

# IE5072

# Cyber Forensic and

# Incident Response

---

# Resource Personnel

---

## **Amila Senarathne (Lecturer-in-Charge)**

Senior Lecturer - Department of Computer Systems Engineering

Manager - SLIIT CISCO Academy

Program Coordinator: BSc (Hons) in IT (Sp. in Cyber Security)

Faculty Student Community Advisor

Faculty of Computing

SLIIT | Malabe Campus

+94 11 754 3298

Email: [amila.n@sliit.lk](mailto:amila.n@sliit.lk)      Ext: 3928

# Lecture Delivery

---

<b>Lectures (Face-to-face)</b>	<b>2</b>	<b>Hours/Week</b>
<b>Labs</b>	<b>2</b>	<b>Hours/Week</b>

# Assessment Criteria

---

<b>Continuous Assessments</b>		
• In-Class Test	20	%
• Practical Exam	30	%
<b>End Semester Assessment</b>		
• Final Examination	50	%
<b>TOTAL</b>	<b>100</b>	<b>%</b>

# Recommended Texts

---

B. Nelson, Guide to Computer forensics and investigations, fourth edition. S.l: Cengage Learning, 2011.

## Supplementary text

Computer forensics: investigating data and image files. Clifton Park, NY: Cengage ; EC-Council Press, 2010.

# Topics

---

- Fundamentals of Digital Forensics
- Computer Crimes Investigation Process
- Digital Evidence
- Data Acquisition and Duplication
- Operating System Forensics (Windows/Linux)
- Investigating Email Crimes
- Network Forensics
- Modern Topics in Cyber Forensics (Mobile Forensics/ Cloud Forensics)
- Introduction to Incident Management
- Incident Response and SOC

# Courseweb Access

---

Enrolment Key : IE5072

Lecture - 01

---

# Fundamentals of Digital Forensics

# Forensic Science

---

“Application of physical sciences to law in the search for truth in civil, criminal and social behavioral matters to the end that injustice shall not be done to any member of society.”

*(Source: Handbook of Forensic Pathology College of American Pathologists 1990)*

## **Why Forensic Science?**

To determine the evidential value of a crime scene and related evidence.

# Definition of Computer Forensics

---

“A methodical series of techniques and procedures for gathering evidence, from computing equipment and various storage devices and digital media, that can be presented in a court of law in a coherent and meaningful format.”

- Dr. H.B. Wolfe

“The preservation, identification, extraction, interpretation, and documentation of computer evidence, to include the rules of evidence, legal processes, integrity of evidence, factual reporting of the information found, and providing expert opinion in a court of law or other legal and/or administrative proceeding as to what was found.”

- CSI

# Definition of Computer Forensics

---

"Forensic Computing is the science of capturing, processing and investigating data from computers using a methodology whereby any evidence discovered is acceptable in a Court of Law."

# Who needs Computer Forensics?

---

- The Victim
- Law Enforcement
- Insurance Carriers
- Ultimately the Legal System

# Victims

---

- Private Business
- Government
- Private Individuals

# Reasons for a Forensic Analysis

---

- ID the perpetrator.
- ID the method/vulnerability of the network that allowed the perpetrator to gain access into the system.
- Conduct a damage assessment of the victimized network.
- Preserve the Evidence for Judicial action.

# A Brief History of Computer Forensics

---

By the 1970s, electronic crimes were increasing, especially in the financial sector

- Most law enforcement officers didn't know enough about computers to ask the right questions
  - Or to preserve evidence for trial

1980s

- PCs gained popularity and different OSs emerged
- Disk Operating System (DOS) was available
- Forensics tools were simple, and most were generated by government agencies

# A Brief History of Computer Forensics

---

## Mid-1980s

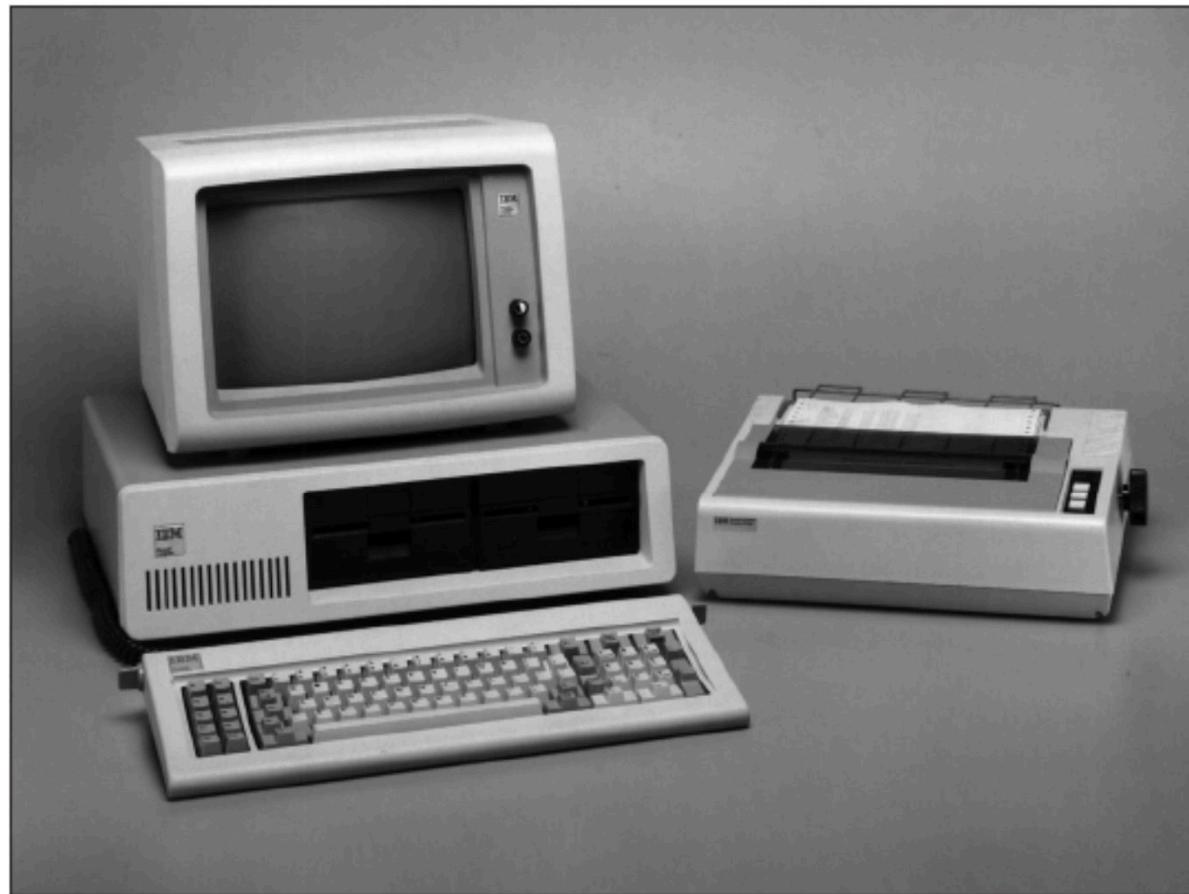
- Xtree Gold appeared on the market
  - Recognized file types and retrieved lost or deleted files
- Norton DiskEdit soon followed
  - And became the best tool for finding deleted file

## 1987

- Apple produced the Mac SE
  - A Macintosh with an external EasyDrive hard disk with 60 MB of storage

# A Brief History of Computer Forensics

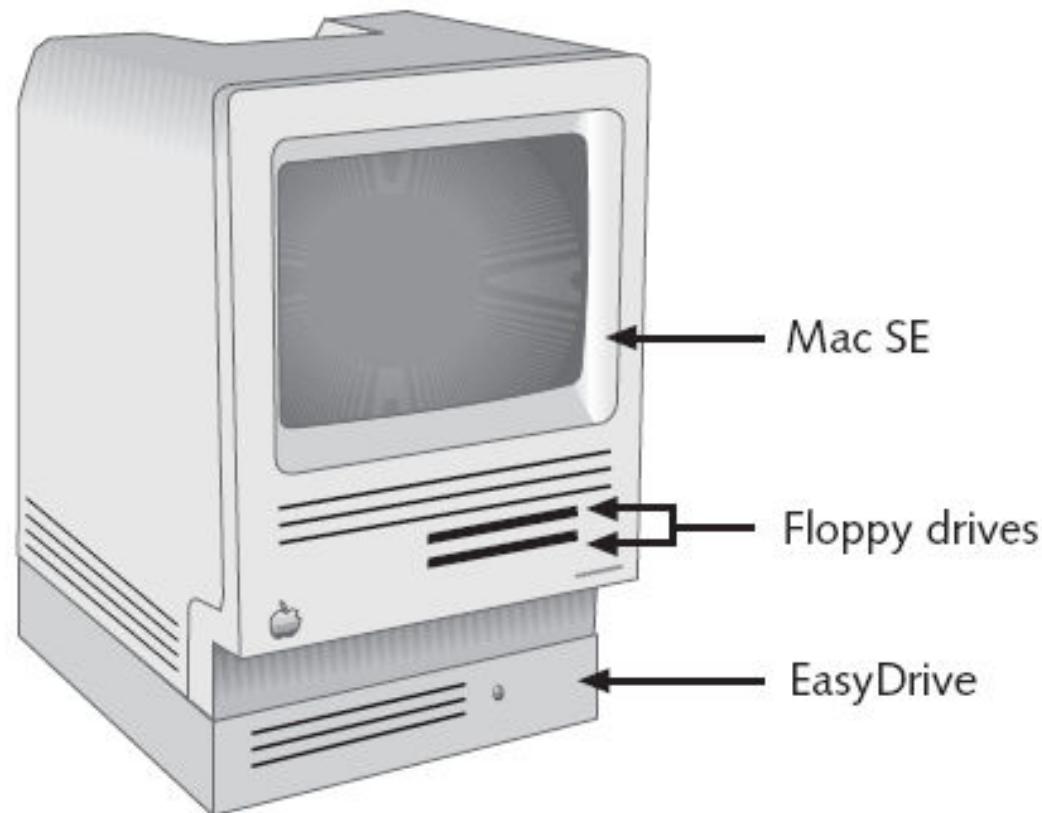
---



**Figure 1-3** An 8088 computer

# A Brief History of Computer Forensics

---



**Figure 1-4** A Mac SE with an external EasyDrive hard disk

# A Brief History of Computer Forensics

---

## Early 1990s

- Tools for computer forensics were available
- **International Association of Computer Investigative Specialists (IACIS)**
  - Training on software for forensics investigations
- IRS created search-warrant programs
- ExpertWitness for the Macintosh
  - First commercial GUI software for computer forensics
  - Created by ASR Data

# A Brief History of Computer Forensics

---

## Early 1990s (continued)

- ExpertWitness for the Macintosh
  - Recovers deleted files and fragments of deleted files

Large hard disks posed problems for investigators

## Other software

- iLook
- AccessData Forensic Toolkit (FTK)

# Preparing for Computer Investigations

---

Computer investigations and forensics falls into two distinct categories

- Public investigations
- Private or corporate investigations

Public investigations

- Involve government agencies responsible for criminal investigations and prosecution
- Organizations must observe legal guidelines

Law of **search and seizure**

- Protects rights of all people, including suspects

# Preparing for Computer Investigations (continued)

---

## Private or corporate investigations

- Deal with private companies, non-law-enforcement government agencies, and lawyers
- Aren't governed directly by **criminal law**
- Governed by internal policies that define expected employee behavior and conduct in the workplace

Private corporate investigations also involve litigation disputes

Investigations are usually conducted in civil cases

# Digital Forensics

---

The use of scientifically unexpressed and proven methods towards

- Preserving
- Collecting
- Confirming
- Identifying
- Analyzing
- Recording
- Presenting

Digital evidence extracted from digital sources

# Key Steps in Forensic Investigations

---

**Step 1:** Computer crime is suspected

**Step 2:** Collect preliminary evidence

**Step 3:** Obtain court warrant for seizure (if required)

**Step 4:** Perform first responder procedures

**Step 5:** Seize evidence at the crime scene

**Step 6:** Transport them to the forensic laboratory

**Step 7:** Create 2 bit stream copies of the evidence

**Step 8:** Generate MD5 checksum on the images

# Key Steps in Forensic Investigations

---

**Step 9:** Prepare chain of custody

**Step 10:** Store the original evidence in a secure location

**Step 11:** Analyze the image copy for evidence

**Step 12:** Prepare a forensic report

**Step 13:** Submit the report to the client

**Step 14:** If required, attend the court and testify as expert witness

## Lecture - 02

---

# Computer Crimes Investigation Process

# Topics to be discussed

---

- Key Steps in Forensic Investigations
- Before the investigation (forensic readiness)
- Computer crimes investigation methodology
- Preparing for a computer investigation
- Conducting an investigation
- Investigative reports and becoming an expert witness

# Key Steps in Forensic Investigations

---

**Step 1:** Computer crime is suspected

**Step 2:** Collect preliminary evidence

**Step 3:** Obtain court warrant for seizure (if required)

**Step 4:** Perform first responder procedures

**Step 5:** Seize evidence at the crime scene

**Step 6:** Transport them to the forensic laboratory

**Step 7:** Create 2 bit stream copies of the evidence

**Step 8:** Generate MD5 checksum on the images

# Key Steps in Forensic Investigations

---

**Step 9:** Prepare chain of custody

**Step 10:** Store the original evidence in a secure location

**Step 11:** Analyze the image copy for evidence

**Step 12:** Prepare a forensic report

**Step 13:** Submit the report to the client

**Step 14:** If required, attend the court and testify as expert witness

# Things to be done before an investigation

---

- Set up a Forensic Workstation / Lab
- Build a Forensic Investigation Team
- Build a Forensic investigation Toolkit
- Establish relationships with Legal/Law enforcement agencies
- Understand Applicable Laws and policies
- Get the authorization from relevant parties
- Conduct relevant Risk Assessments
- Define a Methodology to be used

# Building a Forensic Workstation / Lab

---

Investigations are conducted on a computer forensics lab (or data-recovery lab)

Computer forensics and data-recovery are related but different

## **Computer forensics workstation**

- Specially configured personal computer
- Loaded with additional bays and forensics software

To avoid altering the evidence use:

- Forensics boot floppy disk OR cd
- Write-blocker devices

# Write Blocker

---

Connects a hard drive in trusted read-only mode

There are also Linux boot CDs that mount all drives read-only, such as Helix and some Knoppix distributions



# Setting Up your Computer for Computer Forensics

---

## Basic requirements

- A workstation running relevant operating systems (Windows/Linux/Mac)
- A write-blocker device
- Computer forensics acquisition tools
  - FTK Imager/ encase
- Computer forensics analysis tools
  - FTK/OSF/Encase/Autopsy
- Target drive to receive the source or suspect disk data
- Spare PATA or SATA ports
- USB ports and other relevant ports

# Setting Up your Computer for Computer Forensics (continued)

---

## Additional useful items

- Network interface card (NIC)
- Extra USB ports
- FireWire 400/800 ports
- SCSI card
- Disk editor tool
- Text editor tool
- Graphics viewer program
- Other specialized viewing tools

# Building the investigation Team

---

- Define responsible person to respond to an incident
- Identify team members and assign responsibilities
- Appoint a person to take lead for an investigation
- Ensure team members have necessary authorizations and clearance
- Engage with trusted external parties with forensics investigation capabilities

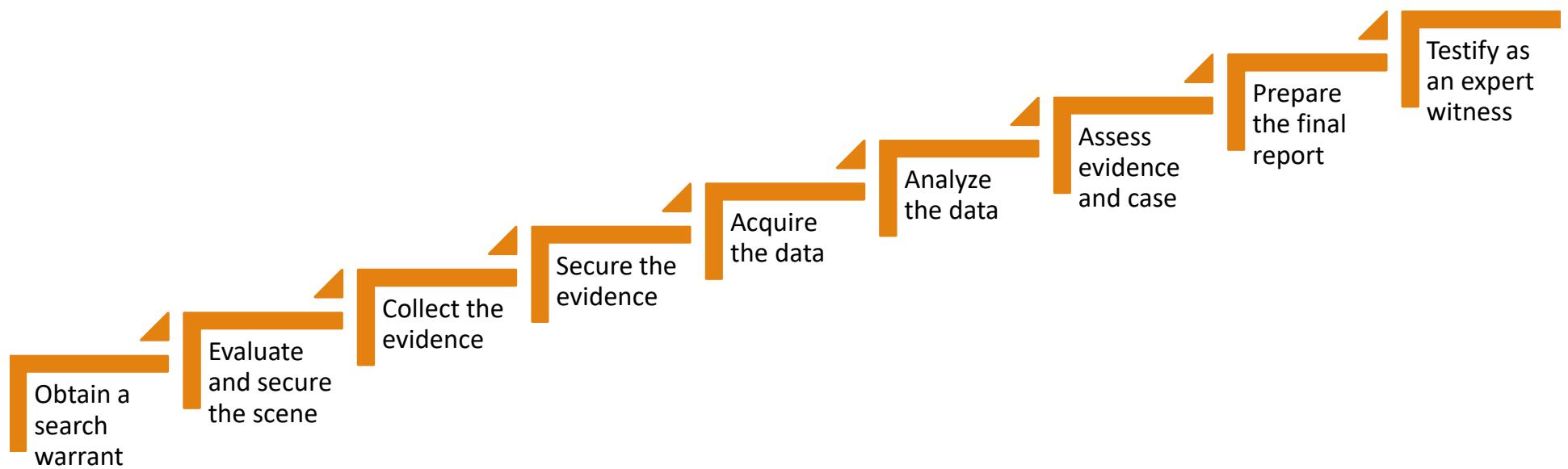
# People Involved in Computer Forensics



Source : EC Council CHFI official courseware

# Computer Forensics Investigation Methodology

---



# Search Warrant

---

---

Public investigation usually begins with the search warrant obtained from court.

---

These may be issued to an organization, a floor, a room, a device, a vehicle, a house, or any company-owned property

---

Defines where the search is performed

---

Determine the suitable approach is to search systems on site or to examine at a field office or under a laboratory environment

---

Determine when and how to return any devices used in the investigation and how to maintain seized data.

# Evaluate and secure the scene

# Forensics Photography

---

Photos of the evidence and subjected area of the incident are required

Label the photos using a predefined approach

Digital images are easily captured, edited and transferred



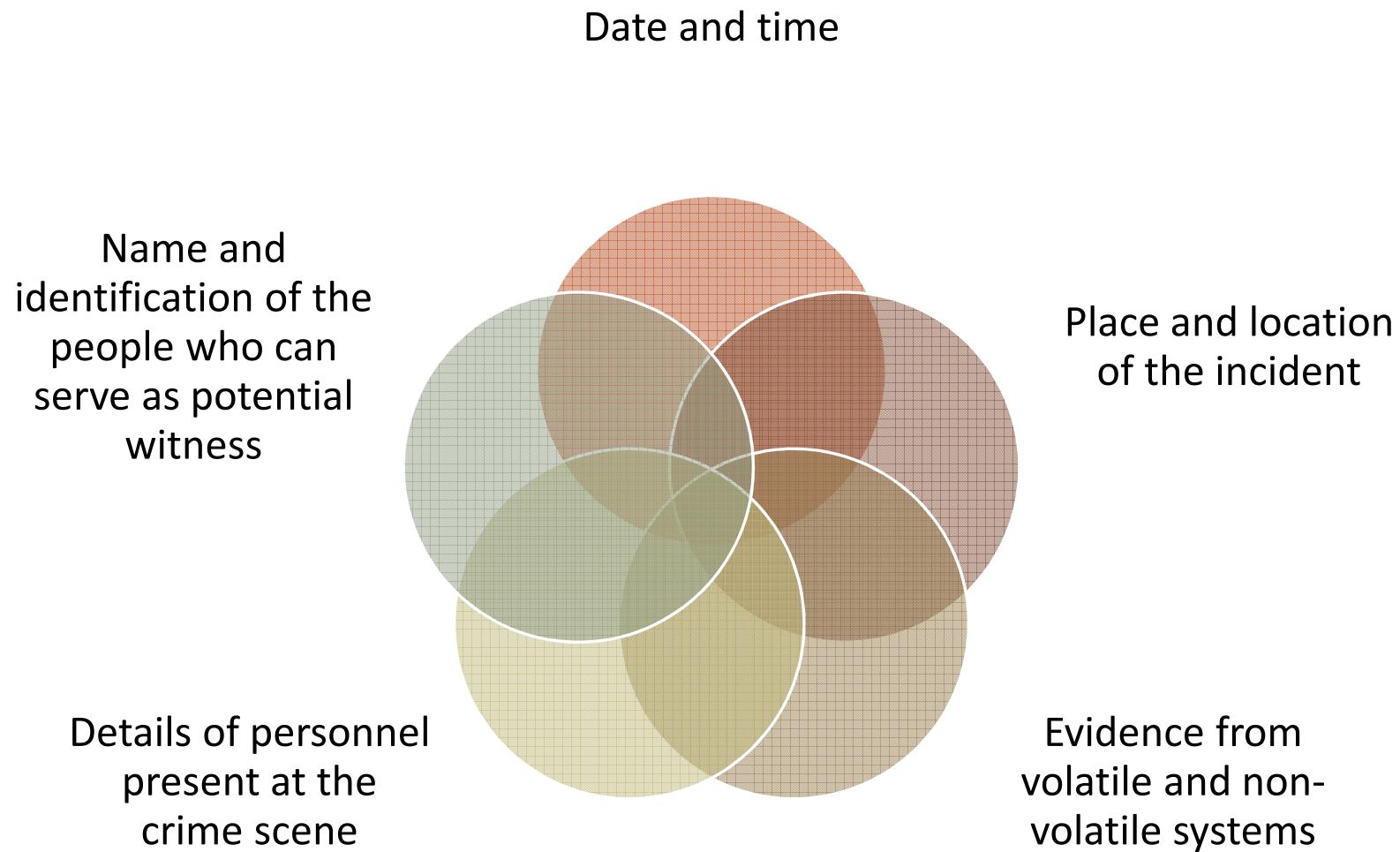
all evidence need to be photographed to help investigative procedure

Photos need to be obtained after labeling

Further digital images help understanding the image perspectives and help take measurements of the evidence

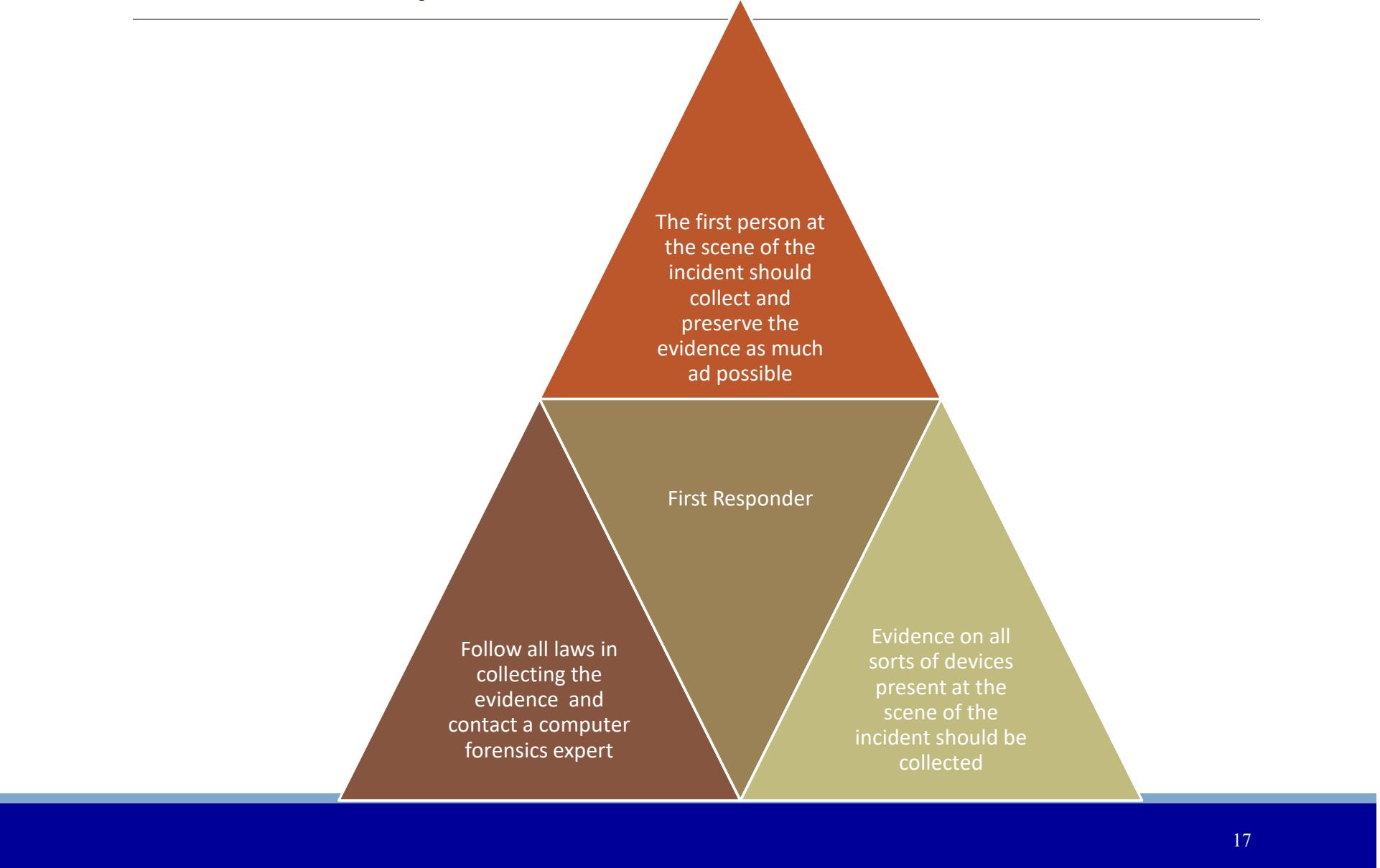
# Obtaining preliminary information

---



# First responder

---



# Collecting evidence – Physical evidence

---

- A. Collect electronic or any other devices present at the crime scene
- B. All devices need to be handled with care to preserve integrity
- C. Objects identified as evidence need to be tagged. Tag provides detailed information about the evidence
- D. Physical evidence include;
  - ✓ Removable media
  - ✓ Cables
  - ✓ Publications
  - ✓ All computer equipment and peripherals
  - ✓ Items taken from the trash
  - ✓ Miscellaneous items

# Evidence collection form

---

Evidence collection form	
Submitting agency:	Case Number:
Item number:	Date of collection:
Time of Collection:	Collected by:
Badge number:	Description of enclosed evidence:
Location where collected:	Type of offence:
Victim's full name:	Suspect's Full Name:

# Evidence custody form

---

An **evidence custody form** helps you document what has been done with the original evidence and its forensics copies.

Two types

- **Single-evidence form**
  - Lists each piece of evidence on a separate page
- **Multi-evidence form**



**Metropolis Police Bureau  
High-tech Investigations Unit**

This form is to be used for only one piece of evidence.  
Fill out a separate form for each piece of evidence.

Case No.:		Unit Number:	
Investigator:			
Nature of Case:			
Location where evidence was obtained:			
Item # ID	Description of evidence:	Vendor Name	Model No./Serial No.
Evidence Recovered by:			Date & Time:
Evidence Placed in Locker:			Date & Time:
Evidence Processed by	Disposition of Evidence		Date/Time
			Page ___ of ___

**Figure 2-3** A single-evidence form

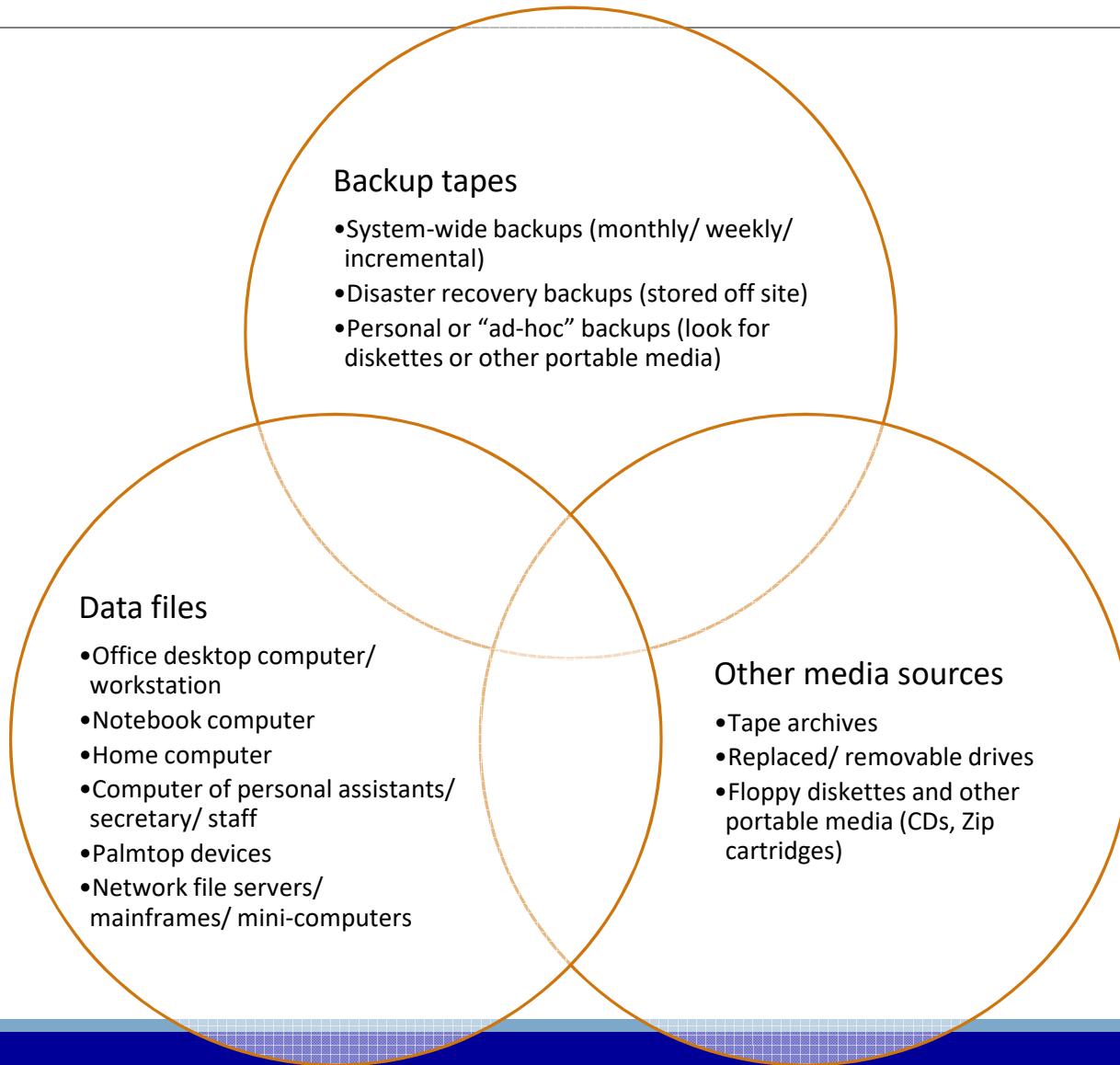
# Collecting evidence – Electronic evidence

---

- A. List the systems subjected to the incident where the evidence could be collected
- B. For each systems, obtain the relevant order of volatility
- C. Record the extent of system's clock drift
- D. Collect evidence from people who are part of the incident
- E. Capture the electronic serial number of the drive and user-accessible, host-specific data
- F. Write protect and virus check all media to maintain the integrity of the media

# Collect electronic evidence

---



# Acquiring evidence

---

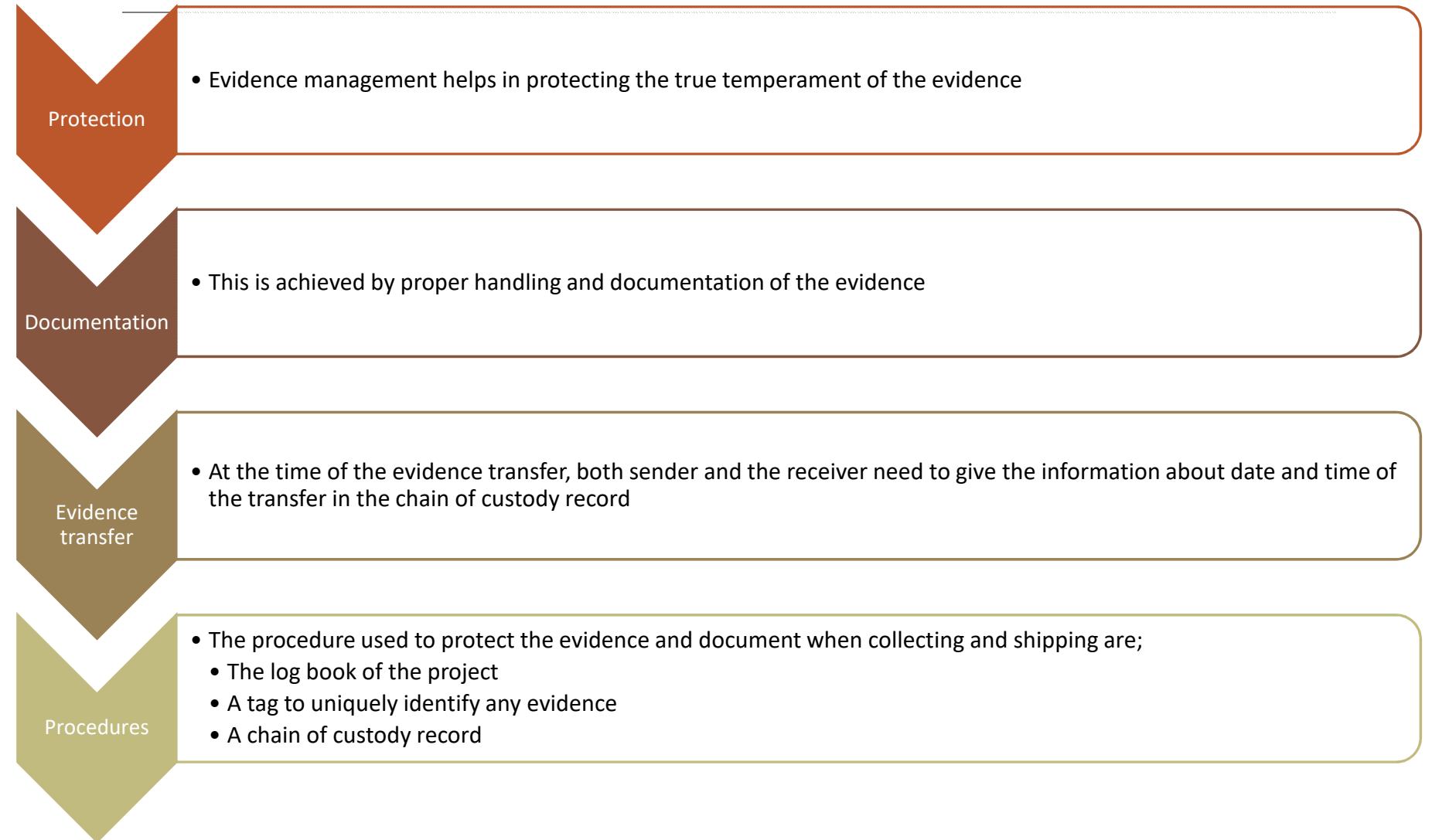
1. Sample banners are used to record the system activities when used by the unauthorized user
2. In warning banners, organizations give clear and unequivocal notice to intruders
3. The equipment is seized which is connected to the case
4. At the time of seizing process, the computers should not be powered down
5. Ensure that the examiner's storage device is forensically clean when acquiring the evidence
6. While protection should be initiated, if available, to preserve and protect the original evidence

# Secure the evidence

---

1. Secure the evidence without damaging the integrity
2. Place the evidence in a secured site
3. Maintain the chain of custody
4. Identify digital and non digital artifacts to separate evidence according to their behavior
5. Maintain a log book at the entrance of the lab
6. Place an intrusion alarm system in the entrance of the forensics lab
7. Contact law enforcement agencies to know how to preserve the evidence

# Evidence management



# Chain of Custody

---

The legal document that demonstrates the progression as it travels from original evidence location to the forensics laboratory

## Functions

- Governs the collection, handling, storage, testing, and disposition of evidence
- Safeguards against tampering with or substitution of evidence
- Documents that these steps have been carried out

**The chain of custody form should identify;**

- Sample collector
- Sample description, type and number
- Sampling data and location
- Any custodians of the sample

# Chain of custody form

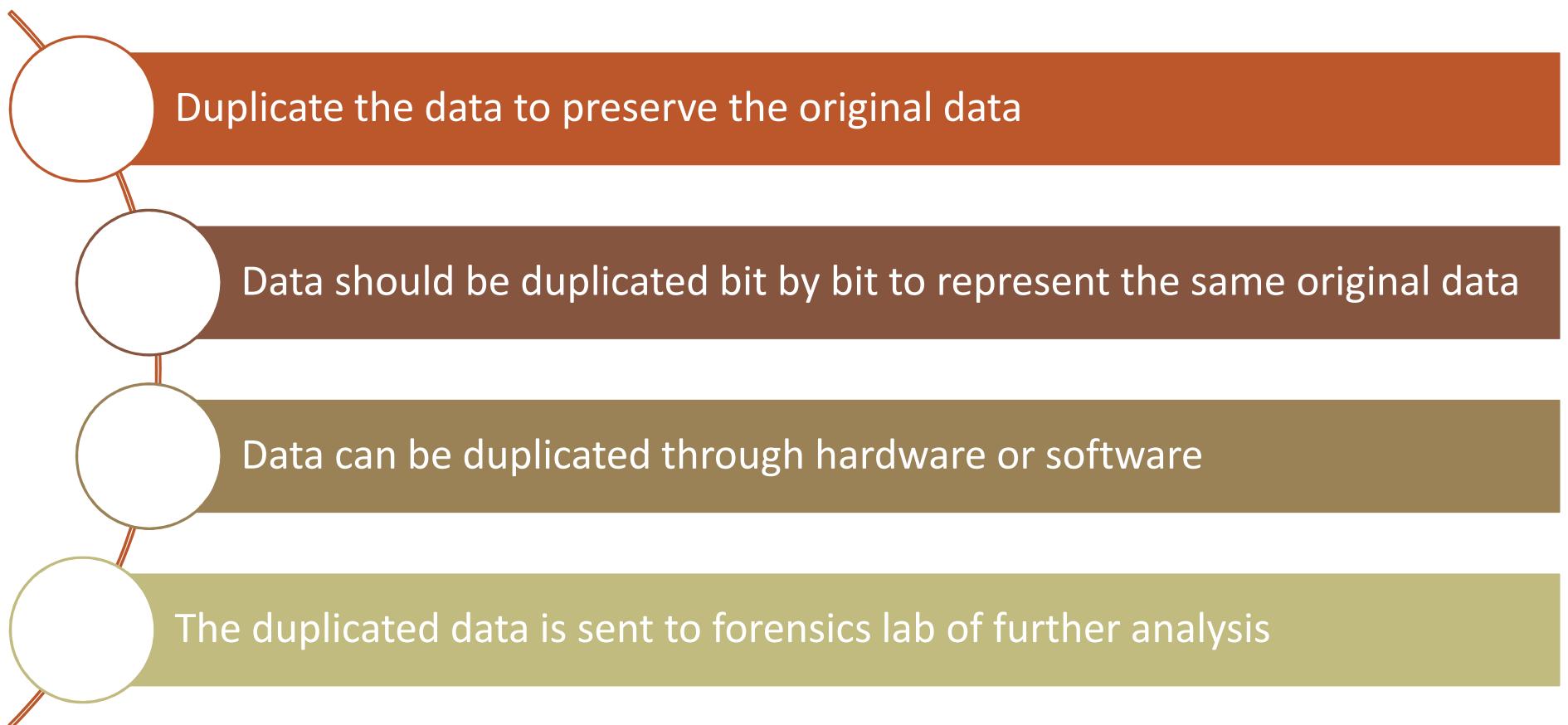
Case number:			
Client reference Number:			
Client Item number:		Description:	
Make:	Model:	Serial number:	Other identifying number:
Client Item number:		Description:	
Make:	Model:	Serial number:	Other identifying number:
Client Item number:		Description:	
Make:	Model:	Serial number:	Other identifying number:

Client Item numbers:	Date/time	Released by:	Received by:	Reason
	Date	Name/ Client	Name/ Client	
Time	Signature	Signature		

# Acquiring the data : Imaging

---

**ORIGINAL DATA SHOULD NEVER BE USED FOR ANALYSIS**



# Verifying integrity of Acquired Data

---

- Calculate and match the hash for the original evidence and the forensics image
- Evidence
  - Same hash value shows that the image is same as the evidence
- Hash value tools are;
  - HashCalc
  - MD5 Calculator
  - HashMyFiles
  - Md5sum

# Recover lost or deleted data

---

- Collect the lost or deleted data for evidence in internal and external devices
- Software used to recover data;
  - Recover my files
  - Digital rescue premium
  - EASEUS data recovery Wizard
  - PC INSPECTOR file recovery
  - Advanced disk recovery
  - Total recall

# Analyze the data

---

- Thoroughly analyze the acquired data to draw conclusions related to the case
- Data analysis techniques depend on the scope of the case or client's requirements
- This phase includes;
  - Analysis of the file's content, date, and time of the file created and modification, user associated with file creation, access and file modification and physical storage location of the file
  - Timeline generation
- Identify and categorize data in order of relevance

# Data analysis tools

---

- Forensic tools help sorting and analysis of large volumes of data to draw meaningful conclusions
- Examples of the data analysis tools;
  - AccessData's FTK
  - Guidance Software's EnCase Forensics
  - Brian Carrier's The Sleuth Kit

# Assess Evidence and the case

---

- Digital evidence should be thoroughly assessed with respect to the scope of the case to determine the course of action

# Investigation report

---

- Most important outcome of the investigation
- Should be clear, concise and written for a specific audience
- Information to be included:
  - Purpose: objectives, target audience and reason for the report
  - Author: details of everyone in the investigation
  - Incident summary: Introduce the incident and explain its impact
  - Evidence: Description of evidence acquired for the case
  - Details: description of evidence analysis and findings
  - Conclusion: summary of the outcome and conclusions based on evidence
  - Appendices: any other important supporting documents

# Expert witness

---

Person with the thorough knowledge of the subject and having the credibility as an expert to testify in court

Should assist the court in understanding evidence and support lawyers to figure out the truth

A person who is unbiased and express the complete truth about the evidence presented disregarding any influence or views

# Completing the Case

---

- In a good computer forensic investigation, the steps can be repeated and the results obtained are same every time

## Maintaining Professional Conduct

- Consider all available facts related to the crime
- Ignore external biases
- Keep the case related things confidential
- Improve technical knowledge
- Maintain credibility, objectivity and Integrity
- Ethics and Morals

## Lecture - 04

---

# Digital Evidence

# Topics to be discussed

---

- Role of digital evidence
- Ensuring chain of custody
- Processing crime and incident scenes
- Process of digital evidence acquisition
- Understanding hard disks and file systems

# Digital Evidence : Definition

---

Digital evidence or electronic evidence is any probative information stored or transmitted in digital form that a party to a court case may use at trial.

[ Casey, Eoghan, Digital Evidence and Computer Crime]

Digital Evidence can be gathered from;

- Digital storage media [volatile and non-volatile]
- Network Traffic

# Digital Evidence

---

Digital evidence can be found in files such as;

- E-mails
- Digital photographs
- ATM transaction logs
- Word processing documents
- Instant message histories
- Files saved from accounting programs
- Spreadsheets
- Internet browser histories
- Databases
- Computer memory

# Digital Evidence

---

Digital evidence can be found in files such as;

- Backups
- Global Positioning System tracks
- Logs from a hotel's electronic door locks
- Digital video or audio files
- IoT devices (smart devices)
- Registries
- OS specific artifacts

# Importance of Digital Evidence

---

1. Businesses are facing the need for gathering evidence on their networks in reply to computer crime
2. Many organizations are taking into account the legal remedies when attackers target their network and focus on gathering the digital evidence in a way that will hold in court
3. Government organizations are also paying attention in using digital evidence to identify terrorists activities and prevent future attacks
4. As a results there is a greater expectation that computer forensic investigators have complete knowledge of handing digital evidence

# Challenges with Digital Evidence

---

1. Chaotic form of evidence and it is critical to handle it correctly
2. Can be altered maliciously or unintentionally without leaving a trace
3. Digital evidence is circumstantial ( difficult for investigators to trace the system's activity)
4. It is an abstraction of some events, when the investigator performs some task on the computer, the resulting activity create data remnants that givens an incomplete view of the actual evidence

# Characteristics of digital evidence

---

1. Admissible in court
2. Evidence must be real (Authenticity)
3. Evidence should prove the attacker's actions or persons innocence
4. Have no doubt about the evidence of its authenticity or veracity
5. Evidence should be clear and understandable to judges and jury

# Fragility of Digital Evidence

---

- If the computer is shut down during the investigation of a crime scene, the data which is not saved will be lost
- If the devices are connected to the internet then the attacker can delete evidence by deleting logs
- After an incident of the person writes data to the computer it can override the crime evidence

# Anti-Digital Forensics

---

- ADF is an approach to manipulate, erase, or obfuscate the digital data
- This makes the forensics examination difficult, time consuming and impossible
- Techniques used in ADF;
  - Overwriting files and meta data (wiping)
  - Exploitation of bugs in forensics tools
  - Hiding data (Steganography, Cryptography and low-tech methods)
  - Obfuscation of data

# Types of digital data

---

- Volatile data
  - Can be modified
  - It contains system time, logged on users, open files, network information, process memory, clipboard contents, services/ driver information, command history
- Non-volatile data
  - Used for secondary storage and is long-term persisting
  - It contains hidden files, slack space, swap file, index.dat files, unallocated clusters, unused partitions, hidden partitions, registry settings and event logs

# Types of digital data

---

- Transient data
  - Contains information such as open network connections, user logout, programs that reside in memory and cache data
  - If the machine is turned off, all this information is lost
- Fragile data
  - Temporarily saved on the hard disk and can be changed
  - It contains information such as last access time stamps, access date on files, etc

# Types of digital data

---

- Temporarily accessible data
  - Stored on the hard disk and are accessible only for a certain time
  - E.g.: encrypted file system information
- Active data
  - Data presently used by the parties for their daily operations
  - Direct and straight forward to recognize and access using the current system

# Types of digital data

---

- Archival data
  - Manages data for a long-term storage and contains records
- Backup data
  - Copy of the system
  - Used at anytime during recovery process after a disaster or system crash

# Types of digital data

---

- Residual data
  - Data that is stored on the computer when a document is deleted
  - When a file is deleted, the computer tags the file space instead of cleaning he file memory
  - The file can be retrieved until he space is reused
- Metadata
  - Maintains a record about a particular document
  - Which includes the file format and how, when and who created, saved and modified the file

# Rules of digital evidence

---

- Evidence that is to be presented in the court must comply with the established rules of evidence
- Prior to the investigation process, it is important that the investigator understands the rules of evidence
- Rules of evidence governs whether, when how and for what purpose proof of a case may be placed before a trier of fact for consideration
- The trier of fact may be a judge or a jury, depending on the purpose of the trial and the choices of the parties

# Best evidence rule

---

- Best evidence rule is established to prevent any alteration of digital evidence either intentionally or unintentionally
- It states that the court only allows the original evidence of the document, photograph or recording at the trial rather than a copy, but the duplicate will be allowed as an evidence under the following conditions.
  - Original evidence destroyed due to fire/ flood
  - Original evidence destroyed in the normal curse of business
  - Original evidence in possession of a third party

# Electronic devices – types and collecting potential evidence

---

- Computer Systems: evidence is found in files that are stored on servers, memory cards, hard drives, removable storage devices and media such as a floppy disks, CDs, DVDs, cartridges and tapes;
  - Use Created Files (address book, database, audio & video files, document & text files, image files, etc.)
  - User Protected Files (encrypted files, hidden files, password protected files, compressed files, misnamed files, steganography files, etc)
  - Computer Created files (backup files, log files, configuration files, swap files, temporary files, history files, system files, etc.)

