

7.0 LAB MANUAL – PASSWORDS & ENCRYPTION

WARNING – You must only crack passwords on your computers, systems where you have written authorization, or on college systems where you have the instructor’s permission. Do **NOT** attempt to crack passwords on systems where you failed to obtain prior authorization. Even attempting to crack passwords on unauthorized systems is illegal and will result in criminal charges.

NOTE – many of the exercises in this section require running a virtual machine in Oracle Virtual Box. If necessary you must download, install and run Oracle Virtual Box, which is available from:

<https://www.virtualbox.org/wiki/Downloads>

If you have problems running Oracle Virtual Box on your computer the instructor will **NOT** be able to help you debug the installation; you will have to come to the CBC Campus and use one of the computers in the assigned Computer Science Lab. If you find yourself in this situation contact the instructor and make an appointment to get situated.

Once you have Oracle Virtual Box installed and running you will need to download and install a virtual machine image. The virtual machine image is **ForensicsPractice.ova** and can be downloaded from Canvas. The ova file is quite large, nearly 10 GB, so it may take some time to download. When the .ova file has downloaded, start Oracle Virtual Box, select **File > Import Appliance**, then browse to where you downloaded the ForensicsPractice.ova file. After the virtual machine has loaded you can start it by using any of the following methods:

- A. Select **Machine > Start**
- B. Select the virtual machine, then click the Green Arrow labelled **Start** in the main toolbar
- C. Right click on the virtual machine, then select **Start**
- D. Double click the virtual machine

7.1 Cracking Local Windows Passwords with Cain and Abel

In this exercise you will gain experience cracking passwords for Windows accounts using Cain and Abel. You will install Cain and Abel, create new Windows user accounts and assign passwords, then use Cain and Abel to decrypt the passwords.

Note – This exercise requires you to create new users accounts. In other words, you will need Administrator privileges. You will also need authorization to run Cain and Abel and crack the passwords on the computer. You won’t be able to do this on any of the CBC computers because Cain and Abel will be blocked from installing by the security software. However, you have the following options:

- A. Install and run Cain and Abel on one of your own computers, as long you have authorization.
- B. Install Cain and Abel on a virtual machine on a computer in the CBC Lab.
- C. Install Cain and Abel on a virtual machine on your own computer.
- D. Use Cain and Abel on the ForensicsPractice virtual machine. It’s already installed in the CS549 account. The password for the CS549 account is **T549cstt**

7.2.1 Cain and Abel Brute Force Attack

1. Download and install Cain and Abel. I suggest you get it from the developer's web site:

<http://www.oxid.it/cain.html>

You may also want to check out the User Manual, which is at the same site. Note - I've had trouble reading the User Manual in Chrome, but it works in Internet Explorer.

2. Create new Windows user accounts. I suggest making at least 3 and using various length passwords for each account. If you need help creating the users and setting passwords you can get instructions from the following sites:

<http://windows.microsoft.com/en-us/windows/create-user-account#create-user-account=windows-7>

<http://pcsupport.about.com/od/windows7/ht/change-another-users-password-windows-7.htm>

- a. Set the password for the first account to something that uses 3 alphanumeric characters like 123 or abc. I know this isn't a good password, and it isn't something you would use in the real world. But it will take Cain and Abel very little time to crack and allow you to gain experience using Cain and Abel. Ensure that you only use lower case alpha characters or numbers. If you use other characters then Cain and Abel will be able to break the password, but you won't be able to use the default character set in the Brute Force attack.
 - b. Set the password for the second account to something that uses 4 or 5 alphanumeric characters like 1234 or house. Cain and Abel will still be able to crack this password, but it will take a little longer.
 - c. Set the password for the third account to something that uses at least 6 alphanumeric characters. This will allow you to see how the number of characters in a password affects the time to crack it.
3. Start Cain and Abel and do the following:
 - a. Click on the Cracker Tab (the icon that looks like a key) to open the password cracker
 - b. Add some accounts (usernames and passwords) to crack by clicking the + symbol on the toolbar. If it's grayed out, click in the right pane.
 - c. Choose **Import Hashes from local system**. All of the accounts for the local Windows system should now be displayed in the right pane.

- d. Start the password crack for an account by right-clicking the account and selecting the attack method. To begin, choose the account you created that uses the 3 character password. If you are using XP select **Brute Force Attack**, and then **LM Hashes**. If you are using Windows Vista, 7 or later select **Brute Force Attack**, and then **NTLM Hashes**.
- e. Once the password is cracked it will be displayed in the dialog box and then in NT Password column of the main display. The 3 character password should take less than a second to crack. However, if you used characters other than lower alpha or numerals, you'll have to enter those in the Custom Character set field and start the attack again.
- f. Repeat this process for the other accounts and passwords. Note the approximate amount of time it takes to crack each password, or if it the approximate time is longer than you want to wait.
- g. OPTIONAL – you can create longer passwords to see how the length of the password affects the approximate crack time. Not how long the passwords have to be before the length of time moves from days into years.

7.2.2 Cain and Abel Dictionary Attack

In this exercise you will gain experience using a dictionary attack. You will download a file of words to use during the attack, and then run the attack with Cain and Abel.

1. Set up the test accounts and passwords in Windows. You can either use the Windows accounts you created previously, or create new accounts. In either case, assign passwords that follow these patterns:
 - a. Create a password that is at least 8 characters but is a common word such as `password`
 - b. Create a password that is at least 8 characters, and is a common word with additional characters before or after the common word. For example `password44` or `66password`
 - c. Create a password that is at least 8 characters that starts with a common word but replace some of the alpha characters with symbols. For example modify `password` by replacing the `s` characters with `$` so it becomes `pa$$word`
2. Use of the following methods to obtain a dictionary or list of words:
 - a. Download a word list from the Internet. Make sure and get a free one, there are plenty available. The following sites have links to various dictionaries and rainbow tables.

<https://xato.net/passwords/more-top-worst-passwords/>

<http://cyberwarzone.com/massive-collection-password-wordlists-recover-lost-password/>
 - b. Most online dictionaries are very large, so it may be simpler to create your own dictionary. You can do this by simply opening a text editor and adding words. However

the file must be saved in plain text format. So if you use an editor like Microsoft Word make sure you choose **Save As** and save the file as plain text.

- c. Copy the file **10k most common.txt** from Canvas. This file contains ~10,000 of the most commonly used passwords. **WARNING** - some of the words in this file are profane so if you profanity bothers you don't use the file, or just don't look at its content.
3. Add words to the dictionary.
 - a. Open the dictionary and add at least one of the passwords you created in step 1.
 - b. Save the dictionary file in a place where you can find it, like the Desktop.
 4. Start Cain and Abel and do the following:
 - a. Click on the Cracker Tab (the icon that looks like a key) to open the password cracker
 - b. Add some accounts (usernames and passwords) to crack by clicking the + symbol on the toolbar. If it's grayed out, left click in the right pane. If you want to clear out the accounts from previous attempts right-click in the right pane and select XXX
 - c. Choose **Import Hashes from local system**. All of the accounts for the local Windows system should now be displayed in the right pane.
 - d. Start the password crack for an account by right-clicking the account and selecting the attack method. If you are cracking an XP account select **Dictionary Attack**, and then **LM Hashes**. If you are using Windows Vista, 7 or later select **Dictionary Attack**, and then **NTLM Hashes**.
 - e. This will open the Dictionary Attack dialog box. Right-click in the **Dictionary** section and select your dictionary file.
 - f. Check the options for creating hybrids of the dictionary words.
 - g. Click **Start** to begin the attack. Note the approximate amount of time required to crack the password.
 5. Repeat Step 4 for the other accounts and passwords you created. Note the amount of time required to crack the password. If the attack fails, note how long it takes to run through all of the words in the dictionary and the selected hybrids.

7.2.3 Cain and Abel Creating Rainbow Tables

In this exercise you will gain experience creating a Rainbow Table, so you have some idea how long the process takes. You will download and use **wirtgen**, a program that creates a Rainbow Table for a brute force attack.

1. If necessary download and install **wirtgen**.

<http://www.oxid.it/projects.html>

2. Start **wirtgen**.

- a. Start by selecting the upper case alpha characters as the character set (charset).
- b. Set the minimum length (Min Len) to 4 as there probably aren't many passwords shorter than 4 characters.
- c. Set the maximum length (Max Len) to 7. Normally you would make this longer, but as you'll see this greatly increases the amount of time required to generate the Rainbow Table.
- d. Leave the other settings alone unless you do some extra research to understand what the Chain Length and Chain Count settings do.
- e. Click the Benchmark button to get an estimate of how long it will take to generate the Rainbow Table with these settings. Write down the estimated time in the space below:

- f. Change the character set to add in more characters. For example select the mix-alpha or alpha-numeric. Leave the other settings the same.
- g. Press the Benchmark button to get an estimate of the generation time. Does adding extra characters seem to add much time? Write down the estimated time in the space below:

- h. Return the character set to Alpha.
- i. Change the maximum length to 10 characters.
- j. Press the Benchmark button to get an estimate of the generation time. Does checking longer passwords seem to add much time? Write down the estimated time in the space below:

3. Use your test results to answer the following questions:

- a. Is the amount of time to generate a Rainbow Table best measured in seconds, minutes, hours, days, weeks or months?

- b. Which has a greater impact on the amount of time required to generate a Rainbow Table, the number of characters in the brute force character set or the maximum password length?

7.2.4 Practice Cracking Windows User Passwords

In this exercise you will practice using Cain and Abel to crack the password for different Windows user accounts in the Forensics Practice virtual machine (ForensicsPractice.ova). The passwords for the following accounts are relatively short and made up from lower case alpha characters only so they should crack fairly quickly with a brute force attack.

- a. Username: Carolyn
Password: _____
- b. Username: Mike Jackson
Password: _____
- c. Username: Cave Johnson
Password: _____

The passwords for the following accounts are all 6 characters in length and comprised of lower case alpha characters, so you could use a brute force attack. However the passwords are also common passwords so you could try a dictionary attack. Hint – if you do the dictionary attack use dictionary file **10k most common.txt**.

- a. Username: jed
Password: _____
- b. Username: serita
Password: _____

The passwords for these accounts are 7 characters or longer which means they could take quite a while to crack using a brute force attack. , However the passwords are also common passwords so it would make sense to try a dictionary attack. Hint – if you do the dictionary attack use dictionary file **10k most common.txt**.attack with the common passwords in the file **10k most common.txt**.

- c. Username: sweetcheeks
Password: _____
- d. Username: ferrari
Password: _____

The user for this account is a Star Trek fanatic. This is a hint for you to use a custom dictionary that includes Klingon words.

- e. Username: Bill Shatner
Password: _____

7.2 Cracking Windows Passwords from an Image

In this set of exercises you will gain experience cracking Windows passwords from a forensics disk image. Most of the process is the same as cracking passwords for a live system; the main difference is that you have to extract the SAM and SYSTEM registry files from the image. Remember that a disk image is like a .zip file, it has many files inside of a single file. So before Cain and Abel can find the passwords, the SAM file (and maybe the SYSTEM file) must be pulled out of the disk image.

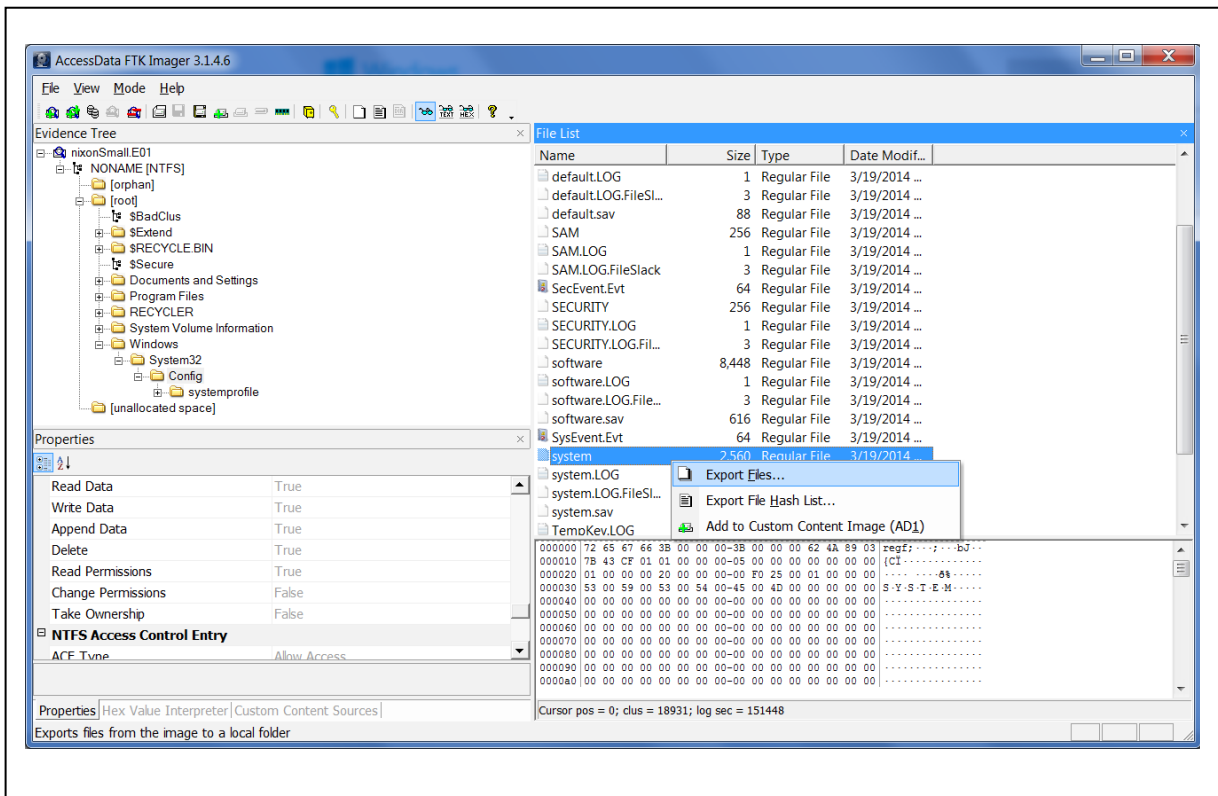
All of the disk images used in this set of exercises are in the zip file **password cracking practice.zip**.

