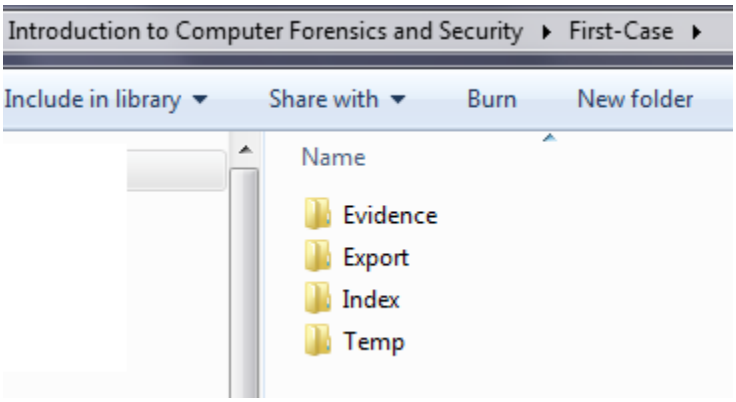
Introduction to Computer Forensics and Security – Independent Lab Work

Task 1: Creating a new case structure on EnCase V6

Objectives **Creating a new case structure**
Method Create the following folder structure on the desktop of the virtual machine; you will need to back it up to your H: drive at the end of the lab.

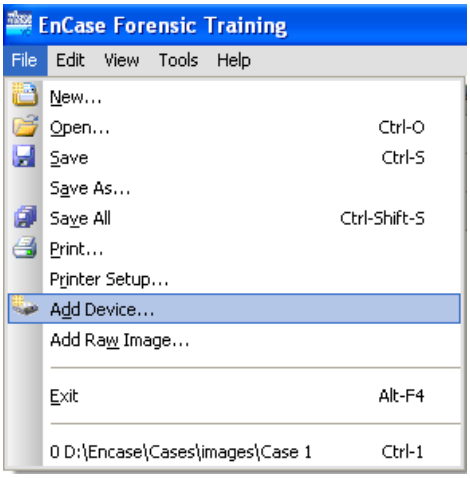


Task 2: Creating new case

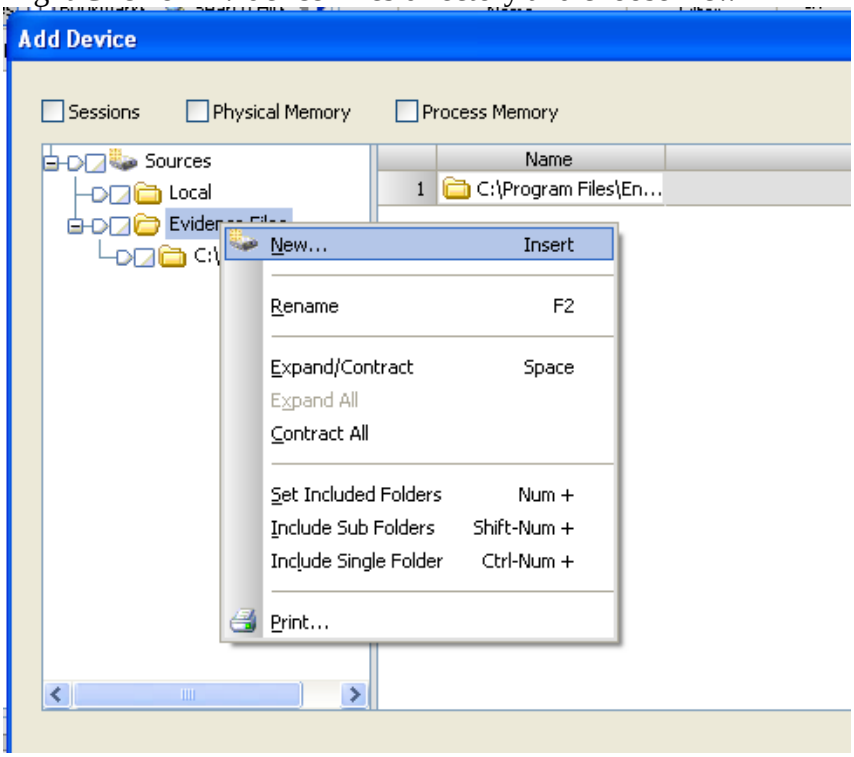
Objectives **Creating a new case**
Method Run EnCase V6 program and create a new case called First-Case.
File > New

