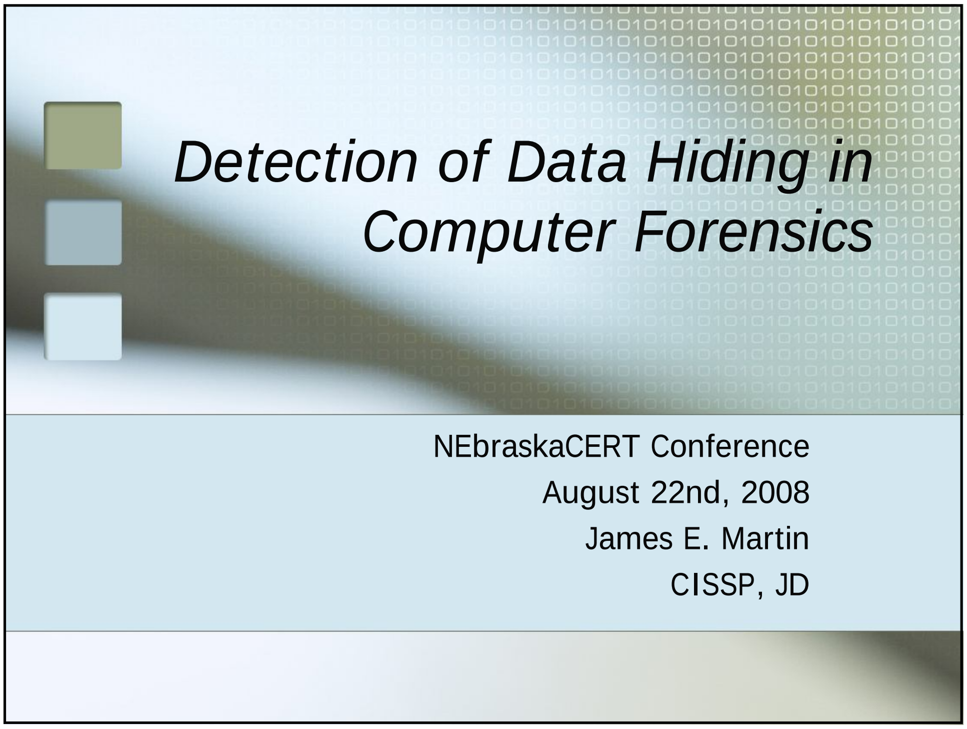
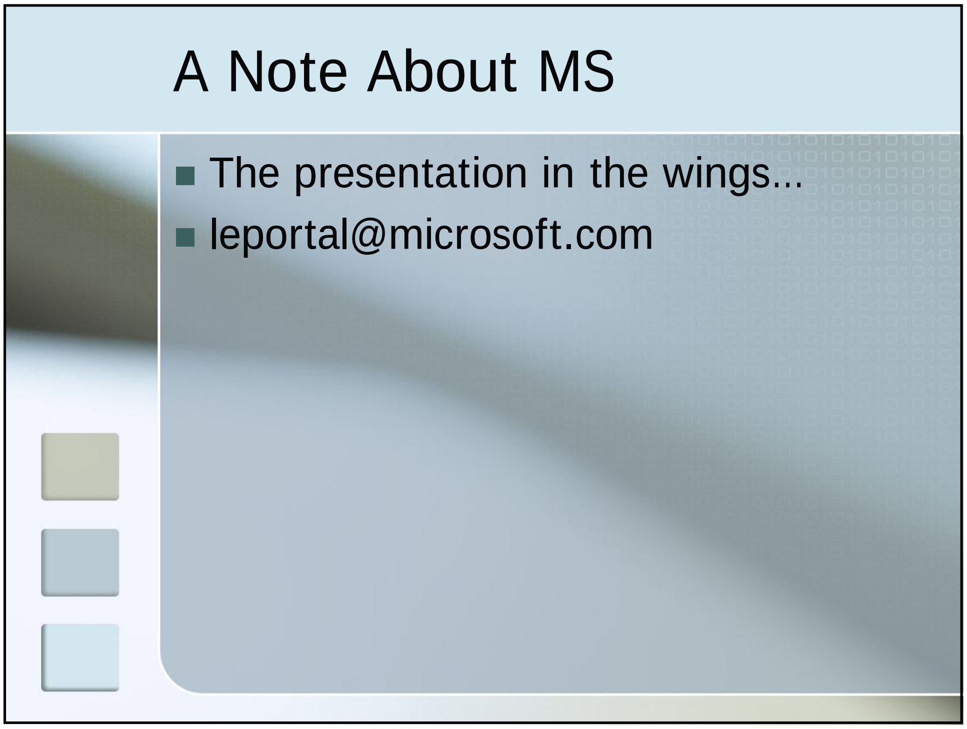


