Air Force
Research Laboratory

Online Safety & Security

Jeffrey Isherwood
Senior Security Analyst
CISSP, C|EH, CRISC, Linux+, LPIC-1
EXELIS | CIRC CYBER INCIDENT RESPONSE CENTER

Integrity ★ Service ★ Excellence

AFRL

1

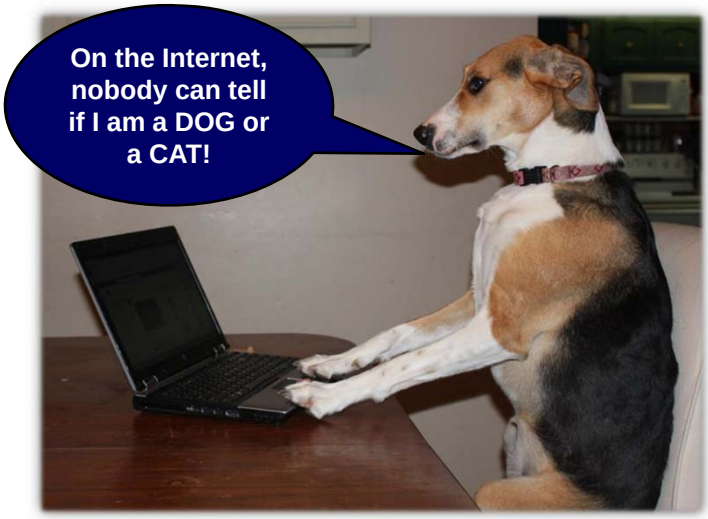
Internet Anonymity

For most people who have “grown up” with the internet…

It does not seem strange to “chat” and interact with people who you cannot see face to face

AFRL

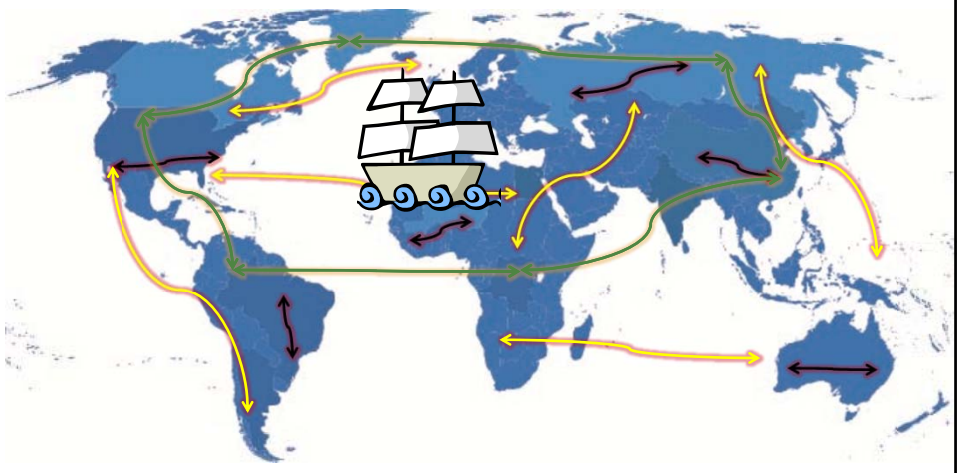
2



AFRL

3

All Points Connected

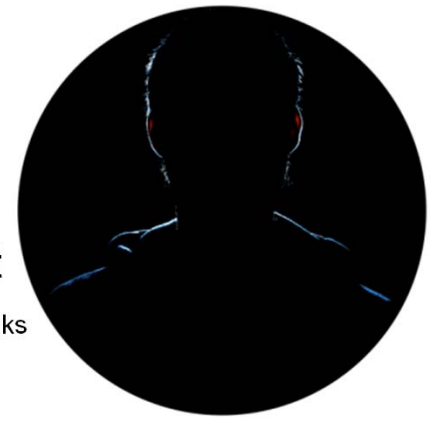


AFRL

4

Dangers Faced In Cyberspace

- Predators
  - Cyber Predators
  - Cyber Stalkers
  - Cyber Bullies
- Fraud and Identity Theft
  - Scams, Phishing, Fake emails, Links
- Inappropriate Content
  - Nudity, violence, drugs, alcohol



AFRL

5

Why is Cyberspace Dangerous

- **Criminals and Predators have the "advantage"**
  - **Sophisticated technological skills and/or equipment**
  - **Distance**
  - **Experience**
  - **Practiced tactics**
  - **Lawlessness**
  - **Anonymity**

AFRL

6

Why is Cyberspace Dangerous

- **Most users have the "disadvantages" of**
  - Innocence, trust
  - Feeling "invincible"
  - A reliance on the technology
  - A desire for acceptance and independence
  - Lack of threat or protection knowledge
  - Place to much information online

AFRL

7

Why is Cyberspace Dangerous

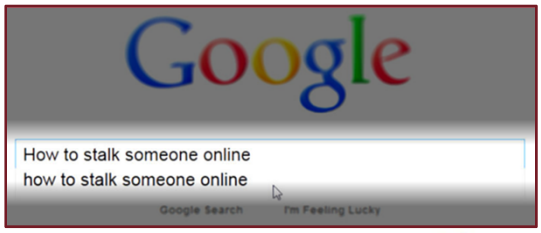
- **Anonymity for criminals & bad guys**
  - Create e-mail accounts with bogus information
  - Services require nothing more than a name or E-mail
  - Services ask for little information
  - Rarely do services validate input
  - Availability of "Anonymizing Services"

AFRL

8

Why is Cyberspace Dangerous

- **Availability Of Personal Information**
  - Interests, hobbies, hangouts, schools, teams
  - Names, addresses, phone numbers
  - Financial information
  - Friends, family
  - Pictures….



AFRL

9

What do YOU do online?

- **Entertainment**
  - Music
  - Movies
  - Games
  - Social Networks
- **Education**
  - Email
  - Online classes
  - Research
  - Collaboration
- **Ecommerce**
  - Auctions
  - Shopping
  - Bargain hunting
- **Communication**
  - Email
  - Instant messenger
  - Social networks

AFRL

10

Poor Selection of "Online Names"

- **Screen Names, Social Media names & Email Addresses**
  - **Are poor when they contain names, schools, locations, or identifying numbe*rs or descriptive terms***

- **EXAMPLES:**
  - **proctorChrLdr**
  - **ClintonBball#22**
  - **RFAGoalie**
  - **NthUticaJIM**
  - **SylvanSally**
  - **BikiniBabe**
  - **HPDiver**
  - **NHHottie**

Poor Passwords

- **Passwords should be something not easily guessed**
  - Like screen names: poor passwords contain names, schools, locations, or identifying and descriptive terms
  - Pets names, favorite songs, books or movies
  - Passwords should not be written down
- **BAD EXAMPLES:**
  - SpongeBob
  - Pink
  - BTRFan
  - volleyball
  - Scruffy
  - Strough

Cyber Predators

- **GATHER INFORMATION ABOUT VICTIMS**
  - Social Networks
  - Instant Messenger Profiles and Directories
  - AOL Profiles
  - Screen names (Handles)
  - Publicly Available Information

- **UTILIZE SOCIAL ENGINEERING TRICKS**
  - Find common interests
  - Target users with low self-esteem
  - Masquerade as a peer, often of the opposite sex
  - Masquerade as other individual the person may be interested in meeting

AFRL

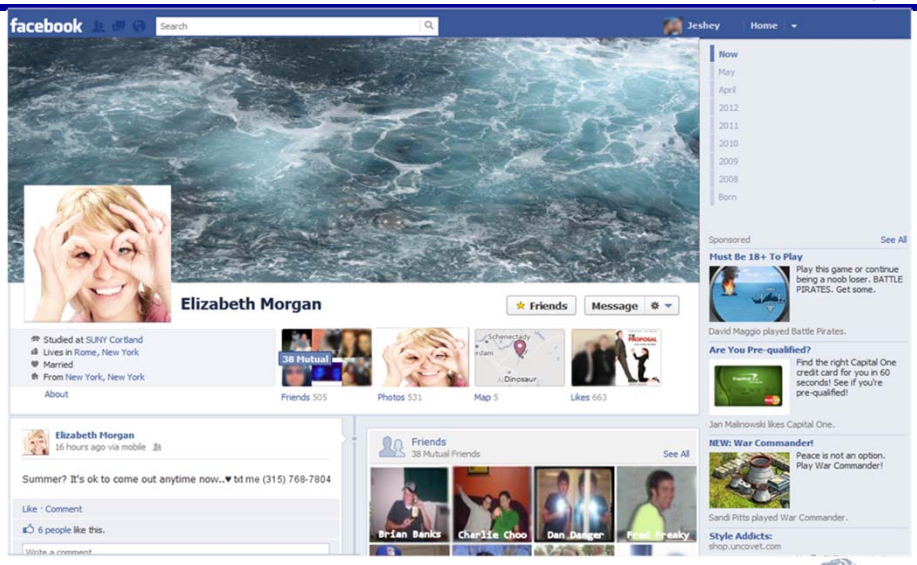
Social Networking

Social Networking allows people to network, interact and collaborate to share information, data and ideas without *geographic boundaries*.

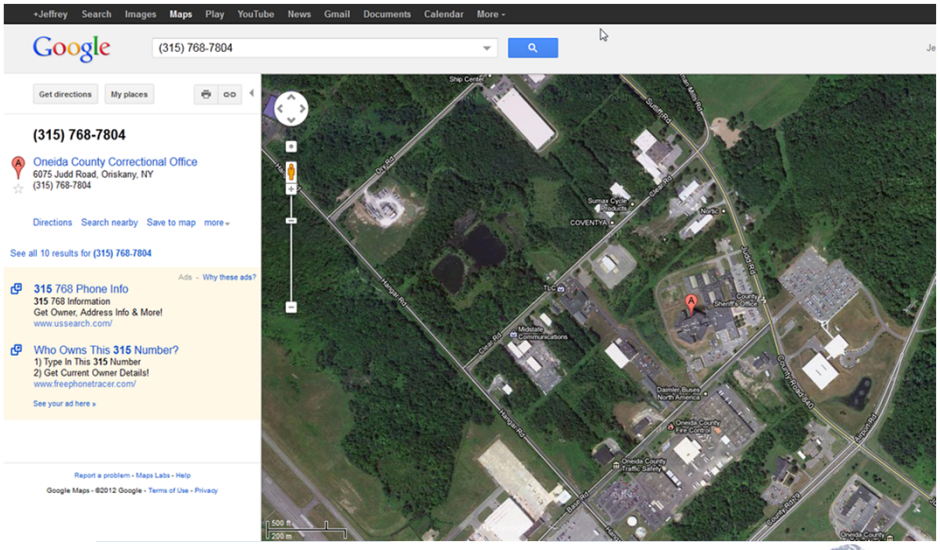
Google Social, friendster, facebook, TAGGED, foursquare, hi5, flickr, ask.fm, orkut, Blogger, USTREAM.TV, kik., xanga, netvibes, digg, myspace.com, PARTY FLOCK, Fropper, YouTube Broadcast Yourself, YAHOO! 360° BETA, del.icio.us, LinkedIn

AFRL

Social Network Profiles



Online Profiles



Use Caution!

Once Data appears on the Internet – it can be there FOREVER!

Data Persistence

www.interesting-people.org/archives/interesting-people/199412/msg00040.html

[Date Prev] | [Thread Prev] | [Thread Next] | [Date Next] -- [Date Index]

Subject: **Microsoft, AP Disavow Story**

- *From*: David Farber <farber@central.cis.upenn.edu>
- *Date*: Sat, 17 Dec 1994 16:44:35 -0500

HOW LONG DOES INFORMATION STAY ONLINE?

NEW YORK (AP) Microsoft Corp. on Friday disavowed a joke circulating on the Internet computer network of a fake news story that said the software company planned to settle with the Roman Catholic church.

The fake news story purported to have been written by The Associated Press. The news service said it had no dealings with the joke.

The joke has circulated on the Internet, the global network of computer networks, for at least a week.

Microsoft issued its statement after several days of calls from people who thought the ``story'' might be true, company spokeswoman Christine Santucci said.

``Given the seriousness of the issue, it's not something we wanted to be associated with,'' she said.

Neither Microsoft nor AP know where the fake story originated.

Microsoft, based in Redmond, Wash., is the world's largest maker of personal computer software. The AP, headquartered in New York, is the world's largest news organization.

CyberBullying

- **Harassing, mean and vicious**
  - Emails
  - Cell phone
    - Calls
    - Pictures
    - Messages
  - Websites
  - Blogs and journals
  - Online polls
  - Instant messages
  - Chat rooms
  - Social Media
  - "Photoshopping"

AFRL

19

CyberBullying

- **What do bullies do?**
  - Reveal embarrassing secrets
  - Impersonate
  - Misrepresent
  - Start rumors
  - Spread lies
  - Blackmail
  - Start "Hate Groups"
  - Create "Slam Books"
  - "Photoshop"

AFRL

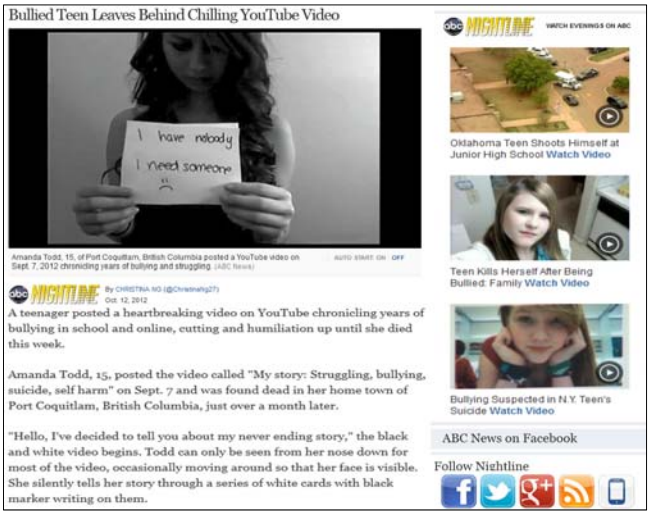
20

CyberBullying: Amanda Todd's Story

- She was not a "shut in" or online addicted child
- Sports
  - Swimming (competitively)
  - Figure Skating
  - Cheerleading
  - Gymnastics
  - Soccer

- Amanda Todd was a 10th grade Canadian high school student
- On September 7, 2012, 15 year old Amanda Todd posted a video on YouTube using flash cards to share her online experiences about being blackmailed, bullied, and then later physically assaulted.
- On October 10, 2012 she committed suicide
- **She Changed Schools Twice**
- **Her family moved to a new city**
- **She tried to commit suicide on two prior occasions**

Cyber Bullying: Amanda Todd



Bullied Teen Leaves Behind Chilling YouTube Video

Amanda Todd, 15, of Port Coquitlam, British Columbia posted a YouTube video on Sept. 7, 2012 chronicling years of bullying and struggling. (ABC News)

NIGHTLINE By CHRISTINA NG (@Christinang27) Oct. 12, 2012

A teenager posted a heartbreaking video on YouTube chronicling years of bullying in school and online, cutting and humiliation up until she died this week.

Amanda Todd, 15, posted the video called "My story: Struggling, bullying, suicide, self harm" on Sept. 7 and was found dead in her home town of Port Coquitlam, British Columbia, just over a month later.

"Hello, I've decided to tell you about my never ending story," the black and white video begins. Todd can only be seen from her nose down for most of the video, occasionally moving around so that her face is visible. She silently tells her story through a series of white cards with black marker writing on them.

NIGHTLINE WATCH EVENINGS ON ABC

Oklahoma Teen Shoots Himself at Junior High School Watch Video

Teen Kills Herself After Being Bullied: Family Watch Video

Bullying Suspected in N.Y. Teen's Suicide Watch Video

ABC News on Facebook

Follow Nightline

CyberBullying

Cobb middle school student files suit alleging cyberbullying

By Gracie Bonds Staples, The Atlanta Journal-Constitution
11:14 a.m. Friday, April 27, 2012

David Goldman, AP

Alex Boston, 14, sits in her home Thursday, April 26, 2012, in Acworth, Ga. Boston's family this month filed a libel lawsuit claiming two classmates humiliated her by using a doctored photo to set up a phony Facebook account in her name, and then stacking the page with phony comments

Enlarge photo

David Goldman, AP

Alex Boston, 14, center, poses with her mom Amy, left, and father Chris and a screen shot of the phony Facebook account that was set up in Alex's name.

She's a slender, rough-and-tumble sort of girl who looked forward to the end of school when she could let loose during her middle school's field day activities.

Next to the last day of school, it was her favorite time of year. Last year was different. Last year, instead of running relay races and trying her hand at the balloon toss, she found herself in a virtual tug of war with her Cobb County classmates, two of whom had posted a fake Facebook page using her name. It included distorted photos of her and made false claims about her friends.

"It turned into hell," the girl's father said Thursday. "It was the worst day of her life."

Early this month, Alexandria Boston filed a defamation suit against the classmates saying they created the fake Facebook page. Her parents hope the suit could lead to legislation that could give schools more authority to stop cyberbullying.

The suit, filed in Cobb County Superior Court, names a boy and girl and their parents, charging them with libel and intentional infliction of emotional distress. (Although the Atlanta Journal-Constitution typically does not name juveniles in these types of cases, Alex agreed to use her name because she wants to raise awareness about cyberbullying.)

The students' parents could not be reached for comment. A spokesman for the Cobb County schools said the district has a policy not to comment on ongoing litigation.

Creating fake Facebook pages to bully someone is not an uncommon practice, said Bill Nigut, the Southeast regional director of the Anti-Defamation League.

"ADL has a good relationship with Facebook," he said, "and we talk to them pretty regularly about issues like this and other examples of their site being used to promote hatred and bigotry."

Harassment & Cyberstalking

THE DENVER POST — Tuesday, November 30, 1999

Killer used 'Net to stalk victim

Online research services gave slain woman's personal information

BOSTON — Ever since junior high, Liam Youens had been obsessed with Amy Boyer. He kept Web pages where he wrote of perverted tastes and his desire to kill her, and used the Internet to find out all about her.

Last month, Youens, armed with a gun and the location of the dentist's office where Boyer worked, shot her to death, then killed himself.

The shootings took place Oct. 15 in Nashua, N.H., where Youens, 21, and his 20-year-old victim had gone to school together.

Youens' thoughts and plans are detailed in a yellow report, drawn partly from the Web sites where he debated with himself whether to kill Boyer, 4-11 another former classmate, or others in the Nashua High School and kill as many people as he could, The Boston Globe reported Monday.

Youens paid hundreds of dollars to on-line research services to determine Boyer's birth date, Social Security number, address and the location of the dentist's office.

"It's actually obscene that you can find out about people on the Internet," he wrote.

Boyer's stepfather, Tim Remsburg, said he is considering a lawsuit against Creative Investigations and Tripod, the two online companies where Youens maintained his Web sites.

Through both graduated from Nashua High in 1997, friends and family say Boyer wasn't aware of Youens or his obsession with her.

Youens' online journal chronicles the one-way relationship, recounting a humiliating day when she brushed past him in the school lunchroom, and a Valentine's Day when he realized she had received a rose from a boyfriend.

He also recalled realizing in the 10th grade that he was in love with her, and deciding shortly thereafter to kill her and himself, the Globe said.

"That was the basic plan for the next half decade," he wrote.

But Youens, who dropped out of college after a year and quit living at his parents' home, found it difficult to stalk Boyer, in part because she often was surrounded by family. So he turned to online research services to track her.

Remsburg said he is angry that Creative and Tripod didn't monitor their Internet and that Youens was able to use their computers, including Docusearch and Intelenetics, to hunt down Boyer's personal information.

Internet companies say monitoring this kind is not technologically feasible. Federal law protects Internet service providers from liability for material posted on Web sites.

A Tripod official said that almost no one visited Youens' site and that they would have told police about it had they seen it. Tripod officials said they destroyed Youens' site as soon as police notified them about it.

A Docusearch spokesman refused to comment on Youens' site there.

A spokeswoman for one research agency told the Globe the information it sells is gathered from public sources such as court or motor vehicle records.

"It's actually obscene what you can find out about people on the Internet."– Liam Youens

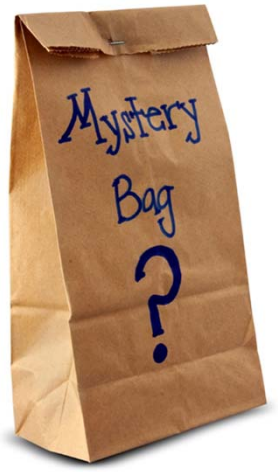
Online Fraud

- **Auction fraud**
  - Shilling
  - Counterfeit
  - Stolen property
  - Bogus merchandise
- **Get-rich-quick schemes**
- **Phishing**
- **Phony Prizes**
- **Cheap Stuff!**
- **FREE STUFF!**
  - Hardware (Mp3 Players, Cameras, DVDs)
  - Software (Windows, MS-Office, Games, Anti-Virus)
  - Cheat codes, "cracked software"

AFRL

Social Scams

- **Profile Viewers and Profile Blockers**
- **Free technology (iPad/iPhone/Xbox etc…)**
- **Free "Game Credits"**
- **Free Items, Gift Cards & Tickets**
- **Breaking News Stories**
- **Phishing Attempts to Steal Your Login Info**
- **Bogus Chat Messages**
- **Shocking Headlines**
- **Fake Celebrity Stories**
- **"Help I'm Stranded and Need Money"**



AFRL

Being Safe Online?

- **Think before you click**
- **If something looks too good to be true – it probably is, free usually isn't actually free!**
- **Should anything online make you uncomfortable – TELL SOMEONE!**
- **Don't post things online you wouldn't posted on the bulletin board at your school or your refrigerator**
- **Information you post can last longer than you think, be careful**
- **NEVER share your password with anybody but your parents!**
- **You are not alone - Tell a friend, tell a parent, tell a teacher, tell a policeman**

AFRL

27

RESEARCH LAB (Choose One)

Using your favorite search engine:

1. **Find one instance of Ethics or Policy Violation that resulted in a crime, or security incident**
   - Give a synopsis of the instance
   - Make a suggestion how it may have been avoided
2. **Find one instance of cyber bullying or inappropriate use of Social Media**
   - Give a synopsis of the instance
   - Make a suggestion how it may have been avoided

AFRL

28

Air Force Research Laboratory

Integrity ★ Service ★ Excellence

Intro to Computers

Lt Trevor Vranicar
Air Force Research Laboratory
Information Directorate

Bottom Line Up Front

Computers are an essential part of our daily lives, but many people do not know the components nor classifications of these parts

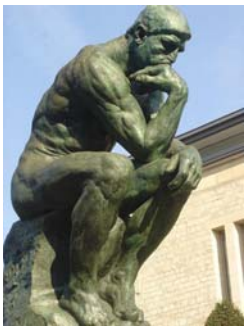
The following lesson will allow you to be able to distinctly identify the parts of a computer and classify the part as hardware or software

Outline

What is a Computer?

