javonnie rutherford

Lab 03: Network Sniffing

Contents

[Introduction 2](#_Toc160977849)

[Network Traffic Analysis with Wireshark 2](#_Toc160977850)

[Applying Display Features 2](#_Toc160977851)

[Use Wireshark to Catalog Protocols 2](#_Toc160977852)

[Follow a TCP Stream 6](#_Toc160977853)

[Protocol Hierarchy Statistics 6](#_Toc160977854)

[Conversation Statistics 7](#_Toc160977855)

[Endpoint Statistics 9](#_Toc160977856)

[IO Graphs Statistics 10](#_Toc160977857)

[Flow Graph Statistics 11](#_Toc160977858)

[Overview and Wireshark’s role in Cybersecurity 12](#_Toc160977859)

[Network Traffic Analysis with Network Miner 13](#_Toc160977860)

[Host and Endpoint Analysis 13](#_Toc160977861)

[File Reconstruction 14](#_Toc160977862)

[Session Analysis 15](#_Toc160977863)

[Credential and Authentication Data 16](#_Toc160977864)

[DNS and Domain Analysis 17](#_Toc160977865)

[Overview and Network Miner’s role in Cybersecurity 17](#_Toc160977866)

[Overview of Wireshark and Network Miner 17](#_Toc160977867)

[Conclusion 18](#_Toc160977868)

[Bibliography 18](#_Toc160977869)

# Introduction

This lab’s goals are to give me a chance to analyze network traffic and get the chance to use both Wireshark and NetworkMiner. Both tools play a crucial role in network traffic analysis and network forensics. It will also give me a chance to analyze frequent protocols and their processes.

# Network Traffic Analysis with Wireshark

* In this section, I will be analyzing the PCAPs using Wireshark and built in tools. Let’s begin!

## Applying Display Features

The first step was me applying filters just to become familiar with it.

A screenshot of a computer

Description automatically generated

## Use Wireshark to Catalog Protocols

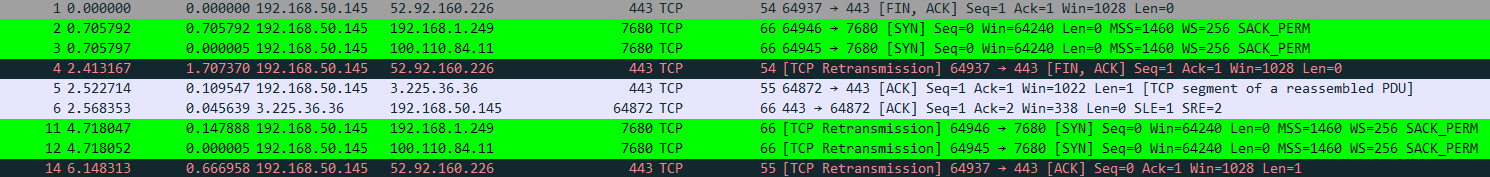
For this step, I will be filtering the different PCAPs for the listed protocols below. I’ll also be giving a summary of each.

* ARP
  + ARP stands for Address Resolution Protocol. Its primary purpose is mapping MAC addresses to IP addresses. Currently, there aren’t any well-known alternatives to ARP. A few alternatives include Inverse ARP, which maps the IP to a MAC address, and Network Discovery Protocol, which utilizes ARP on IPv6 networks. Overall, it’s arguable whether these protocols are better. The ARP protocol operates on port number 3389 and is present in my ShortPCAP and LongPCAP. I believe it is present in those PCAPs because the ARP table is constantly updating, so it sends occasional ARP requests. As for my comfortability with this service, I believe it’s fine if it operates on my network, as it is a necessary service.

A screenshot of a computer

Description automatically generated

* TCP
  + TCP stands for Transmission Control Protocol. Its purpose is to guarantee data transmission by first establishing a secure connection, and then sending data. I believe it is safe, due to it requiring a connection first. Currently, the only alternative is UDP, which is better in certain situations. For example, if you’re streaming a video and don’t care about packet loss, UDP is perfect. However, if you’re sending a message and need to make sure the entirety of the message is received, TCP is much better. As for port TCP uses, TCP can technically use any and every port. TCP handles the transmission to and from that port, so it doesn’t necessarily have a single port it hands all its technology through. TCP was found in my PCAP, and you’ll notice the wide variety of ports used. Additionally, I believe it is found in my PCAP because of its critical role in packet transfer. I feel comfortable with TCP being present on my machine due to its nature of simply transferring packets. “Don’t shoot the messenger”.

