
Digital Forensic Analysis & Cyber Profiling

Presented to the AFCEA Quantico-Potomac Chapter

John J. Irvine

Advanced Programs Manager, Digital Forensics

Crucial Security

A Wholly-Owned Subsidiary of Harris Corporation

john.irvine@harris.com

(703) 961-9456 x148

- Overview of Computer Forensics
- Computer Forensic Specialty Areas
- Focus: Computer Intrusions
- Focus: Counterterrorism
- Focus: Cyber Profiling
- Conclusion/Q&A

Digital Forensic Analysis & Cyber Profiling

OVERVIEW OF COMPUTER FORENSICS



Victim



Instrumentality



Witness

...of a crime or a cyber-attack.

*Sometimes, one computer could play **all three** roles, such as in a Botnet case:*



Victim

- Computer is Compromised by Attacker via Vulnerability Exploit (and made a Zombie)



Instrumentality

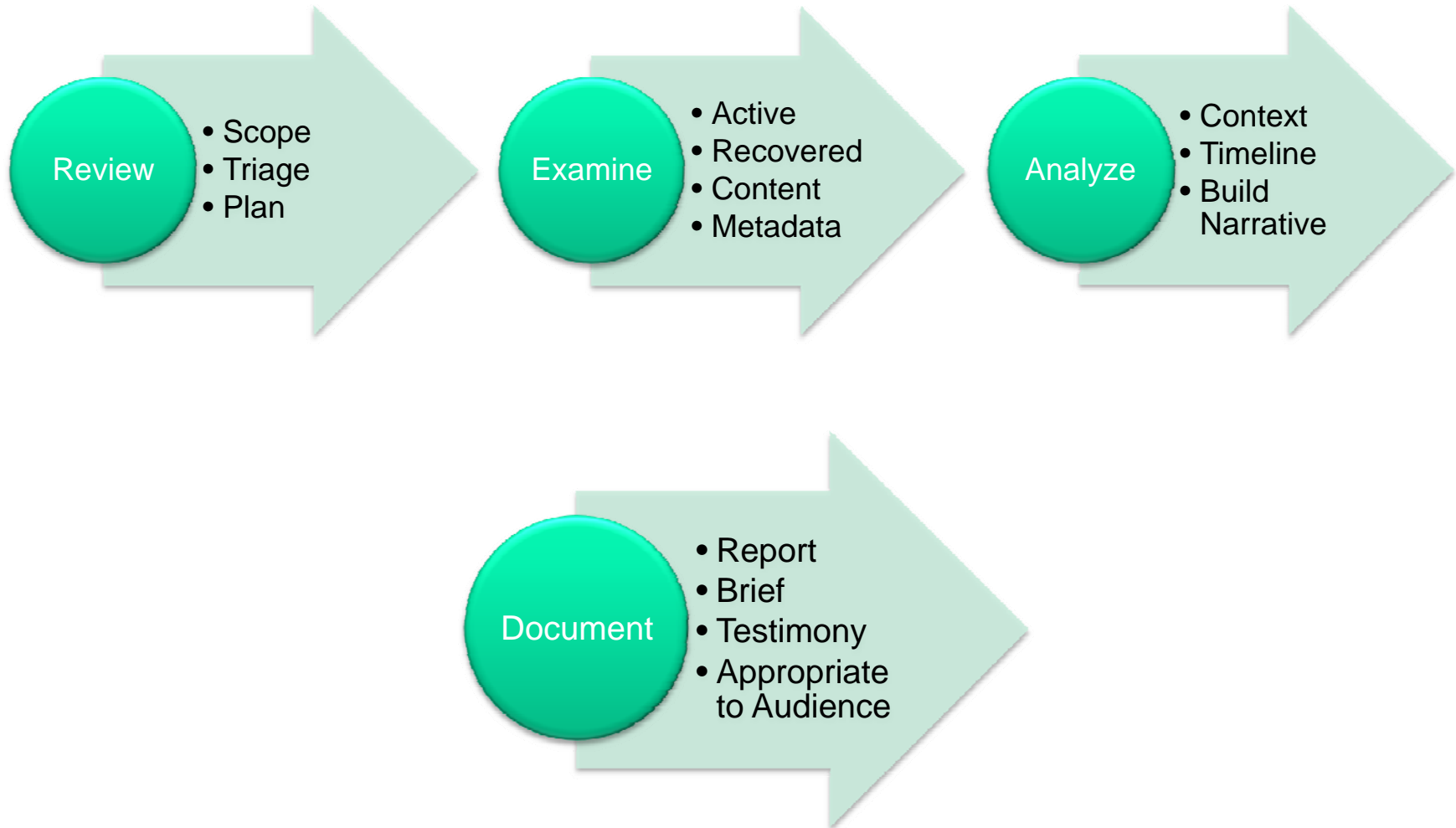
- Compromised System Used to:
 - Stage Attack
 - Email Spam
 - Deny Service
 - Recruit More Zombies



