Chapter 8
Computer Forensics and Cyber Attacks

Michele Perilli
University of Foggia, Italy

Michelangelo De Bonis
University of Foggia, Italy

Crescenzio Gallo
University of Foggia, Italy

ABSTRACT

During investigative activities in the field of contrasting tax evasion and fraud, it is known that law enforcement agencies are increasingly encountering digital documents, which are slowly replacing the paper ones. The chapter has the purpose to explain as data, extracted from an electronic device, turns into evidence in court. The authors describe how hidden data (metadata) can become forensic evidence. In particular, the chapter examines the metadata contained in digital photos, which conceal a mass of data whose existence is not normally suspected. The second part of the chapter consists of miscellaneous cyber-attack descriptions in which computer forensics can be applied. It is finally described how one can protect systems against a cyber-attacks.

INTRODUCTION

The information required during investigation activity that once led to the production of photocopies, folders, paper documents to be examined now frequently ends with the acquisition of many data saved on CDROM or hard disk and a few paper documents.

It is equally known that there is no official methodology that describes the forensic acquisition procedures, still relying on best practices, ISO standards, RFCs and some legislative adjustments ratifying 2001 Budapest Convention (Council of Europe, 2001).

DOI: 10.4018/978-1-7998-5728-0.ch008

Copyright © 2021, IGI Global. Copying or distributing in print or electronic forms without written permission of IGI Global is prohibited.

Computer forensics hardly finds a univocal and exhaustive definition that can correctly describe it in all its nuances. As a first approach, computer forensics could be defined as the technical-investigative activity aimed at identifying, acquiring, protecting, managing, analyzing and interpreting digital traces, found inside electronic devices and their correlation to the facts, circumstances, hypotheses and traces of any nature, related to the investigated fact (Osterburg & Ward, 2010). In addition, the heterogeneity of electronic media hides traces and clues, the constant technological evolution and every situation in which an investigator must confront, unfortunately does not allow to identify a univocal and universal procedure for digital evidence acquisition (Reyes *et al.,* 2007).

The theme therefore clearly refers to the procedures and dynamics that some digital evidence can bring to the case resolution. An accurate application of digital forensics procedures ensures the integrity, authenticity, truthfulness, non-repudiation and completeness of the test, which are the basis of computer forensics itself.

The steps that characterize the computer forensics activity can be summarized in the identification, preservation, acquisition, analysis and correlation of the data assumed, as well as in a complete and exhaustive documentation of what has been done in the individual phases.

Before starting to deal with this topic, it is necessary to give some definition. We have to distinguish two fields in this subject. The first one is Digital Forensics (Reith *et al.*, 2002) and the other one is Computer Forensics.

Digital forensics is the science that allows, through the use of specific methodologies (Beebe & Clark, 2004; Carrier & Spafford, 2003) and tools the identification, storage and analysis of digital evidence. An important concept before continuing to explain the topic is the definition of a "*digital proof*". It's an information, with probative value, that is either stored or transmitted in a digital format.

Computer Forensics is another point of view. It is the discipline that deals with the preservation, identification, study, documentation of computers, or systems information in general, in order to highlight the existence of evidence in the course of an investigative activity (Casey, 2009).

For lawyers, Digital Forensics means to examine digital media and technological systems in order to extract the evidence required to demonstrate or refute the question that has been asked.

We are going to describe which is the accurate application of digital forensics procedures ensuring the integrity, authenticity, truthfulness, non-repudiation and completeness of the test, which are the basis of computer forensics itself.

First of all, we characterize the computer forensics activity summarized in the identification, preservation, acquisition, analysis and correlation of the data assumed, such as a collection of a complete and exhaustive documentation of what has been carried out in every step of process.

In second part of the work we analyze kinds of data that are usually an attack target, such as identity, medical, work, educational, financial data and so on. Today, these data are also well protected by General Data Protection Regulation (GDPR) (European Commission, 2018), but in the last five years, since 2014 to 2019 we had an increasing cyber Crime Activity. Of all cyber attacks in 2019, 83% were due to cybercrime compared to 63% in 2014. Technical community is particularly concerned and attentive. In consequence of intensive use of ICT (Shiuh-Jeng, 2007), especially during COVID-19 pandemic, IT fraud further increased. This period was hard test for ICT infrastructure, but it also shows we are not completely protected in software technology against cyber attacks. Moreover, Internet surfers and company employees (Willison, 2006) do not generally apply any security policy, so many ICT frauds happen due for naivety and lack of knowledge. So, we thought it appropriate to describe all Cyber attack techniques in this work.

17 more pages are available in the full version of this document, which may be purchased using the "Add to Cart" button on the publisher's webpage:
www.igi-global.com/chapter/computer-forensics-and-cyber-attacks/261728

Related Content

Security Challenges in Network Slicing in 5G
Rashmi Mishraand R. K. Yadav (2021). *Evolution of Software-Defined Networking Foundations for IoT and 5G Mobile Networks (pp. 1-14).*
www.irma-international.org/chapter/security-challenges-in-network-slicing-in-5g/265028

A Novel OpenFlow-Based DDoS Flooding Attack Detection and Response Mechanism in Software-Defined Networking
Rui Wang, Zhiyong Zhang, Lei Juand Zhiping Jia (2015). *International Journal of Information Security and Privacy (pp. 21-40).*
www.irma-international.org/article/a-novel-openflow-based-ddos-flooding-attack-detection-and-response-mechanism-in-software-defined-networking/148301

Risk Analysis Using Simulation Software Applied on a Road Infrastructure Project
Vijaya S. Desai (2015). *International Journal of Risk and Contingency Management (pp. 53-62).*
www.irma-international.org/article/risk-analysis-using-simulation-software-applied-on-a-road-infrastructure-project/127541

A Subspace-Based Analysis Method for Anomaly Detection in Large and High-Dimensional Network Connection Data Streams
Ji Zhang (2012). *Privacy, Intrusion Detection and Response: Technologies for Protecting Networks (pp. 193-219).*
www.irma-international.org/chapter/subspace-based-analysis-method-anomaly/60440

Investigating the Concept of Information Security Culture
Daniel Oostand Eng K. Chew (2012). *Strategic and Practical Approaches for Information Security Governance: Technologies and Applied Solutions (pp. 1-12).*
www.irma-international.org/chapter/investigating-concept-information-security-culture/63080