Guide to Computer Forensics and Investigations Fourth Edition

Chapter 14

Report Writing for High-Tech Investigations

Objectives

- Explain the importance of reports
- Describe guidelines for writing reports
- Explain how to use forensics tools to generate reports

Understanding the Importance of Reports

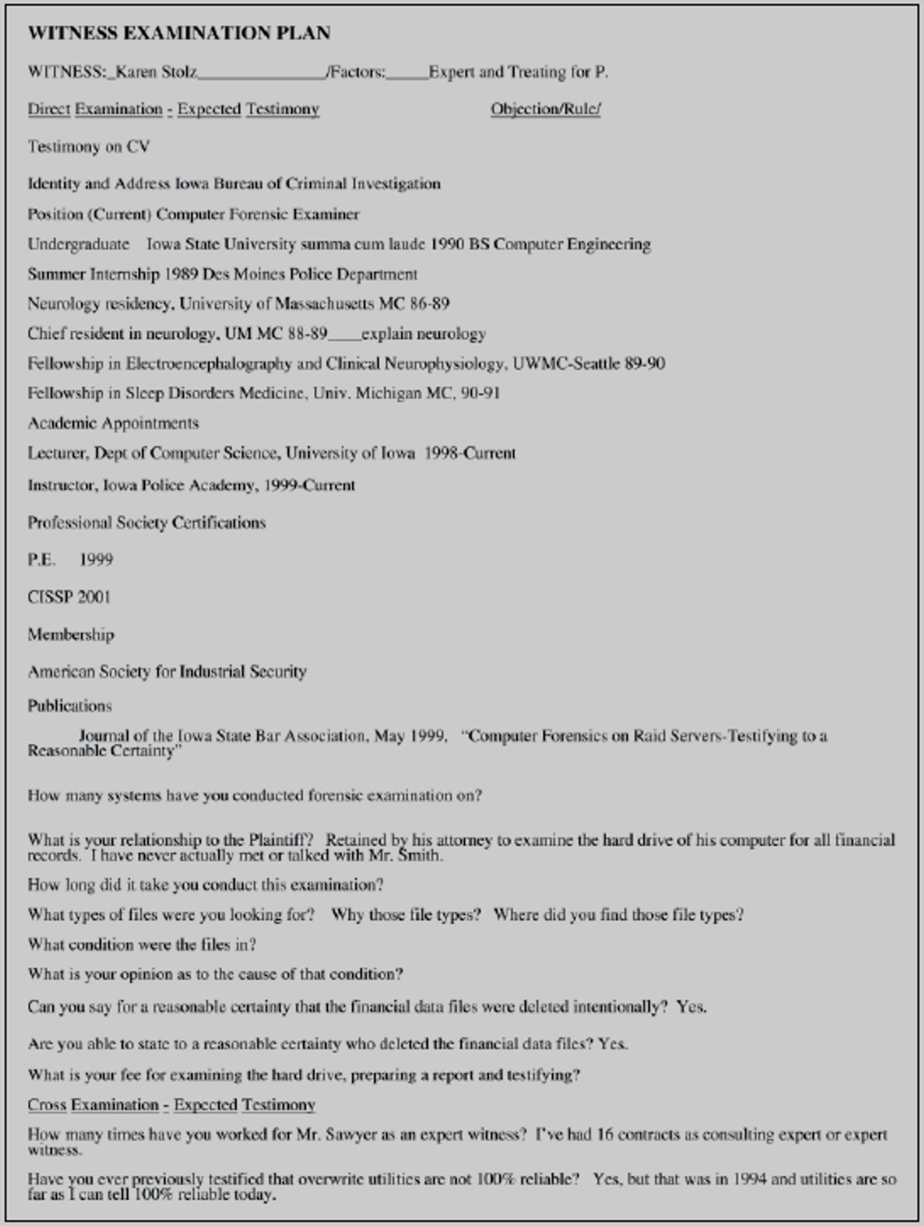
- Communicate the results of your investigation
  - Including expert opinion
- Courts require expert witness to submit written reports
- Written report must specify fees paid for the expert’s services
  - And list all other civil or criminal cases in which the expert has testified
- **Deposition banks**
  - Examples of expert witness’ previous testimonies

Limiting a Report to Specifics

- All reports to clients should start with the job mission or goal
  - Find information on a specific subject
  - Recover certain significant documents
  - Recover certain types of files
- Before you begin writing, identify your audience and the purpose of the report

Types of Reports

- Computer forensics examiners are required to create different types of reports
- **Examination plan**
  - What questions to expect when testifying
  - Attorney uses the examination plan to guide you in your testimony
  - You can propose changes to clarify or define information
  - Helps your attorney learn the terms and functions used in computer forensics



WITNESS EXAMINATION PLAN

WITNESS:_Karen Stolz_______________/Factors:_____Expert and Treating for P.