# Electronic devices – types and collecting potential evidence

---

- Hard disk
- Thumb drive
- Memory card

# Electronic devices – types and collecting potential evidence

- Access Control Devices; evidence is found in recognizing or authenticating the information of the card and the user, level of access, configuration, permissions and in the device itself;
  - Smart card
  - Dongle
  - Biometric Scanner

# Electronic devices – types and collecting potential evidence

---

- Answering machine
- Digital camera
- Handheld devices
- Modems

# Electronic devices – types and collecting potential evidence

---

- LAN Card/ Network Interface Card (NIC)
  - Evidence is found on the Media Access Control address (MAC)
- Routers, Hubs, and Switches
  - Connect different computers or networks
  - For routers; Evidence found in the configuration files
  - Switches and hubs; Evidence found in device itself
- Servers
  - Central computer which gives service to other computers connected in the same network
  - Evidence found in the computer system

# Electronic devices – types and collecting potential evidence

---

- Pagers
- Printers
- Removable storage devices and media
- Scanner
- Telephones
- Copiers
- Credit card skimmers
- Digital watches
- FAX machines
- GPS

## Lecture - 05

---

# Data Acquisition (Part 1)

# Topics to be discussed

---

- Data acquisition formats and methods
- Static and live data acquisition
- Validating data acquisitions
- Software and hardware tools for data acquisition

# Data acquisition

---

- Data acquisition is the process of obtaining data from a digital device using peripheral equipment and media.
- There are two types of acquisition;
  - Static acquisition
  - Live acquisition

# Static acquisition

---

- Process of acquiring nonvolatile data from a system
- Method is used when the systems are shutdown or powered off
- Usually data is acquired from hard drives which includes accessible files and folders, slack space, swap files and unallocated drive space
- Additional nonvolatile data sources; CDs, DVDs, Blu-ray disks, USB thumb drives, smart phones, PDAs, flash cards, external hard drives

# Live Acquisition

---

- Use to acquire data from a live machine
- Use to acquire volatile data that would be lost when the device is powered off
- Such volatile data usually resides in registry, cache and RAM
- Collection of the information should occur in real-time

# Data acquisition considerations

---

- Integrity must be preserved during securing and collecting digital evidence
- Data acquisition and examination should be conducted by a trained professional
- All steps taken should be documented, preserved and available for review

# Data acquisition systems

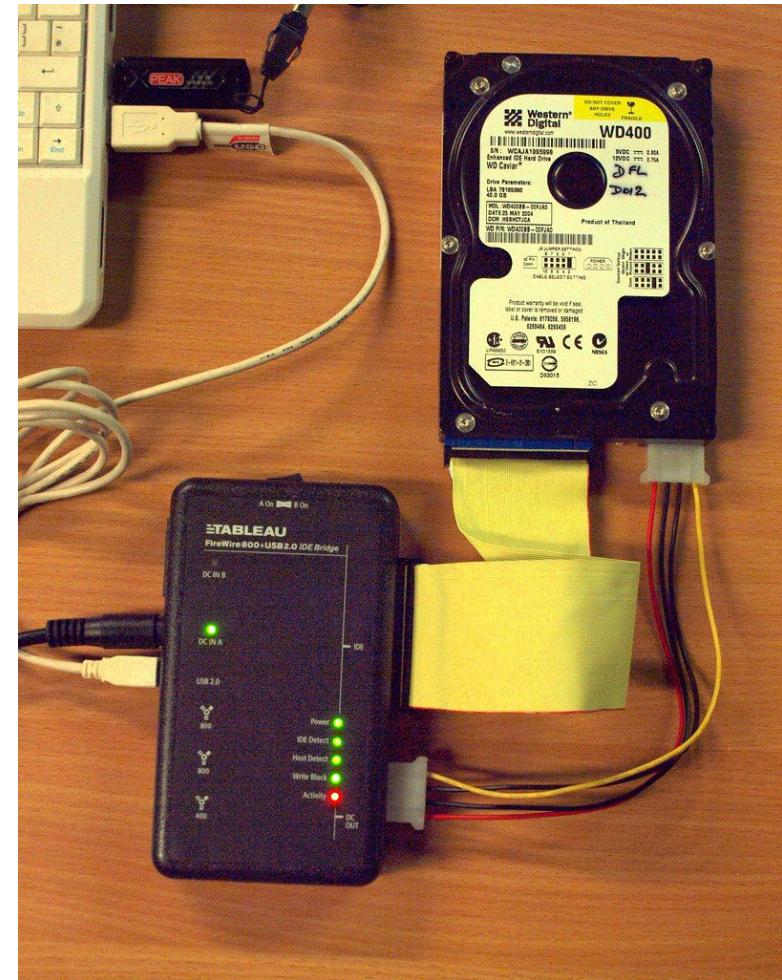
---

- Data acquisition system consists of tools and processes used to acquire data from a source
- Serial communication data acquisition systems;
  - used when location of the data at some distance from the forensic workstation
  - Communication standards such as RS232 or RS485 are used depending on the distance
- USB data acquisition systems;
  - Use to collect data from peripheral devices such as printers, modems and data acquisition devices
  - Easy to use due to simple connectivity and faster data rates
- Data acquisition plugin boards
  - Directly plug in to computer first
  - Useful due to speed and cost effectiveness

# Bit stream disk to image copies

---

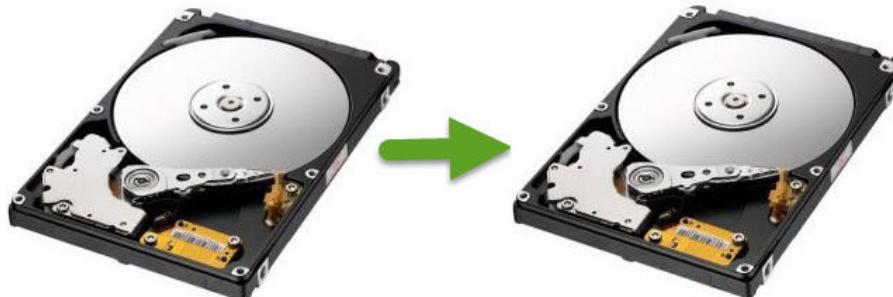
- Acquire a copy of data from a disk to an image file
- Most commonly used method
- Can be used to generate one or more copies of the suspect drive
- Contains a bit to bit replication of original drive
- Supported by most forensics data acquisition tools and data analysis tools



# Bit-stream disk to disk copies

---

- Use to obtain copies from a suspect disk drive to a forensically cleaned disk drive
- Useful when it is unable to create disk to image copies due to software, hardware errors or incompatibilities
- Use tools capable of altering the targets disk geometry (head, cylinder and track configuration) to match the copied data to source drive
- Popular tools; FTK, EnCase, SafeBack, Norton Ghost



# Data Acquisition formats

---

## Raw format

Allows to write bit stream data to files which creates a simple sequential flat file of a data set or a drive

### Advantages

- Fast data transfer
- Can ignore minor data read errors on source drive
- Can be examined using most of the computer forensics tools

### Disadvantages

- Requires same amount of storage as the original disk or data set
- Some tools may not collect bad sectors on source drive

# Data Acquisition formats

---

## Proprietary format

- Format specific to commercial specific tools
- Usually offers features that counterpart the vendors analysis tools

### Advantages

- Data compression capabilities
- Option to split image in to smaller segments
- Ability to integrate meta data (date/time, hash values, case related details)

### Disadvantages

- Limited number of analysis tools supported
- Size restrictions for disk to image files

# Data Acquisition formats

---

## **Advanced Forensics format**

Designed as an open source alternative for current proprietary disk image formats

### Advantages

- No size restriction for disk to image files
- Capable of generating compressed image files
- Capable of splitting an image
- Allow extensive metadata with image or segments
- Support many tools and OSs
- Simple device with extensibility

# Logical and Sparse acquisition

---

- Logical acquisition can be used to capture specific set of files related to the case
  - Examples of logical acquisition; email investigations requires collection of .pst or .ost files
  - Collecting specific files from large RAID server
- Sparse acquisition is similar to logical acquisition. However, is capable of collecting fragments of unallocated (deleted) data
  - Useful when examination of the entire hard drive is not required
- Both methods are used to collect specific information from a large data source which consumes lot of time for acquisition

# Bit stream vs Backups

---

## Bit stream

- Evidence grade backup/ mirror image of source
- Includes hidden and residual data (slack, space, swap, unused space, residue, deleted files)
- Bit stream programs rely upon CRC computations in the validation process

## Backups

- Most Oss pay attentions only to the live file systems structures
- Slack, residue, deleted are not indexed
- Backups usually do not capture this data and they modify the timestamps of data, contaminating the timeline

# Questions

---

# End of Lecture - 5

---

Thank you

# INCIDENT MANAGEMENT

Loshan Wickramasekara  
MSc in Information Security | BSc in IT  
CPISI | CRISC | CISM | CSA  
Manager - FINCSIRT

INCIDENT MANAGEMENT

DISASTER PLANNING

RECOVERY LOSS

SYSTEM PROCESS

ACTIVITY MONITORING

IMT ANALYSIS

EFFECTIVE SUPPORT

CLOSURE

SERVICES OPERATIONS

SLA

ORGANIZATION CONTROL

EVENT BUSINESS

CONTINGENCY RESPONSE

IDENTIFICATION

SECURITY POLICY

DETENTION

DIAGNOSIS

CORRECTION

DISRUPTION

# Event and Incident

- Events: An event is an observable occurrence in an information system that actually happened at some point in time.
  - For example:
    - An email
    - A phone call
    - A system crash
    - A request for virus scans to be performed on a file or attachment
- Incident is an adverse event in an information system – includes the significant threat of an adverse event. In another word, it implies harm or the attempt to harm
- CERT guidelines indicates an incident can be:
  - violation of an explicit or implied security policy
  - the attempts to gain unauthorized access
  - unwanted denial of resources
  - unauthorized use
  - changes without the owner's knowledge, instruction, or consent

# Event vs Incident

- **Cyber Security Event:** An identified occurrence of a system, service or network state indicating a **possible breach of information security policy or failure of controls, or a previously unknown situation** that may be security relevant.
- **Cyber Security Incident:** A single or a series of unwanted or unexpected Cyber Security Events that have a significant **probability of compromising business operations and threatening information security**

# Examples

- Malicious code attacks
  - Event – User reporting that they might have been hit with a particular virus.
  - Potential incident – Their system exhibits behaviors typical for that particular virus.
- Denial of resources
  - Event – User reporting that they can't access a service.
  - Potential incident – Many users reporting that they can't access a service.
- Intrusions
  - Event – A system admin think a system was broken into.
  - Potential incident – A system admin provided the log indicating suspicious activities took place.
- Misuse
  - Event – Web proxy log indicates an user has one hit to a Adult site and company policies dictate that such activities are not allowed.
  - Potential incident – Web proxy log indicates an user has multiple hits to Adult sites and company policies dictate that such activities is not allowed.
- Unauthorized use
  - Event – User tumbled onto an undocumented game within a commercial program by accident.
  - Possible incident – User play the undocumented game within the commercial program and there exist a policy stating that game playing is not allowed.
- Hoaxes
  - Event – User send an email containing false information usually associated with chain emails to the masses.
  - Possible incident – User send an email containing false information usually associated with chain emails to the masses asking them to do the same

# How to classify an EVENT as an INCIDENT

- Is there a risk to data integrity ?
- Is there a risk to the availability of the resource ?
- Is there a risk to the confidentiality of the data ?
- Is the activity abnormal ?
- Is it a violation against company security policies ?

# What is Incident Management

“Capability to effectively manage unexpected disruptive events with the objective of minimizing impacts and maintaining or restoring normal operations within defined time limits.”

ISACA, Certified Information Security Manager® (CISM®) Review Manual

Incident management and response can be considered the emergency operations part of **risk management**.

# Goals of IM

- Detect incidents quickly
- Diagnose incidents accurately
- Manage incidents properly
- Contain and minimize damage
- Restore affected services
- Determine root causes
- Implement improvements to prevent recurrence
- Document and report

# Incident Management :Benefits

- Reduced business impact of incidents by timely resolution
- Proactive identification of possible enhancements
- Management information related to business-focused SLA
- Improved monitoring
- Improved management information related to aspects of service
- Better staff utilization: no more interruption-based handling of incidents
- Elimination of lost incidents and service requests
- Better user/customer satisfaction

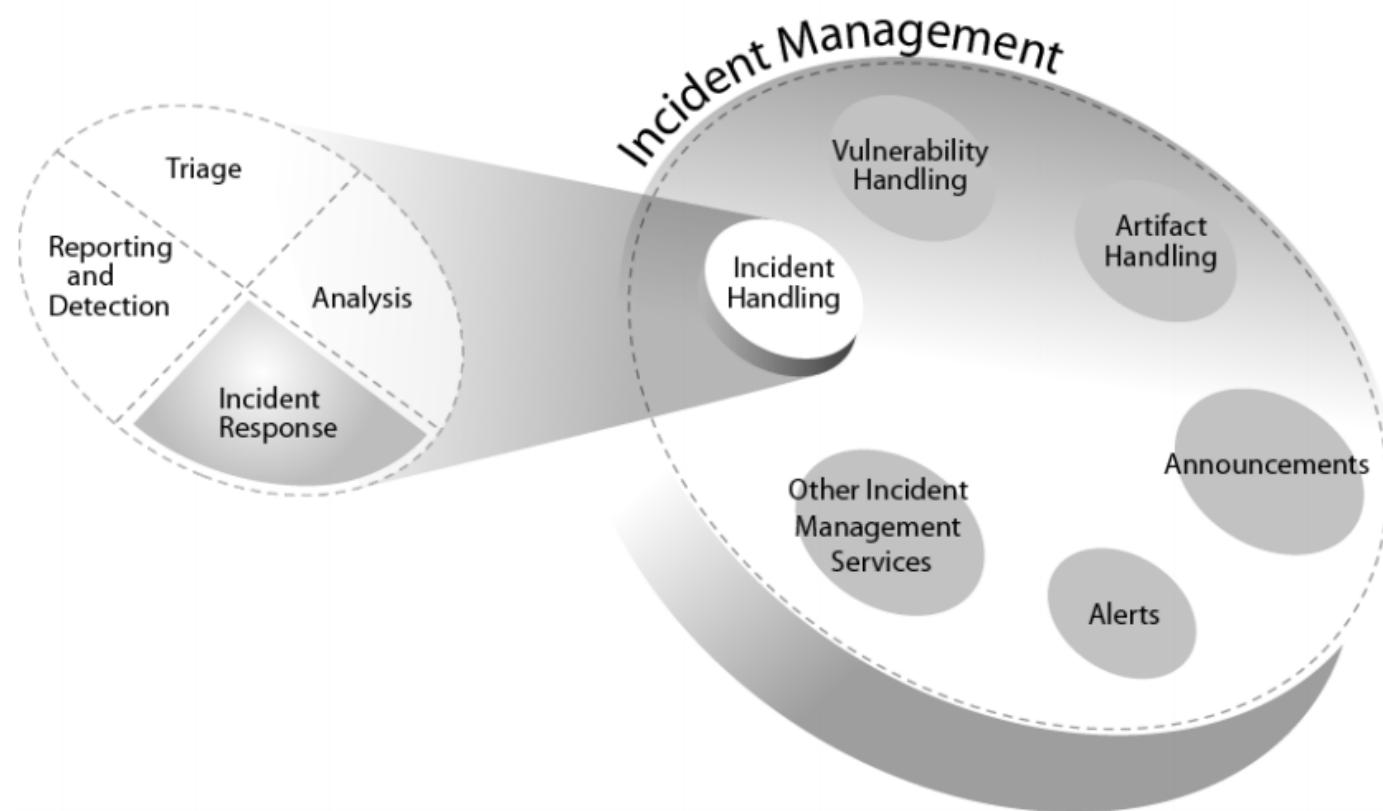
# Causes for poor incident management process

- Absence of visible management or staff commitment, resulting in non-availability of resources for implementation
- Lack of clarity about the business/organisation's needs
- Out of date working practices
- Poorly defined objectives, goals and responsibilities
- Absence of knowledge for resolving incidents
- Inadequate staff training
- Resistance to change

# Standards and Guidelines

- The ISO/IEC 27001 Standard
- The ISO/IEC 27002 Standard
- ISO/IEC 27035 Standard
- The ITIL Framework
- NIST Special Publication (**NIST SP 800-61**)
- ENISA - Good Practice Guide for Incident Management
- NorSIS - Guideline for Incident Management
- SANS: Incident Handler's Handbook

# Incident Management, Incident Handling and Incident Response



# Incident handling

- **Detecting and reporting** – the ability to receive and review event information, incident reports, and alerts
- **Triage** – the actions taken to categorize, prioritize, and assign events and incidents
- **Analysis** – the attempt to determine what has happened, what impact, threat, or damage has resulted, and what recovery or mitigation steps should be followed. This can include characterizing new threats that may impact the infrastructure.
- **Incident response** – the actions taken to resolve or mitigate an incident, coordinate and disseminate information, and implement follow-up strategies to prevent the incident from happening again

# **Best Practices for Building an Incident Response Plan**

- Incident Response Plans are written and documented.
- Incident Response Plans are battled-tested.
- Incident Response Plans evolve over time.
- Incident Response Plans are implemented as a business practice.
- Incident Response Plans are actionable.

# Plan Elements

- Mission
- Strategies and goals
- Senior management approval
- Organizational approach to incident response
- How the incident response team will communicate with the rest of the organization and with other organizations
- Metrics for measuring the incident response capability and its effectiveness
- Roadmap for maturing the incident response capability
- How the program fits into the overall organization.

# Policy Elements

- Policy governing incident response is highly individualized to the organization. However, most policies include the same key elements:
- Statement of management commitment
- Purpose and objectives of the policy
- Scope of the policy (to whom and what it applies and under what circumstances)
- Definition of computer security incidents and related terms
- Organizational structure and definition of roles, responsibilities, and levels of authority; should include the authority of the incident response team to confiscate or disconnect equipment and to monitor suspicious activity, the requirements for reporting certain types of incidents, the requirements and guidelines for external communications and information sharing (e.g., what can be shared with whom, when, and over what channels), and the handoff and escalation points in the incident management process
- Prioritization or severity ratings of incidents
- Performance measures
- Reporting and contact forms.

# Sharing Information With Outside Parties



# Measure the effectiveness and efficiency of the incident management function

- Total number of reported incidents
- Total number of detected incidents
- Average time to respond to an incident
- Average time to resolve an incident
- Total number of incidents successfully resolved
- Proactive and preventive measures taken
- Total number of employees receiving security awareness training
- Total damage from reported and detected incidents if incident response was not performed
- Total savings from potential damages from incidents resolved
- Total labor responding to incidents
- Detection and notification times

# Incident Management Roles

## Computer Security Incident Response

- Team Lead/Chairman
- Group Leaders
- Help Desk
- Incident Handlers
- Vulnerability Handlers
- Artifact Analysis Staff
- Platform Specialists
- Trainers
- Technology Watch
- Legal expert
- PR expert

## Key Incident Management Personnel

- Incident response coordinator (IRC)
  - Central point of contact for all incidents
  - Verifies and logs the incident
- Designated incident handlers (DIHs)
  - Senior-level personnel who have crisis management and communication skills, experience, and knowledge to handle an incident
- Incident response team (IRT)
  - Trained team of professionals that provide services through the incident lifecycle

# Incident Response Life Cycle

NIST SP 800-61

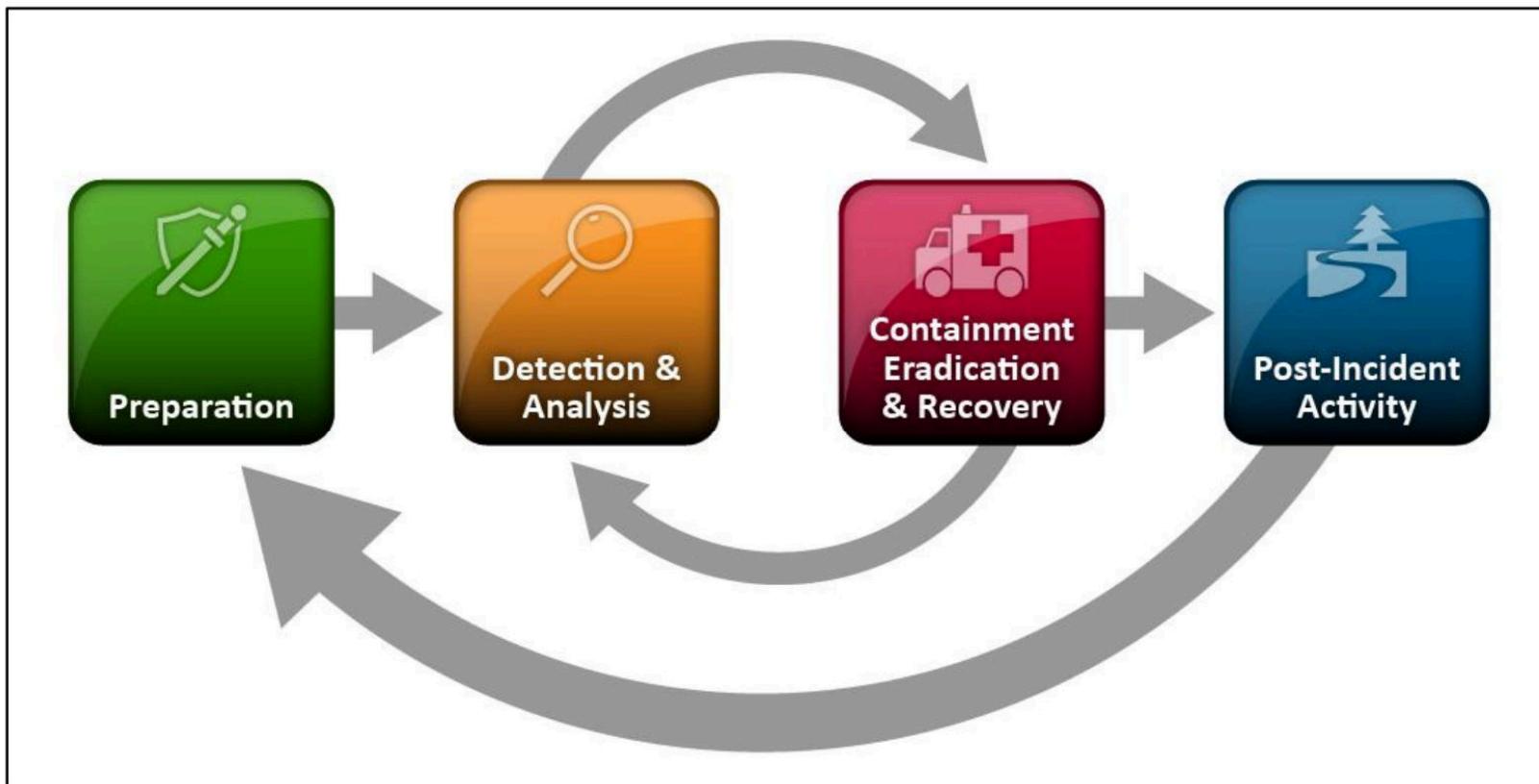


Figure 3-1. Incident Response Life Cycle

# Preparation

- Preparing to Handle Incidents
  - Incident Handler Communications and Facilities
  - Incident Analysis Hardware and Software
  - Incident Analysis Resources
  - Incident Mitigation Software
- Identifying the attack vectors — Removable media, web, email, impersonation, improper usage, loss or theft
- Preventing Incidents
  - Conducting Risk Assessments in defined regular intervals
  - All hosts should be hardened appropriately using standard configurations and patched.
  - The network perimeter should be configured to deny all activity that is not expressly permitted.
  - Malware Prevention Software to detect and stop malware should be deployed throughout the organization.
  - Users should be made aware of policies and procedures regarding appropriate use of networks, systems, and applications. Applicable lessons learned from previous incidents should also be shared with users

# Detection and Analysis

- Incident Detection
  - Alerts
  - Logs
  - Publicly available information
  - People
- Incident Analysis
- Incident Documentation
- Incident Prioritization
- Incident Notification

# **Containment, Eradication, and Recovery**

- Choose a containment strategy
  - Potential damage to and theft of resources
  - Need for evidence preservation
  - Service availability (e.g., network connectivity, services provided to external parties)
  - Time and resources needed to implement the strategy
  - Effectiveness of the strategy (e.g., partial containment, full containment)
  - Duration of the solution (e.g., emergency workaround to be removed in four hours, temporary workaround to be removed in two weeks, permanent solution).

# **Containment, Eradication, and Recovery**

- Evidence Gathering and Handling
- Identifying the Attacking Hosts
  - Validating the Attacking Host's IP Address.
  - Researching the Attacking Host through Search Engines
  - Using Incident Databases
  - Monitoring Possible Attacker Communication Channels
- Eradication and Recovery

# **Containment**

- After an incident has been identified and confirmed, the IMT is activated and information from the incident handler is shared.
- The team will conduct a detailed assessment and contact the system owner or business manager of the affected information systems/assets to coordinate further action.
- The action taken in this phase is to limit the exposure.
- Activities in this phase include:
  - Activating the incident management/response team to contain the incident
  - Notifying appropriate stakeholders affected by the incident – Obtaining agreement on actions taken that may affect availability of a service or risks of the containment process
  - Getting the IT representative and relevant virtual team members involved to implement containment procedures
  - Obtaining and preserving evidence
  - Documenting and taking backups of actions from this phase onward
  - Controlling and managing communication to the public by the public relations team

# Eradication

- When containment measures have been deployed, it is time to determine the root cause of the incident and eradicate it.
- Eradication can be done in a number of ways: restoring backups to achieve a clean state of the system, removing the root cause, improving defenses and performing vulnerability analysis to find further potential damage from the same root cause.
- Activities in this phase include:
  - Determining the signs and cause of incidents
  - Locating the most recent version of backups or alternative solutions
  - Removing the root cause. In the event of worm or virus infection, it can be removed by deploying appropriate patches and updated antivirus software.
  - Improving defenses by implementing protection techniques
  - Performing vulnerability analysis to find new vulnerabilities introduced by the root cause

# Recovery

- This phase ensures that affected systems or services are restored to a condition specified in the RPO.
- The time constraint up to this phase is documented in the **RTO**.
- Activities in this phase include:
  - Restoring operations to normal
  - Validating that actions taken on restored systems were successful
  - Getting involvement of system owners to test the system
  - Facilitating system owners to declare normal operation

# Post-Incident Activity - Lessons Learned

- Exactly what happened, and at what times?
- How well did staff and management perform in dealing with the incident?
- Were the documented procedures followed?
- Were they adequate?
- What information was needed sooner?
- Were any steps or actions taken that might have inhibited the recovery?
- What would the staff and management do differently the next time a similar incident occurs?
- How could information sharing with other organizations have been improved?
- What corrective actions can prevent similar incidents in the future?
- What precursors or indicators should be watched for in the future to detect similar incidents?
- What additional tools or resources are needed to detect, analyze, and mitigate future incidents?

# Lessons Learned Benefits

- Learn from mistakes of the flow.
  - Understand where problems occurred.
  - Recognize success.
  - Retain organizational knowledge.
  - Reduce future risk.
  - Improve future performance.
- Facilitate the recurrence of positive outcomes (“let’s repeat what went well”)
- Prevent the recurrence of negative outcomes (“let’s avoid making the same mistakes”)

# Security Operations Centers (SOC)

- A Security Operations Center is a highly skilled team following defined definitions and processes to manage threats and reduce security risk
- Responsible for monitoring and analyzing an organization's security posture on an ongoing basis.
- Goal is to detect, analyze, and respond to cybersecurity incidents using a combination of technology solutions and a strong set of processes.



# What is a SOC?

Security Operations Centers (SOC) are designed to:

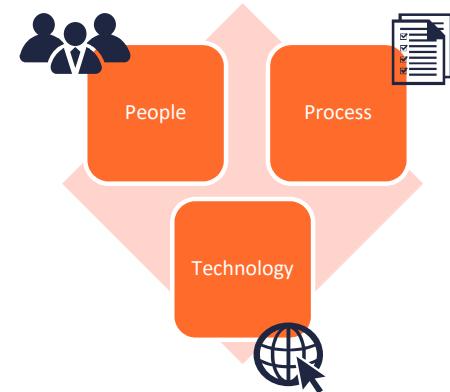
- protect mission-critical data and assets
- prepare for and respond to cyber emergencies
- help provide continuity and efficient recovery
- fortify the business infrastructure

The SOC's major responsibilities are:

- Monitor, Analyze, Correlate & Escalate Intrusion Events
- Develop Appropriate Responses; Protect, Detect, Respond
- Conduct Incident Management and Forensic Investigation
- Maintain Security Community Relationships
- Assist in Crisis Operations



# Triad of Security Operations



## People

- Formal Training
- On the job experience
- Vendor specific training
- Internal Training

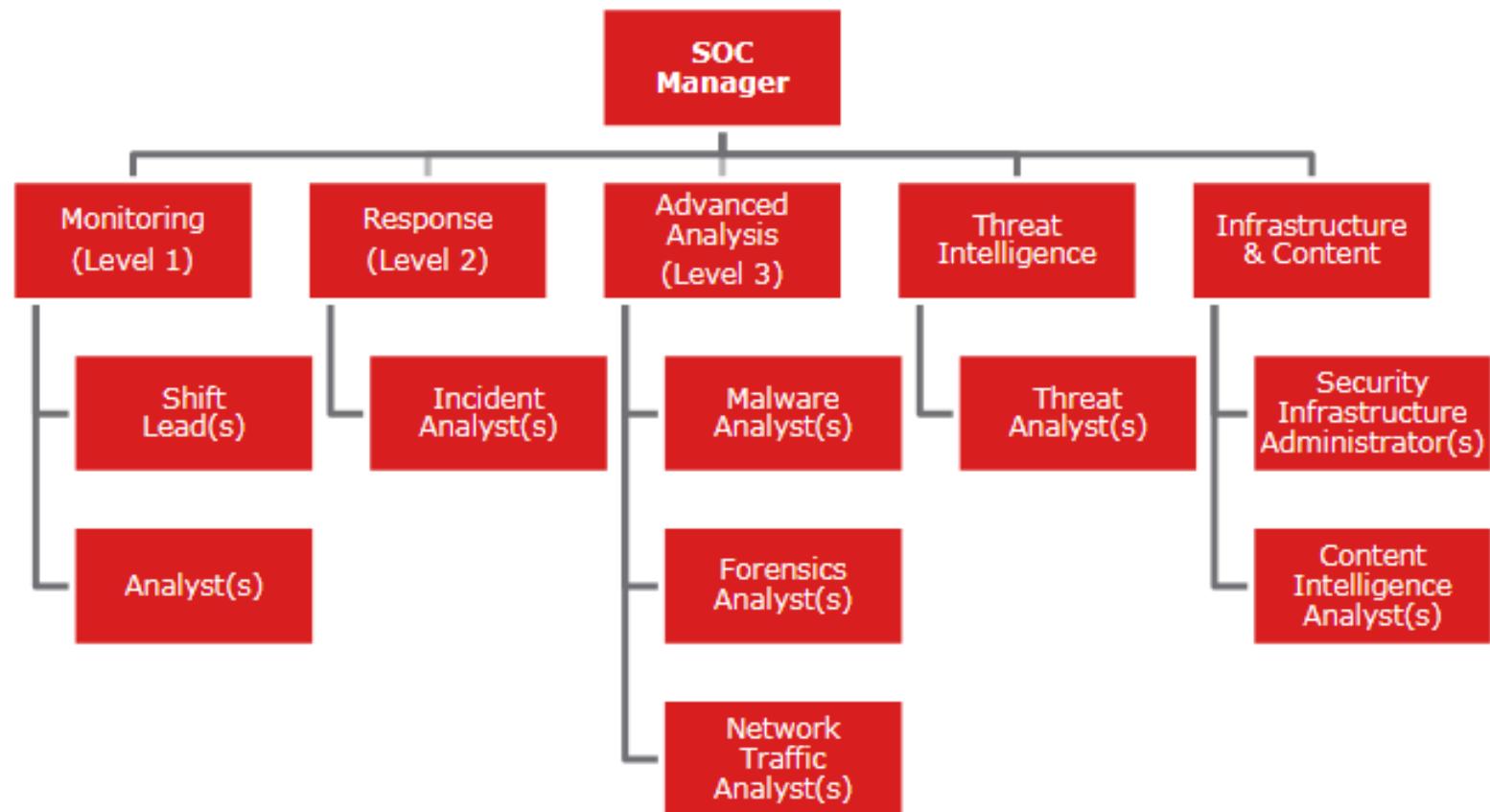
## Process

- Preparation
- Identification
- Containment
- Eradication
- Recovery
- Lessons learnt

## Technology

- End-points
- Net flow
- Network Monitoring
- Threat Intel
- Forensics
- Incident detection/management

# SOC Organization



# Organization Of SOC



**Analyst**

- Continuously monitors the alert queue
- Triage security alerts monitors health of security sensors and endpoints
- Collects data and context necessary to initiate Tier 2 work



**Incident Responder**

- Performs deep-dive incident analysis by correlating data from various sources
- Determines if a critical system or data set has been impacted
- Advises on remediation provides support for new analytic methods for detecting threats



**SME/Hunter**

- In-depth knowledge network, endpoint, threat intelligence, forensics & malware reverse engineering, Specific applications or underlying IT infrastructure
- Acts as an incident “hunter,” not waiting for escalated incidents
- Closely involved in developing, tuning & implementing threat detection analytics.



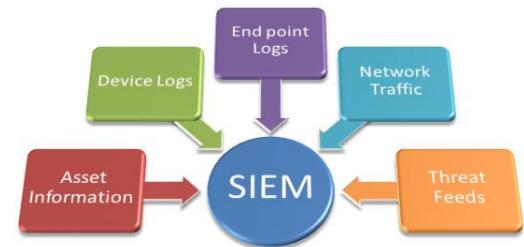
**SOC Manager**

- Manages resources to include personnel, budget, shift scheduling and technology strategy to meet SLAs
- Communicates with management
- Serves as organizational SPOC for business-critical incidents
- Provides overall direction for the SOC and input to the overall security strategy

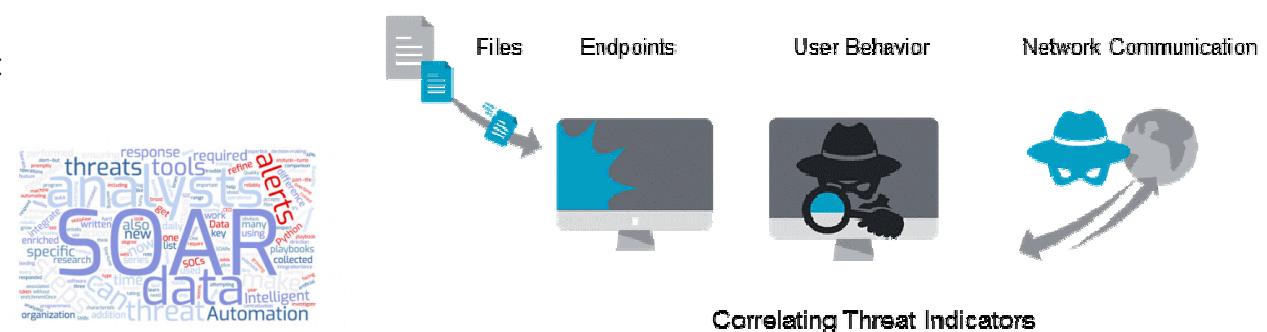
# KPIs for SOC

- Mean Time To Detect - MTTD
- Mean Time To Resolve - MTTR
- Number of False Positives
- Incidents Per Analyst
- Percentage of Recurring Incidents
- Number of SLA Breached Incidents

# Systems available in SOCs



- **SIEM: Security Information and Event Management** (SIEM) software centrally collects, stores, and analyzes logs from perimeter to end user. It monitors for security threats in real time for quick attack detection, containment, and response with holistic security reporting and compliance management
- **EDR: Endpoint Detection and Response** (EDR) is a cybersecurity technology that addresses the need for continuous monitoring and *response* to advanced threats. Helps enterprises detect, investigate and respond to IT security incidents by facilitating active threat hunting
- **SOAR: Security Orchestration, Automation and Response** is a solution stack of compatible software programs that allow an organization to collect data about security threats from multiple sources and respond to low-level security events without human assistance.
  - Main functions of SOAR
    - Threat & Vulnerability Management
    - Security Incident Response
    - Security Operations Automation



## **Incident Management Process (ISO/IEC 27035)**

- Plan and prepare
  - Detection and reporting
  - Assessment and decision
  - Response
  - Lessons learnt
- 
1. **Plan and prepare:** establish an information security incident management policy, form an **Incident Response Team etc.**
  2. **Detection and reporting:** someone has to spot and report “events” that might be or turn into incidents;
  3. **Assessment and decision:** someone must assess the situation to determine whether it is in fact an incident;
  4. **Responses:** contain, eradicate, recover from and forensically analyze the incident, where appropriate;
  5. **Lessons learned:** make systematic improvements to the organization’s management of information risks as a consequence of incidents experienced.

# File Systems

# Lecturer Resources



# File Systems vs. Operating Systems

- **File System:** The underlying system responsible for management, organization, and space allocation of files and directories on digital media.
  - No user interface
- **Operating System:** The software responsible for supporting basic computer functions, application execution, and interfacing with hardware and software.
  - Direct user interface

# Examples of File Systems & Operating Systems

- File Systems:

- File Allocation Table (FAT) - Windows
- New Technology File System (NTFS) - Windows
- Extended File System (EXT 1-4) – Linux
- Hierarchical File System (HFS) – Apple

- Operating Systems

- XP (Windows)
- 7 (Windows)
- Ubuntu (Linux)
- OSX (Apple)

# Remember -

- The File System organizes files and directories on a computer hard drive and the Operating System creates, executes and edits the files. They work together but are not the same!

# Traditional Library Card Analogy

- A file system is like a the Dewey Decimal library card system.
  - Each file is allocated its own card that shows name, location and some other pertinent details.



# Representations of Data

- Binary – Base 2 system.
  - The 1's and 0's of computer storage that form the most basic data structure in computing.
  - Magnetic media is simple positive / negative charges (off / on).
- Octal – Base 8 System
- Decimal – Base 10 system
  - This is the standard numbering system we use on a daily basis.

# Representations of Data

- Hexadecimal – Base 16 System.
  - \*\*Very commonly used in Computer Forensics!\*\*
  - Possible Representations: 0,1,2,3,4,5,6,7,8,9,A,B,C,D,E,F

Offset(h)	00	01	02	03	04	05	06	07	08	09	0A	0B	0C	0D	0E	0F	
00000000	49	46	43	49	20	70	72	6F	76	69	64	65	73	20	74	68	IFCI provides th
00000010	65	20	70	72	65	6D	69	65	72	20	63	79	62	65	72	63	e premier cyberc
00000020	72	69	6D	65	20	69	6E	76	65	73	74	69	67	61	74	69	rime investigati
00000030	6F	6E	20	74	72	61	69	6E	69	6E	67	20	69	6E	20	74	on training in t
00000040	68	65	20	77	6F	72	6C	64	21	21							he world!

- ASCII
  - American Standard Code for Information Interchange
  - 256 different possible representations
  - This is the original (and still common) representation of the English language on computers.

# Representations of Data

- Unicode
  - A.K.A: Universal Character Set
  - Replaced ASCII for data representation to accommodate foreign language characters.
    - Chinese Kanji, Russian Cyrillic, Greek, etc...
  - 65,536 different possible representations
    - 日本語は、ユニコードです。
    - (Japanese is Unicode)

Name	Length (bits)	Binary	Possible Outcomes	Equivalent to
Bit	1	1	2	Smallest possible unit of digital data
Nibble	4	1010	16	½ Byte or 1 Hex character Binary 1010 = Hex A
Byte	8	0100-0010 (Left & Right Nibbles)	256	One ASCII character (ie: 0100-0010 = B)
Word	16	1010-0101-1010-0101	65,536	One Unicode character (ie: 端)
Dword	32	1010-0101-1010-0101 1010-0101-1010-0101	4,294,967,296	4 Bytes (Possible variations in a CRC checksum)
Qword	64	01001001 01000110 01000011 01001001 0101101 01000011 01000011 01001001	A LOT!!!!	8 Bytes ← Binary = hex 43 46 52 53 20 35 30 30 = ASCII “IFCI-CCI”

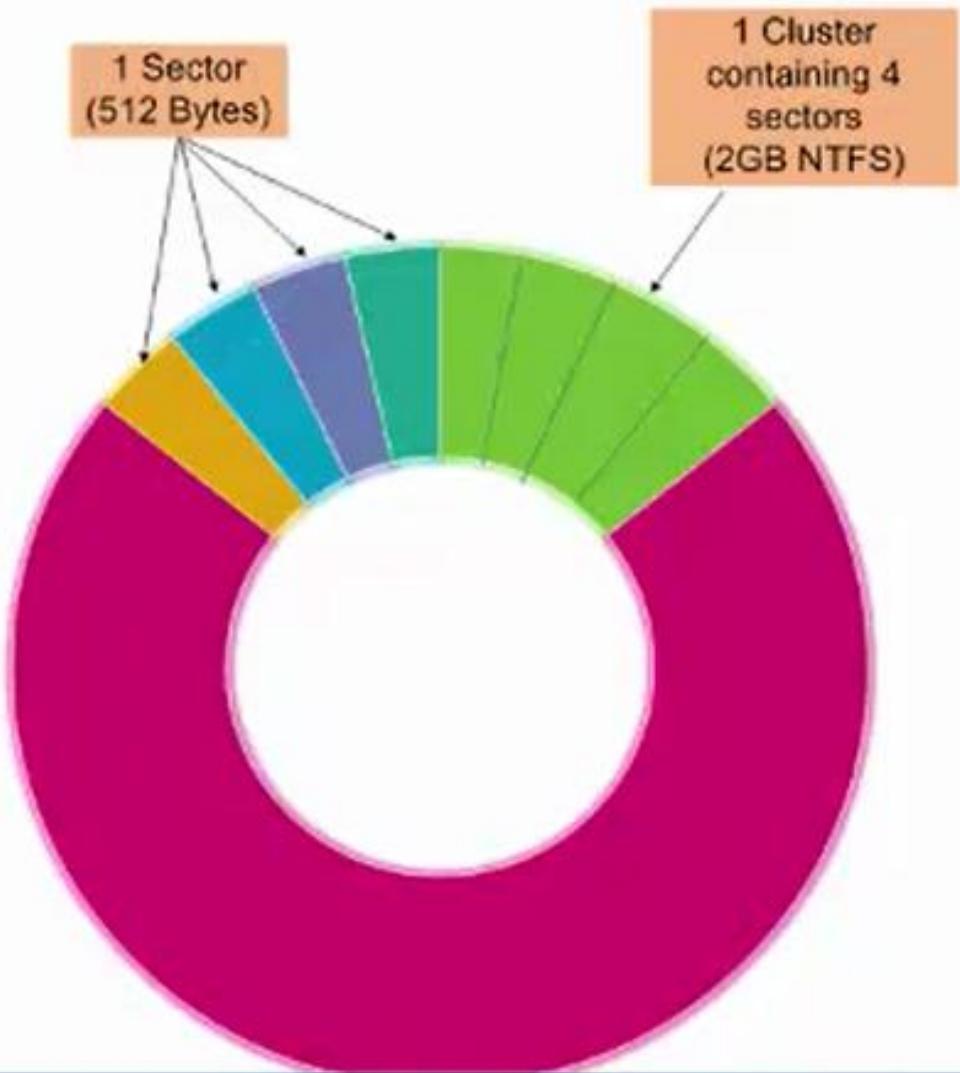
# Data Sizes to Know

- Each increasing unit of measurement 1,024 more than the previous.
  - Kilobyte – 1,024 bytes
  - Megabyte – 1,048,576 bytes
    - Approx: 500 typed pages of text
  - Gigabyte – 1,024 Megabytes
    - Approx: 650,000 typed pages of text
  - Terabyte – 1,048,576 Megabytes
    - Approx: 500 billion typed pages of text
  - Petabyte – 1024 Terabytes
  - Exabyte – 1,048,576 Terabytes
  - Zettabyte – 1 billion Terabytes
    - Still a theoretical size

# Hard Drive Data Structures

- Sector
  - 512 bytes
  - The smallest unit of data that can be written to in a hard drive.
- Cluster
  - The smallest allocation of data that a file system can write to.
  - File system specific.

# Sectors & Clusters



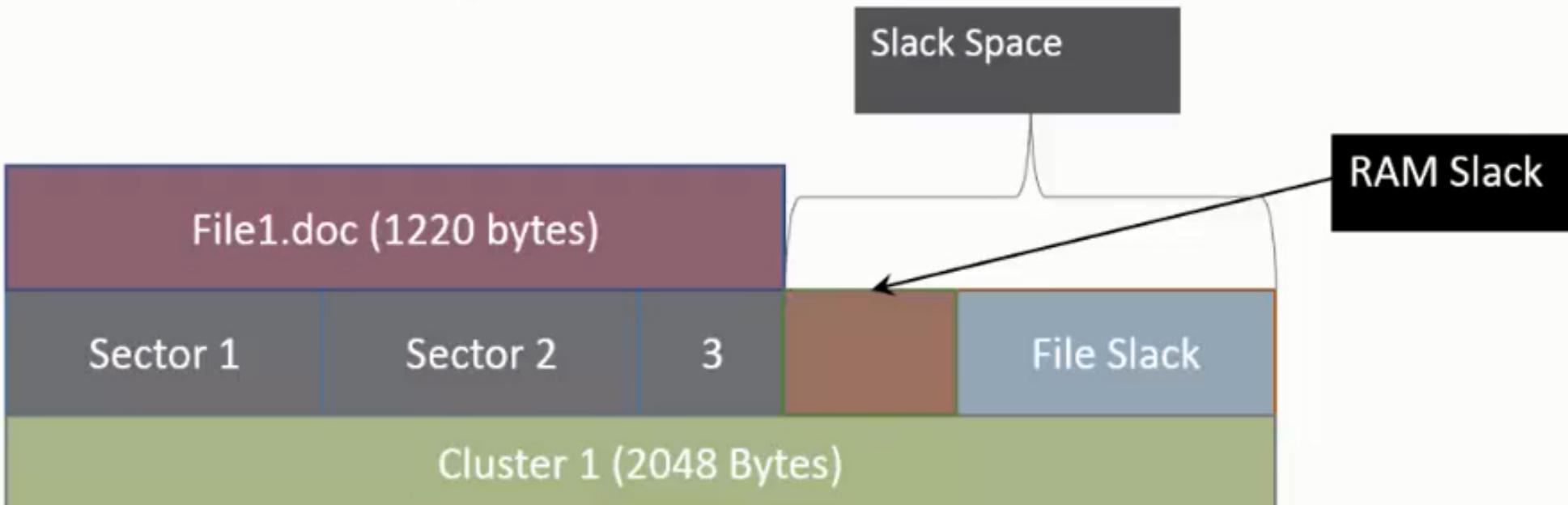
- A computer can save data to a single sector, however, the file system is limited to a cluster.
- Cluster size is dependant on the file system and Hard Drive size.

# File Systems – Sectors per Cluster

- FAT12 (Floppy disks) = 1 sector per cluster
- FAT16:
  - Up to 128 MB, 4 sectors per cluster
  - 128 to 256 MB, 8 sectors per cluster
  - 256 to 512 MB, 16 sectors per cluster
  - 512 MB to 1 GB, 32 sectors per cluster --- INEFFICIENT
  - 1GB to 4 Gb, 64 sectors per cluster --- HUGELY INEFFICIENT
- FAT32:
  - 512 MB to 8 GB, 8 sectors per cluster
  - 8 GB to 16 GB, 16 sectors per cluster
  - 16 GB to 32 GB, 32 sectors per cluster --- INEFFICIENT
  - More than 32 GB, 64 sectors per cluster --- HUGELY INEFFICIENT
- NTFS:
  - Up to 512 MB, 1 sector per cluster
  - 512 MB to 1 GB, 2 sectors per cluster
  - 1 GB to 2 GB, 4 sectors per cluster
  - More than 2 GB, 8 sectors per cluster

# Slack Space

- Slack space is area remaining between the end of a file and the end of the cluster.
  - RAM slack is the area remaining between the end of the file and end of the sector.
  - File Slack is the remaining unused sectors when a file is saved to a cluster.



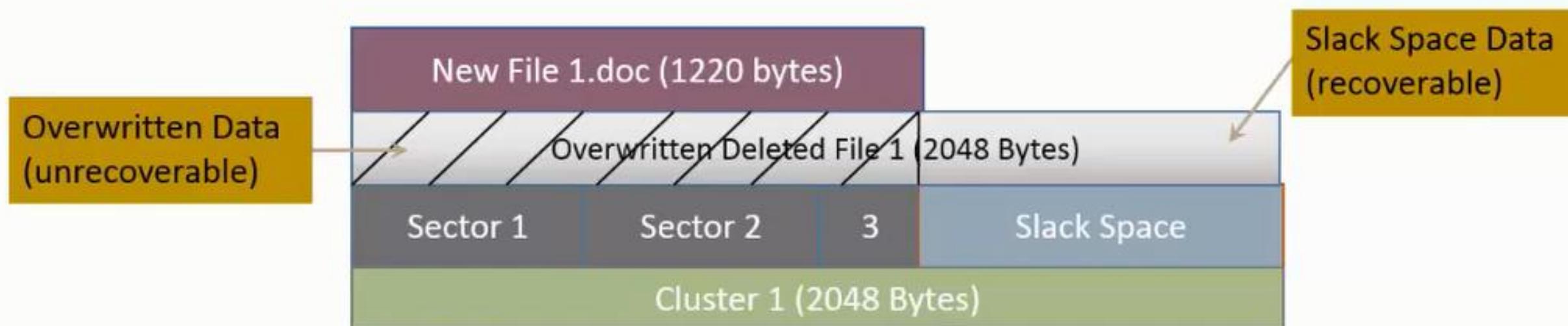
# Deleted Files



- When a file is deleted, the data remains on the hard drive.
  - *File Creation:* File system allocates clusters for the file's physical location on the hard drive.
  - *File Deletion:* File system removes the pointers allocating the clusters to the deleted file and marks them as "available".
  - The data remains in its original location until a new file is saved and written to its clusters.
- Building on the Library Card analogy:
  - When a file is deleted, it is like the library card being removed. The book is still there but its location is unknown. The file is still on the hard drive but the computer no longer recognizes it.

# Deleted File Remnants in Slack Space

- When a new file is saved to the same clusters that a deleted file was allocated, then the file is overwritten.
  - The overwritten data is unrecoverable.
- However, if the new file is smaller than the deleted file, then Slack Space is recoverable.
  - Slack Space may contain valuable evidence for your case.



# Traditional Video Tape Analogy

- Slack space can be compared to recording shows on a VHS tape.
  - You record a 3-hour football game on a video but before you get to watch it, your child records a 30 minute cartoon over your game.
  - The first 30 minutes of your game is gone but 2.5 hours of the football game remain.
  - The remaining 2.5 hours is “slack space”.



# File System Limitations

- FAT12
  - Used primarily in floppy disks. (Near obsolete now)
  - Can address a maximum of 4,096 files
  - Maximum 8 character file name with a three character extension. (ie: LongFilename.txt -> LongFi~1.txt)
  - Max drive volume size is 16MB.

# File System Limitations

- FAT16
  - Used in old versions of Windows.
  - Can address a maximum of 65,536 clusters
  - Maximum 8 character file name with a three character extension. (ie: LongFilename.txt -> LongFi~1.txt)
  - Max drive volume size is 2GB.

# File System Limitations

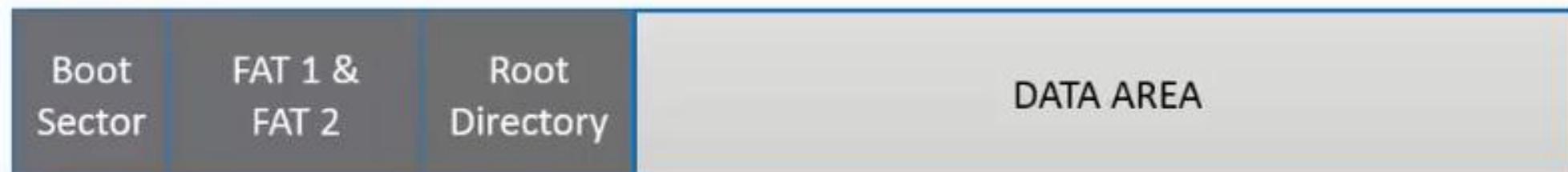
- FAT32
  - Used in old versions of Windows.
  - Can address a maximum of 268,435,456 clusters
  - Supports a 256 character long file name (LFN) and a 3 character extension.
  - Max File Size is 4GB.
  - Max drive volume size is 2TB.

# File System Limitations

- ExFAT (a.k.a FAT64)
  - Modern version of FAT used in USB drives, SD cards and other removable media.
  - Max volume size of 64 Zettabytes (theoretical) and 512 Terabytes (practical).
  - Max File Size is 16 Zettabytes.

# FAT Structure

- The FAT File system has the following components:
  - Boot Record – (Sector 0) Allows the OS to boot and communicate with the File System.
  - FATs – There are 2 FATs for redundancy. The FAT tracks cluster allocation. They are marked as:
    - Allocated, Unallocated, EOF or bad Sector.
  - Root Directory – Contains an entry for each file in the file system containing name, timestamps, starting cluster number, and file size.
  - Data Area – This is where files are physically written to.



# FAT – File Creation Sequence

- The following sequence occurs when a file is created in FAT.
  - The FAT is checked for free clusters.
  - Free clusters are located and the file is written to them.
  - The FAT is updated reflecting the clusters as being actively used.

# FAT – File Deletion Sequence

- When a file is deleted in FAT, the following sequence occurs:
  - The first character of the file to be deleted is changed to hex E5 (sigma character) in the root directory.
  - The FAT is zeroed out.
  - The data area remains untouched and is marked as unallocated and available for the file system.

# File System Limitations

- NTFS (New Technology File System)
  - Ubiquitous in modern Windows Computers.
  - Max File Size is 16 Exabytes (theoretical) & 16 Terabytes (practical).
  - Max Volume size is 256 Terabytes
  - Long File Names are allowed.

# NTFS – The MFT

- NTFS uses a file called the Master File Table (MFT) to track every file in the operating system. (Including the MFT itself and system files)
- The MFT maintains a duplicate of itself for redundancy.
- All Files in the MFT include a set of attributes that record file name, size, timestamps, security settings, etc...
- There are two Attribute sets:
  - Standard Information Attribute
  - File Name Attribute

# NTFS – Resident & Non-Resident Files

- NTFS stores files in one of two ways:
  - **Resident:** Files that are small enough to be stored in the file's actual MFT Entry (less than 1 KB ).
  - **Non-Resident:** Files that are too large for the MFT are stored in the data area and pointers are kept in the MFT to identify the location.

# Unallocated Space

- A.K.A. – White space, Free space, Available area.
- This is the data area that the File System has designated as available to write files to.
- Remember – When a file is deleted, the data remains on the hard drive. Therefore, information in unallocated space may contain useful data from previously deleted files.
- Data in unallocated clusters may also be partially overwritten.

# File Carving

- File carving refers to identifying files in unallocated space and using a forensic tool to mark the beginning and the end of the data and extracting it to a new file.
- Files may be complete or they may be partially overwritten.
- File identification is made easier by finding file headers and footers.  
(This will be discussed further in a later module)

# File Fragmentation

- The file system may identify non-contiguous clusters as available to write a file to.
- In this case, the file may be written to clusters in different parts of the drive.
- The file system retains the location information and the OS renders the files properly.
- However, it makes carving files from unallocated space more difficult.
- This is becoming less of a problem with the increasing size of hard drives.

