

**Computer Forensics
and RIM**

**Alan A Andolsen CMC CRM
President
Naremco Services Inc**

Wyoming ARMA 10 March 2008

NAREMCO

Copyright 2008, Naremco Services Inc

What Is Computer Forensics?

- **Computer forensics involves the identification, extraction, preservation, documentation, and interpretation of computer media for evidentiary analysis.**
- **Multiple methods of**
 - Discovering data on computer system
 - Recovering deleted, encrypted, or damaged file information
 - Monitoring live activity
 - Detecting violations of corporate policy
- **Information collected assists in arrests, prosecution, termination of employment, and preventing future illegal activity**

NAREMCO

Copyright 2008, Naremco Services Inc

What Constitutes Digital Evidence?

- **Any information being subject to human intervention or not, that can be extracted from a computer.**
- **Must be in human-readable format or capable of being interpreted by a person with expertise in the subject.**
- **Examples**
 - Recovering thousands of deleted emails
 - Performing investigation after employment termination
 - Recovering evidence after formatting hard drive
 - Performing investigation after multiple users had taken over the system

NAREMCO

Copyright 2008, Naremco Services Inc

Computer Forensics for Business

- **Theft/destruction of intellectual property**
- **Unauthorized activity**
- **Tracking internet browsing habits**
- **Reconstructing events**
- **Inferring intentions**
- **Selling company bandwidth**
- **Wrongful dismissal claims**
- **Sexual harassment**
- **Software piracy**

Copyright 2008, Naremco Services Inc.

Who Uses Computer Forensics?

- **Criminal Prosecutors**
 - Rely on evidence obtained from a computer to prosecute suspects and use as evidence
- **Civil Litigations**
 - Personal and business data discovered on a computer can be used in fraud, divorce, harassment, or discrimination cases
- **Insurance Companies**
 - Evidence discovered on computer can be used to mollify costs (fraud, worker's compensation, arson, etc)

Copyright 2008, Naremco Services Inc.

Who Uses Computer Forensics?

- **Private Corporations**
 - Evidence obtained from employee computers can be used as evidence in harassment, fraud, and embezzlement cases
- **Law Enforcement Officials**
 - Rely on computer forensics to backup search warrants and post-seizure handling
- **Individual/Private Citizens**
 - Obtain the services of professional computer forensic specialists to support claims of harassment, abuse, or wrongful termination from employment

Copyright 2008, Naremco Services Inc.

Computer Forensics Steps

Acquisition

- Physically or remotely obtaining possession of the computer, all network mappings from the system, and external physical storage devices

Identification

- Identifying what data could be recovered and electronically retrieving it by running various computer forensic tools and software suites

NAREMCO

Copyright 2008, Naremco Services Inc.

Computer Forensics Steps

Evaluation

- Evaluating the information/data recovered to determine if and how it could be used against the suspect for employment termination or prosecution in court

Presentation

- Presentation of evidence discovered in a manner which is understood by lawyers. non-

NAREMCO

Copyright 2008, Naremco Services Inc.

Computer Forensics Goal

Admissibility of Evidence

- Legal rules which determine whether potential evidence can be considered by a court
- Must be obtained in a manner which ensures the authenticity and validity and that no tampering had taken place

No possible evidence is damaged, destroyed, or otherwise compromised by the procedures used to search the computer

No viruses are introduced to a computer during the analysis process

Extracted / relevant evidence is properly handled and protected from later mechanical or electromagnetic damage

NAREMCO

Copyright 2008, Naremco Services Inc.

Computer Forensics Goal

- Establishing and maintaining a continuing chain of custody
- Limiting the amount of time business operations are affected
- Not divulging and respecting any ethical [and legal] client-attorney information that is inadvertently acquired during a forensic exploration

NAREMCO

Copyright 2008, Naremc0 Services Inc.

Computer Forensics Challenges

- Information and data sought after and collected in the investigation must be properly handled.
- Volatile Information
 - Network Information
 - Communication between system and the network
 - Active Processes
 - Programs currently active on the system
 - Logged-on Users
 - Users/employees currently using system
 - Open Files
 - Libraries in use; hidden files; Trojans (rootkit) loaded in system

NAREMCO

Copyright 2008, Naremc0 Services Inc.

Computer Forensics Challenges

- Non-Volatile Information
 - This includes information, configuration settings, system files and registry settings that are available after reboot
 - Accessed through drive mappings from system
 - This information is investigated and reviewed from a backup copy

NAREMCO

Copyright 2008, Naremc0 Services Inc.

