Lab Manual

For

M.Sc.(I.T.)

Part II **Sem IV**

Course :

PSIT403c Computer Forensics

2014 – 2015

Practicals Prepared and Implemented
by
Mr. Mahesh Naik, Valia College, Andheri

List of practicals & tools

Practical	**Tool**
1 File system Analysis using The Slueth kit	Sleuth Kit ,Autopsy
2. Using Windows Forensics toolkit	Access data FTK
3. Using Data acquisition tools	ProDiscover Basic.
4. Using file recovery tools	FTK Imager
5. using FTK	Access data FTK
6. Forensic investigation using Encase	Encase
7. using Steganography tools	ProDiscover Basic.
8. using password cracking tools	Cain & Abel
9 & 10. using Log & traffic capturing and analysis tools	wireshark
11. using email forensics tool	AccessData FTK
12. using mobile forensics tools	Mobiledit & Simmanager
13. Writing report using FTK	AccessData FTK

Practical No.1 : File system Analysis using The Slueth kit

Aim : Exploring Autopsy.

Theory & steps:

Slueth Kit

- Sleuth Kit is a C library and collection of command line file and volume system forensic analysis tools.
- The file system tools allow you to examine file systems of a suspect computer in a non-intrusive fashion.
- Because the tools do not rely on the operating system to process the file systems, deleted and hidden content is shown. It runs on Windows and Unix platforms.
- http://www.sleuthkit.org/

What is Autopsy

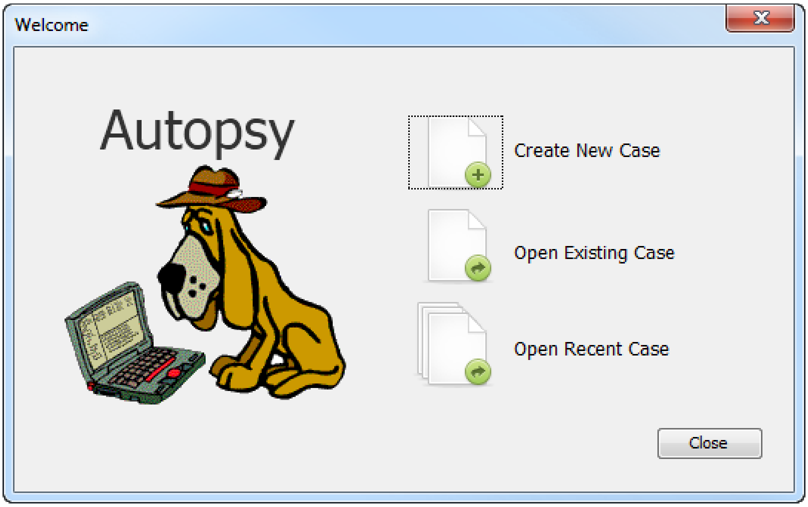
Autopsy is an open source forensics tool that can be compared to FTK or EnCase and is able to assist investigators when working on cases.

The Autopsy is a graphical interface to the command line digital investigation tools in The Sleuth Kit. Together, they allow you to investigate the file system and volumes of a computer.

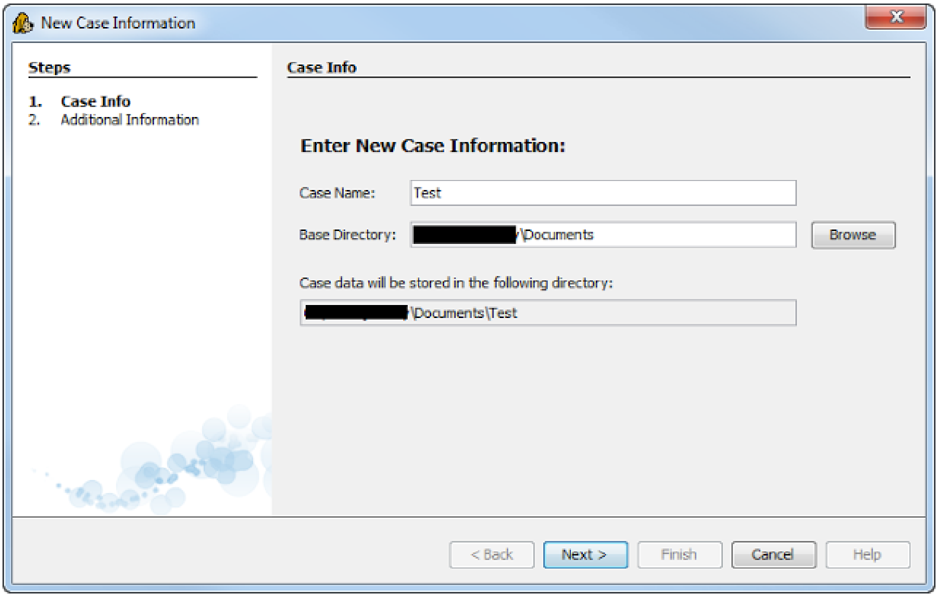
http://www.sleuthkit.org/autopsy/

How to Start a Case

Upon starting Autopsy 3, a window will open with three selections to make: create a new case, open existing case, or to open a recent case.



select the “Create New Case” option and be directed to a new window that will have information to fill in, we will be naming the case “Test.”



Enter New Case Information:

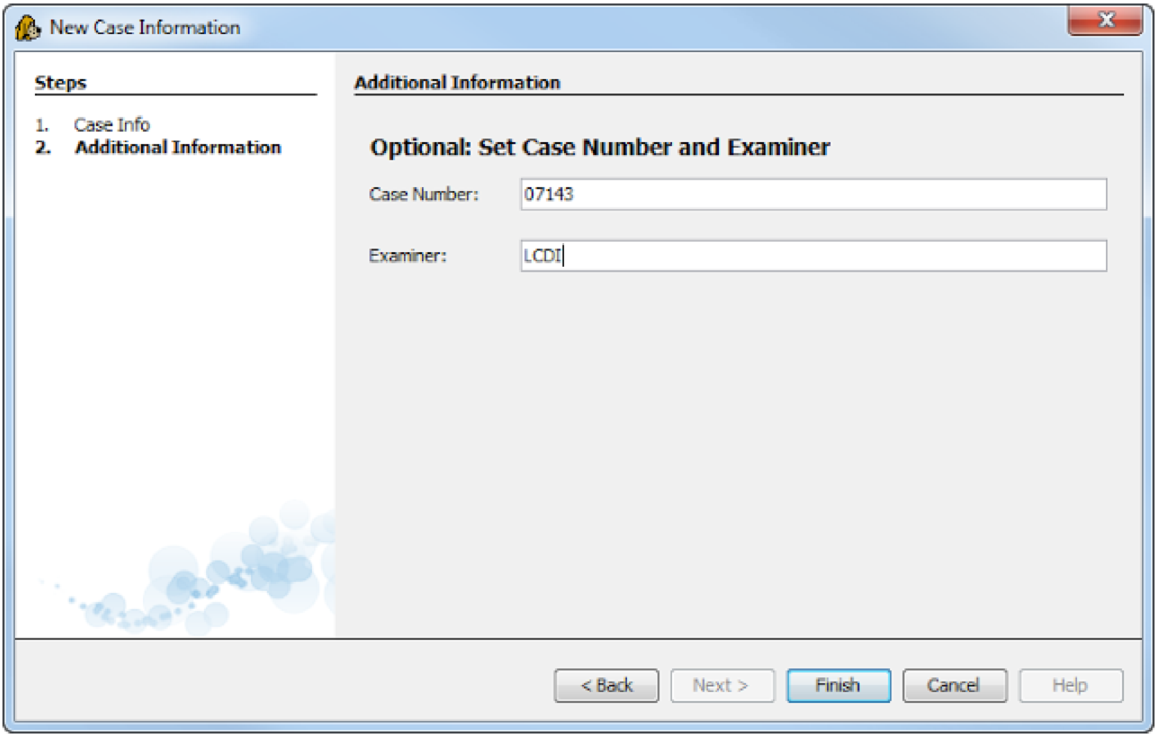
Case Name: Test

Base Directory: [redacted]\Documents

Case data will be stored in the following directory:

[redacted]\Documents\Test

After the information has been filled in select the next button. The next window will allow the investigator to fill in the case number and examiner name. This is for the purpose of creating better documentation and logging. After the information is filled in select the finish button to continue.

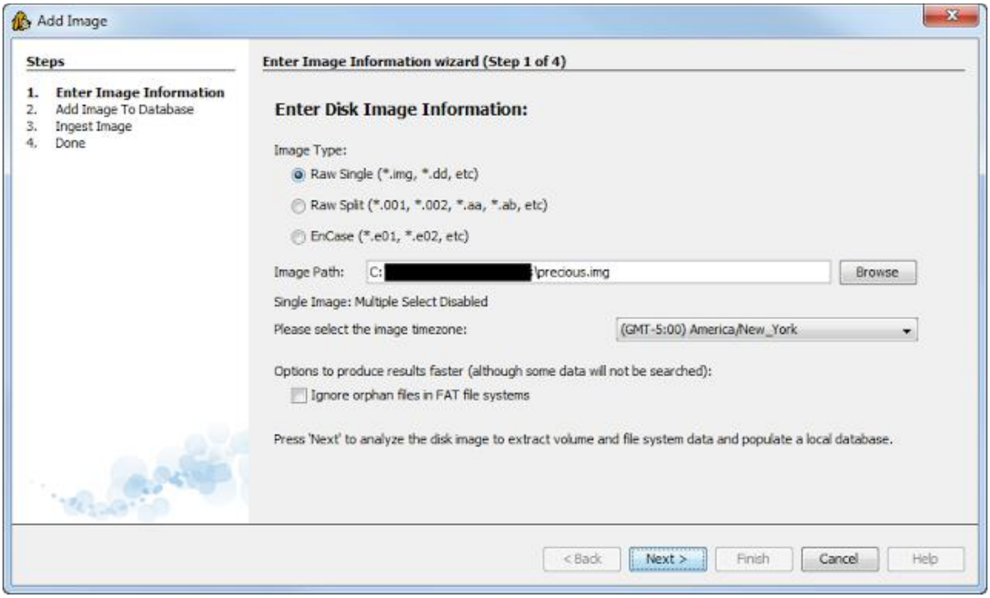


Optional: Set Case Number and Examiner

Case Number: 07143

Examiner: LCDI

The next step in the investigation will be to add an image file to the case. The image file can be chosen from a wide variety of formats including: img, dd, 001, aa, and e01. Use the browse button to find the image that is desired to work with and select add. Options to choose the timezone of where the image came from as well as to ignore orphan files in FAT file systems are available to be selected based on the investigators preference and situation.



Enter Image Information wizard (Step 1 of 4)

Enter Disk Image Information:

Image Type:

● Raw Single (*.img, *.dd, etc)

○ Raw Split (*.001, *.002, *.aa, *.ab, etc)

○ EnCase (*.e01, *.e02, etc)

Image Path: C:[redacted]\precious.img

Single Image: Multiple Select Disabled

Please select the image timezone: (GMT-5:00) America/New_York

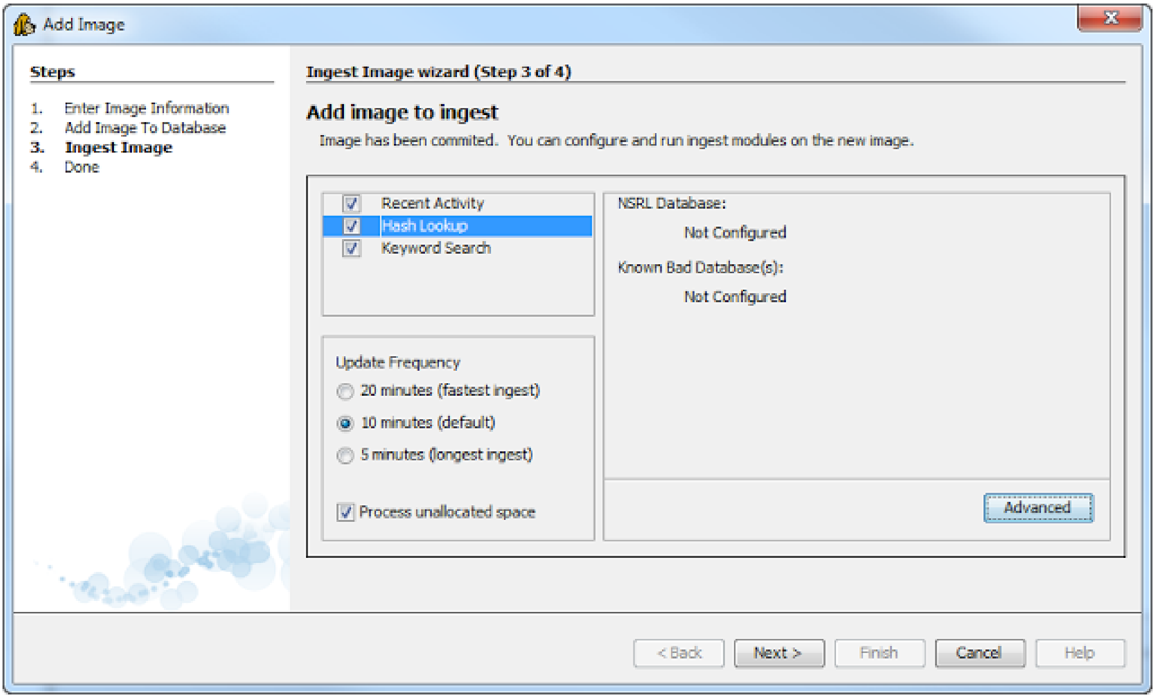
Options to produce results faster (although some data will not be searched):

□ Ignore orphan files in FAT file systems

Press 'Next' to analyze the disk image to extract volume and file system data and populate a local database.

After selecting the next button the image will be added to the case and the next button should be selected again if there are no errors.

The following window will bring the investigator to the Ingest wizard panel, which is one of the new features offered in Autopsy. There are three options in the first box: Recent Activity, Hash lookup, and Keyword Searches.



Add Image

Steps

1. Enter Image Information
2. Add Image To Database
3. **Ingest Image**
4. Done

Ingest Image wizard (Step 3 of 4)

Add image to ingest

Image has been commited. You can configure and run ingest modules on the new image.

☑ Recent Activity
☑ Hash Lookup
☑ Keyword Search

NSRL Database:
Not Configured

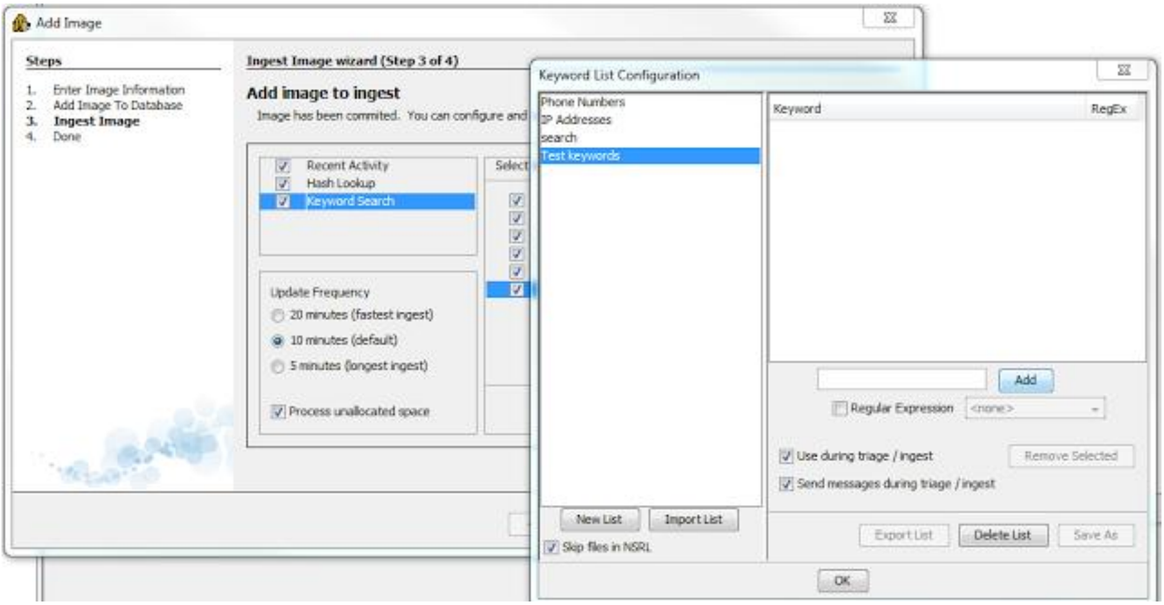
Known Bad Database(s):
Not Configured

Update Frequency
○ 20 minutes (fastest ingest)
● 10 minutes (default)
○ 5 minutes (longest ingest)

☑ Process unallocated space

By selecting any of the options advanced settings can be set to increase the capabilities of the search. Under the Hash Lookup option there is the advanced option to add databases of known hashes.

Under the Keyword Search option are many different lists that can be used to search for information. By default, Phone Numbers, IP Addresses, Email Addresses, and URL's are available. Select the Advanced button and a Keyword List Configuration window will open. In this new window select New List and type the name that is desired for the list. This makes it easier to search by subject matter or other organizational methods. For now the list Test keywords will be used to create a list. In the adjacent pane there is a blank section with a word bar and an Add button next to it. Type the keyword desired (case sensitive) and select Add to add the word to the list. There is also the option to select Regular Expression. This allows the investigator to further narrow the field to search in by selecting what the keyword is that is being searched for including: passwords, emails, text file name, domains, and many more options.



