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

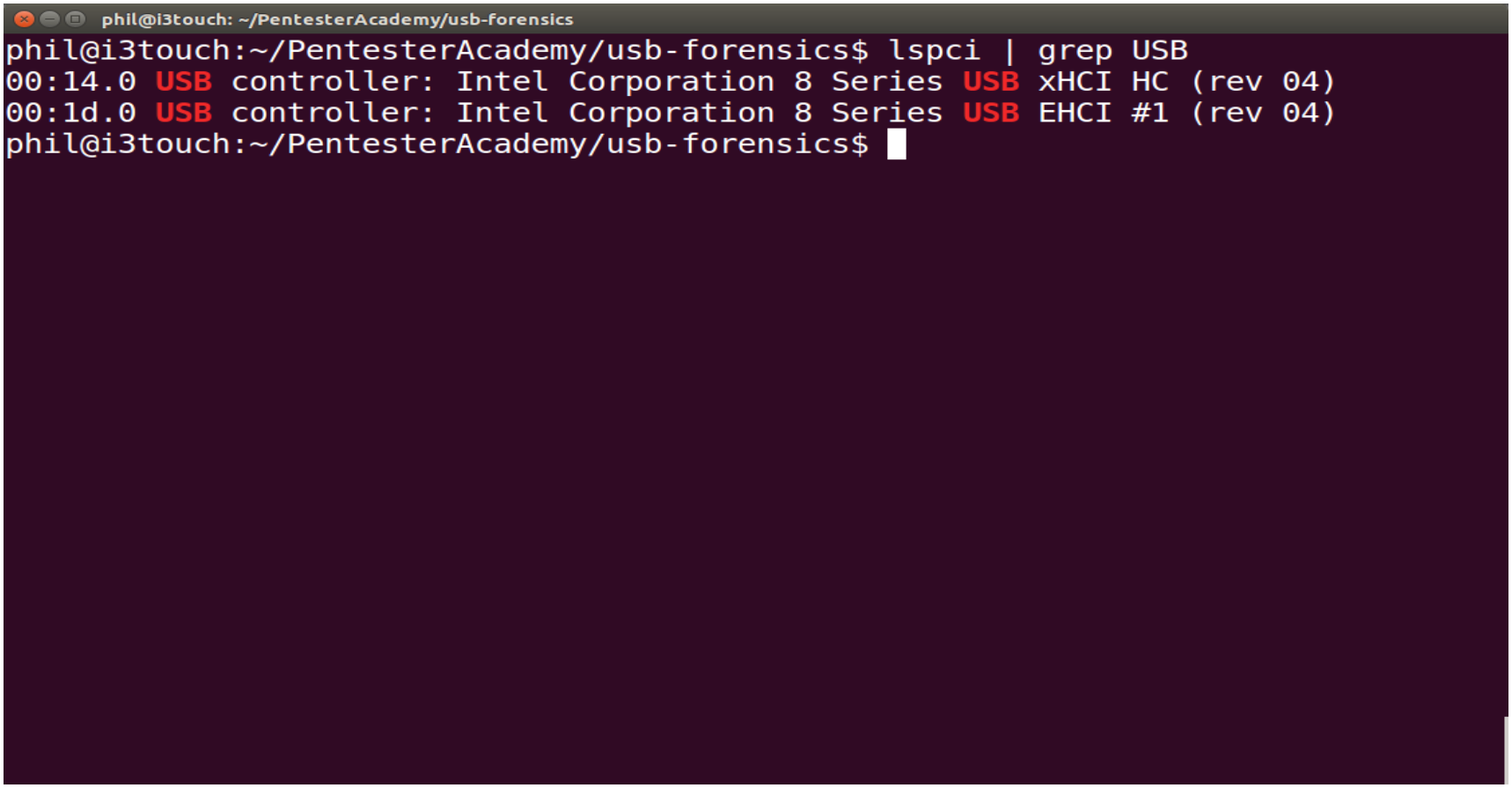
USB Hosts and Hubs

Hosts

- Every PC has at least one host controller
- Manage data on USB bus(es)
- Send/receive data to devices
- Poll devices (where required)
- Most USB 2.0 chipsets support Enhanced Host Controller Interface (EHCI) standard
- Most USB 3.0 chipsets support Extensible Host Controller Interface (xHCI) standard

