

# Evidence Collection and Data Seizure

- **Evidence is difficult to collect at the best of times, but when that evidence is electronic, an investigator faces some extra complexities.**
- This part of the chapter is not aimed at expert forensics analysts, the simple reason for this is that there never is one correct answer that will guide you through all investigations.
- **No two investigations are the same, and the only thing you can ever be sure about when arriving at the scene is that there is nothing you can be sure about.**

# WHY COLLECT EVIDENCE?

- Electronic evidence can be very expensive to collect.
- The processes are strict and exhaustive, the systems affected may be unavailable for regular use for a long period of time, and analysis of the data collected must be performed
- There are two simple reasons for collecting evidence: future prevention and responsibility.

- **Future Prevention**

- Without knowing what happened, you have no hope of ever being able to stop someone else (or even the original attacker) from doing it again.

- **Even though the cost of collection can be high, the cost of repeatedly recovering from compromises is much higher, both in monetary and corporate image terms.**

- **Responsibility**

- **There are two responsible parties after an attack: the attacker and the victim.**
- **The attacker is responsible for the damage done, and the only way to bring him to justice (and to seek recompense) is with adequate evidence to prove his actions.**
- **The victim, on the other hand, has a responsibility to the community. Information gathered after a compromise can be examined and used by others to prevent further attacks.**
- The victim may also have a legal obligation to perform an analysis of evidence collected, for instance if the attack on their system was part of a larger attack.

# COLLECTION OPTIONS

- **Once a compromise has been detected, you have two options: pull the system off the network and begin collecting evidence or leave it online and attempt to monitor the intruder.**
- Both have their pros and cons. **In the case of monitoring, you may accidentally alert the intruder while monitoring and cause him to wipe his tracks any way necessary, destroying evidence as he goes.**
- You also leave yourself open to possible liability issues if the attacker launches further attacks at other systems from your own network system.
- **If you disconnect the system from the network, 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 it's offline.**
- What you choose to do should be based on the situation. The “Collection and Archiving” section later in the chapter contains information on what to do for either case.

# OBSTACLES

- Electronic crime is difficult to investigate and prosecute.
- Investigators have to build their case purely on any records left after the transactions have been completed
- Add to this the fact that electronic records are extremely (and sometimes transparently) malleable and that electronic transactions currently have fewer limitations than their paper-based counterparts and you get a collection nightmare

- Computer transactions are fast, they can be conducted from anywhere (through anywhere, to 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.
- Worse still, auditing programs may automatically destroy the records left when computer transactions are finished with them.

- **Because of this, even if the details of the transactions can be restored through analysis, it is very difficult to tie the transaction to a person.**
- ***Identifying* information such as passwords or PIN numbers (or any other electronic identifier) does not prove who was responsible for the transaction.**
- Such information merely shows that whoever did it either knew or could get past those identifiers.
- **Even though technology is constantly evolving, 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 you can do is to follow the rules of evidence collection and be as assiduous as possible.

# TYPES OF EVIDENCE

- **Before you start collecting evidence, it is important to know the different types of evidence categories.**
- Without taking these into consideration, you may find that the evidence you've spent several weeks and quite a bit of money collecting is useless.
- **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.**
- **This type of evidence is subject to the perceived reliability of the witness, but as long as the witness can be considered reliable, testimonial evidence can be almost as powerful as real evidence.**
- Word processor documents written by a witness may be considered testimonial— as long as the author is willing to state that he wrote it.
- **Hearsay**
- **Hearsay is any evidence presented by a person who was not a direct witness.**
- Word processor documents written by someone without direct knowledge of the incident are hearsay.
- Hearsay is generally inadmissible in court and should be avoided

# THE RULES OF EVIDENCE

- There are five rules of collecting electronic evidence.
- These relate to five properties that evidence must have to be useful.
  - 1. Admissible
  - 2. Authentic
  - 3. Complete
  - 4. Reliable
  - 5. Believable

## Admissible

- *Admissible* is the most basic rule. The evidence must be able to be used in court or otherwise.
- Failure to comply with this rule is equivalent to not collecting the evidence in the first place, except the cost is higher.

## Authentic

- If you can't tie the evidence positively to the incident, you can't use it to prove anything.
- You must be able to show that the evidence relates to the incident in a relevant way.

