iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 4 **Issue:** IX **Month of publication:** September 2016

DOI:

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

Volume 4 Issue IX, September 2016
ISSN: 2321-9653
International Journal for Research in Applied Science & Engineering Technology (IJRASET)

Digital Forensics: Analyze and Monitor Network Traffic Using Sniffer (Application Software)

Neeraj[1], Sonal Beniwal[2]
[1]PG student, [2]Assistant Professor

Abstract: ***Digital forensic is the process of interpreting and uncovering electronic data. The goal of process is to preserve any evidence in its most original form while applying performing a structured investigation by collecting, identifying and validating the digital information for the purpose of reconstructing past events. This dissertation will discuss the need for network forensics to be practiced in legal and an effective way. In this study also confer types of digital forensics and also prevention ideas from online fraud, social networking crime etc. IDS stand for intrusion detection system is a technique by using of we can monitor our network traffic and also take control over suspicious activity and alter the administrator or the network. In this dissertation I also try to define how computer may communicate with each other as well as how they share resources and using same internet. This paper defined types of intrusion detection system and did practical implementation on packet transmission in order to sniff bad data packets and take control over transmission between computers which share resources. The full implementation of the sniffer application software that captures network data as well as provides sufficient means for the decision making process of an administrator. The aim of this application is to rewrite C# language sniffer into .Net, and also develop an application that consumes little memory on the hard disk.***

Keywords: IDS, sniffers, packet transmission, analyze network traffic.

I. INTRODUCTION

With the use of accurate and well understood methodologies to providing accurate information has always been the goal of traditional forensics analysis. Forensic science applied in courts of law has sought to use commonly applied technique and tools only after rigorous, repetitive testing and through scientific analysis. This dissertation focused on three major areas in which forensic analysis is currently being employed in some form. In table shows these areas, associated with primary and secondary objective of forensic analysis as well as the environment required for any analysis to be of use in supporting the primary objective.

Table1. Forensics in different area.

Area	Primary objective	Secondary objective	Environment
Law enforcement	Prosecution		After the fact
Military IW operation	Continuity of operation	Prosecution	Real time
Business & industry	Availability of service	Prosecution	Real time

Investigators employ a different paradigm for each area when performing analysis. That is, law enforcement can't act until there is sufficient reason to believe that a crime has occurred. All these areas in above table mentioned are necessary to achieve total security for our nation, and all are actively pursuing forensic solution to meet their disparate investigative goals toward that end. Similarly, practitioners working in each area have different perspectives about what digital forensic research must offer. As shown in figure to be effective, fundamental digital forensic research must provide suitable solutions with the widest possible applicability to homeland security. To do that the focus must be the foundation science at the root of the technologies we aim to analyze

Fig1. Digital Forensic research areas.

Digital forensics is a relatively new science. Definition of digital forensics more expanded to include the forensics of all digital technology like mobile data investigation, network investigation, data base forensics as well. In simple words we can say a computer forensics is defined as "collection of techniques and tools used to find evidence in a computer". Digital forensics has been defined as the "use of tools and techniques to scientifically derived and proven methods towards the preservation, collection validation, identification, analysis, interpretation, documentation, and presentation of digital evidence which is derived from the digital sources for the purpose of facilitation or furthering the reconstruction of events found to be criminal, or helping to anticipate unauthorized actions shown to be disruptive to planned operations". Digital forensics has become prevalent because law enforcement recognizes that modern day life includes a variety of digital devices that can be exploited for criminal activity. While computer forensics tends to focus on specific methods for extracting evidence from a particular platform, like computer system, laptop etc. but digital forensics must be included all types of digital evidence such as pen drive, network data, mobile data, system penetration testing as well. Unfortunately, there does not exists a standard digital forensics methodology, but rather a set of procedures and tools built from the experience of law enforcement, system administrators, and hackers.

