Week 2 Assignment 2

Course: Cloud and Network Security - C1-2026

Student Name: Bussllus Bertrand

Student Number: CS-CNS11-26004

Wednesday, January 28, 2026

Week two Assignment two:

Class exercise: Introduction to Network Traffic Analysis

Table of Contents

Introduction

This report details the successful completion of the "Intro to Network Traffic Analysis module from Hack the box Academy. Network traffic analysis is a cornerstone of modern cybersecurity, providing the foundational skills necessary to detect malicious activity, respond to security incidents, and diagnose network health issues. By examining the data that flows across a network, security professionals can uncover hidden threats, understand attack methodologies, and verify the integrity of their digital infrastructure.

The core objective of this module was to establish a strong theoretical and practical understanding of network traffic analysis. This involved exploring the fundamentals of network protocols and gaining hands-on experience with industry-standard tools. The exercise focused heavily on the practical application of Wireshark for graphical packet analysis and tcpdump for command-line traffic capture.

The following sections provide a detailed analysis of the module's exercises, demonstrating the process used to solve each challenge.

Module Questions & Answers

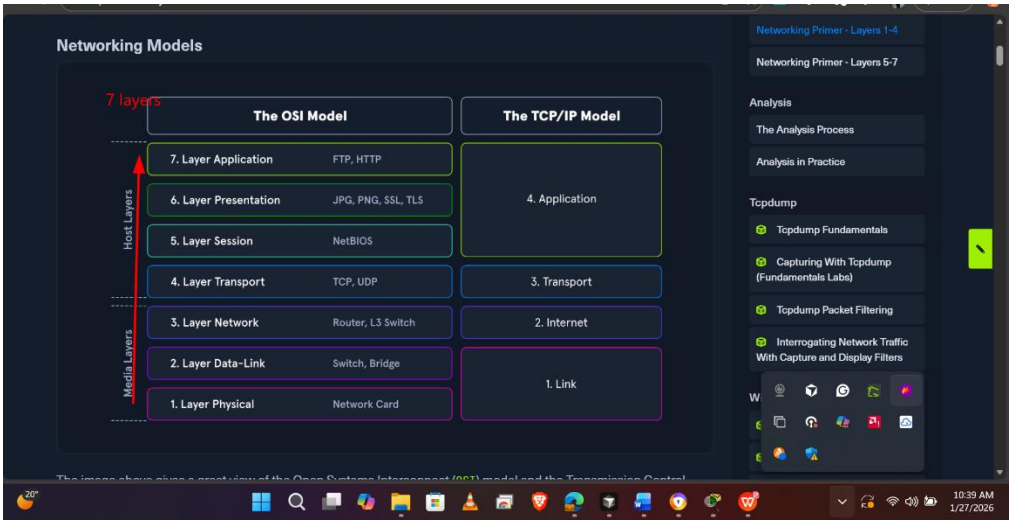
This section provides a systematic walkthrough of the questions presented in the module and the answers, together with supporting evidence.

Networking Primer - Layers 1-4

How many layers does the OSI model have?

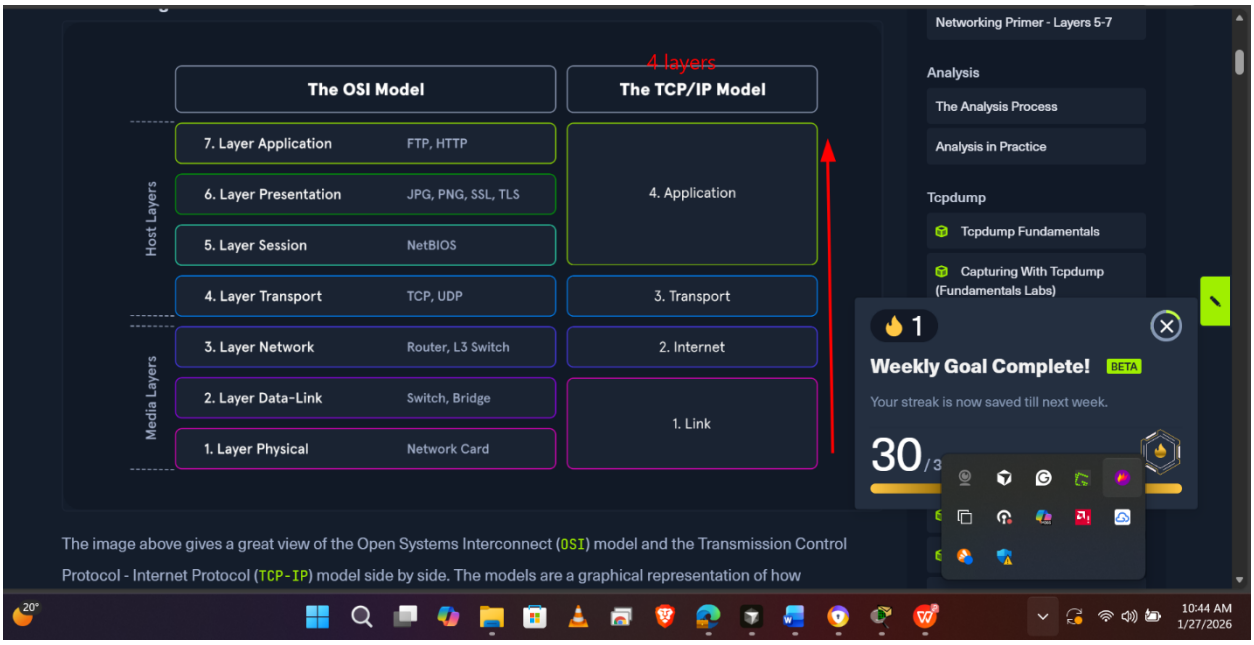
Answer: 7

Week 2 Assignment 2



How many layers are there in the TCP/IP model?

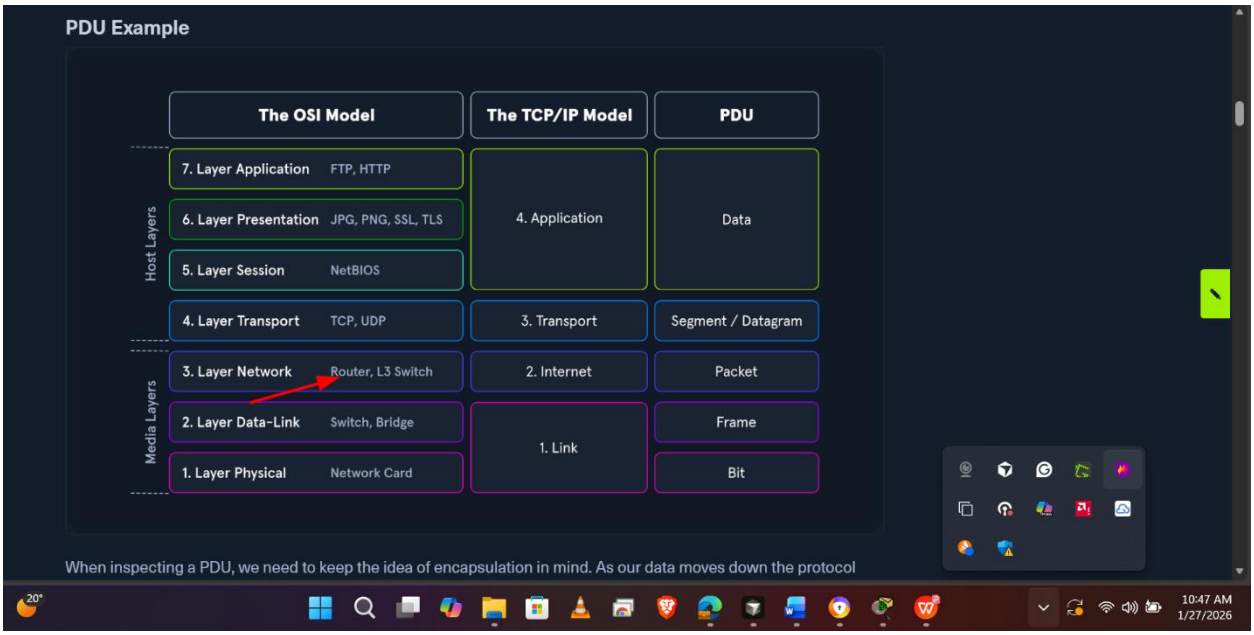
Answer: 4



True or False: Routers operate at layer 2 of the OSI model?

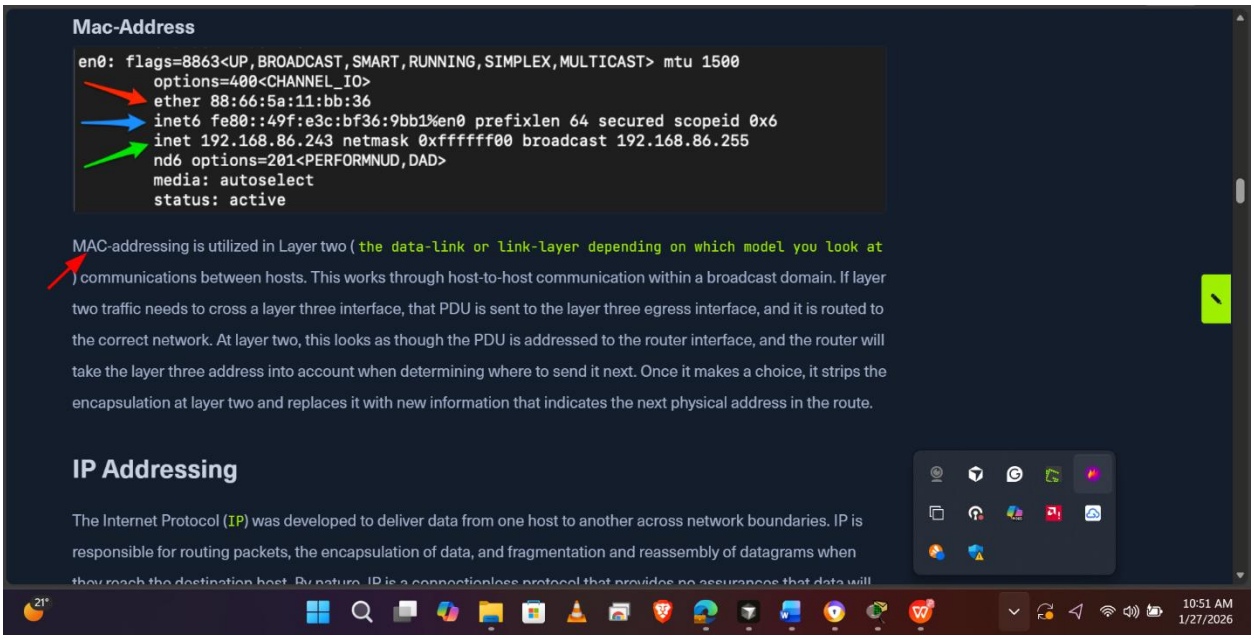
Answer: False

Week 2 Assignment 2



What addressing mechanism is used at the Link Layer of the TCP/IP model?

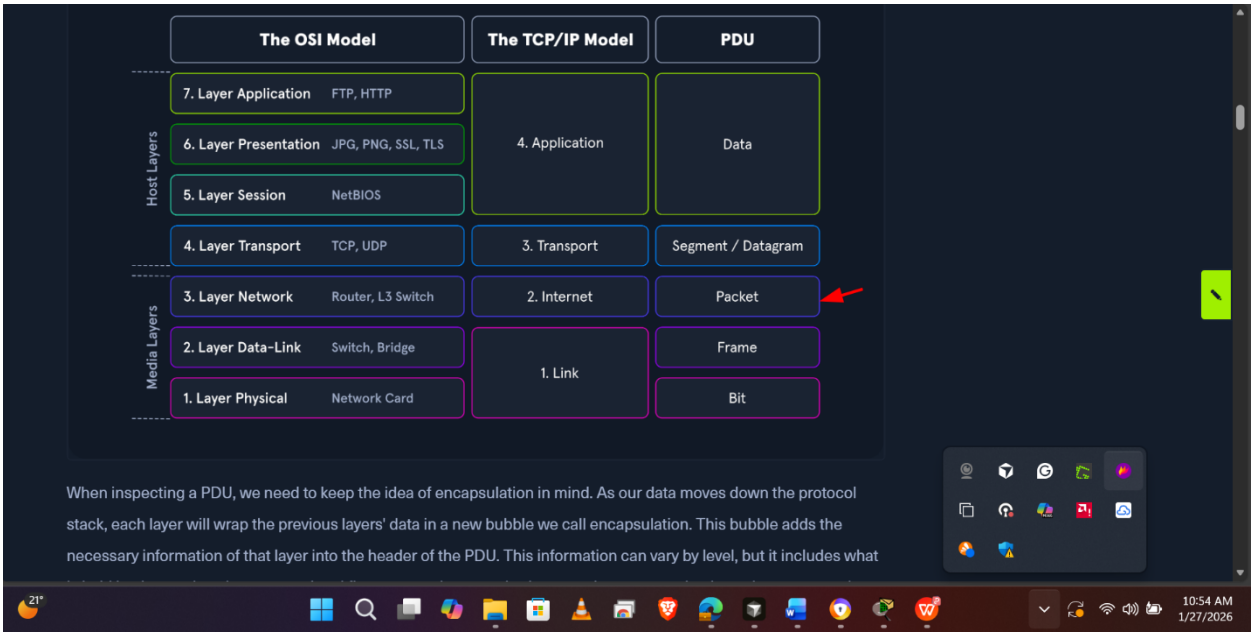
Answer: Mac-address



At what layer of the OSI model is a PDU encapsulated into a packet? (the number)

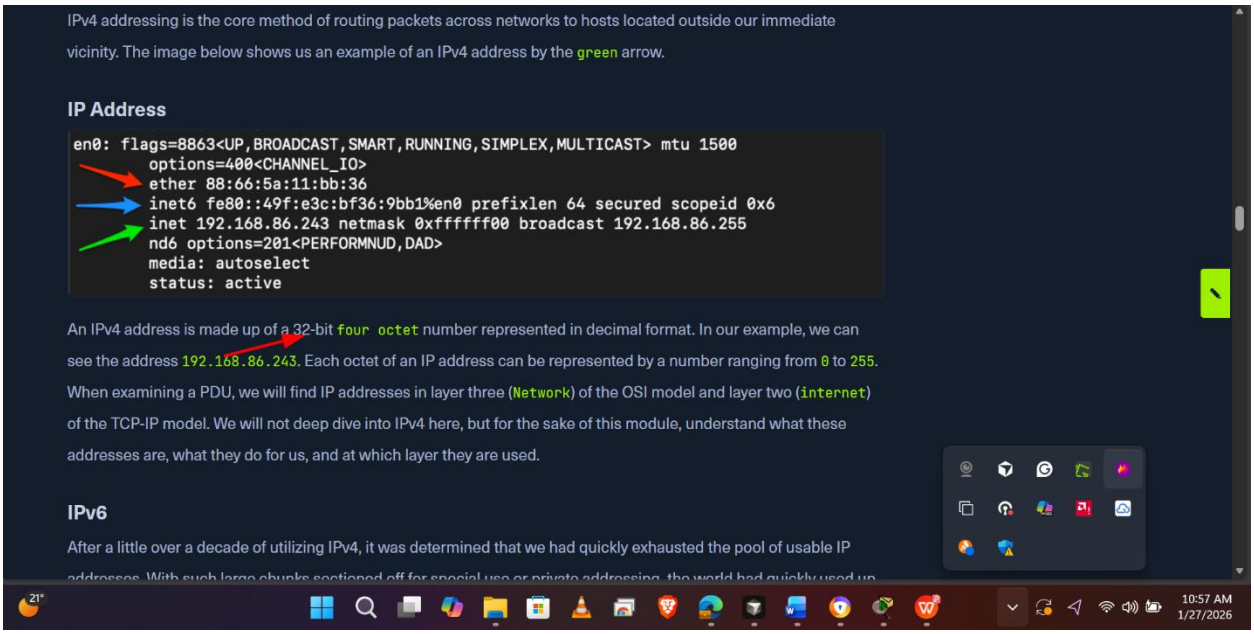
Answer: 3

Week 2 Assignment 2



What addressing mechanism utilizes a 32-bit address?

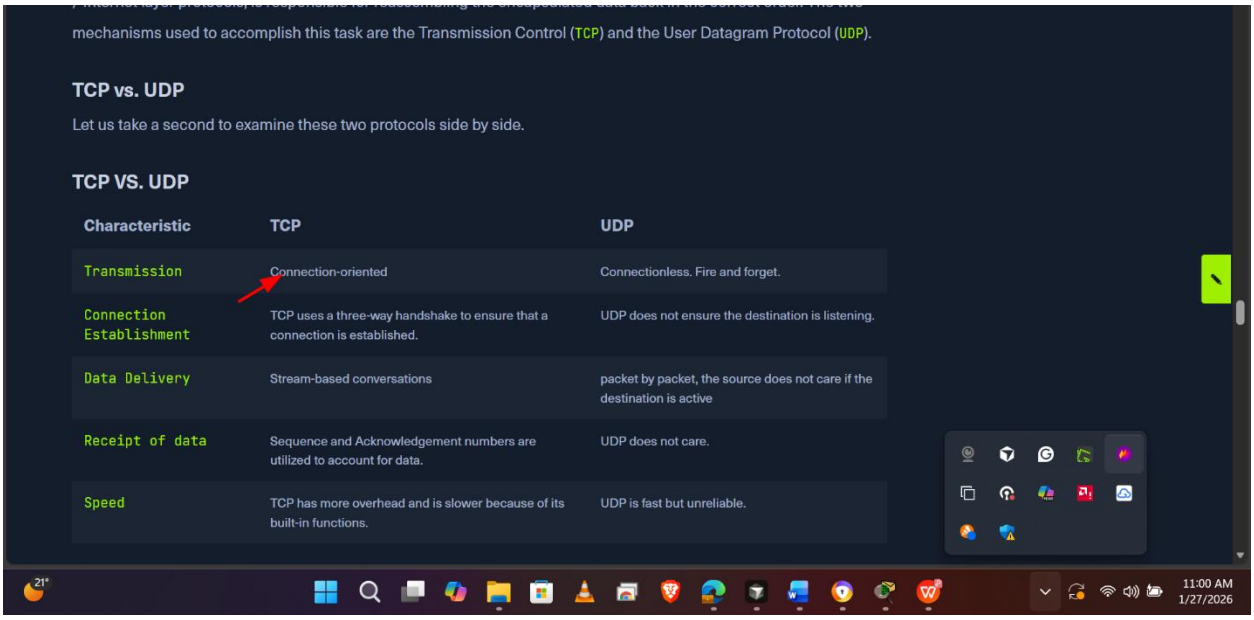
Answer: ipv4



What Transport layer protocol is connection oriented?

