The Journal of The Institute of Internet, Broadcasting and Communication (IIBC)
Vol. 16, No. 5, pp.49-54, Oct. 31, 2016. pISSN 2289-0238, eISSN 2289-0246

http://dx.doi.org/10.7236/JIIBC.2016.16.5.49
JIIBC 2016-5-8

디지털 수사 초동조치 대응인력 및 예비분석관들이 갖추어야 할 요건

Digital Investigation First Responder and Preliminary Analyst Requirements

조슈아 제임스*, 장윤식**

Joshua I. James*, Yunsik Jang**

요 약 디지털 증거를 다루는 범죄 사건 수사가 증가함에 따라 초동조치를 할 수 있는 인력과 개선된 수사절차 모델의 필요성이 증가하고 있다. 최근 들어 디지털 포렌식 분류(triage)와 예비분석 등의 개념이 수사·연구기관에 각광을 받고 있다. 하지만 초동조치 대응인력 및 예비분석관들이 구체적으로 어떤 훈련을 받아야 하는지에 대한 연구는 그다지 주목받지 못했다. 오히려 많은 조직에서 초동조치 대응인력이 전문적인 디지털 포렌식 분석관과 같은 실력을 갖추어야 한다고 여기고 있다. 본 연구에서는 '이상적인' 상황에서 디지털 수사의 초동조치 대응인력과 예비분석관들이 어떤 능력을 갖추어야 하며, 하드웨어 및 소프트웨어 측면에서의 필요사항과, 어쩌면 가장 중요하다 할 수 있는 교육훈련 조건에 대해 논하고자 한다.

Abstract As investigations dealing with digital evidence increase, so to does the need for skilled first responders and improved investigation process models. Recently the concept of digital forensic triage and preliminary analysis has been gaining popularity in investigation laboratories. At the same time, however, there has been little focus on specific training needs of first response and preliminary analysts. Instead, many organizations consider these responders to need the same skills as full digital forensic analysts. In this work we describe the 'ideal' digital investigation first responder and preliminary analyst, hardware and software requirements and most importantly, required training.

Key Words : Digital Forensic Triage, Forensic Preliminary Analysis, Digital Forensic Investigation, First Responder, Digital Forensic Process

Ⅰ. Introduction

Due to the growing problem of backlogs in digital forensic laboratories [1][2], digital forensic laboratories have been considering alternative process models to the standard preserve, acquire, analyze, report process [3]. Recently, the concept of digital forensic triage [4] or preliminary analysis [5] have been presented as ways to deal with the growing case backlog problem. In [2], digital forensic investigators were surveyed on their investigation process. It was found (Fig. 1) that investigators naturally go through an exhibit sorting phase to determine the most likely sources of evidence (triage), the conduct a preliminary analysis to quickly

*정회원, 한림대학교 교수
**정회원, 한림대학교 교수 (교신저자)
접수일자 : 2016년 8월 1일, 수정완료 : 2016년 9월 1일
게재확정일자 : 2016년 10월 7일

Received: 1 August, 2016 / Revised: 1 September, 2016 / Accepted: 7 October, 2016
**Corresponding Author: jakejang@hallym.ac.kr,
College of International Studies, Hallym University, Korea

gain more information about exhibits. From this preliminary analysis social and situational analyses will take place to determine if the exhibit should be sent for a further, time consuming full analysis. The results showed that almost 50% of exhibits are normally not relevant to the case, and can be confidently removed from further investigation through simply triage and preliminary analyses.

Fig. 1. Observed high-level investigation process of child exploitation material when deciding to continue investigation of a suspect exhibit, where the first three phases – and sometimes a situational analysis – are used to make a decision to continue with a full analysis.

그림 1. 용의자 증거의 계속 수사 여부를 결정하기 위해 앞의 세 단계(종종 situational analysis도 포함)가 활용됨을 보여주는 아동음란물의 고수준 수사절차 모델

Prior works have discussed the potential for triage and preliminary analysis, but have neglected a description of required training for such analysts. This work discusses the necessary prerequisites for candidates to the position of preliminary analyst and first responder (aka Triage Personnel) that will be assigned to Computer Forensic Triage Units. Section two covers the minimal and ideal prerequisites of the candidates. Section 3 discusses the hardware and software requirements for the first-response and preliminary investigator functions. Finally, section 4 proposes first and second tier training for successful candidates.

This work contributes to the field of digital forensic investigation by providing one of the first comprehensive training plans for a triage or preliminary analyst in a digital forensic investigation laboratory.

II. PREREQUISITES OF PERSONNEL

We define Computer Forensic Triage Units (CFTU) as generally having the following functions:

a. On scene collection, analysis, profiling, interviewing and documentation
b. Local station analysis, triage, elimination and documentation

Practitioners who will be performing these functions are often the same personnel, both on-scene and at the local station. Personnel under consideration must meet or exceed the following prerequisites before being admitted to the program.

