Computer Forensics Jujitsu for Auditors:

Conducting Legally Defensible Investigations

Inno Eroraha, CISSP-ISSAP, CISM, CISA, CHFI
Founder & Chief Strategist
NetSecurity® Corporation

IIA/ISACA
Chicago Chapter

netSecurity Forensic Labs

netSecurity®

Abstract Condensed

Whether you are conducting or supporting the investigation of illicit pornography, disgruntled employees, malicious software outbreaks, fraud, advanced cyber attacks, or other sophisticated zero-day targeted attacks launched by China, the investigation primitives are the same. The investigators or supporting casts have to quickly identify and collect the most crucial evidence wherever it may be. Evidence can be found in: laptops, mobile devices, servers, desktops, networks, social media, or in the wild and must be collected in a forensically-sound or legally-defensible manner. Further, the investigation must be conducted without preconceived ideas about the guilt or innocence of the suspect.

In this presentation, we will explore what the ultra-busy auditor can do to build up their forensics capabilities, collect and handle evidence properly, conduct a forensics investigation, and produce a credible report that can withstand legal scrutiny. More importantly, we will examine tools of the trades that the auditor can start using today. At the end of the session, all attendees should be able to start conducting an investigation or, at a minimum, start acquiring evidence in a forensically-sound manner.

Investigative Scenario #1: You're Called to Duty!

- Scenario:
  - John, an employee, is surfing illegal porn with a corporate-issued Windows 8 Laptop
  - As an IT Auditor (Cyber Auditor), you are called to conduct the investigation
  - Assume there is a lot of evidence on the laptop
- Questions:
  - What would your steps be in performing the task?
  - What tools would you use?

Investigative Scenario #2: Vicki and the Boss

- Scenario
  - Your best friend, Jack, suspects that his wife, Vicki, is having an unusual relationship with her billionaire boss. Jack has asked you to analyze Vicki's work laptop for any potential evidence. Jack wants to sneak the laptop to you in the middle of the night while Vicki is deep asleep
- Question
  - How would you go about providing Jack with the forensics evidence he needs to confront Vicki?

Agenda*

- Need for Digital Forensics Investigation
- Maintaining Forensics Soundness
- Maze of Computer Forensics Investigation
- Challenges Faced by Cyber Auditors
- Developing an Arsenal for Conducting Forensically-Sound Investigations
- Building Corporate Forensics Capability
- Key Success Factors

**** This slide is intentionally placed here!***

Need for Digital Investigation

- Trojan Defense (Example: US vs. Thomas Ray)
- Illicit pornography
- Sexting
- Computer misuse
- Intellectual property theft
- Fraud, waste, and abuse
- Cyber stalking
- Mobile malware
- Nation-state sponsored cyber crime
- Corporate, civil, or criminal investigation
- Any physical crime – HOMICIDE, etc.

Intellectual Property Theft

System Intrusion

Policy Violation

Illicit Pornography

Encrypted/Deleted/Hidden Files

Denial of Service Attack

Malicious Software Outbreak

Cyber Extortion

Evidence Tampering

Email Spoofing Attacks

Digital Crime

Network Hacking

Confidential Information Leak

Computer Misuse

netSecurity Forensic Labs

netSecurity®

Maintaining Forensic Soundness

- Forensics process that is reliable, repeatable, and documented
- Ensure strict Chain of Custody
- Avoids tampering with the evidence
- Evidence is collected by people that are well trained and experienced
- Employ well-known and tested tools for evidence collection
- Document, dOCuMeNt, DOcUMeNt, and document the investigative process
- End-result must withstand the scrutiny of opposing counsels

Maze of Computer Forensics Investigation

- Obtain Subpoena or Authorization to Search and/or Seize
- Scope the Investigation
- Secure and Document the Scene
- Handle and Secure the Evidence
- Acquire Evidence (Acquisition/Imaging) from Suspect Media
- Define Review Strategy
  - Identify search terms, keywords, or events of interest
- Verify/Authenticate Evidence
- Analyze the Evidence (never the Original or Suspect drive!)
- Report Findings (in "layman" terms)
- Present Findings or Provide Testimony
- Dispose/Archive Case

Evidence Identification

- How do you identify evidence that is part of the investigation?
- What do you collect from the crime scene?
- Where is the evidence?
  - Hint: any computing device with "storage" capability – you name it!
- What is the evidence? Volatile and Non-Volatile
  - Order of volatility
- Evidence Handling
- When do you start collecting evidence – don't wait for days, weeks!

