Forensic science steps to applying on computer to process and analyze digital evidence

Santosh S. Varpe[1]

[1] Assistant Professor, Computer Department, Amrutvahini College Of Engineering, Sangamner, Maharashtra, India

ABSTRACT

Digital investigators collect the crime related information from the crime scene then making document and preserving digital evidence. To perform this task properly digital investigators need a methodology and also need help to find the scientific truth.

For this forensic science is useful, it offer tested methods for processing and analyzing evidence and reaching to final conclusion. This paper provide seven stages of forensic science to process and analyze digital evidence. When applying all this stages of forensic science investigator easily collect and analyze digital evidence.

Keyword - *Forensic Science, Computer science, Digital evidence, Computer crime*

INTRODUCTION

Information stored in a binary form called digital evidence. The sources of digital evidences are digital camera, hard disk, pen drive, memory card etc. Digital evidence helps in tracing how crime was committed. Using digital evidence it is easy to find out offender. Digital investigators collect the crime related information from the crime scene then making document and preserving digital evidence. To perform this task properly digital investigators need a methodology and also need help to find the scientific truth[2].

For this forensic science is useful, it offer tested methods for processing and analyzing evidence and reaching to final conclusion. Places physical evidence into a professional discipline[3].

Following are stages to discovered digital proof from computer.

1. Preparation

2. Survey

3. Documentation

4. Preservation

5. Examination

6. Reconstruction

7. Reporting results

1. PREPARATION

Planning is important for searching evidence on computer. Before going to search site it necessary to understand whether search organization is small or large[3].
Investigator needs authorization to search organization. For this he must take a search warrant to search the organization. if computer is examine on site it is necessary to carry forensic tools for better search also understand the which operating system is used on computer, whether computer is connected to network then take help of network administrator for the search but don't trust on network administrator because he may be friend of suspect or he may try to hide the personal information of suspect, he may be an offender. Search team protects the integrity of the data[2].

At the crime scene investigator must collect the fingerprint of victim and suspect computer before touching keyboard[3]. Precaution is necessary at crime scene. If blood on crime scene then wear the hand glows before touching to any device[1]. Following are the items that can be used at crime scene

- Evidence bags

At crime scene if any damaged hard disk or pen drive is found Evidence bags used to package the evidence.

- Tags

Tags used to label the item.

- Paper and pencil

Paper and pencil used to drawing sketch of crime scene. When agent drawing sketch at crime scene there is chances of finding small items in room or LAN cable that are going from room to the other location of server.

- Digital camera

Digital camera used to capture photo of crime scene.

Use to make documentation. Photograph capture the exact positioning of crime scene.

- Toolkit

Toolkit contains screwdrivers for various size of screws and torch.

- Hard disk

Used to store the acquire data[2].

2. SURVEY

Crime scene survey means finding all sources of digital evidence and used to take decision about which information is relevant and which information is irrelevant. Survey gives idea about which information need to preserve from large set of information[2].
For surveying crime scene need to divide large area into small segments because of this it is easy to find small item on crime scene it also speed up the survey process.
It is two way process, first is survey of hardware and second is survey of software[1].
Survey of hardware includes laptops, PC, servers, firewall, routers, mobile devices, pen drive, CCTV camera, hard disk this devices contains lots of information so for surveying this devices investigator contact to network administrator or system administrator or recovery expert to analyze data[4].
Devices found on crime scene investigator send that devices to forensic labs to gain truth.
Survey of software depends on types of crime means suppose if criminal uses emails to commit crime then investigator need to track the origin of email.
In many cases like child pornography, credit card fraud involves internet, so computer keeps track of information about user activity in sys log file also contain in browser history. So surveying software investigator must search to this places.

3. DOCUMENTATION

Goal of documentation is to keep track of who collected evidence and who handle that evidence.

Well maintain documentation help to show in a court[4].

If judge ask for detail of any evidence then using documentation it is easy to find details of that evidence.

If any case investigator change and new investigator handle the case then using documentation new investigator easily understand case and he will get all information about crime. Photos, videos capture the real state of crime scene. Documentation form contain investigator name, case number, place where evidence found, name of suspect, name of eyewitness[5].

MD5 value of evidence is calculated at the time of collection of evidence and keeping in documentation.

Also documentation contain who having right to handle evidence. Documentation keeps integrity and authenticity of evidence. Documentation also help for new persons how to handle preserve evidences[2].

