CHAPTER 1: INTRODUCTION

INTRODUCTION

Packet capturing is a technique of monitoring every packet that crosses the network also known as packet sniffer. A packet sniffer is a piece of software or hardware that monitors all network traffic. This is unlike standard network hosts that only receive traffic sent specifically to them. The security threat presented by sniffers is their ability to capture all incoming and outgoing traffic, including clear-text passwords and usernames or other sensitive material. In theory, it is impossible to detect these sniffing tools because they are passive in nature, meaning that they only collect data. While they can be fully passive, some are not therefore they can be detected. Packet sniffer is a program running in a network attached device that passively receives all data link layer frames passing through the device's network adapter. It is also known as Network or Protocol Analyzer or Ethernet Sniffer. The packet sniffer captures the data that is addressed to other machines, saving it for later analysis. A network or system administrator to monitor and troubleshoot network traffic can use it legitimately.[1]

When a computer sends a data on the network it sends in the form of packets. These packets are the chunks of data are actually directed to the certain designated system. Actually, every sent data has a predefined receiving point. So, all the data are directly directed to a particular computer. Normally a system in a network is designed to receive and read only those data which are intended for it, the packet sniffing process involves a cooperative effort between software and hardware. Process can be explained down into three steps.

1. Packet sniffer collects raw binary data from the wired or wireless devices. Typically, this is done by switching the selected network interface into promiscuous mode

2. Captured binary data is converted into a readable form.

3. Analysis of the captured and converted data. The packet sniffer takes the captured network data, verifies its protocol based on the information extracted, and begins its analysis of that protocol's specific features [1]

There are different types of network sniffing tools depending on the network, application or protocols are available in markets. This paper considers the primary and most useful packet sniffer like wireshark, tcpdump, Network Miner, Soft Perfect Network Protocol Analyzer, Netflow Analyser,CAPSA etc. the packet sniffing tools can be used in the platforms like Linux, Windows and in iOS platforms.

Network forensics is capture, recording and analysis of network packets in order to determine the source of network security attacks. The major goal of network forensics is to collect evidence. It tries to analyze network traffic data, which is collected from different sites and different network equipment, such as firewalls and IDS. In addition, it monitors on the network to detect attacks and analyze the nature of attackers. Network forensics is also the process of detecting intrusion patterns, focusing on attacker activity.[7]

Wireshark is a packet analyzer. It is used for network troubleshooting, analysis. Originally named Ethereal, in May 2006 the project was renamed Wireshark due to trademark issues. Wireshark is cross-platform, using pcap to capture packets; it runs on various Unix-like operating systems and Solaris, and on Microsoft Windows. Wireshark allows the user to put the network interfaces that support promiscuous mode into that mode, in order to see all traffic visible on that interface, not just traffic addressed to one of the interface's configured addresses and broadcast/multicast traffic. However, when capturing with a packet analyzer in promiscuous mode on a port on a network switch, not all of the traffic travelling through the switch will necessarily be sent to the port on which the capture is being done, so capturing in promiscuous mode will not necessarily be sufficient to see all traffic on the network. [2]

Soft Perfect Network Protocol Analyzer is an advanced, professional tool for analyzing, debugging, maintaining and monitoring local networks and Internet connections. It captures the data passing through your dial-up connection or network Ethernet card, analyzes this data and then represents it in an easily readable form. Soft Perfect Network Protocol Analyzer is a useful tool for network administrators, security specialists, network application developers and anyone who needs a comprehensive picture of the traffic passing through their network connection or segment of a local area

network. Soft Perfect Network Protocol Analyzer presents the results of its network analysis in a convenient and easily understandable format. It also allows you to defrayments and reassembles network packets into streams. The program can easily analyze network traffic based on a Asrodia and Patel 57 number of different Internet protocols. Soft Perfect Network Protocol Analyzer also features a packet builder. This tool allows you to build your own custom network packets and send them into the network. You could use this packet builder feature to check your network for protection against attacks and intruders. Fig. 2 and 3 shows the result generated from this tool. But this tool only work for windows operating system [4][6]

Network Miner is an open source Network Forensic Analysis Tool (NFAT) for Windows (but also works in Linux / Mac OS X / FreeBSD). Network Miner can be used as a passive network sniffer/packet capturing tool in order to detect operating systems, sessions, hostnames, open ports etc. without putting any traffic on the network. Network Miner can also parse PCAP files for off-line analysis and to regenerate/reassemble transmitted files and certificates from PCAP files. Network Miner makes it easy to perform advanced Network Traffic Analysis (NTA) by providing extracted artifacts in an intuitive user interface. The way data is presented not only makes the analysis simpler, it also saves valuable time for the analyst or forensic investigator. [9][4]

CAPSA is a network analyzer for both LAN and WLAN which performs real-time packet capturing, 24/7 network monitoring, advanced protocol analysis, in-depth packet decoding, and automatic expert diagnosis. It provides a comprehensive and high-level visibility to your entire network, helps network administrators or network engineers quickly pinpoint and resolve various application problems, and therefore enhance end user experience and guarantee a productive network environment. Identify and analyze more than 300 network protocols, as well as network applications based on the protocols; Monitor Internet, e-mail and instant messaging traffic, helping keep employee productivity to a maximum; Map out the details, including traffic, IP address, and MAC, of each host on the network, allowing for easy identification of each host and the traffic that passes through each; Visualize the entire network in an ellipse that shows the connections and traffic between each host.[7]

The packet capturing tools are used in the network forensic and it is very much useful in this area. The major aim is the collection of evidence. Network forensics is focused on detecting and monitoring network security concerns such as hacker activities, by beaming the searchlight on intrusion patterns to aid the investigation of cybercrimes. A packet capture program inserts itself into a network stack, to extract copies of frames and store them before they are sent out to an end device, and repeats the same procedure for incoming packet data. In this, I am downloading the widely used tools by the network forensic experts for capturing the packet data. Then using these tools, the packet data from the network is extracted and examined separately and hence finding out the time taken by each tool for capturing the data, advantages and disadvantages of each tool, types of data extracted by each tools and finally the effective tool among them.

CHAPTER 2: LITERATURE REVIEW

LITERATURE REVIEW

Mandeep Kaur1, Navreet Kaur2, Suman Khurana ,Student, Department of Computer Science and Application, K.M.V., Jalandhar, India ,Associate Professor, Department of Computer Science and Application, K.M.V., Jalandhar, India(2002)----------With the advancement in cyber area, frequent use of internet and technologies leads to cyber attacks. Digital forensic is opted for acquiring electronic information and investigation of malicious evidence found in system or on network in such a manner that makes it admissible in court. It is also used to recover lost information in a system. The recovered information is used to prosecute a criminal. Number of crimes committed against an internet and malware attacks over the digital devices have increased. Memory analysis has become a critical capability in digital forensics because it provides insight into the system state that should not be represented by traditional media analysis. In this paper, we study the details of cyber forensics and also provide the vital information regarding distinctive tools operate in digital forensic process. It includes forensic analysis of encrypted drives, disk analysis, analysis toolkit, volatile memory analysis, captures and analyzes packets on network.

