Based on the expertise I have gained throughout the years, navigating this case has allowed me to find evidence through various forensic suites to come to a conclusion on whether or not Mr. John and Don Doe are guilty in the crime of the DOA Arms robbery.

A screenshot of a computer

Description automatically generated

Firstly, using FTK Imager, I was able to open the forensic image and navigate the system to document it and look for suspicious information. I am able to confirm that the file system used for this system is NFTS and it has one volume installed on it. They are also using a Windows operating system as can be seen in the root folder. There are also four users on the system with the “john” folder being the user of the system owner. Though there isn’t a folder to show they are working on a VM, they do have VMWare installed which may hint at the possibility of a VM being used.

A screenshot of a computer

Description automatically generated

To look for and analyze artifacts in this computer, I used FTK Imager, Autopsy, and Paraben’s E3 to navigate the system, find suspicious artifacts of evidence and analyze them. As there are many files on this image, I narrowed down my searches by using each system’s search feature in important parts of the image to look for incriminating evidence like DOA Arms or searches for “guns”.

A screenshot of a computer

Description automatically generated

When looking through the search history of John’s account in E3’s data triage, there were several searches made looking at DOA Arms and looking at a map from Manassas to DOA Arms on January 10, 2023, which was saved as a PDF file on the computer. There were also several other searches made on Google Maps looking at the distance from Manassas to High Velocity Arms which is another gun store. John had also saved an image of the store on his computer and a location which can be presumed to be a gun store.

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

John had also installed suspicious software on this computer which allows him to be able to hide information from others. This software includes Tor browser, steghide, wipefile, tails operating system, and HxD hex editor which were found in E3’s data triage and downloads/desktop folder, FTK Imager’s evidence tree, and Autopsy’s data artifacts web searches. These tools look to be installed on or around January 11, 2023. Using Tor browser, he is able to make searches that can’t be tracked and look in the dark web to find information he wouldn’t be able to find using a regular browser. With steghide and wipefile, these tools allow him to hide information in files and wipe information from files. Tails operating system uses Tor browser to prevent tracking and surveille, and HxD hex editor allows for the manipulation of files’ binary data. There are also suspicious searches made of how to delete a file from a folder permanently, and if you can wipe a folder using minitool partition wizard.

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

On January 10, 2023, John made many suspicious searches surrounding the recent DOA Arms robbery and the laws surrounding selling guns in Nevada. Through web history on Autopsy and Google search history on the data triage in E3, there were searches about a police gun theft in Virginia Beach, the ATF paper trail of guns, and how guns are tracked. These searches make it clear that he is interested in the recent theft that happened in Virginia Beach and how the ATF tracks guns. Other searches made include the gun laws in Nevada and Virginia, selling guns out of state, the price for a handgun and the background check, and gun transfer without tracing. The searches made show that John is looking into the gun laws in both the state he lives in, Virginia, and Nevada. He is also looking into how to sell guns out of state and transfer them without tracing, the price of one handgun and the background check process. These are very suspicious searches to be making which all relate to the recent gun shop robbery and how to sell guns in other states without being traced.

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

A computer screen shot of a blue box

Description automatically generated

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

There have also been searches for flights from Washington’s IAD airport to Guatemala on January 11, 2023, which is the same time the other searches have been made. John could be looking to sell the guns and then escape to Guatemala to not be caught.

A screenshot of a computer

Description automatically generated

Based on the evidence that I have found, I can conclude that the suspect is guilty based on the overwhelming amount of suspicious information that was found. Firstly, there was a lot of suspicious software installed on the computer like Tor browser and steghide which would allow him to hide information and make searches in the dark web. There were also searches looking at the distance from Manassas to DOA Arms which happened before the robbery that shows the suspect was looking at the location and its distance beforehand. Lastly, the suspect had been searching for the robbery that happened, how the ATF tracks guns, and how to sell guns out of state without being tracked. These searches prove that the suspect is gaining information on the gun tracking process of the ATF and how to sell guns that can’t be tracked to allow him to not be found. There were also searches from IAD airport in Washington to Guatemala after the robbery happened which shows the suspect is looking for an escape. Based on this evidence, I personally believe the suspect is guilty.