**Lab 1: Using Wireshark to Integrate a Network Auditing and Log Files Layer of Defense**

**Security Team:** Luis Ruiz, Marcos Vallejos, Ryan Rockett, Kari Hattabaugh

Table of Contents

[Introduction 2](#_Toc83586234)

[Scope 2](#_Toc83586235)

[Wireshark 4](#_Toc83586236)

[Synopsis 4](#_Toc83586237)

[Prerequisites 4](#_Toc83586238)

[Installation, Configuration, and Testing Instructions: 6](#_Toc83586239)

[Recommendations 17](#_Toc83586240)

[Alternatives 18](#_Toc83586241)

[Conclusion 18](#_Toc83586242)

[Citations 19](#_Toc83586243)

# Introduction

Our Security team has been tasked with providing a detailed guideline for implementing an integrated defense in depth architecture to secure Ashburn’s Frog Emporium, the leading amphibious distributor in Northern Virginia. The first tool we have decided to implement is Wireshark to help monitor our network traffic. Wireshark is the most well-known free and open-source network packet analyzer. This is a powerful and cost effective tool that users can use to browse network traffic in real time. It captures packet data being transmitted over the network and outputs it in a readable format so that it can be examined by the user. Through our use of Wireshark, we are adding a Network Auditing and Log Files layer of defense that will monitor our network to secure it. Our main use of Wireshark will be primarily at the network layer to troubleshoot the network and inspect our network activity.

# Scope

Ashburn’s Frog Emporium is a small scale business, which offers online and in person sales. With the growing need for Information Security and their expanding customer base, Ashburn’s Frog Emporium is looking to improve their security. The main consideration was to ensure that their TCP/IP communication was being monitored. After exploring both paid and unpaid options, the tool we implemented was Wireshark. This tool takes captures of network traffic and allows the user to filter the information to gain a better understanding of the network traffic. Wireshark is a free software tool, however if Ashburn’s Frog Emporium were to have a larger budget then they would be able to utilize the paid tool Auvik. Auvik is a network management software that provides some automation and improved performance to the network monitoring process. Through the next 90 days, our team will identify, install, and configure a variety of tools to provide a cost effective layered defense to Asburn’s Frog Emporium. Asburn’s Frog Emporium network consists of workstations, point of sale devices, and servers. The operating systems used are Windows 10 and Windows Server 2016. We have outlined and described the installation configuration and testing processes for Wireshark on a windows machine.

The tools currently applied and the layers of security that these tools are applicable to are listed below:

|  |  |  |
| --- | --- | --- |
| **Layer** | **Description** | **Tools Applied** |
| Physical Security | Measures taken to protect a computer or other network device from theft, fire, or environmental disaster. |  |
| Authentication and Password Security | Password policies, identity verification, etc. |  |
| Operating System Security | Maintaining and managing OS patches. |  |
| Antivirus Protection | Protection from malware for the network and connected devices. |  |
| Packet Filtering | Blocking or allowing the transmission of packets based on configured criteria. |  |
| Firewalls | The tools installed and configured to manage traffic on a network, including firewall policies. |  |
| Demilitarized Zone (DMZ) | The area on the exterior of the network, which focuses on accessibility and the network’s perimeter security. |  |
| Intrusion Detection and Prevention Systems (IDPS) | Technology used to detect and, in some cases, produce an automated response to signatures, or patterns of suspicious network activity. |  |
| Virtual Private Network (VPN) | Technology that allows for secure communication using public internet connection. |  |
| Network Auditing and Log Files | Recording and organizing network activity and performance to allow for analytics. | Wireshark |
| Routing and Access Control Methods | Tools that control or limit movement into and throughout the network. |  |

# Wireshark

## Synopsis

As mentioned earlier, our team has decided to implement the network packet analyzer, Wireshark. It is a network packet analyzer used as a measuring device for examining what is happening inside our networks. The application Wireshark is available for free, is open source, and is one of the best packet analyzers available today. Wireshark is a type of packet sniffer, which is also known as a network protocol analyzer, protocol analyzer, and network analyzer. Our team will run the Windows Installer (64-bit) for our Windows 10 machines and Windows 2016 servers. We will be implementing the latest version of Wireshark (Version 3.4.8) for our network. With a packet sniffer intercepting network traffic, our team will understand the activity being processed and harvest useful insights.

