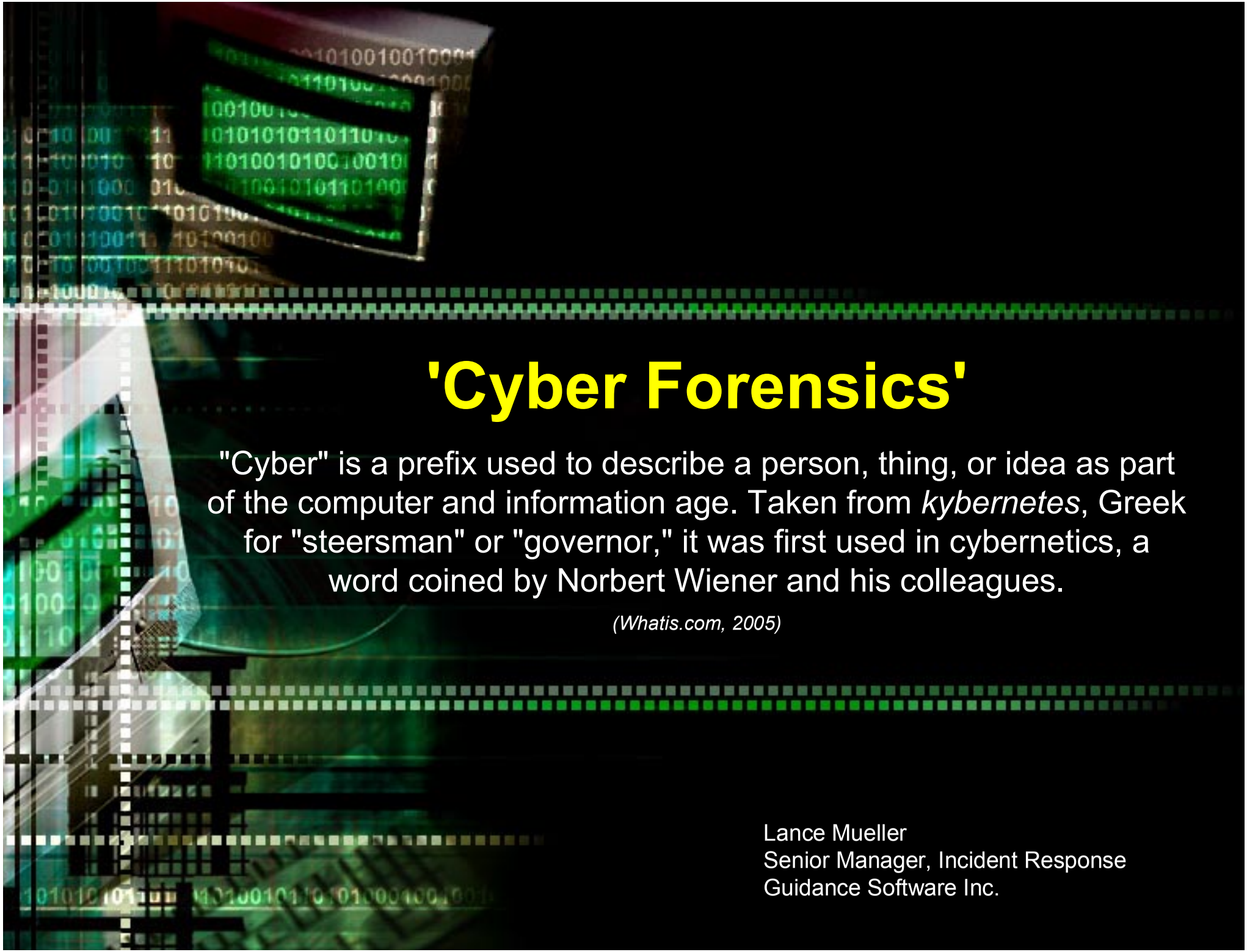


'Cyber Forensics'

"Cyber" is a prefix used to describe a person, thing, or idea as part of the computer and information age. Taken from *kybernetes*, Greek for "steersman" or "governor," it was first used in cybernetics, a word coined by Norbert Wiener and his colleagues.

(Whatis.com, 2005)

Lance Mueller
Senior Manager, Incident Response
Guidance Software Inc.

Cyber Forensics

- What is forensics?
  - **Forensic science** (often shortened to **forensics**) is the application of a broad spectrum of sciences to answer questions of interest to the legal system
    (Source:Wikipedia)
- What is Cyber forensics?
  - **Cyber forensics** can be defined as the process of extracting information and data from computer storage media and guaranteeing its accuracy and reliability
- How does it differ from traditional forensics?
  - Analysis is normally done on a copy of the original and introduction into the legal system is usually copy or a approved representation of the original

Cyber Forensics

- What is the difference between “computer forensics” and the collection of “digital evidence”?
  - “Digital Evidence is any information of probative value that is either stored or transmitted in a binary form,” (SWGDE, July 1998).
  - Digital evidence includes computer evidence, digital audio, digital video, cell phones, digital fax machines, etc.

Cyber Forensics

- When/Why is Cyber Forensics needed?
  - Most common is when dealing with criminal investigations
  - Civil matter
  - Human Resource/Personnel Matters
  - Incident Response
    - Malware/Viruses
    - Intellectual Property Theft
    - Any other event which may be detrimental

Cyber Forensics

Most common use of Computer forensics or digital evidence examinations is criminal investigations:

- What are common computer-related crimes?
  - **Hacking/Cracking**
  - **Intrusions**
  - **Identity Theft/Phishing**
  - **Spamming**
  - **Virus Deployment**
  - **Component Theft/Cargo Theft**
  - **Online Auction Fraud**
  - **Email Threats**

Cyber Forensics

- Some not so common Computer related Crimes:

CHILD PORNOGRAPHY
NARCOTICS
CHILD ABUSE
HOMICIDE
RAPE
THEFT
FRAUD
ROBBERY
EMBEZZLEMENT
IDENTITY THEFT
BURGLARY
CARGO THEFT
AUTO THEFT

Cyber Forensics

- General instances where computers can be involved:

1. Technology is the target of criminals.
   - *Intrusion*
2. Technology is used to commit crime.
   - *Counterfeiting*
3. Technology becomes a repository of potential evidence.
   - *Insurance Fraud*

Definition of a Computer

Computer

Date: 1646

:one that computes; specifically: a programmable electronic device that can store, retrieve, and process data.

What other common devices can be considered computers?

Identification of Evidence

- Desk Top PC's
- Notebook PC's
- Personal Data Assistants
- Digital Cameras
- Digital Camcorders
- Cellular/Wireless Telephones
- Pagers
- Cordless Telephones
- Caller I.D. Devices
- Answering Machines
- Audio Devices
- GPS Devices
- Web TV Devices

*Supporting Storage Media

Desktop PC's

Network PC's

Notebook PC's

Wireless/Cellular Telephone

Digital Cameras

Pagers

Digital Video Recorders

Digital Audio Recorders

Cordless Telephones

Personal Data Assistant

Digital Answering Machines

Caller I.D. Recorders

As an Example

- Mobile Telephone
- Internet Browser
- Text Messaging
- Personal Information Manager
- Built -in GPS Receiver
- Touch-Screen
- Fax Reception
- Infrared Port
- Ready for 144 kbps wireless connections
- Word Document Viewer
- Dictaphone
- Handwriting Recognition

The Way It Was:

- All crimes were “local”
  - criminal/crime/victim all in same city or state
  - evidence never found far from crime scene
  - Tony Baretta, Joe Friday, Steve McGarrett of 5-O
    - never went far to get their man (woman)
  - only Lewis Erskine (*the FBI*) roamed the US
    - Bank robbers across state lines
    - Communist spy
    - Bombings

Today: Revolution in Criminal Activity

- Crimes committed remotely
  - criminal can be 1,000 or 10,000 miles from victim
  - evidence can be thousands of miles away, too
- International element added to any crime
  - by geography or by design
  - *mechanisms for international cooperation can slow or derail many more investigations*

Adding an International Element

- Criminal in San Diego; Victim in Riverside
- Hacker routes communication through:
  - Sweden
  - South Africa
  - Thailand
- Riverside LE needs assistance from Stockholm, Pretoria, Bangkok to solve “local” crime

Current Challenges to Law Enforcement

- Anonymity, Reach More Victims, Intangibility, Rapid Tech Development
- Lack of boundaries
  - No jurisdictional boundaries - domestic or international
  - Conflicting laws
- Resources: Training and retention of technically skilled agents/personnel
- Perishable skill needs constant use and ongoing training

Current Challenges to Law Enforcement

- Adequate substantive and procedural laws
- Educating the public
- As sophistication of attacks has increased, so has the need for computer forensic knowledge and techniques

Corporate America

- Most companies are unwilling to report computer crimes
  - Fear
  - Bad press
  - Lack of confidence in law enforcement
  - Business interruption (seizing computers for evidence)
  - Little to gain

THE GLOBAL INTERNET – Friend or Foe?

Since the commercialization of the Internet in the early 1990s, the Internet has become our best resource and our worst nightmare.

Started in _____ the once experimental Military project, has now grown into a global marketplace and information superhighway with over 500 million users worldwide, and 50% of those come from the U.S.

Although we have laws specific to the Internet, there is no exclusive governing agency.

Today's Technology Experience

- More and more aspects of our lives are becoming virtual/online
  - We pay bills online
  - We shop online
  - We get medical advice online
  - Personal information is stored, updated and communicated in digital form
  - We even save lives over the Internet
  - And catch thieves

Home Page
World
U.S.
Weather
Business at CNNMoney
Sports at SI.com
Politics
Law
Technology
Science & Space
Health
Entertainment
Travel
Education
Special Reports
Video
Autos with Edmunds.com

SERVICES
CNN Pipeline
E-mail Newsletters
Your E-mail Alerts
Podcasts POD
RSS XML
CNNtoGO
Contact Us
SEARCH
WEB CNN.com
SEARCH Powered by YAHOO! search

WORLD

Sons save mom overseas with webcam

Friday, November 18, 2005; Posted: 6:31 a.m. EST (11:31 GMT)

OSLO, Norway (AP) -- A Web camera in a Norwegian artist's living room in California allowed her sons in Norway and the Philippines to see that she had collapsed and call for help, one of the sons said Friday.

Karin Jordal, 69, collapsed Thursday in her living room in Pinon Hills, California, and was motionless on a couch when her son Tore in the Philippines checked in through the Internet.

"He tried to call her, and got no answer," Tore's brother, Ole Jordal, said by telephone from the western Norway city of Bergen. "He had also tried to call the police and ambulances (in California) but couldn't get through."

Ole Jordal said his brother then called him in Norway, as he and his wife, Tammy, originally from Long Island, New York, were having breakfast.

"My wife is American and she knew exactly whom to call for help," he said. "It took five or 10 minutes for the ambulance personnel to arrive."

He said the family was on the verge of tears when they watched on the Web camera as ambulance personnel assisted their diabetic mother, who is recovering in the Desert Valley Hospital in California.

"I thank that camera and my sons for my life," Karin Jordal told the Norwegian newspaper Bergens Tidende by telephone from her hospital bed. She has lived in

BBC NEWS UK EDITION

Last Updated: Friday, 18 February, 2005, 12:53 GMT

E-mail this to a friend Printable version

How to catch a thief - with your PC

By Joe Boyle
BBC News

Cambridgeshire police hailed a software engineer who caught a burglar on his webcam as "absolutely brilliant". But how easy is it to turn your home PC into a surveillance system?

"As long as you're not a complete technophobe, pretty much anyone can do it" says Simon Pickstock, editor of technology magazine PC Answers.

Serial burglar caught on webcam

The first step is buying a webcam.

The tiny bug-eyed devices are available in most electronic shops and sell for anywhere between £15 and £60. They come with their own software

Impact of High Tech Crime

- The 2004 IC3 Annual Internet Fraud Crime Report states 207,449 complaints were received (http://www.ifccfbi.gov/strategy/2004_IC3Report.pdf)
  - Of those 190,143 complaints were referred to law enforcement agencies
  - The loss from the fraudulent criminal behavior was $68.14 million dollars
- Computer Security Institute's (CSI) Annual 2005 Computer Crime survey reports $130,104,542 in total loss estimated by the 639 respondents of the survey, with the highest category being Viruses totaling over $42 million (CSI, 2005 Computer Crime and Security Survey, http://www.gocsi.com)

Impact of High Tech Crime

- According to Symantec Jan-June 2005 Internet Security Threat Report (http://ses.symantec.com/WP000ITR8):
  - The time between the disclosure of a vulnerability and the release of an associated exploit was 6.0 days.
  - The average patch-release time for the past 6 months was 54 days. This means that, on average, 48 days elapsed between the release of an exploit and the release of an associated patch.
  - 73% of reported vulnerabilities this period were classified as easily exploitable.
  - 97% of vulnerabilities were either moderately or highly severe.

Impact of High Tech Crime

- Symantec identified an average of 10,352 bots per day, up from 4,348 in December 2004.
- 33% of Internet attacks originated in the United States, up from 30% last period.
- Symantec documented more than 10,866 new Win32 virus and worm variants, a 48% increase over the second half of 2004 and a 142% increase of the first half of 2004.

Impact of High Tech Crime

- Messages that constitute phishing attempts increased from an average of 2.99 million per day to approximately 5.70 million messages.
- Spam made up 61% of all email traffic.
- 51% of all spam received worldwide originated in the United States.
- Malicious code that exposes confidential information represented 74% of the top 50 malicious code samples received by Symantec.

Computer Crime Laws

Computer crime related laws

- State of California:
  - Penal Code Section 502 covers most aspects of computer related crimes

- State of Washington
  - Malicious Mischief - RCW 9A.48.070
  - Computer Trespass - RCW 9A.52.110 and RCW 9A.52.120

Computer crime related laws

- Federal Statutes
  - 18 U.S.C. 875 Interstate Communications: Including Threats, Kidnapping, Ransom, Extortion
  - 18 U.S.C. 1029 Possession of Access Devices
  - 18 U.S.C. 1030 Fraud and related activity in connection with computers
  - 18 U.S.C. 1343 Fraud by wire, radio or television
  - 18 U.S.C. 1361 Injury to Government Property
  - 18 U.S.C. 1362 Government communication systems
  - 18 U.S.C. 1831 Economic Espionage Act
  - 18 U.S.C. 1832 Trade Secrets Act

Computer crime related laws

- Title III Wiretap (content)
- Pen Trap & Trace (header information)
  - Court order (search warrant)
- Exceptions to Title III
  - Court order
  - Consent
  - Intruder

Other computer crime related legislation

- California Senate Bill 1386 - Civil codes 1798.29, 1798.82:
  - Any person, company, or agency
  - that owns or licenses computerized data that includes personal information
  - shall disclose any breach of the security of the system following discovery or notification of the breach in the security of the data
  - to any resident of California whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person

Other computer crime related legislation

- Sarbanes Oxley Act of 2002 (SOX)
  - Requires Internal controls to stem corporate crime, including computer forensic capability
- Gramm-Leach-Bliley (GLB) Act
  - Mandates Financial institutions to have Computer Incident Response plan, timely investigation and notification
- US Patriot Act
  - ECPA
  - U.S.C. Title 1, Chapter 121, Section 2703

Other Privacy Issues

- Scope of examination
  - Surgical court orders
- Privacy disclaimers
  - Employee/employer relationships
- Notification of subscriber information request
  - Patriot act
  - Search warrants

Evolution of Computers

- 1980s – Small personal computers
  - DOS based programs
  - Tape Drives

- 1990s – Personal computers, networked businesses, Internet, Microsoft Windows Operating System became popular
  - Average Hard drive was 20mb-80mb

- 2000s- Personal computers, workstations, servers, Server class hardware
  - Home = 80 GB hard drives
  - Businesses = multi Terabyte storage arrays

Data Storage

80 Gig
Hard Drive

16 DVD's

74 CD's

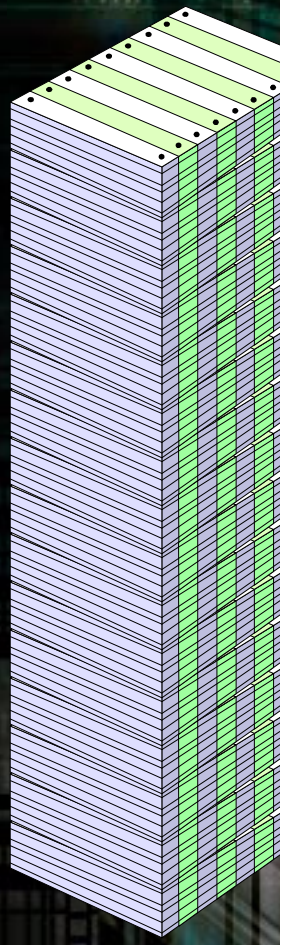
57,142
Floppy Disk's

The
Empire State Building

Stands 1,454'

Height of Paper
Stacked
Top
to
Bottom nine
times:

13,333 feet or
2.5 miles high



Evolution of Digital Forensics

- 1980s – Floppy disks were disk copied and examined using DOS
- 1990s – DOS command line tools were used to copy data from storage devices and examined in a DOS hex editor
- 2000s- GUI applications used to conduct advanced low level analysis of media and digital data
- 2005 – GUI applications & alternate operating systems used for forensic analysis, common digital media examination includes computers, removable media, cameras, PDAs, cell phones

Current Challenges of Computer Forensics

- Larger storage capacity requires need to process more data
  - If an acquisition of 80gb takes 2 hours, what does 1TB take?
  - How do you store this long term?
- Forensic examination process is time consuming, new cases arrive faster than older ones are adjudicated
- Encryption has become easily available and has gained more popularity over time thus thwarting forensic examinations

Current Challenges of Computer Forensics

- New technology such as steganography used to hide data inside data
- Data wiping tools readily available and more common
- Anonymous email, remailers, proxy services
- Public access computers/Internet

Current Challenges of Computer Forensics

- Portable applications (browsers)
- Encrypted instant messaging
- VoIP

The Process of Computer Forensics

- Network Forensics
  - The analysis of network, communication data
- Volatile Data Forensics
  - The analysis of transient, dynamic information on a live machine
- File System Forensics
  - The analysis of static information on digital media

The Process of Computer Forensics

- Network forensics involves
  - Capturing digital communication data with a network capturing tool and interpretation

The Process of Computer Forensics

- Volatile Data Forensics Involves
  - Involves the collection of volatile data and:
    - Analysis of running processes
      - Process list
      - Process/port mapping
    - Analysis of current socket conditions
      - Active communications
      - Processes bound to ports
    - Analysis of the contents of memory (RAM)
      - Current process usage
      - Residual memory data

The Process of Computer Forensics

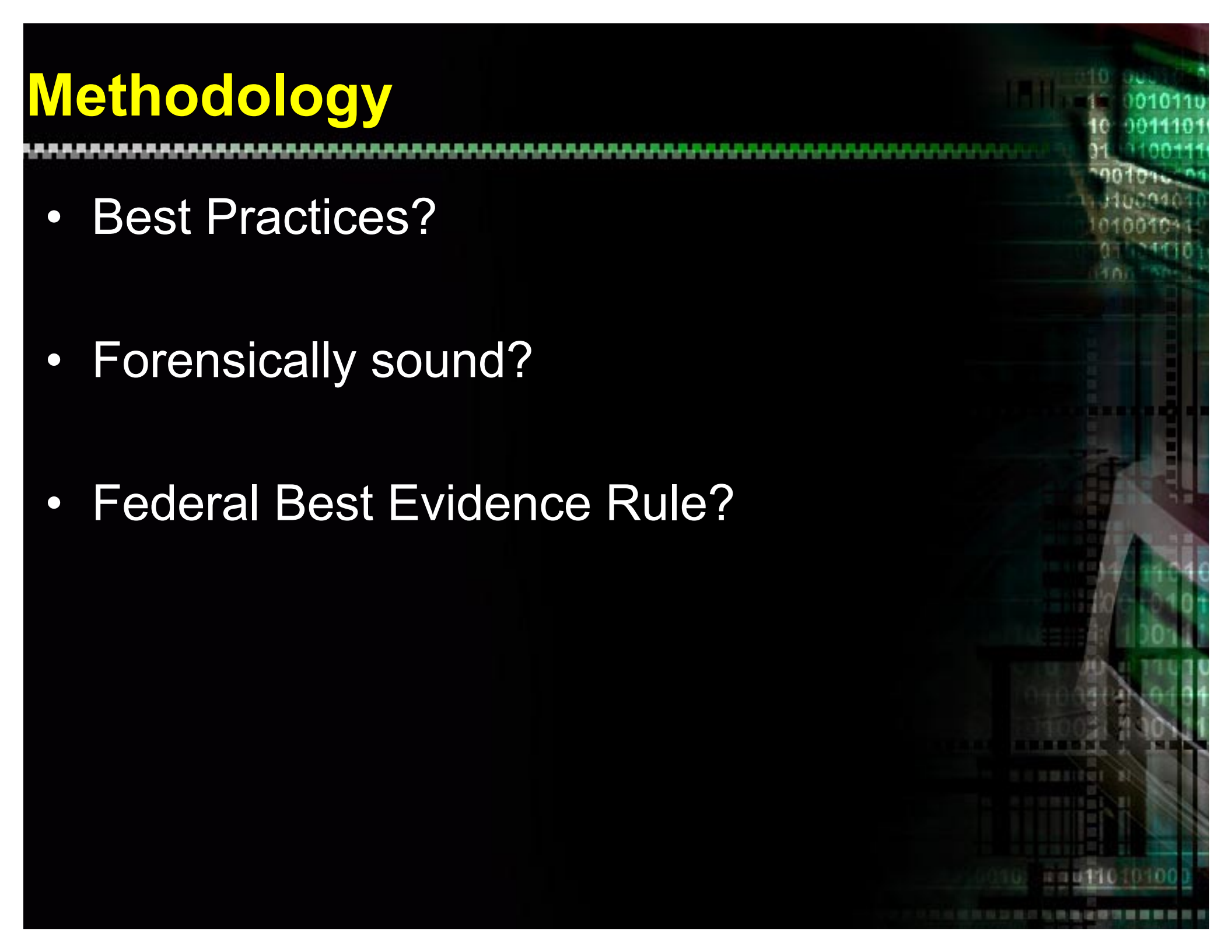
- Static File System Forensics
  - Involves “imaging” the original media and performing the analysis on the digital duplicate
  - Almost always a bit-for-bit copy is obtained
    - Different types of copies?
  - Specific commercial forensic tools or open source tools used to capture digital duplicate

The Process of Computer Forensics

- Live File System Forensics
  - Performed on the system while running
  - Can include capturing a digital duplicate
    - Issues?
  - Used to triage multiple systems quickly
  - Used to deal with portions of data when large storage arrays are encountered

Methodology

- Best Practices?
- Forensically sound?
- Federal Best Evidence Rule?



