MIS 5208 – Lecture 07 – Investigating Theft Acts (Part 1)

Ed Ferrara, MSIA, CISSP
eferrara@temple.edu

To the Student

- Investigation is one of the most interesting facets of being a fraud investigator. This chapter introduces you to the different methods used for investigation, from surveillance to invigilation to electronic and computer searches.

- As you read the chapter, think of where each method would be most useful, and consider the skills you need to master each one.

Learning Objectives

1. Understand the various ways frauds are investigated and when to use each investigation method.
2. Discuss theft investigation methods and how they are used to investigate suspected fraud.
3. Understand how to coordinate an investigation, using a vulnerability chart.
4. Describe the nature of surveillance and covert operations.
5. Understand the effectiveness of invigilation to investigate fraud.
6. Explain how to obtain physical evidence and how it can be used in a fraud investigation.
7. Understand how to seize and analyze electronic information from cell phones, hard drives, e-mail, social networking sites, and other sources.

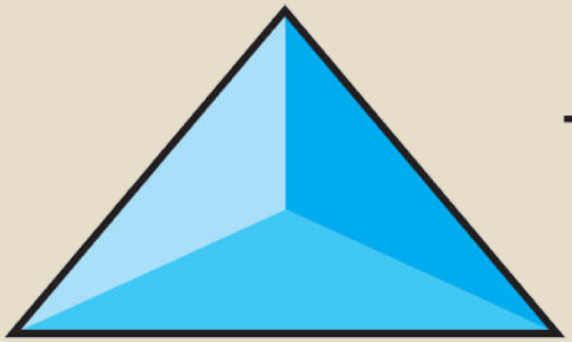
Fraud Investigation Methods

Theft Investigative Methods

1. Surveillance and covert operations
2. Invigilation
3. Seizing and searching computers
4. Physical evidence

Concealment Investigative Methods

1. Document examination
2. Audits
3. Electronic searches
4. Physical asset counts



Conversion Investigative Methods

1. Searching public records
2. Online resources
3. The net worth method

+

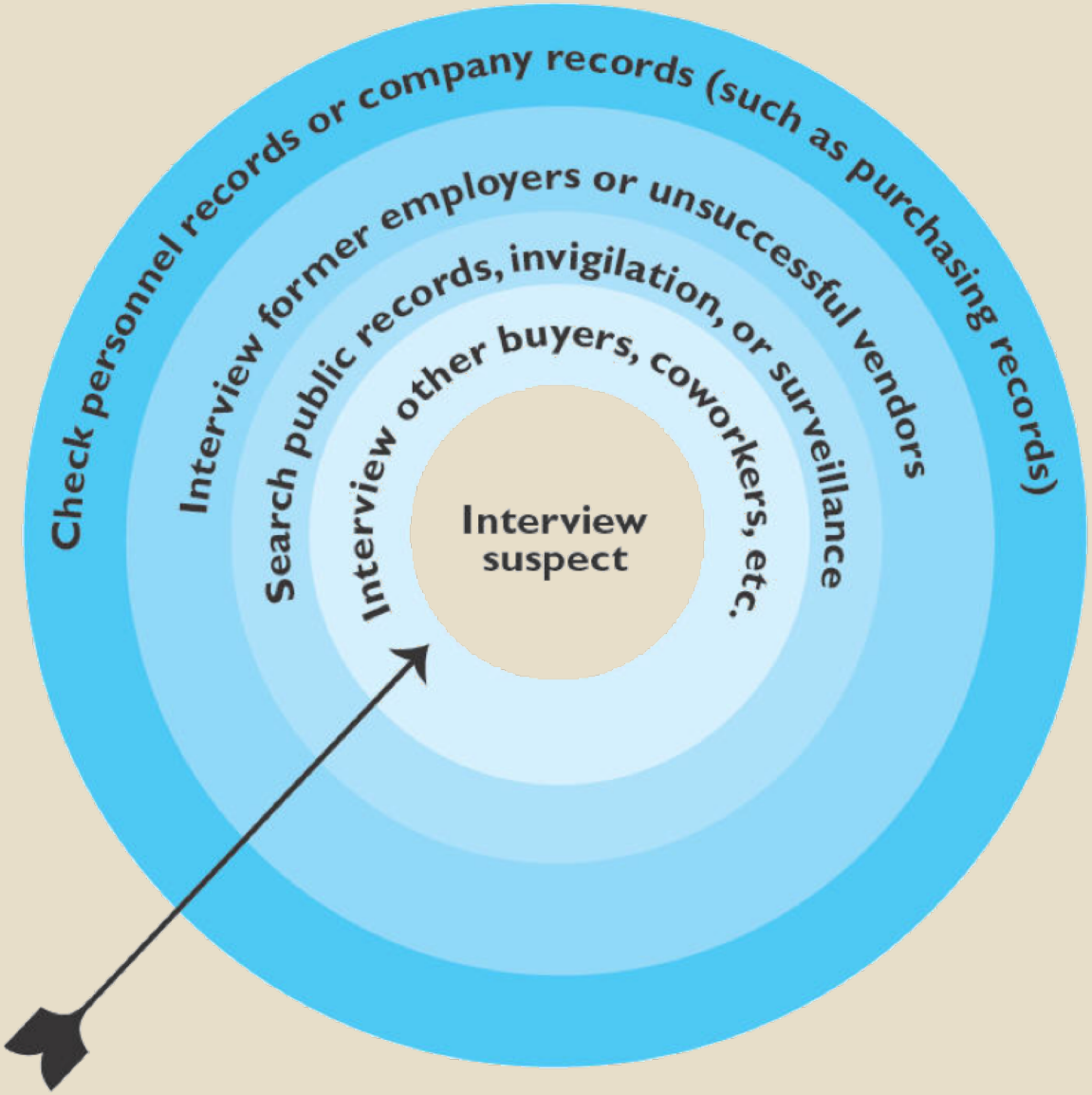
Inquiry Investigative Methods

1. Interviews and interrogation
2. Honesty testing

Theft Investigative Methods – Options

- Check the employee's personnel records for evidence of:
  - Liens
  - Financial Difficulties
  - Previous issues or problems
- Perform "special audits"
- Search the suspect's email and other electronic records for communication with outside vendors, worksheets, or other records:
