Guidance® SOFTWARE

The World Leader in Digital Investigations™

EnCE® Study Guide
Version 7

Certification Background

The EnCase® Certified Examiner program was created to meet the requests of EnCase® users as well as to provide a recognized level of competency for the examiner. While many different certifications exist, the EnCE provides an additional level of certification and offers a measure of professional advancement and qualifications.

Certain qualifications must be met to enter the certification process. An application and a detailed explanation can be found at:

http://www.guidancesoftware.com/computer-forensics-training-ence-certification.htm

The cost is USD 200.00 US and USD 225.00 International payable by credit card, check, or purchase order. The certification program does not generate profits for Guidance Software; the testing fee covers the cost of the written test provided by ExamBuilder. Once payment has been received and processed, the certification coordinator will e-mail testing instructions to you.

The certification process addresses both EnCase® software (EnCase) and general areas of computer forensics. It involves a written test consisting of 180 questions (174 for international candidates; no legal questions). Two hours are provided to complete the written exam, which is true/false and multiple choice.

Once the Phase I results are received, the certification coordinator will ship the Phase II exam to you at the address you provided on your application. You will be notified via e-mail when your package has been shipped. If you fail the Phase I test, you will be required to wait two (2) months from the date the test was taken before being allowed to re-take the test.

In your Phase II package you will receive a thumb drive that has a "certification" version of EnCase® Forensic, evidence files, and objectives or issues you must address. You must "work" the case, compile your report, and then send the report to Guidance Software for review and grading within 60 days. *If you do not finish the Phase II in the time allotted, you will be required to wait two (2) months from the date that the test was due and restart from the beginning.*

Those who fail the EnCE Phase II exam must wait two (2) months prior to retesting. We will not provide feedback on what was missed on the exam. If after resubmitting Phase II you fail again, you must begin the retesting process from Phase I.

Beginning the Certification Process

The first step toward certification is to review the qualifications and complete the application available at:

http://www.guidancesoftware.com/computer-forensics-training-ence-certification.htm

Submit the completed application to the EnCE certification coordinator at the address provided. Once your application has been received and accepted, you will be provided with login credentials to enroll in Phase I of the testing process.

The test is available in English and Spanish.

Phase I Testing Options

- **ExamBuilder**
  - o ExamBuilder provides online testing services available at all times.
  - o Once you receive e-mail instructions from the certification coordinator, visit the ExamBuilder website at https://testing.exambuilder.com/ to enroll in the Phase I testing process. Follow the instructions for log in and complete the enrollment form.
  - o If you have questions about the enrollment process, contact the Guidance Software certification coordinator at (626) 229-9191, ext. 513 or certification@guidancesoftware.com

- **EnCE® Prep Course**

  o This course is designed for EnCase users preparing for certification. The certification is based upon the skills and knowledge presented in Guidance Software's EnCase® Computer Forensics I and EnCase® Computer Forensics II courses. The EnCE Prep course is *not* intended to be a replacement for these two classes; instead it is a thorough but accelerated review of the covered subjects. Student's cannot waive or substitute the prerequisite attendance of Guidance Software's EnCase Computer Forensics II course when applying to attend the EnCE Preparation course.

  o The Phase I written examination will be administered on the final afternoon of the course in a monitored, timed environment.

  o The examination will be administered *only* at Guidance Software-owned sites in Los Angeles, Chicago, Houston, Washington DC, and London; Authorized Training Partners cannot conduct the test as part of this course.

  o Complete details for this course can be found at:

    http://www.guidancesoftware.com/computer-forensics-training-encase-ence.htm

- **CEIC®**

  o Registered attendees at our annual CEIC conference may elect to take the Phase I test at no additional charge during the conference.

  o All requirements must be met prior to attending CEIC. Anyone interested in taking the Phase I test at CEIC must fill out an application and return it to the certification coordinator via fax, e-mail, or mail one (1) month prior to the conference. Only those who have preregistered and been approved will be admitted to take the Phase I test at CEIC.

  o Please visit www.ceicconference.com for more information.

<u>Maintaining Your Certification</u>

As of January 1, 2012 payment of 75 USD via credit card, check, or purchase order along with a completed renewal form and the supporting documentation detailed as follows is required for renewal completion.

As of November 1, 2008 EnCase Certified Examiners are required to achieve *one* of the following items prior to their expiration date in order to renew. For those who have been certified prior to November 1, 2008, the current expiration date will remain the same, but the new requirements listed below will now apply. Once renewed, the expiration date will be changed to a three-year cycle (for example if renewing in 2009, the next renewal date will not be until 2012, and then every 3 years from then on).

- Attend a minimum of thirty-two (32) credit hours of documented, continuing education in computer forensics or incident response to maintain the certification: [*]

    o The training should either be from Guidance Software, your agency, or an accredited source. Training should be either in a classroom lab setting or online. Proof of attendance should be provided via a certificate, transcript, or official letter.

    o Earn one (1) credit hour for each classroom hour of training and ½ credit hour for each one hour of instruction as a computer forensics or incident-response curriculum instructor.

- Achieve a computer forensics or incident-response related certification within the renewal period. A certificate of completion must be submitted as documentation.

- Attend one CEIC conference within the renewal period. Your certification must be current at the time of the conference and you must attend at least 10 sessions to fulfill the requirement to renew your EnCE. Register online at http://www.ceicconference.com/. Renewal forms will be available at the registration desk during the conference. Please check the box on the renewal form, and registration will be on file with Guidance Software, Inc.

---

[*] Training and teaching hours may be combined to reach the total 32 hours required.
Documentation may be a certificate of completion, official letter from the provider, or transcript.

- Guidelines for submitting renewal credit for attendance at any other computer forensic conference other than CEIC are:
    - Only labs count (seminars or product demos are not considered)
    - Calculate one (1) CPE for every hour in a lab
    - To submit credits please send a copy of the conference agenda and indicate the labs attended and how many CPE each one is worth

- Please do not submit your renewal documents separately. Keep all certificates together and only send them when you have the requirement fulfilled. When you are ready, send the renewal form and any certificates/letters/documents via fax, e-mail, or regular mail.

- The requirements need to have been met within the renewal period. (i.e., if the renewal date is June 1, 2009, the requirements must have been achieved between June 1, 2007 and June 1, 2009.)

