Cyber Range Lab Assignment 2

Computer Forensics

Jon Mahoney

SRA 440W

# General Context

In this second lab assignment, there are six lab activities. The first lab, “Command Line Basics for Forensics”, acts as an introduction to computer forensics within Linux. The lab Iterates upon previously established commands for navigating Linux OS as well as providing additional information on notable commands such as ‘find’, ‘grep’, and ‘rm’. The lab briefly describes practices used for computer forensics and such as implementing write blockers to prevent writing over a drive that is being examined. The second lab, “Recovering Data” provides a walkthrough of password storage in Linux and a brief introduction to the password cracker John the Ripper. The lab begins with the process of making the /etc/passwd folder vulnerable to John the Ripper using the unshadow command, creating passwords to be acquired, and then viewing the observing the acquisition process in another console and determining the process ID. The third lab, “Hash Databases”, describes hashing and why it is significant. For instance, the lab describes the process of comparing a file’s cryptographic hash to a hash stored in a database to determine if it was altered. As stated in the lab, any alteration will completely modify the hash value of the file. The hash function used in the lab is SHA-1 which produces a 40-digit long digest.

The next lab, “File Carving” looks at two data carving tools known as Foremost and Scalpel. In computer forensics, disk images are defined as a file which contains all data from a storage drive including the structure and format. These disk image files have the .dd file extension and are examined using file carving tools. As for the other tool, Scalpel, the lab walks through the process of editing the Scalpel configuration file so it can be enabled and used for viewing specific files. The last two labs involve the use of a forensic utility called Volatility. The first of the two, “Memory Forensics with Volatility”, involves investigating an event where someone was sent a malicious link. In order to investigate, the user must navigate to the memory dump (snapshot of RAM) to locate the malicious activity. Additionally, the lab points out the value in examining clipboard contents as well as downloads. As stated above, the next lab is similar in nature. The main difference is the environment meaning many of the commands are similar in nature, but I also made use of commands to view network activity.

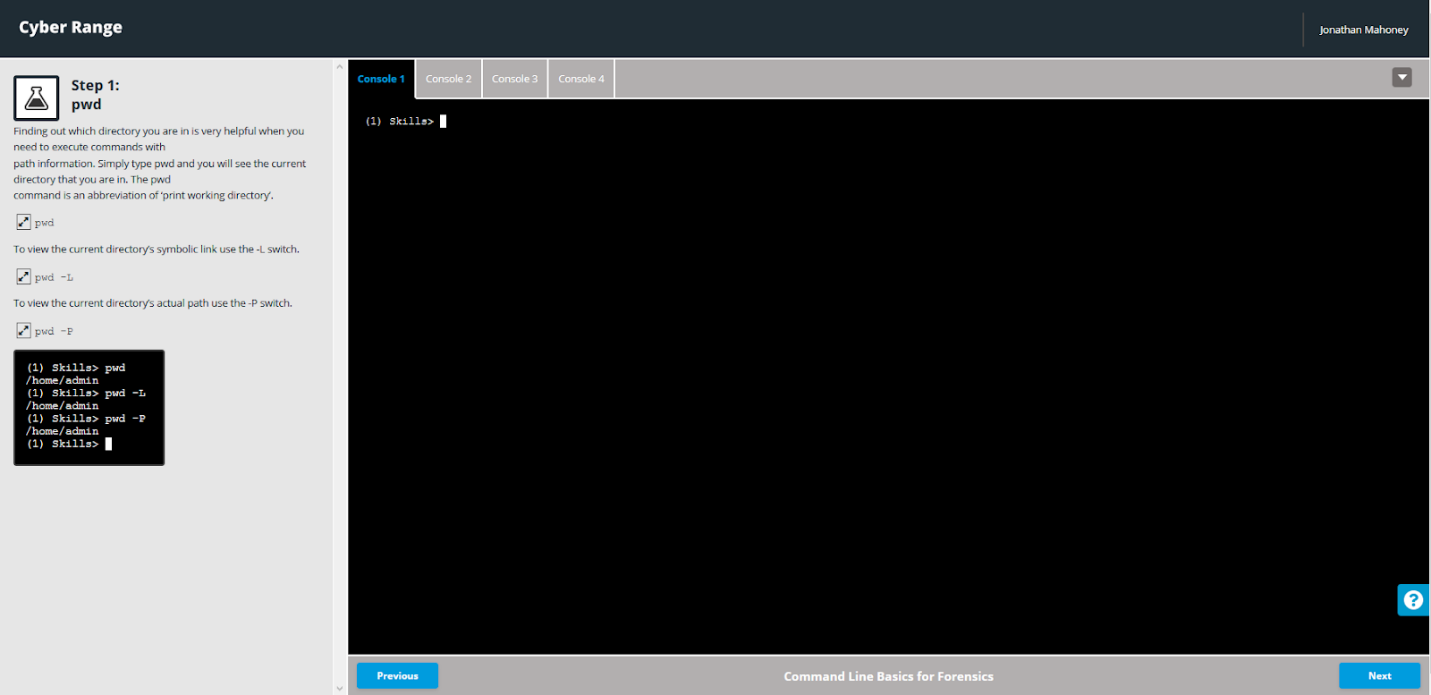
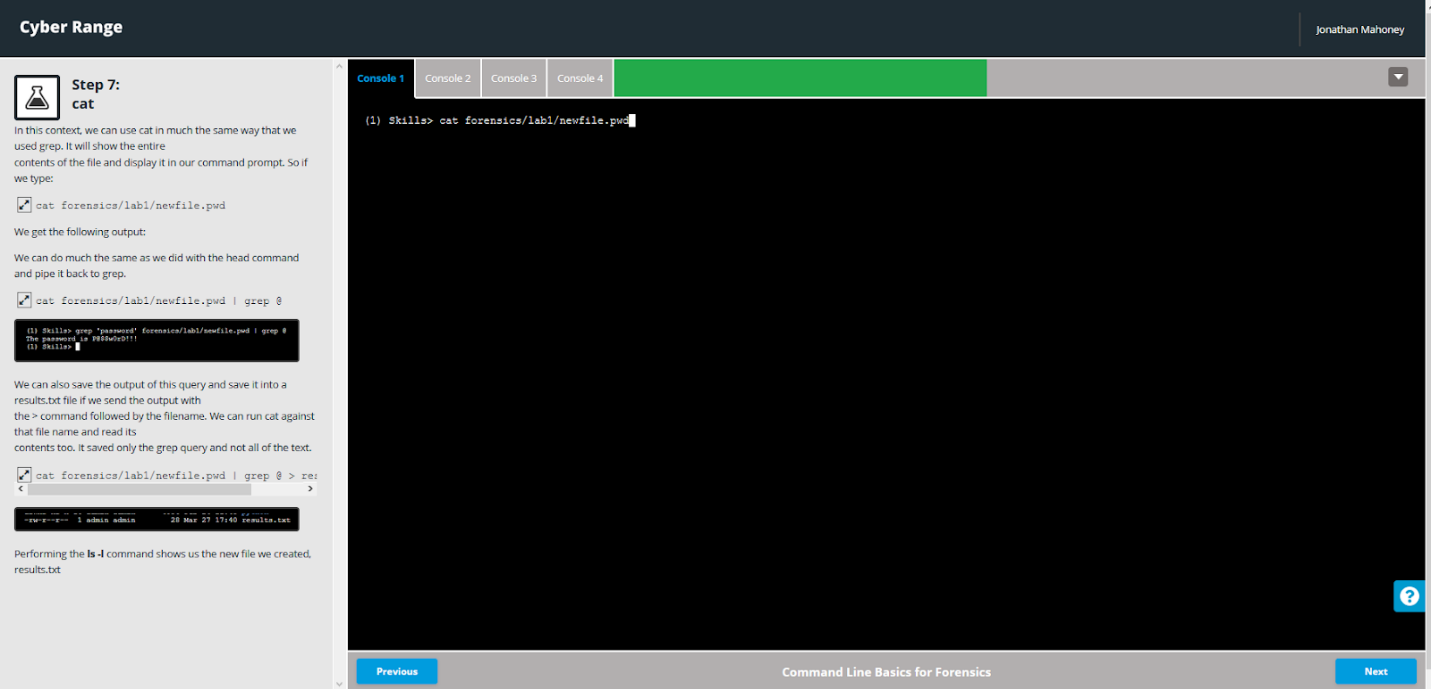
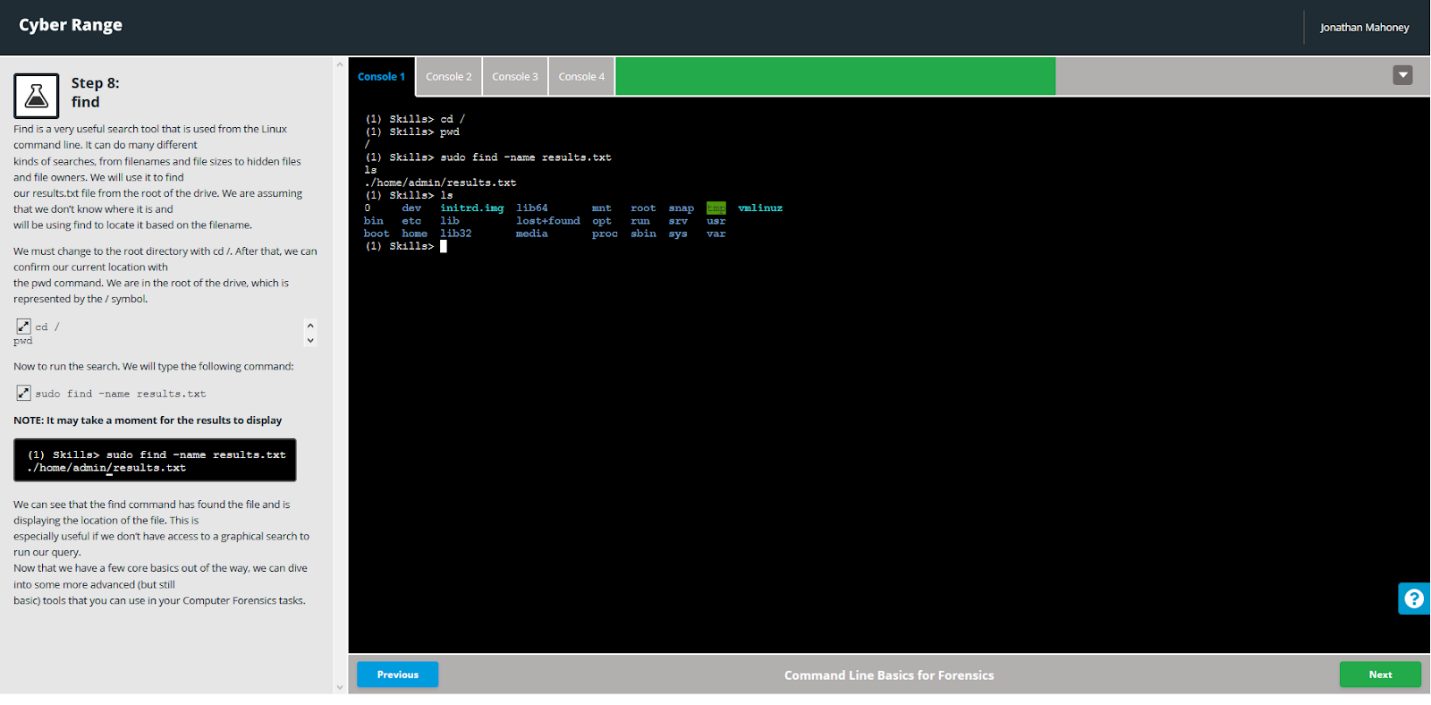
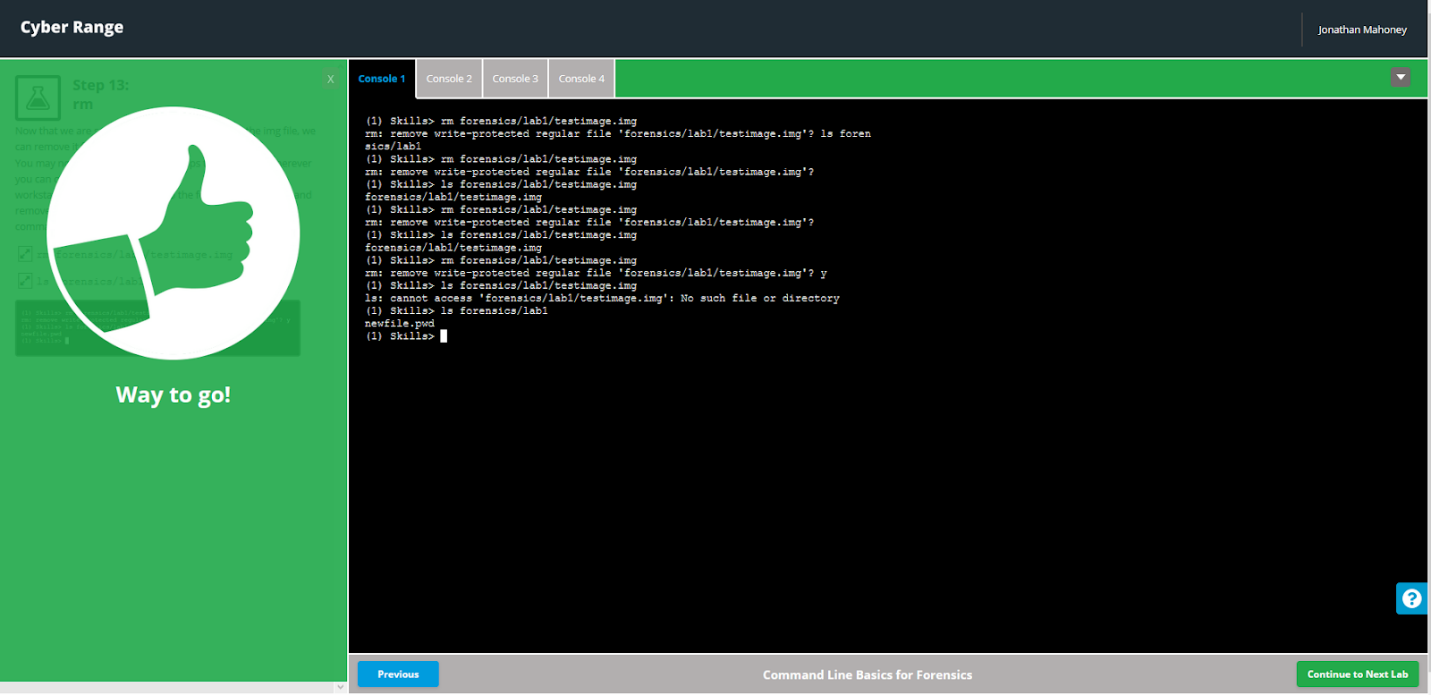
# Solution

