FOCUSED ON THE FACTS

I.R.I.S. LLC
Information Retrieval Investigative Services

COMPUTER FORENSICS

In many ways, digital evidence from a computer must be dealt with the same way as any other type of evidence. It is subject to the same need for defense inspection, the same chain of custody requirements and the same rules of admissibility. Defense counsel has to inspect computerized evidence as carefully as they would a stack of documents that were seized as evidence or any other type of physical evidence. It can be very time sensitive and must be handled properly.

Common Computer Forensics Scenarios

- In criminal cases
- Theft of intellectual property such as customer lists or trade secrets
- Preservation orders/e-Discovery
- Employment issues
- Fraud or embezzlement
- Inappropriate computer usage
- Divorce
- Loss of data

Principles of Digital Evidence

1. Investigation and analysis of digital evidence must be done in accordance with governing industry standards.
2. Actions taken to secure or analyze the digital evidence should not change the integrity of the evidence.
3. Persons conducting an examination of digital evidence should be trained for that purpose.
4. Activity relating to the seizure, examination, storage or transfer of digital evidence should be documented, preserved and available for review.

Best Practices & Industry Standards

The prevailing governing standards are set forth by The Scientific Working Group of Digital Evidence (SWGDE) and The National Institute of Justice (NIJ).

U.S. Department of Justice
Office of Justice Programs
National Institute of Justice

SCIENTIFIC WORKING GROUP FOR DIGITAL EVIDENCE
SWGDE

International Organization Standardization - ISO

ISO is an independent, non-governmental international organization that sets specifications for products, services and systems, to ensure that they follow statutory and regulatory requirements related to a product or program quality, safety and efficiency. Pursuant to the best practices and industry standards, the examination of digital evidence should be conducted in accordance with a quality management system such as ISO 17020 or 17025.

Data Integrity

Digital evidence should never be accessed as this can change data such as dates and times. Operating a computer or accessing files can change the metadata and change the evidence. Steps should be taken to ensure the integrity of the data acquired; this may include one or more of the following:

- Hash values (e.g., MD5, SHA-1 and SHA-256)
- Stored on read-only media (e.g., CD-R and DVD-R)
- Sealed in tamper-evident packaging

Training Levels

Computer forensic examination training levels are dictated by Industry Standards and Best Practices which suggest examiners should be trained as discussed in *SWGDE/SWGIT Guidelines & Recommendations for Training in Digital & Multimedia Evidence*.

Computer Basics

Computers are a device which process electronic information called data using pre-set instructions called programs. The physical machinery is referred to as *hardware* and the data and programs are known as *software*. Computers store data as binary information (0's or 1's) in the memory on storage media known as the hard drive or hard disc drive (HDD). The binary data is called a bit, and 8 bits makes a byte. When grouped in sequence, this binary information is converted to data by the central processing unit (CPU) that is processed by the computer and displayed to the user.

Output Devices
System Unit
Mass Storage Device
Input Devices

<u>HDD Memory Types and Behavior</u>

Computers may use different types of hard drives. Most computers use magnetic hard drives, although solid state hard drives (SSD) have become more popular due to their increased speed as the prices have decreased.

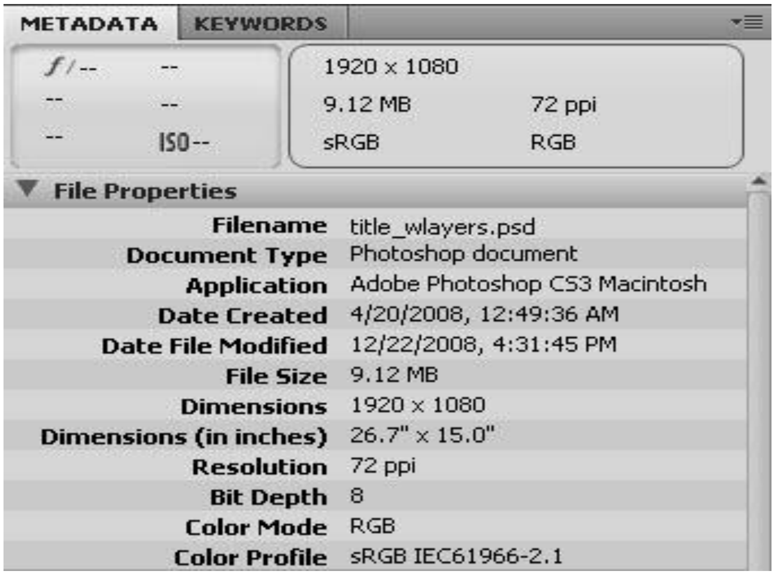
- Magnetic Memory – Data is stored on rotating disk platters.
- Flash Memory (Solid State Drives) – Data is stored on electronic circuits

