Computer Architecture and Imaging

Ifeanyi Uzoukwu

CST 640

University of Maryland Global Campus

**Table of Contents**

Introduction……………………………………………………………………………………….3

Data Location Memo…………………………………………………………………………...…3

Imaging a USB Device using Linux Tools ………………………………………………….……9

Imaging a USB Device using Windows Tools……………………………………………...…...13

Response to Legal Team’s Questions Memo………………………………………………….…18

Acquiring RAM and Swap Space………………………………………………………………..20

Forensic Imaging over a Network……………………………………………………………….24

Conclusion……………………………………………………………………………………….28

References………………………………………………………………………………………..29

**Introduction**

Digital Forensics investigators are often tasked with creating copies of the devices we have retrieved or are given, and creating bit for bit images of those copies so the information on them can be presented in court. Parsing through the data on the devices and separating data that happens to be relevant to the case at hand from the remaining data on the devices is a difficult and tedious procedure. As time passes and technology gets more and more advanced, investigators must keep up with the various methods that threat actors can use to launch attacks against organizations and hide their crimes. Therefore, being a digital forensics specialist requires a desire to constantly hone your craft. As the lead digital forensics investigator for Zerobit, I have been tasked with the imaging of a USB thumb drive and acquiring RAM and swap space using Windows tools and Linux tools.

**Data Location Memo**

**Date: 1:35 P.M., Thursday July 29th, 2021**

**To: ZeroBit Legal Division**

**From: Ifeanyi Uzoukwu; Lead Digital Forensics Specialist**

This memo serves the purpose of informing the legal team of ZeroBit of the various locations on which we can expect to find relevant data, including hard drives, USB sticks, and RAM and swap space. The memo will also go into detail describing the advantaged and disadvantages of various storage formats of digital evidence.

* Universal Series Bus (USB) flash drives (thumb drives) are data storage devices that are made of flash storage memory to and a USB interface. Flash memory is considered an erasable electronic programmable read-only memory (EEPROM), which is popular because the data is non-volatile and the drives themselves are small in size allowing a user to move them easily. USB flash drives range in sizes between 512MB to possibly 128 GB. USB flash drives can hold varying kinds of files which make them a popular option for file storage.
* Operating System Hard Disks are non-volatile memory storage devices that store large amounts of data and offer quick access to said data. The data stored in an operation system hard disk is vital to a digital forensics investigation as it likely contains important evidence and it has to be properly preserved after getting proper authorization so it can be admitted into a court of law. (Miller, 2018)
* Random Access Memory (RAM) and Swap Space: RAM is the memory being used to store short term data. The RAM is responsible for storing the data that is actively used on the device. The Swap Space refers to the disk space that is set aside for the usage of virtual memory, which is only used when the RAM is full. The files that are on the RAM that have not been used recently are transferred to the hard disk in order to free up space for the RAM. Being able to acquire the RAM and Swap Space is pivotal as there is important information stored on it. including the usernames and passwords available on the device, recent network connections, and the identity of the programs that were ran on the device.

**Digital Information Types**

Through the duration of an investigation, digital forensics specialists come across different storage formats based on the activities that the perpetrator partook in using the device. The three items listed above can store different kinds of information.

* Backups for specific devices or programs
* Browser history
* Bookmarked website list
* Calendars and Events
* Compressed and Encrypted Archives
* Cookies
* Databases
* Documents
* E-Mail messages and attachments
* Hidden Files
* Log Files
* Instant Messenger
* Images and Videos
* Social Media Accounts
* System Files
* Temporary Files

**Digital Forensic Images**

Digital Forensic Imaging is the process of retrieving an exact copy of the information on the target device, and places it in a large file for the purpose of analyzing the data on the target device without compromising the information already stored in it. Retrieving an image of the target device is more than just making a backup or copying and pasting the data to another source, as the copy is created is created from the original and placed in memory for later use. Imaging is the preferred method of obtaining digital information because there is less chance of missing evidence. The three main types of forensic imaging are physical, logical, and targeted.

* **Physical Image:** A physical image of a hard drive captures all of the information contained on the drive. This includes the deleted space on the drive and deleted files and file fragments The physical image of a hard drive will always be equal to the total space on that hard drive. The physical image is the most thorough type of forensic image and it is most useful for cases we are there is suspicion of deleted or tampered evidence. (Precise Law, 2017)
* **Logical Image:** Logical forensic imaging copies the active data stored within the hard drive. The active data normally takes up a minute amount of the total disk space. Deleted files, file fragments, and file space are not included in the capture. The contents available in the C drive are copied in a logical forensic image. (Precise Law, 2017)
* **Targeted Collection:** In a targeted collection forensic image, the examiner chooses the set of files or documents that they want to be copied. This is ideal if the examiner knows for certain that the evidence in question can be found in a specific location of the drive. (Precise Law, 2017)

**Storage Formats of Digital Evidence**

Digital crimes are on the rise, and it is necessary to be kept up to date not only with the different types of digital evidence, but also the kinds of formats that can be found during the course of an investigation. There are three primary storage formats for recovered digital evidence: RAW, EWF, and Advanced Forensics.

* **RAW Format:** The RAW image format is a bit-for-bit copy of the RAW data of either the disk or volume stored in single or multiple files. Metadata will not be found in the image files. The advantage of the RAW image format is the fact that the image files only contain unmodified source data. What this means is that every tool, even non-forensic tools support raw images. The aforementioned lack of metadata is a disadvantage to the regular use of this storage format. Due to the lack of metadata, there is no way to determine the source of the image. RAW format images also lack compression, which is why the images are often just as large as the source drive. (Raedtz.Biz, 2017)
* **Expert Witness Files (EWF)**: A type of disk image, which rank right under RAW as the most commonly used storage format. These files are also known as E01 files, which is an abbreviation for the EnCase Evidence File. (Forensicsware, 2018) This storage format contains a physical bitstream copy stored in single or multiple files that have copious amounts of metadata. Inside this metadata, Case Information, notes, checksums, and an MD5 hash can be found. This storage format has clear advantages in its compression, per file checksum, and password protection. The disadvantages lie in the fact that it’s an undocumented closed format. Most forensic tools support EWF, but it is not supported by non-forensic tools. (Raedetz, 2017)
* **Advanced Forensics Format (AFF):** AFF refers to an extensible open format for the storage for the storage of disk images and related forensic metadata. Developed by Simson Garfinkel and Basic Technology. AFF format holds both raw disk data and metadata. AFF files can be divided into a split archive of multiple files that use the .AFD file extension.

