CCSI 410 Forensic Lab Report

1) Investigator’s Name: \_Matt Ferry\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

2) Date of Investigation:08/04/2013 \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

3) Lab Number and Title: Lab 4: Keyword & Statistical Searching

4) Summary of Findings:

Performed the required steps for Lab 4, and answered the required questions. Due to the number of search results and hits received through the keyword searches(71 hits 20 files for individual keyword searchs, 13 hits 6 files for bob and manuel) there is enough evidence to indicate that this investigation should be continued.

5) Details of Investigation

Thursday, 08/01/2013

 3:02 PM: Determined Keyword List:

 **Bid AND fraud\***

 **Bid OR fraud\***

 **Acuerdo\* AND agree\***

 **Acuerdo\* OR agree\***

 **Bid\* AND money**

 **Bid\* OR Money**

 **Sub\***

 **profit**

 **stipulation**

 **account**

 **turn**

 **contract**

U.S. Department of Homeland Security, 03/22/05, 11/08/05\*

 Estado Libre y Soberano de Chihuahua, Mexico, 04/19/05\*, 07/14/05

 U.S. Department of Housing and Urban Development, 01/31/05, 06/08/05\*

 Ciudad Juarez, Mexico, 09/12/05

 Laredo, TX, 02/10/05, 08/29/05, 10/04/05

 Havens, New Mexico, 09/28/05\*, 12/03/05

 Tucson, Arizona, 02/28/05\*, 05/27/05

 Estado Libre y Soberano de Baja California, Mexico, 03/06/05

 U.S. Immigration and Customs Enforcement, 01/05/05, 05/18/05

 3:12 PM: Logged into Lab Environment

 3:18 PM: Created Case File, and added the provided floppy image file for the investigation.

 3:20 PM: Added Keywords to the Search utility

 3:37 PM: Per Step 4 of the Assignment instructions answering question 3.

 3:45 PM: Noting that the floppy.001 image file that is available in this lab assignment’s F: (which is the only image file that I have been able to find), there are absolutely NO email files or other **addressbook.csv files that I should be seeing. Emailing the professor regarding this issue to verify that this lab is loading the correct lab assignment.**

 **7:23 PM: Per the response to my email to the professor, changing the file to be examined to Lab6 floppy image.IMA.**

 **7:24 PM: Logged back into the lab environment, and starting the investigation process over again.**

 **7:29 PM: Setup of Case completed, and set Indexing option to full indexing. Re-Indexed the evidence.**

 7:47 PM: Initial look at .eml files and addressbook.csv file complete moving on to a more thorough search using keywords.

 8:50 PM: Completed in depth Keyword search and collecting of data, beginning to compile the report. (See below for keyword results)

 9:30 PM: Completed Initial draft of report, Summary still needs to be completed.

Sunday, 08/04/2013

 1:20 PM: Filled out the Report Summary

6) Please type the answers to the questions found throughout the lab here.

**Question 1:  What is the definition of bid rigging? Give the URL from where you got your answer. As part of your answer list and define three common bid rigging practices.**

**Bid rigging is the act of “rigging” a bid for a contract so that a specific contractor will win the bid.**

<http://en.wikipedia.org/wiki/Bid_rigging> & <http://www.investopedia.com/terms/b/bid-rigging.asp>

Three common forms of bid rigging are:

Complementary Bids or Cover Bids: Bids are submitted in such a way that the submitter of the bid knows that it will be rejected in order to ensure that the correct bid wins the contract.

Bid Suppression: where entities capable of entering a bid, do not do so in order to ensure that another bid wins the contract.

Bid Rotation: Bids are submitted in such a manner that bids are won in a pre-defined order so that everyone that is involved in the bidding scheme wins something, and thus profits from the bid rigging.

**Question 2: What are some the terms and phrases that you will want to look for in regards to bid rigging? What are some of the obstacles you may face because of the international nature of the bids? How would you solve the multi-lingual problem with determining your keywords? Hint: check online for translation help. Would a search for a Spanish word be completed any differently than an English word? Can you make a complete keyword list at this point with the information you have? Why?**

**Some of the terms that I would probably search for are:**

**Bid, Fraud, agree, agreement, money, profit, stipulation, account, turn, contract and company names where bids were submitted, and company names of competitors, and dates of the bids.**

**Some of obstacles that may be faced because of the difference of the international bids are whether or not the countries in questions have laws against bid rigging, and what exactly are those laws. In some countries, it may even be possible that bid rigging is legal, which means that obtaining any co-operation from those countries may be difficult if not impossible. Another obstacle (as the next question in this assignment suggests) would be that of language barriers in that in order to properly search for words or phrases, you need to know what those words or phrases are in the languages in question.**

