Anti-Forensics

Considering a career in Computer Forensics?

Don’t quit your day job……

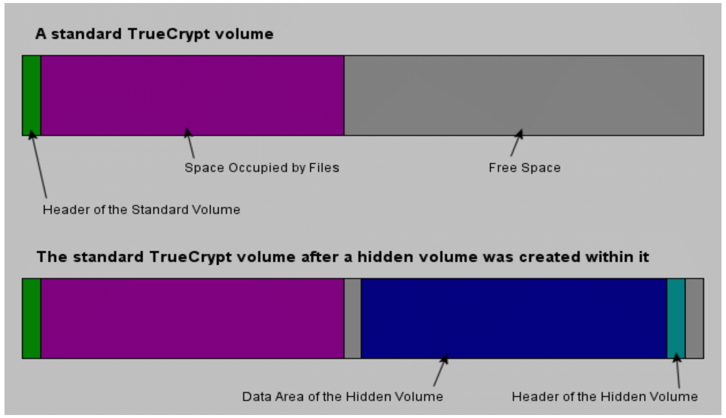
Paul A. Henry
***MCP+I, MCSE, CFSA, CFSO, CCSA, CCSE, CISM, CISA, CISSP, ISSAP* , CIFI**
Vice President
Secure Computing

What We Will Cover

- **Encryption**
  - Plausible Deniability
  - Windows Vista
- **Steganography - Use and Detection**
- **Hiding Collections of Pictures**
- **Disk Wiping – The Tools Are Getting Scarily Good**
- **What Good are Known Good/Bad Signatures**
- **MetaSploit**
  - Slacker – Hide tons of data encrypted in slack
  - Timestomp – So much for MAC
  - Transmorgify – One Click Defense
  - Samjuicer – No More DLL Injection
- **Advanced Anti-Forensics – Everything Happens in RAM**
- **Linux Anti-Forensics – Hide Where The Tools Don't Look**

Encryption

- **Encryption is a forensic analysis's nightmare**
  - A handful of advances – PRTK,EFS Tools, Rainbow Tables etc
  - It is only a matter of time before the bad guys adopt current technology encryption
  - Current offerings provide for multiple levels of "Plausible Deniability"
    - Create a hidden encrypted volume within an encrypted volume
      - Bad guy gives up the password to the first level only
      - Second level remains hidden and looks like random data within the volume (undetectable)


A standard TrueCrypt volume
Space Occupied by Files
Free Space
Header of the Standard Volume
The standard TrueCrypt volume after a hidden volume was created within it
Data Area of the Hidden Volume
Header of the Hidden Volume

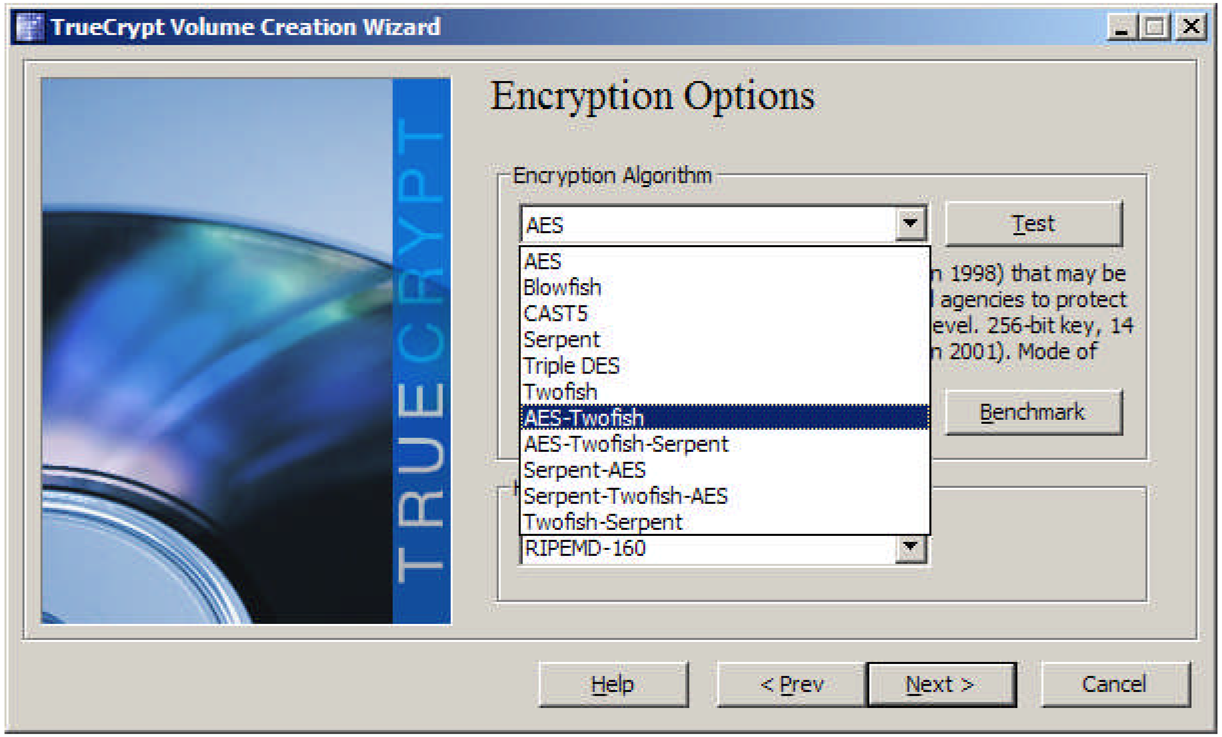
TrueCrypt Is Also Stealthy

- **Settings are not stored in the registry**
- **Uses a “key file” rather then a crypto key**
  - Which of the thousands of files on the image did the bad guy use as the key file?
- **Improvements to plausible deniability**
  - Uses LRW to replace CRW eliminating any possible detection of non random data within an image
- **Creates a virtual encrypted disk within a file and mounts it as a disk**

Gaining In Popularity

Total Number of Downloads 657,121

Average Downloads per Day 1,135



TrueCrypt Volume Creation Wizard

Encryption Options

Encryption Algorithm

AES

AES
Blowfish
CAST5
Serpent
Triple DES
Twofish
AES-Twofish
AES-Twofish-Serpent
Serpent-AES
Serpent-Twofish-AES
Twofish-Serpent

n 1998) that may be
l agencies to protect
evel. 256-bit key, 14
n 2001). Mode of

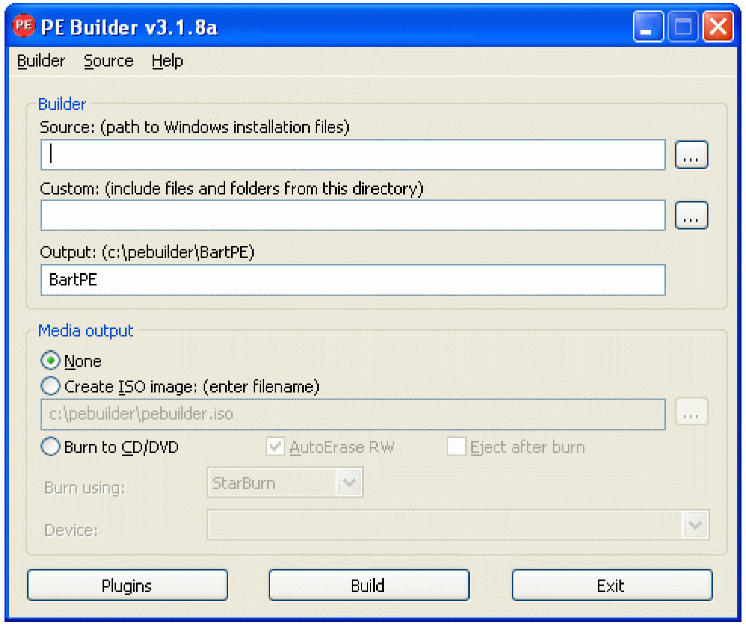
RIPEMD-160

SECURE® COMPUTING

“Traveler” mode with BartPE

With Out A Trace

- **Create an XP bootable CD**
- **Boot from the CD and create an encrypted environment on the HD**
- **No trace on the PC**



Builder

Source: (path to Windows installation files)

Custom: (include files and folders from this directory)

Output: (c:\pebuilder\BartPE)

BartPE

Media output

● None

○ Create ISO image: (enter filename)

c:\pebuilder\pebuilder.iso

○ Burn to CD/DVD ☑ AutoErase RW □ Eject after burn

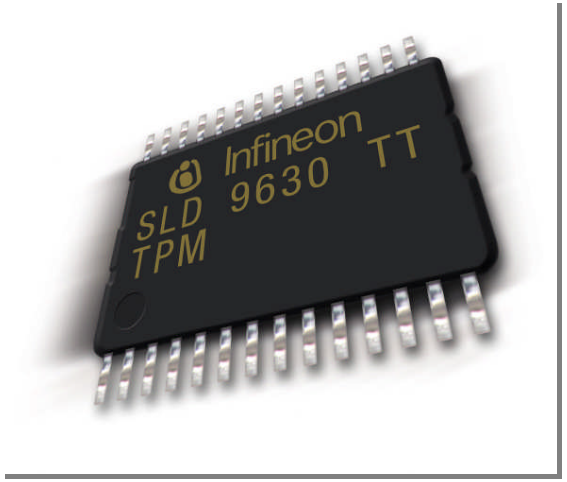
Burn using: StarBurn

Device:

Trusted Platform Module

TPM Chip Version 1.2

- **Hardware present in the computer, e.g. a chip on the motherboard**
- **Securely stores credentials, such as a private key of a machine certificate and is crypto-enabled**
  - Effectively, the essence of a smart smartcard
- **TPM can be used to request digital signing of code and files and for mutual authentication of devices**
- **See www.trustedcomputinggroup.org**

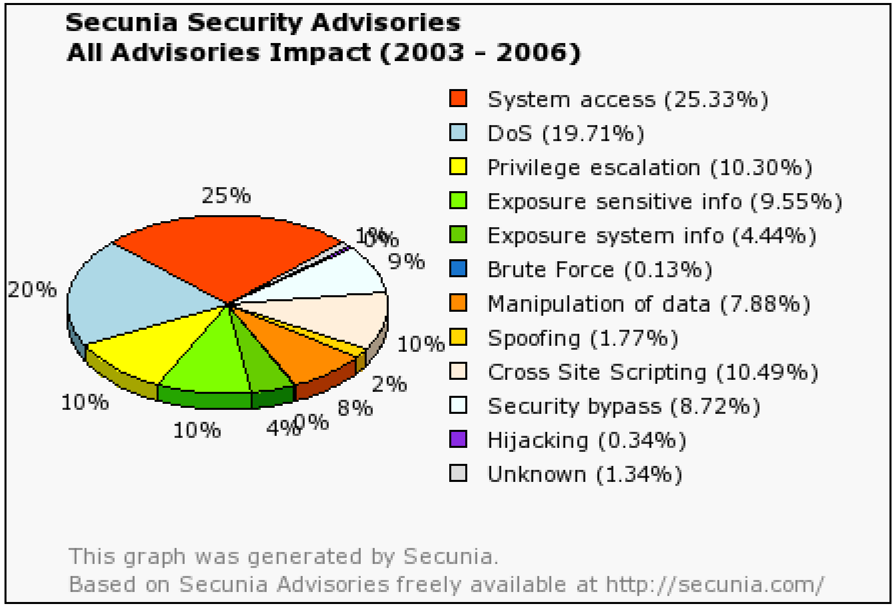


Full Volume Encryption

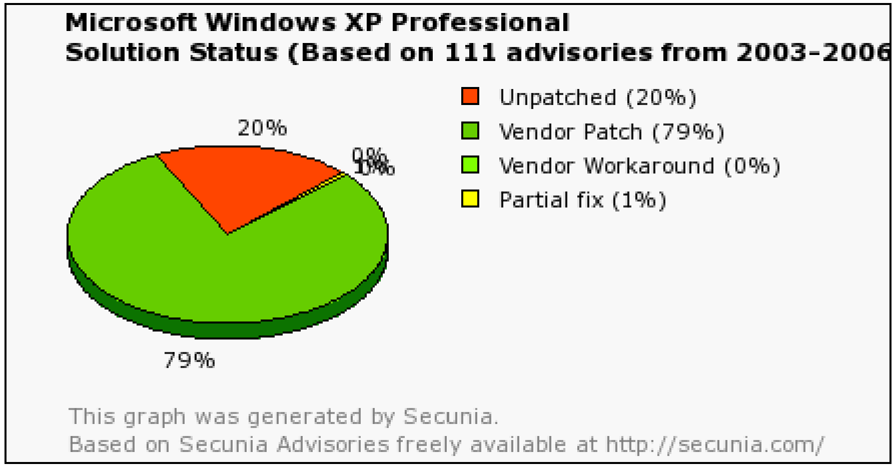
Bitlocker™ FVE

- **FVE strongly encrypts and signs the entire hard drive**
  - TPM chip provides key management
  - Can use additional protection factors such as a USB dongle, PIN or password
- **Any unauthorised off-line modification to your data or OS is discovered and no access is granted**
  - Prevents attacks which use utilities that access the hard drive while Windows is not running and enforces Windows boot process
- **Protection against data loss when machine (laptop) has been stolen**
- **Essential part of the Secure Startup**
  - Plan data recovery strategy carefully!
- **UK Backdoor Fun**

No Backdoor Effort Needed from MS



This graph was generated by Secunia.
Based on Secunia Advisories freely available at http://secunia.com/



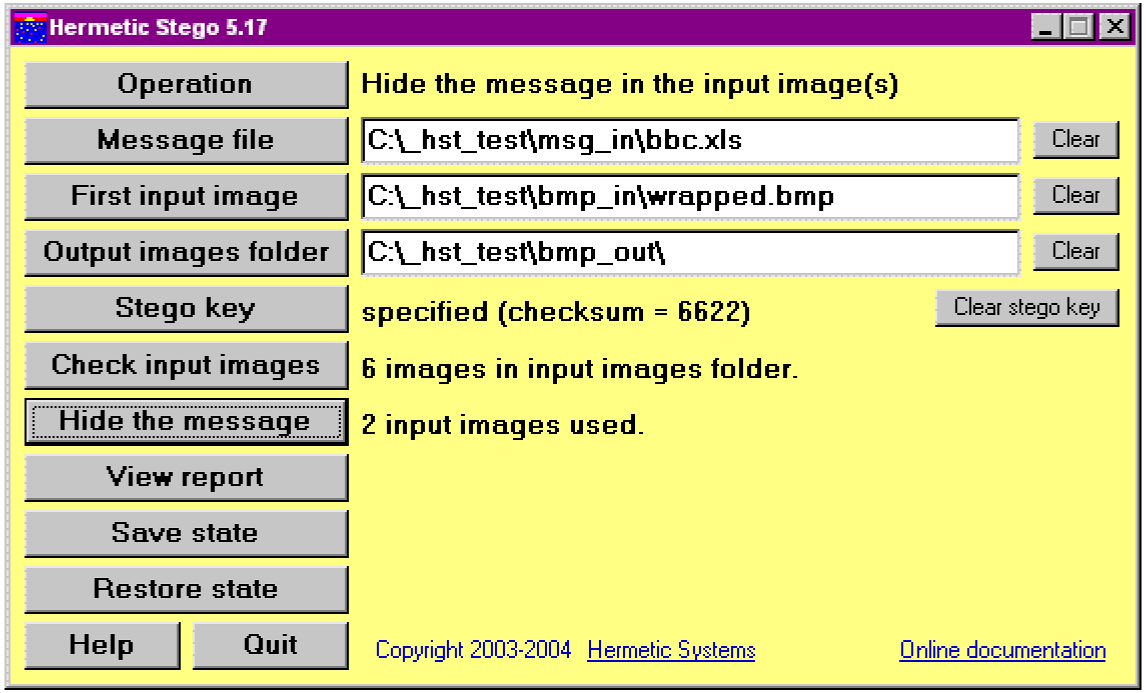
This graph was generated by Secunia.
Based on Secunia Advisories freely available at http://secunia.com/

Free On The Fly Encryption

- **FreOTFE**
- **TrueCrypt**
- **Cryptainer LE**
- **CryptoExpert 2004 Lite**
- **CompuSec**
- **E4M Disk Encryption**
- **Scramdisk Encryption**

Steganography

- Hiding data in graphic or audio files



Hermetic Stego 5.17

Operation Hide the message in the input image(s)

Message file C:_hst_test\msg_in\bbc.xls

First input image C:_hst_test\bmp_in\wrapped.bmp

Output images folder C:_hst_test\bmp_out\

Stego key specified (checksum = 6622)

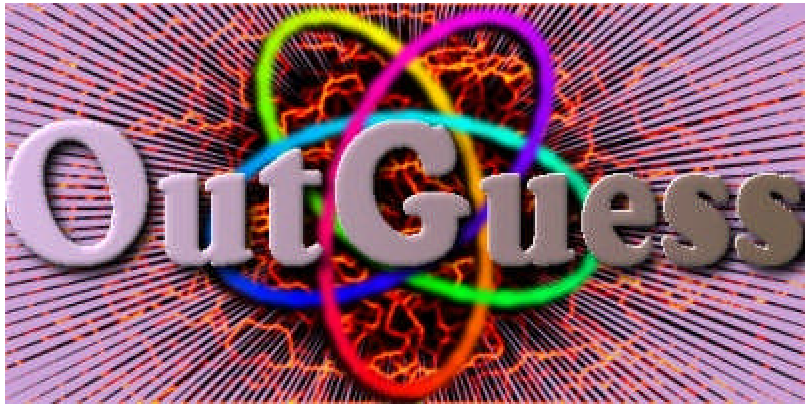
Check input images 6 images in input images folder.

