

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: <https://commons.erau.edu/db-security-studies>



Part of the [Internet Law Commons](#), and the [National Security Law Commons](#)

---

### Scholarly Commons Citation

Kessler, G. C. (2009). Digital Forensics: Everything Leaves a Trace in Cyberspace. , (). Retrieved from <https://commons.erau.edu/db-security-studies/16>

This Presentation without Video 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 Security Studies & International Affairs - Daytona Beach by an authorized administrator of Scholarly Commons. For more information, please contact [commons@erau.edu](mailto: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

© 2003-2009, Gary C. Kessler

2

## 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!!

<http://www.internetworldstats.com/stats.htm>

© 2003-2009, Gary C. Kessler

3

## 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

© 2003-2009, Gary C. Kessler

4

## 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

© 2003-2009, Gary C. Kessler

5

## 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.*

© 2003-2009, Gary C. Kessler

6

## 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

© 2003-2009, Gary C. Kessler

7

## 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

© 2003-2009, Gary C. Kessler

8

## 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

© 2003-2009, Gary C. Kessler

9

## 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

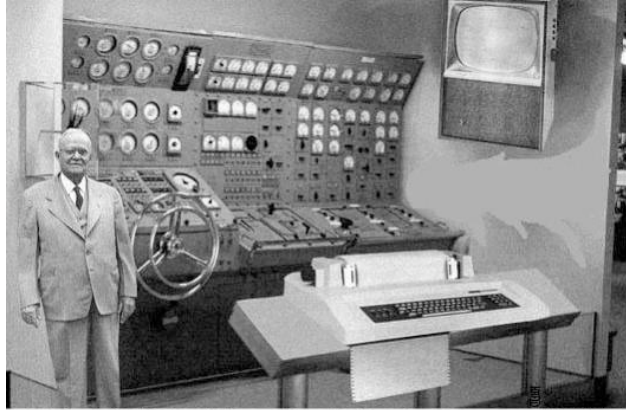
- Bit-for-bit image of original data
  - » Forensically correct copy of media (mirror image)
  - » Maintain evidentiary chain
- Analyze the copies of the data
  - » Files, deleted files, unallocated space, file slack, logs
- Reconstruct picture of what information is/was on that computer
- Link the computer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



*Scientists from the RAND Corporation have created this model to illustrate how a "home computer" could look like in the year 2004. However the needed technology will not be economically feasible for the average home. Also the scientists readily admit that the computer will require not yet invented technology to actually work, but 50 years from now scientific progress is expected to solve these problems. With teletype interface and the Fortran language, the computer will be easy to use and only*

© 2003-2009, Gary C. Kessler

14

## A Typical Home Computer



Source: National White Collar  
Crime Center

© 2003-2009, Gary C. Kessler

15

# Computers

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



© 2003-2009, Gary C. Kessler

16

# 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



© 2003-2009, Gary C. Kessler

17

# Removable Storage Devices

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



© 2003-2009, Gary C. Kessler

18

# Not Enough Can Be Said About Thumb Drives...



© 2003-2009, Gary C. Kessler

19

## 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?

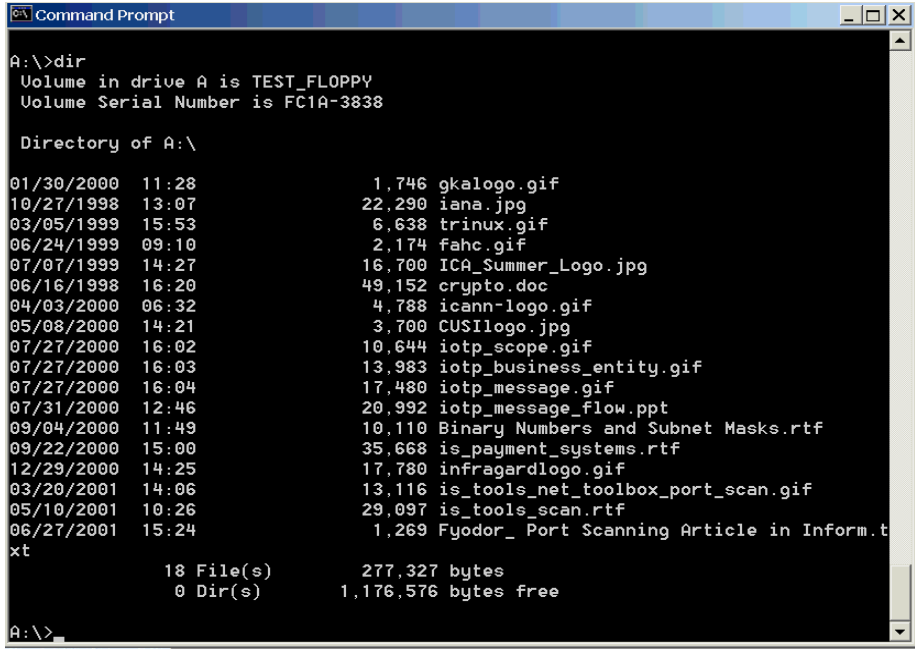
- Example #1: Deleted Files
- Example #2: Web Browsers
- Example #3: Cell Phones
- Example #4: Metadata
- Real Example: The BTK Killer

