiqjoydbu.htb-cloud.com.h
ttp: Flags [.], ack 11983977, win 4796, options [nop,nop,TS val 660713740 ecr 15
3958450], length 0
01:20:21.036337 IP proxy-ca.htb-cloud.com.39176 > htb-riiqjoydbu.htb-cloud.com.h
ttp: Flags [.], ack 12008920, win 4696, options [nop,nop,TS val 660713740 ecr 15
3958450], length 0
01:20:21.036657 IP proxy-ca.htb-cloud.com.39176 > htb-riiqjoydbu.htb-cloud.com.h
ttp: Flags [P.], seq 4341:4357, ack 12008920, win 4963, options [nop,nop,TS val
660713741 ecr 153958450], length 16: HTTP
^C
2453 packets captured
2459 packets received by filter
0 packets dropped by kernel
[us-academy-1]-[10.10.14.40]-[htb-ac-1177144@htb-riiqjoydbu]-[~]
[★]$ sudo tcpdump -i eth0
```



Task #3

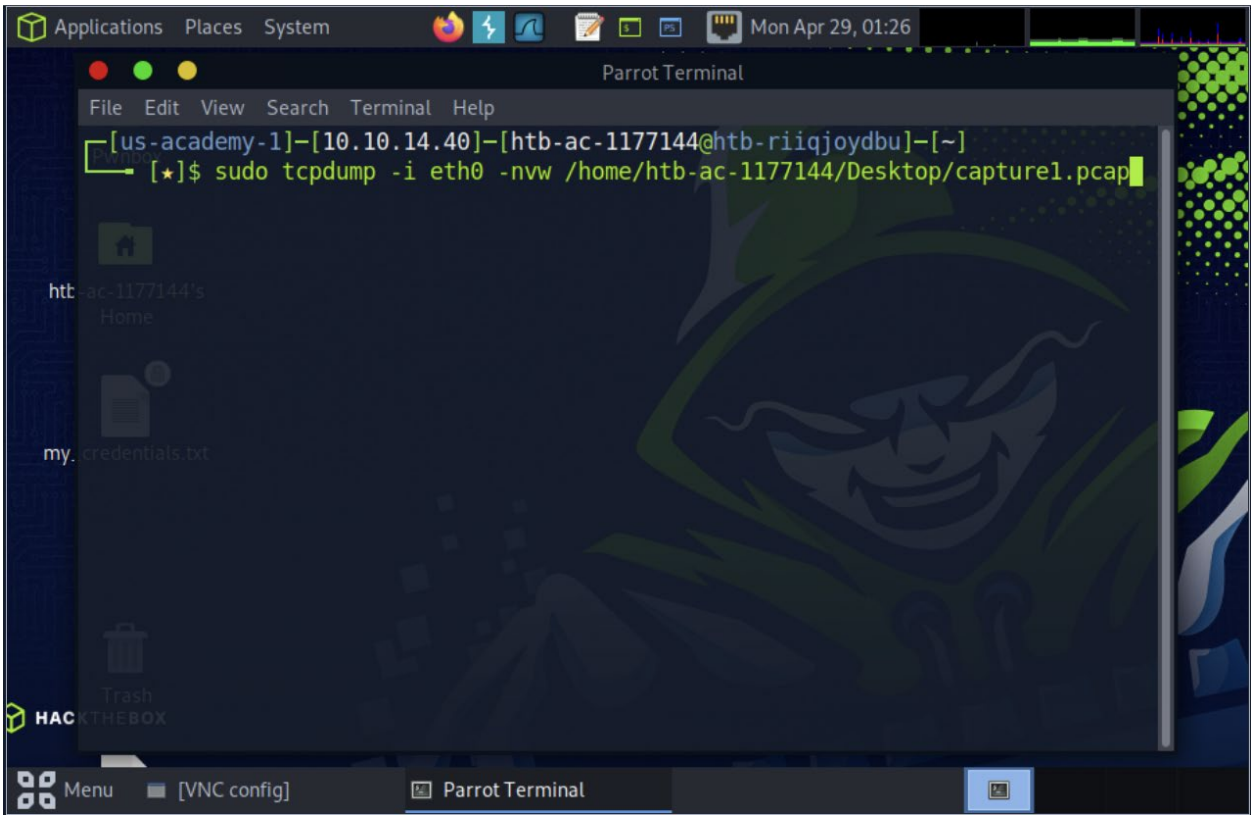
Utilize Basic Capture Filters.

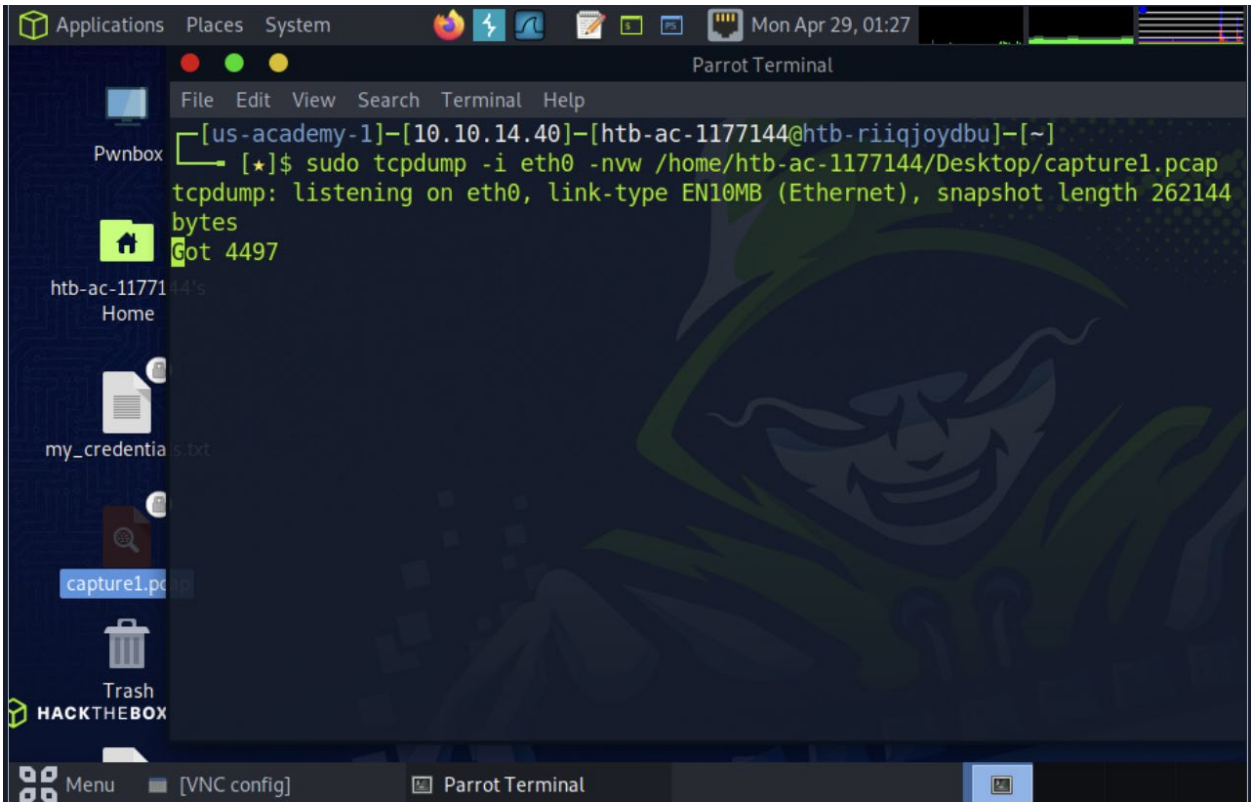

File Edit View Search Terminal Help
[us-academy-1]-[10.10.14.40]-[htb-ac-1177144@htb-riiqjoydbu]-[~]
[★]$ sudo tcpdump -i eth0 -vX
Menu
[VNC config]
Parrot Terminal


File Edit View Search Terminal Help
0x7a70: 8924 bb02 4582 2588 3e13 2370 5033 f8d7 .$..E.%.>.#pP3..
0x7a80: 0e5d 4a2b 339b 776d 474b b6ed 77d2 edd8 .]J+3.wmGK..w...
0x7a90: 5456 b2f4 47ff d901 7500 e100 c000 3300 TV..G...u.....3.
0x7aa0: 0000 0790 bc3f ffd8 ffe0 0010 4a46 4946 .....?......JFIF
0x7ab0: 0001 0100 0001 0001 0000 ffdb 0043 0007 ....C..
0x7ac0: 0505 0605 0407 0605 0608 0707 080a 110b ....
0x7ad0: 0a09 090a 150f 100c 1118 151a 1918 1518 ....
0x7ae0: 171b 1e27 211b 1d25 1d17 1822 2e22 2528 ...'!..%..."."%(
0x7af0: 292b 2c2b 1a20 2f33 2f2a 3227 2a2b 2aff)+,+../3/*2'*+*.
0x7b00: db00 4301 0708 080a 090a 140b 0b14 2a1c ..C...........*.
0x7b10: 181c 2a2a 2a2a 2a2a 2a2a 2a2a 2a2a 2a2a ..**********
0x7b20: 2a2a 2a2a 2a2a 2a2a 2a2a 2a2a 2a2a 2a2a **********
0x7b30: 2a2a 2a2a 2a2a 2a2a 2a2a 2a2a 2a2a 2a2a **********
0x7b40: 2a2a 2a2a ffc0 0011 0800 3300 c003 0111 ****......3.....
0x7b50: 0002 1101 0311 01ff c400 1f00 0001 0501 ....
0x7b60: 0101 0101 0100 0000 0000 0000 0001 0203 ....
0x7b70: 0405 0607 0809 0a0b ffc4 00b5 1000 0201 ....
0x7b80: 0303 0204 0305 0504 0400 0001 7d01 0203 ....}...
0x7b90: 0004 1105 1221 3141 0613 5161 0722 7114 .....!1A..Qa."q.
0x7ba0: 3281 91a1 0823 42b1 c115 52d1 f024 3362 2....#B...R..$3b
Menu
[VNC config]
Parrot Terminal

Task #4

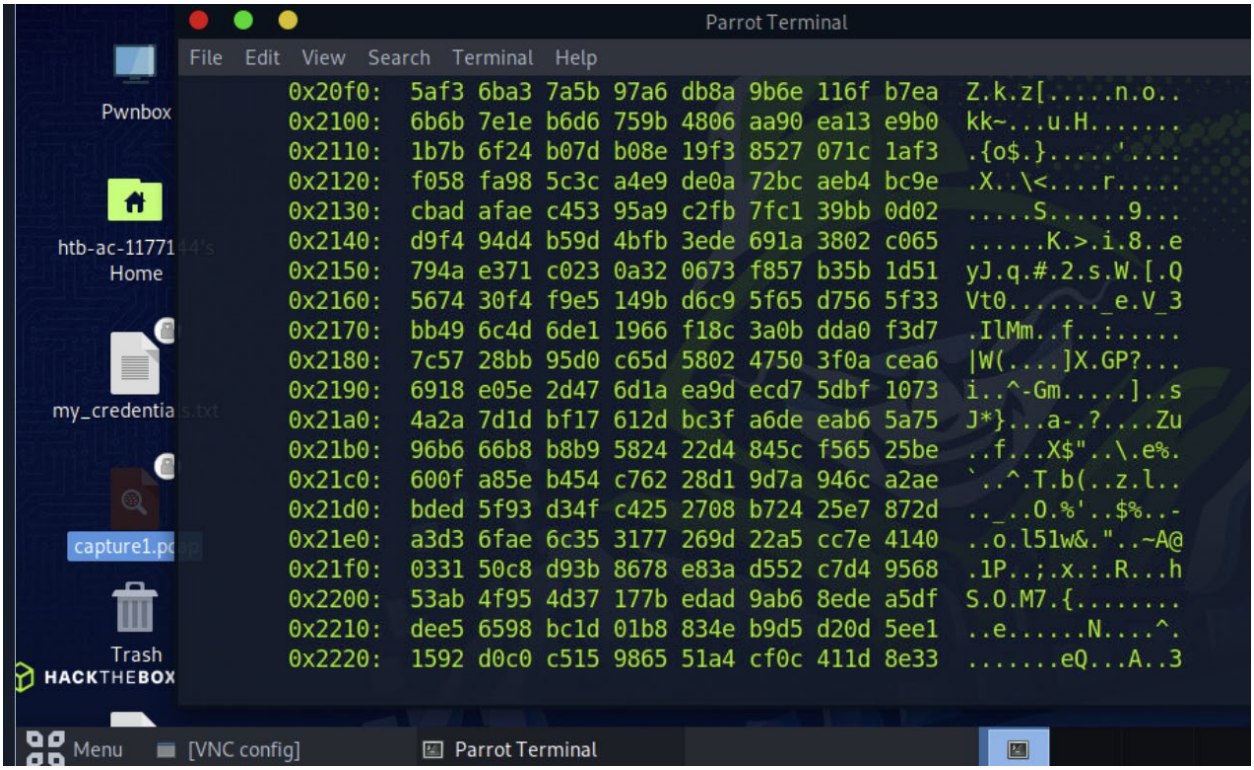
Save a Capture to a .PCAP file.





Task #5

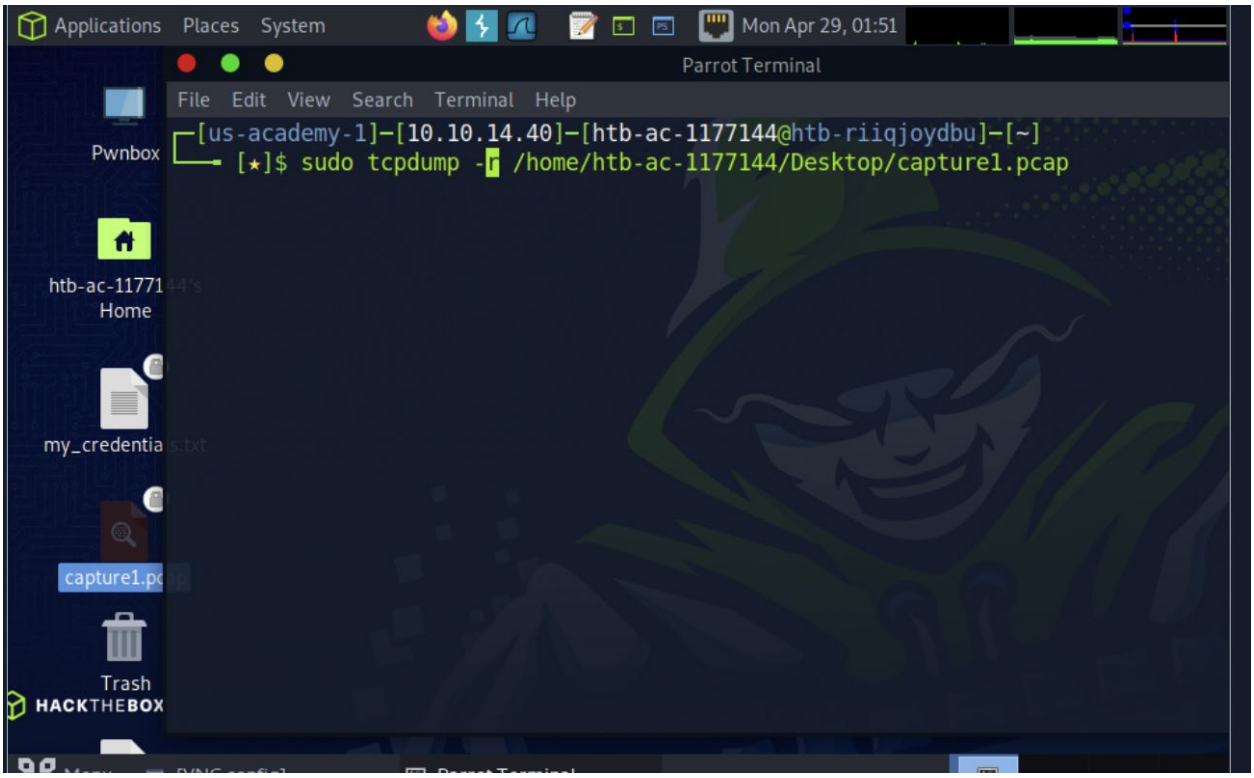
Read the Capture from a .PCAP file.

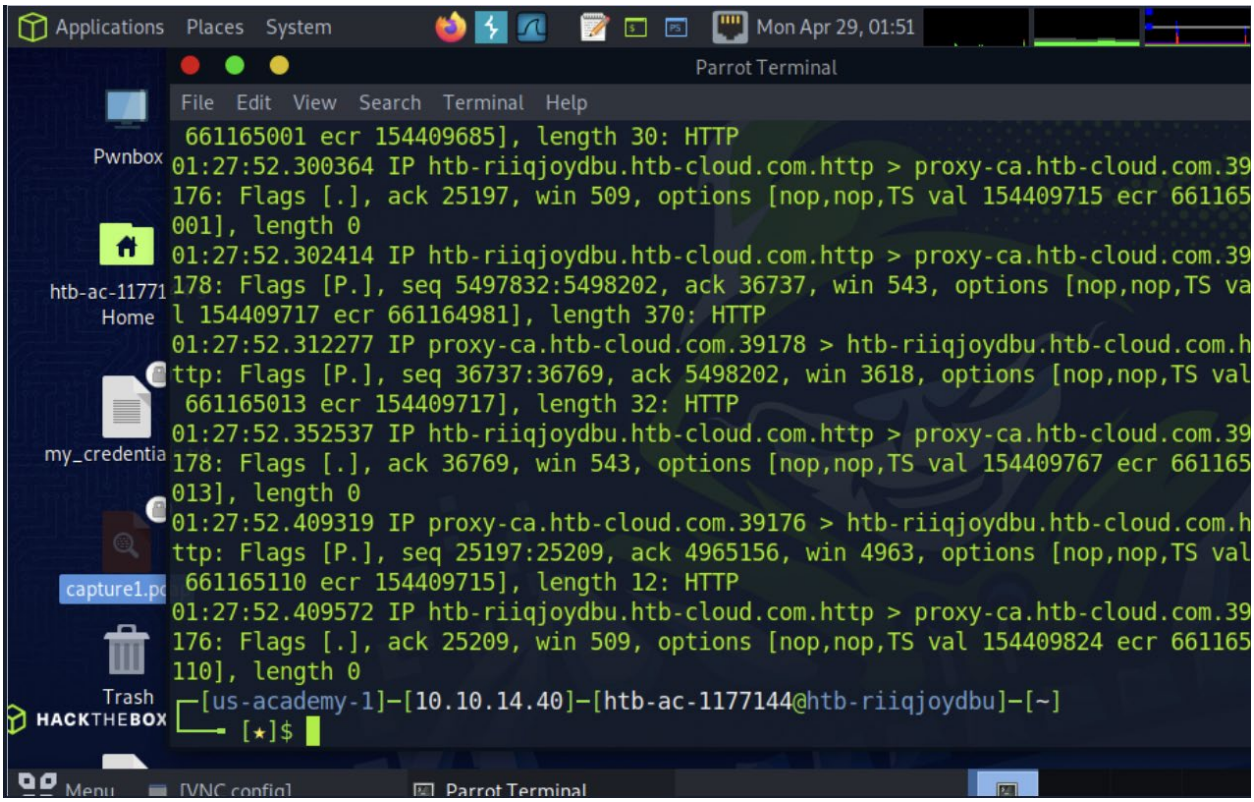


Interrogating Network Traffic With Capture and Display Filters

Task #1

Read a capture from a file without filters implemented.


Applications
Places
System
Mon Apr 29, 01:51
Parrot Terminal
File Edit View Search Terminal Help
[us-academy-1]-[10.10.14.40]-[htb-ac-1177144@htb-riiqjoydbu]-[~]
[★]$ sudo tcpdump -r /home/htb-ac-1177144/Desktop/capture1.pcap
Pwnbox
htb-ac-11771
Home
my_credentia
capture1.pc
Trash
HACKTHEBOX


Applications
Places
System
Mon Apr 29, 01:51
Parrot Terminal
File Edit View Search Terminal Help
661165001 ecr 154409685], length 30: HTTP
01:27:52.300364 IP htb-riiqjoydbu.htb-cloud.com.http > proxy-ca.htb-cloud.com.39
176: Flags [.], ack 25197, win 509, options [nop,nop,TS val 154409715 ecr 661165
001], length 0
01:27:52.302414 IP htb-riiqjoydbu.htb-cloud.com.http > proxy-ca.htb-cloud.com.39
178: Flags [P.], seq 5497832:5498202, ack 36737, win 543, options [nop,nop,TS va
l 154409717 ecr 661164981], length 370: HTTP
01:27:52.312277 IP proxy-ca.htb-cloud.com.39178 > htb-riiqjoydbu.htb-cloud.com.h
ttp: Flags [P.], seq 36737:36769, ack 5498202, win 3618, options [nop,nop,TS val
661165013 ecr 154409717], length 32: HTTP
01:27:52.352537 IP htb-riiqjoydbu.htb-cloud.com.http > proxy-ca.htb-cloud.com.39
178: Flags [.], ack 36769, win 543, options [nop,nop,TS val 154409767 ecr 661165
013], length 0
01:27:52.409319 IP proxy-ca.htb-cloud.com.39176 > htb-riiqjoydbu.htb-cloud.com.h
ttp: Flags [P.], seq 25197:25209, ack 4965156, win 4963, options [nop,nop,TS val
661165110 ecr 154409715], length 12: HTTP
01:27:52.409572 IP htb-riiqjoydbu.htb-cloud.com.http > proxy-ca.htb-cloud.com.39
176: Flags [.], ack 25209, win 509, options [nop,nop,TS val 154409824 ecr 661165
110], length 0
[us-academy-1]-[10.10.14.40]-[htb-ac-1177144@htb-riiqjoydbu]-[~]
[★]$
Pwnbox
htb-ac-11771
Home
my_credentia
capture1.pc
Trash
HACKTHEBOX
Menu
[VNC config]
Parrot Terminal

Task #2

Identify the type of traffic seen.

