



**CYBER CRIME AND CYBER SECURITY** |

# AGENDA

Field of digital forensics

Prepare computer investigation and summarize PS and Private Sector investigations

Importance of professional conduct

How to prepare a digital investigation—systematic approach

Procedures for private sector digital investigations

Requirements for data recovery workstations and softwares

Handson

# DIGITAL FORENSICS

“[t]he application of computer science and investigative procedures for a legal purpose involving the analysis of digital evidence (information of probative value that is stored or transmitted in binary form) after proper search authority, chain of custody, validation with mathematics (hash function), use of validated tools, repeatability, reporting and possible expert presentation”


: Defining Digital Forensics,” Forensic Magazine, 2007

# SEARCH WARRANTS

the Pennsylvania Supreme Court addressed expectations of privacy and whether evidence is admissible (Copenhefer, p. 559)

“[E]ven though his computer was validly seized pursuant to a warrant, his attempted deletion of the documents in question created an expectation of privacy protected by the Fourth Amendment.

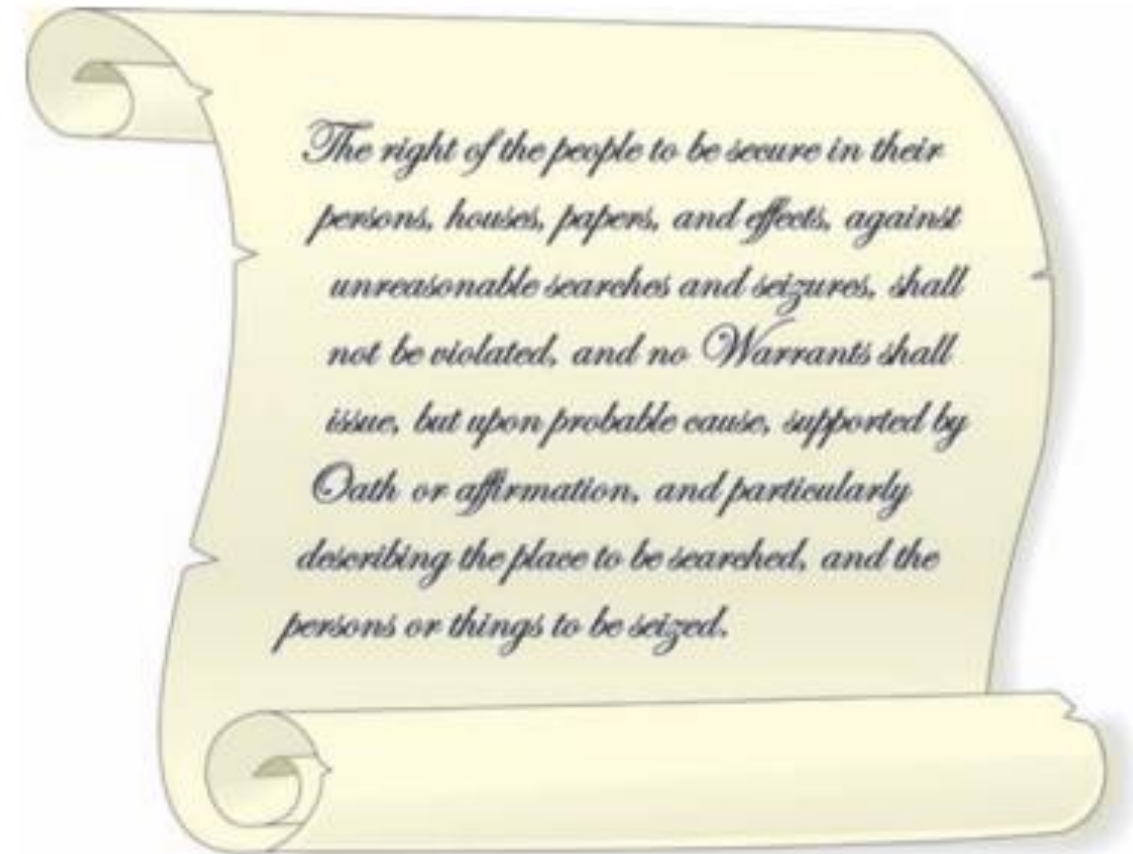
Agent Johnson’s retrieval of the documents, without first obtaining another search warrant, was unreasonable under the Fourth Amendment and the documents thus seized should have been suppressed”



