Combating Cyber Crime: Essential Tools and Effective Organizational Structures

A Guide for Policy Makers and Managers

National Center for Justice and the Rule of Law

The University of Mississippi School of Law

COMBATING CYBER CRIME:
ESSENTIAL TOOLS AND EFFECTIVE ORGANIZATIONAL STRUCTURES
A GUIDE FOR POLICY MAKERS AND MANAGERS©

by

National Center for Justice and the Rule of Law
University of Mississippi
School of Law

Mission Statement

The National Center for Justice and the Rule of Law (NCJRL) is a part of the University of Mississippi School of Law. The Center focuses on issues relating to the criminal justice system, with its purpose to promote the two concepts comprising the title of the Center. The concept of "justice" appeals to basic notions of equality, equity, and fairness, often with an emotive component. In contrast, the phrase "rule of law" refers to the requirement that certain procedures and principles must be followed in each case to reach a correct result. Neither concept is sufficient; rather, both must be utilized to ensure that the criminal justice system fulfills its function in society. The Center implements its mission through projects, conferences, educational programs, and publications that examine important criminal law and procedural issues.

Please visit the Center's website at www.NCJRL.org for additional information.

ACKNOWLEDGMENTS

The following persons contributed to the preparation of this Guide:

From the National Center for Justice and the Rule of Law

Thomas K. Clancy, Director

Donald R. Mason, Associate Director

Marc Harrold, Senior Counsel

Priscilla Adams, Senior Research Counsel

Dawn Jeter, Operations Manager

From the National Association of Attorneys General

Hedda Litwin, Cyber Crime Counsel

Acknowledgement of Federal Funding

This project was supported by grants awarded by the Bureau of Justice Assistance. The Bureau of Justice Assistance is a component of the Office of Justice Programs, which includes the Bureau of Justice Statistics, the National Institute of Justice, the Office of Juvenile Justice and Delinquency Prevention, and the Office of Victims of Crime. Points of view or opinions in this document are those of the NCJRL and do not represent the official position of the United States Department of Justice.

COMBATING CYBER CRIME:
ESSENTIAL TOOLS AND EFFECTIVE ORGANIZATIONAL STRUCTURES
A GUIDE FOR POLICY MAKERS AND MANAGERS

Table of Contents

§1. INTRODUCTION

This Guide is designed to provoke thought and action. It seeks to provide Policy Makers and Managers with information about the need to combat cyber crime, including on a state-wide level. It outlines essential tools needed to engage in that combat and it gives Decision Makers options in structuring state-wide responses to the challenges of cyber crime. The dimensions of cyber crime mirror the uses that modern society makes of information technology: it is ever growing and ubiquitous. To effectively address the vast and varied dimensions of the problem requires international, national, statewide, and local efforts.

In response to the many challenges of cyber crime, the National Center for Justice and the Rule of Law created its Cyber Crime Initiative in 2001, which has sought ways to improve the ability of states to investigate and prosecute persons engaged in sophisticated criminal activity. To implement this goal, the Center's strategy has focused on creating strategic alliances to develop projects that are unique and address concerns of national interest.

The National Center for Justice and the Rule of Law has had a long-standing relationship with the National Association of Attorneys General and individual offices that comprise the Association. Those relationships have produced training and educational programs for state AG offices in all 50 states, projects with individual states such as Mississippi and California to create model projects and tools, a cyber crime newsletter that all state AG offices receive, and other specialized work focused on improving state-level abilities to combat cyber crime. The Center also partners with other organizations to offer cyber crime training to law enforcement and state trial and appellate judges.

The Center is supported by grants from the United States Department of Justice and we gratefully acknowledge that funding and thank the Department of Justice for its continued support.

It is the Center's hope that this Guide furthers our mission by providing information and alternatives to state Policy Makers and Managers that will help them structure an effective response to the challenges of cyber crime.

Thomas K. Clancy
Director
National Center for Justice and the Rule of Law

April 1, 2007

§2. CYBER CRIME AND ITS DIMENSIONS

§2.1. WHAT IS CYBER CRIME?

§2.1.1. "Cyber Crime" defined: *What's in a name?*

There is no consensus definition for cyber crime. It has been variously referred to as:

- "Computer crime"
- "Network crime"
- "Computer-related crime"
- "Computer-facilitated crime"
- "High tech crime"
- "Internet crime"
- "Online crime"
- "Information age crime"

Nomenclature debates and nuances aside, computers are ubiquitous and ever diversifying in their sizes, shapes, uses, and purposes. What they have in common is that they process and store information as data in binary form (1's and 0's) and are "digital devices."

It is helpful to think of "cyber crime" as any crime in which a computer or other digital device plays a role, which is to say that ***digital evidence*** *is involved, regardless of whether the crime fits under any statutory definition of computer crime.*

Functional approach to defining cyber crime.

Rather than attempt a comprehensive definition, cyber crime can be defined by reference to the three ways in which computers can be involved in crime.

- ***Target*****:** A computer may be the *target* of a crime, including such actions as unauthorized access, damage, or theft.

Sometimes referred to as "true computer crime," involving new, technology-specific crimes that did not exist prior to the spread of computer technology and networks.

Examples:

- Hacking or cracking
- Network or computer intrusions and security breaches
- Spam, viruses, worms, Trojan horses
- "Denial of service" attacks
- Web site defacement
- Electronic privacy violations

- ***Tool:*** A computer may by used as a *tool* or "instrument" to commit a crime, including many traditional crimes.

  Almost any kind of crime can be assisted through the use of computers and the Internet.

  Examples:

  - Child pornography or other sexual exploitation
  - Threats and harassment
  - Frauds
  - Embezzlement
  - Electronic thefts (e.g., of intellectual property)
  - Thefts of personally identifiable information

- ***Container*:** A computer may *contain* evidence, including criminal activity that does not necessarily involve a computer for its commission.

  Digital evidence may prove relevant and valuable in any conceivable crime.

  Examples:

- Drug dealers store supplier and customer records on digital devices.
- The BTK killer in Wichita, Kansas was found using information gleaned from the metadata properties of an electronic letter.
- Convicted wife murderer Scott Peterson had incriminating evidence (maps, online shopping information, communications) on his computer.
- Emails and chat logs can lead investigators to the locations of abduction, rape, or murder victims.

§2.1.2. "Digital Evidence"

Digital evidence is information of probative value that is stored or transmitted in binary form that may be relied upon in court.

Volume of digital data

- Almost 95% of all information generated today is in electronic form.
- No more than 30% of that information is reduced to paper form.

Examples of where digital evidence may be found:

- Computers
- Hand-held devices with "embedded computer systems"
- Digital cameras
- Personal digital assistants (PDAs)
- Mobile phones
- Servers, including:
  - Internet service providers

- FTP and web servers
- email servers
- local area network (LAN) servers

- Online activities

§2.1.3. Challenges for Law Enforcement of Cyber Crime

- To assure that digital evidence is acquired, preserved, and analyzed in a forensically safe manner and thus enable its presentation in court, specialized equipment and software is needed and personnel must be trained to recognize, properly seize, and examine the evidence.

- Criminals are rapidly adopting technology.

- Digital devices are ubiquitous.

- Digital devices are diversifying and "converging" into many "hybrid" devices.

- Data storage capacities are rapidly growing.
  example: The Seagate Barracuda hard drive has 750 GB of space, which can hold 25 DVDs, 50 hours of home video, 15,000 songs, 15,000 digital pictures, and 50 computer games -- and still have 300 GB of free space left over.

- Digital storage media are being reduced in size.
  example: USB "thumb drives" are ever smaller and growing in data capacity.

- Crime is "migrating" to the Internet.

- The interstate and international nature of many cyber

crimes raise difficult jurisdictional issues.

§2. 2. SOURCES AND TYPES OF DIGITAL EVIDENCE[1]

The following section lists many of the sources of and types of digital evidence by object and then by crime.

§2.2.1. Containers of Digital Evidence

Computer Systems:

Components:

Main base unit –CPU
Data storage devices
    hard drives
    memory cards
Removable storage devices and media
    floppy disks
    CDs
    DVDs
    Zip disks, cartridges
    backup tapes
    USB drives
    Monitor
    Keyboard
    Mouse or other I/O device
Stand alone or networked
Mini or mainframe, desktop, tower, rack-mounted, laptop, hand-held, hybrid

User-Created Files:

Text files (documents, e-mails, chats, instant messages, etc.)
Address books
Audio/video files
Calendars
Databases
Images/graphics/animations
Internet bookmarks/favorites

[1] This section is adapted from various sources, including *Electronic Crime Scene Investigation: A Guide for First Responders*, National Institute of Justice (2001), and *Best Practices For Seizing Electronic Evidence (v. 3),* United States Secret Service, Department of Homeland Security (2006).

Spreadsheets
Web content

Hidden Files:

Embedded data and metadata ("data about the data")
Compressed files
Encrypted files
Misnamed files
Password-protected files
Steganography

Computer-Created Files:

Backup files
Configuration files
Cookies
Hidden files
History files
Log files
Printer spool files
Swap files
System files
Temporary files

Other Data Areas:

Bad clusters
Computer date, time, passwords
Deleted files
Free space
Hidden partitions
Lost clusters
Metadata
Other partitions
Reserved areas
Slack space
Software registration information
System areas
Unallocated space

Central Processing Units (CPUs):

The device itself may be evidence of component theft, counterfeiting, or remarking.

Memory:

The device itself may be evidence of component theft, counterfeiting, or remarking.

<u>Access Control Devices</u> (Smart Cards, Dongles, Biometric Scanners):

Identification/authentication information of the card and the user
Level of access
Configurations
Permissions
Device itself

<u>Answering Machines</u>:

Stored voice messages
Time and date information about messages (in some cases)
Caller identification information
Deleted messages
Last number called
Memo
Phone numbers and names
Tapes

<u>Cell Phones</u>:

Subscriber/Device identifiers
Electronic serial number
Call logs
Appointment calendars/contact information
Caller identification information
E-mail
Images
Video
Memo
Password
Phone book entries
Text messages
Voice mail
Website content
Web browsers and history files

<u>Digital Cameras</u>:

Images
Removable cartridges/memory cards
Sound
Time and date stamp
Video
Email and most other data may be stored on cameras
(they can act portable storage devices via USB connections)

Digital cameras utilizing the Exchangeable Image file Format (ExIF) produce JPEG or TIFF files that can reveal the following metadata:

- Camera make and model
- Camera settings when picture taken
- Time picture taken
- Time picture modified
- Who took the image (author)
- Copyright information

Hand-held Devices (PDAs and hybrid devices):

- Address book
- Appointment calendars/information
- Documents
- E-mail
- Images
- Videos
- Handwriting
- Password
- Phone book
- Text messages
- Voice messages

Note: Evidence may exist on such devices that was never saved to a computer.

Modems:

- The device itself

Network Components:

Local Area Network (LAN) Card or Network Interface Card (NIC)

- The device itself
- MAC (media access control) address

Routers, Hubs, and Switches

- The devices themselves
- For routers, configuration files

Servers

- Same as computer systems (above)

Network Cables and Connectors

- The devices themselves

Pagers:

Address information
E-mail
Phone numbers
Text messages
Voice messages

Printers:

Documents
Hard drive
Ink cartridges
Network identity/information
Superimposed images on the roller
Time and date stamp
User usage log

Scanners:

The device itself
Showing capability to scan.
Perhaps allowing identification of scanner used to process documents.

Copiers:

Documents
Time and date stamp
User usage log

Credit Card Skimmers

Digital Watches:

Address book
Appointment calendars
E-mail
Notes
Phone numbers

Facsimile Machines:

Documents
Film cartridge
Phone numbers
Send/receive log

Global Positioning Systems (GPS)*:*

Home

Previous destinations
Travel logs
Way point coordinates
Way point name

<u>Vehicle Event Data Recorders</u> ("black boxes"):

Crash data

<u>Other Electronic Devices and Peripheral Evidence</u>:

Audio recorders
Cables
Caller ID devices
Chips (When found in quantity, it may indicate chip theft.)
Digital picture frames
Dongle or other hardware protection devices (keys) for software
Drive duplicators
Game boxes
USB and other external drives (e.g., "thumb" drives)
Flash memory cards
Music, video, and photo players
PCMCIA cards
VCRs
DVRs (e.g., Tivos)
Wireless access points

§2.2.2. Potential Evidence by Crime Category

<u>Computer Fraud</u> (including auction fraud and other online fraud):

Account data from online auction sites
Accounting/bookkeeping software and associated data files
Address books
Calendar
Chat logs
Customer information/credit card data
Databases
Digital camera software
E-mail, notes, and letters
Financial asset records
Image files
Internet activity logs
Internet browser history/cache files
Online banking software
Records/documents of "testimonials"
Telephone records

Child Exploitation/Abuse:

Chat logs
Date and time stamps
Digital camera software
E-mail, notes, and letters
Games
Graphic editing and viewing software
Images
Internet activity logs
Movie files
User-created directory and file names that classify images

Computer/Network Intrusion:

Address books
Configuration files
E-mail, notes, and letters
Executable programs
Internet activity logs
Internet protocol (IP) address and user name
Internet relay chat (IRC) logs
Source code
Text files and documents with user names and passwords

Homicide/Death Investigation:

Address books
Diaries
E-mail, notes, and letters
Financial/asset records
Internet activity logs
Legal documents and wills
Maps or driving directions
Medical records
Telephone records
Photos of victim / suspect
Trophy photos

Domestic Violence:

Address books
Diaries
E-mail, notes, and letters
Financial asset records
Medical records
Telephone records

Economic/Financial Fraud (including counterfeiting):

Address books
Calendar
Check, currency, money order images
Credit card skimmers
Customer information/credit card data
Databases
E-mails, notes, and letters
False financial transaction forms
False identification
Financial asset records
Images of signatures
Internet activity logs
Online banking software

E-Mail Threats /Harassment/Stalking:

Address books
Diaries
E-mails, notes, and letters
Financial asset records
Images
Internet activity logs
Legal documents
Telephone records
Victim background research
Maps to victim locations

Extortion:

Date and time stamps
E-mails, notes, and letters
History log
Internet activity logs
Temporary Internet files
User names

Gambling:

Address books
Calendar
Customer database and player records
Customer information/credit card data
Electronic money
E-mails, notes, and letters
Financial asset records
Image players
Internet activity logs
Online banking software

Sports betting statistics

Identity Theft:

Hardware and software tools

Backdrops
Credit card generators
Credit card reader/writer
Digital cameras
Scanners

Identification templates

Birth certificates
Check cashing cards
Digital photo images
Driver's licenses
Electronic signatures
Fictitious vehicle registrations
Counterfeit insurance documents
Scanned signatures
Social security cards

Internet activity related to ID theft

E-mails and newsgroup postings
Deleted documents
Online orders
Online trading information
System files and file slack
Internet activity logs

Negotiable instruments

Business checks
Cashier's checks
Credit card numbers
Counterfeit court documents
Counterfeit gift certificates
Counterfeit loan documents
Counterfeit sales receipts
Money orders
Personal checks
Stock transfer documents
Traveler checks
Vehicle transfer documentation

Narcotics:

Address books
Calendar

Databases
Drug recipes
E-mails, notes, and letters
False identification
Financial/asset records
Internet activity logs
Prescription form images

Software Piracy:

Chat logs
E-mails, notes, and letters
Image files of software certificates
Internet activity logs
Software serial numbers
Software cracking information and utilities
User-created directory and file names that classify copyrighted software

Telecommunications Fraud:

Cloning software
Customer database records
Electronic Serial Numbers
Mobile Identification Numbers
E-mails, notes, and letters
Financial asset records
"How to phreak" manuals
Internet activity logs
Telephone records

§2.3. STATISTICS AND DIMENSIONS: *A SNAPSHOT*

- Comprehensive national statistics on cyber crimes are lacking for a variety of reasons, including:
    - Lack of consensus on definitions
    - No collection of uniform data
    - Difficulty of detecting the criminal activity
    - Inadequate law enforcement resources
    - Lack of victim awareness
    - Business reluctance to report

- **Illustrative Statistics and Facts**

    - *Child Pornography and Sexual Solicitation of Minors*

- One in seven youth aged 10 to 17 who are regular Internet users are sexually solicited online.
  source: National Center for Missing and Exploited Children.