**Image Collection and Verification**

The notion that digital evidence can only be retrieved by the investigators and examiners at the scene is not necessarily true. Remote collection of evidence is a popular option amongst companies that have to outsource their digital forensics requests. The remote team we employ would send out multiple hard drives, which we would then connect to connect to the device containing the electronically stored information (ESI), once a connection is established, the remote technician connects to the computer while being assisted by a member of our legal team. (TCDI, 2018) Once the data is collected, the drive is sent back to the remote facility it is analyzed and the data on the device is available for review by the legal team. (Special Counsel, 2019) On the other hand, local collection is conducted in regular situations where the investigator has physical access to the system. This method is done in conjunction with seizing the hard drive and other information on the device, and using USB tools to image the device. (Johansen, 2017)

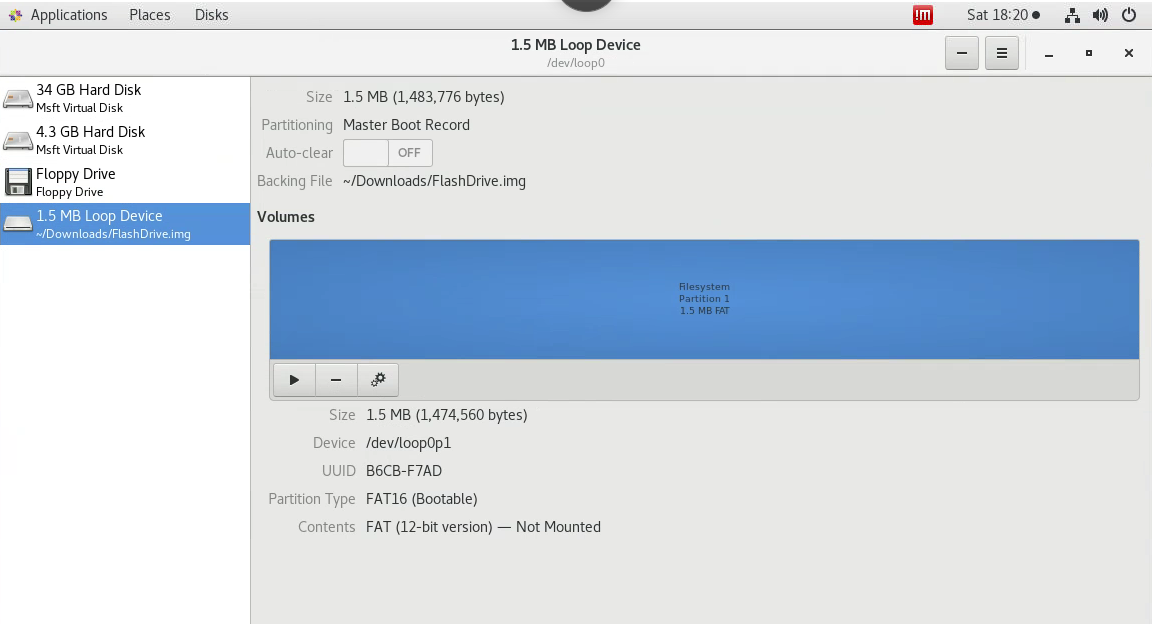
When collecting memory, the goal is to analyze the volatile data that resides in the RAM, in the memory dump of a computer. Memory forensics are performed to investigate and identify attacks or malicious behaviors that would not leave obvious tracks on hard drive data. Because the fruits of a memory dump can include information about open network connections and recently executed processes, being able to get that information when its available is pivotal to an investigation. (Lord, 2020)

Traditionally, examiners and investigators deal with Disk Forensics, which is the science of extracting forensic information from digital storage media such as hard disk drives, USB devices, flash drives, and DVD's. Once the device is identified and seized, evidence is authenticated and preserved. This is done using forensic programs and hardware. The information extracted is then checked against the hash values of the original, and the findings are analyzed and reported.

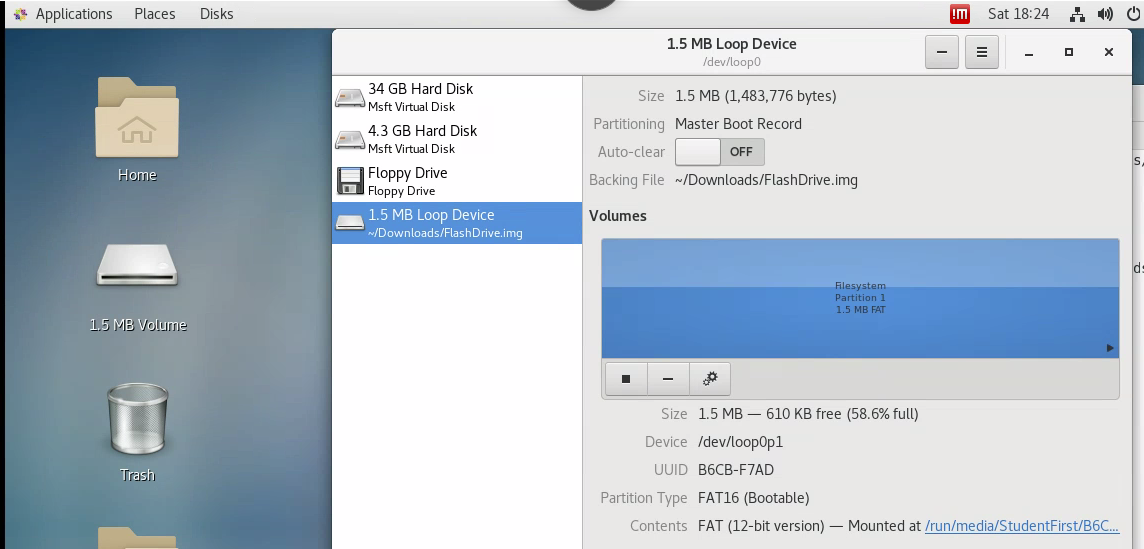
Technology will continue to advance as time moves on and it is imperative that ZeroBit is in the know on the practices and methods that examiners use to get the evidence that convicts these cyber criminals.

**Imaging a USB Drive using Linux Tools (Step 2)**

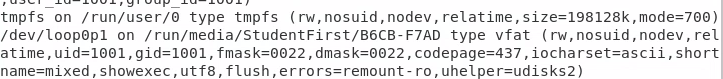
Creating a copy of the target device is the initial step in starting a forensic investigation. It is imperative to create a copy of the device so that when examiners are conducting their analysis of the data, they do kot run the risk of corrupting the original copy of the evidence in the device. The reports below are the results of the steps taken in imaging the device with Linux and Windows-based (Step 3) tools.



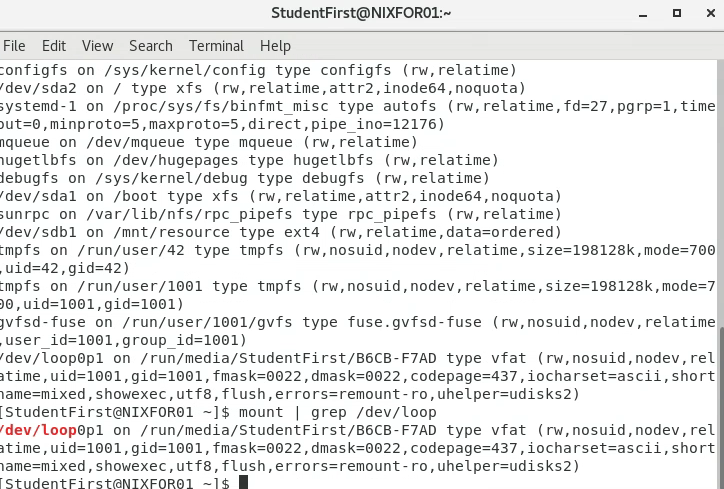
1. Confirmation of the drive being mounted in the NIXFOR01 system as shown by the graphical user interface (GUI)



