Internet Relay Chat Forensic Analysis

Divya Joshi[1] Jenisha Vaidya[2]
[1,2]Students
[1,2]Gujarat Forensic Sciences University Gandhinagar, India

Abstract— Internet Relay Chat, or IRC, is a protocol that allows users that connect to Internet Relay Chat Servers to have conversation with others in real time. Users connect to IRC Servers using an IRC Client. Commercial chat client's like yahoo! and google chat are quite popular in wide use. To other chat clients were worth exploring. These tools are arguably better suited for criminal activity. IRC is one such tool. There are basically two options available to investigators involved in an IRC occurrence. They can look at log files on servers or clients or they can monitor transmission directly. In this paper we have been using X Chat application for the IRC Forensic Investigation. We capture the IRC Client's packets and analyze that packets.

Key words: Dump File, Geo Location, Chat User Information, IPV6 Hash

I. INTRODUCTION

IRC is a multiform or multi-channel chatting system. Imagine sitting in front of your computer and "conversation" through typed messages with either single person or many other people from all over the Internet. IRC is based on a client-server structure. User can run a client program on his/her own computer which connects him to a server computer on the Network. These all servers connect to many other servers to make up an IRC network, which transport messages from single user to another. In this way, people from all over the world can talk to each other live and simultaneously. For all these funny things you need is an Internet Service Provider to get you connected to the Internet and an IRC client user program. The most common clients are mIRC, XChat for the Windows operating system, ircII for UNIX/LINUX, and Ircle for MacOS. A good source should have installed one of these for you already.

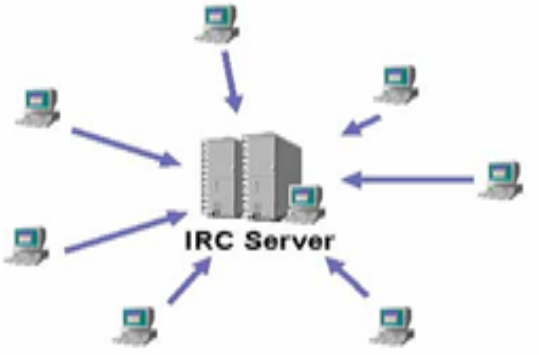

Fig. 1: IRC Structure

II. RELATED WORK

In this paper we deed our findings on weak user validation in messaging applications on smartphones. User authentication is an important area of research in cyber security especially applied to distributed systems or for web base services. number of protocols has been develope to provide secure user authentication, for example based on bit level encyption or public key cryptography and the usage of a PKI

A. *Dead Forensics:*

The first approach is volatile memory image analysis. It is similar to live response, in that an investigator would first establish a trusted command shell. Then analyst would initiate a data collection system and a method for transmitting the data. However, an investigator would only obtain a physical memory dump (RAM dump) of the compromised system and transmit it to the data collection system for analysis.

B. *Live Forensics*

Live forensics examine the value of the data that may be lost by powering down a system and gather it while the user system is still running. The other objective of live forensics is to minimize impacts to the integrity of data while gathering evidence from the suspect system. Many tools are used for the live forensics. Wireshark, Netwrok Minor etc Tool is used for the Packet Capture and Packet Analysis.

III. METHODOLOGY

There are many powerful open source and commercial tool for the packet forensic analysis. Such a tool is often referred to as a network analyzer, network protocol analyzer or sniffer. Wireshark used to examine the details of traffic at a variety of levels ranging from connection-level data to the bits that create single packet. Packet capture can provide a network administrator with information about separate packets such as transmit duration, source, destination, protocol type and header data.

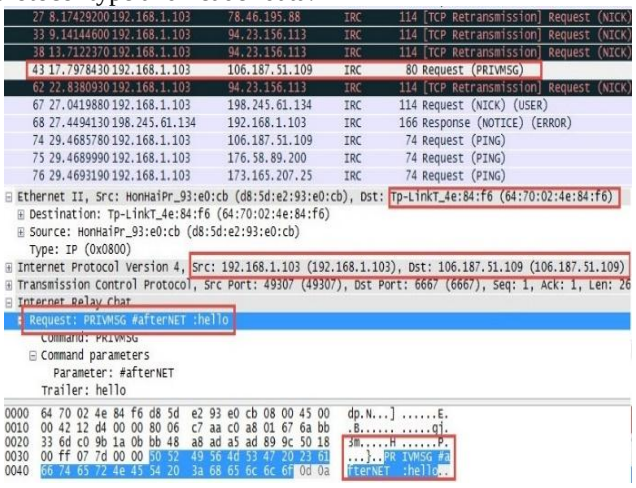

Fig. 2: Chat Evidence in Packets

This information can be useful for evaluating security events and troubleshooting network security device issues. In Fig.2 there are many packets.in packet list there is IRC protocol related request format of particular packet. The packet frame information part shows source device TP-Link router MAC address, soure ip & destination ip. In the last part there is chat(Hello) information in hex format.

