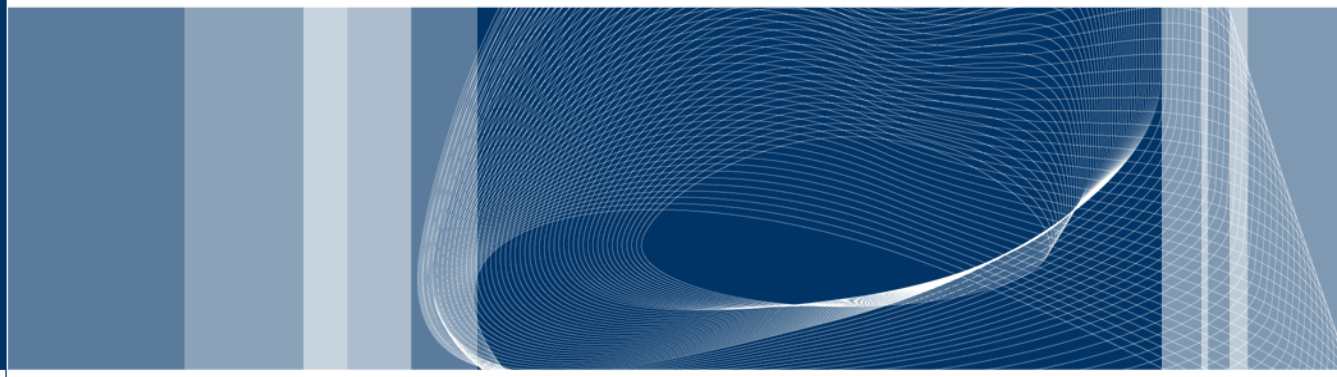
POLITECNICO DI MILANO



AntiForensics: try to catch me if you can!

Ing. Stefano Zanero, PhD
Dip. Elettronica e Informazione – Politecnico di Milano

Recap

- Forensic analysts wish to reconstruct “what has happened”
- Reconstruction must hold up to scrutiny in court
- Phaese
  - Acquisition
  - Identification
  - Evaluation
  - Presentation

Critical points

- Which are the technology-dependent phases?
  - Acquisition (usage of tools for repeatable cloning and custody)
  - Identification (usage of tools for analysis of file systems, data reconstruction and carving)
- Interfering, we can compromise the process
  - Transient antiforensics: if we interfere with identification, in a way which can be defeated if detected
  - Definitive antiforensics: if we interfere with acquisition, by making evidence impossible to acquire, unreliable or tampered

Anti-forensics definition

- Techniques that aim to create confusion in the analyst, to lead him off track, or to defeat tools and techniques used by analysts
- Some are sci-fi, others are simple and effective
- Targets:
  - Timestamps
  - Log analysis
  - File recovery and carving
  - File and executable identification
  - Steganography and data hiding

Timeline...

- As we saw, analysis tools can display a timeline based on MAC(E) values: Modified, Accessed, Changed, (Entry Changed: check value on NTFS)
- We can therefore modify events by making them appear separated, or close, randomizing them or moving them completely out of scope
- Tool: “timestomp” (MACE) o “touch” (MAC)
- You can bet your money that even costly tools such as EnCase cannot do much against this.

Log analysis

- Tipically you don't do it by hand
- You tipically use regular expressions
- If attackers can inject stuff in the logs (very likely), they can try to make your scripts fail, or even to exploit them!

Deleted file recovery

- If forensics = reading the ashes, let's throw the ashes to the wind
  - Secure deletion (heide, sysinternals sdelete, etc)
  - Wiping unallocated space
  - Encryption
    - Note: some secure delete utilities are fake, be advised...
- Note: reading “residuals of magnetization”, a la Gutmann, are science fiction: overwritten means gone.

FISTing (cough...)

- Filesystem Insertion and Subversion Technologies
- We place data where there's no reason to look for them, in particular inside FS metadata
  - fsck is our enemy as it may “repair” metadata and trash our insertions
  - Inside partition table I can hide 32 KB of data
  - In EXT(2/3) I can do:
    - RuneFS: writing in bad block inodes (unlimited space)
    - WaffenFS: adds a fake EXT3 journal in an EXT2 partition (up to 32 MB storage)
    - KY FS: uses directory inodes (unlimited space)
    - Data Mule FS: puts data in padding and metadata structures of FS ignored by forensic tools (up to 1MB of space on a typical FS)

Partition table fun

- Partitions not correctly aligned
  - Using a partition restore tool we can read them, but they may escape a forensic analyst
- Adding multiple extended partitions
  - Windows and Linux manage them, many forensic tools don't
- Generate n logical partitions in an extended
  - With n high enough tools die

Carving and filetype searches

- Most tools use two base methods for filetype detection
  - Extensions (oh, yeah !)
  - Signature on header&footer (not much better)
- ... couple of bash lines, and no more child porn images will be retrieved from a media
- Solution: using more flexible and advanced way to detect files (under research)

Ghost in the shell

- What if the traces are not on the disk?
- Example: Metasploit's meterpreted (or Mosdef, or IMPACT)
  - Injected in a process memory space
  - Gives attacker control
  - Doesn't write anything to disk
  - Can add thread, execute...
- So...
  - When the machine is shut down, evidence is lost!
  - ... and what is the first or second step of the regular S.O.P. when a machine is compromised?
  - Only hope: in-memory forensics; Windows Memory Forensics Tool (M. Burdach) or memdump