Digital Forensics with Autopsy

The Cool One · Follow
7 min read · Mar 1, 2020

When we talk about digital forensics, there are a lot of tools we use like EnCase, FTK Imager, Volatility, Redline etc. But the tool we are going to talk about today is Autopsy, and see how we can use it in investigations.

What is Autopsy?

Autopsy is an open source digital forensics tool developed by Basis Technology, first released in 2000. It is a free to use and quite efficient tool for hard drive investigation with features like multi-user cases, timeline analysis, registry analysis, keyword search, email analysis, media playback, EXIF analysis, malicious file detection and much more.

How to install Autopsy?

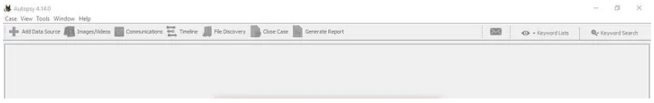
Step 1: Download Autopsy from here.

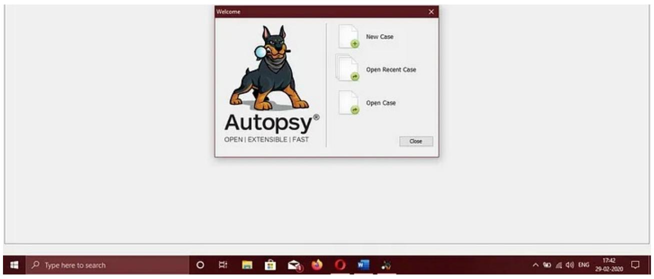
Let me tell you the scenario in brief:

It is suspected that this computer was used for hacking purposes, although cannot be tied to a hacking suspect, Greg Schardt. Schardt also goes by the online nickname of "Mr. Evil" and some of his associates have said that he would park his vehicle within range of Wireless Access Points where he would then intercept internet traffic, attempting to get credit card numbers, usernames & passwords. Find any hacking software, evidence of their use, and any data that might have been generated. Attempt to tie the computer to the suspect, Greg Schardt.

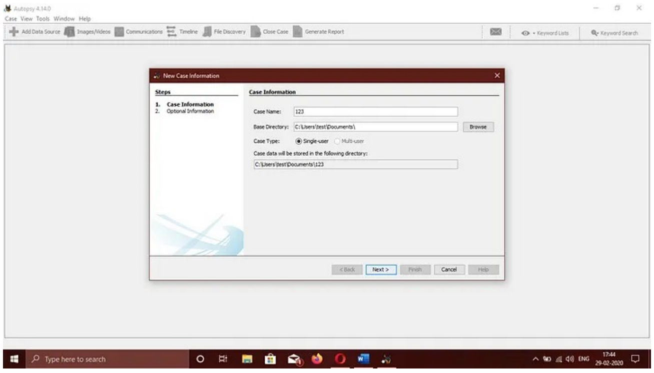
So let's begin…

Step 1: Run Autopsy and select *New Case*.





Step 2: Provide the *Case Name* and the *directory* to store the case file. Click on *Next.*



Steps

1. Case Information
2. Optional Information

Case Information

Case Name: 123

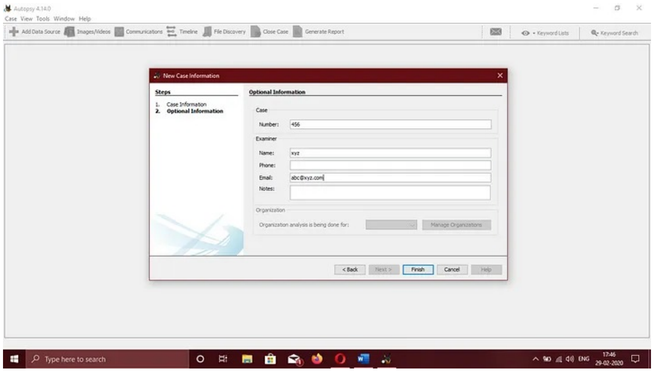
Base Directory: C:\Users\test\Documents\

Case Type: ● Single-user ○ Multi-user

Case data will be stored in the following directory:

C:\Users\test\Documents\123

Step 3: Add *Case Number* and Examiner's details, then click on *Finish*.



