Practical Cyber Forensics

An Incident-Based Approach to Forensic Investigations

Niranjan Reddy

Apress®

Practical Cyber Forensics

An Incident-Based Approach to Forensic Investigations

Niranjan Reddy

Apress®

Practical Cyber Forensics

Niranjan Reddy
Pune, Maharashtra, India

ISBN-13 (pbk): 978-1-4842-4459-3 ISBN-13 (electronic): 978-1-4842-4460-9
https://doi.org/10.1007/978-1-4842-4460-9

Copyright © 2019 by Niranjan Reddy

This work is subject to copyright. All rights are reserved by the Publisher, whether the whole or part of the material is concerned, specifically the rights of translation, reprinting, reuse of illustrations, recitation, broadcasting, reproduction on microfilms or in any other physical way, and transmission or information storage and retrieval, electronic adaptation, computer software, or by similar or dissimilar methodology now known or hereafter developed.

Trademarked names, logos, and images may appear in this book. Rather than use a trademark symbol with every occurrence of a trademarked name, logo, or image we use the names, logos, and images only in an editorial fashion and to the benefit of the trademark owner, with no intention of infringement of the trademark.

The use in this publication of trade names, trademarks, service marks, and similar terms, even if they are not identified as such, is not to be taken as an expression of opinion as to whether or not they are subject to proprietary rights.

While the advice and information in this book are believed to be true and accurate at the date of publication, neither the authors nor the editors nor the publisher can accept any legal responsibility for any errors or omissions that may be made. The publisher makes no warranty, express or implied, with respect to the material contained herein.

Managing Director, Apress Media LLC: Welmoed Spahr
Acquisitions Editor: Nikhil Karkal
Development Editor: Matthew Moodie
Coordinating Editor: Divya Modi

Cover designed by eStudioCalamar

Cover image designed by Freepik (www.freepik.com)

Distributed to the book trade worldwide by Springer Science+Business Media New York, 233 Spring Street, 6th Floor, New York, NY 10013. Phone 1-800-SPRINGER, fax (201) 348-4505, e-mail orders-ny@springer-sbm.com, or visit www.springeronline.com. Apress Media, LLC is a California LLC and the sole member (owner) is Springer Science + Business Media Finance Inc (SSBM Finance Inc). SSBM Finance Inc is a **Delaware** corporation.

For information on translations, please e-mail rights@apress.com, or visit http://www.apress.com/rights-permissions.

Apress titles may be purchased in bulk for academic, corporate, or promotional use. eBook versions and licenses are also available for most titles. For more information, reference our Print and eBook Bulk Sales web page at http://www.apress.com/bulk-sales.

Any source code or other supplementary material referenced by the author in this book is available to readers on GitHub via the book's product page, located at www.apress.com/978-1-4842-4459-3. For more detailed information, please visit http://www.apress.com/source-code.

Printed on acid-free paper

I solely dedicate this book to my beloved parents who have been my role models and supported me all throughout my journey – and well as my one and only charming daughter Anjor Reddy.

Table of Contents

About the Author

Niranjan Reddy is a renowned and passionate Information Security professional who specializes in Cyber Security and Digital Forensics, and who has an obsession for technology. He has hands-on experience in almost all domains of Information Security, specializing in Cyber Forensics. He is an Electronics graduate and possesses numerous international certifications under his belt. Here are some to name a few: MCSE, CCNA, Certified Ethical Hacker (CEH); Computer Hacking Forensics Investigator (CHFI); EC Council Certified Security Analyst (ECSA); Certified Information System Security Professional(CISSP); Offensive Security Certified Professional(CISSP); ISO-27000:2013-Lead Auditor; and many more. He is a Mentor, Entrepreneur, Founder and CTO of NetConclave Systems, which is an IT Security Consulting, Services, and Training firm headquartered in Pune, India.