Should your certification expire, you will be required to restart the EnCE process from Phase I. *Extensions will not be granted.* If you are unsure of your expiration date, please e-mail: certification@guidancesoftware.com

Complete renewal details are available at:

http://www.guidancesoftware.com/EnCE-Renewal.htm

Other Study Material

This Study Guide highlights the topics contained in the EnCE test, including good forensic practices, legal issues, computer knowledge, knowledge of EnCase, evidence discovery techniques, and understanding file system artifacts. If you need reference materials to prepare for a specific topic or portion of the exam, some recommended study materials are listed below:

EnCase® Computer Forensics I manual by Guidance Software

EnCase® Computer Forensics II manual by Guidance Software

EnCase® Legal Journal by Guidance Software

EnCase® User's Manual by Guidance Software

Handbook of Computer Crime by Eoghan Casey

How Computers Work by Ron White

EnCase® Computer Forensics: The Official EnCE: EnCase Certified Examiner Study Guide by Steve Bunting, Third Edition

EnCE® Preparation Training
- Examining computer-based evidence with EnCase® software (EnCase)
- Computer knowledge
- Good forensic practices
- Legal

Examining Computer-based Evidence
- The EnCase® evidence file
- EnCase® concepts
- The EnCase® environment
- EnCase® Evidence Processor
- Index queries and raw keyword searching
- File signature and hash analysis

The EnCase Evidence File
- Bit stream image of evidence written to a file

The EnCase Evidence File Contains Case Data
- Cannot be changed after evidence file is created
- Contains:
  - Case number
  - Examiner name
  - Evidence number
  - Unique description
  - Date/time of computer system clock
  - Acquisition notes
  - Serial number of physical hard drive

The EnCase Evidence File Verification

- Cyclical Redundancy Check
  - 32-bit CRC for (by default) 64 sectors (32 KB) of data
    - If no compression is used
  - Calculated when evidence file is added to a case and rechecked every time the data block is accessed
  - Verification hash – "digital signature" of all data in evidence file
    - MD5 – 128-bit/32 characters
    - SHA1 – 160 bit
    - Can choose either, one, or neither

The EnCase Evidence File Characteristics

- Logical file that can be renamed and moved
- Can be broken into multiple segments, with a maximum segment size dependent on the file system to which the evidence file is written
- Can be compressed during acquisition and/or reacquired with compression for archival without changing the hash value
- Can be password protected or encrypted and can be reacquired to remove or change password/encryption
- Individual segments can be verified by the CRCs when compression is not used
  - If compression is used, the decompression algorithm is used
- Error granularity is often used to adjust the writing of data to an evidence file, when a read error of the subject media occurs
  - Standard – Size of the data blocks
  - Exhaustive – Sector-by-sector

Evidence File Verification

- Data in the entire evidence file is verified by verification hash compared to the acquisition hash value of the original evidence
- Data in each data block is verified by a CRC when no compression is used
- Both the MD5 and/or SHA-1 hash and CRCs must match for the evidence file to be verified
  - If any compression is used, the compression algorithm is used to verify data blocks

EnCase Concepts

- The case file – .case
  - Compound file containing:
    - Pointers to the locations of evidence files on forensic workstation
    - Results of file signature and hash analysis
    - Bookmarks
    - Investigator's notes
- A case file can contain any number of hard drives or removable media
- The case file should be archived with the evidence cache and evidence files as it contains all of the investigator's notes
  - Use the "Create Package" feature

The Configuration .ini Files

- Contain "global options" used for all cases
- Some configuration .ini files:
  - FileTypes.ini
    - Organizes files into groups by extension; determines which viewer to use
    - File Signature Table
  - Local.ini
    - Global configuration settings
  - Viewers.ini
    - Installed viewers associated to EnCase

The EnCase® Methodology

- Case management
  - Use large-capacity, high-RPM (revolutions per minute) hard drives with single partition for evidence files
  - Wipe the drive to eliminate any claims or arguments of cross-contamination
  - Give the hard drive a unique label prior to acquisitions to differentiate your drives from that of the suspect

o Separate folders for each case are recommended

- Use unique directory names

- Each case requires an Export, Temp, and EvidenceCache folder

    ▪ EvidenceCache – Storing cache files and containers for processed evidence

    ▪ Export – Default folder for exporting evidence

    ▪ Temp – Default temporary folder for file viewing

Evidence Processor

- After adding evidence to a case and confirming that the data is valid and browsable, the first task you undertake is to run the EnCase® Evidence Processor.

- The Evidence Processor lets you run, in a single automated session, a collection of powerful analytic tools against your case data.

- Since you can run the Evidence Processor unattended, you can work on other aspects of the case while this tool is processing data.

- After completion, the case data will be processed and ready for you to begin the important analytic and reporting phases of your investigation.

- The following evidence processing functions are available:

    o Recover folders – Recover files that have been deleted or corrupted on FAT and NTFS volumes

    o Hash analysis – Generate MD5 and/or SHA-1 hash values for files and compare against your case Hash Library

    o Expand compound files – Expand compound and compressed files, such as ZIP, RAR, and GZ

    o Find email – Extract individual messages from e-mail archive files, such as PST (Microsoft® Outlook), NSF (Lotus® Notes), DBX (Microsoft® Outlook Express), EDB (Microsoft® Exchange), AOL, and MBOX

    o Find internet artifacts – Collect Internet-related artifacts, such as browser histories and cached web pages

        - You also have the option to search unallocated space for the Internet artifacts

    o Search for keywords – Search raw (not transcript) text for specific keywords

- o Index text – Create an index for when you need to search for keywords in compound files (Microsoft® Office 2007 and 2010) and across large amounts of data
  - – You can adjust the parameters for index creation, such as the minimum word length to index and whether to use a noise file
- o File signature analysis – Determine if the extension of a file has been altered and whether or not the extension matches the file type as specified by the file's header
- o Protected file analysis – Identify encrypted and password-protected files
- o Creating thumbnails from images – Creates image thumbnails for faster display in the EnCase® GUI

Search Queries – Index

- The case index is created with the EnCase Evidence Processor
- Creating an index will allow you to instantly search for terms in a variety of ways
  - o You can adjust parameters for index creation, such as the minimum word length to index or whether to use a noise file (a file containing specific words to ignore)
- Compared to keyword searches that search on the raw text, index searches will search on the transcript output of the file, which is critical for Microsoft Office 2007 and 2010 files.
- Generating an index can take time, however, the trade-off in time spent creating the index yields a greater payoff with near instantaneous search times.
  - o Guidance Software recommends always indexing your case data

Search Queries – Index

- Once your case has been indexed, keyword searched, tagged, or any combination of the three, you can then search for desired information. To create a unified search do the following:
  - o Go to the Home screen and click the Search button
  - o In the Index window, enter the keyword(s) to query the index
  - o A dynamic list is displayed on the right side of the window, showing the terms in the index and the number of occurrence of a term
    - – This is extremely helpful when crafting a query so that you can immediately see if the term exists in the index

- o EnCase v7 will show you all words in the index that start with the term that you have typed and will dynamically update the list as you type additional letters
  - – At any time you can double-click on a query term and it will show the show the information about that term
- o Click on the Play button to run the query

Raw Keyword Searching

- EnCase for Windows®
  - o Logical raw keyword searching is conducted on allocated files
  - o Physical searching is conducted upon the unallocated areas of the physical disk
  - o Logical search will find a word fragmented between two noncontiguous clusters, whereas a physical search will miss the fragmented word
- Case Sensitive
  - o Not set by default
    - – Selecting will limit hits to exact case of words entered
    - – Can be used with GREP and Unicode
- GREP
  - o Box must be selected for EnCase to use GREP expression, otherwise EnCase will search for the literal entered characters
    - – Can be used with Case Sensitive and Unicode options
- Unicode
  - o Selecting this box will enable EnCase to search for keywords in both ANSI and Unicode
    - – Recommended to be selected for most searches
    - – Can be used with GREP and Case Sensitive options
    - – Unicode uses two bytes for each character allowing the representation of 65,536 characters

Global Regular Expression and Print (GREP)

- ***** An asterisk after a character matches any number of occurrences of that character, including zero. For example, "john,*smith" would match "john,smith," "john,,smith," and "johnsmith."

