Research on Capture of Live Digital Evidence

Ying Zhang
Key Laboratory of Information Network Security,
Ministry of Public Security,
People's Republic of China (The Third Research Institute of Ministry of Public Security)
Shanghai, China
zhangying@stars.org.cn

Feng Gao
Key Laboratory of Information Network Security,
Ministry of Public Security,
People's Republic of China (The Third Research Institute of Ministry of Public Security)
Shanghai, China
gaofeng@stars.org.cn

***Abstract*—With the of development of internet, more and more criminals commit the crime via utilizing the information technology, which has aroused the forensic scientists' interests simultaneously. And the concept of digital evidence has been brought to society consequently. Due to the feature of digital evidence such as easy-loss or unstable, how to implement capture of live system is critical to the forensic technicians and other related staff. This paper analyzes the correct procedures of on-site acquisition concretely, including planning, scene-protection, collection, preservation, packaging, transportation, and storage.**

Keywords-electronic evidence; live; capture

I. INTRODUCTION

With the continued development and growth of internet, more and more people have moved their attention to information technology, along with the popularity of electronic devices. Meanwhile, the internet, computer networks and automated data systems present an enormous new opportunity for committing criminal activity.[1] Various electronic devices especially computers and servers are utilized to enable and support crimes, which undermine public safety and social stability greatly. Whether the crime involves attacks against computer systems, the information they contain, or more traditional crimes such as murder, money laundering, trafficking, or fraud, electronic data is involved.[1] All the data mentioned above is treated as digital evidence.

Digital evidence or electronic evidence is any probative information and data of investigative value stored or transmitted in digital form by an electronic device that a party to a court case may use at trial.[2] The use of it has increased in the past few decades in terms of various types including e-mails, digital photographs, word processing documents, internet browser histories, instant messaging histories, databases, the content of computer memory, digital video and audio files, the content of registry and so on.[2]

According to article 23, chapter 4 of "procedure provisions concerning handling administrative cases of the public security organ" which was promulgated on August 24 2006, digital evidences has been treated as one kind of criminal evidence explicitly. Besides that, other related legal provisions such as "PRC, Electronic Signature Law" and "Contract Law of P.R.China" acknowledge and accept the legal effect of digital evidence as well.

It is known to all that acquiring live digital evidence is of great difficulty, as a result of its easy-loss, high-accuracy, unstable, fragility, concealment and multiple-form. That means, investigators or technicians are required to be adequately trained and equipped to properly handle digital evidence. Nevertheless there is not any national standard concerning the correct procedures to commit the live capture of digital evidence nowadays. Therefore this paper will provide guidance to the forensic technicians or investigators on acquiring live digital evidences.

For the scope of this paper, the focus will be on the concrete procedures regarding capturing live digital evidences. The rest of the paper is organized as follows. The pre-planning for on-site acquisition is described in section 2. The procedures to protect the crime scene are demonstrated in section 3. Section 4 explains proper approaches to implement evidence collection. Preservation will be illustrated in section 5. Packaging, transportation and storage is demonstrated in section 6. Conclusion is in section 7.

II. PLANNING

Careful planning is required to be drafted before live evidence acquisition. Concretely speaking, it is constituted of follow components.

- The target and scope of live acquisition.
- National standards and/or technical procedures adopted.
- Investigators or technicians who will participate in the acquisition and their responsibility in this activity respectively.
- Electronic equipment and tools supposed to be utilized in the acquisition.
- The priority order and concrete measures of acquisition.
- The influence which is caused by the procedures probably.
- Restrictions mandated by the courts which may influence the process

All these factors mentioned above are essential to the collection of digital evidences. Here we will take the factor personnel and equipment for example.

A. Personnel

Digital forensics staff could be divided into three levels as follow, depending on the specialist training and knowledge.[3]

- Digital crime scene technicians: individuals who are in charge of collecting data on-site and supposed to be trained in evidence handling and documentation as well as basic crime reconstruction, so as to help them locate all possible evidences.
- Digital evidence examiners: individuals who are in charge of processing particular kinds of evidences and supposed to be trained with specialized technology. In addition, they are likely to grant the certification in their area.
- Digital investigators: individuals who are in charge of investigation and supposed to be trained in the aspect of overall control instead of very specialized technology about one certain field. They are also responsible for reconstructing the actions related to a crime using information from above two kinds of staff to create a complete scene for attorneys.

