After the Incident:
DIY Forensic Collection

Eugene Filipowicz
About me:

- Name: Eugene Filipowicz
- “Grew up” in Florida
- Currently resides in the GTA
- Graduated from Florida State University (FSU) with Undergraduate and Master’s degree
- Graduated from Sheridan College in Ontario with Bachelor degree in Applied Information Sciences, (Information Systems Security)
About me (continued):

- Active member of the Ontario Chapter of HTCIA
- Active member of IACIS - earned CFCE
- Employed at Duff & Phelps as a Computer Forensic Consultant
- Teaches Digital Forensics at Sheridan College
Why conduct a forensic collection?

Example Scenarios

An Employee:

• quits and takes intellectual property to new employer
• is suspected of fraud / embezzlement
• is alleged to have violated corporate usage policy
• is believed to have sent threatening messages to co-workers
You think that’s air that you’re breathing now?
**Spoilation** of evidence refers to intentional or negligent withholding, hiding, alteration, or destruction of evidence relevant to a legal proceeding.
Forensic best practices help to insure that Electronic Evidence:
- is not altered or destroyed
- is properly preserved and protected
- can be authenticated
- is maintained with a chain of custody

In computer forensics, there are often exceptions to standard policy/procedures. Document and explain any deviation from standard practices.
• Testing of *methodology* and *tools*
• Have proper *authorization*

• Take *notes*
• Gather relevant case information
• *Photograph*
• Forensic *acquisition*
• *Verification*

• Make *backup copies* of all forensic images
• Conduct any analysis on the forensic image, never the original source
Take Notes / Document the entire process
Gather information
Access the situation and the device.
Forensic Acquisition

Obtaining all data from the original source and record to a controlled destination drive, while assuring the source is not changed/modified.
• Keep the evidence *secure*
• Assure *no changes are made* to the source during collection

• Acquire a *byte-for-byte* copy of source media

• Confirm the source data and the data copied to the destination are exactly the same
• *Cryptographic hash functions* (MD5, SHA1)
Create a bootable USB stick w/ a forensic Linux “distro”

**CAINE**
http://www.caine-live.net/

**DEFT**
http://www.deftlinux.net/

**KALI**
https://docs.kali.org/general-use/kali-linux-forensics-mode

**PALADIN EDGE**
https://sumuri.com/product/paladin-64-bit-version-7/

“Roll your own” Linux “Distro”
Forensic Distros

- likely use a forensic version of "dd" $\rightarrow$ dc3dd
- "Guymager" is a Linux only application for forensic imaging and works very well with nice features
- Know how "write-blocking" is implemented, and what you need to do to assure source devices are not changed/modified
- There are many more "forensic distros" available:
  - command line only
  - GUI
  - Lite-weight
  – do your research.
Do you want to know
Determine how to boot from USB from the device you want to image.
<Select Source Device>
/dev/sda INTEL SSDSC2BW180A3L 167.68GB
/dev/sda1 INTEL SSDSC2BW180A3L ________ 167.68GB ntfs
/dev/sdb USB Flash Disk 7.47GB
/dev/sdb1 USB Flash Disk PALADIN_7_0 7.47GB vfat
/dev/sdc STORE N GO 14.60GB
/dev/sdc1 STORE N GO EV1DENCE 14.60GB vfat
Classification of Storage Formats for Digital Evidence

Forensic Backup (Image)
Forensic Copy
Forensic Evidence Files
RAW, dd, “flat” File
Application specific formats (E01)
Standard
Compressed
Encrypted
Source
(Original/Evidence Drive)

Destination
(Forensic Backup)

Forensic Copy

RAW, dd, “Flat file”

E01
<table>
<thead>
<tr>
<th>Source</th>
<th>Destination</th>
</tr>
</thead>
<tbody>
<tr>
<td>/dev/sda INTEL SSDSC2BW180A3L 167.68GB</td>
<td>/dev/sdc1 STORE N GO EV1DENCE 14.60GB vfat</td>
</tr>
<tr>
<td></td>
<td>/dev/sdd1 ST500LM012 HN-M500MBB FORENSIC-CLASS 465.76GB ntfs</td>
</tr>
</tbody>
</table>
Status: at 1.5% acquirer 2.5 GiB (2775285760 bytes) of total 167 GiB (180045768656 bytes) completion in 59 minute(s) and 37 second(s) with 47 MiB/s (49558427 bytes/second)
Live Acquisition
ENCRYPTION
Getting it to work...

To think about:

• Encryption
  • What type of encryption, what vendor or application implements it?
  • Do you have the KEY?
  • Can it be turned off?

• Live boot Linux Distro:
  • Can you get it to boot?
  • Secure Boot, TPM, UEFI

• Administrator access
  • Turn off encryption
  • Login for “Live acquisition

• TESTING on duplicate hardware with same software install
FTK Imager

• FTK Imager Lite
  http://www.accessdata.com/product-download
  (lite version intended to be portable – no installation)

• FTK Imager (latest version)
  • May be able to use
  • may have to add your own .dll files
  • test on your systems
Evidence Item Information

Case Number: SECTOR 2017
Evidence Number: 0002
Unique Description: Other_Custodian
Examiner: Eugene Filipowicz
Notes: Lenovo Laptop
Two types of data acquisition:

• **Static acquisition (“Dead Box”)**
  
  Copying a hard drive from a powered-off system
  
  – This is the STANDARD method of forensic collections
  
  – Does not alter the data, repeatable

• **Live acquisition**
  
  Copying data from a running computer
  
  – *Sometimes* needed (EX: of hard disk encryption
    
    – you do not have the passcode/key)
  
  – alters the data on the source
  
  – Not repeatable (hashes between collections are different)
  
  – FYI: RAM data collection often done at this time
I know Kung-Fu.

功夫

...and I know how to do my own forensic collection!
Testing and Practice
QUESTIONS?