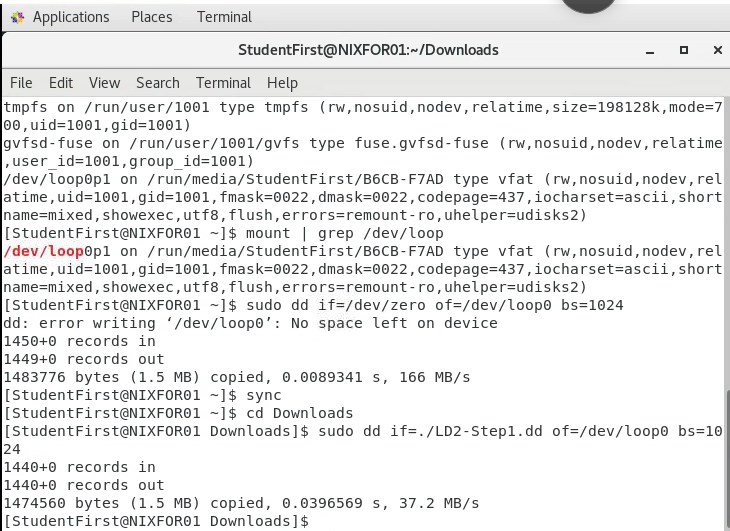
1. Further confirmation of the USB device being mounted as it is showing in the desktop



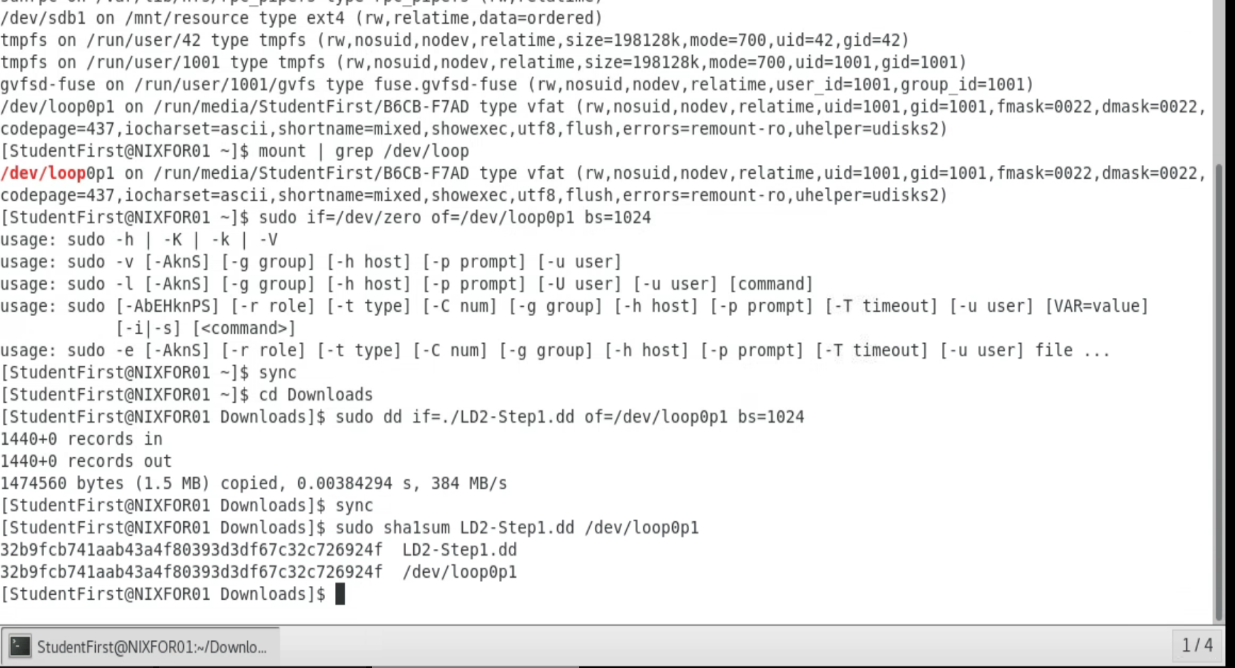
1. The device location I got when doing this exercise was “/dev/loop0p1 on /run/media/StudentFirst/B6CB-F7AD type vfat”



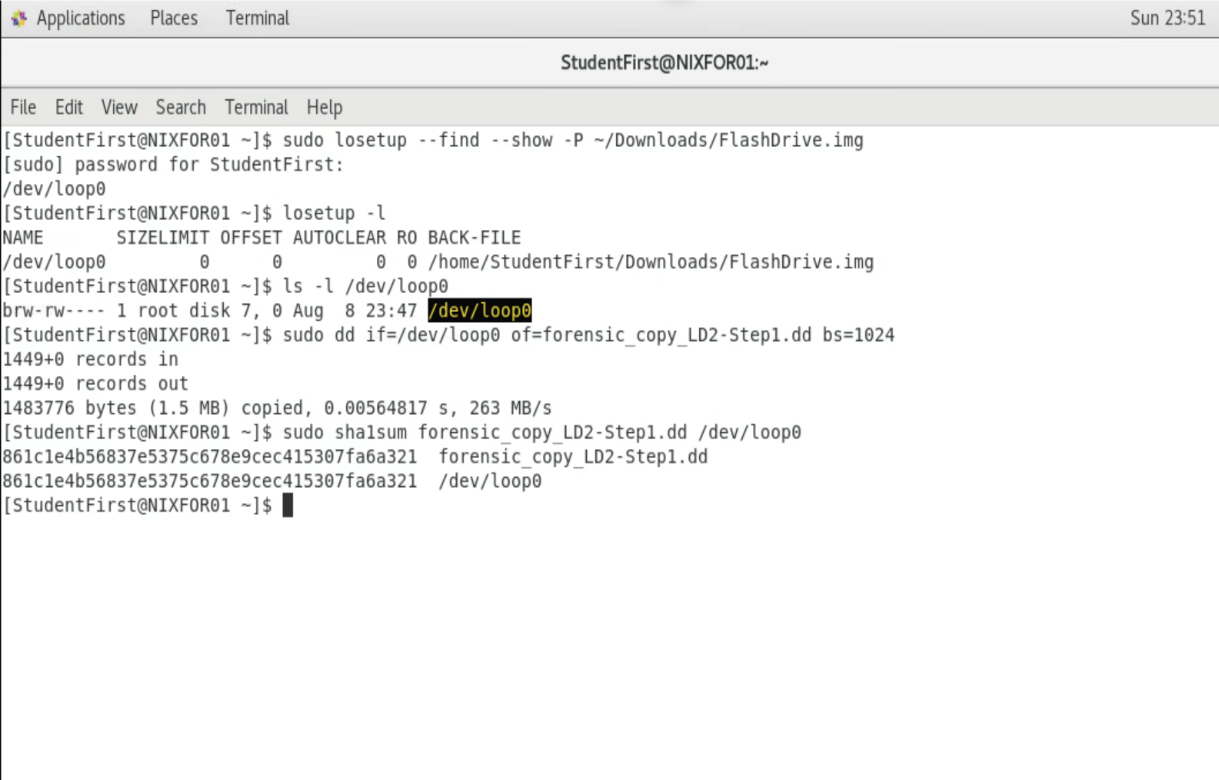
1. I used the mount|grep /dev/loop command to compare my results, the resulting device location is the same as my previous entry.