Add Image

Steps

1. Enter Image Information
2. Add Image To Database
3. **Ingest Image**
4. Done

Ingest Image wizard (Step 3 of 4)

Add image to ingest

Image has been commited. You can configure and

☑ Recent Activity
☑ Hash Lookup
☑ Keyword Search

Update Frequency

○ 20 minutes (fastest ingest)
● 10 minutes (default)
○ 5 minutes (longest ingest)

☑ Process unallocated space

Keyword List Configuration

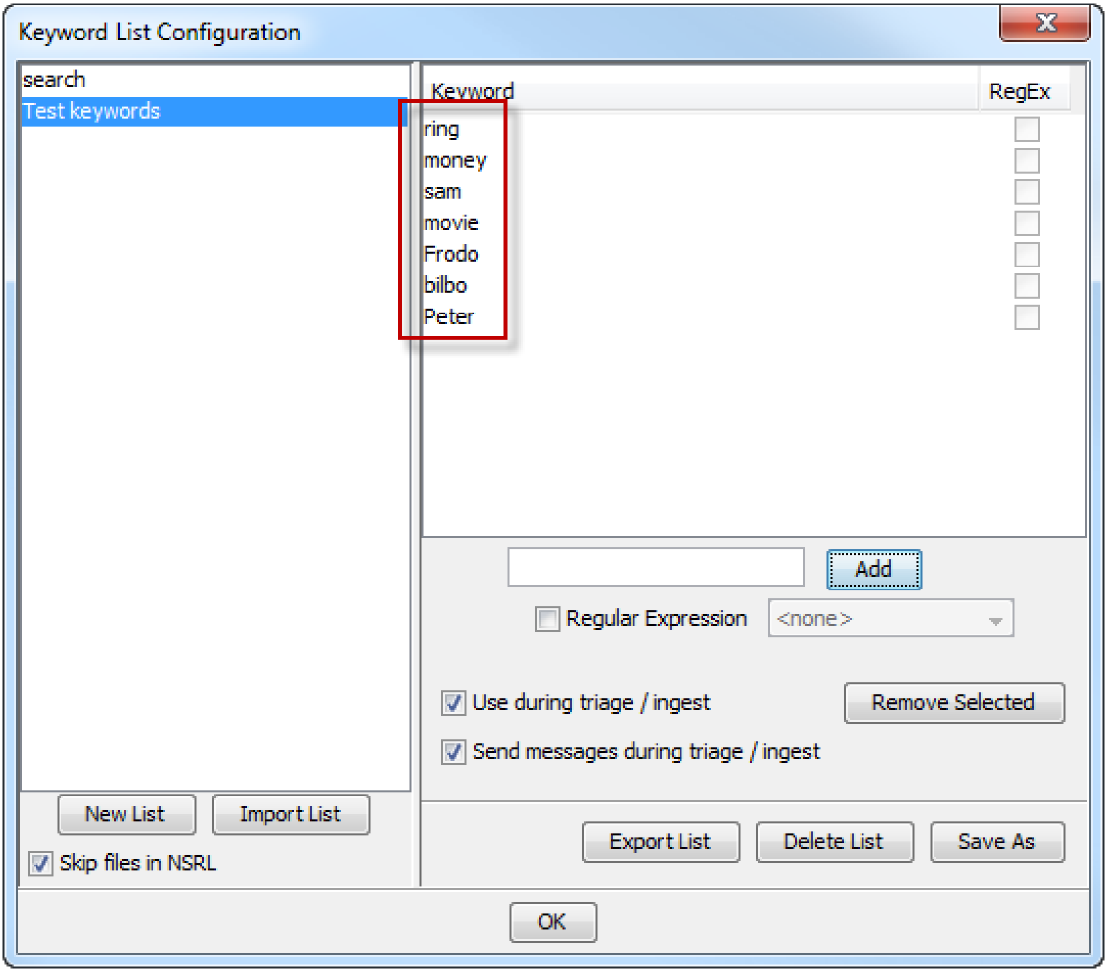
Phone Numbers
IP Addresses
search
Test keywords

Keyword	RegEx

□ Regular Expression <none>

☑ Use during triage / ingest
☑ Send messages during triage / ingest

☑ Skip files in NSRL



Keyword List Configuration

search

Test keywords

Keyword	RegEx
ring	☐
money	☐
sam	☐
movie	☐
Frodo	☐
bilbo	☐
Peter	☐

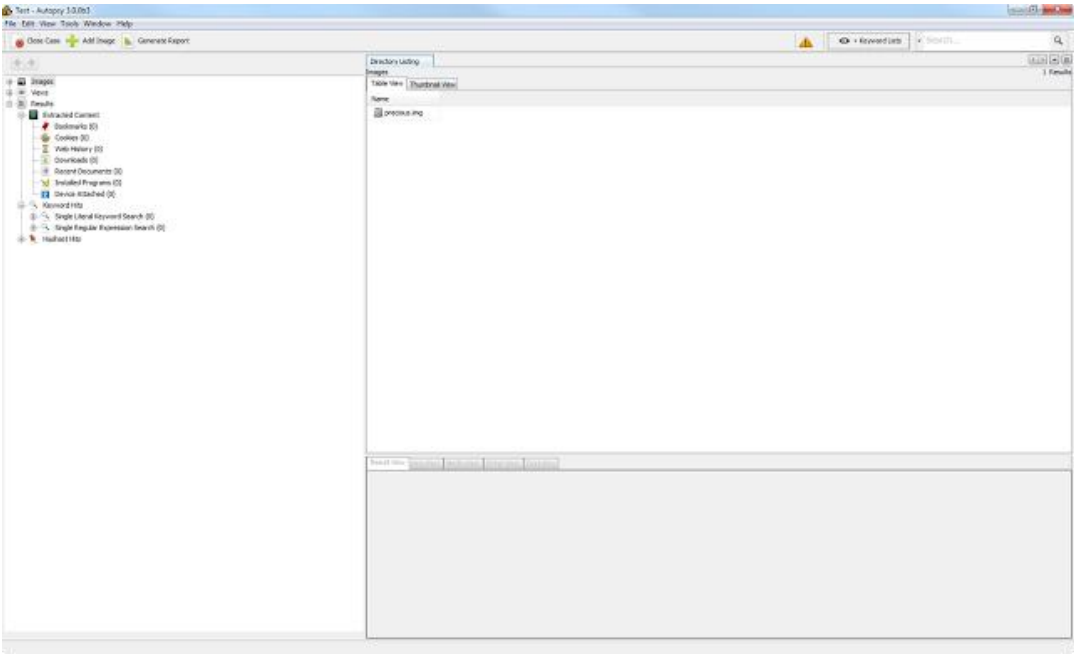
☐ Regular Expression <none>

☑ Use during triage / ingest

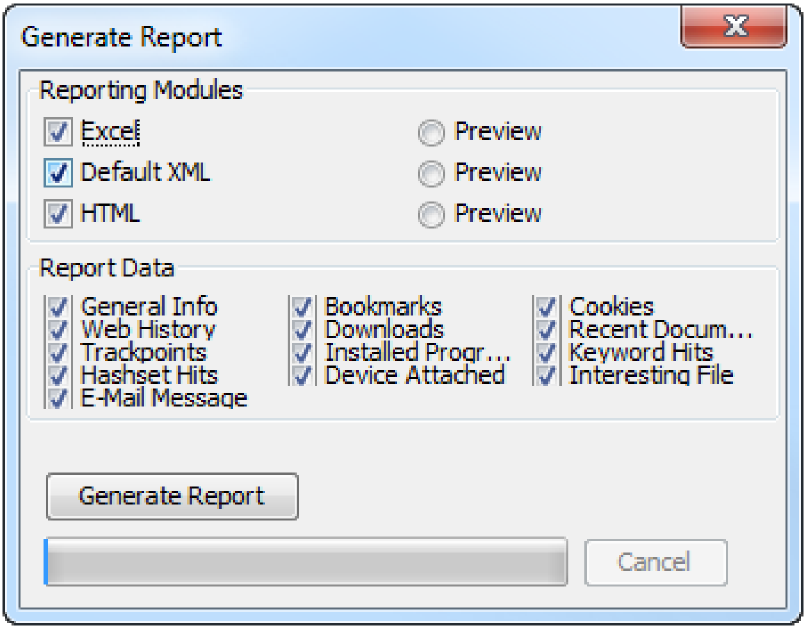
☑ Send messages during triage / ingest

☑ Skip files in NSRL

After finishing the keyword parameters the screen will be laid out for the user.



After the image is indexed the tree will be populated by the file system, extracted content, keyword searches, and the hash list (if any were used). the investigator should generate a report. This will allow the investigator to have an idea of what type of information is available and what to expect. The report can be generated in three formats: Excel, XML, and HTML. It also has the ability to select what information to display with choices that can be seen in the image below.



Generate Report

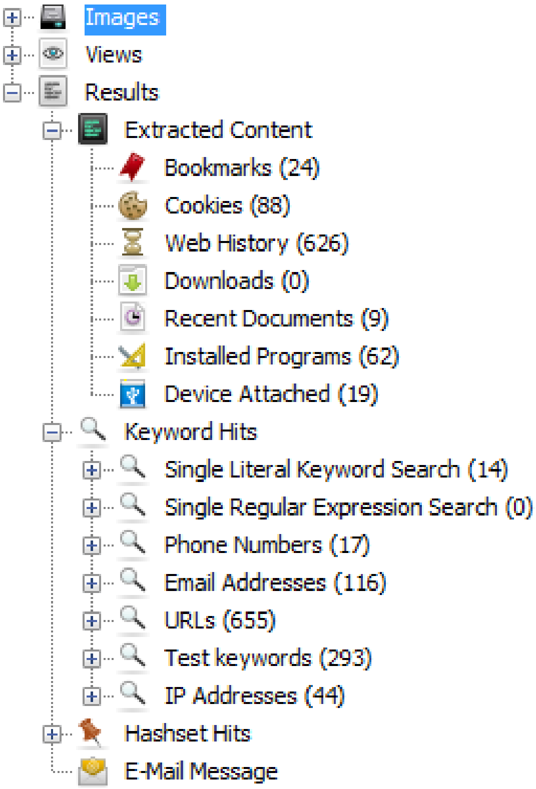
Reporting Modules

☑ Excel ○ Preview
☑ Default XML ○ Preview
☑ HTML ○ Preview

Report Data

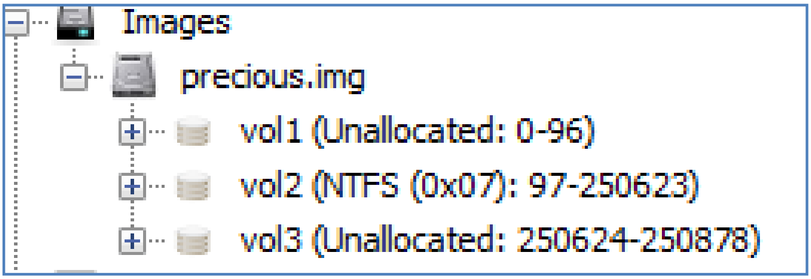
☑ General Info
☑ Web History
☑ Trackpoints
☑ Hashset Hits
☑ E-Mail Message
☑ Bookmarks
☑ Downloads
☑ Installed Progr…
☑ Device Attached
☑ Cookies
☑ Recent Docum…
☑ Keyword Hits
☑ Interesting File

With the report on hand the investigator will have an idea of what to expect as well as a list of programs that are installed on the machine. This can help investigators gather all the evidence they need to perform a complete investigation.



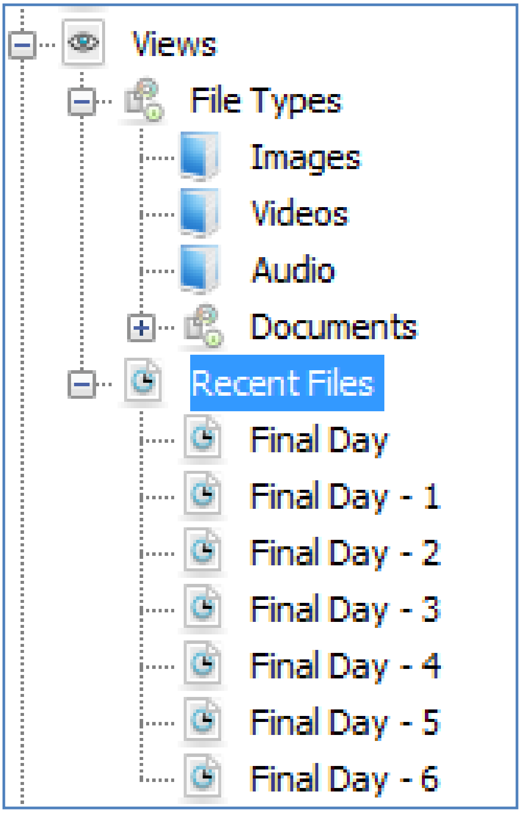
- Images
- Views
- Results
  - Extracted Content
    - Bookmarks (24)
    - Cookies (88)
    - Web History (626)
    - Downloads (0)
    - Recent Documents (9)
    - Installed Programs (62)
    - Device Attached (19)
  - Keyword Hits
    - Single Literal Keyword Search (14)
    - Single Regular Expression Search (0)
    - Phone Numbers (17)
    - Email Addresses (116)
    - URLs (655)
    - Test keywords (293)
    - IP Addresses (44)
  - Hashset Hits
  - E-Mail Message

Looking at the tree, the top selection is titled "Images" this is where the acquired image is located and the bulk of the investigation, will take place. If the Images tab is expanded the investigator will see each image that was added to the investigation. By expanding an images tab the volumes of the image will be seen including the file system and unallocated space. Expanding the tab that contains the Operating System will give the investigator a look at the root directory and the tree that contains most of the relevant information. This is the same as if the investigator would open the default drive when browsing through a system.



- Images
  - precious.img
    - vol1 (Unallocated: 0-96)
    - vol2 (NTFS (0x07): 97-250623)
    - vol3 (Unallocated: 250624-250878)

Below the Images tab is the "Views" tab that will allow the investigator to separate the information in the image into different categories such as by file types and by recent documents. The file type can be broken down into: images, video, audio, and documents which includes the major text formats. Another section in the Views tab is a new feature in Autopsy 3, the Recent Files tab. This tab allows the investigator to get a rough outline of what happened in the last 6 days of use by the suspect. The results include registry files, documents opened, and programs run.



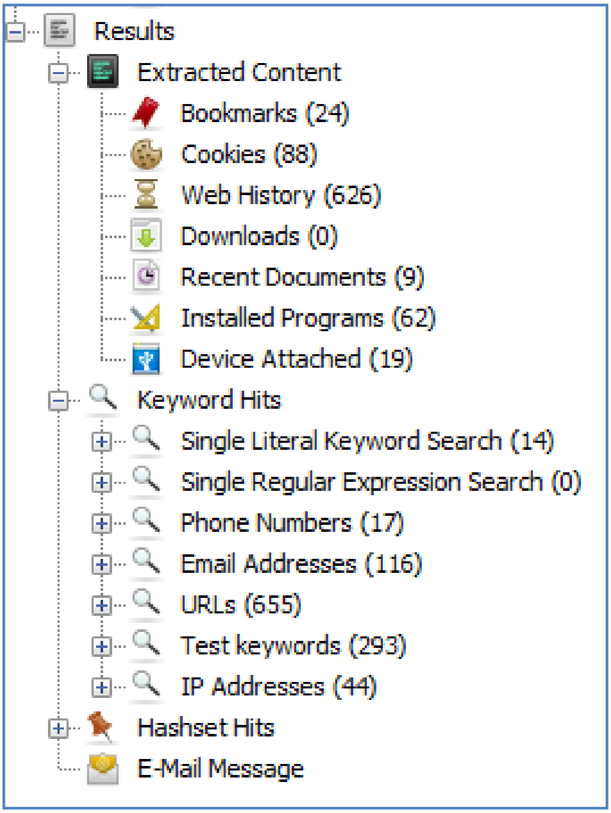
The next tab that is seen is the Results tab, this is a new feature that displays all the information from the ingest process. This uses the program BEViewer to look for certain information inside of the data and separate it into sections that make it easier to search for specific data instead of going through all of the information manually. Although this simplifies the investigation process, it does not mean that this is all of the information that is able to be gained through an investigation.

There are 4 main categories when separating the Results tab: Extracted Content, Keyword Hits, Hashset Hits, and E-mail Messages. Each of these sections has subsections that allow for more specific information divisions. In the Extracted Content tab there are sections for: Bookmarks, Cookies, Web History, Downloads, Recent Documents, Installed Programs, and Device Attached.

The bookmarks tab contains information on bookmarks created in the internet browsers so the investigator can see a list of sites that the suspect frequented enough to create a bookmark for. The cookies tab will allow investigators to see a general idea of where the suspect has been recently by looking through the cookies and seeing which sites have cookies stored on the computer. The Web history tab searches for .dat files and lists them to show another list of internet usage through web browsers. The download tab allows for the search for any downloads on the suspect computer. Recent documents will show documents that were opened on the machine recently by looking at their metadata and deciding how long ago a document was opened. The installed programs tab will give the investigator a list of programs that are currently installed on the machine. The tab for attached devices is obtained by looking through the registry files and determining which hardware devices have been plugged into the system at one point or another.

