Malware Analysis & its Application to Digital Forensic

Gursimran Kaur, Bharti Nagpal

Department of Computer Science & Engineering,
Ambedkar Institute of Advanced Communication Technologies & Research,
Geeta Colony, Delhi, India
researchergursimran@yahoo.com, bhartinagpal24@yahoo.com

Abstract:- **In this paper we present study about how to analyze the malware on the system for digital investigation and also give the superficial knowledge and comparison about forensic model. This paper proposes a plan for achieving a dramatic improvement in research and operational efficiency through the adoption of systematic approaches for representing forensic data and performing forensic computation. This paper describes the nature of Forensic Science. Here we introduce malware analysis tools. Furthermore we also described malware analysis for digital forensic investigation.**

Keywords-*: Malware Analysis, Computer Forensics, Digital Forensic, Cyber Forensics*

I. INTRODUCTION

Forensic Science is the technique to identify that criminal whose involve in illegal action in the organization. It is the application of a broad spectrum of science to answer questions of interest to a legal system [10]. Forensic science is a broad area in which digital forensic is discussed in this paper. Now a day's digital forensics plays an important role in the organization and system. Digital forensics is collection and analysis of the digital evidences. This process is done by some investigation forensics model. Digital forensics is law based method for investigation. Forensics tools are now used to examine and analyze any crime and malicious activity in the organization which is done by attacker, hacker or criminal. Digital forensics is a systematic approach for representing forensics data and performing forensics computation.

Malware Analysis is exciting and big issues for computer security research. It is a type of malicious program that replicate from host machine and propagate through network. By the computer forensics we can identify the malware analysis in the network channel. For the national and economical point, it is important to have knowledge about cybercrime and digital crime. Industrial organizations and private sectors in current scenario have some dangerous significant risks. The Malicious software infects computer systems at an alarming rate, causing economic damages that are estimated at more than ten billion dollars per year. These problem are identified by the number of complains and solved by many research groups. There are some research groups CART, TWGDE, DFRWS and NIJ etc. [8]

The rest of this paper is arranged as follows: Section 2 the detail of digital forensic. Section 3 about malware analysis. Section 4 shows the relationship between malware analysis and digital investigation. Section 5 gives an overview about the Background and related work in the area of malware analysis on digital forensic. Finally, some conclusion and prospect are put forward in Section 6.

II. DIGITAL FORENSIC

Todays the modern use the term forensics in the place of forensics science. That can be considered as the forensic is legal and related to laws [10]. There are various areas of forensics science that play a unique role in an investigation.

S. No.	Forensic Area	Purpose
1.	**Forensic Anthropology**	The application of physical anthropology in a legal setting.
2.	**Digital Forensics**	The gathering of digital data that is used in the court of law
3.	**Forensic Engineering**	The investigation of materials, products, structures or components that fail to operate or do not function as intended
4.	**Forensic Entomology**	The use of insects and their arthropod relatives that inhabit decomposing remains to aid in legal investigations.
5.	**Forensic Odontology**	The study of dentition of all human beings.
6.	**Forensic Psychology**	The legal aspects of human behavior.
7.	**Forensic Toxicology**	Refers to the use of toxicology to aid medico-legal investigations of death involving poison.

In this paper, we focus on the digital forensic and malware analysis. Digital forensic science is a branch of