File1.zip Cluster 1

File 1.zip Cluster 2

File 2.txt Cluster 1

File 1.zip Cluster 3

# Mobile Devices and Cloud Forensics

# Text Book

Nelson, B., Phillips, A., & Steuart, C. (2015). Guide to Computer Forensics and Investigations (5/e). Cengage Learning, Boston, MA

Fifth Edition

# GUIDE TO COMPUTER FORENSICS AND INVESTIGATIONS PROCESSING DIGITAL EVIDENCE

Bill Nelson, Amelia Phillips, Chris Steuart



PREPARING TOMORROW'S  
INFORMATION  
**SECURITY**  
PROFESSIONALS

# Objectives

- Acquisition procedures in mobile devices
- Social media forensics on mobile devices
- Mobile forensics tools
- Conducting a cloud investigation
- Challenges in cloud forensics

# Understanding Mobile Device Forensics

People store a wealth of information on cell phones

- People don't think about securing their phones

Items stored on cell phones:

- Incoming, outgoing, and missed calls
- Multimedia Message Service (MMS; text messages) and Short Message Service (SMS) messages
- E-mail accounts
- Instant-messaging (IM) logs
- Web pages
- Pictures, videos, and music files

# Understanding Mobile Device Forensics

Items stored on cell phones: (cont'd)

- Calendars and address books
- Social media account information
- GPS data
- Voice recordings and voicemail

A search warrant is needed to examine mobile devices because they can contain so much information

Investigating cell phones and mobile devices is one of the most challenging tasks in digital forensics

- No single standard exists for how and where phones store messages
- New phones come out about every six months and they are rarely compatible with previous models

# Inside Mobile Devices

Phones store system data in **electronically erasable programmable read-only memory (EEPROM)**

- Enables service providers to reprogram phones without having to physically access memory chips

OS is stored in ROM

- Nonvolatile memory
- Available even if the phone loses power

# Inside Mobile Devices

**Personal digital assistants (PDAs)** have been mostly replaced by iPods, iPads, and other mobile devices

Their use has shifted to more specific markets

- Such as medical or industrial PDAs

Peripheral memory cards used with PDAs:

- *Compact Flash (CF)*
- *MultiMediaCard (MMC)*
- *Secure Digital (SD)*

# Inside Mobile Devices

## Subscriber identity module (SIM) cards

- Found most commonly in GSM devices
- Consist of a microprocessor and internal memory
- GSM refers to mobile phones as “mobile stations” and divides a station into two parts:
  - The SIM card and the mobile equipment (ME)
- SIM cards come in various sizes
- Portability of information makes SIM cards versatile
- The SIM card is necessary for the ME to work and serves these additional purposes:
  - Identifies the subscriber to the network
  - Stores service-related information
  - Can be used to back up the device

# Understanding Acquisition Procedures for Cell Phones and Mobile Devices

The main concerns with mobile devices are loss of power, synchronization with cloud services, and remote wiping

All mobile devices have volatile memory

- Making sure they don't lose power before you can retrieve RAM data is critical

Mobile device attached to a PC via a USB cable should be disconnected from the PC immediately

- Helps prevent synchronization that might occur automatically and overwrite data

# Understanding Acquisition Procedures for Cell Phones and Mobile Devices (cont...)

Depending on the warrant or subpoena, the time of seizure might be relevant

Messages might be received on the mobile device after seizure

Isolate the device from incoming signals with one of the following options:

- Place the device in airplane mode
- Place the device in a paint can
- Use the Paraben Wireless StrongHold Bag
- Turn the device off

# Understanding Acquisition Procedures for Cell Phones and Mobile Devices (cont...)

The drawback of using these isolating options is that the mobile device is put into roaming mode

- Accelerates battery drainage

SANS DFIR Forensics recommends:

- If device is on and unlocked - isolate it from the network, disable the screen lock, remove passcode
- If device is on and locked - what you can do varies depending on the type of device
- If device is off - attempt a physical static acquisition and turn the device on

# Understanding Acquisition Procedures for Cell Phones and Mobile Devices (cont...)

Check these areas in the forensics lab :

- Internal memory
- SIM card
- Removable or external memory cards
- Network provider

Checking network provider requires a search warrant or subpoena

- A new complication has surfaced because backups might be stored in a cloud provided by the carrier or third party

# Understanding Acquisition Procedures for Cell Phones and Mobile Devices (cont...)

Information that can be retrieved falls into four categories:

- Service-related data, such as identifiers for the SIM card and the subscriber
- Call data, such as numbers dialed
- Message information
- Location information

If power has been lost, PINs or other access codes might be required to view files

# Mobile Forensics Equipment

Mobile forensics is an evolving science

Biggest challenge is dealing with constantly changing phone models

Procedures for working with mobile forensics software:

- Identify the mobile device
- Make sure you have installed the mobile device forensics software
- Attach the phone to power and connect cables
- Start the forensics software and download information

# Mobile Forensics Equipment (cont...)

## SIM card readers

- A combination of hardware/software device used to access the SIM card
- You need to be in a forensics lab equipped with appropriate antistatic devices
- General procedure is as follows:
  - Remove the back panel of the device
  - Remove the battery
  - Remove the SIM card from holder
  - Insert the SIM card into the card reader

# Mobile Forensics Equipment (cont...)

## SIM card readers (cont'd)

- A variety of SIM card readers are available
  - Some are forensically sound and some are not
- Documenting messages that haven't been read yet is critical
  - Use a tool that takes pictures of each screen

## Mobile forensics tools

- AccessData FTK Imager
- MacLockPick 3.0

# Mobile Forensics Equipment (cont...)

NIST guidelines list six types of mobile forensics methods:

- Manual extraction
- Logical extraction
- Hex dumping and Joint Test Action Group (JTAG) extraction
- Chip-off
- Micro read

# Mobile Forensics Equipment (cont...)

- Paraben Software offers several tools:
  - Device Seizure - used to acquire data from a variety of phone models
  - Device Seizure Toolbox - contains assorted cables, a SIM card reader, and other equipment
- BitPam - used to view data on many CDMA phones
- Cellebrite UFED Forensic System - works on smartphones, PDAs, tablets, and GPS devices
- MOBILedit Forensic - contains a built-in write-blocker

# Mobile Forensics Equipment (cont...)

- Roughly half of Facebook users access their accounts via mobile devices
- Following standard procedures, doing a logical acquisition followed by a physical acquisition, can yield solid evidence

# Mobile Forensics Equipment (cont...)

Cellebrite and XRY are often used by law enforcement

- You can determine the device's make and model, hook up the correct cable, turn the device on, and retrieve the data
- There are more than half a million apps for mobile devices and Cellebrite or XRY can analyze data from only a few hundred

# Mobile Forensics Tools in Action

- Many mobile forensics tools are available
  - Most aren't free
- Methods and techniques for acquiring evidence will change as market continues to expand and mature
- Subscribe to user groups and professional organizations to stay abreast of what's happening in the industry

# Mobile Forensics Tools in Action (cont...)

## New Technologies and Challenges

- Type 2 hypervisors for mobile devices are under development and will add another level of complexity to forensics investigations
- The number of devices that connect to the Internet is higher than the amount of people
  - That number is expected to grow even larger as more devices are being developed to attach to the Internet
- Wearable computers will pose many new challenges for investigators

# Basic Concepts of Cloud Forensics

Cloud forensics is considered a subset of network forensics

Cloud forensics can have three dimensions:

- Organizational - addresses the structure of the cloud
- Legal - covers service agreements and other jurisdictional matters
- Technical - deals with procedures and specialized applications designed to perform forensics recovery and analysis in the cloud

# Basic Concepts of Cloud Forensics

Forensic tool capabilities needed to handle acquiring data from a cloud:

- *Forensic data collection* - must be able to identify, label, record, and acquire data from the cloud
- *Elastic, static, and live forensics* - must be able to expand and contract their storage capabilities
- *Evidence segregation* - different businesses and users share the same applications and storage space
- *Investigations in virtualized environments* - should have the capability to examine virtual systems

# Legal Challenges in Cloud Forensics

When investigating a cloud system, consider factors involving a CSP's relationship with cloud users

This section explains:

- A CSP's contract obligations with cloud users
- How warrants and subpoenas are applied to CSPs and users
- Service Level Agreements (SLAs)
  - CSP components must state who is authorized to access data and what limitations are in conducting acquisitions for an investigation

# Jurisdiction Issues

- No plans to revise current laws
  - Many cross-jurisdiction legal issues haven't been resolved
- No law ensures uniform access or required handling procedures for the cloud
- Investigators should be concerned about cases involving data commingled with other customers' data
- Often, figuring out what law controls data stored in the cloud is a challenge

# Jurisdiction Issues

- How privacy rights are defined in different jurisdictions is a major factor in problems with the right to access data
- EU Directive 95/46/EC is more restrictive than rules in other countries, including the U.S.
  - Protects private information for all EU citizens
- Digital forensics examiners could be held liable when conducting an investigation involving cloud data
  - Consult with legal experts to be aware of possible restrictions

# Accessing Evidence in the Cloud

## Search Warrants

- Can be used only in criminal cases and must be requested by a law enforcement officer who has evidence of probable cause that a crime was committed
- Law requires search warrants to contain specific descriptions of what's to be seized
- For cloud environments, the property to be seized usually describes data rather than physical hardware, unless the CSP is the suspect
- Must also describe the location of items to be seized
  - Difficult when dealing with cloud data because servers are often dispersed across state or national borders
- Must establish how it will be carried out
  - Specifying the date and time of day to minimize disruptions to people and business operations

# Accessing Evidence in the Cloud

## Subpoenas and Court Orders

- *Government agency subpoenas* - customer communications and records can't be knowingly divulged to any person or entity
  - Used to get information when it's believed there's a danger of death or serious physical injury
- *Non-government subpoenas* - used to produce information from private parties for litigation
- *Court orders* - written by judges to compel someone to do or not do something

# Technical Challenges in Cloud Forensics

## Challenges in conducting cloud forensics

- Architecture
- Data collection
- Analysis of cloud forensic data
- Anti-forensics
- Incident first responders
- Role management
- Legal issues
- Standards and training

# Acquisitions in the Cloud

- Methods used to collect evidence in cloud investigations depend on the nature of the case
- Recovering deleted data from cloud storage might be limited to the type of file system the CSP uses
- With cloud systems running in a virtual environment, snapshots can give you valuable information before, during, and after an incident
  - Forensic examiners should re-create separate cloud servers from each snapshot, acquire an image of each server, and calculate a hash for all files

# Encryption in the Cloud

Many CSPs and third parties offer encryption services for cloud users as a security measure

- Expect to find encrypted files in cloud investigations

You need assistance from the data owner or the CSP to decrypt data with the right encryption key

- If data owner is uncooperative, you may need to turn to the attorneys handling the case or data owner's management

# Investigating CSPs

If a CSP has no team or limited staff, investigators should ask the following questions to understand how the CSP is set up:

- Does the investigator have the authority to use cloud staff and resources to conduct an investigation?
- Is detailed knowledge of the cloud's topology, policies, data storage methods, and devices available?
- Are there any restrictions on collecting digital evidence from remote cloud storage?

# Investigating CSPs

Investigators should ask the following questions to understand how the CSP is set up (cont'd):

- For e-discovery demands on multitenant cloud systems, is the data to collect commingled with other cloud customers' unrelated data? Is there a way to separate the data to prevent violating privacy rights or confidentiality agreements?
- Is the data of interest to the investigation local or remote? If it's in a remote location, can the CSP provide a forensically sound connection to it?

# Investigating Cloud Customers

If a cloud customer doesn't have the CSP's application installed

- You might find cloud-related evidence in a Web browser's cache file

If the CSP's application is installed

- You can find evidence of file transfers in the application's folder
- Usually found under the user's account folder

# Examining Stored Cloud Data on a PC

- Three widely used cloud services:
  - Dropbox
  - Google Drive
  - OneDrive
- Services are free for storage up to 2 GB for Dropbox and up to 15 GB for Google Drive and OneDrive
- These applications have Registry entries
- Users must maintain control over access to their cloud accounts

# Examining Stored Cloud Data on a PC

- Dropbox offers third-party applications, such as e-mail, chat, Cisco WebEx, and other collaborative tools
- Since 2012, Dropbox has used base-64 format to store content
  - Reading them requires specialized software
  - Magnet Forensics has a tool called Internet Evidence Finder (IEF) Triage designed for this purpose
  - Dropbox Reader is another utility that can read Dropbox files

# Examining Stored Cloud Data on a PC

- Gmail users have access to Google Drive for cloud data storage and applications
- Google Drive is installed in:
  - C:\Program Files (x86)\Google\Drive
- Each user has a configuration file stored in C:\Users\username\AppData\Local\Google\Drive
  - Called a “user profile”
- If Google Drive has been installed, it creates a folder in the path C:\Users\username\Google Drive

# Examining Stored Cloud Data on a PC

## Important Google Drive files:

- sync\_config.db - an SQL database file with Google Drive upgrade number, highest application version number, and local synchronization root path
- snapshot.db - contains information about each file accessed, the URL pathname, the modified and created dates and times in UNIX timestamp format, and the file's MD5 value and size
- sync\_log.log - has a detailed list of user's cloud transactions

# Examining Stored Cloud Data on a PC

- OneDrive - created by Microsoft and was originally called SkyDrive
  - Available with Windows 8
  - Similar to DropBox and Google Drive and offers subscription services for Microsoft software
- OneDrive stores user profiles in the user's account path
- Log files and synchronized files are kept in various places under the user's account (depending on the Windows version)

# Tools for Cloud Forensics

- Few tools designed for cloud forensics are available
- Many digital, network, and e-discovery tools can be combined to collect and analyze cloud data
- Some vendor with integrated tools:
  - Guidance Software EnCase eDiscovery
  - AccessData Digital Forensics Incident Response
  - Forensic Open-Stack Tools (FROST)
  - F-Response
  - ProDiscover Incident Response and Forensics

# Volatile Memory Forensics

By

Chirath De Alwis

# What is volatile memory forensics?

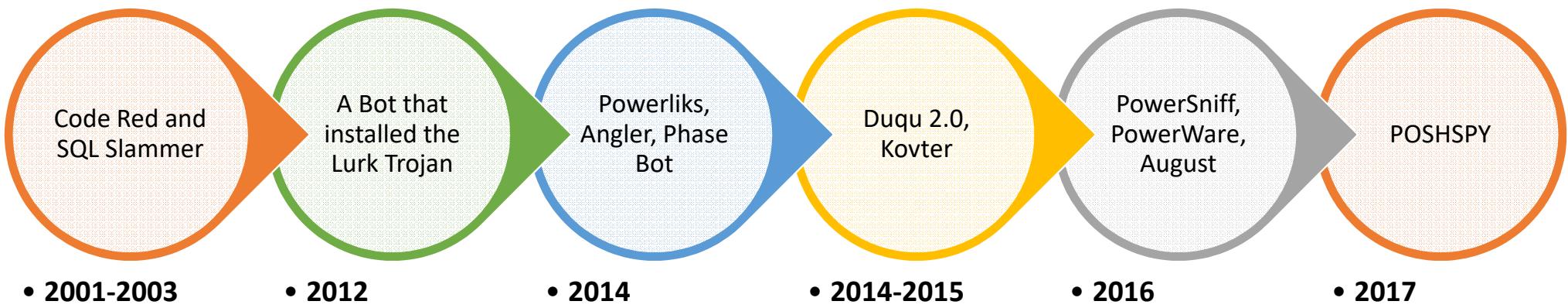
Identification, preservation, extraction, analysis and representation of  
**volatile memory artifacts**

Simplest term “**forensics investigation in volatile memory**”

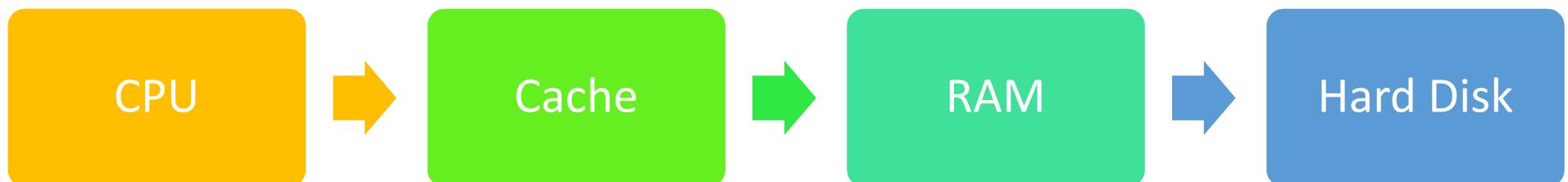
# Why volatile memory forensics?

- Everything in the OS travels **through** memory
- **Best way** to detect & analyze memory-resident malware  
Eg: Slammer worm
- Data encrypted in transport layer is **available** in plain text format
- Private browsing data is **only available** in volatile memory

# History of File-less Malware



# Why volatile memory forensics?



## Recent usage

WannaCry "*does not erase the prime numbers from memory before freeing the associated memory,*" says Guinet (May, 2017).

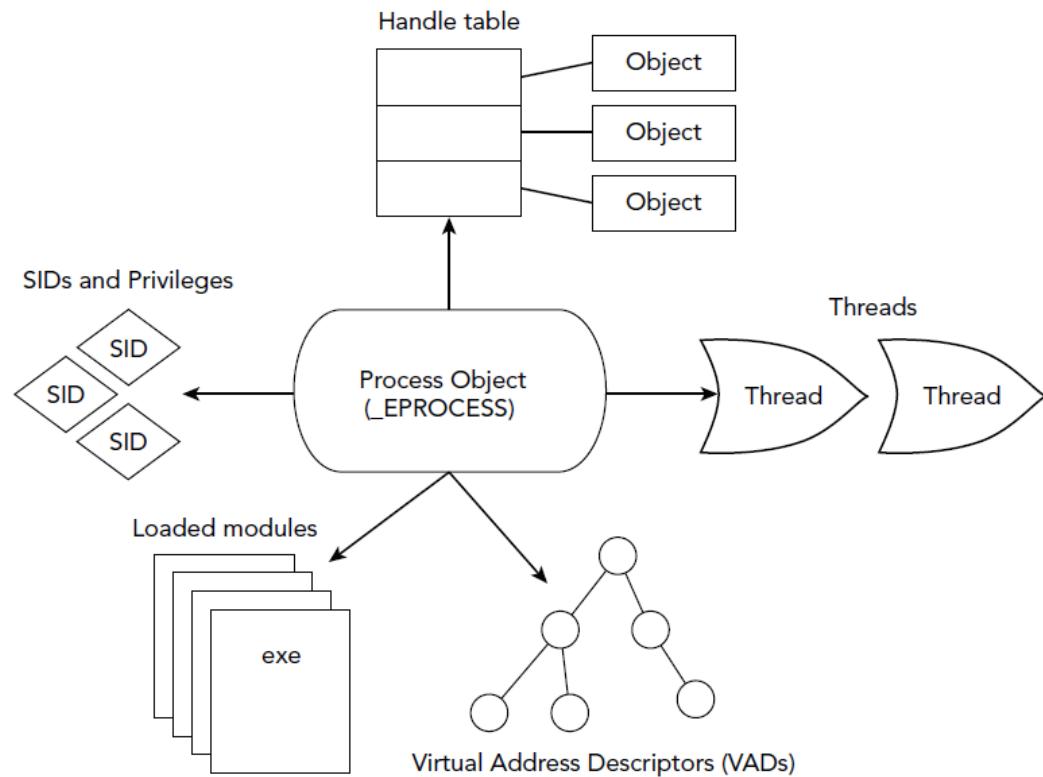
Based on this finding, Guinet released a WannaCry ransomware decryption tool, named [WannaKey](#)

**Complete article:** <http://thehackernews.com/2017/05/wannacry-ransomware-decryption-tool.html>

# Process Management - Processes

- A process is an instance of a program executing in memory
- Multiprogramming allows many processes to appear to execute simultaneously
- New process is created with its own ID (process ID) and address space
- Memory analysis involves enumerating the processes that were executing on a system and analyzing the data stored within their address spaces, including passwords, URLs, encryption keys, e-mail, and chat logs

# Process Management – Processes



A high-level diagram showing basic process resources

# Process Management - Processes

- `_EPROCESS` is the name of the structure that Windows uses to represent a process
- Each process has one or more threads that execute code
- Each process has a table of handles (or file descriptors) to kernel objects such as files and network sockets

# Process Management - Processes

- The process address space contains;
  - process executable
  - its list of loaded modules (DLLs or shared libraries)
  - Stacks
  - Heaps
  - allocated memory regions containing everything from user input to application-specific data structures

# Process Management - Threads

- A thread is the basic unit of CPU utilization and execution
- Often characterized by a thread ID, CPU register set, and execution stack(s), which help define a thread's execution context
- A process with multiple threads can appear to be simultaneously performing multiple tasks
- Thread data structures often contain timestamps and starting addresses

# Process Management - Handles

- Reference to an open instance of a kernel object, such as a file, registry key, mutex, process, or thread
- Before a process can access an object, it first opens a handle to the object
- When a process is finished using an object, it should close the handle by calling the appropriate function

# Process Management – VAD Tree

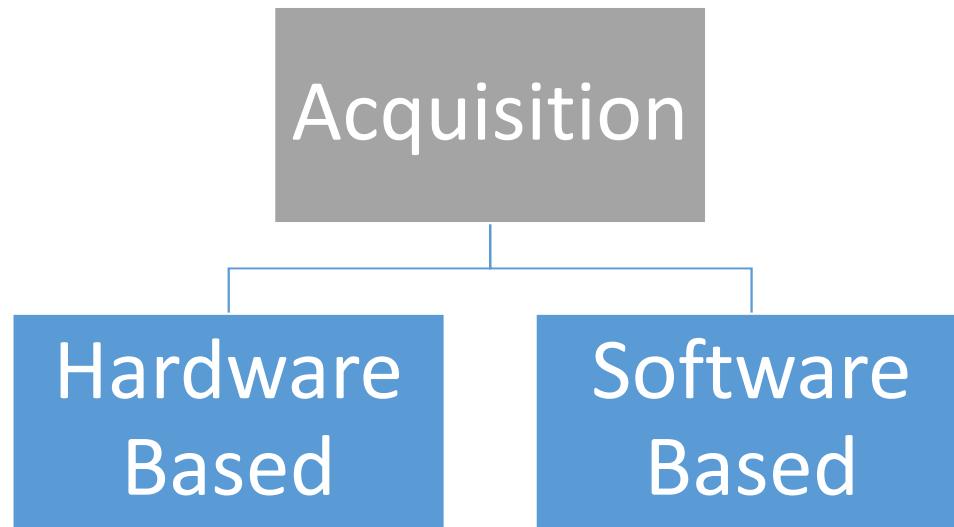
- Processes are stored in Windows in Virtual Address Descriptor (VAD) tree
- It describes memory ranges used by currently-running processes
- Most information about processes can be retrieved from walking VAD tree
- Possible to recover all of the memory-mapped files associated with specific processes

# Acquisition



# Acquisition

- Converting volatile memory into non-volatile state for future analysis



# Acquisition

- **Hardware-based acquisition**

- Involves suspending the computer's processor and using direct memory access (DMA) to obtain a copy of memory
- Do not rely on OS and software
- More reliable
- Expensive

# Acquisition

- **Software-based acquisition**
  - Need trusted software
  - Some tools available in OS (eg: memdump or dd on Unix systems)
  - Need OS
  - Execution can overwrite some data

# Memory Dump Formats

- **RAW memory dump**
  - Widely used
  - Does not contain any headers, metadata, or magic values for file type identification
  - Typically includes padding for any memory ranges that were intentionally skipped (i.e., device memory) or that could not be read by the acquisition tool

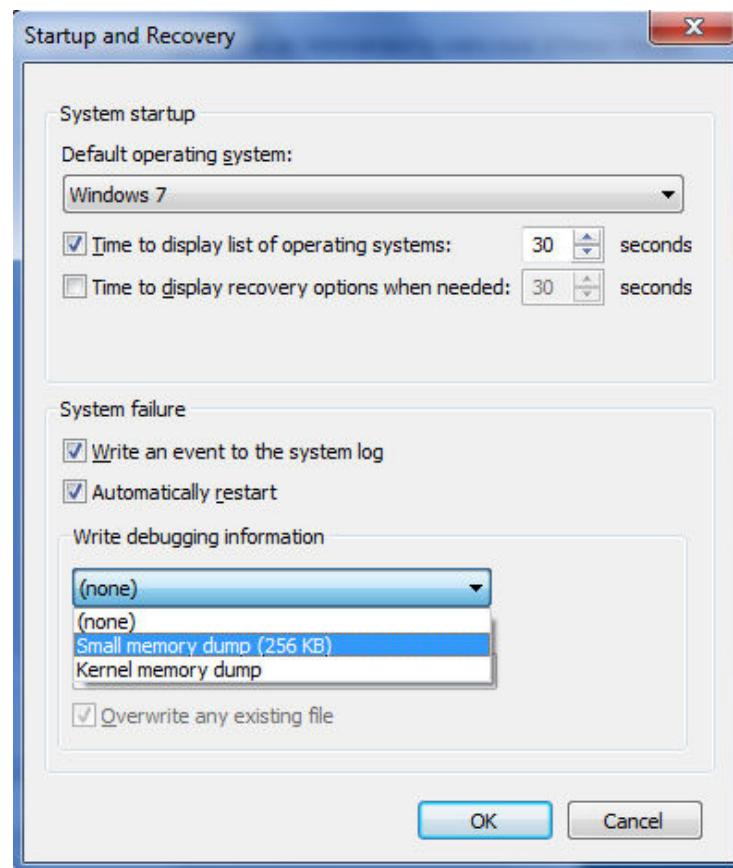
# Memory Dump Formats

- **Windows crash dump**
  - When Windows OS crashes (Blue Screen of Death or BSOD) it dumps all the memory information into a file on disk
  - The default location of the dump file is `%SystemRoot%memory.dmp` or `C:\Windows\memory.dmp` if C: is the system drive
  - Designed for debugging purposes

# Memory Dump Formats

- **Windows crash dump**
  - There are four types;
    - **Complete memory dump** – records all the contents of system memory when your computer stops unexpectedly
    - **Kernel memory dump** - records only the kernel memory
    - **Small memory dump** - records the smallest set of useful information that may help identify why your computer stopped unexpectedly

# Memory Dump Formats

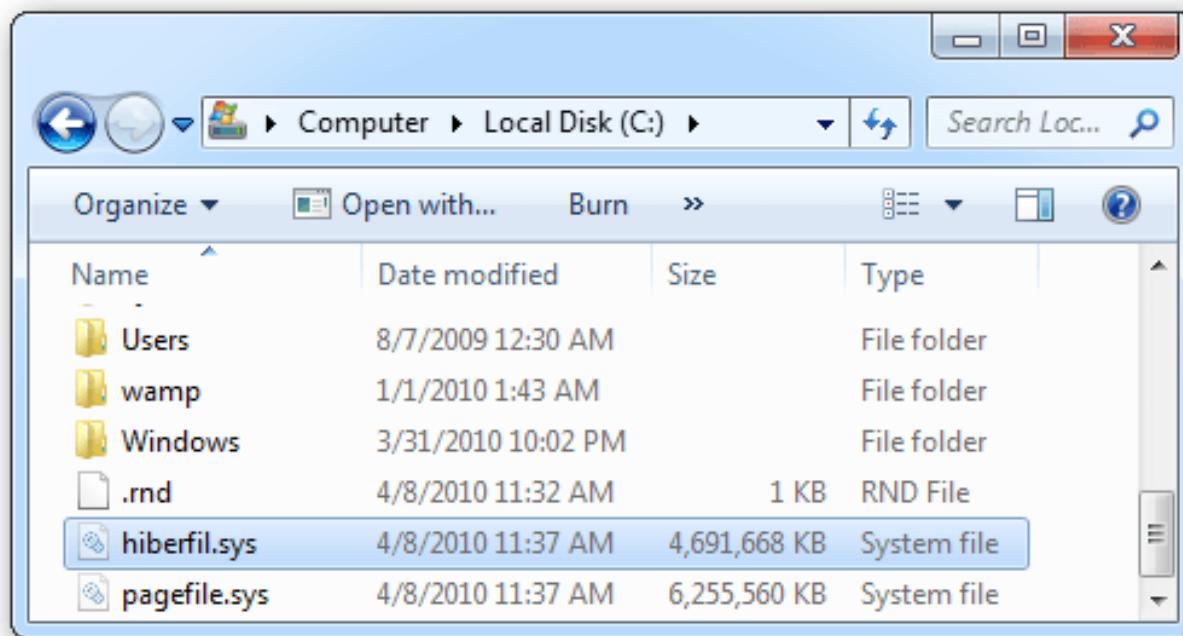


# Memory Dump Formats

- **Windows hibernation file**
  - File name is “hiberfil.sys”
  - Contains a compressed copy of memory that the system dumps to disk during the hibernation process
  - Need to convert into normal memory dump format before analysis

# Memory Dump Formats

- Windows hibernation file



# Memory Dump Formats

- **Expert Witness Format (EWF)**

- EnCase proprietary
- Need to familiar with
  - WEFAddressSpace
  - Mounting with EnCase
  - Mounting with FTK



# Memory Dump Formats

- **HPAK Format**
  - Developed by HBGary
  - It allows a target system's physical memory and page file(s) to embed in the same output file
  - Proprietary format



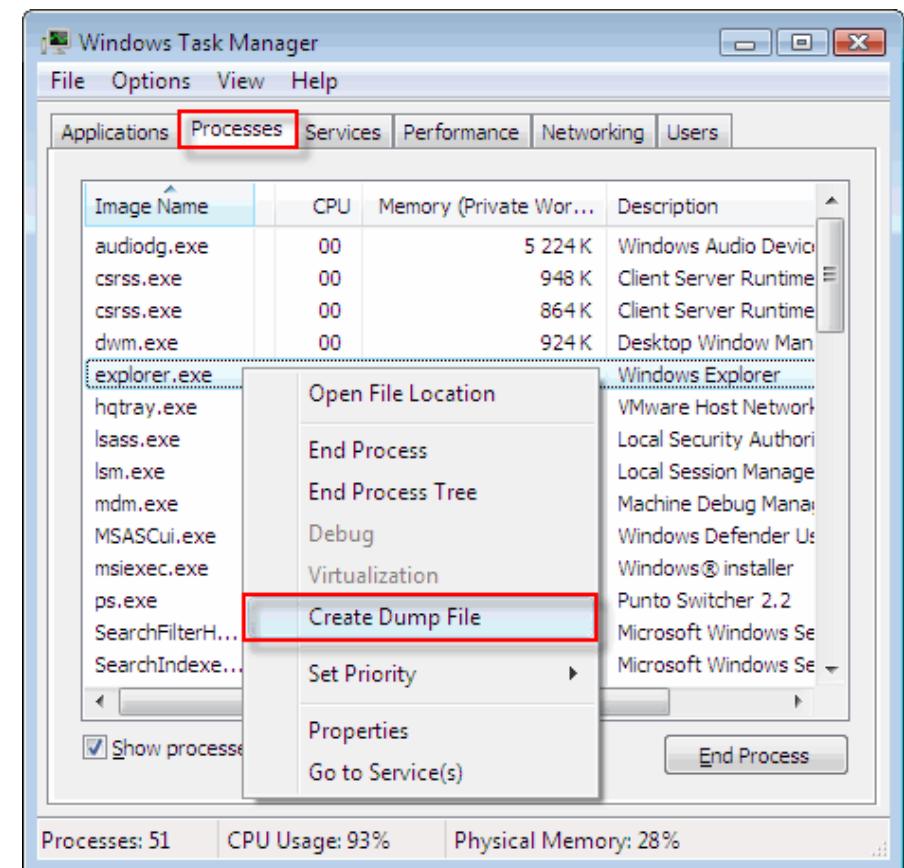
# Memory Dump Formats

- **Virtual machine memory**

- Depend on the virtual machine you use

- **Process dump**

- Small in size
- Memory related to process



# Analysis



# Current Analysis Techniques

- **String search**
  - Looks for specific strings/key words

Address	Hex	ASCII	Description
006CEE090	20 20 20 20 20 3C 53 6B	20 20 20 20 20 <SkypeHomeL	
006CEE0A0	61 73 74 55 70 64 61 74	astUpdate>0</Sky	
006CEE0B0	70 65 48 6F 6D 65 4C 61	peHomeLastUpdate	
006CEE0C0	3E 0D 0A 20 20 20 20 20	> <UserAv	
006CEE0D0	61 74 61 72 50 61 74 68	atarPath>C:\User	
006CEE0E0	73 5C 63 68 69 72 61 74	s\chirath-PC\AppData	
006CEE0F0	44 61 74 61 5C 52 6F 61	\Roaming\Sky	
006CEE100	6D 69 6E 67 5C 53 6B 79	Data\chirathalwi\	
006CEE110	70 65 5C 63 68 69 72 61	pe\chirathalwi\Pictures\</UserA	
006CEE120	74 68 61 6C 77 69 73 5C	vatarPath>	
006CEE130	50 69 63 74 75 72 65 73	<VideoChatHeig	
006CEE140	76 61 74 61 72 50 61 74	ht>214</VideoCha	
006CEE150	68 3E 0D 0A 20 20 20 20	tHeight>	
006CEE160	65 63 68 6F 31 32 33 41	<echo123Added>1<	
006CEE170	64 64 65 64 3E 31 3C 41	/echo123Added>	

# Current Analysis Techniques

- **File signature search**

- Specific patterns of values that are unique to the particular type of file in question
- Content in between header and its corresponding footer is belongs to that particular file
- Helps to carve files from memory

# Current Analysis Techniques

- File signature search

**Header FFD8**



**Footer FFD9**

# Current Analysis Techniques

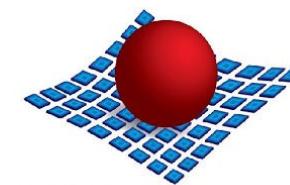
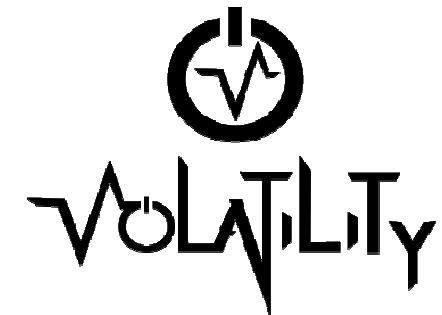
- **Recovering memory-mapped files**
  - Can be recovered from walking VAD tree and pulling the objects of interest

# Challenges in Memory Forensics

- Volatility
- Address space randomization
- OS changes (internal structure, memory utilization and management differences in multiple OS versions)
- Cloud and VM infrastructure
- Dependencies in file carving

# Current Tools

- Volatility
- Redline
- Rekall
- Windows SCOPE



# Sample Analysis



```
# vol.py --f APT.img -profile=WinXPSP3x86 pstree
```

Name	Pid	PPid	Thds	Hnds	Time
<hr/>					
0x823c8830:System	4	0	55	254	1970-01-01 00:00:00
. 0x8230aad8:smss.exe	564	4	3	19	2009-04-16 16:10:01
.. 0x81f63020:winlogon.exe	660	564	16	502	2009-04-16 16:10:06
... 0x81f22020:services.exe	704	660	15	254	2009-04-16 16:10:06
.... 0x81f739b0:svchost.exe	1088	704	70	1445	2009-04-16 16:10:07
..... 0x81f96220:wscntfy.exe	1260	1088	1	39	2009-04-16 16:10:22
.... 0x81da4590:svchost.exe	968	704	10	241	2009-04-16 16:10:07
.... 0x81dc2570:VMwareService.e	1032	704	3	175	2009-04-16 16:10:16
.... 0x8231eda0:msiexec.exe	1464	704	6	294	2009-04-16 16:11:02
.... 0x81e54da0:svchost.exe	884	704	17	208	2009-04-16 16:10:07
.... 0x81dbdda0:iexplore.exe	796	884	8	152	2009-05-05 19:28:28
.... 0x81e91da0:svchost.exe	1212	704	14	208	2009-04-16 16:10:09
.... 0x81d33628:alg.exe	464	704	6	105	2009-04-16 16:10:21
.... 0x8219b630:spoolsv.exe	1512	704	10	129	2009-04-16 16:10:10
.... 0x822cb458:vmacthlp.exe	872	704	1	25	2009-04-16 16:10:07
.... 0x8232c020:svchost.exe	1140	704	5	60	2009-04-16 16:10:08
... 0x82164da0:lsass.exe	716	660	21	342	2009-04-16 16:10:06
.. 0x822ca2c0:csrss.exe	636	564	10	356	2009-04-16 16:10:06
0x81da71a8:explorer.exe	1672	1624	15	586	2009-04-16 16:10:10
. 0x81f1c7e8:VMwareTray.exe	1984	1672	1	37	2009-04-16 16:10:11
. 0x81e4d648:cmd.exe	840	1672	1	33	2009-05-05 15:56:24
.. 0x82161558:MIRAgent.exe	456	840	1	77	2009-05-05 19:28:40
. 0x81dc1a78:VMwareUser.exe	2004	1672	8	228	2009-04-16 16:10:11
. 0x81f1a650:ctfmon.exe	2020	1672	1	71	2009-04-16 16:10:11

- iexplore.exe (PID 796) was spawned from svchost.exe (pid 884)
- Iexplore.exe should be launched from explorer.exe

```
# vol.py --f APT.img -profile=WinXPSP3x86 connscan
```

Offset(P)	Local Address	Remote Address	Pid
0x0205ece0	192.168.157.10:1050	222.128.1.2:443	1672
0x020611f8	192.168.157.10:1053	218.85.133.23:89	796
0x032c01f8	192.168.157.10:1053	218.85.133.23:89	796
0x0337dce0	192.168.157.10:1050	222.128.1.2:443	1672
0x08a4ace0	192.168.157.10:1050	222.128.1.2:443	1672
0x18200ce0	192.168.157.10:1050	222.128.1.2:443	1672

- PID 796 (iexplore.exe) is connecting to a remote system on port 89
- Usually http traffic is directed on port 80 or 443 only

IP Address	218.85.133.23
Location	 China, Fujian, Fuzhou
Latitude & Longitude of City	26.061390, 119.306110 (26°3'41"N 119°18'22"E)
ISP	ChinaNet Fujian Province Network
Local Time	20 Sep, 2017 01:25 PM (UTC +08:00)
Domain	chinatelecom.com.cn
Net Speed	(DSL) Broadband/Cable/Fiber
IDD & Area Code	(86) 0591
ZIP Code	350004
Weather Station	Fuzhou (CHXX0031)
Mobile Country Code (MCC)	460
Mobile Network Code (MNC)	03
Carrier Name	China Telecom
Elevation	12m
Usage Type	(ISP) Fixed Line ISP, (MOB) Mobile ISP

0x76390000	0x1d000	C:\WINDOWS\system32\IMM32.DLL
0x773d0000	0x103000	C:\WINDOWS\WinSxS\x86_Microsoft.Win32_x-ww_35d4ce83\comctl32.dll
0x5d090000	0x9a000	C:\WINDOWS\system32\comctl32.dll
0x10000000	0x9000	C:\WINDOWS\system32\irykmmww.dll
0x78050000	0xd0000	C:\WINDOWS\system32\WININET.dll
0x00710000	0x9000	C:\WINDOWS\system32\Normaliz.dll
0x71ab0000	0x17000	C:\WINDOWS\system32\WS2_32.dll
0x71aa0000	0x8000	C:\WINDOWS\system32\WS2HELP.dll
0x00150000	0xc000	C:\WINDOWS\system32\irykmmww.dll
0x5ad70000	0x38000	C:\WINDOWS\system32\uxtheme.dll
0x76fd0000	0x7f000	C:\WINDOWS\system32\CLBCATQ.DLL
0x77050000	0xc5000	C:\WINDOWS\system32\COMRes.dll
0x00e80000	0x2c5000	C:\WINDOWS\system32\xpsp2res.dll
0x76ee0000	0x3c000	C:\WINDOWS\system32\RASAPI32.dll
0x76e90000	0x12000	C:\WINDOWS\system32\rasman.dll
0x5b860000	0x55000	C:\WINDOWS\system32\NETAPI32.dll
0x76eb0000	0x2f000	C:\WINDOWS\system32\TAPI32.dll
0x76e80000	0xe000	C:\WINDOWS\system32\rtutils.dll
0x76b40000	0x2d000	C:\WINDOWS\system32\WINMM.dll
0x769c0000	0xb4000	C:\WINDOWS\system32\USERENV.dll
0x722b0000	0x5000	C:\WINDOWS\system32\sensapi.dll
0x71a50000	0x3f000	C:\WINDOWS\System32\mswsock.dll
0x76fc0000	0x6000	C:\WINDOWS\system32\rasadhlp.dll
0x662b0000	0x58000	C:\WINDOWS\system32\hnetcfg.dll
0x71a90000	0x8000	C:\WINDOWS\System32\wshtcpip.dll
0x77c70000	0x24000	C:\WINDOWS\system32\msv1_0.dll
0x76d60000	0x19000	C:\WINDOWS\system32\iphlpapi.dll

```
# vol.py -f APT.img -profile=WinXPSP3x86 dlllist --p 796
```

- The dlllist output for PID 796 (iexplore.exe) you will notice that there is a rogue named dll which is hard to see
- Irykmmww.d1l is named odd because the dll is spelled with a 1 (one) in the second letter where an l (lower case L) should be seen
- So it looks as though PID 796 is malware, but it is clear that it isn't started normally

```
# vol.py --f APT.img -profile=WinXPSP3x86 svcscan

Offset: 0x38ab98
Order: 252
Process ID: -
Service Name: irykmmww
Display Name: irykmmww
Service Type: SERVICE_KERNEL_DRIVER
Service State: SERVICE_RUNNING
Binary Path: \Driver\irykmmww
```

- When we run the svcscan (Service Scan) plugin for volatility, we notice a driver running on the system called irykmmww which is the same named rogue dll spotted earlier
- To figure out what this driver is doing, we should check driver hooking in apihooks and ssdt

```
# vol.py --f APT.img -profile=WinXPSP3x86 ssdt | grep -v ntoskrnl | grep -v win32k
```

```
[x86] Gathering all referenced SSDTs from KTHREADS...
Finding appropriate address space for tables...
SSDT[0] at 80501b9c with 284 entries
    Entry 0x0042: 0xf836fe9c (NtDeviceIoControlFile) owned by irykmmww.sys
    Entry 0x0047: 0xf83706dc (NtEnumerateKey) owned by irykmmww.sys
    Entry 0x0049: 0xf837075e (NtEnumerateValueKey) owned by irykmmww.sys
    Entry 0x0077: 0xf837028f (NtOpenKey) owned by irykmmww.sys
    Entry 0x0091: 0xf8370a8c (NtQueryDirectoryFile) owned by irykmmww.sys
    Entry 0x00ad: 0xf836fe3e (NtQuerySystemInformation) owned by irykmmww.sys
    Entry 0x00b1: 0xf837091a (NtQueryValueKey) owned by irykmmww.sys
SSDT[1] at bf999d00 with 667 entries
```

- System Service Descriptor Table (**SSDT**) is an internal dispatch table within Microsoft Windows.
- Hooking SSDT calls is often used as a technique in both Windows rootkits and antivirus software.
- Finally we can tell the driver `irykmmww.sys` is a rootkit loaded in the system

# Memhunter

- Memhunter is an Automated Memory Resident Malware Detection tool.

- Download [link](#)

- Learn [more](#)

The screenshot shows the Memhunter command-line interface running in an Administrator Command Prompt window. The interface displays various command-line options and usage examples. To the right of the command prompt, several windows are open, including a Task Manager showing process details for 'notepad.exe', a 'notepad.exe (1140) Properties' dialog, and a 'Minetest Test Utility' window with a 'Code Injected!' message. The Task Manager lists processes like 'notepad.exe', 'conhost.exe', and 'minetest.exe'. The properties dialog shows memory usage and CPU statistics for 'notepad.exe'. The utility window indicates a successful code injection into 'minetest.exe'.

```
Administrator: Command Prompt
Live Memory Forensics Hunter
Memhunter Version: v0.7

Available Hunters IDs:
1 - Suspicious Threads - It looks for RWX pages on threads base address
2 - Suspicious Callstack - It perform thread callstack analysis to check on suspicious patterns
3 - Suspicious Exports - It looks for know bad exports
4 - Suspicious Hollowed Modules - It performs PE Header comparison of on-memory modules vs on-disk counterpart
5 - Suspicious Modules - It looks for RWX memory regions on modules memory areas
6 - Suspicious Parents - It looks for suspicious parents
7 - Suspicious Regions - It looks for wiped PE headers on section related memory areas
8 - Suspicious Registry - It looks for well-know persistence, evasion techniques on the registry
9 - Suspicious Shellcode - It performs fuzzy matching on committed memory to look for function prologues

Available Options:
-c <config_file>           Path to configuration file
-m <id_list>                List of Hunters to use. All included by Default
-d                          Enable Dissolvable mode. Disabled by Default
-f                          Enable False Positive Mitigations. Enabled by Default
-r <verbose|regular|minimal> Report Verbosity Options. Regular by Default
-e <exclusion_list>         List of Processes To Exclude
-o <console|eventlog>        Report Output Options. Console by Default
-y <path>                   Path to YARA Rules to use
-v <path>                   Path to VirusTotal license to use
-h                          Display help information

Usage Example:
-h for help                  Help
-c <config_file>            Configuration File
-f -o eventlog -m 1,2,3      Normal Usage

C:\tools\memhunter>
```

# Course Work

- Briefly describe Hooking SSDT calls

Refer following URLs:

<https://resources.infosecinstitute.com/hooking-system-service-dispatch-table-ssdt/>

<https://www.adlice.com/kernelmode-rootkits-part-1-ssdt-hooks/>

<https://archive.org/details/RootkitsDay1Part6>

# Study Materials

- **Volatility Foundation**

URL: <http://www.volatilityfoundation.org/>

- **Forensic Focus**

URL: <http://www.forensicfocus.com/>

- **eForensics Magazine**

URL: <https://eforensicsmag.com/>



# Introduction to Email Forensics

By  
Chirath De Alwis

# Motivation for Email Investigations

- Email Has become a primary means of communication
- Email can easily be forged
- Email can be abused
  - Spam
  - Aid in committing a crime
  - Threatening email,...



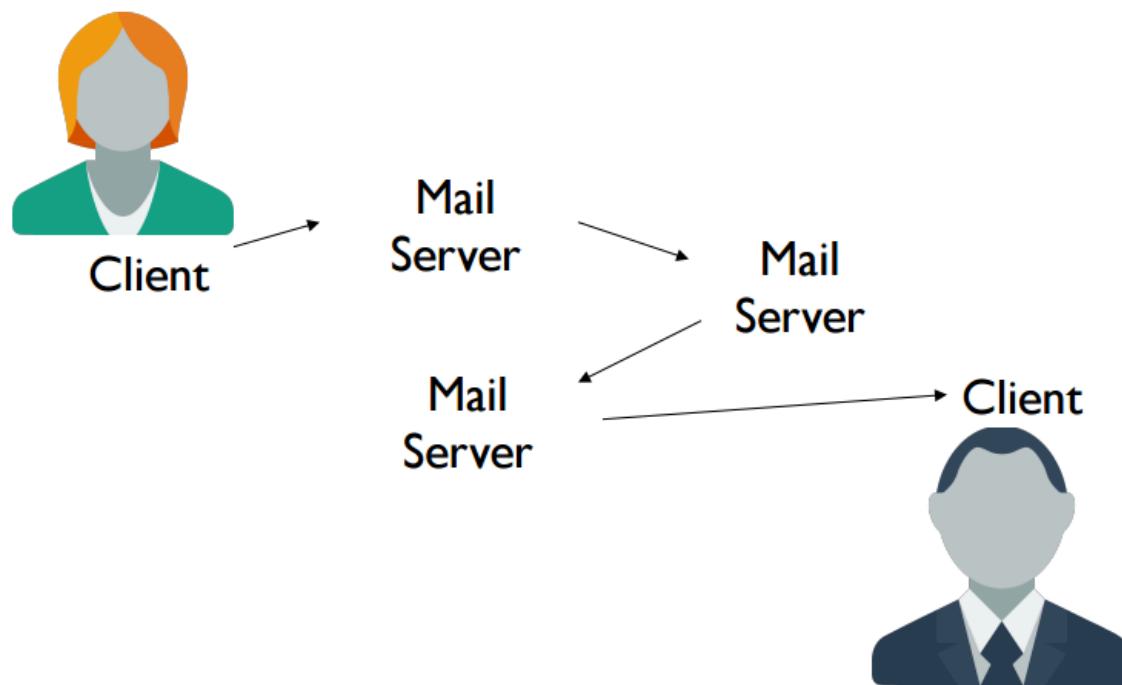
# Importance of email as evidence

- E-mail can be pivotal evidence in a case
- Due to its informal nature, it does not always represent corporate policy
- Many cases provide examples of the use of e-mail as evidence



# Email Fundamentals

- Typical path of an email message



# Email Investigations Overview

- Email evidence is in the **email** itself (header)
- Email evidence is left behind as the email travels from sender to recipient
  - Contained in the various logs
  - Maintained by system admins
- Law enforcement can use subpoenas to collect emails headers and logs

# Client Protocols

<b>Post Office Service</b>	<b>Protocol</b>	<b>Characteristics</b>
Stores only incoming messages	POP	Investigation must be at the workstation.
Stores all messages	IMAP MS' MAPI Lotus Notes	Copies of incoming and outgoing messages might be stored on the workstation or on the server or on both.
Web-based send and receive	HTTP	Incoming and outgoing messages are stored on the server, but there might be archived or copied messages on the workstation

# SMTP Headers

- Reviewing e-mail headers can offer clues to true origins of the mail and the program used to send it
- Common e-mail header fields include:
  - Bcc
  - Cc
  - Content-Type
  - Date
  - from
  - Message-ID
  - Received
  - Subject
  - To
  - X-Priority

# SMTP Headers Example

Delivered-To: MrSmith@gmail.com  
Received: by 10.36.81.3 with SMTP id e3cs239nzb; Tue, 29 Mar 2005 15:11:47 -0800 (PST)  
Return-Path: MrJones@emailprovider.com  
Received: from mail.emailprovider.com (mail.emailprovider.com [111.111.11.111]) by mx.gmail.com with SMTP id h19si826631rnb; Tue, 29 Mar 2005 15:11:47 -0800 (PST)  
Message-ID: <20050329231145.62086.mail@mail.emailprovider.com>  
Received: from [11.11.111.111] by mail.emailprovider.com via HTTP; Tue, 29 Mar 2005 15:11:45 PST  
Date: Tue, 29 Mar 2005 15:11:45 -0800 (PST)  
From: Mr Jones  
Subject: Hello  
To: Mr Smith

# Hint for Investigating of Fake Emails

- Verify all IP addresses
  - Keeping in mind that some addresses might be internal addresses
- Make a time-line of events
  - Change times to universal standard time
  - Look for strange behavior
  - Keep clock drift in mind
- Check server logs



# Working with Resident Email Files

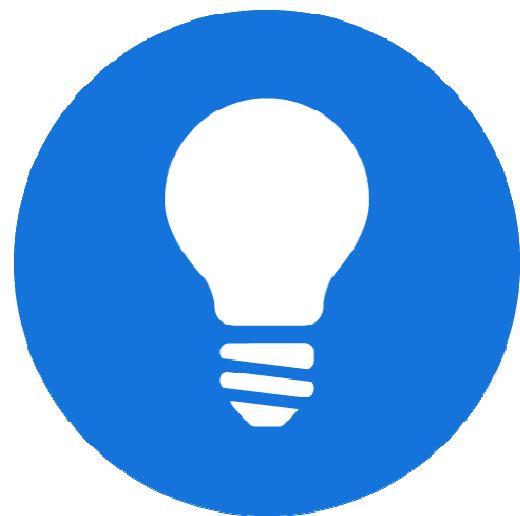
- Some users store email is stored locally
  - Great benefit for forensic analysts because the email is readily available when the computer is seized
- Begin by identifying e-mail clients on system
- You can also search by file extensions of common e-mail clients



# Email Forensics Tools

- FINALeMail
- Sawmail-Group Wise
- DBXtract
- MailBag
- Paraben
- mxtoolbox.com





# Practical

# Exercise 01

- Read the “original\_msg.txt” email header and try to identify what attacker tried to do?

# Exercise 02

- Analyze the “#38589803.eml” email and extract possible evidence from that.

# Exercise 03

- “How to report abuse spam.txt” contains a part of the email header received by an employee. This spam email contained some links for abuse content. Analyze the header and identify the contact point to report this abuse.

