CEIC® 2013

UEFI, MBR and GPT oh my!

Jonathan Rajewski
Champlain College

www.ceicconference.com

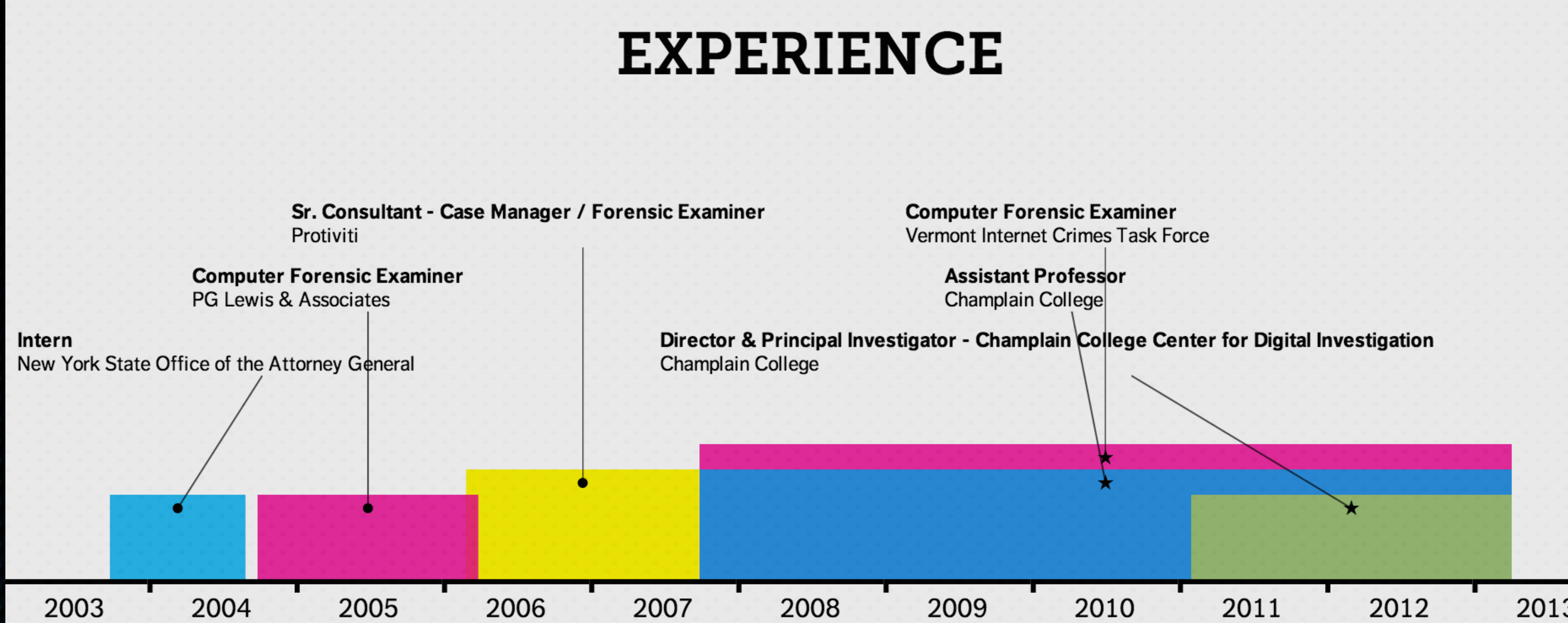
#CEIC2013

Overview

A current copy of this presentation can be obtained from the Print Stations/Mobile App or jonrajewski.com/resources

CEIC 2013

- Explore BIOS/GUID
- Delve into the world of partitioning schemes
- Discuss MBR
- Discuss GPT
- GPT Challenge
- Questions



About Jon

@jtrajewski

Leahy Center for Digital Investigation
at CHAMPLAIN COLLEGE

Jonathan T. Rajewski, MS, CCE, EnCe, CISSP, CFE
Assistant Professor, Digital Forensics, Champlain College
Director/Principal Investigator, Senator Patrick Leahy Center for Digital Investigation (LCDI)
Digital Forensic Examiner, Vermont Internet Crimes Task Force

Champlain College
West Hall
163 South Willard Street
Burlington, VT 05401
Office: +1 802-865-5460
Google Voice - +1 802-318-4804
Mobile - Available via request
Skype – jtrajewski

