Using Wireshark in a Medical Office

Luis A. Pesquera Marrero
Master in Computer Science
Jeffrey Duffany, Ph.D.
Electrical & Computer Engineering and Computer Science Department
Polytechnic University of Puerto Rico

Abstract *—This project is about sniffing the packets in a secured network with electronic health record (EHR) while using Wireshark. I suspect that the packets and the network are going to be encrypted and it won't be possible to sniff them and read their contents. Statistics will be formed based on the findings that state how many packets are sent in a network in each capture of Wireshark.*

Key Terms *—EHR, LLMNR, SQL, Wireshark.*

INTRODUCTION

Recently, doctors that have been in the profession for 30 years are required to adopt new ways to organize their patient information through EHR. This change has caused confusion among those in the medical field on which programs to use that support EHR but also fail to realize they need a software that monitors networks. We want to find out if EHR is secure for hackers that gain access to the network and try to sniff packets using Wireshark. This is important because the information in the EHR is confidential due to HIPPA regulations and everyone that has the EHR can be vulnerable to have their information stolen by a hacker. Wireshark was chosen for this analysis because it's an open source software that everyone can learn and use for monitoring a network. Wireshark can sniff the packets and the packets never lie. This is helpful because we can see the packets and analyze the packets being sent to every computer in the network that the doctor has access to.

RESEARCH

Wire shark is a useful program when it comes to monitoring network for security and performance issues [1]. Wireshark is able to collect data or packets that are sent or received over the network and decode them in a type of analysis that is helpful for the user to find particular information [2]. It is a helpful tool when making sure information is being sent securely and also to check if traffic is coming from an outside source. Wireshark has grown popular because it's an open source which is good for companies who don't have a high budget on protection software that would be used by the IT department. Since Wireshark is free, it is widely used by home consumers [3]. Wireshark can be used on various operating systems such as Windows, OS, and Linux. The fault that Wireshark might have does not lie in the program itself but the tech support available. Even though, most users can find the answers to their questions on forums or mailing lists, an IT pro at an enterprise would need a 1-800 number for immediate help but Wireshark does not have a direct number to contact [4]. However, the main website offers a Questions and Answers section that addresses most of the user's needs [5].

There are very few findings in regards to using Wireshark in a medical office. As part of my research I interviewed doctors and tested their knowledge of network security. I interviewed firstly a pediatrician who is new to EHR. I asked if she knew what were servers and terminals. She said she knew them by name but not what they did or their function. I also asked what the doctor knew about hackers. The doctor was under the notion that computers used in the office could only be hacked from the inside and not from an outside source. I asked if she knew the name of any programs capable to monitor the network but she admitted that she didn't know that any existed. Another pediatrician I interviewed admitted that she finds a hard time knowing the difference between virus protection and network protection. After talking to the pediatricians, I soon realized that many medical professionals have very little to no knowledge of network security. Doctors are growing more

concerned with running into the risk of having their patient files hacked and not knowing how to prevent it. Due to my findings and talking to doctors, I took it upon myself to test Wireshark in a medical office. The next section presents the steps I took in using Wireshark on a computer in a medical office [6].

METHODOLOGY

This project was done in a medical office that has a network composed of three computers and one server. First, the Wireshark program was downloaded from the website and it was installed in one of the computers as a terminal. Then on a normal workday where they used the EHR every time and there is traffic opening up their records, we started to do an image capture using Wireshark. Starting a capture is a matter of simply of clicking the icon that shows a green circle, Clicking on the icon of the red square stops the capture. Wireshark's output consists of two panes: the top pane shows the packets while the bottom pane shows the details of the packets. When you start a Wireshark session, you can always save this file. This enables you to analyze the packets captured in more detail. The session of the capture that I used was about one minute. Using the saved capture file looking into the TCP. Putting in the filters, TCP will allow to highlight which connection is under the TCP protocol usually used in EHR.

Then, I looked for the TCP protocols to see which ones were encrypted and which were not. Wireshark can capture the images instantly as they are being captured from one computer to another.