Common protocols: We should notice a bunch of DNS, HTTP, and HTTPS traffic.

Ports utilized: 53 80 443

Task #3

Identify conversations.

To help make this more straightforward, turning absolute sequence numbers on (-S) will be extremely helpful in determining conversations.

We can also examine the different hosts involved. Servers typically communicate over the well-known port number assigned to the protocol (80 for HTTP, 443 for HTTPS, for example). Hosts or recipients in the conversations will typically utilize a random high port number.

Task #4

Interpret the capture in depth.

To determine the correct timestamp: Read the file with (-r) and then examine the conversations. Find the first one established (Full TCP Handshake "Syn / SYN-ACK / ACK") and look at the first field in the output to find the timestamp. To find the IP of Host ( ), we can filter the traffic only to see conversations Sourcing from it (src 'name-of-host') and then disable Name resolution with (-n). To determine the protocol being utilized in the first conversation, look for the well-known port # while disabling hostname and port name resolution (-nn) or leave off the (-nn), and it will tell you the name of the protocol in the output.

Task #5

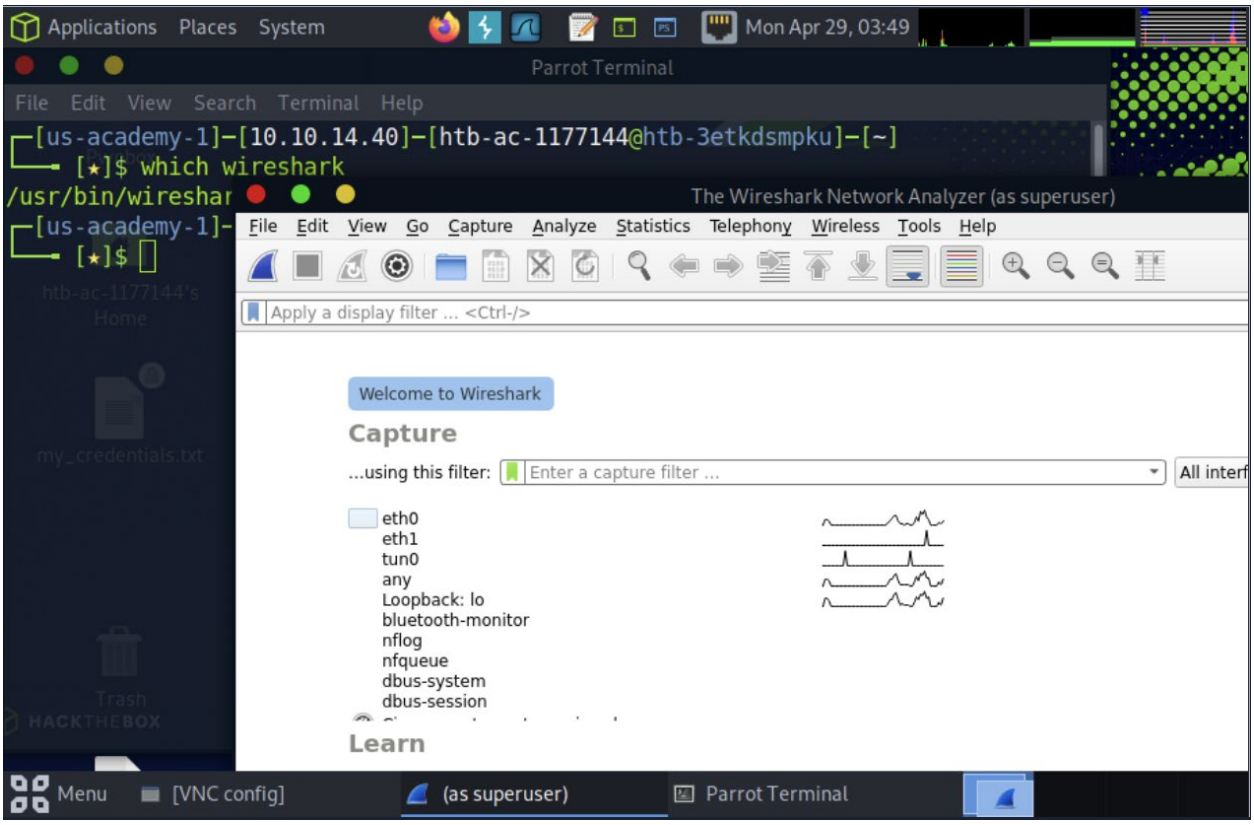
Filter out traffic.

```
Harsh1208@htb[/htb]$ sudo tcpdump -r (file.pcap) udp and port 53
```

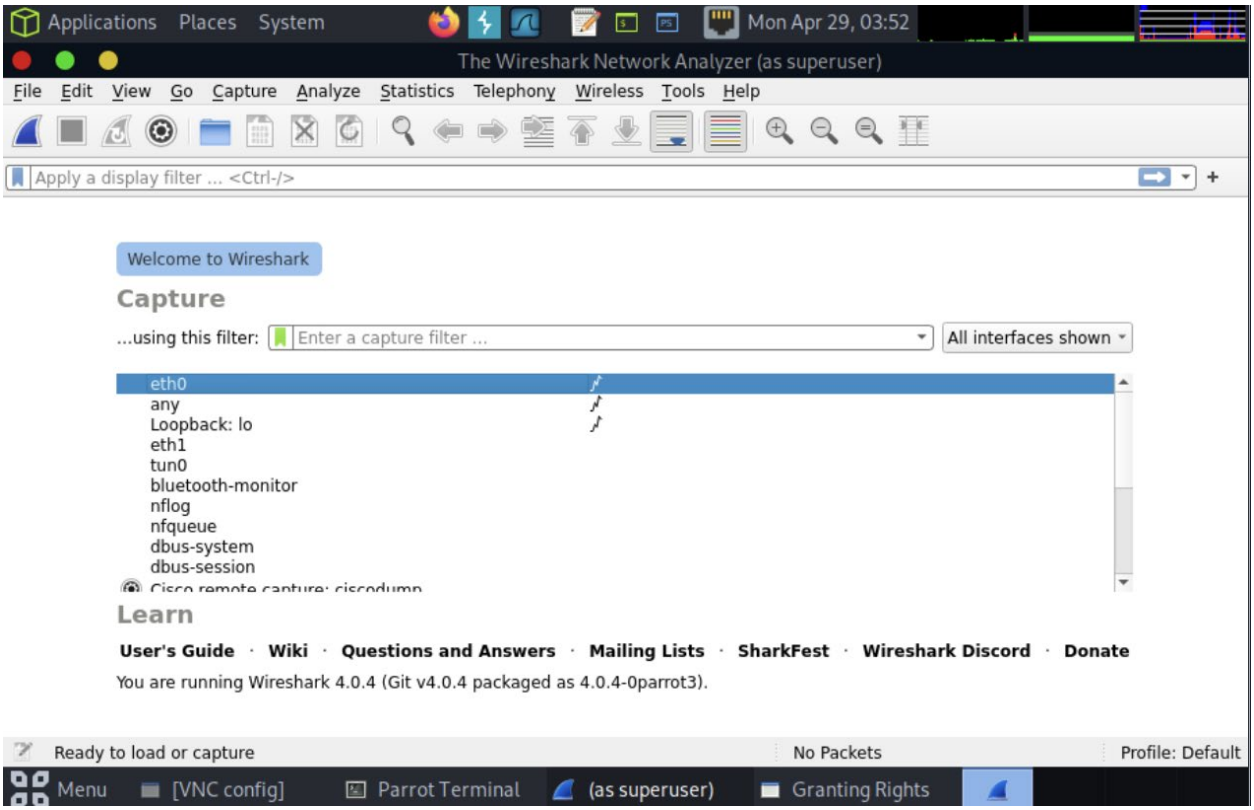
Familiarity With Wireshark

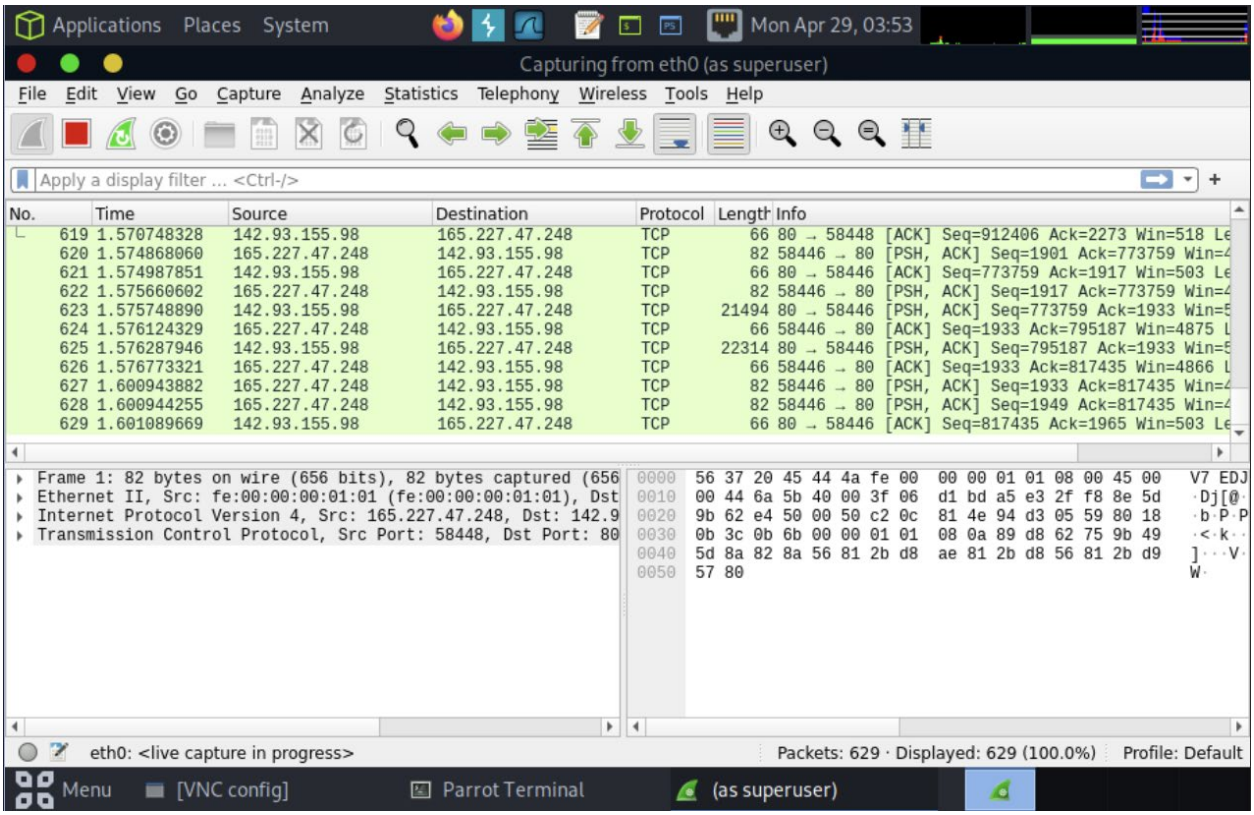
Task #1

Validate Wireshark is installed, then open Wireshark and familiarize yourself with the GUI windows and toolbars.



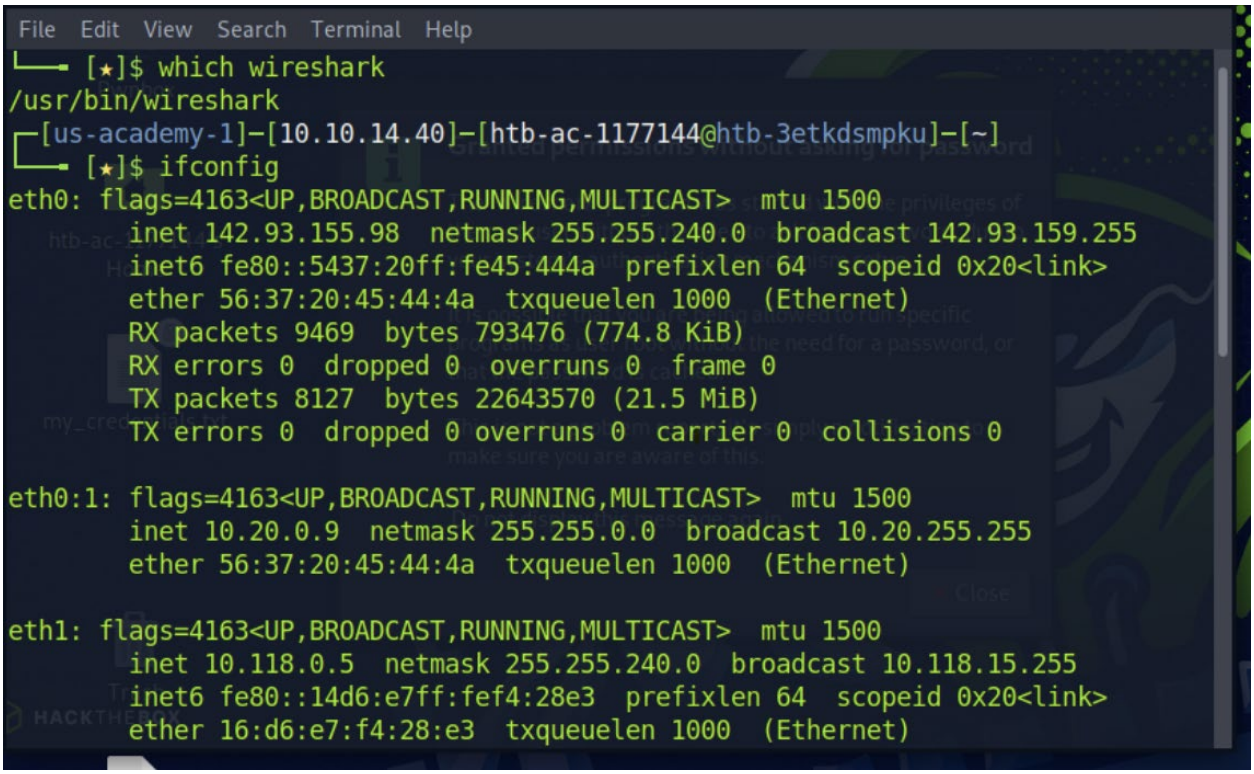
Task #2 Select an interface to run a capture on and create a capture filter to show only traffic to and from your host IP.

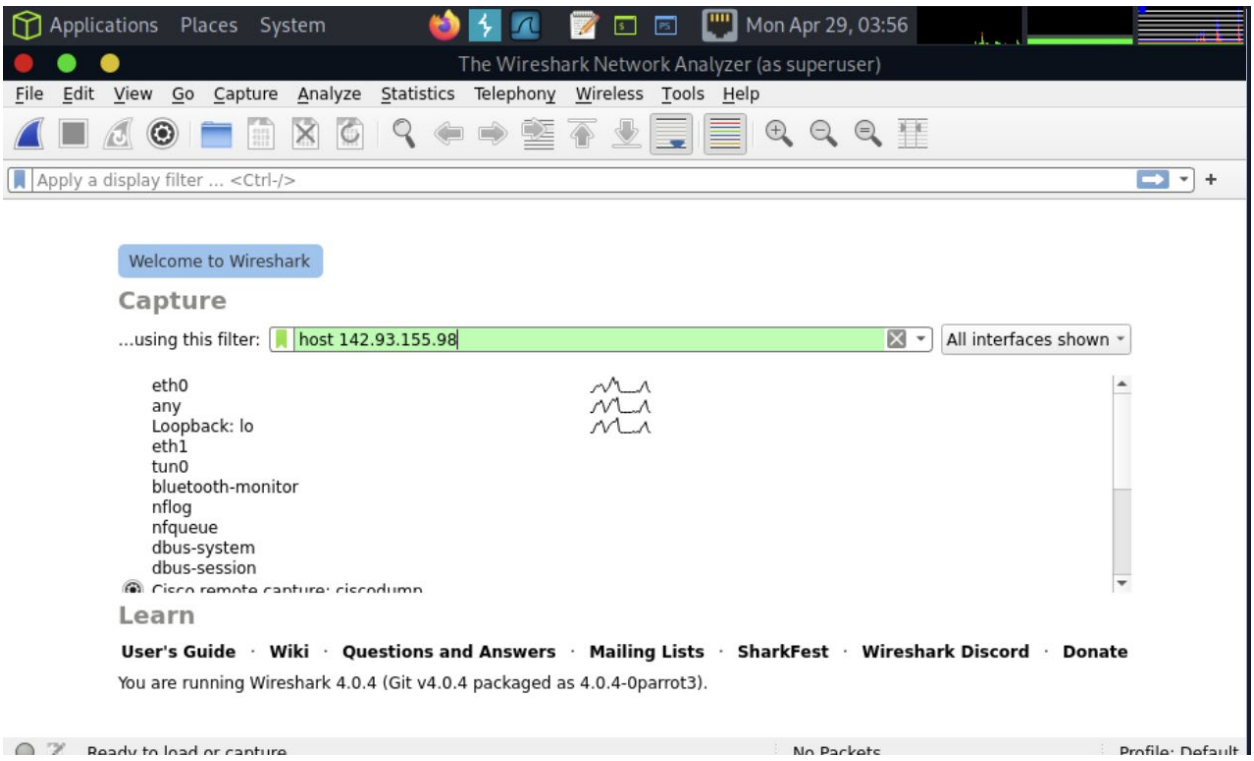

Applications Places System
Mon Apr 29, 03:52
The Wireshark Network Analyzer (as superuser)
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
Welcome to Wireshark
Capture
...using this filter: Enter a capture filter ...
All interfaces shown
eth0
any
Loopback: lo
eth1
tun0
bluetooth-monitor
nflog
nfqueue
dbus-system
dbus-session
Learn
User's Guide · Wiki · Questions and Answers · Mailing Lists · SharkFest · Wireshark Discord · Donate
You are running Wireshark 4.0.4 (Git v4.0.4 packaged as 4.0.4-0parrot3).
Ready to load or capture
No Packets
Profile: Default
Menu
[VNC config]
Parrot Terminal
(as superuser)
Granting Rights

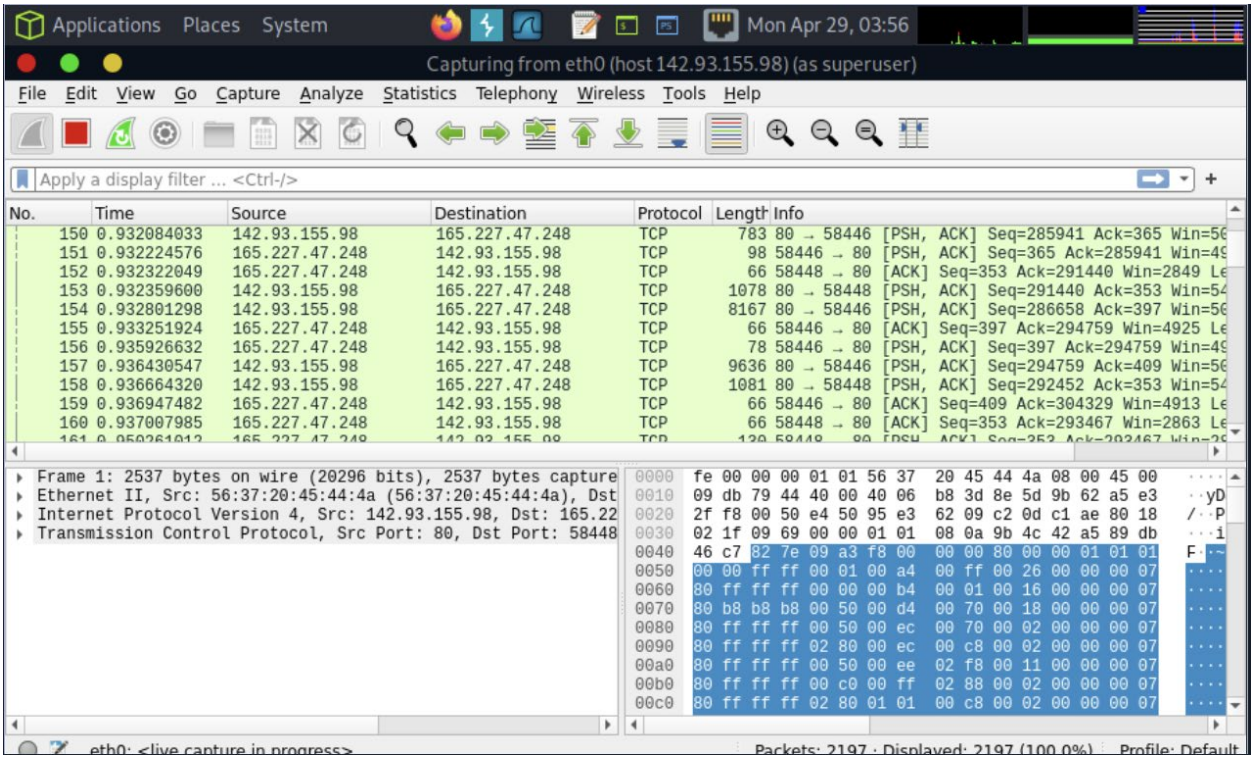

Applications Places System
Mon Apr 29, 03:53
Capturing from eth0 (as superuser)
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
No. Time Source Destination Protocol Length Info
619 1.570748328 142.93.155.98 165.227.47.248 TCP 66 80 → 58448 [ACK] Seq=912406 Ack=2273 Win=518 Le
620 1.574868060 165.227.47.248 142.93.155.98 TCP 82 58446 → 80 [PSH, ACK] Seq=1901 Ack=773759 Win=4
621 1.574987851 142.93.155.98 165.227.47.248 TCP 66 80 → 58446 [ACK] Seq=773759 Ack=1917 Win=503 Le
622 1.575660602 165.227.47.248 142.93.155.98 TCP 82 58446 → 80 [PSH, ACK] Seq=1917 Ack=773759 Win=4
623 1.575748890 142.93.155.98 165.227.47.248 TCP 21494 80 → 58446 [PSH, ACK] Seq=773759 Ack=1933 Win=5
624 1.576124329 165.227.47.248 142.93.155.98 TCP 66 58446 → 80 [ACK] Seq=1933 Ack=795187 Win=4875 L
625 1.576287946 142.93.155.98 165.227.47.248 TCP 22314 80 → 58446 [PSH, ACK] Seq=795187 Ack=1933 Win=5
626 1.576773321 165.227.47.248 142.93.155.98 TCP 66 58446 → 80 [ACK] Seq=1933 Ack=817435 Win=4866 L
627 1.600943882 165.227.47.248 142.93.155.98 TCP 82 58446 → 80 [PSH, ACK] Seq=1933 Ack=817435 Win=4
628 1.600944255 165.227.47.248 142.93.155.98 TCP 82 58446 → 80 [PSH, ACK] Seq=1949 Ack=817435 Win=4
629 1.601089669 142.93.155.98 165.227.47.248 TCP 66 80 → 58446 [ACK] Seq=817435 Ack=1965 Win=503 Le
Frame 1: 82 bytes on wire (656 bits), 82 bytes captured (656
Ethernet II, Src: fe:00:00:00:01:01 (fe:00:00:00:01:01), Dst
Internet Protocol Version 4, Src: 165.227.47.248, Dst: 142.9
Transmission Control Protocol, Src Port: 58448, Dst Port: 80
0000 56 37 20 45 44 4a fe 00 00 00 01 01 08 00 45 00 V7 EDJ
0010 00 44 6a 5b 40 00 3f 06 d1 bd a5 e3 2f f8 8e 5d ·Dj[@·
0020 9b 62 e4 50 00 50 c2 0c 81 4e 94 d3 05 59 80 18 ·b·P·P
0030 0b 3c 0b 6b 00 00 01 01 08 0a 89 d8 62 75 9b 49 ·<·k··
0040 5d 8a 82 8a 56 81 2b d8 ae 81 2b d8 56 81 2b d9]···V·
0050 57 80 W·
eth0: <live capture in progress>
Packets: 629 · Displayed: 629 (100.0%)
Profile: Default
Menu
[VNC config]
Parrot Terminal
(as superuser)

Task #3

Create a capture filter.

