



Digital Forensics

Finding information that has been lost...

BJ Gleason



The Morning Calm - Mar 24, 2003

An investigation revealed that a dependant scanned his military ID card, altered the date of birth and printed it from an off-post computer. The dependant then laminated his ID card and used it to gain access to an off-post drinking establishment. Further investigation revealed that the dependant provided two other underage dependants with scanned ID cards with altered dates of birth. This incident remains under investigation by Criminal Investigation Division.

The Bush Bill

Sep 6, 2004

Accepted at Food Lion in North Carolina for \$150 of groceries.

Cashier gave \$50 change. Another man arrested for using bills later.



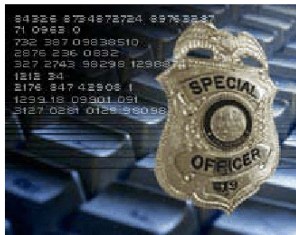
TECHNOLOGY

Cyber-cops to patrol Internet chatrooms

Wednesday, June 9, 2004 Posted: 10:03 AM EDT (1403 GMT)

LONDON, England (Reuters) -- Police plan to patrol Internet chatrooms as part of a multinational crackdown on pedophile rings.

They will also seize the finances of Web site operators who peddle child pornography and freeze the credit cards of their customers.



Korea Times, May 31, 2004

Cyber Crimes by Teens Surge

By Na Jeong-ju
Staff Reporter

Crimes committed by teens on the Internet have been rising steeply over the past several years, despite stepped-up efforts by law enforcement authorities to crack down on cyber crime.



For the first time, the number of minors who received penalties surpassed the 10,000 mark last year, amid fears that more and more youths will be exposed to crimes with expanding subscriptions to the Internet.

Illegal sales of items used on the multi-player online game sites and **hacking** of such items are mostly committed by teens, many having little sense of guilt over crimes committed in the virtual world.

According to the National Police Agency's Cyber Terror Response Center, about 70 percent of the crimes committed by youth were related to multi-user online games. Last year, 10,187 juveniles were arrested by police for their attempts to hack the game sites and trade the items they stole as well as for other Internet-related crimes. This means everyday 28 young people become criminals due to the multi-user games.

STARS AND STRIPES Wednesday, August 4, 2004

Child porn ends petty officer's career

O'Brien sailor gets 3 months in jail and bad-conduct discharge

BY NANCY MONTGOMERY
Stars and Stripes

YOKOSUKA NAVAL BASE, Japan — The long arm of the law reached halfway around the world Monday to pluck a once-promising petty officer from the Navy for viewing and possessing child pornography.

Petty Officer 1st Class Michael Schlink, an electronics technician on the destroyer USS O'Brien, was sentenced Monday to three months in jail and a bad-conduct discharge after pleading guilty to receiving and possessing some 300 pornographic images of girls under 18. The maximum imprisonment military judge Cmdr. John Makoyra could have imposed is one year.

Prosecutors had argued for a six-month sentence, saying that to be an exemplary sailor means more than being a good worker.

"We have to do the right thing," said Lt. Stella Lane.

The defense had asked for three months' confinement and no discharge.

Lt. Mary Thompson told the judge that most of the photos involved teenage girls under 18 in explicit poses, not prepubescent girls. "This is not someone who's obsessed with children," Thompson said. "Simply looking at photographs is all [he's] done."

Schlink, 32, described at sentencing by three senior and master chiefs he'd worked for as "100 percent dependable" and "outstanding," apologized to crewmates and his family. He said he most regretted the damage his actions had contributed to the lives of girls sexually exploited on pornographic Web sites.

He also regretted the damage to himself, he said. "Until Jan. 21 of this year, I was widely respected on the ship," he said.

Naval Criminal Investigative Service agents seized Schlink's computer several months ago after receiving a list of suspected offenders from U.S. Immigration and Customs Enforcement (ICE), in the Washington, D.C., area, prosecutors said.

The federal agency began an ongoing law-enforcement initiative in July 2003 called "Operation Predator" to target child-sex offenders, including human traffickers, pornographers and "Internet predators," among others, according to the ICE Web site.

Numerous arrests resulted from one particular investigation into global Internet child pornography. That investigation targeted a company in Belarus called Regpay, which the government says provided credit card billing services for more than 50 child-pornography sites.

In a February news release, ICE said its agents worldwide were focusing on people who'd purchased child pornography memberships from Regpay-affiliated Web sites, and that some 270,000 credit card transactions had been seized and thousands of suspects were being investigated.

