**COURSE: CLOUD AND NETWORK SECURITY _C1_2025**

**STUDENT NAME: DIANA ROSE OGUDA**

**STUDENT NUMBER: CS-CNS09-25172**

**SATURDAY ,31 MAY,2025**

# WEEK 2 ASSIGNMENT 2

# HTB ACADEMY: INTRODUCTION TO NETWORK TRAFFIC ANALYSIS

# - ASSIGNMENT REPORT

# 1. Introduction

Network traffic analysis is a critical skill in cybersecurity and IT operations. This assignment was aimed at exploring the core concepts and tools used in analyzing network traffic. The goal was to understand how packets are structured and transmitted, how traffic can be captured and filtered, and how tools like tcpdump and Wireshark can be used to detect malicious activity or performance issues.

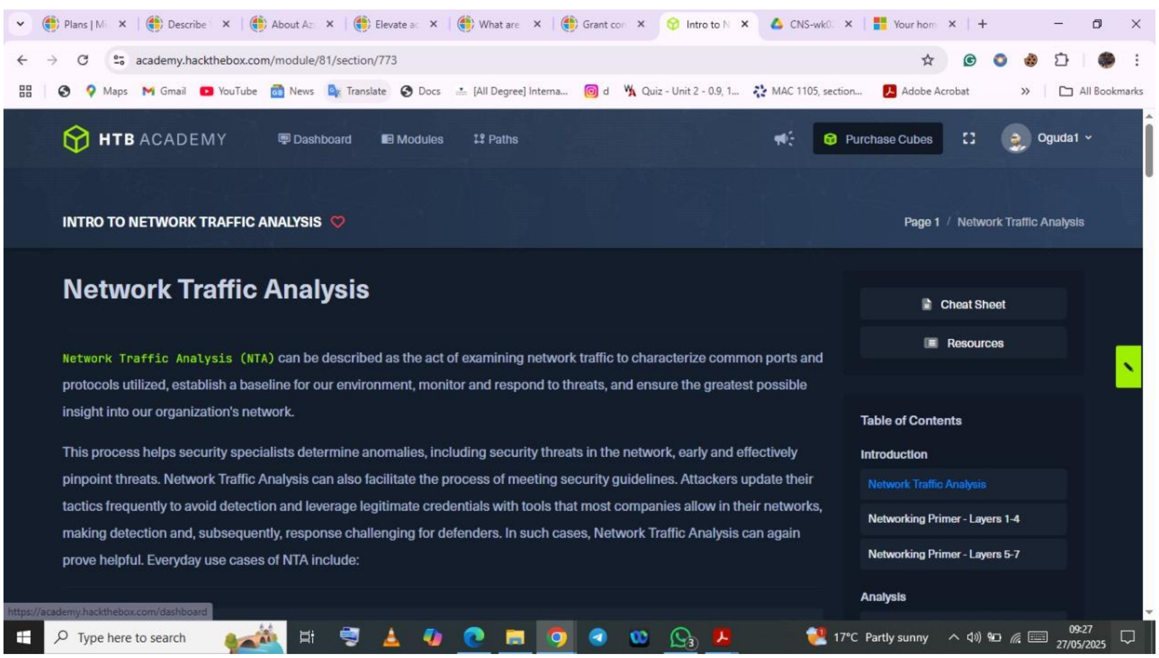
By completing the "Intro to Network Traffic Analysis (Tier 0)" module on Hack The Box Academy, I gained practical insights into inspecting data across the OSI model, capturing and dissecting packets, applying filters, and even decrypting encrypted traffic like RDP sessions. The hands-on labs provided real-world scenarios that helped reinforce theoretical knowledge with practical application.

# 2. Modules

## Introduction

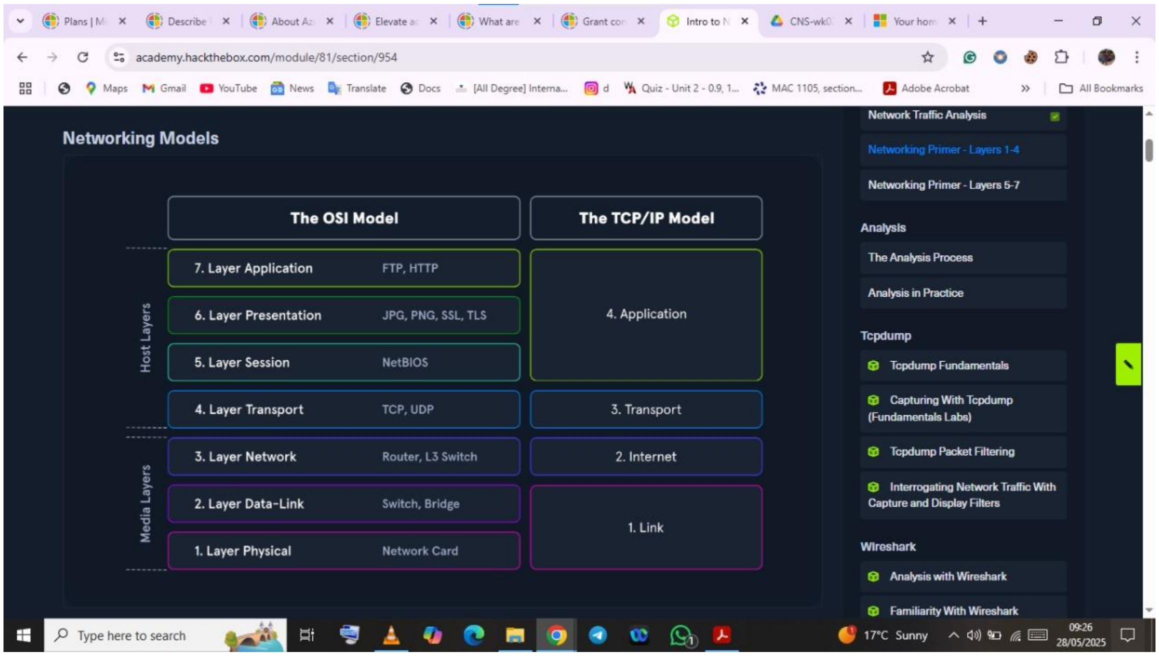
### Network Traffic Analysis

Introduces network traffic fundamentals and their importance in monitoring and security. Emphasizes packet-level inspection.



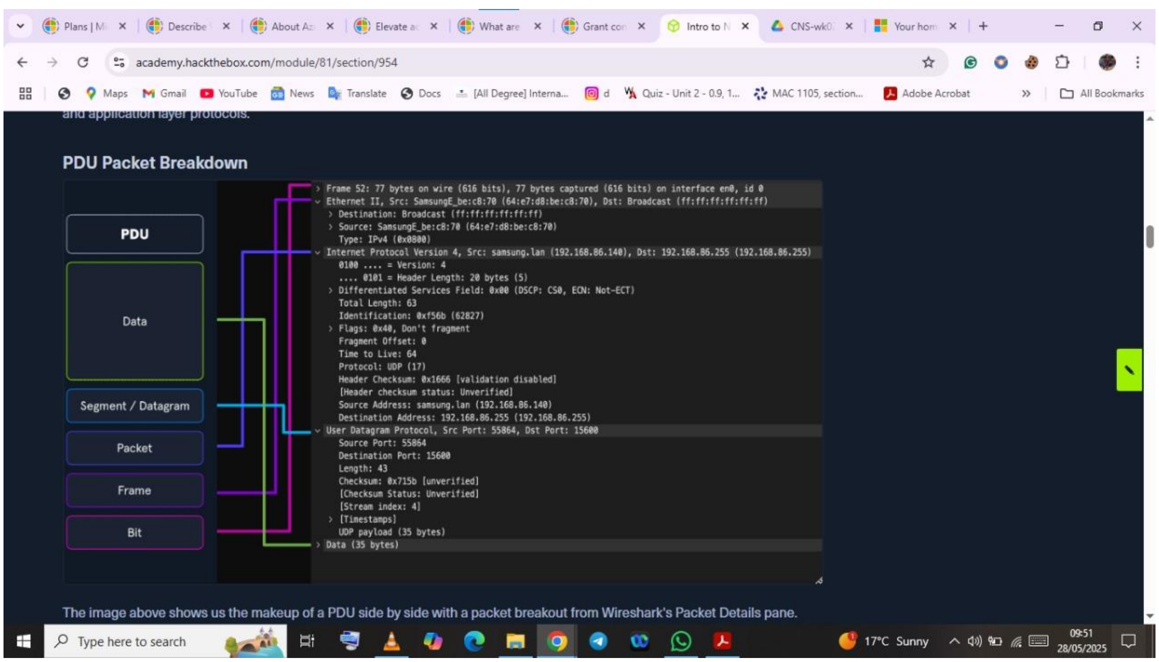

### Networking Primer – Layers 1–4

Explains the lower OSI layers, detailing how data moves through physical and logical channels using MAC addresses, IPs, and transport protocols like TCP/UDP.




### Networking Primer – Layers 5–7

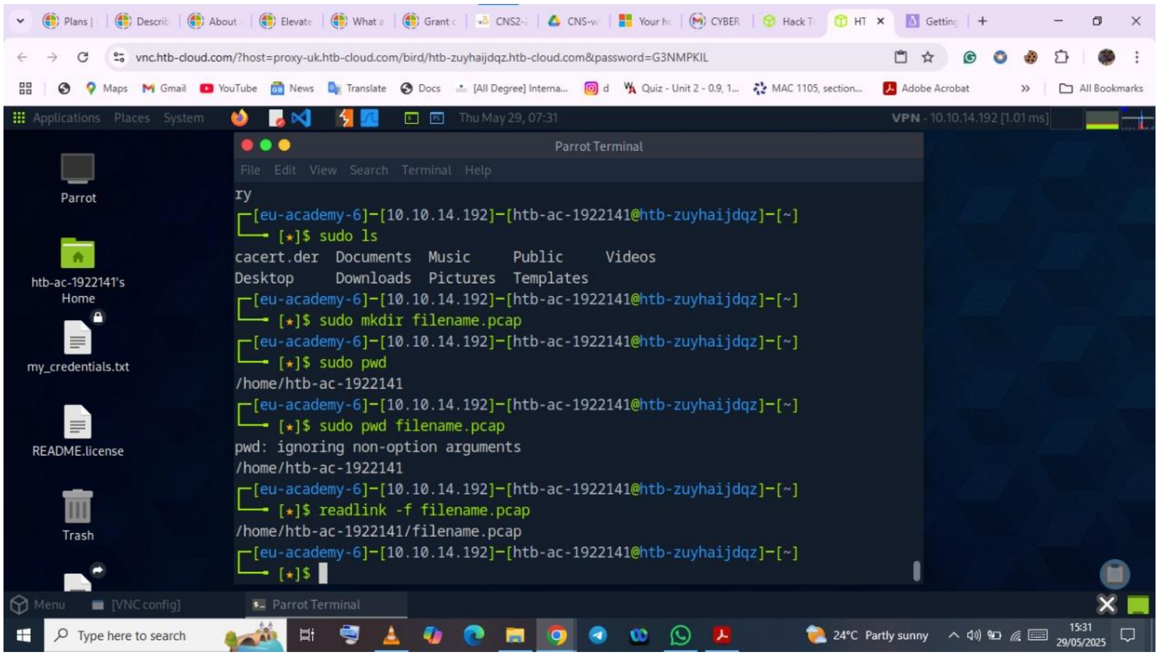
Covers upper OSI layers where session handling, data translation, and application interfaces are managed.




## Analysis

### The Analysis Process

Outlines steps in network traffic analysis: setting objectives, capturing data, applying filters, analyzing patterns, and deriving insights.




### Analysis in Practice

Provides applied practice on real packet captures, teaching how to identify anomalies and extract meaningful information.