7.3.1 Step-By-Step Using Cain & Abel to Crack Passwords from SAM and SYSTEM

This exercise provides step by step instructions for opening a forensics disk image and exporting the registry files required for Cain and Abel to crack passwords.

You can either do this exercise on your own virtual machine, or on the ForensicsPractice virtual machine. If you want to run it on your own VM you must download the image file **Toshiba-password-practice.E01** from Canvas. To do this exercise on the ForensicsPractice vm ensure that it's started, then login to the virtual machine as user **CS549**. The password is **T549cstt**

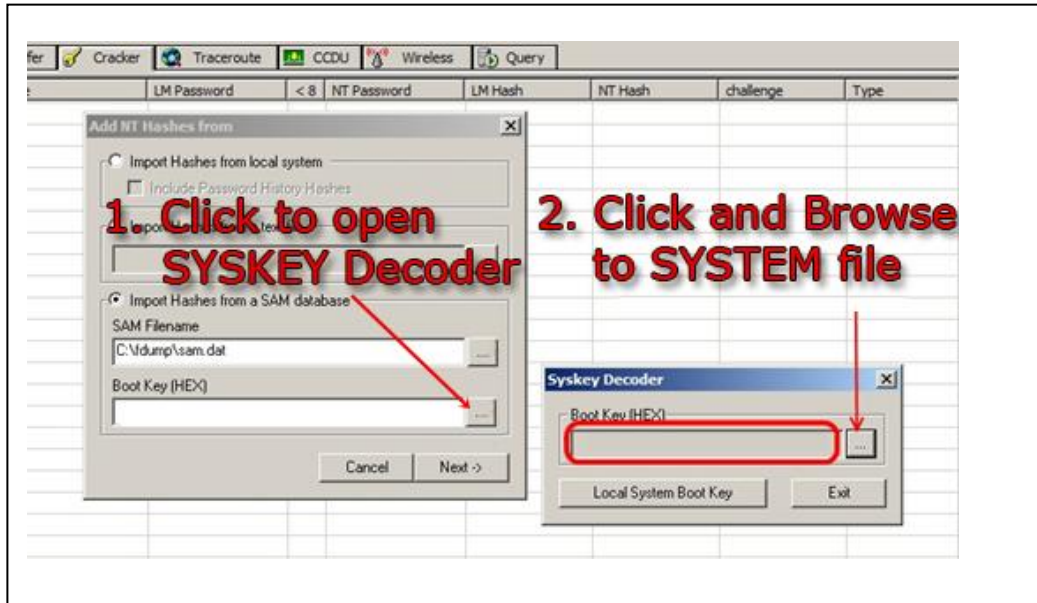
1. Extract the SAM and SYSTEM registry files. For this step you can use either FTK or FTK Imager. Go back to the FTK videos if you need to review using these tools.
 - a. Start FTK Imager. This is on the desktop for the CS549 user in ForensicsPractice.
 - b. Select **File > Add Evidence Item** and open the disk image **Toshiba-password-practice.E01**. This image is in the folder **practice images** on the Desktop for the CS549 user in ForensicsPractice.
 - c. Expand the Evidence Tree to see the main drive, then down into the **Windows\System32\Config** folder.
 - d. Right click the SAM file and select **Export Files**. It is suggested that you save the file to a folder on the Desktop named ToshibaPasswords. You can save the SAM (and SYSTEM) files to a different folder if you wish. Just make sure that you remember where you put them.
 - e. Right click the SYSTEM file and select **Export Files**. It is suggested that you save the file to the same folder as the SAM file.



2. Load the Windows accounts and passwords into Cain by doing the following:
 - a. Start Cain and Abel. This is on the desktop for the CS549 user in ForensicsPractice.
 - b. Select the **Cracker** tab. Have Cain find the Windows accounts and passwords by either clicking the **+** or right-clicking and selecting **Add to list**.
 - c. Select **Import hashes from a SAM database**. Browse to the SAM file you extracted in the previous step and select it.

3. Load the Windows SYSKEY into Cain. Remember that Windows has an option for using a salt called the SYSKEY when it hashes the passwords. If present, the SYSKEY is stored in the **SYSTEM** registry file. NOTE – it's a common mistake to think the SYSKEY is loaded in the SECURITY file.
 - a. Click the Browse button by the **Boot Key (HEX)** box. This will open the **Syskey Decoder** dialog box.

- b. Click the browse button, then browse to the SYSTEM file you exported from the disk image and select it.
- c. The decoded Boot Key will appear in the dialog box. However, this Boot Key will NOT be automatically transferred back to the **Add NT Hashes** dialog box. You must highlight the Boot Key and hit **<ctrl-c>** to copy it. Next, click the Exit button to close the **Syskey Decoder** dialog box. Click inside the **Boot Key (HEX)** text box back on the **Add NT Hashes** dialog box and then hit **<ctrl-v>** to paste the Boot Key.



- d. Click the Next button. The list of users and hashed passwords in the Registry files will now be displayed in Cain. You can begin cracking the passwords.

7.3.2 Practice Cracking Windows User Passwords From Disk Image

All of the disk images used in this set of exercises are in the zip file **password cracking practice.zip**.

1. Crack the passwords for the following accounts from **Mantooth.E01**. If no password is set, write **empty**. Hint – this image is from a computer running XP. Notice that the NTLM hashes for the accounts with passwords are set to different values. These are both clues that the NTLM hash is being used, NOT the LM hash.

- a. Username: Wes Mantooth
Password: _____
- b. Username: Dracula
Password: _____
- c. Username: Laurent
Password: _____
- d. Username: Administrator
Password: _____
- e. Username: Guest
Password: _____

2. Crack the passwords for the following accounts from **Washer.E01**. If no password is set, write **empty**.
Hint – this image is from a computer running XP. Notice that the LM hashes for the accounts with passwords are set to different values. These are both clues that the LM hash is being used, NOT the NTLM hash.

- a. Username: Administrator
Password: _____
- b. Username: Help Assistant
Password: _____
- c. Username: SUPPORT_388945a0
Password: _____
- d. Username: Guest
Password: _____
- e. Username: Billy Bob Brubeck
Password: _____
- f. Username: The Wolf
Password: _____
- g. Username: Mr Smee
Password: _____
- h. Username: Captian Hook
Password: _____

3. Crack the passwords for the following accounts from **toshiba-password-practice.ad1**. If no password is set, write **empty**.

Hint 1 – this image is from a computer running Windows 7. Notice that the NTLM hashes for the accounts with passwords are set to different values, while the LM hashes are all the same. This is a clue that the NTLM hash is being used, NOT the LM hash.

Hint 2 – All of the passwords in this exercise use lower case characters or numerals. The shortest is 5 characters and the longest is 7 characters.

- a. Username: Dash
Password: _____
- b. Username: Miles
Password: _____
- c. Username: race
Password: _____
- d. Username: Ricky Ricardo
Password: _____
- e. Username: Colonel Sanders
Password: _____

4. Crack the passwords for the following accounts from **starwars-password-practice.ad1**. If no password is set, write **empty**.

Hint 1 – this image is from a computer running Windows 7. Notice that the NTLM hashes for the accounts with passwords are set to different values, while the LM hashes are all the same. This is a clue that the NTLM hash is being used, NOT the LM hash.

Hint 2 – All of the passwords in this exercise are related to Star Wars or Clone Wars. You could try a brute force attack, but the passwords are up to 10 characters in length. Since the passwords are so long, you should probably use the starwars.txt dictionary.

- a. Username: han solo
Password: _____
- b. Username: Mace
Password: _____
- c. Username: Jabba
Password: _____
- d. Username: Ventress
Password: _____

5. Crack the passwords for the following accounts from **gateway-password-practice.ad1**. If no password is set, write **empty**.

Hint – this image is from a computer running Windows 7. Notice that the NTLM hashes for the accounts with passwords are set to different values, while the LM hashes are all the same. This is a clue that the NTLM hash is being used, NOT the LM hash.

- a. Username: bob (Hint – all lower case letters)
Password: _____
- b. Username: eric (Hint – all lower case letters)
Password: _____
- c. Username: jim (Hint – 7 characters all lower case.)
Password: _____
- d. Username: sara (Hint – 7 characters. All lower case letters and numerals)
Password: _____
- e. Username: Bruce Wayne (Hint – 7 characters. Lower and upper case letters)
Password: _____

7.3 BITLOCKER EXERCISES

In this set of exercises you will gain hands on experience using BitLocker, using Passware to crack BitLocker passwords, and using Elcomsoft to discover BitLocker recovery keys.

7.3.1 Using BitLocker

This exercise provides you with experience in setting, using and managing BitLocker. If you have previous experience with BitLocker you can skip this exercise. If you are going to do this exercise please make sure and read the following cautionary notes carefully:

- **Check your OS Version** – BitLocker is available in all editions of Windows except the Home edition. If you have the Home edition you will not be able to complete this exercise.
- **Do NOT add BitLocker to any drives you do not own.** In particular, do not enable BitLocker on any of the college computers. If you do you will face penalties that include flunking the class, expulsion, or possible criminal charges.
- **Choosing a drive to encrypt** - This exercise requires setting BitLocker on one your own drives. I strongly suggest you set BitLocker on the smallest thumb drive you own and that you do NOT set BitLocker on your main system drive. Once you gain some experience with BitLocker and understand the costs and benefits you can make the decision whether or not to encrypt your main drive, but for now use a small thumb drive if you have one available.
- **Backup files before enabling BitLocker** – The process of enabling and disabling BitLocker is stable and safe, but you should backup any critical files before enabling BitLocker just to be safe.
- **Do NOT remove the drive during encryption** - When you enable BitLocker Windows will encrypt the data on your disk. If you have a small drive this won't take long, but it can take a significant amount of time on larger drives. Once the encryption starts you must let it complete

before removing the drive. Make sure and heed the warnings that Windows displays and do NOT remove the drive while the files are being encrypted. If you do the drive will be unusable.

- **Document passwords and Recovery Keys** – Make sure and write down your BitLocker password and save your Recovery Key somewhere besides on the drive you encrypt.

1. Insert the thumb drive into your computer. Go to My Computer. Right-click on the thumb drive and select **Turn On BitLocker**
2. Windows will check the drive to ensure that it will be able to run BitLocker. Do not remove the drive during this process. When Windows is ready, it will display the Bitlocker Drive Encryption dialog box. Check the **Use a Password to Unlock the Drive box**, and enter the password you want to use. The password must be at least 8 characters. If you plan on actually using Bitlocker after this exercise you should create a strong password. If you're just adding Bitlocker for this exercise remember that in demo mode Passware will only run for 60 seconds before stopping so your password needs to be one that will be found quickly with a brute force attack such as 00000001, or a common password like Aberdeen that will be found with a dictionary attack using Passware's default dictionary.

Record the password in the space below:

3. Click the **OK** button. Windows will now force you to either print the Recovery Key or save it to a file. I suggest you save it to a file.
4. Click the **OK** button to begin encrypting the drive. This can take a long time, depending on the size of the drive and the amount of data on the drive. Do NOT remove the drive or shut down the computer without first pausing the process.
5. When the encryption has finished test it by performing these steps:
 - a. Safely eject the thumb drive.
 - b. Reinsert the thumb drive. The dialog box that prompts for the BitLocker password should be displayed.
 - c. After the correct password is entered you should be able to use the drive and the files on the drive as you normally would. Verify this by performing basic actions such as copying files to the drive, copying files from the drive, creating folders on the drive etc.



6. When you're finished with the other exercises in this section you can remove the BitLocker encryption if you wish. Don't do this now, wait at least until you've finished creating the forensics disk image of the thumb drive in the next step. When you're ready to turn off Bitlocker follow these steps:
 - a. Go to the Windows Start Button and type "bitlocker" in the Search box.
 - b. Choose **Bitlocker Drive Encryption**
 - c. Find the thumb drive in the display and click on **Turn Off Bitlocker**. Removing the encryption can take a long time, depending on the size of the drive and the amount of data on the drive. Do NOT remove the drive or shut down the computer without first pausing the process.

7.3.2 Use Passware to Crack the Bitlocker Password On Your Drive

In this exercise you will crack Bitlocker password on the drive you encrypted in the previous exercise. This entails creating an image of the Bitlocker enabled drive and then using Passware to crack the password.

1. Create the disk image file of the Bitlocker enabled drive. This is just like the drive imaging you have performed previously, there are no special steps for Bitlocker enabled drives.
 - a. Ensure the Bitlocker enabled thumb drive is mounted in your computer.
 - b. Start FTK Imager. (Note – this is FTK *Imager*, not FTK.)
 - c. Choose **File > Create Disk Image**

- d. Select **Physical Drive** for the Evidence Type and click **Next**
 - e. Select the thumb drive from the pull down list. You should be able to recognize it by the size. Click the **Finish** button.
 - f. The Create Image dialog box will be displayed. Click the **Add** button, then select Raw (dd) for the image type. Click the **Next** button.
 - g. You fill in Evidence Information if you wish, or leave it blank and click the **Next** button.
 - h. Choose the Image Destination Folder. I suggest you choose the Desktop or someplace where the disk image file will be easy to find. Set the Image Filename and click the **Finish** button.
 - i. This returns you to the Create Image dialog box. Verify that the output image file is displayed in the list, then click the **Start** button. The image file will be created. This may take several minutes.
2. Use Passware to crack the Bitlocker password for the thumb drive.

