Password Cracking

The first lab of the module is lab 19, password cracking. During this lab we are learning how to crack simple password-protected files. The lab is to help with identifying which files require a password and how to extract the password so we can enter the file.

To be able to do the password cracking lab, we start with extracting password-protected files. We are using Autopsy and creating a new case to start the first part of the lab. Next, we are using a Forensic Evidence File and finding an image to add to the case. In the configure ingest modules step, we check that all files have been scanned. At this point we can look for encrypted files through the results, extracted content at the category encryption detected. After extracting the encrypted files, we move on to the second part of the lab where we are cracking a PDF file with PDFCrack. The type of cracking that will be done to access the file is the dictionary attack which needs a hash of the encrypted file. At this point in the lab, we move to using the terminal and running a wordlist from john the ripper. After running the command and finding the password, we can now access the pdf file. We move on to look at the software shown to have been used for the encryption, VeraCrypt. We move on to mount the iso file from the FEF using the password from the pdf. Next, we copy the needed zip file back into our folder so we can alter it without changing the original. Moving on to the Fast Crack Zip tool, we are able to run a similar process to the PDFCrack and we are able to run our list to get the simple password.

At the end of the lab, it is strange to think about how fast we were able to get past the encrypted files. I know that the passwords used are simple which is why it runs fast but at the same time, there are not as many steps as one would think. The different software that we used helped show how we can go through the process. Overall, I think that being able to go from encrypted files to files open to use is an interesting process and a fun experience.

ScreenShots:

Section 2 step 6

A screenshot of a computer

Description automatically generated

Section 4 step 6

A screenshot of a computer

Description automatically generated with medium confidence

Chain of Custody

For this lab we are looking at the Chain of Custody to see who all handled and had access to the digital devices. Learning this is important as any misstep and wrong documentation could lead to an entire case being lost in court. Outside of the court, it is also important as a means to show who created what alterations at a specific time so if Joe handled it at 5pm but Paula handled it at 4pm, a change at 4:30pm would likely be Paula clearing Joe.

We start the lab by describing and detailing the devices that were seized so they can be identified. The photos of the device are used so we can gather information on the device such as the manufacture date, capacity, model number, and serial number. We are also looking and marking any physical descriptions of the device like if it has specific writing or stickers. After looking at the drive we move on to look over the cellphone that is in the seized devices. After marking what we find on the devices, we move on to the intake form which allows us to enter the details of the person who handed over the device. We will mark that the devices that need to be examined, the person submitting them, the priority, and the crime type. We move on to the information about when it was seized and the type of seizure. We then enter the purpose and look over the document to make sure nothing is missing or incorrect before signing it. Then we move onto documenting the other devices that we have.

Being able to look over the form and all the details that we need to note was quite the learning experience. There are a lot of specific details that are needed and missing them could lead to bigger problems. Before the class I never really thought of data forensics, so this is quite a learning experience.

ScreenShots:

Section 2 step 12

Graphical user interface, text, application

Description automatically generated

Section 2 Step 23

Graphical user interface, application

Description automatically generated