Our security team will utilize Wireshark for these cases:

· Identify the cause of a slow internet connection

· Investigating lost data packets

· Troubleshooting latency issues

· Detecting malicious network activity

· Identify unauthorized data exfiltration

· Analyzing bandwidth usage

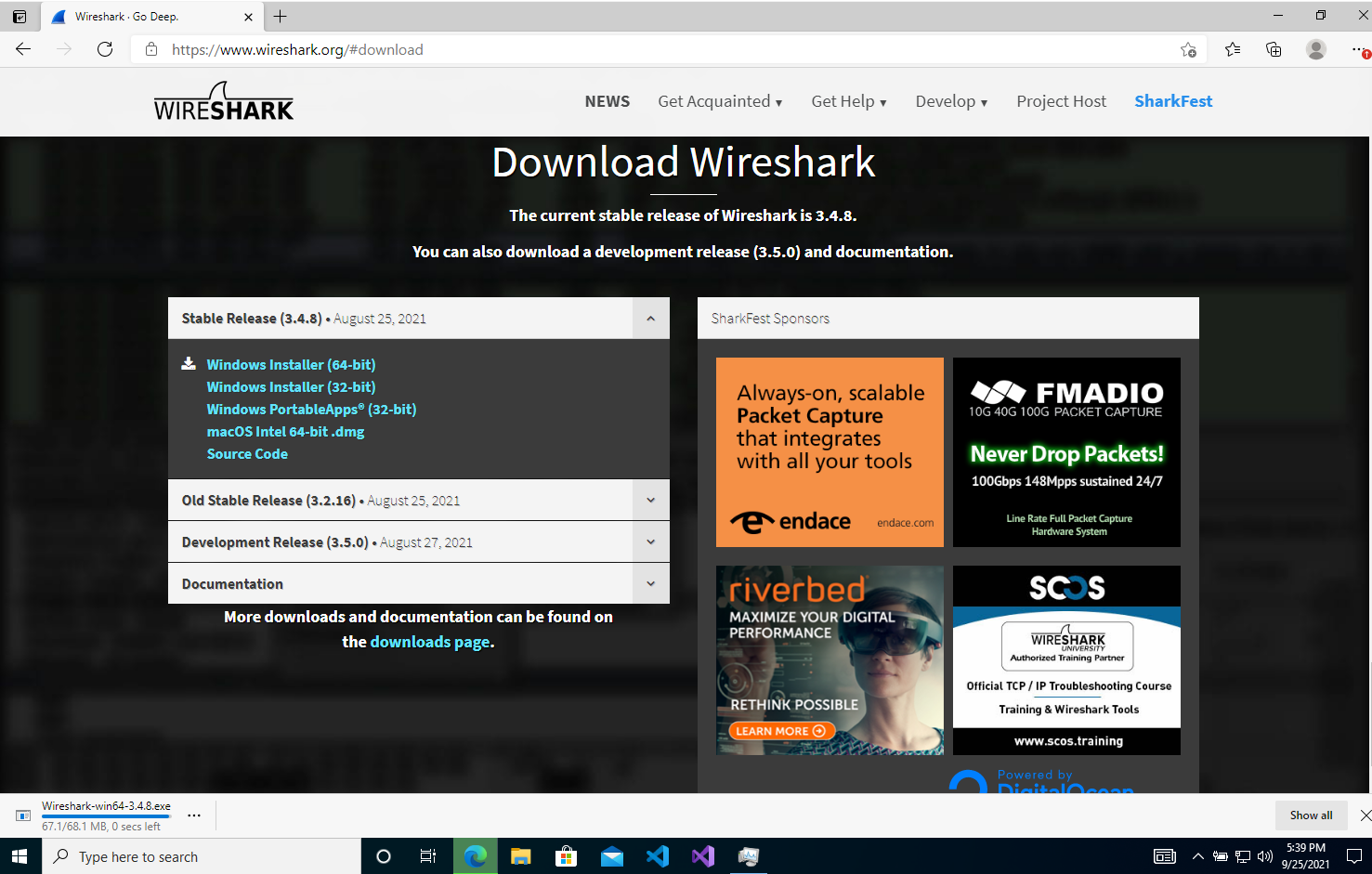
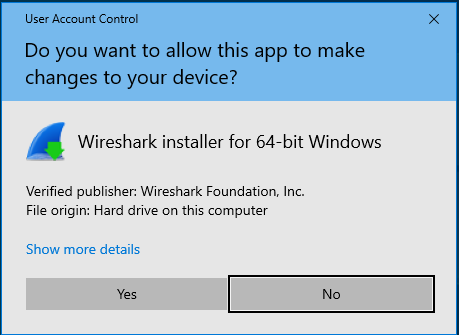
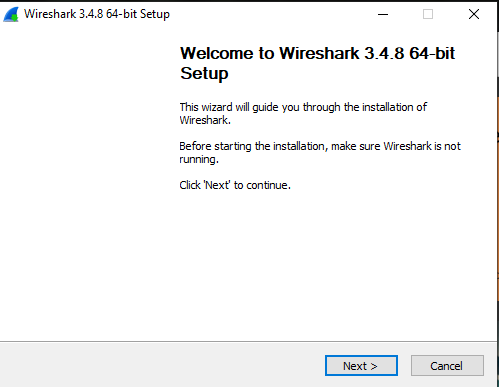
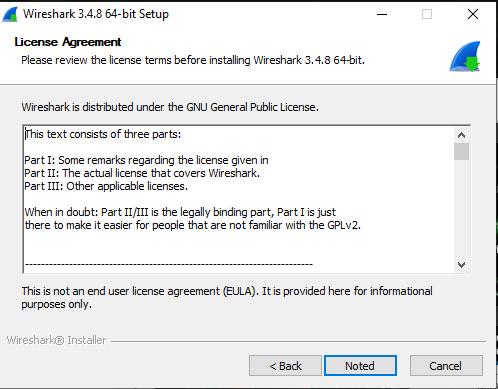
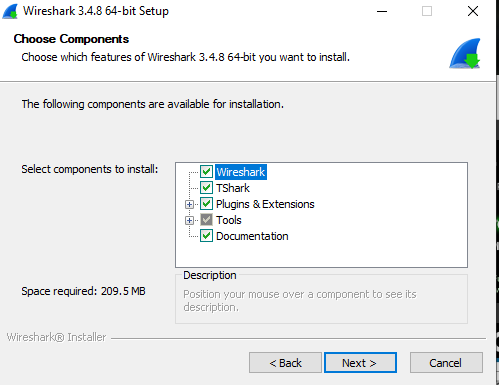
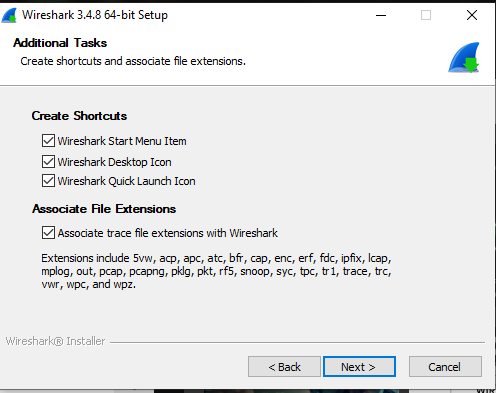
