**Standards of Evidence - The rules of Evidence:**

**Digital evidence types**

**This includes email, text messages, instant messages, files and documents extracted from hard drives, electronic financial transactions, audio files, and video files.**

 There are five rules of collecting electronic evidence. These relate to five properties that evidence must have to be useful.

* Admissible
* Authentic
* Complete
* Reliable
* 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 with 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. Not only should you collect 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 evidences authenticity and veracity.

Believable

The evidence you present should be clearly understandable and believable by 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**:

* Minimize handling/corruption of original data
* Account for any changes and keep detailed logs of your actions
* Comply with the five rules of evidence
* Do not exceed your knowledge
* Follow your local security policy
* Capture as accurate an image of the system as possible
* Be prepared to testify
* Ensure your actions are repeatable
* Work fast
* Proceed from volatile to persistent evidence
* Don’t shutdown before collecting evidence
* Don’t run any programs on the affected system
* Minimize Handling/Corruption of Original Data

Once you’ve created a master copy of the original data, don’t touch it or the original itself—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 (i.e., 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’re just damaging 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 also 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.
* Ensure That Your Actions Are Repeatable
* 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 be collecting 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 (see below) is more volatile than others are. Because of this, 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 (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

Because 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.