Steps

1. Case Information
2. Optional Information

Optional Information

Case

Number: 456

Examiner

Name: xyz

Phone:

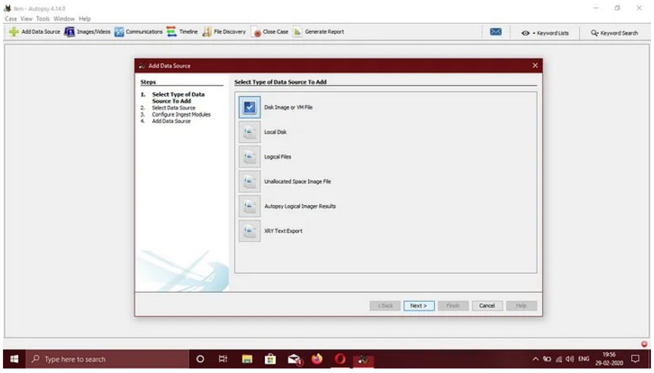
Email: abc@xyz.com

Notes:

Organization

Organization analysis is being done for:

Step 4: Choose the required data source type, in this case *Disk Image* and click on *Next.*



Steps

1. Select Type of Data Source To Add
2. Select Data Source
3. Configure Ingest Modules
4. Add Data Source

Select Type of Data Source To Add

☑ Disk Image or VM File

Local Disk

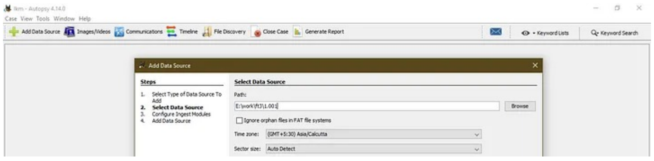
Logical Files

Unallocated Space Image File

Autopsy Logical Imager Results

XRY Text Export

Step 5: Give path of the data source and click on *Next.*



Steps

1. Select Type of Data Source To Add
2. Select Data Source
3. Configure Ingest Modules
4. Add Data Source

Select Data Source

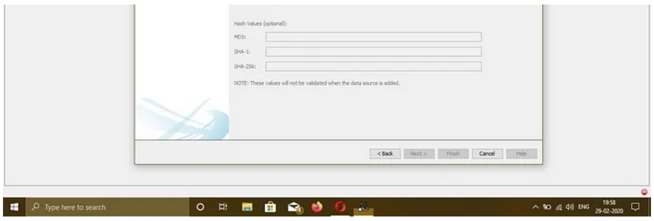
Path:

E:\work\ft3\1.001

□ Ignore orphan files in FAT file systems

Time zone: (GMT+5:30) Asia/Calcutta

Sector size: Auto Detect



Hash Values (optional):

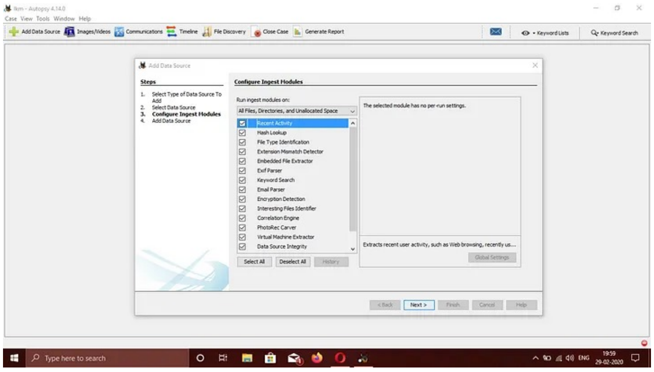
MD5:

SHA-1:

SHA-256:

NOTE: These values will not be validated when the data source is added.

