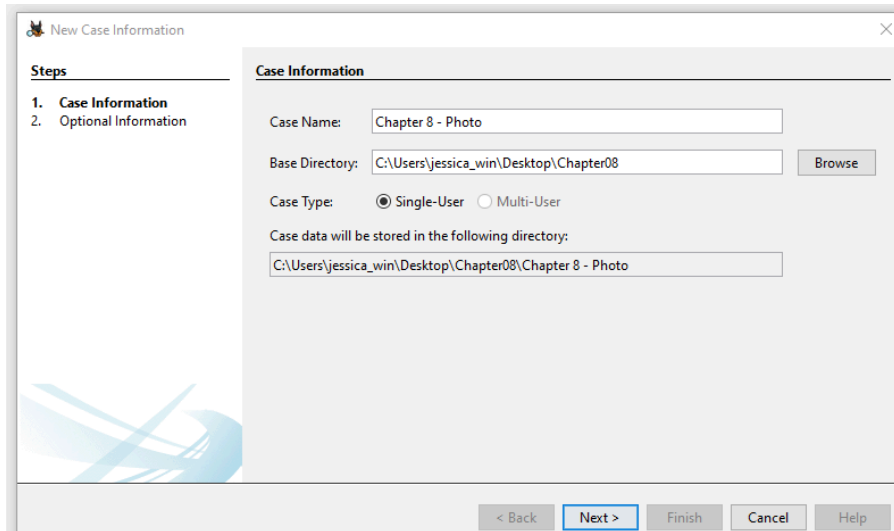


Task 1: Recover Digital Photo Evidence

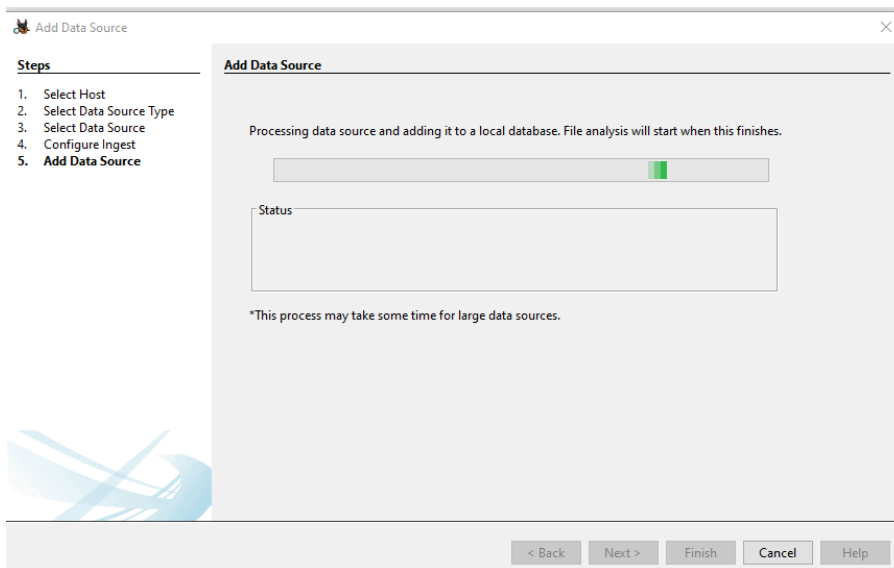
Step 1: Create Case



The 'New Case Information' dialog box is shown. It has a 'Steps' pane on the left with two steps: '1. Case Information' (selected) and '2. Optional Information'. The main area is titled 'Case Information' and contains the following fields:

- Case Name:** Chapter 8 - Photo
- Base Directory:** C:\Users\jessica_win\Desktop\Chapter08 (with a 'Browse' button)
- Case Type:** ☒ Single-User ☐ Multi-User
- Case data will be stored in the following directory:** C:\Users\jessica_win\Desktop\Chapter08\Chapter 8 - Photo

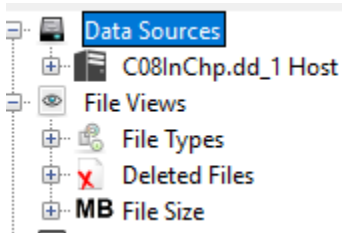
At the bottom are buttons: '< Back', 'Next >', 'Finish', 'Cancel', and 'Help'.



