CALIFORNIA STATE UNIVERSITY SAN MARCOS

THESIS SIGNATURE PAGE

THESIS SUBMITTED IN PARTIAL FULFILLMENT
OF THE REQUIREMENTS FOR THE DEGREE

MASTER OF SCIENCE

IN

CYBERSECURITY

THESIS TITLE: Training Material for the Regular Systems Administrator Facing a Breach

AUTHOR: Lorenia Misiaszek

DATE OF SUCCESSFUL DEFENSE: July 11, 2017

THE THESIS HAS BEEN ACCEPTED BY THE THESIS COMMITTEE IN
PARTIAL FULFILLMENT OF THE REQUIREMENTS FOR THE DEGREE OF MASTER OF SCIENCE IN
CYBERSECURITY.

Teresa Macklin THESIS COMMITTEE CHAIR	SIGNATURE	7-11-17 DATE
Darren Bennett THESIS COMMITTEE MEMBER	SIGNATURE	7/11/17 DATE
Yi Sun THESIS COMMITTEE MEMBER	SIGNATURE	7/14/17 7/14/17 DATE

Training Material for the Regular Systems Administrator Facing a Breach

July 2017

Lorenia Misiaszek

Faculty Advisors

Project Chair: Teresa Macklin, J.D.

Committee Member: Darren Bennett

Committee Member: Yi Sun, PhD

Professional Science Masters

California State University, San Marcos

Table of Contents

List of Figures and Tables

Executive Summary

Training Material for the Regular Systems Administrator Facing a Breach

Lorenia Misiaszek

June 16, 2017

Professional Science Masters

California State University, San Marcos

Although most of today's successful companies are well aware of common data security issues and put a great deal of efforts towards preventing a data security breach, once a breach has occurred it is not unusual for organizations to enter a mist of confusion and chaos. This happens to all sizes of organizations whether big or small. However, large organizations are perhaps better prepared in terms of available resources to respond to a data breach than small to medium-size organizations. Small organizations do not have IT departments. The regular Systems Administrator is a “jack of all trades” and wears multiple hats. He or she is typically in charge of a broad array of duties including installing and updating software and hardware, maintaining servers, and supporting and troubleshooting the company’s network. They are on call and may even have the responsibility of overseeing the overall computer security of the company. What should the regular Systems Administrator do if a breach happens and a forensic investigation is needed? The training material included in this paper (Appendix B) was created as a response to this question and as response to one of the four recommendations *the National Institute of Standards and Technology (NIST) Special Publication 800-86, Guide to Integrating Forensic Techniques into Incident Response* makes on its document: “Organizations should ensure that their IT professionals are prepared to participate in forensic activities.” What if they are not prepared? The training material offers some suggestions on how to initiate the first phase of the forensic process: *Collection*. The regular Systems Administrator can take on the tasks of *identification, labeling* and *recording* and then wait for the arrival of the trained digital forensic investigator who should finalize the forensic process.

Acknowledgment

To all those who *believed* in me and to all those who *didn't*: Thank You. You have taught me a great lesson. This work is a proof of faith, discipline and focused perseverance.

I also gratefully acknowledge the guidance and direction provided by Teresa Macklin and Darren Bennet.

With love to my family, good friends and colleagues.

1. Introduction

Although most of today's successful companies are well aware of common data security issues and put a great deal of efforts towards preventing a data security breach, once a breach has occurred it is not unusual for organizations to enter a mist of confusion and chaos. Some organizations react more rapidly and effectively than others in handling post-breach activities. These organizations are perhaps using the right budget, staff, processes and technology to quickly limit the damage.

When a security incident occurs, many organizations engage incident handlers who have been specially trained and prepared to respond to security incident reports. This is what probably happens at the enterprise level. After all, large organizations have plenty of available resources to respond to a data breach. They have bigger budgets to invest in a more structured IT department. What about the small organization?

Recent reports show that small organizations are not allocating any budget to improve the security of their company even though the statistics that show the impacts of a cyberattack are high and only going higher for small organizations. In a 2016 report from the insurance firm, Nationwide, 78% of small companies still didn’t have a cyberattack response plan, yet 54% were victims of cyberattacks. It is surprising that these organizations are still not investing much in computer security matters - not to mention in post-breach event training such as forensic training.

