ONE POLICY APPROACH REGARDING DIGITAL EVIDENCE ACQUISITION
AND ANALYSIS

FORWARD

This document offers one approach regarding a policy for the preservation and analysis of digital evidence by computer forensic specialists and special agents. It is offered up in the spirit of collaboration that has led to many advances within the field of computer forensics.

In forwarding this policy approach, we are in no way claiming some rare or exclusive insight into the very complex and dynamic field of computer forensics. However, it is our hope this document will help others, particularly law enforcement organizations, with policy development in this growing area of importance. We also hope that others will consider sharing portions of their policy and procedures as they are developed and continuously refined. We fully expect to regularly revise our policy and procedures to adapt to the changing legal and technological landscape affecting the computer forensics discipline.

Setting the stage for the policy approach offered below, it is worth noting emphasis is placed on procedures relating to the initial acquisition of digital evidence. Initial acquisition of digital evidence is emphasized as reasonable doubt regarding the integrity and authenticity of the initial digital evidence acquisition may very well not be recoverable.

We thank members of the Computer Crimes and Intellectual Property Section (CCIPS) of the Department of Justice for taking the time to review and comment on an earlier version of this document. We also thank Doctoral Candidate Nicole Beebe for the time she took to review and comment on an earlier version of this document.

Copyright Notice: This document is a work of the US Government. In accordance with 17 USC 105, copyright protection is not available for any work of the US Government. Additionally, there is no warranty regarding the content of this document.

Please address questions or comments to the authors:

Barry Grundy (bgrundy@imx.hq.nasa.gov);
John Garris (jgarris@imx.hq.nasa.gov).
I. BACKGROUND

A. Introduction. The evolution of information technologies continues at a very fast pace, and is expected to continue at this pace for the foreseeable future. As a result of this ever-changing environment, and the numerous situational dependent variables regularly presented to computer forensic professionals, this document will make no effort to command a checklist of minute steps to be taken in an investigation. The numbers of variables associated with changing computer technology, coupled with the unique facts that define individual investigations, frequently require adaptive problem solving to identify, preserve and accurately interpret volatile digital evidence.

In the place of an inflexible “checklist” approach, this guide establishes a series of conceptual steps, and provides an outline of those data that must be sought to ensure the highest standards as to the integrity of digital evidence and the fidelity of forensic analyses. It is important certain data be consistently and accurately recorded, where available and when situations permit. Such consistency facilitates the uniform presentation of evidence to the end consumer. Also, a consistent framework for the collection and analysis of digital evidence will promote clearer and more consistent communication of findings, as well as promote greater confidence in the integrity and accuracy of those findings.

B. Definitions.

1. **Forensics.** The application of scientific knowledge and technical procedures to legal problems; especially: scientific analysis of evidence (as from a crime scene).

2. **Working Copies of Digital Evidence.** Exact copies of the best digital evidence available. The best available digital evidence will be stored and tracked in accordance with agency evidence handling procedures. The use of approved hash algorithms are used to verify that working copies are an accurate copy of the best digital evidence. Analyses using working copies are highly preferred in the event media failures or unintended alterations are made of the data during the analysis phase.

3. **Working Session.** As applied to calibration (described later in this document), a session is defined as use of a forensic platform during acquisition of digital evidence. For the purpose of calibration, a new session will need to be recorded when any of the following occur: a) A change in date; b) acquisition work shifts to support an unrelated investigation; c) updates to the operating system, device firmware or forensic software; or d) previous failure of calibration attempts. (Note: this definition does not apply to acquisition hardware/software used for monitoring dynamic user activity, such as the acquisition of network traffic.)
4. **Cross Verification.** The use of different software and/or hardware tools to provide a level of assurance that the results of forensic analyses are accurate. For example, if a commercially available software forensic tool provides a result of significance, then a completely different tool (such as a GNU Linux tool) should be used to provide a greater level of assurance that the digital evidence of significance is being interpreted accurately.

5. **Acquisition.** The process of gathering data to preserve and archive. The term refers both to the collection of evidentiary forensic images as well as those data, pertinent to the case, gathered from any digital device in support of an investigation. Acquisitions can be performed through a variety of methods. A few examples include: through the use of a ‘Single-Use Device,’ such as a handheld imaging tool, via a network monitoring device, or via the simple act of obtaining logs from intrusion detection systems.

6. **Forensic Platform.** Any device, to include secondary-use computers and primary-use computer systems (as described below), used for the purpose of forensically acquiring and/or forensically analyzing digital evidence.

7. **Primary Use Forensic Platform.** Any device or computer specifically procured or configured to be used as a forensic platform or acquisition device is referred to as “Primary Use”. These are the hardware devices most commonly used to acquire and analyze digital evidence. The term “Primary Use” is used in consideration of record keeping requirement as set forth in this document.

8. **Secondary Use Forensic Platform.** Any device or computer, not specifically procured or configured for forensic use, that is used for the collection or analysis of digital evidence in those cases where the agent or technician deems the use of such a device appropriate. The term “Secondary Use” is used in consideration of record keeping requirements as set forth in this document.

9. **Single-Use Device.** These are devices designed to be limited to a single specific purpose. Handheld imaging tools and hardware write blockers are examples of Single-use devices. The term “Single-use Device” is used in consideration of calibration requirements.