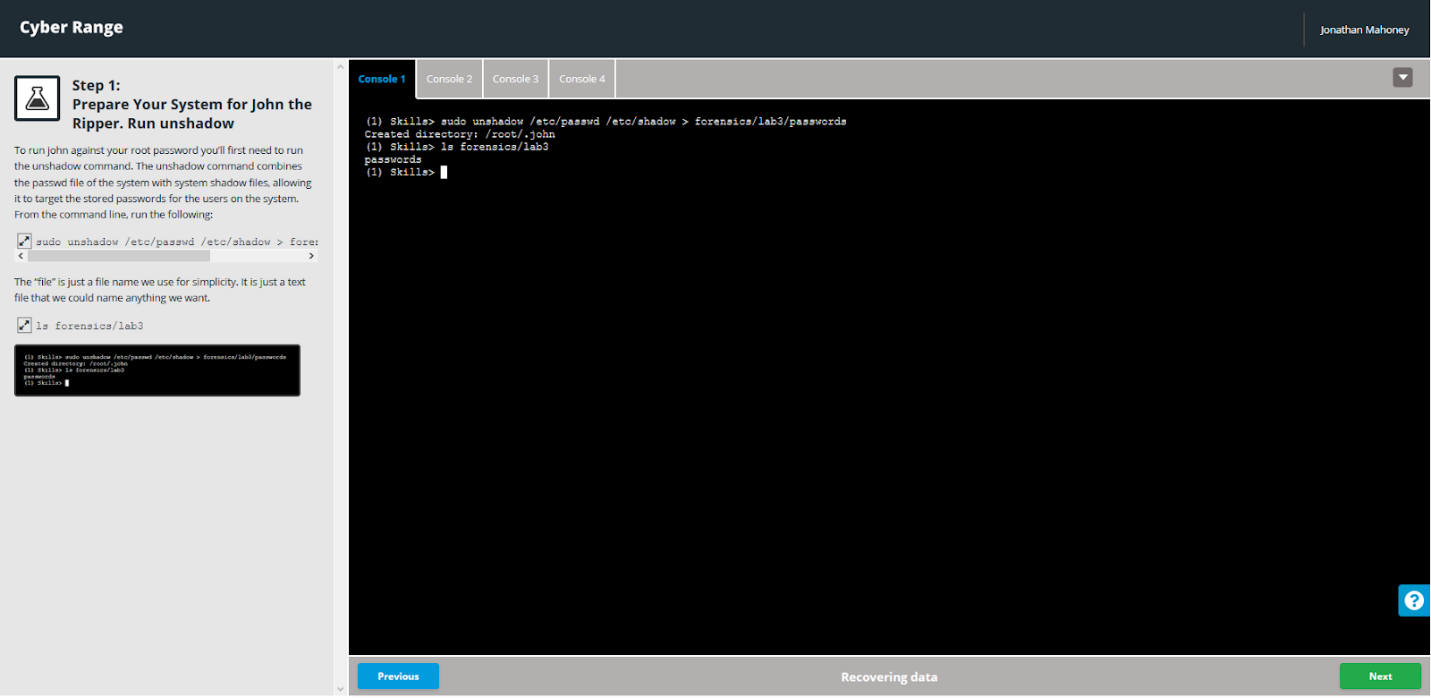
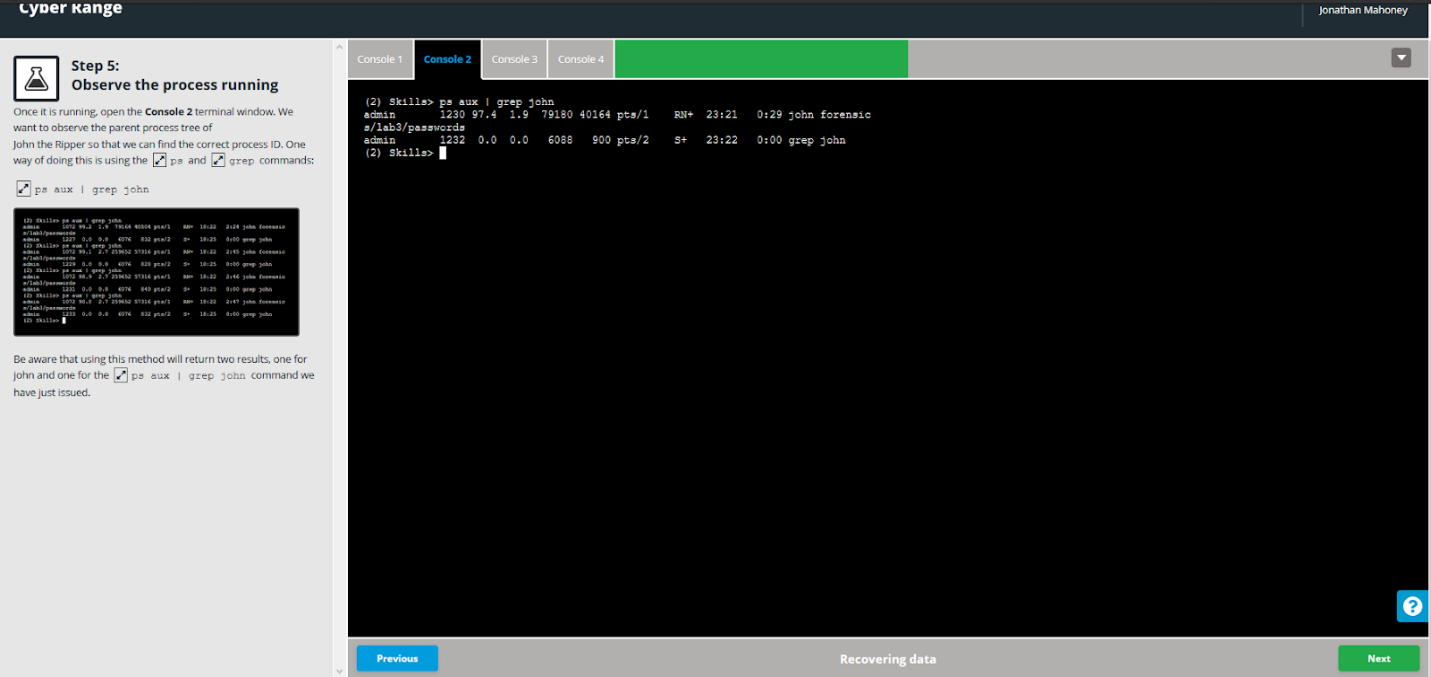
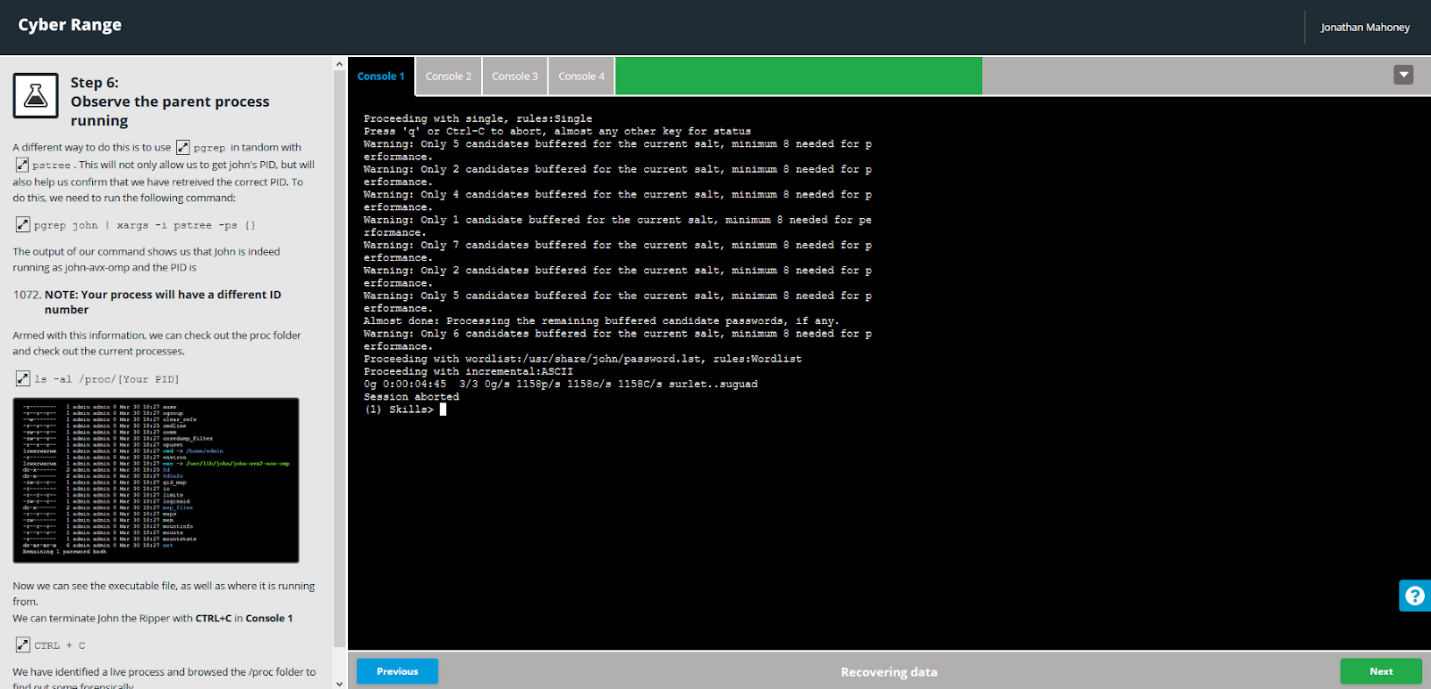
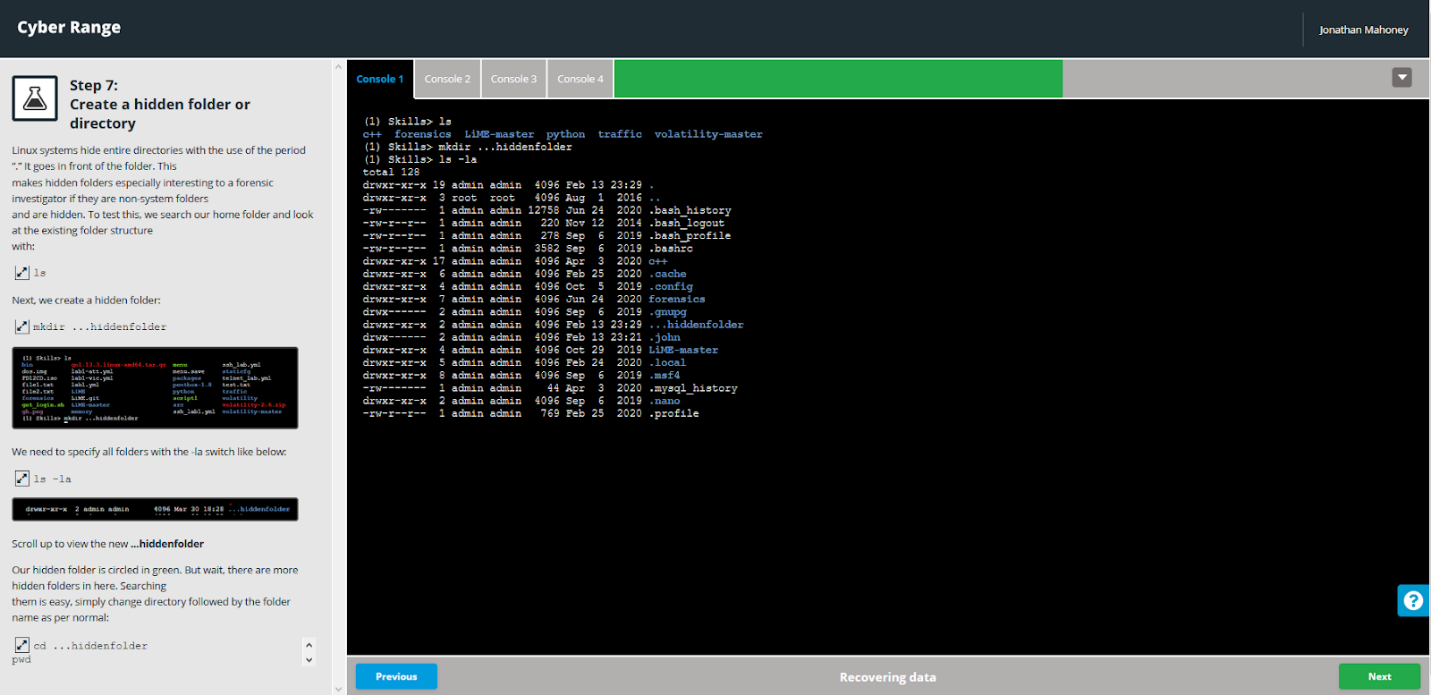
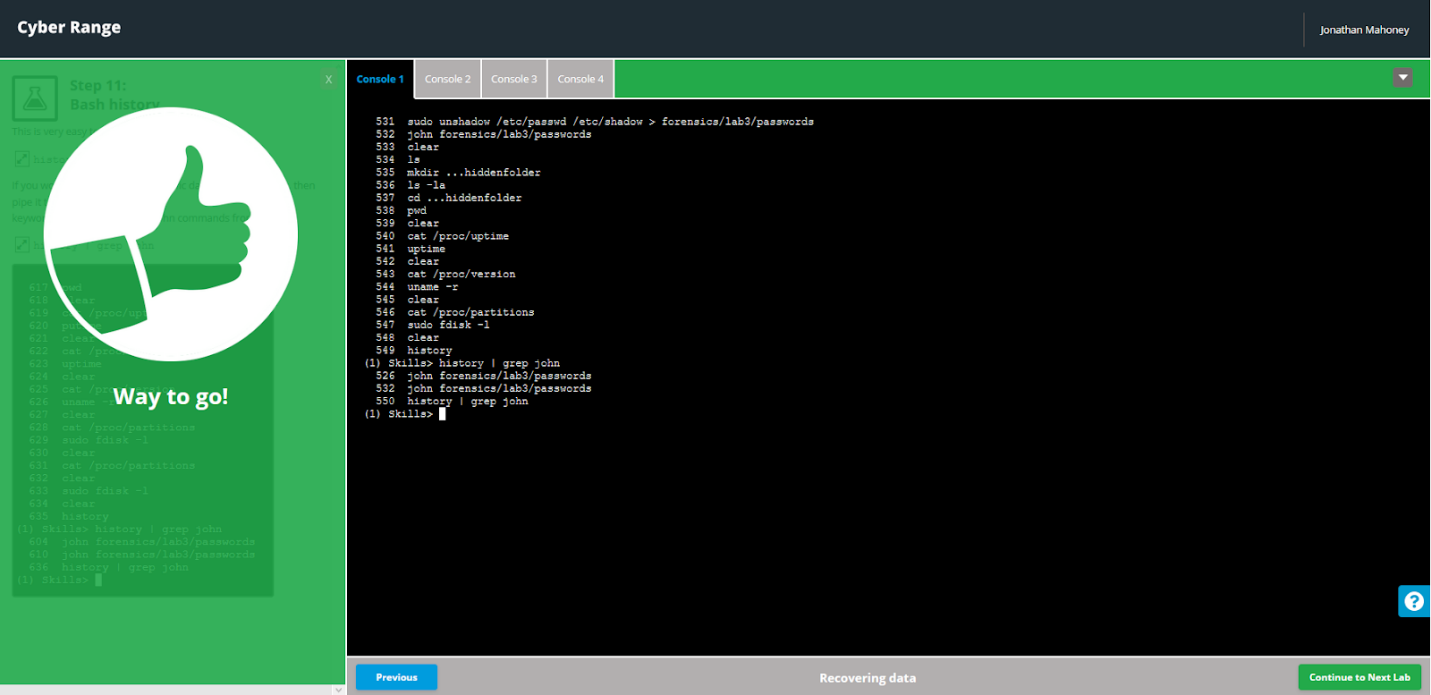
I ran into a few issues during a few of the labs where I completed all the steps, but I was not directed to the next section. When this occurred, there were no additional instructions and I had completed the given task. There was one instance where the error was on me as I had failed to realize I was stuck in the nano text editor and I failed to properly navigate back to the command line. Additionally, the volatility lab steps took exceptionally long to complete. At first, I thought I was doing something wrong but then I stepped away from the lab and returned shortly to find the step had completed. It was then that I realized the steps were working correctly, they were just taking upwards of 5-10 minutes to complete.

