Objectives

- The goal of this training today is for you to:
  - Be an “educated consumer” of computer forensics.
  - Know what a computer or cell phone forensic exam can do for your case.
  - Be familiar with basic computer forensic concepts and what happens when a computer is submitted to the Electronic Crimes Unit.

Authentication

- Is the evidence authentic?
- All forensic analysis is completed on an exact copy, not the original.
- Compare original to working copy in order to show that it was not changed.
- Evidence is validated by comparing the authentication hash.

Scientific Evidence

- Validation of tools used
  - Does the forensic tool used properly represent the data?
- Date/Time issues
  - Is date/time on a computer objectively reliable?
  - Date/time should be taken in the context of other information.
  - Time zones (What is UTC?)

Search Incident to Arrest

- Cell phones
  - Recent Supreme Court case – Need a warrant
Memory – RAM

- RAM = Random Access Memory
- RAM is "volatile" memory
  - No power = no data stored
  - RAM does not store data long-term.
  - As a result, when a computer is turned off, all data in RAM is lost.
- RAM stores data and programs that are being used by the CPU.

Memory – RAM

- RAM provides fast access to programs and data as needed by the CPU.
- When the CPU needs to store a piece of data temporarily to work on another task, it will store the data in RAM.

Memory - RAM

- From a forensic standpoint, anything that is processed by the CPU can be potentially found in RAM.
  - Including passwords, e-mails, chat fragments, etc.
- As a program is loaded, the code from the program is loaded from the hard drive to RAM. Once that data is in RAM, it is pulled from RAM by the CPU.

Memory - RAM

- RAM is connected to the motherboard and with modern computers, has a direct channel to the CPU.

“Virtual Memory” / Paging

- Most operating systems, including Windows, have a system in place for storing data that can not fit into RAM.
- If the system needs more RAM than is available, the overflow will be stored in “Virtual Memory”.
- This concept works differently from operating system to operating system.
“Virtual Memory” / Paging

- Typically, if not enough RAM is available, the system will store older information in from RAM in "virtual memory".
  - In Windows, this is a file or files on the hard drive.

In Windows, this is a file or files on the hard drive.

- Forensically, this means that the information from RAM can be found on the hard drive, even if the computer is off.
  - This includes passwords, chat fragments, etc.

Motherboard

- Everything to the computer connects to the motherboard either directly or indirectly.

- The motherboard is a large piece of circuit board that provides a socket to connect the processor and slots/connectors for system components.

Essential system components connect directly to the motherboard:

- Processor/CPU
- Memory / RAM
- Expansion cards
- Hard drives

Boot – Forensic Implications

- When booting up a suspect system, the examiner does NOT want to allow the computer to boot to the hard drive, why?
  - Just the process of powering on the computer will cause irreversible changes to critical system files (including date/time stamp)
Data Storage – Hard Drives

- Most digital evidence in the computer realm is found on hard drives.
- Types of hard drives
  - IDE (Integrated Drive Electronics)
  - SATA (Serial Advanced Technology Attachment).
    - SATA drives are newer and capable of transferring data faster and more efficiently than IDE drives.
  - SCSI (Small Computer System Interface)

Data Storage – IDE

Data Storage – SATA drive

Data Storage – IDE and SATA

Hard Drive – How Does it Work?

- The inside of a hard drive contains spinning platters made of a light, rigid material.
- Each side of the platter contains a magnetic coating used to record data (1’s and 0’s).
- A read/write arm is used to read this magnetic data, which functions similar to a record needle.

Inside of a Hard Drive

- YouTube – Inside of Hard Drive
Today, digital forensic labs process almost as much removable media (thumb drives, memory cards, etc.) as hard drives.

Responding officers and investigators need to be able to recognize and properly seize different types of digital media.

Memory cards are flash memory, just like USB flash drives.
Optical Media (CDs/DVDs)
- CDs are called optical media because they are read and written by a laser.
- Generally, CDs are "write once". Once they are written, they are read only.
- A CD stores information in the form of "pits and lands". These are the 1's and 0's

Optical Media (CDs/DVDs)
- Pits and lands:

Optical Media (CDs/DVDs)
- When you say to someone you "burned" a CD, that's literally true. The laser from the CD writer burns the "pits and lands" in the CD, permanently storing the data.
- A CD-RW is a rewritable CD. The CD-RW stores the "pits and lands" in the form a dye than can be altered. When the CD-RW needs to overwrite information, it can change a "pit" to a "land" or vice-versa.

External Hard Drives
- An external hard drive functions the same as any other hard drive.
- However, the external hard drive must be connected to the computer via some type of cable.
  - USB, Firewire, eSATA, etc.
- In addition, most external hard drives also require an external power source (need to plugged in to the wall)
Planning / Gathering Intelligence

- Gathering intel about the suspect
  - Determine computer/technical experience
  - Job experience (resumes)
  - Educational experience (resumes/transcripts)
  - Equipment (credit reports / financial records)
  - Criminal history / prior police contacts

Documenting the Scene

- Notes
- Sketches
- Photographs
- Video recordings
- Audio recordings

Documenting the Scene

- Investigators on the scene should document exact actions as they occur:
  - Example: Pulling the plug vs. Start→Shutdown
  - Mis-typed commands, etc.
  - Any keys pressed on the keyboard (i.e. “Shift” or mouse movement to “wake up” computer)
  - Status of any lights on the computer
  - Status of the screen
  - Any date/time info noted on the computer

Documenting the Scene

- Computers record when the computer is shut down and other critical user actions
  - System logs
  - File accessed/modified dates/times
  - The “dirty bit”
- Defense/opposing attorneys will use any discrepancy to invalidate the investigator’s testimony
  - Are you lazy or are you a liar?