The 'Add Data Source' dialog box is shown. It has a 'Steps' pane on the left with five steps: '1. Select Host', '2. Select Data Source Type', '3. Select Data Source', '4. Configure Ingest', and '5. Add Data Source' (selected). The main area is titled 'Add Data Source' and contains the following text and elements:

- Processing data source and adding it to a local database. File analysis will start when this finishes.
- A progress bar showing approximately 25% completion.
- A 'Status' label above a text box.
- A note: *This process may take some time for large data sources.

At the bottom are buttons: '< Back', 'Next >', 'Finish', 'Cancel', and 'Help'.



Successfully added the data source and loaded it onto Autopsy.

Step 2: Identify Image Files

<div> Add Data Source Images/Videos Communications Geolocation Timeline Discovery </div>								
<div> <div>Directory Tree</div> <div>Listing</div> </div>								
XIF Metadata								
<div> <div>Table</div> <div>Thumbnail</div> <div>Summary</div> </div>								
Source Name	S	C	O	Source Type	Score	Conclusion	Configuration	Justification
Odessey11.txt				File	Not Notable			
_MG_1345.jpg				File	Not Notable			
_RBATNM9.jpg				File	Not Notable			
_R2WHGRN.txt				File	Not Notable			
f0006352.jpg			0	File	Not Notable			

<										
Data Content										
Hex	Text	Application	File Metadata	OS Account	Data Artifacts	Analysis Results	Context	Annotations	Other Occu	
Page: 1 of 2	Page			Go to Page: 1	Jump to Offset				Launch in	
0x00000000:	FF D8 FF E0	00 10 4A 46	49 46 00 01	01 01 00 78JFIF.....x					
0x00000010:	00 78 00 00	FF E1 03 1C	45 78 69 66	00 00 49 49	.x.....Exif..II					
0x00000020:	2A 00 08 00	00 00 0B 00	0E 01 02 00	0A 00 00 00	*.....					
0x00000030:	92 00 00 00	0F 01 02 00	12 00 00 00	9C 00 00 00					
0x00000040:	10 01 02 00	12 00 00 00	AE 00 00 00	12 01 03 00					
0x00000050:	01 00 00 00	01 00 00 00	1A 01 05 00	01 00 00 00					
0x00000060:	C0 00 00 00	1B 01 05 00	01 00 00 00	C8 00 00 00					
0x00000070:	28 01 03 00	01 00 00 00	02 00 97 02	31 01 02 00	(.....1...					
0x00000080:	0A 00 00 00	D0 00 00 00	32 01 02 00	14 00 00 002.....					
0x00000090:	DA 00 00 00	13 02 03 00	01 00 00 00	02 00 97 02					
0x000000a0:	69 87 04 00	01 00 00 00	EE 00 00 00	00 00 00 00	i.....					
0x000000b0:	20 20 20 20	20 20 20 20	20 00 4D 69	6E 6F 6C 74Minolt					
0x000000c0:	61 20 43 6F	2E 2C 20 4C	74 64 20 00	44 69 6D 61a Co., Ltd .Dima					
0x000000d0:	67 65 20 32	33 33 30 20	5A 6F 6F 6D	20 00 48	File Explorer 330 Zoom .H.					

Successfully analyzed suspicious txt file that actually has a different file extension.

Step 3: Find Manipulated File Types

The screenshot shows a file analysis tool interface. The top section displays a list of files with columns for file name, file type, file path, creation date, modification date, and size. The files listed are:

File Name	File Type	File Path	Creation Date	Modification Date	Size
gametour2.exe	zzzz<zfif>exif minol	/img_C08InChp.dd/Vacation Pictures/gametour2.exe	2001-08-05 07:50:24 PDT	0000-00-00 00:00:00	2017-07-10
gametour3.exe	zzzz<zfif>exif minol	/img_C08InChp.dd/Vacation Pictures/gametour3.exe	2001-08-07 04:51:44 PDT	0000-00-00 00:00:00	2017-07-10
_REVVHBI.txt	le work, and on the «fifth» calypso sent him fr	/img_C08InChp.dd/\$RECYCLE.BIN/_REVVHBI.txt	2007-02-01 13:03:44 PST	0000-00-00 00:00:00	2017-07-10

