ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 4, Issue 3, March 2015

Ethical Network Monitoring Using Wireshark and Colasoft Capsa as Sniffing Tools

Nedhal A. Ben-Eid

Computer Trainer, Computer Department, HITN, Shuweikh, State of Kuwait

Abstract: With the development and popularization of network, the management and monitoring of network traffic is important to keep the network smooth and efficient. It is increasingly critical that an organization secure the system to avoid external hacking and employee abuse of computers in the workplace. This paper study the problem of employee abuse of computers in the workplace and discuss ethical and legal dimensions of the decision facing employers and network administrators regarding whether it is appropriate to monitor the employee's workstation in the organizations. Packet Sniffer is a tool used by network administrators to capture all the packets on the network and monitor the bottlenecks, alarm the irregular behavior, capture passwords and VoIP from any workstation in that network to keep network secured. We give a brief introduction of what is a packet sniffer, its structure, uses and types. Two of the most popular packet sniffing software are discussed and examined; Wireshark and Colasoft Capsa. They are compared according to their features, characteristic behavior, qualitative and quantitative parameters.

Keywords: Packet capture, Traffic analyzer, Network monitoring, Network Sniffing, Network analyzer, Packet sniffer, Wireshark, Colasoft Capsa.

I. INTRODUCTION

Information technology has emerged as an integral part of today's organizational infrastructure. These technologies have the potential to improve worker efficiency and effectiveness. However, there are risks associated with any technology including the potential for employee abuse resulting in negative consequences [10]. This abuse mostly happened when the employee accessing the Internet using the organization's workstation for non-work related purposes, which will affect the performance of the network and decrease the productivity of the employees at work. Network monitoring is the best solution to capture each packet sent or received in the network in order to keep the network secured and efficient. This monitoring is done by the network administrator who watches all the inappropriate actions happened in the network [2].

II. THE PROBLEM OF ABUSING THE COMPUTER AT WORK

As evidenced by various surveys and studies conducted by media research companies, including Nielson, Burst Media, and eMarketer, the average employee spends between one and two hours each day using the Internet for personal reasons. Another recent survey shows that 51% of employees who use the Internet at work spend between 1 to 5 hours per week surfing the web for personal reasons [10]. A field survey is tested on 500 employees working in different organizations in state of Kuwait to know whether there is a real problem concerning computer abuse in the organizations, which will be reflected on the performance of the network and employees productivity. The survey consists of 20 questions and tested outside the organizations environment due to privacy reasons, and 12 papers have been excluded due to inconsistence. The results of the survey are shown in the following four figures. Figure (1) shows that 86 % of the employees in the survey are using Internet during the work hours for personal purposes, which is a very high percentage and indicates that there is a real problem that needs to be controlled by the employers as well as the network administrator.

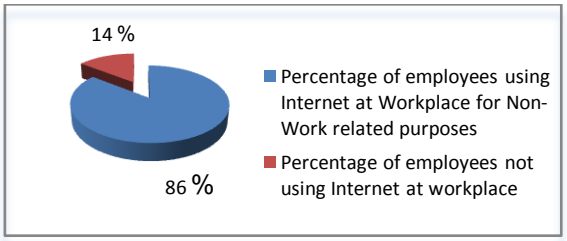

Fig. 1. The percentage of Internet usage at workplace

Most of employees would be hard pressed to deny their use of the Internet at work for non-work related purposes. With sites like YouTube, eBay, Face book, shopping and banking, tempting them at every turn, it can be difficult to resist personal Internet usage at work. While not every person has access to the Internet at work, the majority do [11]. Figure (2) shows the applications that attract the employees during work time in the organization.

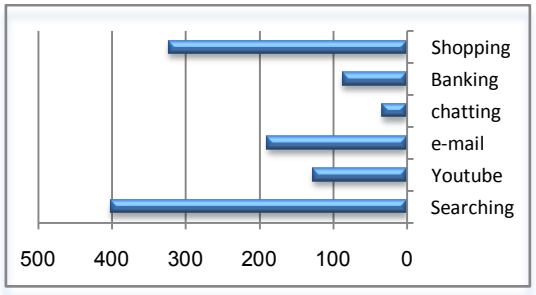

Fig. 2. The Internet activity that attract employees at workplace

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 4, Issue 3, March 2015

It is clearly seen that the first attracting action is "searching" about some topics or images that may be useful for researchers. And the last attracting application is "chatting" because mobiles have substituted this application by WhatsApp, Viber and other mobile chatting applications, which are easier and more practical than desktop chatting applications.

