



NIJ

Special

REPORT



**Forensic Examination of Digital Evidence:
A Guide for Law Enforcement**

visited on 9/07/2012

U.S. Department of Justice
Office of Justice Programs
810 Seventh Street N.W.
Washington, DC 20531

John Ashcroft
Attorney General

Deborah J. Daniels
Assistant Attorney General

Sarah V. Hart
Director, National Institute of Justice

This and other publications and products of the U.S. Department of Justice, Office of Justice Programs, National Institute of Justice can be found on the World Wide Web at the following site:

Office of Justice Programs
National Institute of Justice
<http://www.ojp.usdoj.gov/nij>

visited on 9/07/2012

NIJ

APR. 04

**Forensic Examination of Digital Evidence:
A Guide for Law Enforcement**

NCJ 199408



Sarah V. Hart

Director

This document is not intended to create, does not create, and may not be relied upon to create any rights, substantive or procedural, enforceable at law by any party in any matter civil or criminal.

Opinions or points of view expressed in this document represent a consensus of the authors and do not represent the official position or policies of the U.S. Department of Justice. The products, manufacturers, and organizations discussed in this document are presented for informational purposes only and do not constitute product approval or endorsement by the U.S. Department of Justice.

This document was prepared under Interagency Agreement #1999-IJ-R-094 between the National Institute of Justice and the National Institute of Standards and Technology, Office of Law Enforcement Standards.

The National Institute of Justice is a component of the Office of Justice Programs, which also includes the Bureau of Justice Assistance, the Bureau of Justice Statistics, the Office of Juvenile Justice and Delinquency Prevention, and the Office for Victims of Crime.

Foreword

Developments in the world have shown how simple it is to acquire all sorts of information through the use of computers. This information can be used for a variety of endeavors, and criminal activity is a major one. In an effort to fight this new crime wave, law enforcement agencies, financial institutions, and investment firms are incorporating computer forensics into their infrastructure. From network security breaches to child pornography investigations, the common bridge is the demonstration that the particular electronic media contained the incriminating evidence. Supportive examination procedures and protocols should be in place in order to show that the electronic media contains the incriminating evidence.

To assist law enforcement agencies and prosecutorial offices, a series of guides dealing with digital evidence has been selected to address the complete investigation process. This process expands from the crime scene through analysis and finally into the courtroom. The guides summarize information from a select group of practitioners who are knowledgeable about the subject matter. These groups are more commonly known as technical working groups.

This guide is the second in a series. The first guide, *Electronic Crime Scene Investigation: A Guide for First Responders*, is available through the National Institute of Justice Web site at <http://www.ojp.usdoj.gov/nij/pubs-sum/187736.htm>.

The remaining guides in the series will address—

- Using high technology to investigate.

- Investigating high technology crimes.
- Creating a digital evidence forensic unit.
- Presenting digital evidence in the courtroom.

Because of the complex issues associated with digital evidence examination, the Technical Working Group for the Examination of Digital Evidence (TWGEDE) recognized that its recommendations may not be feasible in all circumstances. The guide's recommendations are not legal mandates or policy directives, nor do they represent the *only* correct courses of action. Rather, the recommendations represent a consensus of the diverse views and experiences of the technical working group members who have provided valuable insight into these important issues. The National Institute of Justice (NIJ) expects that each jurisdiction will be able to use these recommendations to spark discussions and ensure that its practices and procedures are best suited to its unique environment.

It is our hope that, through these materials, more of our Nation's law enforcement personnel will be trained to work effectively with digital evidence and maximize the reliability of that evidence to the benefit of criminal case prosecutions.

NIJ extends its appreciation to the participants in the TWGEDE for their dedication to the preparation of this guide. Their efforts are particularly commendable given that they were not relieved of their existing duties with their home offices or agencies while they participated in the TWGEDE. What is more, it was necessary for

TWGEDE members to attend numerous (and lengthy) guide preparation meetings that were held at locations far removed from their home offices or agencies. In recognition of this, NIJ expresses great appreciation for the commitment made by

the home offices or agencies of TWGEDE members in suffering the periodic unavailability of their employees.

Sarah V. Hart
Director

National Institute of Justice

Technical Working Group for the Examination of Digital Evidence

The process of developing the guide was initiated through an invitational process. Invitees for the Technical Working Group for the Examination of Digital Evidence (TWGEDE) were selected initially for their expertise with digital evidence and then by their profession. The intent was to incorporate a medley of individuals with law enforcement, corporate, or legal affiliations to ensure a complete representation of the communities involved with digital evidence.

A small core of individuals was invited to comprise the planning panel. The task of the planning panel was to formulate a basic outline of topics that would be considered for inclusion.

NIJ thanks Michael P. Everitt of the U.S. Postal Service, Office of Inspector General, and Michael J. Menz. Both of these individuals provided their invaluable time and expertise during the guide's review process.

Planning panel

Susan Ballou

Program Manager, Forensic Science
Office of Law Enforcement Standards
National Institute of Standards and
Technology
Gaithersburg, Maryland

Kenneth Broderick

Special Agent
U.S. Bureau of Alcohol, Tobacco,
Firearms and Explosives
Computer Forensics Branch
Sterling, Virginia

Charles J. Faulk

Special Agent
U.S. Bureau of Alcohol, Tobacco,
Firearms and Explosives
Portland, Oregon

Grant Gottfried

Senior Specialist
National Center for Forensic Science
Orlando, Florida

Kim Herd

Criminal Law and Technology Counsel
National Association of Attorneys General
Washington, D.C.

Mark Johnson

Sergeant
Computer Crimes Unit
Kansas City, Missouri, Police
Kansas City, Missouri

Michael McCartney

Investigator
New York State Attorney General's Office
Criminal Prosecution Bureau—Organized
Crime Task Force
Buffalo, New York

Mark Menz

Digital Evidence Scientist
Folsom, California

Bill Moylan

Detective
Nassau County Police Department
Computer Crime Section
Crimes Against Property Squad
Westbury, New York

Glenn Nick

Assistant Director
U.S. Customs Service
Cyber Smuggling Center
Fairfax, Virginia

Todd Shipley

Detective Sergeant
Reno Police Department
Computer Crimes Unit
Reno, Nevada

Andy Siske

Defense Computer Investigation Training
Program
Linthicum, Maryland

Chris Stippich

Digital Intelligence, Inc.
Waukesha, Wisconsin

TWGEDE members

Additional members were then incorporated into the TWGEDE to provide a full technical working group. The individuals listed below, along with the planning panel, worked together to formulate this guide.

