Keyword Search and Analysis

For this lab we are looking into how to use keyword searches to help analyze data. The amount of data we have on a single piece of technology is large enough that having to search for specifics by hand would take hours or even days depending on the stored amount of data. By using the keyword search we are able to find the essential data faster and we can make sure nothing has been overlooked.

To start this lab, we will use Autopsy to be able to search using the keywords. After launching the virtual machine, we are taken through the application menu to Autopsy under computer forensics. We create a new case where we fill in the information needed such as case name and number while leaving the base directory alone. After this in the Add Data Source window we choose data image or VM file. When selecting the data we will follow the path home, csi, desktop, evidence files, FOR\_LAB\_006, and open FOR\_LAB\_006.E01 for the data. We move on to the configure ingest module we unselect all then check the keyword search and uncheck the keyword lists, clicking on global settings. Moving on to the String Extraction, we highlight enable optical character recognition then we turn to the general tab and then back to lists where we create a new list. With this new list, we create new keywords typing in the given words and setting the search type to exact match. A new search term is created using hack and the substring match as well. A third keyword is made with the same process using hack\* and setting this one to regular expression. Moving back to the Add Data Source, we check the new keywork list we created then finish the Add Data Source process. Back at the Autopsy main window we can see the keyword search run and analyze the files from our selected data. The Ingest Message feature shows the hits of the keyword search. We click the pin next to our keyword hits keyword lists to see the table of hits. We can move on to the different key word types we created in the list and look at the specifics to see which ones were substrings, regular expressions, and exact matches. We can look at the hits and fins their location within the file being shown on the view panel. Moving on, we use the keyword search above the table to find the files indexed and we can use this to search these files like the way we created the keyword lists using the three types and the keyword to use. Then we compare the new results and can double check through the folder.

Keywords are something that I find I use almost every day whether its reading or trying to find a video to watch. At a time I got so used to the keyword search on the computer that my mind tried to tell me to use the search when I was holding a reference book. This lab was interesting as it took a topic that is used in everyday life and showed how it can be applied to digital forensics. Imagining having to look through each file without being able to do a directory keyword search makes me feel stressed so I can’t imagine how people doing that would feel. I find that autopsy becomes more interesting with each lab we work on as it shows just how much this one application can do and the amount of time and energy it saves completing the tasks.

Section 2 Step 32 Output – hackerstream did not appear in the list for mine so I went with the one that only had 1 appearance.

A screenshot of a computer

Description automatically generated

Section 2 Step 35 Output

A screenshot of a computer

Description automatically generated