DIGITAL FORENSICS **Investigation**

Learning Overview / Expectations

- The relevance of computer peripherals especially storage devices, mechanisms and techniques in computer forensics

- Explore the practicality of technologies concerning security controls and requirements through organizations and forensic investigation and analysis of incidents in digital and multimedia environment

- Contrast security and forensic—what it can do with issues concerning the integrity of data within any particular systems

- Gain the technical knowledge and skills to be successful in the investigation of computer incidents and crimes

- Apply widely acceptable practices available in the field of digital forensics

PARTS

I. COMPUTING BASICS: Review on computing and storage

II. SECURITY FUNDAMENTALS: Technology, practices and misconception on scale and its application

III. DIGITAL FORENSIC CONCEPTS: General concepts in scientific discovery in general and its adaptation in digital and multimedia data

IV. FORENSIC LAB SETUP/PRACTICE: Establishment of computer forensic laboratory and practice

V. DIGITAL FORENSIC PROCESS: Industry standard and processes (particularly with Electronic Discovery Reference Model)

VI. INVESTIGATION AND ANALYSIS: Carrying out investigation and analysis based on operating systems, applications and human-interposition

VII. REPORTS AND FINDINGS: Presentation of evidence to the court of law

COMPUTING BASICS

Brief Review / Prerequisites

- Fundamentals and principles of the following:
  - Computer and processes
  - Internetworking and TCP/IP
  - Operating systems / platforms
- Idea in computer security
- Basic terminologies

Computer

- It abide particular command to perform a specific job
- That its own language (binary number system) can understand as well as translate i.e. through the coding system
- Can only perform so fast based on the capacity primarily of its microprocessor and memory
- Allows subsets of system to work in an organize manner and with respect to its dependencies

Binary Number System

- 0s and 1s, computer native language
  - Can understand and initially process
- Building block of computer systems and applications
- Used in conjunction with Boolean algebraic equations including AND, NAND, OR, NOT, and combinations

Memory

- Volatile
  - Registers hold very small amount of data and used to store temporary values during multistep operations
  - RAM will take on larger pieces of data, a second level of memory and outside the processor
  - Cache is intermediate steps between registers and main memory
- Nonvolatile
  - Magnetic media
  - Used as swap space (an opportunity for the investigator) to processor
  - Investigator spent some time going through it

Basic Input and Output System

- Runs series of self-checks called power on self test (POST)
- Transition occurs within the master boot record (MBR) through the operating system
  - Tell where on the disk it should go next to continue booting
- Manages the allocation of resources via interrupt requests (IRQs) and direct memory access (DMA)
- Modern features are power management and digital rights management (DRM)
- Act as the interface between OS and hardware

Operating Systems

- By far the most complex piece of software on any given computer
- Translation layer between end-user applications and hardware
- Manages users, memory, applications and processor time
- Investigator must learn the mainstream of operating systems

Operating Systems / Platforms

- Windows
- Unix
- Linux
- Mac
- OS/400
- zOS

Processes

- Operating system sub-processes
- Applications
- Internetworking, TCP/IP and sockets
- Inter-process communication

Typical Idea in Computer Security

- Protect with the following:
  - Anti-virus
  - Firewall / packet filtering
  - Proxy
  - Encryption e.g. SSL for Web

Computer Storage Interfaces and Controllers

- Interfaces
  - SATA – Serial AT Attachment
  - Parallel ATA – Parallel AT Attachment
    - AT Attachment
    - AT Attachment Packet Interface
  - SCSI – Small Computer System Interface
  - IDE – Integrated Drive Electronics
- Controllers
  - Advance Host Controller Interface (AHCI)
    - Windows 8 / Server 2012 called from **msahci** to **storahci**
  - Redundant Array of Inexpensive Disk (RAID)
  - Automation/Drive Interface-Transport Protocol (ADT)

Interface: PATA

- PATA is originally ATA (T13)
  - Interface standard for the connection of storage devices such as HDD, floppy, optical
  - Standard maintained by INCITS (International Committee for Information Technology Standards, which also maintained T10 (SCSI) and T11 (Fiber Channel)
  - Uses the underlying ATA and ATAPI standards
  - One data channel support two harddrives, configured master and slave

Interface: SATA

- A computer bus interface for connecting host bus adapters to mass storage devices like HDD and optical drives.
- Supersedes PATA or ATA
- Advantages over PATA includes:
  - Reduced cable size, cost (seven conductors instead of 40, hot swappable, faster data transfer through higher signaling rates and more efficient transfer through an (optional) I/O queuing protocol
- Supports both 1.5Gbps (150MB/sec), 3Gbps (300MB/sec) of performance to each drive within a disk drive array

Interface: 3 Gbit/s SATA

- Current widely used standard for the buffer-to-computer interface.
- Can send about 300MB/s (10-bit encoding) from the buffer to the computer, and thus is still comfortably ahead of today’s disk-to-buffer transfer rates

ATA Bridges

- Translates between the drive’s interfaces and the enclosure’s external ports
  - Accordingly his bridging incurs some inefficiency
- Instances
  - IDE-to-SCSI
  - IDE-to-IEEE1394 (Firewire)
  - IDE-to-USB
- Benefits
  - Hardware-based write protection – particularly provides extra layer of protection to evidence processing workflow
  - Harddrive hotswap capability
- Practice in the past that protected harddrives alteration
  - Software-based interrupt 13 write-protection

Interface: SCSI

- Interface choice for server class systems
- Set of standards for physically connecting and transferring data between computers and peripheral devices
- Defines commands, protocols and electrical and optical interfaces
- Signal chain/bus may hold up to 8 or 16 devices
- Divide into logical functional sub-elements
  - Addressed with logical unit numbers (LUN)
- Tape backup with multiple tape-cassettes use LUNs to control tape drive and storage management device
- 3 implementation specifications (SCSI-1,2,3) released by ANSI

Interface: SCSI Command-Set Standards

- SCSI Primary Commands – 4 (SPC-4)
- SCSI-3 Block Commands (SBC-3)
- SCSI Stream Commands (SSC-3)
- SCSI Multimedia Commands (MMC-6)
- SCSI Media Changer Commands (SMC-3)
- SCSI Object-Based Storage Device Commands (OSD-2)
- SCSI Enclosure Services -3 (SES-3)
- SCSI Automation/Drive Interface Commands -3 (ADC-3)
- SCSI Reduced Block Commands (RBC)
- SCSI Optical Card Reader/Writer (OCRW)

Interface: SCSI Signalling

- General concepts i.e. differential signalling
  - A method of transmitting information electrically with two complementary signals sent on two paired wires, called a differential pair.
  - Improves resistance to electromagnetic noise compared with use of only one wire and an un-paired reference(ground)
- Instances:
  - Single-ended
  - Low voltage differential
  - Low voltage differential multinode
  - High voltage differential

Interface: SCSI Cabling

- SCSI Parallel Interface
- Fiber Channel
- Serial Attached SCSI
- iSCSI
- SRP
- USB Attached SCSI
- Automation/Drive Interface

Interfaces: ATA and SCSI Contrasts

- Data throughput very small
- Head and platter assembly same, attach appropriate controller card
- External transfer rate for SCSI can be up to 320MB/s, three times more than current ATA
- SCSI supports, parallel, queued commands where multiple devices can be used at once, ATA can be active at a time on each ATA bus

Interface: IDE

- Integrated Drive Electronics
  - Western Digital's original interface
- Current terminology
  - IDE/Enhance IDE have come to be used interchangeably with ATA/PATA
- Drive acquisition from store will almost yield one that is compatible with PATA
- Marketed EIDEs, compliant with various ATA specifications i.e. ATA-2, ATA-6

Controllers: AHCI

- A technical standard defined by Intel
  - Specifications intended for hardware component designers, system builders and device drivers developers
- Describes the register-level interface for a host controller for SATA
- Supported out of the box on Windows Vista and newer version, Linux from kernel 2.6.19 onwards, OpenBSD (added extended features such as port multiplier support) version 4.1 onwards and so on

Drive Compatibility

- ATA interface standard –
  - 28-bit addressing – approximately 137.4GB
- MS Scandisk and Disk Defragmenter – may not operate properly on drives about 137GB
- OpenBSD with 2TB (or more) HDD, re utilization
- Cables requirement, type and mode
  - ATA/33 standard – 40 conductor / 40 pin
  - Faster than ATA/33 – 80 conductor / 40 pin
  - Mixed cable
  - Cable select, jumper configuration
- Drive/storage capacity issues

Harddisks

- Data is recorded magnetically
- Functional elements may include
  - Capacity
  - Interface
  - Speed (rounds per minute)
  - Seek time, may depend on speed
  - Access time, may depend on speed
  - Transfer time, may depend on speed

Harddisks continuation

- Zone bit recording (ZBR)
  - Also called Zone Constant Angular Velocity (Zone CAV)
- With ZBR, on harddisk, the data on the tracks with the outer most zone will have the highest data transfer rate

Harddisks Drive Performance Characteristics

- Access time
  - Also called the response time of a rotating drive is a measure of the time it takes before the drive can actually transfer data.
- Data transfer rate
  - Covers both the internal (moving data between the disk surface and the controller on the drive) and external rates (moving data between the controller on the drive and the host system)
  - Sustained data transfer rate or sustained throughput will be the slower of the sustained internal and external rates, is less than or equal to the maximum or burst rate because it does not have the benefit of any cache or buffer memory in the drive

Harddisks Drive Performance Characteristics continuation

- Latency – the delay for the rotation of the disk to bring the required disk sector under the read-write mechanism
- Seek time – average seek time ranges from 3ms for high-end server drives, to 15ms for mobile drives, with the most common mobile drives at about 12ms and the most common desktop type typically being around 9ms.

Harddisks Drive Performance Characteristics, Data Transfer Rate

- Internal rate includes (not for SSDs)
  - Media rate
  - Sector overhead time
  - Head switch time
  - Cylinder switch time
- Can be measured by writing a large file to disk using special file generator tools, then reading back the file.

Direct Memory Access

- Made it easier for CPU to perform
  - ATA improves with DMA usage
  - Allow computer to transfer data w/o much of CPU cycles
- Ultra-DMA (UDMA) 5
  - ATA/100, maximum transfer rate
  - ATA/66
  - ATA/44
  - ATA/33, first adaptation
- IDE/ATA mode is backward compatible

File System Storage Layers

- Application-level storage
- Information classification
- File systems / storage space management
- Allocation units
- Information lifecycle management

Application-level Storage and Information Classification

- Operating system and utility files
- Operating system configuration files
- Application and support files
- Application and support files
- Application configuration files
- User data files

File Systems Management

- File System   Max filename length   Max file size   Max vol size
- ext2 255B 2TB 32TB
- ext3 255B 2TB 32TB
- ext4 255B 16TB 1EB
- ReiserFS 4032B/226 char 8TB(v3.6), 2GB(v3.5) 16TB
- FAT32 8.3 4GB (256GB) 2TB(16TB)
- NTFS 255 char 16EB 16EB

Information Lifecycle Management

- Data classification (data management)
  - What data types are available?
  - Where are certain data located?
  - What access levels are implemented?
  - What protection level is implement and does it adhere to compliance regulations and company policies?

