Assignment Title: Final Paper

Wireshark and Network Miner

by

Jason Rodriguez

Jason.rodriguez01@mymail.champlain.edu

By submitting this assignment I acknowledge that I have read and agree to abide by the Champlain College Academic Honesty Policy. I declare that all work within this assignment is my own or appropriately attributed. I accept that failure to follow the academic honesty policy may result in a failure grade, or expulsion from Champlain College.

Date Due: Dec 13,2019

Date Submitted: Dec 13, 2019

The purpose of network analyzing is to know how a network behaves, but more importantly security reasons. Having the ability to review your packet captures can provide a baseline for a network. The two Network analyzers discussed in this paper are Wireshark and Network Miner.

The packet analysis is a pcap file which is associated with Wireshark program. The file has the packet data of a network.

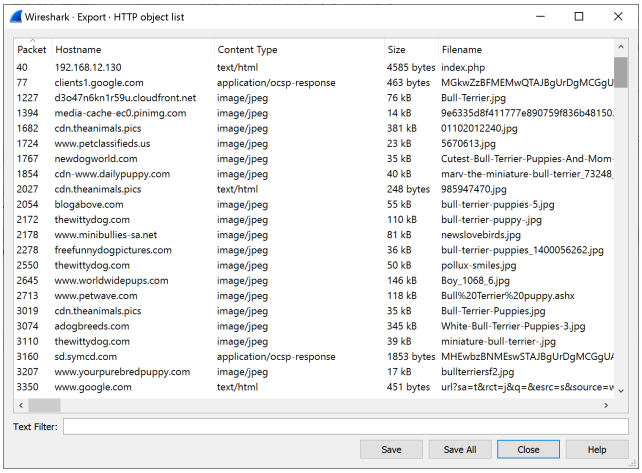
The computer that analyzes the pcap file is running Windows 10 pro v. 1909. The software utilize was Wireshark v.3.0.7 and Network Miner v. 2.5.0

The evidence found in the pcap was a variety of websites visited, images downloaded, username, password, and files. The browser used for the online activity was firefox.

Images

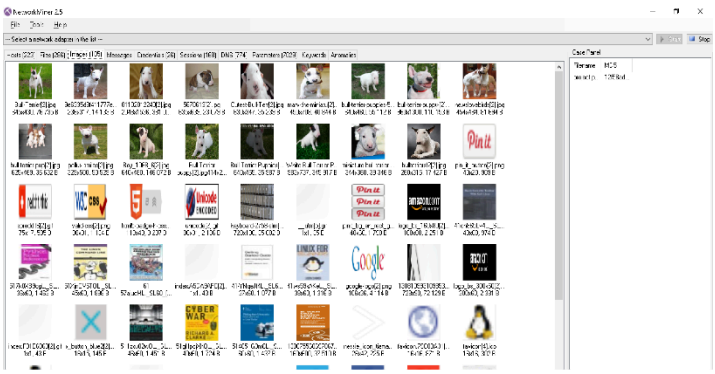
The images found on the file were mostly dog images. Both programs had differences in the way it displayed images on its program. For Wireshark the downside is that you need to save the images in order to display them compared to Network Miner which provides a tab for just images and all of them are displayed.

Fig 1.1 Wireshark



Images/jpeg found in Wireshark.

Fig 1.2 Network miner

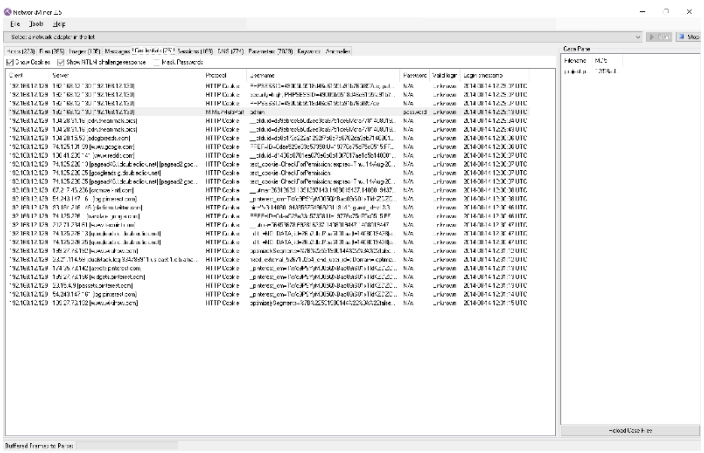


Websites

The websites visited using firefox where:

- Google search for animal pics
- Pinterest.com
- Reddit.com
- Adogbreeds.com
- Tecmint.com

Fig 2.1 Network Miner



Usernames & Passwords

The username and password found on both programs were fairly simple. The reason why the username and password was retrieved was because it wasn't encrypted. Username found was "admin, and password found was "password

