Evidence Collection and Data Seizure

1. Why Collect Evidence?

The simple reasons for collecting evidence are:

- **Future Prevention**: Without knowing what happened, you have no hope of ever being able to stop someone else from doing it again.
- **Responsibility**: The attacker is responsible for the damage done, and the only way to bring him to justice is with adequate evidence to prove his actions. The victim has a responsibility to the community. Information gathered after a compromise can be examined and used by others to prevent further attacks.

2. Collection Options

Once a compromise has been detected, you have two options:

- **Pull the system off the network and begin collecting evidence**: In this case you may find that you have insufficient evidence or, worse, that the attacker left a dead man switch that destroys any evidence once the system detects that its offline.
- **Leave it online and attempt to monitor the intruder**: you may accidentally alert the intruder while monitoring and cause him to wipe his tracks any way necessary, destroying evidence as he goes.

3. Obstacles

- Computer transactions are fast, they can be conducted from anywhere, can be encrypted or anonymous, and have no intrinsic identifying features such as handwriting and signatures to identify those responsible.
- Any paper trail of computer records they may leave can be easily modified or destroyed, or may be only temporary.
- Auditing programs may automatically destroy the records left when computer transactions are finished with them.
- Investigating electronic crimes will always be difficult because of the ease of altering the data and the fact that transactions may be done anonymously.
- The best we can do is to follow the rules of evidence collection and be as assiduous as possible.

4. Types of Evidence

- **Real Evidence:** Real evidence is any evidence that speaks for itself without relying on anything else. In electronic terms, this can be a log produced by an audit function—provided that the log can be shown to be free from contamination.
- **Testimonial Evidence:** Testimonial evidence is any evidence supplied by a witness. As long as the witness can be considered reliable, testimonial evidence can be almost as powerful as real evidence.
- **Hearsay:** Hearsay is any evidence presented by a person who was not a direct witness. Hearsay is generally inadmissible in court and should be avoided.

5. The Rules of Evidence •••••

1. **Admissible**: Admissible is the most basic rule. The evidence must be able to be used in court.
2. **Authentic**: You must be able to show that the evidence relates to the incident in a relevant way.
3. **Complete**: It's not enough to collect evidence that just shows one perspective of the incident.
4. **Reliable**: Your evidence collection and analysis procedures must not cast doubt on the evidence's authenticity and veracity.
5. **Believable**: The evidence you present should be clearly understandable and believable to a jury.

Using the preceding five rules, we can derive some basic do's and don'ts:

- **Minimize handling and corruption of original data:** Once you've created a master copy of the original data, don't touch it or the original. Any changes made to the originals will affect the outcomes of any analysis later done to copies.
- **Account for any changes and keep detailed logs of your actions:** Sometimes evidence alteration is unavoidable. In these cases, it is absolutely essential that the nature, extent, and reasons for the changes be documented.
- **Comply with the five rules of evidence:** Following these rules is essential to guaranteeing successful evidence collection.
- **Do not exceed your knowledge:** If you ever find yourself "out of your depth," either go and learn more before continuing (if time is available) or find someone who knows the territory.
- **Follow your local security policy:** If you fail to comply with your company's security policy, you may find yourself with some difficulties.
- **Capture as accurate an image of the system as possible:** Capturing an accurate image of the system is related to minimizing the handling or corruption of original data.

- **Be prepared to testify:** If you're not willing to testify to the evidence you have collected, you might as well stop before you start. No one is going to believe you if they can't replicate your actions and reach the same results.
- **Work fast:** The faster you work, the less likely the data is going to change. Volatile evidence may vanish entirely if you don't collect it in time. If multiple systems are involved, work parallel.
- **Proceed from volatile to persistent evidence:** Always try to collect the most volatile evidence first.
- **Don't shutdown before collecting evidence:** You should never, ever shutdown a system before you collect the evidence. Not only do you lose any volatile evidence, but also the attacker may have trojaned the startup and shutdown scripts, plug-and-play devices may alter the system configuration, and temporary file systems may be wiped out.
- **Don't run any programs on the affected system:** The attacker may have left trojaned programs and libraries on the system; you may inadvertently trigger something that could change or destroy the evidence you're looking for.

6. Volatile Evidence

Always try to collect the most volatile evidence first. An example an order of volatility would be:

1. Registers and cache
2. Routing tables
3. Arp cache
4. Process table
5. Kernel statistics and modules
6. Main memory
7. Temporary file systems
8. Secondary memory
9. Router configuration
10. Network topology

7. General Procedure

- ✓ **Identification of Evidence**: You must be able to distinguish between evidence and junk data
- ✓ **Preservation of Evidence**: The evidence you find must be preserved as close as possible to its original state.
- ✓ **Analysis of Evidence**: Analysis requires in-depth knowledge of what you are looking for and how to get it.
- ✓ **Presentation of Evidence**: The manner of presentation is important, and it must be understandable by a layman to be effective.

8. Collection and Archiving

Once we've developed a plan of attack and identified the evidence that needs to be collected.

- **Logs and Logging:** You should run some kind of system logging function. It is important to keep these logs secure and to back them up periodically. Messages and logs from programs can be used to show what damage an attacker did.
- **Monitoring**: By monitoring we can gather statistics, watch out for irregular, and trace where an attacker is coming from and what he is doing. Unusual activity or the sudden appearance of unknown users should be considered definite cause for closer inspection. You should display a disclaimer stating what monitoring is done when users log on.

