Autopsy CTF Challenge by Emp3r0rN3r0:

Help a “Student” through this problem:

We intercepted traffic of a criminal network downloading malware onto a victim's computer. We have the network signature of the file, but we do not know where exactly this criminal copied the file. Based on logs, we know it is one of the files contained in the bin.tar.gz directory.

Walk the student through the process to find the file that matches this hash.

The flag is **Autopsy{filename}** where filename is the name of the malware file.

The hash of the downloaded malware is:

6859e1d10d08c1ea91f6e53ba6d601149b08d4efab8f8c2d586f6858ae1773a7

The end-state goal of this problem is for you, the student, to identify the malicious file that exists within the provided directory. Most of the work has been done for us already, so let us explore the most effective avenue of approach using the guided discovery learning process:

Step 1:

The most obvious step here is to identify what type of hash we are looking at. Can you identify this just by looking at it? If not, that is quite alright as Kali Linux has a few identification tools that we can utilize to identify the hash type.

```
┌──(terrifier_rex㉿ DESKTOP-SOGH9DN)-[~]
└─$ hashid 6859e1d10d08c1ea91f6e53ba6d601149b08d4efab8f8c2d586f6858ae1773a7
Analyzing '6859e1d10d08c1ea91f6e53ba6d601149b08d4efab8f8c2d586f6858ae1773a7'
[+] Snefru-256
[+] SHA-256
[+] RIPEMD-256
[+] Haval-256
[+] GOST R 34.11-94
[+] GOST CryptoPro S-Box
[+] SHA3-256
[+] Skein-256
[+] Skein-512(256)
┌──(terrifier_rex㉿ DESKTOP-SOGH9DN)-[~]
└─$
```

Figure 1: We can see that by running the “hashid” command, followed simply by the hash we have received that we are most likely looking at a 256-bit hash. This is great because it rules out most other possibilities.

Figure 1.1: Getting a second opinion with respect to any solution is an absolute must. As you can see above, I have utilized a common command "hash-identifier" to double check the identification. At first glance, I believed that the hash was SHA-256 and, as it turns out, it seems we were right.

Step 2:

Alright, so we have identified that the algorithm utilized in the given hash is indeed SHA-256, GREAT…. What Now?

- Download the "bin.tar.gz" directory as directed.
- DO NOT unzip the file..Why? We should always make a habit of maintaining possible malicious data in a secure laboratory environment to maintain the data in its neutral or dormant state to limit its ability to infect our own environment.
- LET'S MOVE ON!!!!

Step 3: TIME TO PERFORM AN AUTOPSY!

"Autopsy" is an Open-Source and rather simple to utilize digital forensics platform. It provides the investigator with the ability to maintain evidence in a decently secure state while performing digital forensics investigations. This software is secure, free, and incredibly effective. Due to this, I will be utilizing this platform to conduct this CTF challenge. Buckle in and let's crush it!

