

# Anti-Forensics 101



(ekoparty security conference)

Nov. 30 - Dic. 1

Buenos Aires, Argentina

# quien soy ?

- Leonardo Pigñer
- Organizador ekoparty
- Senior Security Specialist en ETEK
- EnCE “EnCase Certified Examiner”
- [KungFooSion.blogspot.com](http://KungFooSion.blogspot.com)

# temario

- Introducción
- Cifrado
- Destrucción
- Ocultamiento
  - Esteganografía
  - ADS “Alternate Data Stream”
- MAFIA
  - Slacker
  - Timestomp
  - Transmogrify
  - SAM Juicer

**cifrado**

# los problemas

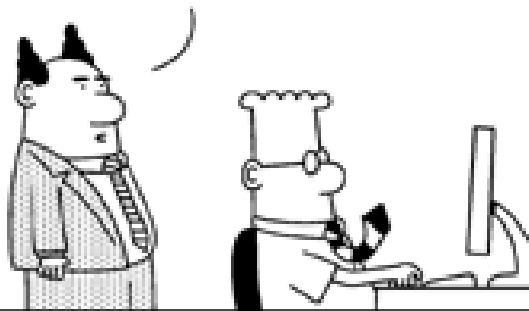
- Usada correctamente impediría acceder a la información de un sospechoso.
- Gran cantidad de avances en esta área.
- Se pueden cifrar e-mails, archivos, volúmenes, discos rígidos...
- Herramientas gratuitas de gran calidad:
  - TrueCrypt, GnuPG
- Varios niveles de “*Negación Plausible*”.

# negación plausible

“la existencia de un archivo o mensaje cifrado es negable en el sentido de que un adversario no puede probar que existe.”

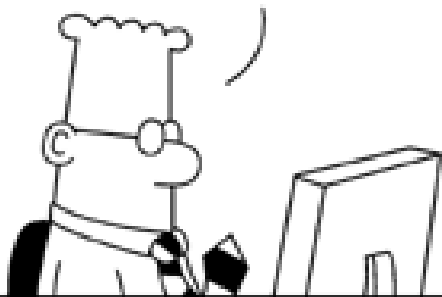
**La Fase Dos no es de tu incumbencia...**

I NEED YOU TO DELETE ALL OF OUR INCRIMINATING E-MAILS BEFORE THE COURT SEES THEM.



www.dilbert.com  
scottadams@aol.com

THAT PLAN IS NO GOOD BECAUSE I'D BE A WITNESS TO THE CRIME... UNLESS YOU HAD ME KILLED.

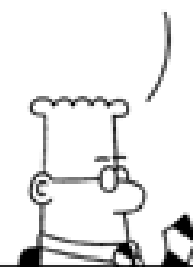


10-19-05 © 2005 Scott Adams, Inc./Dist. by UFS, Inc.

PHASE TWO IS NONE OF YOUR CONCERN.



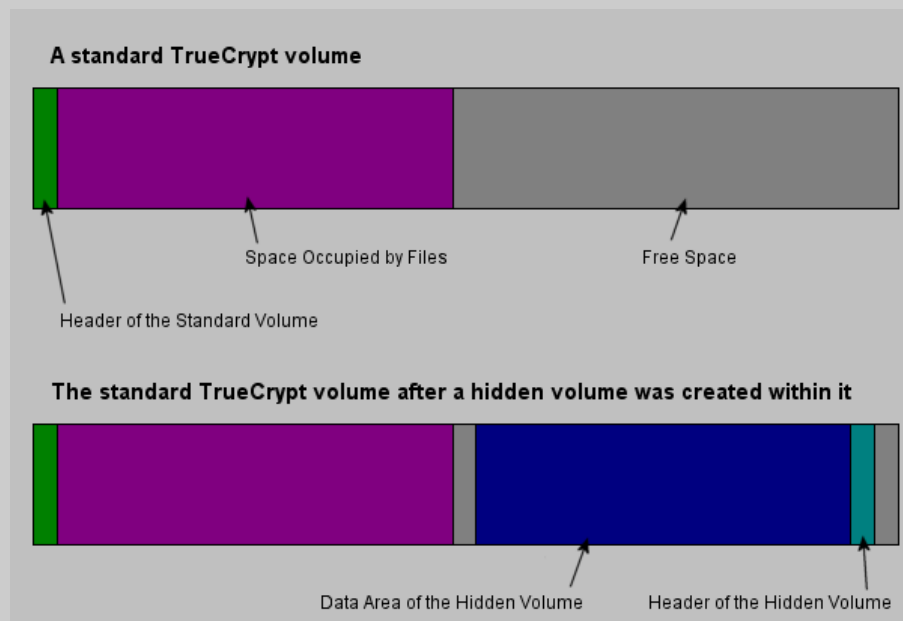
IT HAS A PHASE???