“A defendant’s attempt to secrete evidence of a crime is not synonymous with a legally cognizable expectation of privacy. A mere hope for secrecy is not a legally protected expectation. If it were, search warrants would be required in a vast number of cases where warrants are clearly not necessary” (Copenhefer, p. 562).

The Fourth Amendment to the U.S. Constitution (and each state's constitution) protects everyone's right to be secure in their person, residence, and property from search and seizure.

Find out the equivalent in Indian Constitution.



**Figure 1-5** The Fourth Amendment



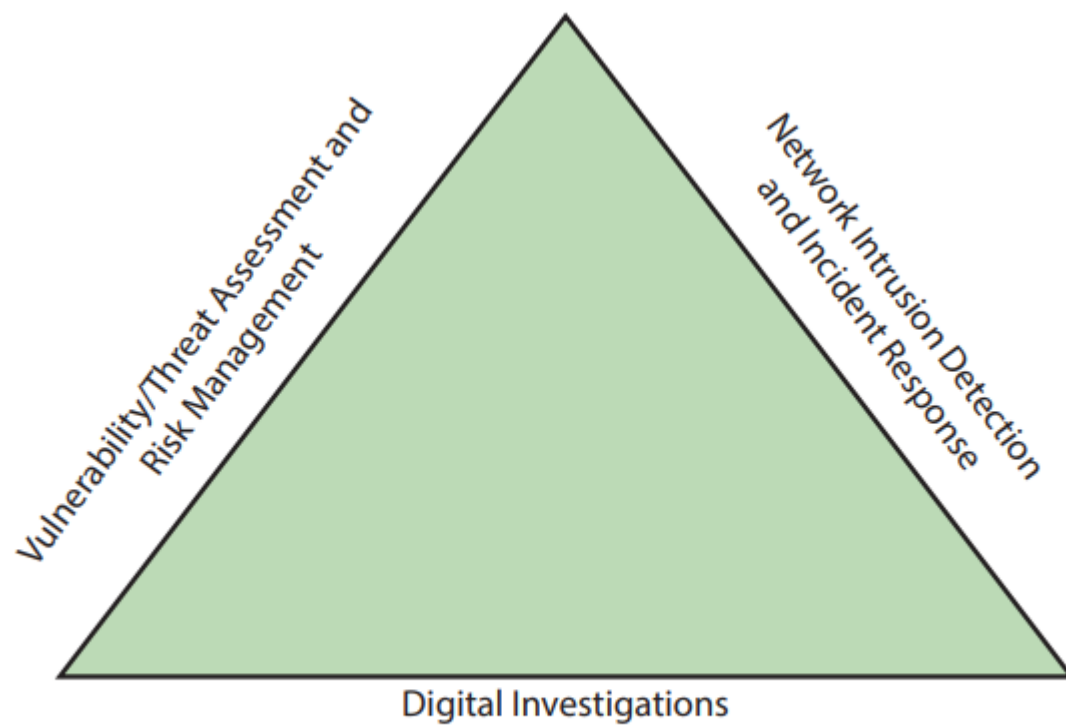
Digital forensics is also different from data recovery,



In data recovery, typically you know what you're looking for

Digital forensics is the task of recovering data that users have hidden or deleted, with the goal of ensuring that the recovered data is valid so that it can be used as evidence





**Figure 1-1** The investigations triad



vulnerability/threat assessment and risk management group, you test and verify the integrity of stand-alone workstations and network servers.

network intrusion detection and incident response detects intruder attacks by using automated tools and monitoring network firewall logs

digital investigations group manages investigations and conducts forensics analysis of systems suspected of containing evidence related to an incident or a crime



# CRIMES

one-half cent crime.



