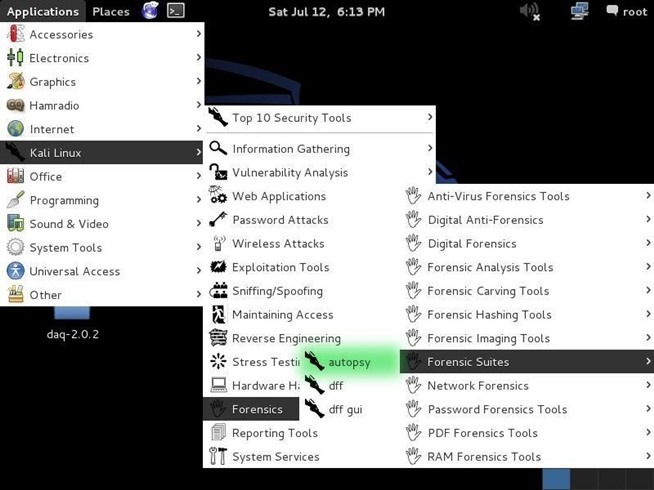
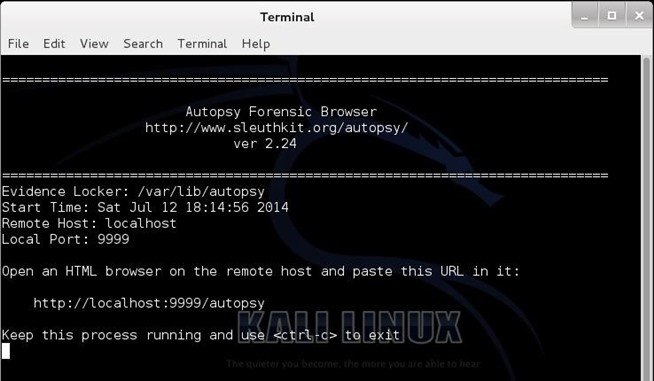
Autopsy was built to sit on top of the Sleuth Kit to offer an intuitive, GUI-based forensic suite that utilizes the strength of Sleuth Kit, while at the same time offering the basics of a case management tool.

**Step 1: Fire Up Kali & Open Autopsy**

Let's fire up Kali and then go to Applications -> Kali Linux -> Forensic Suites and select **autopsy** from the list.

[](http://img.wonderhowto.com/img/original/59/96/63541616874297/0/635416168742975996.jpg)

When you do so, you will open a screen that looks like that below. Notice that it asks you to open up a browser at **http://localhost:9999/autopsy** .

[](http://img.wonderhowto.com/img/original/56/24/63540775022890/0/635407750228905624.jpg)

**Step 2: Open a Web Browser**

Now, let's open any browser and navigate to the address above. This will simply take us to the local web server on our system (localhost) and access port 9999 where Autopsy is running. I am using the default browser in Kali, IceWeasel. When I navigate to that address, I get a webpage like that below.

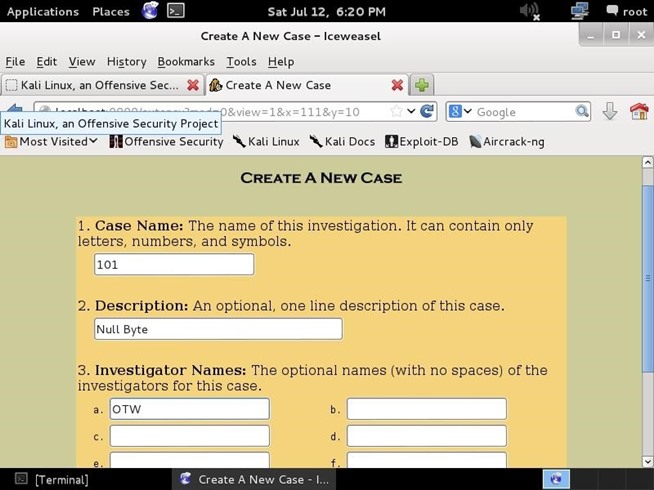
[](http://img.wonderhowto.com/img/original/89/03/63540775167485/0/635407751674858903.jpg)

As I mentioned earlier, autopsy is just a GUI overlay on top of Brian Carrier's excellent suite of forensic tools, Sleuth Kit. Since Sleuth Kit only uses command line instructions, Autopsy makes working with it much simpler and more intuitive.