<u>Direct Examination - Expected Testimony</u>	<u>Objection/Rule/</u>

Testimony on CV

Identity and Address Iowa Bureau of Criminal Investigation

Position (Current) Computer Forensic Examiner

Undergraduate Iowa State University summa cum laude 1990 BS Computer Engineering

Summer Internship 1989 Des Moines Police Department

Neurology residency, University of Massachusetts MC 86-89

Chief resident in neurology, UM MC 88-89____explain neurology

Fellowship in Electroencephalography and Clinical Neurophysiology, UWMC-Seattle 89-90

Fellowship in Sleep Disorders Medicine, Univ. Michigan MC, 90-91

Academic Appointments

Lecturer, Dept of Computer Science, University of Iowa 1998-Current

Instructor, Iowa Police Academy, 1999-Current

Professional Society Certifications

P.E. 1999

CISSP 2001

Membership

American Society for Industrial Security

Publications

Journal of the Iowa State Bar Association, May 1999, "Computer Forensics on Raid Servers-Testifying to a Reasonable Certainty"

How many systems have you conducted forensic examination on?

What is your relationship to the Plaintiff? Retained by his attorney to examine the hard drive of his computer for all financial records. I have never actually met or talked with Mr. Smith.

How long did it take you conduct this examination?

What types of files were you looking for? Why those file types? Where did you find those file types?

What condition were the files in?

What is your opinion as to the cause of that condition?

Can you say for a reasonable certainty that the financial data files were deleted intentionally? Yes.

Are you able to state to a reasonable certainty who deleted the financial data files? Yes.

What is your fee for examining the hard drive, preparing a report and testifying?

<u>Cross Examination - Expected Testimony</u>

How many times have you worked for Mr. Sawyer as an expert witness? I've had 16 contracts as consulting expert or expert witness.

Have you ever previously testified that overwrite utilities are not 100% reliable? Yes, but that was in 1994 and utilities are so far as I can tell 100% reliable today.

Figure 14-1 A sample examination plan

Types of Reports (continued)

- Verbal report
  - Less structured
  - Attorneys cannot be forced to release verbal reports
  - Preliminary report
  - Addresses areas of investigation yet to be completed
    - Tests that have not been concluded
    - Interrogatories
    - Document production
    - Depositions

Types of Reports (continued)

- Written report
  - Affidavit or declaration
  - Limit what you write and pay attention to details
    - Include thorough documentation and support of what you write

Guidelines for Writing Reports

- Hypothetical questions based on factual evidence
  - Less favored today
  - Guide and support your opinion
  - Can be abused and overly complex
- Opinions based on knowledge and experience
- Exclude from hypothetical questions
  - Facts that can change, cannot be used, or are not relevant to your opinion

Guidelines for Writing Reports (continued)

- As an expert witness, you may testify to an opinion, or conclusion, if four basic conditions are met:
  - Opinion, inferences, or conclusions depend on special knowledge or skills
  - Expert should qualify as a true expert
  - Expert must testify to a certain degree of certainty
  - Experts must describe facts on which their opinions are based, or they must testify to a hypothetical question

What to Include in Written Preliminary Reports

- Anything you write down as part of your examination for a report
  - Subject to **discovery** from the opposing attorney
- Considered **high-risk documents**
- **Spoliation**
  - Destroying the report could be considered destroying or concealing evidence
- Include the same information as in verbal reports

What to Include in Written Preliminary Reports (continued)

- Additional items to include in your report:
  - Summarize your billing to date and estimate costs to complete the effort
  - Identify the tentative conclusion (rather than the preliminary conclusion)
  - Identify areas for further investigation and obtain confirmation from the attorney on the scope of your examination

Report Structure

- Structure
  - Abstract
  - Table of contents
  - Body of report
  - Conclusion
  - References
  - Glossary
  - Acknowledgements
  - Appendixes

Writing Reports Clearly

- Consider
  - Communicative quality
  - Ideas and organization
  - Grammar and vocabulary
  - Punctuation and spelling
- Lay out ideas in logical order
- Build arguments piece by piece
- Group related ideas and sentences into paragraphs
  - Group paragraphs into sections