Jonrajewski.com/cyberblog

rajewski@champlain.edu
jtrajewski@gmail.com

PGP Public Key: Located on keyserver.pgp.com

SC MAGAZINE AWARDS 2013 WINNER Honored in the U.S.

twitter

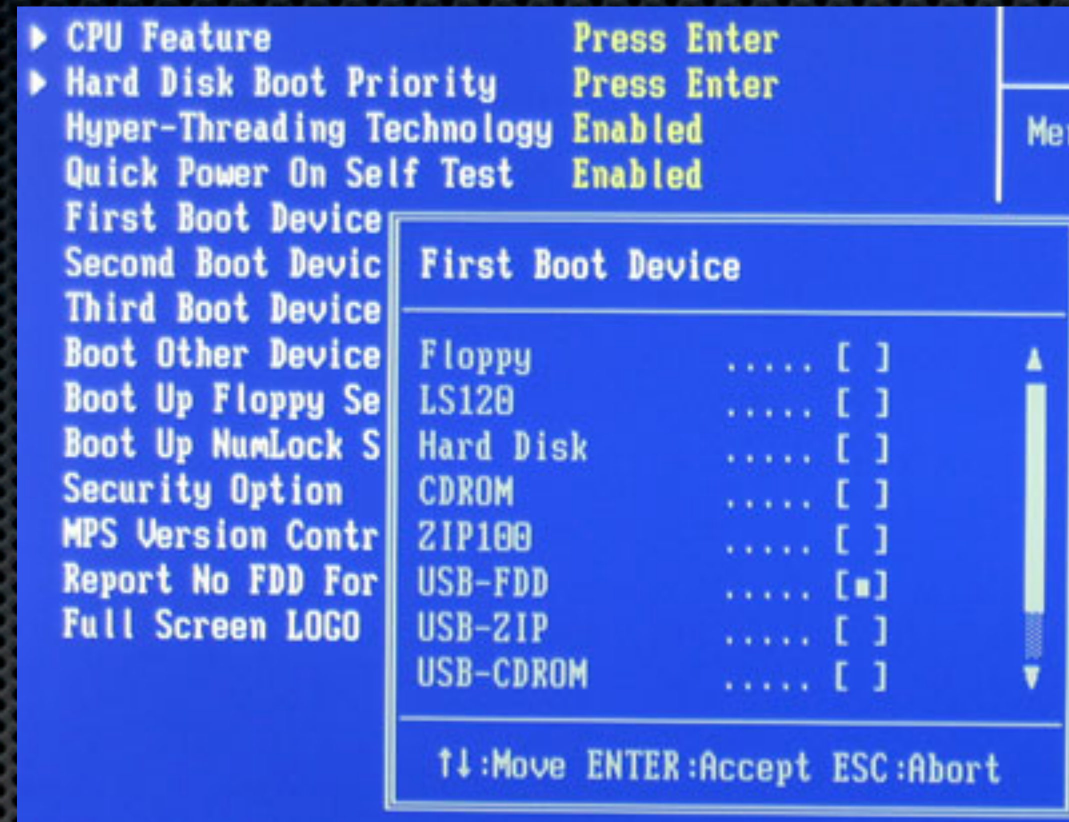
#CEIC_GPT

@jtrajewski

Let’s jump into the fun stuff


POWER


GEAR LIVE

