Topic 3 Acquisition, examination and analysis of evidence in computers and networks Part 3

1

Learning Outcome

After successfully completing this lecture, you will be able to

- Examine, search and recover deleted, hidden and corrupted files

Road Map

- Anti-forensics techniques
- anonymity and pseudonymity
- Recovery of Deleted and Hidden files
- Disk, Partition and Slack Spaces
- String Search
- Data Carving

Digital Forensics Process

- Collection
  - Collection of media/devices at the scene
  - Identification and Preservation
  - Transportation
  - Data Acquisition and Duplication
- Examination
  - Extraction and searching of data
- Analysis
  - Event and Timeline analysis
- Reporting
  - Reporting and documentation

Anti-Forensic Techniques

- Anonymity
- Pseudonymity
- Files Deletion
- Overwritten data
- Hidden Data

Anonymity

- Internet is essentially done anonymously by default, using unidentifiable pseudonyms. e.g. different Internet users access the same Windows IIS web server with the anonymous username called **IUSER**
- While these usernames can take on an identity of their own, they are frequently separated and anonymous from the actual author.
- According to the University of Stockholm this is creating more freedom of expression, and less accountability
- However, the Internet was not designed for anonymity: IP addresses serve as virtual addresses for email and communications
- It means that any time any resource on the Internet is accessed, it is accessed from a particular IP address, and the data traffic patterns to and from IP addresses can be intercepted, monitored, and analysed. This address can be mapped to a particular Internet Service Provider (ISP), and this ISP can then provide information about what customer that IP address was leased to.

Pseudonymity

- A word derived from pseudonym, meaning 'false name', is a state of disguised identity. The pseudonym identifies a holder, e.g. 1812345A@gmail.com permanently used by the person with a real name Peter Lim.
- One or more human beings who possess but do not disclose their true names (that is, legal identities).
- Most pseudonym holders use pseudonyms because they wish to remain anonymous, but anonymity is difficult to achieve, and is often fraught with legal issues. True anonymity requires un-linkability, such that an attacker's examination of the pseudonym holder's message provides no new information about the holder's true name (Extracted from Wikipedia.org)

Deleted and Hidden Files

- Recovery of deleted and hidden files from
  - Live Windows operating systems
    - If only onsite examination of digital evidence is permitted, a forensic examiner must follow a standard procedure to recover the deleted and hidden files from the live Windows operating systems being used by a number of users.
  - Images of a file system
    - Instead of recovery of deleted and hidden files, a file forensic tool will be used to search for any related files (could be deleted or hidden) that contain keywords related to the case.

Where does evidence hide?

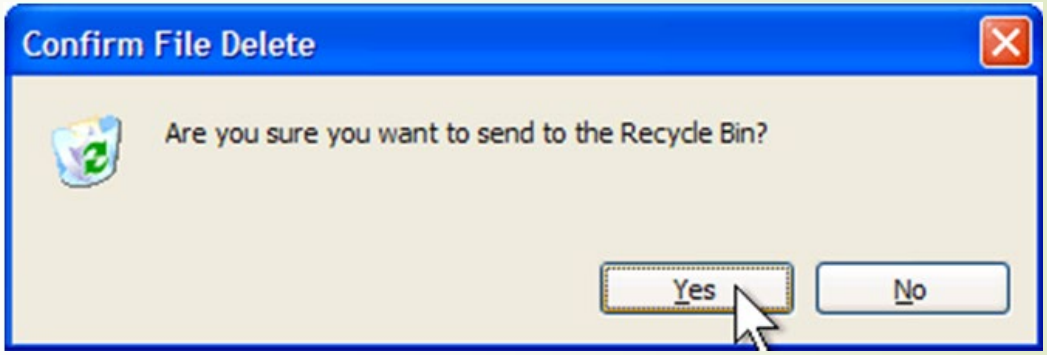
- Physically hidden
  - Deleted data
  - Places not accessible to users through operating system file management tools such as
    - Unused space
    - Slack space
  - Steganography
- Non physically hidden
  - Encrypted files