Fig 3.1 Wireshark

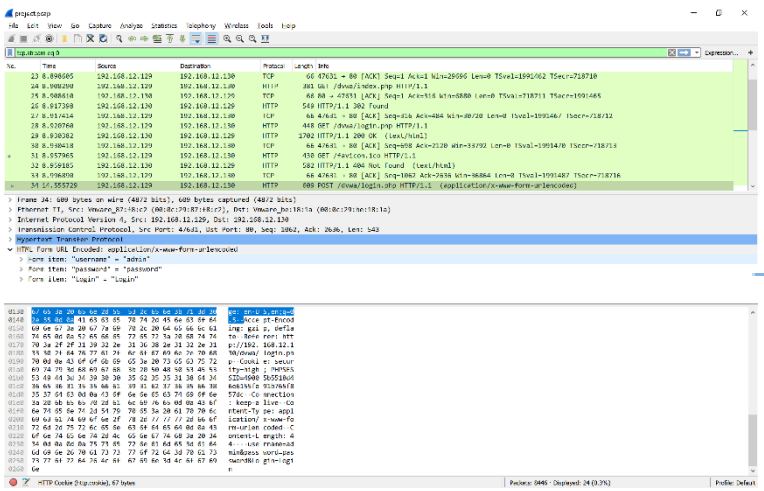
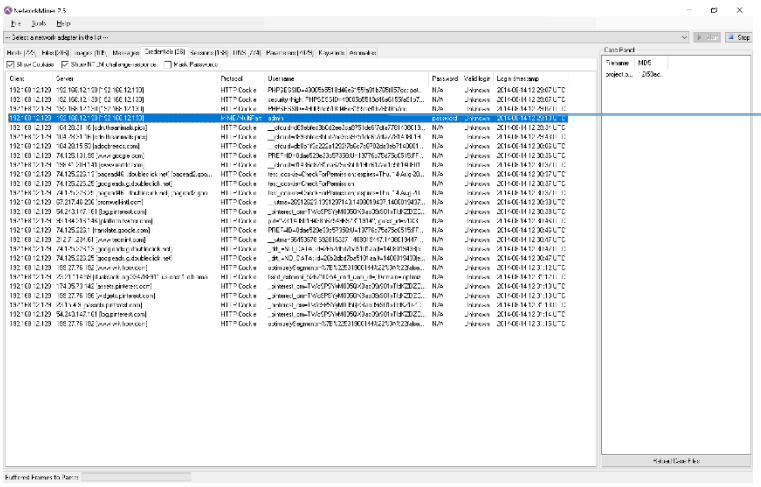


Fig 3.2 Network Miner



Files

The files that were retrieved from both programs was a combination of cookies retrieved from websites visited or images searched. Both programs handle the files found the same. The files found on with program displayed the same information such as size of the file and name of the file

Fig 4.1 Wireshark

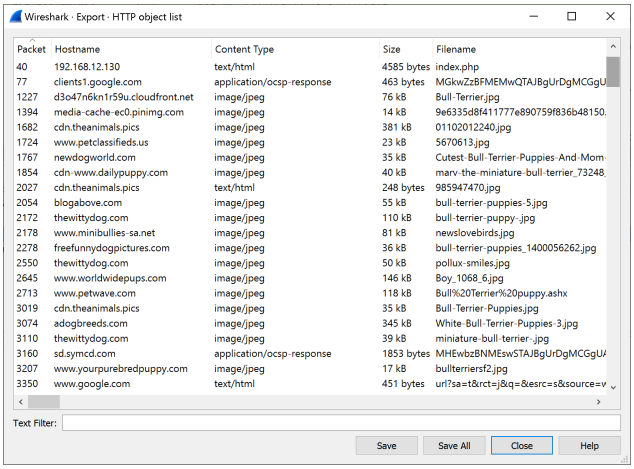
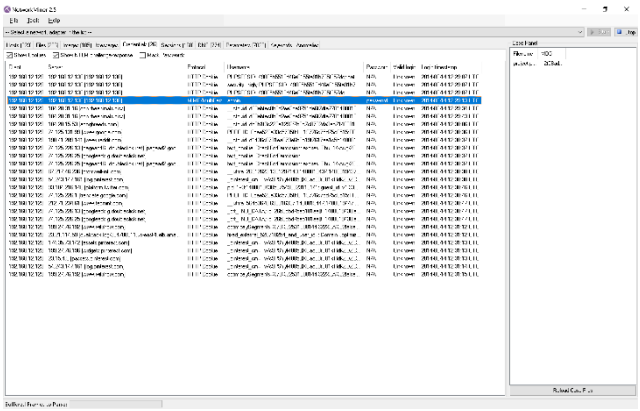


Fig 4.2 Network Miner



When comparing the results of both programs the output is the same. The major difference between both programs is that Wireshark is not as user-friendly as network miner. In order to display usernames, passwords or files you need to filter out your results and follow a specific stream. Compare that to Network miner in which is simply by switching tabs. As far as which one I preferred I would have to lean to Network miner for the simplicity of the program. Easy tabs give a non-technical person the ability to understand the program compared to Wireshark.

References

Guru99. (n.d.). Wireshark Tutorial: Network & Passwords Sniffer. Retrieved from https://www.guru99.com/wireshark-passwords-sniffer.html

Hassan, W. (2017, February 15). The Importance of Network Traffic Analysis. Retrieved from https://menaentrepreneur.org/2017/02/importance-network-traffic-analysis/

Hjelmvik, E. (n.d.). Passive Network Security Analysis with NetworkMiner | ForensicFocus.com. Retrieved from https://www.forensicfocus.com/passive-network-security-analysis-networkminer