Common Training & Skills

- Advanced computer knowledge
- Networking knowledge
- Multiple operating systems
- CS/CIS background
- Investigative knowledge / methodical
- Programming languages helpful
- Low level knowledge of media formats
  - Disk geometry
  - File systems
    - FAT/NTFS/EXT2-3/HFS/HFS+/UFS

Computer Forensics at work

- How Computer Forensics played a crucial role in past criminal matters

Sami Omar Al-Hussayan

UNITED STATES DISTRICT COURT FOR THE DISTRICT OF IDAHO

UNITED STATES OF AMERICA,	)	**Cr. No.**
	)	
	)	**SECOND**
Plaintiff,	)	**SUPERSEDING INDICTMENT**
	)	
vs.	)	**(Vio. 18 U.S.C. 371 , 956, 2339A, 2339B, 1546(a), 1001(a)(2), 3237, 3238)**
	)	
SAMI OMAR AL-HUSSAYEN,	)	
	)	
Defendant.	)	

Case # 1

audi Student's Trial Opens in Idaho

overnment Alleges 'Material Support' for Terrorism in Use of Internet

' Susan Schmidt
ashington Post Staff Writer
ursday, April 15, 2004; Page A05

OISE, Idaho, April 14 -- A Saudi doctoral candidate at the University of Idaho hid his true agenda as webmaster and "money man" r a worldwide Internet network that sought to finance and recruit fighters for violent holy war abroad, prosecutors charged 'ednesday in opening their case against Sami Omar al-Hussayen.

ussayen, arrested a year ago in the tiny northern Idaho university town of Moscow, was a dual personality, federal prosecutor Kim ndquist told the jury. The face he presented to the public was that of a studious family man, but his "private face" was that of a man ho promoted "extreme jihad" and "provided recruitment and funding for terrorism," Lindquist said.

a case that tests the contours of federal statutes barring "material support" for terrorists and terrorist organizations, federal authorities e seeking to prove that the use of the Internet to promote and recruit for jihad constitutes such support. Defense lawyers contend that ussayen's Internet activity amounted to constitutionally protected free speech.

ne case against Hussayen is the result of one of the most intensive terrorism-related investigations since the Sept. 11, 2001, attacks, a assive two-year probe that is tied to other cases, including ongoing investigations of charities suspected of financing terrorism.

ussayen is accused of conspiracy and providing support to terrorists in Chechnya and Israel, and of conspiracy to raise funds for the litary wing of the Islamic Resistance Movement, a designated terrorist organization also known as Hamas. His indictment charges that ussayen "knew and intended that the material support he provided [was] to be used in preparation for, and to commit, violations of deral law involving murder, maiming, kidnapping, and the destruction of property," a contention the government repeated on 'ednesday.

Partition Table

Primary Computer was seized and examined:

Type	Start Sector	Total Sectors	Size
FAT32X	0	41383440	19.7GB
Linux EXT2	41383440	10442250	5.0GB
Linux EXT2	58862160	755055	368.7MB
Linux Swap	59617216	176716	86.3MB
Linux Swap	51825690	498015	243.2MB
Linux EXT2	52323705	6538455	3.1GB

Summary of Forensic Analysis

- The application “SmartFTP” was discovered on the system.
- Analysis of forensic residue from the use of this application revealed 155 user-initiated connections to 20 different computer servers on the Internet, utilizing 16 various user accounts.
- Subsequent forensic examination of the application resulted in the identification of 16 user account passwords.

SmartFTP Folder

- The FAT32X partition of the system was mapped as logical drive “C:” on the suspect system. During examination, the application “SmartFTP” was found to be installed in the directory “C:\Program Files\SmartFTP\”.

Directory Name	Last Accessed	Last Written	File Created
C:\Program Files\SmartFTP	2/23/03	08/15/02 04:36:16PM	08/15/02 04:35:14PM

SmartFTP Application Data

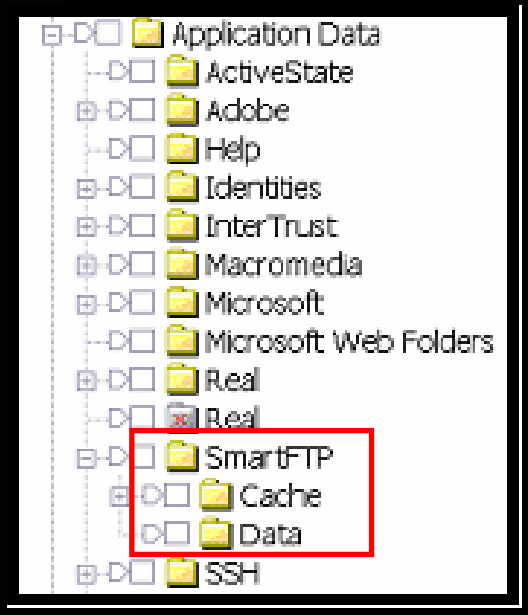
- Additional data associated with this application was found stored in the directory `C:\Documents and Settings\Me\Application Data\SmartFTP\.`

Directory Name	Last Accessed	Last Written	File Created
C:\Documents and Settings\Me\Application Data\SmartFTP	2/23/03	09/24/02 10:00:30AM	09/24/02 10:00:28AM

SmartFTP Cache Folder

- The “SmartFTP” directory contained a subdirectory entitled “Cache”.

Directory Name	Last Accessed	Last Written	File Created
C:\Documents and Settings\Me\Application Data\SmartFTP\Cache	2/23/03	09/24/02 10:00:18:24AM	09/24/02 10:00:22AM



Cache Folder

- The “Cache” directory contained entries for 155 subdirectories which were deleted.
- The subdirectories are created and deleted as part of the normal operation of the program.
- The “Cache” directory and the 155 subdirectories were created by the SmartFTP program.

Cache Folder

- The names of the deleted subdirectories revealed information concerning use of the application by a user of the computer system, to include:
  - the remote destination computer name
  - user identification
  - port the user connected to when utilizing the SmartFTP application.

- SmartFTP
  - Cache
    - 152.160.23.131-sami-21
    - 152.160.23.131-sami-21
    - 152.160.23.131-sami-21
    - 152.160.23.131-sami-21
    - 152.160.23.131-sami-21
    - 152.160.23.131-sami-21
    - 198.169.127.205-root-21
    - 198.169.127.205-root-22
    - 198.169.127.205-sami-21
    - 198.169.127.205-sami-22
    - 198.169.127.211-Administrator-21
    - 198.169.127.211-Administrator-21
    - al-multaqa.com-alm15086-21
    - alasr.net-alasr-21
    - alasr.net-alasr-21
    - alasr.ws-alasr-21
    - alasr.ws-alasr-21
    - alasr.ws-alasr-21
    - alasr.ws-alasr-21
    - alasr.ws-alasr-21
    - alasr.ws-alasr-21
    - alasr.ws-alasr-21
    - almultaqa.com-alm15086-21
    - ci.engboi.uidaho.edu-sami-21
    - ci.engboi.uidaho.edu-sami-21
    - ci.engboi.uidaho.edu-sami-21
    - ci.engboi.uidaho.edu-sami-21
    - ci.engboi.uidaho.edu-sami-21
    - ci.engboi.uidaho.edu-sami-21
    - ci.engboi.uidaho.edu-sami-21
    - ci.engboi.uidaho.edu-sami-21
    - ci.engboi.uidaho.edu-sami-21
    - ci.engboi.uidaho.edu-sami-21
    - ci.engboi.uidaho.edu-sami-21
    - ci.engboi.uidaho.edu-sami-21
    - ci.engboi.uidaho.edu-sami-21
    - ci.engboi.uidaho.edu-sami-21
    - ci.engboi.uidaho.edu-sami-21
    - ci.engboi.uidaho.edu-sami-21
    - ci.engboi.uidaho.edu-sami-21
    - ci.engboi.uidaho.edu-sami-21
    - ci.engboi.uidaho.edu-sami-21
    - ftp.cis.fed.gov-anonymous-21
    - ftp.its.uidaho.edu-anonymous-21
    - islamtoday.net-Administrator-21
    - islamtoday.net-Administrator-21
    - islamway.com-admin-21
    - islamway.com-admin-21
    - liveislam.com
    - liveislam.com-ftpuser-21
    - liveislam.com-ftpuser-6060
    - liveislam.com-ftpuser-6060
    - liveislam.com-samio-21
    - liveislam.com-samio-21
    - liveislam.com-samio-21
    - liveislam.com-samio-21
    - liveislam.com-samio-21
    - liveislam.com-samio-21
    - liveislam.com-samio-21
    - liveislam.com-samio-21
    - liveislam.com-samio-21
    - liveislam.com-samio-21
    - liveislam.com-samio-21
    - liveislam.com-samio-21
    - liveislam.com-samio-21
    - liveislam.com-samio-21
    - liveislam.com-samio-21
    - liveislam.com-samio-21
    - liveislam.com-samio-21
    - liveislam.com-samio-21
    - liveislam.com-samio-21
    - liveislam.com-samio-21
    - liveislam.com-samio-21
    - liveislam.com-samio-21
    - liveislam.com-samio-21
    - liveislam.com-samio-21
    - liveislam.com-samio-21
    - liveislam.com-samio-21
    - liveislam.com-samio-21
    - liveislam.com-samio-21
    - liveislam.com-samio-21
    - liveislam.com-samio-21
    - liveislam.com-samio-21
    - liveislam.com-samio-21
    - liveislam.com-samio-21
    - liveislam.com-samio-21
    - liveislam.com-samio-21
    - liveislam.com-samio-21
    - liveislam.com-samio-21
    - liveislam.com-samio-21
    - liveislam.com-samio-21
    - liveislam.com-samio-21
    - liveislam.com-samio-21
    - liveislam.com-samio-21
    - liveislam.com-samio-21
    - liveislam.com-samio-21
    - liveislam.com-samio-21
    - liveislam.com-samio-21
    - liveislam.com-samio-21
    - liveislam.com-samio-21
    - liveislam.com-samio-21
    - liveislam.com-samio-21
    - liveislam.com-samio-21
    - liveislam.com-samio-21
    - liveislam.com-samio-21
    - liveislam.com-samio-21
    - liveislam.com-samio-21
    - liveislam.com-samio-21
    - liveislam.com-samio-21
    - liveislam.com-samio-21
    - liveislam.com-samio-21
    - liveislam.com-samio-21
    - liveislam.com-samio-21
    - liveislam.com-samio-21
    - liveislam.com-samio-21
    - liveislam.com-samio-21
    - liveislam.com-samio-21
    - liveislam.com-samio-21
    - liveislam.com-samio-21
    - liveislam.com-samio-21
    - liveislam.com-samio-21
    - liveislam.com-samio-21
    - liveislam.com-samio-21
    - liveislam.com-samio-21
    - liveislam.com-samio-21
    - liveislam.com-samio-21
    - liveislam.com-samio-21
    - liveislam.com-samio-21
    - liveislam.com-samio-21
    - liveislam.com-samio-21
    - liveislam.com-samio-21
    - liveislam.com-samio-21
    - liveislam.com-samio-21
    - liveislam.com-samio-21
    - liveislam.com-samio-21
    - liveislam.com-samio-21
    - liveislam.com-samio-21
    - liveislam.com-samio-21
    - liveislam.com-samio-21
    - liveislam.com-samio-21
    - liveislam.com-samio-21
    - liveislam.com-samio-21
    - liveislam.com-samio-21
    - liveislam.com-samio-21
    - liveislam.com-samio-21
    - liveislam.com-samio-21
    - liveislam.com-samio-21
    - mail.islamtoday.net-Administrator-21
    - mail.islamtoday.net-Administrator-21
    - mail.islamtoday.net-Administrator-21
    - mail.islamtoday.net-Administrator-21
    - muntada.islamtoday.net-FreeWheel-21
    - muntada.islamtoday.net-FreeWheel-21
    - muntada.islamtoday.net-jesse-21
    - muntada.islamtoday.net-jesse-21
    - muntada.islamtoday.net-jesse-21
    - muntada.islamtoday.net-root-21
    - nationvoice.com-nationvo-21
    - nationvoice.com-upload-21
    - neuron.engboi.uidaho.edu-ala-21
    - neuron.engboi.uidaho.edu-sami-21
    - neuron.engboi.uidaho.edu-sami-21
    - neuron.engboi.uidaho.edu-sami-21
    - neuron.engboi.uidaho.edu-sami-21
    - neuron.engboi.uidaho.edu-sami-21
    - neuron.engboi.uidaho.edu-sami-21
    - reciter.org-reciterorg-21
    - reciter.org-reciterorg-21
    - reciter.org-reciterorg-21
    - reciter.org-reciterorg-21
    - reciter.org-reciterorg-21
    - reciter.org-reciterorg-21
    - unix.uidaho.edu-alhu6728-21
    - www.islamtoday.net-Administrator-21
  - Data

Cache Folder Entry

- As an example, the directory entry below reveals that the user connected to the computer known on the Internet as "`www.islamtoday.net`" with the User Identification "Administrator" to Port 21.

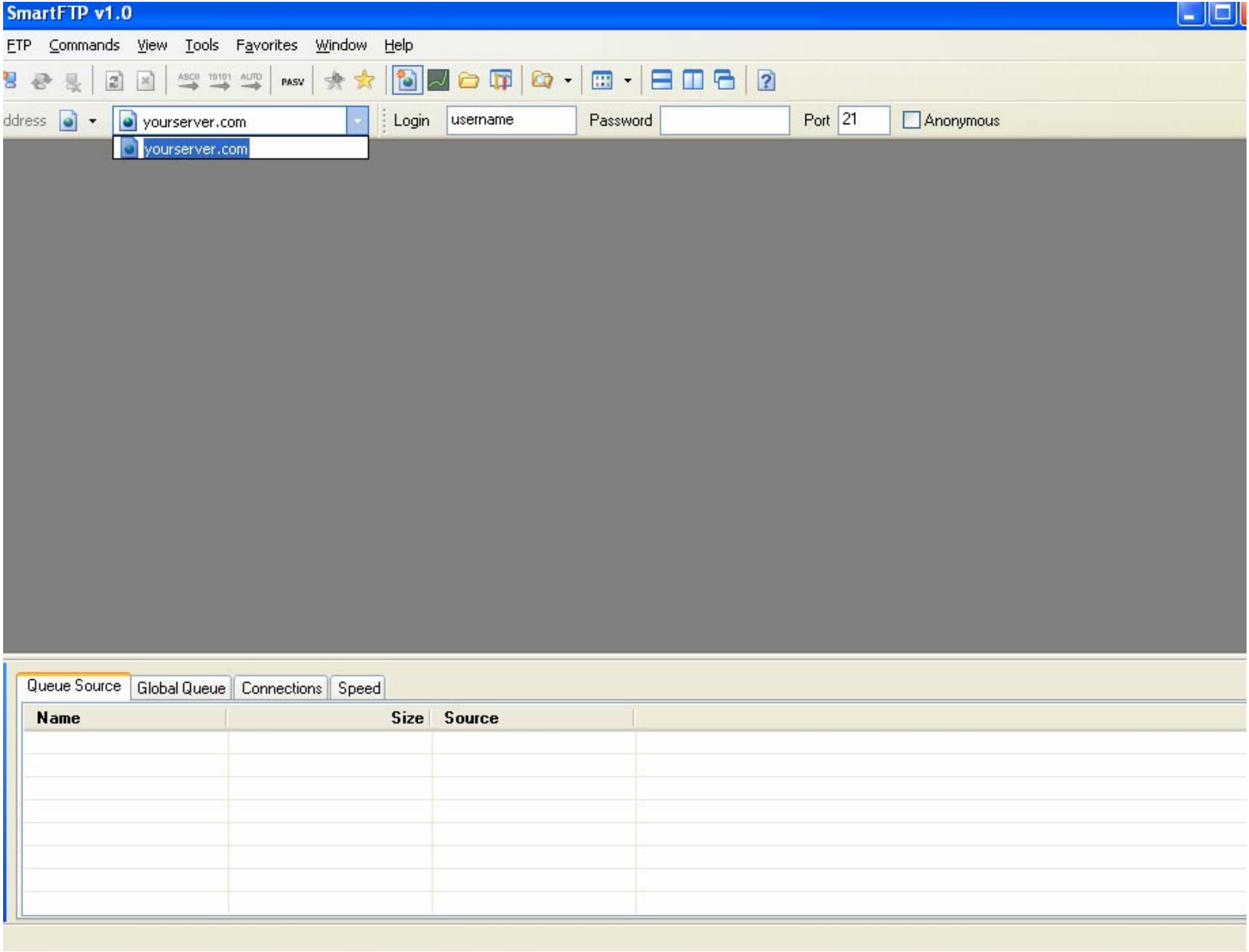
Site	Account	Port
152.160.23.131-sami-21	sami	21 (FTP)
198.169.127.205-root-21	root	21 (FTP)
198.169.127.205-root-22	root	22 (Secure Shell)
198.169.127.205-sami-21	sami	21 (FTP)
198.169.127.211-Administrator-21	Administrator	21 (FTP)
al-multaqa.com-alm15086-21	alm15086	21 (FTP)
alasr.net-alasr-21	alasr	21 (FTP)
alasr.ws-alasr-21	alasr	21 (FTP)
almultaqa.com-alm15086-21	alm15086	21 (FTP)
ci.engboi.uidaho.edu-sami-21	sami	21 (FTP)
ftp.cis.fed.gov-anonymous-21	anonymous	21 (FTP)
ftp.its.uidaho.edu-anonymous-21	anonymous	21 (FTP)
islamtoday.net-Administrator-21	Administrator	21 (FTP)
islamway.com-admin-21	admin	21 (FTP)
liveislam.com-ftpuser-21	ftpuser	21 (FTP)
liveislam.com-ftpuser-6060	ftpuser	6060
liveislam.com-samio-21	samio	21 (FTP)
mail.islamtoday.net-Administrator-21	Administrator	21 (FTP)
muntada.islamtoday.net-FreeWheel-21	FreeWheel	21 (FTP)
muntada.islamtoday.net-jesse-21	jesse	21 (FTP)
muntada.islamtoday.net-root-21	root	21 (FTP)
nationvoice.com-nationvo-21	nationvo	21 (FTP)
nationvoice.com-upload-21	upload	21 (FTP)
neuron.engboi.uidaho.edu-ala-21	ala	21 (FTP)
neuron.engboi.uidaho.edu-sami-21	sami	21 (FTP)
reciter.org-reciterorg-21	reciterorg	21 (FTP)
unix.uidaho.edu-alhu6728-21	alhu6728	21 (FTP)
www.islamtoday.net-Administrator-21	Administrator	21 (FTP)

Privileged Accounts

- The User Accounts “root”, “admin” and “Administrator” usually represent *privileged accounts* generally reserved for the owner or administrator of the computer.
- Based on the account names, the user of the system had privileged access to the sites
  - 198.169.127.205
  - 198.169.127.211
  - islamtoday.net
  - islamway.com
  - mail.islamtoday.net
  - muntada.islamtoday.net
  - www.islamtoday.net
- The rights and privileges of the other accounts cannot be determined from the limited information available.