Documenting the Scene

- Defense/opposing attorneys will also exploit any discrepancy between investigator’s stories.

Seizure Concerns - Computer

- Encryption
  - Windows Vista/7 Ultimate
  - Mac
  - Advanced Users
- Unsaved information
  - I.e. Suicide letter, confession
- Generally, the best thing to do is pull the plug from the back of the computer.
Seizure Concerns–Cell Phone
- Incoming messages
- Remote wiping programs
- Deletion of data from the server side
- The phone locking itself with a passcode/encryption
- Generally, the best thing to do is turn the phone off by removing the battery.
  - Some phones can turn themselves on (i.e. Blackberry alarm)

Seizing Phones
- It is generally recommended that investigators turn the phone off.
- This is due to concerns that incoming messages and data could overwrite what's on the phone.
- Also, this prevents the suspect, his friends, or the carrier from remotely wiping the phone.

Digital Evidence Seizure Rules
- Use evidence collection techniques that entirely prevent or minimize the alteration or destruction of evidence.
- Document the condition of the computer or digital evidence before seizure and the particular steps that were taken to seize the computer properly.
- Cut off network connectivity as soon as possible.

Digital Evidence Seizure Rules
- The computer forensic expert on scene should keep other investigators away from the keyboard.
- Manipulation of the keyboard by untrained individuals could lead to disaster.
  - "Hot key" bomb – keystroke combination
  - "Booby trap" – appears to perform legitimate operation
  - "TSR" – Runs in the background

Turning on the computer
- When officers or investigators at a scene turn on or manipulate a computer that is already on, these officers change the data on that computer.
- For example, when you open a file you change the "last accessed time". We will never be able to recover what the "last accessed time" was before you opened that file.

Turning on the computer
- For example, when you open a file you change the "last accessed time". We will never be able to recover what the "last accessed time" was before you opened that file.
- As a result, the forensic examiner will never be able to determine when the suspect actually opened or accessed the file.
What to Seize?
- Investigators need to decide specifically what to seize and what not to seize.
- Digital evidence can be found in many forms:
  - Computers
  - Cell phones
  - External hard drives
  - Thumb drives / memory cards
  - Cameras
  - iPods/digital music players
  - Other devices (card readers, etc.)

Digital Evidence Seizure
- After identifying what is going to be seized, investigators must determine how each piece of evidence will be seized.
- This will be dependent upon:
  - Type of computer (PC, Mac, other)
  - Operating system
  - Whether the computer is on or off
  - The possibility of encryption

Digital Evidence Seizure
- Traditionally, the old rule was always "pull the plug" when seizing a computer.
- This is no longer the case, however.
- For most Windows computers, pulling the plug from the back of the machine shuts down the computer with the least invasive effect on the hard drive.

Digital Evidence Seizure
- Some operating systems are not conducive to pulling the plug.
  - For example: Linux
- If a computer is encountered while it is on, investigators should attempt to determine the operating system and the possibility of encryption.

Digital Evidence Seizure
- Disconnect the computer(s) from any network connections.
- Document all cables connected to the computer and follow all cables.
- Collect associated software, computer manuals, other written documentation.
- Record the make, model, and S/N.
- Attempt to identify all potential storage devices.
Digital Evidence Seizure
- Package all evidence
  - Keep computers away from magnetic fields
  - Keep digital evidence away from static electricity
  - Store evidence in an anti-static bag, not plastic.
  - Cell phones should be stored in “Faraday bags”

Seizure Concerns - Computer
- Investigators should not look through the suspect computer.
- Also do not manipulate the keyboard, mouse, or connect anything to the computer (like thumb drives or CDs).
- It is not recommended that you shutdown the computer using Start->Shutdown. Pulling the plug remains the safest method to shut it down.

Breaking a locked phone.
- **Ask the suspect!**
- Forensic examiner may be able to break or workaround the password.
  - Note, this is generally the exception.
  - Sometimes we need the suspect’s computer.
- Do not try to “guess” it, many phones will start deleting data.

Locked Smartphones
- A locked Blackberry will wipe itself after so many attempts to get through the password.
- As a result, the data will be gone forever.
- The carrier (Sprint) and the manufacturer (RIM) can not/will not reset or provide us the password.
- Your first attempt to obtain the password: **Ask the suspect!**

Seizing Phones
- It is generally recommended that you turn the phone off.
- This is due to concerns that incoming messages and data could overwrite what’s on the phone.
- Also, this prevents the suspect, his friends, or the carrier from remotely wiping the phone.
The Forensic Image

- It is a generally-accepted practice to create a forensic image (which is a duplicate copy) of the original hard drive.
- The forensic image is authenticated to ensure that it is a true and exact copy of the original.
- All digital forensic analysis is then performed on the forensic image (copy).

Forensic Imaging Process

- The hard drive is removed from the target computer and connected to a forensic computer through a write blocker or imaging device.
- A write blocker is used to ensure that there are no changes to the original evidence drive during the forensic imaging process.