Hardware vs. Software

Parts of a Computer



YOUR THOUGHTS:

What is a Computer?

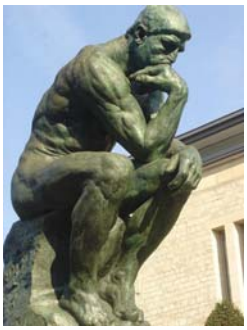
Photo Source: http://en.wikipedia.org/wiki/File:ThinkingMan_Rodin.jpg

Definition: Computer

"A computer is a programmable machine designed to sequentially and automatically carry out a sequence of arithmetic or logical operations."

-Wikipedia.org

Photo Source: http://en.wikipedia.org/wiki/File:Wikipedia-logo-v2.svg



YOUR THOUGHTS:
NOW WHAT IS A COMPUTER?

Photo Source: http://en.wikipedia.org/wiki/File:ThinkingMan_Rodin.jpg

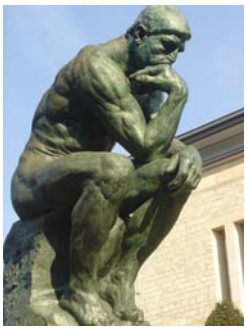
Examples of Computers







Photo Source: http://en.wikipedia.org/wiki/File:Jacquard.loom.full.view.jpg; http://en.wikipedia.org/wiki/File:Columbia_Supercomputer - NASA_Advanced_Supercomputing_Facility.jpg; http://en.wikipedia.org/wiki/File:SSEM_Manchester_museum.jpg; http://en.wikipedia.org/wiki/File:Centcom20040818.jpg; http://en.wikipedia.org/wiki/File:Delta-C_personal_computer.jpg; http://en.wikipedia.org/wiki/File:Xbox-Console-Set.png; http://en.wikipedia.org/wiki/File:Galaxy_Nexus_smartphone.jpg



YOUR THOUGHTS:

Hardware vs. Software

Photo Source: http://en.wikipedia.org/wiki/File:ThinkingMan_Rodin.jpg

Hardware VS Software

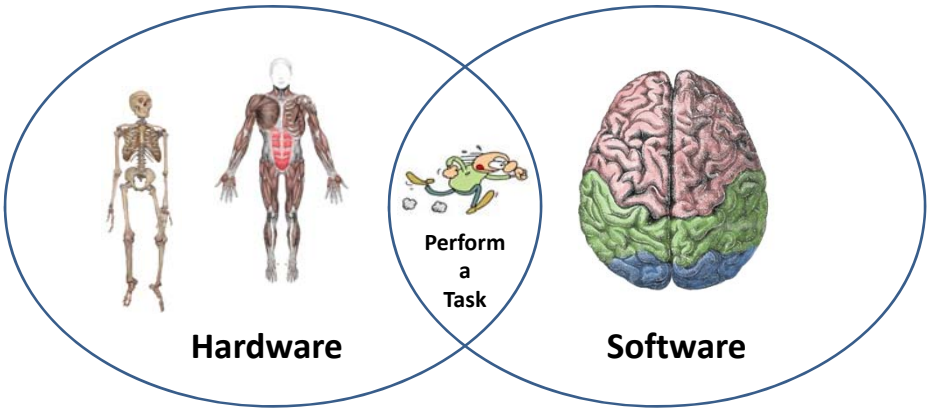


Photo Source: http://en.wikipedia.org/wiki/File:Skeleton2.jpg; http://en.wikipedia.org/wiki/File:Muscles_anterior.png; http://en.wikipedia.org/wiki/File:Cerebral_lobes.png

Hardware VS Software

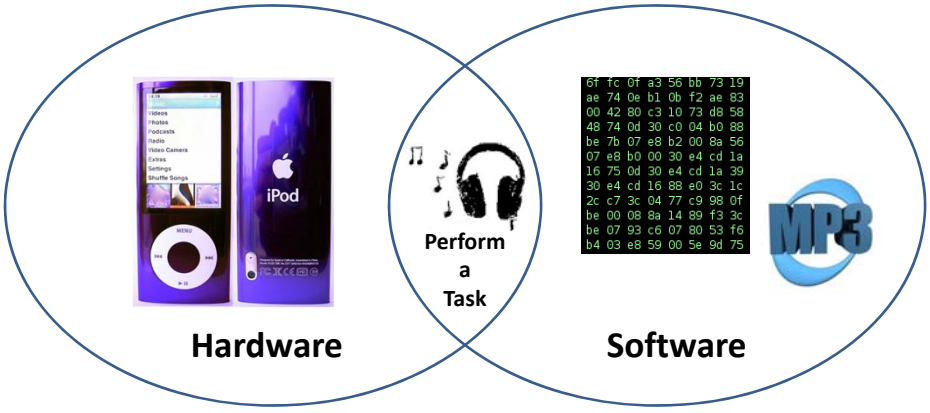


Photo Source: http://en.wikipedia.org/wiki/File:IPod-Nano-5G-front-back.png; http://en.wikipedia.org/wiki/File:Binary_executable_file2.png

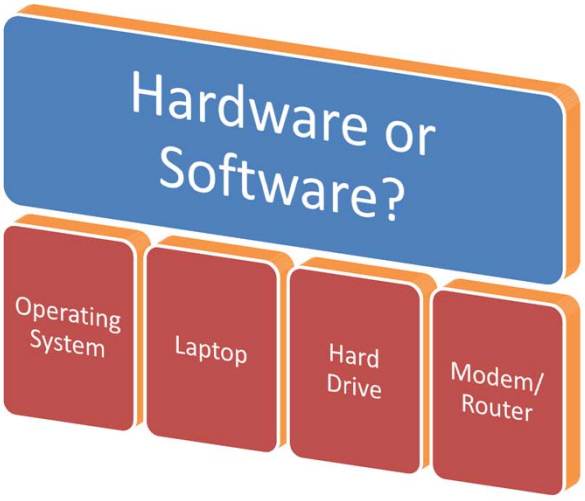
Definitions

- **Hardware*:**
  are component **devices** which are typically installed into or peripheral to a computer case to create a personal computer upon which system software is installed including a firmware interface such as a BIOS and an operating system supporting application software that performs the operator's desired functions.

- **Software*:**
  is a collection of computer programs and related data that provide the instructions for telling a computer what to do and how to do it. In other words, software is a conceptual entity which is a set of computer programs, procedures, and associated documentation concerned with the operation of a data processing system

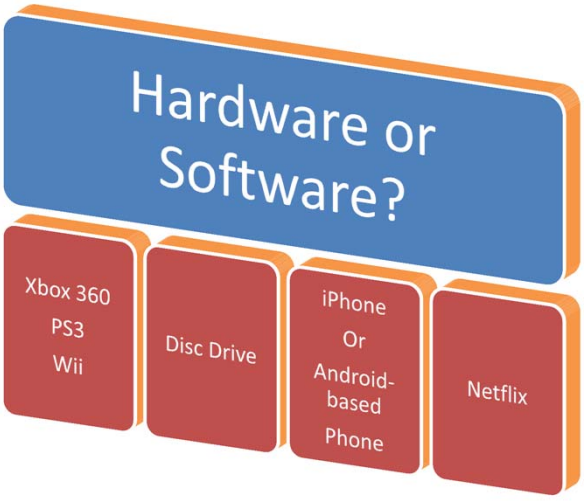
Taken from Wikipedia.org

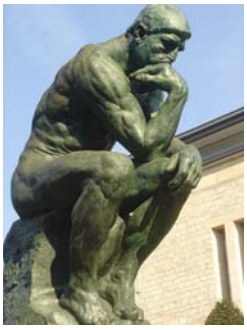
Pop Quiz



Pop Quiz

Pop Quiz





YOUR THOUGHTS:

Parts of a Computer

Photo Source: http://en.wikipedia.org/wiki/File:ThinkingMan_Rodin.jpg

Parts of a Computer

- Processing
  - Central Processing Unit (CPU)
  - Graphics Processing Unit or “video card” (GPU)
- Input/output Devices aka “peripherals”
  - Disk drives
  - Keyboard/Mouse
  - Monitor
  - Game Controllers
- Storage/ Memory
  - Hard Disk Drive (HDD) internal and external
  - Flash/Thumb Drives
  - Read Only Memory (ROM), Read Access Memory (RAM)
- Support (E.G. Power Supplies and Fans)

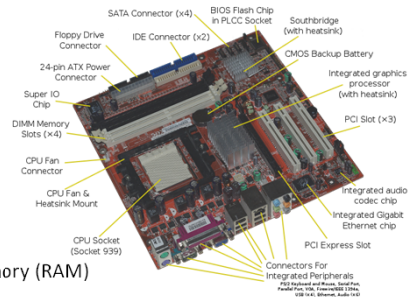
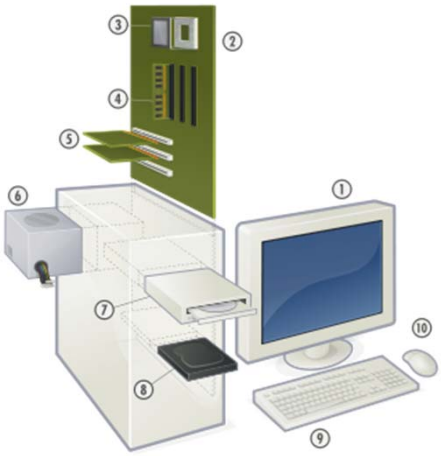


Photo Source: http://en.wikipedia.org/wiki/File:Acer_E360_Socket_939_motherboard_by_Foxconn.svg

Pop Quiz: Guess that part!



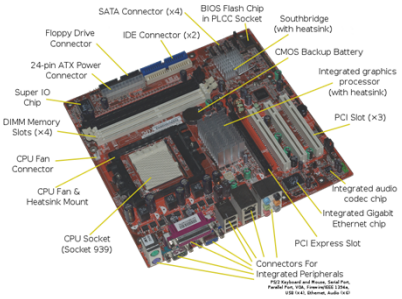


Photo Source: http://en.wikipedia.org/wiki/File:Personal_computer,_exploded_5.svg; http://en.wikipedia.org/wiki/File:Acer_E360_Socket_939_motherboard_by_Foxconn.svg

Guess that part! Answer Key

1. Monitor: Output device - Displays video from computer
2. Motherboard: Is the central component that allows for power and cross communication between devices
3. CPU: The core computational entity on a computer (“The brain”)
4. RAM: Read Access Memory – Stores temporary memory for processing between memory and computing devices
5. Expansion cards: Allows upgrade/additions to computer (e.g. graphics card, sound card, etc)
6. Power supply: Supplies electricity to the computer
7. Optical disc drive: Long term, unpowered storage (lasers)
8. Hard disk drive: Long term, unpowered storage (magnetics)
9. Keyboard: I/O device
10. Mouse : I/O device

Example: How Parts Interact During Startup

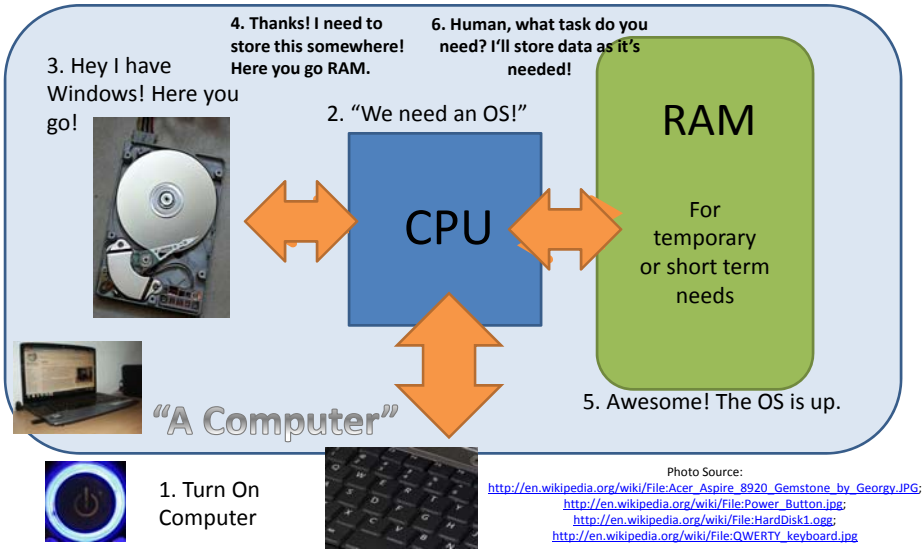


Photo Source:
http://en.wikipedia.org/wiki/File:Acer_Aspire_8920_Gemstone_by_Georgy.JPG;
http://en.wikipedia.org/wiki/File:Power_Button.jpg;
http://en.wikipedia.org/wiki/File:HardDisk1.ogg;
http://en.wikipedia.org/wiki/File:QWERTY_keyboard.jpg

LAB TIME!

SAFETY BRIEF!

Integrity ★ Service ★ Excellence

Networking Fundamentals

Jake Sears
Griffiss Institute

Rules of Engagement

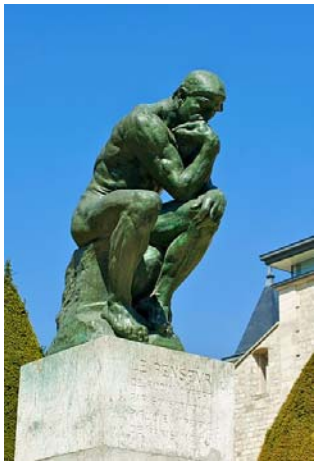
- **Raise your hand**
- **HAVE FUN!**

Approved for Public Release; Distribution Unlimited: 88ABW-2014-2909, 16 JUN 2014

Network Fundamentals Overview

- Network Basics
- Network Exercise
- Wireless Basics
- Wireless Exercise

Network Basics



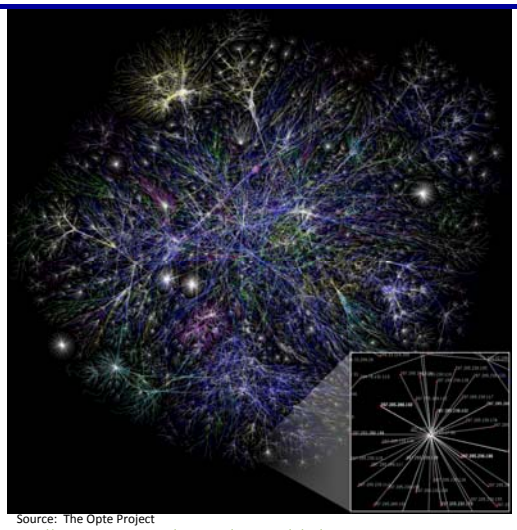
Outline

- Objective
- Types of Networks
- Network Devices
- Dial-Up Access
- Ethernet Wiring
- Summary
- References

Objective

Provide a basic understanding of how computers are connected together via a network.

What is a Network?



Source: The Opte Project
http://upload.wikimedia.org/wikipedia/commons/d/d2/Internet_map_1024.jpg
License:
Creative Commons Attribution 2.5 Generic

What is a Network?

A collection of nodes that are connected to each other and share resources or data

Types of Networks

- **LAN – A Local Area Network covers a small geographic area (like a home, office, or group of buildings)**

Source: http://en.wikipedia.org/wiki/Local_area_network

WAN – Wide Area Network is a computer network that covers a broad area (such as across metropolitan, regional, or national boundaries)

- **A network that uses routers and public communications links**
- **Connect LANs and other types of networks together**

LAN Networking Standards

- **Ethernet**
  - **Operates at many speeds**
  - **Defines a number of wiring and signaling standards for the physical layer**
  - **May be used over Twisted Pair, Coaxial Cable, Fiber Optic Cable, etc. media**
- **Wireless Fidelity (Wi-Fi)**
  - **Wireless LAN standard (IEEE 802.11), used in place of (and in addition to) Ethernet for many home and small office networks**

Network Devices

- **Network Interface Controller (NIC)**
  - **Computer hardware that allows computers to communicate over computer network using cables or wirelessly. It provides physical access to a networking medium and provides a low-level addressing system**

Source: http://en.wikipedia.org/wiki/File:Network_card.jpg
License: Creative Commons Attribution-Share Alike 3.0 Unported

Router

- **Router**
  - **A device that connects multiple LANs and or WANs**
  - **Provide routing of traffic to specific destination devices based on table look ups**
  - **Establishes lines of communication to connect devices together forming a network**
  - **Acts as a switchboard operator. It controls where data will go.**

Switch and Hub

- **Switch**
  - **A networking device that performs transparent bridging (connection of multiple network segments) at up to the speed of the hardware**
- **Hub**
  - **A device for connecting multiple twisted pair or fiber optic Ethernet devices together, making them act as a single segment**

What is the difference between a switch and a hub?

- **Think of a *switch* like a telephone network. You dial a phone and tell a single person the information that they needed to know.**

AFRL

What is the difference between a switch and a hub?

- **A *Hub* can be thought of as a loud speaker in a building. It is going to tell everyone information instead of just one person, even if not everyone need the info**

AFRL

Modem (Modulator-Demodulator)

- Turns the digital '1s and 0s' of a personal computer into sounds that can be transmitted and received over telephone lines
- Cable Modem
  - Provides access to a data signal sent over the cable television infrastructure primarily used to deliver broadband Internet
- DSL Modem
  - Digital Subscriber Line
  - DSL or xDSL, provides digital data transmission over the wires of a local telephone network
- Dial up
  - A form of Internet access through which the client uses a modem connected to a computer and a telephone line to dial into an Internet service provider's (ISP) node to establish a modem-to-modem link, which is then routed to the Internet

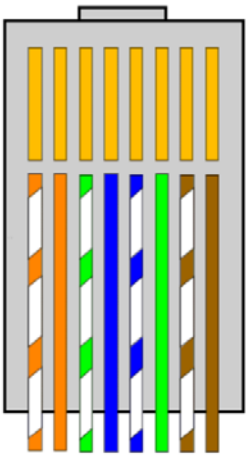
Ethernet Cable

- Ethernet cables connect devices on a local area networks such as PCs, routers and switches

- This cable has an RJ-45 jack on each end

Exercise Time

- **Create your own Ethernet cables**



Summary

This section provided a basic understanding of how our computers are connected together in a network

List of References

- http://en.wikipedia.org/wiki/Local_area_network
- http://en.wikipedia.org/wiki/Metropolitan_Area_Network
- http://en.wikipedia.org/wiki/Wide_area_network
- http://fcit.usf.edu/network/chap5/chap5.htm
- http://www.computerhope.com/jargon/r/ringtopo.htm
- http://en.wikipedia.org/wiki/Dial-up
- http://en.wikipedia.org/wiki/Modem
- http://en.wikipedia.org/wiki/Twisted_pair

Exercise Time!

Set up a network of your own with your group's computers and one of the supplied routers

IP Addressing

- An IP (Internet Protocol) address is assigned to devices on a network.
- Each device gets its own IP address.
- The most commonly used version of IP is IPv4. IPv4 consists of four, one to three digit numbers.
- Example of IPv4: 192.168.1.40
- There are about 4.3 billion IPv4 addresses in the world

http://en.wikipedia.org/wiki/IP_addressing

IP Addressing

- Due to the restraints on the amount of IPv4 address a new version of addressing is coming about called IPv6.
- IPv6 has 340 undecillion (340 followed by 36 zeros different addresses.
  - 340,000,000,000,000,000,000,000,000,000,000,000
- IPv6 Example: 2001:0db8:85a3:08d3:1319:8a2e:0370:7334

http://en.wikipedia.org/wiki/IP_addressing

Domain Name System (DNS)

- A DNS can be thought of as a phone book. If you looked up the Griffiss Institute in a phone Book you would find the number 838-1696
- Websites are the same way. If you wanted to go to Google you could use 8.8.8.8
- Every website has its own IP address

http://en.wikipedia.org/wiki/DNS

Summary

- This section provided background on the IP Model and several frequently used protocols.

List of References

- http://www.ictp.trieste.it/~radionet/1998_school/networking_presentation/page6.html
- http://en.wikipedia.org/wiki/OSI_Model
- http://en.wikipedia.org/wiki/TCP/IP_model
- http://www.cgisecurity.com/lib/bill/encapsulation.gif
- http://www.cisco.com/univercd/cc/td/doc/product/iaabu/centri4/user/scf4ap1.htm
- http://www.visi.com/~mjb/Drawings/TCP_Header.pdf
- http://en.wikipedia.org/wiki/IP_addressing
- http://en.wikipedia.org/wiki/SMTP
- http://en.wikipedia.org/wiki/Telnet
- http://en.wikipedia.org/wiki/FTP
- http://en.wikipedia.org/wiki/HTTP
- http://computer.howstuffworks.com/web-server1.htm
- http://en.wikipedia.org/wiki/HTTPS
- http://www.sportop.com/ClothingPrograms/ordering-faqs.cfm
- http://en.wikipedia.org/wiki/Transport_Layer_Security
- http://en.wikipedia.org/wiki/DNS
- http://www.comptechdoc.org/independent/networking/guide/dns.gif
- http://www.theshulers.com/whitepapers/internet_whitepaper/index.html#http

Wireless Basics

Outline

- Objective
- What is a Wireless LAN?
- How Does It Work?
- WLAN Benefits
- Summary
- List of References

Objective

- This section will provide a basic understanding of how a wireless local area network (WLAN) works.

Just a quick reminder…

- What is a LAN
- A Local Area Network covers a small geographic area (like a home, office, or group of buildings)

What is a Wireless LAN?

- Same as a LAN just wireless!
- Users no longer have to deal with annoying cables
- Links two or more computers through radio waves

http://en.wikipedia.org/wiki/WLAN

What is a Wireless LAN?

- Computers and other devices must have a Wireless Network Card in order to connect to the router

How Does a WLAN Work?

- Suitably equipped computes can enter into either an Ad-hoc (also called Peer-to-Peer) or Infrastructure network

http://en.wikipedia.org/wiki/WLAN

How Does a WLAN Work?

- Currently, the most widely used standards for WLAN operation are 2.4ghz
- Newer devices can use 5ghz band width

http://en.wikipedia.org/wiki/Wifi

How Does a WLAN Work?

- In Infrastructure Mode, many wireless Access Points (APs) broadcast their Service Set ID (SSID) which is used to locate and identify them.