10. **Multi-Use Device.** Devices that, although may be employed for a specific purpose, are capable of being used for any number of computational tasks. Desktop computers and forensic workstations are examples of Multi-use devices. The term “Multi-use Device” is used in consideration of calibration requirements.

11. **Target System.** With regard to this document, target system refers to a computer or digital device from which digital evidence is being sought.
12. Controls and Standards. In the context of these guidelines, “controls” are defined as supplementary procedures set up to allow comparisons. “Standards” are described as a sample containing a qualitative or quantitative known.

13. Network Monitors. These are special purpose computer systems configured specifically for use in acquiring network traffic in support of investigations. These kits are considered primary use forensic platforms.

14. Forensic Tower. This term refers to the PC units employed by the Agency as primary forensic analysis workstations. These systems are considered primary use forensic platforms.

15. Mobile Analysis Platform. Referred to as a “MAP”, these are PC units configured to be portable and provide a flexible on-site forensic analysis and acquisition platform. MAPs are considered primary use forensic platforms.

C. Scope. The field of digital investigation encompasses more and more storage devices everyday. Our most common form of digital evidence is the computer hard drive. Increasingly, however, we are presented with cases where Personal Digital Assistants (PDA), cellular telephones, media storage devices (e.g. TIVO and portable music devices), modified game consoles and other electronic equipment are used to store significant amounts of digital evidence.

The specific data and evidence\(^1\) recording requirements presented in this document will, in most cases, apply to all digital devices. However, it is impossible to accurately predict the nature of digital devices and their potential evidentiary value very far into the future. The investigator must be prepared to apply “best practices” in the collection and review of such evidence, using this document as a framework, and relying on testing and evaluation of available acquisition and analysis tools.

D. Limitations. As previously discussed, this document is limited to providing a framework for baseline standards of forensic digital evidence acquisition, analysis and reporting for the Agency -- emphasis is placed on procedures relating to the acquisition of digital evidence. In addition to the factors noted earlier, this document is bounded by:

- Future information technologies, the make up of which may not conform to the framework provided in this document.
- Common sense application to *prima facie* evidence\(^2\). In other words, not all evidence obtained from electronic devices will require forensic analysis. For example, network logs obtained from a trusted intrusion detection device or network router typically do not require specialized forensic acquisition

---

\(^1\) Not all data recorded will be considered “evidence” in all cases. This document does not intend to set forth a limited definition of what is considered evidence.

\(^2\) *prima facie* evidence is that information sufficient to establish a fact, unless rebutted.
techniques. (This does not, however, preclude proper steps to preserve and ensure the integrity of such evidence).

- Operational constraints that may require deviation from these guidelines. There are a number of variables that will likely affect digital evidence acquisition. For example:

  - There may be cases where a balance must be struck between evidence preservation steps and the potential negative impact those steps may have on systems that affect Agency operations. Legal liability as a result of interruption of computer services outside of the Agency should be carefully considered as part of the response or search warrant execution plan. Also, time constraints or circumstances can limit the practicality of some investigative steps. For example, surreptitious acquisition (so as not to alert the subject), may require skipping, or postponing, some steps, such as normal integrity checks.

  - *In-extremis* responses. When potential digital evidence is presented unexpectedly and the volatility of such evidence requires immediate acquisition with sub-optimal resources.

E. **Overview.** Section II of this chapter will start with a description of basic validation of tools and processes. The section on validation will include procedures to check basic forensic platform functionality, referred to as “calibration,” using controls and standards. In addition, a set of guidelines for documenting validation procedures will be provided.

Additionally, a framework for the acquisition and analysis of digital evidence will be introduced in Section III. Given the considerations noted earlier, our framework will need to be flexible, and to a certain extent, general in nature. This policy will address investigative steps using the following categories, which address the major phases of the digital evidence “life cycle”:

- Acquisition
- Integrity
- Analysis
- Reporting
- Disposal

The analysis of digital evidence will need to be applied to as wide an array of digital devices as possible. For example, digital forensic guidelines cannot be written, with significant specificity, for the analysis of computer hard drives and still be expected to provide adequate guidance on the analysis of PDAs, and/or cell phones. As a result, the analysis guidelines will be written to correspond to abstract “layers” of digital evidence [Carrier 2003]:

---

Aug 2007  PAGE 5 OF 27
The following diagram provides a visual representation of the abstract layers, using a computer hard drive as an example [Carrier 2003].

![Physical Media

<table>
<thead>
<tr>
<th>Physical Media</th>
<th>Media Management</th>
<th>File System</th>
<th>Application</th>
</tr>
</thead>
<tbody>
<tr>
<td>Physical Description</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Head</td>
<td>Cyl</td>
<td>Sectors</td>
<td>Partition Table</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Partition</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>...</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>File</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

(figure 1.)

Framing digital evidence analysis in this manner will allow the analytical process to remain consistent regardless of the device or source of evidence. Further examples of the application of this framework are provided in the “Analysis” section of this document.