Writing Reports Clearly (continued)

- Avoid jargon, slang, and colloquial terms
- Define technical terms
  - Consider your audience
- Consider writing style
  - Use a natural language style
  - Avoid repetition and vague language
  - Be precise and specific
  - Use active rather than passive voice
  - Avoid presenting too many details and personal observations

Writing Reports Clearly (continued)

- Include signposts
  - Draw reader’s attention to a point

Designing the Layout and Presentation of Reports

- Decimal numbering structure
  - Divides material into sections
  - Readers can scan heading
  - Readers see how parts relate to each other
- Legal-sequential numbering
  - Used in pleadings
  - Roman numerals represent major aspects
  - Arabic numbers are supporting information

Designing the Layout and Presentation of Reports (continued)

- Providing supporting material
  - Use material such as figures, tables, data, and equations to help tell the story as it unfolds
- Formatting consistently
  - How you format text is less important than being consistent in applying formatting
- Explaining examination and data collection methods
  - Explain how you studied the problem, which should follow logically from the purpose of the report

Designing the Layout and Presentation of Reports (continued)

- Including calculations
  - If you use any hashing algorithms, be sure to give the common name
- Providing for uncertainty and error analysis
  - Protect your credibility
- Explaining results and conclusions
  - Explain your findings, using subheadings to divide the discussion into logical parts
  - Save broader generalizations and summaries for the report’s conclusion

Designing the Layout and Presentation of Reports (continued)

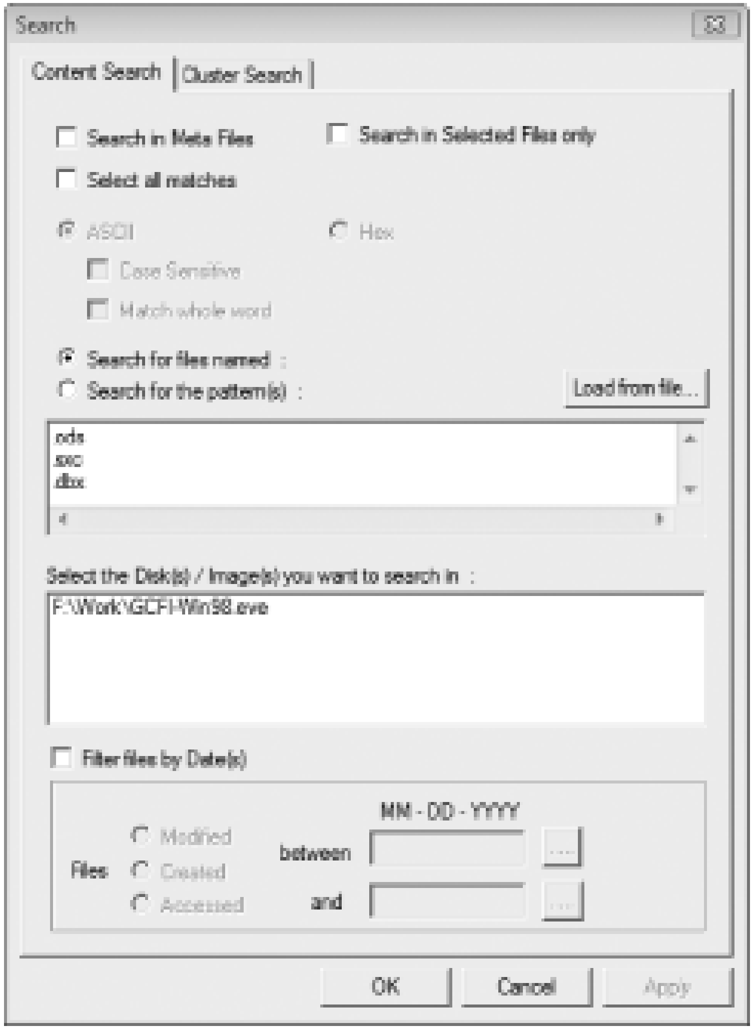
- Providing references
  - Cite references by author's last name and year of publication
  - Follow a standard format
- Including appendixes
  - You can include appendixes containing material such as raw data, figures not used in the body of the report, and anticipated exhibits
  - Arrange them in the order referred to in the report

Generating Report Findings with Forensics Software Tools

- Forensics tools generate reports when performing analysis
- Report formats
  - Plaintext
  - Word processor
  - HTML format

