Incident Handling, Forensics and Hacking Techniques

October 2011

Incident Handling & Forensics by SANS

- Matthew J. Harmon, Owner of IT Risk, Ltd., LLC
    - Community Instructor with SANS, Incident Handler, Penetration Tester, Standards Developer within ISO/ITU, IT Auditor, Security Consultant and Researcher, Risk Analyst
        - I love my work!
        - GCIH, GSEC, CISSP, CISA, ISO 27001 Lead Auditor
- SEC 504 "Hacker Techniques, Exploits and Incident Handling"
- SEC 464 "Hacker Detection for Systems Administrators"
    - Quarterly Continuing Education, Human Sensor Network
- SEC 401 "Security Essentials"

Who do we have here today?

- What positions do we have represented in the room today?
  - Incident Handlers? Security Consultants?
  - Law Enforcement? CISO? Board of Directors?
  - Security Manager? Director of IT? IT Auditors?
- What are the biggest challenges in your day-to-day work?

Incident Response Process

Let’s make sure we are all on the same page

Incident Response Strategy

- Most of the time we are called in after an incident/event has begun
- Our first steps must be to identify the existing Incident Response Plan and who is our Incident Coordinator
- No incident response plan? Our first lesson learned.

Core Concepts

- Don't Panic! Remain Calm.
- Take comprehensive notes
  - If you don't have enough time to take notes, you are moving too fast. Slow down. Take a deep breath.
- Get help, immediately. Work in 2x2 pairs.
- Enforce a need-to-know policy
- Use Out-of-Band Communication

Core Concepts (Cont.)

- Contain the incident and prevent more damage
- Make a bit-by-bit backup. Never operate on the original source.
- Eradicate the attacker and their hold
- Get back to business
- Learn from mistakes made

Preparation

- Getting ready to counter an attack
- Establishing Policies, Procedures and getting Management Buy-In
- Establishing network/traffic baselines
  - Gambling? Social Media? Movies? Doing harm?
- Notification guidelines for media
- Internal/external CIRTs / CERT and LEO contacts

Phases

- Preparation – Getting Ready to Respond
- Identification – What is worth investigating?
- Containment – Triage to Stop the Bleeding
- Eradication – Removing the Threat
- Recovery – Back to business as usual
- Lessons Learned – What went wrong?

Identification

- Determining if an event or incident has occurred
  - Event (no correlating logs, minimal impact)
  - Incident (corroborating evidence, potential for harm)
  - Verify system configuration, identify failures
- Declare an incident early so containment can begin
- Begin chain-of-custody - always work in 2x2 pairs
- Notify management and begin CIRT coordination

Containment

- Limit the scope of damage, stop the bleeding
- Back up the system (bit-by-bit copy) to **new** media
- Never operate from original data source
- Determine risk to continued operations
- Keep a low profile, but change passwords on compromised systems and dependent systems

Eradication

- Isolate the attack, determine vectors and exploited vulnerabilities
- Implement protection measures to treat attack vectors; network/firewall filters, rename/re-IP, if system cannot be trusted rebuild on more hardened platform
- Identify additional vulnerabilities
- Locate a clean backup and prepare for recovery

Recovery

- Return system to operational state
- Restore, Validate, and Prevent future attacks
- After management has decided to bring the system back into production...
- Monitor for back doors and other attempted exploits

Lessons Learned

- How to prevent this from happening again?
- What is the root cause of the attack and what can be done to improve operations to limit risk
- Produce a detailed incident report and circulate to appropriate management
- Implement changes as approved by management

Enough with process...

Let's talk about practical application

Tools

- SANS Investigative Forensic Toolkit (SIFT) Workstation
  - http://computer-forensics.sans.org/community/downloads
- BackTrack
  - http://www.backtrack-linux.org
  - Focused on offense not analysis

The SIFT Workstation

- Developed by SANS
- A ton of tools ready to go
  - Supports images acquired with Expert Witness, RAW (dd) and Advanced Forensic Format (AFF)
  - The Sleuth Kit and GUI's for FS / disk analysis
  - log2timeline for timeline generation
  - Pasco for web history examination
  - the Volatility Framework for memory analysis
  - and many more...
- Covered in SEC 408 and SEC 508

Back|Track

- Back|Track by Offensive Computing
  - http://www.backtrack-linux.org
  - Focused on penetration, not analysis
    - Many of the same tools (under Forensics) but not as Incident Handler friendly
- Metasploit, Kismet, Ophcrack, Wireshark, BeEF (Browser Exploit Framework) and many more.
- Covered extensively in SEC 504