  - Kickbacks
  - Gifts in kind
- Search public records and other sources to gather evidence about the subject's lifestyle
- Perform surveillance and other covert actions
- Interview former buyers and unsuccessful vendors
- Interview current buyers
- Simultaneously interview the suspected buyer and suspected vendor (looking for kickback payments)

Theft Act Investigative Pattern



Vulnerability Chart

1. Assets taken or missing
2. Individuals who had the opportunity to steal the missing materials
3. Theft investigation methods
4. Concealment possibilities
5. Conversion possibilities
6. Symptoms observed
7. Pressures on possible perpetrators
8. Rationalization of potential perpetrators
9. Key internal controls compromised during the event

Vulnerability Chart

Assets taken or missing	Individuals who had the opportunity to steal the missing materials	How Were Assets Moved?	How Was the Theft Concealed?	Conversion possibilities	Symptoms observed	Pressures on possible perpetrators	Rationaliza-tion of potential perpetrators	Key internal controls compromised during the event
Computer Deposit	Teller, Operations Officer, Proof Operator	Entering Verified Credits, Stealing Checks, Endorsing Stolen Checks	Destroying old or creating New Deposit Slips, Forged Signatures,	Unlimited	Change of Behavior, Change of Lifestyle, Customer Complaint	Tax Liens, New Homes, Divorce	Feels underpaid, Poorly treated	Use Processing Jacket Certification, Teller Counts Customers Receipts, Restrict Computer Access, Disallow Employees to Credit Their Own Accounts
Goods Delivered	Receiving Trucker	Assets Not Received (Truck)	Included in Trash	Fenced, Used Personally	Control Not Followed, Goods Not Counted	New Car, Spouse Laid Off, Personal Tragedy	Passed Over for Promotion	Receiving Reports
Goods Overcharge	Purchasing Agent	N/A	Kickback	Cash, Hire Spouse	Extravagant Lifestyle, Assets Sold Significantly Below Market Value	Maintain Lifestyle	Greed	Bids