Witness

- Computer Holds Information About the Attack:
 - IP Addresses
 - Configuration Data
 - Spam Lists
 - Controller Information

- Gain Understanding
 - Who did this?
 - What data was lost, compromised, or altered?
 - When were we first attacked?
 - Which other computers in our network were compromised?
 - Are they attackers still in our system?
- Remediate/Prevent
 - Block or prosecute attackers.
 - Strengthen defenses.
 - Provide awareness.
- Target/Identify/Capture
 - Gather evidence.
 - Map social or electronic networks.
 - Stop evil.



Digital Forensic Analysis & Cyber Profiling

*COMPUTER FORENSIC
SPECIALTIES*

- Originally, one computer forensic examiner “did everything.”
 - Forensics was (and is) a new and growing discipline.
- Now, examiners tend to specialize by operating system and/or case type:
 - Windows Examiners vs. Mac Examiners vs. Linux Examiners
 - Criminal Examiners vs. Intelligence Examiners vs. Counterterrorism Examiners vs. Computer Intrusion Examiners
 - Law Enforcement to Intel? Easy.
 - Intel to Law Enforcement? Misery.
 - ***Different approaches, different techniques, different results.***
- The key to success is ***experience.***

- Computer forensic specialties include:
 - Criminal/Child Exploitation (75-80% of All CF Work)
 - Criminal/Other
 - Counterintelligence
 - Counterterrorism (Shrinking)
 - Counternarcotics
 - Computer Intrusions (Growing)
 - Binary/Malicious Code Reverse Engineering
 - Network Data Analysis
 - Log Analysis and Data Correlation
 - Corporate/Legal Forensics & eDiscovery

- Crucial Security:
 - Purchased by Harris Corporation in April 2009.
 - Has performed Computer Forensic Analysis for the FBI's Special Technologies Applications Section (STAS) since February 2001, specializing in computer intrusion, counterterrorism, counterintelligence, and criminal cases.
 - Maintains a staff of experienced computer forensic examiners, many with multi-agency experience, and many with 10-15 years of experience in the field.

- Crucial/Harris computer forensic examiners have collectively supported:
 - Federal Bureau of Investigation
 - Drug Enforcement Administration
 - Central Intelligence Agency
 - US Army, Navy, Air Force, and Marines
 - Defense Computer Forensics Laboratory (DCFL)
 - Defense Intelligence Agency
 - US Department of Commerce
 - US Department of Agriculture
 - Federal Aviation Administration
 - Fortune 50 Companies

- Crucial's primary focus areas are:
 - Computer Intrusion Investigations, Log Analysis, and Data Correlation
 - Criminal Case Analysis and Testimony
 - Counterterrorism Analysis
 - Malicious Code Reverse Engineering
 - Enterprise Analytics (Large Data Set Analysis and Correlation)

Digital Forensic Analysis & Cyber Profiling

*FOCUS: COMPUTER
INTRUSIONS*



- The Verizon 2010 Data Breach Investigations Report States:
 - 70% of data breaches resulted from external actors
 - 48% were caused by insiders (directly or indirectly)
 - 38% of attacks utilized malware
 - 85% of attacks were not considered highly difficult
 - **96% of attacks were avoidable through simple or intermediate controls**

- Computer Intrusion Examinations can:
 - Provide leads toward identifying the attacker, including his/her skill, sponsorship, intentions, etc.
 - Determine what data was exfiltrated, modified, or otherwise compromised
 - Determine if other systems in the network were also compromised
 - Determine if malicious code was left behind (it was) and what it was designed to do
 - Assist in creating a remediation plan to reduce successful future attacks

- Crucial examiners have seen a significant rise in “spear phishing” attacks over the last two years:
 - Attacks are custom-crafted for specific individuals, mimicking their area of focus
 - “I met you at the conference a few months ago...”
 - Example: PDF documents containing malicious code open a channel to attackers that allows system access
 - “You might find this document on new anti-terror techniques particularly interesting, as it follows Dr. Johnson’s work presented at the conference...”