SECURITY FUNDAMENTALS

Security Incident Occurrences

- Web, everywhere
- Georgia, public services disrupted
- Iran, nuclear reactor
- Air space, US Air Force
- Trading, Bloomberg terminals
- Banking, Philippine banks
- Schools, guess who

Security Breach Launchpad and Targets

- Stand-alone computer
- Locally networked computers
- Computers connected to the Internet
  - Internet services
  - Midrange, mainframe and microcomputers for financial and multinational/local institutions
  - Utility grid i.e. electricity, nuclear, sewerage including distribution facilities
  - National security and armed forces' information systems (IS) confidential/top secret data
- High-end mobile phones

Inflict By Whom

- Individual, personal interest
    - Learner, regardless of maturity
- Politician
- Private companies, corporate leverage
- Security contractors, especially
- Terrorist and brainsick
- Government
- Intelligence service

Verity of Security

- Contextual-based, at least currently
- Scope and parameters, if any, of security
  - Strategies within individual, companies and government
  - Issues, policy-level and practicality
  - Incidents, intent or not
  - War and attacks on individual, companies and government’s critical infrastructure
- Worst can be everything, actually

X-Factor

- Human analysis, motherwit
- Technology capacity
- Resourcefulness, if applicable

Security Technology Adaptation

- Cryptography, PKI, CA
  - PGP, Symantec (Verisign), Comodo
- IP Security
  - Palo Alto Networks, Checkpoint
- Anti-virus/malware
  - Avast, McAfee, Trend Micro
- Firewall / packet filtering
- Invinsibility, invisibility or anonymity internetworking and proxying
  - TOR project

INVESTIGATION AND FORENSIC CONCEPTS

Basic Definitions

FORENSICS equates with FORENSIC SCIENCE, FORENSIC is effectively a synonym for LEGAL or RELATED TO COURTS

Scientific tests or techniques used in the investigation of crimes

Used or applied in the investigation and establishment of facts or evidence in a court of law

The application of a broad spectrum of sciences and technologies to investigate and establish facts of interest in relation to criminal or civil law

The word comes from Latin *foreñsis*, meaning "of or before the forum"

Two modern usages of the word *forensic* include:

- Form of legal evidence
- Category of public presentation

Forensic Principle

EVERY CONTACT LEAVES A TRACE

- Dr. Edmond Locard

(13 December 1877 – 4 May 1966),

pioneer in forensic science who became the Sherlock Holmes of France

Locard’s Exchange Principle

- Helpful in determining what happened
- Shows how much care is required when collecting and evaluating trace evidence
- Cased studies include:
  - The Weimer children murders
  - The Westerfiled-van Dam case

Investigation Comprises

- **Incident response**, identify the systems and resources that have been or currently under attacked
- **Containment and / or control, of environment**, however, may not have to remove computers in question yet in their original setup—consider data classification, if exist
- **Monitoring of current events**, if any
- **Computer forensic laboratory**
- **Forensic scientist**, the most important element, knows how the tradecraft works, knows how and what to discover in a multidimensional level
- **Investigators' send-off,** consists primarily of
  - **Data collection**
  - **Forensic analysis**

Incident Response Causes

- Fraud
- Theft
- Intrusions
- Attacks
- Harassment
- Espionage
- Conspiracy
- Malfeasance (committed by employees and insiders)
- Civil discovery

Incident Response Rationale

- Preparation, important for investigator
  - Hashing critical system files
    - MD5 has been compromised
    - SHA-2 not yet
    - SHA-3 (formerly Keccak, designed successor to SHA-2)
  - Logging tool
  - Command (process) accounting
- Data backup and retention period, done cyclically and regularly, crucial for the victim to support the investigation process

Containment of Environment

- Restrict the use of victim computer(s) and relevant interfaces/connections, if any
- Immediately secure electronic data e.g.
  - Previous and current, if any, logs and backup
  - Replicate victim's computer data
  - Fax machine's stored data
  - Surveillance camera
  - And so on
- Verify and control access to the network
  - Firewall settings and integrity
  - Resources from the LAN

Monitoring of Events

- Network operation, may depend on their classes (and perceived origins/targets of attack)
  - TCP/IP
  - ATM
  - Frame relay
  - ISDN
- Data processing systems e.g. finance, accounting, human resources, et al
- Computer usage

DIGITAL FORENSIC FUNDAMENTALS, LAB SETUP AND PRACTICE

Digital Forensic

- A branch of forensic science encompassing the recovery and investigation of material found in digital devices, often in relation to computer crime.

Know The Subject Explicitly

- A medium of electronic/computer information
- A source of digital evidence
- An instrument for digital forensics
- A mechanism in the establishment of facts

Digital Forensic High-Level Concentrations

- Cyber security
- Cybercrime
- Cyber warfare
- Cyber terrorism

Digital Forensic History

- 1980s-1990s, seen growth of the field
- 2000s, developing standards
- Forward, continuous development of tools

Essential in History, 1980s-1990s

- Rise of computer crime caused law enforcement agencies to begin establishing specialized groups
- 1984, FBI launched Computer Analysis and Response Team
- 1985, British Metropolitan Police setup computer crime department
- 1988, CERT/CC formed at Carnegie Mellon University under U.S. government contract

History, 2000s

- Scientific Working Group on Digital Evidence (SWGDE), 2002, produced “Best practices for Computer Forensics”
- ISO 17025, General requirements for the competence of testing and calibration laboratories, 2005
- Convention on Cybercrime, came into force in 2004
  - It reconciles national computer crime laws, investigative techniques and international co-operation
  - Treaty signed by 43 nations and ratified by 16

Material Found in Digital Devices

- Computer processing of data or an information system itself
- Computer as medium or tool with the following events:
  - Attacks to networks
  - Defrauding of individuals or companies
  - Processing of murder evidence
  - Facilitates investigation, analysis of, and processing of physical evidence from a crime or incident

Cybercrime

- Offences that are committed against individuals or groups of individuals with a criminal motive to intentionally harm the reputation of the victim or cause physical or mental harm to the victim directly or indirectly, using modern telecommunication networks such as Internet and mobile phones.

High Profile Cybercrimes

- Particularly
  - Cracking
  - Copyright infringement
  - Child pornography
  - Child grooming
  - Steganography

Computer Forensic Laboratory

- Spoliation includes:
  - Network access
  - Physical access
  - Poor environmental safeguards
- ISO/IEC 17025
- Cutting-edge equipment caveat

DIGITAL FORENSIC PROCESSES

Computing Forensic Processes

- Scientific Working Groups pertinent to digital and multimedia forensic inlcudes:
  - Scientific Working Group on Digital Evidence
    - Seizing evidence, Equipment preparation, Forensic imaging, Forensic analysis/examination, Documentation, Reports, Review
  - Facial Identification Scientific Working Group
  - Scientific Working Group on Imaging Technology
- Electronic Discovery Reference Model
  - Information management, Identification, Preservation, Collection, Processing, Review, Analysis, Production, Presentation
- EDRM standards include: identification, production, metrics, XML schema and compliance

SWGDE Best Practice

- Define the scope and practice areas of the discipline of digital and multimedia evidence
- Recommend standard practices, protocols, reports and terminology
- Recommend standards for data interpretation and wording of conclusions
- Recommend education, training, and continuing education requirements
- Promulgate and disseminate research and development priorities to the community
- Collect and distribute dscipline-specific information on scientific foundation
- Seek international recognition and harmonization of appropriate SWGDE work products

SWGDE: Seizing Evidence

- Evidence handling
  - Stand-alone computer non-networked
  - Networked computer
- Servers
- General guidelines concerning the seizing of evidence are provided as follows:
  - Consult with the investigating offices to determine the necessary equipment to take to the scene
  - Review the legal authority to seize the evidence, ensuring any restrictions are noted. If necessary during the execution of the seizure, obtain additional authority for evidence outside the scope of the search.

SWGDE: Evidence Handling

- If the computer is turned off, do not turn it on
- A forensic specialist should be consulted when available
  - Before powering down a computer, consider the potential of encryption software being installed on the computer or as part of the operating system. If present, appropriate forensic methods should be utilized to capture the encrypted data before the computer powered down

SWGDE: Evidence Handling continuation

- Assess the power need for devices with volatile memory and follow agency policy for the handling of those devices
- Document the condition of the evidence
  - Take legible photographs (screen, computer front and back, and area around the computer to be seized) and/or make a sketch of the computer connections and surrounding area
- Appropriately document the connection of the external components
- Note and document any pre-existing damage to the evidence

SWGDE: Stand-alone computer

- Disconnect all power sources by unplugging from the back of the computer. Also, remove batteries from laptops.
- Place evidence tape over the power plug connector on the back of the computer.

SWGDE: Networked Computer

- Workstations: remove the power connection from the back of the computer
- Place evidence tape over the power plug connector on the back of the computer
    - Any network computer can be used for file sharing and those systems should follow normal shut down procedures

SWGDE: Servers

- A determination should be made as to the extent of data that should be seized
- Capture volatile data if necessary
- If shutdown is necessary, use the appropriate commands
  - Pulling the plug could severely damage the system, disrupt legit business and/or create and department liability

SWGDE: Server continuation

- Each piece of evidence should be protected from change and a chain-of-custody maintained as determined by agency policy. Appropriate packaging of evidence can include any of the following:
  - Plastic/paper bags or sleeves
  - Computer case sealed with evidence tape over case access points and power connector
  - Devices with volatile memory should be packaged appropriately to allow for power to maintained to the device

SWGDE: Server continuation

- Specific care should be taken with the transportation of digital evidence material, to avoid physical damage, vibration, and the effects of magnetic fields, electrical static and large variations of temperature and humidity

SWGDE: Equipment Preparation

- Equipment refers to the non-evidentiary hardware and software the examiner utilizes to conduct the forensic imaging or analysis of the evidence
- It must be monitored and documented to ensure proper performance is maintained
- Only suitable and properly operating equipment shall be employed
- The manufacturer's operation manual and other relevant documentation for each piece of equipment should be accessible
- Analysis/imaging software should be validated prior to use as discussed in the "*SWGDE Recommended Guidelines for Validation Testing*"

SWGDE: Forensic Imaging

- Examiner should be trained as discussed in the *SWGDE/SWGIT Guidelines and Recommendation for Training in Digital and Multimedia Evidence*
- Document the current condition of evidence
- Precautions should be taken to prevent exposure to evidence that may be contaminated with dangerous substances or hazardous materials
  - Materials are examine for integrity of their packaging

SWGDE: Forensic Imaging continuation

- Hardware of software write blockers are to be used to prevent the evidence from being modified
- Methods of acquiring evidence should be forensically sound and verifiable
- Forensic image(s) should be captured using hardware/software that is capable of capturing a "bit stream" image of the original media
- Digital evidence submitted for examination should be maintained in such a way that the integrity of the data is preserved. See *SWGDE Data Integrity with Computer Forensics*

SWGDE: Forensic Imaging continuation

- Properly prepared media should be sued when making forensic copies to insure no commingling of data from different cases
- Forensic image(s) should be archived to media and maintained consistent with departmental policy and applicable laws

SWGDE: Forensic Analysis/Examination

- Examiner should review documentation provided by the requestor to determine the processes necessary to complete the examination and ascertain legal authority to perform the requested examination.
  - Authority includes: consent to search by owner, search warrant, other legal authority

SWGDE: Forensic Analysis continuation

- Consideration should be given to the following before commencing any examination
  - The urgency and priority of the requestor's need for information
  - The other types of forensic examination, which may need to be carried out on the evidentiary item
  - Which items offer the best choice of target data in terms of evidentiary value
- An examination strategy should be agreed upon and documented between the requestor and examiner

SWGDE: Forensic Analysis continuation

- Conducting an examination on the original evidence media should be avoided if possible. Examinations should be conducted on forensic copies or via forensic image files
- Appropriate controls and standards should be used during the examination procedure
- Examination of the media should be completed logically and systematically consistent the agency’s SOPs

SWGDE: Forensic Analysis of Non-Traditional Computer Technologies

- Caveat
  - Traditional digital forensic techniques and procedures may not be appropriate nor effective in the prcessing of this type of data
- All attempts should be made to utilized accepted best practices and procedures when processing electornic digital devices in an non-traditional format. If these techniques are ineffective and/or not appropriate for the analysis of this type of data, alternate procedures may be used. All steps of the methodology utilized should be documented.

