FIRST RESPONDER FORENSICS

or

Can I Pull the Plug Now…?

Mick Walsh
Special Agent
United States Secret Service
Miami Electronic Crimes Task Force

THE U.S. SECRET SERVICE

Created in 1865 at the end of the U.S. Civil War to stop counterfeiting of currency

Began protecting U.S. Presidents in 1901 after the assassination of President William McKinley

THE U.S. SECRET SERVICE

Investigates...

Counterfeit currency

Fraud involving U.S. financial obligations and securities

Crimes affecting other federally insured financial institutions

Threats against the President & other government officials

Telecommunications fraud

Access Device fraud

Identity fraud

Computer fraud

MY BACKGROUND

- Computer Forensic Examiner since 1998
- Managed U.S. Secret Service’s Network Intrusion Responder (NITRO) program from 2006 to 2008
- Currently manage the Miami Electronic Crimes Task Force

THIS PRESENTATION

Not intended as a comprehensive overview of the subject

Not a detailed technical study

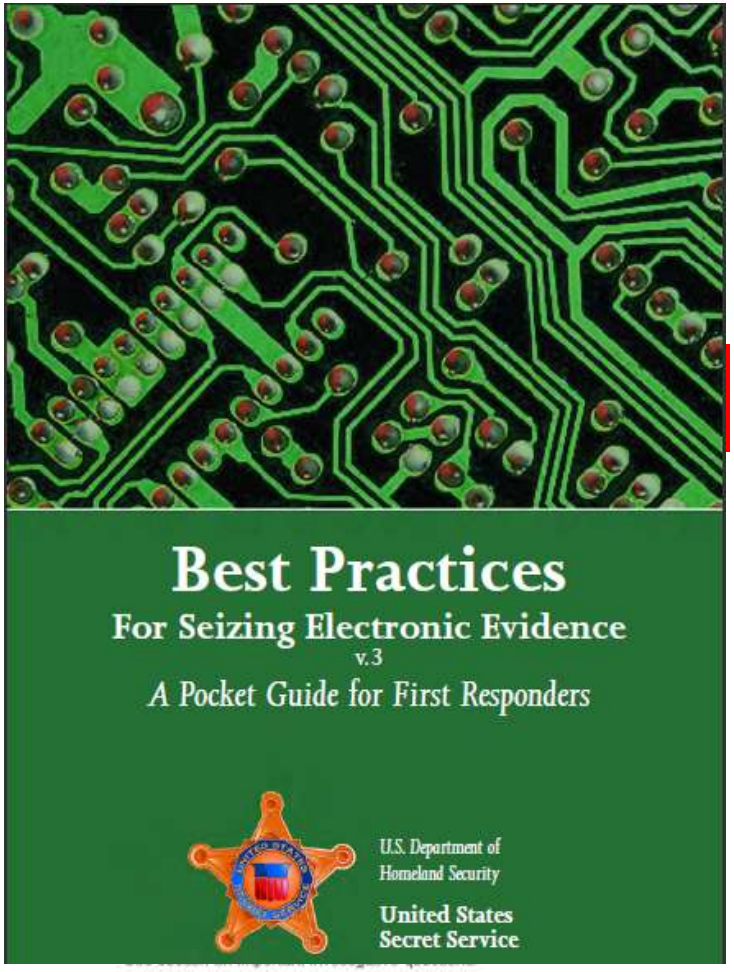
Not the methodology used by most of U.S. Secret Service

IS one laboratory’s practical solution to a problem

FIRST RESPONDER FORENSICS

the OLD way…

Best Practices For Seizing Electronic Evidence: A Pocket Guide for First Responders (2006)



Best Practices

For Seizing Electronic Evidence

v.3

A Pocket Guide for First Responders

U.S. Department of
Homeland Security

United States
Secret Service

Electronic Crime Scene Investigation: A Guide for First Responders (2008)

APR. 08

U.S. Department of Justice
Office of Justice Programs
National Institute of Justice

NIJ

Special REPORT

Electronic Crime Scene Investigation:
A Guide for First Responders, Second Edition

www.ojp.usdoj.gov/nij

WHY NOT JUST PULL THE PLUG?

