DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING

CCS

FALL 2022-2023

CYBER FORENSICS

CSE2037 – 2 2 3 – 5th Semester

PRESIDENCY UNIVERSITY

Private University Estd. in Karnataka State by Act No. 41 of 2013

40 YEARS OF ACADEMIC WISDOM

Module 1

DIGITAL INVESTIGATION

Outline

- Digital Evidence and Computer Crime
- History and Terminology of Computer Crime Investigation
- Technology and Law
- The Investigative Process
- Investigative Reconstruction
- Modus Operandi, Motive and Technology
- Digital Evidence in the Courtroom.

COMPUTER CRIME

- Computer crime and computer-supported criminal activities are booming businesses.
- Criminals, fraudsters, and terrorists seem to strike whenever there is an opportunity.
- Case Study: In January of 2005 the FBI alerted the public to a variety of scams being facilitated online involving the solicitation of additional relief funds for the victims of the recent tsunami disaster. The FBI, through the Internet Crime Complaint Center (IC3), had received reports of Web sites being established purportedly to assist with collection and relief efforts. Complaints identified several schemes that involved both unsolicited incoming emails (SPAM), as well as reports of responses to posted email addresses, to assist for a fee in locating loved ones who may have been victims of the disaster. A fraudulent relief donation Web site has also been detected containing an embedded Trojan exploit which can infect the user's computer with a virus if accessed.

DIGITAL EVIDENCE

- Digital evidence is **information stored or transmitted in binary form that may be relied on in court**. It can be found on a computer hard drive, a mobile phone, among other places.
- Sources of Digital Evidence - **email, text messages, instant messages, files and documents extracted from hard drives, electronic financial transactions, audio files, and video files**.

ROLE OF COMPUTER?

- The use of software may be utilized to **copy usernames and passwords to access private or protected information**. This permits these individuals to peruse systems, websites, databases and other areas of a company or area of the internet. Once information has been stolen and copied, it may be used to commit many crimes.

HISTORY & TERMINOLOGY OF COMPUTER CRIME INVESTIGATION

- The continuing technological revolution in communications and information exchange has created an entirely new form of crime: cyber crime or computer crime.
- Computer crime has forced the computer and law enforcement professions to develop new areas of expertise and avenues of collecting and analyzing evidence. This is what has developed into the science of computer forensics.
- The process of acquiring, examining, and applying digital evidence is crucial to the success of prosecuting a cyber criminal.
- With the continuous evolution of technology, it is difficult for law enforcement and computer professionals to stay one step ahead of technologically savvy criminals. To effectively combat cyber crime, greater emphasis must be placed in the computer forensic field of study, including but not limited to financial support, international guidelines and laws, and training of the professionals involved in the process

- Recently a survey was conducted to determine where the FBI was focusing their computer forensic efforts.
- An alarming 74% of their workload is centered on white collar crime. This type of crime includes health care fraud, government fraud including erroneous IRS and Social Security benefit payments, and financial institution fraud. These are high-dollar crimes made easy by technology.
- The other 26% of the workload is split equally among violent crime (child pornography, interstate theft), organized crime (drug dealing, criminal enterprise), and counter terrorism and national security.
- As shown by this survey, computer crime is widespread and has infiltrated areas unimaginable just a few years ago. The FBI caseload has gone from near zero in 1985 to nearly 10,000 cases in 2003. It is no doubt considerably higher today.
- They have gone from two part-time scientists to 899 personnel in regional field offices throughout the country. Technology has brought this field of study to the forefront.

TECHNOLOGY & LAW

- Defensive information technology will ultimately benefit from the availabilIty of cyber forensic evidence of malicious activity. Criminal investigators rely on recognized scientific forensic disciplines, such as medical pathology, to provide vital information used in apprehending criminals and determining their motives. Today, an increased opportunity for cyber crime exists, making advances in the law enforcement, legal, and forensic computing technical arenas imperative.
- Cyber forensics is the discovery, analysis, and reconstruction of evidence extracted from any element of computer systems, computer networks, computer media, and computer peripherals that allow investigators to solve a crime. Cyber forensics focuses on real-time, online evidence gathering rather than the traditional offline computer disk forensic technology

HI-TEC CRIME

- crimes that use electronic and digitally based technology to attack computers or a computer network.
- Such crimes include the hacking of computers or any unauthorized use or distribution of data, denial of service attacks and distribution of computer viruses.
- High-tech criminals use a suite of malware tools, ranging from banking trojans to ransomware and phishing, to stage their attacks.
- Malware, or malicious software, infiltrates and gains control over a computer system or a mobile device to steal valuable information or damage data. There are many types of malware, and they can complement each other when performing an attack.