Abigail Abraham

Assistant State's Attorney
Cook County State's Attorney's Office
Chicago, Illinois

Chris G. Andrist

Agent
Colorado Bureau of Investigation
Denver, Colorado

Sean Barry

Computer Forensics Assistant Lab
Manager
New Technologies, Inc.
Gresham, Oregon

Bill Baugh

CEO
Savannah Technology Group
Savannah, Georgia

Randy Bishop

Special Agent in Charge
U.S. Department of Energy
Office of Inspector General
Technology Crime Section
Washington, D.C.

Carleton Bryant

Staff Attorney
Knox County Sheriff's Office
Knoxville, Tennessee

Don Buchwald

Project Engineer
The Aerospace Corporation
Los Angeles, California

Jaime Carazo

Special Agent
United States Secret Service
Electronic Crimes Branch
Washington, D.C.

Keith G. Chval

Chief, High Tech Crimes Bureau
Office of the Illinois Attorney General
Chicago, Illinois

Dorothy E. Denning

Professor
Computer Science Department
Georgetown University
Washington, D.C.

Dan Dorman

Inspector
Postal Inspection Service
Atlanta, Georgia

James Doyle

Sergeant
Detective Bureau
New York City Police Department
Computer Investigation and Technology
Unit
New York, New York

Michael Duncan

Staff/Sergeant
Economic Crime Branch
Technological Crime Section
Ottawa, Ontario
Canada

Doug Elrick

Senior Forensic Specialist
Digital Intelligence
Waukesha, Wisconsin

Michael Finnie

Forensic Specialist
Computer Forensics Inc.
Seattle, Washington

Toby M. Finnie

Director
High Tech Crime Consortium
Tacoma, Washington

Paul T. French

Director, Consulting Services
New Technologies, Inc.
Computer Forensics Lab Manager
Gresham, Oregon

Pat Gilmore

Director
RedSiren, Inc.
Pittsburgh, Pennsylvania

Sam Guttman

Postal Inspector
Forensic and Technical Services
U.S. Postal Service
Dulles, Virginia

Dave Heslep

Sergeant
Maryland State Police
Computer Forensics Laboratory
Columbia, Maryland

Al Hobbs

Special Deputy U.S. Marshal
Child Exploitation Strike Force
Arlington Heights Police Department
Arlington Heights, Illinois

Robert Hopper

Sergeant
Arizona Department of Public Safety
Computer Forensic Unit
Phoenix, Arizona

Mary Horvath

Program Manager
FBI-CART
Washington, D.C.

Nigel Jones

Programme Manager
National High Tech Crime Training Centre
National Police Training
Wyboston Lakes Leisure Centre
United Kingdom

Roland Lascola

Cyber Security Specialist
Independent Oversight
U.S. Department of Energy
Washington, D.C.

Barry Leese

Lieutenant
Maryland State Police
Computer Crimes Unit
Columbia, Maryland

Glenn Lewis

Kroll Global Headquarters
New York, New York

Jason Luttgens

Computer Specialist, R&D
NASA Office of the Inspector General
Computer Crimes Division
Washington, D.C.

Dan Mares

President
Mares and Company, LLC
Lawrenceville, Georgia

Ralph McNamara

Assistant Inspector General for
Investigations
National Archives and Records
Administration
Office of Inspector General
College Park, Maryland

Joel Moskowitz

Investigator
Clark County District Attorney's Office
Las Vegas, Nevada

James K. Pace

Senior Special Agent
Chief of Computer Forensics and
Investigations
U.S. Army Criminal Investigation
Laboratory
Forest Park, Georgia

Scott R. Patronik

Chief, Division of Technology and
Advancement
Erie County Sheriff's Office
Buffalo, New York

Greg Redfern

Director
Department of Defense Computer
Investigations Training Program
Linthicum, Maryland

Henry R. Reeve

General Counsel
Second Judicial District
Denver, Colorado

Jim Riccardi, Jr.

Electronic Crime Specialist
National Law Enforcement and Corrections
Technology Center–Northeast
Rome, New York

Greg Schmidt

Investigations/Technical
Computer Forensics Examiner
Plano, Texas

Howard Schmidt

Vice Chair
President's Critical Infrastructure
Protection Board
Washington, D.C.

Raemarie Schmidt

Computer Crimes Training Specialist
National White Collar Crime Center
Computer Crime Section
Fairmont, West Virginia

John A. Sgromolo

President
Digital Forensics, Inc.
Clearwater, Florida

George Sidor

Sr. Computer Forensics Investigator
G-Wag, Inc.
St. Albert, Alberta
Canada

Mike Weil

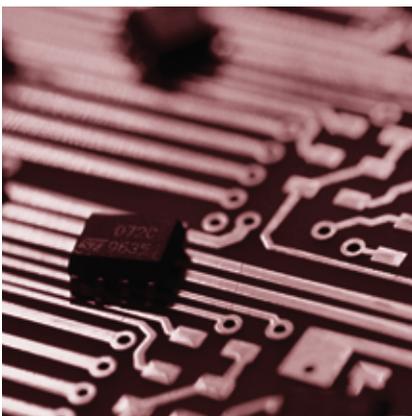
Computer Forensic Examiner
DoD Computer Forensics Laboratory
Linthicum, Maryland

Contents

Foreword	iii
Technical Working Group for the Examination of Digital Evidence	v
Introduction	1
Chapter 1. Policy and Procedure Development	3
Chapter 2. Evidence Assessment	7
Chapter 3. Evidence Acquisition	11
Chapter 4. Evidence Examination	15
Chapter 5. Documenting and Reporting	19
Appendix A. Case Examples	23
Appendix B. Glossary	39
Appendix C. Sample Worksheets	43
Appendix D. Examples of Request for Service Forms	51
Appendix E. Legal Resources List	59
Appendix F. Technical Resources List	61
Appendix G. Training Resources List	83
Appendix H. List of Organizations	87

Introduction

*Note: Terms that are defined in the glossary appear in **bold italics** on their first appearance in the body of the report.*



This guide is intended for use by law enforcement officers and other members of the law enforcement community who are responsible for the **examination** of **digital evidence**.

This guide is not all-inclusive. Rather, it deals with common situations encountered during the examination of digital evidence. It is **not** a mandate for the law enforcement community; it is a guide agencies can use to help them develop their own policies and procedures.