As we all know, all the staff mentioned above could be involved in the live acquisition. For instance, there is no clear distinction between digital crime scene technicians and digital evidence examiners, considering the fact that data recovery requires more specialized technology than basic evidence documentation, collection and preservation.[3]

B. Equippment

Special tools and equipment may be required to collect electronic evidence. Experience has shown that advances in technology may dictate changes in the tools and equipment required.

Equipment and tools are essential to the acquisition for the reason that they are likely to affect the results. Generally speaking, they are classified according to the different stage including documentation, collection, packaging and transportation.[2]Then we will list some equipment and tools for instance.

1) Documentaiton equipemnt and tools

- Indelible felt tip markers
- Stick-on labels

2) Collection equipemnt and tools

- Forensic workstation
- Read-only interface
- SD/TF/MicroSD card reader
- Video cassette recorder
- Specialized screwdrivers
- Small tweezers

3) Packaging tools

- Antistatic bags
- Evidence bags
- Evidence tape
- Packing materials

4) Transportation tools

- Antistatic bubble wrap
- Packing tape
- Sturdy boxes of various sizes

III. Securing, Evaluating and Recording the Scene

Digital crime scene technicians are required to take measures so as to protect the integrity of digital evidences. Besides that, they are also likely to evaluate and record the scene so that backtracking could be committed anytime.

A. Protection

The first responder should isolate irrelevant personnel with belt as well as keep all electronic devices the same condition as before so as to prohibit digital evidences from being destroyed.

B. Record

The technicians are also required to record the site condition in the approach of videotapes and photographs, which includes the condition of electronic device, the cable distribution and so on.

C. Encapsulation

As for the power-off one, the technicians are required to encapsulate related electronic devices and media with authorization. Concrete procedures are listed as follow.

1) Choos the correct means: The encapsulation means is supposed to ensure that encapsulated devices and media could not be utilized without decapsulation.

2) Recording: The technicians should record the encapsulation procedure with the approach of videoes and photographs. And those multimedia records are required to reflect the seal clearly.

3) Encapsulation: The subsidiary electronic devices and media should be encapsulated as well.

IV. Collection

Digital evidence is required to be handled carefully so that its evidentiary value could be guaranteed. That means, it relates not only to the physical integrity of the device and media discussed above, but also to the information contained inside it.

A. Principles

The extraction, preservation and capture of live data should follow some certain principles.

- The extracted electronic data is forbidden to be stored in the original storage medium.
- New applications are forbidden to be installed in the target system. If there is inevitable reason indeed, technicians must record the applications installed and the purpose of installation.
- Detailed and accurate documents are required to be recorded regarding operations implemented and possible affections to target systems.

B. Procedures

All related information on-site is required to be gathered so as to help future analysis. The evidence on-site consists of several types, which will be discussed as follow.

1) Nonelectronic evidence: There is nonelectronic evidence realted to subsequent analysis of digital evidence on site in other forms. For instance,it could be written user name or password or other handwirrten notes, blank pads of paper with indented writing, hardware or software manuals, calendars, literature, text or graphical computer printouts and photographs.[2] Generally speaking, this kind of evidence is frequtently in close proximity to electronic device.

2) Computers stand-alone: "Stand-alone" means the computer is not connected to any network or other computer. When investigating such kind of computers, the first thing required to do is checking whether it is on. If it is on, document existing conditions and commit following procedures.

a) Document: Record all actions technicians played and any abnormality observed in the monitor, computer, printer and other devices.

b) Observation: Observe the monitor and determine whether it is on, off or in sleep mode. Then different actions will be taken according to the situations.

- If monitor is on and screen is visible, photograph the screen and document the information displayed.
- If monitor is on and screen is blank, move the mouse slightly to wake the screen which shows work product or requests a password. Photograph the screen and record the information displayed.
- If monitor is off record the condition. Turn it on and determine whether the monitor is described in above two and take corresponding measures.

c) Acquisition: Acquisition of volatile system information should follow those steps.

