TEST Engineering & Management

*January - February 2020*
*ISSN: 0193 - 4120 Page No. 11672 - 11678*

# Design and Implementation of Net-Fore-Tool for Cyber Crime Analysis

Jagadeesha.G.M[1], Dr.Kotrappa.Sirbi[2], Dr. Veeragangadhara Swamy.T.M[3]
[1] *Rao Bahadur Y Mahabeshwarappa Engineering College, VTU, Belagavi*
[2] *KLE's Dr.M S Sheshgiri College of Engineering and Technology, VTU, Belagavi*
[3] *Rao Bahadur Y Mahabeshwarappa Engineering College, VTU, Belagavi*
*jagadeesh4886@gmail.com*

***Article Info***
***Volume 82***
***Page Number: 11672 - 11678***
***Publication Issue:***
***January-February 2020***

***Article History***
***Article Received****: 18 May 2019*
***Revised****: 14 July 2019*
***Accepted****: 22 December 2019*
***Publication****: 21 February 2020*

**Abstract**
The prime objective of Net-Fore-tool is to create a Analysis and Monitoring Networking tool, a security analysis tool for network modeling and discovery. Net-Fore-tool based on effective model for the network which is also designed for all the layers of the network. With the following data, the Forensic Investigator requires very less time to take appropriate action in case of threat. The tool captures packets from the LAN. The packets are classified based on the protocol. The tool displays the connection statistics and packet statistics. If unsecure data transmission is going on, the user of the tool will also get to know address of the origin and destination address and the payload of each packet that is captured. Using packet header, it determines the IP Address and then resolves Host name. It also shows the topology of the active users i.e. who are involved in data transmission.
The research work is developed using Java Programming Language. Swings are used for User Interface. We use WinPCap and Jpcap API for capturing packets.

***Keywords:*** *Cyber crime forensic, WinPcap, Jpcap, Network Monitoring and Analysis tool.*

## 1. Introduction

Depending on the infrastructure of the network, it can be classified as a public network or a private network. Telecommunication administration or a recognized private operating agency will establish and operate a public network and provide services for the users. A private network used and built with organization computers and dedicated telephone lines is named as private network.

If the rented lines are available ,it gives security to Private network, Information leak become difficult as no outsider can penetrate in to the network. The point of issue is with the cost of lines which are leased. Organizations want their data on to the public network because of the cost cutting. On the other hand they want security for the data. This concept lead to implementation of Virtual Private Network (VPN),

Forensic Investigator knows about the network being protected and this knowledge is gained using many network related tools. The outcome of one tool will be used as the input to other tool for analysis and to get statistics regarding the network traffic. This work comes with coordination of tool executions and is very complicated, which needs the coordination of the all the tools of their results is usually a rigorous job.

So, a tool is required that can monitor network and observe network traffic virtually.

### 1.1 Problem Statement

The problems dealt with in this research work are to get the statistics of the packets which are moving around the network and using this statistic with other parameters like memory and process analysis in cybercrime management system, forensic investigator can come to conclusion regarding the crime occurrence.

TEST Engineering & Management

*January - February 2020*
*ISSN: 0193 - 4120 Page No. 11672 - 11678*

### 1.2 Research work Objectives

**The following objectives will be achieved through this research work :**

1. Providing Network Monitoring and Analysis tool Comprehensive network model that is not limited to a specific network level
2. Developing a Platform, server and network inde-pendent tool.
3. Providing a tool that is platform independent, server independent and network independent

## 2. Literature Survey

- Christos Grantiids presents in his paper Experiment and Learn to Discover Networl Topology [1], the basic techniques and algorithms which can be used for the discovery of a compute network. In this paper , discovery of IP network were concentrated more and also considers th features for the detection of in detailed info (e.g data-link layer components). The technology an algorithms will be generalised and it will b applied for various networks with differen applications. Representing IP network is at graph with vertices are the numerous nodes an connections as edges, so that algorithms are able t discover different information (i.e. gateways subnet masks, etc)

- Bhandari and Ailawadhiv[2] categorized sniffin techniques into client side: where web page o sniffer uses java, script interpreted by user agent t web servers; server side where sniffer attacks fron server side using http communication protocol browser sniffing where websites and application are used to misinterpret html, etc. And ai malicious users steal private data; Content Sniffin where alteration is made in the stream of byte which changes the format of the file to maliciou contents; Password sniffing aims to crac passwords and login information saved in dat packets.