Using ProDiscover Basic to Generate Reports

- Create a new project
- Add an image file to the project
- Search for file extensions



□ Search in Meta Files

□ Search in Selected Files only

□ Select all matches

● ASCII

○ Hex

□ Case Sensitive

□ Match whole word

● Search for files named :

○ Search for the pattern(s) :

```
.ods
.sxc
.dbx
```

Select the Disk(s) / Image(s) you want to search in :

F:\Work\GCFI-Win98.eve

□ Filter files by Date(s)

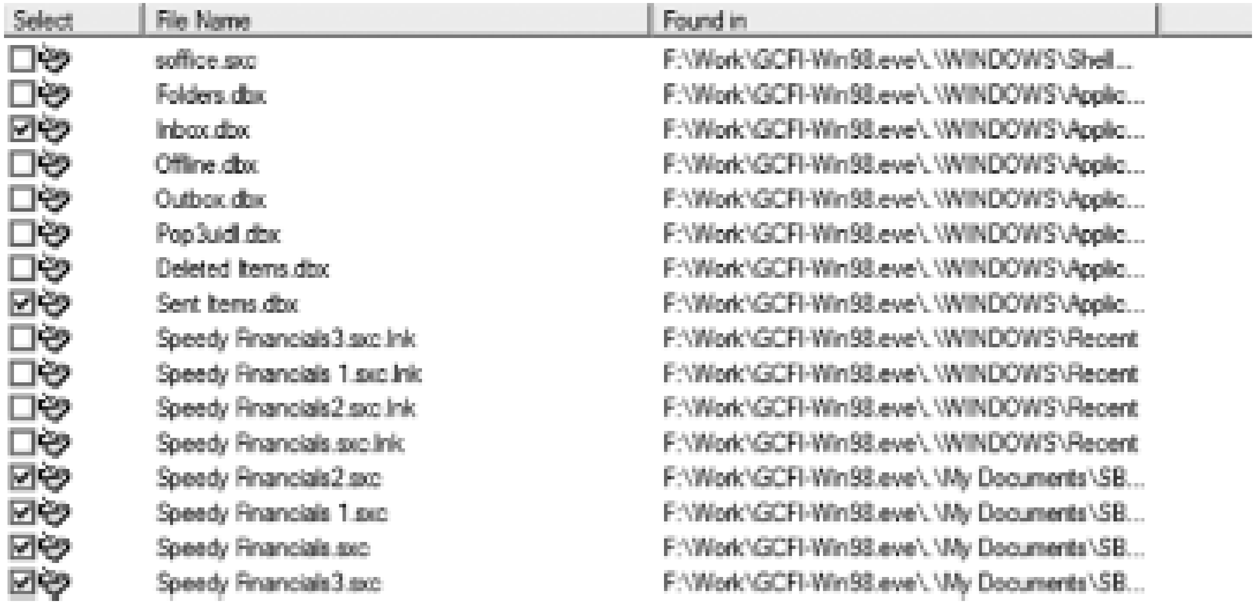
○ Modified

○ Created

○ Accessed

Figure 14-2 Searching for file extensions

Using ProDiscover Basic to Generate Reports (continued)