The past years have seen a rise within the importance of pc networks for several tasks in daily life. Network services square measure crucial for several business work-flows and become additional vital for the non-public life driven by new services reminiscent of social networks or on-line video streaming portals. Because they want for network service availableness will increase, operators see a growing want for understanding this state of their networks. Watching techniques for detective work network failures, attacks on finish systems, or potential bottlenecks that would be mitigated by careful network improvement receive additional attention within the analysis and profession. Several current traffic analysis systems use deep packet review (DPI) so as to investigate network traffic. These systems embody intrusion detection systems, code for network traffic accounting, traffic classification, or systems for watching service-level and ISP networks, however, rework the method of inspecting traffic payload into a difficult task. A traffic analysis setup must be properly designed so as to satisfy the challenges exhibit by traffic volumes in current high-speed networks. This treatise evaluates the performance of current packet capturing solutions of normal operational systems on goods hardware. We have a tendency to determine and make a case for bottlenecks and pitfalls inside the capturing stacks, and supply tips for users on the way to set up their capturing systems for best performance. What is more, we have a tendency to propose enhancements to the operational system's capturing processes that scale back packet loss, and judge their impact on capturing performance. Counting on the machine complexness of the specified traffic analysis application, even the best-tuned capturing setups will suffer packet loss if the used hardware is brief in obtainable machine resources. We have a tendency to address this downside by presenting and evaluating new sampling algorithms which will be deployed before of a traffic analysis application to scale back the number of inspected packets while not degrading the results of the analysis considerably.

II. TYPES OF DIGITAL FORENSICS

There are at least three distinct communities within digital forensics law enforcement, Military, Business & Industry. The technical aspect of an investigation (digital forensics) is divided into several sub-branches, relating to the type of digital devices involved; computer forensics, network forensics, forensic data analysis and mobile device forensics. The typical procedure of any digital forensics is forensic imaging and analysis of information that captured from storage medium of system or device and the production of a report into collected evidence. As well as in digital forensics process identifies sources, confirm alibis or statements and authenticate documents.

A. Computer Forensics

computer forensics science is a branch of digital forensic science pertaining to found the evidence in digital storage media of computer. To examine digital media in a forensically sound manner with the aim of finding the evidence is the goal of computer forensics. Computer forensics is applied with the aim of identifying, preserving, recovering, analyzing and presenting facts and opinion about the digital information. A wide variety of computer crime is associated with the investigation; computer forensics may also be used in civil proceedings. In computer forensics involves some tools and techniques to find the evidence but with additional guidelines and practices designed to create a legal audit trail. These guidelines and rules are also applicable on other digital forensics like network forensic, data base forensics and mobile forensics as well. It has been used in a number of high-profile cases and is becoming widely accepted as reliable within U.S. and European court system.

B. Mobile Forensic

Mobile phones are today's mostly used device for personal as well as organizational purpose for computation. These devices are

useful in number of fields such as managing information like contact details and appointments, and communication or we can say convey message electronically does not matter how far receiver is, and mobile phones are also accumulate a sizeable amount of information about the owner. Whenever mobile devices are used to do a crime there are several tools to investigate the mobile phone data. Mobile phones are also used to investigate the current and last location of the device. So that we can say a mobile phone is play an important role to find out the bad crooks or criminal.

C. Network Forensics

Analysis of network events, record and capture in order to find out the source of security attacks in a particular network as well as investigate a network to find out other problem incidents.(the term, attributed to firewall expert Marcos Ranum, is borrowed from the legal and criminology fields where forensics pertains to the investigation of crimes). According to SimsonGear finkle, author of several books or security networks forensics system can be one of two kinds.

"Catch it as you can"

"Stop-look and listen"

D. Data Base Forensics

Data base forensics is another branch of digital forensics relating to the forensics study of database and their metadata. In data base investigation log files are investigate and RAM memory of system to build a timeline or recover relevant information. In data base forensics process first of all Meta data is investigate because Meta data is data about data so that investigator can get idea of the entire database by investigate the Meta data. Then collect the information from the several addresses where sensitive information has been saved. Importance of data base forensics is it is used to investigate the critical and sensitive information.

III. RESEARCH METHODOLOGY

The sniffer is written in .Net unlike the other Sniffers that are written in C# language The primary motivation of this language was the need for a platform-independent (i.e., architecture neutral) language that could be used to create software to be embedded in various consumer electronic devices. .Net is a programmer's language that is cohesive and consistent, except for constraints imposed by the Internet environment, .Net gives the programmer, full control. Finally, .Net is to Internet programming where C was to system programming. It captures packet, size of the packet, the source and destination machine IP addresses which are involved in the packet transferring. It shows this process in graphical manner and the working of different layers. It gives complete information about the captured packets; like which layers are involved and which protocols are in use at a particular time. Finally, it has a facility to store the information of the packets.

