FORENSICS V2 LAB SERIES

Lab 19: Password Cracking

Document Version: 2021-01-14

Contents

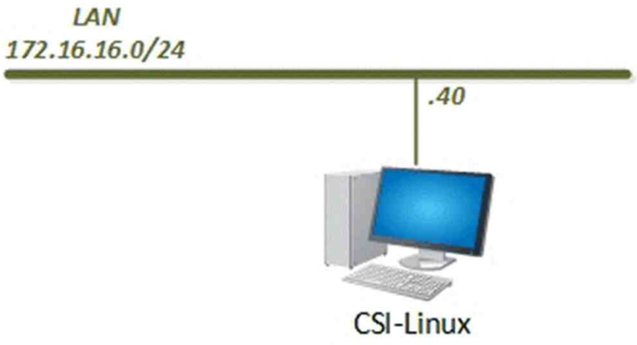
Introduction

Password cracking is a very interesting topic that is always necessary but not very easy. This module will teach how to search for and attempt to crack simple password-protected files that are encountered during the course of an investigation.

Objectives

- Learn how to identify a password-protected file
- Learn about different types of password-protected files
- Learn different types of password cracking methods

Lab Topology



Lab Settings

The information in the table below will be needed in order to complete the lab. The task sections below provide details on the use of this information.

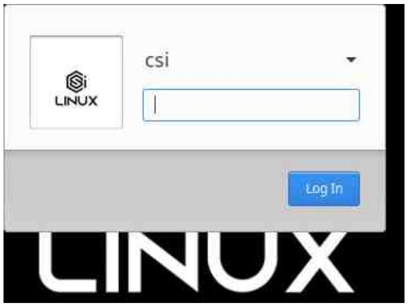
Virtual Machine	**IP Address /** **Subnet Mask**	**Account** (if needed)	**Password** (if needed)
Caine	172.16.16.30	caine	Train1ng$
CSI-Linux	172.16.16.40	csi	csi
DEFT	172.16.16.20	deft	Train1ng$
WinOS	172.16.16.10	Administrator	Train1ng$

1 Identifying and Extracting the Password-protected Files

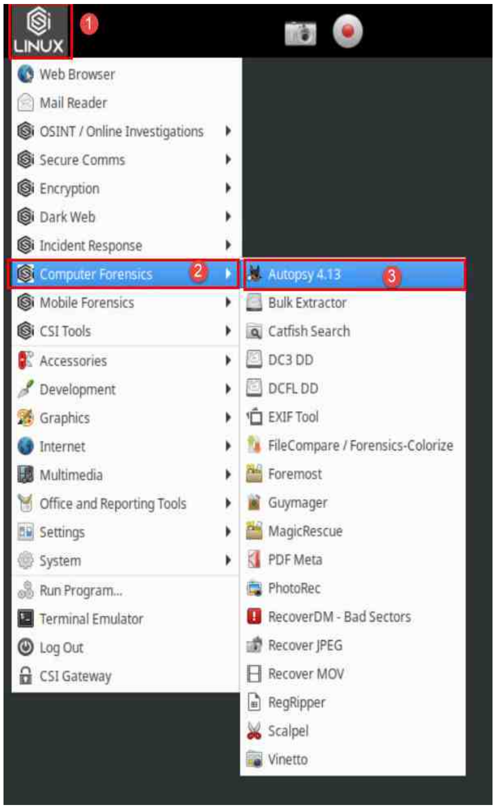
File encryption and password protection are some of the challenges that forensic examiners face. These files, containers, and devices come in various shapes and forms; getting access to the protected data should be considered unless specifically required to do otherwise. In this lab, we will review a simple method to detect password-protected files and how to attempt to gain access to them.

Let us get started by opening Autopsy and loading an FEF.

1. To begin, launch the CSI-Linux virtual machine to access the graphical login screen. Log in as `csi` using the password: `csi`

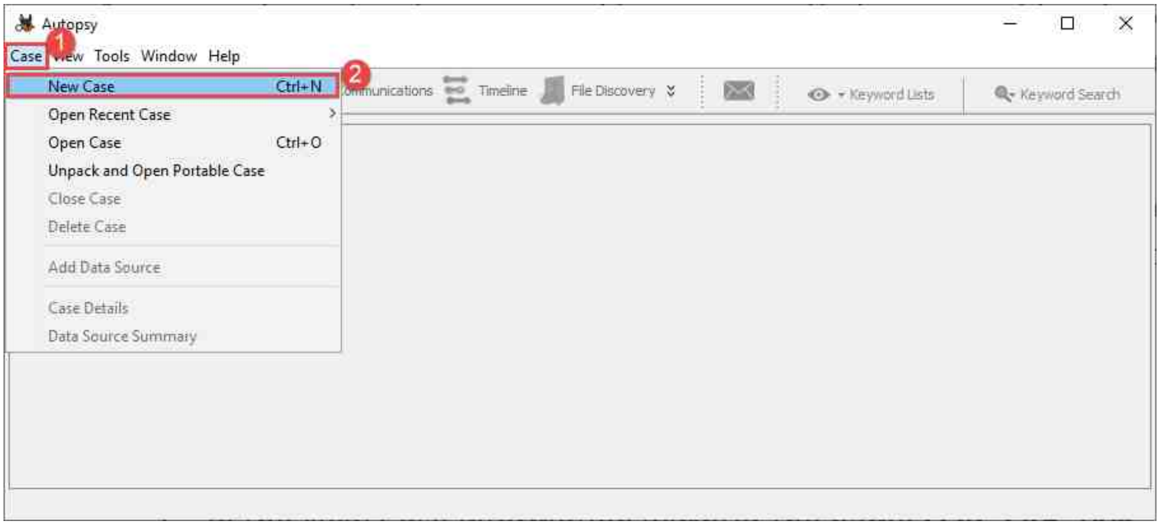


2. Once you are logged into the VM, launch the Autopsy program from the Start menu by navigating to Application Menu (Top-left corner) > Computer Forensics > Autopsy 4.13. Alternatively, you can open Autopsy from the taskbar by clicking the Autopsy icon.

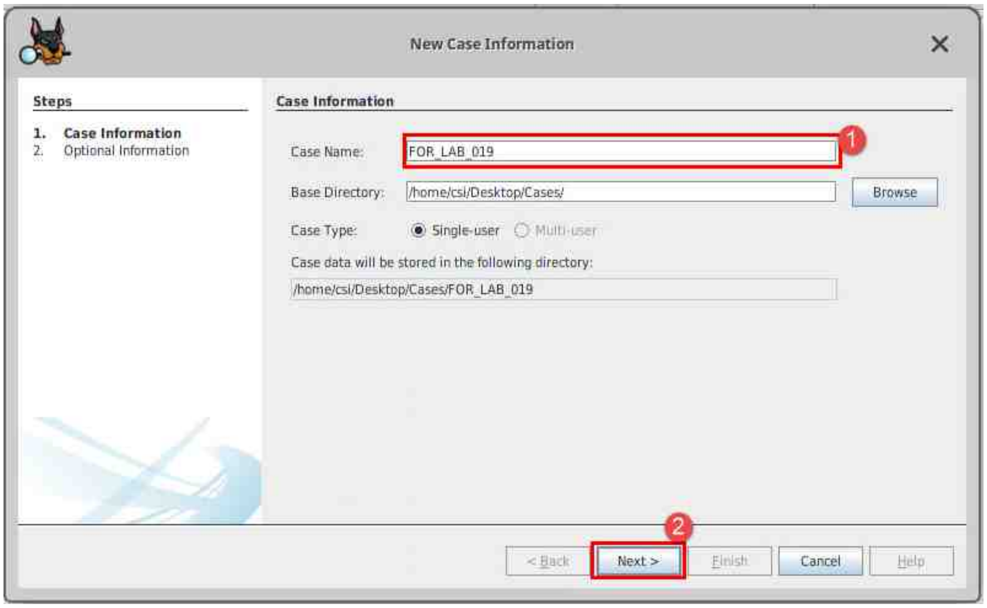


If prompted by Autopsy's welcome screen, click Close and you will be allowed to access the navigation menu.

3. Since you are already familiar with Autopsy, let us jump right in by creating a new case. In Autopsy, click the New Case option from the Case dropdown menu or press Ctrl+N as highlighted below. This will open the New Case Information window.



4. In the New Case Information window, enter FOR_LAB_019 in the Case Name field. The Base Directory field is used to choose the location of the case folder. Let us leave that default selection and click Next as highlighted below.



Case Name: FOR_LAB_019

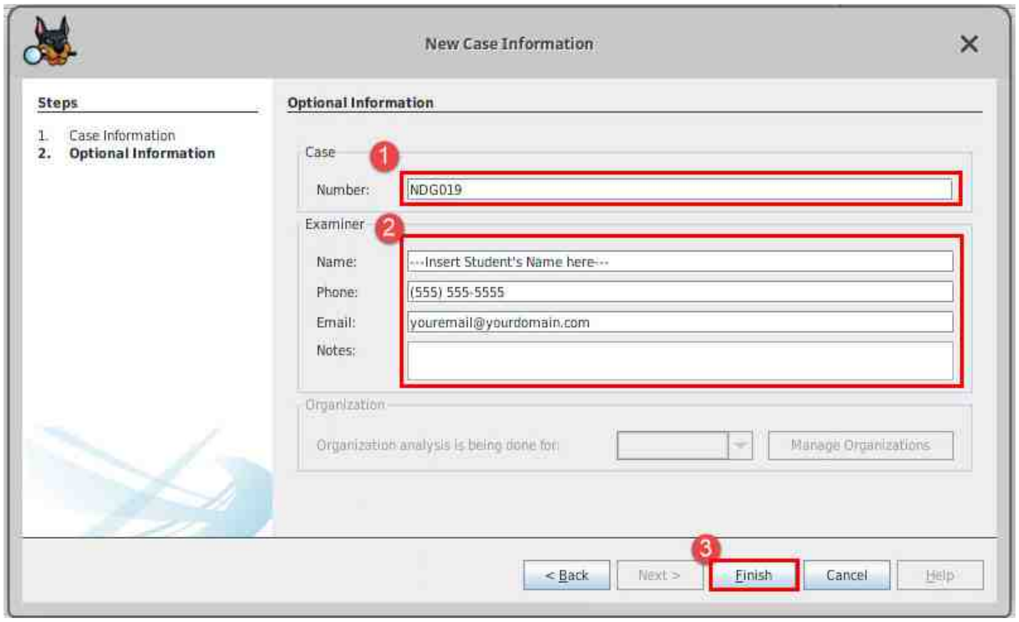
Base Directory: /home/csi/Desktop/Cases/

Case Type: ● Single-user ○ Multi-user

Case data will be stored in the following directory:

/home/csi/Desktop/Cases/FOR_LAB_019

5. The next window in the New Case wizard is the Optional information window. Here you can type more information about the case and examiner. Fill in the information as seen in the fields below and then click Finish when you are done. Remember, the Name field highlighted within the examiner section should contain your name.



