Here we go everyone another round of technical information and tools for you to use for protection and analyzing your network. There are so many different types of tools that can be used for recovery of lost, deleted, altered, files in your system and network. For more information go to [HTTPS://www.aimeesaudios.com](https://www.aimeesaudios.com), and donations are excepted for the creation of the patent to live stream the criminal network and broadcast their telecommunications. [Fundraiser by Amy Holem : Patent Live Stream Criminals, Hackers, Stalkers (gofundme.com)](https://www.gofundme.com/f/256fp-patent-live-stream-criminals-hackers-stalkers).

 When working in digital investigations Wireshark is a tool that any investigator can use for investigation purposes. You can download Wireshark by clicking on this link [Wireshark · Go Deep.](https://www.wireshark.org/) Wireshark can be used as a packet analyzer or sniffer and analyze the network and protocols that have been installed on the network and computing device. Wireshark is capable of capturing packets that reveal signatures and information of attacks and hackers penetrating the network and the devices. Knowing how to use this tool properly is the first tool to use and collect evidence for investigation purposes. We will be discussing the capturing of live packet data from a network interface and capture files using tools such as TCPDump, Windump, and Snort. Wireshark is capable of saving, exporting, and filtering packets and is filter schemes suck as colorizing and categorizing the communications. Knowing and understanding the basics and how to use the Wireshark properly is where all investigations begin with the network.

 Wireshark can capture live data from a network and interface, knowing what type of information can be extracted is extremely important to know and understand the type of evidence and information can be obtained. Wireshark can scan TCP (Transmission Control Protocol) using SYN (Synchronize) to analyze the start of the TCP session and ACK (Acknowledge) the data in the header. The UDP (User Datagram Protocol) is used when there is no connection to the internet, used for speed, VoIP (Voice over Internet Protocol), and live streams connections. ICMP (Internet Control Message Protocol) which can find and fix a network also can ping/echo information and timestamp/synchronize devices. (Schoenfelder, N., 2020). Wireshark can also determine different types of attacks such as trojan horses, worms, bot software, DoS (Denial-0f-Service), and even malware. Wireshark can port scan, see BitTorrent, and convert FTP (File Transfer Protocol) and IRC (Internet Relay Chat) channels, also collect information such as IP (Internet Protocol) addresses, http (Hypertext Transfer Protocol) requests, DNS (Domain Name Server), and ARP (Address Resolution Protocol) as well. You can also choose the type of connection you want to review within different networks such as ethernet, LAN (Local Area Network), WLAN (Wireless Local Area Network), or any network that your connection is associated with using different devices such as routers, switches, hubs, DHCP (Dynamic Host Configuration Protocol), servers, remote access, and even VM’s (Virtual Machine). Knowing the network and traffic that is coming in and out of the system can help secure, gather, and recover data in RAW format for any investigation purposes. (Ndatinya, V., Xiao, Z., Manepalli, V. R., Meng, K., & Xiao, Y., 2017).

 Using different tools such as SolarWinds can capture data like TCPDump using command lines within Wireshark, and capture traffic on a remote server. “TCPDump, logs TCP/IP traffic between the network and computer (Tcpdump, 2020).” Some of the best command lines to use are; tcpdump -w/-c/-s/-i/-n/-v/-vv/-vvv/-F/-list-interfaces, and capture filters such as: host, net, dst/src host, port, portrange, gateway, broadcast, IP multicast, and/or/not operators. For mail information and collection data packets from multiple hosts and subnets for SMTP, IMAP, IMAP, TLS, POP3. (PHILLIPS, A., 2020). WinDump is a windows version for a TCPDump that monitors the network using a UNIX or Linux open-source operating system. Just like a TCPDump open-source operating systems collect data in the form of a libpcap library, you can download different tools such as WinDump, Snort, NMAP. Snort software works on other operating systems such as Fedora, Centos, and FreeBSD. Once the operating system is determined depending on the software that is downloaded and that will determine what type of command lines an investigator enters. Most software installations work in a wizard format and clicking the proper fields will determine the evidence that needs to be extracted. (WinDump, 2018).