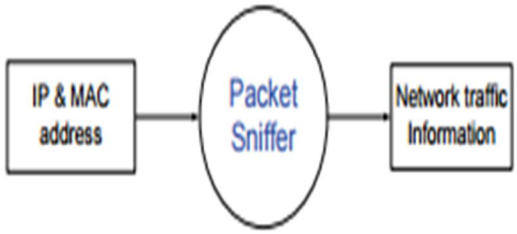


Fig2. *Level 0 DFD.*

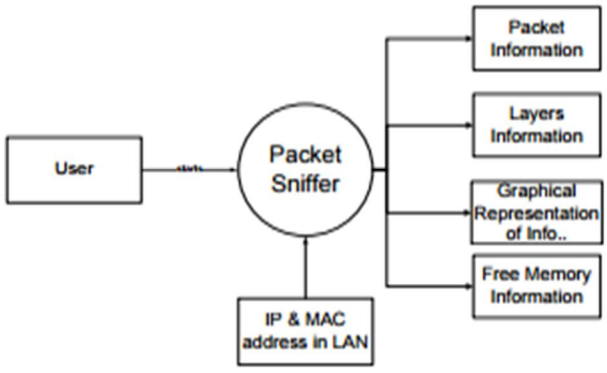


Fig3. *Level 1 DFD.*

Component Diagram A component diagram depicts how components are wired together to form larger software systems. Components are wired together by using an assembly connector to connect the required interface of one component with the provided interface of another component. An assembly connector is a "connector between two components that defines that one component provides the services that another component requires. An assembly connector is a connector that is defined from a required interface or port to a provided interface or port."

Volume 4 Issue IX, September 2016
ISSN: 2321-9653
International Journal for Research in Applied Science & Engineering Technology (IJRASET)

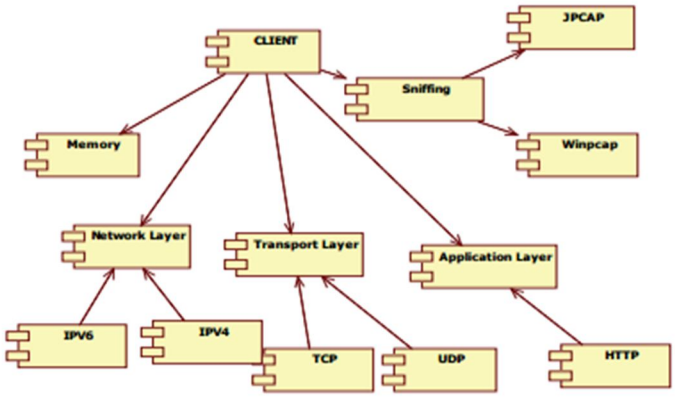


Fig4. *Component of a sniffer*

IV. ARCHITECTURE OF PROPOSED WORK

The design of the proposed system discusses the various requirements that will make up the application. By conducting the requirements analysis we listed out the requirements that are useful to restate the problem definition.
Analyze network Layer.
Analyze Transport Layer.
Analyze Application Layer.
Analyze UDP Protocol
Analyze TCP Protocol
Analyze HTTP Protocol
Analyze Free Memory Size
Find out the Packets over network.

Types of Intrusion Detection System:
Host based IDS
Network based IDS
The Features of Sniffer is a customized software application that has a number of features. These features enable: Administrators to show statistics of received packets. With the help of sniffer we can detect malicious IP addresses according to its number of ARP requests in previously specified time. Network administrator to view all network interfaces and enable them to capture data from that interface and consequently save captured packets. Administrators generate reports that aid effective and efficient decision making. The sniffer is developed in .Net. This application is designed into five (5) independent modules which take care of different tasks efficiently.
User Interface Module.
Packet Sniffing Module.
Analyze layers Module.
Free Memory Module.
Protocol Analysis Module.

