#JonSecOps

Password Recovery and Decryption using AccessData PRTK

Background

Mr. McBride is the senior forensic examiner at ACME Corp. As part of Mr. McBride's annual training and re-certification, his supervisor Alfred Smith has tasked Mr. McBride with demonstrating his abilities in decryption and password cracking. You are to combine the use of AccessData's PRTK program and manual decryption methods to unlock all of the files provided

Request

Mr. McBride's supervisor, Alfred Smith, needs Mr. McBride to examine the encrypted zip files and determine their passwords. He wants Mr. McBride to show both his skill with password cracking programs and his understanding of manual decoding. Below is a list of the files in this exercise. Next to each file is a requirement for either the use of PRTK or manual decoding. Zip one – PRTK Zip two – Manual (DO NOT use an online decoder) Zip three – Manual Zip four – PRTK (Custom Dictionary) DO NOT just double click an archive to decrypt it. This just a preview and Mr. McBride won't be able to keep decrypting files and you will get an error that he is using the wrong password. Instead, always right click and extract. The program will then ask for the password. When performing manual decoding Mr. McBride must show work. This can be in the form of a table to show a character shift or something similar. Mr. McBride must have more than just the encoded and decoded text. I want him to attempt cracking the "Almost There" zip file using the default English, French and Spanish dictionaries and allow the program to run at least 30 minutes. Screenshot the rule progress bar chart to show how far Mr. McBride got during that time. Mr. McBride is welcome to run the program longer if he would like to see how far he can get. Then I want Mr. McBride to use the "Clue Three" text document as his custom dictionary. Load it as a standard dictionary and add the French and English dictionaries. Mr. McBride must disable all rules except rule BAS-2-17.

Summary of Findings

During the investigation, pertinent information such a passwords and hidden text files were obtained from the acquired zip file. This information is displayed in the analysis section of the report.

Evidence

Table 1 outlines the evidence items of this case.

Description	Designation	Filename	MD5 Hash
Evidence Provided	Preservation Copy	PRTK Lab	C1120df1c740a66cde60ae8cdb90a9d3
Evidence Reviewed	Working Copy	PRTK Lab Copy	C1120df1c740a66cde60ae8cdb90a9d3

