**Assignment : Evidence Analysis**

****

**Pawan Chandra, Aditya Subedi, EJ Truscott, Josh Zurbuchen**

**California State University, Sacramento**

**CSC 153, Section 2**

**Part 1: Assess**

Upon receiving the project USB, our team first discussed what we need to acquire and how to approach it without destroying any evidence. Our team came to the conclusion using a software that uses some sort of write blocker.

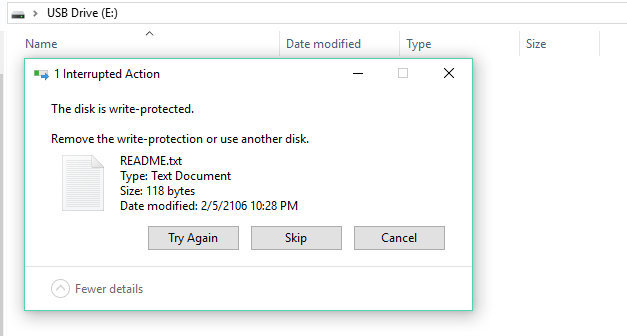
**Software Write Blocker**

* We are using DSi USB Write Blocker to make sure that there is no possibility of accidentally damaging the drive contents.



**Testing Write Blocker**

* We inserted a random flashdrive to make sure the software write blocker works properly.
* When we tried to copy a file to USB it was blocked, so the write blocker works.

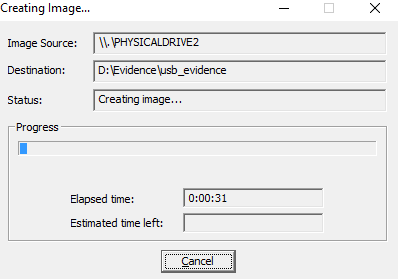


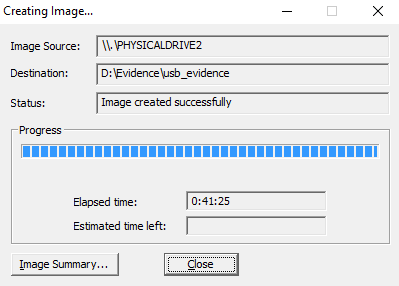
**Part 2 & 3: Acquire/Authenticate**

As demonstrated above, the software DSi works perfectly and we were able to acquire data from the USB without any overwriting or data loss. We then created a image of the USB and copied it to a different USB. That way we don’t tamper with the original files/documentations.

**Forensic Imaging of USB**

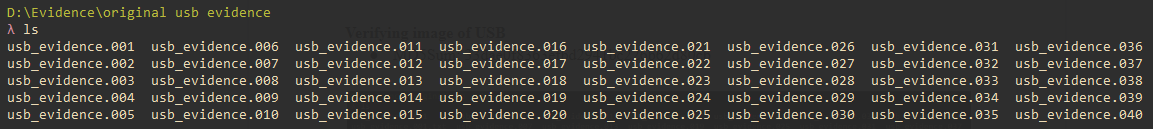
* We are going to create a duplicate image so it preserves the original evidence and prevents inadvertent alteration of original evidence during examination.
* We are also imaging the USB as a backup.
* The D:\ is a clean media we are going to copy to.
* We are using FTK Imager to create an image.