# DATA RETREIVAL

Norton DiskEdit, Xtree Gold

# UNDERSTANDING CASE LAW

law enforcement can certainly confiscate anything an arrested person is carrying and log that a device, such as a smartphone, was on the person, they don't necessarily have the right or authority to search the device. These actions are being challenged in courts constantly

# DEVELOPING DIGITAL FORENSICS RESOURCES

Preparing for Digital Investigations



# FOLLOWING LEGAL PROCESSES

A Digital Evidence First Responder (DEFR) has the skill and training to arrive on an incident scene, assess the situation, and take precautions to acquire and preserve evidence.

A Digital Evidence Specialist (DES) has the skill to analyze the data and determine when another specialist should be called in to assist with the analysis.

submit an affidavit (also called a “declaration”)  
which must include exhibits (evidence)

# UNDERSTANDING PRIVATE-SECTOR INVESTIGATIONS

white-collar crimes

industrial espionage, which involves selling sensitive or confidential company information to a competitor.

Establishing Company Policies

a line of authority for conducting internal investigations

Designating an Authorized Requester



# CONDUCTING SECURITY INVESTIGATIONS

Three types of situations are common in private-sector environments:

- Abuse or misuse of digital assets
- E-mail abuse
- Internet abuse

# TAKING A SYSTEMATIC APPROACH

Make an initial assessment about the type of case you're investigating

Determine a preliminary design or approach to the case

Create a detailed checklist

Determine the resources you need

Obtain and copy an evidence drive

Identify the risks

Mitigate or minimize the risks

Test the design

Analyze and recover the digital evidence

Investigate the data you recover

Complete the case report

Critique the case

# PLANNING YOUR INVESTIGATION

1. Acquire the USB drive from the IT Department, which bagged and tagged the evidence.
2. Complete an evidence form and establish a chain of custody.
3. Transport the evidence to your digital forensics lab.
4. Place the evidence in an approved secure container.
5. Prepare your forensic workstation.
6. Retrieve the evidence from the secure container.
7. Make a forensic copy of the evidence drive (in this case, the USB drive).
8. Return the evidence drive to the secure container.
9. Process the copied evidence drive with your digital forensics tools.



# INTERNET ABUSE INVESTIGATIONS

u need the following:

- The organization's Internet proxy server logs
- Suspect computer's IP address obtained from your organization's network administrator
- Suspect computer's disk drive
- Your preferred digital forensics analysis tool



The following steps outline the recommended processing of an Internet abuse case:

1. Use the standard forensic analysis techniques and procedures described in this book

for the disk drive examination.

2. Search for and extract all Web page URLs and other associated information.

Contact the network firewall administrator and request a proxy server log

Compare the data recovered from forensics analysis with the network server log data to confirm that they match.

URL data matches the network server log and the forensic disk

# E-MAIL ABUSE INVESTIGATIONS (YOU NEED)

An electronic copy of the offending e-mail that contains message header data;  
consult with your e-mail server administrator

- If available, e-mail server log records; consult with your e-mail server administrator to see whether they are available
- For e-mail systems that store users' messages on a central server, access to the server; consult with your e-mail server administrator

For e-mail systems that store users' messages on a computer as an Outlook .pst or .ost file, for example, access to the computer so that you can perform a forensic analysis on it

- Your preferred digital forensics analysis tool

# SETTING UP YOUR WORKSTATION FOR DIGITAL FORENSICS

A workstation running Windows 7 or later

- A write-blocker device
- Digital forensics acquisition tool
- Digital forensics analysis tool
- A target drive to receive the source or suspect disk data
- Spare PATA and SATA ports
- USB ports