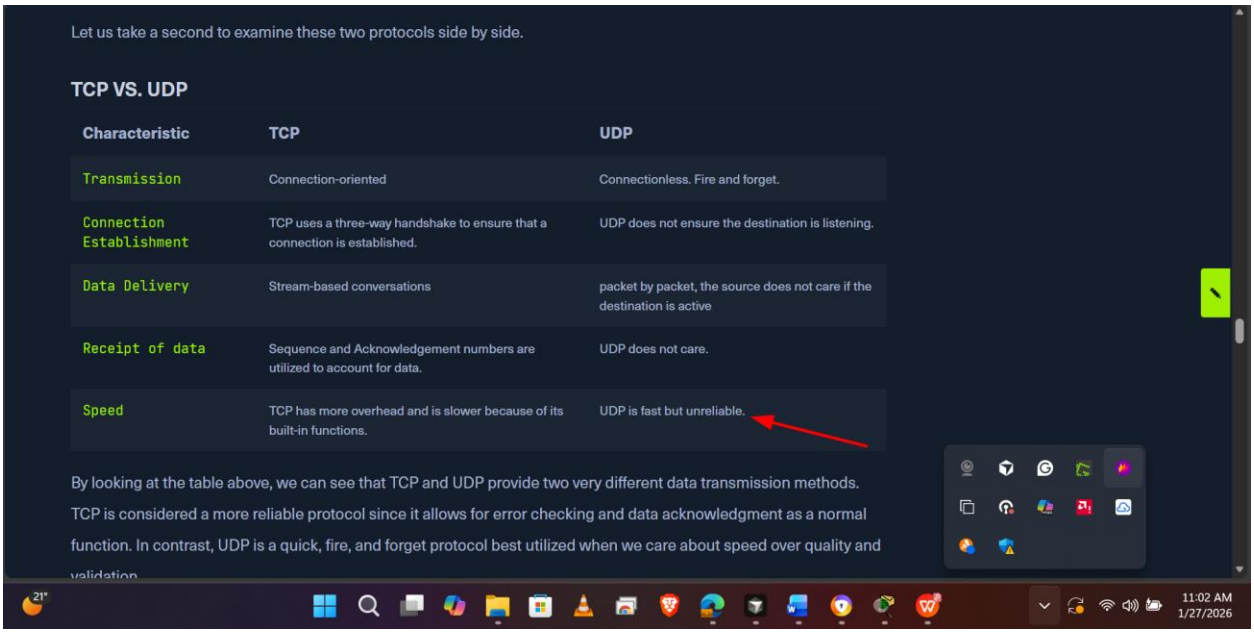
Answer: TCP

Week 2 Assignment 2



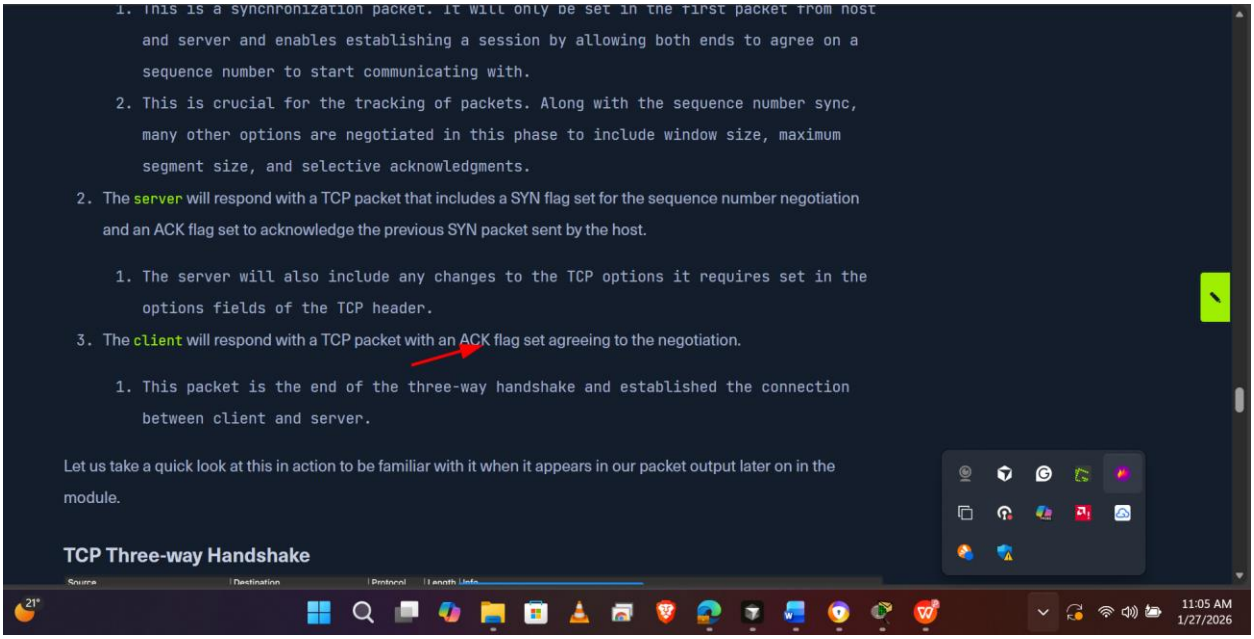
What Transport Layer protocol is considered unreliable?

Answer: UDP



TCP's three-way handshake consists of 3 packets: 1.Syn, 2.Syn & ACK, 3. _? What is the final packet of the handshake?

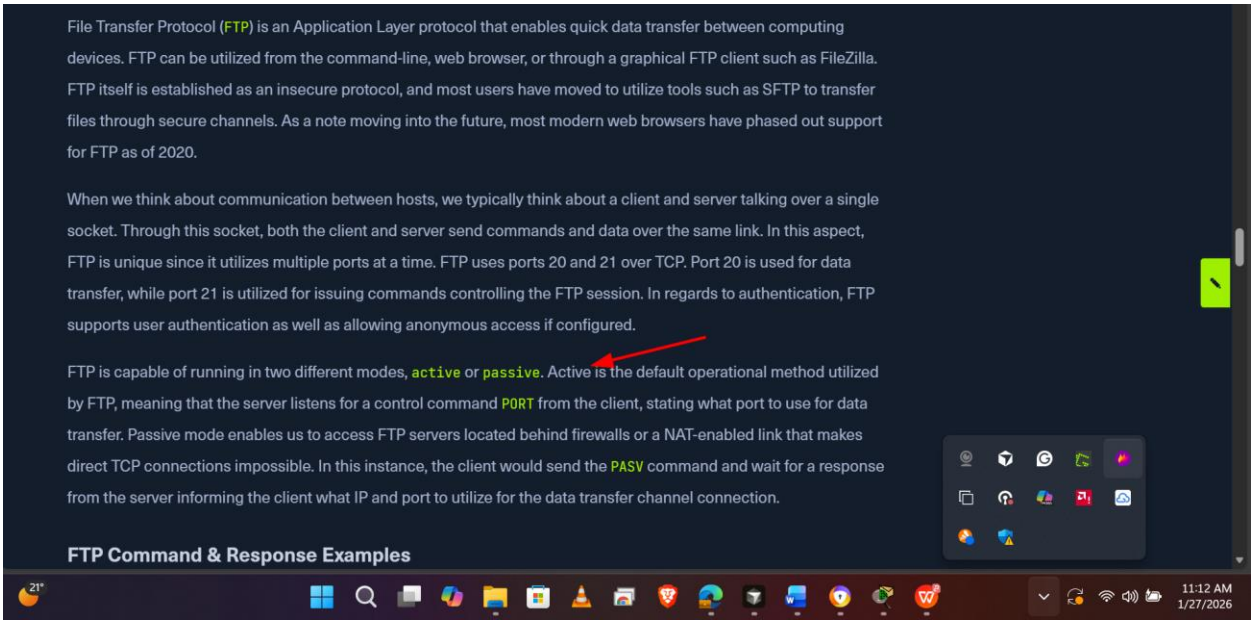
Answer: ACK



Networking Primer - Layers 5-7

What is the default operational mode method used by FTP?

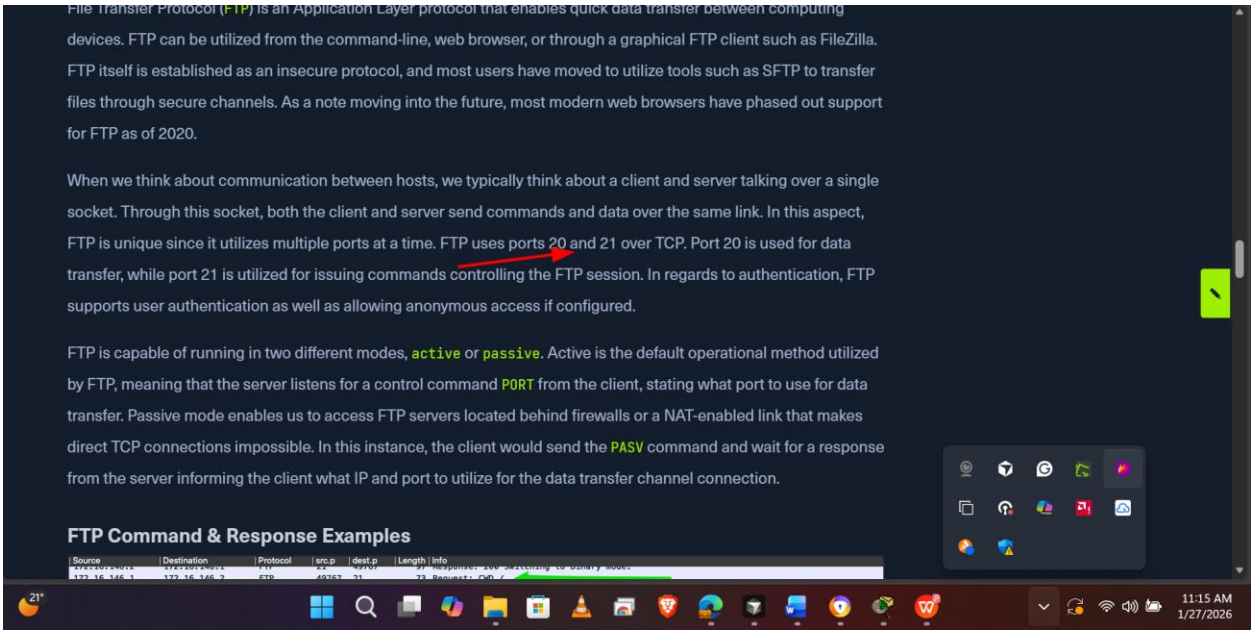
Answer: Active



FTP utilizes what two ports for command and data transfer? (separate the two numbers with a space)

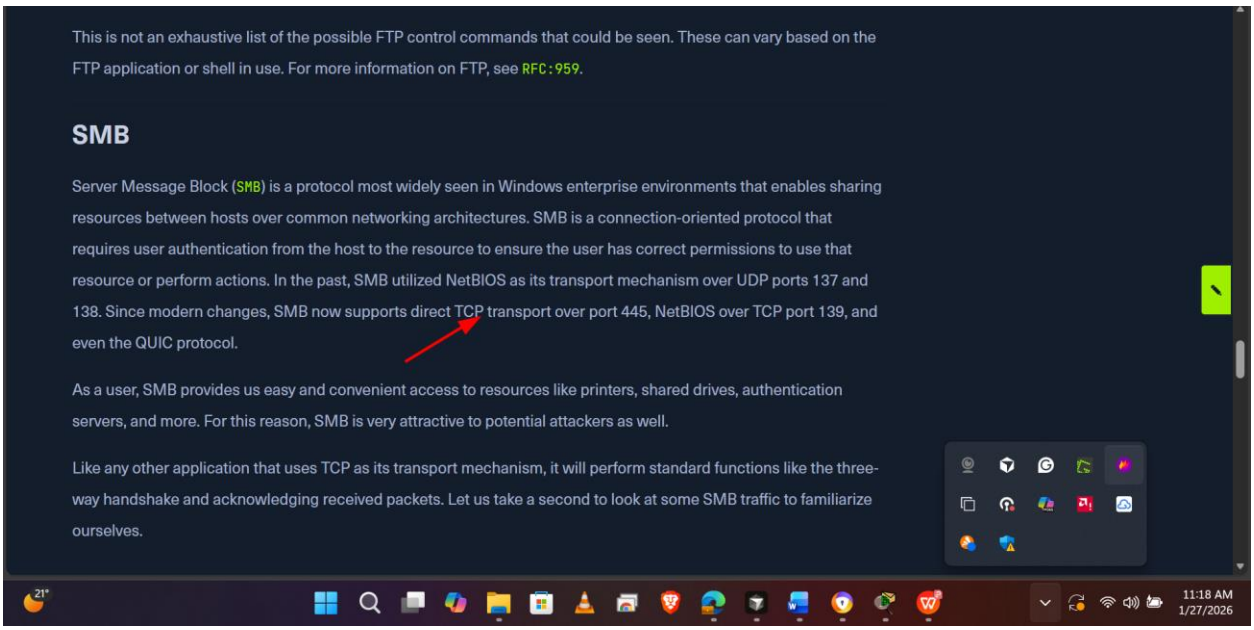
Answer: 20 21

Week 2 Assignment 2



Does SMB utilize TCP or UDP as its transport layer protocol?

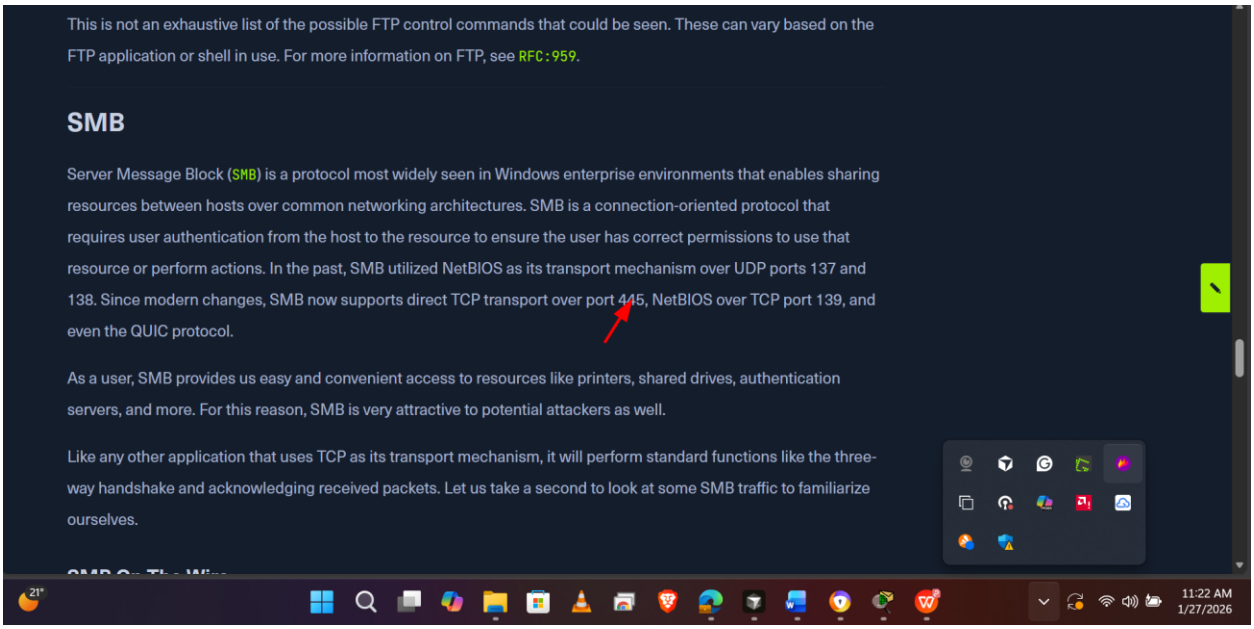
Answer: TCP



SMB has moved to using what TCP port?

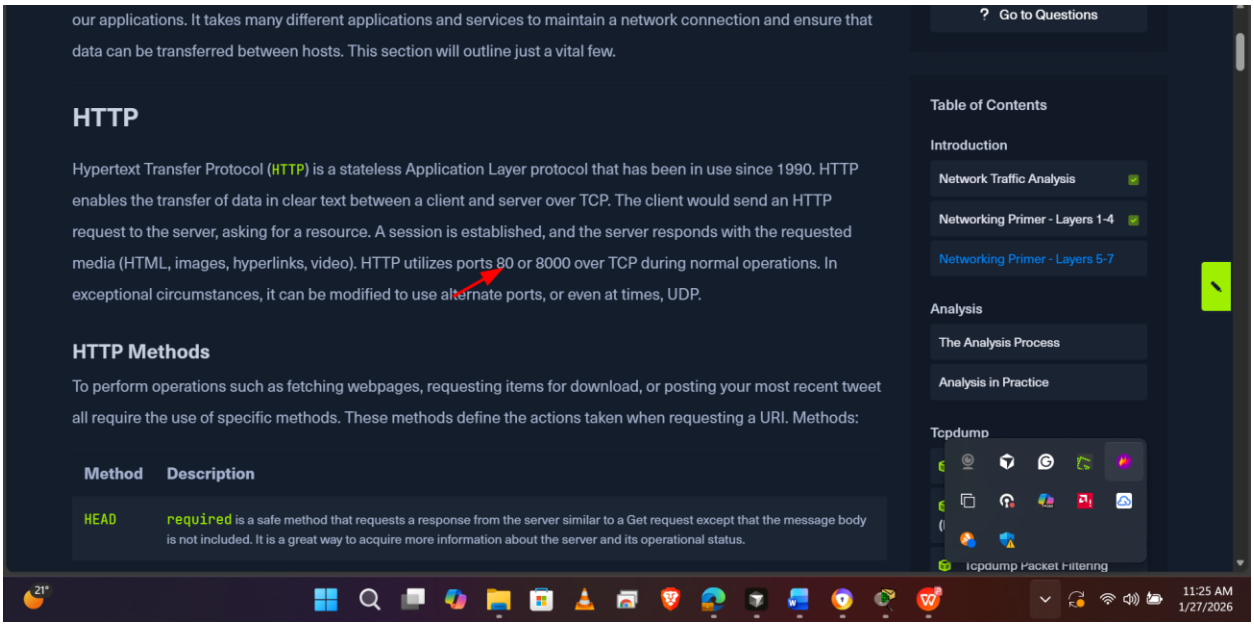
Answer: 445

Week 2 Assignment 2



Hypertext Transfer Protocol uses what well known TCP port number?