Figure 1 shows the Link-Local Multicast Name Resolution (LLMNR) that is a protocol based on the Domain Name System packet format that allows IPv4 and IPv6 hosts to perform name resolution for hosts on the same local link. It is included in most Windows operating systems and because of this Wireshark showed us that the system protocol EHR is LLMNR. This allowed me to understand how the EHR was communicated and once I learned that it was using LLMNR. I also learned that it was using a standard query. Now I proceed to study the contents of this communication protocol.

I could see which computer was interacting between each other and I could see the name of the computer and the packets it was sending and the name length and the table count. Figure 2 shows the LLMNR packets of a Desktop Terminal. Figure 3 is the continuation of Figure 2.

RESULTS

After running Wireshark on the pediatrician's office computer, it was obvious that there was a lot of traffic especially in one workday. Figure 4 presents detailed capture of LLMNR. Figure 5 shows the LLMNR packets of a laptop terminal. Figure 6 is a continuation of Figure 5. Figure 7 shows a UDP Connection. Figure 8 and Figure 9 shows a screen capture of wpad. Wireshark gives you a summary analysis of the capture. An example of a summary analysis is show in Figure 10 and Figure 11, which states that there were 1174, captures. All of them could be displayed. The seconds between the first packet and the last packet were 75.864 seconds. Also, the average packet per second capture was 15.475 and the average packet size was 628 bytes. The computer was connected to the Internet via Ethernet. Figure 12 shows information about an LLMNR Standard query packet requesting all the requests for all the records the server has available. This clearly tells us that we can see the terminal asking the server for the records and which one we can determine is the server and also the name length and label count aside from all the port and the IP addresses.