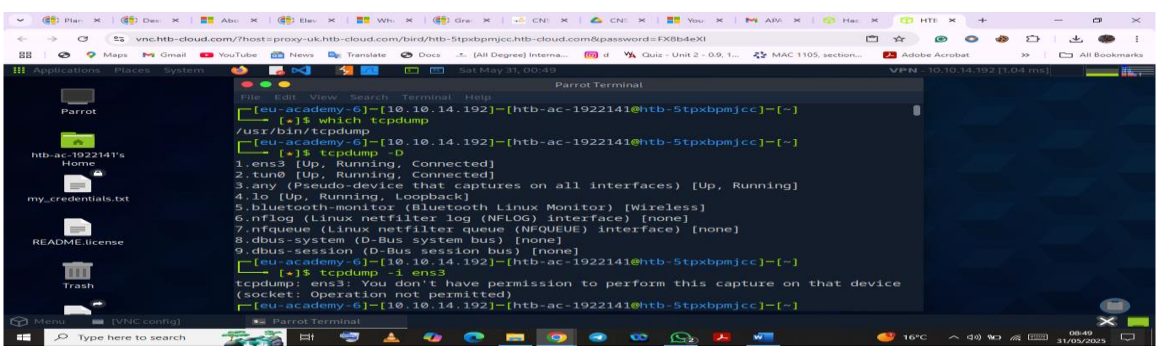
## Tcpdump

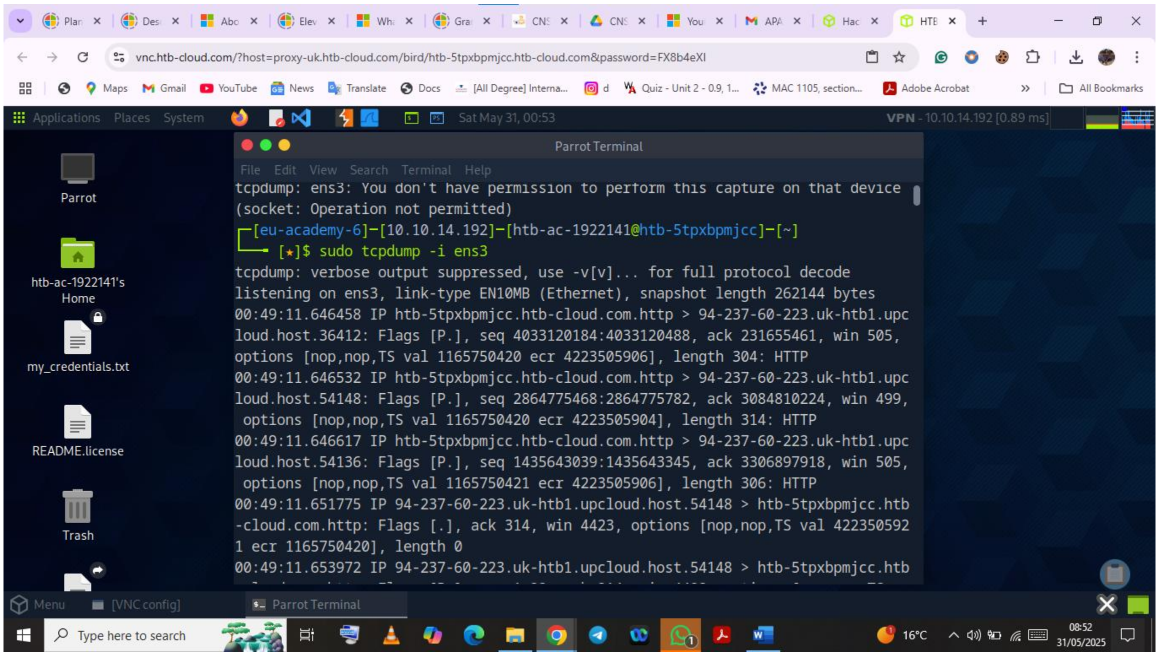
### Tcpdump Fundamentals

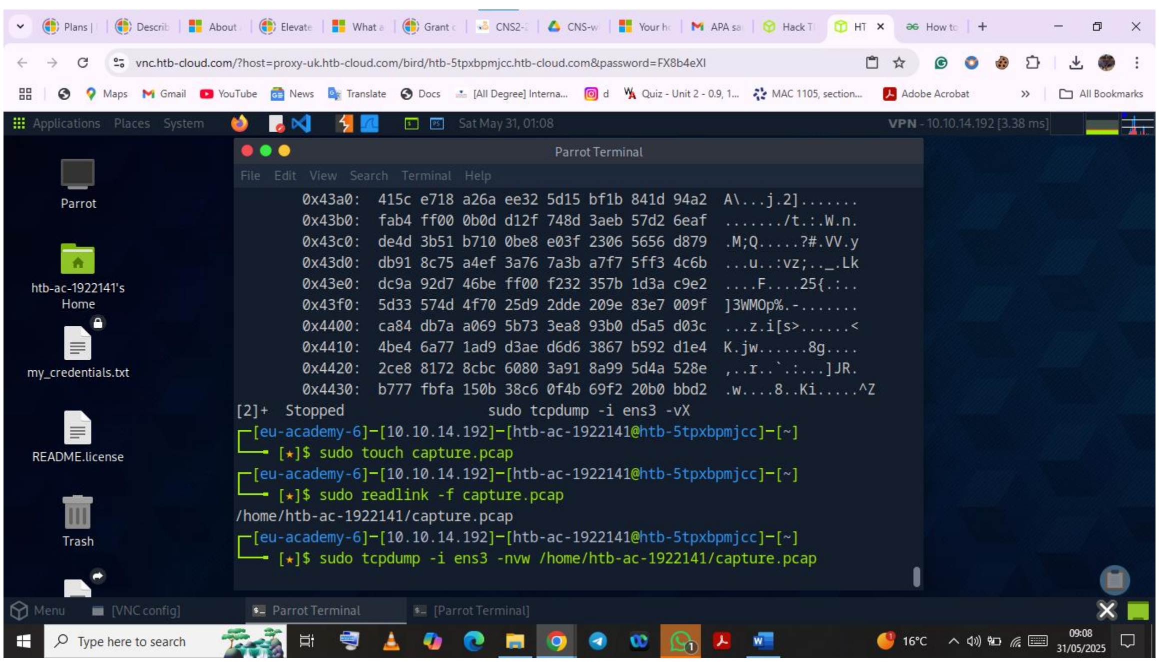
Introduces tcpdump for command-line-based packet capturing. Covers interface selection and output interpretation.

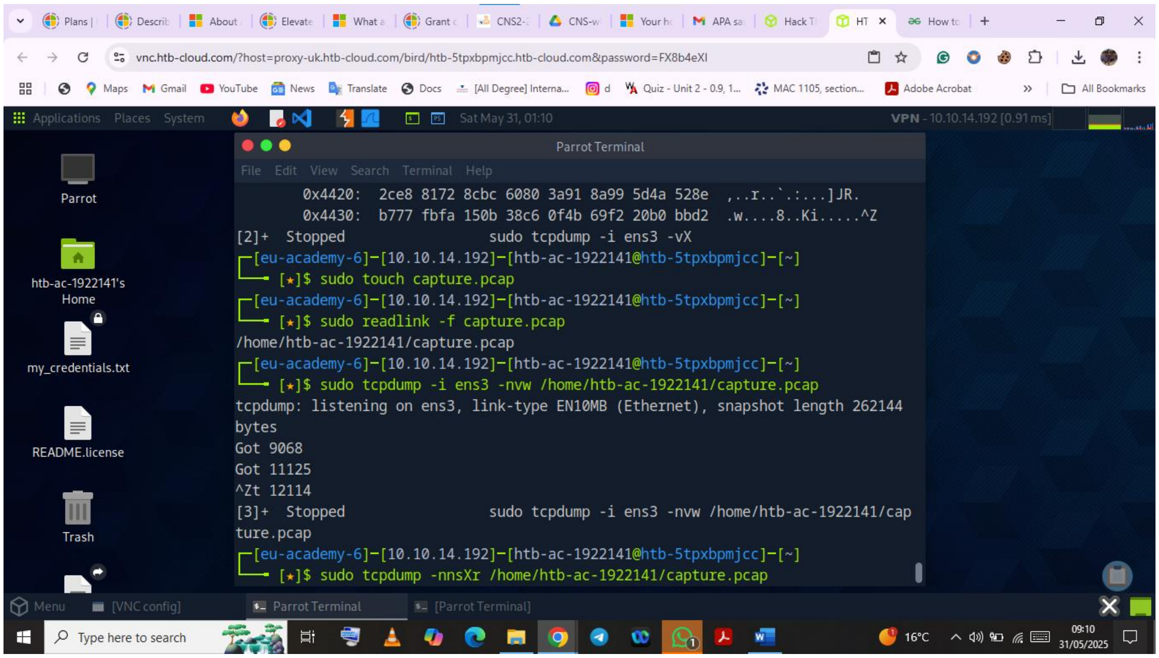
### Capturing With Tcpdump (Fundamentals Labs)

Hands-on lab to practice capturing traffic and saving it for analysis.



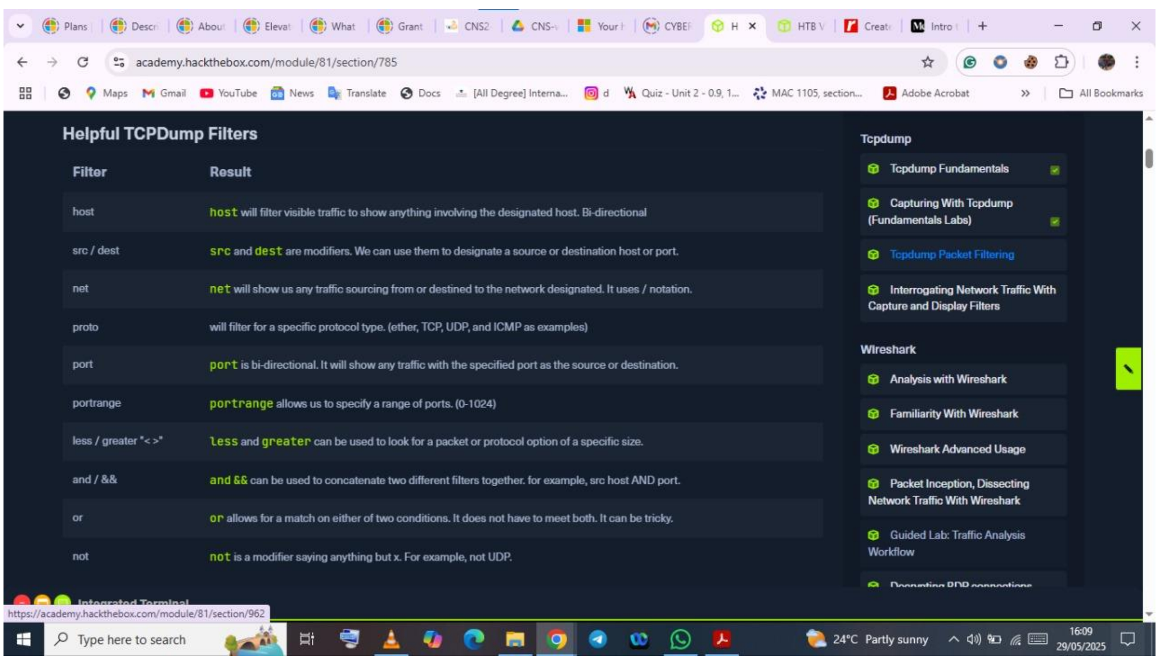

vnc.htb-cloud.com/?host=proxy-uk.htb-cloud.com/bird/htb-5tpxbpmjcc.htb-cloud.com&password=FX8b4eXI
Parrot Terminal
tcpdump: ens3: You don't have permission to perform this capture on that device
(socket: Operation not permitted)
┌[eu-academy-6]─[10.10.14.192]─[htb-ac-1922141@htb-5tpxbpmjcc]─[~]
└──╼ [★]$ 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
00:49:11.646458 IP htb-5tpxbpmjcc.htb-cloud.com.http > 94-237-60-223.uk-htb1.upcloud.host.36412: Flags [P.], seq 4033120184:4033120488, ack 231655461, win 505, options [nop,nop,TS val 1165750420 ecr 4223505906], length 304: HTTP
00:49:11.646532 IP htb-5tpxbpmjcc.htb-cloud.com.http > 94-237-60-223.uk-htb1.upcloud.host.54148: Flags [P.], seq 2864775468:2864775782, ack 3084810224, win 499, options [nop,nop,TS val 1165750420 ecr 4223505904], length 314: HTTP
00:49:11.646617 IP htb-5tpxbpmjcc.htb-cloud.com.http > 94-237-60-223.uk-htb1.upcloud.host.54136: Flags [P.], seq 1435643039:1435643345, ack 3306897918, win 505, options [nop,nop,TS val 1165750421 ecr 4223505906], length 306: HTTP
00:49:11.651775 IP 94-237-60-223.uk-htb1.upcloud.host.54148 > htb-5tpxbpmjcc.htb-cloud.com.http: Flags [.], ack 314, win 4423, options [nop,nop,TS val 4223505921 ecr 1165750420], length 0
00:49:11.653972 IP 94-237-60-223.uk-htb1.upcloud.host.54148 > htb-5tpxbpmjcc.htb