# TrueCrypt

## Posee varios niveles de Negación Plausible:

- Se puede crear un volumen cifrado estándar y dentro de este un volumen oculto.
- Un adversario nos podría forzar a entregar el Password.
- No hay forma de probar que dentro del volumen estándar existe un volumen oculto ya que asemeja ser datos al azar.



# otras características

- Algoritmos de cifrado: AES-256, Serpent y Twofish.
- Modo LRW que elimina la posibilidad de detección de datos que no sean al azar.
- No guarda datos en la *Registry*.
- Puede utilizar un archivo como password en vez de un “password”.

# muy popular

**Descargas Total: 3.674.6**  
**Descargas Ayer: 6135**



[www.truecrypt.org](http://www.truecrypt.org)

# herramientas

Otras herramientas de cifrado “*on the fly*”:

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

**destrucción**

# wiping

“En computación, *“shredding”* o *“wiping”* es el acto de borrar un archivo de forma segura, de manera que no sea posible restaurarlo de ninguna manera.”

<http://en.wikipedia.org/wiki/Shredding>

# métodos de borrado

Metodo	Nivel de Seguridad	Pasadas	Detalles
Quick Erase	Bajo	1	Zeros
RCMP TSSIT OPS-II	Medio	8	Alternating byte write
DoD short	Medio	3	3 phases of Dod 5220
DoD 5220-22.M	Medio	7	Random chars + streams
Gutmann Wipe	Alto	35	Static data + random datastream
PRNG Stream	Medio-Alto	8	Use of Pseudo Random Number Generator (PRNG)

# herramientas

- Eraser
  - Windows, <http://www.heidi.ie/eraser/>
- SDelete
  - Windows, <http://www.microsoft.com/latam/technet/sysinternals/Security/SDelete.mspix>
- The Defiler's Toolkit
  - Linux, [http://www.totse.com/en/hack/hack\\_attack/167627.html](http://www.totse.com/en/hack/hack_attack/167627.html)
- Srm
  - \*nix, <http://srm.sourceforge.net/>
- Darik's Boot and Nuke (dban)
  - Disco Rigido, <http://dban.sourceforge.net/>

**esteganografía**

# que es ?

“La esteganografía es la rama de la criptología que trata sobre la ocultación de mensajes, para evitar que se perciba la existencia del mismo.”