WLAN Advantages and Disadvantages

Advantages	Disadvantages
• Convenience	• Security
• Mobility	• Range
• Productivity	• Reliability
• Deployment	• Speed
• Expandability	
• Cost	

http://en.wikipedia.org/wiki/WLAN

Summary

- This section provided a basic understanding of how a wireless local area network (WLAN) works.

Exercise Time!

Minecraft

List of References

- http://en.wikipedia.org/wiki/WLAN
- http://en.wikipedia.org/wiki/Wifi

Cloud Computing

Outline

- Objective
- Cloud Definition
- Service Models
- Cloud Discussion

Objective

Provide an understanding of what "cloud computing" is and how it works.

What is a Cloud?

The set of hardware, networks, storage, services and interfaces that combine to deliver aspects of computing as a service

What is “Cloud Computing”?

- **Taking files and breaking them apart and storing the parts on different, remote, storage arrays**
- **When the user wants to see the file, they use a client to go out and get the parts and reassemble it into the original file**

Air Force Research Laboratory

Integrity ★ Service ★ Excellence

Cryptography

Dr. Sarah Muccio
Dr. Erich Devendorf
Air Force Research Laboratory
Information Directorate

AFRL

Security Principles

- **Confidentiality – keeping secrets secret**
- **Integrity – protecting data from unauthorized modification**
- **Availability – data / systems available when requested**
- **Authentication – verifying identity**
- **Non-Repudiation – denying actions**

Cryptography

- Assures confidentiality & integrity
- Plays no role in availability
- Permits authentication, non-repudiation
- Substitution v transposition ciphers
- Symmetrical v asymmetrical crypto
- Private-key v public-key crypto
- Passwords and 1-way ciphers

Defense In-Depth

- Badges
- Front door, badge access, PIN
- Locked offices
- Personal computers
- Passwords, CAC, biometrics
- Screen savers
- Shredders

Substitution

Caesar Shift Cipher:

Shift=?

Convertsplaintextintociphertext

Dpowfsutqmbjoufyujoupdjqifsufyu

Transposition

Convertplaintextintociphertext

cttteopeornlxctvatieeiipxrnnht

conver
tplain
textin
tociph
ertext

Cryptography

Ciphertext = Ka (Plaintext)

Plaintext = Kb (Ciphertext)

Symmetrical Cryptography Ka = Kb

aka Private-Key Cryptography

Asymmetrical Cryptography Ka <> Kb

aka Public-Key Cryptography

Data Encryption Standard

- **Controlled by 56-bit key, 7 characters**
- **Input and Output 64 bits, 8 characters**
- **Monoalphabetic Substitution Cipher**
- **Given key, input gives same output**
- **Symmetrical: uses same key to encrypt and decrypt**
- **Strengthened by chaining, blocking**

Advanced Encryption Standard

- Controlled by 128, 192, or 256-bit key
- Input and Output 128 bits
- Substitution-Permutation network
- Given key, input gives same output
- Symmetrical: uses same key to encrypt and decrypt
- All key lengths of the AES algorithm are sufficient to protect classified information up to the SECRET level.
- TOP SECRET information will require use of either the 192 or 256 key lengths

RSA Algorithm

- Rivest, Shamir, and Adleman (RSA)
- $C = (P^e) \bmod n \qquad P = (C^d) \bmod n$
- Choose *p, q* large prime numbers
- $n = p * q \qquad z = (p-1) * (q-1)$
- Pick *e*, find *d* so that

$$(e * d) \bmod z = 1$$

- Publish *e, n*. Keep *d* secret.

UNCLASSIFIED

RSA Example

- ASSUME THAT THE RANDOM VALUES FOR THE PRIMES *P* AND *Q* HAVE BEEN CHOSEN AS

$$P = 47$$

$$Q = 73$$

- THEN THE PRODUCT *N* OF THESE TWO PRIMES IS CALCULATED:

$$N = P \cdot Q = 3431$$

- THE EULER TOTIENT *Z* FOR THESE TWO PRIMES IS FOUND EASILY USING THE FOLLOWING FORMULA:

$$Z = (P - 1) \cdot (Q - 1) = 3312$$

- NOW THAT WE HAVE *N* AND *Z*, WE SHOULD DISCARD *P* AND *Q*, AND DESTROY ANY TRACE OF THEIR EXISTENCE.
- NEXT, WE RANDOMLY SELECT A NUMBER *E* THAT IS GREATER THAN 1, LESS THAN *N*, AND RELATIVELY PRIME TO Z. OF COURSE, THERE IS MORE THAN ONE CHOICE POSSIBLE HERE, AND ANY CANDIDATE VALUE YOU CHOOSE MAY BE TESTED USING THE EUCLIDIAN METHOD.

$$E = 425$$

- THEN THE MODULAR INVERSE OF *E* IS CALCULATED TO BE THE FOLLOWING:

$$D = 1769$$

- WE NOW KEEP *D* PRIVATE AND MAKE *E* AND *N* PUBLIC.

UNCLASSIFIED

11

UNCLASSIFIED

- ASSUME THAT WE HAVE PLAINTEXT DATA REPRESENTED BY THE FOLLOWING SIMPLE NUMBER:

$$\text{PLAINTEXT} = 707$$

- THE ENCRYPTED DATA IS COMPUTED BY $C = ME \pmod N$ AS FOLLOWS:

$$\text{CIPHERTEXT} = 707^{425} \pmod{3431} = 2142$$

- THE CIPHERTEXT VALUE CANNOT BE EASILY REVERTED BACK TO THE ORIGINAL PLAINTEXT WITHOUT KNOWING *D* (OR, EQUIVALENTLY, KNOWING THE VALUES OF *P* AND *Q*). WITH LARGER BIT SIZES, THIS TASK GROWS EXPONENTIALLY IN DIFFICULTY. IF, HOWEVER, YOU ARE PRIVY TO THE SECRET INFORMATION THAT *D* = 1769, THEN THE PLAINTEXT IS EASILY RETRIEVED USING $M = C^D \pmod N$ AS FOLLOWS:

$$\text{PLAINTEXT} = 2142^{1769} \pmod{3431} = 707$$

- If you compile the following code, you will verify that the results shown above are correct. While you look at this code, keep in mind that a realistic RSA implementation uses a much larger modulus than $n = 3431$, and a realistic message typically contains too many bits to be represented by a tiny number such as $m = 707$.

UNCLASSIFIED

12

UNCLASSIFIED

Private v Public

- Private = symmetrical
  - Same key → Trust
  - Key distribution, Key hierarchy
  - Fast, hardware implementations
- Public = asymmetrical
  - Total strangers
  - Much slower than symmetrical
- Session keys: use public-key to distribute private session keys

UNCLASSIFIED

UNCLASSIFIED

Code Example

```
"Operated on this morning.
 Diagnosis not yet complete but
 results seem satisfactory and
 already exceed expectations. Local
 press release necessary as interest
 extends great distance. Dr. Groves
 pleased. He returns tomorrow. I
 will keep you posted."
```

UNCLASSIFIED

Codes

- Encryption: 1-to-1 substitution
- Codes: 1-to-n or n-to-1 substitution
- Require code books
- Superencipherment= ciphers + codes
- Transliteration: 1-to-1 mapping
- Japan used superencipherment and transliteration in WWII

Enigma

- It is an electromechanical machine that used a combination of wired rotors and plugs to change each letter as it is typed. The encryption process began by depressing a lettered key that generated an electrical current. The current passed through a plugboard and three rotors, a reflecting plate, and back through the three rotors and plugboard.
- The “letter” changed each time it encountered a plug, rotor, and the reflecting plate. Eventually, the cipher letter was illuminated on a light panel and the operator wrote that letter down. Because the first of the three rotors moved with each keystroke, the cipher letter changed, even if the same letter key was repeated.

Photo Source: http://en.wikipedia.org/wiki/File:EnigmaMachineLabeled.jpg

SIGABA/ECM

- The U.S. Army's SIGABA, called the ECM (Electric Cipher Machine) in the Navy, was the only machine system used during World War II to remain completely unbroken by an enemy. It utilized the same principle of rotating, removable, wired rotor wheels that the German Enigma employed.
- However, unlike the stepping motion of the Enigma, the SIGABA/ECM's motion appeared to be random. It wasn't, but it was so complicated, the German's never broke it, and the Japanese gave up trying.

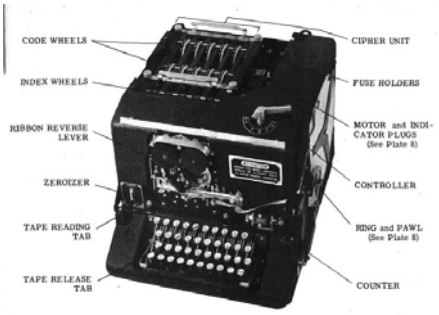


Photo Source: http://en.wikipedia.org/wiki/File:SIGABA-labelled-1.jpg

Code Example

- Plaintext: WE MUST PROTECT THE IMPORTANT DATA.
- Find the first word in your

  "50 Cyber Questions Every Airman Can Answer".
- Write down the Question number, row number, and the Nth word into that row.
  Example: WE = Question 50, Row 2, 6th word in.
- Separate the numbers by a period.
  WE=50.2.6
- Repeat Steps 2-4 for every word in your sentence.
  WE=50.2.6 MUST = 38.7.7 PROTECT = 12.8.1
  THE = 8.10.5 IMPORTANT= 40.15.7 DATA = 13.7.11

50.2.6 38.7.7 12.8.1 8.10.5 40.15.7 13.7.11

One-Way Hash

- Unix Passwords
- User enters plaintext, OS hashes, compares hash to stored value
- No way to recover plaintext from hash
- Common target of dictionary attacks
- Vulnerable locally to key loggers
- Network vulnerable to packet sniffers

Digital Signatures

- Use public-key cryptography
- Require 3rd-party Certificate Authority
- IE browsers use local key + SSL + CA
- Provides authentication
- Ensures non-repudiation
- Provides integrity
- Legally binding

Steganography

- **Steganography is the art and science of communicating in a way which hides the existence of the communication.**
- **Many forms: in text, watermarks, audio, images, MP3s, video**
- **Much different than *Cryptography* (codes and ciphers)**

History

In ancient Greece, text was written on wax covered tablets. In one story Demeratus wanted to notify Sparta that Xerxes intended to invade Greece. To avoid capture, he scraped the wax off of the tablets and wrote a message on the underlying wood. He then covered the tablets with wax again. The tablets appeared to be blank and unused so they passed inspection by sentries without question.

Photo Source: http://en.wikipedia.org/wiki/File:Wachstafel_rem.jpg; http://en.wikipedia.org/wiki/File:Douris_Man_with_wax_tablet.jpg

Historical Examples

Herodotus (485 – 525 BC) is the first Greek historian. His great work, The Histories, is the story of the war between the huge Persian empire and the much smaller Greek city-states.

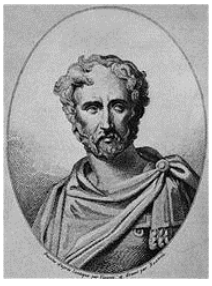
Herodotus recounts the story of Histaiaeus, who wanted to encourage Aristagoras of Miletus to revolt against the Persian King. In order to securely convey his plan, Histaiaeus shaved the head of his messenger, wrote the message on his scalp, and then waited for the hair to regrow. The messenger, apparently carrying nothing contentious, could travel freely. Arriving at his destination, he would shave his head, revealing the secret message.

Photo Source: http://en.wikipedia.org/wiki/File:Herodotusstatue.JPG

Slide provided by the STEGINT group

Historical Examples

- **First techniques included invisible ink, secret writing using chemicals, templates laid over text messages, microdots, changing letter/word/line/paragraph spacing, changing fonts**



- Pliny the Elder and "Invisible Ink"

- Giovanni Porta and the hard boiled egg

Photo Source: http://en.wikipedia.org/wiki/File:Plinyelder.jpg; http://en.wikipedia.org/wiki/File:Chicken_Egg_without_Eggshell_5859.JPG

Slide provided by the STEGINT group

Actually sent by a German Spy in WWII

Apparently neutral's protest is thoroughly discounted and ignored. Isman hard hit. Blockade issue affects pretext for embargo on by products, ejecting suets and vegetable oils.

Apparently neutral's protest is thoroughly discounted and ignored. Isman hard hit. Blockade issue affects pretext for embargo on by products, ejecting suets and vegetable oils.

Taking the second letter in each word the following message emerges:

Pershing sails from NY June 1.

Null ciphers (Example)

News Eight Weather: Tonight increasing snow. Unexpected precipitation smothers eastern towns. Be extremely cautious and use snowtires especially heading east. The highways are knowingly slippery. Highway evacuation is suspected. Police report emergency situations in downtown ending near Tuesday.

Null ciphers (Example)

News Eight Weather: Tonight increasing snow. Unexpected precipitation smothers eastern towns. Be extremely cautious and use snowtires especially heading east. The highways are knowingly slippery. Highway evacuation is suspected. Police report emergency situations in downtown ending near Tuesday.

Newt is upset because he thinks he is President.

Images

- **There are usually two type of files used when embedding data into an image.**
- **The innocent looking image which will hold the hidden information is a "**container**."**
- **A "**message**" is the information to be hidden. A message may be plain-text, ciphertext, other images or any thing that can be embedded in the least significant bits (LSB) of an image.**

Traffic Patterns

- **Presence of data is information**
- **Traffic patterns may indicate activity**
- **“Chatter” before attack**
- **Hide data by hiding traffic patterns**
- **Send encrypted garbage**

Conclusions

- **Strong cryptography unbreakable**
- **Supports confidentiality, integrity, authentication, non-repudiation**
- **Do not develop your own algorithm!**

Cyber Threats to Security

Jeffrey Isherwood
Senior Security Analyst
CISSP, C|EH, CRISC, Linux+, LPIC-1

Integrity ★ Service ★ Excellence

EXELIS | CIRC CYBER INCIDENT RESPONSE CENTER

AFRL

Name that Cyber Crime!

Physical Crimes:

- **Breaking and Entering**
- **Eavesdropping**
- **Harassment**
- **Vandalism**
- **Destruction of Private Property**
- **Possession of Stolen Goods**
- **Theft**

AFRL

Overview

- **What is security & Why do we need it?**
- **Criminals!**
- **Cyber Threats, Weapons & Attacks**
  - **Malware**
  - **Hacking**
  - **Social Engineering**
  - **Google Hacking**

The Many Faces of Computer Crime in the News

Its not just about Hacking!

- < Terrorism - Zacarias Moussaoui
- < Homicides - Scott Peterson, Dennis Rader
- < Espionage - Aldrich Ames
- < Financial Fraud - ENRON

HACKERS!

Hacker is a word that has two meanings:

- **Traditionally, a Hacker is someone who likes to play with Technology.**
- **Recently, Hacker has taken on a new meaning as someone who maliciously breaks into systems for personal gain.**

AFRL

5

Types of hackers

- **Professional hackers**
  - **Working for "Someone"**
  - **White Hats – Professional Security Experts**
  - **Black Hats – the Bad Guys**
    - **Corporate Spies**
    - **Foreign Spies**
- **Script kiddies**
  - **Mostly kids/students**
    - **Use tools created by black hats,**
- **Underemployed Adult Hackers**
  - **Typically Former Script Kiddies**
    - **Can't get employment in the field**
    - **Want recognition in hacker community**
    - **Big in eastern European countries**

AFRL

6

Types of Hackers

- **Criminal Hackers**
  - **Real criminals, are in it for whatever they can get no matter who it hurts**
- **Disgruntled Employees**
  - **Most dangerous to an enterprise as they are "insiders"**
  - **Since many companies subcontract their network services a disgruntled vendor could be very dangerous to the host enterprise**
- **Ideological Hackers {Hackitivists}**
  - **hack as a mechanism to promote some political or ideological purpose**
  - **Usually coincide with political events**

AFRL

7

Weapon Economics

How much does a B2 stealth bomber cost?

How much does an F35 stealth fighter cost?

What does an MQ-9 Reaper Drone cost?

What does a cyber weapon cost?

AFRL

8

After the Attacks?

Nuclear Weapon

Hiroshima

Cyber Weapon

```
6E 6F 6E 00  43 61 6E 6F
68 6F 74 20  41 36 30 00
00 00 00 00  B4 00 00 00
01 00 00 00  32 30 30 34
32 3A 33 30  3A 32 35 00
00 00 86 03  00 00 9D 82
00 00 00 90  07 00 04 00
```

Target HQ

Traditional Cyber Threats

- Viruses, Worms, Spyware, Malicious Apps
  Botnets
  - Peer-to-Peer Networks
  - Pirated Software
- Portable Devices
- Hacking
  - Denial of Service
  - Data Theft
  - Data Corruption
  - Eavesdropping
  - Account Hijacking

Malware

- What is malware?
  - Any malicious code
  - Disrupt computer operation
  - Unauthorized access
  - Numerous forms
    - Viruses
    - Worms
    - Trojans
    - Rootkits
    - Spyware
    - Bots
- Intent vs. features

AFRL

11

Traditional Malware Threats

- MALICIOUS PROGRAMS THAT PERFORM UNDESIRED OR UNEXPECTED FUNCTIONS
  - Relaying personal information to attacker
  - Allow for the recording of computer screen, keys typed
  - Method of obtaining credit card or financial data
- PROGRAMS TRANSMITTED TO VICTIM VIA:
  - E-mail attachments (sometimes from friends)
  - Downloadable games
  - Instant messenger file sharing
  - Masquerading hyperlinks
  - Social Network hooks…

AFRL

12

How Malware Works

Malware Effects

- Plant backdoor
- Network congestion
- Further infection
- Destroys / alters information
- Pivot point / middle ground
- Information Leaks

Malware Effects

- **Indicative Behaviors**
  - Slows Down System
  - Redirects Your Browser
  - Causes Annoying Pop-ups
  - "Strange behavior"

The best malware is that which you do not notice!

AFRL

Viruses

- **A program that can replicate itself**
- **Can infect other files**
  - Execute code
  - Write to memory
- **Can spread with removable media or over networked file systems**
- **Resident**
  - "Live" in memory and intercept operations
  - Replicate when appropriate operations are intercepted
- **Non-resident**
  - "Finder" and "Infector" modules
  - Search for new hosts, infect, transfer control to infected application

AFRL

Worms

- Similar to Viruses
- Replication is often network based
- No need to attach to other executables
- Self-replicating via security vulnerability exploits

Trojans

- Malicious code within a container that appears to be non-malicious
- Two types:
  - Standalone: masquerades as another program like a game or other file
  - Corrupted: a useful application that has been altered to include malicious code

Spyware

- Software that collects personal information about users without their knowledge
- Information recorded with a variety of techniques
- Purposes
  - Criminal: password or credit card number theft
  - Marketing: recording Internet search history for targeted advertising or displaying pop-ups

Botnet

- A collection of software robots (bots)
- Compromised computers (zombies) running programs, usually worms, Trojan horses, or backdoors, under a common command and control infrastructure
- The botnet originator can control the group remotely
- Botnets are exploited for various purposes, including DDoS attacks, creation of mail relays for spam, click fraud (creating false web page accesses), and the theft of application serial numbers, login IDs, and financial information like credit card numbers

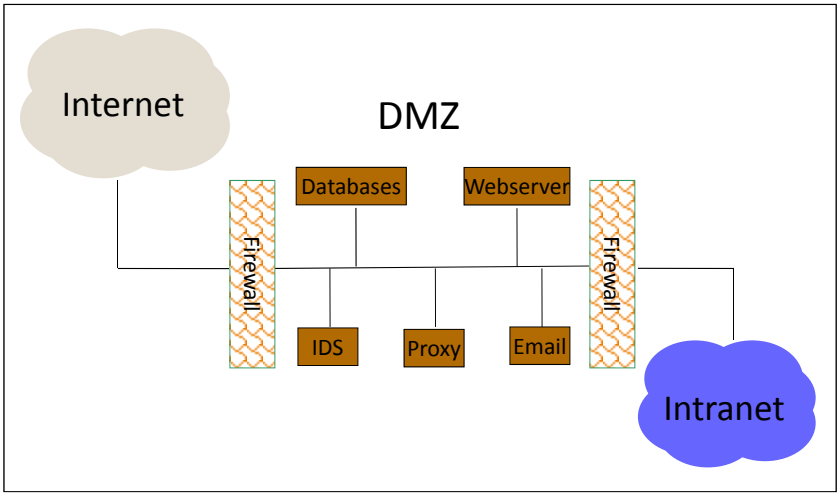
http://en.wikipedia.org/wiki/Botnet

Dangers of Portable Technology

- Mobile Data devices are…
- Easy to lose
- Easy to infect
- Easy to steal
- Bring data where no data has gone before…

21

Network Defenses



22

Hacking – "The Process"

1. Preparation
2. Footprinting
3. Enumeration & Fingerprinting
4. Identification of Vulnerabilities
5. Attack – Exploit the Vulnerabilities

AFRL

Preparation

- Identification of Targets – company websites, mail servers, extranets, etc.
- Signing of Contract
  - Agreement on protection against any legal issues
  - Contracts to clearly specifies the limits and dangers of the test
  - Specifics on Denial of Service Tests, Social Engineering, etc.
  - Time window for Attacks
  - Total time for the testing
  - Prior Knowledge of the systems
  - Key people who are made aware of the testing

AFRL

Enumeration & Fingerprinting

- Specific targets determined
- Identification of Services / open ports
- Operating System Enumeration

Methods

- Banner grabbing
- Responses to various protocol (ICMP &TCP) commands
- Port / Service Scans – TCP Connect, TCP SYN, TCP FIN, etc.

Tools

- Nmap, FScan, Hping, Firewalk, netcat, tcpdump, ssh, telnet, SNMP Scanner

AFRL

25

Identification of Vulnerabilities

Vulnerabilities

- Insecure Configuration
- Weak passwords
- Unpatched vulnerabilities in services, Operating systems, applications
- Possible Vulnerabilities in Services, Operating Systems
- Insecure programming
- Weak Access Control

AFRL

26

Identification of Vulnerabilities

Methods

- **Unpatched / Possible Vulnerabilities – Tools, Vulnerability information Websites**
- **Weak Passwords – Default Passwords, Brute force, Social Engineering, Listening to Traffic**
- **Insecure Programming – SQL Injection, Listening to Traffic**
- **Weak Access Control – Using the Application Logic, SQL Injection**

AFRL

27

Attack – Exploit the vulnerabilities

- **Obtain as much information (trophies) from the Target Asset**
- **Gaining Normal Access**
- **Escalation of privileges**
- **Obtaining access to other connected systems**

Last Ditch Effort – Denial of Service

AFRL

28

Attack – Exploit the vulnerabilities

Network Infrastructure Attacks

- Connecting to the network through modem
- Weaknesses in TCP / IP, NetBIOS
- Flooding the network to cause DOS

Operating System Attacks

- Attacking Authentication Systems
- Exploiting Protocol Implementations
- Exploiting Insecure configuration
- Breaking File-System Security

Physical Access

- **Dumpster diving**
  - Its amazing what people throw in the trash
    - Personal information
    - Passwords
    - Good doughnuts
  - Many enterprises now shred all white paper trash
- **Inside jobs**
  - Disgruntled employees
  - Terminated employees (about 50% of intrusions resulting in significant loss)

Once inside, the hacker can...