Hide the message 2 input images used.

Copyright 2003-2004 Hermetic Systems

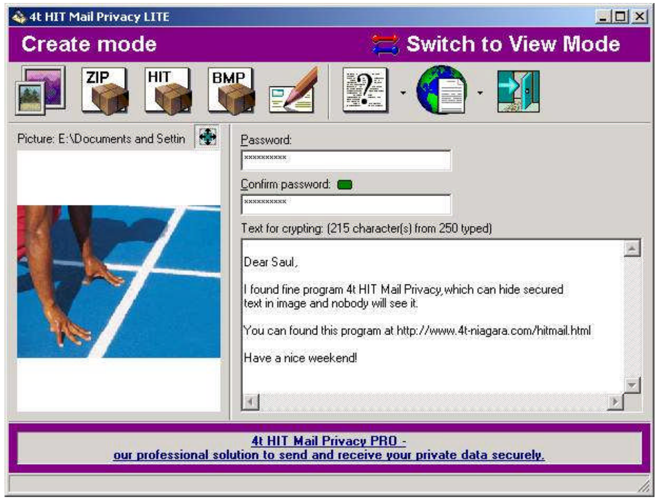
OutGuess

- **Preserves statistics based on frequency counts**
  - Statistical tests based on frequency counts are unable to detect data within an image



Free Steganography

- S-Tools
- 4t HIT Mail Privacy Lite
- Camouflage



Picture: E:\Documents and Settin

Password: xxxxxxxxxx

Confirm password: xxxxxxxxxx

Text for crypting: (215 character(s) from 250 typed)

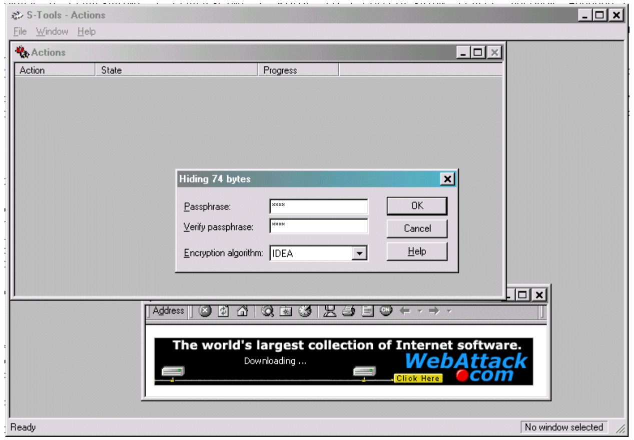
Dear Saul,

I found fine program 4t HIT Mail Privacy,which can hide secured text in image and nobody will see it.

You can found this program at http://www.4t-niagara.com/hitmail.html

Have a nice weekend!

4t HIT Mail Privacy PRO - our professional solution to send and receive your private data securely.



Action	State	Progress

Hiding 74 bytes

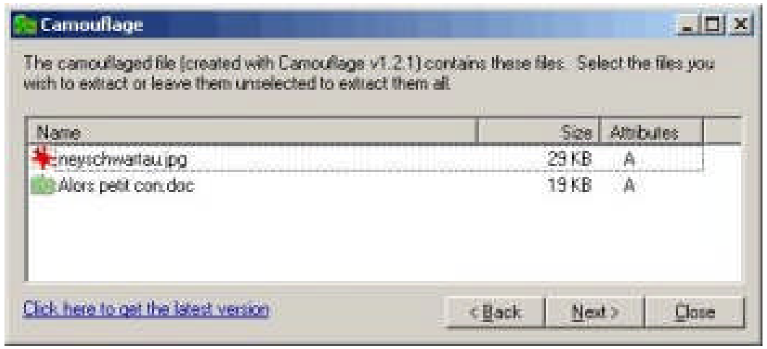
Passphrase: ****

Verify passphrase: ****

Encryption algorithm: IDEA

Ready

No window selected

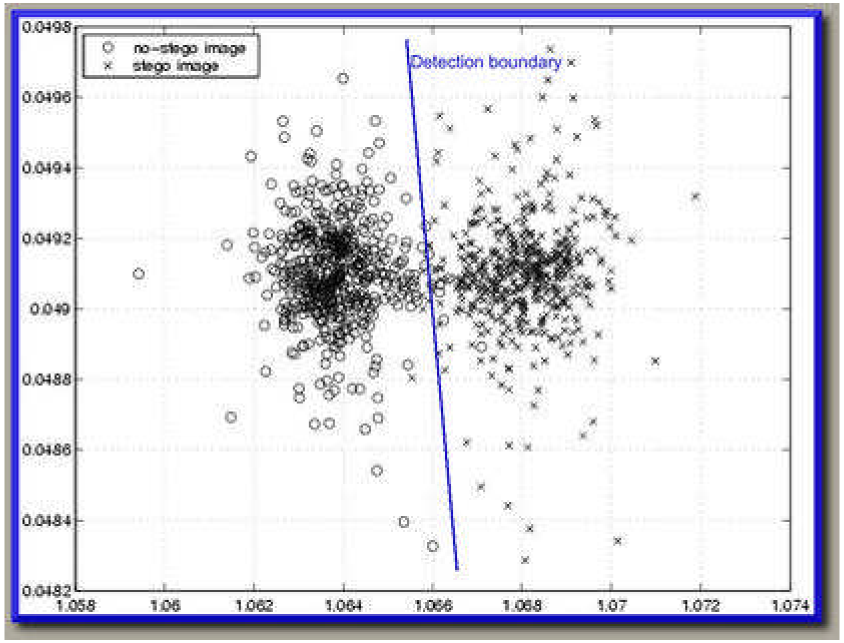


The camouflaged file (created with Camouflage v1.2.1) contains these files. Select the files you wish to extract or leave them unselected to extract them all.

Name	Size	Attributes
neyschwattau.jpg	29 KB	A
Alors petit con.doc	19 KB	A

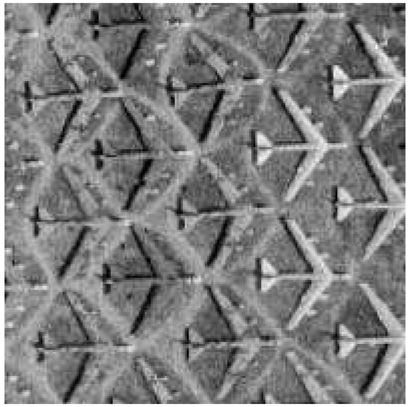
Stegdetect

- **Automated detection of data within an image**
- **Works against:**
  - Jsteg
  - Jphide
  - Invisible secrets
  - Outguess
  - F5
  - appendixX and Comouflage

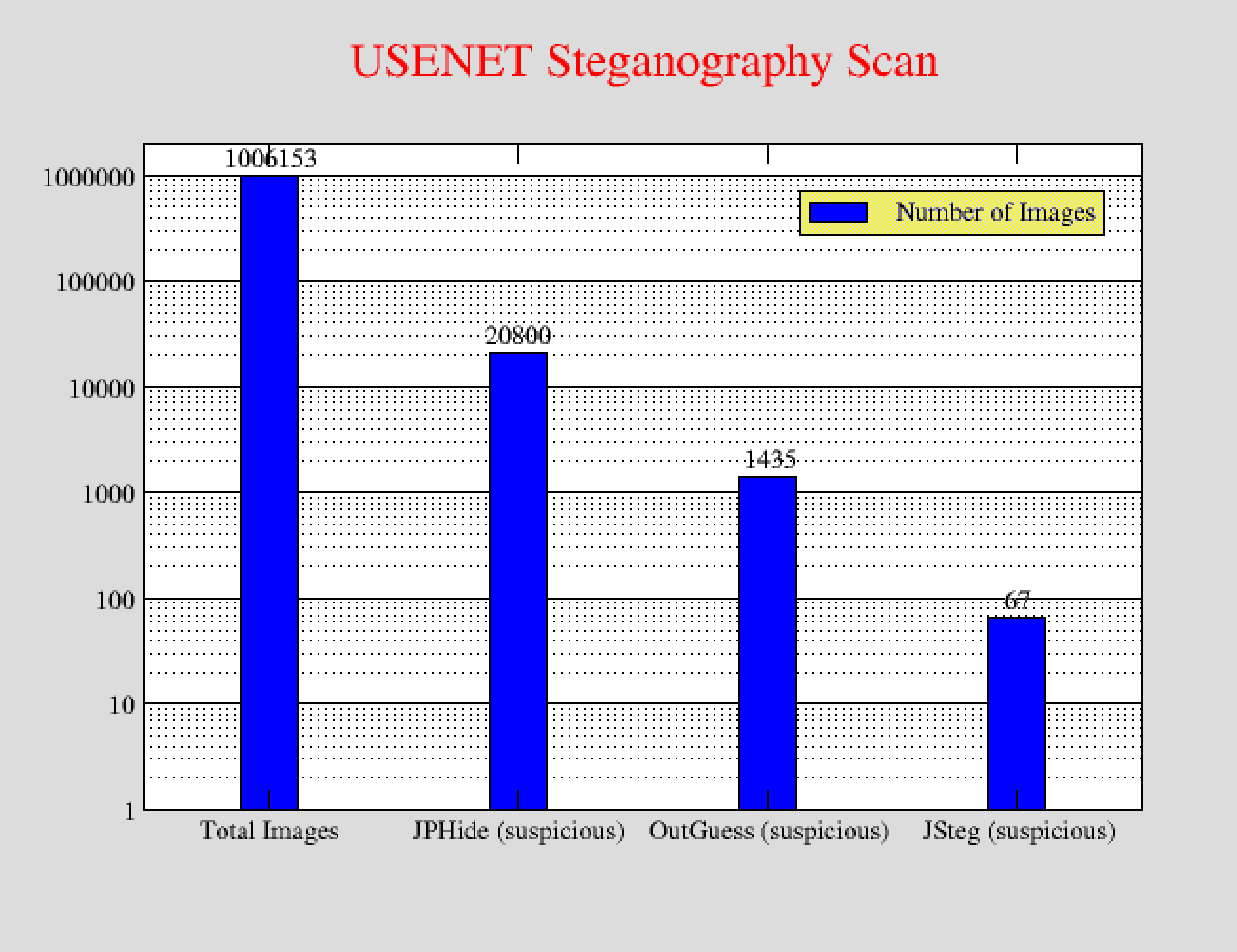


Media Hype - ABC

```
$ stegdetect sovereigntime.jpg sovereigntime.jpg :
jsteg(***) $ stegbreak -tj -f wordlist sovereigntime.jpg
Loaded 1 files... sovereigntime.jpg : jsteg(abc) Processed 1
files, found 1 embeddings. Time: 1 seconds: Cracks: 1156,
1156.0 c/s
```



Perspective

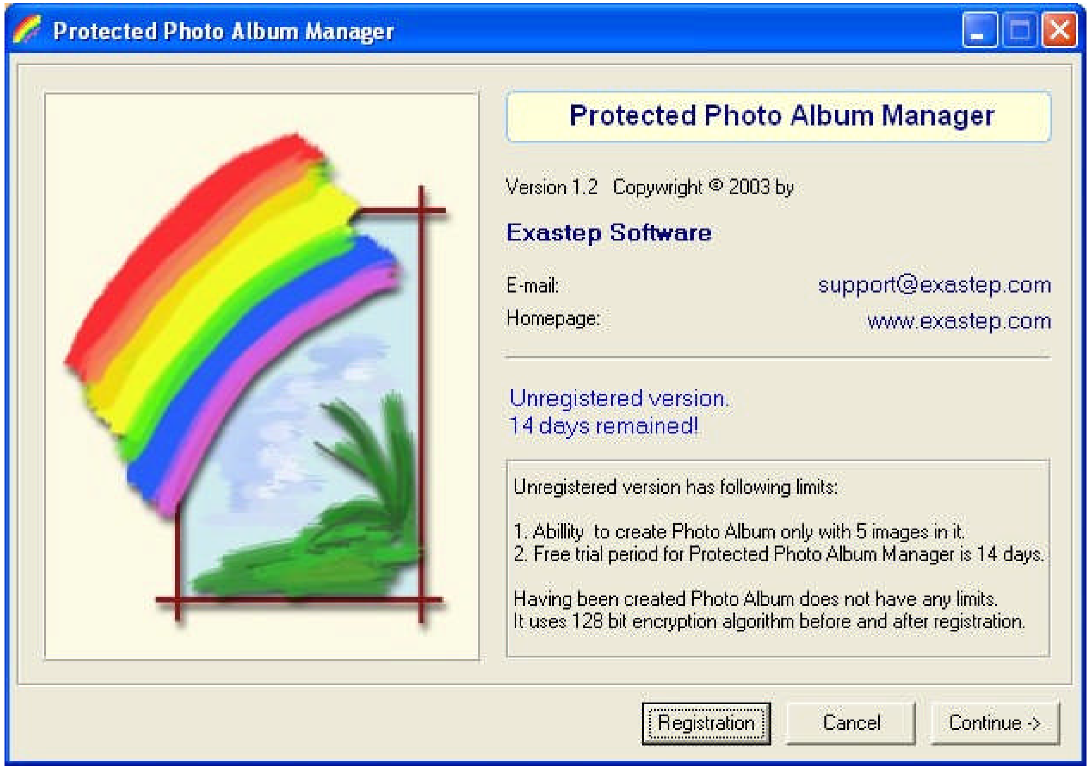


Reality on USENET

- **Processing the one million images with stegdetect results in about 20,000 suspicious images.**
- **They launched a dictionary attack on the JSteg and JPHide positive images.**
  - The dictionary has a size of 1,800,000 words and phrases. The disconcert cluster used to distribute the dictionary attack has a peak performance of roughly 87 GFLOPS.
- ***However, they have not found a single hidden message.***

Old Trick – New Twist

- **Instead of hiding a malicious exe within a picture how about hiding pictures within an encrypted exe**



Protected Photo Album Manager

Version 1.2   Copywright © 2003 by

Exastep Software

E-mail: support@exastep.com

Homepage: www.exastep.com

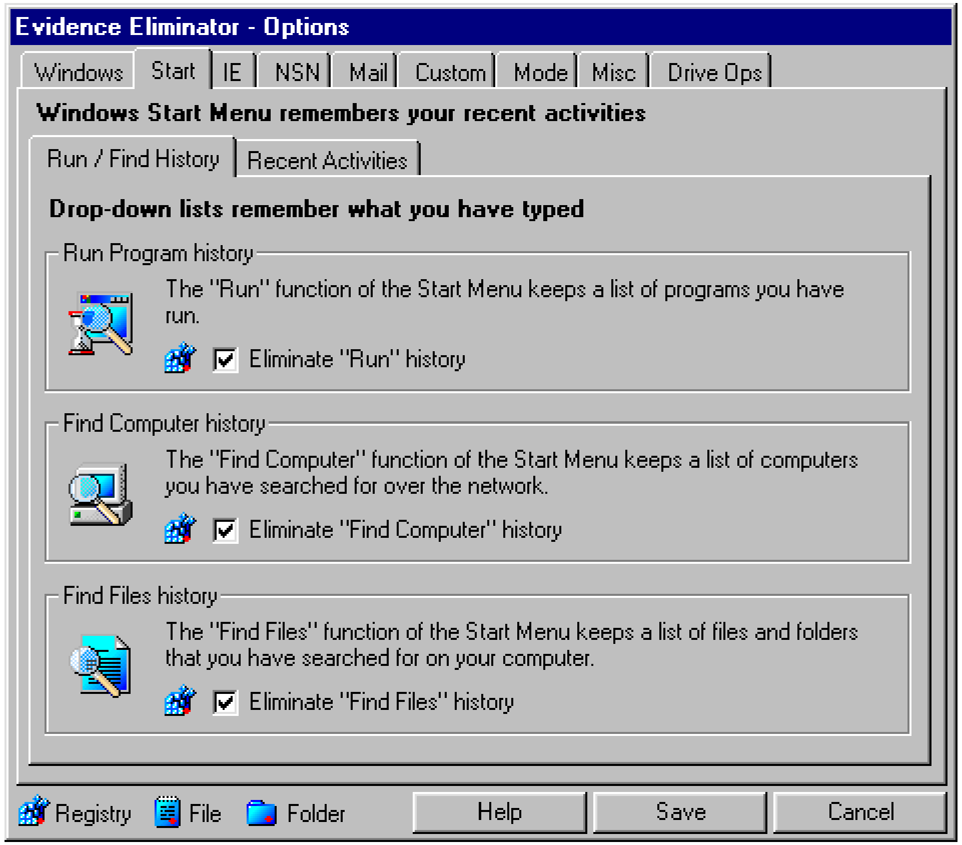
Unregistered version.
14 days remained!