- Install Autopsy on your Linux or Windows system
- Run the Autopsy application

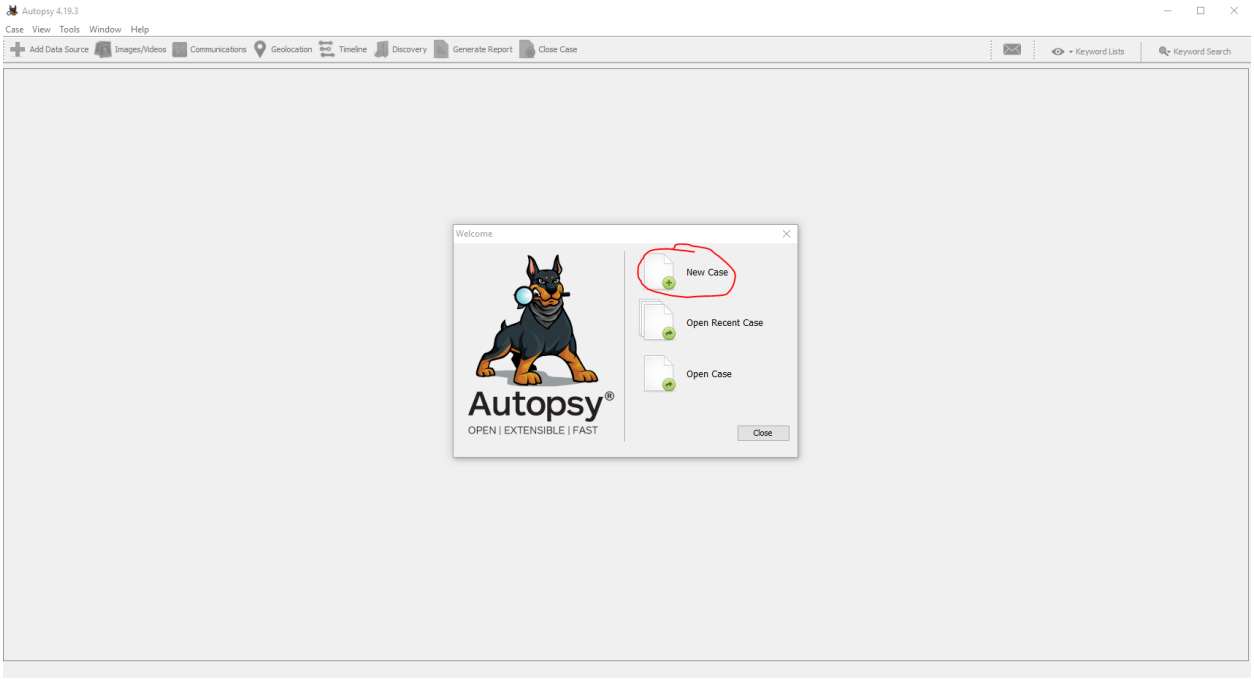


Figure 2: Once you arrive at this page, we will go ahead and create a new case.

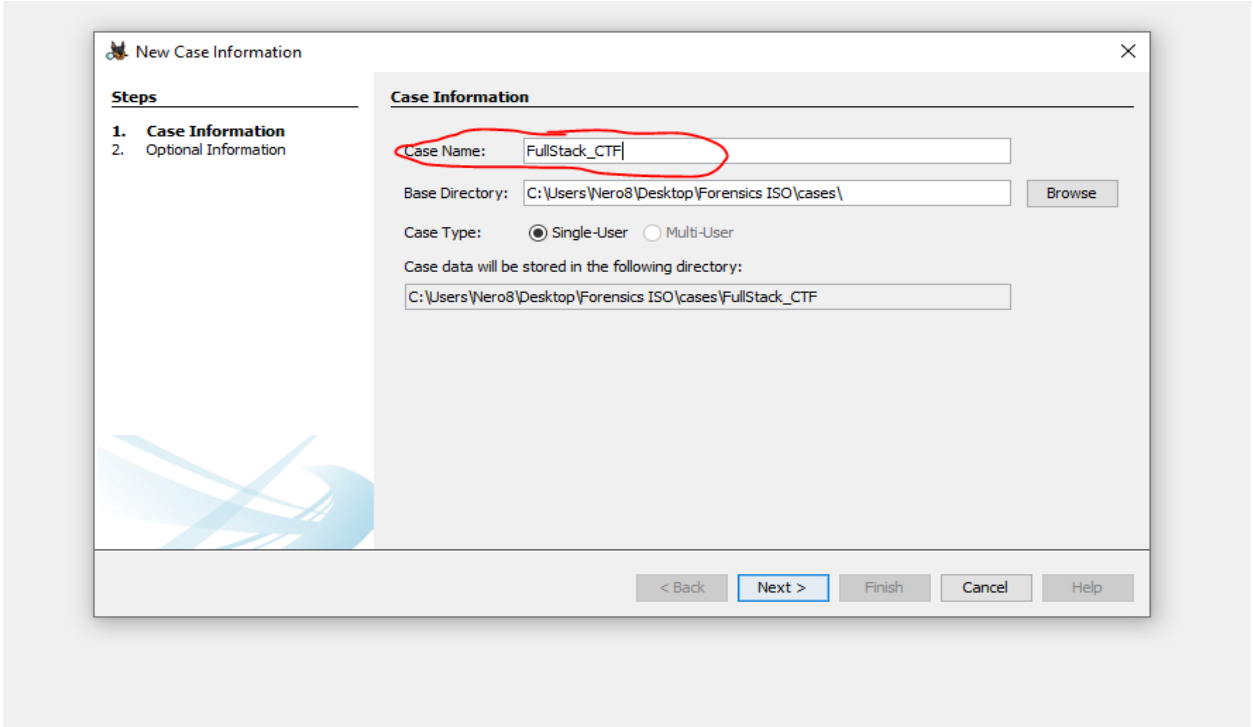


Figure 2.1: Go ahead and give your case a name. For reference, you can see that I have named this case “Fullstack_CTF”. Once complete, click next.

