THE SURREY STAR

LAB

DIGITAL FORENSICS TEAM

DIGITAL FORENSIC INVESTIGATION REPORT

Report Exhibit Reference	680788-1
Case Reference	8870
Investigator	Hud Daannaa //6396086 //hd00240@surrey.ac.uk
Report Date	24th March 2017

I confirm that the submitted work is my own work and that I have clearly identified and fully acknowledged all material that is entitled to be attributed to others (whether published or unpublished) using the referencing system set out in the programme handbook. I agree that the University may submit my work to means of checking this, such as the plagiarism detection service Turnitin® UK. I confirm that I understand that assessed work that has been shown to have been plagiarised will be penalised.

Hud Seidu Daannaa

Executive Summary

A high ranked cybercriminal Bee Bin Gergen has been on the run for years. He was apprehended and released due to lack of evidence to prosecute him. He sells and deals in nuclear blueprints over the dark web. He has been responsible for more than 50 percent of the cybercrimes in his country. His last operation on Mercury labs, where he stole sensitive data and alongside blueprints for a nuclear reactor.

Agents and special forces had him on the chase till one agent Knox had information of his where about. He was finally apprehended and a USB Flash disk was found on him. The USB Disk was sent over to Surrey Star labs to be investigated because their reputation in multimedia and digital forensics were second to none.

Lead by a three-man team, Hud Daannaa oversaw multimedia and digital forensics due to his long team experience in the field. He incorporated the use of specialize chosen forensic tools and analysis, he could point out specific findings which supports and backs the claim that Gergen stole files and documents off Mercury Labs and this was evidence enough to put him behind bars.

Below are the key findings from surrey star labs:

- The MD5 hash images of the nuclear blueprints found on the USB Flash Disk matched the original md5 Hash.
- There were more files and notes relating to the Dark web and other documents on Mercury Labs because of a keyword search to pinpoint and focus on specific areas related to his numerous crimes.
- Lastly, there were extension mismatches to conceal documents, also some deleted documents related to Mercury Labs came up because of the analysis.

overall, these three digital forensics tasks add up to a concrete build and basics to stand and support the USB Flash Disk Drive as a strong piece of evidence to incriminate Bee Bin Gergen.

Contents

1 Investigator Background 5
2 Submission Details 5
3 Case Remit 5
4 Analysis of Exhibits 6
4.1 Initial Examination of CM/4 6
4.2 Forensic Examination of CM/1 – Operating System and User Details ..... Error! Bookmark not defined.
4.3 Forensic Examination of CM/1 – Relevant Photographs 7
5 Exhibits Produced 7
5.1 CM/4 Sub-Exhibits 7
6 Appendix 1 – Technical Glossary 8

1 Investigator Background

With a bachelor's degree in computer science, CHFI certification and a long-term experience in the field of multimedia, I head a team of three in the Star Surrey Labs. The team shares expertise with respect to every team mate, my main role and expertise is multimedia media and digital forensic investigation. Star Surrey Labs are affiliated to two main governmental agencies. Amongst these agencies are the home land security.
My work curtails the sole responsibility for conducting a vivid, sound and detailed forensic analysis on digital multimedia bearing equipment. As a forensic investigator, I deal with the acquisition and preservation of multimedia related data in a lab by onsite capturing and seizure. Data analysis and recovery of files, emails logs and evidence of data tampering, removal, formatting are some relations operation in a digital multimedia investigation.

2 Submission Details

The below listed exhibits were received by the Digital Forensics Team for examination and analysis:

Exhibit Reference	Description	Seal Number
USB_FLASH_DISK_487-001	USB Flash Disk Drive containing evidence for Mercury Labs test case	URN678654SN

3 Case Remit

The goals and aims of the examination, as instructed by the Officer in the Case were to examine the submitted exhibits for:

- Stolen images of nuclear plan blueprints
- PDF documents, Word (Doc) documents, CSV files, TXT files
- PCAP files (Network Data Capture files)

4 Analysis of Exhibits

4.1 Initial Examination of USB_FLASH_DISK_487-001

4.1.1 The forensic examination of Exhibit USB_FLASH_DISK_487-001 commenced when I collected it from the secure store at 13:00 on 25th March 2017. The exhibit was sealed in police evidence bag ITEM_487-001.