## Complete

- It's not enough to collect evidence that just shows one perspective of the incident.
- You collect not only evidence that can prove the attacker's actions, but also evidence that could prove their innocence.
- **For instance, if you can show the attacker was logged in at the time of the incident, you also need to show who else was logged in and why you think they didn't do it.**
- **This is called *exculpatory evidence* and is an important part of proving a case.**

## Reliable

- **The evidence you collect must be reliable.**
- Your evidence collection and analysis procedures must not cast doubt on the evidence's authenticity and veracity.

## Believable

- **The evidence you present should be clearly understandable and believable to a jury.**
- **There's no point presenting a binary dump of process memory if the jury has no idea what it all means.**
- Similarly, if you present them with a formatted, human understandable version, you must be able to show the relationship to the original binary, otherwise there's no way for the jury to know whether you've faked it.

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

1. Minimize handling and corruption of original data.
2. Account for any changes and keep detailed logs of your actions.
3. Comply with the five rules of evidence.
4. Do not exceed your knowledge.
5. Follow your local security policy.
6. Capture as accurate an image of the system as possible.
7. Be prepared to testify.
8. Work fast.
9. Proceed from volatile to persistent evidence.
10. Don't shutdown before collecting evidence.
11. Don't run any programs on the affected system.

## 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.
- **Always handle secondary copies. Any changes made to the originals will affect the outcomes of any analysis later done to copies.**
- You should make sure you don't run any programs that modify the access times of all files (such as tar and xcopy).
- You should also remove any external avenues for change and, in general, analyze the evidence after it has been collected.

## 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.**
- Any changes at all should be accounted for—not only data alteration but also physical alteration of the originals (the removal of hardware components).



## Comply with the Five Rules of Evidence

- **The five rules are there for a reason.**
- **If you don't follow them, you are probably wasting your time and money.**
- Following these rules is essential to guaranteeing successful evidence collection.

## Do Not Exceed Your Knowledge

- **If you don't understand what you are doing, you can't account for any changes you make and you can't describe what exactly you did.**
- 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.
- Never soldier on regardless. You'll just damage your case.

## Follow Your Local Security Policy

- **If you fail to comply with your company's security policy, you may find yourself with some difficulties.**
- Not only may you end up in trouble (and possibly fired if you've done something really against policy), but you may not be able to use the evidence you've gathered.
- If in doubt, talk to those who know.

## 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.**
- Differences between the original system and the master copy count as a change to the data. You must be able to account for the differences

## 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.**
- **Without the collector of the evidence being there to validate the documents created during the evidence-collection process, the evidence becomes hearsay, which is inadmissible.**
- Remember that you may need to testify at a later time. No one is going to believe you if they can't replicate your actions and reach the same results.
- This also means that your plan of action shouldn't be based on trial-and-error.

## 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.**
- This is not to say that you should rush.
- **You must still collect accurate data. If multiple systems are involved, work on them in parallel (a team of investigators would be handy here), but each single system should still be worked on methodically.**
- Automation of certain tasks makes collection proceed even faster.

## Proceed from Volatile to Persistent Evidence

- **Some electronic evidence (discussed later) is more volatile than others are.**
- Thus, you should 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 (via a trojan horse) the startup and shutdown scripts, plug-and-play devices may alter the system configuration, and temporary file systems may be wiped out.**
- Rebooting is even worse and should be avoided at all costs. As a general rule, until the compromised disk is finished with and restored, it should never be used as a boot disk.

## **Don't Run Any Programs on the Affected System**

- **As 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.**
- Any programs you use should be on read-only media (such as a CD-ROM or a write-protected floppy disk) and should be statically linked.

# VOLATILE EVIDENCE

- **Not all the evidence on a system is going to last very long. Some evidence resides in storage that requires a consistent power supply; other evidence may be stored in information that is continuously changing.**
- **When collecting evidence, you should always try to proceed from the most volatile to the least.**
- Of course, you should still take the individual circumstances into account.
- You shouldn't waste time extracting information from an unimportant or unaffected machine's main memory when an important or affected machine's secondary memory hasn't been examined.