Forensic Imager / Write Blocker

- Just the act of connecting a hard drive, thumb drive, or other media to a computer will change the original data.
- Whether the forensic image is created using a forensic computer or an imaging device, a software or hardware write blocker is generally used.
- The write blocker will prevent any attempts to write or modify the original evidence.

Sterile Media

- When a forensic image is created, the “target” hard drive (where the image will initially be stored) should be sterile.
- Sterile media means that it has been previously “wiped” - every bit on the hard drive has been written with a 0, a known character, or random data.

Sterile Media

- Using sterile media ensures that there is absolutely no data on the drive prior to storing a forensic image or evidence on it.
Digital Fingerprint

Original HD → Forensic Image → Match

Forensic Imaging Process

- A hash of the original drive is calculated.
- An exact copy of the drive is created, bit by bit.
  - A forensic image is also called a "bitstream image"
  - A forensic image is **not** a "mirror"

Forensic Imaging Process

- When the imaging process is completed, the hash value of the image is calculated.
- The hash value of the image is compared to the original drive to ensure they match.

Hashing in Action

Original HD → Forensic Image

Hash = 12345

Match

What’s on a Hard Drive

More than just C:\

Logical Copy vs. Physical Copy

- A logical "copy" of a hard drive.

SYSDATA (C:\) ❄ Unallocated Space ❄ Deleted Data
Logical Copy vs. Physical Copy

- A logical “copy” of a hard drive.
- A forensic image/bitstream copy

Hash Values

- A hash is a mathematical algorithm used to authenticate data.
- It is frequently described as a “digital fingerprint” of a file or group of data.
- Hashing is used frequently in computer forensics.
- Each bit in a file is run through the mathematical algorithm, and the resulting value is the “Hash Value”

Hash Values

- If I have a particular file, and hash the file I will obtain one hash value.
- If I change a single bit in that file and hash it again, the resulting hash value will be completely different.
- Two common hashes used in computer forensics are the MD5 hash and the SHA1 hash.

Hash Values

- No two files or sets of data have been found “in the wild” that have the same MD5/SHA1 hash values.
- A hash is a unique identifier for a file, set of files, or an entire hard drive.
- Because of this, a hash is frequently described as a “digital fingerprint” of a file, a group of data, or a hard drive.

Hash Values

- Hash values are used frequently in computing and forensics.
  - Authenticate that a forensic image is a true and exact copy and that it has not been altered.
  - Identify a file (For example, law enforcement agencies and NCMEC maintain a list of hash values for known child porn.)
  - Identify a file as a known “safe” file (for example, a Windows system file)

Double-Check Your Work

- After the exam, the image can be hashed again to show that it has not been altered and is still an exact copy of the original.
- Later, if the integrity of the forensic image is ever called into question or it is suspected that the original image is altered, the image can be hashed by an opposing expert.
Live Acquisition

- As a computer is running, information is constantly stored in memory (RAM), including:
  - Usernames/passwords
  - Fragments of e-mails, chats, web pages
  - Other saved program data / metadata
- When the computer is powered off, all the data in RAM is lost.
  - This is called “volatile” data.

Live Acquisition

- Live Acquisition refers to the process of gathering (copying) this “volatile” data before shutting down the computer.
- During live acquisition, investigators must note what hardware/software are used on the target computer.
- Live acquisition can be used to access encrypted data in its decrypted state by imaging the hard drive while the computer is running.

Live Acquisition

- During Live Acquisition, an examiner will use a known forensic tool to image memory (RAM) and/or the hard drive.
  - The forensic tool will generally be one specifically designed for live acquisition that leaves a small “footprint”.
  - The tool should also have been properly tested/validated to ensure proper functioning.
- Any and all commands and actions taken by the examiner should be documented.

Live Acquisition

- Live Acquisition refers to obtaining “volatile” data from memory or from a running computer for later forensic analysis.
- Live Acquisition may also include creating a forensic image of the target hard drive while the computer is running.
  - This may be necessary to access data in its decrypted state because once the computer is shut down, the data is encrypted.

DIGITAL FORENSICS FOR THE ARSON INVESTIGATOR
BASIC COMPUTER FORENSIC CONCEPTS
A Deleted File
- Blue file is stored on hard drive and deleted.
- Red file is written
- The last four pieces of the blue file remain, even though it had been deleted.

For example, you record a 2 hour long movie on a VHS tape.
You decide to reuse the tape and you record a 30 min TV show on the tape, in the beginning.
The remaining 1 and a half hours of the movie will remain on the tape until it is recorded over.