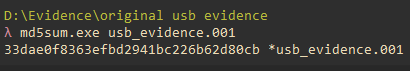




**Verifying image of USB**

* MD5Sum: 33dae0f8363efbd2941bc226b62d80cb

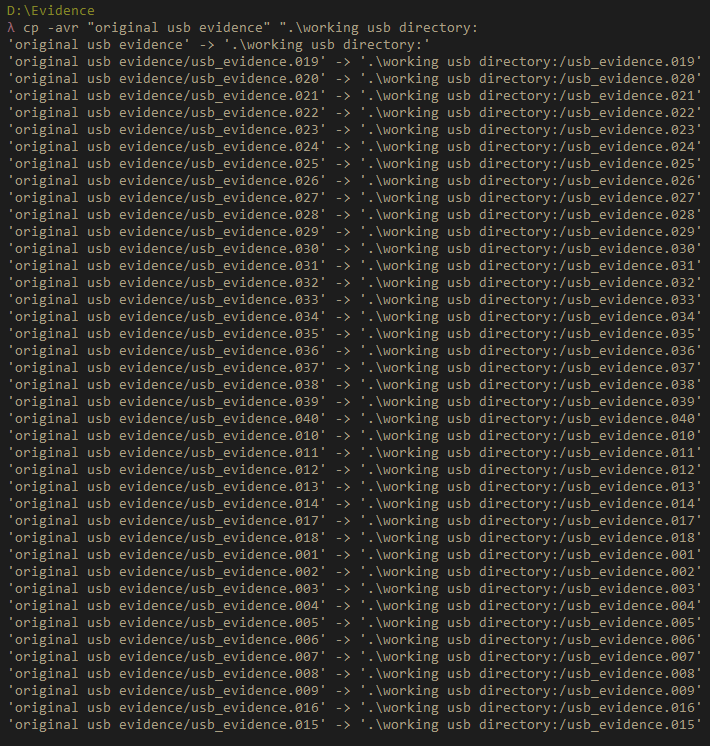




**Making copies of original media**

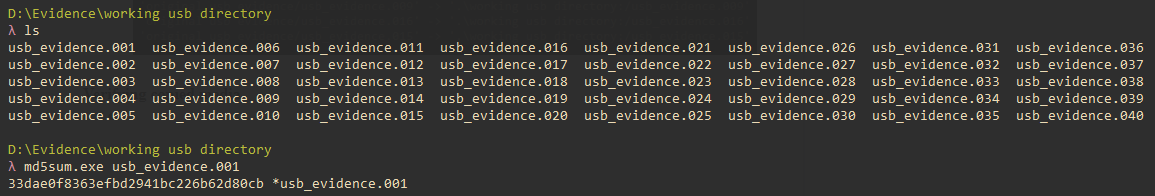
* Total of two copies of the original media
  + One copy is the working copy
  + One copy is the library/control copy, this was made before using FTK Imager
* mkdir "working usb directory"
  + Create the directory if they do not already exist.
* cp -avr "original usb evidence" ".\working usb directory”
  + -a : Preserve the specified attributes such as directory, file mode, ownership, timestamps, if possible additional attributes: context, links, xattr, all.
  + -v : Explain what is being done.
  + -r : Copy directories recursively.





**Verifying copied media**

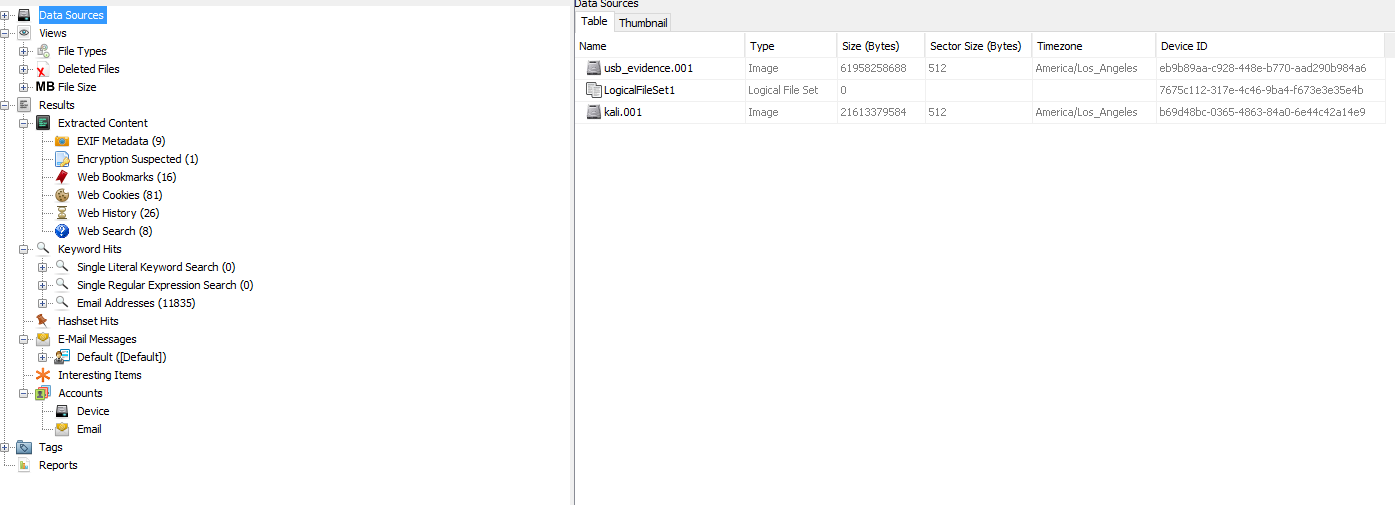
* The copied MD5Sum: 33dae0f8363efbd2941bc226b62d80cb
* The copied MD5Sum matches the original MD5Sum