**I would solve the multi-lingual problem for determining key words, by defining all of my keywords in English first. I would then use a translator such as babble fish or Google’s translator to translate those words into the language(s) in question, and then search for those words and translate several of the results back into English to verify that the translation was the correct word, and spelling.**

**Outside of making sure that sure that translated words have the correct punctuation, I do not think that searching for these words would be any different because the search process is still just a string search that is looking for a match. Whether the word is in English or in Spanish, a match to a specified string would still be a match.**

**At the time of this assignment, a complete keyword list is not possible. In order to create as complete as possible keyword list we would need to know more information about the bids that were placed, such as Project Name’s and other specific information. This is because it is possible that the employee may have been with the company for many years, thus communication with these companies on a regular basis may be the norm, and thus it is possible that he was just outbid.**

**It is also impossible to create a complete keyword list, because we would need to know who this companies competitors are. In order for a bid rigging scheme to succeed there has to be more than one person involved, as such one would expect cross company communication to be occurring that should not be, which means those company names could be valuable in preventing something from being overlooked. However, this does not exclude the ability to expand the keywords to search as information is discovered during the investigation.**

**Also due to the international nature of the case, knowing additional information about the bids placed, and competitors etc. could reveal language information that could be useful.**

**As detail orientated as the computer forensics field is, the more the details the investigator has in regards to what he should be looking for the easier it will be decipher the evidence.**

**Question 3: What kind of files does the floppy disk contain? Can FTK view and search these types of files? Select each file that ends in .eml and select the option to view each in raw text format. List the first and last names of the individuals mentioned in the .eml files. And finally cross-reference that list with the addressbook.csv file. Indicate which of them are probably competitors of the suspect's company.**

Kinds of File on the floppy disk:

|  |  |
| --- | --- |
| **Type** | **Number** |
| Total File Items | 47 |
| Unchecked Items | 47 |
| Filters in  | 47 |
| Other Thumbnails | 1 |
| Duplicate Items | 2 |
| OLE SubItems | 30 |
| Documents | 5 |
| Graphics  | 1 |
| Folder | 1 |
| Slack / Free Space | 4 |
| Other Known Type | 15 |
| Unknown Type | 21 |

Yes, FTK can search these types’ of files, as most of them are not binary files.

Selecting .eml files and cross referencing to addressbook.csv

Agreed.eml - Bob Sellers

Que pasa!\_.eml - Manual Papillo

What’s up\_.eml - Betty Noonan

Addressbook.csv cross reference:

Betty Noonan - email address only

Bob Sellers - Concrete Experts Inc. Texas Rep

Manuel Papillo - Xyz Corporation, Director of Projects. Construction Unit

Probable competitors:

Bob Sellers Concrete Experts Inc. Texas Rep

Manuel Papillo Xyz Corporation, Director of Projects. Construction Unit

**Question 4: What are the number of hits and files the search found? Describe the results.**

|  |  |  |
| --- | --- | --- |
| **Search Term** | **Hits** | **Files** |
| bid | 6 | 5 |
| fraud\* | 2 | 1 |
| acuerdo\* | 3 | 2 |
| agree\* | 5 | 3 |
| bid\* | 9 | 5 |
| money | 2 | 1 |
| sub\* | 25 | 16 |
| next | 1 | 1 |
| turn | 2 | 1 |
| contract | 7 | 4 |
| department | 4 | 4 |
| Mexico | 3 | 3 |
| haven | 4 | 1 |
| arizona | 1 | 1 |
| estado | 1 | 1 |
| libre | 1 | 1 |
| soberano | 1 | 1 |
|   |   |   |
| Cumulative Total | 71 | 20 |

Using the search parings suggested by the assignment

|  |  |  |
| --- | --- | --- |
| **Search Term** | **Hits** | **Files** |
| bid AND fraud\* | 0 | 0 |
| acuerdo\* AND agree\* | 4 | 1 |
| acuerdo\* OR agree\*  | 8 | 4 |
| sub\*  | 25 | 16 |
| bid\* AND money | 0 | 0 |
| bid\* OR money | 11 | 6 |

**Question 5: How many hits did you come up with and how many files?**

**Searching for bob or manuel**

**13 Hits in 6 Files**

**Question 6: How many hits did you come up with and how many files?**

**Searching for sub\* AND next**

4 Hits in 1 File