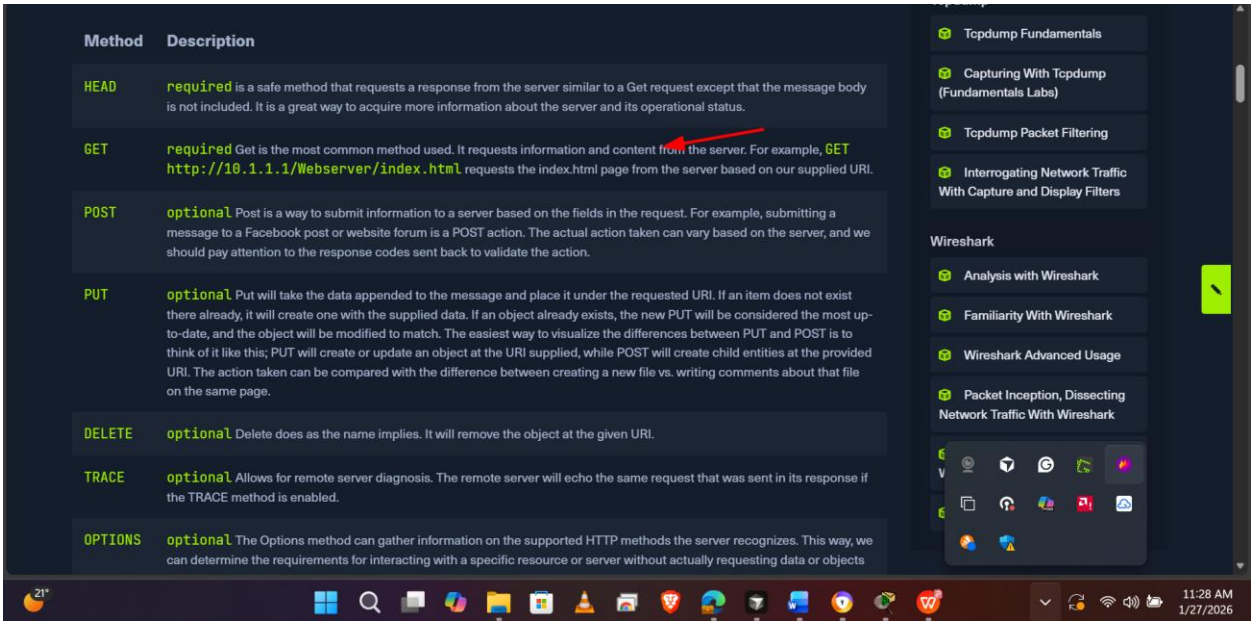
Answer: 80



What HTTP method is used to request information and content from the webserver?

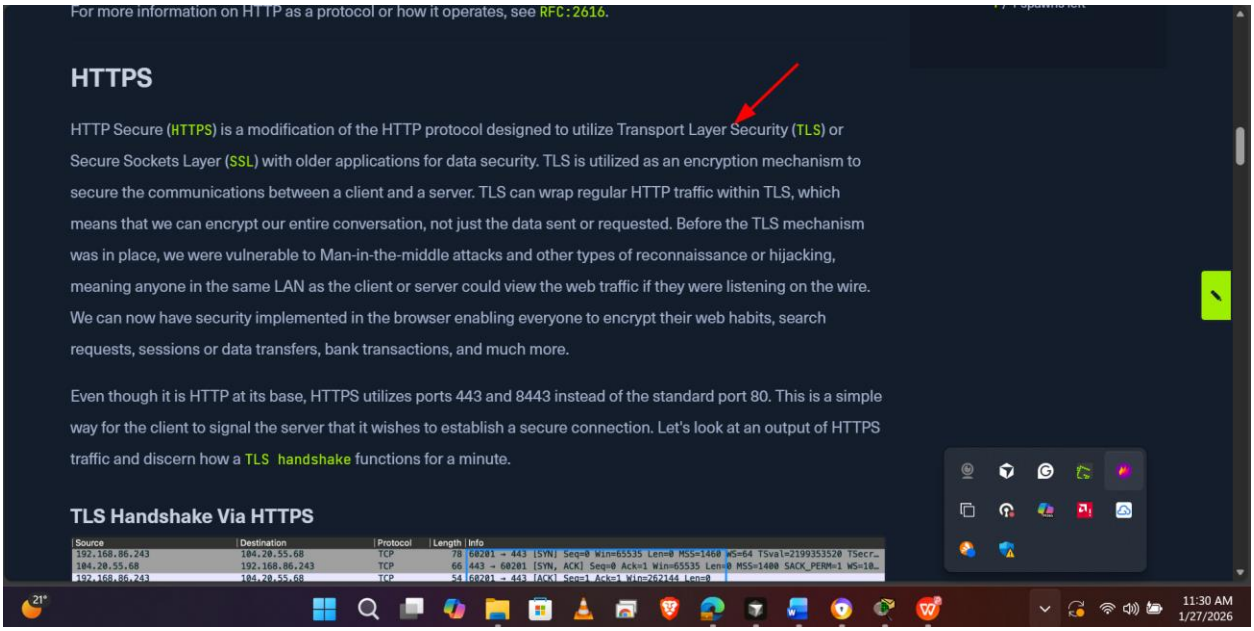
Answer: GET

Week 2 Assignment 2



What web based protocol uses TLS as a security measure?

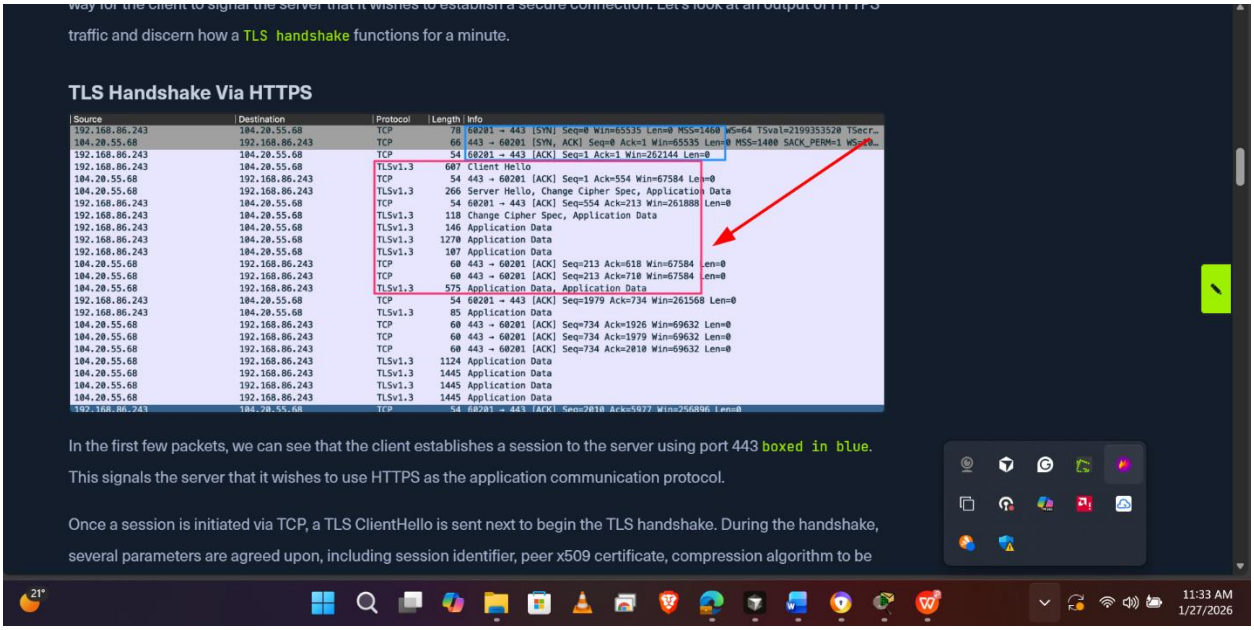
Answer: HTTPS



True or False: when utilizing HTTPS, all data sent across the session will appear as TLS Application data?

Answer: True

Week 2 Assignment 2



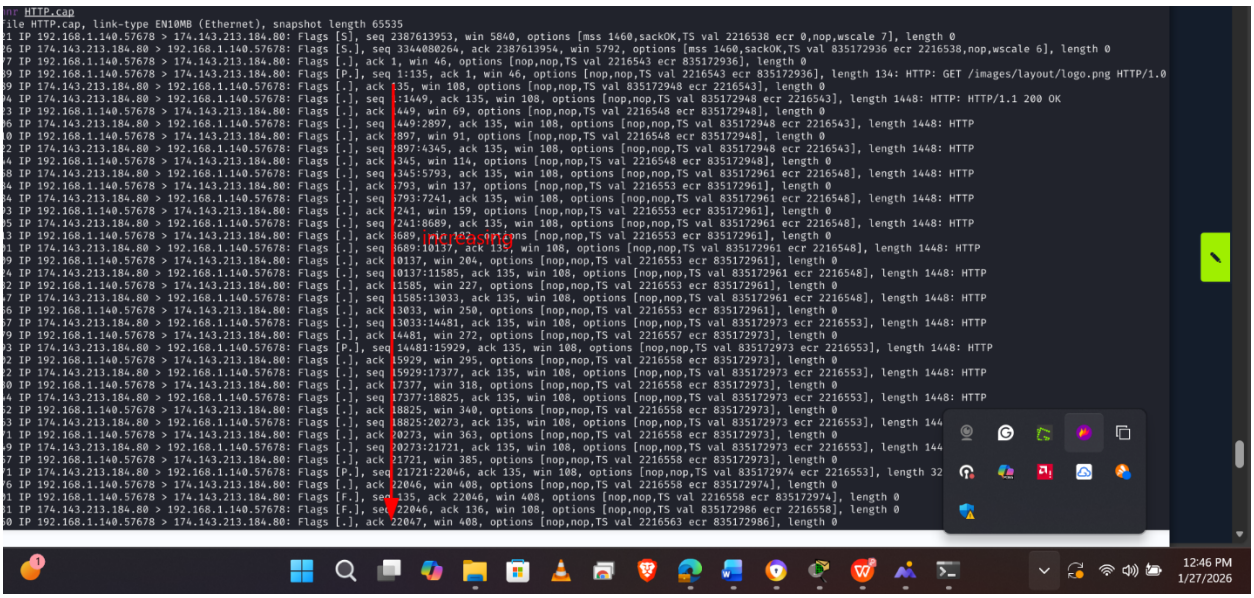
Tcpdump Fundamentals

Utilizing the output shown in question-1.png, who is the server in this communication? (IP Address)

Answer: 174.143.213.184

Were absolute or relative sequence numbers used during the capture? (see question-1.zip to answer)

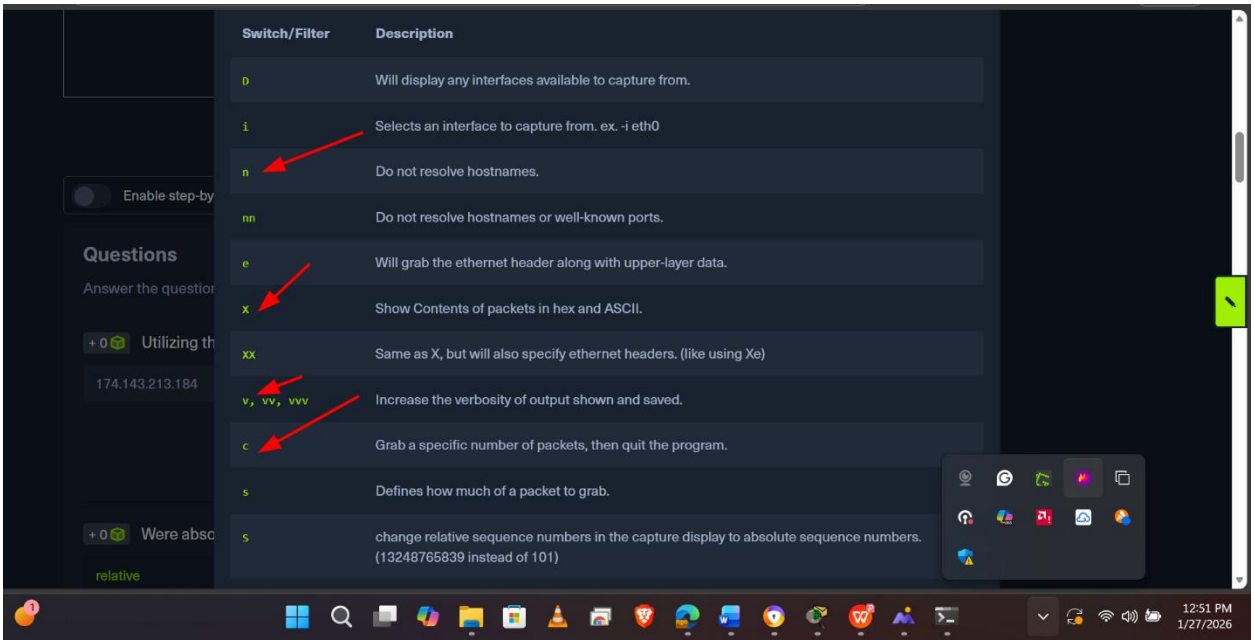
Answer: Relative



Week 2 Assignment 2

If I wish to start a capture without hostname resolution, verbose output, showing contents in ASCII and hex, and grab the first 100 packets; what are the switches used? please answer in the order the switches are asked for in the question.

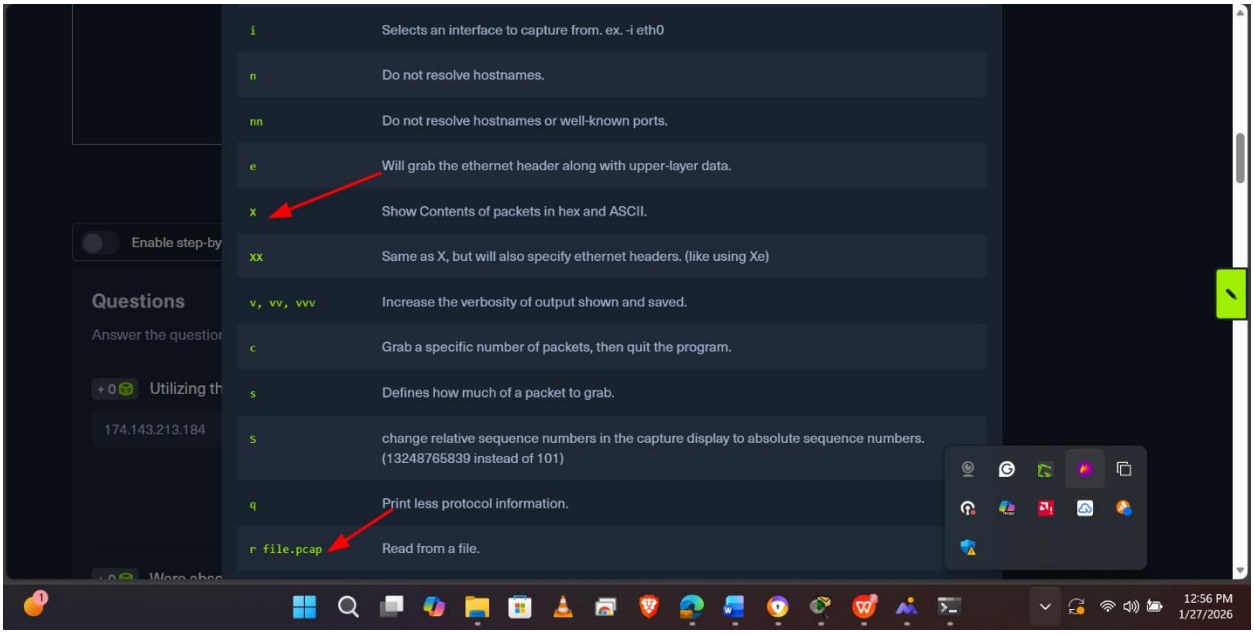
Answer: -nvXc 100



Given the capture file at /tmp/capture.pcap, what tcpdump command will enable you to read from the capture and show the output contents in Hex and ASCII? (Please use best practices when using switches)

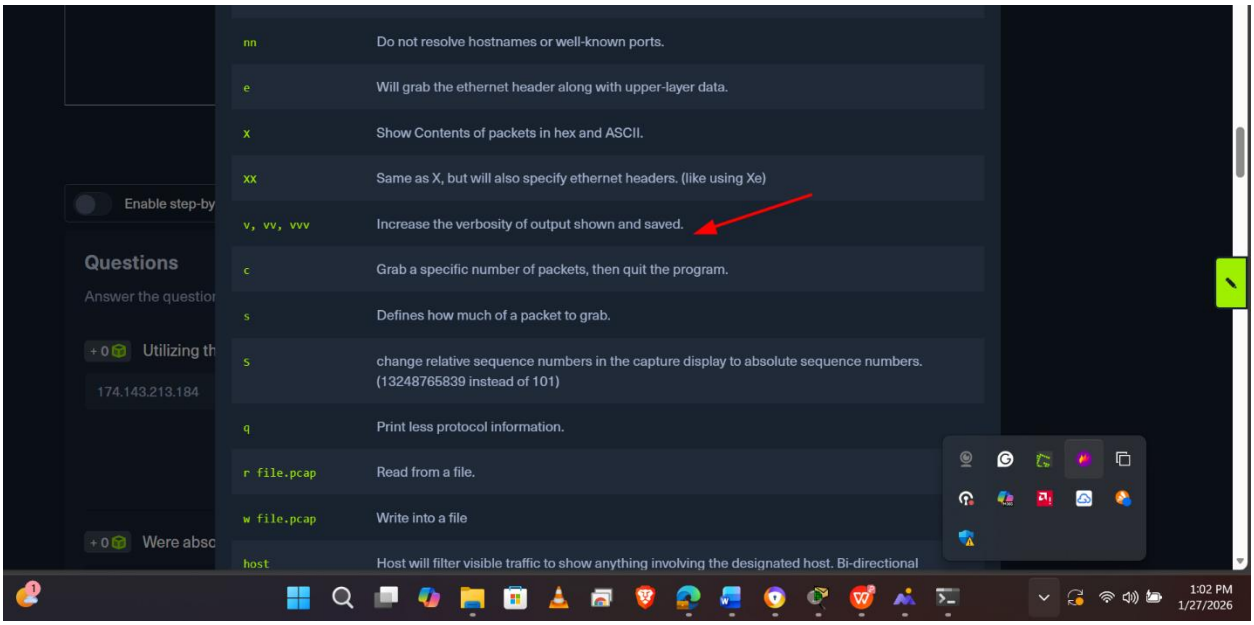
Answer: sudo tcpdump -Xr /tmp/capture.pcap

Week 2 Assignment 2



What TCPDump switch will increase the verbosity of our output? (Include the - with the proper switch)

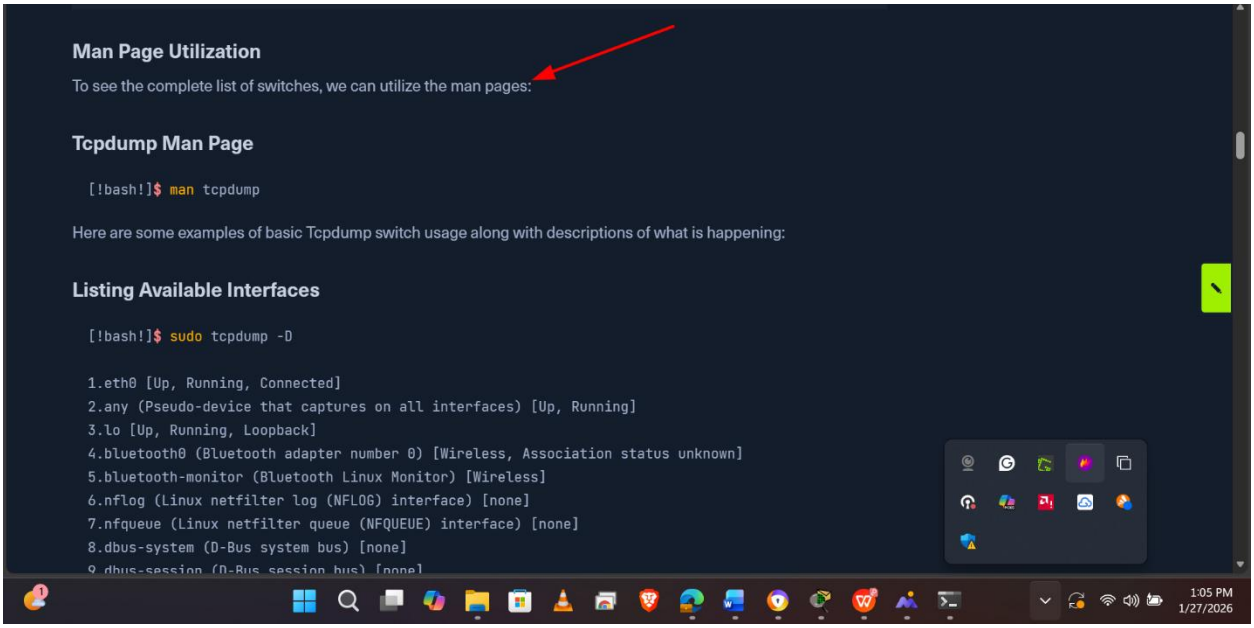
Answer: -v



What built in terminal help reference can tell us more about TCPDump?