1. The device is zeroed out.

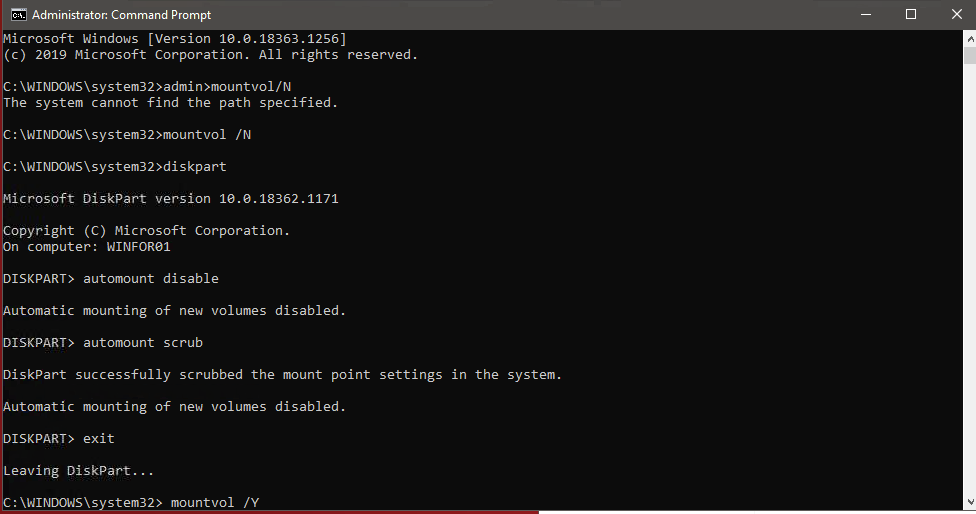


1. I was able to successfully copy the LD2-Step1.dd file to the flash drive stored in the /dev/loop0p1 location. I also confirmed that the SHA1 sums for both LD2-Step1.dd and the /dev/loop0p1 file did indeed match.

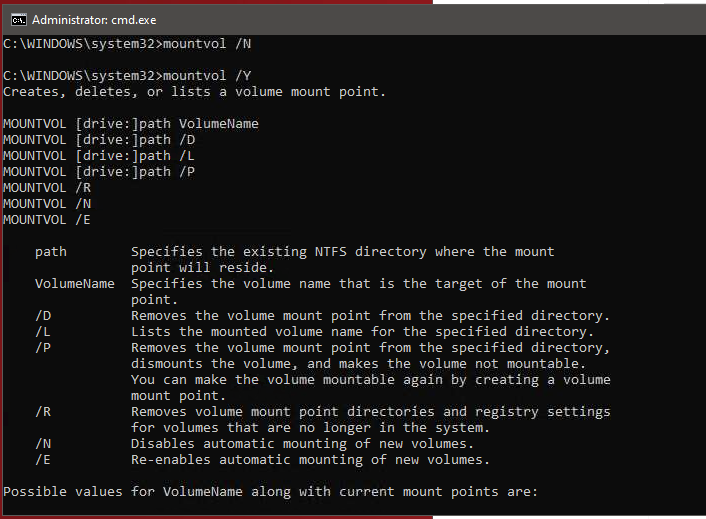


1. After removing the mounted flash drive, I created a forensic copy of the information stored on the flash drive, and confirmed its hash value was equal to that of the original image.

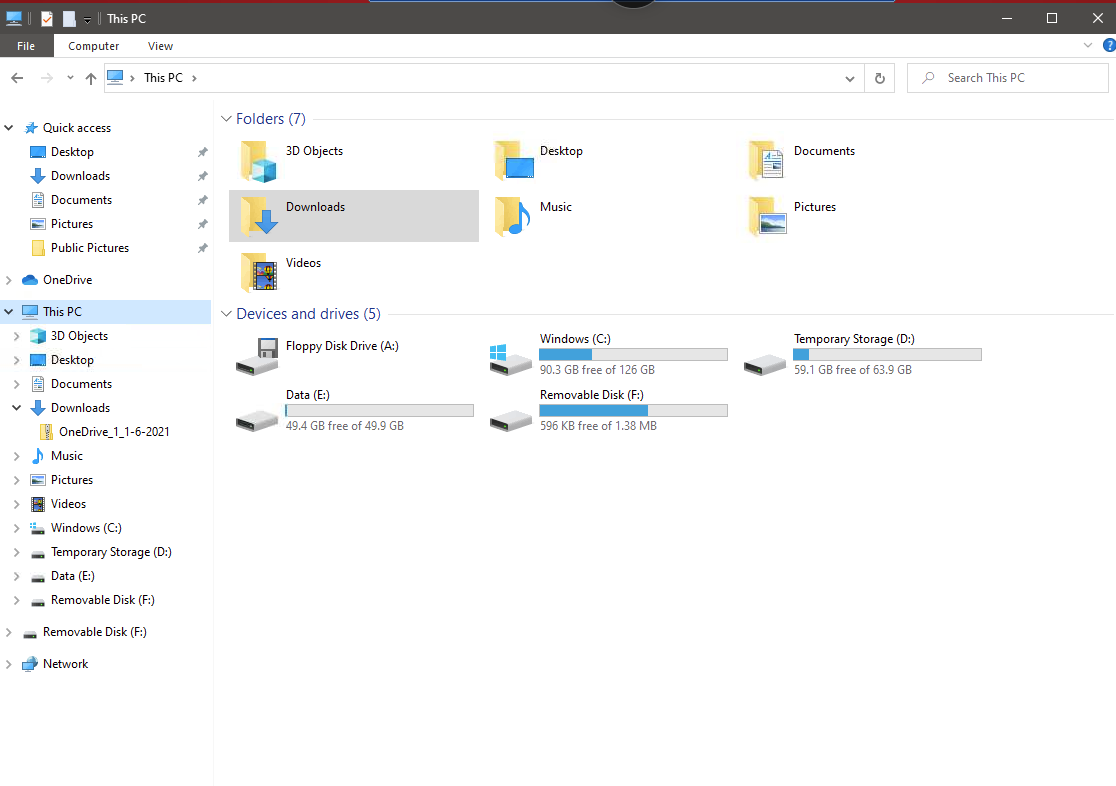
**Imaging a USB Device Using Windows Tools (Step 3)**

****

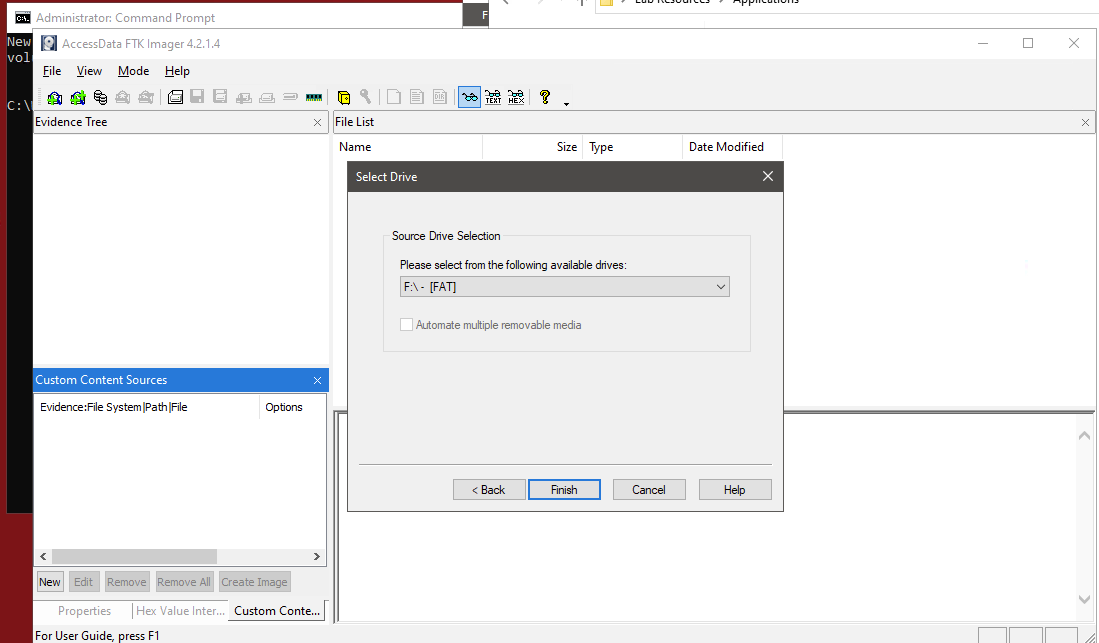
1. Disabling auto-mounting, while logged in as an administrator.