One of the four recommendations that *the National Institute of Standards and Technology (NIST) Special Publication 800-86, Guide to Integrating Forensic Techniques into Incident Response* makes on its document reads: “Organizations should ensure that their IT professionals are prepared to participate in forensic activities.” This is not happening as of 2017. In reality, the regular Systems Administrator in the small organization often:

- Does not have a clear idea of the roles and responsibilities for forensics
- Does not receive training and education on forensic-related policies and procedures
- Does not consult legal advisors in preparation for forensics activities to know which actions should and should not take

- More importantly, it's rare that Management supports forensic capabilities

1.1. Purpose and Scope

The training material is simple and offers some suggestions to the regular Systems Administrator facing a breach. It is not a definitive training guide nor is meant to provide legal advice. The training material covers the basic concepts, tools and activities of identifying, labeling and recording sources of data based on guidelines published by *the National Institute of Standards and Technology (NIST) Special Publication 800-86, Guide to Integrating Forensic Techniques into Incident Response*; *the National Institute of Justice. Electronic Crime Scene Investigation, A Guide for First Responders (first and second edition); and the National Institute of Justice. Electronic Crime Scene Investigation: An On-the-Scene Reference for First Responders.* The role of the regular Systems Administrator during a forensic investigation is limited to three of the four steps of the collection phase. The last step, acquisition of data, should be performed by a trained digital forensic investigator or law enforcement investigator.

1.1. Audience

The work described in this paper is intended for small organizations with less than 300 employees and limited tech resources or organizations that have repurposed their network, systems or IT personnel as Incident Responders (IR). To those small companies that are cognizant of their weaknesses and are calling for help, this paper provides training material for the regular Systems Administrator during the collection phase in the aftermath of a data breach.

1.2. Framework Resources

The training material is based on guidelines published by

- *The National Institute of Standards and Technology (NIST) Special Publication 800-86, Guide to Integrating Forensic Techniques into Incident Response*
- *The National Institute of Justice. Electronic Crime Scene Investigation, A Guide for First Responders (first and second edition)*

- *The National Institute of Justice. Electronic Crime Scene Investigation: An On-the-Scene Reference for First Responders*

2. Literature Review

2.1. Digital Forensic Investigation (DFI)

After an organization has suffered a serious information security or criminal incident and the incident has been contained, another crucial event might be triggered. This post-event response is what is known as Digital Forensic Investigation (DFI). Neal (2014) defined DFI as the "collection and analysis of data from an electronic device or other source using tools and procedures that protect the integrity of the collected data and the analysis."

The goal of digital forensic investigations is to try to answer basic questions such as "was sensitive information compromised?", "Did X malware wipe critical files?" or "were anti-forensic tools used?" Clarke, Tryfonas & Dodge (2012) mentioned in their book that the purpose of a forensic investigation is to find out which events occurred and the individual or individuals responsible for the incident or crime.

It's worth mentioning that the process of a digital forensic investigation has legal aspects and like any other legal process it can get complicated. According to Sommer (1998), digital forensic investigations face considerable scrutiny of both the integrity of the evidence, and the integrity of the investigation process. At the core of digital forensic investigations is digital evidence.

2.2. Digital Evidence

Digital or computer evidence is "information and data of value to an investigation that is stored on, received, or transmitted by an electronic device" (National Institute of Justice, 2008). As stated in the book *Computer Forensics Jumpstart* by Solomon, Rudolph, Tittel, Broom & Barett (2011), the main purpose of computer forensics is the proper identification and collection of computer evidence. Every forensic investigation has a hypothesis. This data may support or refute the hypothesis that was formulated during the investigation. In the article, *Digital Evidence and the U.S. Criminal Justice System. Identifying Technology and Other Needs to More*

Effectively Acquire and Utilize Digital Evidence, Goodison, Davis and Jackson (2015) defined digital evidence as “conceptually the same as any other evidence—it is information leveraged in an attempt to place people and events within time and space to establish causality for criminal incidents." In this article, the authors described that although digital evidence is a new tool for law enforcement investigations, this entity broadly depends on digital evidence for crucial information tied to both the victim and the suspect. The authors Solomon, Rudolph, Tittel, Broom & Barett (2005) wrote in the book previously mentioned that digital evidence is defined as any hardware, software or any data that can answer the questions "who, what, when, where, why and how" of a security incident.

Goodison, Davis and Jackson (2015) list the following three characteristics as essential to differentiate digital evidence from traditional physical records and evidence:

1. Digital evidence has a wider scope.
2. Digital evidence deals with both physically and personally sensitive information.
3. Digital evidence taps into interconnected criminal justice issues that go beyond law enforcement’s typical role in collecting evidence.

