

Electronic Evidence and Computer Forensics

Legal Seminar Outline: 1 hour

I. Introductions:

A. The Staff:

- i. Andrew Fahey - Computer Forensic Specialist
- ii. Eric Smith - Computer Forensic Specialist
- iii. Robert Pelcher - Computer Forensic Specialist
- iv. Dave Gallant – Computer Forensic Specialist

B. Credentials:

- i. e-fense personnel have been trained and certified by the USAF Special Investigations Academy, Andrews AFB, MD, and/or the Federal Law Enforcement Training Center, Brunswick, GA, and/or Guidance Software (EnCase) to conduct digital forensic analysis of affected computers.
- ii. e-fense has a secure in-house forensic lab and uses industry standard software and methodologies. During on-site forensic analysis, e-fense uses a portable Fly-Away System (FAS). One of our unique technical qualifications is our ability to conduct forensics and investigative services for any possible environment. It is important to emphasize, however, that at e-fense, we believe that there is an art as well as a science to computer forensics and investigations. Software tools alone cannot replace forensic and investigative training, especially in the critical area of evidence preservation. Our staff not only possesses the technical tools, but also the extensive training and experience in the step-by-step processes and procedures that produce the most thorough and defensible evidence packages. The forensic recovery techniques used ensure any and all evidence that remains on any type of computer media is discovered and recovered properly to ensure it can be used in any type of legal proceeding.

II. Why Electronic Discovery?

A. Legal Case References

III. Why Computer Forensics?

- A. Legal Case References

IV. Types of Cases

- A. White Collar Cases
- B. Malpractice Cases
- C. Intellectual Property Cases
- D. Contracts
- E. Employment Cases
- F. Divorce Cases
- G. Discrimination Cases
- H. Employee Misconduct
- I. Product Liability Cases
- J. Business Litigation
- K. Criminal Defense
- L. Sexual Harassment Cases
- M. Patents and Trademark Cases
- N. Securities Litigation
- O. Asset Determination

V. Potential Evidence on a Computer:

- A. Active Data
- B. Residual Data
- C. Replicant Data
- D. E-mail
- E. Logs
- F. Date and Time Stamps

VI. Things to Do

VII. Use Computer Forensics Experts to:

- A. Preserve the system
- B. Discover all Data, including Physical, deleted and hidden
- C. Analyze potentially relevant data
- D. Create an expert report
- E. Ensure procedures do not compromise potential evidence
- F. Protect evidence from electromagnetic or physical damage
- G. Maintain a continuing chain of custody
- H. Secure the potential evidence
- I. Testify at any court proceedings

VIII. Duty to Preserve Evidence

- A. Legal Case References

IX. Act Quickly if Opposition Seeks to Delay

- A. Legal Case References

X. Procedure and Methodology

- A. Legal Case References

XI. The Proposed Procedure

- A. Fully identify and document the target system
- B. “Write Protect” target system to prevent inadvertent changing of data
- C. Conduct Mirror Image using approved software and methodology
- D. Use only court approved software and techniques
- E. Preserve any evidentiary findings during analysis to CD-ROM and establish chain of custody for that CD-ROM

XII. How the evidence is found

- A. The Hard Drive – definition of hard drive
- B. The “Mirror” Image – definition
- C. What is a “cluster”?
- D. Deleted files are not deleted until they are overwritten
- E. The File
- F. Files and the FAT
- G. How files are allocated
- H. Deleted and Unallocated

XIII. What to know about the opposing party’s system for discovery

- A. SYSTEM ARCHITECTURE
 - i. Computer system functions –E-mail application(s), file server
 - ii. Network system configuration – Where are files stored?, remote locations, any additional computer systems owned off site, etc...
 - iii. Application software and utilities – Backup software, e-mail applications
 - iv. Data storage and retention – How long are backups kept?, etc...

XIV. Sample system diagram

XV. Discovery

- A. Ask for assistance with discovery questions relating to evidence
- B. Be specific during discovery. Example: “LOGS” is a broad term
- C. Understand that there are vast possibilities. Your forensic expert has experience with a wide variety of cases and can assist with suggestions.

XVI. Don't forget

- A. Various types of digital media

XVII. Areas Ripe for Challenge

- A. Scope of search warrant/discovery request too broad
- B. Failure to follow proper procedures to obtain mirror image
- C. Use of forensic procedures and/or proprietary software that has not been validated in court
- D. Poorly documented forensic procedures
- E. Failure to secure forensic lab and evidence both physically and through internet/ intranet
- F. Unlicensed software used to conduct forensics
- G. Lack of a proper chain of custody
- H. Including improper transport or storage of evidence