That worked for us in the past.

Most of the time it still does. But what if…

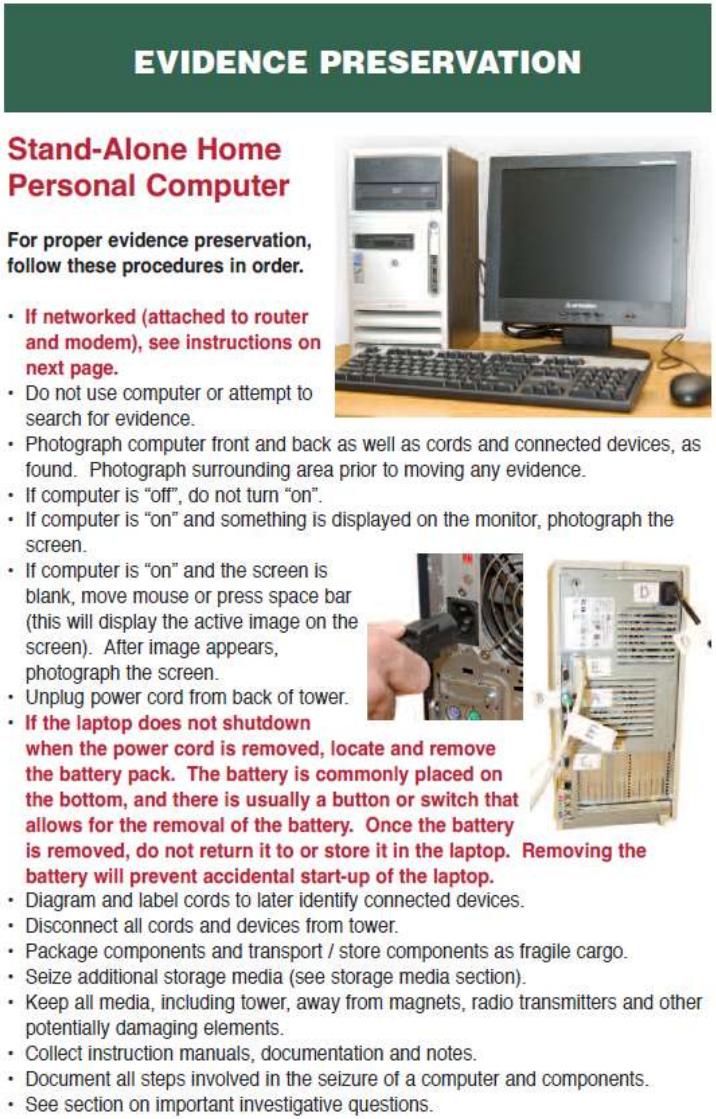
The hard drive is encrypted?

The evidence is on a remote networked device?

The computer has several GB of RAM?

* 2 GB = approximately 100,000 pages

OK, SO WHAT SHOULD I DO NOW?



EVIDENCE PRESERVATION

Stand-Alone Home Personal Computer

For proper evidence preservation, follow these procedures in order.

- **If networked (attached to router and modem), see instructions on next page.**
- Do not use computer or attempt to search for evidence.
- Photograph computer front and back as well as cords and connected devices, as found. Photograph surrounding area prior to moving any evidence.
- If computer is “off”, do not turn “on”.
- If computer is “on” and something is displayed on the monitor, photograph the screen.
- If computer is “on” and the screen is blank, move mouse or press space bar (this will display the active image on the screen). After image appears, photograph the screen.
- Unplug power cord from back of tower.
- **If the laptop does not shutdown when the power cord is removed, locate and remove the battery pack. The battery is commonly placed on the bottom, and there is usually a button or switch that allows for the removal of the battery. Once the battery is removed, do not return it to or store it in the laptop. Removing the battery will prevent accidental start-up of the laptop.**
- Diagram and label cords to later identify connected devices.
- Disconnect all cords and devices from tower.
- Package components and transport / store components as fragile cargo.
- Seize additional storage media (see storage media section).
- Keep all media, including tower, away from magnets, radio transmitters and other potentially damaging elements.
- Collect instruction manuals, documentation and notes.
- Document all steps involved in the seizure of a computer and components.
- See section on important investigative questions.