- **+** A plus sign after a character matches any number of occurrences of that character except zero. For example "john,+smith" would match "john,smith" or "john,,smith," but would NOT match "johnsmith."

- **#** A pound / hash sign matches any numeric character [0-9]. For example ###-#### matches any phone number in the form 327-4323.

- **(ab)** The parentheses allows the examiner to group individual characters together as an AND statement.

- **{m,n}** The curly braces state number of times to repeat, i.e., m to n times

- **|** The pipe is an OR statement and can be used with the parentheses, i.e., (com)|(net)|(org) for the end of an e-mail address.

- **[]** Characters in brackets match any one character that appears in the brackets. For example "smit[hy]" would match "smith" and "smity."

- **[^]** A circumflex at the start of the string in brackets means NOT. Hence [^hy] matches any characters except h and y.

- **[-]** A dash within the brackets signifies a range of characters. For example, [a-e] matches any character from a through e, inclusive.

- **** A backslash before a character indicates that the character is to be treated literally and not as a GREP character.

File Signature and Hash Analysis

- File Signatures
    - ○ Stored in the EnCase® configuration file FileTypes.ini
    - ○ New file signatures can be added manually
    - ○ The terms "file signature" and "file header" mean the same thing, the standard hex characters at the beginning of a certain file type

- File Types – Viewers
  - ○ EnCase uses the FileTypes.ini file to store external viewer information and associate file extensions with external viewers
  - ○ When the examiner double-clicks on a file, EnCase will copy the file to the Temp folder and launch the Windows-associated viewer or user-defined external viewer to read the file

Hash Sets and Hash Library
- Hash sets can be built with one file or any number of selected files
  - ○ The sets contain the hash values of the file(s) in the set and selected metadata
- The hash value of a file is computed only from the logical file independent of the file name, time/date stamps, and the slack space of the physical file
- The Hash Library is built from selected hash sets
  - ○ The examiner can exclude specific hash sets to remain within the scope of the examination
  - ○ You can have two Hash Libraries for each case

Signature and Hash Analysis
- File extensions are compared to the file signature (header) according to the File Types Table
- The hash value of each logical file is computed and compared with the Hash Library composed of the selected hash sets
- Both analyses can be used to help identify suspect files and/or exclude known or benign files
  - ○ The results of both analyses are viewed in the Table view of the Evidence Entry tab

Computer Knowledge
- Understanding data and binary
- The BIOS
- Computer boot sequence
- File systems
- Computer hardware concepts

Understanding Data and Binary

- Bits and Bytes

Bit		Name	Binary
1	=	Bit	1
4	=	Nibble	0000
8	=	Byte	0000-0000
16	=	Word	0000-0000 0000-0000
32	=	Dword	0000-0000 0000-0000
			0000-0000 0000-0000
64	=	Qword	You get the idea

- ASCII and Unicode

  o The ASCII table (American Standard Code for Information Interchange) is based on an 7-bit system

    – The first 128 characters make up the ASCII table and represent alpha/numeric values common punctuation and other values

    – The remaining 128 characters are called "high-bit characters"

    – Together 256 characters can be addressed

  o Selecting Unicode will cause EnCase to search for the keyword in both ASCII and Unicode

    – Unicode uses two bytes for each character, allowing the representation of 65,536 characters

- Basic Input/Output System

  o The BIOS checks and configures the computer system after power is turned on

  o The BIOS chip is usually found on the motherboard

  o The BIOS should be checked during each examination of a computer to check the boot sequence and settings of the internal clock

- Computer boot sequence

File System Fundamentals

- File slack is comprised of drive slack and sector/RAM slack
  - Sector/RAM slack
    - Data from the end of the logical file to the end of that sector
      - The 10-byte file written to a 512-byte sector will have 502 bytes of sector/RAM slack in the same sector that contains the logical data
    - Sector/RAM slack is zeroed out prior to writing it to the drive (00 00)
    - In Windows 95A and older, sector/RAM slack will contain actual data from RAM, and it will be stored on the drive with the file
  - Drive slack
    - Data that is contained in the remaining sectors of a cluster that are not a part of the current logical file
    - A logical file of 10 bytes stored in a four-sector cluster will have three sectors of drive slack
- File Allocation Table
  - Often found on legacy hard drives and removable devices
  - FAT tracks
    - File fragmentation
    - All of the addressable clusters in the partition
    - Clusters marked bad
  - Directory records
    - File name
    - Date/time stamps (Created, Accessed, Written)
    - Starting cluster
    - File logical size
  - A directory (or folder) is a file with a unique header and a logical size of zero
- When a file is deleted from a FAT system
  - 1st character of directory entry changed to E5h
  - FAT entry values change from allocated to unallocated (0)
  - No effect on the data within the clusters

- When EnCase "virtually" undeletes a file
  - o Directory entry read
    - – Obtains starting extent, logical size
    - – Obtains number of clusters by dividing logical size by bytes per cluster
  - o FAT examined to determine if starting cluster/extent is in use
  - o If starting extent is in use, EnCase deems this file to be "Deleted/Overwritten"
- File Allocation Table versions
  - o FAT 16
    - – $2 \wedge 16 = 65{,}536$ total allocation units available (clusters)
  - o FAT 32
    - – $2 \wedge 28 = 268{,}435{,}456$ total allocation units
    - – 4 bits are reserved by Microsoft
  - o Two copies of the FAT are stored for backup purposes
  - o A cluster is composed of multiple sectors
    - – A sector contains 512 user-addressable data bytes

File Systems – exFAT

- exFAT was originally created for USB flash drives and SD cards, but can be used to format volumes under Windows 7
  - o ExFAT is recognized by Windows operating systems XP and after
- The exFAT file system uses 32 bits within the table and has a limit of 4,294,967,285 (232 – 11) cluster addresses
- The exFAT file system uses free space bitmaps to reduce fragmentation and free space allocation/detection issues
  - o Each cluster is tracked in the bitmap
  - o A single bit is used for each cluster on the volume
- When a file is created within exFAT, a different sequence of events may occur than in FAT
  - o If the file is fragmented, then exFAT functions as FAT does
  - o If the file is not fragmented, the FAT is not updated