New Case Information

Steps
1. Case Information
2. **Optional Information**

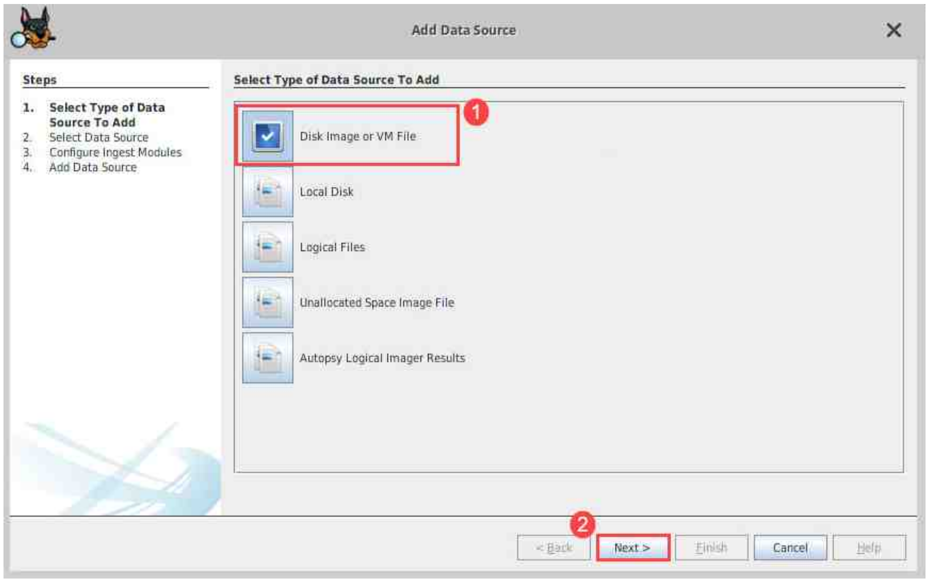
Optional Information

Case
Number: NDG019

Examiner
Name: ---Insert Student's Name here---
Phone: (555) 555-5555
Email: youremail@yourdomain.com
Notes:

Organization
Organization analysis is being done for:

6. You will now be taken to the Add Data Source window. Here you can choose between different evidence sources. In this exercise, we will be using a Forensic Evidence File (FEF) so let us select Disk Image or VM file and click Next as highlighted below.



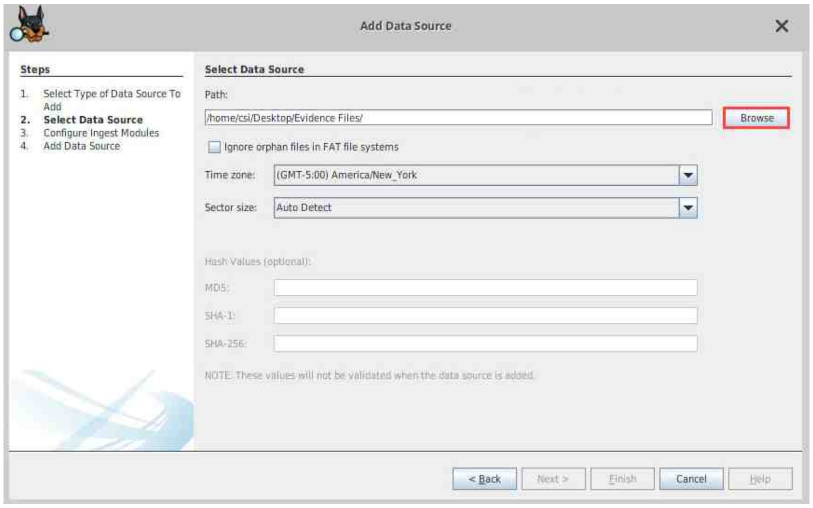
Add Data Source

Steps
1. **Select Type of Data Source To Add**
2. Select Data Source
3. Configure Ingest Modules
4. Add Data Source

Select Type of Data Source To Add

- Disk Image or VM File
- Local Disk
- Logical Files
- Unallocated Space Image File
- Autopsy Logical Imager Results

7. The next window will allow you to choose the image you want to add to the case. Click the Browse button highlighted below to open the Open window that allows you to browse for the FEF.



Add Data Source

Steps

1. Select Type of Data Source To Add
2. **Select Data Source**
3. Configure Ingest Modules
4. Add Data Source

Select Data Source

Path: /home/csi/Desktop/Evidence Files/

□ Ignore orphan files in FAT file systems

Time zone: (GMT-5:00) America/New_York

Sector size: Auto Detect

Hash Values (optional):

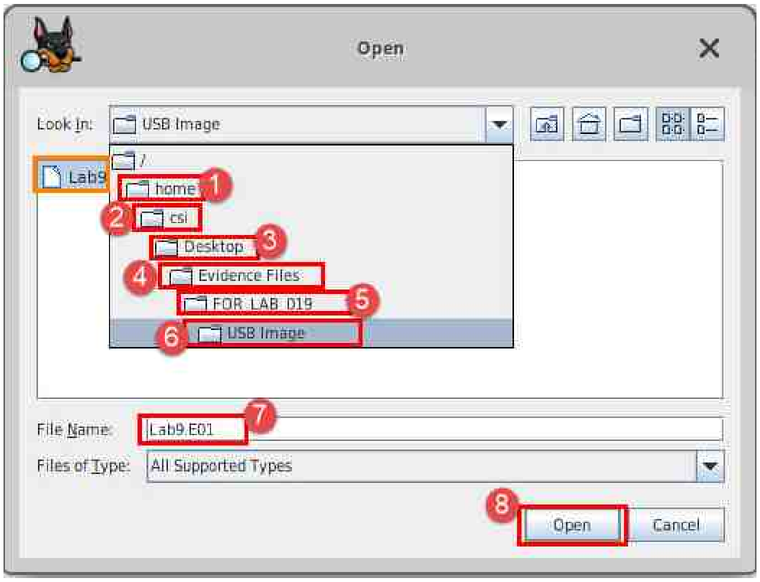
MD5:

SHA-1:

SHA-256:

NOTE: These values will not be validated when the data source is added.

8. In the Open window, browse to Home > csi > Desktop > Evidence Files > FOR_LAB_019 > USB Image and click the file called Lab19.E01 and then click Open as highlighted in steps 1 – 8 below.



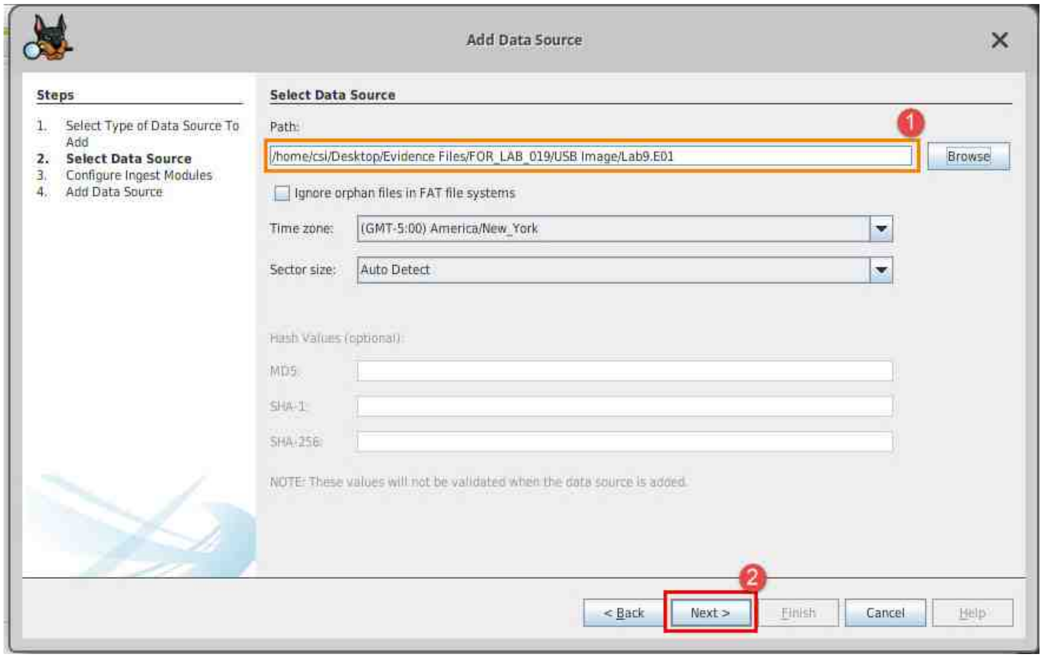
Open

Look In: USB Image

File Name: Lab9.E01

Files of Type: All Supported Types

9. The image path will now appear in the Path field highlighted as item 1 below. We will leave the other options as-is for now and click Next highlighted as item 2 below.