- The NCMEC CyberTipline received 106,176 reports of child pornography in 2004, a 491% increase from the number of reports received in 2001.

- 1500% increase in child pornography images on the Internet from 1997 to 2005.
  source: Internet Watch Foundation.

- *Spam*

  - Represented nearly 93% of all email at the end of 2006.
    source: Postini.

- *Security Threats*

  - 41,536 new security threats were detected in 2006 alone.
    source: Sophos.

- *Phishing*

  - $2 billion lost in 2007 to phishing scams by organized crime.
    source: Gadi Evron, of Beyond Security.

  - Phishing scams for October 2006 were a record of 37,444, which was 9 times as many as in October 2005.
    source: The Anti-Phishing Working Group.

- *Piracy*

  - Worldwide revenue loss from software piracy in

2005 was more than $34 billion.

sources: The Business Software Alliance; IDC

§3. AG OFFICE CYBER CRIME CAPACITIES: THREE STRUCTURAL ALTERNATIVES

This section provides an overview of three different approaches taken by state Attorneys General to create capacity to combat cyber crime.

§3.1. Mississippi - Dedicated In-House Cyber Crime Unit

A dedicated cyber crime unit within an AG's office has self-contained prosecution, investigative, and forensics capacities.

- **Structure within AG office**

AG office has statewide jurisdiction and arrest powers and the authority to impanel statewide grand jury to investigate and indict. Prosecutors from the Attorney General's Office can try cases in any court in the state.

Cyber crime unit is within Public Integrity Division - head of cyber crime unit reports to Division head.

- **Composition of Unit**

One attorney (unit head), 3 investigators, 1 forensics examiner

Note: Some investigators have become qualified to do forensic examinations.

- In house-computer forensics lab
- In-house lab accepts cases for analysis from throughout state

- **Unit Caseload**

  Sources of cases:

  - Unit's own investigations (40%)
    - Unit has worked in 72 of state's 82 counties
    - Accepts cases involving any dollar amount – if it cannot take case, unit refers case to the Internet Crime Complaint Center
  - Requests for computer forensics analysis received from a DA's office or local law enforcement (36%)
    - Sole reason to deny forensic service is if forensics previously started elsewhere
  - Requests for assistance from a DA's office or local law enforcement (24%)

  Types of cases and public education:

  - Child exploitation - 60%
  - Internet fraud and identify theft - 40%
  - Public Education, including 1 to 2 presentations per week on Internet safety and working with Netsmartz on safety programs for children

- **Funding of Unit**

  - Start-up funding from National Center for Justice and the Rule of Law at the University of Mississippi (three years)
    - Unit was subgrantee of federal grant

awarded to NCJRL

- Follow-on $300,000 grant from the Center for Computer Security Research at Mississippi State University

- The Cyber Crime Unit receives a portion of the legislative appropriations for the Attorney General's Public Integrity Division for its operations. There is no separate line item for the Unit.

§3.2. Maine - Statewide Cyber Crime Task Force Model

A task force model is a pooling of prosecution, forensics, and investigative resources from a variety of independent agencies.

- **Members of Maine Computer Crime Task Force (MCCTF)**

  - Lewiston, Maine Police Department promoted idea, formed partnership in 1999 with:

    - Office of the Attorney General of Maine
    - Brunswick, Maine Police Department
    - Maine State Police
    - Portsmouth, Maine Police Department

  - Maine task force partnered with Vermont and New Hampshire police to apply for and receive funding from OJJDP as Northern New England Internet Crimes Against Children (ICAC) Task Force

- **Funding and Staffing History of Task Force**

  Original funding from the Office for Juvenile Justice and Delinquency Prevention was $135,000 every 18 months

- Covered basic operating expenses, such as equipment, training, and costs of two regional computer forensic laboratories, but no personnel costs

- Lewiston PD and Maine State Police each donated experienced detective/certified forensic computer examiner

- Sponsoring agencies do not receive reimbursement for their services as task force members

2001 - Maine Legislature placed task force under Department of Public Safety administratively and fiscally

- Appropriated $160,000 for 2 years of operational expenses plus funding for State Police sergeant to supervise daily operations

2004 - state funding sunsetted, resulting in 54% budget reduction and loss of supervisor position

2005 - State Police restored supervisor position and assigned additional detective

- Continuation funding from OJJDP: $80,000 for 12-month period

2006 - Governor signed emergency measure appropriating funds for establishment of computer crimes unit within State Police under Department of Public Safety

- Provides funding for 2 computer crimes forensic analysts and operational costs

- Appropriations sources (total of $300,498 for FY 2006-07):

- $111,185 from General Fund
- $189,313 from Highway Fund

- **Responsibilities of MCCTF**

  - Coordinates computer crime investigations statewide

  - Conducts computer forensic examinations

  - Responds to requests for assistance from other law enforcement agencies - *e.g.*, drafting subpoenas, contacting ISPs

  - Conducts training programs for law enforcement agencies on investigation of Internet cases

  - Conducts Internet safety programs for public

  - Each member agency responsible for cases within own jurisdiction

  - Each member agency is trained in cyber crime investigative techniques and encouraged to perform outreach on Internet safety

- **Current Composition of MCCTF**

  - Lewiston PD manages unit

  - Includes members of local law enforcement as designated by their agency as responsible for investigating computer crime

  - Three investigators and three computer forensics examiners

  - Two AAGs from Maine AG Office provide legal support

- Problem: some of officers "donated" to task force have been returned to their respective law enforcement agencies

- **Caseload of MCCTF**

  - When first established, received about 20 cases/month from the National Center for Missing and Exploited Children (NCMEC)

  - Priority is Internet Crimes Against Children (ICAC) cases - 80% of workload

  - Present backlog: 44 cases

  - Internet Crime Complaint Center sends cases directly to individual agencies

§3.3. New Hampshire - Model of Distributed Forensics/Prosecution of Cybercrime

This model is structured so that local prosecutors and investigators handle cyber crime cases, not the AG office.

- **Development of Statewide Strategic Plan to Address Cybercrime**

  2003: New Hampshire AG invited state decision makers to meeting to develop plan to address cyber crime, get consensus, set up task force

  - Asked all task force members to identify point person, complete survey of needs

  - Law enforcement task force members established plan to meet quarterly to discuss status of computer crimes in their jurisdictions

- **Implementation of Plan**

  Forensic examiners at state lab receive and image devices, run verifications and indexing, store indexed images on Storage Area Network

  Using viewing stations, local investigators ("case agents") access forensic images via secure, remote access to forensic machines; conduct analysis on read-only prepared media

  2004: New Hampshire AG awarded a grant to Justiceworks at University of New Hampshire to:

  - survey law enforcement needs and existing technologies
  - develop and implement cybercrime training for law enforcement investigators and prosecutors
  - address forensics issues

  2005: Justiceworks

  - completed survey of law enforcement needs and technologies
  - developed plan to implement training and forensics capabilities

- **Major Funding Sources**

  - OJJDP: $620,000 for New Hampshire ICAC support
  - $50,000 grant from Bureau of Justice Statistics of the US Department of Justice to support Statistical Analysis Center, which is used to enhance state forensic laboratory

- State DHS: $250,000 for forensics training of case agent

§4. Essential Capacities Needed to Combat Cyber Crime

§4.1. Personnel

Essential personnel requirements to combat cyber crime reflect the basic functions of a cyber crime unit: investigation, prosecution, legislative assistance, education/public outreach, and training.

- **Investigators**

Well-trained law enforcement officers are needed to conduct cyber crime investigations. Investigations include traditional crimes facilitated by the use of computer technology as well as crimes in which computers are used as an instrument. In addition to traditional skills, training, and qualifications, specialized skills and knowledge of cyber crime technology and legal requirements are needed.

- *Specialized Skills Needed for All Cyber Crime Investigations*

  - Ability to prepare and execute search and arrest warrants for digital evidence
  - Knowledge of how computers work in order to effectively interrogate suspect and establish culpability of evidence found on his computer
  - Willingness and capacity to receive continual specialized training and certifications in such specialities as digital

evidence, computers, networks, and forensic analysis

- Specialized crime scene preservation and examination skills
- Working knowledge of the Internet
- Ability to work with representatives from other jurisdictions

■ *Skills Needed for Proactive Investigation*

Note: Proactive investigations include situations where the investigator uses computers and the Internet to communicate with potential perpetrators, etc.

- Covert, proactive investigations require the investigator to "role-play." Investigators must be knowledgeable of many facets of popular culture and the "slang" used in e-mail and instant messaging communications to effectively pose as an underage person. Further, investigators must be familiar with the typology of Internet predators.
- For examples of successful proactive investigations, *see* §5.

● **Prosecutors**

Cyber crime prosecutors typically team with investigators and computer forensic examiners to investigate and prosecute cases.

■ *Essential Functions of Cyber Crime Prosecutors*

- Oversee operations of cyber crime unit/ task force

- Advise investigators and computer forensic examiners as to the amount and type of evidence necessary for arrest and conviction

- Develop forms, protocols, and procedures for the writing, execution, and return of search and arrest warrants

- Often engages in public outreach and education in an effort to prevent victimization

■ *Essential Skills of Cyber Crime Prosecutors*

- Knowledge of cyber crime statutes and other relevant crimes

- Familiarity with computer technology and computer forensics

- Commitment to continued education in both the legal and technical aspects of cyber crime prosecution

■ *Public outreach and education*

- Due to the nature of cyber crime and efforts to prevent such victimization through community education, prosecutors in this area often engage in public outreach and education

- **Computer Forensic Examiners**

The proliferation of and close linkage between digital and computer evidence and the work of prosecutors and investigators indicates a strong need for in-house computer forensic examiners.

- *Essential Functions*

    - Primary responsibility for analysis of digital evidence
    - Functions include disk imaging, data recovery, data extraction, and system analysis
    - Provide testimony concerning technical aspects of data recovery and analysis
    - Work closely with investigators on such issues as preparation and execution of search warrants, devising surveillance schemes, and other issues related to the technical aspects of an investigation
    - Maintain hardware and software utilized to obtain and analyze digital evidence
    - Maintain the condition and security of the forensic computer laboratory
    - Maintain procedures for handling and securing evidence in the forensic laboratory

- *Essential Skills*

    - Extensive experience with computers, particularly in the law enforcement context
    - Degree in computer science or related field is a plus
    - Experience and certification with the

design and maintenance of computers and computer networks

- Comprehensive knowledge of computer operating systems
- Training and certification in computer forensics
- Ability to testify in court
- Commitment to continued education in computer forensics

§4.2. INFRASTRUCTURE

This section represents our best effort to describe the hardware, software, physical space, and other components needed or desirable to create effective cyber crime investigative and prosecution capacity. These needs constantly evolve and there is some disagreement within the forensic community on infrastructure requirements. The primary needs involve forensic capacity–the ability to obtain, preserve, and analyze digital evidence.

To accomplish its mission, cyber crime capacity demands a commitment of resources to infrastructure.

In addition, the needs of investigators and prosecutors must be met. The quantity of items described in this section will vary with the size and mission of the unit or task force. What is described here are the *minimal requirements* to set up an effective cyber crime unit.

§4.2.1. ESSENTIAL COMPONENTS

- **Hardware, physical tools, and services**
  - DEDICATED FORENSIC COMPUTER SYSTEMS

- Minimum of one workstation for *each* computer forensic examiner to analyze digital evidence.

- Additional computer(s) for acquisition of digital evidence (*imaging* or making copies of media).

- *Note*: This equipment needs to be upgraded frequently.

- STORAGE MEDIA

  - Hard drives, CDs, DVDs, and other media for imaging and data storage.

  - Number needed will depend on the number of computers accepted/imaged for examination. Given the rapidity of change, continual upgrading is needed.

  - *Note:* Forensic experts need to work on a forensically sound copy and not the original and a significant amount of storage media is needed. Bit-stream images can also be stored on servers.

- HARDWARE WRITE BLOCKERS (maintain integrity of digital evidence)

  - *Note:* Block all writes to a connected device and enable forensically safe cursory review.

- WIRELESS NETWORK SIGNAL DETECTOR

- DUPLICATING TOOLS (for data capturing/acquisition/ disk imaging)

  - *Note:* Having multiple devices is

recommended as speeds and capabilities vary and large numbers of devices can be encountered.

- COMMUNICATIONS EQUIPMENT
- OFFICER SAFETY EQUIPMENT AND DEVICES (bullet-proof vests, etc.)
- INTERNET ACCESS (within the investigator work spaces; not in the lab)
- PRINTERS (at least one color and one portable)
- DIGITAL CAMERA
- CABLES AND CONNECTORS
- MODEM
- CD / DVD BURNER
- ATOMIC CLOCK
- UNINTERRUPTIBLE POWER SUPPLY
- TAPE RECORDER(S)
- NOTE PADS AND SKETCH PADS
- EVIDENCE FORMS
- CRIME SCENE TAPE
- MARKERS
- VENT HOOD

- **Software**

    - BOOT DISKS AND WRITE BLOCKERS ("write-protect" software used to preserve integrity of evidence during acquisition)

    - DISK IMAGING/DATA DUPLICATION TOOLS (for making forensic copies)

    - IMAGE VALIDATION/DATA VERIFICATION SOFTWARE (for ensuring that forensic copy/duplicate is pure and entirely accurate)

    - EVIDENCE EXTRACTION / DATA RECOVERY TOOLS (for finding and extracting data from storage devices while working on image)

        examples: password-cracking and file-carving tools

    - EVIDENCE EXAMINATION / DATA ANALYSIS TOOLS

        examples: file viewers, text searchers, metadata verifiers, web browsers

    - EVIDENCE ORGANIZATION TOOLS

        examples: link analysis tools, time liners, file managers, indexers

    - FORENSIC ANALYSIS SOFTWARE SUITES AND OTHER SOFTWARE TOOLS

        Note: Forensic examiners typically use at least two of these for cross-validating results or because each is considered to have strengths for certain types of cases.