- a. Download and install Passware if necessary. If you are using the ForensicsPractice virtual machine there is a copy on the desktop of the CS549 user. If you need to download it, Passware is available from Canvas or from:

<http://www.lostpassword.com/>

- b. Start Passware. In the right panel choose the **Full Disk Encryption** link.
- c. Choose the **Bitlocker** link.
- d. Click the **Browse** button by the **Encrypted Bitlocker Image File** box, and select the disk image you created above. Note – FTK Imager may have added a `.001` to the end of the image file name. For example, if you said to name the image file `thumb1.dd` FTK will call it `thumb1.dd.001`. By default Passware only displays files with image file extensions such as `.dd` or `.E01`, so you'll have to tell Passware to display files of all types. Select the file and click **Open**.
- e. Click the **Next** button. At this point you can set the parameters for the password cracking. You can either run the Wizard, choose predefined settings, or choose Advanced and set up a custom attack. You can test the various settings, but I suggest you set the minimum password length to 8, since this is Bitlocker's minimum.

If you used a "bad" password such as `00000001` or `Aberdeen` Passware should crack it pretty quickly. If you chose a stronger or longer password Passware could probably crack it, but Passware is in demo mode which means it will stop after 60 seconds and you may not get a result.

If it cracks the password Passware will display the first 3 characters. It's cracked the entire password, but since we're running Passware in demo mode they don't show it all to you.

7.3.3 Practice Cracking Bitlocker Passwords with Passware

Use the **Passware Forensics Kit Recovery Demo** to crack the bitlocker passwords on the 5 thumbdrive images. Remember you will only be able to reveal the first 3 characters. The thumb drive images are all in the zip file **bitlocker Practice.zip** which is available from Canvas. Note - always set the attacks for passwords that are 8 characters in length.

- A. First 3 characters of image of **thumbdrive1.dd** – set to dictionary attack using the dictionary **bitlockerDictionary.txt**, 8 characters _____
- B. First 3 characters of image of **thumbdrive2.dd** – set to dictionary attack using the dictionary **bitlockerDictionary.txt**, 8 characters _____
- C. First 3 characters of image of **thumbdrive3.dd** – set to dictionary attack using the dictionary **bitlockerDictionary.txt**, 8 characters _____
- D. First 3 characters of image of **thumbdrive4.dd** – set to dictionary attack using the dictionary **bitlockerDictionary.txt**, 8 characters _____
- E. First 3 characters of image of **thumbdrive5.dd** – set to dictionary attack using the dictionary **bitlockerDictionary.txt**, 8 characters _____
- F. First 3 characters of image of **thumbdrive6.dd** – set to dictionary attack using the default Passware dictionary, 8 characters _____
- G. First 3 characters of image of **thumbdrive7.dd** – set to dictionary attack using the default Passware dictionary, 8 characters _____
- H. First 3 characters of image of **thumbdrive8.dd** – set to brute force attack numbers only, 8 characters _____

7.4 BITLOCKER RECOVERY KEY WITH ELCOMSOFT

Note – this exercise is OPTIONAL.

In this exercise you will use Elcomsoft Forensic Disk Decryptor to retrieve the BitLocker recover key for an encrypted drive. Detailed instructions for using notMyFault and the Elcomsoft tool are available on the video for discovering the BitLocker recovery key

1. If necessary download and install the demo version of Elcomsoft Forensic Disk Decryptor. You can download it from the Elcomsoft web site at <https://www.elcomsoft.com/efdd.html> or from Canvas.

2. If necessary encrypt a thumb drive using BitLocker. (You will need to know the Recovery Key if you want to verify that the recovery found by the Elcomsoft tool is correct or not.) Connect the thumb drive to the computer. You do not have to supply the BitLocker password.
3. Download notMyFault from <https://technet.microsoft.com/en-us/sysinternals/notmyfault.aspx> or Canvas.
4. Generate a memory dump using notMyFault. Make sure that you are capturing all of memory including the protected areas. Remember that this will cause your computer to reboot, so ensure that all of your work is saved before starting the memory dump.
5. Start Elcomsoft Forensic Disk Decryptor, load the memory dump file and check for the recovery key. This tool will display the first few characters of the recovery key after it is found.

7.5 BITLOCKER REVIEW QUESTIONS

1. True or False. BitLocker can only be applied to entire drives. That is, it is not possible to encrypt a single file or folder using BitLocker.
 - a. True
 - b. False
2. Which of the following is true regarding BitLocker passwords?
 - a. The password is encrypted and stored in one of three locations: on the drive, on a smart card, or in a TPM.
 - b. The password is hashed and stored in one of three locations: on the drive, on a smart card, or in a TPM.
 - c. The password is broken into sections and stored in different locations on the drive. When the drive is mounted Windows reconstructs the sections and stores the reconstructed password in memory.
 - d. The password is hashed using the SYSKEY and stored in the SAM file.
 - e. None of the above are true
3. Which of the following is true regarding BitLocker recovery keys?
 - a. The recovery is encrypted and stored in one of three locations: on the drive, on a smart card, or in a TPM.
 - b. The recovery key is hashed and stored in one of three locations: on the drive, on a smart card, or in a TPM.
 - c. The recovery key is broken into sections and stored in different locations on the drive. When the drive is mounted Windows reconstructs the sections and stores the reconstructed password in memory.
 - d. The recovery key is hashed using the SYSKEY and stored in the SAM file.
 - e. None of the above are true

4. Which of the following is true regarding the Passware tool for gaining access to BitLocker encrypted drives?
 - a. The Passware tool attempts to crack the BitLocker password. If the user created a strong password the Passware tool may not crack the password in a reasonable amount of time.
 - b. The Passware tool recovers the BitLocker password from a memory dump. Creating the memory dump may take several minutes, but once this step is completed recovering the password occurs quickly. The strength of the password has no effect on recovery time.
 - c. The Passware tool will only crack the BitLocker password if the user did not specify using the SYSKEY salt.
 - d. The Passware tool attempts to crack the BitLocker recovery key. If the user created a strong recovery key the Passware tool may not crack it in a reasonable amount of time.
 - e. The Passware tool recovers the BitLocker recovery key from a memory dump. Creating the memory dump may take several minutes, but once this step is completed finding the recovery key occurs quickly. The length of the recovery key has no effect on recovery time.
 - f. The Passware tool will only crack the BitLocker recovery key if the user did not specify using the SYSKEY salt.
 - g. None of the above are true.

5. Which of the following is true regarding the Elcomsoft tool for gaining access to BitLocker encrypted drives?
 - a. The Elcomsoft tool attempts to crack the BitLocker password. If the user created a strong password the Elcomsoft tool may not crack the password in a reasonable amount of time.
 - b. The Elcomsoft tool recovers the BitLocker password from a memory dump. Creating the memory dump may take several minutes, but once this step is completed recovering the password occurs quickly. The strength of the password has no effect on recovery time.
 - c. The Elcomsoft tool will only crack the BitLocker password if the user did not specify using the SYSKEY salt.
 - d. The Elcomsoft tool attempts to crack the BitLocker recovery key. If the user created a strong recovery key the Elcomsoft tool may not crack it in a reasonable amount of time.
 - e. The Elcomsoft tool recovers the BitLocker recovery key from a memory dump. Creating the memory dump may take several minutes, but once this step is completed finding the recovery key occurs quickly. The length of the recovery key has no effect on recovery time.
 - f. The Elcomsoft tool will only crack the BitLocker recovery key if the user did not specify using the SYSKEY salt.
 - g. None of the above are true.

6. Assume you are asked to recommend purchasing either the Passware tool or the Elcomsoft tool for decrypting drives that have been encrypted with BitLocker. Which would you recommend and why.

7. Assume you are asked to check a hard drive that has been encrypted with BitLocker for evidence of a crime. In particular you are asked to recover the user names and passwords for the Windows accounts. Which of the following describes the steps in the process you should follow to retrieve the Windows user names and crack the passwords?
 - a. There is no way to accomplish this task. The Windows usernames and passwords cannot be retrieved from a drive encrypted with BitLocker.
 - b. Run a Windows password crack tool such Cain and Abel or OphCrack. These tools will be able to read the SAM and SYSTEM files on the encrypted drive and use this information to crack the user names and passwords.

- c. Create a forensics image of the hard drive. Next extract the SAM and SYSTEM files. Run Cain and Abel and use it to display the Windows user names and crack their passwords.
- d. Use either the tool from Passware to crack the BitLocker password or the tool from ElcomSoft to retrieve the BitLocker Recovery key. Next decrypt the drive and recover the SAM and SYSTEM files. Finish by using a Windows password cracking tool such as Cain and Abel or OPHCrack to retrieve the Windows user names and crack the account passwords.

7.6 EFS EXERCISES

In this exercise you will set up EFS encryption to protect a folder. You will then open the folder in FTK to see how it handles it. To finish, you will try and recover the EFS password. NOTE – EFS isn't available for all versions for Windows. For Windows 7 it's only available for Windows 7 Professional and Ultimate.

Note – These exercises require logging in as different users, so you'll need to either do them on your personal computer, or in a virtual machine. That is, you'll need access to at least two different Windows user accounts. If you are using one of the computers in the CBC Computer Science Labs you will have to use a virtual machine.

7.5.1 Step-By-Step Setup the EFS Encryption

1. Open Windows Explorer, and select the folder you want to encrypt. You can either use an existing folder, or create a new one. Right-click the folder then click **Properties**. The Properties dialog box will be displayed.
2. Ensure you're on the **General** tab, click the **Advanced** button. The Advanced Attributes dialog box will be displayed.
3. Check the **Encrypt Contents to Secure Data** box and click **OK**.
4. The Confirm Attribute Changes dialog box will be displayed. You will be asked if you want to encrypt the current folder, or the current folder and all its sub-folders. For this test, you can choose either option. Click **OK**.
5. That's all there is to the setup. It's so simple that sometimes it's hard to realize that anything has been done. The main clue that you have that the folder is encrypted is that folder will look like any other folder except it will have green text to remind you it's encrypted. Windows will automatically encrypt any files you add to the folder. It will also automatically decrypt them for you, but it uses your login credentials so you'll be the only user that can see the decrypted information.

If you get the message: "Recovery policy configured for this system contains invalid recovery certificate" you may have to renew the certificate. The following web site has the instructions for doing this:

<https://social.technet.microsoft.com/Forums/windowsserver/en-US/f514129b-bab7-4cad-a179-f53f9abdc826/efs-recovery-policy-contains-invalid-recovery-certificate>

7.5.2 Test the EFS Encryption

In this step you will test the EFS encryption/protection by turning on EFS for a folder as one user, then trying to access it as a different user. You can do this on any computer where you have permission to create new users. If you are in the CBC Computer Science Lab you should do this on the virtual machine.

1. Start Windows Explorer and move to the top folder in the C: drive. Create a new folder and add some files including at least 1 plain text file. You can also create Word documents, image files etc.; but ensure that you have at least 1 plain text file as the decryption tool will only decrypt the first 512 bytes of each file when it runs in demo mode. This means that decrypted files like image files or Word file won't display because they need the entire file decrypted to display it. Ensure that you can read or display the files in this folder.
2. Enable EFS for this folder. Ensure that the folder is green
3. Log out of Windows. Log back in as a different user.
4. Return to the top folder in the C: drive and try and access the files in the EFS encrypted folder. Can you view the file names? Can you open and display any of the files?

7.5.3 Step-By-Step Recover the EFS Encrypted Files

If you have paid for FTK and PRTK you can export the folder from FTK, then use PRTK to recover the encrypted files. If you don't have PRTK you can use a demo version of the Elcomsoft Advanced EFS Data Recovery Tool

1. Download and install <http://www.elcomsoft.com/aeafsdr.html> - Elcomsoft Advanced EFS Data Recovery Tool (Scroll to the bottom of the page for the trial download link). If you are using the Virtual Machine **ForensicsPractice** this program is already loaded and available if you are logged in as the CS549 user. Go to the **Windows Start Button**, the select **All Programs > Elcomsoft Password Recovery > Advanced EFS Data Recovery**.
2. Run the Recovery Tool. You can either run the Wizard or do the following 3 steps yourself. Remember that these steps can be run in any order, but you will need to do all of them.
 - a. Find the EFS encryption Keys. Click the **EFS Related Files** tab, then click the **Scan for Keys** button. This may take some time.
 - b. Find the EFS encrypted files. Click the **Encrypted Files** tab, then click the **Scan for Encrypted Files** button. This may take some time.
 - c. Add the other ½ of the PKI key, which is the Windows Username and Password for the owner of the EFS folder. This of course means that you need to know this information. In a real forensics investigation this may require you to crack the Windows password. Return to the

EFS Related Files tab. Click the **Add User Password** button. Enter the Windows username and password, then click the **Add** button. The program will then decrypt any keys associated with this user.

- d. Return to the **Encrypted Files** tab. Any EFS encrypted files owned by the Windows user should now be green, which means they can be decrypted. Check the box for each file, then click the **Decrypt** button on the main toolbar. Choose a folder to store the decrypted files in. I suggest you put it somewhere on the desktop.
- e. When the program has finished, inspect the folder to ensure the files have been decrypted. However, remember that in demo mode the program only decrypts the first 512 bytes, so the only files you'll be able to view or read will be things like plain text files.