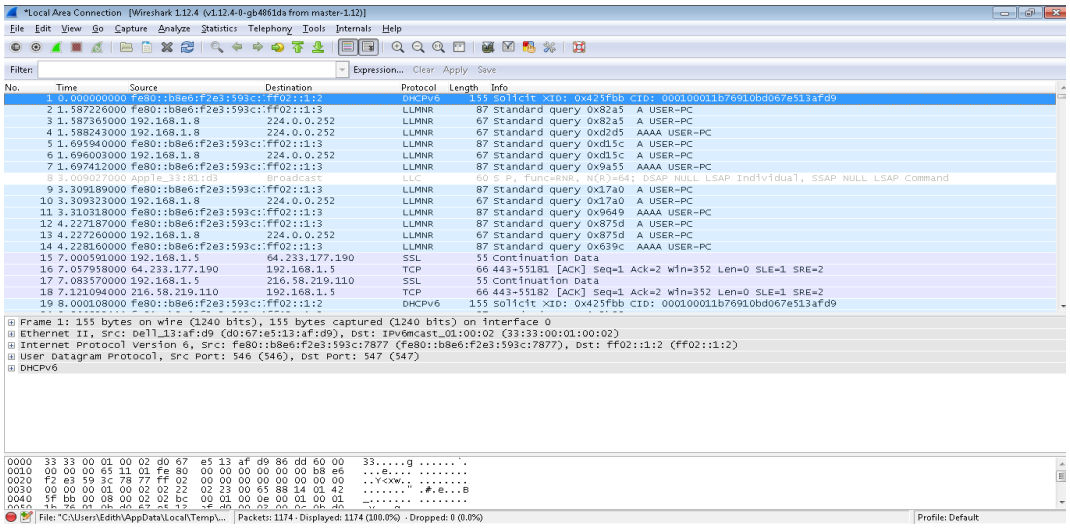

Figure 1

Wireshark LLMNAR Protocol

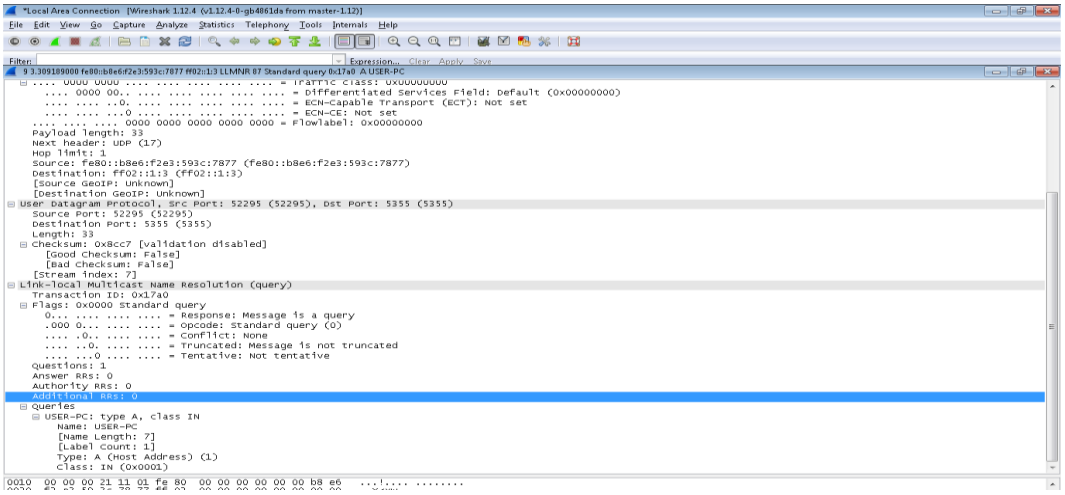

Figure 2

LLMNR Packets of a Desktop Terminal

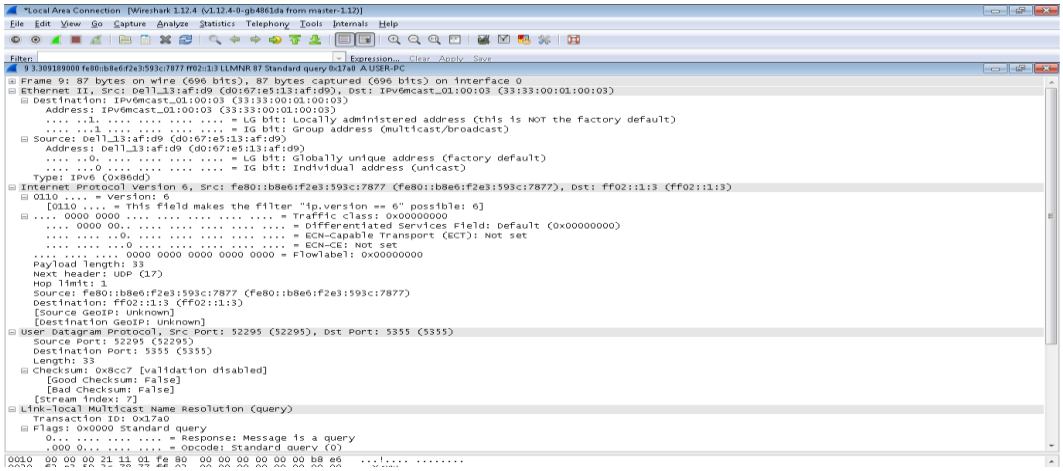

Figure 3

Continuation of LLMNR packets of a Desktop Terminal

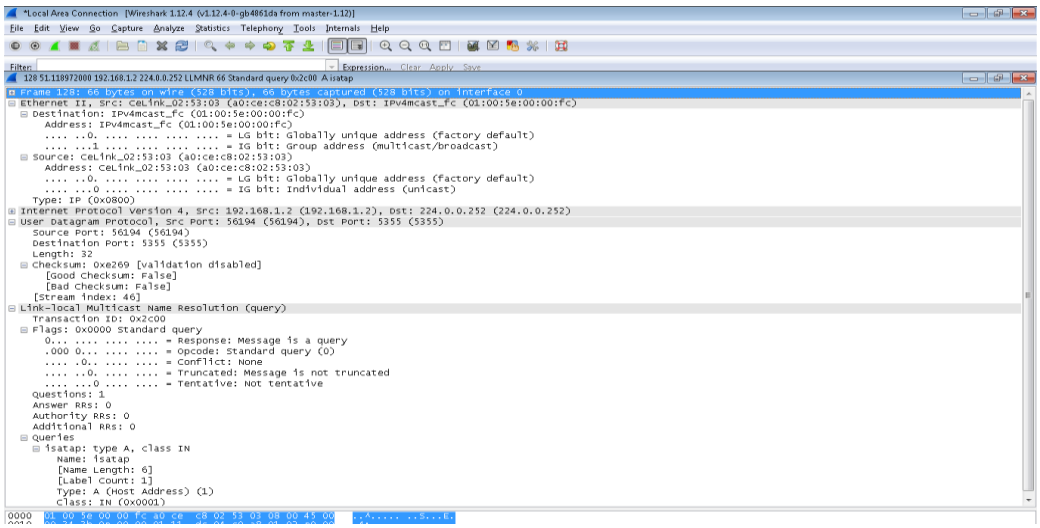

Figure 4

Detailed Capture of LLMNR

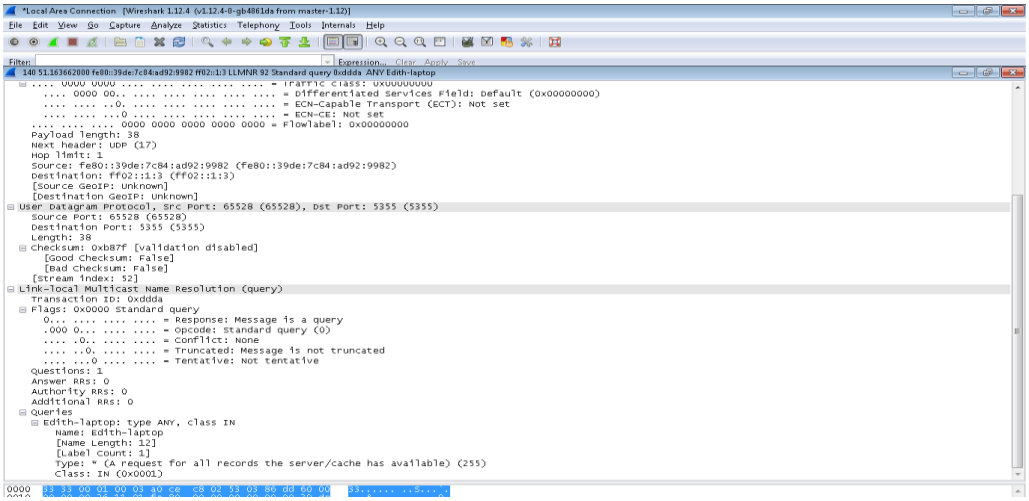

Figure 5

LLMNR Packets of a Laptop Terminal

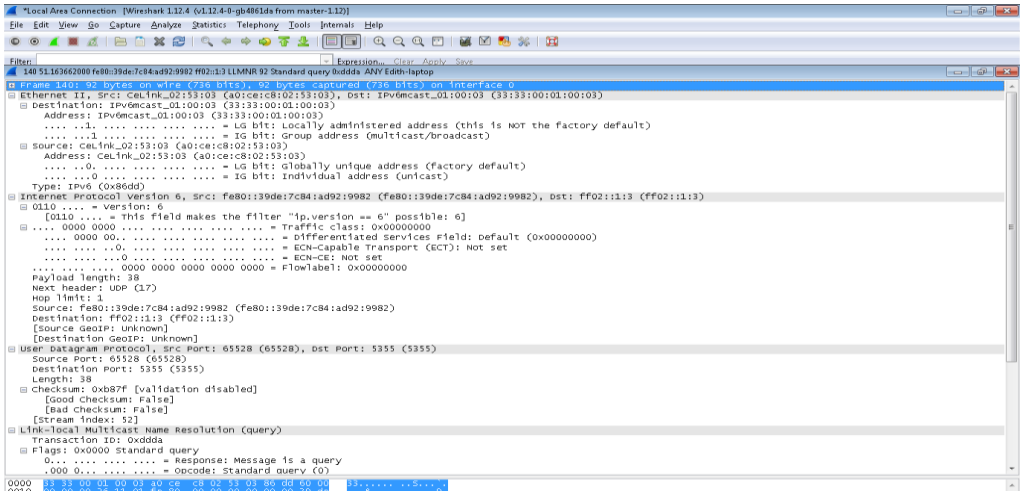

Figure 6

Continuation of LLMNR Packets of a Laptop Terminal

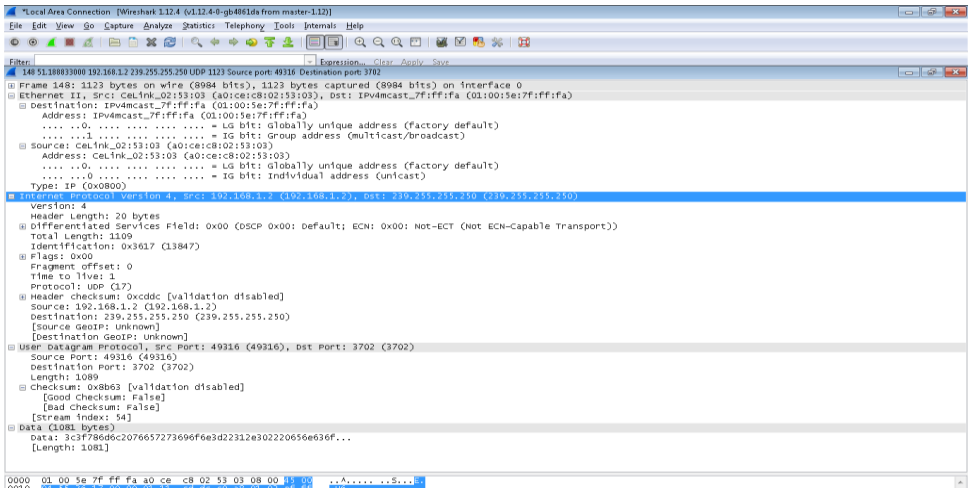

Figure 7

UDP Connection

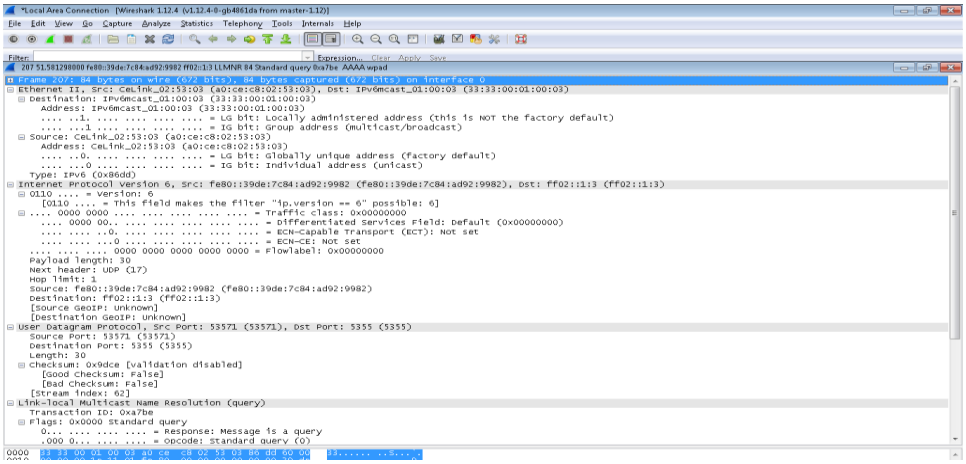

Figure 8

Capture of Wpad

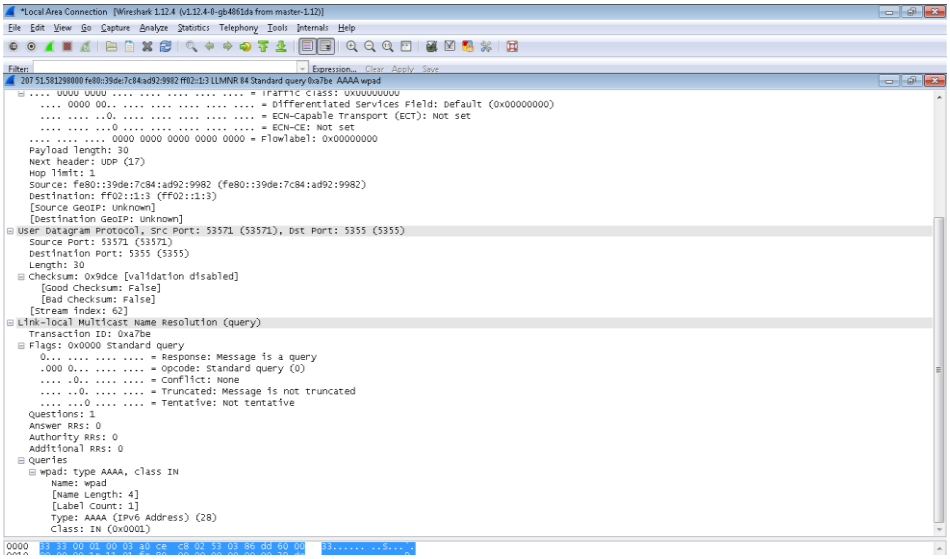

Figure 9

Continuation of Capture of Wpad

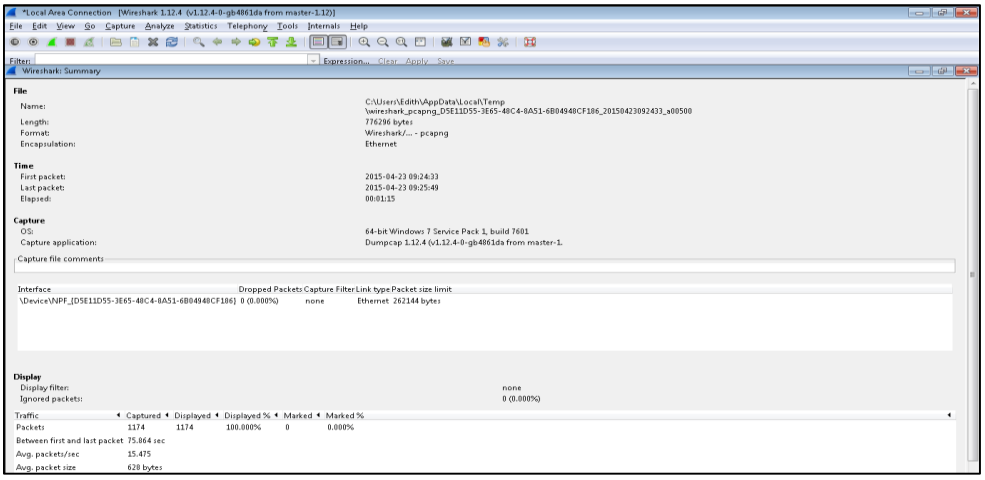

Figure 10

Summary Analysis of Capture

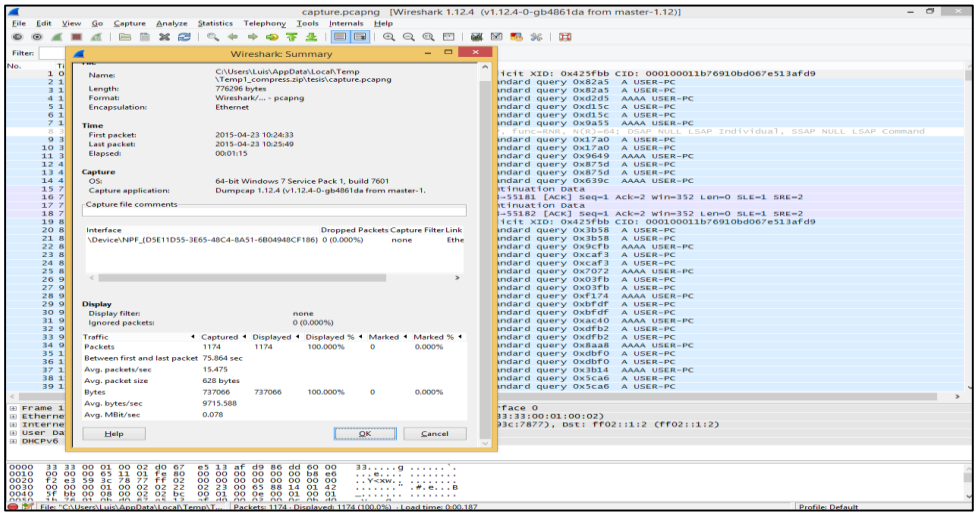

Figure 11

