Using Network Forensic Tools for Analysis and Investigation at Polytechnic University of Puerto Rico

Edgar A. Murray Ortiz
Master in Computer Science
Advisor: Dr. Jeffrey Duffany
Electrical and Computer Engineering & Computer Science Department
Polytechnic University of Puerto Rico

Abstract *— In the world of computer security. The security of networks has become a very important field. More importantly, the tools to provide security cannot guarantee a completely secure network. Is because of that situation that the network forensic field is growing tremendously. If the expectancy of a breach on network, has increased over the years, network forensic examiners need to investigate and analyze traffic. Knowing that there will be a network completely secure, there has to be a change in the state of mind for a more investigative mind oriented and it is with the help forensic tools that investigation and analysis can be done. With the help of these tools, detailed information about what is going in and out of the network, can be analyzed. The explanation of the use of these tools is key for people to understand how to use them and maximize their use.*

Key Terms *— Forensic Tools, Network Forensic, Packet Sniffer, Privacy.*

INTRODUCTION

The field of network forensic has grown tremendously in the last few years. This is because the number of incidents have increased dramatically. It is not that prevention has failed when it comes to network security. It is that there is no way to have a completely secure network. For this there are intrusion detection systems in addition to the intrusion prevention systems. That's why network forensic examiners investigate with the help of tools that will help answer important questions after an intrusion incident. This raises the topic of expectancy of privacy on public or corporate networks. Because in the corporate world employees have no expectancy of privacy every time they use one of the computers of the company. On the other hand, there is no control of the security in the public Wi-Fi and it is difficult to know if someone is gathering the traffic or if a computer is compromised with malware and is sending information without user consent. For these reasons the use of forensic tools like Wireshark and Network Miner is important for network investigation. These forensic tools can help investigate incidents on the criminal level and at the corporate level. These tools can be used for other purposes, but the focus will be on the explanation of these tools for security purposes summarizing two exercises that were made on Wireshark and Network Miner.

EXPECTANCY OF PRIVACY

In the corporate world, the use of non-disclosure agreements is used to protect companies from sensitive information been leaked out or to make sure employees comply with the proper use of the corporate network. Employees know that they don't have an expectancy of privacy and that the computer they used are been monitored. That is why in the two exercises it is explained that employees have no expectancy of privacy. Because we are simulating real world scenarios. Situations like in [1] when an employee is cought using the network to download pirate content can be investigasted and resolved, but not always the user knows that he does not have any expectancy of privacy. In [2] the author explains how users tend to forget they have public folder shared thru the hotel WiFi. Manny times he has connected he have been able to see other's people computer. The problem is that people do not know they are sharing their pulic profile so they do have an expectancy of privacy, but it is not there.

Another situation is the one discribed in [3], when a caraless politician from the Syrian government left the computer alone on the hotel room in London with very sensitve information. The

israli inteligence team installed a Trojan Horse which is a type of malware that collected information that was sent thru the network to the israeli government. This without the syrian politician or the goverment knowing. That gave the Israel government the access to pictures of a nuclear reactor that was in construction in Syria. The Israel government destroyed the construction with an airstike that was done in time thanks to the information they obtained from the Trojan Horse. We can conclude that the expectancy of privacy it is not always present and that not always the parties involve know what scenario they are facing. Other's forget the fact that they are been moitored and do careless things like the one discussed in [1] as mentioned before.

PROBLEM

Security is one of the most important topic in the internet and networking today. The amount of attention to security have increased tremendously over the past few years. Despite new technology has come out and new standards, and procedure have been developed, there is no network that can be completely secure. As mentioned in [4], security breaches are inevitable. Companies suffer sporadic or constant compromise. In the other hand, companies also suffer from insiders that leak information or open the door for intruders to make the breach more easily. To resolve this, they way intrusion is looked at, must change.

INVESTIGATION

Intruders do not breach in to a place in three minutes as mentioned in [4]. They take time, they enter a system several times and for several months. This gives the time for an investigation to be carried out and to take the proper measures. On the other hand, a leaked information from a company will not occur overnight. Here, there will be time to investigate. Even after the incident network traffic can be analyzed and investigated to prevent more leakage from happening. For this purpose, there are tools for network forensic investigations that collect traffic on the network.

PACKET SNIFFERS

These tools also called packet analyzers, intercepts and logs network packets as stated in [5].

Wireshark was one of the two tools used for practice exsercies.It is a free software that can be used for forensics investigsations.

To simulate a network forensic investigation and to show the capabilities of Wireshark, a sample captured file was open using the tool. A breaf explanation of the main menu was explained and the different parts of Wireshark. As shown in Figure – 1.