…

tion

mage?

ked data storage

mage?

ull the plug! (maybe)

Who is a “First Responder”?

- Can identify the general type of setup

  Personal Computer? Stand alone or Networked? Server?

- Can identify the likely operating system

  Windows? Apple? Linux? Other?

- Is trained to use simple forensic software

  Including command-line software

3 Levels of Training in the Secret Service

- Computer forensic examiners

- Network intrusion investigators

- Other agents who’ve taken a basic course in computer crime investigations

SOFTWARE

This is what we need…

1. Image RAM
2. Detect encryption
3. Detect networked data storage

This is what we want…

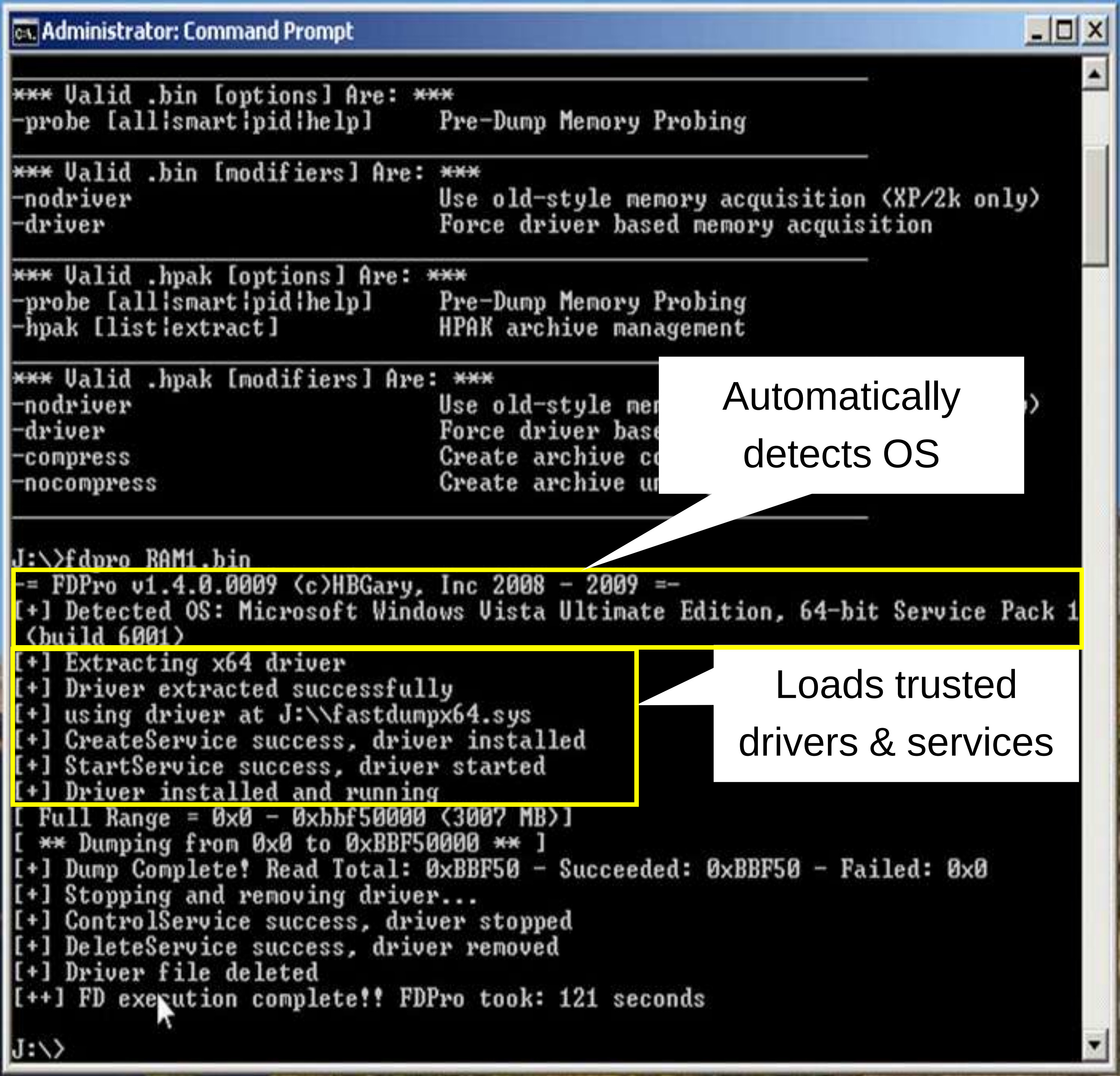
- Fewest number of tools possible to cover every situation
- Reliable
- Easy to use
- Small “footprint”
- Only trusted files are executed
- Can be run from different types of media