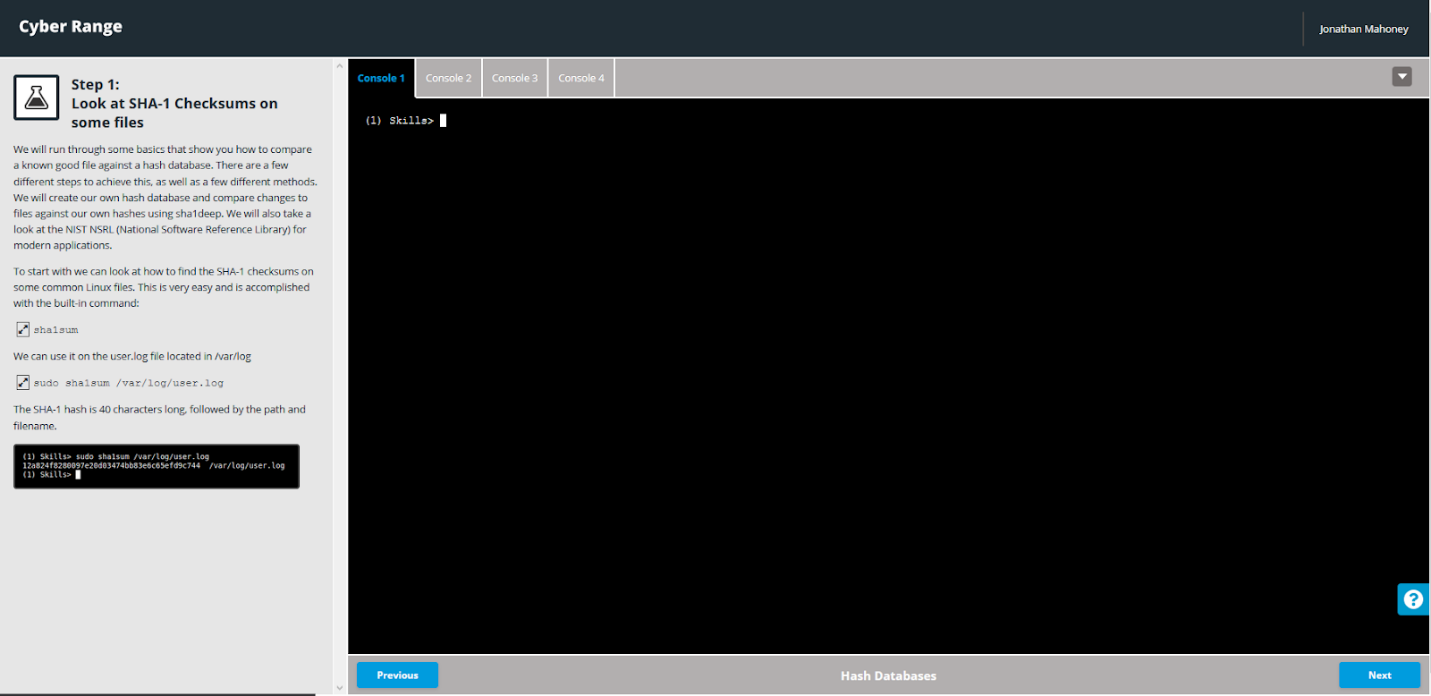
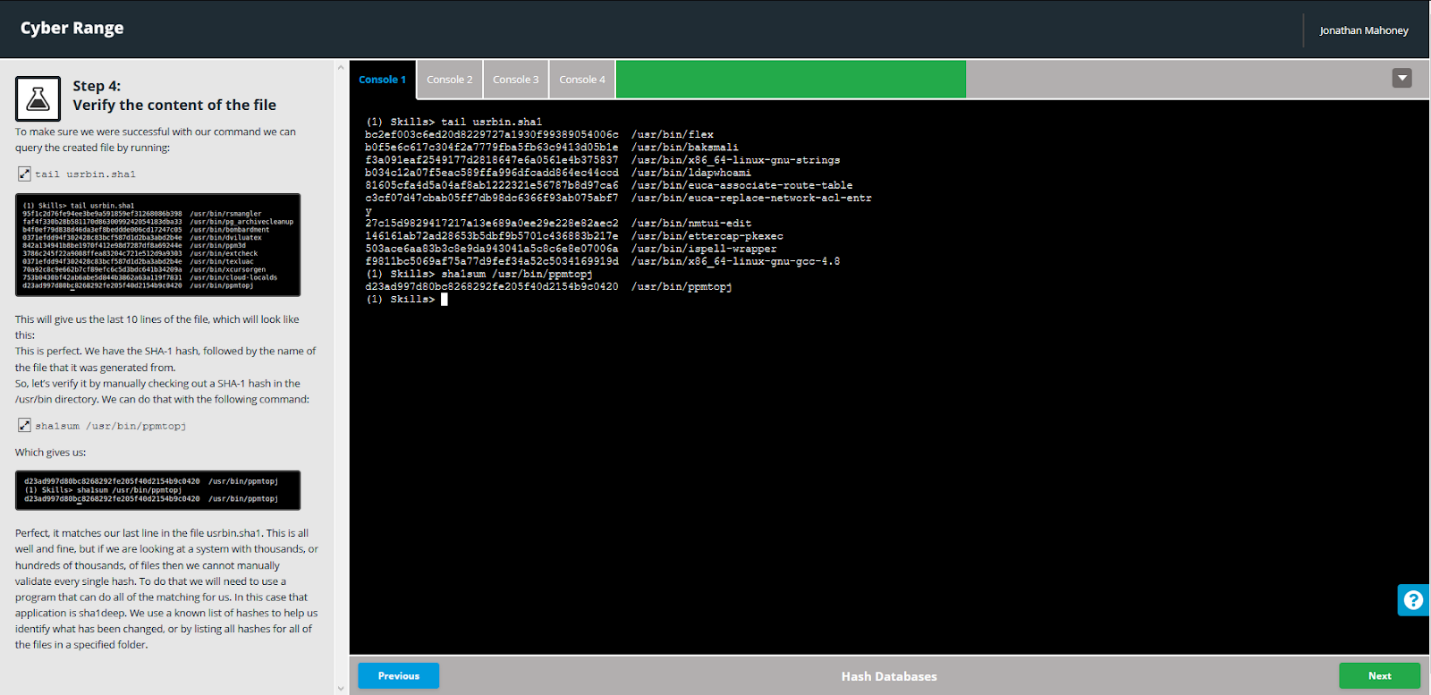
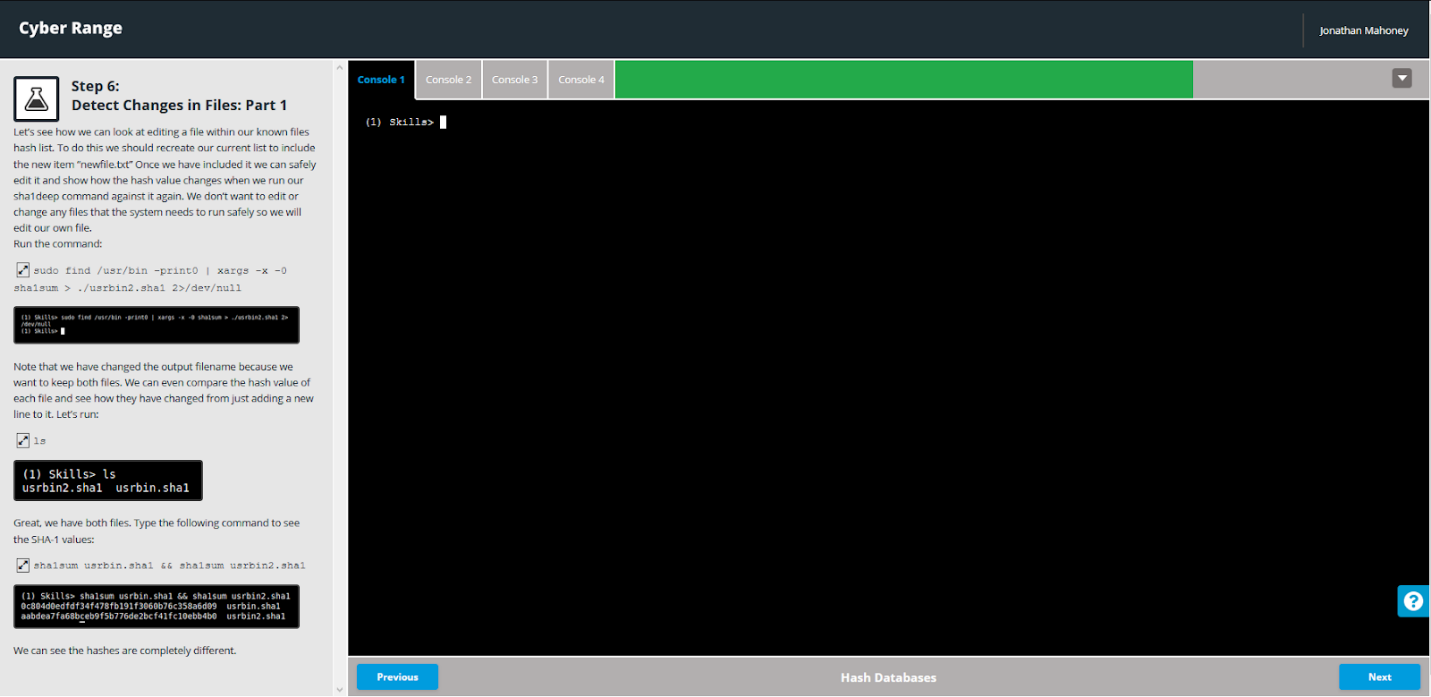
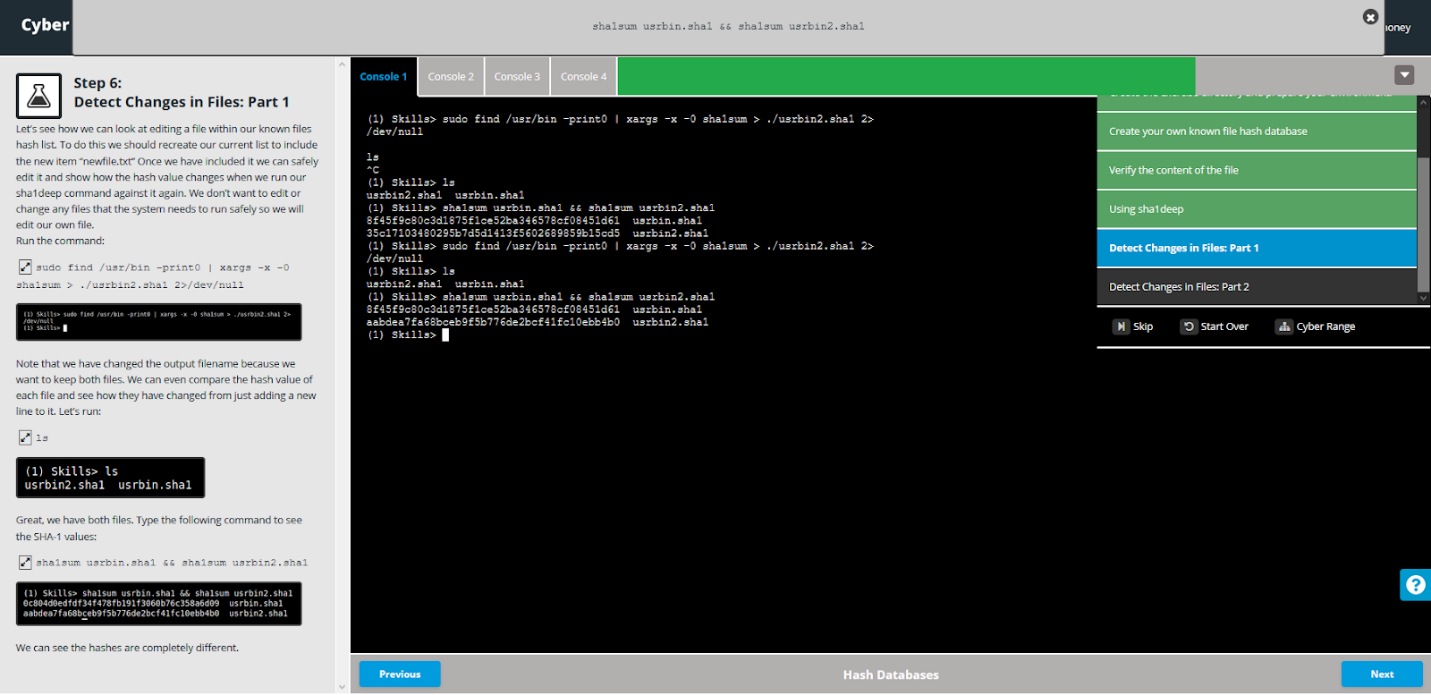
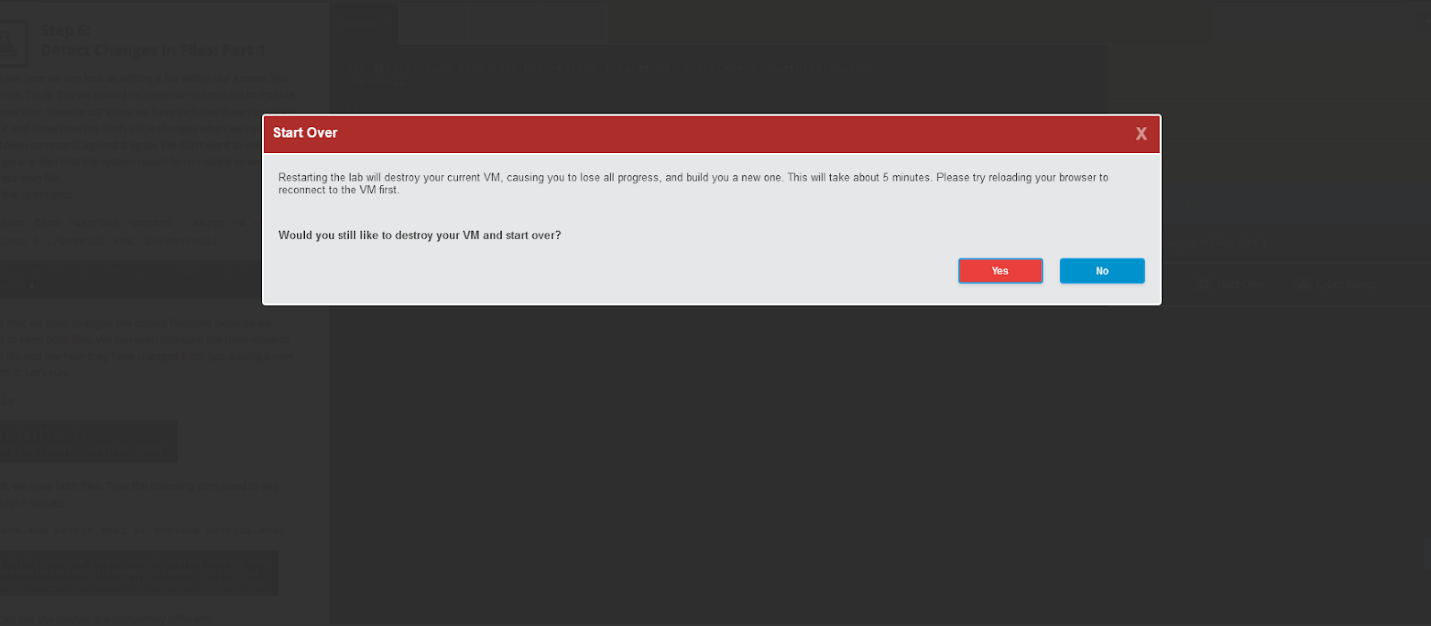
Fortunately, I was familiar with many of the processes which were used in the labs as I have taken IST 454 with professor Bowers where we used the robust program EnCase for computer forensic exercises. That being said, we were running EnCase on windows machines, so we had access to a GUI whereas the Linux environment relies on the command line. I was able to work through all the steps by carefully reading the instructions and thinking back to the things we learned in IST 454. Additionally, the previous lab assignment established a foundation to build on with the most recent lab activities.

