

# Windows FTK Forensics

## Lab Descriptions

Given a disk image, you will use FTK to analyze this image and use FTK to create a report about this incident. (Note: In a real investigation, the investigator will write his/her own report using software generated report as a reference.) After you are done with this exercise, if you want to challenge yourself with more complicated cases, please select Windows cases from <http://www.forensicfocus.com/images-and-challenges>.

## Question 1: What are the types of evidence that can be added to a case in FTK?

Acquired Images, All Images in Directory, Contents of a Directory, Individual Files, Physical Drive, Logical Drive.

---

## Set the Time Zone

When you acquire a computer as evidence it is important to make note of the computer's time and time zone, especially if you need to correlate evidence from different time zones (never assume the time or time zone on a computer is correct.)

Click "OK". Now FTK Data Processing Status window will pop-up to show you the progress. For a large image, this process takes a while since FTK will process the evidence base on your setting defined in evidence processing options.

After it is done, your ACME-FTK case is ready for your examination. If you like, you can close the Data Processing Status window.

## Step 2: Analyzing Evidence Using FTK

First, familiar yourself with the FTK examiner's GUI interface.

The Overview tab groups items into categories. It displays items in Category Pane (top-left pane by default), File list Pane (bottom), and File Content Viewer Pane (top-right). Although these panes can be rearranged, you can always reset the panes to default by choosing View -> Tab Layout -> Reset To Default.

Click the **OVERVIEW** tab; examine each category and note the numbers for each type of file.

**Question 2: What type of files are grouped into the “File Status container”?**

Bad Extensions, Data carved Files, Decrypted Files, Deleted Files, Duplicate Items, Email Attachments, Email Related Items, Encrypted Files, Flagged Ignore, Flagged Privileged, From Recycle Bin, KFF Alert Files, KFF Ignorable, OCR Graphics, OLE Subitems, User-Decrypted Files.

---

## File Signatures

A file type (JPEG, Word Document, MP3 file) can be determined by the file’s extension and by a header that precedes the data in the file. If a file’s extension has been deliberately changed, then the only way to determine its type is by looking at its header.

**Question 3: Examine the information listed in Overview tab to find out where does FTK categorize the files whose extension does not match file type identified in the file header? List Bad Extension files.**

38 Bad Extensions

bbip[1].css,brndlog.bak,browser\_ie[1].js,css-font[1].css,default[1].css,diagram.doc,envoy[1].sb,flash[1].js,home-bb-ie6[1].css,home-ie6[1].css,i\_js\_style[1].css,i\_js\_styleNEWDAY[1].css,join[1].css,javascripts[1].js,master[1].css,mediator[1].sb,newlook[1].css,overlib[1].js,pluginreg.dat,prefs.bak,prefs.js,Project 238x.pdf,Project,47x.xls,slideshow[1].js,styles[1].css,userChrome-example.css,userContent-xample.css,wbk46.tmp,wbk48.tmp,wbk4E.tmp,wbk50.tmp,wbk52.tmp,wbk54.tmp,wbk56.tmp,yg\_csstare[1].js

---

## Data Carved Files:

Data carving is the process of locating files and objects that have been deleted or that are embedded in other files.

**Question 4: Check the number of Data Carved Files from File Status, what is the number?**  
The number is 0

---

Now let’s perform the data carving process.

From the top menu bar, click on Evidence > Additional Analysis.....

In Additional Analysis Window, navigate to miscellaneous tab and check Data Carve. Click carving options to select the types of files to carve.

For this exercise, in order to save time, we only select GIF Files to perform date carving. In real cases, you should select all. Click “OK”.

Click “OK” to perform carving. A “Data Processing Status” Window will pop-up to show you the status of this process. After this job is finished. Close the “Data Processing Status” Window.

**Question 5: Check the number of Data Carved Files again, how many files added to the case by data carving?**

The number of data carved files is now 2

---

**Question 6: What interesting files do you find by performing data carving process? Why is this process so important?**

File for Testing software and test score database  
Configuration file for upgrading the State machine

---

The carved files should be listed in File List Pane at the bottom by default. If you click on the file in the File List Pane, the selected file’s content should be displayed in File Content Pane. If you choose to export the data-carved file, simply right click the file and choose “export...” and save the exported file to your desired location.