Application Analysis

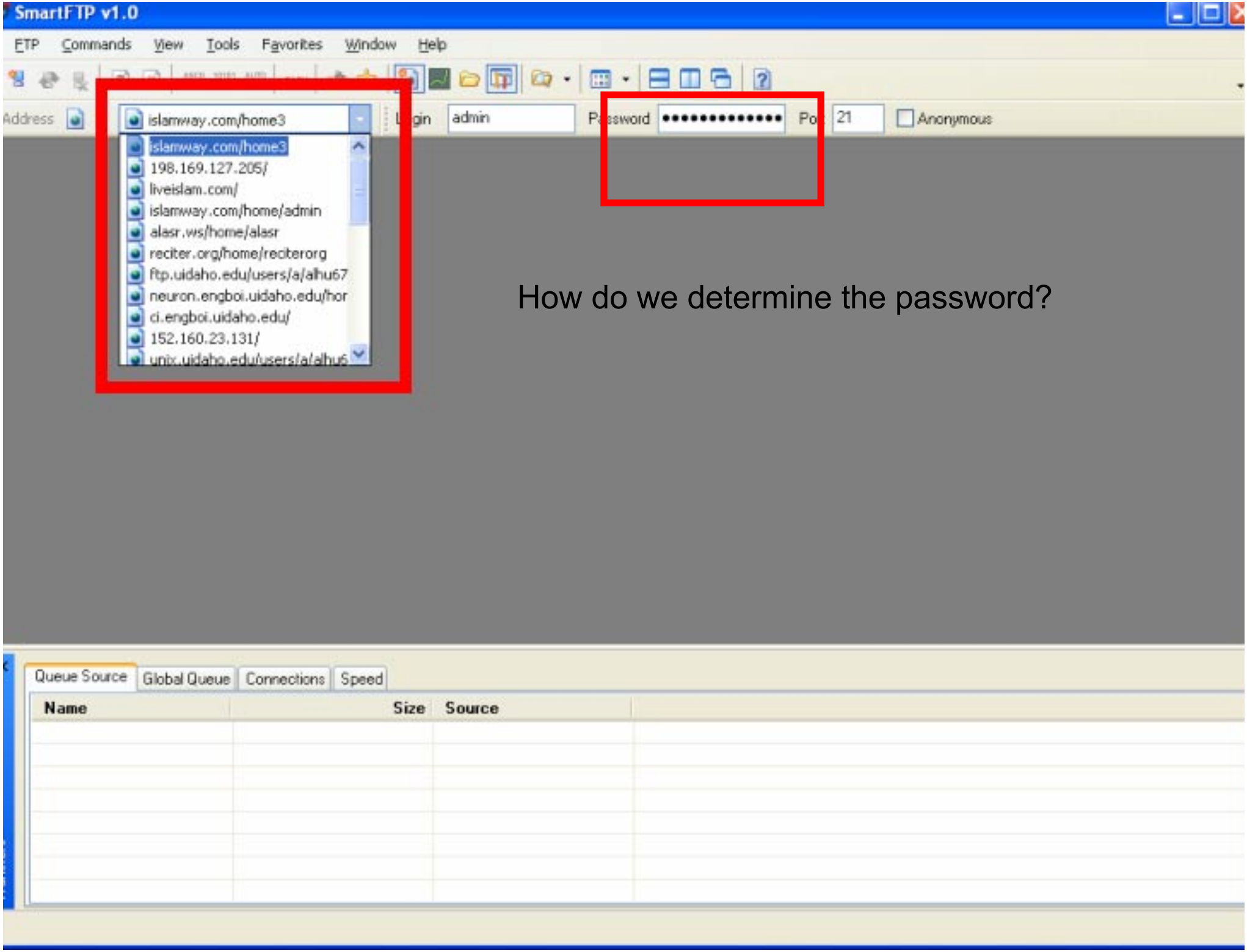
- Forensic examination and testing was performed on the SmartFTP application to confirm the operation of the software and the creation of the contents of the cache directory.
- The application was installed on a forensic workstation which was disconnected from the Internet.
- A default installation of SmartFTP was performed.


SmartFTP v1.0
FTP
Commands
View
Tools
Favorites
Window
Help
ASCII
10101
AUTO
PASV
ddress
yourserver.com
yourserver.com
Login
username
Password
Port
21
Anonymous
Queue Source
Global Queue
Connections
Speed
Name
Size
Source

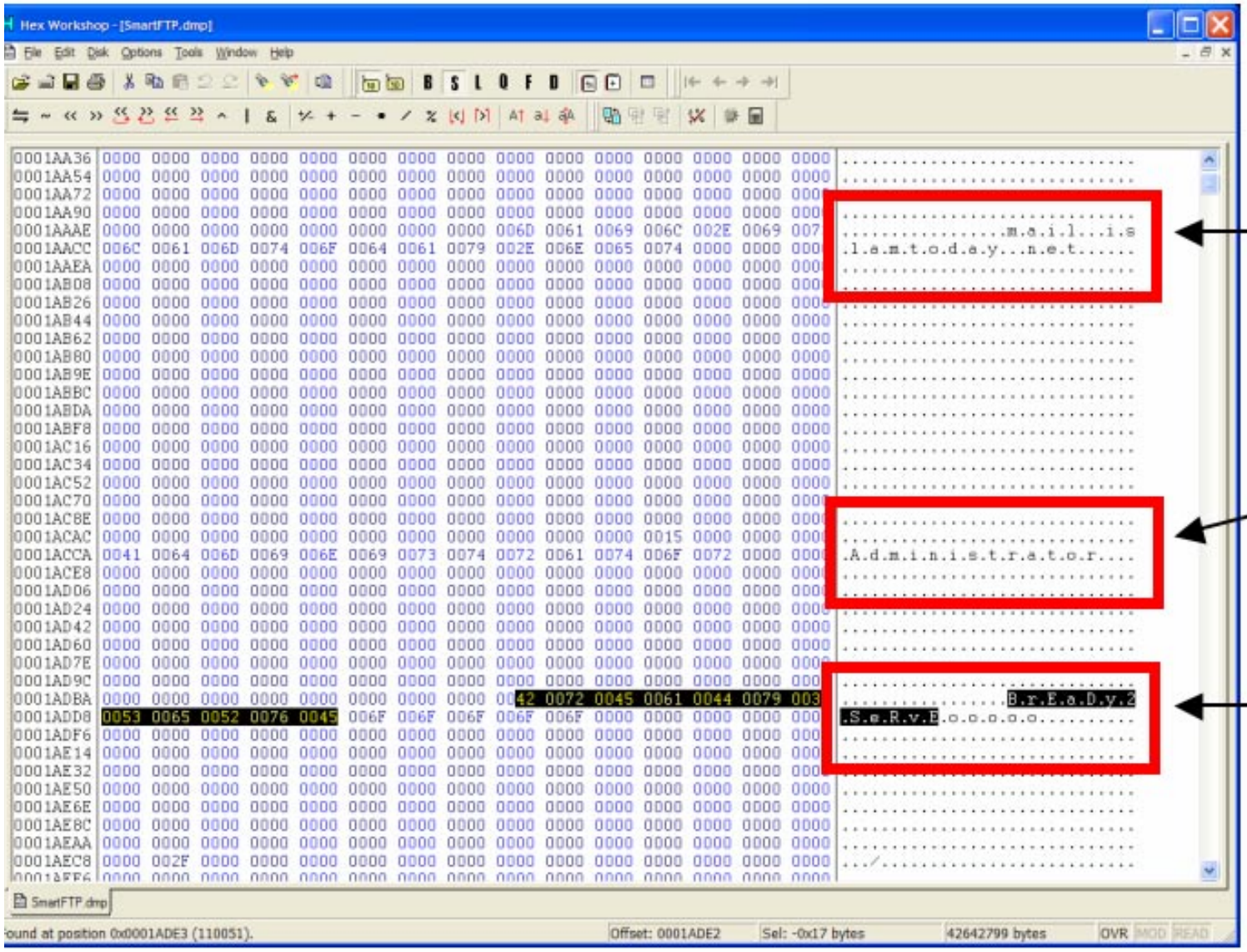
Files of Interest

- During the testing, it was determined that the two files listed below contained the user accounts and passwords in an encrypted and/or proprietary format.
- *By placing the suspect files in the appropriate location on the forensic workstation, the user's application history can be viewed.*

File Name	Last Accessed	Last Written	File Created	Logical Size	Hash Value
C:\Documents and Settings\Me\Application Data\SmartFTP\History.dat	02/23/03	02/23/03 11:55:06AM	09/24/02 10:00:28AM	1,577	e9f90c943a686ca2006ea3ad8e8100f
C:\Documents and Settings\Me\Application Data\SmartFTP\CUSTOM.DAT	02/23/03	02/23/03 11:55:06AM	09/24/02 10:00:30AM	3,361	36f901b0dae05031a021d988a6331a8


SmartFTP v1.0
FTP
Commands
View
Tools
Favorites
Window
Help
Address
islamway.com/home3
admin
21
Anonymous
islamway.com/home3
198.169.127.205/
liveislam.com/
islamway.com/home/admin
alasr.ws/home/alasr
reciter.org/home/reciterorg
ftp.uidaho.edu/users/a/alhu67
neuron.engboi.uidaho.edu/hor
ci.engboi.uidaho.edu/
152.160.23.131/
How do we determine the password?
Queue Source
Global Queue
Connections
Speed
Name
Size
Source

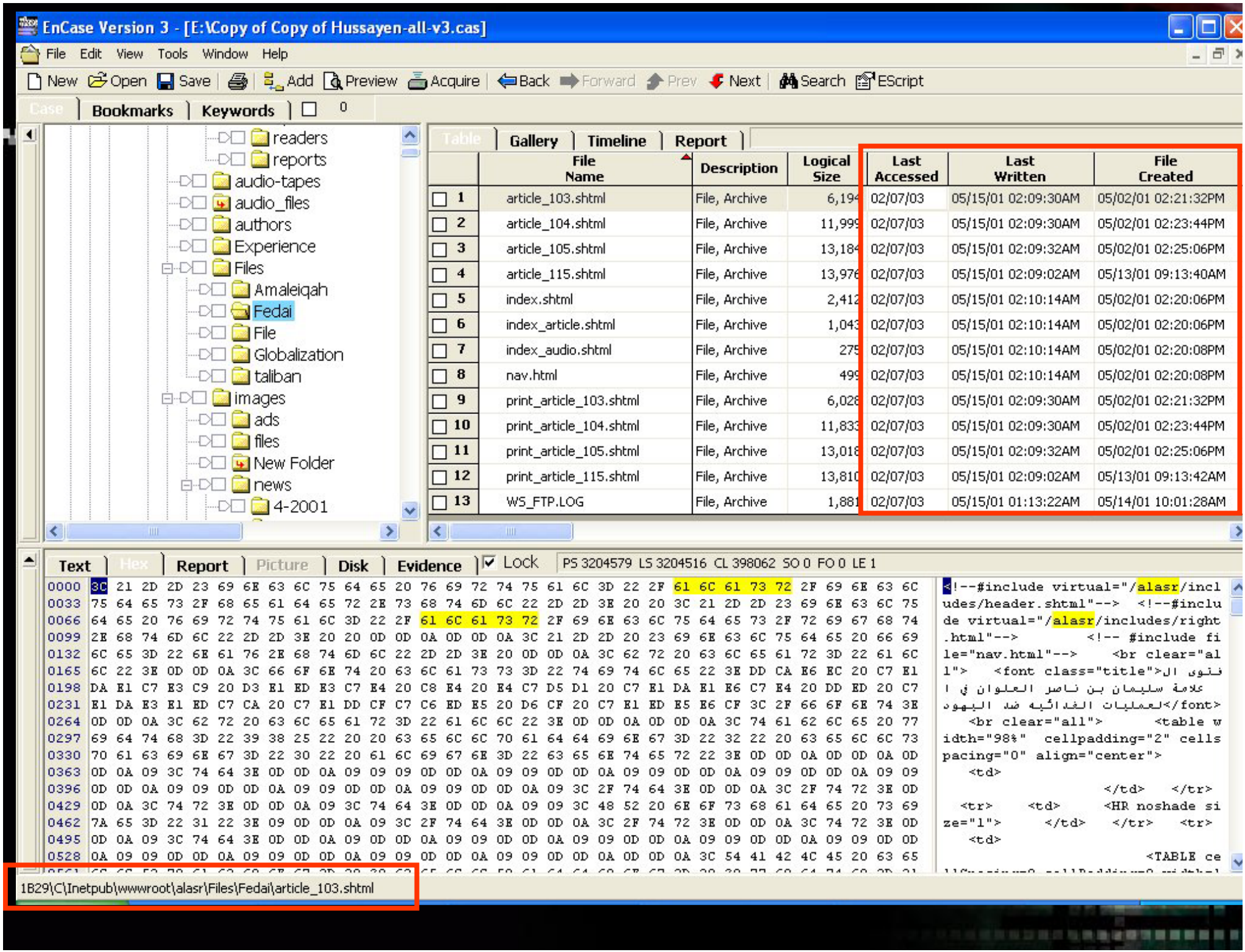
Password Extraction From Application Memory



Remote Site:
mail.islamtoday.net

Account:
Administrator

Password:
BrEaDy2SeRvE


EnCase Version 3 - [E:\Copy of Copy of Hussayen-all-v3.cas]
File Edit View Tools Window Help
New Open Save Add Preview Acquire Back Forward Prev Next Search EScript
Case Bookmarks Keywords 0
readers
reports
audio-tapes
audio_files
authors
Experience
Files
Amaleiqah
Fedai
File
Globalization
taliban
images
ads
files
New Folder
news
4-2001
Table Gallery Timeline Report
File Name
Description
Logical Size
Last Accessed
Last Written
File Created
1 article_103.shtml File, Archive 6,194 02/07/03 05/15/01 02:09:30AM 05/02/01 02:21:32PM
2 article_104.shtml File, Archive 11,999 02/07/03 05/15/01 02:09:30AM 05/02/01 02:23:44PM
3 article_105.shtml File, Archive 13,184 02/07/03 05/15/01 02:09:32AM 05/02/01 02:25:06PM
4 article_115.shtml File, Archive 13,976 02/07/03 05/15/01 02:09:02AM 05/13/01 09:13:40AM
5 index.shtml File, Archive 2,412 02/07/03 05/15/01 02:10:14AM 05/02/01 02:20:06PM
6 index_article.shtml File, Archive 1,043 02/07/03 05/15/01 02:10:14AM 05/02/01 02:20:06PM
7 index_audio.shtml File, Archive 275 02/07/03 05/15/01 02:10:14AM 05/02/01 02:20:08PM
8 nav.html File, Archive 499 02/07/03 05/15/01 02:10:14AM 05/02/01 02:20:08PM
9 print_article_103.shtml File, Archive 6,028 02/07/03 05/15/01 02:09:30AM 05/02/01 02:21:32PM
10 print_article_104.shtml File, Archive 11,833 02/07/03 05/15/01 02:09:30AM 05/02/01 02:23:44PM
11 print_article_105.shtml File, Archive 13,018 02/07/03 05/15/01 02:09:32AM 05/02/01 02:25:06PM
12 print_article_115.shtml File, Archive 13,810 02/07/03 05/15/01 02:09:02AM 05/13/01 09:13:42AM
13 WS_FTP.LOG File, Archive 1,881 02/07/03 05/15/01 01:13:22AM 05/14/01 10:01:28AM
Text Hex Report Picture Disk Evidence Lock
PS 3204579 LS 3204516 CL 398062 SO 0 FO 0 LE 1
0000 3C 21 2D 2D 23 69 6E 63 6C 75 64 65 20 76 69 72 74 75 61 6C 3D 22 2F 61 6C 61 73 72 2F 69 6E 63 6C
0033 75 64 65 73 2F 68 65 61 64 65 72 2E 73 68 74 6D 6C 22 2D 2D 3E 20 20 3C 21 2D 2D 23 69 6E 63 6C 75
0066 64 65 20 76 69 72 74 75 61 6C 3D 22 2F 61 6C 61 73 72 2F 69 6E 63 6C 75 64 65 73 2F 72 69 67 68 74
0099 2E 68 74 6D 6C 22 2D 2D 3E 20 20 0D 0D 0A 0D 0D 0A 3C 21 2D 2D 20 23 69 6E 63 6C 75 64 65 20 66 69
0132 6C 65 3D 22 6E 61 76 2E 68 74 6D 6C 22 2D 2D 3E 20 0D 0D 0A 3C 62 72 20 63 6C 65 61 72 3D 22 61 6C
0165 6C 22 3E 0D 0D 0A 3C 66 6F 6E 74 20 63 6C 61 73 73 3D 22 74 69 74 6C 65 22 3E DD CA E6 EC 20 C7 E1
0198 DA E1 C7 E3 C9 20 D3 E1 ED E3 C7 E4 20 C8 E4 20 E4 C7 D5 D1 20 C7 E1 DA E1 E6 C7 E4 20 DD ED 20 C7
0231 E1 DA E3 E1 ED C7 CA 20 C7 E1 DD CF C7 C6 ED E5 20 D6 CF 20 C7 E1 ED E5 E6 CF 3C 2F 66 6F 6E 74 3E
0264 0D 0D 0A 3C 62 72 20 63 6C 65 61 72 3D 22 61 6C 6C 22 3E 0D 0D 0A 0D 0D 0A 3C 74 61 62 6C 65 20 77
0297 69 64 74 68 3D 22 39 38 25 22 20 20 63 65 6C 6C 70 61 64 64 69 6E 67 3D 22 32 22 20 63 65 6C 6C 73
0330 70 61 63 69 6E 67 3D 22 30 22 20 61 6C 69 67 6E 3D 22 63 65 6E 74 65 72 22 3E 0D 0D 0A 0D 0D 0A 0D
0363 0D 0A 09 3C 74 64 3E 0D 0D 0A 09 09 09 0D 0D 0A 09 09 0D 0D 0A 09 09 0D 0D 0A 09 09 0D 0D 0A 09 09
0396 0D 0D 0A 09 09 0D 0D 0A 09 09 0D 0D 0A 09 09 0D 0D 0A 09 3C 2F 74 64 3E 0D 0D 0A 3C 2F 74 72 3E 0D
0429 0D 0A 3C 74 72 3E 0D 0D 0A 09 3C 74 64 3E 0D 0D 0A 09 09 3C 48 52 20 6E 6F 73 68 61 64 65 20 73 69
0462 7A 65 3D 22 31 22 3E 09 0D 0D 0A 09 3C 2F 74 64 3E 0D 0D 0A 3C 2F 74 72 3E 0D 0D 0A 3C 74 72 3E 0D
0495 0D 0A 09 3C 74 64 3E 0D 0D 0A 09 0D 0D 0A 09 09 0D 0D 0A 09 09 0D 0D 0A 09 09 0D 0D 0A 09 09 0D 0D
0528 0A 09 09 0D 0D 0A 09 09 0D 0D 0A 09 09 0D 0D 0A 09 09 0D 0D 0A 0D 0D 0A 3C 54 41 42 4C 45 20 63 65
<!--#include virtual="/alasr/includes/header.shtml"--> <!--#include virtual="/alasr/includes/right.html"--> <!-- #include file="nav.html"--> <br clear="all"> فتوى ال علامة سليمان بن ناصر العلوان في العمليات الفدائيه ضد اليهود
<br clear="all"> <table width="98%" cellpadding="2" cellspacing="0" align="center">
<td>
</td> </tr>
<tr> <td> <HR noshade size="1"> </td> </tr> <tr>
<td>
<TABLE ce
1B29\C\Inetpub\wwwroot\alasr\Files\Fedai\article_103.shtml


D:\fatwa\Files\Fedai\print_article_103.shtml

فتوى العلامة سليمان بن ناصر العلوان في العمليات الفدائيه ضد اليهود

أرسل هذه الصفحة لصديقك
اطبع هذه الصفحة

فضيلة الشيخ سليمان بن ناصر العلوان حفظه الله تعالى تعلمون ما يحصل للفلسطينيين في هذا الوقت من الإجرام اليهودي والسكوت العربي المخزي . فهل في العمليات الفدائية ضد اليهود مخالفة شرعية ؟

بسم الله الرحمن الرحيم

الجواب : اليهود المرذولون مجمع النقائص والعيوب ومرتع الرذائل والشرور وهم أشد أعداء الله على الإسلام وأهله .

