CONTINUUM
SECURITY SOLUTIONS℠

Best Practices

for Incident Responders Collecting Electronic Evidence

rev. April 2013

Prepared by:

Rick Clyde
Forensic Examiner
rick.clyde@cwc**security**.com
M: (402) 709-6064

Chris Hoke
Principal and Owner
chris.hoke@ cwc**security**.com
M: (402) 650-4304

DISCLAIMER

These are general guidelines. All incidents will have specific issues or concerns which may alter the circumstances under which these steps are implemented to collect and preserve evidence. Continuum Worldwide Corporation cannot be held responsible for any damage or liability of any kind resulting from following any of these general guidelines. Should you implement any of these steps or general guidelines, you do so at your own risk.

TABLE OF CONTENTS

Purpose 3

Recognizing Potential Evidence 3

Preparing for Collection and Preservation 4

Chain of Custody 4

Collection and Preservation of Electronic Evidence 5

- Computers (Desktop & Laptop) 5
- Network Servers 6
- Cell Phones 7
- Digital Cameras/Audio/Video 8
- Storage Media 8
- Other Potential Sources of Electronic Data 9
- General Rules 9

Victim Response and Reporting an Intrusion/Information Security Breach 10

Sample Referral "Incident Response" Form 11

Things to Remember 12

References and Sources 12

PURPOSE

This publication was developed to provide first responders with a basic understanding of key technical factors regarding the collection and preservation of electronic evidence and storage media.

Often times, the first responder may be the system or network administrator, a senior information technology (IT) staff person, or a member of the incident response team. It is important that organizations recognize, protect, collect, and preserve electronic evidence in accordance with best practices and guidelines to reduce the likelihood of errors and claims of spoliation. Rash or hurried actions could damage or destroy potential evidence.

RECOGNIZING POTENTIAL EVIDENCE

There are many items that contain electronically stored information (ESI). These items include, but are not limited to:

- Computers (e.g., mainframe, servers, desktops, laptops)
- User access times
- Computer created files (e.g., applications, backup, configuration, data, dump, hibernation, hidden, history, log, printer spool, swap, system, temporary)
- Slack space
- Unallocated space
- Phones (e.g., cell, smart, VOIP, wireless home phone)
- PDAs
- Storage media (e.g., USB device – thumb drive, CDs, DVDs, memory cards)
- Digital cameras
- Video cameras
- MP3 players (e.g., iPod)
- Electronic gaming devices (e.g., Wii, PlayStation, X-Box)
- Paging devices
- Facsimile machines
- Caller ID devices
- Smart cards

PREPARING FOR COLLECTION AND PRESERVATION

Using evidence obtained from a computer, cell phone or storage media in a civil proceeding requires:

- Consent from the owner of the property
- Appropriate collection techniques to avoid altering or destroying evidence
- Documenting a proper chain of custody
- Forensic examination of the electronic data completed by trained personnel in a timely manner
- Expert or percipient witness testimony available at deposition or trial

The Electronic Crime Scene Investigation – A Guide for First Responders, produced by the U.S. Department of Justice, offers the following suggestions when approaching a digital crime scene:

- Securing and Evaluating the Scene – Steps should be taken to ensure the safety of individuals, and to identify and protect the integrity of potential evidence.
- Documenting the Scene – Create a permanent record of the scene, accurately recording both digital and conventional evidence.
- Evidence Collection – Collect traditional and digital evidence in a manner that preserves evidentiary value.
- Packaging, Transportation, and Storage – Take adequate precautions when packaging, transporting, and storing evidence, maintaining a chain of custody every step of the way.

CHAIN OF CUSTODY

Chain of custody refers to a written account of individuals who had sole physical custody of a piece of evidence from the time it was collected until final disposition. This includes:

- What it is
- Who or where it was taken from
- How it was collected
- Reason for transfer of possession
- Who is taking possession and why
- How it was stored
- How it was protected in storage
- Who took it out of storage
- Why it was taken out of storage
- When, where, and how it was destroyed. (if requested)

Evidence should be collected in a manner that is suitable for admissibility in a court of law. It may not be obvious when an investigation is initiated that court action may subsequently follow. For example, when a computer security incident is first detected, the first instinct might be to solve the problem and not take evidence collection into consideration. In doing so, important evidence might be overlooked, improperly handled, or accidentally destroyed before the seriousness of the incident is realized.

COLLECTION AND PRESERVATION OF ELECTRONIC EVIDENCE

Computers (Desktop & Laptop)

Secure the Scene

- The safety of individuals in the vicinity of the target device or data source, and that of the first responder is paramount.
- Preserve the area for conventional evidence collection (i.e., fingerprints, DNA) as well as electronic evidence.
- Immediately restrict access to computer(s) and attached peripherals (i.e., cables, power cords, printers, USB devices, etc.).
- Remember, there are many methods to access computers remotely.
- Time is very critical, since computer data can be altered and erased quickly.