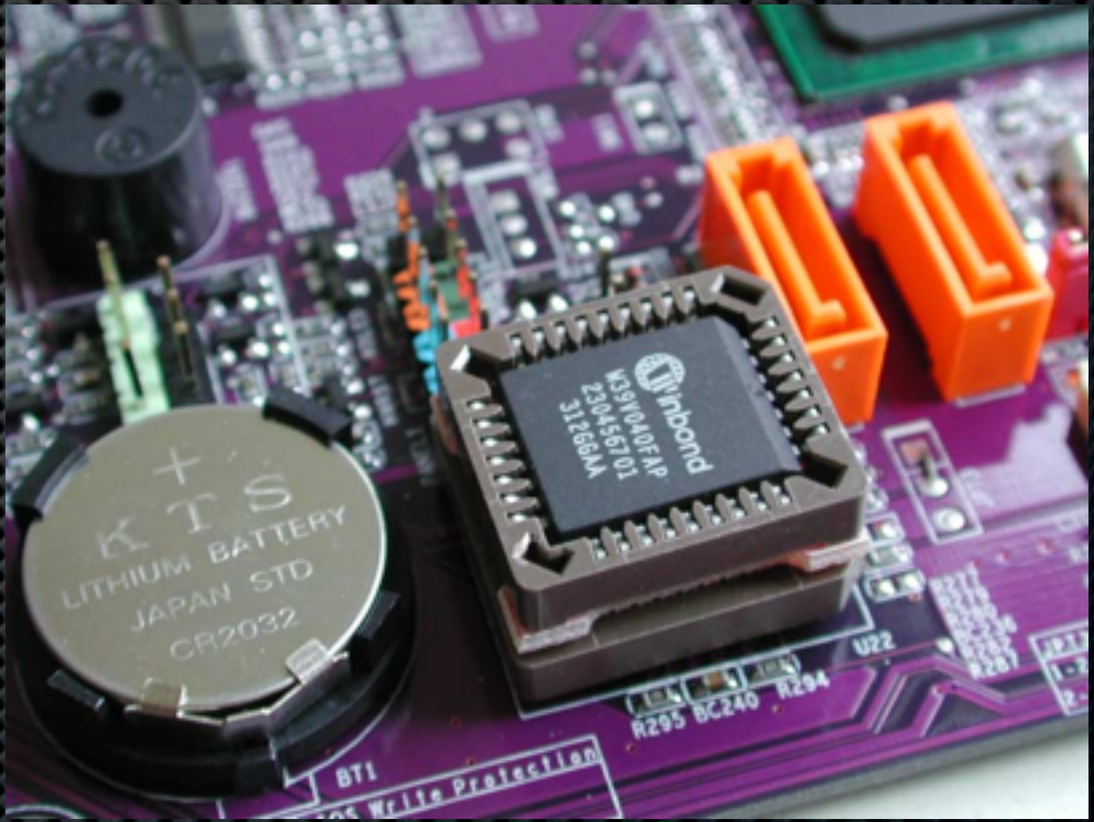


Memory

- SSD
- HDD
- DVD/CD
- NAND

BIOS

- Basic Input and Output System
- Purpose?



BIOS

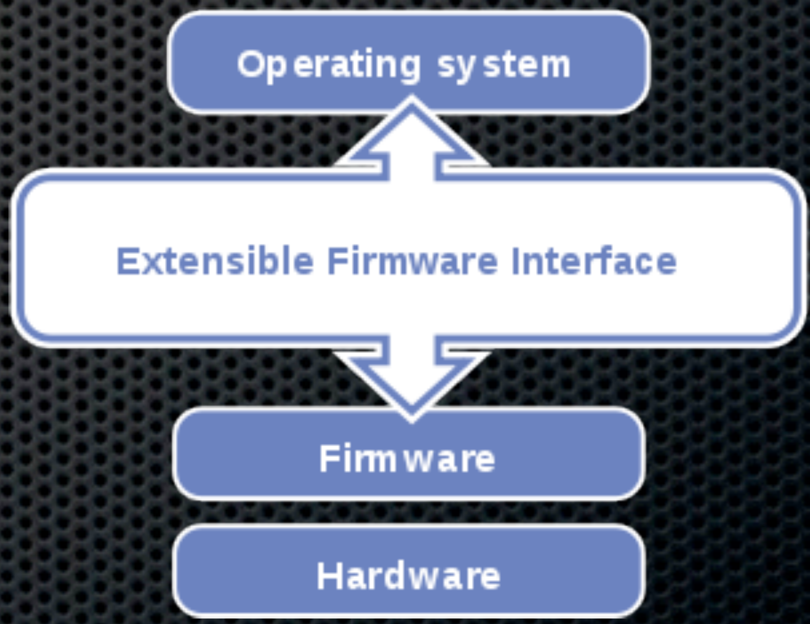
- What is it doing?
  - Check for peripherals
  - Finds boot device
  - Passes control to MBR

BIOS

What other capabilities does the BIOS have?

