Intro to Computer Forensics

Warren G. Kruse II, CISSP, CFCE
wgkruse@computer-forensic.com
http://www.computer-forensic.com
732-695-0530

Copy on www.computer-forensic.com/presentations/)

COMPUTER
FORENSIC
SERVICES, LLC

Topics

- Intro to Computer Forensics
- What may be available

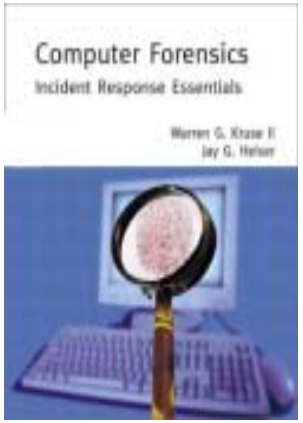
COMPUTER
FORENSIC
SERVICES, LLC

What Is Computer Forensics?

"Computer forensics involves the preservation, identification, extraction, documentation and interpretation of computer data. It is often more of an art than a science, but as in any discipline, computer forensic specialists follow clear, well-defined methodologies and procedures, and flexibility is expected and encouraged when encountering the unusual."

From: "*Computer Forensics: Incident Response Essentials*"

- Finding key pieces of evidence - even if someone has tried to hide, discard, or destroy them.



COMPUTER FORENSIC SERVICES, LLC

Software Recommendations

- Guidancesoftware's Encase: www.encase.com
- Acessdata's Forensic Toolkit: www.accessdata.com
- AccessData Password Recovery Toolkit
- AccessData's Distributed Network Attack
- Prodiscover (DFT or IR), www.techpathways.com
- Safeback, www.forensics-intl.com
- Quick View Plus, http://www.jasc.com/
- Thumbs Plus (Shareware), www.cerious.com
- Irfanview (freeware for non commercial use)
  - www.irfanview.com

COMPUTER FORENSIC SERVICES, LLC

What Computer Forensics is used for:

- High Tech Investigations
- Incident Response
- E-mail recovery and analysis
- Document & File Discovery
  - Locating and recovering previously inaccessible files.
- Data Collection
  - Collecting data while preserving vital date and time stamps, temporary files and other volatile information.

CFS
COMPUTER FORENSIC SERVICES, LLC

CFS
COMPUTER FORENSIC SERVICES, LLC

What Computer Forensics is used for:

- Preservation of Evidence
  - Adherence to carefully developed set of procedures that address security, authenticity, and chain-of-custody.
- Analysis of User Activity
  - Reporting of all user activity on computer and company network including, but not limited to,e-mail, Internet and Intranet files accessed, files created and deleted, and user access times.
- Password Recovery
  - Accessing and recovering data from password protected files.

COMPUTER FORENSIC SERVICES, LLC

Investigative Methods

- Common sense
- Physical surveillance
- Victim\witness interview
- Undercover approach
- Electronic surveillance (network monitoring- sniffers, NIDs, etc.)
- Informants
- Sting operation
- IMAGE!

Does this sound any different then other types of investigations?

COMPUTER FORENSIC SERVICES, LLC

Keys to Success

- Documentation of all action
- Preservation of evidence
- Swift action to collect electronic audit trails
- Resources
- Time – hard drives are getting HUGE!

COMPUTER
FORENSIC
SERVICES, LLC

Tools of our trade

COMPUTER
FORENSIC
SERVICES, LLC

Terminology

- Image: exact copy of a hard drive including deleted files and areas of the hard drive that a normal backup would not copy
- Slack, Swap and Unallocated space