Guidance for Investigation

- Independence
- Integrity
- Objectivity
  - Forensics Examination vs. Expert Testimony
- Conflict of Interest

AICPA Reference:
http://www.aicpa.org/interestareas/forensicandvaluation/resources/practaidsguidance/downloadabledocuments/sr_081_excerpt.pdf

Investigative Scenario #3: Dicck Maxxwell

- Scenario
  - A crime has been committed. The computer used has been identified and is still up and running. The user ("suspect"), "Dicck Maxxwell," is claiming that a malware on the system must have downloaded the illicit pornography onto his computer on his behalf. You have been recruited as the forensics czar to conduct this high-profile investigation involving Mr. Maxxwell. Dicck is still sitting at his computer when you and the SWAT team showed up at the doorstep. Dicck started his career in the IT field as a computer operator in the 1980s and is very tech-savvy. In his office are one Windows workstation, a switch, 2 PCs running Linux, a cracked CD, two thumb drives, Microsoft Surface Pro, and a hammer.
- Questions
  - What items would you collect as evidence?
  - What steps would you take to find reasonable evidence for the defense or prosecuting attorneys?

Order of Volatility of Evidence

- CPU Registers, Cache, and Peripheral memory
- Main/Physical memory
  - Microsoft Windows: \\.\PhysicalMemory
  - Unix, OS X: /dev/mem, /var/vm
  - Linux: /proc/kcore
- Virtual memory
  - Microsoft Windows: pagefile.sys, hiberfil.sys
  - Unix, Linux, OS X: swap file
- Network state
- Running processes
- Disk
- Floppies, backup media, etc.
- Archival media, including: CD-ROMs, USB drives, etc.

Evidence Location

Windows Environment	Other Areas
• Memory • Windows Registry Hives • Internet Activities • Recent Files or Shortcuts (LNK files) • Print Spooler • Recycle Bin • Hard Drive • Log Files	• Windows-Equivalent Locations (for General purpose OS's) • Network Packet Captures • Firewall, Gateway, and Application Logs

Demo / Lab

AccessData FTKImager

AccessData FTK Imager 3.4.0.1

File View Mode Help

Evidence Tree

- files
- info
- ♥ 1D ♥
- 2012-06-12
- 2012-06-26
- 2012-06-28
- 2012-07-02
- 2012-07-05
- All Things One Direction ♥
- Book Covers
- Contacts
- ContentWatch
- Desktop
- Downloads
  - !ehv
  - !ehv.zip
- Favorites
- iPod Photo Cache
- iwontstandinyourway.tumblr.com
- KEEP
- Links
- Microsoft Powerpoints
- MTF Story Chapters