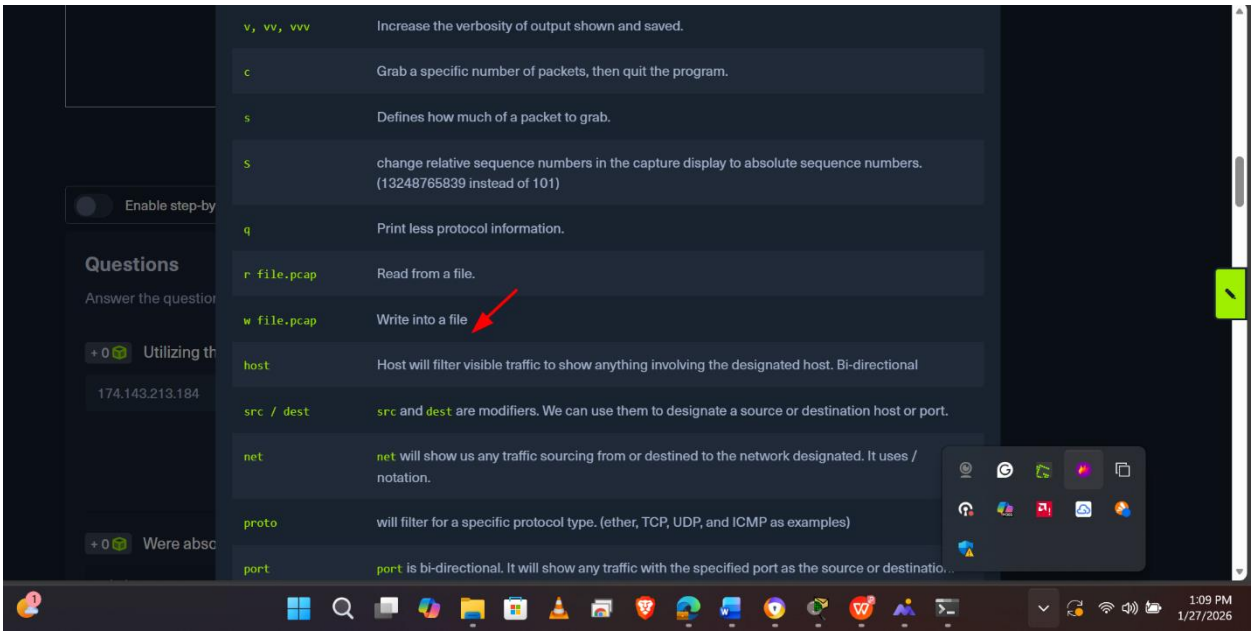
Answer: man

Week 2 Assignment 2



What TCPDump switch will let me write my output to a file?

Answer: -w

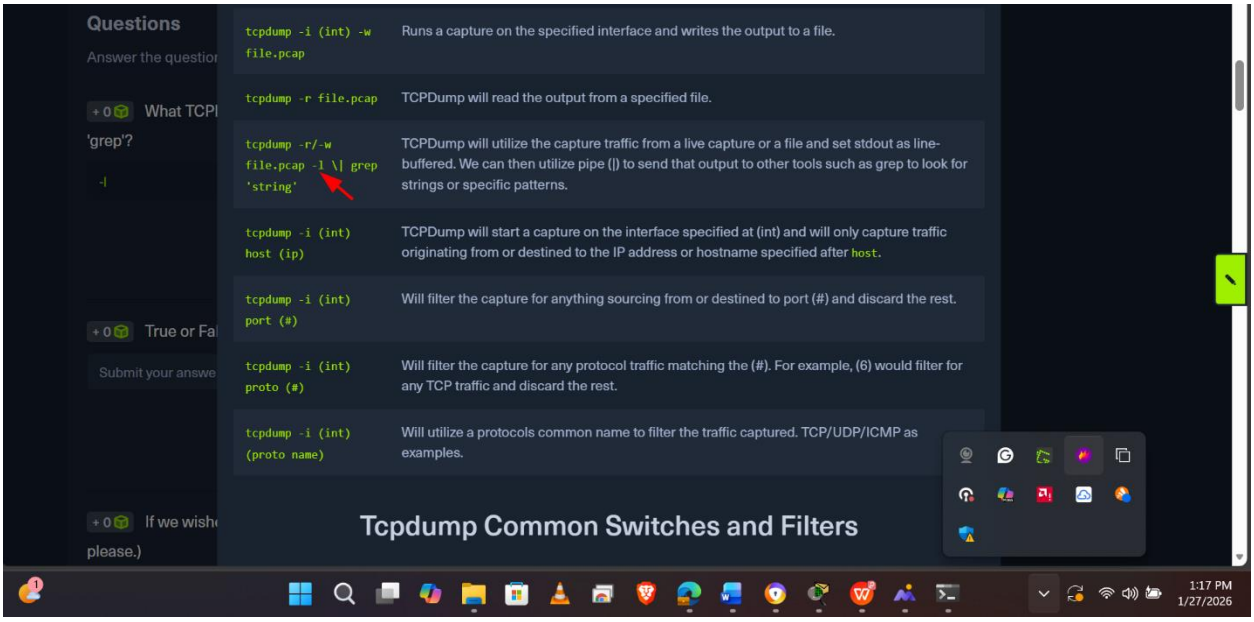


Fundamentals Lab

What TCPDump switch will allow us to pipe the contents of a pcap file out to another function such as 'grep'?

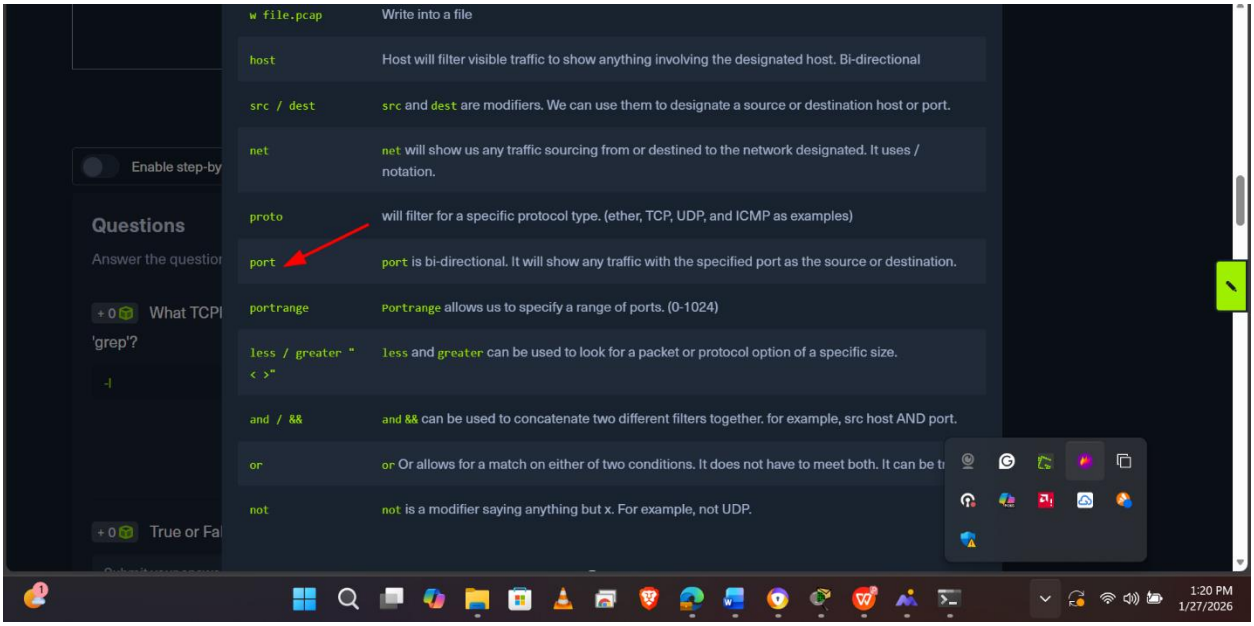
Answer: -l

Week 2 Assignment 2



True or False: The filter "port" looks at source and destination traffic.

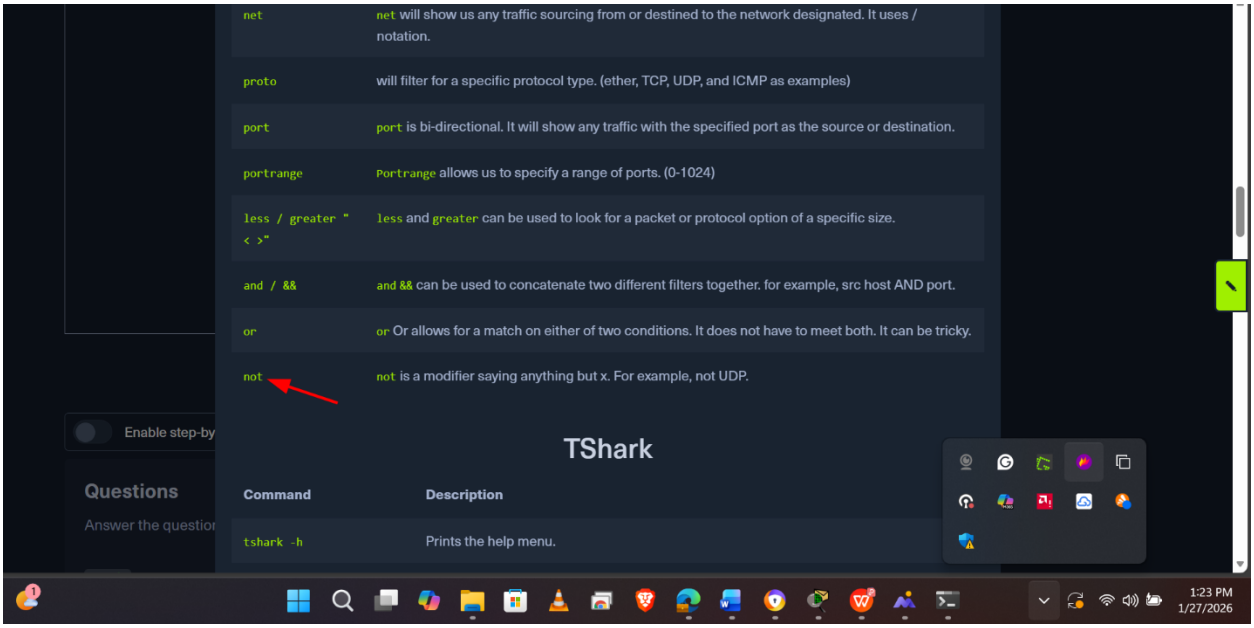
Answer: True



If we wished to filter out ICMP traffic from our capture, what filter could we use? (word only, not symbol please.)

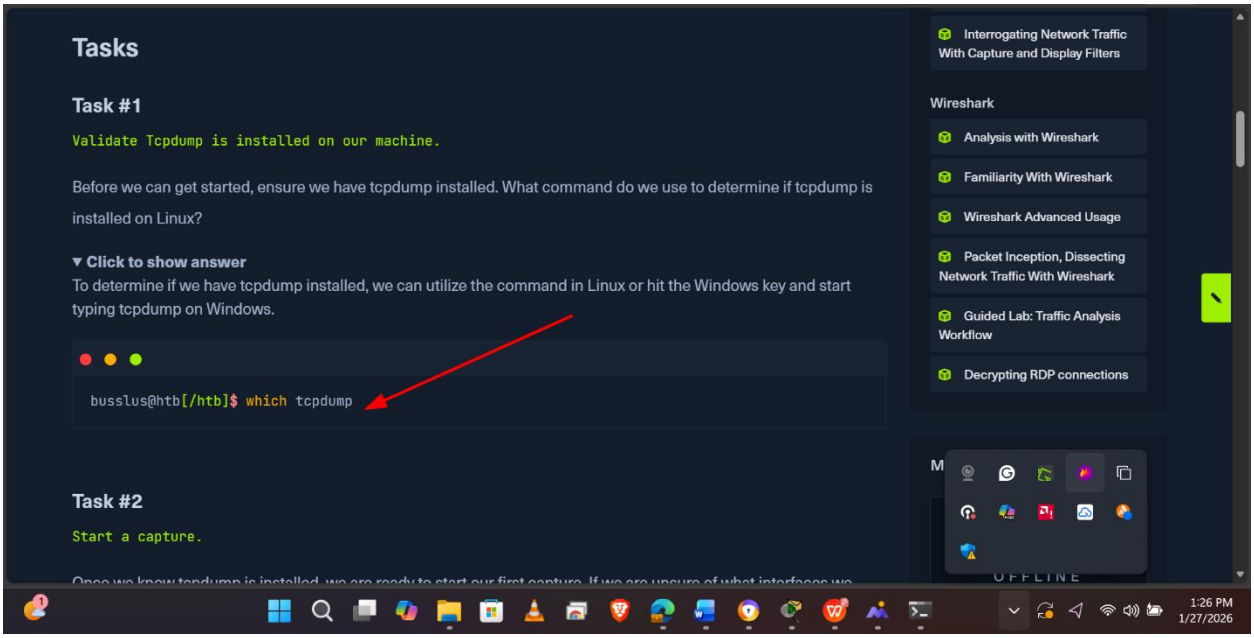
Answer: not ICMP

Week 2 Assignment 2



What command will show you where / if TCPDump is installed?

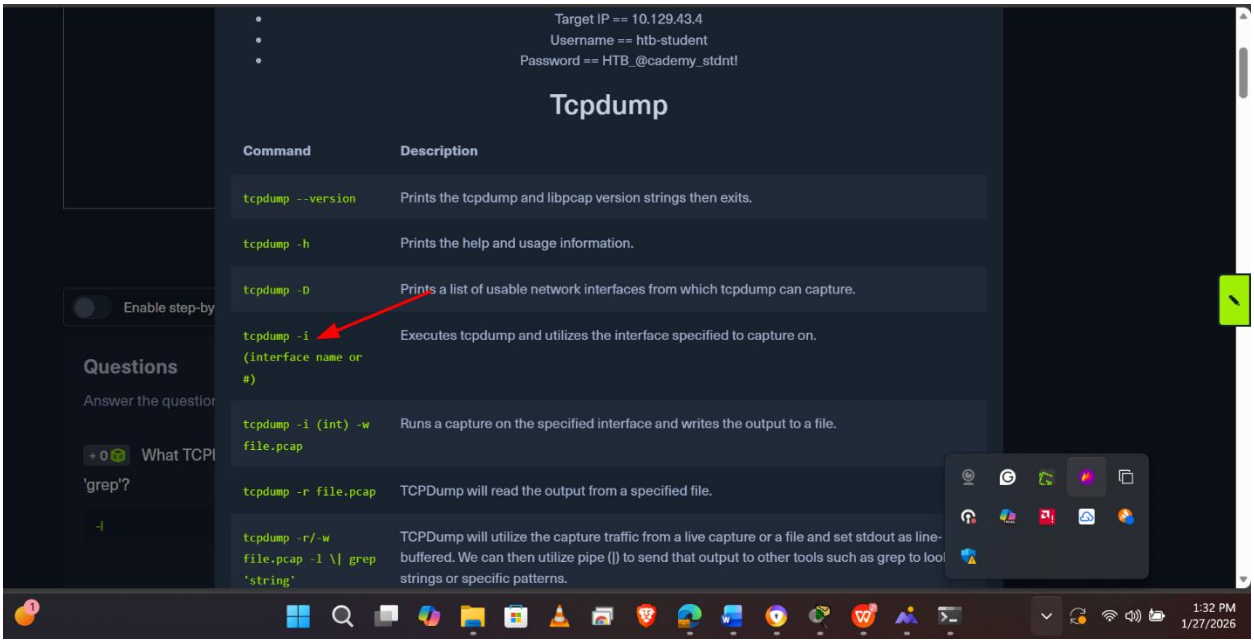
Answer: which tcpdump



How do you start a capture with TCPDump to capture on eth0?