## Example #1: Deleted Files

- Files on a floppy
  - » Use hex editor to see what "deleted" files look like
  - » Use EnCase to examine "deleted" information

© 2003-2009, Gary C. Kessler

22



```
Command Prompt
A:\>dir
Volume in drive A is TEST_FLOPPY
Volume Serial Number is FC1A-3838

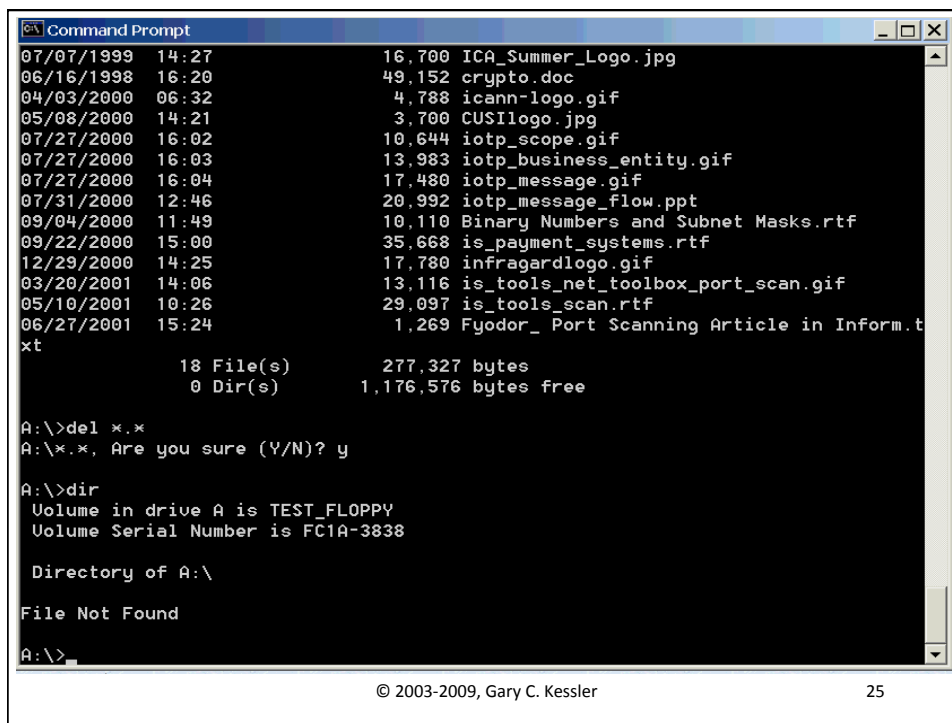
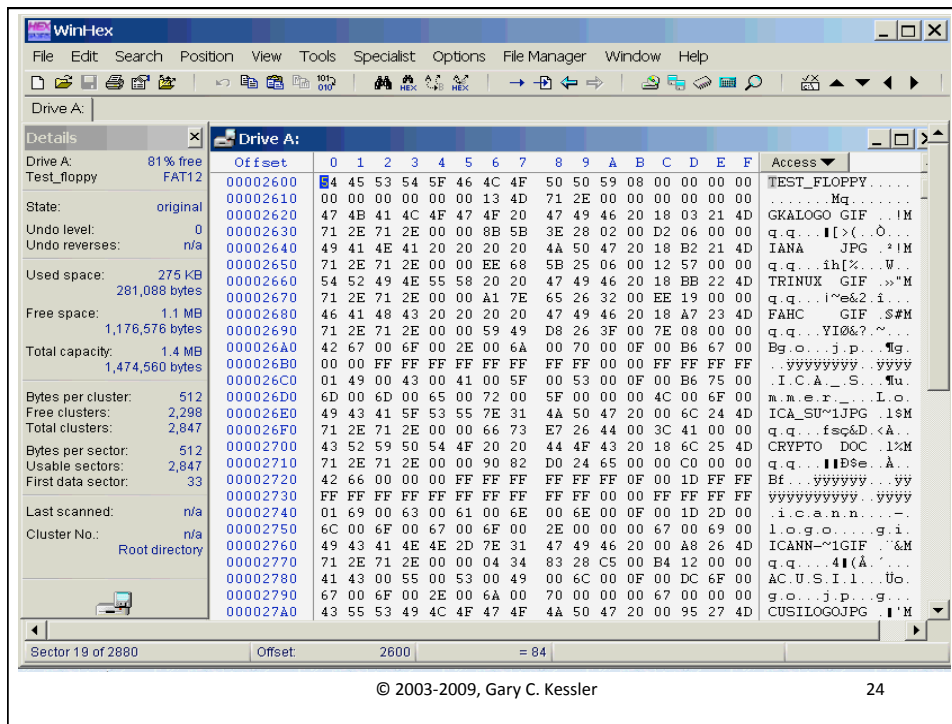
Directory of A:\

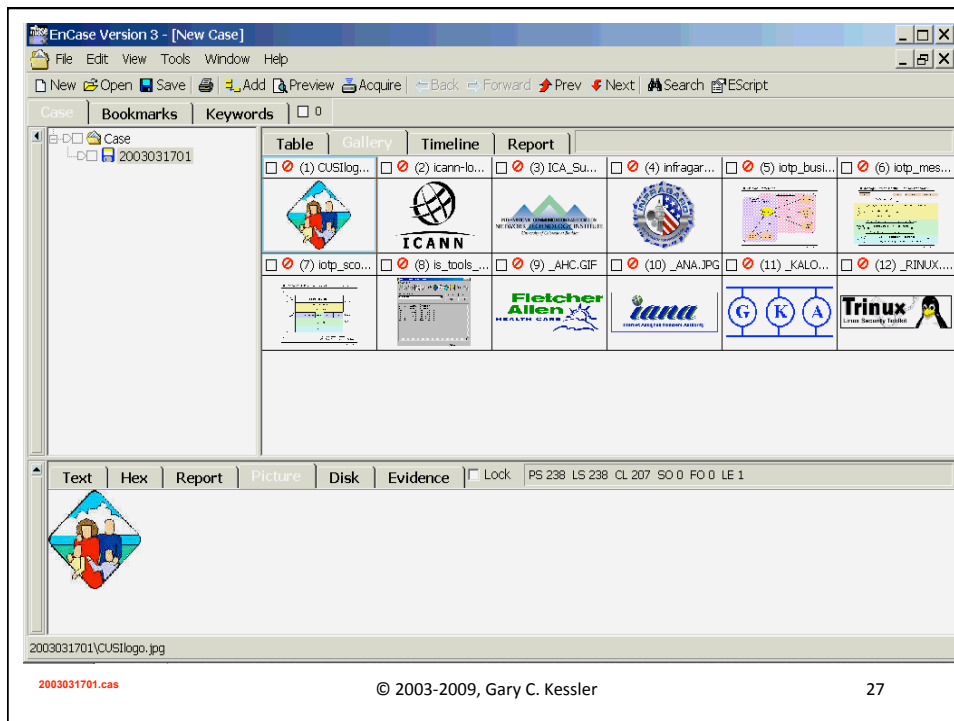
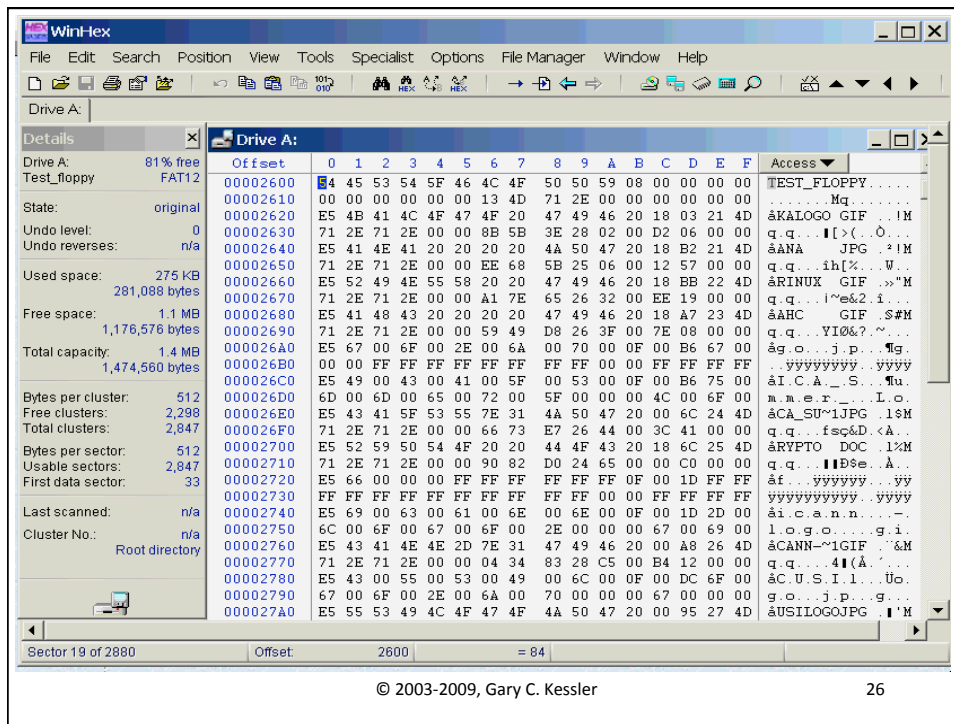
01/30/2000  11:28                1,746 gkologo.gif
10/27/1998  13:07            22,290 iana.jpg
03/05/1999  15:53                6,638 trinux.gif
06/24/1999  09:10                2,174 fahc.gif
07/07/1999  14:27            16,700 ICA_Summer_Logo.jpg
06/16/1998  16:20            49,152 crypto.doc
04/03/2000  06:32                4,788 icann-logo.gif
05/08/2000  14:21                3,700 CUSIlogo.jpg
07/27/2000  16:02            10,644 iotp_scope.gif
07/27/2000  16:03            13,983 iotp_business_entity.gif
07/27/2000  16:04            17,480 iotp_message.gif
07/31/2000  12:46            20,992 iotp_message_flow.ppt
09/04/2000  11:49            10,110 Binary Numbers and Subnet Masks.rtf
09/22/2000  15:00            35,668 is_payment_systems.rtf
12/29/2000  14:25            17,780 infragardlogo.gif
03/20/2001  14:06            13,116 is_tools_net_toolbox_port_scan.gif
05/10/2001  10:26            29,097 is_tools_scan.rtf
06/27/2001  15:24                1,269 Fyodor_ Port Scanning Article in Inform.t
xt
                18 File(s)      277,327 bytes
                0 Dir(s)        1,176,576 bytes free

A:\>
```