vnc.htb-cloud.com/?host=proxy-uk.htb-cloud.com/bird/htb-5tpxbpmjcc.htb-cloud.com&password=FX8b4eXI
Parrot Terminal
0x43a0: 415c e718 a26a ee32 5d15 bf1b 841d 94a2 A\...j.2].......
0x43b0: fab4 ff00 0b0d d12f 748d 3aeb 57d2 6eaf ......./t.:.W.n.
0x43c0: de4d 3b51 b710 0be8 e03f 2306 5656 d879 .M;Q.....?#.VV.y
0x43d0: db91 8c75 a4ef 3a76 7a3b a7f7 5ff3 4c6b ...u..:vz;.._.Lk
0x43e0: dc9a 92d7 46be ff00 f232 357b 1d3a c9e2 ....F....25{.:..
0x43f0: 5d33 574d 4f70 25d9 2dde 209e 83e7 009f ]3WMOp%.-.......
0x4400: ca84 db7a a069 5b73 3ea8 93b0 d5a5 d03c ...z.i[s>......<
0x4410: 4be4 6a77 1ad9 d3ae d6d6 3867 b592 d1e4 K.jw......8g....
0x4420: 2ce8 8172 8cbc 6080 3a91 8a99 5d4a 528e ,..r..`.:...]JR.
0x4430: b777 fbfa 150b 38c6 0f4b 69f2 20b0 bbd2 .w....8..Ki.....^Z
[2]+ Stopped sudo tcpdump -i ens3 -vX
┌[eu-academy-6]─[10.10.14.192]─[htb-ac-1922141@htb-5tpxbpmjcc]─[~]
└──╼ [★]$ sudo touch capture.pcap
┌[eu-academy-6]─[10.10.14.192]─[htb-ac-1922141@htb-5tpxbpmjcc]─[~]
└──╼ [★]$ sudo readlink -f capture.pcap
/home/htb-ac-1922141/capture.pcap
┌[eu-academy-6]─[10.10.14.192]─[htb-ac-1922141@htb-5tpxbpmjcc]─[~]
└──╼ [★]$ sudo tcpdump -i ens3 -nvw /home/htb-ac-1922141/capture.pcap




## Tcpdump Packet Filtering

Teaches how to narrow down captured data using filters by IP, port, and protocol.

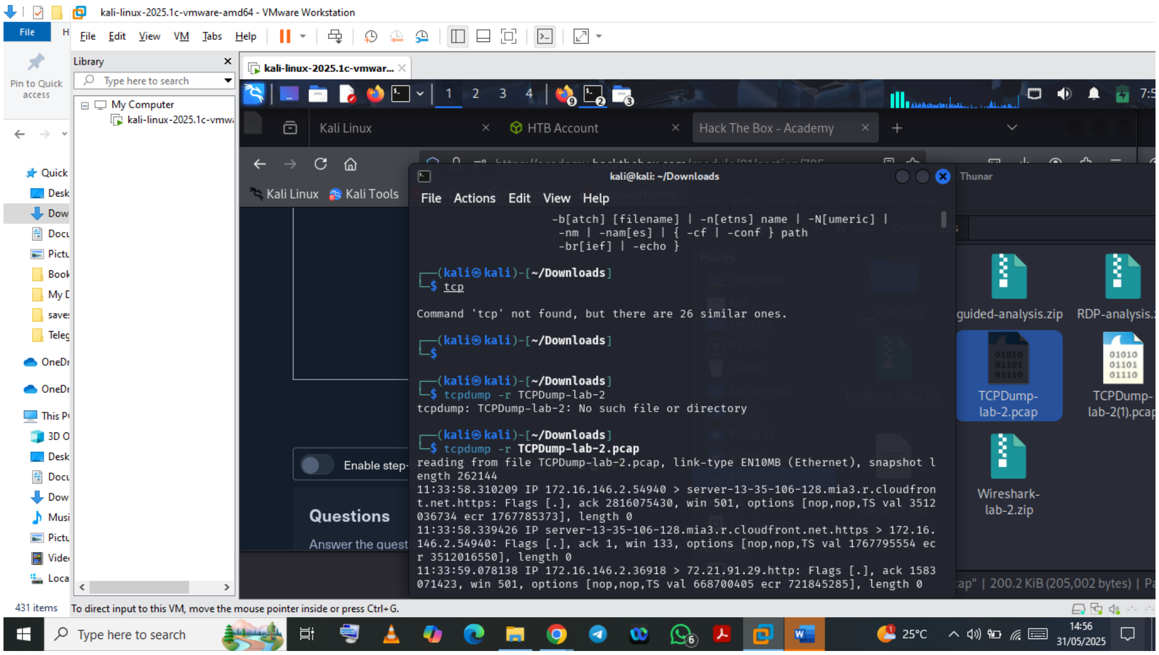



## Interrogating Network Traffic With Capture and Display Filters

Enhances filtering skills using advanced options to target specific network activities.

### Task #1

Read a capture from a file without filters implemented.




**Task #2**

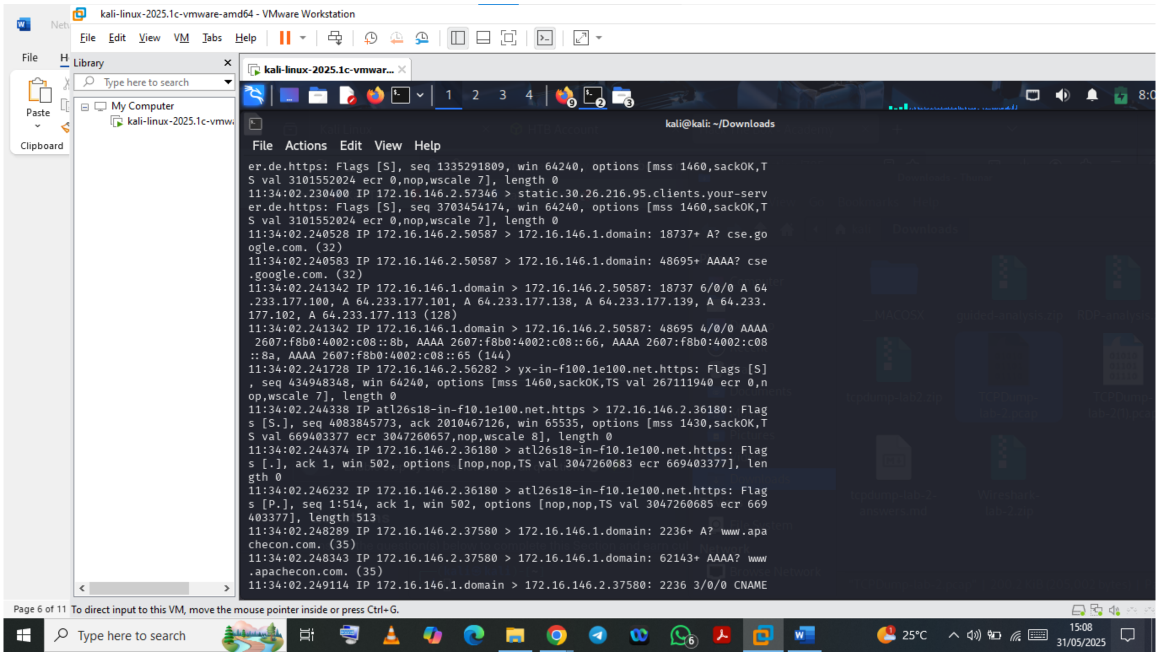
Identify the type of traffic seen.

