

WHITE PAPER

# Maintaining Crime Scene Integrity

WHITE PAPER

# Maintaining Crime Scene Integrity

A. Bryan Sartin  
Managing Principal,  
Investigative Response  
Verizon Business  
Security Solutions

## TABLE OF CONTENTS

- 1. Minimize the handling and corruption of evidence .....2
- 2. Freeze the environment .....2
- 3. Account for changes and keep detailed logs of all actions .....3
- 4. Comply with the five rules of evidence .....3
- 5. Do not exceed your knowledge .....3
- 6. Follow in-house security policy and obtain written permission .....3
- 7. Ensure all actions are repeatable .....3
- 8. Move fast! .....4
- 9. Don't shut down before collecting evidence .....4
- 10. Don't run any programs on the affected system. ....4
- Conclusion .....5



# Maintaining Crime Scene Integrity

Security breaches leading to the compromise of sensitive information have become a very real concern for organizations in a number of industries worldwide. When it comes to investigating these compromises, successfully determining the source and full extent of the breach in a manner sufficient for prosecution is often predicated on whether or not basic evidentiary guidelines are adhered to. In fact, one of the greatest obstacles faced by qualified forensic examiners today involves logical and physical changes to digital evidence, specifically those changes occurring before the start of the investigation. In order to set any given IT investigative or computer forensic engagement up for success from an evidentiary perspective, please consider the following 10 high-level pointers to maintaining crime scene integrity:

## 1. Minimize the handling and corruption of evidence

The successful outcome of a computer forensic investigation is largely based on the availability and preservation of digital evidence. Without any malicious intent, organizations suffering data compromise commonly tamper with evidence sources before engaging a qualified forensic examiner, creating an unnecessary handicap for the ensuing investigation. Handling or otherwise tampering with digital evidence before an investigation begins can lead to unusable evidence sets, limiting the possibility for arrest and prosecution from the start. At the onset of any forensic investigation, planning, thoughts, and actions must be focused on minimizing changes that could negatively impact the evidence set—both digital and hardcopy. The goal is to try and keep the evidence as close as possible to its original state at the time of the incident.

## 2. Freeze the environment

Prior to the start of a forensics investigation, digital evidence can be tainted by the actions taken by otherwise well-intentioned first responders. Upon recognizing a computer incident, first responders often “poke around” the affected computer systems and, so doing, may alter the evidence set to an extent, sometimes rendering it useless to the qualified forensic examiner. When responding to a suspected or confirmed security breach, it is critical that the environment is locked down until a professional arrives. Determine what your organization’s “freeze point” is. This is the point at which the sophistication and complexity of a given incident exceeds the technical capabilities of the personnel assigned to handle it. Alternately, the freeze point may be reached when the incident involves the possible compromise of external data for which the organization may perceive a conflict of interest. Either way, every organization has a freeze point which varies depending on the in-house incident response capabilities, including experience, tools, and skill sets.

### **3. Account for changes and keep detailed logs of all actions**

When responding to a computer incident, changes to the affected systems may be inevitable. While these changes are to be avoided wherever possible, they can often be safely accounted for in the course of forensics analysis provided that suitable measures are taken to track them. Each system, network, and application-level alteration, no matter how minor, must be carefully recorded during the incident response life cycle; otherwise, they may create unintended consequences during analysis. Consider setting up a system by which incident response actions, including but not limited to containment measures, can not only be written down but also be witnessed by another individual or group. Also, consider videotaping any actions that may be difficult to log. It is of utmost importance that each action performed during the course of the incident response life cycle is accounted for. While this may seem tedious at first, you'll be glad the information is available later on in the investigation.

### **4. Comply with the five rules of evidence**

"Guidelines for Evidence Collection and Archiving" (RFC3227) detail that computer evidence must meet the following conditions:

**Admissible    Authentic    Complete    Reliable    Believable**

Incident response policy and procedural documentation should clearly reflect these evidentiary requirements. Keep in mind that one of the most proven ways to limit negative impacts to the crime scene and the digital evidence therein is to openly communicate these five rules of evidence to in-house incident response personnel. Understanding the complexities surrounding the collection, handling, and usage of digital evidence will reinforce the establishment of a company-standard freeze point and help to ensure that in-house personnel adhere to existing incident-handling policies.