The GREEN File is deleted
- RED File: Clusters 1 to 3
- BLUE File: Clusters 4 to 9
- GREEN File: Deleted, Was clusters 10-20

Now, a new file is written
- RED File: Clusters 1 to 3
- BLUE File: Clusters 4 to 9
- GREEN File: Deleted, Was clusters 10-20
- YELLOW File: Clusters 10 to 13
Unallocated Space
 When clusters on the hard drive are no longer in use, they are called "unallocated space" (like the clusters from the "Green file")

Table

<table>
<thead>
<tr>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
<th>6</th>
<th>7</th>
<th>8</th>
<th>9</th>
<th>10</th>
</tr>
</thead>
<tbody>
<tr>
<td>A</td>
<td>A</td>
<td>A</td>
<td>A</td>
<td>A</td>
<td>A</td>
<td>A</td>
<td>A</td>
<td>A</td>
<td></td>
</tr>
<tr>
<td>11</td>
<td>12</td>
<td>13</td>
<td>14</td>
<td>15</td>
<td>16</td>
<td>17</td>
<td>18</td>
<td>19</td>
<td>20</td>
</tr>
</tbody>
</table>

Another new file is written
- **RED** File: Clusters 1 to 3
- **BLUE** File: Clusters 4 to 9
- **@REEN** File: Deleted, Was clusters 10-20
- **YELLOW** File: Clusters 10 to 13
- **PINK** File: Clusters 24 to 30

Table

<table>
<thead>
<tr>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
<th>6</th>
<th>7</th>
<th>8</th>
<th>9</th>
<th>10</th>
</tr>
</thead>
<tbody>
<tr>
<td>A</td>
<td>A</td>
<td>A</td>
<td>A</td>
<td>A</td>
<td>A</td>
<td>A</td>
<td>A</td>
<td>A</td>
<td></td>
</tr>
<tr>
<td>21</td>
<td>22</td>
<td>23</td>
<td>24</td>
<td>25</td>
<td>26</td>
<td>27</td>
<td>28</td>
<td>29</td>
<td>30</td>
</tr>
</tbody>
</table>

Reformatting a Hard Drive
 A hard drive contains the System Area that has information about how it is set up, where files are stored and a data area where the actual files are.
 When reformatted, only the system area is changed and reset, the data itself remains in tact.

System Area before Reformat
- **RED** File: Clusters 1 to 3 (Date, time, etc)
- **BLUE** File: Clusters 4 to 9 (Date, time, etc)
- **@REEN** File: Deleted (Date, time, etc)
- **YELLOW** File: Clusters 10-13
- **PINK** File: Clusters 24 to 30

Table

<table>
<thead>
<tr>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
<th>6</th>
<th>7</th>
<th>8</th>
<th>9</th>
<th>10</th>
</tr>
</thead>
<tbody>
<tr>
<td>A</td>
<td>A</td>
<td>A</td>
<td>A</td>
<td>A</td>
<td>A</td>
<td>A</td>
<td>A</td>
<td>A</td>
<td></td>
</tr>
<tr>
<td>11</td>
<td>12</td>
<td>13</td>
<td>14</td>
<td>15</td>
<td>16</td>
<td>17</td>
<td>18</td>
<td>19</td>
<td>20</td>
</tr>
</tbody>
</table>

System Area after Reformat
- **EMPTY**: (Note that the data is actually still in tact)

Table

<table>
<thead>
<tr>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
<th>6</th>
<th>7</th>
<th>8</th>
<th>9</th>
<th>10</th>
</tr>
</thead>
<tbody>
<tr>
<td>A</td>
<td>A</td>
<td>A</td>
<td>A</td>
<td>A</td>
<td>A</td>
<td>A</td>
<td>A</td>
<td>A</td>
<td></td>
</tr>
<tr>
<td>21</td>
<td>22</td>
<td>23</td>
<td>24</td>
<td>25</td>
<td>26</td>
<td>27</td>
<td>28</td>
<td>29</td>
<td>30</td>
</tr>
</tbody>
</table>

What’s on a Hard Drive

More than just C:\

Table

<table>
<thead>
<tr>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
<th>6</th>
<th>7</th>
<th>8</th>
<th>9</th>
<th>10</th>
</tr>
</thead>
<tbody>
<tr>
<td>A</td>
<td>A</td>
<td>A</td>
<td>A</td>
<td>A</td>
<td>A</td>
<td>A</td>
<td>A</td>
<td>A</td>
<td></td>
</tr>
<tr>
<td>11</td>
<td>12</td>
<td>13</td>
<td>14</td>
<td>15</td>
<td>16</td>
<td>17</td>
<td>18</td>
<td>19</td>
<td>20</td>
</tr>
</tbody>
</table>

COPYRIGHT © 2013 – Potomac Digital, LLC
Unallocated Space

- During a forensic exam, processing unallocated space can be very time-consuming.
  - Unallocated space typically contains various types of data (pictures, docs, etc. are intermingled).
  - The information about this data (filename, type, date/time, etc.) is no longer present.
  - As a result, forensic examiners must reconstruct the data and then examine it to determine if it is relevant.

Hidden Evidence

- Suspects will attempt to hide evidence by:
  - Making it invisible (hidden files, partitions)
  - Disguised (appears to be something else)
    - Changing extensions, etc.
  - Unreadable (encrypted)

Disguised Data

- Suspects may change a file extension in an attempt to hide data.
  - A suspect may change the file ILLEGAL.JPG to REGULARFILE.DOC.
- Hidden files / hidden partitions
  - A suspect may change a file to a “hidden” or “system” file so that it will appear invisible to other users.
  - A suspect can also create a hidden partition.

Encryption

- Encryption is the process of scrambling data or text by applying an algorithm (or cipher) to the data.
- In order to decrypt the data (change it back to normal), a “key” is needed.
  - Typically this “key” is a user password.