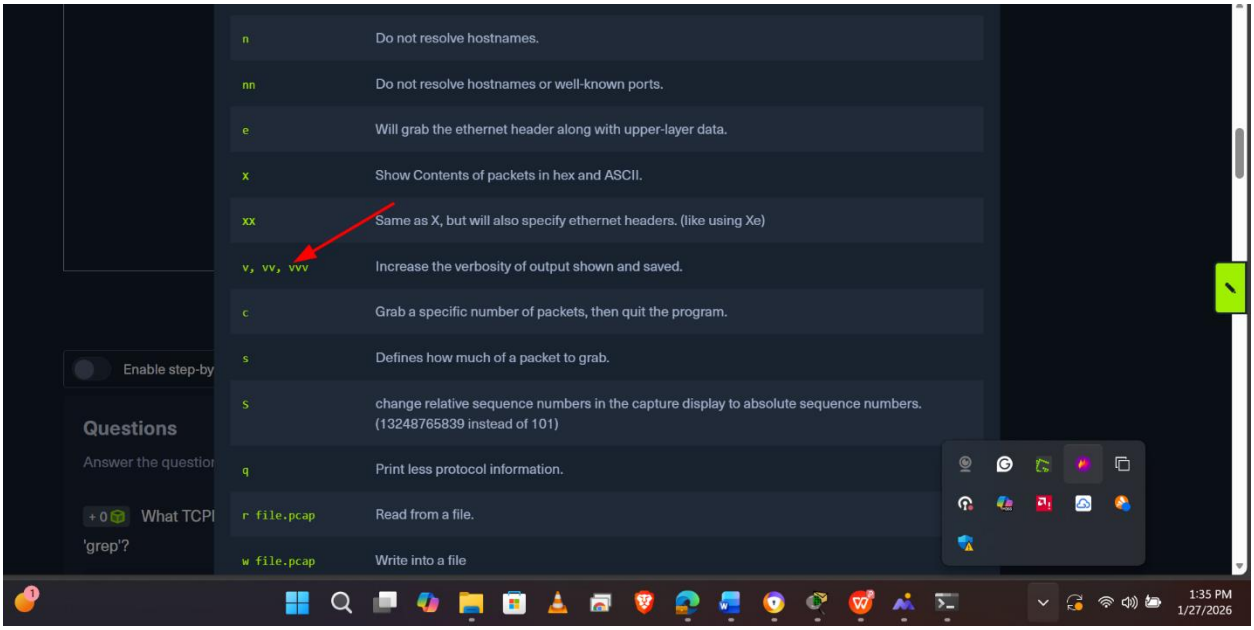
Answer: tcpdump -i eth0

Week 2 Assignment 2



What switch will provide more verbosity in your output?

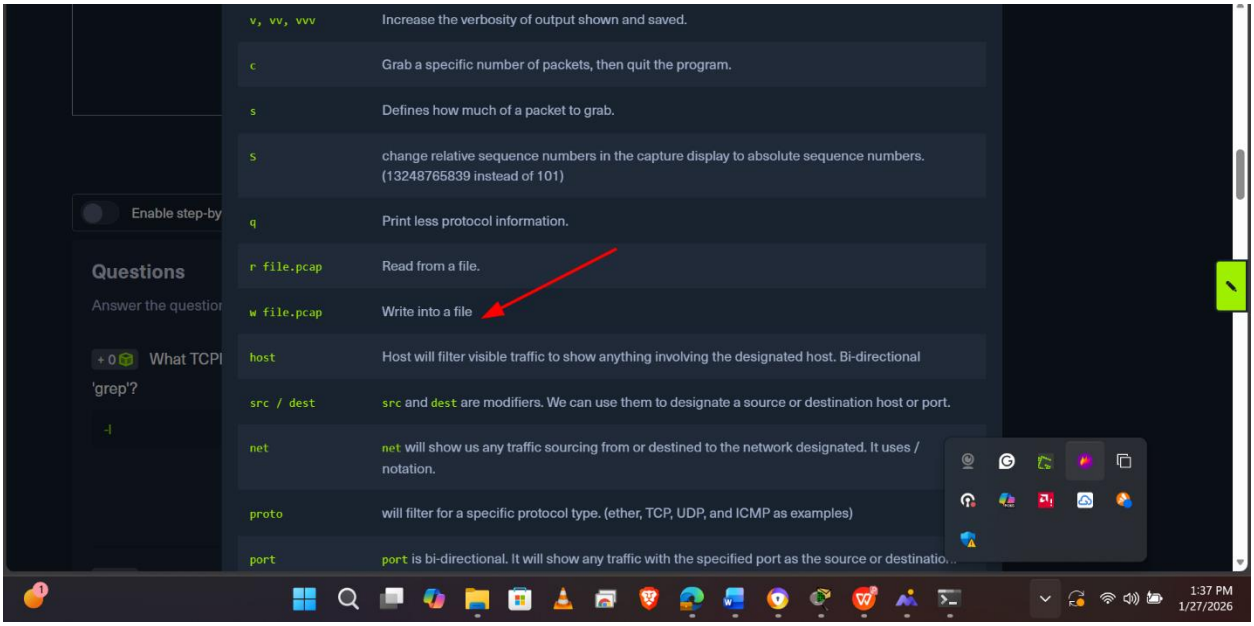
Answer: -v



What switch will write your capture output to a .pcap file?

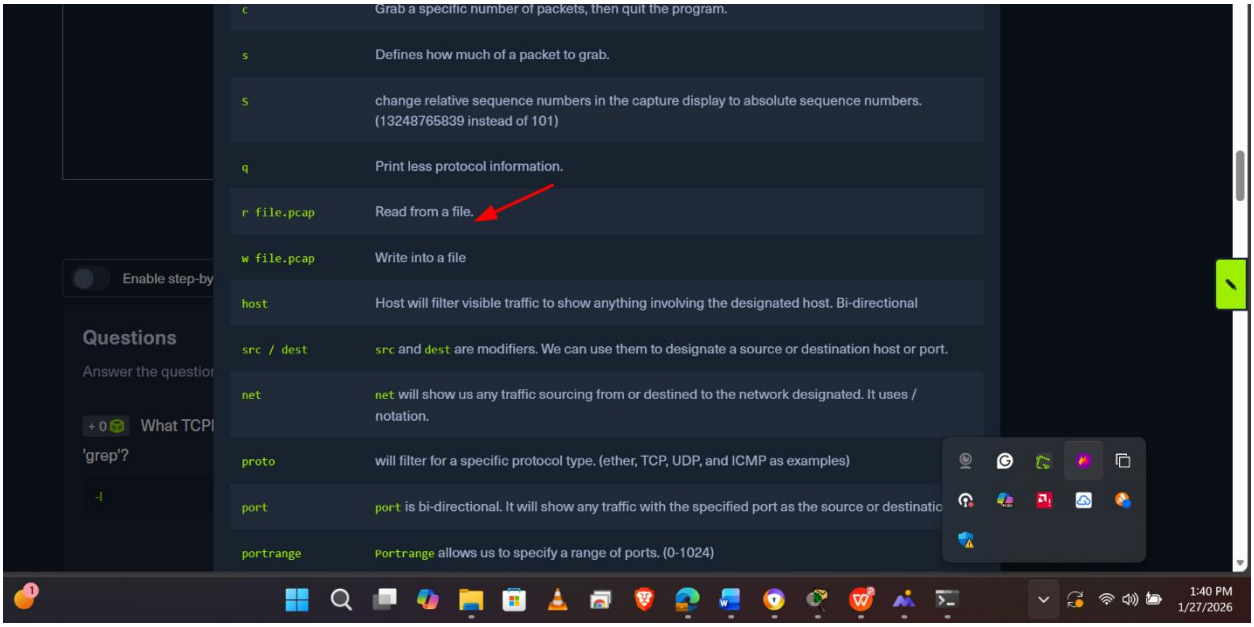
Answer: -w

Week 2 Assignment 2



What switch will read a capture from a .pcap file?

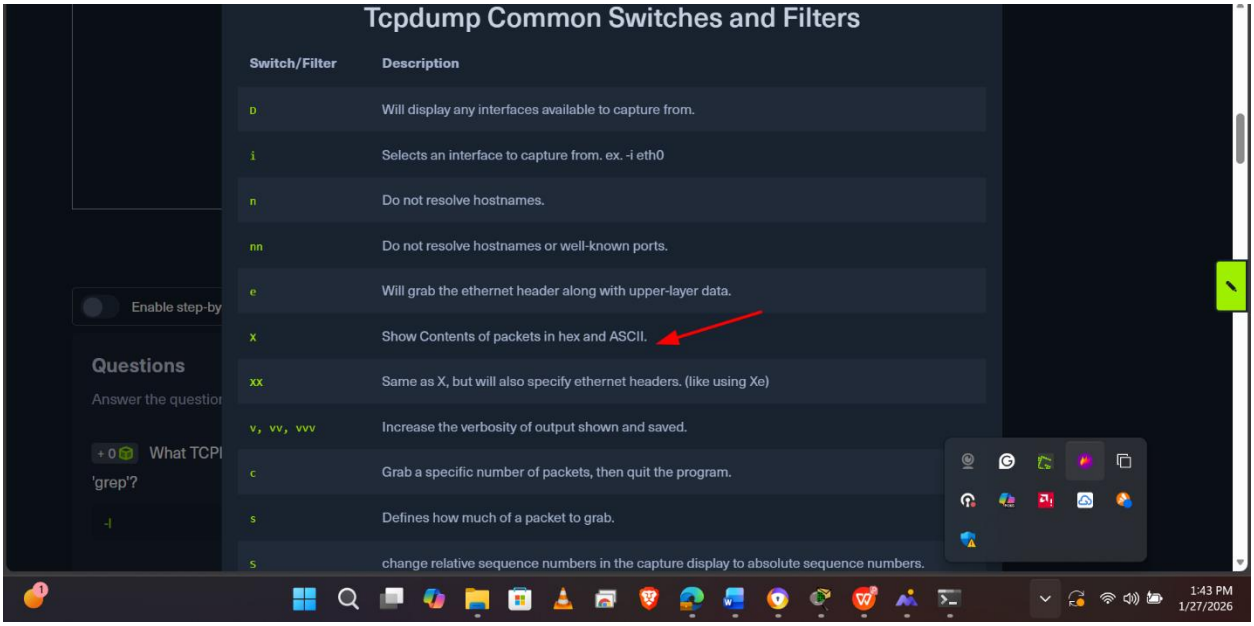
Answer: -r



What switch will show the contents of a capture in Hex and ASCII?

Answer: -X

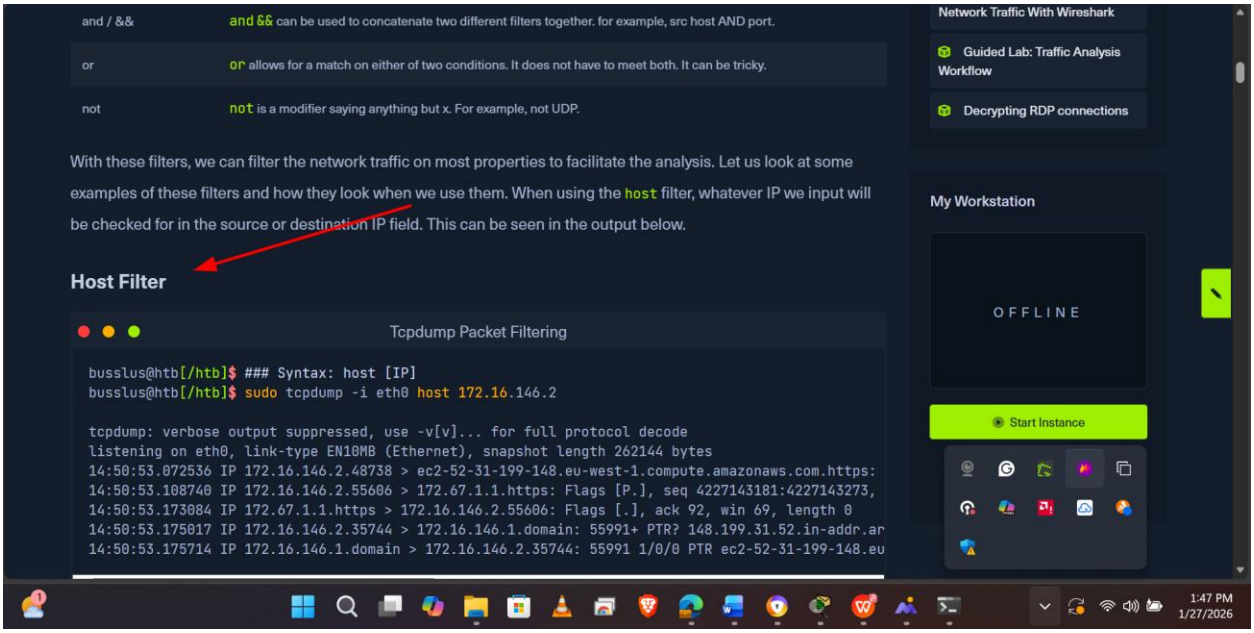
Week 2 Assignment 2



Tcpdump Packet Filtering

What filter will allow me to see traffic coming from or destined to the host with an ip of 10.10.20.1?

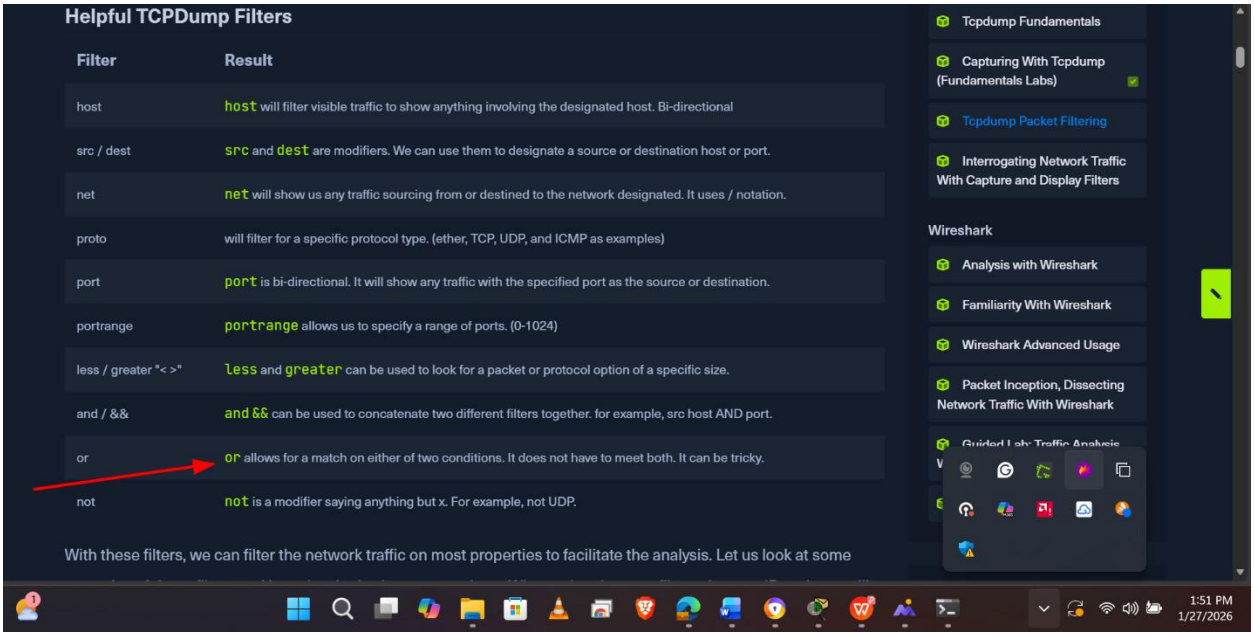
Answer: host 10.10.20.1



What filter will allow me to capture based on either of two options?

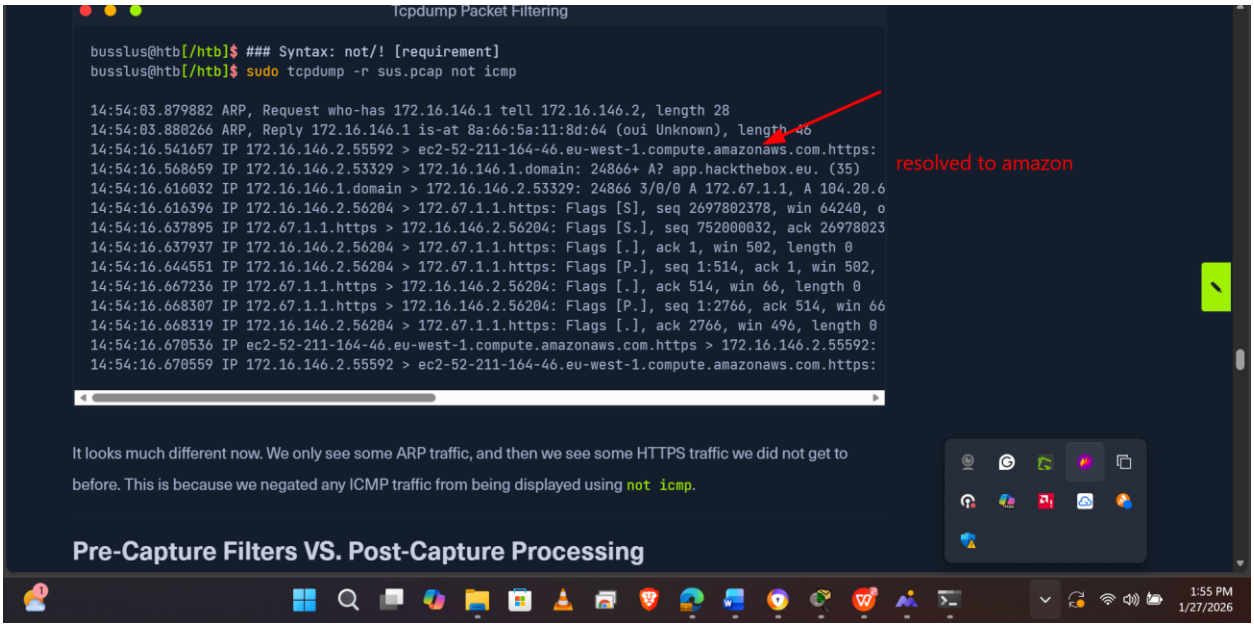
Answer: or

Week 2 Assignment 2



True or False: TCPDump will resolve IPs to hostnames by default.