Under the keyword hits tab the investigator will see all the options that were selected in the ingest index window when starting the case. The information includes: phone numbers, URLs, email addresses, search words by the user, IP addresses, and regular expression searches.
The tab for hashset hits only has results if a list library was added to the case before hand to run matches against. If the investigators had a hash library of known child pornography or pirated material they could run all the information on the computer against the library and all of the results would be placed in the hashset hits tab.

The e-mail message tab will place any emails from a desktop client in the tab for review. The supported programs are Microsoft Outlook and Mozilla Thunderbird as of now but more are scheduled for support in the future.



- Results
  - Extracted Content
    - Bookmarks (24)
    - Cookies (88)
    - Web History (626)
    - Downloads (0)
    - Recent Documents (9)
    - Installed Programs (62)
    - Device Attached (19)
  - Keyword Hits
    - Single Literal Keyword Search (14)
    - Single Regular Expression Search (0)
    - Phone Numbers (17)
    - Email Addresses (116)
    - URLs (655)
    - Test keywords (293)
    - IP Addresses (44)
  - Hashset Hits
  - E-Mail Message

Practical No. 2 : working with windows forensiscs toolkit.

Aim: Exploring AccessData FTK windows & working with new case ,existing case, processing evidence & search options.

Theory & steps:

- Forensic Toolkit, or FTK, is a computer forensics software made by AccessData. It scans a hard drive looking for various information.It can for example locate deleted emails and scan a disk for text strings to use them as a password dictionary to crack encryption.

Task to be performed in this practical:

1. **Starting a new case**

Starting a Case
Completing the New Case
Entering Forensic Examiner Information
Selecting Case Log Options

Selecting Evidence Processes

Refining the Case .

Refining the Index

Managing Evidence

Adding
Evidence
Editing
Evidence
Removing
Evidence .
Refining Evidence
Reviewing Case
Summary
Processing the
Evidence .

Backing Up the Case
Storing Your Case Files
Recovering Evidence from a System Failure
Backing Up Cases Automatically

2. Working with Existing Cases

Opening an Existing Case
Opening an Existing Case from a Different Location
Opening a Case in Case Agent Mode (Read-only)
Using the Case Agent Mode Manager
Adding Evidence
Completing the Add Evidence Form
Selecting Evidence Processes
Managing Evidence
Refining the Index
Reviewing Evidence Setup
Processing the Evidence
Viewing File Properties
General Info
File Source Info
File Content Info
Case-Specific Info
E-mail Info
Setting Up Multiple Temporary Files

3. Processing Evidence

Using Bookmarks
Creating a Bookmark
Adding Files to a Bookmark
Removing a Bookmark
Creating Thumbnails
Importing KFF Hashes
Verifying Image Integrity
Using Analysis Tools
Using the Case Log
Viewing the Case Log
Adding Entries to the Case
Copying Information from FTK
Exporting Files
About Recursive File Exporting
Exporting the Word List

4. Searching a Case

Conducting a Live Search
Conducting an Indexed Search
Single-Term Searches
Multi-Term Searches
Importing Search Terms

Viewing Search Results
Reloading a Search Query
Wildcard Characters
Indexed Search Options
Documenting Your Search Results
Copying Search Results to the Clipboard
Using Copy Special to Document Search Results
Bookmarking Search Results

(For details refer FTK manual chapter 4,5,6 & 7)

Practical No. 3 Using Data acquisition tools

Aim : Exploring ProDiscover Basic.

Task to be performed

Creating a New Project
Save a project
Preview a directly connected evidence drive
Conducting Live Preview of a Remote Disk
Capture an image of an attached drive
Capturing Physical Memory
Add an image file to a project
Add a UNIX "dd" image file to a project
Copy a directly connected drive to another directly connected drive
Restore an Image to directly connected drive
Copy Selected Files
List detail information about image files associated with a project
View the contents of a directly connected disk as files
View the contents of a disk, or image file as clusters
Viewing the Windows Event Logs
View Windows Registry

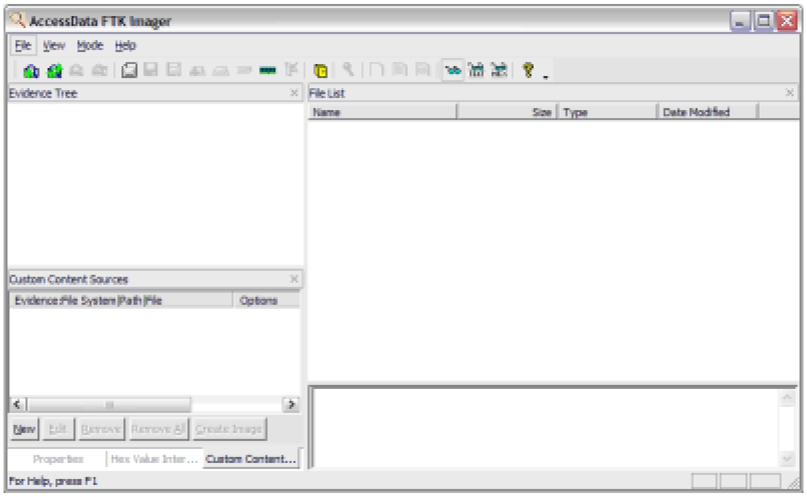
Search the Windows Registry
View Graphic Files in Gallery
View
Adding Thumbnail Images to Report for Graphic Evidence
View Image EXIF Meta Data
Recover a Deleted File
Search for key words in image file or disk
Extracting Internet History
Creating Hash Database Files
Comparing HashKeeper hash sets
To compare hash sets to a directory and all contents recursively:
To compare hash sets to a single file:
Match File Signatures and File Extensions
Detecting file systems within the
HPA
Recover a group of clusters
Detecting Disk or Image Installed OS
Cross Reference File Cluster
Locations
To find a list of specific clusters in which a file is written:
To find the file associated with a specific cluster:
Determining and Cross Referencing a File's Cluster
Locations
Flagging or Bookmarking Evidence of Interest
Adding and Editing Comments to Evidence of Interest
Adding Subsets of Data as Evidence of Interest

Practical No. 4 **Using File recovery Tools**

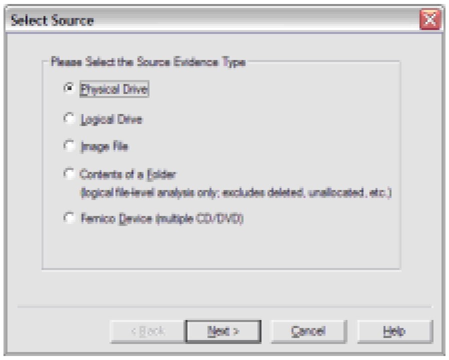
Aim: understanding & working with the process of the process of taking a drive image using AccessData's FTK Imager tool.

FTK Imager is a Windows acquisition tool included in various forensics toolkits.

Run **FTK Imager.exe** to start the tool.



From the **File** menu, select **Create a Disk Image** and choose the source of your image. **NOTE**: FTK Imager does not guarantee data is not written to the drive, so it is important to use a write blocker like the Tableau T35es.



Select Source

Please Select the Source Evidence Type

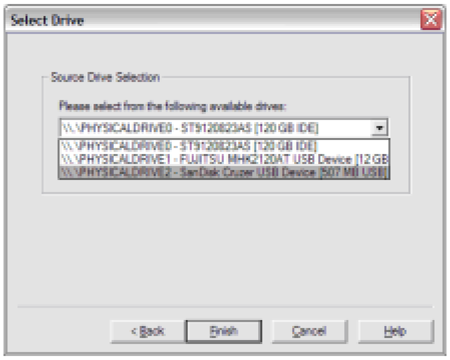
● Physical Drive

○ Logical Drive

○ Image File

○ Contents of a Folder
(logical file-level analysis only; excludes deleted, unallocated, etc.)

○ Fernico Device (multiple CD/DVD)



Select Drive

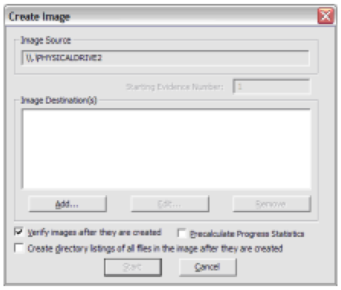
Source Drive Selection

Please select from the following available drives:

\\.\PHYSICALDRIVE0 - ST9120823AS [120 GB IDE]

\\.\PHYSICALDRIVE0 - ST9120823AS [120 GB IDE]
\\.\PHYSICALDRIVE1 - FUJITSU MHK2120AT USB Device [12 GB
\\.\PHYSICALDRIVE2 - SanDisk Cruzer USB Device [507 MB USB]

Click **Add...** to add the image destination. Check **Verify images after they are created** so FTK Imager will calculate MD5 and SHA1 hashes of the acquired image.



Create Image

Image Source: \\.\PHYSICALDRIVE2

Starting Evidence Number: 1

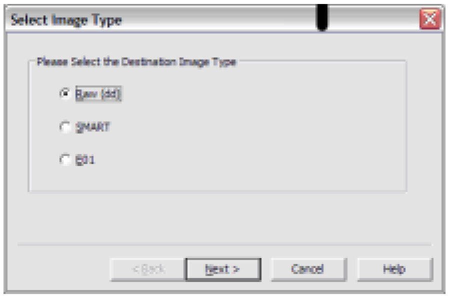
Image Destination(s)

☑ Verify images after they are created

□ Precalculate Progress Statistics

□ Create directory listings of all files in the image after they are created

Next, select the image type. The type you choose will usually depend on what tools you plan to use on the image. The dd format will work with more open source tools, but you might want SMART or E01 if you will primarily be working with ASR Expert Witness or EnCase, respectively.



Select Image Type

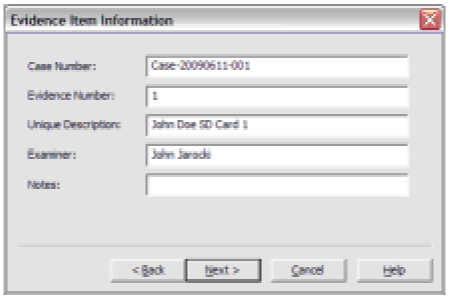
Please Select the Destination Image Type

● Raw (dd)

○ SMART

○ E01

If your version of FTK requests evidence information, you can provide it. If you select raw (dd) format, the image meta data will *not* be stored in the image file itself.



Case Number: Case-20090611-001
Evidence Number: 1
Unique Description: John Doe SD Card 1
Examiner: John Jarocki
Notes:

Select the Image Destination folder and file name. You can also set the maximum fragment size of image split files. Click Finish to complete the wizard.

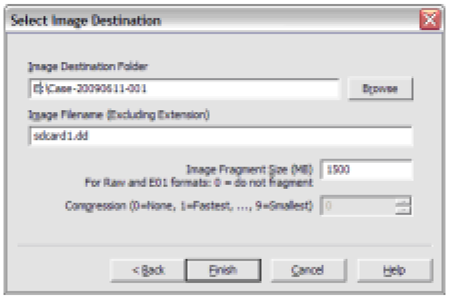


Image Destination Folder: E:\Case-20090611-001
Image Filename (Excluding Extension): sdcard1.dd
Image Fragment Size (MB): 1500
For Raw and E01 formats: 0 = do not fragment
Compression (0=None, 1=Fastest, ..., 9=Smallest): 0

Click Start to begin the acquisition:

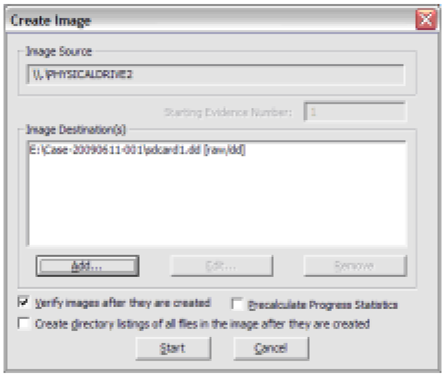
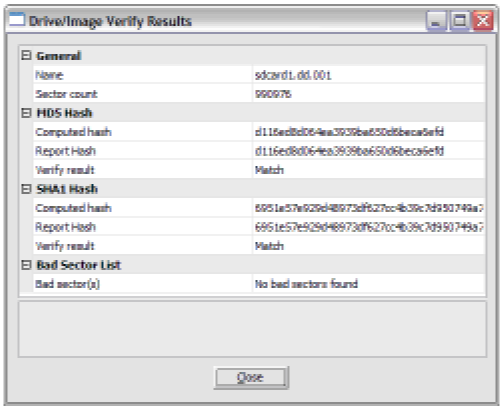


Image Source: \\.\PHYSICALDRIVE2
Starting Evidence Number: 1
Image Destination(s): E:\Case-20090611-001\sdcard1.dd [raw/dd]
☑ Verify images after they are created
☐ Precalculate Progress Statistics
☐ Create directory listings of all files in the image after they are created

A progress window will appear. Now is a good time to refill that coffee cup! Once the acquisiton is complete, you can view an image summary and the drive will appear in the evidence list in the left hand side of the main FTK Imager window. You can right-click on the drive name to Verify the Image:


Drive/Image Verify Results

⊟ **General**	
Name	sdcard1.dd.001
Sector count	990976
⊟ **MD5 Hash**	
Computed hash	d116ed8d064ea3939ba650d6beca6efd
Report Hash	d116ed8d064ea3939ba650d6beca6efd
Verify result	Match
⊟ **SHA1 Hash**	
Computed hash	6951e57e929d48973df627cc4b39c7d950749a7
Report Hash	6951e57e929d48973df627cc4b39c7d950749a7
Verify result	Match
⊟ **Bad Sector List**	
Bad sector(s)	No bad sectors found

FTK Imager also creates a log of the acquisition process and places it in the same directory as the image,***image-name*.txt**. This file lists the evidence information, details of the drive, check sums, and times the image acquisition started and finished:

For example:

Created By AccessData® FTK® Imager 2.6.0.49 090505

Case Information:
Case Number: Case-20090611-001
Evidence Number: 1
Unique description: John Doe SD Card 1
Examiner: John Jarocki
Notes:

Information for E:\Case-20090611-001\sdcard1.dd:

Physical Evidentiary Item (Source) Information:
[Drive Geometry]
Cylinders: 61
Tracks per Cylinder: 255
Sectors per Track: 63
Bytes per Sector: 512
Sector Count: 990,976
[Physical Drive Information]
Drive Model: SanDisk Cruzer USB Device
Drive Interface Type: USB
Source data size: 483 MB
Sector count: 990976
[Computed Hashes]

MD5 checksum: d116ed8d064ea3939ba650d6beca6efd
SHA1 checksum: 6951e57e929d48973df627cc4b39c7d950749a70

Image Information:
Acquisition started: Fri Jun 12 07:39:02 2009
Acquisition finished: Fri Jun 12 07:49:55 2009
Segment list:
E:\Case-20090611-001\sdcard1.dd.001

Image Verification Results:
Verification started: Fri Jun 12 07:49:56 2009
Verification finished: Fri Jun 12 07:50:00 2009
MD5 checksum: d116ed8d064ea3939ba650d6beca6efd : verified
SHA1 checksum: 6951e57e929d48973df627cc4b39c7d950749a70 : verified

Practical No. 5 using AccessData FTK

Aim: Exploring Access data FTK for the following:

- Data Carving
  - Searching for Embedded and Deleted Files (Data Carving)
  - Data Carving Files in an Existing Case
  - Adding Carved Files to the Case
  - Bookmarking Carved Files
- Using Filters
  - Applying an Existing Filter
  - Using The File Filter Manager
  - Modifying or Creating a Filter
  - Deleting a Filter
- Searching the Registry
  - Starting Registry Viewer
  - Launching Registry Viewer as a Separate Application
- Launching Registry Viewer from FTK
- Understanding the Registry Viewer Windows
- The Full Registry Window
- The Common Areas Window
- The Report Window
- Opening Registry Files
- Opening a Registry File in Registry Viewer
- Opening Registry Files within FTK
- Obtaining Protected Registry Files Using FTK Imager
- Working with Registry Evidence
- Adding Keys to the Common Areas Window
- Deleting Keys from the Common Areas Window
- Adding Keys to the Report Window
- Deleting Keys from the Report Window
- Creating Registry Summary Reports
- Using Pre-defined AccessData Templates
- Creating Your Own Registry Report Templates
- Changing RSR Settings in the FtkSettings.0.ini File
- Searching for Specific Data
- Generating a Report
- Exporting a Word List

(refer chapter 9,10 & 11 of the FTK manual)

Practical No. 6 : **Forensics Investigation Using Encase**

Aim: Exploring Encase

Task to be performed

1. Case Management

Overview of Case Structure
Case Related Features
New Case Wizard
Using a Case
Opening a Case
Saving a Case
Closing a Case

2. Working with Evidence

Overview
Supported File Systems and Operating Systems
Using Snapshots
Getting Ready to Acquire the Content of a Device
Acquiring
Delayed Loading of Internet Artifacts
Hashing
Logical Evidence Files
Recovering Folders
Recovering Partitions
Restoring Evidence
Snapshot to DB Module Set
WinEn
Wipe Drive

3. Source Processor

Overview
Collection Jobs
Modules
Analysis Jobs
Reports
Managing EnCase Portable

4. Analyzing and Searching Files

Signature Analysis
EnScript Programming Language
Hash Analysis
File Hashing
Hash Sets
Keyword Searches
Encode Preview
Indexing
Searching for Email
Tag Records
App Descriptors

5. Viewing File Content

Viewing Files
File Viewers
View Pane
Viewing Compound Files
Viewing Base64 and UUE Encoded Files
NTFS Compressed Files
Gallery Tab

6. Bookmarking Items

Bookmarks Overview
Bookmark Features
Creating a Bookmark
Using Bookmarks
Copying Selected Items from One Folder to Another

7. Reporting

Reporting
Report User Interface
Creating a Report Using the Report Tab
Creating a Report Using Case Processor

Practical No. 7 : using steganography tools

Aim: Exploring S tools

Following steps Show how to use freeware S-Tools utility to hide and reveal files inside pictures

Steps:

1. Select the S-Tools.exe file and open the steganography software tool.
2. The main window of the program appears.
3. Three buttons are available on the main window:

    i. File
    ii. Window
    iii. Help

4. With both the working directory and the S-Tools program open minimize both windows and place side-by-side.

5. The S-Tools program is a drag and drop software. The files used to create the steganography file can be dragged from the directory into the S-Tools program.
6. Select a base file that will be used to hide a hidden file. A *.jpg file was selected as the base file. Select the file from the directory and drag it over the S-Tools main window and release the file.