Computer Forensics Steps

- What are you investigating?
- Document the Scene
- Identify Data Sources and Locations
- Preserve the Evidence
- Analyze the collected data
- Present findings

Scenarios

- What are you investigating?
- Scenarios
  - Malware
  - Malicious Insider / Espionage
  - Phishing
  - Criminal Investigation

Document the Scene

- Documentation is key
- Before touching anything use your pen and notebook
- Photograph, sketch and label everything
- Take copious notes with date and time
  - These may end up in court

Identify Data Sources

- Forensics are both in-person and remote
- Data sources include servers, workstations, PDA's / smartphones, backups and network devices such as routers and switches...

  ➡ and people!

- Logs are your friend, logs build a timeline and give insight
- Intrusion Detection Systems, Firewalls, Switch ports

Preserving Evidence

- Data Extraction
  - Before pulling the plug
  - After pulling the plug
  - Methods – in-line drive duplication, USB
  - Imaging – DD (unix)
    - EnCase by Guidance Software
    - FTK (Forensic Toolkit) by Access Data
- Backup Data, **NEVER** use original source
- Chain-of-Custody, Checksums, Photographs

Presenting Evidence

- Who is the audience?
- Local law enforcement, FBI, Secret Service
- Corporate “Legal”, HR, Audit, InfoSec
- Making your case, what is your conclusion?

Analyze Collected Data

- Some data will be in log format, timestamped, formatted and easily translated
- Most data will be “hidden” or abstracted
- Process, procedures and tools make this easier
- Understanding how technology works and is integrated into business is key

Hiding Data Intentionally

Not really steganography...