#1 Image RAM

Lots of RAM imaging tools available...

My forensic lab uses **FastDump Pro** by HBGary, Inc.

- Supports all versions of Windows, all service packs, 32 & 64 bit
- Images up to 64 GB of RAM
- Relatively easy to use
- Small “footprint” in memory
- Also acquires the pagefile
- Loads its own trusted drivers & services
- Low cost for Pro version
- “Community Edition” is less capable, but it’s free



```
*** Valid .bin [options] Are: ***
-probe [all|smart|pid|help]      Pre-Dump Memory Probing

*** Valid .bin [modifiers] Are: ***
-nodriver                        Use old-style memory acquisition (XP/2k only)
-driver                          Force driver based memory acquisition

*** Valid .hpak [options] Are: ***
-probe [all|smart|pid|help]      Pre-Dump Memory Probing
-hpak [list|extract]             HPAK archive management

*** Valid .hpak [modifiers] Are: ***
-nodriver                        Use old-style me                              )
-driver                          Force driver base
-compress                        Create archive co
-nocompress                      Create archive un

J:\>fdpro RAM1.bin
-= FDPro v1.4.0.0009 (c)HBGary, Inc 2008 - 2009 =-
[+] Detected OS: Microsoft Windows Vista Ultimate Edition, 64-bit Service Pack 1
 (build 6001)
[+] Extracting x64 driver
[+] Driver extracted successfully
[+] using driver at J:\\fastdumpx64.sys
[+] CreateService success, driver installed
[+] StartService success, driver started
[+] Driver installed and running
[ Full Range = 0x0 - 0xbbf50000 (3007 MB)]
[ ** Dumping from 0x0 to 0xBBF50000 ** ]
[+] Dump Complete! Read Total: 0xBBF50 - Succeeded: 0xBBF50 - Failed: 0x0
[+] Stopping and removing driver...
[+] ControlService success, driver stopped
[+] DeleteService success, driver removed
[+] Driver file deleted
[++] FD execution complete!! FDPro took: 121 seconds

J:\>
```

Automatically detects OS

Loads trusted drivers & services

#2 Detect Encryption

CryptHunter by the CERT Software Engineering Institute at Carnegie Mellon University detects whole disk encryption, as well as encrypted volumes and encrypted virtual disks.