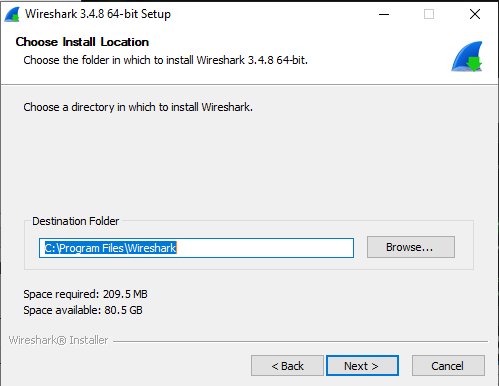
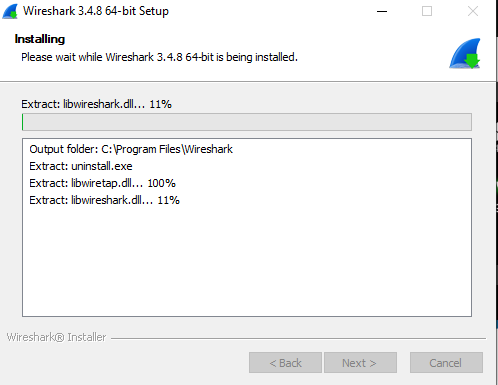
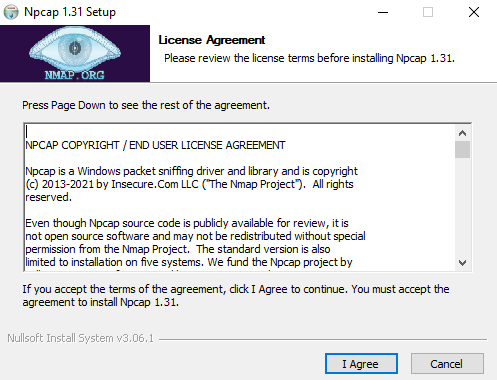
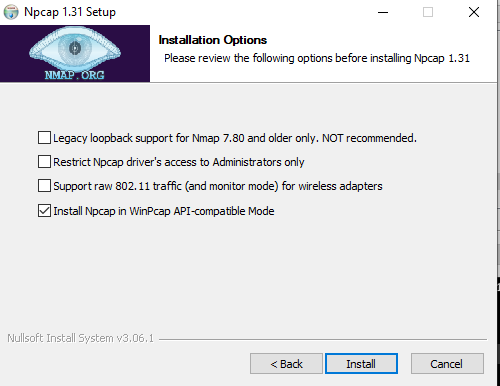
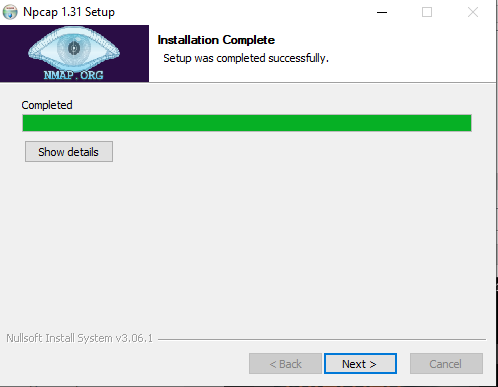
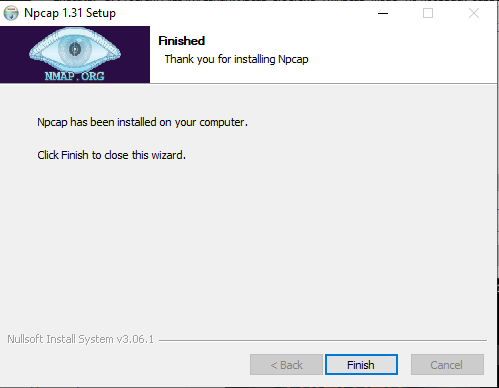