<http://es.wikipedia.org/wiki/Esteganografía>



original



extraída

# 11/09/2001

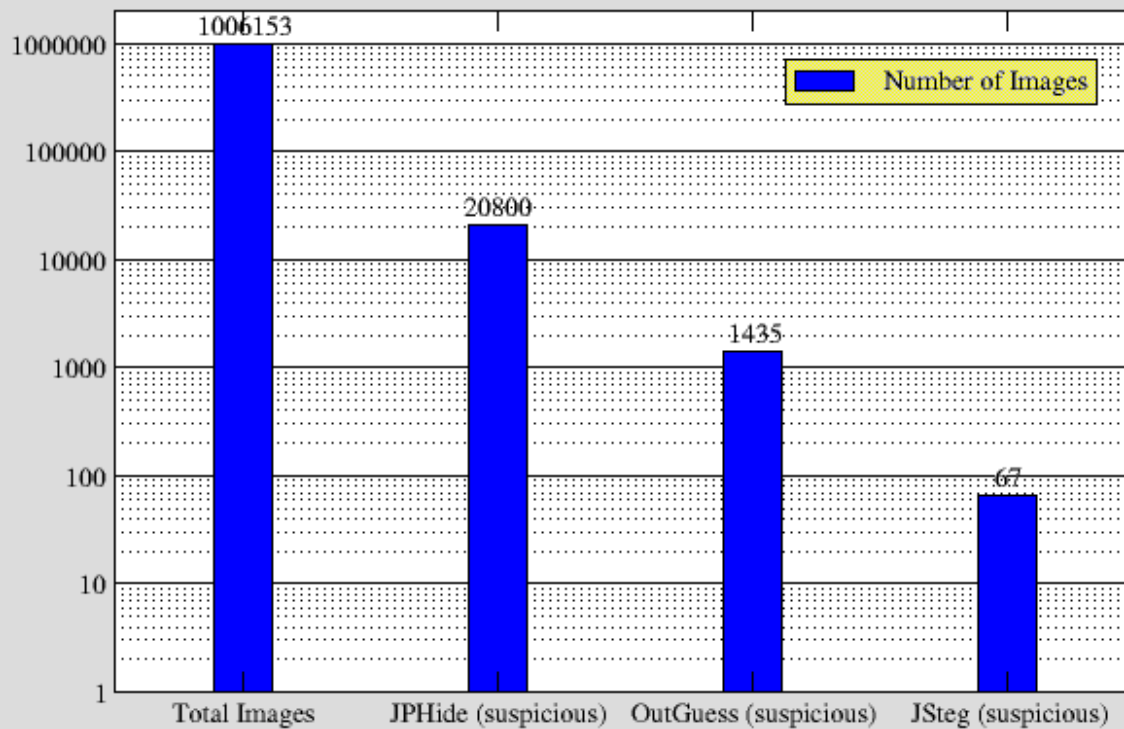
“U.S. officials say Osama bin Laden is posting instructions for terrorist activities on sports chat rooms, pornographic bulletin boards and other Web sites.”

USA TODAY (<http://www.usatoday.com/tech/news/2001-02-05-binladen.htm>)



# Scan of the USENET

## USENET Steganography Scan



**Scan of the USENET for steganography**

<http://niels.xtdnet.nl/stego/usenet.php>

# Scan of the USENET

- Se procesaron un millón de imágenes con *stegdetect* de las cuales 20.000 resultaron sospechosas.
- Se lanzó un ataque de diccionario sobre las imágenes en las que se detectó *Jsteg* y *JPHide*.
- El diccionario tenía 1.800.000 palabras.
- No se encontró ningún mensaje oculto.

# Universidad de Purdue

- Reciente estudio sobre el uso de esteganografía:

## Research Shows Image-Based Threat on the Rise

**New Purdue University research shows steganography, long considered a minor threat, may be on the rise**

OCTOBER 18, 2007 | 6:00 PM

**By Kelly Jackson Higgins**  
Senior Editor, *Dark Reading*

Until recently, steganography, the stealth technique of hiding text or images within image files, has mostly been considered too complex – and conspicuous – to be much of a threat. But some forensics experts now worry that the bad guys are starting to use the tactic more frequently, especially in child pornography and identity theft trafficking.

[http://www.darkreading.com/document.asp?doc\\_id=136702&WT.svl=news1\\_1](http://www.darkreading.com/document.asp?doc_id=136702&WT.svl=news1_1)

# Universidad de Purdue

- Buscaron en 1.000.000 de imágenes en Internet utilizando 25 firmas de herramientas.
- Mas de 800 herramientas disponibles.
- Cambiaron el foco de la investigación en comprobar si los criminales están usando esteganografía.
- Encontraron herramientas instaladas en las computadoras de criminales que han sido encarcelados.
- Se esta utilizando en pornografía infantil y fraudes financieros.