- Modify logs
  - To cover their tracks
  - To mess with you
- Steal files
  - Sometimes destroy after stealing
  - A pro would steal and cover their tracks so to be undetected
- Modify files
  - To let you know they were there
  - To cause mischief
- Install back doors
  - So they can get in again
- Attack other systems

AFRL

Social Engineering

- Psychological manipulation
- Pretexting: inventing a scenario (pretext) to persuade a target to do what you want
  - More than a simple lie
  - Usually involves prior research or set up and the use of pieces of known information

- LINK1: Jack Vale Social Media Experiment Video
- LINK2: Jack Vale Reveal Video

AFRL

Meet Sophie Draufster

- **Parent: Filip Maertens**
- **Her last name is an anagram of Fraudster**
- **Born in 2010 on facebook & LinkedIn**
- **Purpose: Social engineering of executives at large consulting firms**
- **Facebook Friends: 105**
- **LinkedIn Requests: 133**
- **Divulging Personally Identifying Information (PII): 73**
- **Date Requests: 33**

AFRL

33

Spam

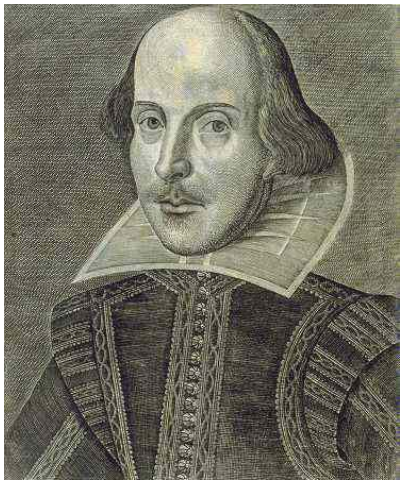
- Spam is electronic junk e-mail
- Spam costs the ISPs and others a lot of $$$ to prevent and/or to remove.
- At its worst spam is used by scammers, hackers, and others to market and prey on literally millions of users at a very low cost.

"I'm hungry. Find some Spam and cookies!"

AFRL

34

Identity Theft



"But he that filches from me my good name

Robs me of that which not enriches him

And makes me poor indeed." - Shakespeare, *Othello*, Act III. Scene III.

Phishing Example

From: eBay Billing Department <aw-confirm@ebay.com>
To: you@uml.edu
Subject: Important Notification

This link points to a bogus site that often will infect and attempt to corrupt or steal data from your computer or to coerce you into divulging private information when You access it.

The World's Online Marketplace®

Register for eBay

Dear valued customer

Need Help?

We regret to inform you that your eBay account could be suspended if you don't re-update your account information. To resolve this problems please click here and re-enter your account information. If your problems could not be resolved your account will be suspended for a period of 3-4 days, after this period your account will be terminated.

For the User Agreement, Section 9, we may immediately issue a warning, temporarily suspend, indefinitely suspend or terminate your membership and refuse to provide our services to you if we believe that your actions may cause financial loss or legal liability for you, our users or us. We may also take these actions if we are unable to verify or authenticate any information you provide to us.

Due to the suspension of this account, please be advised you are prohibited from using eBay in any way. This includes the registering of a new account. Please note that this suspension does not relieve you of your agreed-upon obligation to pay any fees you may owe to eBay.

Regards,

Safeharbor Department

eBay, Inc

The eBay team.

This is an automatic message. Please do not reply.

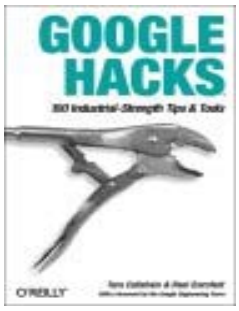
Google™

Google Hacking Basics

AFRL

Intro: “Google Hacking”

- "Google Hacking” is the use of Google’s data stores for naughty things.
- Makes extensive use of the advanced Google syntaxes.
- Is trivially easy to do and is rather trendy.
- An *excellent* guide to get up to speed on the techniques of "Google Hacking” is the O‘Reilly book *Google Hacks* by Tara Calishain.



AFRL

Google Hacking

- Good to understand how Google works
  - Understand then how Google can work for attackers to gain sensitive information
  - It can also help you do research for homework and science projects! ☺
  - On the surface, searching Google is straight forward.
  - But, there are many special parameters (some of which are undocumented)
  - You can use these parameters to exclude everything but the data you're looking for.

AFRL

39

Google Syntax Examples

- " "/-/+/( )
- **Site:**
- **Filetype:**
- **Related:**
- **Link:**
- **[all]inanchor**
- **[all]inurl:**
- **[all]intext:**
- **[all]intitle:**

- (interz0ne | outerz0ne) extraz0ne
- site:.mil
- filetype:.doc
- related:yak.net
- inanchor:"miserable failure"
- inurl:robots.txt
- intext:keyword
- inurl:TITLE

AFRL

40

Hacking???

- Ponder this:
  - What if it were surface mail and not email?
  - What if the voyeur were standing outside your dorm room or your sister's bedroom?
  - What if the break-in was to your house or dorm room and the only thing they did was to leave you a note saying: "Ha-ha, I can get in any time!"
  - What if the stolen property was your car?
  - Where sensitive information is involved, can we afford to believe that nothing has been changed or compromised even by accident?

AFRL

Exercise

- **See handouts**

AFRL

Information & Data Hiding:

Steganography, Metadata and Hidden Objects

Jeffrey Isherwood
Senior Security Analyst
CISSP, C|EH, CRISC, Linux+, LPIC-1

Integrity ★ Service ★ Excellence

EXELIS | CIRC CYBER INCIDENT RESPONSE CENTER

AFRL

Data Hiding

- **Concepts**
  - **Steganography**
  - **Metadata**
  - **Hidden Objects**
- **Discussion**
  - **Potential uses**
- **Challenges to security**

AFRL

Data Hiding

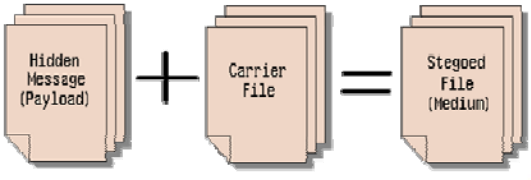
- **Steganography**
  - Data intentionally hidden INSIDE another peice of data
- **Metadata**
  - Data ABOUT other data

- **Hidden Objects**
  - Data EMBEDDED inside a file that contains data

3

Steganography Defined:

- Steganography comes from the Greek word “steganos” which means “covered” and “graphie” which means “writing.”
- Allows users to create a covert channel for secret communication by utilizing various types of media to conceal a message:
  - Images (.bmp, .gif, .jpg, .png, etc.)
  - Text
  - Executable Files
  - Audio
  - Video



4

Definitions of Key Stego Terms

- ***Embedding Program:*** A program designed to hide a payload within a carrier file, this produces a "stegoed file"
- ***Payload File:*** A file that is to be hidden
- ***Carrier File:*** A file that is selected to carry the payload/hidden file
- ***Stegoed File:*** A file that contains a payload/hidden file, also called a stego medium
- ***Clean File:*** A file that does not contain a payload/hidden file
- ***False Negative:*** Is the result of a detection tool identifying a stegoed file as a clean file
- ***False Positive:*** Is the result of a detection tool identifying a clean file as a stegoed file
- ***Stego-Key:*** The password used to encode the payload file

History of Steganography

Earlier Steganography Techniques:

440 B.C.

- **Shaving the head of a messenger**
- **Wax Tablets**

World War I & II

- **Invisible Inks (Milk, vinegar, fruit juices, urine, chemical)**
  - **Revealed via heat, chemicals or light**
- **Micro dots (Photographic Reduction)**
- **Plain sight message (null ciphers)**
  - *(more on this one later…)*

Uses of Steganography

- **Secret Communications**
  - **Spies**
  - **Criminals**
  - **Terrorists**
- **Concealing Incriminating Evidence such as:**
  - **Illegal data (pictures, videos, audio)**
  - **Financial records**
  - **Contact information**
  - **Diagrams for building bombs and weapons**
  - **Communication between individuals**
  - **Instructions**

Methods of Steganography

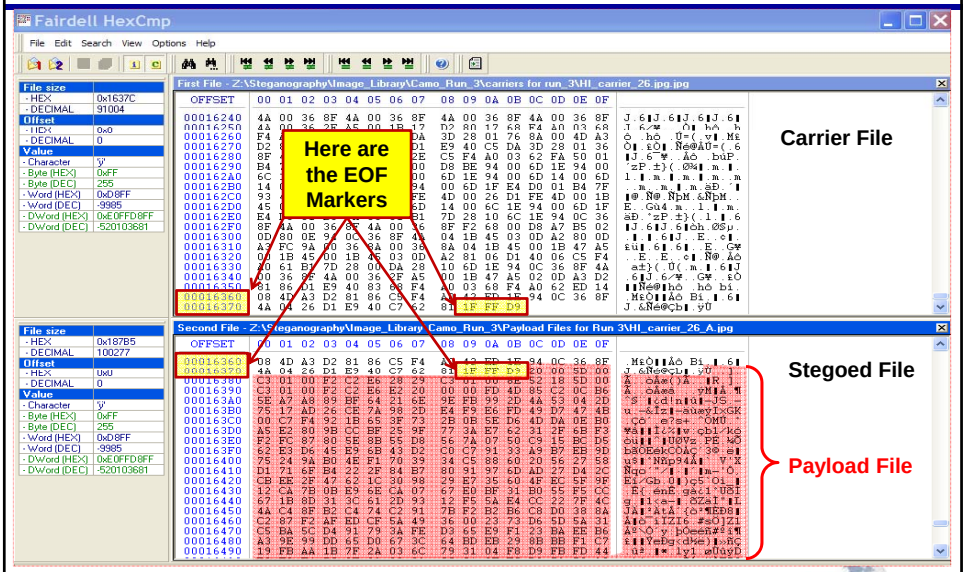
- **The methods utilized by Steganography Embedding Tools can be *"generally"* categorized into three groups:**
  1. ***Insertion***
  2. ***Substitution***
  3. ***Generation***
- **In each method, the end-user needs to know the Steganography embedding program, the type of encryption used and the stego-key, in order to extract the payload file**

Insertion-Based Stego

A hiding technique that appends the hidden message/payload file to the END of the carrier file

- **Carrier file may be many types**
- **File size of stegoed image is increased as compared to the carrier file**
- **Original composition (appearance) of the carrier file is unchanged to the naked eye**

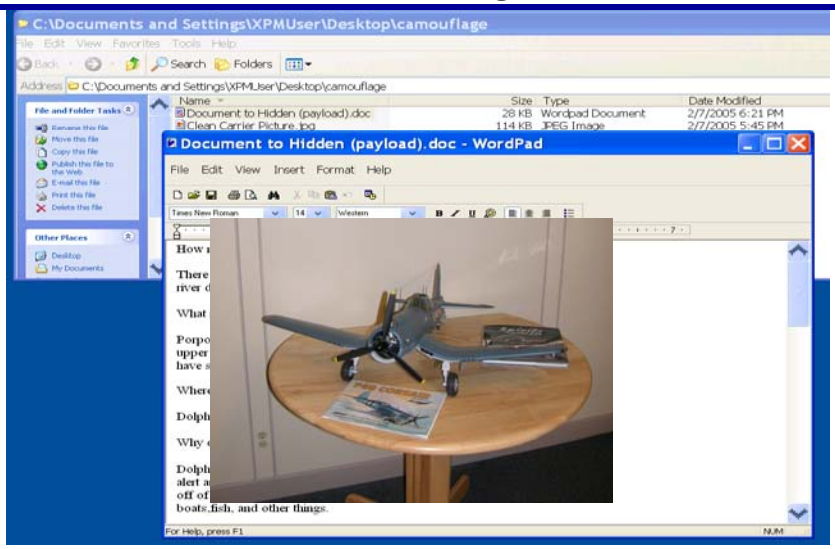
Insertion-Based Hiding Area: After EOF Marker



Insertion-Based Program: Camouflage

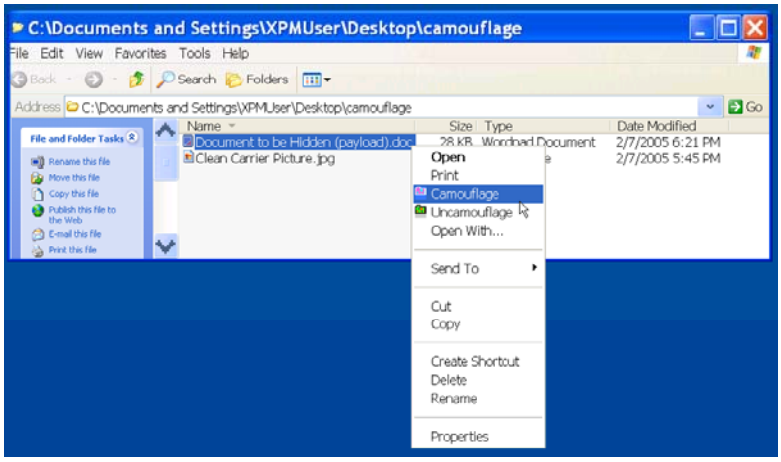
11

Insertion-Based Program: Camouflage

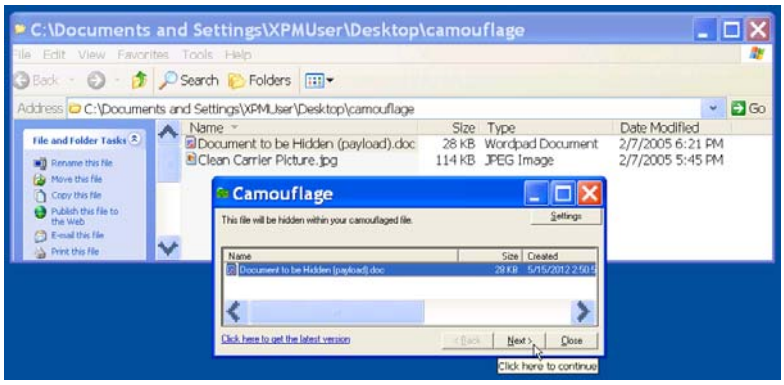


12

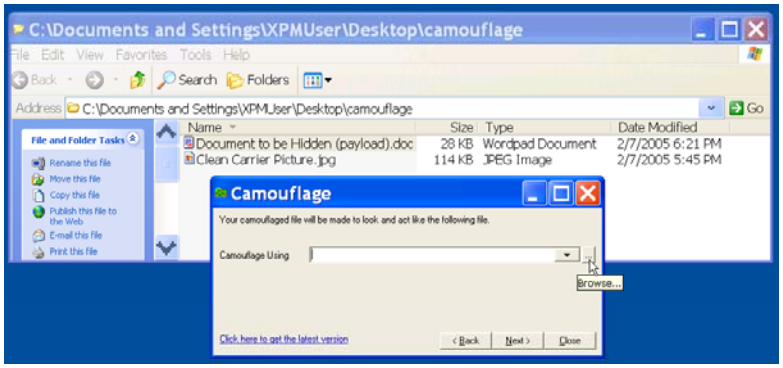
Insertion-Based Program: Camouflage



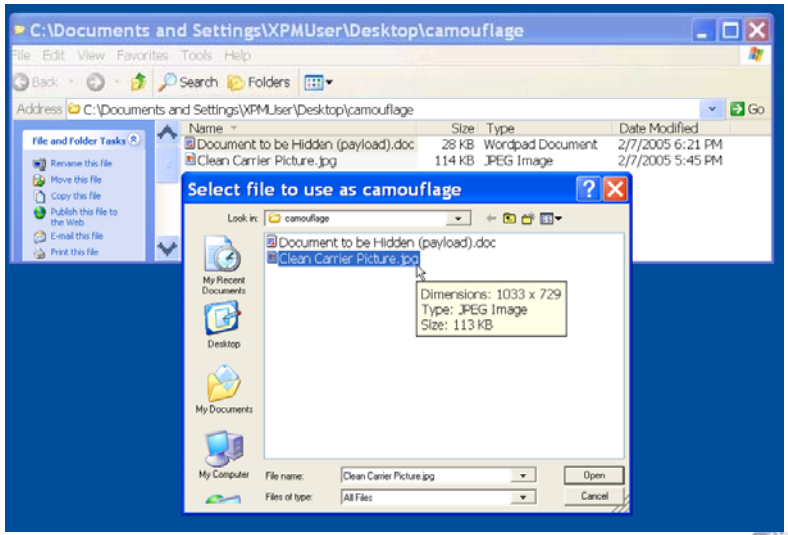
Insertion-Based Program: Camouflage



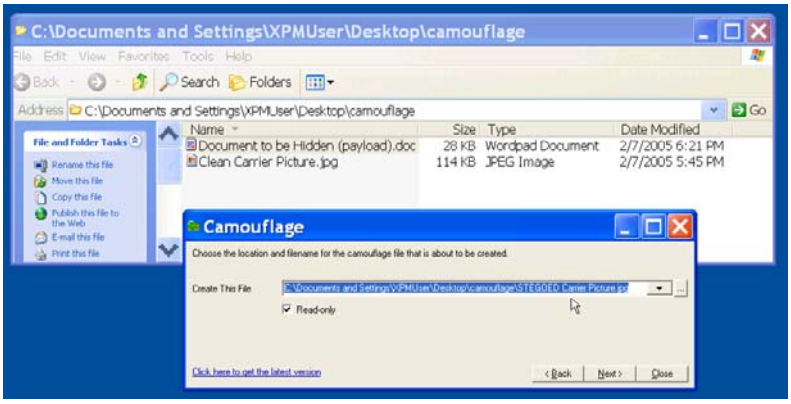
Insertion-Based Program: Camouflage



Insertion-Based Program: Camouflage

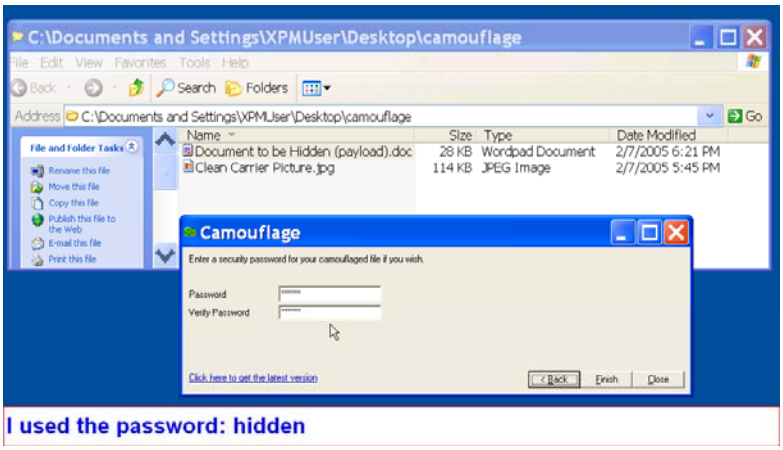


Insertion-Based Program: Camouflage



17

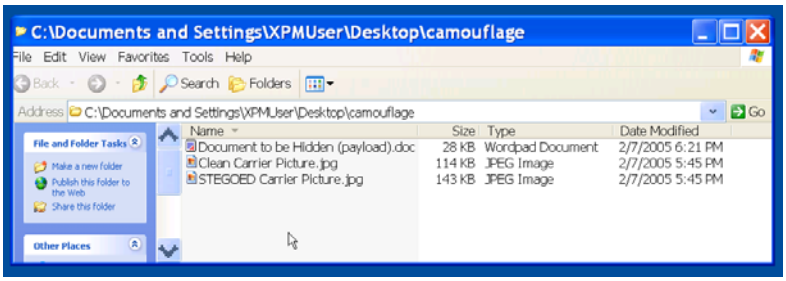
Insertion-Based Program: Camouflage



I used the password: hidden

18

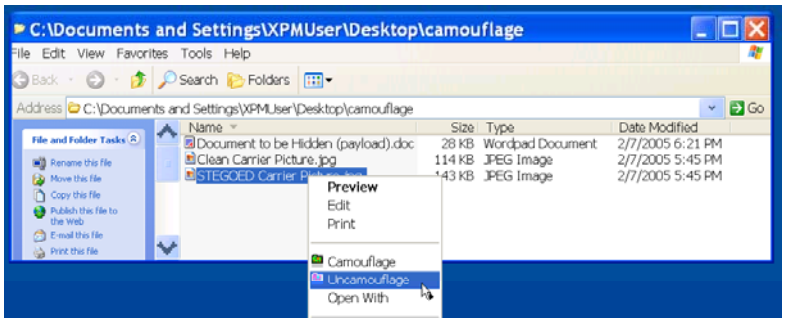
Insertion-Based Program: Camouflage



Insertion-Based Program: Camouflage

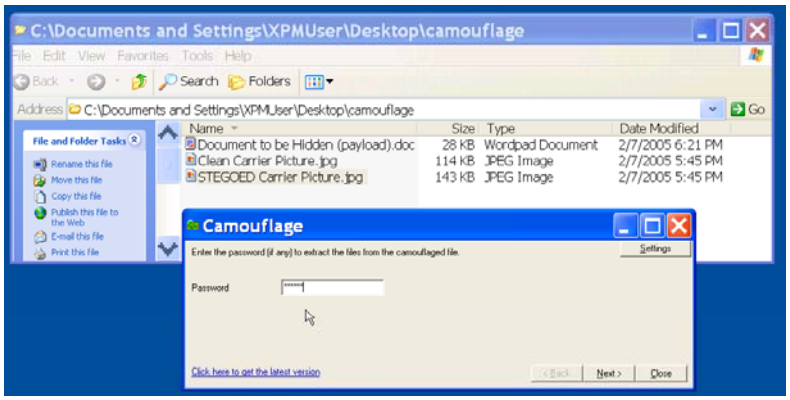
- **Can you spot which of these two files contains our camouflaged file?**

