CTF Skills - Forensics
Autopsy & Volatility

presented by Mandy Galante, NJCCIC Education Outreach Services
New Jersey Cybersecurity and Communications Integration Cell

Welcome! During the workshop:

- Please use Q&A for questions
- Please use Chat for whole group chat topics
- If you will be following along, start up your VM and your CyberStart Game.

Workshop Info - Forensics

Capture The Flag (CTF) competitions for CyberStart NCS and PicoCTF are coming up soon with opportunities for NJ students to shine and win prizes. Let's get ready! NJCCIC workshops will cover how to use key tools that the experts recommend for solving many CTF challenges.

- The files listed below are needed to follow the workshop demonstrations / slides. An active CyberStart Game license is necessary to access the CSGame files. To find each file, log in to your CSA account and go to the listed Base/Level/Challenge.
- These are BIG files that can take several hours to download. Make sure to save them into your Downloads folder in the CyberStart Virtual Machine.

1. CSGame, Forensics, L3C5 - memdump.zip this will be used to demo both L3C5 and L7C1
2. CSGame, Forensics, L4C3 - nairobi_cafe_suspect.zip.001, nairobi_cafe_suspect.zip.002, nairobi_cafe_suspect.zip.003
3. CSGame, Forensics, L7C5 - pc397 mem dump.zip
4. PicoGym, 2020 mini-competition, Pitter, Patter, Platter – suspicious.dd.sda1

Volatility

Runs on Windows and Linux, but these instructions are for using Volatility on the CyberStart VM. Command structure is different on Windows.

To get help: `vol.py --info`

FIRST step is to get the profile of the memory file. This tells Volatility what OS was running on the PC.

```
vol.py -f <memoryfile> imageinfo
```

Basic command syntax - assumes you are in the directory containing your memory file.

```
vol.py -f <memoryfile> --profile=<profile name> <plugin name>
```

CyberStart - Forensics: L3C5 Volatility

Briefing: When our team in New York came across a couple of PC's they thought might have been compromised by the hackers they took some memory dumps to analyze. Take a look at this one with a tool called Volatility and see if you can identify the running processes and see if you can spot any that look suspicious.

Tip: The suspicious process is the flag.

File: memdump.mem (5.4 GB unzipped) -- I renamed to L3C5memdump.mem

Hint: After identifying the correct profile, use Volatility to identify the process lists to see the flag.

CyberStart - Forensics:L3C5 Volatility

Syntax for Volatility

```
vol.py -f <memoryfile> --profile=<profilename> <plugin>
```

1. Find the memory profile using the imageinfo plugin
   ```
   vol.py -f memdump.mem imageinfo
   ```
2. Run the pslist plugin to list all processes
   ```
   vol.py -f memdump.mem --profile=Win81U1x64 pslist
   ```
3. Skim through the output to find the process name that looks unusual

CyberStart - Forensics:L7C1 Volatility

Briefing: Ok agent, first up we need to recover the NTLM hash of the administrator account. We've had one of the research team send you a memory dump to take a look at.

Tip: The hash is the flag

File: memdump.mem (5.4 GB unzipped) - same L3C5memdump.mem file

Hint: Think about the Volatility filters you may have used previously, as well as other plugins needed for a "hashdump".

CyberStart - Forensics:L7C1 Volatility

1. First we need to get the addresses of the registry hive files that hold password hash data - the System and the SAM hives. We will dump the registry hive offset addresses by using the hivelist plugin.

   ```
   vol.py -f memdump.mem --profile=Win81U1x64 hivelist
   ```

2. Use the virtual offsets for System and for SAM with the hashdump plugin.
   Here is the syntax:

   ```
   vol.py -f memdump.mem --profile=Win81U1x64 hashdump -s <virtual offset of SAM hive> -y <virtual offset of System hive>
   ```

3. Make sure to end the Volatility command by redirecting the output to a text file so it will be easy to read.

   ```
   vol.py -f memdump.mem --profile=Win81U1x64 hashdump -s 0xffffc0000bedb000 -y 0xffffc00006e2c000 > hash.txt
   ```

CyberStart - Forensics:L7C5 Volatility

Briefing: As part of the final report we're producing for the team, they've asked us to make a list of all the user accounts and passwords that have been used on one of the compromised machines. We have a memory dump from that machine, take a look and see what you can find.