4. PRESERVATION

Preservation is important process, preserving digital evidence means no one can change evidence and evidence is stored at secure place. Suppose investigator found a suicide note on victim computer who drink poison, he must take a photo of that screen also save that note in hard disk, then check history of browser that may contain poison related link. In victim harassment case, suppose offender harass a victim by sending emails, then copy email and header of that harass email. Seal that computer[2]. If crime is happen using camera or criminal uses mobile phone or any device then place that devices in carry bags and label that devices include date and time device found. Suppose any damage hard disk found then tape that hard disk and take back up then keep it in secure place[4].

Use forensic tools to acquired digital evidence also disconnect the evidential computer from internet means isolate computer[7].

5. EXAMINATION

There are three levels of forensic examination: 1) survey forensic inspections, 2) preliminary forensic examination, and 3) in-depth forensic examination.

Filtering/Reduction

With the decreasing cost of storage media and increases size of storage media or in operating system investigator need to filter that's lots of data[2].

Evidence That May Be Examined

Questioned material may be consist of id cards, contracts, seals, stamps, bank checks, handwritten material, printed documents. The client should know that examination of this type of evidence can be problematic. Documents that don't contain direct identifiable marks may contain valuable evidence[3].In addition, writing instruments, rubber stamps, bag may be collected by the investigator. In computer documents, evidence could be taken from the metadata of electronic signature files, providing information such as who sign that document and written date of document[4].

6. RECONSTRUCTION

Investigative reconstruction shows more complete picture of crime. Using reconstruction it is easy to understand what happen at crime scene, who committed crime, where crime was committed.

Investigative reconstruction provides the link between victim, criminal and crime scene. The link may be geographical related or school related or business related. Three types of reconstruction first functional, second relational, third temporal. Functional analysis It helps to understand digital evidence. Functional analysis proved whether digital evidence was tempered. Whether computer is capable of performing actions to commit the crime.

It will test whether system work properly or not. For example suppose suspect person claim that when crime committed at that time he was in another city and sending emails to his friend, so using functional analysis it is easy to find the criminal[2]. Relational analysis used to identify the relationship between victim, crime scene and suspect.

Temporal analysis

We know that in any investigation date time and sequence of event are helpful for investigator to find criminals. So operating system keeps tracks of all users data means account access time of user, activity done by user on computer all are stored in a sys log file[4].

7. REPORTING

It is last stage of digital evidence examination. Whatever found in investigation that are integrated together and conclude into final report. This digital evidence examiner present in a court. Report contain all evidences of related to crime called strong report. Report structure contain the introduction means who wrote report, case number, what was found. It contain evidence related summary means what evidences are examine, MD5 value of all evidences.
Report contain which tools are used for examination and where the examine data stored[2].
File related information is stored means date and time of file created,MD5 value of file also how file is recover from disk and where file is stored.

8. CONCLUSIONS

Using seven stages of forensic science it is easy to process and analyze digital evidence. When applying all this stages of forensic science investigator easily collect and store digital evidence. Forensic science helps investigators to find truth behind crime.

9. ACKNOWLEDGEMENT

“Feeling gratitude and not expressing it, is like wrapping a present and not giving it". I take this opportunity to express my profound gratitude and deep regards to my parent.

6. REFERENCES

[1]. Mohd Taufik Abdullah, Ramlan Mahmod, Abdul Azim Ab. Ghani, Mohd Zain Abdullah4, and Abu Bakar Md Sultan(2008), Advances in Computer Forensics, International Journal of Computer Science and Network Security, VOL.8 No.2.

[2]. Digital evidence and computer crime, forensic science, computers and internet, eoghan casey.

[3]. Santosh S. Varpe, Visual Cryptography for Providing Privacy to Biometric data, International Journal of Current Engineering and Technology (ISSN: 2277 – 4106) in Vol.5, No.4 (July/Aug 2015).

[4]. Santosh Varpe, Visual Cryptography for Providing Privacy to Biometric Data, International Journal of Current Engineering and Technology (ISSN: 2277 – 4106) in Vol.4, No.6 (Nov/Dec 2014).

[5]. Amarpreet S. Arora, Susheel Ch. Bhatt, Anamika Pant(2012), Forensics Computing-Technology to Combat Cybercrime, International Journal of Advanced Research in Computer Science and Software Engineering,Volume 2, Issue 7.

[6]. Ashcroft, J., 2001. Electronic Crime Scene Investigation Guide: A Guide for First Responders. National Institute of Justice.

[7]. Beebe, N. L. and Clark, J. G. 2005. A hierarchical, objectives-based framework for the digital investigations process. Digital Investigation, 2 (2). 147-167.

BIOGRAPHIES

	Santosh Varpe obtained M.E.(Hons.) degree in Computer Engineering from the VACOE, Ahmednagar (2016), Savitribai phule pune university, Maharashtra, India. He is currently an Assistant Professor at Amrutvahini College of Engineering, Sangamner, A.nagar, Maharashtra, India.