Encryption

- Unlike Windows access control, when a file is “encrypted” that file is actually changed or scrambled.
- For example, File A containing the text “SECRET” becomes “@!*)YA>F;K2B”
- A user’s password or other passphrase is used to create the cipher.
- The password or passphrase will be required to unscramble (decipher) the data.
Encryption

- Unless the forensic examiner is able to determine or break the user’s password or passphrase, the data cannot be deciphered or examined.
- Encryption can be attacked using brute force (all combinations of all passwords), or dictionary attack (based upon information about the suspect and known words).

Defeating encryption

- In order to decrypt data, you need the key.
- The key can be obtained in a number of ways:
  - Brute force attack
    - All combinations are attempted. For example, the computer tries “aaaaaa”. If that doesn’t work, the computer tries “aaaaab” and so on.
    - This method is very time consuming.

Defeating encryption

- Obtaining the key:
  - Dictionary attack
    - The process of using a predefined dictionary or list of all possible words.
    - This is much faster than brute force, because the list of possibilities is smaller.
  - Cached data
    - Sometimes, the password is stored on the suspect’s hard drive either purposely (saved in a document) or inadvertently (saved by the operating system in virtual memory or operating system artifacts)

Defeating encryption

- Obtaining the key:
  - The “old fashioned way”
    - Suspect wrote it down
    - Suspect tells investigators
  - Keyloggers
    - Programs designed to secretly obtain all keystrokes typed into a computer.

Sometimes, encryption can be circumvented due to a weakness in the encryption or algorithm.
A Deleted File

- Blue file is stored on hard drive and deleted.
- Red file is written
- The last four pieces of the blue file remain, even though it had been deleted. The remaining blue area is called “file slack”.

Unallocated Space

- During a forensic exam, processing unallocated space can be very time-consuming.
  - Unallocated space typically contains various types of data (pictures, docs, etc. are intermingled).
  - The information about this data (filename, type, date/time, etc.) is no longer present.
  - As a result, forensic examiners must reconstruct the data and then examine it to determine if it is relevant.

File Properties

- The operating system uses the system area and other portions of the hard drive to store administrative information about the files on a computer.
- This administrative information may remain long after a file has been deleted and overwritten and can be of value when conducting a forensic exam or investigation.

File Properties

- Examples of these file properties include:
  - File name
  - File extension, type (DOC, JPG, etc)
  - Date/time file was created
  - Date/time file was modified
  - Date/time file was last accessed
  - Username/owner of the file
  - File size

Hidden Data

- Users typically hide data in a number of ways:
  - Changing file names/extensions
  - Putting files in system directories
  - Marking files as “hidden” or “system”
  - Encryption/Password Protection

Computer Forensic Exams

- Searching an entire hard drive is the equivalent of sending one investigator into an entire office building with a number of filing cabinets in each office looking for evidence.
Computer Forensic Exams

- Searching an entire hard drive is the equivalent of sending one investigator into an entire office building with filing cabinets in each office looking for evidence.
- In order to find information that will be useful in the investigation, the investigator needs to know what he is looking for.
  - For example, check all the gray-colored filing cabinets for financial records from Wachovia bank.

Computer Forensic Exams

- The average hard drive capacity of a home user today is 100 GB (Gigabytes).
- This is the equivalent of approximately 70,000 floppy disks.
- In order to get to data of evidentiary or investigative value, the examiner must narrow data down using criteria provided by the client or investigator.

Computer Forensic Exams

- A true computer forensic exam is as much of an investigation as it is a technical examination.
- A forensic exam requires that an examiner reconstruct a user’s computer/Internet activity, determine the user’s habits, and determine where the user has attempted to hide or conceal data.

Getting to the Evidence

- Search terms provided by the client
Getting to the Evidence

- Search terms provided by the client
  - For example: “Gasoline” or known e-mail addresses of usernames for the subject.
- Key dates/times and file dates/times
- By username
- By file type (e-mails, pics, chat logs, etc)

Getting to the Evidence

- Common areas (i.e. “My Pictures”)
- Status of file (deleted, encryption, etc.)
- User’s habits and/or recent activity
- Financial/credit card records
Getting to the evidence
- Computer forensic examiners sort files by type, date, and search for particular keywords.
- In addition, forensic examiners use MD5 hashes in their examinations.
  - To match files up to a database of known child pornography files.

Data Carving
- In order to process unallocated space, a computer forensic examiner will typically "carve" that blocks of data from unallocated space.
- This is accomplished either through an automated process with forensic software or manually by the examiner.

Forensic Analysis - Emails
- Client-based e-mails (i.e. Outlook) are typically stored in a file that is called a "message store"
- Outlook uses a file called "PST" (Personal Information Store).
- Like a computer, the PST has "unallocated" space, where deleted e-mails can be recovered.
Forensic Analysis - Emails

- It is not until a PST is “compacted” that the deleted/unused data of the PST file is actually overwritten.
- Many other e-mail storage files and databases in general function this same way.

Forensic Analysis – E-mails

- PST file after it has been “compacted”:

<p>| | | | | | | | | | | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>2</td>
<td>3</td>
<td>4</td>
<td>5</td>
<td>6</td>
<td>7</td>
<td>8</td>
<td>9</td>
<td>10</td>
<td></td>
</tr>
<tr>
<td>11</td>
<td>12</td>
<td>13</td>
<td>14</td>
<td>15</td>
<td>16</td>
<td>17</td>
<td>18</td>
<td>19</td>
<td>20</td>
<td></td>
</tr>
<tr>
<td>21</td>
<td>22</td>
<td>23</td>
<td>24</td>
<td>25</td>
<td>26</td>
<td>27</td>
<td>28</td>
<td>29</td>
<td>30</td>
<td></td>
</tr>
</tbody>
</table>

Document Forensics

- Individual documents (Word Documents, PDFs) and picture files typically contain a wealth of hidden information that is unknown to the user.
- Much of this information is embedded in the document’s data.

