

DRAFT

DRAFT

DRAFT

DRAFT

REVISED DRAFT

A Guide for Planning and Implementing a Computer Forensics Unit

National Center for Forensic Science

The National Institute of Justice

Revised April 2006

Contents

About This Report 3-5

Guide Overview..... 6-7

Section I. Planning8

Section II. Design 9-14

Section III. Computer Forensic Equipment..... 15-20

Appendices

Appendix 1. Resources and Links22

Appendix 2. Customer Needs Assessment Sample 23-31

Appendix 3. Sample Feasibility Study.....32

Appendix 4. Memorandum of Agreement (MOA) Template..... 33-34

Appendix 5. Sample Facility Manual..... 35-44

Appendix 6.A-E. Sample Floor and Workstation Plans 45-49

About This Report

This document is a guide to the planning, construction and equipping of a computer forensic facility. It is a guide and does not set forth requirements. It is a framework, which is both flexible and incorporates the experience of successful law enforcement agencies and forensic laboratories.

The tremendous growth in digital evidence has driven a requirement for virtually all law enforcement agencies to have access to digital forensic capabilities. Each agency must decide how it wishes to provide access to these services.

Agencies may wish to do either a formal or an informal needs assessment. However, it is important to understand that many potential users of forensic services may not recognize the existent caseload. Historically, the need for digital evidence examination has been consistently underestimated.

The authors of this guide recognize that each agency faces a unique set of circumstances with regard to space, facilities, personnel, caseload, violations, organizational structure, and budget. It is understood that agencies will have to balance the available resources along with the recommended practices contained in this document.

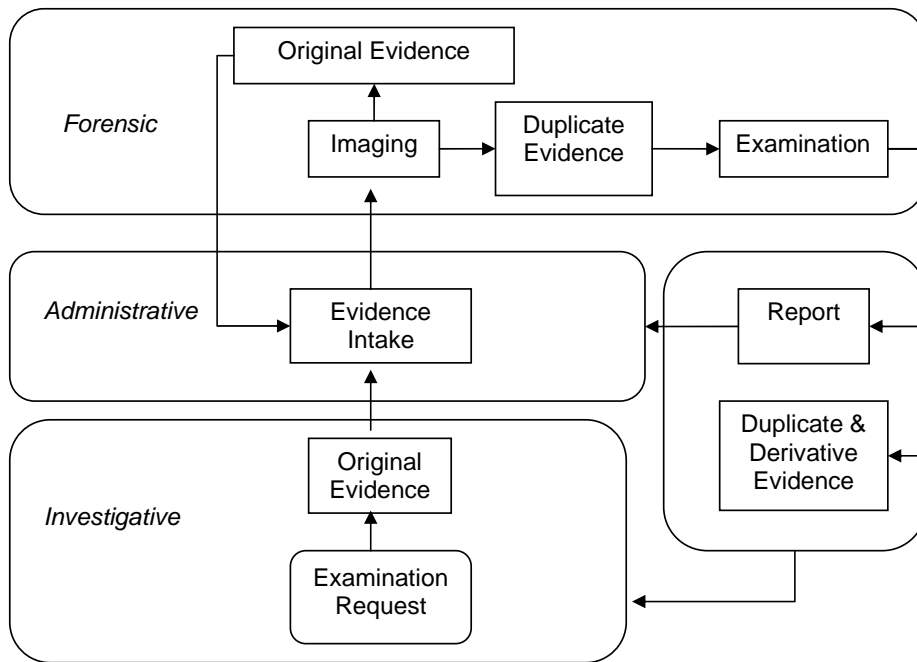
Who should read this report?

This guide was designed for executives, managers, and supervisors who are considering the construction or the expansion of an existing facility for a computer forensic unit.

The tremendous growth in digital evidence has driven a requirement for virtually all law enforcement agencies to have access to digital forensic capabilities. Each agency must decide how it wishes to provide access to these services.

Workflow issues

While each organization will have particular circumstances with respect to its facility, there is a basic set of business processes that have demonstrated themselves in forensic units around the world. These core processes are the investigative, administrative and examination. In most forensic settings, it is the investigators who typically seize evidence, which is submitted for examination. There are administrative requirements by which the evidence control, examination and subsequent reporting process must be documented and of course, the forensic examination itself. This process is depicted in the following diagram:



In this diagram, we see that the investigator submits the evidence, along with a document requesting the examination. Often a copy of the legal authority, such as a copy of the search warrant, is attached. The forensic unit then logs the evidence into the evidence control system or laboratory information management system (LIMS). The forensic examiner then logs the evidence out, duplicates it, returns the original to evidence, conducts the appropriate examinations on the duplicate evidence, and produces two types of product: a laboratory report and derivative evidence, which consists of electronic copies of media, files, or content. A copy of the report is submitted to the administrative system. The original evidence, the report, and derivative evidence is provided to the contributing agency.

In designing the specific processes for a computer forensics unit regarding its evidence handling and administrative processing, care should be taken to ensure that there is no opportunity for cross-contamination. Information systems used for investigative duties, such as investigative report writing, investigative analysis, and undercover activities must not be used for the administrative or examination portions of the forensic process. Therefore, the administrative, forensic, and investigative systems and networks must be separated.

The design of any forensic unit should take workflow into consideration in order to make effective use of available resources.

Organizational Structures

In designing the forensic unit, there are generally four types of organizational structures. These organizational structures have an impact on the design and operation of the unit. Each type of structure has issues, which need to be taken into account in the design of the unit.