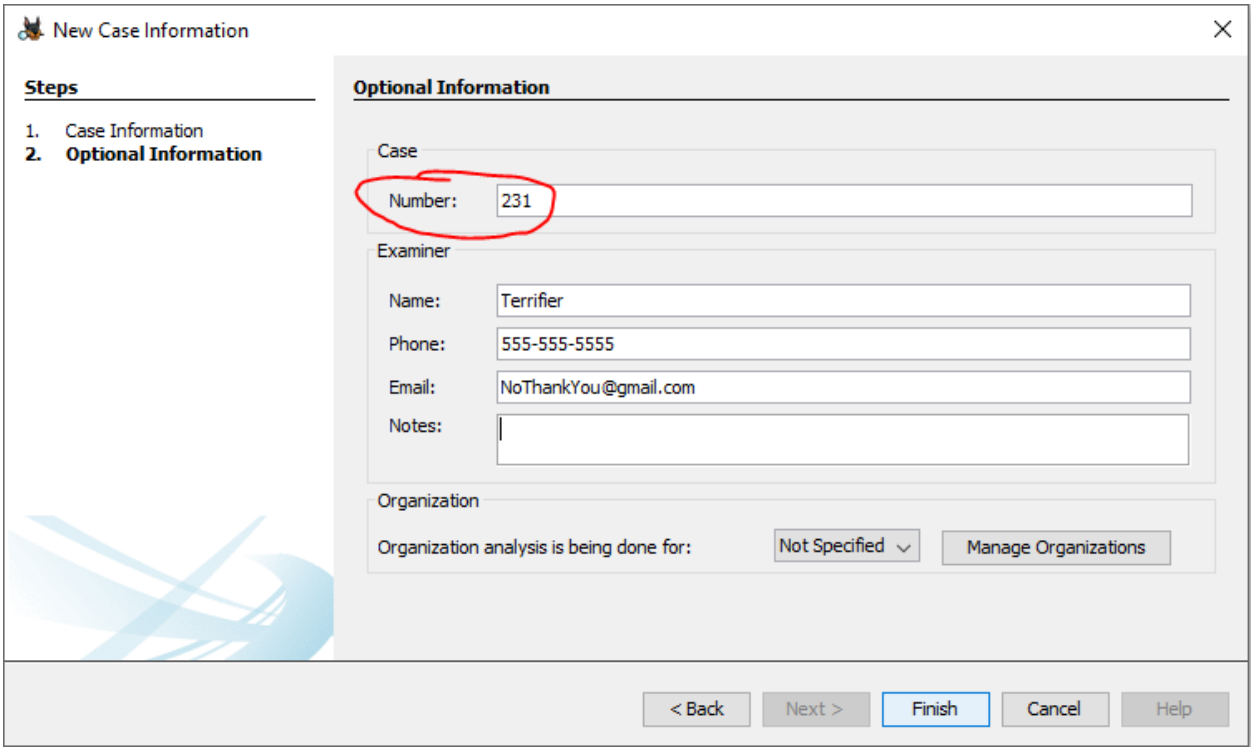


Figure 2.2: All we need to do here is assign our case a number and click “Finish”.