Tip: Find the bad account and that will give you the flag.

File: *pc397 mem dump.zip* extracts to *memdump.mem* (2GB)

Hint: Mimikatz can be used with Volatility to gain certain important information.

CyberStart - Forensics:L7C5 Volatility

To install the Mimikatz plugin on the CSA Linux VM: copy the text from https://raw.githubusercontent.com/dfirfpi/hotoloti/master/volatility/mimikatz.py and paste it into a new text document. Save to the VM desktop as *mimikatz.py,* then move it to the plugins folder with this command:

```
sudo mv mimikatz.py /usr/lib/python2.7/site-packages/volatility/plugins/
```

Alternative: use a Kali Linux VM for memory challenges in level 7 and 8.

1. Find the memory profile using the imageinfo plugin

2. Run the mimikatz plugin to list account names and passwords
   vol.py memdump.mem --profile=Win7SP0x64 mimikatz

CyberStart - Forensics:L4C3 Autopsy

Briefing: Ok agent, slight change of plan with our investigation! Our team in Africa decided to swoop in and arrest one of the hackers when they saw him doing something they thought was especially suspicious whilst in a cafe in Nairobi. The only problem is he closed the file on his laptop before he was arrested. Can you help the team there figure out what file it was? They've sent the image file for you to take a look at.

Tip: Find the recent files and find the flag.

Files = nairobi_cafe_suspect.zip.001, nairobi_cafe_suspect.zip.002, nairobi_cafe_suspect.zip.003

Hint: Look at the recent documents folder on the user profile. Are there any suspicious looking files?

CyberStart - Forensics:L4C3 Autopsy

Change Share Screen
Advanced - Portion of Screen

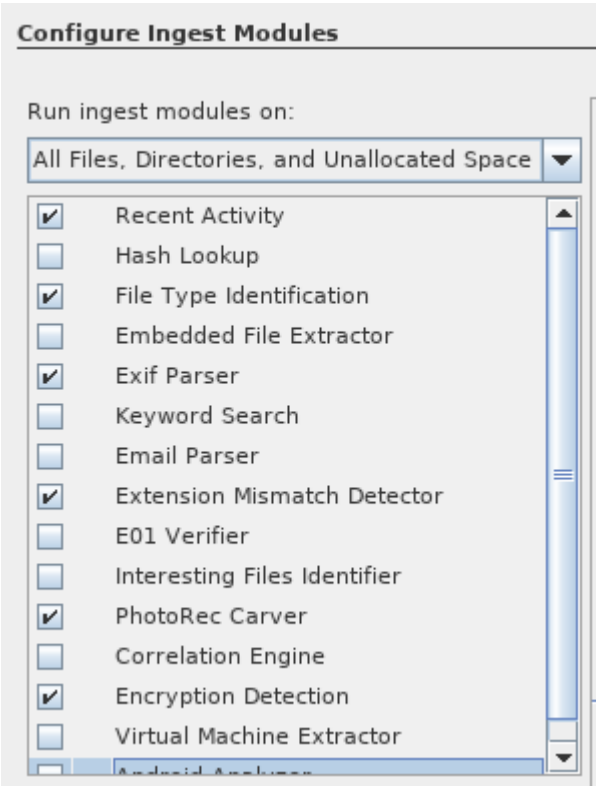
1. Make sure all the zipped files are in the same folder. Rightclick on the 001 file |Open Archive | Extract → it will merge the files and unzip