**Part 4: Analyze**

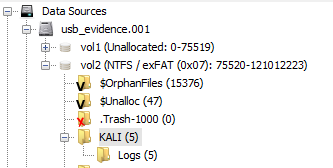
**Analyzing Flash Drive**

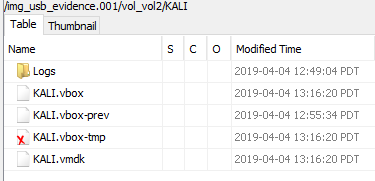
* Loaded the image on Autopsy to analyze



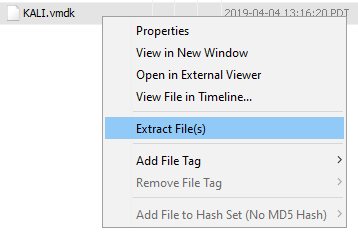
* There is a Virtual machine file format describes containers for virtual hard disk drives to be

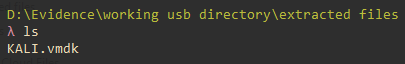
used in virtual machines [KALI.vmdk]



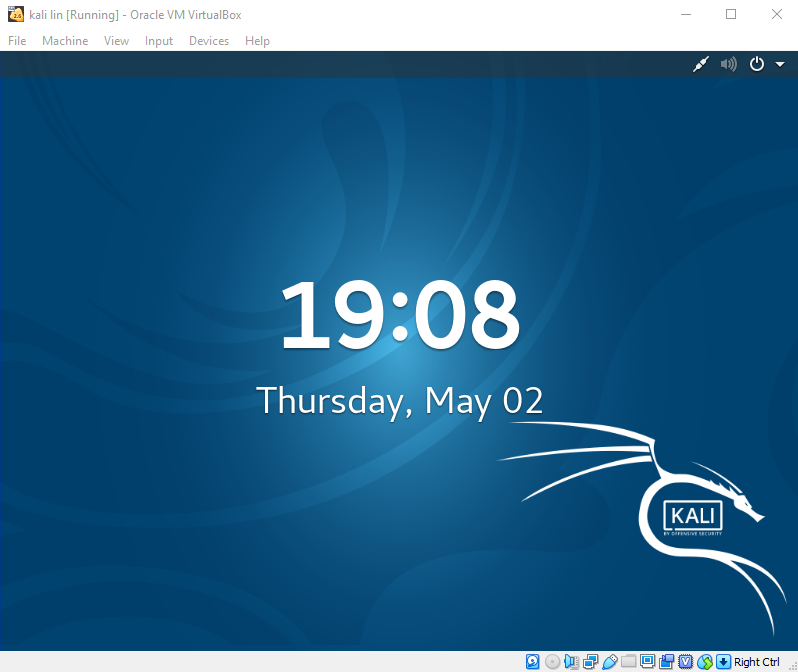


* Extracting the vmdk file to mount

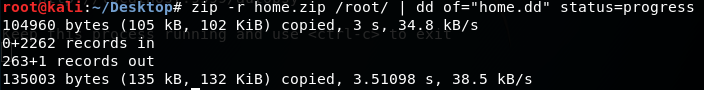




* Running the OS on virtualbox
  + It is running Kali Linux

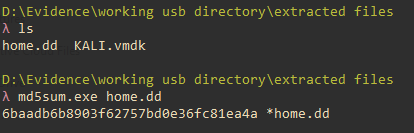


* Imaging home folder in linux
  + zip -r : recurse into directories
  + status=progress : output progress while making an image with dd
  + of: output file.