Custom Content Sources

Evidence:File System|Path|File	Options

New | Edit | Remove | Remove All | Create Image

Properties | Hex Value Interpreter | Custom Content Sources

File List

Name	Size	Type	Date Modif...
iehv.chm	16	Regular File	12/2/2009 ...
iehv.exe	36	Regular File	12/2/2009 ...
readme.txt	13	Regular File	12/2/2009 ...

```
0000 4D 5A 90 00 03 00 00 00-04 00 00 00 FF FF 00 00 MZ··********ÿÿ··
0010 B8 00 00 00 00 00 00 00-40 00 00 00 00 00 00 00 ¸·******@·******
0020 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00 ****************
0030 00 00 00 00 00 00 00 00-00 00 00 00 F0 00 00 00 ************ð···
0040 0E 1F BA 0E 00 B4 09 CD-21 B8 01 4C CD 21 54 68 ··º··´·Í!¸·LÍ!Th
0050 69 73 20 70 72 6F 67 72-61 6D 20 63 61 6E 6E 6F is program canno
0060 74 20 62 65 20 72 75 6E-20 69 6E 20 44 4F 53 20 t be run in DOS 
0070 6D 6F 64 65 2E 0D 0D 0A-24 00 00 00 00 00 00 00 mode.···$·******
0080 45 1E AF 86 01 7F C1 D5-01 7F C1 D5 01 7F C1 D5 E·¯···ÁÕ··ÁÕ··ÁÕ
0090 C2 70 9E D5 03 7F C1 D5-FB 5C 81 D5 02 7F C1 D5 Âp·Õ··ÁÕû\·Õ··ÁÕ
00a0 DB 5C DD D5 0A 7F C1 D5-FB 5C D8 D5 03 7F C1 D5 Û\ÝÕ··ÁÕû\ØÕ··ÁÕ
00b0 C2 70 9C D5 10 7F C1 D5-01 7F C0 D5 EC 7F C1 D5 Âp·Õ··ÁÕ··ÀÕì·ÁÕ
00c0 26 B9 B3 D5 19 7F C1 D5-26 B9 BD D5 00 7F C1 D5 &¹³Õ··ÁÕ&¹½Õ··ÁÕ
00d0 26 B9 B9 D5 00 7F C1 D5-52 69 63 68 01 7F C1 D5 &¹¹Õ··ÁÕRich··ÁÕ
00e0 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00 ****************
00f0 50 45 00 00 4C 01 03 00-D9 FE 15 4B 00 00 00 00 PE··L···Ùþ·K····
0100 00 00 00 00 E0 00 03 01-0B 01 08 00 00 80 00 00 ····à***********
0110 00 20 00 00 00 E0 00 00-30 65 01 00 00 F0 00 00 ·***à··0e···ð··
0120 00 70 01 00 00 00 40 00-00 10 00 00 00 02 00 00 ·p····@*********
0130 04 00 00 00 00 00 00 00-04 00 00 00 00 00 00 00 ****************
0140 00 90 01 00 00 10 00 00-00 00 00 00 02 00 00 00 ****************
0150 00 00 10 00 00 10 00 00-00 00 10 00 00 10 00 00 ****************
0160 00 00 00 00 10 00 00 00-00 00 00 00 00 00 00 00 ****************
0170 18 80 01 00 38 02 00 00-00 70 01 00 18 10 00 00 ····8····p******
0180 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00 ****************
0190 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00 ****************
01a0 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00 ****************
01b0 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00 ****************
01c0 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00 ****************
01d0 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00 ****************
01e0 00 00 00 00 00 00 00 00-55 50 58 30 00 00 00 00 ********UPX0****
01f0 00 E0 00 00 00 10 00 00-00 00 00 00 00 04 00 00 ·à**************
0200 00 00 00 00 00 00 00 00-00 00 00 00 80 00 00 E0 ***************à
0210 55 50 58 31 00 00 00 00-00 80 00 00 00 F0 00 00 UPX1********ð··
0220 00 78 00 00 00 04 00 00-00 00 00 00 00 00 00 00 ·x**************
0230 00 00 00 00 40 00 00 E0-2E 72 73 72 63 00 00 00 ****@··à.rsrc···
0240 00 20 00 00 00 70 01 00-00 14 00 00 00 7C 00 00 · ···p*******|··
```

Cursor pos = 0

\\.\PHYSICALDRIVE1/Partition 1 [1955MB]/NONAME [FAT32]/[root]/Downloads/!ehv.zip/iehv.exe

NUM

BrowserHistoryView

BrowsingHistoryView

File Edit View Options Help

URL	Title	Visit Time	Web browser
http://www.bcrms.com/img/easy-doc...	easy-document-search....	8/23/2012 2:48:33 PM	Chrome
http://www.bcrms.com/img/easy-doc...	easy-document-search....	8/24/2012 9:02:43 AM	Chrome
http://www.bcrms.com/style/style_gif....		8/22/2012 12:37:22 PM	Chrome
http://www.box.com/hellosign	Box | Simple Online Coll...	8/22/2012 12:17:58 PM	Chrome
http://www.box.com/hellosign	Box | Simple Online Coll...	8/22/2012 12:15:40 PM	Chrome
http://www.box.com/signup/o/hellosi...	Box | Simple Online Coll...	8/22/2012 12:17:58 PM	Chrome
http://www.box.com/signup/o/hellosi...	Box | Simple Online Coll...	8/22/2012 12:15:40 PM	Chrome
http://www.codeplex.com/Terminals/...		8/27/2012 8:42:25 AM	Internet Explorer
http://www.computerworld.com/s/arti...	Microsoft warns of 'man...	8/21/2012 1:47:15 PM	Chrome
http://www.copyblogger.com/archives/	Copyblogger Archives | ...	8/21/2012 9:07:58 AM	Chrome
http://www.copyblogger.com/fake-gri...	BECAUSE AWESOME! | C...	8/21/2012 9:07:22 AM	Chrome
http://www.directdial.com/	Printers, Scanners, Tone...	8/27/2012 11:36:08 AM	Chrome
http://www.directdial.com/90-XB1I00B...	90-XB1I00BG00010- - Ca...	8/27/2012 12:21:57 PM	Chrome
http://www.directdial.com/ca/shop/go...	Buy Nylon Notebook Ca...	8/27/2012 12:22:03 PM	Chrome

