Autopsy Walkthrough

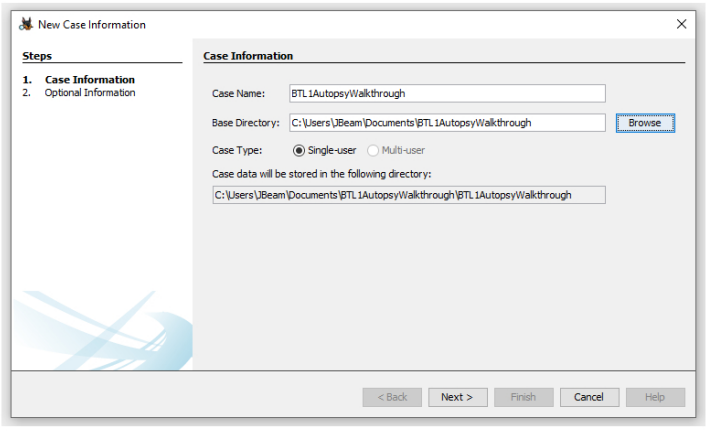
The following walkthrough guide will help you to better understand some features of Autopsy, and ensure you are familiar with the UI and can complete basic investigative actions. This lesson is designed to prepare you for the next practical exercise, and for the BTL1 exam. Below is a link that'll take you to a resource page over at the California Cybersecurity Institute. The file you need to download is **Laptop Image** under the heading "2019 Digital Forensics Downloads". This ZIP file is just over 5 GB in size – we know it's big, but this is to reproduce a realistic forensic investigation on a suspect laptop. Please note that all credit for this disk image goes to the CCI, we are utilizing it as a public resource for training purposes.

Click Here to Visit California Cybersecurity Institute Download Page

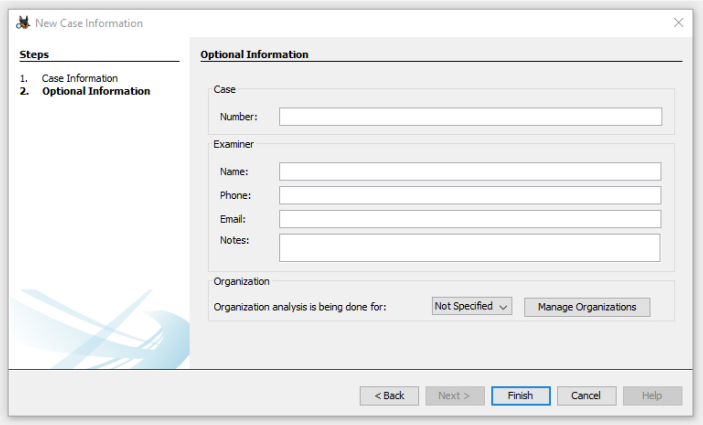
Starting a New Case – Importing a Data Source and Running Ingest Modules

Firstly we need to open Autopsy. When you're presented with the below screen, click New Case.

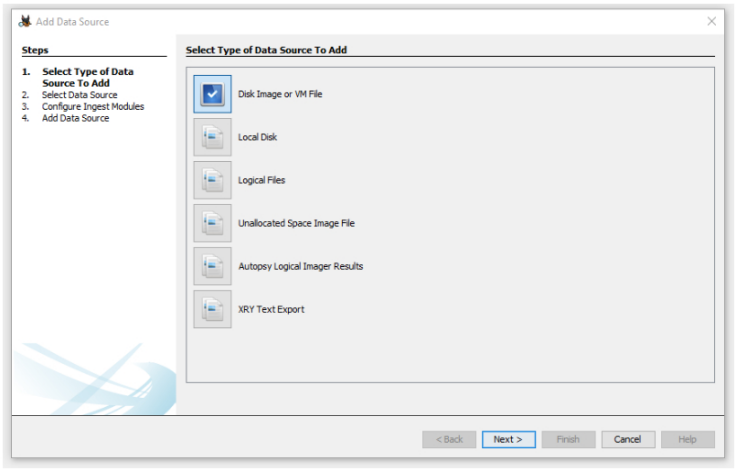
Here we need to provide a name and a base directory to store all our files. We have selected the name "BTL1AutopsyWalkthrough" and saved it to a directory with the same name in our Document folder.