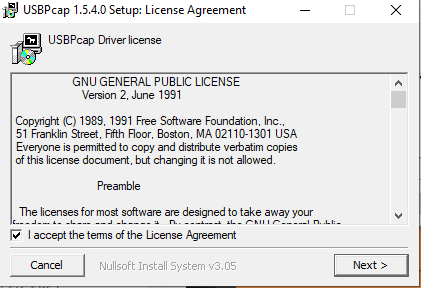
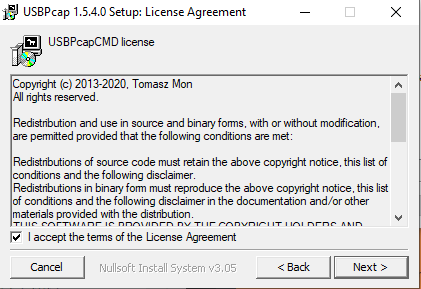
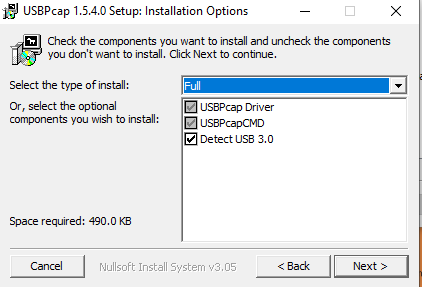
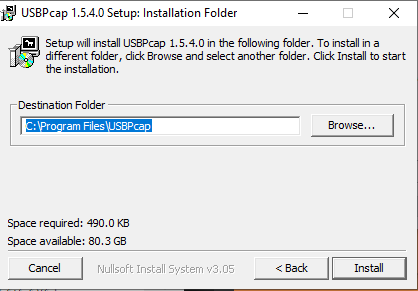
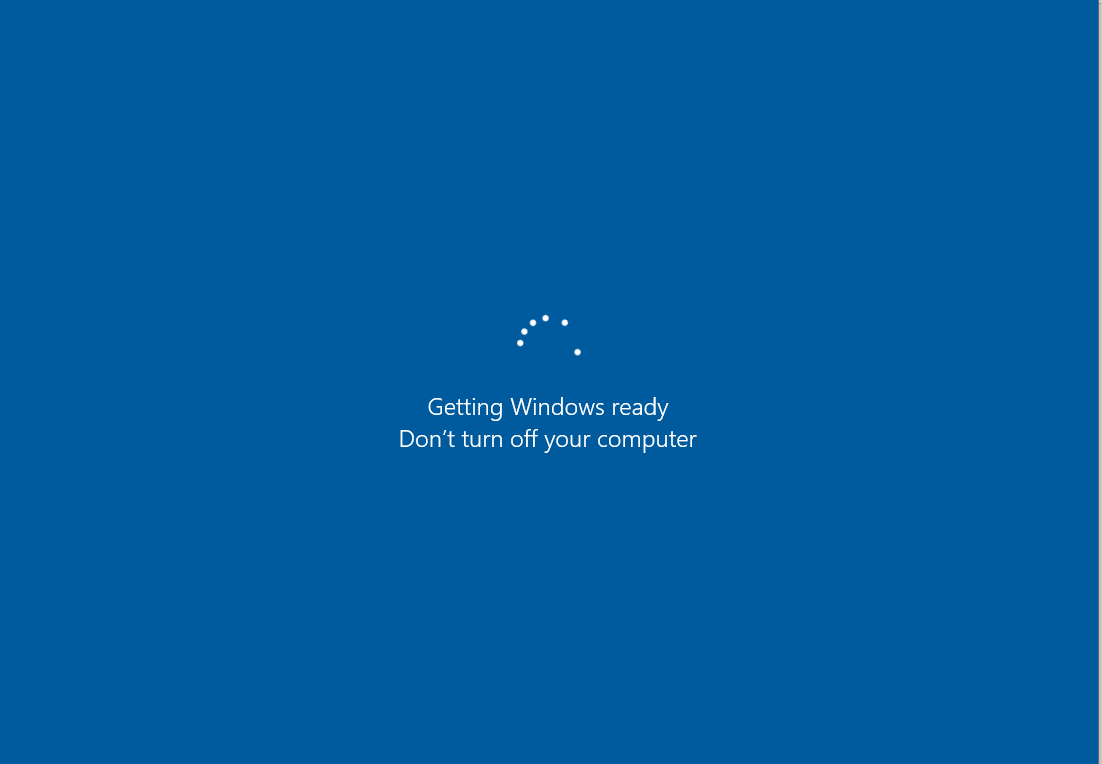
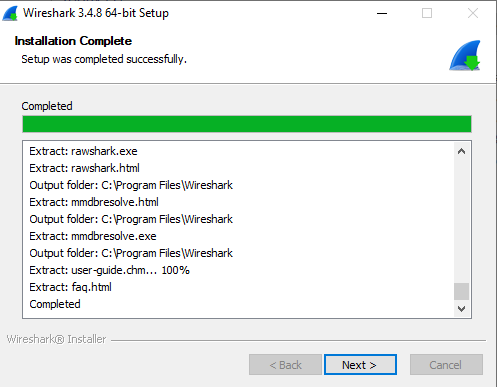