# herramientas

- OutGuess
- JPHide
- Jsteg
- S-Tools

La Web [Imágenes](#) [Grupos](#) [Noticias](#) [Más »](#)

steganography tools

Buscar con Google | Voy a tener suerte

Buscar en:  la Web  páginas en español  páginas de Argentina

**ADS**

**“Alternate Data Stream”**

# que es ?

- Característica única de NTFS.
  - Introducido en Windows NT 3.1 en los comienzos de 1990.
  - Creado para proveer compatibilidad entre los servidores Windows NT y los clientes Macintosh que usan HFS “Hierarchical File System”.
- No se puede visualizar desde Windows Explorer.
- No afecta el tamaño de los archivos.

# como funciona ?

- En NTFS el MFT puede tener mas de un atributo \$DATA.
  - El atributo \$DATA adicional es el “*Alternate Data Stream*”.
  - La mayoría de los programas solo leen el primer atributo \$DATA.
- El tamaño de la información oculta solo depende del tamaño del disco.
- Si el archivo original crece, la información oculta puede ser sobrescrita.
- También es posible usar directorios.

# ejemplos

## Ocultar información:

```
C:\ type archivo-oculto.txt > archivo-normal.txt:archivo-oculto.txt
```

```
C:\ notepad archivo-normal.txt:archivo-oculto.txt
```

## Ocultar un programa:

```
C:\ type rootkit.exe > notepad.exe:rootkit.exe
```

```
C:\ start .\notepad.exe:rootkit.exe
```

**ADS demo!**

**mafia**









## **“MAFIA”**

### **Metasploit Anti-Forensic Investigation Arsenal**

Slacker - Timestomp - SAM Juicer - Transmogrify

<http://www.metasploit.com/projects/antiforensics/>

**mafia : slacker**

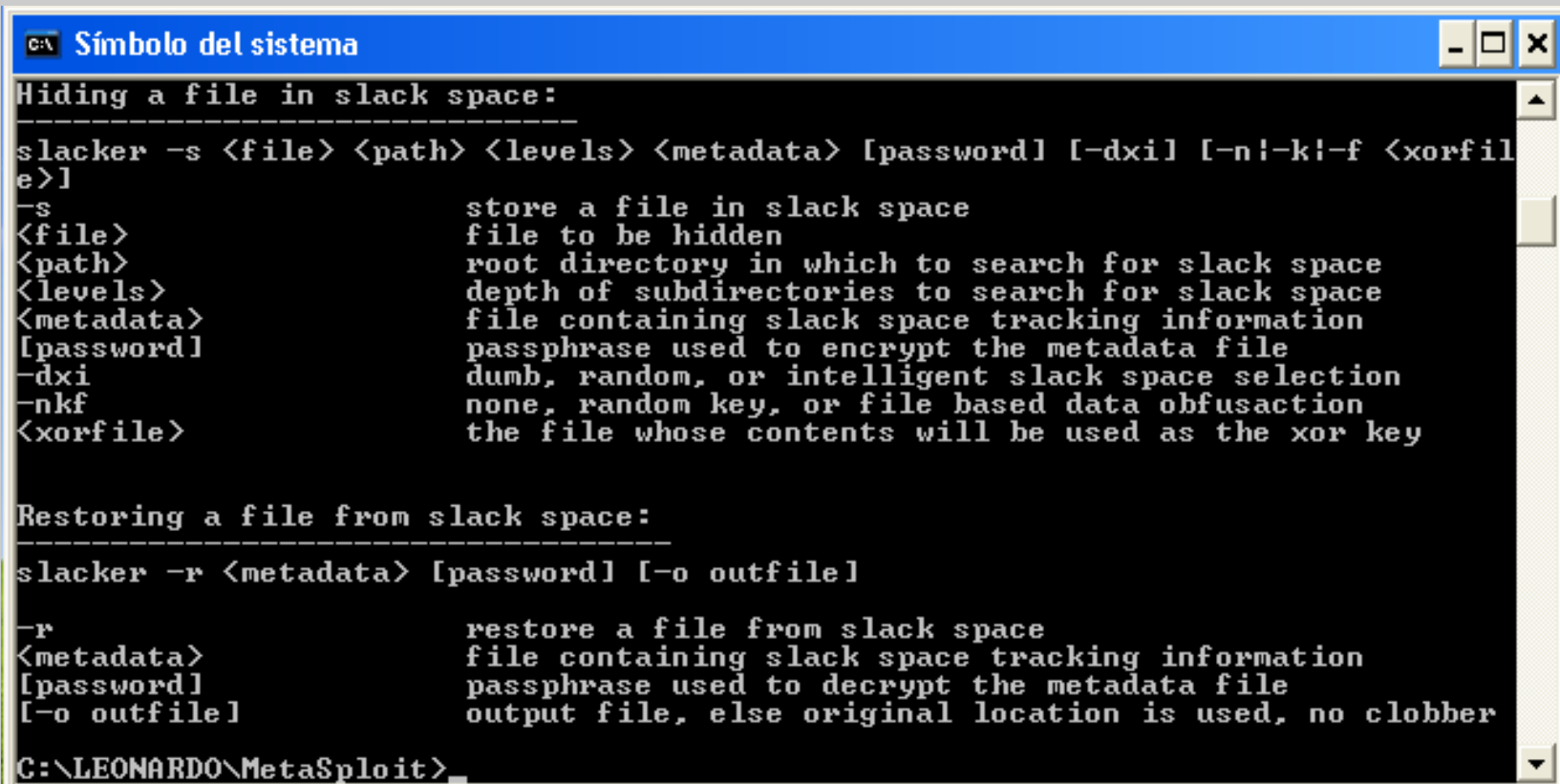
# que es el slack ?