7. A dialogue box appears indicating that the file type is unknown. Supported file types for audio and image files are shown below:

    α. Audio - *.wav
    β. Image - *.bmp and *.gif

8. Select a valid audio file or image as the base file for the steganography file. The zebras.bmp was selected and dragged onto the main window of the S-Tools program. The image is opened.

9. The zebras.bmp and the Actions window are now in the S-Tools program.

10. The Action window is a process window which displays the process steps as a file is being hidden within a base file.
11. Place the working directory and the base file side-by-side.

12. Select a file to hide within the base file.

13. The abc.txt is selected and dragged on top of the base image. Release the file while the cursor is still on top of the base file.
14. A dialogue box will appear asking the user to enter and verify a passphrase. Additionally, the user will have to select an encryption algorithm.

15. Enter a passphrase in both the passphrase and verify passphrase text boxes.

16. If the same passphrase is not entered in both text boxes the 'OK' button will be grayed out and the user will not be able to proceed to creating the steganography file.

17. Select the 'OK' button after entering a valid passphrase.

    9. The S-Tools main window will appear and a new file will be visible. The name of the file will be called hidden_data

by default.

10. At this point, the original file has been selected and opened, a second file have been selected and opened, and a passphrase has been selected.

18. Now the user has to save the steganography file.
19. Place the cursor on top of the hidden data image and select the right mouse button. The user will have four options available to them:

    α. Save
    β. Save As
    χ. Properties
    δ. Reveal

20. Selecting the 'Save' and 'Save As' buttons for the first time will open a 'Save As' dialogue box.

21. Select a directory path and filename, then select the 'Save' button.

22. On this step the user is selecting a filename for the steganography file, which contains a hidden file.

23. If the user is going to use S-Tools to open the steganography file, a filename extension of either *.bmp, *.gif or *.wav must be used when saving the steganography file.

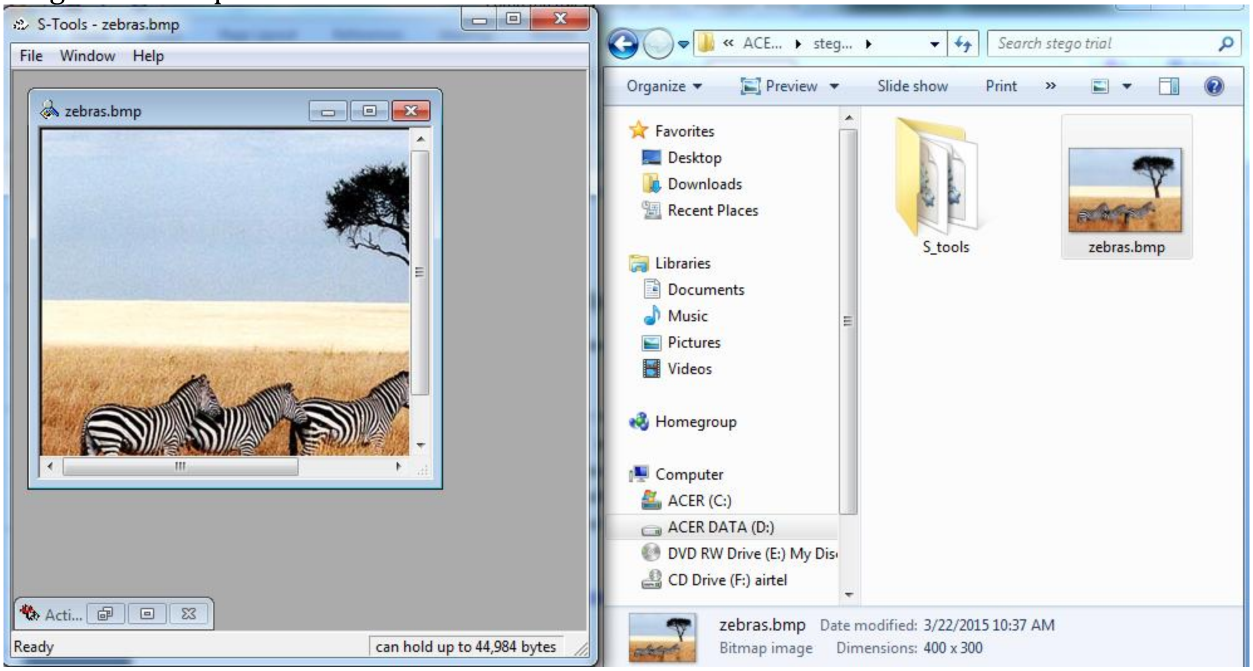
24. After selecting the 'Save' button the user can locate the saved steganography file in the working directory.
25. Selecting the 'Reveal' button will display a passphrase dialogue box.

26. A passphrase must be entered twice in the dialogue box and the correct encryption algorithm must be selected.

27. Notice that the title of the dialogue box has changed to 'Revealing from zebras.bmp'

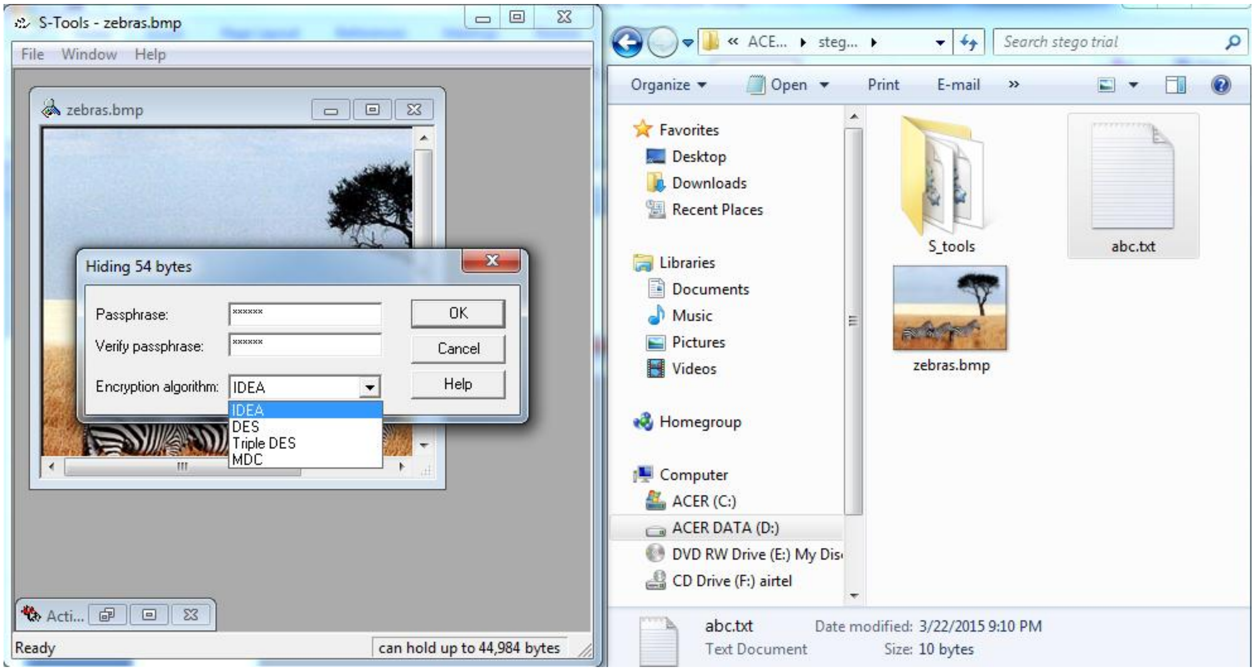
28. Enter a passphrase twice, select the encryption algorithm, and select the 'OK' button
29. The main window of the S-Tools program will appear.

Drag zebras.bmp in S-tools



Create a text file abc.txt

Drag & drop in the image, provide pass phrase& encryption algorithm.



Hiding 54 bytes

Passphrase: ******

Verify passphrase: ******

Encryption algorithm: IDEA

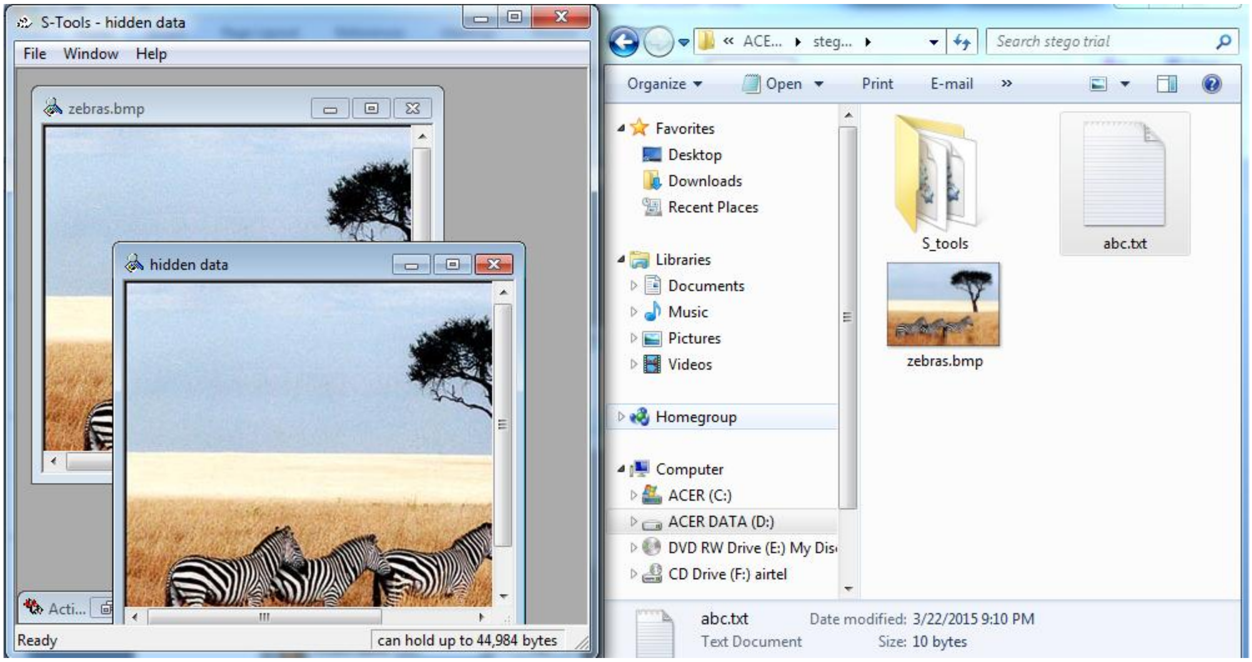
IDEA
DES
Triple DES
MDC

OK

Cancel

Help

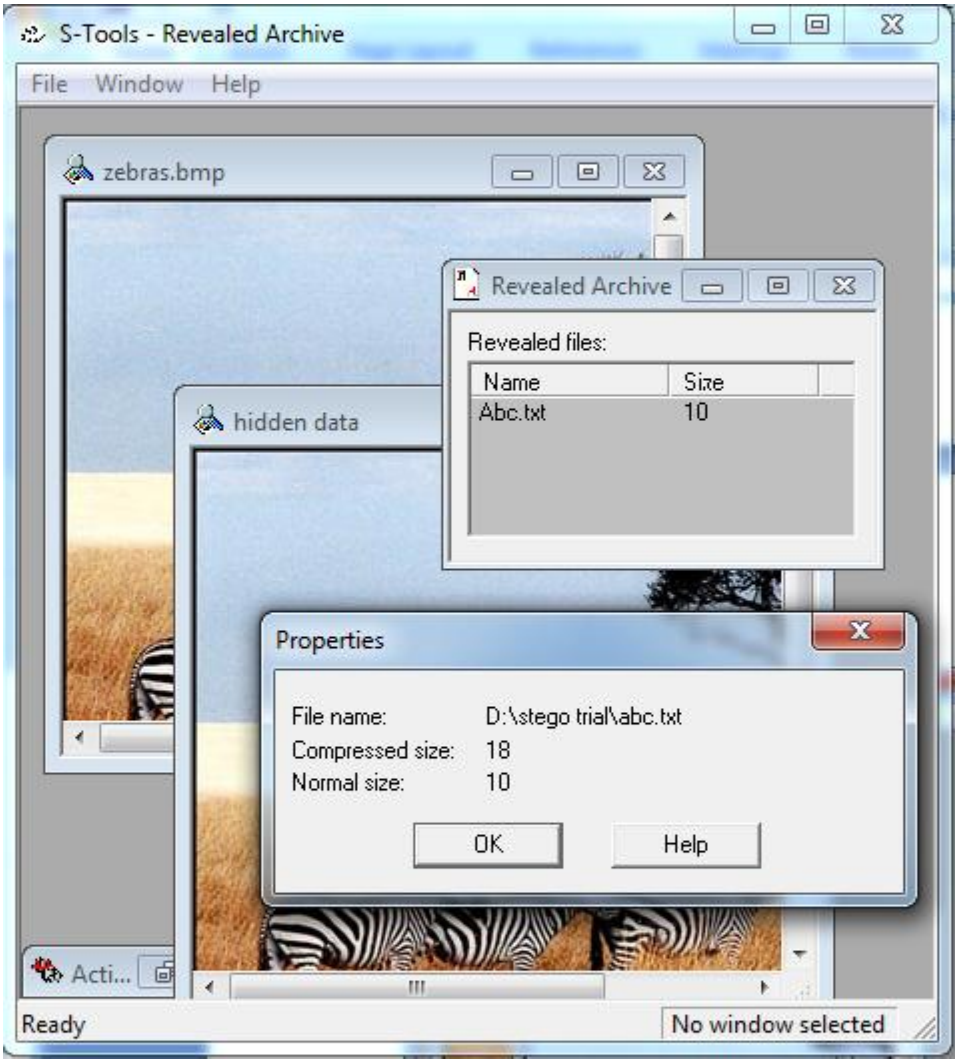
This will create a new file with name hidden data which has the hidden text file



can hold up to 44,984 bytes

abc.txt Date modified: 3/22/2015 9:10 PM
Text Document Size: 10 bytes

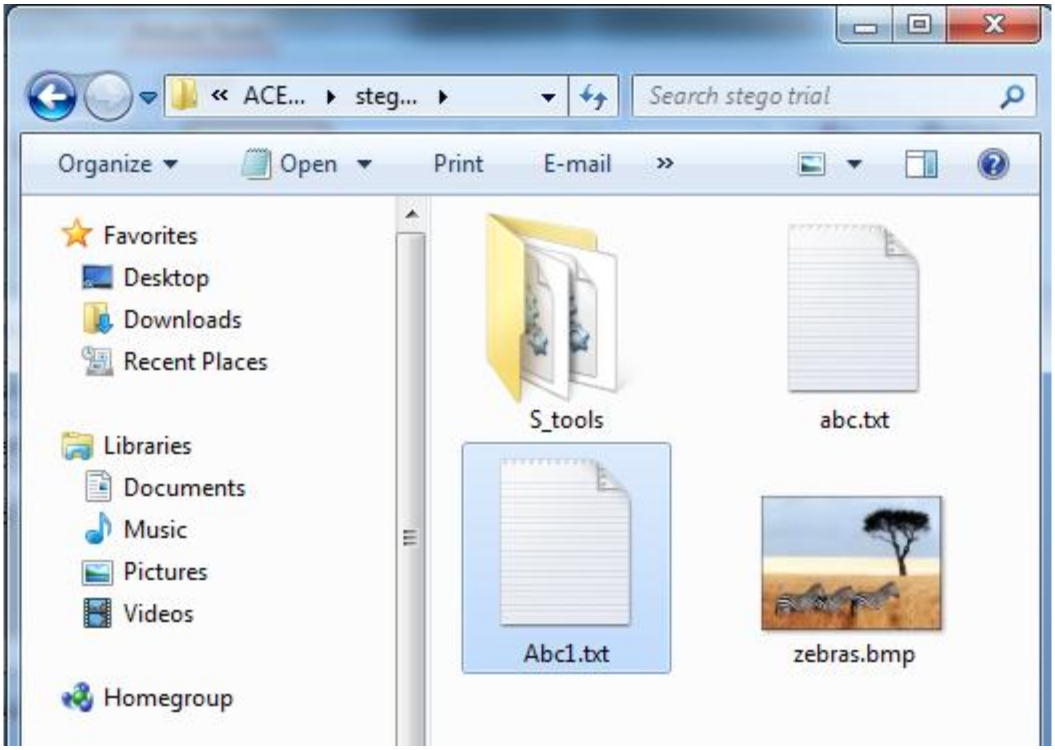
Now to reveal the data from image, right click & click on option reveal.this will show the file which can be saved and verified.