Detection of Data Hiding in Computer Forensics

NEbraskaCERT Conference
August 22nd, 2008
James E. Martin
CISSP, JD

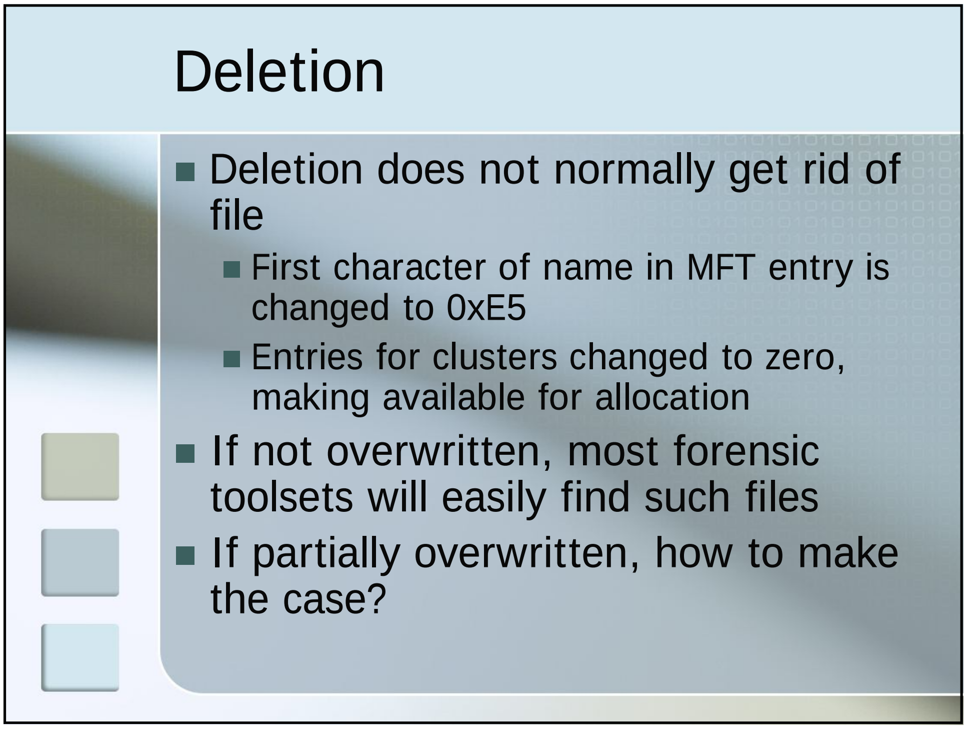
About Your Presenter

- 2008-Present: Security Engineer, West Corporation
- 2004-2008: Senior Forensic Expert for Kaiser Permanente
- 1996-2004: CERT Team Coordinator and Founder for MOREnet
- Email: jericmartin@gmail.com



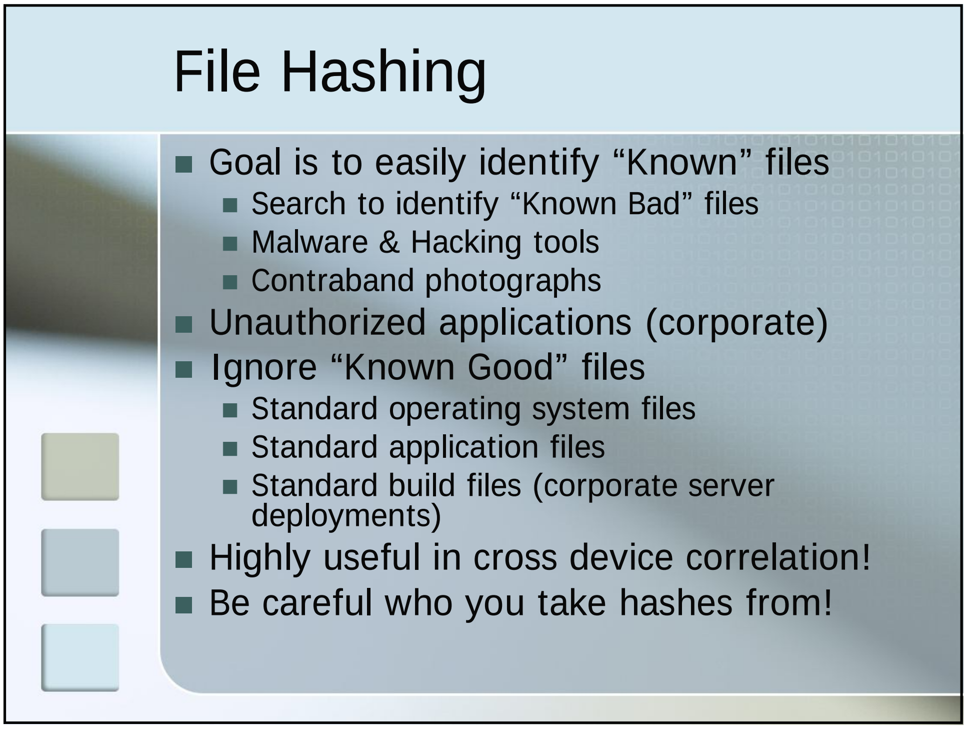
A Note About MS

- The presentation in the wings…
- leportal@microsoft.com



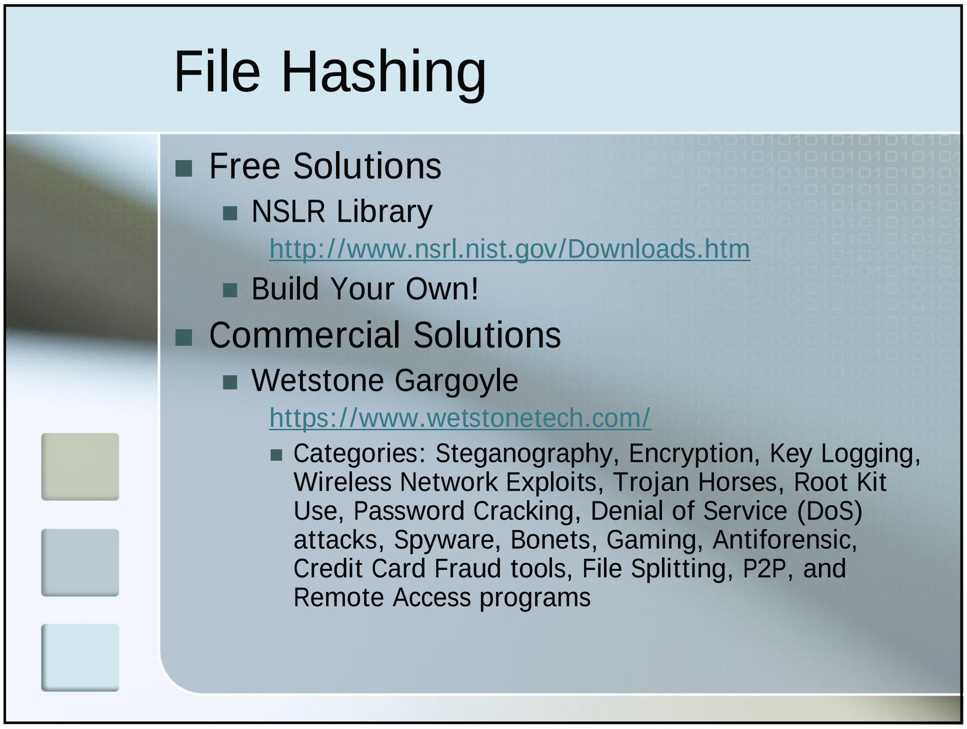
Deletion

- Deletion does not normally get rid of file
  - First character of name in MFT entry is changed to 0xE5
  - Entries for clusters changed to zero, making available for allocation
- If not overwritten, most forensic toolsets will easily find such files
- If partially overwritten, how to make the case?



