

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.”

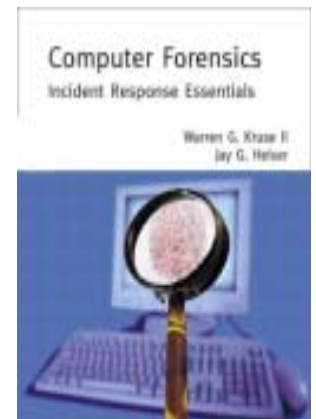
From: “*Computer Forensics: Incident Response Essentials*”

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



COMPUTER
FORENSIC
SERVICES, LLC

Copyright Computer Forensic Services, LLC



Software Recommendations

- Guidancesoftware's Encase: www.encase.com
- Accessdata'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.



COMPUTER
FORENSIC
SERVICES, LLC



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

Forensic

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

AccessData DNA Manager Licensed Clients: 100

File Edit View Actions Help

DNA MANAGER

Current File: Logins.doc Job Type: Decrypt Key File Type: WORD Elapsed Time: 14.02.03.18 Key: 51.774% # Clients: 19 of 28 Tests/Sec: 764.521 Avg/Sec: 40.237 Polling Interval: 120 Seconds

Clients						Queued Jobs				
Client ID	Status	Tests/Sec	Ver (C/S)	Rank	Up Time	File Name	Job...	File Type	Time Added	Ti
forensic_tower	Working	75.915	1.023 / 1.02	1	00.06.19.21	D:\...\Logins.doc	Decr...	WORD	5/18/2000...	5
iscon-1	Working	63.550	1.023 / 1.02	1	00.09.42.40					
n7460gcater	Working	63.550	1.023 / 1.02	1	00.04.41.49					
HDFLESRV	Working	51.150	1.023 / 1.02	2	00.06.34.24					
n7460denvipc3	Working	50.533	1.023 / 1.02	2	00.02.20.03					
n9620macelp	Timed-Out	43.240	1.023 / 1.02	4	00.03.05.34					
n7460wgkruse	Timed-Out	43.018	1.023 / 1.02	3	00.03.58.49					
W2K-NJ7460-SEC1	Working	42.799	1.023 / 1.02	2	00.04.32.09					
ocanoca1	Working	42.690	1.023 / 1.02	2	00.04.35.23					
ocanstestca2	Working	42.581	1.023 / 1.02	2	00.04.38.29					
decisions	Working	42.259	1.023 / 1.02	2	00.09.46.53					
n9620ktaylor1	Working	42.690	1.023 / 1.02	2	01.00.25.10					
n7460wgkruse	Timed-Out	40.329	1.023 / 1.02	3	01.01.01.47					
ocanohoms	Working	41.323	1.023 / 1.02	2	00.04.32.09					
n9620pbrennan1	Timed-Out	41.630	1.023 / 1.02	3	00.04.32.09					
(n9620ktaylor1)	Timed-Out	40.329	1.023 / 1.02	3	00.04.32.09					
NJ9430WKELECHE2	Working	40.041	1.023 / 1.02	2	00.04.32.09					
barbalpt	Timed-Out	29.537	1.023 / 1.02	3	00.04.32.09					
...					

Size: 24,064
Created: 5/13/2002 9:02:10 PM
Modified: 5/13/2002 9:02:11 PM
SHA Hash: 5B63F50CD830C3526651E
Hash Time: 5/13/2002 9:32:19 PM
Profile: Default
Comments:

Hash Complete
Recovery Complete

Decryption Successful

The decryption of file D:\Documents and Settings\wgkruse\Desktop\Logins.doc was completed on 6/6/2000 1:24:55 AM