The Rules of Evidence

Digital evidence is evidence that can have a real impact on legal proceedings (Stone, 2015). In order to prove its case in a legal proceeding, an organization must follow what is known as The Rules of Evidence during evidence collection.

The SANS Institute outlines five rules for the successful collection of evidence:

1. Admissible
2. Authentic
3. Complete
4. Reliable
5. Believable

By admissible means that “the evidence can be legally and properly introduced in a civil or criminal trial” (Glossary of Court Terms). Authentic refers to the bond between evidence and incident - the evidence must be tied to the incident. Completeness implies that collected

evidence will not only prove the attacker's actions but also eliminates alternative suspects (SANS Institute). Reliable evidence does not present any doubts about its validity. Finally, the evidence must be believable meaning that it should be credible and clearly understandable to a jury.

2.3. Chain of Custody

Oppenheimer (n.d.) stated that chain of custody refers to "documentation that identifies all changes in the control, handling, possession, ownership, or custody of a piece of evidence." This "continuity of custody" is a process that involves a series of phases. Based on NIST SP 800-86, every person who has custody of the evidence must be logged, any actions taken by each person should be documented along with the time, evidence must be stored in a safe location when not in use, examination and analysis phases must be completed on a copy of the evidence and never on the original, and equally in importance is to take the necessary steps to validate the integrity of both the original and copy of evidence by computing the message digest before and after the bit stream imaging.

The Importance of the Chain of Custody

In the article *How to Document Your Chain of Custody and Why It's Important*, Coons (2015) described that the most important step in the collection phase is documentation. Being able to document and validate the findings are essential when a matter goes to trial. Because of its unique nature of easy manipulation, digital evidence must be first authenticated prior its acceptance in court. It is challenging to authenticate this type of evidence; the collector must demonstrate that the collection process is free of inconsistencies and alterations. The forensic investigator must establish and maintain a strong chain of custody.

For each item of evidence that is handled a chain of custody must be created. Appendix A shows an example of a chain of custody that the forensic investigator should bring. A typical chain of custody document may include the following list of items published by Coons (2015).

- Date and time of collection
- Location of collection
- Name of investigator(s)

- Name or owner of the media or computer
- Reason for collection
- Matter name or case number
- Type of media
- Serial number of media if available
- Make and model of hard drive or other media
- Storage capacity of device or hard drive
- Method of capture (tools used)
- Physical description of computer and whether it was on or off
- Name of the image file or resulting files that were collected
- Hash value(s) of source hard drive or files
- Hash value(s) of resulting image files for verification
- Any comments or issues encountered
- Signature(s) of persons giving and taking possession of evidence

3. The Creation of the Training Material

This paper is to fulfill a requirement for the Semester-in-Residence program offered at California State San Marcos as part of the Master of Science degree in Cybersecurity. The approach taken on the training material revolves around what the regular Systems Administrator should or should not do when facing a breach that requires a digital forensic investigation. The training material displays the steps that form the Collection phase during a digital forensic investigation and highlights the overall degree of difficulty involved at each phase of the NIST forensic process, particularly the collection phase. The paper concentrates on three of the four steps involved in the collection phase, *Identification, Labeling,* and R*ecording*.

The goal is to provide guidance to the regular Systems Administrator who is facing a breach and has the task of initiating the Collection phase by searching for data sources, recognizing and documenting the data sources, but leaving the actual acquisition of data to the trained forensic investigator or law enforcement investigator for reasons that will be mentioned throughout the document. In addition, the training material makes some suggestions for the regular Systems Administrator to follow at the scene prior the arrival of the investigator.

When I started to write this paper, my intention was to create a document that could help small organizations in the event of a data breach. By small organizations I mean those that lack IT departments in which the Systems Administrator is a "jack of all trades." In situations like these, a regular Systems Administrator has to wear multiple hats and he or she is typically in charge of a broad array of duties such as assisting users, installing and updating software and hardware, maintaining servers and supporting and troubleshooting the company's network. They are also on call for service outages and other technical problems. As if that were not enough, the Systems Administrator may even have the responsibility of overseeing the overall computer security of the organization.

In most cases, not always, regular Systems Administrators would have formal education such as a bachelor's degree in computer science, computer engineering, information systems or some other related technical field. In few other cases, they would simply hold either an associate's degree in systems administration or they would have no formal education at all. This last group is formed by individuals who just took on the job and learned the systems and processes the

organization needed to support along the road. Regardless of the case, regular Systems Administrators seem to share a common goal: making sure that the systems and networks they are in charge are running efficiently and effectively.

