52 pages including cover

CSI Communications

Knowledge Digest for IT Community

Volume No. 39 | Issue No. 12 | March 2016 ₹50

ISSN 0970-647X

www.csi-india.org

DIGITAL FORENSICS

CSI Communications
Contents

Volume No. 39 • Issue No. 12 • March 2016

Chief Editor
Dr. A. K. Nayak

Guest Editor
Dr. Vipin Tyagi

Published by
Hon. Secretary
Mr. Sanjay Mohapatra
For Computer Society of India

Design, Print and Dispatch by
CyberMedia Services Limited

Please note:
CSI Communications is published by Computer Society of India, a non-profit organization. Views and opinions expressed in the CSI Communications are those of individual authors, contributors and advertisers and they may differ from policies and official statements of CSI. These should not be construed as legal or professional advice. The CSI, the publisher, the editors and the contributors are not responsible for any decisions taken by readers on the basis of these views and opinions.

Although every care is being taken to ensure genuineness of the writings in this publication, CSI Communications does not attest to the originality of the respective authors' content.

Cover Story

Research Front

Articles

Practitioner Workbench

Security Corner

PLUS

Complaints of non-receipt of CSIC may be communicated to Mr. Ashish Pawar, 022-29261724, ashish@csi-india.org, indicating name, membership no, validity of membership (other than life members), complete postal address with pin code and contact no.

Printed and Published by Mr. Sanjay Mohapatra on Behalf of Computer Soceity of India, Printed at G.P.Offset Pvt Ltd. Unit-81, Plot-14, Marol Co-Op. Industrial Estate, off Andheri Kurla Road, Andheri (East), Mumbai 400059 and Published from Computer Society of India, Samruddhi Venture Park, Unit-3, 4th Floor, Marol Industrial Area, Andheri (East), Mumbai 400093. Tel. : 022-2926 1700 • Fax : 022-2830 2133 • Email : hq@csi-india.org **Editor: Dr. A. K. Nayak**

Introduction, Goals and Challenges in Digital Forensic Process

Dilpreet Singh Bajwa
Research Scholar, DCSA, Panjab University, Chandigarh

Satish Kumar
Associate Professor, DCSA, Regional Centre, Hoshiarpur,
Panjab University, Chandigarh

Introduction

Today is an era of globalization. The rapid advancement in technology has made computers a tool for communication, data storage and processing. Our life is incomplete without computers and computer networks. It influence our lives from daily basic chores like shopping, sharing information, communication and more specific important services like banking, business etc. As computers are the need of hour and provide us numerous benefits but it also act as a tool in hands of criminals to commit cyber crimes. Cyber crimes are the biggest challenge today. Various types of cyber crimes like hacking, fraud, defamation, credit card cloning, software piracy, SPAM distribution, virus/Trojan distribution, unauthorized use of personal information, pornography, obscene publication, perjury, forgery, sexual harassment, e-mail spoofing, e-mail bombing, phishing, denial of service attacks(DoS), cyber terrorism, data theft, industrial espionage etc., are on rise. Cybercrime is a crime in which digital devices like computers, communication devices and networks can be used as a medium to commit crime and it is harder to stop and detect these cyber crime related activities. To tackle these activities and punish criminals in court of law, a new field has evolved called as Digital Forensics.

Digital Forensic Process

Digital forensics is defined as a process used to identify, preserve, extract, analyze, validate, interpret, document and present the digital evidence. This process is carried out by using proven methods and techniques in such a way that the evidence so collected is admissible in court of law. This process further facilitates the reconstruction of events to punish the culprits. Actually, it is considered as a branch of cyber forensics that deals with investigation and recovery related to digital devices involved in computer crimes. It is generally considered as synonym for computer forensics but includes all digital devices capable of storing digital data. So Digital forensics not only covers computers but all digital devices meant to deal with digital data like networks, mobiles, laptops, PDAs, USB drives etc.

Further, Digital Forensics is broadly categorized into Computer Forensics, Network Forensics and Mobile Forensics depending upon the type of digital devices involved in investigation.

Phases in Digital Forensics: Digital forensics rapidly emerged in last few years as a new field to counter cyber crimes and prosecuting criminals. Prior to the existence of this proven methodology, tools and techniques, many crimes left unsolved. Digital forensics is a process and there are various points the investigators have to keep in mind while investigating the case. The most important point to keep in mind is that the evidence extraction is performed in such a sound manner so that it can be admissible in court. For this purpose certain steps must be follow in particular order. Various researchers and practitioners proposed various frameworks for digital investigation purpose but generally the below given steps are followed while performing digital forensics:

- Identification
- Preservation
- Extraction
- Interpretation
- Documentation and
- Presentation

Identification

It is the initial phase, in which an investigator identifies the devices or containers which possibly contains crime related evidence such as hard-disks, floppy drives, USB Drives, RAM etc.

Preservation

Before performing any forensic analysis, forensic investigator must preserve original data and media. Analysis cannot be directly performed on original media but first we make a forensically sound copy or image of original device containing data and then perform the task of analysis on this forensic copy.

Extraction

In this phase, we extract the evidence pertaining to be found relevant according to the investigation in hand from the forensic image of media.

Interpretation

In this phase, the investigator interprets or relates the extracted information with the crime and culprit. Extracting information is one thing and properly interpret it according to particular investigation is altogether different thing. Many tools are available to analyze the media and extract information but to relate this information with crime is a daunting task that not only needs tools and techniques but expertise and experience too.

Documentation

This phase is going in parallel to other phases that are carried from the start to the end of investigation process. This step is used to create documentation; we called as chain of custody i.e. all the complete documentation/ report pertaining to what steps have been taken, tools and techniques used during the whole process especially while performing extraction and analysis of the evidence. This documentation helps the investigating team to present their case in court strongly. In court the investigators have to authenticate and validate the various tools/ techniques used and steps/ processes followed during investigation on demand.