1. Minimal Preliminary Analysis Personnel Requirements

a. Knowledge of traditional first-responder procedures, practices and issues
b. Traditional criminal investigation experience
c. Experience in criminal investigation documentation
d. A very basic knowledge of computing (able to complete basic computing tasks such as turning on a computer, word processing and accessing the Internet/email)
e. The candidate should have the ability to strictly follow directions, both spoken and by following a written manual
f. Must have a demonstrated interest
g. Self-motivated

2. Ideal Candidate

An ideal candidate will meet the minimal requirements (II.1), and also possess some or all of the following traits:

a. The candidate should have prior experience with computing fundamentals, for both hardware and software, through either university or self-taught. Ideally having obtained either a degree (in Computer Science or related) or having acquired technology -related certifications (CompTia A+, MCP, etc.).
b. Basic programming experience
c. Experience acquiring or analyzing digital evidence highly preferred
d. Experience with suspect interviews and interview techniques

e. Highly observant of their surroundings, and sensitive to the reactions of others
f. Be able to think quickly, adapting to and incorporating new information as it is discovered
g. The candidate must be patient. Patience for documentation, working with technology, and working with people.
h. The candidate should be 'competent' in their current position.

Ⅲ. HARDWARE AND SOFTWARE REQUIREMENTS

When dealing with various types of digital devices, each containing large amounts of data, hardware and software to access and process such devices is required [6]. This work will not discuss the costs of such hardware and software, but instead make minimal and ideal hardware and software recommendations.

Triage personnel function in two physical locations, on-scene and at the local station, and thus have two different sets of hardware and software requirements.

1. First Responder (each)

The first responder will need a library of tools available, as well as a method for saving the output of those tools. While tools such as Deepthought [6] and ANT [4] attempt to utilize the suspects hardware as much as possible, the ideal situation assumes the following hardware:

a. Writable CDs
b. External hard-drive (USB + FireWire) larger than the amount of data collected (ideally 500GB +)
c. A Laptop with a Gigabit Ethernet port, Wireless network card (preferably A, B, G, N and AC support), 6GB or more installed memory, writable CD/DVD ROM drive, FireWire and USB ports
d. A standard write-blocker and adapter kit
e. A 10/100/1000 network switch/hub+Gigabit-capable network cables

2. Preliminary Analyst

The preliminary analyst will have the task of collection, analysis as well as pre-incident setup. The preliminary analyst will reuse much of the hardware and software needed by the first-responder. Assuming the use of the tools, for example, provided by Europol, the following hardware and software is required:

a. Internet-accessible desktop PC with a writable CD/DVD ROM drive, 6GB or more installed memory, FireWire and USB ports, and a Gigabit Ethernet port.
b. A high-speed Internet connection
c. Writable CDs
d. External hard-drive (USB + FireWire) larger than the amount of data collected (ideally 500GB +)
e. A standard write-blocker and adapter kit
f. A 10/100/1000 network switch/hub+Gigabit-capable network cables

Ⅳ. TRAINING REQUIREMENTS

Training is a key point for the acceptance of any decisions from the CFTU [7], especially if those analysts should be experts in court [8]. Not only must the preliminary analyst have a 'better than basic' set of skills, but these skills must be updated a least annually, with the ideal being a high-level review, update and recertification every 6 months [9]. The initial training defined will be described as basic level 1 and advanced level 2. Level one training will be one week, and will include:

a. Introduction to Computers, Peripheral Devices & Networking

This lecture will discuss the components of modern computers, auxiliary storage solutions and provide a brief introduction to local networks.

'what is a computer', boot sequence, hardware, peripherals, media and connectors, operating systems, applications, Windows Registry, networks, cell phones, wireless

b. Forensic Documentation

Scene/media/connection photography, forensic reporting, suspect reactions/behaviors, who owns media, where media was found, if machine was running, determining the relationship between owner and suspect

c. Legislation

This topic summarizes the current legislation that is specific to IT crime and outlines some practical considerations for investigators.

d. Search and Seizure Guidelines

At the end of this lecture, participants will be able to explain the principles of electronic evidence seizure and demonstrate how to identify, seize and transport electronic evidence.

Basic First Response: search and seizure, what to take (laptop cables), health and safety, keep suspect away from devices

e. Email

At the end of this lecture, participants will be able to summarize the operation of e-mail and effectively analyze the meta-data contained within e-mail headers, for the purposes of tracing their origin. This lecture will also discuss the issues regarding traceability and anonymity.

f. Online Groups, Social Networking and User Generated Content

This lecture discusses the operation of news groups and how illicit material can be distributed via this technology. Other topics include an introduction to social networking sites and the issues around privacy and harassment, and the reliability of user generated content.

g. Introduction to IT Forensics

This lecture serves as a basic introduction to the processes of forensic computing. Topics include the purposes of analyzing images of storage devices, chain of custody concerns and the hashing algorithms used to verify the integrity of evidence.