Insertion-Based Program: Camouflage



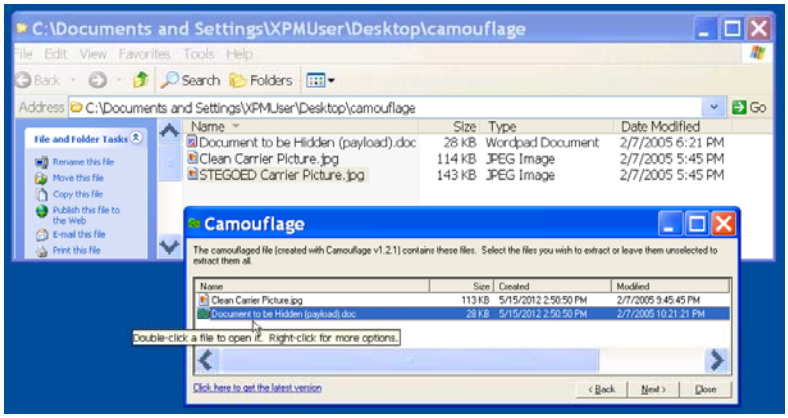
21

Insertion-Based Program: Camouflage

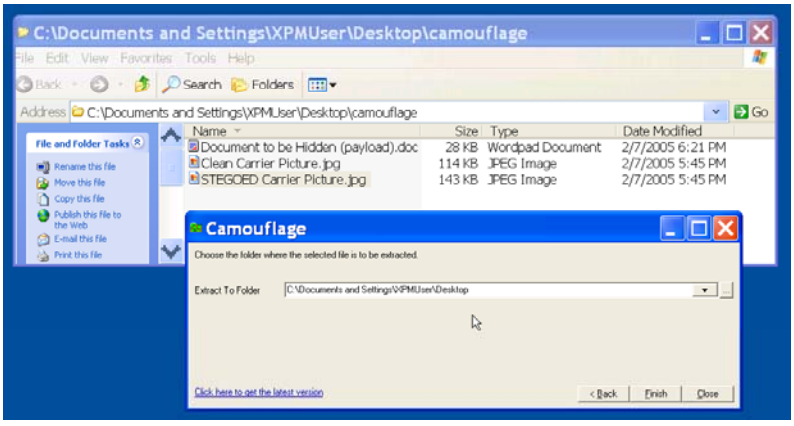


22

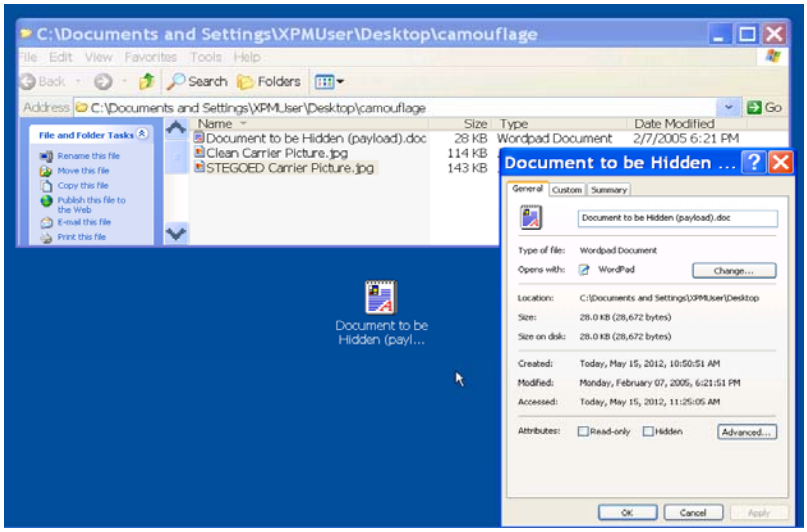
Insertion-Based Program: Camouflage



Insertion-Based Program: Camouflage



Insertion-Based Program: Camouflage

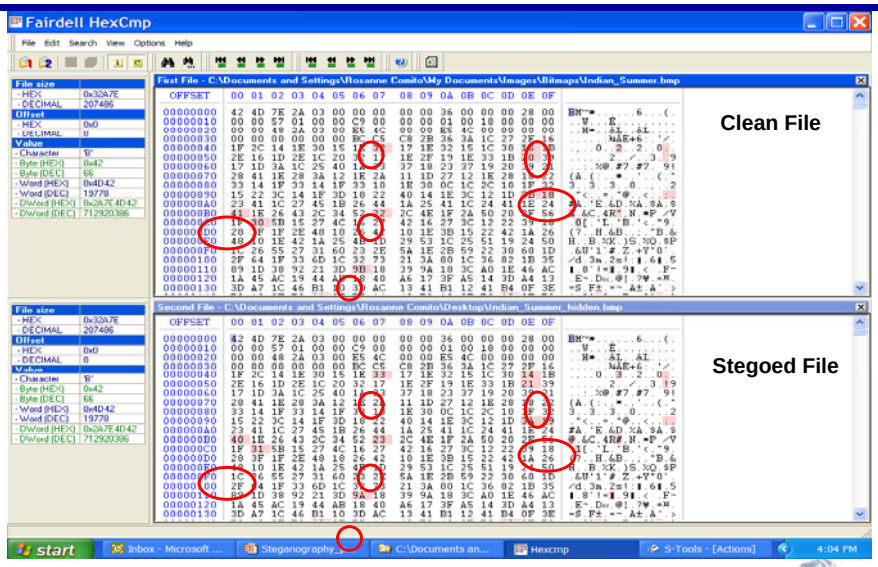


Substitution-Based Stego

A hiding technique that substitutes bits of the carrier file with the bits of the payload file without having creating visual anomalies

- **Typically, stego changes the "least significant bits" (LSB)**
  - **Usually shifting it during encoding to enter the data**
- **Carrier file degradation is not detectable to the naked eye**
- **Most programs randomly select which LSBs to substitute**
- **The "map" to decode the LSB changes is encrypted and hidden inside the carrier file**

Substitution-Based Hiding Area "Least Significant Bit"