In order to create training material for the regular Systems Administrator - who is already overwhelmed with computers being up and running, protecting the network or replacing the ink cartridges on the printers - I needed to understand more about the details of the digital forensic process. I am not an expert on this subject. For this important task, I decided to follow the guidelines published by the National Institute of Standards and Technology (NIST) Special Publication 800-86, Guide to Integrating Forensic Techniques into Incident Response, and the guidelines from the National Institute of Justice (NIJ) versions 2004-2009. The forensic process as portrayed on NIST Special Publication 800-86 has four phases: Collection, Examination, Analysis and Reporting (Figure 1).

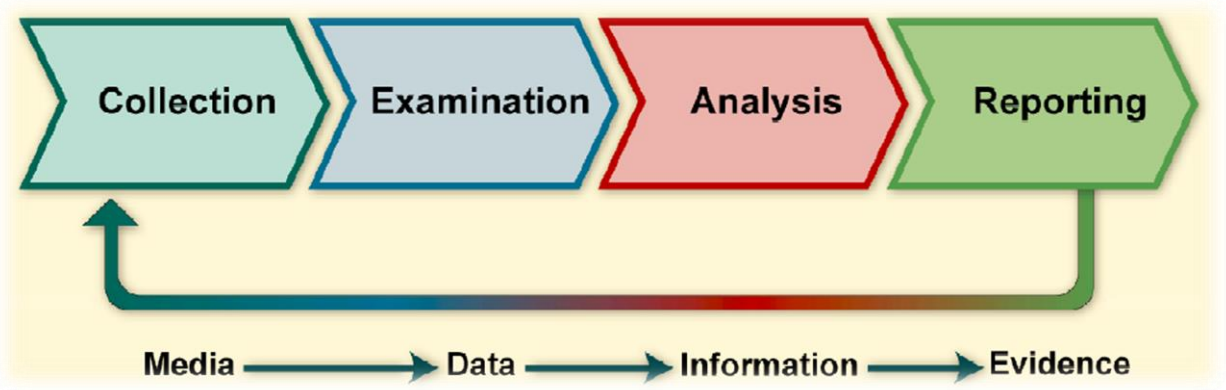

Figure 1. NIST SP 800-86 Forensic Process

Basically, the NIST 800-86 forensic process is a process of transformation from raw data all the way to evidence. During the collection phase, relevant data sources are identified, labeled, recorded and data is collected from these sources. After the data is collected, the examination phase takes place. In here, the data is extracted using forensic tools and appropriate methodologies and techniques. The result of the examinations goes through the analysis phase to gain useful information. Finally, a report is issued presenting all the findings and describing

every action taken during the investigation with some recommendations. A more detailed description based on NIST 800-86 publication is given next.

3.1. Collection Phase

It includes four steps: identification, labeling and recording of potential sources of data and the actual acquisition of data (NIST 800-86). A sound chain of custody should be followed when the digital forensic investigator begins with the acquisition of data. This final step is a time-consuming and difficult process even when it is performed on a powered down system. The acquisition of data described in this paper is on systems that have been powered down or "dead boxes" (traditional post-mortem forensics). The acquisition of data from live systems or "live boxes" (live box forensics) is beyond the scope of this paper.

Data acquisition requires making multiple copies of a hard drive to avoid changing or altering the original data. One of the imaging process widely used is bit stream imaging or bit-for-bit copy. The resulting copy can be a disk-to-disk copy or disk-to-file image of a disk depending on the preferences. Every step of the imaging process must be documented including name, version number and licensing information of the imaging software or hardware.

To protect the integrity of the original data during the imaging process, a write-blocker tool must be used to prevent any writes from the computer to the connected storage media. To verify the integrity of the original data, a message digest must be computed prior imaging the original data using a hashing algorithm. MD5 (Message Digest 5) and SHA1 (Secure Hash Algorithm 1) are the two most commonly used hashing algorithms. SHA1 is the approved federal standard (NIST 800-86). The resulting 160-bit hash value must be documented and stored in a secure location.

To verify the integrity of the copied data, a message digest must be computed as well on the copied data to prove that it is an exact duplicate of the original data. The resulting hash value must then be compared to the hash value of the original data. Things don't end here just yet. Then the investigator will compute the message digest one more time on the original data to verify that the imaging process did not change the original data. In addition, the message digest of every tool used in the process must be computed to verify file integrity. The resulting hash value must be documented and stored securely along with the exact commands that were used to run each tool including time and output.