SWGDE: Documentation

- Copy of legal authority
- Chain of custody
- Initial count of evidence to be examined
- Information regarding the packaging and condition of the evidence upon receipt by the examiner
- Description of the evidence
- Communications regarding the case

SWGDE: Examination Documentation

- Be case specific, and contain sufficient details to allow another forensic examiner, competent in the same area of expertise, to be able to identify what has been done and to access the finding indepently

SWGDE: Reports

- Examination reports should meet the requirements of the examiner's agency
- Report issued by the examiner should address the requestor's needs
- To provide the reader will the relevant information in a clear and concise manner

SWGDE: Review

- The examiner’s agency should have written policy establishing the protocols for technical/peer and administrative review

Computer Assisted Review Reference Model (EDRM Resource)

- Process of having computer software electronically classify documents based on input from expert reviewers, in an effort expedite the organiztaion and prioritization of the document collection.
- May dramatically reduce the time and cost of reviewing electronically stored information (ESI), by reducing the amount of human review needed on documents classified as potentially non-material.
- A useful reference for e-discovery practitioners at corporations, law firms and elsewhere; e-discovery services and software providers; and organizations evaluating e-discovery tools.

EDRM Best Practice

- Organized as projects, working groups and committees

- Improve the electronic discovery process
- Seeks to achieve improvement on e-discovery by establishing guidelines, setting standards and delivering resources

EDRM: Information Management

- Getting your electronic house in order to mitigate risk & expenses should e-discovery become an issue, from initial creation of electronically stored information through its final disposition

EDRM: Identification

- Locating potential sources of ESI & determining its scope, breadth & depth

EDRM: Preservation

- Ensuring that ESI is protected against inappropriate alteration or destruction

EDRM: Collection

- Gathering ESI for further use in the e-discovery process (processing, review, etc.)

EDRM: Processing

- Reducing the volume of ESI and converting it, if necessary, to forms more suitable for review & analysis

EDRM: Review

- Evaluating ESI for relevance & privilege

EDRM: Analysis

- Evaluating ESI for content & context, including key patterns, topics, people & discussion

EDRM: Production

- Delivering ESI to others in appropriate forms & using appropriate delivery mechanisms

EDRM: Presentation

- Displaying ESI before audiences (at depositions, hearings, trials, etc.), especially in native & near-native forms, to elicit further information, validate existing facts or positions, or persuade an audience

EDRM Standards

- Identification
- Production
- Metrics
- XML Schema
- XML Compliance

EDRM Standards Identification

- Provide
  - Counsel with a guide for identification
  - Baseline for investigation and depth investigation
- 2 main components
  - Early case assessment
  - Early data assessment

EDRM Standards
Early Case Assessment

- Serves as a foundation for developing overall case strategies as well as early data assessment
- Items to consider during early case assessment
  - Type of triggering event
  - Facts of case
  - Case value
  - Outside counsel
  - Case strategy
  - Date range
  - Key words
  - Key departments/custodians includin gformer employees
  - Case merit, risk analysis
  - Legal hold requirements

EDRM Standards
Early Data Assessment

- Should provide counsel with the information necessary to understand the types of relevant data and where it is located
- Should cover any policies related to the retention or destruction of relevant data so appropriate steps can be taken to preserve relevant data and avoid spoliation

EDRM Standards
Early Data Assessment

- 3 key areas to focus
  - Records management interviews
  - Custodial interviews
  - IT interviews

EDRM: 3 Key Areas to Focus Records Management Interviews

- Roles and responsibilities of the records manager
- Records management program / policy
- Retention schedule
- Possible locations of relevant data
- Access to relevant data

EDRM: 3 Key Areas to Focus Custodial Interviews

- General employee information
- General computer information
- Relevant data
- Legal hold

EDRM: 3 Key Areas to Focus
IT Interviews

- E-mail servers
- File servers
- Laptops/desktops
- Transaction data
- Offsite media backup storage
- Web-based applications and cloud computing
- Portable devices
- Instant messaging
- Voice mail

Best Practice Management

- SWGDE
- EDRM

INVESTIGATION AND ANALYSIS

Evidence Collection and Archiving

- RFC 3227 (Request for Comments)
- BCP 55 (Best Current Practice)
  - Accordingly, security incident is a security relevant system event in which the system's security policy (system/written-based) is disobeyed or otherwise breached.

Guiding Priciples during Evidence Collection

- Adherence to policies and state law and involvement of enforcement personnel
- Capture as accurate the picture of the system as possible
- Keep detailed notes, the difference between time and UTC, timestamp provided
- Remove external avenues for change
- When confronted with collection and analysis, do the former first and the latter second
- Be methodical
- Make bit-level copy of the system’s media

Privacy Consideration during Evidence Collection

- Make sure no information collected along with the evidence you are searching for is available to anyone who would not normally have access to such information
- Do not intrude on people's privacy without strong justification
- Do not collect information from areas you do not normally have reason to access unless sufficient indication there is a real incident there
- Make sure investigator have backing of the company's established procedures in taking the steps you do to collect evidence of an incident

Computer Evidence Must Be

- Admissible
- Authentic
- Complete
- Reliable
- Believable
- Detailed
- Transparent

Collection Steps

- Where is the evidence?
- Establish what is likely to be relevant and admissible
- For each system, obtain the relevant order of volatility
- Collect the evidence with relevant tools
- Record the extent of the system’s clock drift
- Question what else may be evidence as you work through the collection steps
- Document each step
- Do not forget the people involved

The Forensic Expert / Investigator

- Creative in the discovery of evidence
- Rigorous in the application of a disciplined process
- Understanding of the legal issues that are involved every step of the way
- Complete understanding of the risks when embarking on a case
- Perform analysis in skillful manner
- Play an unbiased third party
- Resolve bias by practicing always full disclosure
- Discuss potential conflict of interest
- Incompetence or arrogance destroys or ruins case

Expert / Investigator Qualifications

- Gone through training, seminars and have practiced the skill
- Have track record in the industry
- Have enough credentials to imply competency often conduct civil investigations
- It is imperative that it used deterministic, repeatable process that is clear, concise and simple
- Common
  - IT administrators conduct internal investigation
  - Special division of a company conducts large-scale corporate investigation
  - Skilled IT manager is not always as good or qualified to be a forensic examiner

Preliminary Investigation

- Know if incident really occurred
- Retrieve systems volatile data (ROM), if any
- Create and prepare a response toolkit
- Labeling toolkit media
- Understanding if a system is compromise
- Determining whether a live response is in order

Know if Incident Really Occurred, What to Do About It

- Initial notification of an incident
- Conducting interviews and confirm further from others that has knowledge of the situation
- What effect, if not damage, have been occurred
- Probe what could have been the reason of the incident and who could be the initial suspect, if any, that they have in mind
- Identify primary stakeholders including management, technology officers and others who has immediate information about the event
- Determine what could be type of incident, when did it happen, location, initial detection of the incident

Retrieve Systems Volatile Data

- Volatile data remains only, at least, until the computer is turned off
- Determine the following:
  - Time and date
  - Currently logged on users
  - Modification, creation and access times of files
  - Open ports if any
  - Running processes
  - Connections to the machine
- Record the commands used in identify the foregoing

Order of Volatility

- Items that are apt to change or expire more quickly due to the passage of time e.g. processes, network connections, should be collected first
- Less volatile includes physical configuration can be collected at a later time
  - Identify what types of information we need to collect from a system, where to look for, what tools to use to retrieve it and how to get that information off the system

Create and Prepare a Response Toolkit

- Determines the audit policy of the system
- Dumps specific information (keys) within the registry
- Dumps registry into a text file
- Dumps database so that password can be tracked
- Monitors for successful and failed logons
- Detects hidden files
- Searches file system and accesses during specific timeframes
- Dumps system logs

Labeling Toolkit Media

- Making the toolkit as the evidence itself
  - Case number
  - Time and date
  - Name of the investigator who created the response media
  - Name of the investigator using the response media

Understanding Compromise System

- Investigators and regulatory bodies confirm that a system has been compromised by asking basic questions:
  - Was the system compromised?
  - Did the compromised system contain “sensitive data”, see appropriate legislation in particular to understanding the definition of “sensitive” data
  - If the answer to both of the preceding questions is “yes”, did the compromise of the system lead to the exposure of that sensitive data?

Live Response

- The collection of information about the state of systems while they are running, which includes information about processes and the files they are accessing, as well as information about network connections originating from and terminating at the system and which processes are using those network connections.

Determine if Live Response is in Order

- Why it is important
  - Even a system is not used, processes are running and actions are occurring on the system
  - Wait (Windows XP) 24 hours and a System Restore Point will be created automatically (by default). 3 days and the system conduct limited defragmentaion
  - If someone has infiltrated the system, while waiting, more data are being taken out

Determine if Live Response is in Order

- It may address
  - Shorter life of information from the system
  - Connection time out if it was not used for several minutes
  - Connection state may change overtime
  - Clipboard (Windows) may remain constant until they are changed or power is removed from the system
  - Processes or daemon live or run for a long time while others disappear very quickly

Whether to Engage in Live Response

- Do nothing, or
- Take the correct actions to protect my system/company as best under circumstance?
  - Performance of it depends on the situation, the environment, taking into consideration the investigators' intent, corporate policies or applicable laws) and the nature of issue investigators have been presented
  - Be aware of the fact that actions leave artifacts

Live Response: Collecting, Analyzing Volatile/RAM

- System time
- Logged-on user(s)
- Open files
- Network information
- Network connections
- Process information
- Process-to-port mapping
- Process memory
- Network status
- Clipboard contents
- Service/driver information
- Command history
- Mapped drives
- Shares
- Registers, cache
- Routing table, Arp cache, Process table, Kernel statistics
- Temporary file systems
- Remote logging and monitoring data
- Physical configuration, network topology
- Archival media

Order of Volatility

- Registers, cache
- Routing table, Arp cache, Process table, Kernel statistics
- Temporary file systems
- Remote logging and monitoring data
- Physical configuration, network topology
- Archival media

Live Response Methodologies

- Local
- Remote
- Hybrid of the above
  - Depends on factors such as the network infrastructure, deployment options and could be even political structure of the company

Live Response Data Analysis

- Generally characterized by stress, pressure, and confusion.
- Investigators can use data reduction and automation techniques to provide effective response
- Final response can be about business or political factor of the environment
- Root cause analysis can save both time and money
- Minimalist approach to system configuration can often serve to hamper or even inhibit an incident altogether

Investigative Uses of Advance Technology

- Answering machines and voice mail systems (digital and analog)
- Home entertainment
- Mass media copiers and duplicators
- Pens and traps
- Personal digital assistants
- Vehicle black boxes and navigation system

Answering Machines and Voice Mail Systems

- Records messages from callers when the called party is unavailable or declines to answer
- Plays a message from the called party before recording a message
- Retains date and time stamp information
- May have multiple settings include:
  - Users or voice boxes
  - Built into telephone
  - Separate device
  - Stored on an onsite device
  - Located remotely at a communications provider