When to pull the plug, do not turn on powered-down system, suspect applications, ACPO guidelines [10], image acquisition, searching archives, Windows registry, cell phones, file structures, deleted files, solid state drives

h. Forensic Analysis with developed tools

Identification of user activities, previously connected devices, how to identify indicative images (child models), image categorization, search terms, Internet history, how to sort media by case relevance (triage), using the developed manual

i. Interviewing Techniques

Techniques and tactics, get suspect to describe content and divulge investigation-relevant information

j. Awareness

Victim identification, health and safety (traps/bombs), hidden or disguised devices, identification of risk to life; wrongfully accused; risk of committing an offense, assess suspects level of knowledge

k. Practical Experience

Two days of practical labs will take place that will involve the collection, triage, and preliminary analysis of suspect media.

l. Internship

It was also identified that as part of the primary training, the candidate should undertake an internship between one week and one month with the experts at a main investigation unit. One major point of the internship should be the exposure to child exploitation material (CEM) and how experts decide what is and is not CEM. This will allow the preliminary analyst to better understand and categorize suspect images.

m. Updating documentation, knowledge and software

An information portal would allow triage personnel and expert investigators to collaborate and update documentation, such as the triage field manual. If this portal will be created, its usage and updating process will be included in the training.

Level two 'Advanced Triage Training'will be one week, and will include:

a. Live Data Forensics

A two-part introduction into the principles of Live Data Forensics data collection and analysis

b. PABX, Online Chat and VoIP

This lecture discusses communications technologies such as MSN messenger and Skype. It also introduces participants to the concept of PABX fraud, how to protect against it, and what to do if it occurs.

c. Online Groups, Social Networking and User Generated Content

This lecture discusses the operation of news groups and how illicit material can be distributed via this technology. Other topics include an introduction to social networking sites and the issues around privacy and harassment, and the reliability of user generated content.

d. Investigative Resources

This two part lecture will provide participants with the necessary skills to locate and extract information from the Internet, resolve IP addresses and domain names, perform basic live forensics on computer systems, and examine web server logs. Also discussed will be the issues regarding traceability and anonymity.

V. CONCLUSIONS

As digital forensic investigation laboratories advance, their investigation process models also need to be streamlined. Currently investigation processes are the focus, but first responder and preliminary analyst training is also necessary. As investigations dealing with digital evidence increase, so to does the need for skilled first responders and improved investigation process models. In this work we described the 'ideal' digital investigation first responder and preliminary analyst, hardware and software requirements and most importantly, required training. Once a candidate meets the minimum requirements, they will require hardware, software and training to be a productive member of the CFTU. The required hardware and software has been given in section 3, and a listing of the proposed courses for first and second tier training has been given in section 4.

References

[1] E. Casey, M. Ferraro, and L. Nguyen, "Investigation Delayed Is Justice Denied: Proposals for Expediting Forensic Examinations of Digital Evidence*," J. Forensic Sci., vol. 54, no. 6, pp. 1353 - 1364, Nov. 2009.

[2] J. I. James and P. Gladyshev, "A survey of digital forensic investigator decision processes and measurement of decisions based on enhanced preview," Digit. Investig., vol. 10, no. 2, pp. 148 - 157, Sep. 2013.

[3] G. Palmer, "A Road Map for Digital Forensic Research," Utica, New York, Nov. 2001.

[4] M. B. Koopmans and J. I. James, "Automated network triage," Digit. Investig., vol. 10, no. 2, pp. 129 - 137, Sep. 2013.

[5] A. Shaw and A. Browne, "A practical and robust approach to coping with large volumes of data submitted for digital forensic examination," Digit. Investig., vol. 10, no. 2, pp. 116 - 128, Sep. 2013.

[6] A. Shaw and A. Browne, "A practical and robust approach to coping with large volumes of data submitted for digital forensic examination," Digit.

Investig., vol. 10, no. 2, pp. 116 - 128, Sep. 2013.

[7] N. Jones, "Training and accreditation - who are the experts?," Digit. Investig., vol. 1, no. 3, pp. 189 - 194, Sep. 2004.

[8] R. Jones, "Your day in court - the rôle of the expert witness," Digit. Investig., vol. 1, no. 4, pp. 273 - 278, Dec. 2004.

[9] J. I. James and Y. Jang, "Practical and Legal Challenges of Cloud Investigations," The Journal of the Institute of Webcasting, Internet and Telecommunication, vol. 14, no. 6, pp. 33 - 39, Dec. 2014.

[10] ACPO E-Crime Working Group, "Good Practice Guide for Computer-Based Electronic Evidence," 7safe Inf. Secur. website,[URL] http//7safe. com/electronic_evidence/index. html, 1996.

저자 소개

Joshua Issac James(정회원)

- 2013년 9월 : University College Dublin, Dublin, Ireland. PhD Computer Science by research in Digital Forensic Investigation
- 2016년 ~ : 한림대학교 국제학부 조교수
- joshua@CybercrimeTech.com

<주관심분야 : 디지털 포렌식, IoT 보안, 빅데이터 분석>

장 윤 식(정회원)

- 2014년 8월 : 고려대 정보경영공학전문대학원 졸업 (공학박사)
- 2015년 ~ : 한림대학교 국제학부 조교수
- 2005년 2월 ~ 2014년 2월 : 경찰대학 경찰학과 교수
- jakejang@hallym.ac.kr

<주관심분야 : 사이버범죄, 디지털 포렌식, IoT 보안, 범죄분석>

※ This research was supported by Hallym University Research Fund, 2015(HRF-201503-005).