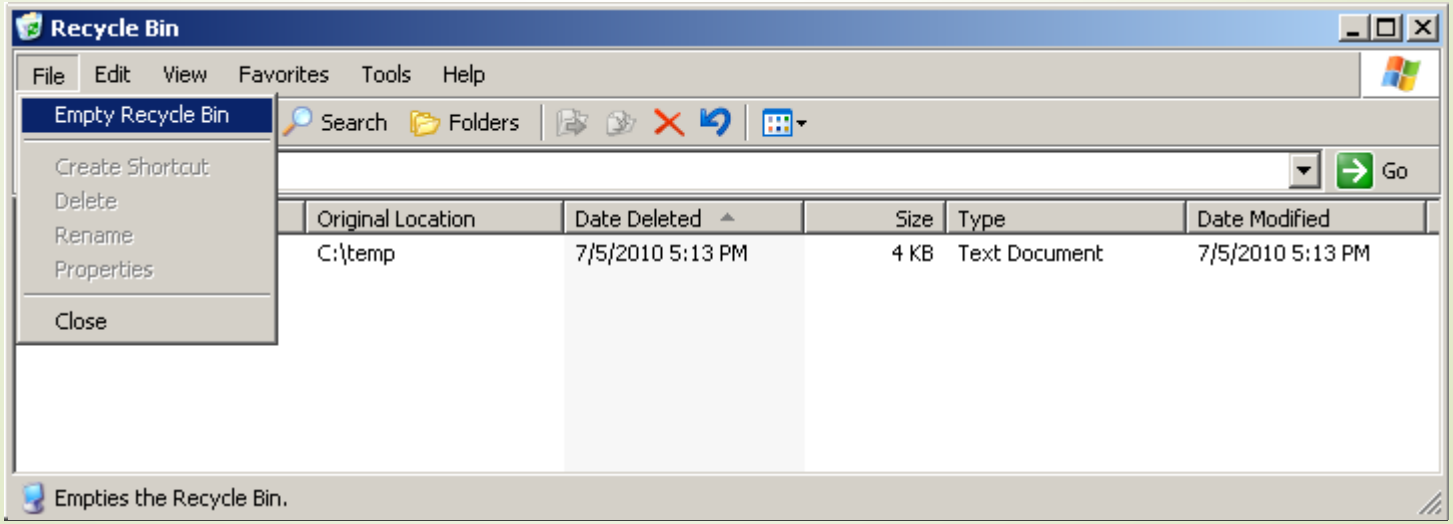
Recovery of deleted and hidden files

- In the examination phase of a digital forensic process, searching and extraction of related data require the recovery of deleted and hidden files

- Objective: To recover all deleted and hidden files that related to the case

Files Deleted?





Recovery of Deleted Data from Live Windows System - Recycle Bin

- When a file is deleted from a drive (e.g. C:\), the file is moved to
  - Drive:\RECYCLED in Windows 95 and 98 (FAT)
  - Drive:\RECYCLER in Windows 2000, NT and XP (NTFS)
  - Drive:\$Recycle.Bin in Windows Vista /Windows 7

