Windows Forensics

Dr. Phil Polstra
PhD, CISSP, CEH

@ppolstra
http://philpolstra.com

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

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

FAT Directory Entries

Directory Entries

- Contain
  - Filename (8.3)
  - MAC timestamps
  - File size
  - First cluster
- 32 bytes long
- First two entries for subdirectories: . & ..
- Kludge for long filename support

Directory Entries

Offset	Length	Item
0 (0x00)	11 (0x0B)	File name
11 (0x0B)	1 (0x01)	Attributes: B0-5: RO, hidden, system, volume label, subdirectory, archive B6-7: unused
14 (0x0E)	4 (0x04)	Creation Time & Date
18 (0x12)	2 (0x02)	Last Access Date (no time)
20 (0x14)	2 (0x02)	Starting cluster high word (FAT32)
22 (0x16)	4 (0x04)	Modified Time & Date
26 (0x1A)	2 (0x02)	Starting cluster low word
28 (0x1C)	4 (0x04)	File size in bytes (0 for directories)

Directory Times and Dates

	Bits	Length (bits)	Item
Time	B11-B15	5	Hours
	B5-B10	6	Minutes
	B0-B4	5	Double seconds
Date	B9-B15	7	Years since 1980
	B5-B8	4	Month
	B0-B4	5	Day

Long Filename Entries

- Added in Windows 95
- Long entries also 32 bytes
- Long entries contain no metadata only name in Unicode
- Long filenames grow upward from single short entry

Long Filename Entries

Offset	Length	Item
0 (0x00)	1 (0x1)	Sequence number B0-B4; B6(0x40)=final part
1 (0x01)	10 (0x0A)	Part of filename in Unicode
11 (0x0B)	2 (0x02)	Always 0x0F 0x00
13 (0x0D)	1 (0x01)	Checksum for short filename
14 (0x0E)	12 (0x0C)	Part of filename in Unicode
26 (0x1A)	2 (0x02)	Always 0x00 0x00
28 (0x1C)	4 (0x04)	Part of filename in Unicode

Deleted Files

- First byte in directory entry/entries changed to 0xE5
- File clusters marked as available in FAT
- In some versions of Windows FAT32 cluster high word zeroed