**Sri Lanka Institute of Information Technology**

Final Project Report

****

**Systems and Network Programming (SNP) \_\_ IE2012**

**2nd year 1st semester**

**Submitted by:**

|  |  |
| --- | --- |
| **Student ID** | **IT21169076** |
| **Student Name** | **Athukorala D.A.S.M** |

Contents

[Abstract 3](#_Toc121243158)

[Acknowledgement 4](#_Toc121243159)

[Declaration 5](#_Toc121243160)

[Introduction 6](#_Toc121243161)

[Solve traffic analysis | A Comprehensive Walkthrough 7](#_Toc121243162)

[Task 01 \_ Wireshark introduction 8](#_Toc121243163)

[Task 2 \_ wireshark tools 10](#_Toc121243164)

[capinfos 10](#_Toc121243165)

[Dumpcap 10](#_Toc121243166)

[editcap 10](#_Toc121243167)

[Task 3 – capturing packets 12](#_Toc121243168)

[What is Packet Capture? 12](#_Toc121243169)

[How to Read a Packet Capture 12](#_Toc121243170)

[Task 4 \_ operating systems with wireshark 14](#_Toc121243171)

[Microsoft Windows 14](#_Toc121243172)

[MacOS 15](#_Toc121243173)

[UNIX, LINUX and BSD 15](#_Toc121243174)

[TASK 5 \_ practice with basic linux command 17](#_Toc121243175)

[LINUX COMMAND 17](#_Toc121243176)

[TASK 6 \_ knowledge about block chain 19](#_Toc121243177)

[How fraudsters attack blockchain technology 19](#_Toc121243178)

[TASK 7 \_ network traffic analysis 20](#_Toc121243179)

[TASK 8 – virus Total 22](#_Toc121243180)

[*Free and unbiased* 22](#_Toc121243181)

[*Many contributors* 22](#_Toc121243182)

[*Raising the global IT security level through sharing* 22](#_Toc121243183)

[*Real-time updates* 23](#_Toc121243184)

[*Detailed results* 23](#_Toc121243185)

[TASK 9 – versions of pcap 25](#_Toc121243186)

[TASK 10 – advantage and disadvantages of packet capturing and pcap 27](#_Toc121243187)

[Advantage 27](#_Toc121243188)

[Disadvantages 27](#_Toc121243189)

[Challenges - 29](#_Toc121243190)

[Conclusion 30](#_Toc121243191)

[References 31](#_Toc121243192)

# Abstract

Wireshark is most often used. It offers a comprehensive traffic analysis and capture interface. GUIs simplify network forensics. This report is great for learning Wireshark packet analysis. Instant Wireshark Starter is perfect for network newbies. It starts with tools, packet capture, wireshark, etc. Wireshark is discussed in detail. Instant Wireshark Starter considers beginners. After simple setup, the report leads you through your first packet capture and crucial subjects including traffic analysis. Recorded packets, basic Linux commands, and network traffic analysis follow. The report finishes with blockchain knowledge. Learn from this report Wireshark. Datenpakete. Wireshark protocol representation. Display. Transfer capture files. Approach Get comfortable with a new technology, discover what it can achieve, and then focus on the most crucial features and tasks. Wireshark Starter teaches network traffic collection and analysis. It's beneficial for network administrators, forensic experts, and penetration testers who understand network protocols and implementation.

# Acknowledgement

I would like to express our gratitude towards Dr. Lakmal Perera, eshandi aththanayaka for their kind co-operation and encouragement which helped us in successfully completion of this project.

# Declaration

I declare that this project report or part of it was not a copy of a document done by any organization, university any other institute or a previous student project group at SLIIT and was not copied from the Internet or other sources.

**Project details:**

|  |  |
| --- | --- |
| Project Title | Tryhackme |

**Member:**

|  |  |
| --- | --- |
| Student ID | IT21169076 |
| Student name | Athukorala D.A.S.M |

# Introduction

This project was completed in accordance with the Systems and Network Programming (SNP)-IE2012 for the first semester of the second year of the Cyber Security Specialization program. As its final assignment, Tryhackme. I did network protocol analyzer here. Wireshark was prioritized as a grant. Wireshark is a network packet analyzer. A network packet analyzer presents captured packet data in as much detail as possible. You could think of a network packet analyzer as a measuring device for examining what’s happening inside a network cable, just like an electrician uses a voltmeter for examining what’s happening inside an electric cable (but at a higher level, of course). In the past, such tools were either very expensive, proprietary, or both. However, with the advent of Wireshark, that has changed. Wireshark is available for free, is open source, and is one of the best packet analyzers available today.

Some intended purposes

Here are some reasons people use Wireshark:

• Network administrators use it to troubleshoot network problems

• Network security engineers use it to examine security problems

• QA engineers use it to verify network applications

• Developers use it to debug protocol implementations

• People use it to learn network protocol internals

Wireshark can also be helpful in many other situations

# Solve traffic analysis | A Comprehensive Walkthrough

This section contains a comprehensive walkthrough of the wireshark “solve traffic analysis ” on the scenario. The complete workplace is based on a scenario. If it In a traffic analysis attack, a hacker tries to gain access to the same network as you to listen (and capture) all of your network traffic. From there, the hacker can analyze that traffic to learn something about you or your company. Imagine that you are trying to find out all the information through an attacker to know what has happened in the network... You have been given a pcap file to help you.... Get the information from that file. Terms and references are included in the relevant sections for the ease of the user. This will flow in the same order the challenges have been implemented in the Tryhackme platform. All the tasks are properly addressed with screenshots to guide the user.

## Task 01 \_ Wireshark introduction

The main goal is to give the user an understanding of Wireshark in the first task.

Wireshark is a network packet analyzer. A network packet analyzer displays collected packet data in as much detail as feasible.