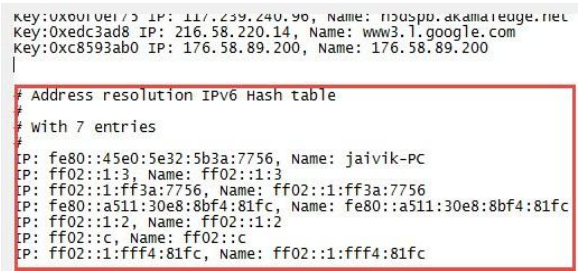

Fig. 3: IPV6 Hash Information

In the evidence report source is is very useful for case. In the Fig.3 Host name and address resolution IPv6 hash information available. There are 7 entries of rout IP addresses.

In the sub part of chat analysis Network Miner is a very useful for parsing network packet data. Network Miner can be used as network sniffer/packet capturing tool in order to detect operating systems, sessions, host names, open ports etc. without importing any traffic flow on the network. This tool can also parse pcap files for off-line analysis and to reassemble transmitted data files and certificates from pcap files.

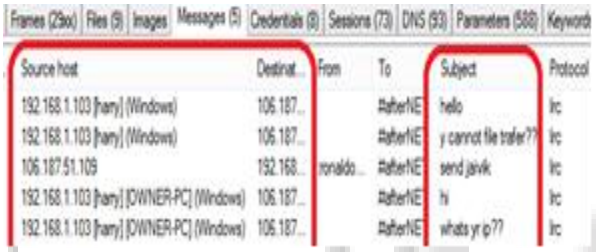

Fig. 4: Chat Analysis in Network Miner

In Fig.4 there are many evidence parts. In the source host information source IP address and host name or OS information. In second part there is destination address, last part is very important evidence part ,it shows the all chat information in message-subject part using IRC protocol.

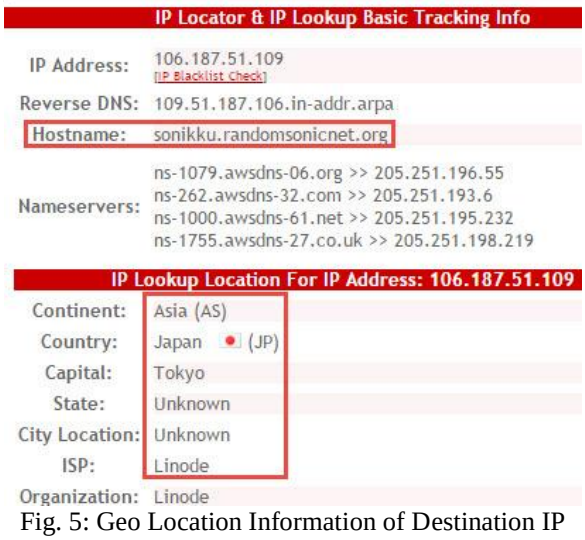

Fig. 5: Geo Location Information of Destination IP

Most of the cases are solve via destination IP addresses .If any social networking crime like email tracking and tracing, facebook fake profile, fake mail etc crimes, for all these crimes Geo location is very important evidence for defense team. In Fig.5 destination location information of particular IRC user,host name, routing servers, country name, ISP or Organization name.

A. Dead Forensics Investigation:

Dead Forensic used in computer forensics is the recovery of deleted files. Current time forensic software has their own tools for retriving or carving out deleted data. Most operating systems and file systems do not always wipe physical file/user data, allowing investigators to reconstruct it from the physical disk sectors. Take Process dump is the Example of dead forensic. A dump file is a snapshot of an app at the point in time the memory dump is taken. It shows what process list was performing and what modules were loaded.

