CHAMPLAIN COLLEGE

Computer and Digital Forensics

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

© 2003-2009, Gary C. Kessler

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

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

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

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

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

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

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

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

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

© 2003-2009, Gary C. Kessler

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?

© 2003-2009, Gary C. Kessler

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

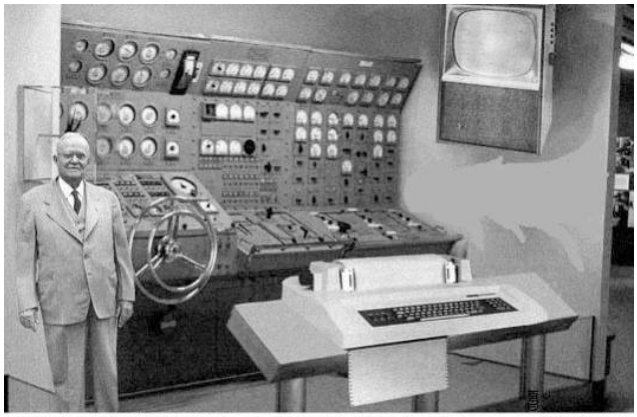
© 2003-2009, Gary C. Kessler

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}."

© 2003-2009, Gary C. Kessler

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 30 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

A Typical Home Computer

Source: National White Collar Crime Center

© 2003-2009, Gary C. Kessler

Computers

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



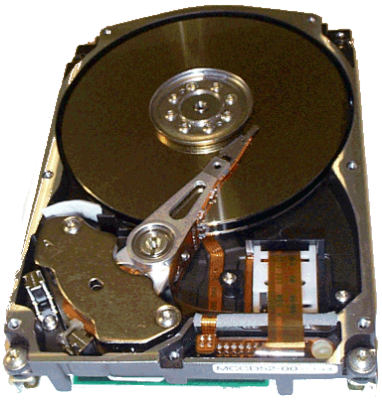





© 2003-2009, Gary C. Kessler

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



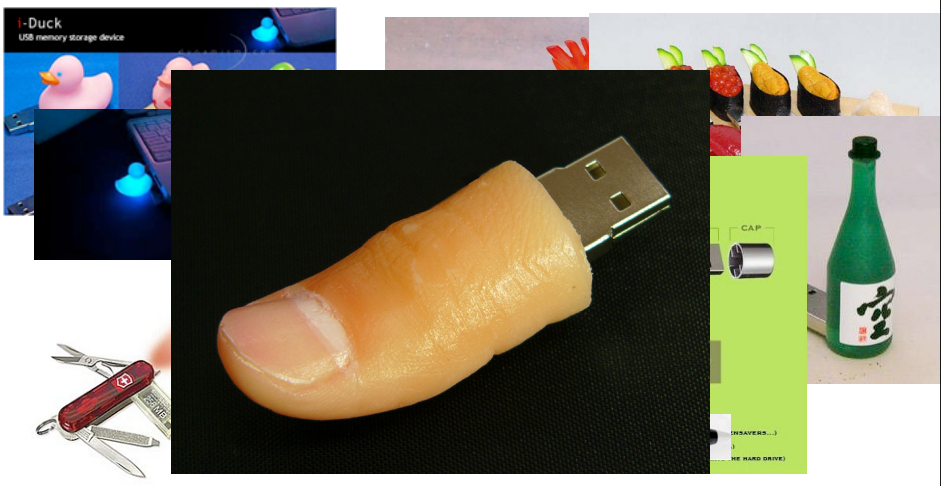
© 2003-2009, Gary C. Kessler

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

© 2003-2009, Gary C. Kessler

So, Where is All This Information?

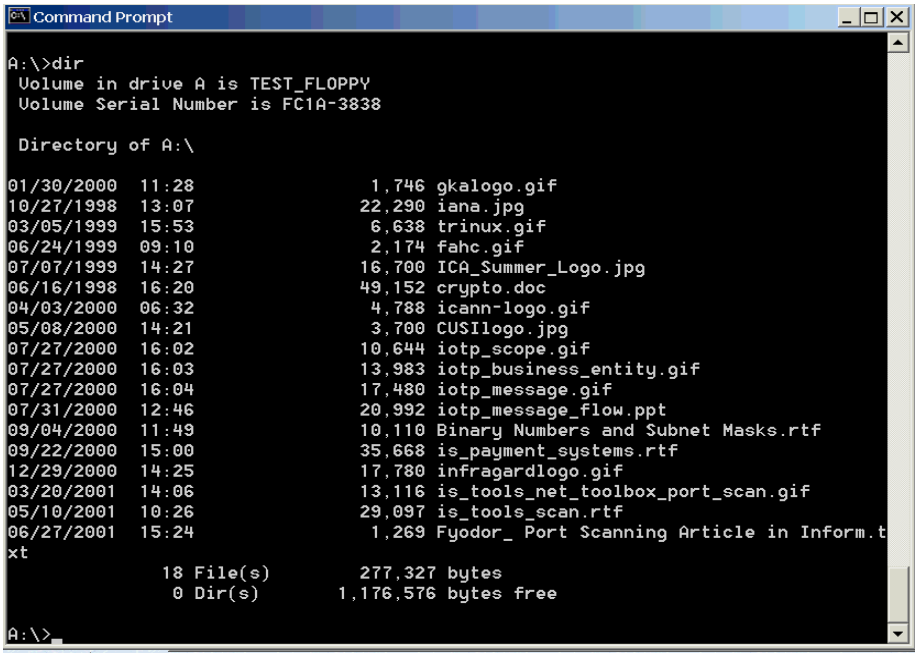
- Example #1: Deleted Files
- Example #2: Web Browsers
- Example #3: Cell Phones
- Example #4: Metadata
- Real Example: The BTK Killer