Surveillance

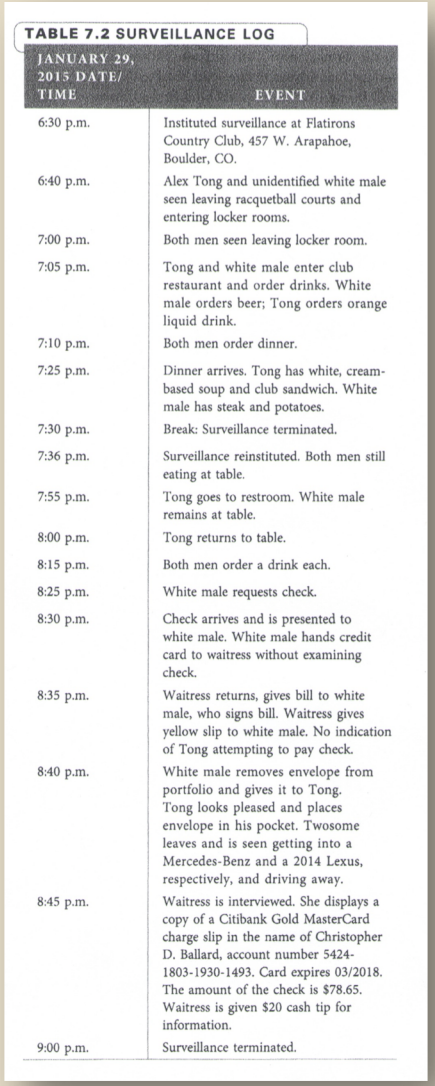


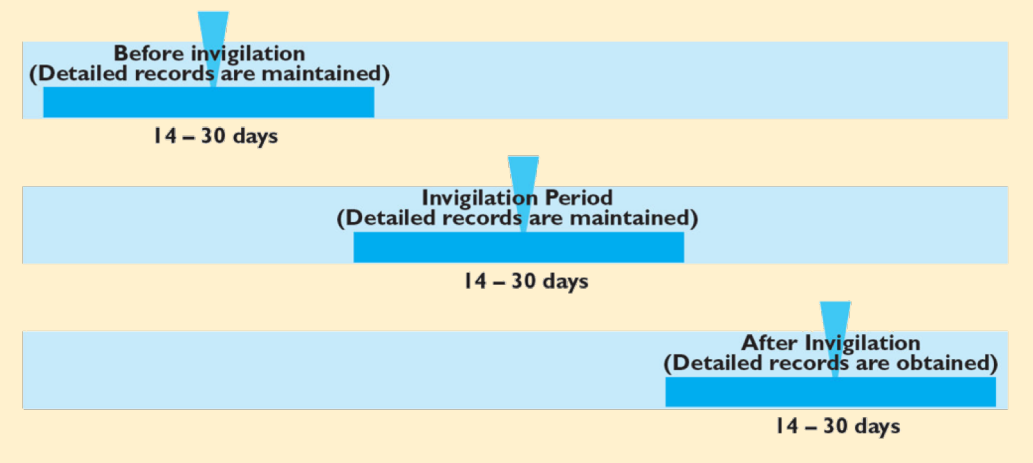
TABLE 7.2 SURVEILLANCE LOG

JANUARY 29, 2015 DATE/ TIME	EVENT
6:30 p.m.	Instituted surveillance at Flatirons Country Club, 457 W. Arapahoe, Boulder, CO.
6:40 p.m.	Alex Tong and unidentified white male seen leaving racquetball courts and entering locker rooms.
7:00 p.m.	Both men seen leaving locker room.
7:05 p.m.	Tong and white male enter club restaurant and order drinks. White male orders beer; Tong orders orange liquid drink.
7:10 p.m.	Both men order dinner.
7:25 p.m.	Dinner arrives. Tong has white, cream-based soup and club sandwich. White male has steak and potatoes.
7:30 p.m.	Break: Surveillance terminated.
7:36 p.m.	Surveillance reinstituted. Both men still eating at table.
7:55 p.m.	Tong goes to restroom. White male remains at table.
8:00 p.m.	Tong returns to table.
8:15 p.m.	Both men order a drink each.
8:25 p.m.	White male requests check.
8:30 p.m.	Check arrives and is presented to white male. White male hands credit card to waitress without examining check.
8:35 p.m.	Waitress returns, gives bill to white male, who signs bill. Waitress gives yellow slip to white male. No indication of Tong attempting to pay check.
8:40 p.m.	White male removes envelope from portfolio and gives it to Tong. Tong looks pleased and places envelope in his pocket. Twosome leaves and is seen getting into a Mercedes-Benz and a 2014 Lexus, respectively, and driving away.
8:45 p.m.	Waitress is interviewed. She displays a copy of a Citibank Gold MasterCard charge slip in the name of Christopher D. Ballard, account number 5424-1803-1930-1493. Card expires 03/2018. The amount of the check is $78.65. Waitress is given $20 cash tip for information.
9:00 p.m.	Surveillance terminated.

