United States Secret Service

BASIC COMPUTER FORENSIC ANALYSIS

INITIAL REVIEW OF SEIZED IMAGES

Special Agent
Sheila. M. Gorriz
Sheila.Gorriz@usss.dhs.gov
Miami Field Office

MECTF@usss.dhs.gov

Organization & Mission
Of the U.S. Secret Service today

- ***PROTECTION***

- President
- Vice President
- Foreign Dignitaries
- Former Presidents
- Other Officials

INVESTIGATIONS

- Intelligence
- Counterfeit Obligations
- Financial Crimes
- Electronic Crimes

USSS Enhanced Mission

The Director of the United States Secret Service shall take appropriate actions to develop a national network of electronic crime task forces, based on the New York Electronic Crimes Task Force model, throughout the United States, for the purpose of preventing, detecting, and investigating various forms of electronic crimes, including potential terrorist attacks against critical infrastructure and financial payment systems.

Public Law 107-56, Section 105

- Impact on the Community
- Investigations & Prosecutions
- Forensics
- New Technology
- Research & Development
- Academia
- Legislation

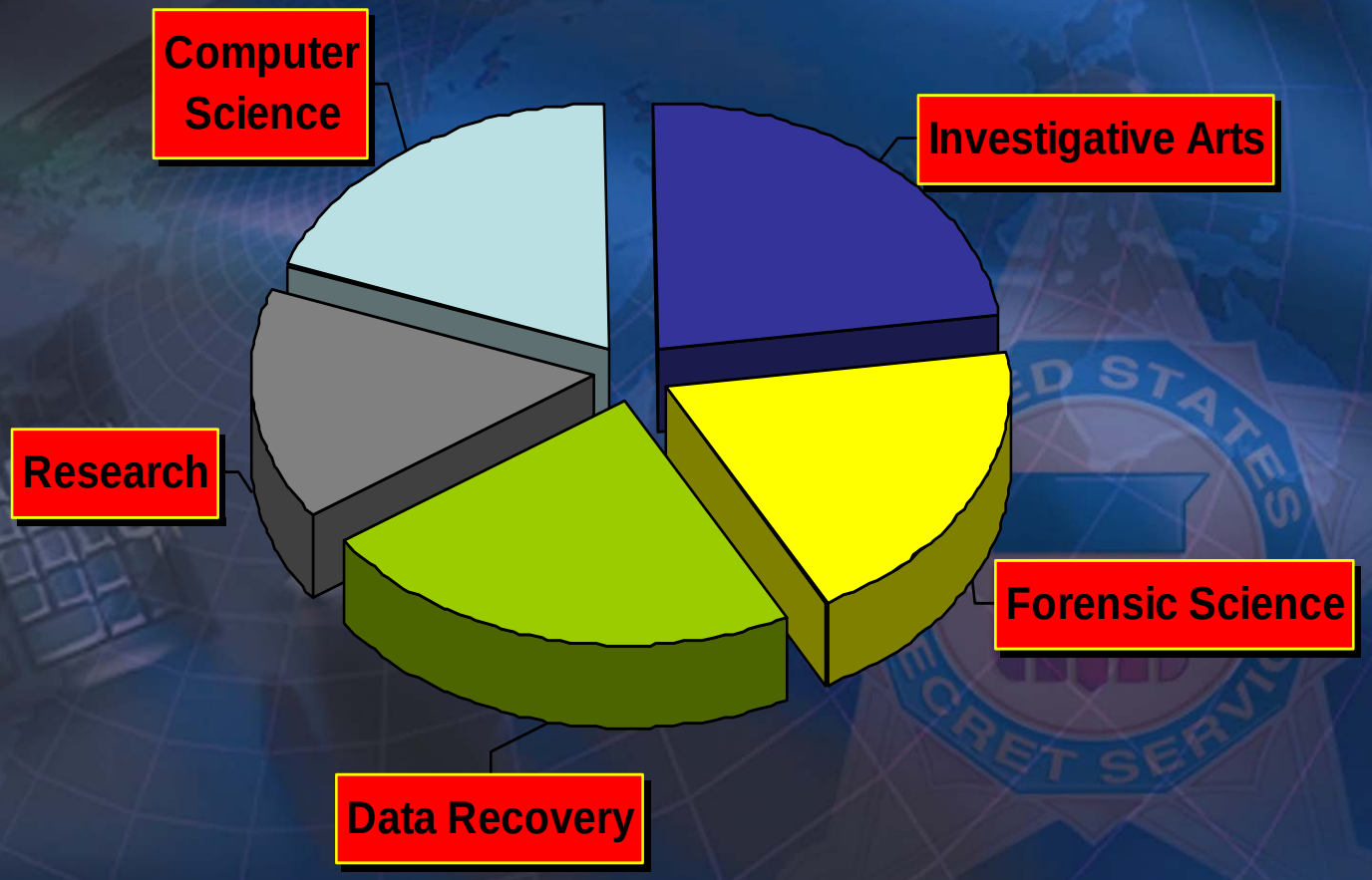
Cooperation with Foreign Authorities

BASIC COMPUTER FORENSIC ANALYSIS

Digital Forensics Defined

The preservation, identification, extraction, analysis, and interpretation of digital data, with the expectation that the findings will be introduced in a court of law.

What is Computer Forensics?



Practical Computer Forensics

- **Reveals <u>direct evidence</u> on the machine.**
- **Associates a machine with questionable data.**
- **Reveals investigative leads.**
- **Reveals circumstantial evidence which corroborates or refutes allegations or alibis.**