Technology is advancing at such a rapid rate that the suggestions in this guide are best examined in the context of current technology and practices. Each case is unique and the judgment of the examiner should be given deference in the implementation of the procedures suggested in this guide. Circumstances of individual cases and Federal, State, and local laws/rules may also require actions other than those described in this guide.

When dealing with digital evidence, the following general forensic and procedural principles should be applied:

- Actions taken to secure and collect digital evidence should not affect the integrity of that evidence.
- Persons conducting an examination of digital evidence should be trained for that purpose.
- Activity relating to the seizure, examination, storage, or transfer of digital evidence should be documented, preserved, and available for review.

Through all of this, the examiner should be cognizant of the need to conduct an accurate and impartial examination of the digital evidence.

How is digital evidence processed?

Assessment. Computer forensic examiners should assess digital evidence thoroughly with respect to the scope of the case to determine the course of action to take.

Acquisition. Digital evidence, by its very nature, is fragile and can be altered, damaged, or destroyed by improper handling or examination. Examination is best conducted on a **copy** of the **original evidence**. The original evidence should be acquired in a manner that protects and preserves the integrity of the evidence.

Examination. The purpose of the examination process is to extract and analyze digital evidence. Extraction refers to the recovery of data from its media. **Analysis** refers to the interpretation of the recovered data and putting it in a logical and useful format.

Documenting and reporting. Actions and observations should be documented throughout the forensic processing of evidence. This will conclude with the preparation of a written report of the findings.

Is your agency prepared to handle digital evidence?

This document recommends that agencies likely to handle digital evidence identify appropriate external resources for the processing of digital evidence before they are needed. These resources should be readily available for situations that are beyond the technical expertise or resources of the department. It is also recommended that agencies develop policies and procedures to ensure compliance with Federal, State, and local laws.

The following five topics describe the necessary basic steps to conduct a computer forensic examination and suggest the order in which they should be conducted. Although documentation is listed as the last step, a well-trained examiner understands that documentation is continuous throughout the entire examination process.

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

Each of these steps is explained further in the subsequent chapters. The chapters are further supported by the specialized information provided in the appendixes.

Chapter 1. Policy and Procedure Development



Principle: Computer forensics as a discipline demands specially trained personnel, support from management, and the necessary funding to keep a unit operating. This can be attained by constructing a comprehensive training program for examiners, sound digital evidence recovery techniques, and a commitment to keep any developed unit operating at maximum efficiency.

Procedure: Departments should create policies and procedures for the establishment and/or operation of a computer forensics unit.

Protocols and procedures

Mission statement

Developing policies and procedures that establish the parameters for operation and function is an important phase of creating a computer forensics unit. An effective way to begin this task is to develop a mission statement that incorporates the core functions of the unit, whether those functions include high-technology crime investigations, evidence collection, or forensic analysis.

Personnel

The policies and procedures should consider defining the personnel requirements for the unit. Topics that might be included in this section are job descriptions and minimum qualifications, hours of operation, on-call duty status, command structure, and team configuration.

Administrative considerations

Software licensing. Ensure that all software used by the computer forensics unit is properly licensed by the agency or an individual assigned to the unit.

Resource commitment. Establishing and operating a computer forensics unit may require *significant* allocation of financial resources and personnel. Many of the expenses are recurring and will have to be budgeted on a yearly basis. Resource allocation should include the type of facility that will house the unit, equipment used by examiners, software and hardware requirements, upgrades, training, and ongoing professional development and retention of examiners.

Training. It is important that computer forensics units maintain skilled, competent examiners. This can be accomplished by developing the skills of existing personnel or hiring individuals from specific disciplines. Because of the dynamic nature of the field, a comprehensive

ongoing training plan should be developed based on currently available training resources and should be considered in budget submissions. Consideration may also be given to mentor programs, on-the-job training, and other forms of career development.

Service request and intake

Guidelines should be developed to establish a process for the submission of forensic service requests and the intake of accepted requests for examination of digital evidence. Topics to consider in these guidelines include request and intake forms, point of contact, required documentation, acceptance criteria,* and requirements for the submission of physical evidence. Field personnel are expected to know the policies for service request and intake.

Case management

Once a request for forensic services is approved, criteria for prioritizing and assigning examinations should be determined and implemented. Criteria may include the nature of the crime, court dates, deadlines, potential victims, legal considerations, volatile nature of the evidence, and available resources.

Evidence handling and retention

Guidelines should be established for receiving, processing, documenting, and handling evidence and work products associated with the examination. The guidelines should be consistent with existing departmental policy. However, criteria for digital evidence handling and retention may exceed established departmental policies. **Note:** Evidence identified as contraband, such as child pornography, may require special consideration, such as obtaining specific contraband-related seizure and search warrants.

It is important to remember that other forensic disciplines might be able to recover other evidence, such as fingerprints on the hard drive, hair or fibers in the keyboard, and handwritten disk labels or printed material. In these instances, procedures should be developed to determine the order and manner in which examinations should be performed to reap full evidentiary value.

Case processing

Standard operating procedures (SOPs) should be developed for preserving and processing digital evidence. SOPs should be general enough to address the basic steps in a routine forensic examination while providing flexibility to respond to unique circumstances arising from unforeseen situations.

*One particular scenario for which an acceptance criteria policy and procedure may be helpful is one in which field personnel have made post-seizure changes to the evidence. This sometimes occurs when field personnel, often unaware of the effects of their actions, attempt to look for files on the original media, thereby changing date and time stamps associated with those files and possibly affecting other data on the media. Although perhaps not fatal to the case, this is one factor that likely would require documentation and should be considered before accepting this service request. One step in this procedure might be to submit the facts to the relevant prosecuting agency to determine whether it would consider the case to be viable, given the post-seizure alteration.

Developing technical procedures

Established procedures should guide the technical process of the examination of evidence. Procedures should be tested prior to their implementation to ensure that the results obtained are valid and independently reproducible. The steps in the development and validation of the procedures should be documented and include:

- Identifying the task or problem.
- Proposing possible solutions.
- Testing each solution on a known control sample.
- Evaluating the results of the test.
- Finalizing the procedure.



Original evidence should never be used to develop procedures.

Chapter 2. Evidence Assessment



Principle: The digital evidence should be thoroughly assessed with respect to the scope of the case to determine the course of action.

Procedure: Conduct a thorough assessment by reviewing the search warrant or other legal authorization, case detail, nature of hardware and software, potential evidence sought, and the circumstances surrounding the **acquisition** of the evidence to be examined.

