|  |  |
| --- | --- |
| **Digital Forensics**  Diploma in CSF/IT  Year 2/3 (2022/23) Semester 4/6 | Week 1 |
| Practical 2 |
| **Acquiring Digital Evidence** | |

**OBJECTIVES**

1. To be able to create an Evidence file from a USB Thumb Drive.
2. To learn to acquire evidence file using the hardware forensic tool (Write-Blocker) & software forensic tool (FastBloc® SE)

**Activity A: Creating Evidence Files from USB Thumb Drive (Write Blocker)**

One of the most vital steps in the digital forensics process is the acquisition process. An evidence file can be created from any type of media that the computer system recognizes. Similar procedures are used to image various types of media.

Before inserting a thumb drive into a USB port, perform the following:

* Write protect the thumb drive or portable HDD. *Your tutor will show you how this is carried out using the* ***Tableau T8-R2 Write-Blocker****.*

Create a new case in EnCase. Name it as Thumb Drive.

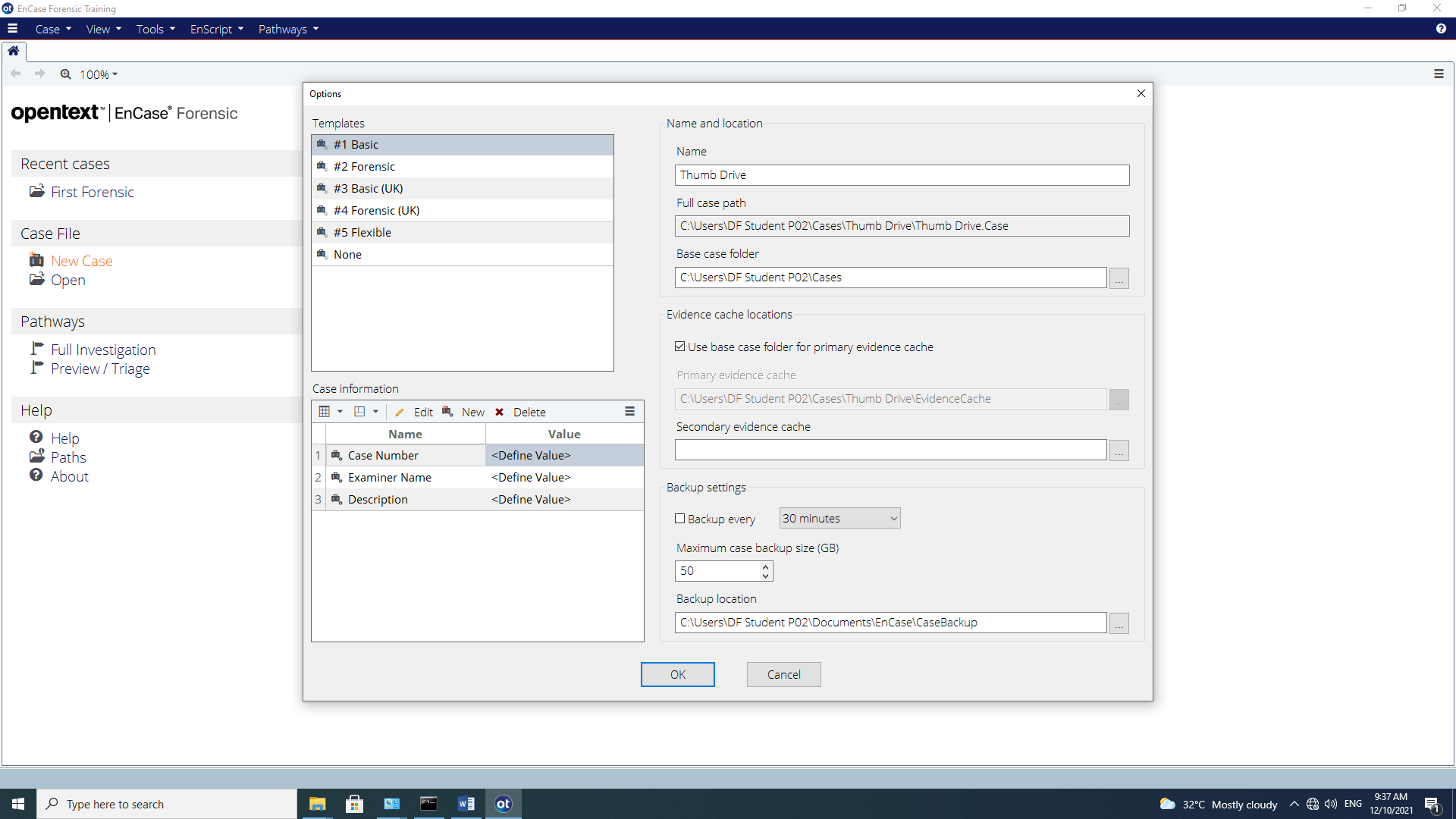


Figure A-1: Creating a new Case

***Note: You may like to refer to the Week 2 Practical 1 worksheet for detail steps.***

Click **Add Evidence** to find the evidentiary thumb drive and then **Add Local Device**:

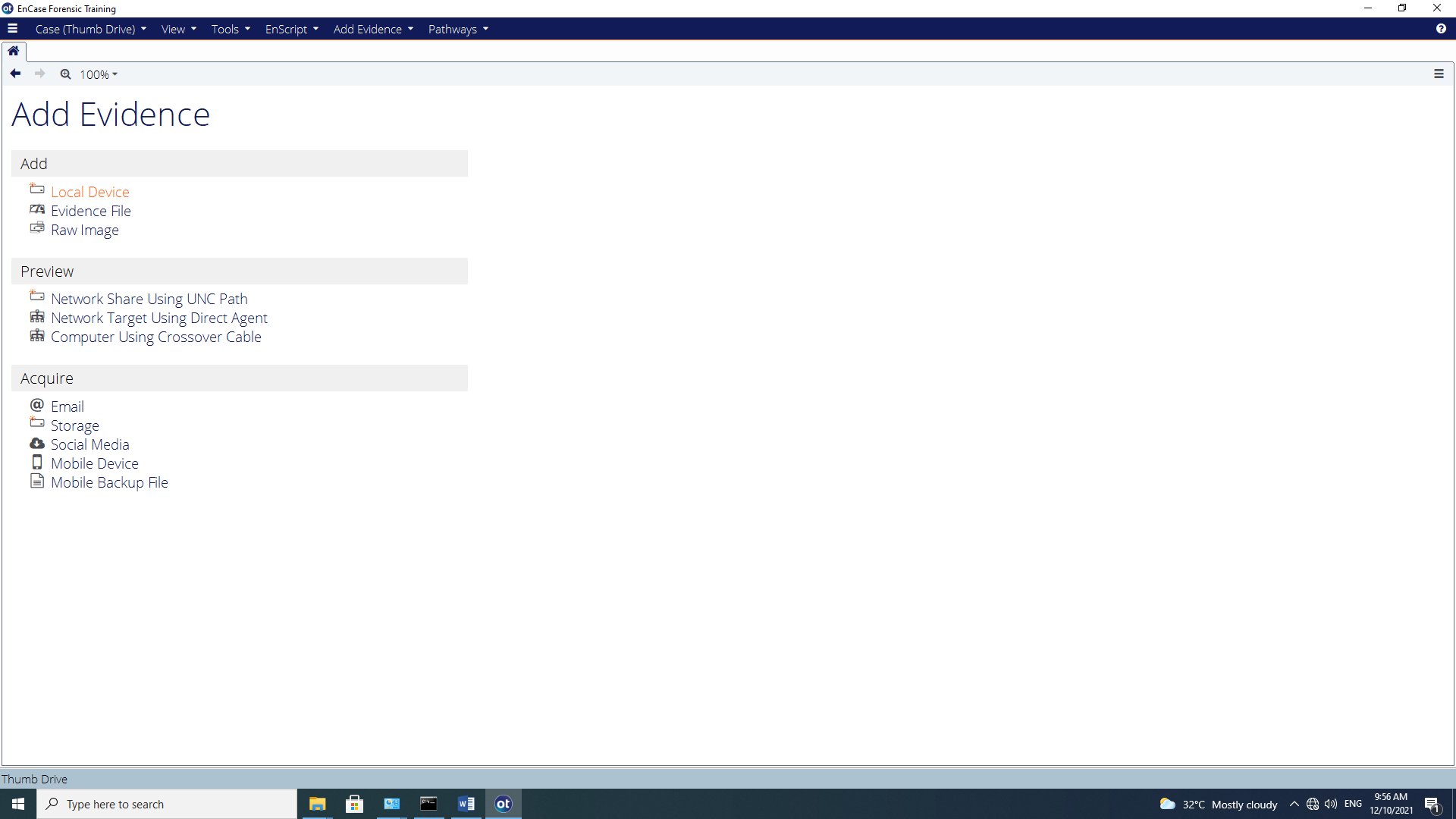


Figure A-2: Selecting Local Device

The following display will appear. Select (Blue Check) ‘Detect Tableau Hardware’ and click **Next.**

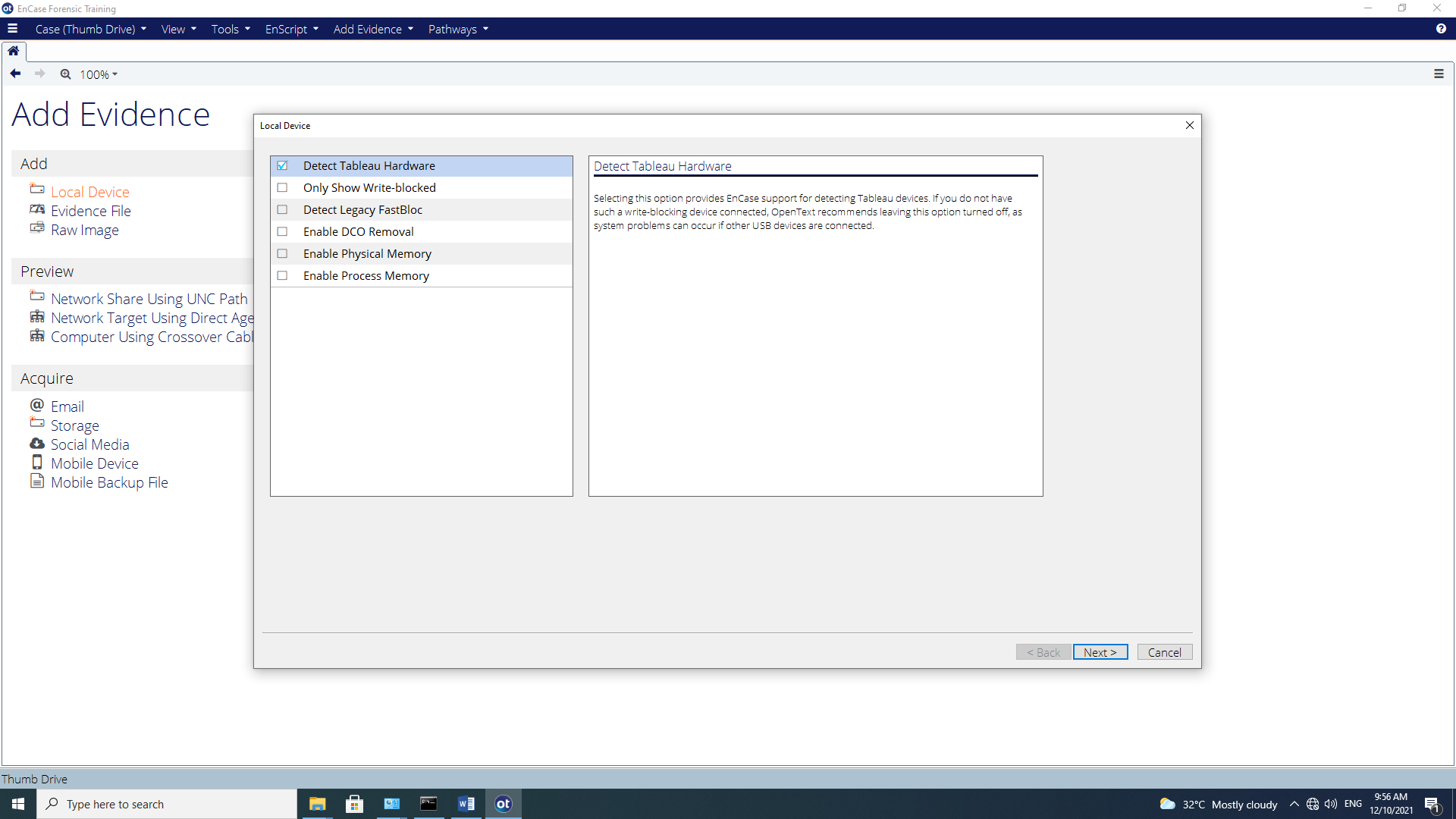


Figure A-3: Add Local Device

The local drive will be displayed as shown in the following dialog box. Put a check in the checkbox next to the drive letter associated with the USB device (Sony Storage) that is being write-blocked.

