Linux Forensics

Dr. Phil Polstra
PhD, CISSP, CEH

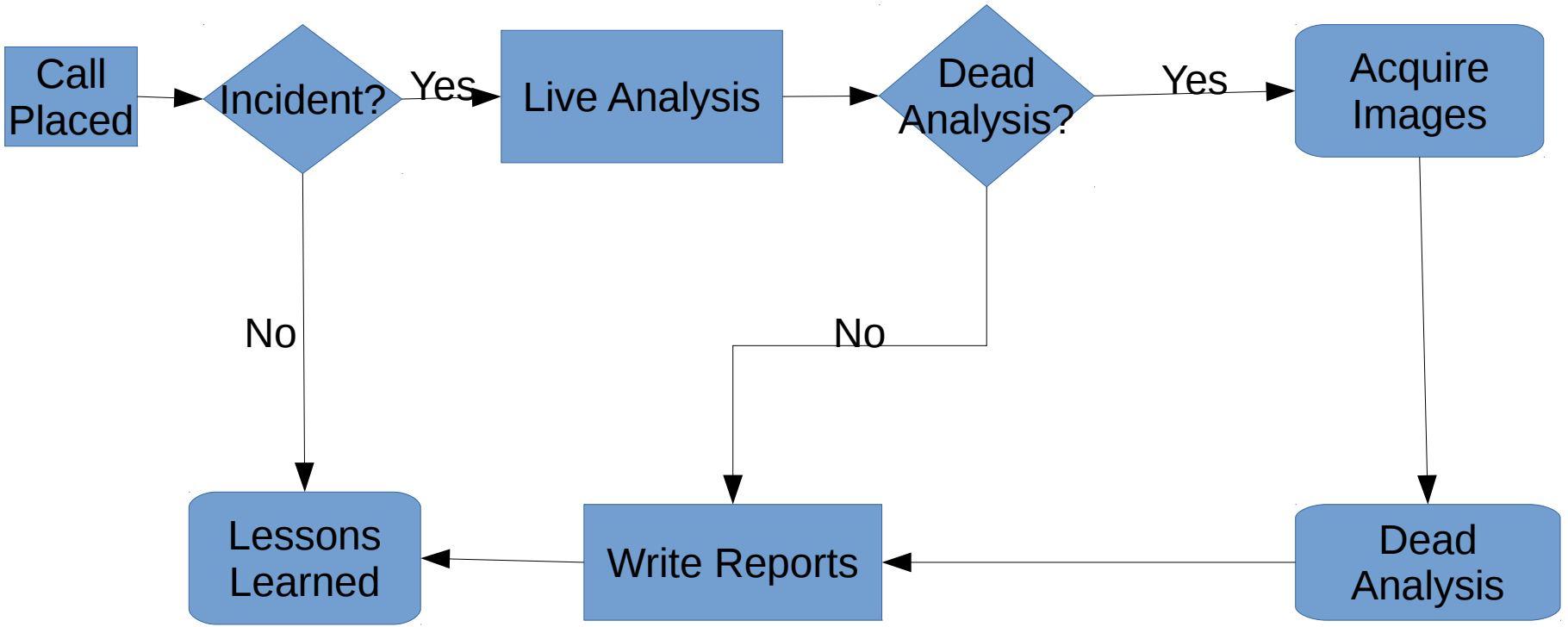
@ppolstra
http://philpolstra.com

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

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

Shutting Down the Subject System

High Level Process



Last Steps Before Shutdown

- We have memory dump
- Any last minute scans or repeats of initial scans
- Decide on normal shutdown or pulling the plug

Normal Shutdown

- Filesystems should be clean
- Malware might cleanup after itself and/or destroy evidence

Pulling the Plug

- Filesystem may not be clean
  - Could call sync before pulling the plug
- No chance for malware to destroy any info
- Memory image already collected

Shutdown time