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

Hardware Write Blocking

High Level Design

- Use the FTDI VNC2 chip again
- Device enumerates USBMS drive and presents itself as a standard USBMS device to PC
- Only safe (whitelisted) commands are passed through to the real USBMS device
- Handler functions for each possible command

Important Notes

- Some devices have poor performance at full-speed
- Linux loads more information initially than Windows which might result in a noticeable delay
- 64-bit Windows seems to have issues
- New FT90x chip might address these issues

Hardware