3.2. Examination Phase

After data is collected it is ready to be examined. Examining data is also a time-consuming & difficult process since it requires specialized software, equipment, and technical expertise. Data is extracted using forensic tools and appropriate techniques dictated by the type of data being examined while preserving the integrity of the data. This phase absolutely requires the use of forensic tools to reveal deleted files existing in free or slack space, or hidden data, data protected by passwords, encryption, access control mechanisms or file compression - which can contain malicious payloads. The media containing the forensic tools must be write-protected and the data that is accessed must be in read-only format to ensure the integrity of the data being examined.

3.3. Analysis Phase

The result of the examinations goes through analysis to gain useful information in an attempt to answer the questions that led to the investigation. All methods and techniques used must be "legally justifiable”. This can be a lengthy process. Data that has been collected from the various sources of data can produce more information than the investigator can feasibly review. NIST recommends the use of a forensic toolkit to expedite data reviews.

3.4. Reporting Phase

Finally, a report is issued presenting all the findings and describing in high detail the actions taken, roadblocks encountered, further actions that might need to be taken, and making recommendations on ways to improve tools, guidelines and procedures. This phase finalizes the forensic process.

3.5. What the Regular Systems Administrator Should and Should Not Do?

The regular Systems Administrator should not play a prominent role in the forensic process. The regular Systems Administrator should only do the first three steps of the collection phase, identifying, labeling and recording of sources of data. The actual acquisition of data is a resource-intensive step that should be left to the digital forensic investigator. Acquiring data requires knowledge of forensic principles and techniques, tools, guidelines and procedures as well as knowledge of anti-forensic tools and techniques that could obscure or destroy data. The

regular Systems Administrator simply lacks the adequate forensic training and could unintentionally eliminate the opportunity to collect potentially important information.

The following list was taken from NIJ (2009). The regular Systems Administrator should give the forensic investigator:

- Case summary
- Preliminary reports and documents
- Investigation point of contact
- Suspected criminal activity
- Suspect information and nicknames
- Authorization to collect evidence
- Passwords

The forensic investigator should bring his or her own forensic tools, computer, backup devices, blank media, and initiate and maintain a strict chain of custody. The forensic investigator should have a detailed log of every step that was taken during the forensic investigation.

4. Training Material (Based on NIST SP 800-86 & NIJ Guidelines)

4.1. Verify Company's Policy

Confirm your organization has a policy in place that applies to forensic investigations

Policies, Guidelines and Procedures

Before any investigation begins, a policy must be in place or a court order from the law enforcement investigator (NIST 800-86). I am not going to talk about legal matters or details of policy writing on the training material but it is important to mention that clear policies, guidelines and procedures about privacy exist to support the position that the user had provided implied consent to a search and seizure by using the organization's networks under such a policy.

Written employment policies simplify the task of "reasonable expectation of privacy" when policies plainly state inspection, audit and/or monitoring of the employee's workspace should a forensic investigation occurs. This is very important. Keep in mind that it will not matter how good the evidence is if it's disqualified because it was acquired without proper consent.

In addition, it would be a great approach for organizations to have a forensic policy in place that clearly defines the roles and responsibilities of the staff assisting with the forensic activities (NIST 800-86). This facilitates the task of the regular Systems Administrator when identifying, labeling and recording possible sources of data and interacting with the forensic investigator.

Evidence Handling Supplies

The tasks of identifying, labeling and recording possible sources of data take some basic resources. The list may include:

- ✓ Digital camera
- ✓ Evidence tape
- ✓ Hard-bound notebook

- ✓ Chain of custody forms (Appendix B)
- ✓ Evidence storage bags and tags
- ✓ Antistatic bracelet
- ✓ Gloves

4.2. Secure the Scene

Make sure the area of potential sources of data is inaccessible to unauthorized people. One way to do it is by blocking the area with evidence tape.

4.3. Identify

Take a picture of the system setup at the scene as soon as possible.

4.3.1. Evaluate all Potential Sources of Data

Hard drives, storage devices and external media are examples of potential sources of evidence because they store user-created files and computer-created files such as backup files, log files, configuration files, cookies, history files and more. The scope of the training material will only cover two sections of sources of data in the IT infrastructure, hardware and data management. A brief description of each category is provided in the next section.