- Within the directory entries of the exFAT file system, there are multiple, 32-byte records at least three for each directory entry. Each record has an identifier byte:
  - Directory Entry Record – Record ID 85 (hex) – Contains Attributes, Created, Accessed, and Last Written dates/times
  - Stream Extension Record – Record ID c0 (hex) – Contains logical size, starting extent, size of filename, CRC of filename, and whether the FAT is being used to track the clusters allocated to the file
  - File Name Extension Record – Record ID C1 (hex) – Contains the filename in Unicode; additional records may be needed for longer file names
- When a file is deleted, the first bit of the identifier of the record is changed from 1 to 0, changing the identifier to reflect a record not in use
  - It is also possible for the Directory Entry Record to be changed in this manner if the file is renamed
- This means that if the file was fragmented and there was a cluster chain, the chain is not destroyed on deletion
- In exFAT, since allocation status is in the bitmap, there is no need to zero out the cluster run
  - As long as the clusters themselves have not been reused for newer files, it is possible to accurately recover even heavily fragmented files that were deleted because the cluster run would still be intact

File Systems – NTFS

- Master File Table (MFT) – administratively documents all files/folders on NTFS volume
- MFT – comprised of records – 1024 bytes each
- MFT grows but doesn't shrink
- At least one MFT record is allocated to each file and folder on volume
- Bitmap file documents if clusters are allocated or unallocated
- Two types of files: Resident and Nonresident
- File Systems – NTFS
- Resident files
  - Data resides within MFT record for file
  - Data does not begin at the beginning of a sector/cluster
  - Logical size = physical size

- Nonresident files
    - Data not within MFT Record
    - MFT record houses pointers to clusters storing file
    - Pointers in the form of a "data run"
- Both types of files may be hashed as long as logical size is greater than 0

Computer Hardware Concepts
- The computer chassis or case is often incorrectly referred to as the CPU
- The CPU is the Central Processing Unit installed on the motherboard
- Also installed on the motherboard are the Random Access Memory, the Read Only Memory, and add-in cards, such as video cards, Network Interface Cards (NIC), Small Computer System Interface (SCSI) cards
- Integrated Drive Electronics (IDE) and Serial Advanced Technology Attachment (SATA) disk drives can be attached directly to the motherboard with a ribbon cable
- Legacy SCSI hard disk drives require a controller card on the motherboard
- Geometry of hard drives
    - Cylinder/Heads/Sectors (older drives)
        - C x H x S x 512 bytes per sector = total bytes
    - Logical Block Addressing
        - Total number of sectors available x 512 bytes = total bytes
- Master Partition Table
- Volume Boot Record
- Partition tables
- Partition recovery

Good Forensic Practice
- First response
- Acquisition of digital evidence
- Operating system artifacts

First Response

- At the scene
  - Photograph, take notes, sketch
  - Image RAM
    - EnCase® Portable or WinEn
  - Take down the system – whether pull plug or shut down depends on circumstances
    - Shut down – if UNIX/Linux or server
    - Pull plug – it depends on circumstances
- Booting turned-off machines
  - LinEn (Linux EnCase) CD
    - Disk-to-disk imaging with Tableau hardware write-blocker
    - Network cross-over cable
  - EnCase Portable
- Onsite triage
  - Tableau – fastest
    - Gallery view, hash/file signature analysis, logical and physical searches with GREP, copy/unerase, EnScript programs, etc.
  - Network cable preview – fast
    - Gallery view, hash/file signature analysis, logical and physical searches with GREP, copy/unerase, EnScript programs, etc.
      - Evidence Processor available on live devices in EnCase v7.03 and higher
  - EnCase Portable – fast
    - Triage and Collection jobs: Pictures, keyword search, hash sets, filtering with conditions, Snapshot, Internet history
    - Acquisition of digital evidence

Computer Forensic Examiner

- Must be trained
- Must use best forensic practices available
- Must avoid damaging or altering evidence
- Should test and validate computer forensic tools and techniques prior to using them on original evidence

Acquisition of Digital Evidence

- File Systems Supported by EnCase
  - FAT 12, 16, 32, exFAT
  - NTFS
  - EXT2/3/4 (Linux)
  - Reiser (Linux)
  - UFS (Solaris)
  - CDFS (Joliet, ISO9660, UDF)
  - DVD
  - Macintosh HFS/HFS+, Mac OS X (BSD)
  - HP-UX
  - Etc…
- Smartphones and tablets
- If the file system is not supported by EnCase, the examiner can still conduct a physical text search, run EnScript programs for file headers and footers, etc.
- The examiner can also restore the physical drive to a drive of equal or larger size
  - The restored drive is verified by the MD5 and/or SHA1 hash value
- A volume may also be restored to a partition containing the same file system
  - The restored partition is verified by the MD5 and/or SHA1 hash value

Laboratory Procedures

- Cross contamination
  - Wipe lab examination drives
  - Use EnCase® case management methodology
- Chain-of-custody
  - Controlled access to lab area
  - Evidence locker or depository
- Storage
  - Clean, temperature-controlled environment
  - Legacy portable electronic devices may lose battery power, potentially erasing all data

Operating System Artifacts

- Recycler
- NTFS directory entries and structure
- Windows artifacts
  - Recent
  - Link files
  - Desktop
  - Send To
  - Temp
  - Internet Explorer history, cache, favorites, cookies
  - Enhanced metafiles; print spooler
  - Windows 7 – C:\Users\
  - Registry files – global and user account specific
  - Swap file – pagefile.sys
  - Hibernation/Standby file – hyberfil.sys

Legal Issues

- Best Evidence Rule
  - A printout of data stored in a computer can be considered as an original under the Federal Rules of Evidence if it is readable by sight and accurately reflects the stored data
  - Compression of acquired data does not affect admissibility under the Best Evidence Rule
  - If original evidence must be returned to the owner, the forensic image could be considered the Best Evidence
- Daubert/Frye
  - Legal test to determine if a scientific or technical process for obtaining, enhancing, or analyzing evidence is acceptable
- Elements of Daubert
  - Has the process been tested and subject to peer review?
  - Does the process enjoy general acceptance in the related community?
  - Can the findings be duplicated or repeated?
- Commercially available software has a greater opportunity for peer review, testing, and validation

EnCE® Preparation Training

Guidance SOFTWARE

- Examining computer-based evidence with EnCase® software (EnCase)

- Computer knowledge

- Good forensic practices

- Legal

Examining Computer-based Evidence

Guidance SOFTWARE

- The EnCase® evidence file

- EnCase® concepts

- The EnCase® environment

- EnCase ® Evidence Processor

- Index queries and raw keyword searching

- File signature and hash analysis

The EnCase Evidence File

P A G E 3

- Bit stream image of evidence written to a file

- Case Data
  - Cannot be changed after evidence file is created
  - Contains:
    - Case number
    - Examiner name
    - Evidence number
    - Unique description
    - Date/time of computer system clock
    - Acquisition notes
    - Serial number of physical hard drive