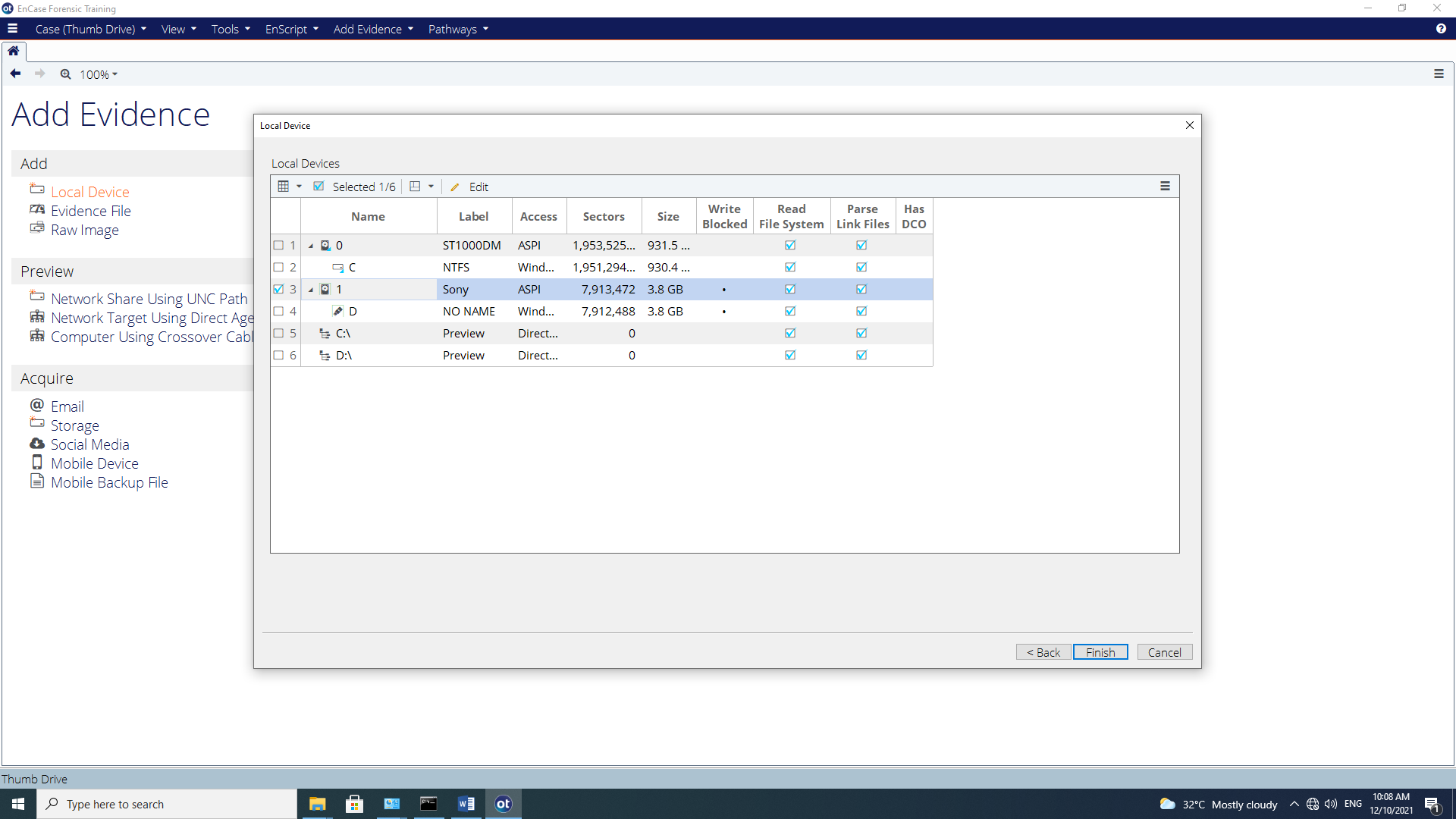


Figure A-4: Selecting the Thumb Drive

You will know which physical and logical drives are currently being write-blocked by the following icons:

|  |  |
| --- | --- |
|  | Drives that are write-blocked are indicated by the normal icon for the selected media surrounded by a green square. |

You should also see a column - “Write Blocked”. For those devices that are write-blocked, it is indicated by a black dot in that column.

Q1: What do you understand about “write-blocking”? Why is this important in forensic investigation?

Click OK. This will load the attached Thumb Drive to the Evidence view. Blue Check the physical drive entry and double-click the entry (or select **Open** to load into the Entry view.)

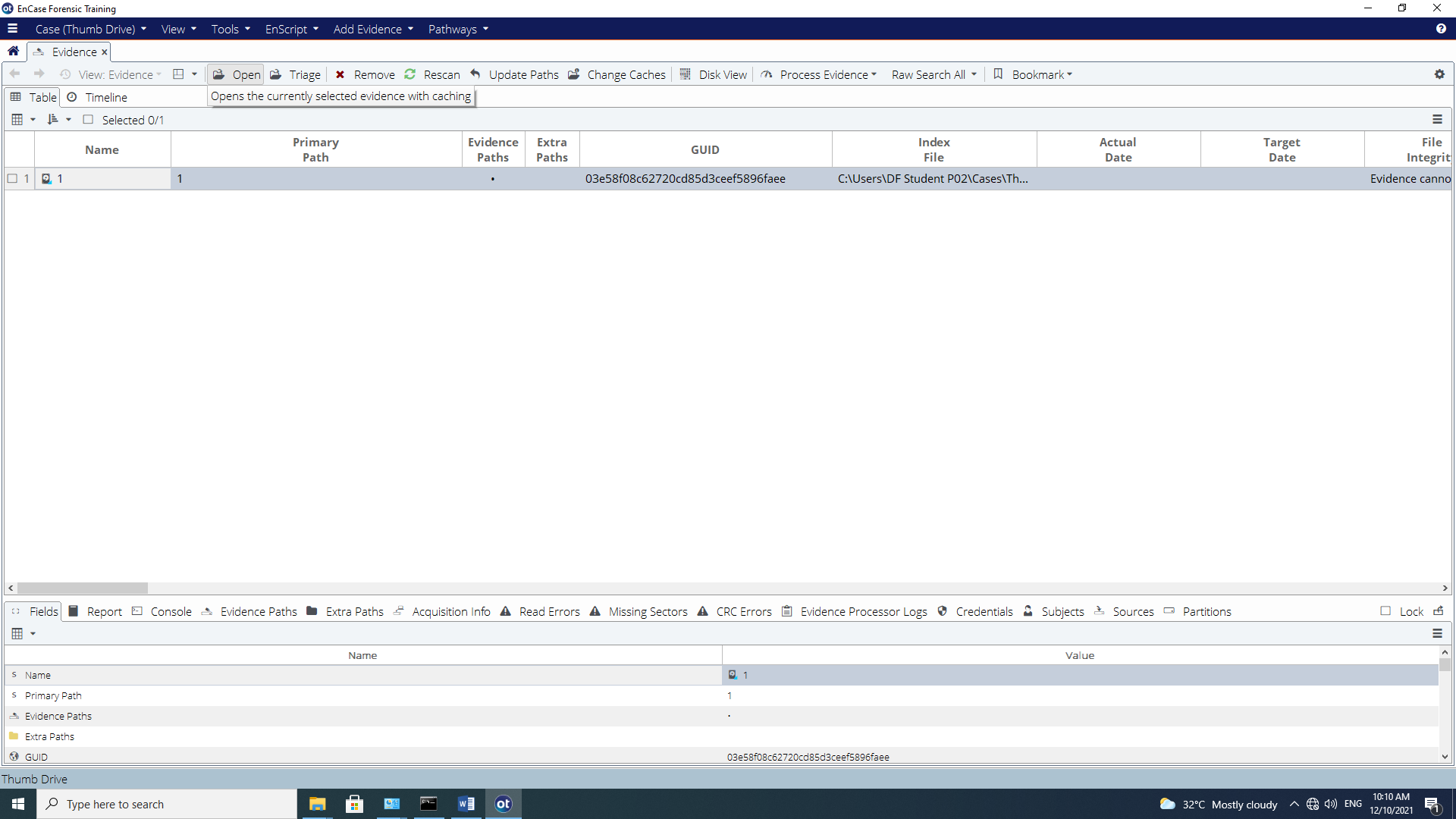


Figure A-5: Opening an evidence item to view as an entry

At the Entry view, you can navigate and view the structure of our evidentiary thumb drive. To make a forensic working image of this thumb drive, right click on the thumb drive and select the **Acquire Menu** and the **Acquire**… option.

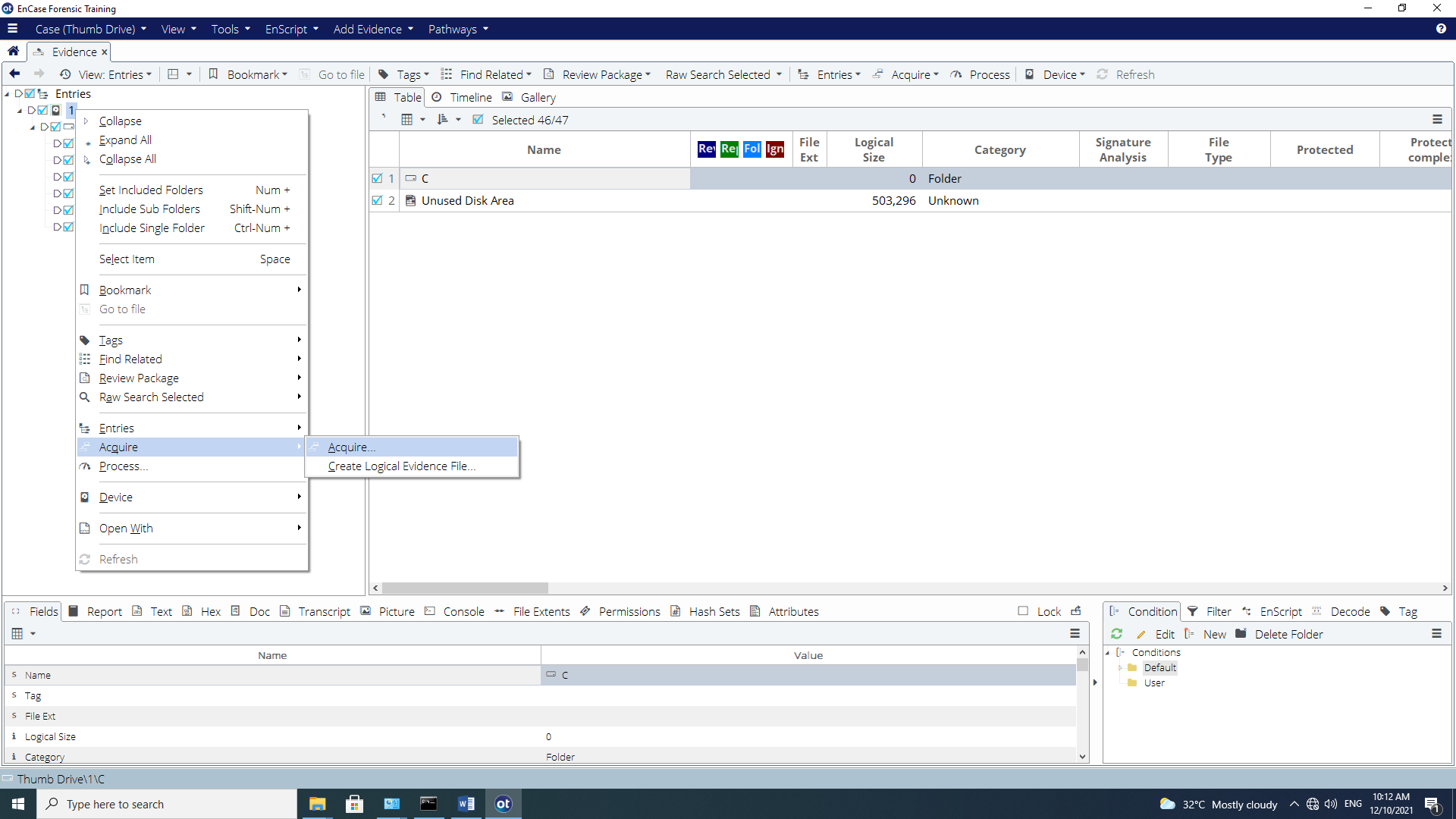


Figure A-6: Starting an acquisition of thumb drive

Upon selecting Acquire, an Acquire Device Thumb Drive window is displayed with several available options. Several tabs are available within the Acquire Device window, allowing examiner to define desired acquisition options.