- **Adware** displays advertising banners or pop-ups that include code to track the user's behavior on the internet.
- A **backdoor/remote-access trojan (RAT)** accesses a computer system or mobile device remotely. It can be installed by another piece of malware. It gives almost total control to the attacker, who can perform a wide range of actions, including:
    - monitoring actions
    - executing commands
    - sending files and documents back to the attacker
    - logging keystrokes
    - taking screen shots
- A **botnet** (short for robot network) is made up of computers communicating with each other over the internet. A command and control center uses them to send spam, mount distributed denial-of-service (DDoS) attacks and commit other crimes.
- A **file infector** infects executable files (such as .exe) by overwriting them or inserting infected code that disables them.
- **Ransomware** stops users from accessing their devices and demands that they pay a ransom through certain online payment methods to regain access. A variant, police ransomware, uses law enforcement symbols to lend authority to the ransom message.

- **Scareware** is fake anti-virus software that pretends to scan and find malware/security threats on a user's device so that they will pay to have it removed.
- **Spyware** is installed on a computer without its owner's knowledge to monitor their activity and transmit the information to a third party.
- A **rootkit** is a collection of programmes that enable administrator-level access to a computer or computer network, thus allowing the attacker to gain root or privileged access to the computer and possibly other machines on the same network.
- A **trojan** poses as, or is embedded within, a legitimate programme, but it is designed for malicious purposes, such as spying, stealing data, deleting files, expanding a botnet, and performing DDoS attacks.
- A **worm** replicates itself over a computer network and performs malicious actions without guidance.

- The theft and resale of personal and corporate data could be the goal of cybercriminals.
- In India, cyber crimes are covered by the Information Technology Act, 2000 and the Indian Penal Code, 1860. It is the Information Technology Act, 2000, which deals with issues related to cyber crimes and electronic commerce. However, in the year 2008, the Act was amended and outlined the definition and punishment of cyber crime. Several amendments to the Indian Penal Code 1860 and the Reserve Bank of India Act were also made.

INVESTIGATIVE PROCESS

1. Assess the Situation

- As with any investigation, the officer must first determine the specific elements of the crime and whether the laws in their jurisdiction support prosecution. For example, can the charges be sustained even if guilt is proven? Given the many new technologies in use, very often common law, and federal and state statutes have not caught up to the offenses. Another factor to consider when investigating cyber crimes is the global nature of the Internet. It is often beneficial to consult with your prosecutor to gain additional insight into specific crimes.

2. CONDUCT THE INITIAL INVESTIGATION

- When conducting a cybercrime investigation, normal investigative methods are still important. Asking who, what, where, when, why and how questions is still important. The investigator should also still ask the following questions:
  - Who are the potential suspects?
  - What crimes were committed?
  - When were the crimes committed?
  - Were these crime limited to US jurisdiction?
  - What evidence is there to collect?
  - Where might the physical and digital evidence be located?
  - What types of physical and digital evidence were involved with the crime?
  - Does any of the evidence need to be photographed/preserved immediately?
  - How can the evidence be preserved and maintained for court proceedings?

3. INVESTIGATIVE RECONSTRUCTION

- Reconstruction refers to the systematic process of piecing together evidence and information gathered during an investigation to gain a better understanding of what transpired between the victim and the offender during a crime.
- A core tenet of this process is that, when they commit a crime, criminals leave an imprint of themselves at the scene. This is provided by Locard's Exchange Principle, which states that when any two objects come in contact, there is a cross-transfer.
- Footwear impressions, fingerprints, and DNA from bloodstain patterns are clear examples of imprints left by an offender at a crime scene. Reconstruction involves taking physical imprints a step further, using them to infer offense related behavior, or *behavioral imprints.* For example, footwear impressions show who walked on a particular surface (and perhaps even when), fingerprints show who touched a particular object, and DNA from bloodstain patterns can demonstrate who bled where, when, and in what sequence.

IDENTIFY POSSIBLE EVIDENCE

- Digital evidence can come in many file types and sizes. For example, see *Most Common Electronic Devices*. Further, the evidence may be encrypted, protected, or otherwise hidden. If your agency does not have the resources, tools, or specific expertise necessary to identify and collect this evidence, consider partnering with other agencies that do have these capabilities. See the *Community page* for more information.

SECURE DEVICES AND OBTAIN COURT ORDERS

- In many cases, investigators may seize electronic devices without a warrant, but must obtain a warrant in order to conduct a search on the device(s). Multiple warrants may need to be obtained if a particular device is connected to multiple crimes.
- Warrants should clearly describe all files, data, and electronic devices to be searched as specifically as possible and seek approval to conduct analysis off-site (e.g. at a specialized forensics laboratory).
- Subpoenas can also be used to obtain digital evidence. Many Internet- and communication-based companies have guides to assist law enforcement in understanding their information sharing policies (see *Handling Evidence from Specific Sources*).
- Non-disclosure agreement (NDA) are often times needed when law enforcement is requesting information from an Electronic Service Provider (ESP) and they don't want the ESP to notify the user of someone requesting information from their account.
- Court order is required to compel the ESP for information above the basic subscriber information. This could include but not limited to message headers or IP addresses. This does not include content.

ANALYZE RESULTS WITH PROSECUTOR

- It will also be important to work with the prosecutor to identify the appropriate charges (based on existing common law and state and federal statutes), and to determine what additional information or evidence will be needed prior to filing charges.