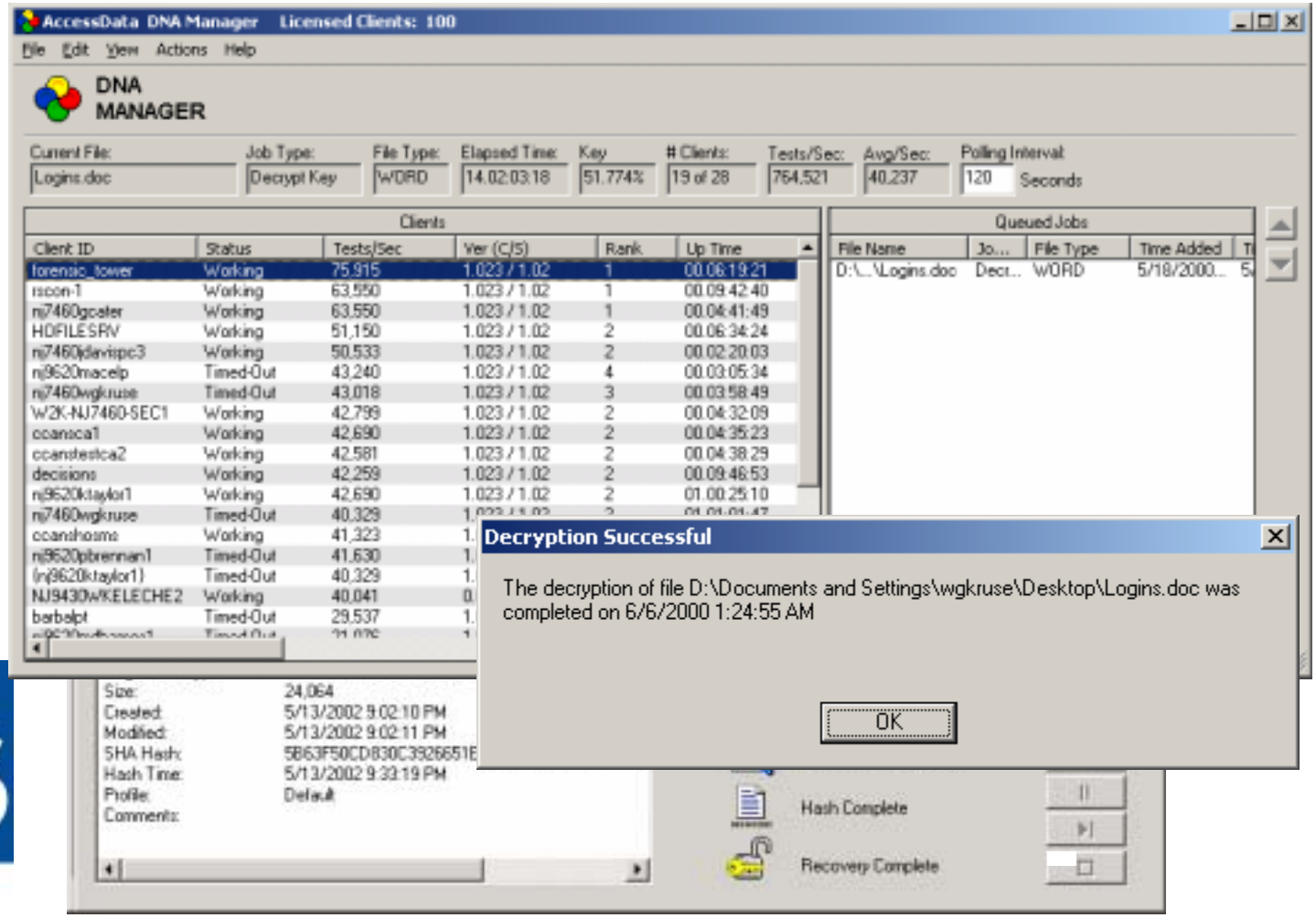
COMPUTER FORENSIC SERVICES, LLC

Show Me Something!

- Password Protected files
- Deleted Files Demo's

COMPUTER
FORENSIC
SERVICES, LLC

Password Protection



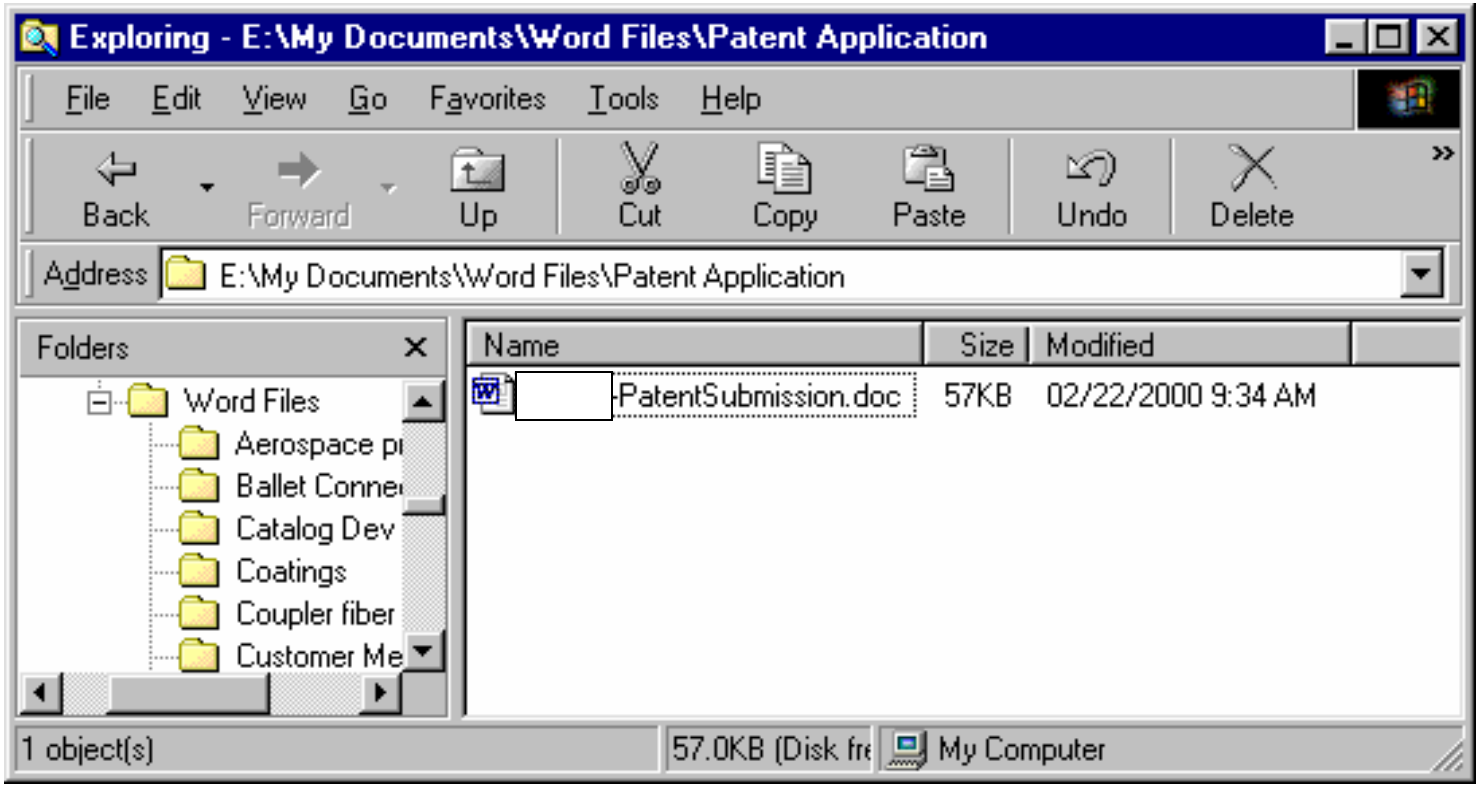
COMPUTER FORENSIC SERVICES, LLC

Show Me Something Else!