# Need More?

- <https://ctf.metaspike.com/>

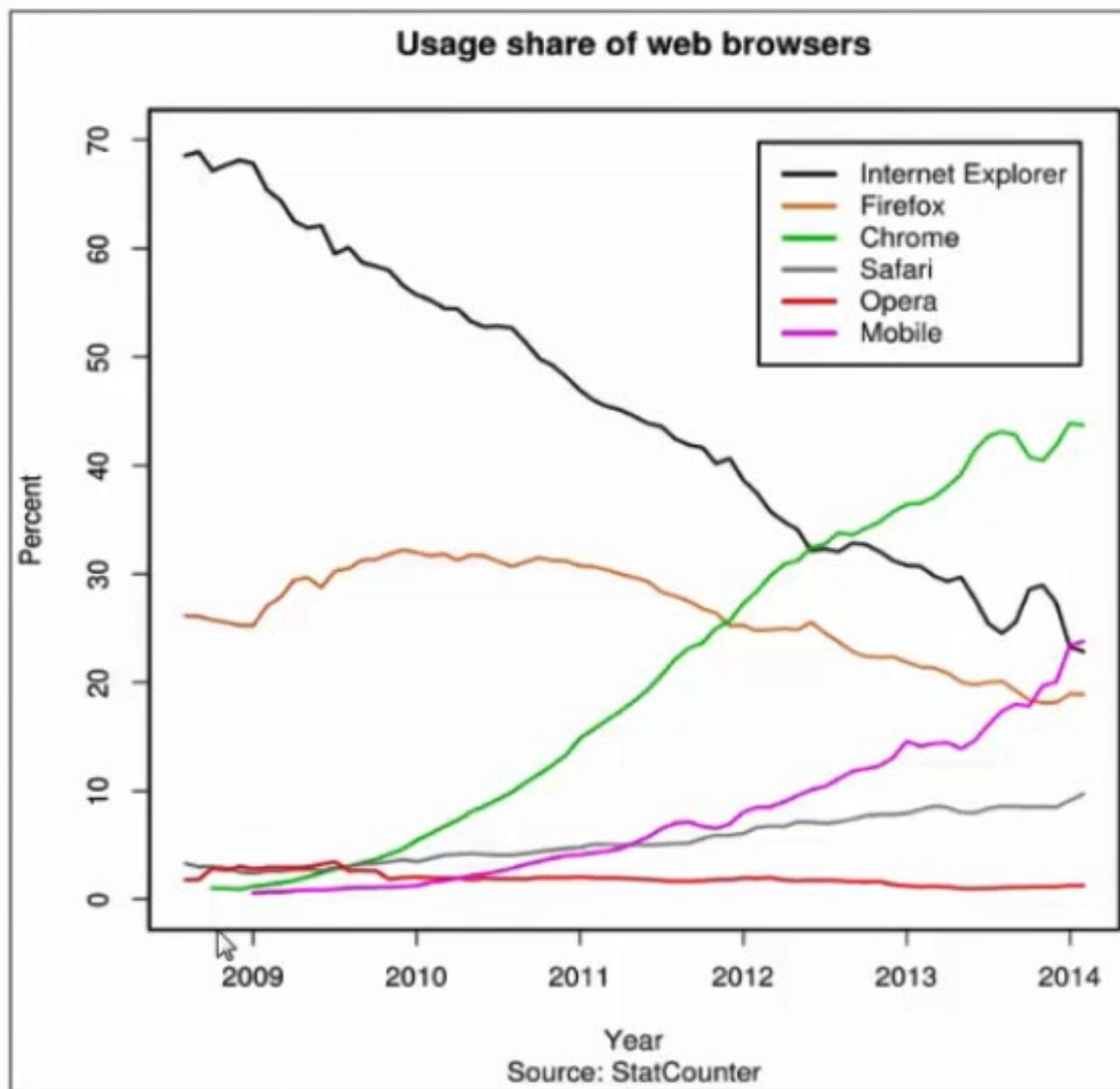
# Internet Activity Analysis

# Internet Activity Analysis

- User Internet activity can be recreated by examining the system's Internet history.
- Information may include:
  - Search Engine search terms
  - Files downloaded
  - Research
  - Webmail
  - Social Networking activity / Friend List
  - And much more...

# Internet Browsers

- Internet Explorer
  - Microsoft developed, supplied by default with all Windows systems.
- Mozilla Firefox
  - Open Source project that began as Netscape. Versatile, with many add-on tools.
- Google Chrome
  - Fast, lightweight and secure. Now the most popular browser.
- Apple Safari
  - Browser supplied with all Apple systems.



# SQLite Databases

- Mozilla Firefox and Google Chrome use SQLite database file to house their Internet browsing history.
- These files can be analyzed using a tool like SQLite Database Browser.
  - Firefox – Places.sqlite
  - Chrome – History.sqlite

The screenshot shows the SQLite Database Browser interface. On the left is a tree view of database tables:

- 1 Archived History
- 2 Bookmarks
- 3 Bookmarks.bak
- 4 Cache
- 5 Cookies
- 6 Current Session
- 7 Current Tabs
- 8 Favicons
- 9 History
- 10 History Index 2011-03
- 11 Last Session
- 12 Last Tabs
- 13 Local Storage
- 14 Login Data
- 15 Plugin Data
- 16 Preferences
- 17 Top Sites
- 18 User StyleSheets
- 19 Visited Links
- 20 Web-Data

The main window displays the 'urls' table with the following data:

ID	url	title	visit count	tweet count	last visit
1	http://www.msn.com/	MSN.com	0	0	2944
2	http://www.mozilla.org/	Home of the Mozilla	0	0	2944
3	http://www.microsoft.com/windows/intel	Internet Explorer 8:	0	0	2944
4	http://www.cnn.com/	CNN.com - Breaking	2	0	2944
5	http://windowsupdate.microsoft.com/		0	0	2944
6	http://www.google.com/chrome/chrome		0	0	2944
7	http://www.google.com/chrome/eula.html	Google Chrome for Windows	0	0	2944
8	https://id-esd.google.com/tag/i/appguid		0	0	2944
9	http://www.update.microsoft.com/favic		0	0	2944
10	http://www.mozilla.com/en-US/firefox	Mozilla   Firefox web browser	0	0	2944
11	http://www.update.microsoft.com/lived	Microsoft Windows Update	0	0	2944
12	http://www.bing.com/search?q=firefox RSS		0	0	2944
13	http://www.mozilla.com/		0	0	2944
14	http://www.mozilla.com/products/download		0	0	2944
15	http://www.mozillaMessaging.com/thun		0	0	2944
16	http://fp-stud.hs-esslingen.de/pub/Mi		0	0	2944
17	http://www.google.com/chrome/thankyou	Google Chrome for Windows	0	0	2944

Google Chrome  
Browsing History

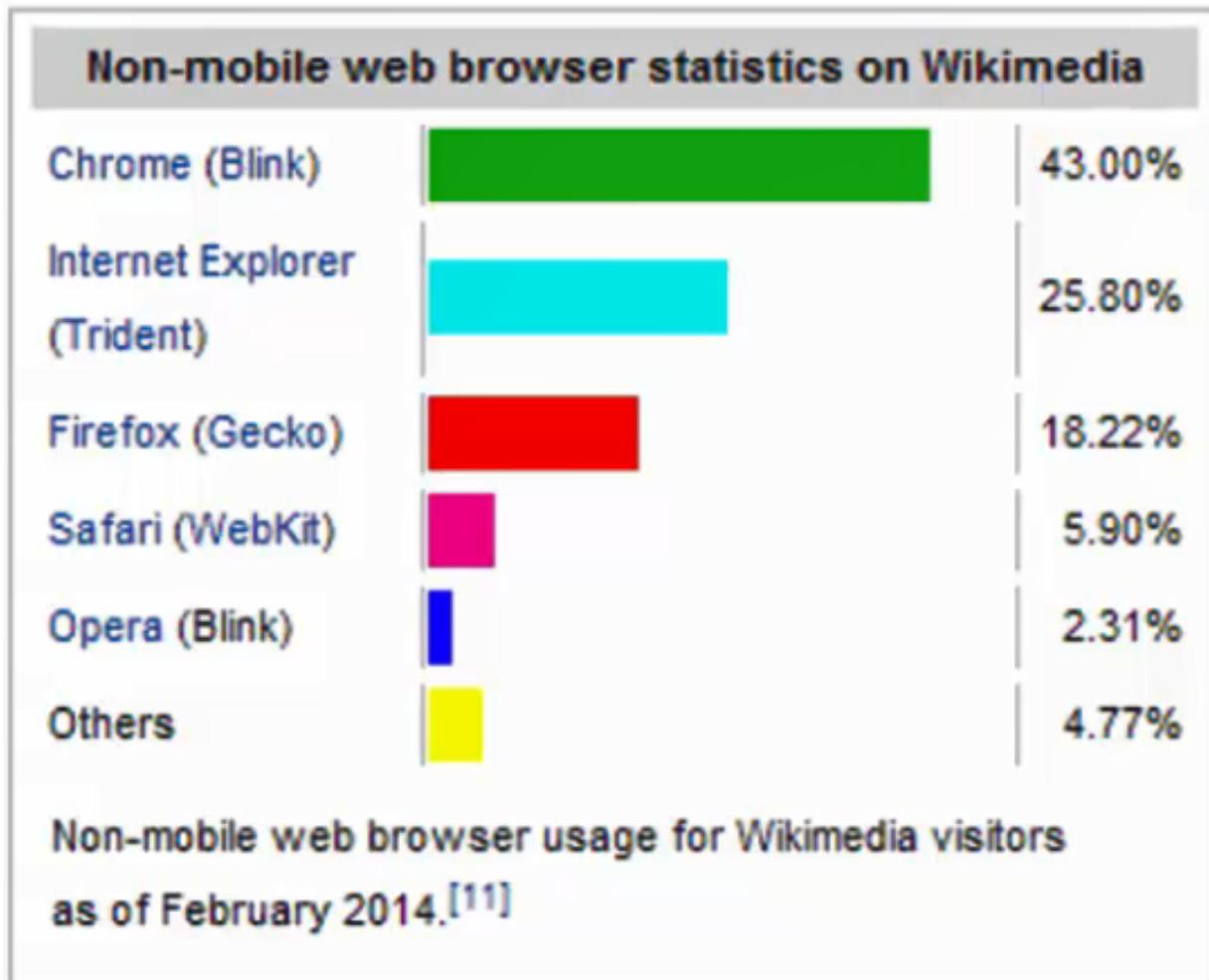
# Google Chrome Internet Browser

- Google Chrome Stores History of websites visited in a SQLite database in the following locations
  - **Windows 2000 and XP:** C:\Documents and Settings\%USERNAME%\Local Settings\Application Data\Google\Chrome\User Data\Default\Preferences
  - **Windows Vista / 7:** C:\Users\%USERNAME%\AppData\Local\Google\Chrome\User Data\Default\Preferences
- Chrome Timestamps
  - Chrome Downloads History uses standard Unix epoch time – The number of seconds since January 1, 1970 UTC.
  - Chrome Web History uses a different style of epoch time that counts the number of *microseconds* since January 1, 1601 UTC.
  - Online converters and forensic tools can help you to decipher these times.



# Internet Explorer

- Formerly the most popular browser, usage dropping recently.
  - IE6 – Older version, seen in Windows 2000 and XP
  - IE7 – Standard on Vista and new XP systems
  - IE8 – Released in 2009; standard on Windows 7
  - IE9 – Released in 2011
  - IE10 – Released in 2012
  - IE11 – Released 2013; Standard on Windows 8



# Internet Explorer – Important Locations XP

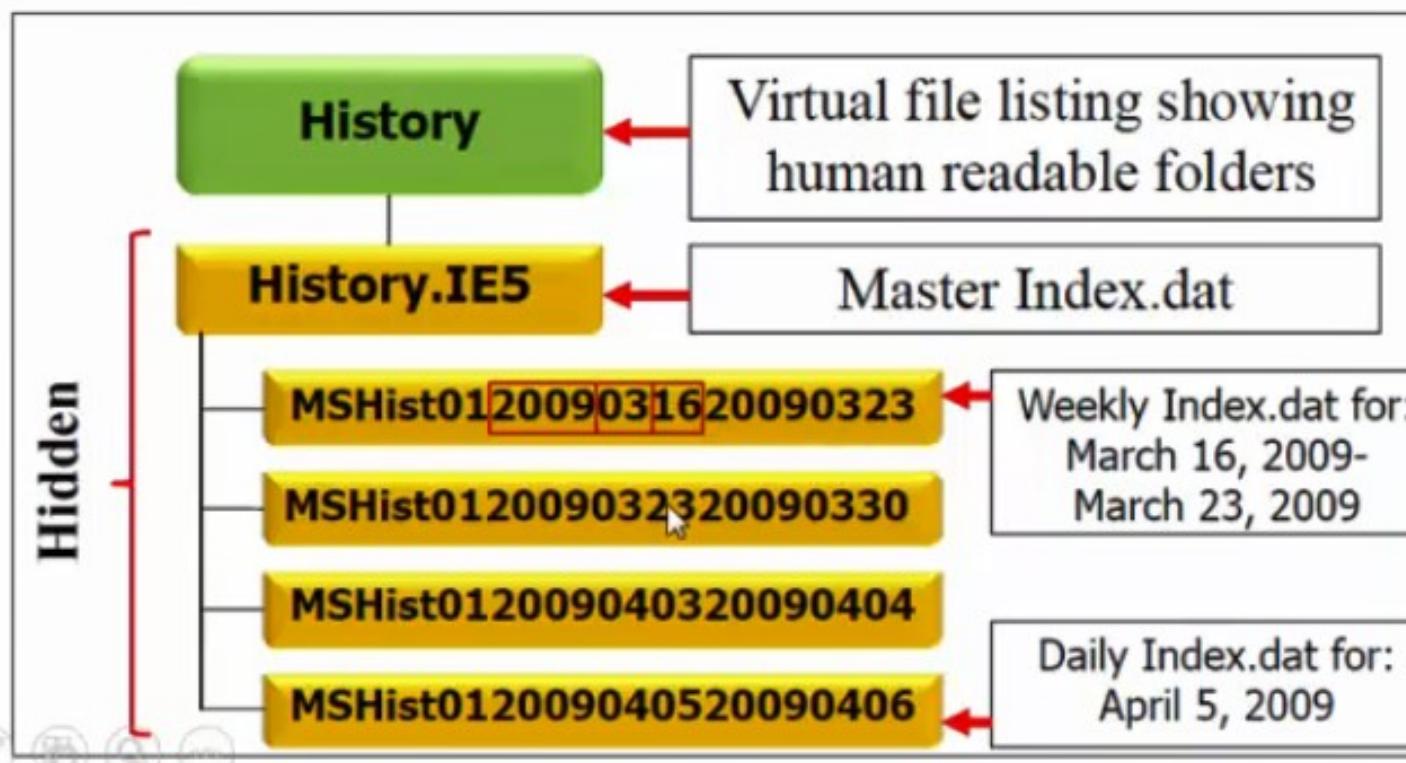
- History Files
  - C:\Documents and Settings\<UserProfile>\Local Settings\History\History.IE5
- Cache
  - C:\Documents and Settings\<UserProfile>\Local Settings\Temporary Internet Files\Content.IE5
- Cookies
  - C:\Documents and Settings\<UserProfile>\Cookies
- Favorites
  - C:\Documents and Settings\<UserProfile>\Favorites

# Internet Explorer – Index.dat

- Index.dat files are found in Cookies, History and Cache (Temporary Internet Files)
- Contains a binary database that logs Internet activity
- File format has not changed since IE4
- Located in hidden, system directories

# Internet Explorer - History

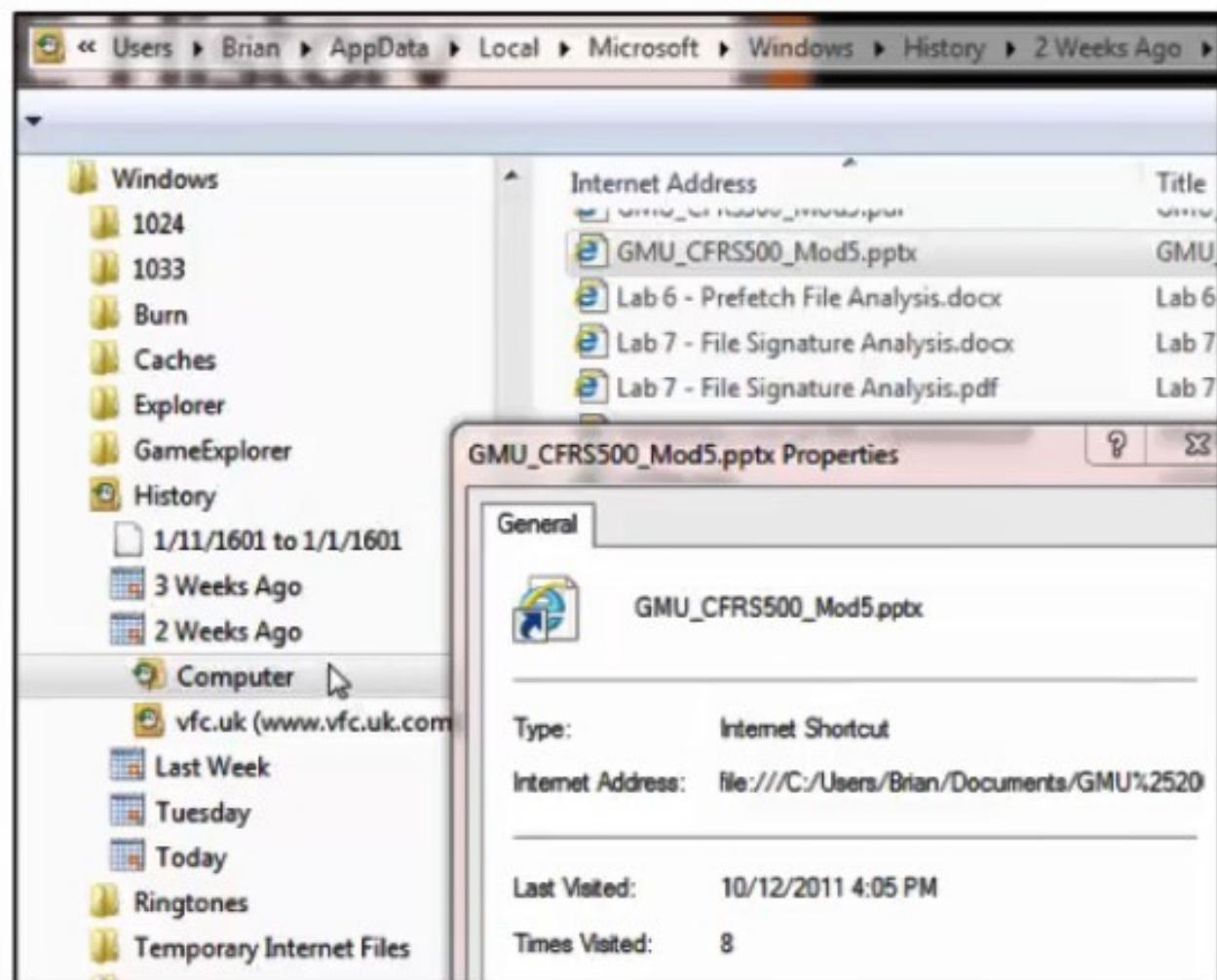
- History is stored in a chronological format. (Weekly and Daily) directories.
- Master Index.dat contains information for all subdirectories.
- Each subdirectory contains an index.dat for that specific time period.



\*Lee / Tilbury ; Internet  
Browser Forensics

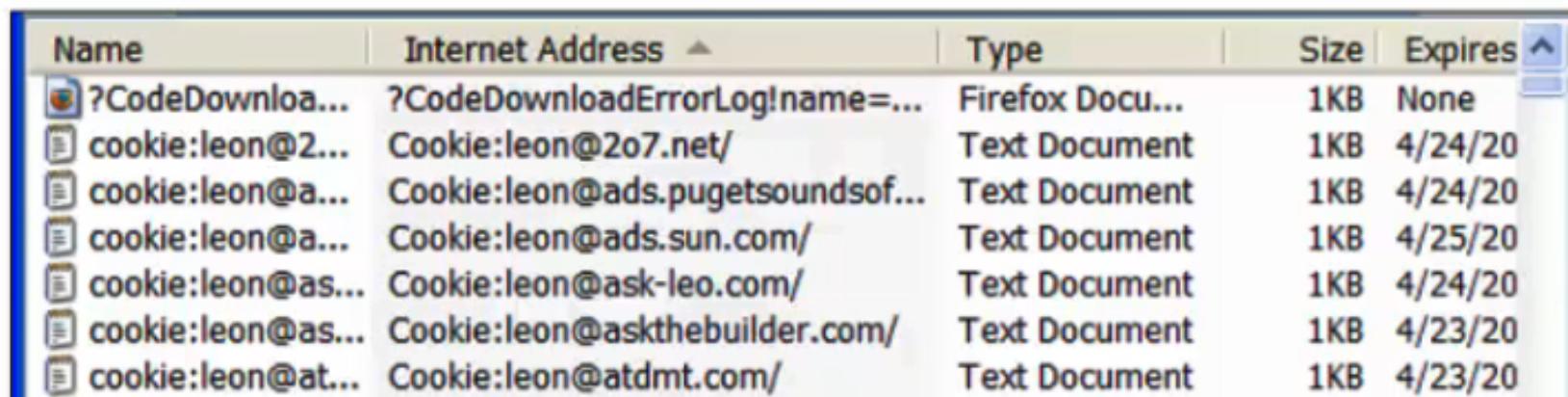
# IE History – Local File Access

- IE History also records local file access in the index.dat file.
- Even though this is IE History, it is not necessarily related to the Internet.



# Internet Explorer - Cookies

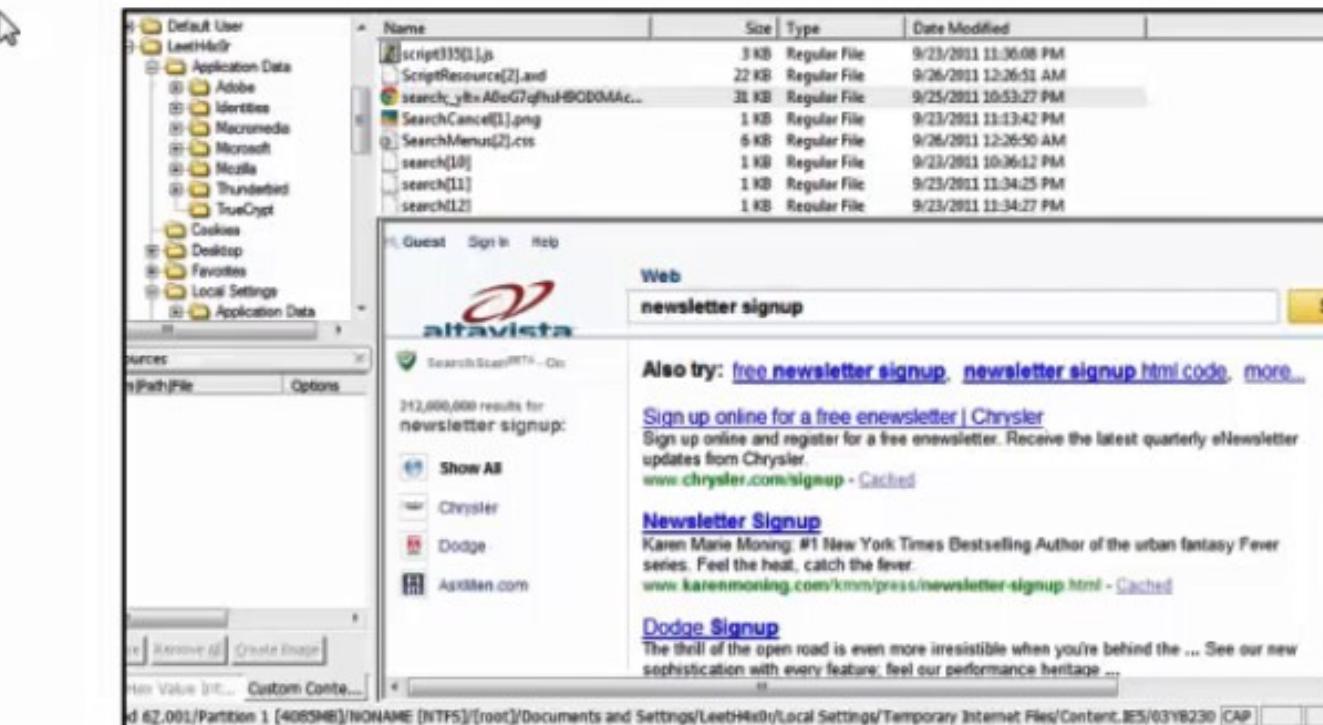
- Cookies are short text files that web servers save on visiting computers.
- Cookie Information:
  - Naming convention: **user@domain**
  - Host (Domain)
  - Modified Date
  - Expiration Date
- Managed by a single index.dat file
- For forensics, they prove that a user visited a specific site and provide a time / date.



Name	Internet Address	Type	Size	Expires
?CodeDownloadErrorLog!name=...	?CodeDownloadErrorLog!name=...	Firefox Document	1KB	None
cookie:leon@2o7.net/	Cookie:leon@2o7.net/	Text Document	1KB	4/24/20
cookie:leon@ads.pugetsoundof...	Cookie:leon@ads.pugetsoundof...	Text Document	1KB	4/24/20
cookie:leon@ads.sun.com/	Cookie:leon@ads.sun.com/	Text Document	1KB	4/25/20
cookie:leon@ask-leo.com/	Cookie:leon@ask-leo.com/	Text Document	1KB	4/24/20
cookie:leon@askthebuilder.com/	Cookie:leon@askthebuilder.com/	Text Document	1KB	4/23/20
cookie:leon@atdmt.com/	Cookie:leon@atdmt.com/	Text Document	1KB	4/23/20

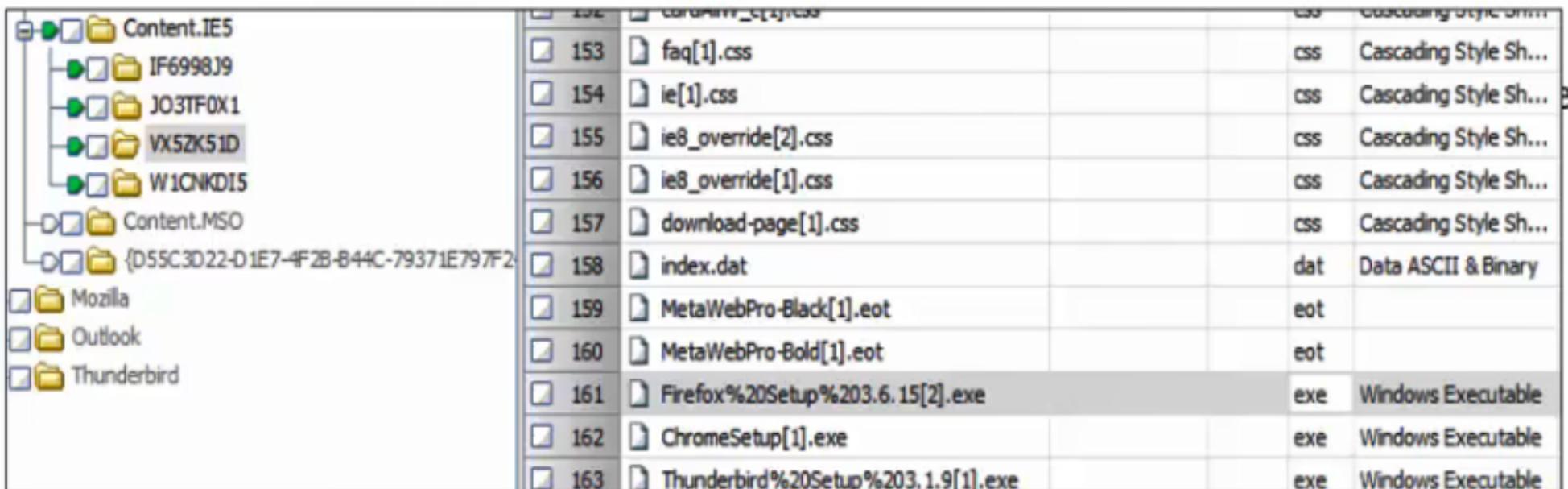
# Internet Explorer - Cache

- The Cache can contain countless types of information about browsing history
  - Complete html pages containing completed or partially completed forms
  - Search terms, e-mail addresses, webmail
  - All the files necessary to completely rebuild websites
  - Downloaded malware and exploits



# Internet Explorer Cache

- Temporary Internet Files are files downloaded from web servers.
  - When a user visits a website, the browser checks for the files in the cache. If present, the browser load them locally and not need to download.
  - This speeds Internet browser performance.
- The Cache is composed of:
  - Four randomly named subdirectories under Temporary Internet Files\Content.IE5.



The screenshot shows the Windows File Explorer interface. On the left, a tree view displays the following directory structure:

- Content.IE5
  - IF6998J9
  - J03TF0X1
  - VX52K51D
  - W1CNK0I5
- Content.MSO
- {D55C3D22-D1E7-4F2B-B44C-79371E797F2}
- Mozilla
- Outlook
- Thunderbird

On the right, a detailed list of files is shown in a table format:

File	Description	Type	Size
faq[1].css	Cascading Style Sheet	css	1.2 KB
ie[1].css	Cascading Style Sheet	css	1.2 KB
ie8_override[2].css	Cascading Style Sheet	css	1.2 KB
ie8_override[1].css	Cascading Style Sheet	css	1.2 KB
download-page[1].css	Cascading Style Sheet	css	1.2 KB
index.dat	Data ASCII & Binary	dat	1.2 KB
MetaWebPro-Black[1].eot		eot	1.2 KB
MetaWebPro-Bold[1].eot		eot	1.2 KB
Firefox%20Setup%203.6.15[2].exe	Windows Executable	exe	1.2 KB
ChromeSetup[1].exe	Windows Executable	exe	1.2 KB
Thunderbird%20Setup%203.1.9[1].exe	Windows Executable	exe	1.2 KB

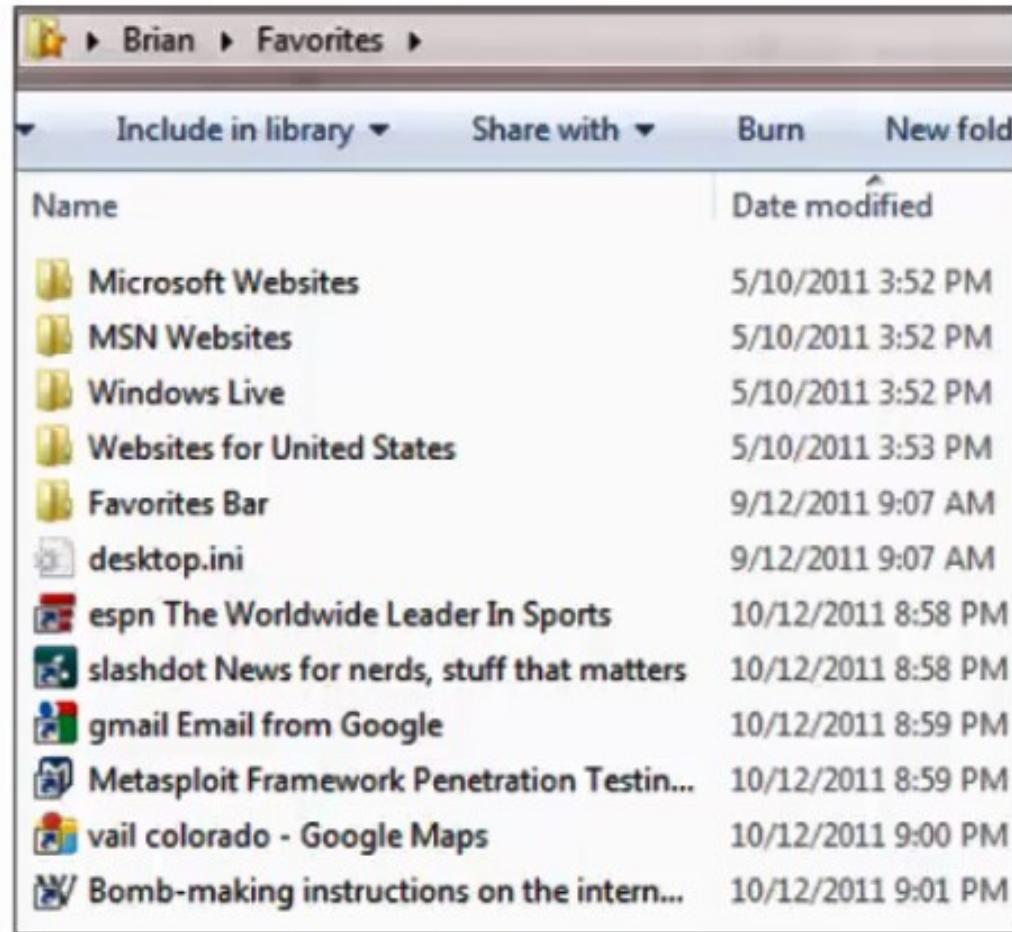
# Internet Explorer - Downloads

- When files are downloaded from the internet they are saved to a central folder by default
  - C:\users\downloads
- This is a primary location to identify files purposefully downloaded by the suspect

Name	Date
AccessData_FTK_Im...	8/28/2011 1:17 PM
avg_free_stb_all_201...	6/11/2011 10:30 AM
avg_free_stb_all_201...	6/11/2011 10:29 AM
cnet_DiskUtil_zip.exe	9/4/2011 5:38 PM
cnet_HxDSetupEN_z...	9/4/2011 6:24 PM
emx-demo.exe	10/9/2011 8:59 PM
iTunes64Setup.exe	8/18/2011 6:53 PM
KillDiskSuiteFree-Se...	9/4/2011 5:10 PM
Microsoft_Windows...	9/10/2011 1:29 PM
MIP-Setup.exe	9/4/2011 8:08 PM
picasa38-setup.exe	9/18/2011 4:17 PM
setup.exe	10/11/2011 8:06 AM
snagit.exe	6/12/2011 1:42 PM
TrueCrypt Setup 7.1...	9/25/2011 10:16 PM
usbkey.exe	10/11/2011 8:05 AM

# Internet Explorer - Favorites

- Favorites (bookmarks) are Internet shortcuts that a user can easily visit a website with a single click.
- A favorite can give an indication of the type of websites suspects frequent.
- Be aware that malicious code can write favorites to a user's profile



A screenshot of a Windows File Explorer window titled "Brian > Favorites". The window shows a list of items with columns for Name and Date modified. The items include "Microsoft Websites", "MSN Websites", "Windows Live", "Websites for United States", "Favorites Bar", "desktop.ini", "espn The Worldwide Leader In Sports", "slashdot News for nerds, stuff that matters", "gmail Email from Google", "Metasploit Framework Penetration Testin...", "vail colorado - Google Maps", and "Bomb-making instructions on the intern...". Most items were modified on 10/12/2011, except for "desktop.ini" and the last item which were modified on 10/10/2011.

Name	Date modified
Microsoft Websites	5/10/2011 3:52 PM
MSN Websites	5/10/2011 3:52 PM
Windows Live	5/10/2011 3:52 PM
Websites for United States	5/10/2011 3:53 PM
Favorites Bar	9/12/2011 9:07 AM
desktop.ini	9/12/2011 9:07 AM
espn The Worldwide Leader In Sports	10/12/2011 8:58 PM
slashdot News for nerds, stuff that matters	10/12/2011 8:58 PM
gmail Email from Google	10/12/2011 8:59 PM
Metasploit Framework Penetration Testin...	10/12/2011 8:59 PM
vail colorado - Google Maps	10/12/2011 9:00 PM
Bomb-making instructions on the intern...	10/12/2011 9:01 PM



# Timeline Analysis

# Timeline Analysis

Timeline analysis is useful for a variety of investigation types and is often used to answer questions about when a computer is used or what events occurred before or after a given event.

# Windows Dates & Times

- Timeline analysis
  - A primary job of the forensic analyst is to be able to recreate the series of events that led up to a crime.
  - This is applicable in all subfields of Computer Forensics:
    - Intrusions – Examples of events to supply date and time for:
      1. Original attack vector
      2. Creation of malware
      3. Execution of malware
      4. Creation of data exfiltration file
      5. Exfiltration of stolen information
      6. Deletion of malware and attack artifacts
      7. Forensic Acquisition

# Sample Intrusion Timeline

Time & Date	Event	Explanation
9/8/2011 07:45:02AM	E-mail arrives from Admin@UPS1154billing.com containing a malicious attachment called: invoice.xls.exe	The e-mail containing Invoice.xls.exe was a phishing e-mail designed to trick the victim into opening the file by saying it is an actual bill.
9/8/2011 08:37:18AM	Prefetch file for invoice.xls.exe is created.	This indicates that invoice.xls.exe was executed at this time.
9/8/2011 08:37:19AM	Filezilla.exe and keylogger.txt is created in C:\Windows\System32	Filezilla.exe is a FTP server and keylogger.txt is a file the malware uses to store all keystrokes on the victim system.
9/8/2011 08:37:29AM	Prefetch File for Filezilla.exe is created.	This indicates that Filezilla was executed and an FTP server was then operational on the victim system.
9/28/2011 11:17:45PM	FTP log shows that an FTP connection that transmitted keylogger.txt to the IP address 77.47.48.65.	77.47.48.65 is confirmed to have received the keylogger file. This IP address is associated with the National Technical University of the Ukraine.
9/28/2011 11:19:21PM	Keylogger.txt is deleted.	Directly after successful exfiltration, keylogger.txt is deleted. It contained usernames, passwords, credit card number and bank account information for the victim.

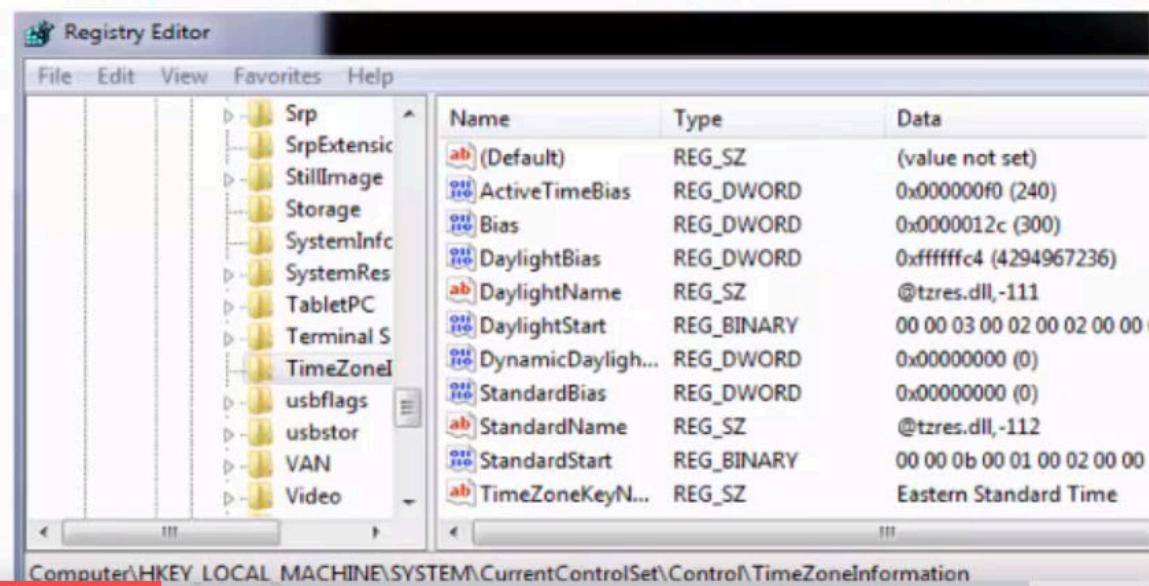
## Other Examples of Relevant Times and Dates

- Kidnapping case – times and dates of:
  - DHCP assignment of local IP addresses . (Location can be tracked via IP addresses)
- Intellectual Property Case
  - The creation of Link files for IP on a thumb drive. (Authorized if prior to leaving unemployment, criminal if after)
- Murder Case
  - The suspect conducted Google Searches for poison and an online order for strychnine one week prior to the victim being poisoned via strychnine.



# Time Zones

- It is important to know the time zone that the system was configured to display. This will help the examiner to determine the actual time events occurred.
- The time zone settings are stored in the registry at:  
**HKLM\System\CurrentControlSet\Control\TimeZoneInformation**



## Daylight Savings Time

- It is also important to note the date that the crime occurred and the status of daylight savings time.
- If you are doing analysis during standard time and the victim system is set to daylight savings time, then your forensic tool may not parse times correctly.
- Rule of thumb: if times in your case are exactly an hour different than the expected time, then research a potential DST issue.

## File System Differences

- FAT file system stores times in the local system time zone.
- NTFS stores times in GMT (UTC) and translates presentation of the times in Windows Explorer based on the system's time zone settings.

# Timestamps

## Where do you find timestamps?

- File & folder timestamps as maintained in the MFT
- Internal file metadata
- Log files
  - Windows Event Logs
  - Anti-virus logs
  - SetupAPI.log / Setupapi.dev.log
  - NTFS Change Journal
  - Prefetch File last run times
  - Internet History times
  - Web / Mail Server logs
  - Windows Registry Keys

# MFT File Timestamps (MAC)

In the MFT there are four types of time stamps

- File Created
  - Time the file was created
- Last Accessed
  - Time the contents of the file was last accessed
- Last Modified
  - Time the content of the file was last modified
- MFT Entry Modified
  - Time the metadata of the file was last modified

## Important notes about time stamps

- Create date does not follow files between systems. The create date is reset every time a file is copied to a new device / system.
- Accessed times are unreliable, do not frequently update, and can be all updated by an antivirus scan.
- The File System MAC times may be different from an actual file's internal timestamps. (metadata) Both should be examined.

# Timestamps

- Timestamps come in many forms
  - Anyone know what this is?
    - 1299691326

# Timestamps

- Timestamps come in many forms
  - Anyone know what this is?
    - 1299691326 

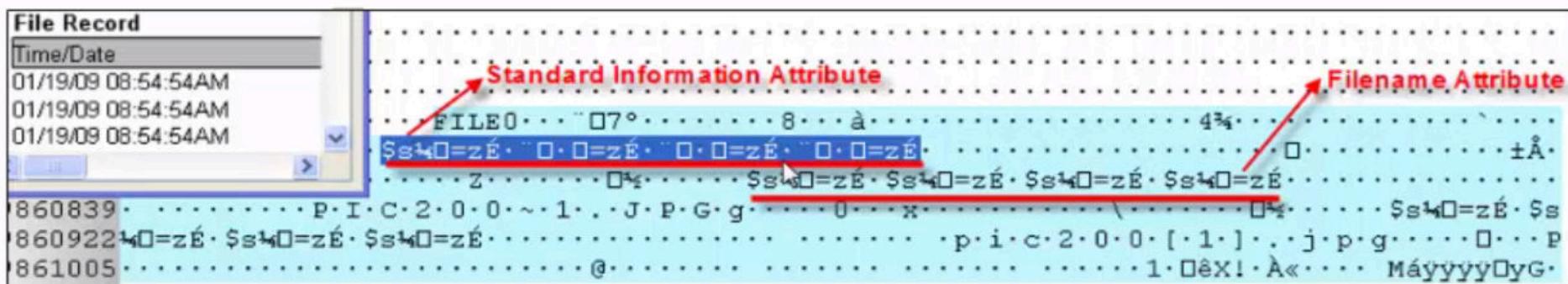
March 9<sup>th</sup>, 2011 17:22:42 UTC  
(Epoch time – the amount of seconds since midnight of 1/1/1970)

- How about this one?



January 19<sup>th</sup>, 2009 08:54:54 UTC  
(Windows 64 bit (8 byte) timestamp in ASCII)

# SIA & FNA Timestamps (Anti-forensics)



- The \$MFT stores file times in two locations
  - Standard Information Attribute (SIA)
  - File Name Attribute (FNA)
- Most programs, including forensic tools and anti-forensic tools, only use the SIA
- Usually the SIA and the FNA are identical. If they do not match – this is a RED FLAG
  - Turns an anti-forensic technique into an investigative aid

SANS Time Rules  
– Even this is  
variable,  
depending on  
OS, FS or virtual  
systems...

# Windows Time Rules

\$ STDINFO

File Rename	Local File Move	Volume File Move	File Copy	File Access	File Modify	File Creation	File Deletion
Modified – No Change	Modified – Change	Modified – No Change	Modified – No Change				
Access – No Change	Access – No Change	Access – Change	Access – Change	Access – Change No Change on Vista/Win7	Access – No Change	Access – Change	Access – No Change
Creation – No Change	Creation – No Change	Creation – No Change	Creation – Change	Creation – No Change	Creation – No Change	Creation – Change	Creation – No Change
Metadata – Changed	Metadata – Changed	Metadata – Changed	Metadata – No Change				

\$ FILENAME

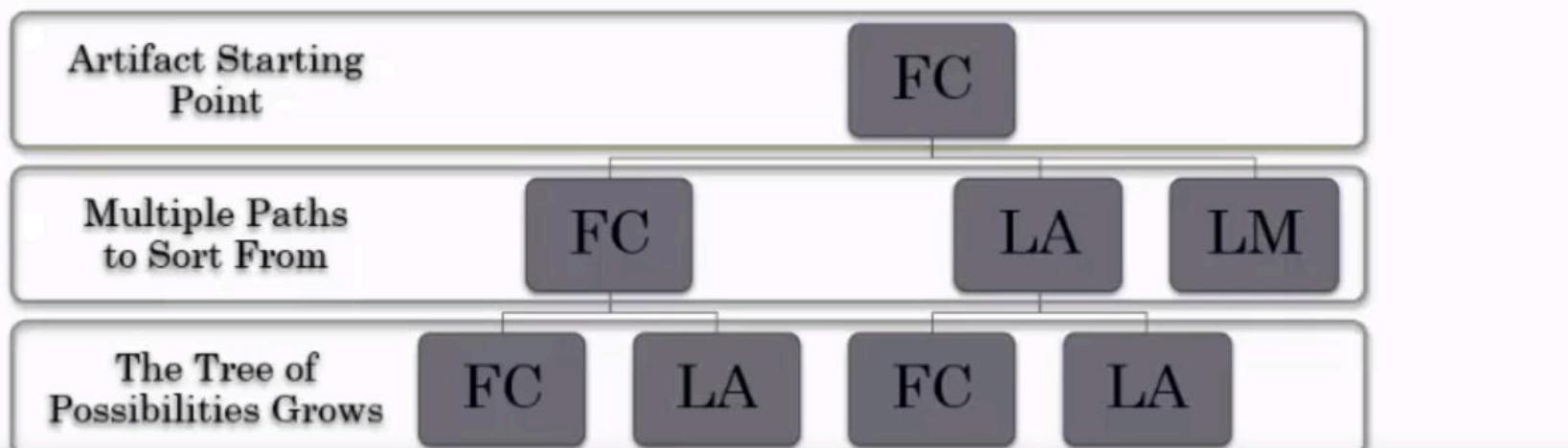
File Rename	Local File Move	Volume File Move	File Copy	File Access	File Modify	File Creation	File Deletion
Modified – No Change	Modified – Change	Modified – Change	Modified – Change	Modified – No Change	Modified – No Change	Modified – No Change	Modified – No Change
Access – No Change	Access – No Change	Access – Change	Access – Change	Access – No Change	Access – No Change	Access – Change	Access – No Change
Creation – No Change	Creation – No Change	Creation – Change	Creation – Change	Creation – No Change	Creation – No Change	Creation – Change	Creation – No Change
Metadata – No Change	Metadata – Changed	Metadata – Changed	Metadata – Changed	Metadata – No Change	Metadata – No Change	Metadata – Changed	Metadata – No Change

# MAC Time Triangulation

- Times are variable and stored in different ways on a computer
- Many convictions rely on timestamps – hopefully they were correct...
- When times are important, always try to verify times from multiple sources
  - File Create Time from MFT
  - File Create Time from metadata
  - NTUser.dat MRU time stamp
  - Link File
- Relying only on File system MAC times is a common but very dangerous practice.

# Timeline Analysis

- Timeline Analysis requires examining everything occurring on a system around the suspect time and building the chain from there.
- Timeline analysis is continual from case start to finish. Every new relevant time requires new timeline searches.



# Timeline Analysis with Autopsy

<https://www.sleuthkit.org/autopsy/timeline.php>



## **Setting up a Windows based forensics workstation (Virtual Machine) for Forensics Labs.**

**Step 1:** Install latest version of Oracle VM Virtual Box or VMware

Download Links :

Oracle VM Virtual Box

<https://www.virtualbox.org/wiki/Downloads>

VMware

<https://www.vmware.com/products/workstation-pro/workstation-pro-evaluation.html>

**Step 2:** Create a VM and Install a latest version of MS Windows operating system to the VM

**Step 3:** Setup a shared folder to transfer files between base machine and virtual machine

**Step 4:** Installing necessary tools for forensic related activities

- **FTK Imager**

FTK Imager is a data preview and imaging tool that lets you quickly assess electronic evidence to determine if further analysis with a forensic tool such as AccessData,Forensic Toolkit (FTK) is warranted.

- **OSFMount**

OSFMount allows you to mount local disk image files (bit-for-bit copies of an entire disk or disk partition) in Windows as a physical disk or a logical drive letter. By default, the image files are mounted as read only so that the original image files are not altered.

OSFMount supports mounting disk image files as read/write in "write cache" mode. This stores all writes to a "write cache" (or "delta") file which preserves the integrity of the original disk image file.



- **Autopsy**

Autopsy is computer software that makes it simpler to deploy many of the open source programs and plugins used in The Sleuth Kit. The graphical user interface displays the results from the forensic search of the underlying volume making it easier for investigators to flag pertinent sections of data.

- **Hash calculation and validation tool (HashCalc/HashMyFiles)**

### **HashCalc**

A fast and easy-to-use calculator that allows to compute message digests, checksums and HMACs for files, as well as for text and hex strings. It offers a choice of 13 of the most popular hash and checksum algorithms for calculations.

### **HashMyFiles**

HashMyFiles is a small utility that allows you to calculate the MD5 and SHA1 hashes of one or more files in your system. You can easily copy the MD5/SHA1 hashes list into the clipboard, or save them into a text/html/xml file.

- **Hex Editor (HxD)**

A hex editor (or binary file editor or byte editor) is a computer program that allows for manipulation of the fundamental binary data that constitutes a computer file. The name 'hex' comes from 'hexadecimal': a standard numerical format for representing binary data.

- **Volatility memory forensics tool and volatility workbench**

### **Volatility memory forensics**

It is used to analyze crash dumps, raw dumps, VMware & VirtualBox dumps. The extraction techniques are performed completely independent of the system being investigated and give complete visibility into the runtime state of the system. So, this article is about forensic analysis of RAM memory dump using a volatility tool.



## **Volatility workbench**

Volatility Workbench is a graphical user interface (GUI) for the Volatility tool. Volatility is a command line memory analysis and forensics tool for extracting artifacts from memory dumps. Volatility Workbench is free, open source and runs in Windows. It provides a number of advantages over the command line version including,

- No need of remembering command line parameters.
- Storage of the platform and process list with the memory dump, in a .CFG file. When a memory image is re-loaded, this saves a lot of time and eliminates the need to get a process list each time.
- Simpler copy & paste.
- Simpler printing of paper copies (via right click).
- Simpler saving of the dumped information to a file on disk.
- A drop down list of available commands and a short description of what the command does.
- Time stamping of the commands executed.
- Auto-loading the first dump file found in the current folder.
- Support for analysing Mac and Linux memory dumps.

- **Tool to create Memory Dumps (MAGNET RAM)**

MAGNET RAM Capture is a free imaging tool designed to capture the physical memory of a suspect's computer, allowing investigators to recover and analyze valuable artifacts that are often only found in memory.

- **Windows File Analyzer**

Windows File Analyzer is a program designed to help you maintain your system in optimum shape by analyzing different elements that could come in handy when you need to repair some error, or figure out why something keeps crashing.

Windows File Analyzer works by analyzing your system's main elements, for example thumbnails, the Prefetch folder (which stores information that speeds up certain processes), direct accesses, the index.dat file (which stores cookies and temporary files), and the recycling bin.



- **Thumbcache viewer**

Thumbcache Viewer allows you to extract thumbnail images from the thumbcache\_\*.db and iconcache\_\*.db database files found on Windows Vista, Windows 7, Windows 8, Windows 8.1, and Windows 10. The program comes in two flavors: a graphical user interface and command-line interface.