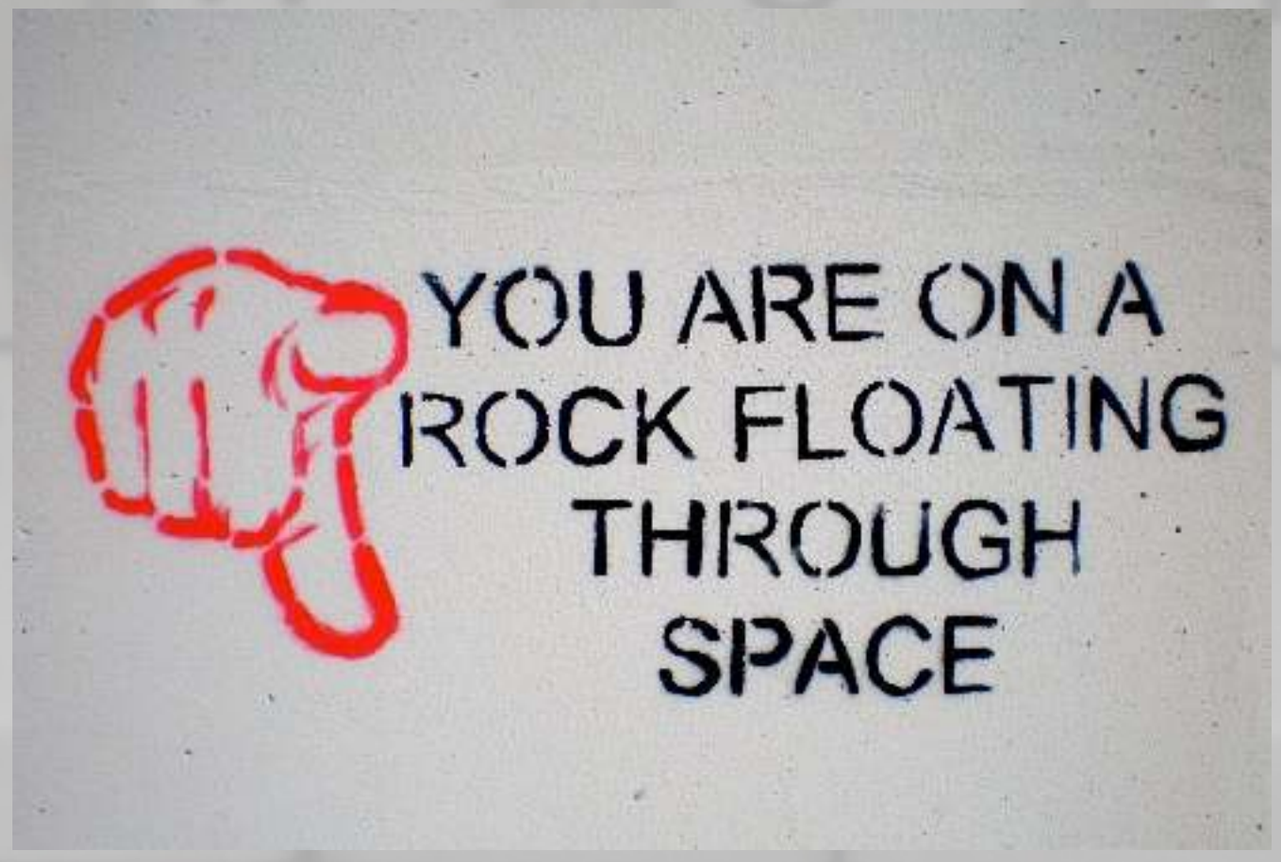
Hiding data intentionally

- Anyone watch CSI?
- You cannot "enhance the pixels"
- But you can store stuff in pictures!

```
mjh@kryptos:~/Pictures$ file rock-floating-demo.jpg
rock-floating-demo.jpg: JPEG image data, JFIF standard 1.01
mjh@kryptos:~/Pictures$ echo "Hello Class" >> hello.txt
mjh@kryptos:~/Pictures$ zip hello.zip hello.txt
  adding: hello.txt (stored 0%)
mjh@kryptos:~/Pictures$ cat hello.txt
Hello Class
mjh@kryptos:~/Pictures$ cat hello.zip >> rock-floating-demo.jpg
mjh@kryptos:~/Pictures$ rm hello.txt hello.zip
mjh@kryptos:~/Pictures$ file rock-floating-demo.jpg
rock-floating-demo.jpg: JPEG image data, JFIF standard 1.01
mjh@kryptos:~/Pictures$ unzip rock-floating-demo.jpg
Archive:  rock-floating-demo.jpg
warning [rock-floating-demo.jpg]:  172836 extra bytes at beginning or within zipfile
  (attempting to process anyway)
 extracting: hello.txt
mjh@kryptos:~/Pictures$ cat hello.txt
Hello Class
mjh@kryptos:~/Pictures$
```

Hiding Data in Images

- This image contains a ZIP file
- This is not steganography



File Formats & Data Structures

- A .zip file in an JPEG? How? Magic numbers.

```
FF D8 FF E0 xx xx 4A 46          ÿØÿà..JF
49 46 00                         IF.
```

JFIF, JPE, JPEG, JPG — JPEG/JFIF graphics file

Trailer: FF D9 (ÿÙ)

rock-floating-demo.jpg - GHex

File Edit View Windows Help

```
00000000 FF D8 FF E0 00 10 4A 46 49 46 00 01 01 00 00 01 00   ......JFIF.......
00000011 01 00 00 FF DB 00 43 00 01 01 01 01 01 01 01 01 01   ......C..........
00000022 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01   .................
```

- File formats are designated by magic numbers
- http://www.garykessler.net/library/file_sigs.html
- File extensions (.jpg, .zip) are for humans only

File Formats & Data Structures

- ZIP at the End

50 4B 03 04

PK..

ZIP PKZIP archive file (Ref. 1 | Ref. 2)

Trailer: *filename* 50 4B *17 characters* 00 00 00

Trailer: (*filename* PK *17 characters . . .*)