- Once Upon a Time There Was a File Named PatentSubmission.Doc

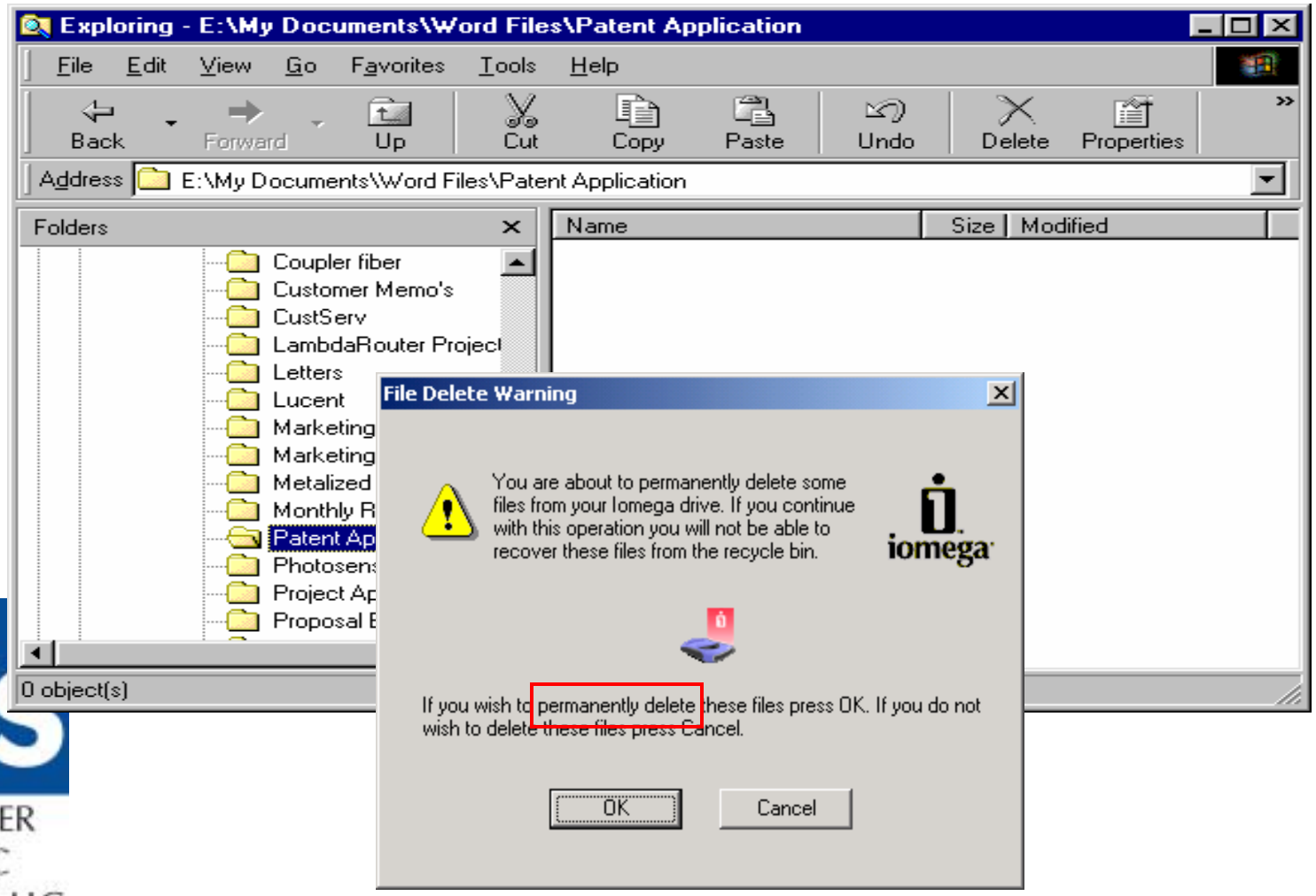
COMPUTER FORENSIC SERVICES, LLC

A File Is Born



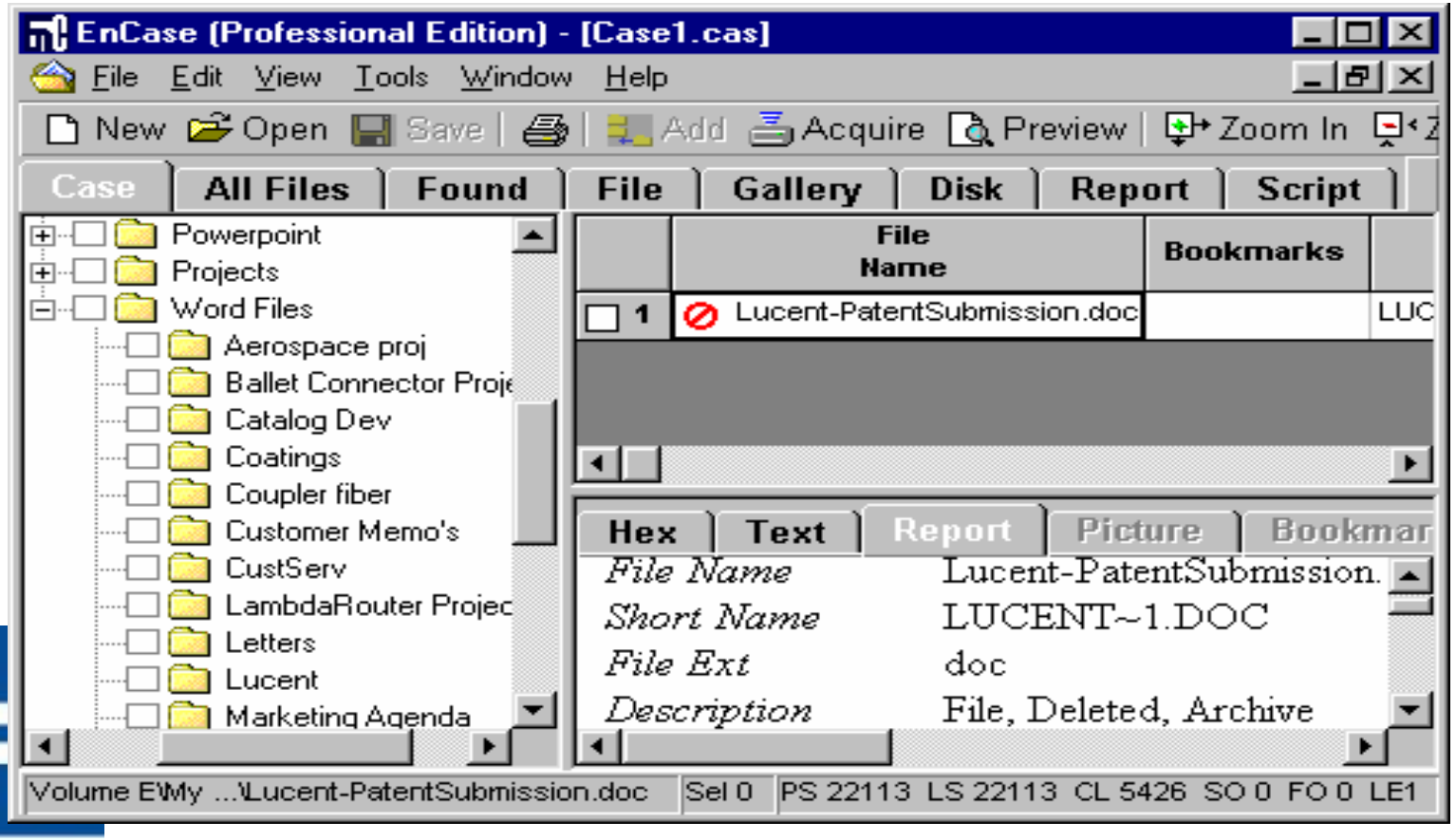
COMPUTER FORENSIC SERVICES, LLC

The File Dies…or Does It?