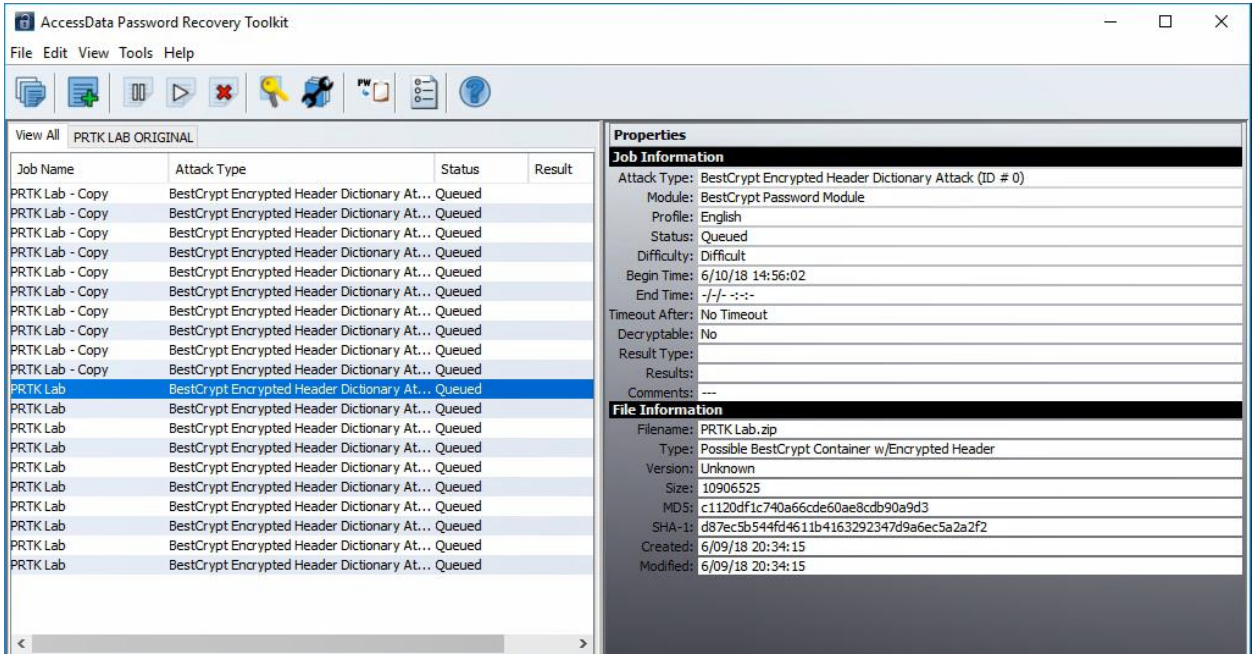
Table 1: Case evidence items

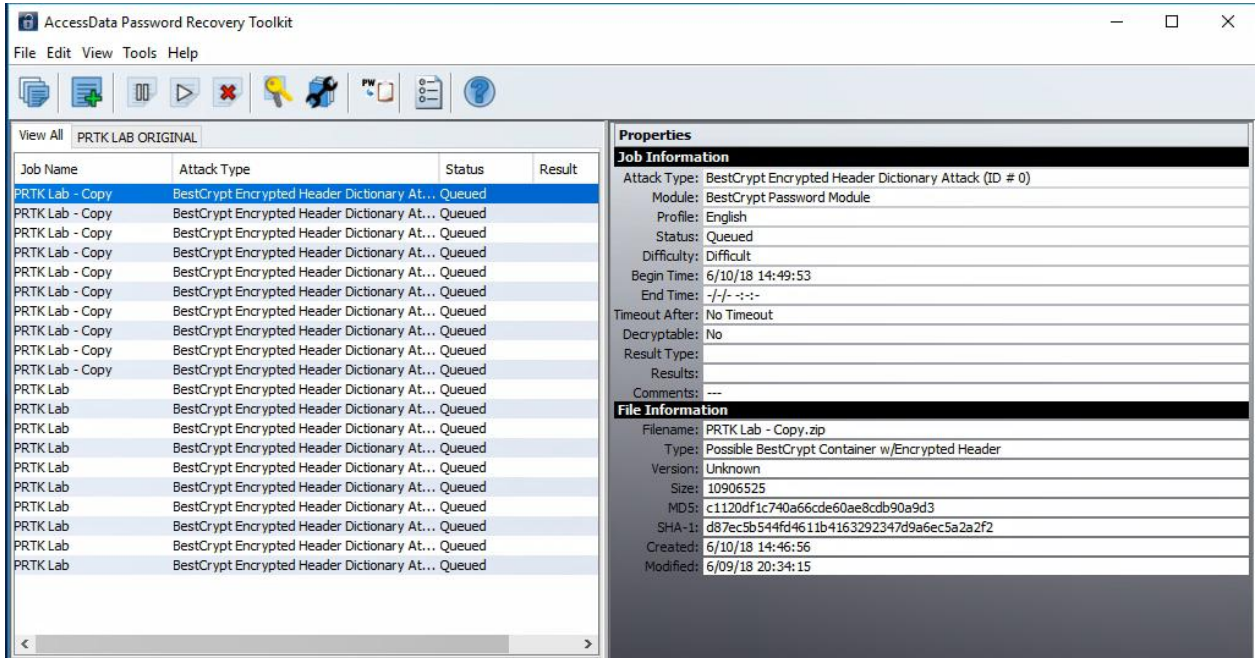
Collection and Analysis

Collection

The file provided named PRTK Lab was investigated for the encrypted zip files. Once the file was downloaded it was copied and hashed by adding both the original and copied file into the Access Data Password Recovery Toolkit software. The PRTK software revealed matching MD5 hash values for both the original and copied PRTK Lab file which is revealed in Figure 1.