Case assessment

- Review the case investigator's request for service.
 - Identify the legal authority for the forensic examination request.
 - Ensure there is a completed request for assistance (see appendix D for examples).
 - Complete documentation of chain of custody.
- Consult with the case investigator about the case and let him or her know what the forensic examination may or may not discover. When talking with the investigator about the facts of the case, consider the following:
 - Discuss whether other forensic processes need to be performed on the evidence (e.g., DNA analysis, fingerprint, toolmarks, trace, and questioned documents).
 - Discuss the possibility of pursuing other investigative avenues to obtain additional digital evidence (e.g., sending a **preservation order** to an **Internet service provider (ISP)**, identifying remote storage locations, obtaining e-mail).
 - Consider the relevance of peripheral components to the investigation. For example, in forgery or fraud cases consider noncomputer equipment such as laminators, credit card blanks, check paper, scanners, and printers. In child pornography cases consider digital cameras.
 - Determine the potential evidence being sought (e.g., photographs, spreadsheets, documents, databases, financial records).
 - Determine additional information regarding the case (e.g., aliases, e-mail accounts, e-mail addresses, ISP used, names, **network** configuration and users, system logs, passwords, user names). This information may be obtained through interviews with the **system administrator**, users, and employees.

- Assess the skill levels of the computer users involved. Techniques employed by skilled users to conceal or destroy evidence may be more sophisticated (e.g., **encryption**, booby traps, **steganography**).
- Prioritize the order in which evidence is to be examined.
- Determine if additional personnel will be needed.
- Determine the equipment needed.



The assessment might uncover evidence pertaining to other criminal activity (e.g., money laundering in conjunction with narcotics activities).

Onsite considerations

The following material does not provide complete information on examination of digital evidence; it is a general guide for law enforcement agencies that assess digital evidence at the crime scene. Readers may also want to consult *Electronic Crime Scene Investigation: A Guide for First Responders*, available at <http://www.ojp.usdoj.gov/nij/pubs-sum/187736.htm>.



Consider safety of personnel at the scene. Always ensure the scene is properly secured before and during the search.

In some cases, the examiner may only have the opportunity to do the following while onsite:

- Identify the number and type of computers.
- Determine if a network is present.
- Interview the system administrator and users.
- Identify and document the types and volume of media, including **removable media**. Document the location from which the media was removed.
- Identify offsite storage areas and/or remote computing locations.
- Identify **proprietary software**.

- Evaluate general conditions of the site.
- Determine the operating system in question.



Determine the need for and contact available outside resources, if necessary. Establish and retain a phone list of such resources.

Processing location assessment

Assess the evidence to determine where the examination should occur. It is preferable to complete an examination in a controlled environment, such as a dedicated forensic work area or laboratory. Whenever circumstances require an onsite examination to be conducted, attempt to control the environment. Assessment considerations might include the following:

- The time needed onsite to accomplish evidence recovery.
- Logistic and personnel concerns associated with long-term deployment.
- The impact on the business due to a lengthy search.
- The suitability of equipment, resources, media, training, and experience for an onsite examination.

Legal considerations

- Determine the extent of the authority to search.
- Identify possible concerns related to applicable Federal statutes (such as the Electronic Communications Privacy Act of 1986 (ECPA) and the Cable Communications Policy Act (CCPA), both as amended by the USA PATRIOT ACT of 2001, and/or the Privacy Protection Act of 1980 (PPA)), State statutes, and local policies and laws.



If evidence is located that was not authorized in the original search authority, determine what additional legal process may be necessary to continue the search (e.g., warrant, amended consent form). Contact legal advisors for assistance if needed.

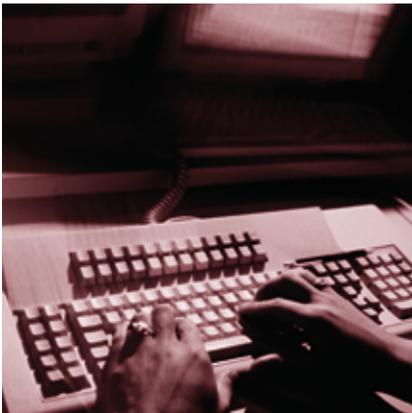
Evidence assessment

- Prioritize the evidence (e.g., distribution CDs versus user-created CDs).
 - Location where evidence is found.
 - Stability of media to be examined.

- Determine how to document the evidence (e.g., photograph, sketch, notes).
- Evaluate storage locations for ***electromagnetic interference***.
- Ascertain the condition of the evidence as a result of packaging, transport, or storage.
- Assess the need to provide continuous electric power to battery-operated devices.

Note: The procedures outlined are based on a compilation of generally accepted practices. Consult individual agency policy and seek legal advice, if necessary, before initiating an examination. Actual conditions may require alternative steps to those outlined in this guide. A thorough case assessment is a foundation for subsequent procedures.

Chapter 3. Evidence Acquisition



Principle: Digital evidence, by its very nature, is fragile and can be altered, damaged, or destroyed by improper handling or examination. For these reasons special precautions should be taken to preserve this type of evidence. Failure to do so may render it unusable or lead to an inaccurate conclusion.

Procedure: Acquire the original digital evidence in a manner that protects and preserves the evidence. The following bullets outline the basic steps:

- Secure digital evidence in accordance with departmental guidelines. In the absence of such guidelines, useful information can be found in *Electronic Crime Scene Investigation: A Guide for First Responders* (<http://www.ojp.usdoj.gov/nij/pubs-sum/187736.htm>).
- Document hardware and software configuration of the examiner's system.
- Verify operation of the examiner's computer system to include hardware and software.
- Disassemble the case of the computer to be examined to permit physical access to the storage devices.
 - Take care to ensure equipment is protected from static electricity and magnetic fields.
- Identify storage devices that need to be acquired. These devices can be internal, external, or both.
- Document internal storage devices and hardware configuration.
 - Drive condition (e.g., make, model, geometry, size, jumper settings, location, drive interface).
 - Internal components (e.g., sound card; video card; network card, including **media access control (MAC)** address; personal computer memory card international association (PCMCIA) cards).
- Disconnect storage devices (using the power connector or data cable from the back of the drive or from the motherboard) to prevent the destruction, damage, or alteration of data.