- Stationary
  - Anyone can do this
  - Record events occurring at a scene
  - Log includes time, place, and events
- Moving (Tailing)
  - More risk
  - Usually Experienced Professionals
- Electronic
  - Video Cameras
  - Wiretapping (law enforcement only)
  - Corporate policies:
    - All data on company owned including personal e-mail and documents are the property of the company
- Legality: Surveillance and covert operations are normally legal – provided that do not invade a "person's expectation of privacy".

Invigilation

- Theft act investigative technique – close supervision of suspects during an examination period.



An oil distributor was experiencing inventory losses of 0.23 percent of the inventory. The manager suspected that fraud was taking place but was not sure how or when. Observation and other investigative methods failed to produce evidence. For a 30-day period, the installation was saturated with security guards and auditors. Every movement of goods both in and out was checked, all documents were verified, and inventory and equipment were regularly reviewed. During the period of invigilation, losses ceased. After the invigilation, records kept at the plant were examined for absolute, proportional, and reasonableness changes during the invigilation period. Two service stations—which before the exercise had bought an average of only 2,000 gallons of gasoline a week—suddenly doubled their orders. During the 30 days, in fact, each received more than 19,000 gallons. In addition, a shift foreman, who in 23 years of service had taken no sick leave, was away from work on 19 of the 30 days. Two or three months were allowed to elapse, and during this time, covert observation was maintained on the service stations, whose orders by this time had reverted to 2,000 gallons per week. Using night vision equipment and cameras, unrecorded deliveries to the service stations were detected. The owners were interviewed, and their books were examined. They were subsequently charged with fraud extending back two years and involving 62,000 gallons of gasoline.

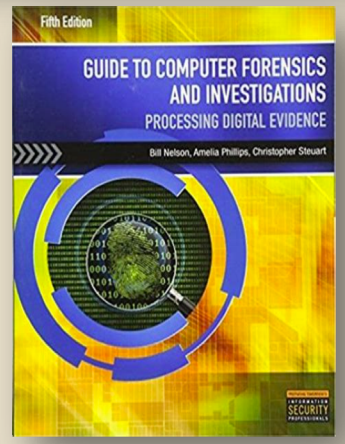
Theft Act Investigative Methods

Physical Evidence

Involves analyzing objects such as:

- Inventory, assets, and broken locks
- Substances such as grease and fluids
- Traces such as paints and stains
- Impressions such as cutting marks, tire tracks, and fingerprints

Or searching computers…



Theft Act Investigative Methods

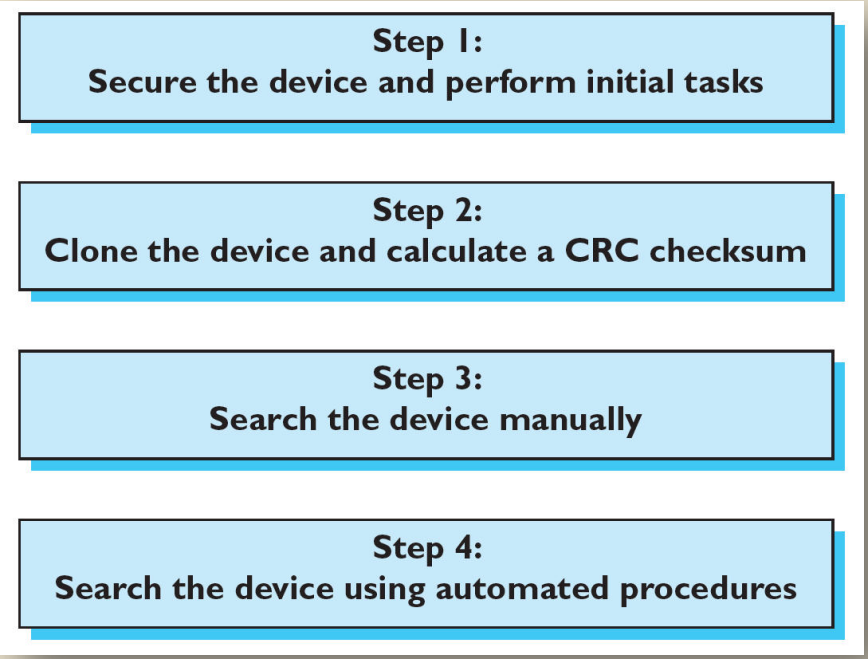
- E-mail Systems
  - Many copies may exist (sender, receiver, e-mail server)
  - Includes text messaging in certain countries
  - Web-based e-mail (Outlook.com, GMail, Yahoo! Mail) is more difficult to search