© 2003-2009, Gary C. Kessler

23







EnCase Version 3 - [C:\My Documents\Powerpoint\Forensics\FloppySample\2003031701.cas]

File Edit View Tools Window Help

New Open Save Add Preview Acquire Back Forward Prev Next Search ESript

Case Bookmarks Keywords

Table Gallery Timeline Report

Bookmark Type	Preview	File Name	Hit Text
28 Search Hit	ck will always be encrypt	Unallocated Clus...	crypt File
29 Search Hit	every time it is encrypt	Unallocated Clus...	crypt File
30 Search Hit	y used secret-key encrypt	Unallocated Clus...	crypt File
31 Search Hit	today is the Data Encrypt	Unallocated Clus...	crypt File
32 Search Hit	of other secret-key crypt	Unallocated Clus...	crypt File
33 Search Hit	oupled with three encrypt	Unallocated Clus...	crypt File
34 Search Hit	nternational Data Encrypt	Unallocated Clus...	crypt File
35 Search Hit	used in commercial crypt	Unallocated Clus...	crypt File
36 Search Hit	es, and number of encrypt	Unallocated Clus...	crypt File
37 Search Hit	e data. Public-Key Crypt	Unallocated Clus...	crypt File
38 Search Hit	ography Public-key Crypt	Unallocated Clus...	crypt File
39 Search Hit	lem with secret-key crypt	Unallocated Clus...	crypt File

Text Hex Report Picture Disk Evidence Lock PS 145 LS 145 CL 114 SO 314 FO 54586 LE 5