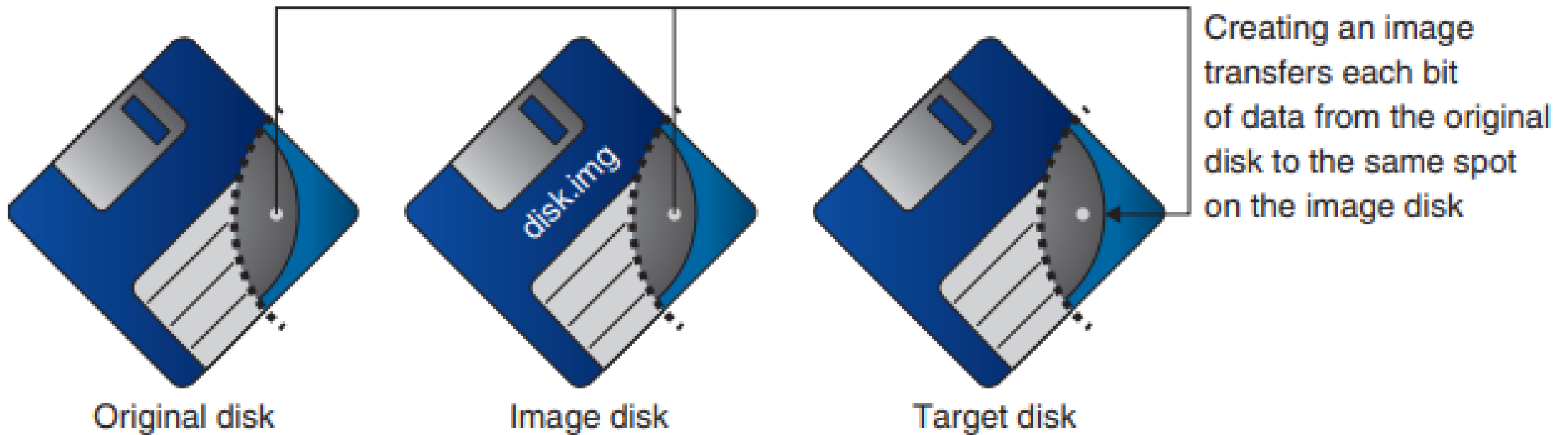


# ADDITIONAL TOOLS

Network interface card (NIC)

- Extra USB ports
- FireWire 400/800 ports
- SCSI card
- Disk editor tool
- Text editor tool
- Graphics viewer program
- Other specialized viewing tools

# UNDERSTANDING BIT-STREAM COPIES



**Figure 1-11** Transfer of data from original to image to target

# ANALYZING YOUR DIGITAL EVIDENCE

<https://sourceforge.net/projects/autopsy/files/autopsy/4.3.0/>

Double-click the Ch01InChap01.exe file in File Explorer to uncompress it into Ch01InChap01.dd. Start Autopsy for Windows.

Create a new case

New Case Information

**Steps**

1. Case Info
2. Additional Information

**Case Info**

**Enter New Case Information:**

Case Name: InChap01

Base Directory: C:\Work\Chap01\Chapter Browse

Case Type: ☒ Single-user ☐ Multi-user

Case data will be stored in the following directory:

C:\Work\Chap01\Chapter\InChap01

< Back Next > Finish Cancel Help

Figure 1-12 The New Case Information window



### Steps

1. Case Info
2. **Additional Information**

### Additional Information

#### Optional: Set Case Number and Examiner

Case Number:

Examiner:

< Back

Next >

Finish

Cancel

Help

**Steps**

1. **Select Data Source**
2. Configure Ingest Modules
3. Add Data Source

**Select Data Source**

Select data source type: Disk Image or VM File

Browse for an image file:

C:\Work\Chap01\Chapter\Inchp01.dd

Browse

Please select the input timezone: (GMT-8:00) America/Los\_Angeles

☐ Ignore orphan files in FAT file systems

(faster results, although some data will not be searched)

< Back

Next >

Finish

Cancel

Help

# STEPS TO DISPLAY THE CONTENTS

In the Tree Viewer pane on the left, click to expand Views, File Types, By Extension, and Documents

2. Under Documents, click Office. In the Result Viewer (upper-right pane), click the first file, Billing Letter.doc, to display its contents in the Content Viewer (lower-right pane).
3. Right-click Billing Letter.doc, point to Tag File, and click Tag and Comment.
4. In the Create Tag dialog box, click the New Tag Name button. In the New Tag section, type Recovered Office Documents in the Tag Name text box, click OK, and then click OK again.