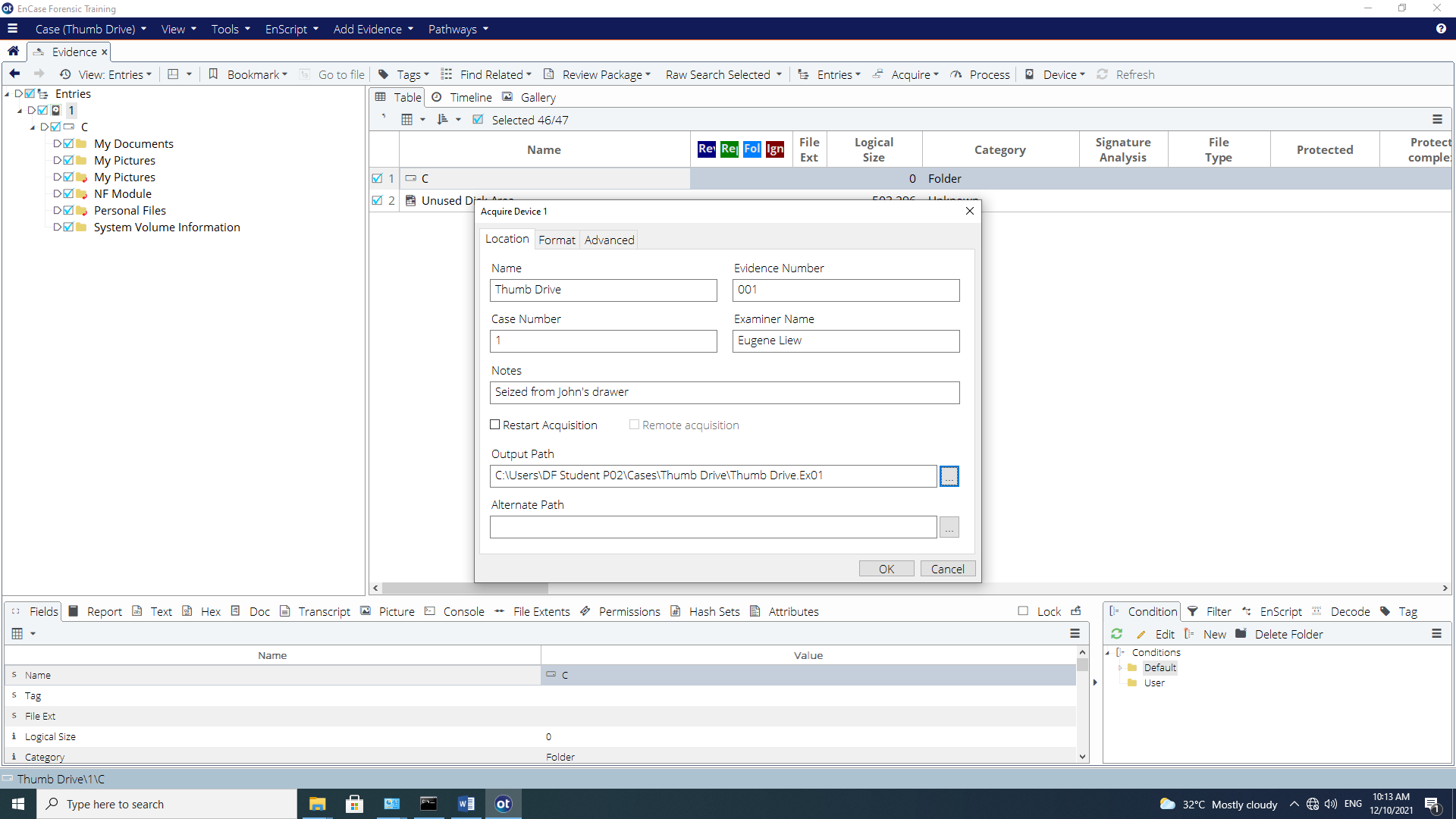


Figure A-7: Acquire Device Window (Acquisition information and options)

At the Location tab, enter the necessary acquisition information. You Do Not need to select Restart Acquisition (This allows the examiner to restart a prior acquisition process).

Click the **Format** tab:

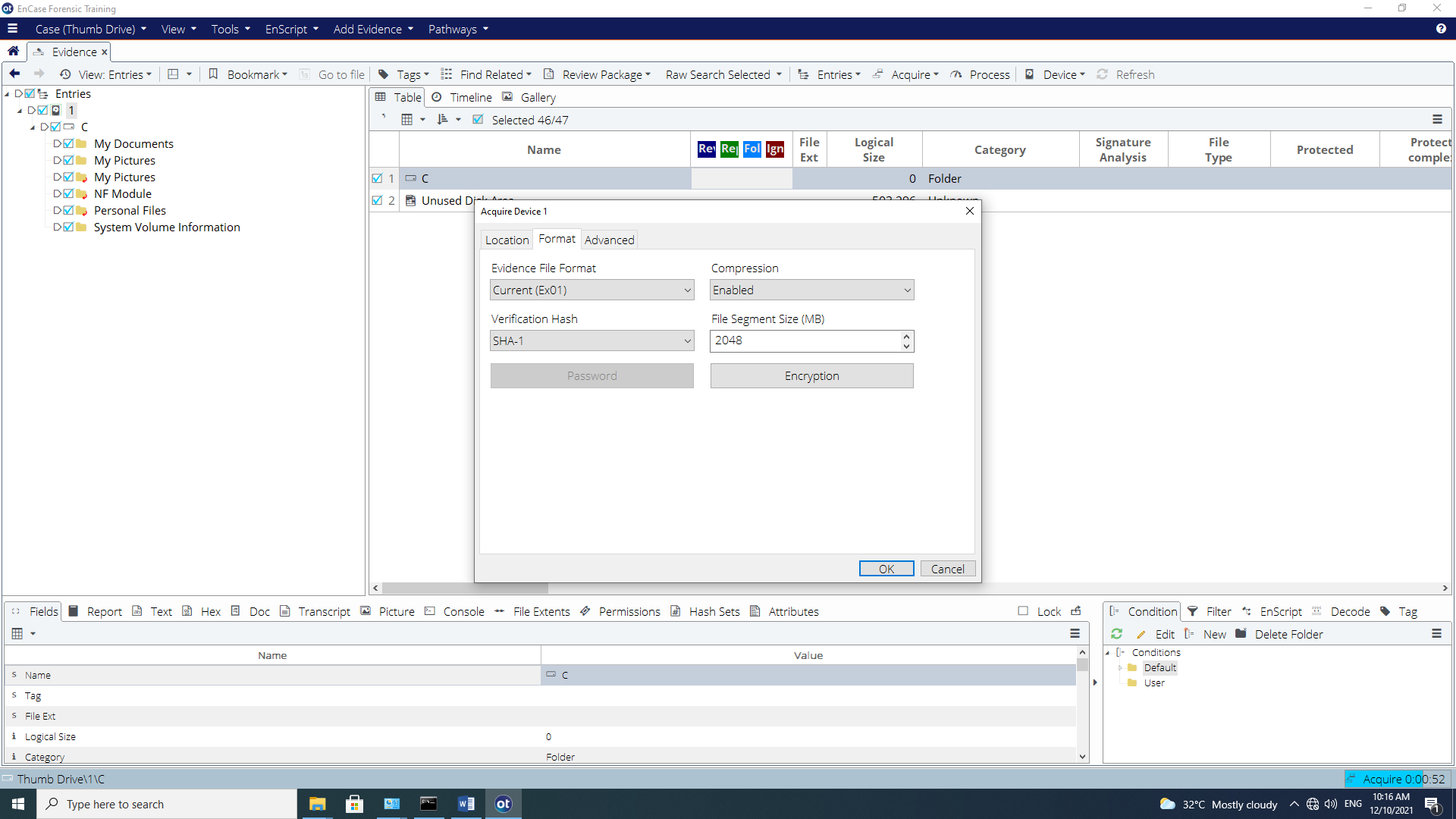


Figure A-8: Acquisition format and options

Another Options dialog box will appear with the followings:

* Evidence File Format – There are two choices: Current (Ex01) or Legacy (E01). The chosen option determines the evidence file format and alters the extension of the filename in the Location tab.
* Compression – The level of compression has no effect on the evidence, but may affect the amount of time that it takes to acquire the evidence file.
* Verification Hash – Generate an MD5 hash or SHA1 hash.
* File Segment size – This is for storage and archiving purposes (the default is 2048 MB). As far as EnCase is concerned, the minimum file segment size is 30MB and the theoretical maximum file segment sizeis 8,796,093,018,112 MB.
* Password – If the evidence file is to be protected from unauthorized use, enter a password. *Do not use this feature if there is a chance the password will be forgotten. There is no simple way to recover a forgotten password.*  A password can be applied to the .Ex01 format through the Encryption button. This creates a symmetric key to encrypt the evidence file contents.
* Encryption – This only applies if the examiner selects the current (Ex01) evidence file format. The encryption option allows for the assignment of a password. It also requires the use of asymmetric public/private encryption keys, which are used to encrypt the contents of the evidence file. These keys can be created or chosen from existing keys.

{Tutor’s note: those in RED is not given to students and it is for your reference}

Q2: Explain why it is necessary to generate MD5 and/or SHA1 hash of disk acquired.

Q3: Explain the key differences between MD5 and SHA1.

Q4: Briefly explain how asymmetric encryption work?

At the Verification Hash option, select **‘SHA1’**. Leave the rest of the fields unselected.

After all appropriate options are selected, click **OK**. When the acquisition has started, the right-bottom of the screen will show the status bar with the estimated time of acquisition.



Figure A-9: Progress of Acquisition

Immediately upon conclusion of the acquisition, Encase will begin generating a verification MD5/SHA-1 hash. (depending upon what hashing options were selected for the evidence file).



Figure A-10: Verification of Acquisition

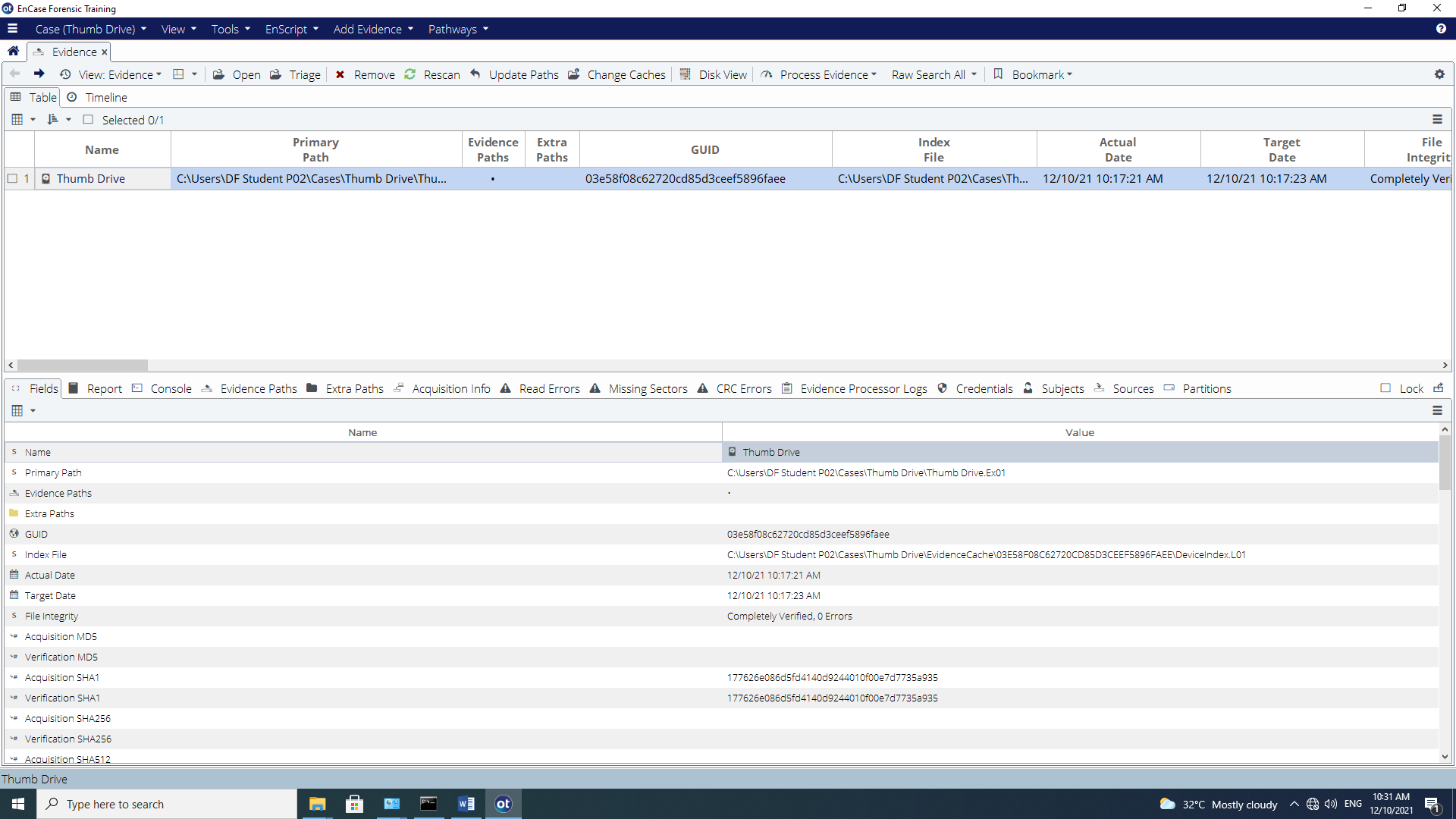


Figure A-11: Viewing file integrity and verification hash results

**Note**: When the acquisition completes, if desired, close EnCase and use the hardware removal tool in the System Tray in the lower right corner of the task bar to remove the device. Remove the device physically when a message appears confirming safe removal.