- **WinPrefetchView**

WinPrefetchView is a small utility that reads the Prefetch files stored in your system and displays the information stored in them. By looking in these files, you can learn which files every application is using, and which files are loaded on Windows boot.

- **RegRipper**

RegRipper is an open source tool, written in Perl, for extracting/parsing information (keys, values, data) from the Registry and presenting it for analysis.

RegRipper consists of two basic tools, both of which provide similar capability. The RegRipper GUI allows the analyst to select a hive to parse, an output file for the results, and a profile (list of plugins) to run against the hive.

- **RegistryBrowser**

Registry Browser is a forensic software application. It's designed specifically for examining the Windows Registry. Users of Registry Browser are typically in the computer forensics or incidence response industry or anyone with a strong interest in Windows Registry Forensics.

- **Browsinghistoryview**

BrowsingHistoryView is a utility that reads the history data of different Web browsers (Mozilla Firefox, Google Chrome, Internet Explorer, Microsoft Edge, Opera) and displays the browsing history of all these Web browsers in one table.



- **Mitec mail viewer**

MiTeC Mail Viewer lets you read old email messages easily, including the complete text of the message and any attachments. Mail Viewer lets you access mail databases from Microsoft Outlook Express 4, 5, and 6; Windows Mail/Windows Live Mail; and Mozilla Thunderbird, as well as single EML files.

- **Rifiuti**

Rifiuti, the Italian word meaning "trash", was developed to examine the contents of the INFO2 file in the Recycle Bin. The foundation of Rifiuti's examination methodology is presented in the white paper located here. Rifiuti will parse the information in an INFO2 file and output the results in a field delimited manner so that it may be imported into your favorite spreadsheet program. Rifiuti is built to work on multiple platforms and will execute on Windows (through Cygwin), Mac OS X, Linux, and \*BSD platforms.

- **EXIFRead**

EXIFRead is a small freeware utility that extracts image information from EXIF/JPG files. Many new digital cameras (including the Nikon Coolpix 900, Fuji MX700, Kodak DC 260, and Minolta 1500) create image files that store information about the image and the camera that took it. Information about shutter speed, aperture, focal length is typically included. EXIFRead will extract and display all the information that it finds in the file. The information that EXIFRead displays can be copied to the clipboard and saved as a text file.

- **ExifTool**

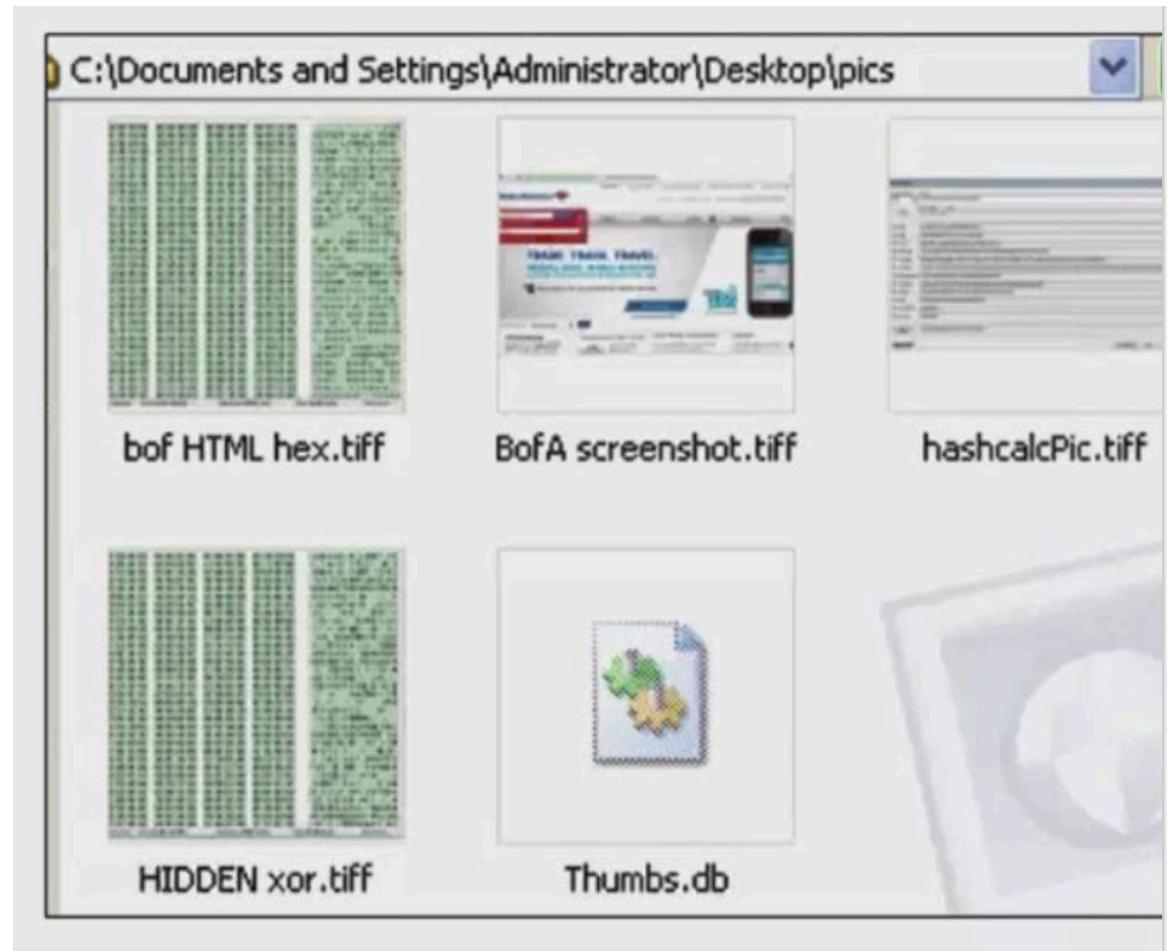
ExifTool is a free and open-source software program for reading, writing, and manipulating image, audio, video, and PDF metadata. It is platform independent, available as both a Perl library and command-line application.

# Thumbs.db and Thumbcache Analysis

Cyber Forensics and Incident Response

## Thumbnail database (Thumbs.db)

- Windows provides a thumbnail view of pictures saved in directories.
- The thumbnail, is a very small, low resolution version of the original picture.
- The thumbnails are saved in a hidden database file called thumbs.db.
- A thumbs.db file exists in each directory that contains pictures viewed as a thumbnail icon.



# Thumbs.db Analysis

- Thumbs.db is a hidden file and it does not delete the thumbnail when the original picture is deleted.
- Therefore, when users attempt to delete picture files, they may neglect to delete thumbs.db.
- Thumbs.db contains:
  - q File name
  - q File Path
  - q File Create time and Date
  - q Low resolution version of original picture

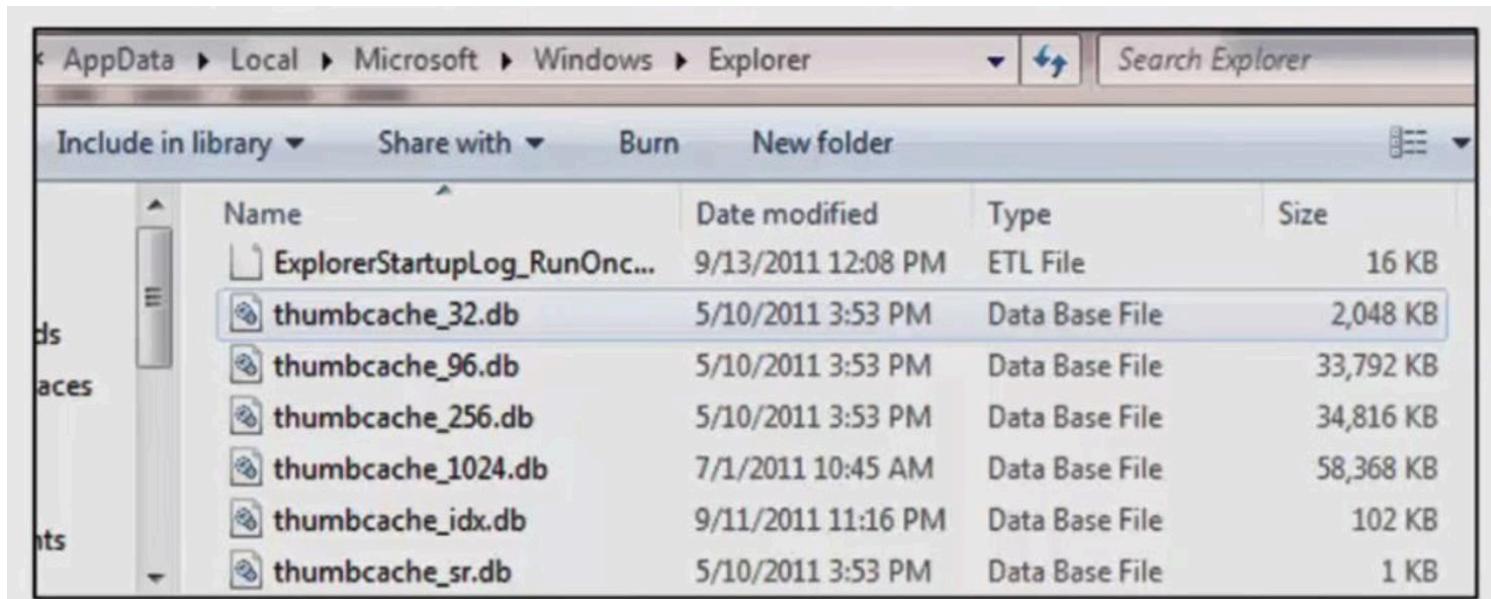
## Thumbs.db Analysis

- Several tools exist to parse Thumbs.db files.
- Screenshot shows output of Mitec's Windows File Analyzer.

Thumbnail Image	Filename	Timestamp
	screenshot of malicious mail from Mr. Magoo.jpg	7/23/2009 2:52:26 PM
	wnlog32_exe taskman autorun.jpg	7/27/2009 3:04:56 PM
	output of login info from Ophcrack.jpg	7/27/2009 2:44:34 PM
	registry entry showing winlog32 in registry.jpg	7/27/2009 3:56:34 PM

## Thumbcache.db (Windows Vista and Windows 7)

- Windows Vista & Windows 7 eliminated the directory specific thumbs.db file.
- It was replaced with a centralized thumbnail database called thumbcache.db.

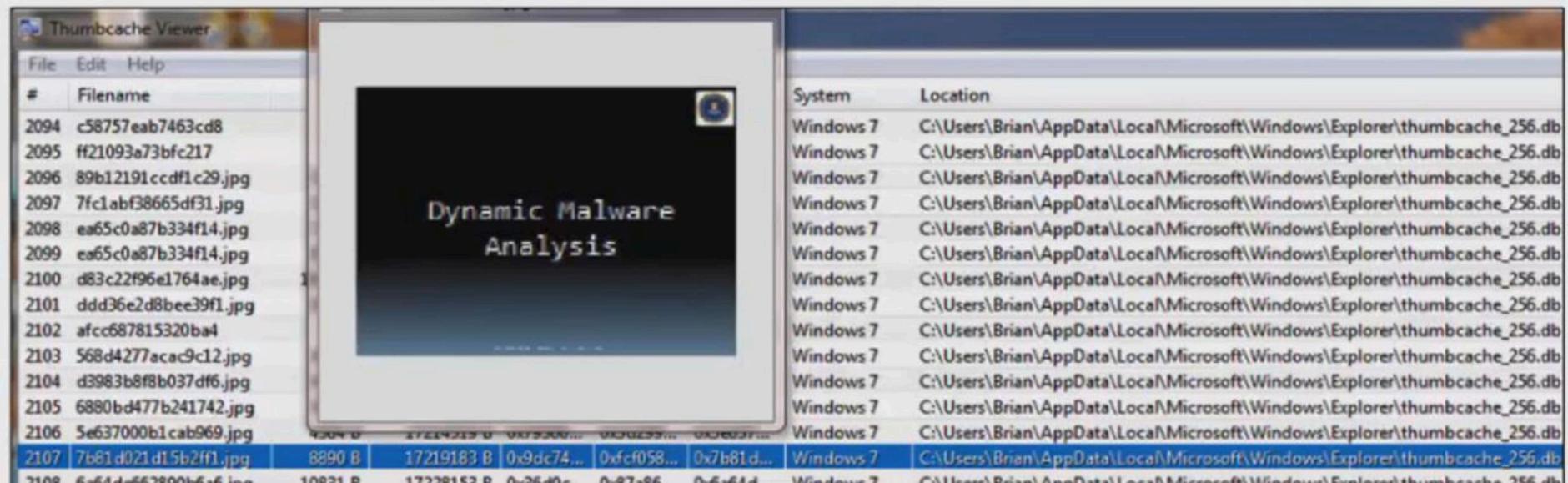


Name	Date modified	Type	Size
ExplorerStartupLog_RunOnc...	9/13/2011 12:08 PM	ETL File	16 KB
thumbcache_32.db	5/10/2011 3:53 PM	Data Base File	2,048 KB
thumbcache_96.db	5/10/2011 3:53 PM	Data Base File	33,792 KB
thumbcache_256.db	5/10/2011 3:53 PM	Data Base File	34,816 KB
thumbcache_1024.db	7/1/2011 10:45 AM	Data Base File	58,368 KB
thumbcache_idx.db	9/11/2011 11:16 PM	Data Base File	102 KB
thumbcache_sr.db	5/10/2011 3:53 PM	Data Base File	1 KB

C:\users\<profile>\AppData\Local\Microsoft\Windows\Explorer

# Thumbcache.db Analysis

- Thumbcache.db files are structured differently than thumbs.db but they can still parse. (See thumbcache Viewer below).
- File path, name and creation time no longer exist.



The screenshot shows the Thumbcache Viewer application interface. On the left is a table titled "Thumbcache Viewer" with columns for "#", "Filename", and other metadata. In the center is a preview window showing a dark screen with the text "Dynamic Malware Analysis". On the right is another table showing a list of system entries with columns for "System" and "Location".

#	Filename	File Size	File Type	File Hash	File Path	System	Location
2094	c58757eab7463cd8	4304 B	Image	0x7259213 B	0x975000... 0x9C9559... 0x9E9535...	Windows 7	C:\Users\Brian\AppData\Local\Microsoft\Windows\Explorer\thumbcache_256.db
2095	ff21093a73bfc217	10231 B	Image	0x72591E2 B	0x975000... 0x9C9559... 0x9E9535...	Windows 7	C:\Users\Brian\AppData\Local\Microsoft\Windows\Explorer\thumbcache_256.db
2096	89b12191ccdf1c29.jpg	8890 B	Image	0x9dc74...	0xfc058...	Windows 7	C:\Users\Brian\AppData\Local\Microsoft\Windows\Explorer\thumbcache_256.db
2097	7fc1abf38665df31.jpg	10231 B	Image	0x9dc74...	0x7b81d...	Windows 7	C:\Users\Brian\AppData\Local\Microsoft\Windows\Explorer\thumbcache_256.db
2098	ea65c0a87b334f14.jpg	8890 B	Image	0x9dc74...	0x7b81d...	Windows 7	C:\Users\Brian\AppData\Local\Microsoft\Windows\Explorer\thumbcache_256.db
2099	ea65c0a87b334f14.jpg	8890 B	Image	0x9dc74...	0x7b81d...	Windows 7	C:\Users\Brian\AppData\Local\Microsoft\Windows\Explorer\thumbcache_256.db
2100	d83c22f96e1764ae.jpg	8890 B	Image	0x9dc74...	0x7b81d...	Windows 7	C:\Users\Brian\AppData\Local\Microsoft\Windows\Explorer\thumbcache_256.db
2101	ddd36e2d8bee39f1.jpg	8890 B	Image	0x9dc74...	0x7b81d...	Windows 7	C:\Users\Brian\AppData\Local\Microsoft\Windows\Explorer\thumbcache_256.db
2102	afcc687815320ba4	8890 B	Image	0x9dc74...	0x7b81d...	Windows 7	C:\Users\Brian\AppData\Local\Microsoft\Windows\Explorer\thumbcache_256.db
2103	568d4277acac9c12.jpg	8890 B	Image	0x9dc74...	0x7b81d...	Windows 7	C:\Users\Brian\AppData\Local\Microsoft\Windows\Explorer\thumbcache_256.db
2104	d3983b8f8b037df6.jpg	8890 B	Image	0x9dc74...	0x7b81d...	Windows 7	C:\Users\Brian\AppData\Local\Microsoft\Windows\Explorer\thumbcache_256.db
2105	6880bd477b241742.jpg	8890 B	Image	0x9dc74...	0x7b81d...	Windows 7	C:\Users\Brian\AppData\Local\Microsoft\Windows\Explorer\thumbcache_256.db
2106	5e637000b1cab969.jpg	8890 B	Image	0x9dc74...	0x7b81d...	Windows 7	C:\Users\Brian\AppData\Local\Microsoft\Windows\Explorer\thumbcache_256.db
2107	7b81d021d15b2ff1.jpg	8890 B	Image	0x9dc74...	0x7b81d...	Windows 7	C:\Users\Brian\AppData\Local\Microsoft\Windows\Explorer\thumbcache_256.db
2108	6880bd477b241742.jpg	8890 B	Image	0x9dc74...	0x7b81d...	Windows 7	C:\Users\Brian\AppData\Local\Microsoft\Windows\Explorer\thumbcache_256.db

However, the thumbcache.db file name can be cross referenced with C:/ProgramData\Microsoft\Search\Data\Application\Windows\Windows.edb to determine the original file name.

# Prefetch File Analysis

# Prefetch Files

- Prefetch files are created to speed application execution on Windows systems. For computer forensic examiners, they provide a history of programs run on a computer.
  - Contain a list of files and folders accessed by the program.
  - Created 10 seconds after the execution of the program.
  - The prefetch folder can contain up to 128 prefetch files.
- Located at:
  - C:\Windows\Prefetch

# Prefetch Files

There are three types of prefetch files:

- Boot trace
  - Used when system is booted up.
    - NTOSBOOT-BOODFAAD(pf)
- Application
  - Normal Windows & 3rd party programs
    - Notepad.exe, Microsoft Word
- Hosting Application
  - Files used to start other processes
    - RUNDLL32.exe
    - DLLHOST.exe
    - MMC.exe

# Prefetch File Naming Convention

- Application Prefetching file
  - NC.EXE-06264562.pf
    - Name of file executed + extension + hash
      - Hash is a 32 bit number represented in hex
    - Algorithm uses pi (3.14159) as a seed for randomizing, plus the prime number 37 + file's path
      - $\text{hash} = (37 * \text{hash}) + \text{path}$
    - Path hashes can be identical across systems

- Prefetch Files contain:
  - Name and path of executable
  - Run Count of Executable
  - Time and date of execution
  - File Create time equals first execution time
  - List of Files and folders the program accesses
- OS specifics
  - Windows XP / Vista / 7 all use Prefetch
  - Windows Server does not use prefetch. (NTOSBoot only)

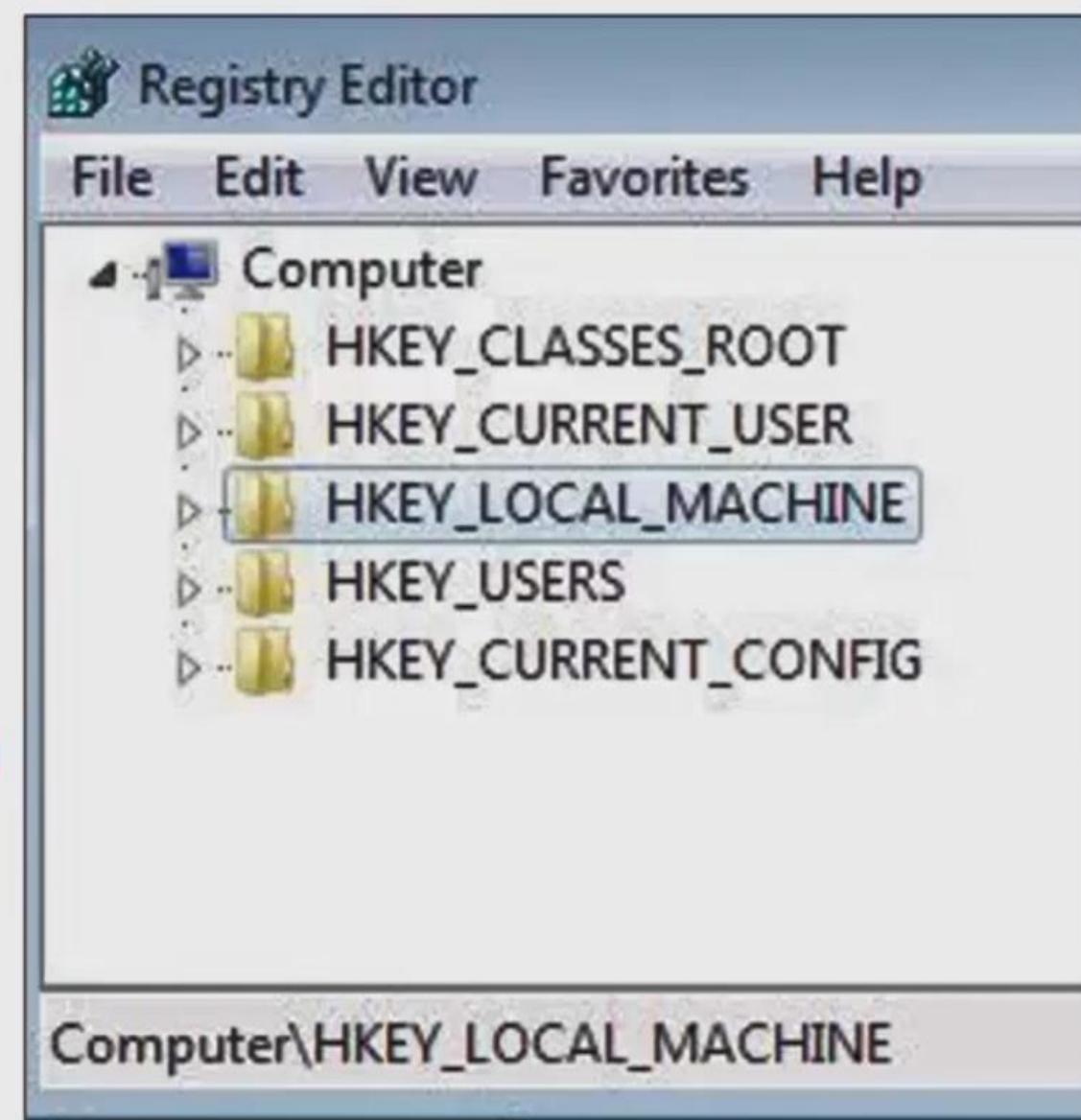
**Prefetch**

Name	Size	Type	Date Modified
BLASTCLN.EXE-2C69E3EA(pf	9 KB	PF File	4/11/2011 11:48 AM
IE4UINIT.EXE-169A5A39(pf	34 KB	PF File	4/11/2011 11:48 AM
LOGAGENT.EXE-027AF92B(pf	9 KB	PF File	4/11/2011 11:48 AM
MOFCOMP.EXE-01718E95(pf	11 KB	PF File	4/11/2011 11:48 AM
MSDTC.EXE-0E6E4AF7(pf	16 KB	PF File	4/11/2011 11:48 AM
REGSVR32.EXE-25EEFE2F(pf	20 KB	PF File	4/11/2011 11:48 AM
RUNDLL32.EXE-2F26E69F(pf	21 KB	PF File	4/11/2011 11:48 AM

# Introduction to the Windows Registry

# Windows Registry

- Hierarchical central database storing configurations for applications, hardware devices, and users
- Made up of keys and values found in five logical hives:
- **\*\*Disclaimer\*\*** This registry module discusses Windows XP. Newer, OS versions may not be identical but there is usually an equivalent. Use this section to understand the concepts, then explore more to understand OS specific details.
- **\*\*2<sup>nd</sup> Disclaimer\*\*** This is just a sample of registry artifacts. NOT A **COMPREHENSIVE LIST!**



# Windows Registry Files

- The following Registry files are accessible via a forensic image:
  - C:\WINDOWS\System32\config\SAM
  - C:\WINDOWS\System32\config\SECURITY
  - C:\WINDOWS\System32\config\SOFTWARE
  - C:\WINDOWS\System32\config\SYSTEM
  - C:Documents and Settings\<user\_profile>\ntuser.dat.
    - There is a ntuser.dat file for every user profile.
- Windows 7 introduced USRCLASS.DAT
  - Contains the muicache & shellbags

# Registry File Descriptions

- **SAM (Security Accounts Manager)**
  - Only applicable to local or domain administrators.
  - Contains user name, SID and encrypted password hash for all users in a domain.
- **SECURITY**
  - Contains the security permissions for administrators. Used by the system to enforce security policy.
  - Limited usefulness for forensics.

# Registry File Descriptions

- SOFTWARE
  - Contains programs and Windows settings for all software on the system.
  - Subkey exists for each vendor.
- SYSTEM
  - Contains Windows Operating system setup, mounted devices, hardware settings, and services.
- NTUSER.DAT
  - Settings specific to individual users. Tracks user activity and preferences.
  - Stored in the root of the user profile and moves between systems with roaming profiles.

## **Windows Registry Analysis**

### **Objectives:**

- **Use Registry Browser to access the suspect system's registry and extract evidence pertinent to the investigation.**

1. Open / Install Access Data's FTK Imager 3
2. Select File > Image Mounting > Browse to the Suspect image and mount it to a local drive letter.
3. Confirm that you now have a local drive letter containing the suspect image's folder structure.
4. Install and open Registry Browser. \*\*Remember to run as Administrator if you are using Windows 7\*\*
5. Select *File > Open Registry* and navigate to the mounted suspect image and select the *WINDOWS* folder on the root.
6. Within the registry, navigate to HKLM\System\CurrentControlSet\Enum\USBSTOR
  - a. **What is the Friendly name of the “Disk&Ven\_Memorex&Prod\_Mini&Rev\_PMAP” thumb drive that was attached to this system?** \_\_\_\_\_
  - b. **What is the Parent Prefix ID for this device?** \_\_\_\_\_
7. Navigate to HKLM\System\Mounted Devices. Go to *DosDevices\F:*. Look at the Value Data, the number following the *\??\Storage#RemovableMedia#* is the Parent Prefix ID for the F: Volume. What is it? \_\_\_\_\_
  - a. **Based on those two-parent prefix IDs, what Drive letter was assigned to the Disk&Ven\_Memorex&Prod\_Mini&Rev\_PMAP?** \_\_\_\_\_

**F:** \_\_\_\_\_

8. Navigate to the *HKEY\_USERS\S-1-5-21-1715567821-308236825-725344543-1003\Software\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs.bmp* path. What was the only .bmp file opened on this system?  
\_\_\_\_\_

9. Select *Tools > Generate Report*
- a. Go to the *Run, Run-, Runonce, RunOnceEX* section of the report. These are all autostarted. Do any of them look suspicious? What was the key name?
  - b. Go to the *Network Interfaces*. What was the system's IP address?
  - c. Go to *Windows Explorer - Recent Documents Cache by Extension*. What time and date was *Fake Light Saber Authenticity Papers.zip* last accessed?
-

# Metadata Analysis and Exif Data Analysis

# Metadata

- Metadata technically means “data about data”.
- Files may contain data about themselves, such as: author, last saved by, company, created time, modified time, and more.
- This can be very important to an intellectual property case.
  - If a person is suspected of stealing information from a former employer a first place to look is in the file metadata.

# Microsoft Word Metadata

- *Cybercrime.doc* – downloaded from:

- [cyber.law.harvard.edu/sites/cyber.law.harvard.edu/files/cybercrime.doc](http://cyber.law.harvard.edu/sites/cyber.law.harvard.edu/files/cybercrime.doc) (9/16/2011)
- Website listed Zittrain as the sole author, however, first page of document and file metadata all list different authors.
- File was downloaded and copied, therefore invalidating file system timestamps. However, file metadata timestamps retain original times.

Internet Law  
(forthcoming, Foundation Press)

Jonathan Zittrain  
Charles Nesson  
Lawrence Lessig  
William Fisher  
Yochai Benkler

Chapter 17: Cybercrime  
(preliminary version)

Authors

	Name	File Created	Last Accessed	Last Written
1	Cybercrime.doc	09/16/11 03:05:19PM	09/16/11 03:05:19PM	09/16/11 03:03:58PM

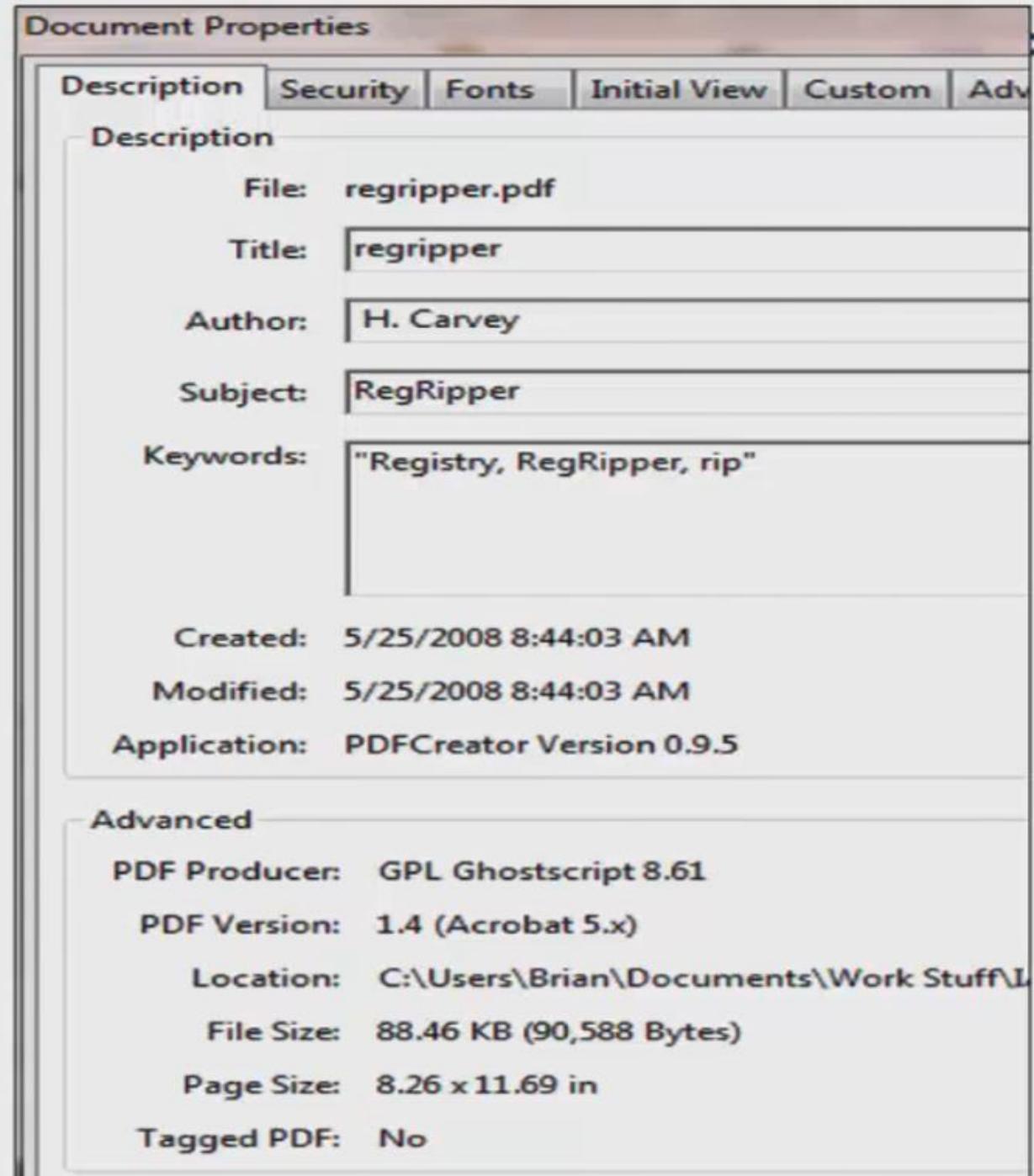
Working on entry: Cybercrime.doc  
Name Of Document: Case 1\Single Files\Cybercrime.doc  
Company:  
Title: COMPUTER CRIME CHAPTER  
Subject:  
Author: Andrew Ting ???  
Keywords:  
Comments:  
Last Saved By: rfink Possible editor?  
Template: Normal  
Version: Microsoft Office Word  
Revision: 2  
Create Date: 12/10/07 01:00:00PM  
Last Revision Date: 12/10/07 01:00:00PM  
Last Print Date:  
Number of Pages: 1  
Number of Characters: 176250  
Number of Paragraphs: 413  
Number of Words: 30920  
Hash: DC218744BE8DF0FEB6D4605F6E5B0A38

File System Timestamps Lost

Internal file timestamps

# PDF file Metadata

- PDF files contain extensive metadata that is displayed by Adobe: *File > Properties*.
- This information can give the analyst an idea about the history of a file.



# Picture Metadata – EXIF data

- Exif - Exchangeable Image File Format
  - Applies to: .JPG image files, .TIF image files, .WAV audio files.
  - Data can include:
    - Make and model of camera
    - Photo specifications
    - Date and Time
    - GeoLocation (Latitude & Longitude)
    - Camera owner & contact info
    - Serial number of camera
    - And Much More...
  - Cases potentially applicable to:
    - Kidnapping, child porn, terrorism, fugitive on the run, etc...

# Exif Data Example

- What important information does this picture's Exif Data Provide?

(downloaded from Flickr.com 9/18/11)



Creator Tool	Adobe Photoshop CS3 Windows
Metadata Date	2009:06:05 22:06:34+02:00
Lens	10.0-20.0 mm
Image Number	16
Flash Compensation	0
Owner Name	Zaza
Legacy IPTCDigest	FDF71F4CFCAC92102D21CBEC7A2284AF
Color Mode	3
Format	image/jpeg
Creator	Julien Rochas
Subject	SERIAL VW PASSION 74
Creator City	Gap
Creator Region	Hautes Alpes
Creator Postal Code	05000
Creator Country	France
Creator Work URL	<a href="http://zazaka.deviantart.com/">http://zazaka.deviantart.com/</a>

# Apple Iphone Exif Data

- Significant Exif data is saved by the Iphone.



ItemName	Information
JFIF_APP1	Exif
<b>Main Information</b>	
Make	Apple
Model	iPhone 4
Orientation	left-hand side
XResolution	72/1
YResolution	72/1
ResolutionUnit	Inch
Software	Camera+ 2.3.1
DateTime	2011:09:08 09:14:11
HostComputer	iPhone (iPhone OS 4.3.5)
YCbCrPositioning	centered
ExposureTime	1/686Sec
ExifInfoOffset	270
GPSInfoOffset	620
<b>Sub Information</b>	
FNumber	F2.8
ExposureProgram	Program Normal
ISO Speed Ratings	80
ExifVersion	0221
DateTimeOriginal	2011:09:08 09:14:11
DateTimeDigitized	2011:09:08 09:14:11
ComponentConfiguration	YCbCr
ShutterSpeedValue	1/686Sec
ApertureValue	F2.8
MeteringMode	Division
Flash	Not fired[Compulsory]
FocalLength	3.85(mm)
SubjectLocation	1255,967,639,636
FlashPixVersion	0100
ColorSpace	sRGB
ExifImageWidth	2592
ExifImageHeight	1936
SensingMethod	OneChipColorArea sensor
ExposureMode	Auto
WhiteBalance	Auto
SceneCaptureType	Standard
Sharpness	Hard
<b>GPS Information</b>	
GPSVersionID	2,2,0,0
GPSLatitudeRef	N
GPSLatitude	35 336.49 [DMS]
GPSLongitudeRef	W
GPSLongitude	80 5109.0159 [DMS]
GPSTimeStamp	09:14:09

# Calculating GPS Data

- GPS Data

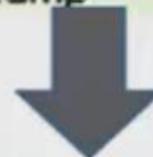
- Reference Points: **East = Positive, West = Negative, North = Positive, South = Negative**
- DMS = Degrees, Minutes Seconds
  - Minutes & Seconds must be a value between 1 - 59
  - Must convert to a decimal value.
    - Formula:  $\text{Degrees} + (\text{Min} + (\text{Sec}/60)) / 60 = \text{Lat / Long Decimal value}$
    - Or... Online Longitude / Latitude Calculator: <http://transition.fcc.gov/mb/audio/bickel/DDDMMMSS-decimal.html>

The screenshot shows a web page titled "transition.fcc.gov/mb/audio/bickel/DDDMMMSS-decimal.html". On the left, there is a vertical sidebar with the text "Bureau", "n", "n", "n", "n", "lysis", and "Division". The main content area has two input fields. The first field is labeled "Enter Degrees Minutes Seconds latitude:" and contains the values 35, 33, and 6.49. The second field is labeled "Enter Degrees Minutes Seconds longitude:" and contains the values 80, 51, and 9.0159. Below these fields are two buttons: "Convert to Decimal" and "Clear Values". At the bottom, the results are displayed: "Results: Latitude: 35.551803" and "Longitude: 80.852504".

# Calculating GPS Data



GPS Information	
GPSVersionID	2.2.0.0
GPSLatitudeRef	N
GPSLatitude	35 336.49 [DMS]
GPSLongitudeRef	W
GPSLongitude	80 5109.0159 [DMS]
GPSTimeStamp	09:14:09



Enter Degrees Minutes Seconds latitude:

Enter Degrees Minutes Seconds longitude:

Results: Latitude:  Longitude:

- Final Calculation: 35.551803 North (pos), 80.852504 West (neg).
- Google Maps entry: **35.551803 -80.852504**

# Exif Data Geo-location

Google maps

35.551803 -80.852504



Get directions

My places

A 101-179 Medical Park Rd  
Mooresville, NC 28117

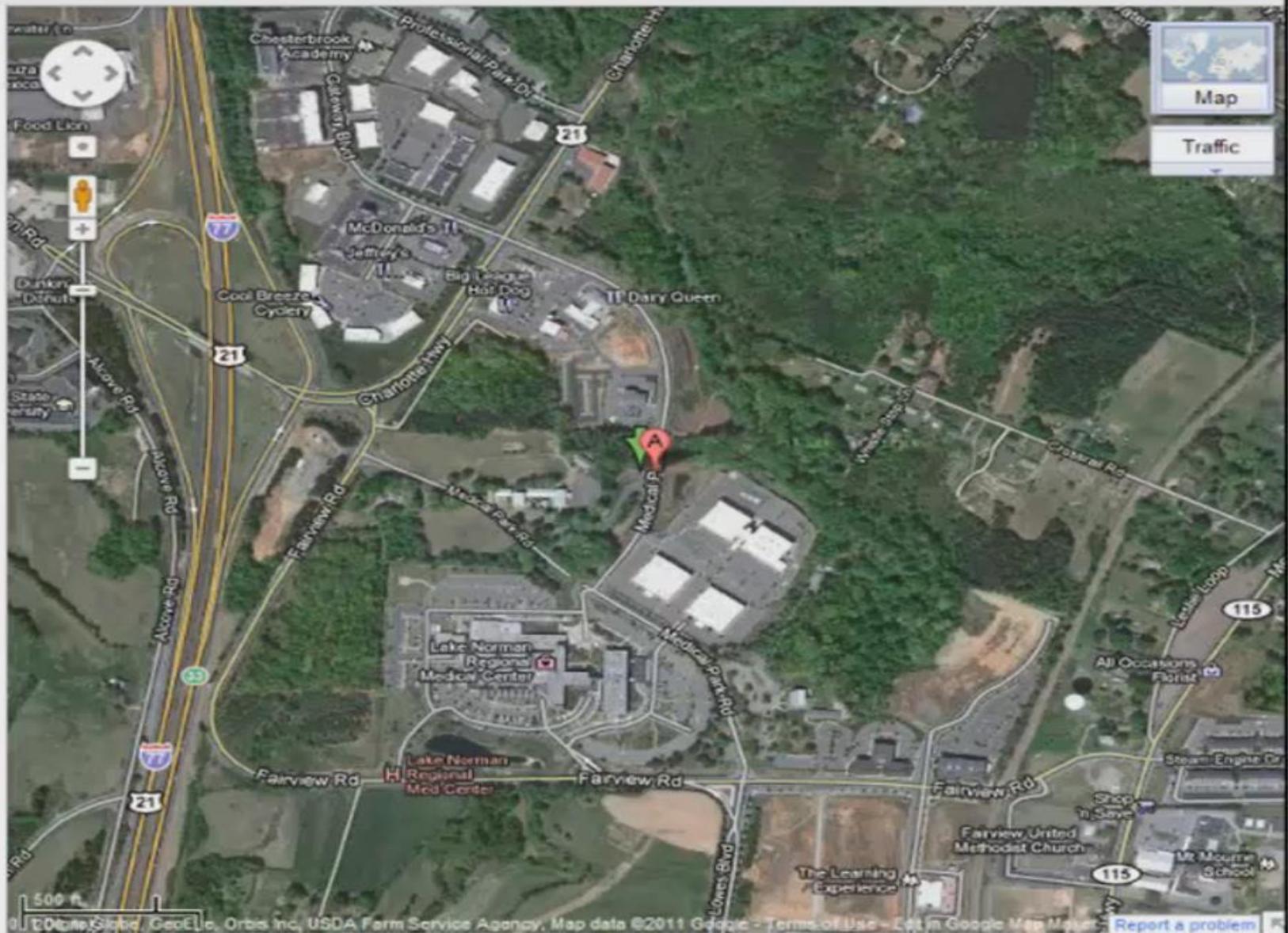


Directions Search nearby Save to map more ▾

Explore this area »

Places

Centre Presbyterian Church



## **Metadata and Exif Data Analysis**

### **Objectives:**

- **Use ExifRead.exe to extract Exif data embedded in each picture, including camera, time/date, and GPS data.**
  - **Use Google Maps to geo-locate the location of where pictures were taken, based on internal GPS data.**
  - **Determine where the picture was taken.**
1. Open ExifRead.exe
  2. Use ExifReader to open IMG 2812.jpg.
    - a. Examine the Exif data that is extracted from the IMG 2812.jpg and answer the following questions.
    - b. What is the Make and Model of the camera that took the photo?
    - c. What is the date and time that the picture was taken?
    - d. What are the Degrees, Minutes & Seconds, and Reference Points (N, S, W, E) of the picture?
    - e. Go to <https://www.fcc.gov/media/radio/dms-decimal> and calculate the decimal version of the Latitude and Longitude Points from which this picture was taken. What are they?
    - f. Go to Google Maps and type in the latitude and longitude points. (Remember: W = Neg, E = Pos, N = Pos, S = Neg). Where, exactly is the first bombing target?
  3. Use ExifReader to open IMG 5027.jpg.
    - a. Examine the Exif data that is extracted from the IMG 2812.jpg and answer the following questions.
    - b. What is the Make and Model of the camera that took the photo?
    - c. What is the date and time that the picture was taken?
    - d. What are the Degrees, Minutes & Seconds, and Reference Points (N, S, W, E) of the picture?
    - e. Go to <https://www.fcc.gov/media/radio/dms-decimal> and calculate the decimal version of the Latitude and Longitude Points from which this picture was taken. What are they?
    - f. Go to Google Maps and type in the latitude and longitude points. (Remember: W = Neg, E = Pos, N = Pos, S = Neg). Where, exactly is the second bombing target?

# File Signature Analysis

# File Signatures

 WinPrefetchView.doc	43 KB	Microsoft Office Word 97 - 2003 Document
 WinPrefetchView.exe	43 KB	Application
 WinPrefetchView.jpg	43 KB	JPEG image
 WinPrefetchView.ppt	43 KB	Microsoft Office PowerPoint 97-2003 Pres...

- Windows identifies files by their extension.
- Extensions are linked to programs. For example, Windows knows to open a .doc file with Microsoft Word.
- A basic, but often effective, file obfuscation technique is to simply alter a file name & extension to appear as a different file type.
  - For Example: **Malware.exe** becomes **1.jpg**

# File Signatures

- Computer Forensics uses a much more reliable file identification technique: **Signature Analysis**.
- A file signature is the first few bytes of a file.
- The file signature should match the extension. If it doesn't, this could indicate efforts to hide it.
- Forensic tools can automatically analyze all files on a hard drive.

The screenshot shows a software interface for file analysis. At the top, there's a header with columns: Name, File Ext, File Category, and Logical Size. A single row is visible, showing a file named "WinSvc.gif" with a ".gif" extension, categorized as "Picture", and a logical size of 340,319. Below this is a toolbar with various icons: Text, Hex, Doc, Transcript, Picture, Report, and Console. The main area is a hex editor window. The first few bytes of the file are displayed, starting with "MZ", which is highlighted with a green box. The text view below shows the ASCII representation of these bytes: "MZÿÿ@í!,·LÍ!||This program must be rrun under Win32 \$7...". The rest of the file content is mostly binary data represented by dots and other characters.

# File Signature Analysis

- File signatures are also referred to as:
  - Header
  - Magic Number
- Some Important headers to know:
  - MZ = Executable (.exe)
  - ÿØÿà = JPG picture file
  - PK = Zipped files & Microsoft Office 2007 and newer files (.zip, .docx, .pptx, .xlsx, etc...)
  - ĐI.àj±.á = 2003 & older Microsoft Office files (.doc, .ppt, .xls, etc...)
  - %PDF = Adobe Acrobat PDF files (.pdf)
  - Rar! = WinRar compressed files (.rar)

# Lab – Internet Activity Analysis

## Objectives:

- Use Nirsoft's BrowsingHistoryView to Parse Internet History Files
- Determine if the victim's Internet History indicates criminal activity or an attack vector.

1. Open Access Data's FTK Imager 3
  2. Mount the Suspect image (File > Image Mounting > Select the suspect image file)
  3. Install / Open Nirsoft's BrowsingHistoryView. (**If you are using Windows 7 or Vista be sure to right-click and select *Run as Administrator***)
    - a. In the *Advanced Options* box note the *Filter by visit date/time* box and select *Load History Items from any time*.
    - b. Leave all Web Browsers checked.
    - c. Under the *Load history from..* option select: *Load history from the specified profile* (For example: *c:\users\admin*)
    - d. In the next box, click the box with three dots to open the Windows navigation browser and navigate to your mounted suspect image and the folder *\Documents and settings\Owner*.
    - e. Click *OK*.
  4. You can sort by any of the header bars. You can also search for terms by clicking *Edit > Find*.
  5. What Internet browser's did this profile use?
-

6. Find the terms “search, google search, bing”. This will give you an idea of what kind of terms the suspect searched for on the Internet. What search terms did the suspect search for that might be of interest to this investigation? What Search engine did he use? What was the time / date?
- 
- 
- 

- a. Did the user have webmail? What was his email address?

=

---

- b. Search for the term “file:///”. This will show the file’s that were accessed on the local system but were logged in the Index.dat file. \*\*%20 indicate a space\*\* Are there any files relevant to this investigation?

=

---

---

---

- c. Were any of the relevant files mentioned above in a location other than the computers C:/ drive? What were their names?

d. This computer is believed to be the victim of a malware attack. Can you confirm or deny this, based on your Internet Analysis? If it did occur, what was the name of the malware and where did it come from?

---

---

---

---

# Email Analysis

# E-mail

- E-mail is the primary method of communication in modern corporations
- It is a fast and easy way to transmit large amounts of data to external points
- Attachments may include executables / malicious code
- Primary means of phishing & spear-phishing attacks
- Important tool in social engineering attacks

# Typical E-mail Folder Structure

- **Inbox** – Mail that was received by the user
  - May include user-specific subfolders for organization
- **Outbox** – Temporary holding area for messages sent by the user but not yet processed by the server
- **Sent Items** – Mail that the user sent
- **Drafts** – Unfinished e-mail messages
- **Deleted Items** – Mail that the user deleted

# E-mail Process

## Process of sending e-mail

User writes mail  
(Saved in Drafts until complete)

User sends mail  
(Saved in Outbox until sent by server)

Server completes sending mail  
(Saved in Sent Mail)

User Deletes e-mail (Saved in Deleted Items until purged)

## Process of receiving e-mail

User receives mail  
(Saved in Inbox)

User deletes mail  
(Saved in Deleted Items)

User purges deleted items (May still be recoverable from container file unallocated space)

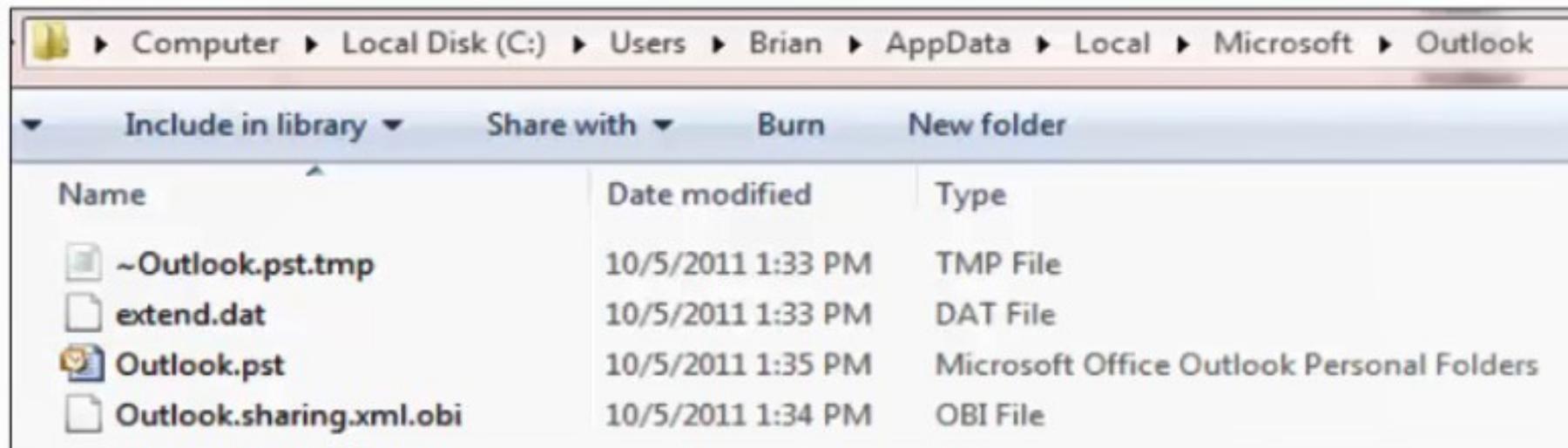
# E-mail Analysis

- E-mail can exist on a computer system in a number of different formats.
  - Outlook
    - Personal Storage Files (.pst)
    - Offline Storage Table (.ost)
    - Exchange Database File (.edb)
  - Outlook Express (.dbx files)
  - Lotus Notes (.nsf file)
  - Thunderbird (.msf file)



# Outlook Container Files

- E-mail container files store user's e-mail in a single file on the hard drive.  
(Including inbox, sent items, deleted items, etc...)
- Microsoft Outlook uses the .pst file format.
  - XP Location: C:\Documents and Settings\<User Profile>\Local Settings\Application Data\Microsoft\Outlook\<user profile>.pst
  - Windows 7: C:\Users\Brian\AppData\Local\Microsoft\Outlook
  - You may also find Archive.pst (for archived items) or .ost files (offline storage) here.



# Web Based E-mail

- Many user's primary e-mail communication is via web services.
  - Windows Live (Hotmail)
  - Yahoo Mail
  - Gmail
- Web Based e-mail stores mail contents on the web server, not on the local machine.
  - Therefore, the recoverable contents of webmail is limited.
  - However, fragments are often recovered from Temporary Internet Files, pagefile.sys, or unallocated space.
- Webmail keywords:
  - Yahoo! Mail: Showletter, ShowFolder Compose,
  - Hotmail: HoTMail, hmhome, getmsg, doattach, compose
  - Gmail: Mail[#]

## Lab - Email Analysis

### **Objectives:**

- Use Access Data's FTK Imager to mount a suspect image and locate E-mail Files.
  - Use Mitec's Mail View to parse e-mail files
  - Determine if the user's e-mail files contain evidence of illegal activity.
1. Open FTK Imager.
  2. Mount the Suspect image: Vader\_Home\_Computer.001. (File > Image Mounting > Select the suspect image file>click Mount)
  3. Open Mitec's Mail View Program (MailView.exe). **\*\*If you are using Windows 7 or 8, make sure you right-click and select “Run As Administrator” rather than just double-clicking the program.\*\***
    - a. Select the button for *Mozilla Thunderbird message database*.
    - b. Click the folder to browse to the Thunderbird email.
    - c. Navigate to the following directory on your mounted suspect image: *E:\Documents and Settings\Owner\Application Data\Thunderbird\Profiles\cnllzbsb.default\Mail\pop.mail.yahoo.com*
    - d. Select *Inbox*. **\*\*Not Inbox.msf – Choose the one with the largest size, if you aren't sure.\*\***
    - e. In Mitec Mail Viewer, click *File > View* and repeat the previous process to also open *Trash and Sent*.
    - f. You can sort messages by any header (From, Subject, To, Received, Size) by clicking on their header bar. You can click *Messages > Collect Email Addresses* to show all email addresses in the file. You can create a filter to search for terms but be sure to also select a location in the grey bar to the left of the search term box. (the searches may take a minute, be patient).