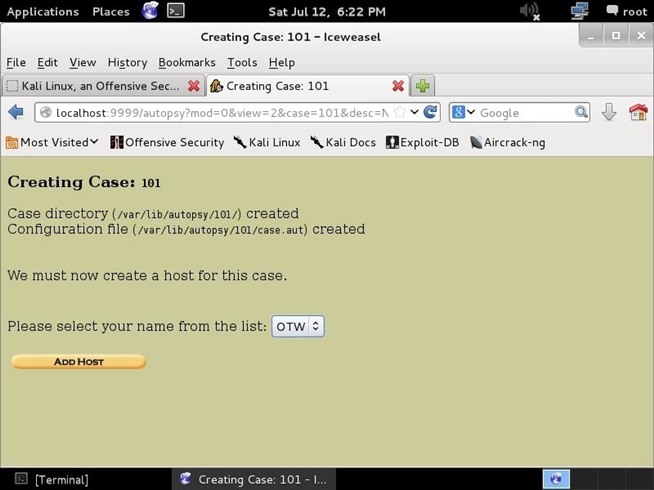
**Step 3: Create a New Case**

As in any real forensic investigation, you will need to create a case and organize all of your evidence and information. In this regard, autopsy requires that you start a case to get started.

Here, I have given this case a numerical case name (101) and a description of "Null Byte", and I have provided my name as the investigator (OTW). Please note that I can provide up to six (6) investigator names. In a real forensic investigation, you will seldom be working alone.

[](http://img.wonderhowto.com/img/original/98/22/63540775313452/0/635407753134529822.jpg)

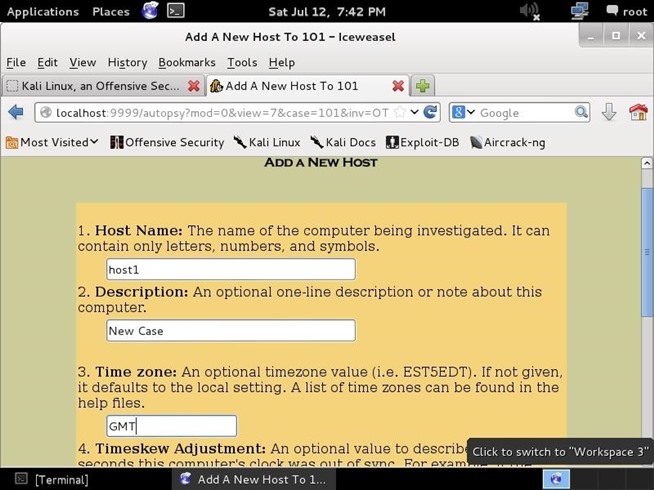
After hitting the "NEXT" button in the previous screen, I will be greeted with a screen like below.

[](http://img.wonderhowto.com/img/original/17/01/63540775406656/0/635407754066561701.jpg)

This screen simply gives us the name of the case, where the case will be stored (/var/lib/autopsy/101), and where its configuration file will be stored (/var/lib/autopsy/101/case.aut). Our next step to add a host.

**Step 4: Add a New Host**

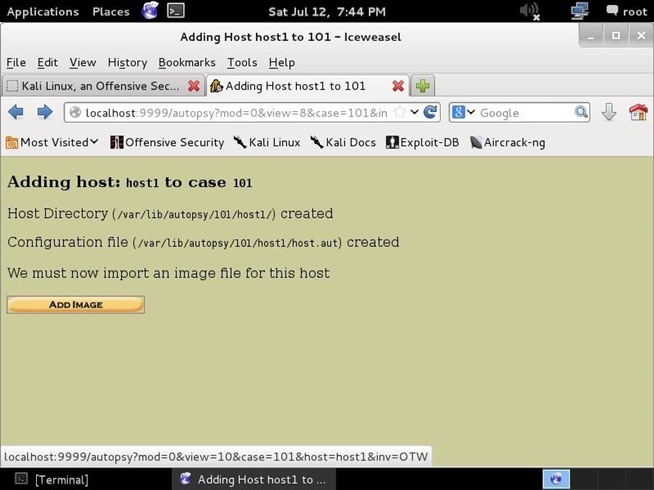
Click on the "Add Host" button below the line where you can select your name. When we click on that, it takes us to another screen where we can add information about our host like that below.