Secure the Computer as Evidence

- If the computer is on, leave it on (unless it's running a destructive process).
- Slightly move the mouse to determine whether or not the computer's screensaver is running or the computer is in sleep mode. You can also look for any lit lights on the tower or base of the laptop.
- If the computer is on, photograph or take note of what is on the screen and what programs may be running.
- Turning it off could activate the lockout feature.
- Do not open any programs on the computer in question.
- Do not attempt to view data on the computer. Viewing files on a Windows machine can alter or destroy evidence.
- Power down prior to collecting evidence.
- Don't forget to acquire the power supply cord!
- If computer is off, leave it off. Turning it on could alter evidence in the computer.
- When you acquire the computer, deliver it to an expert as soon as possible and document all transports and exchanges in the chain of custody.
- Make every effort to gather any instruction manuals and power supply cords.
- Delays in conducting an examination may result in loss of information due to insufficient internal power supply.
- Take appropriate care in handling and storage (avoid cold, dampness, etc.).

Prepare Computer for Transportation

- Unplug the power cable from the back of the computer (not at the wall outlet) to ensure you unplug the proper cable and to prevent the computer from running on battery power versus the uninterrupted power supply.
- Laptops should be unplugged from the power source and the battery should be removed.
- Do not remove any CDs, DVDs, or floppy disks. USB devices can be removed after the power is off. Seize any removable media as well.
- Take photos and record the serial number of the computer and all devices connected to it.
- If the computer has a phone or network connection, identify the phone number, the serial number of the modem, and any identifying characteristic to link the computer to its network connection.

Prepare Computer for Transportation (Continued)

If you are not qualified to perform the following, consult a specialist for further assistance.

- Remove or open the computer's case.
- Remove power and data cables from hard drive(s). Write down which connector was attached to each drive so you can reconnect them when done.
- Remove each hard drive from the computer, unless you can easily see the drive's serial number and other identifiers.

The following list is an example of the types of electronic data that may be found on hard drives of computers and/or servers:

- Email/Instant Messages
- Pornography
- History of Internet sites visited
- Contracts
- Financial reports
- Spreadsheets
- Files created and deleted (metadata)

NOTE: This list is merely an example of some of the more commonly analyzed data.

Network Servers

Servers

If you are not qualified to perform the following, consult a specialist for further assistance.

Secure the scene and do not allow anyone to access the targeted equipment except persons trained to handle network systems.

Do not unplug any equipment, as it could:

- Severely damage the system
- Disrupt legitimate business operations
- Disrupt business partner operations that rely on your business continuity
- Create liability

Networks

The following is a sampling of information to gather when dealing with networks and servers:

- Describe the configuration.
- Attach a diagram of the configuration.
- Identify the Operating System (OS): Windows, Unix/Linux, MS DOS, etc.
- Identify any external devices.
- Identify how many servers are involved.
- Determine the role of each server in the system.
- Determine the type of the file systems: FAT/NTFS.
- Identify how many work stations are involved.
- Determine if any unauthorized software was found in a computer.
- Determine if any unauthorized hardware was connected.

Cell Phones

Before handling a cell phone, consider what other types of evidence, such as DNA or fingerprints, are needed from the phone and follow the appropriate handling procedures.

On/Off Rules:

- Switching the phone off is advisable, because of the potential for loss of data if either the battery expires or network activity occurs.
- If the phone remains on, it should be kept charged and not be tampered with. Always turn off a phone during transport.
- While the phone is on, make all efforts to remove the phone from the network; this includes putting it into airplane mode or wrapping it in several layers of aluminum foil.
- To prevent accidental operation in transit, the phone should be packaged so it's immobile.
- The phone should be placed into an evidence bag, sealed to restrict access, and the labeling procedures completed for the exhibit to maintain a proper chain of custody.