A network packet analyzer may be thought of as a measuring instrument for analyzing what's going on within a network cable, like how an electrician uses a voltmeter to examine what's going on inside an electric wire (but at a higher level, of course).

In the past, such tools were either prohibitively expensive, proprietary, or both. That has altered after the introduction of Wireshark. Wireshark is a free and open-source packet analyzer that is widely used today. Wireshark is an open-source network protocol analysis application that is widely regarded as the industry standard. Wireshark is supported by a global team of network professionals and software engineers, and it is constantly updated to accommodate new network technology and encryption methods.

A picture containing text

Description automatically generated

Graphical user interface, application

Description automatically generated

Questions are there asking about basic knowledge about wireshark.

**Q1**  - what is Wireshark?

**Answer**  - network packet analyzer

**Q2** - is it possible to start Wireshark from command line on windows

**Answer**  - yes

**Q3** - What kind of shark is Wireshark?

**Answer** - carcharodon photoshopia

## Task 2 \_ wireshark tools

The main goal is to give the user an understanding of Wireshark tools in the second task.

Wireshark comes with a few command-line utilities. These tools come in handy when working with capture files.

### capinfos

capinfos is a software that reads one or more capture files and provides some or all available statistics (infos) for each infile > in either long or table format .

The lengthy output is adequate for human reading. The table output may be used to create a report that can then be simply imported into a spreadsheet or database.

By supplying flags (options) that correspond to the report type and required information, the user decides what type of output (long or table) and which statistics to display. capinfos will report all statistics available in "long" format. Later options supersede or add to previous options as they are processed from left to right

### Dumpcap

It lets you capture packet data from a live network and write the packets to a file. dumpcap's default capture file format is pcapng. When the **-P** option is specified, the output file is written in the pcapformat.

Without any options set, it will use the libpcap, Npcap, or WinPcap libraries to capture traffic from the first available network interface and write the received raw packet data, along with the packets' time stamps, into a pcap file.

If the **-**w option is not specified, Dumpcap writes to a newly created pcap file with a randomly chosen name. If the **-w**option is specified, Dumpcap writes to the file specified by that option.

Packet capturing is performed with the pcap library. The capture filter syntax follows the rules of the pcap library.

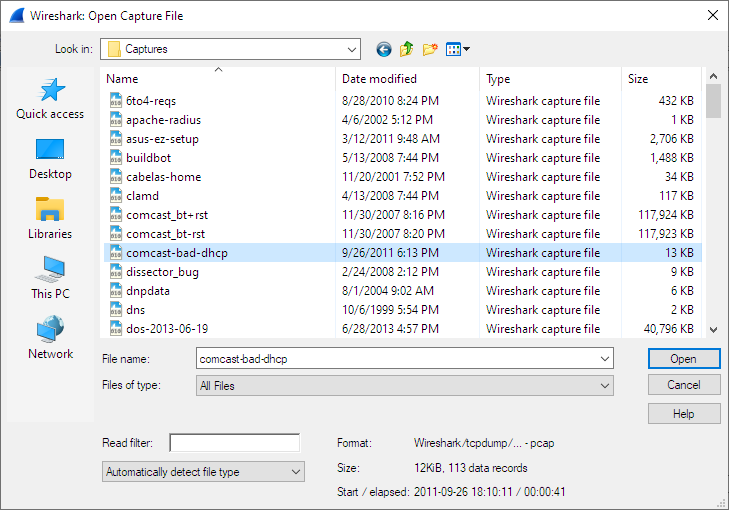
### editcap

editcap is a program that reads some or all of the captured packets from the infile, optionally converts them in various ways, and writes the resulting packets to the capture outfile (or outfiles).

By default, it reads all packets from the infile and writes them to the outfile in pcapng file format. Use "-" for infile or outfile to read from standard input or write to standard output, respectively.

The -A and -B options allow you to limit the time range in which packets are read from the infile.

An optional list of packet numbers can be specified on the command tail; individual packet numbers separated by whitespace and/or ranges of packet numbers can be specified as start-end, referring to all packets from start to end. By default, the selected packets with those numbers will not be written to the capture file. If the **-**r flag is specified, the whole packet selection is reversed; in that case, only the selected packets will be written to the capture file.



A questions are there asking about basic knowledge about wireshark.

**Q2** - what protocol does wireshark use?

**Answer** - pcap

## Task 3 – capturing packets

The main goal is to give the user an understanding of packet capture in the third task.

### What is Packet Capture?

The action of collecting Internet Protocol (IP) packets for examination or analysis is referred to as "packet capture." The phrase can also refer to the files produced by packet capture programs, which are commonly saved in the. pcap format. Capturing packets is a typical network administrator's troubleshooting tool that is also used to analyze network traffic for security issues. Following a data breach or other incident, packet captures give critical forensic information that aids investigations. From the standpoint of a threat actor, packet captures might be exploited to steal passwords and other sensitive data. Capturing packets, unlike active spying techniques such as port scanning, may be conducted without leaving any trail for investigators.

***Why do I only see packets to and from my machine when I use Wireshark to capture them? Or do I not see all of the traffic I expect to observe from or to the system I'm attempting to monitor?***

**How do I answer this question?**

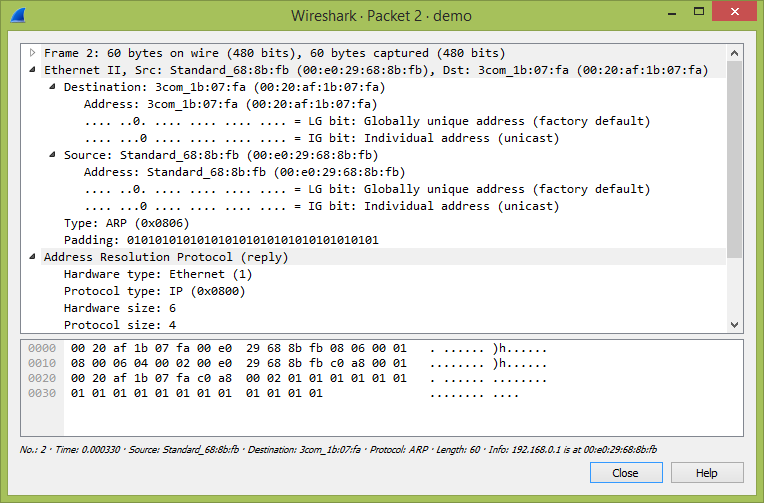
This might be because the interface is connected to an Ethernet or Token Ring switch; on a switched network, unicast communication between two ports does not always show up on other ports; only broadcast and multicast data is routed to all ports.

