Chapter 8
The Fundamentals of Digital Forensics

Kirti Raj Bhatele
Rustamji Institute of Technology, India

Shivangi Jain
Rustamji Institute of Technology, India

Abhishek Kataria
Rustamji Institute of Technology, India

Prerana Jain
Rustamji Institute of Technology, India

ABSTRACT

This chapter simply provides a brief introduction to the various fundamentals and concepts that are related to the digital forensics. The overview of the digital forensics comprises the life cycle of the digital forensics with different stages, i.e., the preparation, collection, analysis, and reporting. The evaluation of the digital forensics tools comprises the encase forensic, The FTK(forensics tool kit), and The Helix digital forensic tool with their benefits and limitations. The digital forensics tools and techniques examination comprises the digital examination techniques, along with the live forensics analysis and the recovery of window registry, and the comparison of the digital forensics tools, and also focuses on the ACPO guidelines for digital forensics analysis.

INTRODUCTION

Digital forensics is a branch of science which deals with a collection of evidences, investigation and reverse engineering, which can determine that how the computer was compose. There are multifarious tools and methods which are available to work properly and to help investigators to authenticate and analyze the evidence (Bennett, 2012). The goal which comes under the prospects of digital forensics is to preserve any kind of digital evidence in the most primitive form. Digital forensic is based on perform-

DOI: 10.4018/978-1-7998-2701-6.ch008

ing structured research by collecting, identifying and validating the digital evidences or information for the major purpose of reimagining past events related to the cyber crime which took place on a victim's computer.

Despite this, there are Challenges which are faced by digital forensics investigators that are categorize into three parts:-

1. Technical challenge like encryption, stagnography, different media formats and analysis.
2. Legal challenge like privacy issue, lack of standardized international legislation and administrative issue.
3. Resource challenge like time taken for acquiring and analyzing forensic media.

Crimes occur and the investigations hit a dead end because there appears to be no witness or evidence—that is, until digital forensics comes into play. The FBI solved a case using computer forensics in 2008 where a Incident Response and Digital Forensics A case was received by the FBI govt in 2011 in which the two children being sexually abused at a hotel. Unfortunately, by the time the tip was received, the crime had occurred. At that time there was no evidence so that the charges can be imposed on the culprit until the computer of the accused was analyzed. The evidence on the computer, a deleted e-mail with directions to the hotel where the abuse occurred, was enough to charge three adults, who are now serving life sentences in prison. There are also times when you do not know a crime was committed until a forensic analysis is performed. Recall the situation described about the trade secret accessed by an executive after she quit and before she left to work for a competitor. The point is that an incident may appear to be innocuous or impossible to solve until the situation is analyzed. For example, in a situation where the server seemingly went off-line for no reason, after analyzing the log files, you may determine that the cause was malware installed after an intrusion. If a crime has been committed or is even suspected, it is of the utmost importance that the investigator has collected and documented the evidence in a forensically sound manner because the next step would be to hand all of the evidence off to law enforcement (Beebe, 2009).

There was another application for digital forensics is gathering of evidences for e-discovery—the pre-trial phase where electronic evidence is collected. For example, a lawyer may want to prove a spouse's infidelity and may use a forensic analysis of e-mail files to prove the accusation. In evidence gathering, technique and accuracy are critical to ensure the authenticity of the data collected when an incident occurs. The forensic investigator needs always to keep in mind that he or she may be called on to defend the techniques utilized to gather the evidence. A case law is presented to demonstrate what can happen, when the law is not followed while collecting and preserving evidence. Handling digital evidence is a complex process that should be handled by a professional (Beebe, 2009). If not handled with care, it can be easily destroyed and rendered inadmissible if a court case ensues. There is some evidence that can be easily found but there may be some other evidence that have been hidden, deleted, or encrypted and cannot access by anyone. Adding to the complexity, if the evidence is not handled properly, it will be thrown out or the case will be lost.

LIFE CYCLES OF DIGITAL FORENSICS

There are four main stages of the digital forensics life cycle.