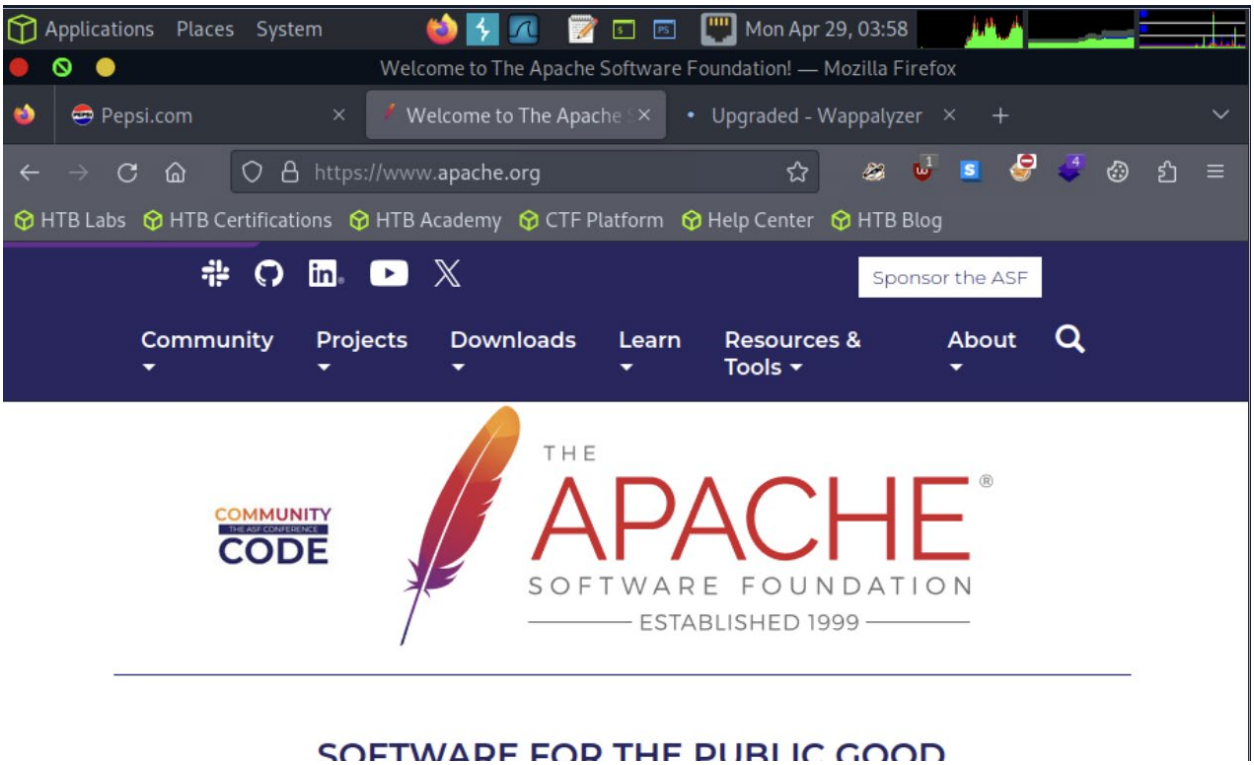


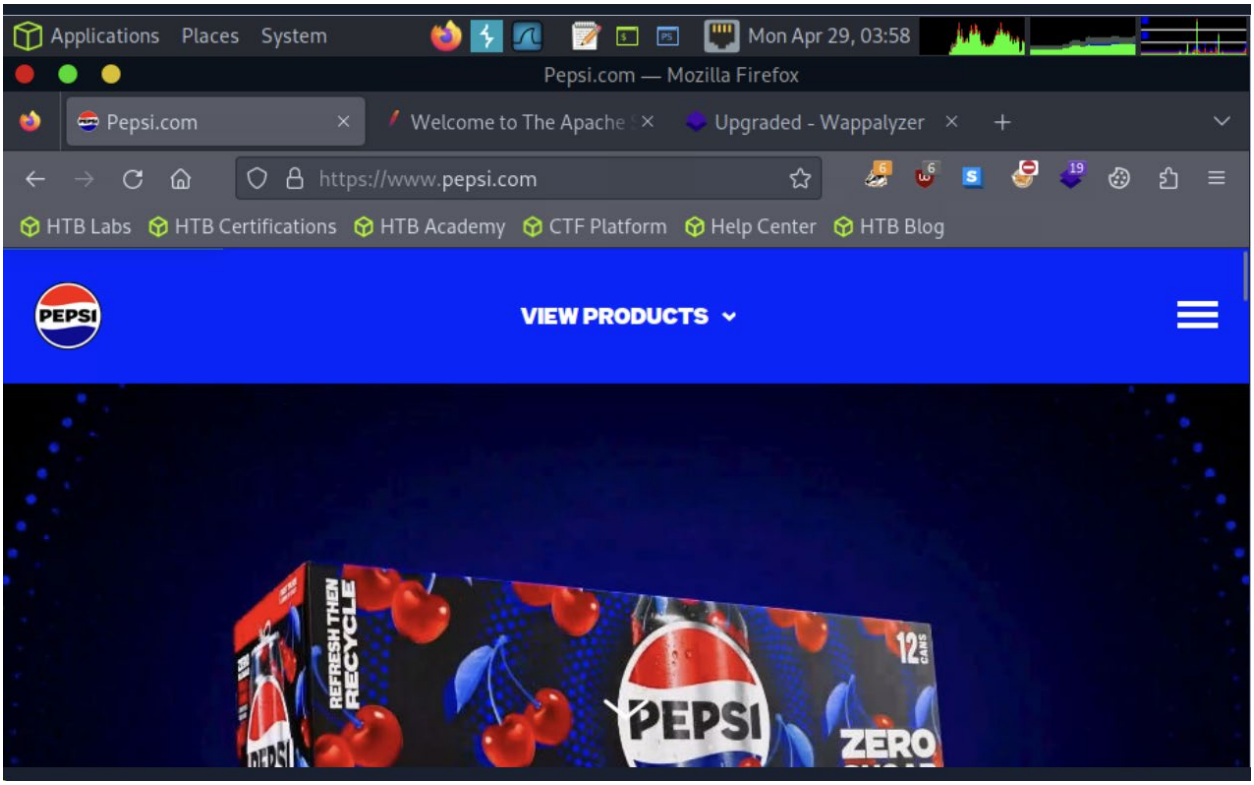




Task #4

Navigate to a webpage to generate some traffic.


Applications Places System
Mon Apr 29, 03:58
Welcome to The Apache Software Foundation! — Mozilla Firefox
Pepsi.com
Welcome to The Apache
Upgraded - Wappalyzer
https://www.apache.org
HTB Labs
HTB Certifications
HTB Academy
CTF Platform
Help Center
HTB Blog
Sponsor the ASF
Community
Projects
Downloads
Learn
Resources & Tools
About
COMMUNITY
CODE
THE
APACHE
SOFTWARE FOUNDATION
ESTABLISHED 1999
SOFTWARE FOR THE PUBLIC GOOD


Applications Places System
Mon Apr 29, 03:58
Pepsi.com — Mozilla Firefox
Pepsi.com
Welcome to The Apache
Upgraded - Wappalyzer
https://www.pepsi.com
HTB Labs
HTB Certifications
HTB Academy
CTF Platform
Help Center
HTB Blog
PEPSI
VIEW PRODUCTS
REFRESH THEN RECYCLE
PEPSI
12 CANS
ZERO

Task #5

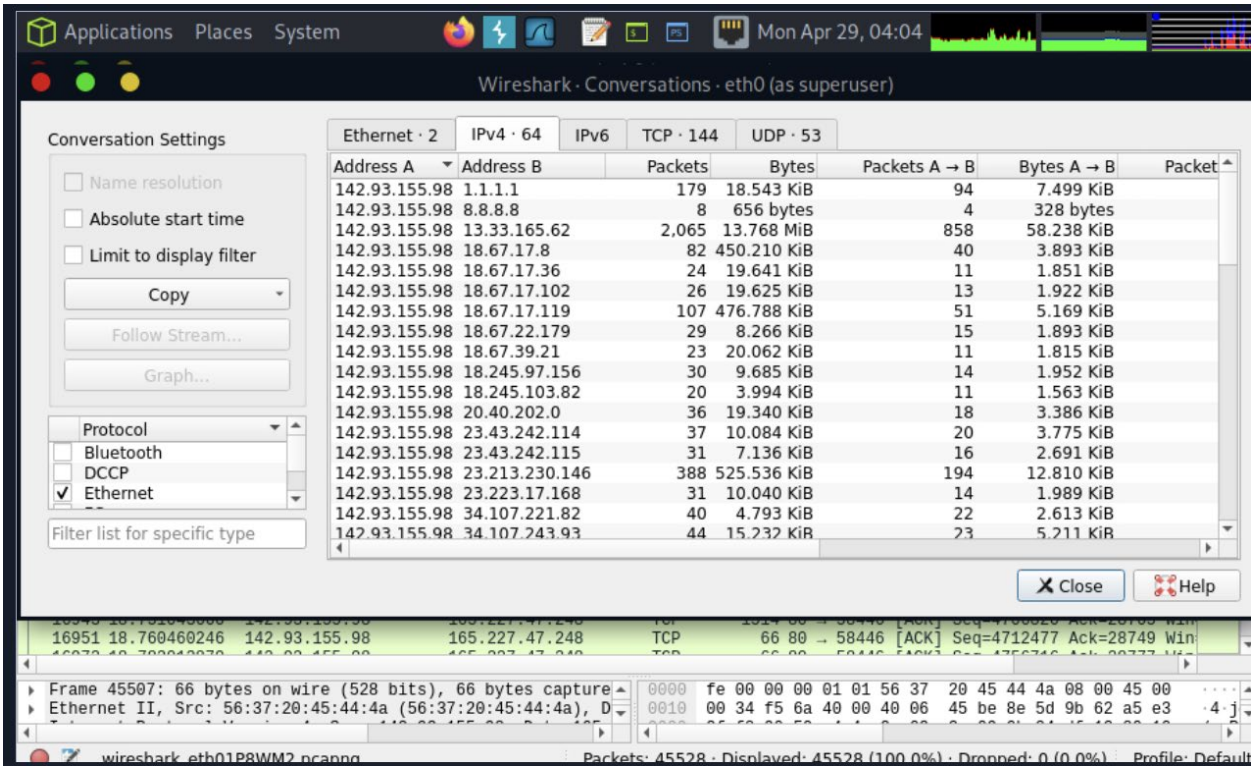
Use the capture results to answer the following questions.

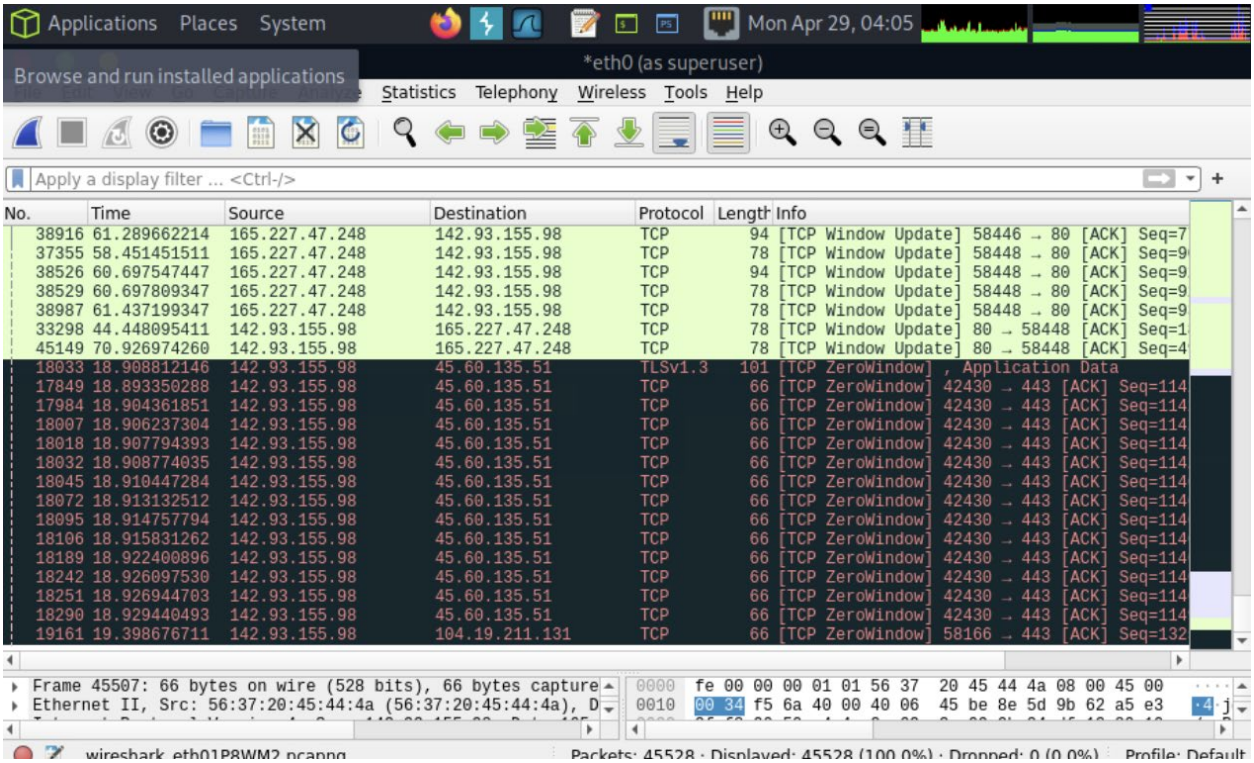
Are multiple sessions being established between the machine and the webserver? How can you tell?

What application-level protocols are displayed in the results?

Can we discern anything in clear text? What was it?

When visiting pepsi.com and http://apache.org you would have gotten several different streams and many different protocols. DNS to request the records for the pages, HTTP for the apache.org site, HTTPS for Pepsi.com, along with any other traffic happening in your network segment at the time. If you noticed a difference between the traffic, you are on the right track. If you look at the output from apache.org it will be in plain text. This happens because HTTP is not encrypted. Looking at HTTPS traffic will be much different, however.


Applications Places System
Mon Apr 29, 04:04
Wireshark · Conversations · eth0 (as superuser)
Conversation Settings
Name resolution
Absolute start time
Limit to display filter
Copy
Follow Stream...
Graph...