UEFI

- Unified Extensible Firmware Interface
- Next generation BIOS



UEFI

- Enhancement!
- Has it's own device drivers
  - Can read and mount partitions
- Provides many more options and flexibility when compared to BIOS

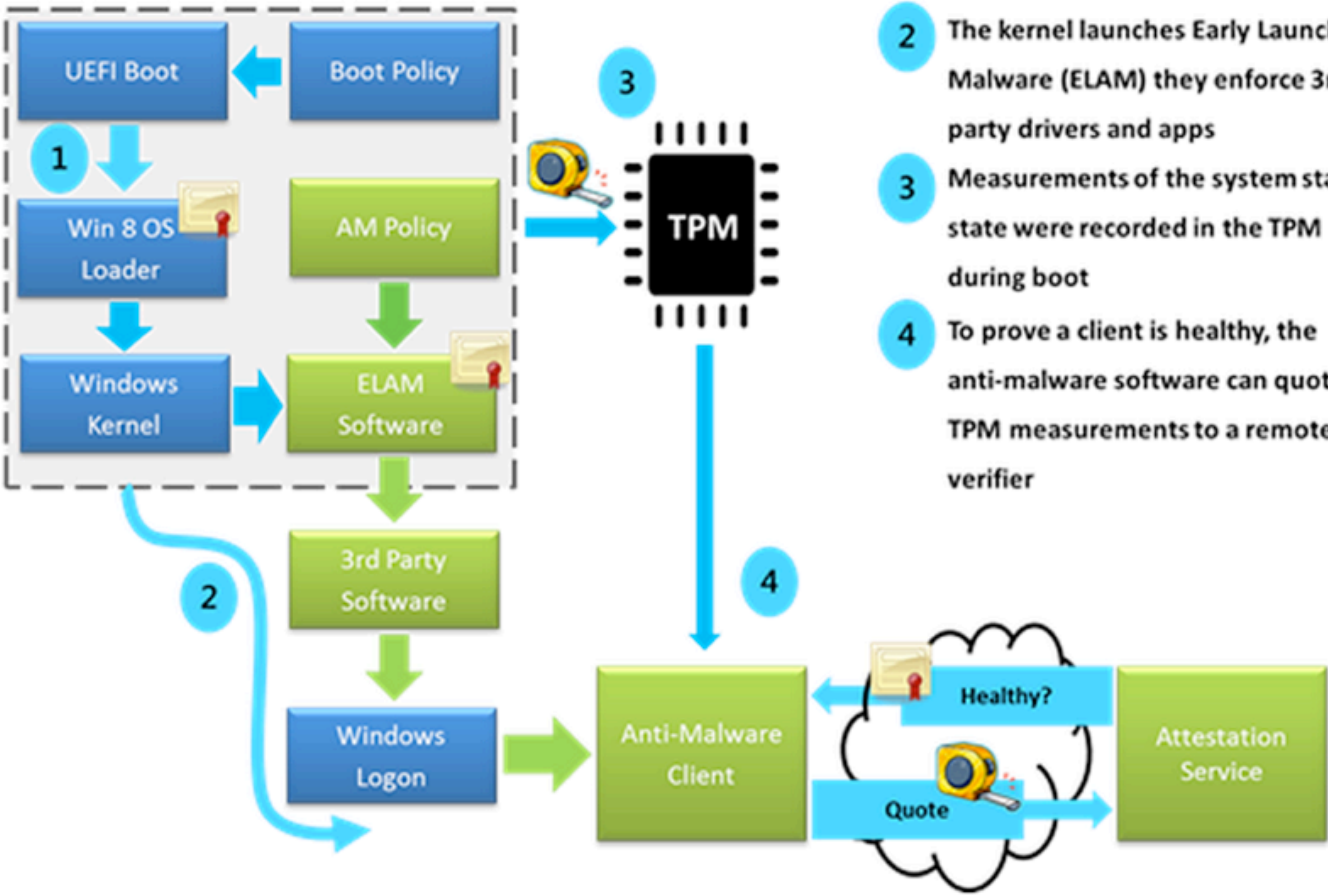
Why should we use UEFI?

- Rootkit prevention
  - UEFI supports Authenticode digital signatures in the pre-OS environment
    - Certificate Authority - Signing environment
    - Whitelist/Blacklist
- Network Authentication
  - Client/Server authentication on the motherboard!

Wait a second...

- Pre-OS environment?
  - What about booting from USB with a Linux distribution to access a disk directly?