- Searching and preserving the following data should be a priority.

i. Open an unsaved documents
ii. User password
iii. And other information related to the investigation

- Obtain digital evidence relevant to investigation in the system ,which includes

i. Running processes
ii. Operating system information
iii. Unsaved data
iv. And other information related to the investigation

d) Arrangement: After the collection, electronic devices should be taken from on-site and serveral operations are supposed to be played.

- Remove the power source cable from the computer instead of the wall outlet. If it is a laptop, the battery pack is supposed to be removed as well.
- Check for outside connectivity and identify it.
- Remove any floppy disks that are present and label them as evidences as well. CDs are forbidden to be removed.
- Document the model, producer and serial numbers.
- Photograph and diagram the connections of the computers and corresponding cables.
- Label all connectors and cable ends so as to allow for later reassembly. And unused connection ports should be labeled as "unused".

3) Computers networked: Most business environments frequently have multiple computers connected to each other through network. In this condition live acquisition is more complicated than the "stand-alone" one. Following procedures are supposed to be taken.

a) Document: Record all actions as described in last pragraph.

b) Observation: Observe the monitor as described in last pragraph.

c) Acquisition: Acquisition of volatile system information should follow those steps.

- Searching and preserving the following data should be a priority.

i. Open an unsaved documents
ii. Chat records recently
iii. User password
iv. And other information related to the investigation

- Obtain digital evidence relevant to investigation in the system ,which includes

i. Running processes
ii. Operating system information
iii. Unsaved data
iv. Connected network users
v. And other information related to the investigation

If necessary, online acquisition is required and following information is supposed to be collected.

i. Chat records via using instant messaging.
ii. Open webpage
iii. Open emails in the client
iv. And other information related to the investigation

d) Arrangement: The arrangement is supposed to be taken as listed in last paragraph.

V. PRESERVATION

All digital evidences obtained on-site must be preserved in the following manners.

A. Verification of integrity

Hash values of extracted digtial data and storage medium are required to be calcualted and recorded.

B. Back-up

Copy and produce the back-up of original stroage medium and encapsulate it as described in chapter 3.

C. Encapsulation

Regarding the original storage medium which could not be verfied via using above two methods, it is supposed to be encapsulated as described in chapter 3. Moreover, the reason why it is not verfied via using above two methods should be recored as well.

VI. PACKAGING, TRANSPORATION AND STORAGE

Generally speaking, electronic device and media are sensitive to temperature, humidity, physical shock, static electricity and magnetic sources. Therefore, careful measures are likely to be taken during the process of packaging, transporting and storage.

A. Packaging

The packaging procedures are listed as follow.

- Digital evidences collected must be properly labeled, photographed and recorded before packaging.
- Magnetic media must be packed in antistatic packaging. Materials that can produce static electricity are forbidden.
- Folding, bending or scratching electronic device and media are forbidden.
- Containers utilized to store evidences must be properly labeled.

B. Transportation

The transporting procedures are listed as follow.

- Digital evidences collected must be placed away from magnetic sources.
- Storing digital evidences in vehicles for long time is prevented as much as possible.
- Poor environment such as excessive heat, cold or humidity is forbidden.
- Ensure the electronic device and media are placed correctly so as to avoid shock and vibrations.

C. Storage

The storage procedures are listed as follow.

- Digital evidences collected must be inventoried in accordance with related policies.
- Digital evidences collected must be stored in a particular area, which could protect them from magnetic sources, moisture, dust and other harmful particles or contaminants.

VII. CONCLUSION

In this paper we briefly describe the development of information technology, thereby introducing the concept of digital evidence and its significances. Nevertheless, due to the feature of it such as easy-loss or unstable, there is inevitable difficulty in the digital forensics. Besides that, there is not any authorized standard regarding procedures of on-site acquisition. This paper provides guidance to forensic community concerning the live acquisition of digital evidences, including pre-planning, scene securing, evaluating and recording, evidence collection, preservation, packaging, transportation and storage.

ACKNOWLEDGMENT

This work was financially supported by the basic science project of Ministry of public security, project number: 2012GABJC035.

REFERENCES

[1] David E. Learner, “Electronic Crime Scene Investigation,” Nova Science Pulishers, 2009, pp. 5–6.

[2] Information on “http://en.wikipedia.org/wiki/Digital_evidence”.

[3] Information on “http://en.wikipedia.org/wiki/Digital_forensic_process”.