§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 where the criminal activity did 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

- An estimated 95% of all information generated today is in electronic form.
- No more than 30% of that information is ever 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 OF CYBER CRIME FOR LAW ENFORCEMENT

- To assure that digital evidence is acquired, preserved, and analyzed in a forensically safe manner, and thus enable its presentation to the 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

The following section lists many of the sources of digital evidence and types of such evidence that each may contain, 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 input/output device

Standalone 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

Hidden Files:
Embedded data and metadata
Compressed files
Encrypted files

Computer-Created Files:
Backup files
Configuration files
Cookies

-----------

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).
Printer spool files  
Swap 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.

**Access Control Devices** (Smart Cards, Dongles, Biometric Scanners):
- Card and user identification/
  authentication information
- Level of access

**Answering Machines:**
- Stored voice messages
- Message time and date
  information (in some cases)
- Caller identification information
- Deleted messages
- Last number called
- Memo
- Phone numbers and names
- Tapes

**Cell Phones:**
- 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

**Digital Cameras:**
- Images
- Removable cartridges/memory cards
- Sound
- Time and date stamps
- 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
- Video
- Email and most other data may be stored on cameras (as portable storage devices via USB)
Hand-held Devices (PDAs and hybrid devices):
Address book                     Handwriting
Appointment calendars/information Password
Documents                         Phone book
E-mail                            Text messages
Images                            Voice messages
Videos

Note: Evidence may exist on such a device 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              Text messages
E-mail                           Voice messages
Phone numbers

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

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

Copiers:
Documents                       User usage log
Time and date stamp

- 6 -
Credit Card Skimmers

**Digital Watches:**  
- Address book  
- Appointment calendars  
- E-mail

**Facsimile Machines:**  
- Documents  
- Film cartridge

**Global Positioning Systems (GPS):**  
- Home  
- Previous destinations  
- Travel logs

**Vehicle Event Data Recorders** (“black boxes”):  
- Crash data

**Other Electronic Devices and Peripheral Evidence:**  
- Audio recorders  
- Cables  
- Caller ID devices  
- Chips (When found in quantity, may indicate chip theft.)  
- Digital picture frames  
- Dongle or other hardware protection devices (keys) for software  
- Drive duplicators

§2.2.2. POTENTIAL EVIDENCE BY CRIME CATEGORY

**Computer Fraud** (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
<table>
<thead>
<tr>
<th><strong>Child Exploitation/Abuse:</strong></th>
<th>Images</th>
<th>Internet activity logs</th>
<th>Movie files</th>
<th>User-created directory and file names that classify images</th>
</tr>
</thead>
<tbody>
<tr>
<td>Chat logs</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Date and time stamps</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Digital camera software</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>E-mail, notes, and letters</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Games</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Graphic editing and viewing software</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>Computer/Network Intrusion:</strong></th>
<th>Internet protocol (IP) address and user name</th>
<th>Internet relay chat (IRC) logs</th>
<th>Source code</th>
<th>Text files and documents with user names and passwords</th>
</tr>
</thead>
<tbody>
<tr>
<td>Address books</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Configuration files</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>E-mail, notes, and letters</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Executable programs</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Internet activity logs</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>Homicide / Death Investigation:</strong></th>
<th>Maps or driving directions</th>
<th>Medical records</th>
<th>Telephone records</th>
<th>Photos of victim / suspect</th>
<th>Trophy photos</th>
</tr>
</thead>
<tbody>
<tr>
<td>Address books</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Diaries</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>E-mail, notes, and letters</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Financial / asset records</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Internet activity logs</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Legal documents and wills</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>Domestic Violence:</strong></th>
<th>Financial / asset records</th>
<th>Medical records</th>
<th>Telephone records</th>
</tr>
</thead>
<tbody>
<tr>
<td>Address books</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Diaries</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>E-mail, notes, and letters</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>Economic / Financial Fraud</strong> (including Counterfeiting):</th>
<th>False financial transaction forms</th>
<th>False identification</th>
<th>Financial / asset records</th>
<th>Images of signatures</th>
<th>Internet activity logs</th>
<th>Online banking software</th>
</tr>
</thead>
<tbody>
<tr>
<td>Address books</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Calendar</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Check, currency, money order images</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Credit card skimmers</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Customer information / credit card data</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Databases</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>E-mails, notes, and letters</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>E-Mail Threats / Harassment / Stalking:</strong></th>
<th>Internet activity logs</th>
<th>Legal documents</th>
<th>Telephone records</th>
<th>Victim background research</th>
<th>Maps to victim locations</th>
</tr>
</thead>
<tbody>
<tr>
<td>Address books</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Diaries</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>E-mails, notes, and letters</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Financial / asset records</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Images</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>Extortion:</strong></th>
<th>Internet activity logs</th>
<th>Temporary Internet files</th>
<th>User names</th>
</tr>
</thead>
<tbody>
<tr>
<td>Date and time stamps</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>E-mails, notes, and letters</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>History log</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
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

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

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 criminal activity
- Inadequate law enforcement resources
- Lack of victim awareness
- Business reluctance to report

Some 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 – nine times as many as in October 2005.
    

- **Piracy**
  - Worldwide revenue loss from software piracy in 2005 was more than $34 billion.
    
    source: The Business Software Alliance; IDC