

Computer Forensics

Introduction to Computing

Darren Hayes

April, 2008



Computer Forensics

Definition

The Use of Digital Data to Solve or Prevent a
Crime

*The advantage of the emotions is that they lead
us astray, and the advantage of science is that
it is not emotional – Oscar Wilde*

Why Bother?

*We teach people how to remember, we never
teach them how to grow – Oscar Wilde*

Importance

- Growth in Digital Crime:
 - National White Collar Crime Center Survey:
 - 50% of American Households Affected by White Collar Crime in 2005
 - Between 2001 and 2005, the Number of Corporate Fraud Cases, Handled by FBI, Increased 300%



Careers

- ❑ Salaries Range from \$85,000 to \$120,000 p.a.
- ❑ Consulting: \$300 to \$600 per hour
- ❑ Numerous Job Openings



Employers

- ❑ Accounting Firms
- ❑ Local Law Enforcement
- ❑ District Attorney
- ❑ Federal Bureau of Investigation (FBI)
- ❑ U.S. Secret Service
- ❑ U.S. Drug Enforcement Administration (DEA)
- ❑ Homeland Security
- ❑ Private Investigation
- ❑ Software Companies

Complimentary Skills

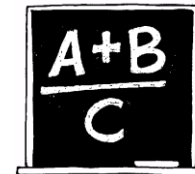


Second Language



Writing

Mathematics



Computing



Law





Skills Acquired

- ❑ Software
- ❑ Hardware
- ❑ Legal
- ❑ Security
- ❑ Ethics & Social Responsibility

Computer Forensics in Action

*The true mystery of the world is the visible, not
the invisible – Oscar Wilde*



Scott Peterson Murder Trial

- Searched Online for
 - Boats
 - Boat Ramps
 - Tides
 - Knots



BTK Killer

- Letter Sent, via E-mail to News Station in Wichita, Kansas
- File Metadata Showed:
 - Author (Dennis)
 - Organization (Christ Lutheran Church)
- Church Website Showed Dennis Rader as Church President

Enron

- ❑ Fastow, Skilling & Lay found Guilty
- ❑ Hundreds of Employee Computers Examined
- ❑ Thousands of E-mails Researched
- ❑ Documents Required Full Text Search Capabilities
- ❑ 31 Terabytes (10^{12} bytes) of Data (~15 Academic Libraries)



BotNets

- Short for ro**BOT NET**work
- A.K.A. *Zombie Army*
- A Network of Compromised Computers
 - Distributed Denial of Service Attack (DDoS)
 - Spam
 - Viruses
 - Ransom
 - Manipulation of Online Polls
 - Keylogging



How Does a BotNet Work?

- ❑ Trojan that Initiates by Opening an Internet Relay Chat (IRC) Channel that Waits for Instructions
- ❑ Hijack Your Connection

BotNet Detection

- ❑ Computer Runs Slower
- ❑ Mysterious Messages Appear

- ❑ Detection:

<http://www.microsoft.com/protect/products/computer/safetyscanner.msp>

- ❑ Event Logger

- ❑ Removal:

<http://www.microsoft.com/security/malwareremove/default.msp>



BotNets for Spam

- 1,500,000 Boxes Infected (ZDNet)
- 70% of Spam Sent Through Infected Boxes
- <http://www.spamhaus.org>



Other Crimes

- Data Hiding
 - Partitions
 - Slack
 - File Manipulation
- Unsecured Networks
- Rootkits
 - Control of Operating System
- Phishing

The Evidence

Consistency is the last refuge of the unimaginative – Oscar Wilde



How to Convict

- Control
- Ownership
- Intent



Data Recovered

- Passwords
- Websites Visited
- Emails (Sent / Received)
- File Creation, Access, Modified, Deletion Dates & Times
- Chat Sessions
- Files Copied
- Programs Installed
- Files Transferred
- Images Viewed or Saved



Devices

- Hard Disk
- Floppy Disk
- Zip Disk
- CD
- DVD
- Blackberry
- USB
- Tapes
- TiVo
- Xbox
- DVR
- Smartphone

Applications

The only thing to do with good advice is pass it on. It is never any use to oneself – Oscar Wilde