rock-floating-demo.jpg - GHex

File Edit View Windows Help

```
0002A2D2 C2 21 52 BD B4 57 C2 2B B3 14 6D E7 C1 04 AA 66 DA   .!R..W.+..m....f.
0002A2E3 64 0B 24 48 EA AE 62 8D 15 99 55 82 B3 E3 2E 41 76   d.$H..b...U....Av
0002A2F4 39 6C 02 A5 C6 0D B7 CB 53 57 7F 76 34 DC 77 5F 0B   9l......SW.v4.w_.
0002A305 95 58 CA DD B9 A2 9E 8A E8 C3 95 3B 36 E7 7D 2F A4   .X.........;6.}/.
0002A316 5E BE ED F5 53 8E BA 3E 8B 5B 76 D3 FF D9 50 4B 03   ^...S..>.[v...PK.
0002A327 04 0A 00 00 00 00 00 A3 71 2F 3D 14 47 27 3F 0C 00   ........q/=.G'?..
0002A338 00 00 0C 00 00 00 09 00 1C 00 68 65 6C 6C 6F 2E 74   ..........hello.t
0002A349 78 74 55 54 09 00 03 C2 1A 91 4C A4 1A 91 4C 75 78   xtUT......L...Lux
0002A35A 0B 00 01 04 E8 03 00 00 04 E8 03 00 00 48 65 6C 6C   .............Hell
0002A36B 6F 20 43 6C 61 73 73 0A 50 4B 01 02 1E 03 0A 00 00   o Class.PK.......
0002A37C 00 00 00 A3 71 2F 3D 14 47 27 3F 0C 00 00 00 0C 00   ....q/=.G'?......
0002A38D 00 00 09 00 18 00 00 00 00 00 00 01 00 00 00 A4 81 00   ..................
0002A39E 00 00 00 68 65 6C 6C 6F 2E 74 78 74 55 54 05 00 03   ...hello.txtUT...
```