- File Slack, es el espacio que hay entre el final de un archivo lógico y el final del cluster.
- 1 cluster = 8 sectores
  - 1 sector = 512 bytes / 1 cluster = 4096 bytes
- Si escribimos 513 bytes debemos utilizar 2 sectores.

- 
- Tambien podemos encontrar RAM Slack o Sector Slack

# que hace slacker ?

- Oculta información en el espacio de Slack de los archivos en NTFS.



```
C:\> Símbolo del sistema
Hiding a file in slack space:
-----
slacker -s <file> <path> <levels> <metadata> [password] [-dxi] [-nkf <xorfile>]
-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 obfuscation
<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:\LEONARDO\MetaSploit>
```

# slacker











- Puede seleccionar el espacio de Slacka utilizar.
  - Dumb: primeros X archivos.
  - Random: selección de archivos al azar.
  - Safe: selecciona los archivos mas viejos.
- Ofuscación.
  - none: no realiza ofuscación.
  - XOR key: llave de 8 bits al azar.
  - One-time pad: usa un archivo de tamaño fijo.

# que se puede hacer ?

- Wiping periódico de la zona de slack.
  - Eraser
- Realizar estudios estadísticos en busca de patrones anómalos en la zona de slack.
- Algunas herramientas forenses pueden detectar a slacker.
  - EnScript de Tim Mullen  
([http://www.lancemueller.com/blog/Detect\\_Slacker.EnPack](http://www.lancemueller.com/blog/Detect_Slacker.EnPack))