1693 item(s)

NirSoft Freeware. http://www.nirsoft.net

Process Explorer (with VirusTotal Intelligence)

Process Explorer - Sysinternals: www.sysinternals.com [

File Options View Process Find Handle Users Help

Process	rate Bytes	Working Set	Description	Company Name	Autostart L...	Process Timeline	VirusTotal
nvtray.exe	8,236 K	14,928 K	NVIDIA Settings	NVIDIA Corporation			0/48
chrome.exe	38,228 K	14,888 K	Google Chrome	Google Inc.			0/50
nvvsvc.exe	6,920 K	14,480 K	NVIDIA Driver Helper Servic...	NVIDIA Corporation	HKLM\Syste...		0/50
wmpnetwk.exe	16,368 K	12,784 K	Windows Media Player Netw...	Microsoft Corporation	HKLM\Syste...		0/50
daemonu.exe	6,316 K	12,588 K	NVIDIA Settings Update Ma...	NVIDIA Corporation	HKLM\Syste...		0/48
dllhost.exe	10,780 K	12,564 K	COM Surrogate	Microsoft Corporation	HKLM\Syste...		0/50
svchost.exe	8,172 K	12,084 K	Host Process for Windows S...	Microsoft Corporation			0/50
nvstreamsvc.exe	7,164 K	12,036 K	NVIDIA Streamer Service	NVIDIA Corporation	HKLM\Syste...		0/47
updatesrv.exe	7,188 K	11,920 K	Bitdefender Update Service	Bitdefender	HKLM\Syste...		0/48
svchost.exe	5,940 K	10,976 K	Host Process for Windows S...	Microsoft Corporation			0/50
procexp.exe	5,780 K	10,680 K	Sysinternals Process Explorer	Sysinternals - www.sysinter...			1/51
nvstreamsvc.exe	4,072 K	9,560 K	NVIDIA Streamer Service	NVIDIA Corporation	HKLM\Syste...		0/47
AppleMobileDeviceService...	3,208 K	9,348 K	MobileDeviceService	Apple Inc.	HKLM\Syste...		0/50
NisSrv.exe	13,912 K	9,292 K	Microsoft Network Realtime I...	Microsoft Corporation	HKLM\Syste...		0/48
services.exe	5,036 K	8,756 K	Services and Controller app	Microsoft Corporation			0/50
winlogon.exe	4,288 K	8,724 K	Windows Logon Application	Microsoft Corporation			0/50
NvTmru.exe	4,228 K	8,436 K	NVIDIA NvTmru Application	NVIDIA Corporation	HKLM\SOFT...		0/50
nvvsvc.exe	3,600 K	8,288 K	NVIDIA Driver Helper Servic...	NVIDIA Corporation	HKLM\Syste...		0/50
SnagPriv.exe	3,796 K	8,196 K	Snagit RPC Helper	TechSmith Corporation			0/47
svchost.exe	4,180 K	8,072 K	Host Process for Windows S...	Microsoft Corporation			0/50
SbieCtrl.exe							

Type	Name
Desktop	\Default
Directory	\KnownDlls
Directory	\Sessions\1\BaseNamedObjects
Event	\BaseNamedObjects\BDAgent-WTS-event
Event	\BaseNamedObjects\BDAgent-stop
Event	\BaseNamedObjects\BDAgent-seccenter
Event	\BaseNamedObjects\TermSrvReadyEvent
Event	\KernelObjects\MaximumCommitCondition
File	C:\Windows\System32
File	C:\Windows\winsxs\amd64_microsoft.windows.common-controls_6595b64144ccf1df_6.0.7...
File	\Device\KsecDD
File	\Device\NamedPipe\UpdateCommPipe
File	\Device\NamedPipe\quarcommpipe
File	\Device\NamedPipe\VSSERV

CPU Usage: 2.87% | Commit Charge: 29.08% | Processes: 86 | Physical Usage: 52.15%