OK



COMPUTER
FORENSIC
SERVICES, LLC

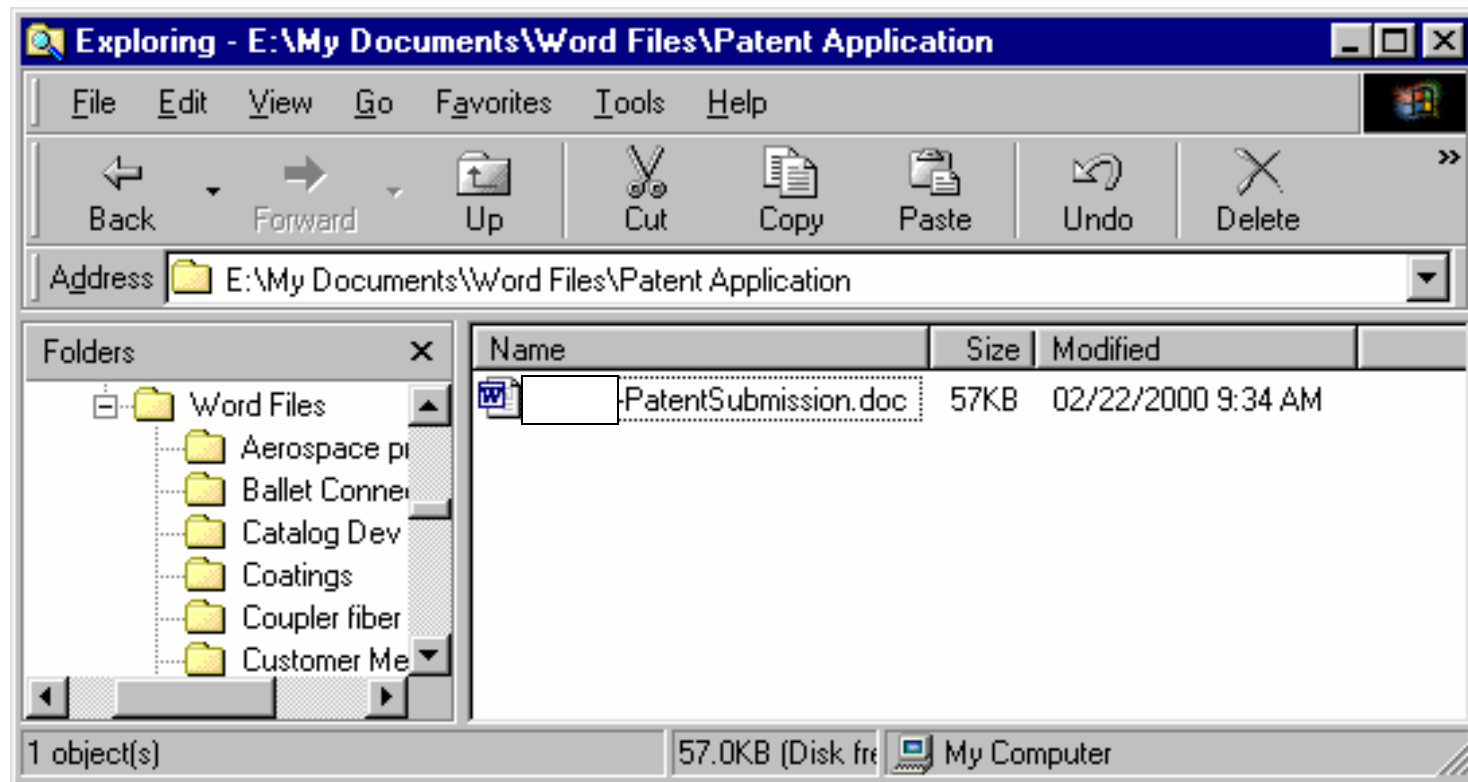
Show Me Something Else!

