Advanced Computer Forensics
Windows FTK Forensics Lab

Deliverable: Submit **all your answers to the questions** to the Windows FTK Lab dropbox **by 11/11/2018 midnight**.

Read the ENTIRE document before starting to be sure you have all the necessary tools and files required to complete the lab. You are encouraged to further explore other features of FTK that are not covered in this lab, using the FTK user guide.

Objective

In this exercise, you will utilize FTK to conduct an analysis of an incident. This project will help you tie all of the pieces and techniques together, so that you have a better understanding of the whole picture of forensics investigation.

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.)

Lab Setup

This lab is designed to function on the RLES vRealize Automation (vRA). The interface is available by navigating to https://rlescloud.rit.edu. **Google Chrome works better than Firefox**. The steps are as follows.

1. Go to https://rlescloud.rit.edu
2. Log in with your RIT username & password
3. Click on the **Catalog** tab
4. Click the **Request** button for "FTK and EnCase"
5. Click the **Submit** button (in the lower-right corner of the window) to deploy the VM
6. Click on the **Requests** tab to monitor your request. It could take up to 10 minutes to deploy. Click the refresh button at the bottom of the page to update the status of your request.
7. When your request has successfully completed deployment, click on the **Items** tab.
8. **Expand the disclosure triangle** next to your deployment item, then click the name of the VM (for example, Win10-0015). From the Actions menu, choose "**Connect to Remote Console**".

The Windows virtual machine is ready to use. In case you need to re-login, the Windows login credential is:
Username: Student
Password: student

FTK software including FTK 6.2 along with FTK User Guide the and Registry Viewer are installed on the Windows 10. Please read FTK User Guide located on the desktop of the VM.

The evidence file, WinLabEnCase.E01, is located in the ***images*** folder on desktop.

Scenario: ACME Industry develops custom software for the aviation industry. Its main competitors are companies Raytheon, Boeing, and a few smaller contractors. Pat Smith has worked for ACME Industry for 5 years. His supervisor has noted that after being past over several times for a promotion, Pat has become quite disgruntled. The company fears that Pat may be offering proprietary company information to a competitor in exchange for a job.
The first investigator has created an Encase image of Pat's computer's hard drive. Your job is to examine the image using FTK and extract all pertinent information to support or disprove the statement of Pat may be offering proprietary company information to a competitor in exchange for a job.

Steps involved:

1) Locate the evidence file "WinLabEnCase.E01" in images\ on desktop.
2) Create a new case and add the EnCase evidence file to FTK for investigation.
3) Analyze the image.
   Show the activities such as recovering deleted files; finding information that have been purposefully hidden; analyzing MAC time, signatures and Hash sets; searching keywords; gathering pertinent information from compound files such as outlook express .dbx files and registry files; examining IE history file, searching recycled files though the hidden Recycled folder and printer's spool files located in WINDOWS\system32\spool\PRINTERS etc.
4) Generate a report

Note: All information in your report should be verifiable and repeatable in order to be admissible in court.

DETAILED PROCEDURES THAT MAY HELP YOU TO GO THROUGH THE FTK SOFTWARE ARE SHOWN BELOW

Step 1: Starting a New Case

Launch FTK 6.2 (be patient. It takes a while) and login with Admin, netsys.

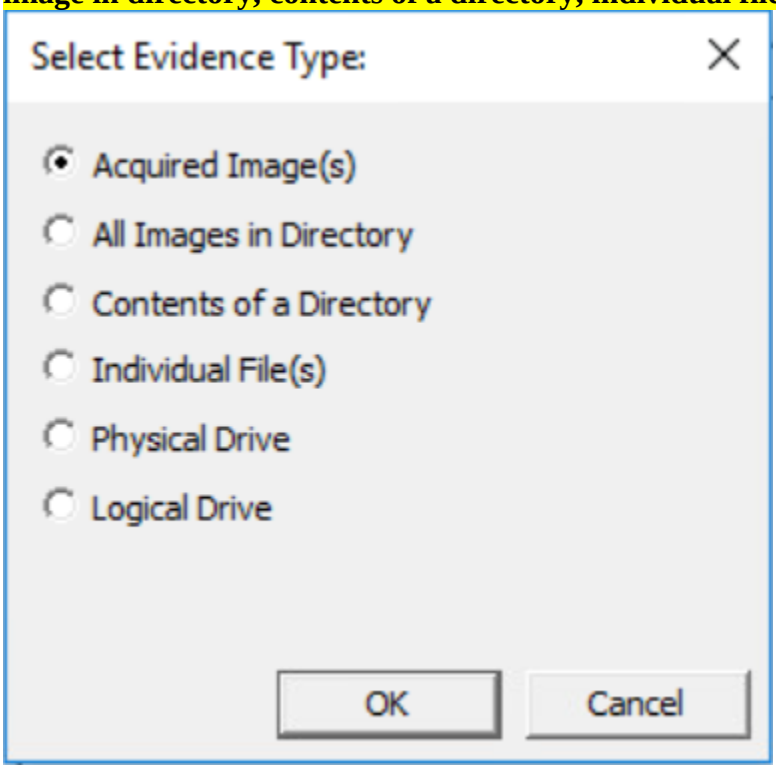
Create a new case by click on "Case -> New…", and name the case "ACME-FTK".
Make the Case Folder Directory to be "C:\Users\Student\Desktop" and include the Database in the case folder by checking "In the case folder" under Database location. Feel free to fill in other information.

Click on "Customize…" to read the default options for Evidence Processing, Evidence Refinement, Index Refinement and Custom File Identification. It is safe to use all default options. However, you should try to understand these options. Click OK.

Add an Image to the exist case

After the case is create, the Manage Evidence window will pop-up.
To add the "WinLabEnCase.E01" file to your newly created case, you click "Add" and choose the evidence type as "Acquired Image(s)"

Question 1: What are the types of evidence that can be added to a case in FTK?
There are 6 types of evidence that can be added to a case in FTK: Acquired Image, All image in directory, contents of a directory, individual files, physical drive and 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.)
In the FTK's Manage Evidence Window, choose Eastern Time with Daylight Saving (US-New York) from the Time Zone dropdown list.

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.

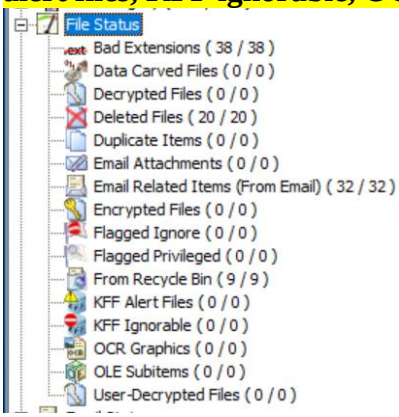
Step 2: Analyzing Evidence Using FTK

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"?
There are 16 files type grouped in the file status container as follow: Bad extensions, data carved files, decrypted files, deleted files, duplicated 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.

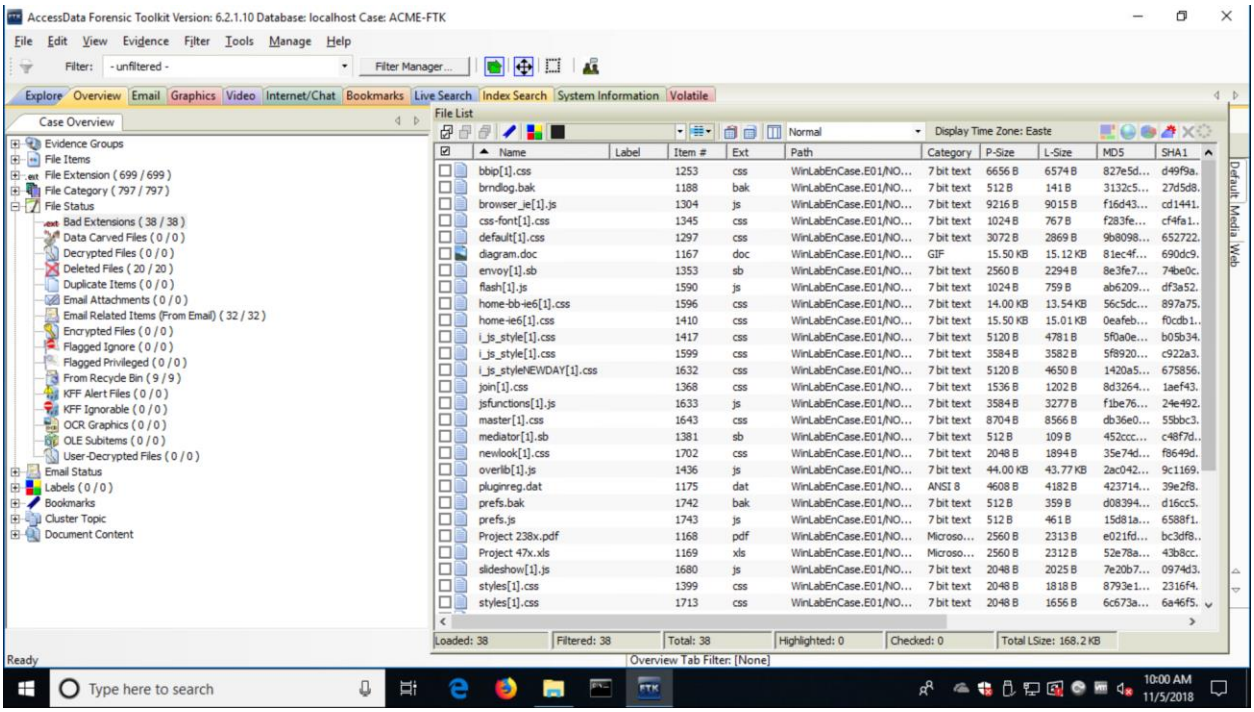


File Signatures

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.

