**Project Overview:** This project compares two different digital forensics tools on the basis of their respective acquisition properties like acquisition speeds, hashing methodologies, and graphic user interfaces by undergoing a data acquisition on an approximately 30-gigabyte USB drive containing approximately 15 gigabytes of data.

**Project Relevance:** I chose to conduct this research in an effort to discover which forensic tool has a friendlier interface, which forensic tool better serves the purpose of acquiring data, which forensic tool creates hashes for data more efficiently, and which forensic tool acquires data in a more timely manner and more effectively. In the event that a data acquisition for a digital forensic investigation is necessary, this research can be used as a reference to determine which digital forensic tool is more efficient and convenient to use as well as methodologies used to conduct the digital forensic investigation. The results of this research can be used to create more efficient forensically-sound digital forensics frameworks, tools, and methodologies to forensically-image and analyze data while also maintaining data integrity.

**Methodology:** I compared FTK Imager and Paladin to each other on the basis of data acquisition speeds, hashing methodologies, and graphical user interface friendliness and convenience. During the data acquisition, I kept note of how fast each forensic tool acquired the data, the hashing method used by each forensic tools to maintain integrity, and I was cognizant of which digital forensic tool was easier to navigate.

* **Setup and Environment:** **Setup** - Scenario – GitBusiness, a moderate-size clothing company, is making strides in enhancing its cybersecurity posture. Its SOC team has made the necessary adjustments that are needed to mature its security posture. The digital forensics and incident response team are also making strides to improve its forensics and incident response protocols. To do so, it has hired me as a digital forensics consultant to decide on which forensics tool is more efficient, FTK Imager or Autopsy. The objective is to use identical data, on which to conduct a data acquisition to determine which digital forensic tool is more efficient in its acquisition speed, hashing algorithm(s) used, and graphical user interface usability.  
    
  **Environment** – FTK Imager will be used within a Windows 11 operating system environment. Paladin will be used as a bootable tool within a Linux-based environment.
* **Tools, Frameworks, and Datasets:** One of the tools that will be used is FTK Imager, a free digital forensics tool used to create forensically-sound images of digital devices and data without making modifications to the original digital data or device. FTK Imager also allows for the verification of data by way of MD5 and SHA-1 hashing algorithms and generates hashing reports. The other tool that will be used is Paladin, a Linux-based bootable digital forensics tool, also used to create forensically-sound images of digital devices and data without make modifications to the original digital data or device by having read-only mounting capabilities. Paladin also allows for the verification of data by way of MD5 and SHA-1 hashing algorithms and generates hashing reports. The data that will be used was provided by a distinguished professor of the Digital Forensics and Information Security department of the University at Albany. The data is contained on a (1) 30-gigabyte USB flash drive with approximately 15 gigabytes of data that will be utilized for the data acquisition for each digital forensic tool.
* **Architecture or Workflow:** **Architecture** - The computers used for the FTK Imager and Paladin data acquisitions were approximately 476.83 gigabyte Dell Optiplex 790 computer with an NTFS file system and 259.24 gigabytes of free space on a network.   
    
  **Workflow** – The workflow was to conduct a digital forensic acquisition using FTK Imager first, record the steps of the process, take note of the data acquisition duration, take note of the hashing duration, and take note of the hashing methodology. Then, conduct a digital forensic data acquisition using Paladin, record the steps of the process, take note of the data acquisition duration, take note of the hashing duration, and take note of the hashing methodology. Afterwards, note the process from a graphical user interface perspective.

Step-by-Step Process and Screenshots:   
**Step-by-Step Process - FTK Imager - Evidence Acquisition**