Answer: true

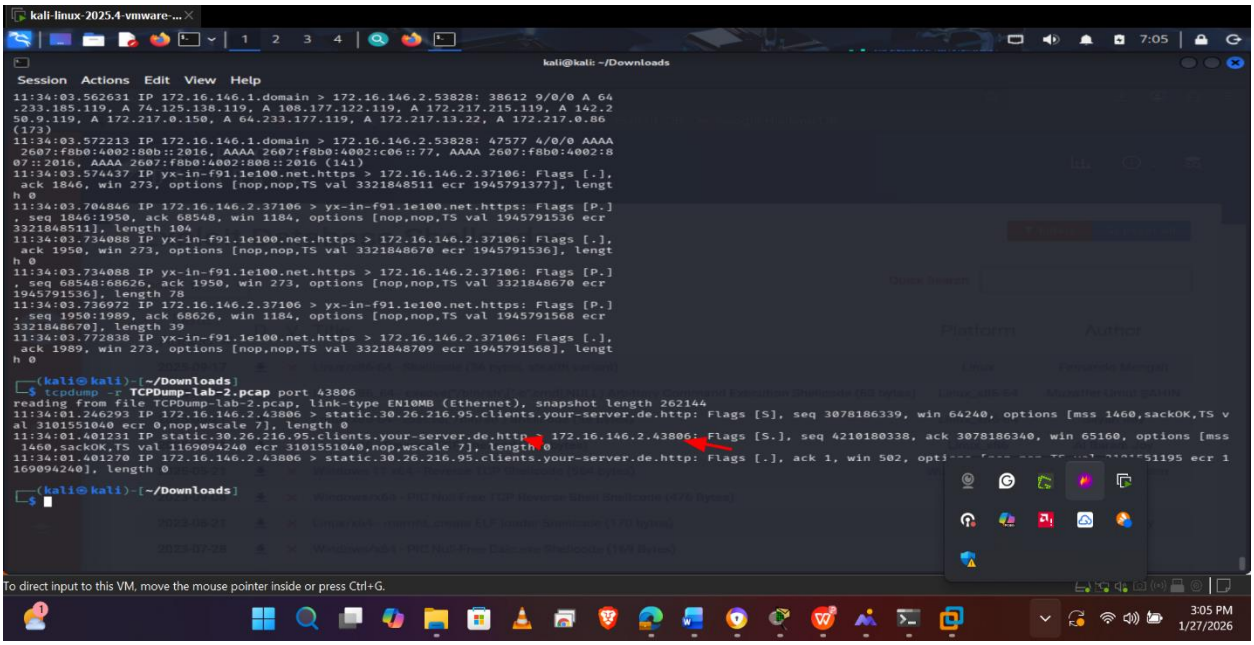


Interrogating Network Traffic With Capture and Display Filters

What are the client and server port numbers used in first full TCP three-way handshake? (low number first then high number)

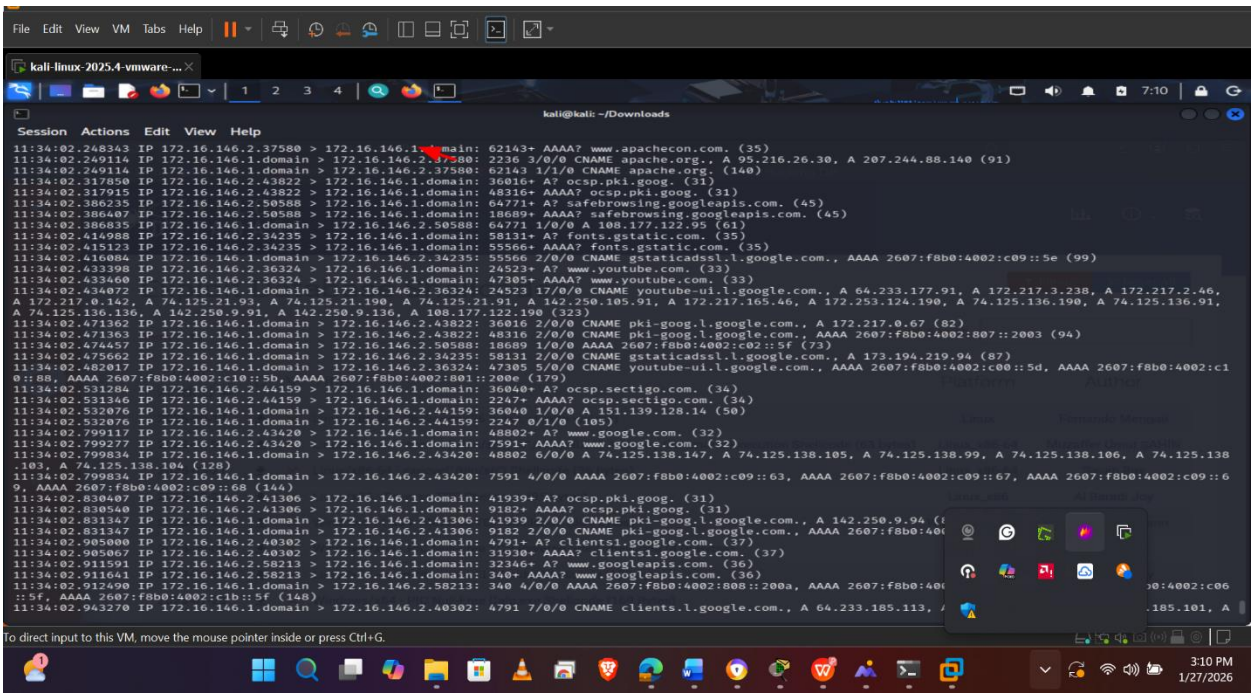
Answer: 80 43806

Week 2 Assignment 2



Based on the traffic seen in the pcap file, who is the DNS server in this network segment? (ip address)

Answer: 172.16.146.1

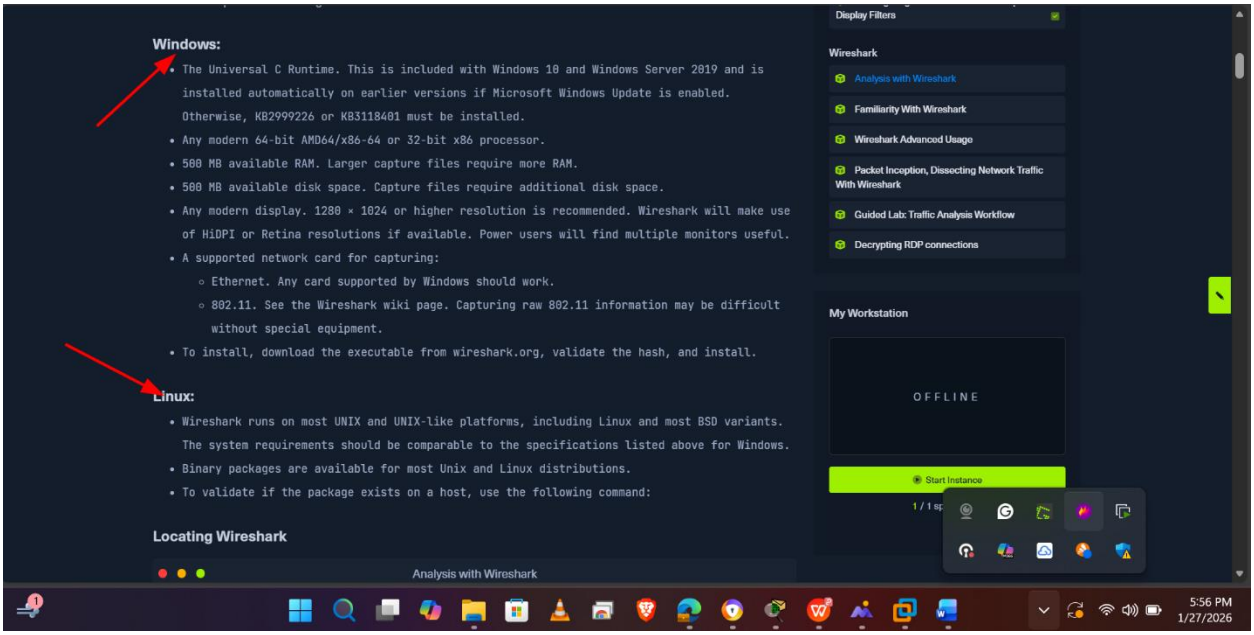


Analysis with Wireshark

True or False: Wireshark can run on both Windows and Linux.

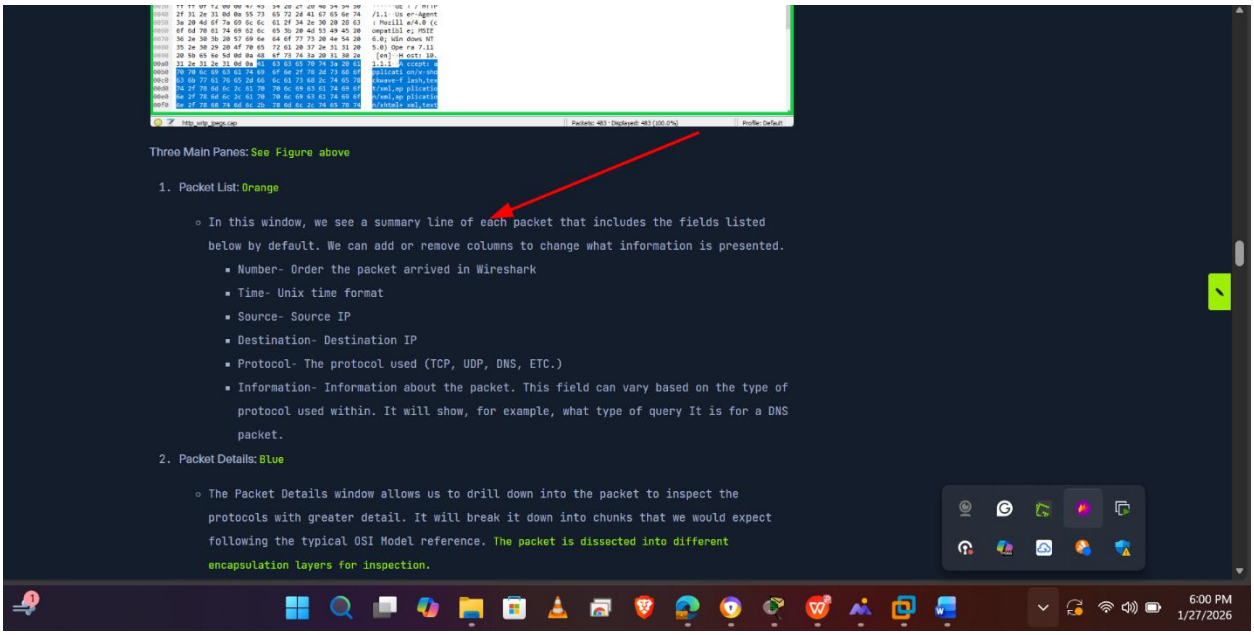
Answer: True

Week 2 Assignment 2



Which Pane allows a user to see a summary of each packet grabbed during the capture?

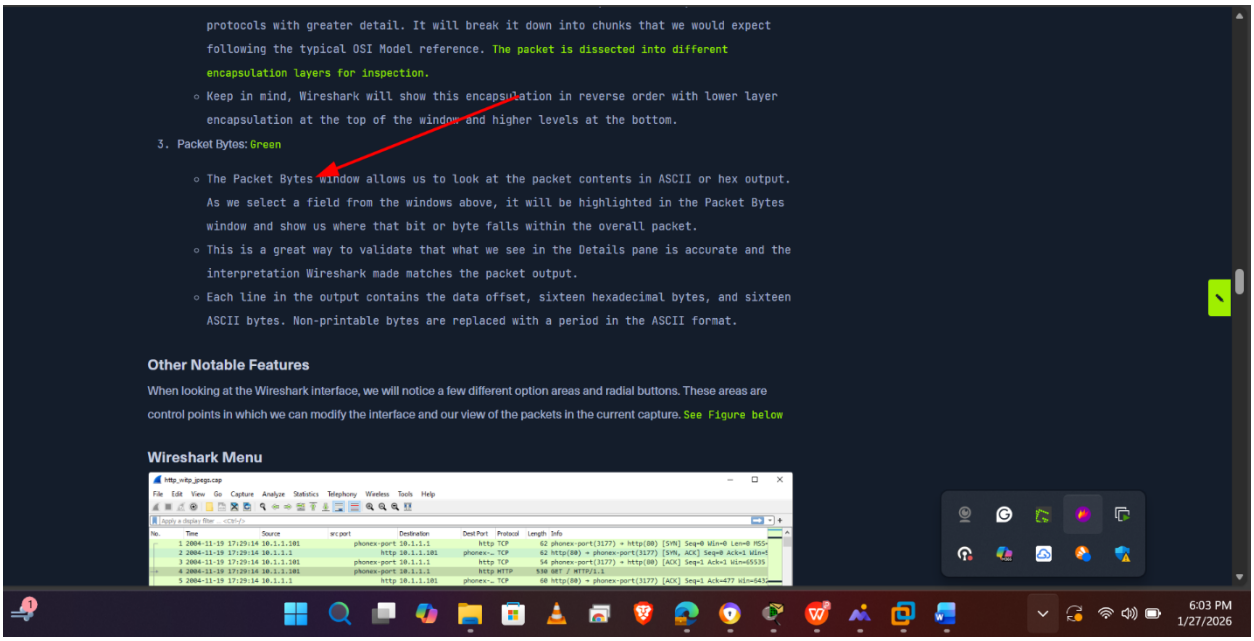
Answer: Packet List



Which pane provides you insight into the traffic you captured and displays it in both ASCII and Hex?

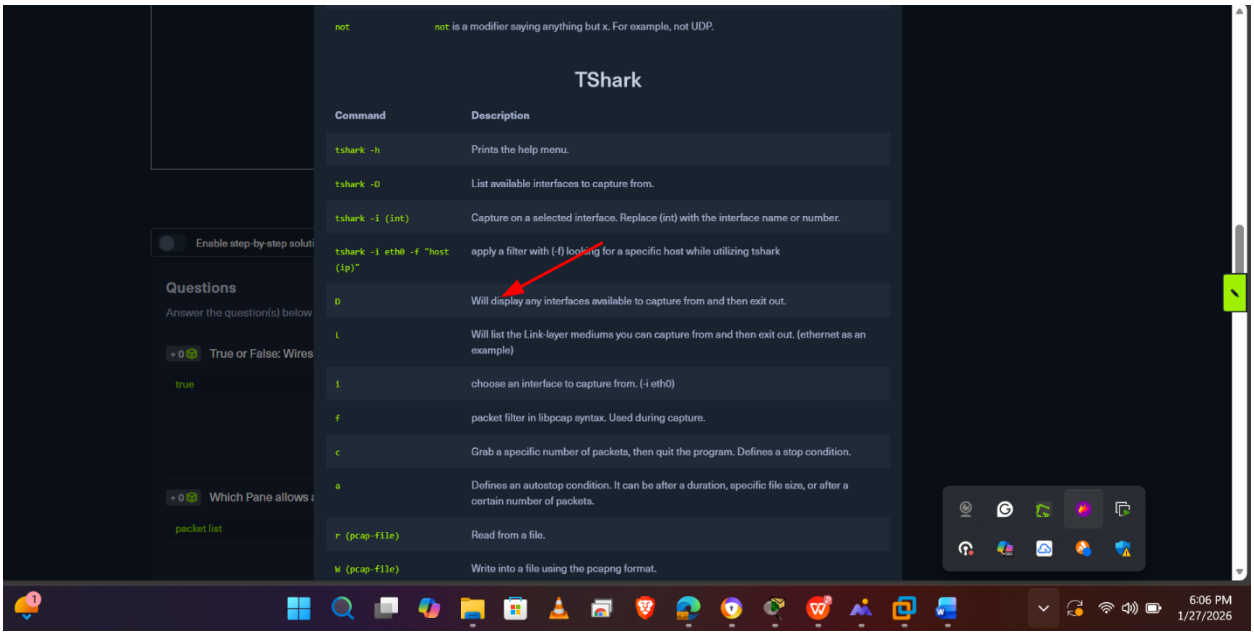
Answer: Packets byte

Week 2 Assignment 2



What switch is used with TShark to list possible interfaces to capture on?

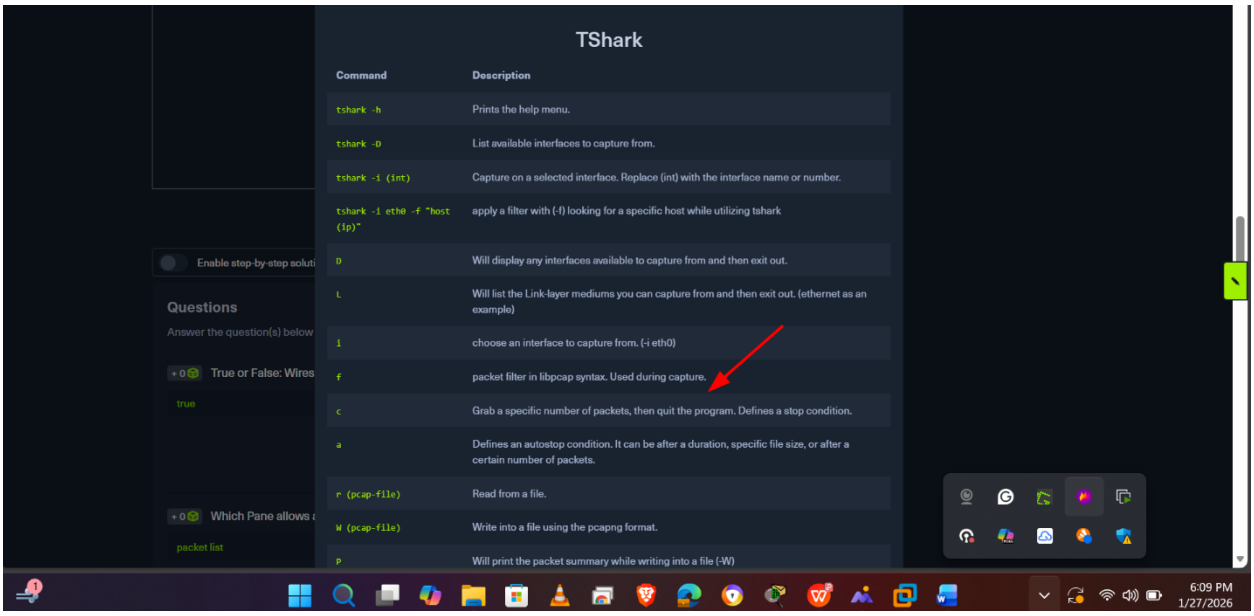
Answer: -D



What switch allows us to apply filters in TShark?