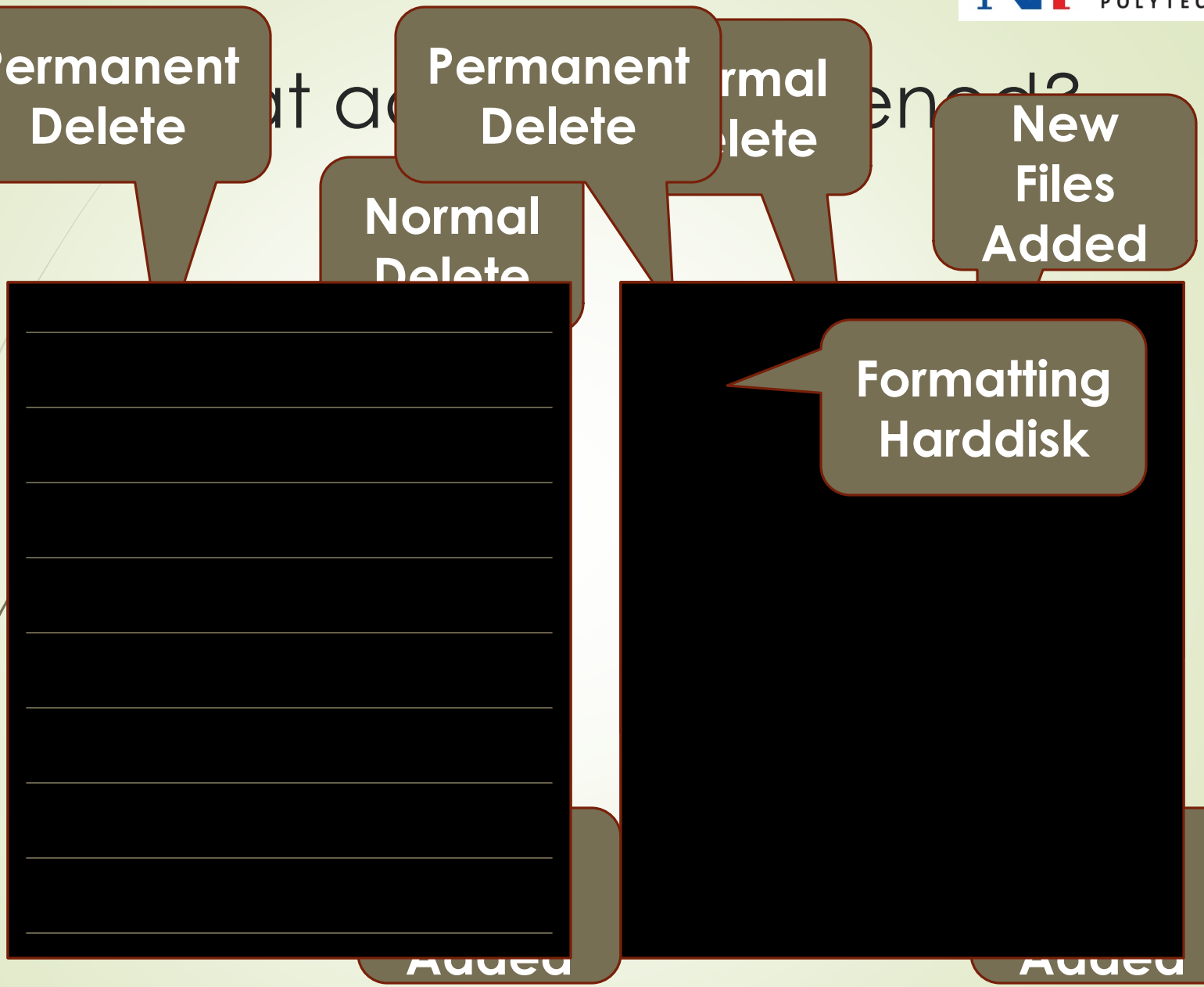
Recovery of Deleted Data from Live Windows System - Recycle Bin

- In Windows Vista/Windows 7, when a file is deleted , it's moved to Drive:\$Recycle.Bin\<user-SID>
  - e.g. c:\$Recycle.Bin\S-1-5-21-2005415734-817711203-1879287733-1001
- There is no recycle bin on removable drive or network drive
  - USB flash (thumb) drives
  - SD flash memory used in cameras
  - re-writable CD/DVDs

Recovery of Deleted Data from Live Windows System - Recycle Bin

- Starting in Vista, when a file is deleted, it is moved to a subdirectory of the Recycle Bin directory on it volume (e.g. C:\$Recycle.Bin\<user-SID>), and a data file containing information on the deleted file's name and path is also created in the Recycle Bin
  - User-SID – security ID for the user that deleted the file
  - The file being deleted is renamed to $Rxxxxx.EXT
  - The information file is name $Ixxxxx.EXT, where XXXXX is the same value used in the name of the $R file
  - The file extension EXT is the same as the deleted file
- The $I file contains:
  - Full path and name of the deleted file
  - Size of the deleted file
  - When the file was deleted

...at a... ...end?


