Windows Forensics

Dr. Phil Polstra
PhD, CISSP, CEH

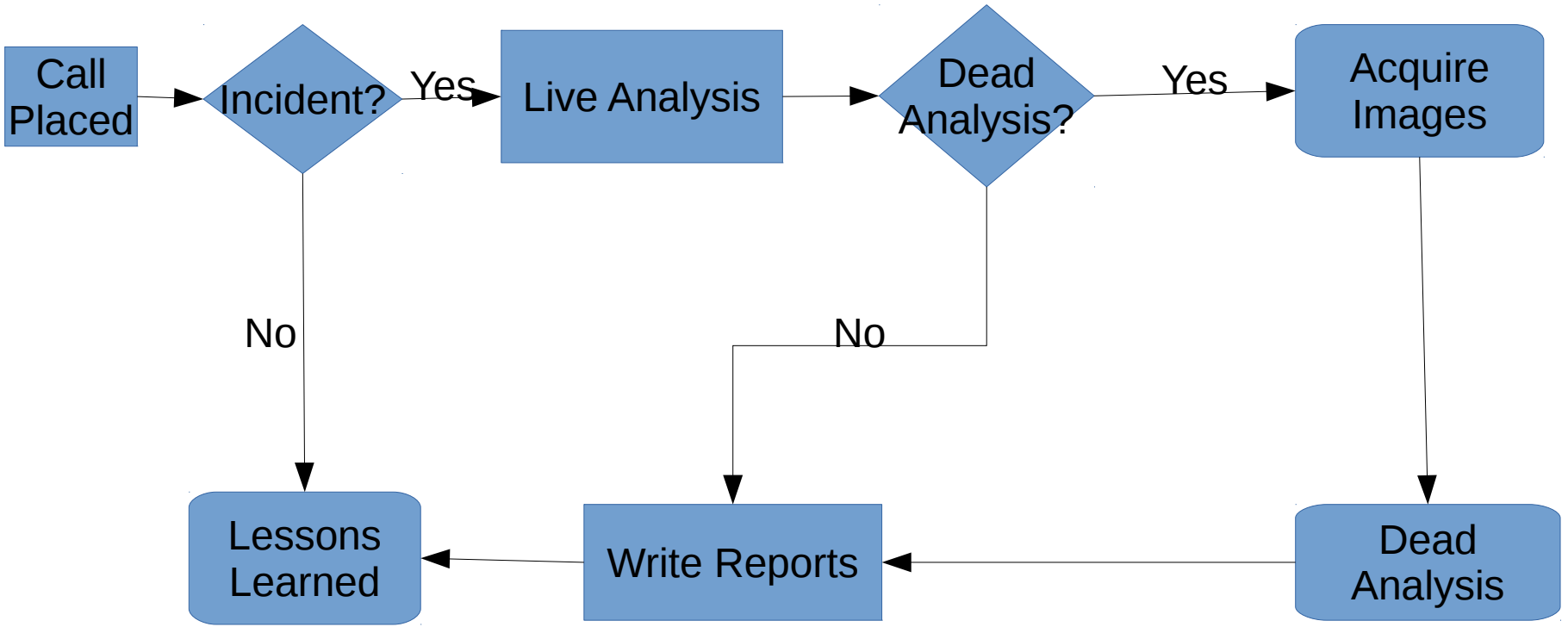
@ppolstra
http://philpolstra.com

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

- More complicated than Linux equivalent
- Check path to point to your programs first
- Cannot completely replace Windows binaries
- Advanced malware can hide its presence
- USB 3.0 Flash drive recommended
  - For practice you might want USB 2.0 for use in VirtualBox

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