Even if you put your machine into a hub, the "hub" might be a switched hub, in which case you're still on a switched network.

It's also worth noting that Linksys' auto-sensing hubs "broadcast the 10Mb packets to the ports that operate at 10Mb only and broadcast the 100Mb packets to the ports that operate at 100Mb only," implying that if you sniff on a 10Mb port, you won't observe data delivered to a 100Mb port, and vice versa. This issue has also been noticed with Netgear dual-speed hubs, and it is possible that it exists with other "auto-sensing" or "dual-speed" hubs.

### How to Read a Packet Capture

To comprehend and analyze a packet capture, you must first grasp basic networking principles, particularly the OSI model. While individual techniques may differ, packet captures will always consist of a payload and certain headers. The payload is the actual data being carried; this may be parts of a streaming movie, e-mails, malware, or anything else moving over a network. Packet headers provide all of the important information that network equipment uses to determine what to do with each packet. The source and destination addresses are the most significant, but IP packets include 14 headers that cover everything from Class of Service to Protocol Type.



**Q2** - Which is used for packet capture?

**Answer** - Libpcap

**Q4 -** what is the main Couse of packet loss?

**Answer** - network congestion

**Q7** - what is capture and examples?

**Answer** - capture verb [T] (CATCH)

## Task 4 \_ operating systems with wireshark

### Microsoft Windows

Wireshark should support any version of Windows that is still within its extended support lifetime. At the time of writing this includes Windows 10, 8.1, Server 2019, Server 2016, Server 2012 R2, and Server 2012. It also requires the following:

* The Universal C Runtime. This is included with Windows 10 and Windows Server 2019 and is installed automatically on earlier versions if Microsoft Windows Update is enabled. Otherwise You must install KB2999226 or KB3118401.

       •  Any modern 64-bit AMD64/x86-64 or 32-bit x86 processor.

      •  500 MB available RAM. Larger capture files require more RAM.

       •  500 MB available disk space. Capture files require additional disk space.

       •  Any modern display. 1280 × 1024 or higher resolution is recommended.

       •A supported network card for capturing

◦ Ethernet. Any card supported by  Windows  should work. See the wiki pages on Ethernet capture and offloading for issues that  may affect your environment.

◦ 802.11. See the Wireshark wiki page. Capturing raw  802.11 information may be difficult without special equipment.

Older versions of Windows which are outside Microsoft’s extended lifecycle support window are no longer supported. It is often difficult or impossible to support these systems due to circumstances beyond our control, such as third party libraries on which we depend or due to necessary features that are only present in newer versions of Windows such as hardened security or memory management.

• Wireshark 3.6 was the last release branch to officially support 32-bit Windows.

• Wireshark 3.2 was the last release branch to officially support Windows 7 and Windows Server 2008 R2.

• Wireshark 2.2 was the last release branch to support Windows Vista and Windows Server 2008 sans R2

• Wireshark 1.12 was the last release branch to support Windows Server 2003.

• Wireshark 1.10 was the last release branch to officially support Windows XP.

### MacOS

Wireshark supports macOS 10.14 and later. Like Windows, supported macOS versions depend on third party libraries and on Apple’s requirements. Apple Silicon hardware is supported natively starting with version 4.0

• Wireshark 3.6 was the last release branch to support macOS 10.13.

• Wireshark 3.4 was the last release branch to support macOS 10.12.

• Wireshark 2.6 was the last release branch to support Mac OS X 10.6 and 10.7 and OS X 10.8 to 10.11. • Wireshark 2.0 was the last release branch to support OS X on 32-bit Intel.

• Wireshark 1.8 was the last release branch to support Mac OS X on PowerPC.

The system requirements should be comparable to the specifications listed above for Windows.

### UNIX, LINUX and BSD

Wireshark runs on most UNIX and UNIX-like platforms including Linux and most BSD variants. The system requirements should be comparable to the specifications listed above for Windows.

Binary packages are available for most Unices and Linux distributions including the following platforms:

• Alpine Linux

• Arch Linux

• Canonical Ubuntu

• Debian GNU/Linux

• FreeBSD

• Gentoo Linux

• HP-UX

• NetBSD

• OpenPKG

• Oracle Solaris

• Red Hat Enterprise Linux / CentOS / Fedora

**Q1** - Does Windows have Wireshark?

**Answer** - yes

**Q2** - can wireshark run on Android?

**Answer** - no

**Q3** - can you run wireshark without installing ?

**Answer**  – yes

**Q6** - is wireshark available for mac m1?

**Answer** – yes

**Q9** - which linux is used for networking?

**Answer** – tcpdump

## TASK 5 \_ practice with basic linux command

This section contains a comprehensive walkthrough of the wireshark “solve traffic analysis ” on the scenario. The complete workplace is based on a scenario. If it In a traffic analysis attack, a hacker tries to gain access to the same network as you to listen (and capture) all of your network traffic. From there, the hacker can analyze that traffic to learn something about you or your company. Imagine that you are trying to find out all the information through an attacker to know what has happened in the network... You have been given a pcap file to help you.... Get the information from that file.

