Objectives:

- Use Nirsoft's BrowsingHistoryView to Parse Internet History Files
- Determine if the victim's Internet History indicates criminal activity or an attack vector.

1. Open Access Data's FTK Imager 3
2. Mount the Suspect image (File > Image Mounting > Select the suspect image file)
3. Install / Open Nirsoft's BrowsingHistoryView. **(If you are using Windows 7 or Vista be sure to right-click and select *Run as Administrator*)**
    a. In the *Advanced Options* box note the *Filter by visit date/time* box and select *Load History Items from any time.*
    b. Leave all Web Browsers checked.
    c. Under the *Load history from..* option select: *Load history from the specified profile (For example: c:\users\admin)*
    d. In the next box, click the box with three dots to open the Windows navigation browser and navigate to your mounted suspect image and the folder *Documents and settings**Owner*.
    e. Click *OK*.
4. You can sort by any of the header bars. You can also search for terms by clicking *Edit > Find*.
5. What Internet browser's did this profile use?

_____

6. Find the terms “search, google search, bing”. This will give you an idea of what kind of terms the suspect searched for on the Internet. What search terms did the suspect search for that might be of interest to this investigation? What Search engine did he use? What was the time / date?

_____

_____

_____

   a. Did the user have webmail? What was his email address?

= _____

   b. Search for the term “file:///”. This will show the file’s that were accessed on the local system but were logged in the Index.dat file. **%20 indicate a space** Are there any files relevant to this investigation?

= _____

_____

_____

   c. Were any of the relevant files mentioned above in a location other than the computers C:/ drive? What were their names?

_____

d. This computer is believed to be the victim of a malware attack. Can you confirm or deny this, based on your Internet Analysis? If it did occur, what was the name of the malware and where did it come from?