

# Anàlisi Forense de Sistemes Informàtics

**R. Rallo**

**Dep. Enginyeria Informàtica i Matemàtiques, ETSE.**

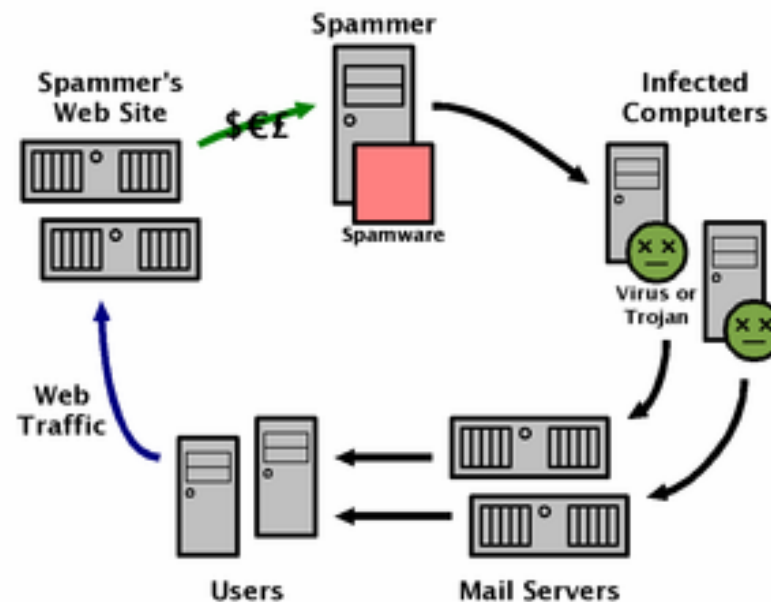
**Universitat Rovira i Virgili, Tarragona, Catalunya, SPAIN**





# La meva màquina és un zombi?

- Ordinador connectat a internet compromès per un hacker un trojà o un virus/cuc
- Perfil típic:
  - Windows
  - Usuari amb pocs coneixements tècnics
- Entre el 50-80% de l'spam està enviat per zombis
- Les xarxes de zombis s'anomenen botnets



- Accions legals
  - Usuaris privats: complicat
  - Empreses: factible
- Aprendre i evitar-ho
  - estudiar l'atac
- Eines:
  - L'anàlisi forense



# Què és l'anàlisi forense?

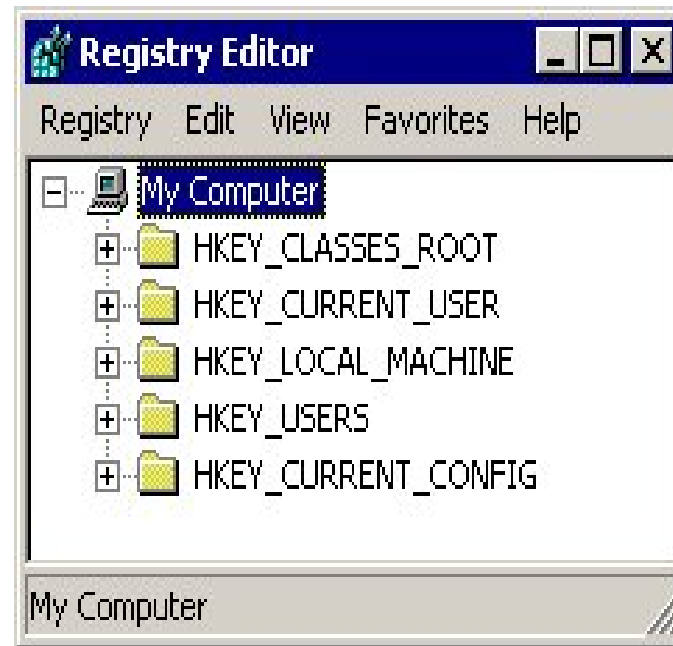
- Es basa en l'aplicació de mètodes i tècniques per a recollir, analitzar i preservar les dades d'un sistema informàtic
- Tot s'ha de fer de manera que sigui “legal”
- L'objectiu bàsic de l'anàlisi forense és preservar les evidències
- L'anàlisi dependrà fortament del programari i maquinari infectat: (Linux vs. Windows, Xarxa vs. Disc, etc...)
- Objectius secundaris:
  - Recuperar els sistemes el més aviat possible

