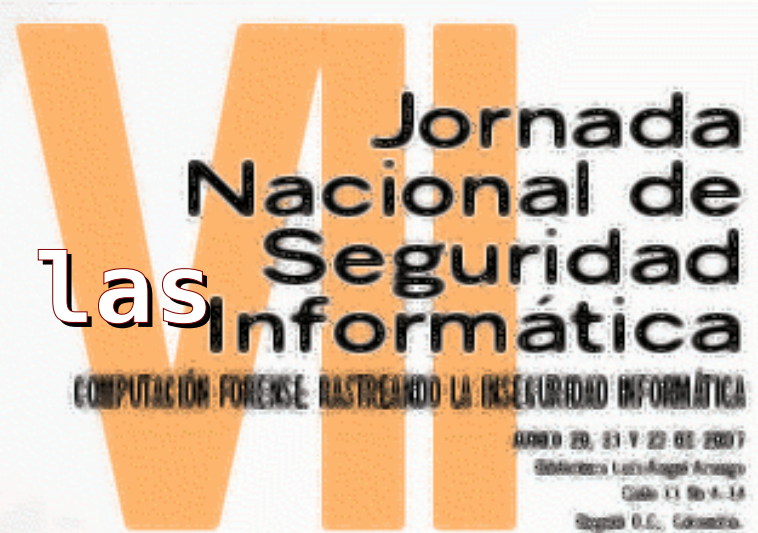


# Ciencias Antiforenses . . . . Un Nuevo Reto para las Organizaciones



El desafío del lado  
oscuro de la  
fuerza . . . . .

Andrés R. Almanza, Ms(c)  
[andres\\_almanza@hotmail.com](mailto:andres_almanza@hotmail.com)



# Propósitos

- ✓ Mostrar como las ciencias antiforenses enfrentan la dualidad de la inseguridad de la información.
- ✓ Cuales son uno de los nuevos escenarios en los cuales se debe prestar atención dado que ellos nos muestran cuan lejos estamos de encontrar soluciones completas que resuelven todos los problemas de seguridad.
- ✓ Mostrar los retos y desafíos que presentan las herramientas de nuestros días en temas de apoyo al proceso forense.
- ✓ Mostrar la forma en como la evidencia digital puede verse comprometida desde el punto de vista del proceso forense.