COMPUTER FORENSIC SERVICES, LLC

Encase Doesn’t Think So

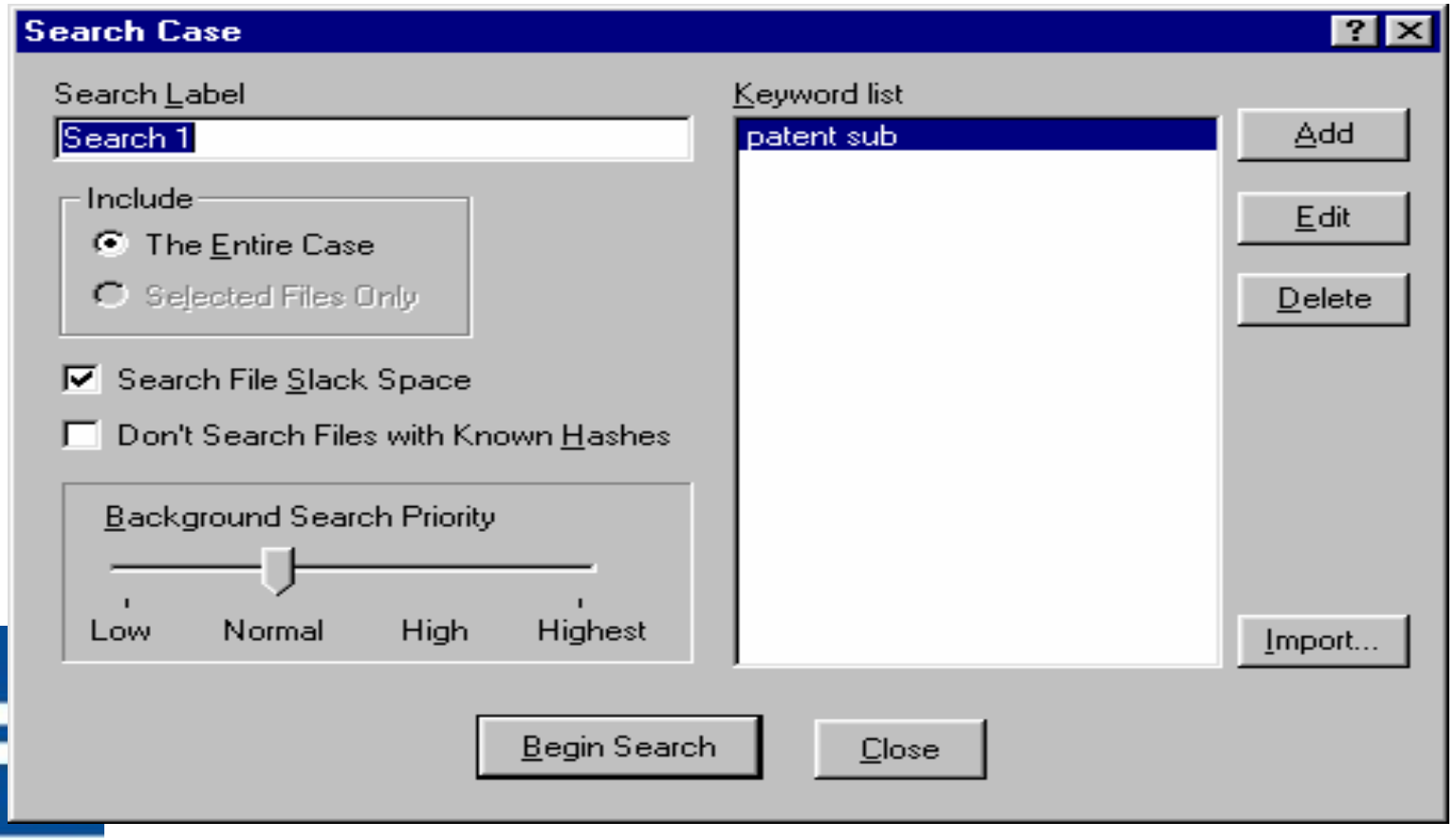


COMPUTER FORENSIC SERVICES, LLC

How About Now?

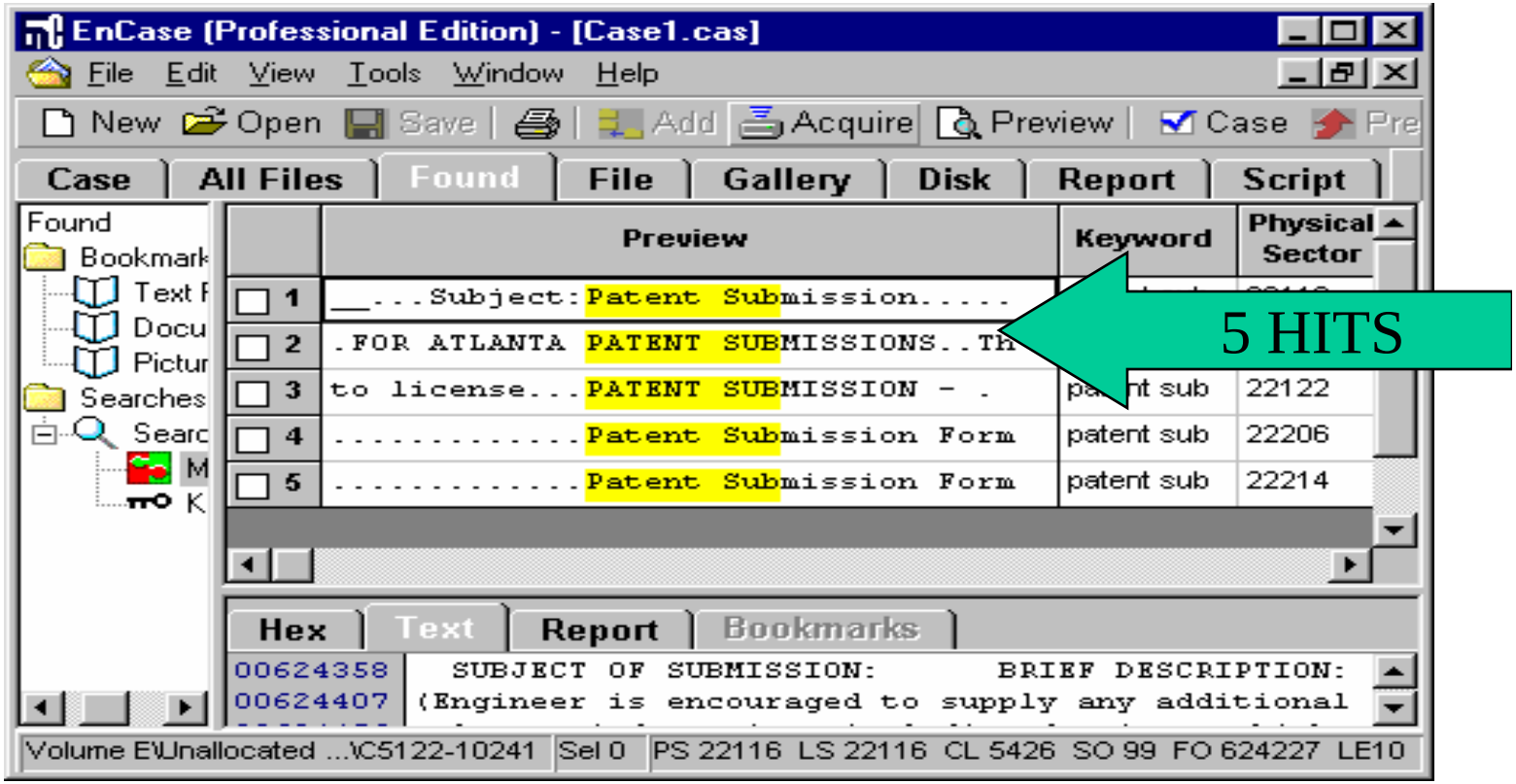
COMPUTER FORENSIC SERVICES, LLC

Let’s See Shall We?