File Hashing

- Goal is to easily identify “Known” files
  - Search to identify “Known Bad” files
  - Malware & Hacking tools
  - Contraband photographs
- Unauthorized applications (corporate)
- Ignore “Known Good” files
  - Standard operating system files
  - Standard application files
  - Standard build files (corporate server deployments)
- Highly useful in cross device correlation!
- Be careful who you take hashes from!



File Hashing

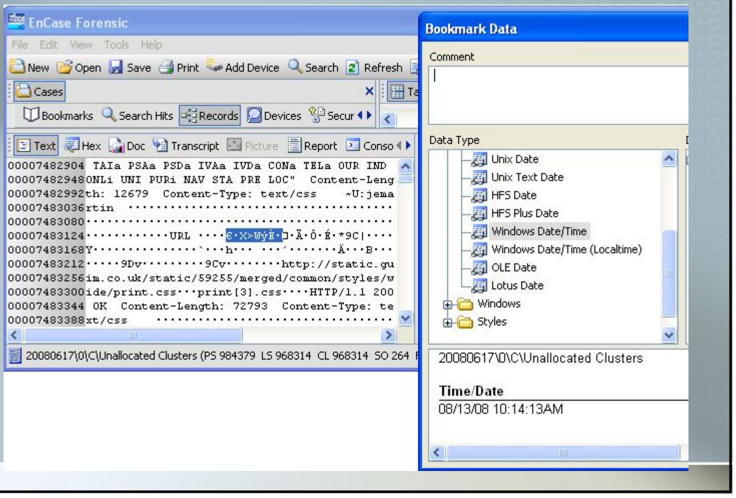
- Free Solutions
  - NSLR Library

    http://www.nsrl.nist.gov/Downloads.htm
  - Build Your Own!
- Commercial Solutions
  - Wetstone Gargoyle

    https://www.wetstonetech.com/
    - Categories: Steganography, Encryption, Key Logging, Wireless Network Exploits, Trojan Horses, Root Kit Use, Password Cracking, Denial of Service (DoS) attacks, Spyware, Bonets, Gaming, Antiforensic, Credit Card Fraud tools, File Splitting, P2P, and Remote Access programs

Deleted IE Index.dat Files

- Records of history can still be found in unallocated, pagefile and hiberfil! Don't trust built in searches.


EnCase Forensic
File Edit View Tools Help
New Open Save Print Add Device Search Refresh
Cases
Bookmarks Search Hits Records Devices Secur
Text Hex Doc Transcript Picture Report Conso
Bookmark Data
Comment
Data Type
Unix Date
Unix Text Date
HFS Date
HFS Plus Date
Windows Date/Time
Windows Date/Time (Localtime)
OLE Date
Lotus Date
Windows
Styles
Time/Date

```
00007482904 TAIa PSAa PSDa IVAa IVDa CONa TELa OUR IND
00007482948ONLi UNI PURi NAV STA PRE LOC"  Content-Leng
00007482992th: 12679  Content-Type: text/css    ~U:jema
00007483036rtin  ·····································
00007483080···········································
00007483124············URL ····Є·X>WýÈ·□·Ã·Ô·É·*9C|····
00007483168Y················`···h··· ···´·······Ä···B···
00007483212·····9Dv·········9Cv········http://static.gu
00007483256im.co.uk/static/59255/merged/common/styles/w
00007483300ide/print.css···print[3].css····HTTP/1.1 200
00007483344 OK  Content-Length: 72793  Content-Type: te
00007483388xt/css   ··································
```

20080617\0\C\Unallocated Clusters (PS 984379 LS 968314 CL 968314 SO 264 F

20080617\0\C\Unallocated Clusters

Time/Date: 08/13/08 10:14:13AM

- Search for URL · · · ·

Deleted/Wiped Mozilla 2.x History

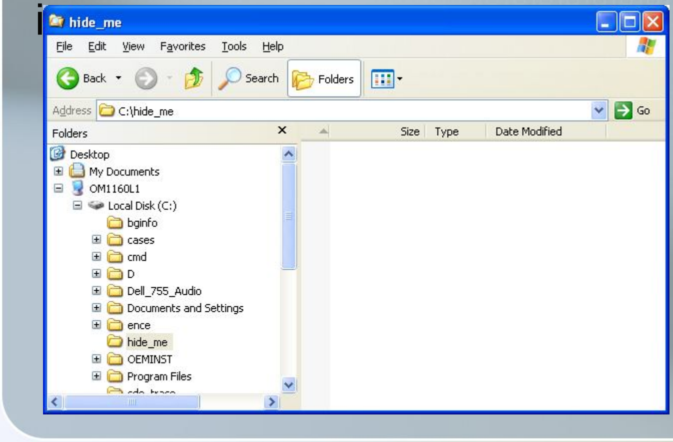
- Search this string to find partial Firefox cache records, including deleted ones: **`http:http`**
  - Records contain HTML headers
  - Contains a time stamp after the URL that appears to be the time of the web server response to the GET or other request.
  - May also contain an expires time stamp which is different). This time comes from the web server.
  - Connect to the interesting web server in a test environment and get a reference time stamp.

Favorite Locations to Hide Interesting Files

- %WINDOWS%, system32
- Internet History
- False Path
- False User Profile
- Recycler, $R
  - No INFO2 or $I records matching!
- False Control Panel Icon

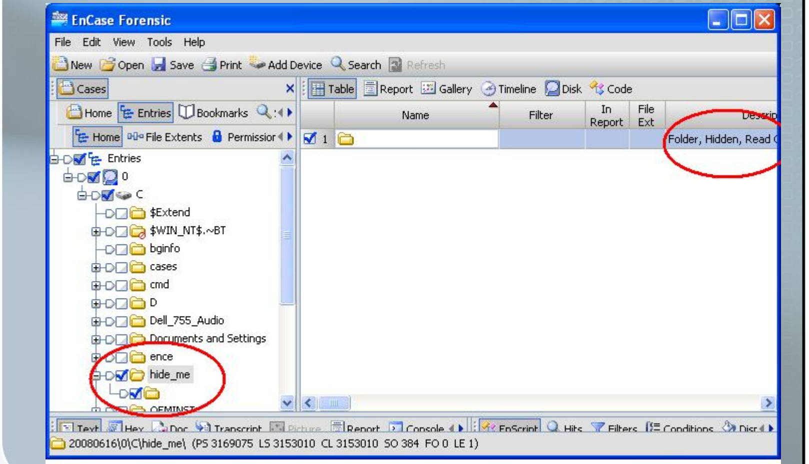
Directories – Alt-0160

- Simple trick of renaming directory with Alt+0160 and replacing folder i



Directories – Alt-0160 Part 2

- Forensic tools like Encase detect this nicely.


