Windows Forensics

Dr. Phil Polstra
PhD, CISSP, CEH

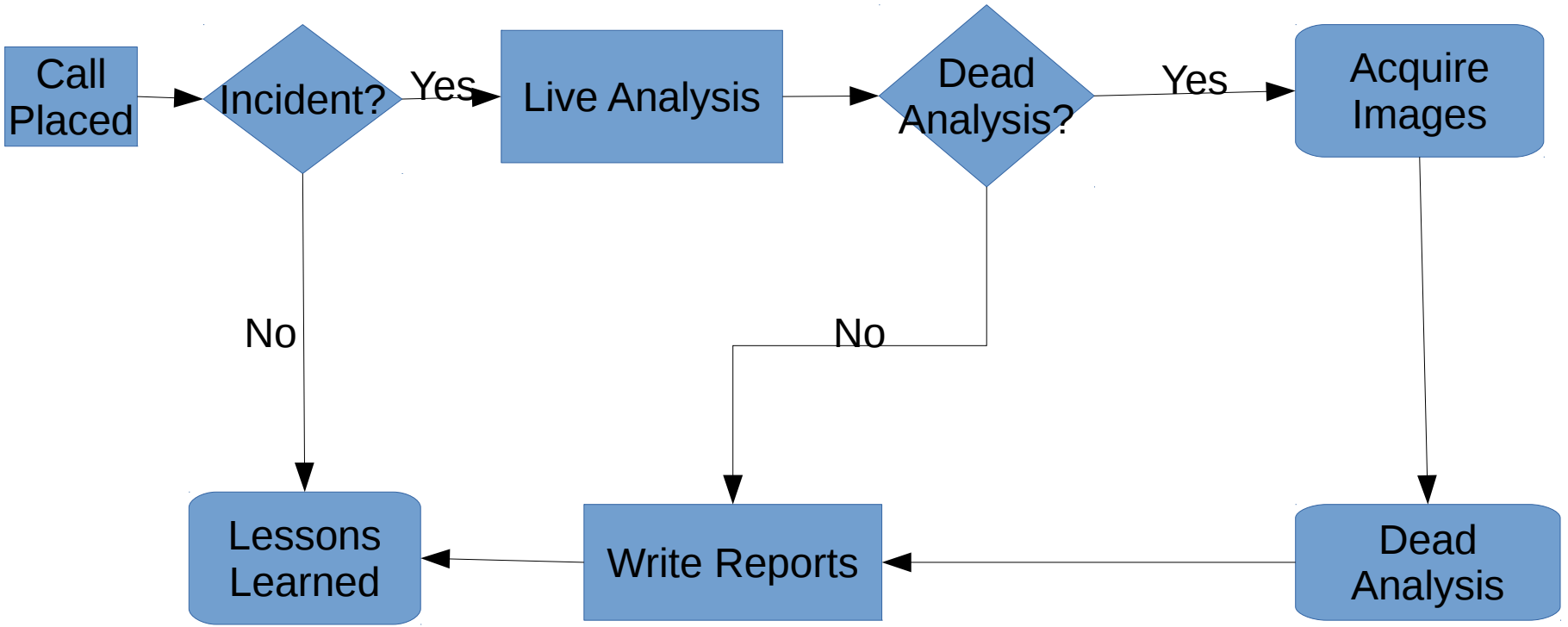
@ppolstra
http://philpolstra.com

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

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

Mounting Images: GUID Partitions

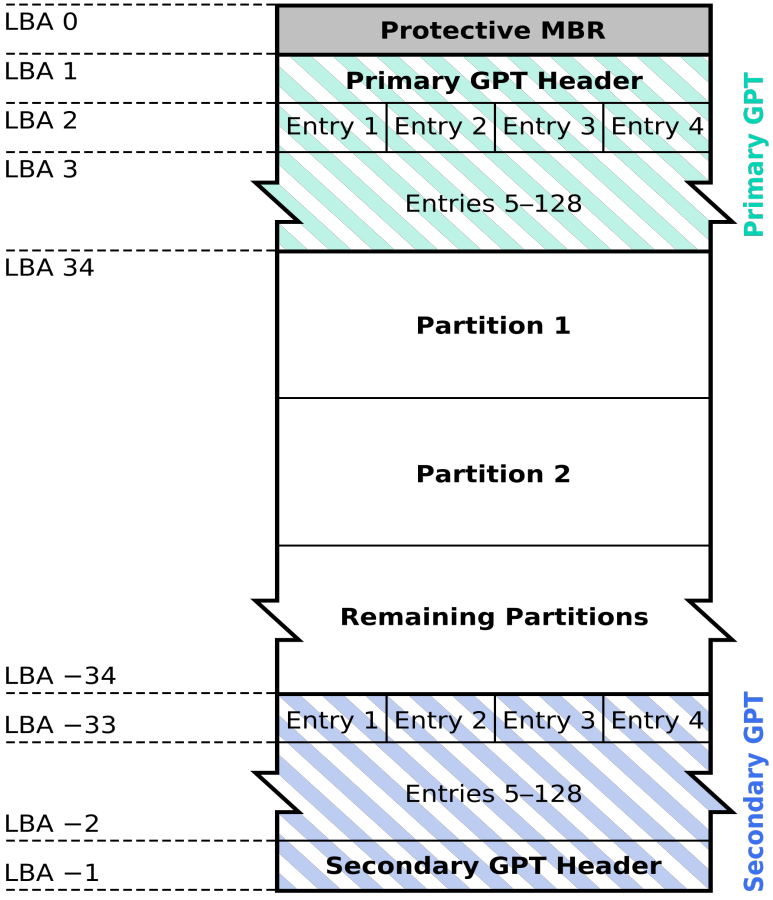
High Level Process



GUID Partitions

- Part of the UEFI system to replace BIOS boot
- Allows up to 128 partitions
- Simple
- The new standard
- All current 64-bit systems ship with this

GUID Partition Tables



Partition Record Format

Offset	Length	Item
0 (0x00	16 (0x10)	Partition type GUID
16 (0x10)	16 (0x10)	Unique partition GUID
32 (0x20)	8 (0x08)	First LBA
40 (0x28)	8 (0x08)	Last LBA
48 (0x30)	8 (0x08)	Attributes
56 (0x38)	72 (0x48)	Partition name

Partition Attributes

Bit	Content	Description
0	System partition	Must preserve partition as is
1	EFI Firmware	Operating system should ignore this partition
2	Legacy BIOS boot	Equivalent to 0x80 in MBR
3-47	Reserved	Should be zeros
48-63	Type specific	Varies by partition type (60=RO, 62=Hidden, 63=No automount for Windows)

Mounting GUID partitions