0053922 sees either two or three different keys, coupled with three encryption steps. CAST-128 (described in Request for Co  
 0054036 ments, or RFC, 2144; CAST is not an acronym but its name is derived from the initials of its inventors, Carlisle  
 0054150 Adams and Stafford Tavares of Nortel) and the International Data Encryption Algorithm (IDEA) are conceptually sim  
 0054264 lar to DES; both are 64-bit block ciphers using 128-bit keys. CAST and IDEA are also internationally available and  
 0054378 , therefore, unnumbered for use by members of the Internet community. Rivest Cipher 4 (RC4), named for its inven  
 0054492 tor Ron Rivest, is a stream cipher using variable-sized keys; it is widely used in commercial encryption product  
 0054606 s, although it can only be exported using keys that are 40 bits or less in length. RCS is a block-cipher supportin  
 0054720 g a variety of block sizes, key sizes, and number of encryption passes over the data. Public-Key Cryptography Pu  
 0054834 blic-key Cryptography (PKC) was invented in 1976 by Martin Hellman and Whitfield Diffie of Stanford University to

2003031701\Unallocated Clusters

© 2003-2009, Gary C. Kessler 28

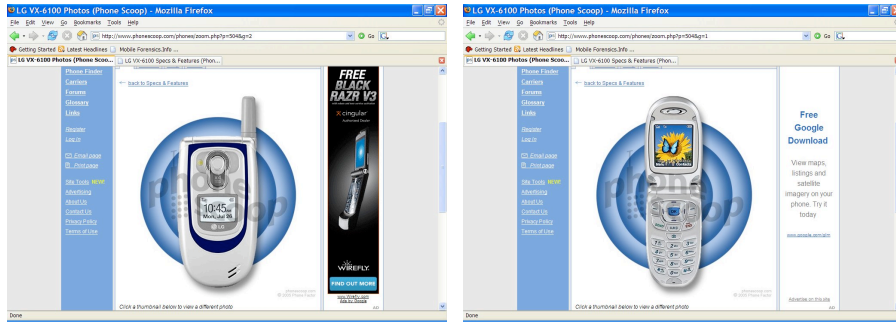
## Example #2: Web Browsers

- 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



© 2003-2009, Gary C. Kessler

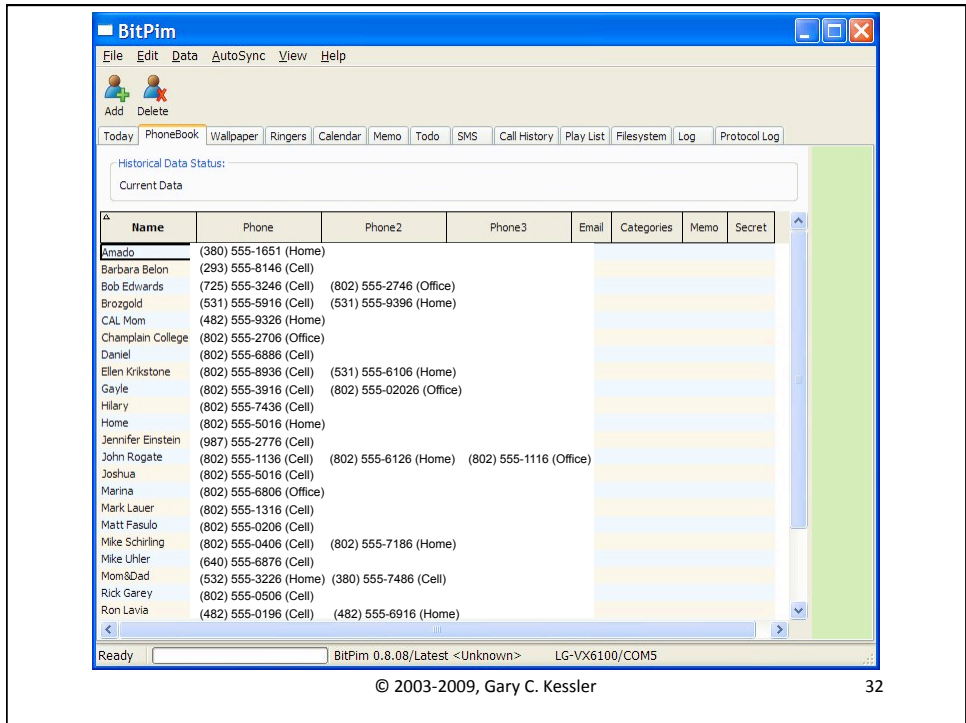
30

**Note PIN and banner message**

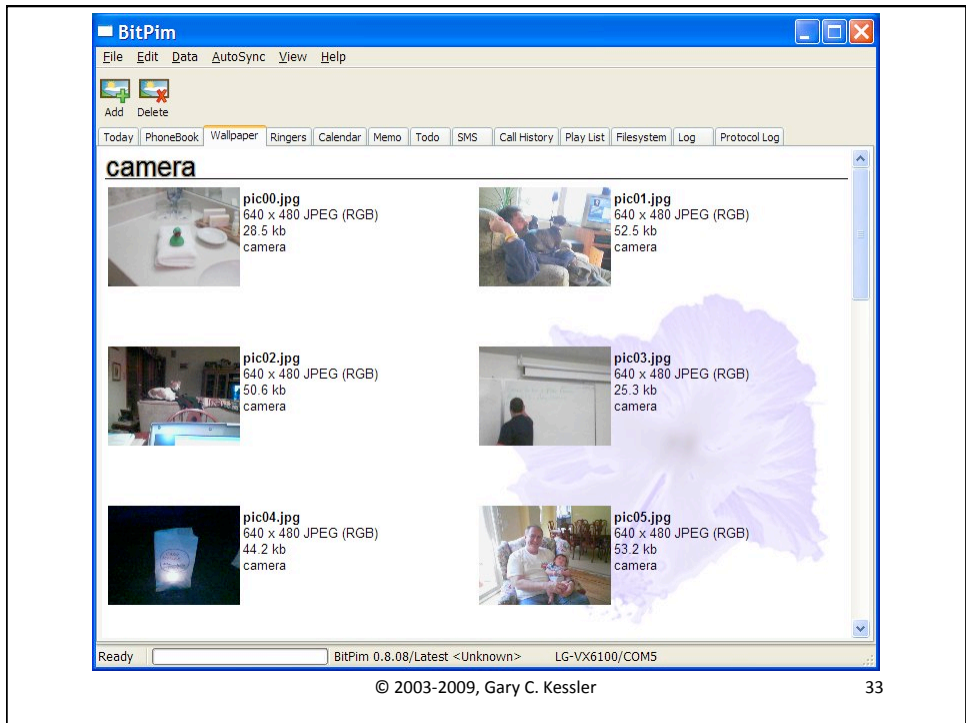
Name	Size	Date
nvm_0005	3764	
nvm_0004	2572	
nvm_0003	836	
nvm_0002	1312	
nvm_0001	8569	
nvm_0000	848	

```

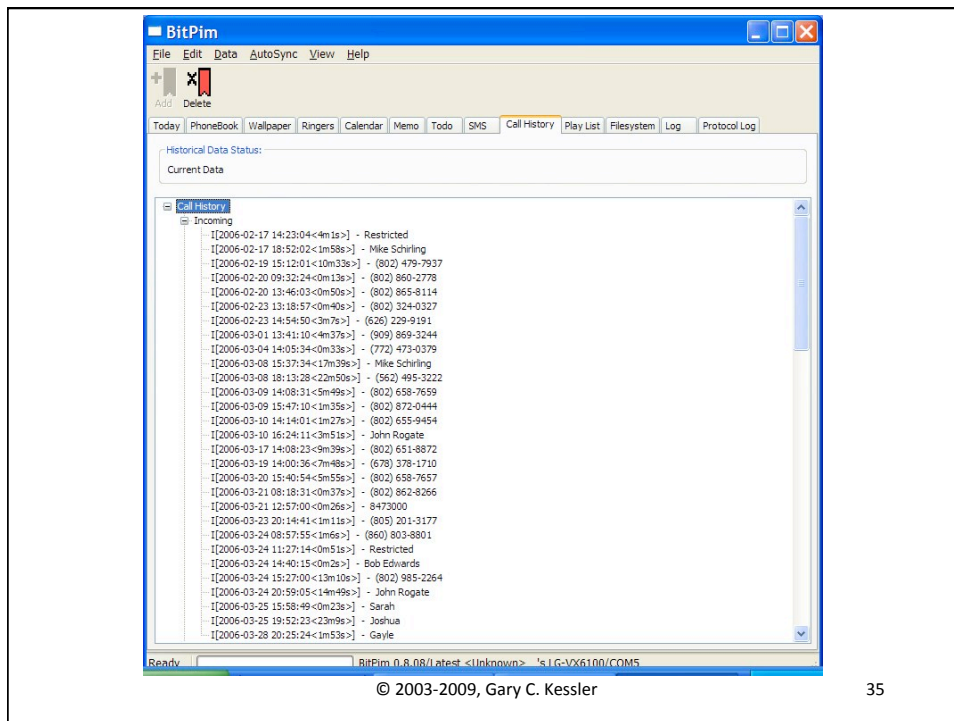
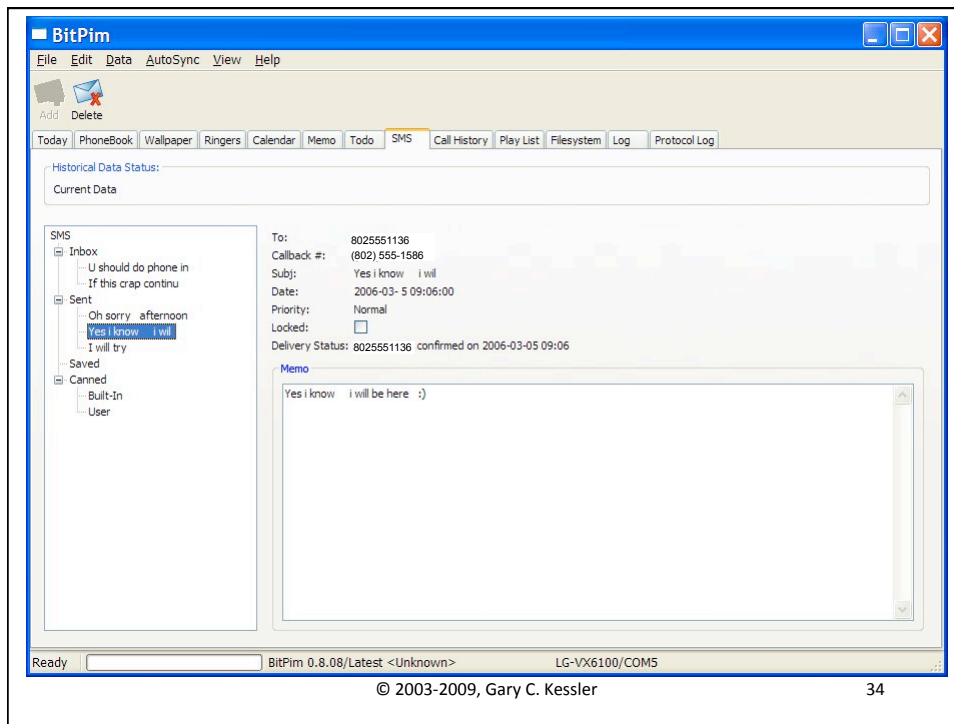
nvm/nvm/nvm_0002 Contents
00000000 00 00 00 00 01 03 01 03 01 05 01 03 00 00 01 03 .....
00000010 00 00 01 03 00 00 01 01 00 00 00 00 00 00 00 00 .....
00000020 01 01 00 00 00 00 01 00 00 00 00 00 01 00 00 00 .....
00000030 01 07 01 47 4B 41 00 00 00 00 00 00 00 00 00 00 .....GKA.....
00000040 00 00 00 00 00 01 01 00 00 00 00 00 00 00 00 00 .....
00000050 01 01 01 00 01 00 01 00 00 01 30 30 30 30 30 30 .....000000