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



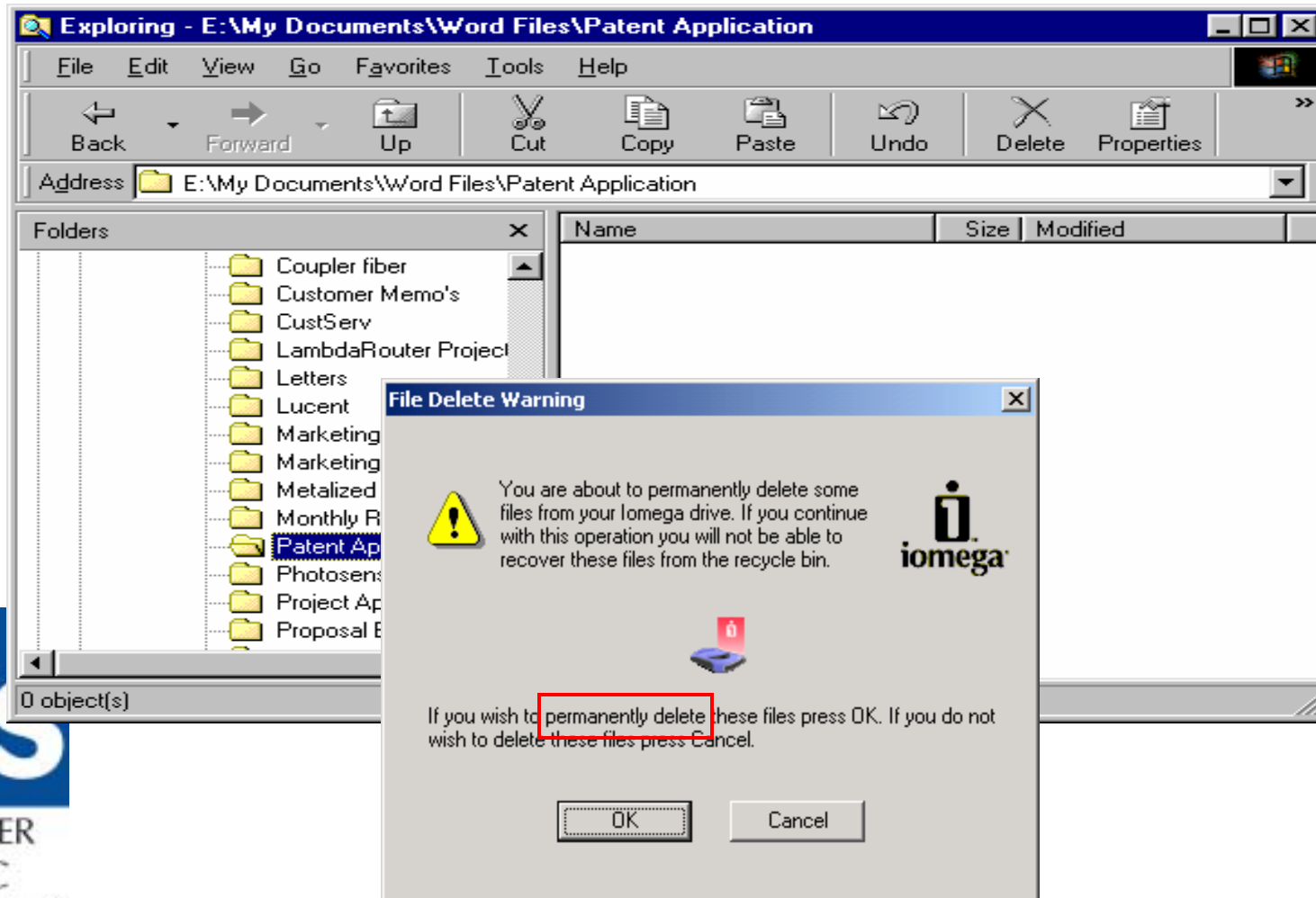
COMPUTER
FORENSIC
SERVICES, LLC