Mohammad Rasmi, Aman Jantan, Hani Al-Mimi, School of Computer Sciences, University Sains Malaysia Faculty of Science & Information Technology, Al-Zaytoonah University, Penang /Malaysia, Amman /Jordan(2004)----------Current network forensics approaches are costly and time consuming. In addition, these approaches normally use active and reactive processes to resolve cyber crimes, and such processes start after the cyber crime has been identified, which makes identifying useful evidence difficult. Moreover, the information required to understand and resolve cyber crimes are limited. This paper proposes a new approach to resolve cyber crime in network forensics. The proposed approach aims to use cyber crime evidence to help investigators to resolve cyber crime efficiently. The paper presents the current network forensics approaches and various existing digital forensics models in order to determine the suitable process to be

used in the proposed approach. Thus, the proposed approach based on the generic and modern process model for network forensics.

Ahmad Almulhem, Computer Engineering Department, King Fahd University of Petroleum and Minerals, Dhahran 31261, Saudi Arabia(2006)---------Network forensics is an extension of the network security model which traditionally emphasizes prevention and detection of network attacks. It addresses the need for dedicated investigative capabilities in the current model to allow investigating malicious behaviour in networks. It helps organizations in investigating outside and inside network attacks. It is also important for law enforcement investigations. In this paper, various aspects of network forensics are reviewed as well as related technologies and their limitations. Also, challenges in deploying a network forensics infrastructure are highlighted.

Voice traffic packet capture and analysis tool for a data network ,HENTRY HOUGH in 2001---------- The present invention utilizes a network processor as part of a test system for testing network environments and devices, and particularly VOIP networks and devices. The network processor is used as part of the test system and is precisely controlled by software to provide a variety of functions in order to test a network environment and devices. The test system incorporating the network processor may be programmed to process packets, create packets, receive packets and analyze packets. The test system thus provides simulation of network conditions using high bandwidth interfaces, a sniffing functionality with packet to flow correlation on high bandwidth interfaces, the capture and/or creation of network profiles, and the capture and analysis of network packets.

International Journal of Network Security & Its Applications 1.1 (2009) 14-25------- Network forensics deals with the capture, recording and analysis of network events in order to discover evidential information about the source of security attacks in a court of law. This paper discusses the different tools and techniques available to conduct network forensics. Some of the tools discussed include eMailTrackerPro to identify the physical location of an email sender; Web Historian to find the duration of each visit and the files uploaded and downloaded from the visited website; packet sniffers like Ethereal to capture and analyze the data exchanged among the different computers in the network. The second half of the paper presents a survey of different IP trace back techniques like packet

marking that help a forensic investigator to identify the true sources of the attacking IP packets.

Journal of Computing Sciences, Volume 20 Issue 4, April 2005-------- here are many free packet-sniffing tools available for download. Ethereal and tcpdump are two of the most popular tools among network administrators. This work compares and contrasts the usefulness and appropriateness of these tools for pedagogical purposes. While ethereal is user-friendlier than tcpdump, tcpdump is less intrusive and hence, can be used in a campus-wide network safer, since it does not readily reveal any data transmitted in a packet. Ethereal can be used in a closed networking lab environment to analyze and study many more protocols. Many class assignments can be designed using these two packet sniffers. Particularly, assignments can be developed to analyze tcpdump's output in real-time for intrusion detection or the understanding of a protocol.

Meghan than, Natarajan (Jackson State University) ; Allam, Sumanth Reddy (Jackson State University) ; Moore, Loretta A (Jackson State University)(2006),----------Network forensics deals with the capture, recording and analysis of network events in order to discover evidential information about the source of security attacks in a court of law. This paper discusses the different tools and techniques available to conduct network forensics. Some of the tools discussed include: eMailTrackerPro to identify the physical location of an email sender; Web Historian to find the duration of each visit and the files uploaded and downloaded from the visited website; packet sniffers like Ethereal to capture and analyze the data exchanged among the different computers in the network. The second half of the paper presents a survey of different IP traceback techniques like packet marking that help a forensic investigator to identify the true sources of the attacking IP packets. We also discuss the use of Honey pots and Honey nets that gather intelligence about the enemy and the tools and tactics of network intruders.

Ahmad Al-Qerem, Zarqa University/Department of Computer Science, Zarqa, 13132, Jordan(2008)----------According to the Cyber Security Watch Survey, cyber crime attacks incurred an average monetary loss of $123,000 per organization in the USA in 2011. The cost incurred by cybercrimes per company ranges from $1.5 million to $36.5 million each year. In reality, a strong relationship exists between the time required to resolve a cyber

crime and the cost. Based on a previous study [2, 25], cyber crimes could become costly if they are not resolved quickly. Current investigation techniques are very costly and time consuming because extensive effort is required to analyze the overwhelming amount of evidence presented in each cyber crime case. In addition, gathering useful evidence is difficult because most techniques utilize active and reactive processes to analyze cyber crimes; such processes start right after the detection of the cyber crime. Network forensic systems can be classified into two approaches: proactive and reactive. Proactive network forensics is a new approach in live investigation that deals with the phases of network forensics during an attack. As reported by, proactive forensic approaches reduce the time and cost of investigation by identifying potential evidence and reducing the resources needed in the investigation phase. These approaches are utilized in the preliminary analysis of a cyber crime and help improve and accelerate the decision making process. This paper is proposed a new approach to resolve cyber crime for network forensics, the process of the proposed approach will be described in section 3. The approach will be compared with the generic process model for network forensics as mentioned in, which will be described in section 4. The next section will present a related work of network forensics approaches.

CHAPTER 3: AIM & OBJECTIVES

AIM:

To analyze the Comparison of tools used for the packet data capture

OBJECTIVES:

- To check the efficiency of the tools.
- To determine whether the tool will be capturing all the things.
- To determine the advantages and disadvantages of tools.
- To know which tool will provide correct information.
- To determine which tool is good for an investigating officer.
- To know what are things that are captured by each tool.
- To identify any mistakes are done by the tools.
- To compare the difference between each tool.