Permanent Delete
Permanent Delete
...rmal ...lete
New Files Added
Normal Delete
Formatting Harddisk
Added
Added

Anti-Forensic Technique – Overwritten Data

- Artifact wiping
  - Disk and files wiping tools
  - Disk degaussing and destruction techniques
- Example - Ccleaner from Piriform
  - A drive wiping tool that can wipe all the data from your hard drive
    - a simple one-pass overwrite,
    - a Department of Defense-level three-pass option,
    - a National Security Administration-level seven-pass cleaning, and
    - a 35-pass Gutmann-level deep scrub. The more passes you select, the slower the deletion process.
  - Empty your recycle bin, delete temporary files, and clean up Registry
  - Remove cookies, surfing history and traces from different Internet browsers

Discover and Recover Hidden Files

- Data or executable files could be hidden by the following methods
  - Files hidden as Alternate Data Streams
  - Files with attributes set to system and hidden
  - Files hidden by disguise
  - Hiding data in the Registry
  - Hiding data in MS Office documents as meta data
  - Hiding data in OLE structured storage in MS Excel files
  - Stenganography
  - Data encryption

Files Hidden as Alternate Data Streams

- ADS (Alternate Data Streams)
  - It is used by users or applications to attach additional file attributes, thumb nail pictures or zone information
  - An attacker or malware can hide information as ADS in any files or folders. (e.g. using the command notepad abc.txt:secret.txt)
  - It cannot be discovered by Windows explorer or earlier version of DIR (MSDOS command)
  - Only the recent Windows Vista DIR with /R option can display the attached ADS file name

Files with Attributes Set to System and Hidden

- An attacker or malware can use the MSDOS command attrib to set any files to be system and hidden
  - e.g. `attrib +S +H filename`
- System and hidden files cannot be displayed in Windows Explorer and the DIR command
- To discover files hidden by the S and H attributes, use one of the following methods
  - In Command prompt window, type in `attrib` command
  - In Windows Explorer>Tools>Folder Options>View, enable "show hidden files and folders" and disable "hide protected operating system files

Files Hidden by Disguise

- Case 1 – Place the data file at an unsuspicious directory
  - Rename data file to a .dll file such as ses.dll in c:\Windows\system32
- With good change management process, new and unknown .dll .com or .exe can be identified after regular scan for unknown files in controlled folders
- Right-click to open the unknown file with notepad and check for any text strings to recover hidden data in the file

Files Hidden by Disguise

- Case 2 – Use unsuspicious names
  - Rename a malware executable file to an unsuspicious name such as systabl.exe
- With good change management process, new and unknown .dll .com or .exe can be identified after regular scan for unknown files in controlled folders
- Move the new and unknown executable file to c:\temp folder and rename the executable file to another name such as Test2.exe
- If any known applications displays error message on the missing the executable file, rename the file back to the original name and move it back to the original folder.

How to recover data or files hidden by the following methods?

- Hiding data in the Registry
- Hiding data in MS Office documents as meta data
- Hiding data in OLE structured storage in MS Excel file
- Hiding data in Winzip or virtual disk image file encapsulation program
- Hiding data using stenganography and data encryption

Find your answers from books or Internet

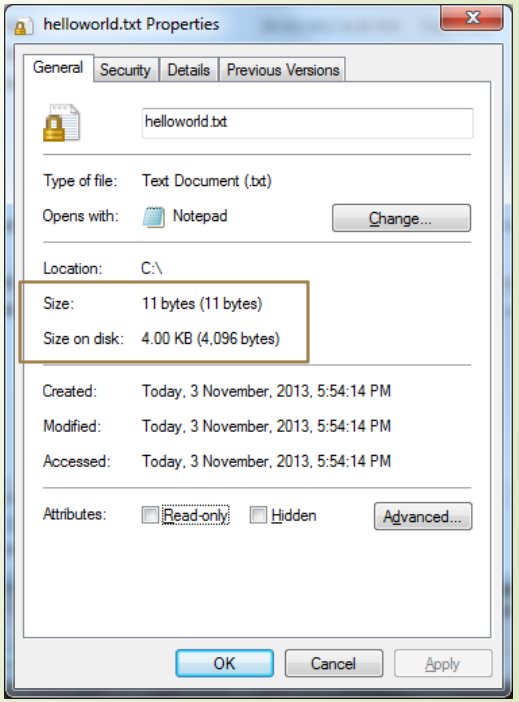
Anti-Forensic Technique – Hidden Data

- Hidden Data
  - System facilities such as hidden files and alternate data streams in Windows OS
  - Data encryption
  - Steganography
  - Different languages