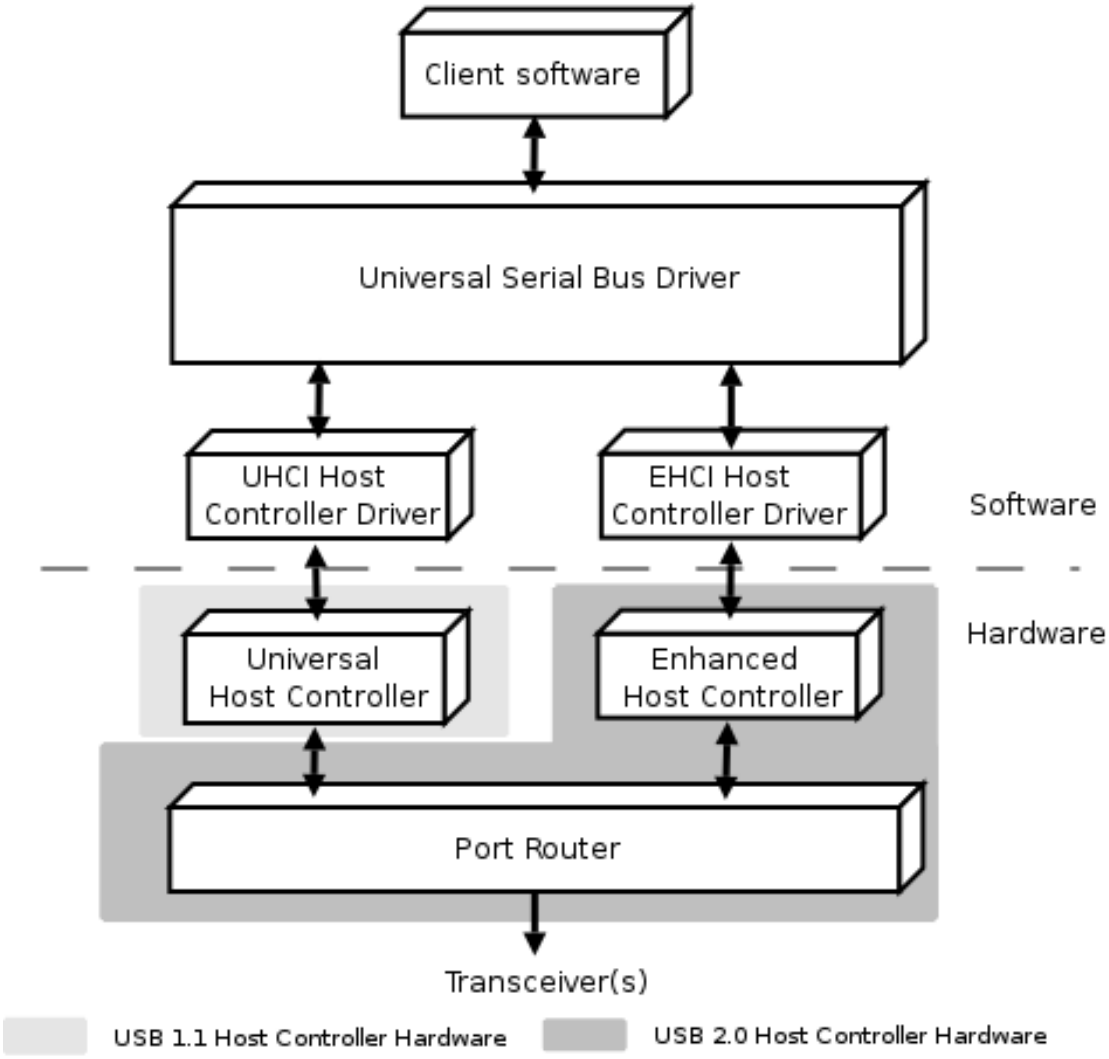
Finding USB Host Controllers

- Lspci | grep USB



Host Controller Architecture

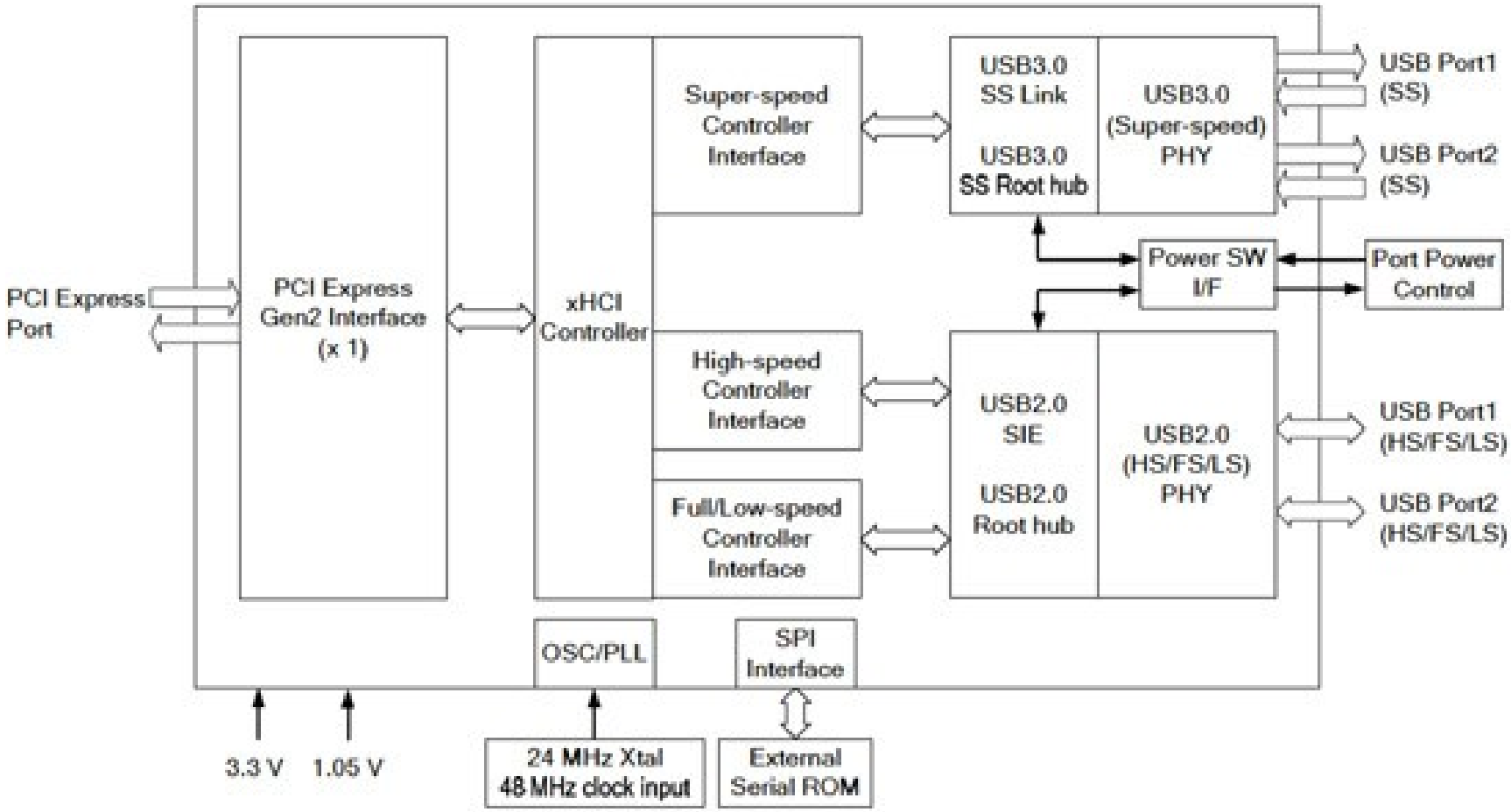
http://www.gaisler.com/images/grusbhc-host.png



Hubs

- Monitor insertion/removal
- Manage power
- Root hubs directly connected to host controller
- USB 3.0 hubs
  - Contain a USB 2.0 hub
  - Are actually switches

Hubs and USB 3.0



http://hothardware.com/newsimages/Item10987/NECUSB3-2.jpg

Host and Hub Demo