Unregistered version has following limits:

1. Abillity to create Photo Album only with 5 images in it.
2. Free trial period for Protected Photo Album Manager is 14 days.

Having been created Photo Album does not have any limits.
It uses 128 bit encryption algorithm before and after registration.

Evidence Eliminator



Evidence Eliminator - Options

Windows Start Menu remembers your recent activities

Drop-down lists remember what you have typed

Run Program history

The "Run" function of the Start Menu keeps a list of programs you have run.

☑ Eliminate "Run" history

Find Computer history

The "Find Computer" function of the Start Menu keeps a list of computers you have searched for over the network.

☑ Eliminate "Find Computer" history

Find Files history

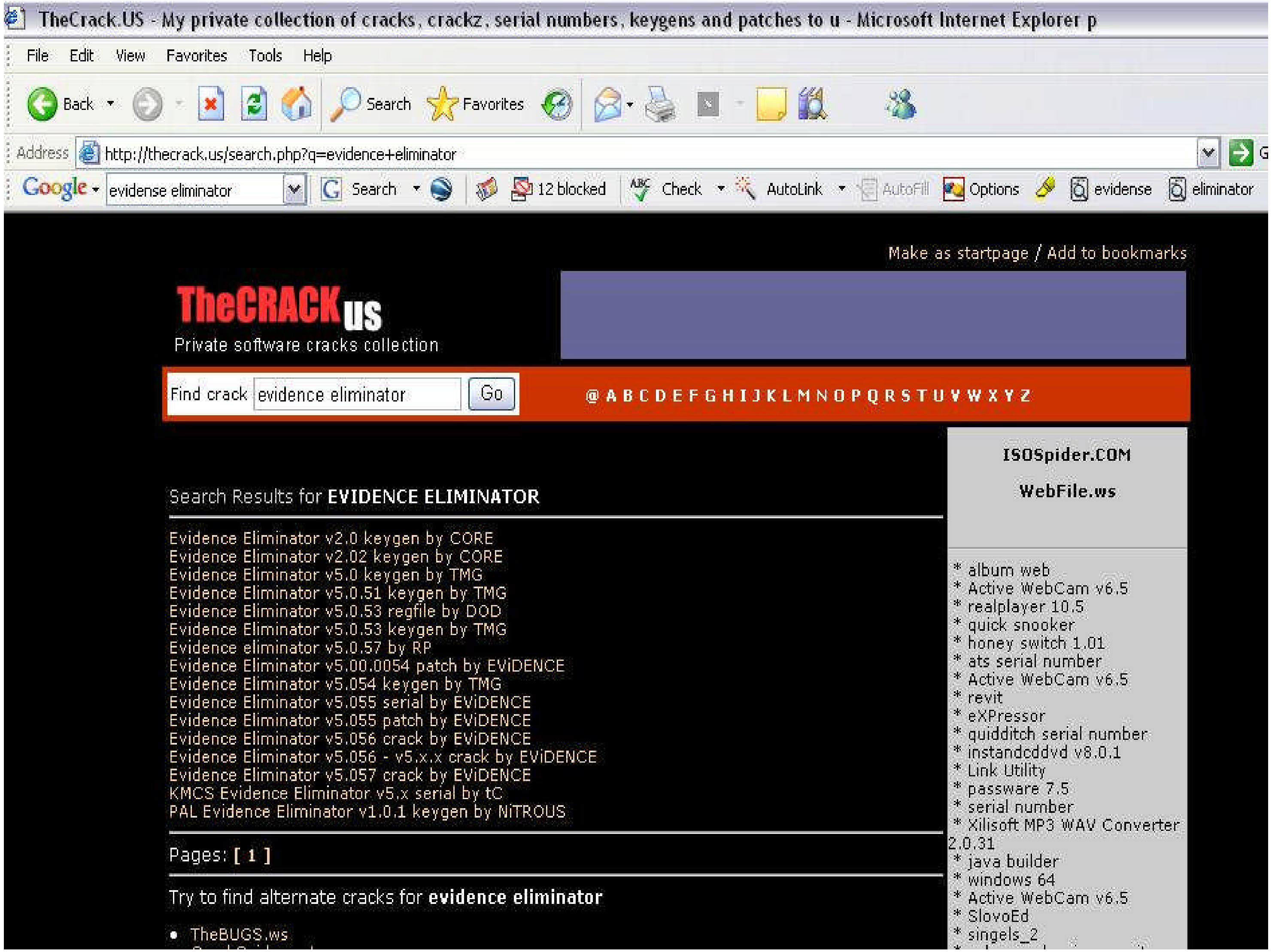
The "Find Files" function of the Start Menu keeps a list of files and folders that you have searched for on your computer.

☑ Eliminate "Find Files" history

Evidence Eliminator

- Windows SWAP file
- Windows Application logs
- Windows Temporary Files
- Windows Recycle Bin
- Windows Registry Backups
- Windows Clipboard Data
- Start Menu Recent Documents history
- Start Menu Run history
- Start Menu Find Files History
- Start Menu Find Computer History
- Start Menu Order Data
- Start Menu Click History
- Microsoft Internet Explorer temporary typed URLs, index files, cache and history
- Microsoft Internet Explorer AutoComplete memory of form posts and passwords
- Microsoft Internet Explorer Cookies (Selective cookie keeping for versions 5 and above)
- Microsoft Internet Explorer Internet components (Selective keeping of components)
- Microsoft Internet Explorer Download Folder memory
- Microsoft Internet Explorer Favorites List
- Microsoft Outlook Express v5+ database of (Selective keeping of mail and news groups)
- Windows Media Player History
- Windows Media Player PlayLists in Media Library
- America OnLine Instant Messenger contacts
- Netscape Navigator temporary typed URLs, files, cache and history.
- Netscape Navigator Cookies (Selective cookie keeping for versions 4 and above)
- Netscape Mail v4+ sent and deleted e-mails
- Netscape Mail hidden files
- Customizable lists of files and folders, with or without their contents
- Customizable scan lists of file types in specific folders
- Customizable scan lists of file types on all drives
- Deleted filenames, sizes and attributes from drive directory structures
- Free cluster space ("Slack") from all file tips
- Magnetic remenance from underneath existing files/folders
- All free unallocated space on all hard drives
- Evidence of activity in many other programs, using Plug-In modules
- Slack space and deleted entries in the Windows registry
- Created and modified dates and times on all files and folders
- Windows Registry Streams
- Common Dialog load/save location history
- Instant secure deletes of Windows registry data (NT4/2000/XP)

The Bad Guys Won’t Pay For It


TheCrack.US - My private collection of cracks, crackz, serial numbers, keygens and patches to u - Microsoft Internet Explorer p
File Edit View Favorites Tools Help
Back
Search
Favorites
Address http://thecrack.us/search.php?q=evidence+eliminator
Google evidense eliminator
Search
12 blocked
Check
AutoLink
AutoFill
Options
evidense
eliminator

Make as startpage / Add to bookmarks

TheCRACK US
Private software cracks collection

Find crack evidence eliminator Go

@ A B C D E F G H I J K L M N O P Q R S T U V W X Y Z

Search Results for **EVIDENCE ELIMINATOR**

Evidence Eliminator v2.0 keygen by CORE
Evidence Eliminator v2.02 keygen by CORE
Evidence Eliminator v5.0 keygen by TMG
Evidence Eliminator v5.0.51 keygen by TMG
Evidence Eliminator v5.0.53 regfile by DOD
Evidence Eliminator v5.0.53 keygen by TMG
Evidence eliminator v5.0.57 by RP
Evidence Eliminator v5.00.0054 patch by EViDENCE
Evidence Eliminator v5.054 keygen by TMG
Evidence Eliminator v5.055 serial by EViDENCE
Evidence Eliminator v5.055 patch by EViDENCE
Evidence Eliminator v5.056 crack by EViDENCE
Evidence Eliminator v5.056 - v5.x.x crack by EViDENCE
Evidence Eliminator v5.057 crack by EViDENCE
KMCS Evidence Eliminator v5.x serial by tC
PAL Evidence Eliminator v1.0.1 keygen by NiTROUS

Pages: [1]

Try to find alternate cracks for **evidence eliminator**

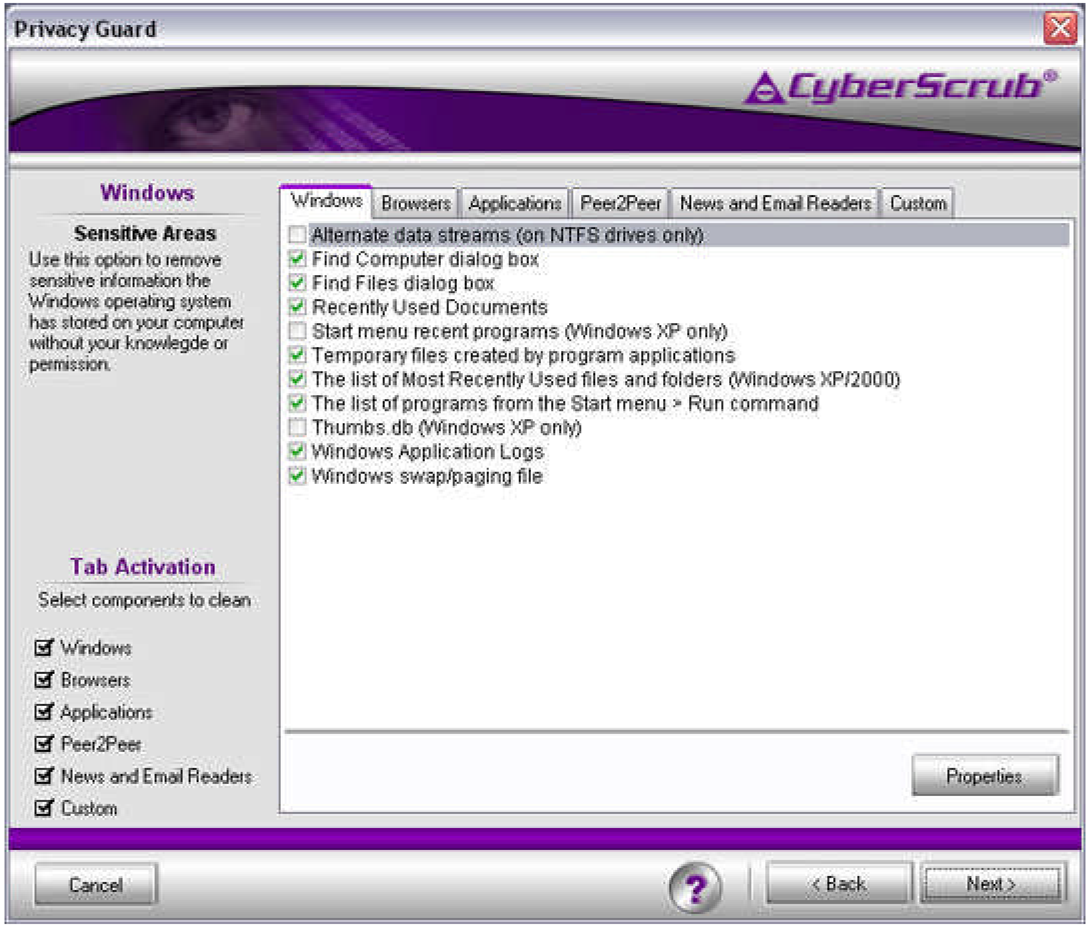
- TheBUGS.ws

ISOSpider.COM

WebFile.ws

* album web
* Active WebCam v6.5
* realplayer 10.5
* quick snooker
* honey switch 1.01
* ats serial number
* Active WebCam v6.5
* revit
* eXPressor
* quidditch serial number
* instandcddvd v8.0.1
* Link Utility
* passware 7.5
* serial number
* Xilisoft MP3 WAV Converter 2.0.31
* java builder
* windows 64
* Active WebCam v6.5
* SlovoEd
* singels_2

Disk Wiping



Windows

Sensitive Areas

Use this option to remove sensitive information the Windows operating system has stored on your computer without your knowlegde or permission.

□ Alternate data streams (on NTFS drives only)
☑ Find Computer dialog box
☑ Find Files dialog box
☑ Recently Used Documents
□ Start menu recent programs (Windows XP only)
☑ Temporary files created by program applications
☑ The list of Most Recently Used files and folders (Windows XP/2000)
☑ The list of programs from the Start menu > Run command
□ Thumbs.db (Windows XP only)
☑ Windows Application Logs
☑ Windows swap/paging file

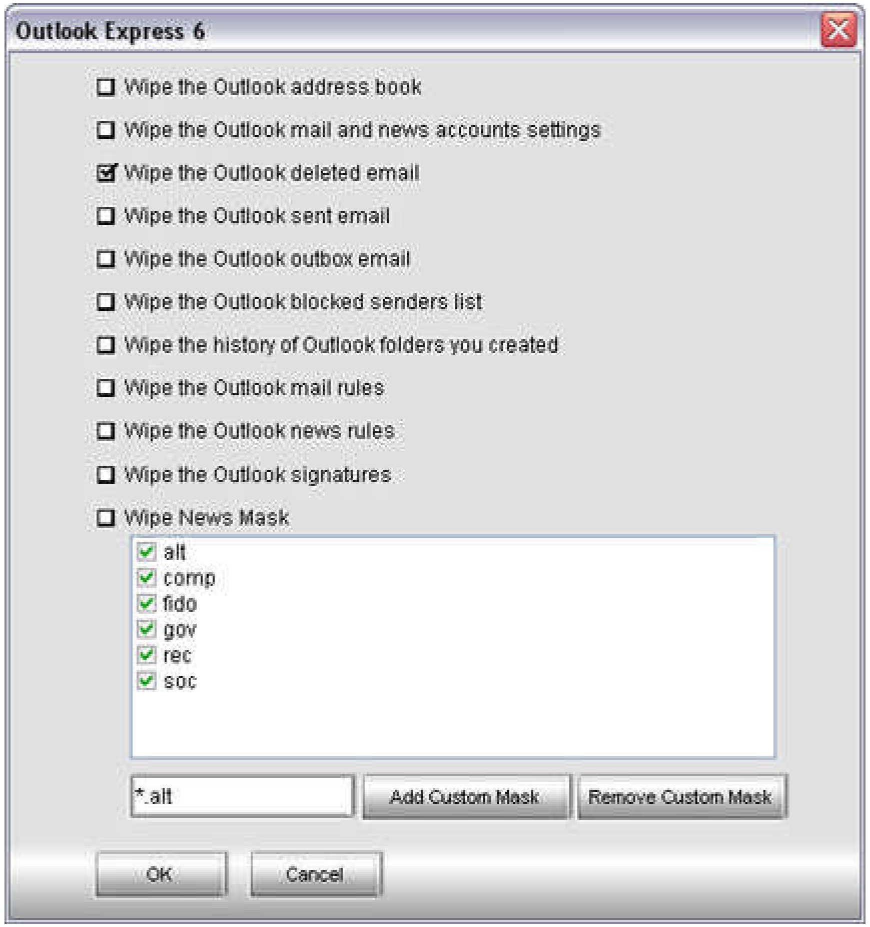
Tab Activation

Select components to clean

☑ Windows
☑ Browsers
☑ Applications
☑ Peer2Peer
☑ News and Email Readers
☑ Custom

SECURE® COMPUTING

Wipes Deeper Then Ever

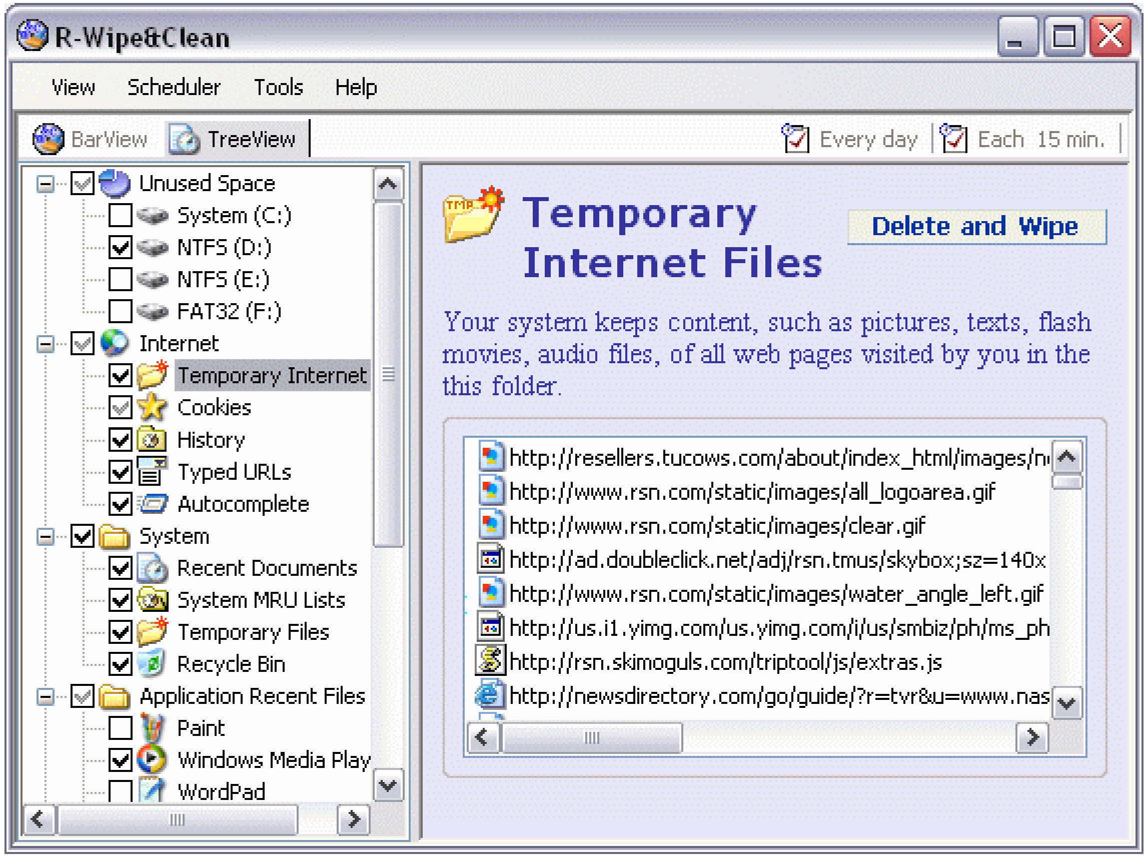


Outlook Express 6

- ☐ Wipe the Outlook address book
- ☐ Wipe the Outlook mail and news accounts settings
- ☑ Wipe the Outlook deleted email
- ☐ Wipe the Outlook sent email
- ☐ Wipe the Outlook outbox email
- ☐ Wipe the Outlook blocked senders list
- ☐ Wipe the history of Outlook folders you created
- ☐ Wipe the Outlook mail rules
- ☐ Wipe the Outlook news rules
- ☐ Wipe the Outlook signatures
- ☐ Wipe News Mask
  - ☑ alt
  - ☑ comp
  - ☑ fido
  - ☑ gov
  - ☑ rec
  - ☑ soc

*.alt

Defeat Forensics For Only $29.95



☑ Every day ☑ Each 15 min.