4. Answer the following questions:
5. Who owns this email box and what is the email address: \_\_\_\_\_
6. When was the first email sent and received by the email box owner.
  - a. \_\_\_\_\_
7. Review the email and determine if there are any indications of criminal activity.
  - a. If yes, what are the names and email addresses of the people involved in the crime?  
\_\_\_\_\_  
\_\_\_\_\_
  - b. Explain the series of events around this crime, based on your email analysis.  
\_\_\_\_\_  
\_\_\_\_\_  
\_\_\_\_\_  
\_\_\_\_\_  
\_\_\_\_\_  
\_\_\_\_\_  
\_\_\_\_\_  
\_\_\_\_\_  
\_\_\_\_\_  
\_\_\_\_\_  
\_\_\_\_\_  
\_\_\_\_\_  
\_\_\_\_\_  
\_\_\_\_\_

# Lab – Volatile Memory Analysis

## Objectives

- Use the Volatility Standalone executable to analyze the memory dump *Vader\_Home\_Memory.raw*.
- Discover further evidence of crime, as it is relevant to this investigation.
- Use the Volatility Standalone executable to analyze the memory dump *SilentBanker.vmem*.

## **PART 1: *Vader\_Home\_Memory.raw* Memory Analysis Lab:**

1. Identify what process(es) and PIDs have open TCP connections.
  - a. What command did you use to obtain this data?
  - b. Does it appear to be malicious? Why?
  - c. What does the local port number indicate to you?

---

---

2. Identify what process(es) and PIDs had previously open TCP connections.
  - a. What command did you use to obtain this data?
  - b. Other than the connection previously mentioned, do any appear to be malicious? Why?
  - c. What does the remote port number indicate to you?

---

---

3. Based on the PIDs you identified in the previous question, determine what processes were responsible for the suspect network connections.  
-What command did you use to obtain this data?

---

---

4. Extract the IRC malware to the local hard drive in both executable file format and in executable memory format. Which one is bigger? Why?

---

---

---

---

## PART 2: SilentBanker Memory Analysis Lab:

1. Identify what process(es) and PIDs have open TCP connections for *SilentBanker.vmem*.  
-What command did you use to obtain this data?

---

---

2. Identify what process(es) and PIDs had previously open TCP connections for *SilentBanker.vmem*.  
-What command did you use to obtain this data?

---

---

3. Identify what process was victimized by injected malicious code for *SilentBanker.vmem*.  
-What command did you use to obtain this data?

---

---

4. Extract the injected malicious code to the hard drive for *SilentBanker.vmem*.  
-What command did you use to obtain this data?



*The Senator Patrick Leahy  
Center for Digital Investigation*



## Cloud Forensics

Written & Researched by:  
Maegan Katz & Ryan Montelbano

175 Lakeside Ave, Room 300A  
Phone: 802/865-5744  
Fax: 802/865-6446  
<http://www.lcdi.champlin.edu>

November 4, 2013

**Disclaimer:**

*This document contains information based on research that has been gathered by employee(s) of The Senator Patrick Leahy Center for Digital Investigation (LCDI). The data contained in this project is submitted voluntarily and is unaudited. Every effort has been made by LCDI to assure the accuracy and reliability of the data contained in this report. However, LCDI nor any of our employees make no representation, warranty or guarantee in connection with this report and hereby expressly disclaims any liability or responsibility for loss or damage resulting from use of this data. Information in this report can be downloaded and redistributed by any person or persons. Any redistribution must maintain the LCDI logo and any references from this report must be properly annotated.*

## Contents

Introduction.....	2
Background.....	2
Purpose and Scope .....	2
Research Questions.....	2
Terminology.....	2
Methodology and Methods .....	4
Equipment Used.....	4
Data Collection .....	5
Analysis.....	5
Results.....	6
SkyDrive .....	6
Dropbox .....	6
Google Drive.....	6
Conclusion .....	7
Further Work.....	7
Appendix A.....	7
SkyDrive .....	7
Dropbox .....	9
Google Drive.....	10
Appendix B .....	12
SkyDrive .....	12
Dropbox .....	13
Google Drive.....	14
References.....	16

## Introduction

Cloud storage is a new technology that makes it possible for users to upload data to the web, allowing for instant accessibility and the ability to share data with others at any time. Cloud technology is creating a challenge for forensic investigators, as data can be uploaded or shared from one computer and opened on another computer without leaving a large amount of traceable evidence. Google Drive, Dropbox, and SkyDrive are a few examples of these cloud storage services that need to be investigated further.

## Background

The use of cloud forensics is an emerging field that requires more attention than standard digital forensics. A large portion of the research done on cloud computing so far has dealt with the increasing legal troubles that law enforcement will face when attempting to seize or retrieve information in the cloud. Many organizations that are using cloud services may not have considered the legal issues that come with public clouds. According to Network World (Messmer, 2013), “any business that anticipates using cloud-based services should be asking the question: What can my cloud provider do for me in terms of providing digital forensics data in the event of any legal dispute, civil or criminal case, cyber-attack, or data breach?” Other studies have compared the actual providers themselves. Each cloud service provider is going to be different; this complicates cloud-based forensics because each company will have different rules, guidelines, and requirements. According to the IATAC (Scott Zimmerman, 2011), “to date, there has been very little research done on the current state of the tools, processes, and methodologies to obtain legally defensible digital evidence in the cloud.”

## Purpose and Scope

The purpose of this research is to find key aspects of different cloud storage applications to aid forensic investigators and law enforcement. It is important to find any and all relevant artifacts that are created during the applications use, as well as any files or metadata of files being uploaded, whether or not they have been deleted.

## Research Questions

- 1) What artifacts are created or modified when the cloud storage application is installed?
- 2) Is there evidence of files after they have been deleted from the cloud storage application folder?
- 3) What changes are made to artifacts and metadata when a file is moved or copied from the base folder to another folder?
- 4) What artifacts remain after the cloud storage application has been unlinked and uninstalled?

## Terminology

**Artifacts** – A digital artifact is any undesired alteration in computer data. Hardware/software malfunctions, compression, deletion, and movement can all be possible causes.

**Cloud Computing** – Cloud computing is a “model for enabling convenient, on-demand network access to a shared pool of configurable computing resources, such as networks, servers, storage, applications, and services, that can be rapidly provisioned and released with minimal management effort or service provider interaction” (Linthicum, 2013).

**Cloud Forensics** – Cloud forensics is “the application of digital forensics in cloud computing as a subset of network forensics. It is a cross discipline between cloud computing and digital forensics” (Cruz, 2012).

**CSV (Comma-separated value)** – CSV files store rows and columns of data in plain-text form, much like an Excel document.

**Digital Evidence** – Digital evidence is “information of probative value that is stored or transmitted in a binary form” (NCFS, 2012). Digital evidence not only includes computers in the traditional sense, but also digital audio, video, and pictures.

**Digital Forensics** – The identification, examination, collection, preservation, and analysis of computer data and information.

**DropBox** – File hosting service operated by Dropbox, Inc. Dropbox offers cloud storage, file synchronization, and client software.

**EnCase** – EnCase is a suite of digital forensics tools created by Guidance Software. The software comes in several forms designed for forensic, cyber security, and e-discovery use. Data recovered by EnCase has been used successfully in various court systems around the world.

**E01** – An E01 is the extension of an image file for EnCase.

**FTK** – Forensic Toolkit, or FTK, is computer forensics software made by AccessData. It scans a hard drive looking for data. It can, for example, locate deleted e-mails and scan a disk for text strings to use as a password dictionary to crack encryptions. The toolkit also includes a standalone disk imaging program called FTK Imager. It saves an image of a hard disk in one file or in segments that may be reconstructed. FTK Imager calculates MD5 hash values and confirms the integrity of the data before closing the files.

**Google Drive** – Google Drive is a file storage and synchronization service provided by Google. It provides cloud storage, file sharing, and collaborative editing. Files shared publicly on Google Drive can be searched for with web search engines.

**Metadata** – Metadata is data providing information about one or more aspects of the data such as: means of creation of the data, purpose of the data, time and date of creation, creator of the data, and the location where the data was created (NISO, 2004).

**Microsoft SkyDrive** – File hosting service that allows users to upload and sync files to a cloud storage and then access them from a Web browser or their local/mobile device. It is part of the Windows Live range of online services and allows users to keep the files private, share them with contacts, or make the files public. Publicly shared files do not require a Microsoft account for access.

**Pagefile** – A pagefile is a form of virtual memory that stores data that can't be held by RAM.

**Unallocated Space** – Unallocated space is where files or pieces of files that are temporary or deleted are stored.

**Virtual Machine** – A virtual machine is a software-based computer that executes and runs programs like a physical machine. A virtual machine supports the execution of a complete operating system. VMs usually emulate an existing architecture and are built with the purpose of either providing a platform to run programs where the real hardware is not available for use, or of having multiple instances of virtual machines. This leads

to more efficient use of computing resources, both in terms of energy consumption and cost effectiveness (known as hardware virtualization).

## Methodology and Methods

Before we began this project, we created a virtual machine (VM) for each of the three cloud services: Dropbox, SkyDrive, and Google Drive. We chose to create a 20GB Windows 7 VM for each cloud service and downloaded Sysinternals Process Monitor to record any and all changes/additions that the cloud services made during their use, from the installation to when the services were uninstalled.

Once we created the VMs and downloaded Process Monitor, we started Process Monitor, downloaded the cloud service, and started the installation process. Before continuing with the installation process, we filtered Process Monitor by the cloud service's setup Process Identifier (PID). We selected to only show results from file system activity and registry activity, as we are mainly looking for changes to the registry and files. We then continued with the installation of the cloud service. After the cloud service finished installing, we saved the results from Process Monitor and shutdown the VM. We then copied the VM to a new folder in order to preserve the original artifacts that were created during the installation process. For our subsequent research, we continued with the following: starting the VM, starting Process Monitor, filtering the process monitor results by the cloud service's PID(s), performing the required action for the step (setup, upload files, copy a file, move a file, open a file, delete a file, unlink the account, and uninstall), saved the results from process monitor, shutdown the VM, and copied the VM to a new folder.

The data set files that we deleted from SkyDrive were turtle.jpg and wildlife.wmv. GettingStarted.pdf and WinPcap\_4\_1\_2.exe were deleted from Dropbox, and Plan.docx and WinPcap\_4\_1\_2.exe were deleted from Google Drive.

After we finished creating the virtual machines, we used FTK Imager 3.1.0.1514 to create E01 files for each VM, which we imported into FTK 4.1.0.165 for analysis. In total, we had seven different images per cloud service to parse through and several dozen CSV files from Process Monitor to view changes made to the files and the registry.

Appendix A shows the steps taken with each of the cloud services.

## Equipment Used

**Table 1: Equipment and Software**

Equipment/Software	Version	Details
VMware Workstation	9.0.2	<i>Used to create and run the Window 7 VMs</i>
Windows 7	64-bit	<i>Used to create the base VM for this project</i>
Process Monitor	3.05	<i>Used to monitor change made to the files and the registry</i>
Dropbox	2.0.26	<i>Cloud service used to generate data</i>
SkyDrive	17.0.2015.0811	<i>Cloud service used to generate data</i>

Google Drive	<i>1.11.4865.2530</i>	<i>Cloud service used to generate data</i>
FTK	<i>4.1.0.165</i>	<i>Used to analyze the images from the VM</i>
FTK Imager	<i>3.1.0.1514</i>	<i>Used to create E01 files for each VM</i>

## Data Collection

The data we collected for this project included CSV files from Process Monitor, as well as files from searches made in FTK. Table 2 shows the number of unique artifacts found using Process Monitor for each of the cloud services. Appendix B shows all of the information related to the two deleted files in each cloud service.

**Table 2: Total Number of Filtered Files**

SkyDrive Process	# of unique paths	# of files with "SkyDrive" in the name	# of registry keys with "SkyDrive" in the name
Install	4959	171	69
Upload	6165	224	80
Move/Copy	179	20	0
Open	1	0	0
Delete	595	14	3
Unlink	1178	48	28
Uninstall	4689	217	56
Dropbox Process	# of unique paths	# of files with "Dropbox" in the name	# of registry keys with "Dropbox" in the name
Install	4163	39	52
Setup	87	60	10
Upload	212	36	2
Move/Copy	75	24	4
Open	106	5	0
Delete	127	17	1
Unlink	3000	19	12
Uninstall	1222	43	10
Google Drive Process	# of unique paths	# of files with "GoogleDrive" in the name	# of registry keys with "GoogleDrive" in the name
Install	9438	7	102
Upload	9449	4	101
Move/Copy	138	0	0
Delete	2767	1	1
Unlink	118	2	2
Uninstall	118	2	2

## Analysis

All of our data for analysis came from the CSV files created by Process Monitor and search results from FTK. Process Monitor has the option to save results by path, folder, and extension. We chose to focus on the path

results and filter those using Excel. We first separated the unique paths by file path and registry path. Then, we filtered the results further so that only the results containing the words ‘Dropbox,’ ‘SkyDrive,’ or ‘GoogleDrive’ were listed, to show the files or registry keys that are definitely related to the cloud service. Next, in FTK, we acquired the deleted, unlinked, and uninstalled images for each of the cloud services and performed a keyword search for the two deleted files from each cloud service. The deleted image is the image we took after deleting a few files from the cloud services. The unlink image is where we unlinked the user account from the application, and the uninstall image is where we uninstalled the application.

## Results

### SkyDrive

4959 artifacts were created or modified when SkyDrive was installed. 171 of those were file paths that contained the word “SkyDrive,” and 69 of those were registry paths that contained the word “SkyDrive.” 6165 artifacts were created or modified when files were uploaded to SkyDrive. 224 of those were file paths that contained the word “SkyDrive,” and 80 of those were registry paths that contained the word “SkyDrive.” 179 artifacts were created or modified when files had been moved or copied within SkyDrive. 20 of those were file paths that contained the word “SkyDrive.” Additionally, we were able to find evidence of turtle.jpg and wildlife.wmv in unallocated space, a number of \$Recycle.Bin CSV files, pagefile.sys, and the AppData folder. There were 24 files related to turtle.jpg and 19 files related to wildlife.wmv that remained after SkyDrive had been unlinked and uninstalled. In total, 1178 unique artifacts were affected when SkyDrive was unlinked and 4689 unique artifacts when SkyDrive was uninstalled.

### Dropbox

4163 artifacts were created or modified when Dropbox was installed. 39 of those were file paths that contained the word “Dropbox,” and 52 of those were registry paths that contained the word “Dropbox.” 212 artifacts were created or modified when files were uploaded to Dropbox. 36 of those were file paths that contained the word “Dropbox,” and 2 of those were registry paths that contained the word “Dropbox.” 75 artifacts were created or modified when files were moved or copied within Dropbox. 24 of those were file paths that contained the word “Dropbox,” and 4 of those were registry paths that contained the word “Dropbox.” We were unable to find evidence of GettingStarted.pdf, but we were able to find a renamed deleted version of GettingStarted.pdf [Getting Started (deleted e8e9f5e1ece9b19af69596f25b4fb39).pdf] in pagefile.sys. We were able to find evidence of WinPcap\_4\_1\_2.exe in unallocated space, as well as in pagefile.sys. There were 2 files related to GettingStarted.pdf and 1 file related to WinPcap\_4\_1\_2.exe that remained after Dropbox had been unlinked and uninstalled. In total, 3000 unique artifacts were affected when Dropbox was unlinked and 1222 unique artifacts when Dropbox was uninstalled.

### Google Drive

9438 artifacts were created or modified when Google Drive was installed. 7 of those were file paths that contained the word “GoogleDrive,” and 102 of those were registry paths that contained the word “GoogleDrive.” 9449 artifacts were created or modified when files were uploaded to Google Drive. Four of those were file paths that contained the word “GoogleDrive,” and 101 of those were registry paths that contained the word “GoogleDrive.” 138 artifacts were created or modified when files had been moved or copied

within Google Drive. We were also able to find evidence of Plan.docx and WinPcap\_4\_1\_2.exe in unallocated space, a number of \$Recycle.Bin CSV files, and pagefile.sys. Additionally, we found evidence of Plan.docx in a configuration file. There are 13 files related to WinPcap\_4\_1\_2.exe and 12 files related to Plan.docx that remained after Google Drive had been unlinked and uninstalled. In total, 118 unique artifacts were affected when Google Drive was unlinked and 118 unique artifacts when Google Drive was uninstalled.

## Conclusion

Our results show that a number of artifacts are left behind after the deletion, unlinking, and uninstalling of SkyDrive, Dropbox, and Google Drive. We found that evidence of the files could be located in unallocated space for each application, along with \$Recycle.Bin CSV files, and pagefile.sys. The number of artifacts that were affected upon creation, deletion, uploading, and moving within each application varied. All three cloud services left behind trace evidence of our target files after being unlinked and uninstalled. With each application, the amount of the evidence found was different, but it was still present in some form.

## Further Work

Within the field of cloud forensics, more research and planning needs to be done, along with the implementation of industry standard law practices. Currently, rules, regulations, guidelines, and standard practices can vary greatly from provider to provider. This makes it increasingly difficult for forensic technicians to work.

For this project, we only used common or popular cloud services. These are services that have been around for a number of years, giving them time to grow and understand the industry that they are working with and have helped create. Additionally, some cloud services are accompanied by a mobile application, which we feel should be researched. To our team, it is important to know if the mobile application also leaves behind artifacts after it is unlinked and uninstalled. We were able to find that there are still remnants of files after they have been deleted, as well. Our next step would be to see if these files are actually recoverable in their original state.

## Appendix A

### SkyDrive

Time	Action/Variable
7/17/13 11:00	Powered on VM
11:01	Filtered Process Monitor by the SkyDrive PIDs
11:02	Used Chrome to navigate to SkyDrive download
11:03	Downloaded SkyDrive and started installed
11:06	Saved log files from Process Monitor
11:06	Shut down VM
11:07	Copied VM to next folder
7/22/13 10:19	Powered on VM

10:21	Copied “DataSet” to VM desktop
10:23	Filtered Process Monitor by the SkyDrive PIDs
10:24	Started SkyDrive > Prompted to create account
10:35	Added MP3, Zip, PDF, RTF, and EXE through desktop version of SkyDrive * Dragged into SkyDrive > automatically removed files from “DataSet” folder
10:40	Navigated to SkyDrive website
10:44	Uploaded XLS, DOCX, JPEG, and WMV through website version of SkyDrive * Did not remove files from “DataSet” folder like with the desktop version
10:50	Saved log files from Process Monitor
10:53	Shut down VM
10:53	Copied VM to next folder
8/2/13 11:49	Powered on VM
11:52	Filtered Process Monitor by the SkyDrive PIDs
12:02	Created folder “CloudStuff”
12:03	Moved RTF to folder
12:07	Copied DOCX to folder
12:10	Saved log files from Process Monitor
12:12	Shut down VM
12:16	Copied VM to next folder
12:44	Powered on VM
12:54	Filtered Process Monitor by the SkyDrive PIDs
12:55	Opened JPG
12:56	Opened RTF
12:58	Saved log files from Process Monitor
13:00	Shut down VM
13:04	Copied VM to next folder
8/5/13 13:41	Powered on VM
13:44	Filtered Process Monitor by the SkyDrive PIDs
13:53	Deleted WMV file via application
13:54	Navigated to SkyDrive website
13:56	Deleted JPG via SkyDrive website
14:00	Saved log files from Process Monitor
14:03	Shut down VM
14:04	Copied VM to next folder
15:01	Powered on VM

15:03	Filtered Process Monitor by the SkyDrive PIDs
15:06	Unlinked Account
15:07	Saved log files from Process Monitor
15:09	Shut down VM
15:09	Copied VM to next folder
16:04	Powered on VM
16:05	Filtered Process Monitor by the SkyDrive PIDs
16:08	Uninstalled Account
16:11	Saved log files from Process Monitor
16:13	Shut down VM

## Dropbox

Time	Action/Variable
7/16/13 9:45	Powered on VM
9:50	Downloaded Dropbox
9:51	Ran Process Monitor
9:51	Ran Dropbox setup
9:53	Filtered Process Monitor by the Dropbox PIDs
9:56	Went through Dropbox installer
9:58	Dropbox finished installing and I closed the window
10:01	Saved the results from Process Monitor
10:04	Shutdown VM
7/22/13 8:39	Powered on VM
8:41	Started process monitor and filtered by the Dropbox process PID
8:50	Going through Dropbox set up
8:51	Clicked next->next->install->next->skip tour->finish
9:04	Shutdown VM
7/26/13 8:18	Powered on VM
8:25	Logged into Dropbox application
8:26	Started process monitor and filtered by the Dropbox process PID
8:06	Copied the dataset files to the VM
8:32	Moved 5 files from the dataset folder to the Dropbox folder
8:38	Saved log files from Process Monitor

8:38	Opened Chrome
8:39	Went to dropbox.com
8:39	Logged in
8:43	Dragged 4 files from the data set folder to the browser
8:45	Saved Process Monitor logs
8:47	Shut down VM
7/29/13 8:07	Powered on VM
8:08	Started process monitor and filtered by the Dropbox process PID
8:18	Created "cm folder" on Dropbox
8:39	Moved "Turtle.jpg" to "cm folder"
8:44	Copied "Plan.docx" to "cm folder"
9:27	Shut down VM
9:34	Powered on VM
9:36	Started process monitor and filtered by the Dropbox process PID
9:40	Opened "wildlife.wmv" in Dropbox folder
9:43	Shut down VM
9:53	Powered on VM
9:56	Started process monitor and filtered by the Dropbox process PID
10:05	Deleted "WinPcap_4_1_2.exe" from dropbox folder
10:09	Deleted "Getting Started.pdf" from dropbox.com
10:31	Shut down VM
11:00	Powered on VM
11:05	Started process monitor and filtered by the Dropbox process PID
11:19	Unlinked Dropbox account through application
11:36	Shut down VM
12:56	Powered on VM
13:00	Started process monitor and filtered by the Dropbox process PID
13:04	Uninstalling Dropbox
13:04	Dropbox uninstalled
13:06	Shut down VM

**Google Drive**

Time	Action/Variable
------	-----------------

7/16/13 14:02	Downloaded Google Drive
14:03	Ran Process Monitor
14:03	Ran Google Drive setup
14:04	Started process monitor and filtered by the Google Drive process PID
14:05	Google Drive finished installing
14:13	Saved the results from Process Monitor
14:15	Shutdown VM
7/30/13 9:32	Powered on VM
9:33	Started Google Drive
9:34	Signed into Google Drive
9:36	Started process monitor and filtered by the Google Drive process PID
9:37	Clicked next->start sync
9:38	Dropbox synced
9:56	Copied over dataset to VM
10:28	Copied 5 files from the dataset folder to the Google Drive folder locate under my username.
10:52	Saved log files from Process Monitor
10:55	Opened Chrome
10:56	Went to drive.google.com and logged in
10:59	Dragged 4 files from the data set folder to the browser
11:18	Shut down VM
7/31/13 9:01	Powered on VM
9:02	Started process monitor and filtered by the Google Drive process PID
9:07	Created a “cm folder” on Google Drive
9:08	Moved “cloudservices.rtf” to “cm folder”
9:18	Copied a “blogs.zip” to “cm folder”
9:28	Shutdown VM
9:52	Powered on VM
9:53	Started process monitor and filtered by the Google Drive process PID
10:15	Opened “Best Coast – The Only Place.mp3” in GD folder
10:23	Opened “wildlife.wmv” in GD folder
10:24	Shut down VM
10:31	Powered on VM
10:33	Started process monitor and filtered by the Google Drive process PID
10:35	Deleted “WinPcap_4_1_2.exe” from GD folder

10:40	Deleted "Plan.docx" from GD.com
10:42	Shut down VM
11:04	Started VM
11:06	Started process monitor and filtered by the Google Drive process PID
11:06	Unlinked Google Drive account through application
11:11	Shut down VM
11:26	Powered on VM
11:28	Started process monitor and filtered by the Google Drive process PID
11:29	Uninstalling Google Drive
11:29	Google Drive uninstalled
11:32	Shut down VM

## Appendix B

### SkyDrive

Turtle.jpg

- Found in unallocated space
  - 0071049
- Found in allocated space
  - \$Recycle.Bin/S-1-5-21-3492179394-1578300877-160631371-1000/\$RUDSTO2.csv
  - pagefile.sys
  - \$Recycle.Bin/S-1-5-21-3492179394-1578300877-160631371-1000/\$RI4LWB8.csv
  - \$Recycle.Bin/S-1-5-21-3492179394-1578300877-160631371-1000/\$RHH9I59.csv
  - Users/nmurray/AppData/Local/Microsoft/SkyDrive/logs/WIN-0BEK5AK8E2S.dev=0.2013-07-22.1023.1532-1.log
  - Users/nmurray/AppData/Local/Microsoft/SkyDrive/logs/WIN-0BEK5AK8E2S.dev=0.2013-08-05.1342.1452-1.log
  - \$Recycle.Bin/S-1-5-21-3492179394-1578300877-160631371-1000/\$RVZ9NEN.csv
  - \$MFT
  - \$Recycle.Bin/S-1-5-21-3492179394-1578300877-160631371-1000/\$RAKFFNG.csv
  - \$Recycle.Bin/S-1-5-21-3492179394-1578300877-160631371-1000/\$RF88HZX.csv
  - Users/nmurray/AppData/Local/Google/Chrome/User Data/Default/Cache/data\_1
  - Users/nmurray/AppData/Local/Google/Chrome/User Data/Default/Cache/data\_3
  - Users/nmurray/AppData/Local/Microsoft/SkyDrive/logs/SyncDiagnostics.log
  - Users/nmurray/AppData/Roaming/Microsoft/Windows/Recent/Turtle.lnk
  - \$Recycle.Bin/S-1-5-21-3492179394-1578300877-160631371-1000/\$R7KXHV3.csv
  - \$Recycle.Bin/S-1-5-21-3492179394-1578300877-160631371-1000/\$R9QC4XQ.csv
  - \$Recycle.Bin/S-1-5-21-3492179394-1578300877-160631371-1000/\$RDR8Y57.csv

- \$Recycle.Bin/S-1-5-21-3492179394-1578300877-160631371-1000/\$RPCUJNQ.csv
- \$Recycle.Bin/S-1-5-21-3492179394-1578300877-160631371-1000/\$RT2O978.csv
- \$Recycle.Bin/S-1-5-21-3492179394-1578300877-160631371-1000/\$RWIWU17.csv
- Users/nmurray/AppData/Local/Microsoft/History/History.IE5/index.dat
- Users/nmurray/AppData/Local/Microsoft/History/History.IE5/MSHist012013080220130803/index.dat
- Users/nmurray/AppData/Local/Microsoft/History/History.IE5/index.dat/entry #00045
- Users/nmurray/AppData/Local/Microsoft/History/History.IE5/MSHist012013080220130803/index.dat/entry #00000

### Wildlife.wmv

-Found in unallocated space

- 0071049

- Found in allocated space

- pagefile.sys
- Users/nmurray/AppData/Local/Microsoft/SkyDrive/logs/WIN-0BEK5AK8E2S.dev=0.2013-07-22.1023.1532-1.log
- \$Recycle.Bin/S-1-5-21-3492179394-1578300877-160631371-1000/\$RI4LWB8.csv
- \$Recycle.Bin/S-1-5-21-3492179394-1578300877-160631371-1000/\$RHH9I59.csv
- \$Recycle.Bin/S-1-5-21-3492179394-1578300877-160631371-1000/\$RUDSTO2.csv
- Users/nmurray/AppData/Local/Microsoft/SkyDrive/logs/WIN-0BEK5AK8E2S.dev=0.2013-08-05.1342.1452-1.log
- \$Recycle.Bin/S-1-5-21-3492179394-1578300877-160631371-1000/\$RVZ9NEN.csv
- \$MFT
- \$Recycle.Bin/S-1-5-21-3492179394-1578300877-160631371-1000/\$RAKFFNG.csv
- \$Recycle.Bin/S-1-5-21-3492179394-1578300877-160631371-1000/\$RF88HZX.csv
- Users/nmurray/AppData/Local/Microsoft/SkyDrive/logs/SyncDiagnostics.log
- \$Recycle.Bin/S-1-5-21-3492179394-1578300877-160631371-1000/\$R7KXHV3.csv
- \$Recycle.Bin/S-1-5-21-3492179394-1578300877-160631371-1000/\$R9QC4XQ.csv
- \$Recycle.Bin/S-1-5-21-3492179394-1578300877-160631371-1000/\$RDR8Y57.csv
- \$Recycle.Bin/S-1-5-21-3492179394-1578300877-160631371-1000/\$RPCUJNQ.csv
- \$Recycle.Bin/S-1-5-21-3492179394-1578300877-160631371-1000/\$RT2O978.csv
- \$Recycle.Bin/S-1-5-21-3492179394-1578300877-160631371-1000/\$RWIWU17.csv
- Users/nmurray/AppData/Local/Google/Chrome/User Data/Default/Cache/data\_1
- Users/nmurray/AppData/Local/Google/Chrome/User Data/Default/Cache/data\_3

### Dropbox

#### GettingStarted.pdf

- None found in unallocated space

- None found directly in allocated space

- For GettingStarted.pdf it said that it was deleted, but I was still able to view the pdf. The name of the document was now Getting Started (deleted e8e9f5e1ece9b19af69596f25b4fb39).pdf
- pagefile.sys

**WinPcap\_4\_1\_2.exe**

- Found in unallocated space
  - 1400229 (Deleted Image Only)
  - 0042851 (Unlinked Image Only)
  - 1988814 (Uninstalled Image Only)
- Found in allocated space
  - pagefile.sys

**Google Drive****WinPcap\_4\_1\_2.exe**

- Found in unallocated space
  - 2527568 (Uninstalled Image Only)
  - 3444093
  - 0012438, 0807322, 3462303 (Unlinked Image Only)
  - 0163109 (Deleted Image Only)
  - /Users/nmyrray/AppData/Local/Microsoft/Media Player/Sync Playlist/en-US/00157A1/08\_Video\_rated\_at\_4\_or\_5\_starts.wpl.FileSlack
  - Users/nmurray/AppData/Local/Temp/\_MEI16762/wxmsw294u\_webview.vc90.dll.FileSlack
- Found in allocated space
  - pagefile.sys
  - \$Recycle.Bin/S-1-5-21-3492179394-1578300877-160631371-1000/\$RBT82LG.csv
  - \$Recycle.Bin/S-1-5-21-3492179394-1578300877-160631371-1000/\$R38TOPG.csv
  - \$Recycle.Bin/S-1-5-21-3492179394-1578300877-160631371-1000/\$R0J80YI.csv
  - \$Recycle.Bin/S-1-5-21-3492179394-1578300877-160631371-1000/\$R71YJQD.csv
  - \$Recycle.Bin/S-1-5-21-3492179394-1578300877-160631371-1000/\$R9CQ29T.csv
  - \$Recycle.Bin/S-1-5-21-3492179394-1578300877-160631371-1000/\$R0J80YI.csv
  - \$Recycle.Bin/S-1-5-21-3492179394-1578300877-160631371-1000/\$R7L7OVL.csv
  - \$Recycle.Bin/S-1-5-21-3492179394-1578300877-160631371-1000/\$RR0Qy8M.csv
  - \$Recycle.Bin/S-1-5-21-3492179394-1578300877-160631371-1000/\$RZMADBD.csv
  - Users/nmurray/AppData/Local/Microsoft/Windows/UsrClass.dat

**Plan.docx**

- Found in unallocated space
  - 0050263, 2527568 (Uninstalled Image Only)
  - 0163109 (Deleted Image Only)
  - 0207322 (Unlinked Image Only)
  - 3444093, 3462303
  - Users/nmurray/AppData/Local/Temp/\_MEI16762/wxmsw294u\_webview.vc90.dll.FileSlack
- Found in allocated space
  - pagefile.sys
  - Config.Msi/24091.rbf
  - \$Recycle.Bin/S-1-5-21-3492179394-1578300877-160631371-1000/\$RBT82LG.csv

- \$Recycle.Bin/S-1-5-21-3492179394-1578300877-160631371-1000/\$R38TOPG.csv
- \$Recycle.Bin/S-1-5-21-3492179394-1578300877-160631371-1000/\$R0J80YI.csv
- \$Recycle.Bin/S-1-5-21-3492179394-1578300877-160631371-1000/\$R71YJQD.csv
- \$Recycle.Bin/S-1-5-21-3492179394-1578300877-160631371-1000/\$R9CQ29T.csv
- \$Recycle.Bin/S-1-5-21-3492179394-1578300877-160631371-1000/\$R0J80YI.csv
- \$Recycle.Bin/S-1-5-21-3492179394-1578300877-160631371-1000/\$R7L7OVL.csv
- \$Recycle.Bin/S-1-5-21-3492179394-1578300877-160631371-1000/\$RR0Qy8M.csv
- \$Recycle.Bin/S-1-5-21-3492179394-1578300877-160631371-1000/\$RZMADBD.csv

## References

- Cruz, X. (2012, November 5). The Basics of Cloud Forensics. *CloudTimes*. Retrieved from <http://cloudtimes.org/2012/11/05/the-basics-of-cloud-forensics/>
- Digital evidence. (2012). *NCFS*. Retrieved from [http://www.ncfs.org/digital\\_evd.html](http://www.ncfs.org/digital_evd.html)
- Linthicum, D. (2013, March 15). The ticking time bomb known as cloud forensics. *InfoWorld*. Retrieved from <http://www.infoworld.com/d/cloud-computing/the-ticking-time-bomb-known-cloud-forensics-214229>
- Messmer, E. (2013, March 6). Cloud forensics: In a lawsuit, can your cloud provider get key evidence you need? *Network World*. Retrieved from <http://www.networkworld.com/news/2013/030613-cloud-forensics-267447.html>
- Understanding metadata* [PDF]. (2004). Bethesda, MD: NISO Press.
- Zimmerman, S., & Glavach, D. (2011, Winter). Cyber forensics in the cloud. *IAnewsletter*, 14, 4-7.



## Digital forensics using Autopsy in Windows

Autopsy Download Link: <https://www.autopsy.com/>

Before we begin the lab, make sure you downloaded the images and NSRL Files that were in the “Lab Resources” link. If you want to confirm that you had no corruption, these are the MD5 values of the files:

- MD5 (device1\_laptop.e01) = dc176d653c5613e305e831525e874090
- MD5 (device2\_mediocard.e01) = c8343d3976eec2985e7580a2b6321591

### **Step 01**

1. Launch Autopsy
2. Choose “Create New Case”
3. Make a case with the following information:
  1. Case Name: cfir1
  2. Base Directory: c:\ (or where ever you'd like to store the case)
  3. Skip case number and examiner
4. Add “device1\_laptop.e01” image as the data source.
5. Deselect ALL ingest modules.
6. Finish Adding Image.
7. Open the “Data Sources” part of the left-hand tree
  1. **Question:** How many volumes does the disk image have?
  2. **Question:** What is the name of the unallocated space file in vol1?
  3. **Question:** Right-click on vol7 and choose “File System Details”. What file system is in vol7?
8. In Windows, open “C:\cfir1” in a file explorer and observe its contents.
  1. Question: What is the database called?
  2. Question: Roughly how big is the database (in megabytes)?



## **Step 02**

Keep the same case open that you created in the last section. Let's look at the data in the tree.

1. Question: By extension, how many databases are there?
2. Question: What is the size of the largest database?
3. Question: Are there any databases by MIME type yet?

Question: What are the names of the files between 200MB and 1GB in size?

## **Step 03**

We are now going to begin analyzing the laptop. We are starting off the case with some clues. Most notably, we have pictures that were sent with the ransom emails to Basis Technology

1. Keep the same case open from the previous lab, or reopen the case ("cfir1").
2. Right-click on device1\_laptop.e01 image in the tree and choose "Run Ingest Modules"
3. Disable all modules except the following:
  1. Hash Lookup
  2. File Type Identification
  3. Extension Mismatch Detector
  4. Embedded File Extractor
  5. Picture Analyzer
  6. Email Parser
4. Configure the Hash Lookup module with two hash sets:
  1. Import the NSRL File ([NSRLComplete.txt-md5.idx](#)) that you previously downloaded in Lab 09 Resources.
    1. You may need to unzip the file you downloaded.
    2. You can use the default values (i.e. Type: [Known](#)).
  2. Create a New Hash Set:
    - Destination: [Local](#)
    - Name: [Ransom Case](#)
    - Hash Set Path: [Any folder on your computer]
    - Type: [Notable](#)
  3. Use the "Add Hashes to Hash Set" button to copy and paste the following MD5 value into the "Ransom Case" hash set. This is the hash of the ransom note.  
[07c94320f4e41291f855d450f68c8c5b](#)
  5. Start the Ingest Modules.



6. Observe:
1. Use Ingest Inbox as an indicator when ‘Known Bad’ hash hits are found.
  2. Use “Go To Result” to go to the tree area of hash hits.
  3. View the hash hit.
  4. Question: Let ingest at least 15% through the drive. How many total hits are found under the “Hashset Hits” results after running the Hash Lookup Ingest Module?
  5. Question: What are the filenames of the hash hits?
  6. One of the hits is in a folder named “Pictures”. Right-click on the file to “View” there.
  7. Question: How many total ".jpg" files are in the folder “Pictures” where the notable hash hit was found?
  8. While reviewing the images in that folder, it is noticed that “IMG\_20191024\_155744.jpg”, We want to tag this as Notable:
    1. Right-click on it
    2. Select “Add File Tag” and choose “Notable Item”

#### **Step 04**

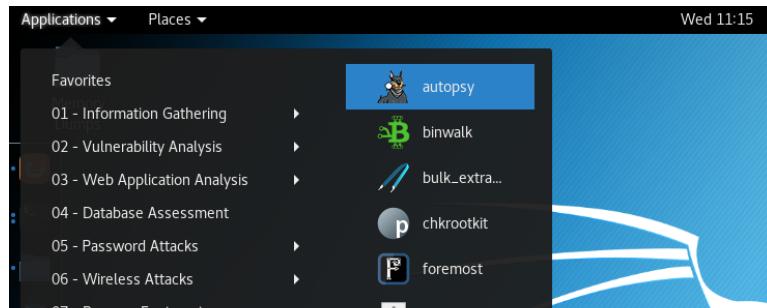
1. Question: Under the “EXIF Metadata” results, how many photos were taken with the following devices?
  1. iPhone 7 Plus?
  2. Samsung Galaxy S8?
  3. BLU R1 HD?
2. From the “Views” area, find the archive file that is named “Archive.zip”.
  1. Go to the original directory (Right-click -> View File In Directory).
  2. Double click on it to go into it.
  3. Question: What is the MIME type listed for the file “D3D11\_Default.shader-db.bin”?
  4. Question: What is the file size for the file “D3D11\_Default.shader-db.bin”?
3. Question: Are there extension mismatch results?
4. Question: What are some common file types with unexpected extensions?
5. Run ingest again with only the Interesting Files module enabled.
  1. Create an Interesting File Set named “Encryption”. With two rules that match files named “veracrypt.exe” or “truecrypt.exe”.
  2. Question: Was VeraCrypt or TrueCrypt found on the system?



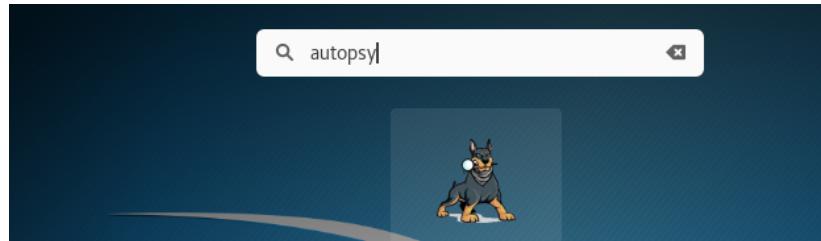
## Digital forensics using Autopsy

### Starting Autopsy

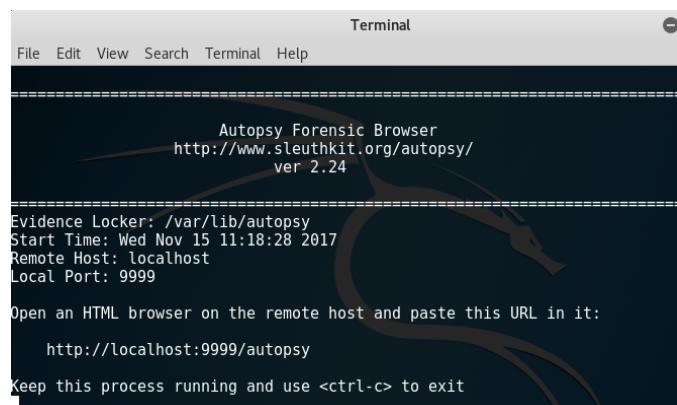
An autopsy can be started in two ways. The first use the Applications menu by clicking on Applications



Or you can click on the Show applications icon (last item in the side menu) and type autopsy into the search bar at the top-middle of the screen and then click on the autopsy icon:

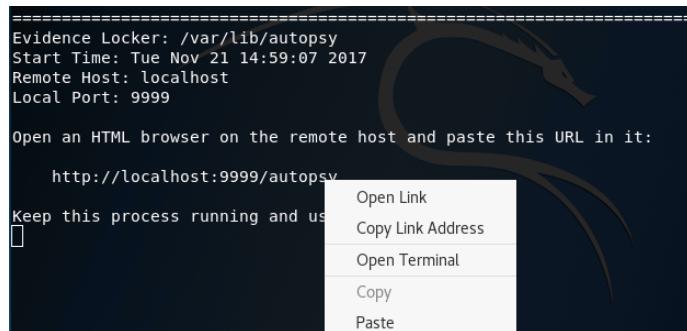


Once the autopsy icon is clicked, a new terminal is opened showing the program information along with connection details for opening The Autopsy Forensic Browser.





To open the Autopsy browser, position the mouse over the link in the terminal, then right-click and choose Open Link, as seen in the following screenshot:



### Creating a new case

To create a new case, follow the given steps:

1. When the Autopsy Forensic Browser opens, investigators are presented with three options.
2. Click on **NEW CASE**:



3. Enter details for the Case Name, Description, and Investigator Names. For the Case Name, I've entered **SP-8-dft**, as it closely matches the image name **(8-jpeg-search.dd)**, which we will be using for this investigation. Once all information is entered, click **NEW CASE**:



Image Download Link: <http://dftt.sourceforge.net/>

**CREATE A NEW CASE**

1. **Case Name:** The name of this investigation. It can contain only letters, numbers, and symbols.

2. **Description:** An optional, one line description of this case.

3. **Investigator Names:** The optional names (with no spaces) of the investigators for this case.

a. <input type="text" value="Shiva Parasram"/>	b. <input type="text"/>
c. <input type="text"/>	d. <input type="text"/>
e. <input type="text"/>	f. <input type="text"/>
g. <input type="text"/>	h. <input type="text"/>
i. <input type="text"/>	j. <input type="text"/>

**NEW CASE**    **CANCEL**    **HELP**

The locations of the Case directory and Configuration file are displayed and shown as created. It's important to take note of the case directory location, as seen in the screenshot: Case directory (`/var/lib/autopsy/SP-8-dftt/`) created. Click **ADD HOST** to continue:

**Creating Case: SP-8-dftt**

Case directory (`/var/lib/autopsy/SP-8-dftt/`) created  
Configuration file (`/var/lib/autopsy/SP-8-dftt/case.aut`) created

We must now create a host for this case.

**ADD HOST**

4. Enter the details for the Host Name (name of the computer being investigated) and the Description of the host.



5. Optional settings:

- **Time zone**
- **Timeskew Adjustment**
- **Path of Alert Hash Database**
- **Path of Ignore Hash Database**

A screenshot of a software interface titled 'Add Host'. The dialog box has a yellow background and contains six numbered configuration fields.1. **Host Name:** A text input field containing 'host1'.2. **Description:** A text input field containing '10 MB NTFS'.3. **Time zone:** A dropdown menu currently showing a placeholder icon.4. **Timeskew Adjustment:** A text input field containing '0'.5. **Path of Alert Hash Database:** A text input field containing a placeholder icon.6. **Path of Ignore Hash Database:** A text input field containing a placeholder icon. At the bottom of the dialog box are three buttons: 'ADD HOST' (highlighted in yellow), 'CANCEL', and 'HELP'.

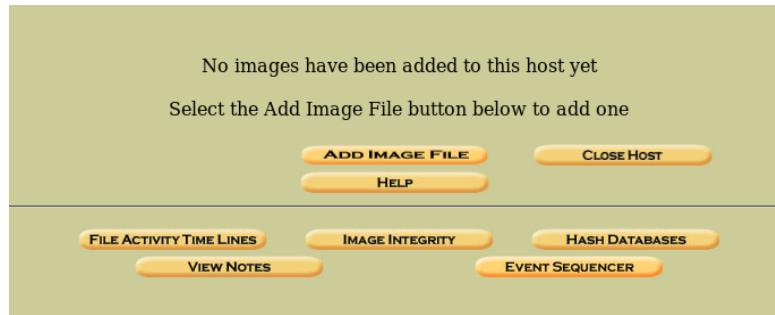
6. Click on the **ADD HOST** button to continue.
7. Once the host is added and directories are created, we add the forensic image we want to analyze by clicking the **ADD IMAGE** button:



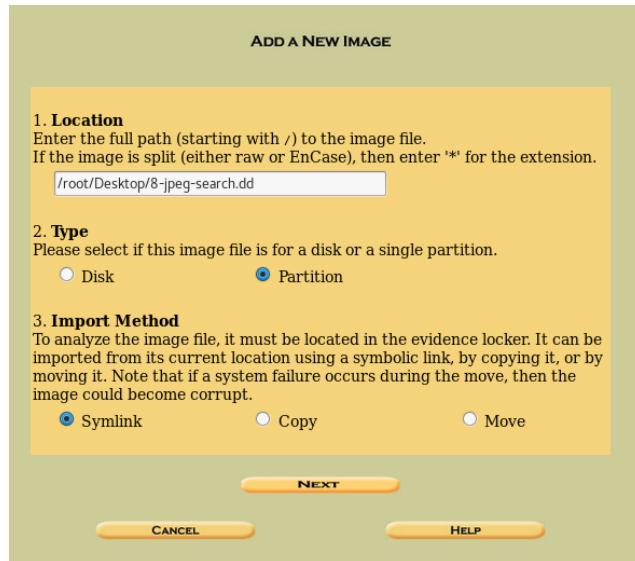
**Sri Lanka Institute of Information Technology**  
**Cyber Forensics and Incident Response**  
**Master of Science in Information Technology – Cyber Security**



8. Click on the **ADD IMAGE FILE** button to add the image file:



9. To import the image for analysis, the full path must be specified. On my machine, I've saved the image file (8-jpeg-search.dd) to the Desktop folder. As such, the location of the file would be **/root/Desktop/ 8-jpeg-search.dd**.



10. If you are presented with the following error message, ensure that the specified image location is correct and that the forward-slash (/) is used:

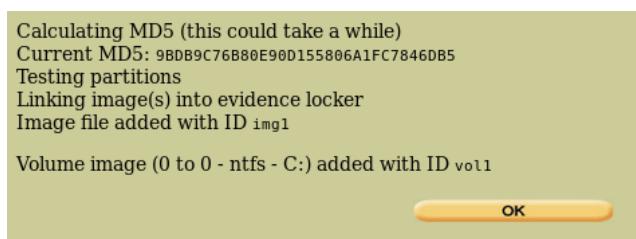
Invalid wild image (img\_path) argument



11. Upon clicking **Next**, the Image File Details are displayed. To verify the integrity of the file, select the radio button to Calculate the hash value for this image, and select the checkbox next to Verify hash after importing?
12. The File System Details section also shows that the image is of a ntfs partition.
13. Click on the **ADD** button to continue:

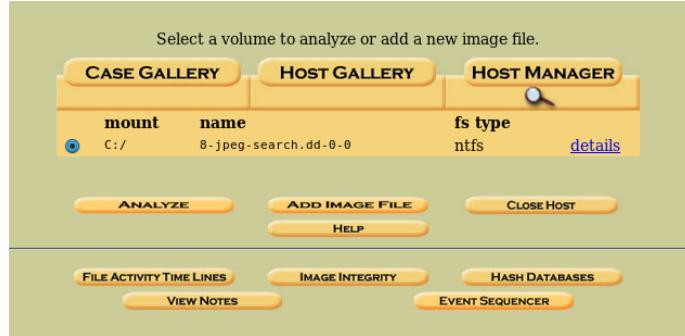
A screenshot of the Autopsy software interface. The top section is titled "Image File Details". It shows the local name "images/8-jpeg-search.dd" and a note about data integrity using MD5 hash. There are three radio button options: "Ignore the hash value for this image." (unchecked), "Calculate the hash value for this image." (checked), and "Add the following MD5 hash value for this image:" (unchecked). Below these is a text input field and a checked checkbox "Verify hash after importing?". The bottom section is titled "File System Details". It shows an analysis of partitions, specifically "Partition 1 (Type: ntfs)" with a mount point of "C:" and a file system type of "ntfs". At the bottom are three buttons: "ADD" (highlighted in yellow), "CANCEL", and "HELP".

14. After clicking the **ADD** button in the previous screenshot, Autopsy calculates the MD5 hash and links the image into the evidence locker. Press **OK** to continue:

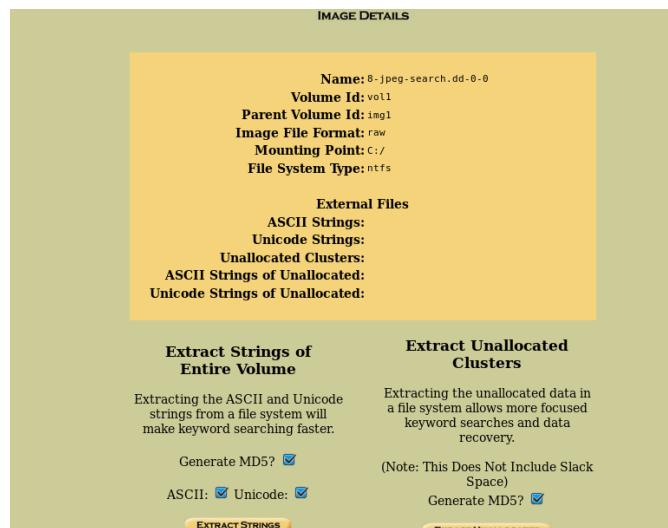




15. At this point, we're just about ready to analyze the image file. If there are multiple cases listed in the gallery area from any previous investigations you may have worked on, be sure to choose the 8-jpeg-search.dd file and case:

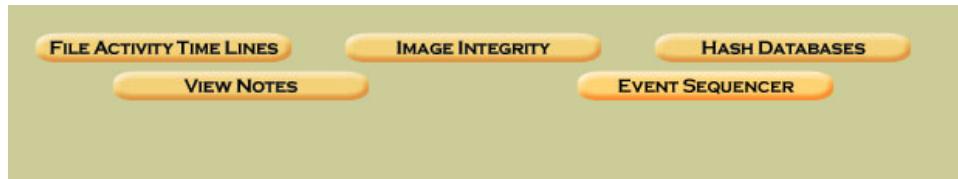


16. Before proceeding, we can click on the **IMAGE DETAILS** option. This screen gives details such as the image name, volume ID, file format, file system, and also allows for the extraction of ASCII, Unicode, and unallocated data to enhance and provide faster keyword searches. Click on the back button in the browser to return to the previous menu and continue with the analysis:





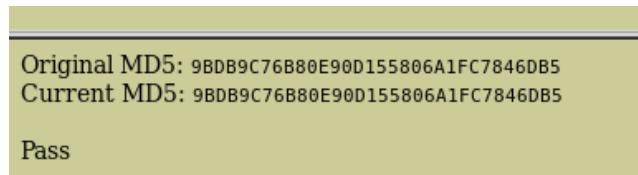
17. Before clicking on the **ANALYZE** button to start our investigation and analysis, we can also verify the integrity of the image by creating an MD5 hash, by clicking on the **IMAGE INTEGRITY** button:



18. After clicking on the **IMAGE INTEGRITY** button, the image name and hash are displayed. Click on the **VALIDATE** button to validate the MD5 hash:

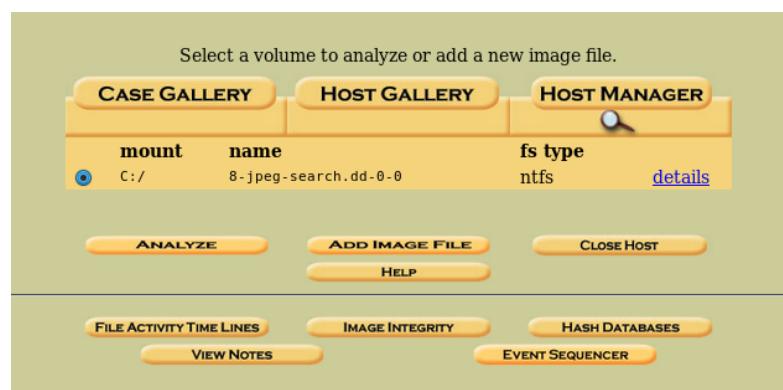


19. The validation results are displayed in the lower-left corner of the Autopsy browser window:



20. We can see that our validation was successful, with matching MD5 hashes displayed in the results. Click on the **CLOSE** button to continue.