**mafia : timestomp**











# ACME

	Name	Last Accessed	File Created	Last Written	Entry Modified
<input type="checkbox"/> 1	 EDISC_WALLPAPER.bmp	11/20/07 03:11:26p.m.	04/16/07 08:28:49p.m.	10/18/05 03:47:30p.m.	04/19/07 10:13:13a.m.
<input type="checkbox"/> 2	 eesac.bmp	11/20/07 03:11:26p.m.	04/16/07 08:28:49p.m.	10/11/05 10:56:00a.m.	04/19/07 10:13:13a.m.
<input type="checkbox"/> 3	 dyods21024x768.jpg	11/20/07 03:11:26p.m.	04/16/07 08:28:49p.m.	06/18/06 07:48:06p.m.	04/19/07 10:13:13a.m.
<input type="checkbox"/> 4	 cwallPDT.jpg	11/20/07 03:11:26p.m.	04/16/07 08:28:49p.m.	06/18/06 07:47:22p.m.	04/19/07 10:13:13a.m.
<input type="checkbox"/> 5	 bdyd1024x768.jpg	11/20/07 03:11:26p.m.	04/16/07 08:28:49p.m.	05/20/06 12:33:12p.m.	04/19/07 10:13:13a.m.
<input type="checkbox"/> 6	 a1wallGSI-2.jpg	11/20/07 03:11:26p.m.	04/16/07 08:28:49p.m.	04/25/06 02:27:50p.m.	04/19/07 10:13:13a.m.
<input type="checkbox"/> 7	 GMakingItHarder.jpg	11/20/07 03:11:27p.m.	04/16/07 08:28:49p.m.	04/25/06 02:28:08p.m.	04/19/07 10:13:13a.m.
<input type="checkbox"/> 8	 HwallGSI-1.jpg	11/20/07 03:11:27p.m.	04/16/07 08:28:49p.m.	06/18/06 07:47:48p.m.	04/19/07 10:13:13a.m.
<input type="checkbox"/> 9	 Imissioncapable.jpg	11/20/07 03:11:27p.m.	04/16/07 08:28:49p.m.	04/25/06 02:15:06p.m.	04/19/07 10:13:13a.m.
<input type="checkbox"/> 10	 Jwall-GSI.jpg	11/20/07 03:11:27p.m.	04/16/07 08:28:49p.m.	06/18/06 07:47:38p.m.	04/19/07 10:13:13a.m.

**Accessed, Created, Modified, Entry  
modified**











# timestamp trabajando

- -z “Monday 12/31/2005 01:01:01 AM”

	Name	Last Accessed	File Created	Last Written	Entry Modified
<input type="checkbox"/> 1	 EDISC_WALLPAPER.bmp	11/20/07 03:11:26p.m.	04/16/07 08:28:49p.m.	10/18/05 03:47:30p.m.	04/19/07 10:13:13a.m.
<input type="checkbox"/> 2	 eesac.bmp	11/20/07 03:11:26p.m.	04/16/07 08:28:49p.m.	10/11/05 10:56:00a.m.	04/19/07 10:13:13a.m.
<input type="checkbox"/> 3	 dyods21024x768.jpg	11/20/07 03:11:26p.m.	04/16/07 08:28:49p.m.	06/18/06 07:48:06p.m.	04/19/07 10:13:13a.m.
<input type="checkbox"/> 4	 cwallPDT.jpg	11/20/07 03:11:26p.m.	04/16/07 08:28:49p.m.	06/18/06 07:47:22p.m.	04/19/07 10:13:13a.m.
<input type="checkbox"/> 5	 bdyd1024x768.jpg	11/20/07 03:11:26p.m.	04/16/07 08:28:49p.m.	05/20/06 12:33:12p.m.	04/19/07 10:13:13a.m.
<input type="checkbox"/> 6	 a1wallGSI-2.jpg	11/20/07 03:11:26p.m.	04/16/07 08:28:49p.m.	04/25/06 02:27:50p.m.	04/19/07 10:13:13a.m.
<input type="checkbox"/> 7	 GMakingItHarder.jpg	11/20/07 03:11:27p.m.	04/16/07 08:28:49p.m.	04/25/06 02:28:08p.m.	04/19/07 10:13:13a.m.
<input type="checkbox"/> 8	 HwallGSI-1.jpg	11/20/07 03:11:27p.m.	04/16/07 08:28:49p.m.	06/18/06 07:47:48p.m.	04/19/07 10:13:13a.m.
<input type="checkbox"/> 9	 Imissioncapable.jpg	12/31/05 01:01:01a.m.	12/31/05 01:01:01a.m.	12/31/05 01:01:01a.m.	12/31/05 01:01:01a.m.
<input type="checkbox"/> 10	 Jwall-GSI.jpg	11/20/07 03:11:27p.m.	04/16/07 08:28:49p.m.	06/18/06 07:47:38p.m.	04/19/07 10:13:13a.m.

