No. 11

ROCB AP

Good Practice Report

Computer Forensics

Hong Kong Customs

Malaysia Customs

Table of contents

Foreword

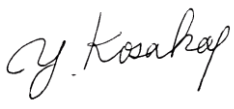
With the advancement of information technology, technology related crimes have also increased sharply in recent years. To gear up the Customs Administrations against the challenge of technology crimes, Hong Kong Customs conducted a regional survey to identify the capacity building needs of the Asia Pacific (A/P) Members on computer forensics in February 2013. The survey revealed that there were capacity building needs for law enforcement agencies on the knowledge and skills in handling technology crime including basic concepts of computer forensics, digital data analysis, application of forensics tools, digital evidence collection, digital evidence preservation and adducing digital evidence in court.

Targeting on these areas, ROCB A/P together with the WCO and Hong Kong Customs jointly organized the WCO A/P Regional Workshop on Computer Forensics in Hong Kong in August 2013 under the sponsorship of CCF/Japan.

Subsequent to the above-mentioned successful workshop, ROCB A/P has consolidated two Good Practice Reports on Computer Forensics for sharing with members in the Asia Pacific region and related parties on this emerging issue.

We do believe that these Good Practice Reports will provide some more guidelines for setting up the Computer Forensics Office and the Computer Forensics Laboratory and will gear up the Customs Administrations against the challenge of technology crimes. It will also strengthen the capability of law enforcement agencies in handling technology crime.

Finally, we would like to give special thanks to Hong Kong Customs and Malaysia Customs for their contributions.



Yoshihiro KOSAKA
Head of WCO Asia Pacific Regional Office for Capacity Building

Good Practice Report

Computer Forensics

By Hong Kong Customs

Content

1 Background

Digital crimes bring serious challenges to law enforcement agencies both in terms of investigation and prosecution of these offences. Unlike crimes committed in the physical world, illegal activities in the cyber world require only a modest computer, a data line and an Internet account. That means almost anyone so inclined can become a cyber criminal without any significant investment of resources. What is more, the digital crime does not work in the open and is often a difficult target for criminal investigation. Besides, distribution at the speed of light makes our investigation process becomes more difficult.

Notwithstanding the many difficulties, we should take proactive measures to deal with the technological challenges. To help members of the ROCB address such challenges and enhance the enforcement effectiveness, a sound foundation of computer forensics must first be in place. With this spirit in mind, Hong Kong Customs has produced this report.

The purpose of this document is to describe the best practices for computer forensics. It is believed that the report would embrace rich, valuable and updated information on how to conduct computer forensics examination and investigation. Nonetheless, this report is not all inclusive and does not contain information relative to specific operating systems or forensics tools.

While referring to this report, please keep in mind it is only for Customs officer's reference. There may be difference in computer forensic practices and standards arising from different jurisdictions. Member should consult with an appropriate specialist if there is any technological issue outside your area of expertise.

2 Establishing Formal Structures

Today's society is in the midst of a technological revolution. With advances in computer technology and telecommunications, connectivity between people escalated, publications and entertainment transformed into digitized format and publicized on-line, commercial activities became borderless and transacted electronically in the Internet. However, these technological achievements have provided avenues that facilitate savvy criminals in the commission of computer-related crimes. Nowadays, many traditional crimes such as narcotics trafficking, money laundering, smuggling, criminal damage, theft, intellectual property right violation, pornographic publication, financial fraud, etc. could be mirrored in the cyber space.

Not surprisingly, the proliferation of these forms of crime has stormed the enforcement world. The challenges bring by these crime fluxes are not only limit in the scope of severity and financial damage but also in ways of investigative skills and presentation of digital evidence in criminal trials. Echoing the problem, Customs agencies should respond proactively by placing resources to setting up the Computer Forensic Laboratory (CFL), the Computer Analysis and Response Team (CART), the Anti-Internet Piracy Team (AIPT) (also known as Cyber Crime Investigation Team), and the Research & Development Team (R&D Team).