9. Methods of Collection

There are two basic forms of collection: freezing the scene and honeypotting.

Freezing the Scene

- ✓ It involves taking a snapshot of the system in its compromised state. You should then start to collect whatever data is important onto removable nonvolatile media in a standard format.
- ✓ All data collected should have a cryptographic message digest created, and those digests should be compared to the originals for verification.

Honeypotting

- ✓ It is the process of creating a replica system and luring the attacker into it for further monitoring.
- ✓ The placement of misleading information and the attacker's response to it is a good method for determining the attacker's motives.

10. Artifacts

- There is almost always something left behind by the attacker—be it code fragments, trojaned programs, running processes, or sniffer log files. These are known as artifacts.
- Never attempt to analyze an artifact on the compromised system.
- Artifacts are capable of anything, and we want to make sure their effects are controlled.

11. Collection Steps

1. **Find the Evidence:** Use a checklist. Not only does it help you to collect evidence, but it also can be used to double-check that everything you are looking for is there.
2. **Find the Relevant Data:** Once you've found the evidence, you must figure out what part of it is relevant to the case.
3. **Create an Order of Volatility:** The order of volatility for your system is a good guide and ensures that you minimize loss of uncorrupted evidence.
4. **Remove external avenues of change:** It is essential that you avoid alterations to the original data.
5. **Collect the Evidence:** Collect the evidence using the appropriate tools for the job.
6. **Document everything:** Collection procedures may be questioned later, so it is important that you document everything you do. Timestamps, digital signatures, and signed statements are all important.

12. Controlling Contamination: The Chain of Custody

Once the data has been collected, it must be protected from contamination. Originals should never be used in forensic examination; verified duplicates should be used.

A good way of ensuring that data remains uncorrupted is to keep a chain of custody. This is a detailed list of what was done with the original copies once they were collected.

Analysis

✓ Once the data has been successfully collected, it must be analyzed to extract the evidence you wish to present and to rebuild what actually happened.

Time

✓ To reconstruct the events that led to your system being corrupted, you must be able to create a timeline.

- ✓ Never, ever change the clock on an affected system.

Forensic Analysis of Back-ups

- ✓ When we analyze back-ups, it is best to have a dedicated host for the job. We need a dedicated host which is secure, clean and isolated from any network for analyzing back-ups.
- ✓ Document everything you do. Ensure that what you do is repeatable and capable of always giving the same results.

Reconstructing the Attack

After collecting the data, we can attempt to reconstruct the chain of events leading to and following the attacker's break-in. We must correlate all the evidence we have gathered. Include all of the evidence we've found when reconstructing the attack---no matter how small it is.

Searching and Seizing

There is no one methodology for performing a computer forensic investigation and analysis.

There are too many variables for to be just one way. Some of the typical variable that comes to the mind includes operating systems; software applications; cryptographic algorithms and applications; and hardware platforms. But moving beyond these obvious variables spring other equally challenging variables: law, international boundaries, publicity, and methodology.

There are a few widely accepted guidelines for computer forensic analysis:

- ✓ A computer forensic examiner is impartial. Our job is to analyze the media and report our findings with no presumption of guilt or innocence.
- ✓ The media used in computer forensic examinations must be sterilized before each use.
- ✓ A true image (bit stream) of the original media must be made and used for the analysis.
- ✓ The integrity of the original media must be maintained throughout the entire investigation

Before the Investigation

- ✓ For the sake of first argument, you must have skilled technicians in-house and a top notch lab----the right equipment, the right computer forensic tools, and so on.
- ✓ District attorneys may require more documentation on the chain of evidence handling.
- ✓ When you have a case arise, you know what is required and can work the case from the inception in support of these requirements.

Methodology Development

- Define your methodology, and working according to this methodology.
- Here methodology defines a method, a set of rules: guidelines that are employed by a discipline.

Document Everything

The chain of evidence is so important in computer forensic investigations. If resources allow, have two computer forensic personnel assigned to each case every step of the way. Important in the documentation are the times that dates steps were taken; the names of those involved; and under whose authority were the steps taken?

Evidence Search and Seizure

Prior to search and seizure, you already have the proper documents filled as well as permission from the authority to search and seize the suspect's machine.

Step 1: Preparation

You should check all media that is to be used in the examination process. Document the wiping and scanning process. Check to make sure that all computer forensic tools are licensed for use and all lab equipment is in working order.

Step 2: Snapshot

We should photograph the scene, whether it is a room in a home or in a business. You should also note the scene. Take advantage of your investigative skills here. Note pictures, personal items, and the like. Photograph the actual Evidence. For example, the evidence is a PC in a home office. Take a photograph of the monitor. Remove the case cover carefully and photograph the internals.

Step 3: Transport

If you have the legal authority to transport the evidence to your lab, you should pack the evidence securely. Photograph/videotape and document the handling of evidence leaving the scene to the transport vehicle and from transport vehicle to the lab examination facility.

Step 4: Examination

You should prepare the acquired evidence for examination in your lab. There are many options to on what tool to use image the drive. You could use *EnCase*, the Unix command DD, *ByetBack*, or also *SafeBack*. It is wise to have a variety of tools in your lab. Each of these tools has its respective strengths. The important note to remember here is: Turn off virus-scanning software. We must record the time and date of the COMS. Do not boot the suspect machine.

When making the image, make sure that the tool you use does not access the file system of the target evidence media. After making the image, seal the original media in an electrostatic-safe container, catalog it, and initial the container. Finally, the examination of the acquired image begins.