First, before you hire an attacker, check if the first attacker has some Linux command knowledge. Should have some knowledge about Linux, Kali

Linux is an operating system's kernel. You might have heard of UNIX. Well, Linux is a UNIX clone. But it was created by Linus Torvalds from Scratch. Linux is free and open source, that means that you can simply change anything in Linux and redistribute it in your own name! There are several Linux Distributions, commonly called â€œdistrosâ€.

* Ubuntu Linux
* Red Hat Enterprise Linux
* Linux Mint
* Debian
* Fedora

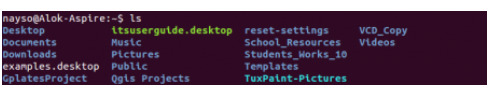
Linux is Mainly used in servers. About 90% of the internet is powered by Linux servers. This is because Linux is fast, secure, and free! The main problem of using Windows servers are their cost. This is solved by using Linux servers. The OS that runs in about 80% of the smartphones in the world, Android, is also made from the Linux kernel. Most of the viruses in the world run on Windows, but not on Linux

### LINUX COMMAND

1**. pwd** â€” When you first open the terminal, you are  in the home directory of your user. To know which directory you are in, you can use the â€œpwdâ€ command. It gives us the **absolute path,** which means the path that starts from the root. The root is the base of the Linux file system. It is denoted by a forward slash( / ). The user directory is usually something like "/home/username".



2**. ls** â€” Use the "ls" command to know what files are in the directory you are in. You can see all the hidden files by using the command â€œls -aâ€.

****

3 **.cd** â€” Use the "cd" command to go to a directory. For example, if you are in the home folder, and you want to go to the downloads folder, then you can type in â€œcd Downloadsâ€. Remember, this command is case sensitive, and you have to type in the name of the folder exactly as it is. But there is a problem with these commands. Imagineyou have a folder named â€œRaspberry Piâ€. In this case, when you type in â€œcd Raspberry Piâ€, the shell will take the second argument of the command as a different one, so you will get an error saying that the directory does not exist. Here, you can use a backward slash. That is, you can use â€œcd Raspberry\ Piâ€ in this case. Spaces are denoted like this: If you just type â€œcdâ€ and press enter, it takes you to the home directory. To go back from a folder to the folder before that, you can type â€œcd ..â€ . The two dots represent back.

****  
4. **mkdir & rmdir** â€” Use the mkdir command when you need to create a folder or a directory. For example, if you want to make a directory called â€œDIYâ€, then you can type â€œmkdir DIYâ€. Remember, as told before, if you want to create a directory named â€œDIY Hackingâ€, then you can type â€œmkdir DIY\ Hackingâ€. Use rmdir to delete a directory. But rmdir can only be used to delete an empty directory. To delete a directory containing files, use rm.

**Q1** - what is linux?

**Answer**  - Unix-based open-source operating system

**Q2** - define linux kernel?

**Answer**  - low-level software system

**Q5**  - which is file permission in linux?

**Answer** - read , write , execute

## TASK 6 \_ knowledge about block chain

Other than before you hire an attacker, check if the attacker has some blockchain security knowledge. Should have some knowledge about cryptography, blockchain …

Blockchain security is a comprehensive risk management system for a blockchain network, using cybersecurity frameworks, assurance services and best practices to reduce risks against attacks and fraud.

[Blockchain technology](https://www.ibm.com/topics/what-is-blockchain) produces a structure of data with inherent security qualities. It's based on principles of cryptography, decentralization, and consensus, which ensure trust in transactions. In most blockchains or distributed ledger technologies (DLT), the data is structured into blocks and each block contains a transaction or bundle of transactions. Each new block connects to all the blocks before it in a cryptographic chain in such a way that it's nearly impossible to tamper with. All transactions within the blocks are validated and agreed upon by a consensus mechanism, ensuring that each transaction is true and correct.

Blockchain technology enables decentralization through the participation of members across a distributed network. There is no single point of failure, and a single user cannot change the record of transactions. However, blockchain technologies differ in some critical security aspects.

### How fraudsters attack blockchain technology

#### Phishing attacks

Phishing is a scamming attempt to attain a user's credentials. Fraudsters send wallet key owners emails designed to look as though they're coming from a legitimate source. The emails ask users for their credentials using fake hyperlinks. Having access to a user's credentials and other sensitive information can result in losses for the user and the blockchain network.

#### Sybil attacks

In a Sybil attack, hackers create and use many false network identities to flood the network and crash the system. *Sybil*refers to a famous book character diagnosed with a multiple identity disorder.

#### 

#### **Routing attacks**

Blockchains rely on real-time, large data transfers. Hackers can intercept data as it's transferring to internet service providers. In a routing attack, blockchain participants typically can't see the threat, so everything looks normal. However, behind the scenes, fraudsters have extracted confidential data or currencies.