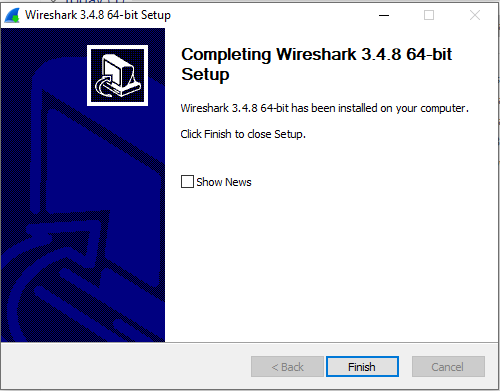
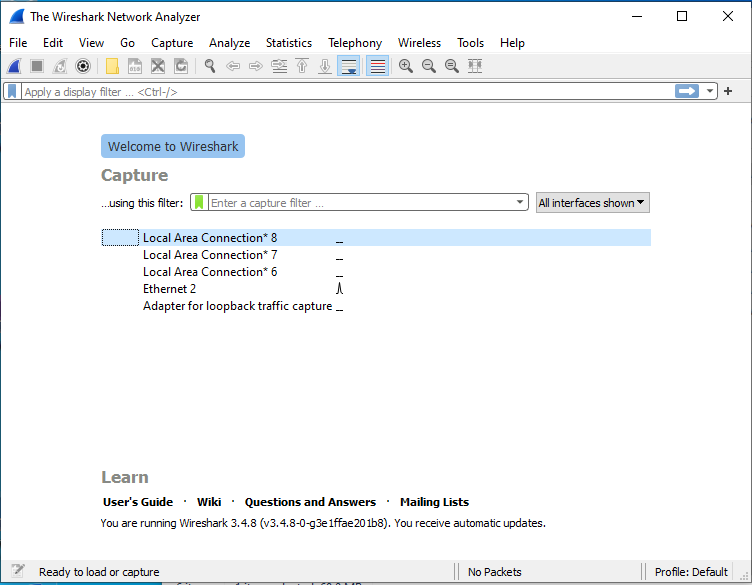
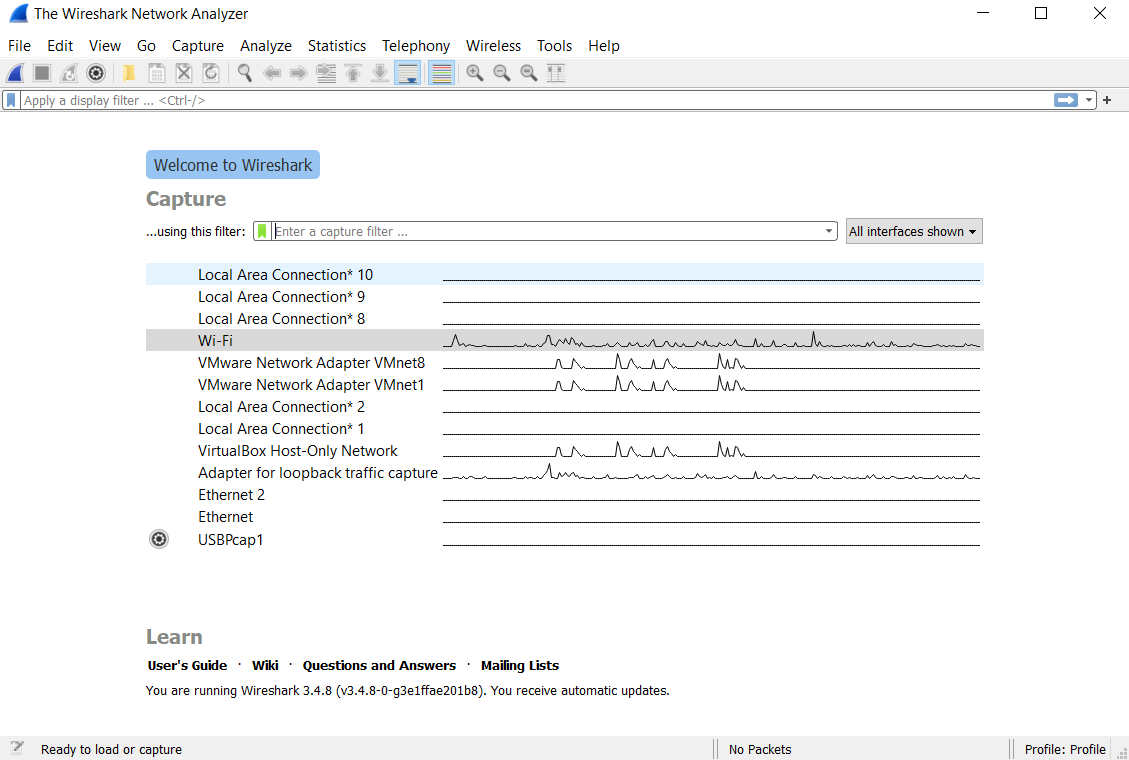
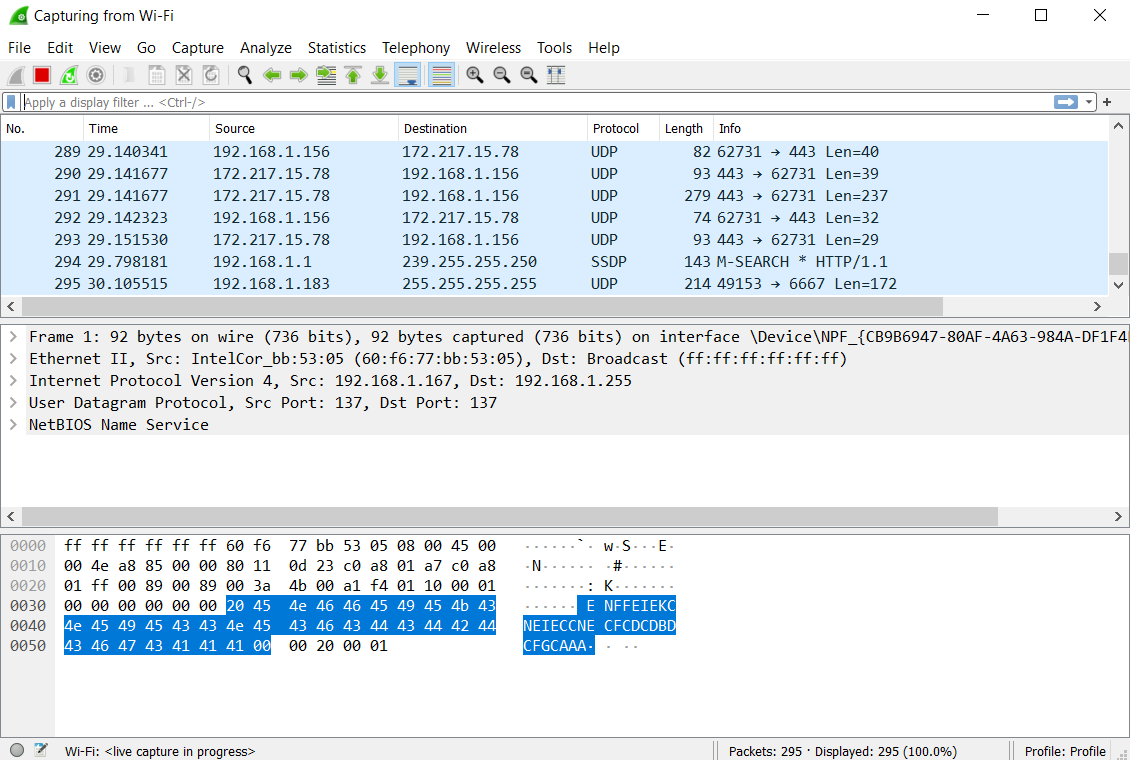
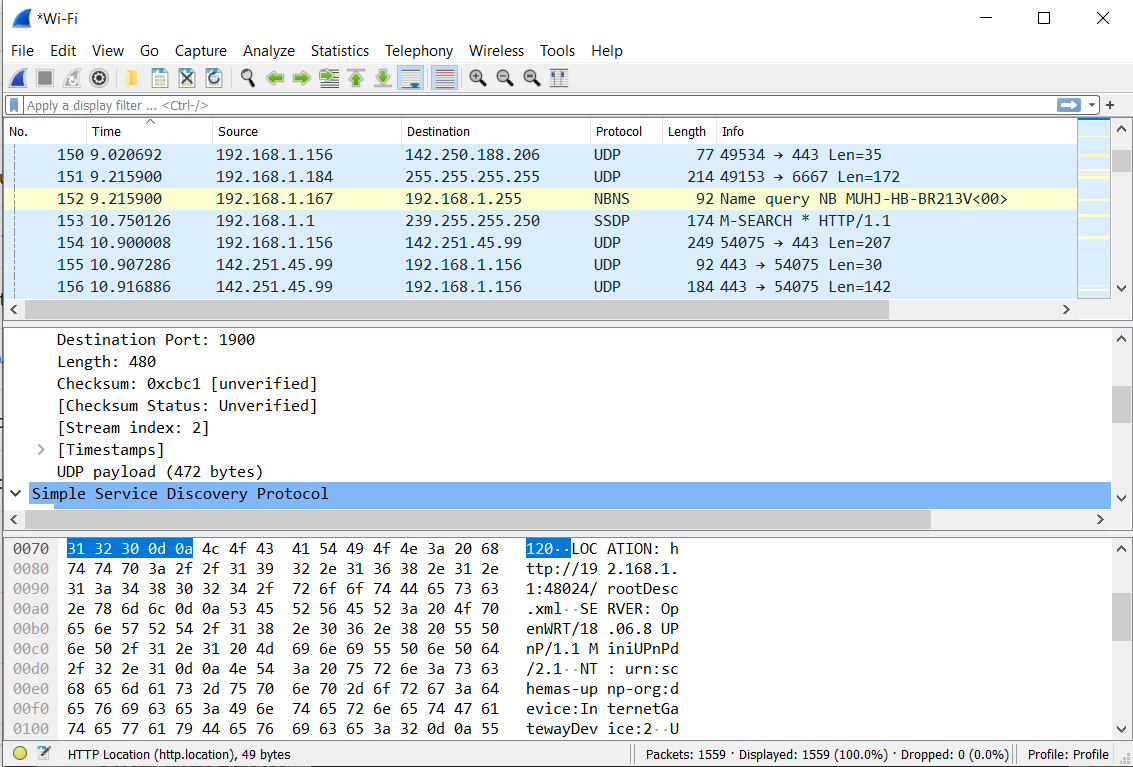
· Tracing voice over Internet (VoIP) calls over the network