Task 3: Adding an evidence file

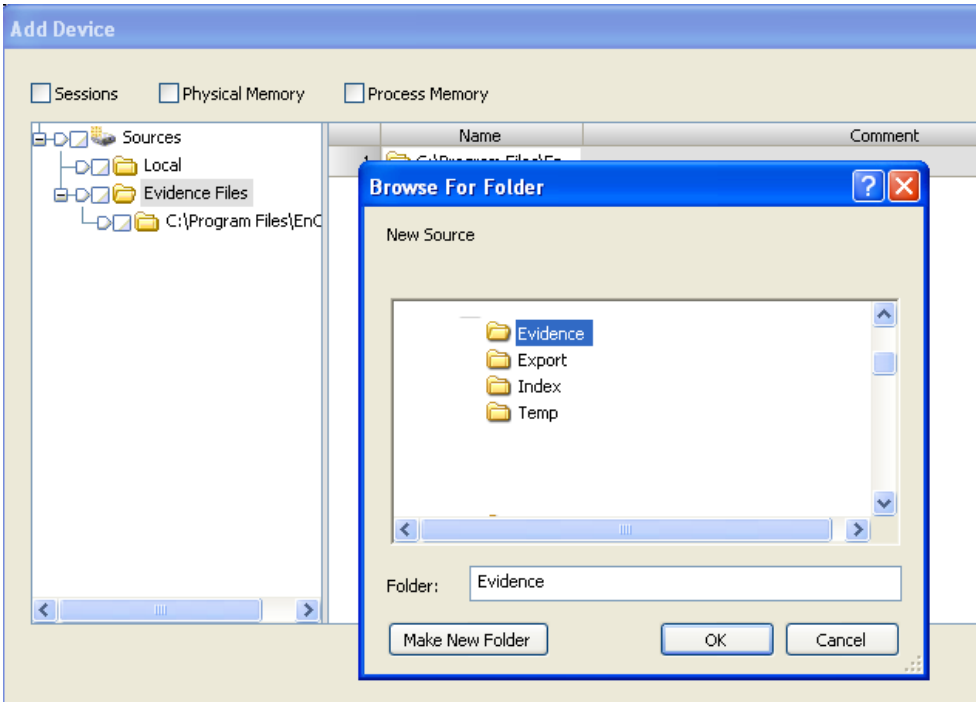
Objectives **Adding an evidence file to the created case**
Method Download the evidence file "**Lab-Forensic-Image-Intermediate-USB32.E01**" from Moodle; located under week 1. Save the file under the sub folder **First-Case > Evidence>.** Follow the screenshots in order to add the evidence file to the case.
File > Add Device



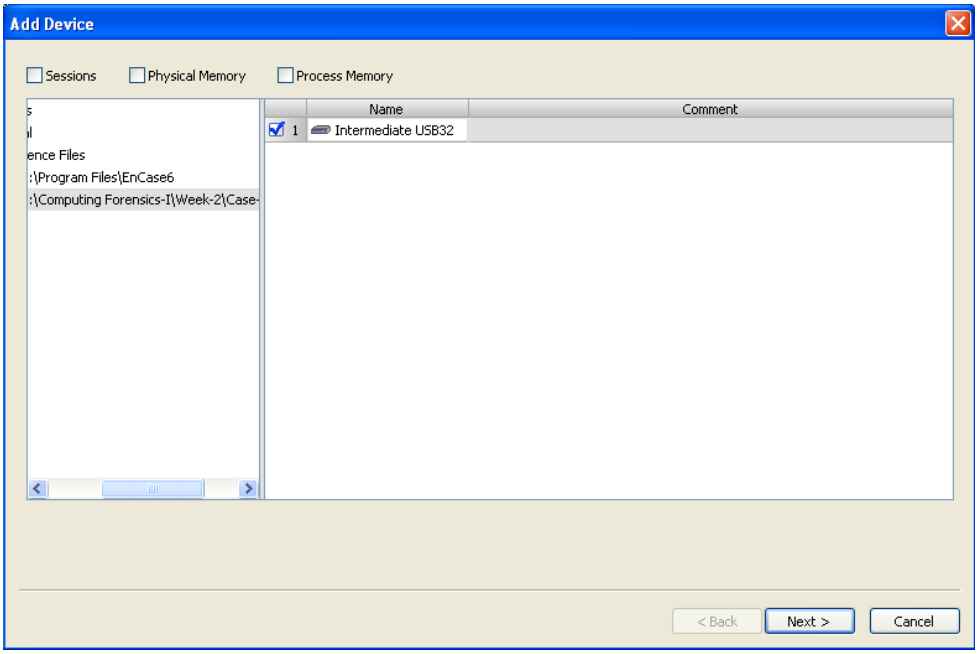
Right Click on **Evidence Files** directory and choose **New**