The following list is by no means exhaustive, but merely provided to be an illustration of some of the various types of electronic data that may be found on cell phones:

- Calls made (date, time, duration)
- Calls received (date, time, duration)
- Last dialed number (LDN)
- Contact list (personal phone book)
- Text messages
- Photographs
- Video clips
- Calendar
- Email
- Customized ring tones (a distinctive ring-tone may be remembered by a witness to place someone at a physical location)
- Location (establish physical location or direction of travel)

Another source of electronic evidence is the SIM card (subscriber identity module) of a phone attached to the GSM cellular network (global systems for mobile communications). The SIM card is simply a smart card containing a processor and non-volatile memory. In cell phones, the SIM card is used as a storage device for subscriber-related data. The types of electronic data one can find on a SIM card include without limitation:

- ***Location Area Identifier*** – This identifies where the cell phone is currently located. This value is retained by the SIM card when the phone is turnedoff. This is useful for determining in which location area the cell phone was last used when it was operating.
- ***Serial Number*** – This number can be retrieved without providing the PIN (personal identification number) and will therefore identify the SIM itself.
- ***Customer Number*** – This is referred to as the IMSI (international mobile subscriber identity) which is the customer identification number and will allow you, with the aid of the network provider, to identify the individual who owns the cell phone.
- ***Cell Phone Number*** – This is referred to as the MSISDN (mobile subscriber integrated services digital network).
- ***Text Messages*** – Normally, there is space on the SIM which is intented to store a small number of text messages that were recently sent. In addition, cell phones also store messages in memory. Most cell phones use the SIM memory first before using the internal memory.
- ***Deleted Messages*** – Similar to deleting a file on a typical hard drive, the first byte is set at zero. This means that deleted messages can be retrieved except for the first byte as long as a new message has not overwritten the old message

- ***Phonebook*** – Most cell phones have the ability to store a minimum of 100 numbers with an associated name.
- ***Last-Dialed Numbers*** – Most cards only store the last few phone numbers dialed on the SIM card. However, many phones store additional last-dialed numbers on internal memory.

Digital Cameras/Audio/Video

If the device is off, leave it off.

If the device is on, consult a specialist.

If a specialist is not available, secure recorded media (tape, memory card) and secure the device:

- Photograph device (screen/display), then disconnect all power sources; unplug from the back of the device. If unable to do so, acquire the device and consult with a specialist as soon as possible.
- Place tape over the areas of access (e.g., drive slots and media slots).
- Photograph/diagram and label the back of components with existing connections.
- Label all connector/cable ends to allow reassembly as needed.
- If transport is required, package components and transport/store components as fragile cargo.
- Delays in conducting the examination may result in loss of information due to an insufficient internal power supply.
- Take appropriate care in handling and storage (avoid cold, dampness).
- When available, all manuals should be collected with equipment.

Storage Media

Storage media is used to store data from an electronic device. Many devices have capabilities for both fixed (internal) storage/memory and the ability to also store data solely or simultaneously to removable storage media (external).

The following list is provided to illustrate various types of storage media:

- USB device (i.e., thumb drive)
- CD/DVD
- Floppy disk
- Flash memory card
- External hard drive
- Removable hard drive

Other Potential Sources of Electronic Data

- Electronic Paging Devices
- Facsimile (FAX) Machines
- Smart Cards & Magnetic Stripe Cards
- Electronic Gaming Devices (e.g., Wii, PlayStation, X-Box)
- Personal Digital Assistant/Hand Held Computers
- Global Positioning System

General Rules

If the device is off, leave it off.

If the device is on, consult a specialist.

If a specialist is not available:

- Photograph the device (screen/display), then disconnect all power sources; unplug from the back of the device. If unable to do so, acquire the device and consult with a specialist as soon as possible.
- Place tape over areas of access (e.g., drive and media slots).
- Photograph/diagram and label the back of components with existing connections.
- Label all connector/cable ends to allow reassembly as needed.
- If transport is required, package components and transport/store components as fragile cargo.
- Delays in conducting the examination may result in loss of information.

VICTIM RESPONSE AND REPORTING AN INTRUSION/INFORMATION SECURITY BREACH

The U.S. Department of Justice has outlined best practices for victim response and reporting regarding an intrusion or information security breach. These recommendations are found in "Prosecuting Computer Crimes," see Appendix C of Best Practices for Victim Response and Reporting, a publication of the Computer Crime and Intellectual Property Section (CCIPS) Criminal Division, U.S. Department of Justice, published by the Office of Legal Education, Executive Office of United States Attorneys.

The outline of the recommended best practices is set forth below. Appendix C can be reviewed in its entirety at http://www.usdoj.gov/criminal/cybercrime/ccmanual/index.html.

1. Steps before confronting an intrusion:
   - Be familiar with procedures, practices, and contacts.
   - Consider using banners.
2. Responding to a computer incident:
   - Make an initial identification and assessment.
   - Take steps to minimize continuing damage.
   - Notify law enforcement.
   - Do not hack into or damage the source computer.
   - Record and collect key info including a mirror image, notes, records, and data.
   - Record and log continuing attacks.
   - Do not use the compromised system to communicate.
   - Notify people within the organization, the computer incident-reporting organization, and any potential victims.
3. After a computer incident:
   - Take steps to prevent similar attacks.
   - Conduct a post-incident review.

