

Windows Forensics

Dr. Phil Polstra

PhD, CISSP, CEH

@ppolstra

<http://philpolstra.com>

Certifications:

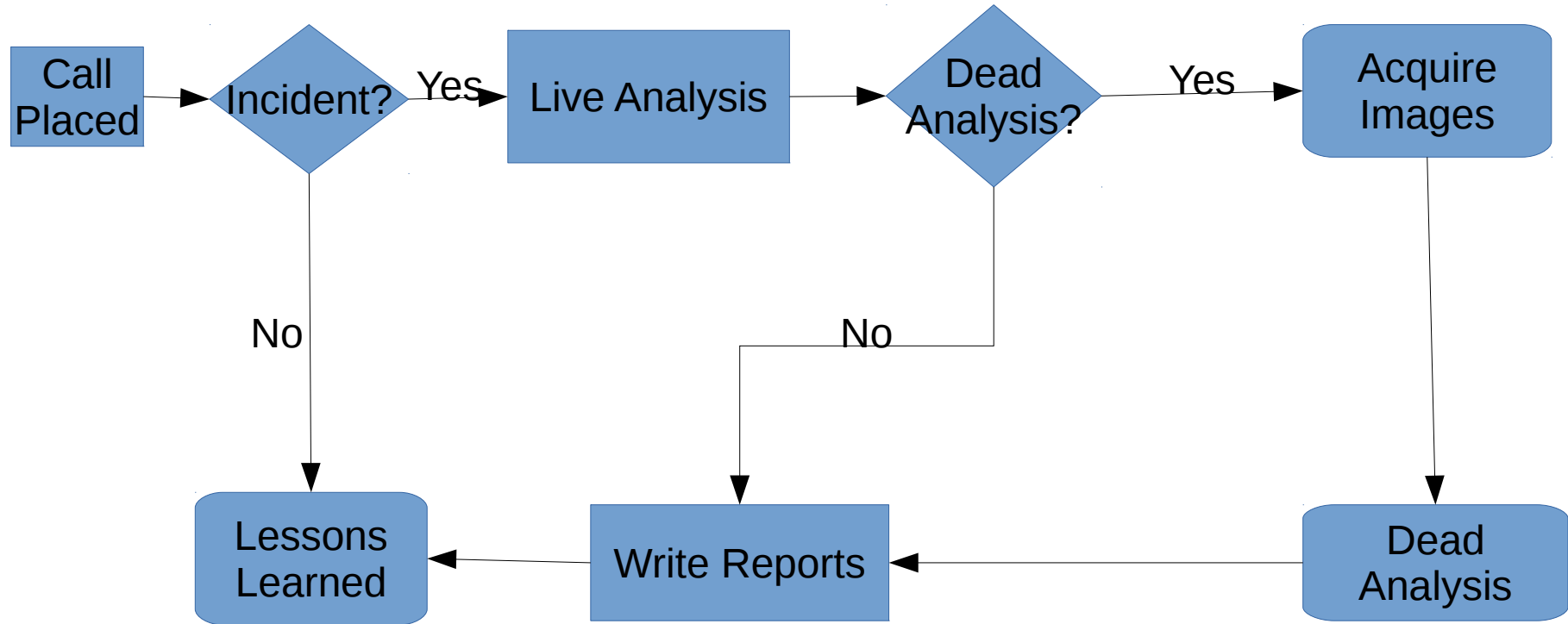
<http://www.securitytube-training.com>

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

©SecurityTube.net

Mounting Images: MBR Basics

High Level Process



Master Boot Record

- Ancient standard (from the 80s)
- Allows up to four partition
- At most one partition can be active (bootable)
- Some partitions may be extended partitions
 - Can contain multiple partitions inside them
 - Partitions are stored in a linked list
- Being replaced with GUID partition tables

Master Boot Record Format

Offset	Length	Item
0 (0x00)	446 (0x1BE)	Boot code
446 (0x1BE)	16 (0x10)	First partition
462 (0x1CE)	16 (0x10)	Second partition
478 (0x1DE)	16 (0x10)	Third partition
494 (0x1EE)	16 (0x10)	Fourth partition
510 (0x1FE)	2 (0x2)	Signature 0x55 0xAA

Partition Record Format

Offset	Length	Item
0 (0x00)	1 (0x01)	Active flag (0x80 = bootable)
1 (0x01)	1 (0x01)	Start head
2 (0x02)	1 (0x01)	Start sector (bits 0-5); upper bits of cylinder (6-7)
3 (0x03)	1 (0x01)	Start cylinder lowest 8 bits
4 (0x04)	1 (0x01)	Partition type code (0x83 = Linux)
5 (0x05)	1 (0x01)	End head
6 (0x06)	1 (0x01)	End sector (bits 0-5); upper bits of cylinder (6-7)
7 (0x07)	1 (0x01)	End cylinder lowest 8 bits
8 (0x08)	4 (0x04)	Sectors preceding partition (little endian)
12 (0x0C)	4 (0x04)	Sectors in partition

Mounting an Image with a MBR