The enormity of potential productivity loses, as reported by Court (2004), is approximately one million dollars annually for a company with 500 employees surfing the Internet for just a half hour a day. Using these facts, if an employee spends two hours per day on the Internet, and the organization has 500 unmonitored employees, the potential annual loss could be nearly $4 million. If a business owner does nothing to stop these counter-productive activities, then it is not likely the owner could stay in business. Workplace monitoring can be beneficial for an organization to obtain productivity and efficiency from its employees [9].

According to our survey, figure (3) shows that 40% of the employees spend 6 hours a week or more using Internet at work for personal purposes; which is equivalent to 1.2 hours a day of computer abuse.

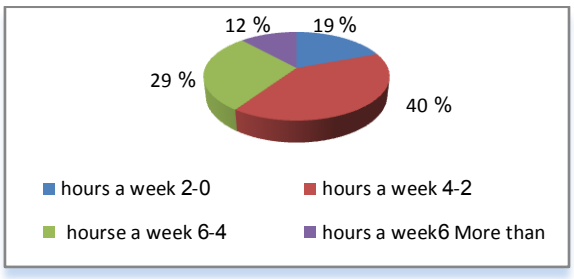

Fig. 3. Number of hours employees spend using Internet at workplace

Every Employee accessing the Internet at work for non-work related purposes has some personal purpose or reason to do so. Figure (4) shows some suggested reasons and the percentage of employees that consider it the main reason that force them for computer abuse at workplace.

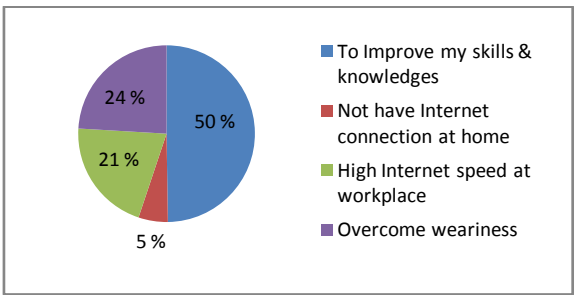

Fig. 4. The main reason for using Internet at workplace

As we can see from the previous figures that there is a real problem concerning the computer abuse at workplace, which will affect the performance of the network and requires some kind of control and monitoring.

Security is yet another reason that gives rise to an organization's need for employee monitoring at workplace. Woodbury (2003) explains that opening unsolicited e-mail at work creates danger because attached files could contain a virus, wreaking havoc on a workstation hard drive and then spreading through a business' entire computer network. Many articles from Management and law journals such as the American Management Association and Mealey's Cyber Tech Litigation Report support a perceived need for employers to monitor their employees. The need comes from more than just a desire to increase productivity, but there are also issues relating to protection from potential legal liability [9].

III. NETWORK MONITORING

In most workplaces, all employees' computers are connected to the system administrator's computer. This allows the system administrator to gain access to an employees' computers, which will facilitate his work when a specific problem occurs. However, remote access also allows the system to check log files, including e-mails, web site visits, and even downloads, that the user might believe to be deleted or cleared.

Internet surveillance and desktop surveillance are the two basic types of administrator monitoring. Internet surveillance is the active monitoring of a user's online activity. And desktop surveillance involves the physical monitoring of a specific computer and every action taken by its users [11].

Network monitoring provides information regarding network related problems even before a problem develops. It also provides guidance on how to improve the network by studying performance charts of the network activities. Built- in pagers and e-mail alarm keeps network administrator informed on all the important happening in the network [15].

Although the employees' monitoring technology is extremely sophisticated, it is in practice by large and small businesses throughout the world and it is growing rapidly [9]. The American Management Association (AMA) survey reported that 82% of employers engage in some form of network monitoring (AMA,2001). In USA an estimated 14 million employees have their Internet use under continuous monitoring. Worldwide, an estimated 27 million workers are under such monitoring (Firoz et al,2006) [10].

People, the employees, by nature generally tend to desire more freedom and less monitoring. Many people and organizations are against monitoring the activities of people in the work place. Opponents include civil liberty groups, privacy advocates, and many employees themselves. Among the major criticisms of electronic employee monitoring, as noted by Watson (2001), are increased levels of stress, decreased job satisfaction, decreased work life quality, lower levels of customer

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 4, Issue 3, March 2015

service and employers can use it unfairly, which will create a hostile workplace.