A File Is Born

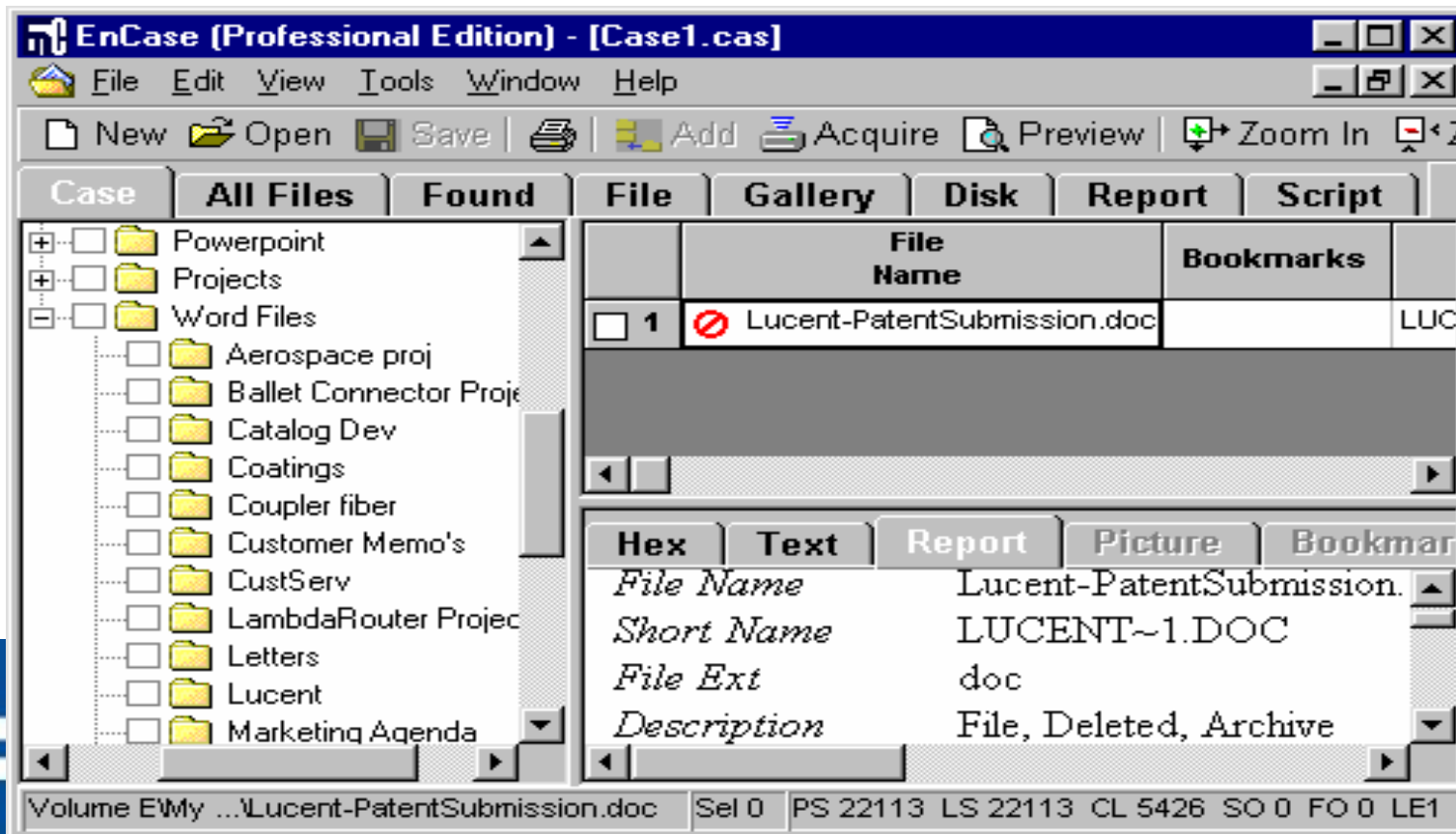


COMPUTER
FORENSIC
SERVICES, LLC

The File Dies...or Does It?