- Retrieve configuration information from the suspect's system through controlled boots.
 - Perform a controlled boot to capture **CMOS/BIOS** information and test functionality.
 - Boot sequence (this may mean changing the BIOS to ensure the system boots from the floppy or CD-ROM drive).
 - Time and date.
 - Power on passwords.
 - Perform a second controlled boot to test the computer's functionality and the forensic boot disk.
 - Ensure the power and data cables are properly connected to the floppy or CD-ROM drive, and ensure the power and data cables to the storage devices are still disconnected.
 - Place the forensic boot disk into the floppy or CD-ROM drive. Boot the computer and ensure the computer will boot from the forensic boot disk.
 - Reconnect the storage devices and perform a third controlled boot to capture the drive configuration information from the CMOS/BIOS.
 - Ensure there is a forensic boot disk in the floppy or CD-ROM drive to prevent the computer from accidentally booting from the storage devices.
 - Drive configuration information includes logical block addressing (LBA); large disk; cylinders, heads, and sectors (CHS); or auto-detect.
- Power system down.
- Whenever possible, remove the subject storage device and perform the acquisition using the examiner's system. When attaching the subject device to the examiner's system, configure the storage device so that it will be recognized.
- Exceptional circumstances, including the following, may result in a decision not to remove the storage devices from the subject system:
 - RAID (redundant array of inexpensive disks). Removing the disks and acquiring them individually may not yield usable results.
 - Laptop systems. The system drive may be difficult to access or may be unusable when detached from the original system.
 - Hardware dependency (legacy equipment). Older drives may not be readable in newer systems.
 - Equipment availability. The examiner does not have access to necessary equipment.

- Network storage. It may be necessary to use the network equipment to acquire the data.

When using the subject computer to acquire digital evidence, reattach the subject storage device and attach the examiner's evidence storage device (e.g., hard drive, tape drive, **CD-RW, MO**).

- Ensure that the examiner's storage device is **forensically** clean when acquiring the evidence.



Write protection should be initiated, if available, to preserve and protect original evidence.

Note: The examiner should consider creating a known value for the subject evidence prior to acquiring the evidence (e.g., performing an independent cyclic redundancy check (CRC), **hashing**). Depending on the selected acquisition method, this process may already be completed.

- If hardware write protection is used:
 - Install a write protection device.
 - Boot system with the examiner's controlled operating system.
- If software write protection is used:
 - Boot system with the examiner-controlled operating system.
 - Activate write protection.
- Investigate the geometry of any storage devices to ensure that all space is accounted for, including host-protected data areas (e.g., nonhost specific data such as the partition table matches the physical geometry of the drive).
- Capture the electronic serial number of the drive and other user-accessible, host-specific data.
- Acquire the subject evidence to the examiner's storage device using the appropriate software and hardware tools, such as:
 - Stand-alone duplication software.
 - Forensic analysis software suite.
 - Dedicated hardware devices.
- Verify successful acquisition by comparing known values of the original and the copy or by doing a sector-by-sector comparison of the original to the copy.

Chapter 4. Evidence Examination



Principle: General forensic principles apply when examining digital evidence. Different types of cases and media may require different methods of examination. Persons conducting an examination of digital evidence should be trained for this purpose.

Procedure: Conduct the examination on data that have been acquired using accepted forensic procedures. Whenever possible, the examination should not be conducted on original evidence.

This chapter discusses the extraction and the analysis of digital evidence. Extraction refers to the recovery of data from the media. Analysis refers to the interpretation of the recovered data and placement of it in a logical and useful format (e.g., how did it get there, where did it come from, and what does it mean?). The concepts offered are intended to assist the examiner in developing procedures and structuring the examination of the digital evidence. These concepts are not intended to be all-inclusive and recognize that not all of the following techniques may be used in a case. It is up to the discretion of the examiner to select the appropriate approach.

When conducting evidence examination, consider using the following steps:

Step 1. Preparation

Prepare working directory/directories on separate media to which evidentiary files and data can be recovered and/or extracted.

Step 2. Extraction

Discussed below are two different types of extraction, physical and logical. The physical extraction phase identifies and recovers data across the entire physical drive without regard to **file system**. The logical extraction phase identifies and recovers files and data based on the installed operating system(s), file system(s), and/or application(s).

Physical extraction

During this stage the extraction of the data from the drive occurs at the physical level regardless of file systems present on the drive. This may include the following methods: keyword searching, file carving, and extraction of the partition table and unused space on the physical drive.

- Performing a keyword search across the physical drive may be useful as it allows the examiner to extract data that may not be accounted for by the operating system and file system.

- File carving utilities processed across the physical drive may assist in recovering and extracting useable files and data that may not be accounted for by the operating system and file system.
- Examining the partition structure may identify the file systems present and determine if the entire physical size of the hard drive is accounted for.

Logical extraction

During this stage the extraction of the data from the drive is based on the file system(s) present on the drive and may include data from such areas as active files, **deleted files**, **file slack**, and unallocated file space. Steps may include:

- Extraction of the file system information to reveal characteristics such as directory structure, file attributes, file names, date and time stamps, file size, and file location.
- Data reduction to identify and eliminate known files through the comparison of calculated hash values to authenticated hash values.
- Extraction of files pertinent to the examination. Methods to accomplish this may be based on file name and extension, file header, file content, and location on the drive.
- Recovery of deleted files.
- Extraction of **password-protected**, encrypted, and compressed data.
- Extraction of file slack.
- Extraction of the **unallocated space**.

Step 3. Analysis of extracted data

Analysis is the process of interpreting the extracted data to determine their significance to the case. Some examples of analysis that may be performed include timeframe, data hiding, application and file, and ownership and possession. Analysis may require a review of the request for service, legal authority for the search of the digital evidence, investigative leads, and/or analytical leads.

Timeframe analysis

Timeframe analysis can be useful in determining when events occurred on a computer system, which can be used as a part of associating usage of the computer to an individual(s) at the time the events occurred. Two methods that can be used are:

- Reviewing the time and date stamps contained in the file system metadata (e.g., last modified, last accessed, created, change of status) to link files of interest to the timeframes relevant to the investigation. An example of this analysis would be using the last modified date and time to establish when the contents of a file were last changed.

- Reviewing system and application logs that may be present. These may include error logs, installation logs, connection logs, security logs, etc. For example, examination of a security log may indicate when a user name/password combination was used to log into a system.

Note: Take into consideration any differences in the individual's computer date and time as reported in the BIOS.