**Activity B: Creating Evidence Files from USB Thumb Drive (FastBloc® SE)**

Guidance Software includes the FastBloc SE module with EnCase. This is a software write blocker that can be applied to devices connected by USB, FireWire, or SCSI interfaces. When FastBloc SE module's write blocking capability is enabled, it ensures that no data are written to or modified on a write blocked device.

You can activate FastBloc SE with a case open within EnCase by selecting **Tools** and **FastBloc SE**.

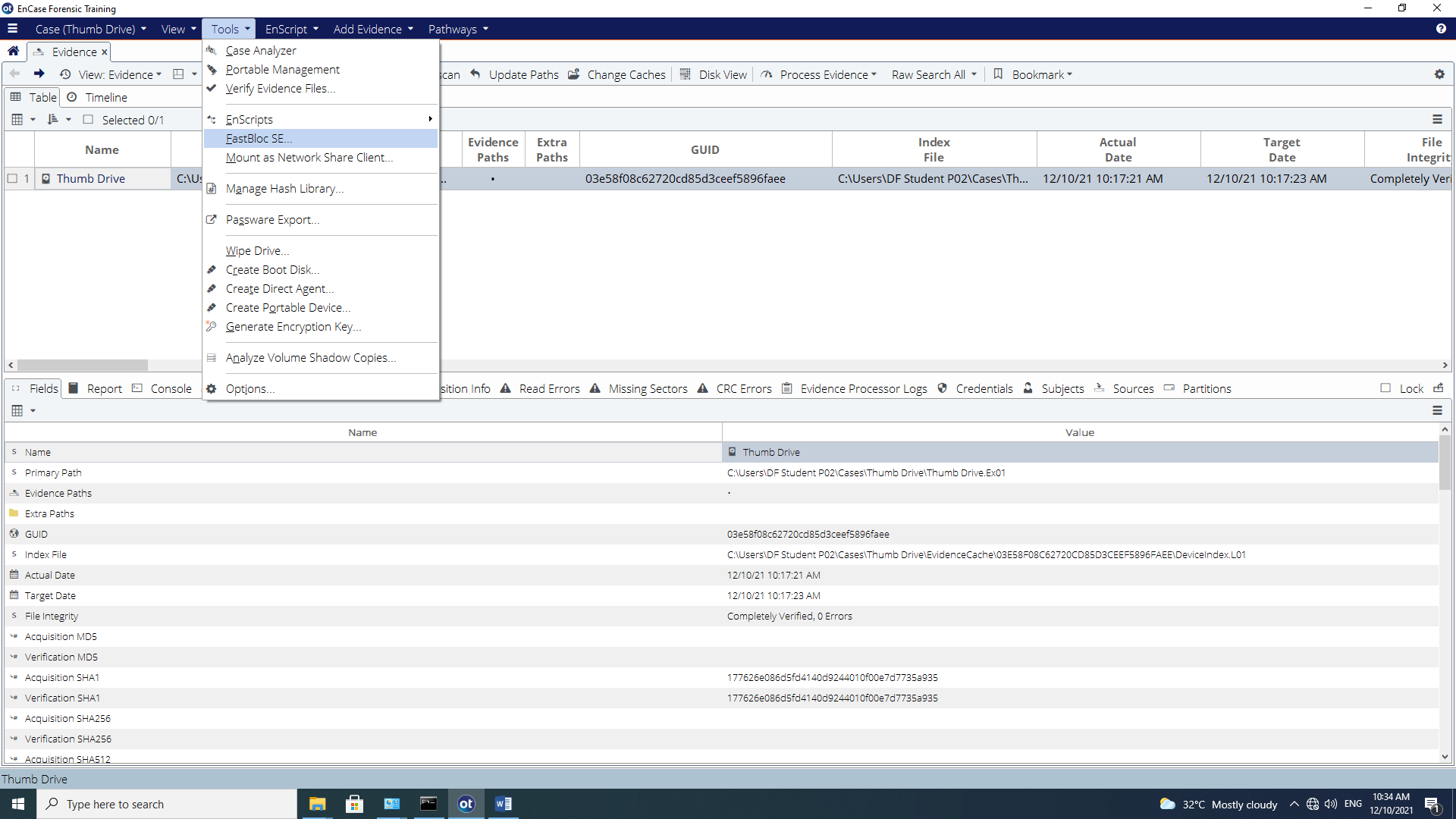


Figure B-1: FastBloc SE for Encase

Create a new case like before, and name it as Thumb Drive 1 (or you could open the previous case).

To write block a USB, FireWire, or SCSI device:

1. Make sure that the thumb drive is not attached.

2. Click Tools > FastBloc SE.

3. In the FastBloc SE dialog, select the Plug and Play tab. There are three Write-Block modes to choose.

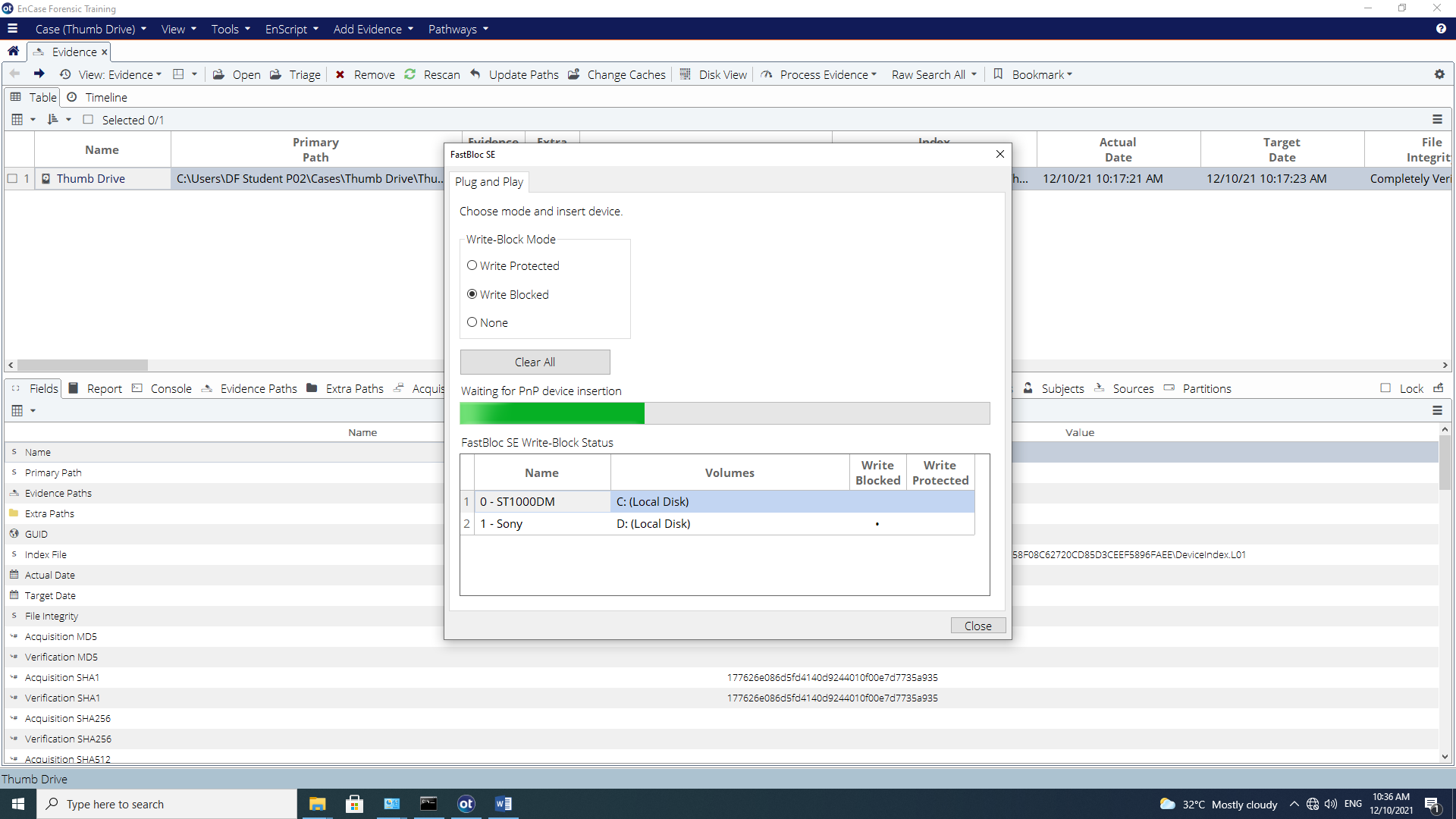


Figure B-2: Pop-Up for Write-Block mode

Q5: Briefly explain the above three mode options. (You may get some help from your tutor on this)

1. Select **Write Blocked** mode. The progress bar indicates EnCase is waiting for a device to be inserted.
2. Insert the thumb drive into the USB port. After the media is placed into the USB port and it is recognized by the operating system, a pop-up window will appear, indicating that the media is connected and the status of the device. (Please note that this may take some time for the thumb drive to be recognized).
3. After the media is detected, click **Close.**

From the Add Evidence dropdown menu, select **Add | Local Device.**

(You may need to click Home button)

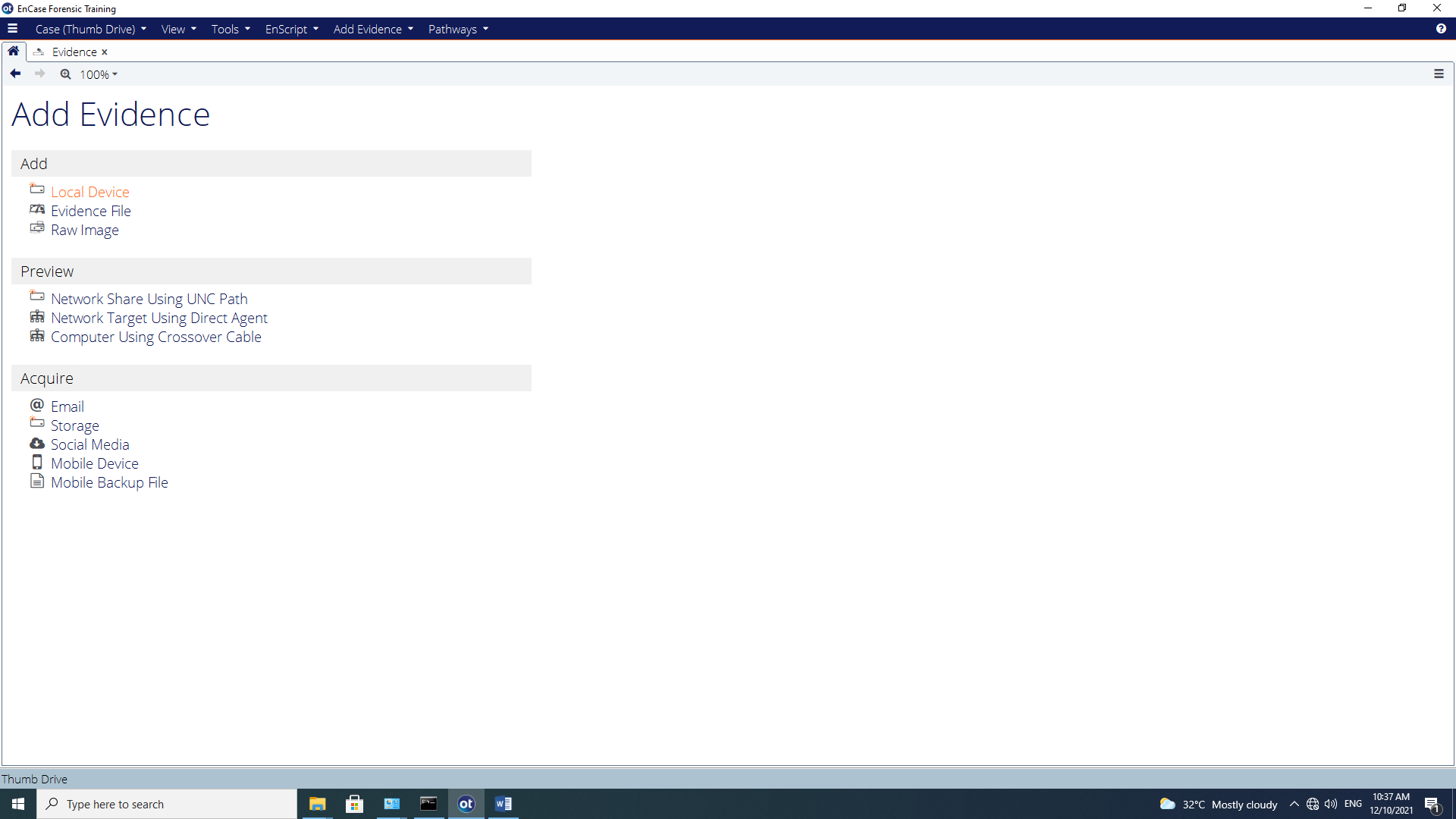


Figure B-3: Add Evidence 🡪 Add Device

Remove all blue checks and select Next.