© 2003-2009, Gary C. Kessler

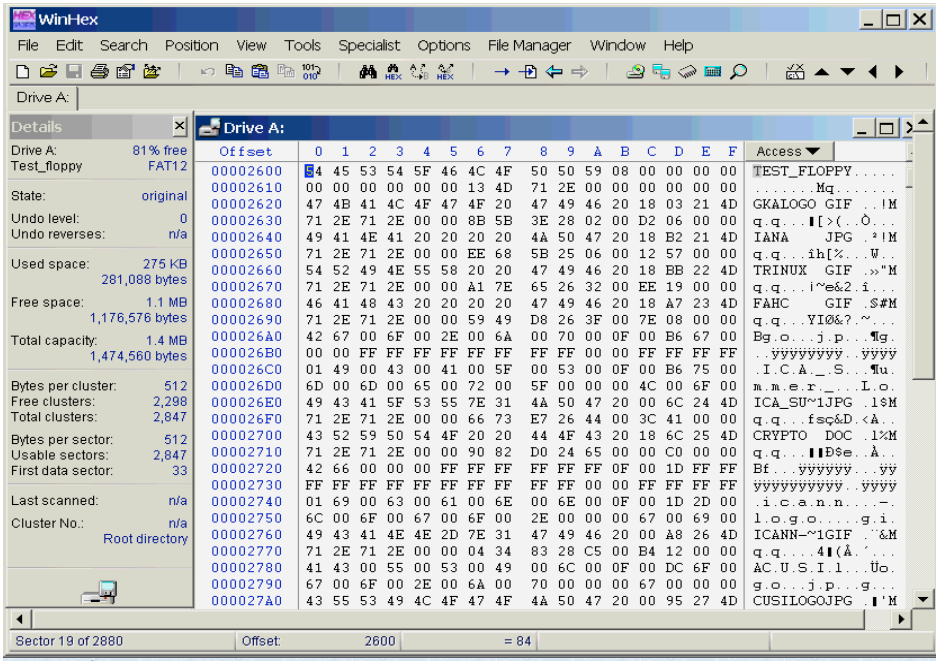
Example #1: Deleted Files

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

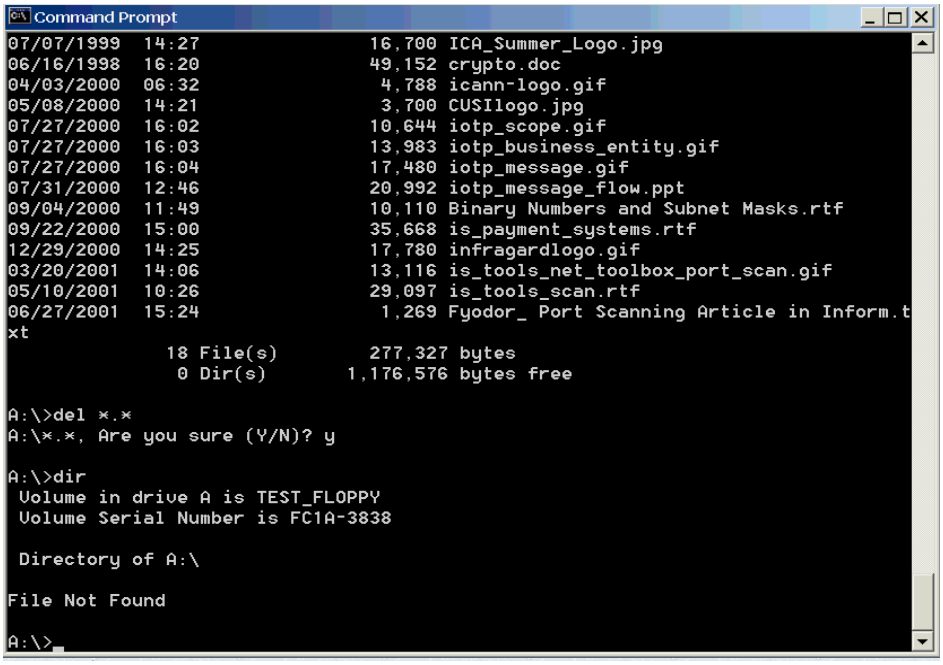
© 2003-2009, Gary C. Kessler



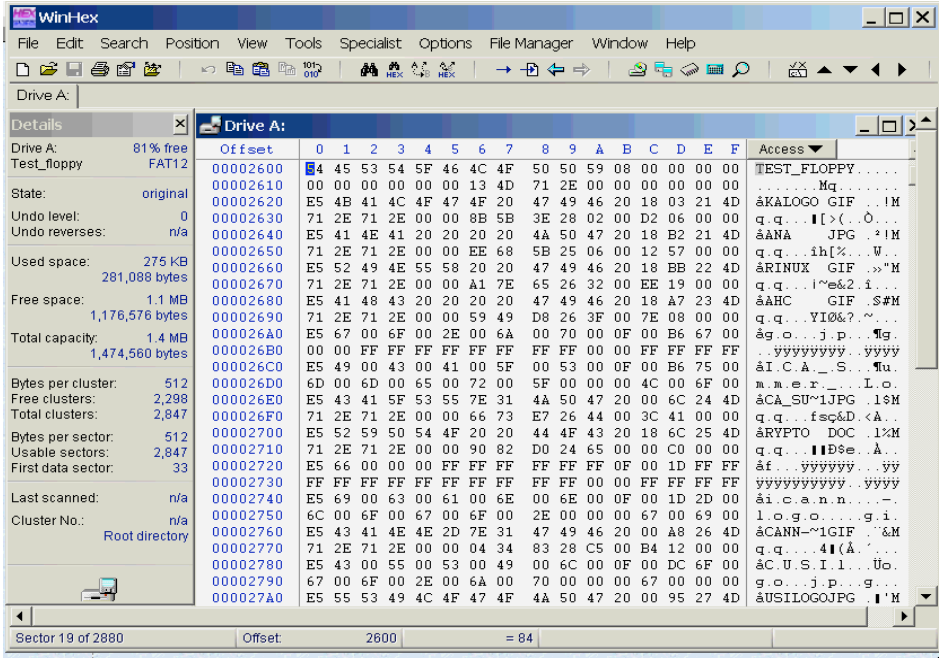
© 2003-2009, Gary C. Kessler

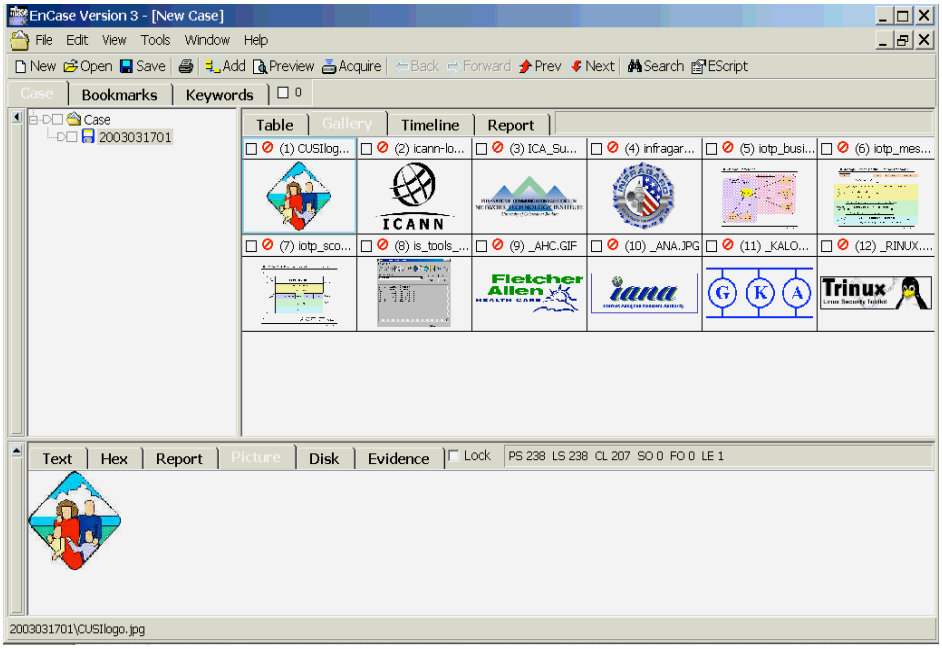


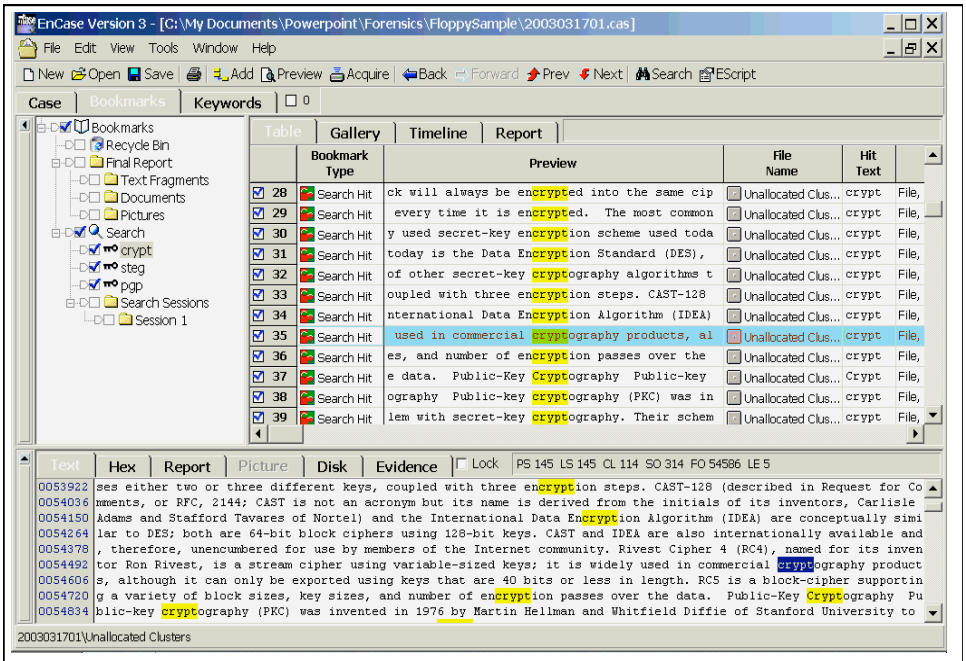
© 2003-2009, Gary C. Kessler



© 2003-2009, Gary C. Kessler


WinHex
File Edit Search Position View Tools Specialist Options File Manager Window Help
Drive A:
Details
Drive A: 81% free
Test_floppy FAT12
State: original
Undo level: 0
Undo reverses: n/a
Used space: 275 KB
281,088 bytes
Free space: 1.1 MB
1,176,576 bytes
Total capacity: 1.4 MB
1,474,560 bytes
Bytes per cluster: 512
Free clusters: 2,298
Total clusters: 2,847
Bytes per sector: 512
Usable sectors: 2,847
First data sector: 33
Last scanned: n/a
Cluster No.: n/a
Root directory
Drive A:
Offset 0 1 2 3 4 5 6 7 8 9 A B C D E F Access