Sources of Data Sections in the IT Infrastructure

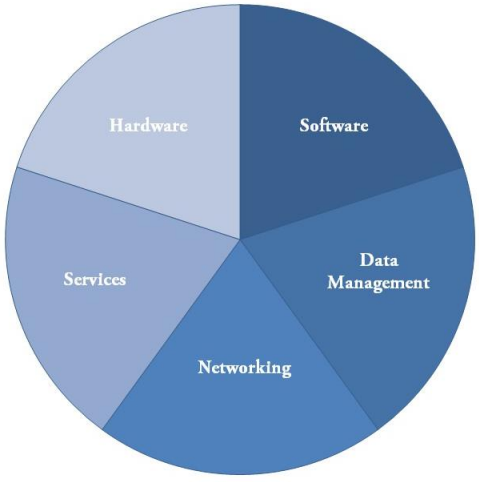

Figure 2. IT Infrastructure Components

Hardware

- Computer systems such as desktops, laptops, tablets and smartphones. The components include the system unit containing the processor, main memory, hard disk drive, monitor, keyboard, mouse, and CD/DVD drive. Peripheral devices attached to the systems include digital cameras, printers and scanners.

Software

- Application software such as accounting packages for evidence of fraud, ERP packages for employee records and activities, system and management files.

Services

- Remote resources that are *public* such as website used for social networking, discussion forums and newsgroups.
- Remote resource that are *private* such as an Internet Service Provider (ISP) logs of user's activity or a mobile phone company's records of customers' including text messages, voice calls, emails or internet chats.

Data Management

- External hard drives, removable media, flash drives and memory cards.

Networking

- Network infrastructure devices such as servers, switches, routers, and firewalls are examples of network devices (Davidoff, 2012).

4.3.2. Evaluate Each Source of Data Based on the Data Type It Holds

The two most common type of data are *volatile* and *non-volatile*.

Volatile Data

It's data that can be found in a "live system" or "live box" that has not lost power since the breach was noticed. Volatile data that exist in primary memory (Random Access Memory, RAM) include user names, password hashes, open documents, emails, registry information, malicious software code, recent commands and other valuable information. This information has a short shelf life that is lost after power is removed. Critical evidence like this needs to be retained before removing the power.

Non-Volatile Data

This data refers to data at rest. This type of data persist even after a system is powered down hence the name data from a "dead box". Non-volatile data can be found on read-only memory, flash memory, hard drives, optical disks and magnetic tapes. The filesystem is the largest and richest source of data on a hard drive. According to Johnson (2013), it contains most of the information recovered in a conventional forensic investigation. Filesystem data can be collected by performing logical backups and bit stream imaging.

The types of data commonly found within the filesystems are:

- Configuration Files
- Log Files
- Application Files
- Data Files
- Swap Files
- Dump Files
- Hibernation Files
- Temporary Files

4.3.3. Determine the Power State of the System or Device

- Watch the screen. Is the system or device on, off or in sleep mode?
- Look for LED lights or listen to fans running/drives spinning on a system.

If a computer or an electronic device is ON, leave it ON

- ✓ Do not move the computer
- ✓ Do not press any keys or click the mouse
- ✓ Do not try to explore or recover information
- ✓ Record all activity and processes visible on the display and photograph the screen
- ✓ Note changes in the display. If changes, photograph the screen.
- ✓ Check display screen for signs of data destruction. Look out for words such as “delete,” “format,” “remove,” “copy,” “move,” “cut” or “wipe”
- ✓ Look for indications that the computer is being accessed remotely or signs of ongoing communications
- ✓ Take note of all cameras and determine whether they are active
- ✓ Do not accept offers of help or technical assistance from unauthorized persons
- ✓ Request the assistance of a forensic investigator

Exceptions

According to NIJ (2009), immediate disconnection of power is recommended when:

- Activity on screen indicates information being deleted or overwritten
- A destructive process seems to be in progress
- Active data exfiltration is occurring (especially if it is sensitive data)

If a computer or an electronic device is OFF, leave it OFF

- ✓ Use antistatic bracelet to guard equipment against electrostatic discharges
- ✓ Document and photograph make, model, serial numbers, location, and user-assigned labels
- ✓ Document and photograph wires, and devices connected to the computer
- ✓ Identify external storage devices
- ✓ Remove and secure the power supply cord

- ✓ Disconnect and secure all wires and devices
- ✓ Place tape over the CD or DVD drive trays
- ✓ Place tape over the power switch

4.4. Label

If the computer is ON:

- Do not touch the computer
- Do not press any keys or click the mouse
- Wait for the digital forensic investigator

If the computer is OFF:

- Wear gloves and an antistatic bracelet when handling equipment
- Label all components
  - Computer
  - Storage devices
  - Media
  - Peripheral devices
  - Wires
  - Other
- Give a unique ID to each item.
  - This ID will be used on the evidence log, and a record will be created for every person who handles that evidence (NIST 800-86 & NIJ)

4.5. Record

Follow the five W's and an H: who, what, when, where, why and how.