Data hiding analysis

Data can be concealed on a computer system. Data hiding analysis can be useful in detecting and recovering such data and may indicate knowledge, ownership, or intent. Methods that can be used include:

- Correlating the file headers to the corresponding file extensions to identify any mismatches. Presence of mismatches may indicate that the user intentionally hid data.
- Gaining access to all password-protected, encrypted, and **compressed files**, which may indicate an attempt to conceal the data from unauthorized users. A password itself may be as relevant as the contents of the file.
- Steganography.
- Gaining access to a **host-protected area (HPA)**. The presence of user-created data in an HPA may indicate an attempt to conceal data.

Application and file analysis

Many programs and files identified may contain information relevant to the investigation and provide insight into the capability of the system and the knowledge of the user. Results of this analysis may indicate additional steps that need to be taken in the extraction and analysis processes. Some examples include:

- Reviewing file names for relevance and patterns.
- Examining file content.
- Identifying the number and type of operating system(s).
- Correlating the files to the installed applications.
- Considering relationships between files. For example, correlating Internet history to cache files and e-mail files to e-mail attachments.
- Identifying unknown file types to determine their value to the investigation.
- Examining the users' default storage location(s) for applications and the **file structure** of the drive to determine if files have been stored in their default or an alternate location(s).
- Examining user-configuration settings.

- Analyzing file metadata, the content of the user-created file containing data additional to that presented to the user, typically viewed through the application that created it. For example, files created with word processing applications may include authorship, time last edited, number of times edited, and where they were printed or saved.

Ownership and possession

In some instances it may be essential to identify the individual(s) who created, modified, or accessed a file. It may also be important to determine ownership and knowledgeable possession of the questioned data. Elements of knowledgeable possession may be based on the analysis described above, including one or more of the following factors.

- Placing the subject at the computer at a particular date and time may help determine ownership and possession (timeframe analysis).
- Files of interest may be located in nondefault locations (e.g., user-created directory named "child porn") (application and file analysis).
- The file name itself may be of evidentiary value and also may indicate the contents of the file (application and file analysis).
- Hidden data may indicate a deliberate attempt to avoid detection (hidden data analysis).
- If the passwords needed to gain access to encrypted and password-protected files are recovered, the passwords themselves may indicate possession or ownership (hidden data analysis).
- Contents of a file may indicate ownership or possession by containing information specific to a user (application and file analysis).

Step 4. Conclusion

In and of themselves, results obtained from any one of these steps may not be sufficient to draw a conclusion. When viewed as a whole, however, associations between individual results may provide a more complete picture. As a final step in the examination process, be sure to consider the results of the extraction and analysis in their entirety.

Chapter 5. Documenting and Reporting



Principle: The examiner is responsible for completely and accurately reporting his or her findings and the results of the analysis of the digital evidence examination. Documentation is an ongoing process throughout the examination. It is important to accurately record the steps taken during the digital evidence examination.

Procedure: All documentation should be complete, accurate, and comprehensive. The resulting report should be written for the intended audience.

Examiner's notes

Documentation should be contemporaneous with the examination, and retention of notes should be consistent with departmental policies. The following is a list of general considerations that may assist the examiner throughout the documentation process.

- Take notes when consulting with the case investigator and/or prosecutor.
- Maintain a copy of the search authority with the case notes.
- Maintain the initial request for assistance with the case file.
- Maintain a copy of chain of custody documentation.
- Take notes detailed enough to allow complete duplication of actions.
- Include in the notes dates, times, and descriptions and results of actions taken.
- Document irregularities encountered and any actions taken regarding the irregularities during the examination.
- Include additional information, such as network topology, list of authorized users, user agreements, and/or passwords.
- Document changes made to the system or network by or at the direction of law enforcement or the examiner.
- Document the operating system and relevant software version and current, installed patches.
- Document information obtained at the scene regarding remote storage, remote user access, and offsite backups.



During the course of an examination, information of evidentiary value may be found that is beyond the scope of the current legal authority. Document this information and bring it to the attention of the case agent because the information may be needed to obtain additional search authorities.

Examiner's report

This section provides guidance in preparing the report that will be submitted to the investigator, prosecutor, and others. These are general suggestions; departmental policy may dictate report writing specifics, such as its order and contents. The report may include:

- Identity of the reporting agency.
- Case identifier or submission number.
- Case investigator.
- Identity of the submitter.
- Date of receipt.
- Date of report.
- Descriptive list of items submitted for examination, including serial number, make, and model.
- Identity and signature of the examiner.
- Brief description of steps taken during examination, such as string searches, graphics image searches, and recovering erased files.
- Results/conclusions.

The following sections have been found to be useful in other report formats. See appendix A for sample reports.

Summary of findings

This section may consist of a brief summary of the results of the examinations performed on the items submitted for analysis. All findings listed in the summary should also be contained in the details of findings section of the report.

Details of findings

This section should describe in greater detail the results of the examinations and may include:

- Specific files related to the request.
- Other files, including deleted files, that support the findings.
- String searches, keyword searches, and text string searches.
- Internet-related evidence, such as Web site traffic analysis, chat logs, cache files, e-mail, and news group activity.
- Graphic image analysis.
- Indicators of ownership, which could include program registration data.
- Data analysis.
- Description of relevant programs on the examined items.
- Techniques used to hide or mask data, such as encryption, steganography, hidden attributes, hidden partitions, and **file name anomalies**.

Supporting materials

List supporting materials that are included with the report, such as printouts of particular items of evidence, digital copies of evidence, and chain of custody documentation.

Glossary

A glossary may be included with the report to assist the reader in understanding any technical terms used. Use a generally accepted source for the definition of the terms and include appropriate references.

Appendix A. Case Examples

The following two case briefs are examples of what could be involved in case analysis.

Disclaimer: The chosen case scenarios are for instructional purposes only and any association to an actual case and litigation is purely coincidental. Names and locations presented in the case scenarios are fictitious and are not intended to reflect actual people or places. Reference herein to any specific commercial products, processes, or services by trade name, trademark, manufacturer, or otherwise does not constitute or imply its endorsement, recommendation, or favoring by the U.S., State, or local governments, and the information and statements shall not be used for the purposes of advertising.

Case brief 1

SUBJECT owned a roofing company. SUBJECT gave his laptop computer to an employee to take to Mom & Pop's Computer Repair for monitor problems. Upon repairing the laptop, Mom of Mom & Pop's started the laptop to ensure the monitor had been fixed. A standard procedure of Mom & Pop's was to go to the *Recent* menu on the *Start Bar* of Windows® 98 systems and select files for viewing. Mom was presented with what appeared to be an image of a young child depicted in a sexually explicit manner. Mom telephoned the county sheriff. A sheriff's deputy responded and observed the image and confirmed it to be a violation of a State statute. The laptop was seized because it contained contraband. The seizure was performed in a manner consistent with recommendations found in *Electronic Crime Scene Investigation: A Guide for First Responders*. The laptop was entered into evidence according to agency policy, and a search warrant was obtained for the examination of the computer. The computer was submitted for examination.