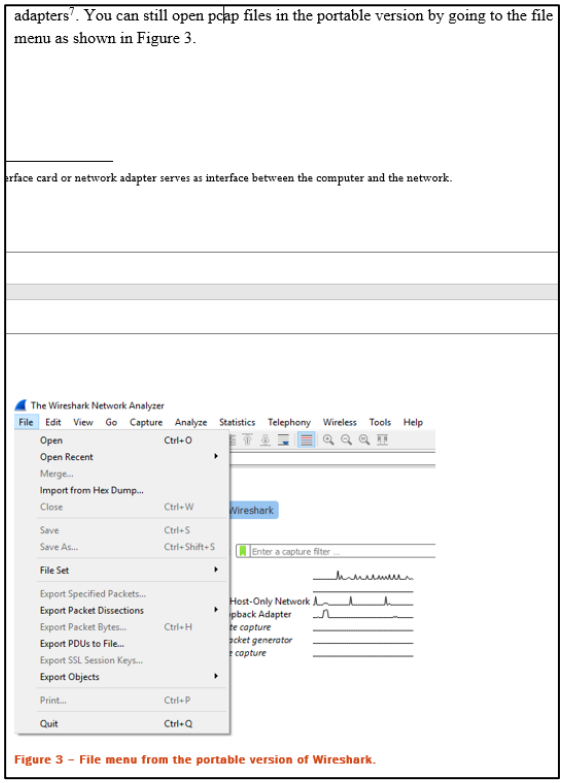


Figure 1
Sample of the Explanation of the Menu in the Exercise using Wireshark

The exersice focus was to be able to find pictures in the trafic using filters to narrow the search for a specific traffic as sown in Figure – 2.

This packet analyzers use some kind of software that collect the traffic named WinPcap. As described in [6], WinpCap is an open source library for packet

capture. In order for softwares like Wireshark collect the traffic, they need this type of software. In the case of the instalation of Wireshark. It will also install WinPcap.

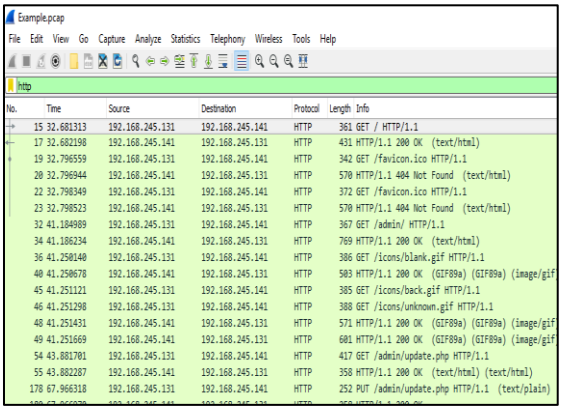


Figure 2
File Opened in Wireshark with Http Traffic Filter

After that the examiner could export and open the file to see what was in the picture as shown in Figure – 3 .

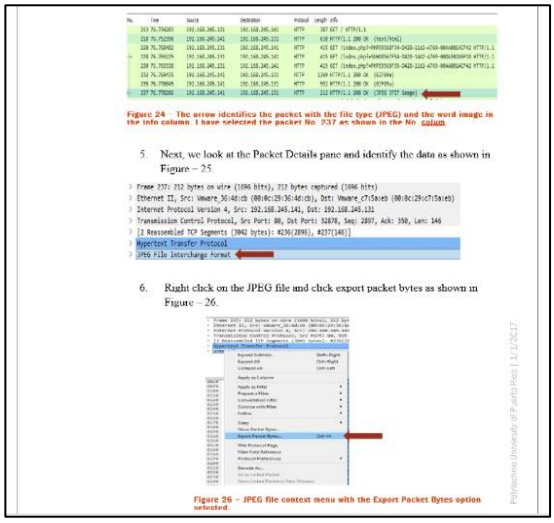


Figure 3
Sample of the Exercise done to Export a Picture in Wireshark

After the explanation on how to use Wireshark to filter http traffic and export a picture, the final part of the exercise was composed of questions to simulate a scenario where a real situation was happening. The examiner had to open a captured file that was provided and make an analysis to answer que questions as shown in Figure – 4.