Add Data Source

Steps

1. Select Type of Data Source To Add
2. **Select Data Source**
3. Configure Ingest Modules
4. Add Data Source

Select Data Source

Path: /home/csi/Desktop/Evidence Files/FOR_LAB_019/USB Image/Lab9.E01

□ Ignore orphan files in FAT file systems

Time zone: (GMT-5:00) America/New_York

Sector size: Auto Detect

Hash Values (optional):

MD5:

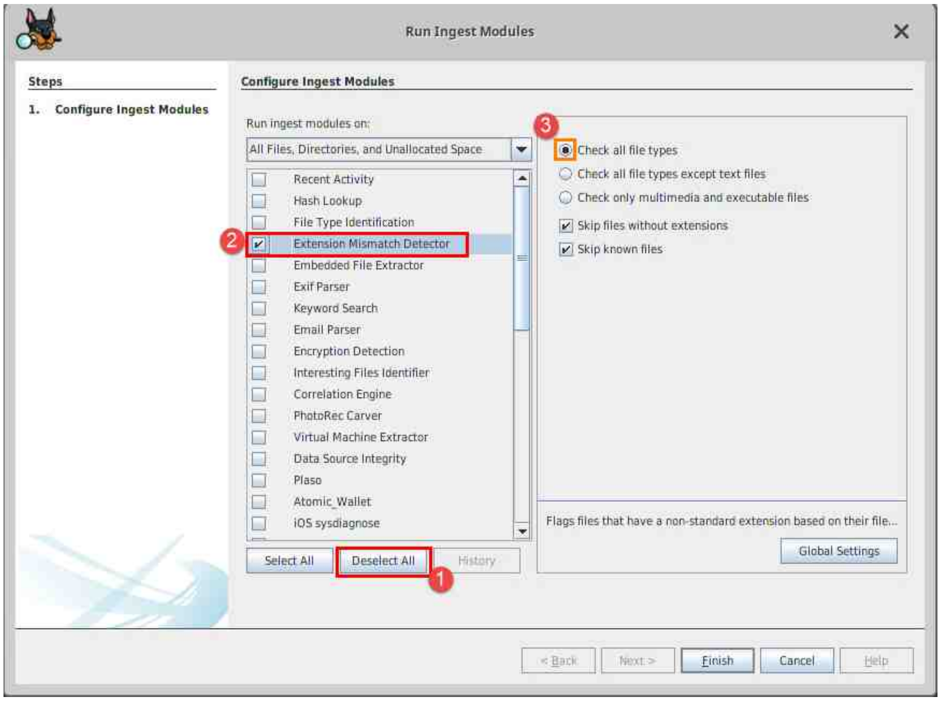
SHA-1:

SHA-256:

NOTE: These values will not be validated when the data source is added.

Time zone is an important aspect to any forensic investigation. Feel free to adjust the time zone to match your respective time zone.

10. You will be taken to the Configure Ingest Modules step of the case creation process. We will be using 2 Ingest Modules in this exercise. Begin by unchecking any selected Ingest Module by clicking the Deselect All button as seen in item 1 below and then scroll and check the Extension Mismatch Detector Ingest Module as seen in item 2 below. You will see some options appear in the Ingest Module settings pane to the right of the ingest Modules, click the radio button beside the Check all file types option to ensure all files are scanned. (This option is best for small evidence files that do not have lots of known files.)



Run Ingest Modules

Steps
1. Configure Ingest Modules

Configure Ingest Modules

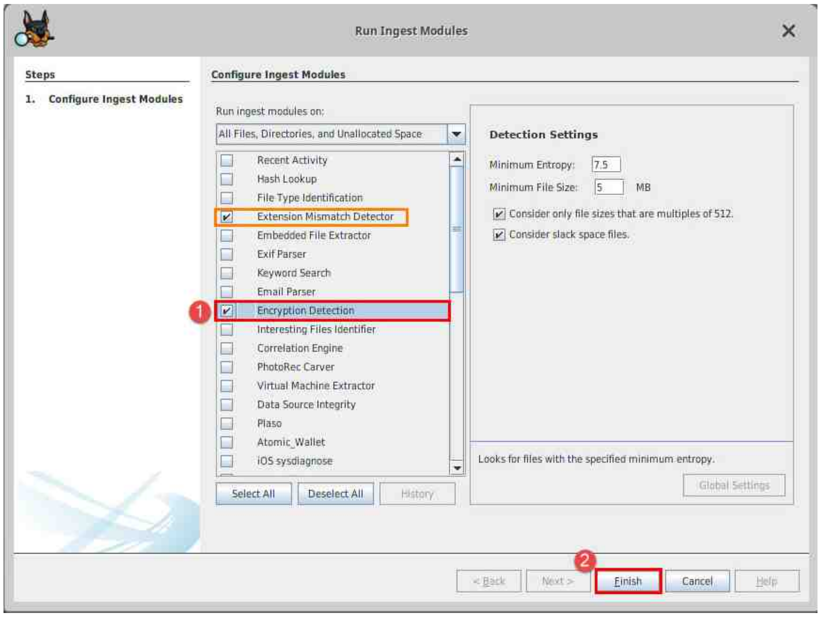
Run ingest modules on: All Files, Directories, and Unallocated Space

- □ Recent Activity
- □ Hash Lookup
- □ File Type Identification
- ☑ Extension Mismatch Detector
- □ Embedded File Extractor
- □ Exif Parser
- □ Keyword Search
- □ Email Parser
- □ Encryption Detection
- □ Interesting Files Identifier
- □ Correlation Engine
- □ PhotoRec Carver
- □ Virtual Machine Extractor
- □ Data Source Integrity
- □ Plaso
- □ Atomic_Wallet
- □ iOS sysdiagnose

- ● Check all file types
- ○ Check all file types except text files
- ○ Check only multimedia and executable files
- ☑ Skip files without extensions
- ☑ Skip known files

Flags files that have a non-standard extension based on their file...

11. Next, select the checkbox beside the Encryption Detection Ingest Module as seen in item 1 below. Leave the options as default for this Ingest Module and click Next as seen in item 2 below.



Run Ingest Modules

Steps
1. Configure Ingest Modules

Configure Ingest Modules

Run ingest modules on: All Files, Directories, and Unallocated Space

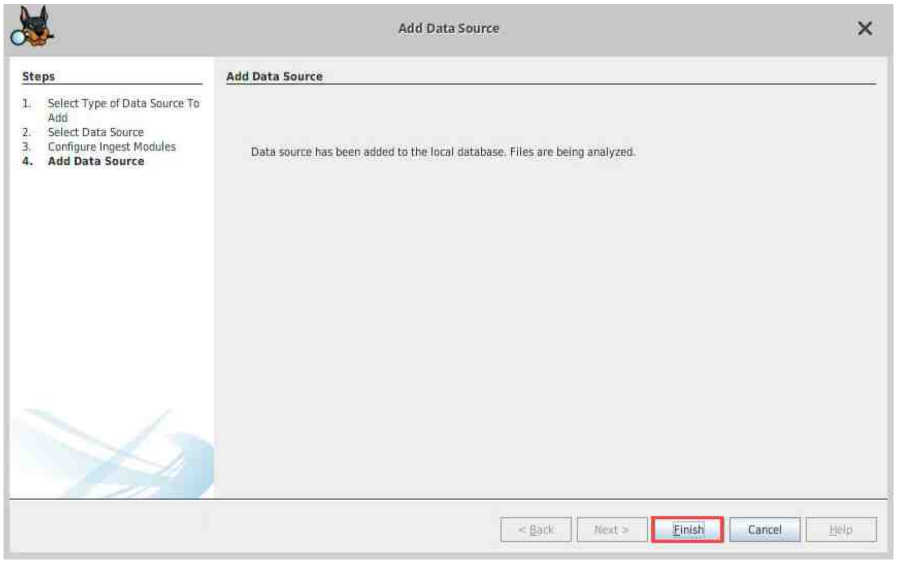
- □ Recent Activity
- □ Hash Lookup
- □ File Type Identification
- ☑ Extension Mismatch Detector
- □ Embedded File Extractor
- □ Exif Parser
- □ Keyword Search
- □ Email Parser
- ☑ Encryption Detection
- □ Interesting Files Identifier
- □ Correlation Engine
- □ PhotoRec Carver
- □ Virtual Machine Extractor
- □ Data Source Integrity
- □ Plaso
- □ Atomic_Wallet
- □ iOS sysdiagnose

Detection Settings

Minimum Entropy: 7.5
Minimum File Size: 5 MB
- ☑ Consider only file sizes that are multiples of 512.
- ☑ Consider slack space files.

Looks for files with the specified minimum entropy.

12. In the final window in the Add Data Source process, click Finish as highlighted below.



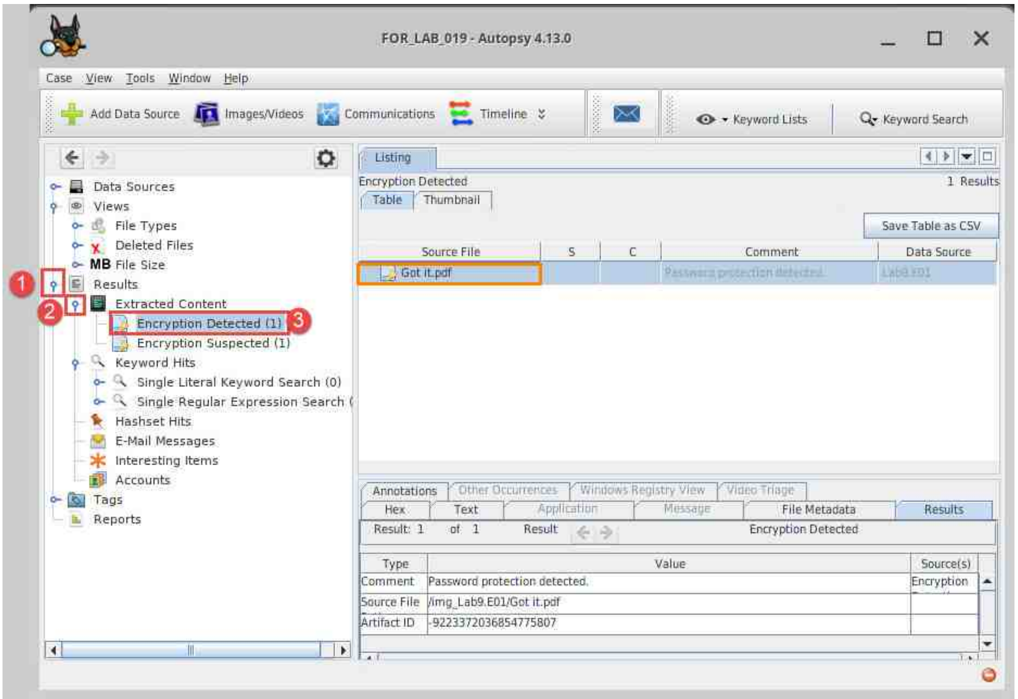
Add Data Source

Steps
1. Select Type of Data Source To Add
2. Select Data Source
3. Configure Ingest Modules
4. **Add Data Source**

Add Data Source

Data source has been added to the local database. Files are being analyzed.

