# 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

# Write Blocking

# Write Blocking in Windows

- HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\StorageDevicePolicies\ WriteProtect
- All or nothing blocking for USB mass storage devices

# Write Blocking in Linux

- Udev rules allow you to handle what happens when devices are connected, disconnected, etc.
- Every block device connected downstream of magic hub (parent with appropriate VID/PID) is automatically mounted read only
- Suitable for hard disks and **ANYTHING** that can be mounted via USB

# Write Blocking in Linux

- The way that USB devices are handled by udev rules requires multiple rules
- This is because all the required data is not available when a single rule is running