FIGURE 1: MATCHING MD5 HASH VALUES

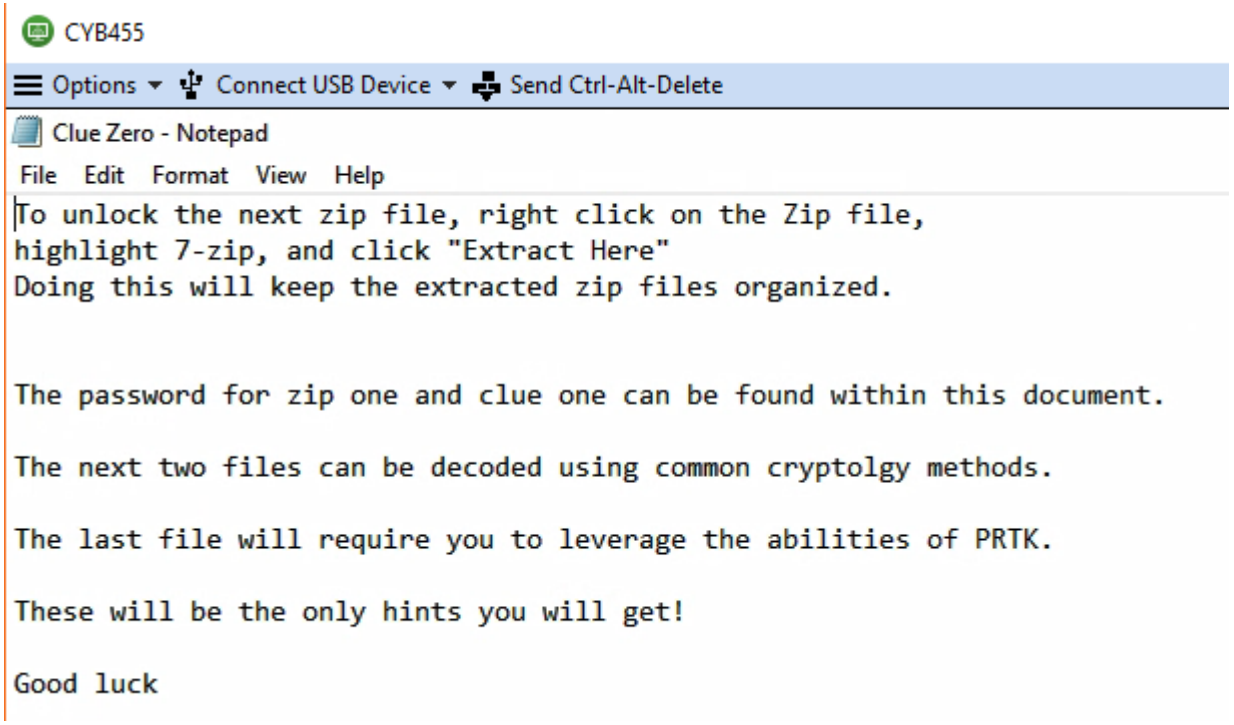




Analysis

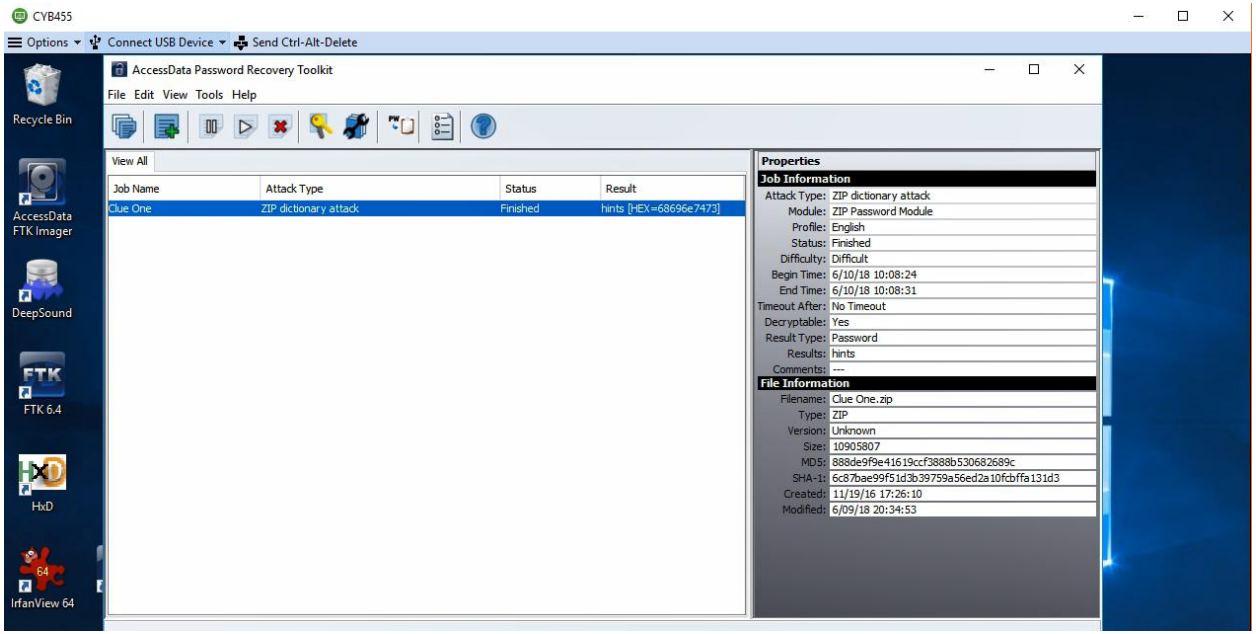
After the files were copied for evidence preservation purposes, the PRTK Lab copy file was investigated and the Clue Zero txt file revealed the following message displayed in Figure 2.