قال تعالى [لَتَجِدَنَّ أَشَدَّ النَّاسِ عَدَاوَةً لِّلَّذِينَ ءَامَنُوا الْيَهُودَ وَالَّذِينَ أَشْرَكُوا ....} المائدة .

وقد أوجب الله قتالهم وجهادهم لتكون كلمة الله هي العليا وكلمة الذين كفروا السفلى .

وهذا حين يقتع أعداء الله في ديارهم ولا ينقضون العهد والميثاق ولا يسلبون أموال المسلمين و يغتصبون ديارهم قال تعالى [قَاتِلُوا الَّذِينَ لاَ يُؤْمِنُونَ بِاللَّهِ وَلاَ بِالْيَوْمِ الأَخِرِ وَلاَ يُحَرِّمُونَ مَا حَرَّمَ اللَّهُ وَرَسُولُهُ وَلاَ يَدِينُونَ دِينَ الْحَقِّ مِنَ الَّذِينَ أُوتُوا الْكِتَابَ حَتَّى يُعْطُوا الْجِزْيَةَ عَنْ يَدٍ وَهُمْ صَاغِرُونَ (29)] التوبة.

فأما حين يضع أعداء الله سيوفهم في نحور المسلمين ويرعبون الصغير والكبير ويغتصبون الديار وينتهكون الأعراض فترض على أهل القدرة من المسلمين قتالهم وسفك دمائهم والجهاد الدائم حتى التحرير الشامل لفلسطين وعامة بلاد المسلمين .

ولا يجوز شرعاً التنازل لليهود عن أيّ جزء من أراضي المسلمين ولا الصلح معهم فهم أهل خديعة ومكر ونقض للعهود .

وأرى في وقت تخاذل المسلمين عن قتال اليهود والتنكيل بهم وإخراجهم عن الأرض المقدسة أن خير علاج وأفضل دواء نداوي به إخوان القردة والخنازير القيام بالعمليات الاستشهادية وتقديم النفس فداءً لدوافع إيمانية وغايات محمودة من زرع الرعب في قلوب الذين كفروا وإلحاق الأضرار


D:\fatwa\Files\Fedai\print_article_104.shtml

فتوى الشيخ حمود بن عقلاء الشعيبي في العمليات الاستشهادية

أرسل هذه الصفحة لصديقك
اطبع هذه الصفحة

فضيلة الشيخ حمود بن عقلاء الشعيبي حفظه الله من كل سوء

يقوم المجاهدون في فلسطين والشيشان وغيرهما من بلاد المسلمين بجهاد أعدائهم والإثخان بهم بطريقة تسمى العمليات الاستشهادية .. وهذه العمليات هي ما يفعله المجاهدون من إحاطة أحدهم بحزام من المتفجرات، أو ما يضع في جيبه أو أمتعته أو سيارته بعض القنابل المتفجرة ثم يقتحم تجمعات العدو ومساكنهم ونحوها ، أو يظهر الاستسلام لهم ثم يقوم بتفجير نفسه بقصد الشهادة ومحاربة العدو والنكاية به .

فما حكم مثل هذه العمليات ؟ وهل يعد هذا الفعل من الانتحار ؟ وما الفرق بين الانتحار والعمليات الاستشهادية ؟ جزاكم الله خيرا وغفر لكم ..

الجواب ..

الحمد لله رب العالمين والصلاة والسلام على أشرف الأنبياء والمرسلين نبينا محمد وعلى آله وصحبه أجمعين أما بعد

قبل الإجابة على هذا السؤال لابد أن تعلم أن مثل هذه العمليات المذكورة من النوازل المعاصرة التي لم تكن معروفة في السابق بنفس طريقتها اليوم ، ولكل عصر نوازله التي تحدث فيه ، فيجتهد العلماء على تنـزيلها على النصوص والعمومات والحوادث والوقائع المشابهة لها والتي أفتى في مثلها السلف، قال تعالى: (ما فرطنا في الكتاب من شيء) وقال عليه الصلاة والسلام عن القرآن : (فيه فصل ما بينكم)، وان العمليات الاستشهادية المذكورة عمل مشروع وهو من الجهاد في سبيل الله إذا خلصت نية صاحبه وهو من انجع الوسائل الجهادية ومن الوسائل الفعّالة ضد أعداء هذا الدين لما لها من النكاية وإيقاع الإصابات بهم من قتل أو جرح ولما فيها من بث الرعب والقلق والهلع فيهم، ولما فيها من تجرئة المسلمين


D:\fatwa\Files\Fedai\print_article_105.shtml

حكم العمليات الاستشهادية .... للشيخ / حامد العلي

أرسل هذه الصفحة لصديقك
اطبع هذه الصفحة

الحمد لله والصلاة والسلام على نبينا محمد وعلى آله وبعد :

يجد الناظر في مسألة حكم اقتحام المجاهد على العدو إذا كان لايرجو نجاة ، يجدها تنقسم إلى قسمين ، غير أنهما يندرجان تحت حكم واحد بحســـــــب الاستدلال والنظر ، كما سيتبين إن شاء الله :

أما أحد القسمين : فهو حكم الإقتحام على العدد الكبير من الأعداء إذا علم أنهم سيقتلونه لامحاله ، لأن فرصة النجاة تكاد تكون معدومة ، كأن يحمل على ألف من الأعداء فينغمس فيهم وحده ، ومـــــــــــــن صوره العصرية أن يدخل في معسكر للأعداء لعملية تفجير وهو يعلم أن احتمـــــــال الخروج من المعسكر معدوم لأن التدابير الأمنية محكمة ، وبسبب كثرة الجند والحرس مثلا ، غير أنه في هذه الحالـــــــــــــــة تكون مباشر القتل مـــــــــــن الأعداء فهم الذين يباشرون قتله ، لا من نفسه ، لكنه كان السبب غير المباشـــــر في قتل نفسه لأنه اقتحم بها إلى موضع يعلم أنه سيقتل فيـــــــه ، غير أنه فعل ذلك لأنه لاسبيل في هذه المثال إلى إحداث التفجير في ذلك المعسكر إلا بإدخال عنصر بشري إلى داخله 0

وأما الثاني فهو : حكم مباشرة المجاهد قتـــــــل نفسه إذا علم أن ذلك سيؤدي إلى أن يقتل معه عددا كبيرا من الأعداء ، ولايمكنه قتلهم بلا قتل


D:\fatwa\Files\Fedai\print_article_115.shtml

العمليات الاستشهادية

الكاتب: الشيخ سلمان بن فهد العودة

أرسل هذه الصفحة لصديقك
اطبع هذه الصفحة

مختارات

- حكم العمليات الاستشهادية .... للشيخ / حامد العلي
- فتوى الشيخ حمود بن عقلاء الشعيبي في العمليات الاستشهادية

الشيخ سلمان العودة حفظه الله .. آمين

السلام عليكم ورحمة الله وبركاته ..

فضيلة الشيخ كثر الحديث والجدل حول العمليات الإستشهادية ,وأقيمت ندوات وحوارات وكتبت مقالات وطبعت نشرات ..مابين مؤيد ومعارض ومتحمس ومندفع ومتحفظ ومتردد...ولكلٍ آرائه وأنصاره .. وأصبحنا نرى ونسمع العجب..!! وفي هذه الأيام صدرت أقوال من بعض أهل العلم كان لها ماكان من أثر .... فضيلة شيخنا الكريم نرجوا منكم وفقكم الله وأعانكم أن توضحوا لنا ما يلي :-

1ـ الحكم في هذ المسألة على ضوء الكتاب والسنة وأقوال سلف الأمة رحمهم الله تعالى

2ـ حدود ومجال تنفيذها بمعنى هل تكون ضد الكفار في بلادهم فقط أو تكون ضدهم خارج حدودهم في بلاد لهم نفوذ ومصالح فيها ؟

3ـ هل تقام ضد الأهداف العسكرية فقط أو على كل مايؤثر على العدو ؟!

4ـ هل تشمـــــــــل المدنيين أو الحربيين فقط ؟؟

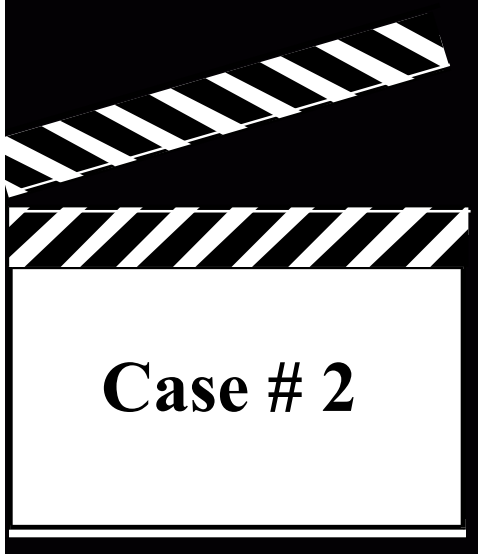
5ـ حد الاثخان فمتى ..فاذا كان المقصود بعد العملية ,حال واحد ولكنه مع القسنة للعدو كأن يكون قائداً كبيراً مثلاً أو دار حةً ...بخلاف لو كان

WS_FTP.LOG

```
2001.05.14 10:01 B C:\Inetpub\wwwroot\alasr\Files\Fedai\article_115.shtml --> ftp.alasr.ws
/home/alasr/www/alasr/Files/Fedai article_115.shtml
2001.05.15 01:13 B C:\Inetpub\wwwroot\alasr\Files\Fedai\article_103.shtml --> ftp.alsunnah.net
/alasr/Files/Fedai article_103.shtml
2001.05.15 01:13 B C:\Inetpub\wwwroot\alasr\Files\Fedai\article_104.shtml --> ftp.alsunnah.net
/alasr/Files/Fedai article_104.shtml
2001.05.15 01:13 B C:\Inetpub\wwwroot\alasr\Files\Fedai\article_105.shtml --> ftp.alsunnah.net
/alasr/Files/Fedai article_105.shtml
2001.05.15 01:13 B C:\Inetpub\wwwroot\alasr\Files\Fedai\article_115.shtml --> ftp.alsunnah.net
/alasr/Files/Fedai article_115.shtml
2001.05.15 01:13 B C:\Inetpub\wwwroot\alasr\Files\Fedai\index.shtml --> ftp.alsunnah.net
/alasr/Files/Fedai index.shtml
2001.05.15 01:13 B C:\Inetpub\wwwroot\alasr\Files\Fedai\index_article.shtml --> ftp.alsunnah.net
/alasr/Files/Fedai index_article.shtml
2001.05.15 01:13 B C:\Inetpub\wwwroot\alasr\Files\Fedai\index_audio.shtml --> ftp.alsunnah.net
/alasr/Files/Fedai index_audio.shtml
2001.05.15 01:13 B C:\Inetpub\wwwroot\alasr\Files\Fedai\nav.html --> ftp.alsunnah.net
/alasr/Files/Fedai nav.html
2001.05.15 01:13 B C:\Inetpub\wwwroot\alasr\Files\Fedai\print_article_103.shtml -->
ftp.alsunnah.net /alasr/Files/Fedai print_article_103.shtml
2001.05.15 01:13 B C:\Inetpub\wwwroot\alasr\Files\Fedai\print_article_104.shtml -->
ftp.alsunnah.net /alasr/Files/Fedai print_article_104.shtml
2001.05.15 01:13 B C:\Inetpub\wwwroot\alasr\Files\Fedai\print_article_105.shtml -->
ftp.alsunnah.net /alasr/Files/Fedai print_article_105.shtml
2001.05.15 01:13 B C:\Inetpub\wwwroot\alasr\Files\Fedai\print_article_115.shtml -->
ftp.alsunnah.net /alasr/Files/Fedai print_article_115.shtml
2001.05.15 01:13 B C:\Inetpub\wwwroot\alasr\Files\Fedai\WS_FTP.LOG --> ftp.alsunnah.net
/alasr/Files/Fedai WS_FTP.LOG
```

Computer Forensics at work

Bombing / Extortion



The Crime . . .

- 9/22/99 at 5:44 p.m. a pipe bomb detonated at Lowe's Home Improvement Warehouse, Salisbury, N.C.

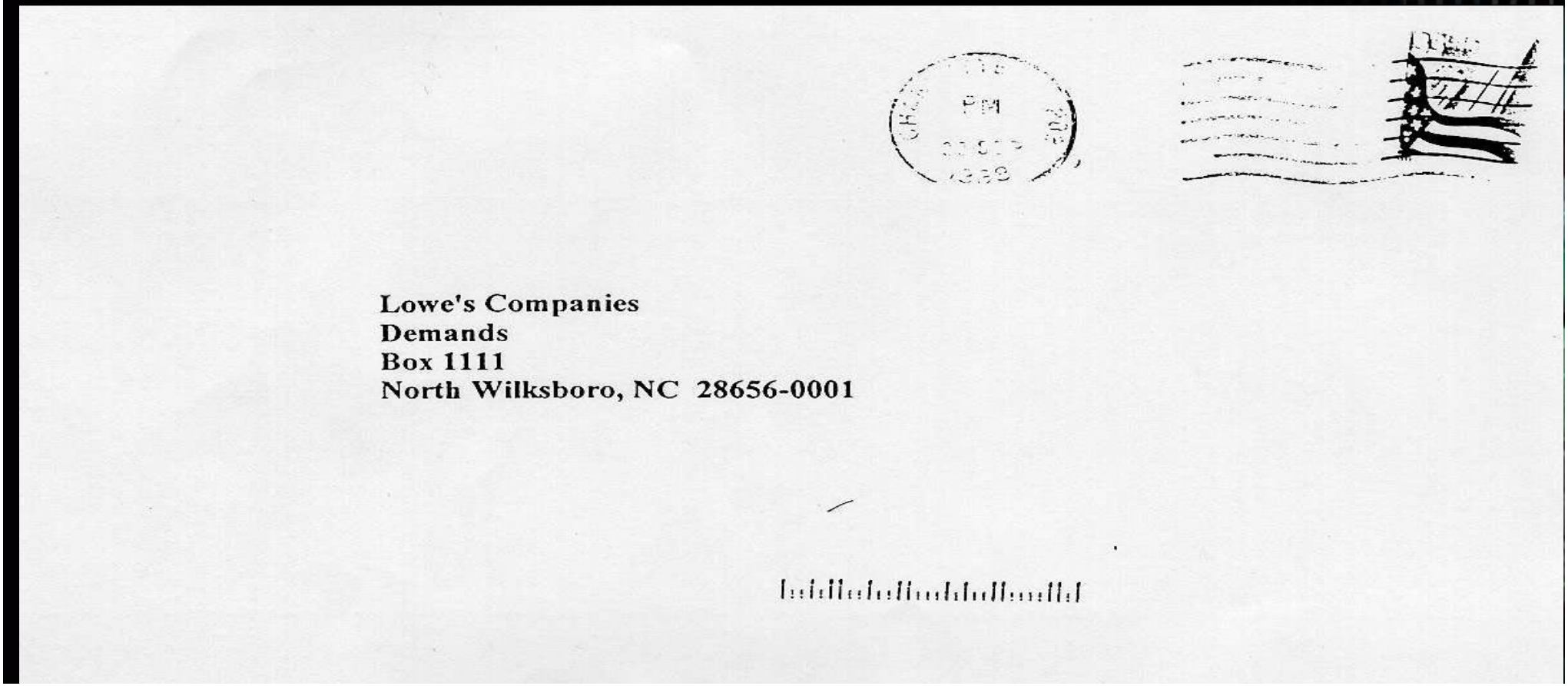

LOWE'S

Another Crime . . .

- 9/22/99 at 5:52 p.m. another pipe bomb detonated at another Lowe's Home Improvement Warehouse, Asheboro, N.C.

Lowe's receives demands . . .

- 9/23/99 - Two separate and identical letters were received at Lowe's Headquarters in Wilkesboro, N.C.



Lowe's Companies

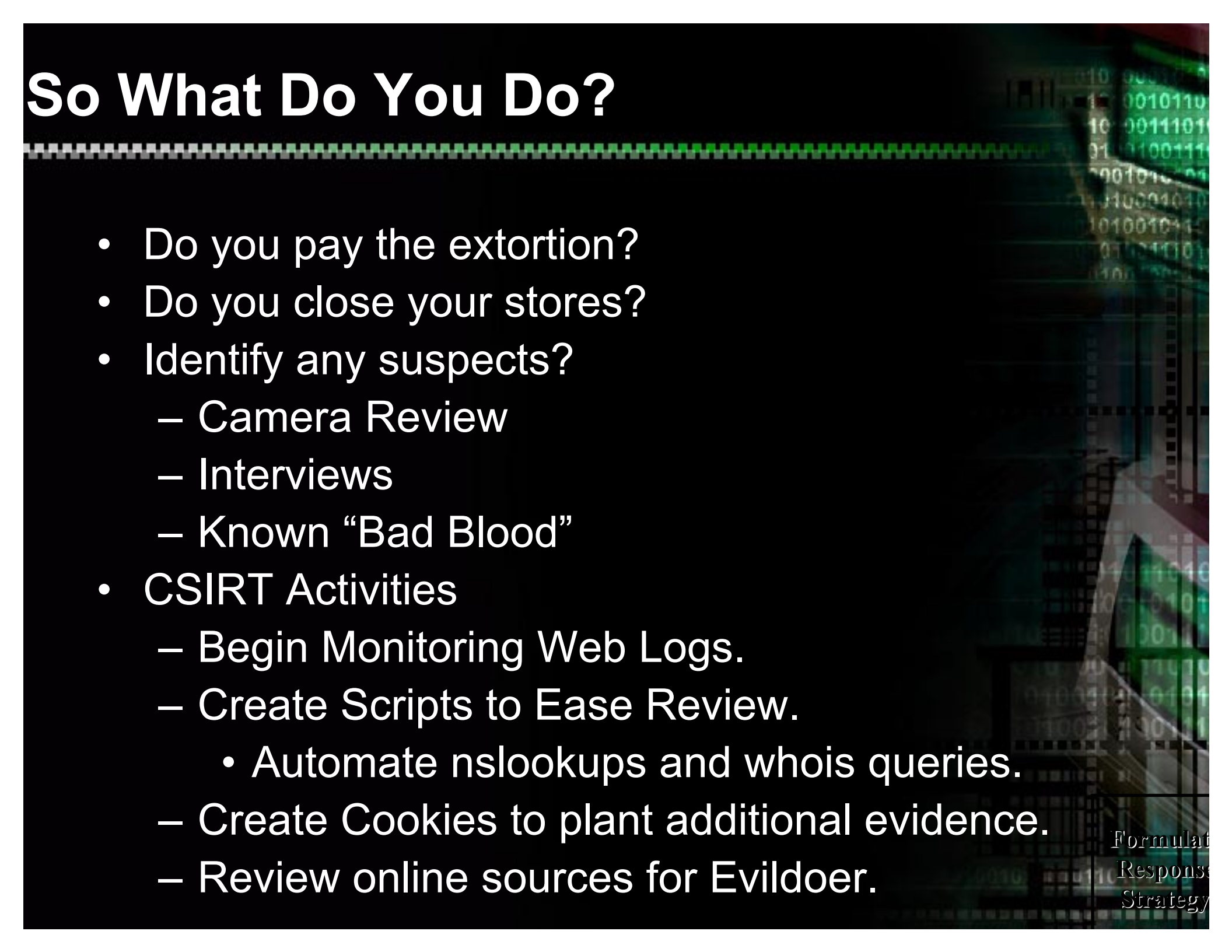
I have been forced to take drastic measures due to the lack of help for two of my friends. At the lowe's motor speedway you killed many people and hurt many more. Since the speedway refuses to help my friends I must resort to other measures.