- Who located and identified the sources of data?
- What time?
- When were the sources of data located and identified?
- Where are the sources of data located?
- Why? For what purpose was the sources of data located and identified?
- How the sources of data are being protected?

If the computer is ON:

Without touching the system,

- Document and photograph the computer setup
    - Document how each item is connected to each other
- Document and photograph the screen
    - Record all activity visible on the display
        - Screen saver
        - Running processes
        - Open documents, etc.
- Document and photograph all other components
    - Storage devices
    - Media
    - Peripheral devices
    - Wires
    - Other

If the computer is OFF:

Wearing gloves and an antistatic bracelet when handling equipment,

- Document and photograph the computer setup
    - Make, model, serial number
    - Location
    - User-assigned label (tag)
    - Document how each item is connected to each other
- Document and photograph the screen
- Document and photograph all other components
    - Storage devices
    - Media
    - Peripheral devices
    - Wires
    - Other

5. Conclusions

Without a doubt, no one knows an organization's IT infrastructure better than its Systems Administrator. They know in detail the IT infrastructure landscape inside and out, including hardware, software, data management, networks, and technology services. The regular Systems Administrator should *initiate* the collection phase by starting the tasks of *identification, labeling g* and *recording* of data sources without interfering with the company's daily business processes and operations. All what is needed is a few inexpensive evidence supplies. A digital camera and a notepad are simple, yet important tools, for the regular Systems Administrator when capturing and documenting evidence such as what was displaying on a computer screen when the breach was first noticed. Because proper collection of digital evidence is crucial to digital forensic investigations, the acquisition of data should be left to those that have specialized software, equipment, and technical expertise in digital forensics.

References

ACPO Good Practice Guide for Digital Evidence (2011). Electronic version retrieved from http://symas6b5.gb-02.live-paas.net/wp-content/uploads/2017/03/ACPO-digital-evidence-v5.pdf

Anti-Forensic Study (2015). NATO Cooperative Cyber Defense Centre of Excellence. Retrieved from https://ccdcoe.org/sites/default/files/multimedia/pdf/AF_with%20intro.pdf

Asha, J. & Singh, J.K. (2016). Review of Digital Forensic Models and A Proposal For Operating System Level Enhancements. Electronic version retrieved from http://www.academia.edu/30927690/Review_of_Digital_Forensic_Models_and_A_Proposal_For_Operating_System_Level_Enhancements

Ashcroft, J. (2001). Electronic Crime Scene Investigation. A Guide for First Responders. U.S. Department of Justice. Office of Justice Programs National Institute of Justice.

Ashcroft, J. (2001). National Institute of Justice. Electronic Crime Scene Investigation: A Guide for First Responders

Ashcroft, J., Daniels, D.J. & Hart, S.V. (2004). National Institute of Justice. Forensic Examination of Digital Evidence: A Guide for Law Enforcement.

Baggili, I. & Breitinger, F. (2015). Data Sources for Advancing Cyber Forensics: What the Social World Has to Offer. Electronic version retrieved from https://www.researchgate.net/publication/274065229

Carvey H. (2009). Windows Forensic Analysis DVD Toolkit. Syngress: Burlington, MA.

Carrier, B. D. (2006). Basic Digital Forensic Investigation Concepts. Electronic version retrieved from http://www.digital-evidence.org/di_basics.html

Clarke, N., Tryfonas, T. & Dodge, R. (2012). Proceedings of the Seventh International Workshop on Digital Forensics and Incident Analysis. Electronic version retrieved from https://books.google.com/books.

Chva, K. G. (2006). How to Preserve Digital Evidence in Case of Legal Investigation. Electronic version retrieved from https://edtechmagazine.com/higher/article/2006/10/how-preserve-digital-evidence-case-legal-investigation

Coons, P. (2015). How to Document Your Chain of Custody and Why It's Important. Electronic version retrieved from http://d4discovery.com/discover-more/how-to-document-your-chain-of-custody-and-why-its-important#sthash.9D9JU2v1.dpuf

Cosic, J. & Cosic, Z. (2012). Chain of Custody and Life Cycle of Digital Evidence. Electronic version retrieved from http://www.davidpublishing.com/davidpublishing/Upfile/3/29/2012/2012032902750283.pdf

Davidoff, S. & Ham J. (2012). Network Forensics: Tracking Hackers through Cyberspace. Upper Saddle River, NJ:Pearson Education.