FIGURE 2: CLUE ZERO TEXT FILE MESSAGE



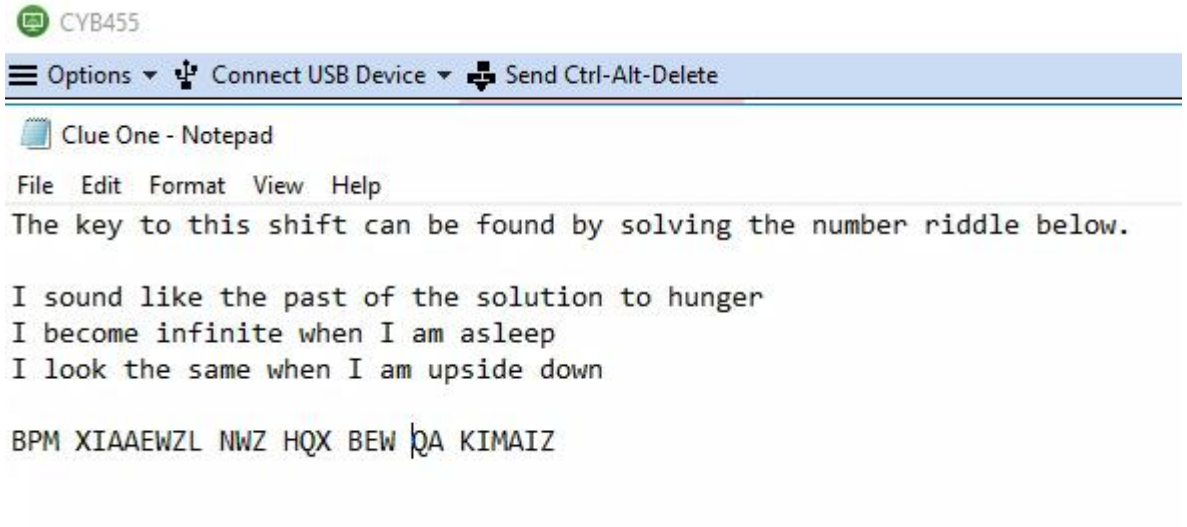
The Clue One zip file was encrypted and needed a password. To reveal the password to this file it this file was added to the PRTK software to be examined and revealed that the password to the Clue One zip file was hints as revealed in Figure 3.

FIGURE 3: CLUE ONE ZIP PASSWORD



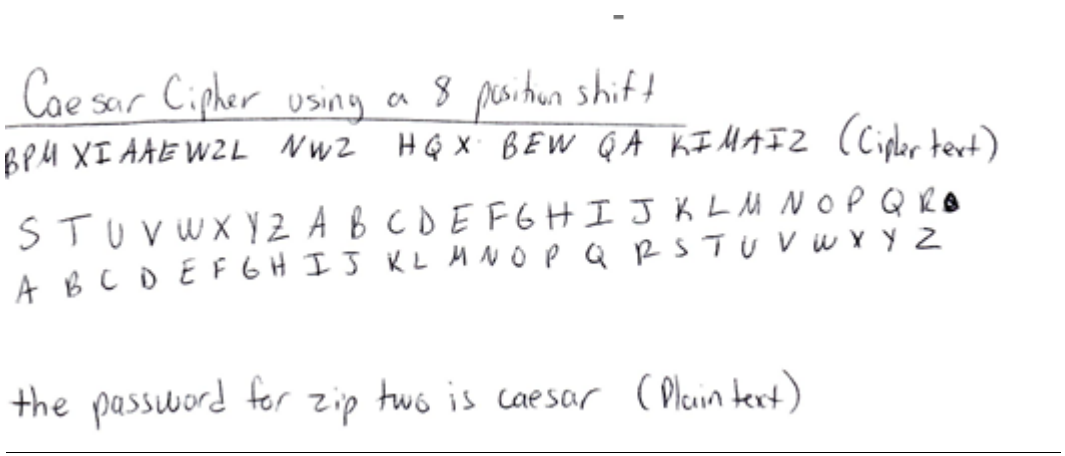
After the password hints was entered the following message was revealed from the Clue One text file as displayed in Figure 4.