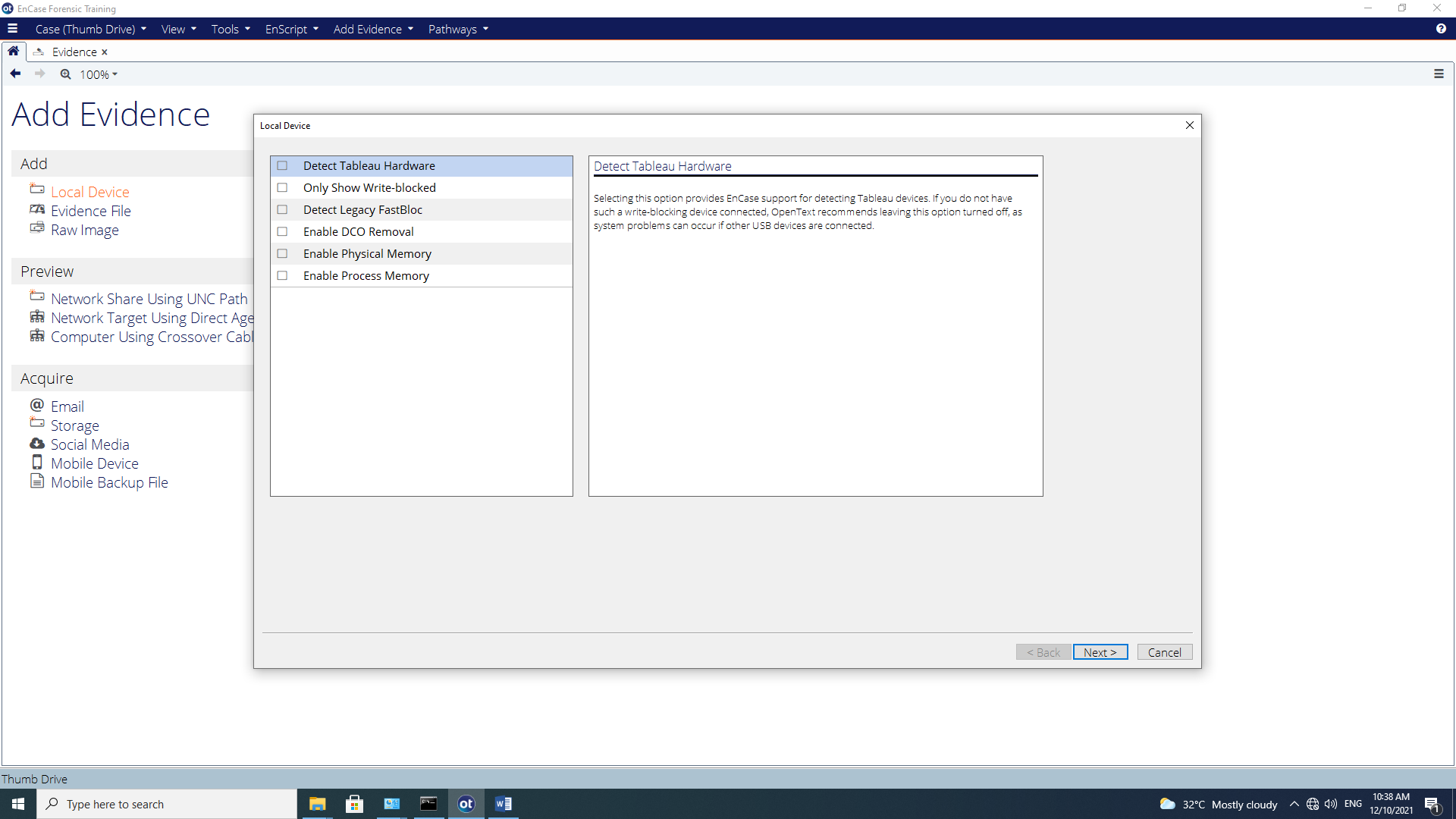


Figure B-4: Uncheck all options

Start the acquisition process as we did before…

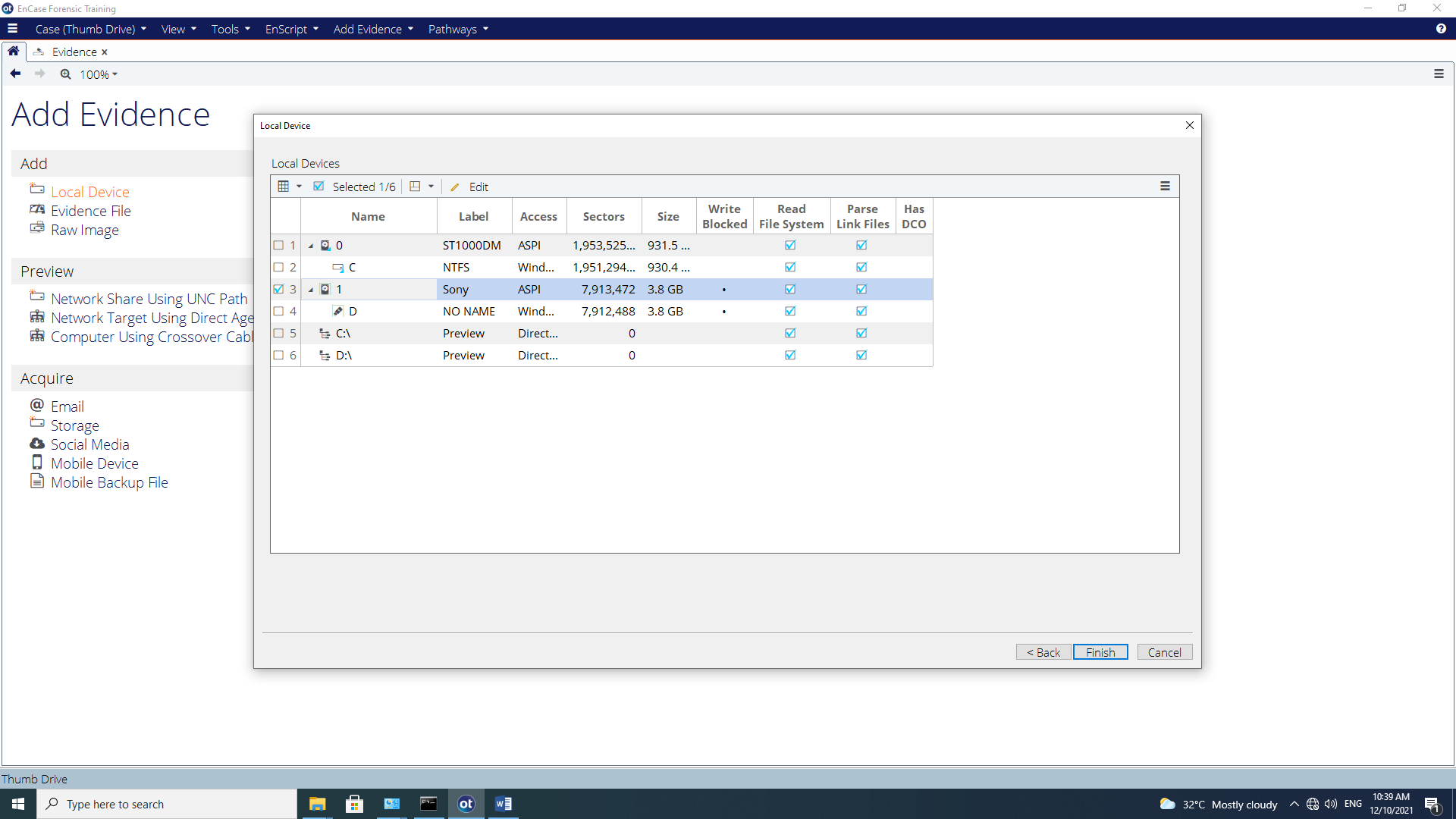


Figure B-5: Blue check Sony Thumb Drive

Select (blue check) the appropriate device. In this case, the **Sony** Thumb Drive and click Finish.

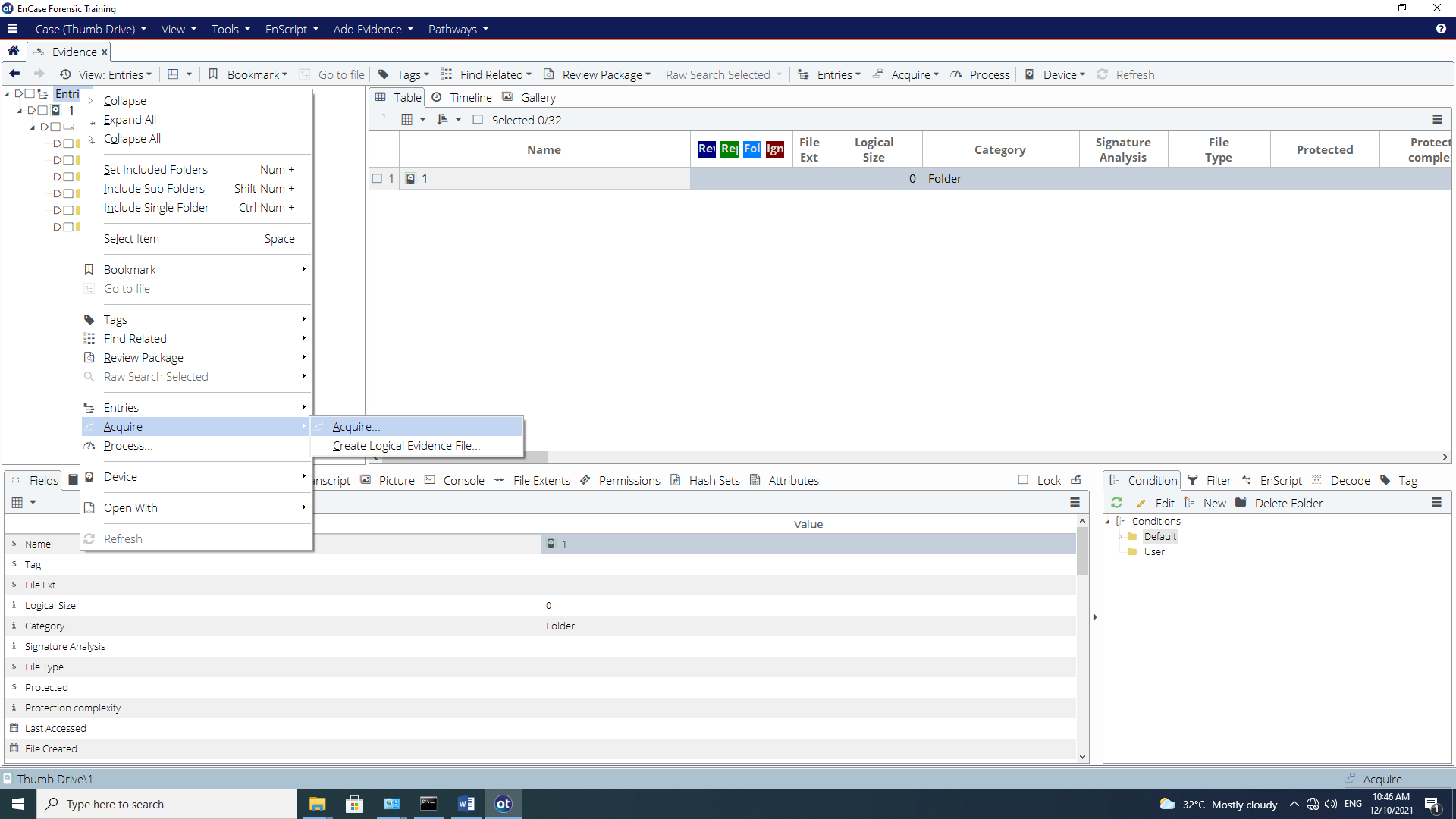


Figure B-6: Acquire Evidence

Select the newly added evidence, Click Open. In the Tree Pane, blue check the entire evidence and right click | Acquire | Acquire. Enter Name, Evidence Number, Case Number, Examiner Name, Notes and Output Path (based on your own Student’s Case Path).