II. RECORD KEEPING, VALIDATION AND CALIBRATION OF FORENSIC PLATFORMS

A. Types of Forensic Platforms. As noted in the “Definitions and Terms” section, the term *Forensic Platform* is used to describe any device used for the purpose of acquiring and/or analyzing digital evidence in a forensically sound manner. In an attempt to make record keeping with respect to validation and calibration of forensic platforms more meaningful and manageable, we differentiate between two types of platforms: *primary-use*; and *secondary-use*. Examples of *primary-use* systems include handheld systems such as LogiCube devices, as well as Forensic Towers, MAPS, and Network Monitoring Kits. A *secondary-use* platform could include a laptop or other computer not specifically purchased for exclusive use as a computer forensic platform.

*Primary-use* devices are specifically procured or configured for the collection and/or analysis of digital evidence. Given this fact, it is very helpful to document the configuration and maintenance of a *primary-use* platform in a manner different from
that used to document configuration and calibration information for secondary-use forensic platforms.

In addition to the primary-use and secondary-use platform record keeping practices, we differentiate between single-use and multi-use devices with regard to calibration procedures prior to forensic acquisition. A single-use device is designed for a particular purpose and can be considered self-calibrating. Multi-use devices are designed for a multitude of computing functions, and as such should be properly calibrated prior to use as a digital evidence acquisition device. Note: calibration should not be confused with validation. Calibration is done to help ensure a device is functioning properly in its current configuration. Validation is performed prior to entering a device or certain software into service to help ensure that it performs as expected.

1. **Primary-use Forensic Platform Record Book.**

   a. Each primary-use forensic platform will have a dedicated record book. The cover of the record book should lend itself to accurate and easy association with one specific primary-use platform.

   b. The front of each Forensic Platform record book will be marked conspicuously with:

      o Make and Model
      o Serial Number
      o Serialized equipment accounting tag

   c. The book will contain the following information:

      1) Description, make and model number. Examples of descriptions include:

         o “MAP”.
         o “Silver Tower”.
         o “LogiCube Talon”
         o “Network Monitoring Kit”

      2) Unique Identifying Information.

         o Agency serialized equipment accounting tag
         o Serial Number (if available).
         o Unique Identification Mark (such as etched initials and a date, if a SN or equipment tag is unavailable)

      3) BIOS and/or firmware identification and version.

      4) Current hardware configuration (if applicable).
Motherboard model.

5) Operating System(s) and version(s) (if applicable).

6) The date that the device went into service.

d. In addition to the description and identification information, the record book will be used to track the following events with regard to the pedigree of the device:

   1) Major Operating System (or firmware) updates, to include the date and source of update.

   2) Hardware updates to include each item added or replaced and by whom.

   3) Platform calibration tests, as described below.

e. Entries to the primary-use platform record book will be made as a “running log,” where subsequent additions will be made without spaces and with each entry initialed – similar to the style used in an evidence logbook. Note: Where an action is being taken in conjunction with investigative activity, the case number should be recorded. This is to allow for reviews of Forensic Platform Record Books as required for legal actions, such as appeals, long after the device has been removed from service.

f. When a record book has been filled, it will be closed with an entry that includes the date, name of the examiner and the statement “Record book closed, No Further Entries.” After being closed, the forensic platform record book will be preserved in accordance with Agency guidelines for document retention.

g. A supervisor will review the record books on an annual basis. The record book will be reviewed for proper labeling and content, to ensure that updates have been recorded correctly by comparison to the current configuration of each platform, and for overall legibility.

h. The supervisor review will be noted immediately following the last entry in the record book and will include the statement:

   On [date], I [name] [title] conducted a review of this record book in accordance with [Agency Forensic Procedures reference] and found [no] [the following] discrepancies [note remedy, if applicable]. [signature and date].

2. Secondary-use Forensic Platforms and Record Keeping.
a. As noted earlier, a secondary-use platform offers a great deal of flexibility. While not specifically deployed for primary use as forensic tools, equipment such as laptops can be configured to support a wide range of computing functions, to include evidence acquisition and/or analysis. There may be instances where an agent or examiner will use a laptop to acquire evidence. When such a situation presents itself, a laptop or other electronic device, given proper documentation and procedures, can prove to be an acceptable platform for gathering and/or analyzing evidentiary data.

b. However, unlike in the case of primary-use platforms, the maintenance of platform specific record books for secondary-use platforms would introduce burdensome record keeping requirements of questionable value. Although the maintenance of a record book for secondary-use platforms is not required, there is real value in recording basic information, to include calibration steps, regarding secondary-use platforms prior to using for acquisition and/or analysis of digital evidence.

c. Where applicable, the following information must be recorded by the agent or specialist, when using a secondary-use system to acquire digital evidence. The information should be recorded as working notes that are tied to the investigation being supported.

The working notes will record the following information:

1) Case number of supported investigation
   - If a case number is unavailable, specify the name of the requestor and date of request or “proactive”.

2) Date and initials of agent/specialist

3) Description, make and model number of the acquisition/analysis platform.

4) Unique Identifying Information.
   - Agency serialized equipment accounting tag
   - Serial Number (if available).
   - Unique Identification Mark (such as etched initials and a date, if a SN or Agency equipment tag is unavailable)

5) BIOS and/or firmware identification and version.

6) Operating System(s) and version(s) (if applicable).
7) Description of Configuration used, such as write blockers, imaging software, etc.