00000060 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 .....
00000070 38 39 31 33 01 00 00 00 00 00 00 00 00 00 00 00 .....8913.....
00000080 00 00 01 0B 6D 6E 76 00 00 00 00 77 02 00 01 .....cmnv...w...
00000090 FF 6D 63 00 00 00 00 00 00 83 0E 00 01 FF 66 73 .....fs
000000A0 5F 6F 70 73 00 00 00 F3 01 00 01 01 6D 63 00 00 .....ops...mc...
000000B0 00 00 00 B3 0E 01 01 6D 63 00 00 00 00 00 00 00 .....mc...
000000C0 11 0F 00 01 01 6D 63 00 00 00 00 00 00 00 00 .....mc...
000000D0 01 01 6D 63 00 00 00 00 00 00 1D 1E 00 01 01 6D .....mc...m
000000E0 63 00 00 00 00 00 00 29 1E 00 01 01 75 69 73 73 .....uis...
000000F0 6D 73 00 00 F0 04 00 01 01 6D 63 00 00 00 00 00 .....ms...
00000100 00 34 1E 00 01 FF 75 69 78 6E 76 00 00 00 7A 05 .....4...uixnv...z
00000110 00 01 01 6D 63 00 00 00 00 00 00 3F 1E 00 01 01 .....mc...?...
00000120 6D 63 00 00 00 00 00 00 4B 1E 00 01 01 72 66 00 .....mc...K...rf.
00000130 00 00 00 00 00 50 07 00 01 01 6D 63 63 64 6D 61 .....P...mccdma
    
```