FTK categorize the file that its extension and header doesn't match in Bad extension category in the file status container. Here are some of the bad file extension in the list: bbip[1].css, brndlog.bak, flash[1].js, diagram.doc, envoy[1].sb, pluginrag.dat, project47x.xls, project238x.pdf, wbk44.tmp, etc.

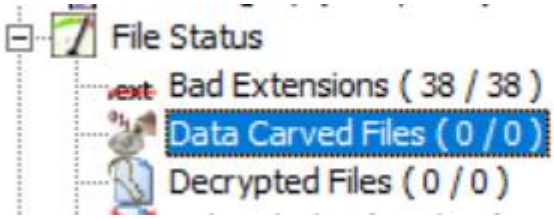


Data Carved Files:

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?

It has zero files.

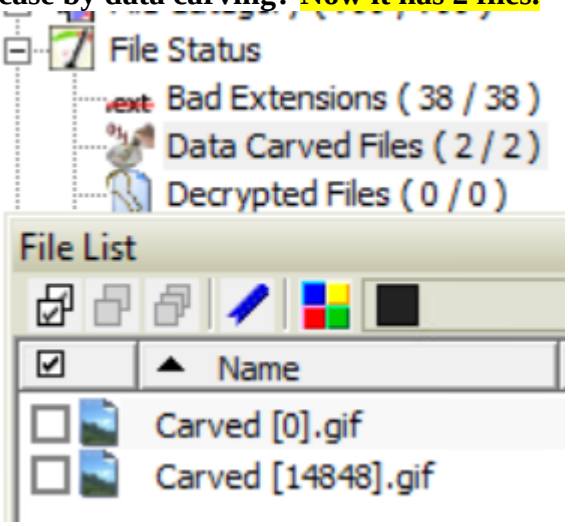


Now let's perform the data carving process.

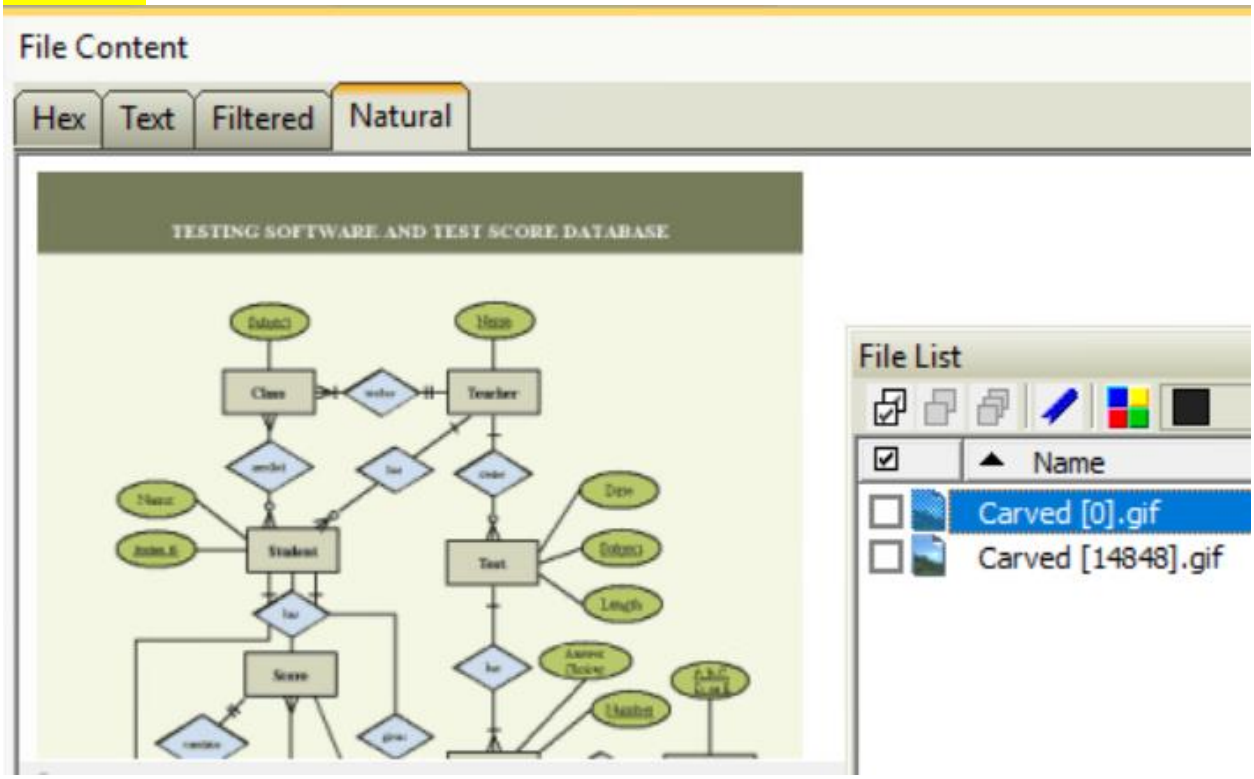
From the top menu bar, click on Evidence > Additional Analysis…..
In Additional Analysis Window, navigate to miscellaneous tab and check Data Carve. Click carving options to select the types of files to carve.
For this exercise, in order to save time, we only select GIF Files to perform date carving. In real cases, you should select all. Click "OK".

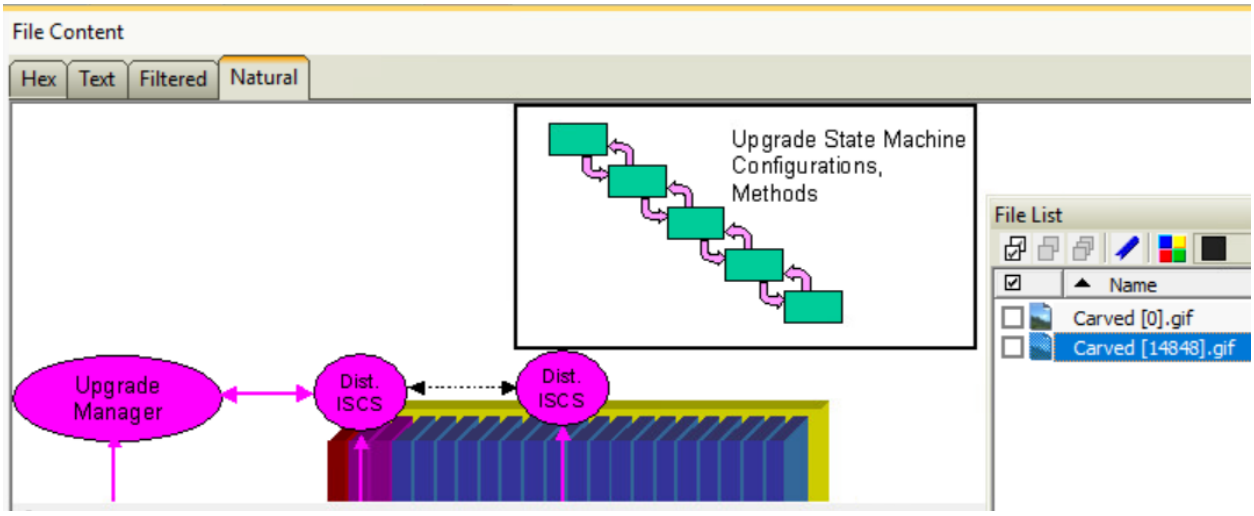
Click "OK" to perform carving. A "Data Processing Status" Window will pop-up to show you the status of this process. After this job is finished. Close the "Data Processing Status" Window.

Question 5: Check the number of Data Carved Files again, how many files added to the case by data carving? Now it has 2 files.



Question 6: What interesting files do you find by performing data carving process? Why is this process so important? After performing data carving process, we find two interested GIF files displayed in the content files as it shown it the below screenshots. The GIF files are about machine configuration and software testing. This process is important because it recovers the deleted or embedded files, and without this process, we won't be able to get those files.





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.