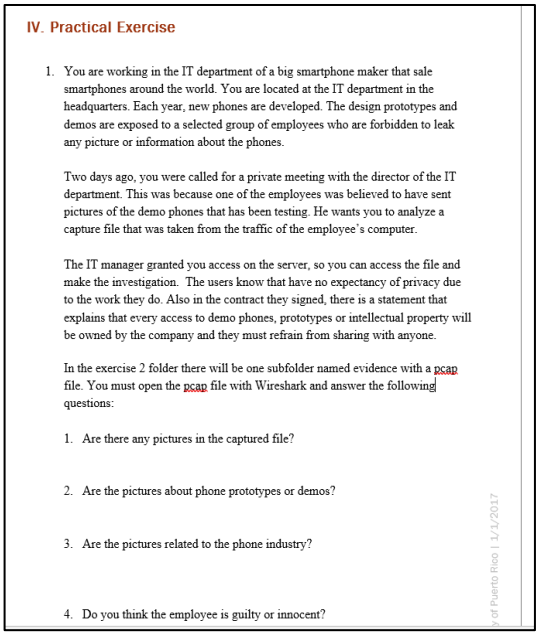


Figure 4
Sample of the Scenario Presented to the Examiner with Questions

A mobile company believed one of their employees was filtering information about a new phone prototype. The examiner was given the task to examine a captured file and to answer some questions.

This exercise shows small portion of the power of Wireshark. This tool can be used to analyze malware and intrusion patterns, to learn how they behave. It will also help to track were the connection is initiated so the intruder can be referred to the proper authorities in case of a crime.

A company also, will want to know if someone is stealing information to close the door and stop the leakage.

It is important to understand that many cases can start as a corporate and civil investigation but could change to a criminal investigation if the examiner fins criminal violations and the company refers them to the police.

Some companies refrain from referring criminal cases to authorities because they will have to admit that their network have been breached and they are more worried about the loss of money and clients due to the bad publicity.

The other tool used was Network Miner as shown in Figure – 5.

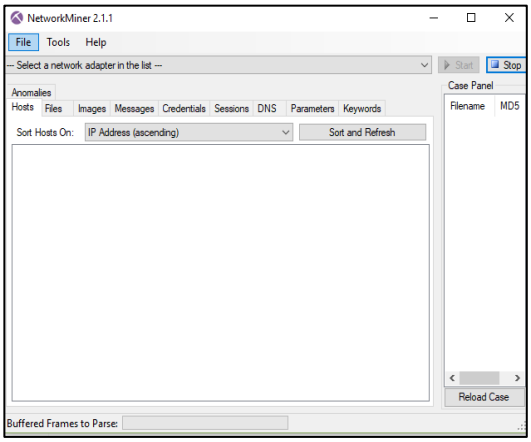


Figure 5
Network Miner Main GUI

Network Miner collects information about hots in the network. The difference between Network Miner and Wireshark is that Network Miner classifies the information as show in Figure – 6.

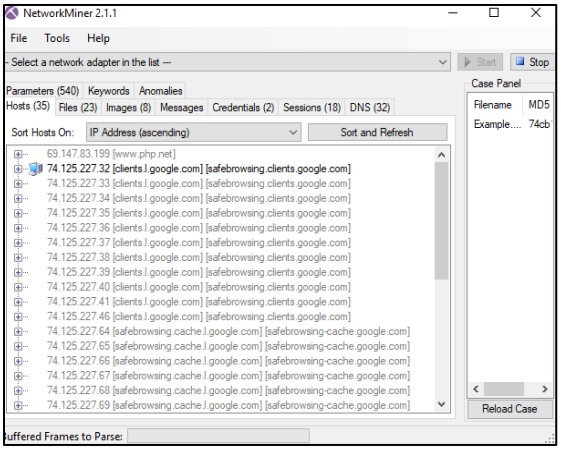
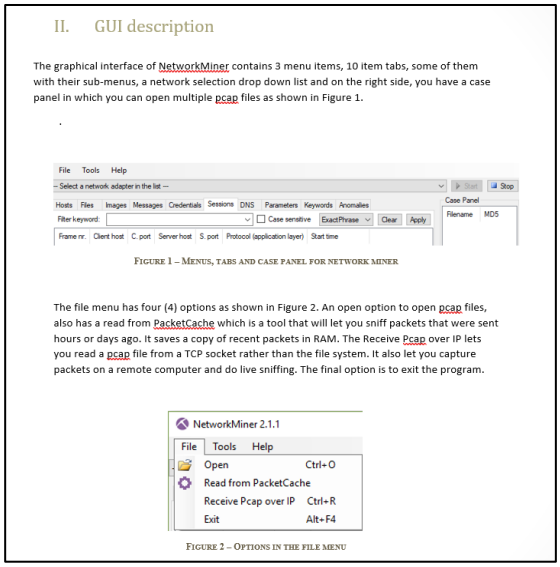


Figure 6
Traffic Classified in Different Tabs in Network Miner

Another difference is that it can open and work with multiple files at the same time in Network Miner. Also, as stated in [7], Network Miner with a feature called Pcap-over-IP can capture network traffic from a remote PC or device. This traffic collection to a remote computer can be encrypted with SSL for security.