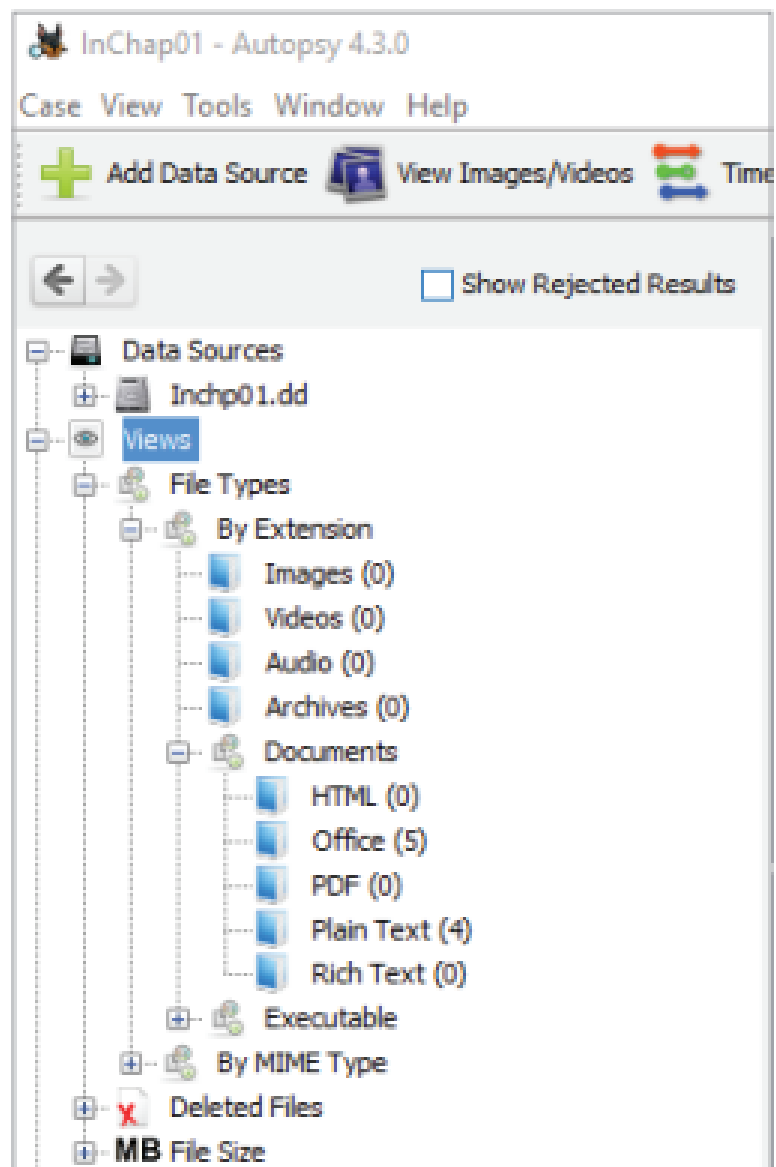
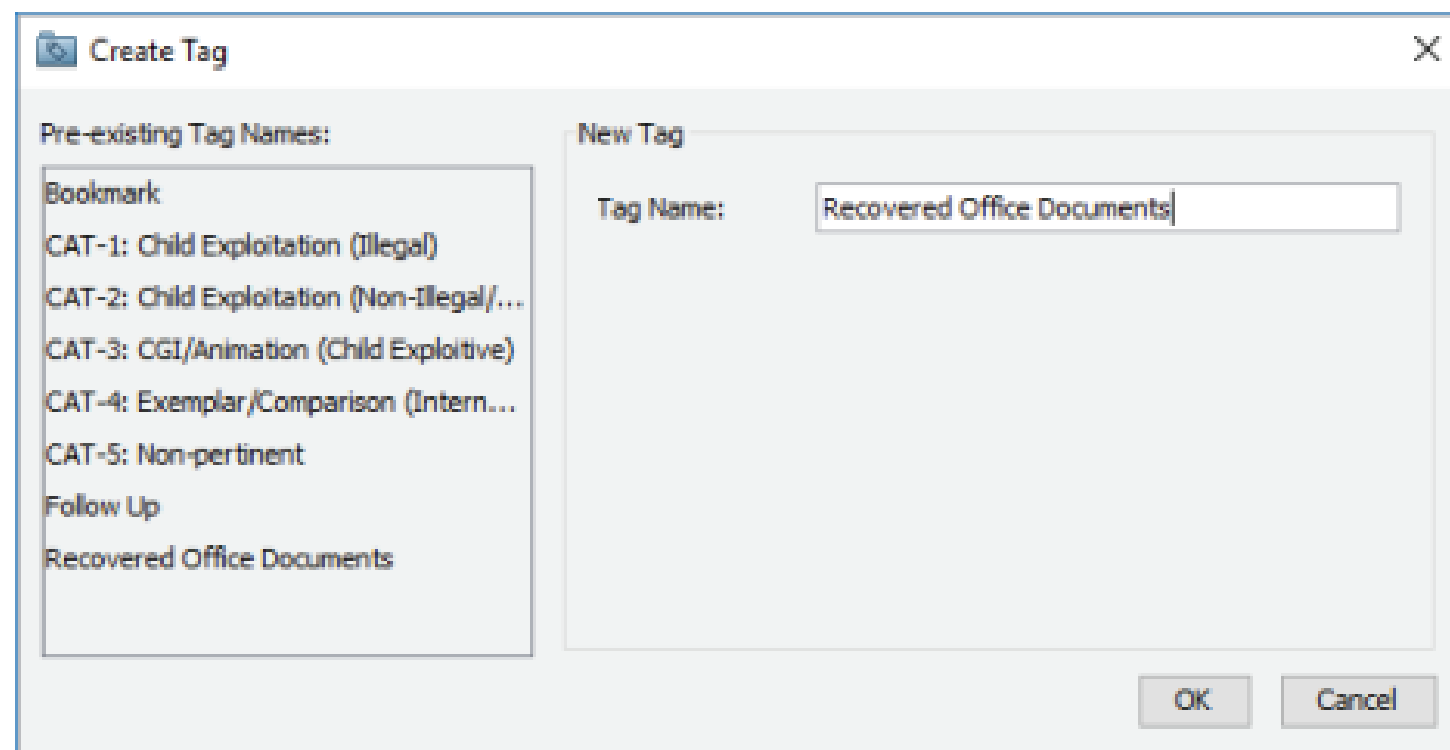