Step 6: Select the required modules and click on *Next*.



Steps

1. Select Type of Data Source To Add
2. Select Data Source
3. **Configure Ingest Modules**
4. Add Data Source

Configure Ingest Modules

Run ingest modules on: All Files, Directories, and Unallocated Space

☑ Recent Activity
☑ Hash Lookup
☑ File Type Identification
☑ Extension Mismatch Detector
☑ Embedded File Extractor
☑ Exif Parser
☑ Keyword Search
☑ Email Parser
☑ Encryption Detection
☑ Interesting Files Identifier
☑ Correlation Engine
☑ PhotoRec Carver
☑ Virtual Machine Extractor
☑ Data Source Integrity

The selected module has no per-run settings.

Extracts recent user activity, such as Web browsing, recently us...

Step 7: After the data source has been added, click on *Finish.*

Step 8: You reach here once all the modules have been ingested. You can begin begin investigating but i recommend waiting until analysis and integrity check is complete.

There are a lot of things we can investigate to solve the scenario described earlier but for tutorial purposes we will be finding answers to the following 20 questions.

Q1. What is the image hash?

Soln. AEE4FCD9301C03B3B054623CA261959A.

To check the image hash, click on image and go to *File Metadata* tab. (We check the image hash in order to verify that it is the same as the hash created during the time when the image was created.)

Q2: What operating system was used on the computer?

Soln: Microsoft Windows XP.

For this, in the left side panel, we go to *Results > Extracted Content > Operating System Information*.

Q3: When was the install date?

Soln: GMT: Thursday, August 19, 2004 10:48:27 PM

Q4. Who is the registered owner?

Soln. Greg Schardt

Q5. What is the computer account name?

Soln. N-1A9ODN6ZXK4LQ (Click on *System* file)

Q6. When was the last recorded computer shutdown date/time?

Soln. 2004/08/27–10:46:27

To find this we go to ***C:\WINDOWS\system32\config\software\Microsoft\WindowNT\CurrentVersion\Prefetcher\ExitTime***

Q7. How many accounts are recorded (total number)?

Soln. 5 accounts: Administrator, Guest, HelpAssistant, Mr. Evil, and SUPPORT_388945a0 (Look at the *Account Type* column).

In the left side panel, we go to ***Results > Extracted Content > Operating System User Account***

Q8. Who was the last user to logon to the computer?

Soln. Mr. Evil (Can be checked through *Date Accessed* column)

Q9. List the network cards used by this computer?

Soln. Xircom CardBus Ethernet 100 + Modem 56 (Ethernet Interface)

Compaq WL110 Wireless LAN PC Card

We find answer at
C:\WINDOWS\system32\config\software\Microsoft\Windows NT\CurrentVersion\NetworkCards\

Q10. What is the IP address and MAC address of the computer?

Soln. IP=192.168.1.111

MAC=00:10:a4:93:3e:09

We go to *C:/Program Files/Look@LAN/irunin.ini*

Q11. List down the programs that can be used for hacking purpose?

Soln. Cain & Abel v2.5 beta45 (password sniffer & cracker)

Ethereal (packet sniffer)

123 Write All Stored Passwords (finds passwords in registry)

Anonymizer (hides IP tracks when browsing)

CuteFTP (FTP software)

Look@LAN_1.0 (network discovery tool)

NetStumbler (wireless access point discovery tool)

WinPcap (provide low-level network access and a library that is used to easily access low-level network layers.)

In the left side panel, we go to ***Results*** **>** ***Extracted Content*** **>** ***Installed Programs***

Q12. Which Email client is used by Mr. Evil?

Soln: Outlook Express, Forte Agent, MSN Explorer, MSN (Hotmail) Email

Go to ***C:/WINDOWS/system32/config/Clients/Mail***

Q13. What is the SMTP email address for Mr. Evil?

