

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: Host Enumeration

Host Enumeration

- Once enumeration is complete a variable is set to other thread and semaphore is signaled
- Thread mostly sleeps and occasionally checks for connect/disconnect of USBMS device

Host Enumeration Demo