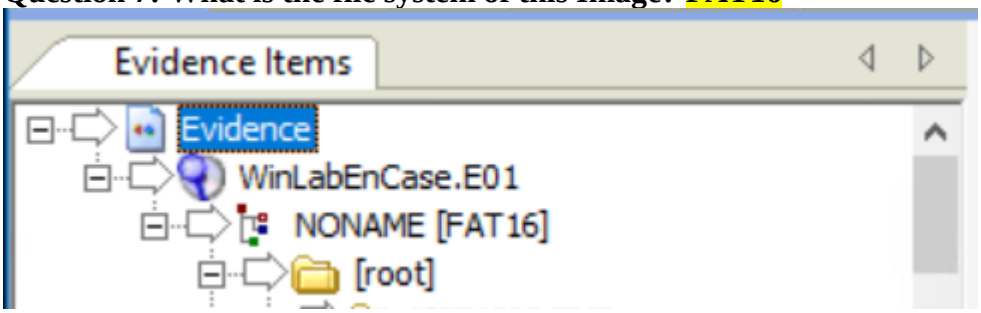
Explore Tab

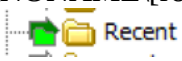
Click on **Explore** tab.

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

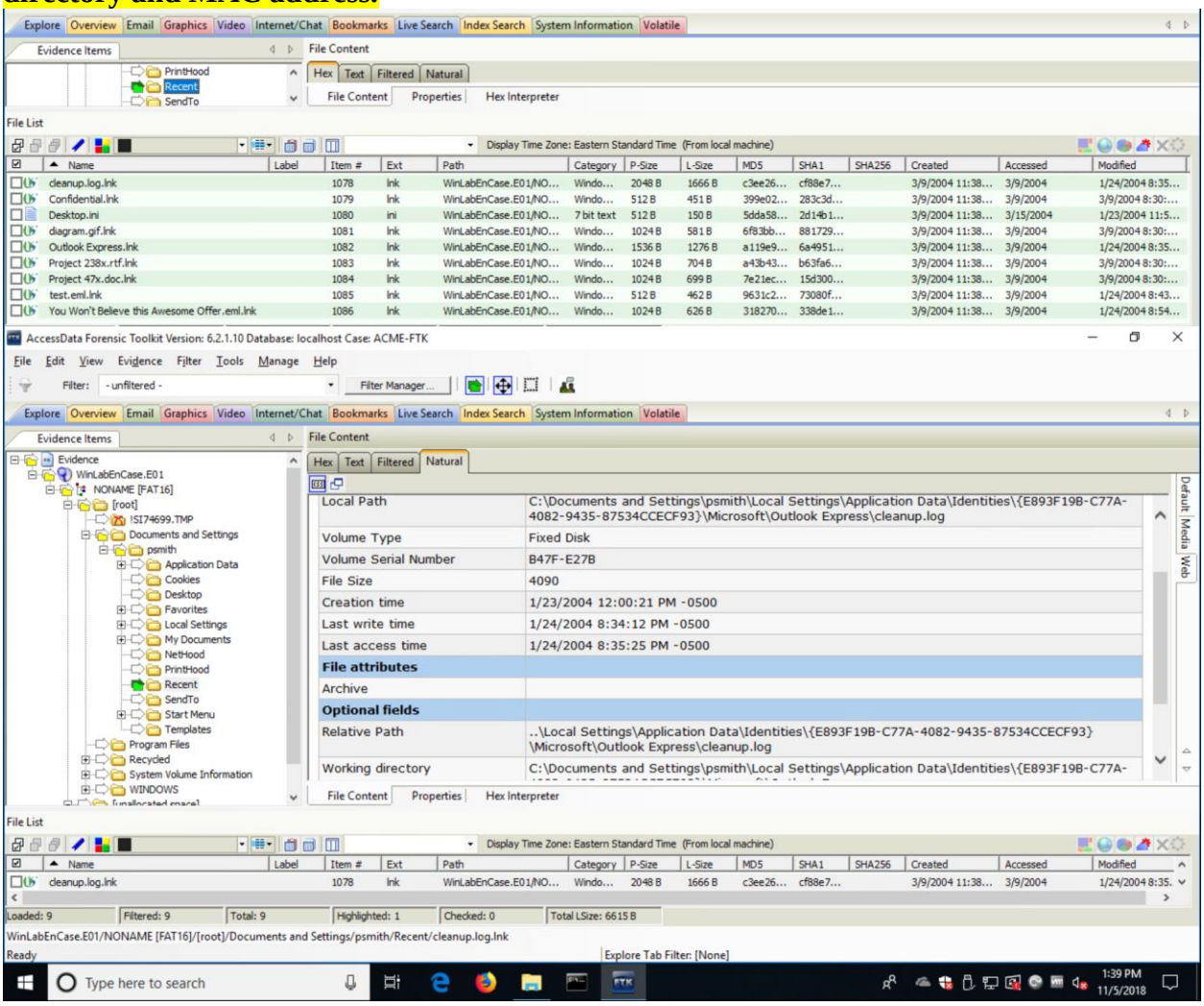
Question 7: What is the file system of this Image? FAT16



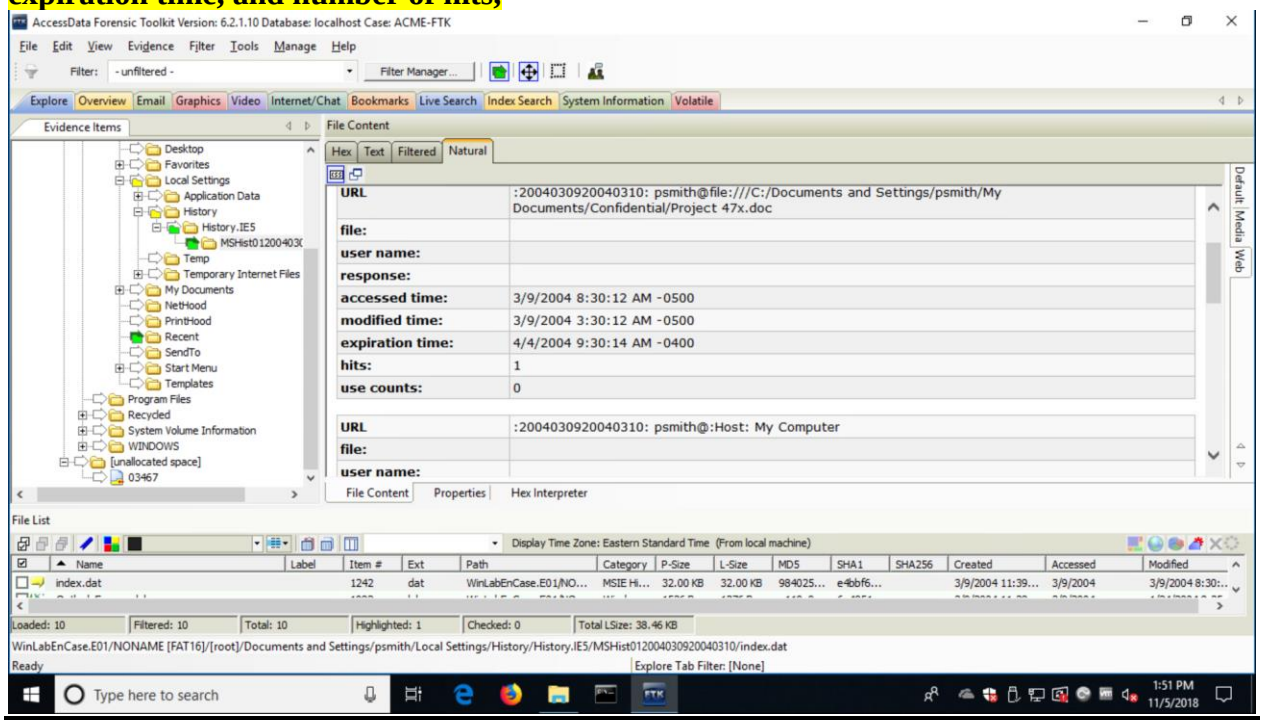
Expand WinLabEnCase.E01\NONAME\[root]\Documents and Settings\psmith\Recent, and green-select Recent folder 

. When you green-select a folder, the files and subdir in this folder will be listed in the bottom File List pane.

