

# Roichuddin Rana

*by* Iftekhar Efat

---

**Submission date:** 13-Mar-2022 12:46AM (UTC-0500)

**Submission ID:** 1782971512

**File name:** ASH1925003M.pdf (195.1K)

**Word count:** 1992

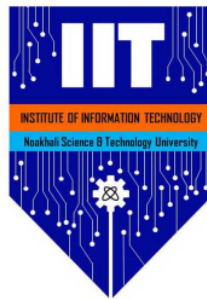
**Character count:** 10458

# Computer forensics on the rise- How significant is it in the current digital era?

*Roichuddin Rana*  
ASH1925003M

March 13, 2022

Report submitted for **SE2206: Information Security Lab** under BSc. in Software Engineering Program, **Institute of Information Technology (IIT)**, Noakhali Science and Technology University




Project Area: **Information Security** .....

Project Supervisor: **MD. IFTEKHARUL ALAM EFAT**

Assistant Professor

Institute of Information Technology (IIT)

Noakhali Science and Technology University

 In submitting this work I am indicating that I have read the University's Academic Integrity Policy. I declare that all material in this assessment is my own work except where there is clear acknowledgement and reference to the work of others.

I give permission for this work to be reproduced and submitted to other academic staff for educational purposes.

## Abstract

With the development of Computer and information technology, the digital crimes are also on the rise. Computer forensics is an emerging research area that applies computer investigation and analysis techniques to help detection of these crimes and gathering of digital evidence suitable for presentation in courts. This paper provides foundational concept of computer forensics, outlines various principles of computer forensics, discusses the model of computer forensics and presents a proposed model. The adoption of computers into every aspect of modern society has been accompanied by the rise of E-crime. The processes and techniques employed by the field of computer forensics offer huge potential for the extraction and presentation of electronic evidence in a court of law. This report analyzes the increasing issues that currently or could potentially impact the computer forensics field from the perspective of information security.

**Keywords:** Computer forensics, digital evidence, e-crime, electronic evidence.

## 1 Introduction

The use of information technology has grown swiftly all over the world in the twenty first century. Readily correlated to this enhancement is the increased amount of criminal performances that include digital crimes or e-crimes throughout the world. These digital crimes set new challenges on inquisition, prevention, detection and prosecution of the corresponding offences.

Among other issues in gathering proof from computers, one basic difference between paper documents and digital data is that electronic data can be easily copied and modified. A suspect may easily traverse that the evidence found in his/her computer was implanted by the law enforcement agency after the computer has been taken by the agency. It is very urgent to identify the file system integrity of the suspect's computer after it has been taken by the law enforcement agency.

## 2 Background

### 2.1 Definition of Computer Forensics

A classical definition of Computer forensics is “The scientific examination and analysis of data held on, or retrieved from, computer storage media in such a way that the information can be used as evidence in a court of law”. [2]

Computer forensics can be an fundamental facet of modern investigations. When a crime is committed and an investigation is started, one of the more common places to look for clues is the computer or cell phone of a suspect. This is where a computer forensics professional enters the picture.

When a suspect has been identified and their personal computer or cell phone taken into evidence, a computer forensics professional goes searching for data that is relevant to the investigation. When searching for information, they need to be careful to follow detailed procedures that allow their findings to be used as evidence. The information they uncover, whether it be documents, browsing information or even metadata, may then be used by prosecution to create a compelling case against the suspect.

Computer forensics is a field of information technology that uses investigative techniques to identify and store evidence from a computer device. Often, computer forensics is used to uncover evidence that could be used in a court of law. Computer forensics also encompasses areas outside of investigations. Sometimes professionals in this field might be called upon to recover lost data from drives that have failed, servers that have crashed or operating systems that have been reformatted.

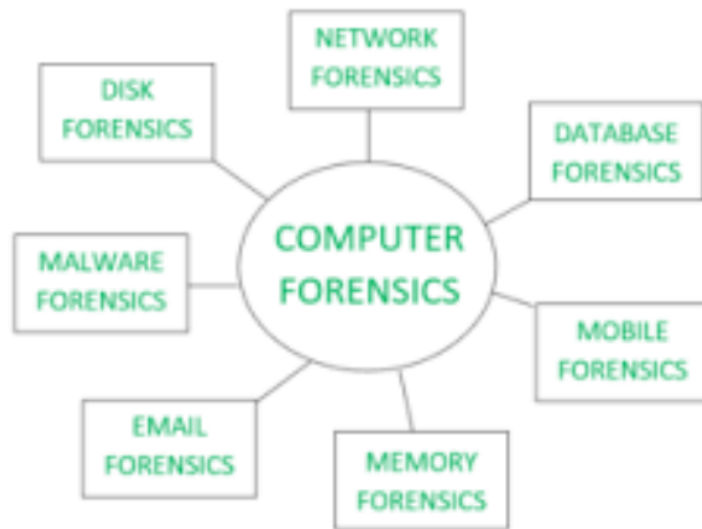


Figure 1: Branch

of Computer Forensics

## 2.2 Principles of Computer Forensics

According to computer forensics, the term “evidence” has the following meaning: “Any information and data of value to an investigation that is stored on, received, or transmitted by an electronic device. This evidence is acquired in physical or binary (digital) form that may be used to support or prove the facts of an incident. the properties of digital evidence as follows:

- Is latent, like fingerprints or DNA evidence.
- Crosses jurisdictional borders quickly and easily.
- Is easily altered, damaged, or destroyed.
- Can be time sensitive.