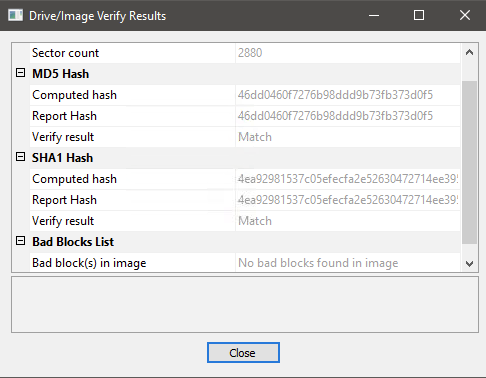
1. Remounting the USB drive



1. Locating the Removable Disk Drive (F:)



1. Selecting the F: Drive in FTK Imager



1. FTK Imaging Verification Results



1. FTKFlash.001 text document contents



1. Unmounting of the (F:) Drive

**Response to Legal Team’s Questions Memo**

**Date: August 6th,2021: 1:37 PM**

**To: ZeroBit Legal Team**

**From: Ifeanyi Uzoukwu; Lead Digital Forensics Specialist**

Your team presented some intuitive questions in response to the imaging I performed on the USB Flash Drive. For the purpose of informing our team about imaging and hashing so they can be as prepared as possible for the impending trial of our soon-to-be ex-coworker, I want to take the time out to respond to the questions you’ve left me regarding the imaging I recently completed.

1. *Assuming that this is a criminal case that will be heard in a court of law, which hashing algorithm will you use and why?*

The Message-Digest 5 algorithm (MD5) and the Secure Hash Algorithm (SHA-1) are amongst the most popular algorithms and are both recognized by most forensic tools, especially seeing as both offer a very low chance of the same hash value being produced in a set. However, there is a crucial difference in quality that makes the SHA-1 hashing algorithm the preferred choice for regular use. MD5 is more susceptible to collision attacks, which finds two different inputs that produce an identical hash value. These clear vulnerabilities make MD5 a risk to use on a regular basis, making SHA-1 the preferred hashing algorithm, even though it is not as fast as MD5. (Geeks for Geeks, 2020)

1. *What if your hashes do not match? What does this mean? What might be the ramifications? What may have caused the hashes not to match?*

When comparing hash values, if they are not matching, this can likely mean that the image itself has been compromised. (Electronic Evidence Retrieval, 2005) This predicament can come back to affect our chances of being successful in trial, seeing as there would be significant issues with trying to get the evidence verified. The digital forensics investigator handling the case would likely have their reputation damaged, seeing as the discovery of two hashes that do not match would likely infer that the images may have been tampered with, which is strictly against the set of ethics that a digital forensics specialist, much less someone that works in law enforcement, is supposed to follow.

1. *What if the OS automounts drives/devices? What might happen if drives/devices are automatically mounted?*

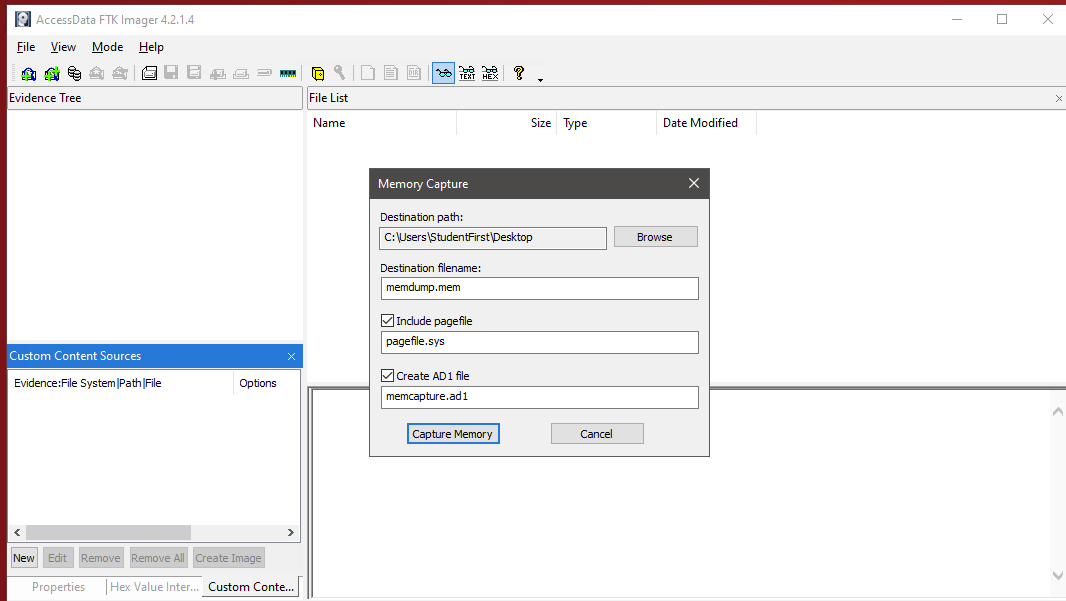
If the OS automounts drives or devices than the digital forensics specialist has made an error in not disabling automounting prior to starting the preservation process. Most competent legal defense teams would argue that due to the fact the information was handled incorrectly, the examiner had a chance to alter the information on the drive in a manner that would have benefitted the prosecution. In this situation any evidence that may have been on the drive being examined will more than likely be rendered inadmissible because of the examiner’s error.

1. *How can you tell the OS is configured****not****to automount the drive? Describe the process.*

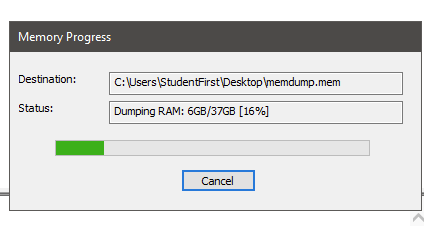
Comparing the hashes of both the Original and Forensic Copy of the images is the easiest way to tell if the drive has been mounted or not. Additionally, executing the command “mountvol/N” or using the diskpart command, which would require opening command prompt as an administrator, typing in the diskpart command and entering, then entering “automount disable”, then entering would result in a message saying “Automount has been disabled”, would allow anyone to check if their device was automounted when it was installed into the imaging device. (Oracle, 2018)

**Acquiring the RAM and Swap Space**

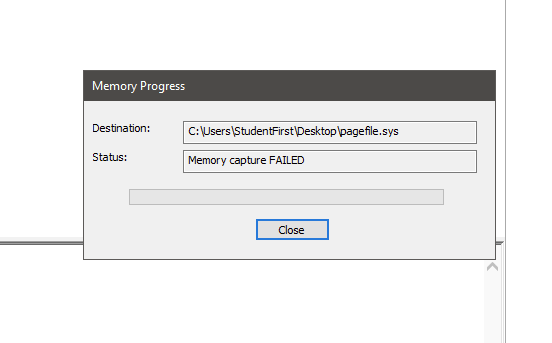
The employee under suspicion is in a meeting, so we have an opportunity to obtain the information that resides in our suspicious employee’s RAM and Swap Space, utilizing the FTK imager tool.