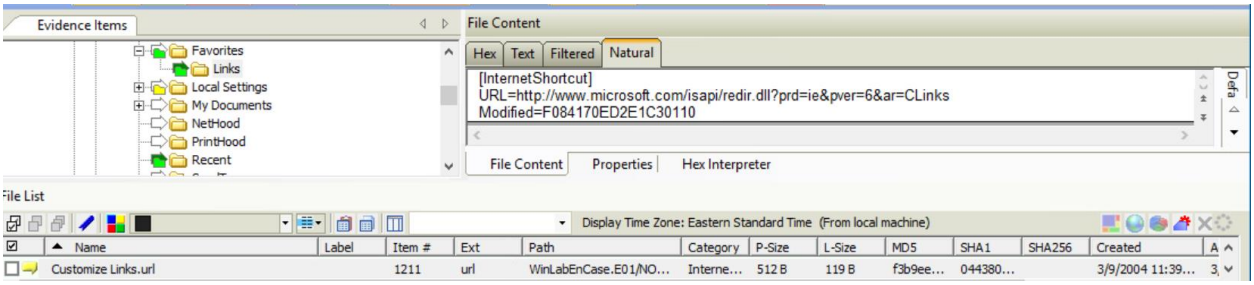
Question 8: Select Documents and Settings\psmith\Recent, what kind of files contain in this folder? Select one file in this folder, what kind of information do you get from the up-right window (File Content, Natural)? It has 9 files. One file has ini extension which is a plain text file, and the rest of the files have lnk extension which are shortcuts that point to different kind of files; for example, log, gif, rtf, doc and eml files. By selecting the first lnk file in the folder, cleanup.log.lnk, we can see from the file content a lot of useful information about the file. Such as, local path, file size, create and last access time, working directory and MAC address.

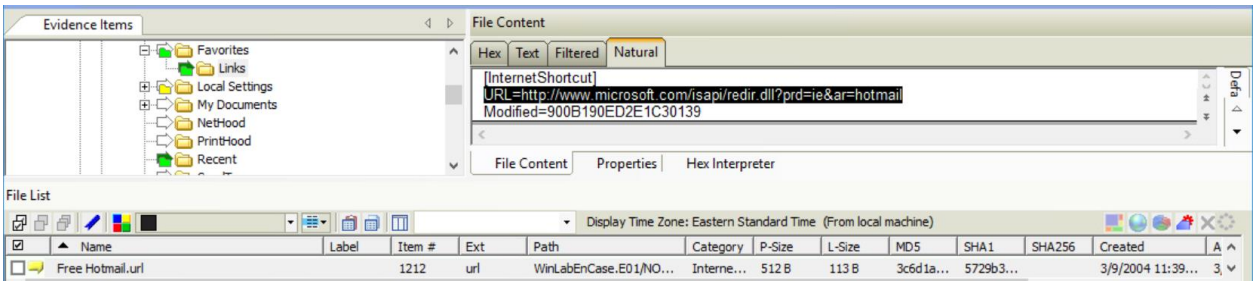


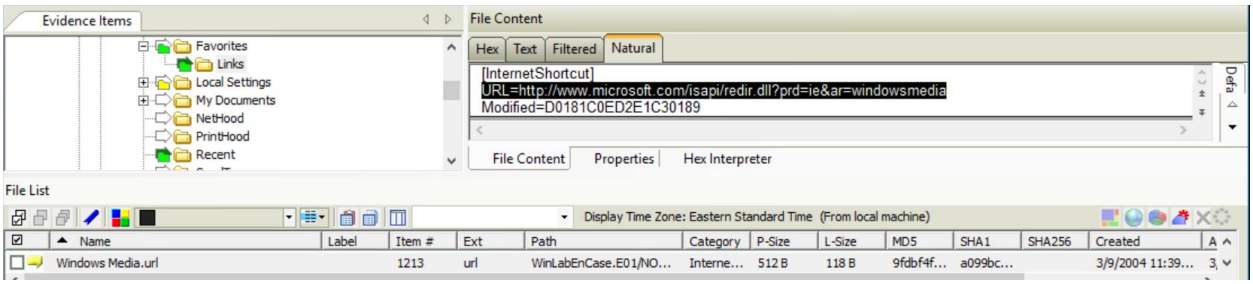
Question 9: Select Documents and Settings\psmith\Local Settings\History\History.IE5\index.dat, click "File Content" and "Natural" from the up-right window, what kind of information contain in this file? The file contains many useful information about IE history index. For example, URL, access time, modification time, expiration time, and number of hits,

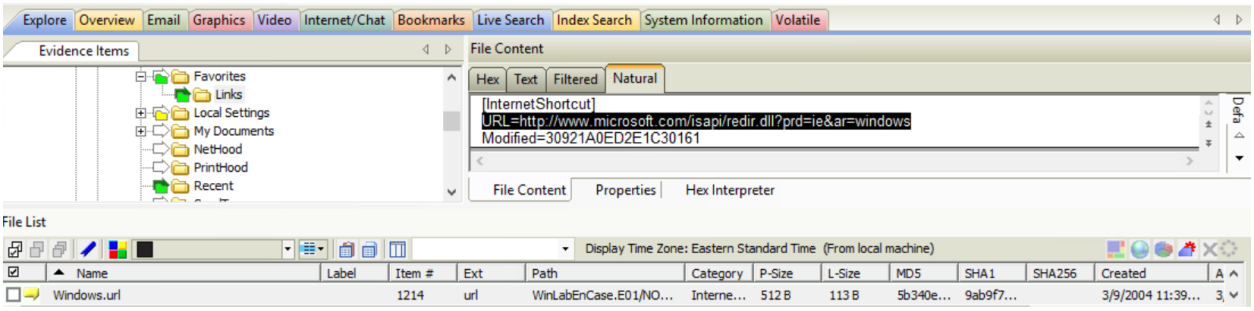


Question 10: Select Documents and Settings\psmith\Favorites, what are psmith's favorite links? There are 4 links in his favorite links: customize, free Hotmail, windows media and windows.