Windows 8 Platform Integrity Architecture



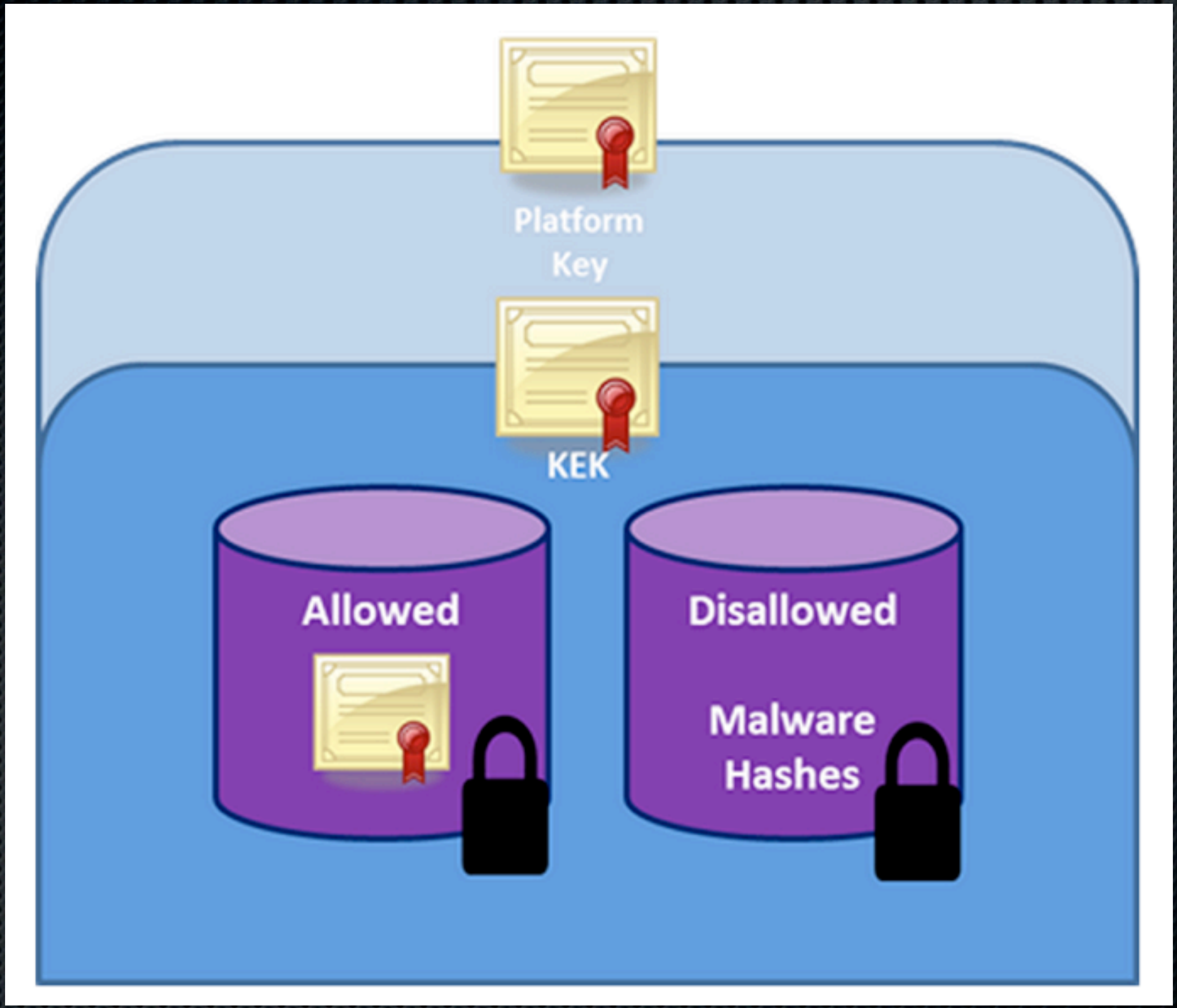
1. Secure boot (UEFI) prevents running a unknown OS loader
2. The kernel launches Early Launch Anti-Malware (ELAM) they enforce 3rd party drivers and apps
3. Measurements of the system start state were recorded in the TPM during boot
4. To prove a client is healthy, the anti-malware software can quote TPM measurements to a remote verifier

[1]

- The BIOS starts any OS loader, even malware

- UEFI will only launch a verified OS loader – such as in Windows 8
- Malware cannot switch the boot loader

[1]



[1]

Microsoft Windows 8 UEFI Secure Boot complaint: The case for and against

Summary: *A Linux user group filed a complaint with the European Commission alleging Microsoft's UEFI practices violate antitrust laws. Does the complaint have legs?*