Protocol
Bluetooth
DCCP
Ethernet
Filter list for specific type
Ethernet · 2
IPv4 · 64
IPv6
TCP · 144
UDP · 53
Address A Address B Packets Bytes Packets A → B Bytes A → B Packet
142.93.155.98 1.1.1.1 179 18.543 KiB 94 7.499 KiB
142.93.155.98 8.8.8.8 8 656 bytes 4 328 bytes
142.93.155.98 13.33.165.62 2,065 13.768 MiB 858 58.238 KiB
142.93.155.98 18.67.17.8 82 450.210 KiB 40 3.893 KiB
142.93.155.98 18.67.17.36 24 19.641 KiB 11 1.851 KiB
142.93.155.98 18.67.17.102 26 19.625 KiB 13 1.922 KiB
142.93.155.98 18.67.17.119 107 476.788 KiB 51 5.169 KiB
142.93.155.98 18.67.22.179 29 8.266 KiB 15 1.893 KiB
142.93.155.98 18.67.39.21 23 20.062 KiB 11 1.815 KiB
142.93.155.98 18.245.97.156 30 9.685 KiB 14 1.952 KiB
142.93.155.98 18.245.103.82 20 3.994 KiB 11 1.563 KiB
142.93.155.98 20.40.202.0 36 19.340 KiB 18 3.386 KiB
142.93.155.98 23.43.242.114 37 10.084 KiB 20 3.775 KiB
142.93.155.98 23.43.242.115 31 7.136 KiB 16 2.691 KiB
142.93.155.98 23.213.230.146 388 525.536 KiB 194 12.810 KiB
142.93.155.98 23.223.17.168 31 10.040 KiB 14 1.989 KiB
142.93.155.98 34.107.221.82 40 4.793 KiB 22 2.613 KiB
142.93.155.98 34.107.243.93 44 15.232 KiB 23 5.211 KiB
Close
Help
16951 18.760460246 142.93.155.98 165.227.47.248 TCP 66 80 → 58446 [ACK] Seq=4712477 Ack=28749 Win
Frame 45507: 66 bytes on wire (528 bits), 66 bytes capture
Ethernet II, Src: 56:37:20:45:44:4a (56:37:20:45:44:4a), D
0000 fe 00 00 00 01 01 56 37 20 45 44 4a 08 00 45 00
0010 00 34 f5 6a 40 00 40 06 45 be 8e 5d 9b 62 a5 e3
wireshark_eth01P8WM2.pcapng
Packets: 45528 · Displayed: 45528 (100.0%) · Dropped: 0 (0.0%)
Profile: Default

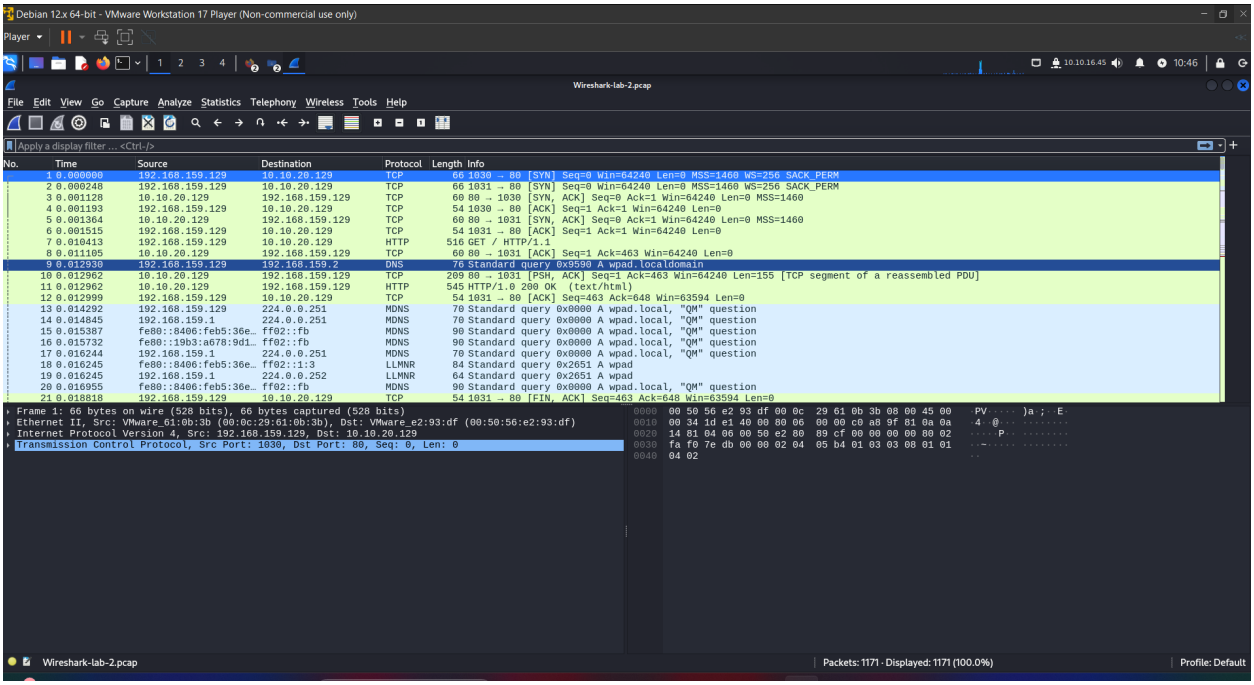

Applications Places System
Mon Apr 29, 04:05
Browse and run installed applications
*eth0 (as superuser)
Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
No. Time Source Destination Protocol Length Info
38916 61.289662214 165.227.47.248 142.93.155.98 TCP 94 [TCP Window Update] 58446 → 80 [ACK] Seq=7
37355 58.451451511 165.227.47.248 142.93.155.98 TCP 78 [TCP Window Update] 58448 → 80 [ACK] Seq=9
38526 60.697547447 165.227.47.248 142.93.155.98 TCP 94 [TCP Window Update] 58448 → 80 [ACK] Seq=9
38529 60.697809347 165.227.47.248 142.93.155.98 TCP 78 [TCP Window Update] 58448 → 80 [ACK] Seq=9
38987 61.437199347 165.227.47.248 142.93.155.98 TCP 78 [TCP Window Update] 58448 → 80 [ACK] Seq=9
33298 44.448095411 142.93.155.98 165.227.47.248 TCP 78 [TCP Window Update] 80 → 58448 [ACK] Seq=1
45149 70.926974260 142.93.155.98 165.227.47.248 TCP 78 [TCP Window Update] 80 → 58448 [ACK] Seq=4
18033 18.908812146 142.93.155.98 45.60.135.51 TLSv1.3 101 [TCP ZeroWindow] , Application Data
17849 18.893350288 142.93.155.98 45.60.135.51 TCP 66 [TCP ZeroWindow] 42430 → 443 [ACK] Seq=114
17984 18.904361851 142.93.155.98 45.60.135.51 TCP 66 [TCP ZeroWindow] 42430 → 443 [ACK] Seq=114
18007 18.906237304 142.93.155.98 45.60.135.51 TCP 66 [TCP ZeroWindow] 42430 → 443 [ACK] Seq=114
18018 18.907794393 142.93.155.98 45.60.135.51 TCP 66 [TCP ZeroWindow] 42430 → 443 [ACK] Seq=114
18032 18.908774035 142.93.155.98 45.60.135.51 TCP 66 [TCP ZeroWindow] 42430 → 443 [ACK] Seq=114
18045 18.910447284 142.93.155.98 45.60.135.51 TCP 66 [TCP ZeroWindow] 42430 → 443 [ACK] Seq=114
18072 18.913132512 142.93.155.98 45.60.135.51 TCP 66 [TCP ZeroWindow] 42430 → 443 [ACK] Seq=114
18095 18.914757794 142.93.155.98 45.60.135.51 TCP 66 [TCP ZeroWindow] 42430 → 443 [ACK] Seq=114
18106 18.915831262 142.93.155.98 45.60.135.51 TCP 66 [TCP ZeroWindow] 42430 → 443 [ACK] Seq=114
18189 18.922400896 142.93.155.98 45.60.135.51 TCP 66 [TCP ZeroWindow] 42430 → 443 [ACK] Seq=114
18242 18.926097530 142.93.155.98 45.60.135.51 TCP 66 [TCP ZeroWindow] 42430 → 443 [ACK] Seq=114
18251 18.926944703 142.93.155.98 45.60.135.51 TCP 66 [TCP ZeroWindow] 42430 → 443 [ACK] Seq=114
18290 18.929440493 142.93.155.98 45.60.135.51 TCP 66 [TCP ZeroWindow] 42430 → 443 [ACK] Seq=114
19161 19.398676711 142.93.155.98 104.19.211.131 TCP 66 [TCP ZeroWindow] 58166 → 443 [ACK] Seq=132
Frame 45507: 66 bytes on wire (528 bits), 66 bytes capture
Ethernet II, Src: 56:37:20:45:44:4a (56:37:20:45:44:4a), D
0000 fe 00 00 00 01 01 56 37 20 45 44 4a 08 00 45 00
0010 00 34 f5 6a 40 00 40 06 45 be 8e 5d 9b 62 a5 e3
wireshark_eth01P8WM2.pcapng
Packets: 45528 · Displayed: 45528 (100.0%) · Dropped: 0 (0.0%)
Profile: Default

Packet Inception, Dissecting Network Traffic With Wireshark

Task #1

Open a pre-captured file (HTTP extraction)

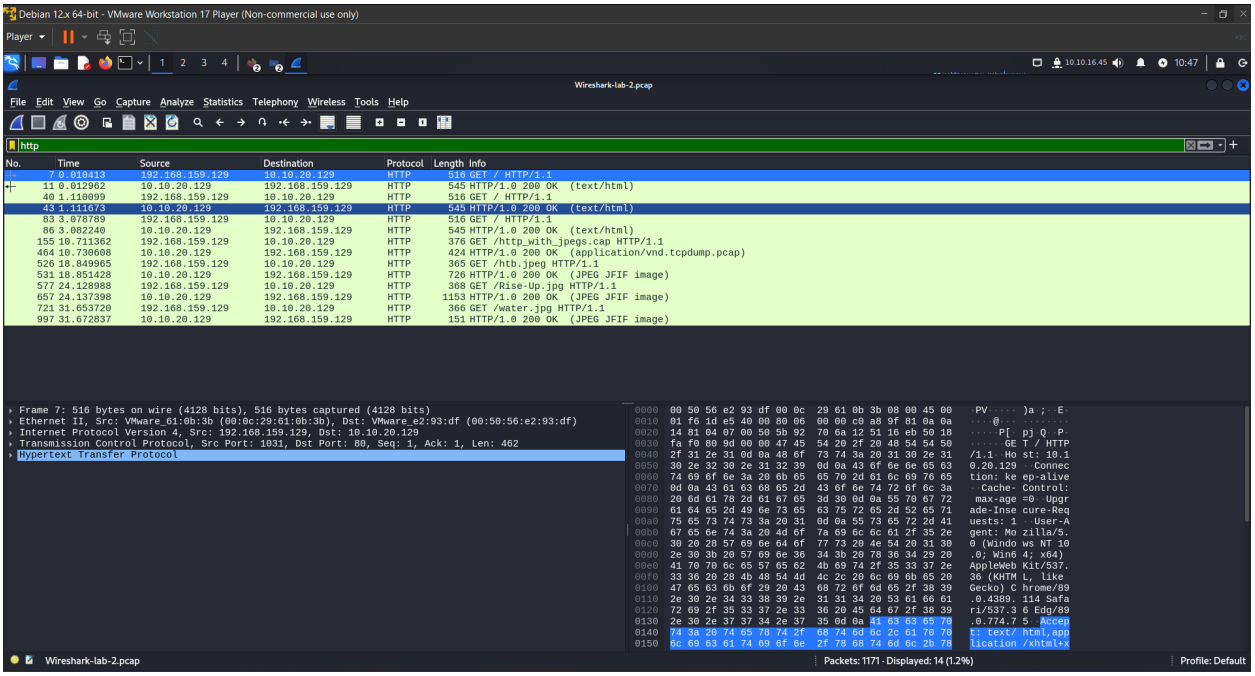
In Wireshark, Select File → Open → , then browse to Wireshark-lab-2.pcap. Open the file.



Task #2

Filter the results.

Now that we have the pcap file open in Wireshark, we can see quite a lot of traffic within this capture file. It has around 1171 packets total, and of those, less than 20 are HTTP packets specifically. Take a minute to examine the pcap file, become familiar with the conversations being had while thinking of the task to accomplish. Our goal is to extract potential images embedded for evidence. Based on what has been asked of us, let's clear our view by filtering for HTTP traffic only.

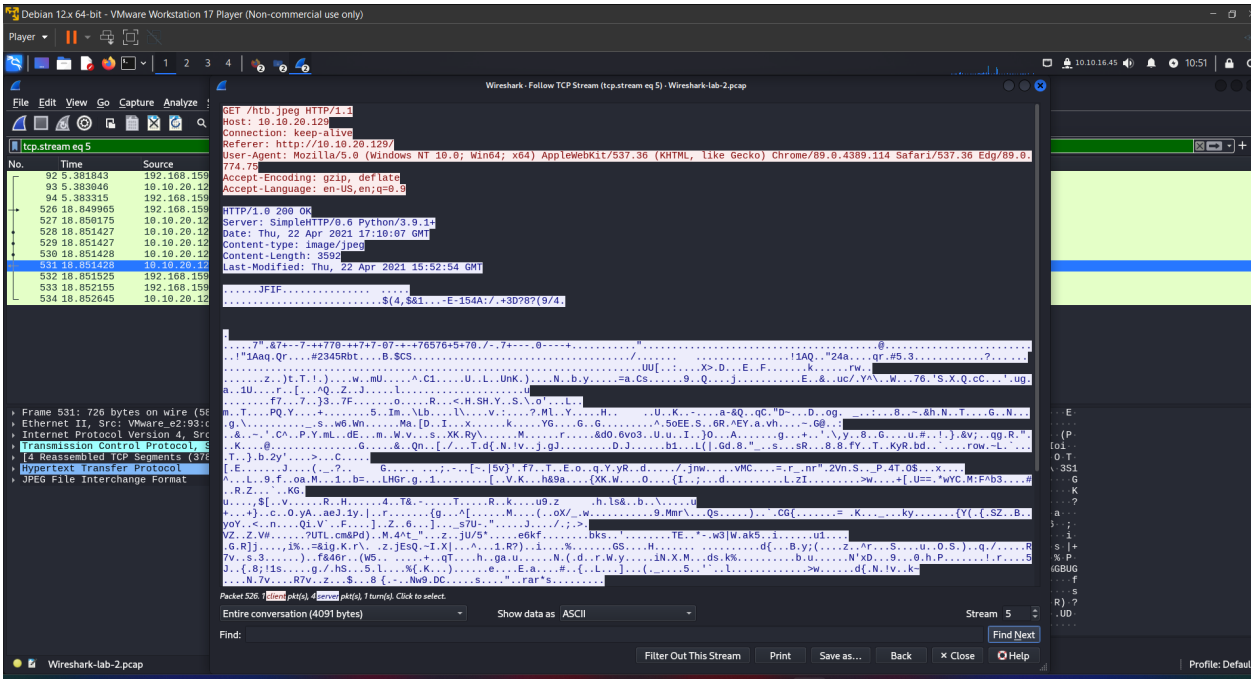


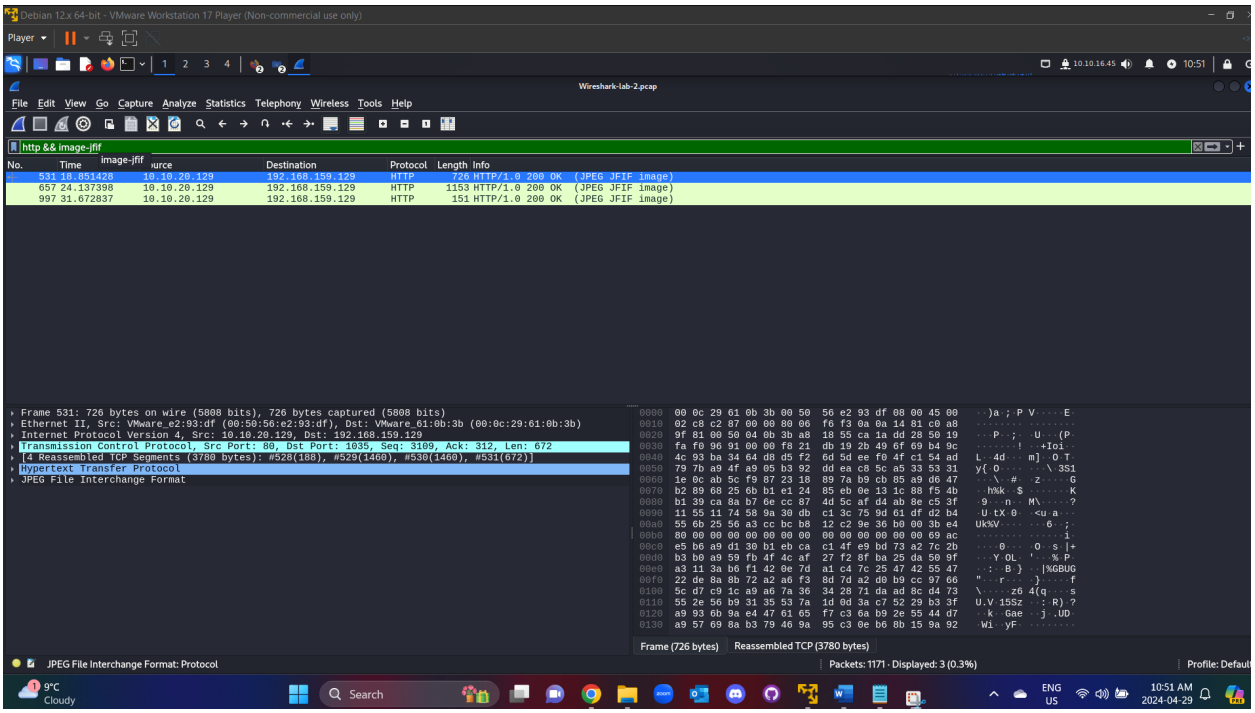
Task #3

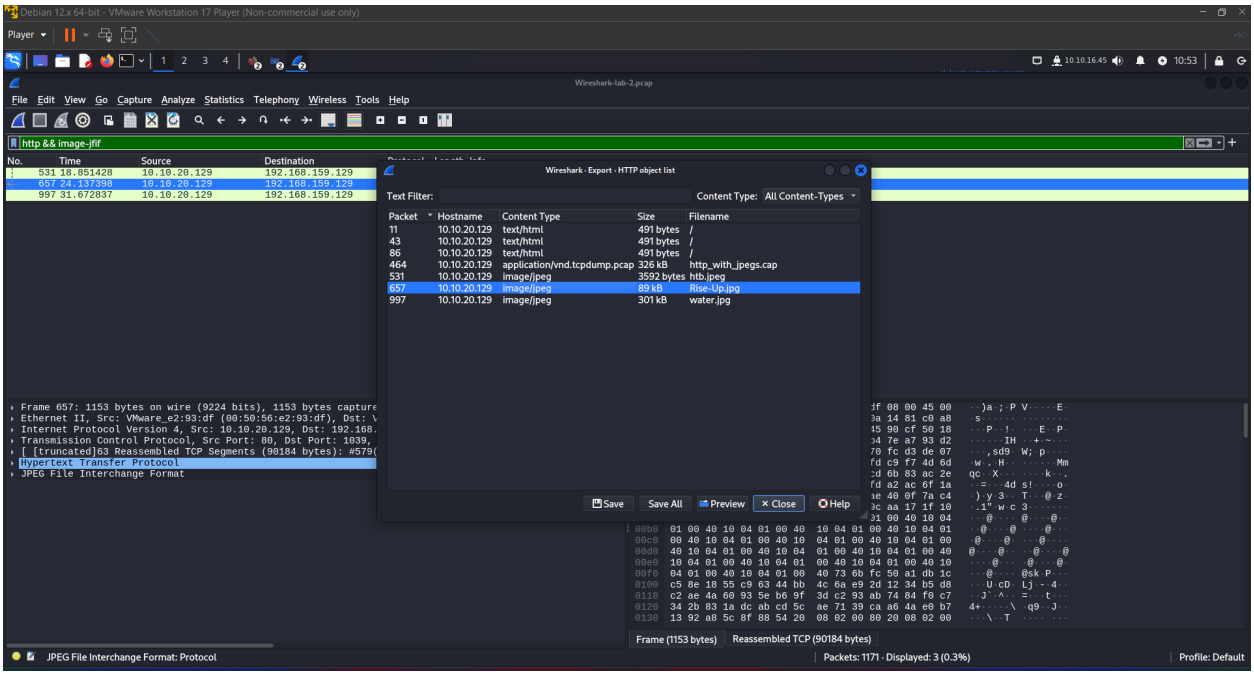
Follow the stream and extract the item(s) found.

So now that we have established there is HTTP traffic in this capture file, let's try to grab some of the items inside as requested. The first thing we need to do is follow the stream for one of the file transfers. With our http filter still applied, look for one of the lines in which the Web Server responds with a

“200 OK” message which acts as an acknowledgment/receipt to a users’ GET request. Now let's select that packet and follow the TCP stream.







Guided Lab: Traffic Analysis Workflow

Task #1

Connect to the live host for capture.

Analysis

Follow this workflow template and examine the suspicious traffic. The goal is to determine what is happening with the host in question.

1. what is the issue?

1. a brief summary of the issue.

2. define our scope and the goal (what are we looking for? which time period?)
    1. Scope: what are we looking for, where?
    2. when the issue started:
    3. supporting info: Files, data sources, anything helpful.

3. define our target(s) (net / host(s) / protocol)
    1. Target hosts: Network or address of hosts.

4. capture network traffic / read from previously captured PCAP.
    1. Perform actions as needed to analyze the traffic for signs of intrusion.

5. identification of required network traffic components (filtering)
    1. once we have our traffic, filter out any traffic not necessary for this investigation to include; any traffic that matches our common baseline, and keep anything relevant to the scope of the investigation.

6. An understanding of captured network traffic
    1. Once we have filtered out the noise, it's time to dig for our targets. Start broad and close the circle around our scope.

7. note taking / mind mapping of the found results.
    1. Annotating everything we do, see, or find throughout the investigation is crucial. Ensure you are taking ample notes, including:
    - Timeframes we captured traffic during.
    - Suspicious hosts/ports within the network.
    - Conversations containing anything suspicious. (to include timestamps, and packet numbers, files, etc.)

8. summary of the analysis (what did we find?)
    1. Finally, summarize what has been found, explaining the relevant details so that superiors can decide to quarantine the affected hosts or perform a more critical incident response mission.

2. Our analysis will affect decisions made, so it is essential to be as clear and concise as possible.

This task was best completed using the PCAP file provided for the lesson. Following the steps in the workflow, we filled in the information and performed our analysis.

1. what is the issue?
    1. Suspicious traffic coming from within the network.
2. define our scope and the goal (what are we looking for? which time period?)
    1. target: traffic is originating from 10.129.43.4
    2. when: within the last 48 hours. Capture traffic to determine if it is still happening.
    3. supporting info: file: NTA-guided.pcap
3. define our target(s) (net / host(s) / protocol)
    1. scope: 10.129.43.4 and anyone with a connection to it. Unknown protocol over port 4444.
4. capture network traffic
    1. plug into a link with access to the 10.129.43.0/24 network to capture live traffic attempting to see if anything is happening.
    2. We have been given a PCAP with historical data that contains some of the suspect traffic. We will examine this to analyze the issue.
5. identification of required network traffic components (filtering)
    1. First, we will filter out anything that does not have a connection to 10.129.43.4, since this is our primary suspicious target for the moment.

After checking out the conversations plugin pictured above, we can see there are only three conversations captured in this pcap file, and they all pertain to our suspicious host. Next, we will look at the protocol hierarchy plugin to see what our traffic is.

We can see here that this PCAP is mostly TCP traffic, with a bit of UDP traffic. Since there is less UDP than TCP traffic, let us look into that first.

2. Once we have filtered out the noise, it's time to dig for anything unusual. We are going to filter out everything but `UDP traffic first.

When filtering on just UDP traffic, we only see nine packets. Four arp packets, four Network Address Translation NAT, and one Simple Sevice Discovery Protocol SSDP packet. We can determine based on their packet types and information they contain that this traffic is normal network traffic and nothing to be concerned about.

3. Now, let's move on to looking at TCP traffic. We should have quite a bit more here to sift through. We are going to utilize the display filter !udp && !arp. This filter will clear out anything we have already analyzed.

4. Now that we have cleared our view a bit, we can see the remaining packets are all TCP, and all appear to be the same conversation between hosts 10.129.43.4 and 10.129.43.29. We can determine this since we can see the session establishment via a three-way handshake at packet 3, and the same ports are used through the rest of the packets in the output below.

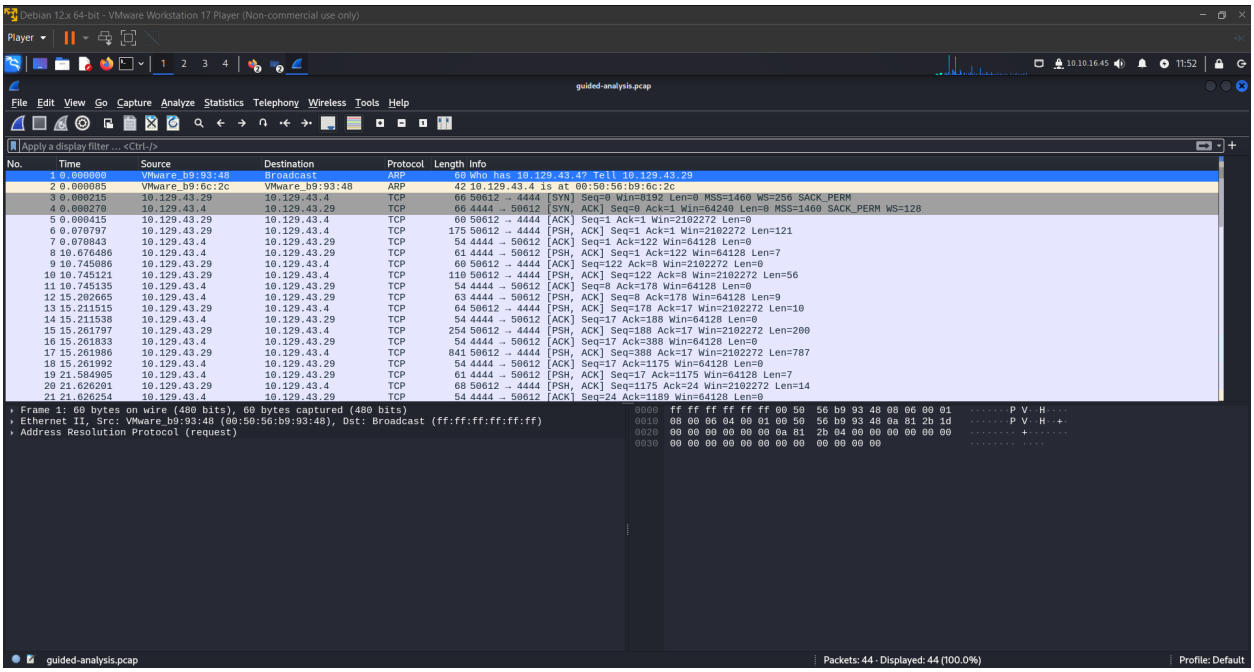
5. What does appear interesting is that we do not see a TCP session teardown in this PCAP file. This could mean the session was still active and not terminated. We believe this to be true since we do not see any Reset packets either.
