Linux Forensics

Dr. Phil Polstra
PhD, CISSP, CEH

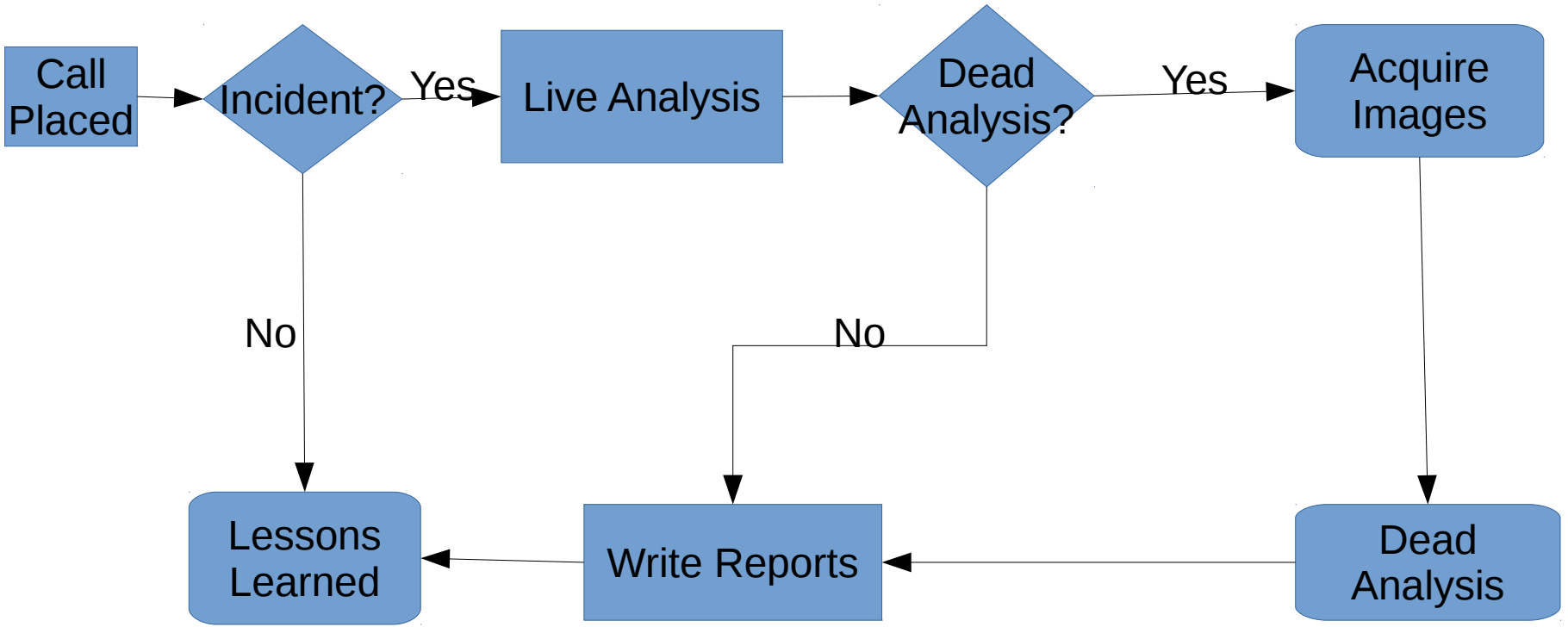
@ppolstra
http://philpolstra.com

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

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

Starting an Investigation: Netcat

High Level Process



Minimize disturbance to system

- Don't install anything on subject system
- Don't create new files on the system
- Minimize memory footprint
- Possible solutions
  - Netcat (best)
  - Store to USB drive

Using Netcat to Transport Data