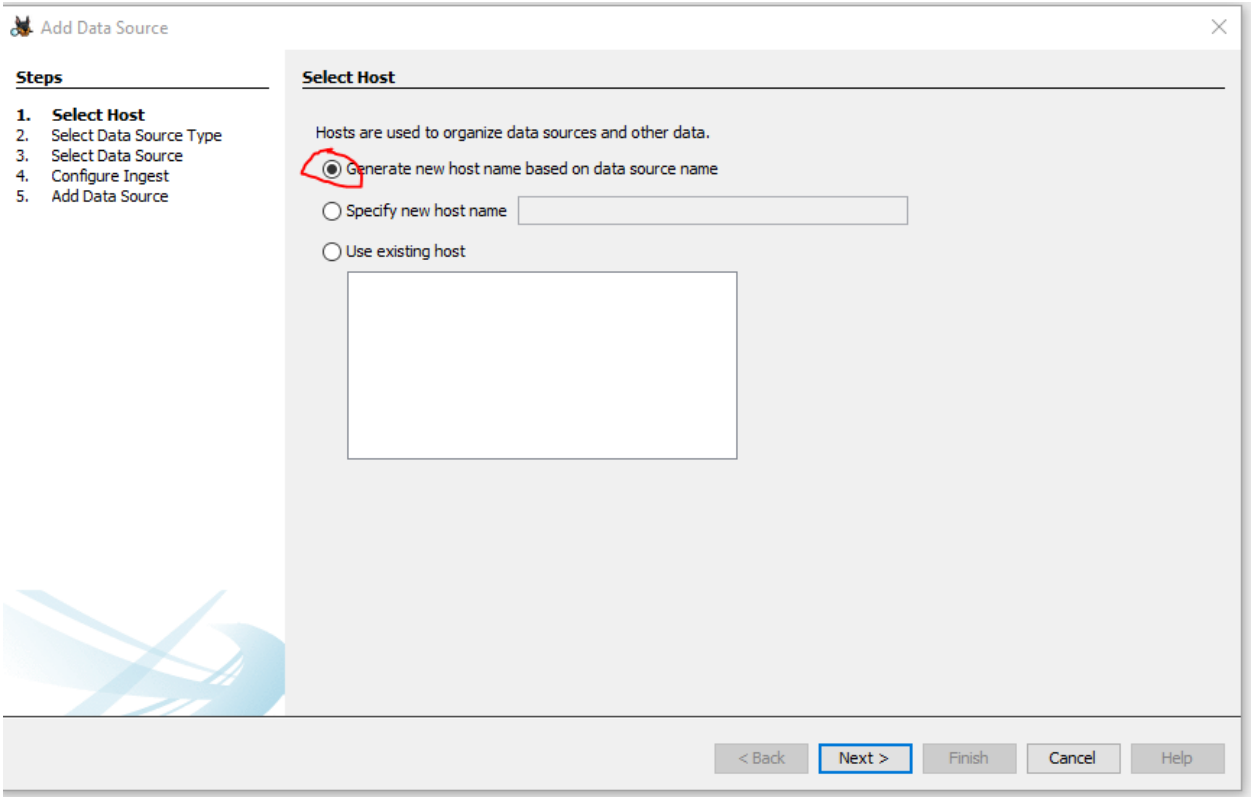


Figure 2.3: Here, we are directing “Autopsy” to generate a new host name based purely on the data source name, so it will share the name of the file system. Go ahead and click next.