CHAPTER 4: MATERIALS &METHODOLOGY

MATERIALS

Computer, various forensic tools like, wireshark, SoftPerfect Network Protocol Analyzer, CAPSA, network miner etc, network packets and logs

METHODOLOGY

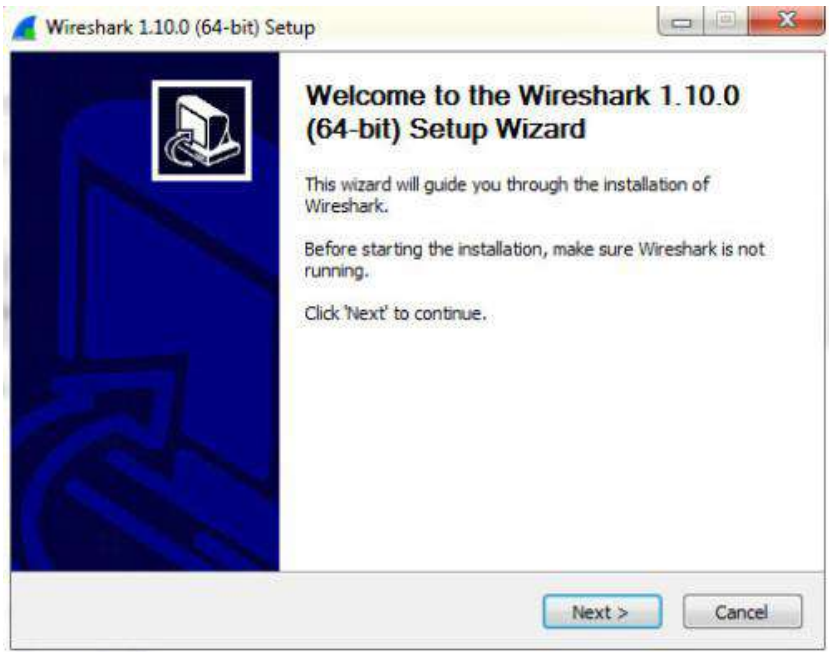
Firstly the 4 tools (wireshark, SoftPerfect Network Protocol Analyzer, CAPSA, network miner,) are downloaded and installed in the computer and then using the software. Examine the network packages separately by each tool and results should be noted separately by taking the screenshots.

Firstly, we had to install the 4 tools separately and the installation procedure is following:

- **Installing wireshark**

Step 1: **Download Wireshark from the below link [5]**

Step 2: install the software



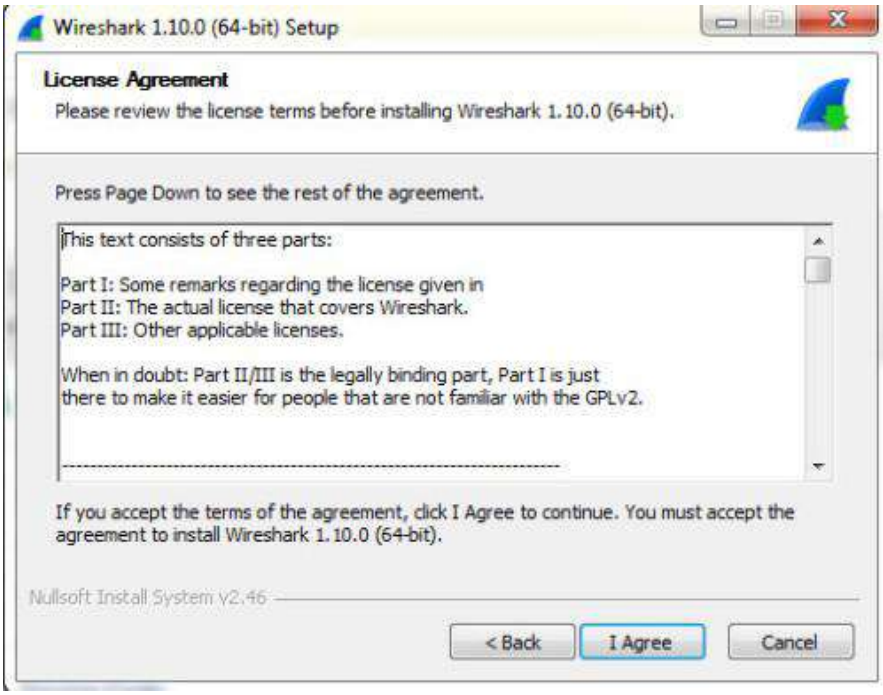


Fig.1.1

Choose the components

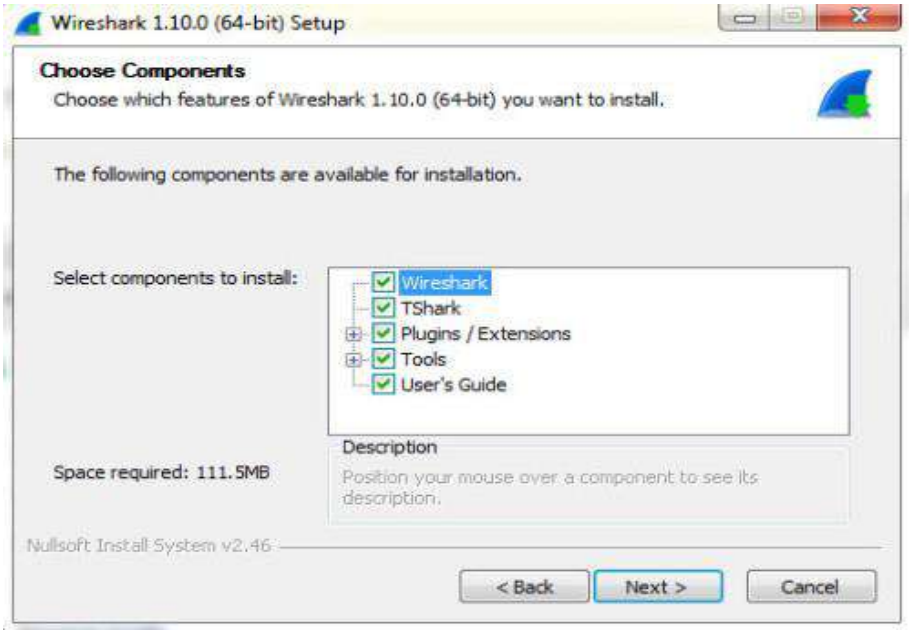


Fig.1.2

Choose the location

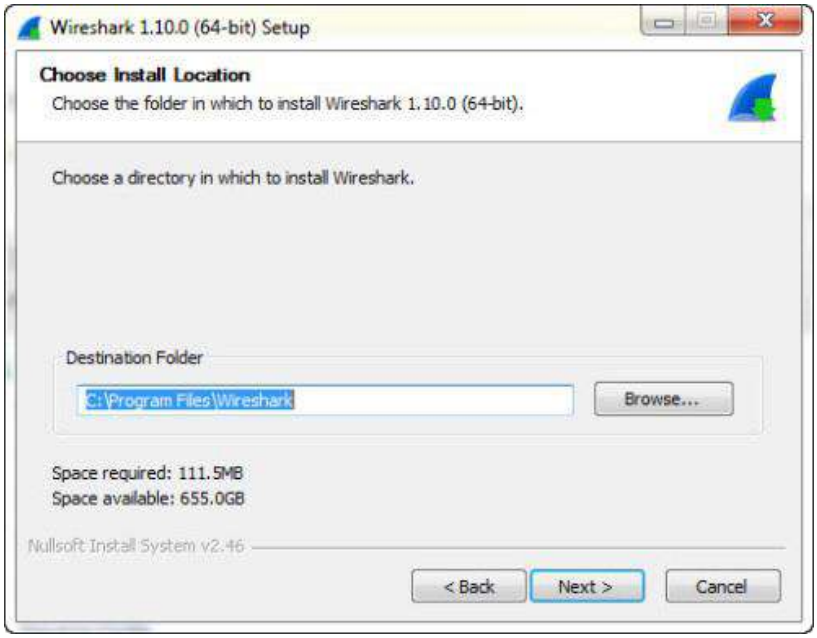


Fig.1.3

Step 3: Install WinPcap – as Wireshark won't work otherwise

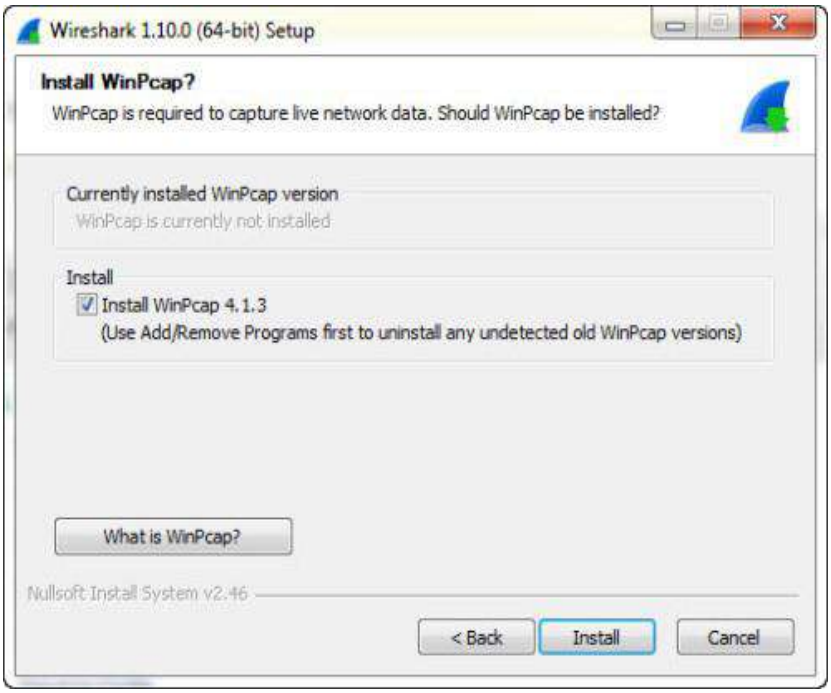


Fig.1.4

Click on next

Fig.1.5

Click on install tab

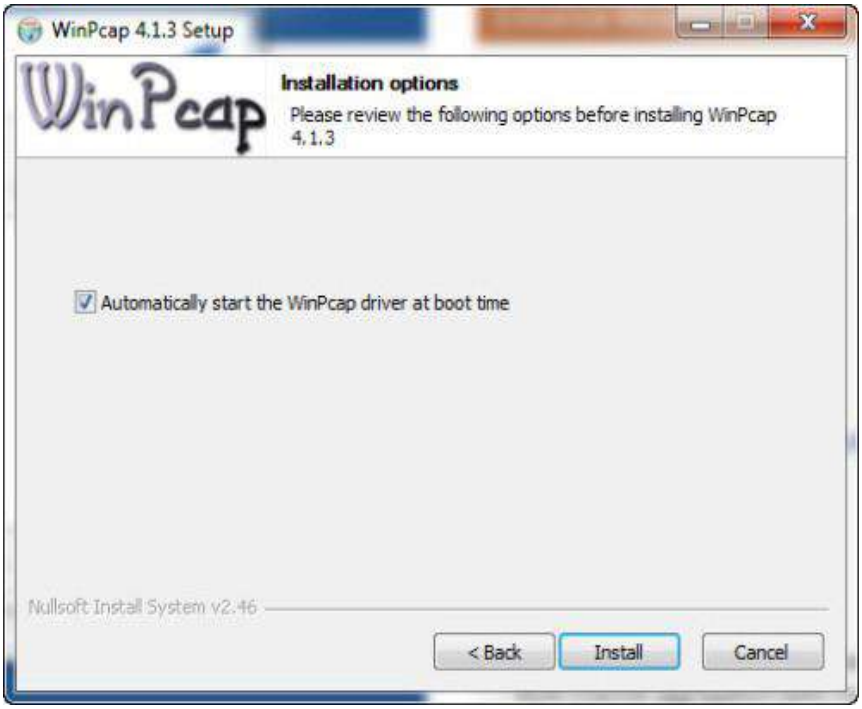


Fig.1.6

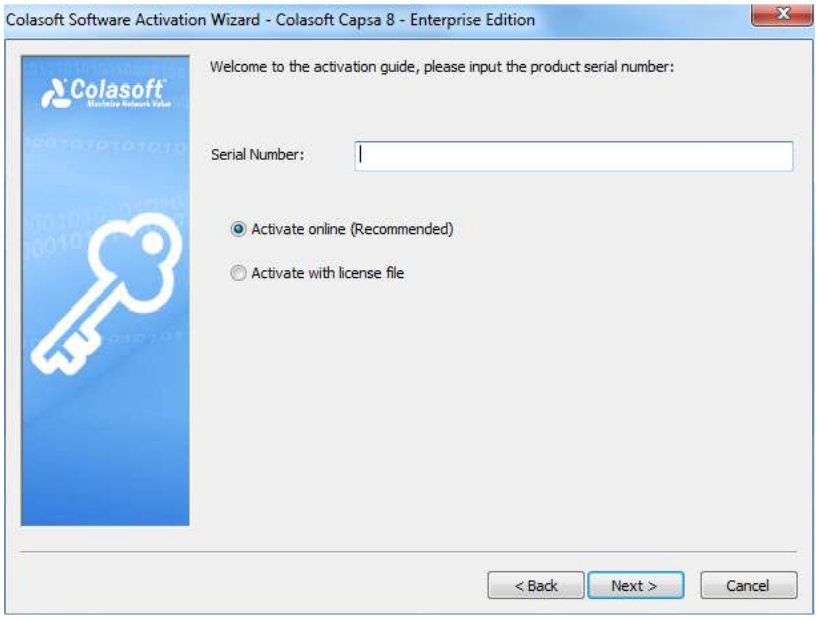
Click on finish

Fig.1.7

- **Installing CAPSA**

Step 1: download software from the below link [7]