00002600 E4 45 53 54 5F 46 4C 4F 50 50 59 08 00 00 00 00 TEST_FLOPPY.....
00002610 00 00 00 00 00 00 13 4D 71 2E 00 00 00 00 00 00 ....Mq.......
00002620 E5 4B 41 4C 4F 47 4F 20 47 49 46 20 18 03 21 4D åKALOGO GIF ..!M
00002630 71 2E 71 2E 00 00 8B 5B 3E 28 02 00 D2 06 00 00 q.q...‹[>(..Ò...
00002640 E5 41 4E 41 20 20 20 20 4A 50 47 20 18 B2 21 4D åANA JPG .²!M
00002650 71 2E 71 2E 00 00 EE 68 5B 25 06 00 12 57 00 00 q.q...îh[%...W..
00002660 E5 52 49 4E 55 58 20 20 47 49 46 20 18 BB 22 4D åRINUX GIF .»"M
00002670 71 2E 71 2E 00 00 A1 7E 65 26 32 00 EE 19 00 00 q.q...¡~e&2.î...
00002680 E5 41 48 43 20 20 20 20 47 49 46 20 18 A7 23 4D åAHC GIF .S#M
00002690 71 2E 71 2E 00 00 59 49 D8 26 3F 00 7E 08 00 00 q.q...YIØ&?.~...
000026A0 E5 67 00 6F 00 2E 00 6A 00 70 00 0F 00 B6 67 00 åg.o...j.p...¶g.
000026B0 00 00 FF FF FF FF FF FF FF FF 00 00 FF FF FF FF ..ÿÿÿÿÿÿÿÿ..ÿÿÿÿ
000026C0 E5 49 00 43 00 41 00 5F 00 53 00 0F 00 B6 75 00 åI.C.A._.S...¶u.
000026D0 6D 00 6D 00 65 00 72 00 5F 00 00 00 4C 00 6F 00 m.m.e.r._...L.o.