- **Reveals Behavioral Evidence.**

Practical Computer Forensics

- **Requires a close enough relationship with the investigation to understand the goals and nuances of the examination;**

Requires enough distance to remain objective and impartial.

Competency + Objectivity + Reliability = Good Forensics

Applied Computer Forensics

Use of the computer *as a tool* or weapon
Use of the computer *as a repository* of evidence
Use of the computer as a *communication device*
Use of the computer *as a target*

Hard Drive Storage Issues

- Dramatically increases the time it takes to acquire and image of a suspect drive.
- Causes severe problems with archiving suspect hard drive images (A 80 Gb drive will fill 128 CD-ROM disks without compression). *An 80GB HD is equivalent to 20,971,520 pages of paper = about 41,943 reams of paper = You would need about 3 semi trucks to carry that.*
- Severely hinders the investigators ability to search the computer evidence.
- Greatly increases the time it takes to complete a computer forensic analysis.

WHAT CAN WE FIND DURING AN EXAM?

-DELETED FILES

-TEXT FRAGMENTS

-ENHANCED METAFILES (PREVIOUSLY PRINTED FILES)

-ENHANCED METADATA (EMBEDDED INFORMATION)

-DATE/TIME STAMP INFORMATION

-E-MAIL MESSAGES AND CHAT LOGS

-INTERNET USAGE INFORMATION (HISTORY)

-VARIOUS ARCHIVE/COMPRESSED FILES (ZIP)

-BASE-64 ENCODED E-MAIL ATTACHMENTS

-IMAGES (ACTIVE AND DELETED)

Volatility Considerations

- **File removal/transfer**
- **Drive destruction or removal**
- **Intentional Data Destruction**

Digital Evidence Awareness

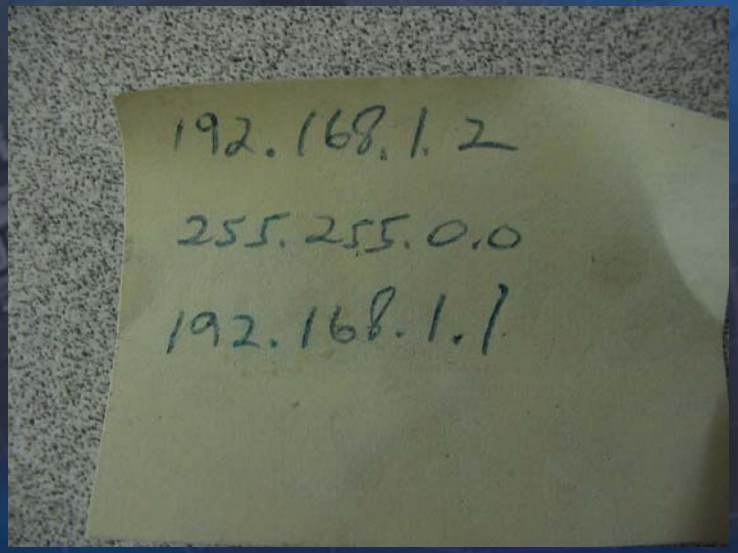
The biggest mistake a officer/investigator can make is to fail to see the evidentiary possibilities!

