Chapter 6

Development and Various Critical Testing Operational Frameworks in Data Acquisition for Cyber Forensics

Abhineet Anand
https://orcid.org/0000-0003-3505-8563
Chitkara University Institute of Engineering and Technology, Punjab, India

M. Arvindhan
Galgotias University, India

ABSTRACT

Digital forensics is the science of preserving and analyzing digital data; this data can then be used in court cases as well as for crime detection and prevention. Digital forensics began in the 1970s and was initially used as a tool for fighting financial crime. Today, with computers and digital devices being an integral part of our professional and private lives, digital forensics are used/needed in a wide variety of disputes. Data Acquisitions is described and discuss different techniques or methodology obtain the data, facts, and figures from different resource and at a different level of the system.

DOI: 10.4018/978-1-7998-1558-7.ch006

Copyright © 2020, IGI Global. Copying or distributing in print or electronic forms without written permission of IGI Global is prohibited.
INTRODUCTION

The field of digital forensics is continually changing as new technology is developed both as the focus of a digital forensic practitioner’s activities and concerning the tools available to undertake those activities. This has led to the difficulties being faced by the U.S. National Institute of Standards and Technology (NIST) who have been unable to keep pace with new digital forensic software being released or even updates to existing software (Allemang D., 2011). For instance, the NIST handbook revised on 1 February 2012 refers to the testing results of EnCase version 6.5, but by 23 February 2012, the production version of EnCase was v7.03. This problem comes about because the tools themselves are victims of the fast-moving environment of digital forensics and the need for those “tools designed solely for forensic purposes to keep abreast of the broad range of technology” (Alzaabi M., 2013). Digital forensics is the science of preserving and analyzing digital data; this data can then be used in court cases as well as for crime detection and prevention. Digital forensics began in the 1970s and was initially used as a tool for fighting financial crime. Today, with computers and digital devices being an integral part of our professional and private lives, digital forensics are used/needed in a wide variety of disputes (ALfahdi M, 2016).

Common Data Acquisitions Considerations

Broadly classification of data acquisition can be done into two categories

1. Static Acquisition: In this environment, data is copied from a hard drive from a powered-off system. The normal procedure is taking out the evidence form the suspected computer, by using any of the write blockers is attached to the investigating system, which makes copies/images of the original files. With the help of different tools various type of analysis is done on this evidence and try to find out the proof for any type of unethical breach (Ayers D., 2009).

2. Live Acquisition: In this type of environment, the tools are directly included in the system, which runs various background processes on the suspected system. From the live stream, images are created and different analysis is applied on online mode and the targeted system are being protected from any type of threat. This type of Acquisition is used most nowadays because shutting down the servers or websites is nowadays being not possible. For Live Acquisition, write blockers are in use at the various level of data acquisition. Mainly these devices are used to monitor the commands given to hard disk. They never allow data to be written or copied to any other device. Even they don’t allow the disk packs to be mounted on the system with write access on them, only
Related Content

Digital Steganography Security
[www.igi-global.com/chapter/digital-steganography-security/247291?camid=4v1a](www.igi-global.com/chapter/digital-steganography-security/247291?camid=4v1a)

Trends in Malware Attacks: Identification and Mitigation Strategies
[www.igi-global.com/chapter/trends-in-malware-attacks/247286?camid=4v1a](www.igi-global.com/chapter/trends-in-malware-attacks/247286?camid=4v1a)

Financial Statement Fraud Detection and Investigation in Digital Environment
Dynamical Forensic Inference for Malware in IoT-Based Wireless Transmissions
Rashmi Bhardwaj and Aashima Bangia (2020). *Forensic Investigations and Risk Management in Mobile and Wireless Communications* (pp. 51-79).
www.igi-global.com/chapter/dynamical-forensic-inference-for-malware-in-iot-based-wireless-transmissions/234072?camid=4v1a