Windows Forensics

Dr. Phil Polstra
PhD, CISSP, CEH

@ppolstra
http://philpolstra.com

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

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

Deleted Files

What happens on deletion

- First byte in directory entry/entries changed to 0xE5
- Clusters are marked available (zeros) in FATs
- For FAT32 high word of starting cluster may be zeroed

The easy scenario

- File uses only one cluster
- Not FAT32
- Guaranteed recovery if cluster is not reused
- Even if FAT32 might still be recoverable

The medium difficulty scenario

- File is contiguous (not fragmented)
- Not FAT32
- Recovery is likely if clusters have not been reused
- FAT32 recovery far from guaranteed

The scenario you don't want

- File is fragmented
- If you are extra unlucky also FAT32
- Must rely on best guess of cluster allocation
- If it is even possible, manual intervention may be required

Technique

- If < 1 cluster
  - If not FAT32 check for cluster unallocated
  - If FAT32 scan through possible clusters looking for unallocated and data of appropriate size
- If > 1 cluster
  - If not FAT32
    - If block of clusters beginning at start cluster unallocated probably it
  - If FAT32
    - Attempt to find a block of clusters with the stated cluster low word
      - Check that data size matches last partial sector appropriately

Technique (continued)

- If you have gotten this far chances of success are low
- If not FAT32
  - Start from starting cluster and search forward for unallocated sectors
  - Unless the disk is very full if the file was recently deleted this is probably right
- If FAT32
  - Look for possible solutions with largest contiguous set of unallocated clusters at beginning that are not empty

The good news

- FAT filesystems are primarily used for removable media and not internal hard drives
- We will learn that NTFS undeletion is much simplier