- Works on Windows NT, 2000, XP, 2003 and Vista

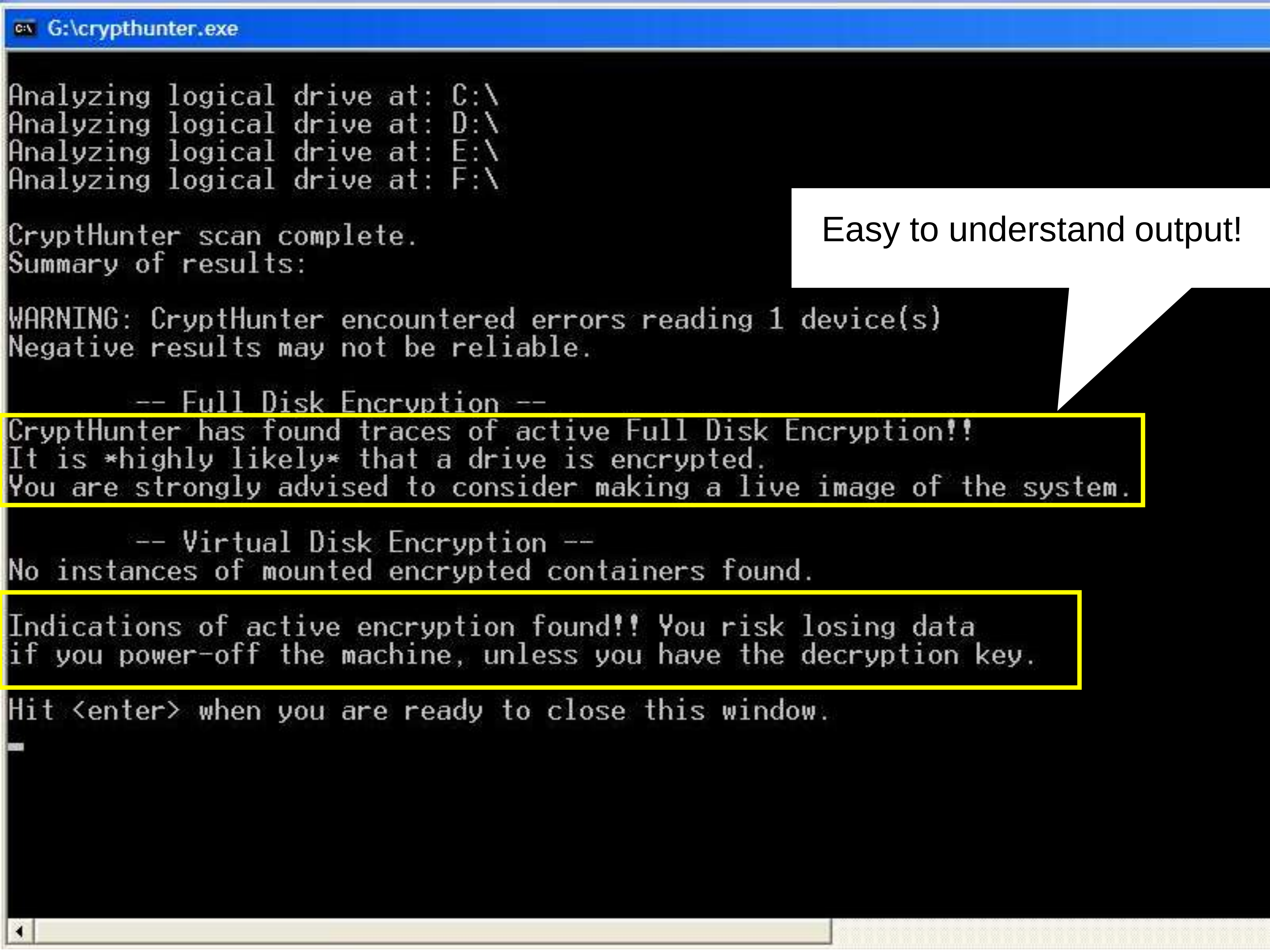
- Relatively easy to use

- Easy to understand output

- Small “footprint”

- Creates a detailed log of files “touched” by CryptHunter

- It’s free for use by law enforcement!



```
Analyzing logical drive at: C:\
Analyzing logical drive at: D:\
Analyzing logical drive at: E:\
Analyzing logical drive at: F:\

CryptHunter scan complete.
Summary of results:

WARNING: CryptHunter encountered errors reading 1 device(s)
Negative results may not be reliable.

        -- Full Disk Encryption --
CryptHunter has found traces of active Full Disk Encryption!!
It is *highly likely* that a drive is encrypted.
You are strongly advised to consider making a live image of the system.

        -- Virtual Disk Encryption --
No instances of mounted encrypted containers found.

Indications of active encryption found!! You risk losing data
if you power-off the machine, unless you have the decryption key.

Hit <enter> when you are ready to close this window.
```

Easy to understand output!