Encase Doesn't Think So

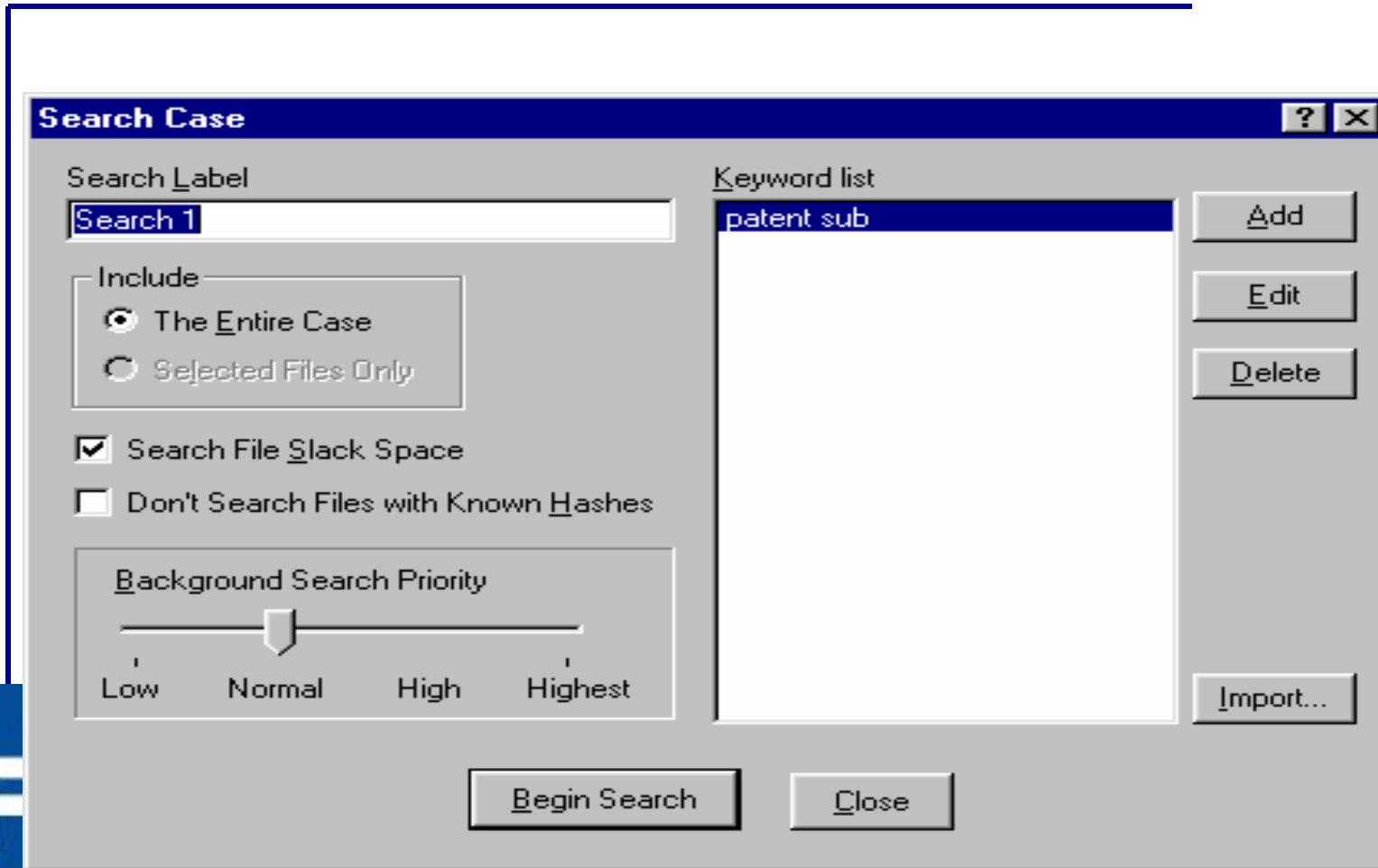


How About Now?



COMPUTER
FORENSIC
SERVICES, LLC

Let's See Shall We?



It's ALLLLLLLIVE!

The screenshot shows the EnCase (Professional Edition) interface. The 'Found' tab is active, displaying a list of search results. A green arrow points to the first five results, which are highlighted in yellow. The results are as follows:

	Preview	Keyword	Physical Sector
<input type="checkbox"/> 1	___... Subject: Patent Submission....		22118
<input type="checkbox"/> 2	. FOR ATLANTA PATENT SUBMISSIONS.. TH		
<input type="checkbox"/> 3	to license... PATENT SUBMISSION - .	patent sub	22122
<input type="checkbox"/> 4 Patent Submission Form	patent sub	22206
<input type="checkbox"/> 5 Patent Submission Form	patent sub	22214

Below the search results, the 'Report' tab is selected, showing the following text:

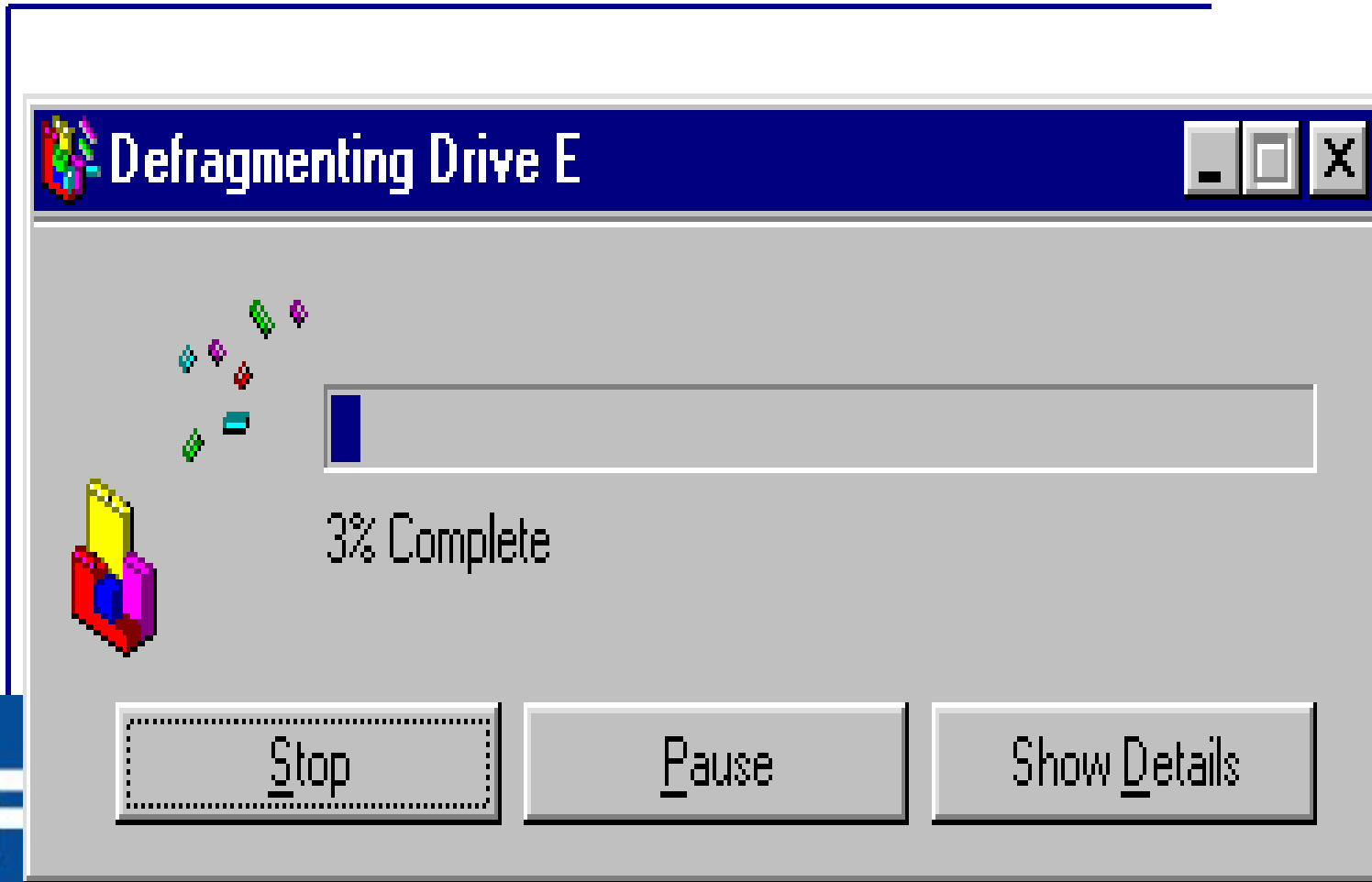
```
00624358 SUBJECT OF SUBMISSION: BRIEF DESCRIPTION:
00624407 (Engineer is encouraged to supply any additional
```

A green arrow with the text "5 HITS" points to the first five rows of the search results table.