Nether Yokosuka prosecutors use Yokosuka's NCTS assistant special agent in charge could confirm Monday that Schlink's prosecution was among those resulting from the Regpay investigation.

Schlink, a married father of two, told investigators he thought he had developed a problem with pornography in general, viewing it frequently during the week until his wife returned home from work, and that it had created tension in his marriage.

On Monday, the judge offered that he often went home after work and logged on to the "BBC, CNN," or kept up with sports on his computer. What did Schlink do on his computer? the judge asked.

"Surf for porn, sir," Schlink said.

Send Nancy Montgomery at: montgomery@stripes.com

In The News

Toronto police find hotel where child-porn pictures taken

Fri, 04 Feb 2005 19:47:04 EST
CBC News

TORONTO - Tips from people living in the Toronto area have led investigators to a hotel in the southern United States where pornographic photos of an unidentified child were taken.

One of the altered pictures police used to identify the U.S. hotel. The photos have been widely distributed on the internet by pedophiles.

On Thursday, Toronto Police released copies with the victim digitally removed, in hopes that someone could tell them who the victim is and where the crimes took place.



In the News

Police Hope photo of possible witness leads to child porn victim.

Thursday, April 28, 2005 Posted: 5:15 AM EDT

ORLANDO, Florida (CNN) -- Florida and Canadian law enforcement officials Wednesday released the picture of a young girl, reclining on a couch, who authorities described as a possible witness in an Internet child pornography investigation.

Authorities said they found the image of the girl, who appears to be about 11, on child pornography Web sites, although not photographed in an inappropriate way. They did not say specifically what the girl may know.

\$5000

FOR INFORMATION

If you know the identity of the material witness involved in a child pornography case pictured below, please call **Crimeline** at **866-635-HELP (4357)**.

CRIMELINE
866.635.HELP
(4357)

Case Study

The CSI Effect

The CSI Effect

Serious concerns that the general public (who comprise the juries) are learning bad science from TV shows like CSI. They often have unrealistic ideas of what criminal science can deliver.



FBI believe that CSI is educating criminals in how to leave a "squeaky clean" crime scene.

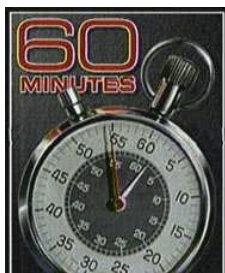
Biggest problems

- Wearing too many hats
- Obvious clues
- Unrealistically quick results
- Complete databases
- Abuse of civil rights
- Obvious motives ignored
- Questionable technology
- Unlimited zoom on surveillance videos

Remember: It's entertainment, not science.

Case Study

The Bush Memos



60 Minutes II

September 8, 2004

CBS produced 32-year-old memos detailing President Bush's National Guard Duty.

CBS said its experts who examined the documents concluded that they were authentic.

The Memo

18 August 1973

Memo to File

SUBJECT: CYA

1. Staudt has obviously pressured Hodges more about Bush. I'm having trouble running interference and doing my job. Harris gave me a message today from Grp regarding Bush's OETR and Staudt is pushing to sugar coat it. Bush wasn't here during rating period and I don't have any feedback from 187th in Alabama. I will not rate. Austin is not happy today either.

2. Harris took the call from Grp today. I'll backdate but won't rate. Harris agrees.

The problems

"from 187th in"
Typewriters in 1973 didn't have superscripts.

Proportional Fonts
Most typewriters in 1973 used fixed fonts. Proportional not widely used, and probably not in the military.

The Word Document

18 August 1973

Memo to File

SUBJECT: CYA

1. Staudt has obviously pressured Hodges more about Bush. I'm having trouble running interference and doing my job. Harris gave me a message today from Grp regarding Bush's OETR and Staudt is pushing to sugar coat it. Bush wasn't here during rating period and I don't have any feedback from 187th in Alabama. I will not rate. Austin is not happy today either.

2. Harris took the call from Grp today. I'll backdate but won't rate. Harris agrees.

Both Documents Superimposed

18 August 1973

Memo to File

SUBJECT: CYA

1. Staudt has obviously pressured Hodges more about Bush. I'm having trouble running interference and doing my job. Harris gave me a message today from Grp regarding Bush's OETR and Staudt is pushing to sugar coat it. Bush wasn't here during rating period and I don't have any feedback from 187th in Alabama. I will not rate. Austin is not happy today either.

2. Harris took the call from Grp today. I'll backdate but won't rate. Harris agrees.

Results

CBS: Bush Memo Story A 'Mistake'

NEW YORK, Sept. 20, 2004



(Photo: CBS)

(CBS/AP) CBS News said Monday it cannot prove the authenticity of documents used in a *60 Minutes* story about President Bush's National Guard service and that airing the story was a "mistake" that CBS regretted.

