NCIS Overview

• NCIS, a civilian organization, is the primary law enforcement and counterintelligence arm of the United States Department of the Navy. It works closely with other local, state, federal, and foreign agencies to counter and investigate the most serious crimes threatening the war fighting capability of Navy and Marine Corps. To accomplish this mission, NCIS pursues three strategic priorities:

  – Prevent Terrorism
  – Protect Secrets
  – Reduce Crime

• NCIS employees approximately 2400 personnel worldwide in over 140 locations:
  – Special Agents
  – Professional Support
  – Analyst
  – Forensic Experts
  – Security Specialists
Cyber Department Mission

• Directly support NCIS' mission objectives of preventing terrorism, protecting secrets and reducing major crimes. The Cyber Department leverages, deploys and executes advanced technologies and methodologies to process, identify and present electronic data of intelligence or evidentiary value to identify the human element behind the computer.

• **Special Agents** = Control of Investigations and Operations

• **Investigative Computer Specialist** = Conduct forensic analysis of media

• **Computer Scientist** = Provide technical expertise and guidance with new technologies and forensic tools

• **Analyst** = Provide detailed analysis of recovered data for additional leads/actions

• Approximately 110 personnel world wide
Where Do Internet Users Live?

729.2 Million Total Worldwide Users (2003-2004)

- Only 35% of Websites are in English.
- 14% Chinese.
- 9.6% Japanese.
- 9% Spanish.
- 7.3% German.
- 4% Korean.
A Typical Computer Crime Scene

Tower CPU

Other Storage media

Removable Storage Media
Computer Crime Scene cont.

- **Media & Storage**
  - Pirated Software
  - Backed-up Files
  - Contraband

- **Other Leads**
  - Website names
  - Other Names and addresses
  - Real / e-mail
  - Telephone Numbers
  - Bills from ISP, etc.
Hackers & Pedophiles are pack rats. Don’t overlook any area it may contain potential evidence.

More storage media, contraband, & leads on other suspects
Hope there are no fish in here!

Upstairs Room Secondary Computer Search Location

Wireless Router
A Computer Crime Scene cont.

What else?

- Pictures of serial numbers
- Pictures of wiring setup
Suspect’s Automobile

1. IPOD in gym bag
2. CD/DVD jukebox residing under the seat
3. Game device*
4. 2nd cell phone*
   • 250 contacts
   • 30 min audio
   • text messaging log
5. GPS Navigation System
   • routes/locations
   • continuous “breadcrumbs”
6. PDA wireless internet ready*
7. LoJack tracking device (hidden)
Digital Devices (Scary !)

Examples of Portable Storage

Each of these can hold up to 256MB and beyond
Suspect’s Work Office

Workspace contains desktop and server storage information.

1. Laptop computer* 500GB
2. Assorted Media 100GB
3. PDA* 20GB
4. External Hard Drive 500GB
5. Cellular Phone* 1-16 GB
6. KVM Switch
7. Network Switch/Hub*
8. CD DVD Burner
9. Multi-Card Reader
10. USB Hub

*Possible network interface
Law Enforcement Points

- Any Crim/Fraud/CI investigation can benefit from analysis of digital storage media and digital devices.
- Contact a Cyber Department Agent for help when seizing digital media.
- When in doubt, consult your digital evidence field manual for techniques of proper seizures methods.
NCIS Cyber Department

The Forensic Acquisition & Examination Process
Electronic Media Forensics

What is the goal?

☑ Safely Seize Original Media.
☑ Acquire a Forensic Image to guarantee the preservation of the original data.
☑ Conduct Analysis of the data to find the puzzle pieces that fit.
☑ Work with the case agent to present evidence to the Courts.
Electronic Media Forensics

The Process

Device Acquisitions: “Bit-by-Bit” copying of digital storage media to preserve the original and provide a working copy for examination
Computer Forensics

- Forensic Tools
  - EnCase: One industry standard tool for forensic analysis of digital media
  - View contents of media, complete file structure, restore deleted files
Cyber Dept. Forensic Roadmap

- Probable Cause
  - Search & Physical Seizure
    - Forensic Image Acquisition
      - Detailed Analysis
        - Report Generation
      - Testify
Computer Investigation and Operations

THREATS
Many Potential Cyber Threats

1. Insiders (highest threat)
2. Black Hat/White Hat Hackers
3. Recreational Hackers
4. Terrorists
5. Foreign Military
6. Organized Crime
7. Industrial Espionage
8. Hacktivists
Malicious Code

- **Viruses & Trojans**
  - A program that executes unwanted commands while also sometimes copying itself to make removal difficult and transmission easy.