User Interface Module Actually every application has one user interface for accessing the entire application. The user interface for the sniffer application is designed completely based on the end users. It provides an easy to use interface to the users. This user interface has an attractive look and provides ease of navigation. Technically, the swing is used in core .Net for preparing this user interface. Packet Sniffing Module This module takes care of capturing packets that are seen by a machine's network interface. It grabs all the packets that go in and out of the Network Interface Card (NIC) of the machine on which the sniffer is installed. This means that, if the NIC is set to the promiscuous mode, then it will receive all the packets sent to the network.
Analyze Layers Module This module contains the code for analyzing the layers in the system. Mostly in this module we have to discuss about three layers Transport layer, Application Layer, Network Layer. The module shows the graphical representation of the

usage of different layers in packet capturing time. It can show the graph in two manners like line graph and pie graph. Free Memory Module This module analyzes computer memory usage at the time of packet capturing. It can show the memory size in number format as well as graphical representation. Protocol Analysis Module This module analyzes the protocols of the layers. Like Transmission Control Protocol (TCP), User Datagram Protocol (UDP), Hypertext Transfer Protocol (HTTP) etc. It can show the source port, destination port and packet length of the system of each protocol.

V. SNIFFER COMPONENTS

A sniffer can be divided into several components. Or we can say it is a combinations of different components.

Hardware when we are working with sniffer, hardware is required sometimes for analyzing hardware problems like voltage problems, cable problem.

Drive Program this is main component of sniffer, each sniffer contain its own drive program. Using this we can capture traffic in network and filter it to restrict data.

Buffer a buffer is a storage device for captured data from network. In general, there are two types of buffer used. First one is where data captured continuously and second one where new packets replace old packets.

Packet Analysis Packet analysis can be done on real time or we can analyze packets after storing it. We can analyze both header and actual data, when we store data in memory or we perform real time analysis, decoder is used to decode the data store in packets. Problems.

VI. CONCLUSION AND FUTURE SCOPE

Compared to similar works this application shows the layer involved in sniffing and the protocols. This Sniffer would be installed on a collision domain that makes use of the switch rather than the broadcast domain (HUB). The collision domain would be used since the use of HUBS in network setting is gradually reducing due to its broadcasting nature. Sniffer has a very rich and user friendly GUI developed in .NET Technology. Thus it is totally easy to use. With .NET, the most considerable advantage is platform independence; therefore sniffer is also platform independent. The installation file for sniffer is only 587 KB, so it is highly economical in terms of memory use and because it is based on object-oriented design, any further changes can be easily adaptable.

It is not possible to develop a system that meets all the requirements of the user. User requirements keep changing as the system is being used. Some of the future enhancements that can be done to this system are:

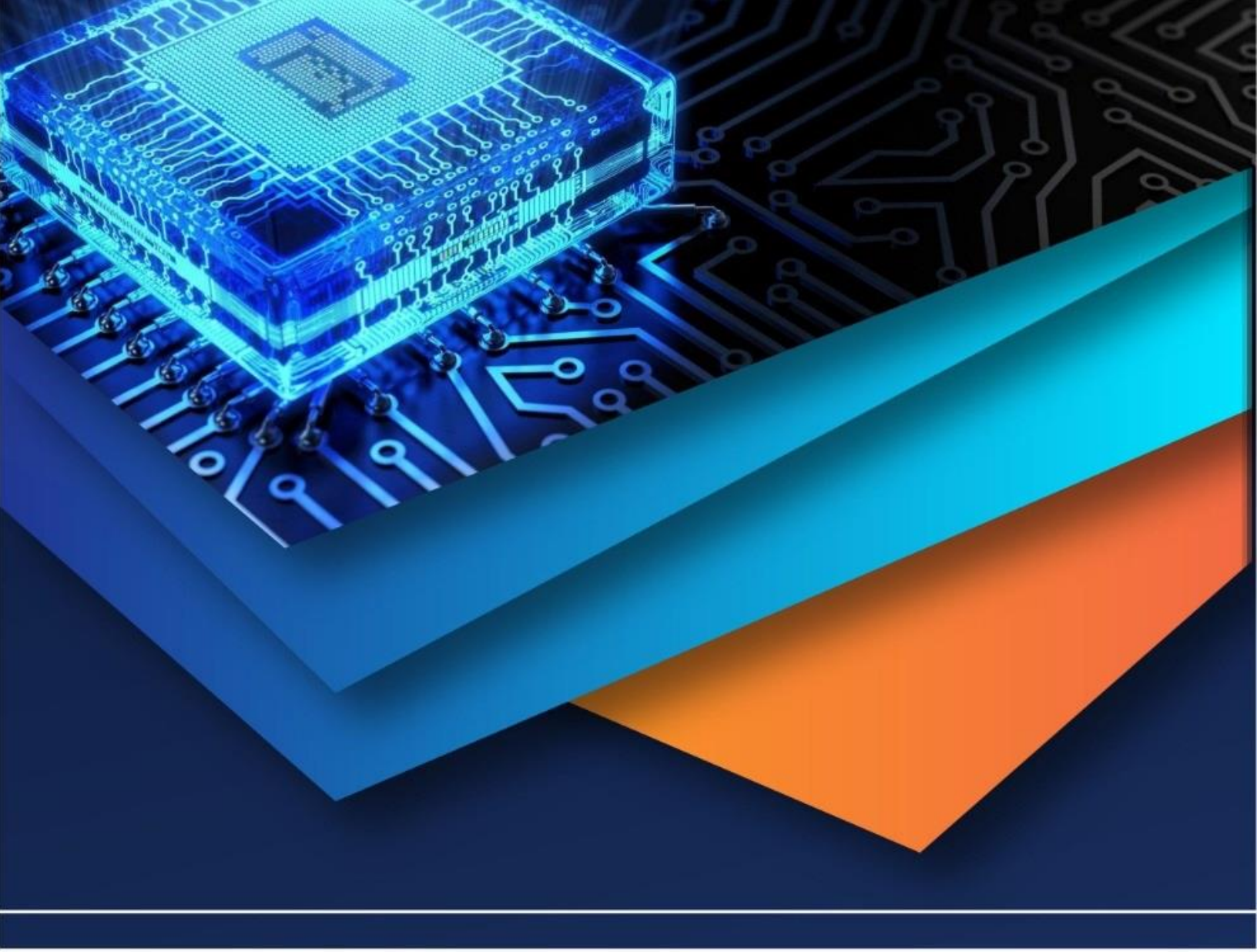
As the technology emerges, it is possible to upgrade the system that can be adaptable to desired environment.

The present application is a standalone application, i.e. only in intranet. So we have chance to extend this in internet.

Based on the future security issues, security can be improved using emerging technologies.

REFERENCES

[1] McCanne, S. and Jacobson, V., The BSD Packet Filter: A New Architecture for User-level Packet Capture, 12 1992.
[2] Hwu, W. and Kirk, D., Ece 498 al programming massively parallel processor textbook, 2006-2008.
[3] NVIDIA, NVIDIA CUDA Programming Guide 2.3, 4 2009.
[4] University of Minesota., Minnesota Internet Traffic Studies (MINTS), 2008.
[5] Omnipeek, http://www.wildpackets.com/products/network_analysis/ omnipeek_network_analyzer.
[6] IEEE, IEEE 802.3 LAN/MAN CSMA/CD (Ethernet) Access Method, 2008.
[7] IEEE, IEEE 802.11 LAN/MAN Wireless LANS, 2007.
[8] Zhang, H., Ma, J., Wang, Y. and Pei, Q., an Active Defense Model and Framework of Insider Threats Detection and Sense, 2009.
[9] Doss, G. and Tejay, G., Developing Insider Attack Detection. Model: A Grounded Approach., 2009.
[10] Anderson, J. P., Computer Security Threat Monitoring and Surveillance, 1980.
[11] Denning, D. and Neumann, P., Requirements and Model for IDES A RealTime Intrusion Detection Expert System. Final report., 1985.
[12] Wikipedia, Timeline of computer security hacker history, http://en.wikipedia. org/wiki/Timeline_of_computer_security_hacker_history, 2009.
[13] Chen, W. W., Statistical Methods in computer security, 2005.
[14] Wang, Y., Statistical techniques for Network security, 2009.
[15] Bejtlich, R., The TAO of network security: Beyond Intrusion Detection, 2004.
[16] Wang, Kim, Mbateng, Ho et al., A latent class modeling approach for anomaly intrusion detection, 2006.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY