**What is Autopsy?**

Autopsy is an open-source and powerful digital forensics platform. Several features within Autopsy have been developed by the **Department of Homeland Security** **Science** and **Technology**funding. You can read more about this [here](https://www.dhs.gov/science-and-technology/news/2017/12/12/snapshot-st-enhancing-autopsy-digital-forensics-tool).

[**The official description**](https://www.autopsy.com/): "*Autopsy is the premier open source forensics platform which is fast, easy-to-use, and capable of analysing all types of mobile devices and digital media. Its plug-in architecture enables extensibility from community-developed or custom-built modules. Autopsy evolves to meet the needs of hundreds of thousands of professionals in law enforcement, national security, litigation support, and corporate investigation.*"

This room's objective is to provide an overview of using the Autopsy tool to analyse disk images. The assumption is that you are familiar with the Windows operating system and Windows artefacts in relation to forensics. Before proceeding, start the attached virtual machine. The VM is ready to use with the **"Split View"** feature. If you wish to use **RDP**, the credentials are below.

**Workflow Overview**

Before diving into Autopsy and analysing data, there are a few steps to perform; such as identifying the data source and what Autopsy actions to perform with the data source.

Basic workflow:

1. Create/open the case for the data source you will investigate
2. Select the data source you wish to analyse
3. Configure the ingest modules to extract specific artefacts from the data source
4. Review the artefacts extracted by the ingest modules
5. Create the report

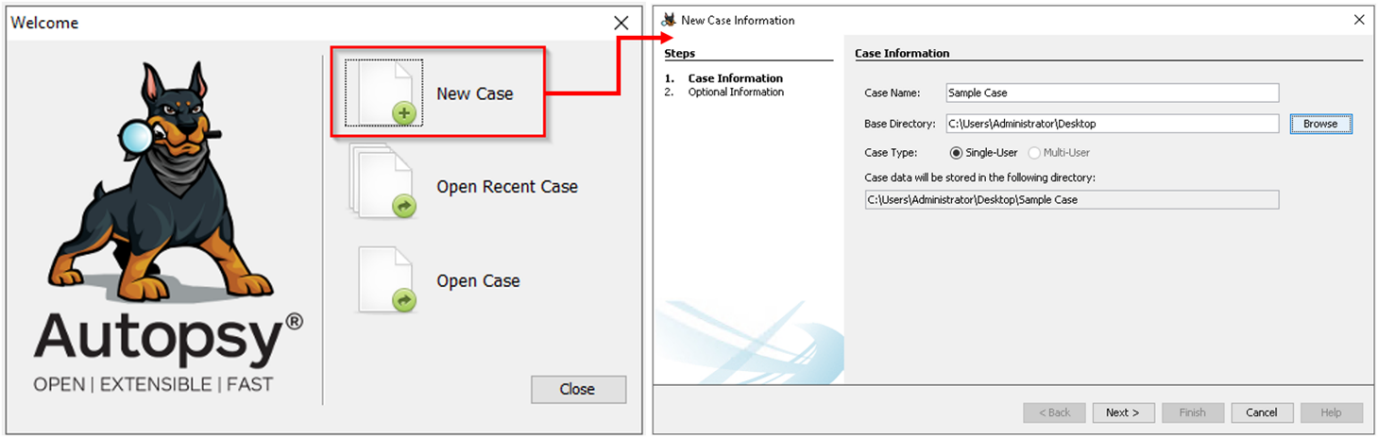
**Case Analysis | Create a New Case**

To prepare a new case investigation, you need to create a case file from the data source. When you start Autopsy, there will be three options. You can create a new case file using the**"New Case"** option. Once you click on the "New Case" option, the **Case Information**menu opens**,** where information about the case is populated.

* **Case Name**: The name you wish to give to the case
* **Base Directory**: The root directory that will store all the files specific to the case (the full path will be displayed)
* **Case Type**: Specify whether this case will be local (**Single-user**) or hosted on a server where multiple analysts can review (**Multi-user**)

**Note**: In this room, the focus is on **Single-User**. Also, the room doesn't simulate a new case creation, and the given VM has a sample case file to practice covered Autopsy features.

The following screen is titled "**Optional Information"** and can be left blank for our purposes. In an actual forensic environment, you should fill out this information. Once you click on "Finish", Autopsy will create a new case file from the given data source.