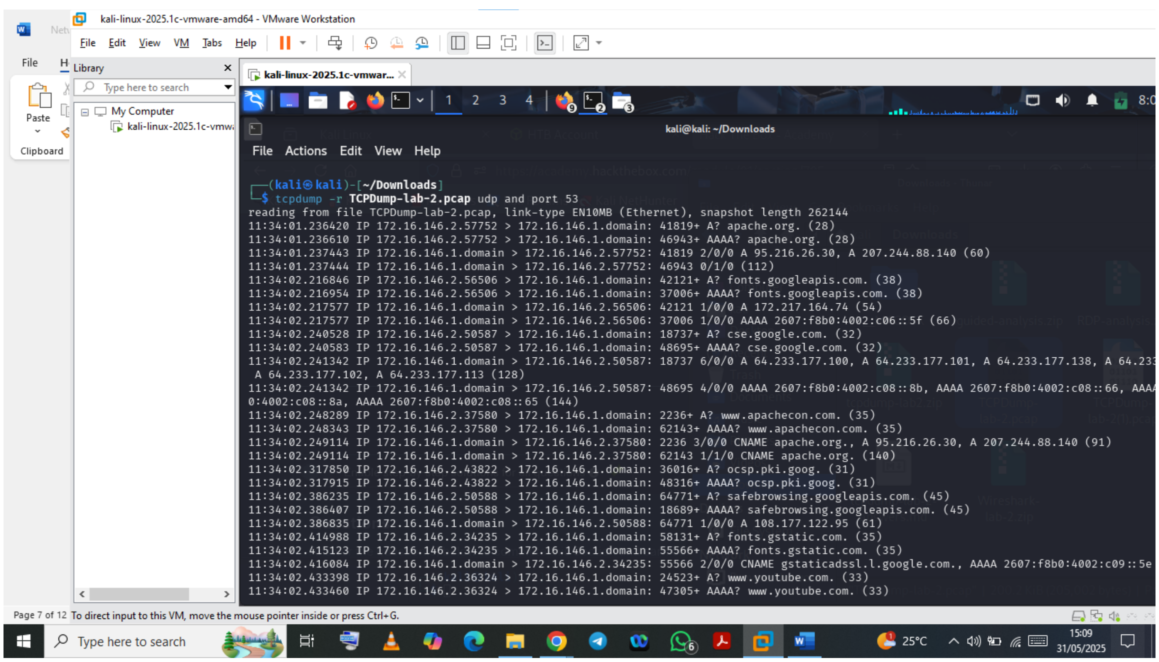
Common protocols: HTTP/HTTPS/DNS

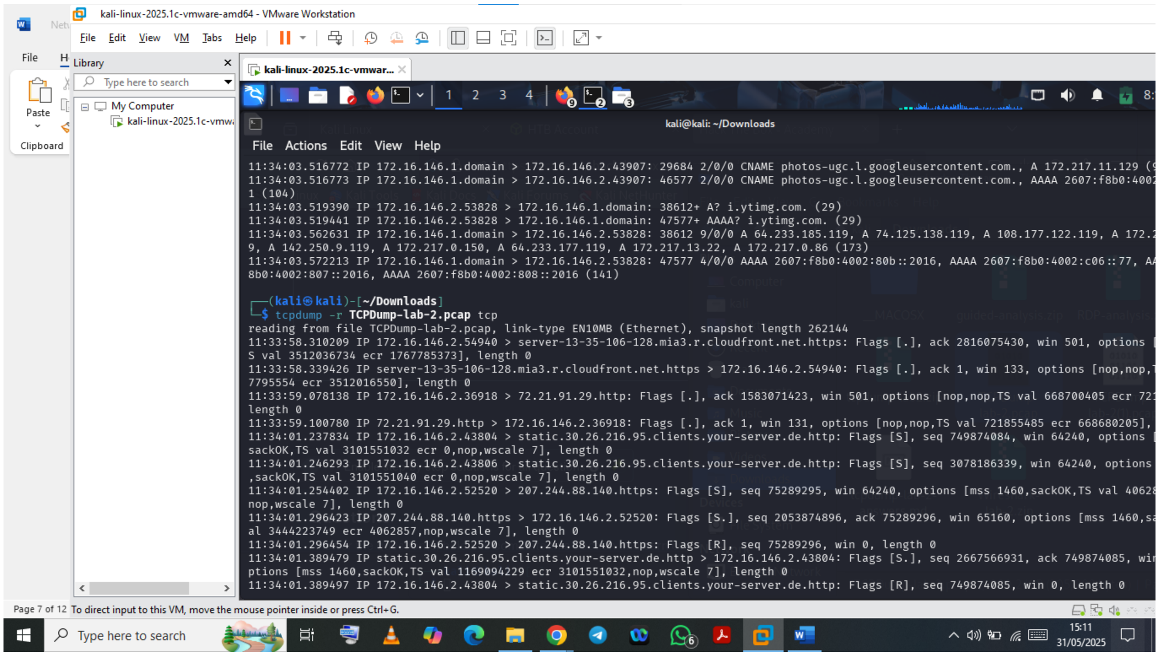
Ports utilized:53/80/443

**Task #3**

Identify conversations.


kali-linux-2025.1c-vmware-amd64 - VMware Workstation
kali@kali: ~/Downloads
File Actions Edit View Help
er.de.https: Flags [S], seq 1335291809, win 64240, options [mss 1460,sackOK,TS val 3101552024 ecr 0,nop,wscale 7], length 0
11:34:02.230400 IP 172.16.146.2.57346 > static.30.26.216.95.clients.your-server.de.https: Flags [S], seq 3703454174, win 64240, options [mss 1460,sackOK,TS val 3101552024 ecr 0,nop,wscale 7], length 0
11:34:02.240528 IP 172.16.146.2.50587 > 172.16.146.1.domain: 18737+ A? cse.google.com. (32)
11:34:02.240583 IP 172.16.146.2.50587 > 172.16.146.1.domain: 48695+ AAAA? cse.google.com. (32)
11:34:02.241342 IP 172.16.146.1.domain > 172.16.146.2.50587: 18737 6/0/0 A 64.233.177.100, A 64.233.177.101, A 64.233.177.138, A 64.233.177.139, A 64.233.177.102, A 64.233.177.113 (128)
11:34:02.241342 IP 172.16.146.1.domain > 172.16.146.2.50587: 48695 4/0/0 AAAA 2607:f8b0:4002:c08::8b, AAAA 2607:f8b0:4002:c08::66, AAAA 2607:f8b0:4002:c08::8a, AAAA 2607:f8b0:4002:c08::65 (144)
11:34:02.241728 IP 172.16.146.2.56282 > yx-in-f100.1e100.net.https: Flags [S], seq 434948348, win 64240, options [mss 1460,sackOK,TS val 267111940 ecr 0,nop,wscale 7], length 0
11:34:02.244338 IP atl26s18-in-f10.1e100.net.https > 172.16.146.2.36180: Flags [S.], seq 4083845773, ack 2010467126, win 65535, options [mss 1430,sackOK,TS val 669403377 ecr 3047260657,nop,wscale 8], length 0
11:34:02.244374 IP 172.16.146.2.36180 > atl26s18-in-f10.1e100.net.https: Flags [.], ack 1, win 502, options [nop,nop,TS val 3047260683 ecr 669403377], length 0
11:34:02.246232 IP 172.16.146.2.36180 > atl26s18-in-f10.1e100.net.https: Flags [P.], seq 1:514, ack 1, win 502, options [nop,nop,TS val 3047260685 ecr 669403377], length 513
11:34:02.248289 IP 172.16.146.2.37580 > 172.16.146.1.domain: 2236+ A? www.apachecon.com. (35)
11:34:02.248343 IP 172.16.146.2.37580 > 172.16.146.1.domain: 62143+ AAAA? www.apachecon.com. (35)
11:34:02.249114 IP 172.16.146.1.domain > 172.16.146.2.37580: 2236 3/0/0 CNAME
Page 6 of 11 To direct input to this VM, move the mouse pointer inside or press Ctrl+G.
Type here to search
25°C
15:08
31/05/2025


kali-linux-2025.1c-vmware-amd64 - VMware Workstation
kali@kali: ~/Downloads
File Actions Edit View Help
(kali㉿kali)-[~/Downloads]
$ tcpdump -r TCPDump-lab-2.pcap udp and port 53
reading from file TCPDump-lab-2.pcap, link-type EN10MB (Ethernet), snapshot length 262144
11:34:01.236420 IP 172.16.146.2.57752 > 172.16.146.1.domain: 41819+ A? apache.org. (28)
11:34:01.236610 IP 172.16.146.2.57752 > 172.16.146.1.domain: 46943+ AAAA? apache.org. (28)
11:34:01.237443 IP 172.16.146.1.domain > 172.16.146.2.57752: 41819 2/0/0 A 95.216.26.30, A 207.244.88.140 (60)
11:34:01.237444 IP 172.16.146.1.domain > 172.16.146.2.57752: 46943 0/1/0 (112)
11:34:02.216846 IP 172.16.146.2.56506 > 172.16.146.1.domain: 42121+ A? fonts.googleapis.com. (38)
11:34:02.216954 IP 172.16.146.2.56506 > 172.16.146.1.domain: 37006+ AAAA? fonts.googleapis.com. (38)
11:34:02.217577 IP 172.16.146.1.domain > 172.16.146.2.56506: 42121 1/0/0 A 172.217.164.74 (54)
11:34:02.217577 IP 172.16.146.1.domain > 172.16.146.2.56506: 37006 1/0/0 AAAA 2607:f8b0:4002:c06::5f (66)
11:34:02.240528 IP 172.16.146.2.50587 > 172.16.146.1.domain: 18737+ A? cse.google.com. (32)
11:34:02.240583 IP 172.16.146.2.50587 > 172.16.146.1.domain: 48695+ AAAA? cse.google.com. (32)
11:34:02.241342 IP 172.16.146.1.domain > 172.16.146.2.50587: 18737 6/0/0 A 64.233.177.100, A 64.233.177.101, A 64.233.177.138, A 64.233
A 64.233.177.102, A 64.233.177.113 (128)
11:34:02.241342 IP 172.16.146.1.domain > 172.16.146.2.50587: 48695 4/0/0 AAAA 2607:f8b0:4002:c08::8b, AAAA 2607:f8b0:4002:c08::66, AAAA
0:4002:c08::8a, AAAA 2607:f8b0:4002:c08::65 (144)
11:34:02.248289 IP 172.16.146.2.37580 > 172.16.146.1.domain: 2236+ A? www.apachecon.com. (35)
11:34:02.248343 IP 172.16.146.2.37580 > 172.16.146.1.domain: 62143+ AAAA? www.apachecon.com. (35)
11:34:02.249114 IP 172.16.146.1.domain > 172.16.146.2.37580: 2236 3/0/0 CNAME apache.org., A 95.216.26.30, A 207.244.88.140 (91)
11:34:02.249114 IP 172.16.146.1.domain > 172.16.146.2.37580: 62143 1/1/0 CNAME apache.org. (140)
11:34:02.317850 IP 172.16.146.2.43822 > 172.16.146.1.domain: 36016+ A? ocsp.pki.goog. (31)
11:34:02.317915 IP 172.16.146.2.43822 > 172.16.146.1.domain: 48316+ AAAA? ocsp.pki.goog. (31)
11:34:02.386235 IP 172.16.146.2.50588 > 172.16.146.1.domain: 64771+ A? safebrowsing.googleapis.com. (45)
11:34:02.386407 IP 172.16.146.2.50588 > 172.16.146.1.domain: 18689+ AAAA? safebrowsing.googleapis.com. (45)
11:34:02.386835 IP 172.16.146.1.domain > 172.16.146.2.50588: 64771 1/0/0 A 108.177.122.95 (61)
11:34:02.414988 IP 172.16.146.2.34235 > 172.16.146.1.domain: 58131+ A? fonts.gstatic.com. (35)
11:34:02.415123 IP 172.16.146.2.34235 > 172.16.146.1.domain: 55566+ AAAA? fonts.gstatic.com. (35)
11:34:02.416084 IP 172.16.146.1.domain > 172.16.146.2.34235: 55566 2/0/0 CNAME gstaticadssl.l.google.com., AAAA 2607:f8b0:4002:c09::5e
11:34:02.433398 IP 172.16.146.2.36324 > 172.16.146.1.domain: 24523+ A? www.youtube.com. (33)
11:34:02.433460 IP 172.16.146.2.36324 > 172.16.146.1.domain: 47305+ AAAA? www.youtube.com. (33)
Page 7 of 12 To direct input to this VM, move the mouse pointer inside or press Ctrl+G.
Type here to search
25°C
15:09
31/05/2025




Filtering out traffic

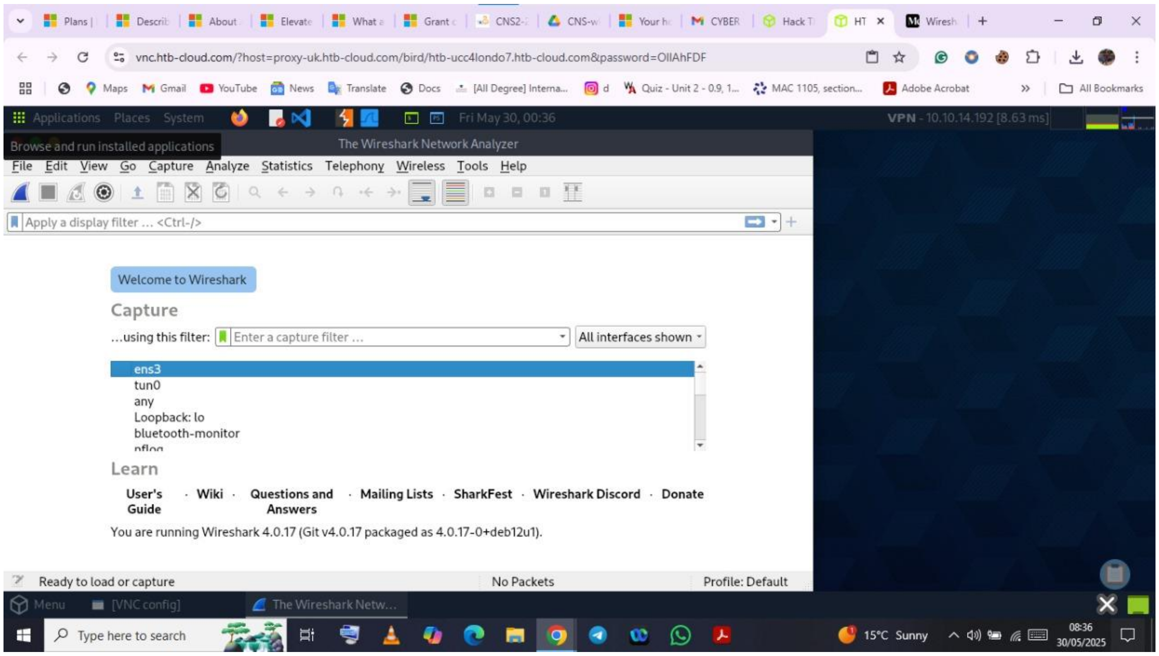
# Wireshark

## Analysis with Wireshark

Overview of Wireshark for graphical packet analysis—navigating the interface and viewing packet details.