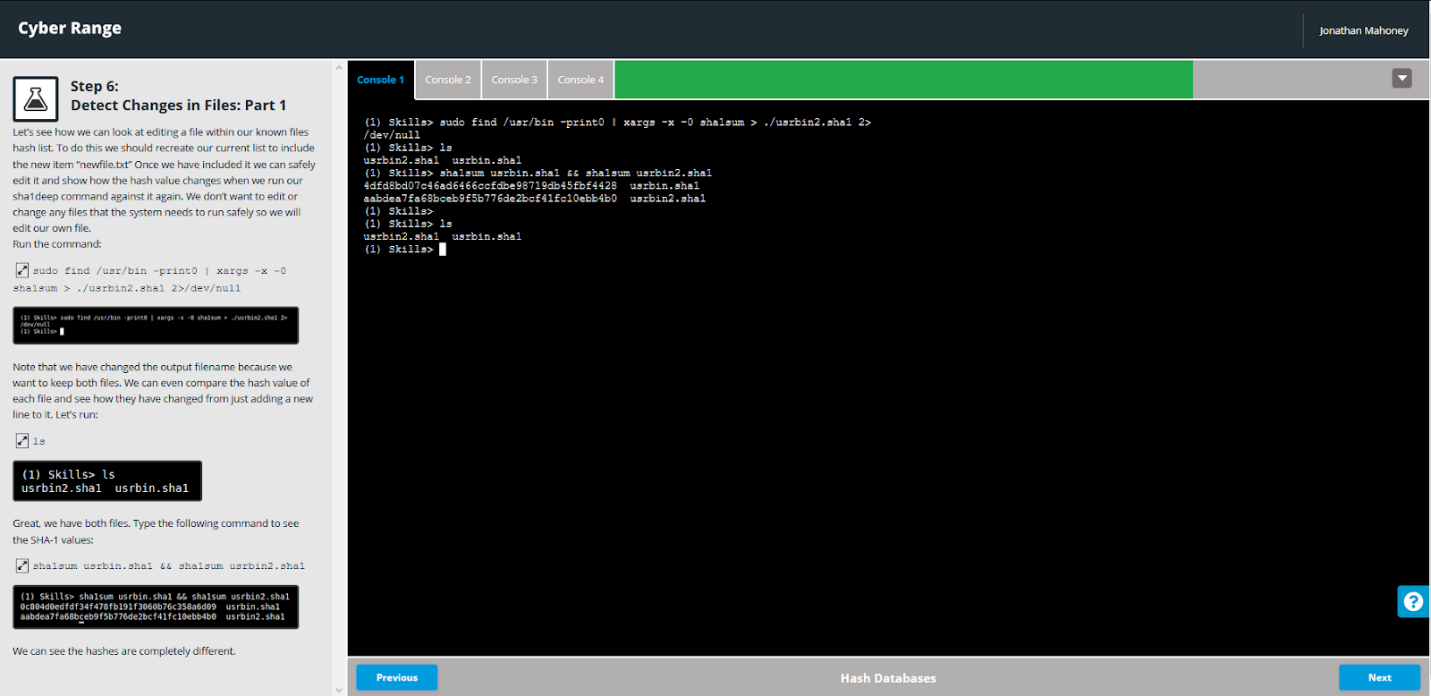
# Screenshots

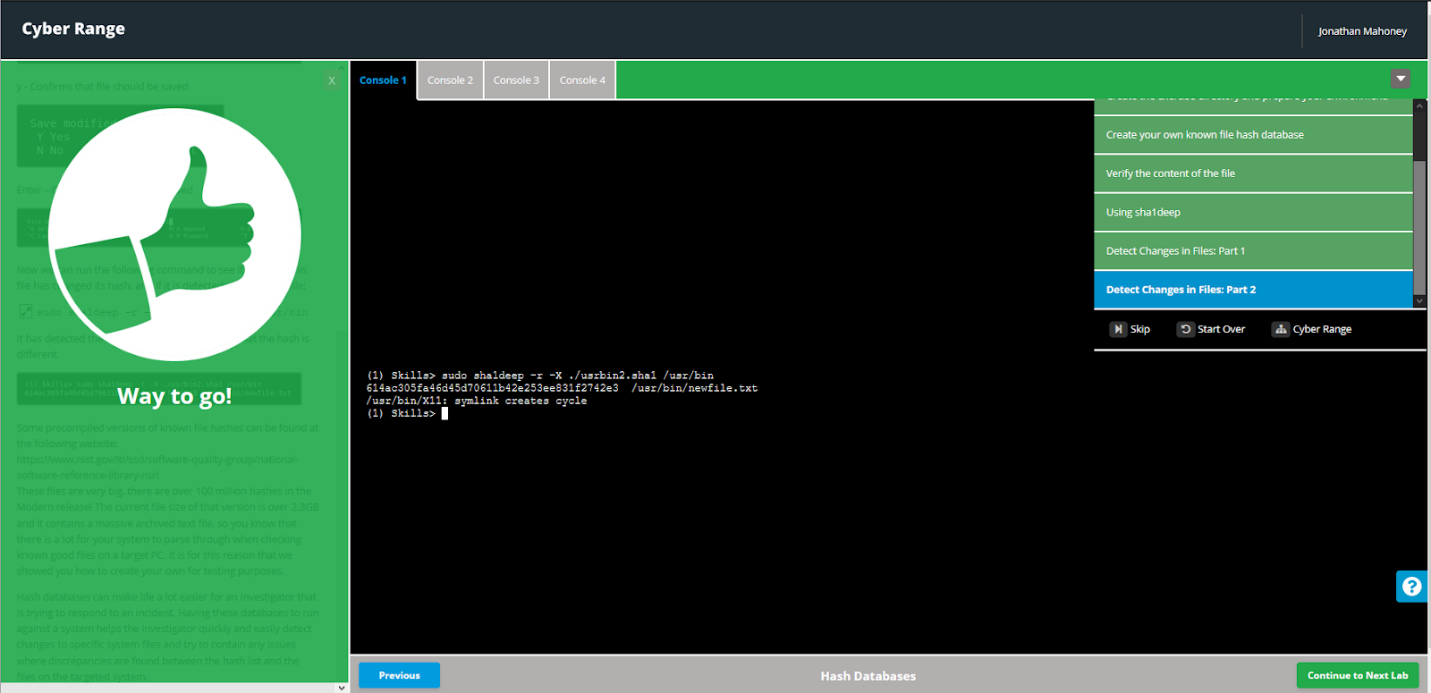
Command Line Basics for Forensics:

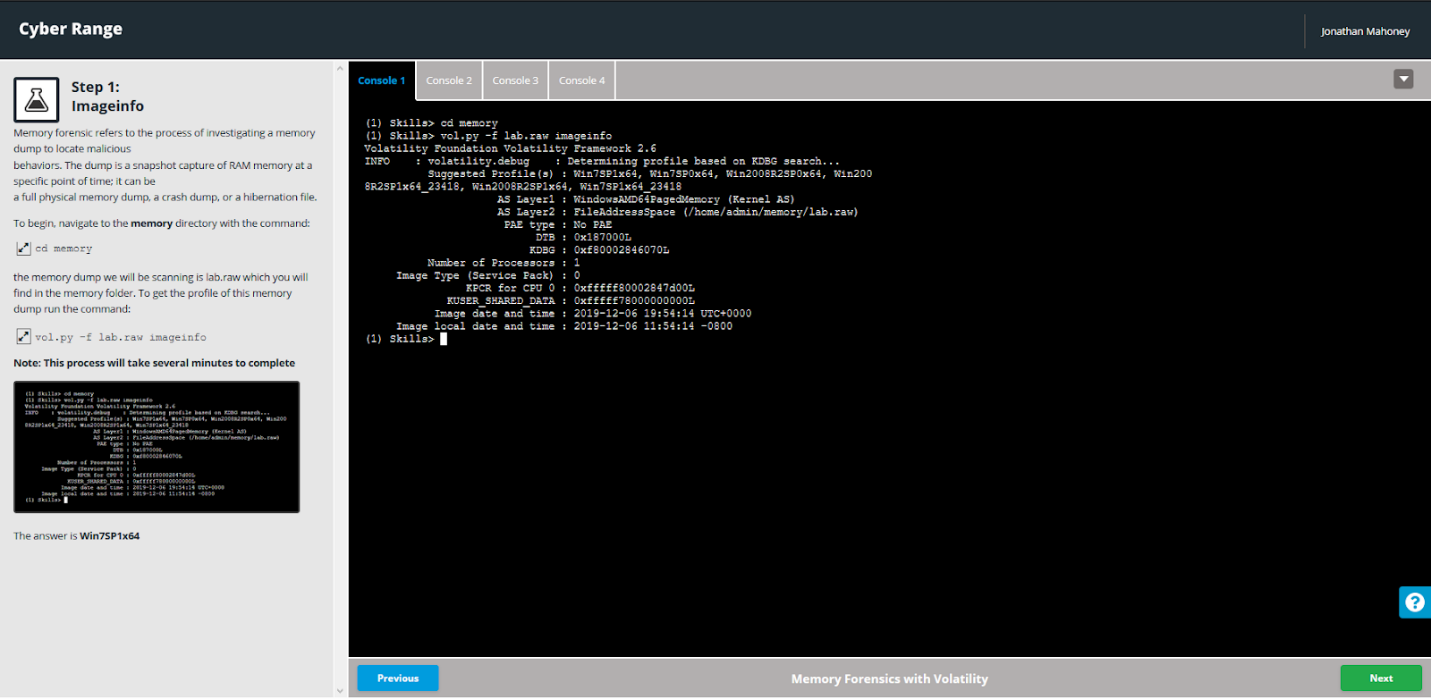
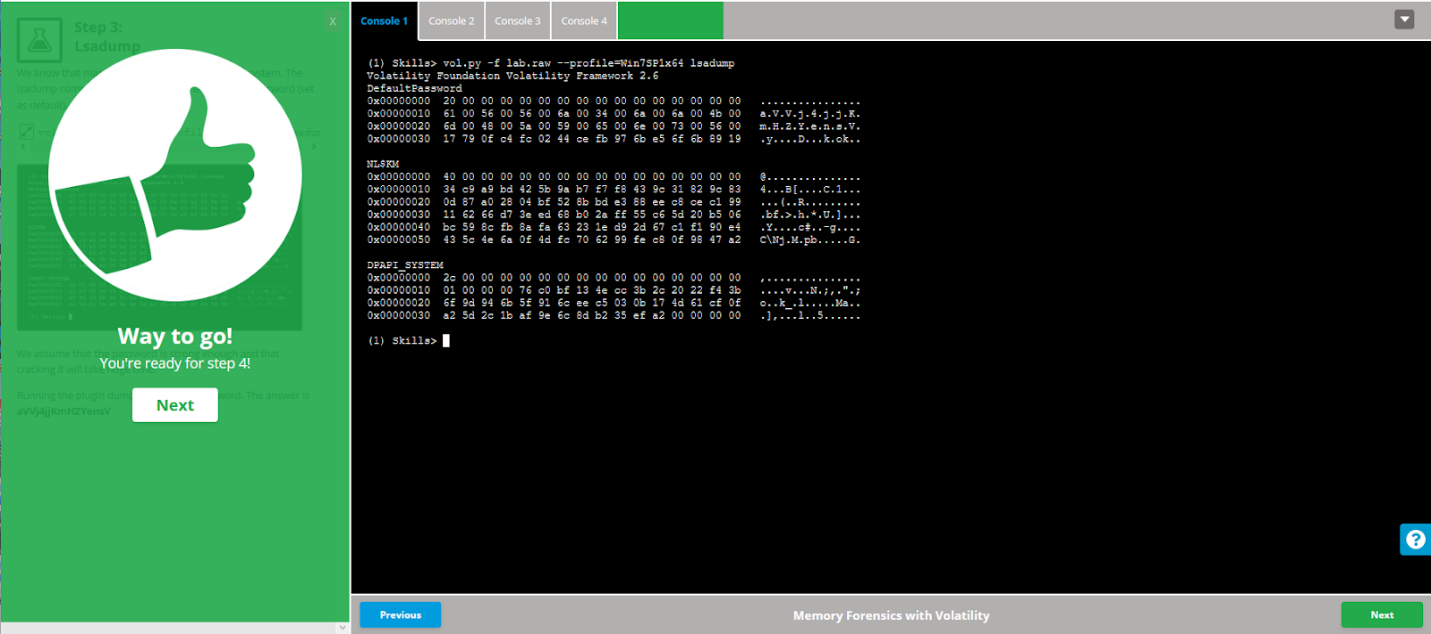
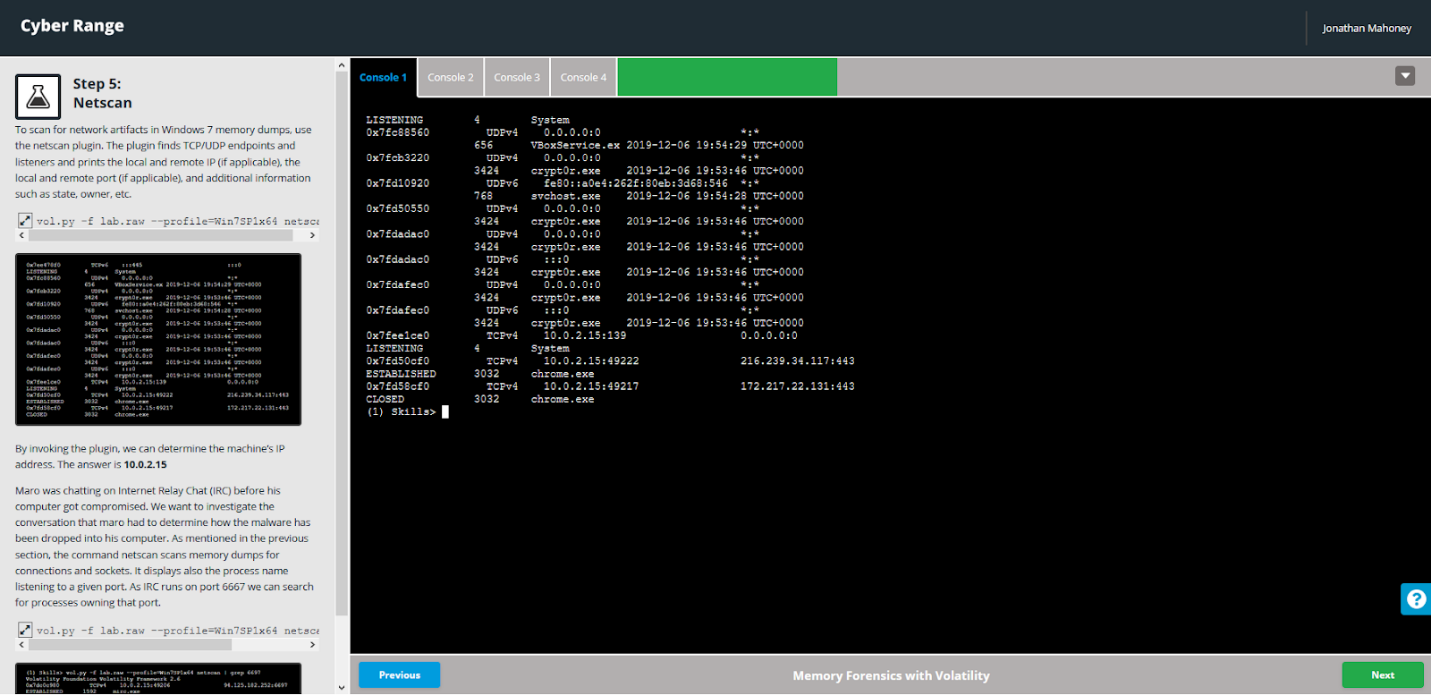