**Q1** - what are the different types of blockchain ?

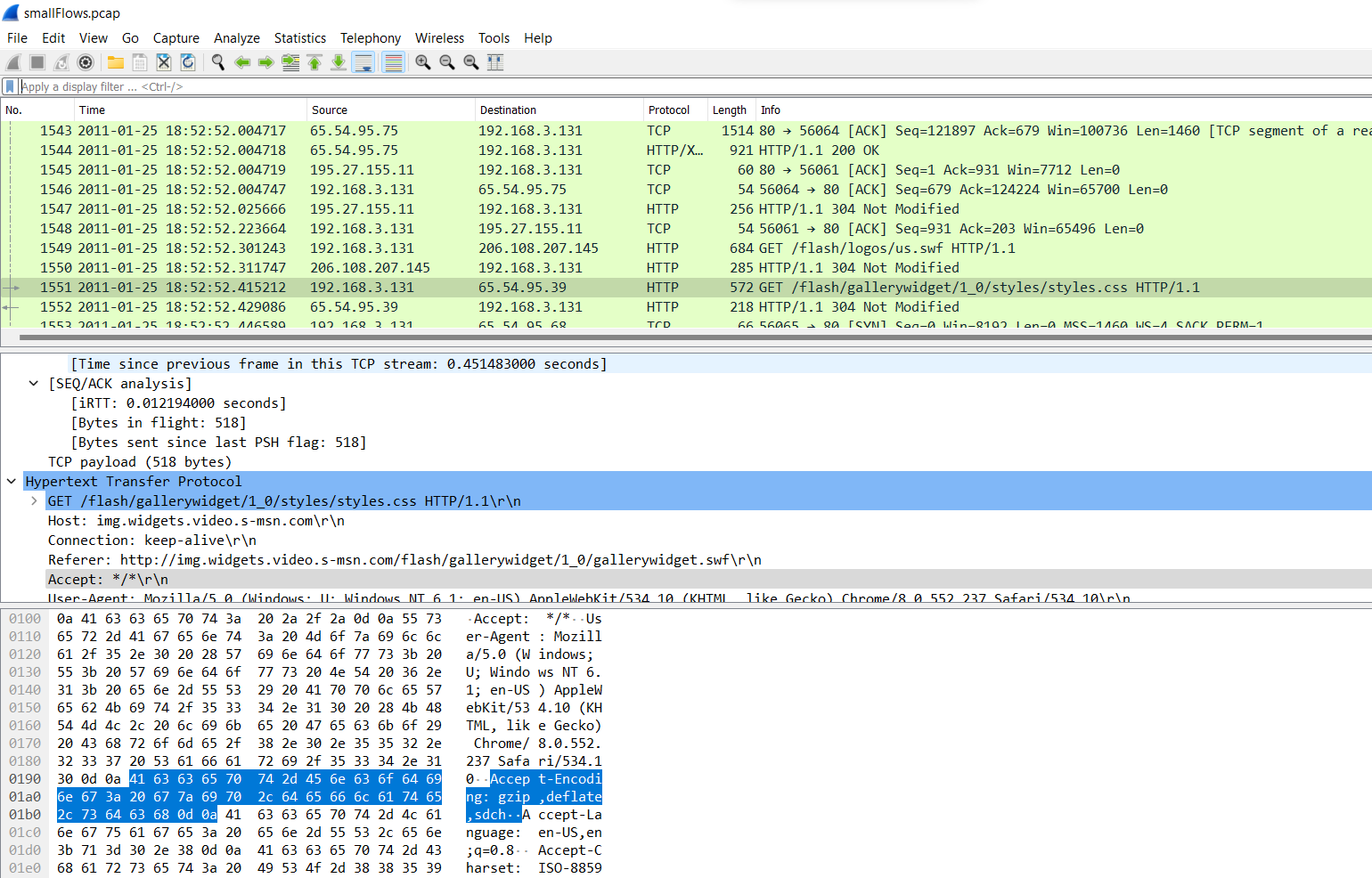
**Answer** - public , consortium, private

**Q4** - bitcoin is based on \_\_\_\_\_\_ blockchain?

**Answer** - public

## TASK 7 \_ network traffic analysis

Here, first download the pcap file and open it with wireshark



**Q1** – what is the date and time of this activity ?

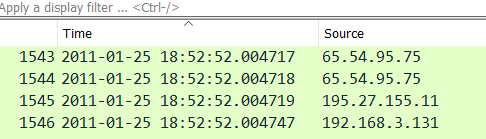
**Answer**  - 2011-01-25 /18:52:22

Graphical user interface, text, application, chat or text message

Description automatically generated

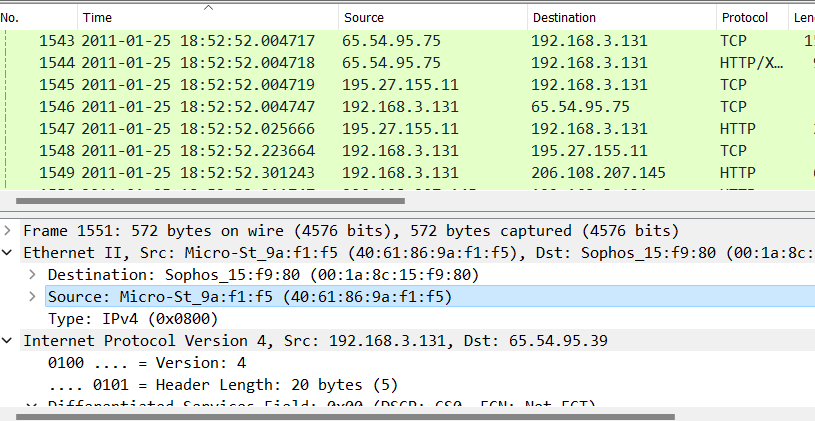
**Q2**  - What is the IP address of the Windows host that gets infected?

**Answer** - 192.168.3.131



**Q 3** -  What is the MAC address of the infected Windows host?

**Answer** - (40:61:86:9a:f1:f5)

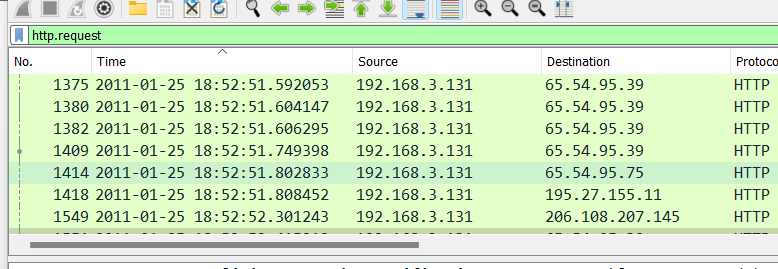


**Q4**  - **What is the host name of the infected Windows host?**

**Answer - student01-PC**

**Q5**  -What is the IP address of the compromised web site?

**Answer** -65.54.95.39



## TASK 8 – virus Total

Analyze the virus – related information in the pcap file by following the given link .