4.1.2 The Exhibit USB Flash Disk Drive was detailed as:

Ref	Make	Serial Number	Capacity (***Gigabytes***)
USB_FLASH_DISK_487-001	Kingston	URN678654SN	2 Gigabytes

4.1.3 I used a specialist tool (software) "Access Data FTK Imager 3.1.2.0", this tool was used to create a (Raw) "dd" forensic image, as detailed below. The forensic image was successfully verified using an MD5 hash with the resultant output:

Ref	Image File	Acquisition MD5	Verification MD5
USB_FLASH_DISK_487-001	The_Mercury labs case_881	cebf90d792aee8cd71a025f6eba57f0d	cebf90d792aee8cd71a025f6eba57f0d

4.1.4 I used a stop watch to establish date and time, this helped me to keep track of the examination process. Basically, the process involved the creation of the forensic disk image and the applications of digital forensic tasks on the given image.

4.1.5 At 20:00 on 25th March 2017 I resealed the exhibit USB_FLASH_DISK_487-001 in the evidence bag and returned it to the Digital Forensics Team secure store.

4.2 Forensic Examination of USB_FLASH_DISK_487-001 – Relevant Photographs

4.2.1 A picture of the USB flash Disk drive was taken and recorded into the report.

4.2.2

5 Exhibits Produced

5.1 CM/4 Sub-Exhibits

5.1.1 At 21:00 on 25th March 2017, I presented the exhibit CR/ USB_FLASH_DISK_487-001 /1. An "interactive Report Disk" This contained a summary files and their attributes. A single master copy was made together with a working copy. The master copy was kept safe, in case the working copy was corrupted during the process of examination. Both CDs were sealed in the bad ITEM_487-001. At 21:30 on 25th March

6 Appendix 1 – Technical Glossary

USB -	USB (Universal Serial Bus) is a connection type used by many to connect computers and devices like cameras, mobile phones and other forms of digital media or computer peripherals. It serves as a de facto and is used across platforms by most vendors in computing.
Disk Drives -	a device which provides storage for data, and allows a computers and other forms of data relating systems to read from and write on to computers
Gigabyte -	This determines the size of storage data on a disk, from the smallest unit of measure with regards to data, Gigabyte forms 1 of 8e+9 bits, hence find bellow the table: 8 bits – 1 byte 1024 bytes – 1 Kilobyte 1024 Kilobytes – 1 Megabyte 1024 Megabytes – 1 Gigabyte 1024 Gigabytes – 1 Terabyte
USB Flask Disk Drive -	This is a disk bearing USB connector. It serves as a storage medium for data.
MD5 Hash -	A hash value is a type of digital signature that can be computed for an area of data such as an entire hard disk, or individual file. The odds of two (2) files with different content having the same hash value are approximately one (1) in three hundred and forty (340) billion, billion, billion.
Disk Image -	This is an enveloped copy of a disk drive saved onto another storage medium in a form of a virtual drive, which maintains the properties of the original disk copied.

7 Appendix 2 –

Star surrey labs is a computer forensic investigation firm that plays a major role in the security, diagnosis and, the data analysis of data on systems. Star surrey labs is affiliated to two governmental agencies like the military and home land security.
Since Surrey star labs are specialized in multimedia research and digital forensics, these agencies tend to rely on star labs for a more detailed, vivid and sound scientific approach to solutions.