13. You will now be taken to the Autopsy main window. Here we can review the processed data to see if there were any encrypted or password-protected files located. To do this, click the blue pin beside Results > Extracted Content, which will expand and reveal the Categories Encryption Detected or Encryption Suspected, as seen in items 1 and 2 below. Click the category called Encryption Detected to view the encrypted file identified on this volume as seen in item 3. As you can see in the view pane, there is one file called Got it.pdf that is encrypted. If you try to open this file, it will prompt for a password. The file bears a .pdf extension, which means we can use a PDF cracking tool to get access to it.



FOR_LAB_019 - Autopsy 4.13.0

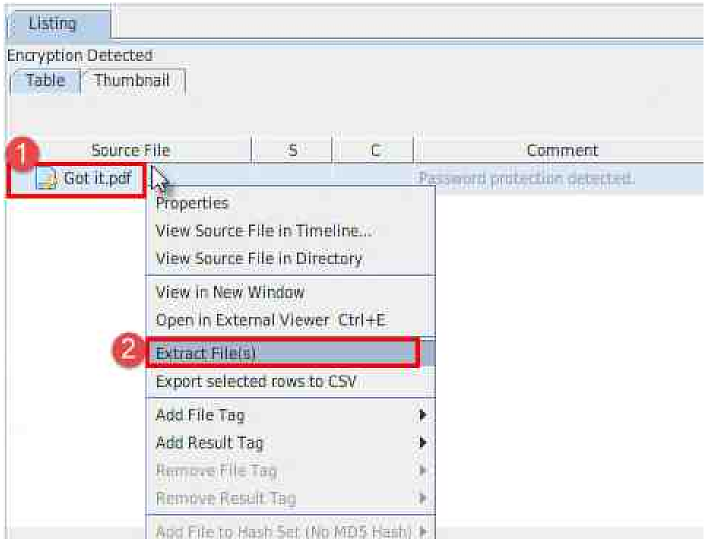
Encryption Detected 1 Results

Source File	S	C	Comment	Data Source
Got it.pdf			Password protection detected.	Lab9.E01

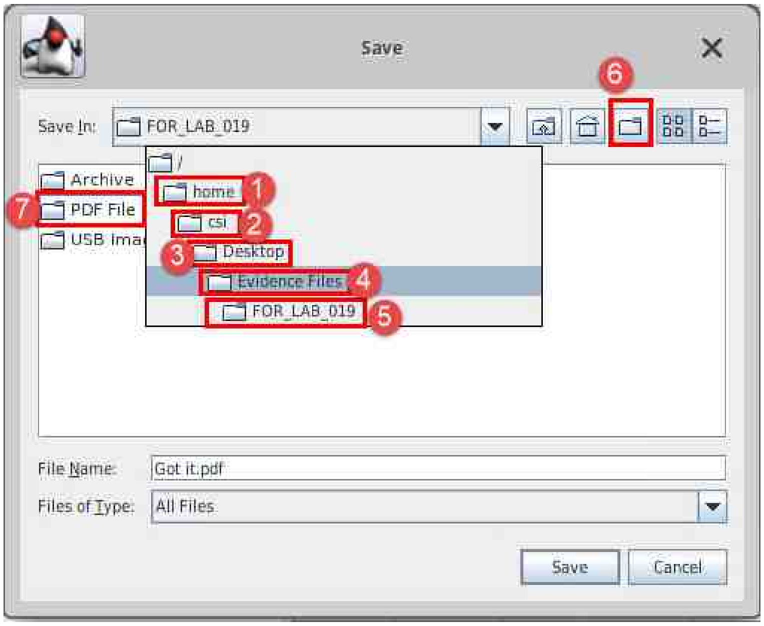
Result: 1 of 1 Result Encryption Detected

Type	Value	Source(s)
Comment	Password protection detected.	Encryption
Source File	/img_Lab9.E01/Got it.pdf	
Artifact ID	-9223372036854775807	

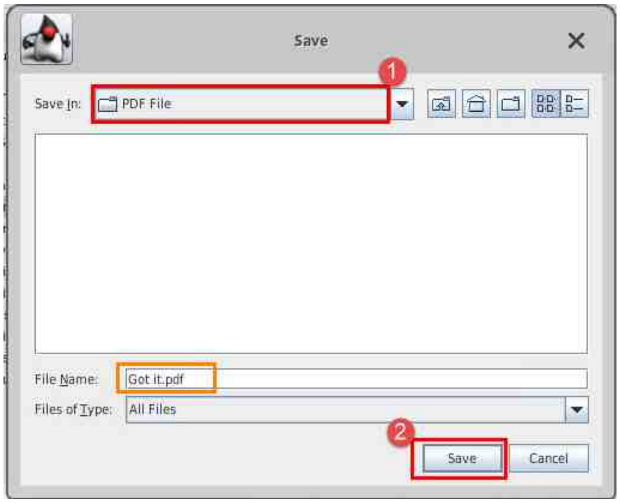
14. We will attempt to crack the password for this file using a command line tool called pdfcrack, so we will need to export it. Do this by right-clicking on the file and clicking Extract File(s) from the context menu that appears as seen in items 1 and 2 below.


Listing
Encryption Detected
Table
Thumbnail
Source File
S
C
Comment
1
Got it.pdf
Password protection detected.
Properties
View Source File in Timeline...
View Source File in Directory
View in New Window
Open in External Viewer Ctrl+E
2
Extract File(s)
Export selected rows to CSV
Add File Tag
Add Result Tag
Remove File Tag
Remove Result Tag
Add File to Hash Set (No MD5 Hash)

15. In the Save window that appears, navigate to home > csi > Desktop > Evidence Files > FOR_LAB_019 as seen in items 1 – 5 below. Once there, click the Make new folder button and name the new folder `pdf_file` as seen in items 6 and 7 below.



16. Next, double-click the folder you just created called pdf_file to open it and then click Save as seen in items 1 and 2 below.

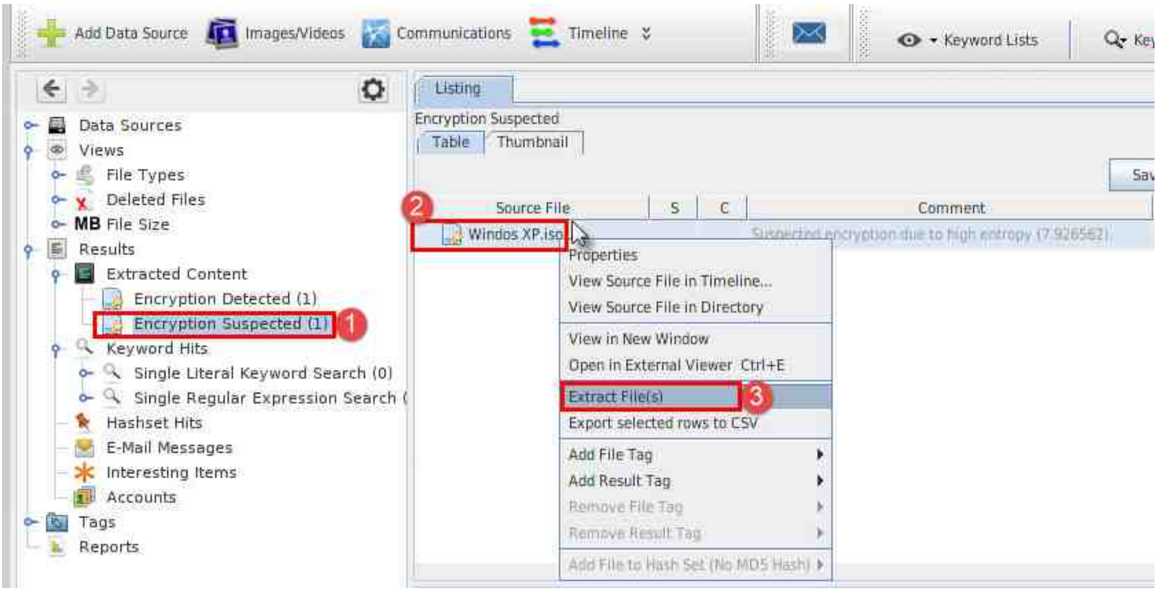


Save In: PDF File

File Name: Got it.pdf

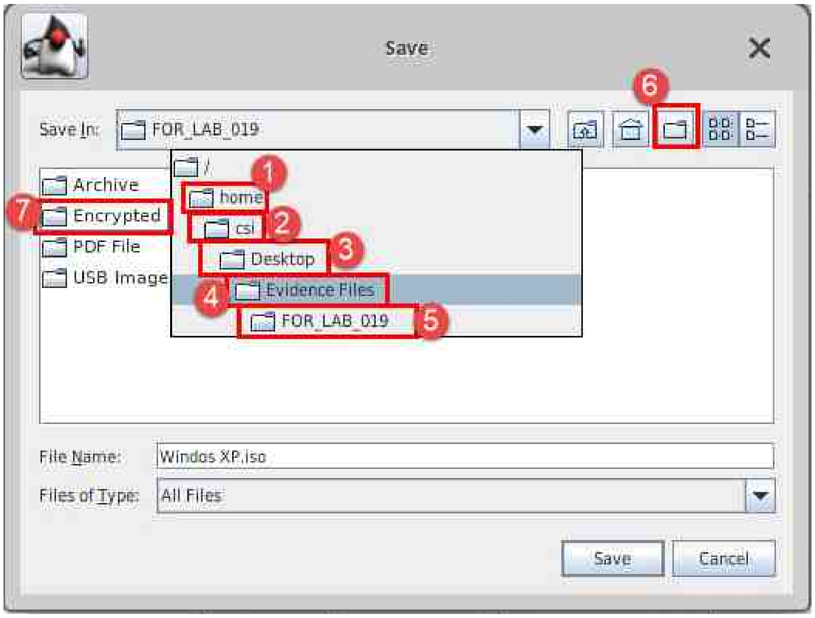
Files of Type: All Files

17. Now, before we attempt to crack the password for that file, let us look at the other file that was tagged Encryption Suspected. Do this by clicking Encryption Suspected in the Extracted Content tab, as seen in item 1 below. The file we see here is called Windows XP.iso and was flagged suspicious because it had high entropy, which means the data in the file is unusually random. Let us export this file as well by right-clicking the file called Windows XP.iso and then clicking Extract File(s) from the context menu that appears as seen in items 2 and 3 below.