[](http://img.wonderhowto.com/img/original/92/55/63540780221749/0/635407802217499255.jpg)

Here we can add the host name (host1), a description (new case), and the time zone (GMT) we are working in. Of course, you can add your own host name, description, and time zone, as appropriate.

**Step 5: Add an Image File**

Next, we need to import an image file. An image file is a [bit-by-bit copy](http://null-byte.wonderhowto.com/how-to/hack-like-pro-digital-forensics-using-kali-part-2-acquiring-hard-drive-image-for-analysis-0155533/) of the storage device that we captured for evidence when we arrived at the crime scene. For instructions on making a forensically sound image, check out my previous guide on [creating a forensic image of a hard drive](http://null-byte.wonderhowto.com/how-to/hack-like-pro-digital-forensics-using-kali-part-2-acquiring-hard-drive-image-for-analysis-0155533/).

[](http://img.wonderhowto.com/img/original/55/77/63540780334765/0/635407803347655577.jpg)

Below, I have captured a new image file using **dcfldd** of the hard drive **sda** (the first SATA or SCSI hard drive), and written it to a file **/media/nullbyte** with a block size of 512 bytes.

[http://img.wonderhowto.com/img/90/22/63540782682249/0/hack-like-pro-digital-forensics-using-kali-part-3-creating-cases-autopsy-sleuth-kit.w654.jpg](http://img.wonderhowto.com/img/original/90/22/63540782682249/0/635407826822499022.jpg)

Now, I can import that image to Autopsy by giving it the location where I saved the image (/media/nullbyte), tell autopsy what type of image (disk), and the import method (copy).

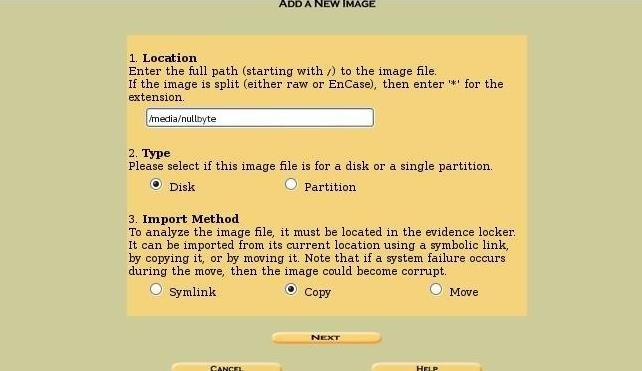
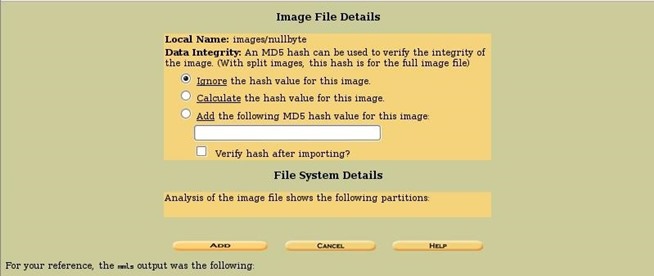
[](http://img.wonderhowto.com/img/original/58/12/63541619121047/0/635416191210475812.jpg)

Image via [wonderhowto.com](http://wonderhowto.com)

**Step 6: Data Integrity**

Whenever we are creating an image or saving an image that might be used in any legal proceeding, it is critical to make certain that we can maintain the integrity of the image. This means that we can prove that the image has not been tampered with from the time that the image was captured until the time of the trial.

We can do that by creating a hash of the image.

[](http://img.wonderhowto.com/img/original/10/15/63540786185422/0/635407861854221015.jpg)

In this screen, Autopsy asks us whether we want to:

* **Ignore** the hash value for this image,
* **Calculate** the hash value for this image, or
* **Add** the following MD5 hash value for this image.

If you did not calculate the hash value when you captured the image (best practice), now is the time to do that. If you have created a hash value when you created the image, you can attach it to the image file here.