Value of Answering Machines and Voice Mail Systems

- Obtain actual recordings of telephone call content and date/time stamp of the message, and determine whether the message has been listened to or not
- Identify callers by content of incoming messages
- Identify owners by pre-recorded outgoing messages
- Establish undercover identities
- Covertly monitor incoming calls in threat or stalking investigations

Value of Answering Machines and Voice Mail Systems continuation

- Subjects can additionally use these to do the following
  - Alter or erase original recording to redirect or mislead investigators
  - Facilitate and lend credibility to criminal enterprise
  - Communicate with one another
- Special investigatory and other considerations
  - Information can be remotely purged or altered, anyone with the password can access the systems, and there may be automatic destruction policies
  - Backed-up data may be accessible for long timeframes if an investigator is seeking voice mail at a business
  - Remove the telephone cord form a local answering machine to prevent remote purging
  - Data on answering machines may be subject to loss if the devices loses power. Consider using a tape recorder to record messages before removing power.
  - Day, date and time settings found on the device should be verified against the actual day, date and time

Home Entertainment

- Investigators should be aware of home entertainment that these may contain information relevant to investigations
  - TiVo, uses a digital video recorder, has hard drive, console can be modified to store information unrelated to recorded television programs
  - Game consoles e.g. Xbox, PlayStation, Nintendo are used to play video games, many come with internal hard drives and capable of internet connectivity, can be modified to store information

Home Entertainment continuation

- – Cable and satellite access devices, allow the user access to cable and satellite programming, may store information relating to the viewing history of the subscriber, can be altered to allow unauthorized access to premium channels
- – WebTV, device used to access the Internet, newer ones have hard drives

Home Entertainment, Value to Investigators

- Video recording may contain evidence of crimes such as child pornography or subjects' films of their own criminal activities
- The presence of large numbers of these devices may be evidence of copyright piracy or unauthorized access to subscription service
- The device may archive viewing histories that can be used to establish timelines or to confirm or refute alibis. For subscriber-based devices, the service provider may maintain additional records

Home Entertainment
Special Investigatory Consideration

- Because of the majority of these items are associated with televisions, when they are not connected to a television, illicit use should be suspected
- Examine the device for signs of physical tampering as evidence of modification, which may yield probative information

Mass Media Copiers and Duplicators

- Copies media in bulk
- It may retain data from the duplicated media
- May maintain records pertaining to recent actions performed by a device

Mass Media Copiers and Duplicators, Value to Investigators

- Mass media duplicators may have historical information that can provide proof of duplication
- Mass media duplicators can assist with preparing discovery or large amounts of evidence
- Possession of mass media duplicators may be evidence of software piracy, copyright infringement or duplication of contraband material

Pens and Traps

- Pen registers record the numbers as they are dialed from a specific phone number (outbound calls)
- A trap and trace records the telephone numbers as they are received by a specific phone number (inbound calls)
- They are used to identify e-mail and IP addresses of senders and recipients in real time
- They are not intended to capture the content of the communications but only the telephone number, IP or e-mail
  - May provide location information to wireless telephones

Personal Digital Assistants

- These are handheld computers designed with similar capabilities as those available on a standard computer such as
  - Personal information management (PIM) functions
    - Calendar
    - Contacts
    - To-do-list
    - E-mail
  - Word processors
  - Spreadsheet
  - Database utilities
  - What is available to smartphones also exist here except that it is not capable of the functions of telephone

PDAs Value to Investigators

- Managing cases
- Storing important reference material such as addresses or PDF files
- Sending and receiving e-mail with attachments that may contain evidence
- Brief note taking
- Storing templates of commonly used documents or forms (go-bys) for immediate access in the field
- Determining the precise location of the device (when GPS is enabled)

Vehicle Black Boxes and Navigation System

- Many vehicles e.g. cars, planes, trains, boats, produced today contain black boxes or navigation systems that are capable of capturing data regarding the vehicles operation, status and location
- Information available from these devices can be used
  - Accident reconstruction
  - To pinpoint the physical location of a vehicle
  - To determine speed
  - To monitor conversations in a vehicle
- It is placed by manufacturers for diagnostic purposes and are not normally accessed by vehicle operators

Investigation and Analysis: Platform-based

- Windows, UNIX/Linux, Macintosh including live response (volatile data from the system) and acquisition (imaging the running harddrive)
  - File systems
  - Harddisk
  - Digital media
  - Solid state devices
  - Smartphones
  - Boot processes

Windows FAT File Systems

- File Allocation Table (FA T) 12, 16, 32 (still in existence as of this writing) – been around for a quarter century

FAT Type	Maximum number of clusters supported
FAT 12	4,084
FAT 16	65,524
FAT 32	67,092,481 (MBR imposed limit)

Windows FAT 32

- FAT, generally, tracks which clusters the file uses, also which allocation units (clusters) are allocated and which are not
- 32-bit entries, 28 only are used
  - Cluster is group of sectors and within a partition, cluster is the basic storage unit for that partition’s file system
  - Sector is 512 bytes, the smallest unit that can be written on the media
- Supports up to a theoretical maximum of 268,435,445 clusters
- Two FAT tables, FAT 1 will mirror FAT2 and is used for redundancy in the event FAT 1 is correupted

Windows FAT 32 continuation

- In a Notepad (text file content properties) it can be determined easily the following sizes (may be applied not only to this particular file system):
  - Logical - 1 character equivalent to 1-byte and represents to the file's size (data content)
  - Physical – refer to the size it occupies on the disk, however, size varies according to the file system being used, may be contrasted/compared with NTFS file

Windows FAT 32 continuation

- In an instance of 1-byte file, knowing the logical size there seems to be considerable wasted space physically.
- Forensically, such wasted space holds valuable information known as ***slack space***
- The area from the 1 byte of data until the end of the sector in which it is contained is ***sector slack,*** it is padded with zeros in versions of Windows starting with Windows95b

Windows FAT 32 continuation

- The end of the first sector until the end of the last sector in the cluster, this space contains data from file(s) previously occupying this cluster, is called file slack, and from a forensic perspective, it is a gold mine of information and hardly a wasted space

FAT Values

Status	Meaning	Values
Unallocated	Available for use by the OS to store a file or directory	0x00
Allocated	Value represents the next cluster used by the file	Any value other than zero or other reserved values noted next
Allocated	Last cluster used by the file and is signified by the End of File marker value	Value that is greater than 0xFF8 for FAT 12, greater than 0xFFF8 for FAT16, or greater than 0xFFFF FFF8 for FAT 32
Bad	Not available for use by the OS	Value will be 0xFF7 for FAT 12, 0xFFF7 for FAT 16, and 0xFFFF FFF7 for FAT 32

Windows FAT File System continuation

- Clusters 0 and 1 are used for purposes other than storing data. The very first cluster in which data can be stored is cluster 2 and not, therefore, 0 or 1
- Directory entry is its other major component, it tracks file’s name, its length in bytes and its starting cluster number
- Recovery success of file depends on time elapsed, if it is fragmented (data resided in consecutive clusters), and tools that is dependable on the required job
- Signature for a FAT directory entry begins with the classic “dot (0x2E, first byte) double dot (0x2E2E, 32 bytes later)” structure (recall the CLI command with **`cd`**.., will change into the parent directory)

FAT Bit Flag Values for Attribute Field at Byte Offset 11

BIT FLAG VALUES (Binary)	Description
0000 0001	Read only
0000 0010	Hidden
0000 0100	System
0000 1000	Volume label
0000 1111	Long filename
0001 0000	Directory
0010 0000	Archive

FAT MAC Timestamps

- Directory entries that can shed light in network investigations namely MAC times and attributes
  - Time can tell when is file/directory created, last written or accessed
  - Can be used to determine when a piece of malware was placed on the system
  - Used to examine network logs and source of the file through network connectivity

FAT MAC Timestamps continuation

MAC	Time Directory	Entry Notes
Modified	Byte offsets 22-25	Last written date and time of file, stored as MS-DOS 32-bit timestamp
Accessed	Byte offsets 18-19	Date only of when file was last accessed-no time
Created	Byte offsetts 14-17	Date and time file was "created" in its present location, stored as MS-DOS 32-bit timestamp

FAT MAC Timestamps Limitations

- Appear in even seconds
- Only 5 bits allocated for tracking seconds in the MS-DOS 32-bit timestamp scheme
  - Tracks seconds in increment of 30 and multiples by 2 to convert to seconds
- Occurs with the last accessed timestamp, which in fact contains no time at all, only a date
  - For the last accessed time, there are only 2 bytes allocated, sufficient to tract a date and not a time

Windows NTFS File System

- Robust
- Stronger security
- Greater recoverability
- Better performance to read and write
- Better search capabilities
- Support long filenames
- Highly granular system of file permissions and access control
- Compression of individual files and directories
- Disk space utilization
- Improved support for metadata
- Encrypting file system
- Journalling file system (logging)—gives tremendous stability to NTFS

Windows NTFS File System continuation

- Partition identifier – 0x07 (check basic data partition)
- Directory contents – B+ tree
- File allocation – Bitmap
- Bad blocks - $badclus (MFT Record

Windows NTFS File System Limits

- Max file size: 16EB – 1KB (format), 16TB – 64KB (Windows 7, Server 2008 R2 or earlier implementation), 256TB – 64KB (Windows 8, Server 2012 implementation)
- Max number of files: 4,294,967,295 (2^{32}-1)
- Max filename length: 255 UTF-16 code units
- Max volume size: 2^{64} clusters – 1 cluster (format), 256TB (254 x 1024^4 bytes) – 64KB (64 x 1024 bytes) implementation
- File system permission: ACLs
- Forks: Yes
- Transparent encryption, see next slide
- Data deduplication: Yes (Windows Server 2012)

NTFS Transparent Encryption

- Per file
- DESX (Windows 2000 onward)
- Triple DES (Windows XP onward)
- AES (Windows XP Service Pack 1, Windows Server 2003 onward)

Windows NTFS File System continuation

- Several technical improvements over FAT and HPFS (high performance file system)
- Supersedes FAT file system as the preferred file system Windows operating systems
- It has gone from 3.1 and ends with NTFS4 with Windows NT to Windows 200 and XP uses NTFS5, could be used by newer versions too, if not even more advance NTFS version

NTFS On-Disk Format

Released versions	Windows operating system	NTFS versions
V1.0	NT 3.1	3.1
V1.1	NT 3.5	3.5
V1.2	NT 3.51 / 4	3.51 / 4
V3.0	Windows 2000	5
V3.1	Windows XP	5.1

Windows NTFS File System continuation

- Uses master file table (MFT)—remember FAT uses directory entry—wherein there is a kilobyte entry for every file and directory on the system
- Everything is a file (with FAT it is not the always the case)
- An MFT entry is a file record, each contain 1024 bytes
  - Each entry has header, first 42 bytes have a defined purpose and the remainder store the attributes of the file or directory

Master File Table

- The heart of NTFS
- The list, database of file records, starting with record 0, sequentially numbered
- Typical file record entry with attributes
  - HEADER
  - $STANDARD_INFORMATION
  - $FILE_NAME
  - $SECURITY_DESCRIPTORS
  - $DATA

System-Defined MFT Attribute Types

Attribute type identifier (Hex)	Name	Description
0x10	$STANDARD_INFORMATION	Constains fundamental properties such as MAC times, owner, SID, and basic attribute flags. In addtion to traditional MAC times, another timestamp describes when the MRT was last modified. Al ltimes are store in a 64-bit Windows timestamp and in GMT
0x20	$ATTRIBUTE_LIST	Shows where other attributes for the file or directory can be located.