On the other hand, giving employees open, unmonitored, computer access causes productivity and efficiency to suffer. There has to be a balance between protecting the company's information assets without going overboard to the point where employees feel alienated. Education and communication are the best tools to attain this balance [9].

IV. LEGAL AND ETHICAL ISSUES OF NETWORK MONITORING

This paper takes a look at a neglected area of most computer security professional's training; how to deal with the ethical issue that can crop up during the course of doing their job. Physicians, attorneys and other professionals whose job duties affect other's lives usually receive, as part of their formal training courses that address ethical issues common to their professions. IT security personnel often have access to much confidential data and knowledge about individuals and companies networks and systems that give them a great deal of power. That power can be abused, if it is not controlled with ethical issues. The education and training of IT professionals, including security specialist, usually focuses on technical knowledge and skills. You learn how to perform tasks, but with little consideration of how those abilities can be misused.

A common concept in any ethics discussion is the "slippery slope". This pertains to the ease with which a person can go for doing something that doesn't really seem unethical to doing things that are increasingly unethical. So, it's easy to notice that each legal action could "morph" into much less justifiable actions. For example, the information you gained from reading someone's e-mail could be used to embarrass that person, to gain political advantage within the company [6].

New technologies often create the need for new rules. Marshall (2001) uses the example of the U.S. postal system to show how laws change to address new technologies. In 1825, Congress enacted mail anti-tampering laws in response to increased reliance on the mail system, brought about because of growing literary in the young nation. However, it was not until 1877 did the Supreme Court extend Fourth Amendment Constitutional protection to mail, requiring government officials to get a court order to open mail. Marshall's postal system example shows how laws often lag behind technological development. E-mail is like a new version of postal mail. While laws currently protect someone from opening or tampering with postal mail, the same type of laws do not currently (and may never) protect e-mail [9].

However, the question of ethical behavior in IT professions is beginning to be addressed. Voluntary professional associations such as the Association for Computing Machinery (ACM) have developed their own codes of ethics and professional conduct, which can serve as a guideline for individuals and other organizations [7].

Current laws do not specifically state that monitoring employees is illegal. In fact, some organizations have used information obtained from monitoring employees as key evidence in many legal cases. An article by Meade (2001) on workplace privacy notes that e mail and Internet-use evidence has been used to prove critical legal issues in a wide variety of lawsuits. More than one fourth of employers have fired workers for misusing e-mail and approximately one third have fired employees for misusing the Internet, according to the 2007 Electronic Monitoring & Surveillance Survey from American Management Association (AMA, 2008) and The ePolicy Institute.

Another legal issue arising from employee monitoring is an organization's legal obligation to do so. Court (2004) discusses a survey reporting that 68% of employers who monitor employees' computer activities cite legal liability as their main motivation. Although Court writes, no court of law has ever ruled that an employer is required to monitor employees' electronic communications; some have suggested that such monitoring would be wise.

The courts can hold companies liable if they do not seek to prevent other employees from creating a hostile work environment.

Ethically speaking, create and update a clear Acceptable Use Policies is essential to outline how employees can use company system and what they can expect as privacy. This must be done by cross-functional team effort that includes, representatives from human resources and if available, legal council, along with system administrators. Educate the workers about the privacy issues of the workplace and let them know what monitoring is, what it will monitor, and convey the message that this monitoring is not due to lack of trust, but is being used to protect the organization. Training session can be established to notify all employees about organization's monitoring [9].

V. NETWORK SNIFFING

Network sniffing describes the process of monitoring, capturing and interpreting all incoming and outgoing traffics as it flows across a network, it is typically performed by a packet sniffer; a tool used to capture raw network data going across the wire [12]. Network sniffing can help to understand network characteristics, learn who is on the network, determine who and what is utilizing available bandwidth, identifying peak network usage time, identifying possible attacks or malicious activity, and find unsecured and bloated applications [1].

The information that travels across a network is transmitted in form of "packets" that is broken up into smaller segments with destination and source address attached. A Packet sniffers can show you all sorts of things going on behind the scenes, including unknown communication between network devices, actual detailed error codes provided by layer-specific protocols, and even poorly designed programs going crazy [19].