Two years ago, an Arabian born dissident Bee bin Gergen, who is known for cyber-attacks across the country was reported to have made away with a nuclear blueprint file from the Mercury labs and other sensitive relating data that poses treat to the country. The news report claims he has been on the run and is responsible for the sale of number nuclear weapons and blueprints on the dark web. Gergen also holds a strong position in the nuclear weapons trade chain. He gained fame on the wanted list and rose to the top five most wanted cyber criminals in the whole country. Gergen was once held in custody by one agent Knox but manage to break free due to lack of incriminating evidence.
Two weeks ago, agent Knox had word from an informant that Gergen was back in town and had plans to steal the blueprints of a nuclear power reactor, agent Knox then moved in and closely monitored Gergen's movements and actions, this made Knox and his other team mates draft a solid and strategic plan to lockdown Gergen. When the time was due for agent Knox to move in, he seek backup from the special skill force, the SWAT, this is because Gergen became dangerous and had a group of thugs working for him called in on backup and his house was raided by the SWAT team. To Gergen's surprise agent Knox and the SWAT team gashed into his doors and windows like blood running through human veins. Gergen was apprehended and sent to custody. He had on him a mat black USB flash disk with a red flip top.

Due to of Gergen's cyber technical know-how and his ability to execute cyber-attack and other forms of theft swiftly by leaving behind no trail and cleaning his tracks, the military and SWAT teams thought is wise and fitting to send the USB the star labs team in charge of forensic investigations. For a more detailed, vivid and scientific analysis.
Since I was the head of the three-man team in charge of the forensic team the USB flash disk was handed in to my department and I rank labelled the case as delicate, since it was a matter of urgency to gather and hold some evidence against Gergen.

To start with the process, I prepare a sandbox like environment and connect the USB flash disk. I used the access FTK Imager, it helps to copy or convert a byte by byte detailed and verified disk to image. It can be used on storage media like hard disk, USB flash drives and other forms of storage. It reconstructs saved storage media into selected formats. It has a verification option where it calculates MD5 hashes of disk images before and after conversion, to help check integrity. I used FTK imager because, the case was labeled a matter of urgency. I needed to quickly use a fast, easy and efficient tool that could get the job done.

. The tool makes an image file with the extension ".dd". We create two image files, a master and the image to be worked on.

I calculated the md5 hash of the image. This is to serve as a reference point to how the image might or might not depreciate in originality. An important part of this is to monitor the veracity of the image.

Created By Access Data® FTK® Imager 3.1.2.0

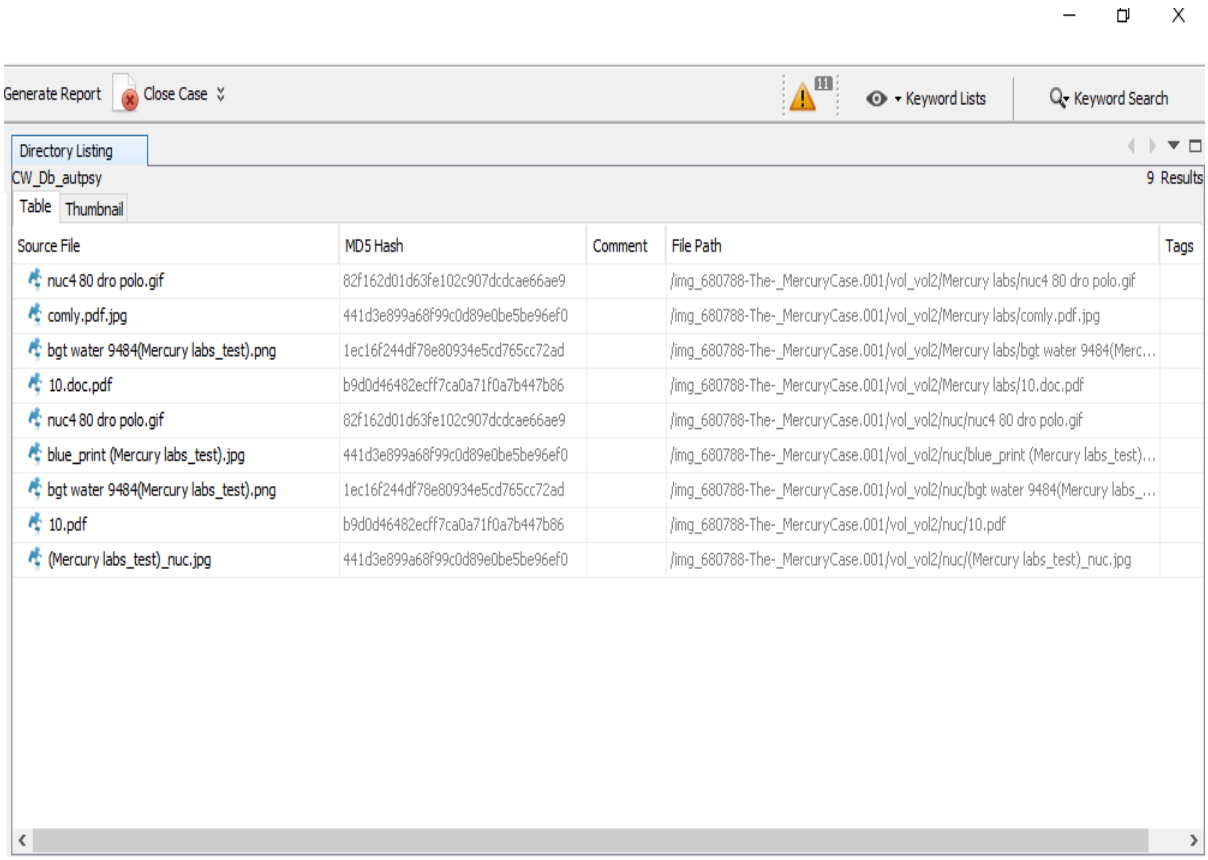
Case Information:
Acquired using: ADI3.1.2.0
Case Number: 680788-1
Evidence Number: 1-88
Unique description: the Mercury labs case_881
Examiner: Hud Daannaa
Notes: 680788-1//the Mercury labs case_881//Hud Daannaa