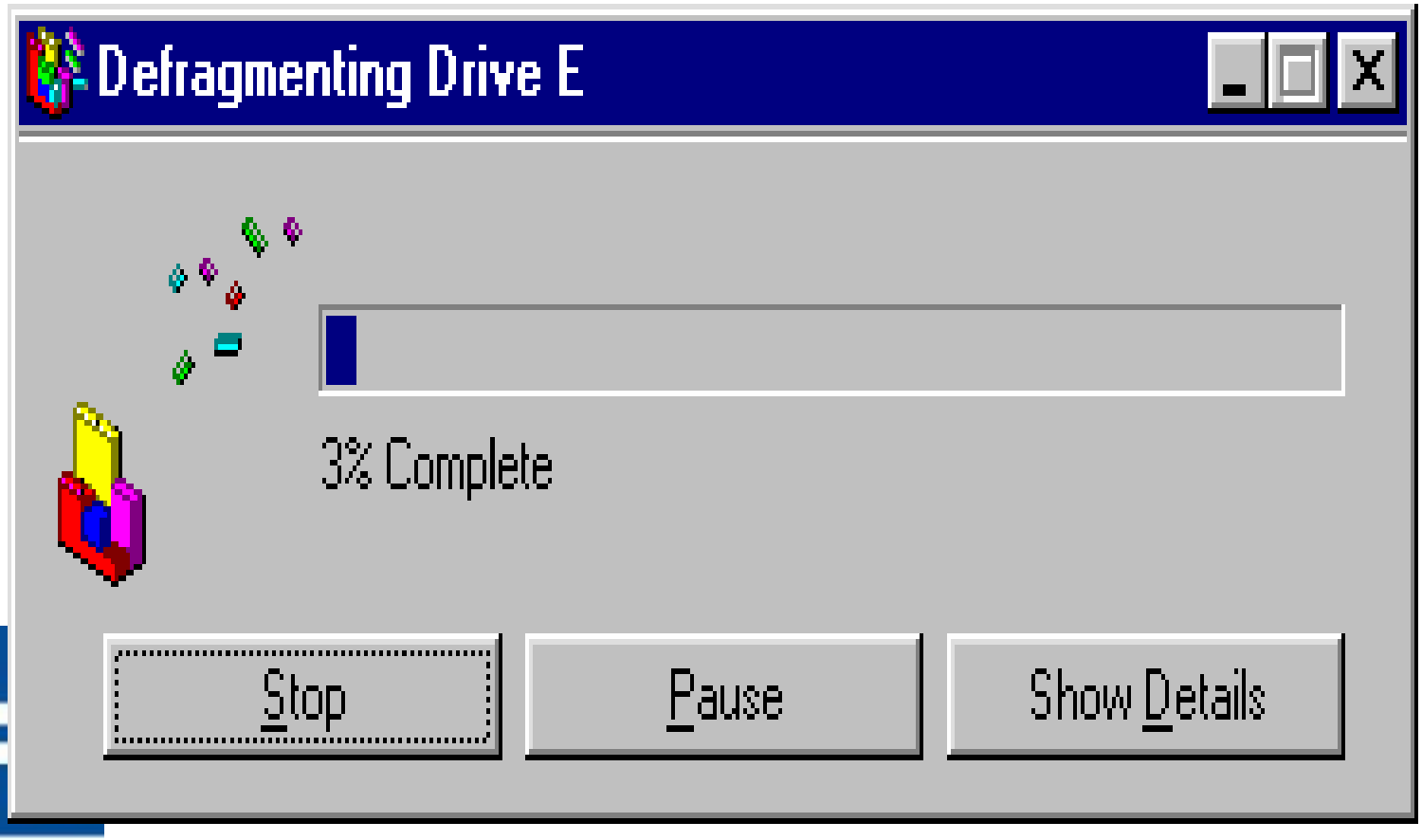
COMPUTER FORENSIC SERVICES, LLC

It’s ALLLLLLLLIVE!



