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: Descriptors & Endpoints

USBMS Descriptors

- Class: 0x08 – USB Mass Storage
- Subclass: 0x06 – Bulk only transport
- Protocol: 0x50 – SCSI instruction set
- Normally found at interface level even when the only interface
- Serial number is required

USBMS Endpoints

- At least two bulk endpoints (in/out) are required
- Must support full and high-speed
  - Full speed might be far from optimal
- Max packet size is typically 64/512 for full/high speed

Descriptors & Endpoints Demo