

Guidance
SOFTWARE

The World Leader in Digital Investigations™

Forensic Basics

Fred B. Cotton
Solutions Consultant
Guidance Software, Inc.
2200 Powell Street, Suite 800
Emeryville, CA 94608
(510)705-3528
Fred.cotton@guidancesoftware.com

© 2009 Guidance Software, Inc. All Rights Reserved.

Guidance
SOFTWARE

Forensic Process

PAGE 1

- The Forensic Examiner must strive to collect and preserve digital evidence in a forensically sound manner.
- The protocols used should;
 - Be Repeatable
 - Be Defensible
 - Protect the data from tampering
 - Protect the metadata
- Court evidence must be the "best evidence."
- In the interest of time, this will be a high-level overview of the Forensic process.

© 2009 Guidance Software, Inc. All Rights Reserved.

Guidance
SOFTWARE

Forensic Protocols

PAGE 2

- Examiner training and certification.
- The Examiner should follow a set of tested protocols in each case.
- The protocols are designed to maintain the integrity of the digital evidence from identification through collection and preservation.
- Case notes are a critical part of the protocol.
- Good documentation allows another Examiner, using the same evidence and the same protocols to arrive at the same result.

© 2009 Guidance Software, Inc. All Rights Reserved.

Before the Case Galdance SOFTWARE

PAGE 3

- Establish good case management.
- Establish a good template and standard glossary of terms.
- Document your forensic platform.
 - Tested OS
 - Tested forensic tools (version and build)
 - Documented licensing
 - Current anti-virus
 - Clean storage media
- Avoid contamination.
 - Evidence storage and chain of custody
 - Maintain a clean forensic environment
 - Establish a work flow

© 2009 Guidance Software, Inc. All Rights Reserved.

Opening a case Galdance SOFTWARE


PAGE 4

- Establish a Known Good Local Time (KGLT).
- Identify the scope of the case.
 - Document involved computers and media
 - Witness devices
 - Logs and alerts
- Whenever possible, conduct a physical examination of the evidence computer.
 - Process for indicia of ownership (don't forget physical evidence)
 - Document a time stamp for each device
 - Save volatile information
 - Identify and document hardware


© 2009 Guidance Software, Inc. All Rights Reserved.

Opening a Case Galdance SOFTWARE

PAGE 5





© 2009 Guidance Software, Inc. All Rights Reserved.

Make a forensic copy  PAGE 6


- Use a write-blocker device. (FastBloc is available from Guidance)
- Make a physical disk image of each involved device if possible.
 - Make a logical file system image in cases where the physical disk image is not possible.
 - Make forensic copies of log files and witness device settings.
- Use forensically sound protocols to collect "live" devices over the network if necessary.
- Do not examine original media.

© 2009 Guidance Software, Inc. All Rights Reserved.

Open and verify the Disk Image  PAGE 7

- EnCase does the verification for you when you open the file.
- Establish the basics.
 - Owner
 - Organization
 - Time Zone settings
 - SID and User RID's
 - Last login
 - Time lines
 - MAC and IP information

© 2009 Guidance Software, Inc. All Rights Reserved.

Hash / Signature / Entropy Analysis  PAGE 8

- Perform Hash analysis of the files on the system.
- Eliminate Known Good or ID Known wanted files.
 - Bit9
 - NSRL
 - Custom hash sets
- You may also perform Signature Analysis if necessary.
 - Compares header and file extension information
- Entropy set analysis (CyberSecurity)

© 2009 Guidance Software, Inc. All Rights Reserved.

Guidance SOFTWARE

Timeline analysis

PAGE 9

- Review activity of the system during the time of the incident.
- Limit by Modified, Created, Accessed dates if necessary.
- Compare against the System, Application and Security logs.

© 2009 Guidance Software, Inc. All Rights Reserved.

Guidance SOFTWARE

Process EFS and ID Encrypted Files

PAGE 10

- ID EFS secure storage passwords.
 - EnCase will process EFS and identify stored passwords.
- Identify encrypted files for additional processing.
- Whole Disk Encryption may require EnCase Enterprise and servlet deployment or Connectors.
 - Credant
 - Utimaco
 - PGP

© 2009 Guidance Software, Inc. All Rights Reserved.

Guidance SOFTWARE

Identify Compound Files

PAGE 11

- Examples of Compound files include;
 - .zip
 - .gzip
 - .gz
 - .rar
 - MS Office 2007 "x" documents
- Mount compound files for searching and extraction.

© 2009 Guidance Software, Inc. All Rights Reserved.

Key word searching Galdanica SOFTWARE

PAGE 12

- Identify key words and phrases in the case.
- Conduct keyword searches against files not identified as known good by hash analysis.
- Review keyword hits.
- Refine keyword searches.
- Re-conduct searches as necessary.

© 2009 Guidance Software, Inc. All Rights Reserved.

Process User data Galdanica SOFTWARE

PAGE 13

- Review the user profile.
- Verify access and location of network shares.
 - Collect shares if necessary.
- Identify Email servers, Webmail, and archived Email files.
- Process user artifacts.
 - Process web history.
 - Identify recent documents.
 - Process Link files.
 - Process INFO2 files.
 - Process print spool files.
 - View Graphics.
 - Conduct Data carving if necessary.

© 2009 Guidance Software, Inc. All Rights Reserved.

Bookmark and document findings Galdanica SOFTWARE

PAGE 14

- Create bookmarks of files and data of interest.
- Follow-up on any leads developed.
- Prepare a complete and concise report of your findings.
 - Document your protocols and how you found items.
 - You may not testify for two to three years after the examination. Will you remember?

© 2009 Guidance Software, Inc. All Rights Reserved.



■ **The Leader in Digital Investigations software, training & services**

- Over 27,000 users of EnCase® software worldwide
- Over 4,500 trained annually
- Nearly 500 organizations rely on EnCase® Enterprise software:
 - Major federal government agencies
 - *Over half of the Fortune 50, and over 100 of the Fortune 500*

■ **Global support offices and training facilities**

- Pasadena, NY, Chicago, Washington DC, San Francisco, Houston, Atlanta, London, Japan, Singapore & Brazil

■ **Public company with a strong financial position**

- Founded 1997 (NASDAQ: GUID)



Fred B. Cotton
Solutions Consultant
Guidance Software, Inc.
2200 Powell Street, Suite 800
Emeryville, CA 94608
(510)705-3528
fred.cotton@guidancesoftware.com

Matthew Fee
Senior Account Executive
Guidance Software, Inc.
Matthew.fee@guidancesoftware.com