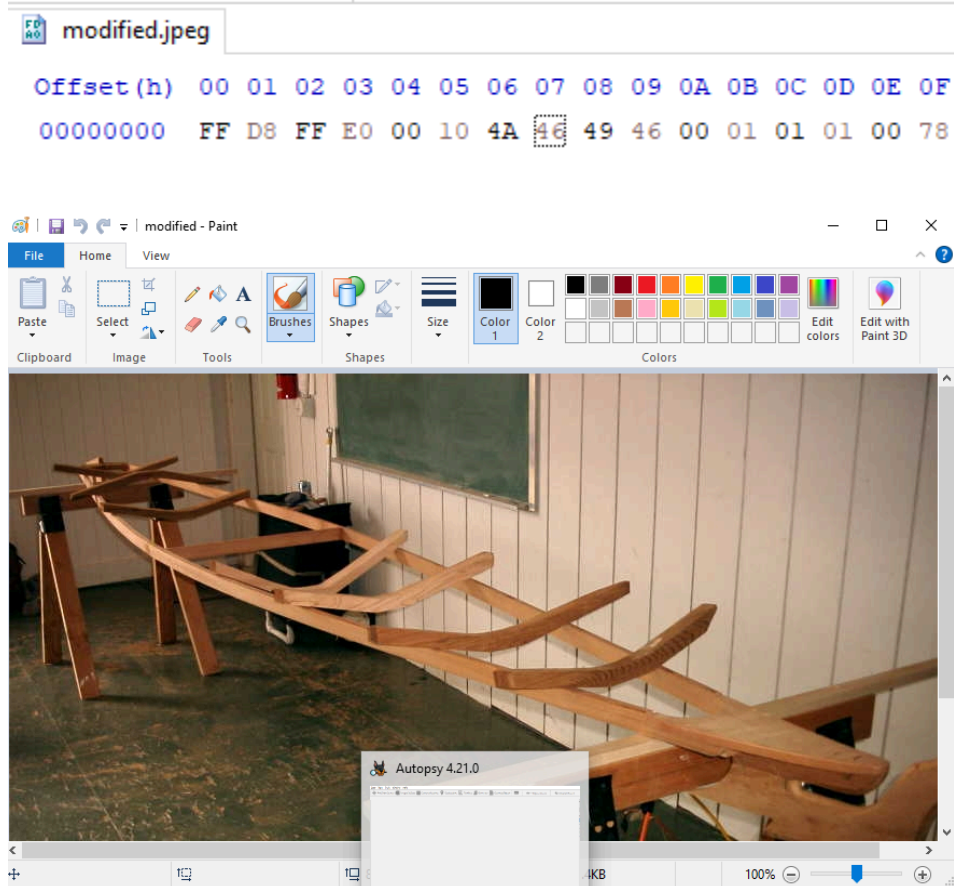
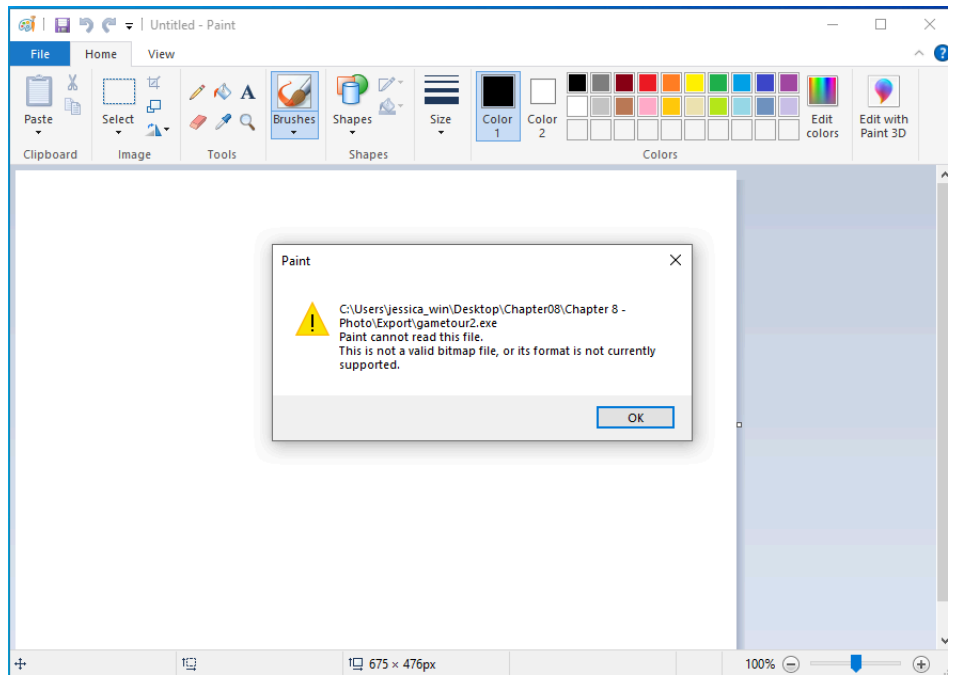
The bottom section shows a hex view of the file data. The hex data is displayed in a grid format, with the first column showing the hex value and the second column showing the corresponding ASCII characters. The hex data is:

```
0x00000000: 7A 7A 7A 7A 00 10 7A 46 49 46 00 01 01 01 00 78 zzzz...zFIF....x
0x00000010: 00 78 00 00 FF E1 03 1C 45 79 69 66 00 00 49 49 .x.....Exif...II
0x00000020: 2A 00 08 00 00 00 0B 00 0E 01 02 00 0A 00 00 00 *.....
0x00000030: 92 00 00 00 0F 01 02 00 12 00 00 00 9C 00 00 00 .....
0x00000040: 10 01 02 00 12 00 00 00 AE 00 00 00 12 01 03 00 .....
```