FIGURE 4: CLUE ONE TEXT FILE MESSAGE



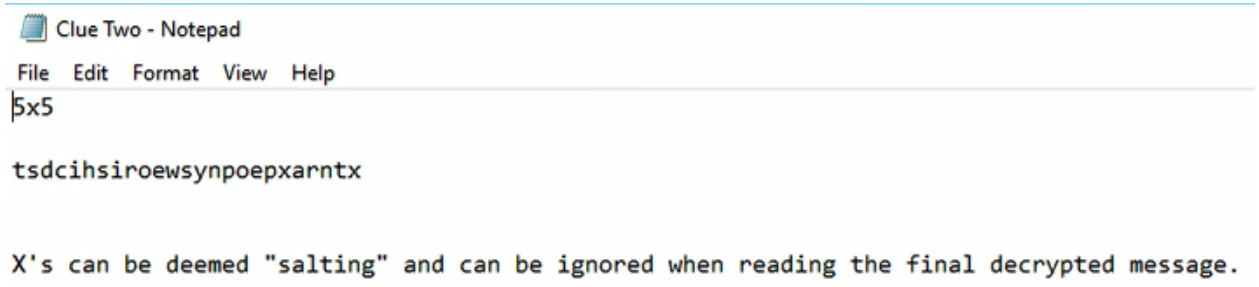
The key shift number using a caesar cipher that was obtained through critical thinking was the number 8. The cipher text was translated into plain text as displayed in Figure 5.

FIGURE 5: CLUE ONES'S CIPHER TEXT TRANSLATED TO PLAINTEXT



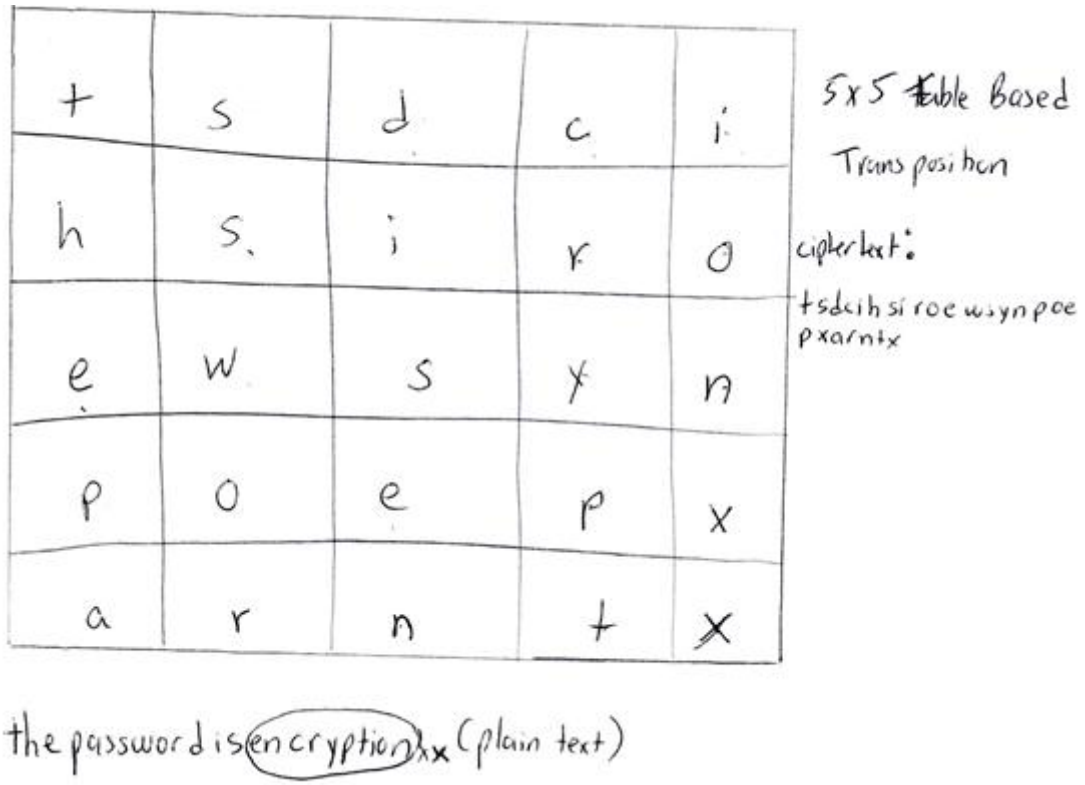
The password caesar was entered into the password encrypted Clue Two zip file and revealed the following txt file message displayed in Figure 6.