CASE STUDY

- In July 2021, hackers targeted Kaseya, a U.S. information technology firm, in a ransomware attack that affected up to 1,500 businesses worldwide, from the U.S. to Sweden to New Zealand. The hackers demanded $70 million to restore the impacted services. Nearly every type of organization — from public schools and health services systems to oil pipelines and beef processing plants — has fallen victim to this type of attack in 2021.

- https://www.youtube.com/watch?v=hClc3QNCh2E
- https://www.youtube.com/watch?v=1mTviSphUDU

Module 2

UNDERSTANDING INFORMATION

Outline

- Methods of storing data: number systems, character codes, record structures, file formats and file signatures
- Word processing and graphic file formats
- Structure and Analysis of Optical Media Disk Formats
- Recognition of file formats and internal buffers
- Extraction of forensic artifacts
- Understanding the dimensions of other latest storage devices – SSD Devices.

DATA STORAGE

- Files and documents are recorded digitally and saved in a storage system for future use.
- Storage systems may rely on electromagnetic, optical or other media to preserve and restore the data if needed.
- Data storage makes it easy to back up files for safekeeping and quick recovery in the event of an unexpected computing crash or cyberattack.
- Data storage can occur on physical hard drives, disk drives, USB drives or virtually in the cloud. The important thing is that your files are backed up and easily available should your systems ever crash beyond repair.
- Some of the most important factors to consider in terms of data storage are reliability, how robust the security features tend to be and the cost to implement and maintain the infrastructure. Browsing through different data storage solutions and applications can help you arrive at the choice that is the best fit for your business' needs.

TYPES OF DATA STORAGE

- Direct Attached Storage (DAS)
  - Hard Drives
  - Solid-State Drives (SSD)
  - CD/ DVD Drives
  - Flash Drives
  - And More
- DAS solutions are great for creating local backups and can be more affordable than NAS solutions, but sharing data between machines can be cumbersome.

- Network Attached Storage (NAS)
  - allows for multiple machines to share storage over a network. This is accomplished with multiple hard drives or other storage devices in a RAID configuration. One of the key benefits of NAS is the ability to centralize data and improve collaboration. Data can be easily shared among connected machines, and permission levels can be set to control access. While NAS solutions tend to be more costly than DAS solutions, they are still very affordable as storage technology has advanced significantly.

METHODS OF STORING DATA

- Number Systems
  - Decimal Numbering System (base 10)
  - Binary Numbering System (base 2)
  - Hexadecimal Numbering System
- Character Codes
  - UTF-8
  - UTF-16
  - UTF-32

- Record Structures
  - A record is **a database entry that may contain one or more values**. Groups of records are stored in a table, which defines what types of data each record may contain. Databases may contain multiple tables which may each contain multiple records.
- File formats
  - A **file format** is a standard way that information is encoded for storage in a computer file. It specifies how bits are used to encode information in a digital storage medium. File formats may be either proprietary or free.

- Some file formats are designed for very particular types of data: PNG files, for example, store bitmapped images using lossless data compression.
- Other file formats, however, are designed for storage of several different types of data: the Ogg format can act as a container for different types of multimedia including any combination of audio and video, with or without text (such as subtitles), and metadata.
- A text file can contain any stream of characters, including possible control characters, and is encoded in one of various character encoding schemes.
- Some file formats, such as HTML, scalable vector graphics, and the source code of computer software are text files with defined syntaxes that allow them to be used for specific purposes.
- JPEG (Joint Photographic Experts Group), PNG (Portable Network Graphics), GIF (Graphics Interchange Format), PDF (Portable Document Format), SVG (Scalable Vector Graphics), MP4 (Moving Picture Experts Group) etc.

- File Signatures - is a unique sequence of identifying bytes written to a file's header.
  - On a Windows system, a file signature is normally contained within the first 20 bytes of the file. Different file types have different file signatures
  - for example, a Windows Bitmap image file (.bmp extension) begins with the hexadecimal characters *42 4D* in the first 2 bytes of the file, characters that translate to the letters “BM.”
  - Most Windows-based malware specimens are executable files, often ending in the extensions.exe, .dll, .com, .pif, .drv, .qtx, .qts, ocx, or .sys. The file signature for these files is “MZ,” or the hexadecimal characters *4D 5A*, found in the first 2 bytes of the file. Humorously, the letters “MZ” are the initials for Mark Zbikowski, one of the principal architects of MS-DOS and the Windows/DOS executable file format.

- Word processing and Graphic file formats
  - A word processing file contains user information in **plain text or rich text format.** A plain text file format contains unformatted text and no font or page settings etc.
  - Graphic images are stored digitally using a small number of standardized graphic file formats, including **bit map, TIFF, JPEG, GIF, PNG**; they can also be stored as raw, unprocessed data.
- Structure and Analysis of Optical Media Disk Formats
  - There are three main types of optical media: **CD, DVD, and Blu-ray disc.** CDs can store up to 700 MB (megabytes) of data, and DVDs can store up to 8.4 GB (gigabytes) of data. Blu-ray discs, which are the newest type of optical media, can store up to 50 GB of data.