## Familiarity With Wireshark

Explores packet breakdowns, stream following, and basic display filters.




## Wireshark Advanced Usage

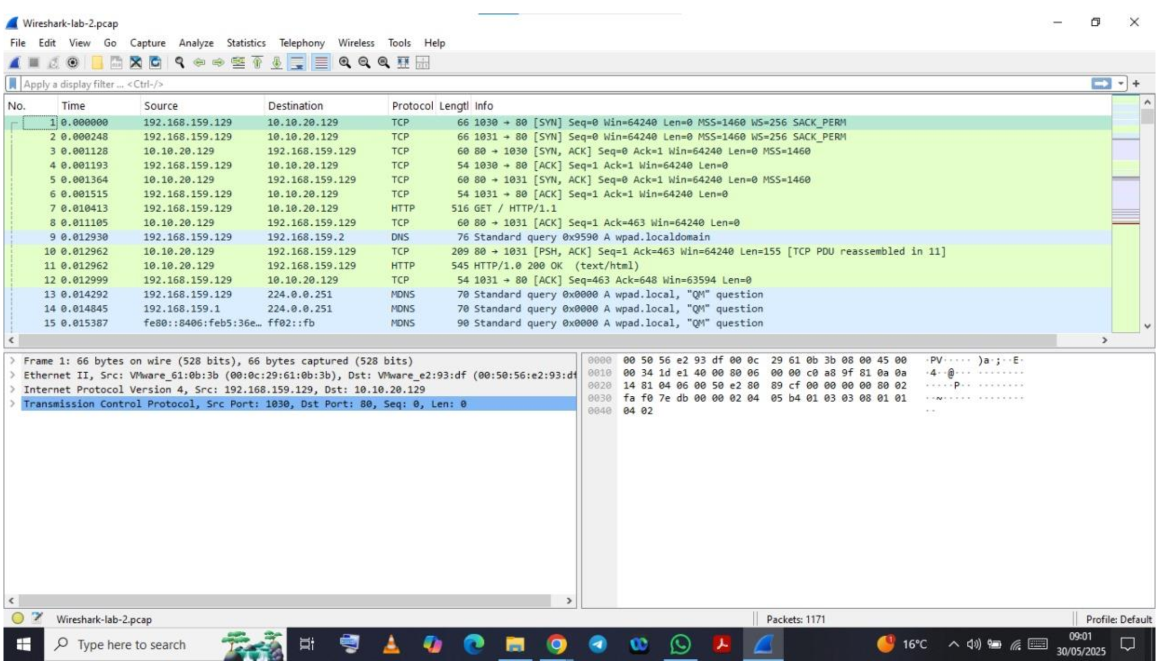
Advanced topics like customizing views, protocol hierarchies, and complex filters.

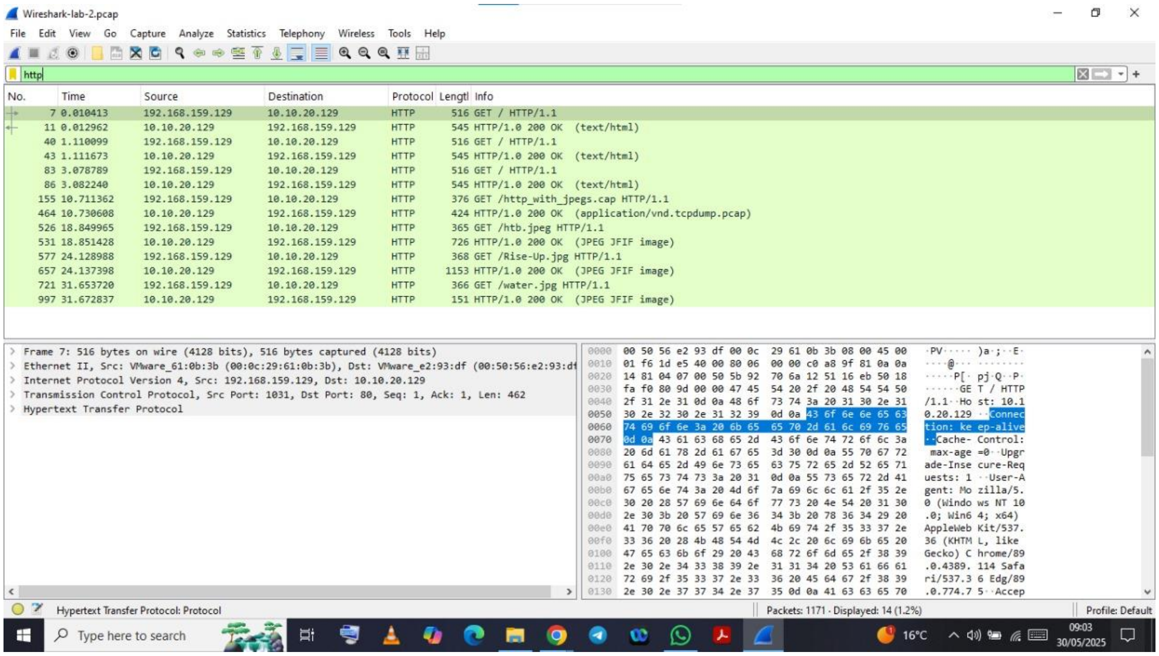
## Packet Inception, Dissecting Network Traffic With Wireshark

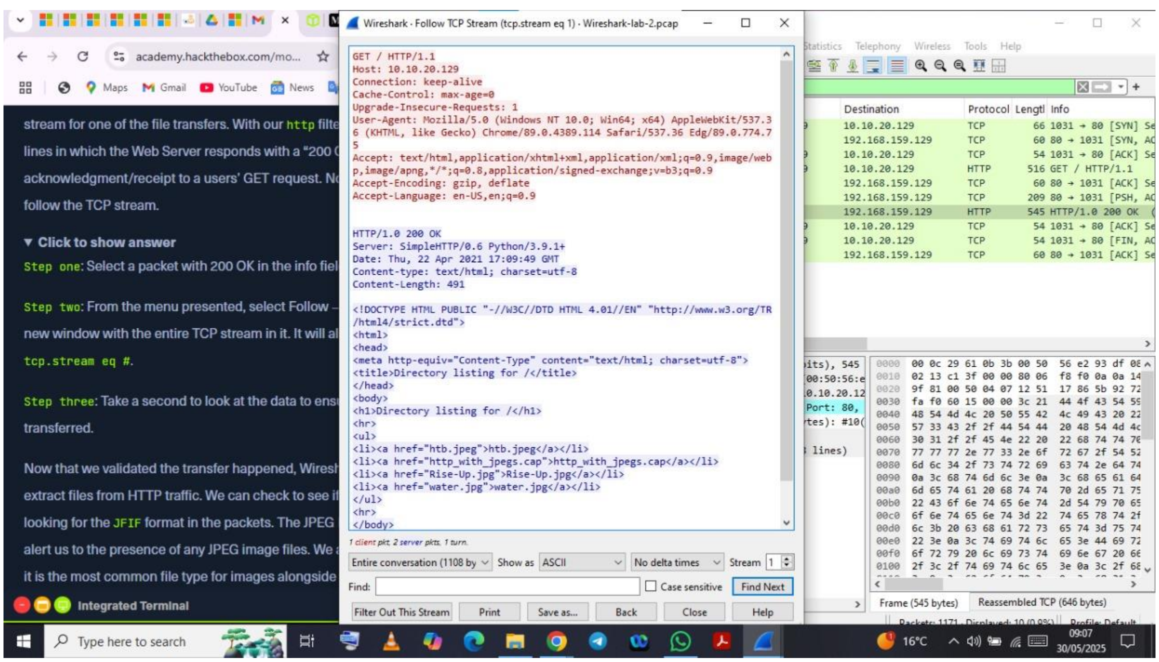
Hands-on analysis of how traffic flows from Layer 2 to Layer 7 and what each component reveals.

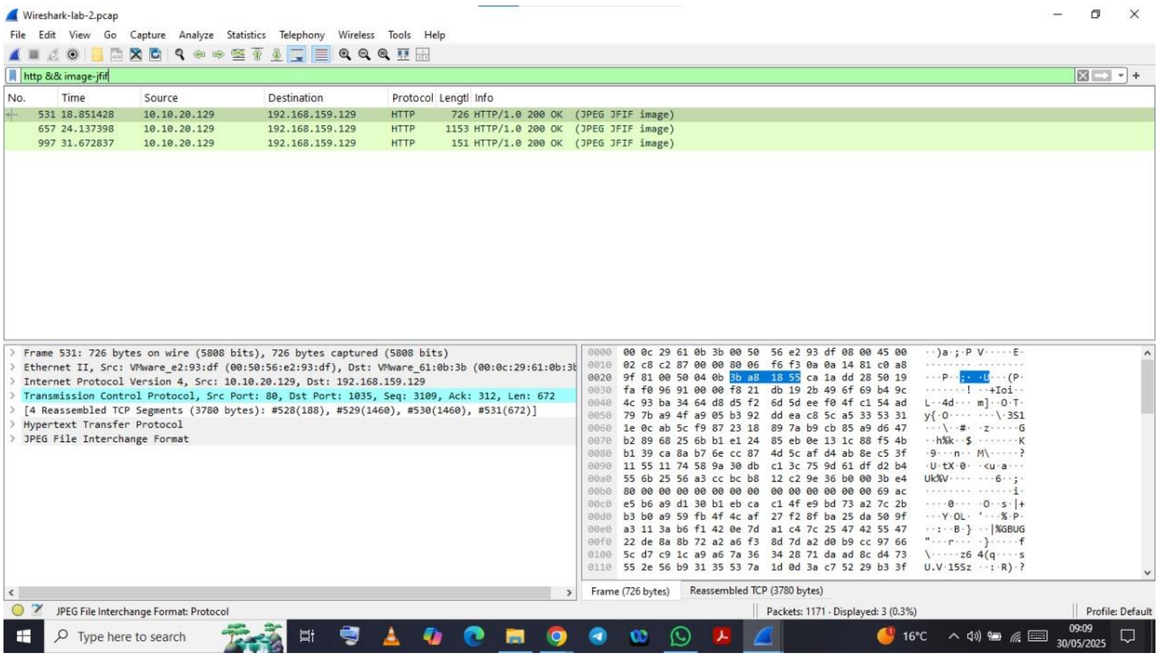
## Guided Lab: Traffic Analysis Workflow

Lab-based traffic investigation using Wireshark tools in a real-case simulation.