* I created folders within my Export Drive for organization categorization purposes. The folders were: Export, Tool Data, Tool Reports, and Screenshots
* I connected my Export Drive to the evidence media
* I opened FTK Imager version 4.5.0.3 and ran it as Administrator
* I clicked File and scrolled down to Create Disk Image
* On the Select Source window, I clicked Contents of a Folder and clicked Next
* On the Select File window, to select the Evidence media, I clicked Browse and selected the Evidence folder and clicked on Finish
* On the Select Image Type window, I selected Raw (dd) to acquire all of the raw data bit for bit to make an exact copy of the data and I clicked Next
* On the Evidence Item Information window, for Case Number, I entered FTK1. For Evidence Number, I entered 01. For Unique Description, I entered Black and Red Sandisk USB Flash Drive. For Examiner, I entered Craig Perkins. For Notes, I entered BFOR 519 FTK Evidence Acquisition
* On the Select Image Destination window, under Image Destination Folder, I clicked on Browse and selected my Export Drive’s Export Folder. Under Image Filename (Excluding Extension), I entered FTK Evidence 1. For Image Fragment Size, I left it as 1500(MB). For Compression, I entered 0. For Use AD Encryption, I left it unchecked. For Filter by File Owner, I left it UNCHECKED and clicked OK
* On the Create Image window, it shows the directory path for where I am going to save the image. I left this window as it was with the Verify images after they are created box CHECKED. I left the Pre-calculate Progress Statistics box UNCHECKED. I left the Create directory listings of all files in the image after they are created box UNCHECKED. I clicked the Start button
* On the Create Image window, under Image Source, it shows the directory path for the Evidence folder. Under Image Destination(s), I clicked on Add to fill out the Evidence Item Information. For Case Number I entered FTK1. For Evidence Number, I entered 01. For Unique Description, I entered Black and Red Sandisk USB Data Folder. For Examiner, I entered Craig Perkins. For Notes, I entered BFOR 519 FTK Evidence Acquisition
* The Creating Image window showed me the Image Source, Destination, Status of the image creation process, a Progress animation, and Elapsed time.

The Image Creation process took 06:56 (6 minutes and 56 seconds)  
  
  
**Step-by-Step Process – Paladin – Evidence Acquisition**

* I booted the computer with Paladin
* I inserted the Evidence USB flash drive
* I inserted my Export Drive
* I opened the Paladin Tool box at the bottom of the Paladin interface by clicking the Paladin Toolbox icon
* I clicked on the Mount Media folder to mount my Export Drive
* I clicked on the row labeled /dev/sdd1 and clicked the button labeled Mount-RW
* The Export Drive mounted
* I clicked on Imager inside of the Paladin Toolbox
* For the Source label, I selected the dropdown menu and selected /dev/sdc1 Cruzer Glide EVIDENCE 29.82GB vfat
* For the Image Type label, I selected EWF (E01)
* An Image Details window populated
* On the Image Details window, for Case Number, I entered Pal1. For Evidence Number, I entered 01. For Examiner Name, I entered Craig Perkins. For Description, I entered Red and Black USB Flash Drive. For Compression Level, I left it as None and clicked on Done
* On the Paladin Toolbox window, for Destination, I clicked the dropdown menu and selected /dev/sdd1 SanDisk 3.2Gen1 57.28GB vfat. For Label, I entered Paladin Evidence 1. I checked the box for Verify after creation. I checked the box for Segment Size of 2000 and then I clicked Start.

**Results:** For the FTK Imager acquisition on the data, it began at 11:02:51pm and it ended at 11:09:34pm. It took approximately 6 minutes and 56 seconds (06:56) for FTK Imager to create a forensic image. For the Paladin acquisition on the data, it began at 7:58:07pm and it ended at 20:20:11pm. It took approximately twenty-two minutes and 4 seconds (22:04) for Paladin to create a forensic image. After the FTK Imager acquisition was completed, it automatically created hashes using the MD5 and SHA-1 hashing algorithms. After the Paladin acquisition was completed, it also automatically created hashes using the MD5 and SHA-1 hashing algorithms. The graphical user interface for FTK Imager was plain-white, allowing a lot space for data to be output to the screen. The plain interface makes this digital forensics tool boring, unattractive, and causes utilities within the tool to be difficult to locate. Hovering over the different button options within FTK Imager allows for the user to understand what the different tools are used for only if the user has prior experience with digital forensic tools. The process of preparing FTK Imager to conduct a forensic acquisition took more time in comparison to that of Paladin. The graphical user interface for Paladin was yellow, grey, black, and white, making the interface a lot more appealing than that of FTK Imager. Clicking on the second utility in the row of utilities at the bottom of the Paladin interface allows a window to populate that will contain options to begin a forensic acquisition. The process of preparing Paladin to conduct a forensic acquisition was much less tedious and a lot easier to navigate than that of FTK Imager. (Duration for each tool to do the acquisition, hashing algorithms used, and describe the graphical user interface)

