5 Lab Manual – Search (Index & Live)

In this set of exercises you will gain experience using FTK to search files within an image files or set of folders. For the analysis you will be using the items on FTK's Search tab.

5.1 Index Search Exercises

The following exercises all use the image **String Search Practice 1.ad1**. Copy this folder to your computer, open it in FTK, and find the files containing the specified strings. You don't need to build a report for these exercises, just find the files.

5.1.1 Simple and Compound Index Search

A. Find the files that contain word `Bulgaria`

B. Find the files that contain word `hacker`

C. Doing a compound search. Find the files that contain ***both*** `Bulgaria` and `hacker`

5.1.2 Index Search Using Imported Word List

Find the files that contain any of the words in the file "Ring Names.txt". Use that information to answer the following questions.

A. Which elf is suspected of being a "plant"?

B. Which elf has an email address and what is it?

C. Which elves have been used previously for finding "stuff"?

5.2 Live Search Exercises

These exercises provide you with experience in using the Live Search option in FTK. The exercises all use the folder **String Search Practice 1.ad1**, which is the same image used in the previous exercises. You don't need to build a report for these exercises, just find the files.

5.2.1 Pattern Search – Text Pattern

Find the files that contains the pattern "`hungry like a wolf`". Note – you could find this pattern by doing a compound search, but try to use the pattern search instead.

5.2.2 PATTERN SEARCH – REGULAR EXPRESSIONS

A. Find the files with phones numbers. The area code may or may not be enclosed in parentheses. For example, either (405) 544-5444 or 405 544-5444 should be found.

B. Doing a pattern search. Find the files containing a MAC address. These are 6 sets of 2 digit hex numbers that use either a : or a dash as a delimiter. For example:

`4D:44:D2:65:8A:76` or `4D-44-D2-65-8A-76`

Also note that the hex digits may be either upper or lower case. So the following strings would also be valid MAC addresses:

`4d:44:d2:65:8a:76` or `4d-44-d2-65-8a-76`

Remember that it's often easier to use the built-in FTK regular expressions or look up regular expressions on the Internet than it is to write your own.

5.3 SEARCH AND ANALYSIS EXERCISES

This set of exercises provides you with more experience searching an image for evidence.

5.3.1 WHAT THE FLUX?

You have been hired by Doc Brown & Associates to investigate an employee. They believe that the suspect is stealing information about the flux capacitor sharing it with their competitors.

The image file for this investigation is **btf delorean.ad1**. Use FTK to perform your analysis, bookmark files you think should be included as evidence, and build your report.

Hint 1 – During your analysis you should look at the easy things first, like looking at graphics; and then move to looking for the words `flux` and/or `capacitor` within files. In other words, start on the Overview Tab in FTK, then move to the Search Tab.

Hint 2 – There are 5 images and 4 documents.

Bonus Points – Explain why the Index Search results show more than 4 documents that contain the words `flux` and `capacitor`.

THE CASE OF THE HARD TARGET

You have been hired by the Secret Service to search a computer for evidence of a gang hit or assassination attempt. Their ultimate goal is to discover who the intended victim is, where the attempt will take place and who is funding the crime. The only thing you have been given to work with is the disk image **hard target.ad1** and a list of currently known hit men. This list is in the file **known assassins list.txt**.

Use this information to answer the following questions:

A. Who is the target of the proposed hit?
B. Where will the hit take place?
C. Who is funding the hit?

Hint – First find files with the any of the assassin's names in them. Inspect the files closely, and also look at any other files in the folders where these documents are located. You're going to have to actually read the contents of the files to answer the questions.