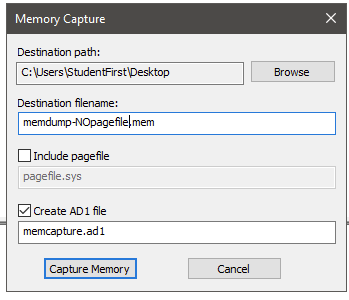
1. Creation of the memory capture file.



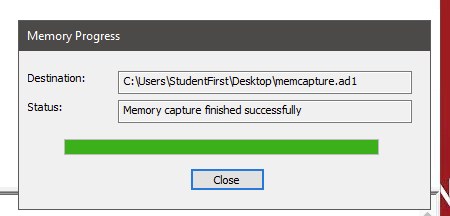
1. Initial Memory Capture is in progress



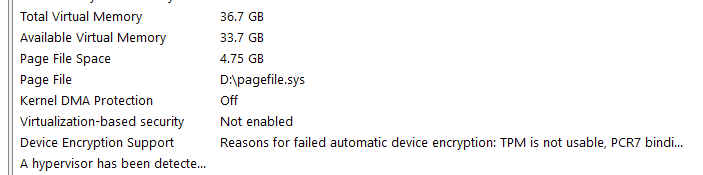
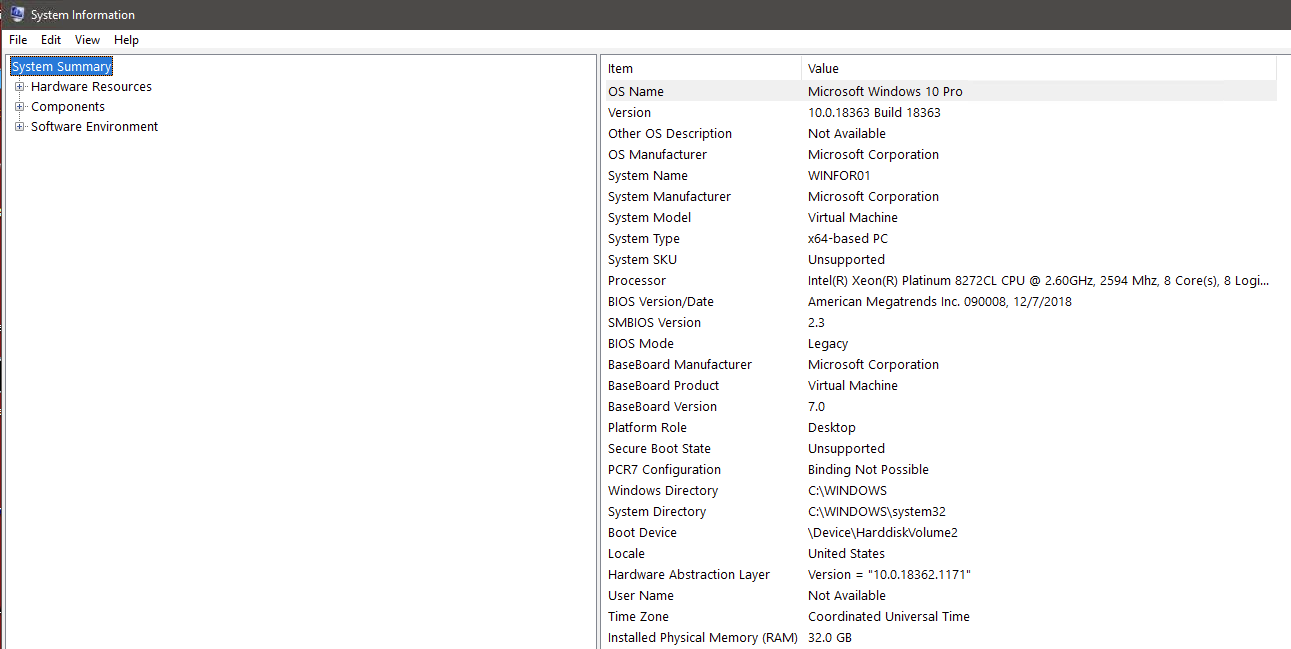
1. Initial Memory Capture failed due to missing Pagefile.sys



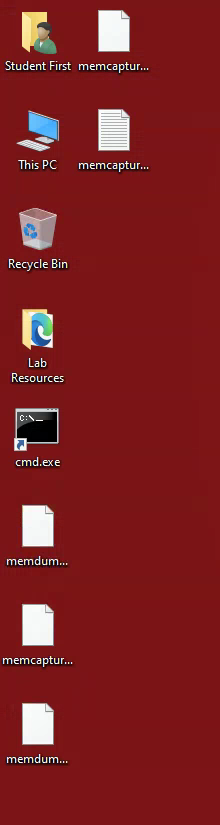
1. Recreation of Memory Capture per, Professor’s Instructions



1. Completion of Memory Capture



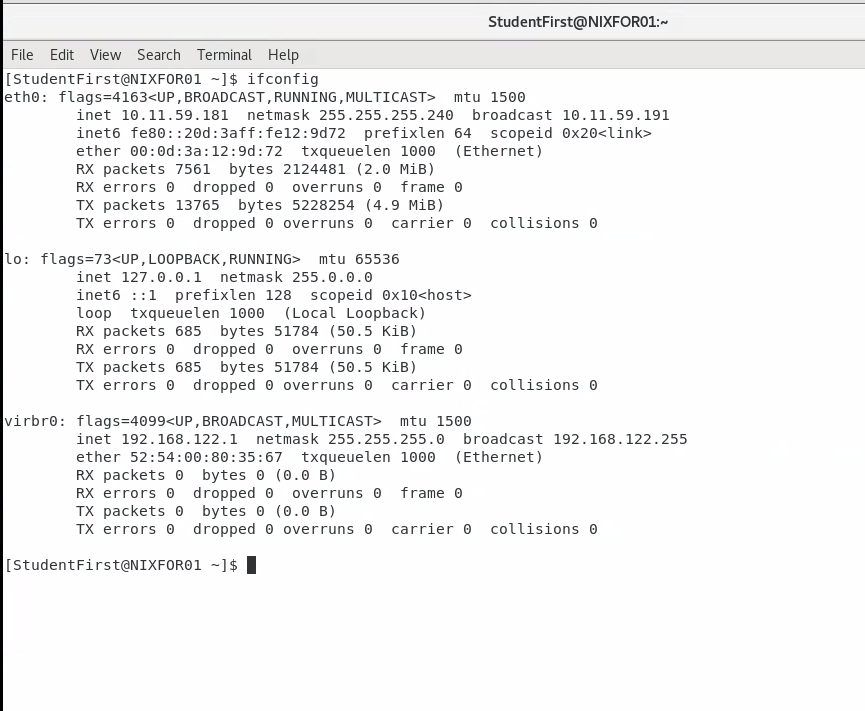
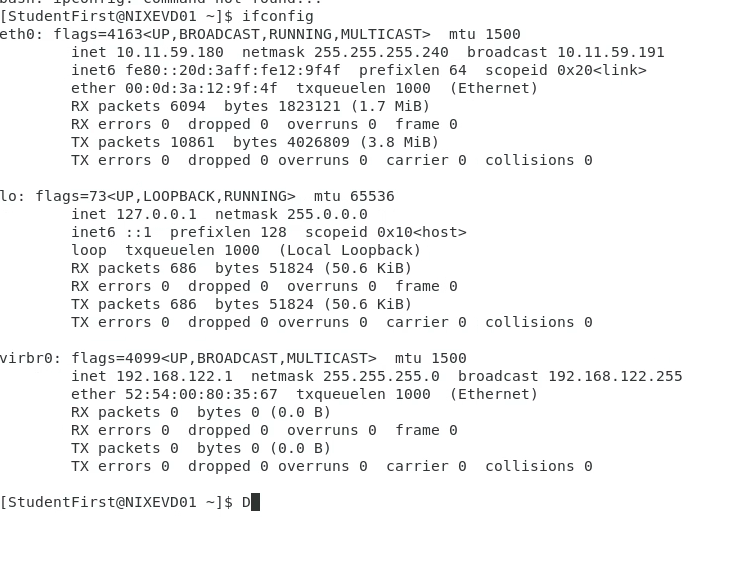
1. System Information