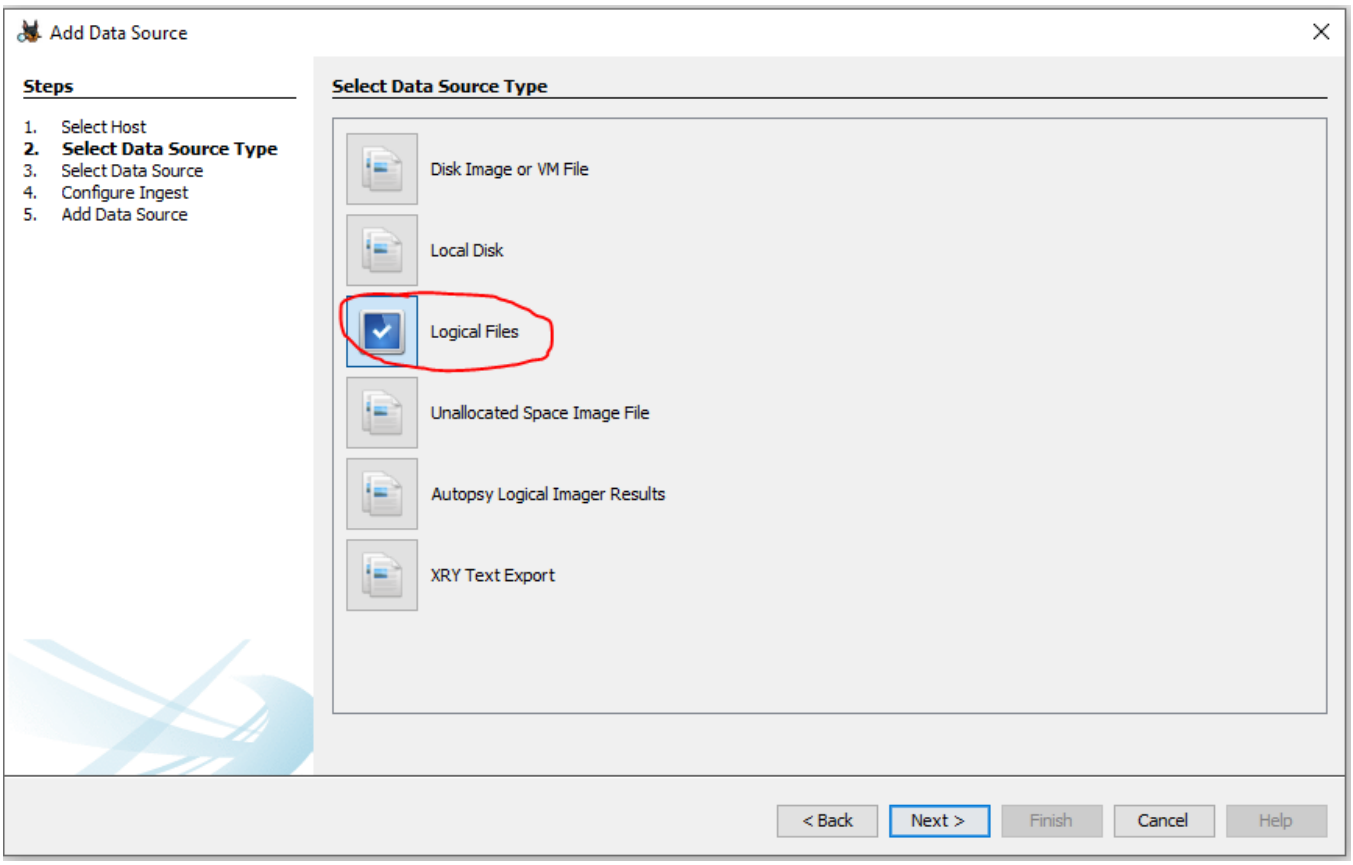


Figure 2.4: Alright, this step can look complicated, however, it is not. The Autopsy platform has many digital forensics capabilities, and this step is giving the investigator the opportunity to identify the type of file system that will be automatically scanned. Regardless, for this CTF challenge, we will be utilizing “Logical Files”. Once that is highlighted, go ahead, and click Next.

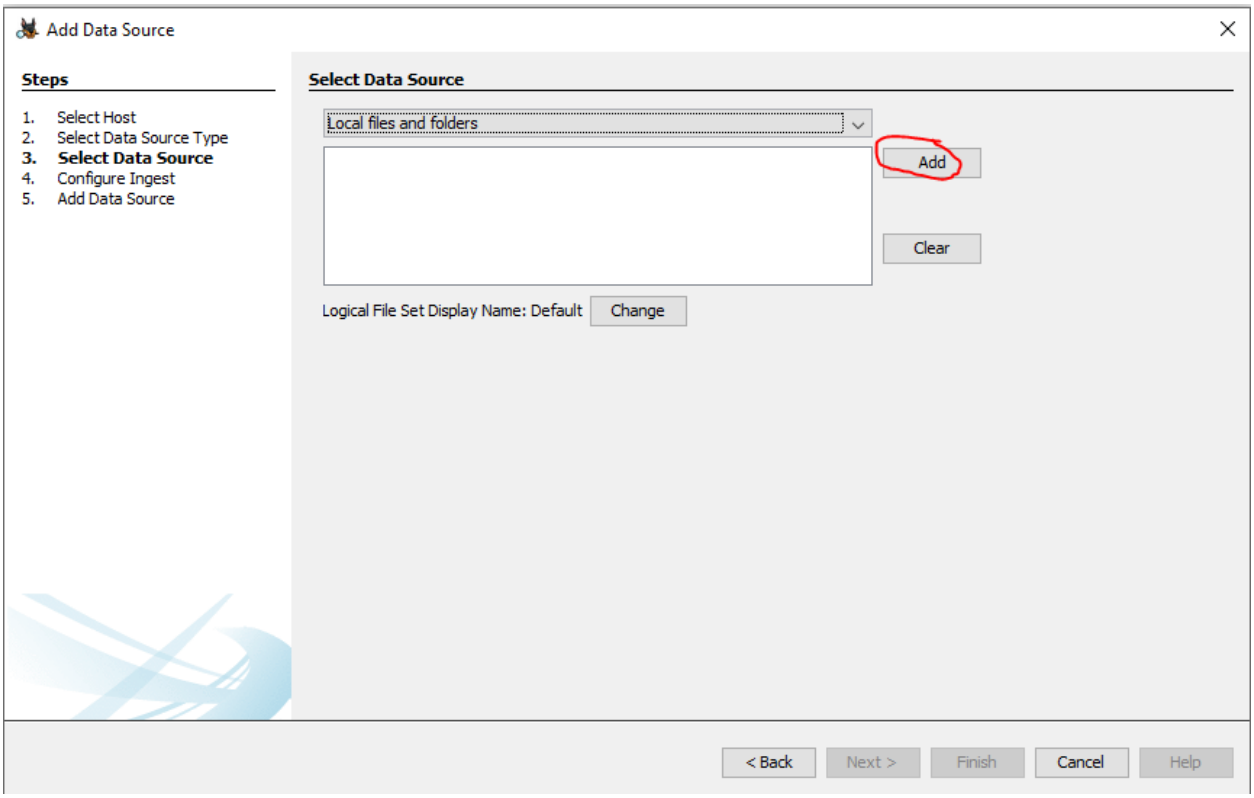


Figure 2.5: Alright, do we remember the file directory that we downloaded earlier? Still in its tar.gz form? We will ensure that we are looking at Local files and folders, as depicted above, and click on Add. When your file explorer pops up, go ahead, and identify your “bin.tar.gz” file and double click to add it to data source.