Single Practitioner – Dual Role

In this model, a single law enforcement officer acts as both the investigator and the forensic examiner. This is a very common practice, especially in smaller organizations. This is also the most challenging from a design perspective. As described above, there needs to be a clear separation of the functions and documentation. A single forensic or administrative error could contaminate a number of forensic or investigative cases. Use of designated areas for the different functions, separate computers, and/or networks coupled with rigorous adherence to strong policies will do much to minimize the challenges in this organizational structure.

Single Practitioner – Forensic Role

In this structure, the potential for investigative contamination is greatly reduced. Because the practitioner has to serve in both the administrative and examination roles, designated areas, computers/systems, and policies are needed to minimize the potential for contamination.

Multiple Practitioners – Dual Role

Many of the problems associated with the single practitioner–dual role organization can be further exacerbated when there are multiple practitioners. Organizing the available space and resources by tasks and implementing strong investigative, administrative and examination policies can minimize contamination.

Multiple Practitioners – Forensic Role

This model matches the traditional forensic laboratory model. There is a well-established body of knowledge, which can be used to design the most effective unit. The DOJ guide *Forensic Laboratories: Handbook for Facility Planning, Design, Construction, and Moving* can provide much useful information.

Guide Overview

This guide is intended to assist with planning and implementation of a computer forensic unit. This guide does not provide a detailed explanation of the design, construction, and moving of such a facility. These topics are covered in depth in the DOJ document *Forensic Laboratories: Handbook for Facility Planning, Design, Construction, and Moving*. Rather, this guide is intended to point out special concerns related to a computer forensics unit that are not addressed in the aforementioned DOJ document. It should be noted that due to the continuing rapid advancements of technology, the above referenced document should be viewed in light of current technology.

The creation of a new computer forensic unit could involve any of the following steps:

- Planning
- Design
- Computer Forensic Equipment

Formatted: Bullets and Numbering

Specific activities vary within each phase of the process, and each phase is addressed in detail in the following pages. Throughout the process, ensure that careful planning and effective communication occurs among all involved parties.

Note: It is strongly recommended that the computer forensic examiners and their managers who will occupy the unit participate in its planning, design, and equipping.

I. Planning

A strategic plan for the creation of a computer forensic unit relies on the following considerations:

- Customer needs – the unit must identify the types of examinations and the volume of work required by their customers.
- Services provided – the unit must clearly state the types of examination and support services that will be provided to prevent unfulfilled expectations
- Business plan – the unit must have a strategic plan to provide for continued provision of services, staffing and fiscal support

II. Design

The facility design will vary according to each unit's specific needs. Facilities should be designed with the flexibility to change with the evolving needs of their occupants, available technologies, and improved scientific methodologies.

<p>Note: A phased implementation plan for the construction, moving, staffing, and equipping of the unit is recommended.</p>
--

III. Computer Forensic Equipment

Equipping and maintaining a computer forensic unit is a major financial investment. Determining what is needed and when to replace it are critical for determining costs.

It is not only initially expensive to establish a computer forensic unit, but the ongoing operational costs, as well as maintenance and upgrade, will require the commitment of substantial financial resources for as long as the unit remains in existence. Creating a budget line item for this unit will help to ensure its long-term effectiveness.

Section I. Planning

Detailed planning helps ensure the computer forensic unit's success. Involve appropriate personnel, including unit staff, throughout the entire process to help minimize concerns and problems before they arise.

A. Customer Needs

A customer needs assessment can be used to evaluate current and anticipated operations. Involving potential clients will increase support for the creation of the unit. See Appendix 2 for additional considerations. However, the following represents the principle steps:

1. Identify internal and external customer needs
2. Determine current capabilities
3. Identify the extent of outsourcing required
4. Evaluate crime trends involving digital evidence

Note: Consider how digital evidence can be associated with any type of crime. See the NIJ publication *Electronic Crime Scene Investigation: A Guide for First Responders*, Chapter 7, "Forensic Examination by Crime Category".

B. Services provided

Determine the specific services that the unit will provide. These may include crime scene search and seizure, computer forensic examination/analysis, and courtroom testimony.

Experience has shown that computer forensic units provide two types of service: investigative support services and forensic examinations

Investigative support services may include consultation on computer related investigative matters, assistance with drafting legal documentation to include search warrants and affidavits, consultation on investigative strategies, etc.

Forensic examination services may include onsite investigative support and the specific types of evidentiary examinations that may be performed. It should be clearly stated if examinations services will include computers, cell phones, PDAs, audio or video imaging analysis, etc.

Section II. Design

Because situations will differ according to the needs of users, there is no universally correct plan for establishing a computer forensic unit or for renovating existing space. A number of functional elements will determine a unit's architectural and engineering design.

Flexibility is of major importance in a computer forensic unit's design and configuration, as it supports adaptability. For example, it enables a unit to alter existing floor plans or to add new buildings, rooms, and equipment to meet the changing needs of its occupants. As science and technology evolve, a computer forensic unit risks falling into obsolescence if it is unable to meet future challenges (i.e., projected long-term growth).

Other design-related elements that need to be addressed include site dimensions and elevation, access, critical adjacencies of functional areas, state and local building codes, access and proximity to parking areas, high-speed and secure telecommunications. In addition, the design team is expected to work closely with the individuals who will ultimately use the unit. Here is an example:

A Specific Considerations: Computer Forensics Unit

1. There are two fundamental requirements for an examiner's workspace. These include:
 - a. Design workstations to minimize the exposure of highly sensitive materials (e.g., place computer monitors displaying sensitive information in such a way that only the case examiner can view it).
 - b. Such physical security for each work area that the integrity of the evidence will be preserved. This may be accomplished in a variety of ways. Two examples might be limiting the access to a restricted area by authorized personnel or providing secure space to be used for unattended, after-hours processing of large amounts of data.

Note: Functional areas may be separate or combined depending on the needs of the unit. If combined, then security and evidence authentication issues must be addressed.

