Linux Forensics

Dr. Phil Polstra
PhD, CISSP, CEH

@ppolstra
http://philpolstra.com

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

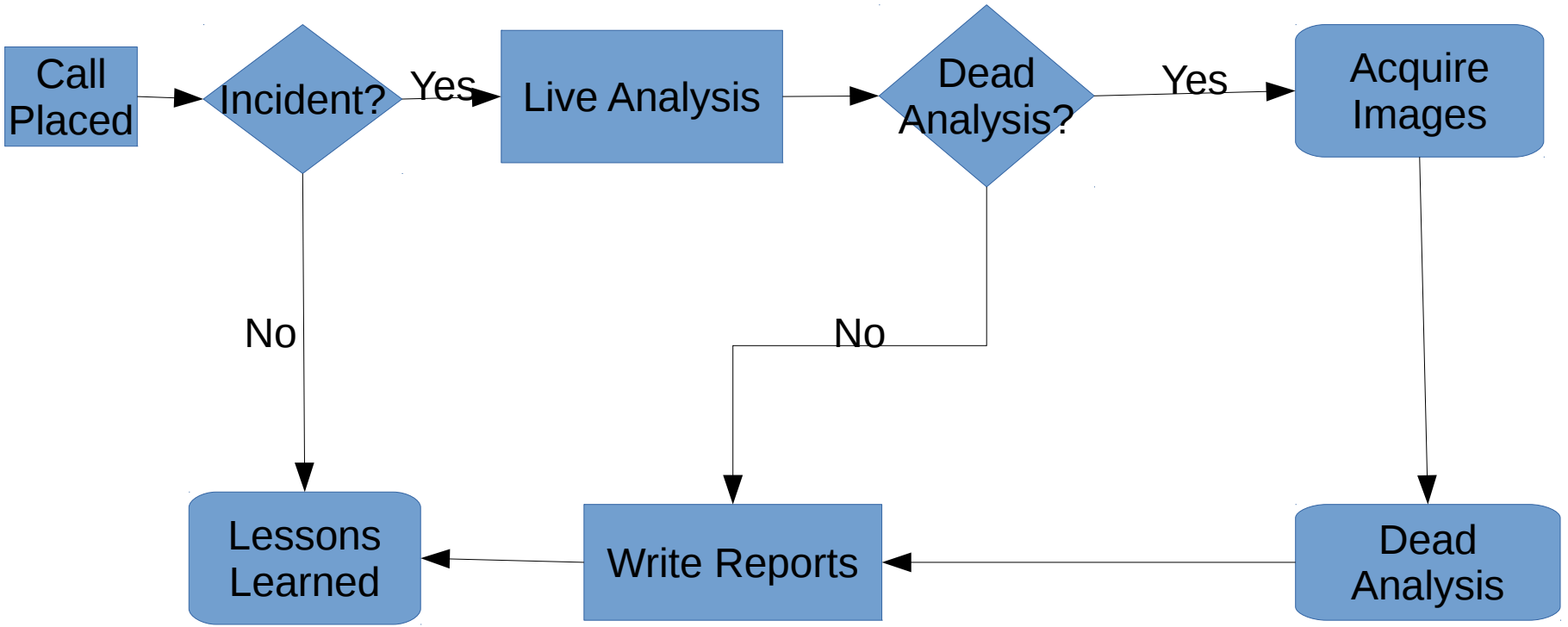
Pentester Academy: http://www.PentesterAcademy.com

©SecurityTube.net

Live Analysis: Dumping RAM

©SecurityTube.net

High Level Process



©SecurityTube.net

In simpler times

- Physical memory could be dumped via /dev/mem
- Virtual memory could be dumped via /dev/kmem
- Both of these are now disabled, limited, or flat out removed
  - Serious security issue to have these in userland
  - /dev/mem was limited to first 896MB of RAM

©SecurityTube.net

Modern Acquisition: Hard Way

- Download fmem from http://hysteria.sk/~niekt0/foriana/fmem_current.tgz
  - make
  - sudo make install
- Works just like /dev/mem but creates /dev/fmem
- Use /proc/iomem to determine appropriate bits
- Raw memory image is difficult to use for more than simple searches

©SecurityTube.net

Modern Acquisition: Easy Way

- Use Linux Memory Extractor (LiME)
  - Must be built for an exact kernel
  - Should not be built on subject machine
  - For **identical** versions of Ubuntu can use sudo apt-get install lime-forensics-dkms
  - For every other situation must download from https://github.com/504ensicsLabs/LiME and compile with correct kernel headers
  - Compile with “make” for current kernel or “make -C /lib/modules/<kernel version>/build M=$PWD” for other kernels

©SecurityTube.net

Using LiME

- Pick format
  - Raw (every segment concatenated together)
  - Padded (same is raw, but with zeroes in right bits
  - Lime (recommended format with metadata)
- Pick destination (path)
  - File (external drive please!)
  - Network port (use netcat on forensics workstation)
- sudo insmod lime.ko “path=<path> format=<format>”

©SecurityTube.net

Dumping RAM with LiME

©SecurityTube.net