Revealed files:

Name	Size
Abc.txt	10

File name: D:\stego trial\abc.txt
Compressed size: 18
Normal size: 10


« ACE... ▸ steg... ▸
Search stego trial
Organize ▾
Open ▾
Print
E-mail
»
Favorites
Desktop
Downloads
Recent Places
Libraries
Documents
Music
Pictures
Videos
Homegroup
S_tools
abc.txt
Abc1.txt
zebras.bmp

Practical No. 8 **Using Password Cracking Tools**

Aim: Exploring Cain & Abel is a password recovery tool for Microsoft Operating Systems

- Cain & Abel is a password recovery tool for Microsoft Operating Systems. It allows easy recovery of several kind of passwords by sniffing the network, cracking encrypted passwords using Dictionary, Brute-Force and Cryptanalysis attacks, recording VoIP conversations, decoding scrambled passwords, recovering wireless network keys, revealing password boxes, uncovering cached passwords and analyzing routing protocols.
- **Source: http://www.oxid.it/cain.html**

Tasks to be performed

- Protected Storage Password Manager

  Reveals locally stored passwords of Outlook, Outlook Express, Outlook Express Identities, Outlook 2002, Internet Explorer and MSN Explorer.

- Credential Manager Password Decoder

  Reveals passwords stored in Enterprise and Local Credential Sets on Windows XP/2003.

- LSA Secrets Dumper

  Dumps the contents of the Local Security Authority Secrets.

- Dialup Password Decoder

  Reveals passwords stored by Windows "Dial-Up Networking" component.

- APR (ARP Poison Routing)

  Enables sniffing on switched networks and Man-in-the-Middle attacks.

- Route Table Manager

  Provides the same functionality of the Windows tool "route.exe" with a GUI front-end.

- SID Scanner

  Extracts user names associated to Security Identifiers (SIDs) on a remote system.

- Network Enumerator

Retrieves, where possible, the user names, groups, shares, and services running on a machine.

- Remote Registry

  Allows modification of registry parameters from the network.

- Service Manager

  Allows you to stop, start, pause/continue or remove a service.

- Sniffer

  Captures passwords, hashes and authentication information while they are transmitted on the network. Includes several filters for application specific authentications and routing protocols. The VoIP filter enables the capture of voice conversations transmitted with the SIP/RTP protocol saved later as WAV files.

- Routing Protocol Monitors

  Monitors messages from various routing protocols (HSRP, VRRP, RIPv1, RIPv2, EIGRP, OSPF) to capture authentications and shared route tables.

- Certificates Collector

  Grab certificates from HTTPS, IMAPS, POP3S, LDAPS, FTPS web sites and prepares them to be used by relative APR-* sniffer filters.

- MAC Address Scanner with OUI fingerprint

  Using OUI fingerprint, this makes an informed guess about what type of device the MAC address from.

- Promiscuous-mode Scanner based on ARP packets

  Identifies sniffers and network Intrusion Detection systems present on the LAN.

- Wireless Scanner

  Can scan for wireless networks signal within range, giving details on its MAC address, when it was last seen, the guessed vendor, signal strength, the name of the network (SSID), whether it has WEP or not (note WPA encrypted networks will show up as WEPed), whether the network is an Ad-Hoc network or Infrastructure, what channel the network is operating at and at what speed the network is operating (e.g. 11Mbps). Passive scanning and WEP IVs sniffing are also supported using the AirpCap adapter from CACE Technologies.

- 802.11 Capture Files Decoder

  Decode 802.11 capture files (wireshark, pcap) containing wireless frames encrypted with WEP or WPA-PSK.

- Access (9x/2000/XP) Database Passwords Decoder

  Decodes the stored encrypted passwords for Microsoft Access Database files.

- Password Crackers

  Enables the recovery of clear text passwords scrambled using several hashing or encryption algorithms. All crackers support Dictionary and Brute-Force attacks.

- Microsoft SQL Server 2000 Password Extractor via ODBC

  Connects to an SQL server via ODBC and extracts all users and passwords from the master database.

- Oracle Password Extractor via ODBC

  Connects to an Oracle server via ODBC and extracts all users and passwords from the database.

- MySQL Password Extractor via ODBC

  Connects to an MySQL server via ODBC and extracts all users and passwords from the database.

- Box Revealer

  Shows passwords hidden behind asterisks in password dialog boxes.

- RSA SecurID Token Calculator

  Can calculate the RSA key given the token's .XML activation file.

- Hash Calculator

  Produces the hash values of a given text.

- TCP/UDP Table Viewer

  Shows the state of local ports (like netstat).

- Remote Console

  Provides a remote system shell on the remote machine.

- Remote Route Table Manager

  Enable to manage the route table of the remote system.

- Remote TCP/UDP Table Viewer

  Shows the state of local ports (like netstat) on the remote system.

Practical No. 9 & 10 : **Using Log capturing ,traffic capturing & analysis tools**

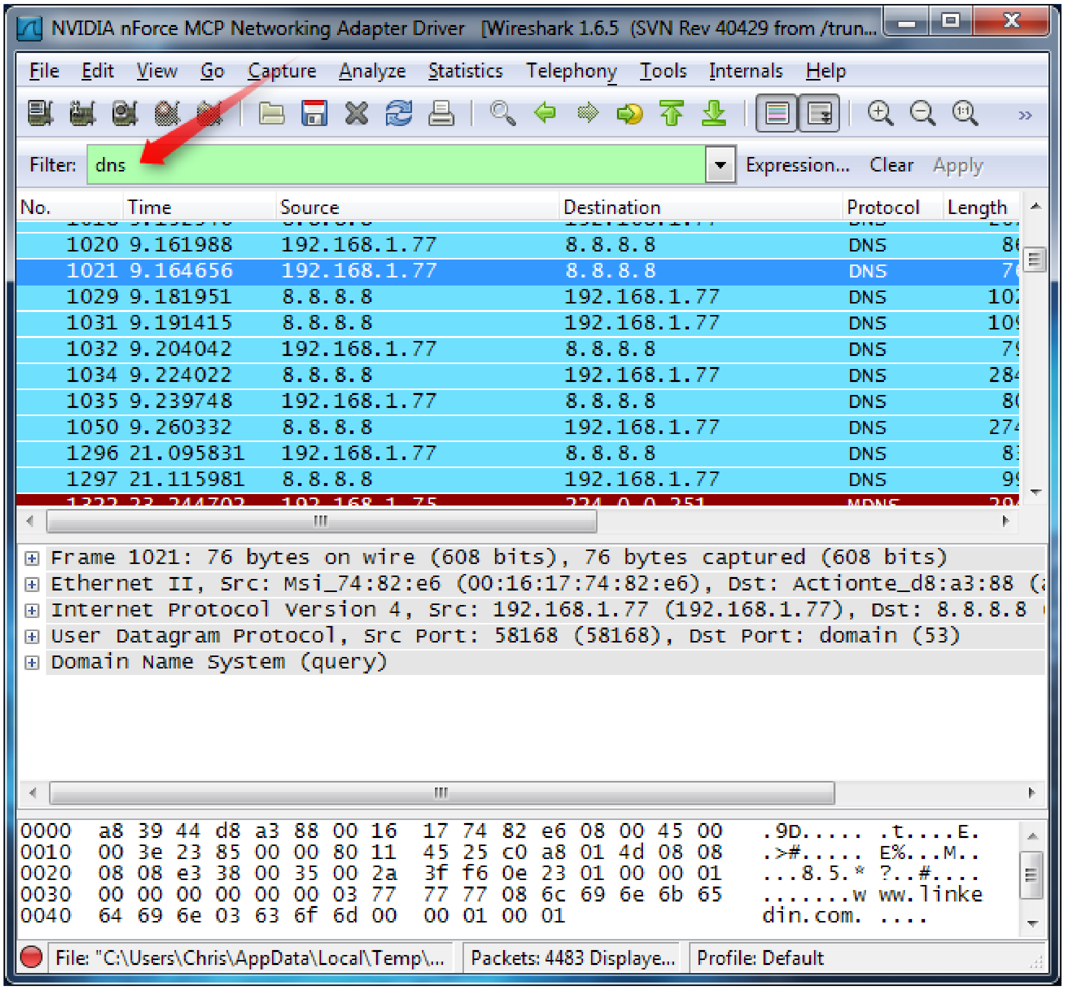
Aim : Exploring wireshark

Wireshark is a network packet analyzer that intercepts, captures and logs information about packets passing through a network interface. This is useful for analyzing network problems, detecting network intrusions, network misuse, and other security problems, monitor usage and gather statistics, and many other applications.

Filtering Packets

If you're trying to inspect something specific, such as the traffic a program sends when phoning home, it helps to close down all other applications using the network so you can narrow down the traffic. Still, you'll likely have a large amount of packets to sift through. That's where Wireshark's filters come in.

The most basic way to apply a filter is by typing it into the filter box at the top of the window and clicking Apply (or pressing Enter). For example, type "dns" and you'll see only DNS packets. When you start typing, Wireshark will help you autocomplete your filter.



Filter: dns

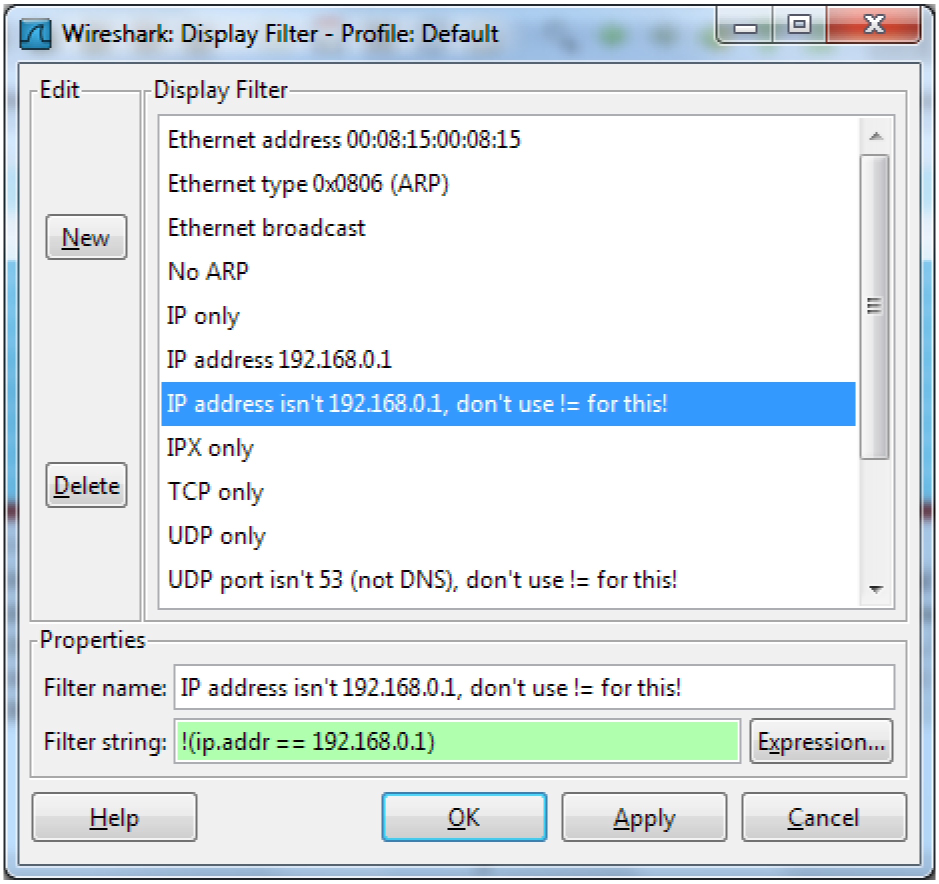
```
No.    Time        Source         Destination    Protocol  Length
1020   9.161988    192.168.1.77   8.8.8.8        DNS       8
1021   9.164656    192.168.1.77   8.8.8.8        DNS       7
1029   9.181951    8.8.8.8        192.168.1.77   DNS       10
1031   9.191415    8.8.8.8        192.168.1.77   DNS       10
1032   9.204042    192.168.1.77   8.8.8.8        DNS       7
1034   9.224022    8.8.8.8        192.168.1.77   DNS       28
1035   9.239748    192.168.1.77   8.8.8.8        DNS       8
1050   9.260332    8.8.8.8        192.168.1.77   DNS       27
1296   21.095831   192.168.1.77   8.8.8.8        DNS       8
1297   21.115981   8.8.8.8        192.168.1.77   DNS       9
```

```
⊞ Frame 1021: 76 bytes on wire (608 bits), 76 bytes captured (608 bits)
⊞ Ethernet II, Src: Msi_74:82:e6 (00:16:17:74:82:e6), Dst: Actionte_d8:a3:88 (
⊞ Internet Protocol Version 4, Src: 192.168.1.77 (192.168.1.77), Dst: 8.8.8.8
⊞ User Datagram Protocol, Src Port: 58168 (58168), Dst Port: domain (53)
⊞ Domain Name System (query)
```

```
0000  a8 39 44 d8 a3 88 00 16  17 74 82 e6 08 00 45 00   .9D..... .t....E.
0010  00 3e 23 85 00 00 80 11  45 25 c0 a8 01 4d 08 08   .>#..... E%...M..
0020  08 08 e3 38 00 35 00 2a  3f f6 0e 23 01 00 00 01   ...8.5.* ?..#....
0030  00 00 00 00 00 00 03 77  77 77 08 6c 69 6e 6b 65   .......w ww.linke
0040  64 69 6e 03 63 6f 6d 00  00 01 00 01               din.com. ....
```

File: "C:\Users\Chris\AppData\Local\Temp\... | Packets: 4483 Displaye... | Profile: Default

You can also click the Analyze menu and select Display Filters to create a new filter.

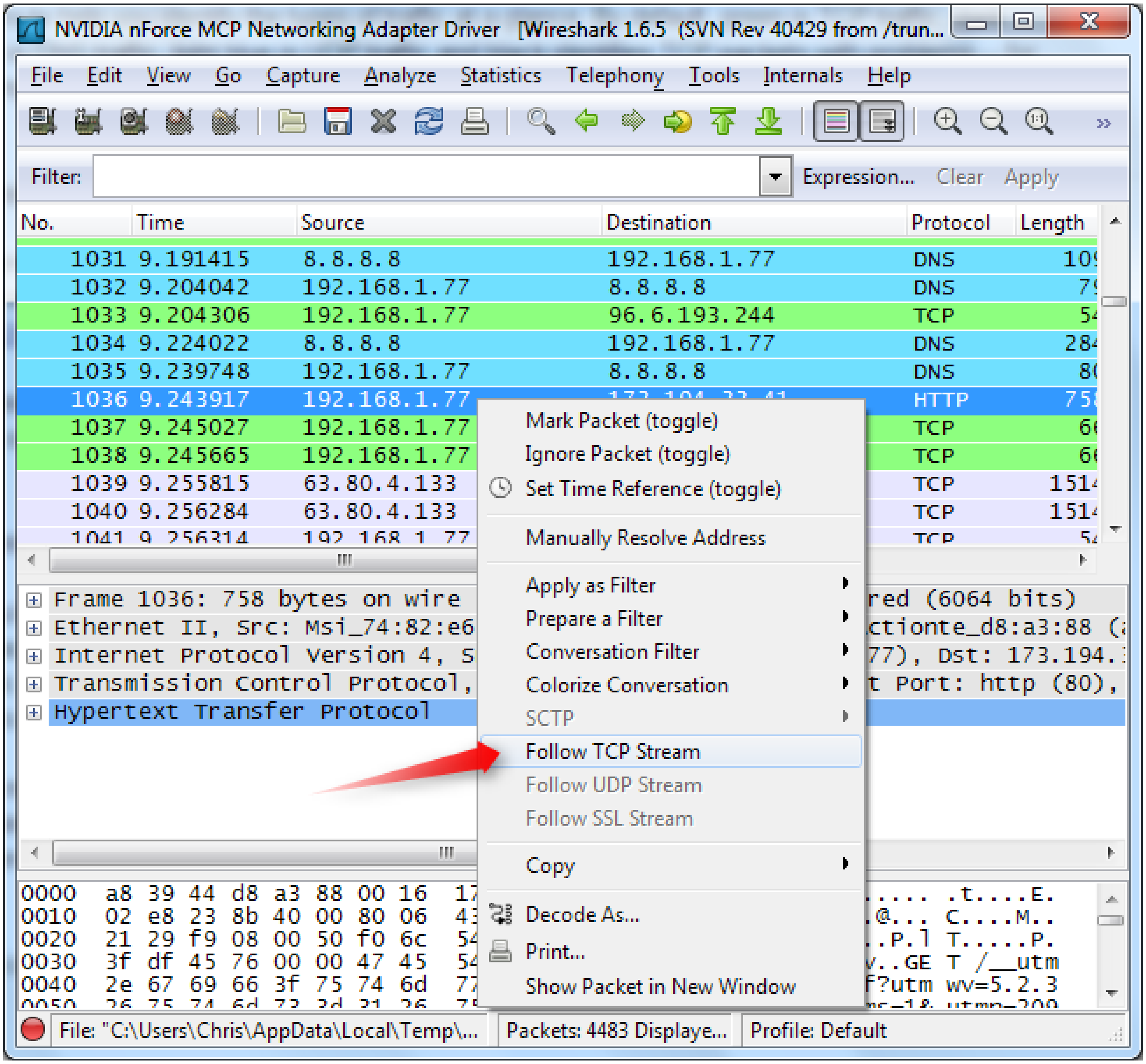


Ethernet address 00:08:15:00:08:15
Ethernet type 0x0806 (ARP)
Ethernet broadcast
No ARP
IP only
IP address 192.168.0.1
IP address isn't 192.168.0.1, don't use != for this!
IPX only
TCP only
UDP only
UDP port isn't 53 (not DNS), don't use != for this!