The first section, in many cases, that you present should present related background material [?]. It might include:

- literature review or related work section;
- common notation and definitions; and/or

- references for techniques to be used.
-

### 3 Methods

For digital evidence to be admissible in court, investigations should be conducted in a manner that adopts the principles of computer forensics. The following steps are involved in computer forensics investigations:

1. A computer system containing crucial evidence is secured to ensure that data are safe.
2. All files in a computer system that are not encrypted are copied.
3. Deleted information is retrieved.
4. Contents of hidden files are revealed using specific software to identify hidden data.
5. Protected files are decrypted and accessed.
6. Inaccessible parts of computer disks are analyzed to locate files that could contain crucial data.
7. All steps of the procedure are documented. [1]



Figure 2: Methods of Computer Forensics

### 3.1 Preservation

- Ensure that all digital evidence collected is properly documented, labeled, marked, photographed, video recorded or sketched, and inventoried.
- Ensure that special care is taken with the digital evidences material during transportation to avoid physical damage, vibration and the effects of magnetic fields, electrical static and large variation of temperature and humidity.
- Ensure that the digital evidence is stored in a secure, climate-controlled environment or a location that is not subject to extreme temperature or humidity.
- Ensure that the digital evidence is not exposed to magnetic fields, moisture, dust, vibration, or any other elements that may damage or destroy it.



## 4 Results

According to a snippet from the United States Security Service, the functions computer has in different kinds of crimes could be divided into aspects as follow:

- As contraband or fruits of a crime

E.g. some criminals obtain copies of software without permissions from the software producers so that this action violates the law of copyright. In this case, the computer (more accurately, the application stored on a CD or installed in a computer) is a contraband and fruits of the crime.

- As an instrumentality of the offense

E.g. a criminal uses a computer to attack another computer on the internet, or uses a printer to print kidnap letters.

- As a tool which is only incidentally used in a crime Since computer and digital media are so widely used today, sometimes they are used unintentionally by the criminals, such as storing account tables or communicating with their accomplices.

- As a tool both instrumentality to the offense and a storage device for evidence

In most courts, there are four types of evidence. Computer files that are extracted from a subject machine and presented in court typically fall into one or more of these types:

- Documentary evidence is paper or digital evidence that contains human language. It must meet the authenticity requirements outlined below. It is also unique in that it may be disallowed if it contains hearsay. Emails fall into the category of documentary evidence.

- Real evidence must be competent (authenticated), relevant, and material. For example, a computer that was involved in a court matter would be considered real evidence provided that it hasn't been changed, altered, or accessed in a way that destroyed the evidence. The ability to use these items as evidence may be contingent on this fact, and that's why preservation of a computer or digital media must be done.

- Witness testimony. With ESI, the technician should be able to verify how he retrieved the evidence and that the evidence is what it purports to be, and he should be able to speak to all aspects of computer use. The witness must both remember what he saw and be able to communicate it.

- Demonstrative evidence uses things like PowerPoint, photographs, or computer-aided design (CAD) drawings of crime scenes to demonstrate or reconstruct an event. For example, a flowchart that details how a person goes to a Web site, enters her credit-card number, and makes a purchase would be considered demonstrative.

For any of these items to be submitted in court, they each must, to varying degrees, pass the admissibility requirements of relevance, materiality, and competence. For evidence to be relevant, it must make the event it is trying to prove either more or less probable. A forensic analyst may discover a certain Web page on the subject hard drive that shows the subject visited a Web site where flowers are sold and that he made a purchase. In addition to perhaps a credit-card statement, this shows

that it is more probable that the subject of an investigation visited the site on his computer at a certain time and location.

Materiality means that something not only proves the fact (it is relevant to the fact that it is trying to prove) but is also material to the issues in the case. The fact that the subject of the investigation purchased flowers on a Web site may not be material to the matter at hand.

