An Improved Approach towards Network Forensic Investigation of HTTP and FTP Protocols

T. Manesh, B. Brijith, and Mahendra Prathap Singh

Dept. of Computer Engineering,
National Institute of Technology, Karnataka, Surathkal 575025, India
{maneshmon,brijithb,mahoo15}@gmail.com

Abstract. Network packet analysis and reconstruction of network sessions are more sophisticated processes in any network forensic and analysis system. Here we introduce an integrated technique which can be used for inspecting, reordering and reconstructing the contents of packets in a network session as part of forensic investigation. Network analysts should be able to observe the stored packet information when a suspicious activity is reported and should collect adequate supporting evidences from stored packet information by recreating the original data/files/messages sent/received by each user. Thus suspicious user activities can be found by monitoring the packets in offline. So we need an efficient method for reordering packets and reconstructing the files or documents to execute forensic investigation and to create necessary evidence against any network crime. The proposed technique can be used for content level analysis of packets passing through the network based on HTTP and FTP protocols and reports deceptive network activities in the enterprise for forensic analysis.

Keywords: Network Forensics, Packet Reordering and reconstruction, HTTP and FTP session reassembly, Pcap File.

1 Introduction

Network forensics is the process of capturing information that moves over a network and trying to make sense of it in some kind of forensics capacity. This method is based on reconstructive traffic analysis. It could be used for forensic analysis to read and analyze the contents of the Internet raw data in PCAP format for a particular session on the network. This technique also performs content level analysis and reconstruction of pre-captured internet or network raw data containing HTTP and FTP sessions and thus perform offline packet processing for creating more accurate forensic evidences. The aim of this work is to provide detailed overview of HTTP and FTP reconstruction process as part of network forensic investigation with help of a new improved network forensic investigation tool that we have developed.

Currently the development of the tool is in progress towards forensic investigation of P2P, HTTPS, VoIP protocols. This paper is organized as follows: Sections 2 and 3 gives an introduction about HTTP and FTP analysis respectively. The section 4 explains basic Idea behind the algorithm for packet reordering and reconstruction that we have developed. Sections 5 and 6 gives the flow diagram of our approach towards

D. Nagamalai, E. Renault, and M. Dhanushkodi (Eds.): PDCTA 2011, CCIS 203, pp. 385–392, 2011.

HTTP and FTP analysis for packet reconstruction respectively followed by explanation of each process involved in the analysis. Conclusions are given in the section 7 followed by acknowledgements and References.

2 Introduction to Http Analysis Process

This section deals with the digital forensic analysis of the HTTP traffic. This approach is used for analyzing the http traffic and often finds evidence that someone did or did not commit a crime. Thus we are interested in the message exchange sequence in the HTTP traffic. The proposed method includes capturing the Ethernet packets, filtering IP packets followed by the TCP packets and reconstruction of the http traffic after identifying the request, response messages included in a particular http network session and to produce necessary forensic information.

2.1 HTTP Headers

It forms the core of an HTTP request and response. The header specifies the details about the data which are transmitted in a that session which is crucial forensic information in the investigation of HTTP protocol. The management of these forensic information is well explained in the section 5.

3 Introduction to FTP Analysis Process

In FTP environment the clients and servers may interact with each other for the purpose of file transfer. FTP protocol can operate over network channels where packets move directly from source to destination.FTP is a TCP based connection services only. FTP does not use UDP content. FTP maintains two types of ports; one is known as the control port which is for maintaining connection details and second is data port used for maintaining original data transferred across TCP connection. The port numbers for these two connections are well defined. The control connection normally uses port number 21 and data connection normally uses port number 20. The port number for the data connection can be set by the FTP client also. Some valuable forensic information like source IP, destination IP, source and destination port number, name of the file transferred and time etc can be found by examining the control connection of FTP protocol. These forensic information will be extracted and processed to create the evidences in investigation.

3.1 Different Data Transfers in FTP Connection

There are basically two types of FTP data transfer. One is called “active ” and second is called “passive”. An FTP client program fixes the active mode by sending the "PORT" command to server to instruct it that it should connect back to a specified IP address and port number and then send the data, In FTP passive connection, a client program will fix passive mode by using the "PASV" command to ask that the server should tell the client an IP address and port number that the client can connect to and receive the data.