- Opening the PDF file results in:
 - The legitimate PDF file being displayed for review, and
 - The execution of malicious code placed within the PDF file to give an attacker access to the target computer, unbeknownst to the user
- Attackers will swiftly use this access to establish a virtual beachhead, then they will compromise other computers in the network as necessary to achieve their goals.
- **This happens to everyone from toy companies through intelligence agencies.** Your data is just as important to them, too!

- What do computer intrusion exams analyze?
 - Malicious Code
 - Data Exfiltration Files
 - Unallocated Space/Hibernation Files/Swap Files
 - Restore Points
 - Dr. Watson Logs
 - NTFS Change Journals
 - System Logs
 - Registry Entries (Windows)
 - Unknown Binaries/Executables
 - Browsing Histories
 - Link Files
 - Prefetch Files (Windows)
 - Start-up Directories (and Registry Entries)
 - User Accounts/Permissions
 - Live Memory Processes
 - Timelines (and sometimes Super-Timelines)



Experience performing computer intrusions will mean the difference between a “No Findings” report and “We’ve been owned by a foreign government for six months” report.

Digital Forensic Analysis & Cyber Profiling

FOCUS:
COUNTERTERRORISM

- *Completely* different mindset from Intrusion Analysis Forensics:
 - Somewhat less technical, significantly more investigative.
 - Less based in procedure, more based in experience.

- CT forensics aims to:
 - Identify actors
 - Identify immediate threat
 - Identify developing plans or attack preparation
 - Map social networks
 - Gauge intentions, abilities, and timelines

- Content is king in CT forensics:
 - Email Messages
 - Chat Transcripts
 - Web Pages/Forums
 - Social Networks
 - Documents (and Scanned Documents)
 - Photographs, Videos, and Illustrations
 - Calendar Appointments, To-Do Lists (**Seriously!**)

- If content is king, **context** is queen:
 - *Where* were those images found on the drive?
 - (e.g. *Microsoft Civilians and Chicago Maps*)
 - *Which* pieces fit together?
 - (e.g. *GPS Waypoint Data and Video Footage*)
 - (e.g. *Finished Documents/Videos vs. Piecemeal Sections*)
 - *When* were the documents created, copied, or modified?
 - *What* was the system used for, and where was it physically?
 - (e.g. *School Newsletter*)

Counterterrorism computer forensics can produce actionable intelligence available from *no other source.*

Digital Forensic Analysis & Cyber Profiling

FOCUS: CYBER PROFILING

Cyber profiling takes computer forensics to the next step, based upon the experiences gained from processing hundreds of drives.

It should only be attempted by experienced examiners, preferably those who have had some education or training in the behavioral sciences.

It blends aspects of technology, investigation, psychology, and sociology to provide a larger picture than may be documented.

Over time, similarities develop and patterns emerge in examinations.

Examples:

Pornography

(Content and Timing)

Resumes

(Experience and Role)

Collections

(Packrats vs. Producers, General vs. Specifics)

Programs

(Collected vs. Installed vs. Used vs. Used Correctly)

- Cyber Profiling may be able to:
 - Identify users of a computer who were previously unknown
 - Map a subject's familial, social, professional, or organizational network, including his/her standing in the hierarchy
 - Provide information about the user's technical abilities, threat level, or immediacy of threat
 - Identify actors who are candidates for turning

Cyber profiling may provide insight in criminal, counterintelligence, or counterterrorism cases that generates new leads, particularly on cold cases.

-
- THANK YOU for allowing me to present to you today.
 - Individual success in computer forensics is based on the following, ***in order of relevance:***
 - Computer Forensic Experience Performing Casework
 - General Investigative Experience
 - General Computer Experience
 - Computer Forensic Training
 - Computer Forensic Education
 - All computer forensic examiners are not the same. Use them how they best fit YOUR needs.

Questions?

Contact Information

John J. Irvine

Advanced Programs Manager, Digital Forensics

Crucial Security

A Wholly-Owned Subsidiary of Harris Corporation

john.irvine@harris.com
(703) 961-9456 x148