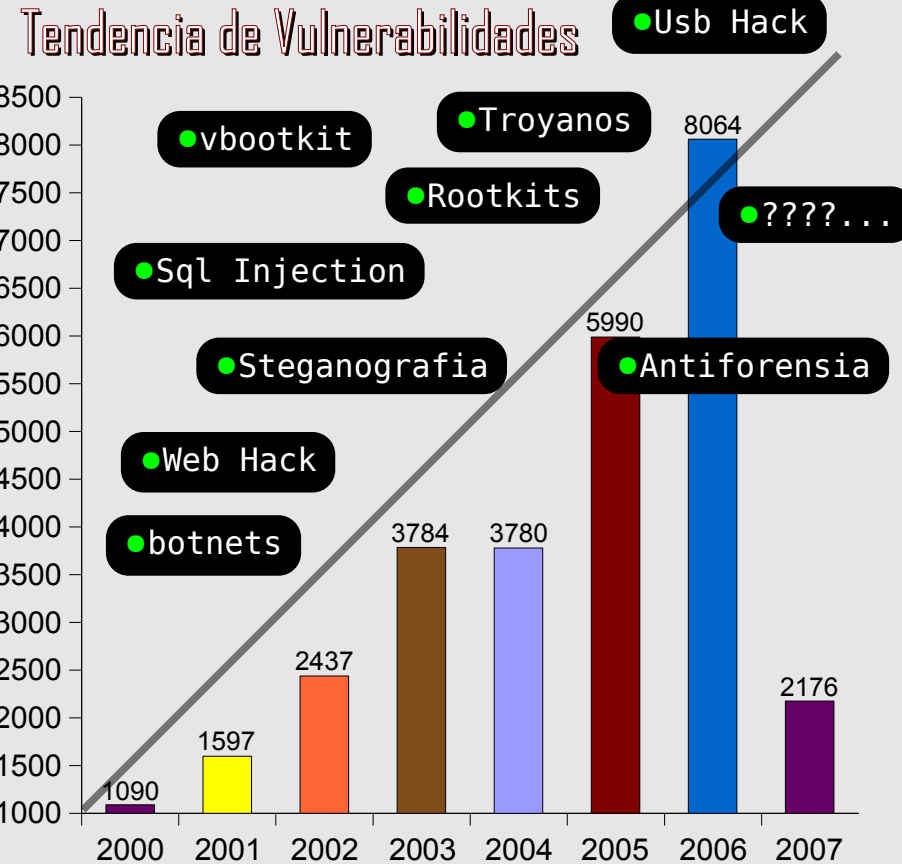
# Agenda

- ✓ Introducción
- ✓ Ciencias antforenses. El lado oscuro de la fuerza
  - ✓ Definiciones
  - ✓ Taxonomía
  - ✓ Herramientas
  - ✓ Nivel de Operatividad.
- ✓ Retos y Conclusiones
- ✓ Radiografía



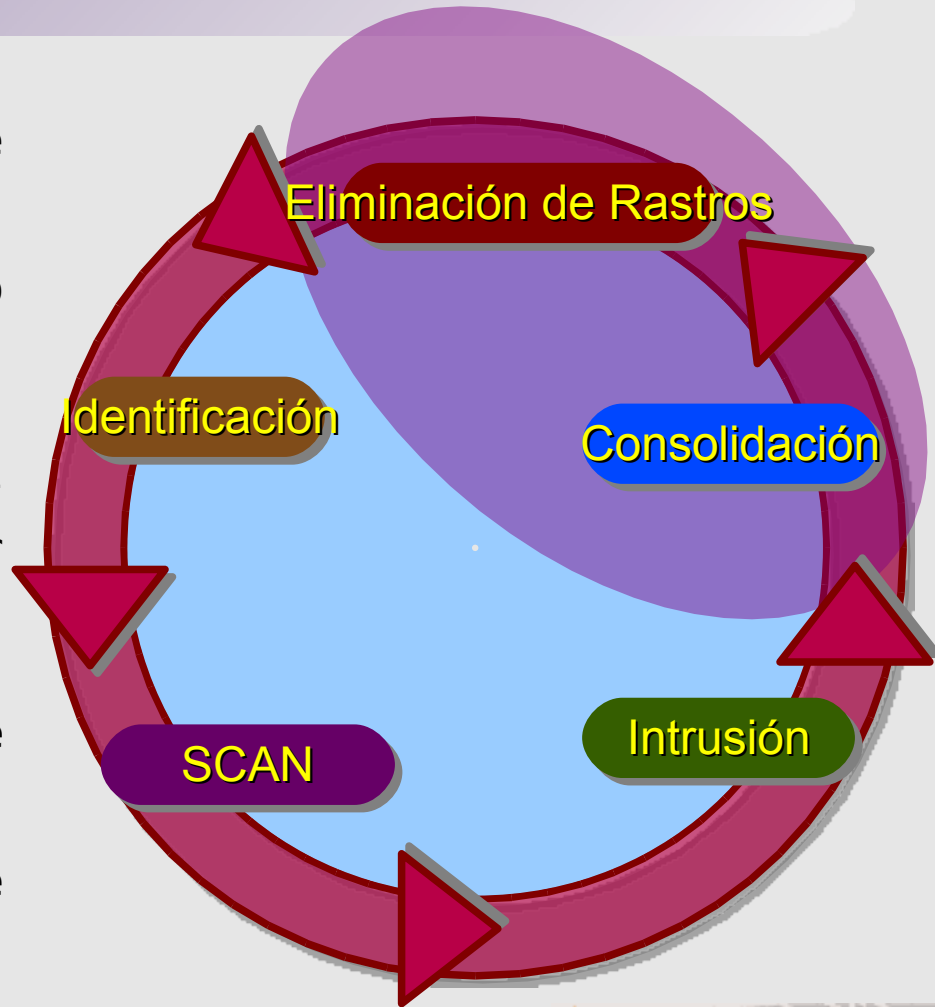
# Introducción

- ✓ Creciente es el número de ataques que se realizan
- ✓ Evolución y complejidad en los tipos de ataques
- ✓ Profundidad de los ataques
- ✓ Diversidad en la forma de ejecución
- ✓ Esfuerzos continuos del lado oscuro de la fuerza, por replantear los esquemas existentes.