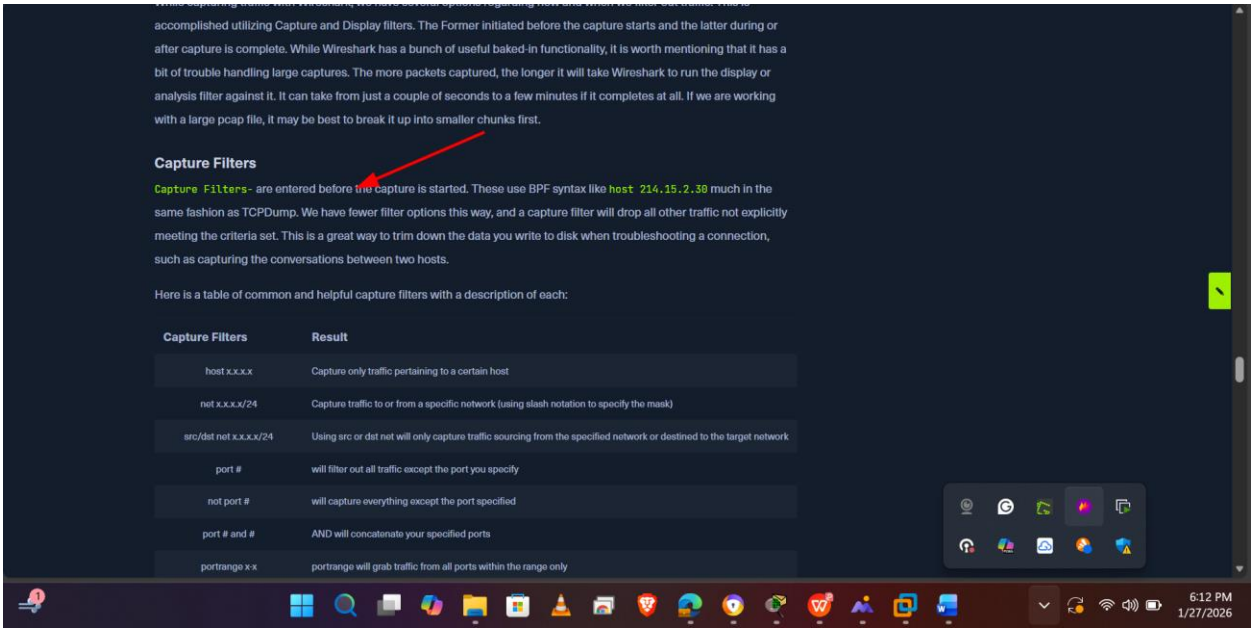
Answer: -f

Week 2 Assignment 2



Is a capture filter applied before the capture starts or after? (answer before or after)

Answer: Before

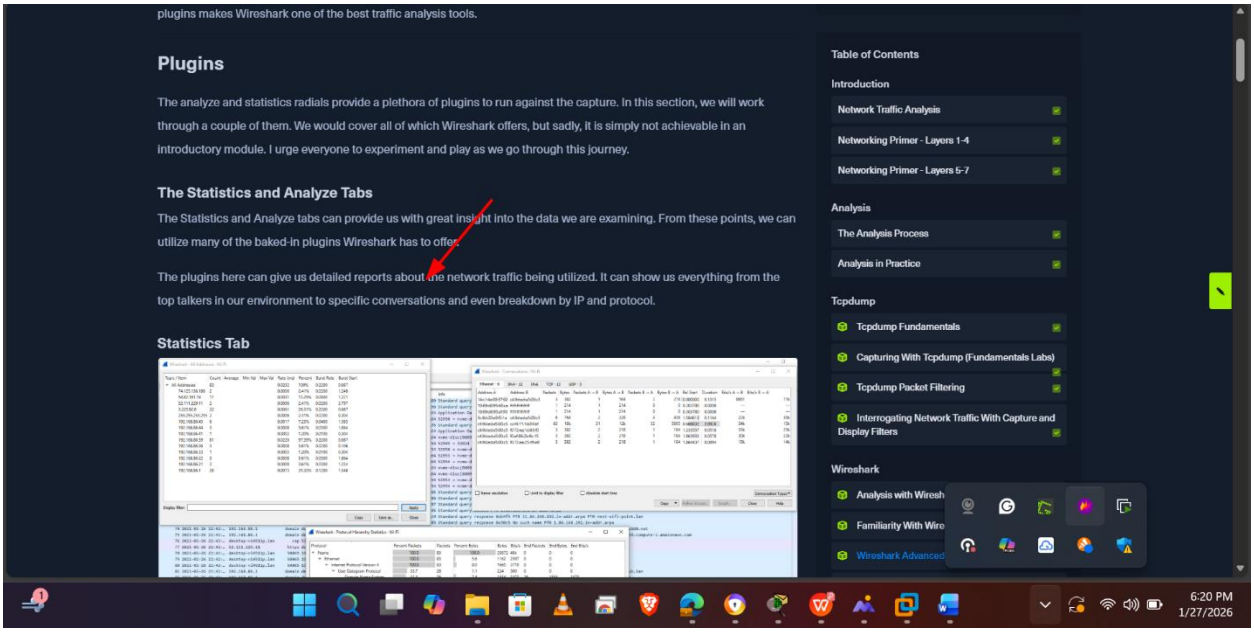


Wireshark Advanced Usage

Which plugin tab can provide us with a way to view conversation metadata and even protocol breakdowns for the entire PCAP file?

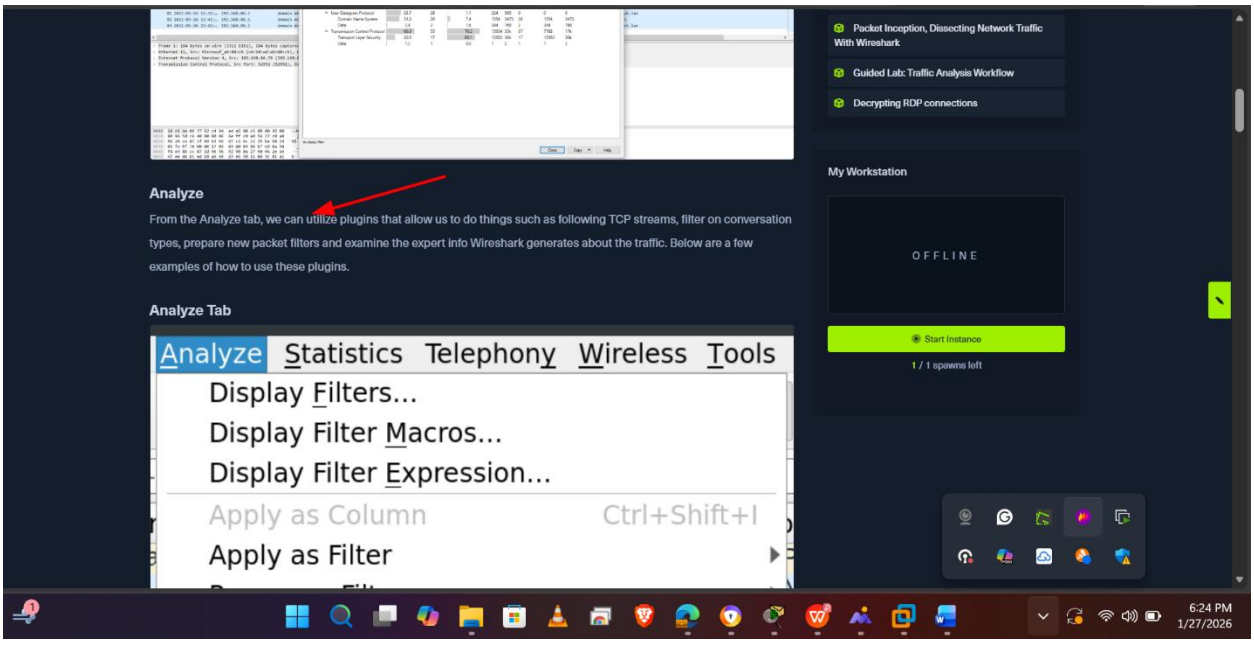
Answer: statistics

Week 2 Assignment 2



What plugin tab will allow me to accomplish tasks such as applying filters, following streams, and viewing expert info?

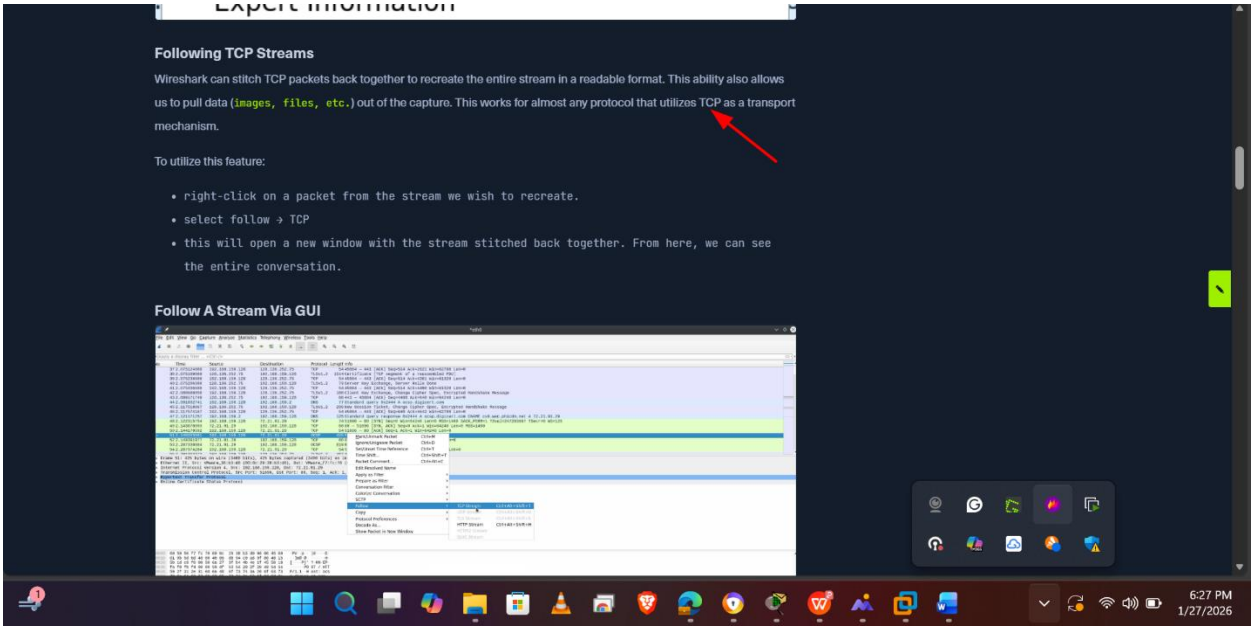
Answer: Analyze



What stream oriented Transport protocol enables us to follow and rebuild conversations and the included data?

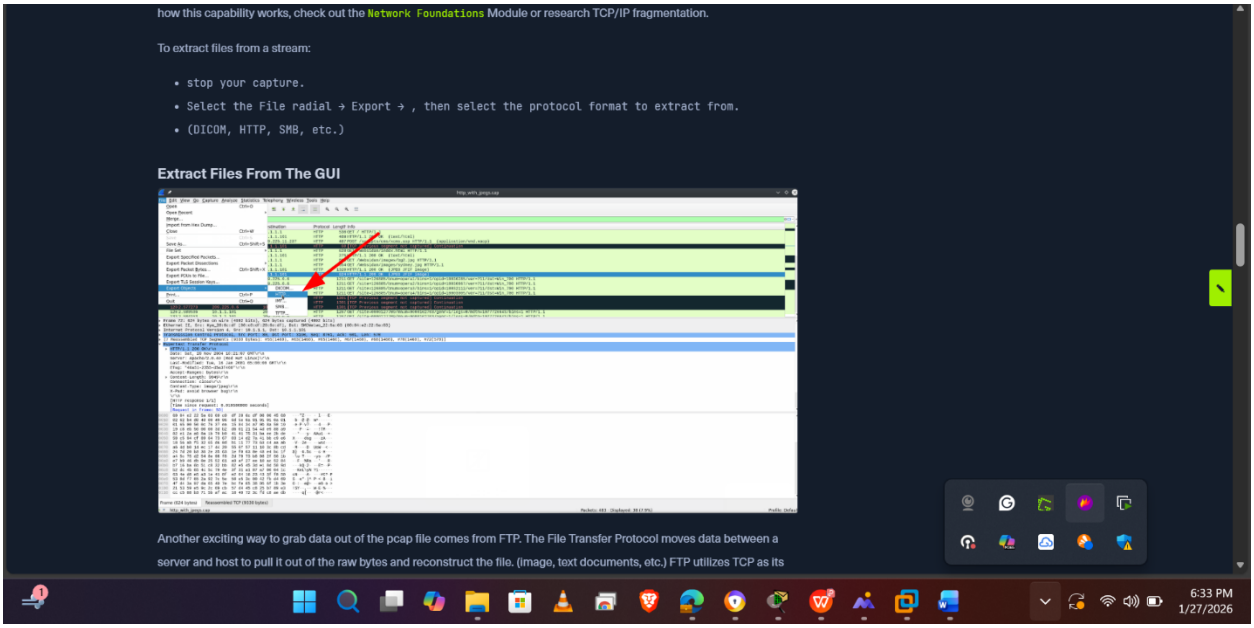
Answer: TCP

Week 2 Assignment 2



True or False: Wireshark can extract files from HTTP traffic.

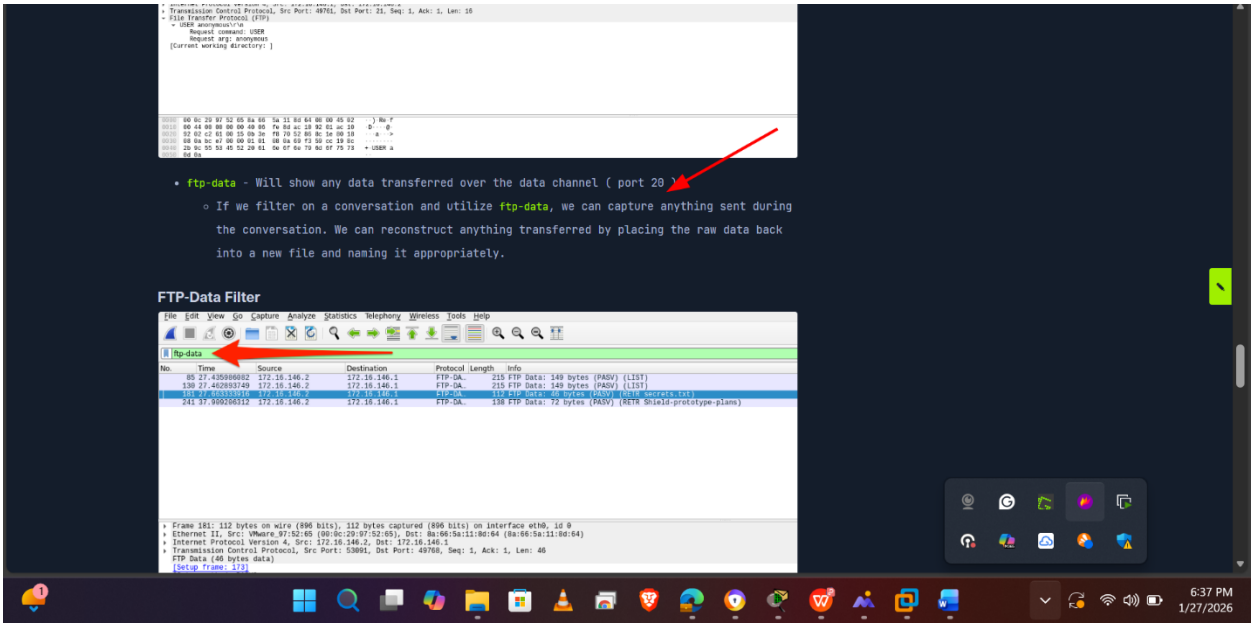
Answer: True



True or False: The ftp-data filter will show us any data sent over TCP port 21.