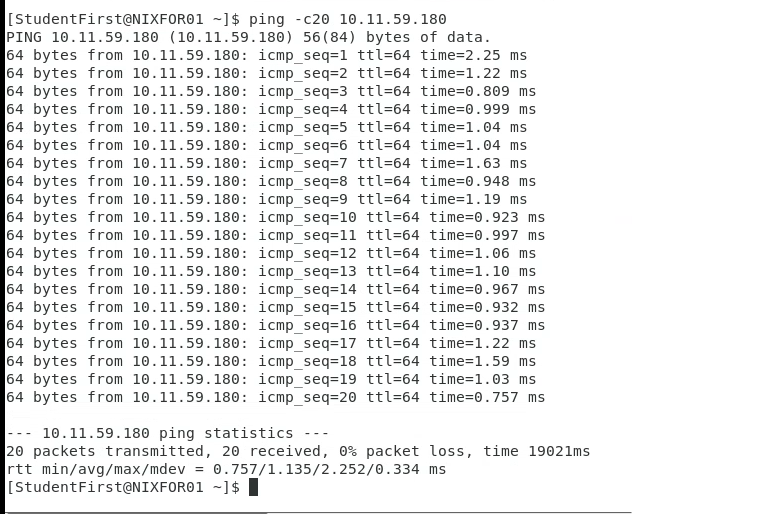
1. Confirmation of the following files: “memdump.mem”, “memcapture.ad1”, “memdump-NOpagefile.mem”, “memcapture.ad2”, and a “memcapture.ad1”, text file. There are five new files available instead of four, this is most likely due to the fact that the memory capture process was ran more than once.

**Forensic Imaging over a Network**

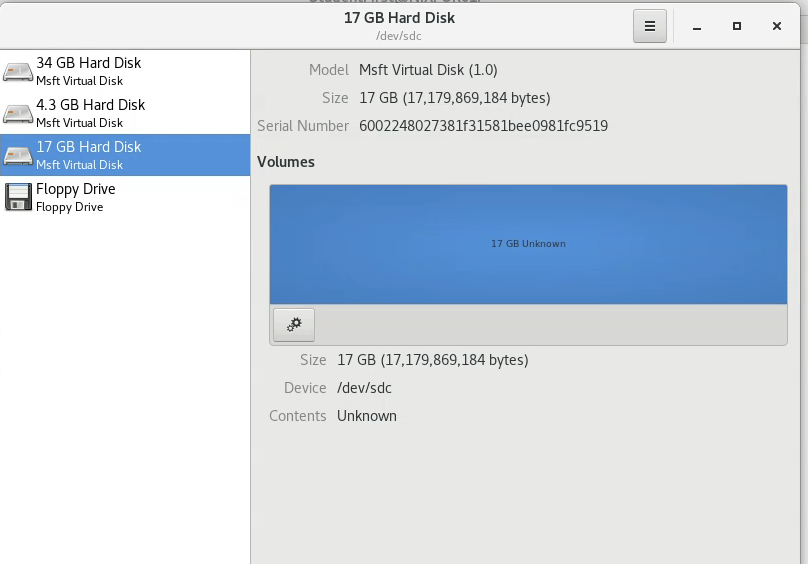
Now that it is the weekend and ZeroBit is certain that our suspicious employee is out until next week, we can go retrieve the information stored on our suspect’s remote computer. The Linux machine, NIXFOR01, will be used to store the information that is available on the Linux machine, NIXEVD01.



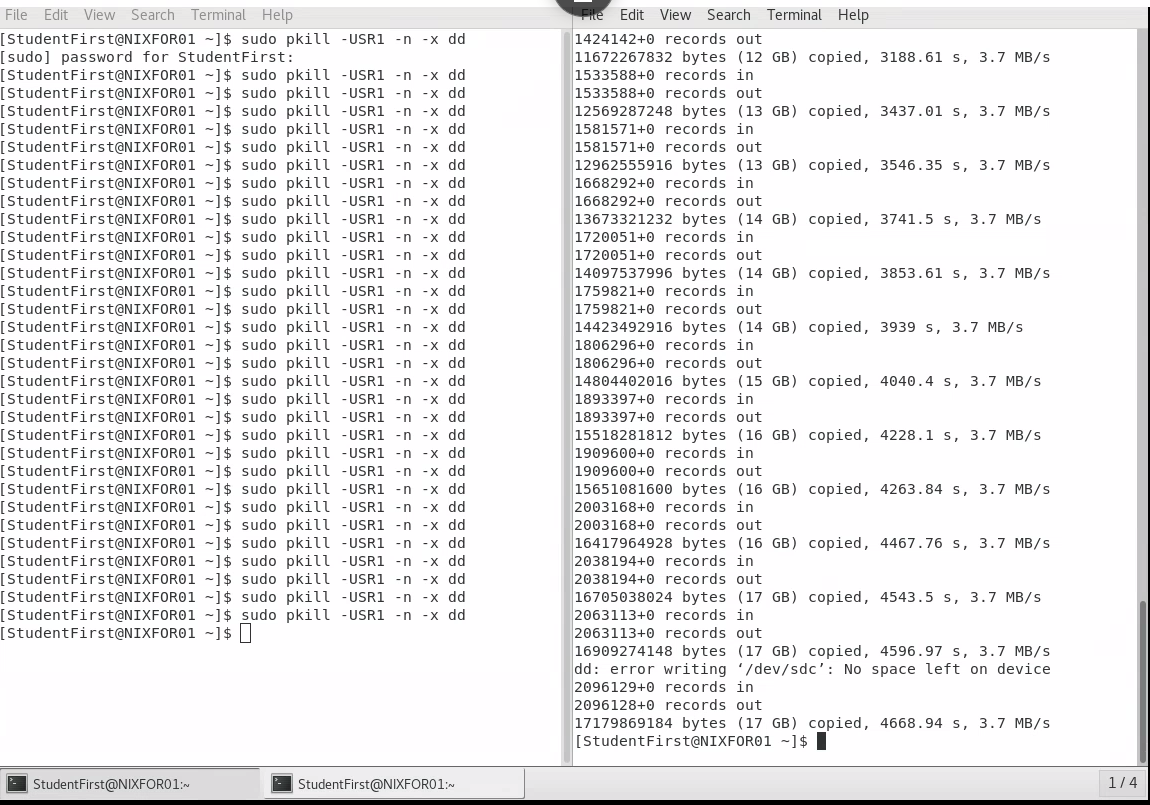
1. These images show the results of applying the “ifconfig” command into the terminals for both NIXFOR01 and NIXEVD01. From these results we could confirm that the IP address of NIXFOR01 is 10.11.59.181, and the IP address of the NIXEVD01 device is 10.11.59.180.