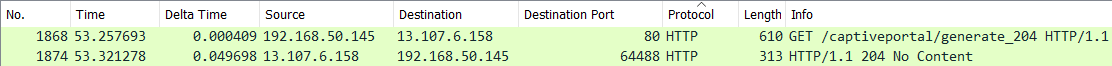


* UDP
  + UDP stands for User Datagram Protocol. Its primary purpose is to transfer data without the need for a connection first. Compared to TCP, UDP is a lot less safe, since anyone can send a packet to you using the UDP protocol. As mentioned above, I believe TCP can be argued to be a better alternative, depending on what you are doing. Similar to TCP, UDP can also operate on any port due to it being a data transfer protocol. UDP was present on my PCAP, which I believe is due to me being on YouTube at the time. I also believe UDP is fine to be running on a network, but I could see companies blocking UDP, which in turn would prevent access to time-wasting services, such as YouTube and Netflix.

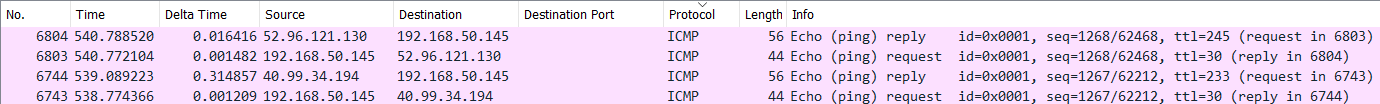
A screenshot of a computer

Description automatically generated

* HTTP
  + HTTP stands for HyperText Transfer Protocol, and its purpose is to fetch web resources. HTTP is the legacy version, and HTTPS is the newer, much more secure version. I do believe HTTPS is the much better alternative. HTTPS employs certificates to ensure security at the cost of processing times. HTTP operates on port 80 and was found in my PCAP. I believe it was found because I tried to contact the Ubuntu Web Server. Personally, I don’t like HTTP being used, due to its unsecure nature, but browsers do a good job of informing you the website is not secure, so that does help negate some of the risk.



* HTTPS
  + HTTPS stands for HyperText Transfer Protocol Secure, and its purpose is also to fetch web resources. HTTPS is the newer version of HTTP and employs security via digital certificates, which makes it much safer. At the present time, the only alternative is HTTP, which is a worser option in comparison. The port HTTPS uses is port 443. Unfortunately, I didn’t get a capture of HTTPS in use. However, in the TCP screenshot, you do see that the HTTPS port was being sent data. I believe HTTPS wasn’t captured since I wasn’t visiting any websites.
* FTP
  + FTP stands for File Transfer Protocol. FTP’s purpose is to transfer files from server to client. Unfortunately, FTP is not secure since it doesn’t implement any kind of encryption during transport (Barney, 2022). Therefore, a much more secure alternative is SFTP (Secure File Transfer Protocol). FTP operates on port 20 and was not present in my PCAP. I believe it wasn’t due to not being a part of a client-server relationship. As for comfortability with the protocol, I believe you should not have the port activated if you are not part of a business or client-server model. FTP is used very often for data exfiltration, which is one of the later stages of the MITRE ATT&CK Matrix (MITRE, n.d.).
* ICMP
  + ICMP stands for Internet Control Message Protocol and its purpose is to communicate problems that occurred during data transmission. I believe ICMP is safe, but there are cases where it can be abused, such as with the ICMP ping flooding attack, so it should be monitored. I don’t believe there are any alternatives since it’s more of a fundamental protocol. Similarly to TCP and UDP, ICMP does not use a singular port. ICMP was found on my PCAP, but I’m not sure why. To me, it looks like the machine was trying to map out a path for packet transmission. However, the obvious answer feels like a packet might have gotten lost. I believe ICMP is fine as long as you monitor it for possible flood attacks.