Optical Disk

- Optical disks rely on a red or blue laser to record and read data. Most of today's optical disks are flat, circular and 12 centimeters in diameter. Data is stored on the disk in the form of microscopic data pits and lands. The pits are etched into a reflective layer of recording material. The lands are the flat, unindented areas surrounding the pits.

- The type of material selected for the recording material depends on how the disk is used. Prerecorded disks such as those created for audio and video recordings can use cheaper material like aluminum foil. Write-once disks and rewritable disks require a more expensive layer of material to accommodate other types of digital data storage.
- Data is written to an optical disk in a radial pattern starting near the center. An optical disk drive uses a laser beam to read the data from the disk as it is spinning. It distinguishes between the pits and lands based on how the light reflects off the recording material. The drive uses the differences in reflectivity to determine the 0 and 1 bits that represent the data.

Optical disk vs. magnetic storage media

- When first introduced for commercial use, the optical disk could hold much more data than similarly sized magnetic storage media, but improvements in hard disk drive (HDD) technology led to HDDs with much greater capacities on a per-centimeter basis than could be achieved with optical disks. At the same time, solid-state memory technologies continued to improve in both capacity and endurance, while prices steadily dropped.

- However, optical disks have one big advantage over other types of storage: durability. Optical storage is less likely to degrade over time compared to magnetic tape, HDDs or solid-state drives (SSDs). The data stored on them is relatively impervious to most environmental threats, such as power surges or magnetic disturbances. Not only does this make optical disks well suited for prerecorded audio and video content, but also for backing up and archiving data, including cold storage.

FORENSIC ARTIFACTS

- Traces are the tiny pieces left behind that forensic investigators use to help determine in a given situation *what* happened, *where* it happened, *who* it happened to, *when* it happened, and *how* it happened, and who did it.
- Like the footprints, DNA, fingerprints, or the blood Kirk's example criminal left behind, **forensic artifacts** are the digital equivalent–the things left behind unintentionally, unconsciously, often invisibly, that help us get to the bottom of an incident. An artifact in a digital forensics investigation includes things like registry keys, files, timestamps, and event logs – all of these are the traces we follow in digital forensic work.
- Every form of storage, every different file system, and every different operating system works differently and creates different artifacts as a response to what you do while using it. These artifacts are tiny and invisible, although you see their effects every time you access a computer system, a network, a phone, or a tablet. You'd be surprised at what we can learn about the behavior of somebody accessing your device just by looking at the artifacts they leave behind!

- Here are just a few of the artifacts:
  - Smartphone User Dictionaries
  - Smartphone Context Log-0 (Samsung)
  - SQLite database files
  - $Logfile Artifacts
  - Link Files
  - Shell Bags
  - Prefetch Files
  - Amcache Artifacts

TYPES OF DATA STORAGE DEVICES

- SSD Flash Drive Arrays
- Hybrid Flash Arrays
- Hybrid Cloud Storage
- Backup Software
- Backup Appliances
- Cloud Storage

OTHER EMERGING DATA STORAGE TRENDS

- **Cloud storage that is accessible from different devices** for users is another growing segment that shows promise to become even faster and more efficient.
- **Flash storage and flash storage chips within SSD drives** are being developed as a storage option on which you can rely.
- **Artificial Intelligence (AI)** is also becoming more prevalent in newer types of data storage to handle repetitious tasks, such as managing backup schedules and setting custom recovery points for specific data sets.

Module 3

COMPUTER BASICS FOR DIGITAL INVESTIGATORS

PRESIDENCY UNIVERSITY
Private University Estd. in Karnataka State by Act No. 41 of 2013
40 YEARS OF ACADEMIC WISDOM

Outline

- Computer Forensic Fundamentals
- Information Warfare
- Computer Forensic Cases

APPLYING FORENSIC SCIENCE TO COMPUTERS

- Computer forensics is the **application of investigation and analysis techniques to gather and preserve evidence from a particular computing device in a way that is suitable for presentation in a court of law.**
- Steps involved
  - Preparation
  - Survey
  - Documentation
  - Preservation
  - Examination & Analysis
  - Reconstruction
  - Reporting

PREPARATION

- Planning is especially important in cases that involve computers. Whenever possible, while generating a search warrant, the search site should be researched to determine what computer equipment to expect, what the systems are used for, and if a network is involved. If the computers are used for business purposes or to produce publications, this will influence the authorization and seizure process. Also, without this information, it is difficult to know what expertise and evidence collection tools are required for the search. If a computer is to be examined on-site, it will be necessary to know which operating system the computer is running (e.g., Mac OS, UNIX, or Windows). It will also be necessary to know if there is a network involved and if the cooperation of someone who is intimately familiar with the computers will be required to perform the search.
- Before the search begins, the search leader should prepare a detailed plan for documenting and preserving electronic evidence, and should take time to brief carefully the entire search team to protect both the identity and integrity of all the data. At the scene, agents must remember to collect traditional types of evidence (e.g. latent fingerprints off the keyboard) before touching anything.