        ▸ The most popular include:
            - Forensic Toolkit®(FTK™) from Access Data
            - EnCase® Forensic Edition from Guidance Software
            - ILook Investigator© [free to law enforcement] from the I.R.S.

- Other popular and emerging software tools:
  - DriveSpy, Image, Part, PDBlock and PDWipe from Digital Intelligence
  - Password Recovery Toolkit and Registry Viewer from Access Data
  - Forensic software for PDAs, password recovery, text searching, data acquisition, e-mail examination, etc. from Paraben
  - SMART from ASR Data
  - ProDiscover® "family of products" by Technology Pathways
  - Maresware by Mares and Company
  - Knoppix (open-source "first responder" tool for on-site previewing)
  - FastBack
  - SafeBack 3.0, and other tools available from NTI (an Armor Forensics Division)
  - Norton Ghost by Symantec
  - WinHex by X-Ways Software Technology AG
  - CD/DVD Inspector by InfiniDyne
  - The Sleuth Kit and Autopsy Forensic Browser (both open source), which can be obtained from www.sleuthkit.org.
  - The Coroner's Toolkit (TCT) (a collection of free programs), available through www.porcupine.org/forensics/tct.html
  - Black Bag Macintosh Forensic Suite by Black Bag Technologies

- **Workspace and Furnishings**

  - "*Laboratories and/or forensic workspace for the examination of digital technology items should be designed and equipped for efficient, secure, safe and effective use.*"

    International Organization on Computer Evidence
    Guidelines for Best Practice

  - Dedicated space is required for accomplishment of the mission, with appropriate office space for each staff member and lab space, fixtures, lighting, ventilation, and static control features that will enable efficient use of the forensics hardware.

- Designs and layouts vary but privacy and security are crucial.
    - Forensic examiners recover and view highly sensitive evidence (e.g., images of child pornography)
    - Forensic Lab requirements:
        - separate from other offices or public spaces
        - secure access control system
        - must be climate controlled
- Other physical structure needs:
    - viewing room for defense counsel/experts to examine digital media in a controlled environment
    - conference room secure from the forensic lab and other staff offices, for meetings, search preparations, and other uses by investigators, forensic examiners, prosecutors, and outside personnel

- **Secure Storage**
    - All evidence, including seized computers, media, and forensic images, must be retained in a climate-controlled setting where access can be strictly controlled and monitored for security and chain of custody
    - Space must be adequate to meet projected need, considering evidence acquisition and retention policies and the anticipated volume of evidence
    - Needs to be in close proximity to the lab

- Limited personnel clearance to access the evidence vault

§4.2.2. DESIRABLE RESOURCES

- **Equipment and subscriptions**
  - Additional flat-screen monitors so examiners can work with dual monitors
  - Drives separately containing each version of Windows and other popular operating systems pre-installed
  - Apple Mac computer for examinations of Apple computers
  - Portable forensic labs for onsite imaging and previewing
  - Subscriptions to computer and technology periodicals
- **Vehicles**
  - Unmarked cars for investigators
  - Wagons, vans, or SUVs for responding to crime scenes and transporting evidence in forensically sound manner

§4.2.3. SPECIAL CONSIDERATIONS (depends on the type of forensics conducted)

- **Bag and Tag Tool Kit**

For a general listing of additional items that may be useful – or indispensable – at an electronic crime scene,

See National Institute of Justice, *Electronic Crime Scene Investigation: A Guide for First Responders* at 23-24 (NCJ 187736, July 2001)

- **Online, undercover investigations**

  Cyber crime units that choose to engage in proactive, online investigations (e.g., chat room investigations to detect child predators) have particular needs.

  See "Setting up an Online Investigative Computer: Hardware, Connectivity and Software Recommendations," by Keith Daniels (SEARCH Group, Inc.) (2004)

- **Cell phone/hand-held forensics**

  Investigations involving seizure and examination of cell phones and other hand-held and hybrid devices require specialized equipment, tools, and techniques.

  See "Creating a Cell Phone Investigation Toolkit: Basic Hardware and Software Specifications," www.search.org/files/pdf/CellphoneInvestToolkit-0806.pdf

- **Internet Crimes Against Children grants**

  Special protocols on equipment, personnel, and space are mandated, including, for example:

  - ICAC computers and software are reserved for exclusive use of ICAC personnel. No personally owned equipment shall be used in ICAC investigations and all software shall be properly acquired and licensed.

  - In general, ICAC online investigations must be conducted in government workspace as designated by the agency.

§4.3. FORENSICS CAPABILITY

Digital evidence is information stored or transmitted in binary form that may be relied on in court. The ubiquity of digital evidence, its wide use in criminal activity, and the special challenges that it presents for law enforcement require that all states be able to support investigators and prosecutors through

skilled computer forensics.

§4.3.1. COMPUTER FORENSICS

Forensics is the application of scientific techniques of investigation to the problem of finding, preserving, and exploiting evidence to establish an evidentiary basis for arguing about facts in court.

Computer Forensics is the scientific study and use of processes involved in the identification, preservation, recovery, extraction, examination, interpretation, documentation, and presentation of the contents of computer media (digital evidence) for evidentiary and/or root cause analysis. Usually pre-defined procedures are followed, but flexibility is expected and encouraged because the unusual will be encountered.

> *See* Warren Kruse and Jay Heiser, Computer Forensics: Incident Response Essentials (2002)

Digital forensics is preferred by some when referring to the application of forensics to information stored or transmitted by computers but *computer forensics* remains in common use.

- **Features of Digital Evidence and Computer Forensics Methodology**

  - Digital evidence can be duplicated exactly.
  - Computer forensics requires duplication of the original evidence so that a copy can be examined as if it were the original.
  - Computer forensics involves both data recovery and analysis.
  - Even if "deleted," digital evidence can be recovered from computer media (at least until completely overwritten).

- Even when attempts have been made to destroy digital evidence, it can remain and be detected.

- Computer forensics is governed by valid laboratory principles.

- **Guiding Principles**

  - The rules of evidence apply to digital evidence.

  - Actions taken to secure, collect, and analyze digital evidence should not change the evidence in any way (i.e., not affect the integrity of the evidence).

  - Persons accessing or conducting examinations of digital evidence should be trained for that purpose.

  - All activity relating to the seizure, access, examination, storage, or transfer of digital evidence must be fully documented and that documentation must be preserved and available for review.

§4.3.2. BASIC MODEL OF COMPUTER FORENSICS

Computer forensics is typically reactive and after-the-fact – essentially the "post-mortem" examination of media to gather digital evidence from hard drives, disks, etc. The following briefly describes the steps that must be taken.

- ***Policy and Procedure Development***

  - Effective computer forensics capability requires that policies and procedures be in place to govern the unit's or task force's functions and operating parameters.

- ***Assessment***

  - Forensic examiners should assess digital evidence thoroughly with respect to the scope of the case to determine the course of action to take. This includes review of the search warrant or other legal authorization, consultation with the case investigator (goals and avenues of investigation, search terms, etc.), assessment of the hardware and software anticipated and of the location where they will be found, and planning of steps to acquire the evidence.

- ***Acquisition / Preservation***

  - *in general*

    - Proper "bag & tag" procedures are employed to protect and preserve the integrity of the computer and/or media.

    - Hard drives or other media are duplicated to create bit-stream images – each is a "forensic copy" that preserves everything on the drive or disk.

    - At least two copies of the bit-stream forensic image are made.

    - A strict chain of custody is established.

  - *special cautions due to the nature of computers and digital evidence*

    - Improper shutdown of networked computers may cause loss of evidence, damage to the network system, disruption of a business, and potential civil liability.

- Collection and transportation of computer evidence must reflect awareness of the susceptibility of the evidence to damage or alteration. Concerns include electro-magnetic fields from static, radio transmitters, speaker magnets etc., and heat, cold, or humidity (e.g., from placement on heated seats or prolonged storage in the trunk of a patrol car).

- Exposure to shock and vibrations during transport can cause damage or alteration.

- Evidence such as times, dates, or system information in battery-powered devices may be lost or altered due to the passage of time or prolonged storage if the batteries are allowed to discharge.

- ***Authentication***

  - The evidence is proven to be exactly what the suspect left behind, generally through calculation of *hash values* of the original evidence and the forensic copies.

  - The strict chain of custody, with limited personnel access, is maintained.

  - The examiner conducts *validation of tools* (hardware, software, methods, etc.) to ascertain and demonstrate reliability of the tools and the results.

- ***Analysis/Examination***

  - Unlike other types of evidence, analysis can be performed on an exact copy of the original.

- A forensic copy (never the original) is examined in a controlled environment.

- Time stamping/hash code techniques can be used to prove evidence has not been compromised.

- A specialist recovers, extracts, and analyzes data in all of the following:

  - present/active files (documents, spreadsheets, images, email, etc.)
  - all file system types
  - archive files (backups)
  - deleted files
  - "slack" space
  - other unallocated space
  - swap space
  - temporary files (cache, print records, temporary Internet files, etc.)
  - encrypted or otherwise hidden files
  - compressed or corrupted files
  - non-partitioned areas

- The specialist also examines how the computer was being used.

- ***Reporting***

  - All steps, actions, and observations are documented.

  - All findings and the results of automated processes are reported.

  - If necessary, testimony is given.

§4.3.3. SPECIAL AND EMERGING ACTIVITIES OR PROCESSES

As computer forensic techniques evolve in response to ever

changing technologies and due to expanding knowledge, specialized forensic "models" or processes are emerging to modify or supplement the model set out in §4.3.2.

Variations include:

- **Rolling forensics** ("on-site previewing")
    - Uses write blocking hardware and software for on-site previewing, enabling on-site "triage" to find evidence and determine whether an image should be made or the computer seized for off-site examination.
    - Useful in knock-and-talk situations or for probation and parole officers to monitor compliance with conditions of release.
- **Hand-held** (or "Mobile" or "Portable Electronic Device") **forensics**
    - Specialized techniques and tools to examine small devices with embedded computers and memory, such as cellular phones, wrist watches, personal digital assistants (PDAs), digital cameras, and hybrid devices.
    - Preserves and examines data on solid-state devices.
- **CD and DVD forensics**
    - Preserves and examines data stored on optical devices.
- **Live forensics**
    - Bag and tag procedures for when a running

computer is encountered (especially in home and small office networks).

- Used to acquire or analyze evidence in volatile memory, such as RAM.

- **Network forensics**

  - Captures, records, and analyzes events occurring on a functioning/operating computer network.

  - Useful for intrusion detection, monitoring, etc.

  - Involves examining audit logs; traffic, time, and packet analysis; session reconstruction; and identifying connections.

- **Software forensics**

  - Examination of computer code or text and analysis of data to determine authorship.

  - Examination of questioned *electronic* documents.

§4.3.4. FOR MORE INFORMATION

Scientific Working Group on Digital Evidence (SWGDE), *Best Practices for Computer Forensics*, Ver. 2.1 (July 2006)

United States Secret Service, *Best Practices for Seizing Electronic Evidence, A Pocket Guide for First Responders* (v. 3)

National Institute of Justice, *Forensic Examination of Digital Evidence: A Guide for Law Enforcement*, NCJ 199408, Special Report (April 2004)

National Institute of Justice, *Electronic Crime Scene*

Investigation: A Guide for First Responders, NCJ 187736, Guide (July 2001)

§4.4. PRIORITIZATION OF CASES: AN EXAMPLE

No prosecutor's office can accept every request for service or case referral that comes to its attention. Many factors affect the decision to accept cases, including the original jurisdiction the state agency has, the level of cooperation between agencies, the type of crime, and multi-state or international aspects of the crime. Such considerations are beyond the scope of this Guide.

Instead, this section highlights one important aspect of the case screening process, establishing priorities among accepted cases, which is a major concern due to the high volume of cases involving digital evidence.

The following chart, created by Maryland State Police's Technical Investigation Section's Digital Evidence Laboratory, provides a good example of the difficult decisions that must be made in creating priorities among cases:

Priority 1	Immediate Priority – Immediate threat to life and / or property or cases designated by the Unit Commander: ● Homicide ● Child Endangerment w/ Suspect-at-Large ● Crimes of Violence w/ Suspect-at-Large
Priority 2	High Priority – Potential threat to life and / or property: ● Critical missing child / computer involved ● Child Endangerment / molestation cases ● Solicitation for Sex Cases (involving minors)
Priority 3	Moderate Priority – Low potential threat to life and/ or property: ● Child Pornography
Priority 4	Low Priority – No potential threat to life and/or property: ● Theft cases; losses greater than $20,000 ● Exam needed to further current investigation
Priority 5	Lowest Priority – No potential threat to life or pending court dates: ● Property Crimes w/no pending deadlines ● General Criminal Intelligence

§5. FUNCTIONS OF A CYBER CRIME UNIT

§5.1. INVESTIGATION

There are two basic approaches to the investigation of cyber crime: proactive and reactive.

- *Reactive*

  Reactive cases usually result from citizen contacts, victim complaints, referrals from other law enforcement agencies, or complaint screening entities.

- *Proactive*

  A proactive case is one where the cyber crime unit or task force initiates the investigation that leads to prosecution.

  - Media interest in these types of cases raises public awareness of the agencies who engage in such investigations.

  - Proactive investigations can be highly effective. For example:

    - *Florida* – An investigator with the Attorney General's office assumed the identity of a 13-year-old boy that led to a guilty plea for sexual solicitation of a minor and a 10 year sentence for a man who intended to have a sexual encounter. Five years of sex offender probation was added, requiring electronic monitoring and registration as a sex offender.

    - *Michigan* – A man was arrested after disseminating sexually explicit material

to an individual he believed was a 14-year-old girl, but who was actually an investigator with the Attorney General's office.

- *New Mexico* – A former police officer received a 6 ½ year sentence for, *inter alia*, child solicitation by computer, harassment, and attempted criminal sexual penetration when he traveled to meet and have sex with a 15-year-old girl but who was, instead, an investigator with the Attorney General's Internet Crimes Against Children Unit.

