# Lab-14-1: Computer Forensics Investigation

In today’s lab, we will perform an in-depth forensic investigation. We will use a specialised forensic analysis tool – named Autopsy. The Autopsy tool provides a graphical interface for ease of use. The tool comes with a collection of plugins to examine data on a hard drive and produce relevant information. We can then analyse the information and extract digital evidence.

Lab setup:

* Copy the “lab-14-1-files” folder to your Desktop.

**Exercise-14-1-0: Installing Autopsy**

Before we start analysing evidence we need to install Autopsy. This is a straightforward task.

* In Windows Explorer navigate to the Desktop
* Open the lab-14-1-files folder
* Double-click autopsy-4.3.0-64bit.msi to install Autopsy
* We can use default installation settings:
  + Select: Next > Next > Install > Accept Admin Rights > Finish

**Exercise-14-1-1: Creating a Case in Autopsy**

Most forensic tools create “cases” to store important information about an investigation. This functionality means that we can ensure evidence integrity. Before we start performing any analysis we must create a case and add some evidence.

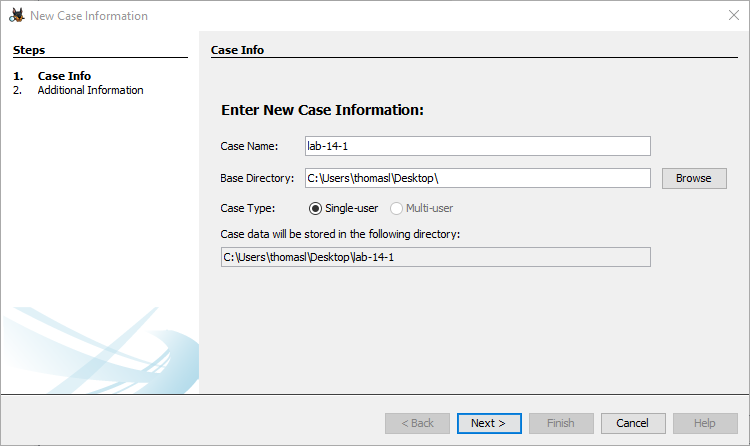
Start Autopsy by finding the link in the program link in the Start Menu. When Autopsy opens, you will be prompted to create or open a new case. Since we do not have a case, select “Create New Case”:



Now, we must enter some important information for our new case:

Case name: “case-14-1”

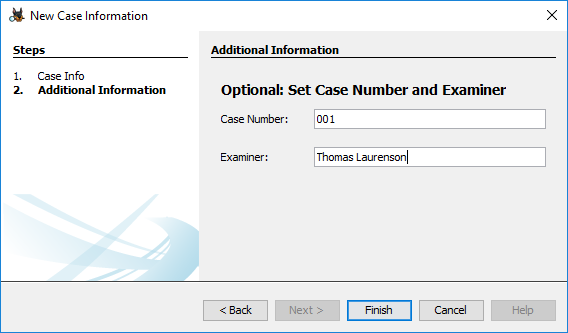
Base directory: “Desktop”



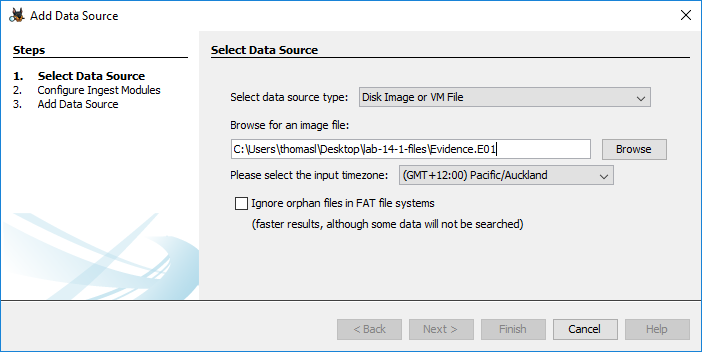
An output folder will be created automatically in the “base directory” with your selected case name. This is where all the important files will be stored.

Case number: 001

Examiner name: “Your name”



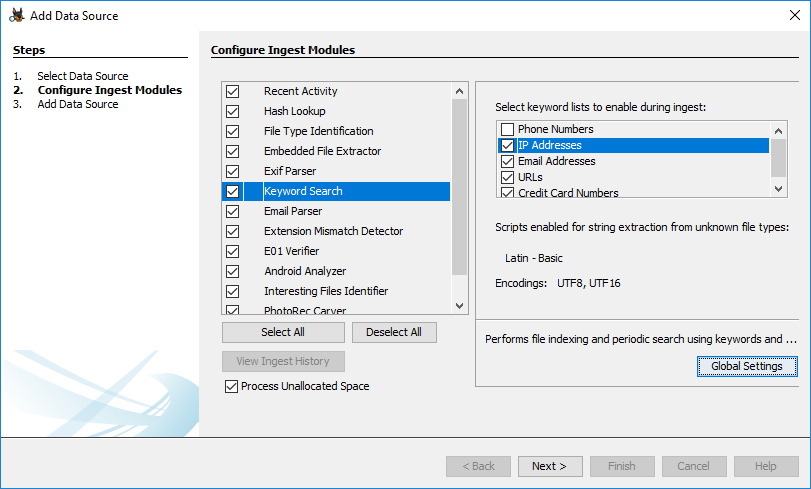
We must add an evidence source, or else we won’t have anything to analyse! Use the “Browse” button to locate and select the “Evidence.E01” file from the “lab-14-1-files” folder that should be on the Desktop.



