

Course: **Cloud and Network Security -C2 -2025**

Student Name: **Daniel-Caleb Cheruiyot**

Student No: **CS-CNS09-25014**

Saturday, May, 31st 2025

Week 2 Assignment 2:

Introduction to Network Traffic Analysis

<https://academy.hackthebox.com/achievement/1095115/81>

Table Of Contents

Introduction.....	3
TCP Fundamentals	3
File Input/Output with Tcpdump.....	8
Tcpdump Packet Filtering	8
Host Filter	8
Source/Destination Filter	9
Protocol Filter - Common Name.....	10
Port Range Filter	11
Tips and Tricks.....	11
Questions.....	12
Analysis with Wireshark	12
Following TCP Streams	14
Filter For A Specific TCP Stream	15
Packet Inception, Dissecting Network Traffic With Wireshark	15
Tasks	15
Guided Lab: Traffic Analysis Workflow.....	18
Decrypting RDP connections.....	21
Summary	24

Introduction

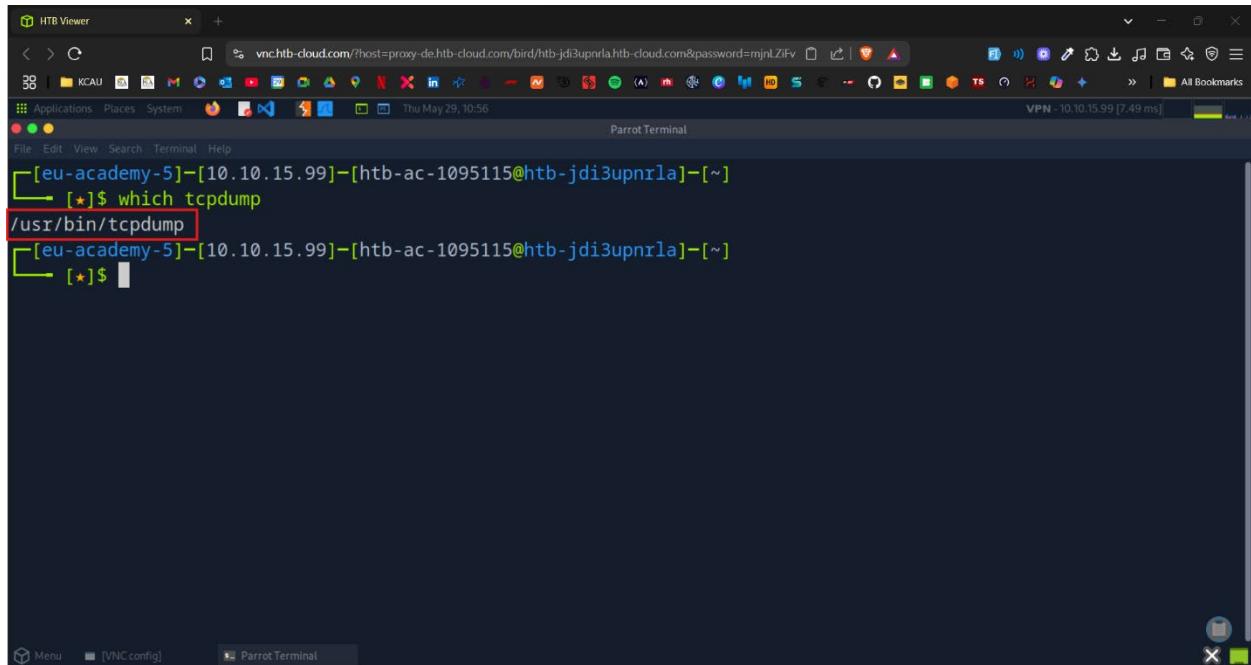
This report outlines my detailed investigation into suspicious network traffic and encrypted Remote Desktop Protocol (RDP) sessions associated with an internal host and also undertook multiple analysis tasks using Wireshark to:

- i. Extract transferred images over HTTP suspected of hiding data.
- ii. Investigate ongoing FTP and HTTP traffic during a live capture.
- iii. Conduct a full traffic analysis workflow to identify signs of intrusion.
- iv. Decrypt and analyze an RDP session using a recovered RSA private key.

TCP Fundamentals

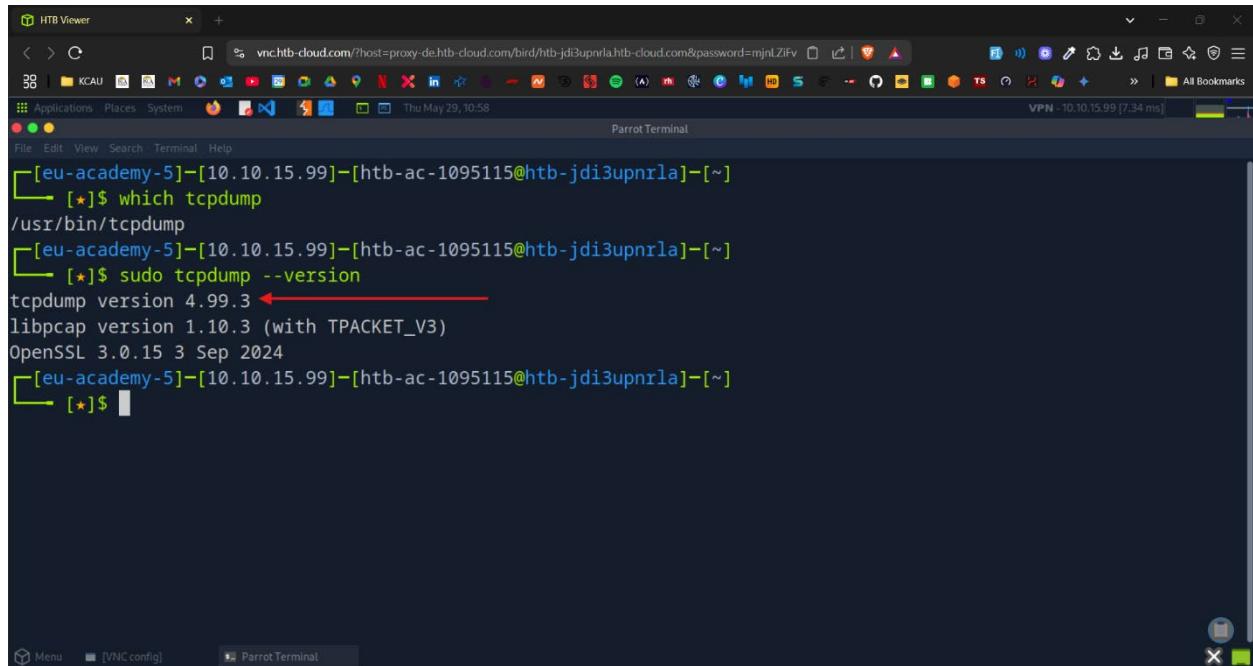
Tcpdump is a command-line packet sniffer that can directly capture and interpret data frames from a file or network interface.

First things first, is to locate tcpdump and validate if it exists



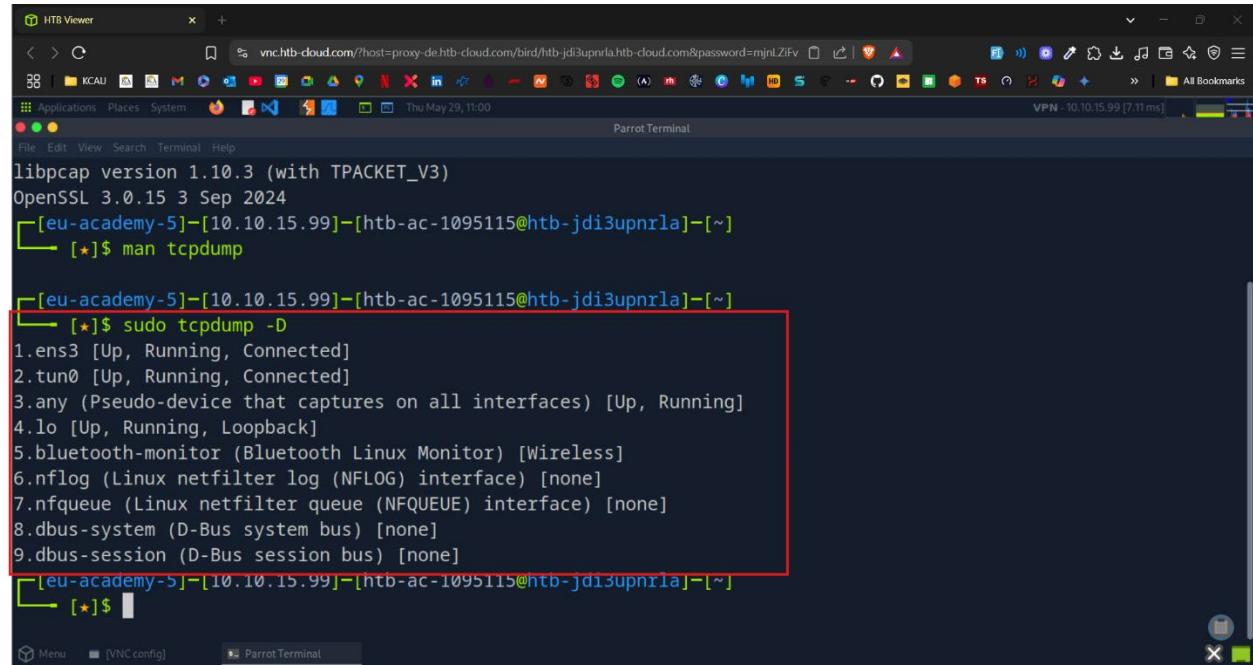
```
[eu-academy-5]-[10.10.15.99]-[htb-ac-1095115@htb-jdi3upnrla]-[~]
└── [★]$ which tcpdump
/usr/bin/tcpdump
[eu-academy-5]-[10.10.15.99]-[htb-ac-1095115@htb-jdi3upnrla]-[~]
└── [★]$
```

Hence no need for me to install. I then proceeded to check the version of the tcpdump installed which was **4.99.3**



```
[eu-academy-5]@[10.10.15.99]-[htb-ac-1095115@htb-jdi3upnrla]~
[*]$ which tcpdump
/usr/bin/tcpdump
[eu-academy-5]@[10.10.15.99]-[htb-ac-1095115@htb-jdi3upnrla]~
[*]$ sudo tcpdump --version
tcpdump version 4.99.3
libpcap version 1.10.3 (with TPACKET_V3)
OpenSSL 3.0.15 3 Sep 2024
[eu-academy-5]@[10.10.15.99]-[htb-ac-1095115@htb-jdi3upnrla]~
[*]$
```

To list the available interfaces, I used the command **tcpdump -D** which displayed a list of network interfaces to choose from as shown below.



```
libpcap version 1.10.3 (with TPACKET_V3)
OpenSSL 3.0.15 3 Sep 2024
[eu-academy-5]@[10.10.15.99]-[htb-ac-1095115@htb-jdi3upnrla]~
[*]$ man tcpdump
[eu-academy-5]@[10.10.15.99]-[htb-ac-1095115@htb-jdi3upnrla]~
[*]$ sudo tcpdump -D
1.ens3 [Up, Running, Connected]
2.tun0 [Up, Running, Connected]
3.any (Pseudo-device that captures on all interfaces) [Up, Running]
4.lo [Up, Running, Loopback]
5.bluetooth-monitor (Bluetooth Linux Monitor) [Wireless]
6.nflog (Linux netfilter log (NFLOG) interface) [none]
7.nfqueue (Linux netfilter queue (NFQUEUE) interface) [none]
8.dbus-system (D-Bus system bus) [none]
9.dbus-session (D-Bus session bus) [none]
[eu-academy-5]@[10.10.15.99]-[htb-ac-1095115@htb-jdi3upnrla]~
[*]$
```