- *Pennsylvania* – An undercover agent with the Attorney General's Child Predator Unit assumed the identity of a 12-year-old girl as part of an Internet "child sex sting" operation that resulted in multiple arrests.

- *South Carolina* – In a sting conducted by the Internet Crimes Against Children Task Force, the Attorney General's office arrested a man for criminal solicitation of minor after he used his computer web cam to solicit sex and demonstrate sex acts to an individual he believed was a 13-year-old girl but who was, instead, a sheriff's deputy working with the task force.

§5.2. PROSECUTION

The ultimate goal is to obtain convictions against individuals who perpetrate cyber crimes. For example:

- *Arizona* – Attorney General's office announced that a man was sentenced to 17 years in prison after pleading guilty to one count of sexual exploitation of a minor. By statute, he is required to serve the entire sentence.

- *Florida* – Attorney General's office announced the 10 year prison sentence of a man convicted of sexually soliciting a minor in a case prosecuted by the Attorney General's Office of Statewide Prosecution.

- *Massachusetts* – Attorney General's office announced a conviction for attempted dissemination of child pornography, possession of child pornography, and possession with intent to distribute obscene matter.

- *Virginia* – Attorney General's office announced that a man was found guilty of 127 counts of possession of child pornography and 26 counts of reproduction of child pornography.

§5.3. ASSISTANCE WITH LEGISLATIVE PROCESS

Due to the specialized nature and rapid evolution of cyber crime, AG offices can provide essential information and data that clarifies issues for state legislators attempting to craft cyber crime legislation. For example:

- *Kansas* – Attorney General's office assisted the state Senate Judiciary Committee, which introduced two bills that targeted sex offenders, including requiring that sex offenders register their e-mail addresses and online identities.

- *North Carolina* – Attorney General's office recommended changes to state laws to stop child predators, including increased penalties for soliciting minors for sex over the Internet, requiring social networking sites to get parental permission before allowing minor children to join the site, and requiring

that computer technicians and photo developers report child pornography to law enforcement.

- *Virginia* – Attorney General's office proposed legislation requiring e-mail addresses and online identity information to be included on the Sex Offender Registry, minimum sentences for the production and financing of child pornography and online solicitation of minors, allowing out-of-state warrants to go directly to Internet Service Providers, and funding for the Youth Internet Safety Fund for Prevention and Awareness Campaign.

§5.4. EDUCATION/PUBLIC OUTREACH

Some AG offices undertake public awareness activities for two reasons:

- Increased public awareness changes citizen behavior, reducing the incidence of cyber crime.

- Increased public awareness of cyber crimes generally, and the work of the AG's office specifically, builds support for efforts to combat cyber crime.

Note: Public educational efforts include publication and dissemination of brochures, public service announcements, and public speaking engagements (often with an emphasis on schools and youth). There are numerous organizations that can assist with such efforts by providing materials, training, and even lesson plans.

For example:

- *Arizona* – Attorney General's office made an Internet safety presentation for sixth through eighth graders in Ahwatukee, Arizona. The presentation emphasized precautions young people should take on social

networking sites and provided examples of teens who had been victims of Internet exploitation.

- *Alabama* – Attorney General's office sponsored a conference "*Lost in Cyberspace,*" designed to help parents keep their children safe on the Internet. The program included information on current trends in Internet crimes and discussed social networking sites. Printed materials were distributed to help parents "translate" chat room language and understand how chat rooms work.

- *Iowa* – Attorney General Tom Miller delivered a speech at *"Internet Safety: Information for Teachers, Parents and Communities,"* designed to introduce teachers and administrators to Internet safety issues.

- *Mississippi* – Attorney General's office makes presentations to parents, educators, students, and the community on Internet victimization. In 2006, 26 presentations were made to 1000 members of the public and 7 presentations made to 1700 students at schools. The office actively uses NETSMARTZ software.

§5.5. SPECIALIZED LEGAL TRAINING

Because of the specialized nature of cyber crime, including search and seizure principles and practices, new laws, and complicated forensic evidence, procedures in and out of the courtroom have changed significantly. Specialized training opportunities for the following groups are important:

- Prosecutors in AG cyber crime units and task forces

- Local prosecutors

- Law enforcement officers

- Warrant drafters / issuers

  Note: "Warrant issuers" are included here because some courts treat the search and seizure of computers as a special category, requiring unique language in warrants detailing what may be searched and how, with a focus on the technical aspects of obtaining digital evidence.

§6. FUNDING SOURCES AND ALTERNATIVES

§6.1. LEGISLATIVE FUNDING

This is the most sustainable source, especially for start-up funding, but results from a lengthy process that requires a significant lobbying effort.

Approaches to obtaining legislative funds

- Educate legislature and governor's office with accurate and supportable statistics on state cyber crime.

  Good source for compiling statistics: www.ic3.gov (Internet Crime Complaint Center web site). Its annual report compiles for each state:

  - Total number of complaints received.
  - Most prevalent computer crimes by percentage.
  - Median dollar amount lost to computer crime.
  - Amount lost by individuals by type of computer crime.

- "Economy of scale" argument: it is not economical for every local jurisdiction to create and operate a cyber crime unit. AG's office could manage state caseload in cooperation with local law enforcement.

- Develop united front with other state agencies in emphasizing need for cyber crime initiative.

Example: New Hampshire Attorney General's Office collaborated with other state agencies to develop strategic plan to address cyber crime in 2004. Multi-year plan to:

- *Provide cyber crime investigation and prosecution training.*
- *Track state's investigative capabilities.*
- *Develop and deliver statewide cyber forensics capabilities.*

Result: New Hampshire Legislature appropriated $238,000 for cyber crime effort.

- *Legislative funding example*: In 2006 Florida Legislature passed legislation establishing cyber crime unit within Florida Attorney General's office. In FY 2005-06, Legislature funded four positions and provided $411,350.

§6.2. FEDERAL GRANTS

§6.2.1. INTERNET CRIMES AGAINST CHILDREN (ICAC) GRANTS

- ICAC grants are largest source of funds for state and local cyber crime capability.
  - Program created by Office of Juvenile Justice and Delinquency Prevention to help states and locals respond to child predators on the Internet and child pornography.
  - Program details:
    - Applicants submit plan to create and foster multi-disciplinary task force to

prevent Internet crimes against children in a defined region. Plan must contain proactive component (online undercover investigations, usually based in Internet chat rooms).

- What grant covers (very few restrictions):
  - Personnel
  - Training
  - Specialized equipment
- Typical budget: $300,000 for 18-month period with no state matching funds required.
- Grantees can also send personnel to ICAC training programs at no cost - states only pay for transportation and meals.

  Example: Program pays for five task force members to attend annual Crimes Against Children Conference in Dallas, which has extensive curriculum tracks, including hands-on training.

■ Example of what can be accomplished with an ICAC grant:

Louisiana's statewide task force is composed of 42 local agencies with the AG's office providing coordination and oversight. The first grant of $300,000 was used to fully fund three staff members: prosecutor; investigator; forensic computer examiner. It also purchased two new crew cab pick-up trucks with mobile and portable 800 Mhz radios.

A $400,000 renewal of the grant was approved based on the task force's performance, with the new funds fully funding the original three employees, including a cost of living increase, training for task force members from the Attorney General's office, and the purchase of a new sport utility vehicle with a distinctive, highly visible exterior to make it attractive to young people during school demonstrations. The vehicle was also equipped with satellite communications capability for use as a mobile computer forensics platform.

- ICAC program status

  Currently 45 ICAC task forces in operation, including those in the offices of Attorneys General of Hawaii, Illinois, Louisiana, Michigan, New Mexico, North Dakota, Oregon, South Carolina, South Dakota, Texas, Utah, and Wisconsin. (Other ICAC task forces may involve participation from AG offices.)

  The Adam Walsh Child Protection and Safety Act. (Public Law No. 109-248, July 2006) appropriated funding for a minimum of 10 additional ICAC task forces.

- Alternate program: Investigative Satellite Initiative (ISI)

  - For jurisdictions lacking sufficient personnel resources for full time ICAC task force.

  - Funding for specialized equipment and training.

§6.2.2. GRANTS AUTHORIZED BY ADAM WALSH ACT - NOT YET AVAILABLE

- Grants to investigate sexual exploitation of children are to be implemented by Bureau of Justice Assistance, with funding for 2007-08.

- Grants for the development and implementation of educational programs for parents and children on best ways to stay safe on the Internet are to be implemented by DOJ, with funding for 2007-11.

§6.2.3. SEARCHING FOR OTHER FEDERAL GRANTS

- Other grant programs do not address combating cybercrime specifically, but this does not mean that grant money cannot be so used. A possible approach could identify the common elements of cyber crime and the goals of the grants.

  Example: The Weed and Seed Communities Competitive Program grant provides grants to combat violent crime and drug abuse at the neighborhood level. In seeking cyber crime funding, one might use the nexus of the Internet as a source of drug sales. Although this does not guarantee the acceptance of such an application, it is an example of how to think broadly when searching and applying for a grant.

- Best web sites to search for federal funding:

  - www.grants.gov

    - Official federal government web site for funding opportunities.
    - Can search by keyword, category, or federal agency.
    - Can also sign up to be notified by email of grant announcements.

- www.ojp.usdoj.gov/funding

  - Posts DOJ funding opportunities with links to grant announcement.

§6.3. PRIVATE FOUNDATION GRANTS

www.fdncenter.org – lists private, corporate, and community foundations and is searchable by grant maker and geographical area.

§6.4. OTHER CREATIVE SOURCES OF FUNDING

- Partnerships with other state agencies, universities, or private organizations.

- Settlement funds from litigation.

APPENDIX A. FEDERAL COMPUTER CRIME STATUTES

*This section outlines federal legislation used to combat cyber crime. It is useful to define cyber crime in reference to the function that the computer plays in the crime. There are three basic roles that the computer can play in a crime: it can be the **target**, the **tool**, or the **container**. Legislation dealing with substantive crimes involving computers tend to focus on instances in which the computer is the target or the tool. Therefore, this outline focuses on these two categories.*

§A.1. THE COMPUTER AS TARGET

Note: These crimes are technology-specific and did not exist prior to the spread of computer technology and networks. Examples of crimes include hacking, virus dissemination, fraud, and denial of service attacks.

- **Computer Fraud and Abuse Act (CFAA) 18 U.S.C. § 1030 (2000)** and its amendments under the **Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001 (USA PATRIOT ACT)**

  - *Note: CFAA is the primary federal statute aimed at combating computer crime. It applies to conduct aimed at a "protected computer," which is any computer connected to the Internet. The USA Patriot Act broaden the scope of culpable conduct.*

  - Criminal offenses under § 1030(a):

    - (1): accessing and subsequently transmitting classified government information without authority or by exceeding authority;

    - (2): obtaining, without authorization or by exceeding authority, information from financial

institutions, United States government, or protected computer;

- (3): intentionally accessing and affecting a U.S. department or agency nonpublic computer without authorization;

- (4): accessing, without authorization or by exceeding authority, a protected computer with the intent to defraud and obtain something of value;

- (5): (anti-hacking/anti-cracking provision) prohibits the following acts without authority:

  - knowingly causing the transmission of a program, information code, or command and intentionally causing damage to a protected computer; or
  - intentionally accessing a protected computer and recklessly causing damage; or
  - intentionally accessing a protected computer and negligently causing damage.

  To prove violation of (5), government must show that the conduct caused either:

  - loss exceeding $5000 in one year,
  - impairment of medical records,
  - harm to a person,
  - threat to public safety, or
  - damage to a computer system used by or for a government entity in furtherance of the

administration of justice, national defense, or national security.

Note: Loss is defined as any reasonable cost to the victim including: costs incurred responding to an offense, conducting a damage assessment, remedying any system damage, revenue lost, or any cost or consequential damages due to interruption in services.

- (6): with the intent to defraud, trafficking in passwords that would permit unauthorized access to a government computer or affect interstate or foreign commerce; and

- (7): transmitting in interstate or in foreign commerce any threat to cause damage to a protected computer with intent to extort something of value.

- **The Electronic Communications Privacy Act (ECPA), 18 U.S.C. §§ 2510-2521, 2701-2710 (2000)**

  - *Note: ECPA updated existing federal prohibitions against intercepting wire and electronic communications.*

  - Offenses:

    - § 2701(a) addresses stored communications. It is a crime to intentionally access without authority, or by exceeding authority, a facility through which an electronic communication service is provided and thereby obtain, alter, or prevent access to the wire or electronic communication while it is in storage.

- § 2511 addresses communications in transit. It is a crime to intentionally intercept, use, or disclose (or attempt to do so) any wire, oral, or electronic communication.

§A.2. THE COMPUTER AS TOOL

Note: A computer is a tool used to commit many traditional crimes, for example, child pornography, stalking, identity theft, copyright infringement, and mail and wire fraud.

- **18 U.S.C. § 875 (2000)** addresses online harassment and threats
  - Criminalizes the transmission of the following communications in interstate or foreign commerce:
    - demand for ransom for the release of any kidnaped person;
    - intent to extort money;
    - threat to injure a person; or
    - threat to damage property.
- **18 U.S.C. § 2261A (2000)** addresses online stalking
  - Criminalizes using any facility of interstate or foreign commerce to engage in a course of conduct that places a person in reasonable fear of death or serious bodily injury to themselves or to a family member.
- **Controlling the Assault of Non-Solicited Pornography and Marketing Act of 2003 "CAN-SPAM", 15 U.S.C. §§ 7701-7713, 18 U.S.C. § 1037(a)**
  - *Note: Enacted to establish a national standard for commercial email solicitations.*

- Definition of commercial electronic mail message: any electronic mail message, the primary purpose of which is the commercial advertisement or promotion of a commercial product or service.

- Businesses and marketers can send unsolicited emails to anyone with a computer if they:

  - identify themselves clearly;

  - do not use fraudulent headers; and

  - honor consumer requests to stop sending them unsolicited commercial email.

- Criminal Acts:

  - using a protected computer without authorization to relay email messages so as to prevent the email from being traced back to its sender

  - sending a message containing sexually explicit material without a warning label

- **Child Pornography Statutes**

  - *Note: Federal child pornography statutes are codified at 18 U.S.C §§ 2251-2260, which are powerful tools in outlawing the production, receipt, transportation, and possession of child pornography through all means, including computers. Portions have been modified through subsequent amendments and narrowed by Ashcroft v Free Speech Coalition, 535 U.S. 234 (2002), which held that child pornography must be of actual children rather than virtual images. The two major child pornography statutes are 18 U.S.C. § 2252 and 18 U.S.C. § 2252A*

18 U.S.C. § 2252

- Offenses:
  - (1) knowingly transporting or shipping in interstate or foreign commerce a visual depiction of a minor engaging in sexually explicit conduct,
  - (2) receiving or distributing such depictions that have been sent in interstate or foreign commerce, or which contain materials that have been transported in interstate commerce, or reproducing such materials for distribution in interstate or foreign commerce,
  - (3) selling or having possession of such depictions with intent to sell,
  - (4) possessing such depictions.