Soln: whoknowsme@sbcglobal.net

We find the answer at *C:\Program Files\Agent\Data\AGENT.INI*

Q14. How many executable files are in the recycle bin?

Soln. There are 4 namely, Dc1.exe, Dc2.exe, Dc3.exe, Dc4.exe

We find those at *C:/RECYCLER* *(RECYCER* is the directory for Recycle Bin.)

Q15. Are there any viruses on the computer?

Soln. Yes, a zip bomb(unix_hack.tgz) is present.

For this, in the left side panel, we go to *Results* > *Interesting Items* > *Possible ZipBomb* > *Interesting Files* *(Interesting Items* is where Autopsy shows possibly malicious files.)

Q16. A popular IRC (Internet Relay Chat) program called MIRC was installed. What are the userid, username, email and nickname used when the user was online in a chat channel?

Soln. user=Mini Me, email=none@of.ya, nick=Mr, anick=mrevilrulez

We can find that at *C:\Program Files\mIRC\mirc.ini*

Q17. Ethereal, a popular “sniffing” program that can be used to intercept wired and wireless internet packets was also found to be installed. When TCP packets are collected and re-assembled, the default save directory is that users /My Documents directory. What is the name of the file that contains the intercepted data?

Soln. File name is ‘Interception’

As hinted we need to go to through My Documents which in this case would be *Documents and Setting/Mr.Evil*

Q18. What type of wireless computer was the victim (person who had his internet surfing recorded) using?

Soln: Internet Explorer 4 on Windows CE

We find this in *Interception file*.

Q19. What websites victim was accessing?

Soln. Mobile.msn.com, MSN (Hotmail) Email

Q20. What is the web-based email address for main user?

Soln. mrevilrulez@yahoo.com (Through web history)

To find this, in the left side panel, we go to *Results* > *Extracted Content* > *Web History* and look at websites where login might be required.

With the above discoveries we can conclude that this machine was tied to *Greg Schardt and* our suspicions were true about it being used for hacking.

And with this our tutorial for using Autopsy for digital investigation ends here.

Digital Forensics Autopsy Cybersecurity Hacking Digital Forensic Tools

196 2

Written by The Cool One

54 Followers

Follow

More from The Cool One

The Cool One

Buffer Overflow: Detailed Tutorial

CVE-2018–7886 CloudMe Sync 1.11.0—Local

The Cool One

Heartbleed: Simple yet dangerous!

The vulnerability we're going to talk about in

Buffer Overflow

8 min read · May 24, 2020

37

this articleis CVE-2014–0160, known as the...

5 min read · Feb 8, 2020

23

See all from The Cool One

Recommended from Medium

Ross Andrews

HackTheBox: Recollection

Sherlocks: Digital Forensics

7 min read · Mar 9, 2024

7

igor_sec

TryHackMe | Disk Analysis & Autopsy

6 min read · Nov 17, 2023

59

Lists

Tech & Tools

16 stories · 217 saves

Medium's Huge List of Publications Accepting...

302 stories · 2585 saves

Staff Picks

632 stories · 933 saves

Natural Language Processing

1417 stories · 912 saves

Motasem Hamdan

Introduction to Digital Forensics and Incident Response |...

We covered basic and essential concepts and tools in Digital Forensics and Incident...

4 min read · Nov 20, 2023

65

paulpierce34

Active Directory Enumeration & Exploitation

Welcome to my second blog post! Here I will outline the steps taken to complete one of t...

7 min read · Nov 7, 2023

26

Enleak

LetsDefend—Memory Analysis

In this article, I use Volatility 3 to aid in memory forensics. The memory dump file...

4 min read · Dec 4, 2023

1

#$ubh@nk@r

HackTheBox Iclean Writeup

Intro : Hello Hackers welcome to my new HTB machine writeup → Iclean. Here we will lear...

5 min read · Apr 12, 2024

3 1

See more recommendations