For quality assurance and effective operation of respective setups, officers being recruited must be well trained and experienced in cyber technology and investigation. Besides, apart from observing the laid down procedure and guidelines of one Customs agency, all officers involved in digital forensic related work should follow the following four forensic principles when dealing with digital evidence in the course of their investigation and examination:-

- Actions taken to secure and collect digital evidence should not affect the integrity of that evidence.

- Persons conducting an examination of digital evidence should be trained for that purpose.

- Activity relating to the seizure, examination, storage, or transfer of digital evidence should be documented, preserved, and available for review.

- The examiner should be cognizant of the need to conduct an accurate and impartial examination of the digital evidence.

2.1 Computer Forensic Laboratory

The prime functions of the Computer Forensic Laboratory (CFL) are to provide quality computer forensic services to frontline staff and to escalate officers' capability in the handling of computer equipment and digital information at the scene of crime through seminars and training. To assure integrity, accuracy and court admissibility, officers of the CFL have to closely observe the standards and best practices in the performance of computer forensic examinations or analysis and to revise procedural and quality manuals when required. On the technical front, CFL officers have to keep abreast to the latest technology, exploring and evaluating new forensic software and hardware in order to defeat "hi-tech" crimes. Furthermore, they have to constantly liaise with local and overseas law enforcement agencies to enhance knowledge and to share experience in cyber crime investigation and computer forensic.

2.2 Computer Analysis and Response Team

The establishment of the Computer Analysis and Response Team (CART) aims to render frontline officers technical support and computer investigation at the scene of crime. Since digital data may be volatile, field officers could summon CART members to the scene of crime to provide technical assistance in the retrieval and preservation of possible digital evidence on-spot. In other words, the CART can be considered as the first responder of digital crime scene.

Given the diversity of computer technology and the fast pace of its development, the CART should be developed into several groups with each specializes in particular fields of expertise. As such, flexibility and mobility can be achieved and this in turn can strengthen support to field officers in resolving technological hurdles during enforcement actions.

2.3 Anti-Internet Piracy Team (also known as Cyber Crime Investigation Team)

In parallel with the development of expertise on computer forensics examination, a team of professionals should be established whose primary role is to delve proactively into the cyber world to deter Internet piracy. This Anti-Internet Piracy Team (AIPT) is a dedicated unit with members selected amongst the most experienced investigators in the field of cyber investigation. One Customs agency may establish several AIPTs with each specializes in particular fields of expertise to tackle different digital crimes effectively.

In order to discharge the covert investigation on the Internet effectively, members of the AIPT should be familiar with the internal functions and the networking framework of the Internet based on the Open System Interconnection (OSI) model.

Host Layers	Application layer (7)	Network process for computer programmes
	Presentation layer (6)	Data presentation
	Session layer (5)	Session and connection coordination
	Transport layer (4)	End-to-end connections and flow control
Media Layers	Network layer (3)	Path and logical addressing
	Data-link layer (2)	Physical addressing
	Physical layer (1)	Electrical and physical aspects for data transmission

AIPT should be equipped with the latest investigative tools and Internet access facilities with a view to detecting complicated Internet cases in the ever-changing digital world. To acquire skills on cyber crime investigation as well as gaining technical know-how in the area of computer forensics, AIPT members should also receive regular training courses at both local and overseas professional institutions.

2.4 Research and Development Team

Recognizing the growing use of the latest technologies to commit Customs related offences, a Research and Development (R&D) Team should be established to face such challenges and to step up the strike on illegal activities

on the Internet.

The R&D Team should comprise competent officers with strong background and experience on computer science as well as frontline investigation. Unlike the other formal establishments, the mission of the R&D Team is to strengthen the research on how criminals are using the latest technologies to commit offence. After understanding the modus operandi of the criminals, the R&D Team will develop enforcement strategies and formulate relevant guidelines to enable the frontline officers to identify, collect and preserve digital evidence at the crime scene. The R&D Team should also deliver specialized training to frontline officers. By simulating how criminals committing cyber crimes, frontline officers can learn the techniques and skills in collecting and preserving digital evidence during the investigation process. Besides, the R&D Team should develop IT monitoring systems to strengthen the capacities to monitor the Internet with a view to detecting cyber crimes.