Digital Forensics

Objectives

- Explain the rules for controlling digital evidence
- Describe how to collect evidence at private-sector incident scenes
- Explain guidelines for processing law enforcement crime scenes
- List the steps in preparing for an evidence search
- Describe how to secure a computer incident or crime scene
- Explain guidelines for seizing digital evidence at the scene
- List procedures for storing digital evidence
- Explain how to obtain a digital hash
- Review a case to identify requirements and plan your investigation

Process for Gathering Electronic Evidence



- General tasks you perform in any computer forensics case:
  - Identify the case requirements
  - Plan your investigation
  - Conduct the investigation
  - Complete the case report
  - Critique the case

Identifying Digital Evidence

- **Digital evidence**
  - Can be any information stored or transmitted in digital form
- U.S. courts accept digital evidence as physical evidence
  - Digital data is treated as a tangible object
- Groups such as the **Scientific Working Group on Digital Evidence (SWGDE)** set standards for recovering, preserving, and examining digital evidence

Identifying Digital Evidence

- General tasks investigators perform when working with digital evidence:
  - Identify digital information or artifacts that can be used as evidence
  - Collect, preserve, and document evidence
  - Analyze, identify, and organize evidence
  - Rebuild evidence or repeat a situation to verify that the results can be reproduced reliably
- Collecting digital devices and processing a criminal or incident scene must be done systematically

Understanding Rules of Evidence

- Consistent practices help verify your work and enhance your credibility
- Comply with your state's rules of evidence or with the Federal Rules of Evidence
- Evidence admitted in a criminal case can be used in a civil suit, and vice versa
- Keep current on the latest rulings and directives on collecting, processing, storing, and admitting digital evidence

Understanding Rules of Evidence

- Data you discover from a forensic examination falls under your state's rules of evidence
  - Or the Federal Rules of Evidence (FRE)
- Digital evidence is unlike other physical evidence because it can be changed more easily
  - The only way to detect these changes is to compare the original data with a duplicate
- Most federal courts have interpreted computer records as hearsay evidence
  - Hearsay is secondhand or indirect evidence

Understanding Rules of Evidence

- Business-record exception
  - Allows “records of regularly conducted activity,” such as business memos, reports, records, or data compilations
- Generally, digital records are considered admissible if they qualify as a business record
- Computer records are usually divided into:
  - **Computer-generated records**
  - **Computer-stored records**

Understanding Rules of Evidence

- Computer and digitally stored records must be shown to be authentic and trustworthy
  - To be admitted into evidence
- Computer-generated records are considered authentic if the program that created the output is functioning correctly
  - Usually considered an exception to hearsay rule
- Collecting evidence according to the proper steps of evidence control helps ensure that the computer evidence is authentic

Understanding Rules of Evidence

- When attorneys challenge digital evidence
  - Often they raise the issue of whether computer-generated records were altered or damaged
- One test to prove that computer-stored records are authentic is to demonstrate that a specific person created the records
  - The author of a Microsoft Word document can be identified by using file metadata
- Follow the steps starting on page 141 of the text to see how to identify file metadata

Understanding Rules of Evidence

- The process of establishing digital evidence's trustworthiness originated with written documents and the "best evidence rule"
- Best evidence rule states:
  - To prove the content of a written document, recording, or photograph, ordinarily the original writing, recording, or photograph is required
- Federal Rules of Evidence
  - Allow a duplicate instead of originals when it is produced by the same impression as the original