7.5.4 EFS Practice 1

The following exercises provide practice breaking EFS encryption. Use the Virtual Machine ForensicsPractice for these exercises.

1. Login to Virtual Machine as user **CS549**. The password for this account is **T549cstt**.
2. Click the **Windows Start Button** and select either **Computer** or **Documents**. Navigate to the home directory for the **jed** user which is **C:\Users\jed\My Documents**. Which folder is encrypted with EFS?
3. Open EFS encrypted folder. Try and view files. Are you successful or do you see an error message?
4. Run **Elcomsoft aefsd** tool and decrypt the files in this folder. If you are using the Virtual Machine **ForensicsPractice** this program is already loaded and available if you are logged in as the CS549 user. Go to the **Windows Start Button**, then select **All Programs > Elcomsoft Password Recovery > Advanced EFS Data Recovery**.

You will need the username and password for the Jed account. Obviously the username is **Jed**, but you will need to use the password that you cracked previously. Remember you will only be able to see the first 512 bytes of decrypted files. Inspect the files and try to determine what the main subject of all the files in the folder is:

- A. Tea
- B. Tornadoes
- C. Tesla
- D. Turkey
- E. Telephones
- F. Tacos
- G. None of the Above

7.7 EFS REVIEW QUESTIONS

1. What is EFS?
 - a. *A feature of Microsoft Windows that allows users to encrypt files and folders.
 - b. A feature of Microsoft Windows that allows users to encrypt email messages.
 - c. A third party product that allows users to encrypt files and folders.
 - d. A third party product that allows users to encrypt email messages.

2. Assume you encrypt a file or folder using EFS. Where is the encrypted FEK used to decrypt the files stored?
 - a. In the SAM portion of registry.
 - b. In the local secrets portion of registry.
 - c. In the users NTUser.dat.
 - d. *In an Alternate Data Stream called \$EFS for the encrypted file.
 - e. In the file header.

3. Who can read files protected by EFS (without hacking the encryption)?
 - a. *The owner.
 - b. The owner and any user with Administrator privileges.
 - c. The owner, any user with Administrator privileges, and any user with the EFS password.
 - d. The owner and any user with the EFS password.

4. True or False. Once EFS encryption is enabled it cannot be disabled or turned off.
 - a. True
 - b. *False

5. Which of the following that once enabled cannot be disabled or turned off?
 - a. *Windows password salting with SYSKEY
 - b. BitLocker
 - c. EFS
 - d. Application level encryption (such as Word or PDF encryption)

6. Assume a user has enabled EFS on a folder. What steps are required to read or write files from the folder?
 - a. The user must supply the password each and every time they read files in the folder or try to write new files into the folder.
 - b. The user only needs to supply the password once when they login. After that they will be able to read files in the folder or write new files in the folder without supplying any other information.
 - c. The user only needs to supply the password once per login, when they first try to access the folder. After that they will be able to read files in the folder or write new files in the folder without supplying any other information.
 - d. *The user only needs to login to Windows. Windows will then automatically allow users to access any EFS encrypted files or folders.
 - e. None of the above are true.

7.8 APPLICATION ENCRYPTION EXERCISES

In this set of exercises you will use the encryption built into applications like Microsoft Word or .ZIP files to protect the content of the file. You will then use different tools to crack the password used to protect the encrypted file.

7.5.1 Practice Cracking Microsoft Office Passwords

In this exercise you will create your own password protected Word files, and then use a tool to crack the password. Note – you must do this exercises on a computer that has Microsoft Word installed. Word is NOT installed on the ForensicsPractice Virtual Machine, but it is installed on all of the computers in the CBC Computer Science Labs.

1. Create a test document (or two)

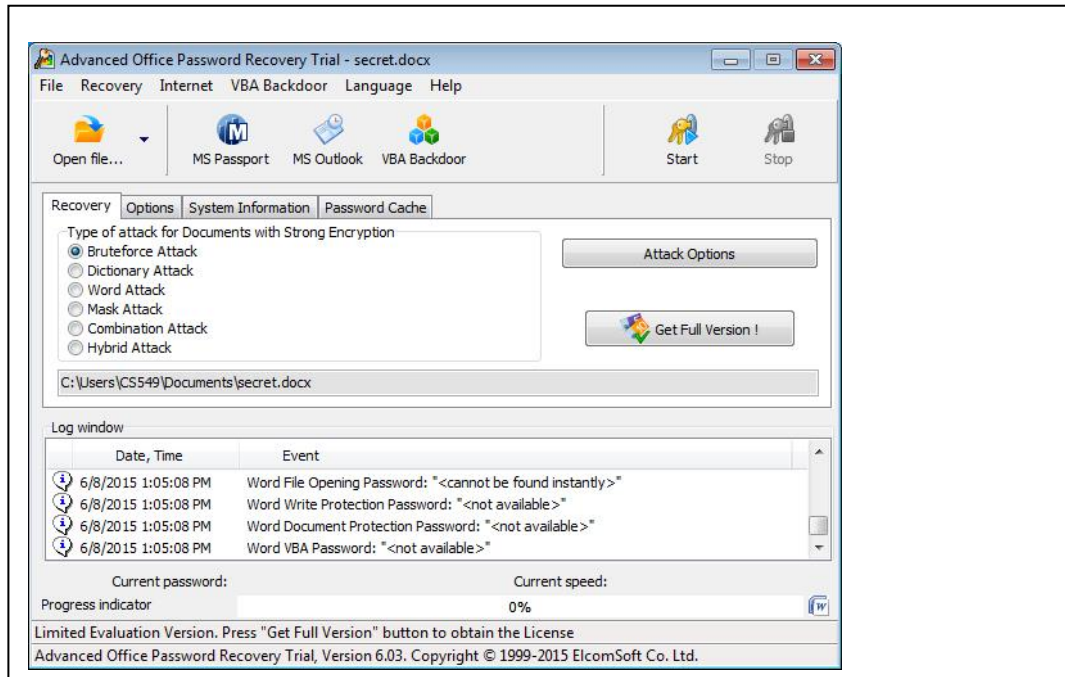
- A. Create a New Document in Microsoft Word. Enter some text.
- B. Save the file, encrypt it and add a password. **IMPORTANT** – The encryption used in older versions of Office was much easier to break, so you must save this document as an older version. If you save it as a newer version the password recovery tool won't be work. Choose **File / Save As**, then go to the **Save As Type** box and save the document as Word 97 – 2003 Document (*.doc) Also note where you save the file, as you'll need to use it later.
- C. Add a password to the file by selecting **File / Protect Document**. In newer versions of Office you will select **File > Info** and then click the **Protect Document** button. . Choose **Encrypt with Password**.
- D. You will be prompted to enter a password, and then to repeat the password. For the first test you should keep the passwords short, **3 characters or less**, and only use **lower case alpha characters**. For later tests you can make more complex passwords if you wish.
- E. Close the file
- F. Test the password protection by trying to reopen the file. You should be prompted to enter the password, and denied access if you fail to provide the correct password.

2. Crack the password

- A. If necessary download and install the demo version of the Elcomsoft **Advanced Office Password Recovery** (AOPR) tool. Check at the bottom of the following page for the link to the download for the demo version:

<https://www.elcomsoft.com/aopr.html>
- B. Start the AOPR tool
- C. Open the protected Word Document. AOPR will do a "Preliminary" attack using the default attack profile, which means it's going to do a brute force attack, starting with single character passwords. This isn't the most efficient attack, and AOPR takes a little time to calculate each password hash, so the Preliminary attack will take a long time to complete or to even find a 3 character password.

- D. To change the attack profile, click the **Stop** button. Click OK to clear all of the dialog and information boxes. Next, click the type of attack you want to perform, for example **Brute Force Attack** or **Dictionary Attack**. Click the **Attack Options** button to set options such as password length or dictionary to use. Click **OK** to close the Attack Options dialog box, then click Start to begin the attack.



It can take several minutes to even crack simple passwords, but if you followed directions and used 3 characters AOPR should be able to crack it.

3. Create harder test cases

- A. Repeat the steps for adding a password to a word document and create 4 new Word documents to use as test files. Save all of your Word documents in the same folder.
- 1) Create 1 file with a password that is 3 alphanumeric characters
 - 2) Create 1 file with a password that is 4 alphabet characters
 - 3) Create 1 file with a password that is 4 alphanumeric characters
- B. Run the AOPR and see if it can recover the passwords from the new files. Keep track of the relative time it takes for the different password lengths.

4. Default Dictionary and Custom Dictionaries

As you've experienced previously, using a dictionary can really speed up password recovery. That is it will speed it up if the password is found in the dictionary. AOPR will use a dictionary, but it doesn't come with a default so you have to specify a dictionary file any time you use the dictionary attack.

- A. Repeat the steps for adding a password to a word document and create 1 or 2 new Word documents to use as test files. Add passwords that are at least 8 characters, but that are also words that are found in the 10,000 most common passwords text file.
 - B. Run the AOPR and see if it can recover the passwords from the new files. Keep track of the relative time it takes for the different password lengths, and compare it with the amount of time required for the brute force attacks.
5. Trade files with another student, and see if you can recover the passwords they added.

7.5.2 Practice Cracking Microsoft Office Passwords Using Brute Force

In this exercise you will use the brute force attack in the AOPR tool to crack the passwords in the several Word Docs. If you are using the **ForensicsPractice** virtual machine the files are all in **Users\CS549\My Documents\secret word files** Folder. If you login as user CS549 (password T549cstt), you will see the folder in your **Documents** folder. Or, you can download the zip file secretWordFilesPractice.zip from Canvas and run AOPR on any computer.

1. File: **Why did the chicken cross the road.docx** (Hint - the password is 3 characters, all lower case alpha)
Password: _____
2. File: **Chicken2.docx** (Hint - the password is 3 characters, all numerals)
Password: _____
3. File: **Chicken3.docx** (Hint - the password is 4 characters, all lower case alpha. This may take a long time, so you can skip it if you wish.)
Password: _____
4. File: **Chicken4.docx** (Hint - the password is 3 characters, all lower case alpha)
Password: _____
5. File: **pwtest.docx** (Hint - the password is 4 characters, all numerals)
Password: _____
- 6.
7. File: **pwtest2.docx** (Hint - the password is 3 characters, all numerals)
Password: _____

7.5.3 Practice Cracking Microsoft Office Passwords Using A Dictionary Attack

In this exercise you will use the dictionary attack in the AOPR tool to crack the passwords in the several Word Docs. If you are using the **ForensicsPractice** virtual machine the files are all in **Users\CS549\My Documents\secret word files** Folder. If you login as user CS549 (password T549cstt), you will see the folder in your **Documents** folder. Or, you can download the zip file secretWordFiles.zip from Canvas and run AOPR on any computer.

1. File: **cn.docx** (Hint - use the dictionary **10k most common.txt**)
Password: _____
2. File: **lawyer.docx** (Hint - use the dictionary **10k most common.txt**)
Password: _____

7.0 LAB MANUAL – PASSWORDS & ENCRYPTION

WARNING – You must only crack passwords on your computers, systems where you have written authorization, or on college systems where you have the instructor's permission. Do **NOT** attempt to crack passwords on systems where you failed to obtain prior authorization. Even attempting to crack passwords on unauthorized systems is illegal and will result in criminal charges.

NOTE – many of the exercises in this section require running a virtual machine in Oracle Virtual Box. If necessary you must download, install and run Oracle Virtual Box, which is available from:

<https://www.virtualbox.org/wiki/Downloads>

If you have problems running Oracle Virtual Box on your computer the instructor will NOT be able to help you debug the installation; you will have to come to the CBC Campus and use one of the computers in the assigned Computer Science Lab. If you find yourself in this situation contact the instructor and make an appointment to get situated.

Once you have Oracle Virtual Box installed and running you will need to download and install a virtual machine image. The virtual machine image is **ForensicsPractice.ova** and can be downloaded from Canvas. The ova file is quite large, nearly 10 GB, so it may take some time to download. When the .ova file has downloaded, start Oracle Virtual Box, select **File > Import Appliance**, then browse to where you downloaded the ForensicsPractice.ova file. After the virtual machine has loaded you can start it by using any of the following methods:

- E. Select **Machine > Start**
- F. Select the virtual machine, then click the Green Arrow labelled **Start** in the main toolbar
- G. Right click on the virtual machine, then select **Start**
- H. Double click the virtual machine

7.9 Cracking Local Windows Passwords with Cain and Abel

In this exercise you will gain experience cracking passwords for Windows accounts using Cain and Abel. You will install Cain and Abel, create new Windows user accounts and assign passwords, then use Cain and Abel to decrypt the passwords.

Note – This exercise requires you to create new users accounts. In other words, you will need Administrator privileges. You will also need authorization to run Cain and Abel and crack the passwords on the computer. You won't be able to do this on any of the CBC computers because Cain and Abel will be blocked from installing by the security software. However, you have the following options:

- E. Install and run Cain and Abel on one of your own computers, as long you have authorization.
- F. Install Cain and Abel on a virtual machine on a computer in the CBC Lab.
- G. Install Cain and Abel on a virtual machine on your own computer.
- H. Use Cain and Abel on the ForensicsPractice virtual machine. It's already installed in the CS549 account. The password for the CS549 account is **T549csstt**

7.2.5 Cain and Abel Brute Force Attack

4. Download and install Cain and Abel. I suggest you get it from the developer's web site:

<http://www.oxid.it/cain.html>

You may also want to check out the User Manual, which is at the same site. Note - I've had trouble reading the User Manual in Chrome, but it works in Internet Explorer.

