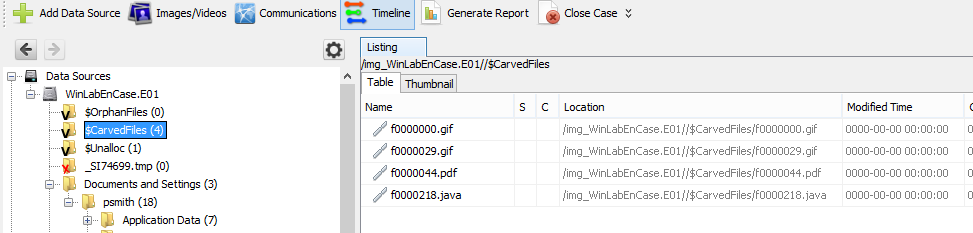
Lab #5: Marco Seman & Jason Lu

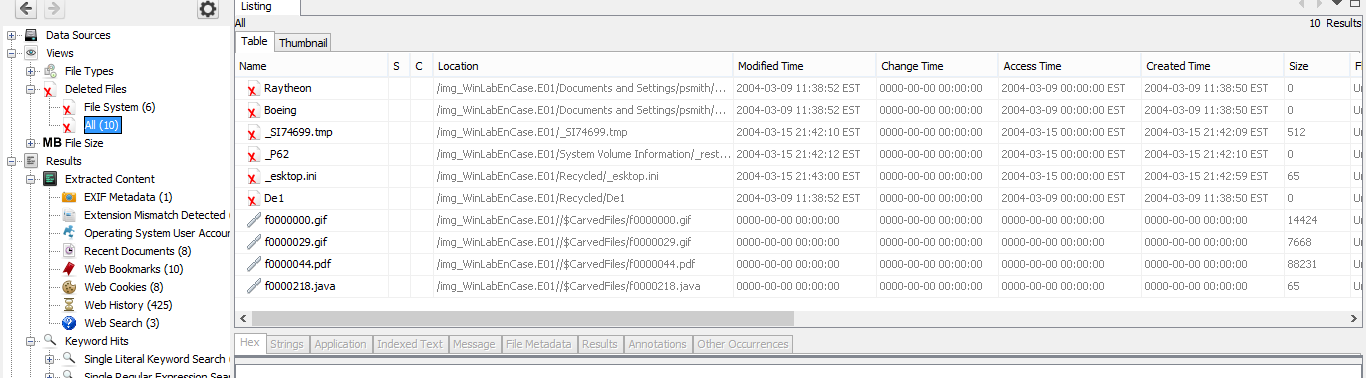
1. Data carving is the process of extracting files and objects that have been deleted or are Embedded in other files. Check under Data Sources > WinLabEnCase.E01> $CarvedFiles. How many embedded files did Autopsy extract by performing the data carving process? List all the files.

Autopsy carved out 4 files f00000000.gif, f0000029.gif, f0000044.pdf, f0000218.java