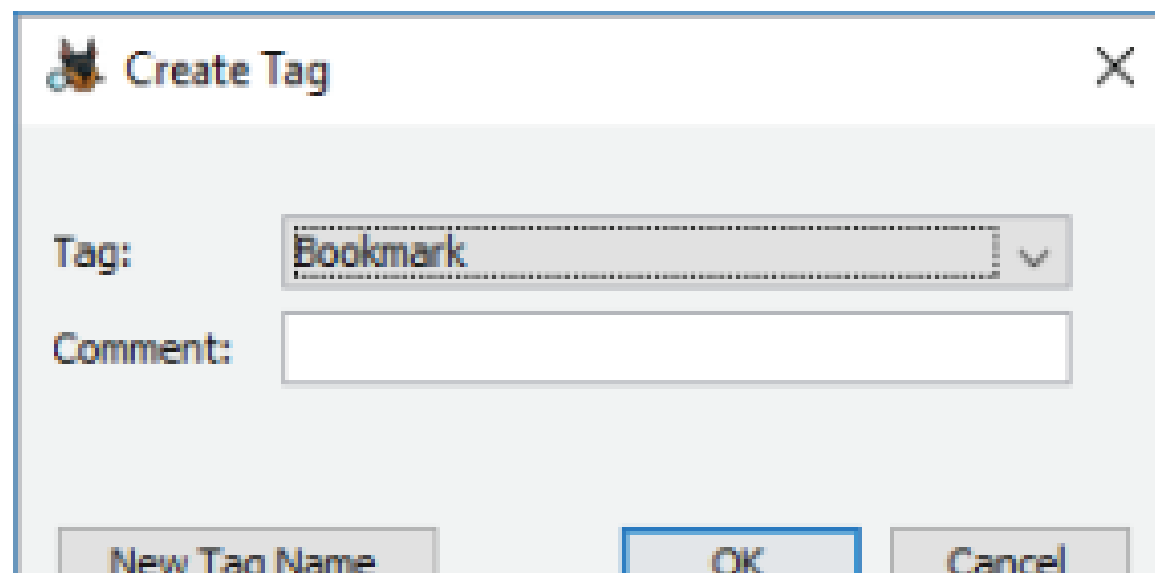