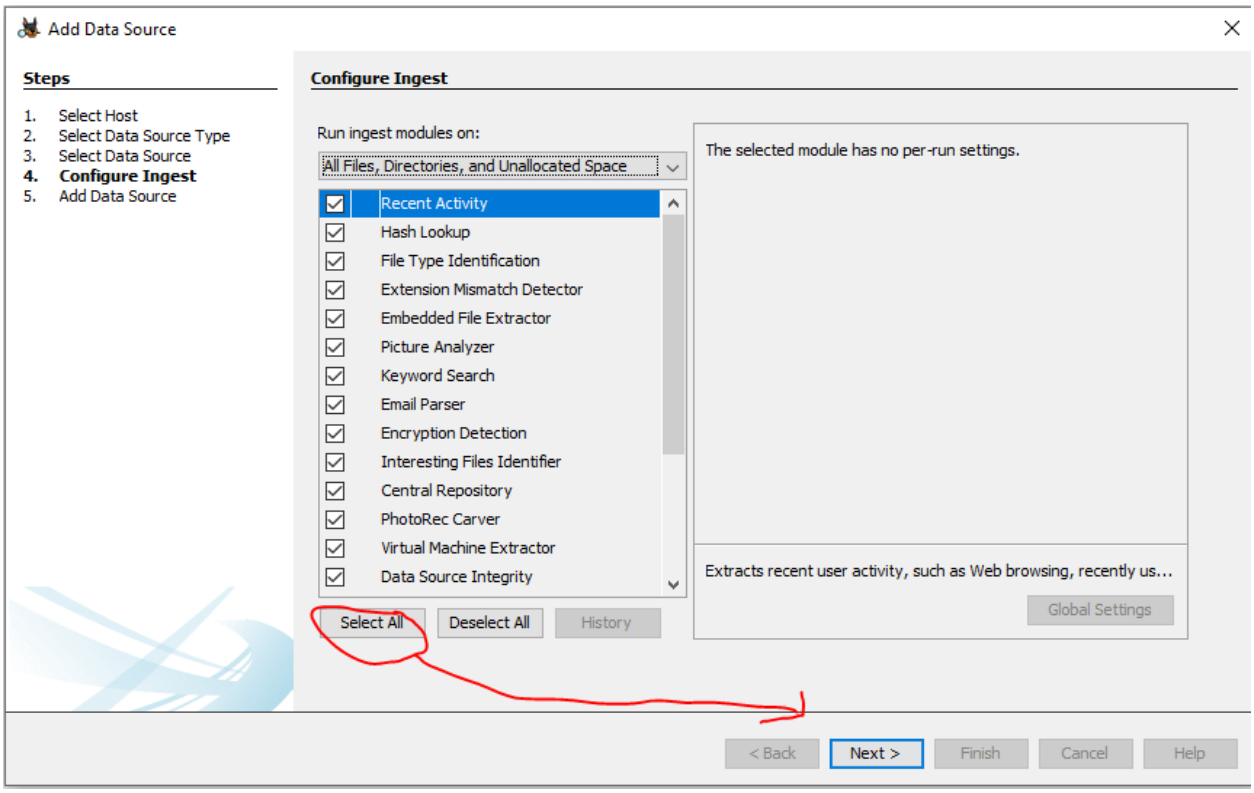


Figure 2.6: Alas, we arrive at another, somewhat, confusing step. Again, Autopsy has many different scanning options to meet the needs of modern cyber investigators and therefore, to get used to this application, I will have you click “Select All” and then Next. This will allow you, the student, to identify what each plugin or option does and further your understanding of the forensics process.