I will keep bombing your 500 stores until you pay $250,000.00 . If you don't agree I am very sure your business will drop off greatly. I have your red aprons and vests and will be able to get in and out of your stores without much trouble.

When you decide to pay the money, let me know by putting "Ready to meet demands" on the bottom of your WWW/Lowes.com home page under where it says "Please review our privacy/security information and terms of use", at that tim I will stop the pipe bombs and make arrangements to be paid

So What Do You Do?

- Do you pay the extortion?
- Do you close your stores?
- Identify any suspects?
  - Camera Review
  - Interviews
  - Known “Bad Blood”
- CSIRT Activities
  - Begin Monitoring Web Logs.
  - Create Scripts to Ease Review.
    - Automate nslookups and whois queries.
  - Create Cookies to plant additional evidence.
  - Review online sources for Evildoer.



Only communication with bomber – Lowe's homepage

- 9/24/99 - Lowe's placed "Will meet your demands." on the bottom of their homepage

Good Morning !

Help Can't Wait

Please join the American Red Cross and Lowe's Home Improvement Warehouse in helping victims of Hurricane Floyd. **Contribute to the American Red Cross Disaster Relief Fund**. Lowe's customers have demonstrated their generosity by already donating $275,000 to Red Cross Disaster Fund collection sites in stores in the Carolinas and Virginia. 'We're proud to work side-by-side with Lowe's to help residents recover from Hurricane Floyd,' said Joe Fay, acting vice president of Marketing at the American Red Cross. 'It's thanks to the support of companies like Lowe's that the Red Cross is able to be there for the people who have been so hard hit by disasters like Hurricane Floyd.' **Read more about the relief efforts**.

Featured How-To's:

How to Highlight Your Home's Decor with Lighting
Learn how to use lighting to enhance the look of your home. Find lighting ideas for every room in this how-to.

How to Renew the Look of Stucco
Is your stucco fading or cracking? Learn how to repair the surface and protect it with a fresh coat of paint.

How to Install Undercabinet Lighting
Don't prepare food under shadowy cabinets--under-cabinet lighting is simple to install.

Quick Tips

Fall is the best time to plant trees that have been machine-burlapped or container-grown. Take advantage of this planting time so your new trees will be ready to burst forth with spring growth. Need more tips on planting trees? Click here.

Web Access Logs

```
#Software: Microsoft Internet Information Server 4.0
#Version: 1.0
#Date: 1999-09-24 15:35:44
#Fields: time c-ip cs-method cs-uri-stem sc-status
15:35:44 146.11.21.13 GET /Default.asp 200
15:35:44 146.11.21.13 GET /iissamples/default/SQUIGGLE.GIF 200
15:35:44 146.11.21.13 GET /iissamples/default/MSFT.GIF 200
15:35:44 146.11.21.13 GET /iissamples/default/IISTitle.gif 200
15:35:44 146.11.21.13 GET /iissamples/default/nav2.gif 200
15:35:44 146.11.21.13 GET /iissamples/default/IE.GIF 200
15:35:44 146.11.21.13 GET /iissamples/default/IISSide.GIF 200
```

Look for IP Addresses in the NC Area

Another bomb is located . . .

- 9/28/99 at 3:00 p.m. - an unexploded pipe bomb was located in the paint department at the Lowe's Home Improvement store in Concord, N.C.

Analysis of bombs revealed no leads . . .

- No fingerprints were found
- Readily available components
- Only 1 pubic hair found in tape on bomb

More instructions . . .

- 11/9/99 at 3:00 p.m. - Two separate and identical letters were received at Lowe's Headquarters in Wilkesboro, N.C.

BOMBING DEMANDS

Gentlemen:

I would just like to clarify a few things and give you instructions for the transfer of monies. I had nothing to do with the fires in your other stores. I did place the third pipe bomb in your store but it was not turned on. I was going to turn it on if you didn't agree to my terms. At this time there are no other bombs in any of your stores, I have not called in any bomb threats anywhere.

Enclosed is the bank information to make a wire transfer in the amount of 250,000.00 as agreed. This is to be done Tuesday or Wednesday of this week. The funds should received by the end of the week in this account. If not I will start the bombings again. Also, if **anyone** tries to tamper with this account (FBI etc.) and close it or seize the funds, I will resume the bombings. This account has nothing to do with me and is not traceable back to me. It is a Panamanian Corporation. For your own good pay the monies and don't get the FBI or ATF involved. It is getting close to the busiest time of the year in your stores and if there are any problems I will start again.

When the funds have been sent please underline the last line of your privacy statement on the bottom of your homepage on the internet, leave it there for a week and then remove it.

CORRESPONDENT ACCOUNT
for payments in USD

AMOUNT	_____
BENEFICIARY NAME	**NPC**
BENEFICIARY ADDRESS	
BENEFICIARY ACCOUNT NUMBER	**0000 3291 1241**
BENEFICIARY BANK NAME	**PARITATE BANK**
BENEFICIARY BANK ADDRESS	**4 Terbatas Street, Riga, Latvia**
INTERMEDIARY BANK NAME	**SVENSKA HANDELSBANKEN**
INTERMEDIARY BANK ADDRESS	**Stockholm, Sweden** **SWIFT HAND SE SS**
BENEFICIARY BANK ACCOUNT NUMBER	**99-47 848 979**
DETAILS OF PAYMENT	**ANY**

Lowe's again complies . . .

- On 11/11/99, Lowe's wire transfers $250,000.00 to the Paritate Bank as directed

- Lowe's underlined the last line of the privacy statement on the bottom of their homepage

Paritate Online Banking

- Can be initiated with online request
- Paritate bank required:
  - physical address to which signature cards were to be mailed
  - Cards must be notorized
  - Corporate Account agreement also snail mailed
  - Must install a client software for remote banking
- Account cost $250.00 U.S. dollars to setup

Extortion bank account created . .

- Created online in the name of Bruce Phillips
- Phillipps' address was 399 Peters Creek Parkway, Winston Salem, N.C.
  - Address belonged to a Dunkin Doughnuts
  - Paritate Fed X package delivered and signed for here
- Paritate Bank received e-mail correspondence from brucephillips99@hotmail.com requesting Fed X tracking number for package

What Computer Evidence Do We Have??

- SUBJECT Used Hotmail
- On Subjects Machine
  - Cookies?
  - Account Name in Slack?
  - History … Bookmarks … Cache?
- On Hotmail Servers
  - When the brucephillips99@hotmail.com account is accessed
  - What IP Addresses Use the Account
  - Any IP's Same as the Ones on Lowe's Web Servers???

"Bruce Phillips" <brucephillips99@hotmail.com>

01.11.99 23:43

To: agnese@paritate.lv

cc:

Subject: new account

A. Kasparova:

Thank your for your quick service opening this account. You informed me that the opening documentation was sent out fedex on 01 November 1999. If at all possible can you supply me with the tracking number? Thank you.

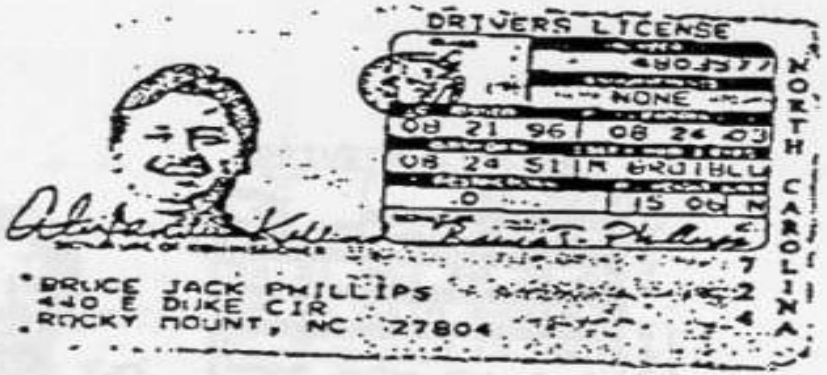
Bruce. Phillips

brucephillips99@hotmail.com

Account #0000-3291-1241

Fake identities continue . . .

- Signature card from Paritate Bank had to be notorized for the foreign bank account



NOTARIZED COPY 10/22/99

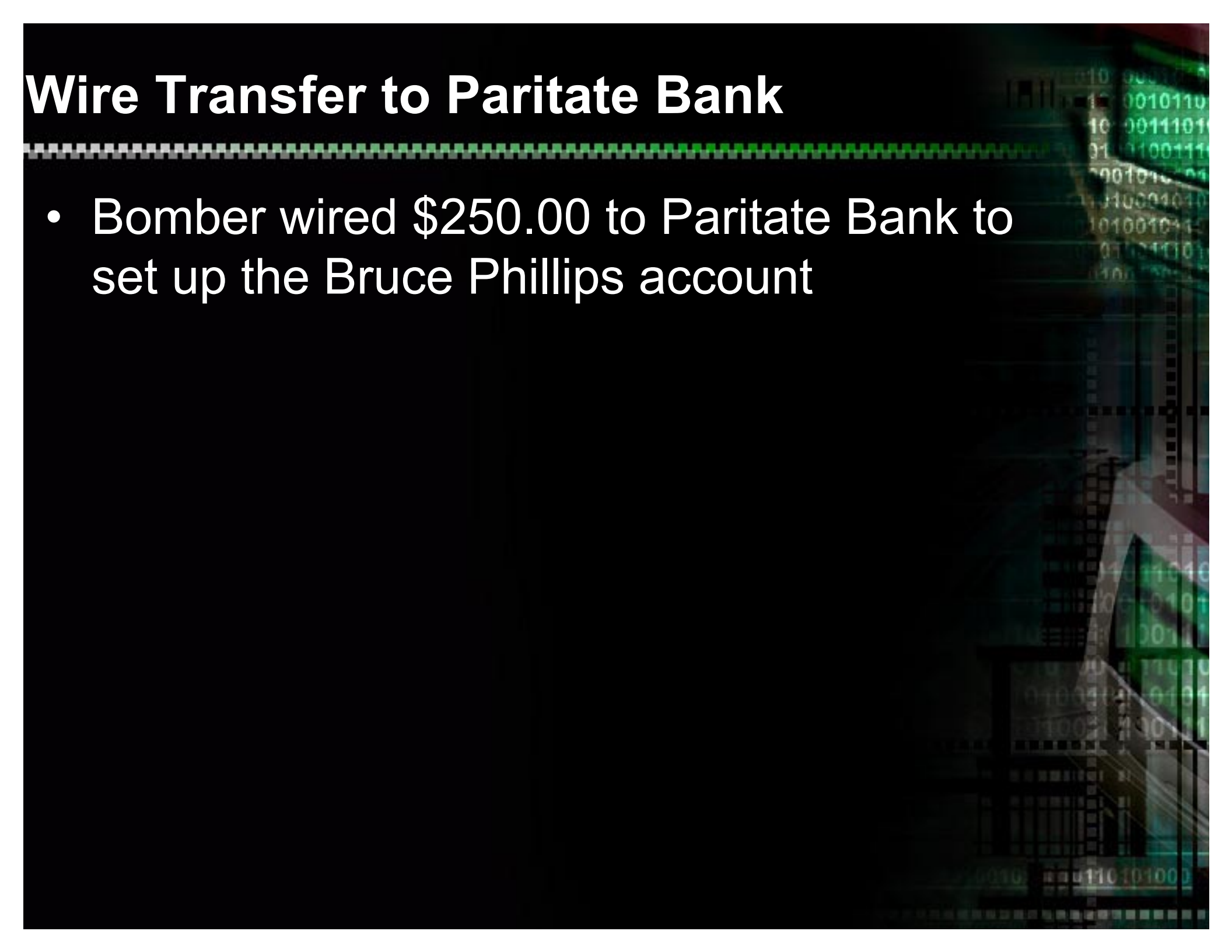
JOHN V. PEILAN.
Notary Public
Guilford County
State of North Carolina
My Commission Expires Feb. 22, 2003

John V. Peilan

NOTARY PUBLIC

Wire Transfer to Paritate Bank

- Bomber wired $250.00 to Paritate Bank to set up the Bruce Phillips account



To send a Quick Collect® payment

WESTERN UNION | QUICK COLLECT℠

The fastest way to make a payment.℠

Dollar amount in words: Two hundred fifty

Dollar amount (Not to exceed $5,000): $250.00

If sending $3,000 or more, you must provide valid I.D. and your social security number.

Pay to: Paritate Bank (Company name)

Code City: Paritate, La State: La

Sender's name: Steve A Boyd

Sender's telephone (area code): 336 number: 456-2944

Sender's address: 3620 Clemmons Rd (Street)

City: Clemmons State: NC Zip: 27012

Sender's account number with company: 000-3295-0004

Reference number: P2A - 3049

Attention: Paritate Corp

Customer's signature: Steve A. Boyd

BY SIGNING, THE SENDER ACKNOWLEDGES AN UNDERSTANDING OF THE TERMS AND CONDITIONS OF THIS CONTRACT.

Do not write in shaded area

Agency

Operator number

Time Date 1/11 19

Sent time Date / /

I.D. Type Number

Social Security No.

Money Transfer Control Number: 4048231594

Amount: 250.00

Charge: 15.00

Tax

Total amount received: 265.00

Agent's signature: DC

FSI 9030 (R11/96)

Bomber Needs to Install Software

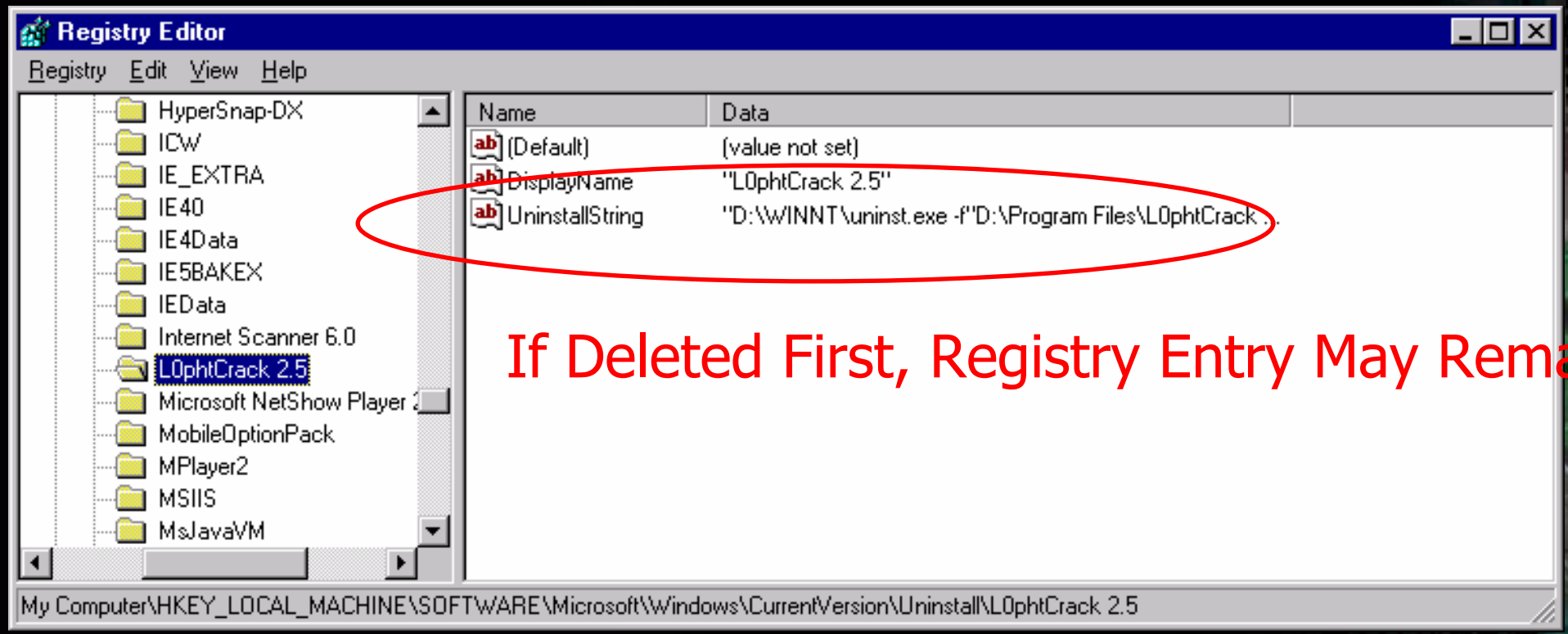
- In order to use an Online Bank Account at Paritate, you must run software that they mail to you on a floppy disk.

What Computer Evidence Do We Have??

- SUBJECT Installed Software
- Subjects Machine
  - Registry Entries
  - Presence of the Paritate Bank Software
- Paritate Bank
  - Perhaps IP Address
  - What else can they get??

Traces of Installed Programs

Remnants of Installed Programs Deleted Improperly



If Deleted First, Registry Entry May Remain

Bomber Needs to Install Software

- During the installation of the client software for remote online banking, information from the bomber's hard drive was transmitted to Paritate bank without his knowledge
- A text file was created on the Latvian bank's computer which actually revealed the bomber's true identity

Npc.txt

```
Client-Bank installed!
Date: 11/07/99 23:14:39
MailBox: NPC
Company:
Owner: George M. Rocha
CLW32.WZD product version 3.32.2.6
CLW32.BIN product version 3.32.3.4
Volume name:
Volume SerialNo = $253C16F2
Run mode: FULL
```


Let's Not Forget About the Hotmail Account

Net Force aka Cyber Swat is called in . . .

- 2703(d) court order was served on Hotmail in California
- Received information only of the Internet Protocol Addresses which accessed the e-mail account

key	value	description
login	brucephillips99	the name of the Hotmail account
lname	Phillips	last name
fname	Bruce	first name
country	US	n/a
zip	27804	n/a
timezone	America/New_York	n/a
maildomain	hotmail.com	n/a
Headers	basic	how message headers are viewed by the user
UserDefinedReplyTo	No	n/a
gender	male	n/a
regfromip	198.85.26.106	the Internet Protocol address the account was registered from
age	1979	n/a
PpBirthday	29101	n/a

** Not every field may appear in your report.*
This data was provided to us by the user,
and Hotmail does not make any representations
regarding its authenticity.

ame.space
dot everything people™

Name.Space

SWHOIS Search

Smart Whois Query Result from: **whois.arin.net**

ome
boul
vitch
nage
vare
w to
ress
olicy
law
faq
imin
arch
ntact
ices
new
ntlds
vote

CONCERT Network (NETBLK-CONCERT-CIDR2) NETBLK-CONCERT-CIDR2
198.86.0.0 - 198.86.
Greensboro Public Library (NET-GPL1) GPL1 19

To single out one record, look it up with "!xxx", where xxx is the handle, shown in parenthesis following the name, which comes first.

The ARIN Registration Services Host contains ONLY Internet Network Information: Networks, ASN's, and related POC's. Please use the whois server at rs.internic.net for DOMAIN related Information and nic.mil for NIPRNET Information.