The next screen will ask us to input some optional information about the investigation. We don't need to use this, but this is how security teams and law enforcement will add investigation-related metadata to Autopsy

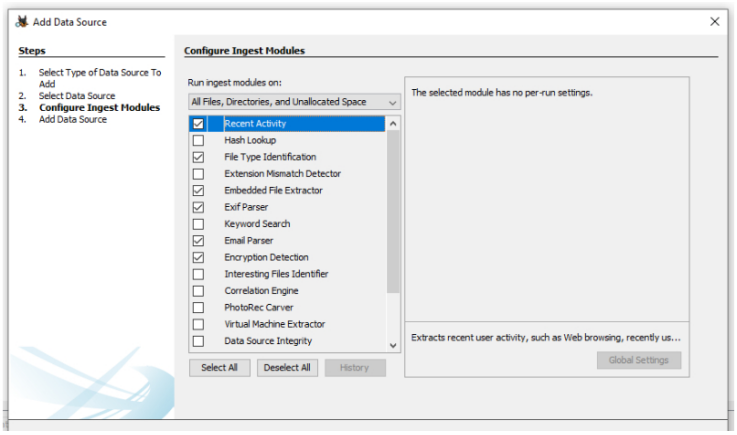


Autopsy should then prompt us to add our Data Source, in this case, it is a disk image, so we need to select "Disk Image or VM File" and then click Next.

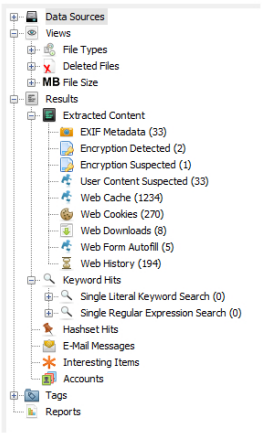


Click Browse and select the Craig Tucker Desktop.E01 file we linked to at the start of this lesson then click Next to add this as a data source for our investigation. Next we'll be asked if we want to run any ingest modules, these are automated actions that can be conducted against a data source to retrieve information that is useful to the forensic examiner, saving them time. For this walkthrough we want to select "All Files, Directories, and Unallocated Space" from the drop-down menu, as this chooses the targets that ingest modules will be run against. Then you should select the following:

- Recent Activity
- File Type Identification
- Embedded File Extractor
- Exif Parser
- Email Parser
- Encryption Detection

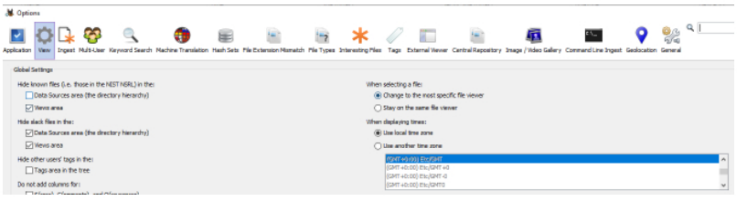


In the bottom right corner you will see a progress bar that will let you know when each ingest module has completed. Give Autopsy a few minutes to complete analysis of the data source. You should also notice that the values on the left-hand pane increase while the ingest modules are running, because they are discovering important information and placing it into the artifact tree to make it easy for the examiner to take a deeper look.



Changing Your Time Zone

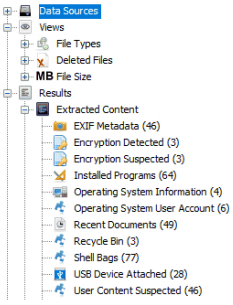
Depending on what you set your timezone as when you created the case, you should now change it to GMT +0:00. You can do this by navigating to Tools > Options > View > changing to GMT on the right-hand side, as shown below.



Analyzing Ingest Module Results

By now all of the ingest modules should've completed, and you won't see the progress bar in the bottom right corner of Autopsy. The navigation tree in the left pane should also have numbers next to the headings, showing that information has been found and sorted into different categories. Next we'll walk you through some of the information that Autopsy has pulled from the hard drive image.