The exercise started with a description of the tool and an explanation of the GUI as show in Figure – 7.


II. GUI description

The graphical interface of NetworkMiner contains 3 menu items, 10 item tabs, some of them with their sub-menus, a network selection drop down list and on the right side, you have a case panel in which you can open multiple pcap files as shown in Figure 1.

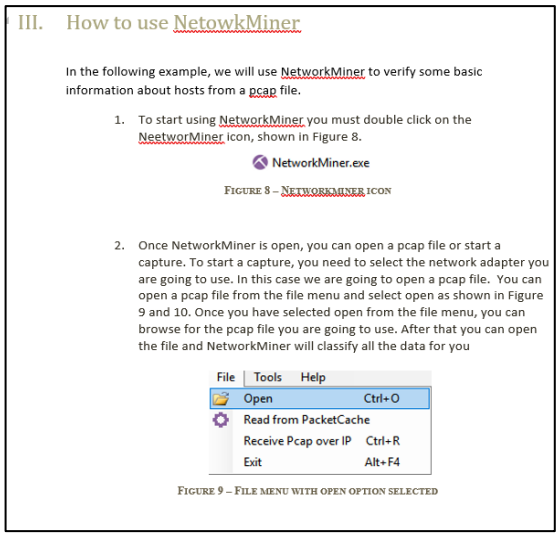
FIGURE 1 – MENUS, TABS AND CASE PANEL FOR NETWORK MINER

The file menu has four (4) options as shown in Figure 2. An open option to open pcap files, also has a read from PacketCache which is a tool that will let you sniff packets that were sent hours or days ago. It saves a copy of recent packets in RAM. The Receive Pcap over IP lets you read a pcap file from a TCP socket rather than the file system. It also let you capture packets on a remote computer and do live sniffing. The final option is to exit the program.

FIGURE 2 – OPTIONS IN THE FILE MENU

Figure 7
Explanation of the Network Miner GUI

Next comes a practical example on how to use Network Miner as shown in Figure – 8.


III. How to use NetowkMiner

In the following example, we will use NetworkMiner to verify some basic information about hosts from a pcap file.

1. To start using NetworkMiner you must double click on the NeetworMiner icon, shown in Figure 8.

NetworkMiner.exe

FIGURE 8 – NETWORKMINER ICON

2. Once NetworkMiner is open, you can open a pcap file or start a capture. To start a capture, you need to select the network adapter you are going to use. In this case we are going to open a pcap file. You can open a pcap file from the file menu and select open as shown in Figure 9 and 10. Once you have selected open from the file menu, you can browse for the pcap file you are going to use. After that you can open the file and NetworkMiner will classify all the data for you

FIGURE 9 – FILE MENU WITH OPEN OPTION SELECTED

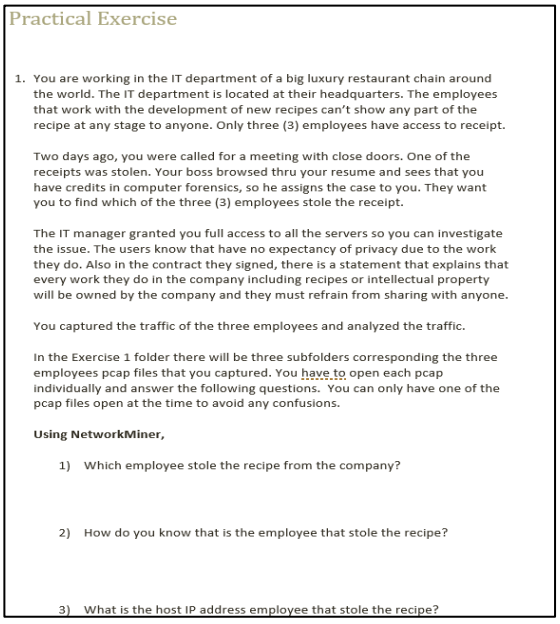
Figure 8
Practical Example on How to Use Network Miner

Network Miner will show metadata about the capture, so the examiner will know at what time the capture started and at what time it ended. Also, it will have the information about the operating system a host is using. This will help the examiner understand what type of operating system the intruder was using.

The last part was a practical exercise where the examiner was pretended to work at famous luxury

restaurant chain were one of the new recipes was stolen. The IT manager assigned the case to an examiner to investigate the employees that had access to the recipes and answer the questions as Figure – 9 shows.