Information for C:\Users\Hud\Desktop\image_destination_881\680788-The-_MercuryCase:

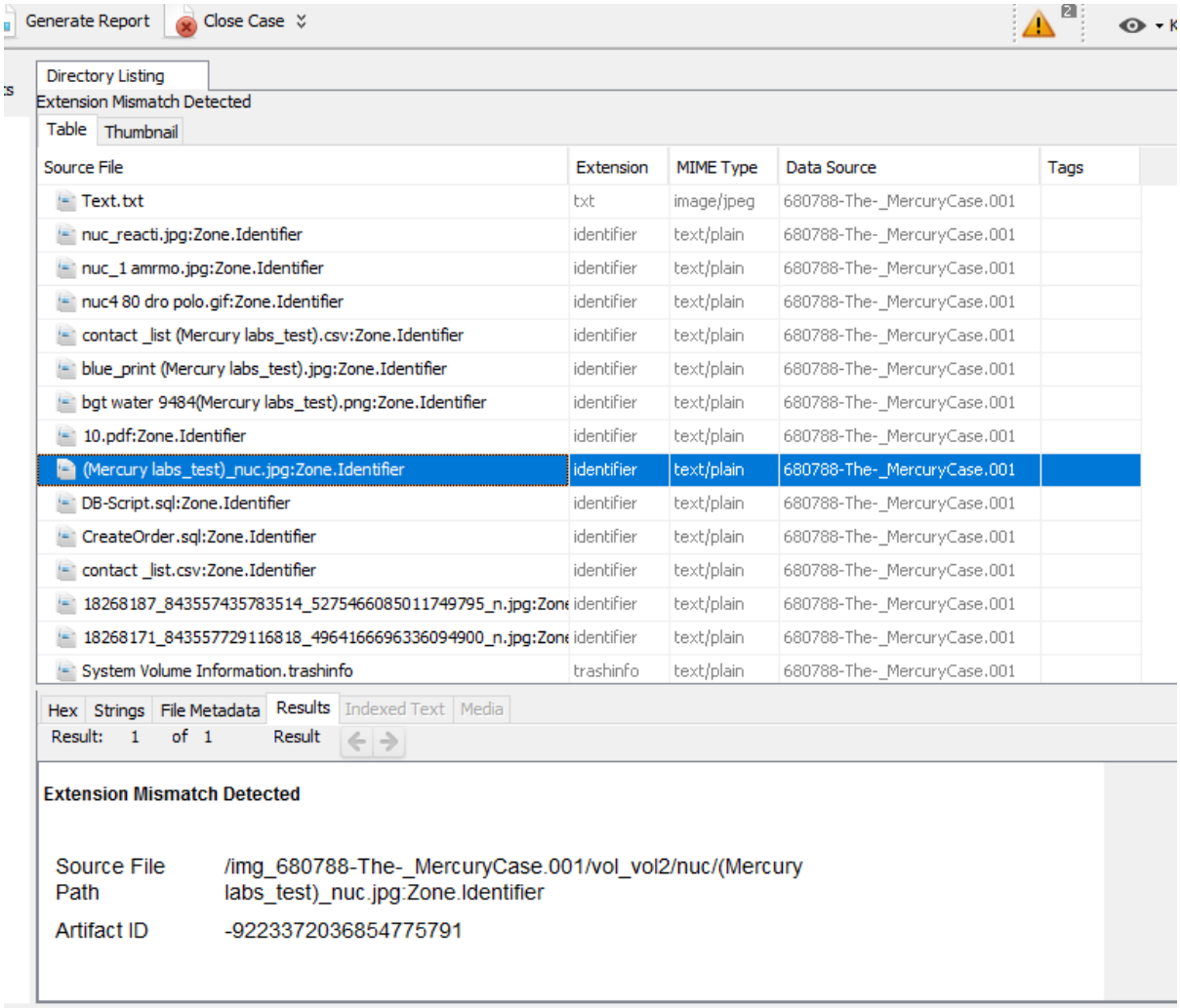
Physical Evidentiary Item (Source) Information:
[Device Info]
Source Type: Physical
[Drive Geometry]
Cylinders: 489
Tracks per Cylinder: 255
Sectors per Track: 63
Bytes per Sector: 512
Sector Count: 7,864,320
[Physical Drive Information]