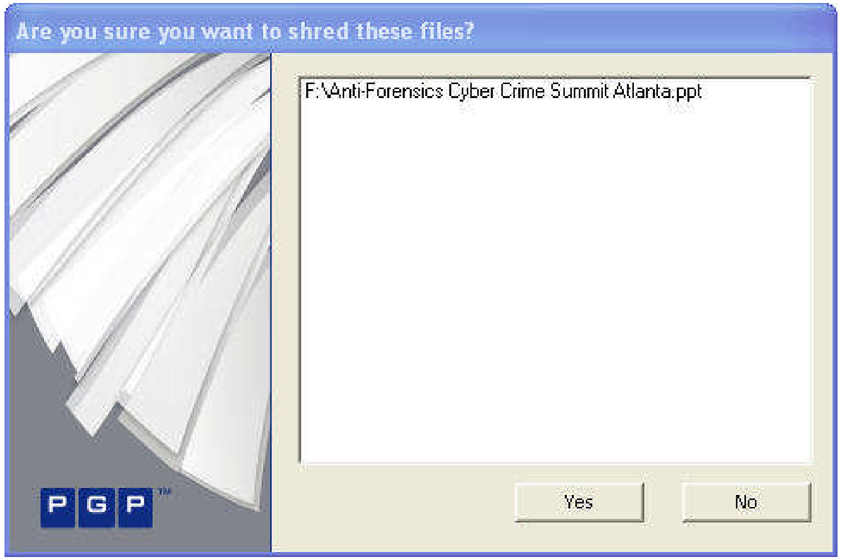
- ☑ Unused Space
  - □ System (C:)
  - ☑ NTFS (D:)
  - □ NTFS (E:)
  - □ FAT32 (F:)
- ☑ Internet
  - ☑ Temporary Internet
  - ☑ Cookies
  - ☑ History
  - ☑ Typed URLs
  - ☑ Autocomplete
- ☑ System
  - ☑ Recent Documents
  - ☑ System MRU Lists
  - ☑ Temporary Files
  - ☑ Recycle Bin
- ☑ Application Recent Files
  - □ Paint
  - ☑ Windows Media Play
  - □ WordPad

Temporary Internet Files

Your system keeps content, such as pictures, texts, flash movies, audio files, of all web pages visited by you in the this folder.

```
http://resellers.tucows.com/about/index_html/images/n
http://www.rsn.com/static/images/all_logoarea.gif
http://www.rsn.com/static/images/clear.gif
http://ad.doubleclick.net/adj/rsn.tmus/skybox;sz=140x
http://www.rsn.com/static/images/water_angle_left.gif
http://us.i1.yimg.com/us.yimg.com/i/us/smbiz/ph/ms_ph
http://rsn.skimoguls.com/triptool/js/extras.js
http://newsdirectory.com/go/guide/?r=tvr&u=www.nas
```

PGP hmmmmm



Are you sure you want to shred these files?

F:\Anti-Forensics Cyber Crime Summit Atlanta.ppt

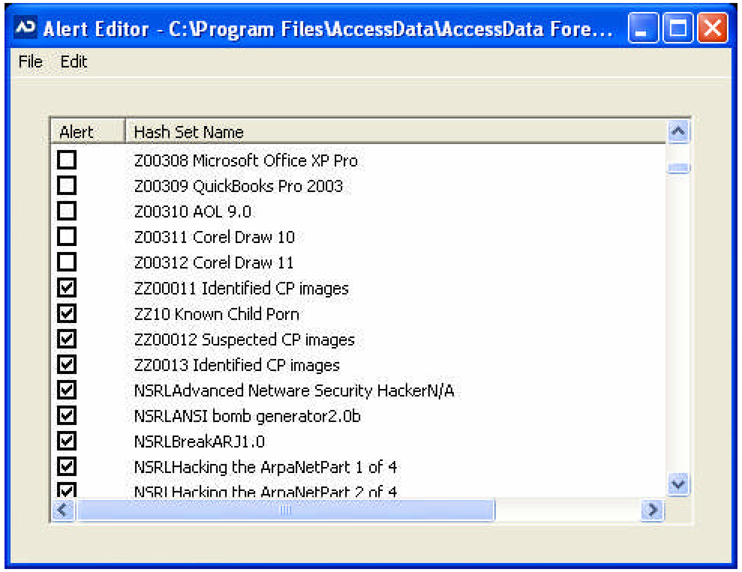
- Wiping small files: Wiping small files (under 1 K) on some NTFS-formatted disks can leave remnants of the file behind due to an NTFS optimization that stores file data in internal data structures for very small files. These structures are not considered freespace even after deleting a file, and thus they also will not be wiped using PGP Desktop’s Freespace Wipe feature. In addition, NTFS supports Journaling, which can save wiped file data in an internal operating system cache. For the highest security wiping on NTFS disks, we recommend starting your system from an OS on a different partition and using PGP Desktop’s option in the Freespace Wipe feature to overwrite these NTFS data structures (the Wipe NTFS internal data structures checkbox). This does not affect FAT32 or other supported filesystems. [NBN]

Other Popular Wiping Tools

- **srm,**
- **dban,**
- **Necrofile,**
- **Tracks Eraser Pro**

Signatures

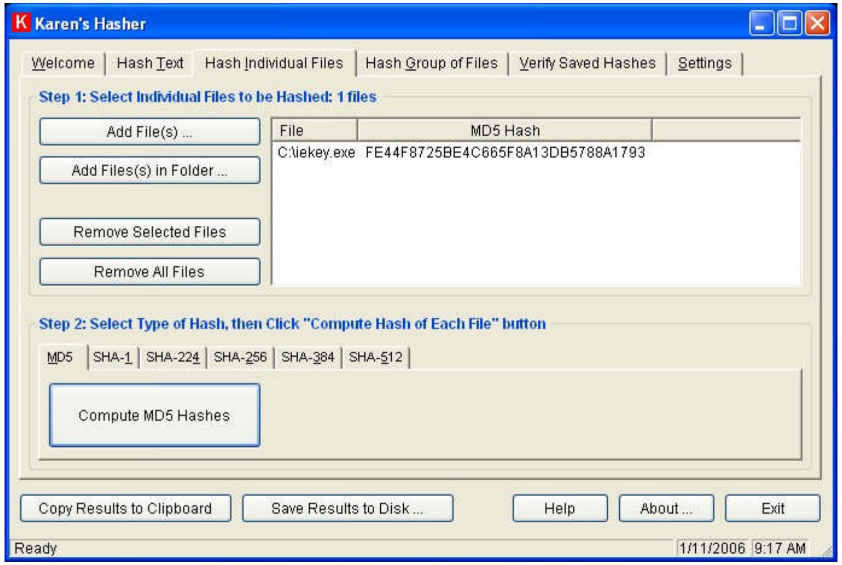
- **Examining hashes is a quick way to determine if specific files are or are not on the image that is being examined**
  - NIST – National Software Reference Library (NSRL)
    - Used to be known good – now simply known
  - Access Data – Has their own and also uses NSRL
  - Encase – Small collection but relies on NSRL


Alert Editor - C:\Program Files\AccessData\AccessData Fore...
File
Edit

Alert	Hash Set Name
□	Z00308 Microsoft Office XP Pro
□	Z00309 QuickBooks Pro 2003
□	Z00310 AOL 9.0
□	Z00311 Corel Draw 10
□	Z00312 Corel Draw 11
☑	ZZ00011 Identified CP images
☑	ZZ10 Known Child Porn
☑	ZZ00012 Suspected CP images
☑	ZZ0013 Identified CP images
☑	NSRLAdvanced Netware Security HackerN/A
☑	NSRLANSI bomb generator2.0b
☑	NSRLBreakARJ1.0
☑	NSRLHacking the ArpaNetPart 1 of 4
☑	NSRLHacking the ArpaNetPart 2 of 4

Signatures

- **However altering a single byte will alter the hash but still leave a malicious program executable**



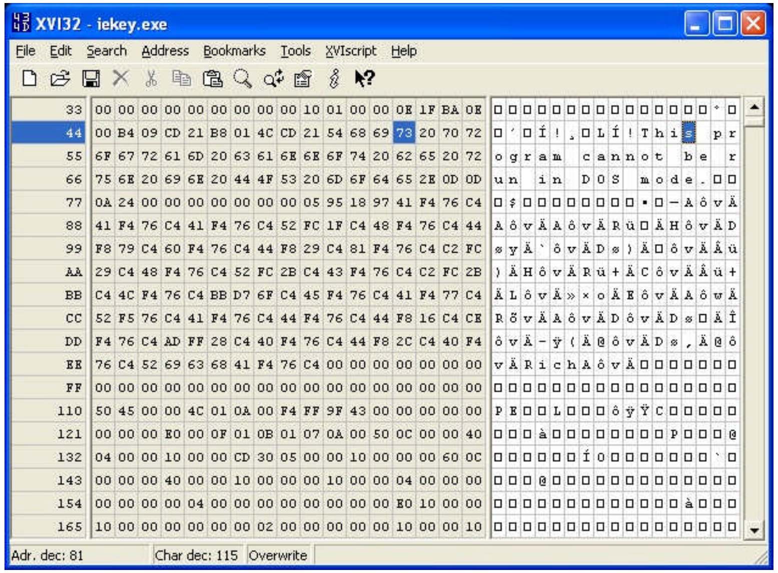
Karen's Hasher
Welcome | Hash Text | Hash Individual Files | Hash Group of Files | Verify Saved Hashes | Settings
Add File(s) ...
Add Files(s) in Folder ...
Remove Selected Files
Remove All Files
MD5 | SHA-1 | SHA-224 | SHA-256 | SHA-384 | SHA-512
Compute MD5 Hashes
Copy Results to Clipboard
Save Results to Disk ...
Help
About ...
Exit

Step 1: Select Individual Files to be Hashed: 1 files

File	MD5 Hash
C:\iekey.exe	FE44F8725BE4C665F8A13DB5788A1793

Step 2: Select Type of Hash, then Click "Compute Hash of Each File" button

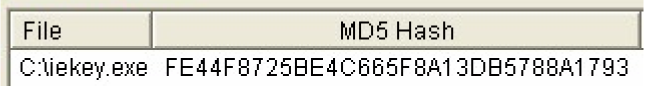
Ready 1/11/2006 9:17 AM



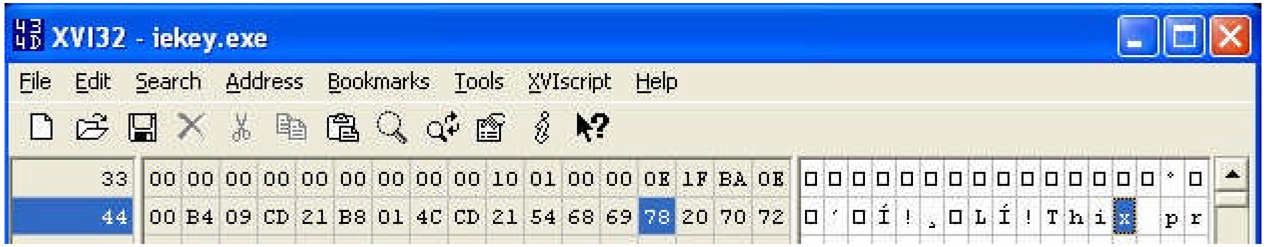
```
 33  00 00 00 00 00 00 00 00 00 10 01 00 00 0E 1F BA 0E  □□□□□□□□□□□□□□□º□
 44  00 B4 09 CD 21 B8 01 4C CD 21 54 68 69 73 20 70 72  □´□Í!¸□LÍ!This pr
 55  6F 67 72 61 6D 20 63 61 6E 6E 6F 74 20 62 65 20 72  ogram cannot be r
 66  75 6E 20 69 6E 20 44 4F 53 20 6D 6F 64 65 2E 0D 0D  un in DOS mode.□□
 77  0A 24 00 00 00 00 00 00 00 05 95 18 97 41 F4 76 C4  □$□□□□□□□□•□—AôvÄ
 88  41 F4 76 C4 41 F4 76 C4 52 FC 1F C4 48 F4 76 C4 44  AôvÄAôvÄRü□ÄHôvÄD
 99  F8 79 C4 60 F4 76 C4 44 F8 29 C4 81 F4 76 C4 C2 FC  øyÄ`ôvÄDø)Ä□ôvÄÂü
 AA  29 C4 48 F4 76 C4 52 FC 2B C4 43 F4 76 C4 C2 FC 2B  )ÄHôvÄRü+ÄCôvÄÂü+
 BB  C4 4C F4 76 C4 BB D7 6F C4 45 F4 76 C4 41 F4 77 C4  ÄLôvÄ»×oÄEôvÄAôwÄ
 CC  52 F5 76 C4 41 F4 76 C4 44 F4 76 C4 44 F8 16 C4 CE  RõvÄAôvÄDôvÄDø□ÄÎ
 DD  F4 76 C4 AD FF 28 C4 40 F4 76 C4 44 F8 2C C4 40 F4  ôvÄ-ÿ(Ä@ôvÄDø,Ä@ô
 EE  76 C4 52 69 63 68 41 F4 76 C4 00 00 00 00 00 00 00  vÄRichAôvÄ□□□□□□□
 FF  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  □□□□□□□□□□□□□□□□□
110  50 45 00 00 4C 01 0A 00 F4 FF 9F 43 00 00 00 00 00  PE□□L□□□ôÿŸC□□□□□
121  00 00 00 E0 00 0F 01 0B 01 07 0A 00 50 0C 00 00 40  □□□à□□□□□□□□P□□□@
132  04 00 00 10 00 00 CD 30 05 00 00 10 00 00 00 60 0C  □□□□□□Í0□□□□□□□`□
143  00 00 00 40 00 00 10 00 00 00 10 00 00 04 00 00 00  □□□@□□□□□□□□□□□□□
154  00 00 00 00 04 00 00 00 00 00 00 00 00 E0 10 00 00  □□□□□□□□□□□□□à□□□
165  10 00 00 00 00 00 00 02 00 00 00 00 00 10 00 00 10  □□□□□□□□□□□□□□□□□
```

Adr. dec: 81 | Char dec: 115 | Overwrite

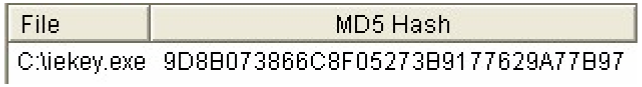
Unreliable



File	MD5 Hash
C:\iekey.exe	FE44F8725BE4C665F8A13DB5788A1793



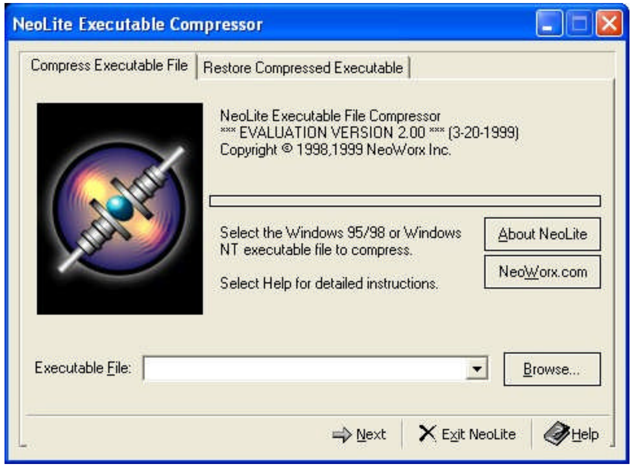
```
33  00 00 00 00 00 00 00 00 00 10 01 00 00 0E 1F BA 0E  □□□□□□□□□□□□□□□°□
44  00 B4 09 CD 21 B8 01 4C CD 21 54 68 69 78 20 70 72  □´□Í!¸□LÍ!Thix pr
```



File	MD5 Hash
C:\iekey.exe	9D8B073866C8F05273B9177629A77B97

EXE Packers

- **A Packer can change the signature of any exe file and render a search for a known MD5 useless**
- **The potentially malicious file will not be found with an antivirus scanner**



NeoLite Executable Compressor

NeoLite Executable File Compressor
*** EVALUATION VERSION 2.00 *** (3-20-1999)
Copyright © 1998,1999 NeoWorx Inc.