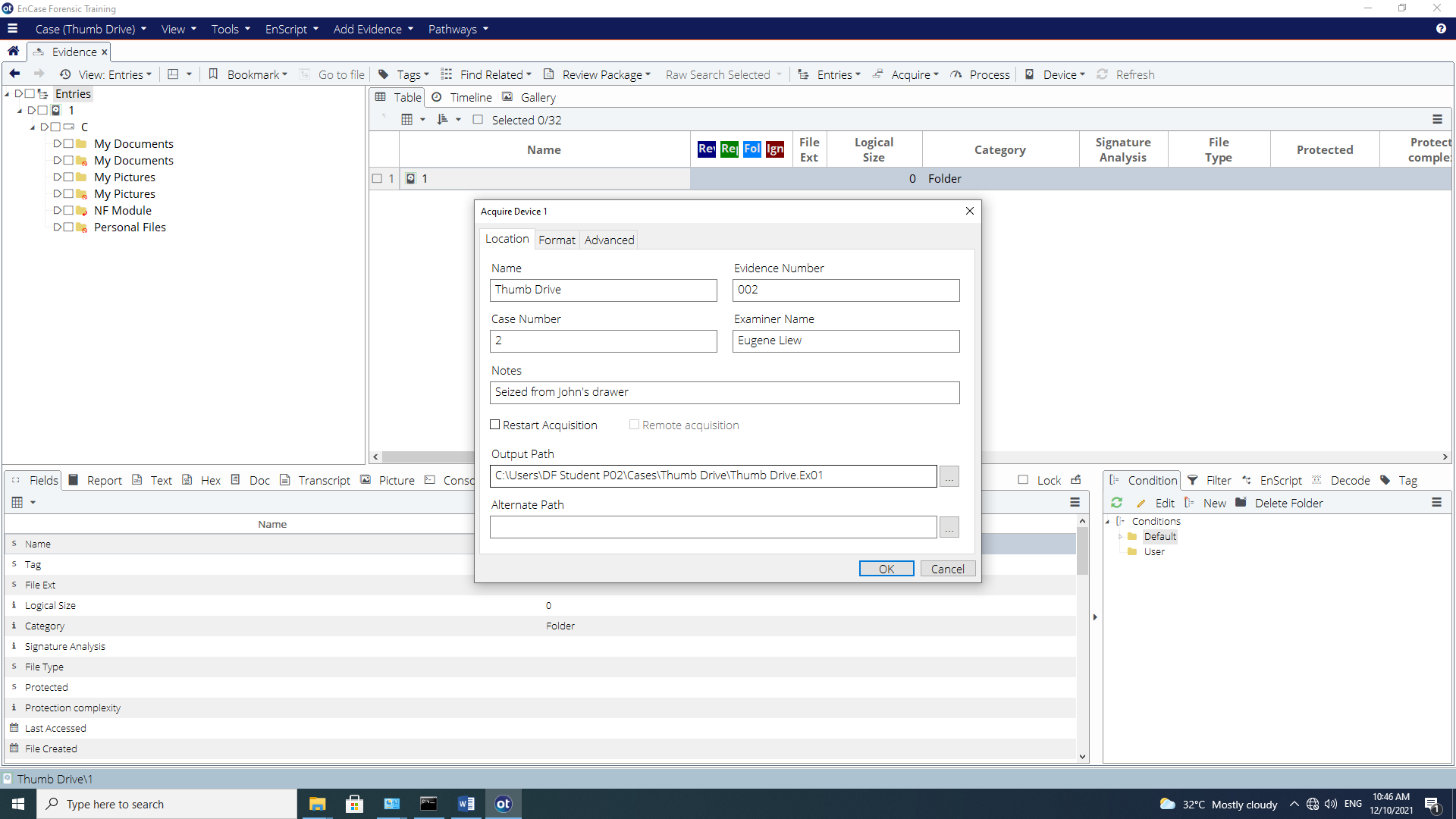


Figure B-7: Location option dialog for Acquisition

Before we proceed with the acquisition of the evidence file, let’s encrypt the evidence file. EnCase is capable of performing symmetric encryption and asymmetric encryption. This can be done by selecting the **Encryption** option in the **Format** tab.

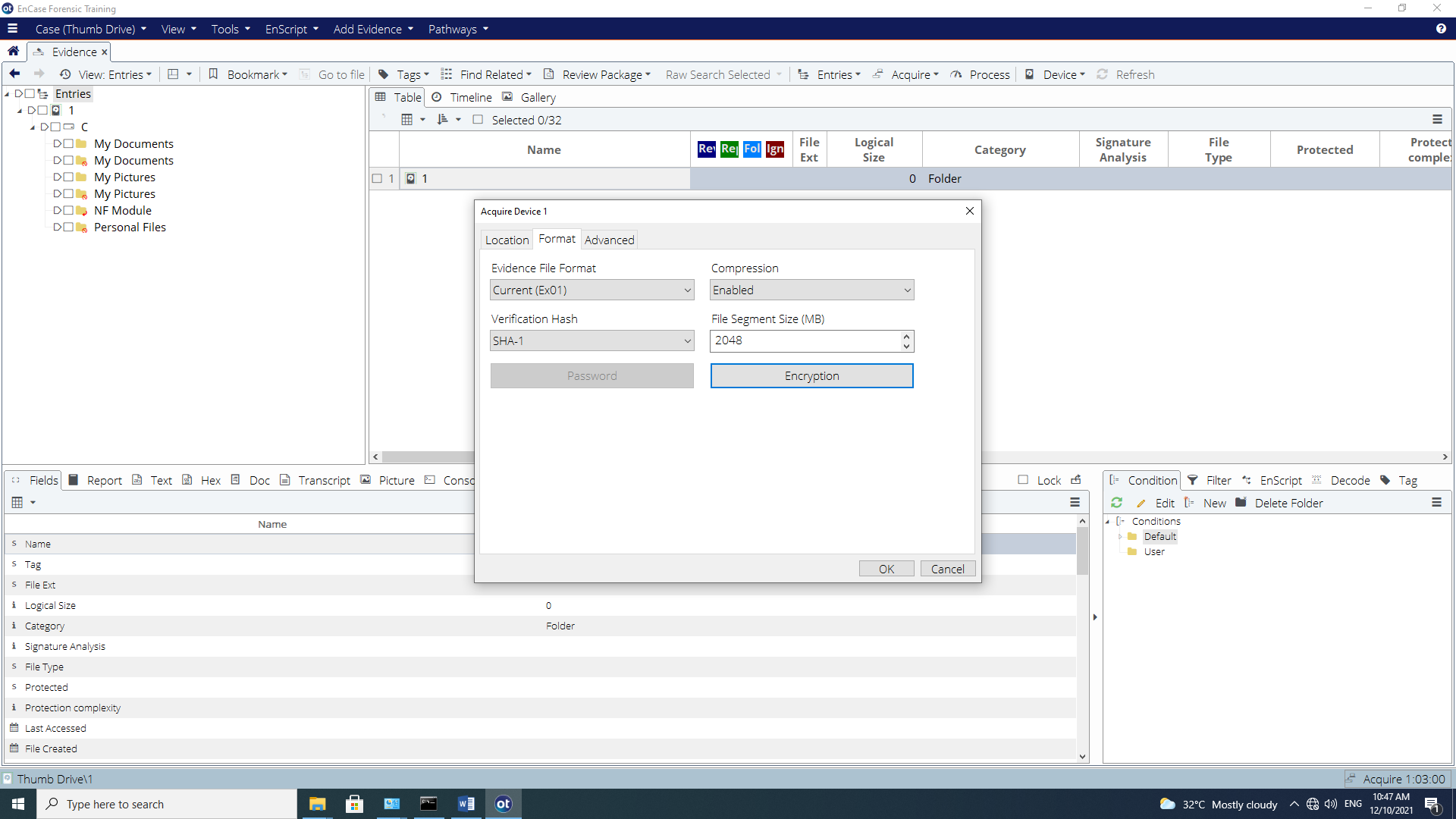


Figure B-8: Applying Encryption

The following Encryption Details window will appear.

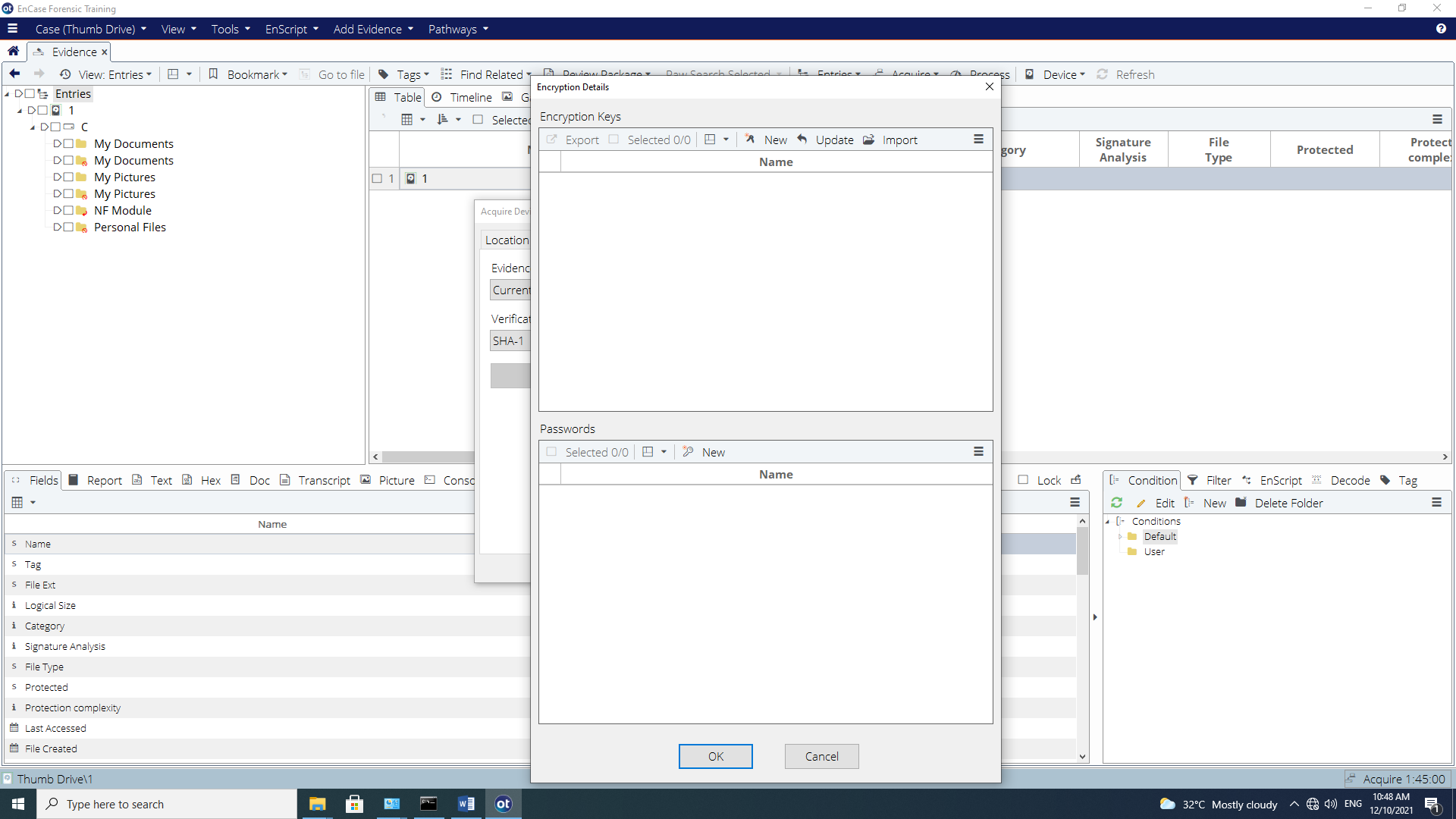


Figure B-9: Encryption Keys

We can start by applying a password to encrypt the evidence file with a symmetric key. Under the Password section click **New**. For the New Password, let’s use ‘Password’ (without quotes).

Click **OK** to continue.

