Introduction: What is the purpose of your project? What problem in digital forensics does it solve?

The purpose of this project is to design a digital forensics tool that is able to collect, organize, and present evidence. In digital investigations, forensic analysts face challenges including a ton of data, information not being organized, and a time-consuming process of gathering critical artifacts. This project also addresses those issues by using a tool that automates the process of collecting forensic data which essentially helps investigators reconstruct timelines, identify suspicious activity, and better understand the events in an incident.

The tool developed in this project gets several important forensic artifacts using Python, such as the system's IP and MAC addresses, operating system details, running processes, installed applications, startup programs, recent system event logs, and the user's default browser. These types of artifacts are used in digital forensics to identify unauthorized activity, trace network connections, and analyze patterns in system behavior. By automating data-extraction tasks using built-in modules, the tool doesn't need any manual commands, and it also lessens the risk of human error when collecting evidence.

Additionally, investigators can interact with the user-friendly dashboard to organize different categories of data, which makes the investigation process more efficient. Instead of running multiple PowerShell commands or navigating system logs manually, the tool organizes these operations into just one single interface. As a result, investigators can recieve information faster, organize evidence more effectively, and reach more accurate solutions during the forensic process. Overall, this tool aims to help digital investigations by combining automation and system analysis into one creating a better forensic experience.

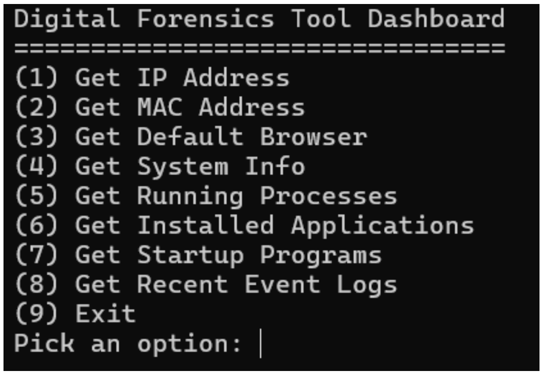
Technical Implementation: Describe the technical details of your project. What languages, libraries, and techniques did you use, and why?

Our tool was implemented in Python. We chose Python as we were most familiar with it and it's easy to implement. We also used many of the Python libraries to build the forensic tool. Our program is made up of several functions that are responsible for collecting different information about computers. To get basic information like the OS, version, and computer name, we used the platform library. To get information about the network like IP address and MAC address, we used socket and uuid libraries with re to format the MAC address. For information like running processes, installed applications, startup programs, and event logs we could not get through python, so we used the subprocess libraries. The subprocess allowed us to run windows commands into PowerShell scripts to find the information needed. Finally, we used winreg library to check the windows registry to find the computer's default browser as winreg stores the systems settings. Then to bring everything together, we made a simple dashboard in which the user can pick an option from the dashboard, and it will run the correct function and show the results. Overall, the project uses Python and built in windows commands to collect digital forensic information in one tool, so it saves time.

Results : Provide a clear outline of the results your tool produces1. Include sample outputs, screenshots, or generated reports.

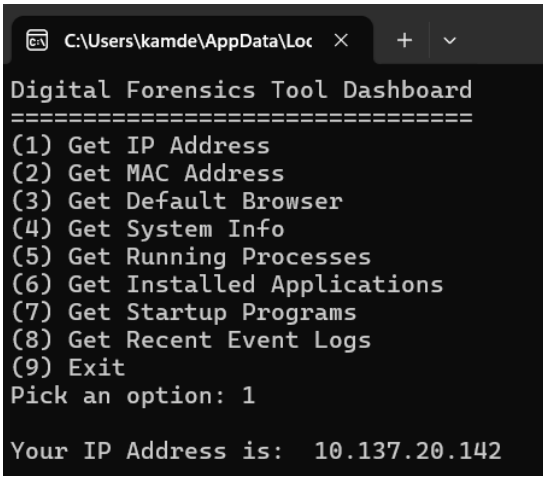
Will provide screenshots of some of the outputs from simple to most important

Dashboard:



```
Digital Forensics Tool Dashboard
================================
(1) Get IP Address
(2) Get MAC Address
(3) Get Default Browser
(4) Get System Info
(5) Get Running Processes
(6) Get Installed Applications
(7) Get Startup Programs
(8) Get Recent Event Logs
(9) Exit
Pick an option: 
```

