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

HW Write Blocking: Threads & Helpers

Application Threads

- Two application threads
- One enumerates attached USBMS device
- Second presents a fake USBMS to PC
  - Safe commands from PC are passed to actual USBMS device
- Semaphores are used to coordinate the threads

Helper Functions

- Open devices
- Attach devices
- Close devices
- Check USBMS device status

Threads & Helpers Demo