Magnetic Drive

Solid State Drive

<u>Metadata</u>

Files and programs have unique identifying information such as created date, modified date accessed dates also called metadata. Metadata is the data that describes data.



f / --	--	1920 x 1080	
--	--	9.12 MB	72 ppi
--	ISO --	sRGB	RGB

File Properties

Filename	title_wlayers.psd
Document Type	Photoshop document
Application	Adobe Photoshop CS3 Macintosh
Date Created	4/20/2008, 12:49:36 AM
Date File Modified	12/22/2008, 4:31:45 PM
File Size	9.12 MB
Dimensions	1920 x 1080
Dimensions (in inches)	26.7" x 15.0"
Resolution	72 ppi
Bit Depth	8
Color Mode	RGB
Color Profile	sRGB IEC61966-2.1

Memory Retention & Overwrite

The biggest difference between the two drive types is how data that has been deleted is handled. A magnetic hard drive can record new data directly over old data. A solid state drive must first erase the old data by resetting the entire area to be reused to binary “zeros.” Deleted data on a magnetic hard drive may remain indefinitely and can often be recovered by forensic techniques.

Data Recovery

Computers must be able to quickly find the data stored on an HDD. The computer operating system (OS) has a method to track the files on a computer. Bytes are grouped into sectors which are grouped into clusters, which is set-up during the initial formatting of the HDD by the OS. A cluster is the smallest unit that can be written to. When a file on a magnetic HDD is deleted and a new file is later saved to the same location, partial data from the old file may still exist within the cluster.

Partial data from a deleted file may still exist within the cluster and be recovered.