Objective: To determine whether SUBJECT possessed child pornography. This was complicated by the number of people who handled the laptop.

Computer type: Generic laptop, serial # 123456789.

Operating system: Microsoft® Windows® 98.

Offense: Possession of child pornography.

Case agent: Investigator Johnson.

Evidence number: 012345.

Chain of custody: See attached form.

Where examination took place: Criminal investigations unit.

Tools used: Disk acquisition utility, universal graphic viewer, command line.

Processing

Assessment: Reviewed the case investigator's request for service. The search warrant provided legal authority. The investigator was interested in finding all information pertaining to child pornography, access dates, and ownership of the computer. It was determined that the equipment needed was available in the forensic lab.

Acquisition: The hardware configuration was documented and a **duplicate** of the hard drive was created in a manner that protected and preserved the evidence. The CMOS information, including the time and date, was documented.

Examination: The directory and file structures, including file dates and times, were recorded. A file header search was conducted to locate all graphic images. The image files were reviewed and those files containing images of what appeared to be children depicted in a sexually explicit manner were preserved. Shortcut files were recovered that pointed to files on floppy disks with sexually explicit file names involving children. The last accessed time and date of the files indicated the files were last accessed 10 days before the laptop was delivered to Mom & Pop's.

Documentation and reporting: The investigator was given a report describing the findings of the examination. The investigator determined that he needed to conduct interviews.

Next step: The employee who delivered the laptop computer to Mom & Pop's Computer Repair was interviewed, and he indicated that he had never operated the computer. Further, the employee stated SUBJECT had shown him images of a sexual nature involving children on the laptop. SUBJECT told the employee that he keeps his pictures on floppy disks at home; he just forgot this one image on the laptop.

The State's Attorney's Office was briefed in hope of obtaining a search warrant for SUBJECT's home based on the examination of the digital evidence and the interview of the employee. A warrant was drafted, presented to a judicial officer, and signed. During the subsequent search, floppy disks were discovered at SUBJECT's house. Forensic examination of the floppies revealed additional child pornography, including images in which SUBJECT was a participant. This resulted in the arrest of SUBJECT.

Case brief 1 report

REPORT OF MEDIA ANALYSIS

MEMORANDUM FOR: County Sheriff's Police
Investigator Johnson
Anytown, USA 01234

SUBJECT: Forensic Media Analysis Report
SUBJECT: DOE, JOHN
Case Number: 012345

1. Status: Closed.

2. Summary of Findings:

- 327 files containing images of what appeared to be children depicted in a sexually explicit manner were recovered.
- 34 shortcut files that pointed to files on floppy disks with sexually explicit file names involving children were recovered.

3. Items Analyzed:

<u>TAG NUMBER:</u>	<u>ITEM DESCRIPTION:</u>
012345	One Generic laptop, Serial # 123456789

4. Details of Findings:

- Findings in this paragraph related to the Generic Hard Drive, Model ABCDE, Serial # 3456ABCD, recovered from Tag Number 012345, One Generic laptop, Serial # 123456789.
 - 1) The examined hard drive was found to contain a Microsoft® Windows® 98 operating system.
 - 2) The directory and file listing for the media was saved to the Microsoft® Access Database TAG012345.MDB.
 - 3) The directory C:\JOHN DOE\PERSONAL\FAV PICS\, was found to contain 327 files containing images of what appeared to be children depicted in a sexually explicit manner. The file directory for 327 files disclosed that the files' creation date and times are 5 July 2001 between 11:33 p.m. and 11:45 p.m., and the last access date for 326 files listed is 27 December 2001. In addition, the file directory information for one file disclosed the last access date as 6 January 2002.
 - 4) The directory C:\JOHN DOE\PERSONAL\FAV PICS TO DISK\ contained 34 shortcut files that pointed to files on floppy disks with sexually explicit file names involving children. The file directory information for the 34 shortcut files disclosed

the files' creation date and times are 5 July 2001 between 11:23 p.m. and 11:57 p.m., and the last access date for the 34 shortcut files was listed as 5 July 2001.

- 5) The directory C:\JOHN DOE\LEGAL\ contained five Microsoft® Word documents related to various contract relationships John Doe Roofing had with other entities.
- 6) The directory C:\JOHN DOE\JOHN DOE ROOFING\ contained files related to operation of John Doe Roofing.
- 7) No further user-created files were present on the media.

5. Glossary:

Shortcut File: A file created that links to another file.

6. Items Provided: In addition to this hard copy report, one compact disk (CD) was submitted with an electronic copy of this report. The report on CD contains hyperlinks to the above-mentioned files and directories.

IMA D. EXAMINER
Computer Forensic Examiner

Released by _____

Case brief 2

A concerned citizen contacted the police department regarding possible stolen property. He told police that while he was searching the Internet, hoping to find a motorcycle for a reasonable price, he found an ad that met his requirements. This ad listed a Honda motorcycle for a low price, so he contacted the seller. Upon meeting the seller he became suspicious that the motorcycle was stolen. After hearing this information, police alerted the Auto Theft Unit. The Auto Theft Unit conducted a sting operation to purchase the motorcycle. Undercover officers met with the suspect, who, after receiving payment, provided them with the vehicle, a vehicle title, registration card, and insurance card. The suspect was arrested and the vehicle he was driving was searched incident to his arrest. During the search, a notebook computer was seized. Although the documents provided by the suspect looked authentic, document examiners determined that the documents were counterfeit. The auto theft investigator contacted the computer forensic laboratory for assistance in examining the seized computer. The investigator obtained a search warrant to analyze the computer and search for materials used in making counterfeit documents and other evidence related to the auto theft charges. The laptop computer was submitted to the computer forensic laboratory for analysis.

Objective: Determine if the suspect used the laptop computer as an instrument of the crimes of Auto Theft, Fraud, Forgery, Uttering False Documents, and Possession of Counterfeit Vehicle Titles and/or as a repository of data related to those crimes.

Computer type: Gateway Solo® 9100 notebook computer.

Operating system: Microsoft® Windows® 98.

Offenses: Auto Theft, Fraud, Forgery, Uttering False Documents, and Possession of Counterfeit Vehicle Titles.