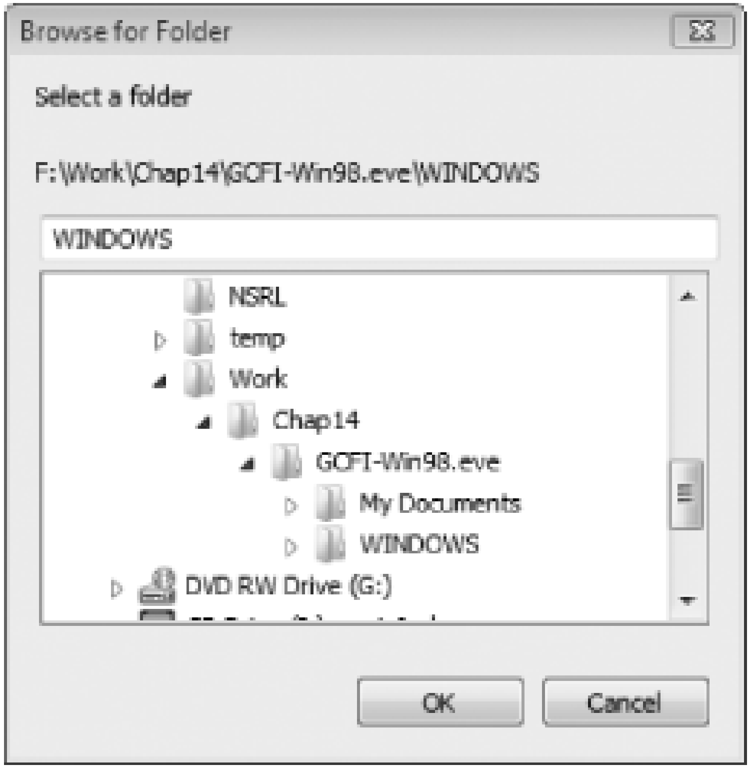
Select	File Name	Found in
□	soffice.sxc	F:\Work\GCFI-Win98.eve\.\WINDOWS\Shell...
□	Folders.dbx	F:\Work\GCFI-Win98.eve\.\WINDOWS\Applic...
☑	Inbox.dbx	F:\Work\GCFI-Win98.eve\.\WINDOWS\Applic...
□	Offline.dbx	F:\Work\GCFI-Win98.eve\.\WINDOWS\Applic...
□	Outbox.dbx	F:\Work\GCFI-Win98.eve\.\WINDOWS\Applic...
□	Pop3uidl.dbx	F:\Work\GCFI-Win98.eve\.\WINDOWS\Applic...
□	Deleted Items.dbx	F:\Work\GCFI-Win98.eve\.\WINDOWS\Applic...
☑	Sent Items.dbx	F:\Work\GCFI-Win98.eve\.\WINDOWS\Applic...
□	Speedy Financials3.sxc.lnk	F:\Work\GCFI-Win98.eve\.\WINDOWS\Recent
□	Speedy Financials 1.sxc.lnk	F:\Work\GCFI-Win98.eve\.\WINDOWS\Recent
□	Speedy Financials2.sxc.lnk	F:\Work\GCFI-Win98.eve\.\WINDOWS\Recent
□	Speedy Financials.sxc.lnk	F:\Work\GCFI-Win98.eve\.\WINDOWS\Recent
☑	Speedy Financials2.sxc	F:\Work\GCFI-Win98.eve\.\My Documents\SB...
☑	Speedy Financials 1.sxc	F:\Work\GCFI-Win98.eve\.\My Documents\SB...
☑	Speedy Financials.sxc	F:\Work\GCFI-Win98.eve\.\My Documents\SB...
☑	Speedy Financials3.sxc	F:\Work\GCFI-Win98.eve\.\My Documents\SB...

Figure 14-3 Selecting files in the search results

Using FTK Demo to Generate Reports

- Create a new case
- Add evidence to the case
- Analyze evidence with FTK
  - Look for image files
  - Locate encrypted files
  - Search for specific keywords
    - Indexed search
    - Live search

Using FTK Demo to Generate Reports (continued)



