

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: USBMS Emulation

Device Emulation Thread

- Interpret commands in CBW
- Call an appropriate handler
- Makes use of helper functions
 - Forward CBW
 - Send/receive data
 - Return CSW

USBMS Emulation Demo