Case agent: Auto Theft Unit Investigator.

Where examination took place: Computer Forensic Laboratory.

Tools used: Guidance Software™ EnCase®, DIGit®, Jasc Software™ Quick View Plus®, and AccessData™ Password Recovery Tool Kit™.

Processing

Assessment

1. Documentation provided by the investigator was reviewed.
 - a. Legal authority was established by a search warrant obtained specifically for the examination of the computer in a laboratory setting.
 - b. Chain of custody was properly documented on the appropriate departmental forms.
 - c. The request for service and a detailed summary explained the investigation, provided keyword lists, and provided information about the suspect, the stolen vehicle, the counterfeit documents, and the Internet advertisement. The investigator also provided photocopies of the counterfeit documents.

2. The computer forensic investigator met with the case agent and discussed additional investigative avenues and potential evidence being sought in the investigation.
3. Evidence intake was completed.
 - a. The evidence was marked and photographed.
 - b. A file was created and the case information was entered into the laboratory database.
 - c. The computer was stored in the laboratory's property room.
4. The case was assigned to a computer forensic investigator.

Imaging

1. The notebook computer was examined and photographed.
 - a. The hardware was examined and documented.
 - b. A controlled boot disk was placed in the computer's floppy drive. The computer was powered on and the BIOS setup program was entered. The BIOS information was documented and the system time was compared to a trusted time source and documented. The boot sequence was checked and documented; the system was already set to boot from the floppy drive first.
 - c. The notebook computer was powered off without making any changes to the BIOS.
2. EnCase® was used to create an evidence file containing the **image** of the notebook computer's hard drive.
 - a. The notebook computer was connected to a laboratory computer through a null-modem cable, which connected to the computers' parallel ports.
 - b. The notebook computer was booted to the DOS prompt with a controlled boot disk and EnCase® was started in server mode.
 - c. The laboratory computer, equipped with a magneto-optical drive for file storage, was booted to the DOS prompt with a controlled boot disk. EnCase® was started in server mode and evidence files for the notebook computer were acquired and written to magneto-optical disks.
 - d. When the imaging process was completed, the computers were powered off.
 - i. The notebook computer was returned to the laboratory property room.
 - ii. The magneto-optical disks containing the EnCase® evidence files were write-protected and entered into evidence.

Analysis

1. A laboratory computer was prepared with Windows® 98, EnCase® for Windows, and other forensic software programs.
2. The EnCase® evidence files from the notebook computer were copied to the laboratory computer's hard drive.
3. A new EnCase® case file was opened and the notebook computer's evidence files were examined using EnCase®.
 - a. Deleted files were recovered by EnCase®.
 - b. File data, including file names, dates and times, physical and logical size, and complete path, were recorded.
 - c. Keyword text searches were conducted based on information provided by the investigator. All hits were reviewed.
 - d. Graphics files were opened and viewed.
 - e. HTML files were opened and viewed.
 - f. Data files were opened and viewed; two password-protected and encrypted files were located.
 - g. Unallocated and slack space were searched.
 - h. Files of evidentiary value or investigative interest were copied/unerased from the EnCase® evidence file and copied to a compact disk.
4. Unallocated clusters were copied/unerased from the EnCase® evidence file to a clean hard drive, wiped to U.S. Department of Defense recommendations (DoD 5200.28-STD). DIGit® was then used to carve images from unallocated space. The carved images were extracted from DIGit®, opened, and viewed. A total of 8,476 images were extracted.
5. The password-protected files were copied/unerased to a 1.44 MB floppy disk. AccessData™ Password Recovery Tool Kit™ was run on the files and passwords were recovered for both files. The files were opened using the passwords and viewed.

Findings

The analysis of the notebook computer resulted in the recovery of 176 files of evidentiary value or investigative interest. The recovered files included:

1. 59 document files including documents containing the suspect's name and personal information; text included in the counterfeit documents; scanned payroll, corporate, and certified checks; text concerning and describing stolen items; and text describing the recovered motorcycle.

2. 38 graphics files including high-resolution image files depicting payroll, corporate, and certified checks; U.S. currency; vehicle titles; registration cards and driver's license templates from Georgia and other States; insurance cards from various companies; and counterfeit certified checks payable to a computer company ranging from \$25,000 to \$40,000 for the purchase of notebook computers. Most graphics were scanned.
3. 63 HTML files including Hotmail® and Yahoo® e-mail and classified advertisements for the recovered motorcycle, other vehicles, and several brands of notebook computers; e-mail text, including e-mails between the suspect and the concerned citizen concerning the sale of the recovered motorcycle; and e-mails between the suspect and a computer company concerning the purchase of notebook computers.
4. 14 graphics files carved from unallocated space depicting checks at various stages of completion and scanned images of U.S. currency.
5. Two password-protected and encrypted files.
 - a. WordPerfect® document containing a list of personal information on several individuals including names, addresses, dates of birth, credit card and bank account numbers and expiration dates, checking account information, and other information. Password [**nomoresecrets**].
 - b. Microsoft® Word document containing vehicle title information for the recovered motorcycle. Password [**HELLO**].

Documentation

1. Forensic Report – All actions, processes, and findings were described in a detailed Forensic Report, which is maintained in the laboratory case file.
2. Police Report – The case agent was provided with a police report describing the evidence examined, techniques used, and the findings.
3. Work Product – A compact disk containing files and file data of evidentiary value or investigative interest was created. The original was stored in the laboratory case file. Copies were provided to the case agent and the prosecutor.

Summary

Based on the information revealed by the computer analysis, several new avenues of investigation were opened.

- ✓ By contacting the victims listed in the password-protected WordPerfect® document, investigators learned that the victims had all been robbed in the same city during the previous summer by an individual meeting the description of the suspect.

- ✓ Contact with the computer company revealed the counterfeit checks found on the suspect's computer had been accepted for the purchase of computers, and that the computers were shipped to him and were the subject of an ongoing investigation. Model numbers and serial numbers provided by the computer company matched several of the Hotmail® and Yahoo® classified ads found on the suspect's computer.
- ✓ Several of the counterfeit checks found on the suspect's computer were already the subject of ongoing investigations.
- ✓ Information recovered concerning other vehicles led to the recovery of additional stolen vehicles.
- ✓ The specific information sought in the search warrant concerning the sale of the stolen motorcycle and the counterfeit documents was recovered from the suspect's computer.

Conclusion

The suspect eventually plead guilty and is now incarcerated.