2. There are three functional areas for a computer evidence examiner. The recommended examination space includes both area (square feet) and the linear bench dimensions (linear feet). The suggestions regarding the linear bench space recognizes that the forensic examination of computers and other digital

evidence requires a great deal of horizontal space to accommodate numerous computers and peripherals.

Note: These are recommended requirements for space.
--

- a. It is recommended that the workstation space for each examiner measures a minimum of 7.63 linear m/25 linear ft (e.g., a U-shape or a square with one side open).
 - b. It is recommended that the multipurpose work area within the computer evidence examination area measures 1.53 linear m/5 linear ft per examiner, or a minimum of 7.63 linear m/25 linear ft, whichever is greater. "Multipurpose" includes specialty hardware shared among other examiners.
 - c. It is recommended that the administrative workstation space for each examiner measures a minimum of 2.44 linear m/8 linear ft. This space should be designed to accommodate a wide range of functions, which can include reviewing investigative data, conducting literature searches, writing reports, and preparing for court testimony. Adequate distance must separate the administrative work station from forensic work stations to eliminate the possibility of evidence processing on administrative stations.
3. Experience has shown that a separate digital imaging area provides efficiency and ensures evidence authenticity.
- a. It is recommended that this area measures 1.53 linear m/5 linear ft per examiner or a minimum of 7.63 linear m/25 linear ft, whichever is greater.
 - b. This area, depending on staffing, space, and critical adjacencies, may be incorporated into an examiner's work area.
4. The examination of digital evidence requires a practical digital evidence storage area.
- a. It is recommended that this room provides 110 ft²/6.97 m² for each examiner or a minimum of 220 ft²/13.94 m² for the facility.
 - b. Make controlled access an integral part of the security/access control system.
 - c. Evidence storage must have sufficient electrical power to preserve volatile digital evidence.

d. Consider adjustable shelving to accommodate a variety of differently sized evidence.

5. Consider additional space requirements for the following:

- a) Fire-rated ventilated storage rooms, or ventilated flame-proof storage cabinets.
- b) Short- and long-term evidence storage.
- c) Archival storage (off- or onsite).
- d) Dedicated server(s) for digital evidence and administrative storage.

Note: Isolate the evidence-processing computer from non-forensic systems to prevent the contamination of evidence. Use the administrative computer for report preparation and various administrative functions.

B Specific Considerations: Administrative Area

1. General storage area (for related supplies or archived equipment)

- a. Provide 50 ft²/4.62 m² for each analyst (or a minimum room size of 100 ft²/9.24 m²).
- b. Provide adjustable shelving to accommodate a variety of computer equipment and supplies.

2. Network room with restrictive access to designated personnel. Connectivity between the following networks should be in accordance with agency policy.

- a. Provide a minimum of 100 ft²/9.24m² to accommodate the different network systems that may be required at the facility, such as:
 - 1) Commercial Internet.

Note: It is *strongly* recommended that the forensic network not have Internet access.

- 2) Agency network.

- 3) Laboratory information management system.
- 4) Telecommunication system.
- 5) Covert network and communications

Note: The forensic network should be located in a secure area with restrictive access to designated personnel
--

3. Conference room/case presentation room.

It is recommended that adequate space (a minimum of 2.32² m/25² ft per person) be designated for the review and presentation of digital evidence, and that this space be located outside of evidence controlled areas.

4. Administrative offices/areas.

a. Provide staff with private offices to discuss personnel and sensitive case issues.

- 1) It is recommended that managers' offices are 200 ft²/18.58 m² (or designed according to specific agency space requirements).
- 2) It is recommended that supervisors' offices are 150 ft²/13.94 m² (or designed according to specific agency space requirements).
- 3) It is recommended that the administrative offices/areas are 100 ft²/9.24 m² per staff member (or designed according to specific agency space requirements).
- 4) Include voice and data access in each office or area.

5. Evidence intake and return.

- a. Evidence receiving and return counter to and from contributors.
- b. After-hours secure evidence lockers in accordance with agency policy.
- c. Evidence disbursal and return counter to and from examiners.
- d. Evidence custodian workstations (minimum 64 ft²/5.95 m²).

- e. Evidence supervisor's office (minimum 120 ft.²/11.48 m²).
- f. Evidence storage.
- g. Mailroom for packing, sending, and receiving evidence.
- h. Appropriate connectivity to administrative and laboratory information systems
- i. Adequate storage space for evidence packing supplies

6. Training.

Experience has demonstrated the value of having a training facility located within a digital evidence facility for both internal examiner and customer training.

- a. Classrooms.
- b. Audiovisual media rooms.
- c. Storage for training aids.
- d. Mock crime scene rooms (if applicable).
- e. Training facility.
- f. Video conferencing.
- g. Computer and television networking.

8. Administrative support area.

- a. Clerical, administrative, and case support staff.
- b. Active and archive case files (in accordance with agency policy).
- c. Mail, photocopy, printers, and facsimile equipment.
- d. Laboratory information system and telecommunications equipment space

9. Reference library / shared server for electronic documents.

Due to the evolving nature of the technology, examiners require current and legacy reference materials to conduct examinations effectively and to maintain proficiency

- a. Book/CD-ROM stacks.
- b. Periodical shelves.
- c. Research and reading workspace.
- d. Computer information workstations with Internet connectivity.

Note: The following applies to units, which conduct investigations in addition to forensic examinations.

C. Investigative Area

1. Field response area.
 - a. Equipment storage.
 - b. Staging area.
2. Undercover operations
3. Long-term Physical Evidence Storage
4. Investigative Work area

Section III. Computer Forensic Equipment

A computer forensic unit's equipment and networks are as important as the unit's plan, design, and construction. Unlike building and design elements, every aspect of a unit's equipment is susceptible to rapid technological advances, which often render the most advanced technology obsolete within a few years of installation.