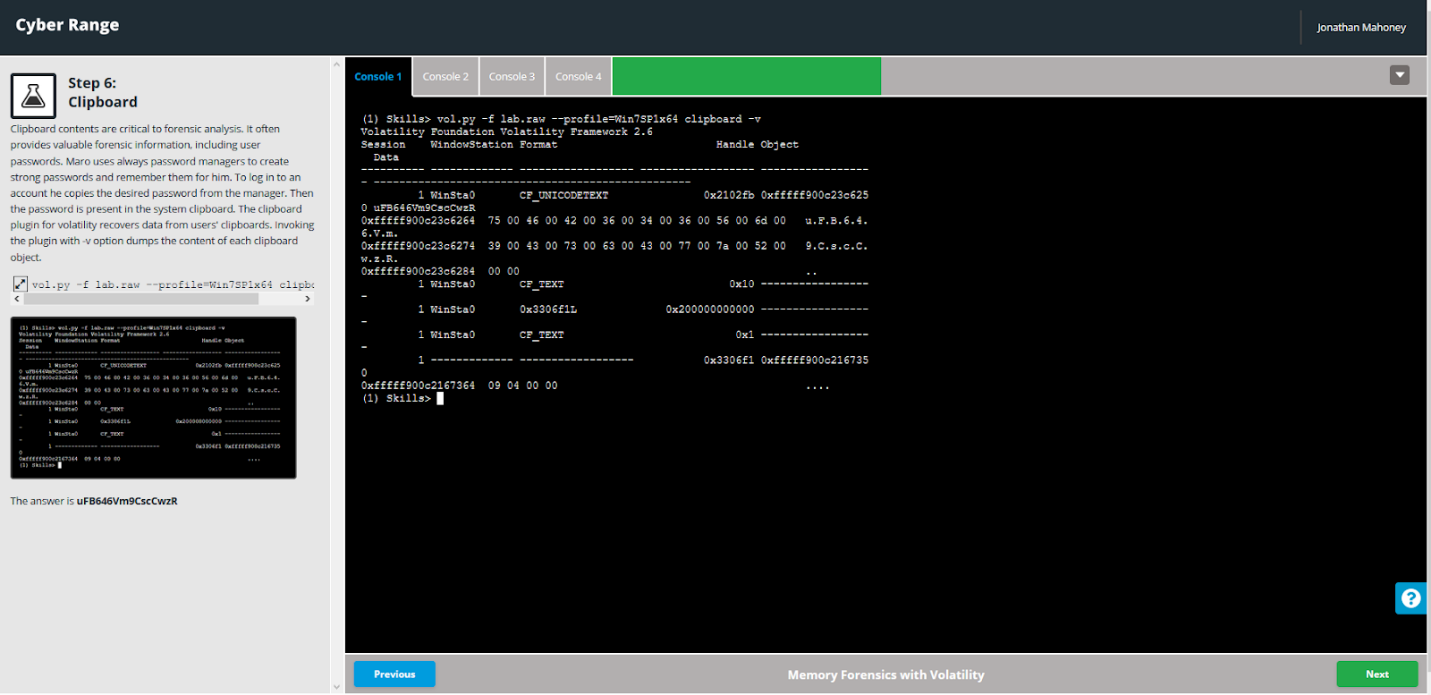
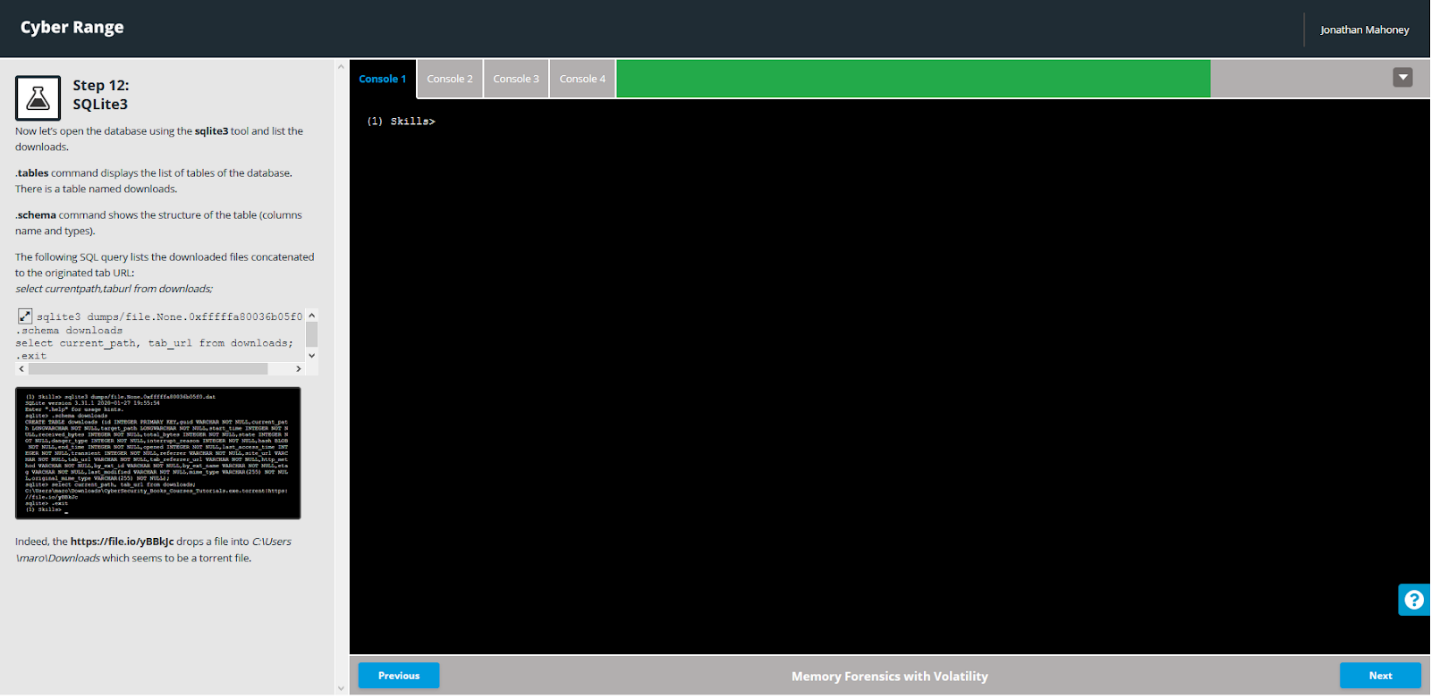
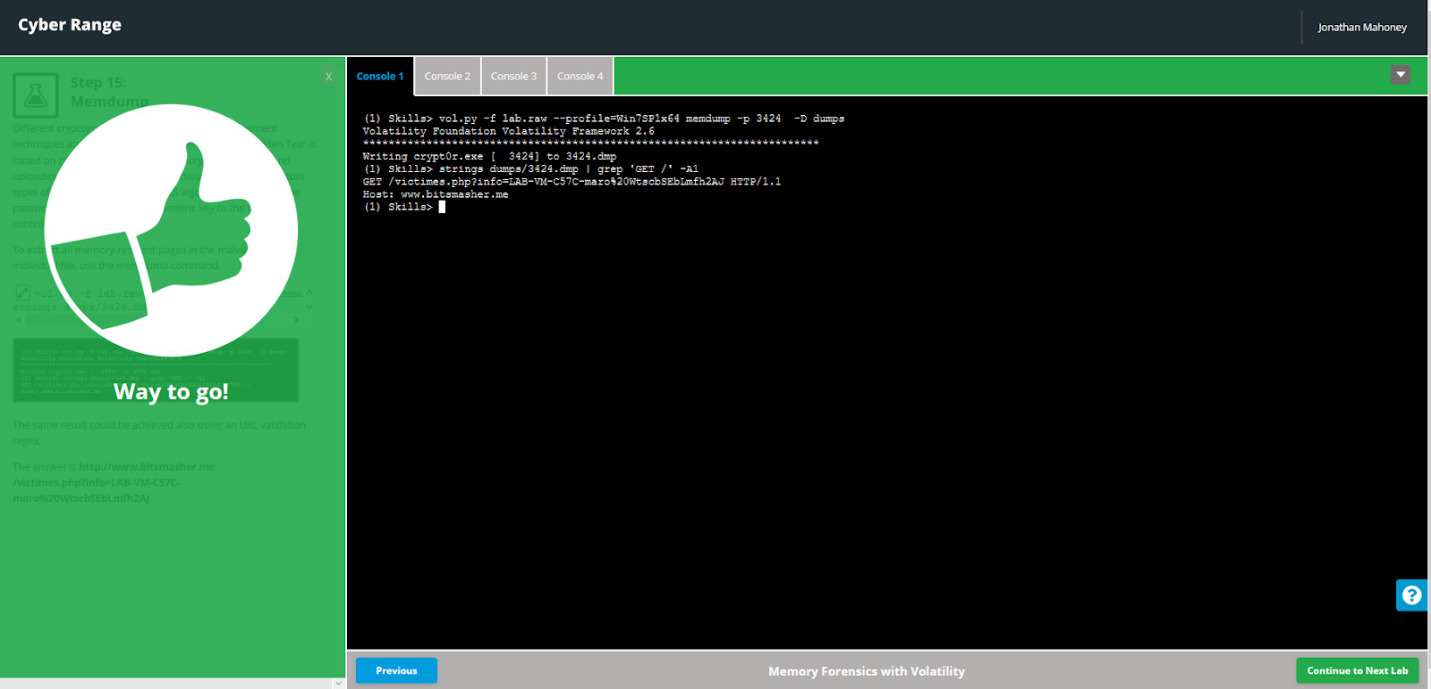
Recovering Data:     