He was awarded the Global EC Council Excellence Instructor Award for nine years in a row (2009–2017) in the South Asia category by EC Council, USA, for corporate trainings and contributions to the Infosec domain. His articles on forensics and cyber security have been featured in many international and domestic publications such as *Hakin9*, *E-Forensics*, *D46 Magazine*, *India Legal*, etc.

He has 14+ years plus of rich global experience in the field of Information Security, Digital Forensics, Security Audits, Cyber Laws, and Incident Response and has handled critical runaway projects worldwide. He has been a speaker at various international and domestic conferences such as GroundZero, National Information Security Summit (NISS), EC Council International Cyber Security Summit in Colombo, HAKON, Hackers Day, NASSCOMM, Inforsecon at GFSU National Cyber Defence Research Centre (NCDRC), ISACA Pune chapter, and many more. He has also authored various articles on information security and digital forensics, cyber crime investigations in many domestic and international print media like *e-forensics*, *Hakin9*, *India Legal*, *Digital 4N6 magazine*, *Gulf Times*, *Daily-Financial Times Daily-Colombo*, *Times of India*, *Mid-Day*, *Sakal Times*, and many more in addition to being featured on radio and television channels.

About the Technical Reviewer

Sagar Rahalkar is a seasoned Information Security professional having 12 years of experience in various verticals of IS. His domain expertise is Cybercrime investigations, Forensics, AppSec, VA/PT, Compliance, IT GRC, etc. He has a master's degree in computer science and several certifications such as Cyber Crime Investigator, CEH, ECSA, ISO 27001 LA, IBM AppScan Certified, CISM, and PRINCE2. He has been associated with Indian law enforcement agencies for around four years dealing with cybercrime investigations and related training. He has received several awards and appreciations from senior officials of the police and defense organizations in India. He has also been an author and reviewer for various books and online publications.

Acknowledgments

First, I would like to thank my mother for her full support to make sure that I was able to write and complete this book. She has always been my inspiration of doing something unique that would help the masses and be remembered for the good. I would further like to extend my sincere gratitude to all my mentors and thought leaders: Mr. Dinesh Bareja, Mr. Santosh Khadsare, Mr. Haja Mohideen, Mr. Amar Prasad Reddy, Advocate Prashant Mali, Mr. Anupam Tiwari and law enforcement senior officials Mr. Rajendra Dahale and Dr. Sanjay Tungar.

Introduction

This book is a guide to practical digital forensics and provides a great collection of hands-on techniques and ample real-time examples followed by a few real-time case studies carried out by me. It starts with the fundamentals and introduction of cyber forensics with real-time cybercrime case studies and scenarios. The book then deep dives into the investigating process on various platforms like Windows, different distributions of the Linux System, and Apple's MacOS. One of the major challenges and hardships faced by any Forensics Investigator is the Anti-forensics techniques carried out by cybercriminals. In Network forensics, we talk of real-time packet analysis using numerous open source tools like Wireshark, Network Miner, and Xplico.

In today's digital world, everyone possesses a personal mobile device of their own, and the crime rates are alarmingly increasing. This book showcases how basic forensic analysis and evidence gathering can be done using Android and iOS mobile devices. The Cloud forensics chapter will provide you with details about Forensics as a Service (FaaS) and demonstrates hands-on forensic analysis of Google drive, Dropbox, and WhatsApp.

You will also learn about different malware attacks and how to analyze them as well as how the investigation process is carried out for them. Web attacks forensics covers how forensic investigation and analysis of web server logs and the Tor browser is done and how the dark net is accessed and used as a medium to carry out different crimes, followed by examples.

We discuss the investigation of email crimes like phishing and scamming with in-depth knowledge about email header analysis. You will learn about SSD forensics; and in this cryptocurrency age where payments in bitcoins are demanded by hackers, we will learn about various tools and techniques that can be used by a forensic investigator to analyze bitcoin transactions. Last but not least, we will learn about cyber laws and cyberwarfare followed by data protection regulations for different countries; and finally, cover how a forensics investigator should prepare and follow guidelines while preparing an investigative report.