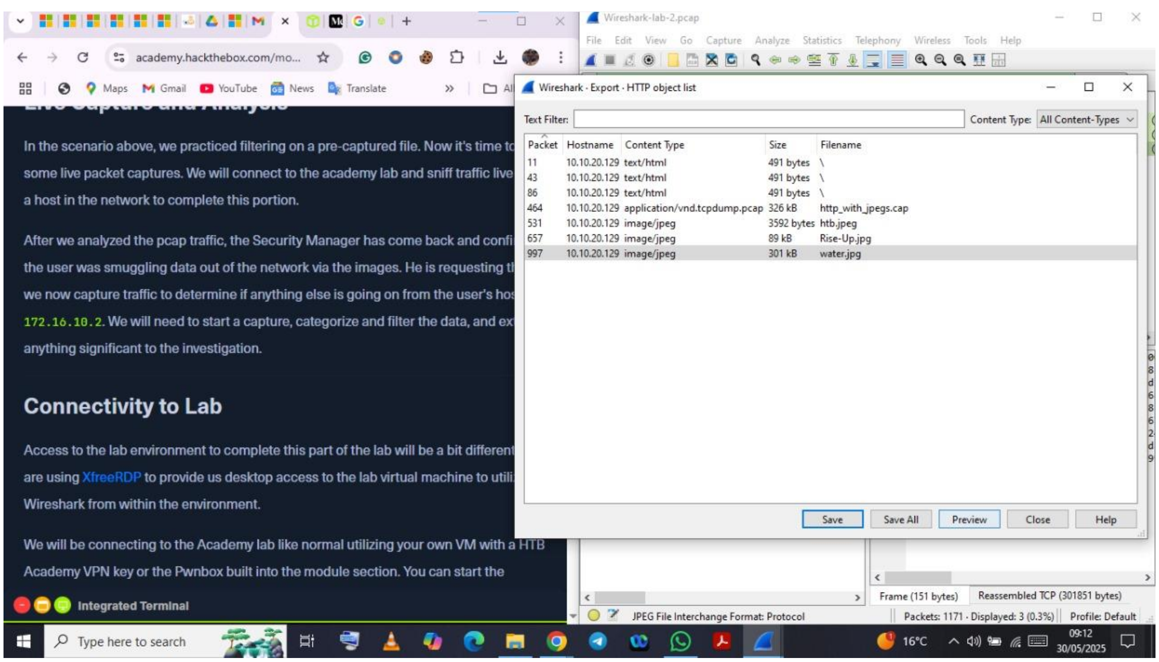



Wireshark-lab-2.pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
http
No. Time Source Destination Protocol Length Info
7 0.010413 192.168.159.129 10.10.20.129 HTTP 516 GET / HTTP/1.1
11 0.012962 10.10.20.129 192.168.159.129 HTTP 545 HTTP/1.0 200 OK (text/html)
40 1.110099 192.168.159.129 10.10.20.129 HTTP 516 GET / HTTP/1.1
43 1.111673 10.10.20.129 192.168.159.129 HTTP 545 HTTP/1.0 200 OK (text/html)
83 3.078789 192.168.159.129 10.10.20.129 HTTP 516 GET / HTTP/1.1
86 3.082240 10.10.20.129 192.168.159.129 HTTP 545 HTTP/1.0 200 OK (text/html)
155 10.711362 192.168.159.129 10.10.20.129 HTTP 376 GET /http_with_jpegs.cap HTTP/1.1
464 10.730608 10.10.20.129 192.168.159.129 HTTP 424 HTTP/1.0 200 OK (application/vnd.tcpdump.pcap)
526 18.849965 192.168.159.129 10.10.20.129 HTTP 365 GET /htb.jpeg HTTP/1.1
531 18.851428 10.10.20.129 192.168.159.129 HTTP 726 HTTP/1.0 200 OK (JPEG JFIF image)
577 24.128988 192.168.159.129 10.10.20.129 HTTP 368 GET /Rise-Up.jpg HTTP/1.1
657 24.137398 10.10.20.129 192.168.159.129 HTTP 1153 HTTP/1.0 200 OK (JPEG JFIF image)
721 31.653720 192.168.159.129 10.10.20.129 HTTP 366 GET /water.jpg HTTP/1.1
997 31.672837 10.10.20.129 192.168.159.129 HTTP 151 HTTP/1.0 200 OK (JPEG JFIF image)
Frame 7: 516 bytes on wire (4128 bits), 516 bytes captured (4128 bits)
Ethernet II, Src: VMware_61:0b:3b (00:0c:29:61:0b:3b), Dst: VMware_e2:93:df (00:50:56:e2:93:df)
Internet Protocol Version 4, Src: 192.168.159.129, Dst: 10.10.20.129
Transmission Control Protocol, Src Port: 1031, Dst Port: 80, Seq: 1, Ack: 1, Len: 462
Hypertext Transfer Protocol
Hypertext Transfer Protocol: Protocol
Packets: 1171 · Displayed: 14 (1.2%)
Profile: Default
Type here to search
16°C
09:03
30/05/2025

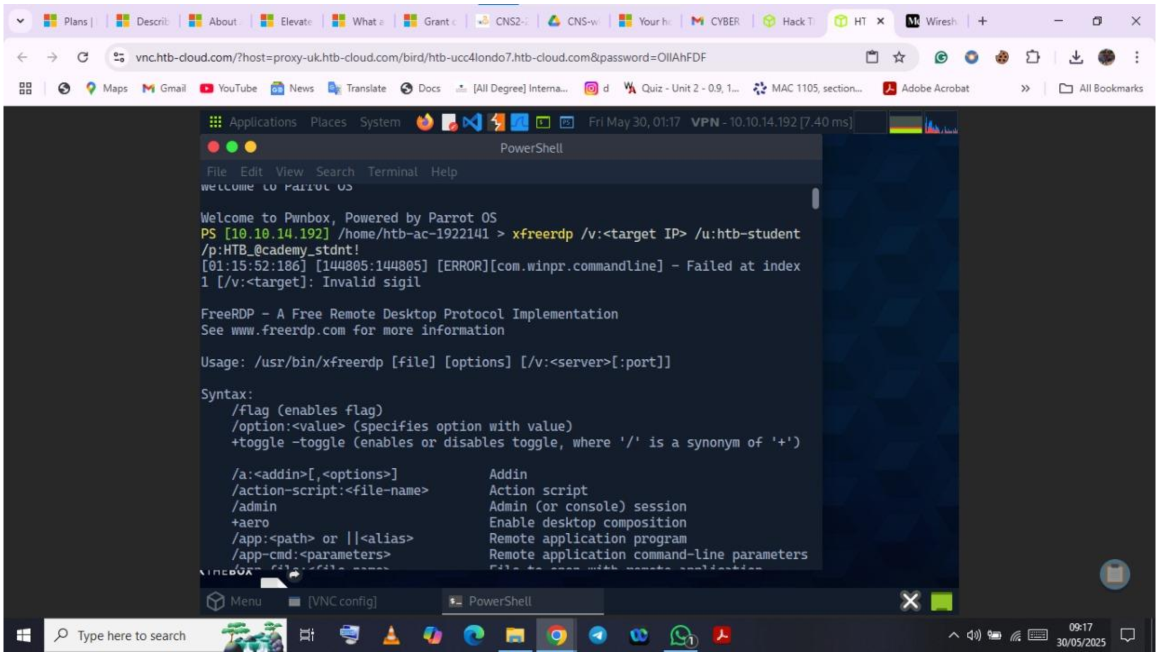

Wireshark · Follow TCP Stream (tcp.stream eq 1) · Wireshark-lab-2.pcap
GET / HTTP/1.1
Host: 10.10.20.129
Connection: keep-alive
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/89.0.4389.114 Safari/537.36 Edg/89.0.774.75
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
HTTP/1.0 200 OK
Server: SimpleHTTP/0.6 Python/3.9.1+
Date: Thu, 22 Apr 2021 17:09:49 GMT
Content-type: text/html; charset=utf-8
Content-Length: 491
<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01//EN" "http://www.w3.org/TR/html4/strict.dtd">
<html>
<head>
<meta http-equiv="Content-Type" content="text/html; charset=utf-8">
<title>Directory listing for /</title>
</head>
<body>
<h1>Directory listing for /</h1>
<hr>
<ul>
<li><a href="htb.jpeg">htb.jpeg</a></li>
<li><a href="http_with_jpegs.cap">http_with_jpegs.cap</a></li>
<li><a href="Rise-Up.jpg">Rise-Up.jpg</a></li>
<li><a href="water.jpg">water.jpg</a></li>
</ul>
<hr>
</body>
1 client pkt, 2 server pkts, 1 turn.
Entire conversation (1108 bytes) Show as ASCII No delta times Stream 1
Find: Case sensitive Find Next
Filter Out This Stream Print Save as... Back Close Help
academy.hackthebox.com/mo...
stream for one of the file transfers. With our http filte
lines in which the Web Server responds with a "200 O
acknowledgment/receipt to a users' GET request. N
follow the TCP stream.
Click to show answer
Step one: Select a packet with 200 OK in the info fiel
Step two: From the menu presented, select Follow -
new window with the entire TCP stream in it. It will al
tcp.stream eq #.
Step three: Take a second to look at the data to ens
transferred.
Now that we validated the transfer happened, Wiresh
extract files from HTTP traffic. We can check to see if
looking for the JFIF format in the packets. The JPEG
alert us to the presence of any JPEG image files. We
it is the most common file type for images alongside
Integrated Terminal
Type here to search
16°C
09:07
30/05/2025



Wireshark-lab-2.pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
http && image-jfif
No. Time Source Destination Protocol Length Info
531 18.851428 10.10.20.129 192.168.159.129 HTTP 726 HTTP/1.0 200 OK (JPEG JFIF image)
657 24.137398 10.10.20.129 192.168.159.129 HTTP 1153 HTTP/1.0 200 OK (JPEG JFIF image)
997 31.672837 10.10.20.129 192.168.159.129 HTTP 151 HTTP/1.0 200 OK (JPEG JFIF image)
Frame 531: 726 bytes on wire (5808 bits), 726 bytes captured (5808 bits)
Internet Protocol Version 4, Src: 10.10.20.129, Dst: 192.168.159.129
Transmission Control Protocol, Src Port: 80, Dst Port: 1035, Seq: 3109, Ack: 312, Len: 672
[4 Reassembled TCP Segments (3780 bytes): #528(188), #529(1460), #530(1460), #531(672)]
Hypertext Transfer Protocol
JPEG File Interchange Format
Frame (726 bytes)
Reassembled TCP (3780 bytes)
JPEG File Interchange Format: Protocol
Packets: 1171 · Displayed: 3 (0.3%)
Profile: Default