Digital Evidence Awareness

- Consider the computer as a communication tool.
- Consider the computer as a personal diary or activity log.
  - Diary of interests?
  - Hobbies?
  - Shopping hobbies?
  - Thoughts - Fantasies?

Digital Evidence Awareness

- **Non-electronic evidence**
  - Fingerprints
  - Hair
  - Body fluids (wear gloves?)



Case warranty seals

Bills and other printed data

Phone number jack information

Paper (with Passwords)

INITIAL REVIEW OF SEIZED IMAGE

Initial Review Process

- MILESTONES

- ***Sit down with case agent to determine scope of examination!!!***
- Identify legal authority to search the media (court order, consent, other….)
- Obtain explanation of the case
- Determine evidence expected on media

- ***Create Destination Folder on Forensic Computer / Analysis Hard Drive***
- Identify which drive will hold the image file of the evidence hard drive
- Create a folder on this hard drive to save the image (normally the slave internal forensic hard drive)
- Inside this folder, create two additional folders (***Export*** and ***Trash***)

Initial Review Process

- ***Start EnCase and Open New Case***
- Initiate under ***File*** and then select ***New***
- Fill in Create New Case window fields
- Identify Default Export Folder (using the drop-down menu button, identify the ***Export*** folder created at the beginning of this process)
- Identify Temporary Folder (using the drop-down menu button, identify the ***Trash*** folder created at the beginning of this process)
- Fill in Create New Case window fields

- ***Add Evidence File***
- Initiate under ***File*** and then select ***Add*** and ***Evidence File***
- Select evidence file created during acquisition process

Options

Case Options | Global | NAS | Colors | Fonts | EnScript | Storage Paths

Name
GallileoTest

Examiner Name
SA Brian C. Russell

Default Export Folder
C:\Documents and Settings\qwerty\Desktop\Presentation\Cases\Gallileo\Galli ...

Temporary Folder
C:\Documents and Settings\qwerty\Desktop\Presentation\Cases\Gallileo\Galli ...

OK | Cancel

Options

Case Options | Global | NAS | Colors | Fonts | EnScript | Storage Paths

Auto Save Minutes (0 = None)
10

Show True
Yes

Show False
No

- [ ] Use Recycle bin for cases
- [x] Enable Picture Viewer
- [x] Enable ART and PNG image display
- [ ] Flag Lost Files

