Windows Forensics

Dr. Phil Polstra
PhD, CISSP, CEH

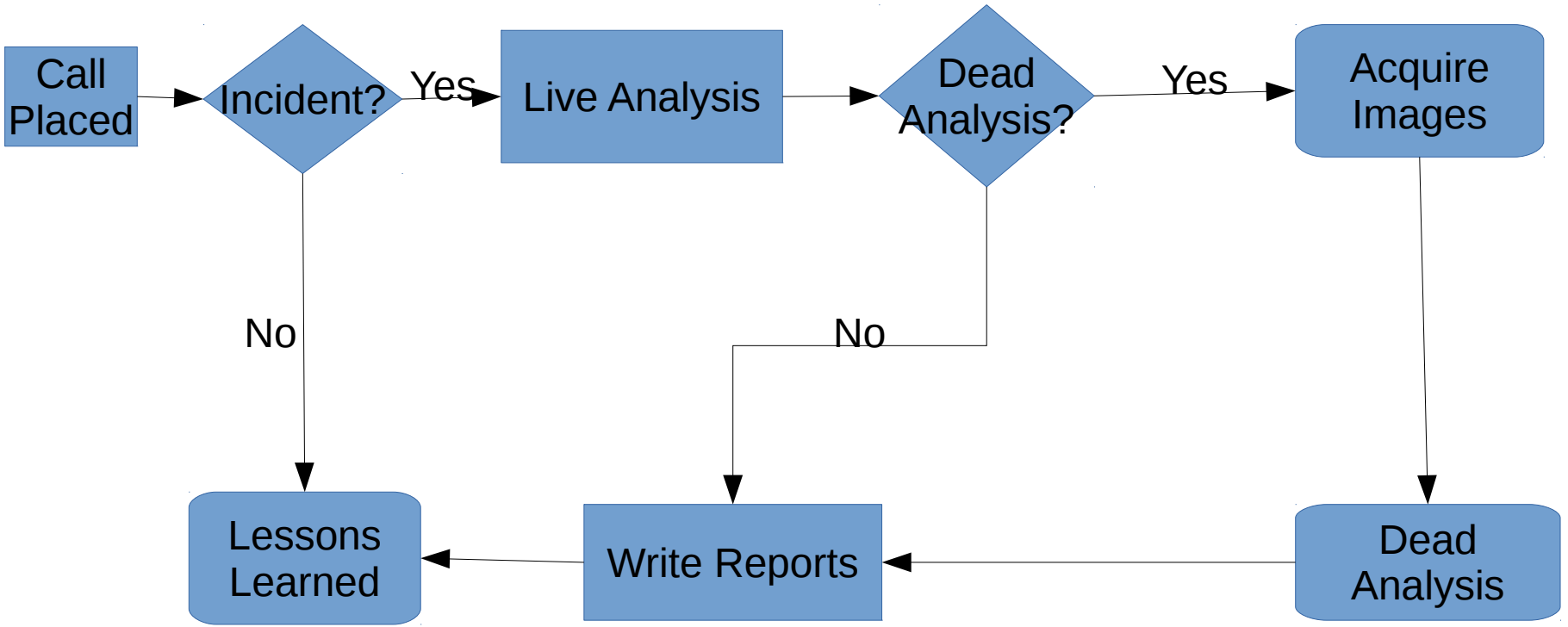
@ppolstra
http://philpolstra.com

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

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

Forensic Basics: First Steps

High Level Process



Be Prepared

- Have a response kit with a complete set of forensics tools
  - Both 32-bit and 64-bit versions
  - Ideally CDROM and USB
  - We will build this set of tools throughout this course
- Hardware
  - Write blockers
  - Media
  - Forensic laptop
- Notebook, etc. for documentation

Your Forensics Workstation

- At least 8GB of RAM is recommended
- Ideally with USB 3.0 port(s)
- Wired networking available
- Linux distro (64-bit)
  - Specialized distros such as SIFT or
  - Ubuntu or
  - Your favorite distro

Installing SIFT (or at least tools)

- To install all of it on top of Ubuntu 14.04:

```
wget --quiet -O - https://raw.github.com/sans-dfir/sift-bootstrap/master/bootstrap.sh | sudo bash -s -- -i -s -y
```

- To install just the tools on top of Ubuntu 14.04:

```
wget --quiet -O - https://raw.github.com/sans-dfir/sift-bootstrap/master/bootstrap.sh | sudo bash -s -- -i
```

Installing Tools