Microsoft Applications

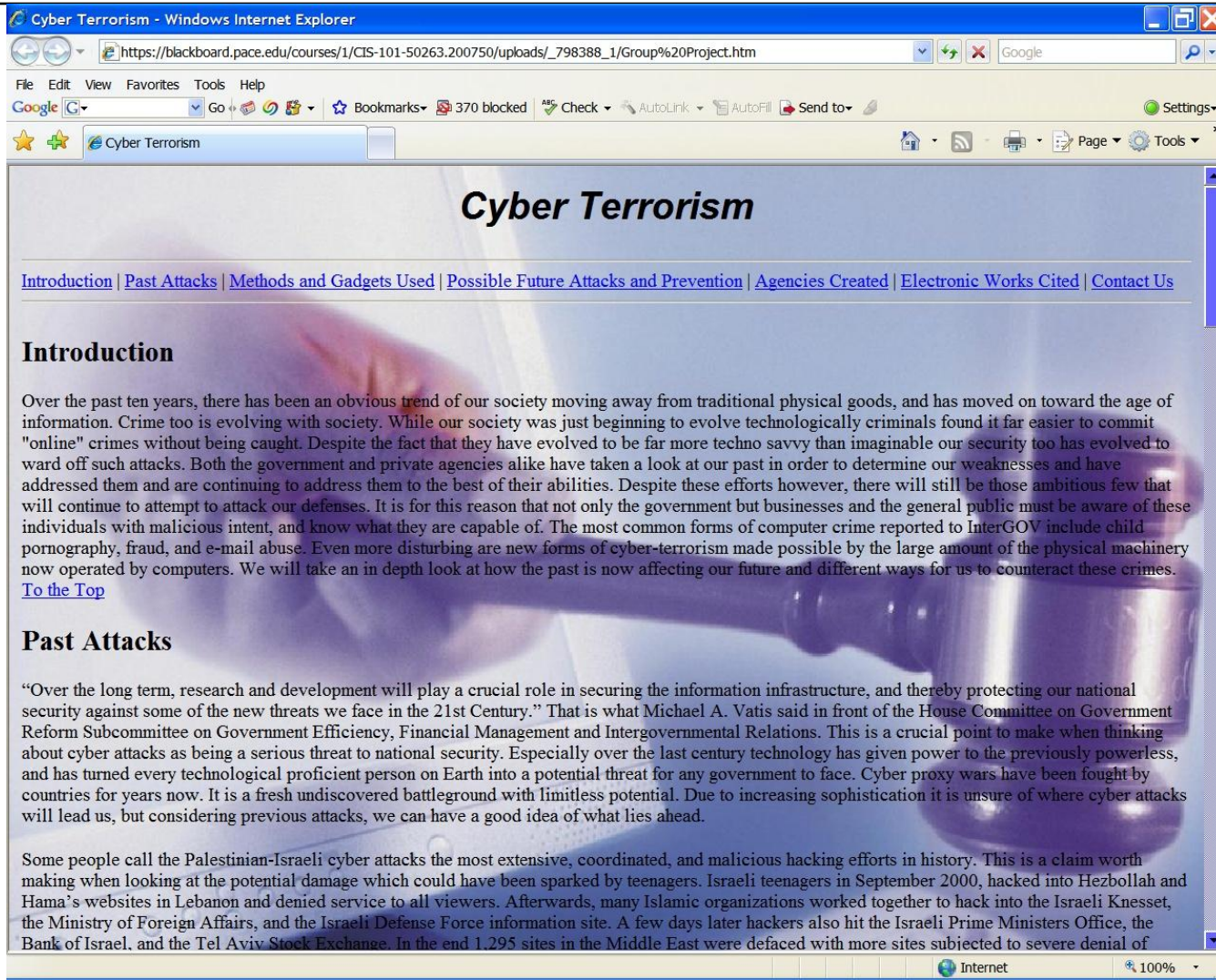
- PowerPoint
 - Student Presentations [Sample](#)
 - Lab Layout [Lab](#)



Microsoft Applications

- Excel
 - Crimes
 - Hardware Inventory
 - Evidence Form (Form)
- Word
 - Research Paper
 - Evidence Form (Form)

Web Design



The screenshot shows a Windows Internet Explorer browser window. The title bar reads "Cyber Terrorism - Windows Internet Explorer". The address bar contains the URL "https://blackboard.pace.edu/courses/1/CIS-101-50263.200750/uploads/_798388_1/Group%20Project.htm". The browser's menu bar includes File, Edit, View, Favorites, Tools, and Help. The toolbar shows the Google search engine, navigation buttons (Go, Back, Forward, Stop, Reload), and other utility buttons like Bookmarks, Check, AutoLink, AutoFill, and Send to. The page content features a large background image of a hand holding a computer mouse. The main heading is "Cyber Terrorism" in a large, bold, black serif font. Below the heading is a horizontal navigation menu with links: Introduction, Past Attacks, Methods and Gadgets Used, Possible Future Attacks and Prevention, Agencies Created, Electronic Works Cited, and Contact Us. The "Introduction" link is selected. The "Introduction" section contains a paragraph of text discussing the evolution of cyber crime and the role of technology. The "Past Attacks" section contains a paragraph of text discussing the role of research and development in securing information infrastructure. The browser's status bar at the bottom shows "Internet" and "100%".