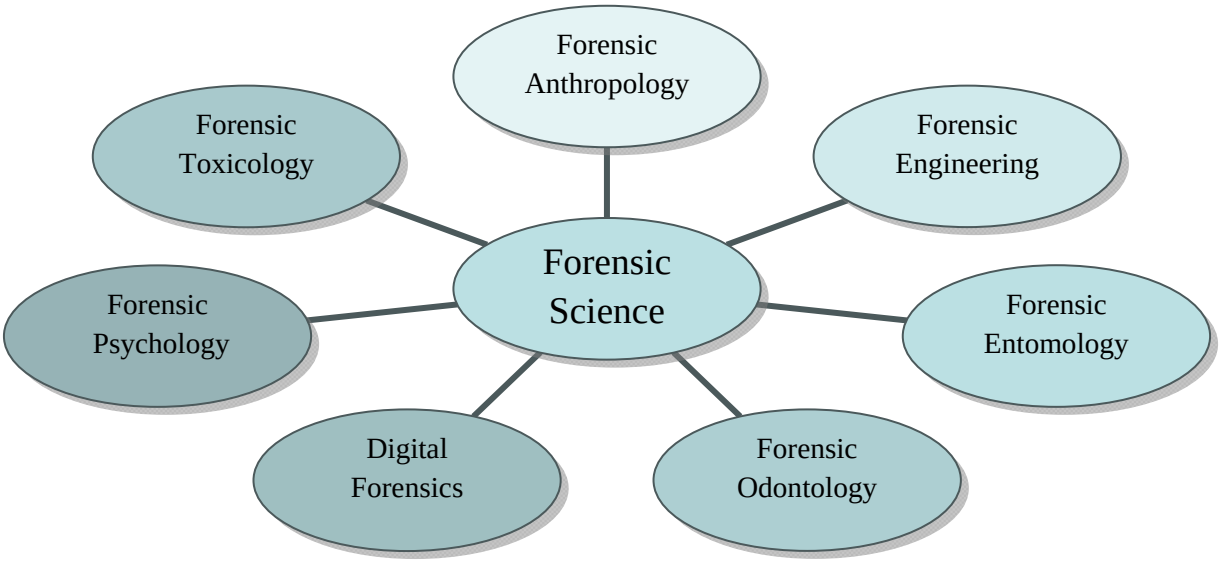


Figure 1 (Classification of Forensic Science)

computer science. Digital forensics is recovery and investigation of digital evidence which found after crime.

Digital forensic is a relatively hidden tradecraft is an important part of many investigations [1]. Digital Forensics is categorized into following:-

1. Computer Forensics
2. Cyber Forensics
3. Digitized Document
4. Software Forensics

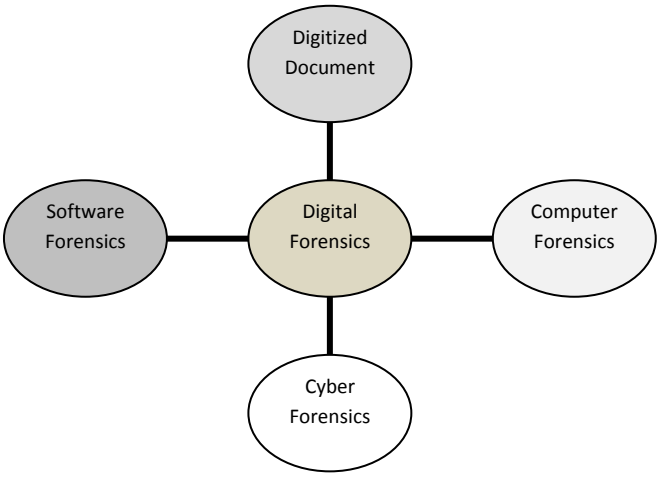


Figure 2 (Categories of Digital Forensics)

Computer Forensics: Computer forensics is disciplined including the need for a standardization approach to examination. It is also known as media forensics. Computer forensic science, is branch of digital science which is deals with the investigation and analysis of a stand –alone computer involved in crime. Here the investigators gather evidence from the computer media seized at the crime scene by extracting hidden or deleted information from the storage devices. For extracting this information we used computer investigation and analysis techniques. Computer forensic use the methods towards the Preservation, collection, validation, identification, analysis, interpretation and presentation for find out the digital evidence.