- **Scripts**
  - A string of OS specific commands. Can be hidden inside other, useful, applications & launched via backdoors, etc.

- **Worms**
  - More invasive but less destructive. They spread like a virus by scanning network they are attached to for other open computers.
Computer Intrusions

Who is doing it and why?

- **Intelligence agencies**: Theft of research & technology (Source code/databases/contract data)
- **Industrial espionage**: Money (theft of copyright & proprietary data/trade secrets)
- **Hackers**: Mainly just for the phun of it, bragging rights... and now profit!
Industrial Espionage

Who’s spying now? *Everyone!*

Targets
- Private & Commercial Companies
- DoD Sponsored Contracts
- Universities
- Military Computer Systems
Hacker Behavior

- **Distributed Denial of Service Attack:**
  - Electronic bombardment of data to a server, clogging its ports and making access impossible or causing shutdown

- **Backdoors:**
  - Code left on a computer lies dormant until activated;
  - High Unused Ports left open allows hackers remote access to the system.
  - Can be used for anything from stealing files to enabling full simulated control over the machine and its resources

- **Cyber War:**
  - International Hacker groups wage war on the Internet. Systems may contain ticking time bombs. Only the hackers may know.
Identity Theft

- Information is freely available & for sale on the net
  - DOB’s
  - Mailing addresses (Physical & Email)
  - Social Security Numbers
  - Family Information
  - Credit Card Numbers
- While suspicious, much of this is still legal
Identity Theft

Company

Voluntary Information

3rd Party Database Companies

Other Corporate Divisions

3rd Parties

Marketing Divisions

Insiders

HACKERS?
Pedophiles, Child Predators & Stalkers

- Unprecedented access to unsuspecting victims
- IM/IRC/Email
- Potential anonymity
- Network with other offenders to share
- Unclear and incomplete state laws
Computer Investigation and Operations

COUNTERMEASURES
Prevention

- Viruses, Worms, Scripts
  - Install and maintain utilities such as Virus Detectors at user computers as well as at network systems such as Mail servers
  - Practice smart usage habits. Do not download “free” apps from non-trusted sources, do not open suspicious email attachments
  - Do not use “file trading” software
Prevention

- **Hackers**
  - Install and maintain personal/network firewall software (Zone Alarm/Norton/Black Ice)
  - Consider removing computers with sensitive information (ssn’s, employee addresses, etc...) from networked computers
  - Be vigilant. Sluggish performance, unexpected errors, and other uncharacteristic activity may be evidence of a virus infection, trojan or hacked computer.
Prevention

Protecting your privacy On-Line

- Only signup for websites you will use
- Give the minimum amount of information
- Read the website’s/company’s privacy statement
- Don’t sign up for promotional mailings (especially if they have a separate privacy statement)
- Don’t even open spam when possible
- If you do by mistake do not reply
- Don’t reply to any solicitation of “money-for-free”
- Don’t send passwords, acct. #’s, bank routing codes
Prevention

- Protecting your money
  - Shop only on trusted websites featuring encrypted credit card servers (https://)
  - Have 1 credit card with a small limit for online purchases
  - Check your credit card statements for questionable activity and report it immediately
  - Periodically check your own credit report for suspicious inquiries into your credit
Prevention

- Protecting your children
  - Put computer in open, often used, place (Family Room, Living Room, Kitchen)
  - Monitor your child’s online capabilities
  - Learn as they learn and show an interest
  - Limit usage to certain hours or type of use
  - Be aware of drastic changes in behavior
Where can I get more Information?

- www.sans.org
- www.securityportal.com
- www.securityfocus.com
- www.cert.org
- www.nipc.gov
- www.securiteam.com
- www.attrition.org
- www.iss.net/xforce
- www.symantec.com/avcenter
- Mailing Lists/Listservs