# timestamp trabajando

- -b (debilidad en EnCase y otros)

	Name	Last Accessed	File Created	Last Written	Entry Modified
<input type="checkbox"/> 1	 EDISC_WALLPAPER.bmp	11/20/07 03:11:26p.m.	04/16/07 08:28:49p.m.	10/18/05 03:47:30p.m.	04/19/07 10:13:13a.m.
<input type="checkbox"/> 2	 eesac.bmp	11/20/07 03:11:26p.m.	04/16/07 08:28:49p.m.	10/11/05 10:56:00a.m.	04/19/07 10:13:13a.m.
<input type="checkbox"/> 3	 dyods21024x768.jpg	11/20/07 03:11:26p.m.	04/16/07 08:28:49p.m.	06/18/06 07:48:06p.m.	04/19/07 10:13:13a.m.
<input type="checkbox"/> 4	 cwallPDT.jpg	11/20/07 03:11:26p.m.	04/16/07 08:28:49p.m.	06/18/06 07:47:22p.m.	04/19/07 10:13:13a.m.
<input type="checkbox"/> 5	 bdyd1024x768.jpg	11/20/07 03:11:26p.m.	04/16/07 08:28:49p.m.	05/20/06 12:33:12p.m.	04/19/07 10:13:13a.m.
<input type="checkbox"/> 6	 a1wallGSI-2.jpg	11/20/07 03:11:26p.m.	04/16/07 08:28:49p.m.	04/25/06 02:27:50p.m.	04/19/07 10:13:13a.m.
<input type="checkbox"/> 7	 GMakingItHarder.jpg	11/20/07 03:11:27p.m.	04/16/07 08:28:49p.m.	04/25/06 02:28:08p.m.	04/19/07 10:13:13a.m.
<input type="checkbox"/> 8	 HwallGSI-1.jpg	11/20/07 03:11:27p.m.	04/16/07 08:28:49p.m.	06/18/06 07:47:48p.m.	04/19/07 10:13:13a.m.
<input type="checkbox"/> 9	 Imissioncapable.jpg				
<input type="checkbox"/> 10	 Jwall-GSI.jpg	11/20/07 03:11:27p.m.	04/16/07 08:28:49p.m.	06/18/06 07:47:38p.m.	04/19/07 10:13:13a.m.

# **Windows Explorer demo!**

**mafia : SAM Juicer**

# que hace ?

- Lo mismo que *pwdump* pero sin tocar el disco.
  - Pwdump abre un share, tira ejecutables en el disco y arranca un servicio para inyectarse a si mismo en LSSAS.
- Rehúsa el mismo canal de transporte que MetaSploit.
- Se inyecta a si mismo directamente en LSSAS y obtiene los passwords cifrados sin dejar archivos, tocar la registry o arrancar un servicio.
  - Al no usar archivos o servicios las soluciones basadas en firmas no lo pueden detectar.