Select the Windows 95/98 or Windows NT executable file to compress.

Select Help for detailed instructions.

Executable File:

Available Packers

- Alloy 4.14
- Aspack 21
- Cexe NT only
- Diet
- Lzexe 1.00a
- Pack 1.0
- Pecompact 1.20
- Pecompact 1.23
- Petite21
- Petite22
- Pklite32
- Stoner_Compress
- Gui for several packers
- UPX101
- wWinlite
- WWpack 3.05b3
- ProTools

Binders

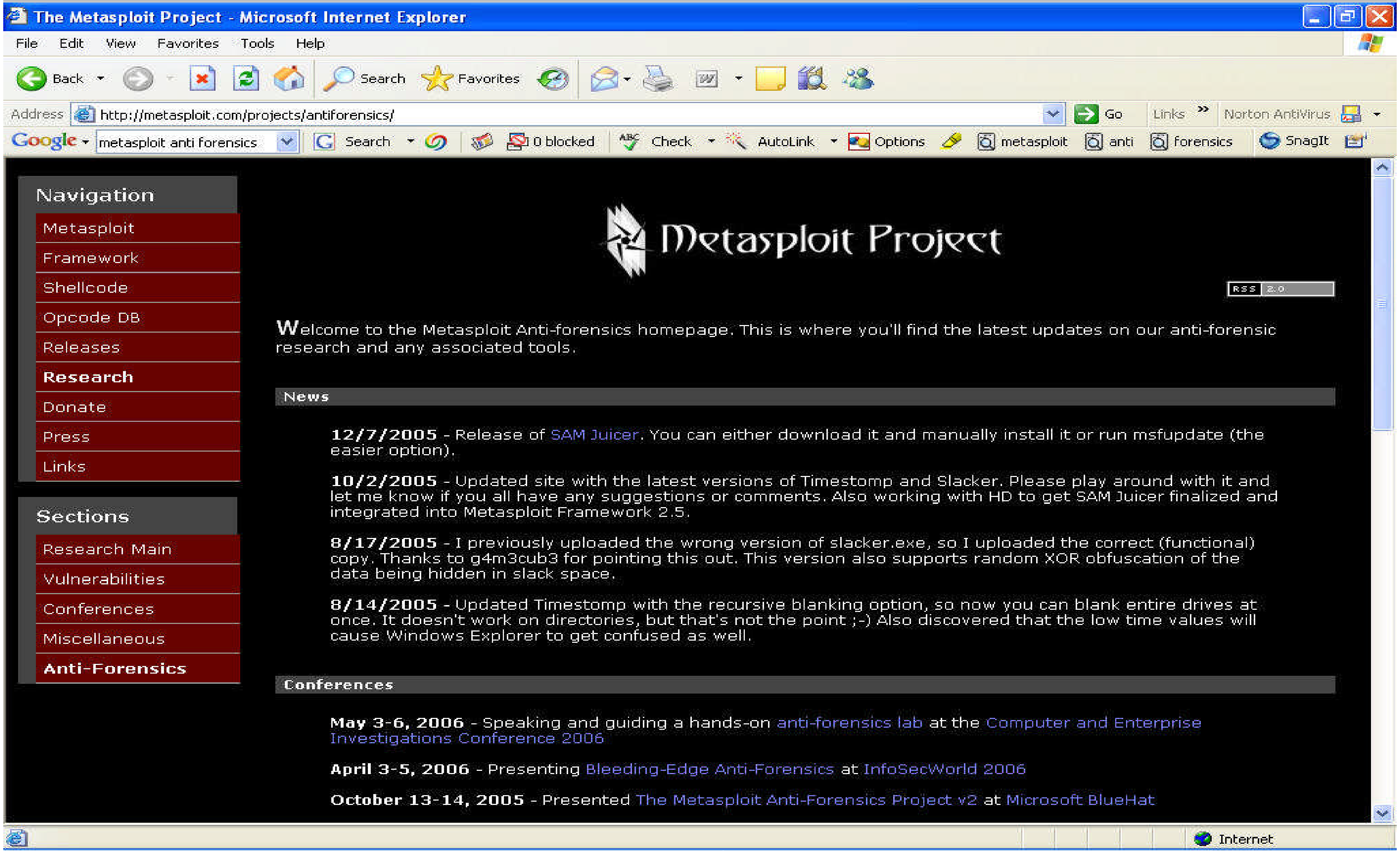
- **Binders combine two or more executable in to a single executable file**
- **Allows the bad guy to attach a Trojan, Key logger or other malicious program to a common exe file**
- **The resulting MD5 will not match a known bad database**
- **37 different free binders are downloadable at http://www.trojanfrance.com/index.php?dir=Binders/**

SECURE® COMPUTING

Downloadable Binders

- Dropper Source Generator 0.1
- Attach
- Asylum Binder 1.0 by Slim
- BigJack Joiner
- Binder
- Binding Suite
- BladeJoiner 1.0 by Blade
- BladeJoiner 1.5 by Blade
- BladeJoiner 1.55 by Blade
- Blade-Bogart Joiner
- Blade-Stoner Joiner
- Concealer
- EliteWrap
- Embedder 1.50
- Exe Bind 1.0
- Exe Maker
- FC Binder
- GoboWrap 1.0b
- Infector 2.0
- Infector 9.0
- Juntador Beta
- MultiBinder
- PE-intro adder
- Rat Packer
- RNS Exe Joiner
- SaranWrap
- Senna Spy One Exe Maker
- Senna Spy One Exe Maker 2000
- Senna Spy One Exe Maker 2000 - 2.0a
- SilkRope 1.0
- SilkRope 1.1
- SilkRope 2.0
- SilkRope2k
- TOP 1.0 by DaRaT
- TOP 2.0 by DaRaT
- TOP 2.0 beta by DaRaT
- TOP 2.1 by DaRaT
- TOP 4.0 by DaRaT
- TOP GUI by DaRaT
- TOP GUI 2 by DaRaT
- TrojanMan
- WeirdBinder by Weird
- X-Exejoiner and Icon changer by Lazarus
- Zyon 1.0 multibinder
- Sudden Discharge Compresso

Metasploit Anti Forensics


The Metasploit Project - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites
Address http://metasploit.com/projects/antiforensics/
Go Links Norton AntiVirus
Google metasploit anti forensics Search 0 blocked Check AutoLink Options metasploit anti forensics SnagIt
Internet

Navigation

- Metasploit
- Framework
- Shellcode
- Opcode DB
- Releases
- **Research**
- Donate
- Press
- Links

Sections

- Research Main
- Vulnerabilities
- Conferences
- Miscellaneous
- **Anti-Forensics**

Metasploit Project

RSS 2.0

Welcome to the Metasploit Anti-forensics homepage. This is where you'll find the latest updates on our anti-forensic research and any associated tools.

News

12/7/2005 - Release of SAM Juicer. You can either download it and manually install it or run msfupdate (the easier option).

10/2/2005 - Updated site with the latest versions of Timestomp and Slacker. Please play around with it and let me know if you all have any suggestions or comments. Also working with HD to get SAM Juicer finalized and integrated into Metasploit Framework 2.5.

8/17/2005 - I previously uploaded the wrong version of slacker.exe, so I uploaded the correct (functional) copy. Thanks to g4m3cub3 for pointing this out. This version also supports random XOR obfuscation of the data being hidden in slack space.

8/14/2005 - Updated Timestomp with the recursive blanking option, so now you can blank entire drives at once. It doesn't work on directories, but that's not the point ;-) Also discovered that the low time values will cause Windows Explorer to get confused as well.

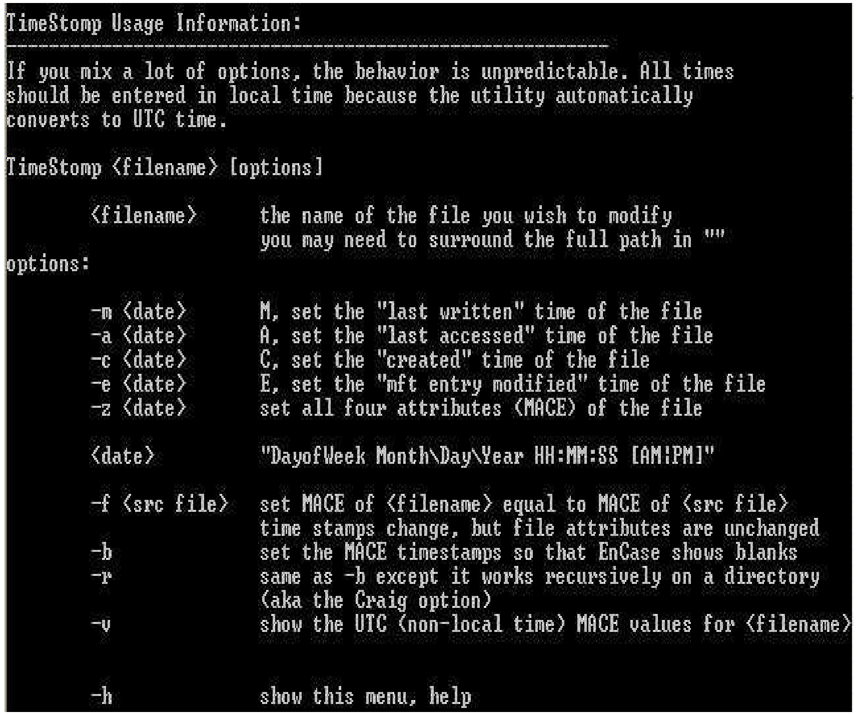
Conferences

May 3-6, 2006 - Speaking and guiding a hands-on anti-forensics lab at the Computer and Enterprise Investigations Conference 2006

April 3-5, 2006 - Presenting Bleeding-Edge Anti-Forensics at InfoSecWorld 2006

October 13-14, 2005 - Presented The Metasploit Anti-Forensics Project v2 at Microsoft BlueHat

Timestomp



```
TimeStomp Usage Information:
---------------------------------------------------------------
If you mix a lot of options, the behavior is unpredictable. All times
should be entered in local time because the utility automatically
converts to UTC time.

TimeStomp <filename> [options]

        <filename>      the name of the file you wish to modify
                        you may need to surround the full path in ""
options:

        -m <date>       M, set the "last written" time of the file
        -a <date>       A, set the "last accessed" time of the file
        -c <date>       C, set the "created" time of the file
        -e <date>       E, set the "mft entry modified" time of the file
        -z <date>       set all four attributes (MACE) of the file

        <date>          "DayofWeek Month\Day\Year HH:MM:SS [AM|PM]"

        -f <src file>   set MACE of <filename> equal to MACE of <src file>
                        time stamps change, but file attributes are unchanged
        -b              set the MACE timestamps so that EnCase shows blanks
        -r              same as -b except it works recursively on a directory
                        (aka the Craig option)
        -v              show the UTC (non-local time) MACE values for <filename>


        -h              show this menu, help
```

Metasploit

AntiForensics

Project

www.metasploit.com/projects/antiforensics/

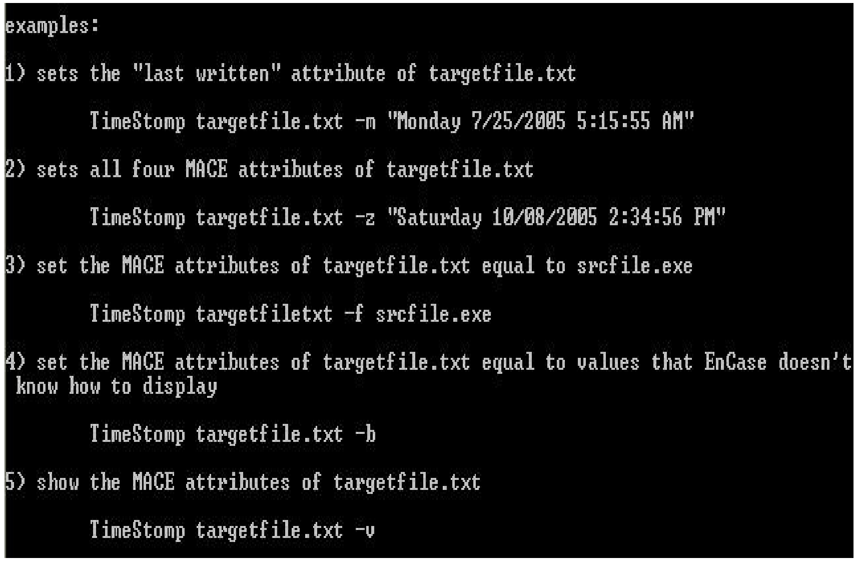
uses the following Windows system calls:

- NtQueryInformationFile()
- NtSetInformationFile()

doesn't use

- SetFileTime()

Timestomp



```
examples:

1) sets the "last written" attribute of targetfile.txt

        TimeStomp targetfile.txt -m "Monday 7/25/2005 5:15:55 AM"

2) sets all four MACE attributes of targetfile.txt

        TimeStomp targetfile.txt -z "Saturday 10/08/2005 2:34:56 PM"

3) set the MACE attributes of targetfile.txt equal to srcfile.exe

        TimeStomp targetfiletxt -f srcfile.exe

4) set the MACE attributes of targetfile.txt equal to values that EnCase doesn't
 know how to display

        TimeStomp targetfile.txt -b

5) show the MACE attributes of targetfile.txt

        TimeStomp targetfile.txt -v
```