# Introducción

- ✓ Creciente de necesidad de utilizar las ciencias forenses como herramientas de respaldo en los ambientes corporativos.
- ✓ Creciente la necesidad del atacante de no ser identificado.
- ✓ Centran esfuerzos en afianzarse sobre un sistema o eliminar sus rastros o evidencia de intrusiones.



# Ciencias AntiForenses

✓ Computacion forense:

✓ Uso del medio científico para establecer la información efectiva para una revisión jurídica.

✓ Se apoya en un proceso forense y unas herramientas con las cuales se obtiene información "confiable".

Recoleccion

✓Cadenas de custodia, preservacion de evidencia, documentacion

Analisis

Presentacion

✓Reconstruccion de eventos, analisis soportado con herramientas.

✓Presentacion oral, escrita ante los entes respectivos, lenguajes correctos, soportes adecuados

# Ciencias AntiForenses

## Genericas

✓ Uso del medio científico a los medios digitales para invalidar la información efectiva para una revisión jurídica.

✓ Uso del conocimiento científico, para obstruir el proceso forense.

## Incompletas

✓ “Intento por limitar la cantidad y calidad de la evidencia forense”<sup>[1]</sup>

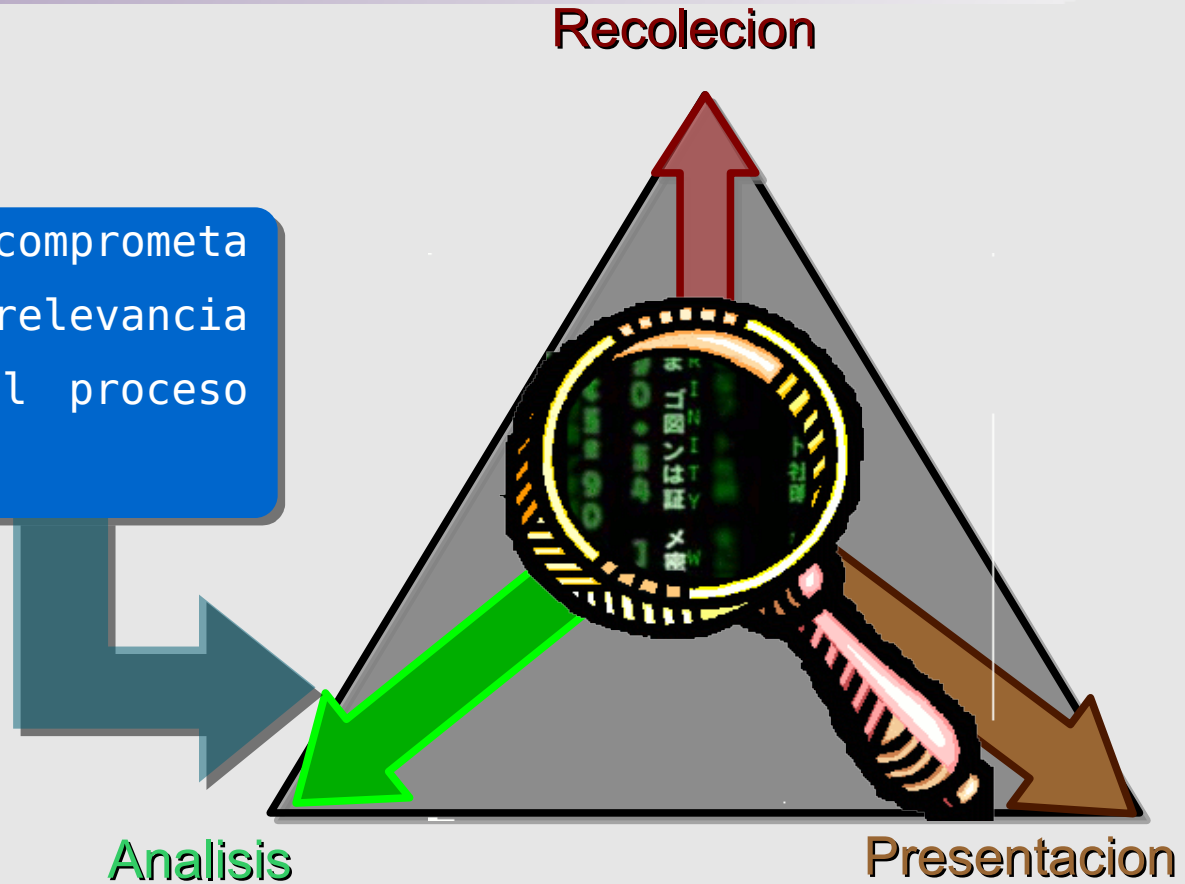
✓ “Intento por limitar la identificación, colección, recopilación y validación de datos electrónicos, con el fin de entorpecer la investigación.”<sup>[1]</sup>