# que se puede hacer ?

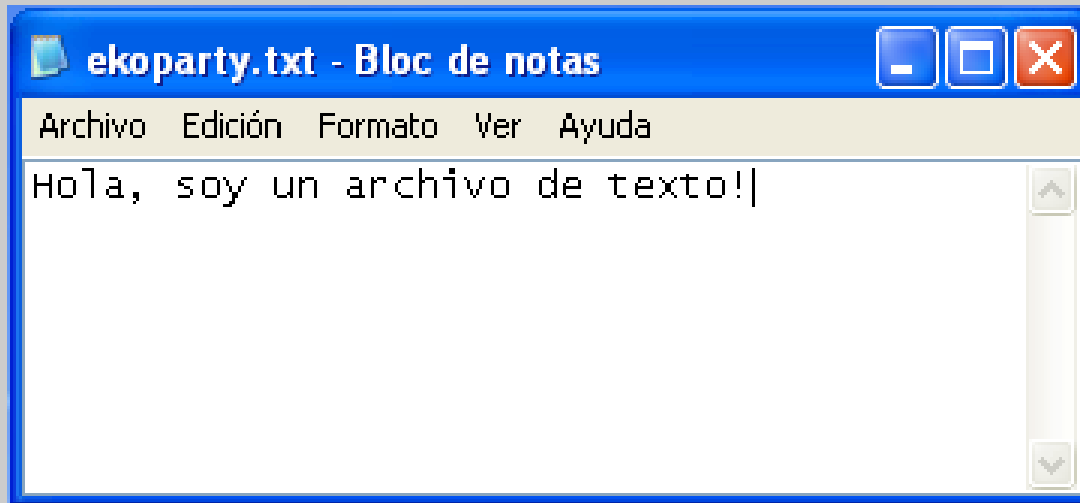
- Muchas herramientas forenses pueden capturar los procesos corriendo, puertos abiertos, conexiones activas, etc.
- SAM Juicer no abre otros canales de conexión ni corre nuevos servicios.
- Una posibilidad es leer la memoria para detectarlo.

**mafia : transmogrify**

# File Carving

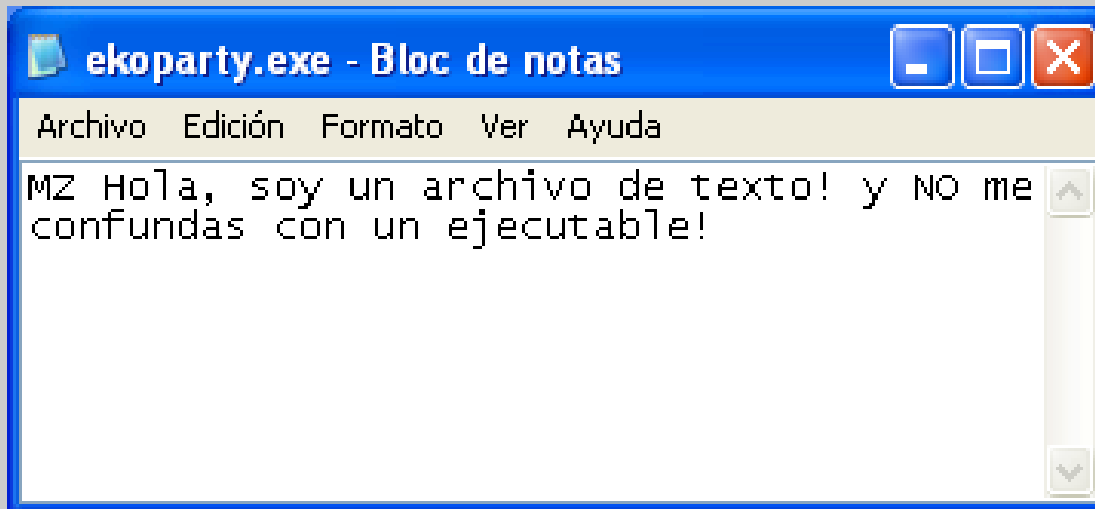
- Uno de los grandes problemas del análisis forense.
- Windows solo usa la extensión del archivo para identificar su formato.
- Las herramientas forenses también analizan los “headers” de los archivos.


# detección



	Name	File Ext	File Category	File Type
 1	 ekoparty.txt	txt	Document	Text

# evasión



	Name	File Ext	File Category	File Type
<input type="checkbox"/> 1	 ekoparty.exe	exe	Code\Executable	Windows Executable

# **transmoglify**

- Va a automatizar el cambio de headers y extensión de los archivos para poder ocultar información.
- Coming Soon (?)



**preguntas ?**

**Gracias!!!**