---

## **Explore Tab**

Click on **Explore** tab.


The Explore tab displays all the contents of the case evidence in Explorer Tree Pane, File list Pane, and File Content Viewer Pane. You can resize the panes by dragging the edges of the pane according to your need and can always reset the panes to default by choosing View -> Tab Layout -> Reset To Default.

Select the WinLabEnCase.E01 Image

**Question 7: What is the file system of this Image?**

FAT16

---

Expand WinLabEnCase.E01\NONAME\[root]\Documents and Settings\psmith\Recent, and green-select Recent folder  . When you green-select a folder, the files and subdir in this folder will be listed in the bottom File List pane.

**Question 8: Select Documents and Settings\psmith\Recent, what kind of files contain in this folder? Select one file in this folder, what kind of information do you get from the up-right window (File Content, Natural)?**

7 of the 8 files listed under psmiths recent folder are LNK extensions. LNK files can be helpful for an investigation because although the originals were likely deleted or stored on USb, LNK files associate with the originals and may reveal important info.

The file content for “you wont believe this awesome offer.eml.lnk”, (hex/text/filtered) will all indicate the name of the file and show the full path to the file. When the natural tab is selected, it will reveal more link target information(for example: file size and mae times), file attributes, optional fields, target system information(for example: netBios name and MAC address), etc.,

---

**Question 9: Select Documents and Settings\psmith\Local Settings\History\History.IE5\index.dat, click “File Content” and “Natural” from the up-right window, what kind of information is contained in this file?**

A URL with a file path to project47x.doc, and its mae times.

C:/Documents and Settings/psmith/My Documents/Confidential/Project 47x.doc  
accessed time: 3/9/2004 8:30:12 AM -0500  
modified time: 3/9/2004 3:30:12 AM -0500  
expiration time: 4/4/2004 9:30:14 AM -0400

A URL with a file path to a project 238x.rtf, and its mae times.

C:/Documents and Settings/psmith/My Documents/Confidential/diagram.gif  
accessed time: 3/9/2004 8:30:38 AM -0500  
modified time: 3/9/2004 3:30:38 AM -0500  
expiration time: 4/4/2004 9:23:30 AM -0400

Additionally the each of these files have 1 hits each and 0 use counts

---

**Question 10: Select Documents and Settings\psmith\Favorites, what are psmith’s favorite links?**

Customize Links.url  
Free Hotmail.url  
Windows Media.url  
Windows.url

---

**Question 11: Looking into the Recycled folder, which files are currently in the recycler? Select the INFO2 file from the Recycled folder, what information do you get from that file?**

!esktop.ini, De1, De2, INFO2, desktop.ini, J\_computer\_commun.ps, ogdiagram.gif, tse082800.pdf

The information found when investigating INFO2 is a path to a folder titled Boeing and it was last recycled on 3/15/2004

E:\Documents and Settings\psmith\My Documents\Boeing

---

**Question 12: Looking into WINDOWS\System32\spool folder, what information can you get from this folder?**

EMF print spool includes print job details:

Specifies the port IP address and page count

port = IP\_192.168.1.106 & page count = 1

⇒ Project 238x.rtf

⇒ Project 47x.doc

---

## Windows Registry

Green select Documents and Settings\psmith folder in the category pane (top-left) and Locate ntuser.dat in File List pane (bottom).

Right click ntuser.dat and choose “Open in Registry Viewer”. (You could export the ntuse.dat and then launch the AccessData Registry Viewer to view this file in Registry Viewer.)

In the **Registry Viewer**, explore this registry file using the techniques covered in the Registry analysis lecture. For example, you may search for registry key, TypedURL, via Edit -> Find...