## Compleja

✓ “Metodos usados para prevenir la aplicación de la ciencia a las leyes que son aplicadas por los entes judiciales en un sistema judicial”<sup>[1]</sup>

# Ciencias AntiForenses

“Cualquier intento que comprometa la disponibilidad y la relevancia de la evidencia sobre el proceso forense”<sup>[1]</sup>





# Ciencias AntiForenses

- ✓ Lo que buscan las ciencias antiforenses es crear debilidades en la evidencia y el proceso forense
  - ✓ Evitar la detección de alguna clase de evento ocurrido
  - ✓ Interrumpir el proceso de recolección de evidencia
  - ✓ Incrementar los tiempos necesarios de dedicación en un caso
  - ✓ Generar dudas sobre un proceso forense o testimonio.
  - ✓ Afectar la ejecución y utilización de las herramientas forenses



# Ciencias AntiForenses

- ✓ Existen aspectos tanto positivos como negativos de las ciencias antiforenses
  - ✓ Positivo:
    - ✓ Replantean y validan: Procesos forenses, Herramientas Forenses, Habilidades.
  - ✓ Negativo:
    - ✓ Pueden exonerar a un culpable
    - ✓ Pueden inculpar a un inocente
    - ✓ Afectar a un proceso forense.



# Ciencias AntiForenses

## ✓ Historia

- ✓ En el principio solo se hablaba de : Renombrar archivos, encriptación
- ✓ Luego: Borrado Seguro, ADS, Esteganografía
- ✓ Hoy se ve: MAFIA, FragFS, Defiler
- ✓ Mañana: .?..?..?..?..?

✓

## ✓ Que se ataca con las ciencias antiforenses

- ✓ Datos: Destrucción, Ocultamiento, Manipulación, Fabricación
- ✓ Herramientas: Devilidades en las herramientas, fallas en los analisis de las herramientas
- ✓ Analisis: Inconsistencias del analisis y evidencia presentada



# Ciencias AntiForenses

## Clasificación

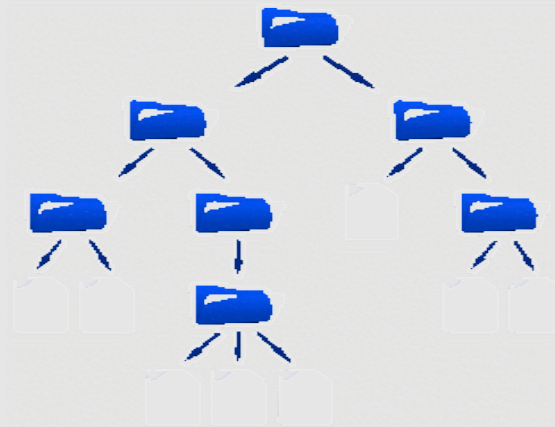
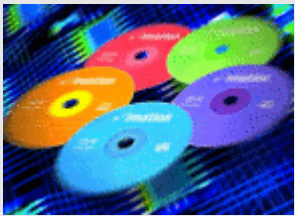
✓ Destruir