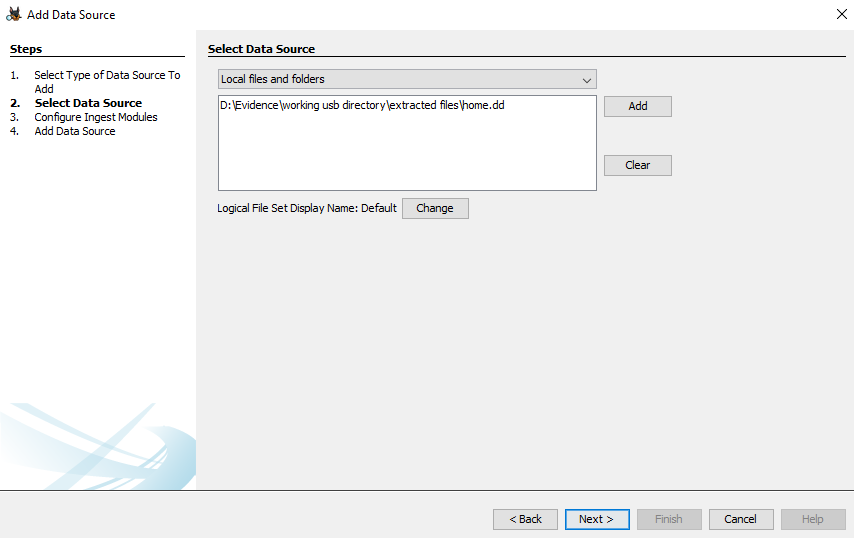




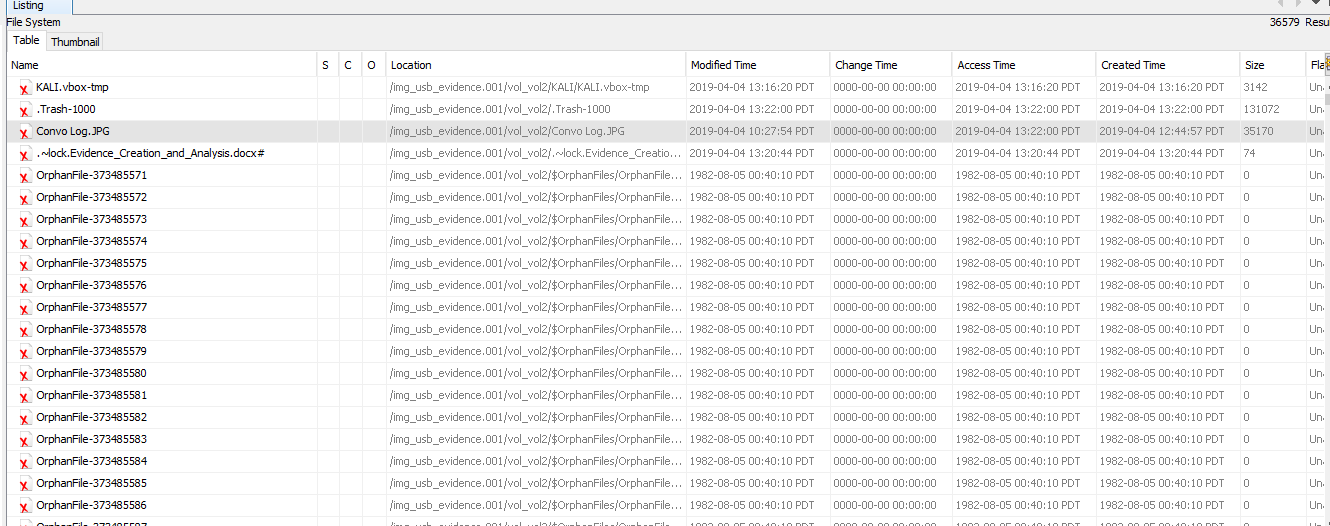
* Transferring the raw home.dd file to working directory
  + The md5 sum matches



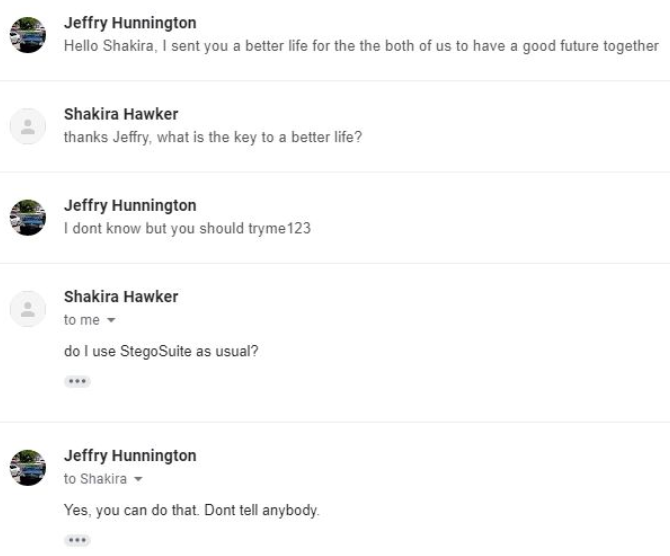
* Analyzing home.dd on autopsy



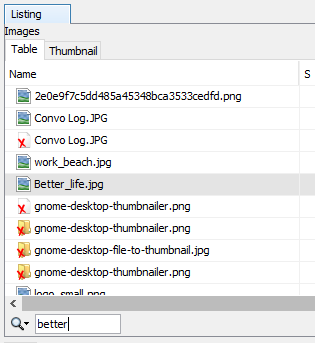
* Looking at deleted files
  + There is a deleted file called Convo Log.JPG which looks suspicious.