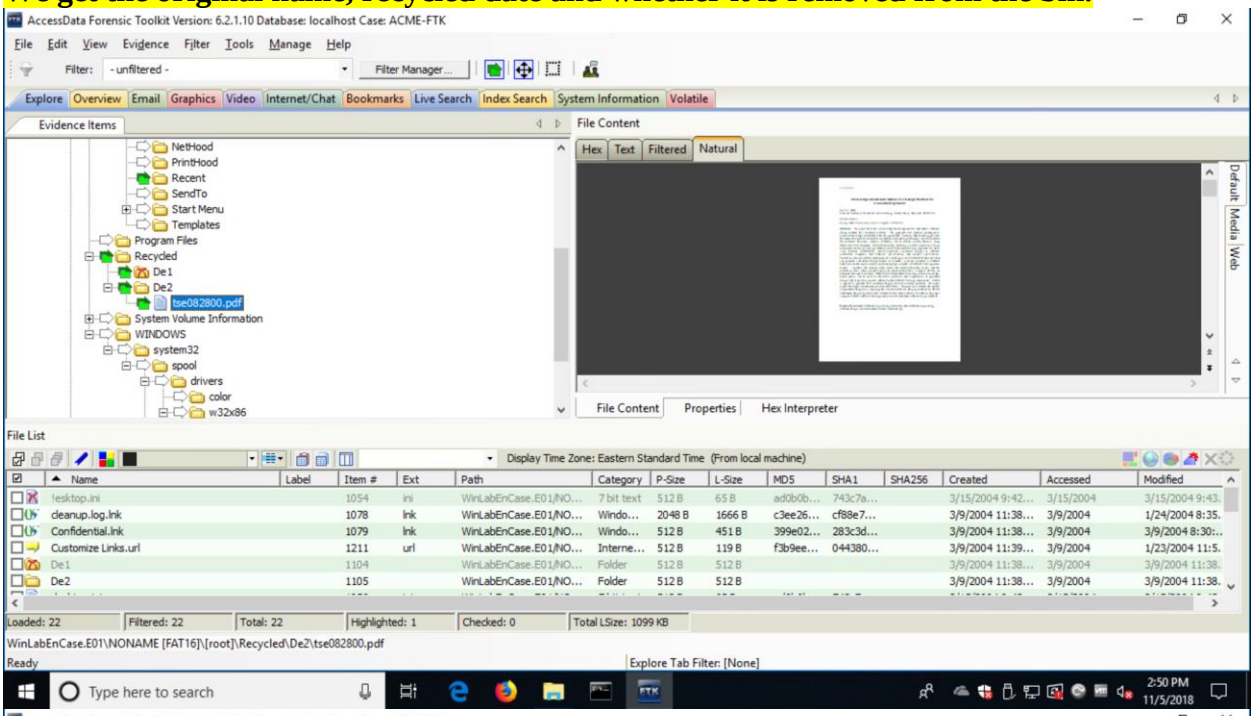


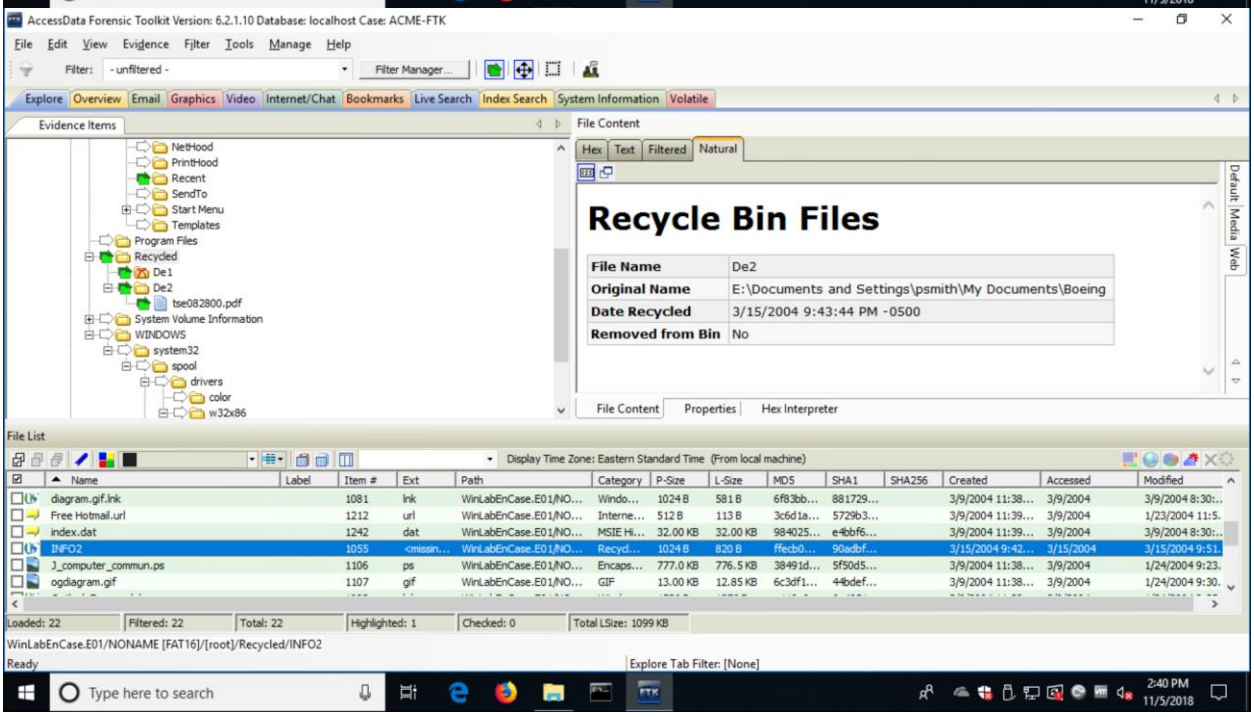






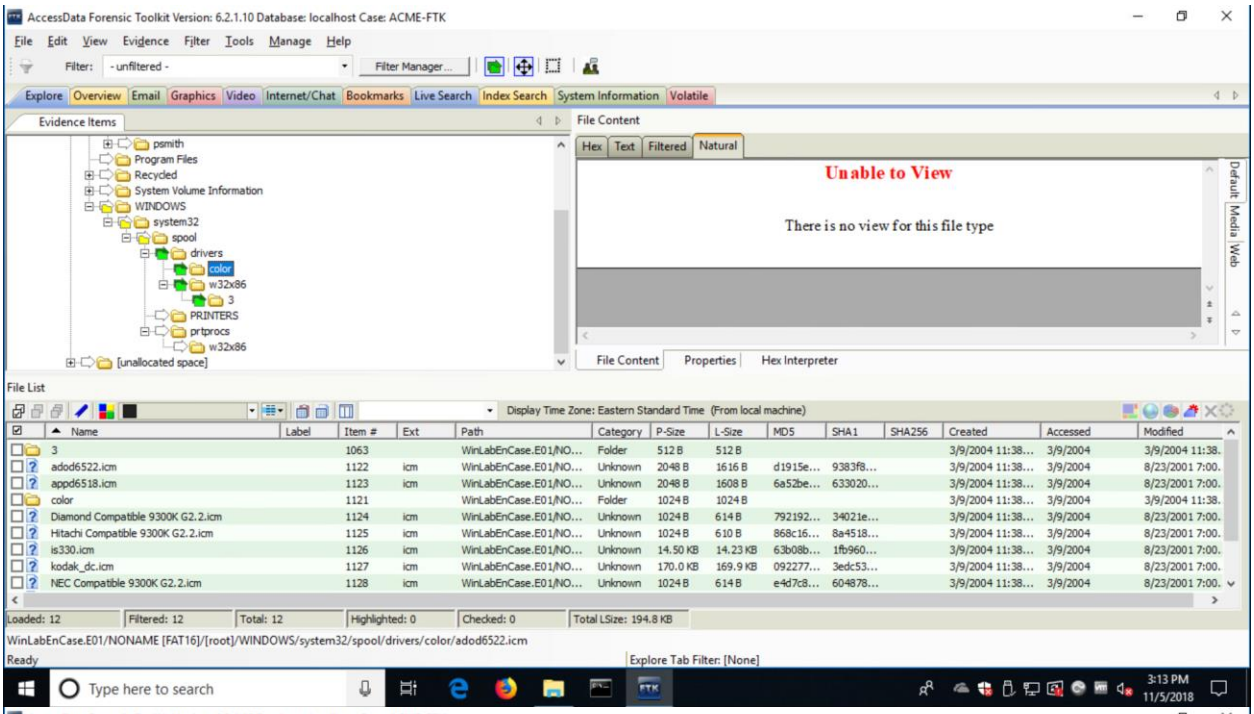
Question 11: Looking into the Recycled folder, which files are currently in the recycler? Select the INFO2 file from the Recycled folder, what information do you get from that file?
In the recycler, we can find tes082800.pdf file along with De1 and De2 folders.
We get the original name, recycled date and whether it is removed from the bin.

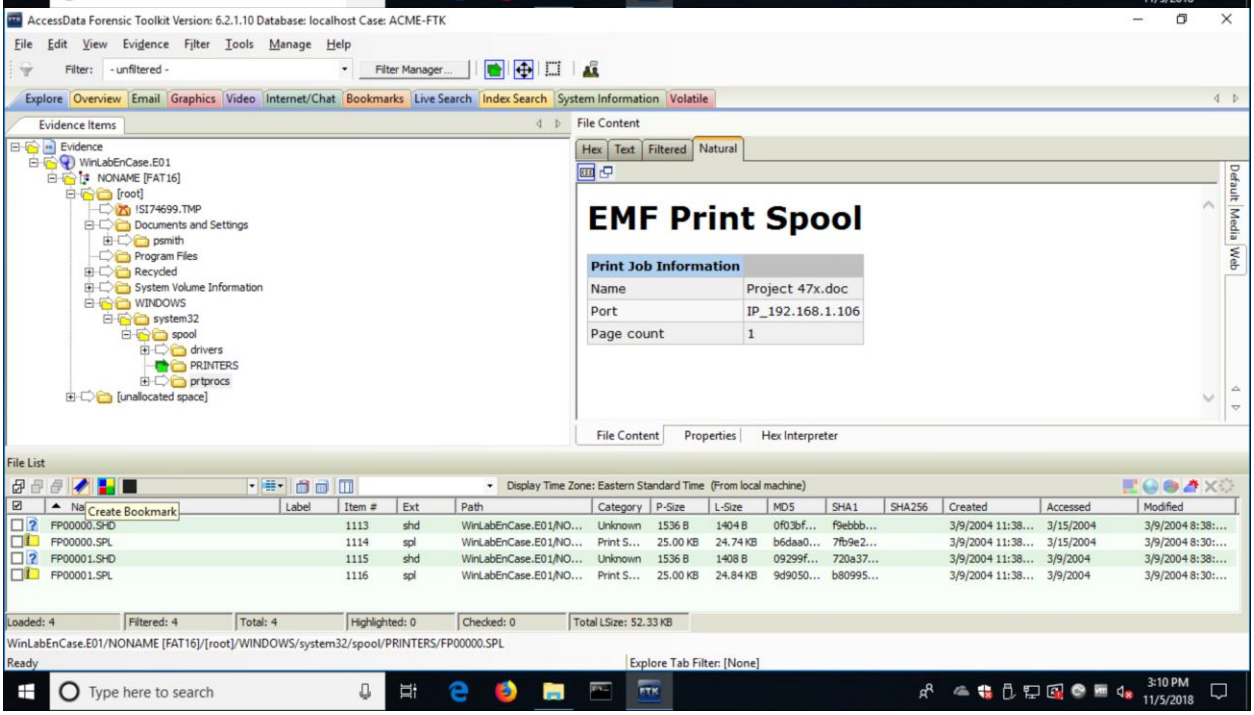




Question 12: Looking into WINDOWS\System32\spool folder, what information can you get from this folder?

Spool older have useful information about processing and printing. There are three folders inside the spool folder: drivers, printers and prtprocs. In the drivers folder, we have color and w32 subfolder. In the printing folder, we got the IP number.