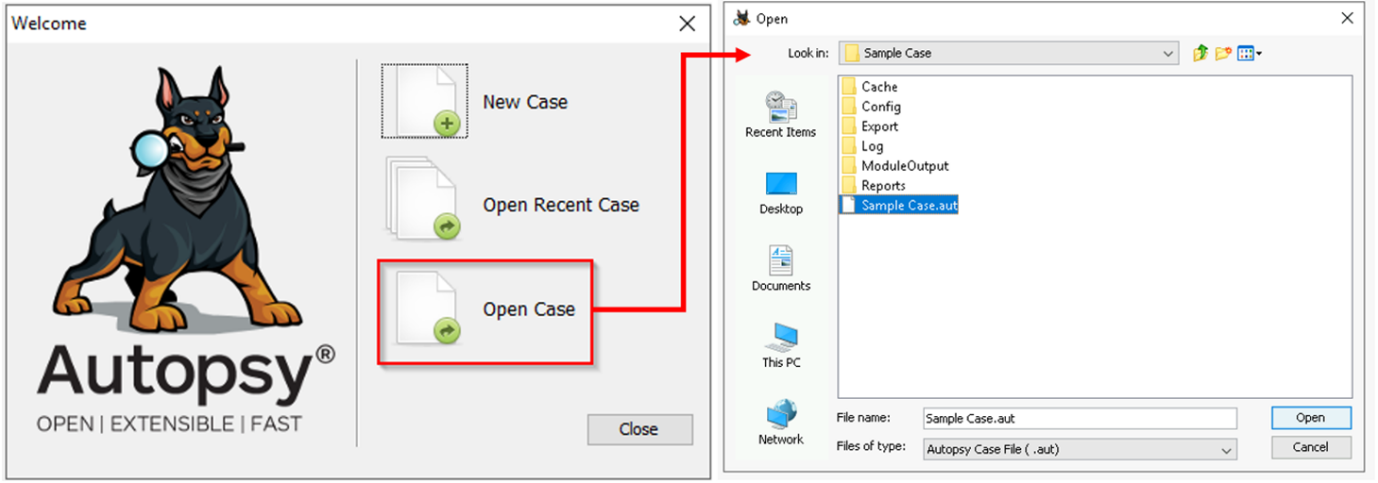


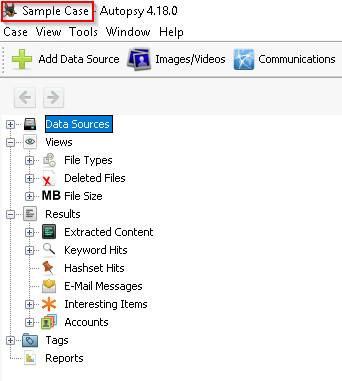
**Case Analysis | Open an Existing Case**

The Autopsy can also open prebuilt case files. Note that supported data sources are discussed in the next task. This part aims to show how to create/open case files with Autopsy.

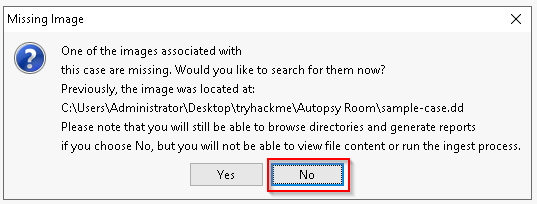
**Note:** Autopsy case files have a ".aut" file extension.

**In this room, you will import a case.** To open a case, select the "Open Case" option. Navigate to the case folder (located on the desktop) and select the .aut file you wish to open. Next, Autopsy will process the case files and open the case. You can identify the name of the case at the top left corner of the Autopsy window. In the image below, the name of this case is**"Sample Case"**.





**Note**: A warning box will appear if Autopsy cannot locate the disk image. At this point, you can point to the location of the disk image it's attempting to find, or you can click **NO**; you can still analyse the data from the Autopsy case.



Once the case you wish to analyse is open, you are ready to start exploring the data.

Answer the questions below

What is the file extension of the Autopsy files?

Top of Form

Correct Answer

Bottom of Form

**Import the "Sample Case.aut" file (located on the Desktop) as shown in the task and continue to the next task.**

Top of Form

Correct Answer

Bottom of Form

https://motasem-notes.net/the-complete-guide-to-phishing-attacks-tryhackme/