Step 2: open the downloaded file and enter the activation code of the software



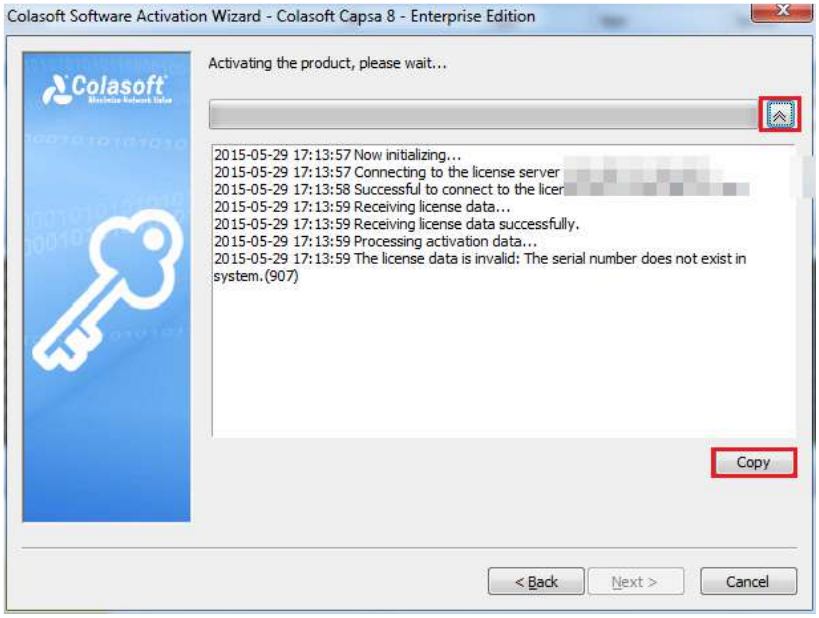


Fig.2.1

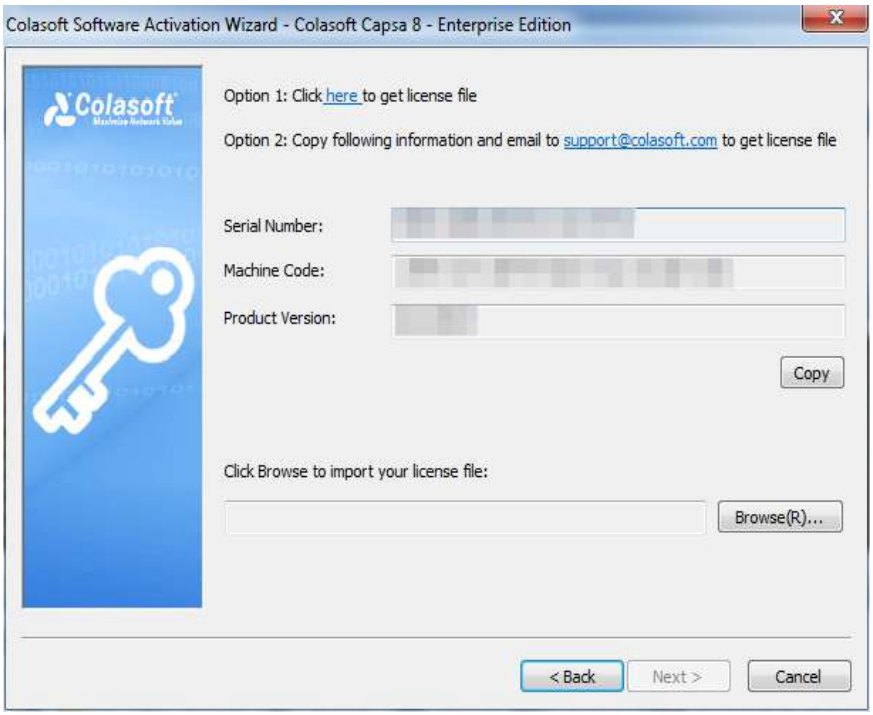


Fig.2.2

Click on finish

- **Installing SoftPerfect Network Protocol Analyzer**

Step 1: download the software from the below link[6]