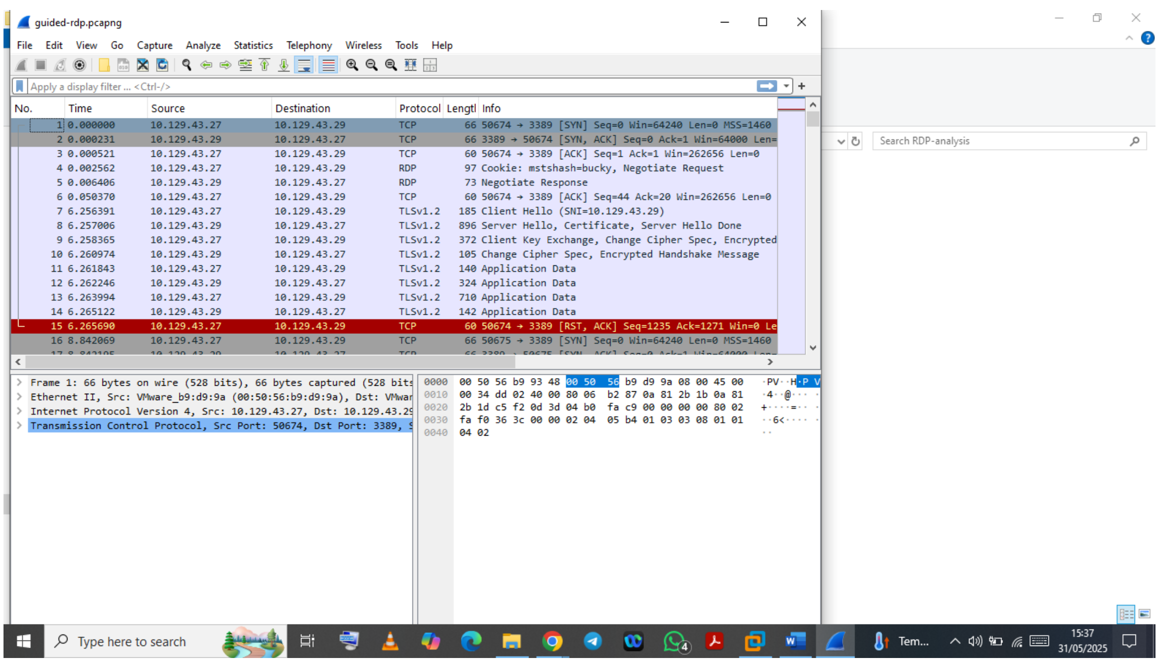



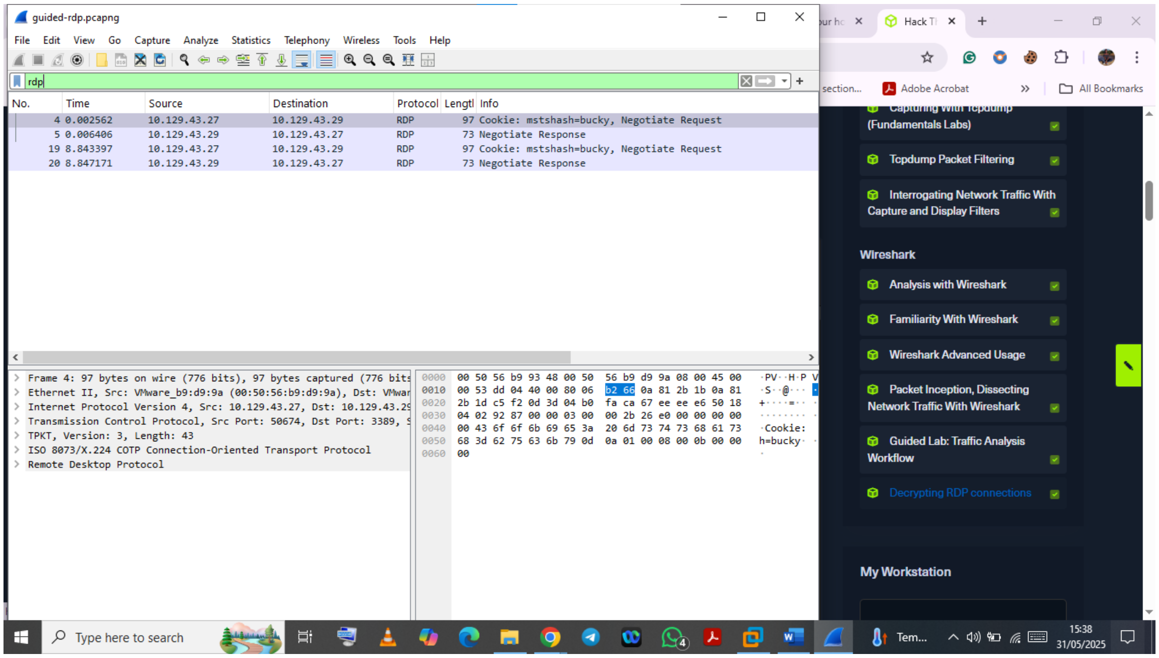
academy.hackthebox.com/mo...
In the scenario above, we practiced filtering on a pre-captured file.
After we analyzed the pcap traffic, the Security Manager has come back and confi
172.16.10.2
Connectivity to Lab
Integrated Terminal
Wireshark · Export · HTTP object list
Text Filter:
Content Type: All Content-Types
Packet Hostname Content Type Size Filename
11 10.10.20.129 text/html 491 bytes \
43 10.10.20.129 text/html 491 bytes \
86 10.10.20.129 text/html 491 bytes \
464 10.10.20.129 application/vnd.tcpdump.pcap 326 kB http_with_jpegs.cap
531 10.10.20.129 image/jpeg 3592 bytes htb.jpeg
657 10.10.20.129 image/jpeg 89 kB Rise-Up.jpg
997 10.10.20.129 image/jpeg 301 kB water.jpg
Save
Save All
Preview
Close
Help

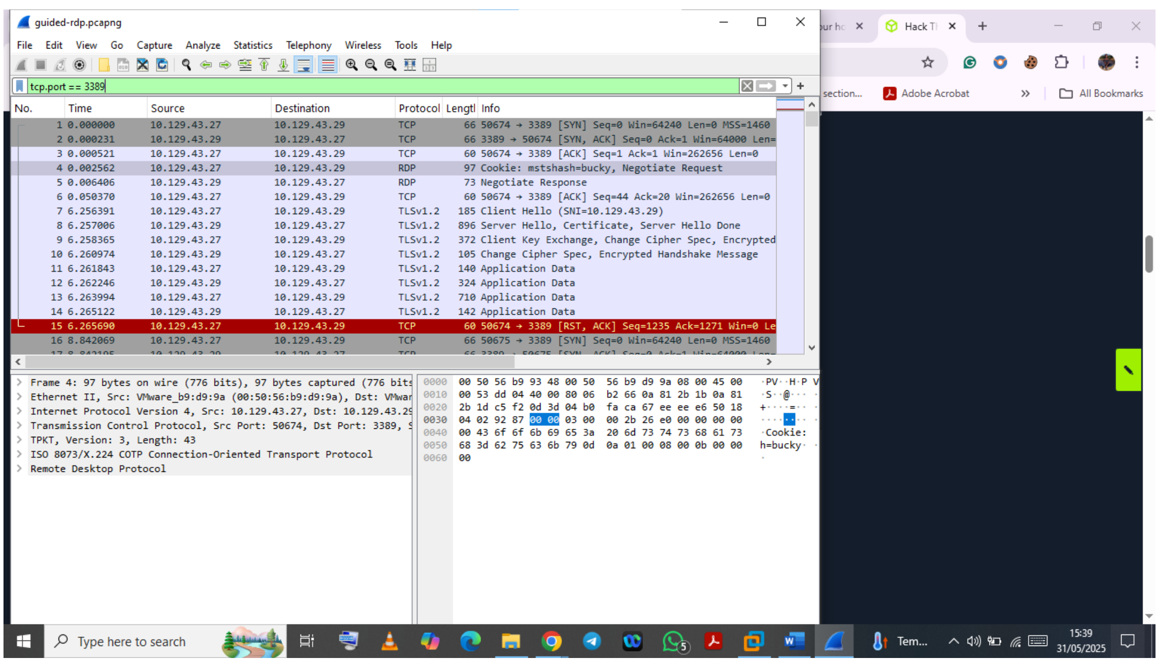


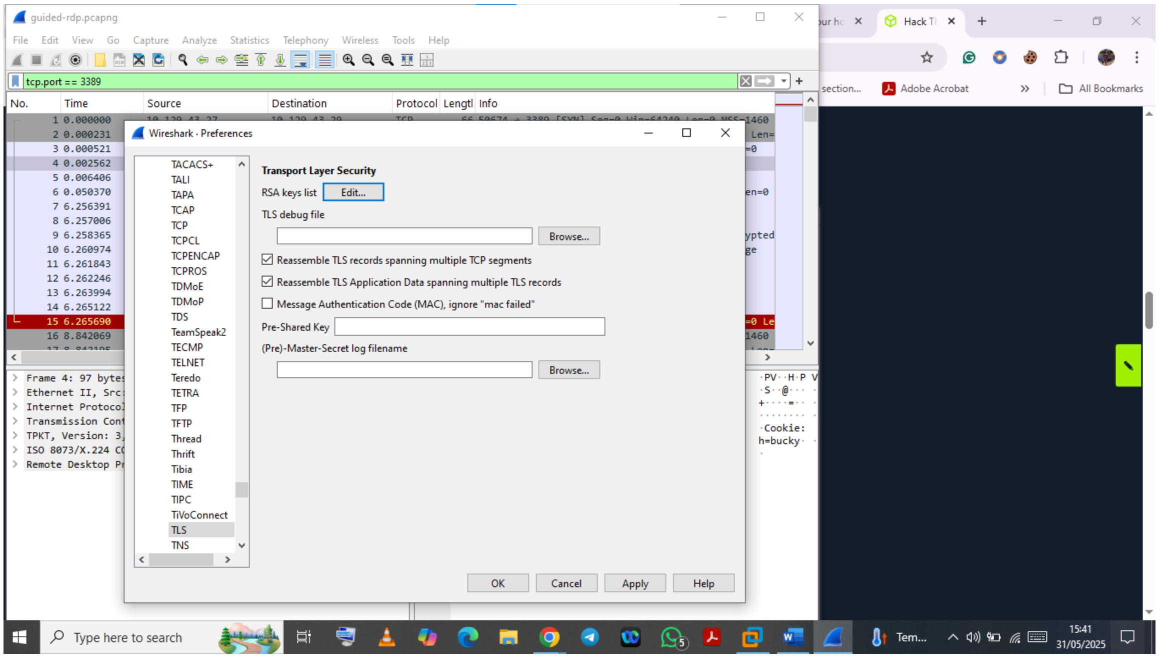
## Decrypting RDP Connections

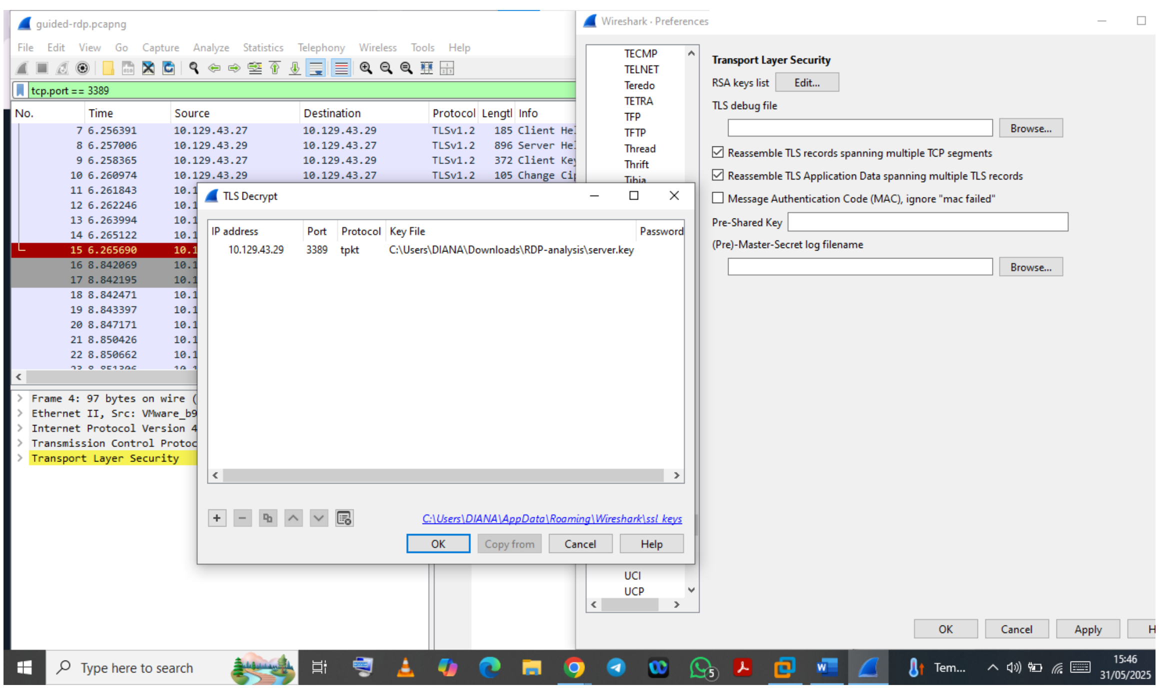
Shows how to decrypt Remote Desktop Protocol traffic using session secrets to inspect content that would normally be encrypted.