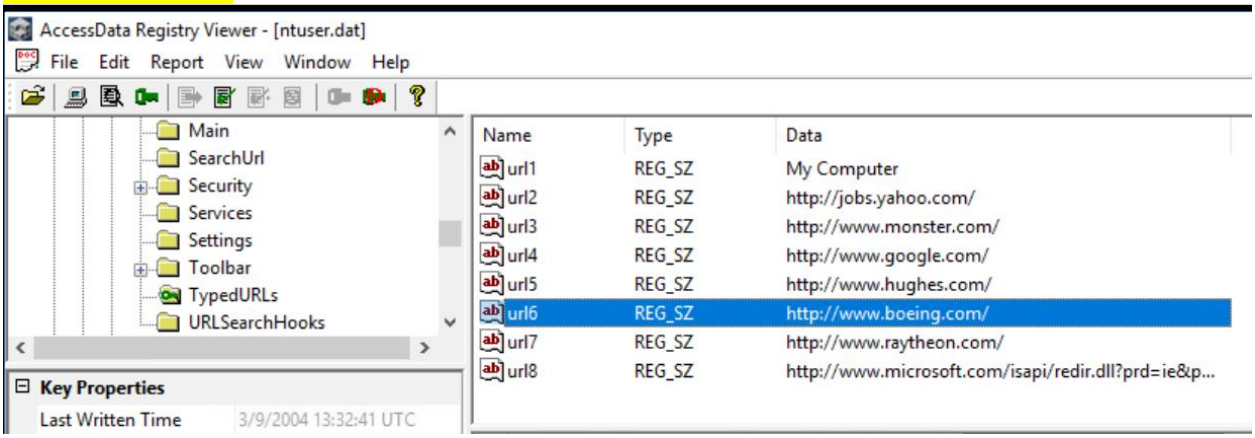


Windows Registry

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…

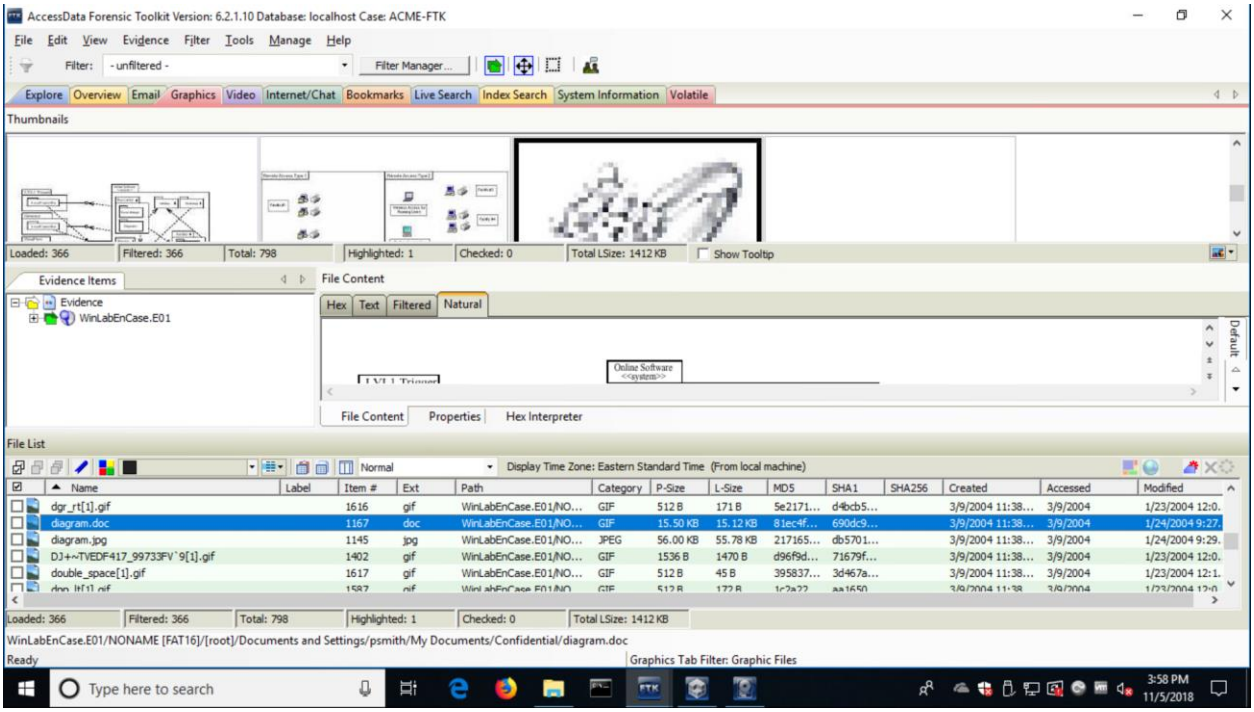
Question 13: Based on the values of the registry key TypedURL, which URLs did psmith search for ACME's competitor companies? List any other interesting results from ntuser.dat (if any). The result shows that Psmith search for competeror company like: boeing and Raytheon. He also searched jobs in yahoo, and was trying to find jobs using monster website.



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. Yes it will still be displayed in the gallery view. For example, we can see here diagram.doc which is non-graphics file but it still show in the Gallery.



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?
Export option will create a copy from the file and move that copy to the destination that the user choose while copy special will copy information (metadata) about specific file and then the user can paste this information in excel or other files.

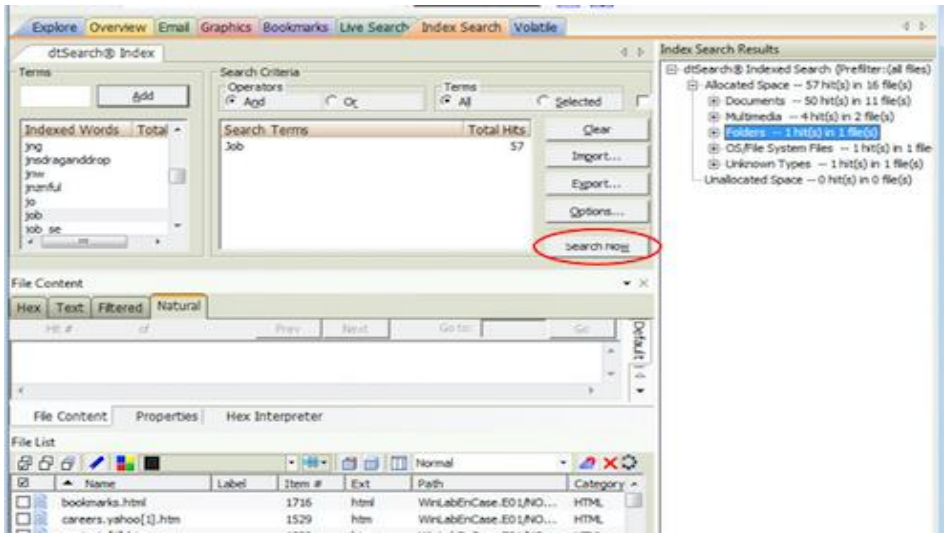
Keywords and Searching

Searching evidence for information pertaining to a case can be one of the most crucial steps in the examination. FTK support 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.

Click "Search Now". (If "Search Now" is hidden, you may have to pull the File Content pane down to see the "Search Now" button at the bottom of *dtSearch Index* pane.) (see the Figure below).



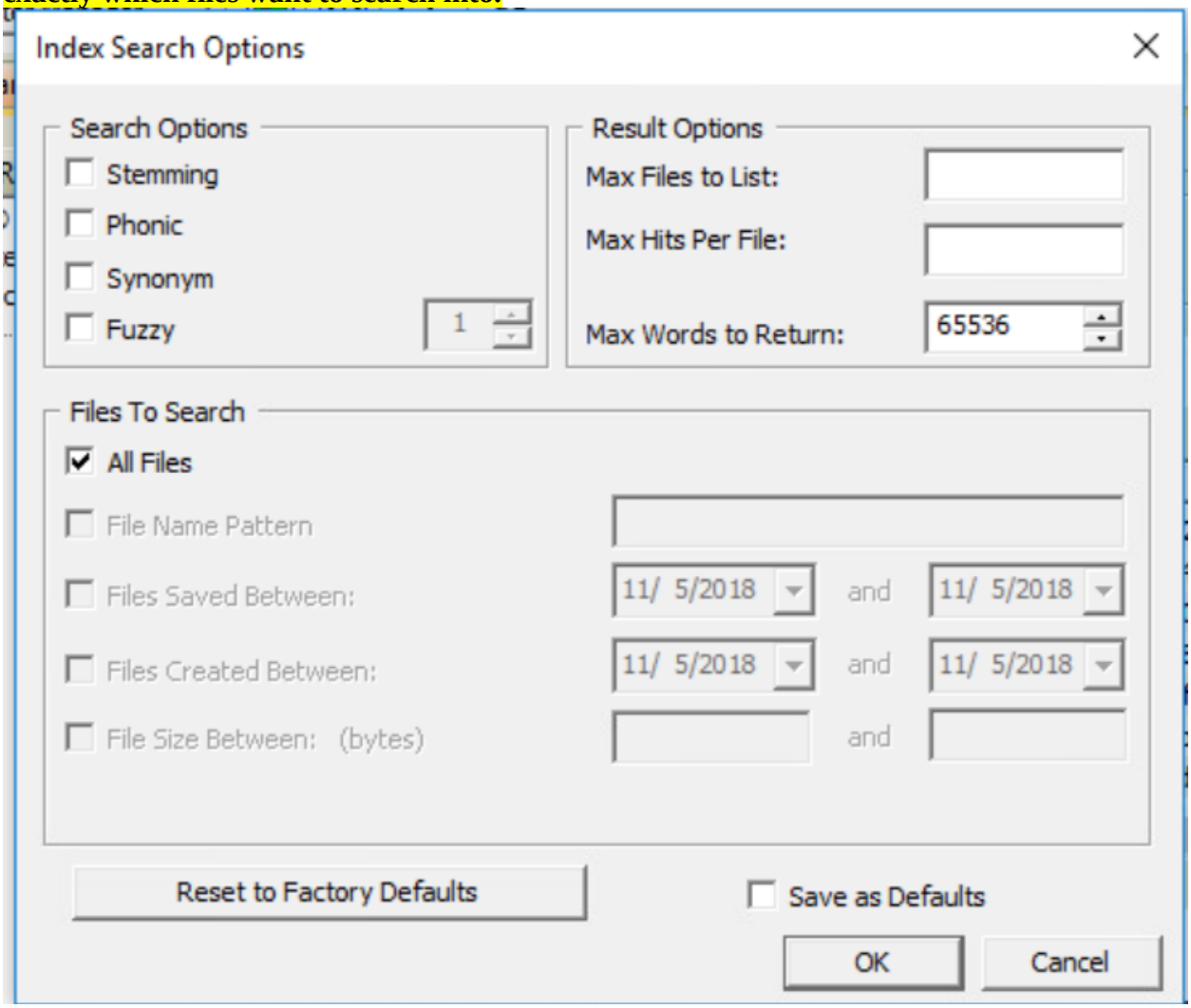
Check **Index Search Results** at the up-right pane and expand the search results.