By Liam Tung | March 28, 2013 -- 14:57 GMT (07:57 PDT)

Follow @liamT

James Bottomley's random Pages

A collection of information

HOME UEFI SECURE BOOT

Owning your Windows 8 UEFI Platform

15 Replies

Even if you only ever plan to run Windows or stock distributions of Linux that already have secure boot support, I'd encourage everybody who has a new UEFI secure boot platform to take ownership of it. The way you do this is by installing your own Platform Key. Once you

Building Windows 8

An inside look from the Windows engineering team

MSDN Blogs > Building Windows 8 > Protecting the pre-OS environment with UEFI

Protecting the pre-OS environment with UEFI

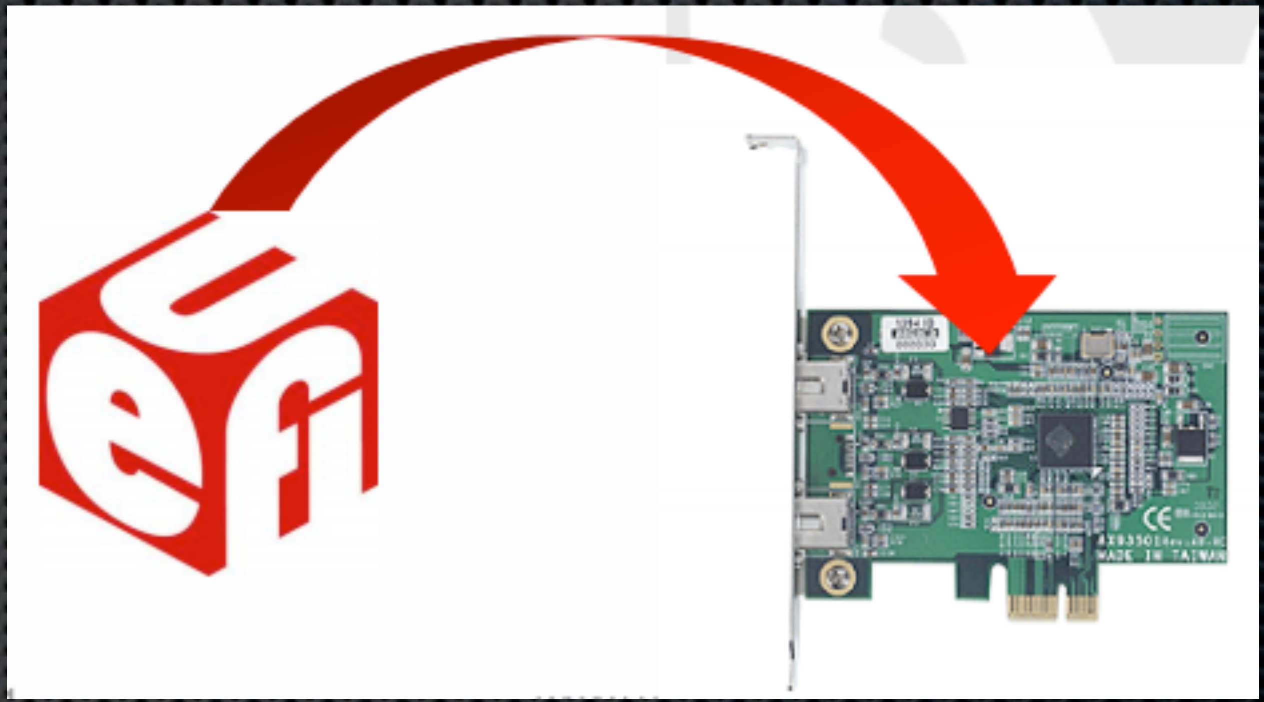
Steven Sinofsky Published Thursday, September 22, 2011 6:00 PM

186 comments

[1] [2] [3]

Wait a second...

- What about ROM?
  - Factory provisioning?




We then polish
and texture them.

A quick aside...