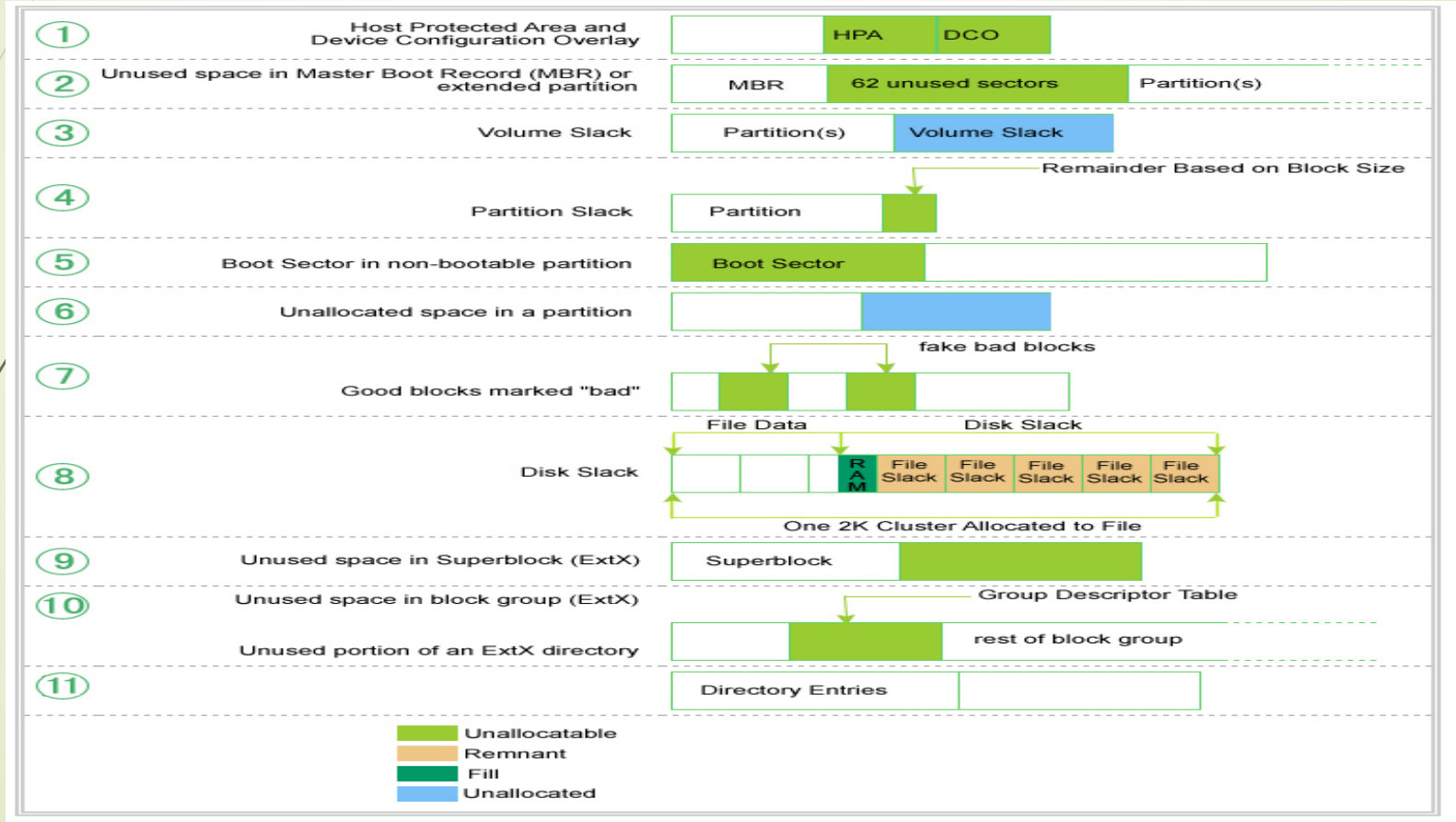
Difficult to recover

Unused and Slack Space

- Unused space
  - Free or unallocated space
  - Space that is currently not in use
- Slack space
  - Space that is currently in use, but not fully occupied