Below the hex view is a 'Save' dialog box. The 'Save in' field is set to 'Export'. The 'File name' field is set to 'gametour2.exe'. The 'Files of type' dropdown is set to 'All Files'. The 'Save' button is highlighted.

Successfully found more suspicious files and extracted them into the export folder of the case.

Step 4: Repair File Header



Successfully repaired header of partially lost file and viewed image.

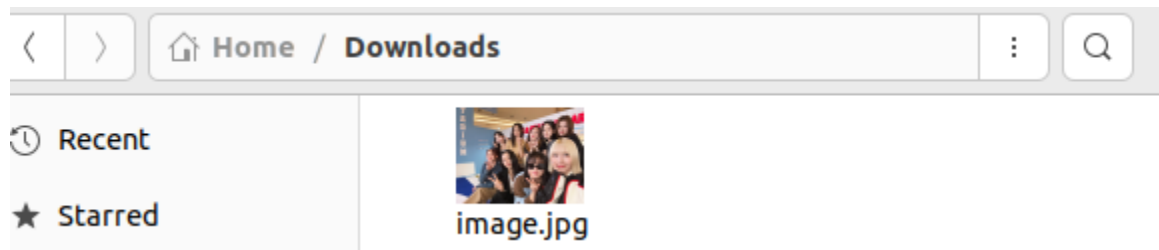
Task 2: Hide a Message

Step 1: Install Steghide

```
jessica@ubuntu:~$ sudo apt install steghide -y
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following additional packages will be installed:
  libmcrypt4
Suggested packages:
  libmcrypt-dev mcrypt
The following NEW packages will be installed:
  libmcrypt4 steghide
0 upgraded, 2 newly installed, 0 to remove and 277 not upgraded.
```

Successfully installed Steghide.

Step 2: Obtain a JPG



Downloaded an image from the internet.

Step 3: Create a Secret Message

```
jessica@ubuntu: ~
jessica@ubuntu:~$ echo "Launch Codes: 123123" > secret.txt
jessica@ubuntu:~$
```

Created a secret message and piped it into a txt file.

Step 4: Hide the Message

```
jessica@ubuntu:~$ steghide embed -ef secret.txt -cf ~/Downloads/image.jpg  
Enter passphrase:  
Re-Enter passphrase:  
embedding "secret.txt" in "/home/jessica/Downloads/image.jpg"... done  
jessica@ubuntu:~$
```



Hid the message in the jpg image.

Step 5: Extract the Secret

```
note extracted data to secret.txt.  
jessica@ubuntu:~/Downloads$ steghide extract -sf image.jpg  
Enter passphrase:  
the file "secret.txt" does already exist. overwrite ? (y/n) y  
wrote extracted data to "secret.txt".  
jessica@ubuntu:~/Downloads$ cat secret.txt  
Launch Codes: 123123  
jessica@ubuntu:~/Downloads$
```

Successfully extracted secret message from image file.