- Brief description (written or sketched) of configuration

d. In addition to the description and identification information above, the *working notes* will be used to note applicable platform *calibration tests*, as described below.

B. **Hardware Calibration Using Basic Controls and Standards**. The purpose of calibration is to minimize the risks of failures inherent to all complex systems. With regard to the calibration of forensic hardware and software, those risks largely relate to possible hardware failures, software/firmware bugs, incompatibilities, or the risk the user incorrectly configures a system in such a way as to unintentionally alter results.

*Multi-use* devices, whether *primary* or *secondary* forensic platforms, have been previously defined as devices that, while perhaps used for a specific purpose, are capable of being used for any number of computing tasks. Desktop and laptop computers and forensic workstations are examples of Multi-use devices. As a result of the fact that hardware/software can be added and removed, and updates to operating systems can be made frequently (potentially via automated updates), the proper functioning of these devices with regard to forensic use should be checked through proper calibration.

Each “*working session*” for a given device will require calibration. A new session will have been started under one of the following four circumstances:

- A change in date.
- Acquisition work shifts to support a different investigation.
  - For example, a new working session is started if the agent or analyst acquires a device in support of an investigation, analyzes something else from a different case on that same forensic device, and then resumes imaging in support of the first investigation once again.
- Updates to the Operating System, device firmware or forensic software.
- Previous failure of calibration attempts.
  - Previous failure of calibration” can include a failure to POST correctly. For example, on a single day while imaging five different hard drives, the analyst or agent might swap drives with a reboot in between acquisitions. A session will be considered “over” if a POST fails between reboots. Rebooting to a successful POST immediately following a failure will trigger a requirement to completely re-calibrate,
including the use of the control and standard as discussed below, where applicable.

(Note: the definition of working session does not apply to acquisition hardware/software used for monitoring dynamic user activity, such as the collection of network traffic.)

1. Before beginning an acquisition of digital evidence in any given session, the basic operation of the forensic platform should be calibrated using appropriate controls and standards. Controls can be defined as supplementary procedures set up to allow comparisons. Standards can be described as a sample containing a qualitative or quantitative known.

   a. Hardware calibration will be accomplished using a two-stage process:

      1) By observing and recording a successful system Power On Self Test (POST) or other normal system startup; and

      2) Using the platform to produce a forensic image and verifying the accuracy of that image using standard media in a controlled test,

   Or, in the limited instances of Forensic Platforms used exclusively to acquire live network communications (eg. network monitors);

      3) Using the platform to capture a network session controlled by the tester to ensure the device accurately captures the communications session initiated by the tester³. The tester must use the same protocol(s) used in the network where the monitor will be deployed for evidence capture.

   b. The results of both tests will be documented in the Forensic Platform Record Book (for primary-use devices), or in working notes (for secondary-use devices). Note that the tests need only be performed once per session regardless of the number of reboots, or whenever the agent or analyst begins working on a different case in the same session. (Note: procedures regarding calibration requirements apply if a reboot results in a failed POST as outlined in this document).


   a. The primary purpose of recording the Power On Self Test (POST) prior to using a forensic platform for either analysis or acquisition is to provide

³ Given data traversing via network communications is presented very differently from data on electronic storage media, this procedural exception is intended to provide a relevant test regarding the basic functionality of network monitors prior to their deployment.
documentation of proper “calibration.” For the analysis of digital evidence, a successful POST and a successful completion of the booting process into the operating system should be sufficient to determine that the computer is in proper working order and that it is properly “calibrated” [Barbara 2005].

b. Prior to acquisition, the POST operation will be recorded in the Forensic Platform Record Book. The record will simply include the date and time along with the initials of the examiner recording the POST and the status of the POST (“success” or “fail”).

3. Hardware Calibration: “Controls and Standards”.

a. One of the most basic components of digital evidence examination is the forensic image and its verification. The probative value of analytical results derived from the forensic image is dependent on the accuracy of the image and the ability to show that it is a true representation of the data on the original media. When discussing controls and standards with regard to digital evidence analysis, the most useful “control” would be a set of repeatable steps, utilizing a known “standard” item that confirms consistent imaging and hash verification.

b. Some forensic platforms, particularly hand-held units, are designed for the singular purpose of obtaining an image. These single-use devices are self calibrating and, under nominal conditions, undergo a “benchmark” or self check routine when powered on and need not be further calibrated.

c. Multi-use forensic analysis platforms are based on PC architecture, and while tested and built to rigorous specifications, they are controlled by operating systems and hardware designed for a wide range of functions. As a result of this multi-function design, PC based forensic platforms will be further calibrated using a known standard prepared for the sole purpose of confirming a computer’s capability, in its current configuration, to provide a forensic image of known physical media and a hash for that image [Barbara 2005].

d. For multi-use platforms, specialists and agents will use a set of standard files placed on physical media (for example, a CD-R, floppy disk, USB drive, etc.). The disk image will have known Message Digest (md5) and Secure Hash Algorithm (sha1) signatures. The standard image will be assigned a version number and made available for specialists and agents.

e. When practical, prior to any acquisition using a multi-use platform (forensic tower or mobile analysis platform), the examiner will apply the following procedure:

1) Insert the physical media with the known image (known hash).
2) Produce a hash, ensuring that it matches the known hash.
3) Produce a forensic image (non-specific software).
4) Produce a hash of the resulting image.

