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: Windows

USBMS Windows Registry

- Registry stores lots of information on past and current USB devices
- All USB devices SYSTEM\CurrentControlSet\Enum\USB
- Mass Storage SYSTEM\CurrentControlSet\Enum\USBSTOR
- User that mounted NTUSER.dat\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2

Windows Registry Demo