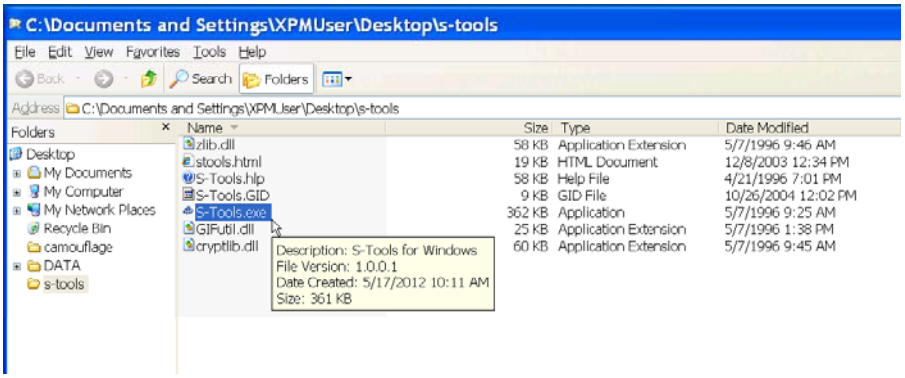
27

Substitution-Based Program: S-tools

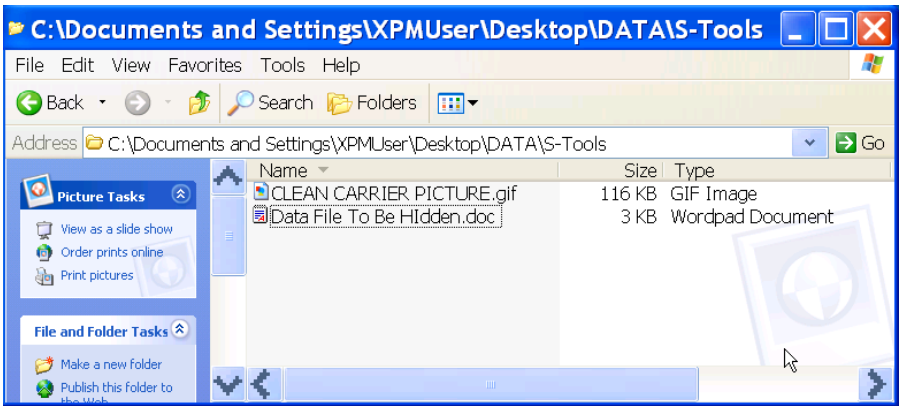
S-Tools Demo

28

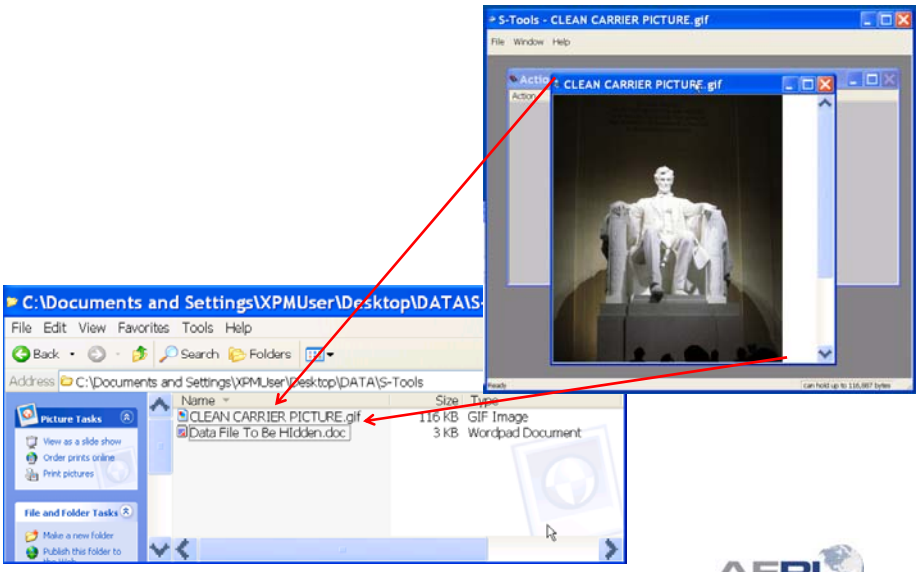
Substitution-Based Program: S-tools



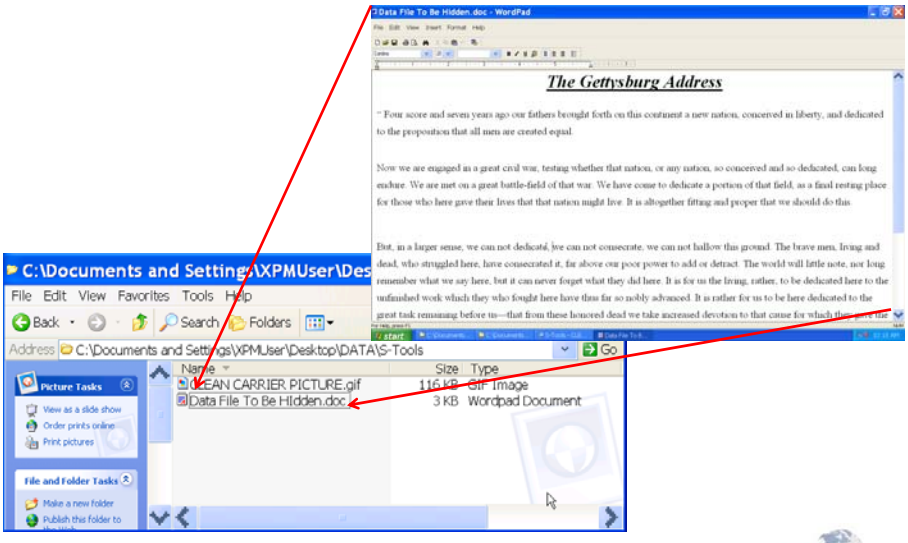
Substitution-Based Program: S-tools



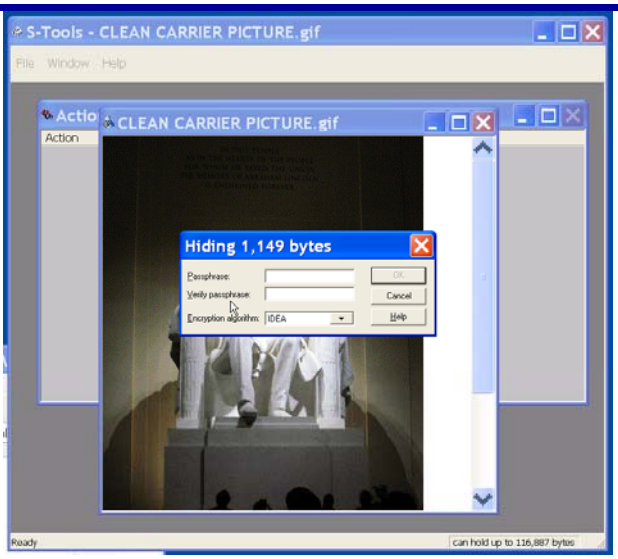
Substitution-Based Program: S-tools



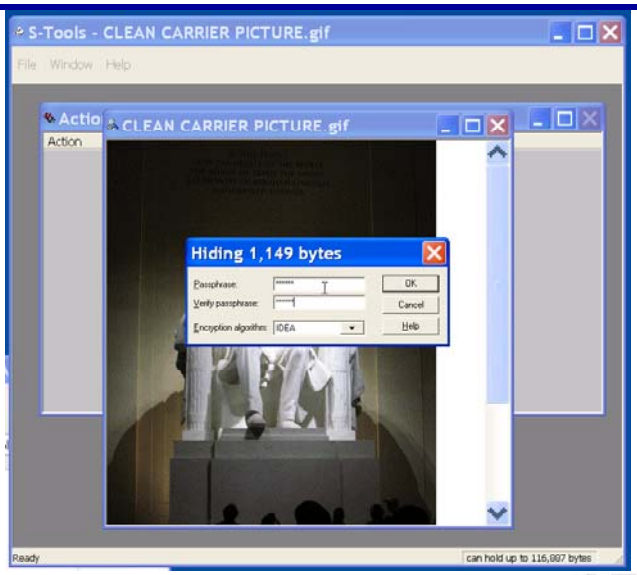
Substitution-Based Program: S-tools



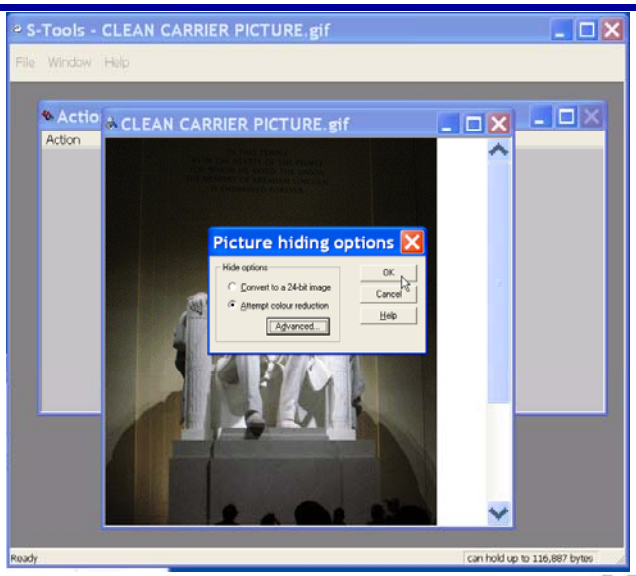
Substitution-Based Program: S-tools



Substitution-Based Program: S-tools

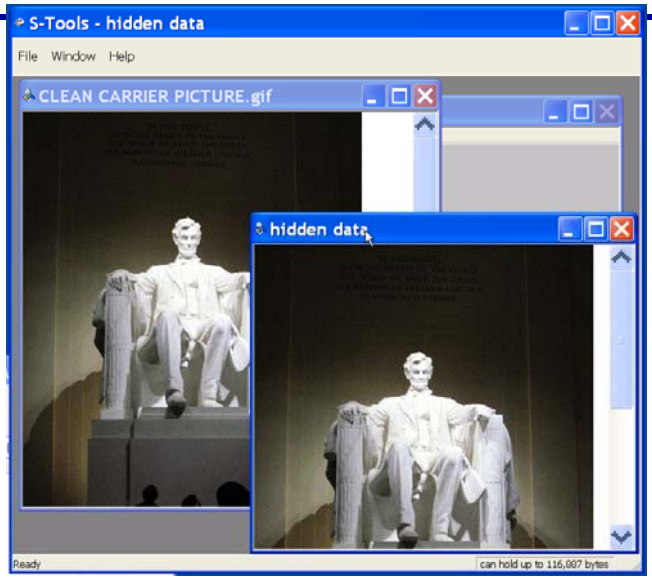


Substitution-Based Program: S-tools



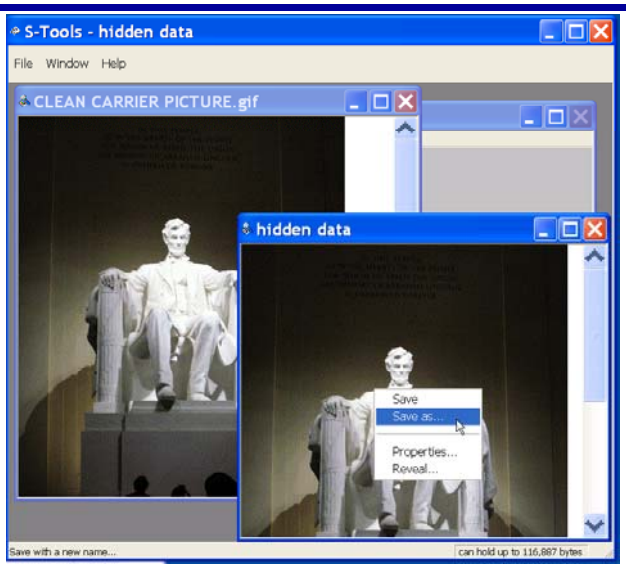
35

Substitution-Based Program: S-tools



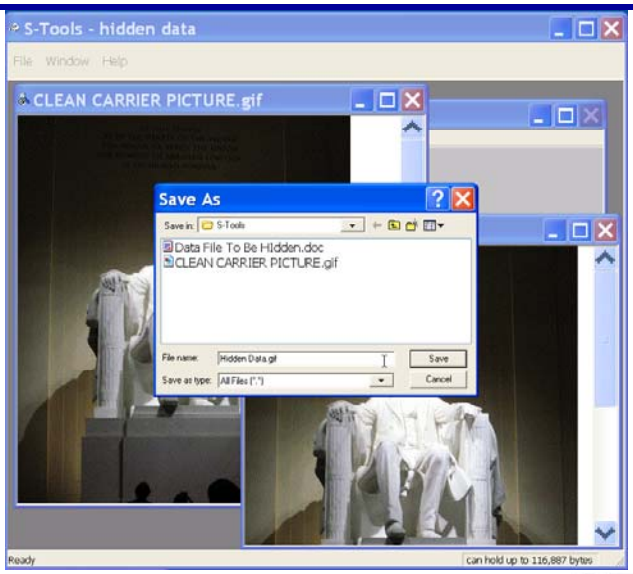
36

Substitution-Based Program: S-tools



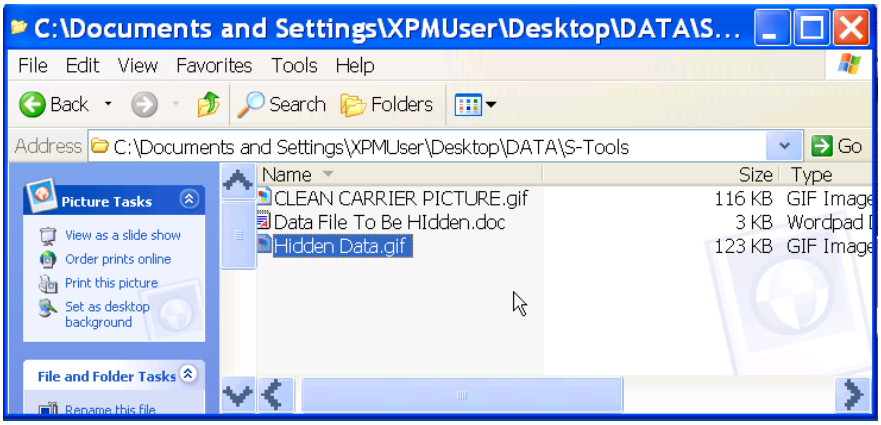
37

Substitution-Based Program: S-tools

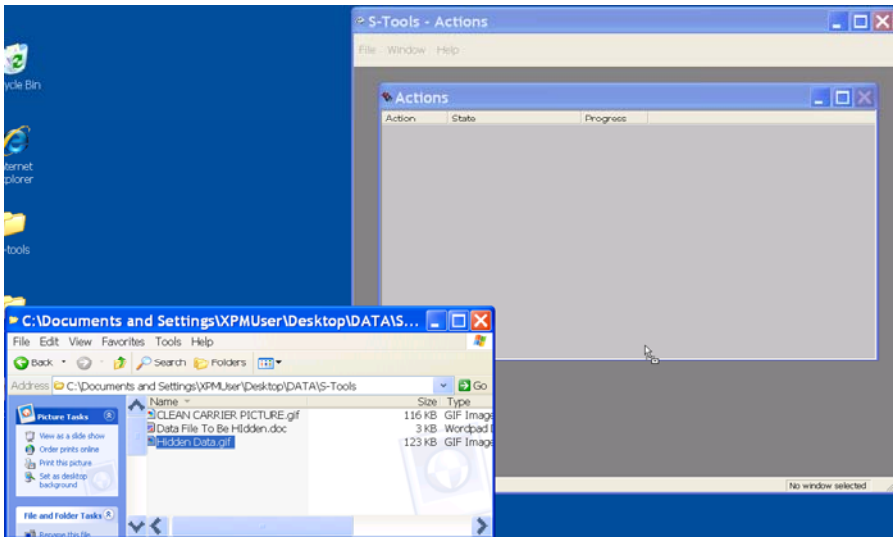


38

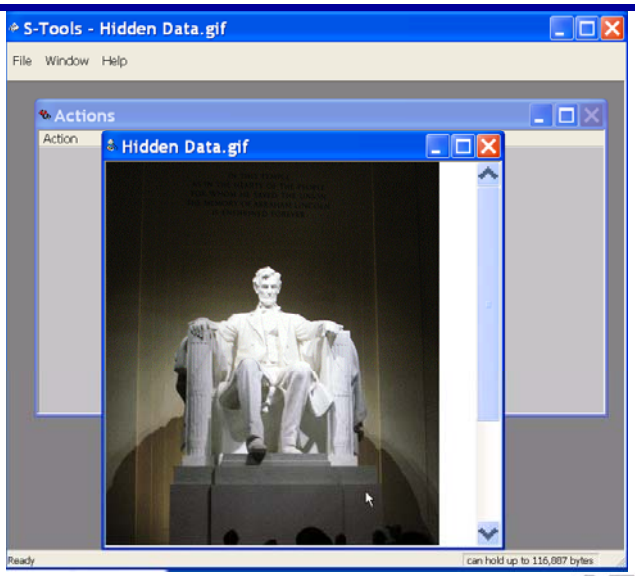
Substitution-Based Program: S-tools



Substitution-Based Program: S-tools

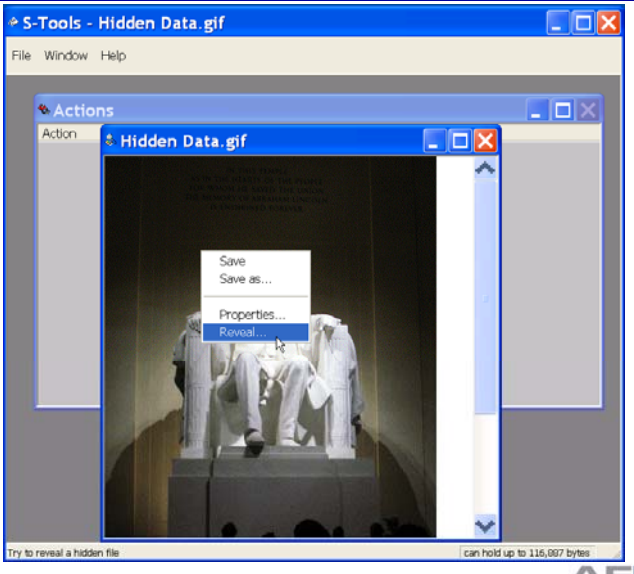


Substitution-Based Program: S-tools



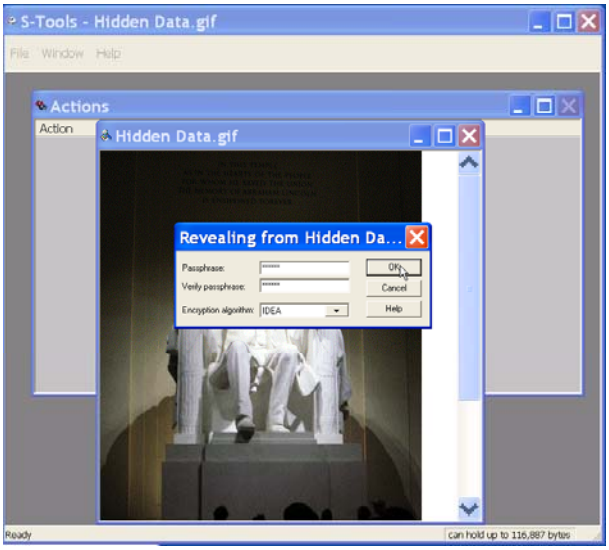
41

Substitution-Based Program: S-tools

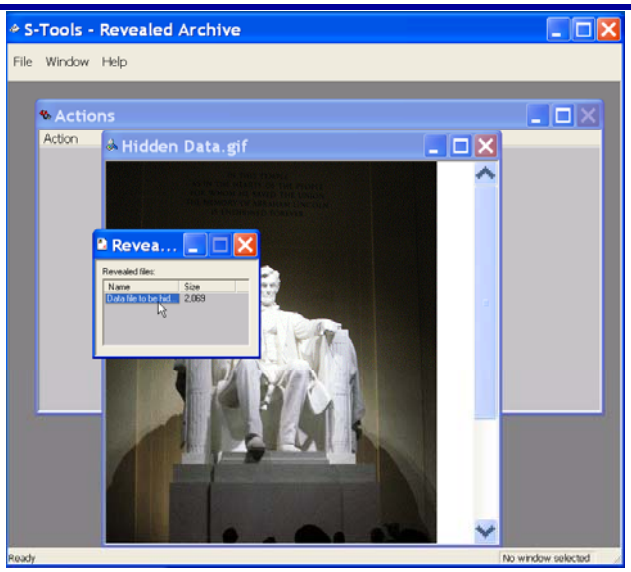


42

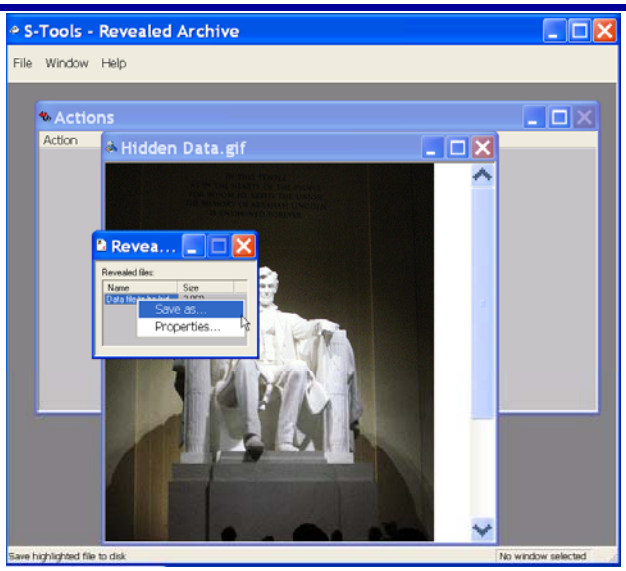
Substitution-Based Program: S-tools



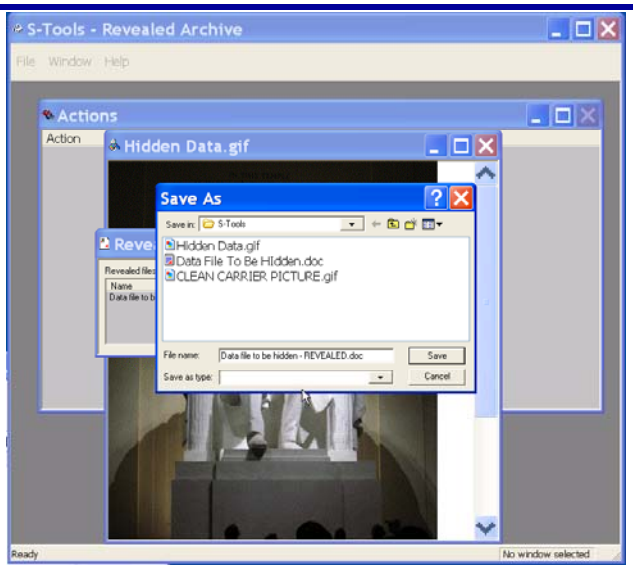
Substitution-Based Program: S-tools



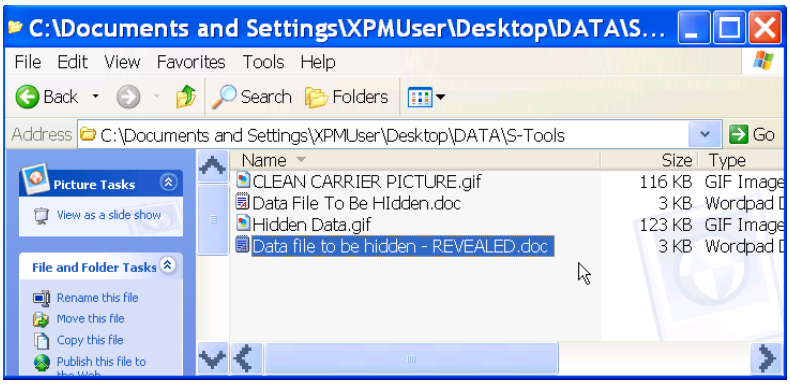
Substitution-Based Program: S-tools



Substitution-Based Program: S-tools



Substitution-Based Program: S-tools



47

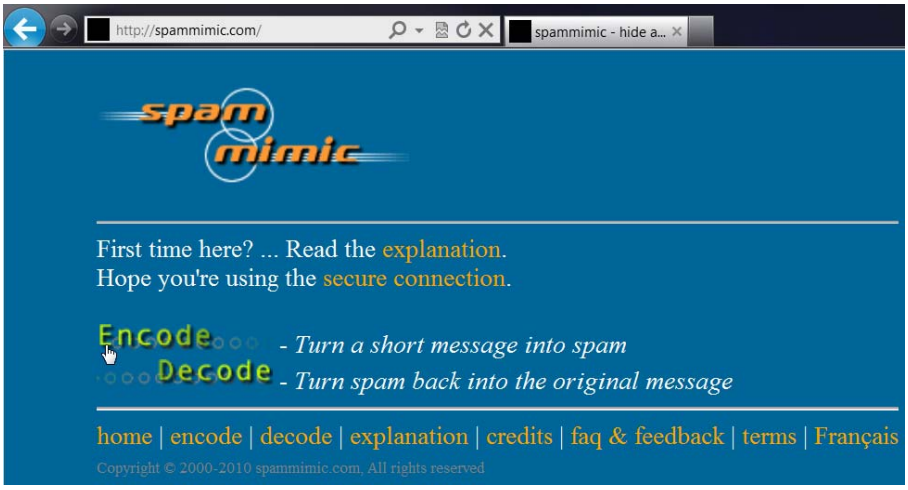
Generation-Based Stego

- **A hiding technique that generates a new carrier file for the intended hidden/payload file**
  - **Most carrier files that are generated are text files and geometric image files**
  - **No original carrier file exists for comparison**
  - **Creates a brand new file of data that does not LOOK like the original message**

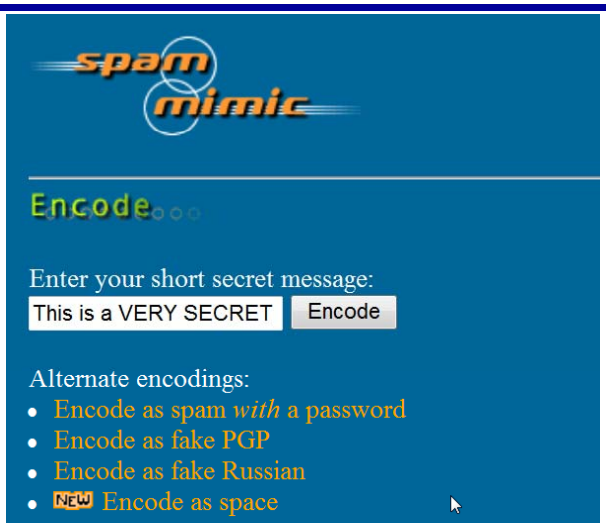
48

Generation-Based Program: Spam Mimic

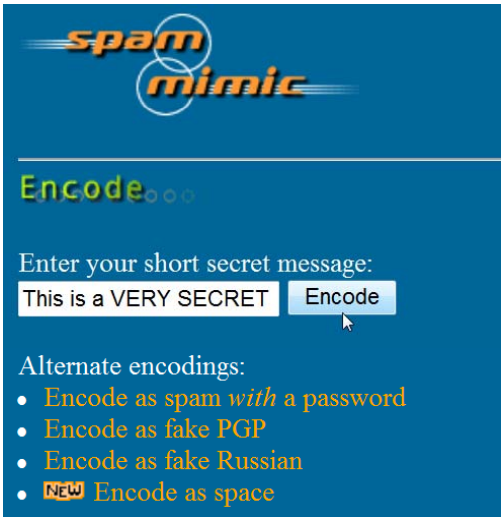
Generation-Based Program: Spam Mimic



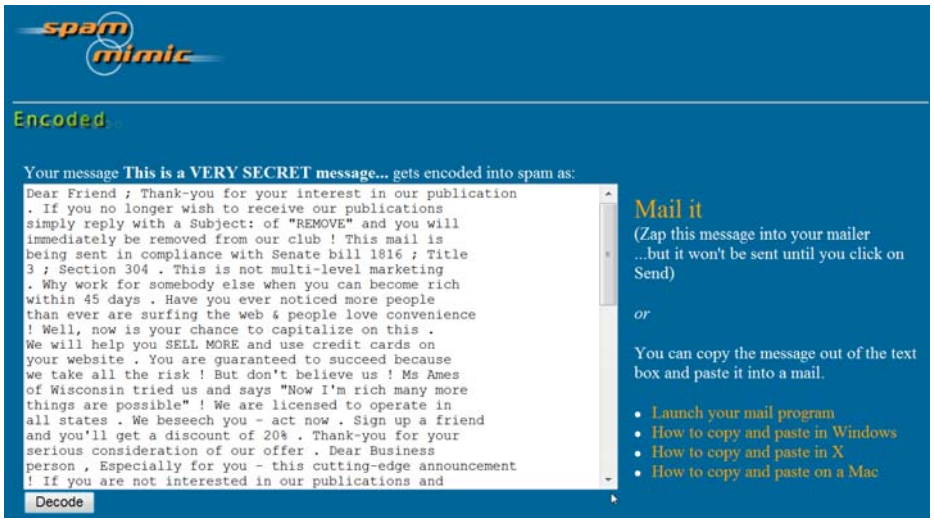
Generation-Based Program: Spam Mimic



Generation-Based Program: Spam Mimic



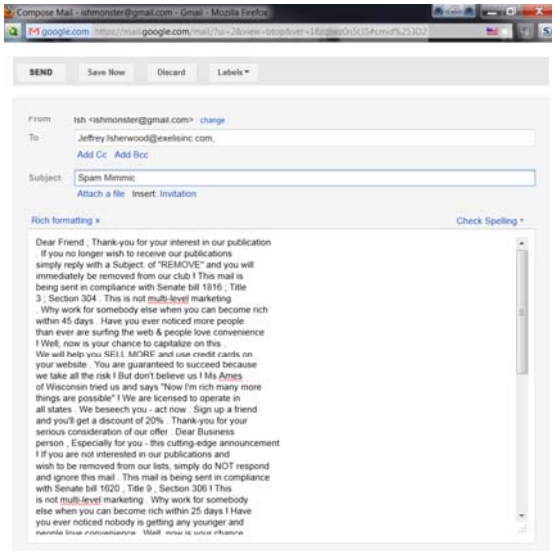
Generation-Based Program: Spam Mimic



AFRL

53

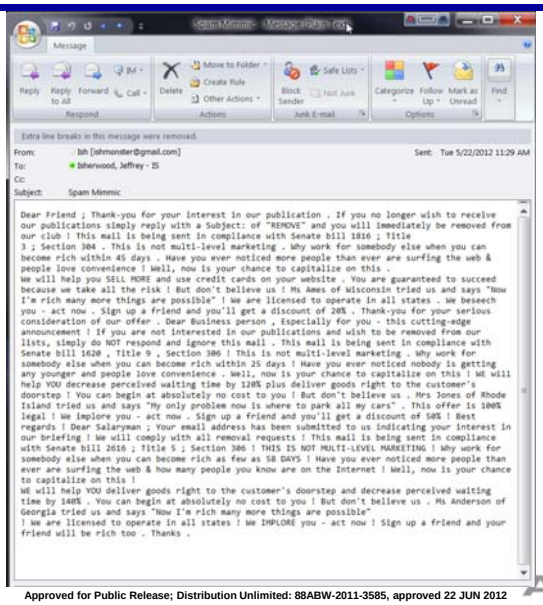
Generation-Based Program: Spam Mimic



AFRL

54

Generation-Based Program: Spam Mimic



Dear Friend ; Thank-you for your interest in our publication . If you no longer wish to receive our publications simply reply with a Subject: of "REMOVE" and you will immediately be removed from our club ! This mail is being sent in compliance with Senate bill 1816 ; Title 3 ; Section 304 . This is not multi-level marketing . Why work for somebody else when you can become rich within 45 days . Have you ever noticed more people than ever are surfing the web & people love convenience ! Well, now is your chance to capitalize on this .
We will help you SELL MORE and use credit cards on your website . You are guaranteed to succeed because we take all the risk ! But don't believe us ! Ms Ames of Wisconsin tried us and says "Now I'm rich many more things are possible" ! We are licensed to operate in all states . We beseech you - act now . Sign up a friend and you'll get a discount of 20% . Thank-you for your serious consideration of our offer . Dear Business person , Especially for you - this cutting-edge announcement ! If you are not interested in our publications and wish to be removed from our lists, simply do NOT respond and ignore this mail . This mail is being sent in compliance with Senate bill 1620 , Title 9 , Section 306 ! This is not multi-level marketing . Why work for somebody else when you can become rich within 25 days ! Have you ever noticed nobody is getting any younger and people love convenience . Well, now is your chance to capitalize on this ! WE will help YOU decrease perceived waiting time by 120% plus deliver goods right to the customer's doorstep ! You can begin at absolutely no cost to you ! But don't believe us . Mrs Jones of Rhode Island tried us and says "My only problem now is where to park all my cars" . This offer is 100% legal ! We implore you - act now . Sign up a friend and you'll get a discount of 50% ! Best regards ! Dear Salaryman ; Your email address has been submitted to us indicating your interest in our briefing ! We will comply with all removal requests ! This mail is being sent in compliance with Senate bill 2616 ; Title 5 ; Section 306 ! THIS IS NOT MULTI-LEVEL MARKETING ! Why work for somebody else when you can become rich as few as 58 DAYS ! Have you ever noticed more people than ever are surfing the web & how many people you know are on the Internet ! Well, now is your chance to capitalize on this !
WE will help YOU deliver goods right to the customer's doorstep and decrease perceived waiting time by 140% . You can begin at absolutely no cost to you ! But don't believe us . Ms Anderson of Georgia tried us and says "Now I'm rich many more things are possible"
! We are licensed to operate in all states ! We IMPLORE you - act now ! Sign up a friend and your friend will be rich too . Thanks .

55

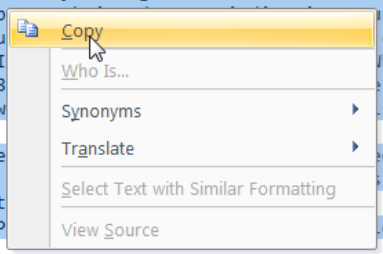
Generation-Based Program: Spam Mimic

Dear Friend ; Thank-you for your interest in our publication . If you no longer wish to receive our publications simply reply with a Subject: of "REMOVE" and you will immediately be removed from our club ! This mail is being sent in compliance with Senate bill 1816 ; Title 3 ; Section 304 . This is not multi-level marketing . Why work for somebody else when you can become rich within 45 days . Have you ever noticed more people than ever are surfing the web & people love convenience ! Well, now is your chance to capitalize on this .
We will help you SELL MORE and use credit cards on your website . You are guaranteed to succeed because we take all the risk ! But don't believe us ! Ms Ames of Wisconsin tried us and says "Now I'm rich many more things are possible" ! We are licensed to operate in all states . We beseech you - act now . Sign up a friend and you'll get a discount of 20% . Thank-you for your serious consideration of our offer . Dear Business person , Especially for you - this cutting-edge announcement ! If you are not interested in our publications and wish to be removed from our lists, simply do NOT respond and ignore this mail . This mail is being sent in compliance with Senate bill 1620 , Title 9 , Section 306 ! This is not multi-level marketing . Why work for somebody else when you can become rich within 25 days ! Have you ever noticed nobody is getting any younger and people love convenience . Well, now is your chance to capitalize on this ! WE will help YOU decrease perceived waiting time by 120% plus deliver goods right to the customer's doorstep ! You can begin at absolutely no cost to you ! But don't believe us . Mrs Jones of Rhode Island tried us and says "My only problem now is where to park all my cars" . This offer is 100% legal ! We implore you - act now . Sign up a friend and you'll get a discount of 50% ! Best regards ! Dear Salaryman ; Your email address has been submitted to us indicating your interest in our briefing ! We will comply with all removal requests ! This mail is being sent in compliance with Senate bill 2616 ; Title 5 ; Section 306 ! THIS IS NOT MULTI-LEVEL MARKETING ! Why work for somebody else when you can become rich as few as 58 DAYS ! Have you ever noticed more people than ever are surfing the web & how many people you know are on the Internet ! Well, now is your chance to capitalize on this !
WE will help YOU deliver goods right to the customer's doorstep and decrease perceived waiting time by 140% . You can begin at absolutely no cost to you ! But don't believe us . Ms Anderson of Georgia tried us and says "Now I'm rich many more things are possible"
! We are licensed to operate in all states ! We IMPLORE you - act now ! Sign up a friend and your friend will be rich too . Thanks .

56

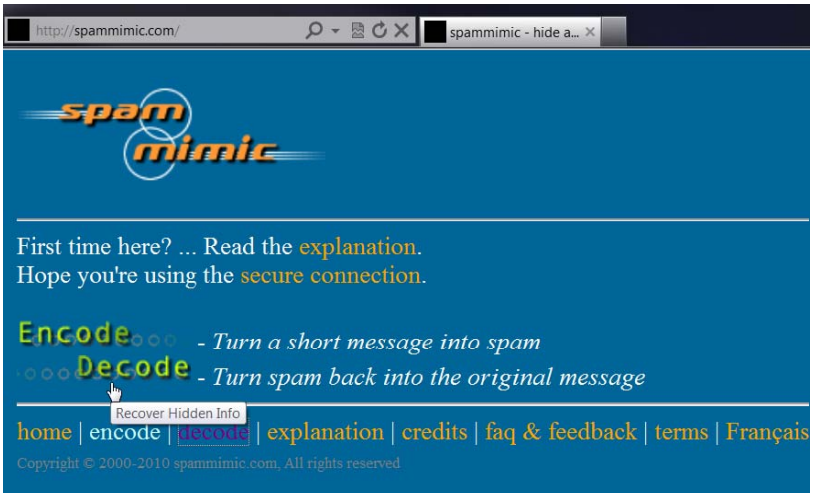
Generation-Based Program: Spam Mimic

ple love convenience . Well, now is your chance to capitalize on this ! WE will
erceived waiting time by 120% plus deliver goods right to the customer's
begin at absolutely no cost to you ! But don't believe us . Mrs Jones of Rhode
says "My only problem now is where to park all my cars" . This offer is 100%
you - act now . Sign up a friend and you'll get a discount of 50% ! Best
ryman ; Your email address has b ur interest in
ill comply with all removal requ compliance
16 ; Title 5 ; Section 306 ! THI Why work for
you can become rich as few as 58 people than
e web & how many people you know s your chance
is !
liver goods right to the custome d waiting
can begin at absolutely no cost Anderson of
d says "Now I'm rich many more t
o operate in all states ! We IMP end and your
too . Thanks .