System-Defined MFT Attribute Types continuation

Attribute type identifier (Hex)	Name	Description
0x30	$FILE_NAME	Stores the file or directory name in Unicode (long filename), as well as the short filename and all four times (last wrtten, last modified, last accessed, and MFT last changed)
0x40	$VOLUME_VERSION	Shows volume information for Windows NT 1.2 only
0x40	$OBJECT_ID	For Windows 2000 and later, this contains a 16-byte unique ID for the file or directory

System-Defined MFT Attribute Types continuation

Attribute type identifier (Hex)	Name	Description
0x50	$SECRUITY_DESCRIPTOR	Lists the access control and security properties of the file or directory
0x60	$VOLUME_NAME	Shows the volume name
0x70	$VOLUME_INFORMATION	Contains the file system version (other flags too)
0x80	$DATA	If resident, stores data contents. If non-resident, stores starting cluster and cluster run information
0x90	$INDEX_ROOT	Describes the root node of an index tree

System-Defined MFT Attribute Types continuation

Attribute type identifier (Hex)	Name	Description
0xA0	$INDEX_ALLOCATION	Describes the nodes of the index tree that is rooted in the previous $INDEX_ROOT attribute (attribute 0x90)
0xB0	$BITMAP	Shows the cluster allocation bitmap used by the $MFT file to track which MFT entries are allocated and also used by $INDEX_ALLOCATION to track which index records in $INDEX_ALLOCATION are allocated to an index record.

System-Defined MFT Attribute Types continuation

Attribute type identifier (Hex)	Name	Description
0xC0	$SYMBOLIC_LINK	For Windows NT 1.2 only, contains soft link information
0xC0	$REPARSE_POINT	For Windows 2000 and later, contains data for reparse points, which is a soft link
0xD0	$EA_INFORMATION	Used for legacy compatibility with OS/2 applications (HPFS)
0xE0	$EA	Same as above, immediate
0x100	$LOGGED_UTILITY_STREAM	For Windows 2000 and higher, describes encrypted attributes

Alternate Data Stream(s)

- Used to contain either the resident data of the file or the runlist information pointing to the clusters containing the nonresident data
- When data is inserted to ADS, it is not visible to the user, even if it has admin rights—make an ideal place for an intruder to hide data and make use of it
  - Investigator must be aware of this capability when dealing with NTFS
- Unique to NTFS, ADS must be created and preserved within an NTFS environment

Windows Systems

- Default processes of Windows specific platform, listed in a knowledge base, if any
- Memory
- Registry
- File
- Executable

Windows Process

- Thread
- Access token
- Process memory
  - Main program is stored in its specific section and the thread simply provides the instruction one a time to the CPU

Windows Process, Programs and Threads

- Each process contains a number of key elements:
  - Memory for the storage of the machine-language version of the program's instruction
  - Memory for any variables declared in the program
  - Tables tracking the location of included DLLs, their particular functions, and so on
  - An access token that specifies which rights and permissions the process has if it tries to access other system resources or the resources of another networked computer
  - One or more threads of execution

Process Memory

- DLL is loaded in the process’s memory space
  - MS provided DLLs are stored on the comptuer’s system disk (ordinarily in the %SystemRoot%\System32)
- System creates a table within the process’s memory listing each function available within the included DLLs

Windows Memory

- Dumping full content of physical memory / RAM
  - More comprehensive than dumping a process is different
- Collect physical memory by accessing object from user mode
- Access memory object itself
- Converting a raw memory
- Establishment of remote deployment module for cryptographic verification of binaries before data is executed
- Parsing contents of RAM extracts information about processes, network connections and so on (see earlier slide)

Windows Memory

- Dumping full content of physical memory / RAM
  - More comprehensive than dumping a process is different
- Collect physical memory by accessing object from user mode
- Access memory object itself
- Converting a raw memory
- Establishment of remote deployment module for cryptographic verification of binaries before data is executed
- Parsing contents of RAM extracts information about processes, network connections and so on (see earlier slide)

Alternative Approaches for Dumping Windows RAM Content

- Hardware devices – Tribble
- Firewire
- Crash dumps (Blue Screen of Death)
  - Types
    - Small (64KB)
    - Kernel
    - Complete (full content of RAM)
  - May cause based on KBQ244139 in a registry key

Windows Registry, 5 Root Keys

- HKEY_CLASSES_ROOT
- HKEY_CURRENT_USER
- HKEY_CURRENT_CONFIG
- HKEY_LOCAL_MACHINE
- HKEY_USERS

Windows Registry, Master Keys

- HKLM (HKEY_LOCAL_MACHINE)
  - It is used to established per-computer settings
- HKU
  - When SID is referenced, it is the SID of the console user or other past logged-on user
  - When UserName is referenced, it is the username corresponding with the SID

Windows Registry, HKLM

Hive Key	Hive File
HKLM\SAM	%SYSTEMROOT%\System32\config\SAM
HKLM\SECURITY	%SYSTEMROOT%\System32\config\SECURITY
HKLM\SOFTWARE	%SYSTEMROOT%\System32\config\software
HKLM\SYSTEM	%SYSTEMROOT%\System32\config\system

Registry Evidence: Mapping of Hive Filenames to Restore Point

Original Hive Filename	Restore Point Hive Filename	Notes
SAM	_REGISTRY_MACHINE_SAM	
SECURITY	_REGISTRY_MACHINE_SECURITY	
SOFTWARE	_REGISTRY_MACHINE_SOFTWARE	
SYSTEM	_REGISTRY_MACHINE_SYSTEM	
NTUSER		SID is the Security Identifier for the individual user. To locate a particular user's NTUSER.DAT file, you need to know a SID# for the user in question.

Registry Evidence: MRU Keys of Interest to Network-Intrustion

Key	Description
HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\RunMRU	List most-recently-used commands in the Run windows by user
HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\Map Network Drive MRU	List most-recently-mapped network drives by user
HKCU\Printers\Settings\Wizard\ConnectMRU	List most-recently-used network printers by user

Registry Evidence: MRU Keys of Interest to Network-Intrustion

Key	Description
HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\ComD1g32	LastVisitMRU lists programs and the files opened by them. OpenSaveMRU lists files opened and saved, grouped by extension, there is a key named for each file in the list
HKCU\Software\Microsoft\SearchAssistant\ACMru	Contains two subkeys that store searches carried out in Windows Explorer, which is useful in determining if the user/intruder was searching his local or network drives for files/directories or works/phrases, with the former stored in key 5603 and latter in key 5604

Local Security Authority

- SECURITY\Policy\Secrets
- Cannot be accessed through regedit
- Contains security information regarding various service accounts and other accounts necessary for the operation of Windows and is stored in this location by the service control manager
- Its job is that the system stores the credentials for service accounts so that they can be automatically be launched under the appropriate account

Local Security Authority continuation

- LSA secrets are encrypted and stored on disk in the Registry but Windows decrypts them upon boot and stores them in clear text in the memory space allocated to the LSA process
- Extracting information from LSA memory space only require the context of administrator

Startup in the Registry

- Common startup locations in the registry
- User startup folder registry settings
- Startup files outside the registry

*nix File System

- UFS is a file system used by many Unix and Unix-like (including Linux) operating systems. It is also called the Berkeley Fast File System, the BSD fast file system (FFS)
  - UFS volume is composed of the following parts:
    - Few blocks at the beginning of the partition reserved for boot blocks
    - Superblock, containing a magic number identifying this as a UFS filesystem, and some other vital numbers describing FS’s geometry and statistics and behavioural tuning parameters
    - Collection of cylinder groups

*nix File System Superblock

- Stores all the metadata about the file system. Each group has its own superblock, and a master superblock stores the data about the entire file system
- It is vital to the operation of the system since it is read when the file system is mounted.
  - If this becomes corrupted, the file system will no longer mount

*nix File System Group Descriptors

- Contains information about the group. Within it is the table of inodes and the allocation bitmaps for inodes and data blocks
- Allocation bitmap is of huge importance to the investigator since it tells the file system which blocks are used and which aren’t

*nix File System continuation

- Each cylinder group has the following components:
  - A backup copy of the superblock
  - A cylinder group header, with statistics, free lists, about the cylinder group, similar to those in the superblock
  - A number of inodes, each containing file attributes
  - A number of data blocks

*nix Directory Structure

- Uses forward slashes
- / is the top level
  - /bin, short for binary, where many of user commands are stored
  - /sbin, commands that only can execute
  - /etc, directory where nearly all configuration are stored
  - /home, is where user's home directories are located
  - /mnt, uses to mount removable media including CD/DVD drives

*nix File System, ext2

- Second extended file system
- Partition id, 0x83 (MBR)
- File allocation, bitmap (free space), table (metadata)
- Bad blocks, Table

*nix File System, ext2 Limits

- Max file size, 16GB – 2TB
- Max number of files, 10^{18}
- Max filename length, 255 bytes
- Max volume size, 2-32 TB
- Allowed characters in filenames, All bytes except NUL (‘\0’) and ‘/’+

*nix File System, ext2 Features

- Dates recorded, modification (mtime), attribute modification (ctime), access (atime)
- Date range, December 14, 1901 – January 18, 2038
- Date resolution, 1s
- File system permissions, POSIX
- Transparent compression, No (Available through patches)
- Transparent encryption, No
- Supported OS, Linux, BSD, Windows and Mac OS X (through IFS)
- Initially designed for the Linux Kernel by Remy Card, replacement of the extended file system (ext)

*nix ext3/ext4 Structure

- Commonly referred to as ext2 + journalling—is a concept used to protect the structure of the files by chaging the read/write process on the disk into an atomic transaction
- Journalling uses an atomic write and has the file system first write to a buffer, or journal
  - It addresses file system failures that occur when a disk crashes midwrite and loses half of the information that it was writing to disk

Linux Swap

- Supports in two forms
  - Swap file
  - Swap partition
    - The kernel uses the disk blocks to act as additional memory blocks for program usage (a memory paging system to be semantically correct)
- Usefule in memory and file reconstruction

*nix Inode

- Every file and directory is represented by it
- A data structure found in many Unix file system
- Each stores all the information about a file system object such as file itself, device node, socket, pipe et al except data content and file name
- It includes data about the size, permission, ownership and location on disk of the file or directory

*nix POSIX Inode Description

- The size of the file bytes
- Device ID (this ids the device containing the file)
- The user ID of the file’s owner
- The group ID of the file
- The file node which determines the file type and how the file’s owner, its group, and others can access the file
- Additional system and user flags to further protect the file (limit its use and modification)
- Timestamps telling when the inode itself was last modified (ctime, inode change time), the file content last modified (mtime, modification time), and last accessed (atime, access time)
- A link count
- Pointers to the disk blocks that store the file’s contents

*nix stat(system call)

- Retrieves a file’s inode number and some of the information in the inode
- Returns file attribute about inode
- Time of last access, atime, `ls -lu`
- Time of last modification, mtime, `ls -l`
- Time of last status change, ctime, `ls -lc`
- Stat structure is defined in <sys/stat.h> with members including st_dev (identifier of device containing file), st_ino (inode number) and so on

*nix File System Signatures

- Finding the true superblock which is 0xef53
- Backup copies are all over the system and can be used to re-create it

*nix Distros Differences, Linux

- Ubuntu – uses the Advance Packaging Tool and the graphical front-end Synaptic to install new applications
- Red Hat / Fedora – uses RedHat Package Manager to install new programs
- Gentoo – is installed which everything is compiled for the machine, nothing is done from a binary package. It uses portage/emerge and acts imilarly to the BSD ports system
- Suse – it uses Yast which has capabilities similar to Red Hat's RPM
- Debian – has one of the best package management tools, APT, and the default installation is geared toward development tools and testing