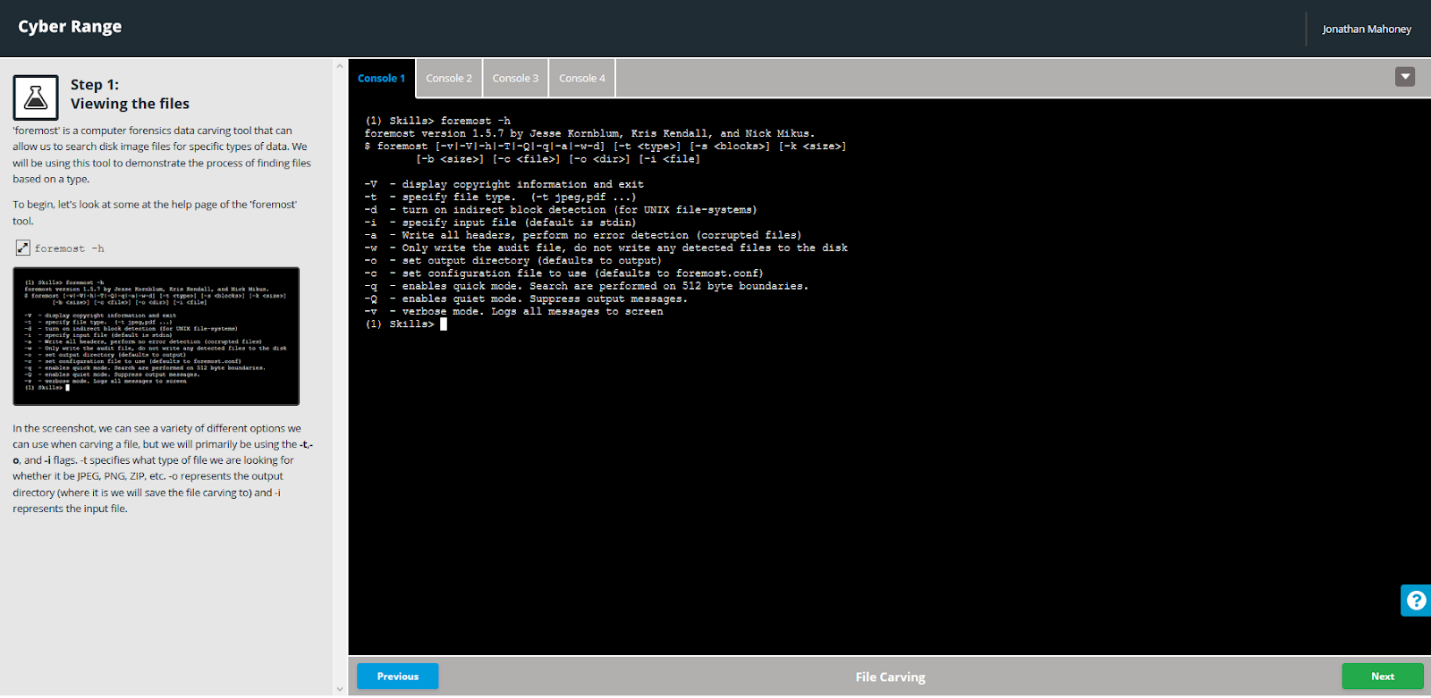
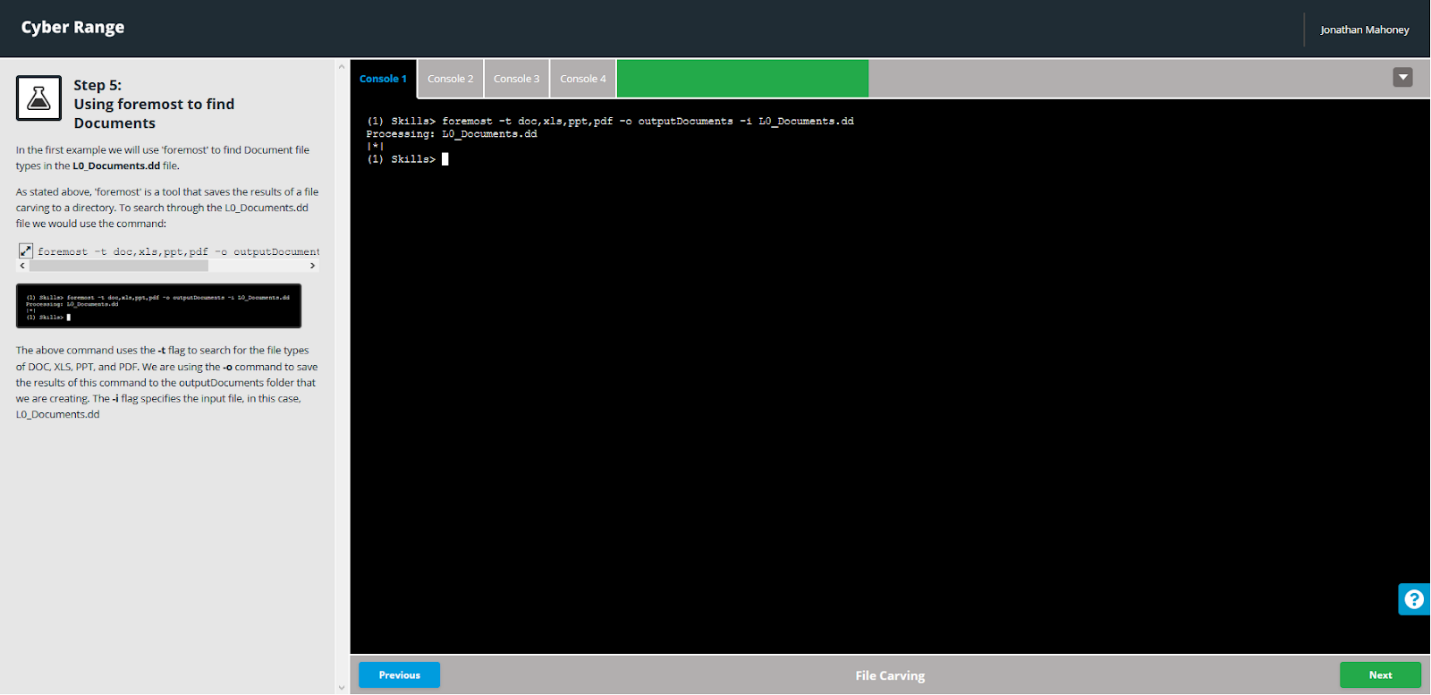
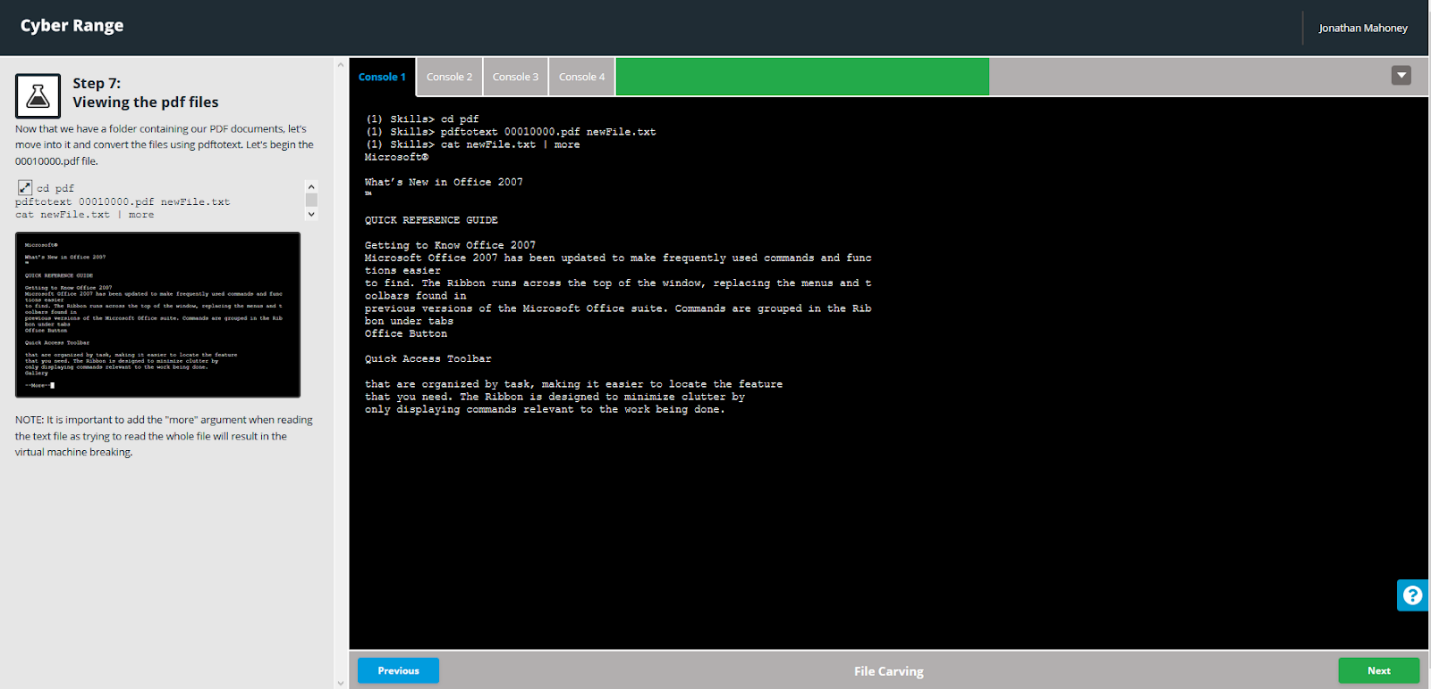
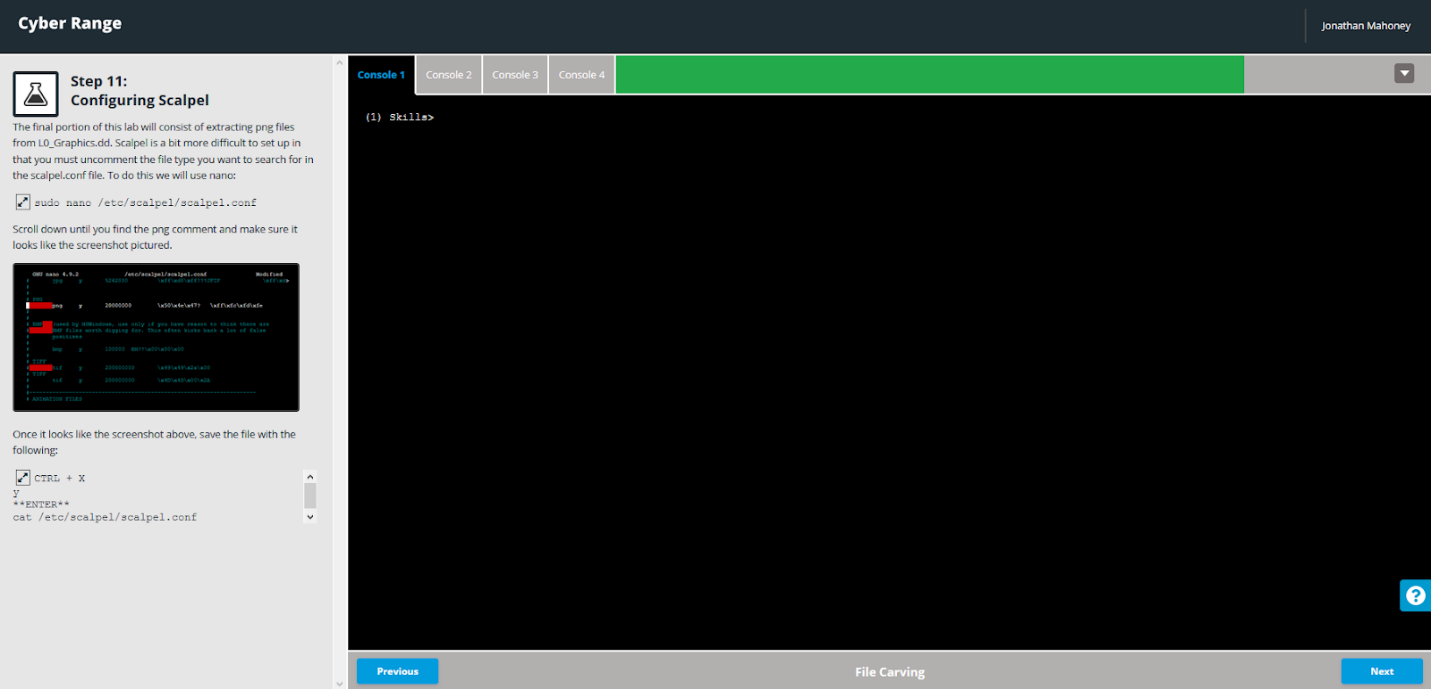
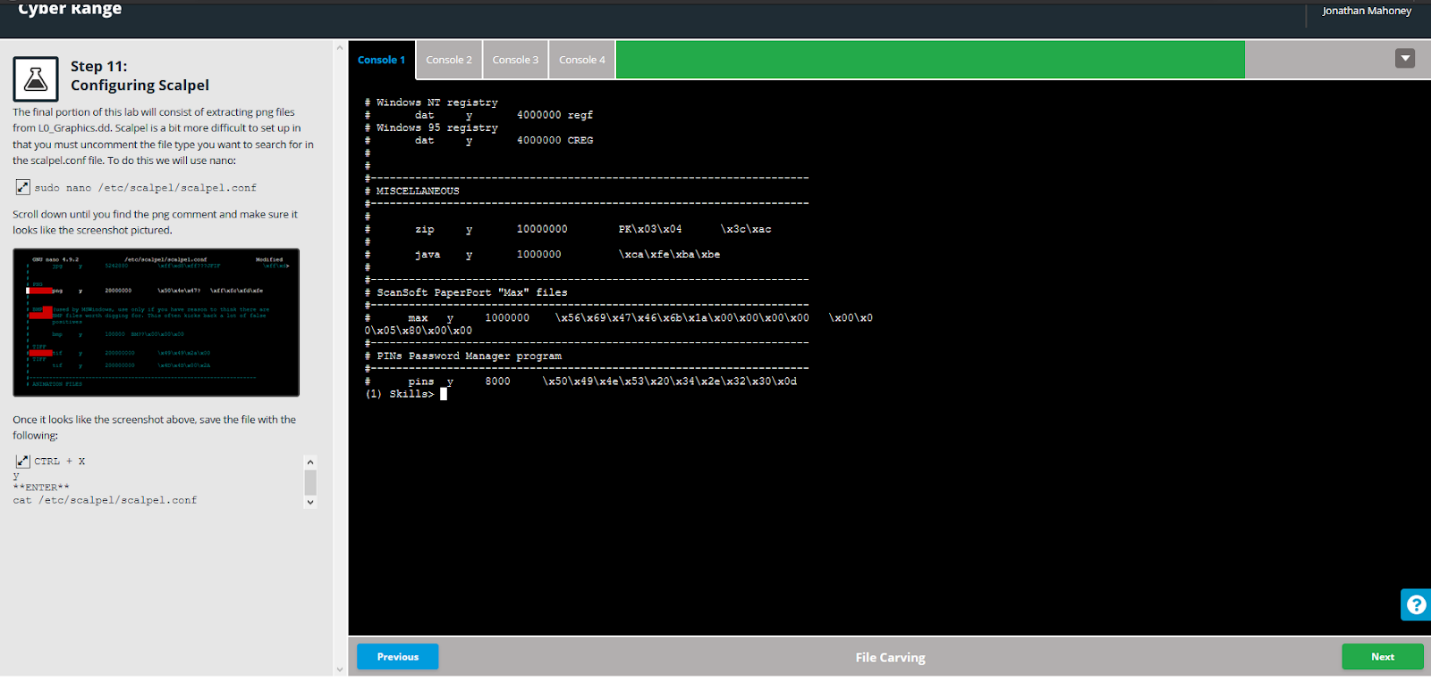