EnCase Forensic
File Edit View Tools Help
New Open Save Print Add Device Search Refresh
Cases
Table Report Gallery Timeline Disk Code
Home Entries Bookmarks
Home File Extents Permission
Text Hex Doc Transcript Picture Report Console EnScript Hits Filters Conditions Disc

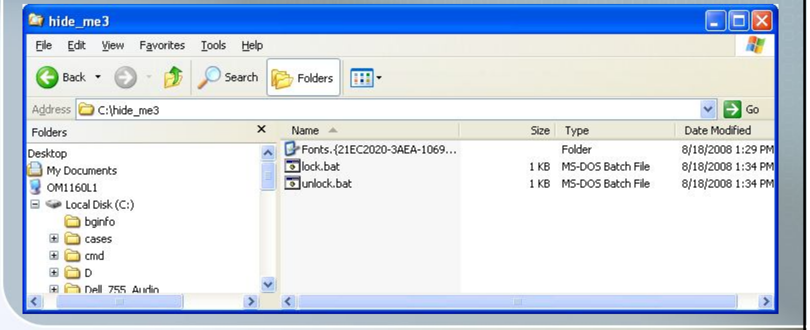
	Name	Filter	In Report	File Ext	Descrip
☑ 1					Folder, Hidden, Read (

```
Entries
  0
    C
      $Extend
      $WIN_NT$.~BT
      bginfo
      cases
      cmd
      D
      Dell_755_Audio
      Documents and Settings
      ence
      hide_me
      OEMINST
```

20080616\0\C\hide_me\ (PS 3169075 LS 3153010 CL 3153010 SO 384 FO 0 LE 1)

Directories – False Control Panel Icon

- When opened in Explorer, leads to Control Panel
- Uses reserved CLSID for Control Panel icon



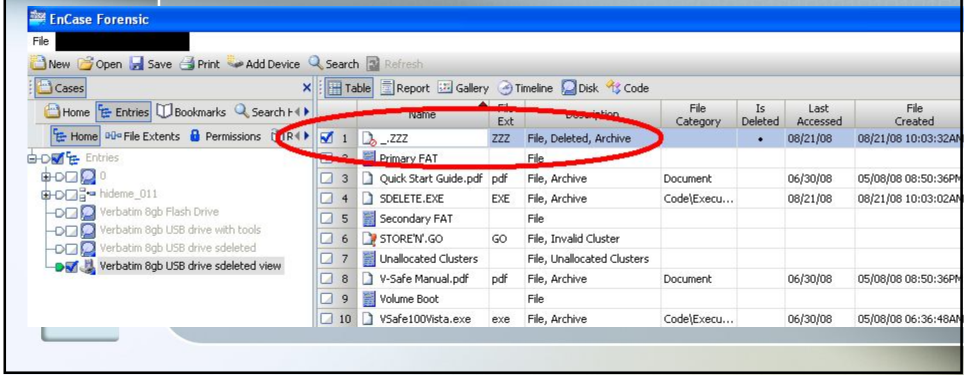
Address C:\hide_me3

```
Desktop
My Documents
OM1160L1
Local Disk (C:)
  bginfo
  cases
  cmd
  D
  Dell_755_Audio
```

Name	Size	Type	Date Modified
Fonts.{21EC2020-3AEA-1069...		Folder	8/18/2008 1:29 PM
lock.bat	1 KB	MS-DOS Batch File	8/18/2008 1:34 PM
unlock.bat	1 KB	MS-DOS Batch File	8/18/2008 1:34 PM

SDELETE

- "Secure" cleaning or wiping tools can also have their own signatures...



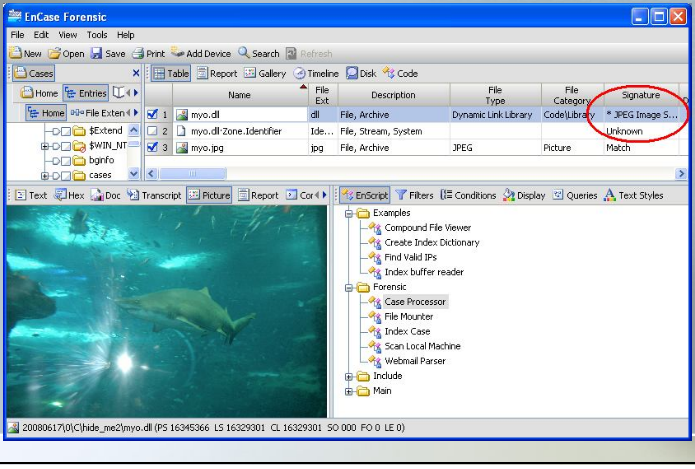
EnCase Forensic

File [redacted]

		Name	File Ext	Description	File Category	Is Deleted	Last Accessed	File Created
☑	1	_.ZZZ	ZZZ	File, Deleted, Archive		•	08/21/08	08/21/08 10:03:32AM
□	2	Primary FAT		File				
□	3	Quick Start Guide.pdf	pdf	File, Archive	Document		06/30/08	05/08/08 08:50:36PM
□	4	SDELETE.EXE	EXE	File, Archive	Code\Execu...		08/21/08	08/21/08 10:03:02AM
□	5	Secondary FAT		File				
□	6	STORE'N'.GO	GO	File, Invalid Cluster				
□	7	Unallocated Clusters		File, Unallocated Clusters				
□	8	V-Safe Manual.pdf	pdf	File, Archive	Document		06/30/08	05/08/08 08:50:36PM
□	9	Volume Boot		File				
□	10	VSafe100Vista.exe	exe	File, Archive	Code\Execu...		06/30/08	05/08/08 06:36:48AM

Files - Renamed

- JPEG File Renamed to *.dll
- Predictable EXIF header so...