Browse for Folder

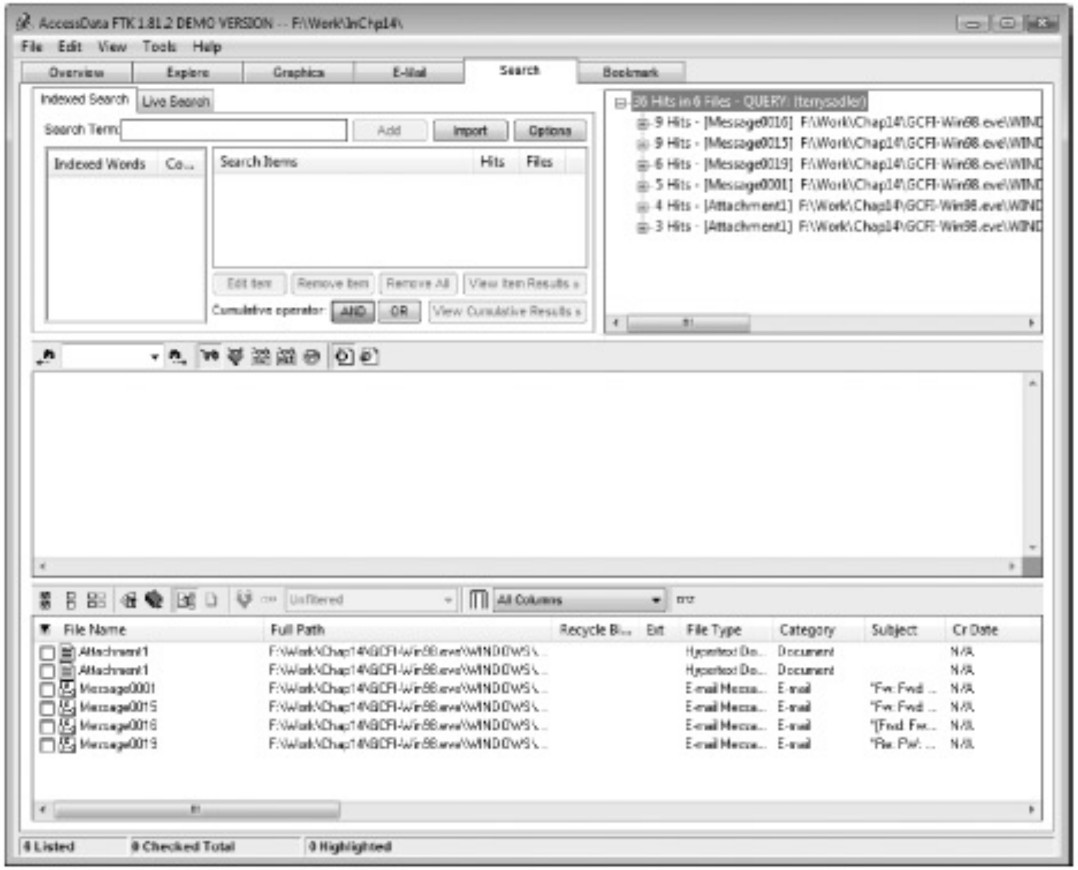
Select a folder

F:\Work\Chap14\GCFI-Win98.eve\WINDOWS

WINDOWS

Figure 14-4 Selecting the folder for extracted e-mail files

Using FTK Demo to Generate Reports (continued)



36 Hits in 6 Files - QUERY: (terrysadler)
- 9 Hits - [Message0016] F:\Work\Chap14\GCFI-Win98.eve\WIND
- 9 Hits - [Message0015] F:\Work\Chap14\GCFI-Win98.eve\WIND
- 6 Hits - [Message0019] F:\Work\Chap14\GCFI-Win98.eve\WIND
- 5 Hits - [Message0001] F:\Work\Chap14\GCFI-Win98.eve\WIND
- 4 Hits - [Attachment1] F:\Work\Chap14\GCFI-Win98.eve\WIND
- 3 Hits - [Attachment1] F:\Work\Chap14\GCFI-Win98.eve\WIND

File Name	Full Path	Recycle Bi...	Ext	File Type	Category	Subject	Cr Date
□ Attachment1	F:\Work\Chap14\GCFI-Win98.eve\WINDOWS\...			Hypertext Do...	Document		N/A
□ Attachment1	F:\Work\Chap14\GCFI-Win98.eve\WINDOWS\...			Hypertext Do...	Document		N/A
□ Message0001	F:\Work\Chap14\GCFI-Win98.eve\WINDOWS\...			E-mail Messa...	E-mail	"Fw: Fwd: ...	N/A
□ Message0015	F:\Work\Chap14\GCFI-Win98.eve\WINDOWS\...			E-mail Messa...	E-mail	"Fw: Fwd: ...	N/A
□ Message0016	F:\Work\Chap14\GCFI-Win98.eve\WINDOWS\...			E-mail Messa...	E-mail	"[Fwd: Fw:...	N/A
□ Message0019	F:\Work\Chap14\GCFI-Win98.eve\WINDOWS\...			E-mail Messa...	E-mail	"Re: FW: ...	N/A

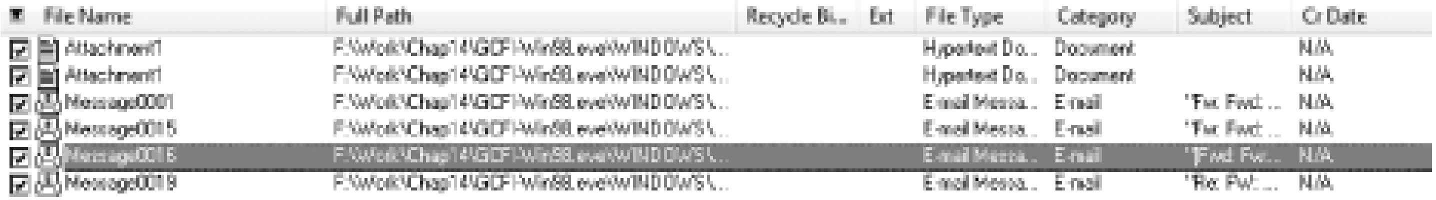
6 Listed | 0 Checked Total | 0 Highlighted