Microsoft Office Metadata

- Metadata is “data about data”.
- A forensic examiner can obtain valuable information from Microsoft Office Metadata, including:
  - Who was the original author?
  - Who last saved the document?
  - Who has edited the documented?
  - When was the document last printer?
  - For how long was the documented edited?
  - When was it created/edited/saved, etc?

Microsoft Office Metadata

I see you are typing a personal document, do you want me to remember and store all of your private information?
- Yes
- Ok
- I don’t have a choice, do I?

Adobe PDF Metadata

- Similar information is stored in PDF files and other similar document files.
- Many other document types and files contain “hidden” metadata.
Pictures/JPG Metadata
- Picture/Image files, including JPGs (which is a common picture file extension), also contain metadata.

Metadata from picture files can tell examiner important information, including:
- Make/model/serial # (sometimes) of camera or phone used to take picture.
- Date/time picture was taken
- GPS location where picture was taken (geotagging)
- Date/time from the camera
- Other useful information

Introduction
- Internet and e-mail records are used regularly in most major crime investigations.
- Forensically, when a suspect or victim computer is examined in the lab, the most frequently requested items are Internet/Web activity and E-mails

Web Browsers
- Many different types of web browsers “in the wild”
  - Internet Explorer
  - Firefox
  - Google Chrome
  - Safari (Mac)
  - AOL
- Despite many differences, web browsers share many common features that are of forensic interest.

Web Cache
- As a user “surfs” the Internet, the web pages that he visits are downloaded locally, to his hard drive.
- This was initially designed to improve performance when using a web browser.
  - When the user visits the same web site, if it has not changed, the browser loads the local copy instead of the copy from the Internet.
  - This has the appearance of the web page loading instantaneously.
Web Cache

- The web cache performance increase comes with a privacy tradeoff.
- Web pages, pictures, and other information stored in the web cache remains there for some period of time.
  - It varies by browser, operating system, and user settings.
  - Forensic analysis has recovered web pages from the cache dating back several years.

Internet History

- In addition to the web cache (actual content/HTML files), web browsers store “Internet History” data.
- This information contains the web sites visited, date/time, title of web pages, etc.
- Internet History is stored independently of the web cache, and typically dates back longer than the web cache.

Deleted Cache/History

- When Internet History records and web cache files are “cleared” they are marked as deleted and moved to the unallocated space of the hard drive.
- These are recoverable through forensic analysis.
- The web cache and Internet History are examples of “Internet artifacts”

Web Cache

- Anything visited from a web browser can be recovered from the cache.
- This includes web-based e-mails, chat activity, dating websites, Facebook chat/messages, etc.
- Items in the web cache are saved as they appeared on that web site when viewed by the user at the time they were downloaded.

Internet History

- A typical forensic exam will generally recover approximately 500,000 to 1,000,000 Internet History records.
- Typical results include webmail links, Google searches, MapQuest/Google Map directions, etc.

Cookies

- Another example of an Internet artifact, is a cookie.
- A cookie is a basic text file that a website sends to your computer so the web site can identify you next time.
- For example, you go to your bank web site and log in. The next time you visit the web site, it recognizes the cookie and says “Welcome back, John.”
Chat Programs / Text
- If a web-based chat program is used, chat logs, chat fragments, and other activity can potentially be recovered from the web cache.
- If a chat program is installed locally (i.e. Yahoo chat, AOL Instant messenger, etc.), chat logs may be saved by the user or can be recovered from RAM or the hard drive.
  - Chat logging is on by default for some programs, off by default for others.

Chat Programs / Text
- Chat logs/fragments can be recovered from unallocated space.
  - However, typically the subject’s screen name or content of the exact chat must be known.
  - This is due to the sheer volume of data in unallocated space.

Chat Programs / Video
- Generally, video chats are not stored on the hard drive or anywhere, unless the user records the chat using a screen capture or other utility.

How Does E-mail Work?
- There are two main types of e-mail:
  - Client-based: A program like Microsoft Outlook downloads your e-mail regularly.
  - Web-mail: You log into your web mail via an Internet Browser (like Internet Explorer) and read your mail directly from the server.

E-mail Basics – Client-based
- There are two major types of e-mail: client-based e-mail and web-based e-mail.
- Client-based e-mail is downloaded from the server and then stored locally on the user’s computer.
- When an e-mail is sent, it is created on the local computer and then uploaded to the mail server to be delivered to its destination.

Client Based E-mail - Receive
Hey Server, Give me my e-mail! Here is my username and password.
Ok. Here are 3 E-Mails

**E-mail Basics - Webmail**
- Webmail (i.e., G-mail, Yahoo mail, etc.) is stored on the server and accessed by the user through a web browser, such as Internet Explorer.
- The e-mails themselves are not downloaded to the local computer.
- Since the e-mails are read via a web-based client, the e-mails may be recoverable as part of the Internet/Web Cache.