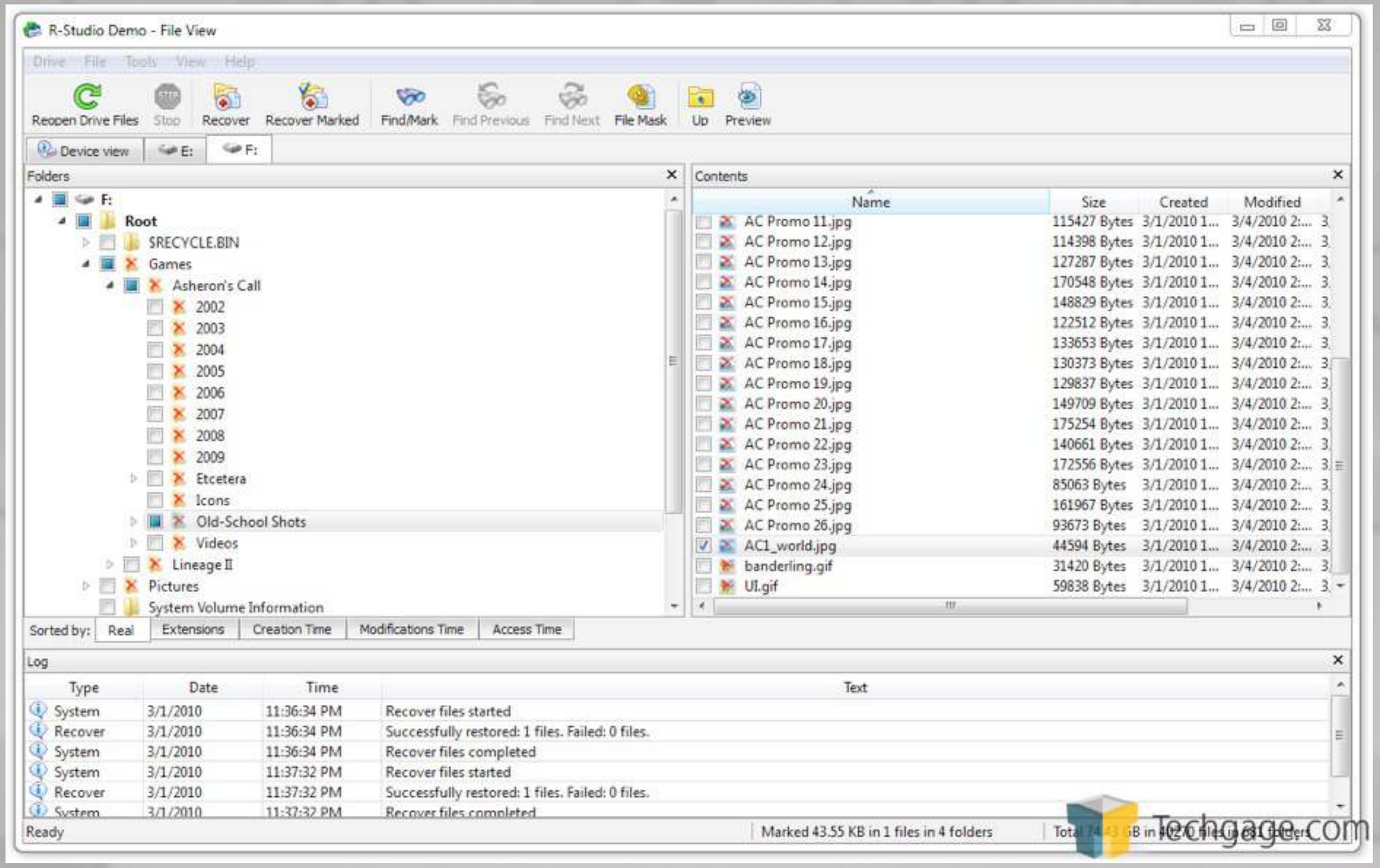
Hiding Data Accidentally

The State of Solid State Drives

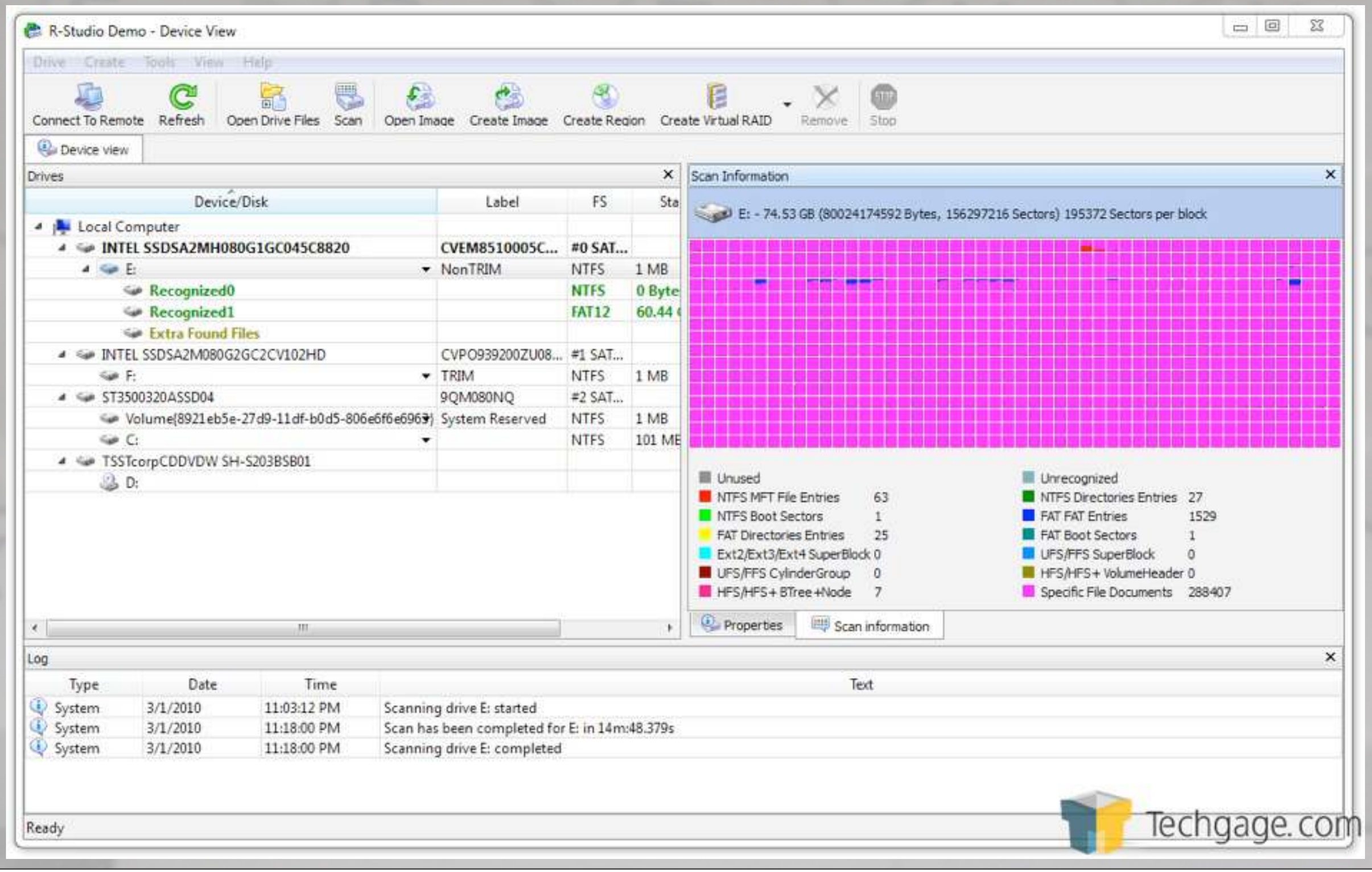
Solid State Drives

- SSD (Solid State Drives) bring new questions to forensic activities
- New models of SSD come with the TRIM function
- Windows 7, Windows Server 2008, Linux kernel 2.6.33 are TRIM compatible
- TRIM does “garbage collection” essentially defeating forensic activities by zeroing data and complicating drive wiping