In my case, I chose interface **ens3**:

```
[eu-academy-5]@[10.10.15.99]@[htb-ac-1095115@htb-jdi3upnrla]~
[*]$ sudo tcpdump -i ens3
tcpdump: verbose output suppressed, use -v[v]... for full protocol decode
listening on ens3, link-type EN10MB (Ethernet), snapshot length 262144 bytes
11:03:22.716533 IP 94-237-101-137.de-htb1.upcloud.host.35366 > htb-jdi3upnrla.htb-cloud.com.http: Flags [P.], seq 569986044:569986060, ack 2132008608, win 8409, options [nop,nop,TS val 1631647268 ecr 911825137], length 16: HTTP
11:03:22.716561 IP htb-jdi3upnrla.htb-cloud.com.http > 94-237-101-137.de-htb1.upcloud.host.35366: Flags [.], ack 16, win 498, options [nop,nop,TS val 911825161 ecr 1631647268], length 0
11:03:22.716905 IP 94-237-101-137.de-htb1.upcloud.host.35366 > htb-jdi3upnrla.htb-cloud.com.http: Flags [P.], seq 16:32, ack 1, win 8409, options [nop,nop,TS val 1631647269 ecr 911825161], length 16: HTTP
11:03:22.716910 IP htb-jdi3upnrla.htb-cloud.com.http > 94-237-101-137.de-htb1.upcloud.host.35366: Flags [.], ack 32, win 498, options [nop,nop,TS val 911825161 ecr 1631647269], length 0
11:03:22.717276 IP htb-jdi3upnrla.htb-cloud.com.http > 94-237-101-137.de-htb1.upcloud.host.35366: Flags [P.], seq 1:1777, ack 32, win 498, options [nop,nop,TS val 911825162 ecr 1631647269], length 1776: HTTP
11:03:22.717410 IP 94-237-101-137.de-htb1.upcloud.host.49942 > htb-jdi3upnrla.htb-cloud.com.http: Flags [P.], seq 1131017145:1131017161, ack 2314927648, win 9190, options [nop,nop,TS val 1631647269 ecr 911825136], length 16: HTTP
11:03:22.717410 IP 94-237-101-137.de-htb1.upcloud.host.35366 > htb-jdi3upnrla.htb-cloud.com.http: Flags [.], ack
```

```
[eu-academy-5]@[10.10.15.99]@[htb-ac-1095115@htb-jdi3upnrla]~
[*]$ sudo tcpdump -i ens3 -nn
11:03:23.352362 IP htb-jdi3upnrla.htb-cloud.com.http > 94-237-101-137.de-htb1.upcloud.host.49942: Flags [.], ack 418, win 500, options [nop,nop,TS val 911825797 ecr 1631647863], length 0
11:03:23.369058 IP htb-jdi3upnrla.htb-cloud.com.http > 94-237-101-137.de-htb1.upcloud.host.35376: Flags [.], ack 464, win 504, options [nop,nop,TS val 911825813 ecr 1631647878], length 0
11:03:23.375689 IP htb-jdi3upnrla.htb-cloud.com.http > 94-237-101-137.de-htb1.upcloud.host.35366: Flags [.], ack 400, win 498, options [nop,nop,TS val 911825820 ecr 1631647887], length 0
11:03:23.452654 IP 94-237-101-137.de-htb1.upcloud.host.49942 > htb-jdi3upnrla.htb-cloud.com.http: Flags [P.], seq 418:436, ack 389356, win 9190, options [nop,nop,TS val 1631648004 ecr 911825797], length 18: HTTP
11:03:23.452707 IP htb-jdi3upnrla.htb-cloud.com.http > 94-237-101-137.de-htb1.upcloud.host.49942: Flags [.], ack 436, win 500, options [nop,nop,TS val 911825897 ecr 1631648004], length 0
^C11:03:23.487552 IP htb-jdi3upnrla.htb-cloud.com.56956 > 154-57-165-57.static.isp.htb.systems.1337: UDP, length 148

281 packets captured
723 packets received by filter
326 packets dropped by kernel
[eu-academy-5]@[10.10.15.99]@[htb-ac-1095115@htb-jdi3upnrla]~
[*]$
```

By issuing the **-nn** switches as seen below, we tell Tcpdump to refrain from resolving IP addresses and port numbers to their hostnames and common port names.

```

[eu-academy-5]@[10.10.15.99]-[htb-ac-1095115@htb-jdi3upnrla]-[~]
[*]$ sudo tcpdump -i ens3 -nn
tcpdump: verbose output suppressed, use -v[v]... for full protocol decode
listening on ens3, link-type EN10MB (Ethernet), snapshot length 262144 bytes
11:04:28.977962 IP 94.237.101.137.35366 > 5.22.214.30.80: Flags [P.], seq 570023644:570023660, ack 2149560433, win 8409, options [nop,nop,TS val 1631713530 ecr 911891417], length 16: HTTP
11:04:28.978017 IP 94.237.101.137.49942 > 5.22.214.30.80: Flags [P.], seq 1131053365:1131053381, ack 2340345421, win 9190, options [nop,nop,TS val 1631713530 ecr 911891417], length 16: HTTP
11:04:28.978283 IP 94.237.101.137.49942 > 5.22.214.30.80: Flags [P.], seq 16:32, ack 1, win 9190, options [nop,nop,TS val 1631713530 ecr 911891417], length 16: HTTP
11:04:28.978298 IP 5.22.214.30.80 > 94.237.101.137.49942: Flags [.], ack 32, win 500, options [nop,nop,TS val 911891423 ecr 1631713530], length 0
11:04:28.978585 IP 94.237.101.137.35366 > 5.22.214.30.80: Flags [P.], seq 16:32, ack 1, win 8409, options [nop,nop,TS val 1631713531 ecr 911891417], length 16: HTTP
11:04:28.978602 IP 5.22.214.30.80 > 94.237.101.137.35366: Flags [.], ack 32, win 498, options [nop,nop,TS val 911891423 ecr 1631713530], length 0
11:04:28.982232 IP 94.237.101.137.35376 > 5.22.214.30.80: Flags [P.], seq 3128796877:3128796893, ack 1095781951, win 12069, options [nop,nop,TS val 1631713534 ecr 911891417], length 16: HTTP
11:04:28.982255 IP 5.22.214.30.80 > 94.237.101.137.35376: Flags [P.], seq 16:32, ack 16, win 504, options [nop,nop,TS val 911891424 ecr 1631713534], length 0

```

When utilizing the **-e** switch, we are tasking tcpdump to include the ethernet headers in the capture's output along with its regular content. We can see this worked by examining the output.

```

[eu-academy-5]@[10.10.15.99]-[htb-ac-1095115@htb-jdi3upnrla]-[~]
[*]$ sudo tcpdump -i ens3 -e
tcpdump: verbose output suppressed, use -v[v]... for full protocol decode
listening on ens3, link-type EN10MB (Ethernet), snapshot length 262144 bytes
11:06:15.507526 a6:ba:3b:08:09:c1 (oui Unknown) > 9a:7e:32:38:97:79 (oui Unknown), ethertype IPv4 (0x0800), length 120: htb-jdi3upnrla.htb-cloud.com.http > 94-237-101-137.de-htb1.upcloud.host.49942: Flags [P.], seq 2379427414:2379427468, ack 1131114859, win 500, options [nop,nop,TS val 911997952 ecr 1631820024], length 54: HTTP
11:06:15.507555 a6:ba:3b:08:09:c1 (oui Unknown) > 9a:7e:32:38:97:79 (oui Unknown), ethertype IPv4 (0x0800), length 120: htb-jdi3upnrla.htb-cloud.com.http > 94-237-101-137.de-htb1.upcloud.host.35376: Flags [P.], seq 1129719293:1129719347, ack 3128855245, win 503, options [nop,nop,TS val 911997952 ecr 1631819904], length 54: HTTP
11:06:15.507585 a6:ba:3b:08:09:c1 (oui Unknown) > 9a:7e:32:38:97:79 (oui Unknown), ethertype IPv4 (0x0800), length 120: htb-jdi3upnrla.htb-cloud.com.http > 94-237-101-137.de-htb1.upcloud.host.35366: Flags [P.], seq 2179381871:2179381925, ack 570081756, win 498, options [nop,nop,TS val 911997952 ecr 1631819904], length 54: HTTP
11:06:15.507768 9a:7e:32:38:97:79 (oui Unknown) > a6:ba:3b:08:09:c1 (oui Unknown), ethertype IPv4 (0x0800), length 66: 94-237-101-137.de-htb1.upcloud.host.35376 > htb-jdi3upnrla.htb-cloud.com.http: Flags [.], ack 54, win 12069, options [nop,nop,TS val 1631820060 ecr 911997952], length 0
11:06:15.507768 9a:7e:32:38:97:79 (oui Unknown) > a6:ba:3b:08:09:c1 (oui Unknown), ethertype IPv4 (0x0800), length 66: 94-237-101-137.de-htb1.upcloud.host.49942 > htb-jdi3upnrla.htb-cloud.com.http: Flags [.], ack 54, win 9190, options [nop,nop,TS val 1631820060 ecr 911997952], length 0

```

By issuing the **-X** switch, we can see the packet a bit clearer now. We get an ASCII output on the right to interpret anything in clear text that corresponds to the hexadecimal output on the left.

```

[eu-academy-5]@[10.10.15.99]-[htb-ac-1095115@htb-jdi3upnrla]-[~]
└── [★]$ sudo tcpdump -i ens3 -X
tcpdump: verbose output suppressed, use -v[v]... for full protocol decode
listening on ens3, link-type EN10MB (Ethernet), snapshot length 262144 bytes
11:08:32.486442 IP htb-jdi3upnrla.htb-cloud.com.56956 > 154-57-165-57.static.isp.htb.systems.1337: UDP, length 148
    0x0000: 4500 00b0 90d6 4000 4011 8ebf 0516 d61e E.....@.@.....
    0x0010: 9a39 a539 de7c 0539 009c 1b55 4800 0048 .9.9.|.9...UH..H
    0x0020: ba7b 76a6 162f 1740 4a50 d0c5 f3f3 4df4 .{.../.@JP....M.
    0x0030: 3e14 d029 40bc a413 32d9 5cf1 1b78 cc86 >...@...2.\..x..
    0x0040: 0782 7a18 38a4 e298 7ef9 669c c31b ed7d ..z.8....~.f....}
    0x0050: 9cc2 548b 73d8 bc6f fe7e da8e 28e4 20b2 ..T.s..o.~.(...
    0x0060: ace8 3902 e8c4 dfde 907b b9bd ff2e 02cd ..9.....{.....
    0x0070: 5138 6355 34e0 f9c6 1270 de3d 61db c375 Q8cU4....p.=a..u
    0x0080: 6f72 0bf0 6811 c8b4 b469 db20 5193 21d8 or..h....i..Q!.#
    0x0090: ce7b a887 2c48 9789 7807 6663 bc10 2350 .{.,H..x.fc..#P
    0x00a0: 4b7a ad44 69e6 b092 ab04 1e4b f151 031e Kz.Di.....K.Q..
11:08:32.486681 IP 94-237-101-137.de-htb1.upcloud.host.49942 > htb-jdi3upnrla.htb-cloud.com.http: Flags [.], ack 2524930544, win 9190, options [nop,nop,TS val 1631957040 ecr 912134890], length 0

```

After trying the few different switches shown above, I learnt that we can also chain them e.g
`sudo tcpdump -i ens3 -nnvXX`

as shown below:

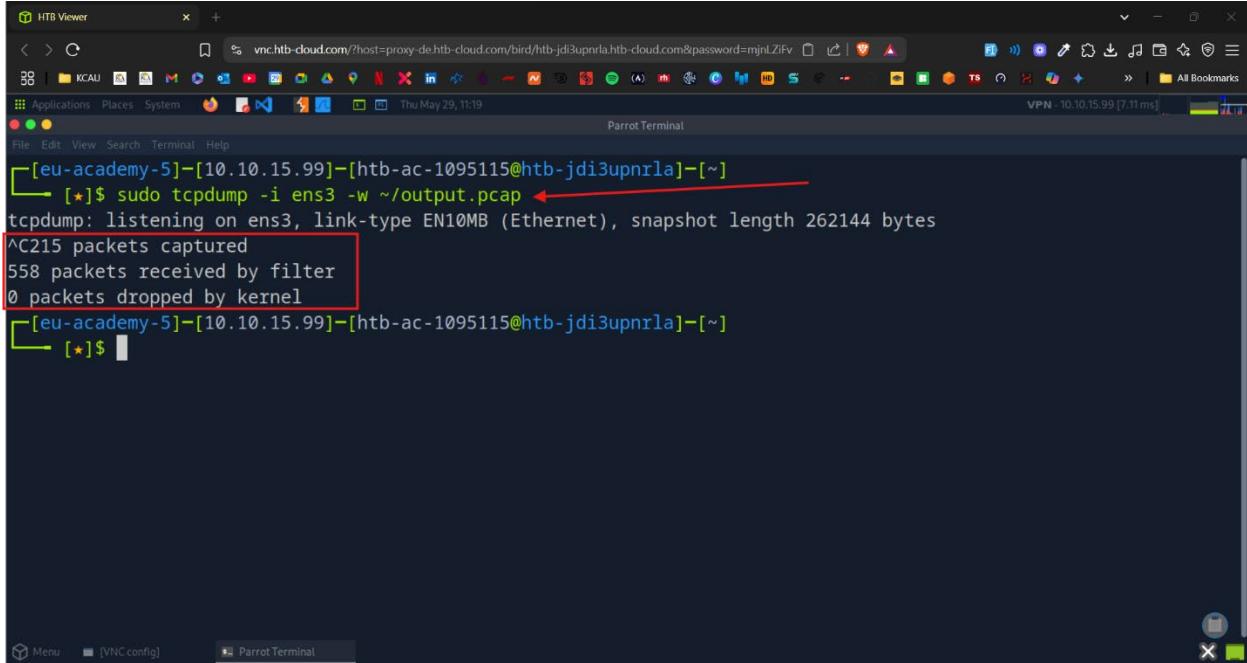
```

[eu-academy-5]@[10.10.15.99]-[htb-ac-1095115@htb-jdi3upnrla]-[~]
└── [★]$ sudo tcpdump -i ens3 -nnvXX
tcpdump: listening on ens3, link-type EN10MB (Ethernet), snapshot length 262144 bytes
11:10:20.919208 IP (tos 0x0, ttl 58, id 30453, offset 0, flags [DF], proto TCP (6), length 68)
    94.237.101.137.49942 > 5.22.214.30.80: Flags [P.], cksum 0x6297 (correct), seq 1131277047:1131277063, ack 25
    33632221, win 9190, options [nop,nop,TS val 1632065473 ecr 912243342], length 16: HTTP
        0x0000: a6ba 3b08 09c1 9a7e 3238 9779 0800 4500 ..;....~28.y..E.
        0x0010: 0044 76f5 4000 3a06 2a14 5eed 6589 0516 .Dv.@.*.^e...
        0x0020: d61e c316 0050 436d eaf7 9704 28dd 8018 .....PCm....(...
        0x0030: 23e6 6297 0000 0101 080a 6147 57c1 365f #.b.....aGW.6_
        0x0040: ba8e 828a 0bb1 c983 f3b1 c983 0bb1 c982 .....
        0x0050: 0ab0 ..
11:10:20.919223 IP (tos 0x0, ttl 64, id 48160, offset 0, flags [DF], proto TCP (6), length 52)
    5.22.214.30.80 > 94.237.101.137.49942: Flags [.], cksum 0x9fd1 (incorrect -> 0x7956), ack 16, win 498, options [nop,nop,TS val 1632065473, length 0
        0x0000: 9a7e 3238 9779 a6ba 3b08 09c1 0800 4500 .~28.y..;....E.
        0x0010: 0034 bc20 4000 4006 def8 0516 d61e 5eed .4..@. ....^.
        0x0020: 6589 0050 c316 9704 28dd 436d eb07 8010 e..P....(.Cm....
        0x0030: 01f2 9fd1 0000 0101 080a 365f baa4 6147 .....6_.aG