The resulting comparison between the hashes obtained in steps 2 and 4 above will be recorded in the Forensic Platform Record Book as “pass” or “fail”, along with the date, time and initials of the specialist or agent. The test image produced in step 3 can then be deleted.

C. Validation. Validation is an important component of computer forensic procedure. When based on sound testing principles, validation is used to demonstrate that tools and techniques are suitable for their intended purpose. Such tools and techniques should be validated or considered reliable by the information technology community prior to their initial use in a forensic process. Again, in keeping with the focus of this document, and the need to prioritize finite resources, validation efforts will center on hardware and software used in the acquisition (as opposed to subsequent analyses) of digital evidence.

According to the Scientific Working Group on Digital Evidence (SWGDE), tools, techniques and procedures that are in widespread use and accepted by the larger information technology community are generally acknowledged as reliable and trustworthy. Consideration may be given to the general acceptance of a tool, technique or procedure in its determination of whether validation is required. [SWGDE 2004]

As has already been established in the Hardware Calibration section, all of our investigative and forensic efforts derive from properly acquired evidence. Given that we rely on our acquisition devices and software to provide the foundation for proper analytical results, we will concentrate our validation efforts on those devices and software that are used for imaging and evidence collection. Often, the agent or examiner will have only one opportunity to accurately acquire evidence.

Software used during the course of an analysis and not during evidence acquisition can be tested for the appropriate functionality by the examiner prior to first use. While we will not exhaustively validate, per the requirements enumerated below, each and every software utility employed during an investigation, care should be taken to cross verify significant results, when feasible, through comparison with the output of a another utility. In other words, if two utilities produce substantively different results regarding the same data, then further evaluation will be necessary to ensure valid analytical results. In some instances, consideration should be given to maintaining specific versions of software used during the analysis for later corroboration of results.

1. Accepted Validation Methods. Validation of forensic hardware and software will be accomplished by one of the following procedures:

   o Internal testing.
   o General community acceptance.
   o Adoption of “trusted” validation by another organization
a. The category “general community acceptance” will be reserved for those devices, programs and utilities in widespread use within the information technology community, and should include hardware and system administration tools and processes commonly used throughout the information technology community. For example, the various common Unix/Linux and Microsoft Windows archive and compression utilities (tar, gzip, Winzip, etc.) are in common use throughout the information technology community, and are also often employed in forensic analysis. The same can be said for common multi media players and some search utilities like UNIX grep. As a result of the fact that these utilities and programs are commonly used and accepted by the general information technology community, they need not be individually tested. Of course, these tools should always be obtained from trusted sources, and significant findings cross verified using other trusted tools when practicable.

b. As one source, the Agency will centrally maintain a list and/or reference of forensic hardware and software that has been properly validated. In those cases where validation has been adopted from another agency, documentation of that process should be referenced where that tool is listed. The list of properly validated software should be maintained in a manner that makes the list readily accessible to agents and analysts in the field.

c. In those cases where circumstances dictate a tool not yet validated is required to complete a task, permission of an Agency supervisor should be obtained. If such permission is not available, and as a result of exigent circumstances an un-validated tool is used in an acquisition, documentation of the circumstance should be included in the Agent's notes. A copy of the tool should, if practicable, be preserved as part of the case file in the event the accuracy of the tool is later challenged.

2. Software Validation. Software validation need only be performed once for each major release of an acquisition tool or utility. Normally the validation of software is concerned with verifying that software does what it is advertised to do. It is not required that validations “grade” software, attempt to reverse engineer the software, or validate every function found within the software. The validation only requires that the software is suitable for its intended purpose without adding, deleting, or altering any evidence. Documentation of the validation process is discussed below.

3. Hardware Validation. Testing and verification should be targeted to the specific task of the tool. For example, while hardware write blockers, used during evidence acquisition, will need to be tested on a variety of interfaces and adaptors, the file systems present on the media used in these tests will be largely unimportant for the purposes of validating the basic functionality of a write blocker. On the other hand, imaging tools will have to be tested with regard to various file systems to ensure they produce accurate forensic images when writing to a given file system. Validation test plans, as described below, should take these details into account.
4. Validation Process. When conducting internal testing and validation of computer forensic hardware and/or software, the following process should be followed [SWGDE 2004]

a. Develop and document a test plan that contains the following:
   
   1) Purpose and scope of the test.
   2) Requirements (what the tool is expected to accomplish).
   3) Methodology (how the test will be conducted).
      
      o Identify support tools.

b. Develop test scenarios

   1) Condition or environment required for the test (hardware and operating system, etc).

   2) Actions that will be performed.

   3) Expected results.

   4) Provide for multiple scenarios to cover configured options or multiple possible environments.

c. Perform test scenarios

   1) Use media or sample materials that are in a known state.

   2) Use test equipment with known configuration corresponding to a known examination requirement.

   3) Document all tests, including re-tests.

   4) Document pass/fail status for each requirement.

   5) Validation results: comparison between actual and expected results.

5. Validation Documentation.

   a. When documenting the results of the validation of computer forensic tools, the following, at a minimum, should be included [NIST 2001]:

      1) A title stating what product was tested.