 Once Wireshark has been properly downloaded using the proper tools with the correct operating system, there are some unique features that should be taken into consideration. The save feature within Wireshark allows an investigator to save specific files from the data that has been analyzed and collected as evidence. Make sure when you are saving the files that it is in the correct format otherwise you might lose information from the timestamp and SYN process. Timestamps are important information and evidence for warrants, subpoenas, in different regions, time zones, and jurisdictions. The easiest way to separate the evidence that is extracted is using the filter bar. The filter bar allows you to look up all queries in different areas such as HTTP, DNS, ARP, SSDP, UDP and DHCP and more. Once again it depends on the type of network evidence that is under examination of which you need to extract, the filter bar can help you analyze the specific areas faster and more efficiently. Once the evidence is identified you can choose an export option as well. This will allow you to extract in different formats such as packet lists/details and bytes, plain text, and formats such as CSV and JSON. These provide different scripts and layouts for the details and information that is collected, reading the language and the conversation in a RAW, binary, and hexadecimal language.

 When searching Wireshark using the filer the packets can be categorized in using different expressions such as a filed name, relation, value and even the range. These filters can use different expressions such as; and/or/not, integers, values, and flags to determine the protocol that links together in a string like fashion. The way a protocol works is a conversation going back and forth from an event or log within the network. An investigator can review the entire protocol and verify the information that is being sent and the understand the conversation that the network had with the device. For example, when a person searches a website it requests information from that location to be displayed on your screen. The network sends packets back and forth on the network to display the image or the website. Collecting the two different IP addresses can be calculated with a string using an expression and can data specific information on that web address. The conversation then can be analyzed to make sure that everything was validated and no interference of interception. Choosing the right filtration can and expressions will make the investigation run more smoothly.

 Another feature to look at more closely is the colorization filter within Wireshark, this can help separate and look at protocols more effectively and efficiently. The color code feature will allow the investigator to color code different data and be assigned to different addresses. For an example if you are working on a DHCP network an investigator or IT Technician can assign specific IP’s that are connected to each their own color, this can help determine any unknown IP addresses that they are connected too and make them easily more identifiable. You can also assign the DNS, TCP, ARP their own colors as well, to easily identify the category and what type of evidence that can be collected and analyzed. With added features like the colorization filter can help you learn and categorize the evidence properly. (scribd).

 As an investigator Wireshark is one of the best forensic tools that is being used today for investigations on the network. The best part is that it is a free tool that is used for forensics and live acquisitions. The best way to learn Wireshark is to go through the Wireshark Users Guide to learn more advanced and Expert techniques. Remember when retrieving and collecting the evidence that it is encrypted using a standard SHA-1 or MD5 encryption. All investigations start with the Network and learning your own system and how it talks to other devices can help protect, analyze, and collect evidence when needed.

**References**

Ndatinya, V., Xiao, Z., Manepalli, V. R., Meng, K., & Xiao, Y. (2017, February 15). Network forensics analysis using Wireshark. In *Research Gate*. Retrieved from [file:///C:/Users/amy\_h/AppData/Local/Temp/MicrosoftEdgeDownloads/d6ee0a38-ab87-4f52-9ade-b8ad83696ef1/IJSN\_2015\_Wireshark.pdf](file:///C%3A/Users/amy_h/AppData/Local/Temp/MicrosoftEdgeDownloads/d6ee0a38-ab87-4f52-9ade-b8ad83696ef1/IJSN_2015_Wireshark.pdf).

PHILLIPS, A. (2020, July 2). How to run a remote packet capture with Wireshark and tcpdump. In *comparitech*. Retrieved from <https://www.comparitech.com/net-admin/tcpdump-capture-wireshark/#Using_command-line_options_for_tcpdump>.

Schoenfelder, N. (2020). What are the differences between TCP, UDP, and ICMP packet types?. In *PingPlotter*. Retrieved from <https://www.pingplotter.com/wisdom/article/packet-type-differences#:~:text=What%20are%20the%20differences%20between%20TCP%2C%20UDP%2C%20and,and%20UDP.%204%20Packet%20up%2C%20packet%20in.%20>.

scribd. (n.d.). Version 3.5.0. In *Wireshark User’s Guide*. Retrieved from <https://www.wireshark.org/docs/wsug_html_chunked/>.

Tcpdump (2020). In *techopedia*. Retrieved from <https://www.techopedia.com/definition/16162/tcpdump>.

WinDump (2018). In *Riverbed Technology*. Retrieved from <https://www.winpcap.org/windump/>.