Three basic functions of the R&D Team are:-

- Research and Development – Through the research work of the R&D Team, frontline officers can stay in pace with the development of technology and be able to formulate suitable operational strategies to tackle cyber crimes using the latest technology.

- System Development – With the increase in number and types of Internet platforms, it is impracticable to spot cyber crimes by manual means. The R&D Team should develop Internet monitoring and investigation systems to enhance the efficiency of Internet investigation.

- Capacity Training – Based on the research findings, the R&D members will formulate procedures and guidelines to standardize the methodologies on cyber investigation and evidence collection. Besides, the R&D Team will deliver training programmes on cyber investigation and handling of digital evidence to the frontline officers through simulation of how cyber crimes are committed.

3 Hardware and Software for the Computer Forensic Laboratory

3.1 Forensic Analysis Workstation

Digital forensics is a time-sensitive enterprise and consists of a number of computer-resource intensive tasks which are governed by the finite nature of the machines they run on. Digital forensic processes such as keyword and file indexing always push the hardware to its finite physical limits. Therefore, it is critical for the laboratory manager to select the fastest available systems for forensic examinations and to review their performance on a timely basis. The recommended specifications for a forensic workstation are listed below:-

- Motherboard --- This should be a vendor-approved list item. It should have a suitable number of peripheral slots available and support high-speed USB/FireWire connections.

- Central Processing Unit (CPU) --- The system should be installed with several 64-bit processors.

- Random-Access Memory (RAM) --- The memory should be certified to the motherboard. Maximum possible size of RAM with the fastest speed should be installed for the operating system.

3.2 Forensic Software

For most computer forensic professionals, the choice of whether to use open source and free tools or commercial tools comes down to budget. Open source software is free but does require a significant amount of testing and verification to ensure the results obtained using it can be replicated with other tools. Besides, open source tool has no vendor support and bug fixing guarantee. Regardless of whether the forensic tool is open source or commercial, the software used on examination must be tested to make sure that it performs as specified. Examples of commercial and open source forensic tools are listed below:-

	Commercial Tool	Open Source Tool
Hard Disk Analysis Software	● Forensic Toolkit (FTK) ● EnCase ● X-Ways	● SANS Investigative Forensics Toolkit (SIFT) ● WinHex
Mobile Phone Analysis Software	● XRY ● CelleBrite ● Aceso ● Oxygen Forensic Suite ● Paraben Device Seizure	● TULP2G (for SIM card examination only)
Virtualization Software	● VMWare ● Virtual PC	● Xen ● Qemu

4 Recruitment and Training of Staff for Computer Forensic Laboratory

One Customs agency should always actively recruit innovative, dynamic, and cutting edge professionals to join the computer forensics teams. Besides, adequate training should also be given to staff involving in the computer forensics in order to keep their momentum as well as to escalate their professional skills and knowledge.

4.1 Recruitment

(i) Qualifications and Experience

- Such as a degree or equivalent years of experience in related field
- Enforcement experience is preferable

(ii) Assessment

- To ensure an individual competence on process and or equipment they use during the forensics process

(iii) Proficiency Test

- Adopt as an integral part of an effective quality assurance program on computer forensics
- To monitor performance and to identify areas where improvements may be needed

4.2 Staff Training

Ordinary computer systems involve technologies incorporating electrical engineering, electronic engineering, mechanical engineering, computer science, mathematics and physics. On the other hand, computer forensics is multi-disciplinary by nature because of its foundation in two different fields – computing and law. In additional, several other fields are also involved, mostly related to criminology, information technology science, computer

engineering, and telecommunication. Nevertheless, the most significant part of computer forensic analysis is to have competent staff equipped with appropriate expertise.