Final step. This window displayed will provide the option to customise certain modules (plugins). We want to make sure we extend the default “Keyword Search” module. Select the module by left clicking it, then check the following boxes:

* Email Addresses
* URLs
* *See image below for an example*

This change will make Autopsy perform a keyword search for all these different types of digital artifacts.



Click “Next”. Them make sure you click “Finish”. Autopsy will automatically start analysing the data. A progress bar will appear in the bottom left corner. NOTE: You do not need to wait for Autopsy to finish processing before manually checking the extracted information.

**Exercise-14-1-2: Analysing Evidence**

This exercise works towards you understanding how a forensic investigation is performed. Today there is no set of specific steps – as the Autopsy Forensic Browser is quite east to navigate and use. Instead of direct instructions, you will be provided hints for each question.

If you get stuck try asking a fellow student and work together to find the problem. Also try some google searches to find useful information or tutorials. Also, feel free to ask the lecturer for help if you really get stuck!

**Q1.** What is the MD5 hash of the forensic image?

MD5 Hash: aee4fcd9301c03b3b054623ca261959a

HINT: In the “tree pane” click on the “Data Sources” link

**Q2.** What version of Microsoft Windows is installed?

|  |  |
| --- | --- |
|  | Windows\_NT |

HINT: In the “tree pane” click on the “Operating System Information” link

**Q3.** Who is the owner of the computer?

Greg Schardt

HINT: You can find this in the same place as the location used in Question 2.

**Q4.** Who is the primary user on the system (user account name)?

Mr. Evil

HINT: In the “tree pane” click on the “Operating System User Account” link.

HINT: In the “tree pane” try expanding “Data Sources > 4Dell Latutude CPi.E01 > vol2”. This will show you all the file system entries. Check the “Documents and Settings” folder (similar to the “Users” folder in newer Windows versions.

**Q5.** Find and document 5 hacking programs installed on the system?

* Cain and Abel
* Faber Toys
* Ethereal
* 123 Write All Stored Passwords
* Anonymizer bar

HINT: In the “tree pane” click on the “Installed Programs” link.

HINT: Like you did for question 4, look through the file system, specifically the “Program Files” directory.

HINT: You can confirm a program is a hacking tool by using google!

**Q6.** What is the email address of the suspect (the primary user)

mrevilrulez@yahoo.com

HINT: The suspect/primary user was identified in Question 4.

HINT: In the “tree pane” expand “Keyword Hits” and select “Email Addresses” link.

HINT: It may help to organise the list using the “Files with Hits” column. Click on the header to sort by ascending or descending order.

**Q7.** When did the suspect last login to their email account?

2004-08-26 03:26:44

HINT: In the “tree pane” expand “Web Cookies”.

HINT: Try looking for web cookies that correlate to the domain name of the suspect’s email addess (e.g., gmail.com).

**Q8.** The suspect recently performed two google searchers: What were they keywords used and the time of the search?

Keyword: who am i

Search time: 2004-08-25 16:07:32

Keyword: what is my ip

Search time: 2004-08-25 16:07:51

HINT: In the “tree pane” select “Web Search” module.

**Q9.** What web browser is the suspect using?

Internet Explorer

HINT: You can find this information in the same place as the Question 8 location.

Up to now, we have performed most of the tasks using the Autopsy modules. We will need to **perform the remainder of the tasks by analysing the file system entries.**

To access file system information, expand the following items from the “tree pane”

* Expand “Data Sources”
* Expand “4Dell Latitude CPi.E01”
* Expand “vol2”
* This is where all the file system entries are!

**Q10.** It seems the suspect recently deleted files. Try examining the Recycling Bin content for more information. What four files did the suspect delete?

1. lalsetup250.exe

2. netstumblerinstaller\_0\_4\_0.exe

3. WinPcap\_3\_01\_a.exe

4. ethereal-setup-0.10.6.exe

HINT: Find the recycling bin folder in the file system.

HINT: The programs names are not “Dc1.exe” etc. Try looking at all entries!

**Q11.** It seems the suspect has been using the mIRC program for communication. Provide a list of channels that the suspect has joined.

1. Chataholics

2. Cybercafe

3. Elite.Hackers

4. evilfork

5. funny

6. houston

HINT: Try looking in the “Program Files” directory for the mIRC application.

HINT: Log files remember everything!

HINT: There are a total of 12 channels

**Q12.** It seems the suspect has been capturing network traffic of a target. They have used the Ethereal program (now known as Wirehsark) to capture network traffic. What is the name of the packet capture file they have collected? (include the file system path)

Interception

C:\Documents and Settings\Mr. Evil\interception

HINT: Try looking in the “Application Data” folder for the suspect for information on “Ethereal”.

HINT: It is probably a recent file.

**Exercise-14-1-3: Advanced Analysis Techniques**

This exercise is **optional depending on time available for the lab.**

**Q13.** You now know that the suspect has collected network traffic of a target. What type of device is the **target** using?

Windows CE (Pocket PC)

HINT: In Autopsy you can extract files by right-clicking the file and selecting “Extract file(s)”.

HINT: You can open the packet capture file in Wireshark.

HINT: Remember from the network traffic labs, we can “Follow HTTP Stream”

**Q14.** Decrypt the suspects Windows password (eg. NTLM password). What is the suspects password? While you are at it, you might as well crack the Administrators password as well !!

Suspect’s password: EMPTY

Administrators password: EMPTY

HINT: Hashed passwords are stored in “C:\WINDOWS\System32\config” in the “SAM” file. The “system” file can also be useful depending on the attack method.

HINT: The password file is protected, you cannot simply open the file to find the hash. Try out OPHCrack portable version for Windows (<http://ophcrack.sourceforge.net/>).