Presentation

In this phase, the investigating team presents their findings or results in a standard format and produce the same before court or some other legal authority. The results, reports and evidences etc. must be based on some proven methodology, tools and techniques that can reproduce the same results when required on demand by court. The evidence produced must be authentic and admissible in court.

Digital Forensics is not only concerned with the evidence, computer or digital containers of evidence but also with the forensically sound procedure, tools, techniques used and legal proceedings. The whole process must be performed in lawful manner and must take care of chain of custody to prove every aspect of the investigation in court with reliability and authentication otherwise the evidence may not be admissible in court.

Goals

The primary goals of Digital Forensics are as follows:

- Identification of criminal and unauthorized activities that is not permissible under law in a given state.
- Preserving, extracting, storing, analyzing and presenting the evidence in a lawful manner.
- To gain insight into criminal activities and techniques used by criminals to perform cyber crimes and make system more secure by proposing methods and techniques to counter crimes. This not only helps in prosecuting criminals in court but also helps in reducing crime in future.

Challenges for Digital Forensics

Various issues need to address during Digital Investigation process are as follows:

Different Media Formats and Devices: A variety of devices, from different vendors, is available in market. Similarly, different formats for data storage and communication are defined. So, it is not possible for a single forensic examiner to have expertise in all. With time more and more formats for image, text data, video and audio file formats are available to use. Further, various types of operating systems and hardware architectures adds in problem.

Media Volume: In earlier devices, the size of storage media, like hard-disk, were small in size but with time its size increased gradually. Now a day, Tera bytes of data is a normal thing. With growing size, it takes more time to create and analyze forensic images. This delays the investigation process.

Encryption: Encryption refers to the process of encoding information and messages with help of keys/passwords such that only the persons having access to keys can read the message. Many efficient encryption algorithms are available. In addition, the tools like TrueCrypt are available to encrypt the data. Even full encryption of a disk is possible. Moreover, sometimes, it is easier to recover data during forensic process but it can't be interpreted or further processed due to non availability of encryption passwords.

Steganography: Steganogaphy is a technique used to hide a message so that it could not be detected or used by an unauthorized person. Text, file, image or video can be concealed within another message, file, image or video. Steganography poses a big challenge for digital forensic practitioners.

Anti Forensics: Digital Forensics is a set of techniques used to collect and analyze the evidences to punish culprits. To escape themselves, the criminals are using anti-forensic techniques. The overall purpose is to counter and forestall the digital investigation process and continue illegal activities. The example is the use of an artifact wiping technique that erase the potential data and traces of criminal activities from the system.

Acquisition and Analysis of Live Systems: In traditional digital forensics process, examiner first shutdown the system by removing the plug or through proper shutdown mechanism. In both cases, the potential evidences like system state, recent open process list, traces of malwares and anti-forensic activities, unencrypted data etc. reside in volatile memory are lost. Some time, it is not possible to shutdown the system. So in both scenarios, live acquisition of evidence and analysis is required on running system. This process of live data acquisition is also a difficult task in context of forensic procedure as the memory state of a working system change continuously. Second, the tools used for acquisition and analysis may also affect the memory and can overwrite potential evidence present in memory. Further, the malicious softwares and anti-forensic softwares can interfere and manipulate the investigation results.

Lack of availability of proper Tools and Expertise: Digital forensics field is a new field. There is lack of available standard tools, procedures and/or methodologies to deal with criminal activities. In addition, there is a vast number of devices, data formats, softwares and operating systems present in market and a single tool and/or technique is not perfect for all. The investigators need to update all these regularly. Similarly, a single investigator can't have full expertise in all such techniques. Hence, there is dire need of hour to train the experts in field.

Legal Issues: Several legal issues roadblocks the investigation process. A cybercrime can happened on Internet that can extend beyond the jurisdiction boundary of a state. The different states have different law and legal procedure. An activity may be legal in one country but illegal in another. For example pornographic sites are allowed by some countries but are not allowed in another. As technology is growing very fast. The new systems give birth to new crimes too. There is no proper law defined to tackle with such crimes and punish the criminals. The progress is going on and the legal procedure is in process to get mature corresponding to cyber crime.

Conclusion

Digital forensics is required to counter cyber crime, unauthorized activities in cyber space and punish the culprits through legal process. Cybercrime is much more disastrous and have vast effect than traditional crimes. Digital Forensics is a new field and gaining maturity with time and can be used efficiently to produce evidence in lawful manner to punish criminals and to counter criminal activities. Since, the crimes are on rise with the use of digital technology and any one can be victim of it. Such rise in crime can be tackled with the use of digital forensics. Some tools and techniques are available but much more is required to be done to boost the digital forensics. ■

About the Authors

Mr. Dilpreet Singh Bajwa is a Research Scholar at Department of Computer Science and Applications, Panjab University Chandigarh and currently works with CGC, Landran, Mohali, Punjab. His areas of interests include Cyber Forensics, Digital Forensics, Volatile Data Forensics and Cyber Security. He can be reached at pu.dilpreetbajwa@gmail.com.

Dr. Satish Kumar [CSI - I1501531] is Associate Professor in Department of Computer Science and Applications in Panjab University (PU), Chandigarh (India), currently posted at Panjab University SSG Regional Centre, Hoshiarpur, Punjab, India (a multi faculty prestigious campus of PU). He has more than fifteen years experience of teaching post-graduate classes. His areas of interest are Image Processing, Pattern Recognition, computer graphics and Artificial Intelligence. He can be reached at satishnotra@yahoo.co.in.