Windows Forensics

Dr. Phil Polstra

PhD, CISSP, CEH

@ppolstra

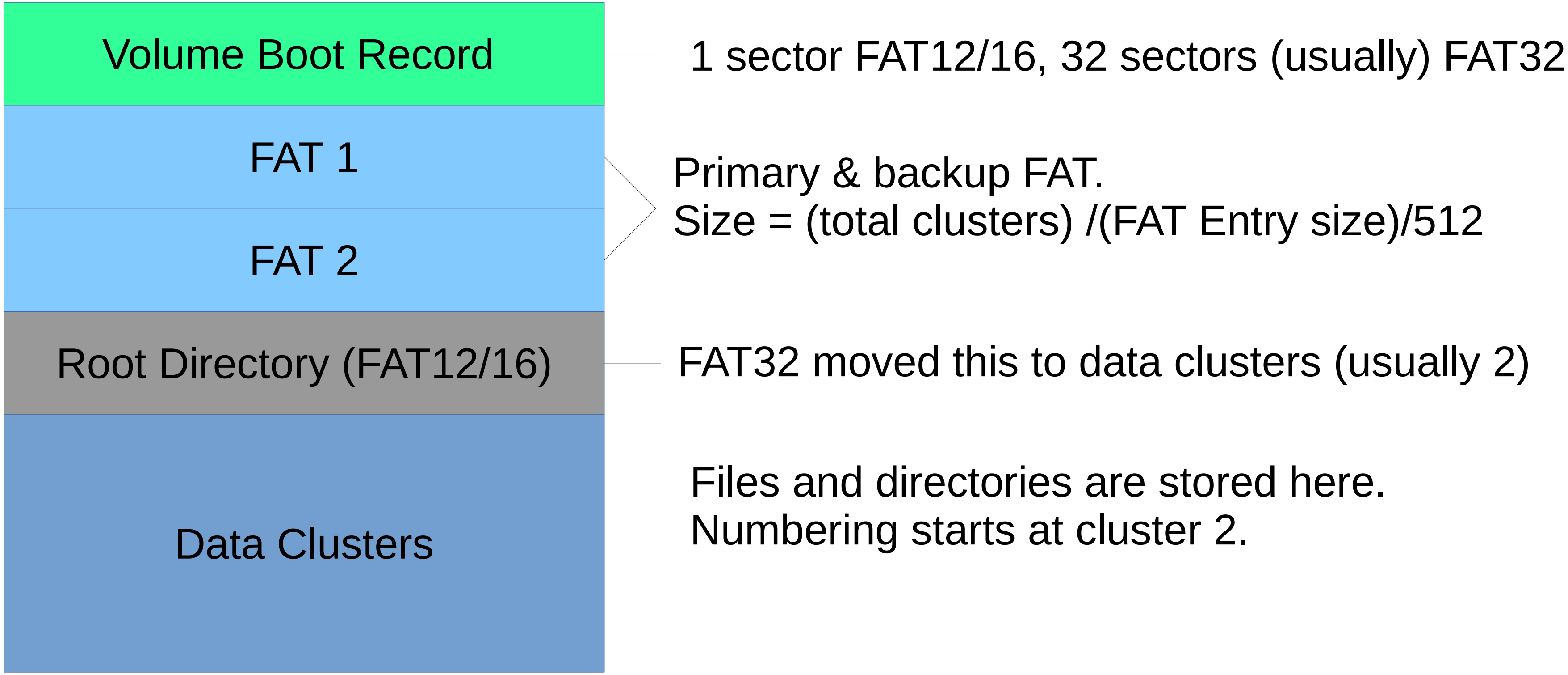
http://philpolstra.com

FAT Filesystem Basics

FAT Filesystem

- Been around since DOS
- Three flavors: FAT12, FAT16, & FAT32
- Contains File Allocation Tables
- De facto standard
- Modern versions of Windows won't install on it

FAT Layout



Volume Boot Record

1 sector FAT12/16, 32 sectors (usually) FAT32

FAT 1

FAT 2

Primary & backup FAT.
Size = (total clusters) /(FAT Entry size)/512

Root Directory (FAT12/16)

FAT32 moved this to data clusters (usually 2)

Data Clusters

Files and directories are stored here.
Numbering starts at cluster 2.

Volume Boot Record

- Allows filesystem to tell operating system about itself
- Contains needed and extended parts
- One sector for FAT12/16
- Normally 32 sectors for FAT32

File Allocation Table

- Gives status for each cluster
  - Available
  - Used and file continues to another cluster
  - Used and last cluster in a file
- First two entries are special
- Used to create a cluster chain
- Two FAT are normally updated together

Directory Entries

- Contain metadata
  - MAC times
  - File size
- Contains the starting cluster for a file
- Relate file names to cluster chains

Data Clusters

- Where all the files live
- All directories (with the possible exception of root directory) live here too
- The only part of the disk that isn't overhead
- Collection of sectors