Invalid picture timeout (seconds)
12

Default Codepage
1252

Date Format

- (•) MM/DD/YY
- ( ) DD/MM/YY
- ( ) Other MM/dd/yy

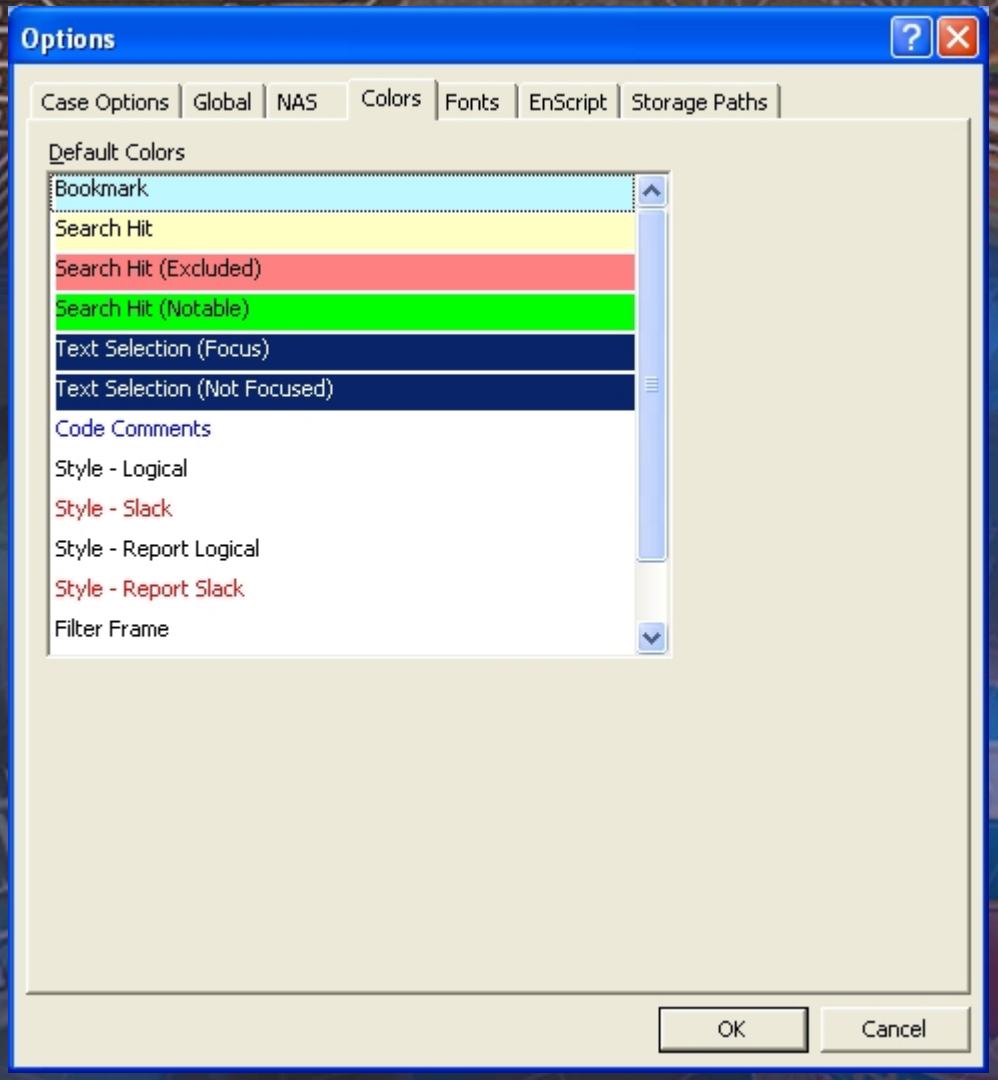
Current Day
12/03/06

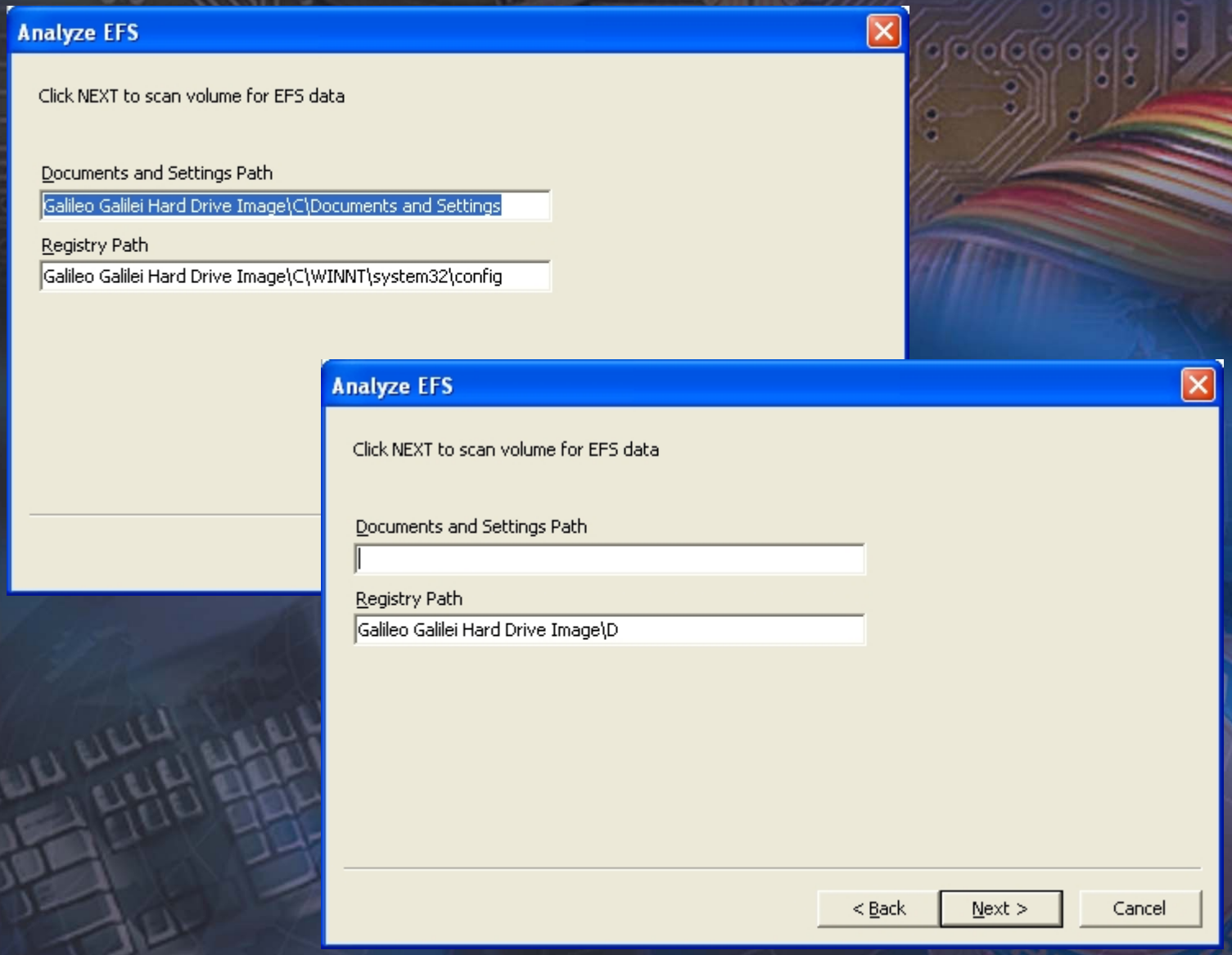
Time Format

- (•) 12:00:00PM
- ( ) 24:00:00
- ( ) Other hh':'mm':'sstt

Current Time
06:00:54PM

OK | Cancel