**E-mail in Investigations**
- E-mail providers such as G-mail, Yahoo, Hotmail, etc. typically store user information and e-mail content.
  - With a court order, law enforcement officers and attorneys can obtain e-mail content.
  - This includes actual e-mail and attachments.
- Similarly, sites such as MySpace and Facebook that have a "messaging" feature similar to e-mail also store this content.

**E-mail as Evidence**
- E-mails frequently become evidence in criminal and civil cases.
- These evidentiary e-mails generally come from two places:
  - Stored on the suspect's computer (either downloaded by mail client or in the web activity)
  - Stored on the e-mail server or backups.

**E-mail Headers**
- When an investigator has a particular e-mail as a piece of evidence, the e-mail header may contain critical information.
- The e-mail header is used by the mail servers to deliver e-mail. Like an envelope, the header contains useful information.
- E-mail headers typically contain things like the sender's IP address, critical date/time information, and unique identifiers.
The IP Address

- In an investigation, obtaining a suspect's IP address will frequently give investigators a suspect's location and other useful intelligence information.
  - A suspect's IP address is the closest thing to a traceable footprint.
- With a suspect's IP address, investigators can subpoena the ISP and determine who and where the suspect is.

Obtaining a Suspect IP

To obtain an IP address, investigators need a piece of known suspect information:

- The suspect's e-mail address
- Web sites frequented by the suspect
- Chat screen names
- The suspect's ISP
- The suspect's name, address, etc.
- Other known Internet activity

Obtaining a Suspect IP

For example…

- If the suspect is known to use e-mail badguy@gmail.com, investigators can subpoena Google and request registration IP addresses and any IP address that badguy@gmail.com has logged in from.
- With the suspect's IP address, investigators can now subpoena Google and search for other G-mail accounts associated with that IP address.

Obtaining a Suspect IP

For example…

- If investigators have a screen name (like BadGuy on AOL Instant Messenger), investigators can subpoena AOL and request captured logon IP addresses associated with AOL S/N “BadGuy”
- If investigators know the suspect uses TD Bank, they can subpoena TD bank to request IP addresses “associated with log-ins to online banking for checking account # 123456789”

Obtaining a Suspect IP

For example…

- If the suspect frequents particular websites, like Facebook or MySpace, investigators can subpoena Facebook for log-on IP addresses associated with Facebook user “Bad Guy”
- If the suspect is known to play World of Warcraft, investigators can subpoena login IP addresses associated with World of Warcraft Account “BadGuytheElfSlayer”.

Obtaining a Suspect IP

For example…

- If investigators know the suspect uses Verizon FIOS and his name, investigators can subpoena Verizon and request “IP addresses assigned to Bad Guy, date of birth 01/01/1970”.
Internet Records as Evidence

- Two types of typical Internet records used as evidence are web records and e-mail records/content.
- Internet Records can be used for:
  - Actual direct evidence itself (illegal child pornography, e-mails confession to a crime)
  - Circumstantial evidence (research on a victim or target, research on how to commit a crime)
  - Corroborate or refute a suspect story or alibi (i.e. date/time a suspect logs into a website)

Web Records in Investigations

- Social networking sites (Facebook, etc.)
  - With a suspect's IP address, e-mail address, or screen name, investigators can get chat details, stored messages, list of friends, stored photos, etc.
- Online storage sites (Photobucket, etc.)
  - With suspect IP, e-mail, or profile name, investigators can get stored photos and other files.
- Search Engines (Google, Yahoo, Bing, etc.)
  - With suspect IP, e-mail, etc. investigators can obtain search activity and other Internet activity.

Web Records in Investigations

- Chat sites (AOL IM, Google Chat, Yahoo)
  - With suspect IP/e-mail address, investigators can obtain friend lists, log in dates/times, etc.
  - With some sites (like Google Chat), the actual content and chat logs can be obtained. With other services, these are not stored on the server.
- Voice over IP sites (Skype, Google Voice, etc)
  - With suspect IP/e-mail address, investigators can obtain call logs, text messages, and in some cases recorded conversations.

Cell Phone Forensics

- Cell phones and wireless devices present a unique challenge to forensic examiners.

Cell Phone Forensics

- Cell phones and wireless devices present a unique challenge to forensic examiners.
- Computers, generally have standard operating systems, file systems, and connections.
Cell Phone Forensics

- Cell phones and wireless devices present a unique challenge to forensic examiners.
- Computers, generally have standard operating systems, file systems, and connections.
- Phones have hundreds of different operating systems and connectors.

Today’s Smartphone is a computer.

- With all of the processing power and storage capabilities of many computers you will find sitting on an office desk.
- For example, the new Motorola Droid X has a 1 GHz processor, 8 GB of embedded memory, and up to 32 GB of storage.

What’s stored on a phone?

- Forensic exams of cell phones typically provide:
  - Contact lists
  - Call logs
  - Text Messages / MMS messages
  - E-mails
  - Pictures / Videos
  - Deleted pictures, text messages, and call logs.

Cell Phones – Deleted Data

- Like a computer, when a text message or other piece of data is “deleted” from a cell phone, this data is marked as available until that space is needed for a new message.
- Because cell phones only have limited storage capacity, that space is likely to be re-used a lot faster than a computer.

Some cell phones (generally older, cheaper cell phones) can only hold a limited number of text messages.