The EnCase Evidence File

P A G E 4

- Cyclical Redundancy Check
  - 32-bit CRC for (by default) 64 sectors (32 KB) of data
    - *If no compression is used*
  - Calculated when evidence file is added to case and rechecked every time the data block is accessed

- Verification Hash - "digital signature" of all data in evidence file
  - MD5 – 128-bit/32 characters
  - SHA1 – 160 bit
  - Can choose either, one, or neither

The EnCase Evidence File

Guidance SOFTWARE

PAGE 5

- Logical file that can be renamed and moved

- Can be broken into multiple segments with a maximum segment size dependent on the file system to which the evidence file is written

- Can be compressed during acquisition and/or reacquired with compression for archival without changing the hash value

- Can be password protected or encrypted and can be reacquired to remove or change password/encryption

- Individual segments can be verified by the CRCs when compression is not used

  - If compression, is used the decompression algorithm is used

© 2012 Guidance Software, Inc. All Rights Reserved.

The EnCase Evidence File

Guidance SOFTWARE

PAGE 6

- Error granularity is often used to adjust the writing of data to an evidence file when a read error of the subject media occurs

  - Standard – Size of the data blocks

  - Exhaustive – Sector-by-sector

© 2012 Guidance Software, Inc. All Rights Reserved.

The EnCase Evidence File

- Evidence file verification

  - Data in the entire evidence file is verified by verification hash compared to the acquisition hash value of the original evidence

  - Data in each data block is verified by a CRC when no compression is used

  - Both the MD5 and/or SHA-1 hash and CRCs must match for the evidence file to be verified

    — If any compression is used, the compression algorithm is used to verify data blocks

EnCase Concepts

- The case file - .case
  - Compound file containing:
    — Pointers to locations of evidence files on forensic workstation
    — Results of file signature and hash analysis
    — Bookmarks
    — Investigator's notes

  - A case file can contain any number of hard drives or removable media

  - The case file should be archived with the evidence cache and evidence files as it contains all of the investigator's notes

    — Use the "Create Package" feature

EnCase Concepts

P A G E   9

- The configuration .ini files

  - Contain "Global Options" used for all cases

  - Some configuration .ini files:
    - FileTypes.ini –
      - Organizes files into groups by extension
        - → Determines which viewer to use
      - File Signature Table
    - Local.ini – Global configuration settings
    - Viewers.ini – Installed external viewers associated to EnCase

The EnCase Environment

P A G E   10

- The EnCase ® methodology

  - Case management
    - Use large-capacity, high-RPM (revolutions per minute) hard drives with single partition for evidence files
    - Wipe the drive to eliminate any claims or arguments of cross-contamination
    - Give the hard drive a unique label prior to acquisitions to differentiate your drives from the that of the suspect
    - Separate folders for each case is recommended
      - Use unique directory names
      - Each case requires an Export, Temp, and EvidenceCache folder

The EnCase Environment

Guidance SOFTWARE

PAGE 11

- The EnCase methodology

- **EvidenceCache** – Storing cache files and containers for processed evidence

- **Export** – Default folder for exporting evidence

- **Temp** – Default temporary folder for file viewing

© 2012 Guidance Software, Inc. All Rights Reserved.

Evidence Processor

Guidance SOFTWARE

PAGE 12

- After adding evidence to a case and confirming that the data is valid and browsable, the first task you undertake is to run the EnCase® Evidence Processor

- The Evidence Processor lets you run, in a single automated session, a collection of powerful analytic tools against your case data

- Since you can run the Evidence Processor unattended, you can work on other aspects of the case while this tool is processing data

- After completion, the case data will be processed and ready for you to begin the important analytic and reporting phases of your investigation

© 2012 Guidance Software, Inc. All Rights Reserved.

Evidence Processor

Guidance ®
SOFTWARE

PAGE 13

- The following evidence processing functions are available:
  - **Recover folders** – Recover files that have been deleted or corrupted on FAT and NTFS volumes
  - **Hash analysis** – Generate MD5 and/or SHA-1 hash values for files and compare against your case Hash Library
  - **Expand compound files** – Expand compound and compressed files, such as ZIP, RAR, and GZ
  - **Find email** – Extract individual messages from e-mail archive files, such as PST (Microsoft® Outlook), NSF (Lotus® Notes), DBX (Microsoft® Outlook Express), EDB (Microsoft® Exchange), AOL, and MBOX
  - **Find internet artifacts** – Collect Internet-related artifacts, such as browser histories and cached web pages
    — You also have the option to search unallocated space for the Internet artifacts

© 2012 Guidance Software, Inc. All Rights Reserved.

Evidence Processor

Guidance ®
SOFTWARE

PAGE 14

- **Search for keywords** – Search raw (not transcript) text for specific keywords
- **Index text** – Create an index for when you need to search for keywords in compound files (Microsoft® Office 2007 and 2010) and across large amounts of data
  - You can adjust the parameters for index creation, such as the minimum word length to index and whether to use a noise file
- **File signature analysis** – Determine if the extension of a file has been altered and whether or not the extension matches the file type as specified by the file's header
- **Protected file analysis** – Identify encrypted and password-protected files
- **Creating thumbnails from images** – Creates image thumbnails for faster display in the EnCase® GUI

© 2012 Guidance Software, Inc. All Rights Reserved.

Search Queries - Index

PAGE 15

- The case index is created with the Evidence Processor

- Creating an index will allow you to instantly search for terms in a variety of ways
  - You can adjust parameters for index creation, such as the minimum word length to index or whether to use a noise file (a file containing specific words to ignore)

- Compared to keyword searches that search on the raw text, index searches will search on the transcript output of the file, which is critical for Microsoft Office 2007 and 2010 files

- Generating an index can take time, however, the trade-off in time spent creating the index yields a greater payoff with near instantaneous search times
  - Guidance Software recommends always indexing your case data

Search Queries - Index

PAGE 16

- Once your case has been indexed, keyword searched, tagged, or any combination of the three, you can then search for desired information. To create a unified search do the following:
  - Go to the **Home** screen and click the **Search** button
  - In the Index window, enter the keyword(s) to query the index
  - A dynamic list is displayed on the right side of the window, showing the terms in the index and the number of occurrence of a term
    — This is extremely helpful when crafting a query so that you can immediately see if the term exists in the index
  - EnCase v7 will show you all words in the index that start with the term that you have typed and will dynamically update the list as you type additional letters
    — You can double-click on a query term at any time and it will show the show the information about that term
  - Click on the **Play** button to run the query

Raw Keyword Searching

Guidance®
SOFTWARE

P A G E   17

- EnCase for Windows

  - Logical raw keyword searching is conducted on allocated files

  - Physical searching is conducted upon the unallocated areas of the physical disk.