WinPrefetchView

WinPrefetchView

File Edit View Options Help

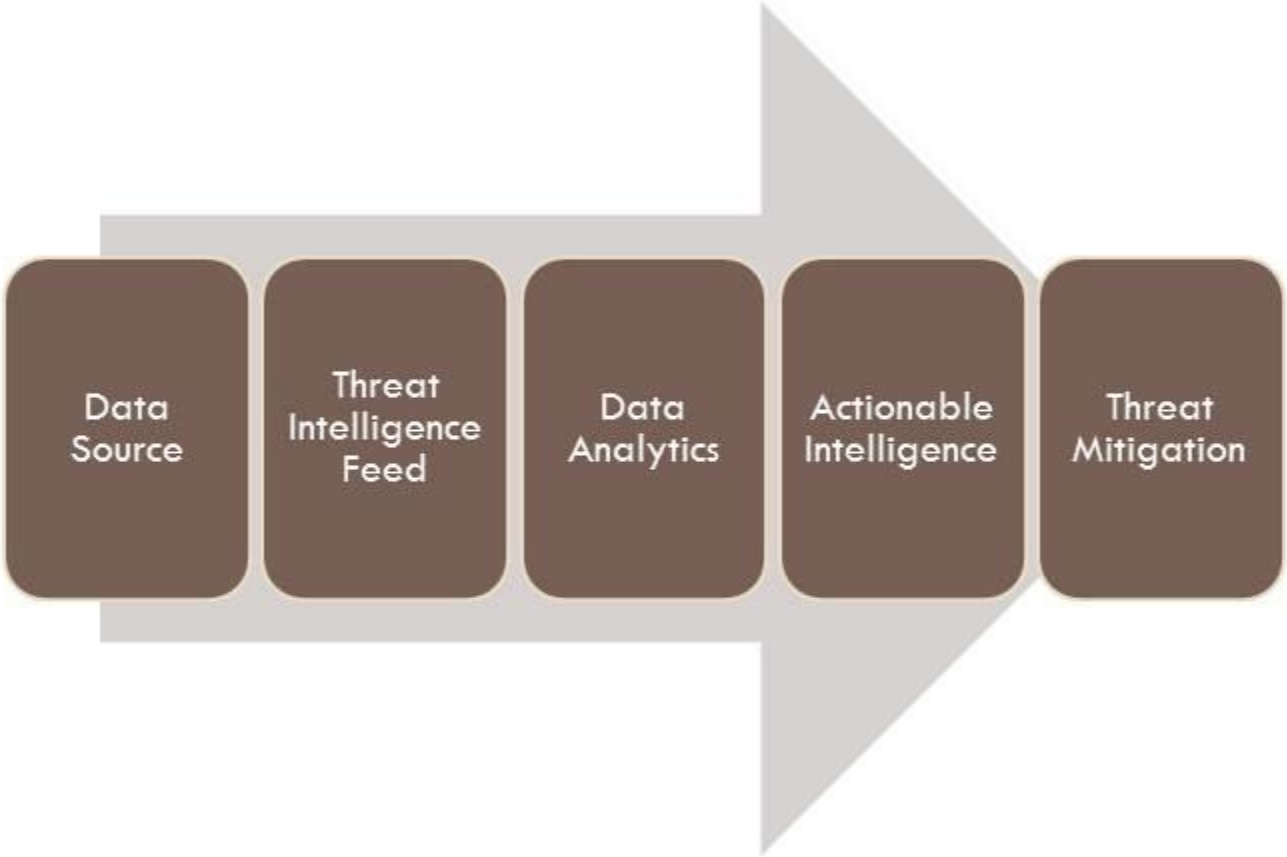
Filename	Created Time	Modified Time	File Size	Process EXE	Process Pa
CL.EXE-13DBEA52.pf	10/05/2009 01:3...	05/01/2010 23:37:05	80,064	CL.EXE	F:\PROGR
BRMFCMON.EXE-08CFACE...	06/08/2009 10:3...	05/01/2010 23:37:00	10,354	BRMFCMON....	F:\PROGR
FIREFOX.EXE-06188867.pf	20/12/2009 23:2...	05/01/2010 23:34:18	73,826		
MSPDBSRV.EXE-0A9C4E89.pf	14/05/2009 10:4...	05/01/2010 23:32:38	7,604	MSPDBSRV.EXE	F:\PROGR
DEVENV.EXE-34433B99.pf	14/05/2009 10:4...	05/01/2010 23:32:19	104,608	DEVENV.EXE	F:\PROGR