Smart Whois Search:
Enter Domain Name, IP Number, or Handle

12 198.86.22.146 sWhois

IP	Time{PST}	Date	Pass/Fail [successful(pass) and failed(fail) authentication]
198.86.22.212	09:05:38	11/10/99	pass
198.86.22.153	10:08:28	11/9/99	pass
198.86.22.153	07:34:02	11/8/99	pass
198.86.22.146	08:16:55	11/5/99	pass
198.85.108.103	09:38:04	11/4/99	pass
216.78.172.148	07:51:36	11/2/99	pass
216.78.172.148	07:42:30	11/2/99	pass
216.78.172.148	13:26:45	11/1/99	pass
216.78.172.148	13:25:44	11/1/99	pass
216.78.172.148	13:13:04	11/1/99	pass
216.78.172.148	12:46:50	11/1/99	pass
216.78.172.148	05:27:59	11/1/99	pass
216.78.172.148	14:33:22	10/31/99	pass
216.78.172.148	08:01:24	10/31/99	pass
216.78.172.148	22:53:34	10/30/99	pass
216.78.172.148	22:52:10	10/30/99	pass
216.78.172.148	06:48:39	10/30/99	pass
216.78.172.148	06:21:26	10/29/99	pass
216.78.172.148	11:05:12	10/28/99	pass
216.78.172.148	06:33:55	10/28/99	pass
216.78.172.148	18:11:20	10/27/99	pass
216.78.172.148	07:29:14	10/27/99	pass

name.space
the dot everything people™

Name.Space

SWHOIS Searc

Smart Whois Query Result from: **whois.arin.net**

home
about
switch
manage
software
how to
press
policy
law
faq
admin
search
contact
services
new gtlds
vote

```
BellSouth.net Inc. (NETBLK-BELLSNET-BLK5)
   1100 Ashwood Parkway
   Atlanta, GA 30338

   Netname: BELLSNET-BLK5
   Netblock: 216.76.0.0 - 216.79.255.255
   Maintainer: BELL

   Coordinator:
      Muir, Ronald  (RM36-ARIN)  ipadmin@BELLSOUTH.NET
      770-522-6363 (FAX) 770-522-6050

   Domain System inverse mapping provided by:

NS.BELLSOUTH.NET                205.152.0.5
NS.ATL.BELLSOUTH.NET            205.152.0.20

   ADDRESSES WITHIN THIS BLOCK ARE NON-PORTABLE

   Record last updated on 06-Apr-1999
```

Subject Checked Hotmail e-mail

Monday, October 4
- 12:13 p.m. Forsyth MIS (library-2-whizzer.co.forsyth
- 12.14 p.m. Forsyth MIS

Wednesday, October 6
- 11:03 a.m. Greensboro Public Library
- 11:07 a.m. Greensboro Public Library
- 11:31 a.m. Greensboro Public Library

Thursday, October 7
- 10:57 a.m. Greensboro Public Library

Friday, October 8
- 9:14 a.m. gso.bellsouth.net
- 10:36 a.m. gso.bellsouth.net
- 11:30 a.m. gso.bellsouth.net
- 2:04 p.m. gso.bellsouth.net
- 3:18 p.m. gso.bellsouth.net
- 7:17 p.m. gso.bellsouth.net
- 10:46.p.m. gso.bellsouth.net

Saturday, October 9
- 9:40 a.m. gso.bellsouth.net
- 9:15 p.m. gso.bellsouth.net
- 9:47 p.m. gso.bellsouth.net

Hotmail account analysis

- The IP numbers were traced back to the Forsyth County Public Library, Greensboro Public Library and the Bellsouth Network

- A “whois” revealed who to serve the next 2703(d) order upon

BellSouth.net Response

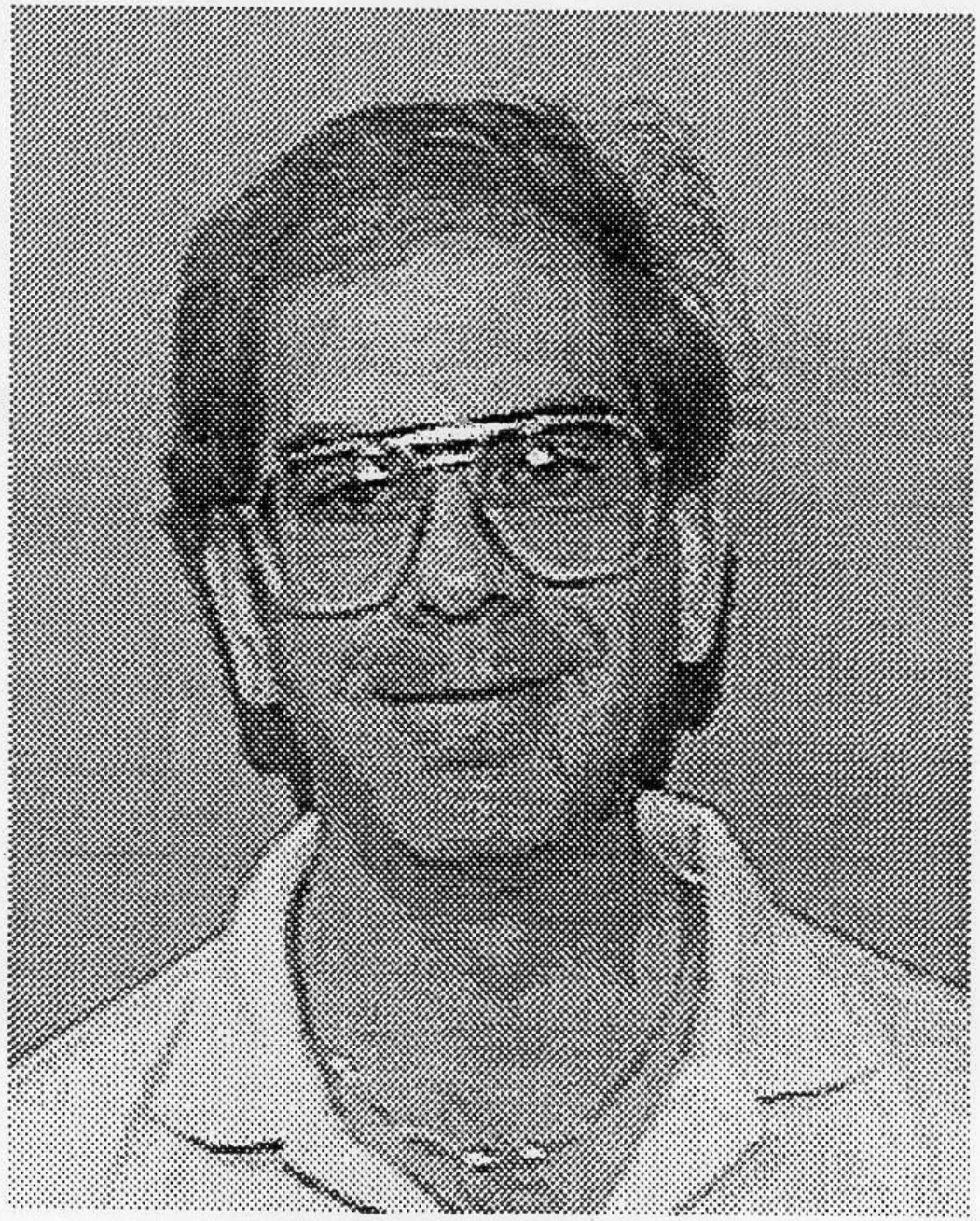
- Had Caller ID on the network modems
- Had some direct dialups from a modem
- Subscriber was:
  - George Rocha
    - 4246 Princeton Avenue
    - Greensboro, NC 27407
    - 336-854-5974

Record Checks

- DMV photo obtained
- Criminal history checked
  - Arrested by Greensboro PD for obtaining property under false pretenses at Lowe's Home Improvement stores
- Utility checks confirm Rocha is subscriber at 4246 Princeton Avenue
  - Power
  - Telecommunications

Image Storage Date: 8/13/99 2:59:40 PM

Portrait:



Signature:

Need physical world validation of cyber information . . .

- Western Union employees confirmed Rocha was the individual who sent the wire

Investigation Continues . . .

- Surveillance of subject is initiated
- Probation Officer is contacted
- Arrest warrant obtained
  - Taken into custody on 11/12/99
- Search warrant obtained
  - Conducted of house, car, and storage area on 11/12/99

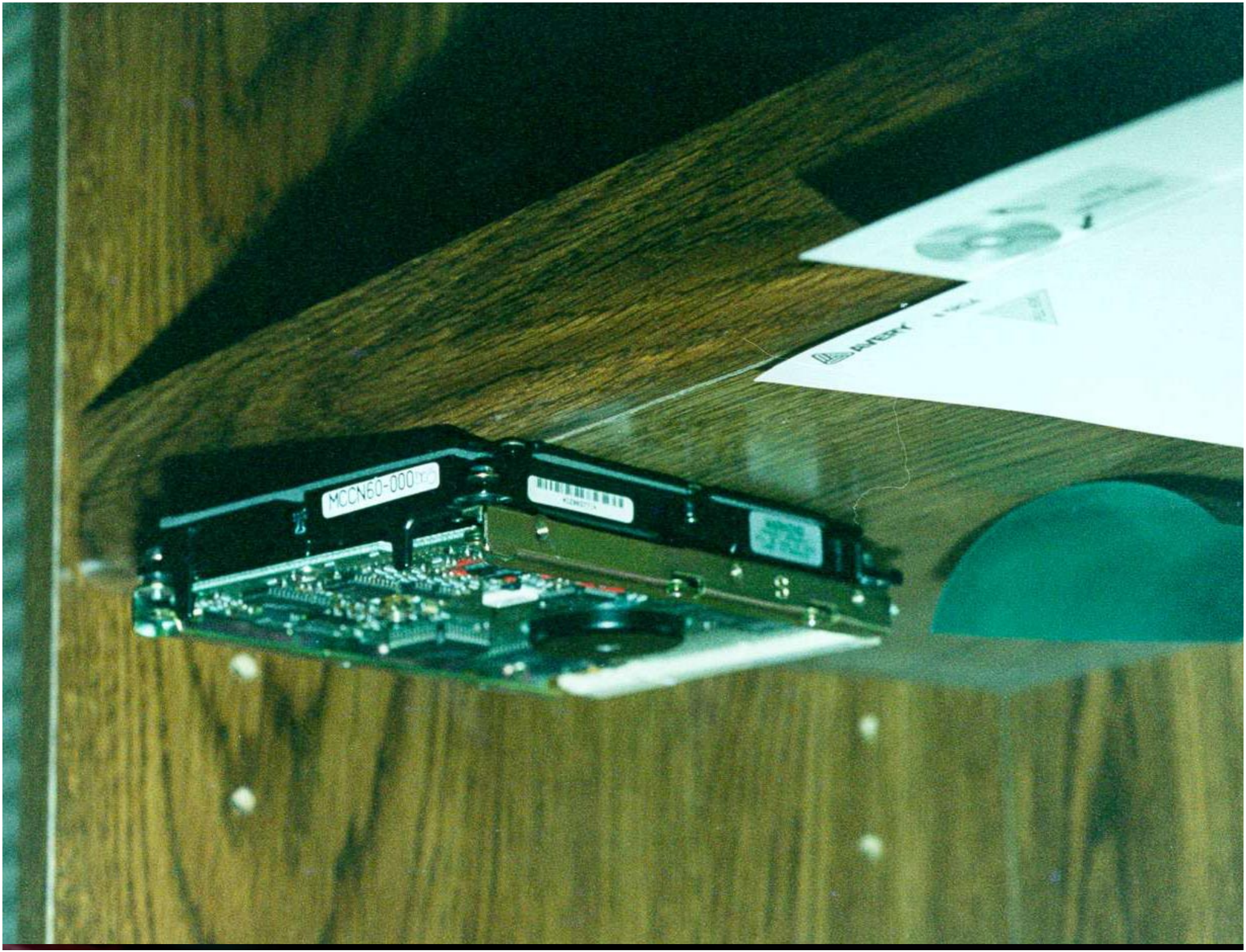
COMPUTER!!!


Let's Grab His Computer!


DeWALT
Belden
WIRECABLE
SK
Series
SK3440

53
53
METRIC


UMAX
Astra 1220S
4020i
HEWLETT
PACKARD
RESET


MCCN60-000


12
EVI-PAQ™ (800) 377-0450 Patent Pending
Maxtor
Manufacture Date: 02-28-98
Made in Singapore
S/N L41413AA
N.M.B
A 33
12V
5V

Computer Forensics at work

- Forensic examination of hard drive revealed hotmail email fragments and Internet History showing he had visited Lowe's website several times during the time of the bombings
- Confirmed software from bank was installed
- Serial number of volume matched data sent to bank

```
Volume name:
Volume SerialNo = $253C16F2
Run mode: FULL
```

Computer Forensics at work

Sutphen Case

Autopsy says cellist was asphyxiated

Durham cellist Janine Sutphen's decomposed body showed no evidence of injuries, leading a medical examiner to conclude she was asphyxiated, according to an autopsy report released Thursday. The report by Dr. Thomas Clark III, an assistant state medical examiner, says he reached that determination after excluding all other injuries and after being unable to find any suitable specimens to undergo toxicology tests, which can show the presence of alcohol or poisons. Updated: Oct. 23, 2005 3:43 AM | **Full story**

Affidavit show items seized in Sutphen case

A computer system, rope and a green mattress were seized from murder suspect Robert Petrick's townhouse two weeks after his missing wife's body was found in Falls Lake, according to an affidavit filed Friday. The affidavit says Investigator Terry Mikels wanted to search the couple's townhouse at 1304 Seaton Road on June 9 after Janine Sutphen's body was found May 29. She was wrapped in "numerous layers of materials, some of which had been identified by family members" as belonging to Sutphen and kept in her home.
Updated: Oct. 23, 2005 12:56 AM | **Full story**

Case # 3

Computer Forensics at work

- Among the circumstantial evidence against Petrick, analysts discovered that one of his computers was used to research the depth, currents and underwater topography of Falls Lake. Someone also used the computer to visit a now-defunct Web site called "Bloodfest 666" and peruse instructions on "22 Ways To Kill A Man With Your Bare Hands," evidence showed.

- In addition, the terms "rigor mortis" and "body decomposition" were looked up on the computer, a prosecution analyst testified.

(Source: http://www.heraldsun.com/durham)

Google: Witness for the Prosecution

Tuesday, December 06, 2005
By Ben Charny

eWEEK.COM

Robert James Petrick, 51, didn't exactly point a Web browser to the Internet search engine Google and type in "how do you kill your wife?"

But he came pretty close, say prosecutors in Durham County, N.C.

Petrick used Google to search the Internet for references to "body decomposition," "rigor mortis," "neck" and "break" in the days before and after he murdered his wife, Janine Sutphen, then dumped her body in a lake, said Durham County assistant prosecutor **Mitchell Garrell**.

By "Googling" his wife's murder, Petrick was inadvertently supporting the prosecutor's time line of events.

Police: Ludwig's computers hold crime plans

Teen charged in killing of girlfriend's parents

Tuesday, November 22, 2005; Posted: 12:31 a.m. EST (05:31 GMT)

LITITZ, Pennsylvania (CNN) -- The images are disturbing: A 14-year-old girl in various stages of undress; two gun-toting young men making plans to break into a house and kill everyone inside.

Source:http://www.cnn.com

According to a court affidavit, police found the images on computers belonging to David Ludwig, the 18-year-old Pennsylvania man charged with shooting his girlfriend's parents and fleeing the state with her.

The affidavit was filed Friday in Lancaster

Detective Christopher Erb, a computer expert, has found nearly 400 pieces of possible evidence, Tobin wrote in the affidavit.

Source:http://www.cnn.com

Other images, besides the ones of Borden, included pictures of Ludwig with family and friends "possessing firearms and swords," the affidavit said.

One video shows the two friends, dressed in dark clothing, entering a room where they handled firearms and ammunition, Tobin said.

The video shows the young men leaving the house with weapons and driving to a house where they are heard planning "an armed forcible entry ... by climbing onto a roof and entering through a dormer window," Tobin says in the document.

The alleged plot was never carried out.

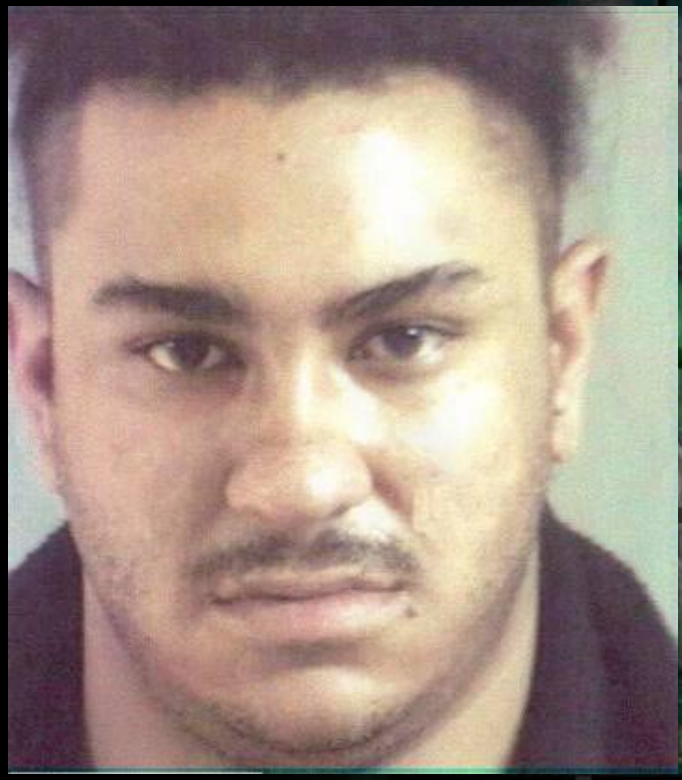
"Ludwig and Lohr talked about using their weapons to shoot and kill family member inside of the residence," the affidavit says.

While the two men walked back to the car, they can be heard discussing having sex with Kara and her 13-year-old sister, Katelyn, and that "the sex would constitute statutory rape and the potential to have to shoot a guy named 'Jonathan' if he found out about it," the affidavit says.

RIVERSIDE COUNTY INTRUSION CASE

People vs. William Grace

& Brandon Wilson



Case # 4

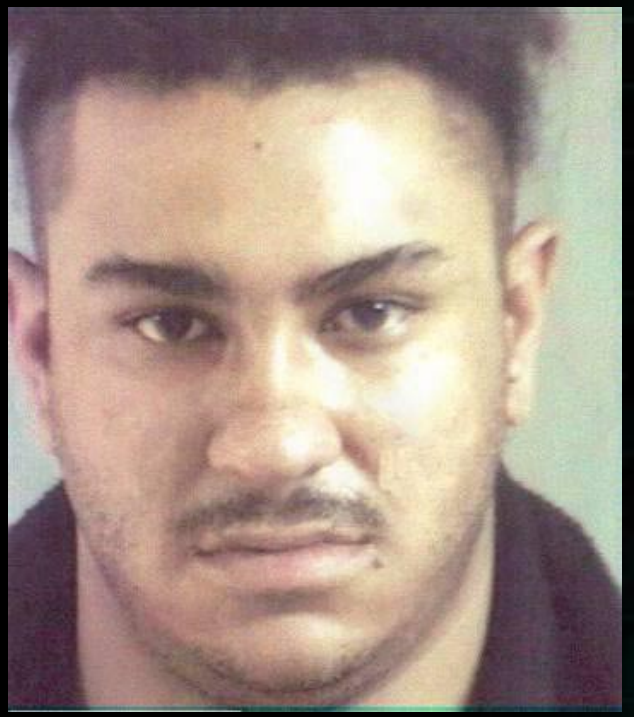
RIVERSIDE COUNTY INTRUSION CASE

WILLIAM GRACE

- 25 year old “anti-social” computer consultant
- Recluse
- Worked odd & end computer jobs, lives paycheck to paycheck.
- No formal computer education.
- Self-taught computer skills.
- Fluent in seven programming languages.
- No Criminal History
- Recognized member of hacking crew known as T.D.U.

RIVERSIDE COUNTY INTRUSION CASE

- BRANDON WILSON
  - 22 year old unemployed collection agent.
  - Good social skills
  - Limited, but above average computer skills
  - Several criminal contacts/arrests for fraud/fake Identification



RIVERSIDE COUNTY INTRUSION CASE

- The two suspects took advantage of host computers visible on the Internet utilizing NetBIOS services and other remotely accessible services to compromise those hosts.

- Once access was gained to those hosts, the suspects were able to “learn” the network topology by probing internal computers that were visible from the compromised computers.

- Once a network topology was acquired, computers of interest were then extensively probed and compromised.