Given that there are a variety of specific demands on computer forensic examiner, there is no surprise that it would be very difficult for a person trained solely in the field of information technology to understand the gist of forensic computing procedures without first being made aware of the relevant legislative requirements. On the other hand, it is very difficult for a person trained in legal matters to fully understand many of the technology tools and procedures without first being made aware of the relevant technology knowledge. It is obvious that the staff working in computer forensic laboratory should have specialized trainings in forensic computing analysis.

In respect of specialized trainings, the CFL should adopt a three-pronged approach in which three different streams of trainings are targeted. They are:-

- practical and hands-on trainings offered by law enforcement organizations;

- academic courses delivered by academic institutions;

- tailor-made trainings offered by non-profit making organizations, vendors, and consultants.

Strictly speaking, there is no recognized standard or extent of training to ensure that the forensic examiner is qualified in the handling and analyzing of digital evidence. Nevertheless, it has been highlighted in the Laboratory Management Manual of the International Organization on Computer Evidence (IOCE) that training needs should be linked to individual examiner certification. As listed in the foregoing paragraphs, computer forensic examiners can, through training, acquire mastering skills in technology and law. These trainings not only maintain capabilities of examiners in handling and analyzing digital evidence, but also ensuring sufficient pools of forensic expertise.

Although training is essential and vital to ensure competency of computer forensic examiners, this does not imply that every examiner requires the same level of training. For instance, an examiner may have attained professional training on Cisco router, whilst another examiner may have obtained in-depth

training on forensic examination on database systems (Oracle, SQL, etc.). Given that computer forensic analysis is highly technological, it is not possible to train law enforcement officers who do not possess in-depth computer knowledge to grasp sophisticated skills in computer forensic within months. Therefore, the CFL should only select those officers who hold academic or professional qualifications in computer-related fields as potential computer forensic examiners.

5 Accreditation for Computer Forensic Laboratory

Computer forensic examiners are adept with the technical knowledge of forensics and have the skills as an investigator. They are required to present the forensic findings in a logical and structured manner. Sometimes, they are even required to provide a coherent explanation under interrogation to a judge and jury with minimal use of the arcane jargon of the computer industry. In order to enhance the recognition of the computer forensic laboratory and examiner by the legal and law enforcement communities, accreditation from world recognized professional bodies have to be sought. There are a number of accreditations and certifications focusing on the standards of computer forensic laboratory. Some of them are listed below:-

- The ASCLD (The American Society of Crime Laboratory Directors) Forensic Laboratory Certification and Accreditation Program --- This program has been used by various law enforcement organizations, crime laboratories, and forensic laboratories. ASCLD has recently announced to implement a digital forensic program.

- The ISO (International Organization for Standardization) 9001 Quality Management System --- The design and implementation of quality management within an organization.

- The ISO 27001 Information Security Management System --- This standard provides guidance for information security management for use by those who are responsible for preservation of confidentiality, integrity and availability of information.

- The ISO 17025 General Requirements for the Competence of Testing and Calibration Laboratory --- The two main sections in ISO 17025 are the management requirements and technical requirements. Management requirements are primarily related to the operation and effectiveness of the quality management system within the laboratory. Technical requirements include factors which determine the correctness and reliability of the tests and calibrations performed in laboratory.

Without accreditation of the operating procedures and standards, there is no way to establish the integrity, accuracy and competency of the relevant forensic

findings produced by the laboratory. As a result of these shortages, there is a possibility that examiner may interpret the digital findings incorrectly and introduce sufficient doubts for the judges. Therefore, there is a looming view that the lack of standard of practice and training in a computer forensic laboratory may allow weakness to persist. This in turn may result in incomplete digital evidence collection, documentation and preservation as well as errors in analysis and interpretation of digital evidence. As a matter of facts, these failures will undermine investigations and prevent the apprehension or prosecution of offenders. As more cases become reliant on digital evidence for successful prosecutions, the CFL must take steps to strengthen the standards of practice and maintain the quality of such standards.