5. Create new Windows user accounts. I suggest making at least 3 and using various length passwords for each account. If you need help creating the users and setting passwords you can get instructions from the following sites:

<http://windows.microsoft.com/en-us/windows/create-user-account#create-user-account=windows-7>

<http://pcsupport.about.com/od/windows7/ht/change-another-users-password-windows-7.htm>

- d. Set the password for the first account to something that uses 3 alphanumeric characters like 123 or abc. I know this isn't a good password, and it isn't something you would use in the real world. But it will take Cain and Abel very little time to crack and allow you to gain experience using Cain and Abel. Ensure that you only use lower case alpha characters or numbers. If you use other characters then Cain and Abel will be able to break the password, but you won't be able to use the default character set in the Brute Force attack.
 - e. Set the password for the second account to something that uses 4 or 5 alphanumeric characters like 1234 or house. Cain and Abel will still be able to crack this password, but it will take a little longer.
 - f. Set the password for the third account to something that uses at least 6 alphanumeric characters. This will allow you to see how the number of characters in a password affects the time to crack it.
6. Start Cain and Abel and do the following:
 - a. Click on the Cracker Tab (the icon that looks like a key) to open the password cracker

- b. Add some accounts (usernames and passwords) to crack by clicking the + symbol on the toolbar. If it's grayed out, click in the right pane.
- c. Choose **Import Hashes from local system**. All of the accounts for the local Windows system should now be displayed in the right pane.
- d. Start the password crack for an account by right-clicking the account and selecting the attack method. To begin, choose the account you created that uses the 3 character password. If you are using XP select **Brute Force Attack**, and then **LM Hashes**. If you are using Windows Vista, 7 or later select **Brute Force Attack**, and then **NTLM Hashes**.
- e. Once the password is cracked it will be displayed in the dialog box and then in NT Password column of the main display. The 3 character password should take less than a second to crack. However, if you used characters other than lower alpha or numerals, you'll have to enter those in the Custom Character set field and start the attack again.
- f. Repeat this process for the other accounts and passwords. Note the approximate amount of time it takes to crack each password, or if it the approximate time is longer than you want to wait.
- g. OPTIONAL – you can create longer passwords to see how the length of the password affects the approximate crack time. Not how long the passwords have to be before the length of time moves from days into years.

7.2.6 Cain and Abel Dictionary Attack

In this exercise you will gain experience using a dictionary attack. You will download a file of words to use during the attack, and then run the attack with Cain and Abel.

6. Set up the test accounts and passwords in Windows. You can either use the Windows accounts you created previously, or create new accounts. In either case, assign passwords that follow these patterns:
 - a. Create a password that is at least 8 characters but is a common word such as `password`
 - b. Create a password that is at least 8 characters, and is a common word with additional characters before or after the common word. For example `password44` or `66password`
 - c. Create a password that is at least 8 characters that starts with a common word but replace some of the alpha characters with symbols. For example modify `password` by replacing the `s` characters with `$` so it becomes `pa$$word`
7. Use of the following methods to obtain a dictionary or list of words:
 - d. Download a word list from the Internet. Make sure and get a free one, there are plenty available. The following sites have links to various dictionaries and rainbow tables.

<https://xato.net/passwords/more-top-worst-passwords/>

<http://cyberwarzone.com/massive-collection-password-wordlists-recover-lost-password/>

- e. Most online dictionaries are very large, so it may be simpler to create your own dictionary. You can do this by simply opening a text editor and adding words. However the file must be saved in plain text format. So if you use an editor like Microsoft Word make sure you choose **Save As** and save the file as plain text.
 - f. Copy the file **10k most common.txt** from Canvas. This file contains ~10,000 of the most commonly used passwords. **WARNING** - some of the words in this file are profane so if you profanity bothers you don't use the file, or just don't look at its content.
8. Add words to the dictionary.
- a. Open the dictionary and add at least one of the passwords you created in step 1.
 - b. Save the dictionary file in a place where you can find it, like the Desktop.
9. Start Cain and Abel and do the following:
- h. Click on the Cracker Tab (the icon that looks like a key) to open the password cracker
 - i. Add some accounts (usernames and passwords) to crack by clicking the + symbol on the toolbar. If it's grayed out, left click in the right pane. If you want to clear out the accounts from previous attempts right-click in the right pane and select XXX
 - j. Choose **Import Hashes from local system**. All of the accounts for the local Windows system should now be displayed in the right pane.
 - k. Start the password crack for an account by right-clicking the account and selecting the attack method. If you are cracking an XP account select **Dictionary Attack**, and then **LM Hashes**. If you are using Windows Vista, 7 or later select **Dictionary Attack**, and then **NTLM Hashes**.
 - l. This will open the Dictionary Attack dialog box. Right-click in the **Dictionary** section and select your dictionary file.
 - m. Check the options for creating hybrids of the dictionary words.
 - n. Click **Start** to begin the attack. Note the approximate amount of time required to crack the password.
10. Repeat Step 4 for the other accounts and passwords you created. Note the amount of time required to crack the password. If the attack fails, note how long it takes to run through all of the words in the dictionary and the selected hybrids.

7.2.7 Cain and Abel Creating Rainbow Tables

In this exercise you will gain experience creating a Rainbow Table, so you have some idea how long the process takes. You will download and use **wirtgen**, a program that creates a Rainbow Table for a brute force attack.

4. If necessary download and install **wirtgen**.

<http://www.oxid.it/projects.html>

5. Start **wirtgen**.

- a. Start by selecting the upper case alpha characters as the character set (charset).
- b. Set the minimum length (Min Len) to 4 as there probably aren't many passwords shorter than 4 characters.
- c. Set the maximum length (Max Len) to 7. Normally you would make this longer, but as you'll see this greatly increases the amount of time required to generate the Rainbow Table.
- d. Leave the other settings alone unless you do some extra research to understand what the Chain Length and Chain Count settings do.
- e. Click the Benchmark button to get an estimate of how long it will take to generate the Rainbow Table with these settings. Write down the estimated time in the space below:

- f. Change the character set to add in more characters. For example select the mix-alpha or alpha-numeric. Leave the other settings the same.
- g. Press the Benchmark button to get an estimate of the generation time. Does adding extra characters seem to add much time? Write down the estimated time in the space below:

- h. Return the character set to Alpha.
- i. Change the maximum length to 10 characters.
- j. Press the Benchmark button to get an estimate of the generation time. Does checking longer passwords seem to add much time? Write down the estimated time in the space below:

6. Use your test results to answer the following questions:

- a. Is the amount of time to generate a Rainbow Table best measured in seconds, minutes, hours, days, weeks or months?

- b. Which has a greater impact on the amount of time required to generate a Rainbow Table, the number of characters in the brute force character set or the maximum password length?

7.2.8 Practice Cracking Windows User Passwords

In this exercise you will practice using Cain and Abel to crack the password for different Windows user accounts in the Forensics Practice virtual machine (ForensicsPractice.ova). The passwords for the following accounts are relatively short and made up from lower case alpha characters only so they should crack fairly quickly with a brute force attack.

- d. Username: Carolyn
Password: _____
- e. Username: Mike Jackson
Password: _____
- f. Username: Cave Johnson
Password: _____

The passwords for the following accounts are all 6 characters in length and comprised of lower case alpha characters, so you could use a brute force attack. However the passwords are also common passwords so you could try a dictionary attack. Hint – if you do the dictionary attack use dictionary file **10k most common.txt**.

- g. Username: jed
Password: _____
- h. Username: serita
Password: _____

The passwords for these accounts are 7 characters or longer which means they could take quite a while to crack using a brute force attack. , However the passwords are also common passwords so it would make sense to try a dictionary attack. Hint – if you do the dictionary attack use dictionary file **10k most common.txt**.attack with the common passwords in the file **10k most common.txt**.

- i. Username: sweetcheeks
Password: _____
- j. Username: ferrari
Password: _____

The user for this account is a Star Trek fanatic. This is a hint for you to use a custom dictionary that includes Klingon words.

- k. Username: Bill Shatner
Password: _____

7.10 Cracking Windows Passwords from an Image

In this set of exercises you will gain experience cracking Windows passwords from a forensics disk image. Most of the process is the same as cracking passwords for a live system; the main difference is that you have to extract the SAM and SYSTEM registry files from the image. Remember that a disk image is like a .zip file, it has many files inside of a single file. So before Cain and Abel can find the passwords, the SAM file (and maybe the SYSTEM file) must be pulled out of the disk image.

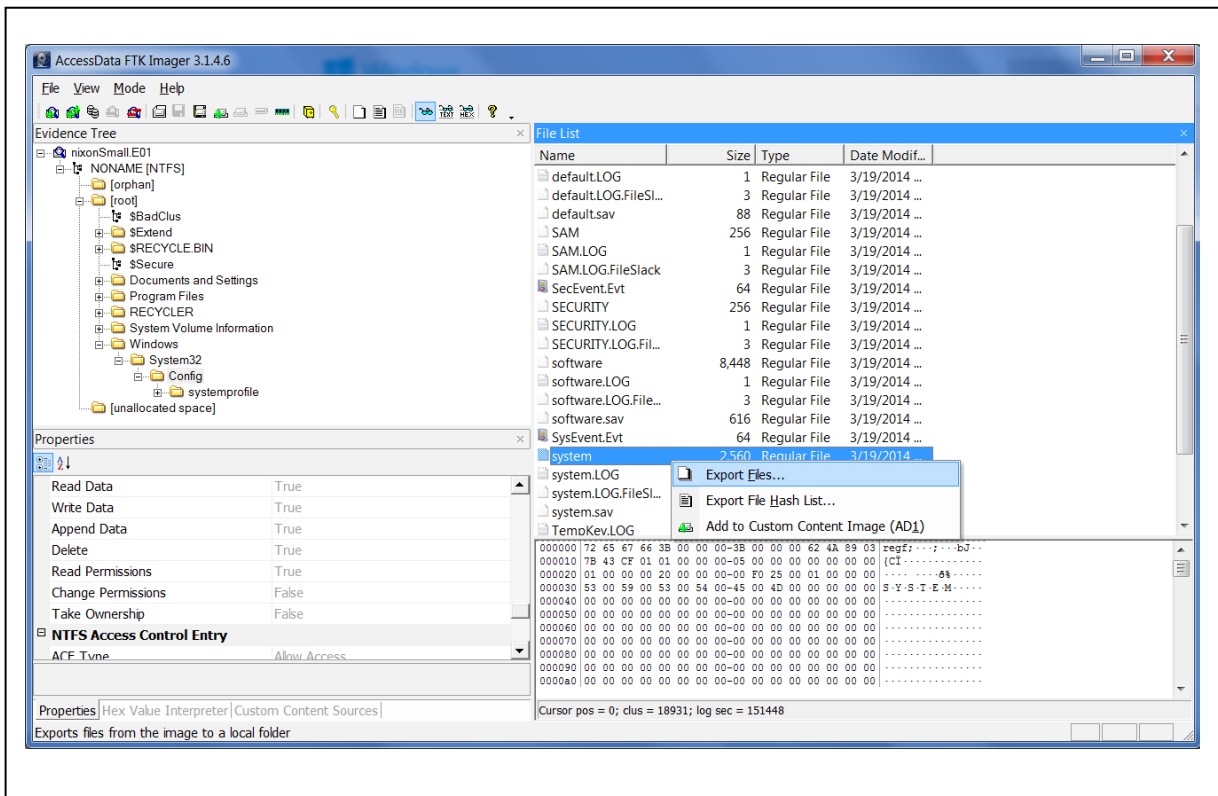
All of the disk images used in this set of exercises are in the zip file **password cracking practice.zip**.

7.3.3 Step-By-Step Using Cain & Abel to Crack Passwords from SAM and SYSTEM

This exercise provides step by step instructions for opening a forensics disk image and exporting the registry files required for Cain and Abel to crack passwords.