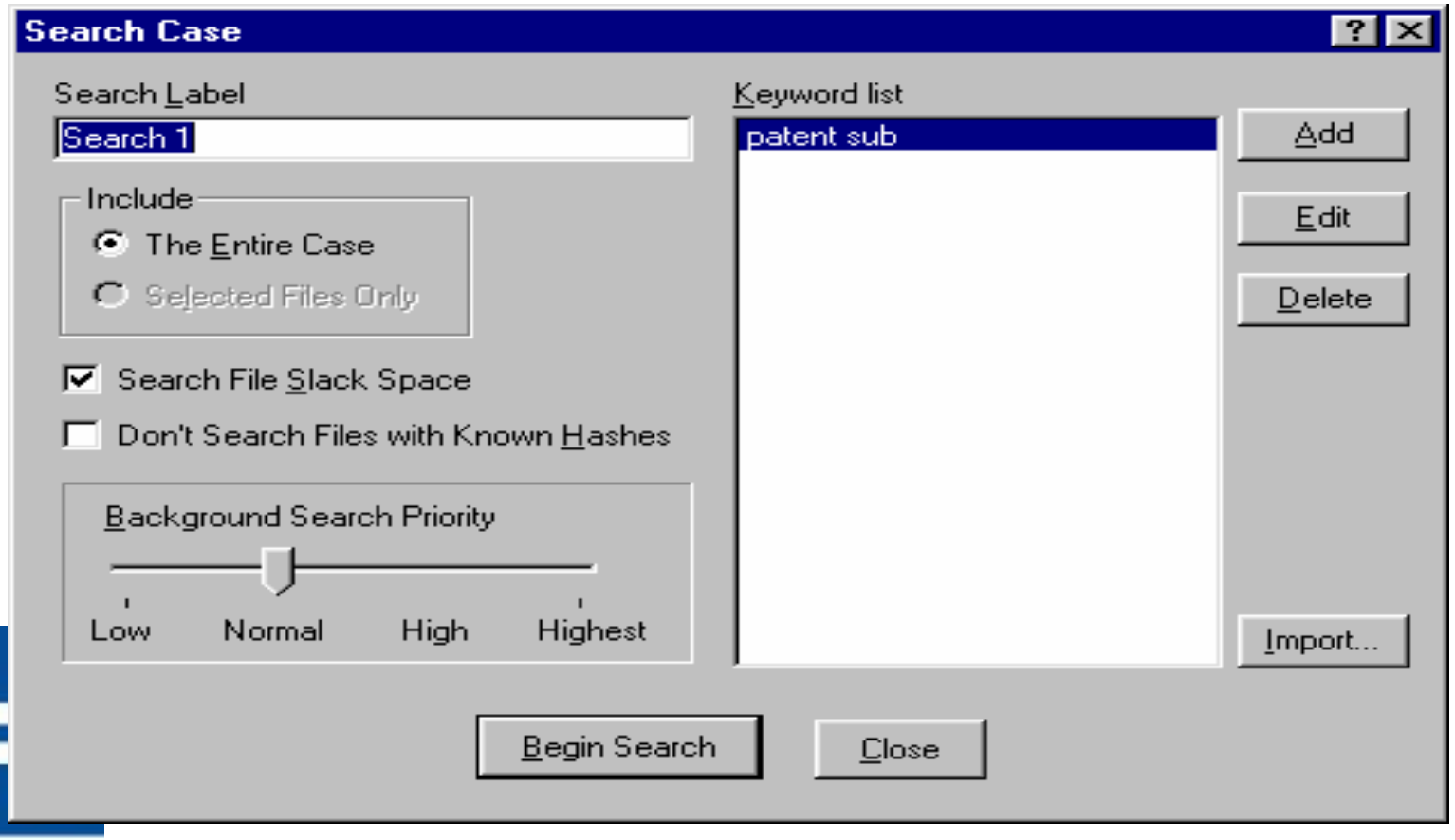
COMPUTER FORENSIC SERVICES, LLC

How About Now?