```

File Input/Output with Tcpdump

Using -w will write our capture to a file and in my case I named the file **output.pcap**



The screenshot shows a terminal window titled "Parrot Terminal" running on a Kali Linux system. The user has entered the command `sudo tcpdump -i ens3 -w ~/output.pcap`. The terminal output indicates that the command was successful, showing statistics for captured and received packets, and noting that no packets were dropped by the kernel. A red arrow points to the command line where it was entered.

```
[eu-academy-5]@[10.10.15.99]-[htb-ac-1095115@htb-jdi3upnrla]-[~]
└── [★]$ sudo tcpdump -i ens3 -w ~/output.pcap ←
tcpdump: listening on ens3, link-type EN10MB (Ethernet), snapshot length 262144 bytes
^C215 packets captured
558 packets received by filter
0 packets dropped by kernel
[eu-academy-5]@[10.10.15.99]-[htb-ac-1095115@htb-jdi3upnrla]-[~]
└── [★]$
```

Tcpdump Packet Filtering

Tcpdump provides a robust and efficient way to parse the data included in our captures via packet filters.

Host Filter

This filter is often used when we want to examine only a specific host or server. With this, we can identify with whom this host or server communicates and in which way.

```
[eu-academy-5]@[10.10.15.99]:[htb-ac-1095115@htb-yfod2hpnw6]~[~]
[*]$ sudo tcpdump -i ens3 host 94.237.29.52
tcpdump: verbose output suppressed, use -v[v]... for full protocol decode
listening on ens3, link-type EN10MB (Ethernet), snapshot length: 262144 bytes
06:25:21.427513 IP htb-yfod2hpnw6.hbt-cloud.com.http > 94-237-101-137.de-htb1.upcloud.host.51938: Flags [P.], seq 2537012480:2537012610, ack 3617520196, win 504, options [nop,nop,TS val 2767408660 ecr 1115707768], length 130: HTTP
06:25:21.427569 IP htb-yfod2hpnw6.hbt-cloud.com.http > 94-237-101-137.de-htb1.upcloud.host.56210: Flags [P.], seq 3550207082:3550207208, ack 6216675, win 504, options [nop,nop,TS val 2767408660 ecr 1115707770], length 126: HTTP
06:25:21.427608 IP htb-yfod2hpnw6.hbt-cloud.com.http > 94-237-101-137.de-htb1.upcloud.host.56208: Flags [P.], seq 1234996256:1234996380, ack 2573969407, win 505, options [nop,nop,TS val 2767408660 ecr 1115707769], length 124: HTTP
06:25:21.427682 IP 94-237-101-137.de-htb1.upcloud.host.51938 > htb-yfod2hpnw6.hbt-cloud.com.http: Flags [., ack 130, win 4959, options [nop,nop,TS val 1115707787 ecr 2767408643]], length 0
06:25:21.427720 IP 94-237-101-137.de-htb1.upcloud.host.56210 > htb-yfod2hpnw6.hbt-cloud.com.http: Flags [., ack 126, win 20532, options [nop,nop,TS val 1115707787 ecr 2767408643]], length 0
06:25:21.427735 IP 94-237-101-137.de-htb1.upcloud.host.56208 > htb-yfod2hpnw6.hbt-cloud.com.http: Flags [., ack 124, win 19832, options [nop,nop,TS val 1115707787 ecr 2767408643]], length 0
06:25:21.443594 IP htb-yfod2hpnw6.hbt-cloud.com.http > 94-237-101-137.de-htb1.upcloud.host.51938: Flags [P.], seq 130:3199, ack 1, win 504, options [nop,nop,TS val 2767408676 ecr 1115707787], length 3069: HTTP
06:25:21.443739 IP htb-yfod2hpnw6.hbt-cloud.com.http > 94-237-101-137.de-htb1.upcloud.host.56210: Flags [P.], seq 126:3196, ack 1, win 504, options [nop,nop,TS val 2767408676 ecr 1115707787], length 3070: HTTP
06:25:21.443777 IP 94-237-101-137.de-htb1.upcloud.host.51938 > htb-yfod2hpnw6.hbt-cloud.com.http: Flags [., ack 3199, win 4959, options [nop,nop,TS val 1115707803 ecr 2767408676]], length 0
06:25:21.443848 IP htb-yfod2hpnw6.hbt-cloud.com.http > 94-237-101-137.de-htb1.upcloud.host.56208: Flags [P.], seq 124:3187, ack 1, win 505, options [nop,nop,TS val 2767408676 ecr 1115707803], length 3063: HTTP
```

Source/Destination Filter

Source and destination allow us to work with the directions of communication. For example, in the last output, we have specified that our source host is **94.237.29.52**, and only packets sent from this host will be intercepted. This can be done for ports, and network ranges as well. An example of this utilizing **src port 80** would look something like this:

```

[eu-academy-5]~[10.10.15.99]~[htb-ac-1095115@htb-yfod2hpnw6]~[~]
[eu-academy-5]$ sudo tcpdump -i ens3 tcp src port 80
tcpdump: verbose output suppressed, use -v[v]... for full protocol decode
listening on ens3, link-type EN10MB (Ethernet), snapshot length 262144 bytes
06:27:07.335413 IP htb-yfod2hpnw6.hbt-cloud.com.http > 94-237-101-137.de-htb1.upcloud.host.51938: Flags [P.], seq 2603095272:2603095534, ack 3617580351, win 504, option s [nop,nop,TS val 2767514568 ecr 1115813662], length 262: HTTP
06:27:07.335473 IP htb-yfod2hpnw6.hbt-cloud.com.http > 94-237-101-137.de-htb1.upcloud.host.56208: Flags [P.], seq 1274727320:1274727582, ack 2574013215, win 505, option s [nop,nop,TS val 2767514568 ecr 1115813662], length 262: HTTP
06:27:07.335511 IP htb-yfod2hpnw6.hbt-cloud.com.http > 94-237-101-137.de-htb1.upcloud.host.56210: Flags [P.], seq 3598212623:3598212885, ack 6268611, win 503, options [nop,nop,TS val 2767514568 ecr 1115813662], length 262: HTTP
06:27:07.376960 IP htb-yfod2hpnw6.hbt-cloud.com.http > 94-237-101-137.de-htb1.upcloud.host.51938: Flags [P.], seq 262:7502, ack 1, win 504, options [nop,nop,TS val 2767514602 ecr 1115813695], length 7240: HTTP
06:27:07.369634 IP htb-yfod2hpnw6.hbt-cloud.com.http > 94-237-101-137.de-htb1.upcloud.host.51938: Flags [P.], seq 7502:14742, ack 1, win 504, options [nop,nop,TS val 2767514602 ecr 1115813695], length 7240: HTTP
06:27:07.369937 IP htb-yfod2hpnw6.hbt-cloud.com.http > 94-237-101-137.de-htb1.upcloud.host.51938: Flags [P.], seq 14742:23494, ack 1, win 504, options [nop,nop,TS val 2767514602 ecr 1115813730], length 8752: HTTP
06:27:07.370288 IP htb-yfod2hpnw6.hbt-cloud.com.http > 94-237-101-137.de-htb1.upcloud.host.56210: Flags [P.], seq 262:7502, ack 1, win 503, options [nop,nop,TS val 2767514602 ecr 1115813695], length 7240: HTTP
06:27:07.37016 IP htb-yfod2hpnw6.hbt-cloud.com.http > 94-237-101-137.de-htb1.upcloud.host.56210: Flags [P.], seq 7502:14742, ack 1, win 503, options [nop,nop,TS val 2767514602 ecr 1115813695], length 7240: HTTP
06:27:07.370288 IP htb-yfod2hpnw6.hbt-cloud.com.http > 94-237-101-137.de-htb1.upcloud.host.56210: Flags [P.], seq 14742:23498, ack 1, win 503, options [nop,nop,TS val 2767514603 ecr 1115813730], length 8756: HTTP
06:27:07.371280 IP htb-yfod2hpnw6.hbt-cloud.com.http > 94-237-101-137.de-htb1.upcloud.host.56208: Flags [P.], seq 262:7502, ack 1, win 505, options [nop,nop,TS val 2767514604 ecr 1115813695], length 7240: HTTP
06:27:07.371293 IP htb-yfod2hpnw6.hbt-cloud.com.http > 94-237-101-137.de-htb1.upcloud.host.56208: Flags [P.], seq 7502:14742, ack 1, win 505, options [nop,nop,TS val 2767514604 ecr 1115813695], length 7240: HTTP
06:27:07.371474 IP htb-yfod2hpnw6.hbt-cloud.com.http > 94-237-101-137.de-htb1.upcloud.host.56208: Flags [P.], seq 14742:23501, ack 1, win 505, options [nop,nop,TS val 2767514604 ecr 1115813695], length 7240: HTTP