CBS News Anchor Dan Rather, the reporter of the original story, **apologized**.

CBS News claimed a source had misled the network on the documents' origins. The network pledged "an independent review of the process by which the report was prepared and broadcast to help determine what actions need to be taken."

Case Study

The BTK Killer

The BTK Killer

Was a serial killer who murdered at least ten people in and around Wichita, Kansas, between 1974 and 1991. He called himself the BTK killer, which stands for Bind, Torture, and Kill. Letters were written soon after the killings to police and to local news outlets, boasting of the crimes and knowledge of details. After a long hiatus, these letters resumed in 2004.

Going Hi-Tech

BTK asked the police that if he put his writings onto a floppy disk if the disk could be traced or not. He received his answer in a newspaper ad posted in the Wichita Eagle saying it would be OK.

On Feb. 16, 2005 he sent a message to Wichita's Fox affiliate on a floppy disk.



Examining the Disk

Name	File Ext	Is Deleted	Last Written	Last Accessed	File Created
X Test A.rtf	rtf	•	02/12/05 11:12:22AM	02/14/05	02/10/05 06:05:34PM
X Test A.rtf	rtf	•	02/10/05 06:05:36PM	02/12/05	02/10/05 06:05:34PM
Test A.rtf	rtf		02/14/05 02:47:44PM	02/14/05	02/10/05 06:05:34PM
● Test A.rtf	rtf		02/10/05 06:05:36PM	02/10/05	02/10/05 06:05:34PM
X _WRD0000.TMP	TMP	•	02/12/05 11:12:22AM	02/12/05	02/10/05 06:05:34PM
X _WRD0000.TMP	TMP	•	02/10/05 06:05:36PM	02/10/05	02/10/05 06:05:34PM
X _WRD0000.TMP	TMP	•	02/14/05 02:47:44PM	02/14/05	02/10/05 06:05:34PM
X _WRL0001.TMP	TMP	•	02/10/05 06:05:36PM	02/12/05	02/10/05 06:05:34PM
○ _WRL0001.TMP	TMP		02/12/05 11:12:22AM	02/14/05	02/10/05 06:05:34PM

Previous versions, other deleted files.

On the Disk

A forensic examination showed a valid file titled 'Test A.RTF.' The document stated:

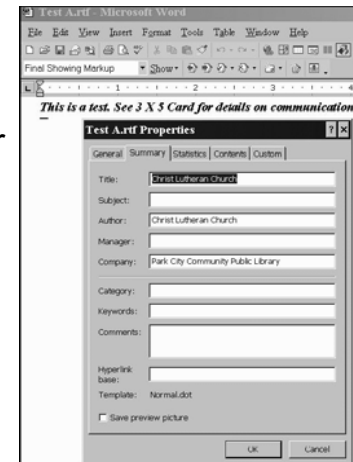
"This is a test. See 3X5 Card for details on Communication with me in the newspaper."

The index card included instructions for future communications through the classified ads.

Examining the File

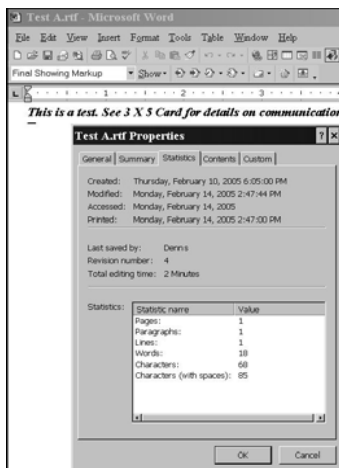
The metadata for the document.

"Christ Lutheran Church"

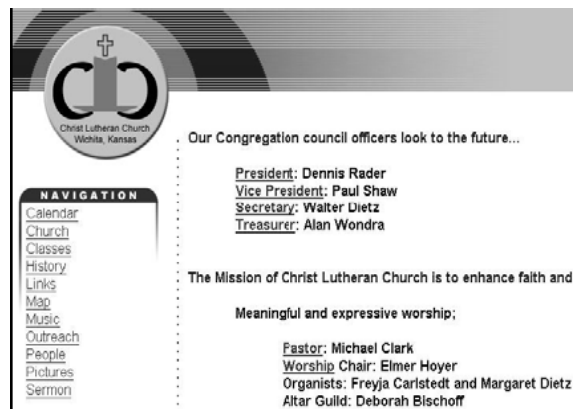


More Clues on the Disk

Saved by "Dennis"



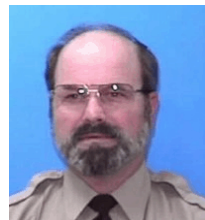
And a Quick Internet Search Later...