18 U.S.C. § 2252A
§ 2252A imposes essentially the same prohibitions as §2252, described above, while adding two offenses.

- Offenses:
  - (1) knowingly advertising, promoting, distributing or soliciting through the mails, or in interstate/foreign commerce by any means, including computer, any material in a manner that reflects the belief, or is intended to cause another to believe, that the material is an obscene depiction of a minor engaging in sexually explicit conduct or a visual depiction of a minor engaging in sexually explicit conduct.

- (2) distributing or offering to a minor any visual depiction that is or appears to be of a minor engaging in sexually explicit conduct for the purpose of inducing a minor to participate in any activity that is illegal.

- **Prosecutorial Remedies and Other Tools to End the Exploitation of Children Today Act (PROTECT Act), 117 Stat. 650 (2003) codified in scattered sections of 18 U.S.C. and 42 U.S.C.**

  - *Note: Amended CPPA in response to the ruling of the Supreme Court in the Ashcroft decision.*

  - Offense to possess, manufacture, or distribute pornography containing visual depictions of:

    - a real child engaging in sexual acts or

    - a digital, computer, or computer-generated image that is, ***or is indistinguishable from***, that of a minor engaged in sexually explicit conduct.

- **18 U.S.C. § 2425 (2000)** addresses use of interstate facilities to transmit information about a minor

  - Offenses:

    - use the mail or any means of interstate or foreign commerce to knowingly initiate the transmission of the name, phone number, address, social security number or email address of one whom he knows to be under the age of 16 with the intent to solicit any person to engage in sexual activity for which that person can be charged with a criminal offense.

- Includes attempt to violate and, under 18 U.S.C. § 371, conspiracy to violate the provisions of the statute.

- **18 U.S.C. § 1341 (2000), 18 U.S.C. § 1343 (2000)** Mail and wire fraud

  - *Note: Although not aimed specifically at cyber crime, statutes addressing mail and wire fraud, are often applicable in prosecuting computer crimes.*

  - § 1341 - (mail fraud)

    - person devises or intends to devise a scheme to defraud; and

    - uses mail to execute that scheme.

  - § 1341 (wire fraud)

    - person intentionally participates in a scheme to defraud or to obtain money or property by means of false or fraudulent pretenses; and

    - uses wire transmissions to execute the scheme.

- **18 U.S.C. § 1029 (2000)** Fraud and related activity in connection with access devices

  - Definitions:

    - access device - "any card, plate, code, account number, electronic serial number, mobile identification number, personal identification number, or other telecommunications service, equipment, or instrument identifier, or other means of account access that can be used...to obtain money, goods, services, or any other thing of value."

- counterfeit access device - “any access device that is counterfeit, fictitious, altered, or forged or an identifiable component of an access device or a counterfeit access device.”

- Offenses to knowingly and with the intent to defraud:

  - produce, use or traffic in a counterfeit access device;

  - traffic in or use one or more access devices during a one year period thereby obtaining anything of value aggregating $1000 or more;

  - possess 15 or more counterfeit or unauthorized devices;

  - produce, traffic in, have control of or possess access device-making equipment;

  - conduct transactions with one or more access devices belonging to another to receive anything of value during any one year period aggregating $1000 or more;

  - solicit someone with an offer of an access device without authorization by the issuer of said device, or selling information regarding the application to obtain an access device;

  - use, produce, traffic in, or possess a telecommunications instrument that has been modified so as to obtain unauthorized use of telecommunications services;

  - use, produce, traffic in, or possess a scanning receiver;

- use, produce, traffic in, or possess hardware or software knowing it has been configured so as to obtain telecommunications services without authorization; or

- without authorization from the owner of a credit card, arrange for another person to present record(s) of transactions made by that access device to the owner for payment.

- Under The USA PATRIOT Act, it is also a crime if anyone acting outside the jurisdiction of the United States, engages in any conduct specified under § 1029, or attempts or conspires to do so, if :

  - the offense involves an access device issued by a financial institution or other entity within the jurisdiction of the United States; and

  - the article used in the commission of the offense is in the jurisdiction of the United States.

- **18 U.S.C. § 2314 (1994)** - Transportation of stolen goods

  - Crime to transport stolen goods worth $5000 or more in interstate or foreign commerce, including stolen computer hardware or data that is sent over the Internet.

- **The Identity Fraud and Theft Statute, 18 U.S.C. § 1028**

  - *Note: This is the primary identity theft statute as amended by the Identity Theft and Assumption Deterrence Act. The Act addresses the theft or criminal use of the underlying personal information, not just the*

fraudulent use, creation, or transfer of identification documents.

- Prohibited acts under § 1028(a):

  - knowingly and without lawful authority produce an identification document, authentication feature, or a false identification document;

  - knowingly transfer a false identification document, authentication feature, or false identification document knowing that it was stolen or produced without lawful authority;

  - knowingly possess with intent to unlawfully use or transfer, five or more identification documents, authentication feature or false identification documents;

  - knowingly possess an identification document, authentication feature or false identification feature or false identification document with the intent to defraud the United States;

  - knowingly produce, transfer, or possess a document-making implement or authentication feature with the intent that it be used in the production of a false identification document or another document-making implement or authentication feature which will so be used;

  - knowingly possess an identification document or authentication feature that is or appears to be an identification document or authentication feature of the United States or a sponsoring entity of an event designated as a special event of national significance which is stolen or produced without lawful authority knowing

that such document or feature was stolen or produced without authority;

- knowingly transfer, possess, or use, without lawful authority, a means of identification of another person with the intent to commit, or to aid and abet, or in connection with, any unlawful activity that constitutes a violation of Federal law, or that constitutes a felony under any applicable state law; or

- knowingly traffics in false or actual authentication features for use in false identification documents, document-making implements, or means of identification.

- **17 U.S.C. § 506(a) (2000)** Criminal copyright infringement

  - *Note: Protects rights of authorship in various kinds of intellectual property, including computer software.*

  - Elements for felony copyright infringement:

    - existence of a valid copyright;

    - infringement of the copyright by defendant;

    - defendant acted willfully; and

    - defendant reproduced or distributed at least ten copies of one or more copyrighted works with a total value of more than $2500 within a 180-day period.

  - Elements for misdemeanor copyright infringement:

    - existence of a valid copyright;

    - infringement of the copyright by the defendant;

- defendant acted willfully; and

- defendant reproduced or distributed the copyrighted material for commercial advantage or private financial gain or distributed or copied one or more copyrighted works with a value of more than $1000 within a 180-day period.

- **18 U.S.C. § 371** (2000): Used for conspiracies to commit criminal copyright infringement

- Defenses to charge of criminal copyright infringement

  - First sale doctrine - one who legally buys a copyrighted work may freely distribute that copy; only available as a defense to a charge of copyright infringement by distribution.

  - Accused did not act willfully - the No Electronic Theft Act amended 17 U.S.C. § 506(a) so it states that the evidence of reproduction or distribution of a copyrighted work, by itself, is not sufficient to establish willfulness

  - Fair use doctrine, 17 U.S.C. § 107 (1976) excepts the otherwise infringing use of a work where it is used for purposes such as criticism, comment, news reporting, teaching, scholarship, or research. Factors in determining fair use:

    - purpose and character of a use, including whether it is of a noncommercial nature;

    - nature of the work;

- ♦ amount and substantiality of the portion in relation to the copyrighted work as a whole; and

- ♦ effect of use upon potential market for the copyrighted work.

- **The Digital Millennium Copyright Act, 17 U.S.C. § 1201-05 (2000)**

  - *Note: enacted to ban the use of computers and other electronic devices to infringe against copyrights on traditional works and to prohibit circumvention of technological measures used to protect copyrighted works.*

  - Offenses:

    - ▸ §1201 - illegal to circumvent measures used to protect copyrighted works, including methods to de-scramble, decrypt, or otherwise impair or deactivate a technological measure.

    - ▸ §1202 - unlawful to tamper with copyright management information, which includes identifying information about the work, author, owner or performer of the work; the terms and conditions for use of the work; numbers or symbols relating to this information; or other information prescribed by the Register of Copyrights.

- **The Lanham Act, 15 U.S.C. § 1051-1141n (2000)**: Civil damages for trademark infringement

  - *trademark* - any word, name, symbol, device or combination thereof -

- used by a person, or
- which a person has an intention to use in commerce for which he has applied to register
- to distinguish his goods from others and identify the source of the goods, even if unknown.

- **The Trademark Counterfeiting Act**, **18 U.S.C. § 2320(a) (2000):** Criminal penalties
  - Offense:
    - intentional trafficking or attempted trafficking in goods or services;
    - use of counterfeit mark on or in connection with the goods or services; and
    - knowledge that the mark was counterfeit.

- **Economic Espionage Act of 1996 ("EEA"), 18 U.S.C. § 1831-39**
  - *Note: Purpose is to protect information guarded by reasonable secrecy measures, valuable because of its secrecy, and related to or included in a product in interstate commerce.*
  - Types of trade secret theft under EEA:
    - §1831: criminalizes the theft of trade secrets with the intent or knowledge that the offense will benefit a foreign entity.
    - § 1832: criminalizes commercial theft of trade secrets regardless of who receives the benefit. Elements:

- stealing, or without authorization of the owner, obtaining, conveying, or destroying information;
- knowledge that the information was proprietary; and
- information was, in fact, trade secret information.

APPENDIX B. REPRESENTATIVE STATE COMPUTER CRIME STATUTES

Every state has enacted some form of computer-specific legislation. Approximately half of the states modeled their statutes on the 1977 or 1979 versions of the proposed Federal Computer Systems Protection Act. Many state statutes categorize computers as to the function they play in a crime: computer as ***target*** of the crime; computer as ***tool*** used to commit a crime; and computer as a ***container*** to store evidence of a crime. That last category is not addressed here, given that the focus of such statutes is not unique to computer crimes. This survey, which is designed to be illustrative, not exhaustive, outlines the definitions of criminal statutes that address the unique issues posed by computers and information technology.

§B.1. Computer as the Target

- **Hacking and Cracking**
  - Common Definitions
    - *hacking* - gaining unauthorized access to a computer
    - *cracking or aggravated hacking* - gaining unauthorized access to computer to commit another crime, such as theft or vandalism
  - Typical Approaches
    - Most states use a **two-tiered** approach - defining simple hacking and aggravated hacking as two distinct crimes and treating simple hacking as a misdemeanor and aggravated hacking as a felony

      DEL. CODE ANN. tit.11, §§ 932 & 933 (1995)
      ALASKA STAT. §§ 11.46.484 & 11.46.740 (Michie 2000)

MD. CODE ANN., CRIM. LAW § 7-302 (1996)
VT. STAT. ANN. tit. 13, §§ 4102 & 4104 (Supp. 2004)
IOWA CODE ANN. § 716.6B (West Supp. 2004)

- Some states use a single statute to criminalize both activities
  CAL PENAL CODE § 502 (c) (West Supp. 2004)
  CONN. GEN. STAT. § 53a-251 (2003)
  IDAHO CODE § 18-2202 (Michie 1997)

- simple hacking - definitional variations in the characterization of the crimes:

  - defining simple hacking as "unauthorized access"
    CAL. PENAL CODE § 502 (West Supp. 2004)
    MD. CODE ANN., CRIM. LAW § 7-302 (1996)
    VT. STAT. ANN. tit. 13, § 4102 (Supp. 2004)

  - defining simple hacking as "computer trespass"
    ARK. CODE ANN. § 5-41-103 (Michie 1997)
    N.Y. PENAL LAW § 156.10 (McKinney 1998)

  - defining simple hacking as "unauthorized use" or "computer tampering"
    CAL. PENAL CODE § 502 (West Supp. 2004) (unauthorized use)
    ARIZ. REV. STAT. ANN. § 13-2316 (West 2000) (computer tampering)

- variations in aggravated hacking:

  - prohibits unauthorized access that results in the copying, alteration, and/or

deletion of data or damage to a computer system

GA. CODE ANN. § 16-9-93 (1999)
N.C. GEN. STAT. § 14-458 (Supp. 2004)

- ▸ crime to break into a computer or computer system with the intent to commit, attempt to commit, or further the commission of a felony

  N.Y. PENAL LAW § 156.10 (Michie 1998)

- ▸ crime to disseminate viruses, worms, and other malware

  720 ILL. COMP. STAT. 5/16D-3 (SUPP. 2004)
  ME. REV. STAT. ANN. tit.17, § 433 (1) (c) (West Supp. 2004)
  MICH. COMP. LAWS ANN.§ 752.795 (West 2004)
  MINN. STAT. Ann.§ 609.88(1) (c)
  NEB. REV. STAT.§ 28-1345 (1995)
  N.C. GEN. STAT. § 14-455 (Supp. 2004)

- **Denial of Service Attacks**

  - Definition

    Intentionally or knowingly engaging in a scheme or attack designed to deny access of information to users of a computer or computer system.