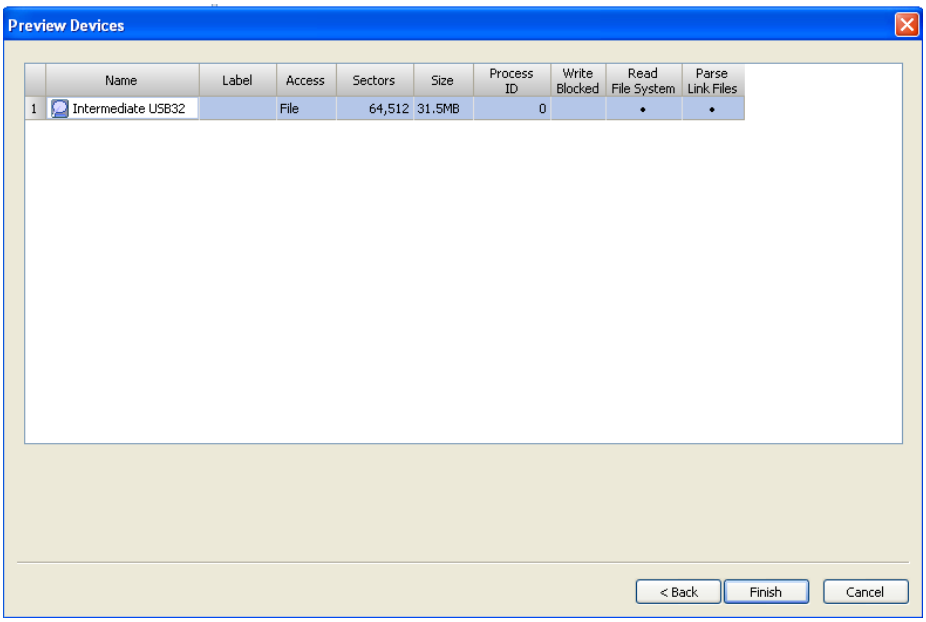
Navigate the directory structure to arrive at **\First-Case\Evidence** and



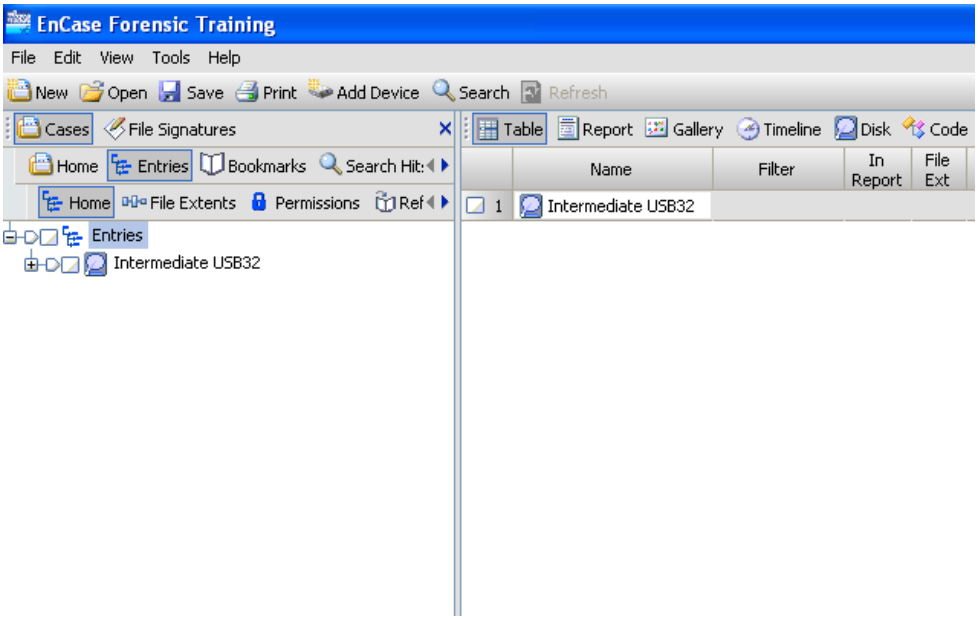
Select **Intermediate USB 32** and press **Next** and then **Next.**