Figure 14-5 Indexed search results for the name terrysadler

Using FTK Demo to Generate Reports (continued)

- Create bookmarks
- Generate a report from your bookmarks

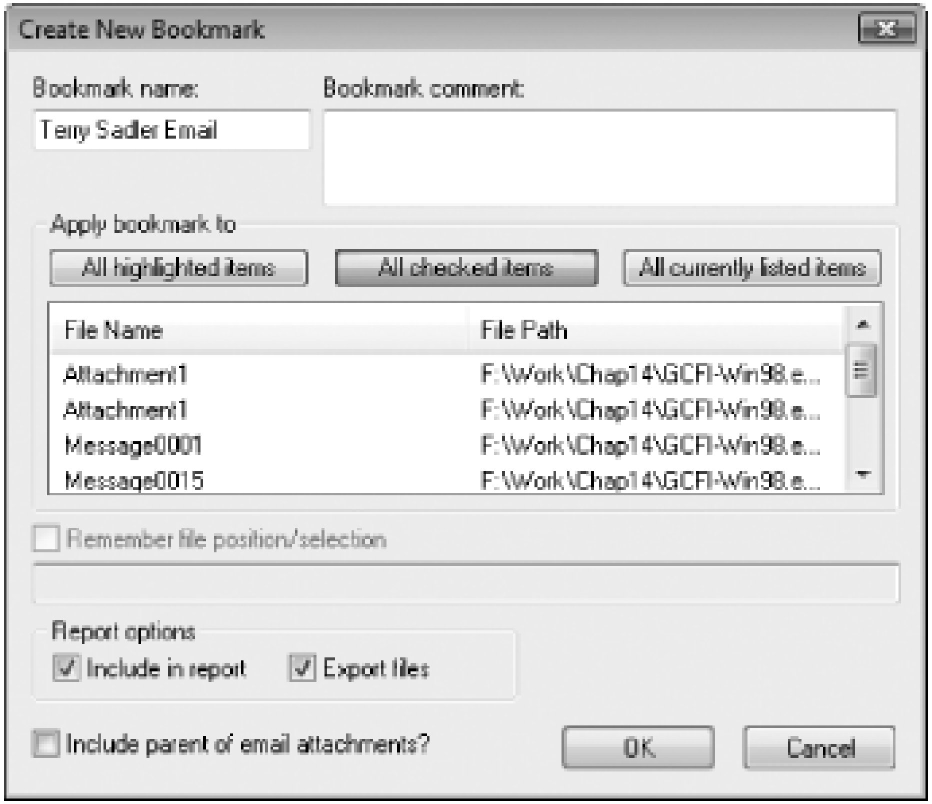
Using FTK Demo to Generate Reports (continued)



	File Name	Full Path	Recycle Bi...	Ext	File Type	Category	Subject	Cr Date
☑	Attachment1	F:\Work\Chap14\GCFI-Win98.eve\WINDOWS\...			Hypertext Do...	Document		N/A
☑	Attachment1	F:\Work\Chap14\GCFI-Win98.eve\WINDOWS\...			Hypertext Do...	Document		N/A
☑	Message0001	F:\Work\Chap14\GCFI-Win98.eve\WINDOWS\...			E-mail Messa...	E-mail	"Fw: Fwd: ...	N/A
☑	Message0015	F:\Work\Chap14\GCFI-Win98.eve\WINDOWS\...			E-mail Messa...	E-mail	"Fw: Fwd: ...	N/A
☑	Message0016	F:\Work\Chap14\GCFI-Win98.eve\WINDOWS\...			E-mail Messa...	E-mail	"[Fwd: Fw:...	N/A
☑	Message0019	F:\Work\Chap14\GCFI-Win98.eve\WINDOWS\...			E-mail Messa...	E-mail	"Re: FW: ...	N/A

Figure 14-6 Files selected to be bookmarked

Using FTK Demo to Generate Reports (continued)



Bookmark name: Terry Sadler Email

Bookmark comment:

File Name	File Path
Attachment1	F:\Work\Chap14\GCFI-Win98.e...
Attachment1	F:\Work\Chap14\GCFI-Win98.e...
Message0001	F:\Work\Chap14\GCFI-Win98.e...
Message0015	F:\Work\Chap14\GCFI-Win98.e...