· Intercepting Man-in-the-Middle (MITM) attacks

## Prerequisites

1. Before installing Wireshark, you must first make sure that it adheres to the company policies, and you are authorized to not only install but capture packets on the network.
2. Wireshark will support the following systems:
   * Windows 8.1
   * Windows 10
   * Windows Server 2012 / R2
   * Windows Server 2016
   * Windows Server 2019
3. Processor required:
   * 32-bit x86 processor - Applicable for the 32 bit version
   * 64-bit AMD64 - Required by the 64 bit version being installed
4. At least 500 MB of usable RAM
5. At least 500 MB of usual hard disk space
6. Make sure that the Network Card you are using is supported and allows for network captures, some examples are:
   * Ethernet
   * 802.11
   * Token-Ring
   * ATM

## Installation, Configuration, and Testing Instructions:

1. Boot up Windows10 device and open an internet browser. In this case we used Microsoft Edge, however Google Chrome and Mozilla Firefox would be acceptable options. Navigate to https://www.wireshark.org/#download. You should see the screen shown below.
   1. 
2. Select the Windows Installer (64-bit) option. If you are running a Mac device you can select macOS Intel 64 bit .dmg. One you select it, it should automatically begin downloading. The User Account Control window should automatically appear on your screen, if not click on the download under the download button in your browser. Select the “Yes” in the User Account Control window as shown below.
   1. 
3. The Wireshark 3.4.8 64-bit Setup wizard will automatically appear. This will guide you through the setup process. Select “Next >” as shown below.
   1. 
4. Next you will see the License Agreement window, this outlines the user agreements and rights associated with using Wireshark. Select “Noted” as shown below.
   1. 
5. On the Choose Components window it allows you to review the different files that will be downloaded with the installation process. You can review the description of these different files by hovering over them. Select the “Next >” option as seen below.
   1. 
6. The Additional Tasks window allows you to select which shortcuts will be created. Ensure all options are selected and select “Next >” as shown below.
   1. 
7. Next the Installation Location must be selected. The default is within the programs file. Ensure the location matches the one below and select “Next >”.
   1. 
8. The next screen allows you to view the installation progress, this may take a few minutes.
   1. 
9. Once the installation process is complete, the License Agreement for Ncap will be displayed. Review this information and select “I Agree” as shown below.
   1. 
10. Next the Installation Options window will appear. Ensure that only the option for installing Npcap is selected and select “Next >”, as shown below.
    1. 
11. The screen will show the installation progress and indicate when the installation is complete. You have the option to review details. Then select “Next >” as shown below.
    1. 
12. The Finished window indicates that Npcap was successfully installed and you can select “Finish” as shown below.
    1. 
13. Next you must use the USBPcap wizard to install USBPcap. The GNU General Public License is displayed. This defines the ownership of this specific tool. You can review this information. Then, check the box next to I accept and the “Next >” option as shown below.
    1. 
14. The next window displays the user agreement, which outlines acceptable use laws. Check the box to accept the terms and the “Next >” option, as shown below.
    1. 
15. Next you must select the Installation Options. Ensure the drop down box has Full selected and each of the check marks are filled next to each option. Then, select “Next >” as shown below.
    1. 
16. The next window is determining where the program files will be stored, the destination folder should be the same as shown below. Once this has been verified, select “Install” as shown below.
    1. 
17. Next the workstation will require a reboot. If your machine does not automatically restart then you will need to initiate a reboot from the start menu. Once the reboot has begun, you should see the screen below. This process may take several minutes.
    1. 
18. Once the reboot has completed, you will see the Installation Complete window as shown below. This shows what was installed and their locations on the local device. You then select “Next >” as shown below.
    1. 
19. Next is the Completing Wireshark 2.4.8 64-bit Setup window. This Indicates the installation was successful and the final steps for setting up the Wireshark tool are ready. Select “Finish” as shown below.
    1. 
20. Once setup is complete Wireshark should open automatically. You can see below the different channels. Next, we will take a capture to verify the functionality of our tool.
    1. 
21. We will next begin a packet capture. First, we would apply capture filters prior to starting the capture to only capture specific types of packets (ports, protocols, etc.). We will not apply any filters during this test capture. We will select the channel of which we would like to sniff on. In the photos below we will be sniffing on the Wi-Fi channel, however you can also do a packet capture on the Ethernet channel. You can either double click on the channel to begin a capture or select Capture>Start at the top of the application.
    1. ****
22. Once the capture has begun, you should see packet information appearing in the three different panes. The first one being the packet list, which lists the packets. You can apply display filters and sort the packets by time, type, and IP address in this pane. The second pane is the packet details. It lists the details for the packet you have selected in the packet list. Lastly there is the packet bytes window, it displays the raw data within the packet selected in the packet list. Once you have captured enough packets, you will select the red square under edit to stop the capture.
    1. ****
23. Below is an example of what your capture might look like after the capture is complete. Since we are just verifying the functionality of this tool, we don’t need to save it and can exit the tool through File > Quit. Then selecting the “Do Not Save” option.
    1. ****