6. We can also examine the conversation by following the TCP stream from packet 3 to determine what it encompasses.

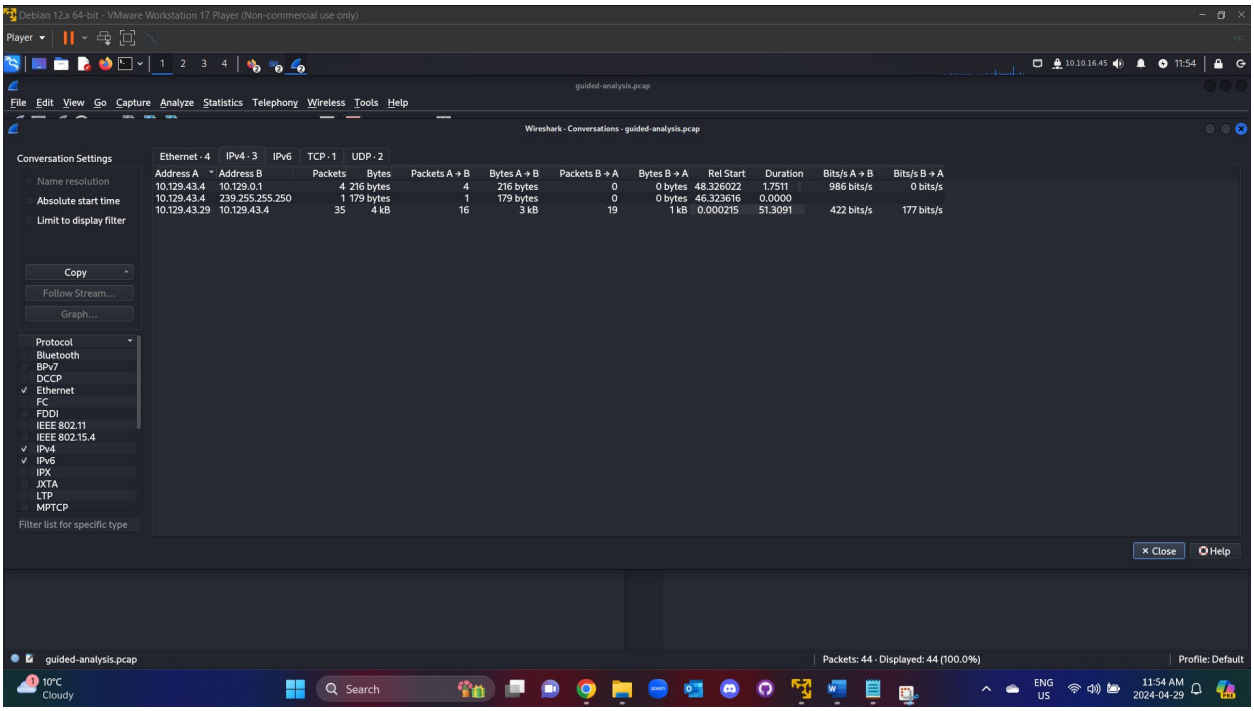
Follow TCP Stream

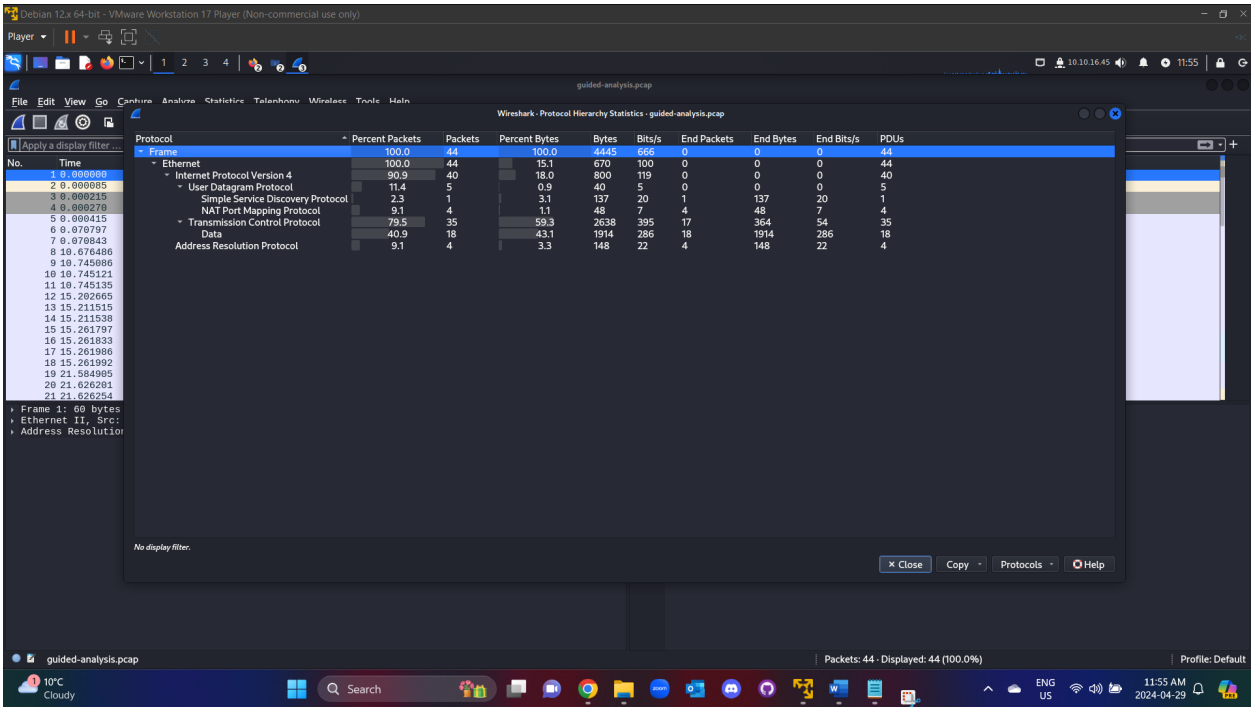
Now that we followed the TCP stream, we should have alarm bells ringing for us. We can see this entire conversation between the two hosts in plain text, and it appears that someone was performing several different actions on the host.

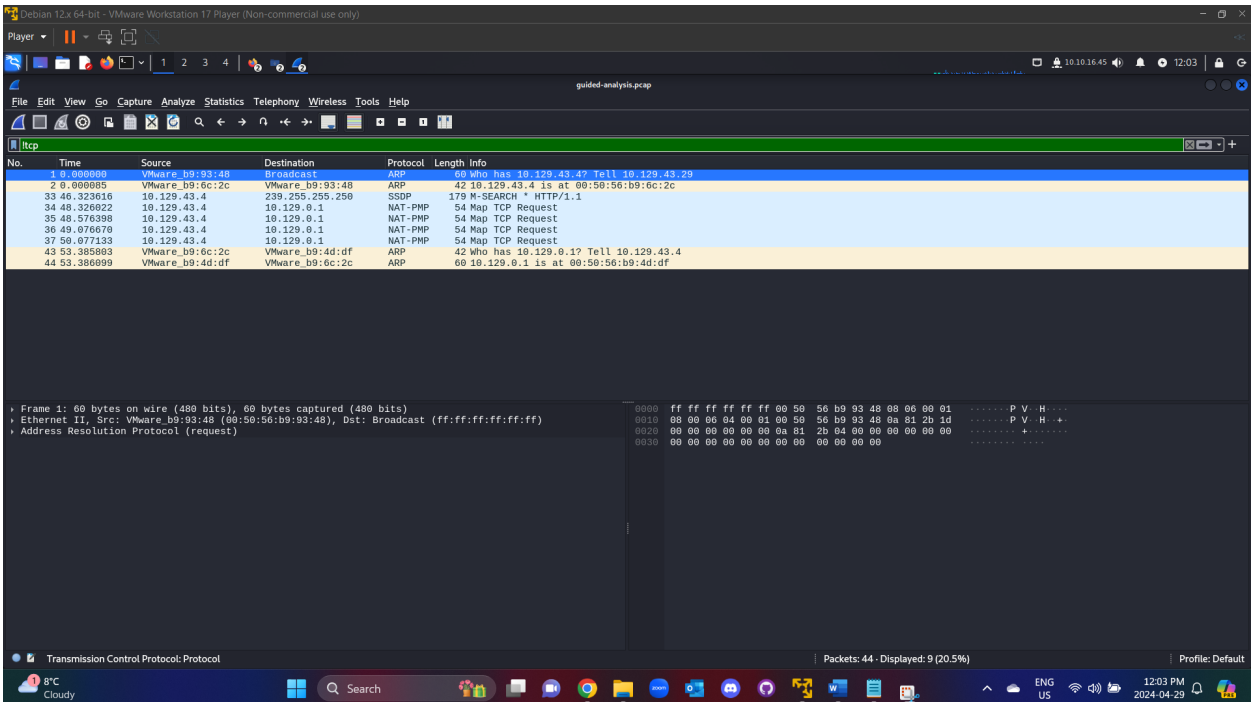
7. Looking at the image above, it appears that someone is performing basic recon of the host. They are issuing commands like whoami, ipconfig, dir. It would appear they are trying to get a lay of the land and figure out what user they landed as on the host. highlighted in orange in the image above.
8. What is truly alarming is that we can now see someone made the account hacker and assigned it to the administrators group on this host. Either this is a joke by a poor administrator. Or someone has infiltrated the corporate infrastructure.
9. note taking / mind mapping of the found results.
    1. Annotating everything we do, see, or find throughout the investigation is crucial. If needed, make a picture to depict the flow of actions.
    2. Using this example workflow, we have already documented our actions and have included screenshots of everything we included for analysis. These will help influence the decision made for a response.
10. summary of the analysis (what did we find?)

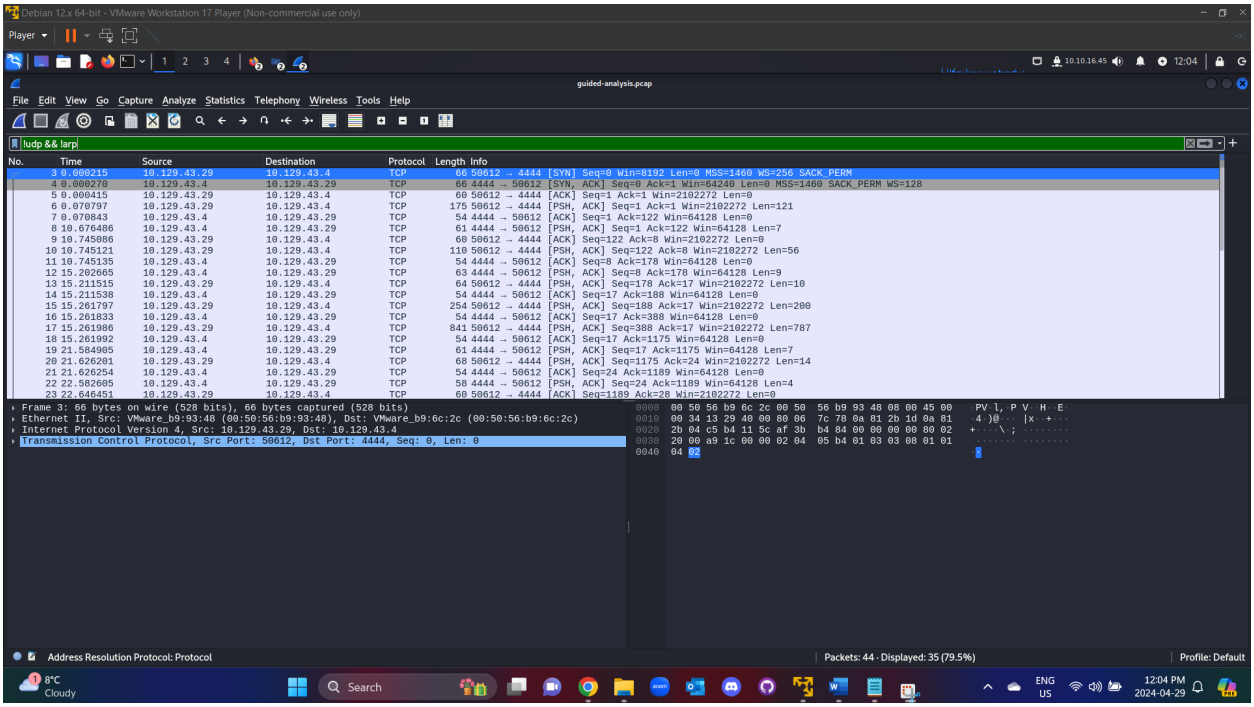
1. Based on our analysis, we determined that a malicious actor has infiltrated at least one host on the network. Host 10.129.43.29 shows signs of someone executing commands to include user creation and assigning local administrator permissions via the net commands. It would look like the actor was using Bob's host to perform said actions. Since Bob was previously under investigation for the exfil of corporate secrets and disguising it as web traffic, I think it is safe to say the issue has spread further. The screenshots included with this document show the flow of traffic and commands utilized.
2. It is our opinion that a complete Incident Response IR procedure be enacted to ensure the threat is stopped from spreading further. We can dedicate resources to clearing the malicious presence and cleaning the affected hosts.

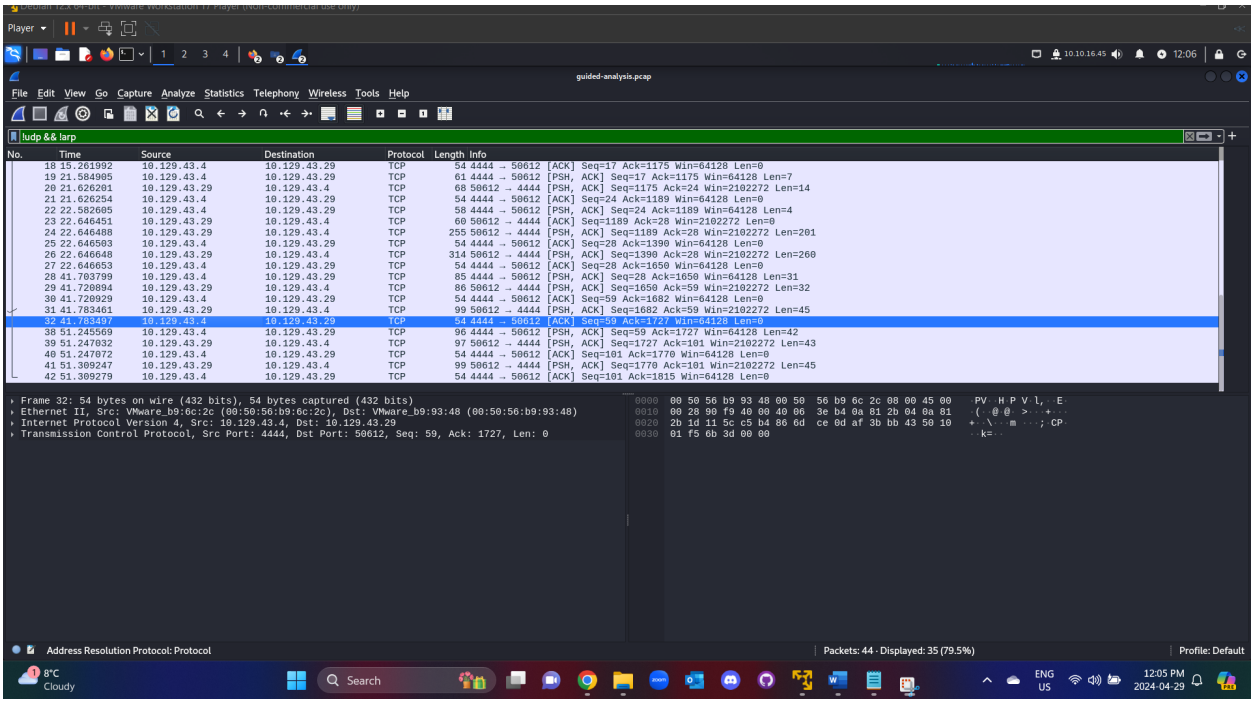


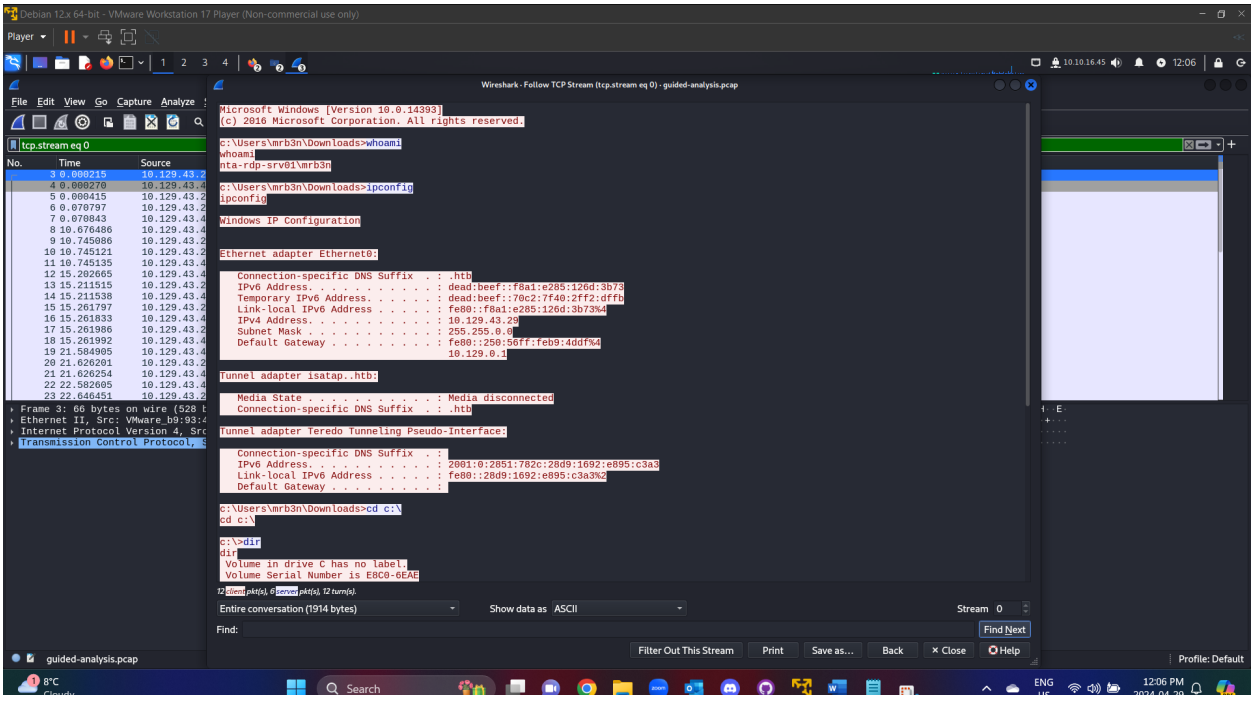

Debian 12.x 64-bit - VMware Workstation 17 Player (Non-commercial use only)
Player
guided-analysis.pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Wireshark · Conversations · guided-analysis.pcap
Conversation Settings
Name resolution
Absolute start time
Limit to display filter
Copy
Follow Stream...
Graph...