- To determine what evidence to collect first, you should draw up an order of volatility—a list of evidence sources ordered by relative volatility.
- 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



# GENERAL PROCEDURE

- When collecting and analyzing evidence, there is a general four-step procedure you should follow.
- Note that this is a very general outline. You should customize the details to suit your situation.

## Identification of Evidence

- **You must be able to distinguish between evidence and junk data.**
- **For this purpose, you should know what the data is, where it is located, and how it is stored.**
- Once this is done, you will be able to work out the best way to retrieve and store any evidence you find.

## Preservation of Evidence

- **The evidence you find must be preserved as close as possible to its original state.**
- Any changes made during this phase must be documented and justified.

## Analysis of Evidence

- **The stored evidence must then be analyzed to extract the relevant information and recreate the chain of events.**
- Analysis requires in-depth knowledge of what you are looking for and how to get it.
- Always be sure that the person or people who are analyzing the evidence are fully qualified to do so.

## Presentation of Evidence

- **Communicating the meaning of your evidence is vitally important—otherwise you can't do anything with it.**
- The manner of presentation is important, and it must be understandable by a layman to be effective.
- It should remain technically correct and credible. A good presenter can help in this respect.

# COLLECTING AND ARCHIVING

- Once you've developed a plan of attack and identified the evidence that needs to be collected, it's time to start the actual process of capturing the data.
- Storage of that data is also important, as it can affect how the data is perceived.

## 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.
- Because logs are usually automatically time-stamped, a simple copy should suffice, although you should digitally sign and encrypt any logs that are important to protect them from contamination.

- Remember, if the logs are kept locally on the compromised machine, they are susceptible to either alteration or deletion by an attacker.
- Having a remote syslog server and storing logs in a *sticky* directory can reduce this risk, although it is still possible for an attacker to add decoy or junk entries into the logs.
- Regular auditing and accounting of your system is useful not only for detecting intruders but also as a form of evidence.
- Messages and logs from programs can be used to show what damage an attacker did.
- Of course, you need a clean snapshot for these to work, so there's no use trying it after the compromise.

## Monitoring

- **Monitoring network traffic can be useful for many reasons—you can gather statistics, watch out for irregular activity (and possibly stop an intrusion before it happens), and trace where an attacker is coming from and what he is doing.**
- Monitoring logs as they are created can often show you important information you might have missed had you seen them separately.
- This doesn't mean you should ignore logs later—it may be what's missing from the logs that is suspicious.
- Information gathered while monitoring network traffic can be compiled into statistics to define normal behavior for your system.
- These statistics can be used as an early warning of an attacker's actions. You can also monitor the actions of your users.
- This can, once again, act as an early warning system.
- **Unusual activity or the sudden appearance of unknown users should be considered definite cause for closer inspection.**
- **No matter the type of monitoring done, you should be very careful.**
- There are plenty of laws you could inadvertently break.
- **In general, you should limit your monitoring to traffic or user information and leave the content unmonitored unless the situation necessitates it.**
- **You should also display a disclaimer stating what monitoring is done when users log on. The content of this should be worked out in conjunction with your lawyer.**

# METHODS OF COLLECTION

- **There are two basic forms of collection: freezing the scene and honeypotting. The two aren't mutually exclusive.**
- You can collect *frozen* information after or during any honeypotting.
- Freezing the scene involves taking a snapshot of the system in its compromised state.
- The necessary authorities should be notified (the police and your incident response and legal teams), but you shouldn't go out and tell the world just yet.
- You should then start to collect whatever data is important onto removable non-volatile media in a standard format.
- **Make sure the programs and utilities used to collect the data are also collected onto the same media as the data.**
- **All data collected should have a cryptographic message digest created, and those digests should be compared to the originals for verification.**

- **Honey potting is the process of creating a replica system and luring the attacker into it for further monitoring.**
- **A related method (sandboxing) involves limiting what the attacker can do while still on the compromised system, so he can be monitored without (much) further damage.**
- The placement of misleading information and the attacker's response to it is a good method for determining the attacker's motives.
- **You must make sure that any data on the system related to the attacker's detection and actions is either removed or encrypted; otherwise they can cover their tracks by destroying it.**
- **Honey potting and sandboxing are extremely resource intensive, so they may be infeasible to perform.**
- There are also some legal issues to contend with, most importantly entrapment. As previously mentioned, you should consult your lawyers