You can either do this exercise on your own virtual machine, or on the ForensicsPractice virtual machine. If you want to run it on your own VM you must download the image file **Toshiba-password-practice.E01** from Canvas. To do this exercise on the ForensicsPractice vm ensure that it's started, then login to the virtual machine as user **CS549**. The password is **T549cstt**

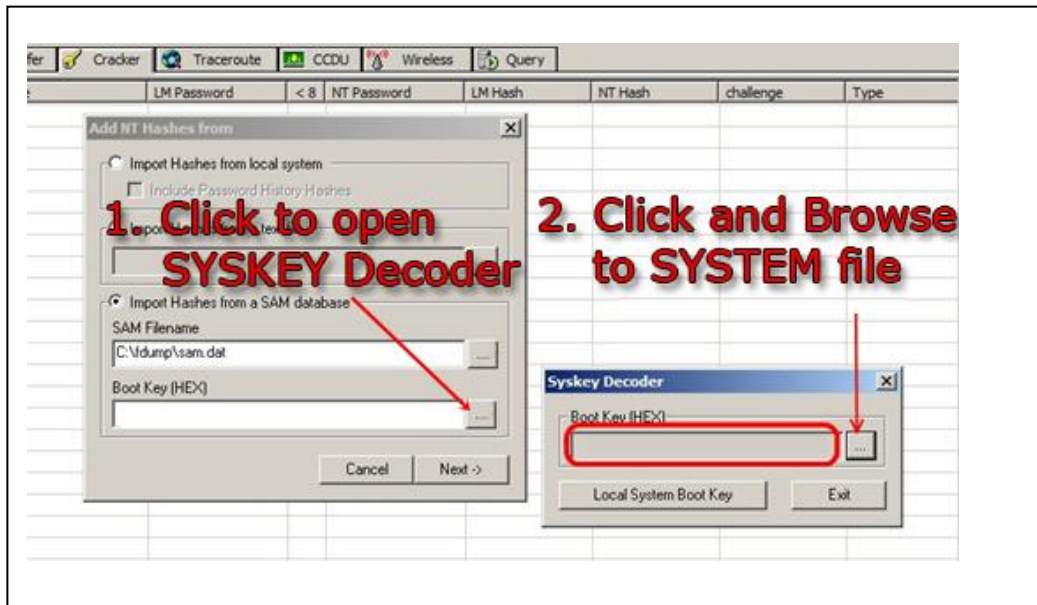
4. Extract the SAM and SYSTEM registry files. For this step you can use either FTK or FTK Imager. Go back to the FTK videos if you need to review using these tools.
 - a. Start FTK Imager. This is on the desktop for the CS549 user in ForensicsPractice.
 - b. Select **File > Add Evidence Item** and open the disk image **Toshiba-password-practice.E01**. This image is in the folder **practice images** on the Desktop for the CS549 user in ForensicsPractice.
 - c. Expand the Evidence Tree to see the main drive, then down into the **Windows\System32\Config** folder.
 - d. Right click the SAM file and select **Export Files**. It is suggested that you save the file to a folder on the Desktop named ToshibaPasswords. You can save the SAM (and SYSTEM) files to a different folder if you wish. Just make sure that you remember where you put them.
 - e. Right click the SYSTEM file and select **Export Files**. It is suggested that you save the file to the same folder as the SAM file.



5. Load the Windows accounts and passwords into Cain by doing the following:
 - a. Start Cain and Abel. This is on the desktop for the CS549 user in ForensicsPractice.
 - b. Select the **Cracker** tab. Have Cain find the Windows accounts and passwords by either clicking the **+** or right-clicking and selecting **Add to list**.
 - c. Select **Import hashes from a SAM database**. Browse to the SAM file you extracted in the previous step and select it.

6. Load the Windows SYSKEY into Cain. Remember that Windows has an option for using a salt called the SYSKEY when it hashes the passwords. If present, the SYSKEY is stored in the **SYSTEM** registry file. NOTE – it's a common mistake to think the SYSKEY is loaded in the SECURITY file.
 - a. Click the Browse button by the **Boot Key (HEX)** box. This will open the **Syskey Decoder** dialog box.

- b. Click the browse button, then browse to the SYSTEM file you exported from the disk image and select it.
- c. The decoded Boot Key will appear in the dialog box. However, this Boot Key will NOT be automatically transferred back to the **Add NT Hashes** dialog box. You must highlight the Boot Key and hit **<ctrl-c>** to copy it. Next, click the Exit button to close the **Syskey Decoder** dialog box. Click inside the **Boot Key (HEX)** text box back on the **Add NT Hashes** dialog box and then hit **<ctrl-v>** to paste the Boot Key.



- d. Click the Next button. The list of users and hashed passwords in the Registry files will now be displayed in Cain. You can begin cracking the passwords.

7.3.4 Practice Cracking Windows User Passwords From Disk Image

All of the disk images used in this set of exercises are in the zip file **password cracking practice.zip**.

6. Crack the passwords for the following accounts from **Mantooth.E01**. If no password is set, write **empty**. Hint – this image is from a computer running XP. Notice that the LM hashes are all set to the same value and the NTLM hashes for the accounts with passwords are set to different values. These are all clues that the NTLM hash is being used, NOT the LM hash.

- a. Username: Wes Mantooth
Password: _____
- b. Username: Dracula
Password: _____
- c. Username: Laurent
Password: _____
- d. Username: Administrator
Password: _____
- e. Username: Guest
Password: _____

7. Crack the passwords for the following accounts from **Washer 17.E01**. If no password is set, write **empty**. Hint – this image is from a computer that used **LM** hashes.

- a. Username: Administrator
Password: _____
- b. Username: Help Assistant
Password: ??? _____
- c. Username: SUPPORT_388945a0
Password: ??? _____
- d. Username: Guest
Password: _____
- e. Username: Billy Bob Brubeck
Password: _____
- f. Username: The Wolf
Password: _____
- g. Username: Mr Smee
Password: _____
- h. Username: Captian Hook
Password: _____

8. Crack the passwords for the following accounts from **toshiba-password-practice.ad1**. If no password is set, write **empty**.

Hint 1 – this image is from a computer running Windows 7. Notice that the NTLM hashes for the accounts with passwords are set to different values, while the LM hashes are all the same. This is a clue that the NTLM hash is being used, NOT the LM hash.

Hint 2 – All of the passwords in this exercise use lower case characters or numerals. The shortest is 5 characters and the longest is 7 characters.

- a. Username: Dash
Password: _____
- b. Username: Miles
Password: _____
- c. Username: race
Password: _____
- d. Username: Ricky Ricardo
Password: _____
- e. Username: Colonel Sanders
Password: _____

9. Crack the passwords for the following accounts from **starwars-password-practice.ad1**. If no password is set, write **empty**.

Hint 1 – this image is from a computer running Windows 7. Notice that the NTLM hashes for the accounts with passwords are set to different values, while the LM hashes are all the same. This is a clue that the NTLM hash is being used, NOT the LM hash.

Hint 2 – All of the passwords in this exercise are related to Star Wars or Clone Wars. You could try a brute force attack, but the passwords are up to 10 characters in length, unless otherwise noted. Since the passwords are so long, you should probably use the starwars.txt dictionary.

- a. Username: han solo (Hint – this password is 6 characters, all lower case alpha).
Password: _____
- b. Username: Mace
Password: _____
- c. Username: Darth Maul
Password: _____
- d. Username: Jabba
Password: _____
- e. Username: Ventress
Password: _____


10. Crack the passwords for the following accounts from **gateway-password-practice.ad1**. If no password is set, write **empty**.

Hint – this image is from a computer running Windows 7. Notice that the NTLM hashes for the accounts with passwords are set to different values, while the LM hashes are all the same. This is a clue that the NTLM hash is being used, NOT the LM hash.

- a. Username: bob (Hint – all lower case letters)
Password: _____
- b. Username: eric (Hint – all lower case letters)
Password: _____
- c. Username: jim (Hint – 7 characters all lower case.)
Password: _____
- d. Username: sara (Hint – 7 characters. All lower case letters and numerals)
Password: _____
- e. Username: Bruce Wayne (Hint – 7 characters. Lower and upper case letters)
Password: _____

PASSWORD CRACKING WITH OPHCRACK

This exercise will provide you with experience using OPHCrack to try and decrypt passwords. It will also provide you with some background in basic decryption, rainbow tables, and password complexity.

1. Download OPHCrack – we'll use the Windows XP version for the hands-on labs, but you can download the other versions if you wish. This part must be done on a computer with a network connection. (You may want to do Step 3 below while you are waiting for the download or disk burning to complete.)
 - A. Go to the OPHCrack Web site at <http://ophcrack.sourceforge.net>
 - B. Go to the download page and select The XP Live CD ISO
ophcrack XP LiveCD 
`ophcrack-xp-livecd-3.6.0.iso`
 - C. Burn this image to a CD
2. Run OPHCrack. This part must be done on a computer in the hardware lab. Do NOT do this on any other CBC computer. You can also try this on your home system if you want more practice.
 - A. Insert the OPHCrack CD in the CD/DVD drive
 - B. Restart the computer and enter the System/BIOS Setup. Ensure that the optical drive is the first in the boot device list.

- C. Save the settings and Exit the System/BIOS Setup.
 - D. The computer should boot into the OPHCrack
 - E. Document any passwords discovered by OPHCrack
3. Test OPHCrack. This part must be done on a computer in the hardware lab. Do NOT do this on any other CBC computer. You can also try this on your home system if you want more practice.
- A. Login as Administrator using the password you discovered
 - B. Create two new user accounts.
 - i. Give one of the new accounts a relatively simple password 4 character password that only uses alphanumeric characters.
 - ii. Give the other account a more complex password using 10 characters and include at least 2 non-alphanumeric characters
 - iii. Document your account names and passwords
 - C. Switch computers with another student.
 - D. Run OPHCrack to try and crack the passwords for the two new accounts
4. Rainbow Tables. Return to the OPHCrack web site, and go to the Tables section.
- A. Read the details associated with each of the different Rainbow Tables
 - B. Compare the complexity of the passwords in the various Rainbow Tables with the size of the associated file. Is there a correlation?
 - C. What is the size of the largest Rainbow Table available at the OPHCrack site?
5. How does OPHCrack function? Hopefully it's obvious the OPHCrack is somehow checking Windows passwords, but exactly where does it get the passwords from?
- A. Read the information at the web site
http://en.wikibooks.org/wiki/Reverse_Engineering/Cracking_Windows_XP_Passwords
- Use this information to describe where Windows XP stores it's password hashes and why OPHCrack requires you to boot from the CD (or thumbdrive) to run.
- B. Do your own research to discover if Windows 7 and Windows 8 store the password hashes in the same location as Windows XP.
 - C. Do your own research to discover why there's a version of OPHCrack for XP and a different version for Windows Vista/7.
6. How secure is a password - (Or how long will it take you to crack a password). In this exercise you'll use an online tool to determine the strength of a password, or at least how long it would take to crack a password using brute force methods. This is really only marginally related to forensics, if someone encrypts a file or drive they usually don't tell you how complex they made the password; but since we're on the topic of passwords I thought it may provide you some objective data when choosing your own passwords.
- A. Read the information at the web site
<http://www.pcworld.com/article/2038067/passwords-youre-doing-it-wrong-heres-how-to-make-them-uncrackable-.html>
 - B. Try your passwords, or similar words at
<https://www-ssl.intel.com/content/www/us/en/forms/passwordwin.html>

7.11 BITLOCKER EXERCISES

In this set of exercises you will gain hands on experience using BitLocker, using Passware to crack BitLocker passwords, and using Elcomsoft to discover BitLocker recovery keys.

7.3.4 Using BitLocker

This exercise provides you with experience in setting, using and managing BitLocker. If you have previous experience with BitLocker you can skip this exercise. If you are going to do this exercise please make sure and read the following cautionary notes carefully:

- **Check your OS Version** – BitLocker is available in all editions of Windows except the Home edition. If you have the Home edition you will not be able to complete this exercise.
 - **Do NOT add BitLocker to any drives you do not own.** In particular, do not enable BitLocker on any of the college computers. If you do you will face penalties that include flunking the class, expulsion, or possible criminal charges.
 - **Choosing a drive to encrypt** - This exercise requires setting BitLocker on one your own drives. I strongly suggest you set BitLocker on the smallest thumb drive you own and that you do NOT set BitLocker on your main system drive. Once you gain some experience with BitLocker and understand the costs and benefits you can make the decision whether or not to encrypt your main drive, but for now use a small thumb drive if you have one available.
 - **Backup files before enabling BitLocker** – The process of enabling and disabling BitLocker is stable and safe, but you should backup any critical files before enabling BitLocker just to be safe.
 - **Do NOT remove the drive during encryption** - When you enable BitLocker Windows will encrypt the data on your disk. If you have a small drive this won't take long, but it can take a significant amount of time on larger drives. Once the encryption starts you must let it complete before removing the drive. Make sure and heed the warnings that Windows displays and do NOT remove the drive while the files are being encrypted. If you do the drive will be unusable.
 - **Document passwords and Recovery Keys** – Make sure and write down your BitLocker password and save your Recovery Key somewhere besides on the drive you encrypt.
7. Insert the thumb drive into your computer. Go to My Computer. Right-click on the thumb drive and select **Turn On BitLocker**
 8. Windows will check the drive to ensure that it will be able to run BitLocker. Do not remove the drive during this process. When Windows is ready, it will display the Bitlocker Drive Encryption dialog box. Check the **Use a Password to Unlock the Drive box**, and enter the password you want to use. The password must be at least 8 characters. If you plan on actually using Bitlocker after this exercise you should create a strong password. If you're just adding Bitlocker for this exercise remember that in demo mode Passware will only run for 60 seconds before stopping so your password needs to be one that will be found quickly with a brute force attack such as 00000001, or a common password like Aberdeen that will be found with a dictionary attack using Passware's default dictionary.

Record the password in the space below:

9. Click the **OK** button. Windows will now force you to either print the Recovery Key or save it to a file. I suggest you save it to a file.
10. Click the **OK** button to begin encrypting the drive. This can take a long time, depending on the size of the drive and the amount of data on the drive. Do NOT remove the drive or shut down the computer without first pausing the process.
11. When the encryption has finished test it by performing these steps:
 - a. Safely eject the thumb drive.
 - b. Reinsert the thumb drive. The dialog box that prompts for the BitLocker password should be displayed.
 - c. After the correct password is entered you should be able to use the drive and the files on the drive as you normally would. Verify this by performing basic actions such as copying files to the drive, copying files from the drive, creating folders on the drive etc.



12. When you're finished with the other exercises in this section you can remove the BitLocker encryption if you wish. Don't do this now, wait at least until you've finished creating the forensics disk image of the thumb drive in the next step. When you're ready to turn off Bitlocker follow these steps:
 - a. Go to the Windows Start Button and type "bitlocker" in the Search box.
 - b. Choose **Bitlocker Drive Encryption**
 - c. Find the thumb drive in the display and click on **Turn Off Bitlocker**. Removing the encryption can take a long time, depending on the size of the drive and the amount of data on the drive. Do NOT remove the drive or shut down the computer without first pausing the process.