This book provides lots of real-time case studies and various examples on how to utilize open source tools available to carry out initial forensic investigations, along with the challenges being faced by forensics investigators.

Before reading this book, readers need to have some basic knowledge in IT security and ethical hacking. This will help you better understand the cyber forensics topics discussed in this book.

CHAPTER 1

Introduction to Cyber Forensics

The rise and growth of cyberspace have led to a chain of events that has shaped the world we live in. We have seen the rise of IT industries, which created millions of jobs all over the world either directly or indirectly. The start of e-commerce has revolutionized the shopping and retail industry. E-governance was adopted by nations all around the globe as it provided a better platform for administration and promoted transparent and efficient working practices. With the development of computer systems, the world has also witnessed the emergence of cybercrime. As computer-related crimes and incidents have increased, investigations have demanded the services of experts with knowledge of computer systems and law enforcement protocols. The pioneers of cyber forensics were computer hobbyists and law enforcement officers who would share their knowledge to investigate computer-related crimes. Over the past years, the world has witnessed computer-related crimes, which have directly or indirectly harmed people or organizations; a term was coined for them – cybercrime.

The traditional methods of crime investigation do not hold well in the case of cybercrimes. Hence, in order to combat such crimes, a new approach toward crime investigation was needed. This led to the development of Computer Forensics/Cyber Forensics/e-discovery (electronic evidence discovery)/Digital Forensics, which are all relevant and mean relatively the same thing. Our aim with this book is to fortify your knowledge about cyber forensics by showcasing standard and advanced digital and cyber forensic tools and techniques.

© Niranjan Reddy 2019
N. Reddy, *Practical Cyber Forensics*, https://doi.org/10.1007/978-1-4842-4460-9_1

CYBERWARFARE

Cyberwarfare is termed to mean a target in a battlespace or warfare context of computer systems and networks. It involves both offensive and defensive operations leading to the threat of cyberattacks, espionage, and sabotage.

Cyber Warfare in 2019 is going to be massive. National Cyber Security Center (NCSC) revealed in a report that it recorded 34 "significant" cyberattacks that demanded a cross-government response last year.

The report discusses the cyber attacks' immense financial impact on the National Health Service (NHS). The attack infected over 200,000 computers in 150 countries. These computers included government, health care, and private systems. Governments around the world are preparing for bigger cyberattacks during the upcoming elections in 2019.

What Is Cyber Forensics?

Cyber forensics is a discipline that involves investigation and analysis techniques to gather and preserve evidence from a particular electronic or digital device, which is a suspect in an investigation, in such a way that the evidence is suitable for presentation in a court of law. The goal of cyber forensics is to perform a structured investigation while maintaining the integrity of evidence and a documented chain of custody for evidence to find out exactly what happened on a suspect device and who was responsible for it. Cyber forensics plays a major and crucial role in cybercrime investigations.

Forensics is the practice of identifying, collecting, preserving, analyzing, and documenting digital evidence. Forensic investigators use a variety of techniques and forensic software applications to examine the collected digital images of the suspect device. Investigators search for hidden folders and unallocated disk space for copies of deleted, encrypted, or damaged files. Any evidence found on the image of the suspect drive is carefully documented in a final report written by the investigator and verified with the original device, before preparing for legal proceedings.

A Brief About Cyber Forensics

The digital revolution started in the 1980s when IBM PCs were rolled out for the public. These systems were powerful but had relatively few programs. Computer hobbyists got hooked on to these devices as it enabled them to write code and play around with the hardware.

The rise of computers also led to a rise in computer-based crimes. Computers were used to hack telephone systems

In 1984, the FBI Magnetic Media program was created, which later became the Computer Analysis and Response Team (CART). CART along with Seized Computer Evidence Recovery Specialist (SCERS), Electronics Crimes Special Agent Program (ECSAP), and Defense Computer Forensics Laboratory (DCFL) were the first recognized efforts to combat cybercrime.