6 The Way Forward

Entering the 21st Century, Customs administrations are facing with immense challenges derived from the fast changing technology in computer facilitated crimes. To ensure that all Customs administrations are prepared to tackle cyber crimes efficiently and effectively, we should begin with the cultivation of technical experts in our own organization. We fully recognize that Customs officers were not born with knowledge of computers and investigating digital crimes requires not only experienced criminal investigators, but also investigators who possess special technical skills. Even though investigation into the criminal mind is technology neutral, enforcement officers must be properly equipped with the latest investigative tools to face the challenges of digital crimes.

Apart from expert cultivation on local territory level, we would expect more expertise sharing on computer forensics between different Customs administrations. A kind of computer forensic special interest group could be formed in order to arrange more seminars, trainings and workshops for all members to build up their skills and to keep the members posted of the new trends in digital crime.

Last but not least, computer forensics examiners should follow forensically sound investigative standards. It is however due to the difference in legal systems, Customs administrations may adopt different standards for putting up evidence to court after forensics examination. To enhance effective cooperation and expertise sharing, all Customs administrations could develop same basic standards and guiding principles on computer forensics examination and investigation. It would not only help to improve the standard of acceptability that applied to our computer forensics laboratories but also escalate our enforcement effectiveness for prosecuting the digital crimes.

REFERENCES:

(1) Information Security & Forensics Society (Hong Kong). An Introduction to Computer Forensics. Available at: http://www.isfs.org.hk

(2) Information Security & Forensics Society (Hong Kong). Best Practices on Computer Forensics. Available at: http://www.isfs.org.hk

(3) National Institute of Justice, US Department of Justice. Forensic Examination of Digital Evidence: A Guide for Law Enforcement. Available at: http://www.ojp.usdoj.gov/nij

Good Practice Report

Computer Forensics

By Malaysia Customs

Content

1 Background

The Royal Malaysian Customs (RMC) is responsible for the collection of revenue; business and trade facilitation; and deterrence of smuggling or fraud activities.

In 2007, RMC has implemented a Strategic Action Plan which includes the establishment of the Computer Forensic Unit under the Enforcement Division. Therefore, Computer Forensics Unit was set up in the same year.

By 2010, through the department restructuring, Computer Forensic Unit is being renamed as "Forensics Science Unit" which is answerable directly to the Director of the Investigation Branch to assist investigation. The unit serves more as a support team to the Investigation Officer.

2 Legislative Framework

The main legal frameworks for computer forensic are contained in Customs Act 1967 and Evidence Act 1950. In addition to the principal legislation, the department has also provides its own guideline which is called the "Enforcement Order: Procedures to seize electronic evidence".

LEGISLATION	***PROVISION***
CUSTOMS ACT 1967	**Access to recorded information or computerized data** *111B. (1) Any officer of customs exercising his powers under sections 106A, 107, 108, 109 and 111 shall be given access to any recorded information or computerized data, whether stored in a computer or otherwise.* *(2) In addition, an officer of customs exercising his powers under sections 106A, 107, 108, 109 and 111—*
CUSTOMS ACT 1967	*(a) may inspect and check the operation of any*

LEGISLATION	***PROVISION***
	computer and any associated apparatus or material which he has reasonable cause to suspect is or has been used in connection with that information or data; and *(b) may require—* *(i) the person by whom or on whose behalf the officer of customs has reasonable cause to suspect the computer is or has been so used; or* *(ii) the person having charge of, or is otherwise concerned with, the operation of the computer, apparatus or material, to provide him with such reasonable assistances he may require for the purposes of this section.* *(3) For the purposes of subsection (1), "access" includes being provided with the necessary password, encryption code, decryption code, software or hardware and any other means required to enable comprehension of recorded information or computerized data.*
EVIDENCE ACT 1950 EVIDENCE ACT 1950	**Interpretation** *3. In this Act, unless the context otherwise requires—* *"computer" means any device for recording, storing, processing, retrieving or producing any information or other matter, or for performing any one or more of those functions, by whatever name or description such device is called; and where two or more computers carry out any one*

LEGISLATION	***PROVISION***
	or more of those functions in combination or in succession or otherwise howsoever conjointly, they shall be treated as a single computer;
Enforcement Order: Procedures to seize electronic evidence	This order provides a guideline to raiding team on the procedure of seizure and handling of electronic evidence. It contains a set of steps that should be performed each time a computer is collected and/or examined. These procedures are needed to ensure that evidence is collected, preserved, and analyzed in a consistent and thorough manner.