  - Logical search will find a word fragmented between two noncontiguous clusters, whereas a physical search will miss the fragmented word

Raw Keyword Searching

Guidance®
SOFTWARE

P A G E   18

- Adding Keywords
  - Case Sensitive
    — Not set by default; selecting will limit hits to exact case of words entered; can be used with GREP and Unicode

☑ ANSI Latin - 1	☐ GREP
☐ UTF8	☐ Case Sensitive
☐ UTF7	☐ Whole Word
☑ Unicode	
☐ Unicode Big-endian	

  - GREP
    — Box must be selected for EnCase to use GREP expression, otherwise EnCase will search for the literal entered characters; can be used with Case Sensitive and Unicode

  - Unicode
    — Selecting this box will enable EnCase to search for keywords in both ANSI and Unicode; recommended to be selected for most searches; can be used with GREP and Case Sensitive; Unicode uses two bytes for each character allowing the representation of 65,536 characters

Searching

Guidance SOFTWARE

PAGE 19

■ Global Regular Expression and Print (GREP)

.	A period matches any single character
\xFF	Character represented by its ASCII value in hex. \x09 is a tab. \x0A is a line feed. Both hex digits should be present even if they are 0.
\wFFFF	Unicode 16 bit character
?	The question mark says repeat the preceding character (or set) one or zero times.

GREP Symbols

\wFFFF	Unicode character
\xFF	Hex character
.	Any character
#	Any number [0-9]
?	Repeat zero or one time
+	Repeat at least once
[A-Z]	A through Z
*	Repeat zero+ times
[XYZ]	Either X, Y, or Z
[^XYZ]	Neither X nor Y nor Z
\[	Literal character
(ab)	Group ab together for ?, +, *, |
{m,n}	Repeat m to n times
a|b	Either a or b

© 2012 Guidance Software, Inc. All Rights Reserved.

Searching

Guidance SOFTWARE

PAGE 20

■ GREP

*	An asterisk after a character matches any number of occurrences of that character, including zero. For example, "john,*smith" would match "john,smith," "john,,smith," and "johnsmith."
+	A plus sign after a character matches any number of occurrences of that character except zero. For example "john,+smith" would match "john,smith" or "john,,smith," but would NOT match "johnsmith."
#	A pound / hash sign matches any numeric character [0-9]. For example ###-#### matches any phone number in the form 327-4323.
(ab)	The parentheses allows the examiner to group individual characters together as an AND statement.
{m,n}	The curly braces state number of times to repeat, i.e., *m* to *n* times
|	The pipe is an OR statement and can be used with the parentheses, i.e., (com)|(net)|(org) for the end of an email address.

© 2012 Guidance Software, Inc. All Rights Reserved.

Searching

PAGE 21

- GREP

  [] Characters in brackets match any one character that appears in the brackets. For example "smit[hy]" would match "smith" and "smity."

  [^] A circumflex at the start of the string in brackets means NOT. Hence [^hy] matches any characters except h and y.

  [-] A dash within the brackets signifies a range of characters. For example, [a-e] matches any character from a through e, inclusive.

  **** A backslash before a character indicates that the character is to be treated literally and not as a GREP character.

File Signature and Hash Analysis

PAGE 22

- File Signature Table

  - Stored in the EnCase® configuration file **FileTypes.ini**

  - New file signatures can be added manually

  - The terms "file signature" and "file header" mean the same thing:

    — The standard hex characters at the beginning of a certain file type

File Signature and Hash Analysis

■ File Types – Viewers

● EnCase uses the FileTypes.ini file to store external viewer information and associate file extensions with external viewers

● When the examiner double-clicks on a file, EnCase will copy the file to the Temp folder and launch the Windows-associated viewer or user-defined external viewer to read the file

File Signature and Hash Analysis

■ File signature analysis

Signature Table Analysis – Explained				
Signature / Header	Extension	Comparison	File Types (Signature) Colum	Signature Analysis Colum
LISTED	LISTED	CORRECT	Name of the Signature (JPEG Image Standard)	Match
NOT LISTED	NOT LISTED	N/A	[blank]	Unknown
NOT LISTED	LISTED	INCORRECT	[blank]	Bad Signature
LISTED	LISTED	INCORRECT	Name of the Signature (JPEG Image Standard)	Alias

File Signature and Hash Analysis

- ■ Hash sets and Hash Library
  - ● Hash sets can be built with one file or any number of selected files
    - — The sets contain the hash values of the file(s) in the set and selected metadata
  - ● The hash value of a file is computed only from the logical file independent of the file name, time/date stamps, and the slack space of the physical file
  - ● The Hash Library is built from selected hash sets
    - — The examiner can exclude specific hash sets to remain within the scope of the examination
    - — You can have two Hash Libraries for each case

File Signature and Hash Analysis

- ■ Signature and hash analysis
  - ● File extensions are compared to the file signature (header) according to the File Types Table
  - ● The hash value of each logical file is computed and compared with the Hash Library composed of the selected hash sets
  - ● Both analyses can be used to help identify suspect files and/or exclude known or benign files
    - —The results of both analyses are viewed in the Table view of the Evidence Entry tab

Computer Knowledge

Guidance SOFTWARE®

- Understanding data and binary

- The BIOS

- Computer boot sequence

- File systems

- Computer hardware concepts

Understanding Data and Binary

Guidance SOFTWARE®

- Bits and Bytes

Bit		Name	Binary
1	=	Bit	1
4	=	Nibble	0000
8	=	Byte	0000-0000
16	=	Word	0000-0000 0000-0000
32	=	Dword	0000-0000 0000-0000 0000-0000 0000-0000
64	=	Qword	You get the idea

Understanding Data and Binary

Guidance® SOFTWARE

- ASCII and Unicode
  - The ASCII table (American Standard Code for Information Interchange) is based on an 7-bit system
    - The first 128 characters make up the ASCII table and represent alpha/numeric values common punctuation and other values
    - The remaining 128 characters are called "high-bit characters"
    - Together, 256 characters can be addressed

Decimal	Hexadecimal	Character	Binary Code
0	00	NUL	0000-0000
1	01	SOH	0000-0001
2	02	STX [1]	0000-0010

  - Selecting Unicode will cause EnCase to search for the keyword in both ASCII and Unicode
    - Unicode uses two bytes for each character, allowing the representation of 65,536 characters

The BIOS

Guidance® SOFTWARE

- Basic Input/Output System
  - The BIOS checks and configures the computer system after power is turned on
  - The BIOS chip is usually found on the motherboard
  - The BIOS should be checked during each examination of a computer to check the boot sequence and settings of the internal clock

Computer Boot Sequence

Guidance
SOFTWARE

Power Button

The BIOS immediately runs POST and then prepares the system for the first program to run.

Add-in cards such as SCSI drive controller cards can have a BIOS on the card that loads at this time. These BIOS normally detect devices and load information into the BIOS data area in RAM.