    18 PA. CONS. STAT. ANN. § 7612(a) (West Supp. 2004)

  - Approaches

    - criminalizing denial of service attacks

      CAL. PENAL CODE § 502 (West Supp. 2004)
      CONN. GEN. STAT. § 53a-251(d) (2003)
      DEL. CODE ANN. tit. 11, § 934 (2004)
      MISS. CODE. ANN. § 97-45-5 (1994)
      N.H. REV. STAT. ANN. § 638:17 (Supp. 2004)

N.C. GEN. STAT. § 14-456 (Supp. 2004)
OKLA. STAT. ANN. tit. 21, § 1953 (Supp. 2004)
W. VA. CODE § 61-3C-8 (2000)

- including denial of service in prohibition on distributing malware
  S.C. CODE ANN. § 16-16-10(k)(3) (Law Co-op. Supp. 2004)

- outlawing attempted denial of service attacks
  CONN. GEN. STAT. § 53-451 (2003)
  R.I. GEN. LAWS § 11-52-1 (2002)
  VA. CODE ANN. § 18.2-152.2 (Michie Supp. 2004)

§B.2. Computer as the Tool

- **Cyberstalking**
  - Approaches
    - require that the offender transmit a "credible threat" to injure the victim, the victim's family or any other person
      COLO. REV. STAT. ANN. § 18-9-111(1)(e) (West Supp. 2004)
      GA. CODE ANN. § 16-5-90(a)(1) (1999)

    - criminalize a course of conduct that would cause a reasonable person to suffer intimidation or serious inconvenience, annoyance or alarm, as well as fear of death or injury to themselves or to members of their family
      ARIZ. REV. STAT. ANN. § 13-2316(5) (West 2000)
      MASS. GEN. LAWS. 265 § 43A(A)(1) (2000)
      OKLA. STAT. tit. 21, § 1953 (Supp. 2004)

- **Spam**

  - *Note: Although the CAN-SPAM Act has preemptive effects with regard to state spam legislation, it does not preempt state laws to the extent that they relate to acts of fraud or computer crime.*

  - Approaches

    - prosecute spammers for fraud, false advertising, trespass, or other crimes

      VA. CODE ANN. § 18.2-152.3:1(A) (Michie)

    - violation of state's unsolicited electronic mail statute is a misdemeanor, unless:

      - there are a specified number of recipients in a certain time period, or

      - specified amount of revenue generated by a spam transmission

        VA. CODE ANN. § 18.2-152.3:1(B) (Michie Supp. 2004)
        ARK. CODE ANN. § 5-41-205 (Michie Supp. 2004)
        DEL. CODE ANN. tit. 11, §§ 937(2) & 937(3) (2004)
        ILL COMP. STAT. §§ 5/16D-3(a)(5) & 5/16D-3 (a-5)(Supp. 2004)
        LA. REV. STAT. ANN. § 14:73.6(B) (West Supp. 2004)
        NEV. REV. STAT. 205.492(1)-(3) (Supp. 2004)
        18 PA. CONS. STAT. § 7661 (West Supp. 2004)
        TENN. CODE ANN. § 39-14-603(a) (Supp. 2004)

- **Cyber Crimes Involving Minors**

  - Soliciting Minor for Sex

- crime to use a computer to solicit a child for sex

  ALA. CODE § 13A-6-110 (1994 & Supp. 2000)
  CAL. PENAL CODE § 288.2 (West 1999)
  GA. CODE ANN. § 16-12-100.2 (1999 & Supp. 2000)
  IND. CODE § 35-42-4-6 (1998)
  N.M. STAT. ANN. § 30-37-3.2 (Michie Supp. 2000)

- offense is committed if perpetrator believed the person he was soliciting for sex was a minor

  720 ILL. COMP. STAT 5/11-6 (Supp. 2004)
  IND. CODE § 35-42-4-6 (1998)
  ME. REV. STAT. ANN. tit. 17A, § 259 (West Supp. 2004)
  MICH. COMP. LAWS. ANN. § 750.145(a) (West 2004)
  OKLA. STAT. Tit. 21, § 1040.13(a) (Supp. 2004)
  S.D. CODIFIED LAWS §22-22-24.5 (Michie Supp. 2004)
  TEX. PENAL CODE ANN. § 15-031 (Vernon Supp. 2004)

- more serious offense to use a computer to solicit a child than to do so in person

  IND. CODE § 35-42-4-6 (1998)

■ Child Pornography & Virtual Child Pornography

- prohibit using computer to create, store and/or distribute child pornography

  CAL. PENAL CODE § 311.11 (West 1999)
  FLA. STAT. Ch. § 847.0135 (2000 & Supp. 2001)
  720 ILL. COMP. STAT., 5/11-20.1 (1993 & SUPP. 2000)
  18 PA. CONS. STAT. ANN. § 6312 (West 1983 & Supp. 2000)
  WYO. STAT. ANN. § 6-4-303 (2000)

- prohibit using computer to send obscene material to a child

  ALA. CODE § 13A-6-111 (1994 & Supp. 2000)

GA. CODE ANN. § 16-12-100.1 (1999 & Supp. 2000)

- prohibit reproduction of sexually explicit images of real children, whether by a computer or by other means

  VA. CODE ANN. § 18.2-374.1

- **Cyber crimes involving Fraud and Other Traditional Misconduct**

  - Forgery

    - computer forgery is a distinct offense, separate from forgery

      GA. CODE ANN. §16-9-93(d) (1999)
      NEV. REV. STAT. § 205-.481 (Supp. 2004)
      VA. CODE ANN. § 18.2-152.14 (Michie 1996)
      W.V. CODE § 61-3C-15 (2000)

    - crime to possess forgery devices including computer equipment and software "specifically designed or adapted to such use"

      N.J. STAT. ANN. §2C;21-1 (c) (West Supp. 2004)

  - Fraud and Theft

    - using computer to commit fraud

      ARIZ. REV. STAT. ANN. § 13-2316(1) (West Supp. 2004)
      CAL. PENAL CODE § 502(c)(1)(A) (West Supp. 2004)
      HAW. REV. STAT. § 708-891 (Supp. 2004)
      KY. REV. STAT. ANN. § 434.845 (Banks-Baldwin Supp. 2004)
      LA. REV. STAT. ANN. § 14:73.5 (West 1997)
      N.J. STAT. ANN. § 2C:20-25©) (West Supp. 2004)
      OR. REV. STAT. § 164.377(2)(a) (Supp. 2004)
      VA. CODE ANN. § 18.2-152.3 (Michie Supp. 2004)

- using computer to commit fraud included in aggravated hacking statute
  - ARIZ. REV. STAT. ANN. § 13-2316(A)(1) (West Supp. 2000)
  - KY. REV. STAT. ANN. § 434.845 (Banks-Baldwin Supp. 2004)

- increased penalties for aggravated hacking if done to defraud
  - ALA. CODE § 13A-8-102(d)(2) (Supp. 2004)
  - DEL. CODE ANN. tit. 11, § 854 (2004)
  - MO. ANN. STAT. § 569.095 (2) (West Supp. 2004)

- embezzlement crimes incorporated into computer fraud statutes
  - N.M. STAT. ANN. § 30-45-3 (Michie 1994)
  - VA. CODE ANN. § 18.2-152.3 (Michie Supp. 2004)

- prohibit computer theft which encompasses various crimes including information theft, software theft, theft of computer services, and using computer to steal other types of property
  - COLO. REV. STAT. § 18-5.5-102(1)(d) (2000)
  - LA. REV. STAT. ANN. § 14:73.2 (West 1997)
  - IDAHO CODE § 18-2202 (Michie 1997)
  - MICH. COMP. LAWS ANN. § 752.795 (West 2004)
  - MINN. STAT. ANN. § 609.89 (West Elec. Supp. 2004)
  - R. I. GEN. LAWS § 11-52-4 (2002)
  - UTAH CODE ANN.§ 76-6-703 (1999)

■ Extortion

- computer extortion included within the definition of computer fraud
  - ARK. CODE ANN. § 5-41-103 (Michie 1999)
  - CAL. PENAL CODE § 502 (West Supp. 2004)
  - OKLA. STAT. tit. 21, § 1953 (Supp. 2004)

- computer extortion imported into general extortion statute

HAW. REV. STAT. § 706-764 (Supp. 2004)

- computer extortion statute incorporates computer hacking and cracking statute
  N.C. GEN. STAT. § 14-457 (1999)

■ Identity Theft / Identity Fraud

- common elements in state identity theft / identity fraud statutes:
  - ▸ knowingly,
  - ▸ with intent to defraud for economic benefit,
  - ▸ obtaining, possessing, transferring, using, or
  - ▸ attempting to obtain, possess, transfer or use,
  - ▸ one or more identification documents or personal identification number of someone else

    ALA. CODE § 13A-8-192(a) (Supp. 2004)
    CAL. PENAL CODE § 530.5 (West Supp. 2004)
    CONN. GEN. STAT. § 53a-129a (2003)
    DEL. CODE ANN. tit. 11, § 854 (2004)
    GA. CODE ANN. § 16-9-121 (Supp. 2004)
    IOWA CODE § 715A.8 (Supp. 2004)
    MASS. GEN. LAWS ANN. Ch. 266, § 37E (West 2000)
    MISS. CODE ANN. § 97-45-19 (Supp. 1994)
    OKLA. STAT. ANN. tit. 21, § 1533.1 (Supp. 2004)
    18 PA. CONS. STAT. ANN. § 4120 (West Supp. 2004)

- prohibiting trafficking in identities or identity information

  ALA. CODE § 13A-8-193(a) (Supp. 2004)
  KY. REV. STAT. ANN. § 514.160

- enhanced penalties if the victim is over sixty or disabled

  ILL. COMP. STAT. § 5/16G-20 (1999)

■ Cyber Terrorism

- Arkansas - incorporates cyber terrorism into its terrorism statute

  ARK. CODE ANN. § 5-54-204 (Michie 2004)

- Connecticut - has computer crime in furtherance of terrorist purpose offense

  CONN. GEN. STAT. § 53a-301(a) (2003)

- Indiana - computer tampering offense enhanced if act is committed for purpose of terrorism and further enhanced if committed for purpose of terrorism and results in serious bodily injury

  IND. CODE ANN. § 35-43-1-4 (West 2004)

- Illinois - includes disabling or destroying usefulness of a computer or computer network in its general definition of terrorism

  ILL. COMP. STAT. §§ 5/29D-10 (Supp. 2004)

- Georgia - prohibits using computer to disseminate information relating to terrorist acts

  GA. CODE ANN. § 16-9-121 (Supp. 2004)

- West Virginia - has "endangering public safety" offense, making it a felony to interrupt or impair utility services, medical services, or public communication service

W.V. CODE § 61-3C-14 (2000)

§B.3. Miscellaneous Cyber Crime Offenses

- Computer Invasion of Privacy
  using a computer to examine, without authority, any employment, salary, credit, financial or personal information about another person
  VA. CODE ANN. § 18.2-152.5 (Michie Supp. 2004)

- damaging or enhancing financial reputation or data record by entering false data into a computer
  ALASKA STAT. § 11.46.740 (Michie 2000)
  N.M. STAT. ANN. § 30-45-4 (Michie 1994)

- modifying or destroying equipment or supplies that are used, or are intended to be used in a computer, computer system, or computer network
  ALA. CODE § 13A-8-103 (SUPP. 2004)
  DEL. CODE ANN. TIT. 11, § 936 (2004)
  LA. REV. STAT. ANN. § 14:73.3 (WEST 1997)
  MISS. CODE ANN. § 97-45-7 (1994)
  WY. STAT. ANN. § 6-3-503 (MICHIE 1999)

- crime to modify data, programs, or documentation in a computer or computer system
  FLA. STAT. § 815.04(1) (SUPP. 2004)

- prohibit copying, receiving or using information that was obtained by violating a hacking or cracking statute
  ALA. CODE § 13A-8-102 (SUPP. 2004)
  CONN. GEN. STAT. § 53A-251 (2003)
  FLA. STAT. § 815.04 (SUPP. 2004)
  N.H. REV. STAT. ANN. § 638:17 (SUPP. 2004)

APPENDIX C. CYBER CRIME INVESTIGATION AND PROSECUTION AGENCIES

§C.1. Federal Agencies

- **Computer Crime and Intellectual Property Section (CCIPS)**

  Agency under Criminal Division of Department of Justice

  Emphasis: computer intrusion and intellectual property crimes

  Contact: www.cybercrime.gov; 202-514-1026 (also: www.usdoj.gov/criminal/cybercrime)

  Electronic crime search and seizure manual can be downloaded from web site

- **Child Exploitation and Obscenity Section (CEOS)**

  Agency under Criminal Division of Department of Justice

  Focus: child pornography and exploitation

  Contact: www.usdoj.gov/criminal/ceos/index.html; 202-514-5780

- **Federal Bureau of Investigation**

  Crimes Against Children (CAC) Program: investigates online child pornography and exploitation and other

crimes against children
www.fbi.gov/cid/cac/crimesmain.htm

Innocent Images Initiative: combats proliferation of child pornography images www.fbi.gov/innocent.htm

Infragard: develops partnerships with private sector to protect against attacks on critical infrastructure

- **Federal Trade Commission**

  Investigates consumer complaints, e.g., fraud and identity theft

  Enforces Children's Online Privacy Protection Act

  Contact: www.ftc.gov; for individual section phone numbers: www.ftc.gov/ftc/telephone.htm

- **Internet Crime Complaint Center (IC3)**

  IC3 is a partnership between the F.B.I. and the National White Collar Crime Center (NW3C).

  Emphasis: To serve as a vehicle to receive, develop, and refer cyber crime related criminal complaints.

  Contact: www.ic3.gov

- **United States Attorneys**

  - *Computer and Telecommunications Coordinator (CTC) Program*

Each U.S. Attorney designates a CTC, who receives cybercrime training, act as advisor to office, and prosecutes primarily intellectual property crimes

Contact: www.usdoj.gov/usao/offices

- *Law Enforcement Coordinating Committee (LECC) Program*

  Each U.S. Attorney designates a LECC coordinator, who fosters cooperation among law enforcement agencies through training seminars to local and state law enforcement

  Contact: LECC Coordinator for each US Attorney's office at www.usdoj.gov/usao/offices/personnel/ALM.html

- **U.S. Immigration and Customs Enforcement (DHS ICE)**

  The C3 Child Exploitation Section, (CES) part of the U.S. Department of Homeland Security (DHS) – Immigration and Customs Enforcement (ICE).

  Emphasis: Investigate trans-border cases of large-scale production and distribution of images of child exploitation.

  Contact: Operation.Predator@dhs.gov; or 1-866-DHS-2ICE.

The C3 Cyber Crime Center Pamphlet can be downloaded at: http://www.ice.gov/doclib/partners/investigations/services/cybercrimescenter.pdf

- **United States Secret Service (USSS)**

  U.S. Secret Service Electronic Crimes Task Force and Electronic Crimes Working Group.

  Emphasis: Investigate and provide support for cases that involve some form of electronic evidence.

  Contact: www.secretservice.gov

- **United States Computer Emergency Readiness Team (U.S.–CERT)**

  U.S.–CERT was established in 2003 to protect the nation's Internet infrastructure.

  Emphasis: U.S.–CERT acts to coordinate the defense against and responses to cyber attacks throughout the United States.

  Contact: www.us-cert.gov

§C.2. State and Local Agencies

- **Internet Crimes Against Children (ICAC) Task Forces**

State and local agencies funded by Office of Juvenile Justice and Delinquency Prevention at the Department of Justice to address Internet crimes against children (online child pornography and exploitation) in their geographic areas

Contact: www.icactraining.org provides map with link to task forces

- **County In-House Cyber Crime Units**

  Example: Westchester County, NY District Attorney's High Technology Crime Unit
  www.westchesterda.net/main.htm

  Contact: county and district attorneys
  www.ndaa-apri.org

- **State In-House Cyber Crime Units**

  Examples:

  - Mississippi Attorney General's Cyber Crime Unit
    www.ago.state.ms.us

  - Florida Attorney General's Cyber Crime Unit
    www.myfloridalegal.com

  Contact: state Attorney General's web site links at www.naag.org

§C.3. International Cyber Crime Prosecution

- **International Association of Prosecutors**

Organization of prosecutors from 40 countries, including the United States, who pledge cooperation on multinational crime, including cyber crime

Contact: www.iap.nl.com

- **Interpol**

  International police organization with 186 member countries, with high tech crime a core function

  Contact: www.interpol.int

APPENDIX D. NON-GOVERNMENTAL RESOURCES

§D.1. ORGANIZATIONS AND PROGRAMS

The following non-governmental resources provide information, resources, and training related to the investigation and prosecution of cyber crime. The website for each organization or program is generally the best way to access further information.