Understanding Rules of Evidence

- As long as bit-stream copies of data are created and maintained properly
  - The copies can be admitted in court, although they aren't considered best evidence
- Example of not being able to use original evidence
  - Investigations involving network servers
  - Removing a server from the network to acquire evidence data could cause harm to a business or its owner, who might be an innocent bystander to a crime or civil wrong

Collecting Evidence -Private-Sector

- Private-sector organizations include:
  - Businesses and government agencies that aren't involved in law enforcement
- Non-government organizations (NGO) must comply with state public disclosure and federal Freedom of Information Act (FOIA) laws
  - And make certain documents available as public records
- FOIA allows citizens to request copies of public documents created by federal agencies

Collecting Evidence in Private-Sector Incident Scenes

- A special category of private-sector businesses includes ISPs and other communication companies
- ISPs can investigate computer abuse committed by their employees, but not by customers
  - Except for activities that are deemed to create an emergency situation
- Investigating and controlling computer incident scenes in the corporate environment
  - Much easier than in the criminal environment
  - Incident scene is often a workplace

Collecting Evidence in Private-Sector Incident Scenes

- Typically, businesses have inventory databases of computer hardware and software
  - Help identify the computer forensics tools needed to analyze a policy violation
    - And the best way to conduct the analysis
- Corporate policy statement about misuse of digital assets
  - Allows corporate investigators to conduct covert surveillance with little or no cause
  - And access company systems without a warrant

Collecting Evidence in Private-Sector Incident Scenes

- Companies should display a warning banner and publish a policy
  - Stating that they reserve the right to inspect computing assets at will
- Corporate investigators should know under what circumstances they can examine an employee's computer
  - Every organization must have a well-defined process describing when an investigation can be initiated

Collecting Evidence in Private-Sector Incident Scenes

- If a corporate investigator finds that an employee is committing or has committed a crime
  - Employer can file a criminal complaint with the police
- Employers are usually interested in enforcing company policy
  - Not seeking out and prosecuting employees
- Corporate investigators are, therefore, primarily concerned with protecting company assets

Collecting Evidence in Private-Sector Incident Scenes

- If you discover evidence of a crime during a company policy investigation
  - Determine whether the incident meets the elements of criminal law
  - Inform management of the incident
  - Stop your investigation to make sure you don't violate Fourth Amendment restrictions on obtaining evidence
  - Work with the corporate attorney on how to respond to a police request for more information

Processing Law Enforcement Crime Scenes

- You must be familiar with criminal rules of search and seizure
- You should also understand how a search warrant works and what to do when you process one
- Law enforcement officer may search for and seize criminal evidence only with **probable cause**
  - Refers to the standard specifying whether a police officer has the right to make an arrest, conduct a personal or property search, or obtain a warrant for arrest

Processing Law Enforcement Crime Scenes

- With probable cause, a police officer can obtain a search warrant from a judge
  - That authorizes a search and seizure of specific evidence related to the criminal complaint
- The Fourth Amendment states that only warrants "particularly describing the place to be searched, and the persons or things to be seized" can be issued

Understanding Concepts and Terms Used in Warrants

- **Innocent information**
  - Unrelated information
  - Often included with the evidence you're trying to recover
- Judges often issue a **limiting phrase** to the warrant
  - Allows the police to separate innocent information from evidence

Concepts and Terms Used in Warrants

- **Plain view doctrine**
  - Objects falling in plain view of an officer who has the right to be in position to have that view are subject to seizure without a warrant and may be introduced in evidence
  - Three criteria must be met:
    - Officer is where he or she has a legal right to be
    - Ordinary senses must not be enhanced by advanced technology in any way
    - Any discovery must be by chance

Understanding Concepts and Terms Used in Warrants

- The plain view doctrine's applicability in the digital forensics world is being rejected
- Example - In a case where police were searching a computer for evidence related to illegal drug trafficking:
  - If an examiner observes an .avi file and find child pornography, he must get an additional warrant or an expansion of the existing warrant to continue the search for child pornography

Preparing for a Search

- Preparing for a computer search and seizure
  - Probably the most important step in computing investigations
- To perform these tasks
  - You might need to get answers from the victim and an informant
    - Who could be a police detective assigned to the case, a law enforcement witness, or a manager or coworker of the **person of interest** to the investigation