7.3.5 Use Passware to Crack the Bitlocker Password On Your Drive

In this exercise you will crack Bitlocker password on the drive you encrypted in the previous exercise. This entails creating an image of the Bitlocker enabled drive and then using Passware to crack the password.

3. Create the disk image file of the Bitlocker enabled drive. This is just like the drive imaging you have performed previously, there are no special steps for Bitlocker enabled drives.
 - j. Ensure the Bitlocker enabled thumb drive is mounted in your computer.
 - k. Start FTK Imager. (Note – this is FTK *Imager*, not FTK.)
 - l. Choose **File > Create Disk Image**
 - m. Select **Physical Drive** for the Evidence Type and click **Next**
 - n. Select the thumb drive from the pull down list. You should be able to recognize it by the size. Click the **Finish** button.
 - o. The Create Image dialog box will be displayed. Click the **Add** button, then select Raw (dd) for the image type. Click the **Next** button.
 - p. You fill in Evidence Information if you wish, or leave it blank and click the **Next** button.
 - q. Choose the Image Destination Folder. I suggest you choose the Desktop or someplace where the disk image file will be easy to find. Set the Image Filename and click the **Finish** button.
 - r. This returns you to the Create Image dialog box. Verify that the output image file is displayed in the list, then click the **Start** button. The image file will be created. This may take several minutes.

4. Use Passware to crack the Bitlocker password for the thumb drive.
 - f. Download and install Passware if necessary. If you are using the ForensicsPractice virtual machine there is a copy on the desktop of the CS549 user. If you need to download it, Passware is available from Canvas or from:

<http://www.lostpassword.com/>
 - g. Start Passware. In the right panel choose the **Full Disk Encryption** link.
 - h. Choose the **Bitlocker** link.
 - i. Click the **Browse** button by the **Encrypted Bitlocker Image File** box, and select the disk image you created above. Note – FTK Imager may have added a `.001` to the end of the image file name. For example, if you said to name the image file `thumb1.dd` FTK will call it

thumb1.dd.001. By default Passware only displays files with image file extensions such as .dd or .E01, so you'll have to tell Passware to display files of all types. Select the file and click **Open**.

- j. Click the **Next** button. At this point you can set the parameters for the password cracking. You can either run the Wizard, choose predefined settings, or choose Advanced and set up a custom attack. You can test the various settings, but I suggest you set the minimum password length to 8, since this is Bitlocker's minimum.

If you used a "bad" password such as 00000001 or Aberdeen Passware should crack it pretty quickly. If you chose a stronger or longer password Passware could probably crack it, but Passware is in demo mode which means it will stop after 60 seconds and you may not get a result.

If it cracks the password Passware will display the first 3 characters. It's cracked the entire password, but since we're running Passware in demo mode they don't show it all to you.

7.3.6 Practice Cracking Bitlocker Passwords with Passware

Use the **Passware Forensics Kit Recovery Demo** to crack the bitlocker passwords on the 5 thumbdrive images. Remember you will only be able to reveal the first 3 characters. The thumb drive images are all in the zip file **bitlocker Practice.zip** which is available from Canvas. Note - always set the attacks for passwords that are 8 characters in length.

- I. First 3 characters of image of **thumbdrive1.dd** – set to dictionary attack using the dictionary **bitlockerDictionary.txt**, 8 characters _____
- J. First 3 characters of image of **thumbdrive2.dd** – set to dictionary attack using the dictionary **bitlockerDictionary.txt**, 8 characters _____
- K. First 3 characters of image of **thumbdrive3.dd** – set to dictionary attack using the dictionary **bitlockerDictionary.txt**, 8 characters _____
- L. First 3 characters of image of **thumbdrive4.dd** – set to dictionary attack using the dictionary **bitlockerDictionary.txt**, 8 characters _____
- M. First 3 characters of image of **thumbdrive5.dd** – set to dictionary attack using the dictionary **bitlockerDictionary.txt**, 8 characters _____
- N. First 3 characters of image of **thumbdrive6.dd** – set to dictionary attack using the default Passware dictionary, 8 characters _____
- O. First 3 characters of image of **thumbdrive7.dd** – set to dictionary attack using the default Passware dictionary, 8 characters _____
- P. First 3 characters of image of **thumbdrive8.dd** – set to brute force attack numbers only, 8 characters _____

7.12 BITLOCKER RECOVERY KEY WITH ELCOMSOFT

Note – this exercise is OPTIONAL.

In this exercise you will use Elcomsoft Forensic Disk Decryptor to retrieve the BitLocker recovery key for an encrypted drive. Detailed instructions for using notMyFault and the Elcomsoft tool are available on the video for discovering the BitLocker recovery key

6. If necessary download and install the demo version of Elcomsoft Forensic Disk Decryptor. You can download it from the Elcomsoft web site at <https://www.elcomsoft.com/efdd.html> or from Canvas.
7. If necessary encrypt a thumb drive using BitLocker. (You will need to know the Recovery Key if you want to verify that the recovery found by the Elcomsoft tool is correct or not.) Connect the thumb drive to the computer. You do not have to supply the BitLocker password.
8. Download notMyFault from <https://technet.microsoft.com/en-us/sysinternals/notmyfault.aspx> or Canvas.
9. Generate a memory dump using notMyFault. Make sure that you are capturing all of memory including the protected areas. Remember that this will cause your computer to reboot, so ensure that all of your work is saved before starting the memory dump.
10. Start Elcomsoft Forensic Disk Decryptor, load the memory dump file and check for the recovery key. This tool will display the first few characters of the recovery key after it is found.

7.13 BITLOCKER REVIEW QUESTIONS

8. True or False. BitLocker can only be applied to entire drives. That is, it is not possible to encrypt a single file or folder using BitLocker.
 - a. True
 - b. False
9. Which of the following is true regarding BitLocker passwords?
 - a. The password is encrypted and stored in one of three locations: on the drive, on a smart card, or in a TPM.
 - b. The password is hashed and stored in one of three locations: on the drive, on a smart card, or in a TPM.
 - c. The password is broken into sections and stored in different locations on the drive. When the drive is mounted Windows reconstructs the sections and stores the reconstructed password in memory.
 - d. The password is hashed using the SYSKEY and stored in the SAM file.
 - e. None of the above are true

10. Which of the following is true regarding BitLocker recovery keys?
- The recovery is encrypted and stored in one of three locations: on the drive, on a smart card, or in a TPM.
 - The recovery key is hashed and stored in one of three locations: on the drive, on a smart card, or in a TPM.
 - The recovery key is broken into sections and stored in different locations on the drive. When the drive is mounted Windows reconstructs the sections and stores the reconstructed password in memory.
 - The recovery key is hashed using the SYSKEY and stored in the SAM file.
 - None of the above are true
11. Which of the following is true regarding the Passware tool for gaining access to BitLocker encrypted drives?
- The Passware tool attempts to crack the BitLocker password. If the user created a strong password the Passware tool may not crack the password in a reasonable amount of time.
 - The Passware tool recovers the BitLocker password from a memory dump. Creating the memory dump may take several minutes, but once this step is completed recovering the password occurs quickly. The strength of the password has no effect on recovery time.
 - The Passware tool will only crack the BitLocker password if the user did not specify using the SYSKEY salt.
 - The Passware tool attempts to crack the BitLocker recovery key. If the user created a strong recovery key the Passware tool may not crack it in a reasonable amount of time.
 - The Passware tool recovers the BitLocker recovery key from a memory dump. Creating the memory dump may take several minutes, but once this step is completed finding the recovery key occurs quickly. The length of the recovery key has no effect on recovery time.
 - The Passware tool will only crack the BitLocker recovery key if the user did not specify using the SYSKEY salt.
 - None of the above are true.
12. Which of the following is true regarding the Elcomsoft tool for gaining access to BitLocker encrypted drives?
- The Elcomsoft tool attempts to crack the BitLocker password. If the user created a strong password the Elcomsoft tool may not crack the password in a reasonable amount of time.
 - The Elcomsoft tool recovers the BitLocker password from a memory dump. Creating the memory dump may take several minutes, but once this step is completed recovering the password occurs quickly. The strength of the password has no effect on recovery time.
 - The Elcomsoft tool will only crack the BitLocker password if the user did not specify using the SYSKEY salt.
 - The Elcomsoft tool attempts to crack the BitLocker recovery key. If the user created a strong recovery key the Elcomsoft tool may not crack it in a reasonable amount of time.
 - The Elcomsoft tool recovers the BitLocker recovery key from a memory dump. Creating the memory dump may take several minutes, but once this step is completed finding the recovery key occurs quickly. The length of the recovery key has no effect on recovery time.
 - The Elcomsoft tool will only crack the BitLocker recovery key if the user did not specify using the SYSKEY salt.
 - None of the above are true.

13. Assume you are asked to recommend purchasing either the Passware tool or the Elcomsoft tool for decrypting drives that have been encrypted with BitLocker. Which would you recommend and why.

14. Assume you are asked to check a hard drive that has been encrypted with BitLocker for evidence of a crime. In particular you are asked to recover the user names and passwords for the Windows accounts. Which of the following describes the steps in the process you should follow to retrieve the Windows user names and crack the passwords?
 - a. There is no way to accomplish this task. The Windows usernames and passwords cannot be retrieved from a drive encrypted with BitLocker.
 - b. Run a Windows password crack tool such Cain and Abel or OphCrack. These tools will be able to read the SAM and SYSTEM files on the encrypted drive and use this information to crack the user names and passwords.
 - c. Create a forensics image of the hard drive. Next extract the SAM and SYSTEM files. Run Cain and Abel and use it to display the Windows user names and crack their passwords.
 - d. Use either the tool from Passware to crack the BitLocker password or the tool from ElcomSoft to retrieve the BitLocker Recovery key. Next decrypt the drive and recover the SAM and SYSTEM files. Finish by using a Windows password cracking tool such as Cain and Abel or OPHCrack to retrieve the Windows user names and crack the account passwords.

7.14 EFS EXERCISES

In this exercise you will set up EFS encryption to protect a folder. You will then open the folder in FTK to see how it handles it. To finish, you will try and recover the EFS password. NOTE – EFS isn't available for all versions for Windows. For Windows 7 it's only available for Windows 7 Professional and Ultimate.

Note – These exercises require logging in as different users, so you'll need to either do them on your personal computer, or in a virtual machine. That is, you'll need access to at least two different Windows user accounts. If you are using one of the computers in the CBC Computer Science Labs you will have to use a virtual machine.

7.5.5 Step-By-Step Setup the EFS Encryption

6. Open Windows Explorer, and select the folder you want to encrypt. You can either use an existing folder, or create a new one. Right-click the folder then click **Properties**. The Properties dialog box will be displayed.
7. Ensure you're on the **General** tab, click the **Advanced** button. The Advanced Attributes dialog box will be displayed.
8. Check the **Encrypt Contents to Secure Data** box and click **OK**.
9. The Confirm Attribute Changes dialog box will be displayed. You will be asked if you want to encrypt the current folder, or the current folder and all it's sub-folders. For this test, you can choose either option. Click **OK**.

10. That's all there is to the setup. It's so simple that sometimes it's hard to realize that anything has been done. The main clue that you have that the folder is encrypted is that folder will look like any other folder except it will have green text to remind you it's encrypted. Windows will automatically encrypt any files you add to the folder. It will also automatically decrypt them for you, but it uses your login credentials so you'll be the only user that can see the decrypted information.

If you get the message: "Recovery policy configured for this system contains invalid recovery certificate" you may have to renew the certificate. The following web site has the instructions for doing this:

<https://social.technet.microsoft.com/Forums/windowsserver/en-US/f514129b-bab7-4cad-a179-f53f9abdc826/efs-recovery-policy-contains-invalid-recovery-certificate>

7.5.6 Test the EFS Encryption

In this step you will test the EFS encryption/protection by turning on EFS for a folder as one user, then trying to access it as a different user. You can do this on any computer where you have permission to create new users. If you are in the CBC Computer Science Lab you should do this on the virtual machine.

5. Start Windows Explorer and move to the top folder in the C: drive. Create a new folder and add some files including at least 1 plain text file. You can also create Word documents, image files etc.; but ensure that you have at least 1 plain text file as the decryption tool will only decrypt the first 512 bytes of each file when it runs in demo mode. This means that decrypted files like image files or Word file won't display because they need the entire file decrypted to display it. Ensure that you can read or display the files in this folder.
6. Enable EFS for this folder. Ensure that the folder is green
7. Log out of Windows. Log back in as a different user.
8. Return to the top folder in the C: drive and try and access the files in the EFS encrypted folder. Can you view the file names? Can you open and display any of the files?

7.5.7 Step-By-Step Recover the EFS Encrypted Files

If you have paid for FTK and PRTK you can export the folder from FTK, then use PRTK to recover the encrypted files. If you don't have PRTK you can use a demo version of the Elcomsoft Advanced EFS Data Recovery Tool

3. Download and install <http://www.elcomsoft.com/aefsdrr.html> - Elcomsoft Advanced EFS Data Recovery Tool (Scroll to the bottom of the page for the trial download link). If you are using the Virtual Machine **ForensicsPractice** this program is already loaded and available if you are logged in as the CS549 user. Go to the **Windows Start Button**, the select **All Programs > Elcomsoft Password Recovery > Advanced EFS Data Recovery**.