SAMPLE REFERRAL "INCIDENT RESPONSE" FORM

From client to law firm or from client/law firm to law enforcement:

CIO CYBERTHREAT REPORT FORM

This form outlines the basic information law enforcement needs on a first call. You can use it as an internal worksheet or fill it out and e-mail or fax it to law enforcement. Additional data that will help agents in their investigation is outlined in the CIO Cyberthreat Response & Reporting Guidelines, but the best way to determine what will be most helpful to investigators in the event of an attack is to ask.

STATUS

☐ Site Under Attack ☐ Past Incident ☐ Repeated Incidents, unresolved

CONTACT INFORMATION

Name_____Title_____

Organization_____

Direct-Dial Phone_____E-mail_____

Legal Contact Name_____Phone_____

Location/Site(s) Involved_____

Street Address_____

City_____State_____IP_____

Main Telephone_____Fax_____

ISP Contact Information_____

INCIDENT DESCRIPTION

☐ Denial of Service
☐ Distributed Denial of Service
☐ Malicious Code (virus, worm)
☐ Intrusion/Hack
☐ Other (specify)_____
☐ Unauthorized Electronic Monitoring (sniffers)
☐ Misuse of Systems (internal or external)
☐ Website Defacement
☐ Probe/Scan

DATE/TIME OF INCIDENT DISCOVERY

Date_____Time_____

Duration of Attack_____

IMPACT OF ATTACK

☐ Loss/Compromise of Data
☐ System Downtime
☐ Damage to Systems
☐ Financial Loss (estimated amount: >$_____)
☐ Damage to the Integrity or Delivery of Critical Goods, Services or Information
☐ Other Organizations' Systems Affected

SEVERITY OF ATTACK, INCLUDING FINANCIAL LOSS, INFRASTRUCTURE, PR IMPACT IF MADE PUBLIC

☐ High ☐ Medium ☐ Low ☐ Unknown

SENSITIVITY OF DATA

☐ High ☐ Medium ☐ Low ☐ Unknown

How did you detect this?_____

Have you contacted law enforcement about this incident before? Who & when?_____

Has the incident been resolved? Explain_____

Source: CIO Cyberthreat Response & Reporting Guidelines (http://www.cio.com/research/security/incident_response.pdf)

THINGS TO REMEMBER

- If the computer or device is turned off, leave it off.
- Do not try to access devices or data unless you are qualified to do so. If you have to act in an emergency situation, provide written and, if possible, photo documentation of what was done and why.
- Identify potential sources of evidence/electronic devices and/or storage media.
- Keep everyone away from the target computer, cell phone or storage media.
- Identify who owns/has control of the device or media.
- Determine whether or not consent has been provided to collect and preserve the computer, cell phone or storage device (if the device is not corporate property or if a privacy right exists).
- Determine whether or not there is remote access to the device.
- Determine whether or not there is off-site data storage.
- Preserve evidence (paper or non-static bags for hard drives, aluminum foil or non-static bags for cell phones).
- Gather all software, power cords/adapters, peripheral devices, etc. used to support or power the collected devices and/or media.
- Attain passwords, encryption keys, physical keys, and other security access control devices located at the scene or collected through interviews.
- Determine suspect, victim, or witness knowledge (e.g., system, hardware, software, Internet, email, chat rooms, person or located target, etc.).
- Determine suspect(s) level of access or control of areas and devices.

REFERENCES AND SOURCES

- Guidelines on Cell Phone Forensics, Recommendations of the National Institute of Standards and Technology (NIST), Special Publication 800-101, May 2007
  http://csrc.nist.gov/publications/nistpubs/800-101/SP800-101.pdf
- Electronic Crime Scene Investigation – A Guide for First Responders, a publication of the U.S. Department of Justice, the National Institute of Justice
  http://www.ncjrs.gov/pdffiles1/nij/187736.pdf
- Best Practices for Seizing Electronic Evidence, Version 2.0, a publication of the Department of Homeland Security, the United States Secret Service
  http://www.cio.com/securitytools/BPGv2.pdf
- Guide to Integrating Forensic Techniques into Incident Response, Recommendations of the National Institute of Standards and Technology (NIST), Special Publication 800-86
  http://csrc.nist.gov/publications/nistpubs/800-86/SP800-86.pdf
- Investigations Involving the Internet and Computer Networks, a publication of the U.S. Department of Justice, the National Institute of Justice
  http://www.ncjrs.gov/pdffiles1/nij/210798.pdf
- Prosecuting Computer Crimes, a publication of the Computer Crime and Intellectual Property Section (CCIPS) Criminal Division, U.S. Department of Justice, published by the Office of Legal Education, Executive Office of United States Attorneys
  http://www.usdoj.gov/criminal/cybercrime/ccmanual/index.html