Filter name: IP address isn't 192.168.0.1, don't use != for this!

Filter string: !(ip.addr == 192.168.0.1)

Another interesting thing you can do is right-click a packet and select Follow TCP Stream.

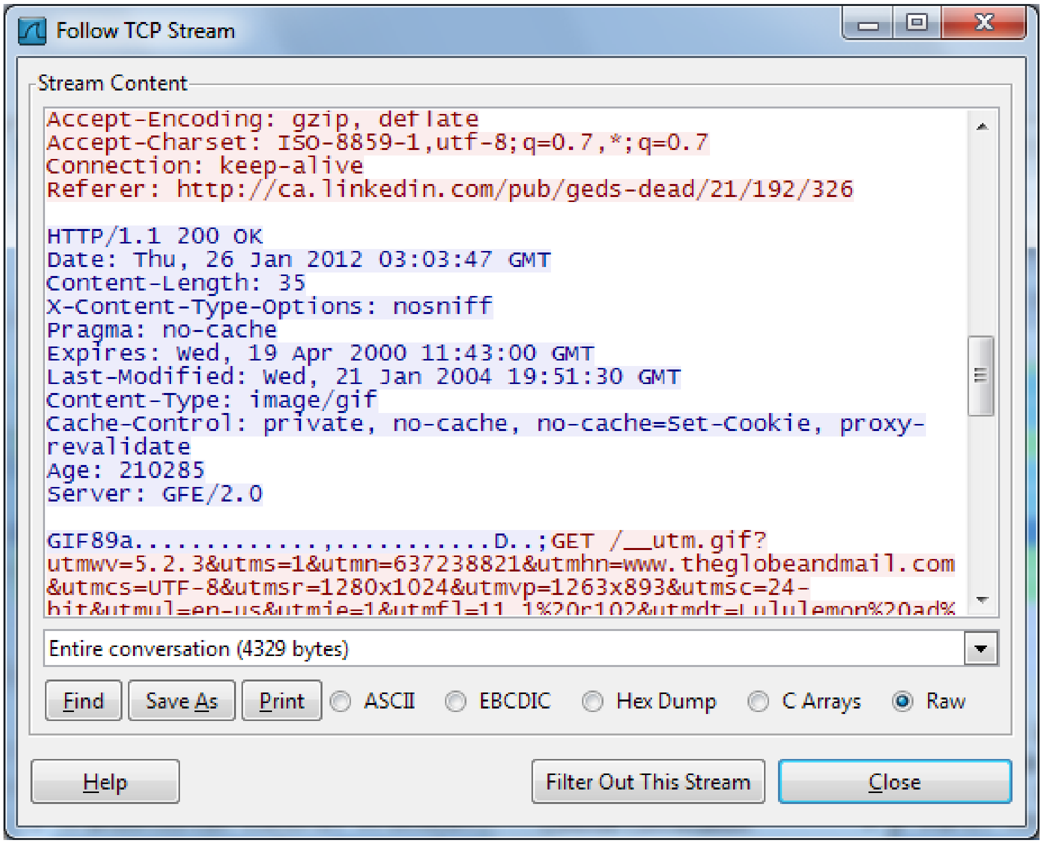

NVIDIA nForce MCP Networking Adapter Driver [Wireshark 1.6.5 (SVN Rev 40429 from /trun...
File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help
Filter:
Expression... Clear Apply
Mark Packet (toggle)
Ignore Packet (toggle)
Set Time Reference (toggle)
Manually Resolve Address
Apply as Filter
Prepare a Filter
Conversation Filter
Colorize Conversation
SCTP
Follow TCP Stream
Follow UDP Stream
Follow SSL Stream
Copy
Decode As...
Print...
Show Packet in New Window
File: "C:\Users\Chris\AppData\Local\Temp\...
Packets: 4483 Displaye...
Profile: Default

No.	Time	Source	Destination	Protocol	Length
1031	9.191415	8.8.8.8	192.168.1.77	DNS	10
1032	9.204042	192.168.1.77	8.8.8.8	DNS	7
1033	9.204306	192.168.1.77	96.6.193.244	TCP	5
1034	9.224022	8.8.8.8	192.168.1.77	DNS	28
1035	9.239748	192.168.1.77	8.8.8.8	DNS	8
1036	9.243917	192.168.1.77	173.194.33.41	HTTP	75
1037	9.245027	192.168.1.77		TCP	6
1038	9.245665	192.168.1.77		TCP	6
1039	9.255815	63.80.4.133		TCP	151
1040	9.256284	63.80.4.133		TCP	151
1041	9.256314	192.168.1.77		TCP	5

```
⊞ Frame 1036: 758 bytes on wire                      red (6064 bits)
⊞ Ethernet II, Src: Msi_74:82:e6                     ctionte_d8:a3:88 (
⊞ Internet Protocol Version 4, S                     77), Dst: 173.194.
⊞ Transmission Control Protocol,                     t Port: http (80),
⊞ Hypertext Transfer Protocol
```

```
0000  a8 39 44 d8 a3 88 00 16  17        ..... .t....E.
0010  02 e8 23 8b 40 00 80 06  43        .@... C....M..
0020  21 29 f9 08 00 50 f0 6c  54        ..P.l T.....P.
0030  3f df 45 76 00 00 47 45  54        v..GE T /__utm
0040  2e 67 69 66 3f 75 74 6d  77        f?utm wv=5.2.3
```

You’ll see the full conversation between the client and the server.



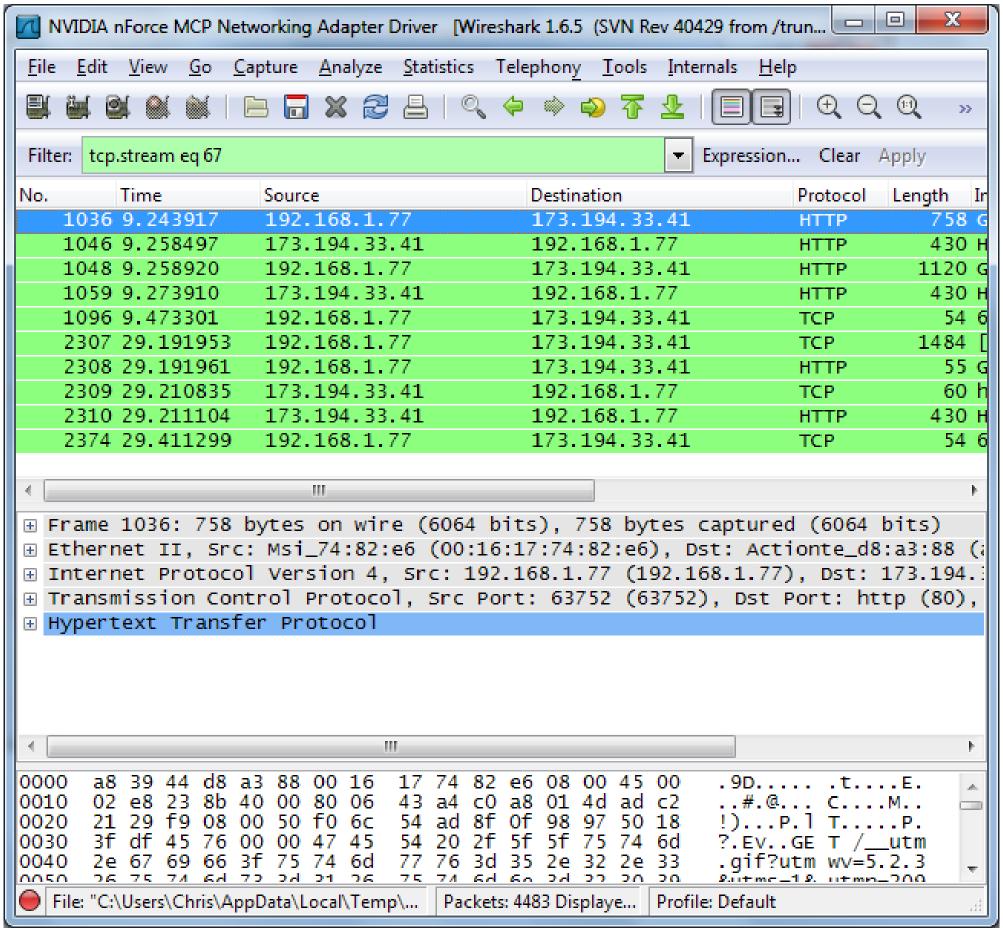
```
Accept-Encoding: gzip, deflate
Accept-Charset: ISO-8859-1,utf-8;q=0.7,*;q=0.7
Connection: keep-alive
Referer: http://ca.linkedin.com/pub/geds-dead/21/192/326

HTTP/1.1 200 OK
Date: Thu, 26 Jan 2012 03:03:47 GMT
Content-Length: 35
X-Content-Type-Options: nosniff
Pragma: no-cache
Expires: Wed, 19 Apr 2000 11:43:00 GMT
Last-Modified: Wed, 21 Jan 2004 19:51:30 GMT
Content-Type: image/gif
Cache-Control: private, no-cache, no-cache=Set-Cookie, proxy-
revalidate
Age: 210285
Server: GFE/2.0

GIF89a.............,..........D..;GET /__utm.gif?
utmwv=5.2.3&utms=1&utmn=637238821&utmhn=www.theglobeandmail.com
&utmcs=UTF-8&utmsr=1280x1024&utmvp=1263x893&utmsc=24-
bit&utmul=en-us&utmje=1&utmfl=11.1%20r102&utmdt=Lululemon%20ad%
```

Entire conversation (4329 bytes)

Close the window and you'll find a filter has been applied automatically — Wireshark is showing you the packets that make up the conversation.


NVIDIA nForce MCP Networking Adapter Driver [Wireshark 1.6.5 (SVN Rev 40429 from /trun...
File
Edit
View
Go
Capture
Analyze
Statistics
Telephony
Tools
Internals
Help
Expression...
Clear
Apply

Filter: tcp.stream eq 67

```
No.     Time         Source            Destination       Protocol  Length  In
   1036 9.243917     192.168.1.77      173.194.33.41     HTTP        758 G
   1046 9.258497     173.194.33.41     192.168.1.77      HTTP        430 H
   1048 9.258920     192.168.1.77      173.194.33.41     HTTP       1120 G
   1059 9.273910     173.194.33.41     192.168.1.77      HTTP        430 H
   1096 9.473301     192.168.1.77      173.194.33.41     TCP          54 6
   2307 29.191953    192.168.1.77      173.194.33.41     TCP        1484 [
   2308 29.191961    192.168.1.77      173.194.33.41     HTTP         55 G
   2309 29.210835    173.194.33.41     192.168.1.77      TCP          60 h
   2310 29.211104    173.194.33.41     192.168.1.77      HTTP        430 H
   2374 29.411299    192.168.1.77      173.194.33.41     TCP          54 6
```

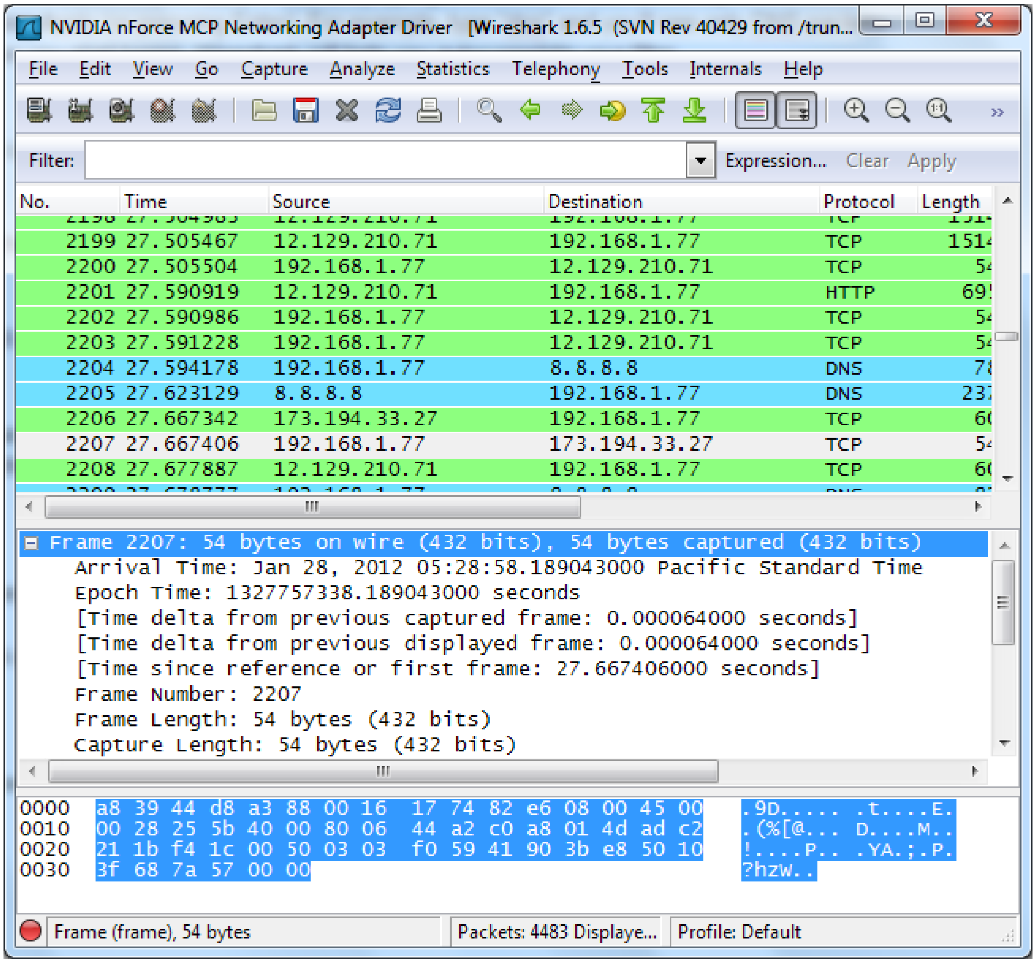
```
⊞ Frame 1036: 758 bytes on wire (6064 bits), 758 bytes captured (6064 bits)
⊞ Ethernet II, Src: Msi_74:82:e6 (00:16:17:74:82:e6), Dst: Actionte_d8:a3:88 (a
⊞ Internet Protocol Version 4, Src: 192.168.1.77 (192.168.1.77), Dst: 173.194.3
⊞ Transmission Control Protocol, Src Port: 63752 (63752), Dst Port: http (80),
⊞ Hypertext Transfer Protocol
```

```
0000  a8 39 44 d8 a3 88 00 16  17 74 82 e6 08 00 45 00   .9D..... .t....E.
0010  02 e8 23 8b 40 00 80 06  43 a4 c0 a8 01 4d ad c2   ..#.@... C....M..
0020  21 29 f9 08 00 50 f0 6c  54 ad 8f 0f 98 97 50 18   !)...P.l T.....P.
0030  3f df 45 76 00 00 47 45  54 20 2f 5f 5f 75 74 6d   ?.Ev..GE T /__utm
0040  2e 67 69 66 3f 75 74 6d  77 76 3d 35 2e 32 2e 33   .gif?utm wv=5.2.3
0050  26 75 74 6d 73 3d 31 26  75 74 6d 6e 3d 32 30 30   &utms=1& utmn=200
```

File: "C:\Users\Chris\AppData\Local\Temp\... | Packets: 4483 Displaye... | Profile: Default

Inspecting Packets

Click a packet to select it and you can dig down to view its details.