# Etapes en l'anàlisi forense

- Congelar l'escenari de l'atac
- El sistema conté informació amb diferents nivells de volatilitat
  - Memòria
  - Registres processador
  - Sistema de fitxers, ...
- Evidència fotogràfica (amb números de sèrie dels components)
- Coses que no s'han de fer:
  - Treure el cable de xarxa
  - Procediments normals d'aturada
  - Mirar els fitxers
  - Executar aplicacions

- Recollida d'informació bàsica
  - who, last, w
  - ls del /root, \$HOME, /dev
  - ps
  - lsof
  - netstat
  - arp
- Intentar fer una còpia del /proc

- La informació més important la tenim al REGISTRY



# Informació al registry (exemples)

## **Dial-up Accounts:**

- HKEY\_CURRENT\_USER\RemoteAccess\Addresses

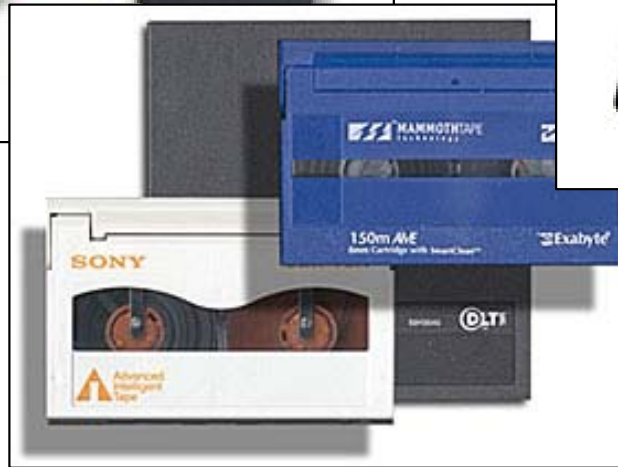
## **Dial-up Account Usernames:**

- HKEY\_CURRENT\_USER\RemoteAccess\Profile\[isp\_name]
- RegisteredOwner/Organization, Version, VersionNumber, ProductKey, ProductID, ProductName
- HKEY\_LOCAL\_MACHINE\Software\Microsoft\Windows\CurrentVersion

## **MSN Messenger Info:**

- HKEY\_CURRENT\_USER\Identities\{string}\Software\Microsoft\MessengerService
- HKEY\_CURRENT\_USER\Software\Microsoft\MessengerService

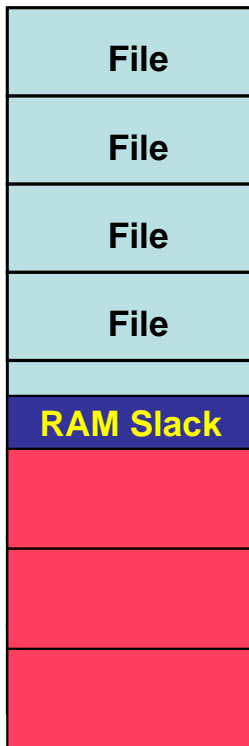
- No treballarem mai sobre l'original



- No és un backup, és una còpia bit a bit
- Algunes eines:
  - SafeBack ([www.forensics-intl.com](http://www.forensics-intl.com))
  - Ghost ([www.symantec.com](http://www.symantec.com))
  - DD (standard unix/linux utility)
    - *#dd if=device of=device bs=blocksize*
  - Encase ([www.encase.com](http://www.encase.com))
  - Mareware
  - FTK ([www.accessdata.com](http://www.accessdata.com))