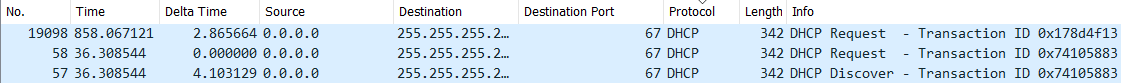


* DNS
  + DNS stands for Domain Name System and its purpose is to translate the host names we type into google, into IP addresses. As for DNS, it is not secure. DNS queries are transmitted over the internet in plaintext, meaning it can be manipulated (Cloudflare, n.d.). Again, there aren’t any alternative protocols to DNS, since it is a fundamental service, but there are different DNS server providers. Additionally, DNS operates on port 53 and was present in my PCAP. I believe it was present since I was visiting a few sites. I believe DNS is fine. DNS can’t be exploited. Instead, it’s the query in transit that gets exploited due to a lack of security.

A screenshot of a computer

Description automatically generated

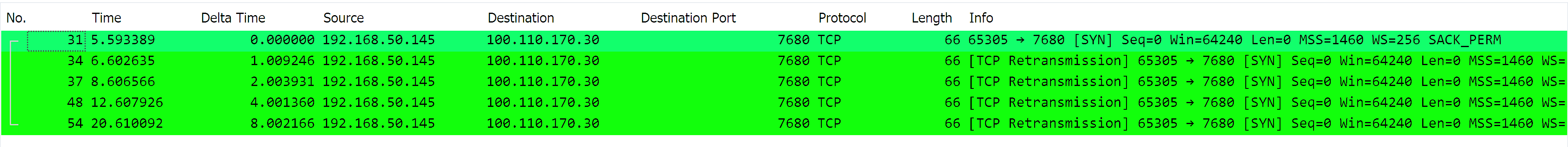
* DHCP
  + DHCP stands for Dynamic Host Configuration Protocol and its purpose is to provide IP addresses to new devices on the network. DHCP is not secure, since it does not provide any sort of authentication. This can lead to cyberattacks, such as the DHCP Starvation Attack, which depletes the server of available IP addresses (aayushhadav, 2022). The port number is 67 and the protocol did appear in my PCAP. I believe it did due to a new device connecting to my router. I think that may have happened due to a roommate getting home. I’m okay with DHCP operating on my network since it is a fundamental protocol and is needed to assign IP addresses.



* SMTP/POP/IMAP
  + SMTP stands for Simple Mail Transfer Protocol, POP stands for Post Office Protocol, and IMAP stands for Internet Message Access Protocol. All three deal with transferring, storing, and accessing mail and messages. All three services have both secure and unsecure ports, so in general it is safe to use the secure ports. The secured ports are 2525 and 587 for SMTP, 995 for POP3, and 993 for IMAP (SiteGround, n.d.). I think the protocols weren’t shown in my PCAP due to me not accessing my mail. If I were to open Gmail and delete or send an email, I believe it would have been in the PCAP. Additionally, I do believe the mail protocols are safe if you use the listed secure protocols. For an everyday user, there is a lot less risk, but for businesses you should be blocking the default unsecure ports.
* SSH
  + SSH stands for Secure Shell and its purpose is to provide remote login and command-line interface from another device. SSH is secure, since it used encryption and authentication to ensure a connection, but I still strongly recommend this port be blocked, since it is very common for attackers to ultimately seek a remote shell on the target machine. I think the only time it should be allowed is in instances of troubleshooting, which should still be strongly monitored. Every day small businesses should have this port blocked, due to them not having their own IT support department. As for alternatives, SSH is the better alternative when compared to remote shell (Rsh). The default SSH port number is 22 and (thankfully) the protocol was not discovered on my laptop. I believe it wasn’t found on my laptop due to there being no remote shell present on my laptop. As for my comfortability with the protocol, I believe it should be handled with strong speculation. If you work at a big company like Google, it’s only natural you may see it more often due to troubleshooting reasons. However, businesses without a designated IT support department should handle this port with extreme suspicion.
* SMB
  + SMB stands for Server Message Block and is used to share printers, files, serial ports, and other services with the network. The newest version of SMB uses AES-128 for encryption and is highly secure (Visuality Systems, n.d.). SMB uses ports 445 and 139 and was not present in my PCAP. I believe it wasn’t present due to me not being a part of a client-server relationship, like FTP protocol. SMB is fine to run on a network if the server is located internally and is secure, and you’re using an up-to-date version of SMB.