```

Protocol Filter - Common Name

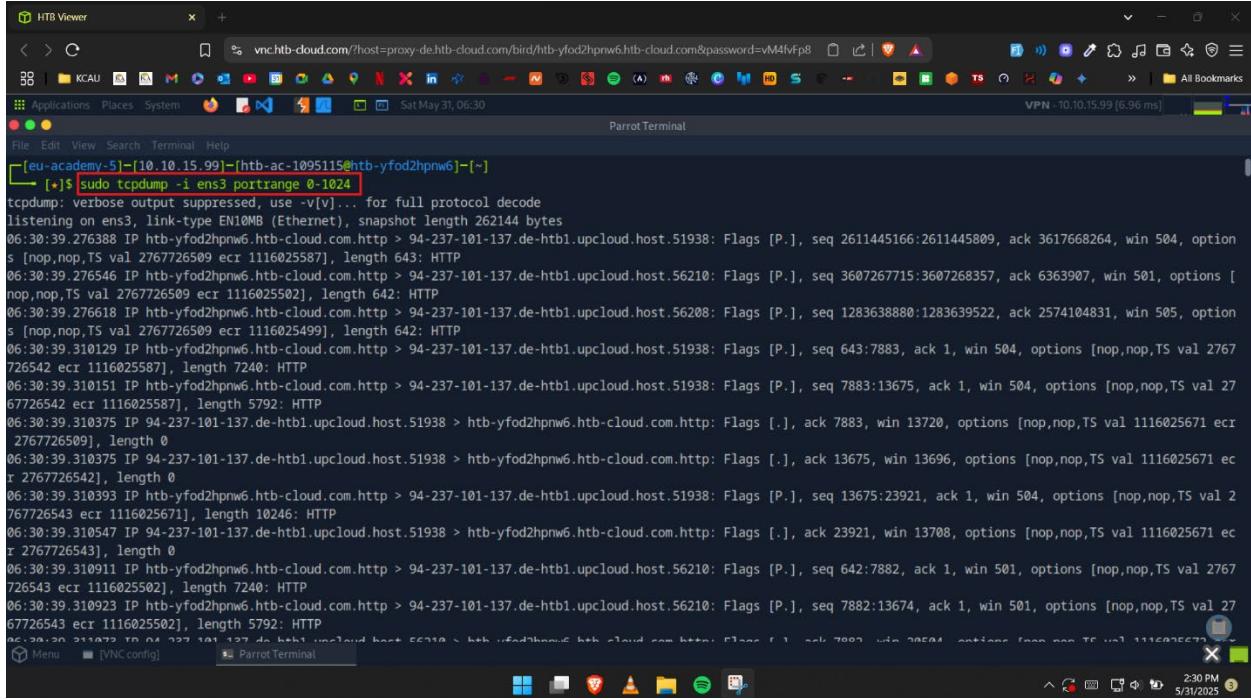
```

[eu-academy-5]~[10.10.15.99]~[htb-ac-1095115@htb-yfod2hpnw6]~[~]
[eu-academy-5]$ sudo tcpdump -i ens3 udp
tcpdump: verbose output suppressed, use -v[v]... for full protocol decode
listening on ens3, link-type EN10MB (Ethernet), snapshot length 262144 bytes
06:28:38.377730 IP htb-yfod2hpnw6.hbt-cloud.com.52847 > 154-57-165-57.static.isp.hbt.systems.1337: UDP, length 148
06:28:38.384558 IP htb-yfod2hpnw6.hbt-cloud.com.52847 > 154-57-165-57.static.isp.hbt.systems.1337 > htb-yfod2hpnw6.hbt-cloud.com.52847: UDP, length 148
06:28:38.440292 IP htb-yfod2hpnw6.hbt-cloud.com.50846 > one.one.one.domain: 3070+ PTR? 57.165.57.154.in-addr.arpa. (44)
06:28:39.379148 IP htb-yfod2hpnw6.hbt-cloud.com.52847 > 154-57-165-57.static.isp.hbt.systems.1337: UDP, length 148
06:28:39.386158 IP htb-yfod2hpnw6.hbt-cloud.com.52847 > 154-57-165-57.static.isp.hbt.systems.1337 > htb-yfod2hpnw6.hbt-cloud.com.52847: UDP, length 148
06:28:39.587203 IP one.one.one.domain > htb-yfod2hpnw6.hbt-cloud.com.50846: 3070 1/0/0 PTR 154-57-165-57.static.isp.hbt.systems. (94)
06:28:39.598734 IP htb-yfod2hpnw6.hbt-cloud.com.55174 > one.one.one.domain: 56103+ PTR? 52.29.237.94.in-addr.arpa. (43)
06:28:39.633735 IP one.one.one.domain > htb-yfod2hpnw6.hbt-cloud.com.55174: 56103 1/0/0 PTR htb-yfod2hpnw6.hbt-cloud.com. (85)
06:28:39.633958 IP htb-yfod2hpnw6.hbt-cloud.com.45521 > one.one.one.domain: 22941+ PTR? 1.1.1.1.in-addr.arpa. (38)
06:28:39.635051 IP one.one.one.domain > htb-yfod2hpnw6.hbt-cloud.com.45521: 22941 1/0/0 PTR one.one.one.one. (67)
06:28:39.892034 IP htb-yfod2hpnw6.hbt-cloud.com.ntp > connected-by.freedominter.net.ntp: NTPv4, Client, length 48
06:28:39.892064 IP htb-yfod2hpnw6.hbt-cloud.com.ntp > 79.133.44.137.ntp: NTPv4, Client, length 48
06:28:39.990003 IP htb-yfod2hpnw6.hbt-cloud.com.38432 > one.one.one.domain: 3385+ PTR? 58.19.239.178.in-addr.arpa. (44)
06:28:39.991907 IP one.one.one.domain > htb-yfod2hpnw6.hbt-cloud.com.38432: 3385 1/0/0 PTR connected-by.freedominter.net. (87)
06:28:39.993010 IP htb-yfod2hpnw6.hbt-cloud.com.46561 > one.one.one.domain: 31090+ PTR? 137.44.133.79.in-addr.arpa. (44)
06:28:39.995489 IP one.one.one.domain > htb-yfod2hpnw6.hbt-cloud.com.46561: 31090 NXDomain 0/1/0 (102)
^C
16 packets captured
16 packets received by filter
0 packets dropped by kernel
[eu-academy-5]~[10.10.15.99]~[htb-ac-1095115@htb-yfod2hpnw6]~[~]
[eu-academy-5]$ 

```

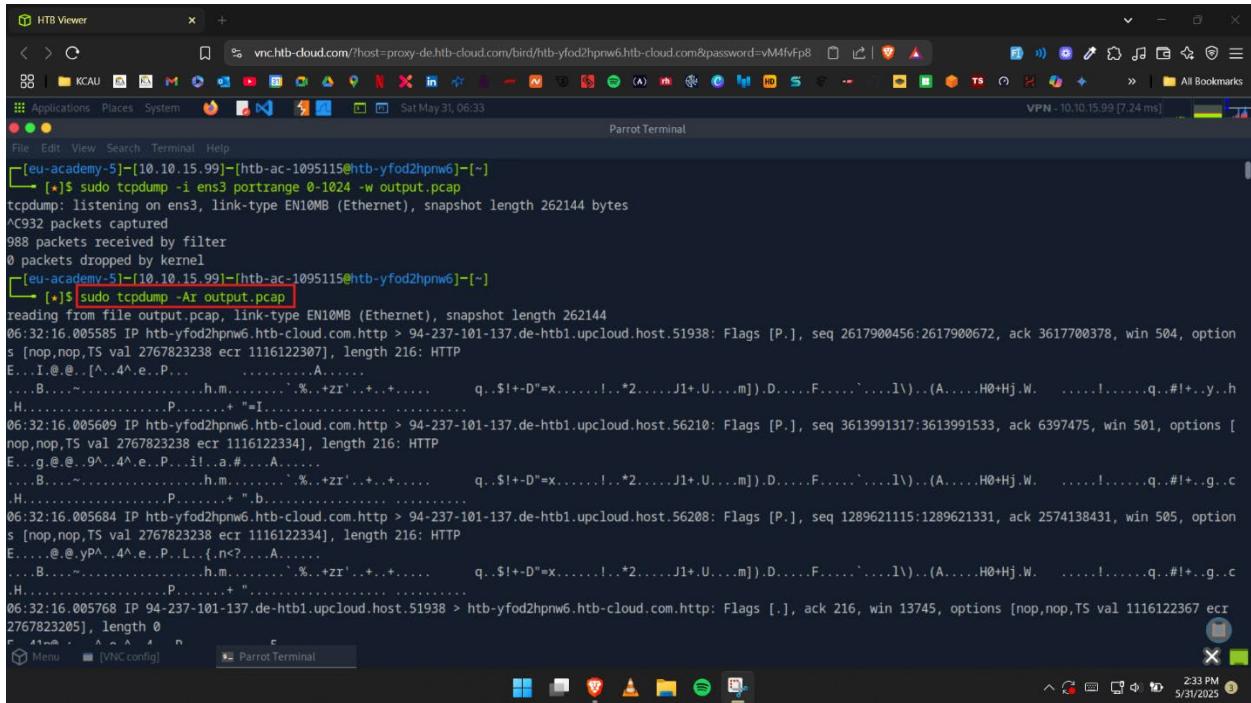
Port Range Filter

This allows us to everything from within the port range.



```
[eu-academy-5]~[10.10.15.99]~[htb-ac-1095115@htb-yfod2hpnw6]~[~]
[~]$ sudo tcpdump -i ens3 portrange 0-1024
tcpdump: verbose output suppressed, use -v[V]... for full protocol decode
listening on ens3, link-type EN10MB (Ethernet), snapshot length 262144 bytes
06:30:39.276388 IP htb-yfod2hpnw6.hbt-cloud.com.http > 94-237-101-137.de-htb1.upcloud.host.51938: Flags [P.], seq 2611445166:2611445809, ack 3617668264, win 504, option s [nop,nop,TS val 2767726509 ecr 1116025587], length 643: HTTP
06:30:39.276548 IP htb-yfod2hpnw6.hbt-cloud.com.http > 94-237-101-137.de-htb1.upcloud.host.56210: Flags [P.], seq 3607267715:3607268357, ack 6363907, win 501, options [nop,nop,TS val 2767726509 ecr 1116025587], length 642: HTTP
06:30:39.276618 IP htb-yfod2hpnw6.hbt-cloud.com.http > 94-237-101-137.de-htb1.upcloud.host.56208: Flags [P.], seq 1283638880:1283639522, ack 2574104831, win 505, options [nop,nop,TS val 2767726509 ecr 1116025499], length 642: HTTP
06:30:39.310129 IP htb-yfod2hpnw6.hbt-cloud.com.http > 94-237-101-137.de-htb1.upcloud.host.51938: Flags [P.], seq 643:7883, ack 1, win 504, options [nop,nop,TS val 276726542 ecr 1116025587], length 7240: HTTP
06:30:39.310151 IP htb-yfod2hpnw6.hbt-cloud.com.http > 94-237-101-137.de-htb1.upcloud.host.51938: Flags [P.], seq 7883:13675, ack 1, win 504, options [nop,nop,TS val 2767726542 ecr 1116025587], length 5792: HTTP
06:30:39.310375 IP 94-237-101-137.de-htb1.upcloud.host.51938 > htb-yfod2hpnw6.hbt-cloud.com.http: Flags [.], ack 7883, win 13720, options [nop,nop,TS val 1116025671 ecr 2767726509], length 0
06:30:39.310375 IP 94-237-101-137.de-htb1.upcloud.host.51938 > htb-yfod2hpnw6.hbt-cloud.com.http: Flags [.], ack 13675, win 13696, options [nop,nop,TS val 1116025671 ecr 2767726542], length 0
06:30:39.310393 IP htb-yfod2hpnw6.hbt-cloud.com.http > 94-237-101-137.de-htb1.upcloud.host.51938: Flags [P.], seq 13675:23921, ack 1, win 504, options [nop,nop,TS val 2767726543 ecr 1116025671], length 10246: HTTP
06:30:39.310547 IP 94-237-101-137.de-htb1.upcloud.host.51938 > htb-yfod2hpnw6.hbt-cloud.com.http: Flags [.], ack 23921, win 13708, options [nop,nop,TS val 1116025671 ecr 2767726543], length 0
06:30:39.310911 IP htb-yfod2hpnw6.hbt-cloud.com.http > 94-237-101-137.de-htb1.upcloud.host.56210: Flags [P.], seq 642:7882, ack 1, win 501, options [nop,nop,TS val 276726543 ecr 1116025502], length 5792: HTTP
06:30:39.310923 IP htb-yfod2hpnw6.hbt-cloud.com.http > 94-237-101-137.de-htb1.upcloud.host.56210: Flags [P.], seq 7882:13674, ack 1, win 501, options [nop,nop,TS val 276726543 ecr 1116025502], length 5792: HTTP
[eu-academy-5]~[10.10.15.99]~[htb-ac-1095115@htb-yfod2hpnw6]~[~]
```

Tips and Tricks



```
[eu-academy-5]~[10.10.15.99]~[htb-ac-1095115@htb-yfod2hpnw6]~[~]
[~]$ sudo tcpdump -i ens3 portrange 0-1024 -w output.pcap
tcpdump: listening on ens3, link-type EN10MB (Ethernet), snapshot length 262144 bytes
^C932 packets captured
988 packets received by filter
0 packets dropped by kernel
[eu-academy-5]~[10.10.15.99]~[htb-ac-1095115@htb-yfod2hpnw6]~[~]
[~]$ sudo tcpdump -Ax output.pcap
reading from file output.pcap, link-type EN10MB (Ethernet), snapshot length 262144
06:32:16.005585 IP htb-yfod2hpnw6.hbt-cloud.com.http > 94-237-101-137.de-htb1.upcloud.host.51938: Flags [P.], seq 2617900456:2617900672, ack 3617700378, win 504, options [nop,nop,TS val 2767823238 ecr 1116122307], length 216: HTTP
E...@. @. [^..4^..e..P... .A....A....B....~...h.m....`.%..+ZI'..+..+..... q..$!+-D"x.....!*2....J1+.U...m]).D.....F....`....l\).(A....H0+Hj.W. ....!....q..#!+..y..h..H....P.....+ "1.
06:32:16.005608 IP htb-yfod2hpnw6.hbt-cloud.com.http > 94-237-101-137.de-htb1.upcloud.host.56210: Flags [P.], seq 3613991317:3613991533, ack 6397475, win 501, options [nop,nop,TS val 2767823238 ecr 1116122334], length 216: HTTP
E...g..@.. @.. ^..4^..e..P... .i!.A.#..A....B....~...h.m....`.%..+ZI'..+..+..... q..$!+-D"x.....!*2....J1+.U...m]).D.....F....`....l\).(A....H0+Hj.W. ....!....q..#!+..g..c..H....P.....+ "b...
06:32:16.005684 IP htb-yfod2hpnw6.hbt-cloud.com.http > 94-237-101-137.de-htb1.upcloud.host.56208: Flags [P.], seq 1289621115:1289621331, ack 2574138431, win 505, options [nop,nop,TS val 2767823238 ecr 1116122334], length 216: HTTP
E....@. @.y^..4^..e..P...L..{.n?....A....B....~...h.m....`.%..+ZI'..+..+..... q..$!+-D"x.....!*2....J1+.U...m]).D.....F....`....l\).(A....H0+Hj.W. ....!....q..#!+..g..c..H....P.....+ ".
06:32:16.005768 IP 94-237-101-137.de-htb1.upcloud.host.51938 > htb-yfod2hpnw6.hbt-cloud.com.http: Flags [.], ack 216, win 13745, options [nop,nop,TS val 1116122367 ecr 2767823205], length 0
[eu-academy-5]~[10.10.15.99]~[htb-ac-1095115@htb-yfod2hpnw6]~[~]
```

Notice how it has the ASCII values shown below each output line because of our use of -A. This can be helpful when quickly looking for something human-readable in the output.