**Download -**<https://www.virustotal.com/gui/home/search>

VirusTotal inspects items with over 70 antivirus scanners and URL/domain blocklisting services, in addition to a myriad of tools to extract signals from the studied content. Any user can select a file from their computer using their browser and send it to VirusTotal. VirusTotal offers several file submission methods, including the primary public web interface, desktop uploaders, browser extensions, and a programmatic API. The web interface has the highest scanning priority among the publicly available submission methods. Submissions may be scripted in any programming language using the HTTP-based public API.

As with files, URLs can be submitted via several different means, including the VirusTotal webpage, browser extensions, and the API.

Upon submitting a file or URL, basic results are shared with the submitter and also between the examining partners, who use the results to improve their own systems. As a result, by submitting files, URLs, domains, etc. to VirusTotal, you are contributing to raising the global IT security level.

This core analysis is also the basis for several other features, including the VirusTotal Community: a network that allows users to comment on files and URLs and share notes with each other. VirusTotal can be useful in detecting malicious content and also in identifying false positives -- normal and harmless items detected as malicious by one or more scanners.

### *Free and unbiased*

VirusTotal is free. Though we work with engines belonging to many different organizations, VirusTotal does not distribute or promote any of those third-party engines. We simply act as an aggregator of information. This allows us to offer an objective and unbiased service to our users.

### *Many contributors*

VirusTotal's aggregated data is the output of many different antivirus engines, website scanners, file and URL analysis tools, and user contributions. The file and URL characterization tools we aggregate cover a wide range of purposes: heuristic engines, known-bad signatures, metadata extraction, identification of malicious signals, etc.

### *Raising the global IT security level through sharing*

Scanning reports produced by VirusTotal are shared with the public VirusTotal community. Users can contribute comments and vote on whether particular content is harmful. In this way, users help to deepen the community’s collective understanding of potentially harmful content and identify false positives (i.e., harmless items detected as malicious by one or more scanners).

The contents of submitted files or pages may also be shared with premium VirusTotal customers. The file corpus created in VirusTotal provides cybersecurity professionals and security product developers valuable insights into the behaviors of emerging cyber threats and malware. Through our premium service commercial offering, VirusTotal provides qualified customers and anti-virus partners with tools to perform complex criteria-based searches to identify and access harmful file samples for further study. This helps organizations discover and analyze new threats and fashion new mitigations and defenses.

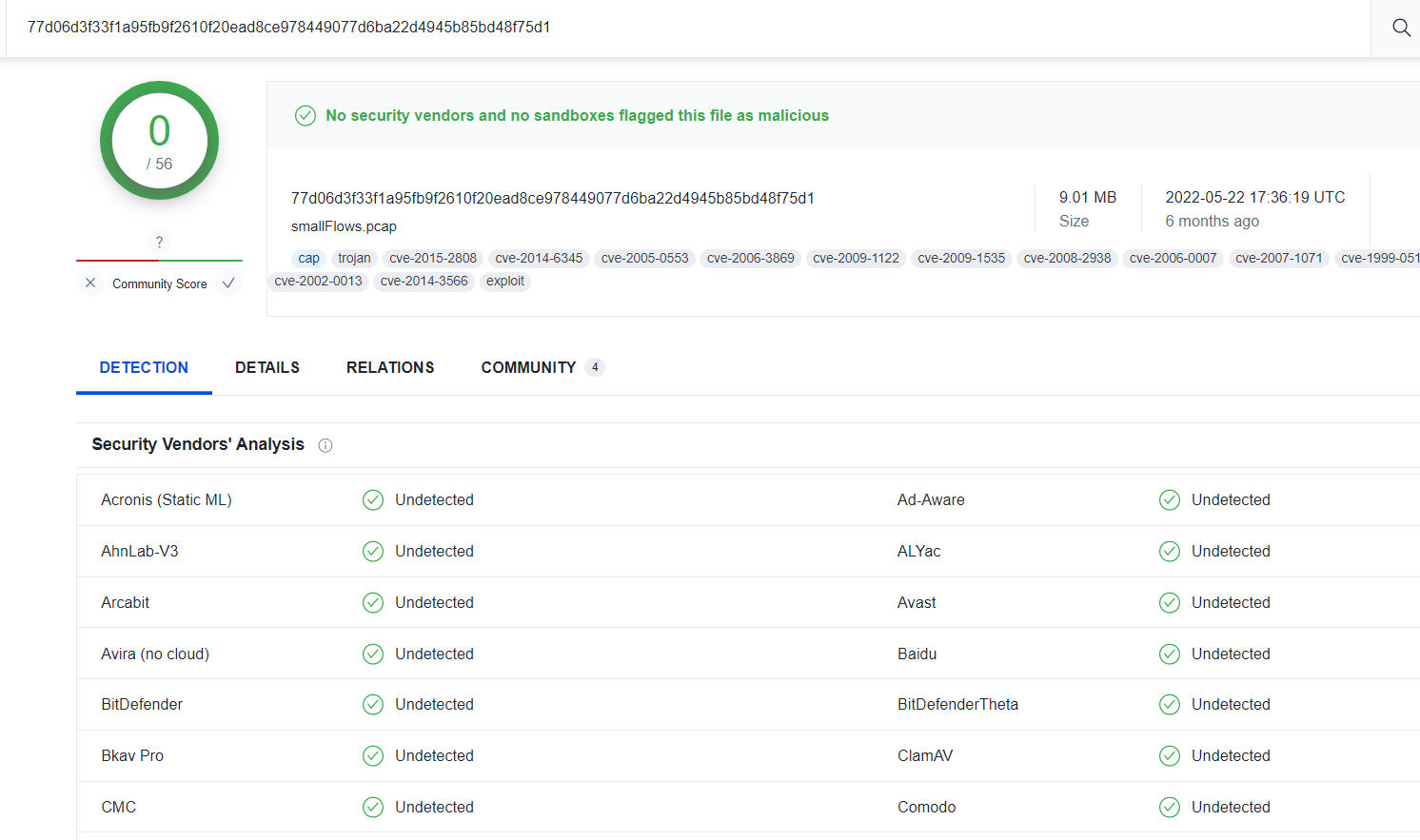
### *Real-time updates*

Malware signatures are updated frequently by VirusTotal as they are distributed by antivirus companies, this ensures that our service uses the latest signature sets.