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 4, Issue 3, March 2015

A. Types of Packet Sniffing

There are basically three types of packet sniffing methods:

- IP Sniffing: This is the original way of packet sniffing. It works by putting the network card into promiscuous mode and sniffing all packets matching the IP address filter. This method only works in non-switched networks [14]
- MAC Sniffing: MAC sniffing also works through a network card which allows the device to sniff all of the information packets that correspond with the MAC address filter [19].
- ARP Sniffing: ARP sniffing involves information packets that are sent to the administrator through the ARP cache of both network hosts. Instead of sending the network traffic to both hosts, it forwards the traffic directly to the administrator [19]. This method works a little different. It doesn't put the network card into promiscuous mode. This isn't necessary because ARP packets will be sent to us. This happens because the ARP protocol is stateless. Because of this, sniffing can be done on a switched network [14].

B. How a Packet Sniffer Works?

The packet sniffing process can be broken down into three steps: collection, conversion and analysis

Collection:

Packet sniffer switches the selected network interface into promotion mode. In this mode, the network card can listen for all network traffic on its particular network segment to capture the raw binary data from the wire.

Conversion:

The captured binary data is converted into readable form. This is where most of advanced command-line-driven packet sniffers stop. At this point, the network data is in a form that can be interpreted only on a very basic level, leaving the majority of the analysis to the end user.

Analysis:

The packet sniffer takes the captured network data, verifies its protocol based on the information extracted, and begins its analysis of the protocols specific features [1].

Each machine on a local network has its own hardware address which differs from other machines. When a packet is sent, it will be transmitted to all available machines on local network. Owing to the shared principle of Ethernet, all computers on a local network share the same wire, so in normal situation, all machines on network can see the traffic passing through but will be unresponsive to those packets which do not belong to them by just ignoring them. However, if the network interface of a machine is in promiscuous mode, the NIC of this machine can take over all packets and frames it receives on network, namely this machine is a sniffer [7][15]. The sniffer program tells a computer's NIC to stop ignoring all the traffic headed to other computers and pay attention to them. It does this by placing the NIC in a state known as promiscuous mode. Once a NIC is promiscuous, a status that requires administrative or root privileges, a machine can see all the data transmitted on its segment. The program then begins a constant read of all information entering the PC via the network card. As we know, data traveling along the network comes as frames, or packets, bursts of bits formatted to specific protocols. Because of this strict formatting, a packet sniffer can peel away the layers of encapsulation and decode the relevant information stored within: source computer, destination computer, targeted port number, payload, in short - every piece of information exchanged between two computers. Sniffers can work differently depending on the type of network they are in. Here is a good set of definitions on the two types of Ethernet environments.

- Shared Ethernet: In a shared Ethernet environment, all hosts are connected to the same bus and compete with one another for bandwidth. In such an environment packets meant for one machine are received by all the other machines. Thus, any machine in such an environment placed in promiscuous mode will be able to capture packets meant for other machines and can therefore listen to all the traffic on the network.
- Switched Ethernet: An Ethernet environment in which the hosts are connected to a switch instead of a hub is called a Switched Ethernet. The switch maintains a table keeping track of each computer's MAC address and delivers packets destined for a particular machine to the port on which that machine is connected. The switch is an intelligent device that sends packets to the destined computer only and does not broadcast to all the machines on the network, as in the previous case. This switched Ethernet environment was intended for better network performance, but as an added benefit, a machine in promiscuous mode will not work here. As a result of this, most network administrators assume that sniffers don't work in a Switched Environment [20].

There are many software solutions available on the market to monitor a vast array of activities which ranges from several thousand dollars down to free. Most solutions can log keystrokes typed, application and website usage, detailed file usage, incoming and outgoing chats and e-mails, internet connections, windows interacted with, internet packet data, desktop screenshots, software installations, and much more. The software can present all activities logged in easy-to-read graphical reports [9]. We will study and compare between two of the most popular Sniffing Programs; Wireshark and Colasoft Capsa.

VI. WIRESHARK

Wireshark is one of the most popular open-source packet analyzer. Originally named Ethereal, in May 2006 the project was named Wireshark due to trademark issue. Wireshark is cross-platform using pcap to capture packets; it runs on Microsoft Windows as well as various Unix-like operating systems including Linux, Mac OS X, BSD, and Solaris [21]. It uses the GTK+ widget toolkit to implement its user interface [5]. Wireshark is an open source software

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 4, Issue 3, March 2015

project, and is released under the GNU General Public License (GPL). You can freely use Wireshark on any number of computers you like, without worrying about license keys or fees or such. In addition, all source code is freely available under the GPL. Because of that, it is very easy for people to add new protocols to Wireshark, either as plugins, or built into the source. It can read hundreds of protocols, which can provide a deluge of data.