      2) Identification of the testing environment.
a) Where the tests were run.
b) Supporting hardware and software.

3) Unique identifier for the test report.

4) Name and address of the source or vendor of the product.

5) Identification of the testing or verification software.

6) Unambiguous identification of the product.
   a) Version
   b) Patches

7) Definition of the test and its specific criteria for measurement.

8) Identification of the test report’s author(s).
   a) Name
   b) Job title
   c) Function in the test
   d) Signatures

9) Additional information
   a) Specific to target audience.
   b) Interpretation where required

(10) Detailed results.
   a) In those cases where validation of a forensic tool is being adopted from an external, trusted agency, a copy of the full documentation of that validation should be obtained.

III. FORENSIC ANALYSIS

A. General Guidelines and Policies.

1. Mission Statement. Policies and procedures that establish the parameters for the operation and function of the Agency are derived directly from an understanding of the mission of the Unit [USDOJ 2004].

   The Agency conducts national and international criminal investigations involving information technology matters in which Agency programs, information, and/or personnel are victimized.
The Agency provides digital evidence acquisition and forensic analysis expertise to support the Agency’s overall investigative mission.

Where/When appropriate, the Agency partners with other personnel to report and counter threats to the Agency’s critical information & operations

2. Software licensing:
   a. Given the nature of the Agency’s mission, special consideration should be given to ensure software used is properly licensed.
   b. Agency Headquarters will maintain a repository of licensed software, and a list of licenses or user keys assigned to Agency personnel or field offices.

3. Training:
   a. It is important that Agency computer forensics specialists and agents maintain their skills as competent examiners.
   b. A training plan will be developed and maintained. A record of an individual’s training history, with regard to relevant training, will be recorded in a manner consistent with agency policy and procedures.
   c. Consideration may also be given to mentor programs, on-the-job training, and other forms of career development [USDOJ 2004].

4. Forensic Support Documentation. The following establishes a process for the submission of computer forensic service requests and the intake of accepted requests for examination of digital evidence by Agency personnel:
   a. Where circumstances and time permit, coordination should be made through respective field supervisors. This ensures Agency management is aware of the over all requirements and potential impact on available resources.
   b. If the support is for an upcoming search warrant or other legal process, the Agency will require a copy of the warrant or draft of the warrant. Documentation should specify all Agency responsibilities for before, during, and after the warrant. A written copy of the search plan should be requested if available.
   c. Agency support will require a fully completed request. In accordance with item (1), the support form will be submitted through the respective field supervisor. At a minimum, the Support Request form will have:
      o Signature of the requesting office’s supervisor
Explanation of authority to search electronic media

d. If the forensic analysis is being conducted under the authority of a warrant, then a copy of the warrant will be attached to ensure the agent/examiner clearly understands the parameters of the search.

e. If the forensic analysis is not being conducted under the authority of a warrant (such as in the case of consent of the data user/owner), the agent or examiner will ensure they clearly understand the source and scope of the search authority they are relying upon.

f. Close and continuous communication between the forensic examiner and the requesting agent is vital to ensure the examination is focused and relevant to the underlying investigative effort.

5. Evidence Handling:

a. Digital evidence is fragile and can be altered, damaged or destroyed by improper handling. For this reason, special precautions must be taken to preserve this type of evidence.

b. Digital evidence received or acquired during the conduct of an investigation, or received through a support request should be handled in accordance with the Agency’s Evidence Procedures Chapter. Additionally, digital evidence should not be analyzed, manipulated or stored in a network environment that allows continuous access to other external networks.

c. Given the nature of the Agency’s mission, we regularly seize, store, and process large quantities of sensitive data. These data include information protected under The Privacy Act, as well as Personally Identifying Information (PII). The data may also include proprietary business data, copy write protected intellectual property, as well as known or suspect contraband (child pornography).

d. When required to transmit digital evidence, working copies of digital evidence or forensic work product from or between Agency controlled areas, the following two step analysis should be applied:

1) Refer to applicable Agency regulations regarding the handling of evidence in general, as well as specific procedures and considerations when handling digital evidence. The Agency evidence policy prohibits the shipping of ORIGINAL (or best evidence) digital evidence, without specific approval from a senior supervisor or higher.

2) After ensuring compliance with applicable regulations, the following options are available for transmitting digital evidence, working copies of
digital evidence, or forensic work product while in transit to, from, or between Agency controlled areas:

a) Send only via methods approved for safeguarding US National Security information (SECRET and below), such as via U.S. Postal system using registered mail. The electronic media, in addition to protections outlined in applicable regulations, must be double wrapped and clearly addressed to an approved recipient. The sender, using a separate channel of communication, must ensure the intended recipient is prepared to receive and properly store the data, and request the recipient confirm receipt. The data are not required to be encrypted while in transit when using this method.

b) Encrypt the data using approved encryption means, and ship via approved carriers, such as UPS, FedEx, USPS, etc. The sender, using a separate secure channel of communication, will provide the recipient the encryption key. The key will not be shipped with the encrypted data.