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

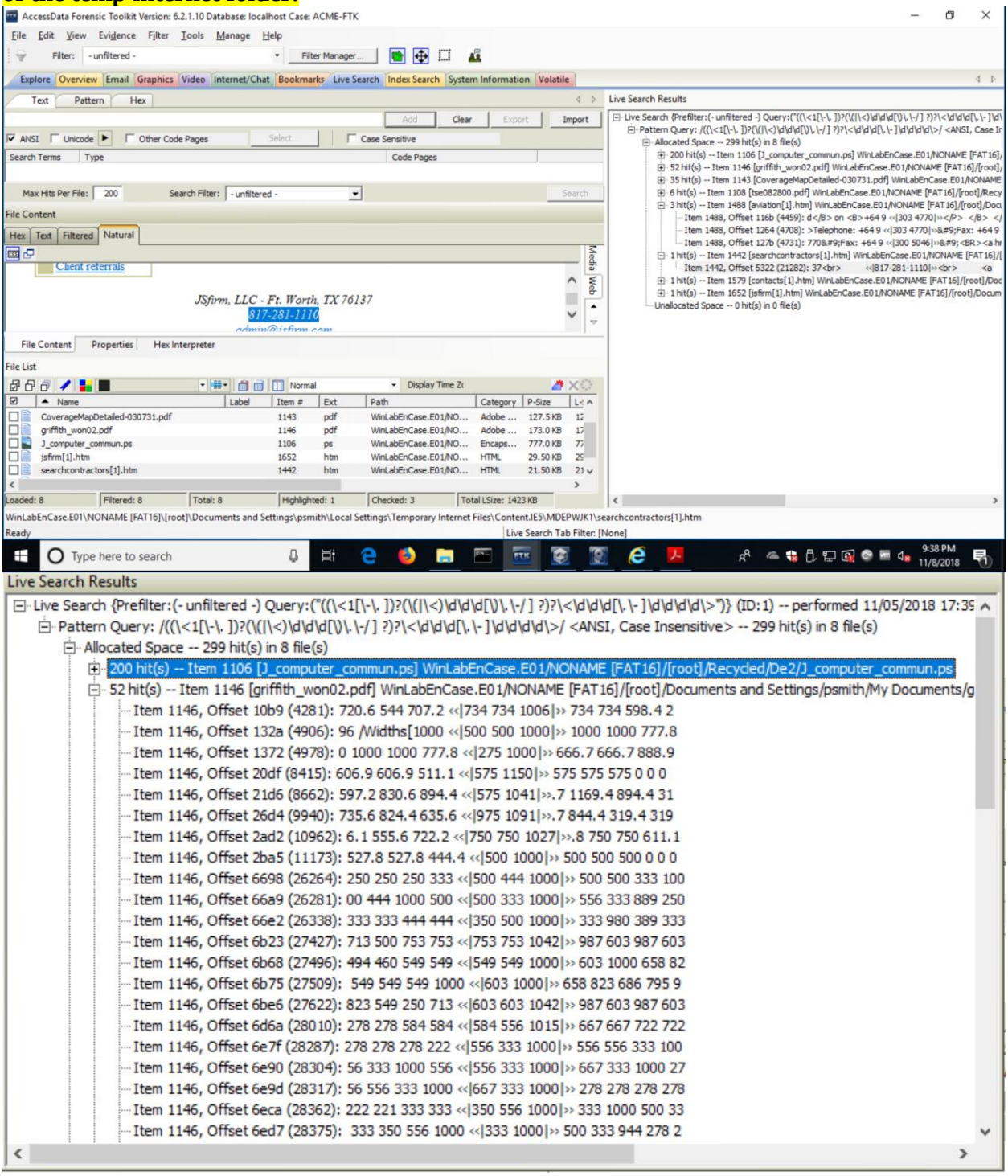
Question 16: What are these two features used for? ”Import” is to select some search term to import to the index research, and “options” is to refine the index search where user can choose different search options stemming-same root-, phonic -same sounds-, synonym -same meaning. Also, result options can set to maximum number, and the user can specify exactly which files want to search into.

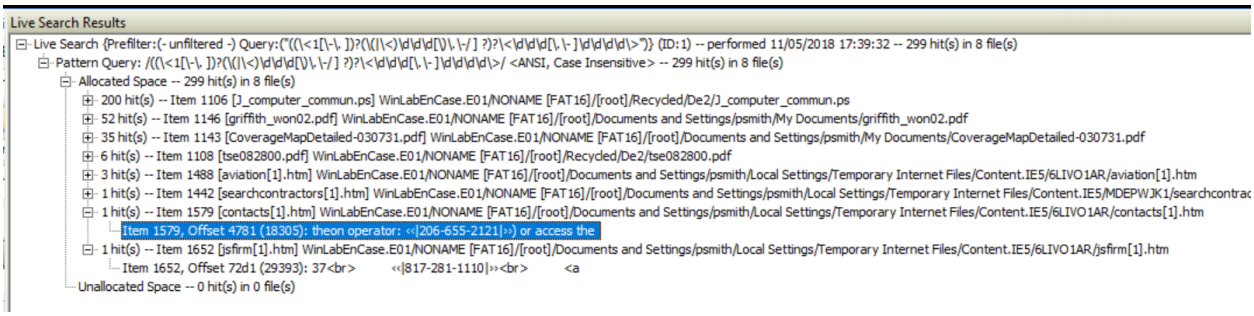


Click the **Live Search** tab**,** then choose **Pattern** tab.

Click the 2nd 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. Yes there are many files that contain US pgone number. Here are three examples: 817-281-1110, 734-734-1006 in psmith document folder and 206-655-2121 in one of the temp internet folder.





Question 18: What is the advantage to use indexed search vs. the live search? The **advantages of indexed search is fast and can search quickly gigabytes of text. Live search, on the other hand, has an advantage of comparing search term with the index file.**