32



33



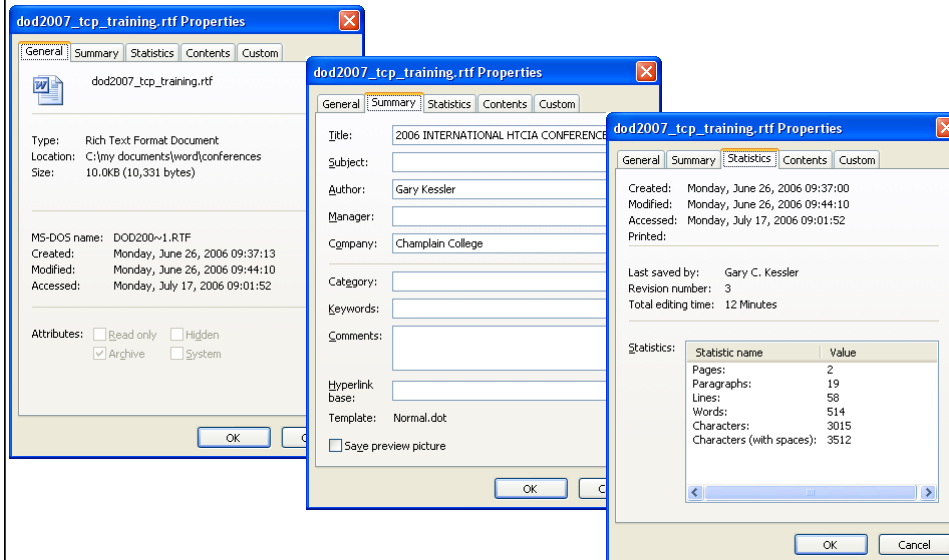
## Example #4: Metadata

- *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

© 2003-2009, Gary C. Kessler

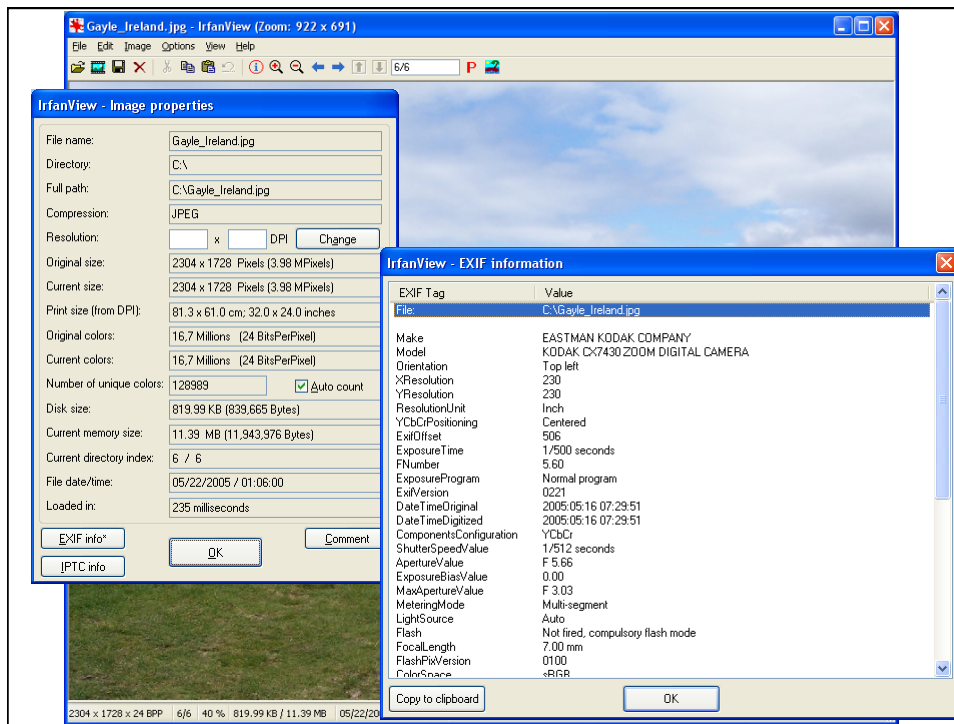
36

## Metadata in MS Office



© 2003-2009, Gary C. Kessler

37



## 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

## Parting 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](mailto:gary.kessler@champlain.edu)  
**Skype:** [gary.c.kessler](https://www.skype.com/people/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.