000026E0 E5 43 41 5F 53 55 7E 31 4A 50 47 20 00 6C 24 4D åCA_SU~1JPG .l$M
000026F0 71 2E 71 2E 00 00 66 73 E7 26 44 00 3C 41 00 00 q.q...fsç&D.<A..
00002700 E5 52 59 50 54 4F 20 20 44 4F 43 20 18 6C 25 4D åRYPTO DOC .l%M
00002710 71 2E 71 2E 00 00 90 82 D0 24 65 00 00 C0 00 00 q.q...ÐÐ$e..À..
00002720 E5 66 00 00 00 FF FF FF FF FF FF FF 0F 00 1D FF åf...ÿÿÿÿÿÿÿ...ÿÿ
00002730 FF FF FF FF FF FF FF FF FF FF 00 00 FF FF FF FF ÿÿÿÿÿÿÿÿÿÿ..ÿÿÿÿ
00002740 E5 69 00 63 00 61 00 6E 00 6E 00 0F 00 1D 2D 00 åi.c.a.n.n....-.
00002750 6C 00 6F 00 67 00 6F 00 2E 00 00 00 67 00 69 00 l.o.g.o.....g.i.
00002760 E5 43 41 4E 4E 2D 7E 31 47 49 46 20 00 A8 26 4D åCANN-~1GIF .¨&M
00002770 71 2E 71 2E 00 00 04 34 83 28 C5 00 B4 12 00 00 q.q....4Ð(Å.´...
00002780 E5 43 00 55 00 53 00 49 00 6C 00 0F 00 DC 6F 00 åC.U.S.I.l...Üo.
00002790 67 00 6F 00 2E 00 6A 00 70 00 00 00 67 00 00 00 g.o...j.p...g...
000027A0 E5 55 53 49 4C 4F 47 4F 4A 50 47 20 00 95 27 4D åUSILOGOJPG .•'M
Sector 19 of 2880
Offset: 2600
= 84