For this investigation, we will use Autopsy. Autopsy is an open source forensic graphical platform used by too much a many to investigate and analyse systems like computers and other forms of storage media. It is used by higher governmental organisations and special security agencies. I prefer autopsy because it is open source, open source application has the advantage of being test and updated by different set of minds all over the world, this make it very difficult to for hidden bugs.

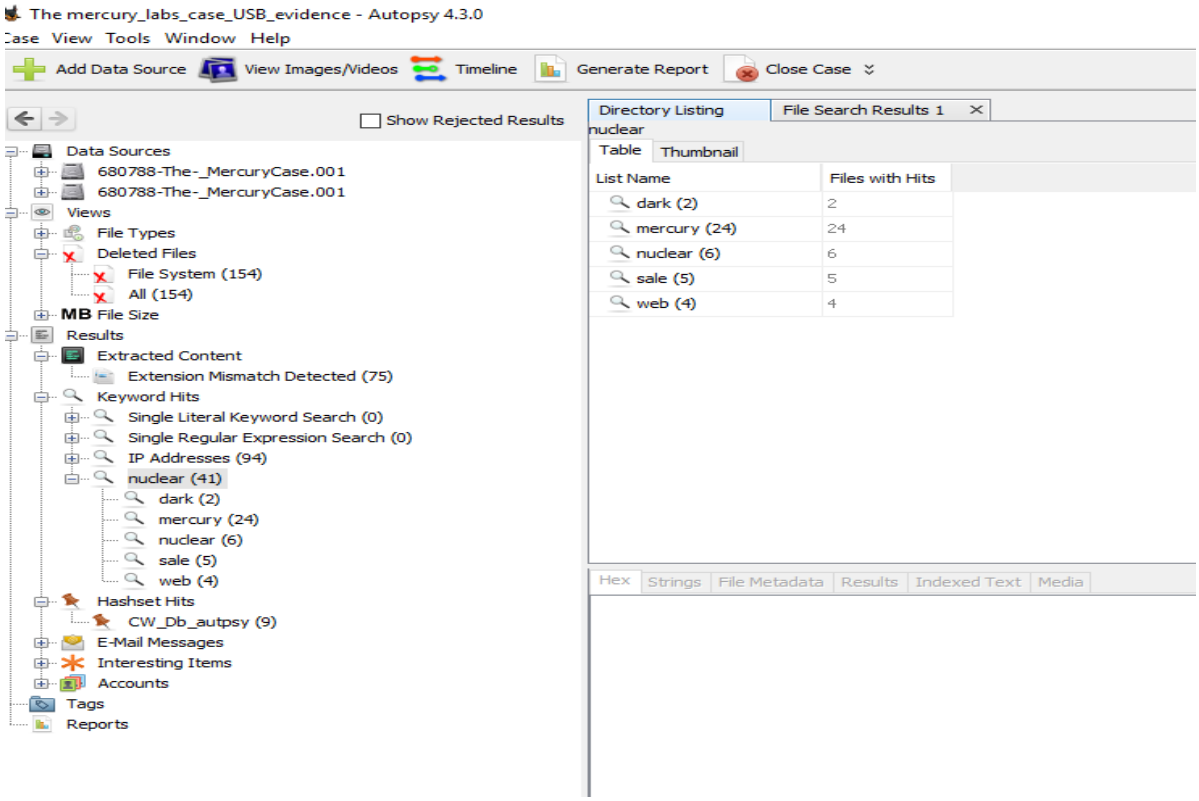
I commenced by computing the hash values of targeted or wanted images using File Checksum Integrity Verifier (FCIV) on windows with the "-md5" option. I chose to use a second