10-24-2009

Digital Forensics: Everything Leaves a Trace in Cyberspace

Gary C. Kessler
Champlain College - Burlington, kessleg1@erau.edu

Follow this and additional works at: http://commons.erau.edu/db-security-studies
Part of the Internet Law Commons, and the National Security Law Commons

Scholarly Commons Citation

This Presentation is brought to you for free and open access by the College of Arts & Sciences at Scholarly Commons. It has been accepted for inclusion in Department of Security Studies and International Affairs - Daytona Beach by an authorized administrator of Scholarly Commons. For more information, please contact commons@erau.edu.
Digital Forensics: 
Everything Leaves a Trace in Cyberspace

Parents Day  
October 24, 2009  
Burlington, VT

Gary C. Kessler  
M.S., Digital Investigation Management Program  
B.S., Computer & Digital Forensics Program

Overview

• What is cyberforensics
• Legal issues
• The computer/network forensics process
• Where does the data go -- Some examples
• Locard's Principle
What is "Cyberforensics"?

- **Forensics**
  - The use of science to investigate and establish facts in criminal or civil courts
  - *Computer forensics, digital forensics, network forensics, cyberforensics*

- Branches include
  - Medical forensics
  - Physical evidence
  - Forensic accounting
  - Computer and network forensics

Why Cyberforensics?

- Computers/Internet are the fastest growing technology tools for criminals and criminal acts
- Access is nearly ubiquitous
  - >1B Internet users, ~23% in North America
  - In U.S., 95% of schools, >50% of classrooms, and >80% of homes have Internet access
  - >8B Web pages listed by Google before they stopped counting...
    - 85B pages at the Internet Archive waybackmachine
- The technology is smaller, cheaper, faster, more mobile than ever!!
Computer Crime is Attractive

- Average armed bank robbery:
  - Nets $7,500 ($60M annual)
  - 16% of money recovered
  - 80% of offenders go to jail
- White collar computer crimes take in about $10B annually
  - <5% of offenders go to jail
  - Juries consider this a non-violent crime
  - Criminal statutes vary internationally

What Crime Scenes Have Computers?

- Murder
- Kidnap
- Rape
- Extortion
- Stalking
- Drug dealing
- Auto theft
- Espionage
- Identity theft/fraud
- Gun dealing
- Robbery/burglary
- Gambling
- Stock/bond scams
- Confidence games
- Web defacement
- Terrorism
- Theft of computer files
- Child sexual exploitation
The Fourth Amendment

The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.

Searching and Seizing Computers

• 4th Amendment protections still in force
• Exceptions to warrant requirement
  » Permission
    • Must get permission from competent authority
      – I still expect privacy on a home system even with multiple users
  » Plain view
    • E.g., child porn screen saver
  » Exigent circumstances
Expectation of Privacy

- Company-owned computers and servers do not generally offer a user an expectation of privacy
  » But it is best if there are explicit policies spelling this out
- No expectation of privacy if third-party is asked to examine a system

Collecting Evidence

- Search of a computer has few rules if the searcher is not an "agent of the state"
  » Before involving the police, private entities are not bound by 4th Amendment
  » This includes system administrators, repair personnel, even "illegal access" by others
- Collecting data after calling police requires special care and, possibly, a search warrant
Federal Laws

- Electronic Communications Protection Act (ECPA) extends federal wiretap protection to computer communications including electronic mail
  » ECPA protects any in-transit communication
  » Unopened e-mail is considered to be in transit
  » Opened e-mail still stored on server is not in transit
  » ECPA extends the workplace into cyberspace
- Privacy Protection Act (PPA) protects documents that are intended for publication

Side Note: Define "ISP"

- Commercial service providers are easy...
  » Sells Internet access, e-mail service, and/or Web hosting for a fee
- What about...
  » College/university campus?
  » Organization that provides Internet access to employees?
  » My neighbor?
Computer Forensics Process

- Bit-for-bit image of original data
  - Forensically correct copy of media (mirror image)
  - Maintain evidentiary chain
- Analyze the copies of the data
  - Files, deleted files, unallocated space, file slack, logs
- Reconstruct picture of what information is/was on that computer
- Link the computer to a specific human being

Cyber Investigations

- Computer/network evidence alone will generally not convict a suspect
  - But if the evidence helps solidify a pattern of behavior, it can be very convincing
- Forensic analysis can also help counter "false defenses"
  - "Someone else put the pictures on the suspect's computer."
  - "My client does not know the victim."
  - "The defendant has never been in contact with {drugs/guns}."
My Idea of a Computer...

