



Assignment Title: Final Paper

Wireshark and Network Miner

by

Jason Rodriguez

Jason.rodriquez01@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.

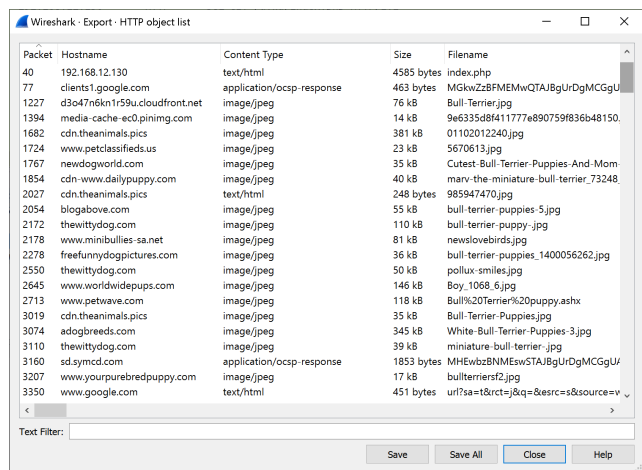
The computer that analyzes the pcap file is running Windows 10 pro v. 1909. The software utilize was Wireshark v.3.0.7 and Network Miner v. 2.5.0

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

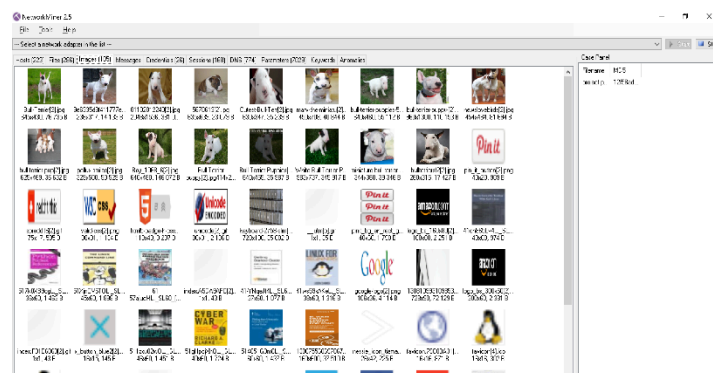
The images found on the file were mostly dog images. Both programs had differences in the way it displayed images on its program. For Wireshark the downside is that you need to save the images in order to display them compared to Network Miner which provides a tab for just images and all of them are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

[illegible]

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

The screenshot displays the Wireshark network protocol analyzer interface. The top menu bar includes File, Edit, View, Capture, Analyze, Statistics, Display, Windows, Tools, and Help. The toolbar contains icons for common actions like opening a file, saving, and capturing. The main window is divided into three panes:

- Packet List:** Shows a list of captured packets. The selected packet is #1, an HTTP GET request from 192.168.1.129 to 192.168.1.100.
- Packet Details:** Provides a hierarchical view of the selected packet's structure. It shows the Ethernet II frame, Internet Protocol Version 4, and the Hypertext Transfer Protocol (HTTP) request. The HTTP request details include the method (GET), the URL (/index.html), and various headers such as Host, User-Agent, and Accept.
- Packet Bytes:** Displays the raw data of the selected packet in hexadecimal and ASCII format.

The status bar at the bottom indicates the current packet is #1, and the display filter is set to 'HTTP GET'. The packet capture is running on the 'eth0' interface.

Fig 3.2 Network Miner

[illegible]

Username & Password displayed

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

Wireshark - Export - HTTP object list				
Packet	Hostname	Content Type	Size	Filename
40	192.168.12.130	text/html	4585 bytes	index.php
77	client1.google.com	application/ocsp-response	465 bytes	McGwZwZ8F6MEwQTAjBgUrgUdMcGGuU
1227	cs447n6n1r3bu.cloudfront.net	image/jpeg	76 kb	Bull-Terrier.jpg
1394	media-cache.ec0.pinimg.com	image/jpeg	14 kb	9w635z8f4f11777e890759836b48150.
1682	cdn.theinimals.pics	image/jpeg	381 kb	01102012240.jpg
1724	www.petclassified.us	image/jpeg	23 kb	5670613.jpg
1767	newdogworld.com	image/jpeg	35 kb	Cutest-Bull-Terrier-Puppies-And-Mom-
1854	cdn.www.dailypuppy.com	image/jpeg	40 kb	mary-the-miniature-bull-terrier-73248
2027	cdn.theinimals.pics	text/html	248 bytes	985947470.jpg
2054	blogabove.com	image/jpeg	55 kb	bull-terrier-puppies-5.jpg
2172	thewittydog.com	image/jpeg	110 kb	bull-terrier-puppy.jpg
2178	www.minibulldogs.sa.net	image/jpeg	81 kb	newslovebirds.jpg
2278	freefunnydogpictures.com	image/jpeg	36 kb	bull-terrier-puppies_1400056262.jpg
2550	thewittydog.com	image/jpeg	50 kb	polluxus1400056262.jpg
2645	www.worldwidepups.com	image/jpeg	146 kb	Boy_1068_5.jpg
2713	www.petwave.com	image/jpeg	118 kb	Bull%20Terrier%20puppy.ashx
3019	cdn.theinimals.pics	image/jpeg	35 kb	Bull-Terrier-Puppies.jpg
3474	adogbreeds.com	image/jpeg	345 kb	White-Bull-Terrier-Puppies-3.jpg
3510	thewittydog.com	image/jpeg	39 kb	miniature-bull-terrier.jpg
3160	sdsymcd.com	application/ocsp-response	1853 bytes	HEmWbzBNMEswSTAjBgUrgUdMcGGuU
3207	www.yourpurebredpuppy.com	image/jpeg	17 kb	bullterrierf2.jpg
3350	www.google.com	text/html	451 bytes	url?sa=t&src=1&q=&src=1&source=ve

[illegible]

Page 4 of 5

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>