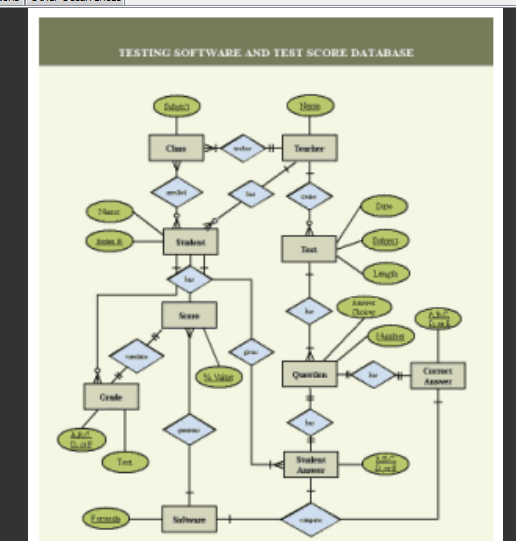
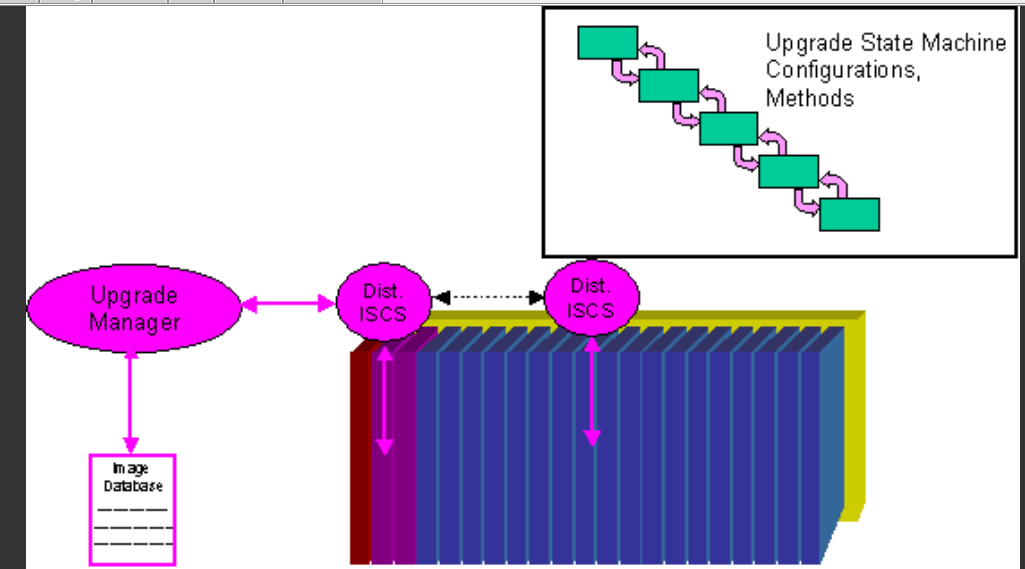


B)

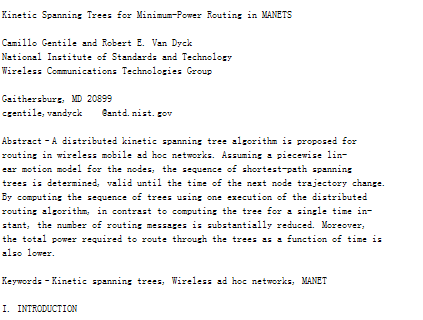
Both company name **Raytheon** and **Boeing** had been found under deleted files



The **TESTING SOFTWARE AND TEST SCORE DATABASE** flowchart and **Upgrade State Machine Configurations, Methods** are also found under deleted files



A PDF file named **“Kinetic Spanning Trees for Minimum-Power Routing in MANFTS”** are also found under deleted files



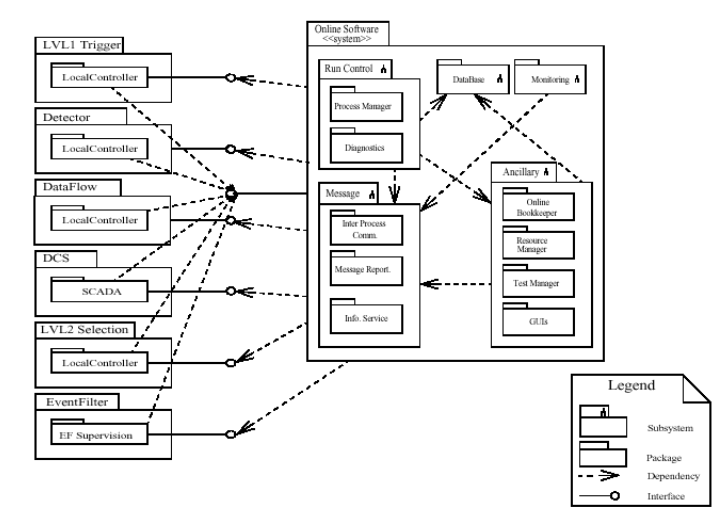
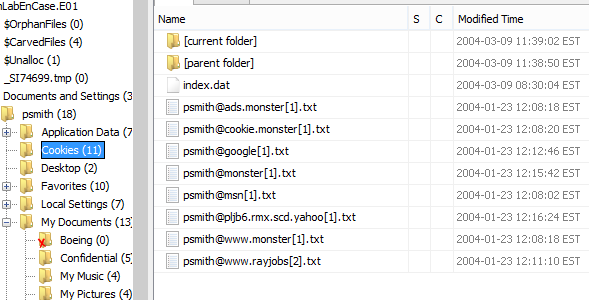
C) This original extension of this file is image/gif 