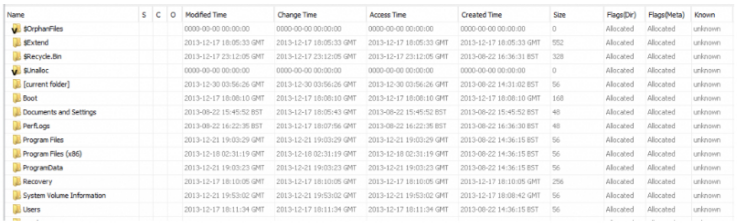
The first thing we want to look at are the volumes of the hardrive so we can collect information such as allocated and unallocated space, the size of these partitions, and the format or formats that are being used. At the top of the navigation tree click the + icon next to Data Sources, then the + icon next to Craig Tucker Desktop.E01, and you'll be presented with three volumes; vol1, vol2, vol3.



If we left-click on Craig Tucker Desktop.E01 in the navigation tree, the right-hand pane will now show information

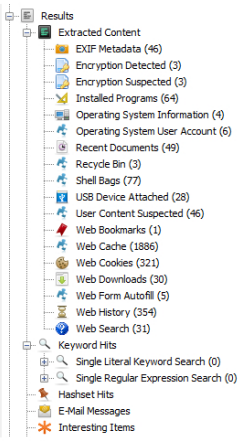
about the detected volumes. This is known as the Partition Table.

In the above screenshot we can see that vol2 is formatted with NTFS / exFAT, and that it starts at sector 2048 and the length is 125825024. This is the main section of the hard drive, and is where the file structure sits. Everything from users to documents and downloads will be in this volume. If you double click vol2, we are presented with a read-only file structure so we can browse files as if we're actually sat at the laptop!

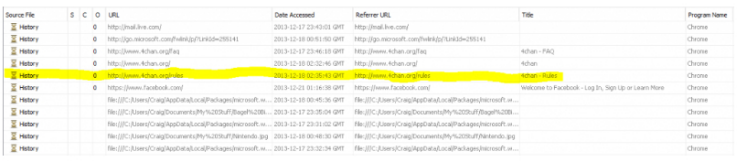


Spend a minute playing around looking through the directories to see what you can find. It's good to be familiar with navigating forensic images this way, as individuals that use Windows on a daily basis will likely be familiar with navigating the file structure.

Now that you've had a look around, it's time to see the results of the ingest modules, which are located on the navigation tree under the **Results** heading, shown below.



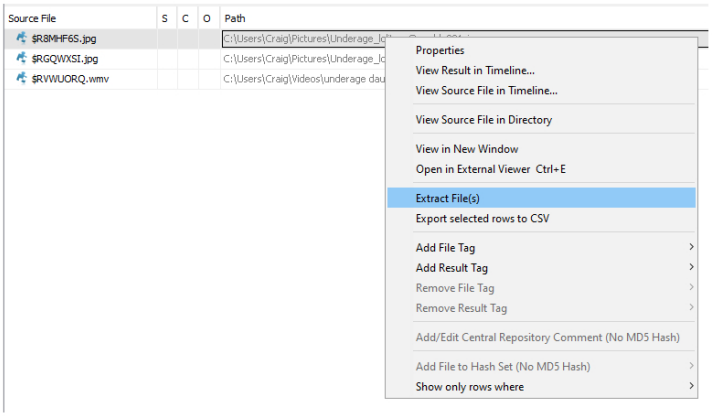
Let's look at a few of these results. To start, click on the Web History near the bottom. This will show us the sites that have been visited on the system including the date accessed, the page title if available, and the program that was used to access the web resource. For example, the highlighted line shows that a user has visited 4chan.org/rules via the Chrome browser on 2013-12-18 02:35 AM GMT.



This is a great way to view the browsing habits and sites accessed by a suspect. Timestamps also help us to create a timeline of events that have occurred and can be used to prove that a user visited resources on a particular day, which could aid an investigation.

Now let's see what files the user has deleted by going to the Recycle Bin in the navigation tree. On the right pane we can now see that the user has deleted three files, and we're given their file paths, the user that deleted them, and the time the file was deleted. This can be a quick-win if we're looking to identify files that have been deleted and gain information about them.