c) Send via secure (encrypted) network communication channel, such as HTTPS, SSH, etc. The sender will first confirm the recipient is prepared to properly receive and store the sensitive data via secure means. When sending via secure network communication protocols the sender will confirm the session is encrypted. Confirmation the session is encrypted can be through the use of features built in to trusted applications, such as the visual confirmation of a closed padlock for HTTPS sessions.

d) Physical Escort - Sensitive electronic data may be transported by Agency personnel when the media is properly protected and in the continuous custody of Agency personnel. Careful thought shall be given when using this means of safeguarding sensitive information. For example, this approach is most practical during relatively short trips, such as during search warrant executions and between Agency controlled areas that are in relatively close geographic proximity.

e) Temporary storage in motels and rental cars may only be authorized by the senior Agency official on-site, and when substantive additional safeguards are in place, such as lock boxes within motel rooms, or lock boxes physically cabled to rental vehicles. This temporary method of storage is sometimes unavoidable given the nature of search warrant executions. Common sense and due diligence are the watch words here.

6. Deviation from these guidelines. All digital evidence examinations are influenced by a wide range of variables. The types of cases and support missions encountered by an examiner will vary greatly. The examiner must consider the
requirements of the mission and the impact of any actions taken. As a result, the examiner may need to adjust to unexpected conditions in the field.

7. **Documentation:**

   a. In addition to the official reporting, the forensic process should be adequately documented in the agent’s or analyst’s case notes. Any substantive actions taken or observations made with regard to the handling or analysis of evidence or work product should be recorded in investigative notes.

   b. Through every phase of the digital evidence “lifecycle,” methods used and especially deviations from these procedures, where required by circumstance, should be adequately documented. This serves to refresh the agent’s or analyst’s memory at a later date should the case become involved in legal or administrative proceedings. Additionally, proper investigative notes provide a reference for other personnel in the event that the original agent or analyst is unavailable.

   c. Investigative notes relating to computer forensic exams should, at a minimum, include the following information on every page:

   o Case Number
   o Date
   o Page number (and total pages)
   o Agent or Analyst Name

   d. When practical, the standard Agency “Investigative Notes” page should be used.

8. **Onsite considerations:**

   a. Collection of digital evidence will require a proper assessment and record of important facts and environment variables. The Agent or examiner should take note of and document the following in case notes [USDOJ 2004]:

   1) Identify the number and type of devices.

   2) Determine if a network is present.

   3) Interview the system administrator and users when appropriate to the investigation.

   4) Identify and document the types and volume of media (including removable media).

   5) Document the location from which the media was removed.
6) Identify offsite storage areas and/or remote computing locations.

7) Identify proprietary software.

8) Evaluate general conditions of the site.

9) Determine the operating system in question.

b. In cases where the agency or examiner is conducting an incident response or is supporting a search, an Agency “Computer Evidence Collection Guide” should be used, when practicable, to record required information and scene specific notes.

c. When available, the “Computer Interview Guideline Collection Sheet” should be used to obtain consistent information when interviewing system administrators and users.

B. Forensic Procedures. This section provides an overview of the “lifecycle” of digital evidence analysis:

- Acquisition
- Integrity
- Analysis
- Reporting
- Disposal

1. Acquisition:

   a. Proper acquisition is the cornerstone of digital forensic investigations. Improperly acquired evidence can lead to the alteration, damage, or destruction of data. Every effort must be made to acquire with minimal invasiveness and impact on the target system.

   b. Documentation of any process used to gather digital evidence must be thorough and provide a detailed description of all steps taken, software used and changes made to any running digital device. It is for this reason that we focus our validation efforts on those hardware and software that are fundamental in the acquisition of digital evidence.

   c. Given the network environment that Agency personnel most often operate in, consideration must be allowed for the fact that the acquisition process normally involves far more that just obtaining a forensic image of a powered-off hard disk drive. The process includes:

      1) Collection of volatile network, memory and system state information (console review).
2) Collection of non-victim server and network appliance logs, to include Intrusion Detection System logs and network streams.

d. The nature of evidence collection in a networked environment is such that it will require an agent or examiner to make minor, unavoidable “changes” to the system in order to obtain a “snapshot” of volatile system state information. This is perfectly acceptable and often necessary, so long as proven techniques are used and the procedures are properly documented through the course of volatile data acquisition.

e. The collection of volatile state data from computer systems and other digital devices will be done in accordance with these guidelines particularly with regard to documentation of steps taken by the analyst and the integrity of evidence or information collected where applicable.

f. Once volatile evidence has been considered and obtained where available, persistent data (evidence) will be acquired using the following general procedural guidelines:

   1) Identify and document digital devices that need to be acquired and document hardware configuration and physical properties. Where practical, use the standard Agency Evidence Collection Worksheet to ensure uniform collection of information.

   2) Correlate system time on the device being acquired with a known time source.

   3) Every reasonable effort should be taken to minimize modifications to the system, especially prior to any forensic acquisition. Where feasible, a write blocker should be employed.

   4) Evidentiary logs and other logical digital evidence (files and file listings, etc.) should be handled in the same manner as a forensic image, especially with regard to integrity checking.