Questions

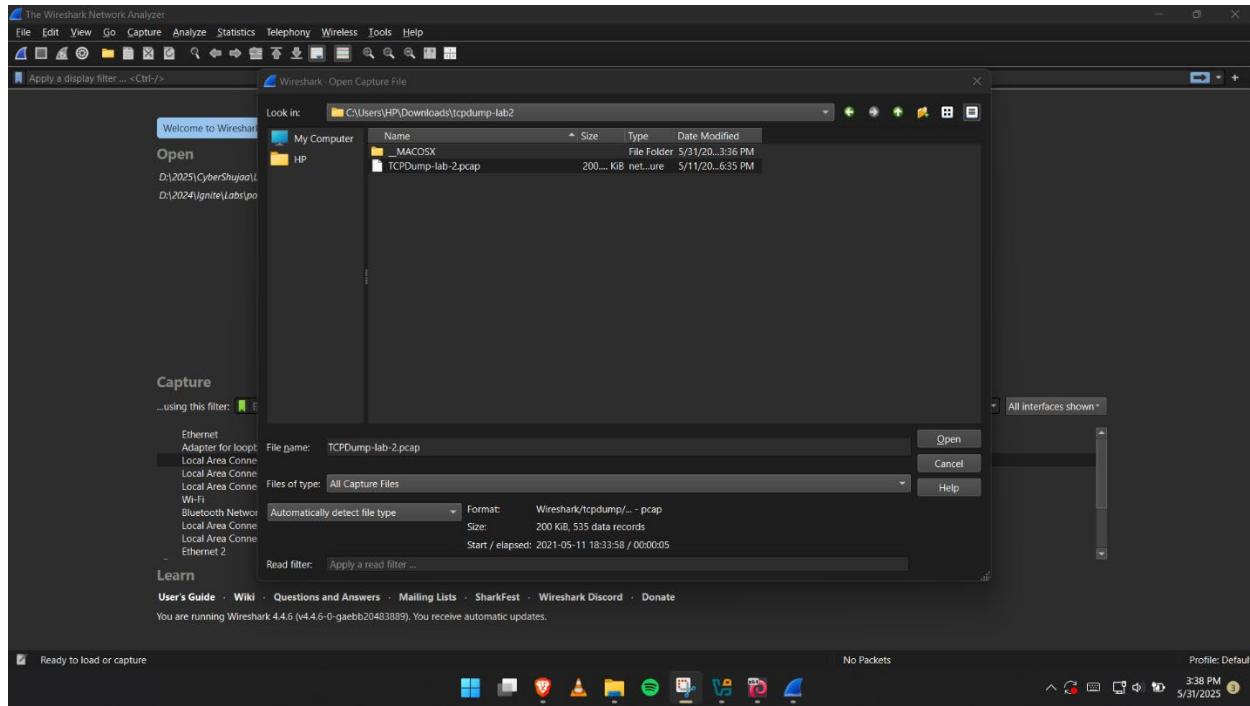
The screenshot shows a web browser window with the URL `academy.hackthebox.com/module/81/section/785`. The page title is "Hack The Box - Academy". The main content area is titled "Questions" and contains three questions:

- What filter will allow me to see traffic coming from or destined to the host with an ip of 10.10.20.1?**
Answer: host 10.10.20.1
Buttons: Submit, Hint
- What filter will allow me to capture based on either of two options?**
Answer: or
Buttons: Submit, Hint
- True or False: TCPDump will resolve IPs to hostnames by default.**
Answer: True
Buttons: Submit, Hint

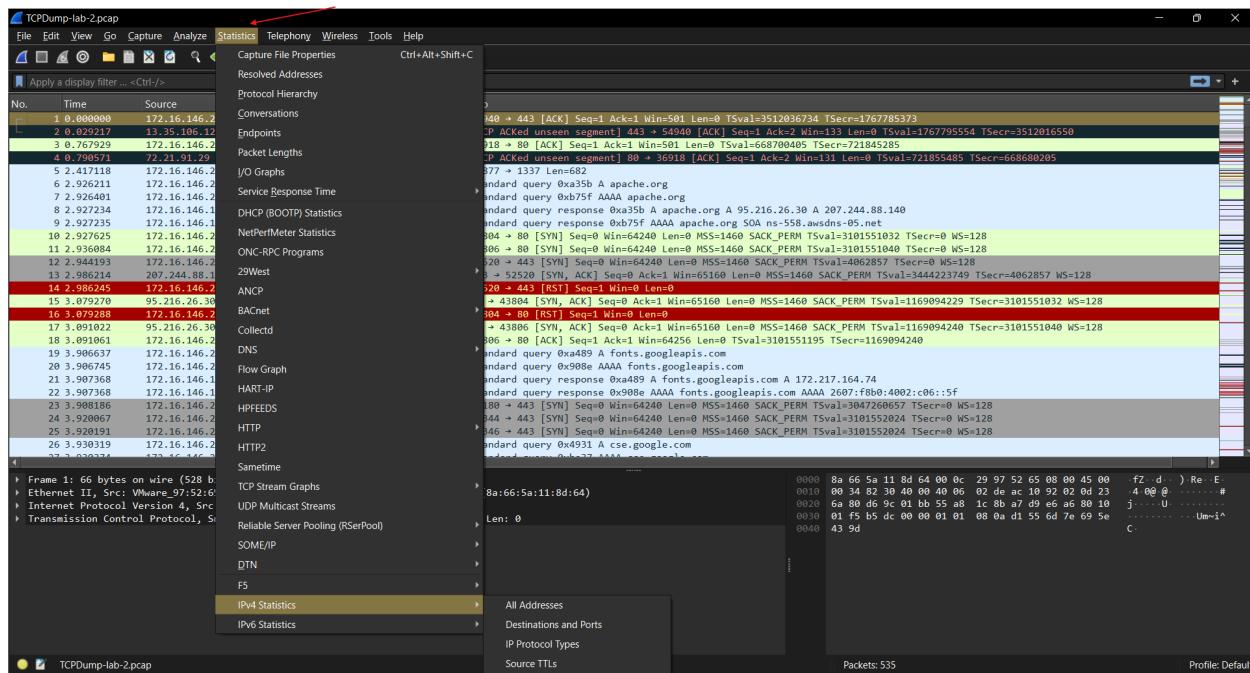
At the bottom of the page, there are navigation buttons for "Previous" and "Next", a "Mark Complete & Next" button, and a "10 Streak pts" badge. The status bar at the bottom right shows the time as 2:36 PM and the date as 5/31/2025.

Analysis with Wireshark

Wireshark is a free and open-source network traffic analyzer much like tcpdump but with a graphical interface. Wireshark is multi-platform and capable of capturing live data off many different interface types (to include WiFi, USB, and Bluetooth) and saving the traffic to several different formats.

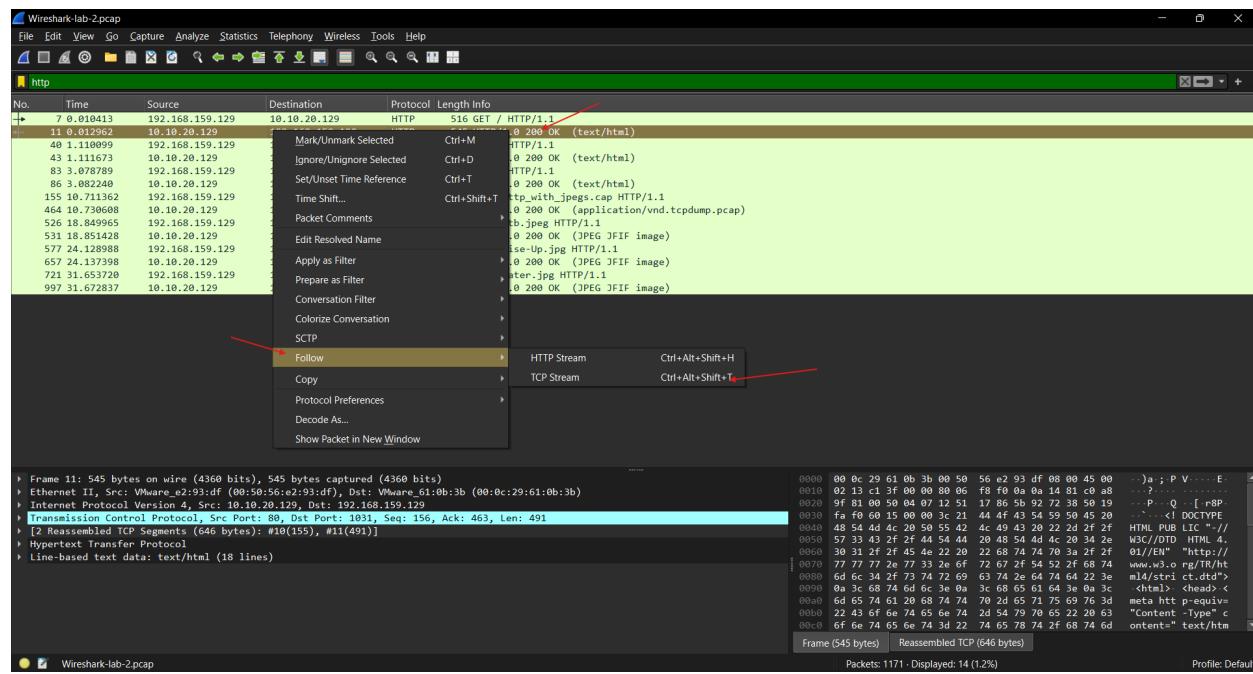
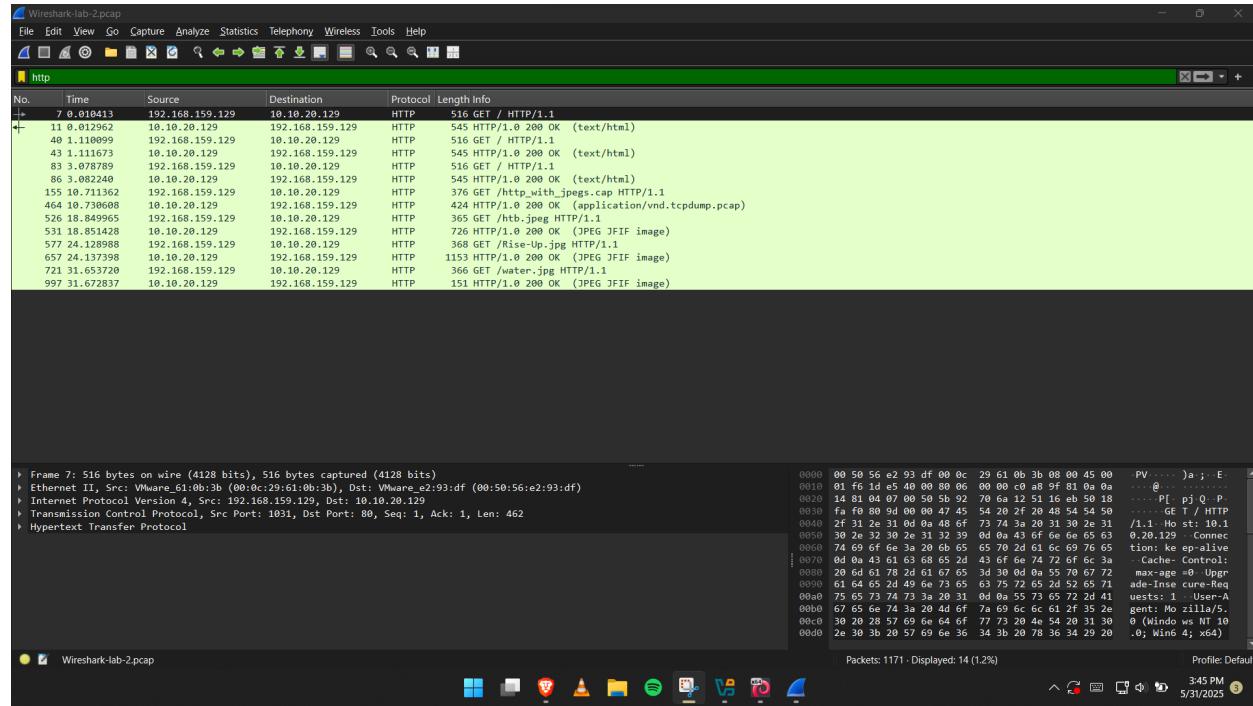


The Statistics tab provides us with great insight into the data we are examining.