Image the RAM (again???)

It’s *possible* that passwords, encryption keys, and other very useful data can be found in RAM.

RAM contents changes frequently, so it’s recommend you image RAM several times. Multiple images means more string cross references, code regions, etc., for analysis.

That increases the likelihood that you’ll uncover passwords, encryption keys, and other data you might be looking for.

Time to Call for Help?

It’s decision time…

Is the First Responder proficient with live imaging of hard drives?

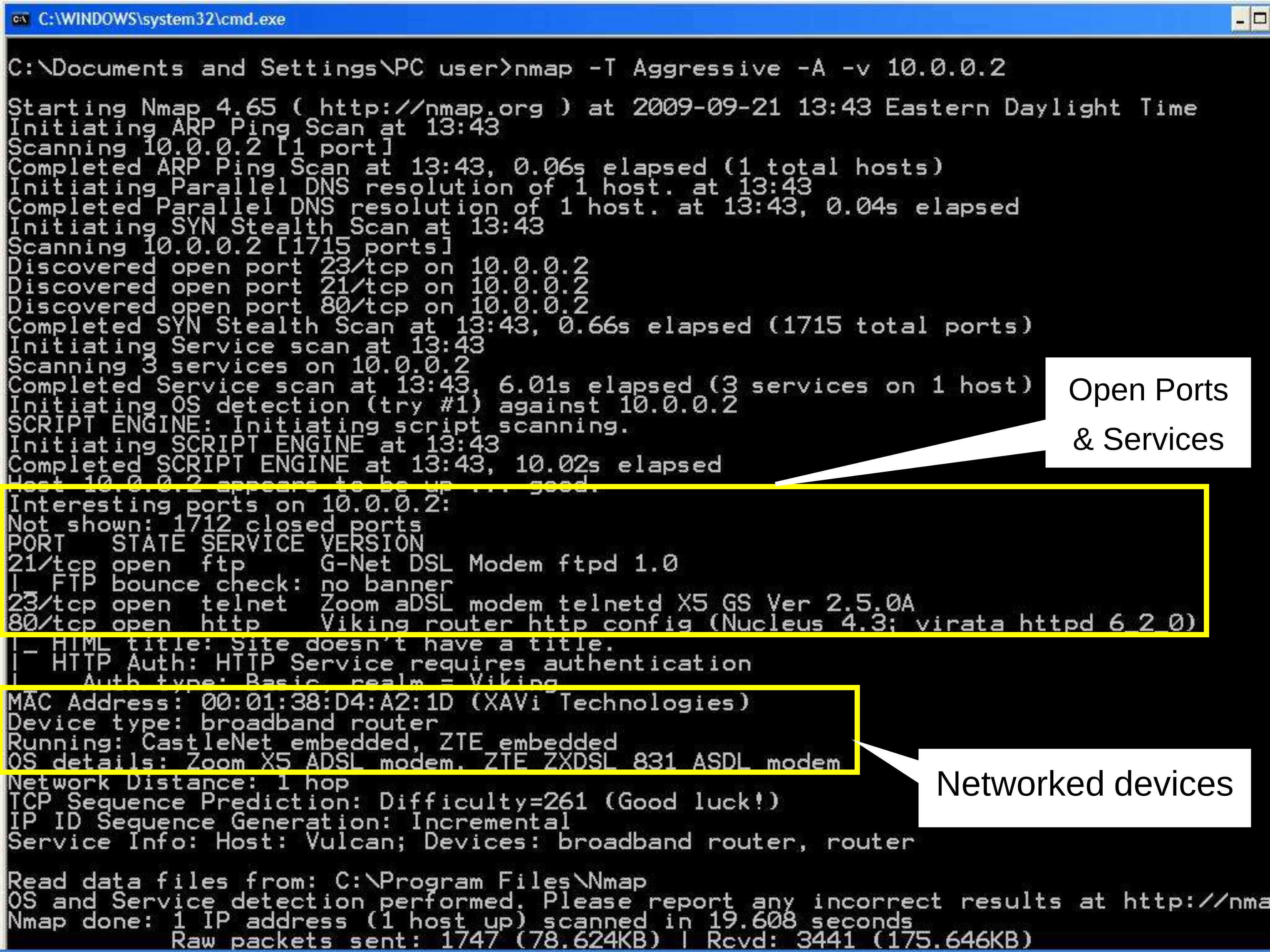
Yes – make a logical image

No – call someone who can…

#3 Detect networked data storage

Nmap is an open source utility for network mapping & security auditing. It shows hosts available on the network, what services the hosts are offering, operating systems, open ports, devices, etc.

- Runs on Windows NT, ME, 2000, XP, 2003 and Vista
- Not exactly easy to use, but the basics can learned fairly quickly
- Straightforward output
- Small “footprint”
- Downside – free version must install WinPcap & MS Visual C++
- Can buy a version that runs directly from CD or USB



```
C:\Documents and Settings\PC user>nmap -T Aggressive -A -v 10.0.0.2

Starting Nmap 4.65 ( http://nmap.org ) at 2009-09-21 13:43 Eastern Daylight Time
Initiating ARP Ping Scan at 13:43
Scanning 10.0.0.2 [1 port]
Completed ARP Ping Scan at 13:43, 0.06s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 13:43
Completed Parallel DNS resolution of 1 host. at 13:43, 0.04s elapsed
Initiating SYN Stealth Scan at 13:43
Scanning 10.0.0.2 [1715 ports]
Discovered open port 23/tcp on 10.0.0.2
Discovered open port 21/tcp on 10.0.0.2
Discovered open port 80/tcp on 10.0.0.2
Completed SYN Stealth Scan at 13:43, 0.66s elapsed (1715 total ports)