Email

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

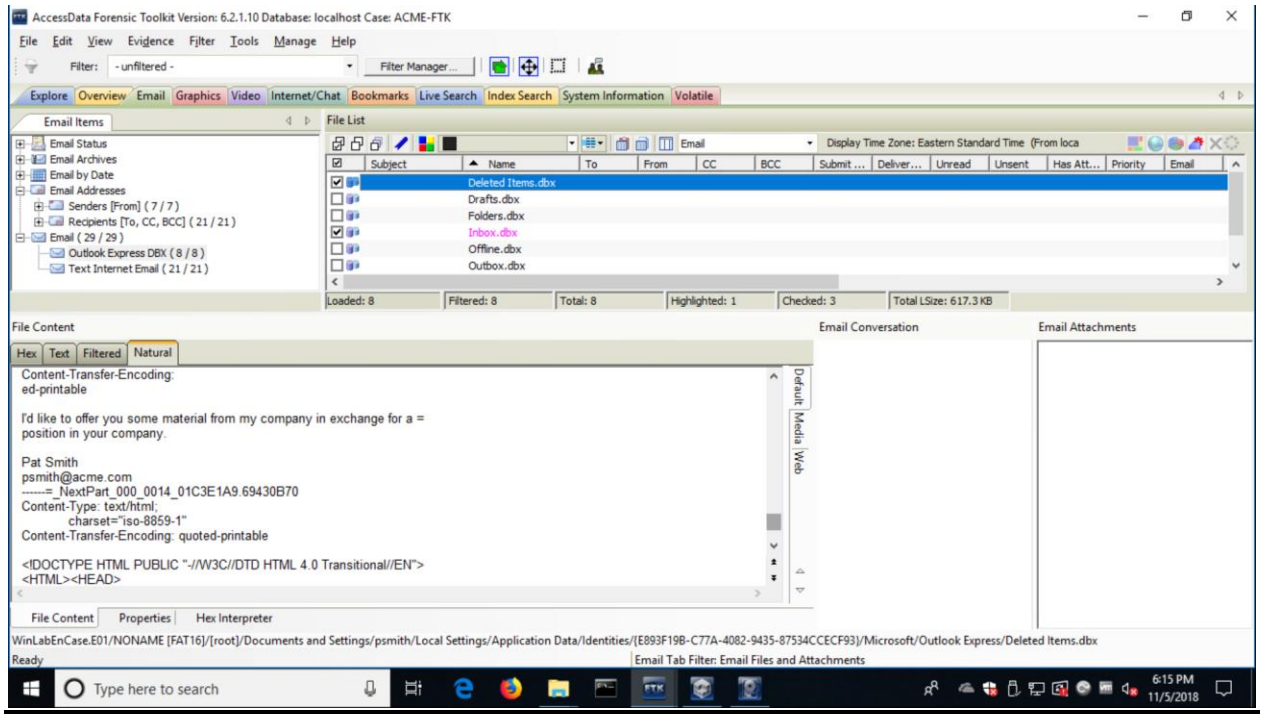
Question 19: Read the manual and find out what kind of email formats do FTK 6 support?

"The display is a coded HTML format"

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? Yes, we find an email from Pat Smith offering some material from the company to a competitor in exchange for a job.



<u>Step 3</u>: 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.

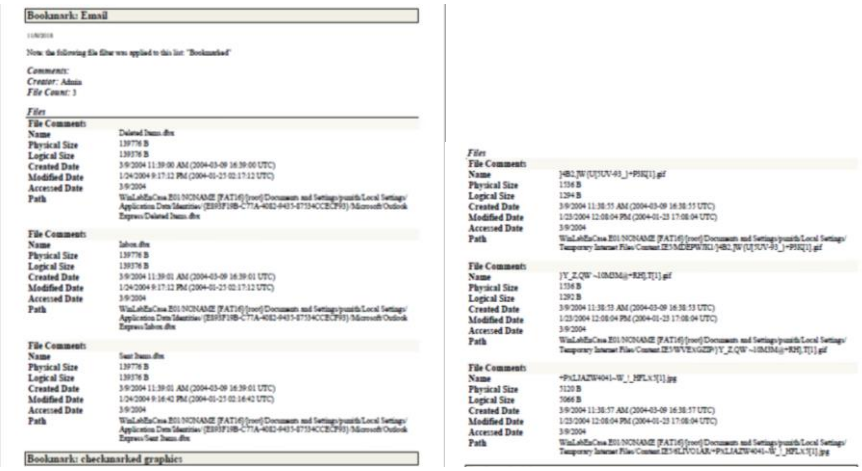
Question 21: Include two screenshots of this report in your submission.

Case Information

11/8/2018
Time zone for display: Eastern Standard Time

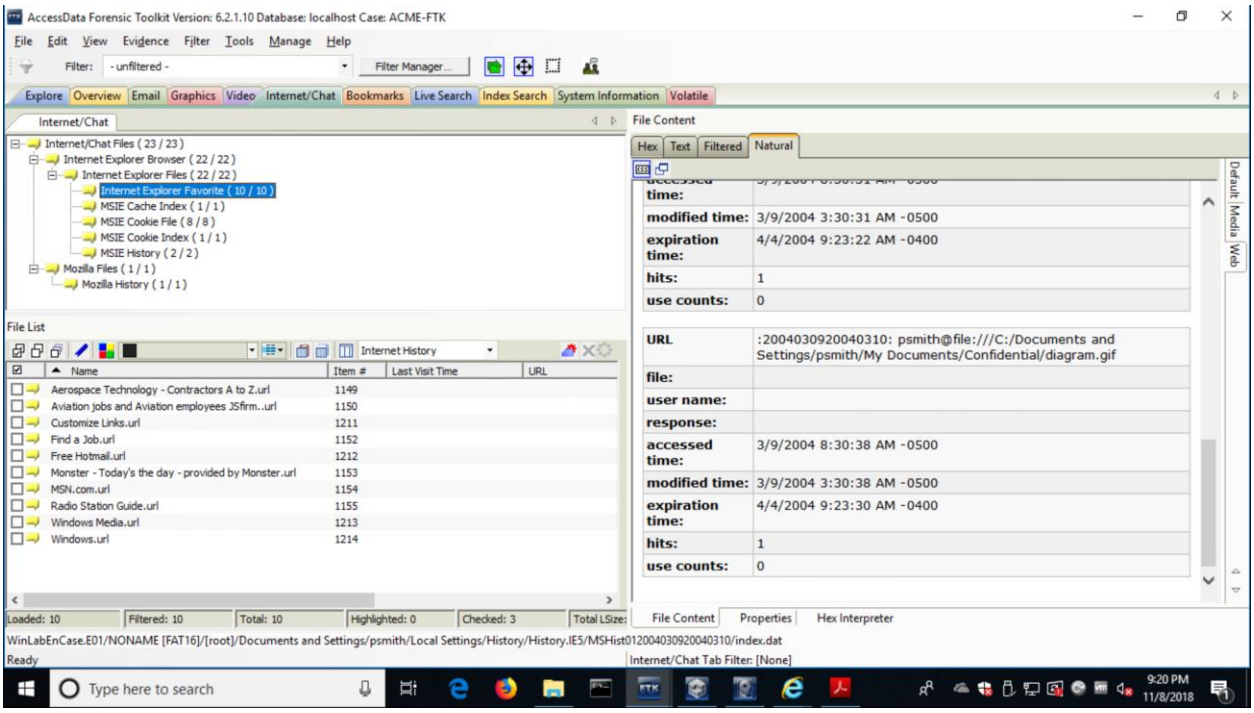
Version	AccessData Forensic Toolkit Version: 6.2.1.10
Case Owner	Admin
Case Name	ACME-FTK
Case Reference	
Case Description	
Report Created	11/8/2018 4:36:22 PM

Agency/Company	ACME Company
Investigator's Name	Sumayyah
Address	
Phone	
Fax	
Email	
Comments	



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.

One feature FTK that can be used to support this case is: Internet/chat. As we can see from the screeshot below that Psmith used online chat in some websites (ex: monistor.com) to find a job in a competitor company. Also, This feature shows that Psmith used MSN.com to communicate, so we can check the chat history to find out more information.


AccessData Forensic Toolkit Version: 6.2.1.10 Database: localhost Case: ACME-FTK
File Edit View Evidence Filter Tools Manage Help
Filter: - unfiltered -
Filter Manager...
Explore Overview Email Graphics Video Internet/Chat Bookmarks Live Search Index Search System Information Volatile
Internet/Chat
Internet/Chat Files (23 / 23)
Internet Explorer Browser (22 / 22)
Internet Explorer Files (22 / 22)
Internet Explorer Favorite (10 / 10)
MSIE Cache Index (1 / 1)
MSIE Cookie File (8 / 8)
MSIE Cookie Index (1 / 1)
MSIE History (2 / 2)
Mozilla Files (1 / 1)
Mozilla History (1 / 1)
File List
Internet History
Name Item # Last Visit Time URL
Aerospace Technology - Contractors A to Z.url 1149
Aviation jobs and Aviation employees JSfirm..url 1150
Customize Links.url 1211
Find a Job.url 1152
Free Hotmail.url 1212
Monster - Today's the day - provided by Monster.url 1153
MSN.com.url 1154
Radio Station Guide.url 1155
Windows Media.url 1213
Windows.url 1214
Loaded: 10 Filtered: 10 Total: 10 Highlighted: 0 Checked: 3 Total LSize:
File Content
Hex Text Filtered Natural
modified time: 3/9/2004 3:30:31 AM -0500
expiration time: 4/4/2004 9:23:22 AM -0400
hits: 1
use counts: 0
URL :2004030920040310: psmith@file:///C:/Documents and Settings/psmith/My Documents/Confidential/diagram.gif
file:
user name:
response:
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
hits: 1
use counts: 0
File Content Properties Hex Interpreter
WinLabEnCase.E01/NONAME [FAT16]/[root]/Documents and Settings/psmith/Local Settings/History/History.IE5/MSHist012004030920040310/index.dat
Ready
Internet/Chat Tab Filter: [None]
Type here to search
9:20 PM
11/8/2018