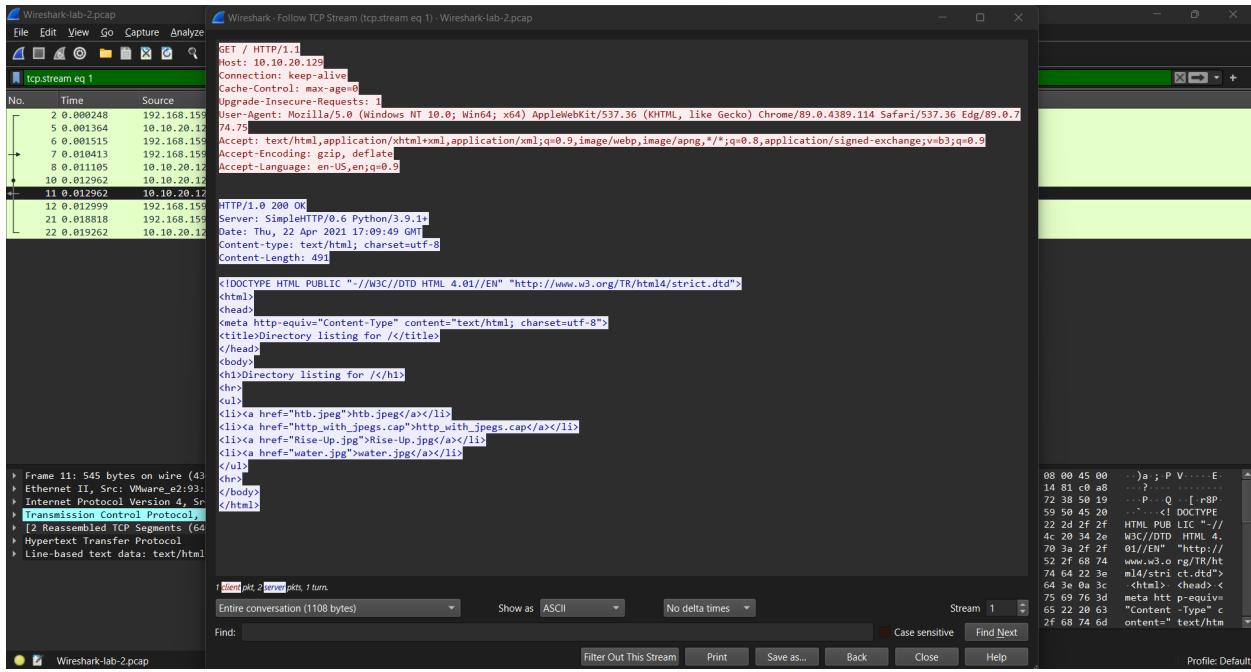
Following TCP Streams

Wireshark can stitch TCP packets back together to recreate the entire stream in a readable format. This ability also allows us to pull data (images, files, etc.) out of the capture. This works for almost any protocol that utilizes TCP as a transport mechanism.



Filter For A Specific TCP Stream

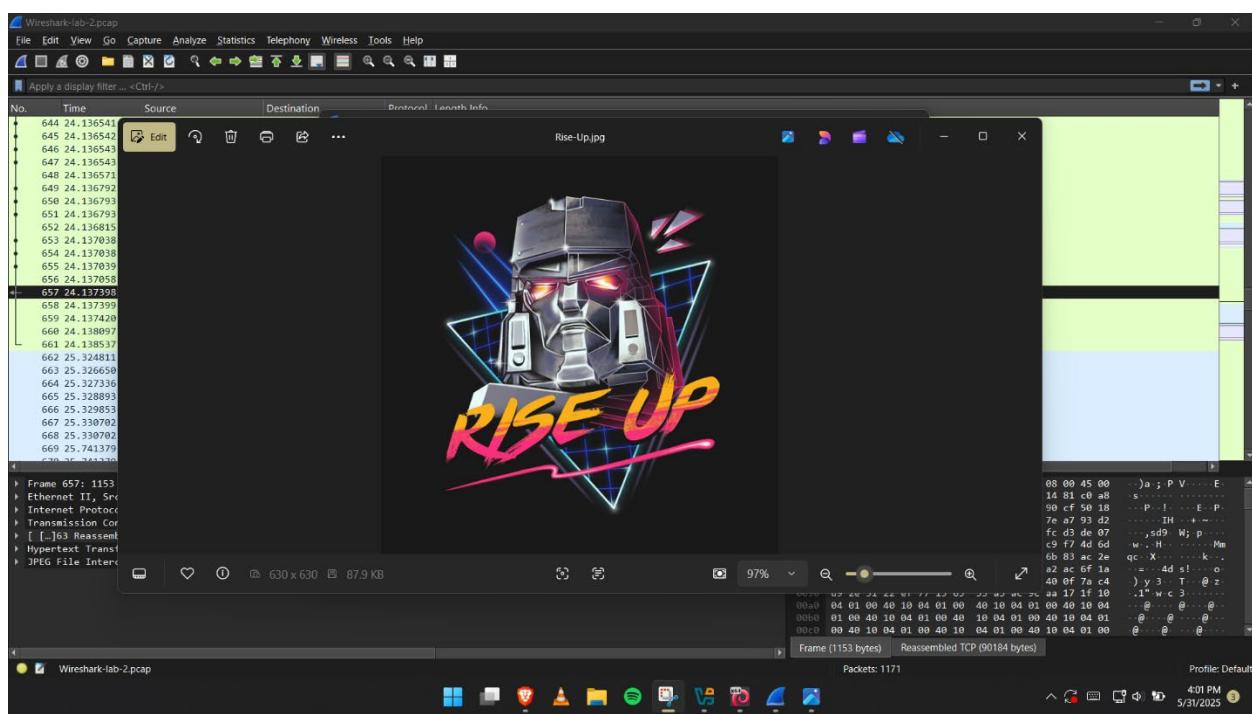
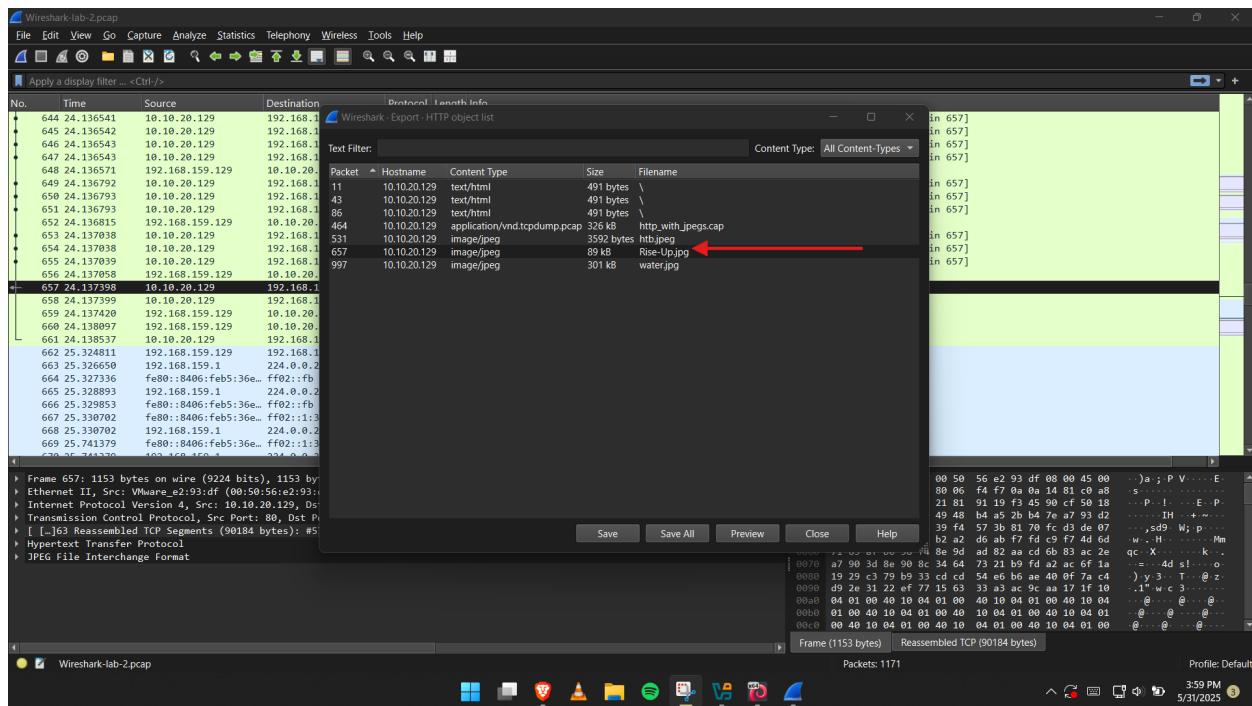
Alternatively, we can utilize the filter `tcp.stream eq ...` to find and track conversations captured in the pcap file for example:

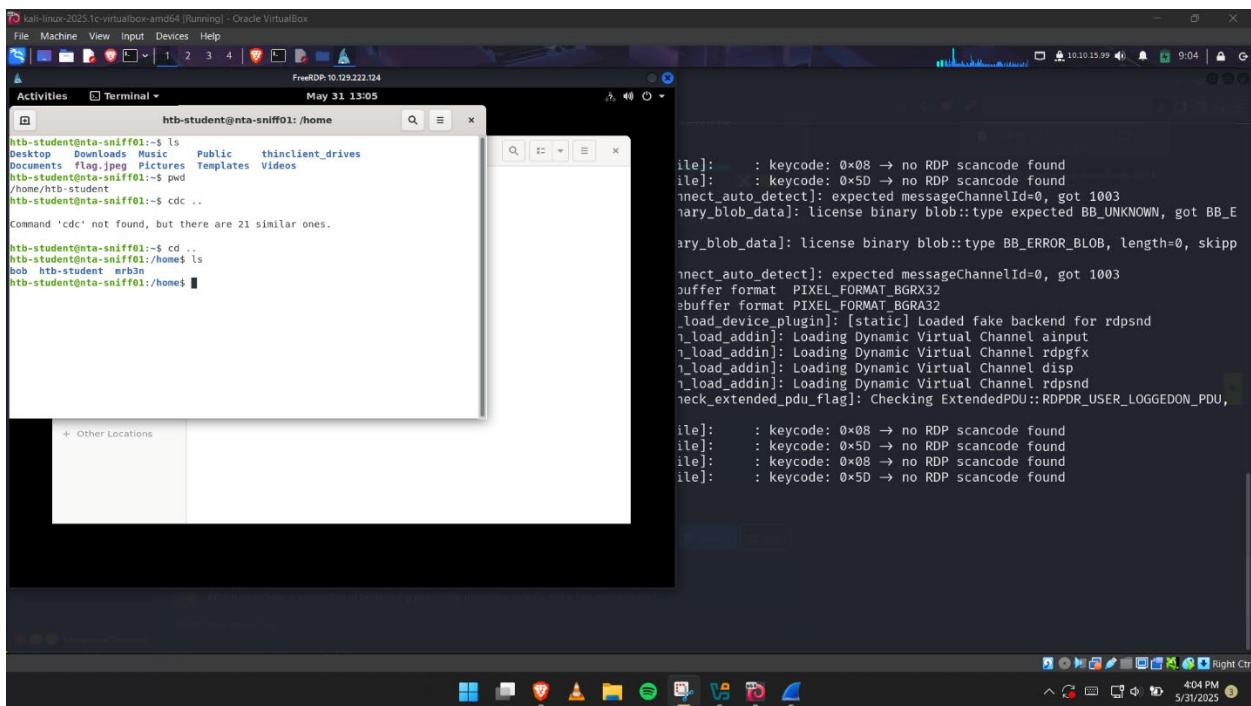


Packet Inception, Dissecting Network Traffic With Wireshark

Tasks

- i. Open a pre-captured file (HTTP extraction).
- ii. Filter the results.
- iii. Follow the stream and extract the item(s) found.





Questions

Answer the question(s) below to complete this Section and earn cubes!