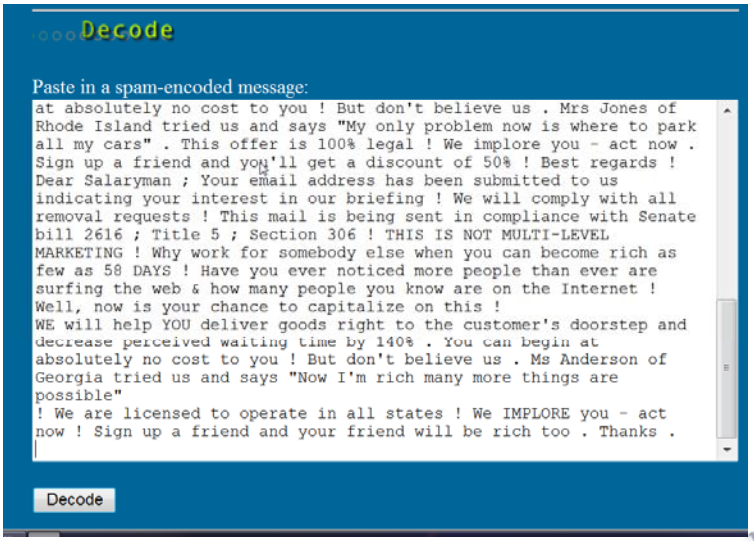
57

Generation-Based Program: Spam Mimic

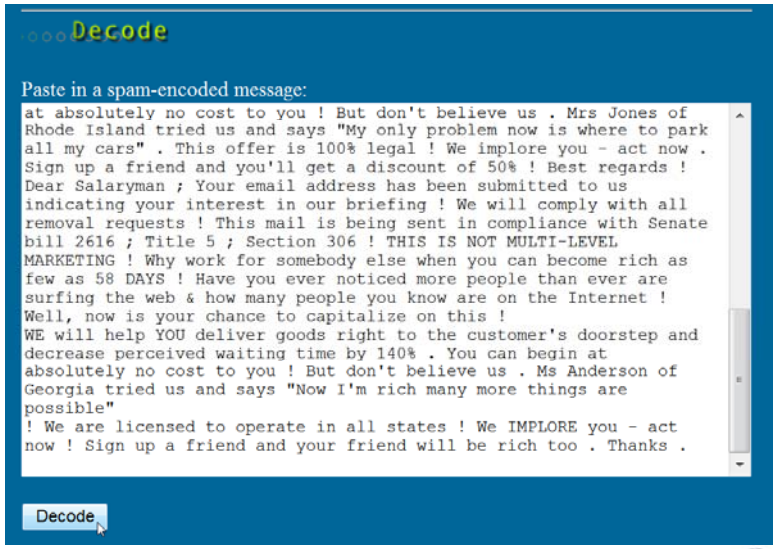


58

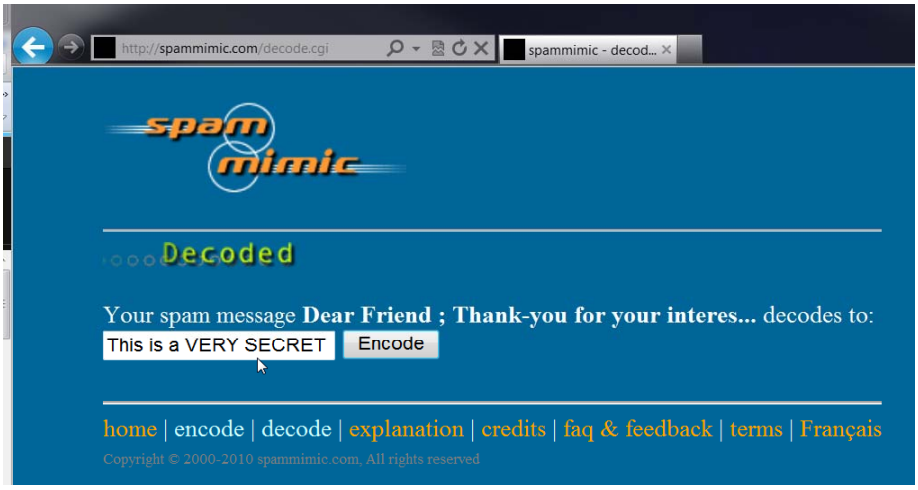
Generation-Based Program: Spam Mimic



Generation-Based Program: Spam Mimic



Generation-Based Program: Spam Mimic



61

Indications That Steganography MAY Have Been Used

- **The presence of Steganography Software**
  - *–There is a list of over 100 tools at http://www.jjtc.com/Steganography/tools.html*
- **Multiple copies of identical files including:**
  - ***Images, executables, text files***
  - ***Audio, video, and others.***
  - **Examine similar files for "differences**
    - **using a hex editor to compare two files for differences or anomalies**
- **Spam Mimic: Text that contain exaggerated formatting**
- **Files that fail to open in their intended program**
- **Files with size not proportionate to actual content**
- **Files that don't fit the suspect's profile**

62

BREAK

Be back in 15 minutes

Metadata and Hidden Objects

- **MetaData is "data about data"**
  - **Revisions**
  - **Changes**
  - **Creation, modification times**
  - **Links**
  - **Embedded resources**
  - **Location**

Metadata vs. Hidden Objects

- **Metadata**
  - Information about the author, computer, organization, or network
  - Embedded in the file by the software itself
  - Author is often unaware of this data
  - Information divulged to those who view the file
  - Provides a means of enumeration for potential hackers, competitors, etc.
- **Hidden Objects**
  - Data that can be hidden or obscured by the user
  - Provides a covert channel of communication for those engaged in malicious activities

Common Forms of Metadata

- Author's name and e-mail address
- Name of organization and e-mail addresses of employees
- Last 10 authors of a file
- Original title and location
- First line of text when document was created
- MAC times, editing times, number of revisions
  - Modified, Accessed, Created times (MAC)
- Location (GPS coordinates)

Metadata Reveals All

Common Forms of Hidden Objects

- Hidden text
- Text matching background
- Text/files/images shrunk down to be virtually invisible
- Images with altered properties
- Document alterations not seen in “normal” view
- Hidden cells, rows, columns or sheets
- Multi-layered text, pictures, links or files

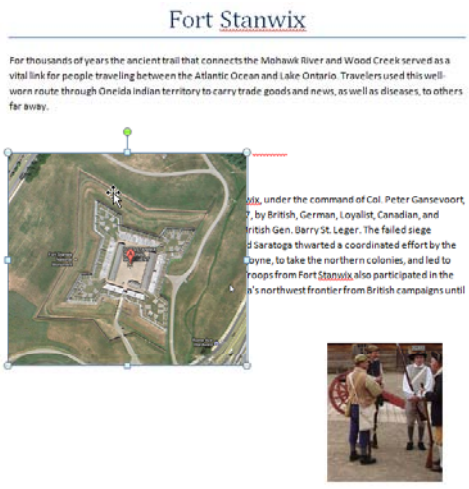
MS Word Document- Data Hidden

There are 4 different forms of hidden data here…

Can you see them?

AFRL

MS Word Document – Data Revealed



Both Text and a picture were hidden behind the image of Fort Stanwix

AFRL

MS Word Document – Data Revealed

Fort Stanwix

For thousands of years the ancient trail that connects the Mohawk River and Wood Creek served as a vital link for people traveling between the Atlantic Ocean and Lake Ontario. Travelers used this well-worn route through Oneida Indian territory to carry trade goods and news, as well as diseases, to others far away. When Europeans arrived they called this trail the Oneida Carrying Place and inaugurated a significant period in American history--a period when nations fought for control of not only the Oneida Carrying Place, but the Mohawk Valley, the homelands of the Six Nations Confederacy, and the rich resources of North America as well. In this struggle Fort Stanwix would play a vital role.

Some text was hidden by turning it WHITE, the same color as the background of the document!

MS Word Document – Data Revealed

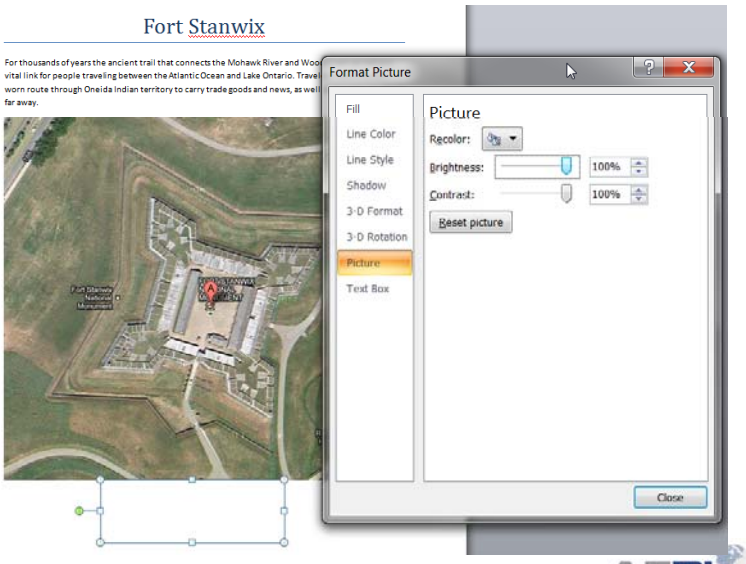
wix

F Mohawk RIver and Wood Creek served as a
v nd Lake Ontario. Travelers used this well-
w goods and news, as well as diseases, to others
fa Oneida Carrying Place and inaugurated a
si ons fought for control of not only the Oneida
C the Six Nations Confederacy, and the rich
re anwix would play a vital role.

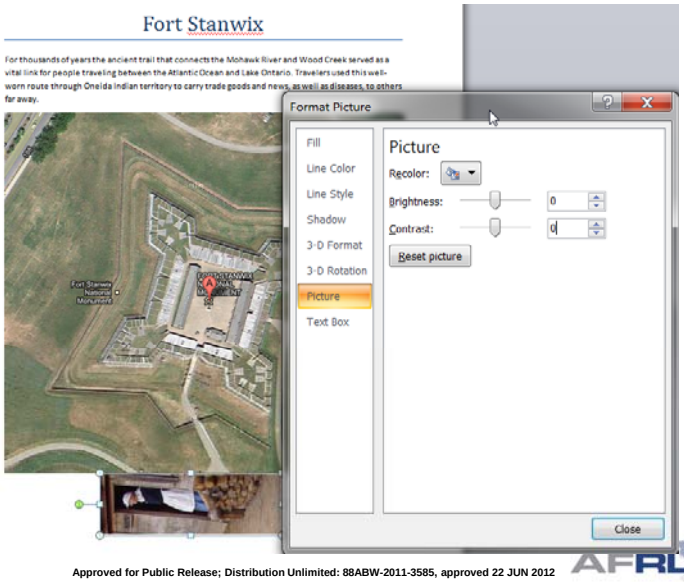
An Image was
Shrunk Down
To Appear as a period

Known as "the fort that never surrendered," Fort Stanwix, under the command of Col. Pete
successfully repelled a prolonged siege, in August 1777, by British, German, Loyalist, Canadian, and American Indian troops and warriors commanded by British Gen. Barry St. Leger. The failed siege combined with the battles at Oriskany, Bennington, and Saratoga thwarted a coordinated effort by the British in 1777, under the leadership of Gen. John Burgoyne, to take the northern colonies, and led to American alliances with France and the Netherlands. Troops from Fort Stanwix also participated in the 1779 Clinton-Sullivan Campaign and protected America's northwest frontier from British campaigns until finally being abandoned in 1781.

Hiding Via Image Modification



Hiding Via Image Modification



Data Hiding LAB

1. **Use Notepad to create a document**
   - Hide the document inside a .jpg using Camouflage
   - Hide the document inside a .gif using S-Tools
   - Trade the images to another team mate for decoding

2. **Use Spam Mimic to create a hidden message**
   - Transfer it to another member of your team for decoding

U.S. AIR FORCE

Cyber Forensics

Tony Martino

Director, Computer Forensics
Research and Development Center
(CFRDC)

Integrity □ Service □ Excellence

AFRL

U.S. AIR FORCE

Objectives

- Define digital evidence
- Identify types of digital evidence
- Describe best practices for evidence collection
- Define cyber forensics
- Provide an overview of basic forensic techniques
- Conduct forensic examinations on sample evidence sets
- Document the results of forensic analysis

AFRL

U.S. AIR FORCE

What is Digital Evidence

AFRL

U.S. AIR FORCE

What is Digital Evidence

Digital Evidence -

Information stored or transmitted in binary form that may be introduced and relied on in court.

U.S. Department of Justice, National Institute of Justice, Electronic Crime Scene Investigation: A Guide for First Responders 52 (2d ed. Apr. 2008)

AFRL

U.S. AIR FORCE

Digital Evidence ID

Digital evidence comes in many flavors

AFRL

5

U.S. AIR FORCE

Digital Evidence ID

- Modern digital evidence is more than just computers
  - Cellular Phones
  - Tablets
  - IPods
  - Game Consoles
  - E Readers
  - Removable Storage media
  - Cloud storage
- Digital media is evolving rapidly
  - Shrinking form factors
  - Increased capacity
  - Connectivity

AFRL

6

Digital Evidence Collection

Basic Rules:

Evidence Collection MUST:

- Be trustworthy
- Be accurate
- Preserve integrity
- Prevent contamination / corruption
- Be documented

Digital Evidence Collection

Digital evidence is fragile & easily altered

- File deletion
- Contamination
- Windows pervasive writes
- Overwriting freespace

Digital Evidence Collection

Digital evidence collection steps

- Do no harm
  - Make no changes
  - If its off, leave it off
  - Do not operate live devices
- Document everything
- Do not perform forensics on live devices*

*Emergency circumstances may be an exception

Digital Evidence Collection

Forensic Images

- A compressed file that contains all of the storage device contents.
- Can not be read or altered by standard apps
- Can be verified as authentic & unchanged
- Eliminates possible damage to the original storage device

U.S. AIR FORCE

Digital Evidence Collection

Write Blocking

- Hardware & Software
- Prevents ALL writes to the device
- Ensures integrity while devices are imaged

AFRL

11

U.S. AIR FORCE

Digital Evidence Collection

Drive Imaging Exercise

Approved for Public Release; Distribution Unlimited: 88ABW-2012-3463, 18-Jun-2012

AFRL

12

U.S. AIR FORCE

Data Storage

In order to analyze data you must 1st understand how it is stored

- MFT / FAT
- Storage area
- Allocated vs. Unallocated space

AFRL

U.S. AIR FORCE

Data Storage

- Are deleted files really deleted?
- What happens when a file is deleted?

AFRL

U.S. AIR FORCE

Data Storage

Deleted File Exercise

1. Locate and examine the FAT entry for a file
2. Delete the file.
3. Return to the FAT entry for the file.
   - What has changed
   - What hasn't changed
4. Correct the FAT entry for the file.
5. Observe results.

AFRL

15

U.S. AIR FORCE

Forensic Analysis

Identification, collection, preservation, examination, analysis and presentation of computer digital evidence in a manner that is legally acceptable.

What Does This Mean?

AFRL

16

U.S. AIR FORCE

Forensic Analysis

Capabilities

- Recovery of deleted information
- Analysis of user activity
- Timeline creation of data changes
- User attribution for activity on shared systems
- Preservation of data for future analysis or litigation.

AFRL

U.S. AIR FORCE

Browser Forensics

What does your web browser know about your online activity?

- History
- Cookies
- Form data
- Bookmarks
- Cache

AFRL

Browser Forensics

- Almost all browsers log and cache by default
- How much / how long is configurable
- The data that is kept is not always easily readable

Browser Forensics

Browser Forensics Exercise

Cellular Forensics

- Cellular phone power and capacity has grown rapidly
- Still a wide variety of operating systems
- Volatile storage

Cellular Forensics

Many standard forensic techniques do not apply.

- Live analysis
- No write blocking
- Proprietary data formats

U.S. AIR FORCE

Cellular Forensics

A wide variety of evidence is stored on phones

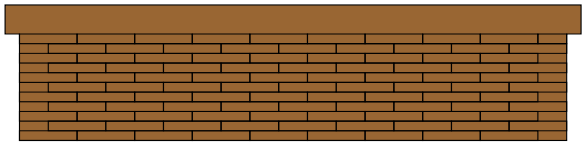
- Call logs
- Contacts
- Pictures / Videos
- Text Messages
- Emails
- Browser history
- Geo location data

AFRL

U.S. AIR FORCE

Cellular Forensics

Cellular Blocking Demonstration



AFRL

U.S. AIR FORCE

Cellular Forensics

Cellular Forensics Exercise

AFRL

25

U.S. AIR FORCE

Forensics Documentation

- Properly and accurately documenting steps in a forensic exam is critical
- Written documentation is often the only thing seen by litigants
- Your forensic report must be easy to read, understandable, and grammatically correct.

AFRL

26

Forensics Documentation

- Write in language that can be understood by non - forensic people
- Define technical terms and acronyms
- Create a template that can be utilized for every examination

Forensics Documentation

Sample Outline

Introduction

Notes and Definitions

Case Tasks

Tools Utilized

Analysis Steps

Results Obtained

Conclusion

Examiner Curricula Vitae

U.S. AIR FORCE

Forensics Documentation

Forensic Report Demonstration

AFRL

U.S. AIR FORCE

Questions

AFRL

Integrity ★ Service ★ Excellence

STEM CAREERS

Helen M. Rico
STEM Coordinator
Griffiss Institute

AFRL

STEM CAREERS

- What do you want to be when you grow up?
- Google that job
  - Duties/Responsibilities
  - Education required
  - Starting Salary
  - Jobs location
  - Security clearance
- What is a STEM career?

AFRL

STEM Preparation

- Science Fairs
- Join a math, science, engineering, or computer club at school
  - DimensionU (Grades 3-9)
  - Mathcounts
  - Robotics
  - Cyber Patriot – (Grades 9-12)
- Math and Science Courses – take as many as you can
- Extra help and or tutoring – ask your teacher
- Summer courses, Summer camps
- Professional Associations provide assistance over the internet
- Trips to science museums – Rochester Museum & Science Center, New York Hall of Science, Blue Mountain Lake

CAPSTONE PROJECT

What is a CAPSTONE PROJECT?

- **A capstone project is a project that demonstrates your competence in a subject**
- **Intended to be an intense, active learning event**
- **It requires significant effort**
  - **A demonstration of the knowledge, skills and abilities that you have acquired**
- **It will allow you to show off what you learned this week**

The Challenge: "The Company"

- You will be divided into 5 teams
- Each team has a similar goal
  - Different companies and suspects
  - "The Company" has been robbed of Intellectual Property (IP)
  - Someone inside of "The Company" stole the IP
  - Find the Mole!
- Each team will have a mentor
  - Mentors will clarify information, won't assist in the investigation
- Once the mole is discovered…
  - Find the evidence
  - Make a report (power point)
  - Appoint a spokesman for your team to present the report

AFRL

Teams & Packets

- Assign teams
- Appoint leaders
- Designate spokesman
- Pick up packets
- Begin Investigation

GOOD LUCK!

AFRL

A

Analog: Continuous and without breaks. A steady uninterrupted flow. Analog is like water flowing in a stream. The opposite of analog is digital. Digital is non-continuous. Digital is like the rain that falls individually as separate drops.

ANSI (American National Standards Institute): A voluntary organization responsible for establishing computer industry standards.

ASCII (American Standard Code for Information Interchange): A code that uses the numbers 1 through 127 to represent characters. This code enables the computer to transfer alphabetic, numeric, and symbolic characters to another computer. For example: With the ASCII code, the capitol letter "A" is represented by the number 65. The small letter "a" is represented by the number 97.

AVI (Audio Video Interleave): The format for Microsoft's Video for Windows files. These files end with the ".avi" extension.

B

BASIC (Beginner's All-purpose Symbolic Instruction Code): An easier to learn programming language. It is ideal for the beginning programmer.

Baud: The number of bits transmitted per second. This unit of measure is pretty accurate for lower data transfer rates. As the rates get faster, (over 1,200 bits per second), the accuracy drops. At higher baud rates, the transfer speed may be two bits per second, or even more. For this reason, transfer rates at higher speeds are normally given in bits per second (bps).

Binary: A system of numbers using only the two digits 1 and 0. A computer only understands binary information, known as machine language. Even though programs are written in C++, Assembly, Java, Basic, and etc., these programs eventually have to be translated into binary, (or machine language), so the computer can understand them. The binary numbering system, which is represented by 0, (for an "off" bit), and 1, (for an "on" bit), is not so hard to understand.

BIOS (Basic Input/Output System): BIOS is the computer's "built-in" operating system. It is always available even without battery power. When you first boot, (or turn on), your computer the BIOS is in charge. Once everything is functioning properly the BIOS turns the computer over to Windows or the primary operating system on your computer. When first starting your computer, (or booting), you are given the option of entering the BIOS setup. BIOS setup is where you can configure the components installed on your computer. This area is for advanced users only! The BIOS setup can cause your computer to go haywire if done wrong!

Bit: A single on/off binary position. If the position is set to 1 the bit is "on." If the position is off the bit would be set to 0. 8 bits make a byte. (Now that makes me hungry!)

BMP (Bit Mapped): Graphic files ending with the ".bmp" extension. They are called "bit-mapped" because they are made up of a bunch of little on/off square bits, grouped together on a graphical map, composed of rows and columns. These bits are so tiny that we do not notice that they are squares. If you keep zooming in on the image eventually the squares will become visible.

Botnet: A network of compromised devices that perform unauthorized activities as directed by a commanding entity.

Browser: A program used to browse files. A Web browser browses Internet files. Both Netscape Navigator and Internet Explorer are Web browsers.

Bus: The connections between the computer's components. PCI busses are paths, (or connections), that connect the PCI slots to the Processor. Busses can be wires, paths, or any other type of electrical circuit used to connect one component to another.

Byte: A group of 8 binary on/off bits. Bytes often have an extra bit known as a "parity bit" that is used for error checking. This type of byte actually has 9 bits instead of 8, but normally a byte is only thought of in terms of 8 bits.

C

Cache: Memory that is readily available to the CPU. Level 1 Cache is located in the CPU itself. Level 2 Cache is located outside the CPU, but can still be accessed much faster than the RAM memory. The CPU stores commonly accessed data in its cache memory. This causes the processing cycle to be much quicker and more efficient.

CAD (Computer-Aided Design): CAD software is sophisticated graphical software used to design 3 dimensional objects. It is commonly used by drafting engineers and architects.

CD-ROM (Compact Disk Read Only Memory): A compact disk player that reads compact disks. CD-ROM disks can hold approximately 700MBs of data.

CD-R (Compact Disk Recordable): A compact disk player that can read compact disks and also record information to them. Although a CD-R drive can record information, it cannot erase it. A special CD-R disk is needed in order to record information.

CD-RW (Compact Disk ReWritable): A compact disk player that can read, record, erase, and rerecord information to and from compact disks. In order to use the rewrite feature one must use a special CD-RW disk.

