Windows Forensics

Dr. Phil Polstra

PhD, CISSP, CEH

@ppolstra

http://philpolstra.com

Certifications:
http://www.securitytube-training.com

Pentester Academy: http://www.PentesterAcademy.com

File Forensics

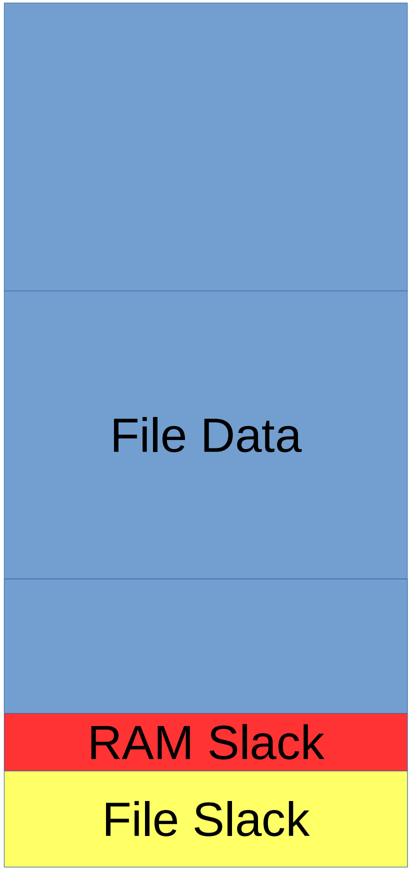
File Forensics

- Examining individual files
- Can be used to find hidden info
  - Mismatched extensions
  - Slack space
  - Unallocated space
  - Page files

File Signatures

- Many files have standard headers
- Some also have standard footers
- Helps
  - Identify mismatched extensions
  - Retrieve files from swap & memory
  - Verify undeleted files
- Comprehensive list http://www.garykessler.net/library/file_sigs.html

Slack Space



- Leftover space in a cluster when file size not an exact multiple of cluster size
- RAM Slack – partial sector
- File Slack – whole sector
- Total Slack = (cluster size)-(file size)%(cluster size)

RAM Slack

- Long time ago what followed in RAM after data was written to disk
- Quickly figured out that this is bad security
- Today it should be all zeroes
- Used portion = filesize%512
- Slack = 512-filesize%512

File Slack

- Can contain fragments of old files
- Whole sectors of slack
- Slack = (total slack)//512
- Slack = ((cluster size)-(file size)%(cluster size))//512

File Carving

- Using file signatures to find files in
  - Swap space
  - Unallocated clusters
  - Unallocated disk space
- General carving tools
  - Foremost
  - Scalpel
- Specialized tools also exist