NAREMCO

Computer Forensic Requirements

- **Hardware**
 - Familiarity with all internal and external devices and components of a computer
 - Thorough understanding of hard drives and settings
 - Understanding motherboards and the various chipsets used
 - Power connections
- **Memory**
- **BIOS**
 - Understanding how the BIOS works
 - Familiarity with the various settings and limitations of the BIOS

Copyright 2008, Naremco Services Inc.

NAREMCO

Computer Forensic Requirements

- **Operating Systems**
 - Windows 3.1/95/98/ME/NT/2000/2003/XP/Vista
 - DOS
 - UNIX, LINUX
 - VAX/VMS
- **Software**
 - Familiarity with most popular software packages such as Office
- **Forensic Tools**
 - Familiarity with computer forensic techniques and the software packages that could be used

Copyright 2008, Naremco Services Inc.

NAREMCO

Evidence Processing Guidelines

- **New Technologies Inc. recommends:**
 - **Step 1: Shut down the computer**
 - Consideration must be given to volatile information
 - Prevent remote access to machine and destruction of evidence (manual or anti-forensic software)
 - **Step 2: Document the Hardware Configuration**
 - Note everything about the computer configuration prior to re-locating
 - **Step 3: Transport to a Secure Location**
 - Do not leave the computer unattended unless it is locked in a secure location

Copyright 2008, Naremco Services Inc.

Evidence Processing Guidelines

- **Step 4: Make Bit Stream Backups of Hard Disks and Floppy Disks**
- **Step 5: Mathematically Authenticate Data on All Storage Devices**
 - To prove that you did not alter any of the evidence after the computer came into your possession
- **Step 6: Document the System Date and Time**
- **Step 7: Make a List of Key Search Words**
- **Step 8: Evaluate the Windows Swap File**

Copyright 2008, Naremc0 Services Inc.

Evidence Processing Guidelines

- **Step 9: Evaluate File Slack**
 - File slack is a data storage area between the end of a file and the end of a sector; a source of significant security leakage.
- **Step 10: Evaluate Unallocated Space (Erased Files)**
- **Step 11: Search Files, File Slack, and Unallocated Space for Key Words**
- **Step 12: Document File Names, Dates and Times**
- **Step 13: Identify File, Program and Storage Anomalies**
- **Step 14: Evaluate Program Functionality**
- **Step 15: Document Your Findings**
- **Step 16: Retain Copies of Software Used**

Copyright 2008, Naremc0 Services Inc.

Hiding Data

- **To human eyes, data usually contains known forms, like images, e-mail, sounds, and text. Most Internet data naturally includes gratuitous headers, too. These employ long lengths using new controversial logical encodings: steganography and marking.**

Copyright 2008, Naremc0 Services Inc.

NAREMCO

Hiding Data

- **To human eyes, data usually contains known forms, like images, e-mail, sounds, and text. Most Internet data naturally includes gratuitous headers, too. These employ long lengths using new controversial logical encodings: steganography and marking.**

Copyright 2008, Naremco Services Inc.

NAREMCO

Hiding Data

- **To human eyes, data usually contains known forms, like images, e-mail, sounds, and text. Most Internet data naturally includes gratuitous headers, too. These employ long lengths using new controversial logical encodings: steganography and marking.**

The duck flies at midnight. Tell Uncle Sam

Copyright 2008, Naremco Services Inc.

NAREMCO

Hiding Data

- **To human eyes, data usually contains known forms, like images, e-mail, sounds, and text. Most Internet data naturally includes gratuitous headers, too. These employ long lengths using new controversial logical encodings: steganography and marking.**

The duck flies at midnight. Tell Uncle Sam

- **Steganography: The art of storing information in such a way that the existence of the information is hidden.**

Copyright 2008, Naremco Services Inc.

Hiding Data

- **Watermarking:** Hiding data within data
- Information can be hidden in almost any file format.
- File formats with more room for compression are best
 - Image files (JPEG, GIF)
 - Sound files (MP3, WAV)
 - Video files (MPG, AVI)
- The hidden information may be encrypted, but not necessarily
- Numerous software applications will do this for you: Many are freely available online

Copyright 2008 Naremc Services Inc.

Computer Forensics Resources

www.computerforensicsworld.com

www.forensics-intl.com

computer-forensics.safemode.org

www.opensourceforensics.org

Computer Forensics and RIM

Alan A Andolsen CMC CRM
President
Naremc Services Inc.
60 East 42nd Street
New York, NY 10165

Voice: +1.812.497.0990
Fax: +1.212.928.1739
E-Mail: AlanAndolsen@NAREMCO.COM
Web Site: WWW.NAREMCO.COM

Wyoming ARMA

10 March 2008

Copyright 2008 Naremc Services Inc.