☐ Remember file position/selection

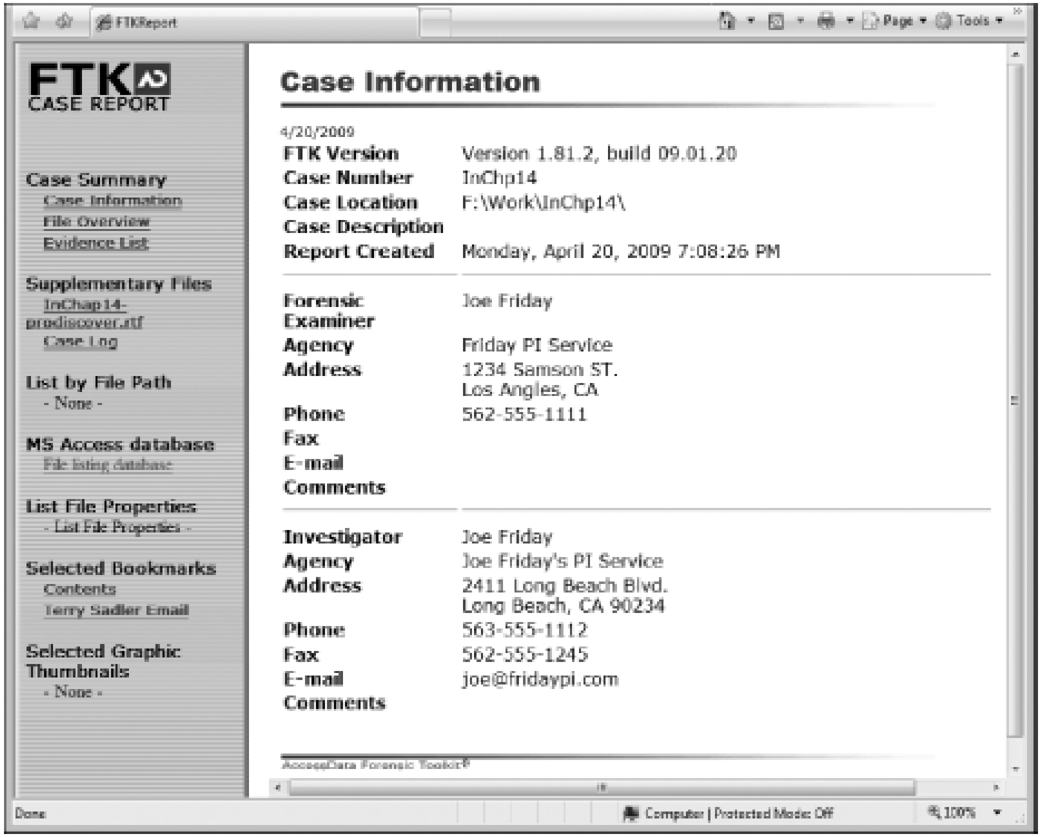
Report options

☑ Include in report ☑ Export files

☐ Include parent of email attachments?

Figure 14-7 Selecting settings in the Create New Bookmark dialog box

Using FTK Demo to Generate Reports (continued)



FTK CASE REPORT

Case Summary
- Case Information
- File Overview
- Evidence List

Supplementary Files
- InChap14-prodiscover.rtf
- Case Log

List by File Path
- None -

MS Access database
- File listing database

List File Properties
- List File Properties -

Selected Bookmarks
- Contents
- Terry Sadler Email

Selected Graphic Thumbnails
- None -

Case Information

4/20/2009

FTK Version	Version 1.81.2, build 09.01.20
Case Number	InChp14
Case Location	F:\Work\InChp14\
Case Description	
Report Created	Monday, April 20, 2009 7:08:26 PM
Forensic Examiner	Joe Friday
Agency	Friday PI Service
Address	1234 Samson ST. Los Angles, CA
Phone	562-555-1111
Fax	
E-mail	
Comments	
Investigator	Joe Friday
Agency	Joe Friday's PI Service
Address	2411 Long Beach Blvd. Long Beach, CA 90234
Phone	563-555-1112
Fax	562-555-1245
E-mail	joe@fridaypi.com
Comments	

AccessData Forensic Toolkit®

Figure 14-8 The completed case report

Summary

- All U.S. district courts and many state courts require expert witnesses to submit written reports
- Attorneys use deposition banks to research expert witnesses' previous testimony
- Reports should answer the questions you were retained to answer
- A well-defined report structure contributes to readers' ability to understand the information you're communicating

Summary (continued)

- Clarity of writing is critical to a report’s success
- Convey a tone of objectivity and be detached in your observations