Hidden Evidence in Hard Disks



See details in http://www.berghel.net/publications/data_hiding/data_hiding.php

How to recover evidence from these places?

1. Perform a physical data acquisition of the hard disk drive to create an image of the drive
2. Import the image into a forensic tool
3. Search the image directly for evidence related to the case

String Searching

- Dirty Word List
  - A list of case-specific words
  - e.g. IP address, email address, a person's name, "trojan"…
- AccessData FTK provides the following searching functions
  - Indexed Search
  - Live Search

Indexed Search

- The indexed search uses the index file to find the search term. Evidence items may be indexed when they are first added to the case or at a later time.
- The index file contains all discrete words or number strings found in both the allocated and unallocated space in the case evidence.
- It does not capture spaces or symbols, like .,:;"'~!@#$%^& =+.

Live Search

- Can be used to search for special characters, case sensitive words, hexadecimal or regular expression
- Time intensive process as it performs item-by-item comparison with the search term
- Sample search terms using regular expression
  - US Phone Number=((\<1[\-\.])?(\(| \<)\d\d\d[\)\.\-/]?)?\<\d\d\d[\.\-]\d\d\d\d\>
  - Credit Card Number=\<((\d\d\d\d)[\-]){3}\d\d\d\d\>
  - Social Security Number=\<\d\d\d[\-]\d\d[\-]\d\d\d\d\>
  - IP Address=\<[1-2]?[0-9]?[0-9]\.[1-2]?[0-9]?[0-9]\.[1-2]?[0-9]?[0-9]\.[1-2]?[0-9]?[0-9]\>

Data Carving

- Data carving is the ability to locate files that
  - have been deleted or
  - are embedded in other files.
- Types of file can be carved (recovered)
  - Graphic files: BMP, JPG, GIF
  - Web pages: HTML
  - Document: PDF, OLE Archived files (MS Office documents)
  - And many more – forensic tools allow you to define custom carving patterns

How Data Carving works?

- The data carving function searches for specific file header signatures. When it finds a file header signature for a recognized file type, it carves the file's associated data.
- It can recover previously deleted content residing at the unallocated space.
- It can be used to reconstruct corrupted contents

File Header Signature

```
Offset(h)  00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F
00000000   25 50 44 46 2D 31 2E 33 0A 25 C4 E5 F2 E5 EB A7   %PDF-1.3.
```

- JPEG file

```
Offset(h)  00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F
00000000   FF D8 FF E0 00 10 4A 46 49 46 00 01 02 01 00 60   ÿØÿà..JFIF.
```

- Powerpoint file

```
Offset(h)  00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F
00000000   50 4B 03 04 14 00 06 00 08 00 00 00 21 00 53 78   PK.....
```

More file header signatures at http://www.garykessler.net/library/file_sigs.html

Data Recovery through Data Carving

- Example – To recover stolen pictures of the new product in the memory of the computer used by the suspect
  - Capture the image of the memory of the suspect's computer at the moment he/she committed the crime
  - Import the memory image to a forensic tool
  - Perform Data Carving (File Signature Analysis) to recover hidden and half-corrupted image files
  - View and locate the pictures of the stolen product

Summary

- Anti-forensics techniques
- anonymity and pseudonymity
- Recovery of Deleted and Hidden files
- Disk, Partition and Slack Spaces
- String Search
- Data Carving

References

1. Guide to Integrating Forensic Techniques into Incident Response SP800-86 NIST, csrc.nist.org
2. File System Forensic Analysis, Brian Carrier, 2005, Addison Wesley