Windows Forensics

Dr. Phil Polstra
PhD, CISSP, CEH

@ppolstra
http://philpolstra.com

Certifications:
http://www.securitytube-training.com

Pentester Academy: http://www.PentesterAcademy.com

Making Filesystem Images

High Level Process

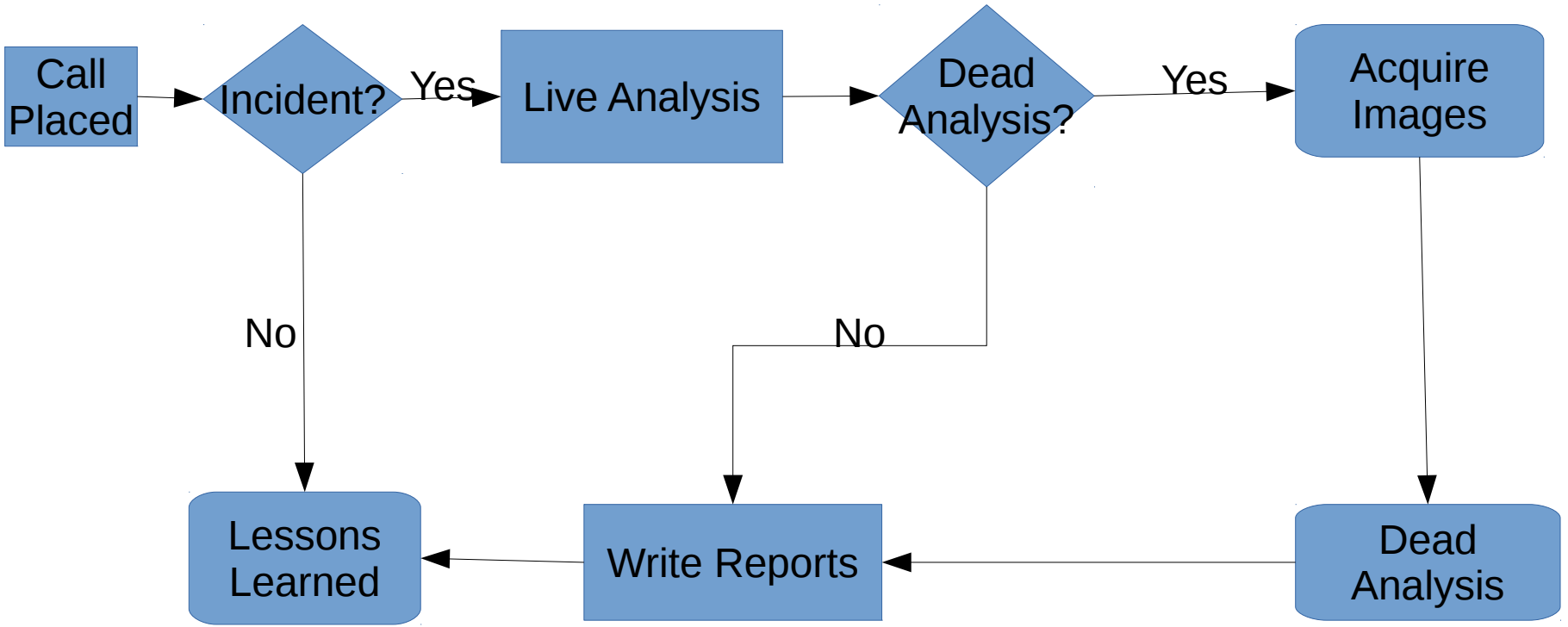

Image File Formats

- Raw
- Proprietary with embedded metadata
- Proprietary with metadata in separate file
- Raw with hashes stored in a separate file

Creating an Image

- Raw: dd if=<subject device> of=<image file> bs=512
- Raw with hashes along the way: dcfldd if=<subject device> of=<image file> bs=512 hash=<algorithm> hash window=<chunk size> hashlog=<hash file>

Write Blocking

- Hardware write blockers
  - Commercial blockers for SATA only $350+
  - USB write blocker described in USB class
    - Cheap at about $25
    - Slow due to limits of microcontroller that is full-speed (12 Mbps) only
- Software write blocking
  - Use udev rules as described in USB forensics course
  - Boot live forensics Linux on subject computer
  - Boot live forensics Linux on forensics workstation

Making the Image