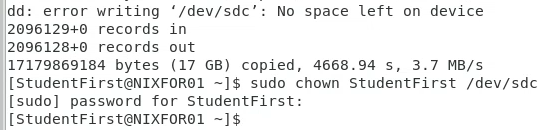
1. This image shows the result of the ping command of the IP address, 10.11.59.180, being executed inside of the terminal application on the NIXFOR01 machine. All packets were successfully sent and received.



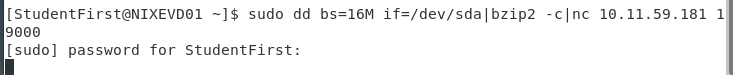
1. This image confirms the existence of the 17 GB Hard drive that our team is imaging.



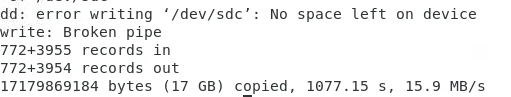
1. This image shows the process that results from zeroing out the 17 GB Hard Drive. The terminal on the left was opened for the purpose of checking on the progress of the procedure.



1. After the device was successfully zeroed out, I had to change the ownership of the remainder of the drive from /dev/sdc to StudentFirst.

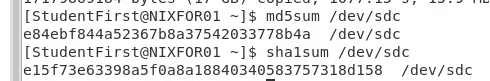


1. After installing the NetCat listener onto NIXFOR01, I executed the command in the image above to retrieve the MD5 and SHA1 sums from the NIXEVD01 device.

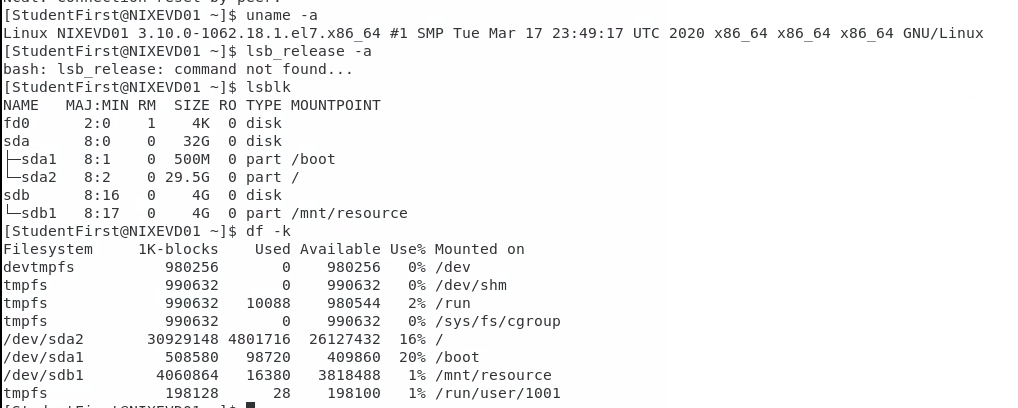
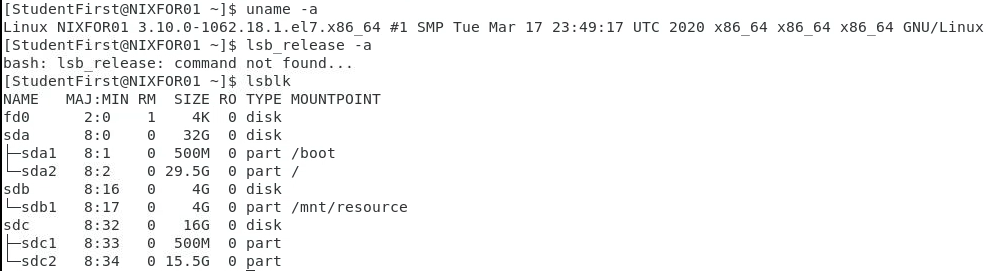




1. This image shows that the connection to the netcat listener reset itself after the process of retrieving the MD5 and SHA1 sums was completed, the second image shows that there was a broken pipe towards the end of the hash retrieval process.



1. The image above shows the MD5 and the SHA1 sums from the NIXEVD01 device.



1. These images show the results of the “uname -a”, “lsb\_release -a” “lsblk”, and “df -k” (only for NIXEVD01) commands when entered into the NIXFOR01 and NIXEVD01 virtual machines. This command shows the system information that was available on each virtual machine.

**Conclusion**

In addition to having a team of experienced digital forensics professionals working beside you, having the necessary tools to extract information safely is paramount to producing evidence that can be presented and admitted into a court of law. Simple procedures like copying and pasting the data from one drive to another is not the most through way to ensure that the information we are looking for can be found or presented.

What is just as important in getting the evidence we are searching for admitted into a court of law is the completion of forms such as the chain-of-custody form. The maintenance of a chain-of custody form goes a long way in assuring to the court that the evidence in our possession was handled responsibly and according to the laws and statutes of our jurisdiction. Using SHA1 and MD5 hashes is a consistent method for authenticating a device, which proves to be useful when admitting the device in question into a court of law. Acquiring the RAM and Swap Space of a drive can prove to be a tedious task, but the reward for being through will surely play a part in the possible conviction of our soon-to-be ex-employee.

**References**

Electronic Evidence Retrieval. (2005). Preserving and protecting computer evidence. Retrieved August 07, 2021, from https://www.electronicevidenceretrieval.com/forensics/articles/preserving-and-protecting-computer-evidence/#:~:text=All%20three%20must%20be%20identical%20for%20the%20image,used%20to%20assure%20the%20integrity%20of%20the%20investigation.

Forensicsware. (2018). E01 (Encase image file format). Retrieved August 06, 2021, from https://www.forensicsware.com/blog/e01-file-format.html

Geeks for Geeks. (2020, July 07). Difference between MD5 and SHA1. Retrieved August 07, 2021, from https://www.geeksforgeeks.org/difference-between-md5-and-sha1/

Johansen, G. (2017, July). Local Acquisition. Retrieved August 05, 2021, from https://learning.oreilly.com/library/view/digital-forensics-and/9781787288683/afb9643b-da47-4c68-a673-79f2f3a8680d.xhtml

Lord, N. (2020, September 29). What are Memory forensics? A definition of memory forensics. Retrieved August 06, 2021, from https://digitalguardian.com/blog/what-are-memory-forensics-definition-memory-forensics

Miller, J. (2018, May 22). What is hard disk? - definition from whatis.com. Retrieved August 06, 2021, from https://searchstorage.techtarget.com/definition/hard-disk

Oracle. (2018, September 25). Enabling Automount for Windows. Retrieved August 07, 2021, from https://docs.oracle.com/en/database/oracle/oracle-database/12.2/cwwin/enabling-automounting-for-windows.html#GUID-6C50678D-7A2C-43F8-9A56-9D85DBE40795

Precise Law. (2017, November 09). What is a forensic image? Retrieved August 04, 2021, from https://discovery.precise-law.com/what-is-a-forensic-image/

Raedts.biz. (2017, August 10). Forensics 101: What is a Forensic image? Retrieved August 06, 2021, from https://www.raedts.biz/forensics/forensics-101-forensic-image/

Special Counsel. (2019, July 05). When to do a Remote FORENSICS collection and 5 more FAQs. Retrieved August 07, 2021, from https://blog.specialcounsel.com/ediscovery/when-to-do-a-remote-forensics-collection-and-5-more-faqs/

TCDI. (2021, June 28). 6 things you should know about Remote digital forensics. Retrieved August 05, 2021, from https://www.tcdi.com/remote-digital-forensics-collection-computer-forensics/