NVIDIA nForce MCP Networking Adapter Driver [Wireshark 1.6.5 (SVN Rev 40429 from /trun...
File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help
Filter:
Expression... Clear Apply

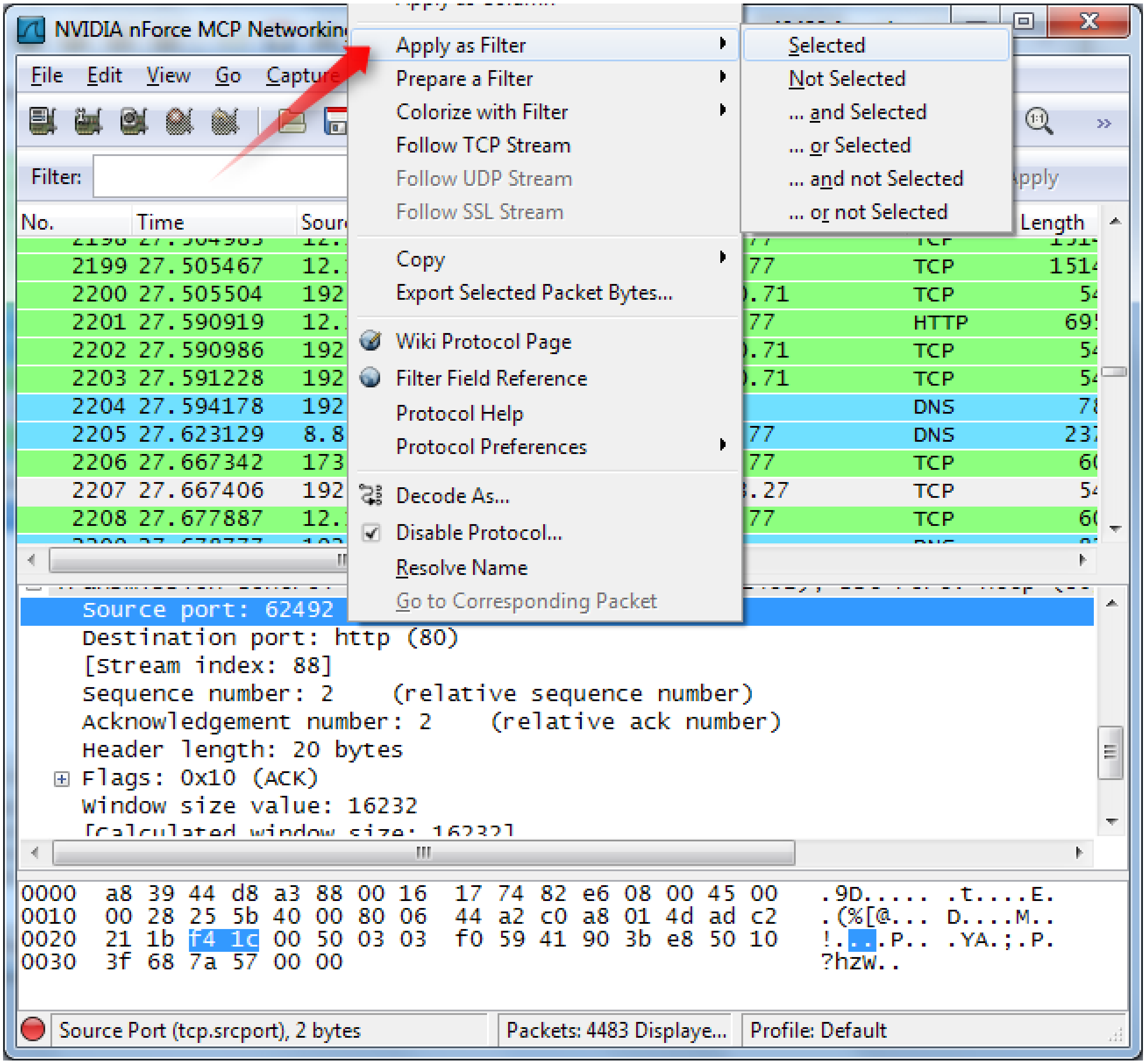
No.	Time	Source	Destination	Protocol	Length
2199	27.505467	12.129.210.71	192.168.1.77	TCP	1514
2200	27.505504	192.168.1.77	12.129.210.71	TCP	54
2201	27.590919	12.129.210.71	192.168.1.77	HTTP	695
2202	27.590986	192.168.1.77	12.129.210.71	TCP	54
2203	27.591228	192.168.1.77	12.129.210.71	TCP	54
2204	27.594178	192.168.1.77	8.8.8.8	DNS	78
2205	27.623129	8.8.8.8	192.168.1.77	DNS	237
2206	27.667342	173.194.33.27	192.168.1.77	TCP	60
2207	27.667406	192.168.1.77	173.194.33.27	TCP	54
2208	27.677887	12.129.210.71	192.168.1.77	TCP	60

```
⊟ Frame 2207: 54 bytes on wire (432 bits), 54 bytes captured (432 bits)
    Arrival Time: Jan 28, 2012 05:28:58.189043000 Pacific Standard Time
    Epoch Time: 1327757338.189043000 seconds
    [Time delta from previous captured frame: 0.000064000 seconds]
    [Time delta from previous displayed frame: 0.000064000 seconds]
    [Time since reference or first frame: 27.667406000 seconds]
    Frame Number: 2207
    Frame Length: 54 bytes (432 bits)
    Capture Length: 54 bytes (432 bits)
```

```
0000  a8 39 44 d8 a3 88 00 16  17 74 82 e6 08 00 45 00   .9D..... .t....E.
0010  00 28 25 5b 40 00 80 06  44 a2 c0 a8 01 4d ad c2   .(%[@... D....M..
0020  21 1b f4 1c 00 50 03 03  f0 59 41 90 3b e8 50 10   !....P.. .YA.;.P.
0030  3f 68 7a 57 00 00                                  ?hzW..
```

Frame (frame), 54 bytes | Packets: 4483 Displaye... | Profile: Default

You can also create filters from here — just right-click one of the details and use the Apply as Filter submenu to create a filter based on it.



```
2199 27.505467  12.   77    TCP   1514
2200 27.505504  192   ).71  TCP   54
2201 27.590919  12.   77    HTTP  69
2202 27.590986  192   ).71  TCP   54
2203 27.591228  192   ).71  TCP   54
2204 27.594178  192         DNS   78
2205 27.623129  8.8   77    DNS   23
2206 27.667342  173   77    TCP   60
2207 27.667406  192   .27   TCP   54
2208 27.677887  12.   77    TCP   60
```

```
    Source port: 62492
    Destination port: http (80)
    [Stream index: 88]
    Sequence number: 2    (relative sequence number)
    Acknowledgement number: 2    (relative ack number)
    Header length: 20 bytes
  ⊞ Flags: 0x10 (ACK)
    Window size value: 16232
```

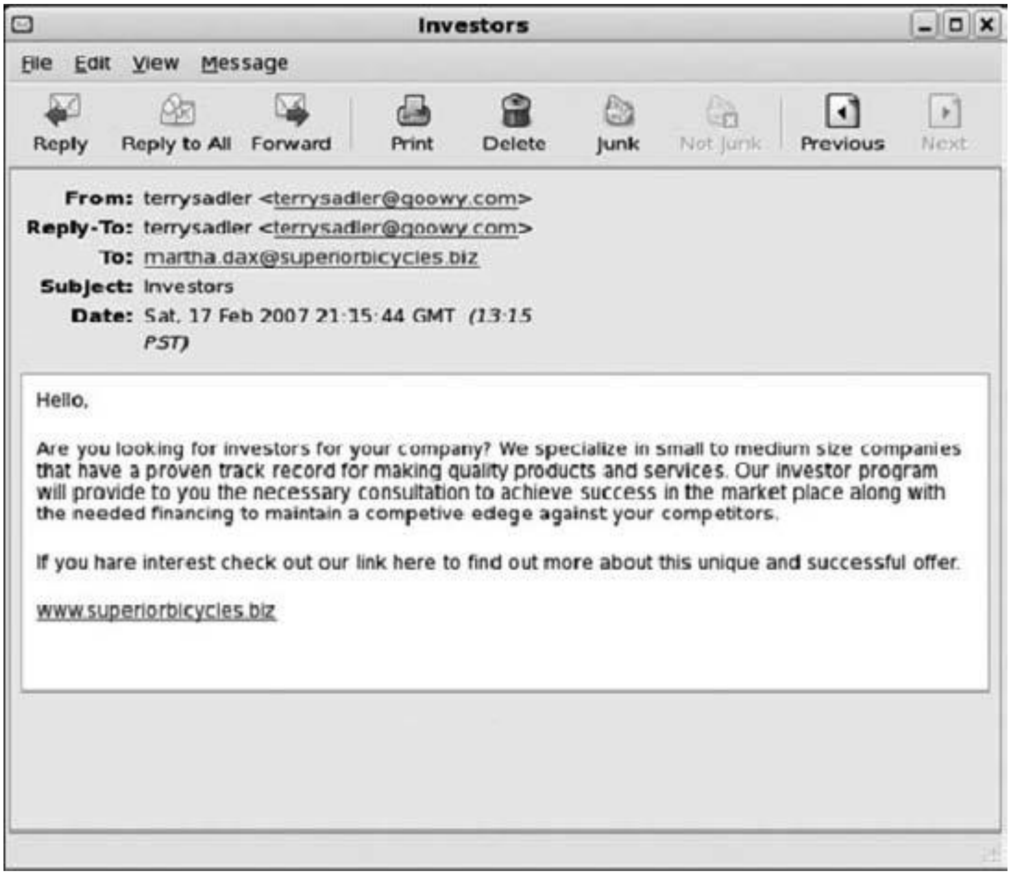
```
0000  a8 39 44 d8 a3 88 00 16  17 74 82 e6 08 00 45 00   .9D..... .t....E.
0010  00 28 25 5b 40 00 80 06  44 a2 c0 a8 01 4d ad c2   .(%[@... D....M..
0020  21 1b f4 1c 00 50 03 03  f0 59 41 90 3b e8 50 10   !....P.. .YA.;.P.
0030  3f 68 7a 57 00 00                                  ?hzW..
```

Practical No. 11: using Email Forensics Tool

Using Email Forensics Tools

- Using AccessData FTK to Recover E-mail
- FTK can filter or find files specific to e-mail clients and servers. You can configure these filters when you enter search parameters. In this section, we will learn how to use FTK and a hexadecimal
  editor to recover e-mails.
- To recover e-mail from Outlook and Outlook Express, AccessData integrated dtSearch (www.dtsearch.com) into FTK 1.x. dtSearch builds a B*-tree index of all text data in a drive, an image file, or a group of files.
- One unique feature is its capability to read .pst and .dbx files and index all text information, including attached files.
- In thenext activity, we're looking for an e-mail from Terry Sadler in the Jim_shu's.pst file.

- Because of Jim’s responses to a poor performance review, the CEO of Superior Bicycles,Martha Dax, suspects he might have obtained sensitive information about the company’s business model that he’s leaking to a competitor.
- Martha asked her CIO, Bob Swartz, to have an IT employee copy the Outlook .pst file from Jim Shu’s old computer to a USB drive.



From: terrysadler <terrysadler@goowy.com>
Reply-To: terrysadler <terrysadler@goowy.com>
To: martha.dax@superiorbicycles.biz
Subject: Investors
Date: Sat, 17 Feb 2007 21:15:44 GMT *(13:15 PST)*

Hello,

Are you looking for investors for your company? We specialize in small to medium size companies that have a proven track record for making quality products and services. Our investor program will provide to you the necessary consultation to achieve success in the market place along with the needed financing to maintain a competive edege against your competitors.

If you hare interest check out our link here to find out more about this unique and successful offer.

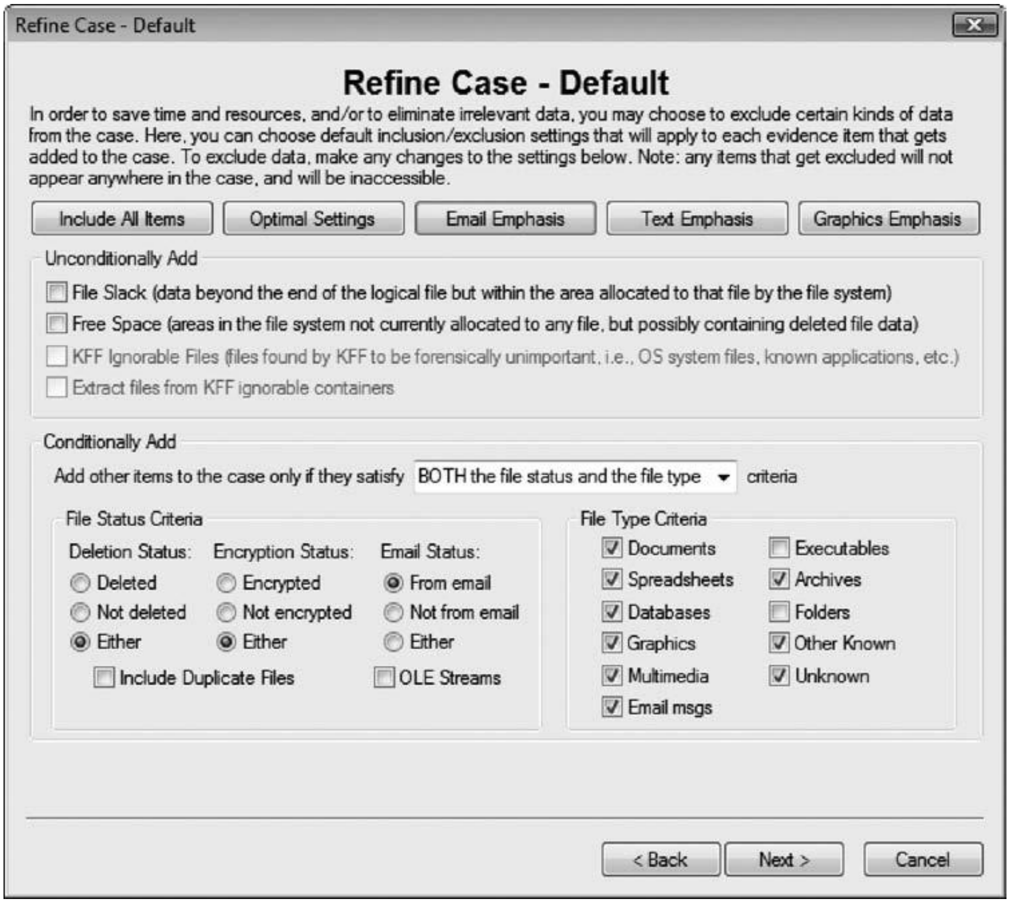
www.superiorbicycles.biz

- She gives you a printout of the message from Terry Sadler along with the USB drive.
- To process this investigation, you need to examine the Jim_shu’s.pst file, locate the message, and export it for further analysis of its header to see how Jim might have received it. Follow these steps:

1. Start AccessData FTK by right-clicking the AccessData FTK desktop icon, clicking Run as administrator, and clicking Continue in the UAC message box. If you’re prompted with a warning message and/or notification, click OK as needed to continue. If asked whether you want to save the existing default case, click Yes.
2. When the AccessData FTK Startup dialog box opens, click Start a new case, and then click OK.

3.In the New Case dialog box, type your name for the investigator name, and type t for the case number and case name. Click Browse, navigate to and click your work folder, click OK, and then click Next.

4. In the Case Information dialog box, enter your investigator information, and then click Next.
5. Click Next until you reach the Refine Case - Default dialog box, shown in Figure .
6. Click the Email Emphasis button, and then click Next.



Refine Case - Default

Refine Case - Default

In order to save time and resources, and/or to eliminate irrelevant data, you may choose to exclude certain kinds of data from the case. Here, you can choose default inclusion/exclusion settings that will apply to each evidence item that gets added to the case. To exclude data, make any changes to the settings below. Note: any items that get excluded will not appear anywhere in the case, and will be inaccessible.

Unconditionally Add

- □ File Slack (data beyond the end of the logical file but within the area allocated to that file by the file system)
- □ Free Space (areas in the file system not currently allocated to any file, but possibly containing deleted file data)
- □ KFF Ignorable Files (files found by KFF to be forensically unimportant, i.e., OS system files, known applications, etc.)
- □ Extract files from KFF ignorable containers

Conditionally Add

Add other items to the case only if they satisfy BOTH the file status and the file type criteria

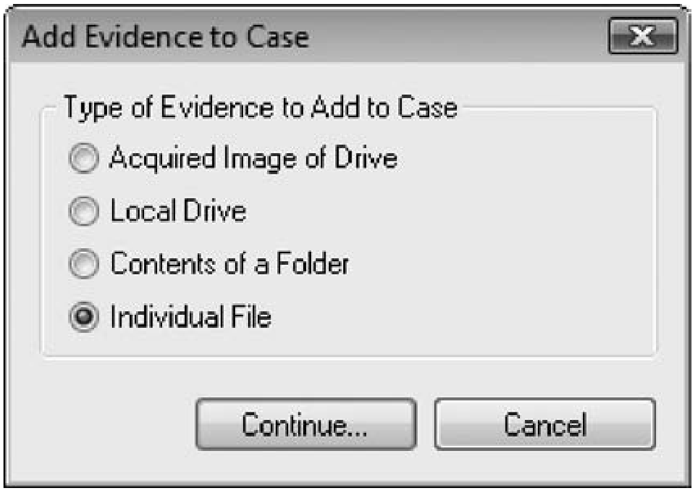
File Status Criteria

Deletion Status:	Encryption Status:	Email Status:
○ Deleted	○ Encrypted	● From email
○ Not deleted	○ Not encrypted	○ Not from email
● Either	● Either	○ Either
□ Include Duplicate Files	□ OLE Streams	

File Type Criteria

☑ Documents	□ Executables
☑ Spreadsheets	☑ Archives
☑ Databases	□ Folders
☑ Graphics	☑ Other Known
☑ Multimedia	☑ Unknown
☑ Email msgs	

6. Click Next until you reach the Add Evidence to Case dialog box, and then click the Add Evidence button.
7. In the Add Evidence to Case dialog box, click the Individual File option button, and then click Continue.
8. In the Select File dialog box, navigate to your work folder, click the Jim_shu's.pst file, and then click Open.
9. In the Evidence Information dialog box, click OK.