Summary Analysis of Capture

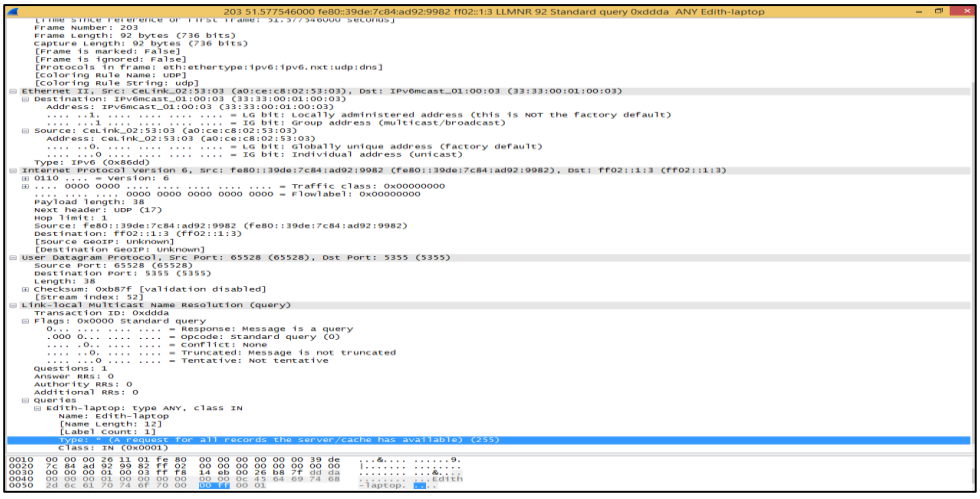

Figure 12

LLMNR Standard Query Packet

DISCUSSION

In order to improve the security in the office network, a risk assessment needs to be done. The steps for risk assessment is the following: scope the assessment, gather information, identify realistic threats, identify potential vulnerabilities, assess current security controls, determine the likelihood and impact, determine the level of risk, recommend security controls, and document the risk assessment results.

Firstly, one needs to decide if scoping the assessment should cover physical, network, application, database, personnel, policy and/or wireless assets as well as the scale of the work and the number if IP addresses [7].

Then gathering information of technical and non-technical such as network maps detailing internal and external connectivity; hardware and software configurations; and policies, standards, and procedures for the operation, maintenance, upgrading and monitoring of technical systems [8].