**Question 13: Based on the values of the registry key TypedURL, which URLs did psmith search for ACME’s competitor companies? List any other interesting results from ntuser.dat (if any).**

<http://jobs.yahoo.com>

<http://www.monster.com>

<http://www.google.com>  
<http://www.hughes.com>  
<http://www.beoing.com>  
<http://www.raytheon.com>  
<http://www.microsoft.com/isapi/redir.dll?prd=ie&p>

---

## Graphics Tab

The Graphics tab allows you to quickly see all of the pictures contained on all of the devices in the case. Click the **Graphics** tab and green-select WinLabEnCase.E01 from the Evidence Items Pane. All pictures in our case are shown in thumbnails alphabetically.

**Question 14: If a file's extension has been changed to a non-graphics file type (such as changing jpg to txt), will it be displayed in the Gallery view? Provide one example to support your statement.**

EX: bbip[1].jpg

This file was renamed / changed to a non graphics file type bbip[1].txt  
bbip[1].jpg is displayed as a thumbnail inside the graphics gallery view

---

## Bookmarking

Bookmarks allow you to mark folders, files, or parts of a file for later reference and for inclusion in reports.

Now let's bookmark some files. Checkmark (or highlight) three graphics in the file list; right click the graphics and select Create Bookmark. Name the bookmark as "Checkmarked Graphics" (or Highlighted Graphics if you choose to highlight). Then select "All Checked" (or "All highlighted") radio button. You should see the graphic files are listed.

Choose a parent directory for this bookmark, and click OK.

You may also bookmark some folders, files, or parts of a file that you feel important for inclusion in your final report.

Go to the **Bookmark** tab to verify the bookmarks.

## Export and Copy Special

Highlight (or checkmark) two graphics and **export** these graphics to your desktop.

Use **Copy Special** to copy a list of the dates and times associated with the exported files to the clipboard. Then paste this data into Microsoft Excel.

**Question 15: What is the major difference between Export a file and Copy Special a file?**

Copy Special a file includes metadata:

name, item #, EXT, Path, Category, P-Size, L-Size, MD%, SHA1, SHA256, MAC

Export includes a thumbnail image exported to desktop. After viewing the image and selecting File Info, it includes: File Name, Date Taken, Size, Dimensions, Folder Path, Source.

‘Export’ is an export of the image, ‘Copy Special’ is Image Data.

---

## **Keywords and Searching**

Searching evidence for information pertaining to a case can be one of the most crucial steps in the examination. FTK supports two kind of search, indexed and live searches. An indexed search uses the index file to find a search term while a live search involves an item-by-item comparison with a search term. The index file could be generated during the creation of a case or be indexed later.

Click the **Indexed Search** tab. In the Terms box, type some keywords, for example “Job”; then click Add. If you add multiple keywords, you will use either “And” or “Or” to cumulate results. Click View Cumulative Results if you add multiple keywords.

Check **Index Search Results** at the up-right pane and expand the search results.

Select one file and find the instances of “Job” in the file.

Create a bookmark to keep a couple of important files in the bookmark called Search Bookmark.

Examining the **Options** and **Import** feature in the indexed Search

**Question 16: What are these two features used for?**

Import → you can import filters that have have been saved as XML files into your system.

Options → allows for different search capabilities. Search options → Stemming Phonic, Synonym, Fuzzy. Result options → max files to list/hits per file, and further filtering by file save times/ size and naming patterns.

---

Click the **Live Search** tab, then choose **Pattern** tab.

Click the 2<sup>nd</sup> arrow to view the default regular expressions.

Select **US Phone Number** and Search.

**Question 17: Do you find any files containing US Phone numbers? List two files that in the result list.**

searchcontractors[1].htm  
contacts[1].htm

---

**Question 18: What is the advantage to use indexed search vs. the live search?**

Both of these support looking into unallocated/slack space.  
live search → item by item comparison / pattern matching w/ regex  
indexed search → requires specific text. however its is faster

---

## Email

Email processing is one of the most important steps in forensics investigation. FTK supports powerful email feature to help you process emails.

**Question 19: Read the manual and find out what kind of email formats do FTK 6 support?**

Exchange and PST Emails can be exported to MSG format. In addition, MSG files resulting from an export of internet email look the way they should.