4. Run the Recovery Tool. You can either run the Wizard or do the following 3 steps yourself. Remember that these steps can be run in any order, but you will need to do all of them.
 - f. Find the EFS encryption Keys. Click the **EFS Related Files** tab, then click the **Scan for Keys** button. This may take some time.
 - g. Find the EFS encrypted files. Click the **Encrypted Files** tab, then click the **Scan for Encrypted Files** button. This may take some time.
 - h. Add the other ½ of the PKI key, which is the Windows Username and Password for the owner of the EFS folder. This of course means that you need to know this information. In a real forensics investigation this may require you to crack the Windows password. Return to the EFS Related Files tab. Click the **Add User Password** button. Enter the Windows username and password, then click the **Add** button. The program will then decrypt any keys associated with this user.
 - i. Return to the **Encrypted Files** tab. Any EFS encrypted files owned by the Windows user should now be green, which means they can be decrypted. Check the box for each file, then click the **Decrypt** button on the main toolbar. Choose a folder to store the decrypted files in. I suggest you put it somewhere on the desktop.
 - j. When the program has finished, inspect the folder to ensure the files have been decrypted. However, remember that in demo mode the program only decrypts the first 512 bytes, so the only files you'll be able to view or read will be things like plain text files.

7.5.8 EFS Practice 1

The following exercises provide practice breaking EFS encryption. Use the Virtual Machine ForensicsPractice for these exercises.

5. Login to Virtual Machine as user **CS549**. The password for this account is **T549cstt**.
6. Click the **Windows Start Button** and select either **Computer** or **Documents**. Navigate to the home directory for the **jed** user which is **C:\Users\jed\My Documents**. Which folder is encrypted with EFS?
7. Open EFS encrypted folder. Try and view files. Are you successful or do you see an error message?
8. Run **Elcomsoft aefsd** tool and decrypt the files in this folder. If you are using the Virtual Machine **ForensicsPractice** this program is already loaded and available if you are logged in as the CS549 user. Go to the **Windows Start Button**, then select **All Programs > Elcomsoft Password Recovery > Advanced EFS Data Recovery**.

You will need the username and password for the Jed account. Obviously the username is **Jed**, but you will need to use the password that you cracked previously. Remember you will only be able to see the first 512 bytes of decrypted files. Inspect the files and try to determine what the main subject of all the files in the folder is:

- H. Tea
- I. Tornadoes
- J. Tesla
- K. Turkey
- L. Telephones
- M. Tacos
- N. None of the Above

7.5.9 EFS Practice 2

The following exercises provide practice breaking EFS encryption. Use the Virtual Machine ForensicsPractice for these exercises.

1. Login to Virtual Machine as user **CS549**. The password for this account is **T549cstt**.
2. Click the **Windows Start Button** and select either **Computer** or **Documents**. Navigate to the Desktop directory for the **felix** user which is **C:\Users\felix\Desktop**. Which folders are encrypted with EFS?
3. Open EFS encrypted folder. Try and view files. Are you successful or do you see an error message?
4. Run **Elcomsoft aefsd** tool and decrypt the files in the **movies** folder. If you are using the Virtual Machine **ForensicsPractice** this program is already loaded and available if you are logged in as the CS549 user. Go to the **Windows Start Button**, the select **All Programs > Elcomsoft Password Recovery > Advanced EFS Data Recovery**.

Remember you will only be able to see the first 512 bytes of decrypted files. Inspect the file **movies\american pie lyrics.txt** and try to determine what the main subject of text in file is:

- A. Star Trek
 - B. Star Wars
 - C. Sharknado
 - D. Snakes on a Plane
 - E. All of the Above
 - F. None of the Above
5. Run **Elcomsoft aefsd** tool and decrypt the files in the **xxx** folder. If you are using the Virtual Machine **ForensicsPractice** this program is already loaded and available if you are logged in as the CS549 user. Go to the **Windows Start Button**, the select **All Programs > Elcomsoft Password Recovery > Advanced EFS Data Recovery**.

Remember you will only be able to see the first 512 bytes of decrypted files. Inspect the files **movie quotes.txt** and **song lyrics.txt**. What is the main subject of the text in these files?

- A. Star Trek
- B. Star Wars – It's Mario on the "Forensics" vm
- C. Sharknado
- D. Snakes on a Plane
- E. All of the Above
- F. None of the Above

7.15 EFS REVIEW QUESTIONS

7. What is EFS?
 - a. A feature of Microsoft Windows that allows users to encrypt files and folders.
 - b. A feature of Microsoft Windows that allows users to encrypt email messages.
 - c. A third party product that allows users to encrypt files and folders.
 - d. A third party product that allows users to encrypt email messages.
8. Assume you encrypt a file or folder using EFS. Where is the encrypted FEK used to decrypt the files stored?
 - a. In the SAM portion of registry.
 - b. In the local secrets portion of registry.
 - c. In the users NTUser.dat.
 - d. In an Alternate Data Stream called \$EFS for the encrypted file.
 - e. In the file header.
9. Who can read files protected by EFS (without hacking the encryption)?
 - a. The owner.
 - b. The owner and any user with Administrator privileges.
 - c. The owner, any user with Administrator privileges, and any user with the EFS password.
 - d. The owner and any user with the EFS password.
10. True or False. Once EFS encryption is enabled it cannot be disabled or turned off.
 - a. True
 - b. False
11. Which of the following that once enabled cannot be disabled or turned off?
 - a. Windows password salting with SYSKEY
 - b. BitLocker
 - c. EFS
 - d. Application level encryption (such as Word or PDF encryption)
12. Assume a user has enabled EFS on a folder. What steps are required to read or write files from the folder?
 - a. The user must supply the password each and every time they read files in the folder or try to write new files into the folder.

- b. The user only needs to supply the password once when they login. After that they will be able to read files in the folder or write new files in the folder without supplying any other information.
- c. The user only needs to supply the password once per login, when they first try to access the folder. After that they will be able to read files in the folder or write new files in the folder without supplying any other information.
- d. The user only needs to login to Windows. Windows will then automatically allow users to access any EFS encrypted files or folders.
- e. None of the above are true.

7.16 APPLICATION ENCRYPTION EXERCISES

In this set of exercises you will use the encryption built into applications like Microsoft Word or .ZIP files to protect the content of the file. You will then use different tools to crack the password used to protect the encrypted file.

7.5.4 Practice Cracking Microsoft Office Passwords

In this exercise you will create your own password protected Word files, and then use a tool to crack the password. Note – you must do this exercises on a computer that has Microsoft Word installed. Word is NOT installed on the ForensicsPractice Virtual Machine, but it is installed on all of the computers in the CBC Computer Science Labs.

6. Create a test document (or two)

- G. Create a New Document in Microsoft Word. Enter some text.
- H. Save the file, encrypt it and add a password. IMPORTANT – The encryption used in older versions of Office was much easier to break, so you must save this document as an older version. If you save it as a newer version the password recovery tool won't be work. Choose **File / Save As**, then go to the **Save As Type** box and save the document as Word 97 – 2003 Document (*.doc) Also note where you save the file, as you'll need to use it later.
- I. Add a password to the file by selecting **File / Protect Document**. In newer versions of Office you will select **File > Info** and then click the **Protect Document** button. . Choose **Encrypt with Password**.
- J. You will be prompted to enter a password, and then to repeat the password. For the first test you should keep the passwords short, **3 characters or less**, and only use **lower case alpha characters**. For later tests you can make more complex passwords if you wish.
- K. Close the file
- L. Test the password protection by trying to reopen the file. You should be prompted to enter the password, and denied access if you fail to provide the correct password.

7. Crack the password

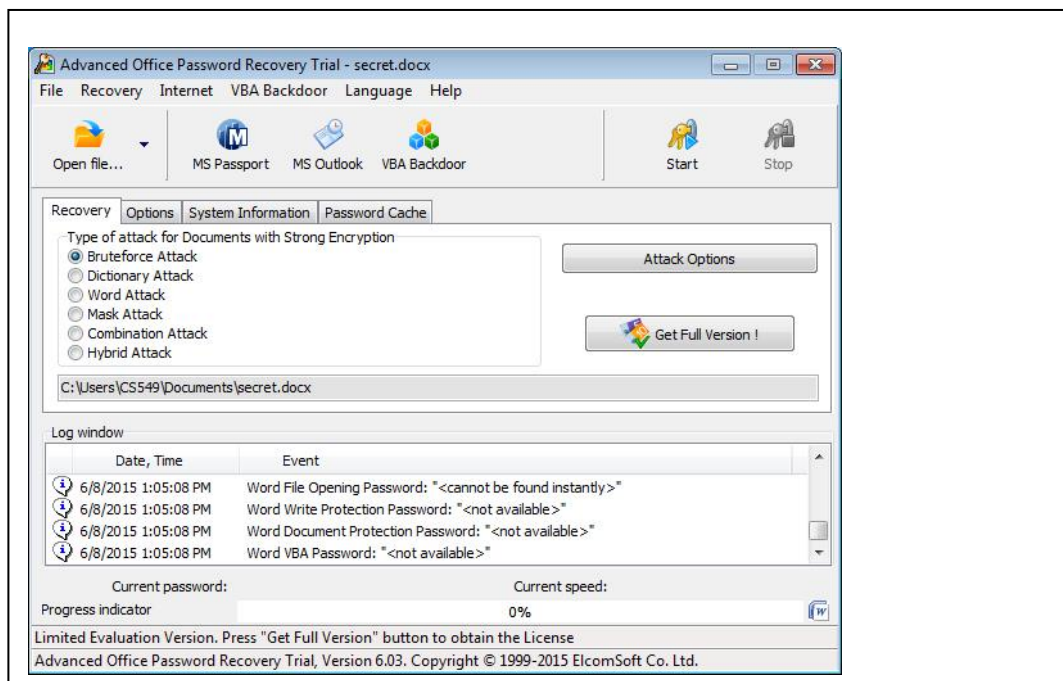
- E. If necessary download and install the demo version of the Elcomsoft **Advanced Office Password Recovery** (AOPR) tool. Check at the bottom of the following page for the link to the download for the demo version:

<https://www.elcomsoft.com/aopr.html>

- F. Start the AOPR tool

- G. Open the protected Word Document. AOPR will do a "Preliminary" attack using the default attack profile, which means it's going to do a brute force attack, starting with single character passwords. This isn't the most efficient attack, and AOPR takes a little time to calculate each password hash, so the Preliminary attack will take a long time to complete or to even find a 3 character password.

- H. To change the attack profile, click the **Stop** button. Click OK to clear all of the dialog and information boxes. Next, click the type of attack you want to perform, for example **Brute Force Attack** or **Dictionary Attack**. Click the **Attack Options** button to set options such as password length or dictionary to use. Click **OK** to close the Attack Options dialog box, then click Start to being the attack.



It can take several minutes to even crack simple passwords, but if you followed directions and used 3 characters AOPR should be able to crack it.

8. Create harder test cases

- C. Repeat the steps for adding a password to a word document and create 4 new Word documents to use as test files. Save all of your Word documents in the same folder.
 - 4) Create 1 file with a password that is 3 alphanumeric characters
 - 5) Create 1 file with a password that is 4 alphabet characters
 - 6) Create 1 file with a password that is 4 alphanumeric characters
- D. Run the AOPR and see if it can recover the passwords from the new files. Keep track of the relative time it takes for the different password lengths.

9. Default Dictionary and Custom Dictionaries

As you've experienced previously, using a dictionary can really speed up password recovery. That is it will speed it up if the password is found in the dictionary. AOPR will use a dictionary, but it doesn't come with a default so you have to specify a dictionary file any time you use the dictionary attack.

- C. Repeat the steps for adding a password to a word document and create 1 or 2 new Word documents to use as test files. Add passwords that are at least 8 characters, but that are also words that are found in the 10,000 most common passwords text file.
 - D. Run the AOPR and see if it can recover the passwords from the new files. Keep track of the relative time it takes for the different password lengths, and compare it with the amount of time required for the brute force attacks.
10. Trade files with another student, and see if you can recover the passwords they added.

7.5.5 Practice Cracking Microsoft Office Passwords Using Brute Force

In this exercise you will use the brute force attack in the AOPR tool to crack the passwords in the several Word Docs. If you are using the **ForensicsPractice** virtual machine the files are all in **Users\CS549\My Documents\secret word files** Folder. If you login as user CS549 (password T549cstt), you will see the folder in your **Documents** folder. Or, you can download the zip file secretWordFilesPractice.zip from Canvas and run AOPR on any computer.

- 8. File: **Why did the chicken cross the road.docx** (Hint - the password is 3 characters, all lower case alpha)
Password: _____
- 9. File: **Chicken2.docx** (Hint - the password is 3 characters, all numerals)
Password: _____
- 10. File: **Chicken3.docx** (Hint - the password is 4 characters, all lower case alpha. This may take a long time, so you can skip it if you wish.)
Password: _____
- 11. File: **Chicken4.docx** (Hint - the password is 3 characters, all lower case alpha)
Password: _____

12. File: **pwtest.docx** (Hint - the password is 4 characters, all numerals)

Password: _____

13. File: **pwtest2.docx** (Hint - the password is 3 characters, all numerals)

Password: _____

7.5.6 Practice Cracking Microsoft Office Passwords Using A Dictionary Attack

In this exercise you will use the dictionary attack in the AOPR tool to crack the passwords in the several Word Docs. If you are using the **ForensicsPractice** virtual machine the files are all in **Users\CS549\My Documents\secret word files** Folder. If you login as user CS549 (password T549cstt), you will see the folder in your **Documents** folder. Or, you can download the zip file secretWordFiles.zip from Canvas and run AOPR on any computer.

3. File: **cn.docx** (Hint - use the dictionary **10k most common.txt**)

Password: _____

4. File: **lawyer.docx** (Hint - use the dictionary **10k most common.txt**)

Password: _____