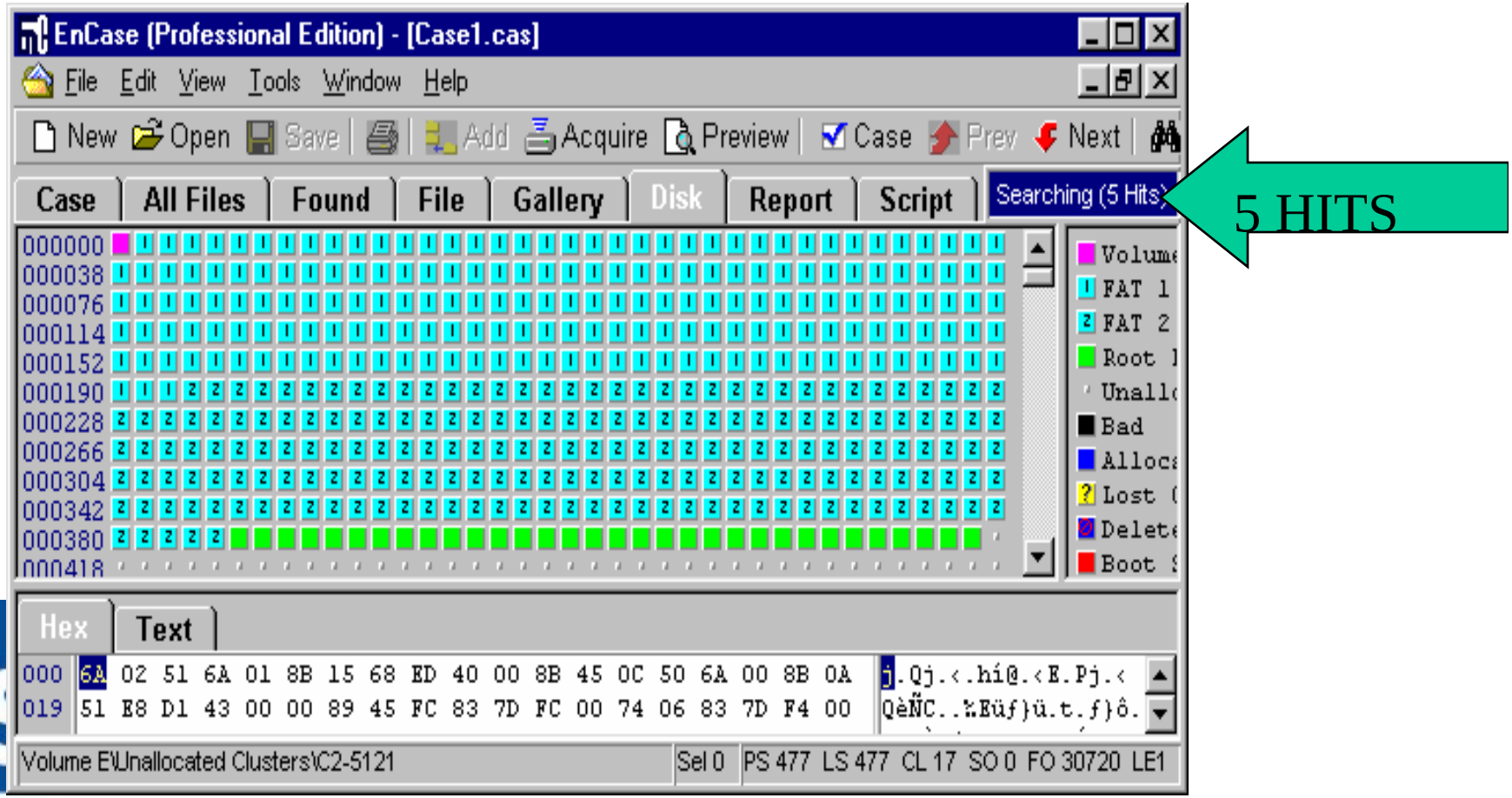
COMPUTER FORENSIC SERVICES, LLC

Let’s See



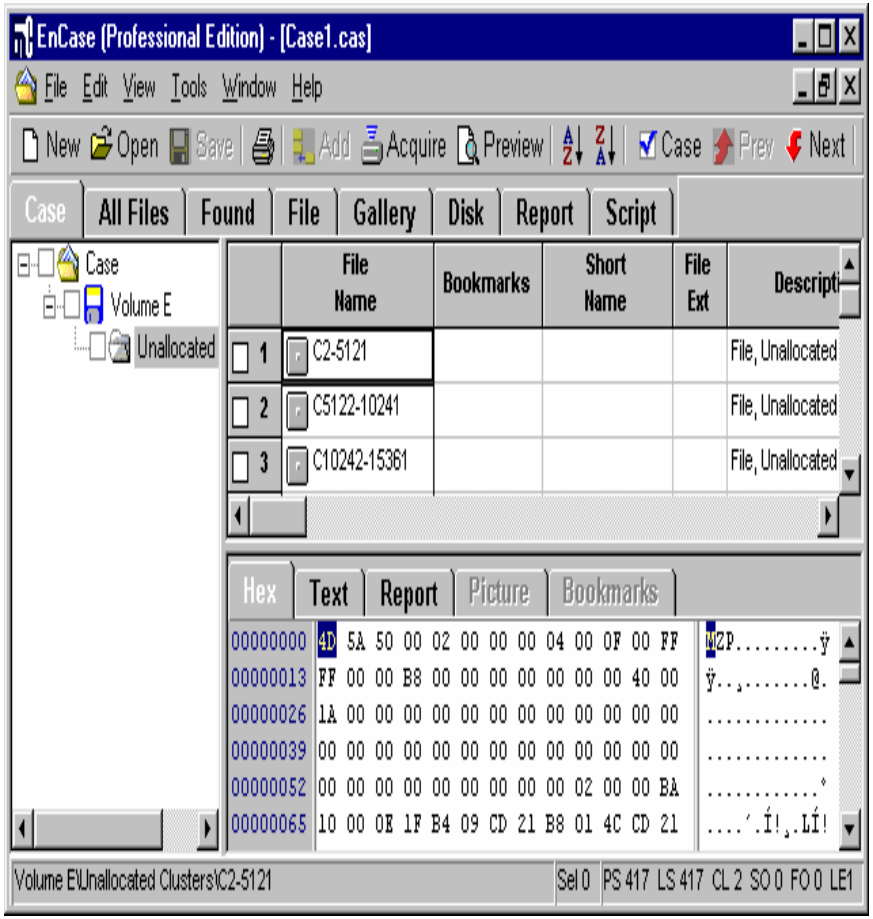
COMPUTER FORENSIC SERVICES, LLC

It’s STILL ALLLLLLLLIVE!



COMPUTER FORENSIC SERVICES, LLC

The Resurrection
("Deleted" File Before and After Format and Defrag)



COMPUTER FORENSIC SERVICES, LLC

Trace Information May Exist From:

- Email
- PDA/Blackberry
- Temp Files
- Recycle Bin
- Info File Fragments
- Recent Link Files
- Spool (printed) files
- Internet History (index.dat)
- Registry
- Unallocated Space
- File Slack

COMPUTER FORENSIC SERVICES, LLC

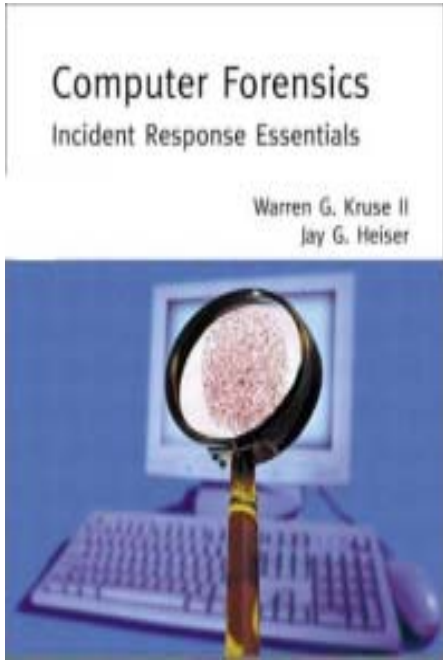
The File Lives On…

- This was made possible only through the forensic practice of treating the entire physical disk as evidence (rather than just files) and handling it as evidence.
- Demos anyone?

COMPUTER
FORENSIC
SERVICES, LLC

Where to go from here

- www.virtuallibrarian.com/legal/
- www.htcia.org
- Shameless Plug Warning:
  - Computer Forensics: Incident Response Essentials
    - **Paperback:** 416 pages
    - **Publisher:** Addison-Wesley Pub Co
    - ISBN: 0201707195



COMPUTER FORENSIC SERVICES, LLC

Computer Forensic Services, LLC

Copy on www.computer-forensic.com/presentations/)

Warren Kruse
20-22 Industrial Way
Eatontown, New Jersey
Toll Free: (732) 695-0530
Email: wgkruse@computer-forensic.com