## Recommendations

Wireshark is a powerful tool in our security arsenal but to bring out Wireshark’s true potential and implement it as part of Ashburn’s Frog Emporium’s long term security strategy then the Wireshark users must also be trained on how to use it successfully beyond its basic usage. The following training recommendations will maximize the effectiveness in which the users will be able utilize Wireshark.

1. **Time Display**: The best way to determine if the network response is on a delay is to analyze the time of the packet. This will help improve network speed, reduce packet loss and the traffic flow that is occurring on the network.
2. **Placement:** If a capture is only set on one endpoint, one side of a firewall or server then it is only giving the user that specific perspective. However, if a capture is placed on both endpoints or sides of a firewall then it will allow the user to see if there is any packet loss as packets are being transmitted and there are no communication issues.
3. **Information Gathering:** To make sure that troubleshooting is as efficient as possible we want the users to be trained in how to gather information to understand the problem they are facing, understand the protocols involved and which systems are being affected. Understanding those components will help the user create more specific capture filters rather than having to search through multiple filters.

# Alternatives

We identified Auvik, a network monitoring and management tool, as an alternative tool to secure the Network Auditing and Log Files layer. Auvik is a subscription based Software-As-A-Service that has a free trial with flexible pricing and requires a custom quote. All plans with Auvik have unlimited users, endpoints, network sites and support but their pricing is billable per device such as switches, routers, firewalls and physical Wi-Fi Controllers. The main advantage of Auvik over Wireshark is that it is more user friendly with a more sophisticated GUI and also has customizable alerting features. The Auvik team can also customize the software for specific organizational needs, but pricing is variable depending on the usage specifications. The total cost of ownership by integrating Auvik will be much larger than that of Wireshark, which is a free tool. However, Auvik will not only increase the efficiency that the IT team can work and monitor the network with but will also have a more robust alerting system. Due to budget constraints, we have selected Wireshark, however, in the future when budget is less of a concern when compared to total effectiveness and efficiency then Auvik would be the better choice for network monitoring and management.

# Conclusion

Ashburn’s Frog Emporium is looking to improve their information security using the concept of integrated defense in depth. Through the exploration of different tools, they have installed Wireshark to provide a level of network monitoring. This is most impactful in the network auditing and log files layer of the integrated defense in depth model. Though there are multiple tools that would provide, the driving factor in implementing Wireshark is the budgetary concerns. As Ashburn’s Frog Emporium expands and has a larger budget, they plan to move towards Auvik, a network monitoring tool that provides higher performance and automation to the monitoring process of network monitoring.

# Citations

Kost, E. (2021, August 19). *What is Wireshark? The free network sniffing tool*. Upguard. Retrieved September 26, 2021, from https://www.upguard.com/blog/what-is-wireshark.

Occhiogrosso, S. (2020, June 22). *The top 4 ways to utilize WIRESHARK SUCCESSFULLY!* Network Management Software - Reviews & Network Monitoring Tools. Retrieved September 26, 2021, from https://www.networkmanagementsoftware.com/top-4-ways-utilize-wireshark-successfully/#wbounce-modal.

Sharpe, R., Lamping, U., & Warnicke, E. (n.d.). *Wireshark User’s Guide*. 1.2. system requirements. Retrieved September 26, 2021, from https://www.wireshark.org/docs/wsug\_html\_chunked/ChIntroPlatforms.html.

softwareadvice.com. (n.d.). *Auvik software*. Auvik Reviews, Demo & Pricing - 2021. Retrieved September 26, 2021, from https://www.softwareadvice.com/crm/auvik-profile/.