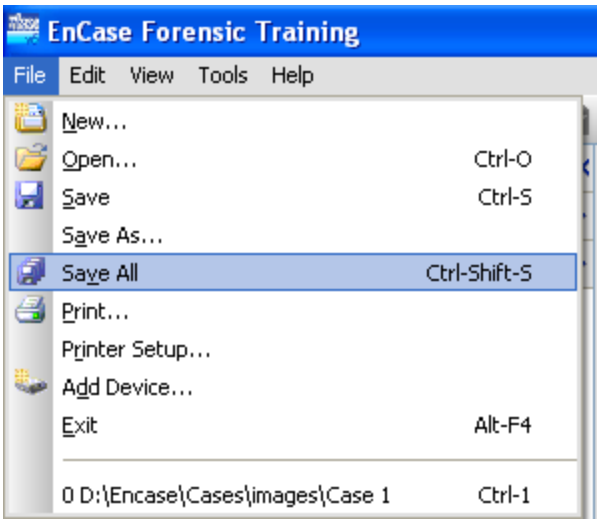
Click on **Finish**



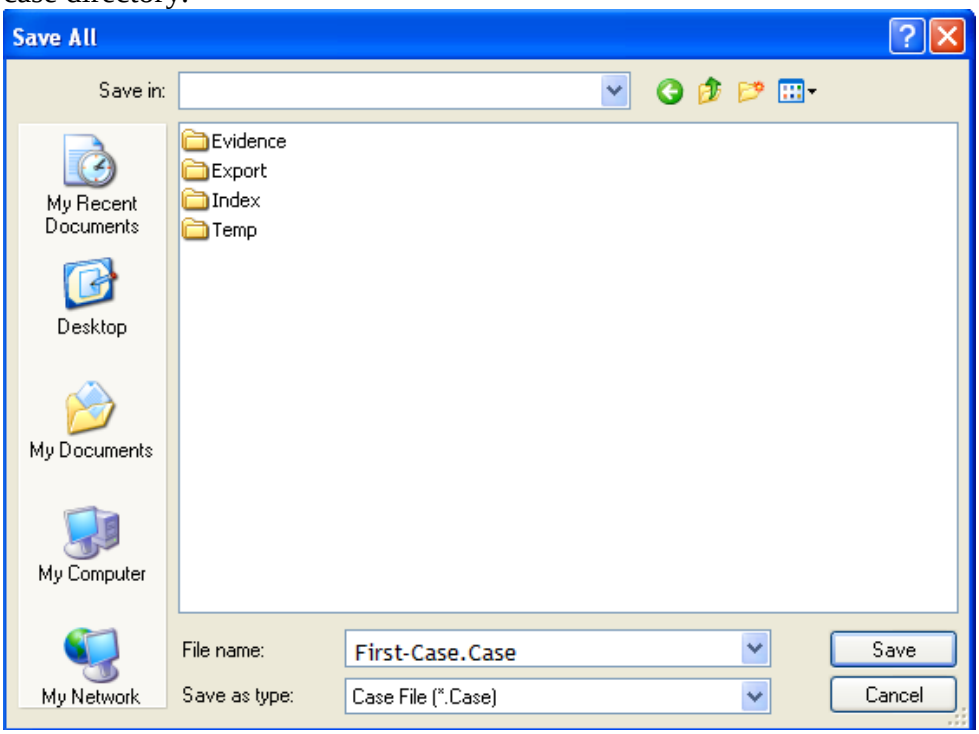
Once your evidence file has been added to the case, you can see it from the tree pane.



Go to **File > Save All**



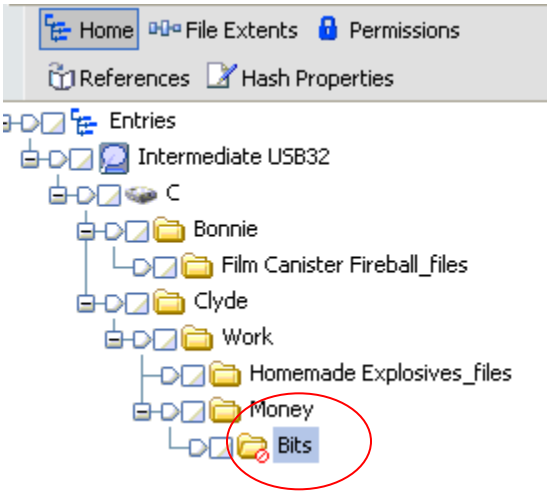
Navigate to your case directory and save the file **First-Case.Case** in the case directory.



Note: You can notice a new file (First-Case.Case) created in the case directory.

Task 4: Explore the tree pane

Objectives **Explore the tree pane to find the deleted folder**
Method Navigate the evidence file using the tree pane and find the deleted folder.