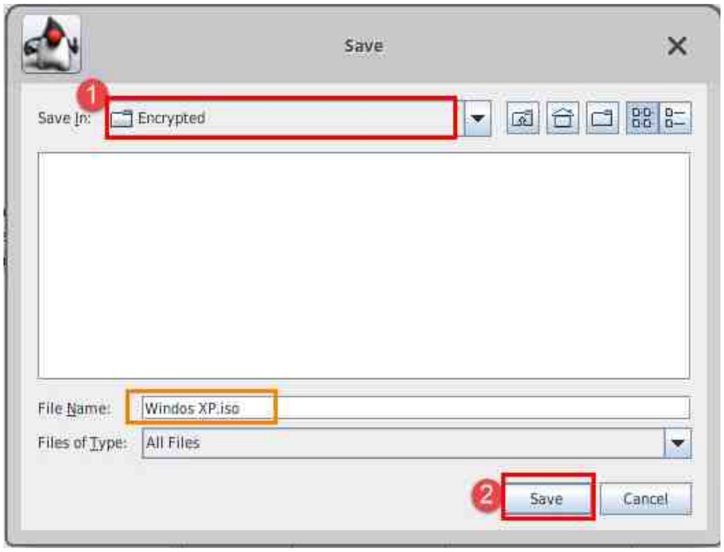


Source File	S	C	Comment
Windos XP.iso			Suspected encryption due to high entropy (7.926562)

18. In the Save window that appears, navigate to home > csi > Desktop > Evidence Files > FOR_LAB_019 as seen in items 1 – 5 below. Once there, click the Create New Folder icon to create a new folder and name the folder `Encrypted` as seen in items 6 and 7 below.



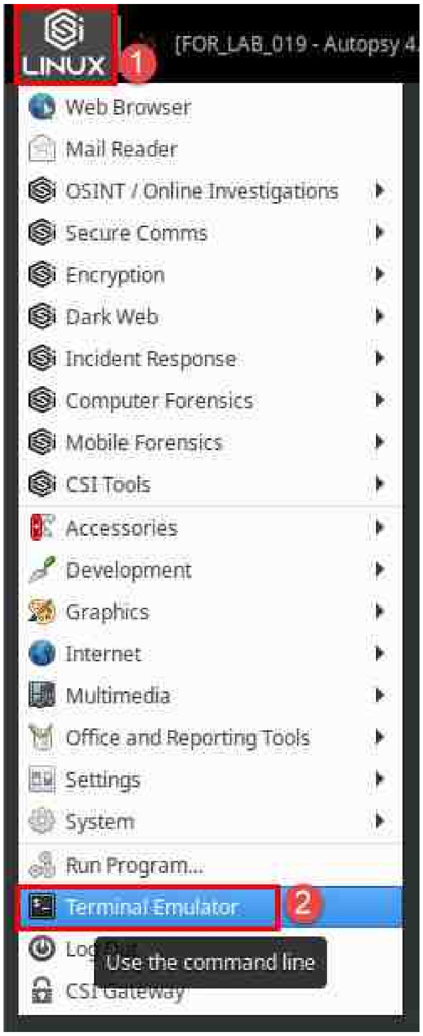
19. Next, double-click the folder you just created called Encrypted to open it and then click Save as seen in item 1 and 2 below.



20. This exercise was simple as the software did the digging to identify encrypted files. There are many other tools out there that can identify password protected and encrypted files. You can research to expand your toolkit. We were able to identify and export these files; now, let us move to cracking with PDFCrack.

2 Cracking a PDF File with PDFCrack

1. Now that we have the Got it.pdf file exported, let's try to crack the password. There are many different password cracking techniques. The popular ones are; Brute-force, which tests random passwords until it gets the right one and can be very time consuming; Dictionary cracking, which checks large wordlists of common passwords against the encrypted file; Rainbow tables, which use extremely large lists of hashes to crack files instead of the passwords themselves. In this exercise, we will use a dictionary attack, but it requires a hash of the encrypted file to run. Let's begin by opening the Terminal. Do this by clicking Terminal Emulator from the application menu, as seen in items 1 and 2 below.



2. Let's change the directory to the folder called pdf_file that we exported the file to. Do this by typing the following command:

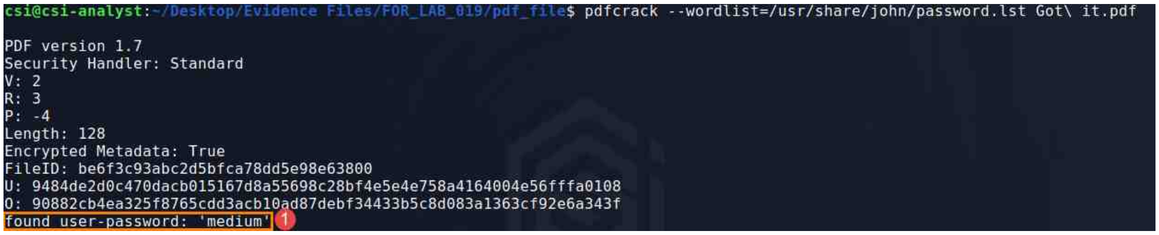
```
cd Desktop/Evidence\ Files/FOR_LAB_019/pdf_file
```

3. You will now be in the folder called pdf_file. Now let's run the pdfcrack command to attempt to crack the password of this PDF file using a wordlist for john the ripper, another password cracking tool that we will cover in more advanced courses. Type the following command to run the process.

```
pdfcrack --wordlist=/usr/share/john/password.lst Got\ it.pdf
```

As you can see from the above command, the command --wordlist= tells pdfcrack what wordlist to use. The path /usr/share/john/password.lst is the location of the wordlist and the final term Got\ it.pdf is the target PDF file.

4. The command you just ran, if successful, will print the screen as seen below. It will indicate that it found user-password. The password is the value in single quotes, as seen in item 1 below.

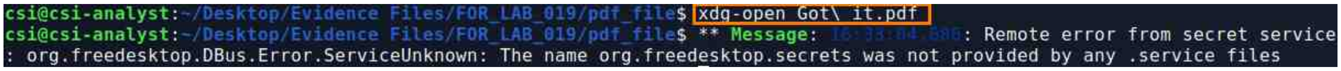


```
csi@csi-analyst:~/Desktop/Evidence Files/FOR_LAB_019/pdf_file$ pdfcrack --wordlist=/usr/share/john/password.lst Got\ it.pdf

PDF version 1.7
Security Handler: Standard
V: 2
R: 3
P: -4
Length: 128
Encrypted Metadata: True
FileID: be6f3c93abc2d5bfca78dd5e98e63800
U: 9484de2d0c470dacb015167d8a55698c28bf4e5e4e758a4164004e56fffa0108
O: 90882cb4ea325f8765cdd3acb10ad87debf34433b5c8d083a1363cf92e6a343f
found user-password: 'medium'
```

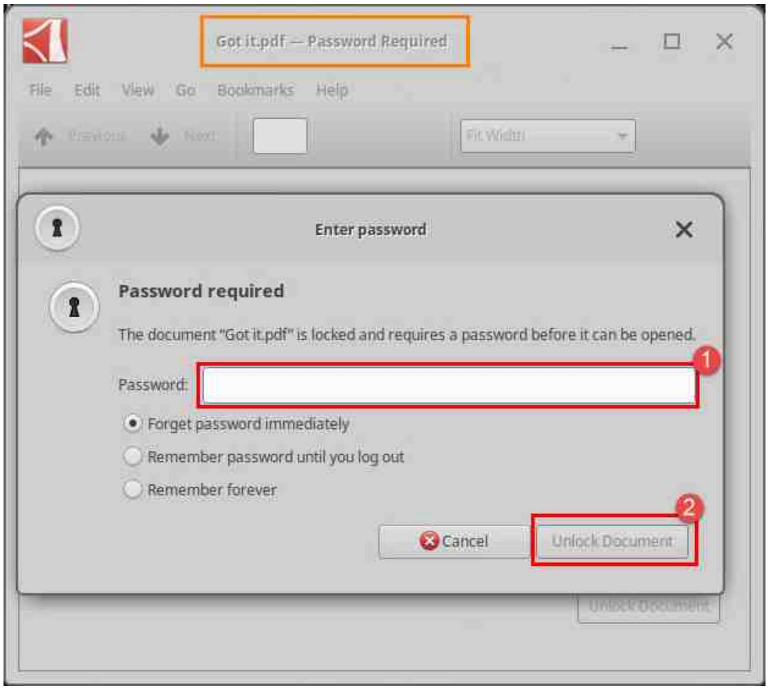
5. Now let's open this file to see its content. Do this by typing the following command and press Enter.

```
xdg-open Got\ it.pdf
```