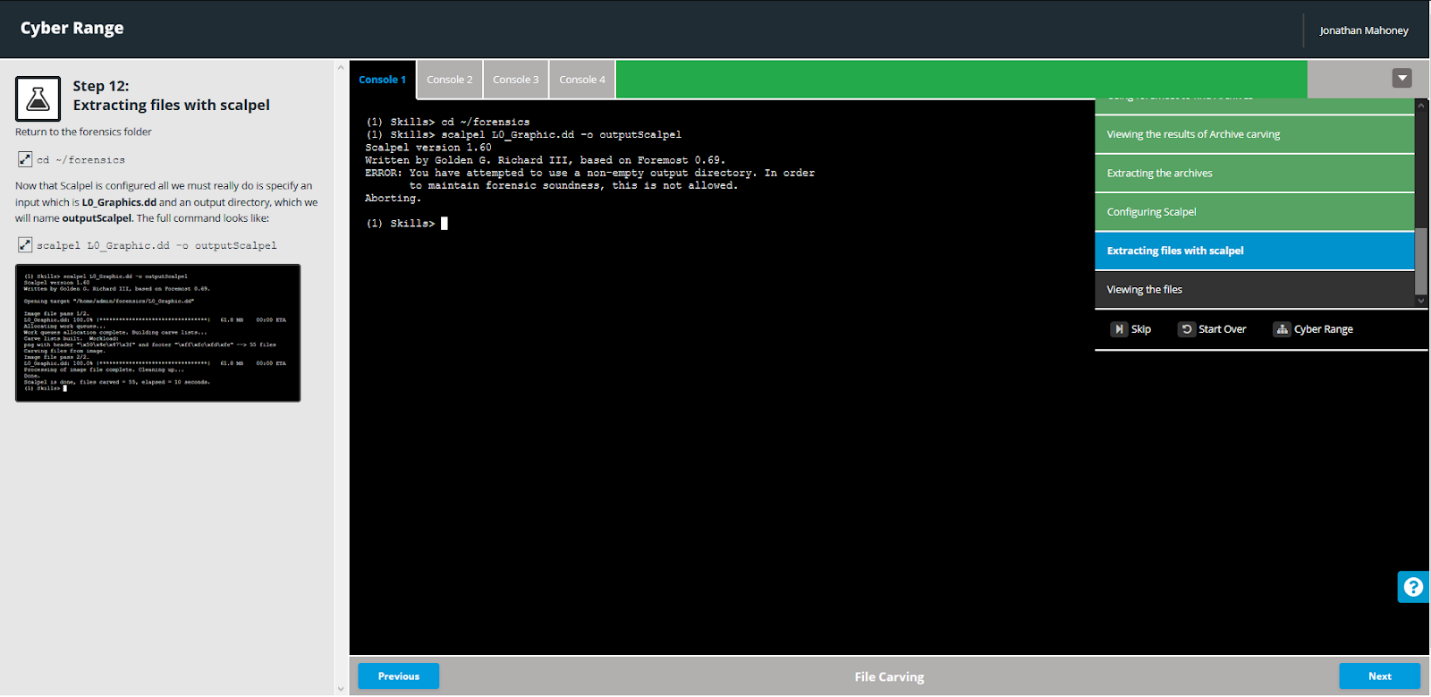
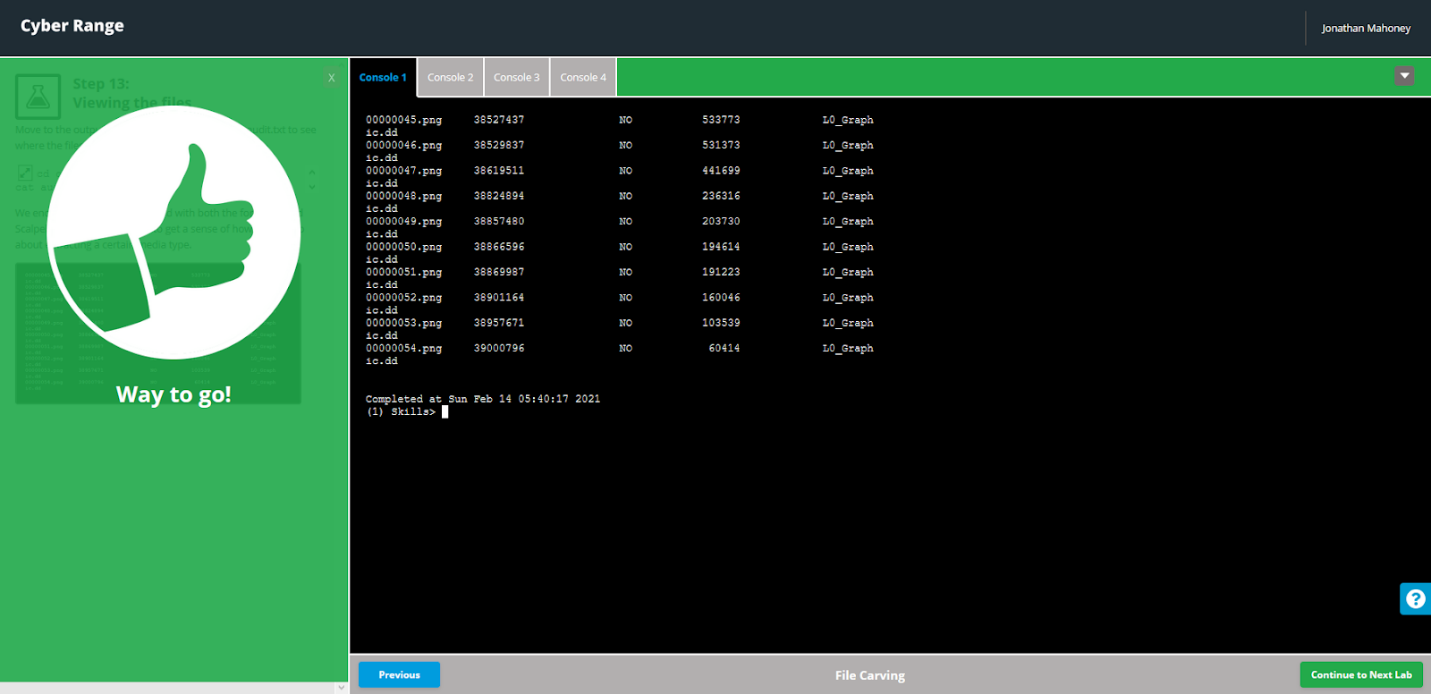
Hash Databases:     





Memory Forensics with Volatility:

File Carving:       

Network Forensics and Volatility