Protocol
Bluetooth
BPv7
DCCP
Ethernet
FC
FDDI
IEEE 802.11
IEEE 802.15.4
IPv4
IPv6
IPX
JXTA
LTP
MPTCP
Filter list for specific type
Ethernet · 4
IPv4 · 3
IPv6
TCP · 1
UDP · 2
Address A Address B Packets Bytes Packets A → B Bytes A → B Packets B → A Bytes B → A Rel Start Duration Bits/s A → B Bits/s B → A
10.129.43.4 10.129.0.1 4 216 bytes 4 216 bytes 0 0 bytes 48.326022 1.7511 986 bits/s 0 bits/s
10.129.43.4 239.255.255.250 1 179 bytes 1 179 bytes 0 0 bytes 46.323616 0.0000
10.129.43.29 10.129.43.4 35 4 kB 16 3 kB 19 1 kB 0.000215 51.3091 422 bits/s 177 bits/s
Close
Help
guided-analysis.pcap
Packets: 44 · Displayed: 44 (100.0%)
Profile: Default
10°C Cloudy
Search
ENG US
11:54 AM 2024-04-29

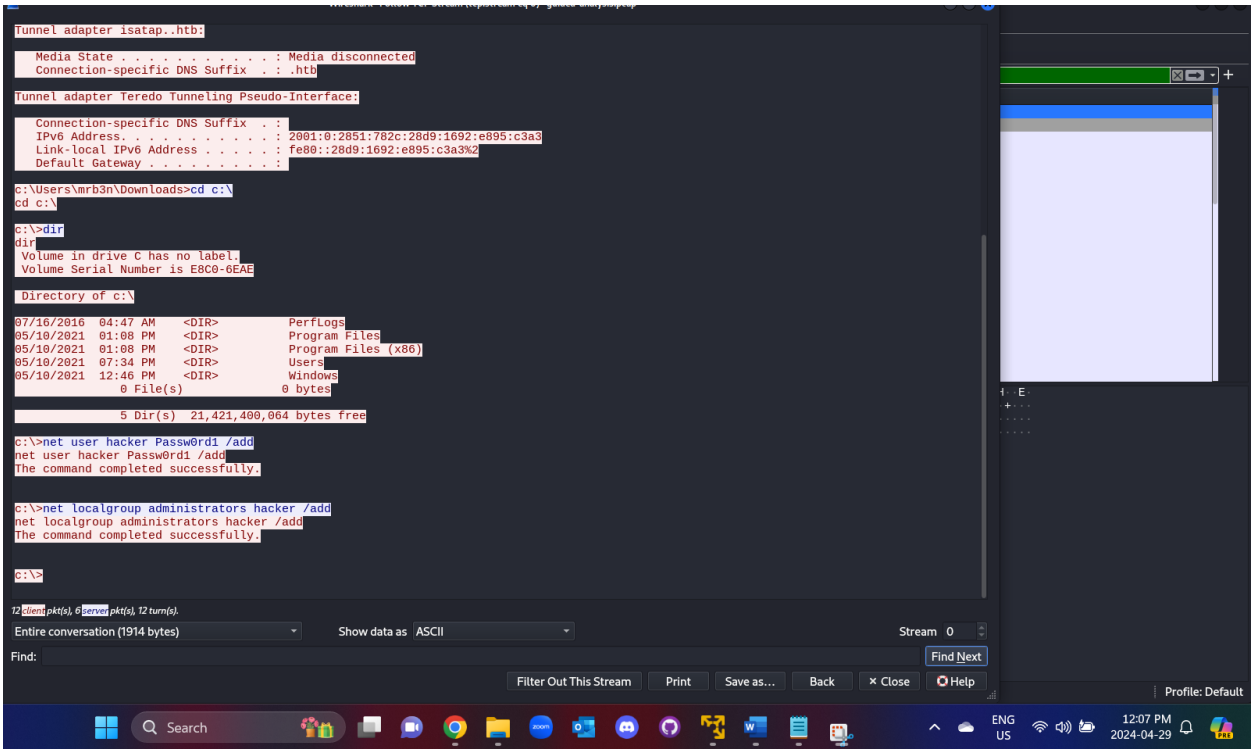

Debian 12.x 64-bit - VMware Workstation 17 Player (Non-commercial use only)
Player
guided-analysis.pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Wireshark · Protocol Hierarchy Statistics · guided-analysis.pcap
Protocol Percent Packets Packets Percent Bytes Bytes Bits/s End Packets End Bytes End Bits/s PDUs
Frame 100.0 44 100.0 4445 666 0 0 0 44
Ethernet 100.0 44 15.1 670 100 0 0 0 44
Internet Protocol Version 4 90.9 40 18.0 800 119 0 0 0 40
User Datagram Protocol 11.4 5 0.9 40 5 0 0 0 5
Simple Service Discovery Protocol 2.3 1 3.1 137 20 1 137 20 1
NAT Port Mapping Protocol 9.1 4 1.1 48 7 4 48 7 4
Transmission Control Protocol 79.5 35 59.3 2638 395 17 364 54 35
Data 40.9 18 43.1 1914 286 18 1914 286 18
Address Resolution Protocol 9.1 4 3.3 148 22 4 148 22 4
No display filter.
Close
Copy
Protocols
Help
No. Time
1 0.000000
2 0.000085
3 0.000215
4 0.000270
5 0.000415
6 0.070797
7 0.070843
8 10.676486
9 10.745086
10 10.745121
11 10.745135
12 15.202665
13 15.211515
14 15.211538
15 15.261797
16 15.261833
17 15.261986
18 15.261992
19 21.584905
20 21.626201
21 21.626254
Frame 1: 60 bytes
Ethernet II, Src:
Address Resolutio
guided-analysis.pcap
Packets: 44 · Displayed: 44 (100.0%)
Profile: Default
10°C Cloudy
Search
ENG US
11:55 AM 2024-04-29


Debian 12.x 64-bit - VMware Workstation 17 Player (Non-commercial use only)
guided-analysis.pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
!tcp
No. Time Source Destination Protocol Length Info
1 0.000000 VMware_b9:93:48 Broadcast ARP 60 Who has 10.129.43.4? Tell 10.129.43.29
2 0.000085 VMware_b9:6c:2c VMware_b9:93:48 ARP 42 10.129.43.4 is at 00:50:56:b9:6c:2c
33 46.323616 10.129.43.4 239.255.255.250 SSDP 179 M-SEARCH * HTTP/1.1
34 48.326022 10.129.43.4 10.129.0.1 NAT-PMP 54 Map TCP Request
35 48.576398 10.129.43.4 10.129.0.1 NAT-PMP 54 Map TCP Request
36 49.076670 10.129.43.4 10.129.0.1 NAT-PMP 54 Map TCP Request
37 50.077133 10.129.43.4 10.129.0.1 NAT-PMP 54 Map TCP Request
43 53.385803 VMware_b9:6c:2c VMware_b9:4d:df ARP 42 Who has 10.129.0.1? Tell 10.129.43.4
44 53.386099 VMware_b9:4d:df VMware_b9:6c:2c ARP 60 10.129.0.1 is at 00:50:56:b9:4d:df
Frame 1: 60 bytes on wire (480 bits), 60 bytes captured (480 bits)
Ethernet II, Src: VMware_b9:93:48 (00:50:56:b9:93:48), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
Address Resolution Protocol (request)
0000 ff ff ff ff ff ff 00 50 56 b9 93 48 08 06 00 01
0010 08 00 06 04 00 01 00 50 56 b9 93 48 0a 81 2b 1d
0020 00 00 00 00 00 00 0a 81 2b 04 00 00 00 00 00 00
0030 00 00 00 00 00 00 00 00 00 00 00 00
Transmission Control Protocol: Protocol
Packets: 44 · Displayed: 9 (20.5%)
Profile: Default
8°C Cloudy
Search
ENG US
12:03 PM 2024-04-29


Debian 12.x 64-bit - VMware Workstation 17 Player (Non-commercial use only)
guided-analysis.pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
!udp && !arp
No. Time Source Destination Protocol Length Info
3 0.000215 10.129.43.29 10.129.43.4 TCP 66 50612 → 4444 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM
4 0.000270 10.129.43.4 10.129.43.29 TCP 66 4444 → 50612 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460 SACK_PERM WS=128
5 0.000415 10.129.43.29 10.129.43.4 TCP 60 50612 → 4444 [ACK] Seq=1 Ack=1 Win=2102272 Len=0
6 0.070797 10.129.43.29 10.129.43.4 TCP 175 50612 → 4444 [PSH, ACK] Seq=1 Ack=1 Win=2102272 Len=121
7 0.070843 10.129.43.4 10.129.43.29 TCP 54 4444 → 50612 [ACK] Seq=1 Ack=122 Win=64128 Len=0
8 10.676486 10.129.43.4 10.129.43.29 TCP 61 4444 → 50612 [PSH, ACK] Seq=1 Ack=122 Win=64128 Len=7
9 10.745086 10.129.43.29 10.129.43.4 TCP 60 50612 → 4444 [ACK] Seq=122 Ack=8 Win=2102272 Len=0
10 10.745121 10.129.43.29 10.129.43.4 TCP 110 50612 → 4444 [PSH, ACK] Seq=122 Ack=8 Win=2102272 Len=56
11 10.745135 10.129.43.4 10.129.43.29 TCP 54 4444 → 50612 [ACK] Seq=8 Ack=178 Win=64128 Len=0
12 15.202665 10.129.43.4 10.129.43.29 TCP 63 4444 → 50612 [PSH, ACK] Seq=8 Ack=178 Win=64128 Len=9
13 15.211515 10.129.43.29 10.129.43.4 TCP 64 50612 → 4444 [PSH, ACK] Seq=178 Ack=17 Win=2102272 Len=10
14 15.211538 10.129.43.4 10.129.43.29 TCP 54 4444 → 50612 [ACK] Seq=17 Ack=188 Win=64128 Len=0
15 15.261797 10.129.43.29 10.129.43.4 TCP 254 50612 → 4444 [PSH, ACK] Seq=188 Ack=17 Win=2102272 Len=200
16 15.261833 10.129.43.4 10.129.43.29 TCP 54 4444 → 50612 [ACK] Seq=17 Ack=388 Win=64128 Len=0
17 15.261986 10.129.43.29 10.129.43.4 TCP 841 50612 → 4444 [PSH, ACK] Seq=388 Ack=17 Win=2102272 Len=787
18 15.261992 10.129.43.4 10.129.43.29 TCP 54 4444 → 50612 [ACK] Seq=17 Ack=1175 Win=64128 Len=0
19 21.584905 10.129.43.4 10.129.43.29 TCP 61 4444 → 50612 [PSH, ACK] Seq=17 Ack=1175 Win=64128 Len=7
20 21.626201 10.129.43.29 10.129.43.4 TCP 68 50612 → 4444 [PSH, ACK] Seq=1175 Ack=24 Win=2102272 Len=14
21 21.626254 10.129.43.4 10.129.43.29 TCP 54 4444 → 50612 [ACK] Seq=24 Ack=1189 Win=64128 Len=0
22 22.582605 10.129.43.4 10.129.43.29 TCP 58 4444 → 50612 [PSH, ACK] Seq=24 Ack=1189 Win=64128 Len=4
23 22.646451 10.129.43.29 10.129.43.4 TCP 60 50612 → 4444 [ACK] Seq=1189 Ack=28 Win=2102272 Len=0
Frame 3: 66 bytes on wire (528 bits), 66 bytes captured (528 bits)
Ethernet II, Src: VMware_b9:93:48 (00:50:56:b9:93:48), Dst: VMware_b9:6c:2c (00:50:56:b9:6c:2c)
Internet Protocol Version 4, Src: 10.129.43.29, Dst: 10.129.43.4
Transmission Control Protocol, Src Port: 50612, Dst Port: 4444, Seq: 0, Len: 0
0000 00 50 56 b9 6c 2c 00 50 56 b9 93 48 08 00 45 00
0010 00 34 13 29 40 00 80 06 7c 78 0a 81 2b 1d 0a 81
0020 2b 04 c5 b4 11 5c af 3b b4 84 00 00 00 00 80 02
0030 20 00 a9 1c 00 00 02 04 05 b4 01 03 03 08 01 01
0040 04 02
Address Resolution Protocol: Protocol
Packets: 44 · Displayed: 35 (79.5%)
Profile: Default
8°C Cloudy
Search
ENG US
12:04 PM 2024-04-29


guided-analysis.pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
!udp && !arp
No. Time Source Destination Protocol Length Info
18 15.261992 10.129.43.4 10.129.43.29 TCP 54 4444 → 50612 [ACK] Seq=17 Ack=1175 Win=64128 Len=0
19 21.584905 10.129.43.4 10.129.43.29 TCP 61 4444 → 50612 [PSH, ACK] Seq=17 Ack=1175 Win=64128 Len=7
20 21.626201 10.129.43.29 10.129.43.4 TCP 68 50612 → 4444 [PSH, ACK] Seq=1175 Ack=24 Win=2102272 Len=14
21 21.626254 10.129.43.4 10.129.43.29 TCP 54 4444 → 50612 [ACK] Seq=24 Ack=1189 Win=64128 Len=0
22 22.582605 10.129.43.4 10.129.43.29 TCP 58 4444 → 50612 [PSH, ACK] Seq=24 Ack=1189 Win=64128 Len=4
23 22.646451 10.129.43.29 10.129.43.4 TCP 60 50612 → 4444 [ACK] Seq=1189 Ack=28 Win=2102272 Len=0
24 22.646488 10.129.43.29 10.129.43.4 TCP 255 50612 → 4444 [PSH, ACK] Seq=1189 Ack=28 Win=2102272 Len=201
25 22.646503 10.129.43.4 10.129.43.29 TCP 54 4444 → 50612 [ACK] Seq=28 Ack=1390 Win=64128 Len=0
26 22.646648 10.129.43.29 10.129.43.4 TCP 314 50612 → 4444 [PSH, ACK] Seq=1390 Ack=28 Win=2102272 Len=260
27 22.646653 10.129.43.4 10.129.43.29 TCP 54 4444 → 50612 [ACK] Seq=28 Ack=1650 Win=64128 Len=0
28 41.703799 10.129.43.4 10.129.43.29 TCP 85 4444 → 50612 [PSH, ACK] Seq=28 Ack=1650 Win=64128 Len=31
29 41.720894 10.129.43.29 10.129.43.4 TCP 86 50612 → 4444 [PSH, ACK] Seq=1650 Ack=59 Win=2102272 Len=32
30 41.720929 10.129.43.4 10.129.43.29 TCP 54 4444 → 50612 [ACK] Seq=59 Ack=1682 Win=64128 Len=0
31 41.783461 10.129.43.29 10.129.43.4 TCP 99 50612 → 4444 [PSH, ACK] Seq=1682 Ack=59 Win=2102272 Len=45
32 41.783497 10.129.43.4 10.129.43.29 TCP 54 4444 → 50612 [ACK] Seq=59 Ack=1727 Win=64128 Len=0
38 51.245569 10.129.43.4 10.129.43.29 TCP 96 4444 → 50612 [PSH, ACK] Seq=59 Ack=1727 Win=64128 Len=42
39 51.247032 10.129.43.29 10.129.43.4 TCP 97 50612 → 4444 [PSH, ACK] Seq=1727 Ack=101 Win=2102272 Len=43
40 51.247072 10.129.43.4 10.129.43.29 TCP 54 4444 → 50612 [ACK] Seq=101 Ack=1770 Win=64128 Len=0
41 51.309247 10.129.43.29 10.129.43.4 TCP 99 50612 → 4444 [PSH, ACK] Seq=1770 Ack=101 Win=2102272 Len=45
42 51.309279 10.129.43.4 10.129.43.29 TCP 54 4444 → 50612 [ACK] Seq=101 Ack=1815 Win=64128 Len=0
Frame 32: 54 bytes on wire (432 bits), 54 bytes captured (432 bits)
Ethernet II, Src: VMware_b9:6c:2c (00:50:56:b9:6c:2c), Dst: VMware_b9:93:48 (00:50:56:b9:93:48)
Internet Protocol Version 4, Src: 10.129.43.4, Dst: 10.129.43.29
Transmission Control Protocol, Src Port: 4444, Dst Port: 50612, Seq: 59, Ack: 1727, Len: 0
0000 00 50 56 b9 93 48 00 50 56 b9 6c 2c 08 00 45 00
0010 00 28 90 f9 40 00 40 06 3e b4 0a 81 2b 04 0a 81
0020 2b 1d 11 5c c5 b4 86 6d ce 0d af 3b bb 43 50 10
0030 01 f5 6b 3d 00 00
Address Resolution Protocol: Protocol
Packets: 44 · Displayed: 35 (79.5%)
Profile: Default
8°C Cloudy
Search
ENG US
12:05 PM 2024-04-29

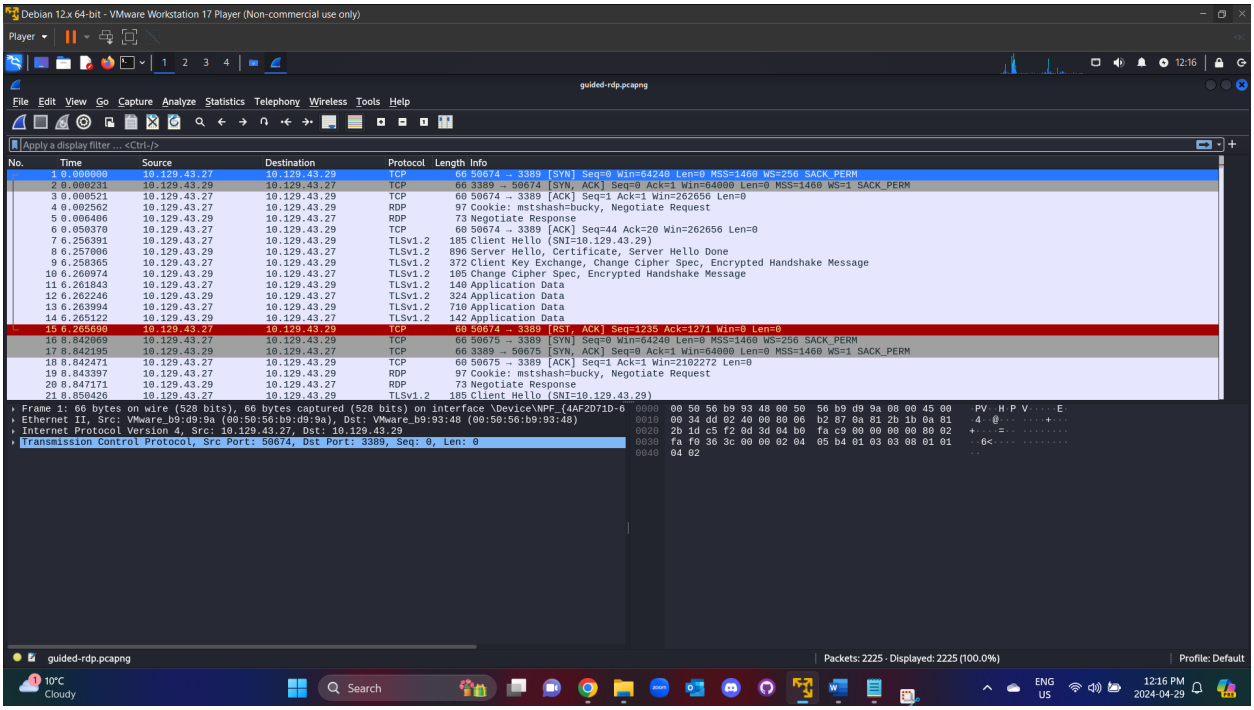

Debian 12.x 64-bit - VMware Workstation 17 Player (Non-commercial use only)
Wireshark · Follow TCP Stream (tcp.stream eq 0) · guided-analysis.pcap
Microsoft Windows [Version 10.0.14393]
(c) 2016 Microsoft Corporation. All rights reserved.
C:\Users\mrb3n\Downloads>whoami
whoami
nta-rdp-srv01\mrb3n
C:\Users\mrb3n\Downloads>ipconfig
ipconfig
Windows IP Configuration
Ethernet adapter Ethernet0:
Connection-specific DNS Suffix . : .htb
IPv6 Address. . . . . : dead:beef::f8a1:e285:126d:3b73
Temporary IPv6 Address. . . . . : dead:beef::70c2:7f40:2ff2:dffb
Link-local IPv6 Address . . . . . : fe80::f8a1:e285:126d:3b73%4
IPv4 Address. . . . . : 10.129.43.29
Subnet Mask . . . . . : 255.255.0.0
Default Gateway . . . . . : fe80::250:56ff:feb9:4ddf%4
10.129.0.1
Tunnel adapter isatap..htb:
Media State . . . . . : Media disconnected
Connection-specific DNS Suffix . : .htb
Tunnel adapter Teredo Tunneling Pseudo-Interface:
Connection-specific DNS Suffix . :
IPv6 Address. . . . . : 2001:0:2851:782c:28d9:1692:e895:c3a3
Link-local IPv6 Address . . . . . : fe80::28d9:1692:e895:c3a3%2
Default Gateway . . . . . :
C:\Users\mrb3n\Downloads>cd c:\
cd c:\
C:\>dir
dir
Volume in drive C has no label.
Volume Serial Number is E8C0-6EAE
Entire conversation (1914 bytes)
Show data as ASCII
Stream 0
Find:
Find Next
Filter Out This Stream
Print
Save as...
Back
Close
Help
guided-analysis.pcap
Profile: Default
8°C
Search
ENG
12:06 PM


Tunnel adapter isatap..htb:
Media State . . . . . : Media disconnected
Connection-specific DNS Suffix . : .htb
Tunnel adapter Teredo Tunneling Pseudo-Interface:
Connection-specific DNS Suffix . :
IPv6 Address. . . . . : 2001:0:2851:782c:28d9:1692:e895:c3a3
Link-local IPv6 Address . . . . . : fe80::28d9:1692:e895:c3a3%2
Default Gateway . . . . . :
c:\Users\mrb3n\Downloads>cd c:\
cd c:\
c:\>dir
dir
Volume in drive C has no label.
Volume Serial Number is E8C0-6EAE
Directory of c:\
07/16/2016 04:47 AM <DIR> PerfLogs
05/10/2021 01:08 PM <DIR> Program Files
05/10/2021 01:08 PM <DIR> Program Files (x86)
05/10/2021 07:34 PM <DIR> Users
05/10/2021 12:46 PM <DIR> Windows
0 File(s) 0 bytes
5 Dir(s) 21,421,400,064 bytes free
c:\>net user hacker Passw0rd1 /add
net user hacker Passw0rd1 /add
The command completed successfully.
c:\>net localgroup administrators hacker /add
net localgroup administrators hacker /add
The command completed successfully.
c:\>
12 client pkt(s), 6 server pkt(s), 12 turn(s).
Entire conversation (1914 bytes)
Show data as ASCII
Stream 0
Find:
Find Next
Filter Out This Stream
Print
Save as...