Viewing the raw information has its benefits, but users can filter and parse the captured data using a mouse click interface to create Boolean filters. Users can also create and save filters for later use. Wireshark supports built-in searches to hone in on specific data or conditions, and will even build I/O graphs to show usage by packet type [19].Wireshark is a versatile and flexible network protocol analyzer that can be extended using plugins and dissectors. Since it is open-source and freely available, it can be adapted to the needs of specific applications. Wireshark can be attached to local network interfaces, thereby overhearing incoming packets that are subsequently analysed and presented to the user. It allows to save packets into files for later analysis and to filter the displayed data. In addition, it allows colorizing the output to ease the interpretation [4].

One specific advantage of Wireshark is that multiple dissectors can analyze the same packet. If a UDP packet is found, the payload of the packet can be passed on to the next dissector for further analysis. This is especially helpful if IPv6 packets are wrapped in IEEE 802.15.4 frames. At the moment, Wireshark supports dissecting IEEE 802.15.4, Zigbee, IPv4, IPv6 and a large number of other protocols [16].

Its output can be exported for use by a variety of popular network analysis products, including Wild Packets Inc.'s Ether Peek and Airo Peek products, Cisco Systems Inc.'s Secure Intrusion Detection System, Microsoft's Network Monitor, Network General Corp.'s Sniffer, Novell Inc.'s LANalyzer, and various other tools using tcp dump's capture format including snoop and libpcap [19].

A. Key Features of Wireshark:

- Data can be captured from the wire from a live network connection or read from a file that recorded already-captured packets.
- Live data can be read from a number of types of network, including Ethernet, IEEE 802.11, PPP, and loopback.
- Captured network data can be browsed via a GUI, or Command Line.
- Captured files can be programmatically edited or converted via command-line switches to the "editcap" program.
- Data display can be refined using a display filter.
- Plug-ins can be created for dissecting new protocols.
- VoIP calls in the captured traffic can be detected. If encoded in a compatible encoding, the media flow can even be played.
- Raw USB traffic can be captured.[8]
- Open and Save packet data captured.
- Display packets with very detailed protocol information.
- Import and Export packet data from and to a lot of other capture programs.
- Filter packets on many criteria; So, it is not for layman as it involves a lot of network layer filtering options [13].
- Search for packets on many criteria.
- Colorize packet display based on filters.
- Create various statistics [18].

Here are some things Wireshark does not provide:

- Wireshark isn't an intrusion detection system. It will not warn you when someone does strange things on your network that he/she isn't allowed to do. However, if strange things happen, Wireshark might help you figure out what is really going on.
- Wireshark will not manipulate things on the network, it will only "measure" things from it. Wireshark doesn't send packets on the network or do other active things (except for name resolutions, but even that can be disabled) [18].

What sets Wireshark apart from most of these is that it is the most widely used, so it provides a larger number of supported protocols (more than 500) and has a user-driven support base that is unrivaled. The only thing the commercial products typically offer special is their ability to produce reports that are more suited to less technical users For the development of protocols, it is essential to have a good and powerful protocol analyzer at hand [18].

VII. COLASOFT CAPSA

Colasoft Capsa is a portable network analyzer application for both LANs and WLANs which performs real-time packet capturing capability, advanced protocol analysis, in-depth packet decoding, and automatic expert diagnosis. Capsa's comprehensive high-level window view of your entire network gives quick insight to network administrators or network engineers allowing them to rapidly pinpoint and resolve application problems. With the most friendly graphical user interface and the most powerful data packet capture and analysis engine in the industry [15].

Capsa assists the user in the specification and in the analysis of cryptographic protocols. It provides an editor for protocol specifications and offers a quick loading procedure for the protocols specified in underlying protocol libraries, and a convenient parsing procedure for user-defined protocol specifications. It gives us, the tool features of a graph management. This automatically generates and displays graphs. Capsa gives us a fully mechanized analyzer that verifies secrecy and authenticity properties on a given graph and displays the results. More precisely, Capsa allows for analyzing the security properties secrecy, weak authenticity, and strong authenticity [5].

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 4, Issue 3, March 2015

It diagnoses the network problems by detecting and locating suspicious hosts, causing the problem and alerts computer against network anomalies. Additional features include reports, logs, and diagnostic capabilities that can be used to discover network problems. One of the demerits of Colasoft Capsa is that it is quite expensive. Whereas, a free version is available with limited features [13].