### **5. Do not exceed your knowledge**

As much as qualified forensic examiners and incident handlers attempt to proceduralize the incident response process, unexpected circumstances will inevitably surface. When it comes to handling the unexpected, consider the following. If you've never handled a similar situation or have no precedence to draw from, you are probably in over your head. Call in support. Guesswork is not a part of the incident response life cycle. Incident response policies should dictate when to call in a professional and identify expert resources that can be called upon in the event of an emergency. If the answer is not to be found in existing documented policy, do not act on your own. Instead, always defer to management-level direction and consensus.

### **6. Follow in-house security policy and obtain written permission**

Pursuant to pointer #5 above, incident-handlers should carefully follow existing incident response policies wherever possible. However unexpected situations will arise. When that happens, seek direction. Do not act on your own. Obtain written management-level permission before performing any actions, including containment measures, for which there are no provisions under existing incident response policies. In the absence of documented policy, expressed consent is a must.

### **7. Ensure all actions are repeatable**

Experienced incident handlers do not experiment during a live exercise. Before committing any action in response to an incident, ensure that action is fully repeatable. This includes making sure that the action is either backed by policy or by management-level discretion, as well as logged and capable of being reversed. Covering these bases in the decision-making process will streamline the entire incident response effort, setting the mission up for success, and also help set the stage for prosecution.

## **8. Move fast!**

The time elapsed between when a computer incident is first detected and when the ensuing investigation begins can be a major problem. This grey area not only adversely impacts the outcome of the incident investigation but can also pose a threat to the organization itself vis-à-vis the illegitimate usage of the information compromised. When sensitive information may be at risk, containment is the primary objective. Act fast. Immediately upon discovering evidence of security breach, the actions taken by first responders should ensure that evidence is preserved in a secure and forensically sound manner. Move quickly toward the company freeze point. Consider the development of scripts within documented incident response procedures to provide timelier collection of evidence while minimizing impacts to the dataset.

## **9. Don't shut down before collecting evidence**

A computer system victimized by security breach may house hidden code designed to destroy evidence on startup and shutdown. Concurrently, rebooting that system can cause hundreds or even thousands of unintended file system changes to occur, including but not limited to the loss of volatile memory and the overwriting of other data. When evidence of security breach is uncovered on a given system, remove that system from the network. Do not power it down. Immediately move to collect volatile memory and a forensic image of the file system. If the system has already been powered down, do not allow the boot process to start until a proper forensic image can be collected. Use a write-blocking device in the image acquisition process.

## **10. Don't run any programs on the affected system**

Pursuant to pointer #9 above, avoid running any programs or performing Q&A on computer systems that may have been victimized by security breach. Interacting with the affected system should be minimized to avoid corruption of the digital evidence it might contain. Do not install an anti-virus package and/or trigger a file system scan on the affected system upon discovering evidence of security breach. Do not download and install trojan scanner software, then search the file system looking for evidence of unauthorized access. These types of measures will contaminate the crime scene by altering file date and timestamps, making forensic analysis unnecessarily difficult. Instead, disconnect the system from the network and do not power it down. Collect volatile memory as quickly as possible and proceed to forensic imaging.

## Conclusion

These 10 pointers for maintaining crime scene integrity are not intended as a comprehensive listing of evidentiary guidelines, nor are they specific to any single type of organization, business, or IT environment. These pointers should be considered as suggested ways to set computer forensics and IT investigative engagements up for success and are based on common mistakes that organizations make when responding to perceived security breaches and investigating suspected compromises of sensitive information. Additional publicly available information on this subject can be found in the following online resources:

Australian Computer Emergency Response Team (AusCERT)

<http://www.uscert.org/>

Carnegie Mellon University Software Engineering Institute CERT

<http://www.cert.org/>

©2008 Verizon. All Rights Reserved. WP12851 03/08

The information contained in this document is solely for example purposes only and not intended to be relied on for implementation purposes or otherwise by the reader. Verizon hereby expressly disclaims any indication to the contrary. Verizon, its affiliates or subsidiaries, and a customer are only bound by the terms and conditions contained in a contract between the parties. The Verizon and Verizon Business names and logos and all other names, logos, and slogans identifying Verizon's products and services are trademarks and service marks or registered trademarks and service marks of Verizon Trademark Services LLC or its affiliates in the United States and/or other countries. All other trademarks and service marks are the property of their respective owners.

WP12851 03/08