Back
Close
Help
Profile: Default
Search
ENG
US
12:07 PM
2024-04-29

Decrypting RDP connections

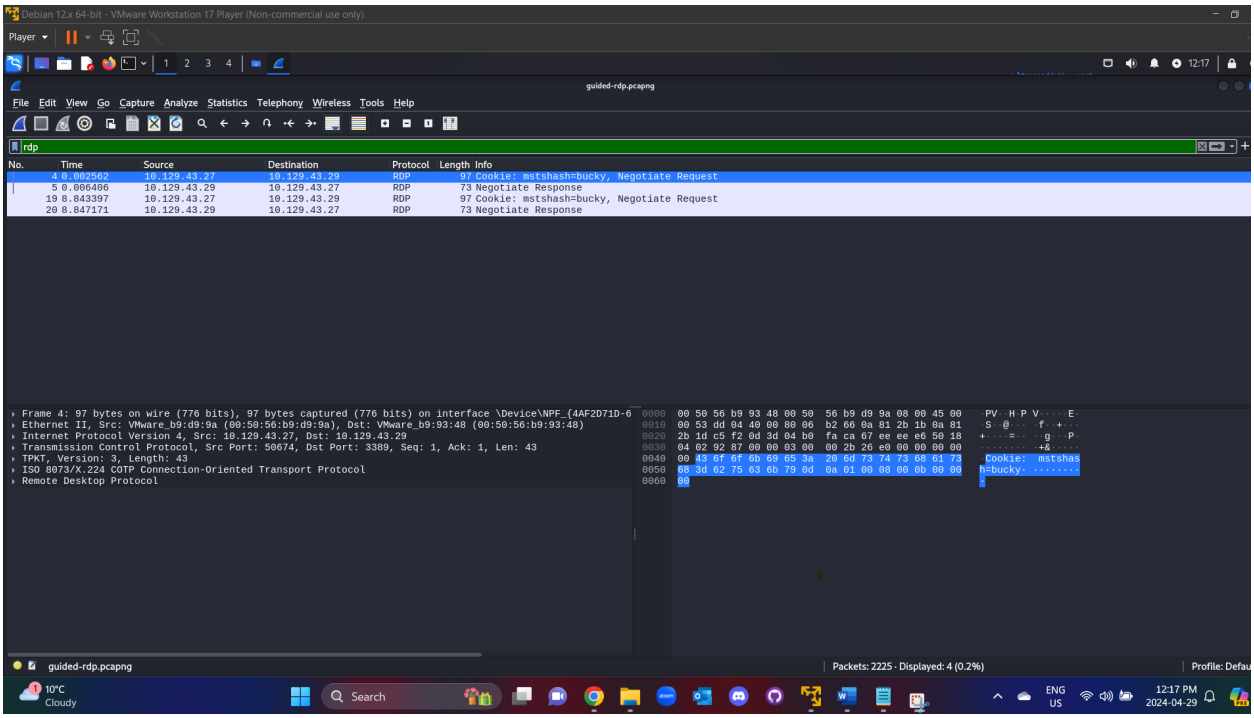
Task #1

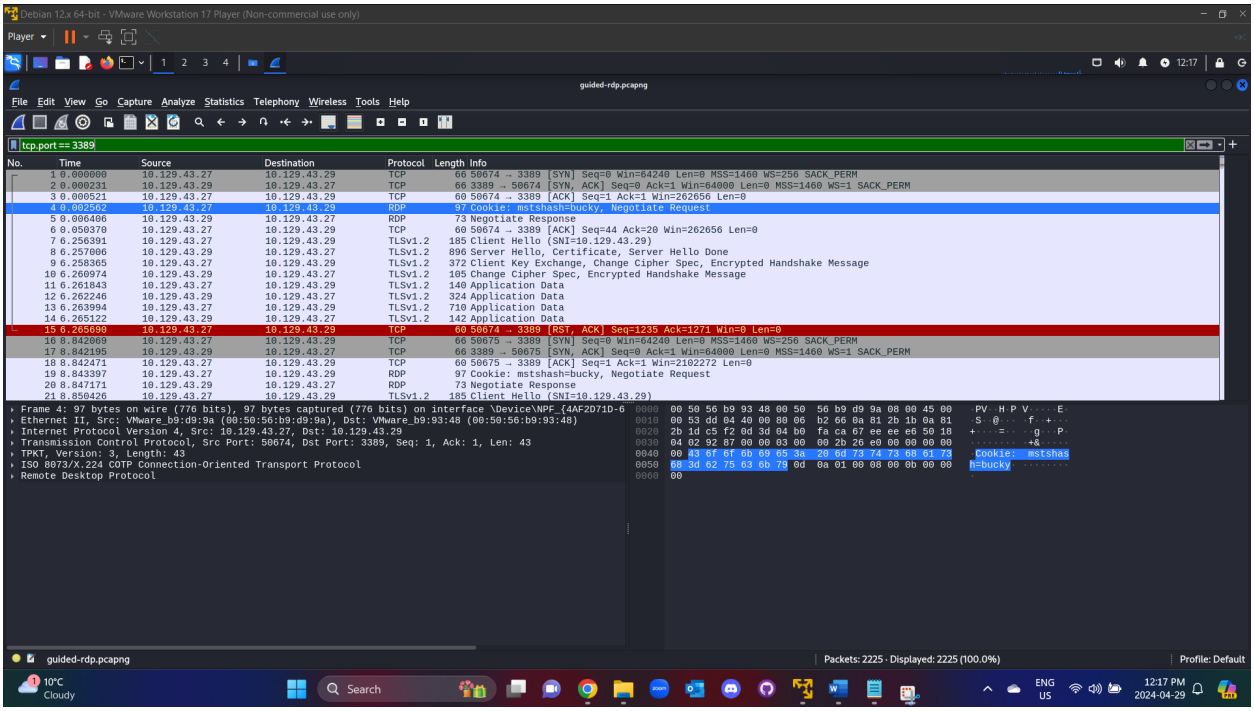
Open the rdp.pcapng file in Wireshark.

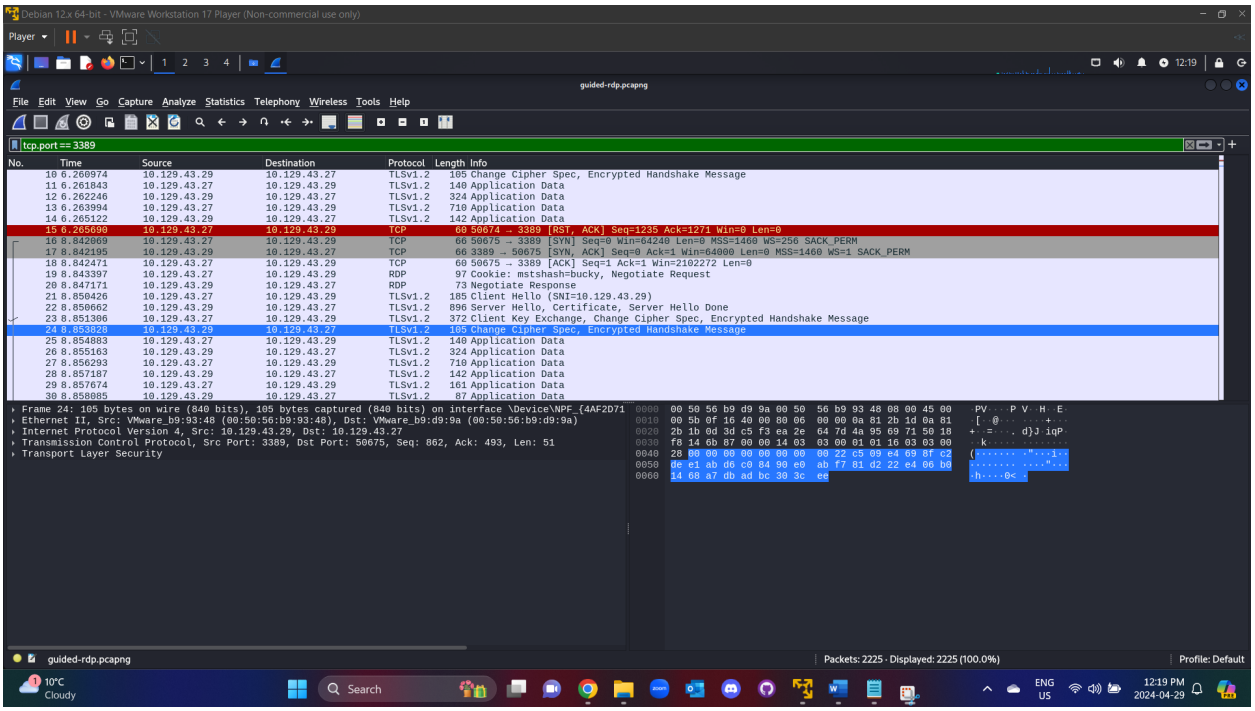


Task #2

Analyze the traffic included.

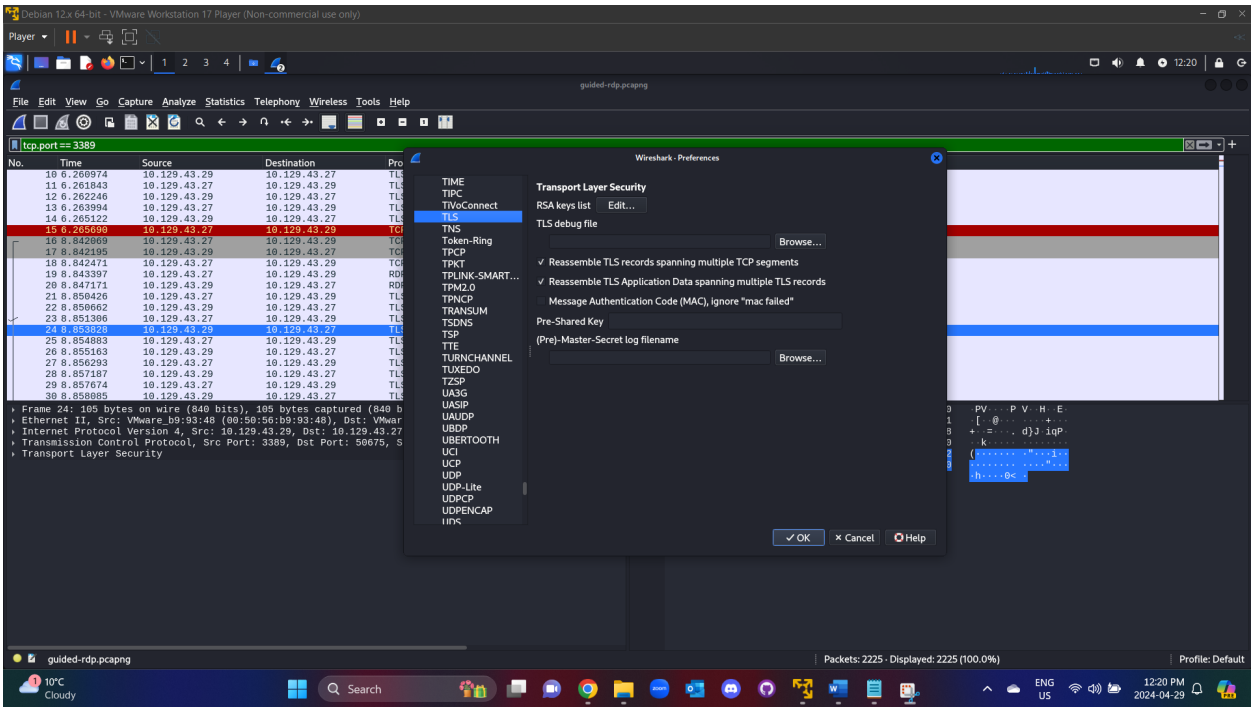

Debian 12.x 64-bit - VMware Workstation 17 Player (Non-commercial use only)
guided-rdp.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
rdp
No. Time Source Destination Protocol Length Info
4 0.002562 10.129.43.27 10.129.43.29 RDP 97 Cookie: mstshash=bucky, Negotiate Request
5 0.006406 10.129.43.29 10.129.43.27 RDP 73 Negotiate Response
19 8.843397 10.129.43.27 10.129.43.29 RDP 97 Cookie: mstshash=bucky, Negotiate Request
20 8.847171 10.129.43.29 10.129.43.27 RDP 73 Negotiate Response
Frame 4: 97 bytes on wire (776 bits), 97 bytes captured (776 bits) on interface \Device\NPF_{4AF2D71D-6
Ethernet II, Src: VMware_b9:d9:9a (00:50:56:b9:d9:9a), Dst: VMware_b9:93:48 (00:50:56:b9:93:48)
Internet Protocol Version 4, Src: 10.129.43.27, Dst: 10.129.43.29
Transmission Control Protocol, Src Port: 50674, Dst Port: 3389, Seq: 1, Ack: 1, Len: 43
TPKT, Version: 3, Length: 43
ISO 8073/X.224 COTP Connection-Oriented Transport Protocol
Remote Desktop Protocol
0000 00 50 56 b9 93 48 00 50 56 b9 d9 9a 08 00 45 00
0010 00 53 dd 04 40 00 80 06 b2 66 0a 81 2b 1b 0a 81
0020 2b 1d c5 f2 0d 3d 04 b0 fa ca 67 ee ee e6 50 18
0030 04 02 92 87 00 00 03 00 00 2b 26 e0 00 00 00 00
0040 00 43 6f 6f 6b 69 65 3a 20 6d 73 74 73 68 61 73
0050 68 3d 62 75 63 6b 79 0d 0a 01 00 08 00 0b 00 00
0060 00
guided-rdp.pcapng
Packets: 2225 · Displayed: 4 (0.2%)
Profile: Defau
10°C Cloudy
Search
ENG US
12:17 PM 2024-04-29

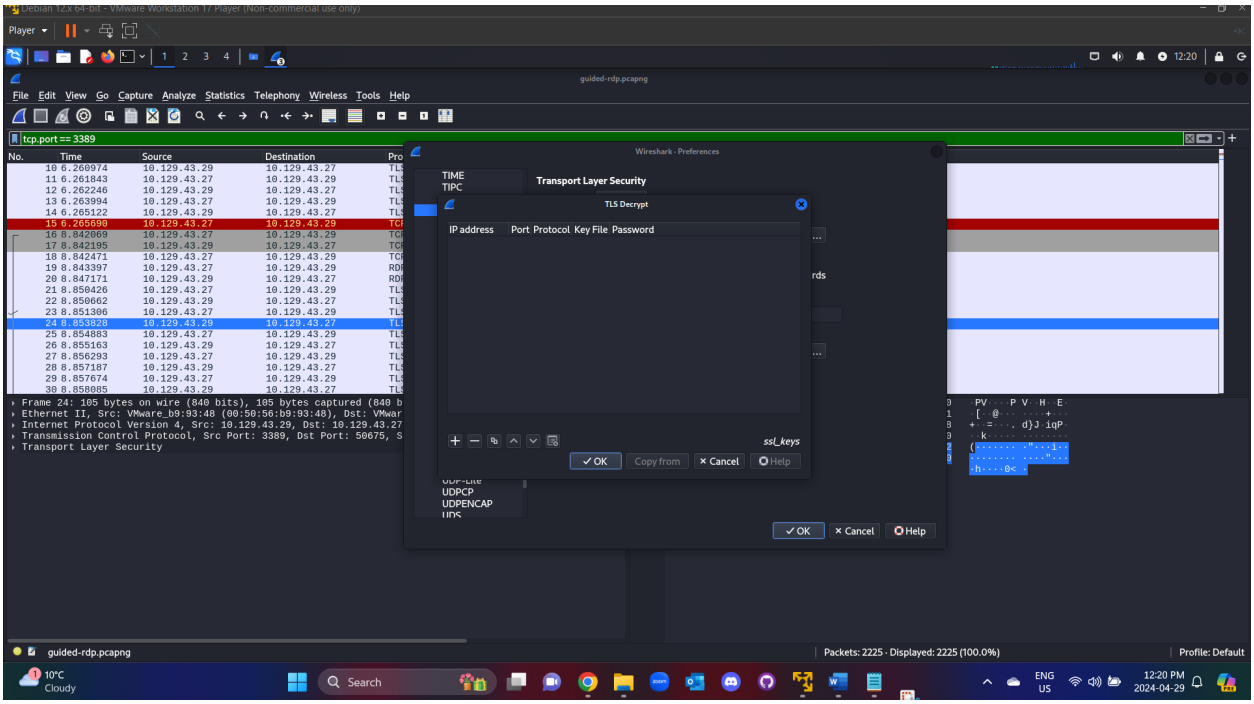

Debian 12.x 64-bit - VMware Workstation 17 Player (Non-commercial use only)
guided-rdp.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
tcp.port == 3389
No. Time Source Destination Protocol Length Info
1 0.000000 10.129.43.27 10.129.43.29 TCP 66 50674 → 3389 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
2 0.000231 10.129.43.29 10.129.43.27 TCP 66 3389 → 50674 [SYN, ACK] Seq=0 Ack=1 Win=64000 Len=0 MSS=1460 WS=1 SACK_PERM
3 0.000521 10.129.43.27 10.129.43.29 TCP 60 50674 → 3389 [ACK] Seq=1 Ack=1 Win=262656 Len=0
4 0.002562 10.129.43.27 10.129.43.29 RDP 97 Cookie: mstshash=bucky, Negotiate Request
5 0.006406 10.129.43.29 10.129.43.27 RDP 73 Negotiate Response
6 0.050370 10.129.43.27 10.129.43.29 TCP 60 50674 → 3389 [ACK] Seq=44 Ack=20 Win=262656 Len=0
7 6.256391 10.129.43.27 10.129.43.29 TLSv1.2 185 Client Hello (SNI=10.129.43.29)
8 6.257006 10.129.43.29 10.129.43.27 TLSv1.2 896 Server Hello, Certificate, Server Hello Done
9 6.258365 10.129.43.27 10.129.43.29 TLSv1.2 372 Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
10 6.260974 10.129.43.29 10.129.43.27 TLSv1.2 105 Change Cipher Spec, Encrypted Handshake Message
11 6.261843 10.129.43.27 10.129.43.29 TLSv1.2 140 Application Data
12 6.262246 10.129.43.29 10.129.43.27 TLSv1.2 324 Application Data
13 6.263994 10.129.43.27 10.129.43.29 TLSv1.2 710 Application Data
14 6.265122 10.129.43.29 10.129.43.27 TLSv1.2 142 Application Data
15 6.265690 10.129.43.27 10.129.43.29 TCP 60 50674 → 3389 [RST, ACK] Seq=1235 Ack=1271 Win=0 Len=0
16 8.842069 10.129.43.27 10.129.43.29 TCP 66 50675 → 3389 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
17 8.842195 10.129.43.29 10.129.43.27 TCP 66 3389 → 50675 [SYN, ACK] Seq=0 Ack=1 Win=64000 Len=0 MSS=1460 WS=1 SACK_PERM
18 8.842471 10.129.43.27 10.129.43.29 TCP 60 50675 → 3389 [ACK] Seq=1 Ack=1 Win=2102272 Len=0
19 8.843397 10.129.43.27 10.129.43.29 RDP 97 Cookie: mstshash=bucky, Negotiate Request
20 8.847171 10.129.43.29 10.129.43.27 RDP 73 Negotiate Response
21 8.850426 10.129.43.27 10.129.43.29 TLSv1.2 185 Client Hello (SNI=10.129.43.29)
Frame 4: 97 bytes on wire (776 bits), 97 bytes captured (776 bits) on interface \Device\NPF_{4AF2D71D-6
Ethernet II, Src: VMware_b9:d9:9a (00:50:56:b9:d9:9a), Dst: VMware_b9:93:48 (00:50:56:b9:93:48)
Internet Protocol Version 4, Src: 10.129.43.27, Dst: 10.129.43.29
Transmission Control Protocol, Src Port: 50674, Dst Port: 3389, Seq: 1, Ack: 1, Len: 43
TPKT, Version: 3, Length: 43
ISO 8073/X.224 COTP Connection-Oriented Transport Protocol
Remote Desktop Protocol
0000 00 50 56 b9 93 48 00 50 56 b9 d9 9a 08 00 45 00
0010 00 53 dd 04 40 00 80 06 b2 66 0a 81 2b 1b 0a 81
0020 2b 1d c5 f2 0d 3d 04 b0 fa ca 67 ee ee e6 50 18
0030 04 02 92 87 00 00 03 00 00 2b 26 e0 00 00 00 00
0040 00 43 6f 6f 6b 69 65 3a 20 6d 73 74 73 68 61 73
0050 68 3d 62 75 63 6b 79 0d 0a 01 00 08 00 0b 00 00
0060 00
guided-rdp.pcapng
Packets: 2225 · Displayed: 2225 (100.0%)
Profile: Default
10°C Cloudy
Search
ENG US
12:17 PM 2024-04-29



Task #3

Provide the RDP-key to Wireshark so it can decrypt the traffic.


Debian 12.x 64-bit - VMware Workstation 17 Player (Non-commercial use only)
guided-rdp.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
tcp.port == 3389
Wireshark - Preferences
Transport Layer Security
RSA keys list
Edit...
TLS debug file
Browse...