## 5 Conclusion

Prosecuting suspects of computer related crimes is becoming more and more effective as a result of improvements in the methods of carrying-out investigations and obtaining evidences from crime scenes. A computer can be used as a tool to perpetuate a crime, a computer can also be the target of a crime, or it can serve as an evidence repository for storing valuable information about a crime. A suspect can be held responsible for a crime when an investigation is still ongoing. Several investigation processes have been proposed but they weren't able to efficiently address the issue of computer crime, as a result of sophistication and change in paradigm in which computer crimes are being committed. A more general approach to investigating a computer crime scene makes evidence from the crime scene admissible in the court so that suspects can be tied to the crime. This report paper explains a recent and general approach of an investigation process that can be used in computer forensics. With this general approach, a computer crime scene can be more effectively investigated. The crime scene conceals detail evidences which are needed to tie a suspect to a crime committed and possibly obtain a conviction.

## 6 Appendices

In businesses, Digital Forensics is an important part of the Incident Response process. Forensic Investigators identify and record details of a criminal incident as evidence to be used for law enforcement. Rules and regulations surrounding this process are often instrumental in proving innocence or guilt in a court of law.

## References

- [1] Hong Guo, Bo Jin, and Daoli Huang. Research and review on computer forensics. In *International Conference on Forensics in Telecommunications, Information, and Multimedia*, pages 224–233. Springer, 2010.
  - [2] Liu Qian, Fredrik Hoglin, and Patricia Alonso Diaz. Computer forensics. *Uppsala University*, 2007.
-

# Roichuddin Rana

## ORIGINALITY REPORT

81 %  
SIMILARITY INDEX

81 %  
INTERNET SOURCES

43 %  
PUBLICATIONS

49 %  
STUDENT PAPERS

## PRIMARY SOURCES

1	<a href="#">dokumen.pub</a> Internet Source	20%
2	<a href="#">pdfs.semanticscholar.org</a> Internet Source	13%
3	<a href="#">www.devry.edu</a> Internet Source	10%
4	<a href="#">journals.co.za</a> Internet Source	10%
5	<a href="#">www.it.uu.se</a> Internet Source	8%
6	<a href="#">www.cs.hku.hk</a> Internet Source	4%
7	<a href="#">www.tandfonline.com</a> Internet Source	3%
8	<a href="#">v1.overleaf.com</a> Internet Source	3%
9	<a href="#">www.eccouncil.org</a> Internet Source	2%

10 [webcache.googleusercontent.com](http://webcache.googleusercontent.com) 2%

---

11 [www.overleaf.com](http://www.overleaf.com) 2%

---

12 [global.oup.com](http://global.oup.com) 2%

---

13 [www.coursehero.com](http://www.coursehero.com) 1%

---

14 [computer-forensics.safemode.org](http://computer-forensics.safemode.org) <1%

---

---

Exclude quotes On

Exclude matches Off

Exclude bibliography On



**Article Error** You may need to use an article before this word. Consider using the article **the**.



**Article Error** You may need to use an article before this word. Consider using the article **the**.



**Article Error** You may need to use an article before this word.



**P/V** You have used the passive voice in this sentence. Depending upon what you wish to emphasize in the sentence, you may want to revise it using the active voice.



**Frag.** This sentence may be a fragment or may have incorrect punctuation. Proofread the sentence to be sure that it has correct punctuation and that it has an independent clause with a complete subject and predicate.



**Article Error** You may need to use an article before this word. Consider using the article **the**.



**P/V** You have used the passive voice in this sentence. Depending upon what you wish to emphasize in the sentence, you may want to revise it using the active voice.



**P/V** You have used the passive voice in this sentence. Depending upon what you wish to emphasize in the sentence, you may want to revise it using the active voice.



**Confused** You have used **an** in this sentence. You may need to use **a** instead.



**P/V** You have used the passive voice in this sentence. Depending upon what you wish to emphasize in the sentence, you may want to revise it using the active voice.



**Article Error** You may need to use an article before this word.



**Article Error** You may need to use an article before this word.



**Article Error** You may need to use an article before this word.



**S/V** This subject and verb may not agree. Proofread the sentence to make sure the subject agrees with the verb.



**Possessive** You may need to use an apostrophe to show possession.



**Article Error** You may need to use an article before this word.



**Possessive** You may need to use an apostrophe to show possession.



**Wrong Form** You may have used the wrong form of this word.



**Missing ", "** You may need to place a comma after this word.



**Prep.** You may be using the wrong preposition.



**Missing ", "** You may need to place a comma after this word.



**P/V** You have used the passive voice in this sentence. Depending upon what you wish to emphasize in the sentence, you may want to revise it using the active voice.



**Article Error** You may need to remove this article.



**Dup.** You have typed two **identical words** in a row. You may need to delete one of them.



**Proofread** This part of the sentence contains a grammatical error or misspelled word that makes your meaning unclear.



**Article Error** You may need to remove this article.



**Missing ", "** You may need to place a comma after this word.



**Missing ", "** You may need to place a comma after this word.



**Article Error** You may need to use an article before this word. Consider using the article **a**.



**Verb** This verb may be incorrect. Proofread the sentence to make sure you have used the correct form of the verb.