Target(s): **10.129.222.124 (ACADEMY-NTA-SNIFF01)**

Life Left: 17 minute(s) + **Terminate** X

RDP to 10.129.222.124 (ACADEMY-NTA-SNIFF01) with user "**htb-student**" and password "**HTB_@cademy_stdnt!**"

+ 2 What was the filename of the image that contained a certain Transformer Leader? (name.filetype)

Rise-up.jpg

Submit Hint

+ 0 Which employee is suspected of performing potentially malicious actions in the live environment?

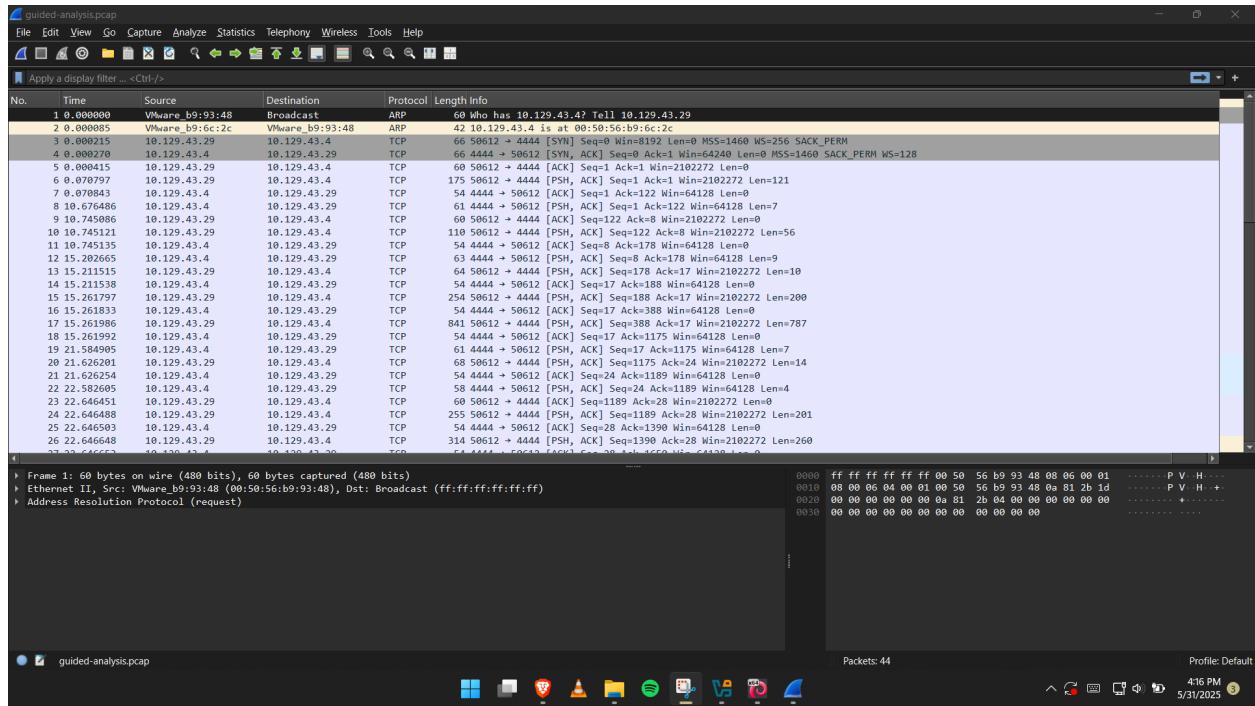
bob

Submit Hint

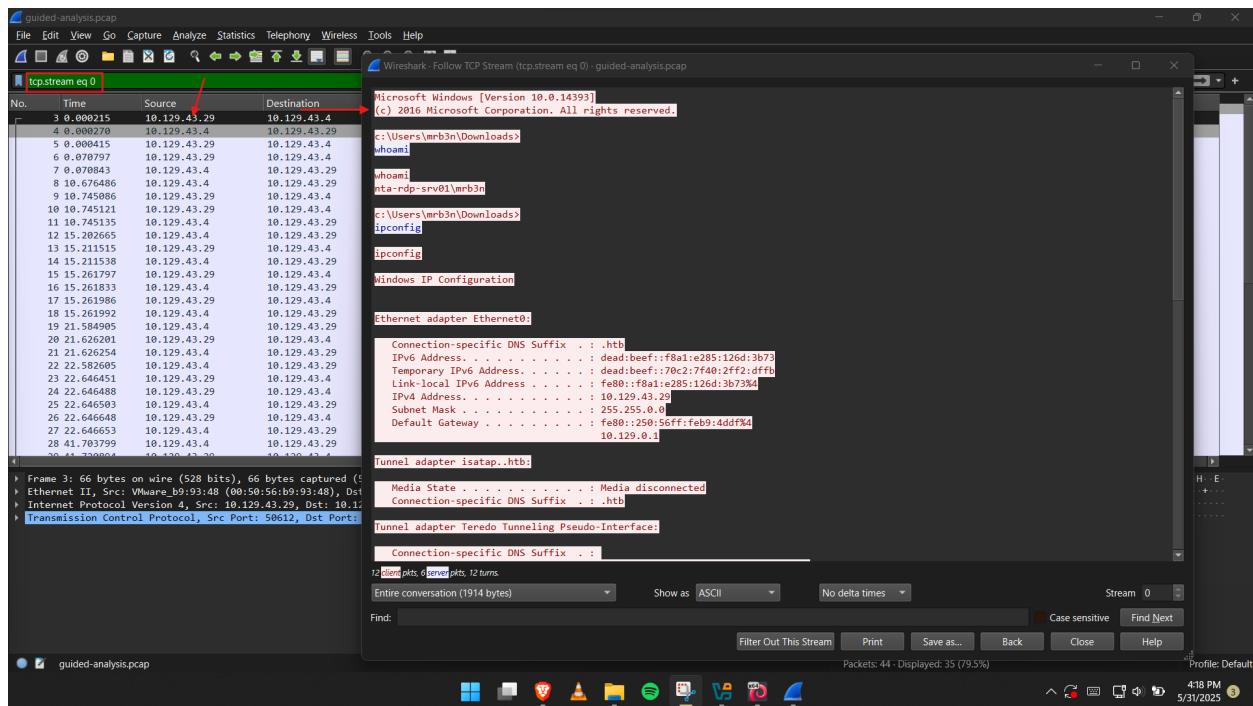
Previous Next Mark Complete & Next

Guided Lab: Traffic Analysis Workflow

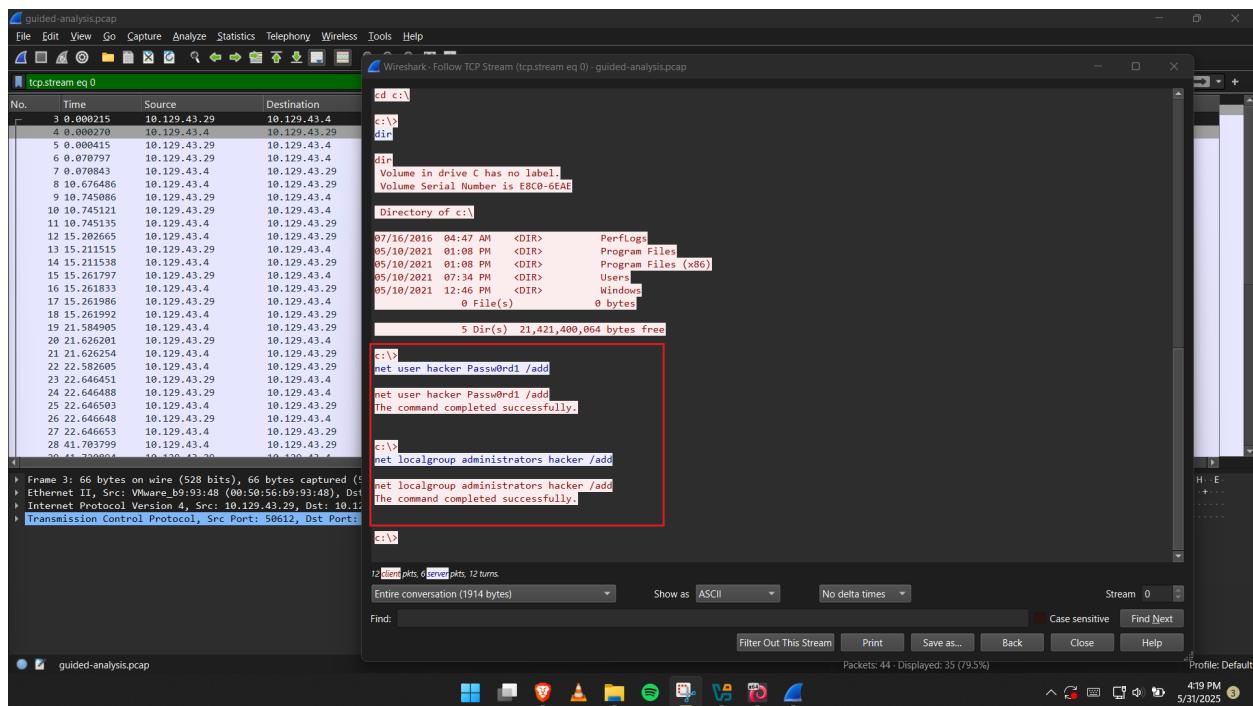
This is an attempt to utilize the concepts from the Analysis Process sections to complete an analysis of the guided-analysis.zip provided in the optional resources and live traffic from the academy network.

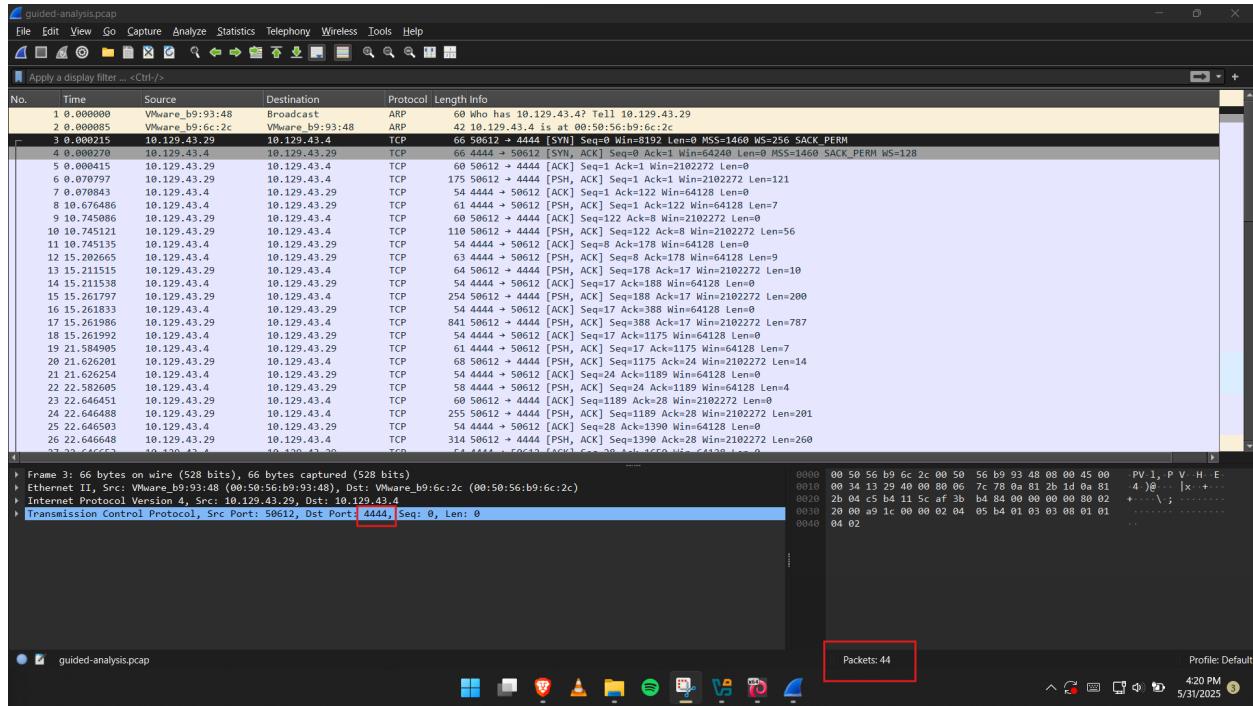


(Overview of the **guided-analysis.pcap** file)



In the above screenshot, I looked at the TCP traffic where I utilized the display filter `!udp && !arp`. the next thing I did was follow the TCP stream and examined it and look at what we got, it appears that someone is performing basic recon of the host. They are issuing commands like `whoami`, `ipconfig`, `dir`. We also see that they created an account `hacker`

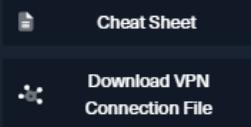




We see the that the total packets of the file are **44** and found the suspicious port that was being used as port **4444**. Which were the answers to the task questions below.

Questions

Answer the question(s) below to complete this Section and earn cubes!



Target(s): 10.129.222.124 (ACADEMY-NTA-SNIFF01)

Life Left: 11 minute(s) + Terminate X

RDP to 10.129.222.124 (ACADEMY-NTA-SNIFF01) with user "htb-student" and password "HTB_@cademy_stdnt!"