Metasploit

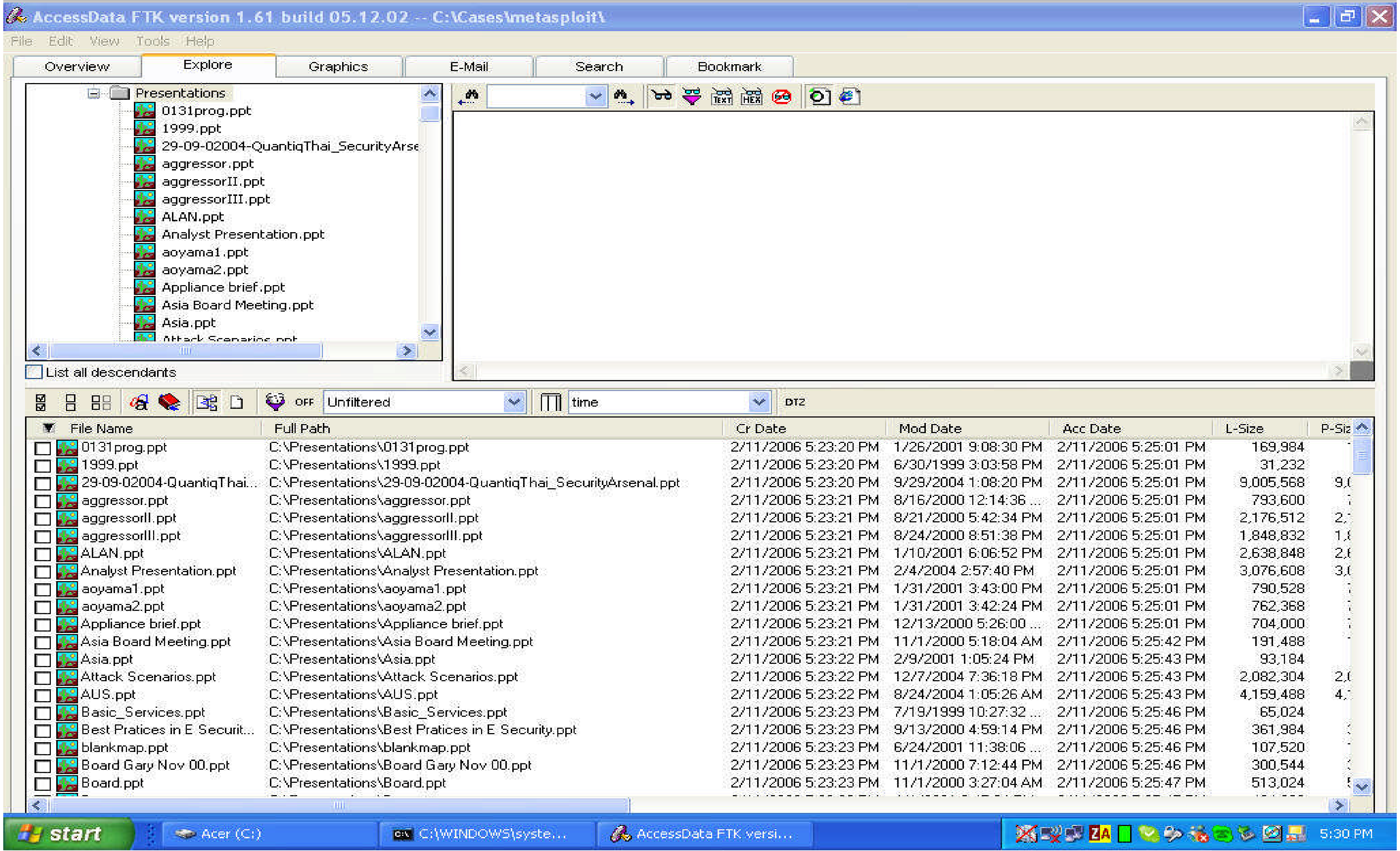
AntiForensics

Project

www.metasploit.com/projects/antiforensics/

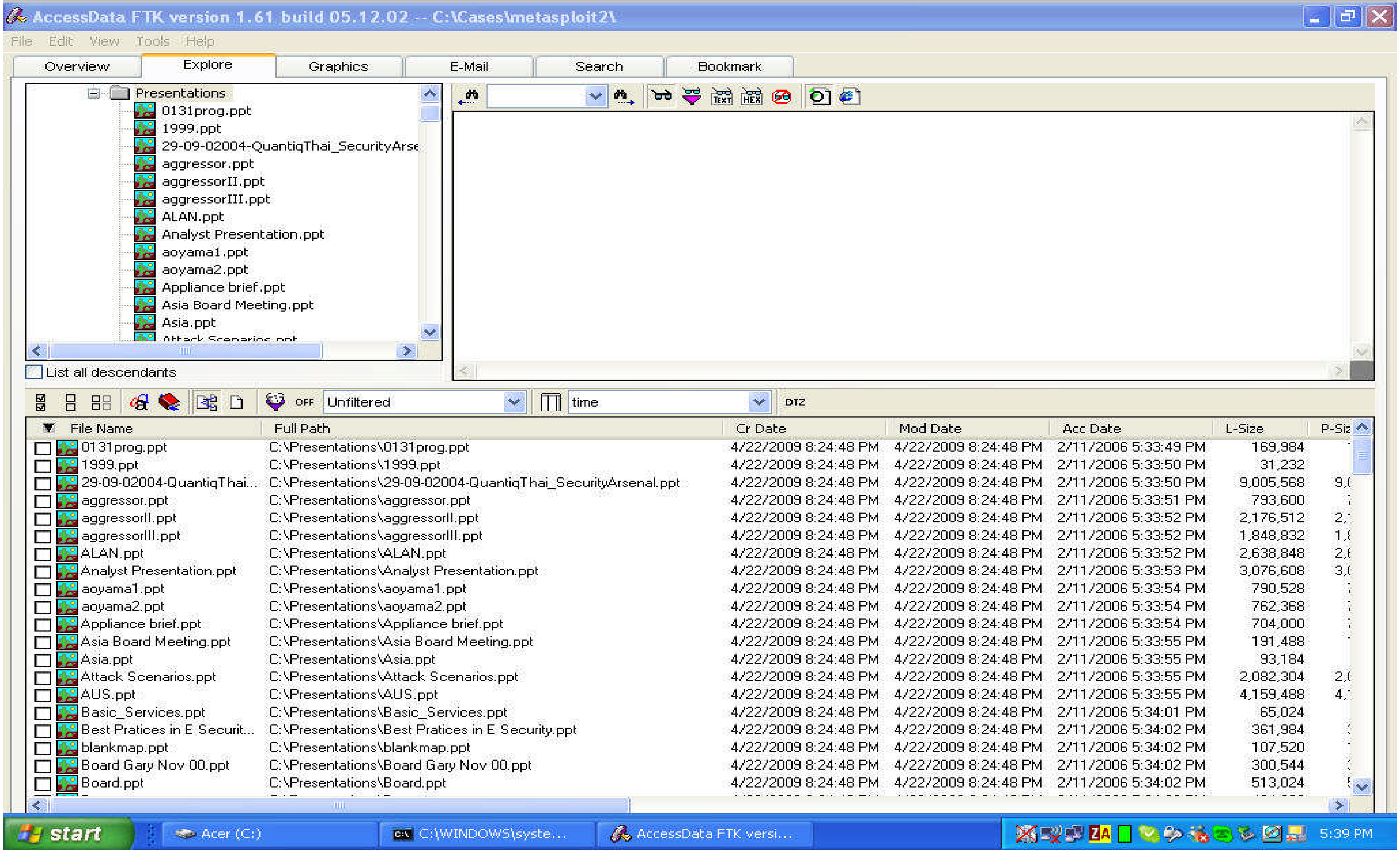
SECURE® COMPUTING

Timestomp – FTK Unmodified



File Name	Full Path	Cr Date	Mod Date	Acc Date	L-Size	P-Siz
0131prog.ppt	C:\Presentations\0131prog.ppt	2/11/2006 5:23:20 PM	1/26/2001 9:08:30 PM	2/11/2006 5:25:01 PM	169,984	
1999.ppt	C:\Presentations\1999.ppt	2/11/2006 5:23:20 PM	6/30/1999 3:03:58 PM	2/11/2006 5:25:01 PM	31,232	
29-09-02004-QuantiqThai...	C:\Presentations\29-09-02004-QuantiqThai_SecurityArsenal.ppt	2/11/2006 5:23:20 PM	9/29/2004 1:08:20 PM	2/11/2006 5:25:01 PM	9,005,568	9,(
aggressor.ppt	C:\Presentations\aggressor.ppt	2/11/2006 5:23:21 PM	8/16/2000 12:14:36 ...	2/11/2006 5:25:01 PM	793,600	
aggressorII.ppt	C:\Presentations\aggressorII.ppt	2/11/2006 5:23:21 PM	8/21/2000 5:42:34 PM	2/11/2006 5:25:01 PM	2,176,512	2,
aggressorIII.ppt	C:\Presentations\aggressorIII.ppt	2/11/2006 5:23:21 PM	8/24/2000 8:51:38 PM	2/11/2006 5:25:01 PM	1,848,832	1,
ALAN.ppt	C:\Presentations\ALAN.ppt	2/11/2006 5:23:21 PM	1/10/2001 6:06:52 PM	2/11/2006 5:25:01 PM	2,638,848	2,
Analyst Presentation.ppt	C:\Presentations\Analyst Presentation.ppt	2/11/2006 5:23:21 PM	2/4/2004 2:57:40 PM	2/11/2006 5:25:01 PM	3,076,608	3,(
aoyama1.ppt	C:\Presentations\aoyama1.ppt	2/11/2006 5:23:21 PM	1/31/2001 3:43:00 PM	2/11/2006 5:25:01 PM	790,528	
aoyama2.ppt	C:\Presentations\aoyama2.ppt	2/11/2006 5:23:21 PM	1/31/2001 3:42:24 PM	2/11/2006 5:25:01 PM	762,368	
Appliance brief.ppt	C:\Presentations\Appliance brief.ppt	2/11/2006 5:23:21 PM	12/13/2000 5:26:00 ...	2/11/2006 5:25:01 PM	704,000	
Asia Board Meeting.ppt	C:\Presentations\Asia Board Meeting.ppt	2/11/2006 5:23:21 PM	11/1/2000 5:18:04 AM	2/11/2006 5:25:42 PM	191,488	
Asia.ppt	C:\Presentations\Asia.ppt	2/11/2006 5:23:22 PM	2/9/2001 1:05:24 PM	2/11/2006 5:25:43 PM	93,184	
Attack Scenarios.ppt	C:\Presentations\Attack Scenarios.ppt	2/11/2006 5:23:22 PM	12/7/2004 7:36:18 PM	2/11/2006 5:25:43 PM	2,082,304	2,(
AUS.ppt	C:\Presentations\AUS.ppt	2/11/2006 5:23:22 PM	8/24/2004 1:05:26 AM	2/11/2006 5:25:43 PM	4,159,488	4,
Basic_Services.ppt	C:\Presentations\Basic_Services.ppt	2/11/2006 5:23:23 PM	7/19/1999 10:27:32 ...	2/11/2006 5:25:46 PM	65,024	
Best Pratices in E Securit...	C:\Presentations\Best Pratices in E Security.ppt	2/11/2006 5:23:23 PM	9/13/2000 4:59:14 PM	2/11/2006 5:25:46 PM	361,984	
blankmap.ppt	C:\Presentations\blankmap.ppt	2/11/2006 5:23:23 PM	6/24/2001 11:38:06 ...	2/11/2006 5:25:46 PM	107,520	
Board Gary Nov 00.ppt	C:\Presentations\Board Gary Nov 00.ppt	2/11/2006 5:23:23 PM	11/1/2000 7:12:44 PM	2/11/2006 5:25:46 PM	300,544	
Board.ppt	C:\Presentations\Board.ppt	2/11/2006 5:23:23 PM	11/1/2000 3:27:04 AM	2/11/2006 5:25:47 PM	513,024	

Timestomp - FTK Modified



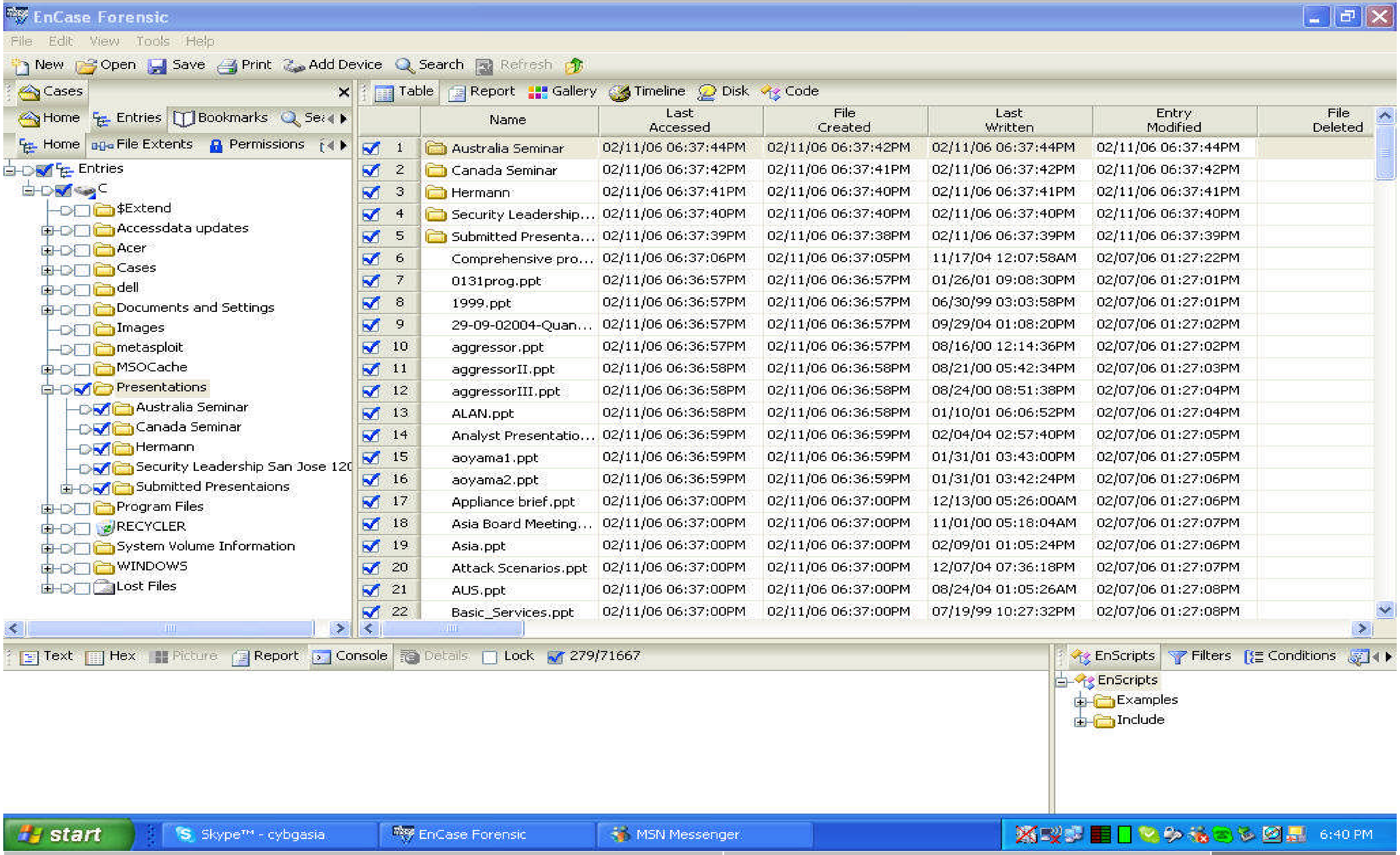
Presentations
- 0131prog.ppt
- 1999.ppt
- 29-09-02004-QuantiqThai_SecurityArse
- aggressor.ppt
- aggressorII.ppt
- aggressorIII.ppt
- ALAN.ppt
- Analyst Presentation.ppt
- aoyama1.ppt
- aoyama2.ppt
- Appliance brief.ppt
- Asia Board Meeting.ppt
- Asia.ppt
- Attack Scenarios.ppt

Filter: Unfiltered

Column setting: time

File Name	Full Path	Cr Date	Mod Date	Acc Date	L-Size	P-Siz
☐ 0131prog.ppt	C:\Presentations\0131prog.ppt	4/22/2009 8:24:48 PM	4/22/2009 8:24:48 PM	2/11/2006 5:33:49 PM	169,984	
☐ 1999.ppt	C:\Presentations\1999.ppt	4/22/2009 8:24:48 PM	4/22/2009 8:24:48 PM	2/11/2006 5:33:50 PM	31,232	
☐ 29-09-02004-QuantiqThai...	C:\Presentations\29-09-02004-QuantiqThai_SecurityArsenal.ppt	4/22/2009 8:24:48 PM	4/22/2009 8:24:48 PM	2/11/2006 5:33:50 PM	9,005,568	9,0
☐ aggressor.ppt	C:\Presentations\aggressor.ppt	4/22/2009 8:24:48 PM	4/22/2009 8:24:48 PM	2/11/2006 5:33:51 PM	793,600	
☐ aggressorII.ppt	C:\Presentations\aggressorII.ppt	4/22/2009 8:24:48 PM	4/22/2009 8:24:48 PM	2/11/2006 5:33:52 PM	2,176,512	2,1
☐ aggressorIII.ppt	C:\Presentations\aggressorIII.ppt	4/22/2009 8:24:48 PM	4/22/2009 8:24:48 PM	2/11/2006 5:33:52 PM	1,848,832	1,8
☐ ALAN.ppt	C:\Presentations\ALAN.ppt	4/22/2009 8:24:48 PM	4/22/2009 8:24:48 PM	2/11/2006 5:33:52 PM	2,638,848	2,6
☐ Analyst Presentation.ppt	C:\Presentations\Analyst Presentation.ppt	4/22/2009 8:24:48 PM	4/22/2009 8:24:48 PM	2/11/2006 5:33:53 PM	3,076,608	3,0
☐ aoyama1.ppt	C:\Presentations\aoyama1.ppt	4/22/2009 8:24:48 PM	4/22/2009 8:24:48 PM	2/11/2006 5:33:54 PM	790,528	
☐ aoyama2.ppt	C:\Presentations\aoyama2.ppt	4/22/2009 8:24:48 PM	4/22/2009 8:24:48 PM	2/11/2006 5:33:54 PM	762,368	
☐ Appliance brief.ppt	C:\Presentations\Appliance brief.ppt	4/22/2009 8:24:48 PM	4/22/2009 8:24:48 PM	2/11/2006 5:33:54 PM	704,000	
☐ Asia Board Meeting.ppt	C:\Presentations\Asia Board Meeting.ppt	4/22/2009 8:24:48 PM	4/22/2009 8:24:48 PM	2/11/2006 5:33:55 PM	191,488	
☐ Asia.ppt	C:\Presentations\Asia.ppt	4/22/2009 8:24:48 PM	4/22/2009 8:24:48 PM	2/11/2006 5:33:55 PM	93,184	
☐ Attack Scenarios.ppt	C:\Presentations\Attack Scenarios.ppt	4/22/2009 8:24:48 PM	4/22/2009 8:24:48 PM	2/11/2006 5:33:55 PM	2,082,304	2,0
☐ AUS.ppt	C:\Presentations\AUS.ppt	4/22/2009 8:24:48 PM	4/22/2009 8:24:48 PM	2/11/2006 5:33:55 PM	4,159,488	4,1
☐ Basic_Services.ppt	C:\Presentations\Basic_Services.ppt	4/22/2009 8:24:48 PM	4/22/2009 8:24:48 PM	2/11/2006 5:34:01 PM	65,024	
☐ Best Pratices in E Securit...	C:\Presentations\Best Pratices in E Security.ppt	4/22/2009 8:24:48 PM	4/22/2009 8:24:48 PM	2/11/2006 5:34:02 PM	361,984	
☐ blankmap.ppt	C:\Presentations\blankmap.ppt	4/22/2009 8:24:48 PM	4/22/2009 8:24:48 PM	2/11/2006 5:34:02 PM	107,520	
☐ Board Gary Nov 00.ppt	C:\Presentations\Board Gary Nov 00.ppt	4/22/2009 8:24:48 PM	4/22/2009 8:24:48 PM	2/11/2006 5:34:02 PM	300,544	
☐ Board.ppt	C:\Presentations\Board.ppt	4/22/2009 8:24:48 PM	4/22/2009 8:24:48 PM	2/11/2006 5:34:02 PM	513,024	