CMOS (Complementary Metal-Oxide Semiconductor): CMOS is the memory used to store computer settings, time and date information, BIOS information, and any other information that must not be erased when the computer is turned off. CMOS memory usually relies on a small battery to provide continuous power while the computer is off.

CODEC (COder/DECoder): CODEC technology is included in software and hardware for coding and decoding data. MPEG is a common CODEC used for video data.

COM (COMmunication port): Refers to the serial communications ports. A computer normally has only two physical serial ports, but each has 2 serial communication ports: COM1, COM2, COM3, and COM4. Usually COM1 and COM3 relate to one serial port and COM2 and COM4 the other. In order to use two devices on the same serial port they both must be set to different COM's. COM's on the same serial port can never be used at the same time or an error will most likely occur.

Compiler: A program that converts higher level languages, (non-binary), into lower level machine language, (binary). A computer can only understand machine language. Humans can understand both, but due to the complexity and difficulties of machine language, (all 1's and 0's), humans better understand the higher level languages like C++, Java, Basic, etc. The higher the language level, the easier it is to understand.

CPU (Central Processing Unit): Often referred to as the brain of a computer. The central processing unit, or CPU, with its level 1 cache memory, contains the control unit and the arithmetic/logic unit, both working together as a team to process the computer's commands. The control unit controls the flow of events inside the processor. It fetches instructions from memory and decodes them into commands that the computer can understand.

CRT (Cathode-Ray Tube): More commonly known as a "Picture Tube," the CRT is what most televisions and monitors use for their display screens.

D

Data: Simply another name for information. While data is correctly known as bits of electronic information stored for computer use, it can also be information written on paper, information stored in our heads, or any other type of information.

Database: A collection of data. A filing system capable of accepting data. Normally referred to as a well organized and easily accessible computer filing system containing a collection of information. A database can also be a file cabinet or any other item that stores data.

DDOS (Distributed Denial of Service): An attack in which a multitude of compromised systems attack a single target, thereby causing denial of service (DOS) for users of the targeted system.

DHTML (Dynamic Hypertext Markup Language): A variation of HTML that allows much better movement, manipulation, and interactivity with WebPages. A user is able to interact with DHTML WebPages without having to go through the Web server. With DHTML better WebPages video games and other things are possible than with regular HTML.

Digital: Non-continuous. Computers are digital. They process information bits at a time. Computers can convert analog information into digital information for processing then back into analog again. A sound card can take your voice, (analog), convert it into digital, (for processing), then convert it back into analog again, playing it through the speakers. A digital clock is a good example of how digital information is handled. The numbers on the clock go from one to the next, stopping for a split second in-between. Clocks with hands move continuously in a slow and steady circular motion, (analog). They never stop moving unless the power goes out.

DIMM (Dual In-Line Memory Module): A memory expansion card that has several memory chips. There are contact points on both sides of this type of module. The contact points are not connected.

DLL (Dynamic Link Library): DLL files are used by programs to access commonly needed functions used with Windows. Programmers use them to eliminate having to write extra code. These files are often shared between many different programs. The winsock.dll file is one example. Programmers can use the winsock.dll functions to eliminate having to write a tremendous amount of extra code to connect to different types of modems, configure the connection, specify protocols that will be used, and many other things.

DMA (Direct Memory Access): DMA refers to accessing the computer's main memory from a device, (like a hard drive), without having to go through the central processing unit.

DNS (Domain Name System): The naming system used on the Internet to identify WebSites.

DOS (Denial of Service): An attack which attempts to make a machine or network resource unavailable to its intended users.

DOS (Disk Operating System): An older 16 bit operating system. DOS is still available on most computers, but people rarely use it today. Computer technicians often use it to access a computer that is having problems starting normally. With time, DOS will probably become obsolete.

DPI (Dots Per Inch): A standard for measuring the quality of an image's resolution. The more dots per inch that an image has the better the picture quality. Commonly used when talking about monitors or printers.

DRAM (Dynamic Random Access Memory): This memory module type is the most commonly used. DRAM holds data only for a short period of time before having to refresh itself.

Dumb Terminal: A keyboard and monitor hooked to a remote computer. The dumb terminal can send and receive information, but it lacks the ability to alter the primary computer's information. It cannot process data or store data by itself. It can only enter, transmit, receive, and display data.

DVD (Digital Video (or Versatile) Disk): DVD disks are capable of storing from 4.7GB to 17GB of data. Eventually DVD drives will replace CD-ROM drives that store much less information.

E

EIDE (Enhanced Integrated Drive Electronics): An interface used by different types of disk drives. This interface is around 4 times faster than the older IDE interface. EIDE supports hard drives up to 8.4GB. It can transfer data up to 16.6MBs per second. Also known as ATA-2 and a later revision ATA-3.

E-mail (Electronic Mail): The electronic transmission of messages over communication networks like the Internet.

EPROM (Erasable Programmable Read Only Memory): EPROM stores its information until it is erased with an ultraviolet light. Once Erased, EPROM must be reprogrammed using a special PROM burner.

F

FAT (File Allocation Table): The table used by the computer to find files on the hard drive and/or disks. FAT keeps track of all the disks files. It is located at the beginning of a disk just after the boot sector.

FAQ (Frequently Asked Questions): A document often found on the Internet that is used to answer frequently asked questions.

Fiber Optics: A technology that will soon replace telephone wires. Fiber optic cables have fishing line type threads, (or fibers), that carry data in the form of light beams. This data travels at the speed of light. It not only is much faster than wired transmission, it is also capable of digital transmission and can carry much more data.

FIFO (First In, First Out): FIFO usually refers to a method of storing information. Drink cans are stacked on top of each other inside of a drink machine. When the drinks are first loaded the first drink placed in the machine goes to the bottom of the dispenser. The first drink purchased will be the first that was put into the machine.

FTP (File Transfer Protocol): An Internet protocol for sending and receiving files via the Internet.

G

GB (Gigabyte): A gigabyte is 1 billion bytes. To be precise, a gigabyte is actually 1,073,741,824 bytes, (or 2 raised to the 30th power).

GHz (Gigahertz): A gigahertz is one billion cycles per second.

GIF (Graphical Interchange Format): A compressed bit-mapped graphics file that is compatible for use over the Internet. GIF files are recognized by the ".gif" extension. Normally, image files with less than 256 colors are best used on the Internet as GIF's. If the image has over 256 colors the JPG format is usually best.

GUI (Graphical User Interface): Graphics that aid the user in using computer programs or applications making things much simpler. Before GUI's commands had to be typed in. Now a person can simply double click an icon to do the same thing. Pointers, menus, pop-up dialogs, icons, and etc., are all part of the GUI. The Windows operating system is a good example of a GUI.

H

Hardware: The physical components of a computer. Computer items that you can see and touch. Disks, keyboards, monitors, chips, computers, wires, and etc., are all hardware items.

HDTV (High Definition Television): HDTV uses digital signals for video output. A standard television uses analog signals. HDTV has much better resolution than regular television. Computer monitors operate with digital signals, but not all monitors are HDTV. HDTV screens are normally thin and flat.

HTML (Hypertext Markup Language): The standard language used for creating WebPages or other HTML files.

HTTP (Hypertext Transfer Protocol): The standard used to transfer WebPages on the Internet.

HTTPS (Hypertext Transfer Protocol Secured): The standard used to transfer Encrypted WebPages on the Internet.

I

Icon: A part of the graphical user interface, (or GUI), used to represent programs and other items. When clicked, the icon opens its corresponding application. Icons are images normally designed to resemble something that will remind you of what the program is or does.

IDE (Integrated Drive Electronics): An IDE interface is a drive interface controlled from the drive itself. The IDE interface supports data transfer rates of approximately 3.3MBs per second, and is limited to 538MBs per drive. Also known as ATA.

IDS (intrusion detection system): A device or software application that monitors network or system activities for malicious activities or policy violations and produces reports to a Management Station.

IEEE (Institute of Electrical and Electronic Engineers): The IEEE organization is responsible for determining the standards for much of the computer and electronic industry.

INI (Information Necessary for Initialization): INI files are text files containing information necessary for initializing a corresponding program or application.

I/O (Input/Output): I/O refers to the process of entering and extracting data to and from a computer. Scanners, keyboards, cameras, and mice are examples of items used for input. Monitors, printers, and speakers, are examples of output devices. Floppy disks, hard disk drives, CD-RW drives, and memory are capable of both inputting and outputting information.

IP Address (Internet Protocol Address): An IP Address is used to identify a specific computer using the Internet. An IP Address consists of 4 numeric parts. The first part denotes the geographic region where the computer is located. The second part identifies the company or organization the computer is linked to. The third part reveals the computer group network. The fourth and final part identifies the specific computer the user is connected to.

IPS (Intrusion Prevention System): Also known as intrusion detection and prevention systems (IDPS). It is a network security appliance that monitor network and/or system activities for malicious activity. The main functions of intrusion prevention systems are to identify malicious activity, log information about said activity, attempt to block/stop activity, and report activity.

IRQ (Interrupt ReQuest line): A computer contains many components that must communicate directly with the central processor. Components must request an interruption when they wish to send information to the processor. If several components try to send their information at the same time the processor will not be able to handle it. It often will cause the computer to make an error or crash. IRQ settings must be made so that no two devices send data at the same time.

ISA (Industry Standard Architecture): ISA slots connect ISA cards to the motherboard. ISA is an 8 or 16-bit interface that operates at speeds of up to 8.33MHz. EISA or Extended ISA is a later 32-bit interface. Although the faster 32 and 64-bit PCI technology has replaced the slower ISA interface, Some sound cards, modems, and other expansion cards can still be found using the older ISA technology.

ISDN (Integrated Services Digital Network): A communication standard that uses special digital telephone lines to transfer data at speeds of 64,000 bits per second per channel. Many ISDN users have 2 of these 64kbps channels and are capable of transferring data at 128kbps. This is much faster than a standard 56kbps telephone connection that often operates even slower than that due to the limitations of telephone services in different locations.

Interface: An interface is an item that connects two or more individual items. A User Interface connects the computer user to the computer. Keyboards, mice, icons, and menus, are examples of user interface items. A Device Interface connects a device to the computer.

J

JavaScript: A scripting language that is an extremely useful companion to HTML for WebPages. JavaScript code is very similar to C++ and Java. It is a great language for advanced WebPage designers to learn. With JavaScript one can write video games and many other things not possible with standard HTML. All you need to write JavaScript is the Windows Notepad application or any other text application.

JPEG (Joint Photographic Experts Group): A compressed image format with the ".jpg" or ".jpeg" extension, (most commonly ".jpg"). This format is especially useful for Internet image files because of its smaller size. An image is normally best saved as a JPEG type when it has over 256 colors. If an image has less than 256 colors and you are going to use in on the Internet it is normally better to save it as a GIF type.

K

KB (Kilobyte): A kilobyte is one thousand bytes. To be precise, a kilobyte is actually 1,024 bytes, (or 2 raised to the 10th power).

KHz (Kilohertz): A kilohertz is one thousand frequency cycles per second.

L

LAN (Local Area Network): A small network, (connection of computers), covering a specific area. A bank would most likely be set up on a LAN.

LCD (Liquid Crystal Display): Liquid Crystal Display screens output graphical data to a video screen that uses a liquid crystal solution to display the information. LCD screens are normally very thin and have a flat viewing surface. Notebook computers have LCD screens.

LIFO (Last In, First Out): LIFO usually refers to a method of storing information. Using the Stack method of storage, data is placed on top of a stack and removed from the top of the stack when needed. Using a stack of CD's as an example, when you're through listening to a CD you place it on top of the stack. When your ready to listen to a CD again you must first pick up the last CD you placed on the stack before listening to any other CD.

Logon: The process of entering a user name and/or password to gain access to a computer system.

M

MAN (Metropolitan Area Network): A computer network that usually spans a city or a large campus. A MAN usually interconnects a number of local area networks (LANs).

MB (Megabyte): A megabyte is 1 million bytes. To be precise, a megabyte is actually 1,048,576 bytes, (or 2 raised to the 20th power).

MHz (Megahertz): A megahertz is one million frequency cycles per second.

MIDI (Musical Instrument Digital Interface): A musical file with the ".mid" or ".midi" extension. MIDI's are musical files in digital form. The computer is able to process midi files quickly, since they do not have to be converted from analog form. MIDI files are much smaller in size than most any other musical files. This makes them an excellent choice for Internet use.

Motherboard (Also called: Mainboard): The main circuit board that connects all of the computer's components together. Everything connected to the computer, whether inside or out, communicates either directly or indirectly with the motherboard. The CPU can be found at the heart of every motherboard.

MPEG (Motion Picture Experts Group): A leading group responsible for the standards used with compressed full motion audio/video files. MPEG files are recognized by the: ".enc", ".m1v", ".mp2", ".mp3", ".mpa", ".mpe", ".mpeg", ".mpg", ".mpv2", and other extensions. The MPEG movie file format is a very good quality file format that is close to VCR quality. The MP3 music file format is another high quality file format that is close to CD quality.

mV (MilliVolt): A millivolt is one thousandth, (or .001), of a volt.

mW (MilliWatt): A milliwatt is one thousandth, (or .001), of a watt.

N

Network: A network is simply two or more computers linked together.

NIC (Network Interface Card): Allows computers to communicate over computer networks.

ns (Nanosecond): A nanosecond is one billionth of a second. In more simple terms, "It's pretty darn fast!" It is commonly used to specify the amount of time it takes to access data.

NVRAM (Non-Volatile Random Access Memory): NVRAM is memory that is preserved by battery power while the computer is off. NVRAM usually contains information like setup settings and other user settings that need to be remembered each time the computer is booted.

O

OCR (Optical Character Recognition): OCR programs allow text from items like pictures or magazine pages to be converted into editable text that is useable in text based applications like MS Word or Notepad.

OEM (Original Equipment Manufacturer): An OEM computer product is usually considerably cheaper than the boxed version of the same item. An OEM product is quite often packaged only in a plastic bag or plain box. Sometimes no manuals or installation instructions are included. The manufacturer may also not provide any product support. Sometimes the software necessary for installation must be downloaded from the Internet as well.

OLE (Object Linking and Embedding): OLE allows a user to create an object with one program and embed it into another, while the object retains its original format.

OS (Operating System): The software that manages your computer environment. Windows XP is an example of an operating system.

P

Parity Bit: A single bit that is added to a byte of memory in order to check for errors. A byte is composed of 8 bits. Counting the parity bit, a byte is actually composed of 9 bits. Sometimes there is more than one parity bit per byte.

PC (Personal Computer): A personal computer conforming to IBM PC standards. While the technical term refers only to IBM PC compatible computers, it commonly refers to almost any "personal" computer.

PCI (Peripheral Component Interconnect): PCI slots connect 32-bit and 64-bit PCI expansion cards to the motherboard. PCI cards send and receive data at speeds of 33Mhz for 32-bit cards and 66Mhz for 64-bit cards.

PCMCIA (Personal Computer Memory Card International Association): The PCMCIA is responsible for the development of the credit card size PC expansion cards. These cards are used to provide additional memory, network connections, additional drives, and other things for notebook computers. To install a PCMCIA card you simply plug it into a PCMCIA slot located on the computer, normally without even rebooting. To uninstall a PCMCIA card you just unplug it.

PIN: A small pin-like connection used on circuit boards, chips, or other hardware to make a connection to a jumper or socket.

Plug-In: A helper application for a program that expands the program's capabilities. Web browsers are a good examples of programs that use plug-ins. Macromedia's Shockwave plug-in allows Web browsers to display Shockwave files.

PnP (Plug and Play): PnP refers to a computer having the ability of automatically configuring device settings for a component without the user having to make any manual adjustments. A computer without a PnP operating system has to be configured manually with the BIOS setup program and/or by setting jumpers located on the device and/or motherboard. Most all versions of Windows are PnP. Most all of today's hardware is PnP also.

POST (Power On Self Test): A computer goes through POST each time it is booted before loading Windows or any other operating system. POST is a test run by the BIOS. It is the first thing a computer does when you turn it on. It checks the memory, connected devices, expansion cards, and other items. It then compares the results with previously stored information on the CMOS chip.

PPP (Point to Point Protocol): A protocol that provides a connection to the Internet. It is used to send and receive information.

PROM (Programmable Read Only Memory): PROM can only be programmed one time and can never be erased. PROM is programmed with a special PROM burner, (also known as a PROM programmer). Unlike ROM that comes preprogrammed, PROM is completely blank when manufactured.

Protocol: A format which is agreed upon and recognized as a method of data transmission between two or more computers.

Q

Query: The process of requesting information.

Queue: A storage area where tasks wait to be processed by the computer or other device. In simplest terms it is a waiting line. Items normally come out of the queue in the same order they went in, although certain items with a higher priority may get to cut line. (That's not fair!) .

R

RAM (Random Access Memory): Memory that the computer readily reads from and writes to. Once the computer is turned off the RAM is erased.

RGB (Red Green Blue): Red, green, and blue, are the three colors an RGB monitor uses to create full color images. Combining red and green makes yellow. Red and blue combine to make magenta, a purplish color. By varying the proportions and combinations of each color the color possibilities are virtually endless.

RPM (Revolutions Per Minute): The number of times an object rotates completely in a 60 second time period.

RPS (Revolutions Per Second): The number of times an object rotates completely in 1 second. Sometimes it is denoted as r/s.

RTC (Real Time Clock): The computer's RTC keeps track of time even while the computer is off. The clock is powered by a small battery located on the motherboard.

ROM (Read Only Memory): Computer memory that never changes. ROM memory contains data that is permanently recorded on the ROM chip. ROM is memory that is normally never erased or altered. It is for reading only. Unlike RAM, ROM retains its data even when the power is off or disconnected.

S

SCSI (Small Computer Systems Interface): The SCSI interface has many different variations. Some of the SCSI interfaces allow up to 15 devices to be connected to a single SCSI port. Ultra320 SCSI-3 can transmit data up to 320MB per second.

SDRAM (Synchronous Dynamic Random Access Memory): Using a clock, the SDRAM module synchronizes the data transfer rate to the CPU with the CPU's clock. SDRAM modules are about 25% faster than EDO modules, because they are able to send and receive data in sync.

Serial Device: A device like a keyboard or mouse that transmits data one bit at a time.

Server: A computer that serves other computers connected to it. When you go to a WebSite you are connecting to that site's Web server computer. The Web server computer is what delivers, (or serves), the WebPages.

SIMM (Single In-line Memory Module): A memory expansion card that has several memory chips. There are contact points on both sides of this type of module. The contact points are connected from one side to the other.

SMTP (Simple Mail Transfer Protocol): A standard used to send electronic mail between computers.

Software: The actual program itself. It does not refer to the disk. A disk is hardware, but the program contained on the disk is software. Software can't be seen.

Spam: Spam is a term referring to mass email forwarded messages, junk email, email hoaxes, and etc. Spam is especially bad, because it bogs down the Internet with unwanted junk email making it slower for us to download files or access WebPages.

Spyware: Software that collects information for unauthorized use.

SQL (Structured Query Language): An extremely popular database management language. SQL is used to request data from a database.

SRAM (Static Random Access Memory): SRAM does not need to be refreshed as often as DRAM. SRAM is accessible at speeds of about 10 nanoseconds, as opposed to a much slower rate of around 60 nanoseconds with DRAM.

SSID (Service Set ID): The public name of a wireless access point.

SSL (Secure Sockets Layer): Cryptographic protocols that provide communication security over the Internet.

SVGA (Super Video Graphics Array): SVGA monitors support 16 million colors and an 800 x 600 resolution.

T

TB (Terabyte): A terabyte is 1 trillion bytes. To be precise, it's actually 1,009,511,627,776 bytes, (or 2 raised to the 40th power).

TCP/IP (Transmission Control Protocol/Internet Protocol): A standard used for transmitting data over the Internet. TCP and IP are actually 2 different standards, but they are used together. TCP/IP is the most widely accepted standard for transmitting data between computers.

TIFF (Tagged Image File Format): An image file format that stores bit-mapped images. The format supports any resolution or color scheme. These files usually have the ".tif" extension. They are compatible with both PC and Macintosh computers.

TLS (Transport Layer Security): An upgrade to SSL that provides better communication security over the Internet.

Trojan Horse: Any program designed to do things that the user of the program did not intend to do or that disguises its harmful intent.

U

UNIX (UNiplexed Information and Computing Service): Originally called UNICS, UNIX is a smaller multitasking operating system with excellent networking capabilities that can be installed on almost any computer.

UPS (Uninterruptable Power Supply): A UPS prevents a computer from shutting off in the event of a power outage. The computer and other components are plugged into the UPS, which has a battery capable of providing power for several minutes. This gives the user time to shut the computer down properly and not loose any of his or her current work. Most UPS units come with software that will close programs and shut the computer down automatically.

URL (Uniform Resource Locator): The address of documents and resources on the Internet. Every item on the Internet has an address. A Web browser uses the URL to retrieve its intended target.

USB (Universal Serial Bus): USB is a 4 pin interface capable of connecting up to 127 devices that operate at transfer speeds up to 12Mbits per second. USB technology is significantly faster than a regular serial port. Devices can be plugged in and installed without shutting the computer down. USB is plug and play compliant. It is also one of the easiest ports for adding expansion devices.

V

VGA (Video Graphics Array): VGA monitors support 262,144 different colors and a resolution of 640 x 480.

VIRUS: A program that replicates itself and spreads throughout your computer or network. A virus usually remains hidden in another program or object and depends on a person to activate it. The virus normally will contain a routine that will destroy files, modify data, open up unwanted access to a computer, hog all your memory, or do anything that is possible with a computer program. Viruses only damage software and cannot destroy hard drives, monitors, or anything else like that as commonly rumored.

W

WAN (Wide-Area Network): A network of computers that span a large geographical area. The Internet is a wide area network.

WAV (WAVeform): The Waveform sound format is used for many audio files. These files are recognized by the ".wav" extension. Most of the standard Windows sound files are WAV files.

WLAN: A Wireless Local Area Network (LAN).

Worm: A computer program that can run independently, can propagate a complete working version of itself onto other hosts on a network, and may consume computer resources destructively.

WWW (World Wide Web): A group of Internet server computers linked to each other all around world. These computers serve documents and files that have links allowing you to jump from one location on the Web to another. Some Internet servers are not part of the World Wide Web.

X

XON/XOFF: A protocol used for controlling the flow of data between computers and other devices.

Y

Y Connector: A Y shaped cable which plugs into a single terminal. The terminal is then capable of connecting two devices instead of one.

Z

ZIP: A very popular method of compressing a file, making it much smaller in size and capable of being transferred from one computer to another more quickly. ZIP files are recognized by the ".zip" extension.