FIGURE 6: CLUE TWO TEXT FILE MESSAGE



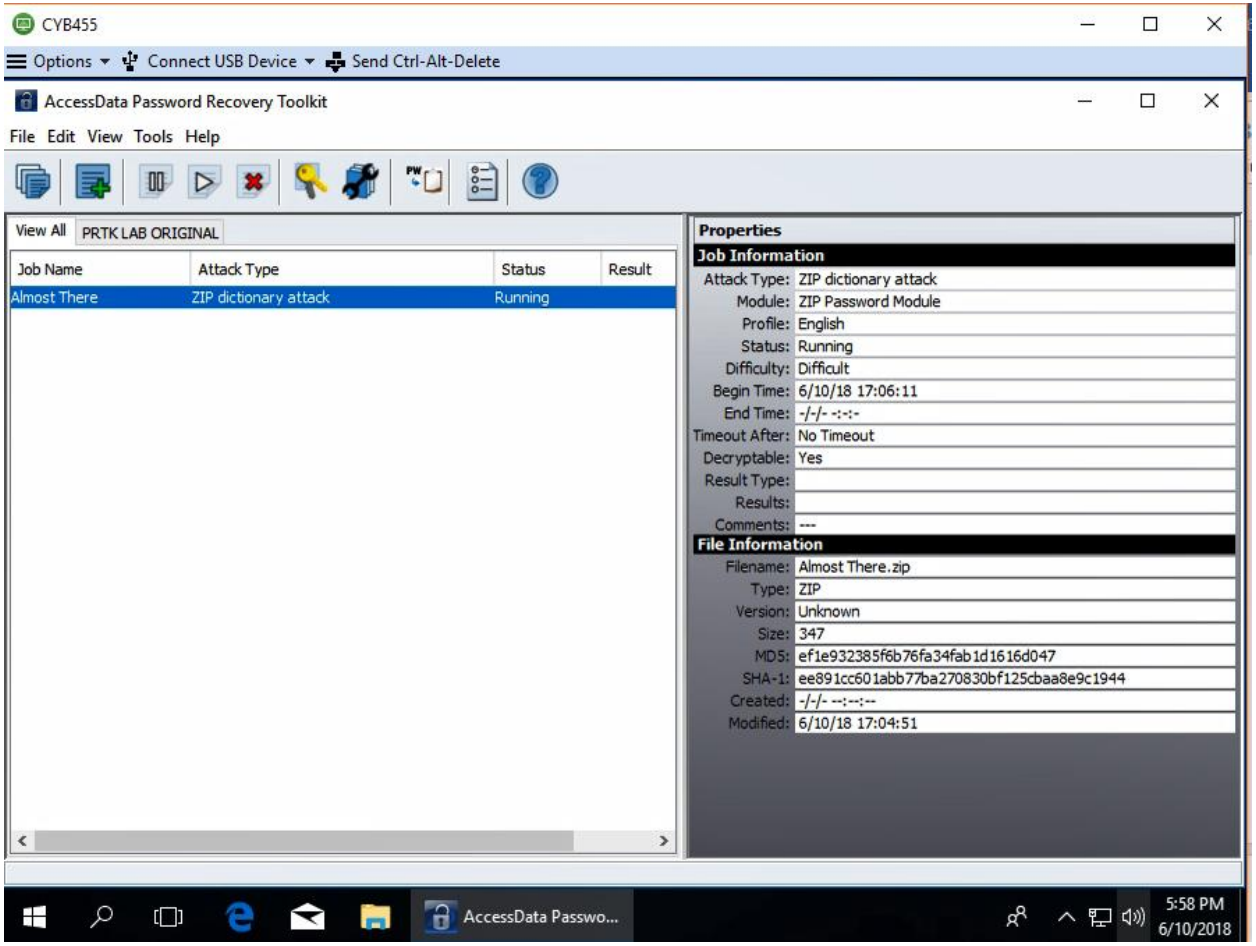
Using a 5x5 table-based transposition, the following message was revealed as well as the password to the encrypted Clue Three zip file displayed in Figure 7.