- **The National Center for Justice and the Rule of Law:**

  (www.NCJRL.org) located at the University of Mississippi School of Law (www.olemiss.edu/depts/law_school) offers four types of training:

  - *Prosecution Training***:** In partnership with the National Association of Attorneys General (www.naag.org), the NCJRL offers the only national training program to help combat computer-related crime for Attorney Generals' Offices from all 50 states.

  - *Judicial Training***:** In partnership with the National Judicial College, (www.judges.org) the NCJRL offers the only national training program for state trial and appellate judges about the search and seizure aspects of computer-related crime.

  - *Law Enforcement Training*: In partnership with Mississippi State University's Center for Computer Security Research, the NCJRL offers specialized courses for law enforcement officers involved in detecting and investigating computer-related crime.

  - *Law Student Training*: The NCJRL offers specialized courses, externship placements, and summer employment with prosecution-related organizations involved in combating computer-related crime.

- **NCJRL/NAAG online cyber crime newsletter:**

  A joint publication of the NCJRL and NAAG that describes current developments, including timely articles, legislative action, corporate initiatives and emerging caselaw in the field of computer-related crime. *See* www.NCJRL.org

- **Better Business Bureau Identity Theft Resource Site**

  (http://www.bbbonline.org/idtheft/index.asp): includes information, educational materials, and resources for businesses and consumers.

- **Business Software Alliance**

  (www.bsa.org): the "voice" of the software industry, dedicated to promoting a safe and legal digital world, works to educate consumers on software management and copyright protection, cyber-security, trade, e-commerce and numerous other Internet-related issues.

- **CyberSecurity Institute**

  (www.cybersecurityinstitute.biz): offers comprehensive computer forensics training and services aimed at attorneys, businesses, and individuals, including the CyberSecurity Forensic Analyst Certification.

- **Community Emergency Response Team (CERT)**

  (www.cert.org): home of the well-regarded CERT Coordination Center, located at Carnegie Mellon University's Software Engineering Institute, studies and provides resources in Internet security vulnerabilities, networked systems, and development and training related to computer security.

- **Crimes Against Children Research Center**

  (www.unh.edu/ccrc/): located at the University of New Hampshire (www.unh.edu), addresses crime victimization of children (birth through 17). It has four primary goals: (1) greater recognition of the extent of child victimization within the justice system; (2) enhanced protection of child crime victims; (3) rehabilitation of child crime victims; and (4) greater public accountability by evaluation of the justice system's policies and programs that are related to children.

- **CyberAngels**

  (www.cyberangels.org): online educational resource for parents, educators, and victims hosted by the online branch of New York's Guardian Angels.

- **Cyber Criminals Most Wanted**

  (www.ccmostwanted.com): focuses on cyber crime awareness, prevention, and safety.

- **Electronic Privacy Information Center**

  (www.epic.org): public interest research center that educates public on emerging issues of civil liberties, privacy, the First Amendment, and other constitutional values.

- **Forensic Association of Computer Technologies**

  (www.comp4n6.org): nonprofit association that provides technical training to law enforcement personnel based on paid membership.

- **Fox Valley Technical College**

  (www.fvtc.edu): nationally recognized leader in training students for careers in law enforcement and provides specialized training for current law enforcement officers in evolving areas such as computer-related crime.

- **High Tech Crime Consortium**

  (www.hightechcrimecops.org): offers cyber crime investigator training and education opportunities in computer forensic examination techniques; also assists in the development of software and other computer forensic examination tools.

- **High Technology Crime Investigation Association**

  (www.htcia.org): membership based association that promotes and facilitates voluntary interchange of information and knowledge about investigation of and security related to advanced technologies.

- **International Association of Computer Investigative Specialists**

  (www.iacis.info/iacisv2/pages/home.php): provides resources and benefits to its members through newsletters, file libraries, and list servs that promote the exchange of information and strategies to assist computer investigative specialists.

- **The National Center for Missing and Exploited Children**

  (www.missingkids.com): offers investigative assistance, resources, and training in cases involving child exploitation (both on-line and off-line) and efforts to recover missing children.

- **National White Collar Crime Center**

  (www.nw3c.org): nonprofit corporation that provides national support for agencies and offices involved in cyber crime detection, investigation, and prosecution; offers a wide-variety of training programs; and is a recognized and often-utilized resource for information related to sophisticated criminal activity.

- **Purdue University Center for Education and Research Information Assurance and Security**

  (www.cerias.purdue.edu): advances knowledge of information assurance and security through research, education, and by serving as an unbiased source of information on an international scale; and considered a world-wide leader in areas of information security crucial to protecting computing infrastructure.

- **The National Consortium for Justice Information Statistics (SEARCH)**

  (www.search.org): offers high tech crimes investigative training and a variety of computer-related crime resources to law enforcement and public safety agencies.

- **Southeast Region Forensics Training Center**

  (www.security.cse.msstate.edu/ftc): part of the Center for Computer Security Research located at Mississippi State University, is dedicated to the scientific exploration of computer vulnerabilities with the objective of improving prevention and detection techniques through training and research. It offers a curriculum of law enforcement-related training opportunities related to computer crime investigations and analysis.

§D.2. Commercial Software / Vendor and Related Resources

The following is a sample of the more prominent commercial offerings related to computer forensics and cyber crime investigation and prosecution.

- **AccessData**

  (www.accessdata.com): a leader in password recovery and applied cryptography. AccessData offers beginner, intermediate and advanced training.

- **ASR Data Acquisition & Analysis, LLC**

  (www.asrdata.com): supports the legal, law enforcement, and investigative communities through litigation and technical support, data recovery services, innovative software solutions, expert witness testimony, custom hardware solutions, and training and instruction in related fields.

- **Digital Intelligence**

  (www.digitalintelligence.com): a leader in software, hardware, training and casework solutions for the computer forensics community

- **Guidance Software**

  (www.guidancesoftware.com): offers training in its forensic software applications, including the commonly used EnCase Forensic Software; geared toward corporate and law enforcement clients.

- **NTI (Armor Forensics division, formerly New Technologies, Inc.)**

  (www.forensics-intl.com): services include computer forensics consulting, training, and software, computer

security software, computer security risk training, computer-related litigation strategy, e-Discovery, expert witness testimony, and probation and parole sex offender computer monitoring.

- **Mares and Company**

  (www.dmares.com): provides a variety of computer forensic software and training services, including computer forensics, incident response, investigations, data analysis and auditing, drive wiping, data/software/hardware validation tools, ownership identification of hard drives for inventory or for theft/ loss recovery, Bates numbering, and other applications.

- **Kroll Ontrack**

  (www.krollontrack.com): provides large-scale electronic and paper-based discovery and computer forensics services and software to assist attorneys, investigators, legal professionals, and corporations.

- **Paraben Corporation**

  (www.paraben.com): offers forensic software, forensic training, forensic hardware, and consumer software, including PDA seizure and Cell Seizure software.

- **Sleuthkit.org**

  (www.sleuthkit.org): Specific forensic assistance resource.

- **The Coroner's Toolkit**
  (www.porcupine.org/forensics/tct.html):specific forensic assistance resource for use in post-mortem analysis of a UNIX system after break in.

- **Technology Pathways**

  (www.techpathways.com): develops, markets, and supports ProDiscover computer forensics software for the government and legal markets.

§D.3. Miscellaneous Resources

The following is a sample of resources available from individuals and groups considered to be experts in fields related to computer forensics, cyber crime investigation, and prosecution.

- "An Explanation of Computer Forensics" by Judd Robbins
  www.computerforensics.net/forensics.htm

- Computer Forensics Tools, a list by Bob Cromwell
  www.cromwell-intl.com/security/security-forensics.htm

- Updated conferences and training list, by David Baker
  www.forensicswiki.org/wiki/Upcoming_events

- Scientific Working Group on Digital Evidence
  www.ncfs.org/swgde/index.html

- International Journal of Digital Evidence
  www.utica.edu/academic/institutes/ecii/ijde

APPENDIX E. GLOSSARY OF COMMON TERMS

Access: To program, to execute programs on, to communicate with, store data in, retrieve data from, or otherwise make use of any resources, including data or programs, of a computer, computer system or computer network.

ASCII: The most popular character set in common use. People often refer to a bare text file without complicated embedded format instructions as an ASCII file. These files can usually be transferred from computer to computer with relative ease.

Addresses: Every device on the Internet has an address that allows other devices to locate and communicate with it. An Internet Protocol (IP) address is a unique number that identifies a device on the Internet. A Uniform Resource Locator (URL) address, such as "http://www.usdoj.gov", is used to access web sites or other services on remote devices.

Application: Collection of one or more related software programs that enables a user to enter, store, view, modify or extract information from files or databases. Applications may include word processors, Internet browsing tools and spreadsheets.

Archival Data: Information that is not directly accessible to the user of a computer system but that the organization maintains for long-term storage and record keeping purposes. Archival data may be written to removable media such as a CD, or may be maintained on system hard drives in compressed formats.

Attachment: Record or a file associated with another record for the purpose of storage or transfer.

Backdoor: Generally circumvents programs and provides access to a program, an online service, or an entire computer system. It can be authorized or unauthorized, documented or undocumented.

Backup: Process of saving a copy of data onto separate media (e.g., a floppy disk) for preservation. Also refers to the copy made.

Backup Data: Information that is not presently in use by an organization but is routinely stored separately upon portable media to free up space and permit data recovery in the event of disaster.

Backup Tape Recycling: Process by which an organization's backup tapes are overwritten with new backup data, usually on a fixed schedule.

Bit: Smallest unit of data.

Bit Stream Copy: Allows for a bit for bit copy or image of the files or drive in question.

Blog (Web Log): Frequent, chronological Web publications consisting of links and postings. The most recent posting appears at the top of the page.

Boot: The act of loading the first piece of software to start a computer.

Buddy List: Collection of screen names, usually compiled by a user for instant messaging on personal computer or cellular phone.

Burn: Process of making a CD-ROM copy of data, whether it is music, software or other data.

Byte: Equal to eight bits. The byte is the measurement of most computer data as multiples of the byte value. A megabyte is one million bytes or eight million bits.

Cache: Computer memory that temporarily stores frequently used information for quick access.

CART: Computer Analysis and Response Team (FBI)

CD-R: Compact disk to which data can be written but not erased.

CD-ROM: Data storage medium that uses compact discs to store about 1,5000 floppy discs worth of data.

CD-RW: A compact disk to which data can be written and erased**.**

CHS Addressing: A system used to locate physical places on the disk.

Clipboard: Temporary computer memory that allows the user to store text and graphics for future use.

Coding: Document coding is the process of capturing case-relevant information (i.e. author, date authored, date sent, recipient, etc.) from a paper document.

Compression: Technology that reduces the size of a file; valuable to network users because they help save time and bandwidth.

Computer Forensics: Refers to the use of specialized techniques for recovery, authentication, and analysis of electronic data when a case involves issues relating to reconstruction of computer usage, examination of residual data, authentication of data by technical analysis, or explanation of technical features of data and computer usage.

Computer Network: Set of related, remotely connected devices and communication facilities including at least one computer system with the capability to transmit data through communication facilities.

Computer Program: Ordered set of data representing coded instructions or statements that when executed by a computer cause the computer to process data.

Computer Software: Set of computer programs, procedures and associated documentation concerned with operation of a computer system.

Computer System: Set of functionally related computer equipment, devices, or computer software.

Cookie: File that is generated by a web site when a remote computer accesses it. The cookie is sent to the user's computer and placed in a directory on that computer, usually labeled "Internet" or "Temporary."

The cookie includes information such as user preferences, connection information such as time and date of use, records of user activity including files accessed or services used, or account information. The cookie is then accessed by the website on subsequent visits to better serve the user's needs.

CPU (Central Processing Unit): The brain of the computer that performs all arithmetic, logic, and control functions.

Credible threat: Threat made with the intent and the apparent ability to carry out the threat so as to cause the person who is the target of the threat to reasonably fear for his or her safety.

DAT (Digital Audio Tape): Storage medium in some backup systems.

Data Compression: Process of reducing the number of bits needed to represent some information, usually to reduce the time or cost of storing or transmitting it. Some methods can be reversed to reconstruct the original data exactly; these are used for faxes, programs, and most computer data.

Deleted Data: Data that existed on the computer that has been deleted by the computer system or end-user activity**.** Deleted data remains on storage media in whole or in part until overwritten by ongoing usage or "wiped" with a software program designed to remove deleted data. Even after the data has been wiped, directory entries, pointers, or other metadata relating to the deleted data may remain on the computer.

Deleted File: File with disk space that has been designated as available for use. The deleted file remains intact until it has been overwritten with a new file.

Denial of Service Attack: Type of network attack in which the objective is to disable the victim host or to block its communication with the rest of the network. Examples include a ping "storm," "SYN flood," smurf attack," and "ping of death." Sometimes abbreviated as DOS. The use of multiple computers to attack a single computer is called a Distributed Denial of Service Attack, or DDOS.

Desktop: Default "work area" presented on screen to the user, or a computer designed for use in a single location, as opposed to a laptop.

Device: Includes, but is not limited to, an electronic, magnetic, electrochemical, biochemical, hydraulic, optical, or organic object that performs input, output, or storage functions by the manipulation of electronic, magnetic or other impulses.

Digital: Storing information as a string of digits - namely "1s" and "0s".

Directory: Organizational area within a file system, typically used to segregate a related group of files. It is referred to as a folder in some operating systems; a directory may contain (or be contained in) other directories.

Disc (disk): A magnetic storage medium on which data is digitally stored (may be a floppy or a hard disk). Disc may also refer to a CD-ROM, which is an optical storage medium.

Disk Slack: Refers to left over sectors used to form the last cluster of the file.

Distributed Data: Information belonging to an organization that resides on portable media and non-local devices such as home computers, laptops, floppy disks, CD-ROMS**,** "PDAs", wireless communication devices, (i.e., Blackberry), zip drives, Internet repositories such as Web pages, and the like. Distributed data also includes data held by third parties, such as application service providers and business partners.