Capital planning needs to take into account that budgets should reflect the need for more frequent equipment upgrade or replacement. Generally, most forensic equipment is obsolete within three years. Some hardware and software require annual refreshment. Timely replacement/upgrade of equipment will allow the unit to remain current with respect to technological advances and maintain the efficiency of its forensic examiners.

The following is a generic list of equipment that might be required in a computer forensic unit. Although the list is not all-inclusive, it provides ideas for what types of equipment might be needed when planning or renovating a site. These recommendations are based on current practice at the time of this guide's publication.

A. Unit Equipment

1. Evidence processing computer.
 - a. Flat screen monitor.
 - b. Uninterruptible power supply (UPS).
 - c. The maximum amount of memory that can be supported by the forensic computer.
 - d. Hard drives of various capacities and interfaces— IDE (Integrated Drive Electronics), SATA (Serial Advanced Technology Attachment), SCSI (Small Computer System Interface)—with a capacity sufficient to support the unit's operations.
 - e. Removable drive trays.
 - f. Sound card.
 - g. Speakers and headphones.
 - h. Tape drive.
 - i. Recordable CD/DVD drive.

- j. Non-recordable CD/DVD drive.
- k. Personal Computer Memory Card International Association (PCMCIA) reader.
- l. Printer.
- m. Memory card readers (multiple formats).
- n. 1.8" and 2.5" to 3.5" hard drive adapter.
- o. External drive bays (read-write and write-block)
- p. SCSI cables, terminators, and adapters.
- q. SCSI controllers.
- r. SATA Controllers
- s. Computer toolkit.
- t. IEEE 1394 fire wire controller.
- u. USB 2.0 Controller.
- v. Universal Serial Bus (USB) hub.
- w. Hardware write blocking devices.
- x. KVM (Keyboard Video Mouse) switches (control box for multiple central processing unit/CPU usage).
- y. Legacy devices

Note: Older computer equipment and peripherals may not be compatible with computers in current use. Therefore, it is often necessary to have available obsolete equipment in order to examine properly these devices. These obsolete devices are referred to as "legacy devices" and should be maintained in order to conduct examinations on both submitted evidence and re-examination of previous submissions.

- 2. Additional hardware (dependent upon the services provided by the facility).
 - a. Forensic network with large, fast storage area for evidence files.

- b. Network server (for network services, file sharing, printing, and storage space).
- c. Laptop computer with docking station.
- d. PDA (Personal Digital Assistant)
- e. Legacy storage devices
- f. Hard drive duplicator.
- g. Networked black-and-white/color printer (one per five examiners).
- h. Networked high-speed and high-quality printer (one per five examiners).
- i. Scanner.
- j. Network routers, hubs, and switches.
- k. Network cards.
- l. Digital camera.
- m. Tape drives (multiple formats).
- n. CD duplicator.
- o. Shredder.
- p. Disintegrator (for CDs, floppy diskettes, video cassettes).¹

3. Software.

Note: Forensic software and applications utilized by the unit should be operated in compliance with appropriate licenses.

- a. Imaging
 - 1) Duplication software.
 - a) Physical/sector level.

¹ High-end equipment.

- b) Partition copy.
 - c) Logical/file copy.
 - d) Backup software.
- b. Examination software tools.
- 1) File header.
 - 2) Text.
 - 3) HEX (Hexadecimal) Viewer
 - 4) Deleted file recovery software.
 - 5) Compression and encryption software.
 - 6) Decompression and decryption software.
 - 7) Partition viewers.
 - 8) Hashing tools.
 - 9) Cataloging software.
 - 10) Wiping software.
 - 11) CMOS (Complimentary Metal Oxide Semiconductor) capturing.
 - 12) Antivirus and spyware software.
 - 13) Steganography and encryption detection.
- c. Additional software (sufficient licenses for the following applications software should be available for forensic, investigative, and administrative purposes)
- 1) Application software.
 - a) Word processing.
 - b) Spreadsheet.
 - c) Presentation.

- d) Database.
 - e) Browser.
- 2) Viewing software.
- a) Graphics.
 - b) Text.
 - c) Multi-format.
 - d) Multimedia.
 - e) Operating systems.
- 3) General facility software.
- a. Miscellaneous processing and application software.
 - b. Maintenance library software (for cataloging older software and operating systems).
4. Field response equipment (the following list of equipment provides suggestions for analysts who are required to secure onsite computer evidence. The recommended equipment includes):
- a. Hard drives and media.
 - b. Portable evidence processing computer.
 - c. Laptop.
 - d. Storage devices (e.g., tape drive).
 - e. Equipment travel cases.
 - f. Packaging material (bubble wrap, boxes).
 - g. Toolkit.
 - h. Accessories (e.g., NIC [Ethernet], SCSI controller, cables, adapters, terminators, USB devices, Fire Wire, crossover cables, hub).

- i. Portable printer.
 - j. Hardware write blocking devices.
 - k. Drive duplicator.
 - l. Crime scene processing supplies (e.g., labels, bags, evidence tape, latex gloves, flashlights).
 - m. Camera.
 - n. Cell phone.
 - o. Video recorder.
 - p. Software (e.g., acquisition, viewing, searching, device driver, password crackers).
 - q. Dollies and carts.
5. Expendables.
- a. Media (e.g., hard drives, DVDs, tapes, CDs, floppies).
 - b. Packaging materials (e.g., bubble wrap, boxes, heat sealer, non-static plastic bags, etc.).
6. Network components
- It may be necessary to create a network environment in connection with forensic examinations or investigative analysis. Sufficient hardware and software should be available to meet reasonably anticipated needs.

