# Digital forensics: hands-on exercise (Scenario & Step by Step Guide)

July 13, 2021 (Tuesday), 11:00 – 11:45 am
Instructor: Claire Seungeun Lee, Ph.D. (UMass Lowell, claire_lee@uml.edu)

## HACKING CASE SCENARIO

On 09/20/04, a Dell CPi notebook computer, serial # VLQLW, was found abandoned along with a wireless PCMCIA card and an external homemade 802.11b antennae. It is suspected that this computer was used for hacking purposes, although cannot be tied to a hacking suspect, G=r=e=g S=c=h=a=r=d=t. (The equal signs are just to prevent web crawlers from indexing this name; there are no equal signs in the image files.) 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 (like Starbucks and other T-Mobile Hotspots) where he would then intercept internet traffic, attempting to get credit card numbers, usernames & passwords.

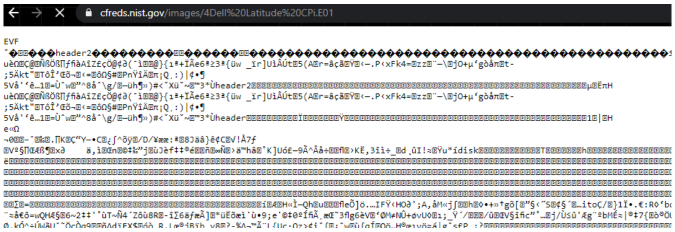
Find any hacking software, evidence of their use, and any data that might have been generated. Attempt to tie the computer to the suspect, G=r=e=g S=c=h=a=r=d=t.

A DD image (in seven parts: 1, 2, 3, 4, 5, 6, 7, 8, and notes) and a EnCase image (second part) of the abandoned computer have already been made.

**For this session, we will only use** a EnCase image (second part) (PC.E01 & PC.E02)**.**

Source: NIST (2018). https://www.cfreds.nist.gov/Hacking_Case.html.

## Snapshot of data we're using



cfreds.nist.gov/images/4Dell%20Latitude%20CPi.E01

```
EVF
header2
uèΩC@Ñßöß∏ƒﬁàAîZ£çÖ@¢∂(ˆì@}{ı²+ÏÃe6²≥3²{üw _ïr]UìÂÚt5(Ar=âçãŸ‹–.P‹xFk4=zz¨–\jO+µ'gòåπt-
;5Äkt"TôÎ'Œõ¬‹=ôΩ§#PnŸîÄπ¡Q.:)|¢•¶
5Vå''ê…1=Ùˆw"^8åˆ\g/–üh¶»)#<˘Xü˘~™3*Ùheader2µËπH
uèΩC@Ñßöß∏ƒﬁàAîZ£çÖ@¢∂(ˆì@}{ı²+ÏÃe6²≥3²{üw _ïr]UìÂÚt5(Ar=âçãŸ‹–.P‹xFk4=zz¨–\jO+µ'gòåπt-
;5Äkt"TôÎ'Œõ¬‹=ôΩ§#PnŸîÄπ¡Q.:)|¢•¶
5Vå''ê…1=Ùˆw"^8åˆ\g/–üh¶»)#<˘Xü˘~™3*ÙheaderÏŸ1|H
e«Ω
¬0–˘.∏KC"Y–•C¿∫^õÿ/D/¥ææ:²8Jäâ}ê¢C√!Å7ƒ
V º§∏Œß¶x∂    ä,ìŒn0‡‰"jùJèf‡‡®éñ∞Ñ›ä™hâ˚K]Uó£–9Ã^Âå÷ﬂ›KË,3îì÷_d ̧ûI!≈Ÿu*ídiskTh
ë
∑=íÆH«Ì–QhuﬂeÕ]ö.…IFŸ‹HO∂';A,åM«j∫h0•+»†gõ["§‹˝S¢§´…itoÇ/}1Ï•.€:R0'b
¨≈å€ô=wQHÆ§6~2‡‡''ùT~Ñ4´Zôù8R-î∑6äƒæÃ]*üËõæì'ù•9;e'©‡0ºÍﬁÃ¸æŒ˜3ﬂg6èV'ØM≠NÛ+øvU0ı;_Ÿ´/ /ûŒV§îﬁc"˚…j/Ù≤û'Æg¨ºbMÉ≈|®‡7{ò®Ö
```

## Tool we're using: Autopsy

Link: https://www.autopsy.com/
MacOS: https://github.com/DuffyAPP-IT/Autopsy-macOS-Install

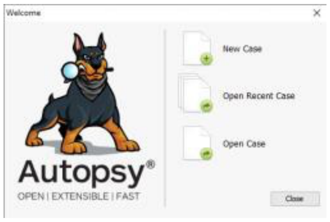
**Create a folder: "Hacking case"**
**Image files to use: EnCase image files ("E01" & "E02")**

## STEP-BY-STEP GUIDE

### 1. Launch Autopsy and create a "New Case"

(Pre-requisite: Install the software (it's already installed on your VM))

a. Click "new case"



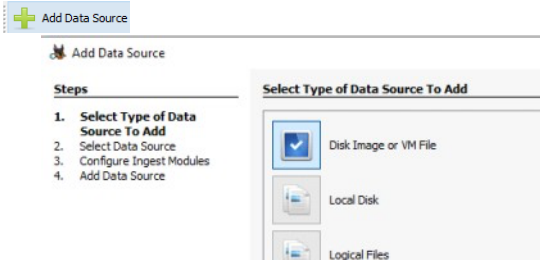
b. Click next

c. Click finish to create the case

d. Now that you have an empty case, click the "Add data source" button in the top left