Document: Writings, drawings, graphs, charts, photographs, phonographs, or other data compilations. Also refers to a collection of pages representing an electronic file. Examples of electronic documents include e-mails, attachments, databases, word documents, spreadsheets, and graphics files.

Document Retention: Preservation of documents and data, including hard copy and electronic documents, databases, and emails that are

created, sent, and received in an organization's ordinary course of business.

Domain: Group of Internet devices that are owned or operated by a specific individual, group, or organization. Devices within a domain name have IP addresses within a certain range of numbers and are usually administered according to the same set of rules and procedures.

Domain Name: Name that identifies a computer or group of computers on the Internet and corresponds to one or more IP addresses within a particular range. A domain name can provide information about the organization, ISP, and physical location of a particular network user.

Dongle: Device that attaches to a computer to control access to a particular application. A dongle provides one of the most effective means of copyright protection.

Dynamic Host Configuration Protocol (DHCP): Service that automates the assignment of IP addresses on a network. DHCP assigns an IP address each time a computer is connected to the network. DHCP uses the concept of a "lease" or amount of time that a given IP address will be valid for a specific computer**.**

ECPA (Electronic Communications Privacy Act): Federal law that sets the procedures law enforcement must follow to obtain information from Internet Service Providers or to intercept communications.

Electronic communication: Any transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature, transmitted in whole or in part by a wire, radio, computer, electromagnetic, photoelectric, or photo-optical system.

Electronic Discovery: Discovery of electronic data including email, Web pages, word processing files, and virtually anything that is stored on a computer**.**

Electronic Mail Message: Document created or received via an electronic mail system, plus any attachments that may be transmitted with the message.

Electronic Record: Information recorded in a form that requires a computer or other machine to process it.

Encryption: Procedure that renders the contents of the record or file unintelligible to anyone not authorized to use it.

Ethernet: Common way of networking PCs to create a LAN.

Extranet: Internet-based access method to a corporate intranet site by limited or total access through a security firewall. Typically utilized in cases of joint ventures and vendor client relationships.

Family Relationship: Relationship formed among two or more documents that have a connection or relatedness because of some factor.

File: Collection of data or information stored under a specific name on a disk.

File Extension: Tag of three or four letters preceded by a period which identifies the data file's format or the application used to create the file. File extensions can streamline the process of locating data, for example if one is looking for pictures stored on a computer, one might start with the .gif and .jpg files.

File Server: When several computers are linked together in a LAN situation, one computer may be utilized as a storage location for files for the group. A file server may be used to store email, financial data, word processing information, or to back up the network.

File Sharing: One of the key benefits of a network is the ability to share files stored on the server among several users.

File Slack: RAM slack + Disk slack = File slack.

Financial instrument: Any check, draft, money order, certificate of deposit, letter of credit, bill of exchange, credit card, or marketable security.

Free Space: Part of the disk that has not been allocated, or had data that has since been deleted.

Firewall: Dedicated computer system or piece of software that monitors the connection between one computer or network and another. The firewall certifies communications, blocks unauthorized or suspect transmissions, and filters content coming into a network. Hackers often sidestep firewalls by acquiring system passwords "hiding" within authorized ISP addresses, using specialized software or routines, or placing viruses in seemingly innocuous files such as email attachments.

First Responder: Initial responding law enforcement officer(s) arriving on the scene.

Forensic Copy: Exact bit by bit copy of the entire physical hard drive of a computer system including slack and unallocated space.

FTK (Forensic Tool Kit): Software used in computer forensics.

FTP (File Transfer Protocol): Internet protocol enabling the transfer of files between computers over the Internet.

Gateway: Device that passes traffic between networks. Typically, a gateway physically sits at the perimeter of an internal network to the Internet.

GIF (Graphic Interchange Format): Computer compression format for pictures.

Gigabyte (GB): Measure of computer data storage capacity**.** It is roughly 1 billion bytes.

GUI (Graphical User Interface): Set of screen presentations and metaphors utilizing graphic elements such as icons in an attempt to make an operating system easier to use.

Hacking: Deliberate infiltration or sabotaging of a computer or a network of computers. Hackers use loopholes in computer security to gain control of a system, steal passwords and sensitive data, and/or incapacitate a computer or group of computers. Hacking is usually done remotely by sending harmful commands and programs through the Internet to a target system The command or program then instructs the target system to operate outside the parameters specified by the administrator of the system. Often causes general system instability or loss of data. ("Cracking" also refers to malicious hacking intended to cause damage or compromise data.).

Hard Drive: Primary storage unit on PCs, consisting of one or more magnetic media platters on which digital data can be written and erased magnetically.

Hard Drive Interfaces: Pertains to the types of hookups for drives. There are at least three interface types: IDE/ATA, SCSI, and Serial ATA.

Hard Drive Structure: Can be separated into two categories: Physical includes the drive, platters, write heads, etc. Logical includes sensors, clusters, files, partitions and file systems.

Header: Source, destination, and routing information attached to the beginning of a packet, email message, or other electronic communication. Most headers can be totally or partially spoofed.

HTML (Hypertext Markup Language): Standard format for describing the intended appearance of text, graphics, and other elements in a web page. Every web browser has the built-in ability to understand HTML.

Instant Messaging (IM): Form of electronic communication that involves immediate correspondence between two or more users who are all online simultaneously.

Intellectual Property: Includes data, computer programs, computer software, trade secrets, copyrighted materials, and confidential or proprietary information in any fixed form or medium.

Internet: Interconnecting global public network made by connecting smaller shared public networks. The Internet is the most well known.

Internet Relay Chat (IRC): Internet service that allows users from around the world to communicate with each other in real time. IRC is organized around a chat room or channel, in which users gather to communicate with each other about a specific topic. Each member of the chat room can see all messages typed by the other users.

Intranet: Network of smaller private networks that are isolated from the public Internet.

IP address:

> **Dynamic IP Address:** When an ISP uses dynamic ISP allocation, each time the user dials into the ISP to connect to the Internet, his machine is randomly assigned one of the available IP addresses in the IP blocks controlled by the ISP. The customer's computer keeps that IP address for the duration of the session, during which time it cannot be assigned to any other computer. Once the computer disconnects, that IP address becomes available to other customers.
>
> **Static IP address:** IP address that is assigned permanently to a given user or computer on a network. A customer of an ISP that assigns static IP addresses will have the same IP address every time.

ISP (Internet Service Provider): Business that delivers access to the Internet.

JPEG (Joint Photographic Expert Group): Image compression standard for photographs.

Keyword Search: Search for documents containing one or more words specified by a user.

Kilobyte (K): One thousand bytes of data.

Known Child Porn Identification: Comparing the files in a child pornography case against the FBI database of known child pornography.

LAN (Local Area Network): Allows users to share files between computers, send email, and access the Internet. Most corporate computer networks are LANs.

Legal Hold: Communication issued as a result of current or anticipated litigation, audit, government investigation, or other matter that suspends the normal disposition or processing of records.

Log: File containing running records of a certain type of network event (e.g., records of web site visitor accesses).

Loss or Damage: Any reasonable cost to any victim, including the cost of responding to an offense, conducting a damage assessment, and restoring the data, program, system, or information to its condition prior to the offense, and any revenue lost, cost incurred, or other consequential damages incurred because of interruption of service.

Malware: Computer viruses, worms, spyware and other software designed to damage or disrupt a system.

Master Boot Record: 512-byte sector at the beginning of the hard drive that contains a sequence of commands for booting an operating system.

Megabyte (Meg): A million bytes of data.

Memory Sticks: Removable memory storage devices created for electronics. These can be smaller than a piece of gum.

Metadata: Information about a particular data set that describe, for example how, when, and by whom it was received, created, accessed, or modified and how it is formatted. Some metadata can easily be seen by users; other metadata can be hidden or embedded and unavailable to most computer users. Metadata describes the content, quality,

condition, history, and other characteristics of the data. ("data about data").

Migrated Data: Information that has been moved from one database or format to another, usually as a result of change from one hardware or software technology to another.

Mirror Image: Bit-by-bit copy of a computer hard drive that ensures the integrity of the data is not altered during the forensic examination.

MIS: Management Information Systems.

Modem: Piece of hardware that lets a computer talk to another computer over a phone line.

Mount/Mounting: Process of making off-line data available for on-line processing. For example, placing a magnetic tape in a drive and setting up the software to recognize or read that tape. Often used in conjunction with the term "load" or "loading" as in "mount and load a tape".

Moving Pictures Expert Group-3 (MP3): Standard for compressing audio recordings so that they can be stored on a computer, transmitted through the Internet to other computers, or listened to using a computer.

Native Format: Electronic documents have an associated file structure defined by the original creating application. This structure is referred to as the "native format" of the document**.** Documents are often converted to a standard file format as part of electronic document processing.

Nesting: Occurs when one document is nested within another (i.e., nesting a graphics file in a word document).

Network: Group of computers or devices connected together for the exchange of data and sharing of resources.

OCR (Optical Character Recognition): Technology that takes data from a paper document and turns it into editable text data. The

document is first scanned, then OCR software searches the document for letters, numbers and other characters.

OLE (Object Linking and Embedding): Program for data sharing that allows two non-compatible applications to work together when creating the document that is to be shared.

Offline Data: Storage of data outside the network in daily use that is accessible through the offline storage system, not the network.

Online: Connected to a network.

Online Service Provider: Internet Service Provider who also provides additional proprietary services such as message boards.

Online Storage: Storage of electronic data as fully accessible information in daily use on the network or elsewhere.

Operating System (OS): Software that the rest of the software depends on to make the computer functional. Windows, Macintosh OS, Unix, and Linux are examples.

Packet Sniffing: While in transit over the Internet, information is contained within packets. Packet sniffing refers to the act of listening to the flow of information on a network for packets containing information such as logins, passwords, or communications such as viruses. After locating the data, the packet sniffer can read, copy, redirect, or block the communication.

Parent-child Relationships: Term used in e-discovery to describe a chain of documents that stems from a single email or folder. A "child" (an attachment) is connected to the "parent" (email).

Partition: Portion of the hard drive that has been subdivided into multiple logical drives, each occupying different storage areas.

PC: Personal computer**.**

PDA (Personal Digital Assistant): Handheld digital organizer**.**

Peer-to-Peer (P2P) Networks: P2P networks differ from conventional networks in that each computer within the network functions both as a client (using the resources and services of other computers) and a server (providing files and services for use by "peer" computers). There is often no centralized server in P2P networks. Often used to disseminate and share music, movies, and software.

Phone Phreaking: Exploiting weaknesses in a telephone network, usually to obtain free long distance and/or conference calling services.

Pirate Software: Software that has been illegally copied.

Point of Presence (POP): Telephone computer dial-up service in a given locality.

Pointer: Index entry in the directory of a disk (or other storage medium) that identifies the space on the disk where an electronic document or piece of electronic data resides, thereby preventing that space from being overwritten by other data. When an electronic document is deleted, the pointer is usually deleted, which allows the document to be overwritten, although it is not actually erased.

Post Office Protocol (POP): Protocol that allows single users to send and receive email from a mail server.

RAM (Random Access Memory): Working memory of the computer into which application programs can be loaded and executed.

RAM Slack: Unused space from sectors if the data does not take up all 512 bytes of memory.

Record: Information, regardless of medium or format, that has value to an organization.

Record Lifecycle: Time period from when a record is created until it is disposed.

Residual Data (or ambient data)**:** Data that is not active on a computer system. It includes: (1) data found on media free space, (2) data found

in file slack space, and (3) data found within files that have functionally been deleted, in that it is not visible without the use of special data recovery techniques.

Restore: To transfer data from a back-up medium to an on-line system, often for the purpose of recovery from a problem, failure, or disaster.

Router: Hardware that routes data from a local area network (LAN) to a phone line.

Sandbox: Network or series of networks that are not connected to other networks.

Sector: Set of bits comprising the smallest addressable unit of information on the hard disk**.**

Server: Computer on a network that contains data or applications shared by the users of the network on their client PCs.

Sibling: Document that shares a common parent with the document in question (e.g., two attachments that share the same parent email).

Slack Space: Form of residual data. Slack space is the amount of on-disk file space from the end of the logical record information to the end of the physical disk record. Slack space can contain information soft-deleted from the record, information from prior records stored at the same physical location as current records, metadata, and other information useful for forensic analysis of computer systems.

Spoliation: Destruction of records which may be relevant to on-going or anticipated litigation, government investigation, or audit.

Spoofing: Practice of transmitting an email so that it appears to have been sent by someone else. Often computer forensic experts are needed to determine if an email has been spoofed.

Stand Alone Computer: Personal computer that is not connected to any other computers or network, except possibly through a modem.

Steganography: Hiding a secret message in a larger one in a way that unauthorized people cannot detect its presence; typically text hidden inside an image.

Swap Space: Area that the computer has allocated for projects that the user is currently not working on when RAM is running low.

System Administrator (sysadmin, sysop): Person in charge of keeping a network working.

Thumb Drive: USB solid state mass storage device about the size of a thumb. Quickly replacing floppy disks and other methods of memory storage.

TIFF (Tagged Image File Format): One of the most widely supported file formats for storing bit-mapped images. Files in TIFF format often end in .tif.

Time Stamps: Information contained inside the file properties that tells when the file was created, last modified, and last accessed.

TCP/IP (Transmission Control Protocol/Internet Protocol): Collection of protocols that define the basic workings of the features of the Internet.

Tracing: Trace programs are used to determine the path that a communication takes to arrive at its destination.

Trojan: Application that overtly does one thing while covertly doing another**.**

User Name or User ID: Most services on the Internet assign users a name or ID, that is a pseudonym the computer systems use to keep track of users. Typically associated with additional user information such as an email.

Virus: Computer program, usually made to spread from computer to computer, that is intended to annoy the user or cause harm to his or her

computer. A virus might place an annoying message on the computer screen or it might re-format the user's hard drive, causing a loss of all data on the hard disk.

Wardriving: Driving around an area in an automobile with a laptop and a wireless network adapter in order to locate unsecured wireless networks.

Wireless Network Card: Expansion card in a computer that allows a cordless connection between that computer and other devices on a computer network; communicates via radio signals to other devices present on the network.

Worm: Type of virus that self-replicates across a network.

Write Blocking: Act of using a piece of technology to prevent the changing of information on the drive in question.

WWW (World Wide Web): WWW is made up of all of the computers on the Internet that use HTML-capable software (Netscape, Explorer, etc.) to exchange data.

Zip: Open standard for compression used widely for PC download archives; used on Windows based programs such as WinZip and Drag and Zip. The file extension given to ZIP files is .zip.

Zip Drive Disk: 3.5-inch removable disk drive. The drive is bundled with software that can catalogue disks and lock files for security.