md5 hash tool just to double check my hash results. I then placed the computed hash values in the database of the autopsy software, by so doing, during execution, the hash values of the computed hash are pair or matched to the hash values in the autopsy's database. I found a couple of image matches, I had just completed a digital forensic task which yielded beneficial results.

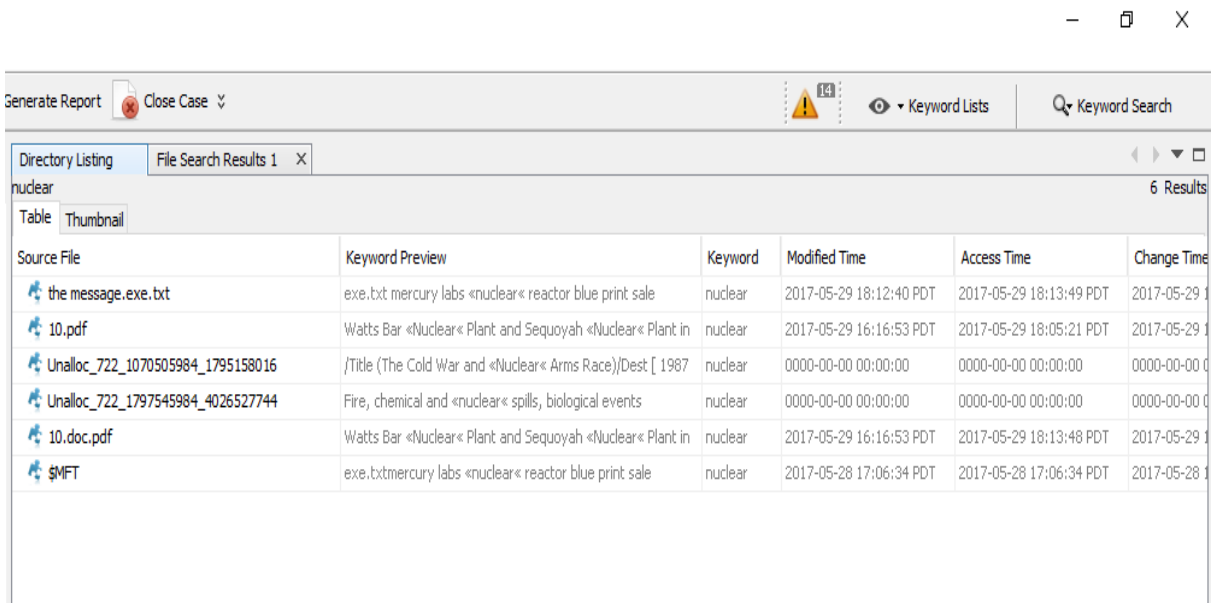


I went on to add another digital forensic task known as “extension mismatch”. This happens when and individual has the intention of concealing some form of information by saying it’s something else. We found one extension mismatch which contained a portion of the stolen blue print.