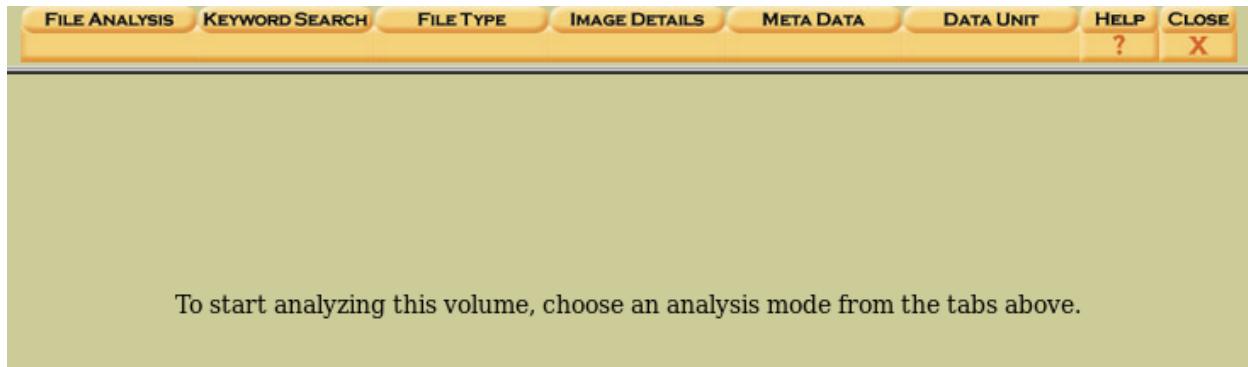
21. To begin our analysis, we click on the **ANALYZE** button:



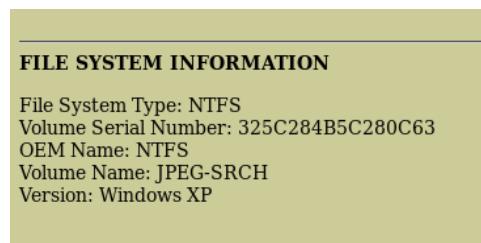


### Analysis using Autopsy

- After clicking on the **ANALYZE** button (see the previous screenshot), we're presented with several options in the form of tabs, with which to begin our investigation:



- Let's look at the details of the image by clicking on the **IMAGE DETAILS** tab. In the following snippet, we can see the Volume Serial Number and the operating system (Version) listed as Windows XP:



- Next, we click on the **FILE ANALYSIS** tab. This mode opens into File Browsing Mode, which allows the examination of directories and files within the image. Directories within the image are listed by default in the main view area:

FILE ANALYSIS										
		Type	Path	Last Modified	Created	Accessed	Size	MD5	SHA1	SHA256
<b>Directory Seek</b>		r / r	\$Secure:\$SDS	2004-06-09	2004-06-09	2004-06-09	263784	0	0	9-128-
Enter the name of a directory that you want to view. C:/		r / r	\$Secure:\$SI	2004-06-09	2004-06-09	2004-06-09	408	0	0	9-144-
		r / r	\$UpCase	2004-06-09	2004-06-09	2004-06-09	131072	0	0	10-128-
		r / r	\$Volume	2004-06-09	2004-06-09	2004-06-09	0	48	0	3-128-
		d / d	.	2004-06-09	2004-06-09	2004-06-09	56	48	0	5-144-
		d / d	_alloc_	2004-06-09	2004-06-09	2004-06-09	256	0	0	27-144
		d / d	archive/	2004-06-09	2004-06-09	2004-06-09	472	0	0	37-144

**File Browsing Mode**

In this mode, you can view file and directory contents.

File contents will be shown in this window.  
More file details can be found using the Metadata link at the end of the list (on the right).  
You can also sort the files using the column headers

**Sri Lanka Institute of Information Technology**  
**Cyber Forensics and Incident Response**  
**Master of Science in Information Technology – Cyber Security**



In File Browsing Mode, directories are listed with the Current Directory specified as C:/.

For each directory and file, there are fields showing when the item was WRITTEN, ACCESSED, CHANGED, and CREATED, along with its size and META data:

Current Directory: C:/										
		<a href="#">ADD NOTE</a>		<a href="#">GENERATE MD5 LIST OF FILES</a>						
DEL	Type dir / ln	NAME	WRITTEN	ACCESSED	CHANGED	CREATED	SIZE	UID	GID	META
	r / r	<a href="#">\$AttrDef</a>	2004-06-09 23:22:22 (EDT)	2004-06-09 23:22:22 (EDT)	2004-06-09 23:22:22 (EDT)	2004-06-09 23:22:22 (EDT)	2560	48	0	<a href="#">4-128-4</a>
	r / r	<a href="#">\$BadClus</a>	2004-06-09 23:22:22 (EDT)	2004-06-09 23:22:22 (EDT)	2004-06-09 23:22:22 (EDT)	2004-06-09 23:22:22 (EDT)	0	0	0	<a href="#">8-128-2</a>
	r / r	<a href="#">\$BadClus:\$Bad</a>	2004-06-09 23:22:22 (EDT)	2004-06-09 23:22:22 (EDT)	2004-06-09 23:22:22 (EDT)	2004-06-09 23:22:22 (EDT)	10289152	0	0	<a href="#">8-128-1</a>
	r / r	<a href="#">\$Bitmap</a>	2004-06-09 23:22:22 (EDT)	2004-06-09 23:22:22 (EDT)	2004-06-09 23:22:22 (EDT)	2004-06-09 23:22:22 (EDT)	2512	0	0	<a href="#">6-128-1</a>
	r / r	<a href="#">\$Boot</a>	2004-06-09	2004-06-09	2004-06-09	2004-06-09	8192	48	0	<a href="#">7-128-1</a>

For integrity purposes, MD5 hashes of all files can be made by clicking on the GENERATE MD5 LIST OF FILES button.

4. Investigators can also make notes about files, times, anomalies, and so on, by clicking on the ADD NOTE button:

**Enter a note for C:/del2/file7.hmm (31-128-3):**

A note works like a bookmark and allows you to later find this data more easily.

Add a Standard Note  
 Error parsing 'ils' output

5. The left pane contains four main features that we will be using:

- **Directory Seek**
- **File Name Search**
- **ALL DELETED FILES**
- **EXPAND DIRECTORIES**



<b>Directory Seek</b>
Enter the name of a directory that you want to view.
C:/
<input type="text"/>
<b>VIEW</b>
<b>File Name Search</b>
Enter a Perl regular expression for the file names you want to find.
<input type="text"/>
<b>SEARCH</b>
<b>ALL DELETED FILES</b>
<b>EXPAND DIRECTORIES</b>

6. By clicking on **EXPAND DIRECTORIES**, all contents are easily viewable and accessible within the left pane and main window. The + next to a directory indicates that it can be further expanded to view subdirectories (++) and their contents:

<input type="text"/> <b>SEARCH</b> <hr/> <b>ALL DELETED FILES</b> <hr/> <b>HIDE DIRECTORIES</b> <hr/> C:/ +/\$Extend +/alloc +/archive +/del1 +/del2 +/invalid +/_misc +/_RECYCLER ++/_S-1-5-21-175798 +/_System Volume Information +/_OrphanFiles	d / d <u>_</u> 2004-06-09 23:29:18 (EDT) r / r <u>file11.dat</u> 2004-06-10 03:44:46 (EDT) r / r <u>file12.doc</u> 2004-06-10 03:20:58 (EDT) r / r <u>file13.dll</u> 2004-06-09 23:29:45 (EDT)
---	---

More file details can be viewed by clicking on the file names.

**Sri Lanka Institute of Information Technology**  
**Cyber Forensics and Incident Response**  
**Master of Science in Information Technology – Cyber Security**



7. To view deleted files, we click on the **ALL DELETED FILES** button in the left pane. Deleted files are marked in red and also adhere to the same format of **WRITTEN**, **ACCESSED**, **CHANGED**, and **CREATED** times.

All Deleted Files										
Type dir / in	NAME	WRITTEN	ACCESSED	CHANGED	CREATED	SIZE	UID	GID	META	
- / r	C:/dell/ file6.jpg	2004-06-10 02:48:08 (EDT)	2004-06-09 23:28:00 (EDT)	2004-06-09 23:28:00 (EDT)	2004-06-09 23:28:00 (EDT)	175630	0	0	32-128-3	
- / r	C:/del2/ file7.hmm	2004-06-10 02:49:18 (EDT)	2004-06-09 23:43:38 (EDT)	2004-06-09 23:43:44 (EDT)	2004-06-09 23:28:00 (EDT)	326859	0	0	31-128-3	

8. We can also view more information about this file by clicking on its **META** entry. By viewing the metadata entries of a file (last column to the right), we can also view the hexadecimal entries for the file, which may give the true file extensions, even if the extension was changed.

In the preceding screenshot, the second deleted file (**file7.hmm**) has a peculiar file extension of **.hmm**.

9. Click on the **META** entry (31-128-3) to view the metadata:

```
$FILE_NAME Attribute Values:  

Flags: Archive  

Name: file7.hmm  

Parent MFT Entry: 47 Sequence: 1  

Allocated Size: 327168 Actual Size: 326859  

Created: 2004-06-09 23:28:00.742657600 (EDT)  

File Modified: 2004-06-10 02:49:18.000000000 (EDT)  

MFT Modified: 2004-06-09 23:28:00.842801600 (EDT)  

Accessed: 2004-06-09 23:28:00.842801600 (EDT)

Attributes:  

$STANDARD_INFORMATION (16-0) Name: N/A Resident size: 72  

$FILE_NAME (48-4) Name: N/A Resident size: 84  

$DATA (128-3) Name: N/A Non-Resident size: 326859 init_size: 326859  

1066 1067 1068 1069 1070 1071 1072 1073  

1074 1075 1076 1077 1078 1079 1080 1081  

1082 1083 1084 1085 1086 1087 1088 1089  

1090 1091 1092 1093 1094 1095 1096 1097  

1098 1099 1100 1101 1102 1103 1104 1105  

1106 1107 1108 1109 1110 1111 1112 1113  

1114 1115 1116 1117 1118 1119 1120 1121  

1122 1123 1124 1125 1126 1127 1128 1129  

1130 1131 1132 1133 1134 1135 1136 1137
```



10. Under the Attributes section, click on the first cluster labelled 1066 to view header information of the file:

3

**Cluster: 1066**  
**Status: Not Allocated**

ASCII Contents of Cluster 1066 in 8-jpeg-search.dd-0-0

```
.....JFIF.....C.....}.....!1A..Qa."q.2....#B...R..$3br.
.....%&' ()*456789:CDEFGHIJKLMNOPQRSTUVWXYZcdefghijklmnopqrstuvwxyz.....w.....!1..AQ.aq."2...B....      #3R..br.
.$4.%.....&' ()*456789:CDEFGHI
```

We can see that the first entry is **JFIF**, which is an abbreviation for **JPEG File Interchange Format**. This means that the file7.hmm file is an image file but had its extension changed to .hmm.

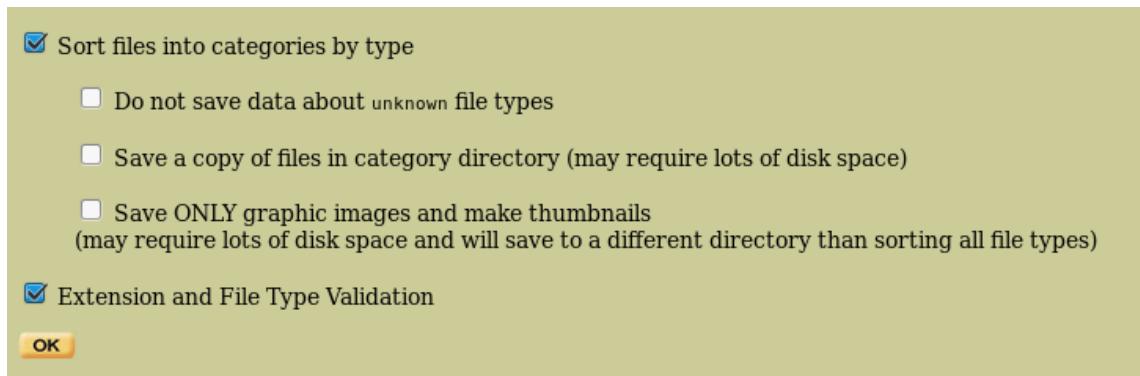
### Sorting files

1. Inspecting the metadata of each file may not be practical with large evidence files. For such an instance, the **FILE TYPE** feature can be used. This feature allows for the examination of existing (allocated), deleted (unallocated), and hidden files. Click on the **FILE TYPE** tab to continue:

A screenshot of the Autopsy digital forensics tool's "File Type Sorting" interface. The top navigation bar includes tabs for FILE ANALYSIS, KEYWORD SEARCH, FILE TYPE (which is highlighted in yellow), IMAGE DETAILS, META DATA, DATA UNIT, HELP, and CLOSE. Below the tabs, the title "File Type Sorting" is displayed. A descriptive text states: "In this mode, Autopsy will examine allocated and unallocated files and sort them into categories and verify the extension." Another line of text says: "This allows you to find a file based on its type and find 'hidden' files." A warning message at the bottom reads: "WARNING: This can be a time intensive process." There is also a magnifying glass icon on the toolbar.



2. Click **Sort files into categories by type** (leave the default-checked options as they are) and then click **OK** to begin the sorting process:



3. Once sorting is complete, a results summary is displayed. In the following snippet, we can see that there are five Extension Mismatches:

Extensions	
• Extension Mismatches (5)	
Categories (31)	
• archive (2)	
• audio (0)	
• compress (1)	
• crypto (0)	
• data (14)	
• disk (1)	
• documents (1)	
• exec (0)	
• images (6)	
• system (0)	
• text (2)	
• unknown (4)	
• video (0)	

4. To view the sorted files, we must manually browse to the location of the output folder, as Autopsy 2.4 does not support viewing sorted files. To reveal this location, click on **View Sorted Files** in the left pane:





The output folder locations will vary depending on the information specified by the user when first creating the case, but can usually be found at `/var/lib/autopsy/<case name>/<host name>/output/sorter-vol#/index.html`.

Once the `index.html` file has been opened, click on the **Extension Mismatch** link:

<b>Extension Mismatch</b>	
C:/alloc/file2.dat	JPEG image data, JFIF standard 1.01, aspect ratio, density 1x1, segment length 16, baseline, precision 8, 437x365, frames 3 (Ext: dat) Image: /var/lib/autopsy/SP-8-dft/11/images/8-jpeg-search.dd Inode: 28-128-3
C:/archive/file9.boo	gzip ERROR: Exec `gzip' failed, No such file or directory (Zip archive data, at least v2.0 to extract) (Ext: boo) Image: /var/lib/autopsy/SP-8-dft/11/images/8-jpeg-search.dd Inode: 40-128-3
C:/del2/file7.hmm	JPEG image data, JFIF standard 1.01, aspect ratio, density 1x1, segment length 16, baseline, precision 8, 698x752, frames 3 (Ext: hmm) Image: /var/lib/autopsy/SP-8-dft/11/images/8-jpeg-search.dd Inode: 31-128-3
C:/invalid/file3.jpg	ASCII text (Ext: jpg) Image: /var/lib/autopsy/SP-8-dft/11/images/8-jpeg-search.dd Inode: 35-128-3
C:/misc/file13.dll:here	JPEG image data, JFIF standard 1.01, aspect ratio, density 1x1, segment length 16, baseline, precision 8, 518x563, frames 3 (Ext: dll:here) Image: /var/lib/autopsy/SP-8-dft/11/images/8-jpeg-search.dd Inode: 44-128-5

The five listed files with mismatched extensions should be further examined by viewing metadata content, with notes added by the investigator.

### Reopening cases in Autopsy

1. Cases are usually ongoing and can easily be restarted by starting Autopsy and clicking on **OPEN CASE**
2. In the **CASE GALLERY**, be sure to choose the correct case name and, from there, continue your examination

The image shows two screenshots of the Autopsy Forensic Browser interface. The left screenshot shows the main dashboard with a cartoon dog icon and links for 'OPEN CASE', 'NEW CASE', and 'HELP'. The URL <http://www.sleuthkit.org/autopsy/> is displayed at the bottom. The right screenshot shows the 'CASE GALLERY' tab selected, displaying a list of cases with columns for Name, Description, and 'details' links. The cases listed are: 321 (None Provided), 001-Forensic-Jo (Autopsy Acquisition), FA-010 (Autopsy Acquisition), and df (None Provided).

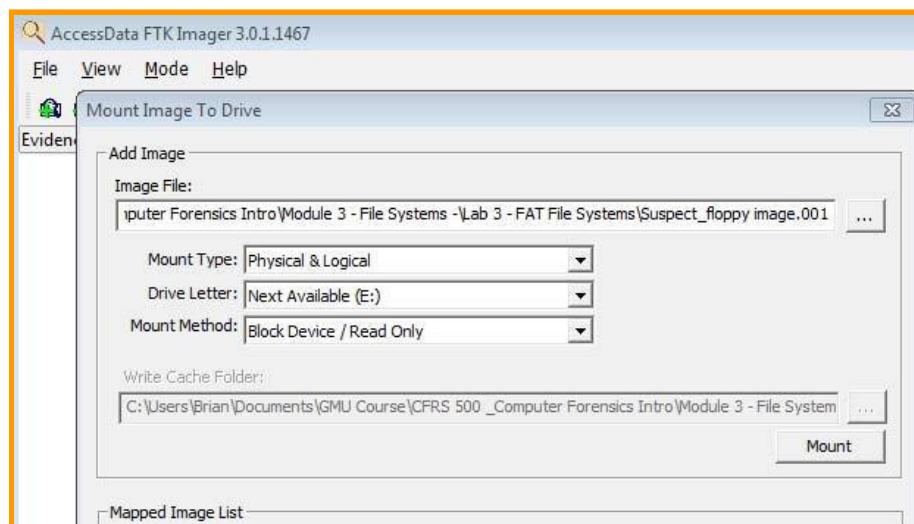
Name	Description	<a href="#">details</a>
321	None Provided	<a href="#">details</a>
001-Forensic-Jo	Autopsy Acquisition	<a href="#">details</a>
FA-010	Autopsy Acquisition	<a href="#">details</a>
df	None Provided	<a href="#">details</a>



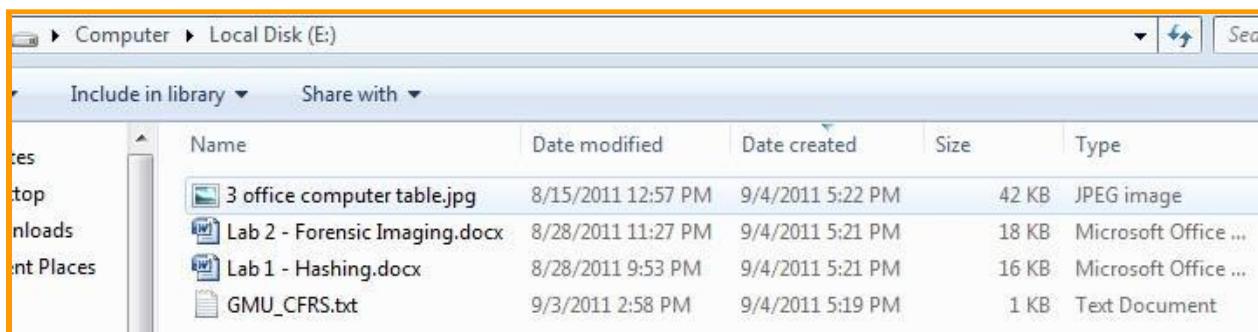
## **Deleted File Recovery**

### **Objectives:**

- Use a hex editor to manually recover a deleted file from a FAT12 image file.
  - Use FTK Imager to mount images and view deleted files.
1. Install and/or open **FTK Imager 3.01**
  2. Select **File > Image Mounting...**
  3. Add the image file "**Suspect\_floppy image.001**", do not change the default options, and click "**Mount**".



4. Go to Windows Explorer and open the "E:" Drive. This is the mounted version of the suspect image. Note the files that are currently on the image.





5. Open the Hex Editor “HxD”.
6. Select “Extras > Open Disk Image...” and open “Suspect\_floppy image - Copy.001”.  
 You are looking at Sector 0, the FAT Boot sector for the floppy image. Note that the file system “FAT12” is clearly shown.

```

HxD - [C:\Users\Brian\Documents\GMU Course\CFRS 500 _Computer Forensics Intro\Module 3 - File Systems -\Lab 3 - FAT File Syst
File Edit Search View Analysis Extras Window ?
File 16 ANSI dec Sector 0 of 2880
Suspect_floppy image - Copy.001
Offset(d) 00 01 02 03 04 05 06 07 08 09 10 11 12 13 14 15
00000000 EB 3C 90 4D 53 44 4F 53 35 2E 30 00 02 01 01 00 <.MSDOS5.0.... Sector 0
00000016 02 E0 00 40 0B F0 09 00 12 00 02 00 00 00 00 00 .à.ø. .....
00000032 00 00 00 00 00 00 29 6E EA 75 A0 4E 4F 20 4E 41 .....nêu NO NA
00000048 4D 45 20 20 20 46 41 54 31 32 20 20 20 33 C9 ME FAT12 3É
00000064 8E D1 BC F0 7B 8E D9 B8 00 20 8E C0 FC BD 00 7C Zñgð(ZÙ,. ZÀùë.|_
00000080 38 4E 24 7D 24 8B C1 99 E8 3C 01 72 1C 83 EB 3A 8N$}S<Ámë<.r.fë:
00000096 66 A1 1C 7C 26 66 3B 07 26 8A 57 FC 75 06 80 CA fí.|sf.;.ëSWùu.ëÈ
00000112 02 88 56 02 80 C3 10 73 EB 33 C9 8A 46 10 98 F7 .“V.ëA.së3ÉSF.”+
00000128 66 16 03 46 1C 13 56 1E 03 46 0E 13 D1 8B 76 11 F..F..V..F..Ñ<v.
00000144 60 89 46 FC 89 56 FE B8 20 00 F7 E6 8B 5E 0B 03 `tFütVp. .æ<^..
00000160 C3 48 F7 F3 01 46 FC 11 4E FE 61 BF 00 00 E8 E6 ÄH÷6.Fü.Npaç..ëæ
00000176 00 72 39 26 38 2D 74 17 60 B1 0B BE A1 7D F3 A6 .r9&8-t.‘t.%}ó|
00000192 61 74 32 4F 74 09 83 C7 20 3B FR 72 F6 FR DC A0 at2Nr.fC :ØræëÜ

```

7. Select “View > Offset Base” and change it to Decimal.
8. Go to Sector 19. This is the beginning of the File Allocation Table (FAT). It stores file metadata, such as size, created time, modified time, and filename abd file’s physical location on the drive.
9. Partially into sector 20, you will see a file that starts with the hex E5 sigma character. This indicates a deleted file. In a FAT file system, the first character of a deleted file is replaced with hex E5 (sigma) and the location of the file is set to zero, thus marking it as available.

```

Suspect_floppy image - Copy.001
Offset(d) 00 01 02 03 04 05 06 07 08 09 10 11 12 13 14 15
00010224 FF FF FF FF FF FF FF FF 00 00 FF FF FF FF yyyy-yyyy-yyyy-yyyy
00010240 02 73 00 69 00 63 00 20 00 49 00 0F 00 F8 6D 00 .s.i.c. .I...em. Sector 20
00010256 61 00 67 00 69 00 6E 00 67 00 00 00 2E 00 64 00 a.g.i.n.g....d.
00010272 01 4C 00 61 00 62 00 20 00 32 00 0F 00 F8 20 00 .L.a.b. .2...ø .
00010288 2D 00 20 00 46 00 6F 00 72 00 00 00 65 00 6E 00 -. .F.o.r....e.n.
00010304 4C 41 42 32 2D 46 7E 31 44 4F 43 20 00 B7 AB 8A LAB2-F~1DOC .«š
00010320 24 3F 24 3F 00 00 65 BB 1C 3F 23 00 DD 46 00 00 $?$.e».?#.ÝF..
00010336 43 67 00 00 00 FF FF FF FF FF FF 00 92 FF FF Cg...yyyyyy..’yy
00010352 FF FF FF FF FF FF FF FF FF 00 0F FF FF FF FF yyyy-yyyy-yyyy-yyyy
00010368 02 75 00 74 00 65 00 72 00 20 00 0F 00 92 74 00 .u.t.e.r. ...’t.
00010384 61 00 62 00 6C 00 65 00 2E 00 00 00 6A 00 70 00 a.b.l.e....j.p.
00010400 01 33 00 20 00 6F 00 66 00 66 00 0F 00 92 69 00 .3. .o.f.f...’i.
00010416 63 00 65 00 20 00 63 00 6F 00 00 00 6D 00 70 00 c.e. .c.o...m.p.
00010432 33 4F 46 46 49 43 7E 31 4A 50 47 20 00 52 D9 8A 3OFFIC~1JPG .RÙš
00010448 24 3F 24 3F 00 00 21 67 0F 3F 47 00 5C A6 00 00 $?$.e».g.?G.\!..
00010464 E5 4F 4D 42 20 20 20 54 58 54 20 18 99 69 8E åOMB TXT .”ic
00010480 24 3F 24 3F 00 00 65 BB 24 3F 9B 00 71 03 00 00 $?$.e».$.q...
00010496 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
00010512 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....

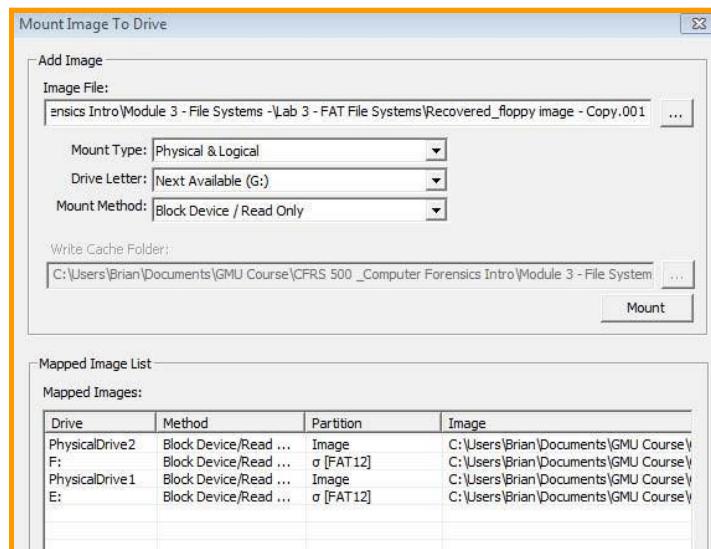
```



10. Select the E5 character and replace it with a “B”.

11. Select “File > Save As” and save this file with the name “Recovered\_floppy image.001”.

12. Return to FTK Imager, use the Mounting utility to mount the “Recovered\_floppy image.001” the same as you mounted the original image.



13. Open the F: drive in Windows Explorer. Note the files that are now on the image.

**\*\*NOTE: The new file “bomb.txt” is now visible with all of its metadata. However, the physical location of the file is still zeroed in the FAT table. So we will not be able to actually open this file.\*\***

File library		Share with			
Name	Date created	Date modified	Size	Type	
3 office computer table.jpg	9/4/2011 5:22 PM	8/15/2011 12:57 PM	42 KB	JPEG image	
bomb.txt	9/4/2011 5:27 PM	9/4/2011 5:27 PM	1 KB	Text Document	
GMU_CFRS.txt	9/4/2011 5:19 PM	9/3/2011 2:58 PM	1 KB	Text Document	
Lab 1 - Hashing.docx	9/4/2011 5:21 PM	8/28/2011 9:53 PM	16 KB	Microsoft Office ...	
Lab 2 - Forensic Imaging.docx	9/4/2011 5:21 PM	8/28/2011 11:27 PM	18 KB	Microsoft Office ...	



14. Return to FTK Imager and close the image mounting utility.
15. Select “File>Add Evidence Item”.
16. Select “Image File” and browse to the “Recovered\_floppy image.001” file and click finish.
17. FTK imager automatically recovers the deleted file’s location and displays it. Look in the root folder for the image contents.

A screenshot of the AccessData FTK Imager software interface. The window title is "AccessData FTK Imager 3.0.1.1467".  
**Evidence Tree:** Shows a tree structure of the mounted image. The root node is "Recovered\_floppy image - Copy.001" (FAT12). It contains a folder "[root]" and an "unallocated space" node.  
**File List:** A table showing recovered files:

Name	Size	Type	Date Modified
3 office computer tabl...	42 KB	Regular File	8/15/2011 12:5...
bomb.txt	1 KB	Regular File	9/4/2011 5:27:1...
GMU_CFRS.TXT	1 KB	Regular File	9/3/2011 2:58:0...
Lab 1 - Hashing.docx	16 KB	Regular File	8/28/2011 9:53:...
Lab 2 - Forensic Imagi...	18 KB	Regular File	8/28/2011 11:2...

  
**Custom Content Sources:** A pane showing "Evidence:File System|Path|File".  
**Hex Editor:** A large pane at the bottom showing the raw hex and ASCII data of the "bomb.txt" file. The ASCII text reads:

The bomb is located in the trash can on 5th and Madison street. It will explode at exactly noon on Saturday. This is an even political dissident! -Sincerely, Jim Smith -jsmith@bombermail.com



## **Event Log Analysis**

### **Objectives:**

- **Use Access Data's FTK Imager to locate and export Windows Event Log Files.**
- **Use Event Log Explorer to Examine the Event Logs and identify information relevant to this investigation.**
- **Understand the general contents of Windows Event Logs.**

1. Open / Install **Access Data's FTK Imager 3**
2. **Select File > Add Evidence Item > Select Image File > Browse** to the Suspect image and add it.
3. Navigate to the Windows System Event Logs. They are in **C:\Windows\System32\Config**. Export the three event logs (**AppEvent.evt, SecEvent.evt, & SysEvent.evt**) to a new directory.
4. Open / Install **Event Log Explorer (elex\_setup.exe)**.
5. **Select File > Open Log File > Direct >** Select the log files that you exported from the suspect image. (Open all 3 log files)
6. Examine the SecEvent.Evt and answer the following questions:
  - a. What user profile was logged on **4/13/2014 at 1:46:08PM**? What type of logon was it?
  - b. When was the user profile **“Tiny\_Tim”** created?



7. Examine the SysEvent.Evt log and answer the following questions:
  - a. What occurred on 4/6/2014 at 6:51:47PM and how could it be relevant to your investigation?
  - b. We are concerned that the remote desktop tool, VNC, may have been used in this attack. Does the System Event log provide any indication of this?
  
8. Examine the AppEvent.Evt log and answer the following questions:
  - a. Does the application event log provide any further indications of how VNC was used in this attack and where the source of the attack may have come from?

# Recycle Bin Analysis

# Recycle Bin in Windows XP

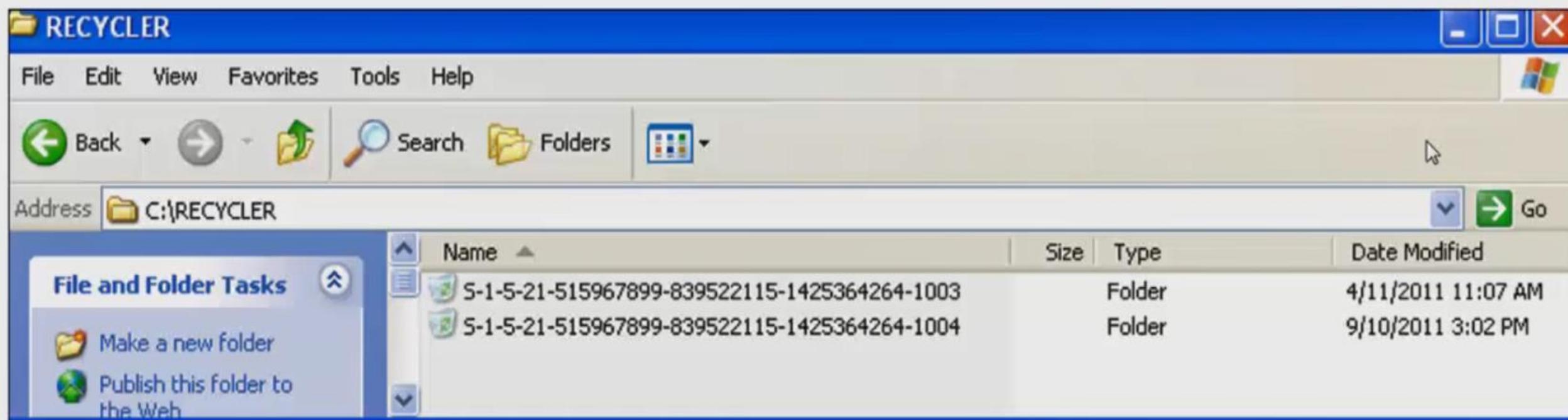
- When a file is deleted and sent to the recycle bin, the following occurs:
  - The file's original MFT entry is deleted.
  - A new MFT entry is made for the file, now in the Recycle Bin.
  - The new file is renamed according to this convention:  
**D[original drive letter][index number].[original extension]**
  - A new entry is made for the file in the INFO2 file
  - Examples would be:
    - DC12.doc
    - DE14.exe

# The INFO2 File in Windows XP

- The Recycle Bin displays the original file name to the user; this information is taken from the INFO2 file.
- The INFO2 file is the Recycle Bin's database containing:
  - The file's original file name and path (entered twice, in both ASCII & Unicode)
  - The date and time of deletion
  - The index number.
- The Index.dat entry is 800 bytes in length.

# Recycle Bin Attribution

- Upon deletion, a file sent to the recycle bin is automatically placed in a subfolder named by the user's SID.
- Tying the SID to a username allows for attribution of who deleted the file.



# Recycle Bin Bypass

- Be aware, there are ways for users to delete files and never use the Recycle Bin.
  - Pressing the shift key while deleting a file is a command for permanent deletion.
  - NukeOnDelete option in the registry will cause all deleted files to bypass the recycle bin.
    - Located at:  
**HKLM\Software\Microsoft\CurrentVersion\Explorer\BitBucket**

# Vista & 7 \$Recycle.Bin

- No longer using the INFO2 file
- Renamed Recycle Bin to **\$Recycle.Bin**
- INFO2 information is stored in a new, individually created index file.
  - There is one index file for each deleted file.
  - Naming Convention: **I[6 character GUID].bin**
- Deleted file is named the same as its partner index file, except it starts with “R”.
- Example names of deleted Index and deleted file:
  - **\$RZO16QK.bin** (deleted file)
  - **\$IZO16QK.bin** (Index File)
- Both files still exist in a subfolder bearing the SID of the user who deleted them.

# 24 Hours @ A Security Operations Centre

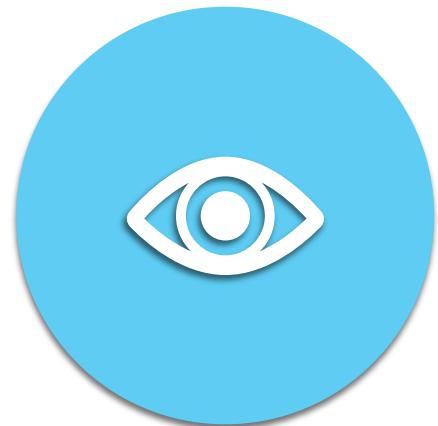
By Thilini Wijewardhana

*Head of Security Operations & Technology  
@ CryptoGen*

9<sup>th</sup> May 2021



# SECURITY OPERATIONS CENTRE



**DETECT**



**ANALYZE**



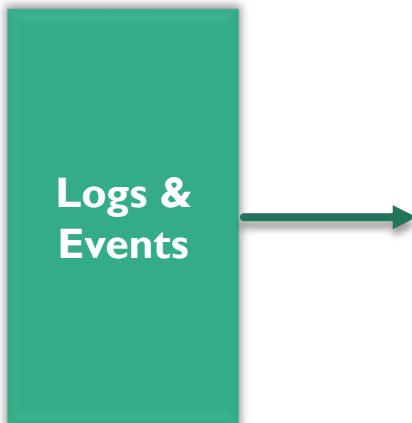
**RESPOND**

# TYPES OF SOC Models



- Internal SOC is owned and managed by the company
- Internal SOC provides more visibility , Control and expensive to establish and manage.
  
- Managed SOC Service (SOC as a Service) is an outsourced SOC,
- Managed SOC Service is cheaper to operate, may have access to advance security tools and technical experts, but less control and visibility.
  
- Mostly Use by Governments or large organizations , Provides Much more visibility.

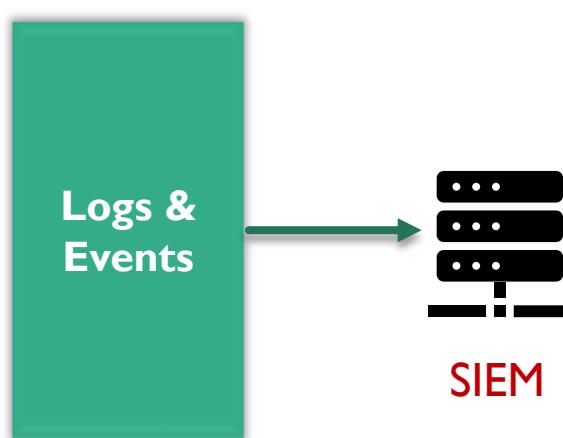
# WHAT HAPPENS IN A 24\*7 SOC



Log Sources examples

1. Windows Logs ( System/Application/Security)
  2. Linux system logs
  3. Cloud platform Logs
  4. Database logs
  5. Firewall Logs
  6. EDR(Endpoint Detection and Response) Logs
  7. WAF (Web Application Firewall) Logs
- .....

# WHAT HAPPENS IN A 24\*7 SOC



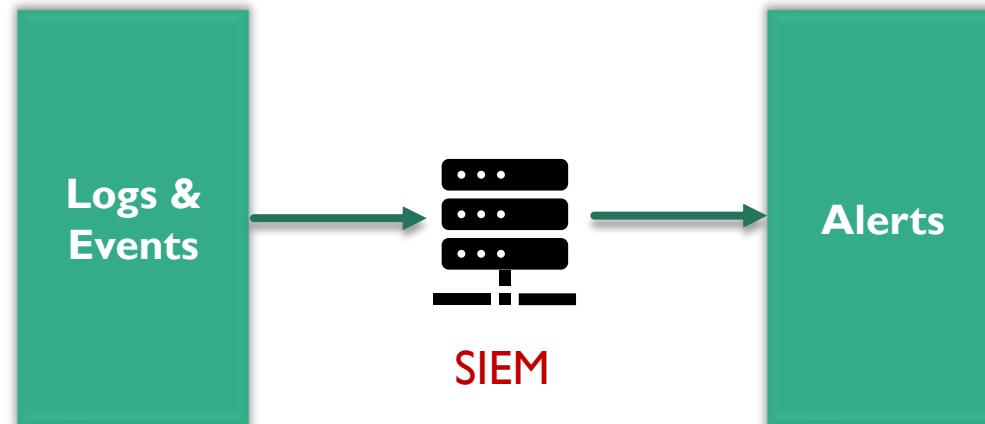
## Security Information and Event Management (**SIEM**)

- Collects data from log sources, stores, aggregates, applies analytics, detect threats, enable to analyze alerts, generate reports.

# SIEM EXAMPLES



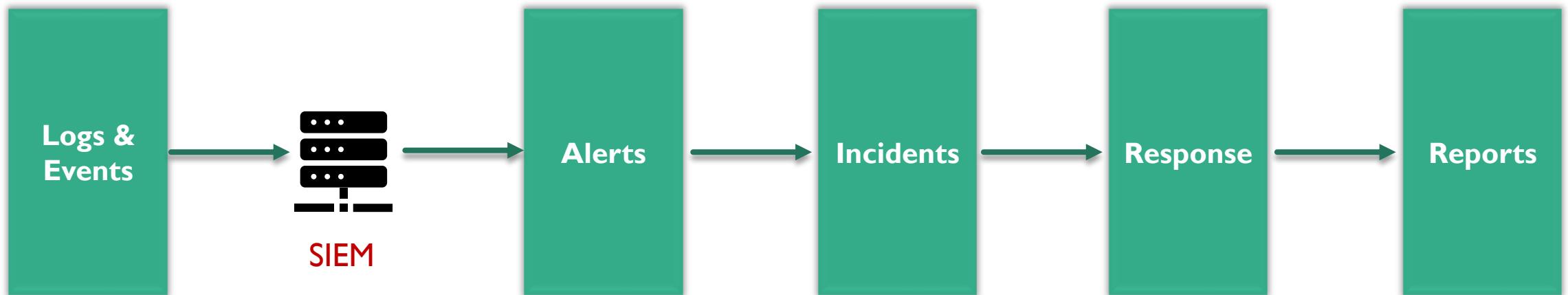
# WHAT HAPPENS IN A 24\*7 SOC



## Sample Alerts/Alarms

- External Brute Force Attempts
- Multiple account passwords modified by Admin
- Account added to Admin group
- Blacklisted Application Detected
- Large Outbound File Transfer
- SQL Injection Attempt
- Port Scan attempt

# WHAT HAPPENS IN A 24\*7 SOC



# WHAT HAPPENS IN A 24\*7 SOC

8 OR 12 Hour Shift

Client Relationship

Reports

Threat Advisory Alerts

SIEM

Shift Handover  
Form



Asset Onboarding

New Use Case

Event Analysis

Ticketing System

Threat Feeds

Security Dashboards

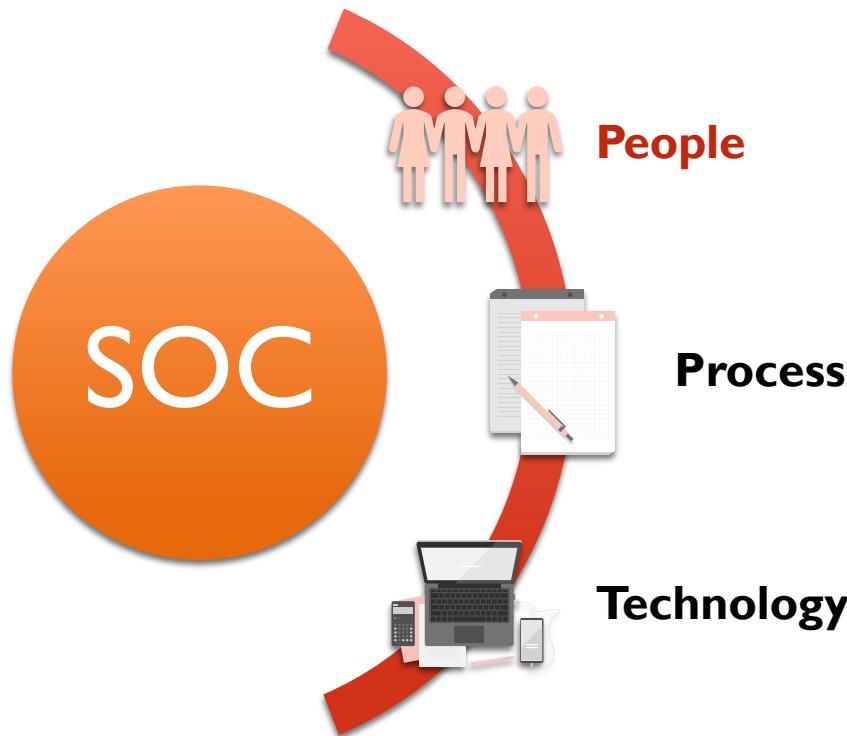
Incident Escalation

Use Case Finetune

Information Requests

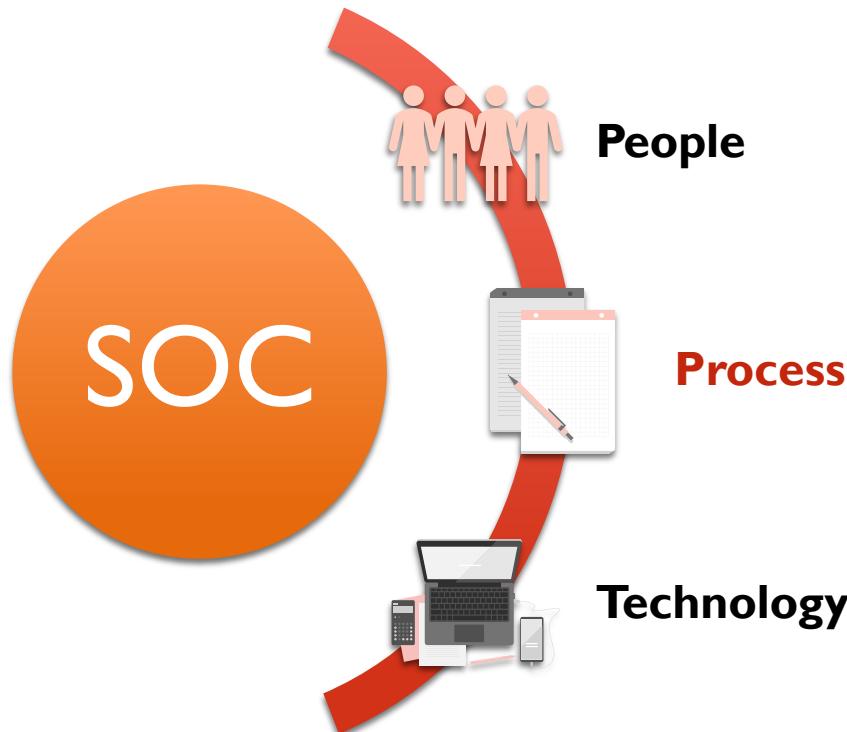
Incident Follow Up

# SOC COMPONENTS



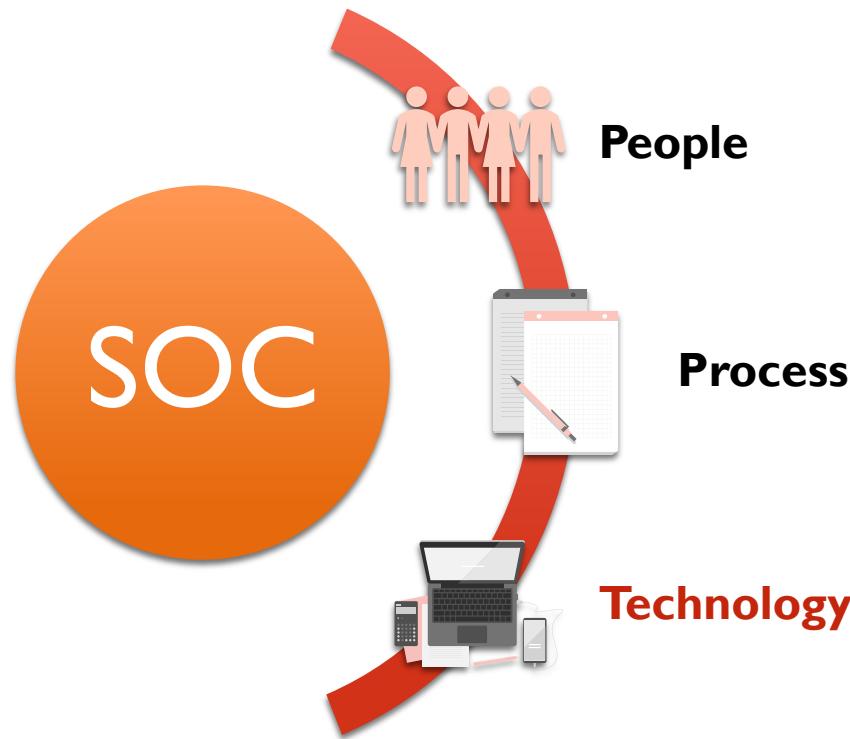
- Security Analysts
- Threat Intelligence Team
- SIEM Engineers
- Incident Responder
- Red Team
- Management

# SOC COMPONENTS



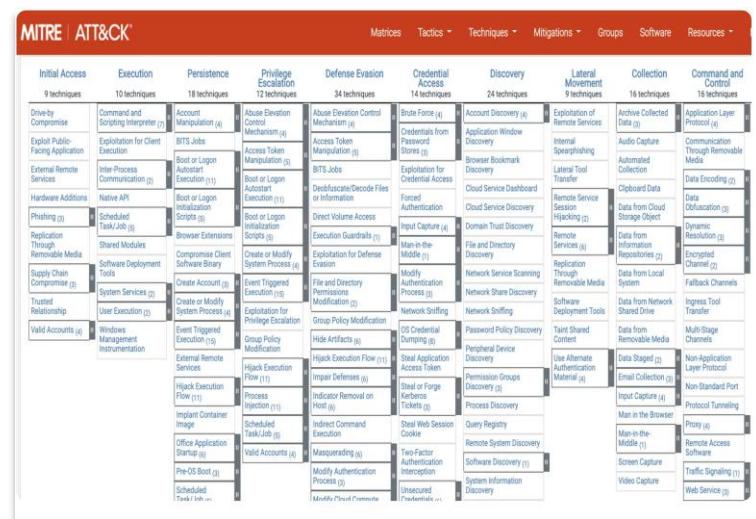
- Asset Management Process
- Use Case Management Process
- Event Monitoring and Incident Management Process
- Threat Intelligence Process
- Incident Response Playbooks

# SOC COMPONENTS



- SIEM
- Security monitoring Dashboards
- Threat Feeds
- Security Testing Tools
- Ticketing System

# FRAMEWORKS AND STANDARDS





THANK YOU

# ACCESSDATA SUPPLEMENTAL APPENDIX

## Registry Quick Find Chart

---

**Important:** At the time of this writing, most of the information contained in this paper is not published by Microsoft and is based on personal research. As such, please consider validating these results prior to relying on them as the basis for any conclusions. Please keep in mind that, as with all Windows artifact behavior, the information contained in this paper is subject to change at any time. In addition to the conditions stated below, there may be additional user actions that may contribute to these entries.

---

This appendix reviews common locations in the Windows and Windows Internet-related registries where you can find data of forensic interest.

- *NTUSER.DAT Information* on page 2
- *SAM Information* on page 19
- *SECURITY Information* on page 21
- *SOFTWARE Information* on page 21
- *SYSTEM Information* on page 28

---

**Note:** Under the Version column, an “XP” indicates that this information is found in XP. A “V” references Vista, and a “7” references Windows 7 in its first release. If no notation is made in the Version column, it means this was found in XP, but not tested in other versions.