2. **Integrity:**

   a. All digital evidence received or directly acquired by examiners or agents, should maintain consistent integrity checks throughout the investigative process. This is most often accomplished using a “hash” algorithm. Agents and specialists will use a message digest version 5 (MD5) 128-bit or SHA1 hash algorithm.

   b. Prior to conducting a forensic acquisition, a hash function should be used on the original media prior to obtaining an image when possible. Immediately following the acquisition, an additional hash of the image should be recorded
and compared to validate the acquisition. This can be accomplished manually or through an automated function of the acquisition software or device.4

c. Through all phases of the investigation, working copies of evidence should be checked for integrity prior to analysis. The agent or examiner’s investigative notes should reflect the results of these integrity checks.

d. Integrity checks should be performed whenever there is a reasonable argument to be made that digital evidence, or working copies of digital evidence, were potentially altered. This is most common where the forensic image or products of an analysis are moved or copied from one volume to another or across a network connection. As a result, the examiner should re-verify the integrity of digital evidence (and working copies):

1) When moving digital evidence, or working copies, across a network (for example, from an evidentiary RAID to local forensic workstation)

2) When copying digital evidence to another file system or to another volume on a local machine.

3) When files or logical objects of evidentiary value have been extracted or identified within digital evidence.

4) At any other time where the agent or analyst feels the integrity of the evidence might reasonably come into question.

3. Analysis:

a. Analysis of digital evidence should be conducted on working copies of evidentiary data. Analysis using the original media (or best evidence) should only be undertaken when all other practical alternatives have been exhausted. Given the variety of digital equipment that may be encountered when conducting an investigation, the analysis guidelines are presented as abstract “layers” of digital evidence [Carrier 2003] (note: figure 1.):

   - Physical (identification)
   - Media Management (data storage areas)
   - File system (data organization)
   - Application (logical analysis - contextual and temporal investigation)

b. The framework outlined below is general enough to cover a very broad range of digital devices. It provides guidance on the analytical process and reporting of findings.

4 Agents and specialists should be fully aware of the process used to verify the integrity of acquired images. If verification is done concurrently with acquisition, ensure that the images on disk are also verified.
1) Physical

This layer applies to any physical item that can be seen or held. It can apply to computer systems, removable media, removed hard disk drives, cell phones, PDA’s, Cameras, etc.

- Device description
- Manufacturer
- Model
- Serial number
- Property control number, or other unique identifier (NEMS)

2) Media Management

This layer applies to the data storage capabilities of the device.

- Size of available storage
- Number of storage volumes on the device
- Type of storage volume (RAM, ROM, DOS partitions, ext3, etc)
- Record the partition or volume table or map.
- Correlate number and size of volumes with available storage.

  a) For example, does the number and size of total user accessible storage volumes match the total number of sectors (HPA/DCO identification)?

  b) Are there deleted partitions or storage volumes?

3) File System

A file system describes the way files or other data records are stored on a disk. File systems are most commonly managed by a computer operating system.

- Type
- Label
- Size
- Allocated block size
- Version

4) Application

Analysis at this layer is completely dependant upon the supporting facts and focus of investigation, support request and type of device being
analyzed. The following should be identified and reported, as applicable:

- Operating system and version, and/or firmware for some electronic storage devices.
- Common operating system configuration settings (time zone, account identification, etc.). This will largely depend on the needs of the investigation.
- Identification of extracted data.
- Meta-data (ownership, time stamps, etc).
- Hashes.

4. Reporting:

a. When reporting the results of a forensic analysis, the following outline will be observed in order to provide a complete report.

b. All digital forensic activity should be reported using the standardized Agency report format. Additional content for forensic activity will include the following:

1) Context: Includes background and general information on the case.
   a) Analysis overview.
   b) Suspected role of the system being examined.

2) Scope
   a) Underlying search authority.
   b) Specific parameters requested by case agent (if any).
   c) Items analyzed.
      - Particularly identify items examined or acquired.
      - System clock, time zone settings.
      - System overview (operating system, volume identification, etc.).
   d) General procedures followed.

3) Findings
a) A summary of findings is provided in the cover report. The summary should, within both the context of the underlying investigation and the scope of the forensic exam, provide the requestor a succinct description of what potentially relevant (either incriminating or exculpatory) data was discovered.

b) Detailed findings, to include complete evidentiary files (when possible), will be noted and attached on additional electronic media, at the discretion of the agent/analyst or field supervisor.

c) Special care will be given to suspected or confirmed contraband material (eg. child pornographic images) in forensic reports. Evidence or reports containing known or suspected child pornography should be clearly labeled as such:

   “Warning: Contains Objectionable Material Handle as Contraband”

d) Agents and examiners will ensure technical reports are written with the target audience in mind. In those cases where technical material is included and definitions are not clear, terms should be defined. When the number of definitions is excessive, a glossary of terms should be included at the end of the report, after the attachments.

e) All forensic reports and substantive notes made through the course of the analysis must be provided to the supported case agent for inclusion in the case file of record.

5. Disposal:

a. Digital evidence seized or obtained through the course of any investigation or support activity will be disposed per the requirements set forth by Agency policy regarding evidence disposition.

b. Questions regarding the return or disposal of digital evidence containing contraband, offensive materials, or questioned intellectual property should be directed toward the prosecuting attorney, Agency counsel, and/or field supervisor.
IV. REFERENCES


John Barbara: ASCLD/LAB Digital Evidence Accreditation, Forensic Magazine, February 2005