BIOS

POST

POST (Power On Self Test) checks the system board, memory (RAM), keyboard, floppy disk, hard disk, etc., for presence and reliability.

BIOS FROM ADD-IN CARDS

LOAD RAM WITH BIOS DATA

A special RAM BIOS data area of 256 bytes contains the results of the system check identifying the location of attached devices.

Boot Sequence?

Computer Boot Sequence

Guidance
SOFTWARE

A:

Boot Sequence?

C:

Present?

No

Other Devices

Master Boot Record

Yes

May display error or shift to boot another device

Go to Boot Partition

Boot Record

Boot Record?

No

Io.sys

Yes

Msdos.sys

Io.sys

Config.sys

Msdos.sys

Optional

Command.Com

Config.sys

Autoexec.bat

Command.Com

Autoexec.bat

File System Fundamentals

P A G E   33

Logical and Physical File Size

My Pic.jpg

Physical File bytes
(1 cluster)

File Slack

Logical File
3045 Bytes
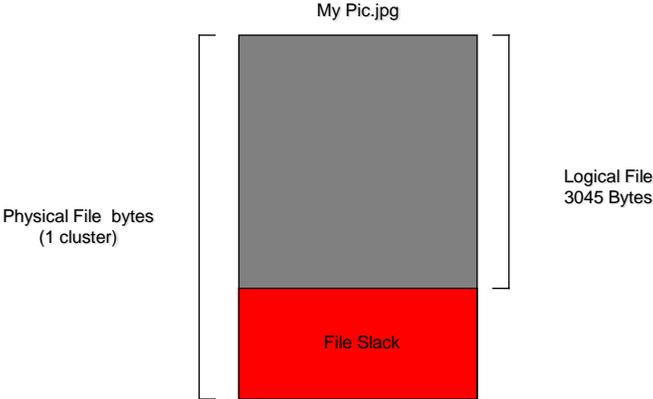
© 2012 Guidance Software, Inc. All Rights Reserved.

File System Fundamentals - Slack Space

P A G E   34

- File slack is comprised of drive slack and sector/RAM slack

  - Sector/RAM Slack

    — Data from the end of the logical file to the end of that sector

      ▪ The 10-byte file written to a 512-byte sector will have 502 bytes of sector/RAM slack in the same sector that contains the logical data

    — Sector/RAM slack is zeroed out prior to writing it to the drive (00 00)

    — In Windows 95A and older sector/RAM slack will contain actual data from RAM, and it will be stored on the drive with the file

  - Drive slack

    — Data that is contained in the remaining sectors of a cluster that are not a part of the current logical file

      ▪ A logical file of 10 bytes stored in a four-sector cluster will have three sectors of drive slack

© 2012 Guidance Software, Inc. All Rights Reserved.

File Systems - FAT

- File Allocation Table
  - Often found on legacy hard drives and removable devices
  - FAT tracks
    — File fragmentation
    — All of the addressable clusters in the partition
    — Clusters marked bad
  - Directory records
    — File name
    — Date/time stamps (Created, Accessed, Written)
    — Starting cluster
    — File logical size
  - A directory (or folder) is a file with a unique header and a logical size of zero

File Systems - FAT

Name	Cluster	Length	Accessed	Written	Created
.					
. .					
MyNote.TXT	1000	952	8/25/00	8/22/00	8/22/00
Picture1.GIF	1002	890	8/25/00	6/15/98	6/15/98
Picture2.JPG	1004	5000	8/25/00	7/12/99	7/12/99
Job Search.DOC	24888	11000	8/25/00	8/25/00	8/1/00
Report.DOC	79415	34212	8/25/00	7/31/00	6/20/00
Personal Letter.DOC	88212	10212	8/25/00	8/25/00	8/25/00

Directory Entry
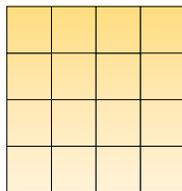
Clusters (Allocation Units)

File Allocation Table

File Systems - FAT
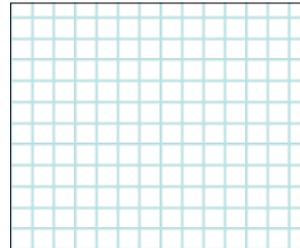
Guidance
SOFTWARE

Directory Entry

Name	Cluster	Length
MyNote.TXT	1000	952
Picture1.GIF	1002	890
Picture2.JPG	1004	5000
Job Search.DOC	24888	11000
Report.DOC	79415	34212
Personal Letter.DOC	88212	10212

File Systems - FAT

Guidance
SOFTWARE

File Allocation Table
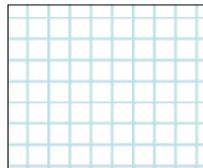
2	3	4	5	6	7
EOF	EOF	EOF	EOF	EOF	EOF

1000	1001	1002	1003	1004	1005
EOF	0	EOF	0	1005	EOF

Guidance SOFTWARE®

FAT

PAGE 39

- When a file is deleted from a FAT system
  - 1st character of directory entry changed to E5h
  - FAT entry values change from allocated to unallocated (0)
  - No effect on the data within the clusters

- When EnCase "virtually" undeletes a file
  - Directory entry read
    — Obtains starting extent, logical size
    — Obtains number of clusters by dividing logical size by bytes per cluster
  - FAT examined to determine if starting cluster/extent is in use
  - If starting extent is in use, EnCase deems this file to be "Deleted/Overwritten"

Guidance SOFTWARE®

File Systems

PAGE 40

- File Allocation Table
  - FAT 16
    — $2 \wedge 16 = 65,536$ total allocation units available (clusters)
  - FAT 32
    — $2 \wedge 28 = 268,435,456$ total allocation units
    — 4 bits are reserved by Microsoft
  - Two copies of the FAT are stored for backup purposes.
  - A cluster is composed of multiple sectors. A sector contains 512 user-addressable data bytes

File Systems - exFAT

Guidance
SOFTWARE

PAGE 41

- exFAT was originally created for USB flash drives and SD cards, but can be used to format volumes under Windows 7
  - ExFAT is recognized by Windows operating systems XP and after
- The exFAT file system uses 32 bits within the table and has a limit of 4,294,967,285 (232 – 11) cluster addresses
- The exFAT file system uses free space bitmaps to reduce fragmentation and free space allocation/detection issues
  - Each cluster is tracked in the bitmap
  - A single bit is used for each cluster on the volume
- When a file is created within exFAT, a different sequence of events may occur than in FAT
  - If the file is fragmented, then exFAT functions as FAT does
  - If the file is not fragmented, the FAT is not updated