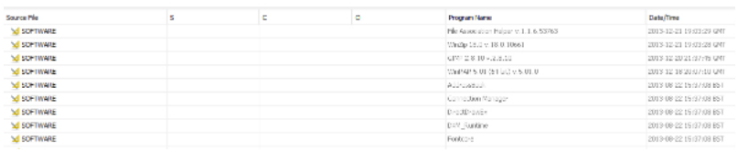
We can actually export these files to look at them (this isn't limited to files in the recycle bin, we can actually do this with any files identified in the disk image!). Right click the path for "Underage_lolita_r@ygold_001.jpg" **(don't worry, this image isn't anything explicit, this is just an example name for the investigation scenario)**.



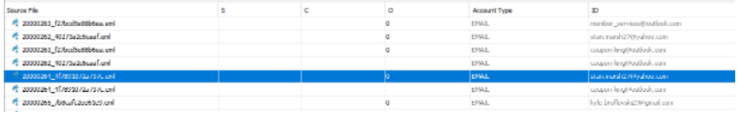
Select the destination that you want to export the file to, and go ahead and open it. Below is the image that we have just extracted from the disk image.

This feature can be useful if the investigation was regarding child exploitation, allowing the forensic examiners to identify potentially explicit images, export them, and confirm whether the material can be used as evidence in a legal prosecution against the suspect.

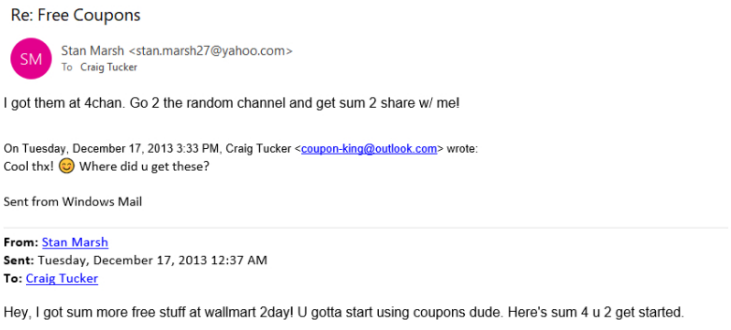
Moving on, let's take a look at the Installed Programs section to identify what software has been installed on this system. Left-click on the heading, and on the right pane we can now see a list of installed programs. From here we can determine when programs were installed and their names, with some entries including WinRAR, GIMP, WinZIP, and Google Chrome.



Let's go through one more section together, "Accounts > Email" right at the bottom of the navigation tree. Here we can see a list of email files that were downloaded to the system, typically through an email client.



Now that you understand how to export file by right-clicking, let's export the highlighted email file and take a look (you'll need an email client if you want to view it as the sender and recipient would see it, such as Mozilla Thunderbird or Microsoft Outlook App. Alternatively you can read the contents by opening the email with a text editor).



Re: Free Coupons

SM Stan Marsh <stan.marsh27@yahoo.com>
To Craig Tucker

I got them at 4chan. Go 2 the random channel and get sum 2 share w/ me!

On Tuesday, December 17, 2013 3:33 PM, Craig Tucker <coupon-king@outlook.com> wrote:
Cool thx! Where did u get these?

Sent from Windows Mail

From: Stan Marsh
Sent: Tuesday, December 17, 2013 12:37 AM
To: Craig Tucker

Hey, I got sum more free stuff at wallmart 2day! U gotta start using coupons dude. Here's sum 4 u 2 get started.

Reading a suspects emails could help to collect evidence regarding the case for a legal investigation, or for incident response purposes we could look to identify malicious emails that were present on the system around the time of the compromise. We could then analyse these to collect indicators such as:

- Email Sender
- Email Recipient
- Date and Time
- Subject Line
- Sending Server IP
- and more!

Spend some time looking through the different content that has been extracted by the ingest modules to see what else you can find on the system (you'll be asked questions about this in the next activity). If you want to take a look at a fresh disk image, considering downloading the other image provided by the California Cybersecurity Institute titled 'Additional Practice Image 1'.

Click Here to Visit California Cybersecurity Institute Download Page

Quizzes

Lab) Autopsy For Disk Analysis

Previous Topic

Back to Lesson