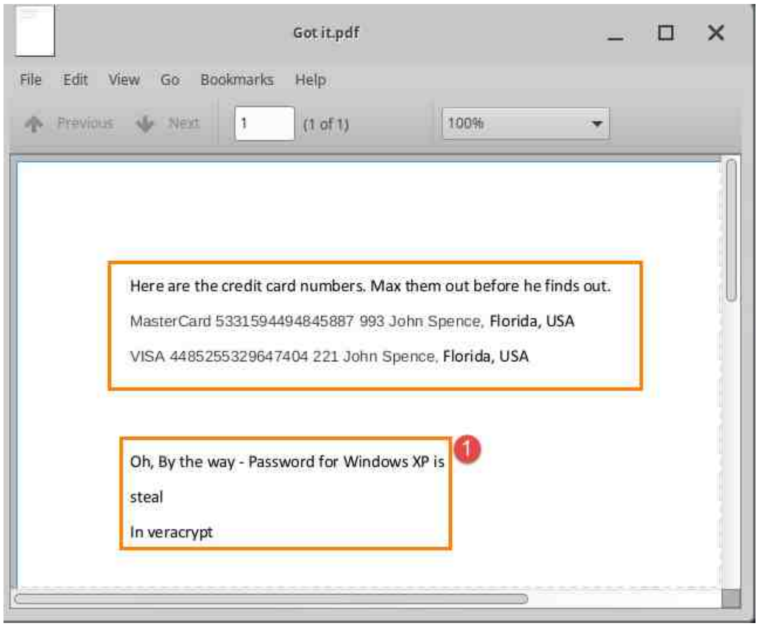


```
csi@csi-analyst:~/Desktop/Evidence Files/FOR_LAB_019/pdf_file$ xdg-open Got\ it.pdf
csi@csi-analyst:~/Desktop/Evidence Files/FOR_LAB_019/pdf_file$ ** Message: 16:33:04.886: Remote error from secret service
: org.freedesktop.DBus.Error.ServiceUnknown: The name org.freedesktop.secrets was not provided by any .service files
```

6. You will now see a prompt appear that asks you to enter the password for the PDF file. Enter the password you found and then click Unlock Document, as seen in items 1 and 2 below.


Got it.pdf — Password Required
File Edit View Go Bookmarks Help
Previous Next
Fit Width
Enter password
Password required
The document "Got it.pdf" is locked and requires a password before it can be opened.
Password:
1
● Forget password immediately
○ Remember password until you log out
○ Remember forever
2
Cancel
Unlock Document

7. As you can see from the document, there are many suspicious things going on here. Pay special attention to the text that talks about Windows XP, as seen in item 1 and make a note of the password mentioned, steal. It also mentions Vercarypt, which is software used to encrypt files, volumes, and partitions. Let's take a quick look to see if the suspicious encrypted file called Windows XP.iso was, in fact, an encrypted container.



Here are the credit card numbers. Max them out before he finds out.

MasterCard 5331594494845887 993 John Spence, Florida, USA

VISA 4485255329647404 221 John Spence, Florida, USA

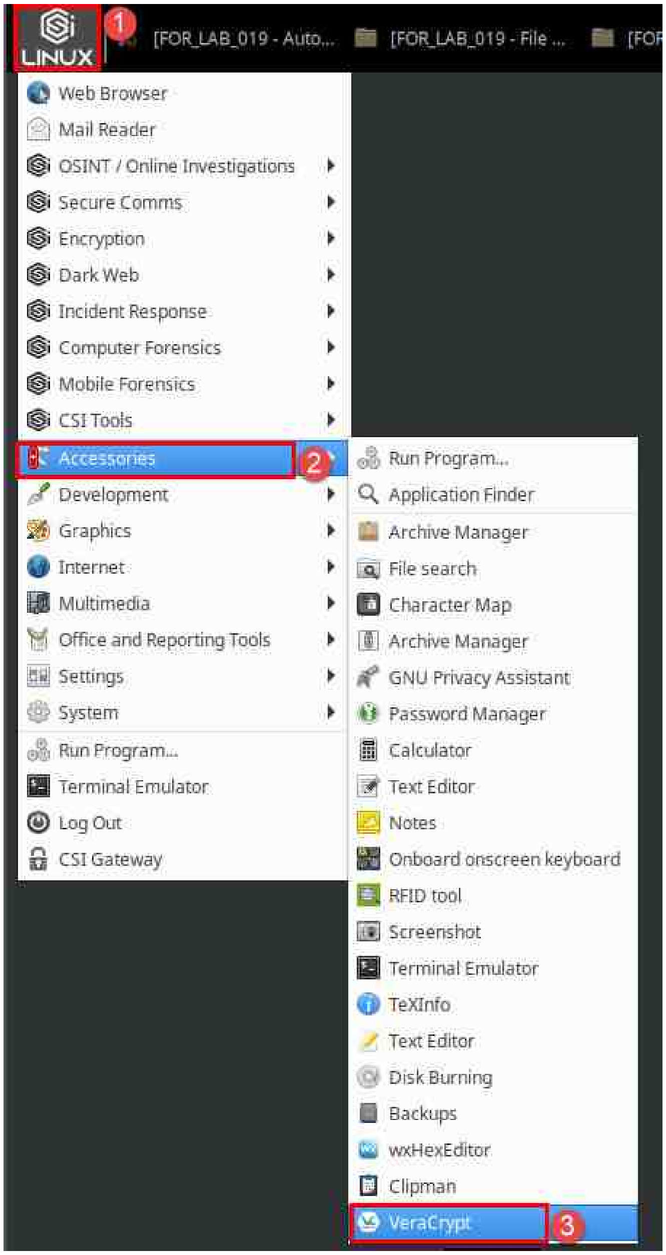
Oh, By the way - Password for Windows XP is

steal

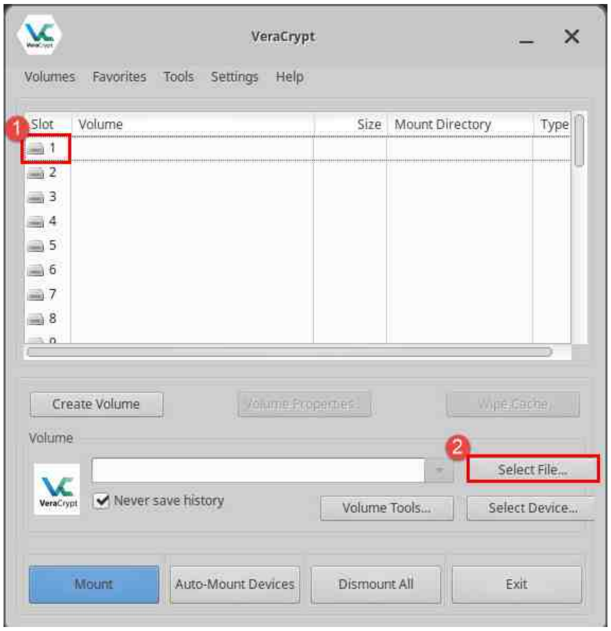
In veracrypt

3 Mounting an Encrypted Container in Veracrypt

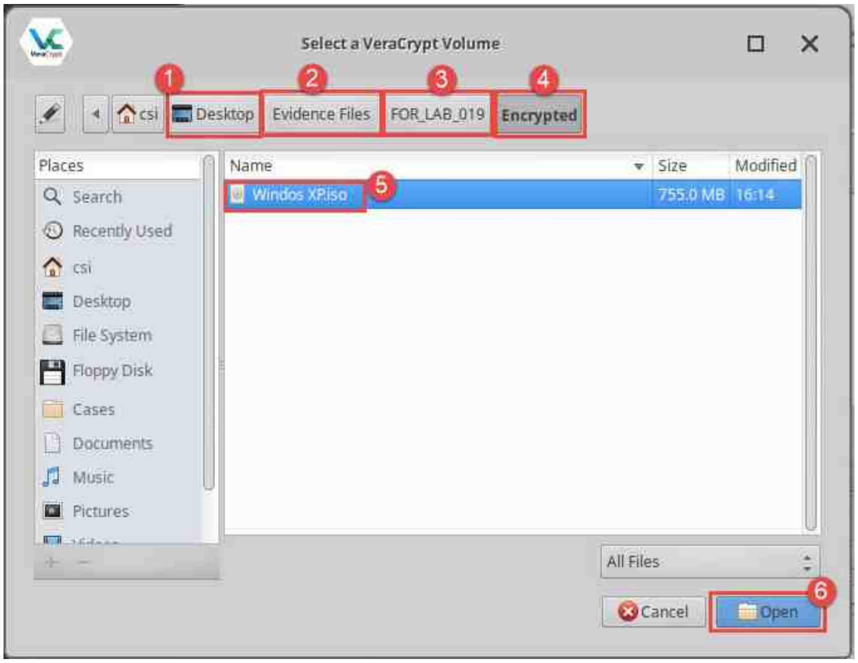
1. Veracrypt is already installed on this computer, so let's jump right in by clicking the applications menu at the top-left corner of the Desktop, as seen in item 1, and typing `veracrypt` in the search box, as seen in item 2 below. Click the veraCrypt icon once it appears, as seen in item 3 below.