File Systems - exFAT

Guidance
SOFTWARE

PAGE 42

- Within the directory entries of the exFAT file system, there are multiple, 32-byte records at least three for each directory entry. Each record has an identifier byte:
  - **Directory Entry Record** – Record ID 85 (hex) – Contains Attributes, Created, Accessed, and Last Written dates/times
  - **Stream Extension Record** – Record ID c0 (hex) – Contains logical size, starting extent, size of filename, CRC of filename, and whether the FAT is being used to track the clusters allocated to the file
  - **File Name Extension Record** – Record ID C1 (hex) – Contains the filename in Unicode
    — Additional records may be needed for longer file names

File Systems - exFAT

- When a file is deleted, the first bit of the identifier of the record is changed from 1 to 0, changing the identifier to reflect a record not in use
  - It is also possible for the Directory Entry Record to be changed in this manner if the file is renamed
- This means that if the file was fragmented and there was a cluster chain, the chain is *not* destroyed on deletion
- In exFAT, since allocation status is in the bitmap, there is no need to zero out the cluster run
  - As long as the clusters themselves have not been reused for newer files, it is possible to accurately recover even heavily fragmented files that were deleted because the cluster run would still be intact

File Systems - NTFS

- Master File Table (MFT) – Administratively documents all files/folders on NTFS volume
  - MFT – Comprised of records – 1024 bytes each
  - MFT grows but doesn't shrink
  - At least one MFT record is allocated to each file and folder on volume
- Bitmap file documents if clusters are allocated or unallocated
- Two types of files: Resident and Nonresident

File Systems - NTFS

Guidance SOFTWARE

- Resident files
  - Data resides within MFT record for file
  - Data does not begin at the beginning of a sector/cluster
  - Logical size = physical size

- Nonresident files
  - Data not within MFT Record
  - MFT record houses pointers to clusters storing file
  - Pointers in the form of a "data run"

- Both types of files may be hashed as long as logical size is greater than 0

Computer Hardware Concepts

Guidance SOFTWARE

- The computer chassis or case is often incorrectly referred to as the CPU

- The CPU is the Central Processing Unit installed on the motherboard

- Also installed on the motherboard are the Random Access Memory, the Read Only Memory, and add-in cards, such as video cards, Network Interface Cards (NIC), Small Computer System Interface (SCSI) cards

- Integrated Drive Electronics (IDE) and Serial Advanced Technology Attachment (SATA) disk drives can be attached directly to the motherboard with a ribbon cable

- Legacy SCSI hard disk drives require a controller card on the motherboard

Computer Hardware Concepts

Guidance
SOFTWARE

- Geometry of hard drives
  - Cylinder/Heads/Sectors (older drives)
    — C x H x S x 512 bytes per sector = total bytes
  - Logical Block Addressing
    — Total number of sectors available x 512 bytes = total bytes

- Master Partition Table

- Volume Boot Record

- Partition Tables

- Partition Recovery

Good Forensic Practice

Guidance
SOFTWARE

- First response

- Acquisition of digital evidence

- Operating system artifacts

First Response

- At the Scene
  - Photograph, take notes, sketch
  - Image RAM
    — EnCase® Portable or WinEn
  - Take down the system – whether pull plug or shut down depends on circumstances
    —Shut Down – if UNIX/Linux or server
    —Pull Plug – it depends on circumstances

First Response

- Booting turned-off machines
  - LinEn (Linux EnCase) CD
    — Disk-to-disk imaging with Tableau hardware write-blocker
    — Network cross-over cable
  - EnCase Portable

First Response

Guidance SOFTWARE

■ Onsite triage

● Tableau – Fastest

— Gallery view, hash/file signature analysis, logical and physical searches with GREP, copy/unerase, EnScript programs, etc.

● Network cable preview – Fast

— Gallery view, hash/file signature analysis, logical and physical searches with GREP, copy/unerase, EnScript programs, etc. Evidence Processor available on live devices in EnCase® v7.03 and higher

● EnCase Portable – Fast

— Triage and Collection jobs: Pictures, keyword search, hash sets, filtering with conditions, Snapshot, Internet history

Acquisition of Digital Evidence

Guidance SOFTWARE

■ Computer Forensic Examiner

● Must be trained

● Must use best forensic practices available

● Must avoid damaging or altering evidence

● Should test and validate computer forensic tools and techniques prior to using them on original evidence

Acquisition of Digital Evidence

- File systems supported by EnCase
  - FAT 12, 16, 32, exFAT
  - NTFS
  - EXT2/3/4 (Linux)
  - Reiser (Linux)
  - UFS (Solaris)
  - CDFS (Joliet, ISO9660, UDF)
  - DVD
  - Macintosh HFS/HFS+, Mac OS X (BSD)
  - HP-UX
  - Etc…
- Smartphones and tablets

Acquisition of Digital Evidence

- File systems supported by EnCase

  - If the file system is not supported by EnCase, the examiner can still conduct a physical text search, run EnScript programs for file headers and footers, etc.

  - The examiner can also restore the physical drive to a drive of equal or larger size

    — The restored drive is verified by the MD5 and/or SHA1 hash value

  - A volume may also be restored to a partition containing the same file system

    — The restored partition is verified by the MD5 and/or SHA1 hash value

Acquisition of Digital Evidence

P A G E 55

- Laboratory procedures
  - Cross contamination
    - — Wipe lab examination drives
    - — Use EnCase® case management methodology
  - Chain-of-custody
    - — Controlled access to lab area
    - — Evidence locker or depository
  - Storage
    - — Clean, temperature-controlled environment
    - — Legacy portable electronic devices may lose battery power, potentially erasing all data

Operating System Artifacts

P A G E 56

- Recycler
- NTFS directory entries and structure
- Windows artifacts
  - Recent
  - Link files
  - Desktop
  - Send To
  - Temp
  - Internet Explorer history, cache, favorites, cookies
  - Enhanced MetaFiles; Print Spooler
  - Windows 7 – C:\Users\

Operating System Artifacts

Guidance® SOFTWARE

PAGE 57

■ Windows artifacts (*continued*)

● Registry files – global and user account specific

● Swap file – pagefile.sys

● Hibernation/Standby file – hyberfil.sys

© 2012 Guidance Software, Inc. All Rights Reserved.

Legal Issues

Guidance® SOFTWARE

PAGE 58

■ Best evidence rule

● A printout of data stored in a computer can be considered as an original under the Federal Rules of Evidence if it is readable by sight and accurately reflects the stored data

● Compression of acquired data does not affect admissibility under the Best Evidence Rule

● If original evidence must be returned to the owner, the forensic image could be considered the Best Evidence

© 2012 Guidance Software, Inc. All Rights Reserved.

Legal Issues

Guidance SOFTWARE

PAGE 59

- Daubert/Frye
  - Legal test to determine if a scientific or technical process for obtaining, enhancing, or analyzing evidence is acceptable

- Elements of Daubert
  - Has the process been tested and subject to peer review?
  - Does the process enjoy general acceptance in the related community?
  - Can the findings be duplicated or repeated?

- Commercially available software has a greater opportunity for peer review, testing, and validation