Step 2: open the download file and click on next

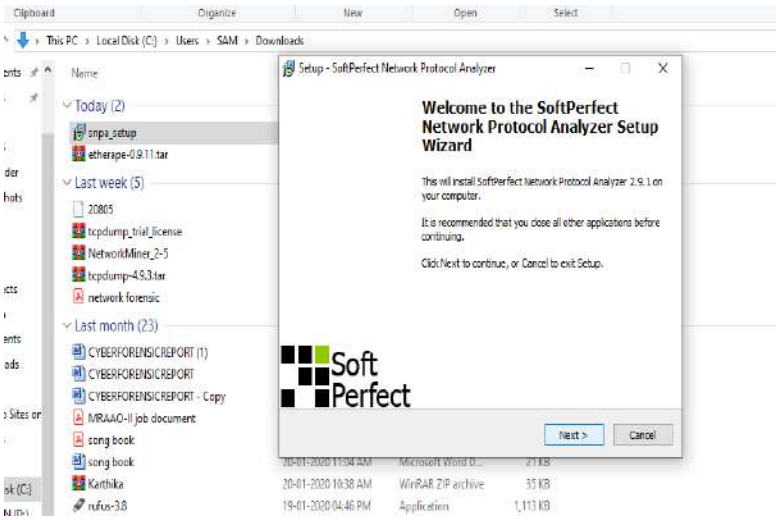


Fig.3.0

Select the location for the file

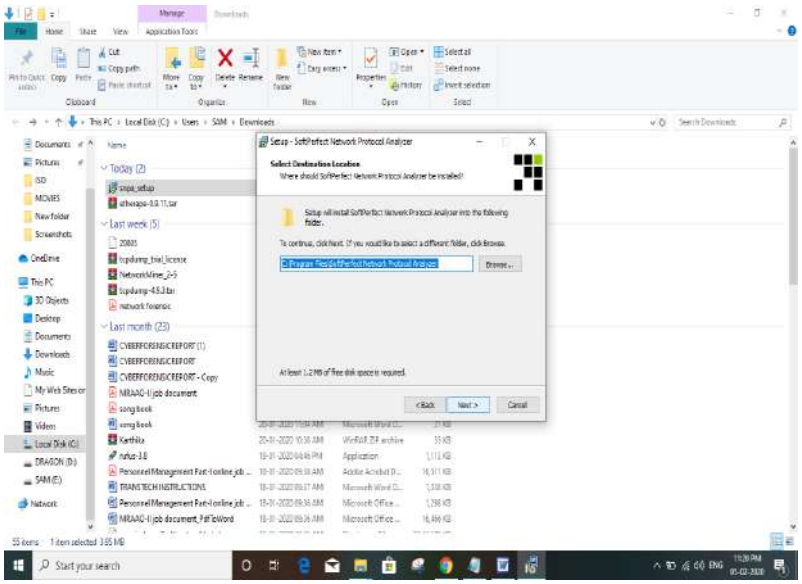


Fig.3.1

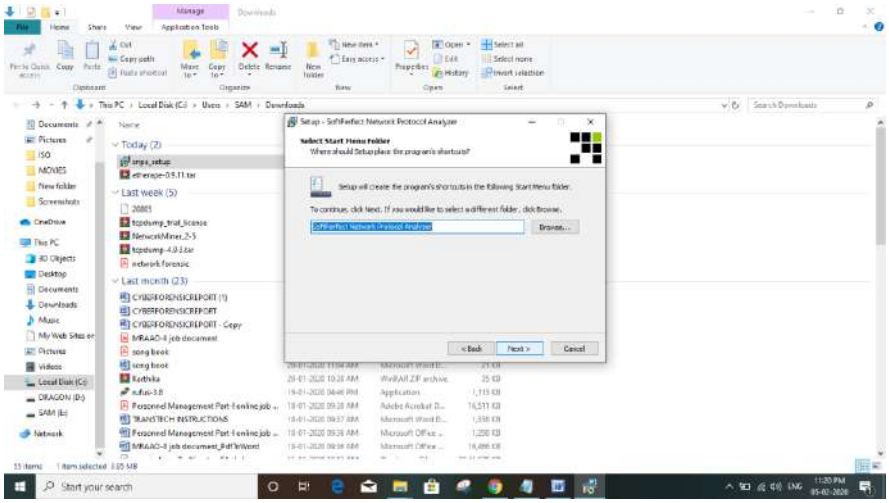


Fig.3.2

Click on finish

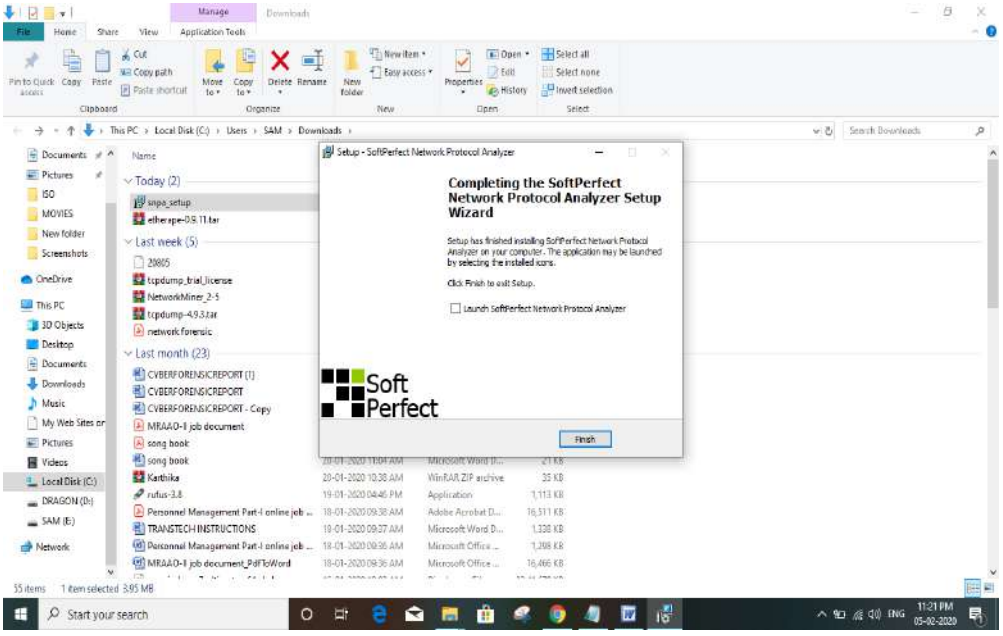


Fig.3.3

- **Installing network miner**

Step 1: download the file from the below link[9]

Step 2: right click on the file and select option extract here

Fig.4.0

Open the folder and click on the network miner file

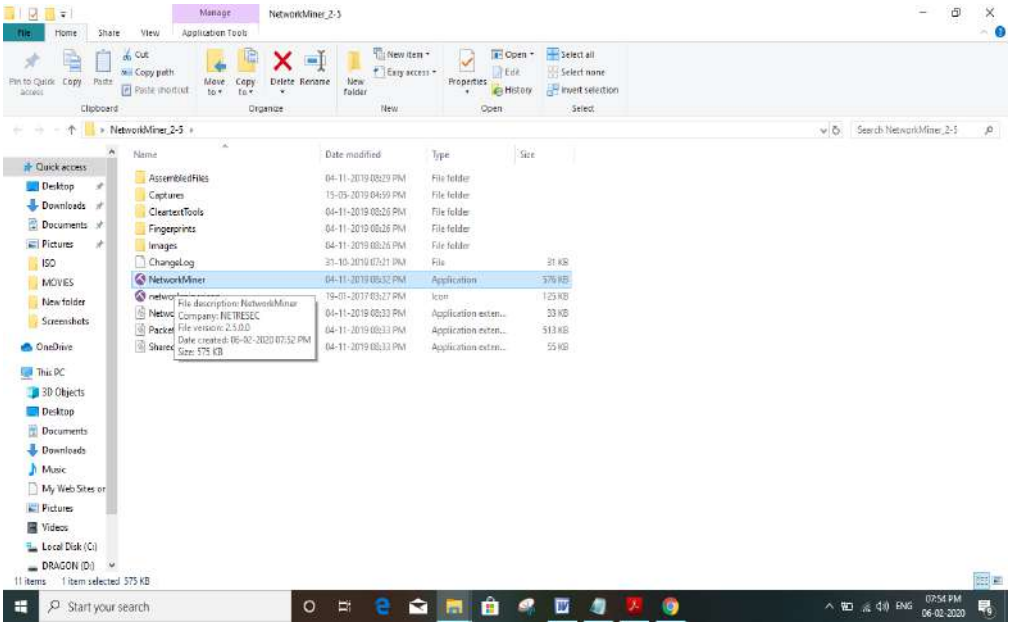


Fig.4.1

CHAPTER 5: OBSERVATIONS

OBSERVATIONS

- **wireshark**

1. Free software
2. Available for multiple platforms – Windows & UNIX
3. Can see detailed information about packets within a network
4. Not proprietary can be used on multiple vendors [4]
5. can save the captured packets
6. Notifications will not make it evident if there is an intrusion in the network [3]

7 .Can only gather information from the network, cannot send [2]

- **CAPSA**

1. Locate hosts running a specific service
2. Identify abnormal protocol[3]
3. Identify packets with forged data[8]
4. Paid version
5. Only supports in windows
6. More packet loss

- **Softperfect Network Protocol Analyzer**

1. packets can be saved separately
2. It is a free tool

3. Fast, graphical scan interface that give you the info you need[1]

4. Many options to scan for more additional device info

5. No possibility to print or export scan results.[2]

6. Limited options for scanning and customisation

7. Mac source address and Mac destination address will be there

- **Networkminer**

1. Suitable for all platforms like windows, Mac, Linux etc.

2. Networkminer can also analyze PCAP records for disconnected examination [4]

3. Cannot filter packets on many criteria.

3. The method in which the data is dispensed not only makes the scrutiny easier.[2]

CHAPTER 6: RESULTS & CONCLUSIONS

RESULT

These packet-capturing tools are capturing and analyzing packets of data that flow through a particular network. It shows the traffic occurring on the network. they are also useful in monitoring the networks. The packet capturing tools provides the information such as time, source address, destination address, protocol, length of the packet and information about the packets.