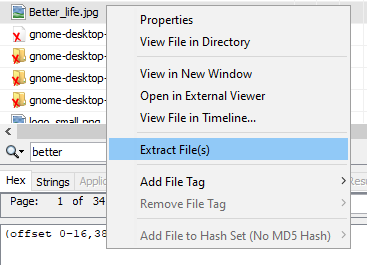
* Viewing the image
  + StegoSuite was being used for steganography
  + Password of some file might be tryme123



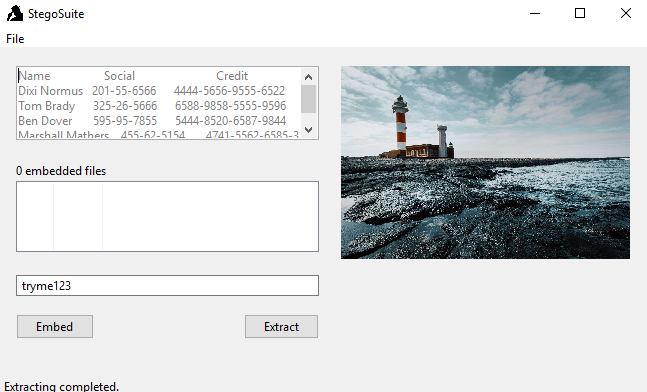
* Searching for “better” “better life” “life” since it was mentioned in the image above
  + Found a file called Better\_life.jpg

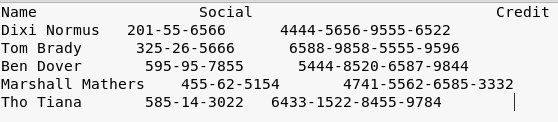


* Exporting Better\_life.jpg to check with StegoSuite steganography



* Running StegoSuite for steganography
  + Loaded Better\_life.jpg with the password tryme123
  + Found people name, social, and credit card numbers





**Part 5 & 6: Articulates & Archive**

Upon analyzing data from the image file, a report was built by our forensic team to present to our professor Dr. Isaac Ghansah. This report contains screenshots and evidence we found during the process stated above.

**Chain of custody**

Professor Isaac Ghansah took out the USB from him backpack and handed it to Aditya.

**Question and Answers**

Q: What is the operating system on the drive?

A: Kali Linux

Q: What is the “key” for decryption?

A: tryme123

Q: Where is the folder with “sent emails”?

A: Did not find any folder containing sent emails

Q: Were there any files on the drive that contained sensitive information about customers?

A: The drive had a image called Better\_life.jpg and the information was hidden in the image. It contained employee’s name. Social, and credit card number

Q: Were there any files that seemed encrypted?

A: The image was a steganography and it was password protected. The password was tryme123.

Q: Were there any files that were deleted?

A: There was a image called “Convo Log.JPG” which was deleted. It had information about the encryption password and steganography tool.

Q: What files were found to have flipped bits in them?

A: An attempt was made to check for flipped bits but did not find any

Q: What forensic tools were used into determining the flipped bits on the files?

A: Our forensic team used URLCrazy in kali Linux to check for flipped bits.

**Team Contributions**

* **Aditya** (Leader)
  + In charge of delegating tasks and keeping members accountable.
  + Ran Autopsy and PC and provided screen shots of each step.
  + Installed Kali Linux on a Virtual Machine and helped educate team members on basics of Linux OS.
  + We rounded expertise i.e. helped everyone.
* **Pawan**
  + Worked with Aditya in using Kali Linux to search the contents of the USB.
  + Helped analyze data using Autopsy
  + In charge of the 6A’s part 4 - 6
* **Joshua**
  + In charge of creating a replica of the flash drive without any alteration of the original content.
  + In charge of researching safe software to use to analyze the contents of the USB
  + In charge of the 6A’s part 1
* **Ernest**
  + Created analysis report and provided answers to the question section using information from group members.
  + Finalizing the documentation/formatting/proofreading.
  + In charge of the 6A’s part 2 & 3