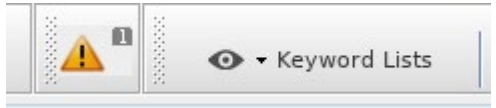
2. Open Autopsy | New Case | Name: CSA| Base Directory: /home/agent/Documents| Next (leave blanks)| Finish

3. Add Data Source screen comes up
Disk Image or VM | browse to the hacked_laptop.01 and select it | Next

4. Configure Ingest Modules screen comes up
recommend unchecking these to speed up| Next | Finish

5. Wait a few minutes to allow time for the Ingest Modules to produce results!! See Ingest Messages at top





CyberStart - Forensics:L4C3 Autopsy

1. In Autopsy, click on *Recent Documents* in left toolbar

2. Two interesting items:
   - C:\Users\Skidrow\Desktop\Flag\secrets.rtf
   - C: Users\Skidrow\AppData\Secrets\secrets.rtf

3. On each, rightclick | View File in Directory

4. Once in the directory with the file selected, look at the bottom section and click on the Strings tab. There you will see the text contents of the file.

PicoCTF - Pitter,Patter,Platters Autopsy

2020 Mini-competition

Description: 'Suspicious' is written all over this disk image.

File: suspicious.dd.sda1

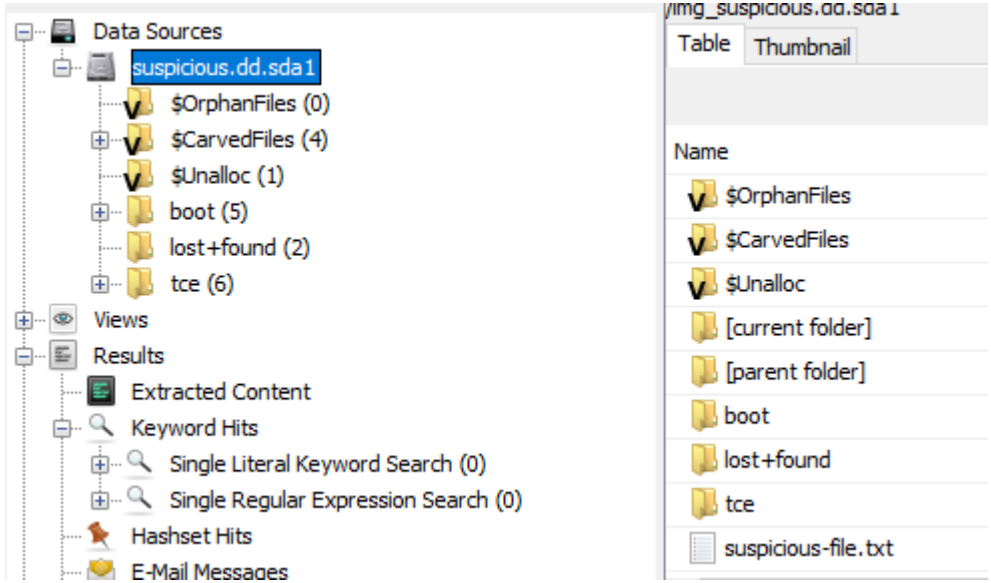
Hint 1: It may help to analyze this image in multiple ways: as a blob, and as an actual mounted disk.