Caught

Obtained Rader's daughter's DNA sample to compare with samples found on victims - familial match.

Rader arrested on Feb 25th, confessed on the 26th. On Aug 18th, he was sentenced to ten consecutive life terms, which requires a minimum of 175 years without a chance of parole.



Introduction to Digital Forensics

Applying Forensic Science to PCs

Authorization and Preparation
Identification
Documentation, Collection (Seizure),
and Preservation
Examination and Analysis
Reconstruction
Reporting Results

Authorization and Preparation

Search must not violate any laws or give
rise to liability

Employees
Obtain written authorization

Law Enforcement
Search Warrants

Identification

Determine what devices contain digital
evidence

Determine what data is relevant

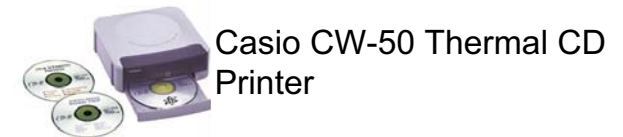
How do we collect and preserve it?

Crime Scene

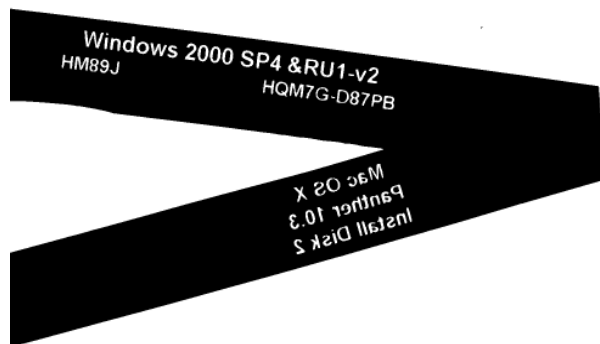


Example: Evidence in Printers

If the printer uses a ribbon, it may
contain clues as to what was printed.



Examining the Ribbon



Next Steps

Collecting
Preserving
Analyzing
Reconstructing

Evidence from a Crime
Where a computer was used

Digging Deep for Clues...

Your Shovel - Helix

Incident
Response

Electronic
Discovery

Computer
Forensics



Helix

www.e-fense.com

700 Meg Download

Auto Runs in Windows

Portable Forensic Workstation

Live System Preview

Many Forensic Tools

Bootable Linux Environment

New Version Available in 2 weeks

Expanded Manual under development

Price: Free!

Helix CD



Main Menu



The Tools

Preview system

Acquire Disk Images

Check for Root Kits

File MD5

File Recovery

Documentation

Photo Search

Only operates at current user level

Incident Response Tools

Windows Forensic Toolchest

Save to Floppy / Network Drive / USB

We will save it to D:\wft

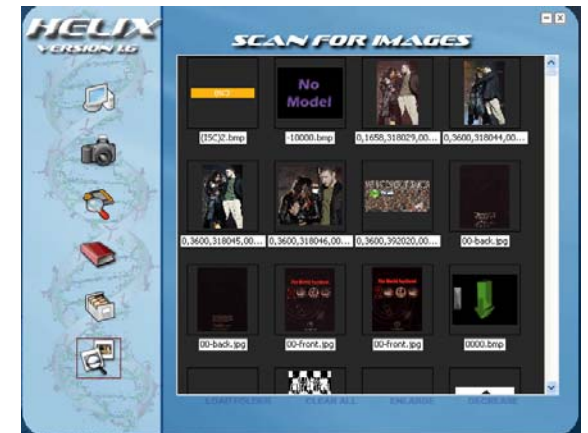
Options: Yes, Yes, Yes

Rootkit: Scan, Save as

D:\wft\txt\rootkit.txt

Open D:\wft\index.html

Photo Search



Problems with previewing a live system

Everything you do modifies the system.

Every time you access a file, you update the access time of the file. Even opening MS office documents, without saving them, modifies their internal content.

Be very careful, or you can contaminate the crime scene.

