USB Forensics and Pentesting

Dr. Phil Polstra
PhD, CISSP, CEH

@ppolstra
http://philpolstra.com

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

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

USB Mass Storage: Presentation

USBMS Presentation

- Nearly all flash drives present themselves as SCSI hard drives
- “Hard drive” sectors are typically 512, 2048, or 4096 bytes
- SCSI transparent command set is used
- Most drives are formatted as one partition or logical unit
- Should check for additional logical units (max LUN >0)
- Should check reported versus actual media size
- Info can be hidden in higher sectors
- Some cheap drives are out there that grossly over report size
- A typical 512 byte sector needs 16 bytes for error correction

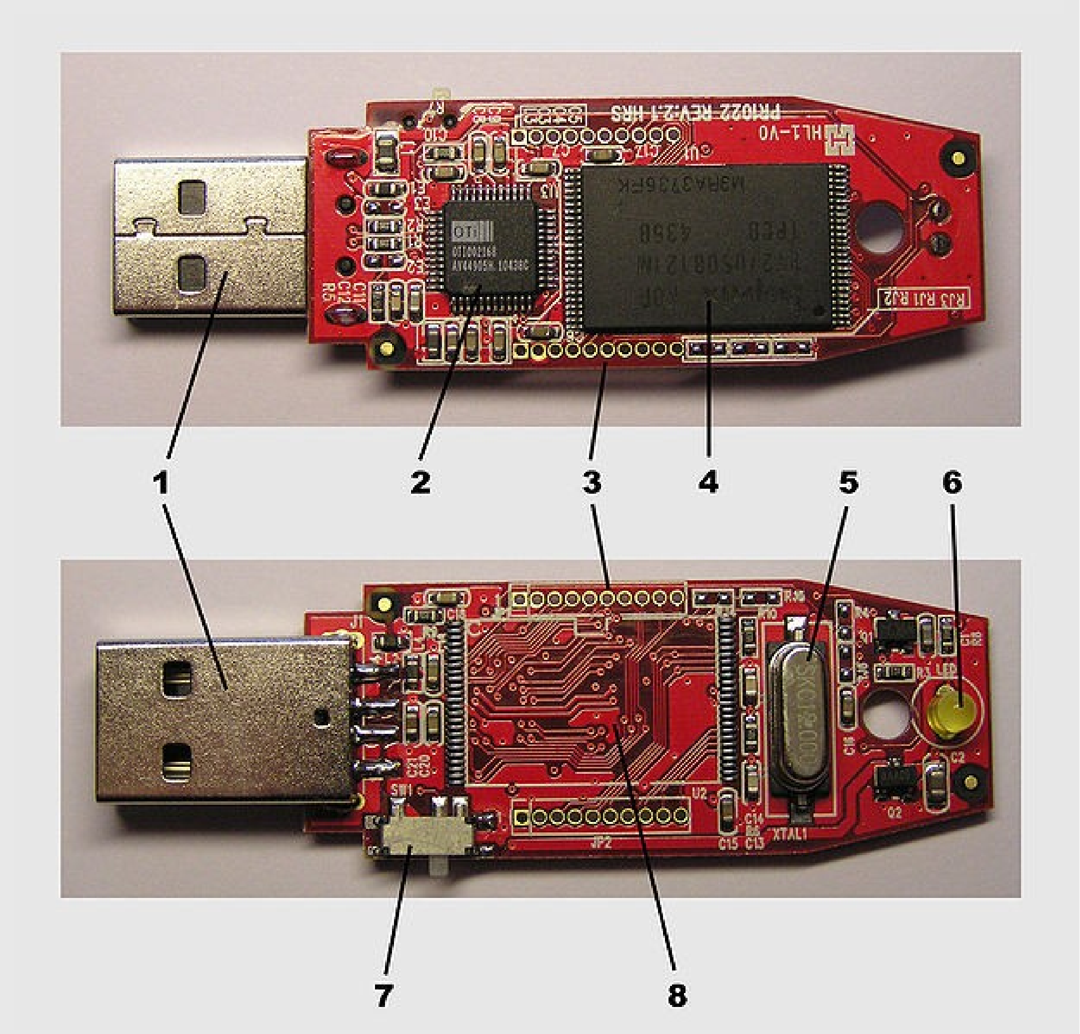
Filesystems

- Most preformatted with FAT or FAT32
- NTFS
- TrueFFS
- ExtremeFFS
- JFFS
- YAFFS
- Various UNIX/Linux file systems

USBMS (Flash) Reality

- Typically utilize NAND flash memory
- Memory degrades after 10,000 write cycles
- Most chips not even close to high-speed USB speed (480 Mbps)
- Can only be written in blocks (usually 512, 2048, or 4096 bytes)
- Chips are somewhat easily removed from damaged drives for forensic recovery
- Some controllers have JTAG capability which can be used for memory access
- Some controller chips steal some flash memory for themselves

Typical Drive Hardware



©SecurityTube.net

Presentation Demo