Some advanced sniffing products (like Colasoft's Capsa Enterprise sniffer) are able to replay the contents of captured packets. These advanced sniffers may even allow you to edit the contents and retransmit the packets to the network.

Capsa can be scheduled to run capture periodically. And it also provides real-time and post-event application performance monitoring with alarms for problem identification. When the alarm is triggered, the emails notifications can be sent to the IT administrators. The Logging function is a quite useful feature for Capsa. It is used to monitor and audit user activities of DNS queries, SMTP and POP3 emails, FTP operations and Yahoo Messenger etc. All activity logs can be saved to files automatically. Even the content of each email sent or received can be saved as well. Another utility feature of Capsa is the valuable built-in tools, including MAC Scanner, Ping Tool, Packet Builder and Packet Player. All are simple but powerful. Colasoft Capsa offers other visual aids such as graphs and a matrix view in which all endpoints that communicate are connected.

We can summarize some Capsa's features:

A. Key Features of Capsa Enterprise:

- Real-time packet capture as well as the ability to save data transmitted over local networks, including wired network and wireless network.
- Identify and analyze about 300 network protocols, and Capsa Enterprise can identify more than 500 protocols, including VoIP, as well as network applications based on the protocol analysis.
- Identify "Top Talkers" by monitoring network bandwidth and usage through packet capture of transmissions over the network and providing summary and decoding information about these packets.
- Easy to use Overview Dashboard allows you to view network statistics at a single glance, allowing for quick interpretation of network utilization data.
- Internet e-mail and instant messaging traffic can be monitored and stored, helping identify security and confidential data handling violations.
- Suspicious hosts can be detected and diagnosed enabling you to pinpoint network problems in seconds.
- Map the 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 segment.
- Visualize the entire network in an ellipse that shows the connections and traffic between each host [15].

VIII. WIRESHARK VS. COLASOFT CAPSA

Colasoft Capsa offers many of the analysis features that are found in Wireshark. For example, both programs can display endpoints and protocols from the captured packets along with statistics on the amount of information sent and received for each. The difference is that Colasoft Capsa adds a visual interpretation to the statistics. Colasoft Capsa offers other visual aids such as graphs and a matrix view in which all endpoints that communicate are connected. Additional features include reports, logs, and diagnostic capabilities that can be used to discover network problems [21].

It is possible to view related packets in Colasoft Capsa by right-clicking a packet and choosing an option from "Select Related Packets". This action will highlight packets related in the specified manner. Choosing "By Flow" from the related packets menu results in highlighting the packets that Wireshark glues together when selecting "Follow TCP Stream".

While this shows the related packets, Colasoft Capsa does not show all packets of a stream in one window as Wireshark does. Other relations for grouping packets in Colasoft Capsa include by source, destination, or protocol.

Colasoft Capsa supports most of the features of Wireshark with powerful TCP flow analysis and its easier interpretation. It has versatile network traffic, bandwidth and utilization analysis. It has in-depth packet decoding feature with multiple network behavior monitoring. It has a matrix representation and eclipse visualization of the network.

Colasoft Capsa extends the network security analysis with notifying alerts only by email and audio. A disadvantage of Colasoft Capsa is that, it works only on windows platform. Further, it covers only about 300 protocols which is very less when compared to Wireshark’s 1100 protocols [13].

Capsa Free is a great combination of powerful monitoring, in-depth packet decoding, reliable network diagnosing, real-time alerting and thorough reporting ability, it provides you innovative solutions to numerous network problems.

Compared with Wireshark, Capsa free has a more friendly Windows 7 style, it provides more visibility as to the status of your network, and it is an simple graphic network analyzer. There no need to worry about those command, you can do everything by clicking the mouse.

Without a doubt, Capsa is a user-friendly program. Even if you don’t know much about the IP stack, you can learn a lot about what’s happening on your network with Capsa. It presents data in a very easy-to-read way. The Graphs tab shows some great visualization of various network statistics.