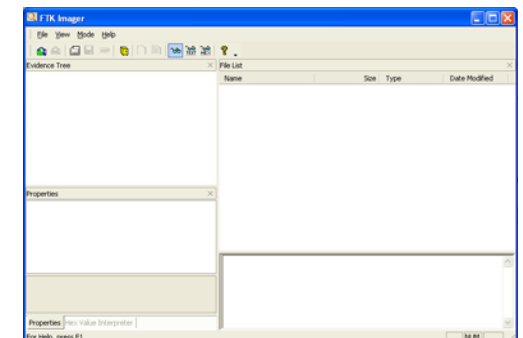
Forensic Demo

Recovering Data from Disks

Examining a Disk - FTK Imager

Page / Acquire / FTK Imager

Start Imager



Let's Start with a blank floppy

Start with clean Floppy

Copy accountinfo.txt to A:

Overwrite it

Delete it

Format it (Quick)

Wipe

This program will do a secure wipe.

3 passes: FF, Random, 00

Page / Incident Response / Misc Tools
Command Shell

```
wipe \\.\a:
```

To use disk again, need to format it.

Disks

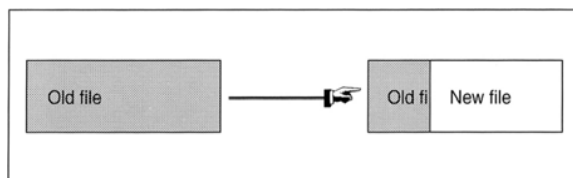
Deleted File only marked
Data Still there

Overwritten files
If smaller, segments can still be there.

Slack Space

A single file occupies a single sector or a single cluster

Slack space can contain left over bits from other files.



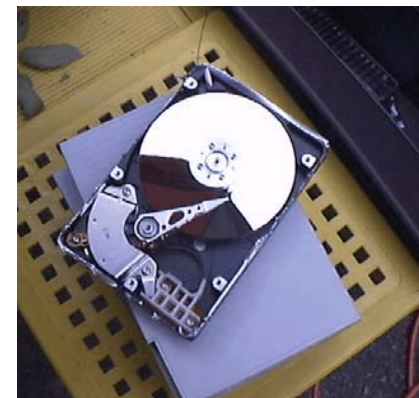
Wiping Drives

With all the problems we had deleting file from the disk, this program will do it for us.

Delete Files
Wipe Free Space, Slack Space, Swap

Wipe Drive - DOS utility Wipe HD
BC Wipe - Windows Utility

Erasing Hard Drives - Step 1



Erasing Hard Drives - Step 2



Case #1

The Blank Disk

Case - Examining a Disk

You have been contacted by the police. They had raided the home of a suspected drug dealer, and as they entered with a no-knock warrant, the dealer grabbed his laptop and fled. They caught him several blocks later, but the laptop was gone. The only thing the police were able to find was a floppy disk in the garbage that appears blank. They have asked you to examine it.

Process

- Write Protect Floppy
- Preview Floppy
- Duplicate Floppy
- Examine with Forensic Tools
- Recover Data
- Reconstruct Evidence
- Explain to the court

Message Digests

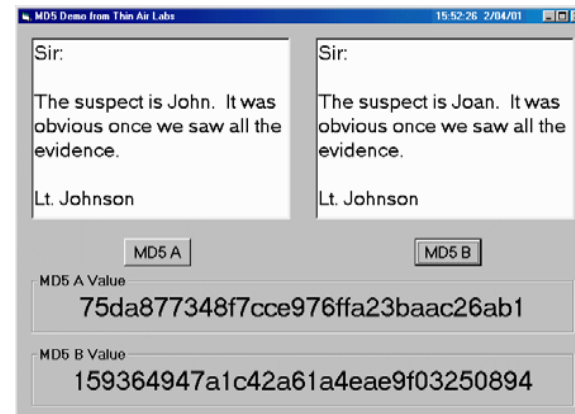
Calculates a checksum for a file

Should be unique

A single character change will alter the checksum

MD5 - generates 32 digit number

MD5 Demo



Reconstruction

Rebuilding deleted, damaged, hidden or encrypted evidence.


- Slack space in files
- Virtual memory files
- Cracking encrypted files

Reconstructing the crime
who, when, where, how, why

Forensic Demo

Cracking Passwords

Try It...

Accent OFFICE Password Recovery 
D:\Class Materials\locked.doc
Step 1: No - Brute Force
Step 2: Next
Step 3: No - Brute Force
Step 4: Next
Step 5: Next
Run

What is the password?
What is the content?



Case #2

Company Porn

Sample Case - Previewing Systems

You are the system administrator for a small company.

Several employees have complained to your boss that Mr. Badguy has pornography on his work computer.

You are asked to check his account.

What to do

Since we can't see anything from the Windows side, let's use the Bootable Helix tool.

This will allow us to bypass Windows Security.

Linux Side



Questions?

End of Presentation