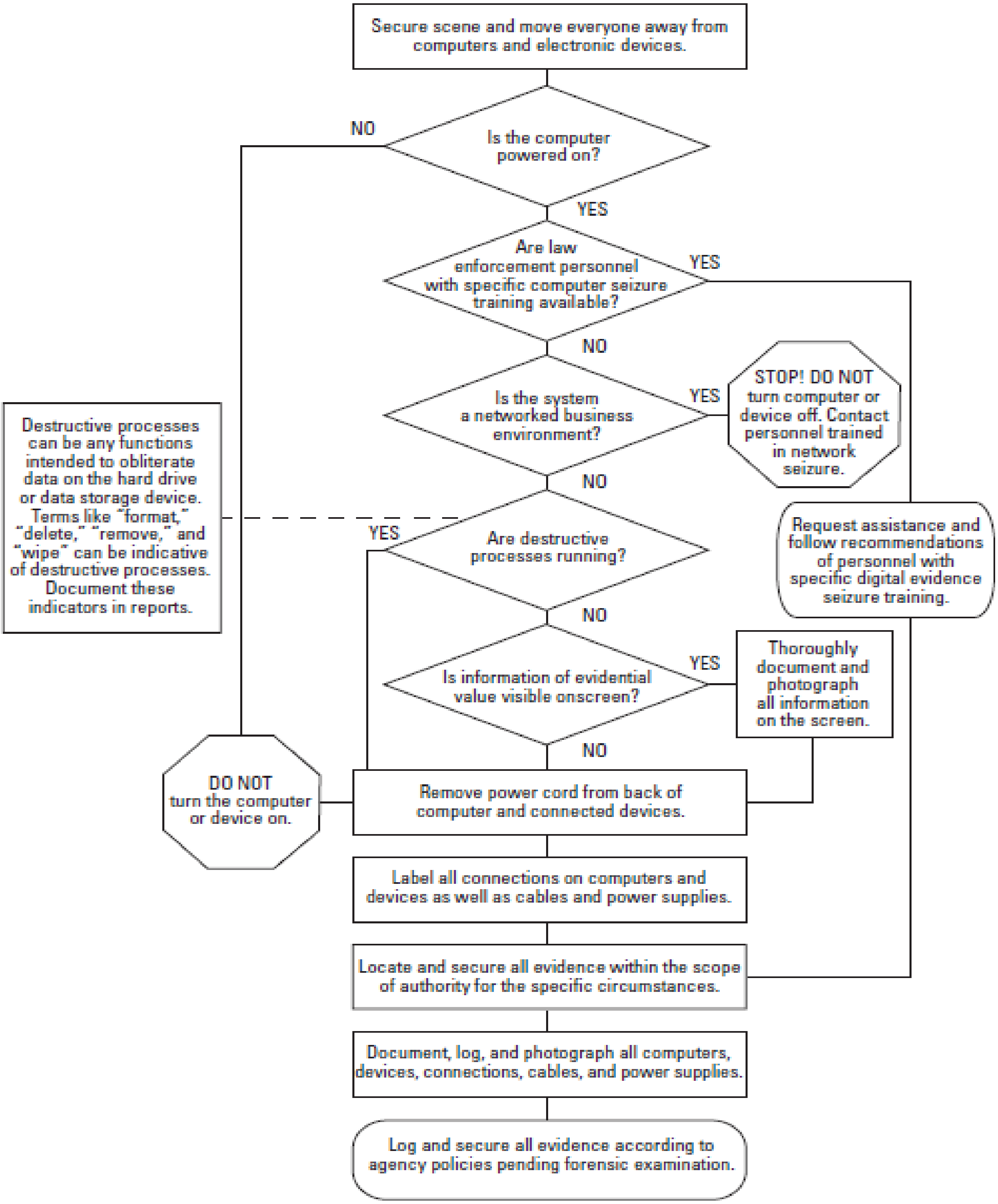
Rapid Assessment and Preservation

On a solid state drive, the operating system will periodically erase deleted data on its own, making recovery impossible. With either a standard hard drive or a solid state drive, recovery of deleted data may be extremely time sensitive. The best practices require rapid assessment and preservation to prevent the permanent loss of data.

Types of Data

- Users
- Multi-media (photos, videos or audio files)
- Documents or spreadsheets
- E-mail
- Internet browsing history (searches, sites visited, typed addresses)
- Program files
- Deleted files
- Deleted programs
- Encrypted files and folders
- File sharing
- Application data
- Social networking data
- Mobile device backups
- Financial records
- File metadata

Collecting Digital Evidence Flowchart (NIJ)


Secure scene and move everyone away from computers and electronic devices.
Is the computer powered on?
NO
YES
Are law enforcement personnel with specific computer seizure training available?
YES
NO
Is the system a networked business environment?
YES
STOP! DO NOT turn computer or device off. Contact personnel trained in network seizure.
NO
Destructive processes can be any functions intended to obliterate data on the hard drive or data storage device. Terms like "format," "delete," "remove," and "wipe" can be indicative of destructive processes. Document these indicators in reports.
YES
Are destructive processes running?
Request assistance and follow recommendations of personnel with specific digital evidence seizure training.
NO
Is information of evidential value visible onscreen?
YES
Thoroughly document and photograph all information on the screen.
NO
DO NOT turn the computer or device on.
Remove power cord from back of computer and connected devices.
Label all connections on computers and devices as well as cables and power supplies.
Locate and secure all evidence within the scope of authority for the specific circumstances.
Document, log, and photograph all computers, devices, connections, cables, and power supplies.
Log and secure all evidence according to agency policies pending forensic examination.

Evidence Packaging & Transport

Each piece of evidence should be protected from damage or alteration, labeled and a chain-of-custody maintained as determined by organizational policy. Specific care should be taken with the transportation of digital evidence to avoid physical damage, vibration and the effects of magnetic fields, electrical static and large variations of temperature and/or humidity.

Forensic Data Acquisition

The first step for investigation of digital evidence begins with the preservation of evidence through the forensic acquisition process. The forensic acquisition process is to create a verified forensic copy of the electronic data to be examined. Methods of acquiring evidence should be forensically sound and verifiable; method deviations shall be documented.

Acquisition Types

- Physical
- Logical
- Live
- Targeted File(s)

Acquisition Documentation should include

- Examiner’s name.
- Acquisition date.
- Acquisition details (e.g., type of acquisition, imaging tool and version number).
- Physical condition of the evidence and unique identifiers (e.g., serial number, description, make and model).
- Original and verification hash values.
- Photographs and/or sketches.
- Any additional documentation as required by the examiner’s organization.

Examination Documentation

The secondary objective is to conduct forensic examination and searching for evidence. Examination documentation should be case specific and contain sufficient details to allow another forensic examiner, competent in the same area of expertise, to identify what was done and to replicate the findings independently.

Report of Finding

- Information should be presented in a format that may be read and understood by non-technical individuals.
- Examiners should be able to explain all information contained within the report.
- Should include any relevant information contained within the acquisition and/or evidence handling documentation.
- Reports issued by the examiner should address the requestor’s needs.
- Document the scope and/or purpose of the examination.

- Give a detailed description of the media examined (e.g., hard disk, optical media or flash drive).
- Include any supplemental reports related to the examination.
- Provide the examiner’s name and date of exam.
- Be reviewed according to organizational policy.

References
NIJ Investigations Involving the Internet and Computer Networks 01-2007
SWGDE Best Practices Computer Forensics 09-05-2014
SWGDE Capture of Live Systems 090514
SWGDE Peer to Peer Technologies 013008

For more information on computer forensics and digital evidence, call now and speak with a certified expert. I.R.I.S. LLC is available 24 hours in emergency cases.