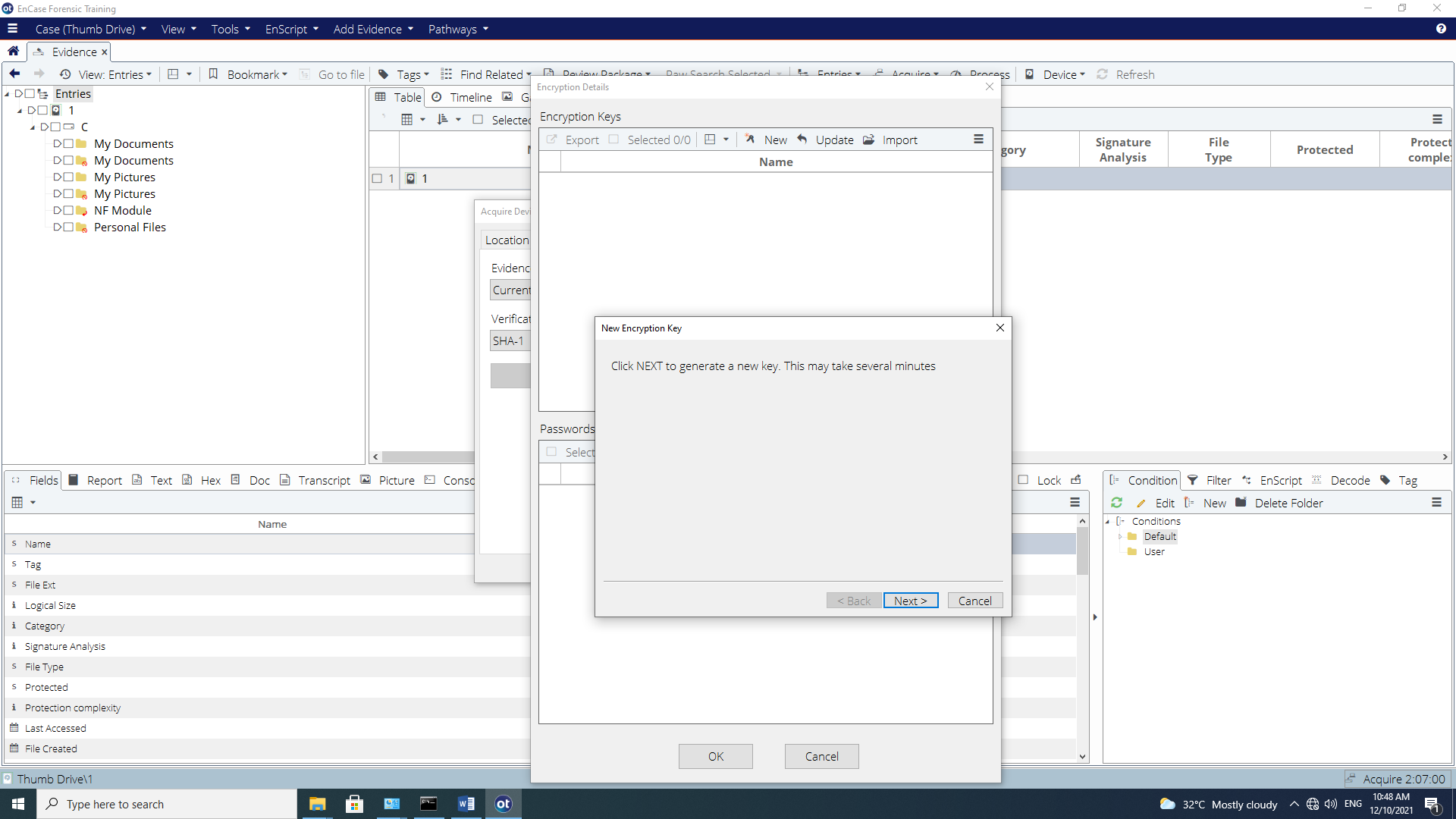


Figure B-10: New Encryption Key

In Encryption Keys Tab, Click **New**. Click **Next** to generate a new key.

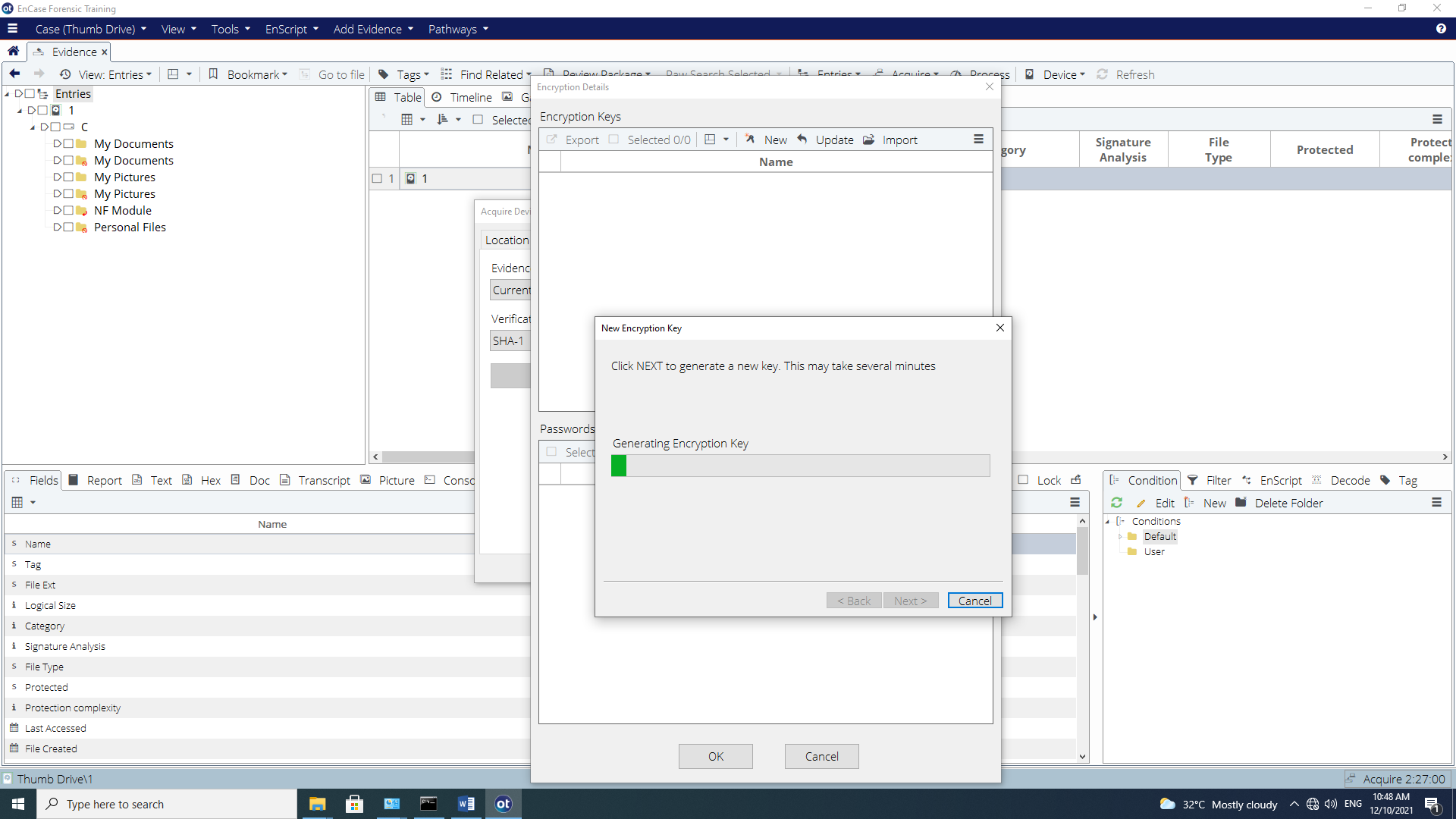


Figure B-11: Generating Encryption Keys

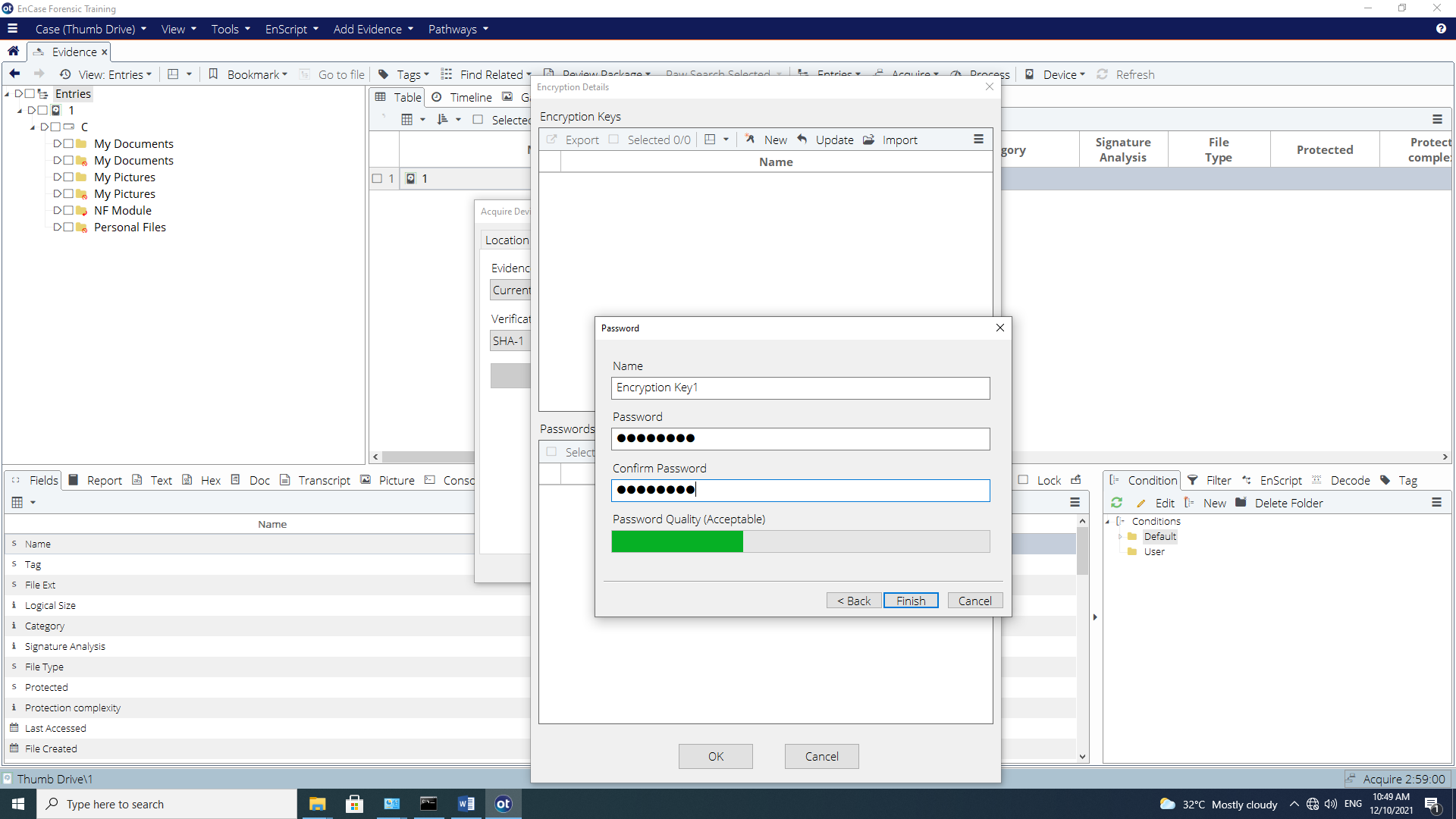


Figure B-12: Creating a new Encryption Key and Applying a password

Enter “Password” for both Password and Confirm Password fields and Click **Finish** to confirm which will then bring you back to the Encryption Details window. You’ll be prompted to save the Public Key. Save the public key on your own student folder.

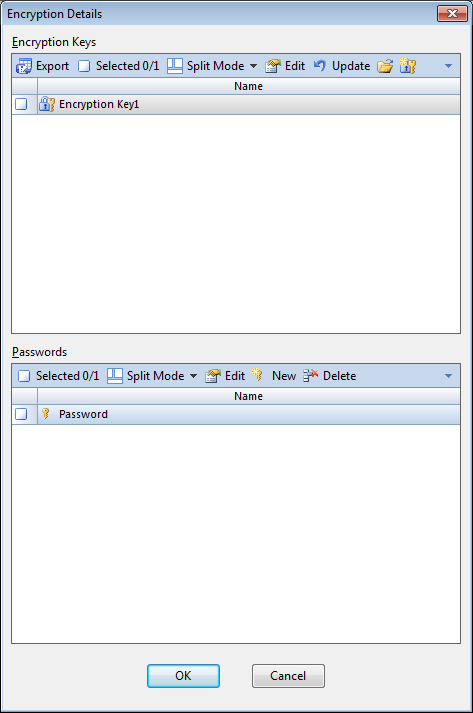


Figure B-13: Selecting a password

This will bring you back to the acquisition options to complete the acquire process.

Let’s go back into the Encryption options and apply asymmetric encryption to the evidence file.

At the Encryption option and in the Format tab, select the **Encryption** option.

You will see the password entry that we have created earlier. Deselect the password in the Password section (as we are now creating asymmetric encryption) and select **Create New Encryption Key** under the Encryption Keys options.

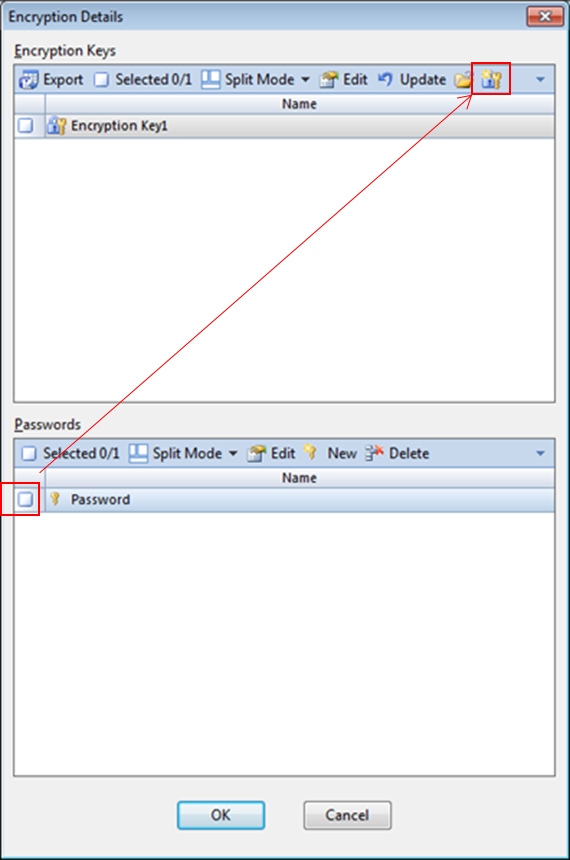


Figure B-14: Creating a new encryption key set

This New Encryption Key prompt will lead us to creating a new set of encryption keys

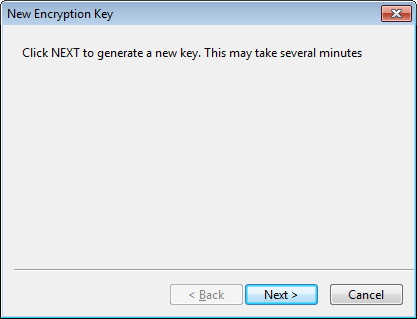


Figure B-15: Generating encryption keys

Click **Next** to proceed where the public/private keypair will be generated.