Wireshark

In wireshark, the packets are captured and by selecting each packet, we can see the details about the packets separately down the tool. In addition, we can save the packets separately

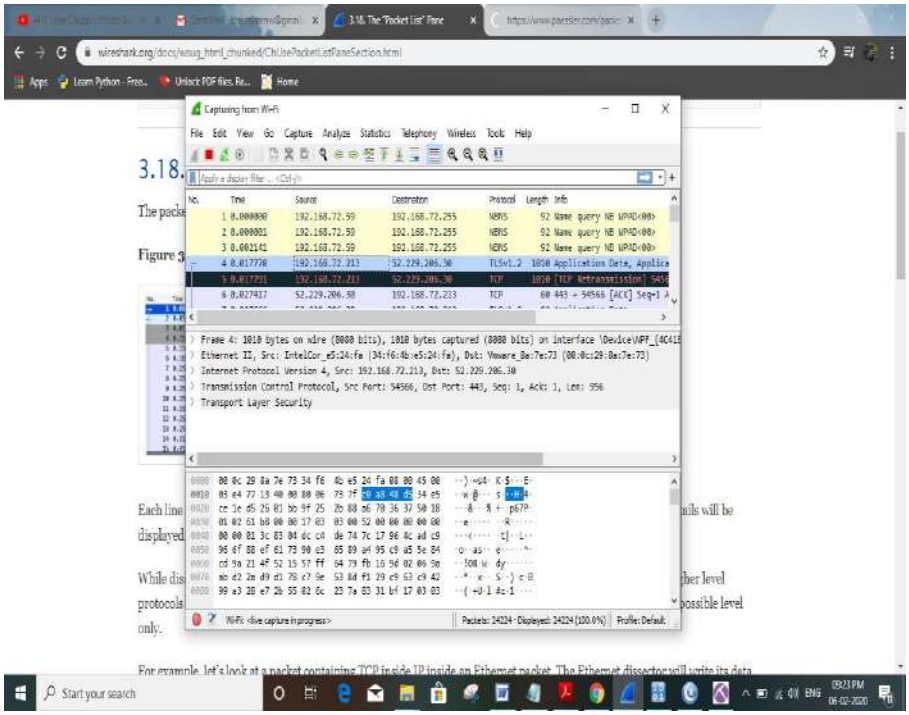


Fig.5.0

CAPSA

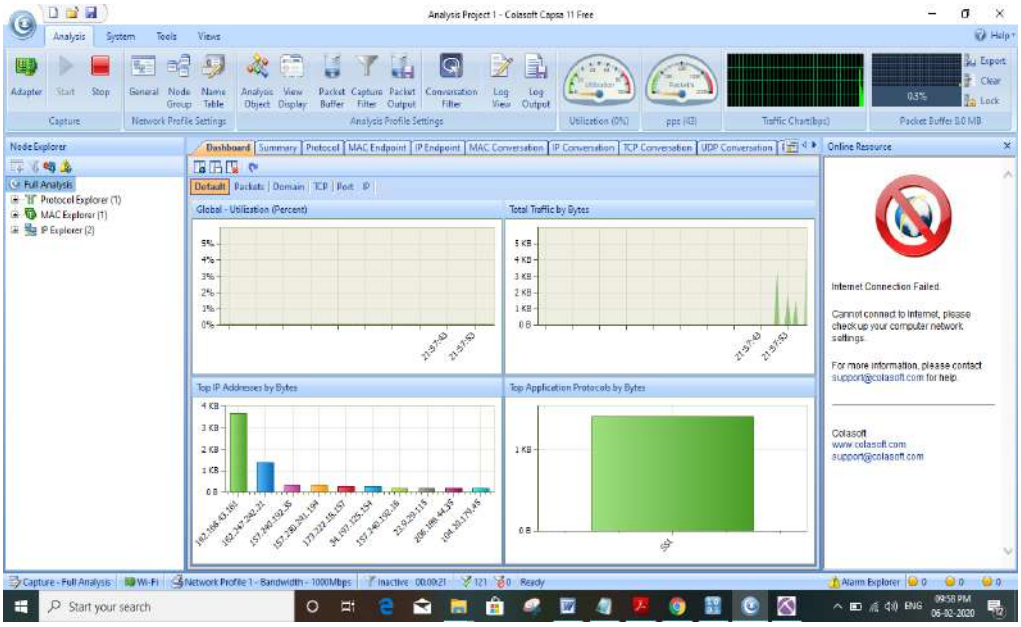


Fig.6.0

The CAPSA is also having the same function like other packet capturing tools but in addition to that, we can use this for complete analysis selecting the 'full analysis tab'. Also we can use this for traffic monitoring, HTTP analysis, Email analysis, DNS analysis, FTP analysis.

Softperfect Network Protocol Analyzer

It captures and analyzes the data passing through your network connection, and represents it in a readable form. The program completely decodes all the major protocols such as IP, TCP, UDP, ICMP, as well as top-level protocols including HTTP, SMTP, POP, IMAP,FTP and others. Network Protocol Analyzer includes detailed filtering options that allow you to limit the capture based on IP address, port, data content and other technical information