Appendices

Appendix 1. Resources and Links22

Appendix 2. Customer Needs Assessment Sample Questionnaire 23-31

Appendix 3. Sample Feasibility Study.....32

Appendix 4. Memorandum of Agreement (MOA) Template 33-34

Appendix 5. Sample Facility Manual..... 35-44

Appendix 6.A-E. Sample Floor and Workstation Plans 45-49

Appendix 1. Resources and Links
--

American Academy of Forensic Sciences (www.aafs.org)

American Society of Crime Laboratory Directors/Laboratory Accreditation Board
(<http://ascl-d-lab.org/>)

Federal Bureau of Investigation (<http://www.fbi.gov/>)

High Tech Crime Task Forces (<http://www.hightechcrimecops.org/links.htm>)

High Technology Crime Investigation Association (HTCIA) (<http://htcia.org/>)

The International Organization on Computer Evidence (<http://www.ioce.org/>)

The International Association of Computer Investigative Specialists
(<http://www.cops.org/>)

Los Alamos Laboratory (<http://www.lanl.gov/worldview/>)

National Center for Forensic Science (<http://www.ncfs.org>)

National Institute of Standards and Technology, Office of Law Enforcement Standards
(<http://www.eeel.nist.gov/oles/>)

National Law Enforcement and Corrections Technology Center (NLECTC) Regional
Centers (<http://www.oletc.org/regional.asp>)

National White Collar Crime Center (www.nw3c.org).

Regional Computer Forensic Laboratories (<http://www.rcfl.gov/>)

Scientific Working Group on Digital Evidence (<http://www.swgde.org/>)

U.S. Department of Defense Computer Forensic Laboratory (<http://www.dcfll.gov/>)

U. S. Drug Enforcement Administration, *Microgram Bulletins*, "Computer Corner"
(<http://www.dea.gov/programs/forensicsci/microgram/index.html>)

Appendix 2. Customer Needs Assessment Sample

The Customer Needs Assessment is used to quantify and evaluate current operations and to predict the facility's proposed operations and future mission. This assessment demands full user, client, and agency participation; justifies the proposed facility's cost and size; and resolves issues related to renovation and expansion. The following are merely suggestions for possible areas of assessment:

- A. Identify internal and external customers and the needs of each.
 1. Identify the needs of internal staff / customers of the proposed facility.
 2. Determine the needs / requirements of potential external customers of the proposed facility, which may include:
 - a. Local, State, and Federal law enforcement offices.
 - b. Other crime laboratories.
 - c. Prosecutors' offices.
 - d. Public defenders' offices.
 3. Determine the existing computer forensic needs of the customers by using the following:
 - a. Caseload.
 - 1) Distribution by types of offense.
 - 2) Number of offenses where computer evidence was involved.
 - b. Use of outsourcing.
 - c. Current internal computer forensic capabilities.

B. Crime trends

A customer needs assessment may include trends in crimes that yield digital evidence. Such crimes include:

1. Terrorism

Formatted: No bullets or numbering

2. Child exploitation
3. Identity fraud
4. Violent crime
5. Drug trafficking
6. Network intrusion
7. White-collar crime
8. Organized crime and gang activity

C. Feasibility study

The feasibility study (see Appendix 3, "Sample Feasibility Study") may include the following:

1. Conducting a risk analysis to determine the consequences of not proceeding; consider the following topics:
 - a. Court challenges resulting in dismissed cases.
 - b. Civil/personal liability.
 - c. Increased crime, resulting in the following:
 - 1) Increased prison population.
 - 2) Community outrage.
 - 3) Negative economic impact.
 - 4) Political ramifications.
 - d. Inability to exonerate the innocent or implicate the guilty.
 - e. Inability to protect your population
 - f. Inability to discover relevant evidence.
 - g. Outsourcing costs.

h. Unqualified examiners.

2. Determine options. These may include:

- a. Establishing partnerships with customers and counterparts (local and regional).
- b. Outsourcing to private facilities.
- c. Not proceeding and accepting the resulting consequences.

Note: If the customer needs assessment and the feasibility study justify the creation of a unit, the next step is drafting a business plan.

D. Business plan

A well-developed business plan is an important element in the development of a computer forensics unit. The following outline offers guidance for formulating a business plan:

1. Preparing the business plan

Note: Information necessary to complete portions of the business plan can be obtained from the customer needs assessment, the feasibility study, and existing organizational policies.

a. Introduction.

- 1) State the mission.
- 2) Identify measurable and attainable objectives.

b. Background.

- 1) Describe the state of computer forensics from Local, State, and Federal perspectives.
- 2) Describe the current capabilities of the organization (if any).

- 3) Describe national and local crime trends, which are impacted by computer forensics.

c. Organization and structure.

- 1) Include a proposed organizational structure that shows where the unit resides within the chain of command.
- 2) Include a proposed unit organizational structure.
- 3) Prepare a personnel management plan.
- 4) Establish written policies and procedures that may address:
 - a) Job descriptions that result in a defined career path.
 - b) Vacancy announcements.
 - c) Recruitment
 - d) Hiring procedures to include skills testing of applicants
 - e) Training.
 - f) Competency and proficiency testing.
 - g) Performance evaluations.
 - h) Retention and career ladder.

Note: Because computer forensic positions are unique, new job descriptions may need to be created.

d. Customer base.

Identify current and potential customers such as:

- 1) Local, State, and Federal law enforcement agencies.
- 2) Prosecutors.
- 3) Defense attorneys.

e. Outreach.

Identify relationships that may be established with external organizations such as:

- 1) Local, State, and Federal agencies.
- 2) Industry.
- 3) Academia.
- 4) Professional organizations and affiliates (see Appendix 1, "Resources and Links", for a list).