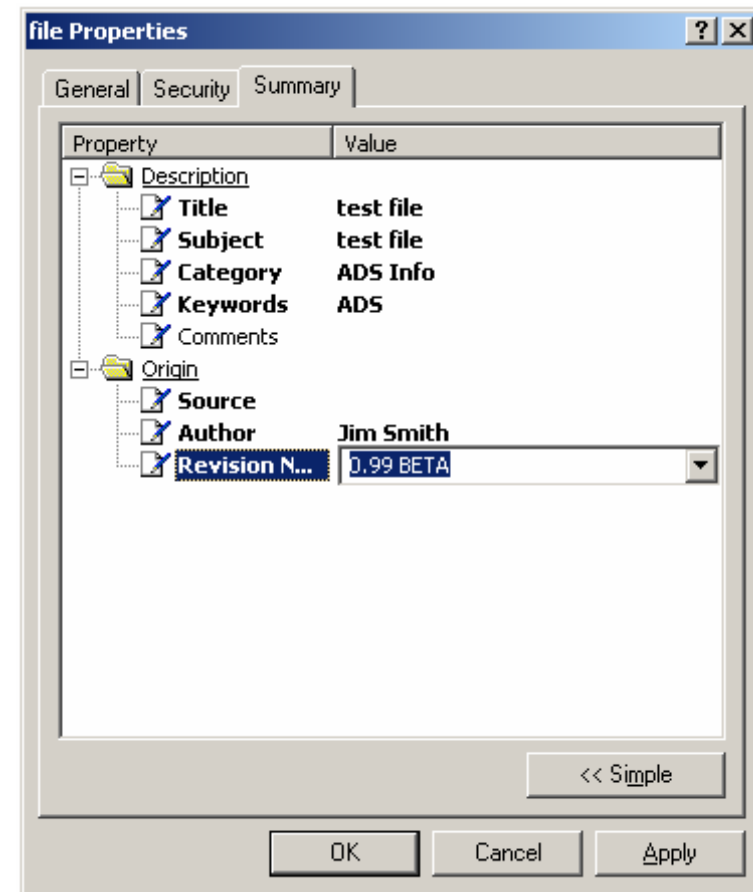
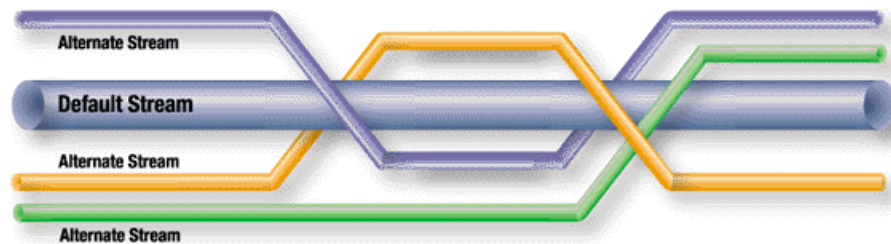
- Canvi de nom dels fitxers:
  - Document.doc → imatge.jpg
- Còpies defectuoses:
  - Copiar a un disc sense tenir prou espai
- Imprimir un fitxer (com funciona?)
- Esborrar o formatar disc
- Específic de Linux
  - Directoris amb noms (. , .., ...)
  - Ocultar un filesystem sota un altre
  - Swap, core dumps

- Espai sobrant per a completar un sector o cluster



# Alternate Data Streams

- Pròpis de NTFS (windows) o HFS (macs)
- La major part d'eines del sistema únicament consideren el default stream



- **Crear un fitxer:**

```
echo text in default stream > myfile.txt
```

```
echo extra text in ADS > myfile.txt:hidden.txt
```

**Amagar la calculadora de Windows al ADS:**

```
C:\>echo some text > c:\temp\file.txt
```

```
C:\>type c:\winnt\system32\calc.exe >  
c:\temp\file.txt:hidden.exe
```

```
C:\>type c:\temp\file.txt
```

```
C:\>start /b c:\temp\file.txt:hidden.exe
```

# Esteganografia