- If the assistance of system administrators or other individuals who are familiar with the system to be searched is required, they should be included in a pre-search briefing. They might be able to point out oversights or potential pitfalls. One person should be designated to take charge of all evidence to simplify the chain of custody. Such coordination is especially valuable when dealing with large volumes of data in various locations, ensuring that important items are not missed. In situations where there is only one chance to collect digital evidence, the process should be practiced beforehand under similar conditions to become comfortable with it.

- A final preparatory consideration is regarding proper equipment. Most plans and procedures will fail if adequate acquisition systems and storage capacity are not provided. Some of the fundamental items that can be useful when dealing with computers as a source of evidence include the following:
  - Evidence bags, tags, and other items to label and package evidence
  - Digital camera to document scene and evidential items
  - Forensically sanitized hard drives to store acquired data
  - Forensically prepared computer(s) to connect with and copy data from evidential hard drives onto forensically sanitized hard drives
  - Hardware write blockers for commonly encountered hard drives (e.g., IDE and SATA)
  - Toolkit, including a flashlight, needle-nose pliers, and screwdrivers for various types and sizes of screws.

- Specific circumstances will dictate the need for more specialized equipment such as forensic boot disks and crossover cables to acquire forensic duplicates of systems when the hard drive cannot be removed (e.g., mini laptop or large servers). When acquiring large amounts of data from servers, it may be prudent to bring a portable RAID storage system to the scene to ensure that there is sufficient space to store all of the acquired data and to reduce the risk of losing any of the acquired data because of hard drive failures.

SURVEY

- surveying a crime scene is a methodical process of finding all potential sources of digital evidence and making informed, reasoned decisions about what digital evidence to preserve. One effective approach to conducting a methodical crime scene survey is to divide the area into a grid and inspect each segment of the grid thoroughly. By dividing the larger area into smaller segments, there is less chance of overlooking important items such as a small memory card or hidden pieces of storage media. This concept can be applied to both the physical area and digital realm.
- surveying a crime scene for potential sources of digital evidence is a twofold process.
  - First, digital investigators have to recognize the hardware (e.g., computers, removable storage media, and network cables) that contains digital information.
  - Second, digital investigators must be able to distinguish between irrelevant information and the digital data that can establish that a crime has been committed or can provide a link between a crime and its victim or a crime and its perpetrator. During a search, manuals and boxes related to hardware and software can give hints of what hardware, software, and Internet services might be installed/used.

SURVEY OF HARDWARE

- There are many computerized products that can hold digital evidence such as telephones, mobile devices, laptops, desktops, larger servers, mainframes, routers, firewalls, and other network devices. There are also many forms of storage media including compact disks, floppy disks, magnetic tapes, high capacity flip, zip, and jazz disks, memory sticks, and USB storage devices
- Digital investigators should look for more than the obvious computer systems. Less obvious sources of digital evidence include the following:
  - Gaming systems (e.g., PS3 and XBox360), which can contain a variety of multimedia and may be configured to run a fully functional operating system such as Linux;
  - Video cameras (camcorders and CCTV), which may store files on internal memory, on removable storage media, or on a central server;
  - Removable memory cards from digital cameras and mobile devices, which are growing in storage capacity while shrinking in size, and are easily overlooked;
  - Printers with an internal hard drive;
  - Digital picture frames;
  - Nonstandard peripherals connected to computers such as an antenna or customized circuit board.

SURVEY OF DIGITAL EVIDENCE

- Different crimes result in different types of digital evidence. For example, cyber-stalkers often use e-mail to harass their victims, computer crackers sometimes inadvertently leave evidence of their activities in log files, and child pornographers sometimes have digitized images stored on their computers. Additionally, operating systems and computer programs store digital evidence in a variety of places. Therefore, the ability to identify evidence depends on a digital investigator's familiarity with the type of crime that was committed and the operating system(s) and computer program(s) that are involved.
- In addition to looking for user-created documents and multimedia on storage media, digital investigators may find relevant information in the Registry, log files, and artifacts associated with applications used on the computer (e.g., logs of instant messaging chat, and files exchanged using P2P programs).
- Again, the different kinds of digital evidence on a computer are limited only by the user's activities and creativity

DOCUMENTATION

- Documentation is essential at all stages of handling and processing digital evidence, and includes the following:
  - Chain of custody: who handled the evidence, when, where, and for what purpose;
  - Evidence intake: characteristics of each evidential item such as make, model, and serial number;
  - Photos, videos, and diagrams: capturing the context of the original evidence;
  - Evidence inventory: a list or database of all evidential items;
  - Preservation guidelines: a repeatable process for preserving digital evidence, which may contain references to specific tools;
  - Preservation notes: notation of steps taken to preserve each evidential item and any necessary deviations from the preservation guideline documentation;
  - Forensic examination guidelines: a repeatable process for examining digital evidence, which may contain references to specific tools;
  - Forensic examination notes: notation of actions taken to examine each evidential item, including a summary of the outcome of each action and details about important findings.