In order to identify realistic threats, one must identify what needs to be protected and what are the already known risks such as an attacker reading other user's messages, user, user may not have logged off on a shared PC, Data validation may allow SQL injection, implement data validation, authorization may fail, allowing unauthorized access, implement authorization checks, browser cache may contain contents of message, implement anti-caching directive in HTTP headers, and if eavesdropping risk is high, use SSL. It take a motivated attacker to exploit a threat. They generally want something from your application or to obviate controls [9].

Vulnerability is a weak spot in your network. Vulnerability assessment is a process that defines, identifies, and classifies the security holes (vulnerabilities) in a computer, network, or communications infrastructure. This type of analysis can forecast the effectiveness of propose countermeasures and evaluate their actual effectiveness. The steps consist of defining and classifying network of system recourses, assigning relative levels of importance to the resources, identifying threats to each resource, developing a strategy to deal with the most serious potential problems first, and defining and implementing ways to minimize the consequences if an attack occurs [10]-[11].

Security controls are safeguards to avoid, counteract or minimize security risk relating to personnel property or any company property. The different criteria: preventive controls, used to prevent and incident from occurring by locking out unauthorized intruders; detective controls, identify an incident in progress; and corrective controls, intended to limit the extent of any damage caused by an incident.

In order to determine the likelihood and impact, it is useful to use an impact/probability chart which helps one understand which risks to pay attention to. Probability is a risk in an event that may occue while impact refers to the size of the negative impact. Figure 13 shows that the bottom left is the lowest risk and the top right is the highest risk [12].

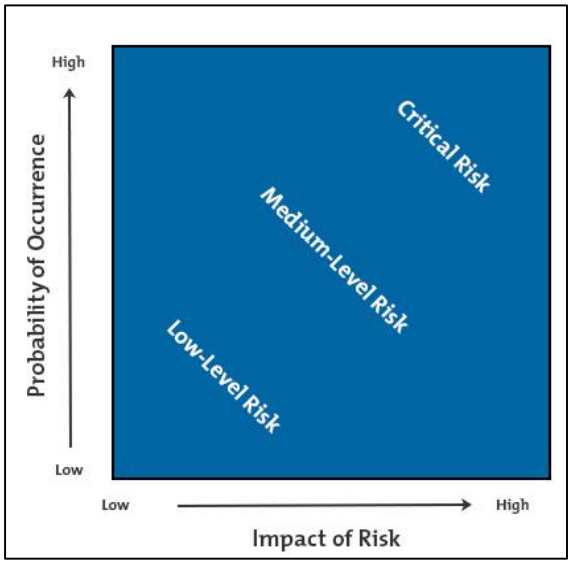

Figure 13
Impact/Probability Chart

The risk level is determined by the outset of a project. "Determining risk may not seem a straight forward enterprise, but often project documents already contain information about perceived risks for a project…In the case of technological risks or risks to the environment or health risks, you may

want to hire an expert in the field" [13]. A help of an expert can recommend security controls that can help minimize security.