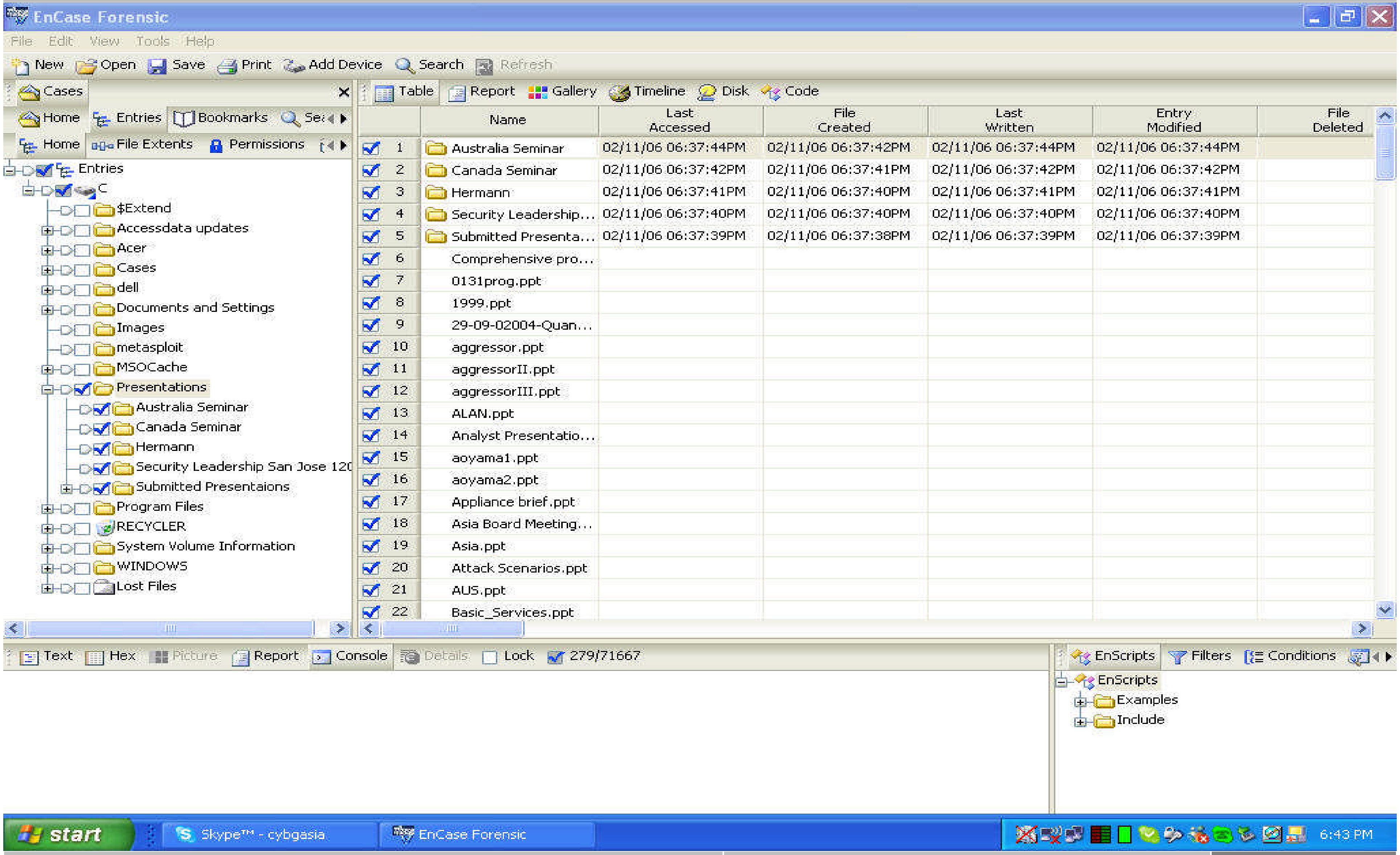
Timestomp – Encase Unmodified



		Name	Last Accessed	File Created	Last Written	Entry Modified	File Deleted
☑	1	Australia Seminar	02/11/06 06:37:44PM	02/11/06 06:37:42PM	02/11/06 06:37:44PM	02/11/06 06:37:44PM	
☑	2	Canada Seminar	02/11/06 06:37:42PM	02/11/06 06:37:41PM	02/11/06 06:37:42PM	02/11/06 06:37:42PM	
☑	3	Hermann	02/11/06 06:37:41PM	02/11/06 06:37:40PM	02/11/06 06:37:41PM	02/11/06 06:37:41PM	
☑	4	Security Leadership...	02/11/06 06:37:40PM	02/11/06 06:37:40PM	02/11/06 06:37:40PM	02/11/06 06:37:40PM	
☑	5	Submitted Presenta...	02/11/06 06:37:39PM	02/11/06 06:37:38PM	02/11/06 06:37:39PM	02/11/06 06:37:39PM	
☑	6	Comprehensive pro...	02/11/06 06:37:06PM	02/11/06 06:37:05PM	11/17/04 12:07:58AM	02/07/06 01:27:22PM	
☑	7	0131prog.ppt	02/11/06 06:36:57PM	02/11/06 06:36:57PM	01/26/01 09:08:30PM	02/07/06 01:27:01PM	
☑	8	1999.ppt	02/11/06 06:36:57PM	02/11/06 06:36:57PM	06/30/99 03:03:58PM	02/07/06 01:27:01PM	
☑	9	29-09-02004-Quan...	02/11/06 06:36:57PM	02/11/06 06:36:57PM	09/29/04 01:08:20PM	02/07/06 01:27:02PM	
☑	10	aggressor.ppt	02/11/06 06:36:57PM	02/11/06 06:36:57PM	08/16/00 12:14:36PM	02/07/06 01:27:02PM	
☑	11	aggressorII.ppt	02/11/06 06:36:58PM	02/11/06 06:36:58PM	08/21/00 05:42:34PM	02/07/06 01:27:03PM	
☑	12	aggressorIII.ppt	02/11/06 06:36:58PM	02/11/06 06:36:58PM	08/24/00 08:51:38PM	02/07/06 01:27:04PM	
☑	13	ALAN.ppt	02/11/06 06:36:58PM	02/11/06 06:36:58PM	01/10/01 06:06:52PM	02/07/06 01:27:04PM	
☑	14	Analyst Presentatio...	02/11/06 06:36:59PM	02/11/06 06:36:59PM	02/04/04 02:57:40PM	02/07/06 01:27:05PM	
☑	15	aoyama1.ppt	02/11/06 06:36:59PM	02/11/06 06:36:59PM	01/31/01 03:43:00PM	02/07/06 01:27:05PM	
☑	16	aoyama2.ppt	02/11/06 06:36:59PM	02/11/06 06:36:59PM	01/31/01 03:42:24PM	02/07/06 01:27:06PM	
☑	17	Appliance brief.ppt	02/11/06 06:37:00PM	02/11/06 06:37:00PM	12/13/00 05:26:00AM	02/07/06 01:27:06PM	
☑	18	Asia Board Meeting...	02/11/06 06:37:00PM	02/11/06 06:37:00PM	11/01/00 05:18:04AM	02/07/06 01:27:07PM	
☑	19	Asia.ppt	02/11/06 06:37:00PM	02/11/06 06:37:00PM	02/09/01 01:05:24PM	02/07/06 01:27:06PM	
☑	20	Attack Scenarios.ppt	02/11/06 06:37:00PM	02/11/06 06:37:00PM	12/07/04 07:36:18PM	02/07/06 01:27:07PM	
☑	21	AUS.ppt	02/11/06 06:37:00PM	02/11/06 06:37:00PM	08/24/04 01:05:26AM	02/07/06 01:27:08PM	
☑	22	Basic_Services.ppt	02/11/06 06:37:00PM	02/11/06 06:37:00PM	07/19/99 10:27:32PM	02/07/06 01:27:08PM	

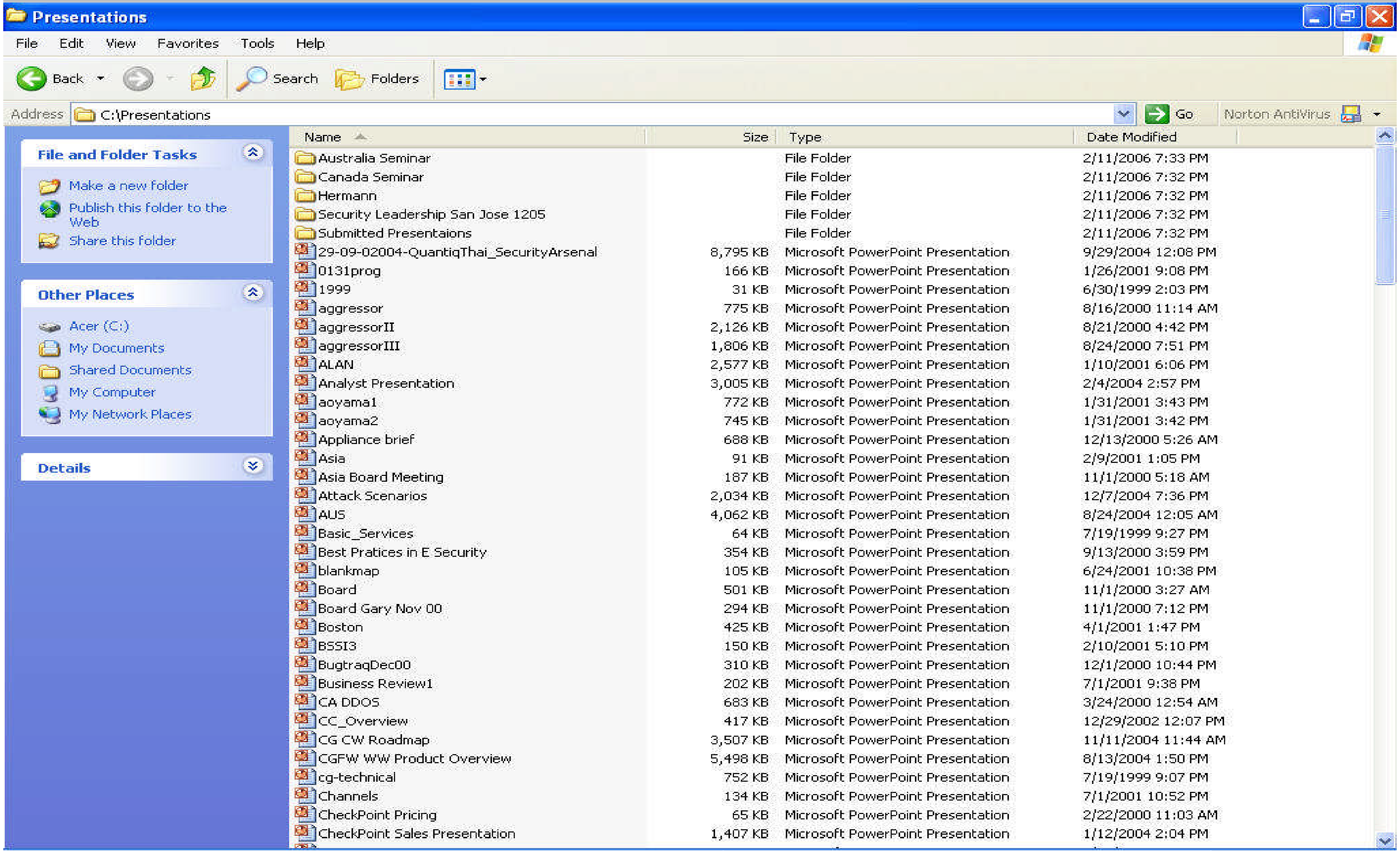
SECURE COMPUTING®

Timestomp – Encase Modified


EnCase Forensic
File Edit View Tools Help
New Open Save Print Add Device Search Refresh
Cases
Home Entries Bookmarks Sea
Home File Extents Permissions
Table Report Gallery Timeline Disk Code
Entries
C
$Extend
Accessdata updates
Acer
Cases
dell
Documents and Settings
Images
metasploit
MSOCache
Presentations
Australia Seminar
Canada Seminar
Hermann
Security Leadership San Jose 120
Submitted Presentaions
Program Files
RECYCLER
System Volume Information
WINDOWS
Lost Files
Text Hex Picture Report Console Details Lock 279/71667
EnScripts Filters Conditions
EnScripts
Examples
Include
start
Skype™ - cybgasia
EnCase Forensic
6:43 PM

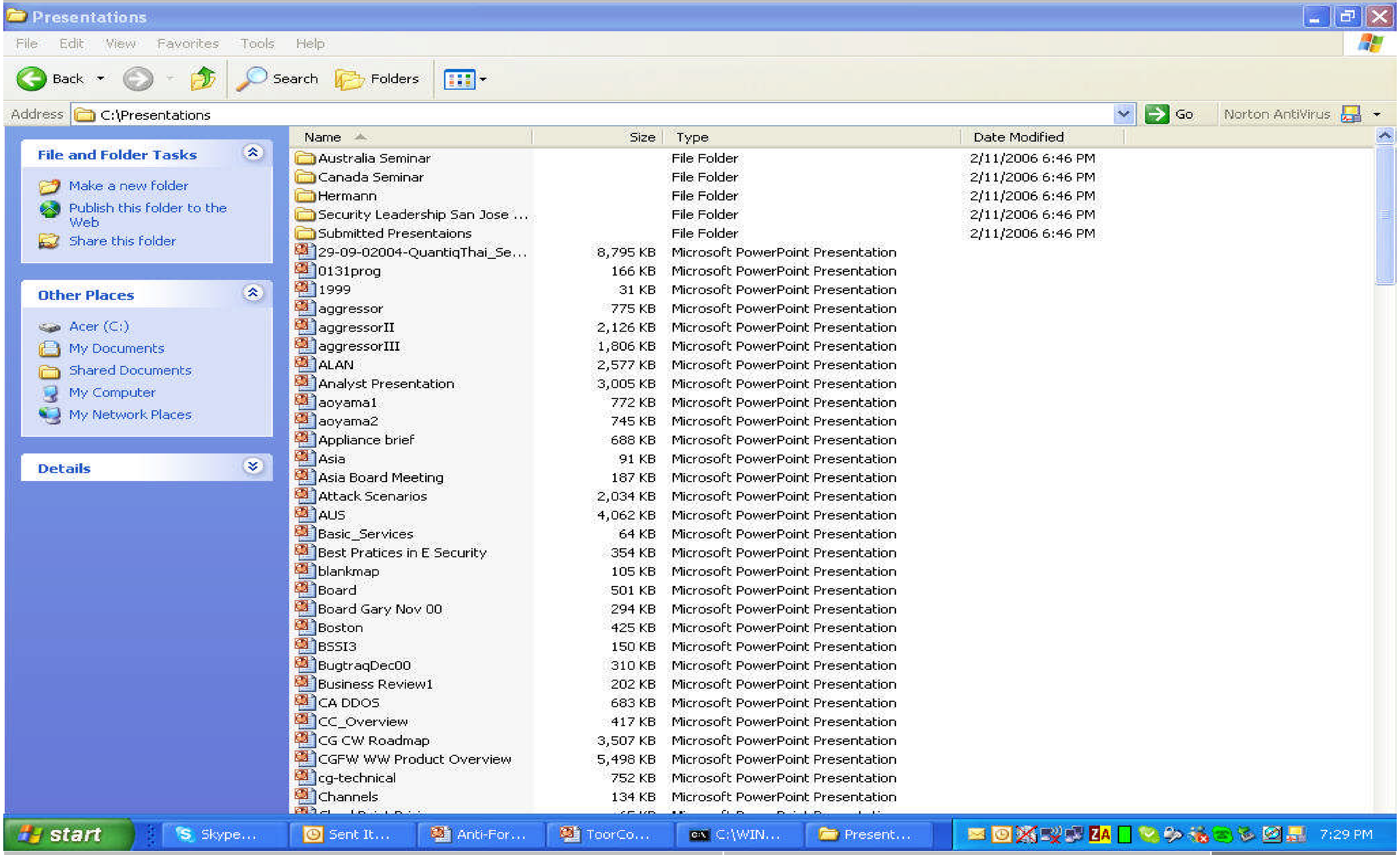
	Name	Last Accessed	File Created	Last Written	Entry Modified	File Deleted
1	Australia Seminar	02/11/06 06:37:44PM	02/11/06 06:37:42PM	02/11/06 06:37:44PM	02/11/06 06:37:44PM	
2	Canada Seminar	02/11/06 06:37:42PM	02/11/06 06:37:41PM	02/11/06 06:37:42PM	02/11/06 06:37:42PM	
3	Hermann	02/11/06 06:37:41PM	02/11/06 06:37:40PM	02/11/06 06:37:41PM	02/11/06 06:37:41PM	
4	Security Leadership...	02/11/06 06:37:40PM	02/11/06 06:37:40PM	02/11/06 06:37:40PM	02/11/06 06:37:40PM	
5	Submitted Presenta...	02/11/06 06:37:39PM	02/11/06 06:37:38PM	02/11/06 06:37:39PM	02/11/06 06:37:39PM	
6	Comprehensive pro...					
7	0131prog.ppt					
8	1999.ppt					
9	29-09-02004-Quan...					
10	aggressor.ppt					
11	aggressorII.ppt					
12	aggressorIII.ppt					
13	ALAN.ppt					
14	Analyst Presentatio...					
15	aoyama1.ppt					
16	aoyama2.ppt					
17	Appliance brief.ppt					
18	Asia Board Meeting...					
19	Asia.ppt					
20	Attack Scenarios.ppt					
21	AUS.ppt					
22	Basic_Services.ppt					