DIGITAL EVIDENCE FORM	
Investigator's Name and Association: Eoghan Casey Knowledge Solutions	*Case No.*: 2003040601 *Date*: April 4, 2003
Location of Computer/Media (full address): Corporation X, Building 6, Redmond, CA	*Name of Suspect(s)/Type of Case*: John Doe/Information Theft
EVIDENTIARY SYSTEM	
Computer/Processor: Sony Vaio/Celeron	*Make and Model*: PCG-R5050TLK (PCG-1362)
Name and Address of System Owner: Corporation X, Main Office Redmond, CA 510-555-3465 NOTE ➡	It is an offense to gain unauthorized access to a computer, its software or data. Do you have authorization to undertake this backup/examination?
Serial No.: 325-67545	*Photographic Exhibit No.*: 2003040601-3
CMOS Date and Time: 04/06/2003, 14:30 *Actual Date and Time*: 04/06/2003, 14:32	
EXAMINATION SYSTEM	*Software*: dd and EnCase
Computer/Processor: Dell/Intel Pentium 4	*Make and Model*: Dimension 4600C
Serial No.: 35-6465466	*CMOS Date and Time*: 04/06/2003, 14:54 *Actual Date and Time*: 04/06/2003, 14:54

EVIDENCE FILES (two independent copies)

Name	Creation Time	Size (bytes)	Message Digest
sony1-1.dd	04/06/2003 15:02	601435	343e16d6551e84d35c176375728fbbf4
sony1-2.dd	04/06/2003 15:22	354676	ab487d36057d446b6a8b72091da72f23
sony1.E01	04/06/2003 15:46	613354	e6dd075b82677fc0be6f88f1fb941224
sony1.E02	04/06/2003 16:30	454643	5d6330ca0adaa43c6639b68f6b2db48b

Other Media:
Floppy disks inventoried on attached sheet

Evidence Bag:
Hard drive stored in evidence room

Comments:
System returned to owner without drive

PRESERVATION

- Once identified, digital evidence must be preserved in such a way that it can later be authenticated. A major aspect of preserving digital evidence is preserving it in a way that minimizes the changes made. Imagine for a moment a questioned death crime scene with a suicide note on the computer screen. Before considering what the computer contains, the external surfaces of the computer should be checked for fingerprints and the contents of the screen should be photographed. It would then be advisable to check the date and time of the system for accuracy and save a copy of the suicide note to sanitized labeled removable media

CASE EXAMPLE

- In one homicide case, law enforcement seized the victim's computer, but instead of treating it as they would any other piece of evidence, they placed the computer in an office, turned it on, and operated it to see what they could find, thereby altering the system and potentially destroying useful date-time stamp information and other data. Additionally, they connected to the victim's Internet account, thereby altering data on the e-mail server and creating log entries that alarmed other investigators because they did not know who had accessed the victim's account after her death.

- In a child pornography investigation, papers, photographs, videotapes, digital cameras, and all external media should be collected. At the very least, hardware should be collected that may help determine how child pornography was obtained, created, viewed, and/or distributed. In one case, investigators found a scrapbook of newspaper articles concerning sexual assault trials and pending child pornography legislation as well as a hand-drafted directory of names, addresses, and telephone numbers of children in the local area. Images are often stored on removable storage media and these items may be the key to proving intent and more severe crimes such as manufacture and distribution. For instance, a USB thumb drive may contain files useful for decrypting the suspect's data or it may become evident that the suspect used removable storage media to swap files with local cohorts.

- The severity of the crime and the category of cybercrime will largely determine how much digital evidence is collected. When dealing with computer hardware as contraband or evidence (e.g., component theft), and the technical and legal issues are not complex, just get the hardware. Additionally, no sophisticated seizure process or analysis of items will be necessary unless the hardware was used to commit a crime. When the computer is an instrumentality used to disseminate child pornography or commit online fraud, greater care is required to preserve the contents of the computer. In homicide and child pornography cases, it is often reasonable to seize everything that might contain digital evidence. However, even in a homicide or child pornography investigation, the other uses of the computers should be considered. If a business depends on a computer that was collected in its entirety when only a few files were required, the digital investigator could be required to pay compensation for the business lost.

EXAMINATION & ANALYSIS

Recall that a forensic examination involves preparing digital evidence to facilitate the analysis stage. There are three levels of forensic examination:

1. survey/triage forensic inspections,
2. preliminary forensic examination, and
3. in-depth forensic examination.

The nature and extent of a digital evidence examination depend on the known circumstances of the crime and the constraints placed on the digital investigator. If a computer is the fruit or instrumentality of a crime, the digital investigators will focus on the hardware. If the crime involves contraband information, the digital investigators will look for anything that relates to that information, including the hardware containing it and used to produce it. If information on a computer is evidence and the digital investigators know what they are looking for, it might be possible to extract the evidence needed quite quickly.