Macintosh File System

- Use guide partition table (GPT, look for its specification for complete details) to describe the layout of the boot volume
  - More extensible than earlier partitioning schemes and resolves several of the limitation inherent in the preceding implementation
  - Much more flexible and extensible than Windows MBR partitioning
- Apple has extensively enhanced the hierarchical file system (HFS) volume format
  - When HFS+ volume specification has been introduced it does also the “wrapper” that would allow older utilities to understand and respect newer file system

Macintosh Computer Fundamentals

- Generally use the same type of Serial ATA hard drives that are found in comparable PCs
- Unlike in the older days some version of disk utilities would work only on Apple-branded drives
  - Nowadays, they become interchangeable and disk can be put from Mac into PC and vice versa

Macintosh Forensic

- When it comes to duplication
  - Firewire mode can be used to boot live operating system
    - When in this mode the computer presents the internal primary master device as a FireWire device, similar to Maxtor or other external IEEE 1394 HDD
- Can be connected to another machine via Firewire cable and image, view and search normally
- Never boot a Macintosh that contains evidence unless you know exactly what you are doing. The normal boot process changes data

Macintosh Forensic, GUID Partition Table

- Protective MBR (LBA0) – the first block on an Apple-formatted GPT
  - Defines a single partition entry that covers the entire area of the disk used by GPT structures and partitions
  - Designed to prevent GPT-unaware programs from accidentally modifying a GPT disk
- LBA1 – the next block which is the primary partition table header, defines the partition table header as a structure that defines various aspects of the disk including GUID to uniquely identify the disk, the starting block of the partition entry array and the size each partition entry in that array

Macintosh Forensic, GUID Partition Table continuation

- Look further on the following
  - 512-byte partition table header
  - 128-byte partition entry, brings to the partition entry array starting at LBA2, is an array or list of all the partitions described in the partition table
    - GPT requires that the partition entry array be at least 16KB, for a 512-byte block size, this is 32 blocks

Macintosh Disks in Three Ways

- Tiny, less than 1GB, created with no reserved free space and no extra partitions
- Small, 1-2GB, created with no extra partitions but have 128MB of free space at the end of each partition
- Big, larger than 2GB, have a 200MB extensible firmware interface (EFI) system partition called the EFI system partition (ESP) as the first partition on the disk and they also have the 128 MB of free space after each partition (not including the ESP partition)

Macintosh File System: HFS

- New HFS is completely different as the older volume, occupation of a special reserved space near the beginning of the volume
  - The older did occupy
- The job of keeping track of the allocation blocks allocated to a file is performed by the allocation file, a new structure introduced with HFS+ and similar to the volume bitmap in HFS
- Each allocation block is represented by 1 bit
- 0 means the block is free
- 1 means the block is in use

Macintosh File System: HFS Internals

- More closely parallels to the behavior of NTFS
- Trees are made up of nodes, logical groupings of information that are interanl to the file system and contain records—contain data or pointers to data
- Different types of nodes appear on the tree
  - Header nodes
  - Index nodes
  - Leaf nodes, gives us information about files—their names, access times, and other attributes

Macintosh File System: HFS Internals continuation

- Nodes are pointed to and/or linked together and may be conceptualized as layers
  - Header node is at the top
  - Index nodes, is under header node, may point to other levels of index nodes or to leaf nodes
- Root node is at the top of the tree, at level 0, contains pointers to B-tree header nodes, which in turn point to index nodes

Macintosh File System: HFS Internals continuation

- Catalog file, a branching tree data structure or B*-tree that contains records for all the files and directories stored in the volume
- HFS+ catalog file is the same as in the HFS
  - The main differences being that records are larger to allow more fields and to allow for those fields to be larger

Macintosh File System: HFS Internals, B*-tree(s)

- Extents overflow file, records the allocation blocks that are allocated to each file as extents
- Attributes file, a new B*-tree in HFS+ that does not have a corresponding structure in HFS
  - It can store 3 different types of 4KB records
    - Inline data
    - Fork data
    - Extension
- Startup file, designed for non-Mac systems that don’t have HFS or HFS+ support, similar to boot blocks of an HFS volume
  - Alternate volume header is the second to last sector equivalent to the alternate Master Directory Block of HFS
  - Last sector is reserved for use by Apple, used during manufacturing process

Macintosh File System: HFS Internals, B*-tree(s)-Attributes

- Inline data attribute, records store small attributes that can fit within the record itself
- Fork data attribute, records contain references to a maximum of eight extents that can hold larger attributes
- Extension attributes, used to extend a fort data attribute record when its eight extent records are already used

Harddisks (Forensic)

- Stores 1s and 0s
- Acquisition through sector-by-sector image may require forensic disk controller, specialized type of computer HD controller made for the purpose of gaining read-only access to computer harddrives without the risk of damaging the drive’s contents
- Most common application is for use in investigations where a computer harddrive may contain evidence

Harddisks, Image Copying

- Creates a complete sector-by-sector copy of the source medium and thereby perfectly replicating the structure and contents of a storage device
- Sector-by-sector sometimes called bit-stream image
- Used to make perfect clones of harddisks
- File formats may be open standards such as the ISO image or proprietary such as the one used by MagicISO, Universal Image Format (UIF)

Harddisks Capacity Calculation

- 512 bytes per sector
- Calculate how many sectors have with a 1TB of hard disk

Digital Media

- All of the following can store data
  - Blu-ray
  - CD
  - DVD including HD/DVD
  - Flash drive or memory
  - Smartphones storage media
  - iPod/iTunes
  - Tape
  - Xbox
  - Zune

Digital Media, Blu-ray

- Refers to blue laser used to read the disk, which allows information to be stored at a greater density that is possible with the longer-wavelength red laser used for DVDs
- Supersedes the DVD format
- Conventional (pre-BD-XL) Blu-ray Discs contain 25GB per layer, with dual layer discs being the industry standard for feature-length video discs

Solid State Devices

- It became prevalent the expression in the 1950’s and 60’s during the transition from the vacuum tube technology to semiconductor diodes and transistors
- Cat’s whiskers first used in the 1930s radio receivers

Solid State Devices

- Types include
  - CF, MMC, MS, SD, SM, xD-Picture
- Further examples
  - Integrated circuit
  - Light emitting diode
  - Liquid crystal display

Popular Solid State Devices

- Flash drive/disk used in handheld devices including
  - Digicam
  - Smartphones
  - Laptop
  - Video/audio/CD/DVD players
  - Game consoles

Common Solid State Devices

- Transistors
- Microprocessors chips
- Random access memory, example is flash RAM used as flash/USB drives

Bootstrap Processes Evolution

- Early days
  - Altair and minicomputers uses front panel, toggle and switches
- PROM chips
  - Apple 1, 1976, eliminated above
  - Uses firmware, enables to enter, display and debug programs (all in hex) from the keyboard
- OS ROM
  - Atari ST microcomputer were instant on, eliminated retrieval of OS from secondary storage
- BIOS
  - IBM introduced it in its PC, one of the functions of that firmware was to perform a POST
- Extensible Firmware Interface
  - Developed by Intel, originally for Itanium-based machines, has become an alternative to BIOS in x86 machines

Basic Input Output System

- First step is power-on self test (POST)
  - Perform a check of the hardware
- Second step is local device enumeration and initialization
- Two parts
  - POST code, after POST is complete, it is flushed from memory
  - Runtime services, remain and are available to the target OS, searches for devices that are both active and bootable in the order of preference defined by the complementary metal oxide semiconductor (CMOS)

Modern Bootstrap Processes

- Small program stored in RAM along with a small amount of needed data to access the nonvolatile device from which the OS programs and data can be loaded into RAM
  - It is called bootstrap loader, bootstrap or boot loader
- Input operation from peripheral devices
- Send hardware commands directly to I/O controller, such as read sector zero
- Automatic boot loader mechanisms to ensure the computer starts quickly, desktop bootstrap begins with the CPU executing software contained in ROM at a predetermined address

Second State Bootloader

- Not considered operating systems, however, are able to load properly and transfer execution to it—OS then subsequently initializes itself and load extra device drivers
  - GNU GRUB (Unix-like or Linux)
  - BOOTMGR (Windows)
  - Syslinux
  - NTLDR (Windows XP/2003
  - Boot Configuration Data (BCD) (Windows Vista, 7 Server 2008 R2)
    - Invokes winload.exe then load the OS kernel ntoskrnl.exe
- Some are capable of multi-boot loaders or multiple booting choices

Other Boot Sequences

- Boot code integrated directly into their silicon, so such a processor could boot from various sources like NAND flash, SD or MMC, not easy to hardwire such devices so boot ROM is used instead
- Hardware debug interface, see JTAG, may be used to write the boot loader program into bootable non-volatile memory
- Microcontrollers allow the insertion of boot code into bootable non-volatile memory via simple protocols
- Most digital signal processors have boot modes:
  - Serial mode boot
  - Parallel mode boot, such as the host port interface (HPI boot)

Boot Sector

- Also called boot block
- Region of a hard disk, floppy, optical, other data storage
  - Contains machine code to be loaded in RAM by a computer system's built in firmware
- Allow a boot process of a computer to load a program
  - Usually, but not necessarily, an OS

Kinds of Boot Sector

- Master boot record (MBR)
  - The first sector (equivalent of 512B) of an entire data storage device that has been partitioned
- Volume boot record (VBR)
  - Also known as volume boot sector, partition boot record or boot sector
  - Invoking it via boot manager is known as chain loading

Boot Sector: Master Boot Record

- Concept was introduced in 1983, storage volumes now commonly exceeding 2TB, the limiting factor in 2010
- Holds the information on how the logical partitions, containing file systems, are organized on that medium
- Functions as an operating systems independent chain boot loader in conjunction with each partition's VBR
- MBR are not present on non-partitioned media like floppies, superfloppies or other storage devices

Boot Sector: Master Boot Record continuation

- In the process of being superseded by the GUID partition table (GPT) scheme in new computers
- GPT can coexist with it in order to provide some limited form of backward compatibility for older systems

Boot Sector: Master Boot Record, Programming Considerations

- Numeric values spanning two or more bytes are stored by the processor in reverse order in memory
- MBR signature appears as the sequence of 55h AAh
- Boot sequence in the BIOS will load the first valid MBR that it finds into the computer's physical memory at address 0000h:7C00h—code expected to be loaded
  - Last instruction executed in BIOS will be a "jump" to direct execution to the beginning of the MBR
- Signature at offset +1FEh, primary validation for most BIOSes
- The last 72 bytes of the 512 byte (equivalent of a sector) MBR are reserved for the partition table
- Boot sector program must be small enough to fit within 440 bytes of memory

Volume Boot Record

- Contains machine code for bootstrapping programs stored in other parts of the device
- It is the first sector of the device, on non-partitioned devices
- It is the first sector of an individual partition on the device
- FAT12, 16, 32, HPFS and NTFS contains a BIOS Parameter Block (BPB) specifies the location and layout of the principal on-disc data structures for the file system

Volume Boot Record Technology, Signature

- Two-byte hexadecimal sequence for sector sizes of 512 bytes (marks the end of the sector) or more
- On smaller and larger sectors show signatures at the end of the actual sector size, however, semantics apply to 16-bit signature at +1FEh
- 55h at fixed offset +1FEh and Aah at +1FFh
- Indicates the presence of at least a dummy boot loader which is safe to be executed, even if it may not actually load OS
  - Does not indicate the presence of file system or OS