Figure 1-15 Autopsy's Tree View



In the Result Viewer pane, Ctrl+click Billing Letter.doc, Income.xls, Regrets.doc, f0000000.doc, and f0000049.doc to select these files, and then release the Ctrl key. Right-click the highlighted files shown in Figure 1-17, point to Tag File and then Quick Tag, and then click Recovered Office Documents.

Directory Listing				
Office				
Table Thumbnail				
Name	Location	Modified Time	Change Time	Access Time
 Billing Letter.doc	/img_Inchp01.dd/Billing Letter.doc	2005-12-09 06:50:28 PST	0000-00-00 00:00:00	2005-12-09 00:00:00 PST
 Income.xls	/img_Inchp01.dd/Income.xls	2005-12-09 06:52:18 PST	0000-00-00 00:00:00	2005-12-09 00:00:00 PST
 Regrets.doc	/img_Inchp01.dd/Regrets.doc	2005-12-09 06:50:52 PST	0000-00-00 00:00:00	2005-12-09 00:00:00 PST
 f0000000.doc	/img_Inchp01.dd/\$CarvedFiles/f0000000.doc	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00
 f0000049.doc	/img_Inchp01.dd/\$CarvedFiles/f0000049.doc	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00



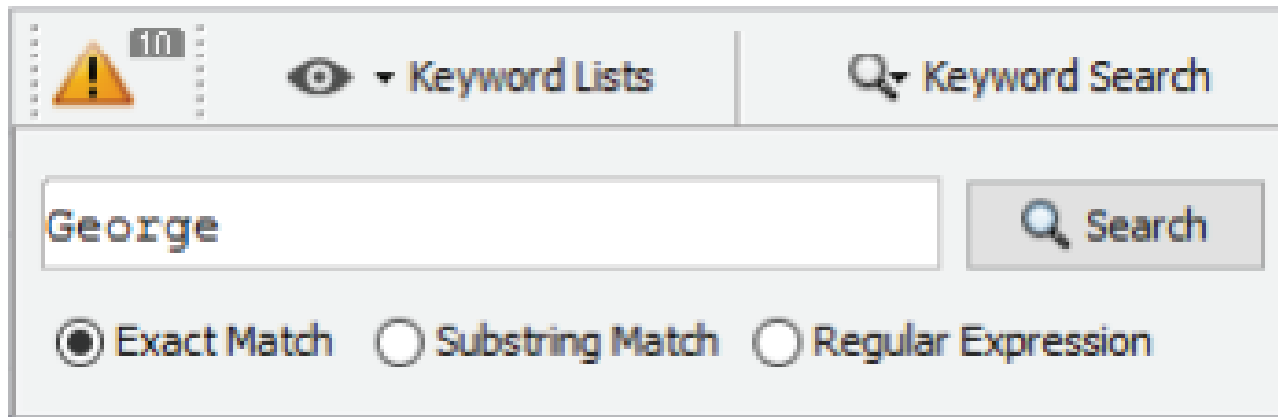


Under Documents in the Tree Viewer pane, click Plain Text to display more recovered files.