- In any case, the forensic examination and subsequent analysis should preserve the integrity of the digital evidence and should be repeatable and free from distortion or bias.
- Filtering/ reduction
  - Eliminating valid system files and other known entities that have no relevance to investigation
  - Focusing on the most probable user-created data
  - Focusing on files within a restricted time frame
  - Managing duplicate files, which is particularly useful when dealing with backup tapes
  - Identifying discrepancies between digital evidence examination tools, such as missed files and MD5 calculation errors

- Class/Individual characteristics and evaluation of the source
  - Three fundamental questions that need to be addressed when examining a piece of digital evidence are what is it (identification), what characteristics distinguish it (classification or individualization), and where did it come from (evaluation of source). In the digital realm, there are currently very few individualizing characteristics that uniquely distinguish a computer or piece of data from all other similar items. Serial numbers are an obvious individualizing characteristic but these numbers are often not useful from an investigative perspective and are mainly used for keeping track of items in case documentation. Therefore, the process of identification generally involves ascertaining what a particular digital object is and classifying it based on similar characteristics, called class characteristics.
- Data recovery/ Salvage

RECONSTRUCTION

- The three fundamental types of reconstruction—functional, relational, and temporal
- Functional Analysis
  - To determine if the individual or computer was capable of performing actions necessary to commit the crime.
  - To gain a better understanding of a piece of digital evidence or the crime as a whole.
  - To prove that digital evidence was tampered with.
  - To gain insight into an offender's intent and motives. For instance, was a purposeful action required to cause damage to the system or could it have been accidental?
  - To determine the proper working of the system during the relevant time period.

- Relational Analysis
  - In an effort to identify relationships between suspects, victim, and crime scene, it can be useful to create nodes that represent places they have been, e-mail and IP addresses used, financial transactions, telephone numbers called, etc. and determine if there are noteworthy connections between these nodes.
- Temporal Analysis
  - In a homicide investigation, one suspect claimed that he was out of town at the time of the crime. Although his computer suffered from a Y2K bug that rendered the date-time stamps on his computer useless, e-mail messages sent and received by the suspect showed that he was at home when the murder occurred, contrary to his original statement. Caught in a lie, the suspect admitted to the crime.

REPORTING

- To perform a forensics disk analysis and examination, you need to create a report. Before Windows forensics tools were available, this process required copying data from a suspect drive and extracting the digital evidence manually. The investigator then copied the evidence to a separate program, such as a word processor, to create a report. File data that couldn't be read in a word processor—databases, spreadsheets, and graphics, for example—made it difficult to insert nonprintable characters, such as binary data, into a report. Typically, these reports weren't stored electronically because investigators had to collect printouts from several different applications to consolidate everything into one large paper report. Newer forensics tools can produce electronic reports in a variety of formats, such as word-processing documents, HTML Web pages, and Acrobat PDF files. The following are subfunctions of the reporting function:
  - Bookmarking or tagging
  - Log reports
  - Timelines
  - Report generator

INFORMATION WARFARE

- Cyber Surveillance
  - Cyber footprint and criminal tracking
    - Signal Direction
    - Signal Times Of Arrival
    - Global Positioning System
    - Server-Assisted GPS
    - Enhanced Signal Strength
    - Location Finger Printing
- The implications of cookies and Integrated Platforms
- Wintel inside, or how your computer is watching You
- Data Mining for what?
- The Internet is Big Brother
- The Wireless Internet: Friend or Foe?

CASE STUDY

- CASE STUDIES FOR PARTICIPATIVE LEARNING

Module 4

COMPUTER FORENSIC EVIDENCE AND DATA RECOVERY

Outline

- Data Recovery Defined
- Data Backup and Recovery
- Data Collection and Data seizure
- Controlling Contamination: The Chain of Custody. Reconstructing the Attack.

DATA RECOVERY DEFINED

- Data recovery is the process in which highly trained engineers evaluate and extract data from damaged media and return it in an intact format. Many people, even computer experts, fail to recognize data recovery as an option during a data crisis, yet it is possible to retrieve files that have been deleted and passwords that have been forgotten or to recover entire hard drives that have been physically damaged.

DATA BACKUP AND RECOVERY

- The following are obstacles to backing up applications:
  - Backup window
  - Network bandwidth
  - System throughput
  - Lack of resources

THE ROLE OF BACKUP IN DATA RECOVERY

- Many factors affect back-up:
  - Storage costs are decreasing.
  - Systems have to be online continuously.
  - The role of backup has changed

THE DATA-RECOVERY SOLUTION

- Shrinking expertise, growing complexity
- Budgets and Downtime
- Recovery: Think before You backup
- Evaluate Your preparations

HIDING AND RECOVERING HIDDEN DATA

- It is common knowledge that what is deleted from the computer can sometimes be brought back. Recent analysis of security implications of “alternative data-streams” on Windows NT has shown that Windows NTFS filesystem allows data hiding in 206 Computer Forensics, Second Edition alternative data-streams connected to files. These data-streams are not destroyed by many file wiping utilities that promise irrecoverable removal of information. Wiping the file means “securely” deleting it from disk (unlike the usual removal of file entries from directories), so that file restoration becomes extremely expensive or impossible

DATA COLLOECTION AND DATA SEIZURE

- Why Collect Evidence?
  - Future prevention
  - Responsibility

COLLECTION OPTIONS

- Once a compromise has been detected, you have two options: pull the system off the network and begin collecting evidence or leave it online and attempt to monitor the intruder. Both have their pros and cons. In the case of monitoring, you may accidentally alert the intruder while monitoring and cause him to wipe his tracks any way necessary, destroying evidence as he goes. You also leave yourself open to possible liability issues if the attacker launches further attacks at other systems from your own network system. If you disconnect the system from the network, you may find that you have insufficient evidence or, worse, that the attacker left a dead man switch that destroys any evidence once the system detects that it's offline. What you choose to do should be based on the situation.

