

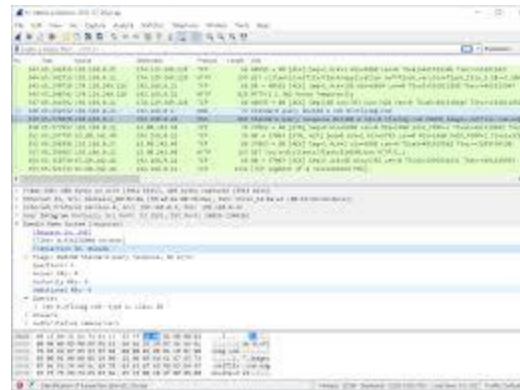
A photograph of a network switch in a server rack. A grey mouse is perched on top of the switch. The front panel of the switch shows several ports with green indicator lights. A large, messy pile of grey Ethernet cables is tangled in front of the switch. Some cables have labels like 'ALLEN TEL PRODUCTIONS' and 'VERIFIED TO FT4'. A blue cable and a yellow cable are also visible. The word 'wireshark' is overlaid in the center in a blue, flaming font.

wireshark

What is Wireshark?



Wireshark is a free, open-source network protocol analyser.



you capture and inspect network traffic in real time. Every single packet is captured



Think of it as a microscope for your network — zooming in on every packet!

WHY ?



- Learn how protocols work.
- Debug network applications.
- Follow streams like conversations

- Troubleshoot network issues.
- Spot suspicious or malicious traffic
- Debugging apps



Guys we did it we found the intruder



- Finding slow networks.
- Detecting intrusions or malware traffic
- Analysing VoIP (record and play back phone calls or determine quality to fix)
- Learning networking

HOW DOES IT WORK



Decodes hundreds of protocols (TCP, HTTP, DNS, etc.). By capturing packets live, Display & capture filters.



1. Captures (sniffs) packets from network interfaces.
2. Decodes protocol layers.
3. Applies filters to narrow results.
4. Displays packet metadata + payload.
5. Allows analysis, exporting, and reporting

W AND L OF WIRESHARK

You get to see what devices are really saying behind the scenes.

Feels like hacking in a movie (but legal!).

You can follow streams like reading a conversation.

Spot weird traffic, misbehaving apps, or even memes being sent over HTTP.

Limitations:

- HTTPS sites are encrypted (SSL/TLS)
 - Can be unencrypted if you own the web server
 - Other protocols aren't – DNS packets show the websites people are accessing on the network you're connected to
- Requires admin permissions
- Can be overwhelming for beginners



Pros:

- Free, powerful, open-source
- Deep protocol support
- Great for learning

Wireshark Filters/Tips

Play around with filters — it's like magic!

Filter

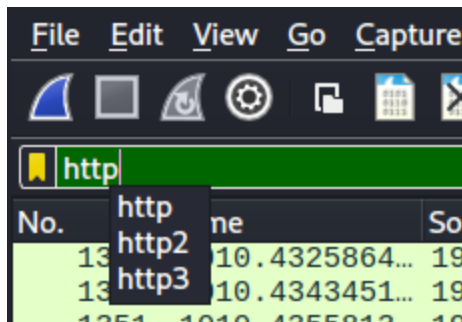
http

DNS

tcp.port == 80

ip.addr == 8.8.8.8

tcp.flags.syn == 1



- Use capture filters to reduce noise.
- Save large captures in segments.
- Use colour rules to highlight patterns.
- Learn display filters—they're powerful!
- Be mindful of sensitive captured data.

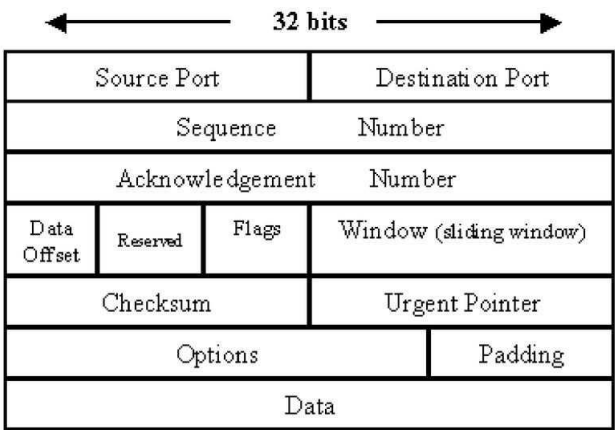


Interface

No.	Time	Source	Destination	Protocol	Length	Info
2731	8.625194349	2.19.252.91	192.168.60.1	TCP	1514	443 → 57369 [PSH, ACK]
2732	8.625194373	2.19.252.91	192.168.60.1	TCP	1514	443 → 57369 [PSH, ACK]

Column	Description
No.	The packet number in the capture sequence.
Time	The time elapsed since the start of the capture.
Source	The IP or MAC address from which the packet originated.
Destination	The IP or MAC address to which the packet is being sent.
Protocol	The protocol type, for example, TLS v1.2, TCP, ICMP, etc.
Length	The size of the packet in bytes.
Info	A summary of the packet's function or contents.