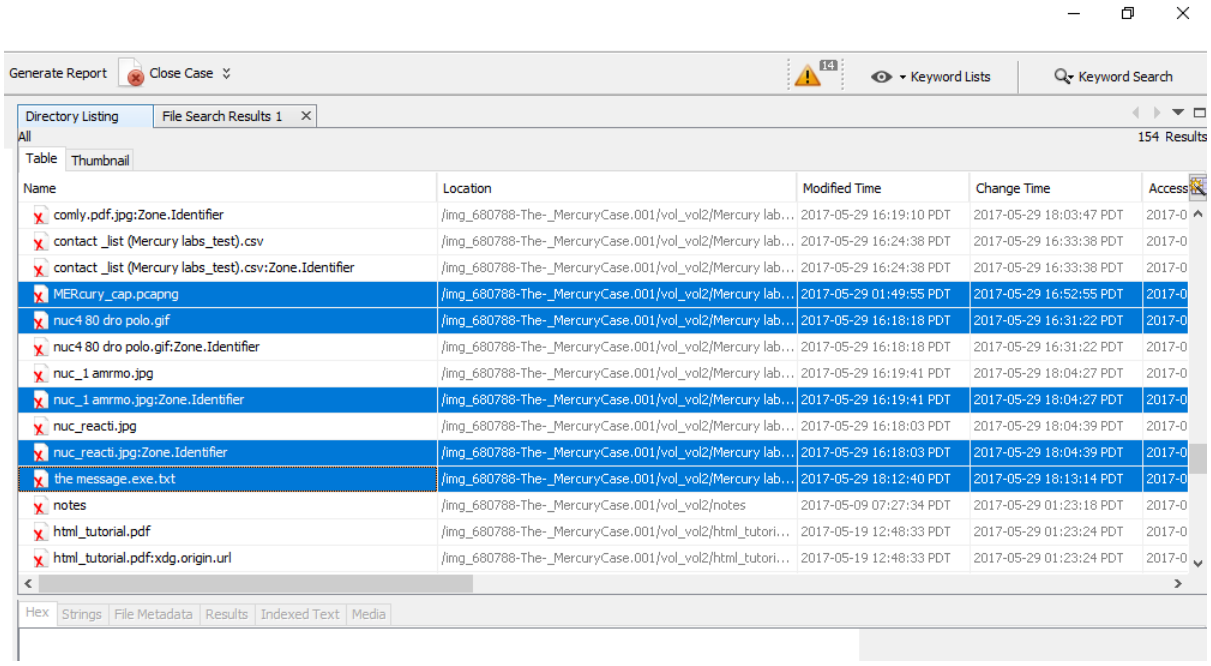


I made a keyword list of keywords in an aim to mine into text files to pick certain topics of areas of interest. This digital forensic task helps to focus and pin point attention to an area of interest, the keywords “Dark web”, “sale”, “Nuclear”, and “Mercury” were found. This was also fruitful, because the more forensic tasks that tallies with the given evidence, the more it strengthens the credibility of the provided evidence. Below are two images the first image details all keywords with relating content. The second image is an example I show to demonstrate the content every keyword brought up, the keyword selected was “Nuclear”.





I also found a long listing of deleted files in the USB flash disk “dd” image. I scrolled and pinpointed relating areas to files containing the nuclear keyword.



Report Exhibit Ref: 680788-1

REFERENCES

[1] S. Li, "Multimedia Security and Digital Forensics (COMM046)", surrey, Guildford, 2017

[2] G. Holt, "Cyber Incident Response & Digital Forensics Lecture", University of Surrey, 2017