SSD w/o TRIM


R-Studio Demo - File View
Drive File Tools View Help
Reopen Drive Files
Stop
Recover
Recover Marked
Find/Mark
Find Previous
Find Next
File Mask
Up
Preview
Device view
E:
F:
Folders
F:
Root
$RECYCLE.BIN
Games
Asheron's Call
2002
2003
2004
2005
2006
2007
2008
2009
Etcetera
Icons
Old-School Shots
Videos
Lineage II
Pictures
System Volume Information
Contents
Name
Size
Created
Modified
AC Promo 11.jpg 115427 Bytes 3/1/2010 1... 3/4/2010 2:...
AC Promo 12.jpg 114398 Bytes 3/1/2010 1... 3/4/2010 2:...
AC Promo 13.jpg 127287 Bytes 3/1/2010 1... 3/4/2010 2:...
AC Promo 14.jpg 170548 Bytes 3/1/2010 1... 3/4/2010 2:...
AC Promo 15.jpg 148829 Bytes 3/1/2010 1... 3/4/2010 2:...
AC Promo 16.jpg 122512 Bytes 3/1/2010 1... 3/4/2010 2:...
AC Promo 17.jpg 133653 Bytes 3/1/2010 1... 3/4/2010 2:...
AC Promo 18.jpg 130373 Bytes 3/1/2010 1... 3/4/2010 2:...
AC Promo 19.jpg 129837 Bytes 3/1/2010 1... 3/4/2010 2:...
AC Promo 20.jpg 149709 Bytes 3/1/2010 1... 3/4/2010 2:...
AC Promo 21.jpg 175254 Bytes 3/1/2010 1... 3/4/2010 2:...
AC Promo 22.jpg 140661 Bytes 3/1/2010 1... 3/4/2010 2:...
AC Promo 23.jpg 172556 Bytes 3/1/2010 1... 3/4/2010 2:...
AC Promo 24.jpg 85063 Bytes 3/1/2010 1... 3/4/2010 2:...
AC Promo 25.jpg 161967 Bytes 3/1/2010 1... 3/4/2010 2:...
AC Promo 26.jpg 93673 Bytes 3/1/2010 1... 3/4/2010 2:...
AC1_world.jpg 44594 Bytes 3/1/2010 1... 3/4/2010 2:...
banderling.gif 31420 Bytes 3/1/2010 1... 3/4/2010 2:...
UI.gif 59838 Bytes 3/1/2010 1... 3/4/2010 2:...
Sorted by: Real Extensions Creation Time Modifications Time Access Time
Log
Type Date Time Text
System 3/1/2010 11:36:34 PM Recover files started
Recover 3/1/2010 11:36:34 PM Successfully restored: 1 files. Failed: 0 files.
System 3/1/2010 11:36:34 PM Recover files completed
System 3/1/2010 11:37:32 PM Recover files started
Recover 3/1/2010 11:37:32 PM Successfully restored: 1 files. Failed: 0 files.
System 3/1/2010 11:37:32 PM Recover files completed
Ready
Marked 43.55 KB in 1 files in 4 folders
Techgage.com

SSD with TRIM



Like what you've seen today?

- Sign up for **SEC 504**, Hacker Techniques, Exploits and Incident handing, taught locally starting January 18th, 2012 with Matthew J. Harmon over 10 weeks
  - http://www.sans.org/mentor/details.php?nid=26769 or http://tinyurl.com/SEC504MplsJan2012
- Sign up for **SEC 464,** Hacker Detection for Systems Administrators, taught at your convenience over 2 days
- or **SEC 401**, Security Essentials starting January 26th, 2012 with Eric Lucero over 10 weeks
  - http://www.sans.org/mentor/details.php?nid=26649

Matthew J. Harmon

+1 612/987.0115 - matthew@itriskltd.com

IT Risk, Ltd., LLC - http://www.itriskltd.com

The SANS Institute

http://www.sans.org - http://computer-forensics.sans.org/

http://pen-testing.sans.org