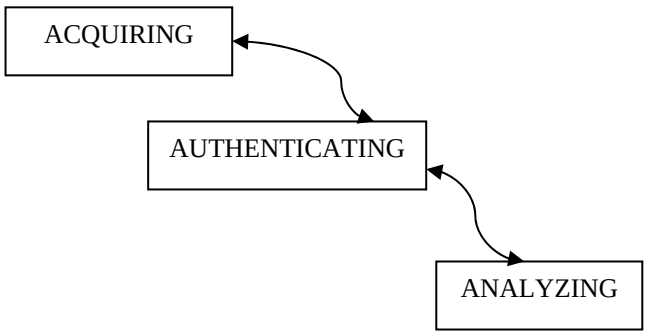
Software Forensics: Software forensics is also called code analysis is that branch of digital forensics science, which deals with the identification and categorization of author of malicious code, E-mail and any other e-document.

Cyber Forensics: Cyber Forensics, also known as network forensics, is the use of scientifically techniques to collect, identify, examine, correlate, analyze, and document digital evidence from multiple, actively processing and transmitting digital sources for the purpose of uncovering facts related to measured success of unauthorized activities meant to disrupt, corrupt, and/or compromise system components as well as providing information to assist in response to or recovery from these activities.

Digitized Document Forensics: Digitized Document Forensics can be defined as an upcoming branch of forensic science, which deals with development of methodologies to detect the fraudulent document and solutions to link generated fraudulent document to source.

In this paper, we focus on the digital investigation and malware analysis. Malware analysis is most important role in digital forensic where as Digital forensics investigation has three phases to go through [9].

PROCESS OF DIGITAL FORENSIC INVESTIGATION:-



1) **Acquiring:** Conquering the digital evidences carefully, so the integrity of evidence can be maintained.
2) **Authenticating:** Examining the validating of evidence, whether it is valid to use or not.
3) **Analyzing**: Close examination of data to sort out the case.

III. MALWARE ANALYSIS

Malware are the malicious programs which infect the system by executable code. Malware focuses on compromising the system Confidentiality, Integrity and Availability (CIA). It execute in internal system without permission [2]. It controls the system totally when it is on victim system. Generally malware is categories into following categories [5]:

Virus: Virus is executable code. It is very harmful for the system. This types program destroy the confidential and modification in the data.

Worm: A worm is self replicated malware computer program which uses computer and network resources without authenticated user permission. In the network it is consuming the network bandwidth. This is security shortcoming on the target computer.

Trojan: Trojan makes copies of themselves and steals information. It is standalone malicious program that does attempt to infect other computers in a completely automatic manner without help from outside forces like other programs.

Root kit: Root kit is malware program which creates a backdoor into the system for the hacker's use alters log files and destroyed the data files.

The goal of malware analysis is to gain an understanding of how a specific piece of malware functions so that defenses can be built to protect organizations hardware. Malware analysis and detection techniques mention below [4]:

1. Signature based
2. Behavioral based
3. Anomaly based

Signature Based: Signature based basically works on binary pattern. In this hash value of malware is identified and store in antivirus product database. When new program execute in the network channel and system compare the malware hash value which is store in antivirus database and identify it is malware or not. There is big issue to find out the new malware version because it store only old malware hash value. In this false positive comparison is impossible. To prevent this problem use the generic signature. The generic product database store signature all new malware and identify all family of malware [6].

Behavioral Based: Behavioral based works on virtual sandbox environment. In this environment sandbox download own environment malware and discard without any harmful for systems and data. The false positive is common so this technique is not use more in the network channel. Malware attacker changes the signature when antivirus protector detect because malware attacker the antivirus vendor signature and according to their behavior it changes malware hash value and signature. In this technique malware use two ways first passing host based antivirus and second passing from antivirus gateway [7].

Anomaly Based: Anomaly Based detecting of the user behavior. If user behaviors get changed in the network then it compares the signature previous stored signature in antivirus database. Anomaly based detection approach is used in two phases. First phase is training phase which identifies the behavior of the system in absence of attacker and machine learning technique. Second phase is compares the user behavior against the current user behavior. If there is any changes current user behavior then it identifies whether it is malware or not [8].