Note: These relationships may require a general memorandum of understanding (MOU) or a more specific Memorandum of Understanding (MOU) (see Appendix 4, "Memorandum of Understanding [MOU] Template").

f. Functions and services.

- 1) Describe the proposed functions and services the unit will offer. Some of these functions may include:
 - a) Crime scene search and seizure.
 - b) Field support.
 - c) Data recovery.
 - d) Computer forensic examination.
 - e) Investigative analysis.
 - f) Court testimony.
 - g) Consultative support.
- 2) Describe the unit's case acceptance policy (see Appendix 5, "Case Acceptance Policy").

g. Budget.

1) Determine startup and recurring expenditures.

- a) Facility.
- b) Personnel.
- c) Training and certification

<p>Note: The initial and recurrent training costs for forensic examiners is substantial. Failure to provide adequate, recurrent training will negate the investment in the initial training and severely affect the forensic examiner's ability to conduct computer casework.</p>
--

- d) Professional organization membership dues
- e) Equipment and supplies.
- f) Equipment service contracts.
- g) Software licenses renewals/upgrades.

2) Identify potential funding sources.

- a) Internal agency funding.
- b) Pooled funds from regional agencies.
- c) Redeployed funds (from canceled programs).
- d) Forfeiture funds.
- e) Grants.
- f) Government agencies.
- g) Fee-for-service charges.
- h) Legislative appropriations.
- i) Municipal bonds.

j) Private foundations.

k) Other.

h. Logistics.

Describe the procedures for integrating the unit into the existing infrastructure. Issues may include:

- 1) Supply/procurement.
- 2) Facility management.
- 3) Employee services
- 4) Book and software library.
- 5) Shipping and receiving.
- 6) Vehicle, equipment, and computer-related maintenance.
- 7) Equipment and supply inventory management.
- 8) Internet, intranet, extranet, and Web site.

i. Security plan.

Describe the policies to address security in the following areas:

- 1) Physical facility.
- 2) Evidence.
- 3) Documents (e.g., files, archives).
- 4) Personnel.
- 5) Information technology resources and infrastructure.

j. Quality assurance program.

Describe a quality assurance program that satisfies the needs of the organization as it relates to best practices. See Appendix 5 of this document or the ASCLD/LAB Accreditation Manual.

Note: Accreditation provides an independent assessment of the quality assurance program, including conformance with industry standards for professional knowledge, skills, and abilities.

k. Communication and information management systems.

Describe the various communication systems required at the proposed facility, which may include:

- 1) Telephone and facsimile communications.
- 2) Computer networks – wired and wireless.
 - a) Agency network.
 - b) Isolated computer forensics examination network.
 - c) Isolated covert network (if appropriate to unit mission).
- 3) Evidence tracking network.
- 4) Management information system (MIS) or laboratory information management system (LIMS).
- 5) Commercial Internet access.

l. Evidence handling procedures.

Describe an evidence handling policy that addresses specialized requirements if the policy differs from existing agency policy. Such a policy should address the following –

- 1) Archiving, retention, and/or disposition of digital evidence.
- 2) Specific storage challenges faced by computer evidence.

3) Storage of evidence seized after hours.

4) Volatile evidence.

C. Summary

Describe in detail the benefits that all proposed initiatives would produce if implemented.

Appendix 3. Sample Feasibility Study

This feasibility study will evaluate data collected from (local geographic area) and prepare a final report with recommendations concerning the feasibility of creating a computer forensics unit.

The following framework will be used by the working group as a guide to accomplishing the following broad objectives:

- 1. Determine the existing level of investigative effort and resources devoted to conducting computer forensics and investigations.
- 2. Determine the existing level of effort and unit resources devoted to analyzing computer evidence.
- 3. Determine the existing level of training effort and resources devoted to teaching computer forensics to unit personnel.
- 4. Determine a possible location and space requirements for establishing a computer forensic unit.
- 5. Estimate the anticipated forensic workload to be processed by the unit.
- 6. Estimate unit staffing requirements and operating structure based on anticipated forensic workload.
- 7. Estimate the type, quantity, and cost of the equipment required to establish and maintain a unit.
- 8. Estimate unit annual operating costs (supplies, furniture, equipment, utilities, training, etc.).
- 9. Determine partnerships and organizations that will support the unit.

Comment [j1]: Are the following bullet points the framework or the objectives?

Comment [b2]: The bulleted list is not really a set of objectives; it is more of a set of guidelines for establishing feasibility. Can this sentence be reworded?

Formatted: Bullets and Numbering

Formatted: Bullets and Numbering

Formatted: Bullets and Numbering

Formatted: Bullets and Numbering

Formatted: Bullets and Numbering

Formatted: Bullets and Numbering

Formatted: Bullets and Numbering

Formatted: Bullets and Numbering

Formatted: Bullets and Numbering

Appendix 4. Memorandum of Understanding (MOU) Template

Memorandum of Understanding

Between

Name of Agency

And

Name of Agency

This **MEMORANDUM OF UNDERSTANDING** is made on this ____ day of _____, _____ between the _____ and _____.

_____ and _____ enter into agreements with other parties, which will enable each party to enjoy the benefits of the other party's experience, assets, skills, and expertise in order to compliment and enhance the capabilities and effectiveness of both parties.

The purpose of this MOU is to define the roles of each party regarding _____.

Purpose of MOU

Define "Purpose of MOU"

Statement of Intent

Include "Statement of Intent"

The results of research projects will be shared jointly between _____ and _____, unless otherwise agreed upon by both parties.

Benefits to _____.

Benefits to _____.