FIGURE 7: CLUE TWO'S CIPHER TEXT TRANSLATED TO PLAINTEXT



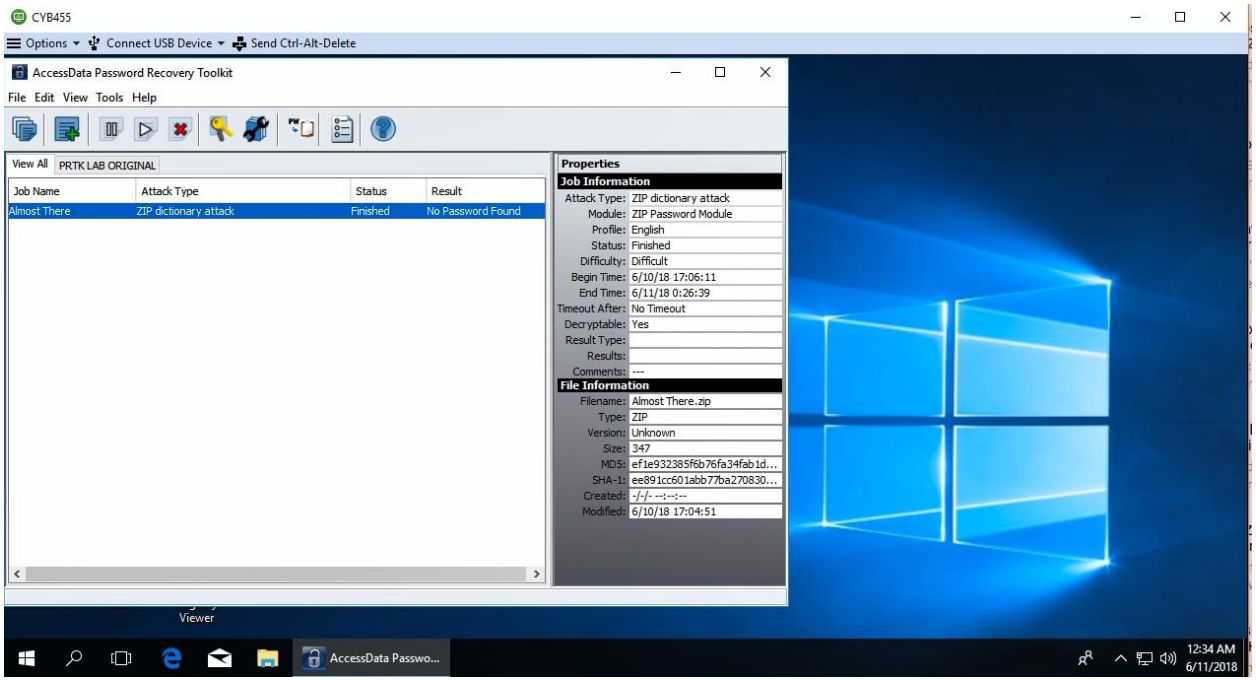
The password encryption was entered into the Clue Three Zip file and displayed a message has a file size of 10,649kb which is too long to display in this report. A password encrypted zip file named Almost There was revealed. This file would have to be added into the PRTK software first. To decrypt this file, the Clue Three txt file was used to create a custom dictionary. After this was completed the Almost There zip file would be examined by the PRTK software as displayed in Figure 8.

FIGURE 8: ALMOST THERE FILE BEING EXAMINED BY PRTK



After the PRTK software examined the Almost There zip file it revealed that there was no password found as displayed in figure 9.

FIGURE 9: ALMOST THERE PASSWORD



Conclusion

The requested information from Alfred Smith was obtained successfully. The AccessData Password Recovery toolkit is a great tool to use when unencrypting files with passwords. The use of the PRTK tool kit also allows users to create a custom dictionary which allows for faster password recovery techniques.