- For example, a phone only holds 100 text messages and your evidence is message number 99.
- If 5 new text messages come in, the evidentiary text message that was number 99 has been overwritten.

Deleted Text Messages:
Cell Phone – Deleted Data

- Forensically, our capabilities vary dramatically from phone to phone.
  - With one model phone, we may be able to recover just contact lists.
  - With another phone, however, we may be able to get everything including deleted text messages, pictures, etc.
- Smart phones generally hold more data and for longer periods.
  - The record?: 10,000 text messages from an iPhone

Cell Phones – Challenges

- Some model cell phones allow the user, owner, or carrier to “wipe” (delete data) from the phone remotely.
- This presents an obvious challenge when a phone contains critical evidence.
- Though most phone locks can be easily bypassed, others are unbreakable.
  - Most handset locks are “breakable”
  - iPhone locks are “breakable” if we have access to the paired computer

iPhones

- Every time a user connects his iPhone to his computer, the iPhone backs up its data to the computer.
- This data includes text messages, call logs, pictures, pretty much everything.
- The computer keeps these backups.
- The backup is like a “snapshot” of that iPhone on the day it was synched.

iPhones

- As a result, if I have a suspect’s computer, I can give you all messages on his iPhone 3 months ago, 6 months ago, etc.
  - Even if the iPhone itself is at the bottom of the Potomac River.
- If the an actual iPhone is locked, we need the suspect to give us the password or we can work around the lock with these backup files.

Cell Phone Forensics

- Unlike a computer, where you can remove a hard drive and process it, removing the internal memory of a phone is usually not an option.
- The examiner will typically recover data from select areas of the phone (i.e. call logs, text messages, etc).
- In some cases, a complete physical acquisition of the phone is possible.

Cell Phone Forensics

- Computer forensics generally allow an examiner to remove the hard drive and process a “dead” machine.
- To process a cell phone, the examiner must turn the phone on.
- Frequently, the examiner has to make changes to the phone to interface it with a computer and/or disable incoming transmissions.
SIM card

- SIM = Subscriber Identity Module
- In addition to the phone containing data that can be recovered forensically, the SIM card also contains data that can be recovered forensically.
  - Typically contact lists, call logs, and text messages but varies by carrier and phone.
  - A phone number does not uniquely describe a phone.

SIM card

- Not every phone has a SIM card.
- Since Verizon phones are not GSM phones (they are CDMA which is another type of phone), they generally do not have SIM cards.

Memory Cards

- Many phones contain memory cards.
- These memory cards can be removed and processed like a computer.
- A forensic image is made and the memory card is analyzed for data like a computer.
- It is typical to recover hundreds to thousands of pictures, including deleted items, from cell phone memory cards.

GPS / Other Wireless Devices

- Typically, a forensic exam of a GPS will recover:
  - Recent destinations
  - Waypoints
  - Saved addresses
- Other wireless/mobile devices (like PDAs, iPads, etc) can also be processed forensically for deleted data.

Cell Phones – Historical Data

- First, determine the carrier
  - LEAP/Neustar
- Critical information you may need for subpoena/court order:
  - Phone number
  - Subscriber info (name/DOB/address)
  - IMSI (Subscriber identity)
  - SIM card number
  - IMEI / MEID (Equipment identifier)
Cell Phone - Geolocation

- There are three ways of locating a phone on a carrier’s network:
  - Cell site/tower data
    - Verizon/RTT data
  - “Pings” (GPS data)
  - Installed Apps
  - Additional equipment

Use caution when plotting cell site/tower information from cell carriers.
- IE if you need to know if the phone was "in the area of" a particular location / cell site
- Versus specifically mapping out the cell sector, azimuth, technical data.
- The technical plotting of specific cell site/historical geolocation data should be performed by somebody that will be able to testify as an expert witness.

GPS Pings

- Pings can be implemented on a phone through:
  - Court order
  - Consent
  - Exigency

Pings can be implemented on a target’s phone from today until a date in the future.
- For example, if you want to track a target phone you can obtain a court order for pings for the next 30 or 60 days.
  - This will allow you to receive the location of the target’s phone over regular intervals.
  - For example, you would receive an e-mail every 15 minutes with the target’s location.
Cell Phones - Geolocation

- Pen register
  - Usually a probable-based court order
  - Will give you live call data for a number of days, including cell tower (as the call occurs)
  - Will usually also include text message info (but not content)
- Pen register data court order is typically combined with pings to locate a target

Pen Register

- Pen registers, like pings, are accomplished by obtaining a court order.
- Pen register allows ETSU to monitor all call activity on a target phone in real time.
- As a suspect places or receives a call, we will basic details about the call
  - Who called
  - What cell tower target’s phone is contacting
  - Length of call, etc

GPS Pings

- GPS pings and other telephone surveillance can be expensive.
  - Costs will be paid from the unit’s general fund but requires prior approval.
- For example:
  - T-Mobile = $100 per day
  - Sprint = $30 per month
  - AT&T = $100 set up + $25 per day
GPS Ping – Not good ping

GPS Ping – Not good ping

Cell Phones – Tower Dumps

- Cell site dumps are useful when you have more than one location/point of reference.
- Generally only active phone activity is reported (i.e., person used phone, sent/received text messages, etc)
- Cell site dumps would have to be executed on all carriers at a particular location.