A Typical Home Computer

Source: National White Collar Crime Center
Computers

• An increasing number of devices have embedded computers... with logs and memory

Secondary Storage

• Storage of data, files, programs, images, videos, music, etc.
• Hard drive capacity commonly 40-160 GB; 600 GB and larger available
• Hard drives may be internal or external
Removable Storage Devices

- Floppy drives, tape, hard drives, CDs, DVDs, ZIP disks, thumb drives, MP3 players, ...

Not Enough Can Be Said About Thumb Drives...
When Are You Done?

• Just because you don't find something doesn't mean it's not there!!
• Do you stop looking when you feel there's enough evidence to convict? It depends on
  » Whose computer
  » Legal basis for the search
  » Nature of crime
• In some cases, scope of search depends on consent of the suspect or the owner

So, Where is All This Information?

• Example #1: Deleted Files
• Example #2: Web Browsers
• Example #3: Cell Phones
• Example #4: Metadata
• Real Example: The BTK Killer
Example #1: Deleted Files

- Files on a floppy
  - Use hex editor to see what "deleted" files look like
  - Use EnCase to examine "deleted" information
<table>
<thead>
<tr>
<th>Offset</th>
<th>0</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
<th>6</th>
<th>7</th>
<th>8</th>
<th>9</th>
<th>A</th>
<th>B</th>
<th>C</th>
<th>D</th>
<th>E</th>
<th>F</th>
</tr>
</thead>
<tbody>
<tr>
<td>000000C0</td>
<td>04</td>
<td>51</td>
<td>54</td>
<td>4F</td>
<td>46</td>
<td>4C</td>
<td>4F</td>
<td>50</td>
<td>50</td>
<td>59</td>
<td>58</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td></td>
</tr>
<tr>
<td>000000C1</td>
<td>0E</td>
<td>00</td>
<td>00</td>
<td>06</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>00</td>
</tr>
<tr>
<td>000000C2</td>
<td>07</td>
<td>4B</td>
<td>41</td>
<td>46</td>
<td>4F</td>
<td>47</td>
<td>4F</td>
<td>20</td>
<td>47</td>
<td>49</td>
<td>46</td>
<td>20</td>
<td>03</td>
<td>1B</td>
<td>24</td>
<td>0D</td>
</tr>
<tr>
<td>000000C3</td>
<td>31</td>
<td>2E</td>
<td>71</td>
<td>72</td>
<td>6E</td>
<td>60</td>
<td>00</td>
<td>08</td>
<td>58</td>
<td>3B</td>
<td>2E</td>
<td>62</td>
<td>00</td>
<td>00</td>
<td>06</td>
<td>00</td>
</tr>
<tr>
<td>000000C4</td>
<td>14</td>
<td>4F</td>
<td>46</td>
<td>41</td>
<td>20</td>
<td>20</td>
<td>20</td>
<td>20</td>
<td>6A</td>
<td>60</td>
<td>47</td>
<td>20</td>
<td>18</td>
<td>B2</td>
<td>24</td>
<td>0D</td>
</tr>
<tr>
<td>000000C5</td>
<td>66</td>
<td>2C</td>
<td>71</td>
<td>72</td>
<td>6E</td>
<td>60</td>
<td>00</td>
<td>08</td>
<td>58</td>
<td>3B</td>
<td>2E</td>
<td>62</td>
<td>00</td>
<td>00</td>
<td>06</td>
<td>00</td>
</tr>
<tr>
<td>000000C6</td>
<td>80</td>
<td>54</td>
<td>52</td>
<td>49</td>
<td>4E</td>
<td>55</td>
<td>58</td>
<td>20</td>
<td>20</td>
<td>47</td>
<td>49</td>
<td>46</td>
<td>20</td>
<td>18</td>
<td>B0</td>
<td>22</td>
</tr>
<tr>
<td>000000C7</td>
<td>4D</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

