Windows Forensics

Dr. Phil Polstra
PhD, CISSP, CEH

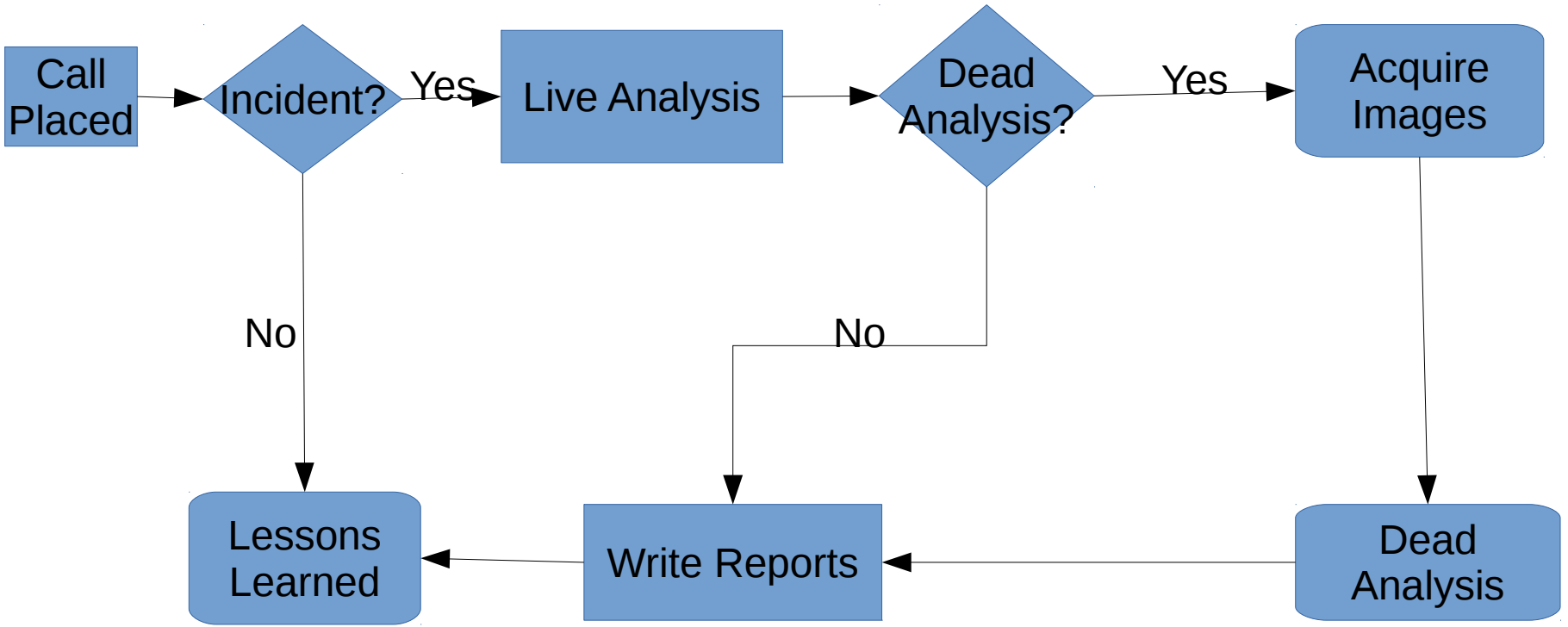
@ppolstra
http://philpolstra.com

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

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

Collecting Volatile Data

High Level Process



Data to Collect

- Date and Time
  - Clock may be skewed
  - Might be in different timezone
- Network interfaces
  - Funny networks
  - Promiscuous mode?
- Network connections

Data to Collect (cont.)

- Open ports
- Programs associated with ports
- Currently logged on users
- Running processes
- Running services
- Open files
- Routing tables
- Mounted filesystems
- Scheduled jobs
- Process memory dumps
- Clipboard contents
- Driver information
- Shares
- Command history

Collecting Data