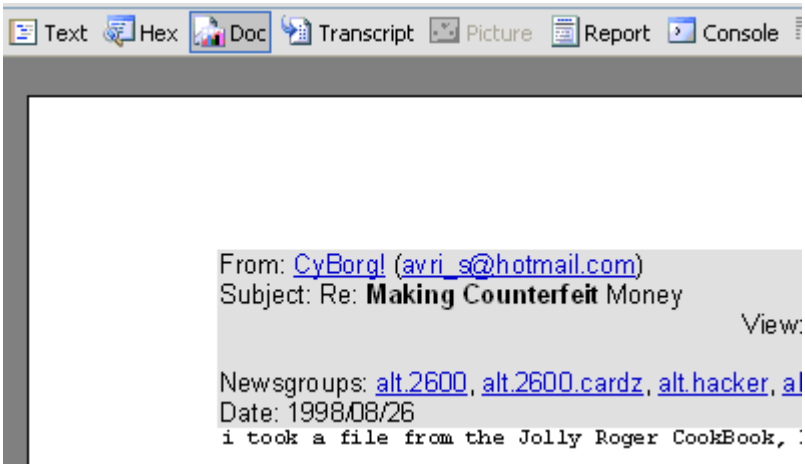
Task 5: Explore the tree pane and table pane

Objectives **Explore the tree pane and table pane to find an image file.**
Method Navigate the evidence file using the tree pane and table pane to find new100back.JPG image and use the view pane to view the image as a picture using the picture tab.

Task 6: Explore the tree pane and table pane

Objectives **Explore the tree pane and table pane to find a Document file.**

Method Navigate the evidence file using the tree pane and table pane to find the MS Word document Currency.doc and use the view pane to view the document using the Doc tab.



Task 7: Record MAC Times

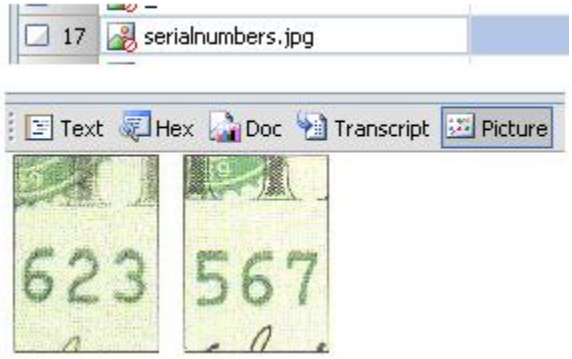
Objectives **Record the MAC times for new100back.JPG**

Method Find the picture called new100back.JPG and record MAC times.

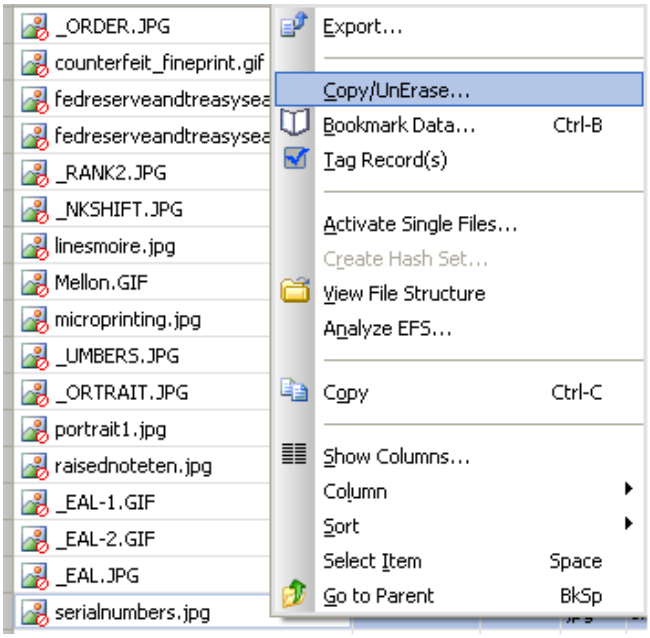
Modified:
Last Accessed :
Created:

Task 8: Recover Deleted Picture

Objectives **Recover deleted picture using EnCase**
Method Find the deleted picture called **serialnumbers.jpg** and right click on it,



Click on **Copy/UnErase** to export the picture from the evidence file. Follow the options **Highlighted File > Logical File Only**. Notice the default export folder.



Task 9: Perform a quick exploration of the evidence file provided and list two potential crimes, ----------

Task 10: Opening Encase 7 Environment

Task 11: Explore the functionalities of menus and sub menus, using page 2 in the EnCase V7 handout.

Task 12: Creating a new case, using pages 3 to 8 from the EnCase handout

Task 13: Configuring EnCase environment, using pages 11 to 18 from the EnCase handout.

Task 14: Adding an evidence file, using pages 18 to 21

Task 15: Explore the different panes (tree pane, table pane, and view pane), using pages 23 to 37

Task 16: Explore the status bar

Task 17: Explore the Dixon Box, the Selection and the Set Include functionalities

Task 18: Perform tasks 3 to 9 using EnCase V7.