RIVERSIDE COUNTY INTRUSION CASE

COMPUTER FORENSIC AFTERMATH

- 1 Terabyte (1,024,000,000,000 bytes) of disk storage seized
- 400 Gigabytes of digital evidence =
    - 180,000,000 pages of data
    - Stack of paper just over 60,000 feet (11.8 miles) high.
- Over 1,000 computers were found to be compromised.
- Over 21,000 passwords were obtained and cracked by Grace & Wilson.

RIVERSIDE COUNTY INTRUSION CASE

- All effected computers had to be completely wiped clean and rebuilt for data integrity and security.

- Estimated loss & expense to clean up intrusion is just under $1 million dollars.

- Several Web Servers, FTP Servers and other Servers were compromised

RIVERSIDE COUNTY INTRUSION CASE

OTHER IDENTIFIED VICTIMS

- Alameda County was probed
- Paging service company
- Internet Service Provider
- Online Credit Union
- Several other small businesses
- Several thousand personal computers compromised and personal data was located on suspect's computers
- Telephone sex entertainment service – Database contained over 12,000 names, addresses & CC#'s which suspects used.
  - Suspects extorted money from victims threatening public disclosure of entertainment service use.

RIVERSIDE COUNTY INTRUSION CASE

Court records were modified on 72 separate occasions.

Each suspect charged with 219 felony counts of unlawful computer access & altering government records for changing.

An additional 150 felony counts were filed claiming unlawful access to various county computers and obtaining user passwords.

The suspects could have been charged with at least 1000 additional felony counts.

Total exposure for each defendant was 99 years.

Technology & Science

Pair who hacked court get 9 years

Former computer consultant tried to dismiss pending cases

By Bob Sullivan
MSNBC

Feb. 7 — Two hackers who broke into Riverside County, Calif., court computers and electronically dismissed a variety of pending cases pleaded guilty to the crime Friday. Both William Grace and Brandon Wilson were sentenced to nine years in jail after pleading guilty to 72 counts of illegally entering a computer system and editing data, along with seven counts of conspiracy to commit extortion.

JANUARY 2003

Case # 6

THR34T KREW

- January 2003 – Law Enforcement was notified by a company that several computers contained unauthorized software which had been installed by unknown persons.

- Forensic examinations conducted on several computers quickly revealed a worm/trojan program present.

- Monitoring network traffic revealed suspicious outbound traffic.

THR34T KREW

- Worm/Trojan designed to perform four major functions:
  - Self replicate by scanning class A address space looking for IIS machines susceptible to Unicode exploit. If found, exploit and install worm to start same process on new victim.
  - Create a TCP proxy service on the default port of 1297 to allow suspects to use victims as proxies.

THR34T KREW

- Install and configure an FTP server (Serv-U deamon) on default port 65130.

- The most devastating feature – install trojan MIRC program as a service, which constantly attempts an outbound connection to one of seven IRC servers where the victim computer will enter a private, invisible, password protected chat room and remain a drone awaiting commands from suspects.

THR34T KREW

- The MIRC trojan completely compromises the victim computer at the administrator level and allows the suspects to have complete control over the entire computer.

- Once in the chat room, the suspects can enter various “trigger” text which will cause the victim computer to execute various functions locally.

THR34T KREW

- Available commands:
  - !HDSTAT — Hard drive stats
  - !PORTFREE — Available ports
  - !NETSPEED — Net Stats
  - !KILL — Kill process
  - !BNCP — Configure Proxy port
  - !PASSWORD — Change password
  - !SCANSTAT — Scanning stats
  - !BNCCONFIG — Configure Proxy
  - !INFO — Machine info
  - !NETWORK — Network Information
  - !DNS — Perform DNS lookup
  - !VERSION — Version of trojan

THR34T KREW

- DANGEROUS COMMANDS
  - !WEBHIT — Hit website x times
  - !UDP — UDP flood
  - !FIND — find file
  - !FS — Start FTP Server
  - !WWW — Get webpage
  - !DCC — Send/Receive
  - !IISHIT — Hit IIS machine
  - !AROOT — Perform rooting

THR34T KREW

- Two additional features:
  - Perform DDOS attack on Microsoft on each November 11th from 12:00 a.m. to 12:01 a.m.
  - Perform DDOS attack on www.natfront.com every 11th reboot.

THR34T KREW

- Trojan/Worm was hard coded with seven different domain names as the IRC servers for the victims to contact.

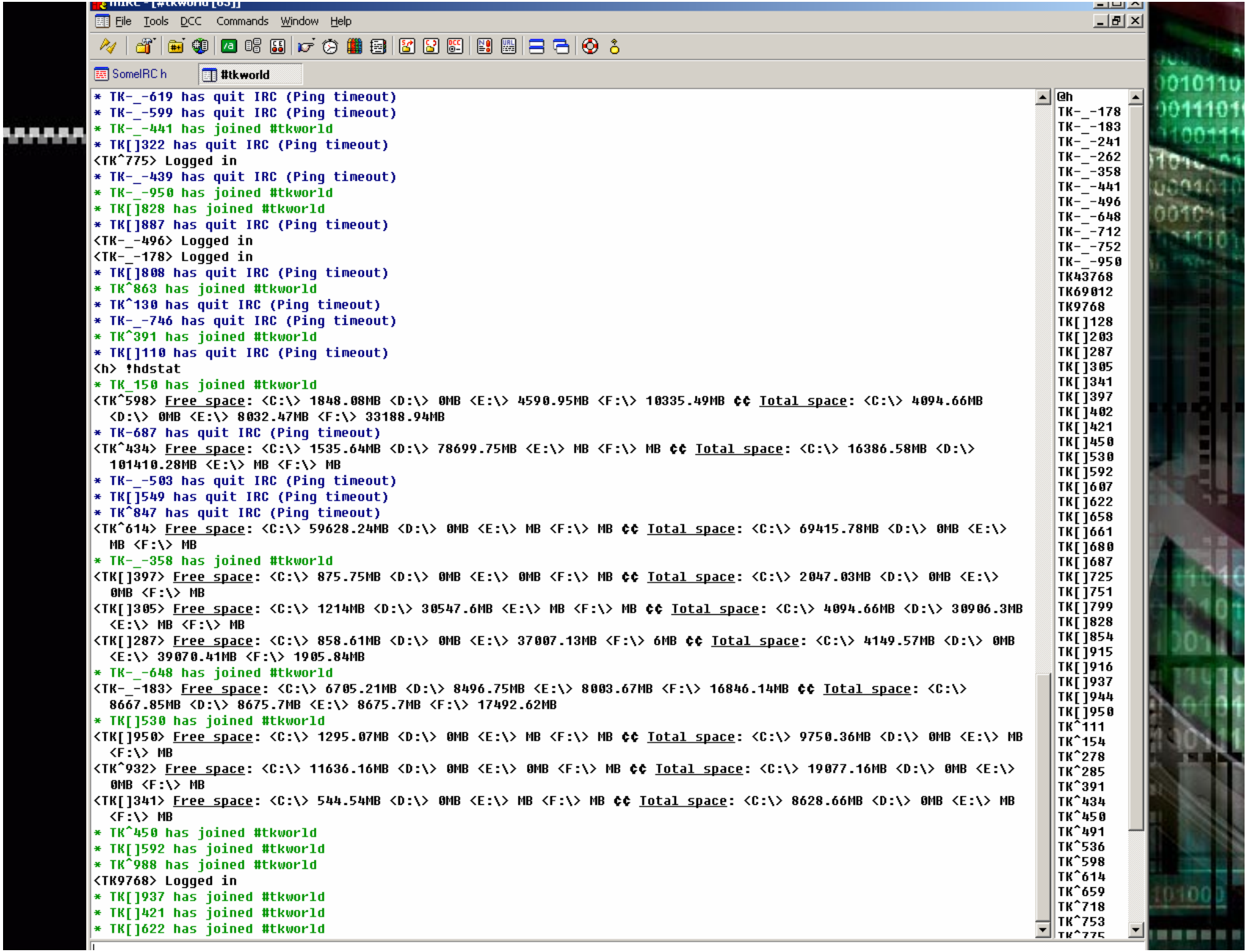
- IRC servers were constantly moved around by the use of a dynamic DNS service which allowed instant DNS updates from a web interface.

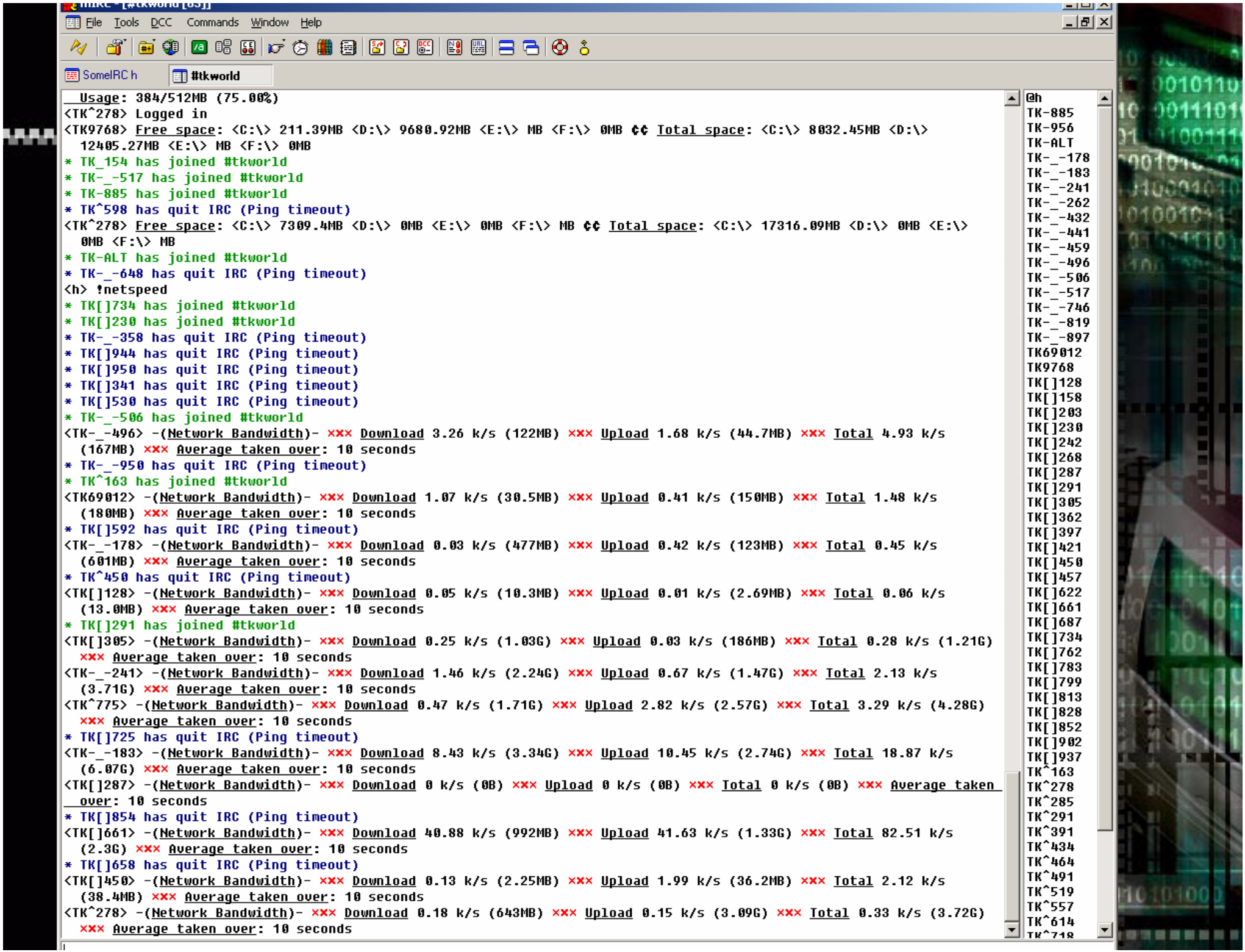
- IRC servers were victim machines that had previously been compromised by the Trojan/Worm.

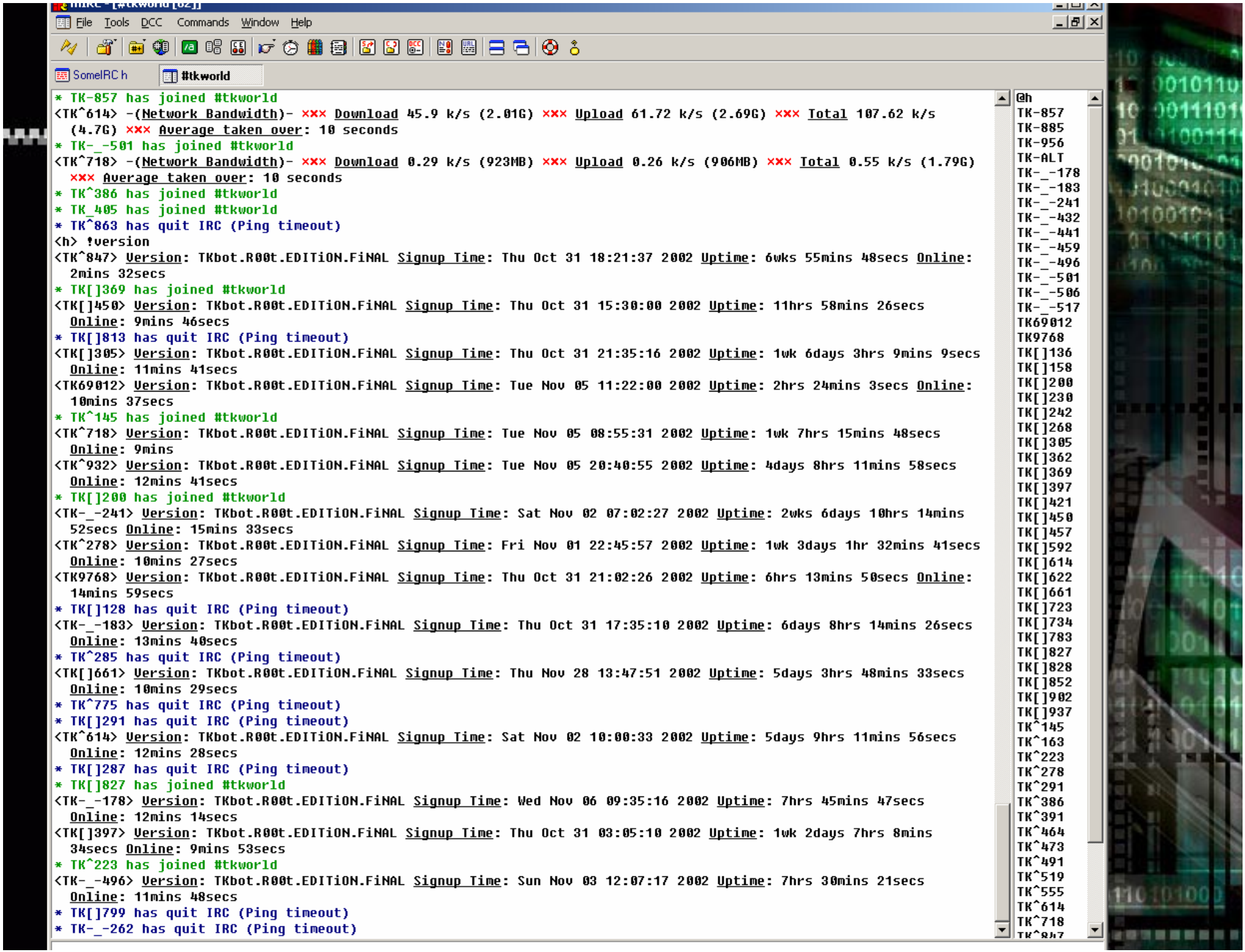
THR34T KREW

- Suspects used publicly available proxies and victim proxies to multi-proxy when connecting to IRC servers and when updating DNS records.

- Following proxy layers backwards and researching email addresses used to register for the DNS service was their downfall.


File Tools DCC Commands Window Help
SomeIRC h
#tkworld
* TK-_-619 has quit IRC (Ping timeout)
* TK-_-599 has quit IRC (Ping timeout)
* TK-_-441 has joined #tkworld
* TK[]322 has quit IRC (Ping timeout)
<TK^775> Logged in
* TK-_-439 has quit IRC (Ping timeout)
* TK-_-950 has joined #tkworld
* TK[]828 has joined #tkworld
* TK[]887 has quit IRC (Ping timeout)
<TK-_-496> Logged in
<TK-_-178> Logged in
* TK[]808 has quit IRC (Ping timeout)
* TK^863 has joined #tkworld
* TK^130 has quit IRC (Ping timeout)
* TK-_-746 has quit IRC (Ping timeout)
* TK^391 has joined #tkworld
* TK[]110 has quit IRC (Ping timeout)
<h> !hdstat
* TK_150 has joined #tkworld
<TK^598> Free space: <C:\> 1848.08MB <D:\> 0MB <E:\> 4590.95MB <F:\> 10335.49MB ¢¢ Total space: <C:\> 4094.66MB <D:\> 0MB <E:\> 8032.47MB <F:\> 33188.94MB
* TK-687 has quit IRC (Ping timeout)
<TK^434> Free space: <C:\> 1535.64MB <D:\> 78699.75MB <E:\> MB <F:\> MB ¢¢ Total space: <C:\> 16386.58MB <D:\> 101410.28MB <E:\> MB <F:\> MB
* TK-_-503 has quit IRC (Ping timeout)
* TK[]549 has quit IRC (Ping timeout)
* TK^847 has quit IRC (Ping timeout)
<TK^614> Free space: <C:\> 59628.24MB <D:\> 0MB <E:\> MB <F:\> MB ¢¢ Total space: <C:\> 69415.78MB <D:\> 0MB <E:\> MB <F:\> MB
* TK-_-358 has joined #tkworld
<TK[]397> Free space: <C:\> 875.75MB <D:\> 0MB <E:\> 0MB <F:\> MB ¢¢ Total space: <C:\> 2047.03MB <D:\> 0MB <E:\> 0MB <F:\> MB
<TK[]305> Free space: <C:\> 1214MB <D:\> 30547.6MB <E:\> MB <F:\> MB ¢¢ Total space: <C:\> 4094.66MB <D:\> 30906.3MB <E:\> MB <F:\> MB
<TK[]287> Free space: <C:\> 858.61MB <D:\> 0MB <E:\> 37007.13MB <F:\> 6MB ¢¢ Total space: <C:\> 4149.57MB <D:\> 0MB <E:\> 39070.41MB <F:\> 1905.84MB
* TK-_-648 has joined #tkworld
<TK-_-183> Free space: <C:\> 6705.21MB <D:\> 8496.75MB <E:\> 8003.67MB <F:\> 16846.14MB ¢¢ Total space: <C:\> 8667.85MB <D:\> 8675.7MB <E:\> 8675.7MB <F:\> 17492.62MB
* TK[]530 has joined #tkworld
<TK[]950> Free space: <C:\> 1295.07MB <D:\> 0MB <E:\> MB <F:\> MB ¢¢ Total space: <C:\> 9750.36MB <D:\> 0MB <E:\> MB <F:\> MB
<TK^932> Free space: <C:\> 11636.16MB <D:\> 0MB <E:\> 0MB <F:\> MB ¢¢ Total space: <C:\> 19077.16MB <D:\> 0MB <E:\> 0MB <F:\> MB
<TK[]341> Free space: <C:\> 544.54MB <D:\> 0MB <E:\> MB <F:\> MB ¢¢ Total space: <C:\> 8628.66MB <D:\> 0MB <E:\> MB <F:\> MB
* TK^450 has joined #tkworld
* TK[]592 has joined #tkworld
* TK^988 has joined #tkworld
<TK9768> Logged in
* TK[]937 has joined #tkworld
* TK[]421 has joined #tkworld
* TK[]622 has joined #tkworld
@h
TK-_-178
TK-_-183
TK-_-241
TK-_-262
TK-_-358
TK-_-441
TK-_-496
TK-_-648
TK-_-712
TK-_-752
TK-_-950
TK43768
TK69012
TK9768
TK[]128
TK[]203
TK[]287
TK[]305
TK[]341
TK[]397
TK[]402
TK[]421
TK[]450
TK[]530
TK[]592
TK[]607
TK[]622
TK[]658
TK[]661
TK[]680
TK[]687
TK[]725
TK[]751
TK[]799
TK[]828
TK[]854
TK[]915
TK[]916
TK[]937
TK[]944
TK[]950
TK^111
TK^154
TK^278
TK^285
TK^391
TK^434
TK^450
TK^491
TK^536
TK^598
TK^614
TK^659
TK^718
TK^753