The encryption key generation will run for a second…and will then prompt for key name and a password. Let’s enter a password the same as before – ‘Password’ (without quotes).

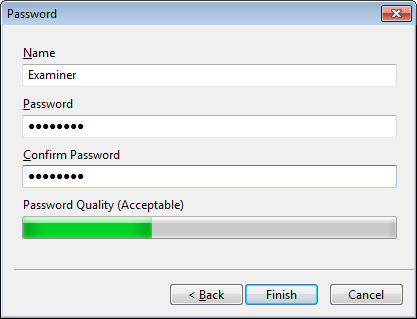


Figure B-16: Entering password for encryption keys

Once this is done, select **Finish**.

A prompt will display asking for the location to store the .PublicKey file. The default location is within the *C:\Users\<user name>\MyDocuments\EnCase\Keys folder*. [At this point, the .PrivateKey has been created.]

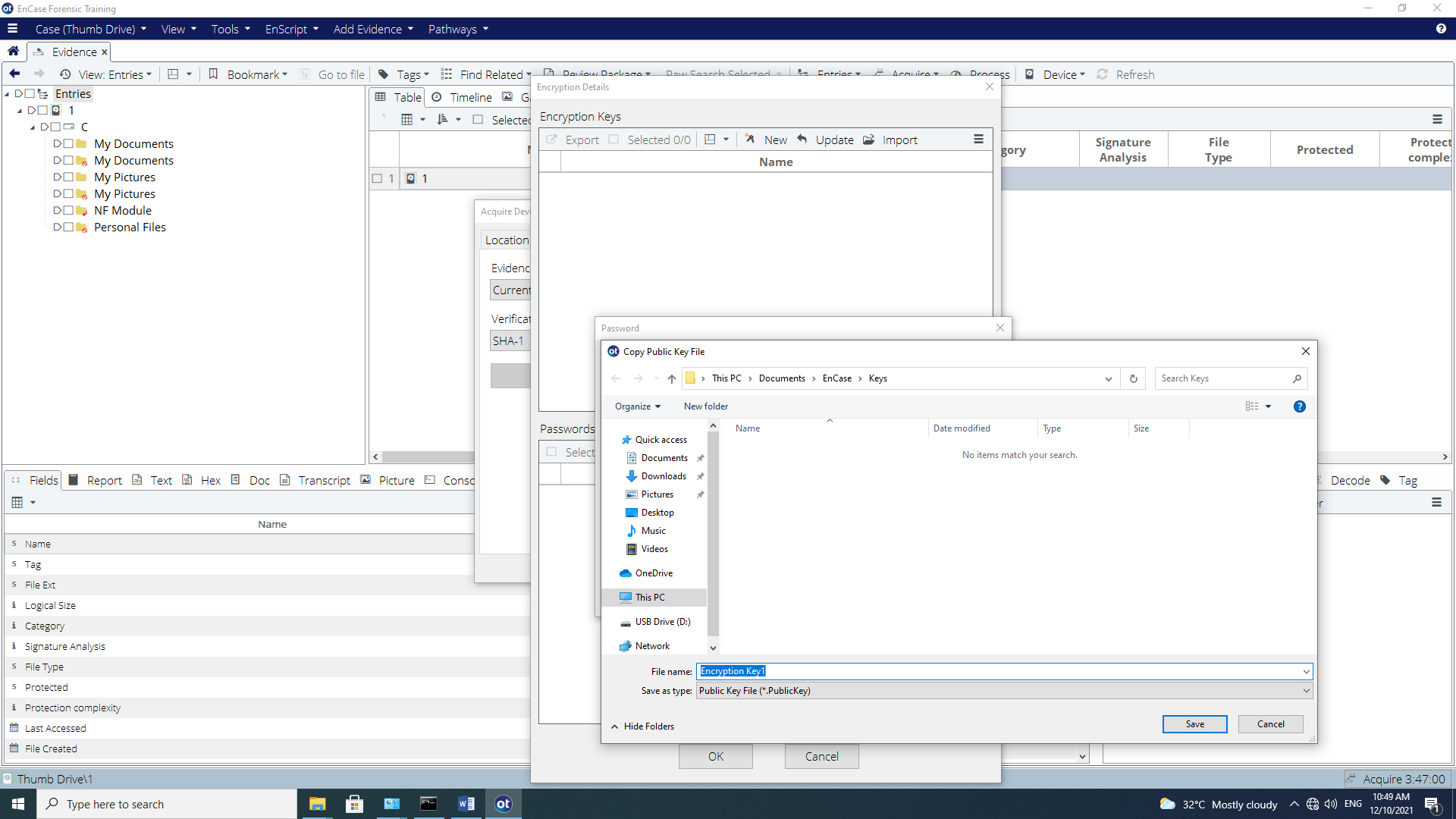


Figure B-17: Saving public encryption key

Select **Save.**  The key is now stored into the desired location.

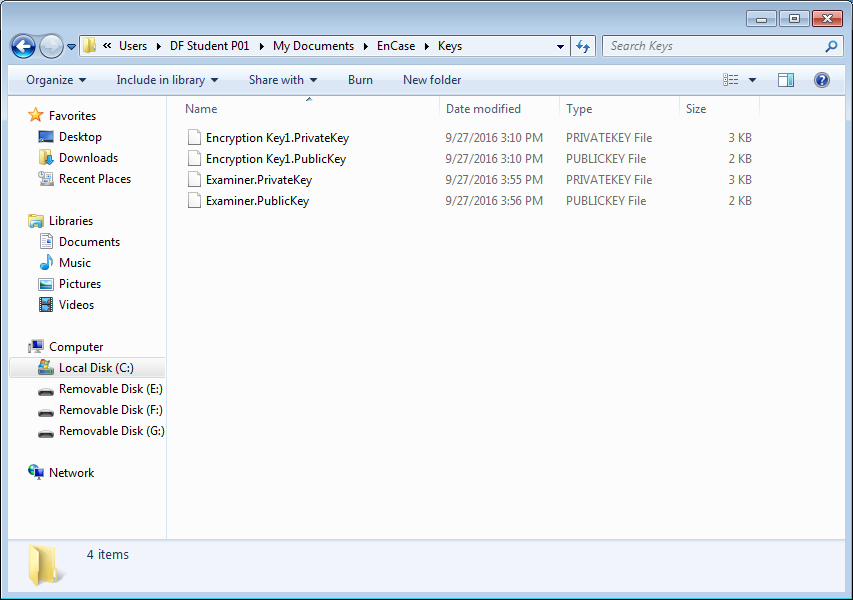


Figure B-18: Encryption key stored on examiner machine

The .PublicKey can now be distribute to another examiner to encrypt the evidence file.

Q6: Is there an issue distributing the .PublicKey? Explain why?

At the Encryption Details window, click **Update** button to refresh the encryption key view.

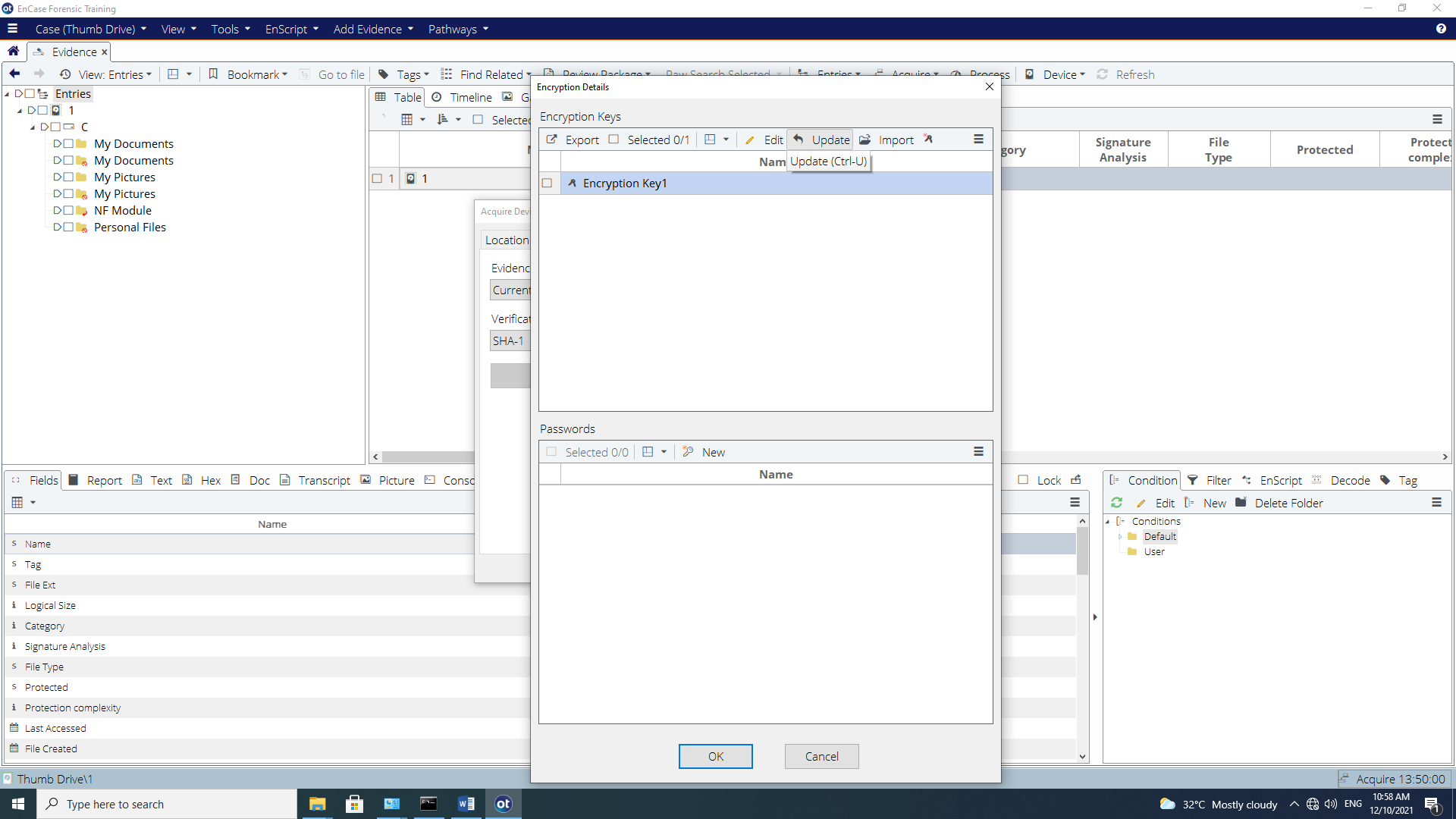


Figure B-19: Refreshed encryption key view

Blue check the **Examiner** encryption key and select **OK.**  After this, commence the acquisition of the evidence file. This evidence file will be encrypted by the examiner’s public key.

After the acquisition process has completed, a prompt asking to enter the password will appear. {Enter the password you have used for the Examiner’s evidence file i.e. Password}

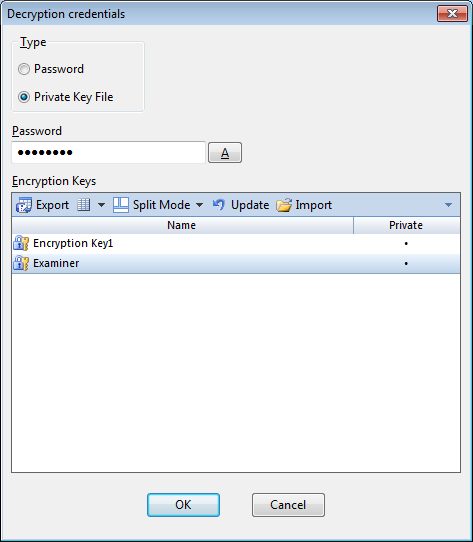


Figure B-20: Decrypting Evidence file

Once the password is entered and select OK, the evidence file will be decrypted and loaded into EnCase.

Reflection: What have you learnt through this practical exercise?

- The End -