COMPUTER
FORENSIC
SERVICES, LLC

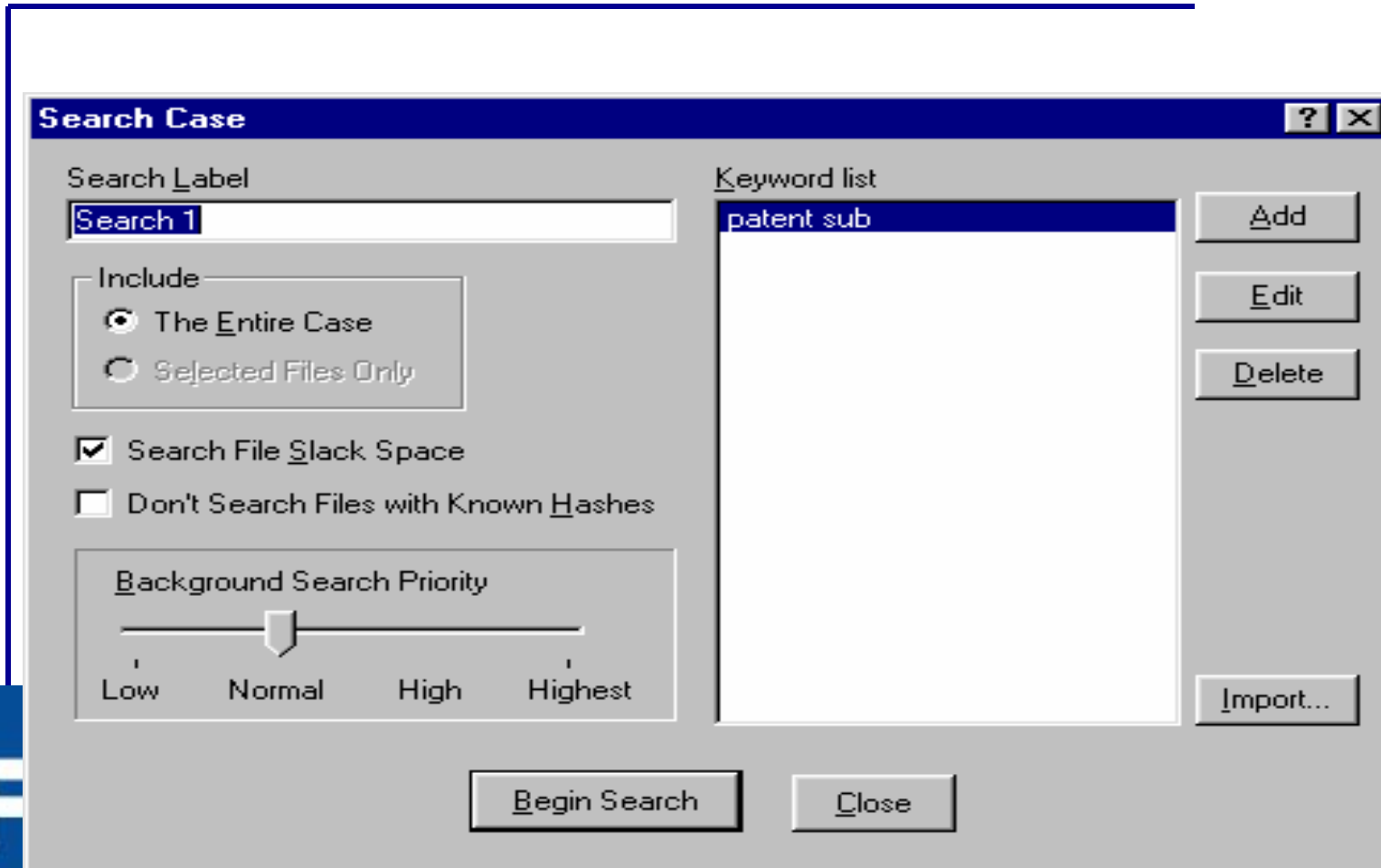
How About Now?



COMPUTER
FORENSIC
SERVICES, LLC

Copyright Computer Forensic Services, LLC

Let's See



It's STILL ALLLLLLLIVE!

The screenshot shows the EnCase (Professional Edition) interface. The main window displays a search results grid with columns for Case, All Files, Found, File, Gallery, Disk, Report, Script, and Searching (5 Hits). The grid contains data for various cases, with the first row (000000) showing a pink square in the 'Found' column. The 'Searching (5 Hits)' tab is highlighted, and a green arrow points to it with the text '5 HITS'. Below the grid, the 'Hex' and 'Text' views are visible. The 'Hex' view shows the following data:

Hex	Text
000 6A 02 51 6A 01 8B 15 68 ED 40 00 8B 45 0C 50 6A 00 8B 0A	j.Qj.<.hi@.<E.Pj.<
019 51 B8 D1 43 00 00 89 45 FC 83 7D FC 00 74 06 83 7D F4 00	QèÑC..%Eüf)ü.t.f)ô.