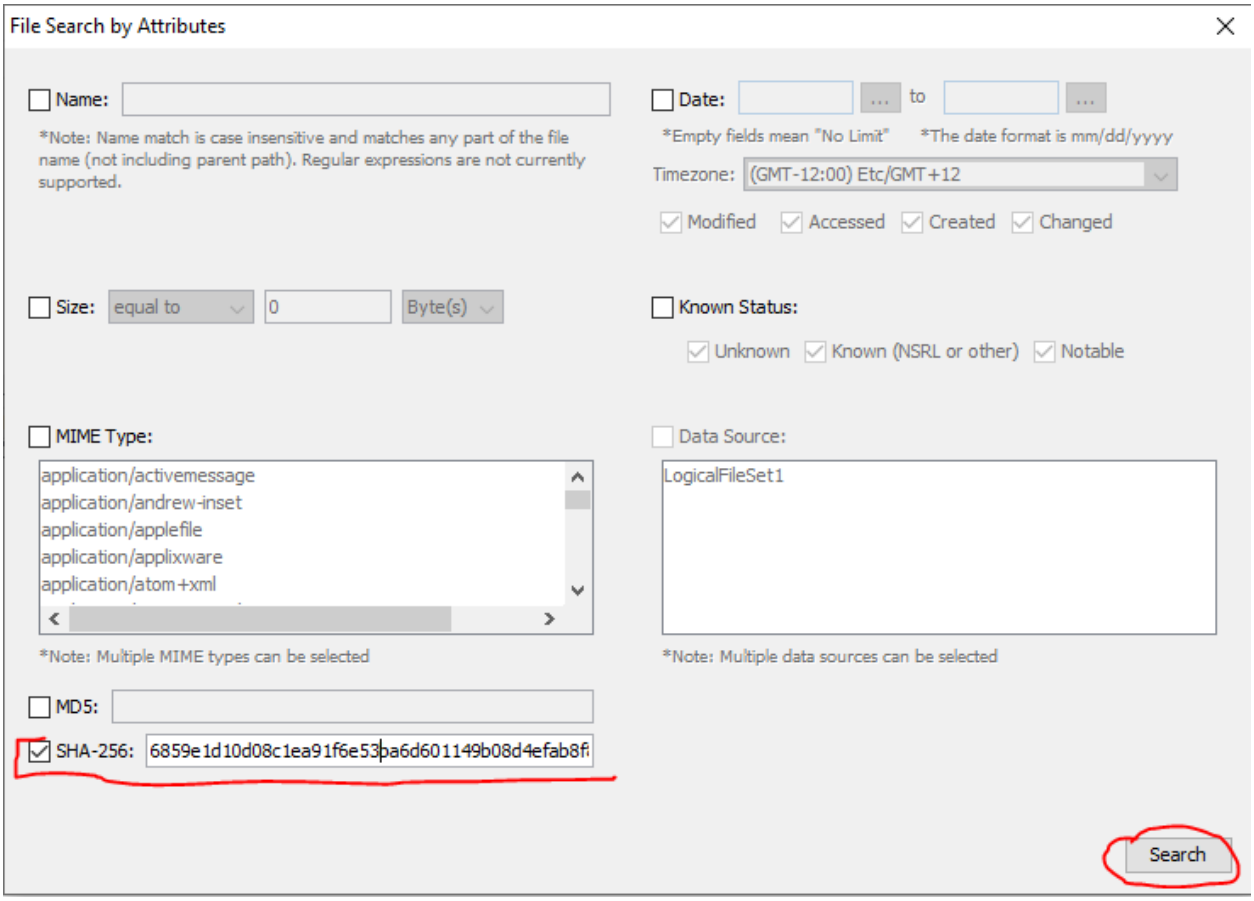


Figure 2.7: Alright, here is why having a known hash is wonderful. Click the “Tools” dropdown from the menu and click “File Search by Attributes”. We remember that we identified the known hash as SHA-256, so go ahead and check the box labeled “SHA-256”, copy and paste our hash into search bar. Click Search and watch the sparks fly 😊!