Identifying the Nature of the Case

- When you're assigned a digital investigation case
  - Start by identifying the nature of the case
    - Including whether it involves the private or public sector
- The nature of the case dictates how you proceed
  - And what types of assets or resources you need to use in the investigation

Identifying the Type of OS or Digital Device

- For law enforcement
  - This step might be difficult because the crime scene isn't controlled
- If you can identify the OS or device
  - Estimate the size of the drive on the suspect's computer
    - And how many devices to process at the scene
- Determine which OSs and hardware are involved

Can You Seize Computers and Digital Devices

- The type of case and location of the evidence
  - Determine whether you can remove digital evidence
- Law enforcement investigators need a warrant to remove computers from a crime scene
  - And transport them to a lab
- If removing the computers will irreparably harm a business
  - The computers should not be taken offsite

Determining Whether You Can Seize Computers and Digital Devices

- Additional complications:
  - Files stored offsite that are accessed remotely
  - Availability of cloud storage, which can't be located physically
    - Stored on drives where data from many other subscribers might be stored
- If you aren't allowed to take the computers to your lab
  - Determine the resources you need to acquire digital evidence and which tools can speed data acquisition

Getting a Detailed Description of the Location

- Get as much information as you can about the location of a digital crime
- Identify potential hazards
  - Interact with your HAZMAT (hazardous materials) team
- HAZMAT guidelines
  - Put the target drive in a special HAZMAT bag
  - HAZMAT technician can decontaminate the bag
  - Check for high temperatures

Determining Who Is in Charge

- Corporate computing investigations
  - Usually require only one person to respond to an incident
- Law enforcement agencies
  - Typically handle large-scale investigations
- Designate lead investigators in large-scale investigations
  - Anyone assigned to the scene should cooperate with the designated leader to ensure the team addresses all details when collecting evidence

Using Additional Technical Expertise

- Determine whether you need specialized help to process the incident or crime scene
- You may need to look for specialists in:
  - OSs
  - RAID servers
  - Databases
- Finding the right person can be a challenge
- Educate specialists in investigative techniques
  - Prevent evidence damage

Determining the Tools You Need

- Prepare tools using incident and crime scene information
- Create an initial-response field kit
  - Should be lightweight and easy to transport
- Create an extensive-response field kit
  - Includes all tools you can afford to take to the field
  - When at the scene, extract only those items you need to acquire evidence

Determining the Tools You Need

Digital forensics kit

Laptop computer

Digital camera

Flashlight

Figure 4-4 Items in an initial-response field kit

Determining the Tools You Need

Table 4-1 Tools in an initial-response field kit

Number needed	Tools
1	Small computer toolkit
1	Large-capacity drive
1	IDE ribbon cable (ATA-33 or ATA-100)
1	SATA cables
1	Forensic boot media containing an acquisition utility
1	Laptop IDE 40- to 44-pin adapter, other adapter cables
1	Laptop or tablet computer
1	FireWire or USB dual write-protect external bay
1	Flashlight
1	Digital camera with extra batteries or 35mm camera with film and flash
10	Evidence log forms
1	Notebook or digital dictation recorder
10	Computer evidence bags (antistatic bags)
20	Evidence labels, tape, and tags
1	Permanent ink marker
10	External USB devices or a portable hard drive

Determining the Tools You Need

Table 4-2 Tools in an extensive-response field kit

Number needed	Tools
Varies	Assorted technical manuals, ranging from OS references to forensic analysis guides
1	Initial-response field kit
1	Laptop or tablet with cables and connectors
2	Electrical power strips
1	Additional hand tools, including bolt cutters, pry bar, and hacksaw
1	Leather gloves and disposable latex gloves (assorted sizes)
1	Hand truck and luggage cart
10	Large garbage bags and large cardboard boxes with packaging tape
1	Rubber bands of assorted sizes
1	Magnifying glass
1	Ream of printer paper
1	Small brush for cleaning dust from digital devices
10	USB drives of varying sizes
2	External hard drives (1 TB or larger) with power cables
Assorted	Converter cables
5	Additional assorted hard drives or flash drives for data acquisition

Thank you