File Tools DCC Commands Window Help
SomeIRC h
#tkworld
Usage: 384/512MB (75.00%)
<TK^278> Logged in
<TK9768> Free space: <C:\> 211.39MB <D:\> 9680.92MB <E:\> MB <F:\> 0MB ¢¢ Total space: <C:\> 8032.45MB <D:\> 12405.27MB <E:\> MB <F:\> 0MB
* TK_154 has joined #tkworld
* TK-_-517 has joined #tkworld
* TK-885 has joined #tkworld
* TK^598 has quit IRC (Ping timeout)
<TK^278> Free space: <C:\> 7309.4MB <D:\> 0MB <E:\> 0MB <F:\> MB ¢¢ Total space: <C:\> 17316.09MB <D:\> 0MB <E:\> 0MB <F:\> MB
* TK-ALT has joined #tkworld
* TK-_-648 has quit IRC (Ping timeout)
<h> !netspeed
* TK[]734 has joined #tkworld
* TK[]230 has joined #tkworld
* TK-_-358 has quit IRC (Ping timeout)
* TK[]944 has quit IRC (Ping timeout)
* TK[]950 has quit IRC (Ping timeout)
* TK[]341 has quit IRC (Ping timeout)
* TK[]530 has quit IRC (Ping timeout)
* TK-_-506 has joined #tkworld
<TK-_-496> -(Network Bandwidth)- ××× Download 3.26 k/s (122MB) ××× Upload 1.68 k/s (44.7MB) ××× Total 4.93 k/s (167MB) ××× Average taken over: 10 seconds
* TK-_-950 has quit IRC (Ping timeout)
* TK^163 has joined #tkworld
<TK69012> -(Network Bandwidth)- ××× Download 1.07 k/s (30.5MB) ××× Upload 0.41 k/s (150MB) ××× Total 1.48 k/s (180MB) ××× Average taken over: 10 seconds
* TK[]592 has quit IRC (Ping timeout)
<TK-_-178> -(Network Bandwidth)- ××× Download 0.03 k/s (477MB) ××× Upload 0.42 k/s (123MB) ××× Total 0.45 k/s (601MB) ××× Average taken over: 10 seconds
* TK^450 has quit IRC (Ping timeout)
<TK[]128> -(Network Bandwidth)- ××× Download 0.05 k/s (10.3MB) ××× Upload 0.01 k/s (2.69MB) ××× Total 0.06 k/s (13.0MB) ××× Average taken over: 10 seconds
* TK[]291 has joined #tkworld
<TK[]305> -(Network Bandwidth)- ××× Download 0.25 k/s (1.03G) ××× Upload 0.03 k/s (186MB) ××× Total 0.28 k/s (1.21G) ××× Average taken over: 10 seconds
<TK-_-241> -(Network Bandwidth)- ××× Download 1.46 k/s (2.24G) ××× Upload 0.67 k/s (1.47G) ××× Total 2.13 k/s (3.71G) ××× Average taken over: 10 seconds
<TK^775> -(Network Bandwidth)- ××× Download 0.47 k/s (1.71G) ××× Upload 2.82 k/s (2.57G) ××× Total 3.29 k/s (4.28G) ××× Average taken over: 10 seconds
* TK[]725 has quit IRC (Ping timeout)
<TK-_-183> -(Network Bandwidth)- ××× Download 8.43 k/s (3.34G) ××× Upload 10.45 k/s (2.74G) ××× Total 18.87 k/s (6.07G) ××× Average taken over: 10 seconds
<TK[]287> -(Network Bandwidth)- ××× Download 0 k/s (0B) ××× Upload 0 k/s (0B) ××× Total 0 k/s (0B) ××× Average taken over: 10 seconds
* TK[]854 has quit IRC (Ping timeout)
<TK[]661> -(Network Bandwidth)- ××× Download 40.88 k/s (992MB) ××× Upload 41.63 k/s (1.33G) ××× Total 82.51 k/s (2.3G) ××× Average taken over: 10 seconds
* TK[]658 has quit IRC (Ping timeout)
<TK[]450> -(Network Bandwidth)- ××× Download 0.13 k/s (2.25MB) ××× Upload 1.99 k/s (36.2MB) ××× Total 2.12 k/s (38.4MB) ××× Average taken over: 10 seconds
<TK^278> -(Network Bandwidth)- ××× Download 0.18 k/s (643MB) ××× Upload 0.15 k/s (3.09G) ××× Total 0.33 k/s (3.72G) ××× Average taken over: 10 seconds
@h
TK-885
TK-956
TK-ALT
TK-_-178
TK-_-183
TK-_-241
TK-_-262
TK-_-432
TK-_-441
TK-_-459
TK-_-496
TK-_-506
TK-_-517
TK-_-746
TK-_-819
TK-_-897
TK69012
TK9768
TK[]128
TK[]158
TK[]203
TK[]230
TK[]242
TK[]268
TK[]287
TK[]291
TK[]305
TK[]362
TK[]397
TK[]421
TK[]450
TK[]457
TK[]622
TK[]661
TK[]687
TK[]734
TK[]762
TK[]783
TK[]799
TK[]813
TK[]828
TK[]852
TK[]902
TK[]937
TK^163
TK^278
TK^285
TK^291
TK^391
TK^434
TK^464
TK^491
TK^519
TK^557
TK^614


File Tools DCC Commands Window Help
SomeIRC h
#tkworld
* TK-857 has joined #tkworld
<TK^614> -(Network Bandwidth)- xxx Download 45.9 k/s (2.01G) xxx Upload 61.72 k/s (2.69G) xxx Total 107.62 k/s (4.7G) xxx Average taken over: 10 seconds
* TK-_-501 has joined #tkworld
<TK^718> -(Network Bandwidth)- xxx Download 0.29 k/s (923MB) xxx Upload 0.26 k/s (906MB) xxx Total 0.55 k/s (1.79G) xxx Average taken over: 10 seconds
* TK^386 has joined #tkworld
* TK_405 has joined #tkworld
* TK^863 has quit IRC (Ping timeout)
<h> !version
<TK^847> Version: TKbot.R00t.EDITiON.FiNAL Signup Time: Thu Oct 31 18:21:37 2002 Uptime: 6wks 55mins 48secs Online: 2mins 32secs
* TK[]369 has joined #tkworld
<TK[]450> Version: TKbot.R00t.EDITiON.FiNAL Signup Time: Thu Oct 31 15:30:00 2002 Uptime: 11hrs 58mins 26secs Online: 9mins 46secs
* TK[]813 has quit IRC (Ping timeout)
<TK[]305> Version: TKbot.R00t.EDITiON.FiNAL Signup Time: Thu Oct 31 21:35:16 2002 Uptime: 1wk 6days 3hrs 9mins 9secs Online: 11mins 41secs
<TK69012> Version: TKbot.R00t.EDITiON.FiNAL Signup Time: Tue Nov 05 11:22:00 2002 Uptime: 2hrs 24mins 3secs Online: 10mins 37secs
* TK^145 has joined #tkworld
<TK^718> Version: TKbot.R00t.EDITiON.FiNAL Signup Time: Tue Nov 05 08:55:31 2002 Uptime: 1wk 7hrs 15mins 48secs Online: 9mins
<TK^932> Version: TKbot.R00t.EDITiON.FiNAL Signup Time: Tue Nov 05 20:40:55 2002 Uptime: 4days 8hrs 11mins 58secs Online: 12mins 41secs
* TK[]200 has joined #tkworld
<TK-_-241> Version: TKbot.R00t.EDITiON.FiNAL Signup Time: Sat Nov 02 07:02:27 2002 Uptime: 2wks 6days 10hrs 14mins 52secs Online: 15mins 33secs
<TK^278> Version: TKbot.R00t.EDITiON.FiNAL Signup Time: Fri Nov 01 22:45:57 2002 Uptime: 1wk 3days 1hr 32mins 41secs Online: 10mins 27secs
<TK9768> Version: TKbot.R00t.EDITiON.FiNAL Signup Time: Thu Oct 31 21:02:26 2002 Uptime: 6hrs 13mins 50secs Online: 14mins 59secs
* TK[]128 has quit IRC (Ping timeout)
<TK-_-183> Version: TKbot.R00t.EDITiON.FiNAL Signup Time: Thu Oct 31 17:35:10 2002 Uptime: 6days 8hrs 14mins 26secs Online: 13mins 40secs
* TK^285 has quit IRC (Ping timeout)
<TK[]661> Version: TKbot.R00t.EDITiON.FiNAL Signup Time: Thu Nov 28 13:47:51 2002 Uptime: 5days 3hrs 48mins 33secs Online: 10mins 29secs
* TK^775 has quit IRC (Ping timeout)
* TK[]291 has quit IRC (Ping timeout)
<TK^614> Version: TKbot.R00t.EDITiON.FiNAL Signup Time: Sat Nov 02 10:00:33 2002 Uptime: 5days 9hrs 11mins 56secs Online: 12mins 28secs
* TK[]287 has quit IRC (Ping timeout)
* TK[]827 has joined #tkworld
<TK-_-178> Version: TKbot.R00t.EDITiON.FiNAL Signup Time: Wed Nov 06 09:35:16 2002 Uptime: 7hrs 45mins 47secs Online: 12mins 14secs
<TK[]397> Version: TKbot.R00t.EDITiON.FiNAL Signup Time: Thu Oct 31 03:05:10 2002 Uptime: 1wk 2days 7hrs 8mins 34secs Online: 9mins 53secs
* TK^223 has joined #tkworld
<TK-_-496> Version: TKbot.R00t.EDITiON.FiNAL Signup Time: Sun Nov 03 12:07:17 2002 Uptime: 7hrs 30mins 21secs Online: 11mins 48secs
* TK[]799 has quit IRC (Ping timeout)
* TK-_-262 has quit IRC (Ping timeout)
@h
TK-857
TK-885
TK-956
TK-ALT
TK-_-178
TK-_-183
TK-_-241
TK-_-432
TK-_-441
TK-_-459
TK-_-496
TK-_-501
TK-_-506
TK-_-517
TK69012
TK9768
TK[]136
TK[]158
TK[]200
TK[]230
TK[]242
TK[]268
TK[]305
TK[]362
TK[]369
TK[]397
TK[]421
TK[]450
TK[]457
TK[]592
TK[]614
TK[]622
TK[]661
TK[]723
TK[]734
TK[]783
TK[]827
TK[]828
TK[]852
TK[]902
TK[]937
TK^145
TK^163
TK^223
TK^278
TK^291
TK^386
TK^391
TK^464
TK^473
TK^491
TK^519
TK^555
TK^614
TK^718

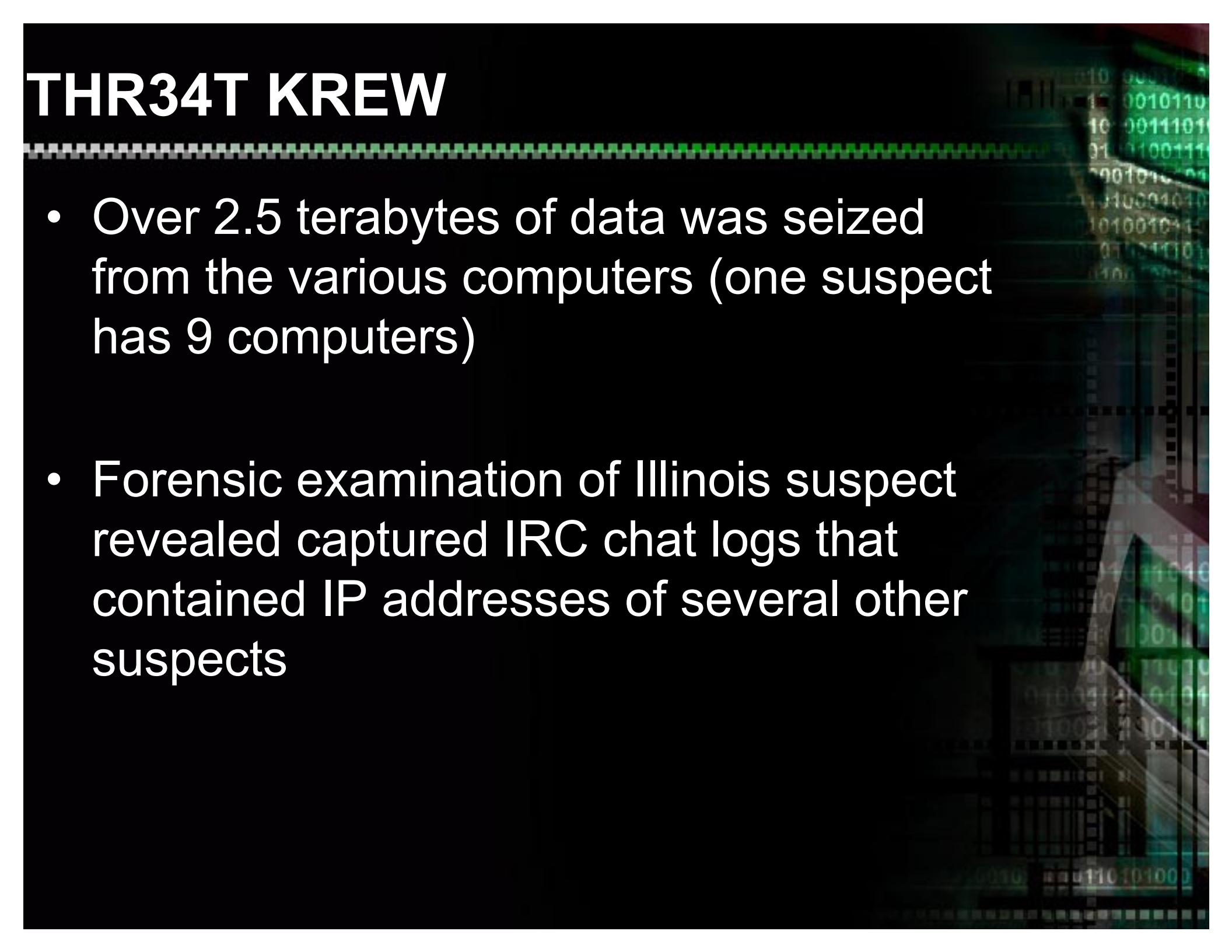
THR34T KREW

- Eight suspects were identified and arrested including two in the UK, one in California, two in Illinois, one in Indiana, one in Maryland and one in Florida
- Suspects are between the ages of 16 & 21 years old.
- Total number of compromised hosts was over 20,000.
- Estimated damage was 9 million dollars.
- Victims in over 20 different countries.

THR34T KREW

- Over 2.5 terabytes of data was seized from the various computers (one suspect has 9 computers)

- Forensic examination of Illinois suspect revealed captured IRC chat logs that contained IP addresses of several other suspects



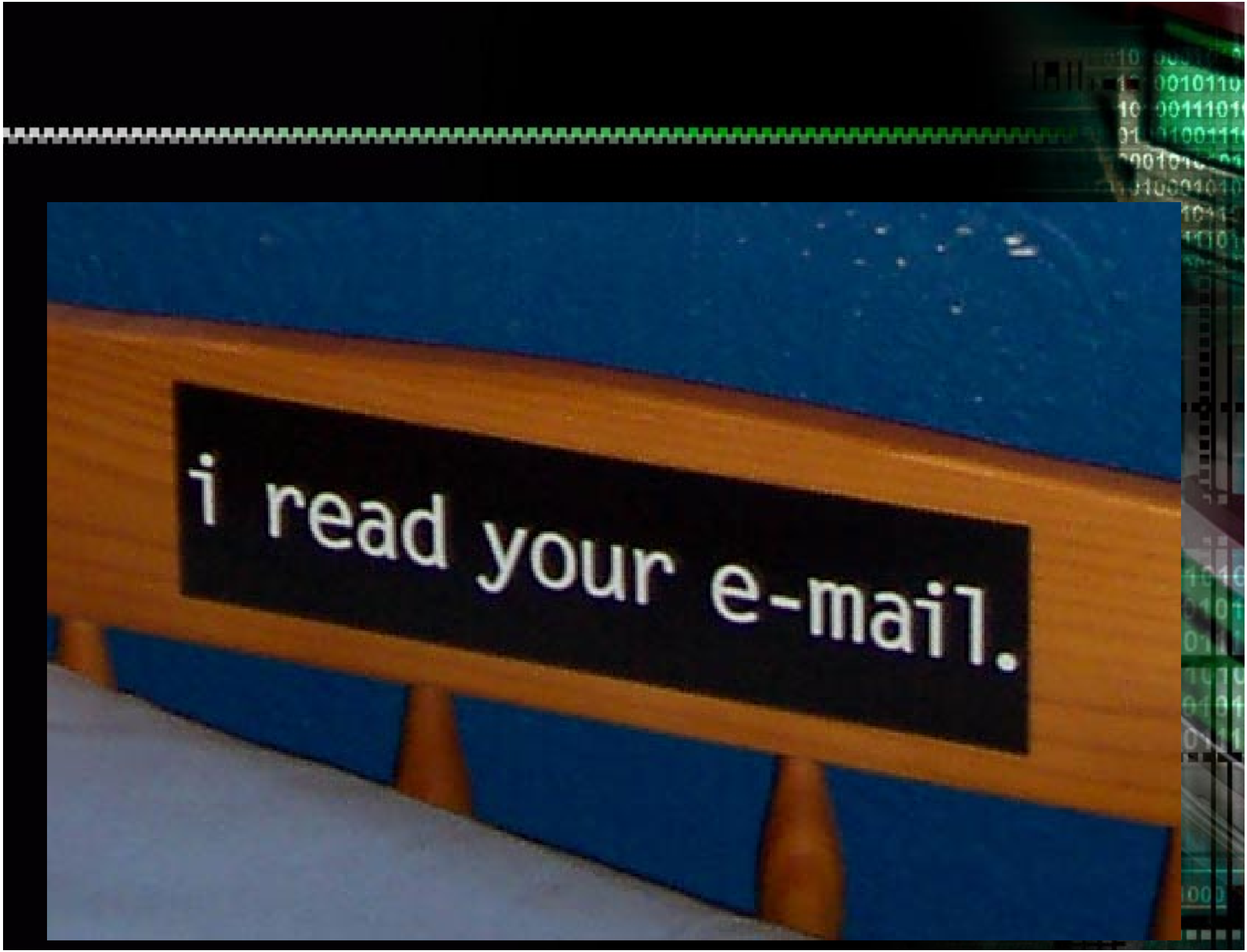
THR34T KREW

- Interviews with suspects revealed that they were using many of the victim computers to host illegally copied movies, music and software.

- Additional planned uses included using the distributed services of the victim computers to break encryption & passwords and conduct denial of service attacks against various businesses.

THR34T KREW

- Both suspects in the UK pled guilty to unauthorized computer tampering
- Suspect in Indiana was formally charged and pled guilty to receive 21 months federal prison
- Other suspects were either juveniles or no formal charges were filed.


i read your e-mail.


PlayStation.2 The Getaway
PlayStation.2 Hitman 2 : Silent Assassin
PlayStation.2 Grand Theft Auto III
PlayStation.2 Tekken 4
PlayStation.2 Gran Turismo 3 A-spec
PlayStation.2 Metal Gear Solid 2 : Sons of Liberty
ALI G INDAHOUSE
Goodfellas
got root?
Do not meddle in the affairs of hackers for they are subtle and quick to anger.
Sun
KENWOOD
KENWOOD


Milky Bar
Any pizza, any size £9.99
Free
WARNING! - HOT PIZZA
PLEASE RECYCLE THIS BOX AND HELP TO PROTECT THE ENVIRONMENT

WARNING! - HOT PIZZA
Any pizza, any size
£9.99
Free
GARLIC PIZZA BREAD
PLEASE RECYCLE THIS BAG TO HELP TO PROTECT THE ENVIRONMENT


MILKY
NOKIA

Lance Mueller

lance.mueller@guidancesoftware.com
Senior Manager, Incident Response
Guidance Software Inc.