Filename	Full Path	Device Path
UA.CSS	F:\PROGRAM FILES\MOZILLA FIREFOX\res\ua.css	\DEVICE\HARDDISKVOLUME2\PROGRAM FILE
HTML.CSS	F:\PROGRAM FILES\MOZILLA FIREFOX\res\html.css	\DEVICE\HARDDISKVOLUME2\PROGRAM FILE
TOOLKIT.JAR	F:\PROGRAM FILES\MOZILLA FIREFOX\chrome\toolk...	\DEVICE\HARDDISKVOLUME2\PROGRAM FILE
QUIRK.CSS	F:\PROGRAM FILES\MOZILLA FIREFOX\res\quirk.css	\DEVICE\HARDDISKVOLUME2\PROGRAM FILE
CLASSIC.JAR	F:\PROGRAM FILES\MOZILLA FIREFOX\chrome\class...	\DEVICE\HARDDISKVOLUME2\PROGRAM FILE
FORMS.CSS	F:\PROGRAM FILES\MOZILLA FIREFOX\res\forms.css	\DEVICE\HARDDISKVOLUME2\PROGRAM FILE
CHARSETDATA.P...	F:\PROGRAM FILES\MOZILLA FIREFOX\res\CHARSE...	\DEVICE\HARDDISKVOLUME2\PROGRAM FILE

74 Files, 1 Selected

NirSoft Freeware. http://www.nirsoft.net

ThreatRESPONDER™



netSecurity®

Challenges Faced by Cyber Auditors

- Windows OS widespread use results in "Handicap" with other OS
- Inadequate Forensics Training/Education
- Technology *Du Jour* (Cloud, BIG Data, Virtualization, Mobile Devices)
- Emerging Cyber Threats
  - Sophisticated Rootkits (Malware)
  - Advanced Persistent Threats (APT)
- Anti-Forensics Techniques
- Live Volatile Data
- Ubiquity of Evidence, which calls for Forensics Specialties
  - Memory Forensics, Remote Forensics, Malware Analysis, Network Forensics, Mobile Devices, Reverse Engineering, etc.
- Massive Data Collection and Analysis
- Laws, Regulations, and Legal System

Developing Arsenal for Conducting Forensically-Sound Investigations that can Withstand Legal Scrutiny

Building a Forensic Capability

- Seek Management Buy-in
- Revise Corporate Policies to Address Forensics Investigation Planning
- Form a Forensics Investigation SWAT Team
- Identify or Appoint a Team Manager
- Get a Firm Grip on Your Data
- Build and Equip a Forensics Investigation Lab
- Create a Standard Operating Procedure (SOP)
- Acquire Tools and Technologies
- Get Trained on Forensics Investigation Procedures
- Test and Rehearse the Plan and Tools
- Conduct Readiness Exercises and Training Frequently
- Update the Tools, Plans, and Policies

Capabilities for Forensics Readiness

- IT/Security Auditing
- Proactive Training
- Incident Response/Handling
- Malware Analysis
- Remote Forensics
- Hard Drive Forensics
- Security Administration
- Log Analysis
- Intrusion Detection
- Reverse Engineering
- Programming
- System/Network Administration

Success Factors

- Secure the evidence (strict Chain of Custody Form)
- Have the knowledge
- Have the right tools and use them properly
- Document your work!
- Stay within laws, regulations, and policies
- Stay within your scope of investigation
  - If your scope is to find intrusion, do not investigate something else
- Know your boundary – Are you providing Expert Testimony or Fact Finding?

Start Investigating Tomorrow

- Be familiar with the proper procedures for conducting digital investigations
- Make sure you have the proper qualifications, training, education, certifications, and licenses
- Make sure you get the **PROPER AUTHORIZATION** from appropriate corporate authority or Legal before proceeding
  - Approval is typically granted by your Legal, HR, Security, Compliance, or other responsible departments
- Stay within your Scope and Expertise

Some Investigation Tools

- Assorted Tool
  - AccessData FTK Imager (http://accessdata.com)
- Internet History
  - NirSoft (http://nirsoft.net)
- Prefetch Files
  - NirSoft (http://nirsoft.net)
- Process Exploration
  - Process Explorer (http://sysinternals.com)
- Breach Investigation/Detection Platform
  - NetSecurity's ThreatResponder® (http://netsecurity.com)

Questions/Feedback?

- If you have critical comments/feedback that can enhance this presentation, please send them

- Direct Comments, Questions, and Feedback to **Inno@NetSecurity.com**