Volume Boot Record Technology, Signature continuation

- Tested for by most System BIOSes since (at least) the IBM PC/AT
- Checked by most MBR boot loaders before passing control to the boot sector
  - Can be disabled in some environment
- Some old boot sectors do not feature this signature

Volume Boot Record Technology, Invocation

- Boot code can assume that the BIOS has set up its data structures and interrupts and initialized the hardware
- Should not assume more than 32KB of memory to be present for fail-safe operation
- If it needs more memory it should query INT 12h for it
- BIOS Boot Specification allows for 64KB of memory and explicitly recommends 0000h:7C00h to 0000h:FFFFh as a temporary scratchpad
- Must not assume better CPUs than the original 8088/8086 and in regard to the exact state of the hardware, the interrupt system of the location and size of the stack

Volume Boot Record Technology, Invocation continuation

- Registers not mentioned aside those below must be treated as not initialized, are used to form a memory address, applied in 16-bit
  - Segment registers (DS, ES, SS, CS), IP (intruction pointer)

GUID Partition Table (GPT)

- Standard for the layout of the partition table on a physical hard disk
  - Forms part of the UEFI specification that defines a software interface between an OS and platform firmware
  - EUFI can support remote diagnostics and repair of computers, even without another OS
  - Meant to replace BIOS, however, has provided legacy support for it

Unified Extensible Firmware Interface

- Provides several technical advantages over a traditional BIOS system
  - Ability to boot from large disks, over 2TiB with GPT
- CPU independent architecture
  - Processor binding exists for Itanium
  - Supports only little-endian processors
- CPU independent drivers
  - Free from many limitations of MBR
  - Limits of 4 primary partitions per disk up to 2TiB (2^{40}bytes) per disk have been relaxed
- Flexible pre-OS environment, including network capability
  - Linux built option “CONFIG_EFI_PARTITION”
  - Microsoft Windows Vista and later
- Modular design
- EFI shell, can be used to execute other EFI applications
- Extensions to EFI can be loaded from virtually any non-volatile storage device attached to the computer

Unified Extensible Firmware Interface Secure Boot

- Under 2.2 specification
- Secure boot process by preventing loading of drivers or OS loaders that are not signed with an acceptable digital signature
- When it is enabled, it is initially placed in “setup” mode, allows a public key known as platform key (PK) to be written to the firmware, then secure boot enters “User” mode, then only drivers and loaders are signed with the platform key can be loaded by the firmware
- Key Exchange Keys can be added to a database stored in memory to allow other certificates to be used, must have connection to the private portion of the PK
- Can be placed in “Custom” mode, where additional public keys can be added to the system that do not match the private key
- Supported, as of this writing, by OS namely
  - Windows 8, Server 2012
  - Select Unix-like distributions

Windows 8 Boot Process

- New and changed features
  - Faster startup through UEFI integration
    - Protect against malware infecting boot process
  - Hybrid boot
    - Hibernates Windows kernel on shutdown to speed up the subsequent boot
  - It made possible for enterprise uesrs to create live USB version of Windows
    - Windows To Go

Windows 8 Boot Process

- New and changed features continuation
  - Support on hard disk 4Kn advance format
    - Long data sector
    - Exceeds the traditional 512-byte-per-sector format
    - Enable integration of strong error correction algorithms to maintain data integrity at higher storage densities

Unix-like Boot Process (Linux)

- Flow of control during boot is through (from power up/reset to operation)
  - BIOS
  - Boot loader
    - First or stage 1, MBR
    - Second or stage 2, GRUB, LILO, Loadlin
  - Kernel (Linux operating system)
  - Init

Linux System Startup

- Depends on the hardware it is being booted on
- On embedded platform, a bootstrap is used when the system is powered on or reset
  - Examples include U-Boot, RedBoot, and MicroMonitor
  - Reside in special region of flash memory on the target hardware and provide the means to download a Linux kernel into flash memory and subsequently execute it
- In PC booting Linux begins in the BIOS at address 0xFFFF0

Extracting Linux MBR

- `# dd if=/dev/had of=mbr.bin bs=512 count=1`
- `# od -xa mbr.bin`
  - Reads the first 512 bytes from /dev/had (the first IDE drive) and writes them to the mbr.bin file
  - The od command prints the binary file in hex and ASCII formats

Grand Unified Bootloader (GRUB)

- LILO disadvantages were corrected here
  - LILO uses raw sectors
- Includes knowledge of file system
  - Can load kernel from ext2 or ext3, by making the two-stage into a three-stage boot loader
    - Stage 1 boots a stage 1.5 boot loader that understands the particular file system containing kernel image e.g. reiserfs_stage1_5 (to load from a Reiser journaling file system) or e2fs_stage1_5 (to load from ext2 or ext3)
    - When 1.5 is loaded and running, the stage 2 boot loader can be loaded
    - With stage 2, GRUB can, upon request display a list of available kernels (defined in /etc/grub.conf, with soft links from /etc/grub/menu.1st and /etc/grub.conf)
    - With stage 2 in memory, the file system is consulted, and initrd (default kernel image) are loaded into memory, then invokes kernel image

Kernel

- Compressed, typically in zImage less than 512KB and bzImage big compressed image greater than 512KB
  - Previously compressed with zlib
- Does minimal amount of hardware setup then decompresses the kernel itself within the image and put into high memory
- Routine calls the kernel and boot begins

Init

- After the kernel is booted and initialized, the kernel starts the first user-space application
- First started application is commonly /sbin/init, however, not always
- Can invoke a simple shell script that starts the necessary embedded application

Investigation and Analysis: Application-based

- Logs
- Cache
- Cookies
- File

Logs (Computer Data Logging)

- Utilizes the management of information, handles generation, interpretation, storage and creation of messages for future reference or in compliance with laws, organizational or statutory
- Process of recording events with regards to computer activities
- Provide audit trail that can be used to understand the activity of the system and end-user and to diagnose a problem
- Essential to understand the activities of complex systems
- Written in a log file within the computer itself or in a network server log

Logs

- Access to the computer or logons
- Computer user activities
- Commands/applications used or executed
- Network connection
- Firewall
- Internet/Web browsing
- Websites/URL visited
- Network services /server
- Recordkeeping of everything about computer activities

Logs: Recordkeeping

- Blogs
- Journal
- Logbook
- Chip log (vessel)
- Blackbox (plane)
- Diagnostic trouble codes
- Transaction log
- Video logging

Cache

- A file that is created and stores activities about Web browsing temporarily
- Users does not have to directly access the page recently visited, it is stored temporarily in the hard disk
  - Decreases traffic
  - Saves time
  - Minimize server load
  - Addresses lag

Cache, Computing

- CPU, a small area of fast memory used by central processing unit
- Disk buffer, the small amount of buffer memory present on a hard drive
- Page, the cache of disk pages kept by the operating systems, stored in unused main memory
- Web, a mechanism for the temporary storage of web documetns to increase performance
- DNS, a server in the domain name system which stores queried results for a period of time
- P2P, a technique used to reduce bandwidth costs for content on peer-to-peer networks
- Database, a mechanism used to cache database content in multi-tier applications

CPU Cache

- Old way
  - Data from main memory is rigidly organized in the cache. When one sectionof the cache is full, new data sent to it kicks out the old data
    - Side-channel attack or exploit exist
- Safe way
  - Data from memory is randomly organized in the cache, so there is less of a chance that incoming data will need to kick out the old data
- Newcache, new technology, foils these so-called cache side-channel attacks by randomizing where data is stored in the cache

Web Cache continuous

- Plays a valuable role in improving service quality for a large ranges of Internet users
- Types
  - Browser
    - Keeps a local copy of all recently displayed pages
  - Proxy
    - Shared network device that can undertake Web transactions on behalf of a client, stores the content

Web Cache continuous

- Proxy
  - Deployed as a user invoked option where user nominates a cache server to the browser as a proxy agent
  - User can change, as always the browser to change or to turn off completely its use of it
- Temporary storage of
  - Web documents including HTML pages, images

Web Cache continuous

- Used in various systems
  - Search engine
  - Forward cache
  - Network aware forward cache
  - Reverse cache
  - Web content reuse
  - Web proxy
  - Content delivery network

Web Cache, Control

- HTTP defines three basic mechanisms for controlling caches:
  - Freshness, allows a rsponse to be used without re-chcking it on the origin server
  - Validation, used to check whether a cached response is still good after it becomes stale
  - Invalidation, is usually a side effect of another request that passes through the cache, take POST, PUT or DELETE request

Web Cache, Application

- Apache HTTP Server
- ApplianSys CACHEbox
- Blue Coat ProxySG
- Microsoft Forefront Threat Management Gateway
- Polipo
- Squid
- Untangle
  - Forward and reverse modes capable

Web Cache, History

- TYPE, request that was made, usually a URL for a GET request
- URL, actual request along with the name of the user who requested it
- MODIFIED TIME, the page was loaded into the history
- ACCESS TIME, the history entry was last accessed
- FILENAME, used if redirection needs to occur, when a URL is requested, this will be URL
- DIRECTORY, samething as FILENAME but for the directory, blank on a URL request
- HTTP HEADERS, holds any headers that may have form data or whatnot for POST request.

Cookie, HTTP

- Known also as Web cookie or browser cookie
- Stored in user’s web browser directory
- Notifies the Website of the user’s previous activity
- Designed to be a reliable mechanism for websites to remember the state of the website or activity the user had taken in the past
    - Include clicking on particular buttons, logging in, or a record of which pages were visited by the user even months or years ago

Cookie, HTTP continuation

- Stores passwords and forms filled in by the user
    - – Including credit cards and mailing addresses
- Cookie, with security vulnerabilities, may allow hacker to read data
    - – Use to gain access to user data and credentials

Cookie, HTTP continuation

- Tracking cookie
  - Commonly used as ways to compile long-term records of individuals' browsing histories
    - A major privacy concern especially of the European and US law makers in 2011
- Authentication cookie
  - Common method used by web servers to know whether the user is logged in or not and which account they are logged in under
  - Without such mechanism, the site would not know whether to send a page containing sensitive information or require the user to authenticate by logging in

Cookie’s Terminologies

- Session cookie
- Persistent cookie
- Secure cookie
- HttpOnly cookie
- Third-party cookie
- Supercookie
- Other supercookie
- Zombie

Session Cookie

- In-memory or transient cookie
- Exists in temporary memory only while the user is reading and navigating the website
- It deletes when the user closes the browser

Persistent Cookie

- It outlasts user sessions
- Has max-age set to 1 year, then, within the year, the initial value set in that cookie would be sent back to the server every time the user visited the server or website
- Use to record vital piece of information such as how the user intially came to the website
- Also called tracking cookies

Secure Cookie

- Has secure attribute enabled
  - Used via HTTPS
- Ensures that the cookie is always encrypted when transmitting from client (end-users' computer) to server (website being accessed)
- Less expose to cookie theft via eavesdropping

HttpOnly Cookie

- First party, set with the same domain as your browser's address bar
- Third-party, set with domains different from the one shown on the address bar
- Techniques used by advertiser when loading their ads or visiting their website
  - Then use to build up browsing history of the user across all the website this advertiser has footprints on

Supercookie

- With origin of a TLD or an effective TLD
  - There are TLDs that are public suffixes, not open for reservation by end-users
- Attacker in control of malicious website with domain could set supercookie and potentially disrupt or impersonate legit user requests to such website

Other Supercookie Uses

- Used for tracking technologies that do not rely on HTTP cookies
- Two supercookie mechanisms were found on MS websites (been disabled due to media attention):
  - Cookie syncing that respawned MUID cookies and ETag cookies
  - Capable of re-creating users' cookies or other identifiers after people deleted regular cookies