✓ Ocultar

✓ Eliminar la fuente

✓ falsificar

## Medios de Almacenamiento



# Ciencias AntiForenses

## ✓ Destruir

- ✓ Prevenir que esta sea encontrada, en caso de ser encontrada reducir su utilidad.
- ✓ Demantelar o inutilizar la evidencia dentro de un proceso forense
- ✓ No busca hacer la evidencia inaccesible, busca que sea irrecuperable la evidencia.
- ✓ Nivel simple de uso, en la mayoría de los casos
- ✓ Nivel Físico y Lógico



# Ciencias AntiForenses

## ✓ Destruir

### ✓ Destrucción Física:

- ✓ A través de campos magnéticos, (Degausser), Guardian Dog ( Dispositivo magnético)

### ✓ Destrucción Lógica:

- ✓ Técnica que busca reinicializar el medio, cambiar la composición de los datos.
- ✓ Buscan sobrescribir datos. ( Metada, Data)
- ✓ Eliminar las referencias a los datos



# Ciencias AntiForenses

## ✓ Destruir

- ✓ Wipe ( Liberar)
- ✓ Sobrecribir utilizando algoritmos

Método	Nivel de Seguridad	Cantidad de Pasadas	Detalles del Método
Borrado Rápido	Bajo	1	Rellena con ceros
RCMP TSSIT OPS-II	Medio	8	Escritura aleatoria en cada pasada
DoD Simple	Medio	3	3 pasadas del DoD 5220. (1,2 y 7)
DoD 5220-22.M	Medio	7	Caractéres aleatorios en las 7 pasadas
Gutman	High	35	27 pasadas con datos específicos, 8 con datos aleatorios
PRNG Stream	Medio-Alto	8	Sobre escibe con datos generados desde PRNG



# Ciencias AntiForenses

## ✓ Destruir

- ✓ Wipe ( Liberar)
  - ✓ Herramientas:
    - ✓ Wipe, shred, PGP secure delete, Evidence Eliminator, eraser, sdelete, srm, sfill (rellena disco), sswap, smem
    - ✓ Live-CD: [DBAN](#)
  - ✓ Nivel de Complejidad: Sencillo
  - ✓ Posibilidad de recuperación a través de software: Casi imposible
  - ✓ Posibles alternativas de Solución: Analisis Magnético.





# Ciencias AntiForenses

## ✓ Destruir

- ✓ Eliminar en \*nix
- ✓ Eliminar residuos

Describe el Sistema de Archivos

Necrofile:  
Libera todos los inodos borrados, y bloques de datos

Super Bloque

Tabla de Inodos

Bloques de Datos

Archivos de Directorio: Son el DNS de un sistema de archivos, jerarquía de directorio

Describe los archivos

Almacenamiento de los datos

Klismafile  
Libera entrada de directorios borradas

# Ciencias AntiForenses

## ✓ Destruir

- ✓ Eliminar
  - ✓ Herramientas:
    - ✓ Evidence Eliminator, Necrofile, Klismafile
  - ✓ Nivel de Complejidad: Sencillo
  - ✓ Posibilidad de recuperación a través de software: Casi imposible
  - ✓ Posibles alternativas de Solución: Analisis Magnético.



# Ciencias AntiForenses

✓ Ocultar

✓ Eliminar

✓ Herramientas:

✓ Evidence Eliminator, Necrofile, Klismafile

✓ Nivel de Complejidad: Sencillo

✓ Posibilidad de recuperación a través de software: Casi imposible

✓ Posibles alternativas de Solución: Analisis Magnético.



# Ciencias AntiForenses

## ✓ Eliminar la fuente

### ✓ Eliminar

#### ✓ Herramientas:

- ✓ Evidence Eliminator, Necrofile, Klismafile

- ✓ Nivel de Complejidad: Sencillo

- ✓ Posibilidad de recuperación a través de software: Casi imposible

- ✓ Posibles alternativas de Solución: Analisis Magnético.



# Ciencias AntiForenses

✓ falsificar

✓ Eliminar

✓ Herramientas:

✓ Evidence Eliminator, Necrofile, Klismafile

✓ Nivel de Complejidad: Sencillo

✓ Posibilidad de recuperación a través de software: Casi imposible

✓ Posibles alternativas de Solución: Analisis Magnético.