OBSTACLES

- Electronic crime is difficult to investigate and prosecute. Investigators have to build their case purely on any records left after the transactions have been completed. 218 Computer Forensics, Second Edition Add to this the fact that electronic records are extremely malleable and that electronic transactions currently have fewer limitations than their paper-based counterparts and you get a collection nightmare.
- Computer transactions are fast, they can be conducted from anywhere, can be encrypted or anonymous, and have no intrinsic identifying features such as handwriting and signatures to identify those responsible. Any paper trail of computer records they may leave can be easily modified or destroyed, or may be only temporary. Worse still, auditing programs may automatically destroy the records left when computer transactions are finished with them.
- Because of this, even if the details of the transactions can be restored through analysis, it is very difficult to tie the transaction to a person. Identifying information such as passwords or PIN numbers does not prove who was responsible for the transaction. Such information merely shows that whoever did it either knew or could get past those identifiers.
- Even though technology is constantly evolving, investigating electronic crimes will always be difficult because of the ease of altering the data and the fact that transactions may be done anonymously. The best you can do is to follow the rules of evidence collection and be as assiduous as possible.

TYPES OF EVIDENCE

- Testimonial evidence
- Hearsay

THE RULES OF EVIDENCE

- There are five rules of collecting electronic evidence. These relate to five properties that evidence must have to be useful.
  - Admissible
  - Authentic
  - Complete
  - Reliable
  - Believable

VOLATILE EVIDENCE

- To determine what evidence to collect first, you should draw up an order of volatility—a list of evidence sources ordered by relative volatility. An example an order of volatility would be:
  - Registers and cache
  - Routing tables
  - Arp cache
  - Process table
  - Kernel statistics and modules
  - Main memory
  - Temporary file systems
  - Secondary memory
  - Router configuration
  - Network topology

GENERAL PROCEDURE

- Identification of evidence
- Preservation of evidence
- Analysis of evidence
- Presentation of evidence

COLLECTING AND ARCHIVING

- Logs and logging
- Monitoring

METHODS OF COLLECTION

- There are two basic forms of collection: freezing the scene and honeypotting. The two aren't mutually exclusive. You can collect frozen information after or during any honeypotting

ARTIFACTS

- Whenever a system is compromised, there is almost always something left behind by the attacker—be it code fragments, trojaned programs, running processes, or sniffer log files. These are known as artifacts. They are one of the important things you should collect, but you must be careful. You should never attempt to analyze an artifact on the compromised system.
- Artifacts are capable of anything, and you want to make sure their effects are controlled. Artifacts may be difficult to find; trojaned programs may be identical in all obvious ways to the originals (file size, medium access control [MAC] times, etc.). Use of cryptographic checksums may be necessary, so you may need to know the original file's checksum. If you are performing regular file integrity assessments, this shouldn't be a problem. Analysis of artifacts can be useful in finding other systems the attacker (or his tools) has broken into.

COLLECTION STEPS

- Find the evidence.
- Find the relevant data.
- Create an order of volatility.
- Remove external avenues of change.
- Collect the evidence.
- Document everything.

CONTROLLING CONTAMINATION: THE CHAIN OF CUSTODY

- Once the data has been collected, it must be protected from contamination. Originals should never be used in forensic examination; verified duplicates should be used. This not only ensures that the original data remains clean, but also enables examiners to try more dangerous, potentially data-corrupting tests. Of course, any tests done should be done on a clean, isolated host machine. You don't want to make the problem worse by letting the attacker's programs get access to a network.
- A good way of ensuring that data remains uncorrupted is to keep a chain of custody. This is a detailed list of what was done with the original copies once they were collected. Remember that this will be questioned later on, so document everything (who found the data, when and where it was transported [and how], who had access to it, and what they did with it). You may find that your documentation ends up greater than the data you collected, but it is necessary to prove your case
- Analysis
- Time

RECONSTRUCTING THE ATTACK

- Now that you have collected the data, you can attempt to reconstruct the chain of events leading to and following the attacker's break-in. You must correlate all the evidence you have gathered (which is why accurate timestamps are critical), so it's probably best to use graphical tools, diagrams, and spreadsheets. Include all of the evidence you've found when reconstructing the attack—no matter how small it is. You may miss something if you leave a piece of evidence out.
- Finally, as you can see, collecting electronic evidence is no trivial matter. There are many complexities you must consider, and you must always be able to justify your actions. It is far from impossible though. The right tools and knowledge of how everything works is all you need to gather the evidence required.

THANK YOU!!!