Reassemble TLS records spanning multiple TCP segments
Reassemble TLS Application Data spanning multiple TLS records
Message Authentication Code (MAC), ignore "mac failed"
Pre-Shared Key
(Pre)-Master-Secret log filename
OK
Cancel
Help
Packets: 2225 · Displayed: 2225 (100.0%)
Profile: Default
10°C
Cloudy
Search
ENG
US
12:20 PM
2024-04-29


Debian 12.x 64-bit - VMware Workstation 17 Player (Non-commercial use only)
guided-rdp.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
tcp.port == 3389
Wireshark - Preferences
Transport Layer Security
TLS Decrypt
IP address
Port
Protocol
Key File
Password
ssl_keys
OK
Copy from
Cancel
Help
Packets: 2225 · Displayed: 2225 (100.0%)
Profile: Default
10°C
Cloudy
Search
ENG
US
12:20 PM
2024-04-29

Import An RDP Key

Steps

Click the + to add a new key

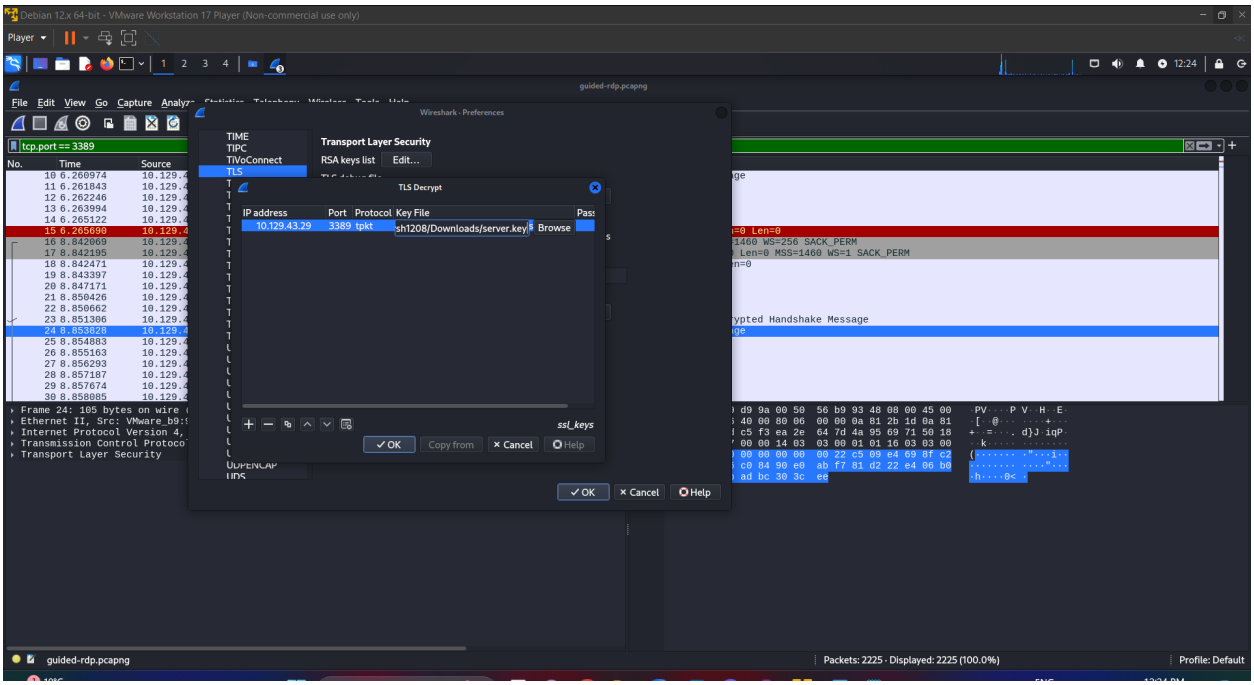
Type in the IP address of the RDP server `10.129.43.29`

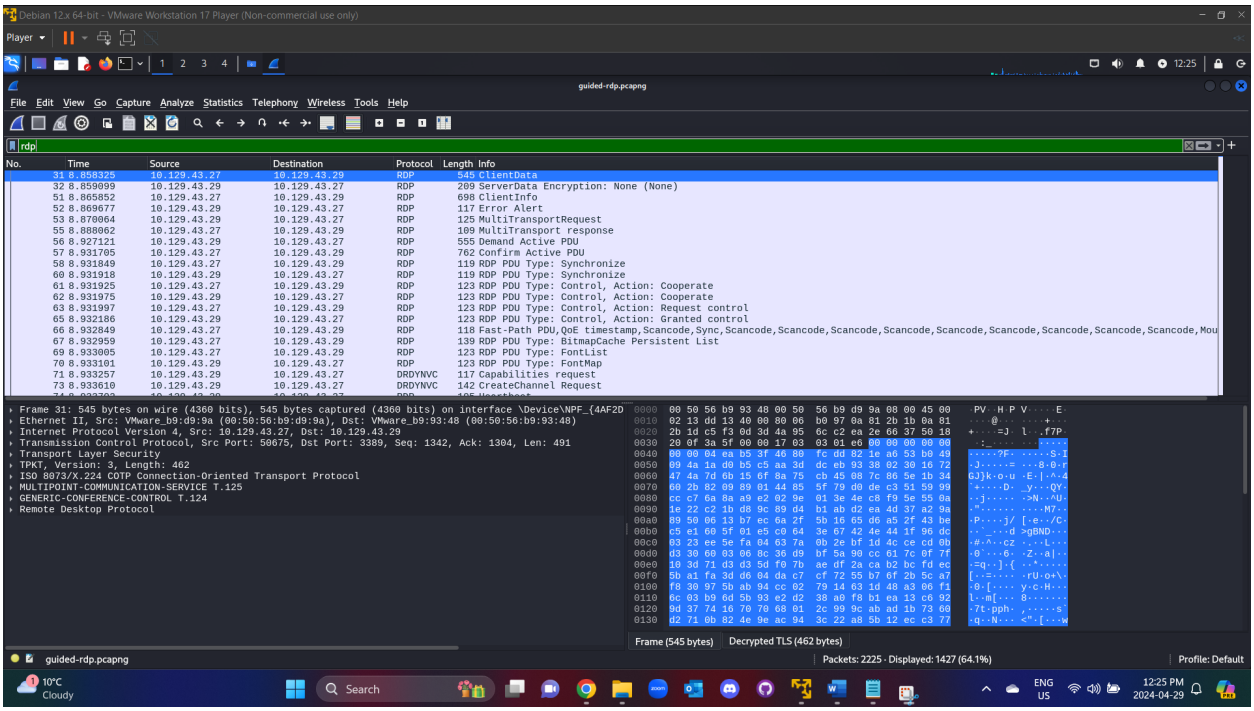
Type in the port used `3389`

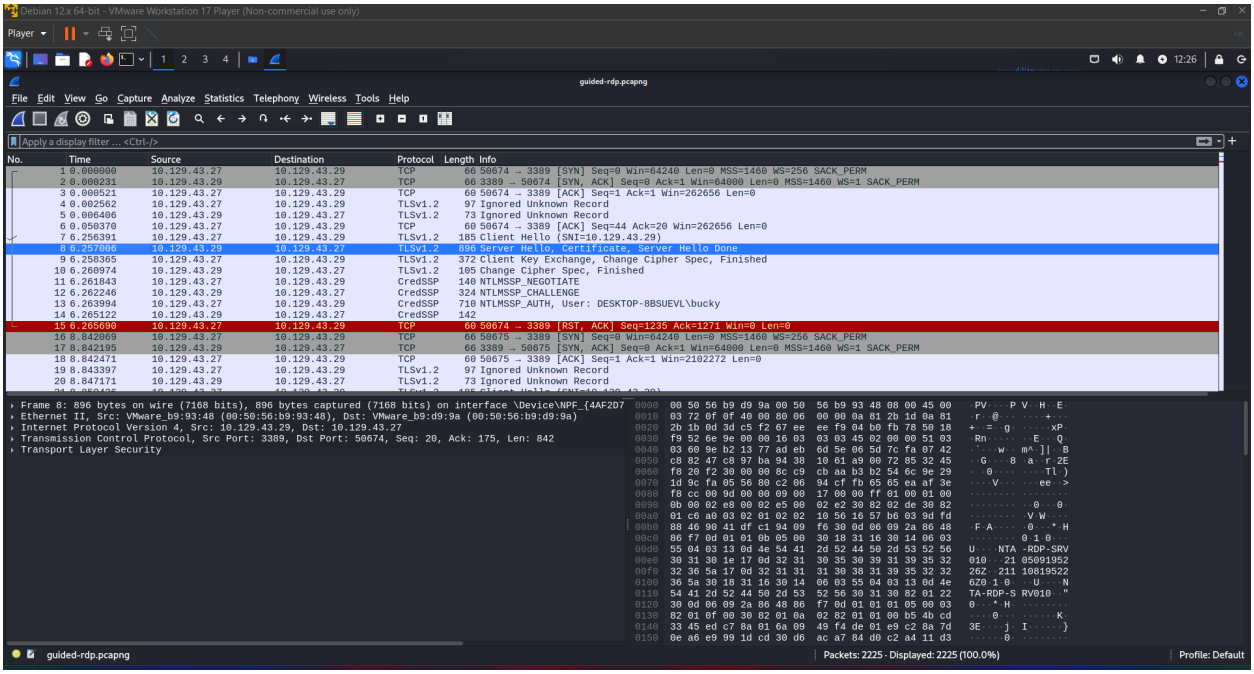
Protocol filed equals `tpkt` or `blank`.

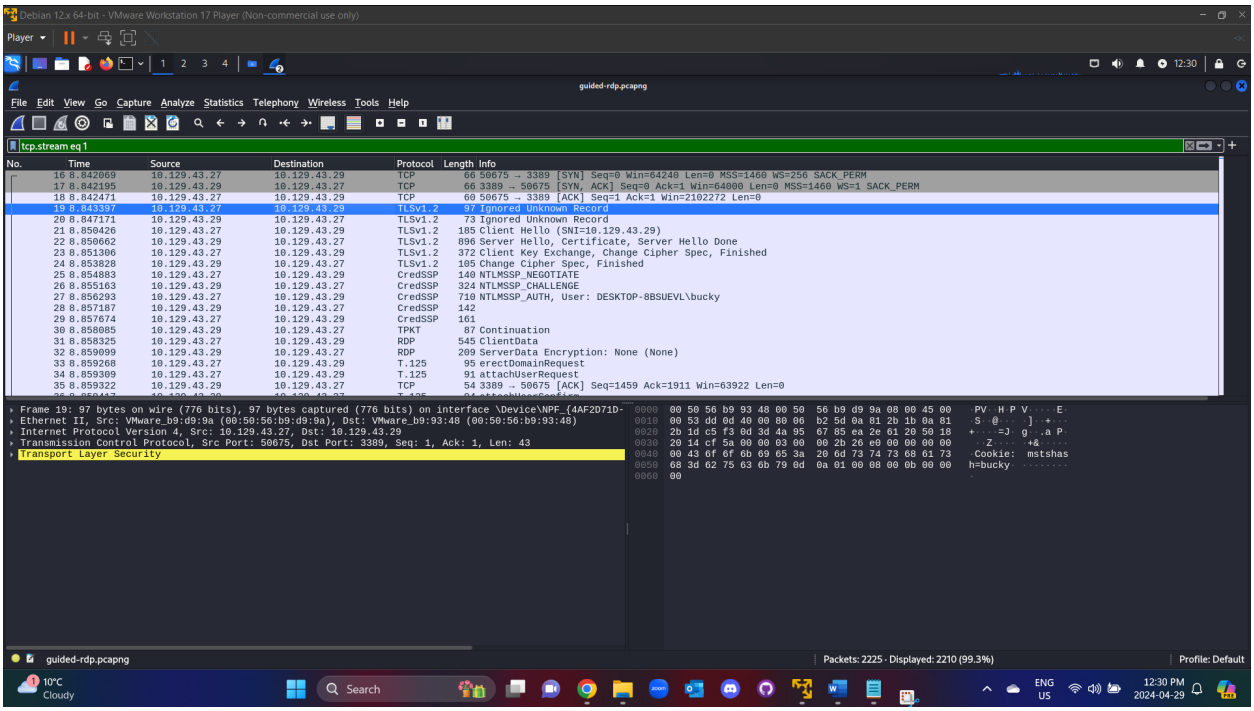
Browse to the `server.key` file and add it in the key file section.

Save and refresh your pcap file.




Debian 12.x 64-bit - VMware Workstation 17 Player (Non-commercial use only)
guided-rdp.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
rdp
No. Time Source Destination Protocol Length Info
31 8.858325 10.129.43.27 10.129.43.29 RDP 545 ClientData
32 8.859099 10.129.43.29 10.129.43.27 RDP 209 ServerData Encryption: None (None)
51 8.865852 10.129.43.27 10.129.43.29 RDP 698 ClientInfo
52 8.869677 10.129.43.29 10.129.43.27 RDP 117 Error Alert
53 8.870064 10.129.43.29 10.129.43.27 RDP 125 MultiTransportRequest
55 8.880062 10.129.43.27 10.129.43.29 RDP 109 MultiTransport response
56 8.927121 10.129.43.29 10.129.43.27 RDP 555 Demand Active PDU
57 8.931705 10.129.43.27 10.129.43.29 RDP 762 Confirm Active PDU
58 8.931849 10.129.43.27 10.129.43.29 RDP 119 RDP PDU Type: Synchronize
60 8.931918 10.129.43.29 10.129.43.27 RDP 119 RDP PDU Type: Synchronize
61 8.931925 10.129.43.27 10.129.43.27 RDP 123 RDP PDU Type: Control, Action: Cooperate
62 8.931975 10.129.43.29 10.129.43.27 RDP 123 RDP PDU Type: Control, Action: Cooperate
63 8.931997 10.129.43.27 10.129.43.29 RDP 123 RDP PDU Type: Control, Action: Request control
65 8.932186 10.129.43.29 10.129.43.27 RDP 123 RDP PDU Type: Control, Action: Granted control
66 8.932849 10.129.43.27 10.129.43.29 RDP 118 Fast-Path PDU,QoE timestamp,Scancode,Sync,Scancode,Scancode,Scancode,Scancode,Scancode,Scancode,Scancode,Scancode,Mou
67 8.932959 10.129.43.27 10.129.43.29 RDP 139 RDP PDU Type: BitmapCache Persistent List
69 8.933005 10.129.43.27 10.129.43.29 RDP 123 RDP PDU Type: FontList
70 8.933101 10.129.43.29 10.129.43.27 RDP 123 RDP PDU Type: FontMap
71 8.933257 10.129.43.29 10.129.43.27 DRDYNVC 117 Capabilities request
73 8.933610 10.129.43.29 10.129.43.27 DRDYNVC 142 CreateChannel Request
Frame 31: 545 bytes on wire (4360 bits), 545 bytes captured (4360 bits) on interface \Device\NPF_{4AF2D
Ethernet II, Src: VMware_b9:d9:9a (00:50:56:b9:d9:9a), Dst: VMware_b9:93:48 (00:50:56:b9:93:48)
Internet Protocol Version 4, Src: 10.129.43.27, Dst: 10.129.43.29
Transmission Control Protocol, Src Port: 50675, Dst Port: 3389, Seq: 1342, Ack: 1304, Len: 491
Transport Layer Security
TPKT, Version: 3, Length: 462
ISO 8073/X.224 COTP Connection-Oriented Transport Protocol
MULTIPOINT-COMMUNICATION-SERVICE T.125
GENERIC-CONFERENCE-CONTROL T.124
Remote Desktop Protocol
Frame (545 bytes)
Decrypted TLS (462 bytes)
guided-rdp.pcapng
Packets: 2225 · Displayed: 1427 (64.1%)
Profile: Default
10°C Cloudy
Search
ENG US
12:25 PM 2024-04-29


Debian 12.x 64-bit - VMware Workstation 17 Player (Non-commercial use only)
guided-rdp.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
No. Time Source Destination Protocol Length Info
1 0.000000 10.129.43.27 10.129.43.29 TCP 66 50674 → 3389 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
2 0.000231 10.129.43.29 10.129.43.27 TCP 66 3389 → 50674 [SYN, ACK] Seq=0 Ack=1 Win=64000 Len=0 MSS=1460 WS=1 SACK_PERM
3 0.000521 10.129.43.27 10.129.43.29 TCP 60 50674 → 3389 [ACK] Seq=1 Ack=1 Win=262656 Len=0
4 0.002562 10.129.43.27 10.129.43.29 TLSv1.2 97 Ignored Unknown Record
5 0.006406 10.129.43.29 10.129.43.27 TLSv1.2 73 Ignored Unknown Record
6 0.050370 10.129.43.27 10.129.43.29 TCP 60 50674 → 3389 [ACK] Seq=44 Ack=20 Win=262656 Len=0
7 6.256391 10.129.43.27 10.129.43.29 TLSv1.2 185 Client Hello (SNI=10.129.43.29)
8 6.257086 10.129.43.29 10.129.43.27 TLSv1.2 896 Server Hello, Certificate, Server Hello Done
9 6.258365 10.129.43.27 10.129.43.29 TLSv1.2 372 Client Key Exchange, Change Cipher Spec, Finished
10 6.260974 10.129.43.29 10.129.43.27 TLSv1.2 105 Change Cipher Spec, Finished
11 6.261843 10.129.43.27 10.129.43.29 CredSSP 140 NTLMSSP_NEGOTIATE
12 6.262246 10.129.43.29 10.129.43.27 CredSSP 324 NTLMSSP_CHALLENGE
13 6.263994 10.129.43.27 10.129.43.29 CredSSP 710 NTLMSSP_AUTH, User: DESKTOP-8BSUEVL\bucky
14 6.265122 10.129.43.29 10.129.43.27 CredSSP 142
15 6.265690 10.129.43.27 10.129.43.29 TCP 60 50674 → 3389 [RST, ACK] Seq=1235 Ack=1271 Win=0 Len=0
16 8.842069 10.129.43.27 10.129.43.29 TCP 66 50675 → 3389 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
17 8.842195 10.129.43.29 10.129.43.27 TCP 66 3389 → 50675 [SYN, ACK] Seq=0 Ack=1 Win=64000 Len=0 MSS=1460 WS=1 SACK_PERM
18 8.842471 10.129.43.27 10.129.43.29 TCP 60 50675 → 3389 [ACK] Seq=1 Ack=1 Win=2102272 Len=0
19 8.843397 10.129.43.27 10.129.43.29 TLSv1.2 97 Ignored Unknown Record
20 8.847171 10.129.43.29 10.129.43.27 TLSv1.2 73 Ignored Unknown Record
Frame 8: 896 bytes on wire (7168 bits), 896 bytes captured (7168 bits) on interface \Device\NPF_{4AF2D7
Ethernet II, Src: VMware_b9:93:48 (00:50:56:b9:93:48), Dst: VMware_b9:d9:9a (00:50:56:b9:d9:9a)
Internet Protocol Version 4, Src: 10.129.43.29, Dst: 10.129.43.27
Transmission Control Protocol, Src Port: 3389, Dst Port: 50674, Seq: 20, Ack: 175, Len: 842
Transport Layer Security
guided-rdp.pcapng
Packets: 2225 · Displayed: 2225 (100.0%)
Profile: Default


Debian 12.x 64-bit - VMware Workstation 17 Player (Non-commercial use only)
guided-rdp.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
tcp.stream eq 1
No. Time Source Destination Protocol Length Info
16 8.842069 10.129.43.27 10.129.43.29 TCP 66 50675 → 3389 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
17 8.842195 10.129.43.29 10.129.43.27 TCP 66 3389 → 50675 [SYN, ACK] Seq=0 Ack=1 Win=64000 Len=0 MSS=1460 WS=1 SACK_PERM
18 8.842471 10.129.43.27 10.129.43.29 TCP 60 50675 → 3389 [ACK] Seq=1 Ack=1 Win=2102272 Len=0
19 8.843397 10.129.43.27 10.129.43.29 TLSv1.2 97 Ignored Unknown Record
20 8.847171 10.129.43.29 10.129.43.27 TLSv1.2 73 Ignored Unknown Record
21 8.850426 10.129.43.27 10.129.43.29 TLSv1.2 185 Client Hello (SNI=10.129.43.29)
22 8.850662 10.129.43.29 10.129.43.27 TLSv1.2 896 Server Hello, Certificate, Server Hello Done
23 8.851306 10.129.43.27 10.129.43.29 TLSv1.2 372 Client Key Exchange, Change Cipher Spec, Finished
24 8.853828 10.129.43.29 10.129.43.27 TLSv1.2 105 Change Cipher Spec, Finished
25 8.854883 10.129.43.27 10.129.43.29 CredSSP 140 NTLMSSP_NEGOTIATE
26 8.855163 10.129.43.29 10.129.43.27 CredSSP 324 NTLMSSP_CHALLENGE
27 8.856293 10.129.43.27 10.129.43.29 CredSSP 710 NTLMSSP_AUTH, User: DESKTOP-8BSUEVL\bucky
28 8.857187 10.129.43.29 10.129.43.27 CredSSP 142
29 8.857674 10.129.43.27 10.129.43.29 CredSSP 161
30 8.858085 10.129.43.29 10.129.43.27 TPKT 87 Continuation
31 8.858325 10.129.43.27 10.129.43.29 RDP 545 ClientData
32 8.859099 10.129.43.29 10.129.43.27 RDP 209 ServerData Encryption: None (None)
33 8.859268 10.129.43.27 10.129.43.29 T.125 95 erectDomainRequest
34 8.859309 10.129.43.27 10.129.43.29 T.125 91 attachUserRequest
35 8.859322 10.129.43.29 10.129.43.27 TCP 54 3389 → 50675 [ACK] Seq=1459 Ack=1911 Win=63922 Len=0
Frame 19: 97 bytes on wire (776 bits), 97 bytes captured (776 bits) on interface \Device\NPF_{4AF2D71D-
Ethernet II, Src: VMware_b9:d9:9a (00:50:56:b9:d9:9a), Dst: VMware_b9:93:48 (00:50:56:b9:93:48)
Internet Protocol Version 4, Src: 10.129.43.27, Dst: 10.129.43.29
Transmission Control Protocol, Src Port: 50675, Dst Port: 3389, Seq: 1, Ack: 1, Len: 43
Transport Layer Security
0000 00 50 56 b9 93 48 00 50 56 b9 d9 9a 08 00 45 00
0010 00 53 dd 0d 40 00 80 06 b2 5d 0a 81 2b 1b 0a 81
0020 2b 1d c5 f3 0d 3d 4a 95 67 85 ea 2e 61 20 50 18
0030 20 14 cf 5a 00 00 03 00 00 2b 26 e0 00 00 00 00
0040 00 43 6f 6b 69 65 3a 20 6d 73 74 73 68 61 73 68
0050 68 3d 62 75 63 6b 79 0d 0a 01 00 08 00 0b 00 00
0060 00
guided-rdp.pcapng
Packets: 2225 · Displayed: 2210 (99.3%)
Profile: Default
10°C Cloudy
Search
ENG US
12:30 PM 2024-04-29