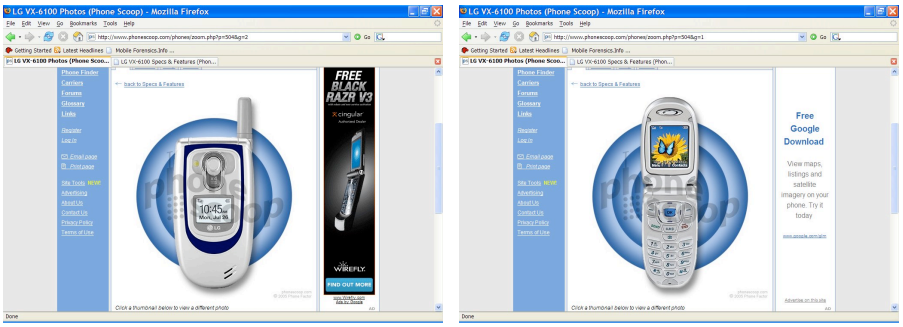

EnCase Version 3 - [New Case]
File Edit View Tools Window Help
New Open Save Add Preview Acquire Back Forward Prev Next Search EScript
Case Bookmarks Keywords 0
Case
2003031701
Table Gallery Timeline Report
(1) CUSIlog...
(2) icann-lo...
(3) ICA_Su...
(4) infragar...
(5) iotp_busi...
(6) iotp_mes...
(7) iotp_sco...
(8) is_tools_...
(9) _AHC.GIF
(10) _ANA.JPG
(11) _KALO...
(12) _RINUX....
Text Hex Report Picture Disk Evidence Lock
PS 238 LS 238 CL 207 SO 0 FO 0 LE 1
2003031701\CUSIlogo.jpg
2003031701.cas



