# Linux Forensics

Dr. Phil Polstra

PhD, CISSP, CEH

@ppolstra

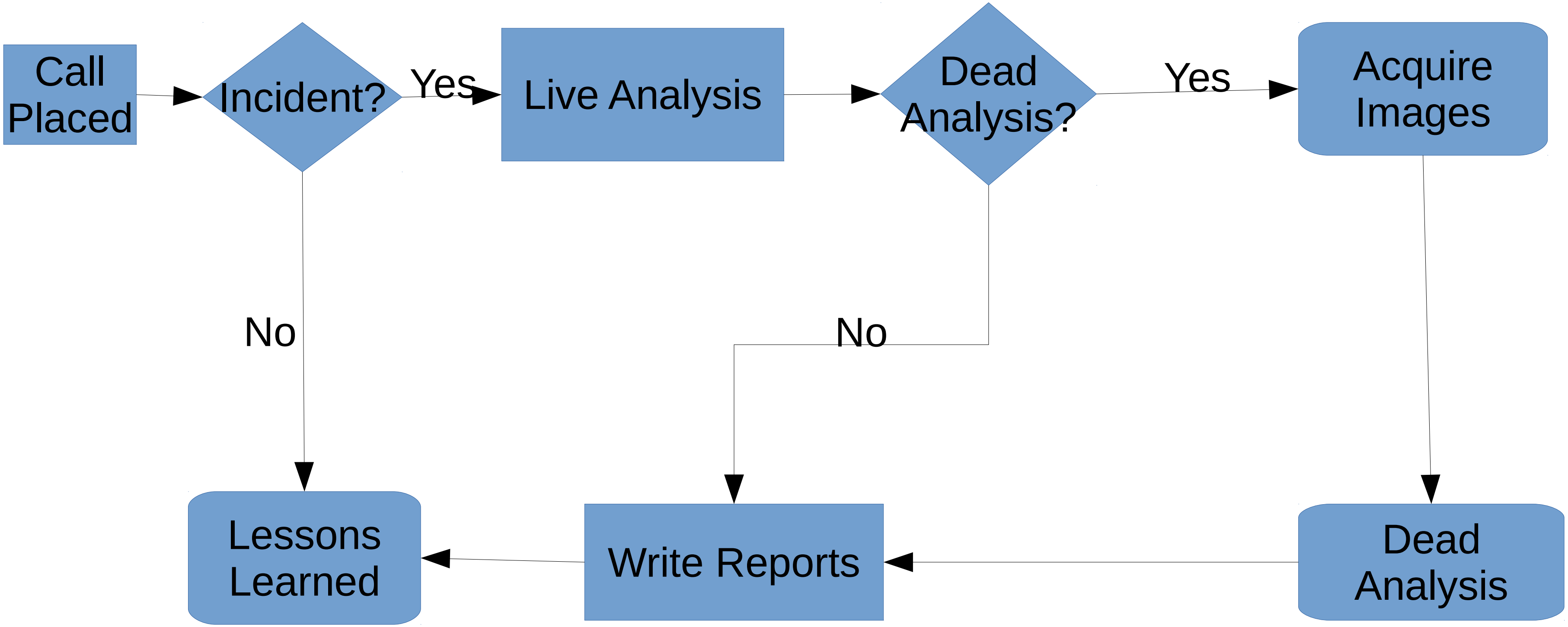
http://philpolstra.com

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

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

# Starting an Investigation

# High Level Process



# Has there been an incident?

- Open a case file
- Talk to the users
  - Why did they call you?
  - Why do they think there is a problem?
  - What is known about the potential victim system:
    - Normal use
    - Origins
    - Recent repairs?

# Documentation

- Write notes in your notebook
    - What users said
    - What you know about the subject system
- Consider taking photos of system and screen if appropriate
- You are now ready to consider actually touching the system

# Mount the known good binaries

- If not automounted mount your drive
- Run known good shell
- Set path to only point to your directories
- Reset LD_LIBRARY_PATH

# Mounting Incident Response Media