Compatible mail applications include:

Notes NSF, Outlook PST/OST, Exchange EDB, Outlook Express DBX, Eudora, EML (Microsoft Internet Mail, Earthlink, Thunderbird, Quickmail, etc.), Netscape, AOL and RFC 833

---

Click on the E-Mail tab

Navigate to Deleted items.dbx, Inbox.dbx and Sent Items.dbx, check for each message and bookmark some important messages to support your final report.

**Question 20: Did anything happen? Do you find any important information? If so, what kind of information you got?**

There are two emails from Pat Smith to bconrad@raytheon.com  
The first is an initial proposal email. The second is a follow up.

Proposal: "I'd like to offer you some material from my company in exchange for a position in your company"



**Follow Up:** “It’s been a week since I sent you my proposal. Have you had a chance to consider it” ?

---

### **Step 3: Case Report (See FTK User Guide)**

After performing a thorough forensic investigation, it is critical that you are able to publish and present your findings. FTK has a sophisticated report wizard that allows you to assemble and publish case information. The final report generated by the FTK wizard is in HTML format.

Click File > Report

Fill in the Case information which will appear on the Case Information page of the report.

Create a report to include the following:

- a) all bookmarks and export all bookmarked files
- b) Export full-size graphics and link them to the thumbnails
- c) Include the Date and Time file Properties for the Bookmarked Files
- d) Include only graphics flagged green in the Graphics View
- e) Group 6 thumbnail per row
- f) Include Bad Extension files in the report and export the files to the report along with its data and time property
- g) Add one or more of your own file to the report that support your statement
- h) Create a custom graphic for the report.

**Question 21: Include two screenshots of this report in your submission.**

[Report PDF included in submission] See below for screenshots.

### Bookmark: Job\_search\_stored\_in\_favorites

11/8/2018

Note: the following file filter was applied to this list: "Actual Files"

**Comments:** 16% - 1 hit(s) -- Item 1120 [Find a Job.url] WinLabEnCase.E01/NONAME [FAT16]/[root]/Documents and Settings/psmith/Favorites/Find a Job.url

**Creator:** Admin

**File Count:** 1

#### Files

##### File Comments

<b>Name</b>	Find a Job.url
<b>Physical Size</b>	512 B
<b>Logical Size</b>	220 B
<b>Created Date</b>	3/9/2004 11:39:01 AM (2004-03-09 16:39:01 UTC)
<b>Modified Date</b>	1/23/2004 12:16:50 PM (2004-01-23 17:16:50 UTC)
<b>Accessed Date</b>	3/9/2004
<b>Path</b>	WinLabEnCase.E01/NONAME [FAT16]/[root]/Documents and Settings/psmith/Favorites/Find a Job.url
<b>Exported as</b>	<a href="#">Report_Files/files/Find a Job.url</a>

### Bookmark: Project\_47\_print\_spool

11/8/2018

Note: the following file filter was applied to this list: "Actual Files"

**Comments:**

**Creator:** Admin

**File Count:** 1

#### Files

##### File Comments

<b>Name</b>	FP00000.SPL
<b>Physical Size</b>	25600 B
<b>Logical Size</b>	25336 B
<b>Created Date</b>	3/9/2004 11:38:49 AM (2004-03-09 16:38:49 UTC)
<b>Modified Date</b>	3/9/2004 8:30:26 AM (2004-03-09 13:30:26 UTC)
<b>Accessed Date</b>	3/15/2004
<b>Path</b>	WinLabEnCase.E01/NONAME [FAT16]/[root]/WINDOWS/system32/spool/PRINTERS/FP00000.SPL
<b>Exported as</b>	<a href="#">Report_Files/files/FP00000.SPL</a> (Binary link)

**Question 22: Choose one FTK feature that is not used in this lab, and provide a hypothetical case that this feature will help to investigate this case.**

### The Known Filter File (KFF)

⇒ compares known file hash values against the FTK case files

⇒ running this analysis during an investigation can identify matches and speed up an investigation or possibly alert the investigator to files that would have gone undetected. For example, in a child pornography case, like the one mentioned here <http://cyb3rcrim3.blogspot.com/2012/11/ftk-kff-and-motion-to-suppress.html>, the investigator included the KFF in his search which increased the scope and identified illegal content on the suspect drive.

---