Finally, documenting the risk assessment which includes the name and function of the person documenting the examination, the risks that were identified, the groups that face those risks, the necessary protection measures, details of subsequent monitoring and reviewing arrangements and details of the parties involved in the risk assessment process [14].

Another way of making the network secure is to implement an open source program called putty, is a free and open-source terminal emulator, serial console and network file transfer application. It supports several network protocols, including SCP, SSH, Telnet, rlogin, and raw socket connection. PuTTY supports many variations on the secure remote terminal, and provides user control over the SSH encryption key and protocol version, alternate ciphers such as 3DES, Arcfour, Blowfish, and DES, and Public-keyauthentication. As for the protocol of comunication the ehr should change from llmnr to a better secure protocol like **Secure Shell**, or **SSH**, is a cryptographic (encrypted) network protocol for initiating text-based shell sessions on remote machines in a secure way [15]-[16].

CONCLUSION

In this project I was able determine the protocol used to communicate EHR uses is LLMNR. I can say that the network is somewhat secure and somewhat encrypted because I was able to read and see which computer is the server and which computers are the terminals.

This information is useful because it gives you an idea on how to attack the server. Meanwhile, by looking at the ports you could find out what is the EHR program used in the office. At the same time, there is some kind of protection because you can't decipher by just sniffing the network. An example of this is that you can see the number of the letters of the person's name but you can't see the actual letters or the name of the person or the number of the records. Therefore the name is still unknown. An experienced hacker has the ability to find the name using other ways. Also, the encryption is not present in the communication between the server and the terminals. This communication should be encrypted since by sniffing the network could show any bit of information and it shouldn't since all the information is confidential.

This communication should be encryted because the act of sniffing the packets could reveal information that shouldn't be seen since infortaion is confidential.

REFERENCES

[1] J .Wallen. (2009) *Review: Wireshark Network Analyzer*. [Online]. Available: http://www.techrepublic.com.

[2] S. Morse (2014, September 18). *Wireshark 101: How To Wireshark*. [Online]. Available: http://www.youtube.com

[3] L. Chappell. *Top 10 Reasons To Learn Wireshark, The Open Source Network Analyzer* [Online]. Available: http://www.SearchNetworking.TechTarget.com

[4] S. Morse. (2012, August15). *How To Capture Packets With Wireshark - Getting Started*. [Online]. Available: http://www.youtube.com

[5] *Wireshark Frequently Asked Questions* [Online]. Available: http://www.wireshark.org.

[6] E. Marrero, *EHR Network Security,* 2015.

[7] (2008, May) *What Is The Scope Of The Assessment?* [Online]. Available: http://www.searchitchannel. techtarget.com.

[8] *FFIEC IT Examination Handbook Infobase-Gather Necessary Information* [Online]. Available: http://www.Ithandbook.ffiec.gov.

[9] *Threat & Risk Assessment* [Online] Available: http://www.pricelangevin.com.

[10] M. Rouse. (2006, March). *Vulnerability analysis (vulnerability assessment)* [Online]. Available: http://searchmarketsecurity.techtarget.com.

[11] *Identifying Vulnerabilities and Risks on your Network* [Online]. Available: http://www.techsoupforlibraries.org.

[12] *Risk Impact/Probability Chart* [Online]. Available: http://www.mindtools.com.

[13] *Determining the Level of Risk in a Project* [Online]. Available: http://www.brighthubpm.com.

[14] *Documenting the risk assessment* [Online]. Available: http://oshaeuropa.eu.

[15] *Download Putty- A free SSH and Telnet Client for Windows* [Online]. Available: http://www.putty.org.

[16] S. Tatham. (2015, April 20). *PuTTY: A Free Telnet/Ssh Client* [Online]. Available: http://www.chiark.greenend.org.uk.