---

## NTUSER.DAT INFORMATION

Information	File	Location	Description	When Updated	Version
Access 2007 MRU	NTUSER.DAT	NTUSER.DAT\Software\Microsoft\Office\12.0\Access\Settings	MRU list for MS Access Database files (MRU1-MRU9).	When database is closed	Office 2007
Access 2007 MRU Dates	NTUSER.DAT	NTUSER.DAT\Software\Microsoft\Office\12.0\Access\Settings	Tracks date of last access associated with MRU1-9 (MRUDate1-MRUDate9).	When database is closed	Office 2007
Access Recent Databases	NTUSER.DAT	NTUSER.DAT\Software\Microsoft\office\version\ Common\Open Find\ Microsoft Office Access\Settings\File New Database\File Name MRU	Microsoft Access* recent databases in the “value” value.	Immediately	Pre Office 2007
Adobe	NTUSER.DAT	NTUSER.DAT\Software\Adobe\*	Lists Adobe products such as Acrobat* and FrameMaker*.		
AIM	NTUSER.DAT	NTUSER.DAT\Software\America Online\AOL InstantMessenger\ CurrentVersion\Users\username	Lists IM contacts, file transfer information, etc.	Immediately	
AIM Away Messages	NTUSER.DAT	NTUSER.DAT\Software\America Online\AOL Instant Messenger(TM)\ CurrentVersion\Users\screen name\IAmGoneList	Shows default and customized Away messages.	Immediately	
AIM File Transfers & Sharing	NTUSER.DAT	NTUSER.DAT\Software\America Online\AOL Instant Messenger\ CurrentVersion\Users\screen name\Xfer	Shows settings for file transfers and sharing.	Immediately	

Information	File	Location	Description	When Updated	Version
AIM Last User	NTUSER.DAT	NTUSER.DAT\Software\America Online\AOL Instant Messenger (TM)\CurrentVersion\Login - Screen Name	Shows the screen name of the last logged-in user.	At login	
AIM Profile Info	NTUSER.DAT	NTUSER.DAT\Software\America Online\AOL Instant Messenger\CurrentVersion\Users\screen name\DirEntry	Shows user profile information (optional).	Immediately	
AIM Recent Contacts	NTUSER.DAT	NTUSER.DAT\Software\America Online\AOL Instant Messenger\CurrentVersion\Users\username\recent IM ScreenNames	Shows a list of recently contacted buddies.	When the application closes.	
AIM Registered Users	NTUSER.DAT	NTUSER.DAT\Software\America Online\AOL Instant Messenger\CurrentVersion\Users	Shows registered AIM users on the machine.	At sign-on	
AIM Saved Buddy List	NTUSER.DAT	NTUSER.DAT\Software\America Online\AOL Instant Messenger\CurrentVersion\Users\username\Config Transport	Shows the directory path of a saved Buddy List, a BLT file.	Immediately	
Application Information	NTUSER.DAT	NTUSER.DAT\Software\%Application Name%	This class of registry keys contains the information each application stores in the registry.	NA	
Autorun USBs, CDs, DVDs	NTUSER.DAT	NTUSER.DAT\Software\Microsoft\Windows\ CurrentVersion\Explorer\AutoplayHandlers / DisableAutoplay	0=Enabled 1=Disabled	N/A	XP, V

Information	File	Location	Description	When Updated	Version
BitLocker To Go	NTUSER.DAT	NTUSER.DAT\Software\Microsoft\Windows\CurrentVersion\FveAutoUnlock<guid>	Indicates the user-selected <b>Remember a USB</b> setting to bypass entering the password on this system.	Upon selecting, recognize the drive on this machine	7
CD Burning	NTUSER.DAT	NTUSER.DAT\Software\Microsoft\Windows\CurrentVersion\Explorer\CD Burning\Drives\Volume<guid>\Current Media	May show previous CD/DVD volume names inserted under Disc Label value. Normally, removes volume name on dismount.	N/A	V, 7
CD Burning	NTUSER.DAT	NTUSER.DAT\Software\Microsoft\Windows\CurrentVersion\Explorer\CD Burning\ Current Media / Disc Label	Current Media subkey created upon mounting drive. Removed on dismount.	Upon mounting and dismounting	XP
Chat Rooms	NTUSER.DAT	NTUSER.DAT\Software\Yahoo\Pager\profiles\screen name\Chat	Shows information for chat rooms visited or created.	Immediately	
Converted Wallpaper	NTUSER.DAT	NTUSER.DAT\Control Panel\Desktop	Identifies graphics that are converted to wallpaper.	Immediately	XP, V, 7
Converted Wallpaper	NTUSER.DAT	NTUSER.DAT\Control Panel\Desktop	Identifies date and time of converted wallpaper.	Immediately	XP, V, 7
Drives mounted by user	NTUSER.DAT	NTUSER.DAT\Software\Microsoft\Windows\ CurrentVersion\Explorer\MountPoints2<guid>	Track the GUID from the MountedDevices GUID in the SYSTEM file	Immediately	XP, V, 7

Information	File	Location	Description	When Updated	Version
EFS	NTUSER.DAT	NTUSER.DAT\Software\Microsoft\Windows\CurrentVersion\EFS\CurrentKeys	Lists the current user's certificate thumbprint. (Each user has a unique certificate thumbprint.) The same certificate thumbprint is contained in the \$EFS alternate data stream for every EFS file encrypted by the current user.	NA	XP, V, 7
Excel 2007 Autosave Info	NTUSER.DAT	NTUSER.DAT\Software\Microsoft\Office\12.0\Excel\Resiliency\Document Recovery\<id#>	Saves info about currently opened Excel documents.	When document is opened and when saves are made	Office 2007
Excel 2007 MRU	NTUSER.DAT	NTUSER.DAT\Software\Microsoft\Office\12.0\Excel\File MRU	MRU List for MS Excel spreadsheets (Item1-Item50). <b>Note:</b> The 2nd bracketed number is a 64-bit date/time stamp of when the document was opened.	When document is opened	Office 2007
Excel Recent Spreadsheets	NTUSER.DAT	NTUSER.DAT\Software\Microsoft\Office\version\Common\Open Find\Microsoft Office Excel\Settings\Save As\File Name MRU	Microsoft Excel recent spreadsheets in the "value" value.	Immediately	Pre Office 2007
File Extension Associations	NTUSER.DAT	NTUSER.DAT\Software\Microsoft\Windows\CurrentVersion\Explorer\FileExts\EXT Type	Lists file extension associations and files that have been opened with the Open With command.	Immediately	XP, V, 7
File Extensions\Program Association	NTUSER.DAT	NTUSER.DAT\Software\Microsoft\Windows\CurrentVersion\Explorer\FileExts	Identifies associated programs with file extensions.	Immediately	XP, V, 7

Information	File	Location	Description	When Updated	Version
Folders - Stream MRUs	NTUSER.DAT	NTUSER.DAT\Software\Microsoft\Windows\CurrentVersion\Explorer\StreamMRU	Info on stored folders.	Immediately	XP
FTP	NTUSER.DAT	NTUSER.DAT\Software\Microsoft\FTP\Accounts\<address>	Local FTP accounts.	N/A	XP, V, 7
Google Client History	NTUSER.DAT	NTUSER.DAT\Software\Google\NavClient\1.1\History	Contains a list of search terms with date and time stamps if Google is included in the Internet Explorer task bar.	Immediately	
ICQ	NTUSER.DAT	NTUSER.DAT\Software\Mirabilis\ICQ\*	Lists IM contacts, file transfer information, etc.	NA	
ICQ Last User	NTUSER.DAT	NTUSER.DAT\Software\Mirabilis\ICQ\Owners - LastOwner	Shows the last logged-in user.	At logon	
ICQ Nickname	NTUSER.DAT	NTUSER.DAT\Software\Mirabilis\ICQ\Owners\UIN - Name	Nickname of user (optional value).	At logon	
ICQ Registered Users	NTUSER.DAT	NTUSER.DAT\Software\Mirabilis\ICQ\Owners\UIN	UIN folder is named for the user.	At logon	
IE Auto Logon and password	NTUSER.DAT	NTUSER.DAT\Software\Microsoft\Protected Storage System Provider\SID\Internet Explorer\Internet Explorer - URL: StringData	Stores IE auto logon IDs and passwords with date and time stamp.	Immediately	IE6 and below
IE Auto-Complete Passwords	NTUSER.DAT	NTUSER.DAT\Software\Microsoft\Internet Explorer\IntelliForms	Stores web page auto-complete passwords. These are encrypted values.	Immediately	IE6 and below

Information	File	Location	Description	When Updated	Version
IE Auto-Complete Web Addresses	NTUSER.DAT	NTUSER.DAT\Software\Microsoft\Protected Storage System Provider	Lists web pages wherein autocomplete was utilized.	Immediately	IE6 and below
IE Cleared Browser History on/off	NTUSER.DAT	NTUSER.DAT\Software\Microsoft\Internet Explorer\Privacy / ClearBrowserHistoryOnExit	0=Off (default) 1=On Privacy subkey appears only on first change by user.	Upon changing value in GUI	XP, V, 7
IE Default Download Directory	NTUSER.DAT	NTUSER.DAT\Software\Microsoft\Internet Explorer	Identifies the default download directory when utilizing Internet Explorer.	Immediately	All
IE Favorites List	NTUSER.DAT	NTUSER.DAT\Software\Microsoft\Windows\CurrentVersion\Explorer\MenuOrder\Favorites\<favoritesfoldername>	Lists favorites from IE Favorites drop down selector.	N/A	XP, V, 7
IE History Status	NTUSER.DAT	NTUSER.DAT\Software\Microsoft\Windows\CurrentVersion\Internet Settings\5.0\Cache\Extensible Cache\<mshistfoldernames>	Mirrors existing history folder storage hidden from the user in the history files.	N/A	XP, V, 7
IE IntelliForms	NTUSER.DAT	NTUSER.DAT\Software\Microsoft\Internet Explorer\IntelliForms	Encrypted user data in Storage1 and Storage2 (old PSSP info)		IE7 and above
IE Search Terms	NTUSER.DAT	NTUSER.DAT\Software\Miscrosoft\Protected Storage System Provider\SID\Internet Explorer\Internet Explorer - q:StringIndex	Stores IE search terms with date and time stamp.	Immediately	IE6 and below

Information	File	Location	Description	When Updated	Version
IE Settings	NTUSER.DAT	NTUSER.DAT\Software\Microsoft\Internet Explorer\ Main	Stores IE settings such as start page, save directory, home page, and download location.	Immediately	Through IE8
IE Typed URLs	NTUSER.DAT	NTUSER.DAT\Software\Microsoft\Internet Explorer\Typed URLs	Stores data entered into the URL Address Bar.	When the application closes	Through IE8
IE URL History — Days Saved	NTUSER.DAT	NTUSER.DAT\Software\Microsoft\Windows\CurrentVersion\Internet Settings\URL History - DaysToKeep	The number of days the system stores URLs visited in IE. The default is 20 days.	Immediately	Through IE8
IE Web Form Data	NTUSER.DAT	NTUSER.DAT\Software\Microsoft\Protected Storage System Provider\SID\Internet Explorer\Internet Explorer - q:StringIndex	Stores form data provided within IE.	Immediately	IE6 and below
IM Contact List	NTUSER.DAT	NTUSER.DAT\Software\Microsoft\MessengerService>ListCache\NET Messenger Service	Contains Contact, Allow, Block, and Reverse entries.	At sign-off	
IM File Sharing	NTUSER.DAT	NTUSER.DAT\Software\Microsoft\MSNMessenger\FileSharing - Autoshare	Shows if file sharing is turned on.	Immediately	
IM File Transfers	NTUSER.DAT	NTUSER.DAT\Software\Microsoft\Messenger Service - FtReceiveFolder	Shows the location of the Received Files folder.	Immediately	
IM File Transfers	NTUSER.DAT	NTUSER.DAT\Software\Microsoft\MSNMessenger\FTReceiveFolder	Shows the location of the Received Files folder.	Immediately	
IM Last User	NTUSER.DAT	NTUSER.DAT\Software\Microsoft\MessengerService>ListCache\NET Messenger Service - IdentityName	Screen name of last logged-in user.	At sign-off	

Information	File	Location	Description	When Updated	Version
IM Logging Enabled	NTUSER.DAT	NTUSER.DAT\Software\Microsoft\MSN Messenger\PerPass portSettings\#####-\ MessageLoggingEnabled	Shown if message logging is turned on.	Immediately	
IM Message History	NTUSER.DAT	NTUSER.DAT\Software\Microsoft\MSN Messenger\PerPass portSettings\#####-\ MessageLog Path	Shows the location of message history files.	Immediately	
IM MSN Messenger	NTUSER.DAT	NTUSER.DAT\Software\Microsoft MessengerService\ ListCache\NET MessengerService\*	Contains IM groups, contacts, file transfer information, etc. for MSN Messenger.	Most on signoff; however, FTReceive is immediate.	
IM Saved Contact List	NTUSER.DAT	NTUSER.DAT\Software\Microsoft\ Messenger Service - ContactListPath	Shows the location of a saved Contact List (CTT) file.	Immediately	
IMV Usage	NTUSER.DAT	NTUSER.DAT\Software\Yahoo\Pager\IMVironments (global value)	Shows usage of IMVironments.	Immediately	
IMVs MRU list	NTUSER.DAT	SNTUSER.DAT\Software\Yahoo\Pager\ profiles\screen name\IMVironments (user-specific value)	Shows usage of IMVironments.	Immediately	
Jump List on Taskbar	NTUSER.DAT	NTUSER.DAT\Software\Microsoft\ Windows\ CurrentVersion\Explorer\ Taskband / Favorites and FavoritesResolve	Shows applications pinned to the taskbar. Retains removed applications.	Upon pinning	7
Kazaa	NTUSER.DAT	NTUSER.DAT\Software\Kazaa\*	Stores configuration, search, download, IM data, etc. for Kazaa.	NA	
Map Network Drive MRU	NTUSER.DAT	NTUSER.DAT\Software\Microsoft\ Windows\CurrentVersion\Explorer\ Map Network Drive MRU	Contains a most recently used list of mapped network drives.	NA	XP, V, 7

Information	File	Location	Description	When Updated	Version
Media Player Recent List	NTUSER.DAT	NTUSER.DAT\Software\Microsoft\MediaPlayer\Player\RecentFileList	Contains the user's most recently used list for Windows Media Player.	Immediately	
MRU—Last Visited	NTUSER.DAT	NTUSER.DAT\Software\Microsoft\Windows\CurrentVersion\Explorer\ComDlg32\	Lists the application and filename of the most recent files opened in Windows.	Immediately	XP, V, 7
MRU—Open Saved	NTUSER.DAT	NTUSER.DAT\Software\Microsoft\Windows\CurrentVersion\Explorer\ComDlg32\OpenSaveMRU	Lists the filename and path of the most recent files saved or copied to a specific location in Windows.	Immediately	XP, V, 7
MRU—Recent Documents	NTUSER.DAT	NTUSER.DAT\Software\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs\	Identifies the documents in the Recent Documents list available from the Windows Start menu.	Immediately	XP, V, 7
MRU—Run MRU	NTUSER.DAT	NTUSER.DAT\Software\Microsoft\Windows\CurrentVersion\Explorer\RunMRU	Lists the most recent commands entered in the Windows Run box.	Immediately	XP, V, 7
MRUs - Common Dialog	NTUSER.DAT	NTUSER.DAT\Software\Microsoft\Windows\CurrentVersions\Explorer\ComDlg32	Last Visited=Application Used OpenSaveMRU=Recent Docs using the Microsoft Save As Dialog Box	Immediately	XP, V, 7
MUICache	NTUSER.DAT	NTUSER.DAT\Software\Microsoft\Windows\Shell\MUICache	Tracks the opening of executable files by the operating system. <b>Note:</b> In Windows 7, MUICache moved from NTUSER.DAT to HKCR\LocalSettings\MuiCache.	Immediately	V
MUICache - XP	NTUSER.DAT	NTUSER.DAT\Software\Microsoft\Windows\ShellNoRoam\MUICache	Tracks the opening of executable files by the operating system	Immediately	XP

Information	File	Location	Description	When Updated	Version
Network - Computer Description	NTUSER.DAT	NTUSER.DAT\Software\Microsoft\Windows\CurrentVersion\Explorer\ComputerDescriptions	Network connections	N/A	
Network - Mapped Network Drive MRU	NTUSER.DAT	NTUSER.DAT\Software\Microsoft\Windows\CurrentVersion\Explorer\Map Network Drive MRU	Listed by drive letter	Immediately	XP, V, 7
Network - Workgroup Crawler	NTUSER.DAT	NTUSER.DAT\Software\Microsoft\Windows\CurrentVersion\Explorer\WorkgroupCrawler\Shares	Network connections crawled while connected.	N/A	
Outlook Account Passwords	NTUSER.DAT	NTUSER.DAT\Software\Microsoft\Protected Storage SystemProvider\SID\Identification\INETCOMM Server Passwords	Stores Outlook and Outlook Express account passwords.	Immediately	
Outlook Recent Attachments	NTUSER.DAT	NTUSER.DAT\Software\Microsoft\office\version\Common\Open Find\Microsoft Office Outlook\Settings\Save Attachment\File Name MRU	Microsoft Outlook recent documents.	Immediately	
Outlook Temporary Attachment Directory	NTUSER.DAT	NTUSER.DAT\Software\Microsoft\Office\version\Outlook\Security	Identifies the location where attachments are stored when they are opened from Outlook.	Immediately	
Paint MRU	NTUSER.DAT	NTUSER.DAT\Software\Microsoft\Windows\CurrentVersion\Applets\Paint\Recent File List	MRU for MS Paint documents (File1-File9)	Upon closing the application	XP, V, 7

Information	File	Location	Description	When Updated	Version
POP3 Passwords	NTUSER.DAT	NTUSER.DAT\Software\Microsoft\Internet Account Manager\Accounts\0000000#	Identifies the current user's POP3 passwords.  <b>Note:</b> # is a digit identifying that particular account.	Immediately	XP
PowerPoint 2007 Autosave Info	NTUSER.DAT	NTUSER.DAT\Software\Microsoft\Office\12.0\PowerPoint\Resiliency\DocumentRecovery\<id#>	Saves info about currently opened PowerPoint documents.	When document is opened and when saves are made	Office 2007
PowerPoint 2007 MRU	NTUSER.DAT	SNTUSER.DAT\Software\Microsoft\Office\12.0\PowerPoint\File MRU	MRU List for MS PowerPoint spreadsheets (Item1-Item50).  <b>Note:</b> The second bracketed number is a 64-bit date/time stamp of when the document was opened.	When document is opened	Office 2007
PowerPoint— Recent PPTs	NTUSER.DAT	NTUSER.DAT\Software\Microsoft\office\version\Common\Open Find\Microsoft Office PowerPoint\Settings\Save As\File Name MRU	Microsoft PowerPoint recent documents.	Unknown	Pre Office 2007
Printer— Default	NTUSER.DAT	NTUSER.DAT\Software\Microsoft\WindowsNT\CurrentVersion\Windows	Identifies the current default printer.	Immediately	XP, V, 7
Printer— Default	NTUSER.DAT	NTUSER.DAT\printers	Identifies the current default printer.	On shutdown	XP, V, 7

Information	File	Location	Description	When Updated	Version
Publisher 2007 MRU	NTUSER.DAT	NTUSER.DAT\Software\Microsoft\Office\12.0\Publisher\Recent File List	MRU List for MS Publisher documents (File1-File9).	When document is opened	Office 2007
Publisher—Recent Documents	NTUSER.DAT	NTUSER.DAT\Software\Microsoft\office\version\Common\Open Find\Microsoft Office Publisher\Settings\Save As\File Name MRU	Microsoft Publisher recent documents.	Unknown	Pre Office 2007
Recycle Bin Info	NTUSER.DAT	NTUSER.DAT\Software\Microsoft\Windows\CurrentVersion\Explorer\BitBucket\Volume<guid>	Tracks recycle bin info by GUID (track GUID back to MountedDevices in the SYSTEM file), Max Capacity in MB, NukeOnDelete.  0=Bin being used (default) 1= Bin is being bypassed	N/A	V, 7
Regedit - Favorites	NTUSER.DAT	NTUSER.DAT\Software\Microsoft\Windows\CurrentVersion\Applets\Regedit\Favorites	Displays user selected favorites in Regedit Utility.	Immediately after entering	XP, V, 7
Regedit - Last Key Saved	NTUSER.DAT	NTUSER.DAT\Software\Microsoft\Windows\CurrentVersion\Applets\Regedit / LastKey	Displays last subkey Regedit was on when closed down	Upon closing Regedit.	XP, V, 7
Run	NTUSER.DAT	NTUSER.DAT\Software\Microsoft\Windows\CurrentVersion\Run	Lists programs that run automatically when the user logs on.	NA	XP, V, 7

Information	File	Location	Description	When Updated	Version
Screen Saver Enabled	NTUSER.DAT	NTUSER.DAT\Control Panel\Desktop / ScreenSaveActive	1=Active 0=Disabled  The path/name displays at SCRNSAVE.EXE.  <b>Note:</b> In Windows 7, ScreenSaveActive retains a 1 whether enabled or not, but the path/name appears on enable and disappears on disable.	Immediately	XP, V, 7
Screen Saver Password Enabled	NTUSER.DAT	NTUSER.DAT\Control Panel\Desktop / ScreenSaverIsSecure	0>No Password Required 1=Password Required if screen saver is active	Immediately	XP, V, 7
Screen Saver Timeout	NTUSER.DAT	NTUSER.DAT\Control Panel\Desktop / ScreenSaveTimeOut	Length of time, in seconds, before the screen saver becomes active.	Immediately	XP, V, 7
Screen Savers and wallpaper	NTUSER.DAT	NTUSER.DAT\Control Panel\Desktop\	Identifies the system's screen saver and wallpaper.	Immediately	XP, V, 7
ShellBags	NTUSER.DAT	NTUSER.DAT\Software\Microsoft\Windows\Shell\BagMRU	Pointers to link history and other file and folder information.	NA	XP
Start Menu Program List	NTUSER.DAT	NTUSER.DAT\Software\Microsoft\Windows\CurrentVersion\Explorer\MenuOrder\Programs<appname>	Program listing drawn to the Start button.	N/A	XP

Information	File	Location	Description	When Updated	Version
Start Searches entered by user	NTUSER.DAT	NTUSER.DAT\Software\Microsoft\Windows\CurrentVersion\Explorer\WordWheelQuery	In Windows 7, traps search terms entered by the user in the Start > Search box.	After hitting the enter button.	7
Start Searches entered by user	NTUSER.DAT	NTUSER.DAT\Software\Microsoft\SearchAssistant\ACMru<5###>	Searches from the built-in search engine. 5001=Internet Searches 5603=Files and Folders 5604=Pictures and Music 5647=Computers and People	Immediately	XP
Startup Software	NTUSER.DAT	NTUSER.DAT\Software\Microsoft\Windows\CurrentVersion\Run	Stores the applications automatically launched at boot time.  This key is a good place to look for trojans.	NA	XP, V, 7
Startup Software	NTUSER.DAT	NTUSER.DAT\Software\Microsoft\Windows\CurrentVersion\RunOnce	Stores the applications automatically launched at boot time.  This key is a good place to look for trojans.	NA	XP, V, 7
Theme—Current Theme	NTUSER.DAT	NTUSER.DAT\Software\Microsoft\Windows\CurrentVersion\Themes	Identifies the Desktop theme and wallpaper.	Unknown	XP, V, 7
Theme—Last Theme	NTUSER.DAT	NTUSER.DAT\Software\Microsoft\Windows\CurrentVersion\Themes\Last Theme	Identifies the Desktop theme and wallpaper.	Immediately	XP, V
Type Paths into Windows Explorer	NTUSER.DAT	NTUSER.DAT\Software\Microsoft\Windows\CurrentVersion\Explorer\TypedPaths	User typed (or pasted) paths into Windows Explorer address bar	Upon hitting <Enter>.	7

Information	File	Location	Description	When Updated	Version
UserAssist	NTUSER.DAT	NTUSER.DAT\Software\Microsoft\Windows\CurrentVersion\Explorer\UserAssist<guid>	Application usage showing last access and number of launches of applications.  <b>Note:</b> GUID 750 is used in versions 2000, XP, and Vista.	Immediately	XP, V
UserAssist	NTUSER.DAT	NTUSER.DAT\Software\Microsoft\Windows\CurrentVersion\Explorer\UserAssist\<guid>	Application usage showing last access and number of launches of applications.  <b>Note:</b> Change to GUID F4E in Windows 7 for application launch info.	Immediately	7
Windows Explorer Settings	NTUSER.DAT	NTUSER.DAT\Software\Microsoft\Windows\CurrentVersion\Explorer\Advanced	Sets Windows Explorer preferences.	Immediately	XP, V, 7
WinZip - Accessed Archives	NTUSER.DAT	NTUSER.DAT\Software\Nico Mak Computing\filenmenu / filenmenu##	Path back to accessed Zip archives	Immediately	11.1
WinZip - Extraction MRU	NTUSER.DAT	NTUSER.DAT\Software\Nico Mak Computing\Extract / extract#	The path to which Zip archives are extracted.	Immediately	11.1
WinZip - Location Extracted To	NTUSER.DAT	NTUSER.DAT\Software\Nico Mak Computing\Directories / ExtractTo	Last location to which a Zip archive was extracted.	Immediately	11.1
WinZip - Registered User	NTUSER.DAT	NTUSER.DAT\Software\Nico Mak Computing\WinIni / Name 1	Registered user for installation	N/A	11.1

Information	File	Location	Description	When Updated	Version
WinZip - Temp File	NTUSER.DAT	NTUSER.DAT\Software\Nico Mak Computing\Directories / ZipTemp	WinZip temporary file location	N/A	11.1
WinZip - Zip Creation Location	NTUSER.DAT	NTUSER.DAT\Software\Nico Mak Computing\Directories / AddDir	Last location from which a Zip file was created.	Immediately	11.1
WinZip - Zip Creation Location	NTUSER.DAT	NTUSER.DAT\Software\Nico Mak Computing\Directories / DefDir	Last location to which a Zip file was created or opened.	Immediately	11.1
Word 2007 Autosave Info	NTUSER.DAT	NTUSER.DAT\Software\Microsoft\Office\12.0\Word\Resiliency\Document Recovery<id#>	Saves info about currently opened Word documents.	When document is opened and when saves are made	Office 2007
Word 2007 MRU	NTUSER.DAT	NTUSER.DAT\Software\Microsoft\Office\12.0\Word\File MRU	MRU List for MS Word documents (Item1-Item50). <b>Note:</b> The second bracketed number is a 64-bit date/time stamp of when document was opened.	When document is opened	Office 2007
Word—Recent Docs	NTUSER.DAT	NTUSER.DAT\Software\Microsoft\office\version\Common\Open Find\Microsoft Office\Word\Settings\Save As\File Name MRU	Microsoft Word recent documents in the “value” value.	Unknown	Pre Office 2007
Word—User Info	NTUSER.DAT	NTUSER.DAT\Software\Microsoft\office\version\Common\UserInfo	Identifies the user information entered when installing Microsoft Office. Note this information may be modified after installation.	Unknown	Pre Office 2007

Information	File	Location	Description	When Updated	Version
WordPad MRU	NTUSER.DAT	NTUSER.DAT\Software\Microsoft\Windows\CurrentVersion\Applets\Wordpad\Recent File List	MRU for MS Paint documents (File1-File9).	When document is closed	XP, V, 7
Yahoo!	NTUSER.DAT	NTUSER.DAT\Software\Yahoo\Pager\Profiles\*	Stores IM contacts, file transfer information, etc. for Yahoo!.	NA	
Yahoo! File Transfers	NTUSER.DAT	NTUSER.DAT\Software\Yahoo\Pager\File Transfer (global value)	Shows number of transfers in and out.	Immediately	
Yahoo! File Transfers	NTUSER.DAT	NTUSER.DAT\Software\Yahoo\Pager\profiles\ screen name\FileTransfer (user specific)	Shows settings for file transfers.	Immediately	
Yahoo! Identities	NTUSER.DAT	NTUSER.DAT\Software\Yahoo\Pager\profiles\screen name - All Identities, Selected Identities	Shows alternate user identities.	Unknown	
Yahoo! Last User	NTUSER.DAT	NTUSER.DAT\Software\Yahoo\Pager - Yahoo! User ID	Last logged-in user.	Immediately	
Yahoo! Message Archiving	NTUSER.DAT	NTUSER.DAT\Software\Yahoo\Pager\profiles\screen name\Archive	Shows settings for message archiving.	Immediately	
Yahoo! Password	NTUSER.DAT	NTUSER.DAT\Software\Yahoo\Pager - EOptions string	Encrypted password.	Immediately	
Yahoo! Recent Contacts	NTUSER.DAT	NTUSER.DAT\Software\Yahoo\Pager\profiles\screen name\IMVironments\Recent	Shows recent contacts and which IMV was used.	Immediately	
Yahoo! Saved Password	NTUSER.DAT	NTUSER.DAT\Software\Yahoo\Pager - Save Password	Shows if the password is saved.	Immediately	

Information	File	Location	Description	When Updated	Version
Yahoo! Screen Names	NTUSER.DAT	NTUSER.DAT\Software\Yahoo\Pager\profiles\screen name	Shows registered screen names and identities.	Immediately	
Yserver	NTUSER.DAT	NTUSER.DAT\Software\Yahoo\Yserver	Points to a directory location for file transfer information.	NA	

## SAM INFORMATION

Information	File	Location	Description	When Updated	Version
Account Expiration	SAM	SAM\Domains\Account\Users\f Key	Bytes 33-40 store the account expiration. If no expiration is set, FF FF FF FF shows.	NA	XP, V, 7
Group Names - Custom	SAM	SAM\Domains\Account\Aliases\Names	List of custom groups by name.	Immediately	XP, V, 7
Group Names - Local	SAM	SAM\Domains\Builtin\Aliases\Names	List of local group names.	Immediately	XP, V, 7
Groups - Custom	SAM	SAM\Domains\Account\Aliases\<rid>	List of custom groups by RID.	Immediately	XP, V, 7
Groups - Local	SAM	SAM\Domains\Builtin\Aliases\<rid>	Listed of local groups by RID.	Immediately	XP, V, 7
Home Group	SAM	SAM\SAMDomains\Account\Users - Home Group in RID and Names		N/A	7
Last Failed Login	SAM	SAM\Domains\Account\Users\f Key	Bytes 41-48 store the last unsuccessful logon.	NA	XP, V, 7
Last Logon Time	SAM	SAM\Domains\Account\Users\f Key	Bytes 9-16 store the last log-on time.	NA	XP, V, 7

Information	File	Location	Description	When Updated	Version
Last Time Password Changed	SAM	SAM\Domains\Account\Users\F Key	Bytes 25–32 store the last time the password was changed.	NA	XP, V, 7
Local Groups	SAM	SAM\Domains\Builtin\Aliases\Names	Lists local account security identifiers.	NA	XP, V, 7
Local Users	SAM	SAM\Domains\Account\Users\Names	Lists local account security identifiers.	NA	XP, V, 7
Machine SID Location	SAM	SAM\Domains\Account / V	Last twelve bytes of the V value.	N/A	XP, V, 7
Password Hint	SAM	SAM\Domains\Account\Users\<RID>\F_Value\UserPasswordHint	Shows a logon password hint if initiated by the user		V, 7
User Name and SID	SAM	SAM\Domains\Account\Users\V Key <b>Note:</b> See “User Name and SID” in <i>SOFTWARE Information</i> on page 21.	Contains the username and SID in hex. You must convert the last three hex numbers to decimal to determine the decimal version of the SID that is used in the Recycler and System Volume Information folder.	NA	XP, V, 7

## SECURITY INFORMATION

Information	File	Location	Description	When Updated	Version
Passwords— Cached Administrative Passwords	SECURITY	SECURITY\Policy\Secrets\ DefaultPassword / CurrVal and OldVal	CurrVal holds the current administrative password and OldVal holds the previous.	N/A	XP, 7
Passwords— Cached Domain Passwords	SECURITY	SECURITY\Cache / NL\$#	Default stores up to 10 set in SOFTWARE file.	N/A	XP

## SOFTWARE INFORMATION

Information	File	Location	Description	When Updated	Version
Auto Logon Set	SOFTWARE	SOFTWARE\Microsoft\Windows NT\ CurrentVersion\Winlogon / AutoAdminLogon	1= allow auto logon 0=disabled  The value won't exist unless the user set up autologon.	Immediately	XP, V
Auto Logon Set - Password	SOFTWARE	SOFTWARE\Microsoft\Windows NT\CurrentVersion\ Winlogon / DefaultPassword	If autologon is set, the password must be present in this value in the clear	Immediately	XP, V
Class Identifiers	SOFTWARE	SOFTWARE\Classes\CLSID	Class identifier information, GUIDs on Applications and processes.	N/A	XP, V, 7
Group Memberships	SOFTWARE	SOFTWARE\Microsoft\Windows\ CurrentVersion\Group Policy\ GroupMembership	List of groups with which user is associated.	Immediately	XP, V, 7

Information	File	Location	Description	When Updated	Version
Home Group	SOFTWARE	SOFTWARE\Microsoft\Windows\CurrentVersion\HomeGroup\SharingPreferences\<sid>		N/A	7
ICQ Information	SOFTWARE	SOFTWARE\Mirabilis\ICQ\Owner	Stores the User Identification Number (UIN).	At logon	
Indexed Folders	SOFTWARE	SOFTWARE\Microsoft\Window Search\CrawlScopeManager\Windows\SystemIndex\WorkingSetRules\#>	Reports the folders currently being indexed for the Search utility.	Upon adding a folder.	V, 7
Install Date	SOFTWARE	SOFTWARE\Microsoft\Windows NT\CurrentVersion	Lists the date the operating system was installed.	NA	XP, V, 7
Installed Application List	SOFTWARE	SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall	List of installed applications to use for uninstall.	N/A	XP, V, 7
Installed Application List	SOFTWARE	SOFTWARE\Wow6432Node\<appname>	List of installed 32-bit applications.	N/A	7
Installed Application List	SOFTWARE	SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\SharedDLLs	List of executables for installed applications.	N/A	7
Installed Application List	SOFTWARE	SOFTWARE\Microsoft\Windows\CurrentVersion\App Paths\<appname>	Installed list of applications	N/A	XP, V, 7
Installed Internet Browsers	SOFTWARE	SOFTWARE\Clients\StartMenuInternet\<appname>	List of installed Internet browsers.	N/A	XP, V, 7

Information	File	Location	Description	When Updated	Version
Installed Internet Browsers - Default Browser	SOFTWARE	SOFTWARE\Clients\StartMenuInternet / default	Default installed Internet browser	N/A	
Last Logged on User	SOFTWARE	SOFTWARE\Microsoft\Windows\CurrentVersion\Authentication\LogonUI	Displays the user name of the last logged on user, computer name, and date/time of last logon in the key last modified date/time stamp. If the shutdown is normal, the subkey is modified to logoff time.	N/A	V, 7
Last User Logged In	SOFTWARE	SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon	Lists the last user that logged in to the system. This can be local or domain account.	NA	
Libraries	SOFTWARE	SOFTWARE\Microsoft\Windows Search\Gather\Windows\SystemIndex\StartPages\#>		Upon creation	7
Logon Banner Message	SOFTWARE	SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System\LegalNoticeText	Contains the banner that appears at boot time. Users must click through the log-on banner to log on to a system.	NA	
Logon Banner Message	SOFTWARE	SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System\LegalNoticeText	Contains user-defined data.	NA	
Logon Banner Title	SOFTWARE	SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System\LegalNoticeCaption	Contains user-defined data.	NA	

Information	File	Location	Description	When Updated	Version
Logon Info—Default User and Domain Name	SOFTWARE	SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon	Identifies the default user and the associated domain name.	NA	
Logon Info—Legal Notices on Bootup	SOFTWARE	SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon	Contains legal notices that appear at boot time. Users must click through the log-on banner to log on to a system.	NA	
Network Cards	SOFTWARE	SOFTWARE\Microsoft\Windows NT\CurrentVersion\NetworkCards\#	Lists installed network cards. The value can match up to the GUID stored in the SYSTEM file at SYSTEM\ControlSet###\Services\tcpip\Parameters\Interfaces<guid>.	N/A	XP, V, 7
O/S Version	SOFTWARE	SOFTWARE\Microsoft\Windows NT\CurrentVersion	Identifies the currently installed OS version and service pack release.	NA	XP, V, 7
Password Hint XP	SOFTWARE	SOFTWARE\Microsoft\Windows\CurrentVersion\Hints\<username>	XP Password hint storage location.	Immediately	XP
Passwords—Cached Logon Password Maximum	SOFTWARE	SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon	Control of max passwords stored in the cached passwords in SECURITY file.	N/A	XP
Printer Properties for Installed Printers	SOFTWARE	SOFTWARE\Microsoft\Windows NT\CurrentVersion\Print\Printers\<printername>	Detailed printer information, including user-entered properties from Control Panel.	N/A	XP, V, 7
Product ID	SOFTWARE	SOFTWARE\Microsoft\Windows NT\CurrentVersion	Lists the Windows OS product key.	NA	XP, V, 7

Information	File	Location	Description	When Updated	Version
Product Name	SOFTWARE	SOFTWARE\Microsoft\Windows NT\CurrentVersion	Lists the name of the operating system.	NA	XP, V, 7
Profile list	SOFTWARE	SOFTWARE\Microsoft\Windows NT\CurrentVersion\ProfileList	Contains the user security identifier for users with a profile on the system.	NA	XP, V, 7
ReadyBoost Attachments	SOFTWARE	SOFTWARE\Microsoft\Windows NT\CurrentVersion\EMDMgmt\<driveid>	List of attached USB devices for ReadyBoost utility.	N/A	V, 7
Recycle Bin Info - XP	SOFTWARE	SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\BitBucket\<driveletter>	Windows XP Recycler info by drive letter, Max Capacity in MB, NukeOnDelete 0=Bin being used (default) 1= Bin is being bypassed	N/A	XP
Registered Organization	SOFTWARE	SOFTWARE\Microsoft\Windows NT\CurrentVersion	Identifies the registered organization entered during installation. Note this information may be modified after installation.	NA	XP, V, 7
Registered Owner	SOFTWARE	SOFTWARE\Microsoft\Windows NT\CurrentVersion	Identifies the registered owner entered during installation. Note this information may be modified after installation.	NA	XP, V, 7
Restore Point Information	SOFTWARE	SOFTWARE\Microsoft\Windows NT\CurrentVersion\SystemRestore	System Restore parameters	N/A	XP
Restricted Access to Removable Media	SOFTWARE	SOFTWARE\Microsoft\WindowsNT\CurrentVersion\Winlogon	Lists allocated CD-ROMS and floppies that are set to 0 (restricted).	NA	XP

Information	File	Location	Description	When Updated	Version
Run	SOFTWARE	SOFTWARE\Microsoft\Windows\CurrentVersion\Run	Lists programs that run automatically when the system boots.	NA	XP, V, 7
Startup Location	SOFTWARE	SOFTWARE\Microsoft\Command Processor / AutoRun	The AutoRun runs any application noted when cmd.exe is run.	N/A	
Startup Location	SOFTWARE	SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon/Userinit	Applications to start on bootup.	N/A	
Startup Software	SOFTWARE	SOFTWARE\Microsoft\Windows\CurrentVersion\Run	Stores the applications automatically launched at boot time. This key is a good place to look for trojans.	NA	XP, V, 7
Startup Software	SOFTWARE	SOFTWARE\Microsoft\Windows\CurrentVersion\RunOnce	Stores the applications automatically launched at boot time. This key is a good place to look for trojans.	NA	XP, V, 7
System Restore Info	SOFTWARE	SOFTWARE\Microsoft\WindowsNT\CurrentVersion\SystemRestore	System Restore settings and info		V, 7
Time Synchronization with Internet - Servers	SOFTWARE	SOFTWARE\Microsoft\Windows\CurrentVersion\DateTime\Servers		N/A	XP, V, 7
Turn off UAC Behavior	SOFTWARE	SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System\ConsentPromptBehaviorAdmin Value	Turn off the prompts to Continue when running a program needing elevated rights. Turns off Cancel or Allow. 0 is off, 2 is on (Default)		V, 7

Information	File	Location	Description	When Updated	Version
UAC – On or Off	SOFTWARE	SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System\EnableLUA_Value	Identifies whether the UAC is on or off. By default it is on: value 1. If off: value 0		V, 7
USB ID linked to Volume Serial Number	SOFTWARE	SOFTWARE\Microsoft\WindowsNT\CurrentVersion\EMDMgmt	Tracks USB keys by identifier and by volume serial number. Date and time if tested to be used as cache is stored along with USB size		V, 7
User Account Control	SOFTWARE	SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System	UAC status 1=Enabled 0=Not Enabled	Upon changing	V, 7
User Name and SID	SOFTWARE	SOFTWARE\Microsoft\WindowsNT\CurrentVersion\ProfileList <b>Note:</b> See “User Name and SID” in SAM Information on page 19.	Contains the username and SID in hex.  You must convert the last three hex numbers to decimal to determine the decimal version of the SID that is used in the Recycler and System Volume Information folder.	NA	XP, V, 7
WinZip Information	SOFTWARE	SOFTWARE\Nico Mak Computing	Contains WinZip information.		XP, V, 7
Wireless Vista, Windows 7	SOFTWARE	SOFTWARE\Microsoft\Windows NT\CurrentVersion\NetworkList\Profiles\<guid>	Each GUID is a connection.	N/A	V, 7
Wireless Vista, Windows 7	SOFTWARE	SOFTWARE\Microsoft\Windows NT\CurrentVersion\NetworkList\Signatures\Managed (or Unmanaged)\<guid>	Managed tracks hardwired connections,  Unmanaged tracks wireless connections.	N/A	V, 7

Information	File	Location	Description	When Updated	Version
Wireless XP	SOFTWARE	SOFTWARE\Microsoft\WZCSV\Parameters\Interfaces\{0E271E68-9033-4A25-9883-A020B191B3C1\} / Static#####	SSIDs are located in the Static# values followed by 4 digits.	Immediately	XP
Wireless XP	SOFTWARE	SOFTWARE\Microsoft\EAPOL\Parameters\Interfaces\{0E271E68-9033-4A25-9883-A020B191B3C1\} / #	SSIDs are located in the decimal number values.	N/A	XP

## SYSTEM INFORMATION

Information	File	Location	Description	When Updated	Version
\$MFT Zone Definition	SYSTEM	SYSTEM\ControlSet###\Control\FileSystem / NtfsMftZoneReservation	Values 1-4: 1=12.5% 2=25% 3=37.5% 4=50%  These values are defined according to Microsoft; however, values of 0 are common defaults and may be the same as a 1.	N/A	XP, V, 7
Automatic time zone adjustment	SYSTEM	SYSTEM\ControlSet###\Control\TimeZoneInformation\DynamicDaylightTimeDisabled Value	0 Default – On 1 Disabled		V, 7
Clearing Page File at Shutdown	SYSTEM	SYSTEM\ControlSet###\Control\Session Manager\Memory Management / ClearPageFileAtShutdown	0=Off (default) 1=On	N/A	XP, V, 7

Information	File	Location	Description	When Updated	Version
Computer Name	SYSTEM	SYSTEM\ControlSet###\Control\ComputerName\ComputerName	Identifies the computer's name defined in System Properties.	NA	XP, V, 7
Current Control Set	SYSTEM	SYSTEM\Select	Identifies which control set is current.	NA	XP, V, 7
Current Control Set	SYSTEM	SYSTEM\Select\Current	Contains information about the system's configuration settings.	NA	XP, V, 7
Display	SYSTEM	SYSTEM\ControlSet###\Enum\Display	Monitor settings	N/A	XP, V, 7
DLLs Loaded at Bootup	SYSTEM	SYSTEM\ControlSet###\Control\SessionManager\KnownDLLs	Listing of implicitly loaded DLL files at startup.		
Dynamic Disk	SYSTEM	SYSTEM\ControlSetXXX\Services\DMIO\Boot Info\Primary Disk Group	Identifies the most recent dynamic disk mounted in the system.	NA	XP, V, 7
Event Log Restrictions	SYSTEM	SYSTEM\ControlSet###\Services\EventLog\Application	Identifies who can read your event logs. A value of 1 restricts access; 0 permits access for guest and null users.	NA	XP, V, 7
Event Logs	SYSTEM	SYSTEM\ControlSetXXX\Services\Eventlog	Identifies the location of Event logs.	NA	XP, V, 7
Firewall Enabled	SYSTEM	SYSTEM\ControlSet###\Services\SharedAccess\Parameters\FirewallPolicy\StandardProfile / EnableProfile	0=Off 1=On (default)	Immediately	XP, V, 7
Floppy Disk Information	SYSTEM	SYSTEM\ControlSet###\Enum\FDC\<device>	Floppy disk controller info.	N/A	XP, V, 7
Home Group	SYSTEM	SYSTEM\ControlSet###\services\HomeGroupProvider\ServiceData		N/A	7

Information	File	Location	Description	When Updated	Version
Human Interface Devices	SYSTEM	SYSTEM\ControlSet###\Enum\HID	Includes keyboards, mice, trackballs, etc.	N/A	XP, V, 7
IDE Device Information	SYSTEM	SYSTEM\ControlSet###\Enum\IDE\<device>	HDD, CD, DVD, and other attached hardware.	N/A	XP, V, 7
Last Accessed Date and Time setting	SYSTEM	SYSTEM\ControlSet###\Control\FileSystem\NtfsDisableLastAccessUpdate Value	0 On 1 Default - Disabled		XP, V, 7
LPT Device Information	SYSTEM	SYSTEM\ControlSet###\Enum\LPTENUM\<device>	Parallel printer information to LPT port.	N/A	XP, V, 7
Memory Saved During Crash	SYSTEM	SYSTEM\ControlSet###\Control\CrashControl / DumpFile	Shows path to crash dump memory capture.	N/A	XP, V, 7
Memory Saved During Crash Enabled	SYSTEM	SYSTEM\ControlSet###\Control\CrashControl / CrashDumpEnabled	0=None 1=Complete 2=Kernel Memory Dump 3=Small Memory Dump (64k)	N/A	XP, V, 7
Mounted Devices	SYSTEM	SYSTEM\MountedDevices	Lists current and prior mounted devices that use a drive letter.	Immediately	XP, V, 7
Mounted Devices	SYSTEM	SYSTEM\MountedDevices\	Change: Now using USB ID and not ParentIDPrefix		
Network Cards	SYSTEM	SYSTEM\ControlSet###\Services\tcpip\Parameters\Interfaces\<guid>	GUID matches the network card GUIDs at Microsoft\Windows NT\CurrentVersion\NetworkCards\#.	N/A	XP, V, 7
Number of Processors in System	SYSTEM	SYSTEM\ControlSet###\Control\Session Manager\Environment / NUMBER_OF_PROCESSORS	The value stored in this value name is the number of processors on the system.	N/A	XP, V, 7

Information	File	Location	Description	When Updated	Version
Pagefile	SYSTEM	SYSTEM\ControlSetXXX\Control\Session Manager\Memory Management	Contains the page file settings such as location, size, set to wipe, etc.	View updates immediately; however, not effective until reboot.	XP, V, 7
PCI Bus Device Information	SYSTEM	SYSTEM\ControlSet###\Enum\PCI	PCI bus device information	N/A	XP, V, 7
PDA Information	SYSTEM	SYSTEM\ControlSet###\Enum\USB	Contains PDA information.	NA	
Prefetch	SYSTEM	SYSTEM\ControlSet###\Control\Session Manager\Memory Management\PrefetchParameters / EnablePrefetcher	0=Prefetch disabled 1=Applications Only 2=Boot Only 3=Application and Boot Prefetcher	N/A	XP, V, 7
Printer Information	SYSTEM	SYSTEM\ControlSet###\Control\Print\Environments\WindowsNTx86\Drivers\Version...	Contains information about the current printer.	Immediately	XP, V, 7
Printers—Currently Defined	SYSTEM	SYSTEM\ControlSet###\Control\Print\Printers	Lists all printers that are configured on the current system.	Immediately	XP, V, 7
Remote Desktop	SYSTEM	SYSTEM\ControlSet###\Control\Terminal Server / fDenyTSConnections	fDenyTSConnections=1 Remote Desktop Off fDenyTSConnections=0 Remote Desktop On	Immediately upon change	XP, V
SCSI Device Information	SYSTEM	SYSTEM\ControlSet###\Enum\SCSI	SCSI device settings; includes VHD device info.	N/A	XP, V, 7

Information	File	Location	Description	When Updated	Version
Serial Port Device Information	SYSTEM	SYSTEM\ControlSet###\Enum\SERENUM	Serial port device settings	N/A	XP, V, 7
Services	SYSTEM	SYSTEM\ControlSet###\Services	List of services.	N/A	XP, V, 7
Shared Folders	SYSTEM	SYSTEM\ControlSet###\Services\lanmanserver\Shares / <shared folder name>	List of shared folders on system.	Immediately	XP
Shutdown Time	SYSTEM	SYSTEM\ControlSetXXX\Control\Windows	Lists the system shutdown time.	NA	XP, V, 7 <b>Note:</b> Removed in Vista first release and returned in service pack
Startup Location	SYSTEM	SYSTEM\ControlSet###\Control\SessionManager\BootExecute	Software startup location. <b>Note:</b> This has not been tested in Windows 7	N/A	XP, V, 7
Storage - Volumes and Removable Media	SYSTEM	SYSTEM\ControlSet###\Control\Enum\Volume<guid>	Stores information on storage media, including beginning volume offset and size.	Immediately	XP, V, 7
Storage - Volumes and Removable Media	SYSTEM	SYSTEM\ControlSet###\Control\Enum\RemovableMedia<guid>	Stores information on removable media.	Immediately	XP, V, 7
Storage Device Information	SYSTEM	SYSTEM\ControlSet###\Enum\STORAGE	HDD info including partition sizes	N/A	XP, V, 7

Information	File	Location	Description	When Updated	Version
TCP\IP data	SYSTEM	SYSTEM\ControlSetXXX\Services\TCPPIP\Parameters	Lists the current system's domain and hostname data.	NA	XP, V, 7
TCP\IP Settings of a Network Adapter	SYSTEM	SYSTEM\ControlSetXXX\Services\adapter\Parameters\TCPPIP	Lists the current system's IP address and gateway information.	Immediately	XP, V, 7
Time Synchronization with Internet - Enabled	SYSTEM	SYSTEM\ControlSet###\Services\W32Time\Parameters / Type	NoSynch=Disabled NTP=Enabled	Immediately	XP, V, 7
Time Synchronization with Internet - Type	SYSTEM	SYSTEM\ControlSet###\Services\W32Time\Parameters / NtpServer	Shows current time provider (or if disabled, the last time provider) - NTP is time.windows.com (default - Microsoft) or time.nist.gov	Immediately	XP, V, 7
Time Zone	SYSTEM	SYSTEM\ControlSet001(or002)\Control\TimeZoneInformation\StandardName	Identifies the time zone entered during installation. Note this information may be modified after installation.	Immediately	XP, V, 7
USB Devices	SYSTEM	SYSTEM\Enum\USBSTOR	Lists the system's USB devices.	Immediately	XP, V, 7
USB Tracking	SYSTEM	SYSTEM\ControlSet###\Enum\USBSTOR	Change: Now using USB ID and not ParentIDPrefix		V, 7
Write Block USB Devices	SYSTEM	SYSTEM\ControlSet###\Control\storageDevicePolicies / Write Protect	0=Disabled 1=Enabled <b>Note:</b> This began with Windows XP Service Pack 2.	N/A	XP SP2, V, 7

| From <http://dcfldd.sourceforge.net/>

dcfldd is an enhanced version of GNU dd with features useful for forensics and security. Based on the dd program found in the GNU Coreutils package, dcfldd has the following additional features

Hashing on-the-fly - dcfldd can hash the input data as it is being transferred, helping to ensure data integrity.

Status output - dcfldd can update the user of its progress in terms of the amount of data transferred and how much longer operation will take.

Flexible disk wipes - dcfldd can be used to wipe disks quickly and with a known pattern if desired.

Image/wipe Verify - dcfldd can verify that a target drive is a bit-for-bit match of the specified input file or pattern.

Multiple outputs - dcfldd can output to multiple files or disks at the same time.

Split output - dcfldd can split output to multiple files with more configurability than the split command.

Piped output and logs - dcfldd can send all its log data and output to commands as well as files natively