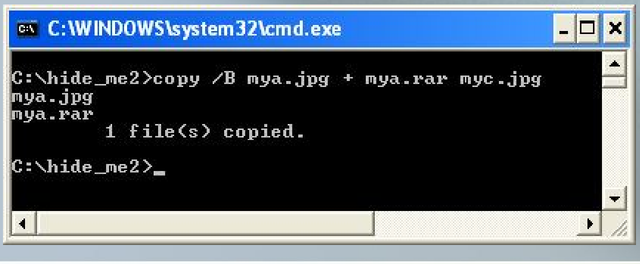
EnCase Forensic

		Name	File Ext	Description	File Type	File Category	Signature
☑	1	myo.dll	dll	File, Archive	Dynamic Link Library	Code\Library	* JPEG Image S...
□	2	myo.dll·Zone.Identifier	Ide...	File, Stream, System			Unknown
☑	3	myo.jpg	jpg	File, Archive	JPEG	Picture	Match

20080617\0\C\hide_me2\myo.dll (PS 16345366 LS 16329301 CL 16329301 SO 000 FO 0 LE 0)

Files – Joined with COPY or CAT

- Double click and open as JPG, but…
- Use “Open With…” and select WinRAR, WinZip or 7Zip as appropriate
- Look at unusual MRUs

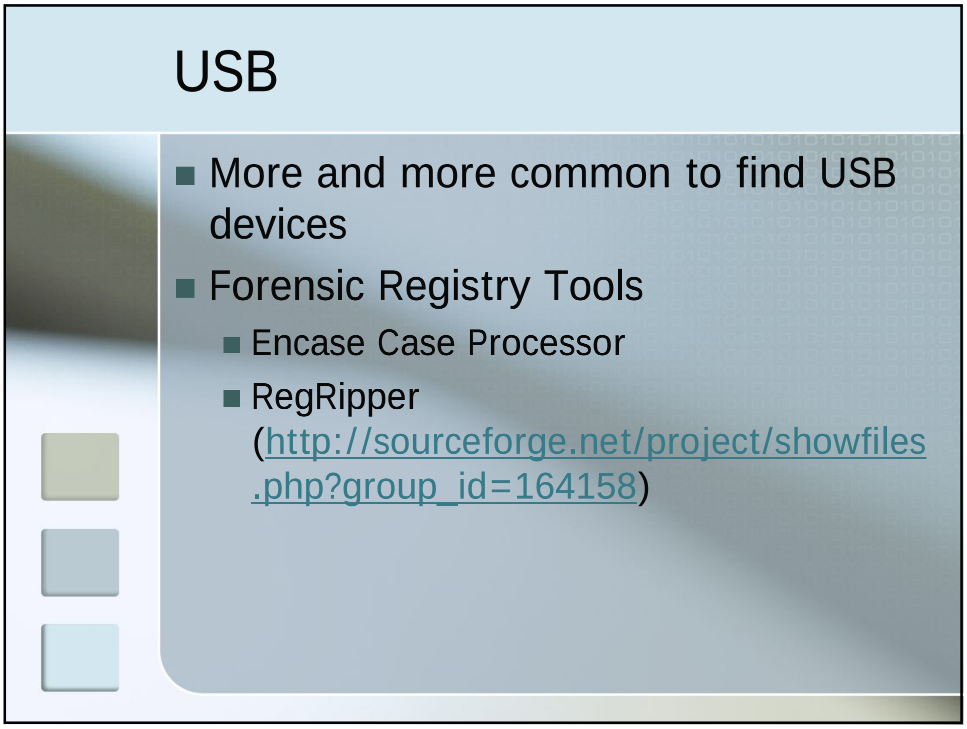


```
C:\hide_me2>copy /B mya.jpg + mya.rar myc.jpg
mya.jpg
mya.rar
        1 file(s) copied.

C:\hide_me2>_
```

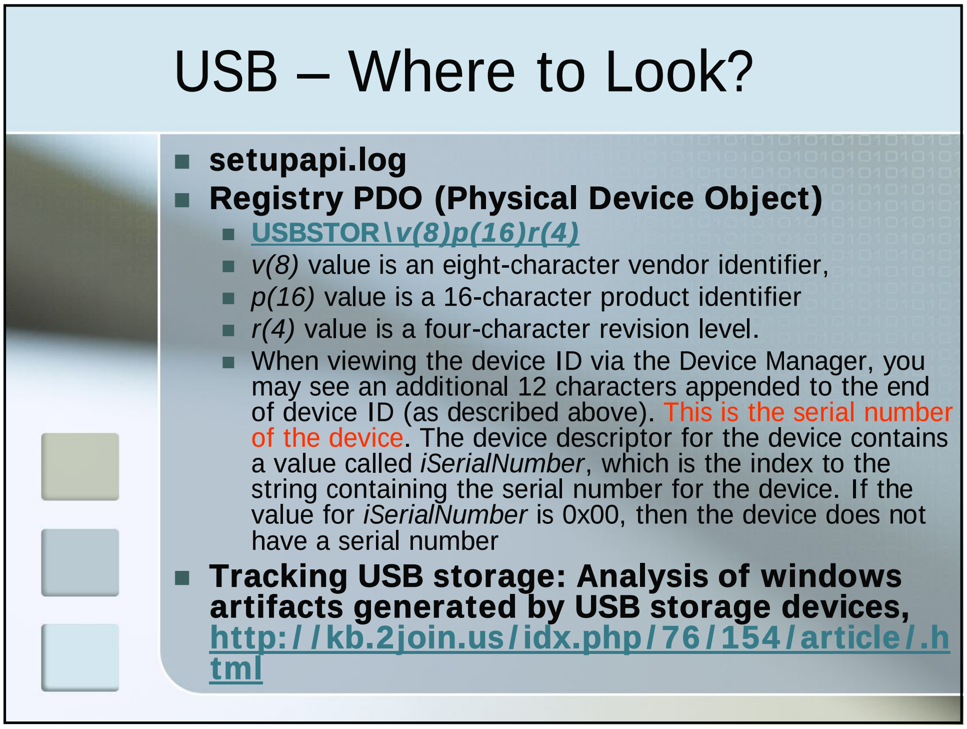
File Renaming

- Renamed extensions
  - Signature Analysis
- Renamed apps
  - Header analysis
  - Hash Analysis



USB

- More and more common to find USB devices
- Forensic Registry Tools
  - Encase Case Processor
  - RegRipper (http://sourceforge.net/project/showfiles.php?group_id=164158)

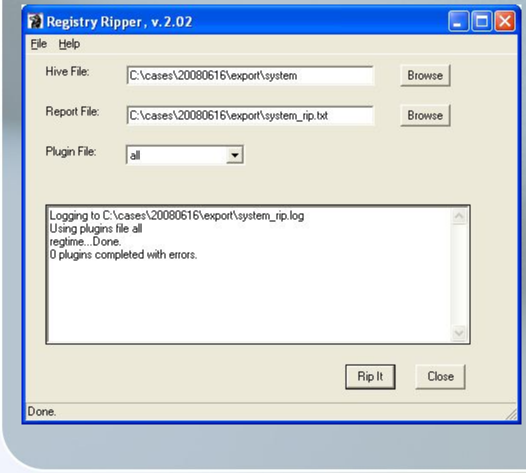


USB – Where to Look?

- **setupapi.log**
- **Registry PDO (Physical Device Object)**
  - **USBSTOR\*v(8)p(16)r(4)***
  - *v(8)* value is an eight-character vendor identifier,
  - *p(16)* value is a 16-character product identifier
  - *r(4)* value is a four-character revision level.
  - When viewing the device ID via the Device Manager, you may see an additional 12 characters appended to the end of device ID (as described above). This is the serial number of the device. The device descriptor for the device contains a value called *iSerialNumber*, which is the index to the string containing the serial number for the device. If the value for *iSerialNumber* is 0x00, then the device does not have a serial number
- **Tracking USB storage: Analysis of windows artifacts generated by USB storage devices, http://kb.2join.us/idx.php/76/154/article/.html**

RegRipper & USB Activity

- Simple to use



Hive File: C:\cases\20080616\export\system

Report File: C:\cases\20080616\export\system_rip.txt

Plugin File: all

```
Logging to C:\cases\20080616\export\system_rip.log
Using plugins file all
regtime...Done.
0 plugins completed with errors.
```

Done.

```
Mon Aug 18 19:29:00 2008Z     \ControlSet001\Control\Network
Mon Aug 18 19:03:27 2008Z     \ControlSet001\Enum\Root
Mon Aug 18 19:03:27 2008Z     \ControlSet001\Enum\Root\LEGACY_APPMGMT
Mon Aug 18 19:03:27 2008Z
      \ControlSet001\Enum\Root\LEGACY_APPMGMT\0000
Mon Aug 18 19:03:27 2008Z     \ControlSet001\Services\AppMgmt
Mon Aug 18 16:06:47 2008Z
Mon Aug 18 15:39:56 2008Z
      \ControlSet001\Enum\Root\LEGACY_STISVC\0000
Mon Aug 18 15:19:00 2008Z
      \ControlSet001\Control\DeviceClasses\{53f56307-b6bf-11d0-94f2-
00a0c91efb8b}\##?#USBSTOR#Disk&Ven_UFD&Prod_USB_Flash_Drive&Rev_1100#AA
04012800000580&0#{53f56307-b6bf-11d0-94f2-00a0c91efb8b}
Mon Aug 18 15:19:00 2008Z
      \ControlSet001\Control\DeviceClasses\{53f56307-b6bf-11d0-94f2-
00a0c91efb8b}\##?#USBSTOR#Disk&Ven_UFD&Prod_USB_Flash_Drive&Rev_1100#AA
04012800000580&0#{53f56307-b6bf-11d0-94f2-00a0c91efb8b}\#
Mon Aug 18 15:19:00 2008Z
      \ControlSet001\Control\DeviceClasses\{53f5630a-b6bf-11d0-94f2-
00a0c91efb8b}\##?#STORAGE#RemovableMedia#7&455bf24&0&RM#{53f5630a-b6bf-
11d0-94f2-00a0c91efb8b}
Mon Aug 18 15:19:00 2008Z
      \ControlSet001\Control\DeviceClasses\{53f5630a-b6bf-11d0-94f2-
00a0c91efb8b}\##?#STORAGE#RemovableMedia#7&455bf24&0&RM#{53f5630a-b6bf-
11d0-94f2-00a0c91efb8b}\#
Mon Aug 18 15:19:00 2008Z
      \ControlSet001\Control\DeviceClasses\{53f5630d-b6bf-11d0-94f2-
00a0c91efb8b}\##?#STORAGE#RemovableMedia#7&455bf24&0&RM#{53f5630d-b6bf-
11d0-94f2-00a0c91efb8b}
Mon Aug 18 15:19:00 2008Z
      \ControlSet001\Control\DeviceClasses\{53f5630d-b6bf-11d0-94f2-
00a0c91efb8b}\##?#STORAGE#RemovableMedia#7&455bf24&0&RM#{53f5630d-b6bf-
11d0-94f2-00a0c91efb8b}\#
Mon Aug 18 15:19:00 2008Z
      \ControlSet001\Control\DeviceClasses\{a5dcbf10-6530-11d2-901f-
00c04fb951ed}\##?#USB#Vid_05dc&Pid_a740#AA04012800000580#{a5dcbf10-
6530-11d2-901f-00c04fb951ed}
Mon Aug 18 15:19:00 2008Z
      \ControlSet001\Control\DeviceClasses\{a5dcbf10-6530-11d2-901f-
00c04fb951ed}\##?#USB#Vid_05dc&Pid_a740#AA04012800000580#{a5dcbf10-
6530-11d2-901f-00c04fb951ed}\#
Mon Aug 18 15:19:00 2008Z
      \ControlSet001\Enum\STORAGE\RemovableMedia\7&455bf24&0&RM
Mon Aug 18 15:19:00 2008Z
      \ControlSet001\Enum\USB\Vid_05dc&Pid_a740\AA04012800000580
Mon Aug 18 15:19:00 2008Z
      \ControlSet001\Enum\USBSTOR\Disk&Ven_UFD&Prod_USB_Flash_Drive&Rev
_1100\AA04012800000580&0
Mon Aug 18 15:19:00 2008Z     \ControlSet001\Services\USBSTOR
Mon Aug 18 14:44:11 2008Z     \ControlSet001\Control\Class\{36FC9E60-
C465-11CF-8056-444553540000}\0025
Mon Aug 18 14:44:11 2008Z
      \ControlSet001\Control\DeviceClasses\{7ab02247-3798-44cd-8472-
243564975f04}
Mon Aug 18 14:44:11 2008Z
      \ControlSet001\Control\DeviceClasses\{7ab02247-3798-44cd-8472-
243564975f04}\##?#USB#Hasp#6&324a3b02&0&00#{7ab02247-3798-44cd-8472-
```

Cleaning Tools

- Are becoming much more popular in recent years, and more are becoming freeware
- None are perfect, most miss some items, create their own footprint, and/or leave traces
- Excellent but dated survey
- Counter-Forensic Privacy Tools: A Forensic Evaluation[2005]: http://reports-archive.adm.cs.cmu.edu/anon/isri2005/CMU-ISRI-05-119.pdf

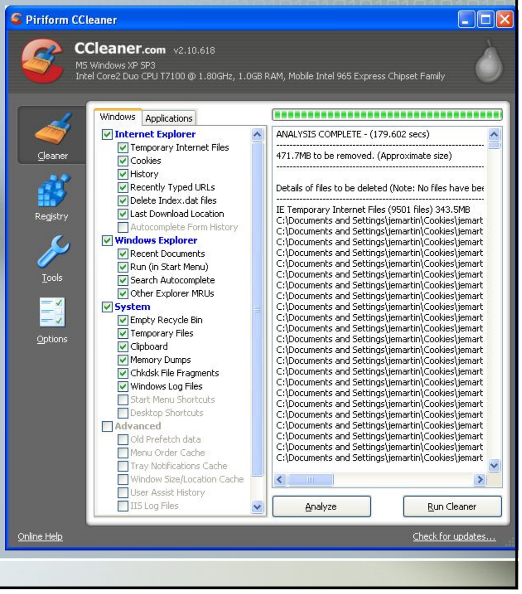
Cleaning Tools 2

- **CCleaner**
  - Got hash?
  - Look (standard and Unicode) in Program Files, Prefetch, Profile, pagefile.sys, hiberfil.sys, unallocated for ccleaner.exe
  - Bring it up in a virtual machine to see the configuration
- **CCleaner as a forensic information source:** http://www.internetrotsyourbrain.com/winapp2/winapp2.zip

```
[*The Cleaner]
LangSecRef=3024
DetectFile=%ProgramFiles%\The Cleaner\cleaner.exe
Default=True
FileKey1=%ProgramFiles%\The Cleaner|logfile.txt
FileKey2=%ProgramFiles%\The Cleaner|moolive.log
FileKey3=%ProgramFiles%\The Cleaner|tca.log
```

Cleaning Tools 3

- Look in places that CCleaner doesn't clean!

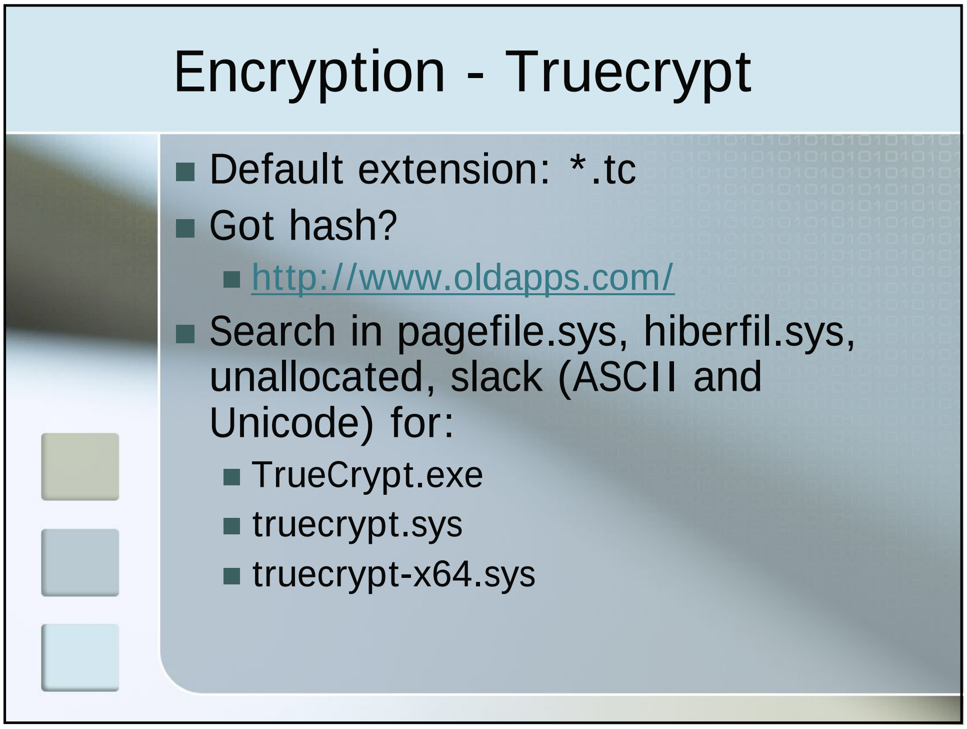


CCleaner.com v2.10.618
MS Windows XP SP3
Intel Core2 Duo CPU T7100 @ 1.80GHz, 1.0GB RAM, Mobile Intel 965 Express Chipset Family

- ☑ **Internet Explorer**
  - ☑ Temporary Internet Files
  - ☑ Cookies
  - ☑ History
  - ☑ Recently Typed URLs
  - ☑ Delete Index.dat files
  - ☑ Last Download Location
  - □ Autocomplete Form History
- ☑ **Windows Explorer**
  - ☑ Recent Documents
  - ☑ Run (in Start Menu)
  - ☑ Search Autocomplete
  - ☑ Other Explorer MRUs
- ☑ **System**
  - ☑ Empty Recycle Bin
  - ☑ Temporary Files
  - ☑ Clipboard
  - ☑ Memory Dumps
  - ☑ Chkdsk File Fragments
  - ☑ Windows Log Files
  - □ Start Menu Shortcuts
  - □ Desktop Shortcuts
- □ **Advanced**
  - □ Old Prefetch data
  - □ Menu Order Cache
  - □ Tray Notifications Cache
  - □ Window Size/Location Cache
  - □ User Assist History
  - □ IIS Log Files

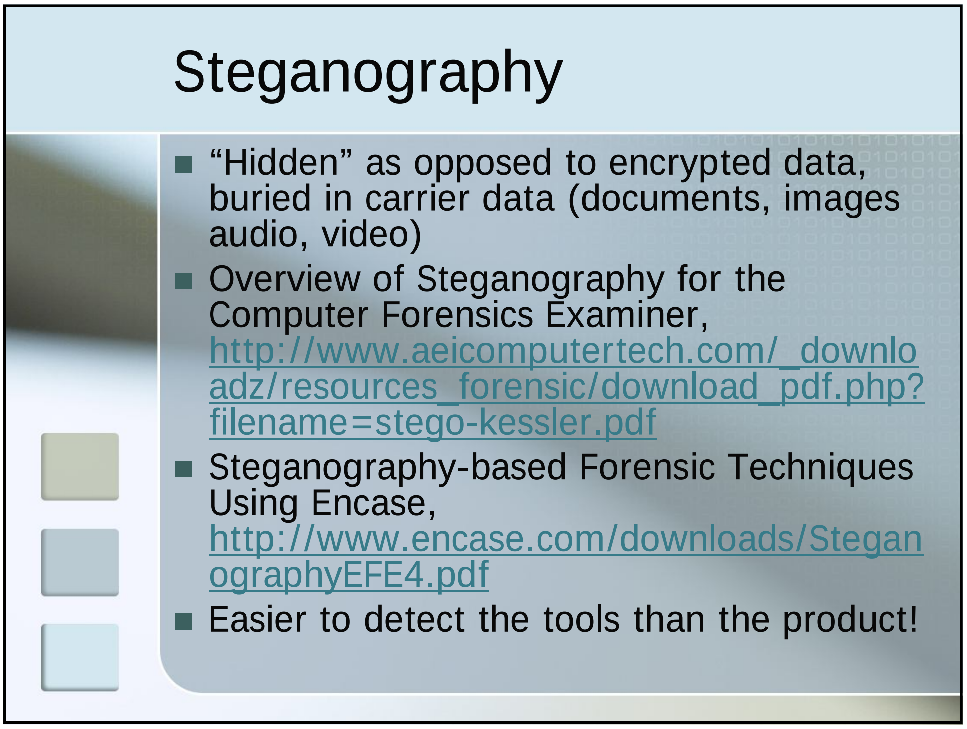
```
ANALYSIS COMPLETE - (179.602 secs)
-----------------------------------------------------------
471.7MB to be removed. (Approximate size)
-----------------------------------------------------------

Details of files to be deleted (Note: No files have bee
-----------------------------------------------------------
IE Temporary Internet Files (9501 files) 343.5MB
C:\Documents and Settings\jemartin\Cookies\jemart
C:\Documents and Settings\jemartin\Cookies\jemart
C:\Documents and Settings\jemartin\Cookies\jemart
C:\Documents and Settings\jemartin\Cookies\jemart
C:\Documents and Settings\jemartin\Cookies\jemart
C:\Documents and Settings\jemartin\Cookies\jemart
C:\Documents and Settings\jemartin\Cookies\jemart
C:\Documents and Settings\jemartin\Cookies\jemart
C:\Documents and Settings\jemartin\Cookies\jemart
C:\Documents and Settings\jemartin\Cookies\jemart
C:\Documents and Settings\jemartin\Cookies\jemart
C:\Documents and Settings\jemartin\Cookies\jemart
C:\Documents and Settings\jemartin\Cookies\jemart
C:\Documents and Settings\jemartin\Cookies\jemart
C:\Documents and Settings\jemartin\Cookies\jemart
C:\Documents and Settings\jemartin\Cookies\jemart
C:\Documents and Settings\jemartin\Cookies\jemart
C:\Documents and Settings\jemartin\Cookies\jemart
C:\Documents and Settings\jemartin\Cookies\jemart
C:\Documents and Settings\jemartin\Cookies\jemart
C:\Documents and Settings\jemartin\Cookies\jemart
C:\Documents and Settings\jemartin\Cookies\jemart
C:\Documents and Settings\jemartin\Cookies\jemart
```



Encryption - Truecrypt

- Default extension: *.tc
- Got hash?
  - http://www.oldapps.com/
- Search in pagefile.sys, hiberfil.sys, unallocated, slack (ASCII and Unicode) for:
  - TrueCrypt.exe
  - truecrypt.sys
  - truecrypt-x64.sys

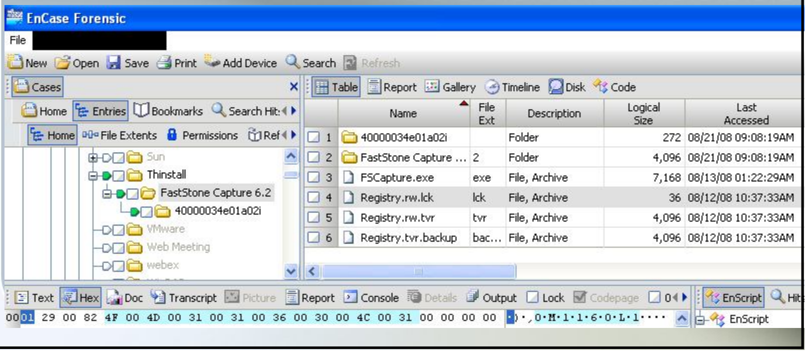


Steganography

- “Hidden” as opposed to encrypted data, buried in carrier data (documents, images audio, video)
- Overview of Steganography for the Computer Forensics Examiner, http://www.aeicomputertech.com/_downloadz/resources_forensic/download_pdf.php?filename=stego-kessler.pdf
- Steganography-based Forensic Techniques Using Encase, http://www.encase.com/downloads/SteganographyEFE4.pdf
- Easier to detect the tools than the product!

Thinstall/ThinApp

- Virtualized application, runs inside own memory space
- So far…no Registry entries found, but Prefetch and the following directory structure under \Documents and Settings\%profile%\Application Data\Thinstall\



[redacted]

	Name	File Ext	Description	Logical Size	Last Accessed
☐ 1	40000034e01a02i		Folder	272	08/21/08 09:08:19AM
☐ 2	FastStone Capture …	2	Folder	4,096	08/21/08 09:08:19AM
☐ 3	FSCapture.exe	exe	File, Archive	7,168	08/13/08 01:22:29AM
☐ 4	Registry.rw.lck	lck	File, Archive	36	08/12/08 10:37:33AM
☐ 5	Registry.rw.tvr	tvr	File, Archive	4,096	08/12/08 10:37:33AM
☐ 6	Registry.tvr.backup	bac…	File, Archive	4,096	08/12/08 10:37:33AM

```
0001 29 00 82 4F 00 4D 00 31 00 31 00 36 00 30 00 4C 00 31 00 00 00 00  ·)·,O·M·1·1·6·0·L·1····
```

Additional Light Reading

- Anti Forensics: making computer forensics hard, http://ws.hackaholic.org/slides/AntiForensics-CodeBreakers2006-Translation-To-English.pdf