TCP Packet header



The image shows a Wireshark packet capture interface. The top pane displays a list of captured packets, including Ethernet II, Internet Protocol Version 4, and Transmission Control Protocol (TCP). The bottom pane shows the detailed view of a selected TCP packet (Frame 184). The packet details include: Source Port: 80, Destination Port: 34006, Sequence Number: 186, Acknowledgment Number: 89, and Window Length: 0. The packet is identified as a FIN, ACK segment. The raw hex data of the packet is displayed in the bottom pane, showing the hexadecimal representation of the packet bytes.

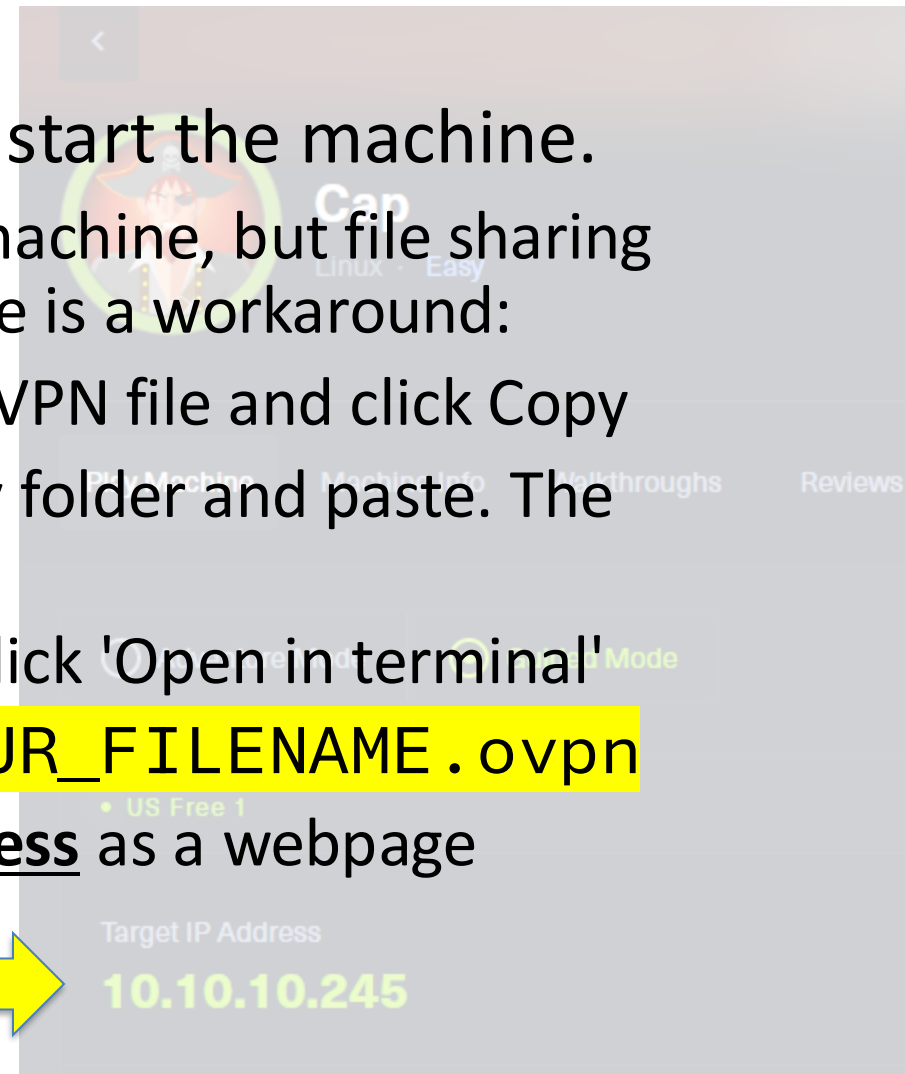
Header information/meta data of packet

ASCII (into letters) translation of the hex data

Raw hexadecimal contents of packet

Cap - HTB

- [Hack The Box :: Hack The Box](#)
- Download the OpenVPN file (top right) then start the machine.
 - You need to run the OpenVPN file on your Kali machine, but file sharing between VM and your desktop is restricted. Here is a workaround:
 - On your Windows machine, right click the OpenVPN file and click Copy
 - On the Kali VM, right click on the desktop or any folder and paste. The clipboard is shared between VM and host.
 - Right click the same folder/desktop again, and click 'Open in terminal'
 - In the terminal, enter `sudo openvpn . /YOUR_FILENAME.ovpn`
 - Open Firefox in Kali and open the target IP address as a webpage



Task Knowledge

- OSI Model – physical, data, network, transport, session, presentation, application
- TCP/IP - link, internet, transport, application
- Linux
- Ports
- Wireshark
- tcpdump and tshark