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 4, Issue 3, March 2015

Table 1 summarizes the properties of Wireshark and Colasoft Capsa:

TABLE 1

No.	Property	Wireshark	Colasoft Capsa
1	OS supported	Windows and Unix	Windows
2	Disk usage	81 MB (Windows) & 449MB (Unix)	32 MB
3	Cost	Free	$999
4	Open source	Yes	No
5	No. of protocols	More than 1000	300
6	Libpcap based	Yes	No
7	Multiple interfaces at a single instance	No	Yes
8	Alarms on traffic, protocol	No	Yes
9	User interface	GUI and CLI	GUI
10	Decode protocol (Hex, ASCII, EBCDIC)	Only Hex and ASCII	Yes
11	Identify abnormal protocol	No (only creates a warning)	Yes
12	Identify packets with forged data	Yes	Yes
13	Display protocol in OSI 7 layers structure	Yes	Yes
14	Locate hosts running a specific service	Yes	Yes
15	Network communicatio n in matrix map	No	Yes
16	Evaluate critical business traffic and non-business traffic	Yes (by creating filters)	Yes (inbuilt)

Wireshark and Colasoft Capsa have similar characteristics. Hence, there is a need to find out distinct parameters which may define the internal load and performance of the tool.

Dr. Charu Gandhi "the assistant professor in the department of computer science of JIIT, Noida" and four of his students have tested some parameters to compare between packet sniffing tools, by applying same scenario for them.

The result is as follows:

A. Packet size distribution

Long packets increase load on the network which means less the long packets, less will be the stress on network. Further, dealing with long packets means dealing with high ratio of packet payload and packet headers. After applying the scenario of the experiment, it is seen that the average length packet size measured in Wireshark is 558.76 B and in Colasoft Capsa is 434B; which means that Colasoft Capsa gets a slight edge over Wireshark. Hence, Colasoft Capsa neither stresses the network nor does it stress the system by sending too many small sized or medium sized packets.

B. Throughput (bits per second bps)

Throughput is the amount of data processed by the system in a second. It is seen that Colasoft Capsa has large range of throughput and is changing swiftly. These random changes in the throughput are not good as it hinders the systems performance and is not good with respect to a network performance. Whereas, Wireshark is ranging in a pattern which is good for the network and shows a constant behavior.

The average bps in Colasoft Capsa is 6.34 Kbps whereas in Wireshark it is 115.398 kbps as we know more the bps, better would be the packet sniffer's performance. Hence, here Wireshark has an edge over Colasoft Capsa due to constant variation and not showing high cut- offs.

C. Packets per Second (PPS)

Packets per second refer to the number of packets transferred in one second. It is seen clearly that Wireshark has lesser packet loss than Colasoft Capsa and hence is preferred over Colasoft Capsa for less packet retransmissions.

D. Response Time

Response time means the length of time taken to respond a given event. Hence, lesser the response time, better the performance. It can be seen after applying the experiment that the response time of Colasoft Capsa is much higher than Wireshark. Hence, in this benchmark too, Wireshark is better than Colasoft Capsa.

The previous experiment shows that none of the tool leads all the parameters. On the one hand, Colasoft Capsa has maximum network security. The present study has been made to suggest best packet sniffing tool, according to the user's requirements.

The advantages and disadvantages would help to develop a new packet sniffer which could hide all the disadvantages of the most used packet sniffers and could outperform them on quantitative and qualitative parameters [13].

DOI 10.17148/IJARCCE.2015.43113

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 4, Issue 3, March 2015

Table 2 summarizes the previous results:

TABLE 2

No.	Case	Best Tool
1	Packet Drop	Wireshark
2	Network Security	Colasoft Capsa
3	Response Time	Wireshark
4	Network Alarms	Colasoft Capsa
5	Throughput (bps)	Wireshark
6	Packet Size	Colasoft Capsa
7	PPS	Wireshark
8	User Interface	Colasoft Capsa
9	Number of Protocols	Wireshark
10	Network Communication	Colasoft Capsa

In my point of view, Wireshark and Capsa are both very powerful and popular packet sniffing tools. But Colasoft Capsa has more user friendly interface and the data in an extremely easy-to-read manner, especially when talking about the graphs and matrix that can be readable from the managers that are not network specialist, which is considered as one of the most advantage of Capsa. Moreover, when talking about network analyzing, both Wireshark and Capsa can auto-detect network errors, but Capsa provides more detailed information on reason and resolution to help resolve errors.

IX. CONLUSION

Maintaining a safe and efficient workplace requires organizations to monitor the employees' computers at workplace. Employees must be educated about monitoring so that they can understand the lack of privacy that currently exists at work as well as to understand the capabilities and limitations. Employers who monitor must be responsible and reasonable. They must explain to workers what they monitor.

As the law slowly catches up with technology, many questions remain. Privacy advocates will likely continue to push for reforms that would offer greater protection for employees.