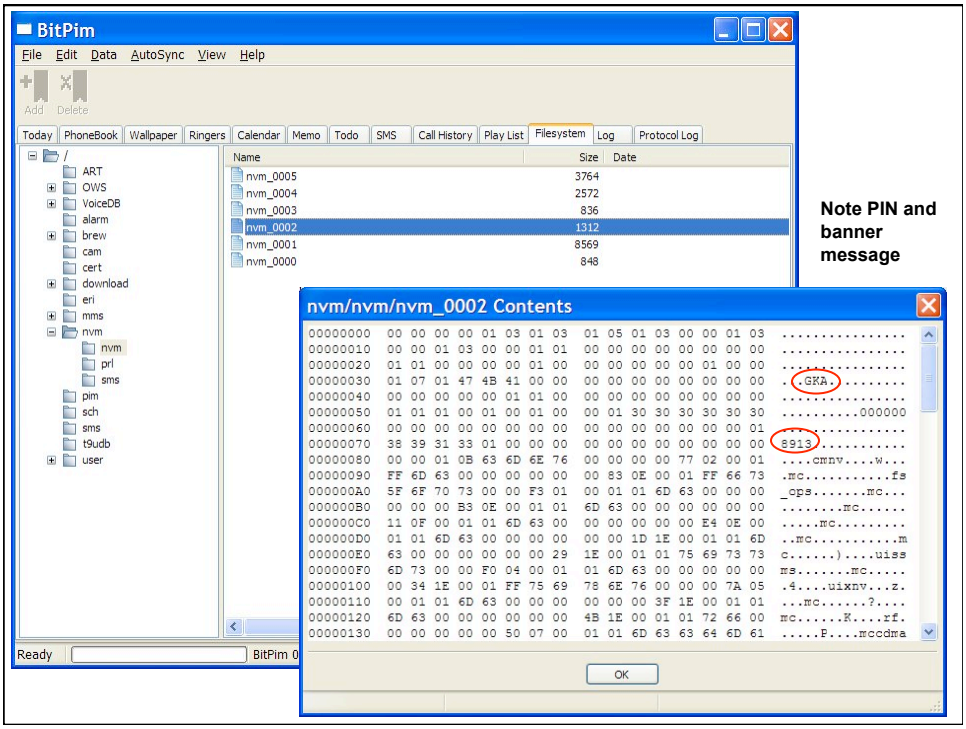
Example #2: Web Browsers

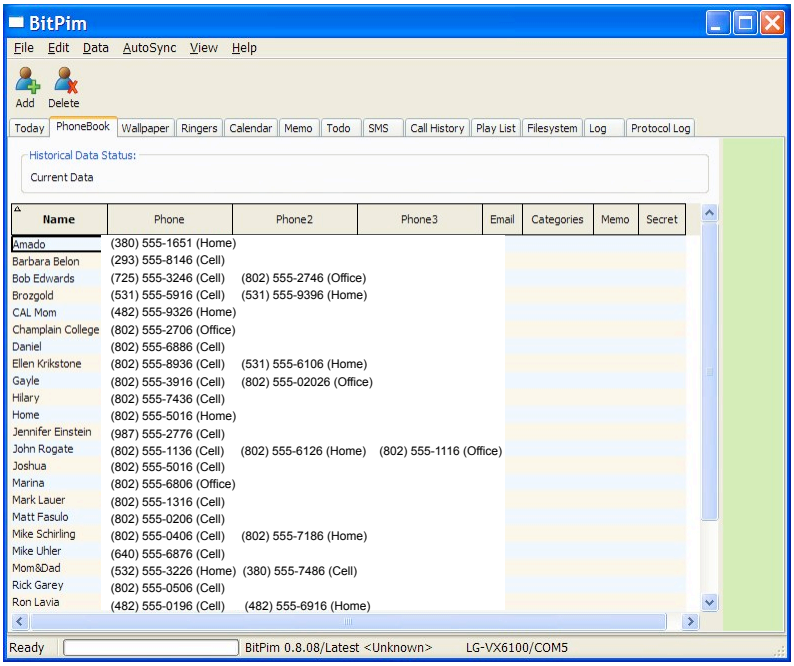
- Browser store just about everything
  - » Registry keys and directories
  - » Bookmarks, cookies, browser history, Internet cache, typed URLs, stored forms, stored passwords, download tracking
- IE and Firefox are predominate browsers but there are many others in wide use
  - » AOL
  - » Epiphany
  - » Netscape
  - » Opera
  - » Safari