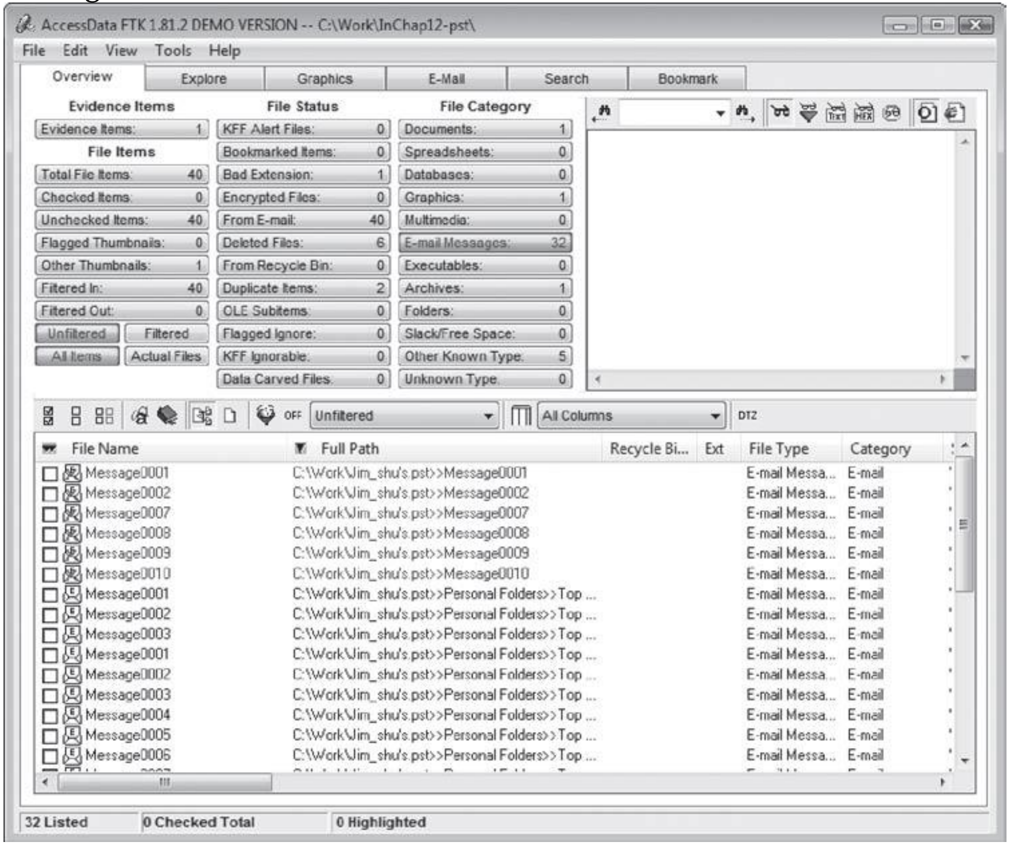
Add Evidence to Case

Type of Evidence to Add to Case

- ○ Acquired Image of Drive
- ○ Local Drive
- ○ Contents of a Folder
- ● Individual File

When the Add Evidence to Case dialog box opens, click Next. In the Case summary dialog box, click Finish.

11. When FTK finishes processing the file, in the main FTK window, click the E-mail Messages button, and then click the Full Path column header to sort the records



AccessData FTK 1.81.2 DEMO VERSION -- C:\Work\InChap12-pst\

Evidence Items		File Status		File Category	
Evidence Items:	1	KFF Alert Files:	0	Documents:	1
File Items		Bookmarked Items:	0	Spreadsheets:	0
Total File Items:	40	Bad Extension:	1	Databases:	0
Checked Items:	0	Encrypted Files:	0	Graphics:	1
Unchecked Items:	40	From E-mail:	40	Multimedia:	0
Flagged Thumbnails:	0	Deleted Files:	6	E-mail Messages:	32
Other Thumbnails:	1	From Recycle Bin:	0	Executables:	0
Filtered In:	40	Duplicate Items:	2	Archives:	1
Filtered Out:	0	OLE Subitems:	0	Folders:	0
		Flagged Ignore:	0	Slack/Free Space:	0
		KFF Ignorable:	0	Other Known Type:	5
		Data Carved Files:	0	Unknown Type:	0

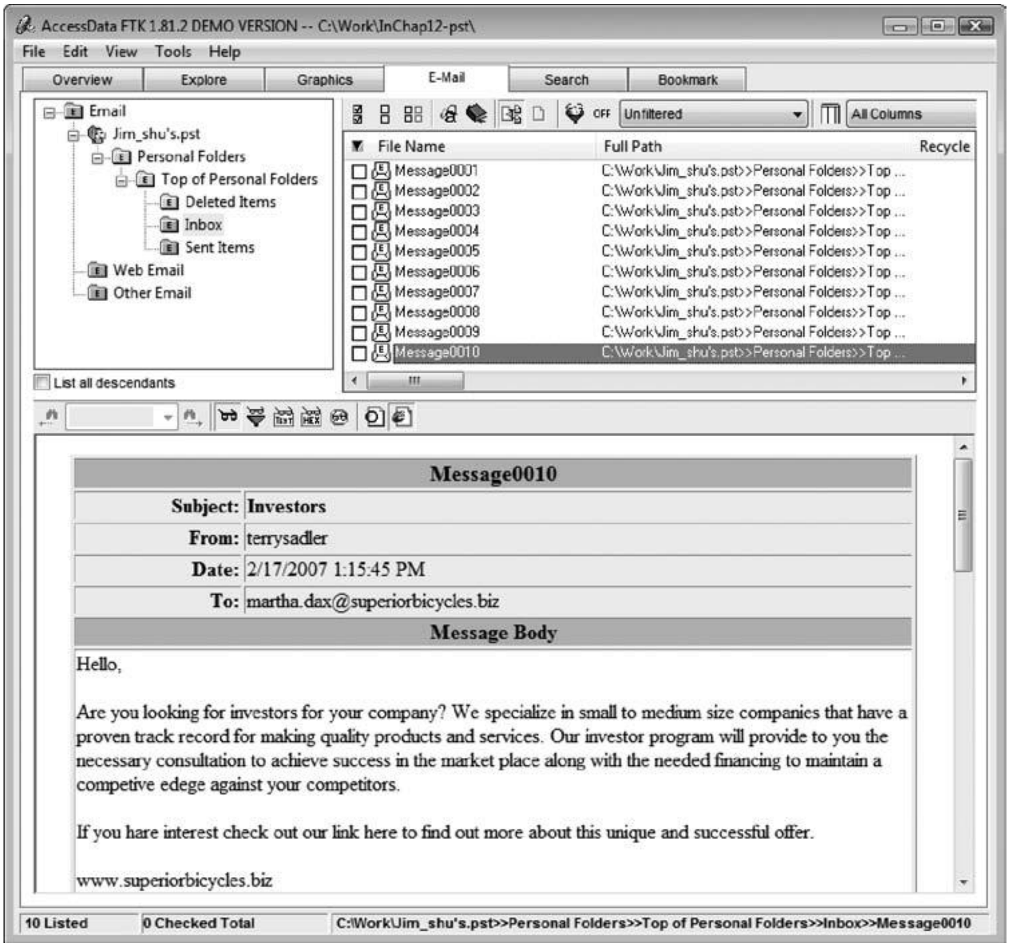
Unfiltered | All Columns

File Name	Full Path	Recycle Bi...	Ext	File Type	Category
□ Message0001	C:\Work\Jim_shu's.pst>>Message0001			E-mail Messa...	E-mail
□ Message0002	C:\Work\Jim_shu's.pst>>Message0002			E-mail Messa...	E-mail
□ Message0007	C:\Work\Jim_shu's.pst>>Message0007			E-mail Messa...	E-mail
□ Message0008	C:\Work\Jim_shu's.pst>>Message0008			E-mail Messa...	E-mail
□ Message0009	C:\Work\Jim_shu's.pst>>Message0009			E-mail Messa...	E-mail
□ Message0010	C:\Work\Jim_shu's.pst>>Message0010			E-mail Messa...	E-mail
□ Message0001	C:\Work\Jim_shu's.pst>>Personal Folders>>Top ...			E-mail Messa...	E-mail
□ Message0002	C:\Work\Jim_shu's.pst>>Personal Folders>>Top ...			E-mail Messa...	E-mail
□ Message0003	C:\Work\Jim_shu's.pst>>Personal Folders>>Top ...			E-mail Messa...	E-mail
□ Message0001	C:\Work\Jim_shu's.pst>>Personal Folders>>Top ...			E-mail Messa...	E-mail
□ Message0002	C:\Work\Jim_shu's.pst>>Personal Folders>>Top ...			E-mail Messa...	E-mail
□ Message0003	C:\Work\Jim_shu's.pst>>Personal Folders>>Top ...			E-mail Messa...	E-mail
□ Message0004	C:\Work\Jim_shu's.pst>>Personal Folders>>Top ...			E-mail Messa...	E-mail
□ Message0005	C:\Work\Jim_shu's.pst>>Personal Folders>>Top ...			E-mail Messa...	E-mail
□ Message0006	C:\Work\Jim_shu's.pst>>Personal Folders>>Top ...			E-mail Messa...	E-mail

32 Listed | 0 Checked Total | 0 Highlighted

12. Click the E-Mail tab. In the tree view, click to expand all folders, and then click the Inbox folder. If necessary, to view all messages, click the List all descendants check box.

13. In the File List pane at the upper right, click Message0010; as shown in the pane at the bottom, it’s from terrysadler and is addressed to martha.dax@superiorbicycles.biz.



File Name	Full Path	Recycle
Message0001	C:\Work\Jim_shu's.pst>>Personal Folders>>Top ...	
Message0002	C:\Work\Jim_shu's.pst>>Personal Folders>>Top ...	
Message0003	C:\Work\Jim_shu's.pst>>Personal Folders>>Top ...	
Message0004	C:\Work\Jim_shu's.pst>>Personal Folders>>Top ...	
Message0005	C:\Work\Jim_shu's.pst>>Personal Folders>>Top ...	
Message0006	C:\Work\Jim_shu's.pst>>Personal Folders>>Top ...	
Message0007	C:\Work\Jim_shu's.pst>>Personal Folders>>Top ...	
Message0008	C:\Work\Jim_shu's.pst>>Personal Folders>>Top ...	
Message0009	C:\Work\Jim_shu's.pst>>Personal Folders>>Top ...	
Message0010	C:\Work\Jim_shu's.pst>>Personal Folders>>Top ...	

Message0010

Subject:	**Investors**
From:	terrysadler
Date:	2/17/2007 1:15:45 PM
To:	martha.dax@superiorbicycles.biz

Message Body

Hello,

Are you looking for investors for your company? We specialize in small to medium size companies that have a proven track record for making quality products and services. Our investor program will provide to you the necessary consultation to achieve success in the market place along with the needed financing to maintain a competive edege against your competitors.

If you hare interest check out our link here to find out more about this unique and successful offer.

www.superiorbicycles.biz

10 Listed | 0 Checked Total | C:\Work\Jim_shu's.pst>>Personal Folders>>Top of Personal Folders>>Inbox>>Message0010

14. Right-click Message0010 in the File List pane and click Export File. In the Export Files dialog box, click OK. If you get a message box about exporting files with a filter applied, click the Do not remind me anymore check box, and then click OK. Click OK again in the Export Files message box.

15. Click File, Exit from the menu, and then click No in the FTK Exit Backup Confirmation message box.

16. When you start a case in FTK, a subfolder is created under the case folder to store data. When you export a file, FTK creates an Export subfolder under this subfolder. FTK saves exported files in the HTML format with no extension.

To view the exported Message0010 file, follow these steps:

1. Open Windows Explorer and navigate to \Export under your work folder.

2. Right-click the Message0010 file and click Rename. Type Message0010.html and press Enter.

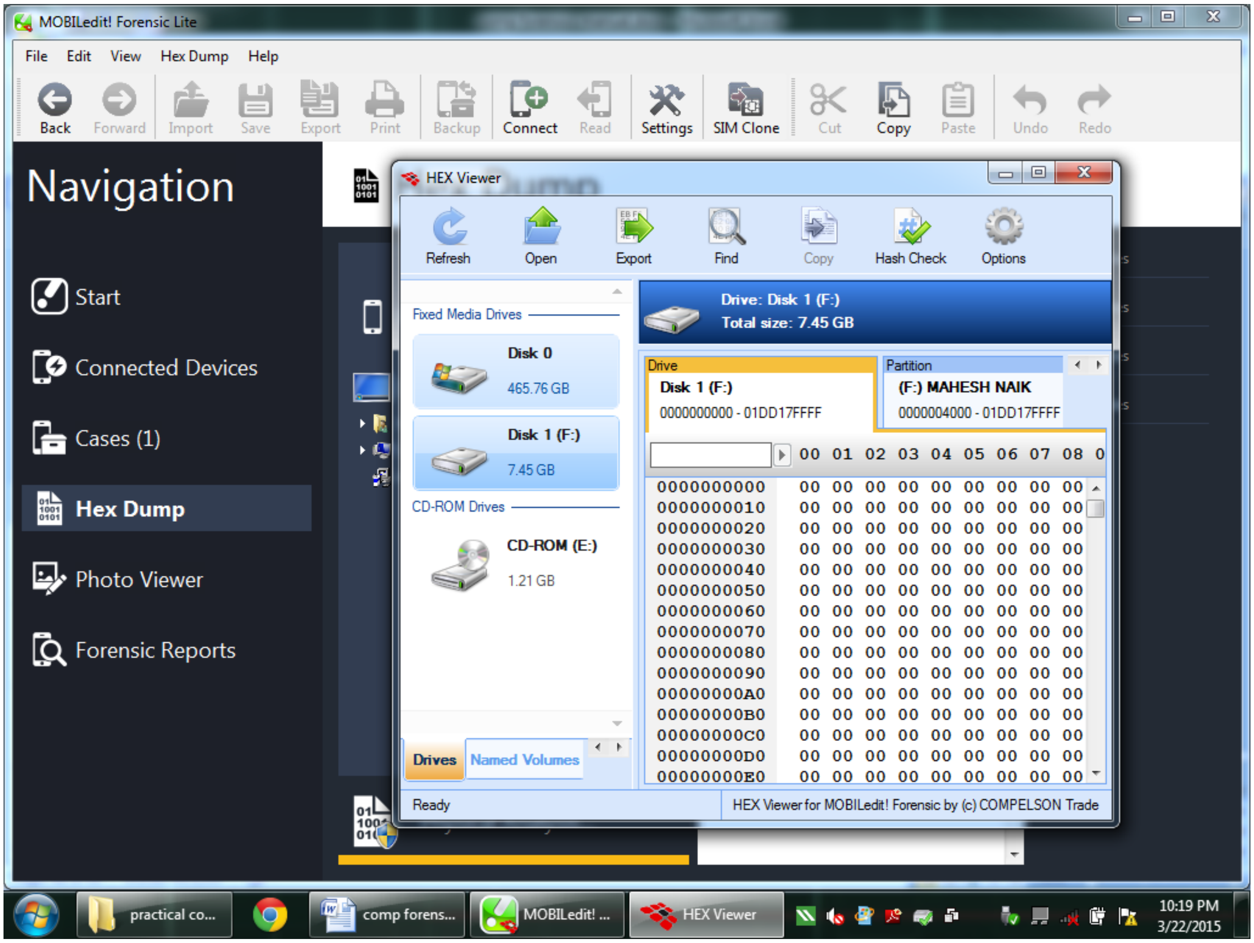
3. Double-click Message0010.html to view it in a Web browser.

4. Print this Web page and save it for further analysis. Exit your Web browser and Windows Explorer.

Practical No. 12 Using Mobile Forensics software tools

Aim: Exploring Mobiledit Forensics

- MOBILedit! (available at www.mobiledit.com) is a forensics software tool containing a built-in writeblocker. It can connect to phones directly via Bluetooth, irDA, or a cable and can read SIM cards by using a SIM reader. It's also notable for being very user friendly.



Disk 0
465.76 GB

Disk 1 (F:)
7.45 GB

CD-ROM (E:)
1.21 GB

Drive: Disk 1 (F:)
Total size: 7.45 GB

Drive
Disk 1 (F:)
0000000000 - 01DD17FFFF

Partition
(F:) MAHESH NAIK
0000004000 - 01DD17FFFF

```
            00 01 02 03 04 05 06 07 08 0
0000000000  00 00 00 00 00 00 00 00 00
0000000010  00 00 00 00 00 00 00 00 00
0000000020  00 00 00 00 00 00 00 00 00
0000000030  00 00 00 00 00 00 00 00 00
0000000040  00 00 00 00 00 00 00 00 00
0000000050  00 00 00 00 00 00 00 00 00
0000000060  00 00 00 00 00 00 00 00 00
0000000070  00 00 00 00 00 00 00 00 00
0000000080  00 00 00 00 00 00 00 00 00
0000000090  00 00 00 00 00 00 00 00 00
00000000A0  00 00 00 00 00 00 00 00 00
00000000B0  00 00 00 00 00 00 00 00 00
00000000C0  00 00 00 00 00 00 00 00 00
00000000D0  00 00 00 00 00 00 00 00 00
00000000E0  00 00 00 00 00 00 00 00 00
```

Ready

HEX Viewer for MOBILedit! Forensic by (c) COMPELSON Trade

Practical No. 13: Using AccessData FTK to Generate Reports

Aim: Generating report Using AccessData FTK.

Task to be performed

Working with Reports

- Creating a Report
- Entering Basic Case Information
- Managing Bookmarks
- Selecting the Properties of Bookmarked Files
- Managing Thumbnails
- Selecting a File Path List
- Selecting a File Properties List
- Selecting the Properties of the File Properties List
- Adding Supplementary Files and the Case Log
- Selecting the Report Location
- Viewing and Distributing a Report
- Updating a Report
- Modifying a Report
- Modifying a Report in the Same FTK Session
- Modifying a Report in a Different FTK Session

(refer chapter 13 of FTK manual)