Although some people and organizations believe that employee monitoring is wrong or unethical, there is a clear need for such practice. Employee monitoring is here to stay. The status of employee monitoring may change if laws tailor to the always-changing computer technology - but employee monitoring will not go away.

In this paper, we studied the problem of Internet usage by employees in the organizations for personal purposes and the need for some kind of network sniffing tool in the workplace to keep watchful eyes on any computer abuse in the organization.

We explore network monitoring as a sniffing tool used by network administrator in the organization and the ethical issue concerning this kind of surveillance. Packet sniffer is not just a hacker's tool. It can be used for network traffic monitoring, traffic analysis, troubleshooting and other useful purposes.

There are many tools which are used for network traffic sniffing but there are some limitations regarding these packet sniffing tools i.e. some tools are only used for packet capturing without any kind of analyzing them. Some tools trace IP packets and some tools only capture TCP packets. At the end, we concluded that with these tools, we can do intrusion detection and penetration testing against particular network. Two packet sniffers are tested, Wireshark and Colasoft Capsa. A comparison based on their features and weakness had been made. Each software has its weakness and strength, and each of them has been designed for some purposes in mind. Capsa is more practical, user friendly and provides more detailed and readable information, whereas Wireshark is more powerful.

REFERENCES

[1] C. Sanders, Practical Analysis Using Wireshark to Solve Real-World Network Problems, 2nd ed., W. Pollock, USA, 2007.
[2] T. Dean, Network+ Guide to Networks, 6th ed., D. Garza, S. Helba, Nelson Education, Canada, 2013.
[3] A. Orebaugh, Wireshark and Ethereal: Network Protocol Analyzer Toolkit, A. Williams, Canada, Syngress, 2007.
[4] K. Hassan, A. Ahsan, and M. Rahman, "IEEE 802.11b Packet Analysis to Imrove Network Performance", in JUJIT, 2012, Vol.1, p. 27-34.
[5] P. Asrodia, H. Patel, "Analysis of Various Packet Sniffing Tools for Network Monitoring and Analysis", in IJEECE, 2012, paper 2277-2626, p. 55-58
[6] D. Shinder (2005) Ethical-Issues-IT-Security-Professionals homepage on windowsecurity. [0nline]. Available: http://www.windowsecurity.com/articlestutorials/misc_network_security/Ethical-Issues-IT-Security- Professionals.html
[7] S. Venkatramulu, C. V. Rao, "Various Solutions for Address Resolution Protocol Spoofing Attack", in IJSRP, 2013, 2250-3153.
[8] S. Suri, V. Batra, "Comparative Study of Network Monitoring Tools", in IJITEE, 2012, paper 2278-3075, p. 63-65.
[9] J. Yerby, "Legal and Ethical issues of employee monitoring", in OJAKM, 2013, Vol. 1, Issue 2, p. 44-55.
[10] G. S. Alder, M. Schminke, T. W. Noel, and M. Kuenzi, "Emplyee Reactions to Internet Monitoring: The Moderating Role of Ethical Orientation", in JBE, 2008, paper 10.1007 , p. 481-498
[11] [online]: http://www.wisegeek.org/how-do-employers-monitor-internet- usage-at- work.htm#didyouknowout
[12] S. Ansari, R. G. Rajeev, H. S. Chandrashekar, "Packet Sniffing: A Brief Introduction", in IEEE, 2003, paper 10.1109, p. 17-19
[13] C. Gandhi, G. Suri, R. P. Golyan, P. Saxena, and B. K. Saxina, "Packet Sniffers- A Comparative Study", IJCNCS, paper 2308-9830, p. 179-187.
[14] R. Spangler, "Packet sniffer Detection with Antisniff", University of Wisconsin-Whitewater, department of Computer and Network Administration, 2003.
[15] [online]. Available: http://www.colasoft.com
[16] W. B. Pottner, L. Wolf, "IEEE 802.15.4 Packet Analysis with Wireshark and off-the-Shelf Hardware", in Proc. SICNSS, 2010.
[17] U. Banerjee, A. Vashishtha, and M. Saxena, "Evalualtion of the Capabilities of Wireshark as a Tool for Intrusion Detection", in IJCA, 2010, paper 0975-8887.
[18] [online]. Available: www.wireshark.org
[19] [online]. Available: www.spamlaws.com
[20] S. Dhar, "Switch Sniff", in LJ, 2002, paper 5869, p. 0-1.
[21] [online].Available: ttp://securitymusings.com/article/1161/colasoft-capsa-vs-wireshark