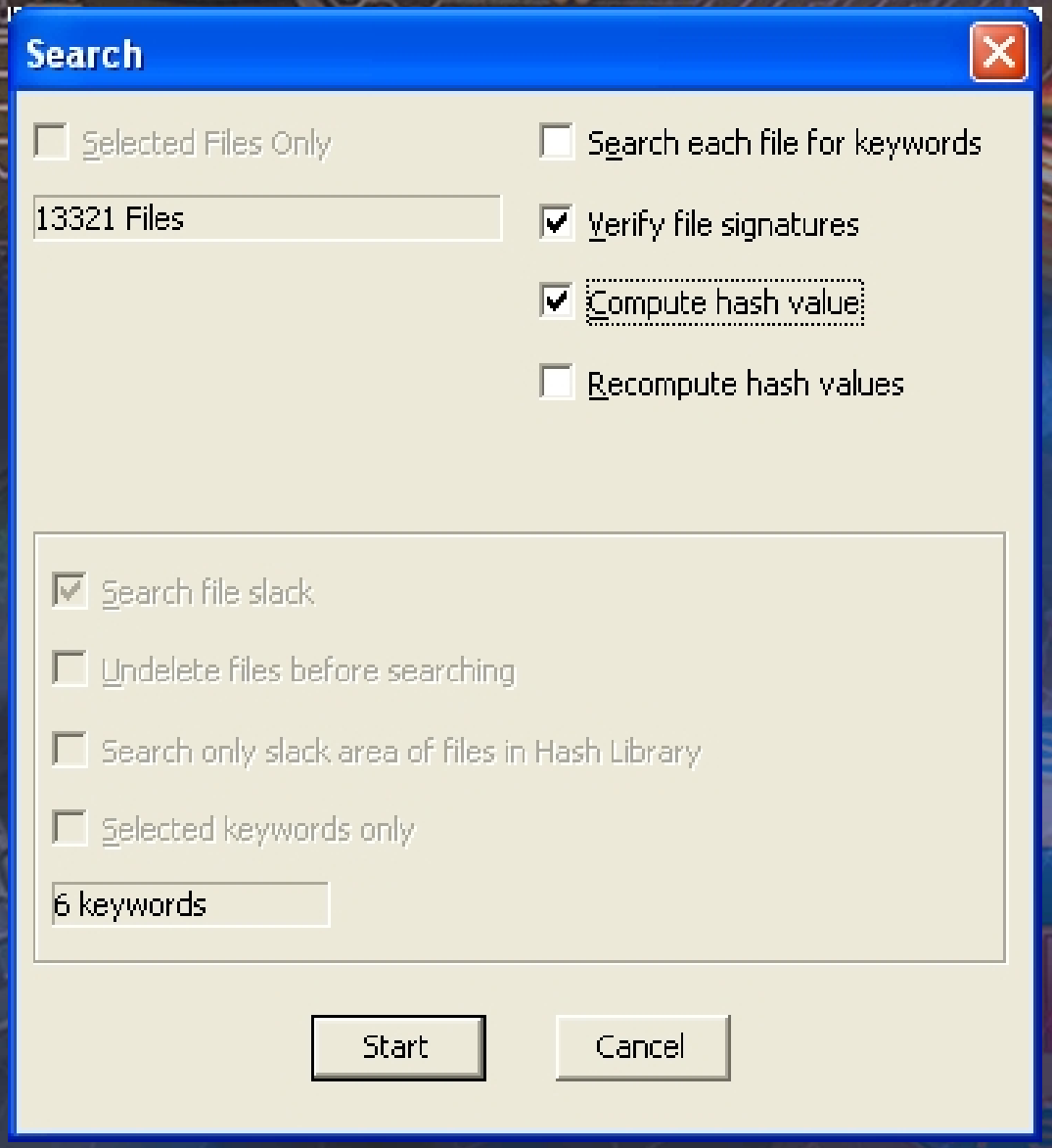

Options
Case Options
Global
NAS
Colors
Fonts
EnScript
Storage Paths
Default Colors
Bookmark
Search Hit
Search Hit (Excluded)
Search Hit (Notable)
Text Selection (Focus)
Text Selection (Not Focused)
Code Comments
Style - Logical
Style - Slack
Style - Report Logical
Style - Report Slack
Filter Frame
OK
Cancel


Analyze EFS
Click NEXT to scan volume for EFS data
Documents and Settings Path
Galileo Galilei Hard Drive Image\C\Documents and Settings
Registry Path
Galileo Galilei Hard Drive Image\C\WINNT\system32\config
Analyze EFS
Click NEXT to scan volume for EFS data
Documents and Settings Path
Registry Path
Galileo Galilei Hard Drive Image\D
< Back
Next >
Cancel