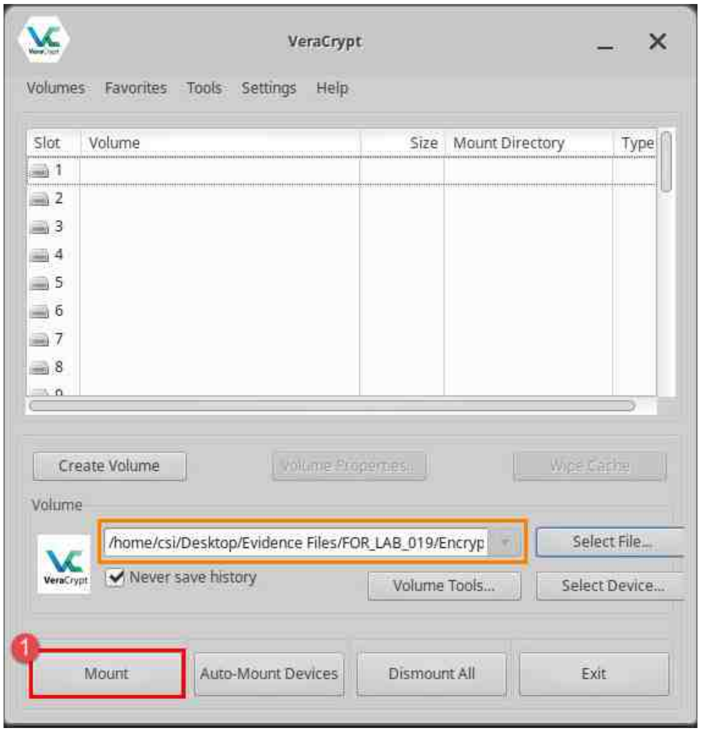
2. Since we will only be opening a volume, we won't get into too much detail about this tool. You can, however, view the help file to learn more. Let's begin by clicking one of the numbered rows, as seen in item 1 below. This row will provide details about the mounted volume. Next, click the Select File… button, as seen in item 2 below, to open the Select a VeraCrypt Volume window, which allows you to browse to your suspected or intended encrypted file.



3. Now navigate to Desktop > Evidence Files > FOR_LAB_019 > Encrypted as seen in items 1, 2, 3, and 4 below. Once there, click the file you exported, called Windows XP.iso, and then click Open as seen in items 5 and 6 below.



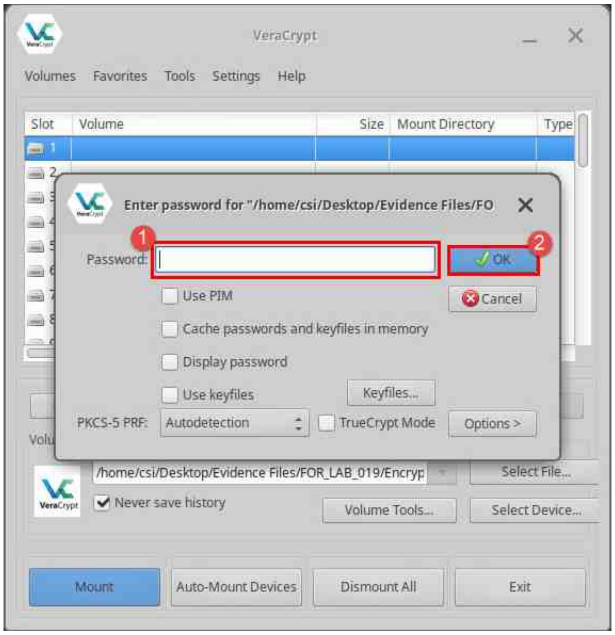
4. You will be taken back to the main VeraCrypt window. Verify that you have a slot number selected and your path is correct. Once you are done, click the Mount button as seen in item 1 below. This will open the Enter password for window.



/home/csi/Desktop/Evidence Files/FOR_LAB_019/Encryp

☑ Never save history

5. Enter the password you saw in the PDF file, which was `steal` and click OK as seen in items 1 and 2 below.



Password:

□ Use PIM

□ Cache passwords and keyfiles in memory

□ Display password

□ Use keyfiles

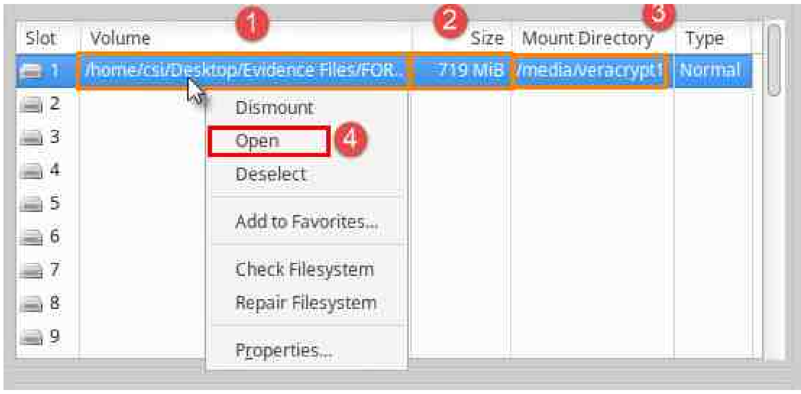
PKCS-5 PRF: Autodetection □ TrueCrypt Mode

/home/csi/Desktop/Evidence Files/FOR_LAB_019/Encryp

☑ Never save history

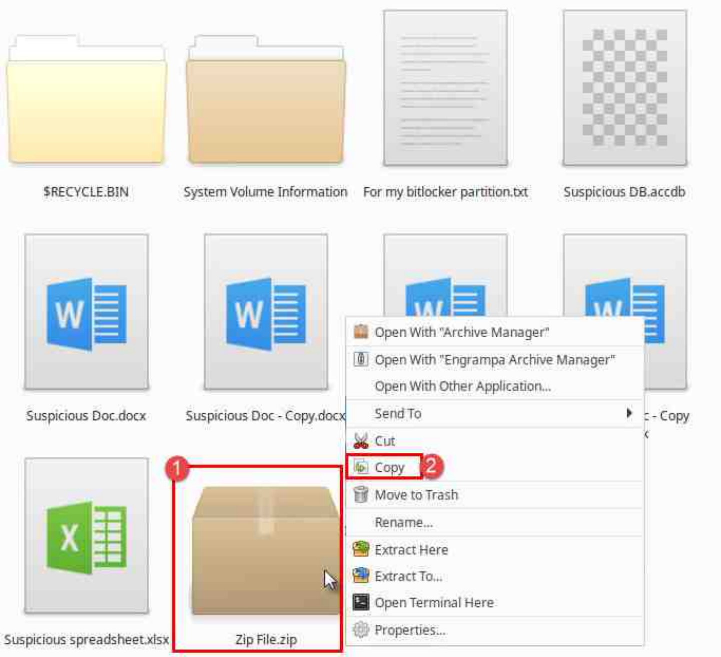
You may also be prompted for the Administrator's password for the computer. If so, enter the password `csi` and then click OK.

6. The volume is now mounted, and you can see that data has appeared in the slot you selected. As you can see, it lists the name of the mounted file, its size, and mount directory as seen in items 1, 2, and 3 below. Let's take a look at the contents of this volume. Do this by right-clicking the slot, as seen in item 4, and then click the Open option from the context menu that appears.



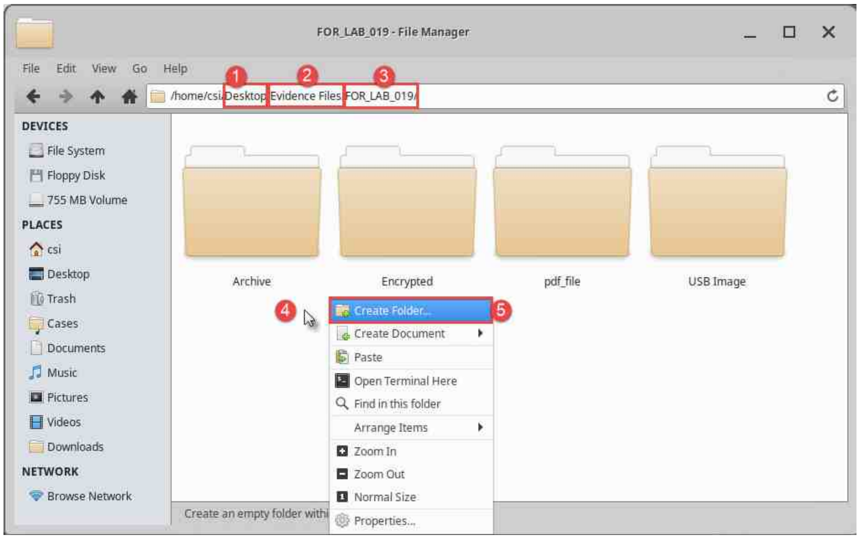
Slot	Volume	Size	Mount Directory	Type
1	/home/csi/Desktop/Evidence Files/FOR...	719 MiB	/media/veracrypt1	Normal
2				
3				
4				
5				
6				
7				
8				
9				

7. The File Manager will automatically open, revealing the contents of the volume. As you can see, there are many suspicious items in the volume. Only one file here is password protected, which is the zip file called Zip File.zip, as seen in item 1. We could repeat the process of adding it to our Autopsy case, but since we are already familiar with that process, let's not repeat it. We can verify that it is password protected by trying to extract it. However, let's first copy it to a different folder. This is because any change made to this mounted volume will be saved because it operates just like an external drive, such as USB drives, etc. To begin, right-click Zip File.zip and click Copy from the context menu that appears as seen in item 2 below.

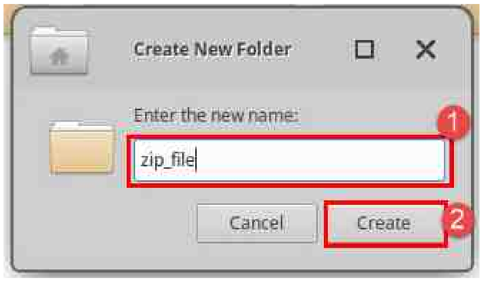


$RECYCLE.BIN
System Volume Information
For my bitlocker partition.txt
Suspicious DB.accdb
Suspicious Doc.docx
Suspicious Doc - Copy.docx
: - Copy
Suspicious spreadsheet.xlsx
Zip File.zip
1
2
Open With "Archive Manager"
Open With "Engrampa Archive Manager"
Open With Other Application...
Send To
Cut
Copy
Move to Trash
Rename...
Extract Here
Extract To...
Open Terminal Here
Properties...