**Conclusion:** Based on the results of the FTK Imager acquisition versus the Paladin acquisition, as it pertains to acquisition speed, FTK Imager was considerably faster than Paladin in acquiring the 15 gigabytes of data from the USB flash drive. Therefore, in terms of speed, FTK Imager is the more effective digital forensics tool. Based on the hashing methodologies used by FTK Imager and Paladin, they both used MD5 and SHA-1 hashing algorithms. For both acquisitions, the process of hashing the data began automatically after the acquisition was completed. Therefore, there were not any extra manual processes that the user would have to initiate in an effort to begin the verification process. FTK Imager displayed a verification start time and a verification end time in its acquisition report. Paladin displayed the verification hash, but not the verification start time and verification end time, allowing the user to know the duration of the verification process. Therefore, based on hashing algorithm standards produced by the National Institute of Standards and Technology (NIST), while FTK Imager is more effective at hashing as it pertains to hashing speed and displaying hashing duration on the interface, both MD5 and SHA-1 hashing algorithms are obsolete hashing algorithms due to vulnerabilities. The standard for hashing algorithms are FIPS 180-4 and SHA-2. Based on the graphical user interfaces of FTK Imager and Paladin, while FTK Imager has icons and capabilities that are necessary for a forensically-sound data acquisition, Paladin encompasses a more user-friendly interface that is colorful, more modern, and more engaging. Paladin’s graphical user interface also makes navigating the Linux-based tool more seamless and simplistic to navigate.

Overall, based on acquisition speed, FTK Imager is more efficient at executing acquisitions and more efficient as it pertains to hashing. Based on graphical user interface, user-friendliness, navigational simplicity, Paladin is more efficient. From a student’s perspective, Paladin appears to be a better forensic tool for engagement and learning how to conduct data acquisitions and imaging. From a professional perspective, FTK Imager is a more effective forensic tools as it promotes time metrics and productivity, which is indicated by its faster acquisition speed and hashing speed displays. To innovate forensic tools, more artificial intelligence and machine learning should be incorporated to automate acquisitions. Engineering machine learning models that can conduct digital forensic acquisitions and extract suspicious evidence would be the next step in innovating digital forensics and the digital forensic acquisition, examination, and data analysis process.

**FTK Imager Screenshots:**

**A screenshot of a computer

AI-generated content may be incorrect.**Export Drive Folders

A screenshot of a computer

AI-generated content may be incorrect.  
Export Drive Properties Screenshot

A screenshot of a computer

AI-generated content may be incorrect.  
Opened FTK Imager

A screenshot of a computer

AI-generated content may be incorrect.  
Select Source Window Screenshot

A screenshot of a computer

AI-generated content may be incorrect.  
Create Image Window Screenshot

A screenshot of a computer

AI-generated content may be incorrect.  
Evidence Item Information Window Screenshot

A screenshot of a computer

AI-generated content may be incorrect.  
Select Image Destination Window Screenshot

A screenshot of a computer

AI-generated content may be incorrect.  
Creating Image Progress Window

A screenshot of a computer

AI-generated content may be incorrect.  
Imaging and Verifying Windows Screenshot

A screenshot of a computer

AI-generated content may be incorrect.  
MD5 and SHA-1 Hash Values Window Screenshot

A screenshot of a computer

AI-generated content may be incorrect.  
Image Summary Window Screenshot Part 1

A screenshot of a computer

AI-generated content may be incorrect.  
Image Summary Window Screenshot Part 2

A screenshot of a computer

AI-generated content may be incorrect.  
Access Data Image Summary Text File Screenshot

**Paladin Screenshots:**

A screenshot of a computer

AI-generated content may be incorrect.  
Mounted Export Drive Screenshot

A screenshot of a computer

AI-generated content may be incorrect.  
Paladin Imager Screenshot

A screenshot of a computer

AI-generated content may be incorrect.  
Image Description Detail Screenshot

A screenshot of a computer

AI-generated content may be incorrect.  
Paladin Toolbox Imager

A screenshot of a computer

AI-generated content may be incorrect.  
Paladin Imaging Evidence Screenshot

A screenshot of a computer

AI-generated content may be incorrect.  
Paladin Imaging Evidence with 15 minutes left Screenshot

A screenshot of a computer

AI-generated content may be incorrect.  
Paladin Imaging Evidence with 5 minutes left Screenshot

A screenshot of a computer

AI-generated content may be incorrect.  
Paladin MD5 and SHA-1 Hash Values Screenshot