- Xinming Ou [3] describes a network security analysis approach called logic-programming, due to software exposures, poor security measures,many attacks will be executed on the network like multi host attack ,misconfiguration attack etc. to do the analysis on these attacks,he proposed an efficient methodology to over come the problem using logic-programming approach. Analysis of the vulnerability for multihost, multistage will be done using an off-the-shelf logic-programming engine which assess Datalog competently. Datalog is effective and accurate technique compared with earlier methods.

- Frédéric Massicotte, Tara Whalen, and Claude Bilodeau [4] in their work, proposes a tool for Security Investigation and Network Mapping at Real-Time. intrusion detection systems will be used with the prototype network mapping at real-time to provide security. This tool will be used for identification of logical and physical connectivity of hosts in the network.
- Ritinder Kour [5] in his work proposes a methodology of ethical hacking to capture all the incoming and outgoing packets in between the hosts in the network. This job will be done by packet sniffer tool.
- Richard A kemmerar [6] proposes a paper, the modeled information is managed by using a suite of composable network tools that can determine various aspects of network configurations through scanning techniques and heuristics. Tools in the suite are responsible for a single, well-defined task. Each tool has an abstract specification of the input, the output, the type of processing, and the requirements for carrying out a task. Tool descriptions are expressed in a Network Tool Language. The tool descriptions are then stored in a database. By using the network model and the tool descriptions, NetMap is able to automatically determine which tools are needed to perform a particular complex task and how the tools should be scheduled to obtain the requested results.
- http://www.wisegeek.org/how-do-employers - onitorinternet- usage [7], Internet surveillance and desktop surveillance are the two basic types of ad-

*January - February 2020*
*ISSN: 0193 - 4120 Page No. 11672 - 11678*

ministrator 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.

- Talekar, Tidake, & Shinde [8] designed a network sniffer with data mining techniques. Their network sniffer differs from the previous existing IDS because it automatically detects the type of the user such as normal user, spy, unauthorized user, and intruder from the network traffic graph. The system can be used as a utility for anti-hacking, Mobile Agent, LAN monitoring as well as for controlling the entire network.
- Von, Wulf, Schröder, & Wolf [9] offered a real time UWB sniffer , custom application software has been developed On the PC which is proficient of identifying the captured incoming and outgoing packets in the network. Collected packets are also forwarded to an open source packet sniffing software named Wireshark.

## 3. Methodology

This research work produce a tool that can monitor the network and give analyzed data to the Forensic investigator for taking quick and effective decision to control and check insecure transactions. The tool should be able to determine:

1. The protocol used in the transaction over the network
2. The type of packets those are being transferred, i.e. encrypted or decrypted
3. The servers and hosts topology.
4. The Domain name of the server and the IP address.
5. Packet statistics.

The intended tool shall include the capability to discover the active node and provide their IP address, the protocols supported and the network topology with a graphical representation for the nodes in the network.

The proposed tool will perform the following operations:

1. Capturing the packets in transaction from the network.
2. Drawing connection and plotting networks i.e in the network traffic visualization, the hosts, servers and the connections will be represented by boxes and lines.
3. The secure and insecure transactions will be collected by the tool and represented at statistics table which includes the packets received and statistics of all the connections. The connection statistics can then be used by the Forensic investigators a measure of network security.

## 4. Design

This process is the first step in moving from problem domain to solution domain.

The components of the tool are:

- Server
- WinPcap
- Jpcap
- Net-Fore-Tool
- User Interface

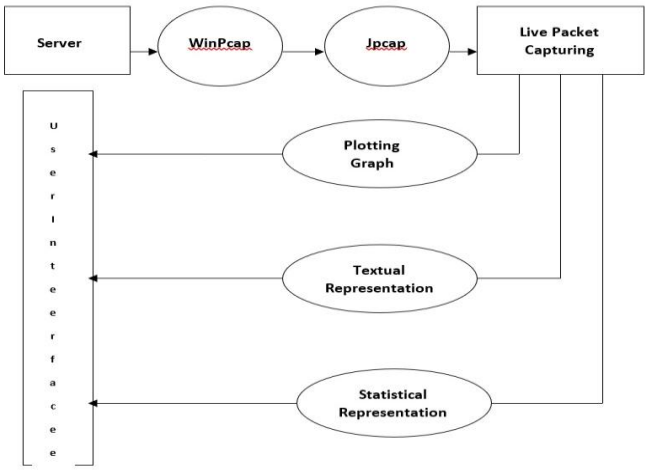


**Figure 4: Network Forensics Architecture with each element**

*January - February 2020*
*ISSN: 0193 - 4120 Page No. 11672 - 11678*

### 4.1. Server

A server is accepting a request from clients and provides services by sending back responses. A server application and also client application can run on same system or they can communicate from different systems on the network. Examples include file server, database server, VPN server, DHCP server, DNS server, WINS server, security server, domain controller, proxy server, firewall, etc.

### 4.2. WinPcap

Pcap is an application programming interface used for packet capturing in the network. The pcap implementation for the Windows operating system is called as WinPcap.

WinPcap is a free, open source software application which can used in windows for direct accessing of the network. All applications related to networking can access the systems through sockets. These application software can transfer data easily on the network.

The WinPcap provides many services on Win32 applications,

They are as follows

1. It will capture raw packets, which are moving from one system to another system in the network.
2. Gather statistical information related to network traffic.

### 4.3. Jpcap

Jpcap is a packet capturing application which captures sending and receiving packets dynamically in the network. It supports Ethernet, IPv4, IPv6, ARP/RARP, TCP, UDP, and ICMPv4. In order capture and generate HTTP data Jpcap will be modified to filter the packets so that HTTP packets are the only packets captured.

Jpcap is based on WinPcap and Raw Socket API. Therefore, Jpcap is supposed to work on any OS on which WinPcap has been implemented. Presently this packet capturing application has been tested on Microsoft Windows 2000/XP, Fedora Core 4, Linux RedHat 6.1, Solaris , FreeBSD 3.x.

The following types of packets supported by Jpcap : TCP, UDP, ARP/RARP, IPv4, IPv6 , Ethernet, ICMPv4 and Other types of packets are captured as raw packets (i.e., instances of the Packet class) which contain the whole data of the packets.

### 4.4. Net-Fore-Tool

Net-Fore-Tool is a Java tool to observe network traffic virtually. Forensic Investigators facilitate to monitor VPN (PPTP / IPSec / SSH) and SSL (HTTPS) connectivity of wire line/wireless networks. The diagrammatic representation makes it easy to display messages which is sent between computer nodes. Users can also read messages which is in plain text. Connection statistics is taken and analyzed the measure of network security. Main functional features of the Net-Fore-Tool on Private Networks

1. Capturing Packets
2. Drawing Connections
3. Plotting Network
4. Dumping Text
5. Collecting Statistics
6. Resolving IP Addresses

### 4.5. User Interface

The tool provides multiple screens (windows) to display information to the users. Java's Swing class technology, that provides different classes to create GUI components, is used for implementing user interfaces. The user interaction is provided by menu selection where a user can select different screens (windows) using a mouse where each window represents one type of information to the users.

TEST Engineering & Management

*January - February 2020*
*ISSN: 0193 - 4120 Page No. 11672 - 11678*

1. Graphical representation.
2. Textual representation.
3. Statistical Information.

## 5. IMPLEMENTATION

### 5.1. Modules

The system can be implemented in four modules:

1. IP address Resolution, Packet capturing and handling
2. Graphical Representation
3. Plain Text Representation
4. Statistical Information

#### 5.1.1. Module 1(IP address Resolution, Packet capturing and handling)

This module is responsible for resolving the IP address to hostname. It also gives the method for capturing packets and carries out operations on the packet received. The operations to be performed on the packets are finding the protocol to which the packets belongs.

#### 5.1.2. Module 2(Graphical Representation)

This module is responsible for the representation of the connection(s) of the node on which the administrator is logged in to with the server of the other network. It will also show the other servers to which the other network is connected. Color code may be used to represent the transaction and the protocols.

#### 5.1.3. Module 3(Plain Text Representation)

This module displays detailed text description of the packets whether the packets involved in transaction are secure or not. If packets are insecure then this module displays the contents of the packet.

#### 5.1.4. Module 4(Statistical Information)

This module keeps all statistics of connections and packets like the number of packets received from a connection and its type. This module also represents the number of packets sent by the individual servers. In addition to these it also gives the IP address of all the hosts that are in the path of the connection. It gives the domain name of the servers if they are not hidden.

## 6. Results and discussions

### 6.1. Case 1

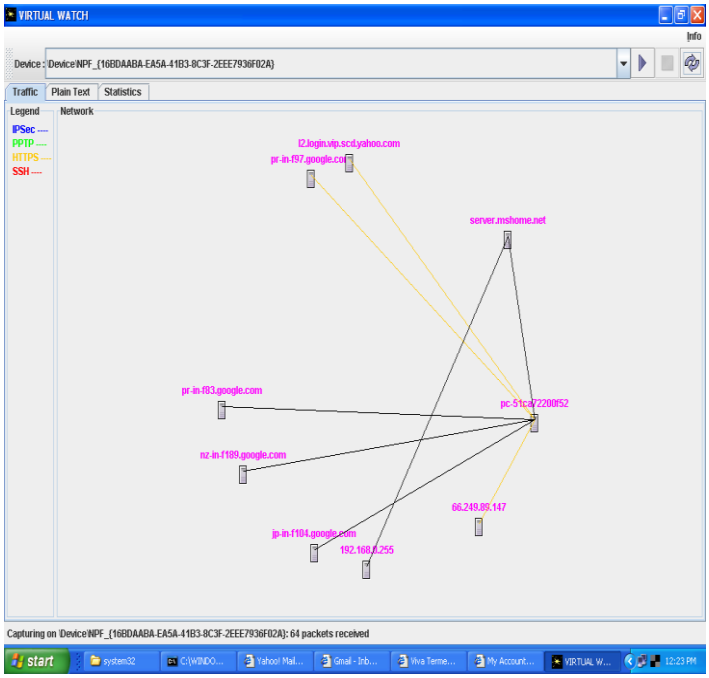


**Figure 6.1: Traffic Panel**

Figure 6.1 shows the Graphical Representation of hosts involved in transaction and protocols used represented by different colors.

TEST Engineering & Management

*January - February 2020*
*ISSN: 0193 - 4120 Page No. 11672 - 11678*

### 6.2.Case 2

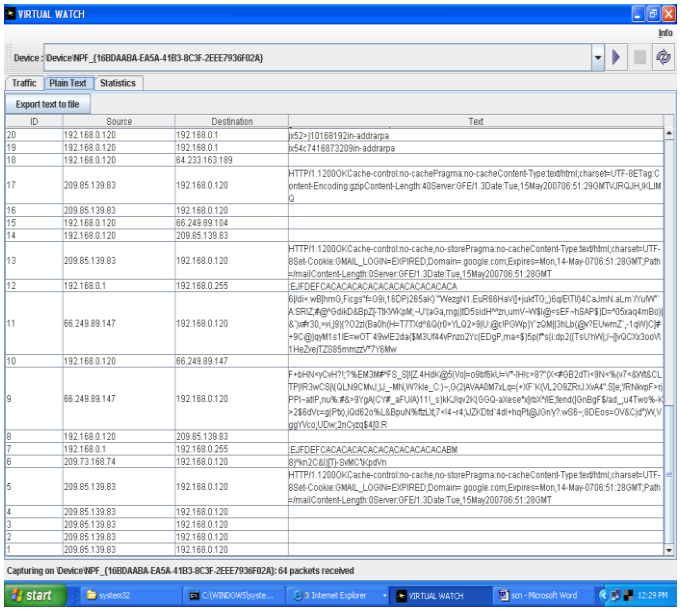


**Figure 6.2: Plain Text Panel**

Figure 6.2 shows the Textual representation of hosts involved in transaction and packet contents if unencrypted.

### 6.3. Case 3

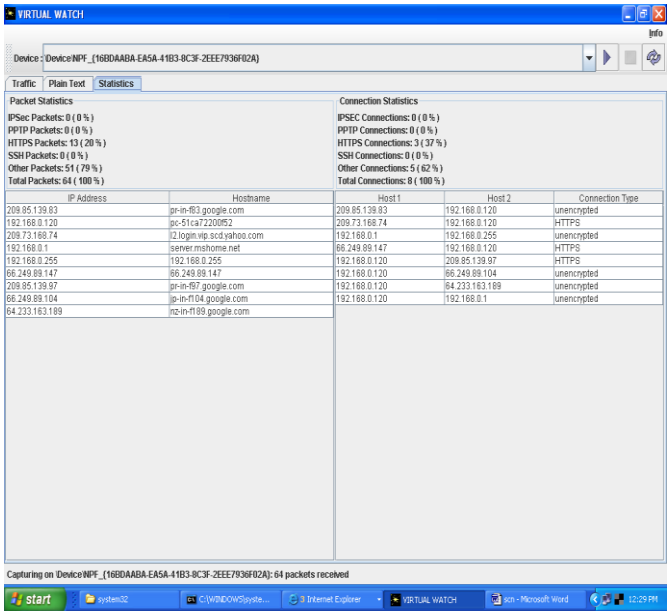


Figure 6.3: Statistics Panel

Figure 6.3 shows the Statistical information of hosts and transactions. The Statistics involve Packet Statistics, Connection Statistics, IP Address and the host names of various entities involved in the transaction.

## 7.CONCLUSION

The forensic investigator will be granted with the overall control of network traffic. If any unauthorized data transforming takes place, then the forensic investigator can observe the communication and take necessary action. Through this tool, the Forensic investigator is equipped with the statistics of the data transaction at the specified network .The tool consist of effective GUI to use and to do analyses and decisions on abnormal operations at the network groups.

## 8.References

[1] *Christos Gkantsidis, "Experiment and Learn to Discover Network Topology", An International Journal (ESTIJ), ISSN: 2250-3498, Vol.2, No.1, 2015,pp.117-124.*

[2] *Bhandari, A. and Ailawadhi, A, "Literature Review on an Approach to Detect Packets Using Packet Sniffing", Journal of Network Communications and Emerging Technologies,JJune 2018.*

[3] *Xinming Ou , "A logic-programming approach to network security analysis", A Dissertation Presented to the Faculty of Princeton University in Candidacy for the Degree of Doctor of Philosophy ,November 2005.*

[4] *Frédéric Massicotte, Tara Whalen, and Claude Bilodeau, "Network Mapping Tool for Real-Time Security Analysis" , Nijmegen, May 2017.*

[5] *Ritinder Kour, "Investigating network traffic using packet sniffing tool-wireshark",JETIR, Volume 6,issue 1,January 2019.*

[6] *Richard A kemmerar,"Composable tools for network discovery and security analysis", DOI: 10.1109 / CSAC.2002. 1176274, 2012.*

[7] http://www.wisegeek.org/how-do-employers - onitorinternet- usage.

[8] *S. Ansari, R. G. Rajeev, H. S. Chandrashekar, "Packet Sniffing: A Brief Introduction", p. 17-19, IEEE, 2013.*

[9] *http://www.wisegeek.org/how-do-employers-monitorinternet- usage-atork.htm#didyouknowout.*

[10] A. Yaar, A. Perrig and D. Song, "A Stateless Internet Flow Filter to Mitigate DDoS Flooding Attacks", 2009. [Online]. Available:

*January - February 2020*
*ISSN: 0193 - 4120 Page No. 11672 - 11678*

http://www.cs.berkeley.edu/~dawnsong/papers/siff.pdf. [Accessed: 26- Feb2016].

[11] M. Salagean, "Anomaly detection of network traffic based on Analytical Discrete Wavelet Transform", 2010. [Online]. Available: http://Anomaly detection of network traffic based on Analytical Discrete Wavelet Transform. [Accessed: 24- Feb- 2016].

[12] U. Banerjee, A. Vashishtha and M. Saxena, "Evaluation of the Capabilities of WireShark as a tool for Intrusion Detection", International Journal of Computer Applications, vol. 6, no. 7, pp. 1-5, 2010.

[13] S. Gupta and R. Mamtora, "Intrusion Detection System Using Wireshark", 2012. [Online]. Available: http://www.ijarcsse.com/docs/papers/11_November2012/Volume_2_issue_11_November2012/V2I11-0205.pdf. [Accessed: 15- Feb- 2016].

[14] E. Golden and J. Coffey, "A Tool to Automate Generation of Wireshark Dissectors for a Proprietary Communication Protocol", 2010.[Online].Available: http://www.iiis.org/CDs2015/CD2015IMC/IMCIC_2015/PapersPdf/ZA537 MD.pdf. [Accessed: 19- Feb- 2016].

[15] A. Yaar, A. Perrig, D. Song, (2004), “The SIFF: introduce a stateless internet flow filter”, Research Paper[Online:4/3/16] [14] Wolf-Bastian Pottner, Lars Wolf, (2010), “IEEE 802.15.4 packet analysis with Wiresharkand off-the-shelf hardware”, article [Online: 4/3/16].

[16] S. Gupta and R. Mamtora, "Intrusion Detection System Using Wireshark", 2012. [Online]. Available: http: //www.ijarcsse.com/docs/papers/ 11_November2012/ Volume_2_issue_ 11_November2012/ V2I11-0205.pdf. [Accessed: 15- Feb- 2016].