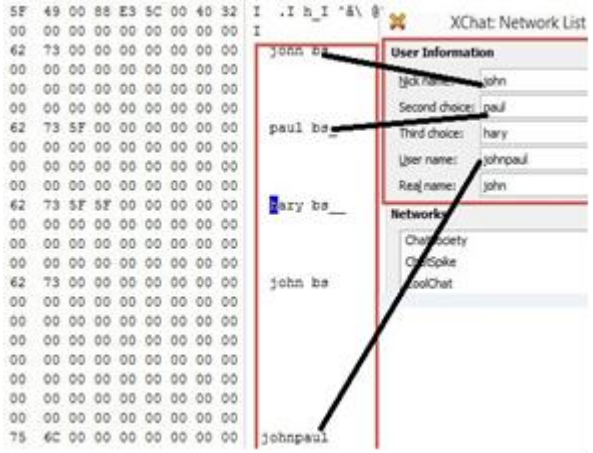

Fig. 6: User information in Dump File

When seizing evidence, if the machine is still power on condition, any user data stored solely in RAM that is not recovered before powering down may be lost. One suit of "live analysis" is to recover RAM data prior to removing an exhibit. Capture agent gateway bypasses Windows user login for blocked computers, allowing for the analysis and acquisition of RAM dump on a locked computer.Memory can be examined for prior content after power off, because the electrical charge stored in the system memory cells takes time to disappear, an result exploited by the cold boot payload attack. The duration of time that data is restorable is expand by low temperatures and higher cell voltages.However, it can be inappropriate to do this during a crime place examination.In Fig.6 XChat information available in dump file, like Nick name,user name etc.

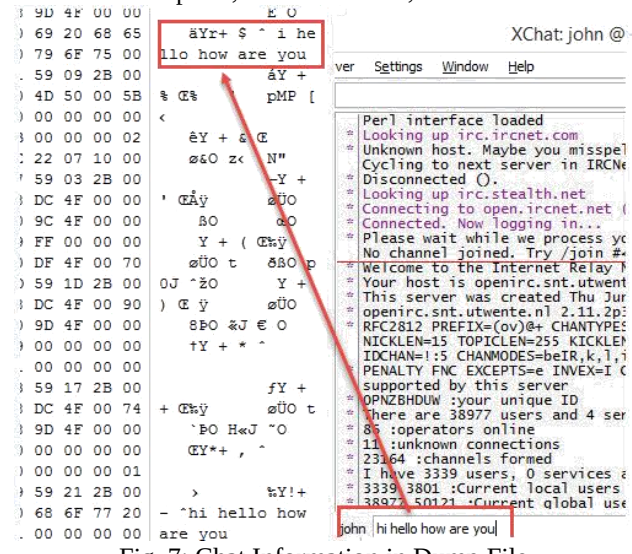

Fig. 7: Chat Information in Dump File

On the other hand, a volatile memory analysis shows promise in that the only source of evidence is the

physical memory dump. Moreover, collection of physical memory has become more commonly practiced. An investigator can then build the case by examination the RAM dump in an isolated environment that is non-obtrusive to the evidence. In Fig.7 X Chat chat information in dump file. this dump file store all chat keywords. these all keywords are stored in hex format.

IV. CONCLUSION

IRC communications by default are in plain-text. In this way communicate with a normal IRC server a client should submit its entire server requests in clear text. The most important things to have when try to investigate an incident require IRC are command of the structure and communication of IRC networks and standard network packet capturing tools, data-recovery methods and anti-encryption techniques. Users who register are assign a user identification number (UIN). It does route traffic through centralized servers so some artifacts may exist there if that server can be found. We done dump file analysis and recover the data like Client's chat, source IP address, Destination IP address, Geo location address etc. We can also do the IRC forensic investigation using dump file analysis.

ACKNOWLEDGEMENT

This work was supported by Gujarat Forensic Sciences University, Faculty of Institute of Forensic Science that provided technical condition and machines use for the development and testing. Also guided by eSF lab network expert.

REFERENCES

[1] www.w3.org/wiki/IRC
[2] http://oldwww.acm.org/conferences/cscw2004/ircIntro.pdf-2004
[3] http://www.irchelp.org/irchelp/ir ctutorial.htmlRonald van Loon,Joseph Lo (Jolo).
[4] Cyber Forensics: A Field Manual for Collecting, Examining, and Preserving.pdf
[5] Handbook of Digital Forensics and Investigation
[6] M. Egele, C. Kruegel, E. Kirda, and G. Vigna. Pios: Detecting privacy leaks in ios applications. In Network and Distributed System Security Symposium (NDSS), 2011.