## Follow a TCP Stream

* The first step of following a TCP Stream is to find the stream you want to follow. After, you can right click the stream > follow > follow TCP stream. This function will allow you to see all of the data transmissions for that specific stream.



* Following a TCP stream can provide crucial information related to troubleshooting. For example, after following a TCP stream, you may notice a RESET packet, which is only used when there is an error with the connection.
* Additionally, TCP streams are incredibly important when it comes to analyze application behavior. For example, if I noticed I received more RESET packets when I connect to a specific server, it would be logical to assume that their may be an inefficiency within that server’s networking capabilities.
* However, TCP does have its own issues. For example, one issue TCP faces is the lack of encryption, meaning that you can analyze the entire stream if it were to be captured. This is amazing in regard to troubleshooting, since it’s transparent, but is a big privacy issue when transmitting packets over the internet. Some ways to overcome these issues would be to encrypt all traffic, for security purposes, and employ decryption keys for those packets. However, the implementation of these solutions could be costly, and could also be abused by malicious actors to cover their footprints.

## Protocol Hierarchy Statistics

* Next, I take a look at the Protocol Hierarchy Statistics to get a better understanding of the total number of the different categories of packets.

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

* The Protocol Hierarchy is important because it gives valuable insight into the number, percent, and total bytes of all the packets in a category. For example, an analysts might notice a huge influx in the number of ICMP packets, meaning there could be an issue with the network or there is a potential DDoS attacking occurring.
* The Protocol Hierarchy can also highlight malicious activity. For example, a deviation such as in influx in the number of SSH or SFTP packets could be evidence of Privilege Escalation or Exfiltration techniques.
* Additionally, long-term, analysts can continually compare unsecure protocols percentages and numbers to previous years in hopes of continually lowering the number. An example would be implementing TLS more in comparison to TCP.
* Overall, I believe the Protocol Hierarchy Statistics is incredibly useful for both immediate analysis and long-term planning as security professionals.

## Conversation Statistics

* In this part, I will be looking at the Conversation Statistics, which shows the amount of packets, bytes, and bits/s being transferred from point a to point b.

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

* Conversation Statistics can show bandwidth issues and suspicious connections. For example, one of my connections in the LongPCAP sent 2.633 kilobytes to point a, but at a speed of 3 bits/s which is an extremely slow connection.
* In relation to Network Security, Conversation Statistics can be invaluable. For example, Conversation Statistics can help create a baseline for normal, everyday operations. After creating a baseline, it can be compared to suspicious Conversation Statistics, which may highlight possible malicious activity, such as a DDoS attack or data exfiltration attempts. A DDoS attack would probably look like Packets B -> A being an abnormally high number, while a data exfiltration attempt would probably have an abnormal Packets A -> B due to it being sent out.
* Comparing Conversation Statistics over long-term periods can highlight issues, such as network inefficiencies and capacity planning, which can lead to more network availability.

## Endpoint Statistics

* To begin, Endpoint Statistics are incredibly important when analyzing network traffic. For example, Endpoint Statistics can be used to find suspiciously highly active endpoints, which can be blocked, managed, or investigated to make sure they aren’t malicious.

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

* Additionally, after identifying the abnormally highly active endpoints, we can analyze for malicious activity. For example, IP address 18.238.171.63, if it were on a local network, could be seen as highly suspicious when you compare it’s IP address to the other endpoints.
* Discuss the significance of Endpoint Statistics in Wireshark for understanding network traffic and behavior. Describe how this feature can aid in identifying the most active or problematic endpoints and the implications for network management and security.
* Explain how Endpoint Statistics can be utilized to detect potential network threats. Consider scenarios such as detecting unauthorized devices, pinpointing malicious traffic sources, or identifying endpoints involved in data exfiltration attempts.
* Illustrate how an analyst might use Endpoint Statistics to troubleshoot network performance issues. Describe a step-by-step approach to isolating problem endpoints and diagnosing issues such as bandwidth hogging, abnormal connections, or misconfigured devices.