The 'Text' view shows the corresponding ASCII characters. The status bar at the bottom indicates 'Volume E:\Unallocated Clusters\C2-5121' and 'Sel 0 PS 477 LS 477 CL 17 SO 0 FO 30720 LE1'.

5 HITS

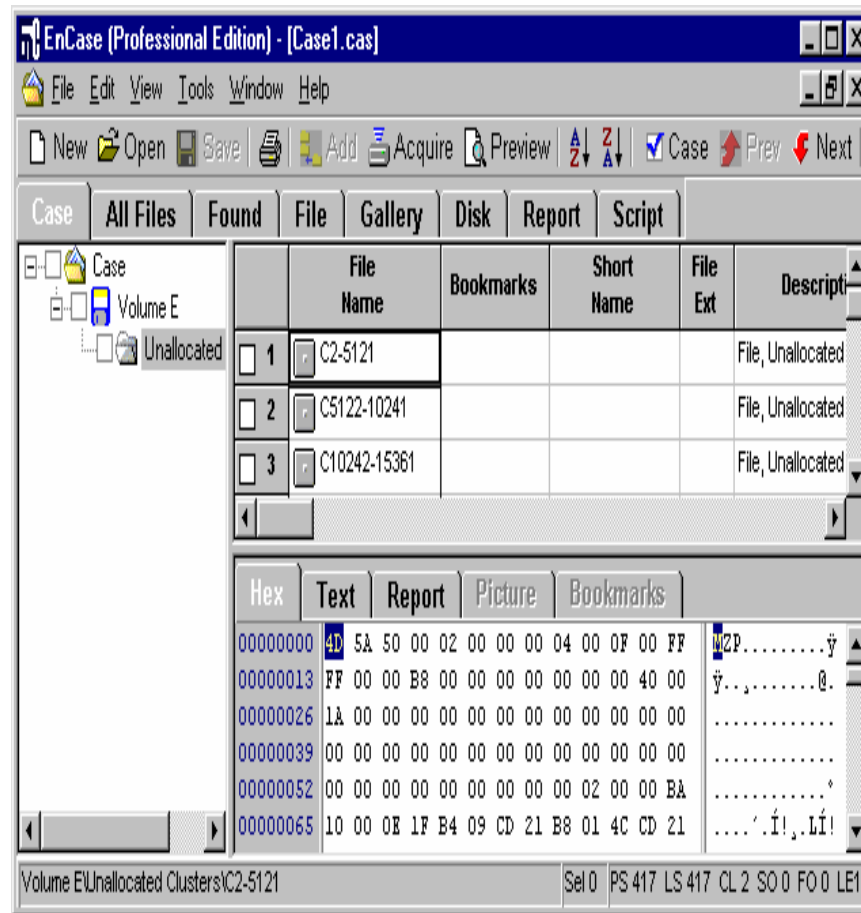


COMPUTER
FORENSIC
SERVICES, LLC

Copyright 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

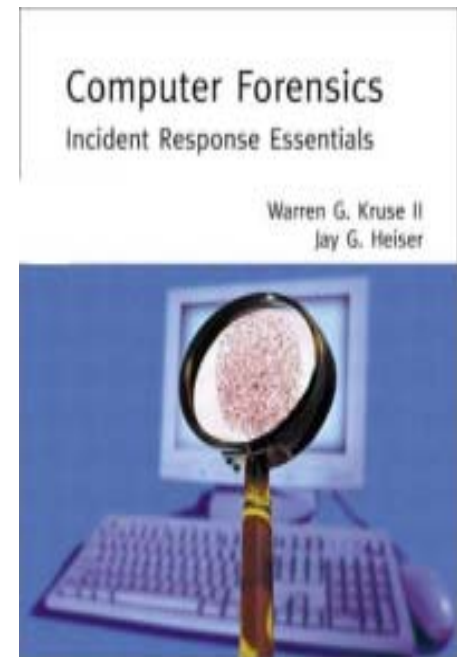
– **Publisher:** Addison-Wesley Pub Co

– **ISBN:** 0201707195



COMPUTER
FORENSIC
SERVICES, LLC

Copyright 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