Initial Review Process

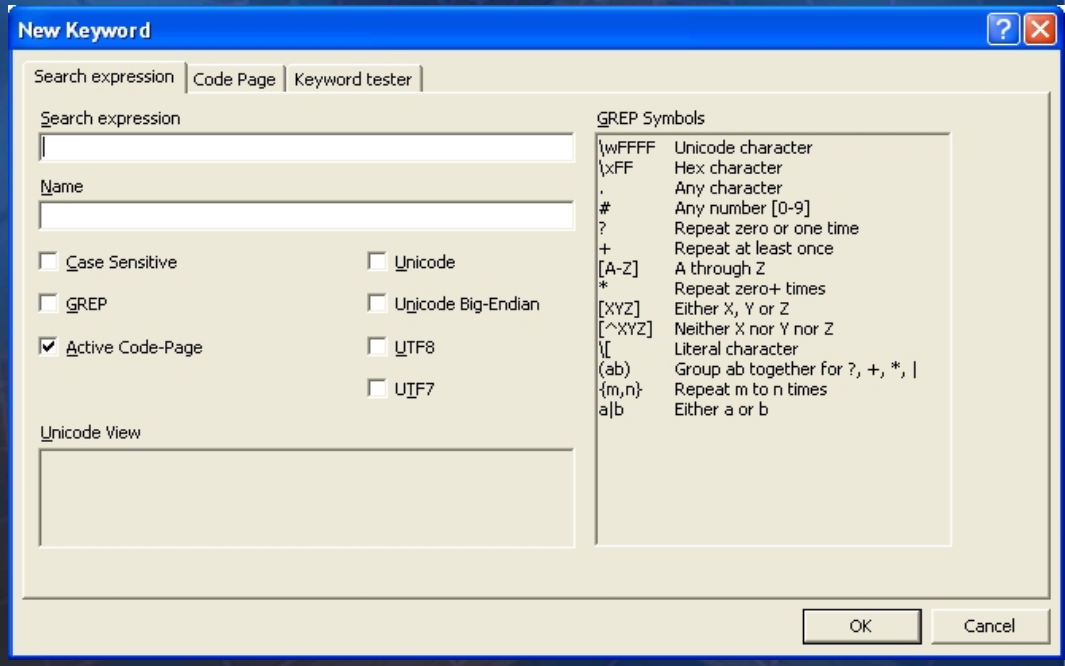
- ***Recover Lost Folders***
- Click on the volume you want to search with your **right** mouse button (each volume must be searched separately)
- Select ***Recover Folders***
- Review resulting information listed in the Recovered Folders virtual folder located at the bottom of the volume directory

- ***Compute Hash Values / Signatures*** (**used to filter out known files**)
- Initiate under ***Tools and then select Search***
- Select ***Verify Signature Files*** and ***Compute Hash Value***, then ***Begin Analysis***
- Review resulting information listed in ***Table*** window in EnCase


Search
Selected Files Only
13321 Files
Search each file for keywords
Verify file signatures
Compute hash value
Recompute hash values
Search file slack
Undelete files before searching
Search only slack area of files in Hash Library
Selected keywords only
6 keywords
Start
Cancel

Initial Review Process

- ***Run Keyword / GREP Searches***
- Found in the ***Keywords*** section of the EnCase program
- Typically used to identify occurrences of:
- Victims' names
- Suspects' names
- SSN's
- Credit card numbers
- Telephone numbers
- Other miscellaneous identifiers



Initial Review Process

- ***Run E-Script Searches***
- Designed to obtain hidden, deleted or unallocated information
- Common files that require E-Script searches:
- .EMF files (previously printed documents no longer visible in the normal file structure of an operating system)
- Deleted image files (.BMP, .JPG, etc…)
- Internet history / links (obtained from Internet .DAT files)
- E-mail addresses (will identify e-mail addresses with 2- or 3-level domain name e-mail addresses)
- ***Gallery View Searches***
- Useful in quickly identifying image files on smaller storage media

Initial Review Process

- ***Complete Text Index (using FTK)***
- ***NOTE:*** Do not run while initially adding evidence to a case file (will lock up forensic CPU)
- FTK has the capability of indexing every text string located on a storage media
- Allows an examiner to conduct instantaneous string searches

- ***Search E-mail Files (using FTK)***
- FTK has a strong native ability to recover complete e-mails from storage media
- (much stronger capability than Encase)

WWW Links

- MECTF@USSS.DHS.GOV
- www.ectaskforce.org
- www.secretservice.gov
- www.ectf.usss.gov
- www.cert.org
- www.forwardedge2.com
- www.forwardedge2.com/pdf/bestPractices.pdf

Special Agent
Sheila Gorriz

United States Secret Service

Miami Field Office

(305) 863-5000

Sheila.Gorriz@usss.dhs.gov

MECTF@usss.dhs.gov

Q&A