## IO Graphs Statistics

* IO Graphs can be accessed by going to Statistics > IO Graph.

A screenshot of a computer

Description automatically generated

A screen shot of a graph

Description automatically generated

A screen shot of a graph

Description automatically generated

* IO Graphs can provide critical information about a network’s performance. For example, just using the default settings, it is easy to notice peak network times. Similar to the previous model, IO Graphs can be used over long period of time to create a baseline. After creating the baseline, it can be used to compare newer captures to, which will in turn highlight suspicious activity. For example, from the LongPCAP alone, it would be safe to assume that the high increase at ~4800 seconds is incredibly suspicious and warrants investigating.
* In addition, comparing traffic patterns over long periods of time can give IT departments a better understanding of future events that may occur. For example, if I ran a business and I knew it could get busy on Black Fridays, by comparing traffic patterns I can get a rough estimate of how much bandwidth may be used.

## Flow Graph Statistics

* The Flow Graph can be found by going to Statistics > Flow Graph

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

* To begin, Flow Graphs can be utilized by analyzing the different network entities the packets go through. For example, for all of the packets on the way to 52.185.211.133 in the LongPCAP, it passed through the Apple\_e4:a5:ee device. If I knew that that was required and compared it to other packets, and saw that other packets skipped that device and ended up lost, that could be an easy to identify and fix error.
* As for network security, analyzing the flow graph could show a man-in-the-middle attack, due to a non-network IP address accessing the packets in transmission. Additionally, communication with a non-internal server could show malware communication via a C2 server.
* From a support standpoint, Flow Graphs provide essential information on identifying and resolving bottlenecks. They can do so by both analyzing the timestamp on the left, and analyzing the number of devices the packets travel through. You can also try to incorporate multiple paths to a specific destination to help prevent overloading. For example, if you know traffic can get congested on it’s way to an internal server, having multiple paths to it can help prevent congestion.

## Overview and Wireshark’s role in Cybersecurity

* Wireshark is an amazing tool as a protocol analyzer. It captures packets, provides amazing filtering capabilities, offers packet analysis, and provides visualization via graphs, such as the IO and Flow Graphs. All of these tools listed help with troubleshooting, performance analysis, and security auditing. For example, the IO Graphs are an amazing graph for performance analysis and troubleshooting. Furthermore, Flow Graphs do an amazing job at giving insight into security, as you’re able to analyze the path the packets take.
* In addition, Wireshark can help with identifying network vulnerabilities and threats as well. For example, suspicious login attempts from outside IP address can be evidence of unauthorized access. Moreover, a high influx within the IO Graph could be evidence of data exfiltration.

# Network Traffic Analysis with Network Miner

* In this lab, I will be using NetworkMiner, which is an amazing networking tool. Let’s begin!

## Host and Endpoint Analysis

* First, I will open the PCAP and investigate one host.

A screenshot of a computer

Description automatically generated

* In networking, host and endpoint analysis is critical to the security of the network’s infrastructure. Depending on the network topology, your packets may be sent to other users before making it to the router, so making sure only valid users are connected is an important step in network security.
* For incident response, I would use Network Miner to focus on host and endpoint analysis, due to the amount of information that can be sorted in each to understand ways. Additionally, once you narrow the search down to a specific host, you can filter based on their information to create attack timelines. Furthermore, that information can be used to gather information, such as what systems were impacted, what information was extracted, etc.

## File Reconstruction

* In this step, I will be looking at the reconstructed files. I think this tab is amazing, especially in relation to digital forensics, incident response, and investigating malware.

A screenshot of a computer

Description automatically generated

* Reconstructed files can significantly aid in cybersecurity investigations. Using file reconstruction, you can look for suspicious files being sent over the network, such as .exe files. It also aids in investigating other suspicious outputs, such as .txt files and large files. Additionally, file reconstruction on Network Miner also provides additional information, such as hash values, that can be plugged into VirusTotal.

## Session Analysis

* The session tab can be used to analyze relationships between two devices who have created a session.