Cyber Terrorism - Windows Internet Explorer

https://blackboard.pace.edu/courses/1/CIS-101-50263.200750/uploads/_798388_1/Group%20Project.htm

File Edit View Favorites Tools Help

Google Go Bookmarks 370 blocked Check AutoLink AutoFill Send to Settings

Cyber Terrorism

Cyber Terrorism

[Introduction](#) | [Past Attacks](#) | [Methods and Gadgets Used](#) | [Possible Future Attacks and Prevention](#) | [Agencies Created](#) | [Electronic Works Cited](#) | [Contact Us](#)

Introduction

Over the past ten years, there has been an obvious trend of our society moving away from traditional physical goods, and has moved on toward the age of information. Crime too is evolving with society. While our society was just beginning to evolve technologically criminals found it far easier to commit "online" crimes without being caught. Despite the fact that they have evolved to be far more techno savvy than imaginable our security too has evolved to ward off such attacks. Both the government and private agencies alike have taken a look at our past in order to determine our weaknesses and have addressed them and are continuing to address them to the best of their abilities. Despite these efforts however, there will still be those ambitious few that will continue to attempt to attack our defenses. It is for this reason that not only the government but businesses and the general public must be aware of these individuals with malicious intent, and know what they are capable of. The most common forms of computer crime reported to InterGOV include child pornography, fraud, and e-mail abuse. Even more disturbing are new forms of cyber-terrorism made possible by the large amount of the physical machinery now operated by computers. We will take an in depth look at how the past is now affecting our future and different ways for us to counteract these crimes.

[To the Top](#)

Past Attacks

"Over the long term, research and development will play a crucial role in securing the information infrastructure, and thereby protecting our national security against some of the new threats we face in the 21st Century." That is what Michael A. Vatis said in front of the House Committee on Government Reform Subcommittee on Government Efficiency, Financial Management and Intergovernmental Relations. This is a crucial point to make when thinking about cyber attacks as being a serious threat to national security. Especially over the last century technology has given power to the previously powerless, and has turned every technological proficient person on Earth into a potential threat for any government to face. Cyber proxy wars have been fought by countries for years now. It is a fresh undiscovered battleground with limitless potential. Due to increasing sophistication it is unsure of where cyber attacks will lead us, but considering previous attacks, we can have a good idea of what lies ahead.

Some people call the Palestinian-Israeli cyber attacks the most extensive, coordinated, and malicious hacking efforts in history. This is a claim worth making when looking at the potential damage which could have been sparked by teenagers. Israeli teenagers in September 2000, hacked into Hezbollah and Hama's websites in Lebanon and denied service to all viewers. Afterwards, many Islamic organizations worked together to hack into the Israeli Knesset, the Ministry of Foreign Affairs, and the Israeli Defense Force information site. A few days later hackers also hit the Israeli Prime Ministers Office, the Bank of Israel, and the Tel Aviv Stock Exchange. In the end 1,295 sites in the Middle East were defaced with more sites subjected to severe denial of

Internet 100%



YouTube

- <http://www.youtube.com/watch?v=9JoX4uxES7Q>
- <http://www.youtube.com/watch?v=cFWRPdn5ywU&feature=related>
- <http://www.youtube.com/watch?v=henEBsGgOdg&feature=related>

Other Applications

- JavaScript
 - Scrolling Text or Forms
- Podcasting (www.camstudio.org)
- Blogging (www.blosxom.com or wordpress.org)
- Wikis (www.wikispaces.com)
- Social Networking (www.ning.com)
- Mashups (www.popfly.com)

Other Applications

- GIS
 - ArcView
 - Google Earth
- <http://jott.com> (Organizer)
- <http://www.scribd.com> (YouTube for Docs)
- <http://twitter.com> (What am I Doing?)
- www.chacha.com (Search Engine)

Computer Forensics Software

- Helix (www.e-fense.com)
 - Imaging (RAM & Hard Drive)
 - NetCat Listener
 - FTK Imager
 - Free

- Invisible Secrets
 - Steganography
 - Costs \$40

Resources

- <http://berghel.com/home.php>
- <http://www.simson.net/cv/pubs.php>
- <http://www.cylab.cmu.edu/>
- <http://www.ne-htcia.org/>
- <http://www.utica.edu/academic/institutes/ecii/ijde/>
- <http://www.ssddfj.org/>



Resources

- <http://www.x-ways.net/>
- <http://www.wireshark.org/>
- <http://www.openwall.com/john/>
- <http://www.oxid.it/>
- <http://www.swgde.org/>
- <http://www.rcfl.gov>



Thanks!

Darren Hayes

dhayes@pace.edu

www.codedetectives.com

*The only thing worse than being talked about is not
being talked about – Oscar Wilde*