Zombie Cookie

- Are automatically recreated after a user has deleted them
  - It is accomplished by a script storing the content of the cookie in some other locations such as the
    - Local storage available to Flash content
    - HTML5 storages and other client side mechanisms
- Recreated it from backup stores when the cookie's absence is detected

Cookie Structures

- Contains no more than 255 characters and cannot take up more than 4K of disk space
- Consists of 6 parameters
  - Name of the cookie
  - Value of the cookie
  - Expiration of the cookie (using GMT)
  - Path the cookie is good for
  - Domain the cookie is good for
  - Need for a secure connection to use the cookie
- Name and value are two parameters that are required for successful operation of the cookie

File (MS Outlook Metadata of File)

Tag name	Format of tag	Description
_TentativeReviewCycleID	Number	The unique ID of the revision of the document
_ReviewCycleID	Number	Often the same as _TentativeReviewCycleID, also a unique ID
_EmailSubject	Text	The subject of the e-mail message in which the doucment was sent
_AuthorEmail	Text	The e-mail address of the person who sent the document
_AuthorEmailDisplayName	Text	The display name (what shows up in Outlook) for the e-mail address

Investigation and Analysis: Human-interposition

- Infringement
- Harassment
- Pornography
- Extortion
- Knavery (Dishonesty and unacceptable behavior to dealings and transactions)
- Terrorism
- Cognitive policing
- Social engineering

Investigation and Analysis: Smartphone

- iOS
- Android
- Windows
- Symbian
- Bada

Smartphone

- Have more advance computing capability and connectivity compared to a feature phone
- First, combined the functions of a PDA and a mobile phone with IBM prototype developed in 1972, demo at the COMDEX
  - Later added functionality of portable media players, digicam, pocket videocam and GPS
- Modern, include high-resolution touchscreens and web browsers, high speed data access including WiFi and LTE
- Major driver, development of mobile apps

Smartphone continuation

- Devices combining telephony and computing were conceptualized as early as 1973, were offered for sale beginning 1994
- Term, smartphone, did not appear until 1997
  - Ericsson described its GS 88 Penelope concept as Smart Phone
- Significant advances of smartphone is its API which is capable of running third-party application

Current Smartphones

- Android, Google
- Windows, Microsoft
- Blackberry, RIM
- Symbian, Nokia
- iOS, Apple
- Bada, Samsung
- webOS, HP
- Maemo and MeeGo, embedded Linux

Upcoming Smartphones

- Firefox OS, Mozilla
- Ubuntu, Canonical
- Tizen

iOS

- PL used are C, C++ and Objective C
- OS families are OS X and Unix
- Source model is closed
- Initial release July 29, 2007
- Latest stable release 6.1.3 (build 10B329)
  - March 19, 2013
- Package manager is .deb
- Platforms supported includes
  - ARM (iPhone, iPod Touch, iPad and its mini-version and 2nd generation, higher Apple TV)
  - Apple A4, A5X, A6, A6X

iOS continuation

- Remote wipe, allows owner to remove all data from the device and restore the settings to factory default
  - Accomplished through MobileMe

iOS continuation

- Kernel type is hybrid (XNU, X is not Unix)
  - Apple acquired (from NeXT) and developed for use in the Mac OS X
  - Released as free and open source software
    - Part of the Darwin OS
- XNU’s details can be seen over the internet or at the Apple’s website

Hackers and iOS (especially mentioned)

- Justified it did not allow certain functions
  - MMS, tethering and customization
  - 3rd party applications other than those available from Appstore
- Splintered to developed jailbreaks
- Developed viruses and exploits jailbroken iPhones
  - Exploits invaded the provider's network to seek out and find jailbroken iPhone
- Bricking the phone was the first crude jailbrakes
  - Circumvented security made iPhone replace the OS with one engineered on user-created firmware
    - It allows the device to run unsigned code

iOS File System

- HFS+, developed in 1996 to accommodate increasing disk size at breakneck speed
- HFSX, variation of HFS+

iOS HFS+

- Same as those in Windows-based sectors
- Two blocks
  - Logical blocks, numbered from the 1st to the last on a given volume
    - Static and are the same as the physical blocks, 512 bytes
  - Allocation blocks, used to track data in a more efficient way
    - Reduce fragmentation on an HFS volume, groups of allocation blocks are tied together as clumps
- Date and time, used absolute or known as local time, Unix time is used as well
- Data utilizes a catalog file system or B*tree to organize files

iOS HFS+ continuation

- B*tree uses catalog file and extents overflows in its organization scheme
  - Comprised of nodes, are grouped together in linear fashion, makes data access faster
  - When data is added or deleted, the extents are constantly balanced to keep its efficiency
- Each file created is given a unique number—a catalog ID number
  - Volume header tracks the numbering of the catalog ID and then will increment

iOS HFS+ Structure

- First 1024 bytes are reserved for boot blocks
- Volume header, next 1024 bytes for volume header
  - Signature is H+
- Allocation file, tracks which allocation blocks are in use
- Extents overflow file, tracks allocation blocks that belong to a file's data forks
- Catalog file, maintains all the information in regards to files and folders within a volume

iOS HFS+ Structure, Header Node

- Attributes file
- Startup file
- Data in a volume is stored and tracked
- Alternate volume header
- Last 512 bytes are reserved

iOS HFSX

- A major difference from HFS+ is case sensitive
  - Two files can have the exact the same name

iOS Partitions

- Application, has symbolic links that point to the /var/stacsh
- Etc, has symbolic link to /private/etc
- Tmp, has symbolic link to
- User, has symbolic link
- Var, has symbolic link to /private/var
- Damaged files, contain artifacts of a previous jailbreak
- Bin, contain one command-line binary, `launchctl`
- Cores, empty
- Dev, empty
- Developer, empty

iOS Partitions continuation

- Library, contains system plug-ins and settings
  - Application support: Bluetooth models and PIN
  - Audio
  - Managed preferences: Symbolic linke to Mobile
  - Ringtones: Contains system-installed ringtones
  - Wallpaper: Numerous PNG files and thumbnails (non-evidentiary)
- Private, contains the Etc and Var folders
- Sbin, command-line binaries
- System, library folder that contains system preferences and settings; includes /System/Library/CoreServices/SystemVersion.plist
- Usr, contains more command-line binaries and time zone data

iOS and SQLite

- Relational database management system
- Small and about ~350KB C programming library
- ACID-compliant and implements most of the SQL-92 standard
- Does not guarantee domain integrity
- Popular choice as embedded DB
- Arguably most deployed DB engine
- Has many bindings to PLs

Smartphones and SQLite

- Windows Phone 8
- Symbian
- Maemo
- Android
- Blackberry
- webOS
- OpenBSD

iOS Incident Response

- Gather effectively system information (with backup data find info.plist)
  - Size of the phone
  - OS version
  - Cellular carrier
  - Serial number
  - Model
  - WiFi and bluetooth MAC
  - IEMI
  - ICCID
  - Modem firmware
- Examine applications used including office, social networking, tools and utilities

iOS Incident Response continuation

- With Mac and Windows
  - OS X: /Private/var/db/Lockdown
  - XP: C:\Document and Settings\username\Local Settings\Application Data\Apple Computer\Lockdown
  - Vista: C:\Users\username\AppData\Roaming\Apple Computer\Lockdown
  - 7: C:\ProgramData\Apple\Lockdown
- Plists, contain the authentication keys, assists the examiner in gaining access to the phone without invasive procedures
  - Use to incorporate language in search warrants

iOS Artifacts

- Windows
  - iPodDevices.xml
  - MobileSync backups
  - Lockdown certificates
- Mac
  - Property list
  - MobileSync database
  - Lockdown certificates

iOS Antiforensic

- Not necessarily evading forensic investigation, however, it benefits the end-users' privacy
- iErase
  - Overwrites free space in iPhone and iPod Touch
- Image vaults
- Picture safe, picture vault (different software)
- Incognito web browser, cache may be addressed but not history, check cookies.plist
- Invisible browser
- Tigertext

Cell Tower Data

- Has geospatial data
- Covers cell towers that comes into contact with
- Can be very extensive and can assist in investigations of placing a phone in a general area
  - In the past, were seen in plist
  - At present, in SQLite
- Item of investigative interest, find the ff directory
  - root/Library/Caches/locationd

iOS Network Analysis and Discovery

- com.apple.wifi.plist
- com.apple.network.identification.plist
- consolidated.db (iOS 4 and later)

REPORTS & FINDINGS

TYPES OF REPORTS

- Internal reports
- Affidavits
- Declarations
- Expert reports

Internal Reports

- Reports whose intended audience is local counsel or your manager
- Most common report the forensic investigator will create
- Serious report that, if action is warranted, may be passed on to the general counsel
- Can be used in preparation to legal action that will be undertaken either an affidavit or declarations
- Reports produced by external forensic must always follow general principles: clear and concise that explain in detail the matter at hand

Construction of Internal Report

- Generated by tools may include based on how evidence have been collected e.g. bookmarked and so on which contains:
  - Executive summary
    - Merely the big picture, what to be expected of the report, and may contain subjects
  - Results
    - Details how the report was created and the processes and mechanism used to identify findings and evidences

Affidavits

- Reports whose intended audience is the court
- Such documents are signed in front of a notary and the statements within them are considered as legitimate as if they were sworn under oath
- Stronger documents than declarations Much like a declaration with the same rules applied

Declarations

- Meant to be factual statement
- Reports whose intended audience is the court
- These documents are not signed in front of a notary but are assumed to be factual
- Used by attorneys to support motions they present to the court
  - Motions to, like for instance, compel, temporary restraining orders, motions to dismiss, motions for summary judgment, motions for sanctions or expedited discovery
- Statements should make sense to someone who does not have technical knowledge and conclusions are not lost in a maze of technical details
- Forensic investigators signs these statements and liability is not on the attorney but the former

Construction of Declaration

- Contains the following
  - Introduction of self e.g. name, company and so on
  - Background primer, that makes the investigator qualify to the job e.g. education, professional affiliation, et al
  - Analysis, opinions and reviews result

Expert Report

- Pinnacle of formal reports to a court
- Serve as dissertation to the court on matters at hand
- Shows forensic investigator abilities to:
  - State facts
  - Explain details
  - Clearly support conclusions and opinions
- It is always a good idea to make use of an outside party's formal paper and reports
  - This makes the expert knowledgeable on some published researched paper or standard that is available for public use
  - Citing public works enhances the credibility of the documentation

Construction of Expert Report

- Contains
  - Overview e.g. should state who you have been retained by, the matter name
  - Qualifications, much like the qualification section written in declarations
  - Prior Expert Witness Experience, list of every case expert have been involved with
  - Items reviewed, limits the expert to sources as potential evidence and quote from and show as support to the report
  - Analysis, the bulk of document
  - Conclusion, much like declarations and affidavits, restates opinions and their impacts on the matter at hand

Stakeholders

- Company or employer
- Government, national security
- Prosecution
- Plaintiff
- Witness
- Defendant

Integrity

- Process, replication technique must be established
- Investigator, familiarity of specific task, links laws/policies provisions against what is being carried out or its actions are paramount
  - Can stand to the attacks of credibility being thrown out of the defense, if any

Overall Summary

- Fundamentals of computer and security
  - Understanding
- Computer crime and security technology
  - Instances of exploits / attacks and solutions
- Forensic lab setup and configuration
  - It varies given every situation
  - One thing an investigator or examiner must cope up with
- Computer forensics investigation
  - Processes
  - Mechanisms
  - Instrument / utilities
- Findings and reports
  - Dealing in the court of law