# ARTIFACTS

- **Whenever a system is compromised, 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*. They are one of the important things you should collect, but you must be careful.**
- **You should never attempt to analyze an artifact on the compromised system. Artifacts are capable of anything, and you want to make sure their effects are controlled.**
- **Artifacts may be difficult to find; trojaned programs may be identical in all obvious ways to the originals (file size, medium access control [MAC] times, etc.).**
- Use of cryptographic checksums may be necessary, so you may need to know the original file's checksum.
- If you are performing regular file integrity assessments, this shouldn't be a problem.
- Analysis of artifacts can be useful in finding other systems the attacker (or his tools) has broken into.



# COLLECTION STEPS

- You now have enough information to build a step-by-step guide for the collection of the evidence.
- Once again, this is only a guide. You should customize it to your specific situation. You should perform the following collection steps:
  - 1. Find the evidence.
  - 2. Find the relevant data.
  - Create an order of volatility.
  - 4. Remove external avenues of change.
  - 5. Collect the evidence.
  - 6. Document everything.

## Find the Evidence

- **Determine where the evidence you are looking for is stored.**
- 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.

## Find the Relevant Data

- **Once you've found the evidence, you must figure out what part of it is relevant to the case.**
- **In general, you should err on the side of over-collection, but you must remember that you have to work fast.**
- Don't spend hours collecting information that is obviously useless.

## Create an Order of Volatility

- **Now that you know exactly what to gather, work out the best order in which to gather it.**
- The order of volatility for your system is a good guide and ensures that you minimize loss of uncorrupted evidence.

## Remove External Avenues of Change

- **It is essential that you avoid alterations to the original data, and prevention is always better than a cure.**
- **Preventing anyone from tampering with the evidence helps you create as exact an image as possible.**
- However, you have to be careful. The attacker may have been smart and left a dead-man switch.
- In the end, you should try to do as much as possible to prevent changes.

## Collect the Evidence

- **You can now start to collect the evidence using the appropriate tools for the job.**
- As you go, re-evaluate the evidence you've already collected. You may find that you missed something important, now is the time to make sure you get it.

## Document Everything

- **Your 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. Don't leave anything out.

# 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.**
- This not only ensures that the original data remains clean, but also enables examiners to try more *dangerous*, potentially data-corrupting tests.
- **Of course, any tests done should be done on a clean, isolated host machine. You don't want to make the problem worse by letting the attacker's programs get access to a network.**
- **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.**
- Remember that this will be questioned later on, so document everything (who found the data, when and where it was transported [and how], who had access to it, and what they did with it).
- **You may find that your documentation ends up greater than the data you collected, but it is necessary to prove your case**

## 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.**
- As always, you must make sure that you fully document everything you do.
- Your work will be questioned and you must be able to show that your results are consistently obtainable from the procedures you performed.

## Time

- **To reconstruct the events that led to your system being corrupted, you must be able to create a timeline. This can be particularly difficult when it comes to computers.**
- **Clock drift, delayed reporting, and differing time zones can create confusion in abundance. One thing to remember is to never, ever change the clock on an affected system.**
- **Record any clock drift and the time zone in use, as you will need this later, but changing the clock just adds in an extra level of complexity that is best avoided.**
- Log files usually use timestamps to indicate when an entry was added, and these must be synchronized to make sense.
- **You should also use timestamps. You're not just reconstructing events, you yourself are making a chain of events that must be accounted for as well. It's best to use the GMT time zone when creating your timestamps.**
- The incident may involve other time zones than your own, so using a common reference point can make things much easier.

## Forensic Analysis of Backups

- **When analyzing backups, it is best to have a dedicated host for the job.**
- **This examination host should be secure, clean (a fresh, hardened install of the operating system is a good idea), and isolated from any network. You don't want it tampered with while you work, and you don't want to accidentally send something nasty down the line.**
- **Once this system is available, you can commence analysis of the backups. Making mistakes at this point shouldn't be a problem.**
- **You can simply restore the backups again if required. Remember the mantra: Document everything you do. Ensure that what you do is repeatable and capable of always giving the same results.**