Initiating Service scan at 13:43
Scanning 3 services on 10.0.0.2
Completed Service scan at 13:43, 6.01s elapsed (3 services on 1 host)
Initiating OS detection (try #1) against 10.0.0.2
SCRIPT ENGINE: Initiating script scanning.
Initiating SCRIPT ENGINE at 13:43
Completed SCRIPT ENGINE at 13:43, 10.02s elapsed
Host 10.0.0.2 appears to be up ... good.
Interesting ports on 10.0.0.2:
Not shown: 1712 closed ports
PORT   STATE SERVICE VERSION
21/tcp open  ftp     G-Net DSL Modem ftpd 1.0
|_ FTP bounce check: no banner
23/tcp open  telnet  Zoom aDSL modem telnetd X5 GS Ver 2.5.0A
80/tcp open  http    Viking router http config (Nucleus 4.3; virata httpd 6_2_0)
|_ HTML title: Site doesn't have a title.
|  HTTP Auth: HTTP Service requires authentication
|    Auth type: Basic, realm = Viking
MAC Address: 00:01:38:D4:A2:1D (XAVi Technologies)
Device type: broadband router
Running: CastleNet embedded, ZTE embedded
OS details: Zoom X5 ADSL modem, ZTE ZXDSL 831 ASDL modem
Network Distance: 1 hop
TCP Sequence Prediction: Difficulty=261 (Good luck!)
IP ID Sequence Generation: Incremental
Service Info: Host: Vulcan; Devices: broadband router, router

Read data files from: C:\Program Files\Nmap
OS and Service detection performed. Please report any incorrect results at http://nma
Nmap done: 1 IP address (1 host up) scanned in 19.608 seconds
           Raw packets sent: 1747 (78.624KB) | Rcvd: 3441 (175.646KB)
```

Open Ports & Services

Networked devices

Another decision point…

What type of networked storage was identified?

Is it local network storage, maybe a wireless drive?

- Tell your fellow officers what they should look for. Hopefully the device is in an obvious location. If not, look hard. Attic? Basement? Crawlspace?

Can’t find the networked drive, or it’s not local?