### 2. Add Data Source

a. Choose "Disk image or VM file" in the popup



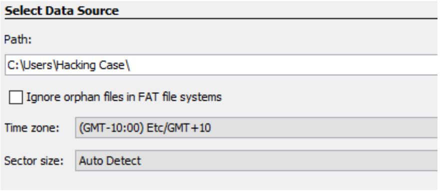
Steps

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

b. For the path, choose the .E01 file we downloaded with PowerShell earlier

- As long as both files (.E01 and .E02) are in the same folder Autopsy will automatically ingest both and give you the full image For the Time Zone choose (GMT -10:00) Etc/GMT+10



Select Data Source

Path:

C:\Users\Hacking Case\

□ Ignore orphan files in FAT file systems

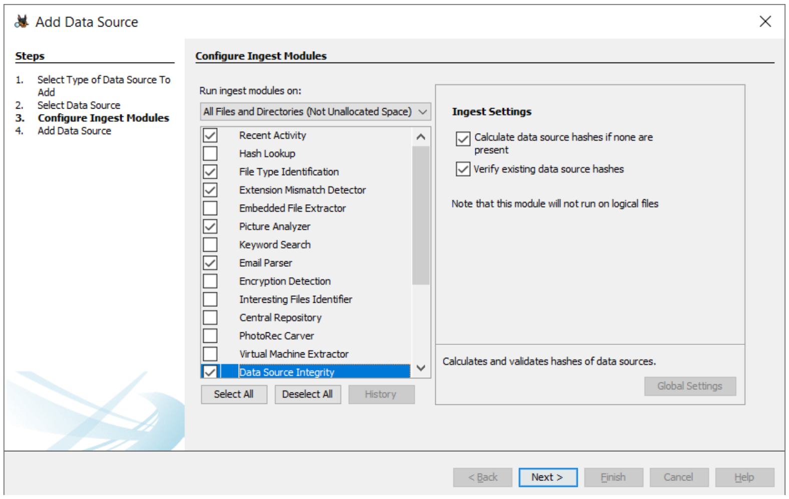
Time zone: (GMT-10:00) Etc/GMT+10

Sector size: Auto Detect

c. Click next

d. The next screen lets you choose ingest modules

- An ingest module takes the data in the image and parses it for various types of information such as most recently accessed programs and email addresses
- Just select all so we have everything. (This file is not too large and you can work while the modules run.)
- Since this session has a time limit, we would select only 6 modules on the 'Not Unallocated Space'.



Add Data Source

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 and Directories (Not Unallocated Space)

☑ Recent Activity
□ Hash Lookup
☑ File Type Identification
☑ Extension Mismatch Detector
□ Embedded File Extractor
☑ Picture Analyzer
□ Keyword Search
☑ Email Parser
□ Encryption Detection
□ Interesting Files Identifier
□ Central Repository
□ PhotoRec Carver
□ Virtual Machine Extractor
☑ Data Source Integrity

**Ingest Settings**

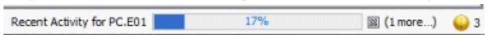
☑ Calculate data source hashes if none are present
☑ Verify existing data source hashes

Note that this module will not run on logical files

Calculates and validates hashes of data sources.

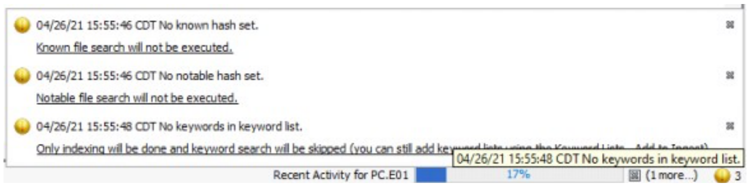
e. You can click each module to read what it looks for

- As the modules run you can get any alerts or progress from two different places in Autopsy The bottom right will show you the module being run as well as the progress



Recent Activity for PC.E01 17% (1 more...) 3

- Clicking on the symbol in the bottom right of this shows you any notifications form the modules



04/26/21 15:55:46 CDT No known hash set.
Known file search will not be executed.

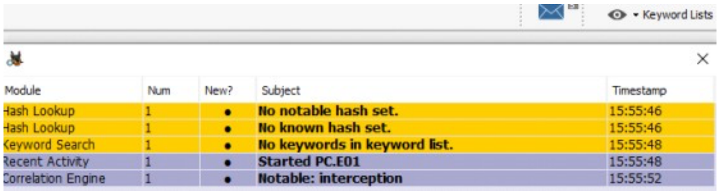
04/26/21 15:55:46 CDT No notable hash set.
Notable file search will not be executed.

04/26/21 15:55:48 CDT No keywords in keyword list.
Only indexing will be done and keyword search will be skipped (you can still add ke

04/26/21 15:55:48 CDT No keywords in keyword list.

Recent Activity for PC.E01 17% (1 more...) 3

- The envelope symbol near the top right corner will show you all of the notifications from all of the modules



| Module | Num | New? | Subject | Timestamp |
|---|---|---|---|---|
| Hash Lookup | 1 | • | **No notable hash set.** | 15:55:46 |
| Hash Lookup | 1 | • | **No known hash set.** | 15:55:46 |
| Keyword Search | 1 | • | **No keywords in keyword list.** | 15:55:48 |
| Recent Activity | 1 | • | **Started PC.E01** | 15:55:48 |
| Correlation Engine | 1 | • | **Notable: interception** | 15:55:52 |

## SCENARIO AND PRACTICE QUESTIONS

**1. What is the image hash? Does the acquisition and verification hash match?**

**2. What operating system was used on the computer?**

**3. When was the install date?**

**4. Who is the registered owner?**

**5. What is the computer account name?**