3 Establishing Formal Structures

3.1 Computer Forensic Laboratory

All acquisition and analysis process is being carried out in a secured analysis room. The safety of the electronic evidence is confirmed through our internal control by preserving the chain of custody of the evidence. The access to the said secure room is strictly confined to our analyst and investigation officer.

Currently, Computer Forensic Laboratory is unavailable in the Department. However, the plan to build Certified Computer Forensic Laboratory has been proposed.

3.2 Computer Analysis and Response Team

The Unit is currently consist of a Response Team and four (4) senior officer as forensic analyst. The Response Team is then divided into two (2) small teams i.e. the MOBILE and COMPUTER Forensic team.

Currently, the former handled mostly cases related to narcotics investigation while the latter is confined in finding electronic documents.

The Response Team is to join any raiding activity to seize identified electronic devices. They are responsible to label, acquire and preserve the electronic evidence. After the acquisition process is done, the image files will be sent to our analyst for data analysis.

3.2.1 Anti-Internet Piracy Team

The team has yet been established. Further study need to be conducted to identify the necessary establishment.

3.2.2 Research and Development Team

The team has yet been established. Further study need to be conducted to identify the necessary establishment.

4 Forensic Tools and Equipment

Forensic tools and solutions are the most important element in carrying out forensic activity effectively and efficiently. The tools and equipment currently being used by our unit are as follows:

4.1 VOOM Hardcopy II and TABLEAU Forensic Duplicator TD1

This tool has been used as portable forensic duplicator to make an image of any electronic evidence in the field and in lab. It has the capabilities to acquire SATA and IDE hard disk drive with hash utilities in MD5.

4.2 EnCase

In analysis process, EnCase is used for capturing, analyzing and reporting on digital evidence. It has filters that enable analysts to find evidence based on forensic image of electronic devices.

Analysts can recover digital evidence residing in deleted files, reformatted disks, swap and slack space, hidden files, print spools and more. In addition, EnCase helps analysts to review data that other tools cannot access, including system files and encrypted data.

4.3 XRY

This tool is used to extract data from mobile devices including the SIM card and memory card. No change is made to the data on the mobile device, nor is the device physically altered in any way. The data retrieved are not analyzed in any way but merely passed on to the intended user.

The details contained in mobile phones are retrieved in and stored in an XRY format. This data may be exported to a semicolon separated text format.

After the data is read by XRY, none of the data can be edited or modified. The data become documentary evidence for judicial, legal and investigative purposes.

5 Recruitment and Staff Training

Annually, RMC Academy provides Basic Concepts of Computer Forensics course to the officer. The objective of the course is to expose the participants to Computer and Mobile Forensics. The course is conducted by experts from RMC, Royal Malaysian Police and Cyber Security Organization.

6 Challenges / Lessons Learned

6.1 Lack of knowledge:

The main challenge is to identify the tools and equipment as well as methods of acquisition to expedite forensic analysis. The evolution of hardware and software engineering has make the acquisition and analysis process extra complex to detect significant evidence.

For example, the data of accounting systems could not be presented in the original format. As a result, the raiding team has to print the document from the system before any forensic activity is being carried out.

Therefore, researches on technologies related to data encryption, data hiding and recovering the evidence is essential.

6.2 Costs of forensic solution and training:

Undoubtedly, the charges for the forensic solution and training available in the market are very high. For that reason, our unit currently subscribes only VOOM, TABLEAU, EnCase and XRY in carrying out our duty.

7 Ways Forward

There are still rooms for improvement in the computer forensic application. Proposal has been made to build a Certified Forensics Lab and the budget is always the major concern. However, we believe that the project is worth in improving our forensic capabilities in future.

We also believe that Accounting Forensics will play a major role in forensic application in the future. Therefore, accounting experts are extremely desirable to analyze and interpret the accounting evidence accurately.