Answer: False

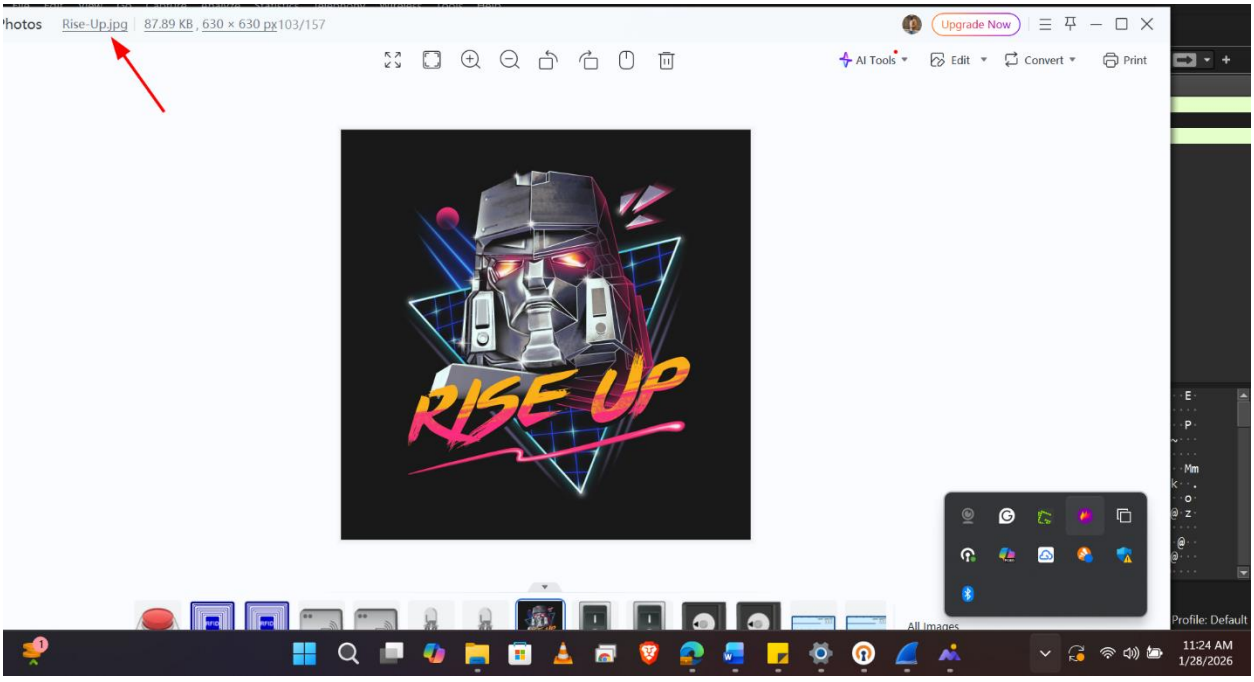
Week 2 Assignment 2



Packet Inception, Dissecting Network Traffic With Wireshark

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

Answer: Rise-up.jpg



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

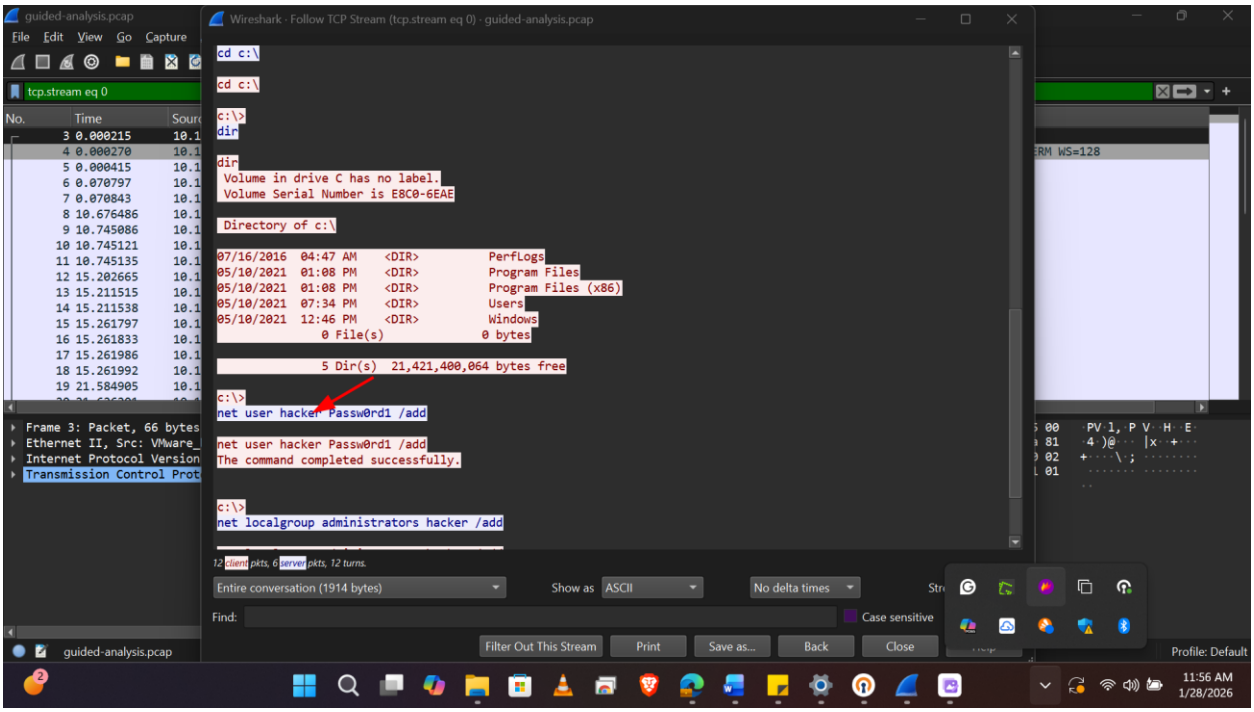
Week 2 Assignment 2

Answer: Bob

Guided Lab: Traffic Analysis Workflow

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

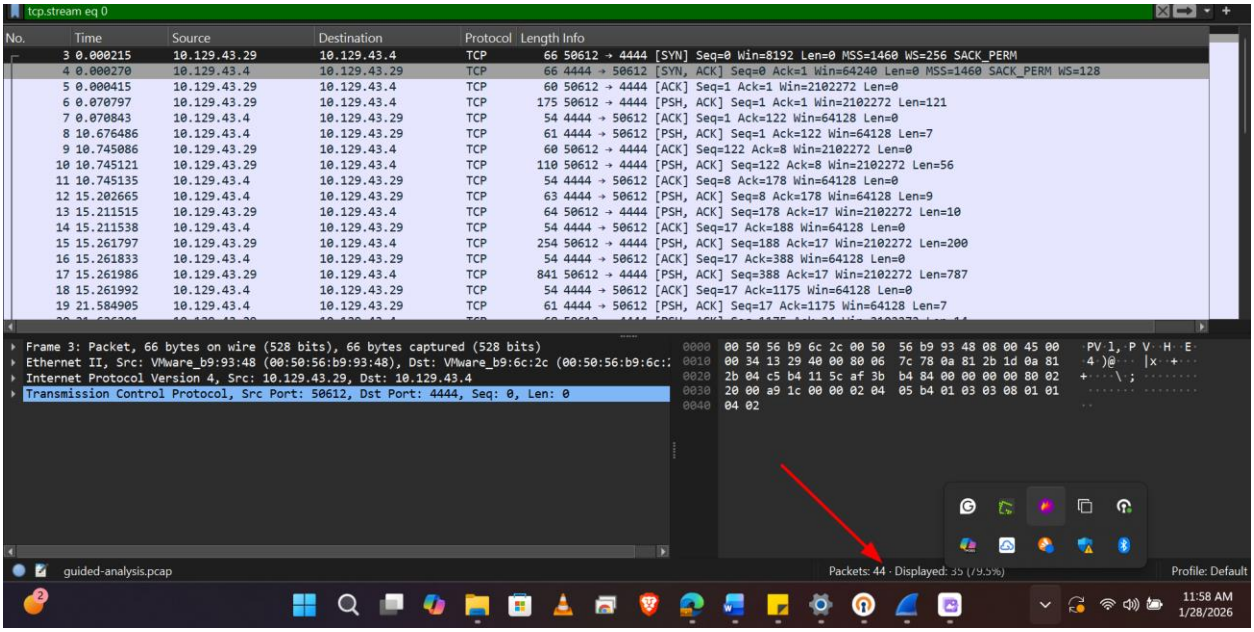
Answer: Hacker



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

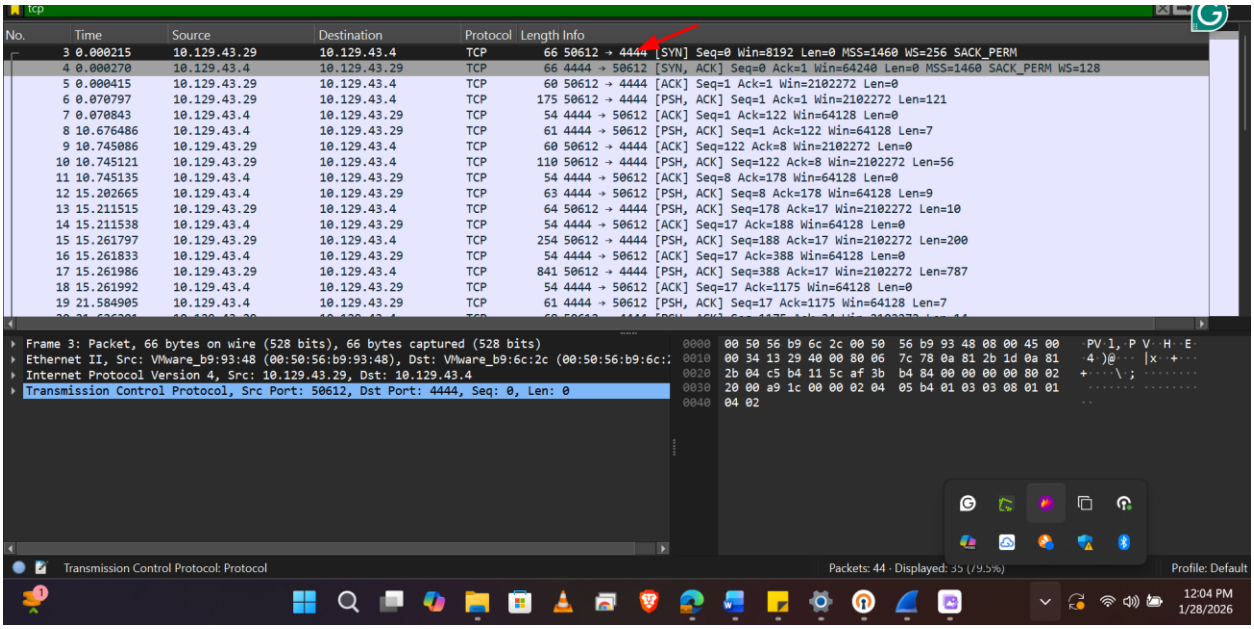
Answer: 44

Week 2 Assignment 2



What was the suspicious port that was being used?

Answer: 4444

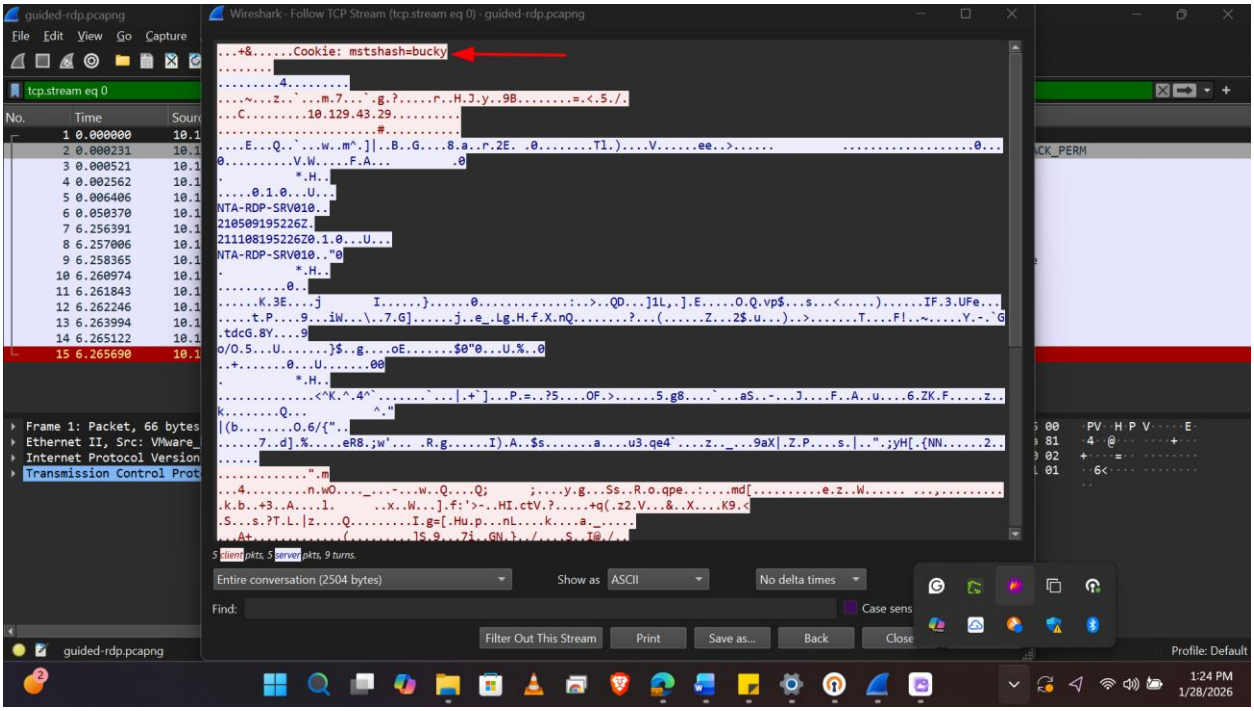


Decrypting RDP connections

What user account was used to initiate the RDP connection?

Answer: bucky

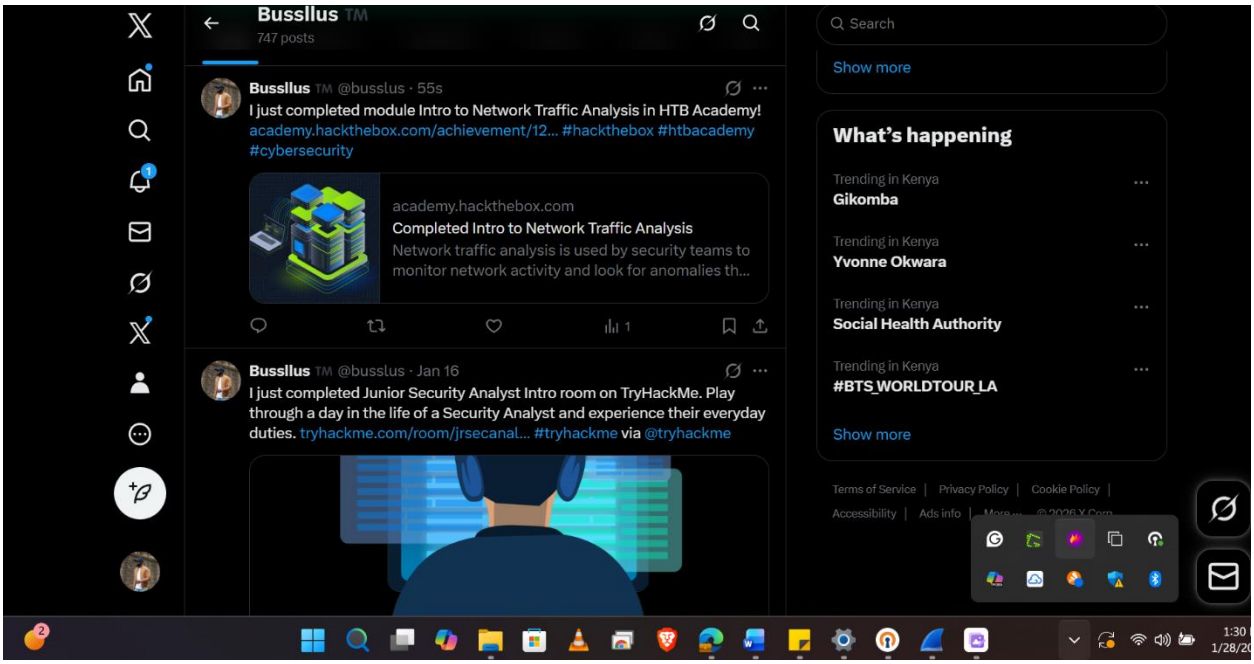
Week 2 Assignment 2



.

Verification of Completion

This completion has been shared on professional networks like Twitter to publicly document my commitment to continuous learning in cybersecurity. This section provides the official verification artifacts for the "Intro to Network Traffic Analysis" module.



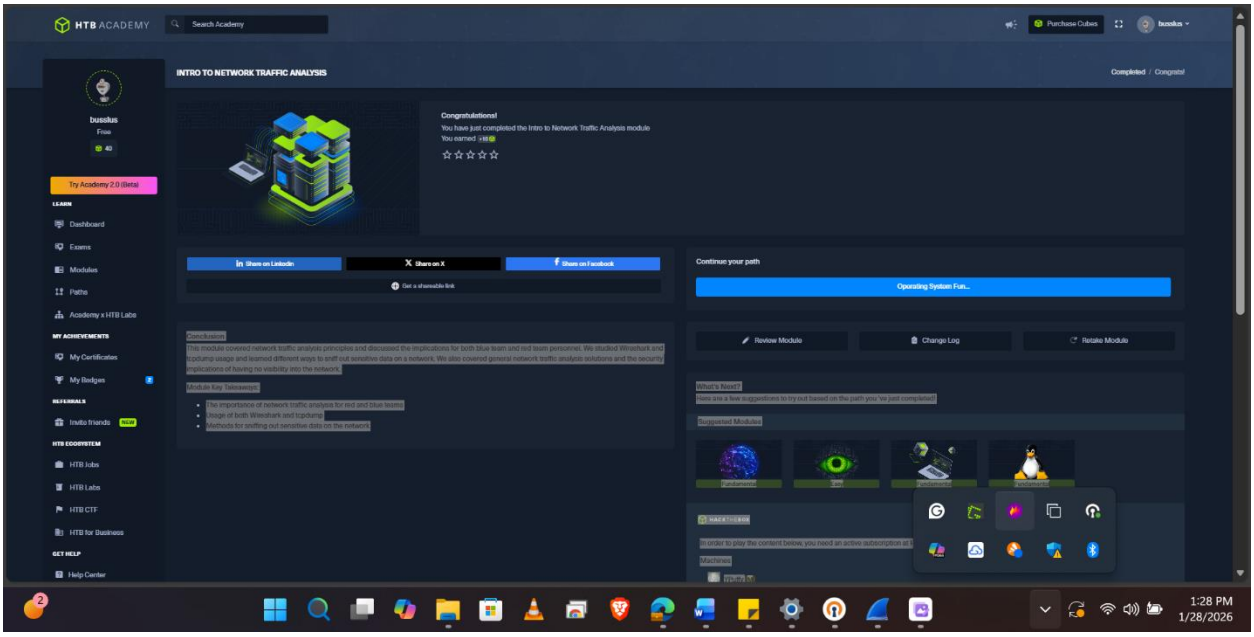
Shareable Link

The following unique link, generated by Hack The Box Academy, provides official validation of the module's completion

https://academy.hackthebox.com/achievement/badge/e6213437-fc33-11f0-9254-bea50ffe6cb4

Completion Screenshot

The screenshot below serves as the official confirmation that all sections and challenges within the module have been completed successfully.



Conclusion & Reflection

This final section serves as a strategic reflection on the learning experience provided by the "Intro to Network Traffic Analysis" module. It synthesizes the key takeaways and evaluates the practical value of the skills acquired, framing them within the context of real-world cybersecurity operations.

The module provided a comprehensive and practical education in network traffic analysis. The most critical skills and concepts gained include:

- **The OSI Model in Practice:** The module provided a tangible link between the OSI model and packet analysis. For instance, identifying the attacker's IP in question 2.1 was a Layer 3 (Network) task focused on IP headers, while extracting credentials in 2.3 was a Layer 7

(Application) task that required reassembling a TCP stream to read HTTP data. This practical application reinforces the model as a critical diagnostic framework.

- **Packet Header Analysis:** A significant portion of the learning involved dissecting the headers of various protocols (IP, TCP, UDP, HTTP). This skill is invaluable for understanding the context of a connection, identifying spoofed or malformed packets, and tracing the path of data across a network.
- **Effective Filtering in Wireshark:** Mastery of Wireshark's display filters is a force multiplier. The module provided hands-on practice moving from simple protocol filters (e.g., http) to complex, compound expressions (ip.addr == X.X.X.X && tcp.port == 80), which is essential for quickly isolating needles of evidence from a haystack of network data.
- **Command-Line Traffic Capture with tcpdump:** Learning tcpdump complements the graphical analysis of Wireshark. Its efficiency and scriptability make it indispensable for use on remote servers, in automated scripts, or in resource-constrained environments where a GUI is unavailable.

The skills acquired in this module are directly applicable to numerous real-world cybersecurity scenarios. For example, if a SOC alert flags a potential data exfiltration event, the tcpdump skills learned here would allow for immediate, targeted traffic capture on the suspect server, even without a GUI, to validate the threat.

This module has solidified my understanding of network communications and provided a robust foundation in the tools of the trade.