In 1987, Access Data was formed, which is recognized as the pioneer in cyber forensics.

The FBI hosted the first International Conference on Computer Evidence, which was held at Quantico in 1993 and was attended by representatives of 26 nations. Unanimously, it was decided they would share experiences and provide assistance to each other. In 1995, the International Conference on Computer Evidence (IOCE) was formed, which was attended by the same representatives from the 26 nations. Again, the participating nations agreed to share experiences and provide assistance to each other. In 1998, IOCE was commissioned by the G8 to establish international guidelines, protocols, and procedures for digital evidence.

Scientific Working Group on Digital Evidence (SWGDE) was a collective of law enforcement personnel, forensic laboratory scientists, and commercial company employees who worked together for the development of cross-disciplinary guidelines of digital evidence. In 2002, SWGDE published their work, “Best Practices for Computer Forensics.”

In 2004 the Budapest Convention on Cybercrime took place, where an international treaty was signed that recognized crimes committed via the internet on computer systems and networks, copyright infringement, child pornography, fraud, etc.

ISO published the ISO 17025 General Guidelines for the competence of testing and calibrating laboratories in 2005.

Cyber forensic tools soon started to make their stride; Encase by Guidance Software and FTK by Access Data spearheaded the commercial tools category, thus becoming a huge success and gaining legal acceptance while the open source community created Sleuth Kit and Autopsy browser, which were used for Linux.

Forensics Investigation Process

The goal of performing a cyber forensics investigation is to gain thorough information about the event. It involves finding and analyzing the digital evidence related to the investigation. Cyber Forensic Experts follow the basic steps of investigation; the intricacies of these steps may vary as per the model of the organization in charge of the investigation.

The Forensic Investigation Process includes various forensic processes such as identification, seizure, imaging, hashing, analysis, report, and preservation during a digital forensic investigation as shown in Figure 1-1.

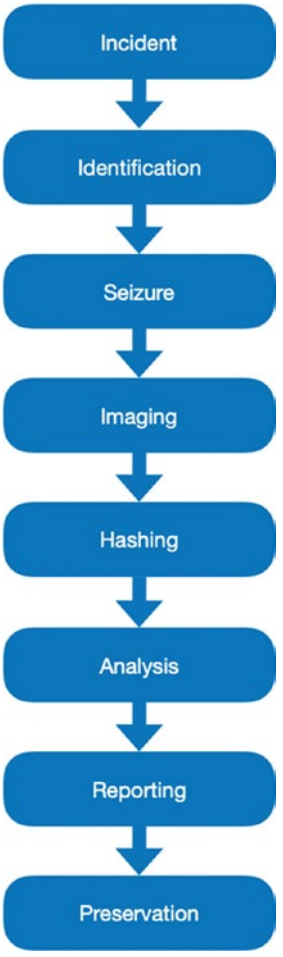

Figure 1-1. *Forensic Investigation Process*

Incident

This is the occurrence of a cybercrime instance where digital devices like computers, mobile devices, etc., have been used to commit a crime.

Identification

Identification is a crucial step in the forensic examination process. It directly affects efforts to develop a plan of action and ultimately the success of the investigation.

Before starting a digital forensic examination, the scope of actions must be identified:

- Who are the prime suspects?
- What are the best sources of potential digital evidence that will be further investigated?

This information will help the investigator in many ways, so that:

- No essential evidence is missed that might affect a case.
- Costs can be estimated in advance for the investigation, and the scope of the case can be adjusted accordingly.

Seizure

Prior to the actual examination, digital media related to the investigation will be seized. In criminal cases, law enforcement personnel, trained technicians to ensure that the evidence is not tampered with, often perform seizing the digital evidence. There are various laws that cover the seizure of digital media. For example, in any criminal investigation, there are laws related to search warrants, which will be applicable here.

