Risk Analysis for Evidence Collection

Technically the main goal of computer forensics is to identify, collect, preserve, and analyze data in a way that preserves the integrity of the evidence collected so it can be used effectively in a legal case.

The following five are the necessary basic steps in that order to conduct a computer forensic examination. Although documentation is listed as the last step, a well-trained examiner should understand that documentation is continuous throughout the entire examination process.

1. Policy and Procedure Development
2. Evidence Assessment
3. Evidence Acquisition
4. Evidence Examination
5. Documenting and Reporting

Digital Evidences :

Data from computer systems, networks, wireless communications, and storage devices collected in a way that is admissible as evidence in a court of law.

Basic types of data are collected in computer forensics.

Persistent data is the data that is stored on a local hard drive (or another medium) and is preserved when the computer is turned off.

Volatile data is any data that is stored in memory, or exists in transit, that will be lost when the computer loses power or is turned off. Volatile data resides in registries, cache, and random access memory (RAM). Since volatile data is ephemeral, it is essential an investigator knows reliable ways to capture it.

Network data is the data obtained from network communication. This data includes protocol, IP addresses, ports, number of packets and information in packets.

Evidence Collection :

Computer evidence, like all other evidence, must be handled carefully and in a manner that preserves its evidentiary value. This relates not just to the physical integrity of an item or device, but also to the electronic data it contains.

Certain types of computer evidence require special collection, packaging, and transportation. Consideration should be given to protect data that may be susceptible to damage or alteration from electromagnetic fields such as those generated by static electricity, magnets, radio transmitters, and other devices.

Electronic evidence should be collected according to guidelines maintained by the United States Department of Justice. The United States Department of Justice's Cyber Crime web site lists recent court cases involving computer forensics and computer crime, and it has guides about how to introduce computer evidence in court and what standards apply. The important point for forensics investigators is that evidence must be collected in a way that is legally admissible in a court case.

In the absence of departmental guidelines outlining procedures for electronic evidence collection follow your agency's protocol regarding evidence collection. Every agency should develop policies and procedures that establish the parameters for operation and function. An effective way to begin this task is to develop a mission statement that incorporates the core functions of the agency, whether those functions include high-technology crime investigations, evidence collection, or forensic analysis.

Risks Involved:

If computer forensics is practiced badly, you risk destroying vital evidence or having forensic evidence ruled inadmissible in a court of law. Also, you or your organization may run afoul of new laws that mandate regulatory compliance and assign liability if certain types of data are not adequately protected.

The risks associated with collecting and preserving digital evidences can be broadly classified as Integrity Risks and Legal Risks.

Integrity Risks - loss of some or whole part of evidence due to the technology applied to collect evidence. Examples

(1) To reduce the risk of manipulating the evidences on a disk the first step in the investigation process is to clone or image the disk. The investigator has to take care of the original disk while talking an image or clone, as it may crash during copying and evidence may be lost. The reason why one first copies and then hashes is to reduce the risk of crashing the disk when hashing it.

(2) When doing live data collection every user and kernel space tool used to collect data by nature changes the state of the target system. By running any tools on a live system we load them into memory and create at least one process which can overwrite possible evidence. By creating a new process, the memory management system of the operating system allocates data in main memory and then can overwrite other unallocated data in main memory or in the swap file system

(3) During live data collection the signs of intrusions found in images of main memory can be untrusted, because they could be created by acquisition tools.

So before taking any action it must be decided whether to acquire some data from a live compromised system or not. It is very often worth it to collect such information.

(4) Programs used to monitor network traffic can become overloaded and fail to retain all packets captured by the kernel. Although TCP is designed to retransmit dropped packets, network sniffers are not active participants in the communication channel and will not cause packets to be resent. (E.g. Network-monitoring programs like tcpdump, Snort, and NetWitness read network traffic that is buffered in memory by libpcap. If the program cannot read the data quickly enough, libpcap records this fact before discarding unread packets to make space for new ones. The number of packets that were not read by the packet capture program are reported by libpcap when the collection process is terminated. Although it may not be possible to infer the content of lost datagrams, it is useful to quantify the percentage loss.)

(5) Network-monitoring applications may show only certain types of data (e.g., only Internet Protocol data) and may introduce error or discard information by design or unintentionally during operation.

Legal Risks - Those companies or individuals that fail to address the regulatory standards risk losing business, paying hefty fines and incurring additional restrictions on future business operations. Examples

(1) Before intercepting the employees email the organization must adopt a policy in which under extenuating circumstances and employees email activities are placed under surveillance. If the policies are not clearly outlined before the surveillance begins the activity could be a breach to the employees private emails.

(2) Violations of any one of the statutes during the practice of computer forensics could constitute a federal felony punishable by a fine and/or imprisonment. It is always advisable to consult a legal counsel if you are in doubt about the implications of any computer forensics action on behalf of your organization.

(3) HP's investigators acknowledged in a memo that they used an electronic ruse to try to trick CNET's News.com journalist Dawn Kawamoto into revealing her sources for stories that included HP's confidential information. HP sent a tracer (Web Bug) to discover Journalist’s sources. By and large, the Web bug is a widely used legal tool but under certain situations, the use of a Web bug might be considered a violation of false advertising laws if HP used the Web bug to spy on someone, particularly when it espouses a privacy policy that says it doesn't do such things.

Risk Analysis :

The investigator before collecting evidences should first know all the risks involved when using a specific tool to collect evidences. Not calculating risks before collecting evidences may lead to loss of evidences. The risk assessment should be thus carried out before collection process is started. In some cases Risk analysis is valuable even after evidence collection process so as not to repeat the mistake again.

References:

(1) Electronic Crime Scene Investigation: A Guide for First Responders
(2) Forensic Examination of Digital Evidence: A Guide for Law Enforcement
(3) Error, Uncertainty, and Loss in Digital Evidence - Eoghan Casey, MA
(4) Computer Forensics US-CERT
(5) www.dfrws.org/2005/proceedings/keneally_risk_slides.pdf
(6) Incident Response & Computer Forensics – Kevin Mandia,Chris Prosise & Matt Pepe