Website scanning is done in some cases by querying vendor databases that have been shared with VirusTotal and stored on our premises, and in other cases by API queries to an antivirus company's solution. As such, as soon as a given contributor blocks a URL, it is immediately reflected in user-facing verdicts.

### *Detailed results*

VirusTotal not only tells you whether a given antivirus solution detected a submitted file as malicious, but also displays each engine's detection label (e.g., I-Worm.Allaple.gen). The same is true for URL scanners, most of which will discriminate between malware sites, phishing sites, suspicious sites, etc. Some engines will provide additional information, stating explicitly whether a given URL belongs to a particular botnet, which brand is targeted by a given phishing site, and so on.



**Q2** - is virus Total free

**Answer** - yes

**Q3** -are there viruses detected in the pcap file?

**Answer** - No

**Q4** - How many data sizes are there?

**Answer** - 9216531 bytes

**Q5**  -what is a file type

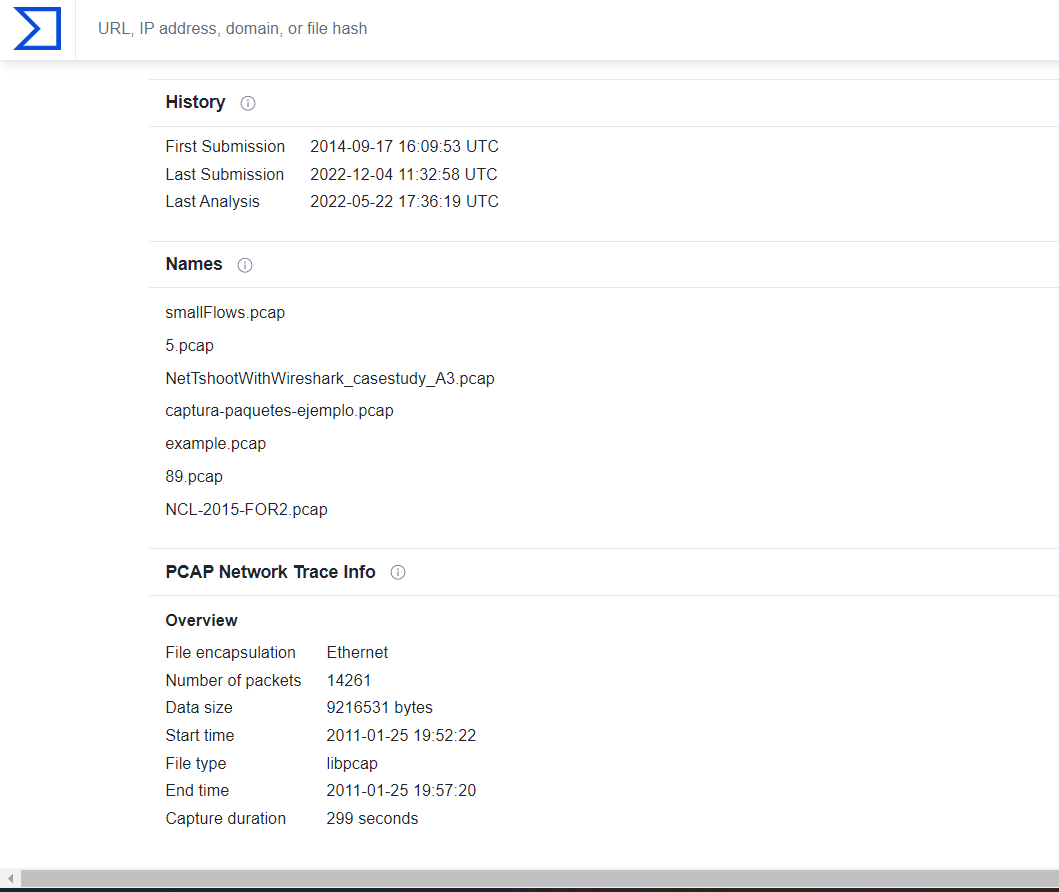
**Answer** - libpcap

**Q6** -when is the end date and time here

**Answer** - 2011-01-25 19:57:20

**Q7** - capture duration

**Answer**  - 299 seconds

****

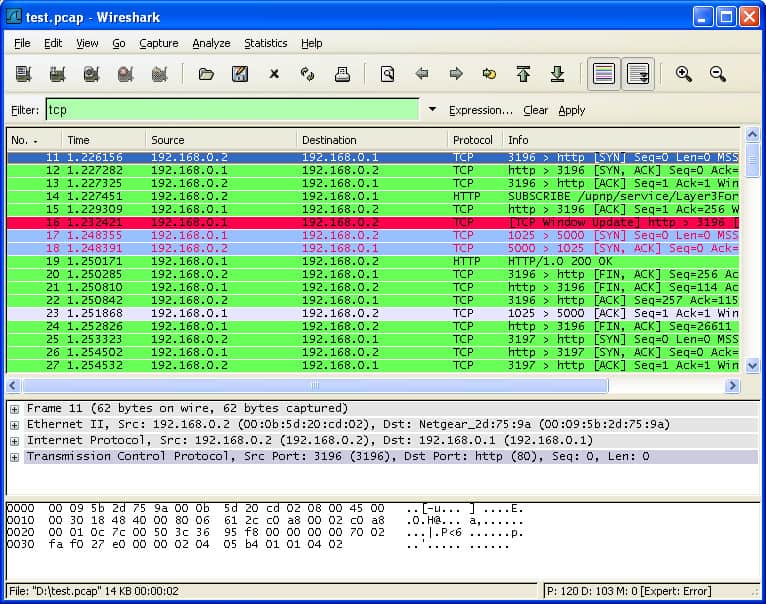
## TASK 9 – versions of pcap

As mentioned above, there are many different types of PCAP files, including:

* Libpcap
* WinPcap
* PCAPng
* Npcap

Each version has its own use cases, and different types of network monitoring tools support different forms of PCAP files. For instance, Libpcap is a portable open-source C/C++ library designed for Linux and Mac OS users. Libpcap enables administrators to capture and filter packets. Packet sniffing tools like tcpdump use the Libpcap format.

For Windows users, there is the WinPcap format. WinPcap is another portable packet capture library designed for Windows devices. WinpCap can also capture and filter packets collected from the network. Tools like **Wireshark**, **Nmap**, and **Snort** use WinPCap to monitor devices, but the protocol itself has been discontinued.



Q1 - What exactly is the PCAP format?

Answer – no need

Q2 – how do i check my pcap

Answer – no need

Q3 – What is PCAP replay?

Answer – no need

Q4- what is pcap over Ip

Answer – no need

Q5 – how do I generate pcap?

Answer – no need

Q6 – can we edit pcap file

Answer –yes

Q7 – can wireshark grab Ip

Answer - no need

## TASK 10 – advantage and disadvantages of packet capturing and pcap

### Advantage

The biggest advantage of packet capture is that it grants visibility. You can use packet data to pinpoint the root cause of network problems. You can monitor traffic sources and identify the usage data of applications and devices. PCAP data gives you the real-time information you need to find and resolve performance issues to keep the network functioning after a security event.

For example, you can identify where a piece of malware breached the network by tracking the flow of malicious traffic and other malicious communications. Without PCAP and a packet capture tool, it would be more difficult to track packets and manage security risks.

As a simple file format, PCAP has the advantage of being compatible with almost any packet sniffing program you can think of, with a range of versions for Windows, Linux, and Mac OS. Packet capture can be deployed in almost any environment.

### Disadvantages

Although packet capture is a valuable monitoring technique, it does have its limitations. Packet analysis allows you to monitor network traffic but doesn’t monitor everything. Many cyberattacks aren’t launched through network traffic, so you need to have other security measures in place.

For example, some attackers use USBs and other hardware-based attacks. Consequently, PCAP file analysis should be part of your network security strategy, but it shouldn’t be your only line of defense.

Another significant obstacle to packet capture is encryption. Many cyber attackers use encrypted communications to launch attacks on networks. Encryption stops your packet sniffer from being able to access traffic data and identify attacks. That means encrypted attacks will slip under the radar if you’re relying on PCAP.

There is also an issue with where the packet sniffer is located. If a packet sniffer is placed at the edge of the network, this will limit the amount of visibility a user has. For example, the user may fail to spot the start of a DDoS attack or malware outbreak. Furthermore, even if you are collecting data in the center of the network, it is important to make sure that you are collecting entire conversations rather than summary data.

**Graphical user interface, application

Description automatically generated**

**Q1 –** what are the 3 benefit of wireshark

**Answer** – no need

**Q2 –** what are the dangers of packet sniffing ?

**Answer – intercept** and log many of the packets that travel over a network.

**Q3 –** which of the following is the main drawback in wireshark?

**Answer –** no need

**Q4 –** can wireshark exploit vulnerability?

**Answer –** no need

## Challenges -

-Finding the necessary tools was very hard

-Environment was unfamiliar

- I implemented a box.but it doesn't affect my project. The reason is because there is no gui interface in the Ubuntu version

-When finding a topic I didn’t know how to manage the topic

-Finding myself in a place where I couldn’t export the OBA

-Finding my way through try hack me was hard

## Conclusion

Analyzing a packet capture file PCAP is a matter of thinking about the problem logically, reasoning what information you are looking for, and then constructing search filters to suit your requirements. Our Telnet example was very basic as it did not require any conversions or decryption, but again, the same principles would apply.

There is a lot that can be done with Wireshark, and it’s a tool that you should at least be familiar with installing and running, even if you are not using it every day. It can help with an investigation into a fault and is a brilliant starting point: the PCAP results that you get on your network can tell you a lot about what is happening around you, especially if you have reasons to be suspicious about any strange activity. Understand protocol representation in Wireshark alongside statistical analysis. Implement display. Import and export capture files. Approach Get to grips with a new technology, understand what it is and what it can do for you, and then get to work with the most important features and tasks. Wireshark Starter will show you all you need to know to effectively capture and analyze network traffic. It requires a basic understanding of network protocols and their implementation and is equally handy for network administrators, forensic experts, and network penetration testers

## References

[1] TryHackMe. (n.d.). *TryHackMe | Wireshark*. <https://tryhackme.com/module/wireshark>

[2] *What Is Packet Capture (PCAP)? - IT Glossary | SolarWinds*. (n.d.). <https://www.solarwinds.com/resources/it-glossary/pcap>

[3] *virustotal*. (n.d.). <https://www.virustotal.com/gui/home/search>

[4] Wikipedia contributors. (2022, October 7). *Wireshark*. Wikipedia. <https://en.wikipedia.org/wiki/Wireshark>

[5] *tryhackme • r/tryhackme*. (2019, March 20). Reddit. <https://www.reddit.com/r/tryhackme/>

[6] Kinzie, K. (2022, August 19). *How to Use Wireshark: Comprehensive Tutorial + Tips*. <https://www.varonis.com/blog/how-to-use-wireshark>