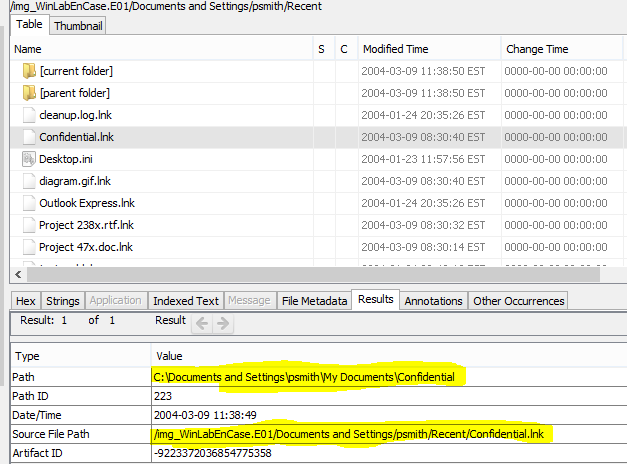
Image is also located at:

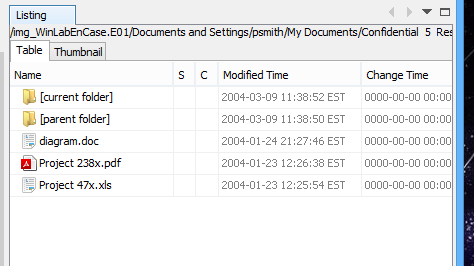
|  |  |
| --- | --- |
|  | /img\_WinLabEnCase.E01/Documents and Settings/psmith/My Documents/Confidential/diagram.doc |

D) Sites that stored cookies on Psmith's machine includes msn.com, google.com. Monster.com, rayjobs.com, and yahoo.com



E)The source file links to C:\Documents and Settings\psmith\My Documents\Confidential

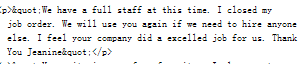




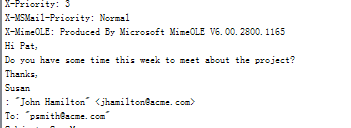
F)

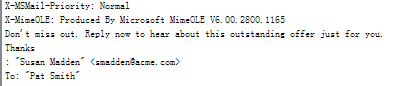
A great number of “AwesomeOffers” has been detected under the [bconrad@raytheon.com](mailto:bconrad@raytheon.com)

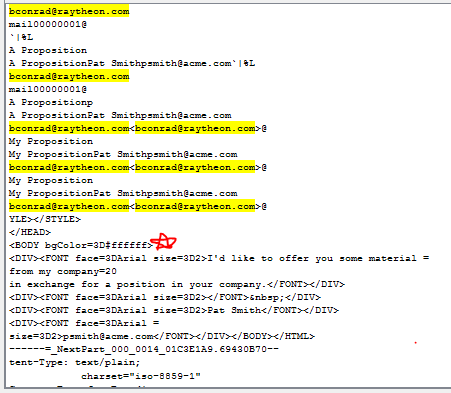
Several

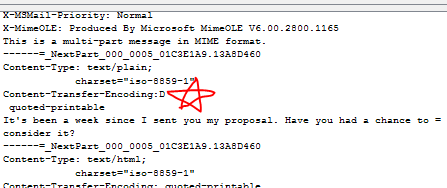


* Possible attempting to leak company information, [day@jsfirm.com](mailto:day@jsfirm.com)

 Possible leakage of trade secrets

Job Offer





It looks like Pam Smith was in discussions with bconrad at raytheon. Psmith was offering some of her company’s materials in exchange for a job position at raytheon. This seems to show that psmith was selling her company’s goods in exchange for a job with another company.

For the fifth lab, we learned how to investigate user information from an .E01 file using Autopsy. Using Autospy, we learned about how effective Autopsy is where it views the contents of a HDD and decompositions the information such as the views, results, and file directories. Autopsy also is able to view the files that were deleted by the user and not overwritten. Autopsy shows the contents of every file as well as their directory location. What was most interesting that we learned in this lab was the ability to view the emails that the user has sent as well as the contents of the message. Another interesting feature from Autopsy that we learned is the option to view only Images/Videos where the software displays the content location of only the images as well as the ones that were recycled.