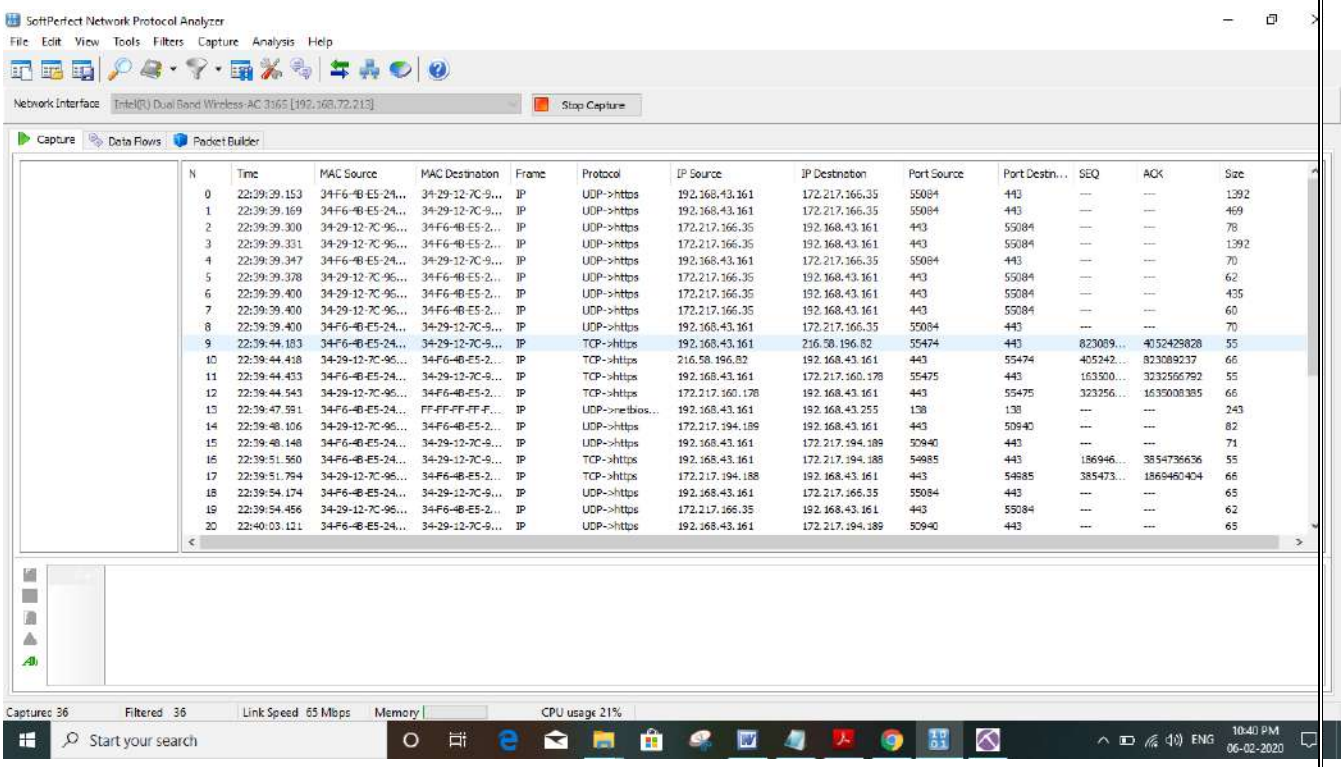


Fig.7.0

NETWORKMINER

NetworkMiner is one of those tools. It is easy to use; you'll be underway in no time; and the resulting data will be of assistance no matter the forensic circumstance. Network Miner makes it easy to perform advanced Network Traffic Analysis (NTA) by providing extracted artifacts in an intuitive user interface.

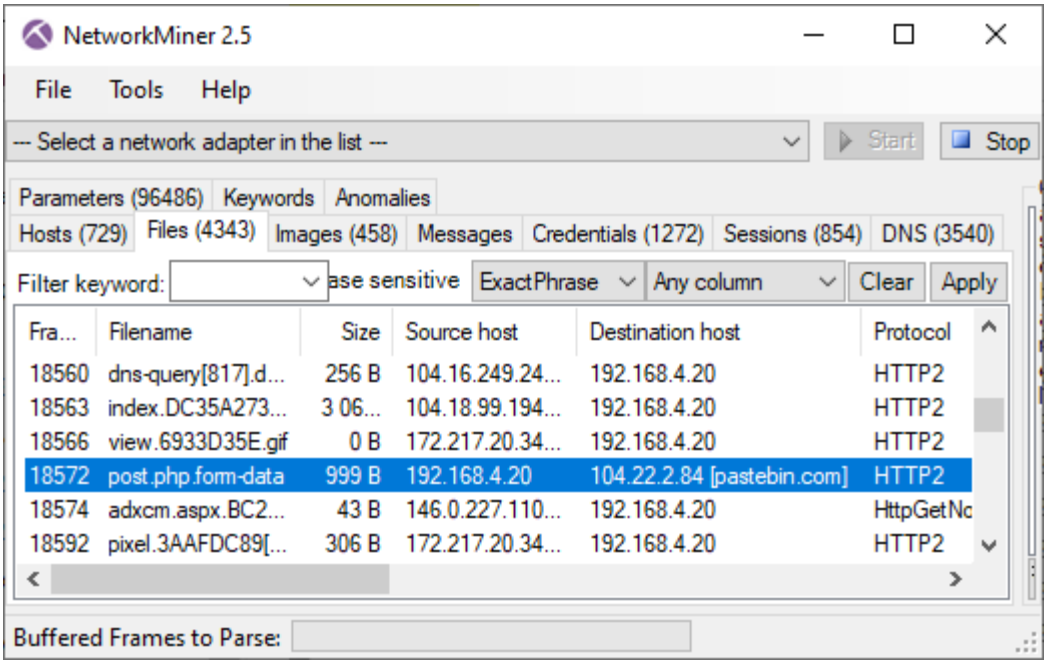


Fig.8.0

CONCLUSION

All the tools are good for packet capturing and the packets can be saved and used for examination. From these packets, we can extract the information like source address, destination address, protocol, length of the packets etc.From the above study of the comparison of tools shows the following features:

1. The wireshark and the softperfect network protocol analyzer is the best tool for capturing the packets in network due to low errors compared to other packet capturing tools

2. While capturing packets, the CAPSA is not capturing all the packets on the network.

3. In networkminer the accuracy of capturing packets is low as compared to other tools

4. In CAPSA and Networkminer people can alter the captured packets but in the other tools it is having less chance to manipulate

5. For a forensic investigator wireshark and softperfect network protocol analyzer will be a useful tool since it is making only less mistakes and almost all packets in the networks are captured without any errors

CHAPTER 7: REFRENCE

REFRENCE

1. S. Ansari, Rajeev S.G. and Chandrasekhar H.S., "Packet Sniffing: A Brief Introduction", IEEE Potentials, Dec 2002-Jan. 2003, Volume: 21 Issue: 5, pp: 17-19 (2002-2003).

2. Qadeer M.A., Zahid M., Iqbal A., Siddiqui M.R "Network Traffic Analysis and Intrusion Detection Using Packet Sniffer"ICCSN'10 Second International Conference, (2010), Page(s): 313-317(2010).

3. A. Dabir, A. Matrawy, "Bottleneck Analysis of Traffic Monitoring Using Wireshark", 4th International Conference on Innovations in Information Technology, 2007, IEEE Innovations '07, 18-20 Nov. (2007), Page(s): 158-162(2007).

4. All about Tools [Online] Available: http://www. sectools.org.

5. All about Wireshark [Online] Available http:// www.wireshark.org/.

6. All about soft perfect network protocol analyzer [Online] Available http://www.softperfect.com/products/networksniffer/

7. All about capsa [Online] Available www.colasoft.com

8. BoYu"Based on the network sniffer implement network monitoring Computer Application and System Modeling (ICCASM), 2010 International Conference on Volume: 7, 2010, Page(s): V7-1-V7-3(2010).

9. www.netresec.com/?page=NetworkMiner