7. In the Result Viewer pane, select the files listed in Step 5 again, right-click the selection, point to Tag File and then Quick Tag, and then click Follow Up. Leave Autopsy running for the next activity

# AFTER GATHERING EVIDENCE

Click the Keyword Search button at the far upper right, type George in the text box



The image shows a software interface for keyword searching. At the top left, there is a yellow warning triangle icon with an exclamation mark and a small '11' in a box. To its right is an eye icon followed by a dropdown menu labeled 'Keyword Lists'. Further right is a button with a magnifying glass icon and the text 'Keyword Search'. Below these elements is a text input field containing the word 'George'. To the right of the text field is a button with a magnifying glass icon and the text 'Search'. Below the text field and search button are three radio buttons: 'Exact Match' (which is selected), 'Substring Match', and 'Regular Expression'.

**Figure 1-18** Entering a keyword search term

In the Result Viewer pane, a new tab named Keyword search 1 opens. Click each file to view its contents in the Content Viewer (see Figure 1-19). Look for files containing the name “George.”

Directory Listing

Keyword search 1 - George

Keyword search

10 Results

Table

Thumbnail

Name	Location	Modified Time	Change Time	Access Time
Unalloc_16_121344_1474560	/img_Inchp01.dd/\$Unalloc/Unalloc_16_121344_1474560	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00
f0000000.doc	/img_Inchp01.dd/\$CarvedFiles/f0000000.doc	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00
f0000047.txt	/img_Inchp01.dd/\$CarvedFiles/f0000047.txt	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00
f0000048.txt	/img_Inchp01.dd/\$CarvedFiles/f0000048.txt	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00
Billing Letter.doc	/img_Inchp01.dd/Billing Letter.doc	2005-12-09 06:50:28 PST	0000-00-00 00:00:00	2005-12-09 00:00:00 PST
f0000049.doc	/img_Inchp01.dd/\$CarvedFiles/f0000049.doc	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00
confirmation.txt	/img_Inchp01.dd/confirmation.txt	2005-12-09 06:52:58 PST	0000-00-00 00:00:00	2005-12-09 00:00:00 PST
Income.xls	/img_Inchp01.dd/Income.xls	2005-12-09 06:52:18 PST	0000-00-00 00:00:00	2005-12-09 00:00:00 PST
letter1.txt	/img_Inchp01.dd/letter1.txt	2005-12-09 06:51:50 PST	0000-00-00 00:00:00	2005-12-09 00:00:00 PST
Regrets.doc	/img_Inchp01.dd/Regrets.doc	2005-12-09 06:50:52 PST	0000-00-00 00:00:00	2005-12-09 00:00:00 PST

Hex

Strings

File Metadata

Results

Indexed Text

Media

Matches on page: 1 of 1

Match

Page: 1 of 1

Page

Search Results

f0000048.txt Earl,  
We need to meet on the 18th of August to confirm the work I am  
doing for you. Please contact me ASAP.  
  
George  
  
-----METADATA-----  
  
Content-Encoding: windows-1252  
Content-Type: text/plain; charset=windows-1252

# CLOSING THE CASE

Click the Keyword Lists button at the far upper right, click the Email Addresses check box, and then click Search.

In the Result Viewer pane, a new tab named Keyword search 2 opens. Click each file to view its contents in the Content Viewer pane and examine all e-mail addresses found in the search.