Proprietary Information:

In those instances where the cooperation may reasonably be expected to result in an invention or other form of intellectual property with commercial application in operational forensic science, the ownership of the intellectual property rights shall recognize the contributions made by the parties to this agreement. The parties shall agree on a case-by-case basis the terms and conditions of such ownership of such intellectual property, including waiving of rights, payment of royalties or sharing of fees.

Non-Exclusivity:

This MOU does not prevent either party from being a party to research grants, academic course offerings or from being involved in the development of multi-party research proposals, which build on the strengths of the parties mentioned in this agreement.

This MOU, however, is not an obligation or commitment of funds, nor a basis for transfer of funds, but rather is a basic statement of the understandings between the parties hereto of the tasks and methods for performing the tasks described herein. Unless otherwise agreed in writing, each party shall bear its own costs in relation to this MOU. Expenditures by each party will be subject to its budgetary processes and to the availability of funds and resources pursuant to applicable law, regulations, and policies.

Termination:

Either party may terminate this Agreement 60 days after notifying the other party in writing.

Signature – Representative of Agency “A”
Representative’s Name and Title

Signature – Representative of Agency “B”
Representative’s Name and Title

Appendix 5. Sample Facility Manual**Scientific Working Group on
Digital Evidence****Recommended Guidelines for Developing
a Quality Management System****Disclaimer:**

As a condition to the use of this document and the information contained therein, the SWGDE requests notification by e-mail before or contemporaneous to the introduction of this document, or any portion thereof, as a marked exhibit offered for or moved into evidence in any judicial, administrative, legislative or adjudicatory hearing or other proceeding (including discovery proceedings) in the United States or any Foreign country. Such notification shall include: 1) The formal name of the proceeding, including docket number or similar identifier; 2) the name and location of the body conducting the hearing or proceeding; 3) subsequent to the use of this document in a formal proceeding please notify SWGDE as to its use and outcome; 4) the name, mailing address (if available) and contact information of the party offering or moving the document into evidence. Notifications should be sent to swgde@mail.ucf.edu.

Redistribution Policy:

SWGDE grants permission for redistribution and use of all publicly posted documents created by SWGDE, provided that the following conditions are met:

1. Redistributions of documents, or parts of documents, must retain the SWGDE cover page containing the disclaimer.
2. Neither the name of SWGDE, nor the names of its contributors, may be used to endorse or promote products derived from its documents.
3. Any reference or quote from a SWGDE document must include the version number (or create date) of the document and mention if the document is in a draft status.

RECOMMENDED GUIDELINES for DEVELOPING a QUALITY MANAGEMENT SYSTEM

Introduction

It is the goal of these guidelines to provide a framework of quality management in the processing of digital and multimedia evidence, including evidence handling, management practices, examinations, and reporting.

Quality Management System (QMS)

The quality management system defines and documents the organizational structure, responsibilities, procedures, processes, and resources for implementing quality management; including all activities that contribute to quality, directly or indirectly. The success of the quality system depends on the commitment of management and the active participation of each staff member. The personnel responsible must be clearly designated and shall have access to the highest level of management responsible for organizational policy.

Some essential elements of the QMS are detailed below. However, this list is not intended to be all-inclusive:

1. Personnel

An examining unit should have a structure that ensures maximum use of the knowledge and capabilities of its staff. It is important that all staff clearly understand what is expected of them.

- a. **Organizational Chart:** The organization and management structure of the examining unit, its place in any parent organization, and relevant organizational charts.
- b. The relationships and responsibilities of management, technical operations, and support services in implementing the quality system. An individual (however titled) may be responsible for more than one of the following duties:
 - (1) **Quality Manager:** A designated person who is responsible for maintaining the quality management system (including an annual review of the program) and who monitors compliance with the program.

- (2) **Health and Safety Manager:** A designated person who is responsible for maintaining the Health and Safety program (including an annual review of the program) and who monitors compliance with the program.
- (3) **Operational Manager:** A designated person who has the overall responsibility and authority for the operations of the unit.
- (4) **Technical Manager / Leader:** A designated person who has the overall responsibility and authority for protocols and methodologies.
- (5) **Examiner:** A designated person who examines digital and multimedia evidence or related materials or directs such examinations to be done, and is responsible for issuing reports for legal and administrative proceedings.
- (6) **Technician / Assistant:** A person who works with evidence, but typically does not issue reports for legal proceedings.

c. Job Description

There must be a written job description for all personnel, which should include responsibilities and duties.

d. Qualification / Education

The agency should articulate its minimum qualifications, training, and education requirements.

e. Training

The agency must establish and document a training program and qualifying procedure for all technical personnel. A written training program, approved by management, should focus on the development of the theoretical and practical knowledge, skills, and abilities necessary to examine digital and multimedia evidence and related materials.

f. Maintaining Qualifications

The agency must establish and document the minimum continuing professional development requirements for all technical personnel.

g. Court Testimony Monitoring

The presentation of testimony is the culmination of the work performed by a forensic examiner. Accordingly, it is vitally important that the

effectiveness of each examiner in this respect be reviewed. The unit must have and follow a written procedure whereby the testimony of each examiner is monitored annually. This monitoring can be accomplished by observation, review of transcripts, having a court officer complete an evaluation or telephonic solicitation by a supervisor.

2. Physical Plant

The facility shall provide adequate safety and security for personnel and operations. The facility must meet required health and safety standards. The facility must contain adequate space to perform required analytical functions and prevent alteration/damage to evidence. For example, a fume hood may be needed when the physical evidence poses a health and/or safety hazard to the examiner (e.g., for digital evidence that was seized in a clandestine drug lab, a crime scene containing biological materials, or other potentially hazardous environment). A facility should maintain general cleanliness. Facilities must be designed to ensure the proper safekeeping of evidence, data, and records to protect from loss, cross-transfer, contamination, and/or deleterious change. Appropriate precautions should be taken with regard to electrostatic discharge, electrical and magnetic fields to ensure the integrity of the digital evidence.