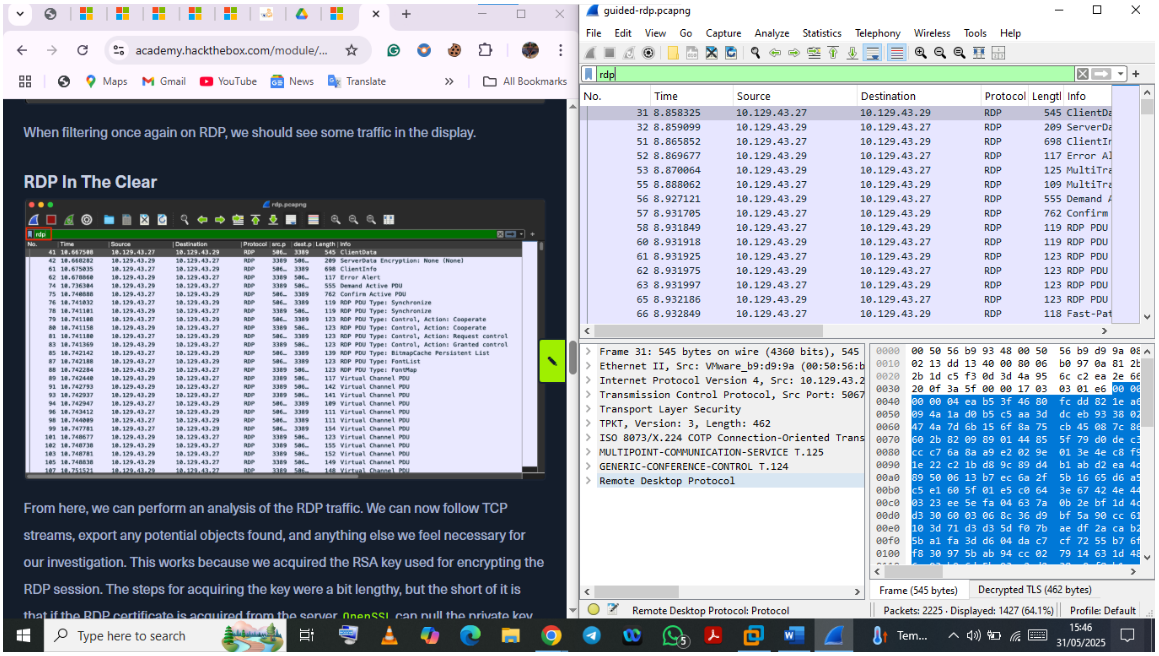


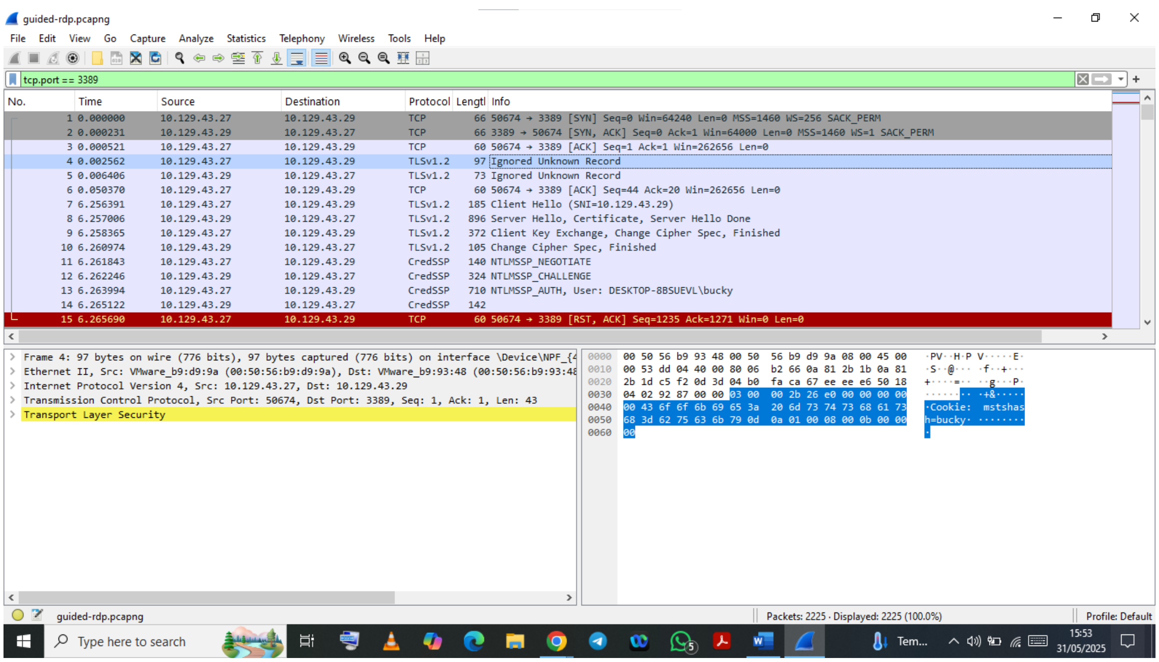

guided-rdp.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
rdp
No. Time Source Destination Protocol Length Info
4 0.002562 10.129.43.27 10.129.43.29 RDP 97 Cookie: mstshash=bucky, Negotiate Request
5 0.006406 10.129.43.29 10.129.43.27 RDP 73 Negotiate Response
19 8.843397 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)
Ethernet II, Src: VMware_b9:d9:9a (00:50:56:b9:d9:9a), Dst: VMwar
Internet Protocol Version 4, Src: 10.129.43.27, Dst: 10.129.43.29
Transmission Control Protocol, Src Port: 50674, Dst Port: 3389,
TPKT, Version: 3, Length: 43
ISO 8073/X.224 COTP Connection-Oriented Transport Protocol
Remote Desktop Protocol
(Fundamentals Labs)
Tcpdump Packet Filtering
Interrogating Network Traffic With Capture and Display Filters
Wireshark
Analysis with Wireshark
Familiarity With Wireshark
Wireshark Advanced Usage
Packet Inception, Dissecting Network Traffic With Wireshark
Guided Lab: Traffic Analysis Workflow
Decrypting RDP connections
My Workstation
Type here to search
15:38
31/05/2025


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
2 0.000231 10.129.43.29 10.129.43.27 TCP 66 3389 → 50674 [SYN, ACK] Seq=0 Ack=1 Win=64000 Len=
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
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 Le
16 8.842069 10.129.43.27 10.129.43.29 TCP 66 50675 → 3389 [SYN] Seq=0 Win=64240 Len=0 MSS=1460
Frame 4: 97 bytes on wire (776 bits), 97 bytes captured (776 bits)
Ethernet II, Src: VMware_b9:d9:9a (00:50:56:b9:d9:9a), Dst: VMwar
Internet Protocol Version 4, Src: 10.129.43.27, Dst: 10.129.43.29
Transmission Control Protocol, Src Port: 50674, Dst Port: 3389,
TPKT, Version: 3, Length: 43
ISO 8073/X.224 COTP Connection-Oriented Transport Protocol
Remote Desktop Protocol
Type here to search
15:39
31/05/2025


guided-rdp.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
tcp.port == 3389
No. Time Source Destination Protocol Length Info
Wireshark · Preferences
TACACS+
TALI
TAPA
TCAP
TCP
TCPCL
TCPENCAP
TCPROS
TDMoE
TDMoP
TDS
TeamSpeak2
TECMP
TELNET
Teredo
TETRA
TFP
TFTP
Thread
Thrift
Tibia
TIME
TIPC
TiVoConnect
TLS
TNS
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
Browse...
OK Cancel Apply Help
Frame 4: 97 bytes
Ethernet II, Src:
Internet Protocol
Transmission Cont
TPKT, Version: 3,
ISO 8073/X.224 CO
Remote Desktop Pr
Type here to search
15:41
31/05/2025


guided-rdp.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
tcp.port == 3389
No. Time Source Destination Protocol Length Info
7 6.256391 10.129.43.27 10.129.43.29 TLSv1.2 185 Client He
8 6.257006 10.129.43.29 10.129.43.27 TLSv1.2 896 Server He
9 6.258365 10.129.43.27 10.129.43.29 TLSv1.2 372 Client Ke
10 6.260974 10.129.43.29 10.129.43.27 TLSv1.2 105 Change Ci
TLS Decrypt
IP address Port Protocol Key File Password
10.129.43.29 3389 tpkt C:\Users\DIANA\Downloads\RDP-analysis\server.key
C:\Users\DIANA\AppData\Roaming\Wireshark\ssl_keys
OK Copy from Cancel Help
Frame 4: 97 bytes on wire (
Ethernet II, Src: VMware_b9
Internet Protocol Version 4
Transmission Control Protoc
Transport Layer Security
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
Browse...
OK Cancel Apply
Type here to search
15:46
31/05/2025

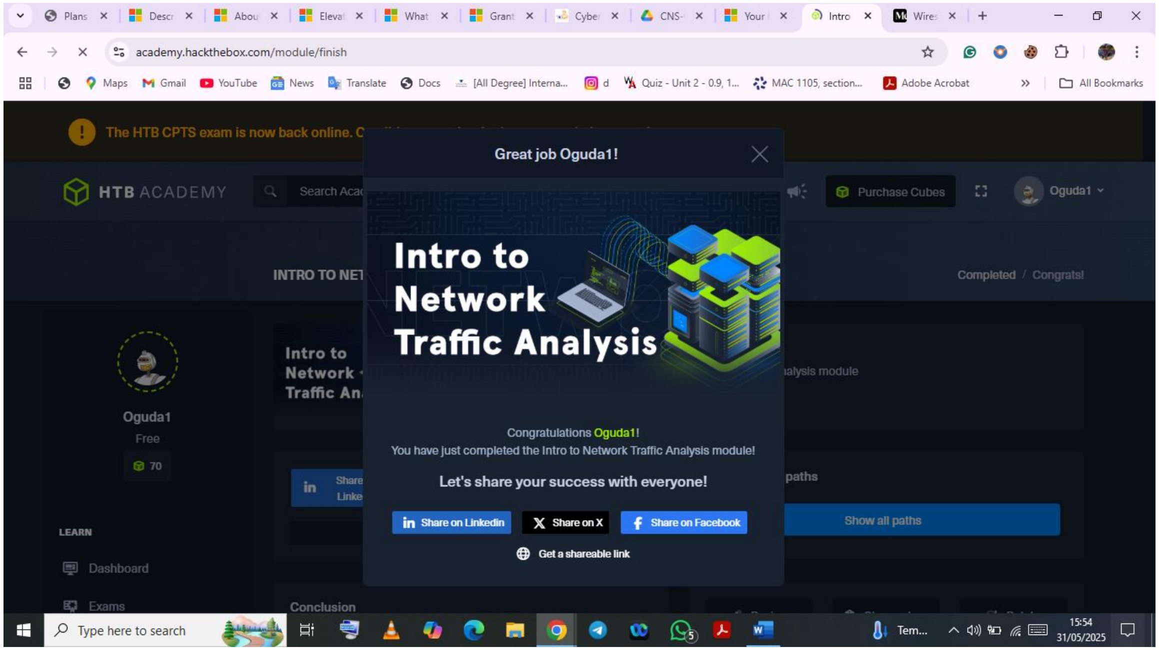



## 3. Module Completion and Proof

All module sections were completed successfully, including practical labs and theoretical content.

Screenshots of completion have been included below:




Shareable Link

https://academy.hackthebox.com/achievement/1922141/81

## 4. Conclusion

This module provided a solid foundation in network traffic analysis, combining both theoretical concepts and practical labs. I now have a much clearer understanding of how to interpret data as it travels across different OSI layers and how to use professional tools like tcpdump and Wireshark to examine, filter, and analyze network traffic.

The ability to decrypt RDP sessions and inspect traffic with confidence has given me a major boost in hands-on cybersecurity skills. These insights are not only valuable in technical troubleshooting but are also essential in detecting suspicious behavior, conducting incident response, and securing networks from attacks.

This experience has deepened my confidence as a cybersecurity learner and practitioner.