© 2003-2009, Gary C. Kessler

<table>
<thead>
<tr>
<th>Offset</th>
<th>0</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
<th>6</th>
<th>7</th>
<th>8</th>
<th>9</th>
<th>A</th>
<th>B</th>
<th>C</th>
<th>D</th>
<th>E</th>
<th>F</th>
</tr>
</thead>
<tbody>
<tr>
<td>000000C0</td>
<td>04</td>
<td>51</td>
<td>54</td>
<td>4F</td>
<td>46</td>
<td>4C</td>
<td>4F</td>
<td>50</td>
<td>50</td>
<td>59</td>
<td>58</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td></td>
</tr>
<tr>
<td>000000C1</td>
<td>0E</td>
<td>00</td>
<td>00</td>
<td>06</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>00</td>
</tr>
<tr>
<td>000000C2</td>
<td>07</td>
<td>4B</td>
<td>41</td>
<td>46</td>
<td>4F</td>
<td>47</td>
<td>4F</td>
<td>20</td>
<td>47</td>
<td>49</td>
<td>46</td>
<td>20</td>
<td>03</td>
<td>1B</td>
<td>24</td>
<td>0D</td>
</tr>
<tr>
<td>000000C3</td>
<td>31</td>
<td>2E</td>
<td>71</td>
<td>72</td>
<td>6E</td>
<td>60</td>
<td>00</td>
<td>08</td>
<td>58</td>
<td>3B</td>
<td>2E</td>
<td>62</td>
<td>00</td>
<td>00</td>
<td>06</td>
<td>00</td>
</tr>
<tr>
<td>000000C4</td>
<td>14</td>
<td>4F</td>
<td>46</td>
<td>41</td>
<td>20</td>
<td>20</td>
<td>20</td>
<td>20</td>
<td>6A</td>
<td>60</td>
<td>47</td>
<td>20</td>
<td>18</td>
<td>B2</td>
<td>24</td>
<td>0D</td>
</tr>
<tr>
<td>000000C5</td>
<td>66</td>
<td>2C</td>
<td>71</td>
<td>72</td>
<td>6E</td>
<td>60</td>
<td>00</td>
<td>08</td>
<td>58</td>
<td>3B</td>
<td>2E</td>
<td>62</td>
<td>00</td>
<td>00</td>
<td>06</td>
<td>00</td>
</tr>
<tr>
<td>000000C6</td>
<td>80</td>
<td>54</td>
<td>52</td>
<td>49</td>
<td>4E</td>
<td>55</td>
<td>58</td>
<td>20</td>
<td>20</td>
<td>47</td>
<td>49</td>
<td>46</td>
<td>20</td>
<td>18</td>
<td>B0</td>
<td>22</td>
</tr>
<tr>
<td>000000C7</td>
<td>4D</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

© 2003-2009, Gary C. Kessler
Example #2: Web Browsers

- Browser store just about everything
  - Registry keys and directories
  - Bookmarks, cookies, browser history, Internet cache, typed URLs, stored forms, stored passwords, download tracking

- IE and Firefox are predominate browsers but there are many others in wide use
  - AOL
  - Epiphany
  - Netscape
  - Opera
  - Safari
Example #3: Mobile Phones

Note PIN and banner message
Example #4: Metadata

- **Metadata** is data about data
  - Information that describes the *contents* of a container or describes the *container* itself

- Type of metadata
  - File system: Location and size, pertinent dates
  - Document: Author, organization
  - Image: Source software/hardware

Metadata in MS Office

© 2003-2009, Gary C. Kessler
Case Study: BTK Killer

- BTK Killer was a serial killer in Wichita, KS, who killed at least 10 people between January 1974 and his arrest in 2005
  » BTK = "Bind, torture, kill"
- BTK sent a message to local media after each killing
  » Communiqués in 2004 were e-mailed to local TV stations
Case Study: BTK Killer (2)

- Examination of metadata in a Word file pointed to a person named Dennis, associated with the Christ Lutheran Church in Wichita
- Web site (http://christ-lutheran.org/) listed "Dennis Rader" as church president
- Police went to church to search computers and found disk given by Rader to pastor with upcoming meeting agenda
  » Also found "deleted" copy of a letter to the TV station
- Dennis L. Rader, 59, arrested Feb. 26, 2005

Paring Thoughts

- Locard's Principle -- "Every contact leaves a trace"
  -- applies to cyberspace as well as realspace...
  "Wherever he steps, whatever he touches, whatever he leaves, even unconsciously, will serve as a silent witness against him. Not only his fingerprints or his footprints, but his hair, the fibers from his clothes, the glass he breaks, the tool mark he leaves, the paint he scratches, the blood or semen he deposits or collects. All of these and more, bear mute witness against him. This is evidence that does not forget. It is not confused by the excitement of the moment. It is not absent because human witnesses are. It is factual evidence. Physical evidence cannot be wrong, it cannot perjure itself, it cannot be wholly absent. Only human failure to find it, study and understand it, can diminish its value."
  
  Prof. Edmond Locard, c. 1910
Author Contact Information

Gary C. Kessler, Ed.S., CCE, CISSP
M.S., Digital Investigation Management Program
Champlain College
163 South Willard Street
Burlington, VT 05401

office: +1 802-865-6460
cell: +1 802-238-8913
fax: +1 802-865-6446
e-mail: gary.kessler@champlain.edu
Skype: gary.c.kessler

http://digitalforensics.champlain.edu
http://www.garykessler.net

This work was partially supported by Grant No. 2006-DD-BX-0282 awarded by the Bureau of Justice Assistance. The Bureau of Justice Assistance is a component of the Office of Justice Programs, which also includes the Bureau of Justice Statistics, the National Institute of Justice, the Office of Juvenile Justice and Delinquency Prevention, and the Office for Victims of Crime. Points of view or opinions in this document are those of the author and do not represent the official position or policies of the United State Department of Justice.