Glossary of Court Terms. Electronic version retrieved from http://www.uscourts.gov/glossary

Goodison, S. E., Davis, R. C. & Jackson, B. A. (2015). Digital Evidence and the U.S. Criminal Justice System. Identifying Technology and Other Needs to More Effectively Acquire and Utilize Digital Evidence. Electronic version retrieved from http://www.rand.org/pubs/research_reports/RR890.html

Holder E., Robinson L. & Rose K. (2009). National Institute of Justice. Electronic Crime Scene Investigation: An On-the-Scene Reference for First Responders.

Johnson, L. (2013). Computer Incident Response and Forensics Team Management: Conducting a Successful Incident Response. Syngress: Waltham, MA.

Kent, K., Chevalier, S., Grance, T. & Dang, H. NIST SP 800-86. Guide to Integrating Forensic Techniques into Incident Response.

Marcella, A. & Menendez, D. (2007). Cyber Forensics: A Field Manual for Collecting, Examining, and Preserving Evidence of Computer Crimes. CRC Press: Boca Raton, FL.

Mukasey, M.B., Sedgwick, J.L. & Hagy, D.W. (2008). National Institute of Justice. Electronic Crime Scene Investigation: A Guide for First Responders, Second Edition.

National Institute of Standards and Technology (NIST) Special Publication 800-86, Guide to Integrating Forensic Techniques into Incident Response

Nationwide (2016). National Survey Reveals Most Small Businesses Unprepared for Cyberattacks. Retrieved from https://www.nationwide.com/about-us/101316-cybersecurity.jsp

Neal, A. (2014). Identifying and Preserving Digital Evidence. Retrieved from https://www.slideshare.net/isightsoftware/i-sight-webinar-andrew-neal-digital-evidence-v2-2

Oppenheimer, P. (n.d.). Computer Forensics: Seizing a Computer. Electronic version retrieved from http://www.priscilla.com/forensics/computerseizure.html

Primeau Forensics. Importance of the Chain of Custody for Digital Media Evidence. Electronic version retrieved from http://www.primeauforensics.com/audio-forensics/7-importance-of-the-chain-of-custody-for-digital-media-evidence/

Rocha, L. (2014). Computer Forensics and Investigation Methodology - 8 Steps. Electronic

version retrieved from

https://countuponsecurity.com/2014/08/06/computer-forensics-and-investigation-methodology-8-steps/

Rowlingson, R. (2004). A Ten Step Process for Forensic Readiness. Electronic version retrieved from https://www.utica.edu/academic/institutes/ecii/publications/articles/A0B13342-B4E0-1F6A-156F501C49CF5F51.pdf

Solomon, M. G., Rudolph, K., Tittel., E., Broom, N., Barett, D. (2011). Computer Forensics Jumpstart. Wiley: Indianapolis, IN.

Sommer, P. (1998). Intrusion Detection Systems as Evidence, Recent Advances in Intrusion Detection. Electronic version retrieved from http://www.raid-symposium.org/raid98/Prog_RAID98/Full_Papers/Sommer_text.pdf

Stevens, M. (2016). 28 Data Breach Statistics That Will Inspire You (To Protect Yourself). Electronic version retrieved from https://www.bitsighttech.com/blog/data-breach-statistics

Stone, A. (2015). Chain of Custody: How to Ensure Digital Evidence Stands Up In Court. Retrieved from https://www.govtechworks.com/chain-of-custody-how-to-ensure-digital-evidence-stands-up-in-court/#gs.NtFzIsI

Xenophontos, M. The cost of a Data Breach and Why the "Chain of Custody" is important. Electronic version retrieved from https://www.linkedin.com/pulse/cost-data-breach-why-chain-custody-important-marios-xenophontos

Appendices

Appendix A. Chain of Custody Template

Hard Drive/Computer Details

Description:		
Manufacturer:	Model #:	Serial #:

Chain of Custody

Date/Time:	From:	To:	Reason:
Date:	Name/Organization:	Name/Organization:	
Time:	Signature:	Signature:	
Date:	Name/Organization:	Name/Organization:	
Time:	Signature:	Signature:	
Date:	Name/Organization:	Name/Organization:	
Time:	Signature:	Signature:	
Date:	Name/Organization:	Name/Organization:	
Time:	Signature:	Signature:	
Date:	Name/Organization:	Name/Organization:	
Time:	Signature:	Signature:	
Date:	Name/Organization:	Name/Organization:	
Time:	Signature:	Signature:	

Appendix B. Training Material for the Regular Systems Administrator Facing a Breach