Imaging

After successfully seizing digital evidence, a forensic image of this evidence is created for further analysis. This image is a bit-stream copy which is an exact bit-by-bit copy of a computer's physical storage device (SSD or HDD). Forensic image formats include disk dump (dd) and encase image file format (.E01). This image contains all the files and folders along with deleted files present on the hard disk of the digital evidence. The forensic image should be created with hashing and without tampering with the contents of the digital evidence, so that it can be admissible in a court of law.

Hashing

After successfully obtaining the forensic image of the digital evidence it is important to maintain the integrity of the image. To ensure such integrity a hash value is created for every forensic image using various hashing algorithms such as MD5 (Message Digest 5), SHA1 (Secure Hash Algorithm), and SHA25. The hash value is generated in accordance to the contents of the data stored in the digital evidence. Any tampering with evidence will result in a different hash value, and thus the digital evidence will not be admissible in a court of law.

Analysis

After the process of imaging and hashing, the evidence is taken for forensic analysis by a forensic examiner to look out for findings that can support or oppose the matters in the investigation. During the analysis the forensic examiner should maintain the integrity of the digital evidence.

Reporting

Upon completion of a forensic analysis, all the relevant findings should be presented in a report format by the forensic investigator. The investigator cannot present their personal views in this report. This report should be precise and must consist of conclusions drawn from the in-depth analysis. It should be easily understandable by any non-technical person such as the law enforcement agency staff.

Preservation

Once evidence is collected, it is important to protect it from any type of modification or deletion. For example, it might be necessary to isolate host systems such as desktops (a suspect system in forensic investigation) from the rest of the network through either physical or logical controls, network access controls, or perimeter controls. It is also important that no other users access a suspect system.

Forensic Protocol for Evidence Acquisition

The basic aim when handling any digital crime scene is to preserve the evidence. According to the circumstances of the crime and the constraints on the digital investigator, the nature and extent of the digital evidence are decided. Therefore, evidence acquisition is led according to an offense category.

This protocol is the basic approach for evidence acquisition, and it can be made applicable in Computer Forensics. This protocol is followed for all Operating Systems like Windows, Linux, Mac, etc. The forensic protocol for the evidence acquisition process is shown in Figure 1-2.

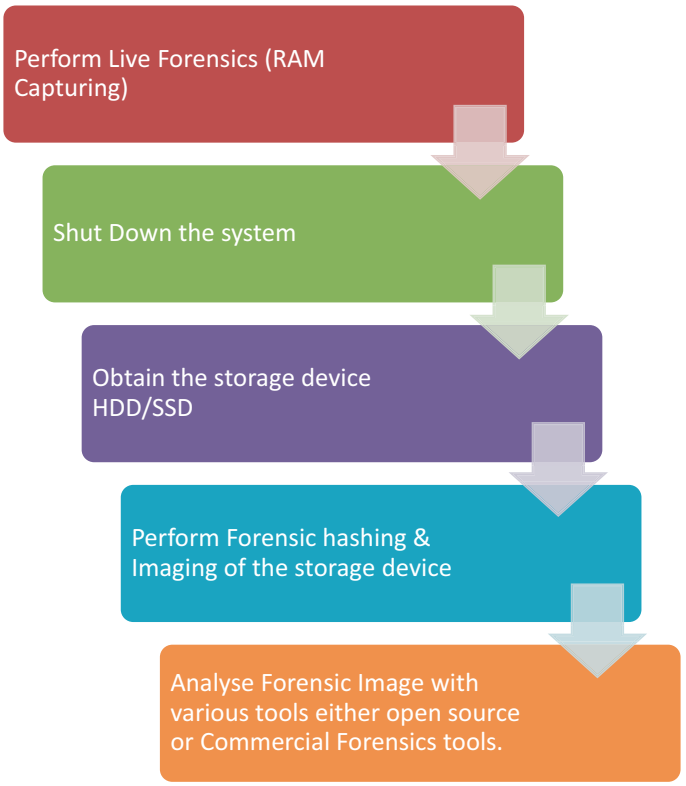

Figure 1-2. *Forensic protocol for evidence acquisition*