+1 🎁 What was the name of the new user created on mrb3n's host?

hacker



+2 🎁 How many total packets were there in the Guided-analysis PCAP?

44



+1 🎁 What was the suspicious port that was being used?

4444

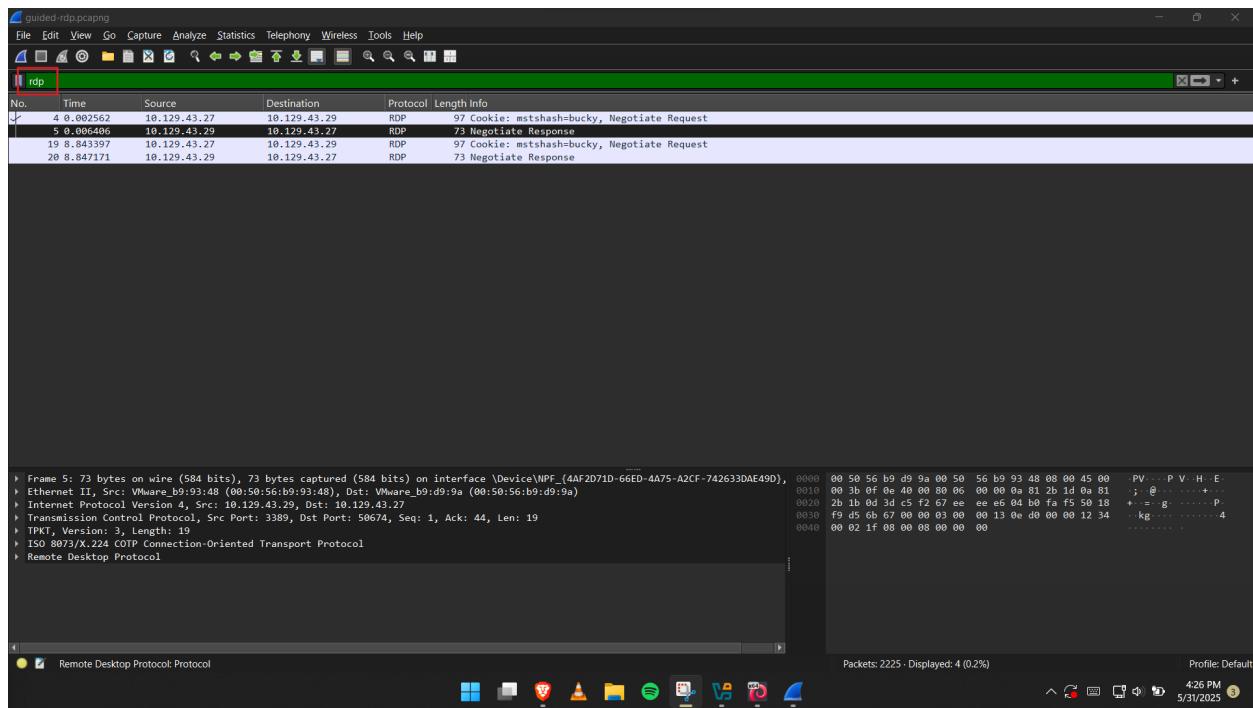


◀ Previous Next ▶

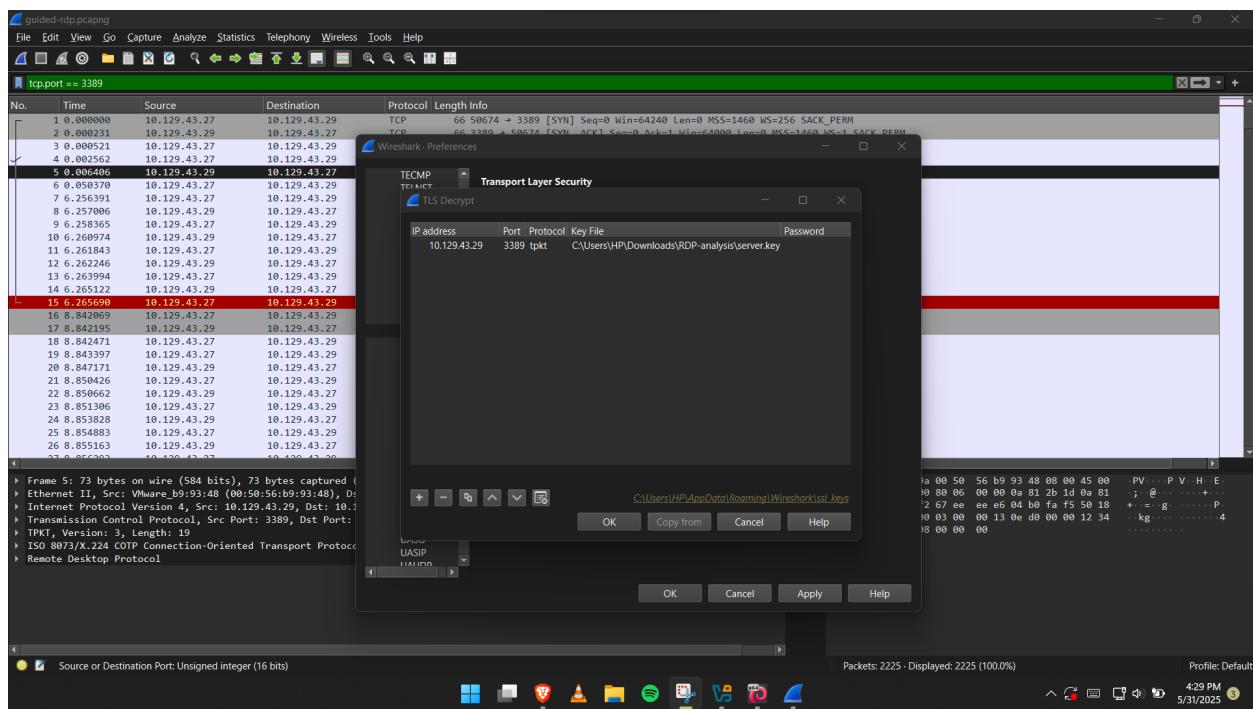
Mark Complete & Next

Decrypting RDP connections

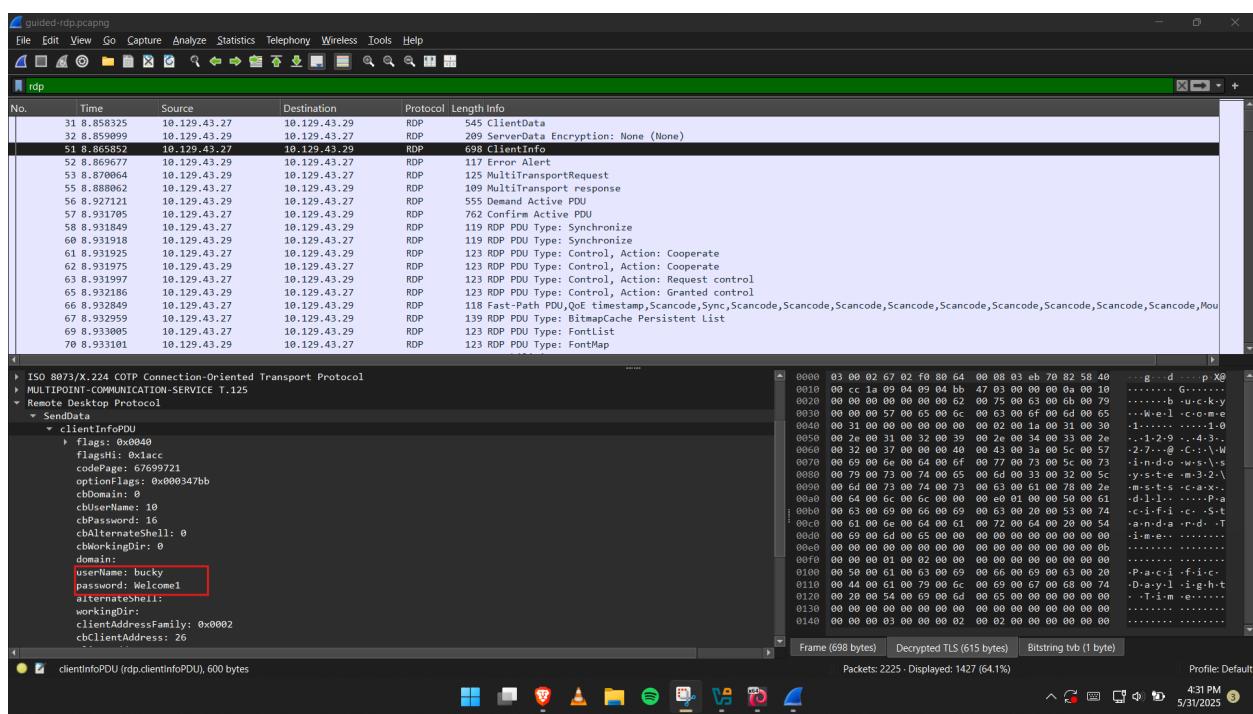
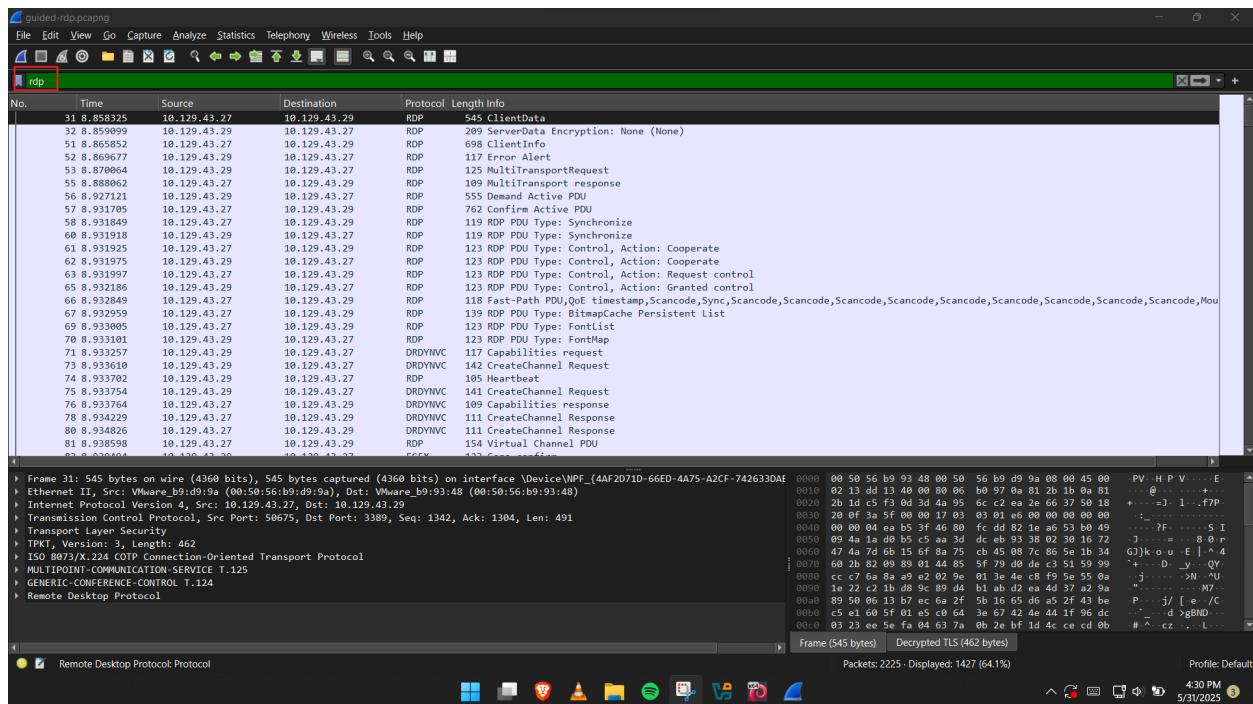
Here we attempt to analyze the RDP-analysis.zip as tasked and first thing first we download the resource and then open the file in Wireshark. Our focus is on RDP so we filtered only *rdp*.



Filter on **port 3389** to determine if any RDP traffic encrypted or otherwise exists and provided the RDP-key to Wireshark so it can decrypt the traffic.



We now able to see more traffic which we couldn't see before as shown in the previous screenshot with **rdp** filter.



Questions

Answer the question(s) below to complete this Section and earn cubes!

Target(s): [Click here to spawn the target system!](#)

+ 2 What user account was used to initiate the RDP connection?

bucky

Submit Hint

Previous Finish

Summary

This lab was to serve as an example of what Wireshark can do with captured data and its plugins. Wireshark's capability to ingest information and illuminate the obscure is robust. Having the ability to decrypt data after ingestion is a powerful capability. This concept could be applied to any protocol that utilizes encryption as long as we have the key that will be utilized to establish the connections.