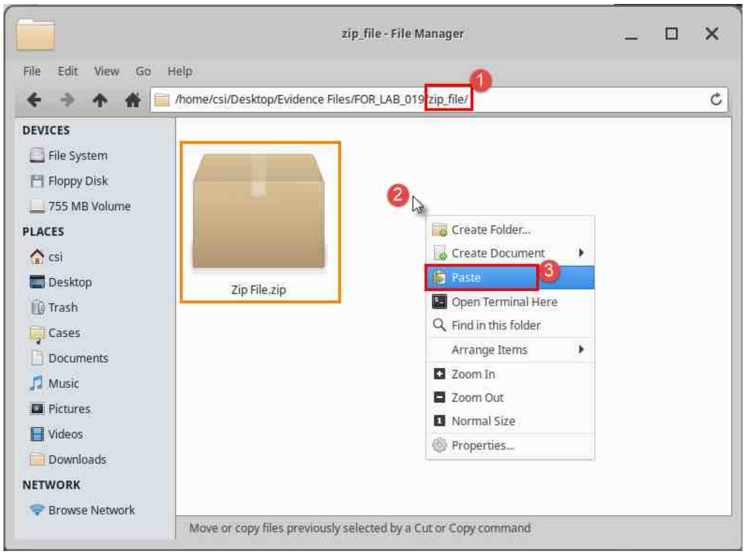
8. Now navigate to Desktop > Evidence Files > FOR_LAB_019 as seen in items 1, 2 and 3 below. Next, right-click in the open area within the folder and click Create Folder as seen in items 4 and 5 below.



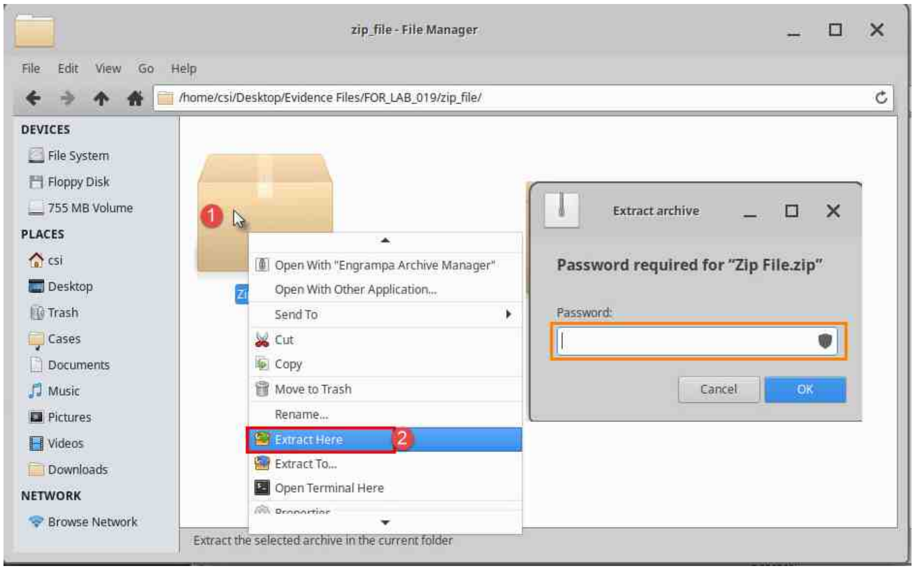
9. Name the new folder `zip_file` and then click Create, as seen in items 1 and 2 below.



10. Then double-click the newly created folder to open it. Once inside, paste Zip File.zip by right-clicking in an empty space in the folder and clicking Paste as seen in items 2 and 3 below.



11. Once this is done, right-click on Zip File.zip once again and click Extract Here from the context menu that appears. You will be prompted with a password required window.

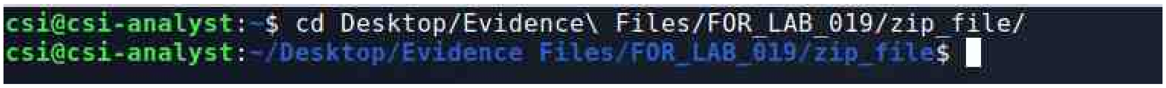


12. Now we're sure this file is password protected. In the next exercise, we will try to crack this file. Cancel the extract archive request for now, and let's proceed.

4 Cracking a Zip File with Fast Crack Zip

1. The Fast Crack Zip tool is like the PDF Crack tool we used. In this exercise, we will perform both brute force and dictionary attacks to compare the two. Let's begin by returning to the terminal emulator. Let's change the directory to the folder called zip_file that we copied the zip file to. Do this by typing the following command:

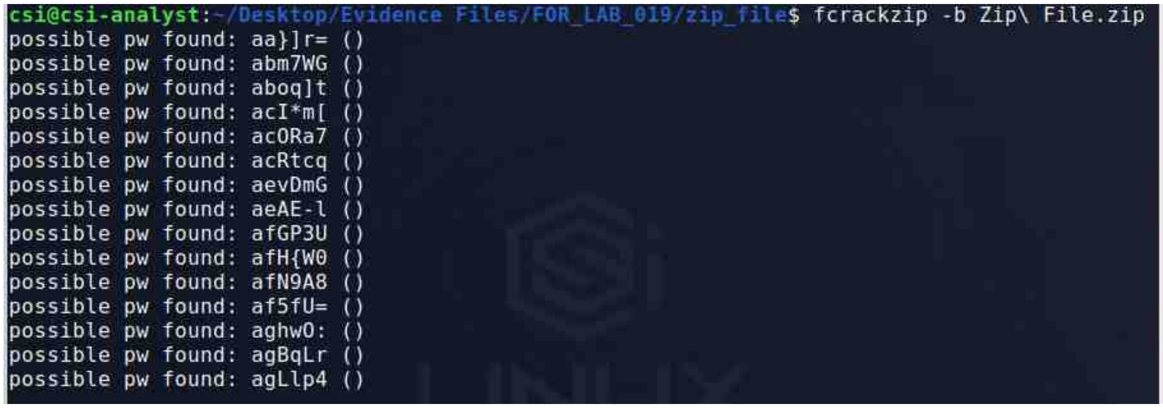
```
cd Desktop/Evidence\ Files/FOR_LAB_019/zip_file
```



```
csi@csi-analyst:~$ cd Desktop/Evidence\ Files/FOR_LAB_019/zip_file/
csi@csi-analyst:~/Desktop/Evidence Files/FOR_LAB_019/zip_file$ 
```

2. You will now be in the folder called zip_file. Now let's run the fcrackzip command to attempt to crack the password of this PDF file using brute force. We won't wait until it's done because this process can be extremely time-consuming. Type the following command and press Enter:

```
fcrackzip -b Zip\ File.zip
```



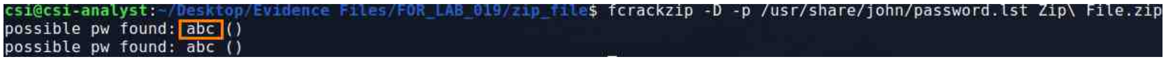
```
csi@csi-analyst:~/Desktop/Evidence Files/FOR_LAB_019/zip_file$ fcrackzip -b Zip\ File.zip
possible pw found: aa}]r= ()
possible pw found: abm7WG ()
possible pw found: aboq]t ()
possible pw found: acI*m[ ()
possible pw found: acORa7 ()
possible pw found: acRtcq ()
possible pw found: aevDmG ()
possible pw found: aeAE-l ()
possible pw found: afGP3U ()
possible pw found: afH{W0 ()
possible pw found: afN9A8 ()
possible pw found: af5fU= ()
possible pw found: aghw0: ()
possible pw found: agBqLr ()
possible pw found: agLlp4 ()
```

The -b in the command will start the brute force process and you will see many possible passwords appear.

3. Since we don't have the time to let this process complete, let's cancel it and use our wordlist. Cancel this by entering Ctrl+C. Next, type the following command and press Enter to use our previous wordlist.

```
fcrackzip -D -p /usr/share/john/password.lst      Zip\ File.zip
```

4. As you can see, the results appear almost instantaneously. This is because the wordlist is small, and the password is extremely easy. In the real world, password cracking requires computers with lots of processing power and huge wordlists, rainbow tables, or brute force waiting times. Even then, recovery is not guaranteed.

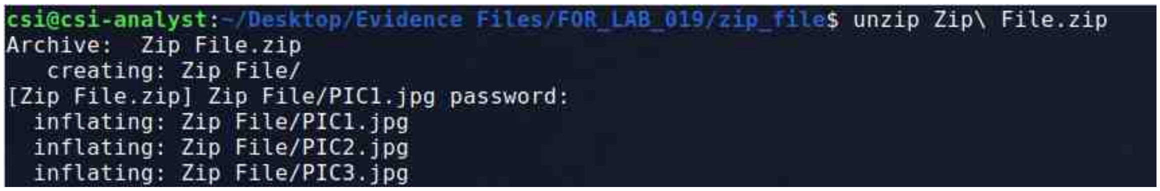


```
csi@csi-analyst:~/Desktop/Evidence Files/FOR_LAB_019/zip_file$ fcrackzip -D -p /usr/share/john/password.lst Zip\ File.zip
possible pw found: abc ()
possible pw found: abc ()
```

5. Now let’s open this file to see its content. Do this by typing the following command and press Enter.

```
Unzip Zip\ File.zip
```

6. You will now see a prompt appear that asks you to enter the password for the zip file. Enter the password you recovered, and press Enter. The contents of the zip file will be exported to the same directory. You can navigate to this location using File Manager to view the extracted files.



```
csi@csi-analyst:~/Desktop/Evidence Files/FOR_LAB_019/zip_file$ unzip Zip\ File.zip
Archive:  Zip File.zip
   creating: Zip File/
[Zip File.zip] Zip File/PIC1.jpg password:
  inflating: Zip File/PIC1.jpg
  inflating: Zip File/PIC2.jpg
  inflating: Zip File/PIC3.jpg
```

7. This exercise covered identifying, extracting, and cracking simple file passwords. In real-world scenarios, the passwords will almost always be complex, and the variety of encryption techniques used will be wide. This should not deter you as an examiner, however. Having a dedicated workstation for password cracking is a great start as well as having commercial tools that make the job a lot easier. That being said, the tools we used here are still widely used, and others like John the Ripper and Hashcat are free, open source tools that are extremely powerful and can get the job done just as well.

8. We are now at the end of our lab. Dismount the VeraCrypt volume and close all the open windows by clicking the X at the top-right corner of each window as seen in items 1 - 5 below.