- Make a logical image if possible (and legal). If it’s located on a server, get a subpoena.

Image the RAM again

You know why…

Considerations

Counter-forensic software may destroy evidence while the computer is running.

Run Netstat, Task Manager, or a similar program to find out which applications & processes are running.

Considerations

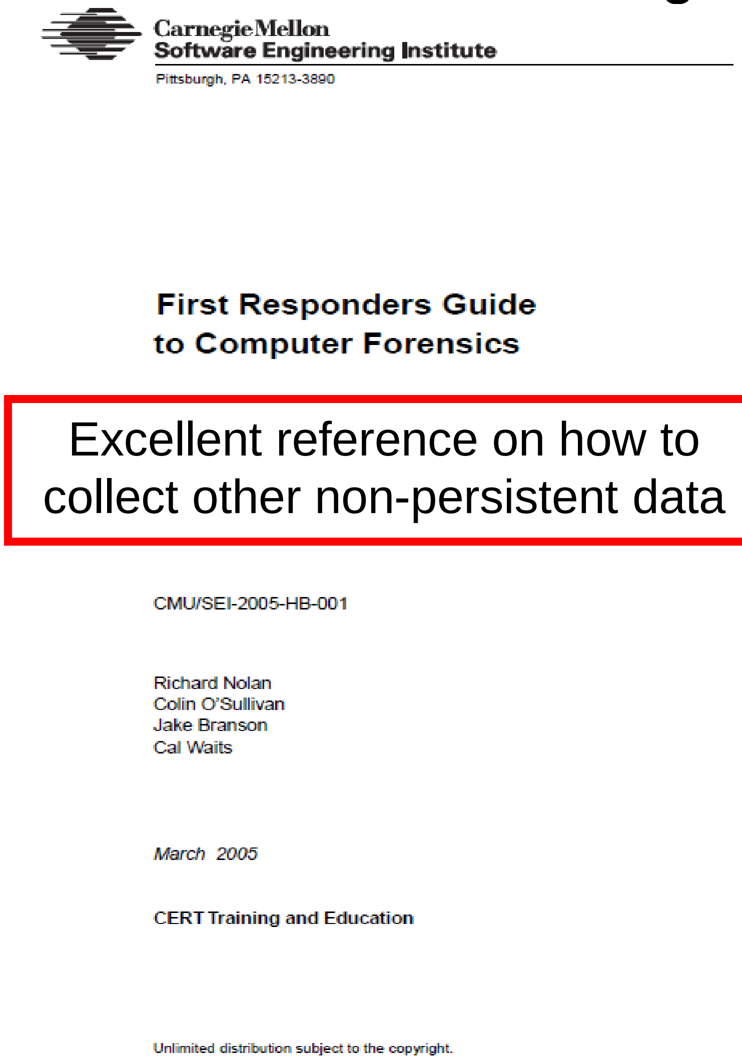
Computer could be accessed remotely while connected to a network.

Continue to monitor network activity if you need to stay connected to the network while imaging.

As soon as you’re able, physically disconnect cables from network adaptors or disable them in the operating system.

Considerations

Consider collecting other non-persistent data:



Carnegie Mellon
Software Engineering Institute
Pittsburgh, PA 15213-3890

First Responders Guide to Computer Forensics

CMU/SEI-2005-HB-001

Richard Nolan
Colin O'Sullivan
Jake Branson
Cal Waits

March 2005

CERT Training and Education

Unlimited distribution subject to the copyright.

Excellent reference on how to collect other non-persistent data

esses

e

n date and time

story

m uptime

ed libraries

a

ers

Now you can pull the plug

maybe…

FIRST RESPONDER FORENSICS

Mick Walsh

Special Agent

United States Secret Service

Miami Electronic Crimes Task Force

Questions?

United States Secret Service
Brasilia Resident Office
Embassy of the United States
SES Quadra 801, Lote 3
70403-900 Brasilia DF

Tel. (61) 3312-7440
Fax (61) 3312-7301
E-mail: SecretServicenoBrasil@usss.dhs.gov