Example #3: Mobile Phones

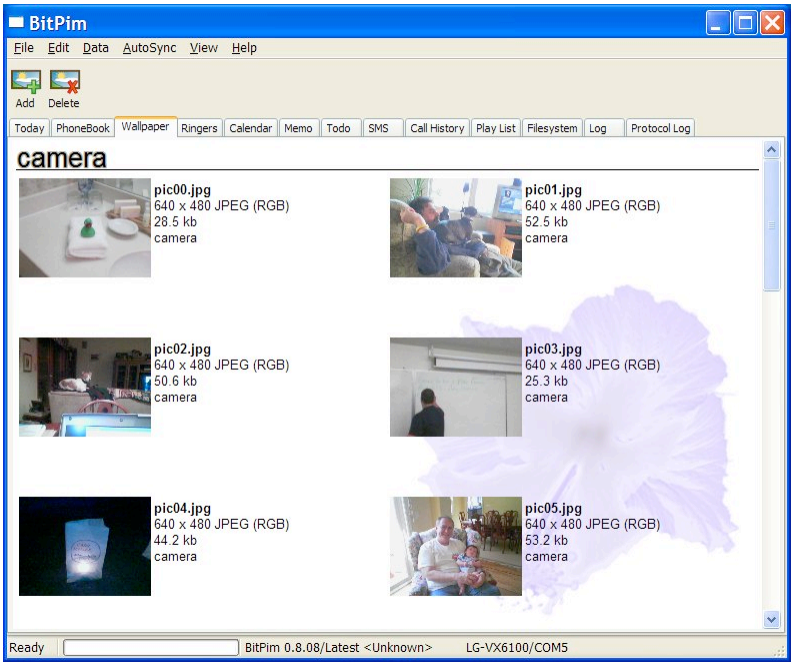


© 2003-2009, Gary C. Kessler

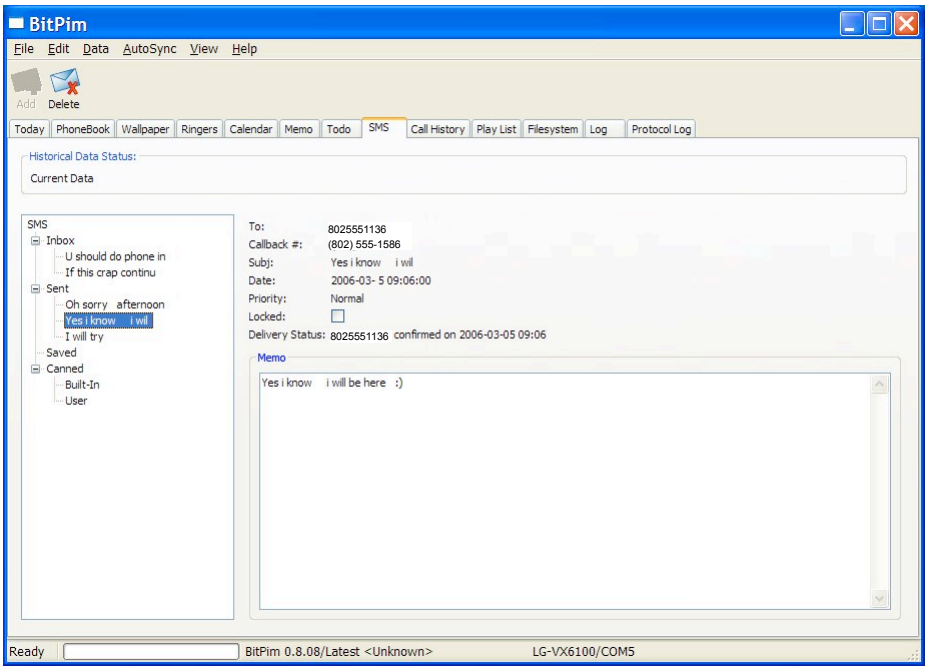




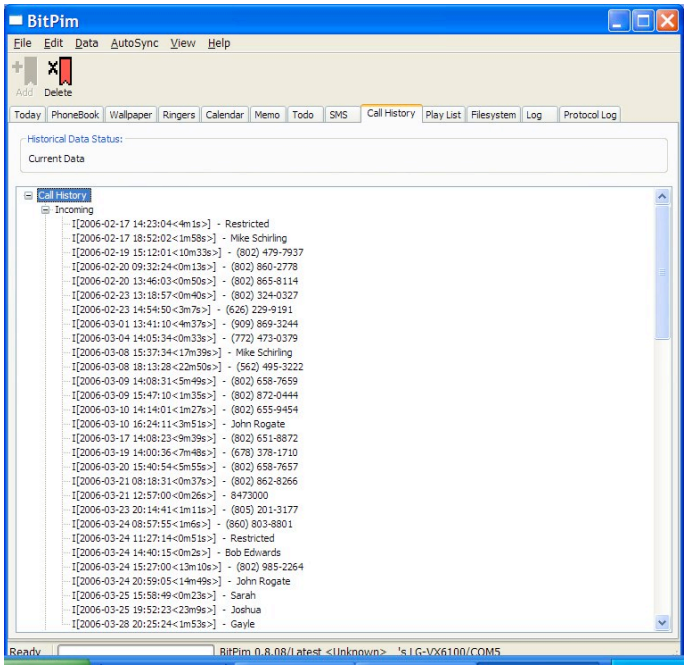
© 2003-2009, Gary C. Kessler 32



© 2003-2009, Gary C. Kessler 33



© 2003-2009, Gary C. Kessler 34



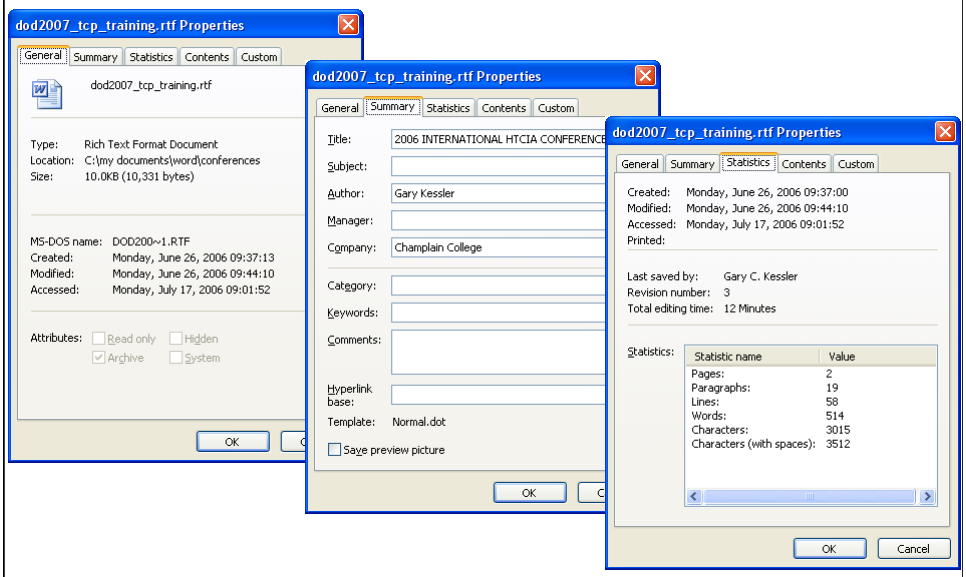
© 2003-2009, Gary C. Kessler 35

Example #4: Metadata

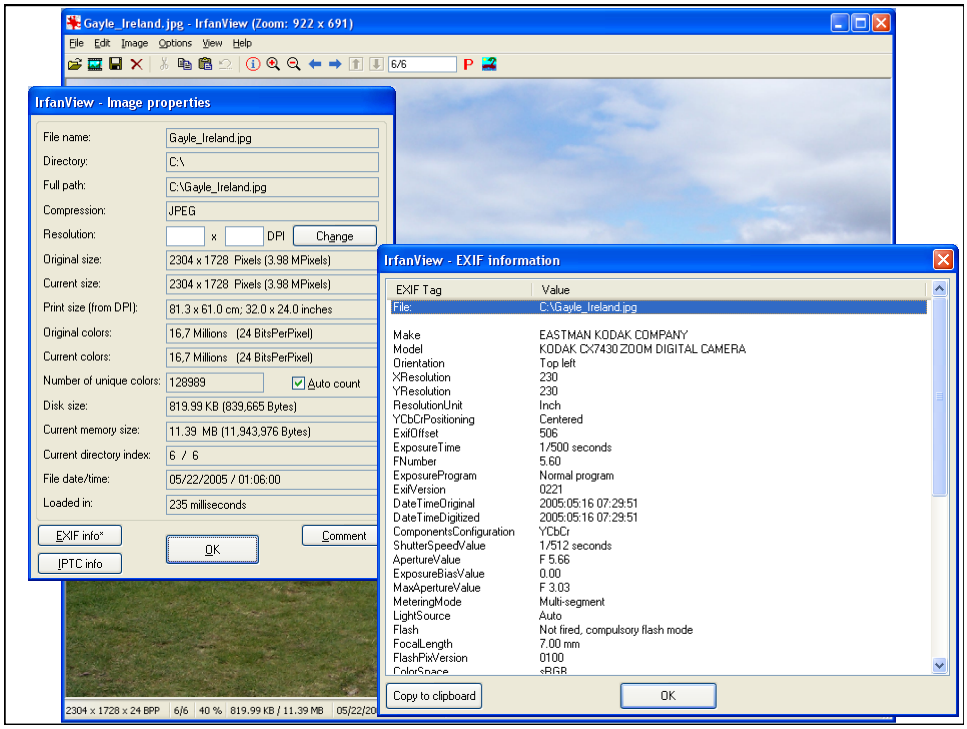
- *Metadata* is data about data
  - » Information that describes the *contents* of a container or describes the *container* itself
- Type of metadata
  - » File system: Location and size, pertinent dates
  - » Document: Author, organization
  - » Image: Source software/hardware

© 2003-2009, Gary C. Kessler

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

© 2003-2009, Gary C. Kessler

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

© 2003-2009, Gary C. Kessler

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

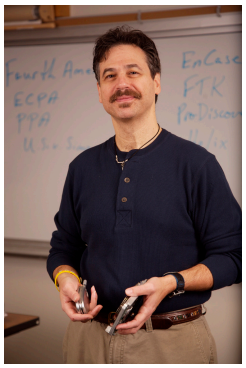
© 2003-2009, Gary C. Kessler

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.

© 2003-2009, Gary C. Kessler