Assignment 4: Password Recovery
CET 4860 Introduction to Digital Forensics

Case Overview:

On Saturday November 11th Officer Linda Mood of the US Secret Service came to your office and requested that you assist her with a case she and her team are having difficulty with. She provided you with an 8GB Selex brand USB drive that contained eight zip files, and SAM and SYSTEM files from a Windows XP box; these contain user info and password hashes. Officer Mood indicated that the zip files were password protected, and she and her team were unable to open the files. She requested that you use your expertise to assist the team in breaking the passwords and returning the files in decrypted form to her. Officer Mood indicated that the suspect grew up in Germany but has resided in the U.S. for the last two years.

Furthermore, there were several accounts on the Windows XP box and she wanted you to break the passwords for those accounts as well; the provided SAM and SYSTEM files contain these passwords.

Finally, Officer Mood indicated that she has a TOPSECRET file of the suspects which is also password protected. Unfortunately, due to the sensitive nature of the contents, she can't provide you the file. She believes that there are clues in the individual documents that, once decrypted, will provide you with the password for that file. She believes that the password is the name of a movie, but the contents of the file will verify what she believes. She said "this is very important; we need that password!"

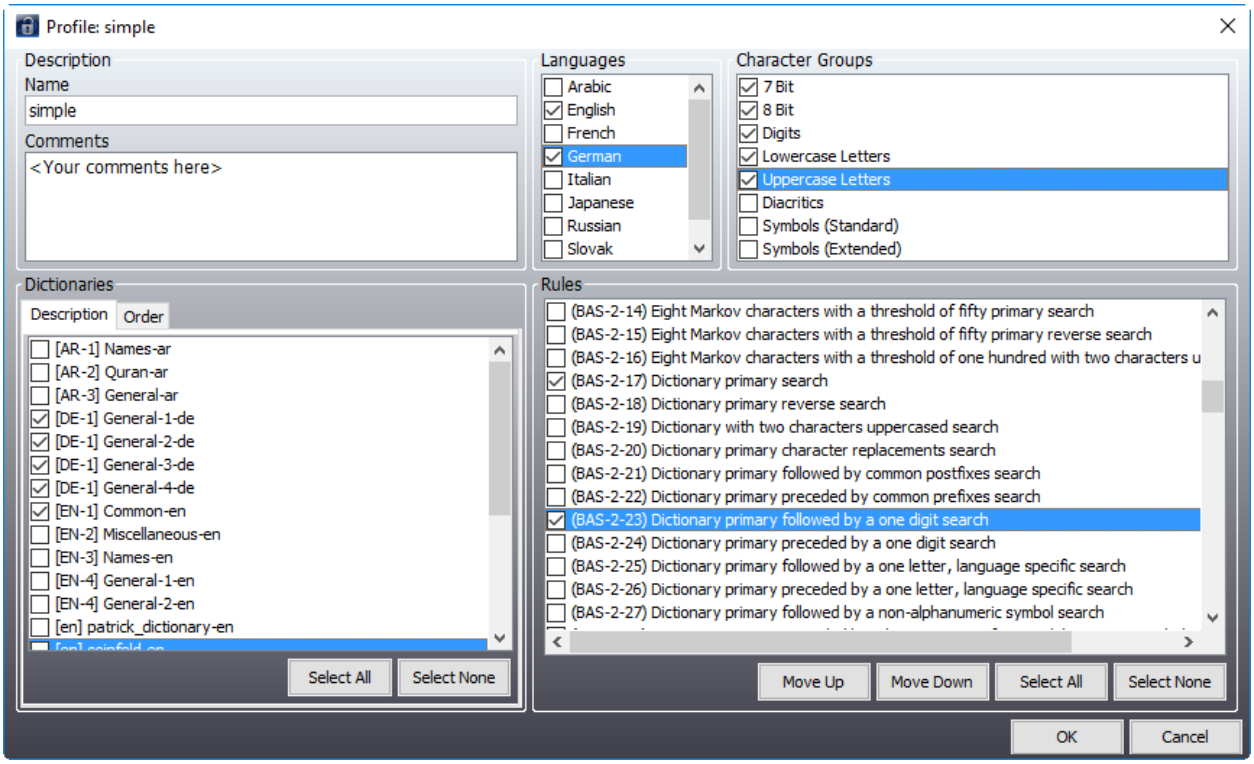
Task:

Watch the video on PRTK. You are to install PRTK on your computer, and use it to:

1. Identify the passwords of as many zip files as you can.
2. Identify the passwords for as many user accounts as you can.

Hints:

1. We have intelligence on the suspect. Let's use that. The suspect grew up in Germany and now resides in the U.S.
2. What PRTK profile will you use? There isn't a single profile that meets all criteria so you'll need to select and modify a profile or create a new one. I created a new profile based upon the European profile and modified it as shown in the figure below. After editing the new profile, set it to DEFAULT (Important!).

3. 

4. Drag and drop the files zip1.zip through zip10.zip into PRTK. Let it run. This should go fast because you are using only five dictionaries with two rules.
5. When it finishes create a PDF report.
6. What about the Windows XP files? You'll need a different profile. Select "English" and set it to DEFAULT BEFORE you input the SAM and SYSTEM file. Note PRTK will ingest the SAM file first and then you need to point it to the SYSTEM file. Finally, after breaking the passwords, create a report. You may have to wait 2-3 days for PRTK to finish.
7. What should you put in the Results section? There are 10 files each of which has minimal text. I would include a table that lists the zip files, their hashes of the zip files that you calculated, and the contents of each file. On the last line, provide me with the name of the movie!
8. Anything else? Yes, the usernames and the passwords in a table. If you can't break a password in 5 days, you can indicate as such.

Deliverables:

There are two deliverables:

1. A forensic report (using our forensics template) that describes your tasking, steps taken, results, and conclusions.
2. Two PRTK reports that contains the passwords for the zip files and for the user account passwords. Run those separately.

Zip those into a single file <first>.<last>.4.zip. .

Have fun!

Here are the hashes of the original files. Note that the SAM and SYSTEM have been compressed to a single file to save space.

There's a neat utility that is free from MS that allows you to hash files from the command line: https://support.microsoft.com/en-us/kb/841290

MD5

1f37788305a495dff3d5696b6f1ba0b9 samsystemt.zip (SAM and SYSTEM zipped to save space)

618ab061dd381dfc4eebc05e98afcdd4 sam

91a1af4c665b82a022ea3e283227a7ac system

664781b2ebc197bbe039383467d7daac zip1.zip

b882919907f04588e3f48e01695729e8 zip2.zip

43633c18d9cdf96d5f50c4fbc4f11b3e zip3.zip

6f6d819504944e29743c6fd8a73b0c8c zip4.zip

02a48d66611e87e914df6989455db438 zip5.zip

8d8064f39a827a8e1dff2452af3dcfc0 zip6.zip

ff2e49f4cce231a7e14040444a941aca zip7.zip

71caedae0acd48de43689588d3a9d24f zip8.zip

349d13fc358e55957323ba1571e96bb9 zip9.zip

d20c60238588621d8af059cec7e39dcc zip10.zip