# Retos y Conclusiones

- ✓ Deben verse como un reto que afecta a todos los implicados, usuarios en la forma en como afecta la evidencia , investigadores en la confianza que se puede depositar en el proceso y las herramientas, y en los fabricantes para mostrar las limitaciones y alcances que las herramientas pueden suministrar.
- ✓ Mostrar un nuevo panorama de acción en el cual el lado oscuro de la fuerza puede actuar, y como este puede afectar significativamente un proceso forense
- ✓ Cuan valido pueden ser las técnicas antiforense en procura de un mejoramiento continuo al proceso forense.
- ✓ Cuales son las implicaciones reales de estas técnicas y como afrontar esta nueva problemática.



# Retos y Conclusiones

- ✓ Las comunidades de investigación forense debe trabajar de tal manera que las brechas que puedan existir entre un crimen y su perpetrador sean muy estrechas.
- ✓ Ver y conocer al enemigo, como mecanismo de aprendizaje en el que se desarrolle una cultura orientada al mejoramiento.



# Referencias

- ✓HARRIS, R. (2006) Arriving at an anti-forensics consensus: Examining how to define and control the anti-forensics problem. *Digital Investigation*. Pp 44-49. Disponible: <http://www.dfrws.org/2006/proceedings/6-Harris.pdf>
- ✓SIEFFER, M., FORBE, R., GREEN, C., POPYACK, L. y BLAKE, T. (2004) Stego intrusion detection system. *Proceedings of Digital Forensic Research Workshop 2004*. Disponible en: <http://www.dfrws.org/2004/bios/day3/D3-Sieffert-SIDS.pdf>
- ✓CASEY, E. (2002) Practical approaches to recovering encrypted digital evidence. *Proceedings of Digital Forensic Research Workshop 2005*. Disponible en: [http://www.dfrws.org/2002/papers/Papers/Eoghan\\_Casey.pdf](http://www.dfrws.org/2002/papers/Papers/Eoghan_Casey.pdf)
- ✓GARFINKEL, S. (2007) Anti-Forensics: Techniques, Detection and Countermeasures. *Proceeding of The 2nd International Conference on i-Warfare and Security (ICIW)*, Naval Postgraduate School, Monterey, CA, March 8-9. Disponible en: <http://www.simson.net/clips/academic/2007.ICIOW.AntiForensics.pdf>
- ✓Herramientas forenses y anti-forenses - [http://www.forensicswiki.org/wiki/Tools#Anti-forensics\\_Tools](http://www.forensicswiki.org/wiki/Tools#Anti-forensics_Tools)
- ✓Investigación forense de sistemas Linux - <http://loquefaltaba.com/documentacion/forense/index.html>
- ✓La era dorada del Hacking <http://www.infoworld.com/articles/hn/xml/02/10/25/021025hngoldenage.html>





# Referencias

✓J. C. Foster and V. Liu. Catch me if you can... In *Blackhat Briefings 2005*, 2005.URL

<http://www.blackhat.com/presentation/bh-usa-05/bh-us-05-foster-liu-update.pdf>

✓Grugg. The art of defiling: Defeating forensic analysis. In *Blackhat Briefings 2005*, 2005. URL

<http://www.blackhat.com/presentations/bhusa-05/bh-us-05-grugg.pdf>

✓C. S. J. Peron and M. Legary. Digital anti-forensics: Emerging trends in data transformation techniques. n.d. URL

<http://www.securis.com/documents/papers/Securis-Antiforensics.pdf>

✓M. Rogers. Anti-forensics. 2005. URL

<http://www.cyberforensics.purdue.edu/docs/Lockheed.ppt>

✓B. Shirani. Anti-forensics. High Technology Crime Investigation Association, 2002. URL <http://www.aversion.net/presentations/HTCIA-02/anti-forensics.ppt>.

✓CANO, J. (2007) Inseguridad informática y computación anti-fosense. Dos conceptos emergentes en seguridad informática. URL

<http://www.virusprot.com/computaci%F3n-anti-forense.htm>

✓PEIKARI, C y CHUVAKIN, A. (2004) *Security warrior*. O'Reilly.