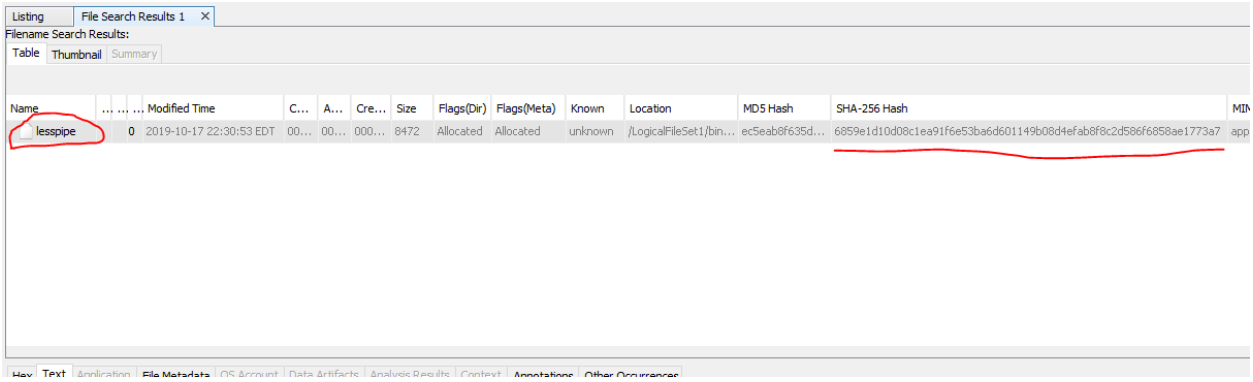
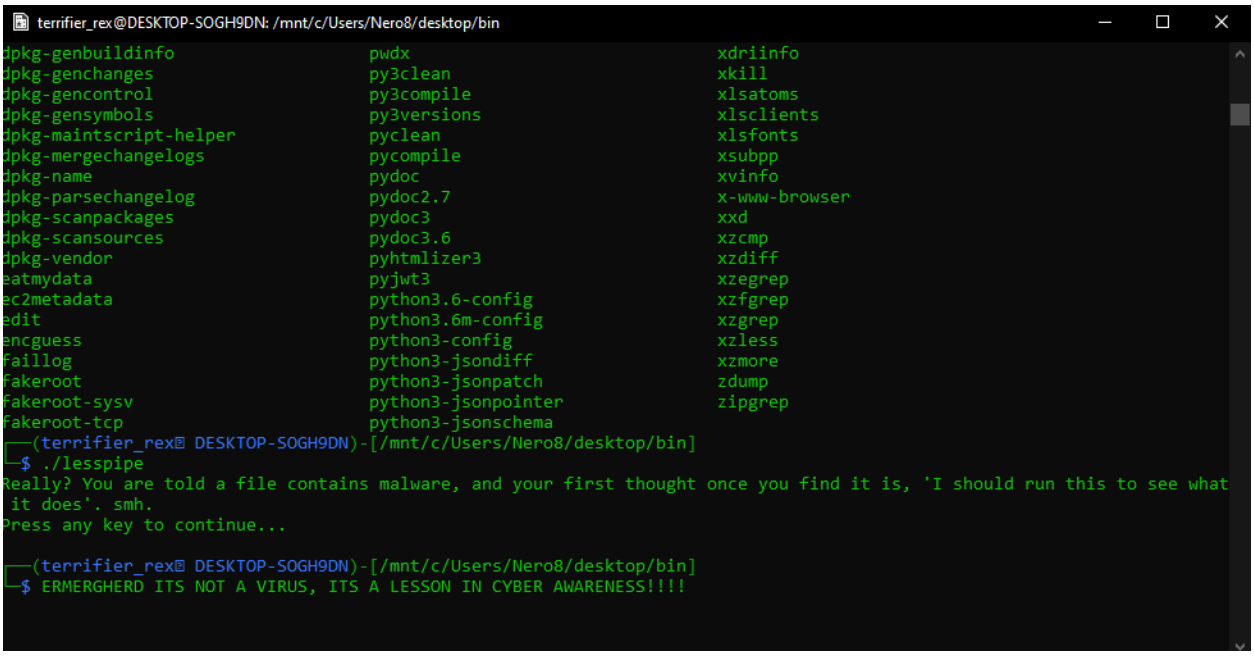


Figure 2.9: Once Autopsy completes the hash search, BOOM, we identified the malicious file and verified by the known hash. Mission complete! Our Flag is **Nero{lesspipe}**


terrifier_rex@DESKTOP-SOGH9DN: /mnt/c/Users/Nero8/desktop/bin
dpkg-genbuildinfo
dpkg-genchanges
dpkg-gencontrol
dpkg-gensymbols
dpkg-maintscript-helper
dpkg-mergechangelogs
dpkg-name
dpkg-parsechangelog
dpkg-scanpackages
dpkg-scansources
dpkg-vendor
eatmydata
ec2metadata
edit
encguess
faillog
fakeroot
fakeroot-sysv
fakeroot-tcp
pwdx
py3clean
py3compile
py3versions
pyclean
pycompile
pydoc
pydoc2.7
pydoc3
pydoc3.6
pyhtmlizer3
pyjwt3
python3.6-config
python3.6m-config
python3-config
python3-jsondiff
python3-jsonpatch
python3-jsonpointer
python3-jsonschema
xdriinfo
xkill
xlsatoms
xlsclients
xlsfonts
xsubpp
xvinfo
x-www-browser
xxd
xzcmp
xzdiff
xzegrep
xzfgrep
xzgrep
xzless
xzmore
zdump
zipgrep
┌──(terrifier_rex㉿ DESKTOP-SOGH9DN)-[/mnt/c/Users/Nero8/desktop/bin]
└─$ ./lesspipe
Really? You are told a file contains malware, and your first thought once you find it is, 'I should run this to see what it does'. smh.
Press any key to continue...
┌──(terrifier_rex㉿ DESKTOP-SOGH9DN)-[/mnt/c/Users/Nero8/desktop/bin]
└─$ ERMERGHERD ITS NOT A VIRUS, ITS A LESSON IN CYBER AWARENESS!!!!