IV. MALWARE ANALYSIS FOR FORENSIC INVESTIGATION

In this section, we present the details of relationship between malware analysis and forensic investigation. To analysis the malware in forensics is using the right tool and technique to overcome the shortcoming in the organization and network channels. These tools are used in the investigation [3] [5]:

i. **Grep:** It is a command line tool writer for UNIX system for searching for text.

ii. **AVG Antivirus:** The antivirus software is use for detecting and removing malware.

iii. **Whois**: This tool is use for querying RIPE database to determine registration information for IP addresses and domains.

iv. **IDA Pro:** To commercial disassembling and debugging software.

v. **hexedit:** This is use for viewing and editing the raw data of a file in hex format.

vi. **VMWare:** To virtualization software used to create a virtual machine to be as a sand box environment for malware analysis.

vii. **FileAlyzer:** File analysis tool developed by safer networking.

viii. **Helix: T**his is a live Linux distribution containing tools and features geared towards forensics analysis.

ix. **Sysinternals:** This is a suite of tools designed to help manage, troubleshoot and diagnose Windows systems and software.

The next generation of automated forensic analysis tools, which present the data in new ways and interact with the guide will allow the investigation.

V. RELATED WORK

Many researchers have looked for way of represent the malware analysis and detection for forensics investigation. Some of these are said that malware analysis is most important in digital forensic investigation.

In order to achieve this, we will first introduce the term Digital Forensics, as it is defined by Kruse and Heiser [11]:
"Preservation, identification, extraction, documentation, and interpretation of computer media for evidentiary and/or root cause analysis".

VI. CONCLUSION AND FUTURE WORK

We provide survey about the research in the area of Digital Forensics' today structure and relation with malware analysis. This paper discusses the need to make digital forensics research more efficient through the creation of new abstractions for data representation forensic processing. There is two purpose of this paper first to help information security professionals, so that they can easily perform malware analysis and second it serve guidelines to perform malware analysis by the readers.

In future we aim to purposed framework for digital investigation through malware analysis and implement it in real dataset. Additionally we plan to investigate how to quality of malware detection will be improved.

REFERENCES

[1] S. L. Garfinkel, "Digital forensics research: The next 10 years," in Proceedings of the Digital Forensics Research Conferences (DFRWS), 2010.
[2] M. Christiansen, Bypassing Malware Defenses," SANS Institute InfoSec Reading Room, pp. 3-4 May 7, 2010.
[3] Amol Vyavhare, Cyber Forensic tools http://www.articleswave.com/computerarticles/top-cyber-forensic-tools.html Accessed on 02/11/2011.
[4] Farid Daryabar,Ali Dehghantanha,Hoorang Ghasem Broujerdi, "Investigation of Malware Defence and Detection Techniques", International Journal of Digital Information and Wireless Communications (IJDIWC) 1(3): 682- 687 The Society of Digital Information and Wireless Communications, 2012.
[5] Computer Economics. "2007 Malware Report: Annual Worldwide Economic Damages from Malware Exceed $13 Billion," June 2007. http://www.computereconomics.com/page.cfm?name=Malware%20Report Accessed 25/01/2012.
[6] Smith, S., & Quist, D. "Hacking Malware: Offense is the new Defense" 2006. http://www.offensivecomputing.net/dc14/valsmith_ _dquist_hacking_malware_us06.pdf Accessed 02/01/2012.
[7] D. Bem Virtual Machine for Computer Forensics - the Open Source Perspective, Open Source Software for Digital Forensics, Springer, 2010.
[8] R. Meadows, Cisco Router and Switch Forensics: Investigating and Analyzing Malicious Network Activity, Elsevier Science, 2009.
[9] Casey, E.: Digital Evidence and Computer Crime, 2nd Edition, Elsevier Academic Press, 2004.
[10] http://www.askoxford.com/concise_oed/forensic?view=uk : forensic accessed on 7 June 20011.
[11] Kruse, W. G. & Heiser, J. G. 2001. Computer Forensics. Incident Response Essentials. Addison-Wesley.