Appropriately secured storage areas must be provided.

3. Evidence Control

The examining unit must maintain records of requests for analysis/service and of the respective items of evidence. A unique identifier must be assigned to each case file or record. This file or record must include at least the following:

- a. The request for service document (request for lab examination) or a copy thereof.
- b. The identity of the party requesting the service and the date of the request.
- c. A description of items of evidence submitted with each having a unique item identifier.
- d. The identity of the person who delivered the evidence, along with the date of submission. For evidence not delivered in person, descriptive information regarding the mode of delivery and tracking information.

- e. The chain of custody record. Maintain chain of custody per established agency standard operating procedures for handling digital evidence
- f. Documentation of evidence disposition.

4. Examination Procedures

- a. The agency shall have and follow written examination procedures. These procedures shall be validated according to agency policy.
- b. Work practices shall be established to prevent contamination of evidence during examination procedures.
- c. Coordination with the investigator and/or other forensic examiners when other forensic examinations may be required. Specifically, the order in which these forensic examinations will be conducted should be determined before any examination (e.g. latent print analysis, DNA analysis, hair fiber analysis).
- d. The unit shall monitor the examination procedures using appropriate controls.

5. Equipment Performance

“Equipment” refers to the non-evidentiary hardware and software the examiner utilizes in the course of an examination.

- a. Equipment must be maintained and documented to ensure proper performance according to established agency policy.
- b. Only suitable and properly operating equipment shall be employed.
- c. The manufacturer's manual(s) and other relevant documentation (e.g. calibration, maintenance records) for each piece of equipment should be readily available.

6. Documentation, Reports, and Review

The Quality Management System should include requirements for the following minimum documentation:

- a. Quality Manual
- b. Standard Operating Procedures

- c. Training
- d. Validation of Tools
- e. Physical Work Space
- f. Equipment Inventory
- g. Maintenance/Calibration
- h. Health and Safety
- i. Evidence Handling Tracking System
- j. Annual Assessment of the Quality Management System
- k. Proficiency Testing
- l. Report of Findings
- m. Court testimony Monitoring
- n. Competency Testing
- o. Evidence Seized
- p. Audits
- q. Reference Materials/Library
- r. Corrective Action Policy/Procedures
- s. Complaints and Conflict Resolution

7. Competency and Proficiency Testing

Competency testing is the evaluation of a person's ability to perform work in any functional area before the performance of independent casework. This is normally conducted upon completion of a training program.

Proficiency testing is used to evaluate the competence of examiners, technical support, and the quality performance of an agency. It is recommended that each examiner be proficiency tested annually.

The administration of these tests should be detailed in the Quality Manual.

8. Validation

Validation is required to demonstrate the examination procedures and tools are suitable for their intended purpose. Minimum acceptability criteria should be described along with means for demonstrating compliance.

9. Internal Audits

Audits should be conducted according to agency policy. Records of each audit must be maintained and should include the scope, date of the audit, name of the person(s) conducting the audit, findings, and corrective action(s) taken, if necessary.

10. Deviations and Deficiencies

The agency must have a written policy to address administrative and technical deviations or deficiencies from the policies set forth in either the SOP or Quality Manual.

11. Health and Safety

All personnel should receive appropriate health and safety training, operate in accordance with agency policy, and comply with any relevant statutory regulations. The agency must have a documented health and safety program in place to meet the needs of the unit and the manual(s) shall be readily available to all personnel.

12. Quality Manual

- a. The agency's quality system policies and objectives shall be defined in a Quality Manual.
- b. A comprehensive Quality Manual must contain or reference the documents or policies/procedures pertaining to the following:
 1. A quality policy statement including objectives and commitments by management
 2. The organization and management structure of the unit, its place in any parent organization, and relevant organizational charts
 3. The relationships and responsibilities of management, technical operations, and support services in implementing the quality system
 4. Job descriptions, education, and up-to-date training records of unit staff
 5. Control and maintenance of documentation of case records and procedure manuals

6. The unit's procedures for ensuring that measurements are traceable to appropriate standards, where available
7. The type and extent of examinations conducted by the unit
8. Validation of test procedures used
9. Handling evidence
10. The use of standards and controls in unit procedures
11. Calibration and maintenance of equipment
12. Practices for ensuring continued competence of examiners including proficiency testing programs, and internal quality control schemes (e.g., technical review)
13. Gaining feedback and taking corrective action whenever discrepancies are detected
14. Monitoring court testimony to ensure the reporting of scientific findings in an unbiased and effective manner
15. Unit protocol permitting departures from documented policies and procedures
16. Dealing with complaints
17. Disclosure of information
18. Audits and quality system review

Reference Materials

The following are available on the SWGDE Website (www.swgde.org):

Proficiency Test Document:

SWGDE/SWGIT Proficiency Test Program Guidelines, V. 1.0 (October 2004)

Standard Operating Procedure Document:

SWGDE/SWGIT Recommended Guidelines for Developing Standard Operating Procedures, V. 1.0 (November 2004)

Training Document:

SWGDE/SWGIT Guidelines and Recommendations for Training in Digital and Multimedia Evidence, V. 1.0 (October 2004)

Validation Testing Document:

SWGDE Recommended Guidelines for Validation Testing, V. 1.0 (July 2004)

History: SWGDE Guidelines for a Quality Management System

Revision	Issue Date	Section	History
	10/22/2004	All	Draft document provided to SWGIT for comment.
	11/15/2004	All	Draft document posted for public comment.
	01/11/2005		Added reference page listing other published documents