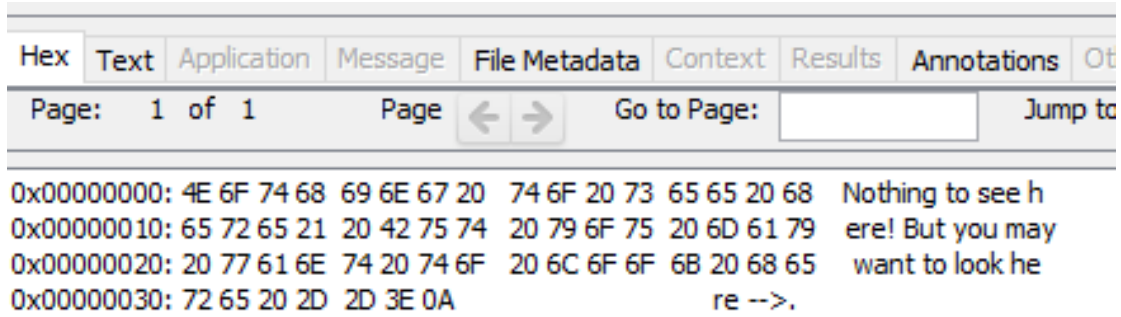
Hint 2: Have you heard of slack space? There is a certain set of tools that now come with Ubuntu that I'd recommend for examining that disk space phenomenon...

PicoCTF - Pitter,Patter,Platters Autopsy

2020 Mini-competition

1. Open Autopsy and create a new case.
2. In the Add Data Source section, select Disk Image or VM
3. When browsing for *suspicious.dd.sda1*, at the bottom of the screen in the Files of Type section you must change to All Files.
4. Complete the ingest modules section, click Finish to start viewing results.

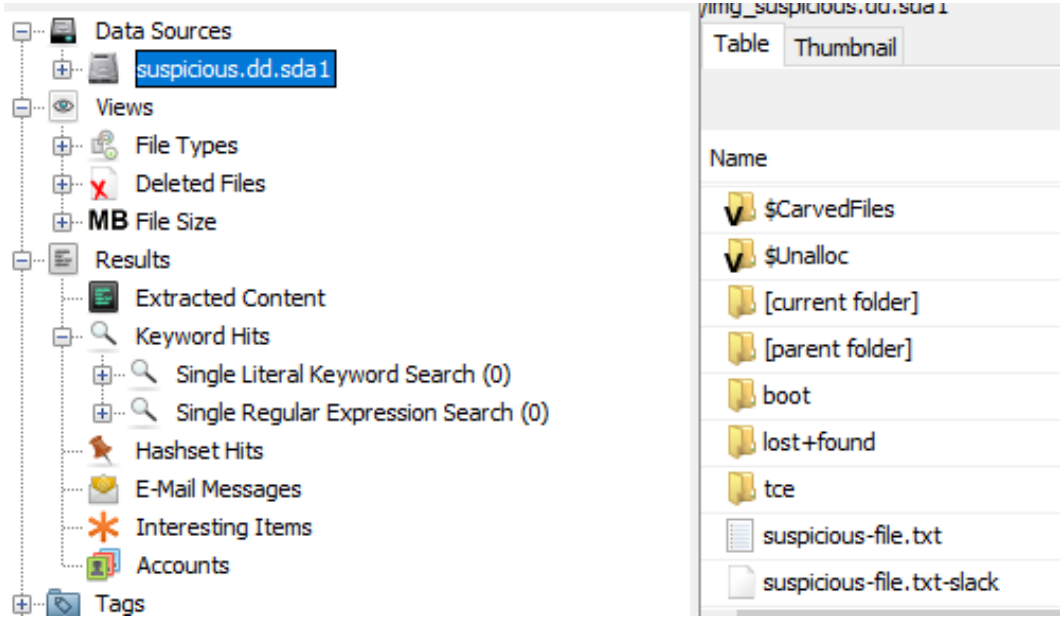




PicoCTF - Pitter,Patter,Platters Autopsy

2020 Mini-competition

1. Message and hints indicate we should be looking in the slack space for this file For that we need to change the settings in Autopsy.
2. Tools | Options | View | Uncheck both boxes in “Hide slack files in the” section Click Apply
3. You will now see a new file at the bottom of the list. Rightclick | Extract to save a copy on your computer.



Connect With Us

NJCCIC@CYBER.NJ.GOV

1-833-4-NJCCIC
(1-833-465-2242)

@NJCYBERSECURITY

CYBER.NJ.GOV