A screenshot of a computer

Description automatically generated

* NetworkMiner’s session analysis tab is an amazing tool for network security investigations. For example, if there is a known malicious server host targeting your network, you can look for connections based on the sessions tab.
* Additionally, session analysis works well with other security incident response protocols, such as packet and endpoint analysis. For example, you may see a suspicious session connection. Based on that, you can conduct packet analysis on the packets interchanged between the client and the server. Then, if there continues to be evidence of suspicious activity, you can conduct endpoint analysis on the client machine.

## Credential and Authentication Data

* In the part, we will be looking at the credentials tab for any captured credentials. Fortunately, protocols, such as FTP and HTTP, which lack encryption, where not being used so no credential data was captured.

A screenshot of a computer

Description automatically generated

* Analyzing credential and authentication data can highlight unsecure protocols, of which may be operating on the incorrect ports. This can help highlight issues that may not have been known, such as default settings, which will result in stronger networks.
* The best strategies for mitigating the risk of exposed credentials and authentication data are customizing network settings and implementing policies to continually monitor for leaked credentials and authentication data.

## DNS and Domain Analysis

* In this last step, we take a look at the DNS and Domain Analysis tab.

A screenshot of a computer

Description automatically generated

* DNS and Domain Analysis is another important tool within cybersecurity. For example, you can identify attacks, such as phishing attacks, by comparing the DNS Query to the DNS Answer.
* Additionally, in the event of a cybersecurity investigation into a phishing campaign, you can obtain the phishing site based on the DNS answer and can report it or further investigate it using sites like VirusTotal.

## Overview and Network Miner’s role in Cybersecurity

* NetworkMiner is an amazing network forensic tool. It extracts and presents the data into multiple categories, such as hosts, sessions, and file reconstruction, by analyzing pcap data.
* NetworkMiner is an amazing utility tool for cybersecurity defense. For example, after capturing a pcap using Wireshark, I may input the pcap into NetworkMiner for additional insight into the pcap. After finding suspicious activity, such as IP addresses and hashes, I can use other sites like VirusTotal to confirm that the network was compromised.

# Overview of Wireshark and Network Miner

* Overall, I believe Wireshark and NetworkMiner complement each other beautifully. While Wireshark provides a more generalized view at packet capture and protocol analysis, NetworkMiner digs deeper in network forensics by offering tools like file reconstruction, DNS and domain analysis, and session insight.
* Additionally, using both can provide insight into cybersecurity investigations, like malware analysis and breach detection. For example, using Wireshark’s IO Graph, you can get an idea of when a DDoS attack may have occurred based on the number of incoming packets. Afterwards, you can investigate it further using NetworkMiner’s host analysis tool. Using both these tools will give analysts a better understanding of why security incidents happened and what caused them.

# Conclusion

* Overall, this was an amazing lab. Tools like NetworkMiner aren’t as popularized as Wireshark, but give just as good insight into network traffic and forensics. Going forward, I hope to continue using the tool and integrating it into my eventual everyday life as a SOC analyst.

# Bibliography

aayushhadav. (2022, July 22). *DHCP Starvation Attack*. Retrieved from GeeksforGeeks: https://www.geeksforgeeks.org/dhcp-starvation-attack/

Barney, D. (2022, November 2). *Secure File Transfer - Is FTP Secure? No. Fortunately, MFT Is!* Retrieved from Progress: https://www.ipswitch.com/blog/secure-file-transfer-ftp-safe-fortunately-mft

Cloudflare. (n.d.). *What is DNS Security?* Retrieved from Cloudflare: https://www.cloudflare.com/learning/dns/dns-security/

MITRE. (n.d.). *ATT&CK Matrix for Enterprise*. Retrieved from MITRE: https://attack.mitre.org/

SiteGround. (n.d.). *What are Email Protocols (POP3, SMTP and IMAP) and their default ports?* Retrieved from SiteGround: https://www.siteground.com/tutorials/email/protocols-pop3-smtp-imap/

Visuality Systems. (n.d.). *What is SMB? What IT Decision Makers Need To Know*. Retrieved from Visuality Systems: https://visualitynq.com/resources/articles/what-is-smb-what-it-decision-makers-need-to-know/