The exercise also, explained how to identify the message that was sent during the period the captured was been made. Another tab will show the images that were collected, and it will show which host was the one sending and receiving the image. While Network Miner do collect messages that were sent from e-mail and received. This feature will work on unencrypted messages. The problem is that almost all major e-mail brands like Hotmail and Google, encrypt the e-mail traffic. In this case Network Miner will not be able to sort the message in the messages tab.



Practical Exercise

1. You are working in the IT department of a big luxury restaurant chain around the world. The IT department is located at their headquarters. The employees that work with the development of new recipes can't show any part of the recipe at any stage to anyone. Only three (3) employees have access to receipt.

   Two days ago, you were called for a meeting with close doors. One of the receipts was stolen. Your boss browsed thru your resume and sees that you have credits in computer forensics, so he assigns the case to you. They want you to find which of the three (3) employees stole the receipt.

   The IT manager granted you full access to all the servers so you can investigate the issue. The users know that have no expectancy of privacy due to the work they do. Also in the contract they signed, there is a statement that explains that every work they do in the company including recipes or intellectual property will be owned by the company and they must refrain from sharing with anyone.

   You captured the traffic of the three employees and analyzed the traffic.

   In the Exercise 1 folder there will be three subfolders corresponding the three employees pcap files that you captured. You have to open each pcap individually and answer the following questions. You can only have one of the pcap files open at the time to avoid any confusions.

   Using NetworkMiner,

   1) Which employee stole the recipe from the company?

   2) How do you know that is the employee that stole the recipe?

   3) What is the host IP address employee that stole the recipe?

Figure 9
Screen Capture of the Last which is a Practical Exercise

Although Network Miner classifies traffic and it is better for finding pictures and messages because they have their own tab, Wireshark in the other hand gives more detailed information about the traffic. The decision of which tool will be used will depend on the work the examiner is going to be doing. Another thing that Wireshark has, is the ability to register keys for decryption. In case que traffic that is going to be collected is encrypted. The examiner has the possibility to put the key if the traffic is local and he has access to the decryption key. This will decrypt the traffic and can be exported for later analysis on a computer that does not has the key.

CONCLUSION

Network security equipment's like intrusion detection systems are not perfect. As stated in [4] attackers adopt over time more sophisticated tactics. It is difficult for organizations to keep up with the evolution of the attacks. There is no network that can guarantee security in all aspects.

What has been tried to achieve in security is to make things more difficult, to try to deterrent intruders. Also, another thing has developed is the investigation.

The network forensic field has the task to investigate incidents that will bring consequences. Is with the network forensic tools that investigations can be done efficiently and intruders can be submitted to justice.

As the tools are very important, it is very important to know how to use them and to understand the variety of tools available to conduct investigations. This was the purpose of the conducted exercise that were explained in this paper.

The ability to know the tools and to use them more efficiently will produce better results on the investigations.

As the attackers will evolve to more sophisticated attacks and try to cover the track. More sophisticated tools will be created and the ones that are used today will be updated with more capacity to still be able to investigate and analyze traffic to make an assessment.

ACKNOWLEDGMENTS

I would like to acknowledge Dr. Jeffrey Duffany for his contribution of ideas, mentorship and guidance throughout the project and the master degree. Also, I would like to thanks Dr. Alfredo Cruz for guidance provided in different courses.

REFERENCES

[1] S. Davidoff and J. Ham, "Network Forensics," in *Tracking Hackers Through Cyberspace*, Massachusetts, Pearson Education, 2012, pp. 7-9.

[2] G. A. Donabue, "Network Warrior," in *Sebastopol*, O'Reilly Media, Inc., 2011, pp. 513.

[3] E. Follath and H. Stark. (2009, November 2). *The Story of 'Operation Orchard': How Israel Destroyed Syria's Al Kibar Nuclear Reactor* [Online]. Available: http://www.spiegel.de/international/world/the-story-of-operation-orchard-how-israel-destroyed-syria-s-al-kibar-nuclear-reactor-a-658663.html.

[4] R. Bejtlich, "The Practice of Network Security and Monitoring," in *Understanding Incident Detection and Response*, San Francisco, No Starch Press, 2013, pp. 5.

[5] M. Meyers, "Network+ Exam N10-005," McGraw-Hill Companies, 2012, pp. 668.

[6] The WinPcap. (2009). *WinPcap* [Online]. Available: https://www.winpcap.org/docs/docs_412/html/main.html.

[7] E. Hjelmvik. (2011, September 7). *Pcap-over-IP in NetworkMiner* [Online]. Available: http://netres.ec/?b=119B126.