Timestomp – Explorer Unmodified



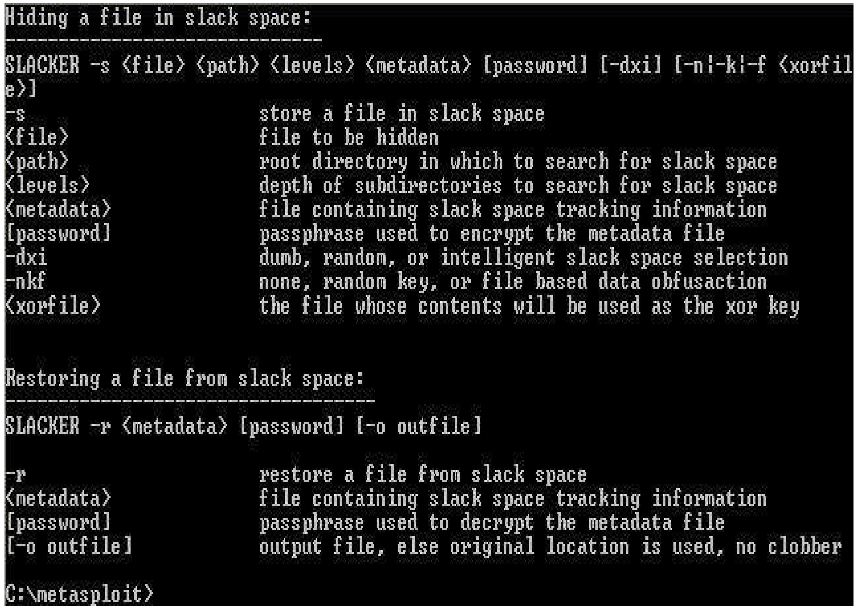
Name	Size	Type	Date Modified
Australia Seminar		File Folder	2/11/2006 7:33 PM
Canada Seminar		File Folder	2/11/2006 7:32 PM
Hermann		File Folder	2/11/2006 7:32 PM
Security Leadership San Jose 1205		File Folder	2/11/2006 7:32 PM
Submitted Presentaions		File Folder	2/11/2006 7:32 PM
29-09-02004-QuantiqThai_SecurityArsenal	8,795 KB	Microsoft PowerPoint Presentation	9/29/2004 12:08 PM
0131prog	166 KB	Microsoft PowerPoint Presentation	1/26/2001 9:08 PM
1999	31 KB	Microsoft PowerPoint Presentation	6/30/1999 2:03 PM
aggressor	775 KB	Microsoft PowerPoint Presentation	8/16/2000 11:14 AM
aggressorII	2,126 KB	Microsoft PowerPoint Presentation	8/21/2000 4:42 PM
aggressorIII	1,806 KB	Microsoft PowerPoint Presentation	8/24/2000 7:51 PM
ALAN	2,577 KB	Microsoft PowerPoint Presentation	1/10/2001 6:06 PM
Analyst Presentation	3,005 KB	Microsoft PowerPoint Presentation	2/4/2004 2:57 PM
aoyama1	772 KB	Microsoft PowerPoint Presentation	1/31/2001 3:43 PM
aoyama2	745 KB	Microsoft PowerPoint Presentation	1/31/2001 3:42 PM
Appliance brief	688 KB	Microsoft PowerPoint Presentation	12/13/2000 5:26 AM
Asia	91 KB	Microsoft PowerPoint Presentation	2/9/2001 1:05 PM
Asia Board Meeting	187 KB	Microsoft PowerPoint Presentation	11/1/2000 5:18 AM
Attack Scenarios	2,034 KB	Microsoft PowerPoint Presentation	12/7/2004 7:36 PM
AUS	4,062 KB	Microsoft PowerPoint Presentation	8/24/2004 12:05 AM
Basic_Services	64 KB	Microsoft PowerPoint Presentation	7/19/1999 9:27 PM
Best Pratices in E Security	354 KB	Microsoft PowerPoint Presentation	9/13/2000 3:59 PM
blankmap	105 KB	Microsoft PowerPoint Presentation	6/24/2001 10:38 PM
Board	501 KB	Microsoft PowerPoint Presentation	11/1/2000 3:27 AM
Board Gary Nov 00	294 KB	Microsoft PowerPoint Presentation	11/1/2000 7:12 PM
Boston	425 KB	Microsoft PowerPoint Presentation	4/1/2001 1:47 PM
BSSI3	150 KB	Microsoft PowerPoint Presentation	2/10/2001 5:10 PM
BugtraqDec00	310 KB	Microsoft PowerPoint Presentation	12/1/2000 10:44 PM
Business Review1	202 KB	Microsoft PowerPoint Presentation	7/1/2001 9:38 PM
CA DDOS	683 KB	Microsoft PowerPoint Presentation	3/24/2000 12:54 AM
CC_Overview	417 KB	Microsoft PowerPoint Presentation	12/29/2002 12:07 PM
CG CW Roadmap	3,507 KB	Microsoft PowerPoint Presentation	11/11/2004 11:44 AM
CGFW WW Product Overview	5,498 KB	Microsoft PowerPoint Presentation	8/13/2004 1:50 PM
cg-technical	752 KB	Microsoft PowerPoint Presentation	7/19/1999 9:07 PM
Channels	134 KB	Microsoft PowerPoint Presentation	7/1/2001 10:52 PM
CheckPoint Pricing	65 KB	Microsoft PowerPoint Presentation	2/22/2000 11:03 AM
CheckPoint Sales Presentation	1,407 KB	Microsoft PowerPoint Presentation	1/12/2004 2:04 PM

Timestomp – Explorer Modified



Name	Size	Type	Date Modified
Australia Seminar		File Folder	2/11/2006 6:46 PM
Canada Seminar		File Folder	2/11/2006 6:46 PM
Hermann		File Folder	2/11/2006 6:46 PM
Security Leadership San Jose ...		File Folder	2/11/2006 6:46 PM
Submitted Presentaions		File Folder	2/11/2006 6:46 PM
29-09-02004-QuantiqThai_Se...	8,795 KB	Microsoft PowerPoint Presentation	
0131prog	166 KB	Microsoft PowerPoint Presentation	
1999	31 KB	Microsoft PowerPoint Presentation	
aggressor	775 KB	Microsoft PowerPoint Presentation	
aggressorII	2,126 KB	Microsoft PowerPoint Presentation	
aggressorIII	1,806 KB	Microsoft PowerPoint Presentation	
ALAN	2,577 KB	Microsoft PowerPoint Presentation	
Analyst Presentation	3,005 KB	Microsoft PowerPoint Presentation	
aoyama1	772 KB	Microsoft PowerPoint Presentation	
aoyama2	745 KB	Microsoft PowerPoint Presentation	
Appliance brief	688 KB	Microsoft PowerPoint Presentation	
Asia	91 KB	Microsoft PowerPoint Presentation	
Asia Board Meeting	187 KB	Microsoft PowerPoint Presentation	
Attack Scenarios	2,034 KB	Microsoft PowerPoint Presentation	
AUS	4,062 KB	Microsoft PowerPoint Presentation	
Basic_Services	64 KB	Microsoft PowerPoint Presentation	
Best Pratices in E Security	354 KB	Microsoft PowerPoint Presentation	
blankmap	105 KB	Microsoft PowerPoint Presentation	
Board	501 KB	Microsoft PowerPoint Presentation	
Board Gary Nov 00	294 KB	Microsoft PowerPoint Presentation	
Boston	425 KB	Microsoft PowerPoint Presentation	
BSSI3	150 KB	Microsoft PowerPoint Presentation	
BugtraqDec00	310 KB	Microsoft PowerPoint Presentation	
Business Review1	202 KB	Microsoft PowerPoint Presentation	
CA DDOS	683 KB	Microsoft PowerPoint Presentation	
CC_Overview	417 KB	Microsoft PowerPoint Presentation	
CG CW Roadmap	3,507 KB	Microsoft PowerPoint Presentation	
CGFW WW Product Overview	5,498 KB	Microsoft PowerPoint Presentation	
cg-technical	752 KB	Microsoft PowerPoint Presentation	
Channels	134 KB	Microsoft PowerPoint Presentation	

Slacker



```
Hiding a file in slack space:
------------------------------
SLACKER -s <file> <path> <levels> <metadata> [password] [-dxi] [-n|-k|-f <xorfil
e>]
-s                      store a file in slack space
<file>                  file to be hidden
<path>                  root directory in which to search for slack space
<levels>                depth of subdirectories to search for slack space
<metadata>              file containing slack space tracking information
[password]              passphrase used to encrypt the metadata file
-dxi                    dumb, random, or intelligent slack space selection
-nkf                    none, random key, or file based data obfusaction
<xorfile>               the file whose contents will be used as the xor key


Restoring a file from slack space:
-----------------------------------
SLACKER -r <metadata> [password] [-o outfile]

-r                      restore a file from slack space
<metadata>              file containing slack space tracking information
[password]              passphrase used to decrypt the metadata file
[-o outfile]            output file, else original location is used, no clobber

C:\metasploit>
```

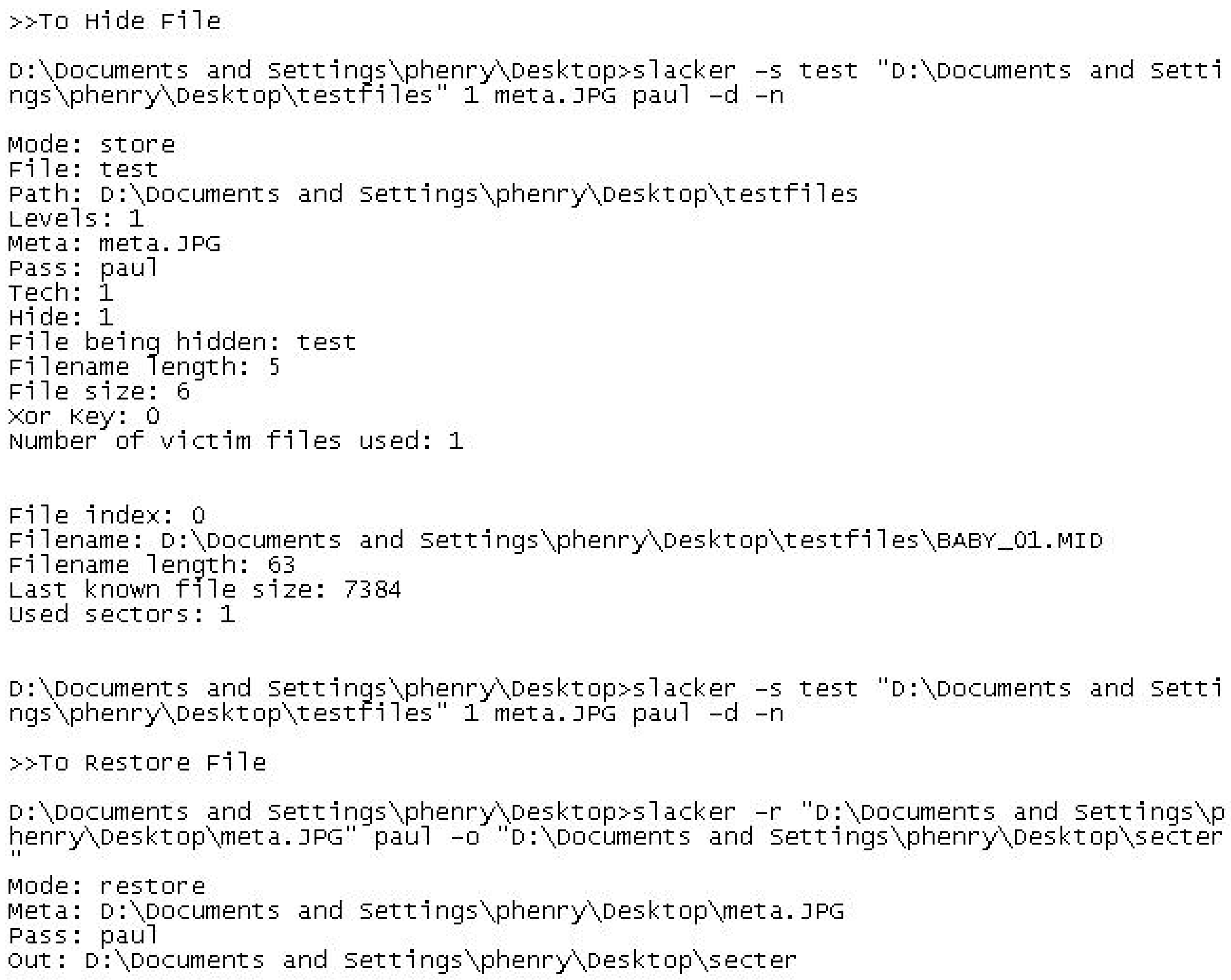
Metasploit

AntiForensics

Project

www.metasploit.com/projects/antiforensics/

Slacker Example



```
>>To Hide File

D:\Documents and Settings\phenry\Desktop>slacker -s test "D:\Documents and Setti
ngs\phenry\Desktop\testfiles" 1 meta.JPG paul -d -n

Mode: store
File: test
Path: D:\Documents and Settings\phenry\Desktop\testfiles
Levels: 1
Meta: meta.JPG
Pass: paul
Tech: 1
Hide: 1
File being hidden: test
Filename length: 5
File size: 6
Xor Key: 0
Number of victim files used: 1


File index: 0
Filename: D:\Documents and Settings\phenry\Desktop\testfiles\BABY_01.MID
Filename length: 63
Last known file size: 7384
Used sectors: 1


D:\Documents and Settings\phenry\Desktop>slacker -s test "D:\Documents and Setti
ngs\phenry\Desktop\testfiles" 1 meta.JPG paul -d -n

>>To Restore File

D:\Documents and Settings\phenry\Desktop>slacker -r "D:\Documents and Settings\p
henry\Desktop\meta.JPG" paul -o "D:\Documents and Settings\phenry\Desktop\secter
"
Mode: restore
Meta: D:\Documents and Settings\phenry\Desktop\meta.JPG
Pass: paul
Out: D:\Documents and Settings\phenry\Desktop\secter
```

Transmogrify – Coming Soon

- Transmogrify - First ever tool to defeat EnCase's file signature capabilities by allowing you to mask and unmask your files as any file type. (Coming Soon)

Metasploit

AntiForensics

Project

www.metasploit.com/projects/antiforensics/

Samjuicer

- **SAM Juicer does what pwdump does without hitting the disk**
  - Pwdump – opens a share, drops binaries to the disk and starts a service to inject itself in to LSASS
- **Reuses a transport channel that the Metaspoit framework uses, remotely and directly injects itself into the LSASS and sucks down the encrypted password files without leaving a file, touching the registry or starting a service.**
  - Not having files or services starting makes protection technologies that rely on that 'signature' to prevent the attack rather impotent.

Metasploit

AntiForensics

Project

www.metasploit.com/projects/antiforensics/

Future Work

- NTFS change journal modification
- Secure deletion
- Documentation of anti-forensic techniques
- Browser log manipulation
- File meta-data modification
- NTFS extended attributes

Metasploit

AntiForensics

Project

www.metasploit.com/projects/antiforensics/

Vincent Liu

Partner in Stach & Liu

vliu@stachliu.com

www.stachliu.com

Advanced Anti-Forensics

- **What if the malicious file never touched the disk?**
- **MOSDEF (mose-def) is short for “Most Definitely”**
  - MOSDEF is a retargetable, position independent code, C compiler that supports dynamic remote code linking
  - In short, after you've overflowed a process you can compile programs to run inside that process and report back to you
- www.immunitysec.com/resources-freesoftware.shtml

Linux Anti-Forensics

- **Simply hide data where commercial forensic tools don’t necessarily look**
  - Rune fs
    - Hide data in bad blocks inode
  - Waffen fs
    - Hide data in spoofed journal file
  - KY fs
    - Hide data in null directory entries
  - Data mule fs
    - Hide data in reserved space

Anti-Forensics

- **In conclusion of our look at Anti-Forensics tools;**
  - *The tools freely available on the public Internet for the cyber criminal to cover his/her tracks and to hide data have clearly rendered file systems as no longer being an accurate log of malicious system activity…*

Thank You….

Paul A. Henry

MCP+I, MCSE, CFSA, CFSO, CCSA, CCSE, CISM, CISA, CISSP, ISSAP , CIFI

Vice President

Secure Computing

Paul_henry@securecomputing.com