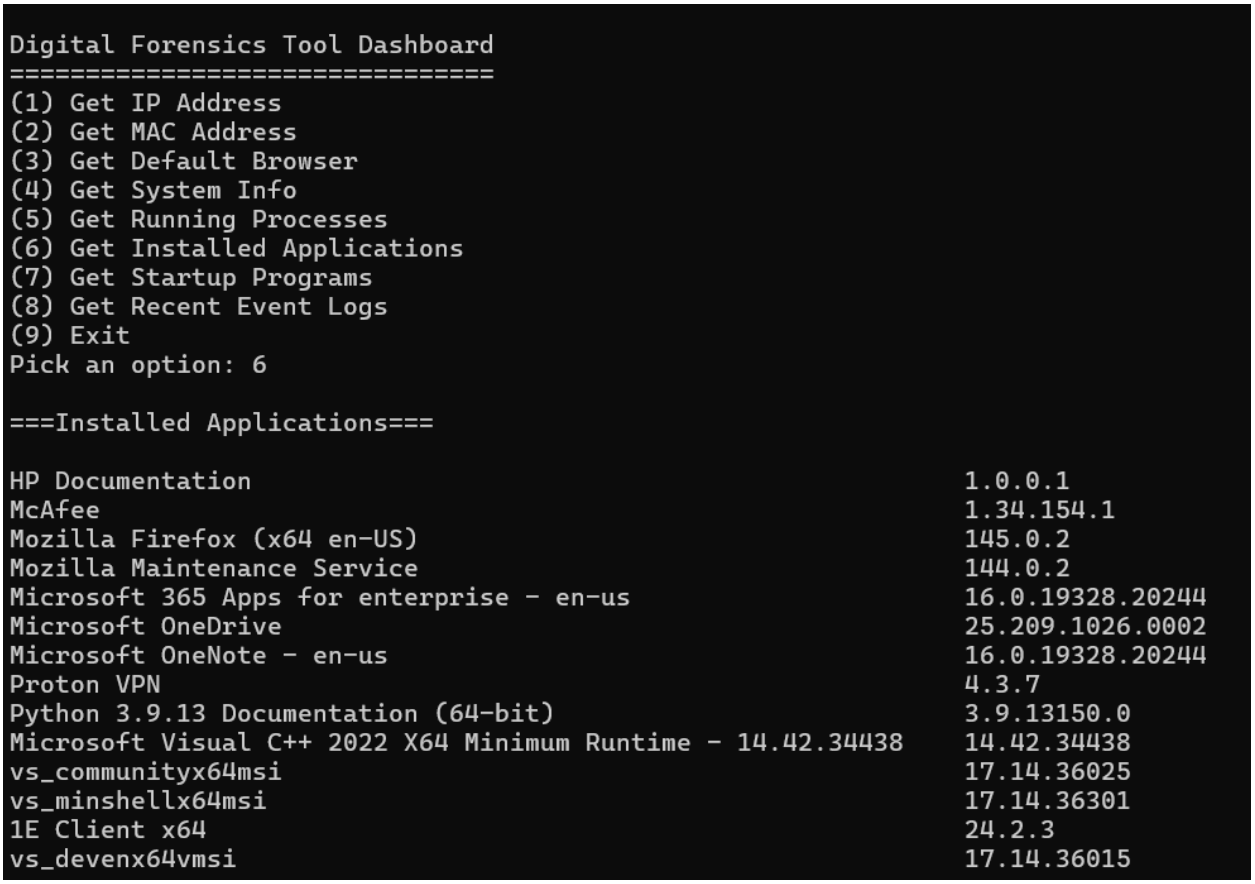
Option 1:



```
Digital Forensics Tool Dashboard
================================
(1) Get IP Address
(2) Get MAC Address
(3) Get Default Browser
(4) Get System Info
(5) Get Running Processes
(6) Get Installed Applications
(7) Get Startup Programs
(8) Get Recent Event Logs
(9) Exit
Pick an option: 1

Your IP Address is:  10.137.20.142
```

Option 6:



```
Digital Forensics Tool Dashboard
================================
(1) Get IP Address
(2) Get MAC Address
(3) Get Default Browser
(4) Get System Info
(5) Get Running Processes
(6) Get Installed Applications
(7) Get Startup Programs
(8) Get Recent Event Logs
(9) Exit
Pick an option: 6

===Installed Applications===

HP Documentation                                               1.0.0.1
McAfee                                                         1.34.154.1
Mozilla Firefox (x64 en-US)                                    145.0.2
Mozilla Maintenance Service                                    144.0.2
Microsoft 365 Apps for enterprise - en-us                      16.0.19328.20244
Microsoft OneDrive                                             25.209.1026.0002
Microsoft OneNote - en-us                                      16.0.19328.20244
Proton VPN                                                     4.3.7
Python 3.9.13 Documentation (64-bit)                           3.9.13150.0
Microsoft Visual C++ 2022 X64 Minimum Runtime - 14.42.34438    14.42.34438
vs_communityx64msi                                             17.14.36025
vs_minshellx64msi                                              17.14.36301
1E Client x64                                                  24.2.3
vs_devenx64vmsi                                                17.14.36015
```

Lessons Learned & Conclusion: Conclude your report with a section on lessons learned. This section should detail what did and didn't work during your project development and what you would do differently in the future.

When developing this project, we learned several lessons which helped us throughout the building of this tool. One key success was our automation system of data extraction. This approach helped us lower the chance of any human error. Our dashboard interface was also something that went well for in our project development. It made navigating the dashboard easy and we can tell for investigators that they'll have no problem organizing their evidence and inputting data. Some challenges included formatting data, advance procedures/methods, troubleshooting and also learning github repositories and libraries. In the future, we would definitely focus more time on early troubleshooting to save us time. Along with that, having different methods than ones were used to would help us and add more creativity into our tool. Overrall this tool helped us understand real world application of digital forensics and how their tools can be used in real world scenarios.