AMI's UEFI Signing Key and BIOS Source Code Leaked

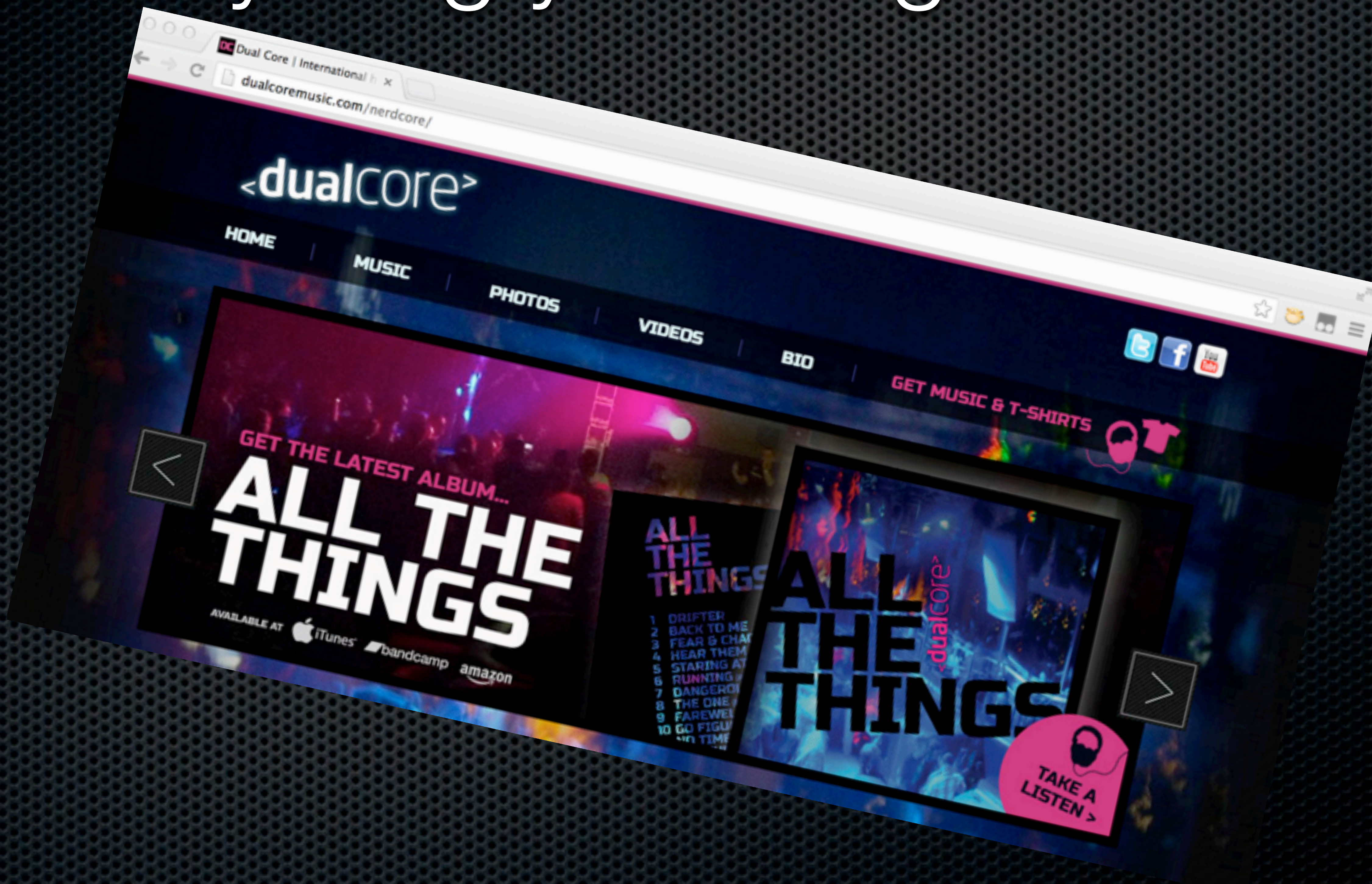
22 COMMENTS

By Tarun Iyer APRIL 8, 2013 6:00 PM - Source: Adam Caudill's Blog

A publicly accessible FTP server in Taiwan has leaked the source code for AMI's Aptio UEFI BIOS.

AMI's Aptio UEFI BIOS source code and its unique UEFI signing key has been leaked onto a publicly accessible FTP server in Taiwan, an event that may have compromised the security of every motherboard running AMI Aptio. The release of the latter item malware gives developers the ability to develop "signed" malicious BIOS updates, replace legitimate system BIOS updates, and gain access to most ring-0 OS functions.

Then we backdoor the firmware on anything you bring...

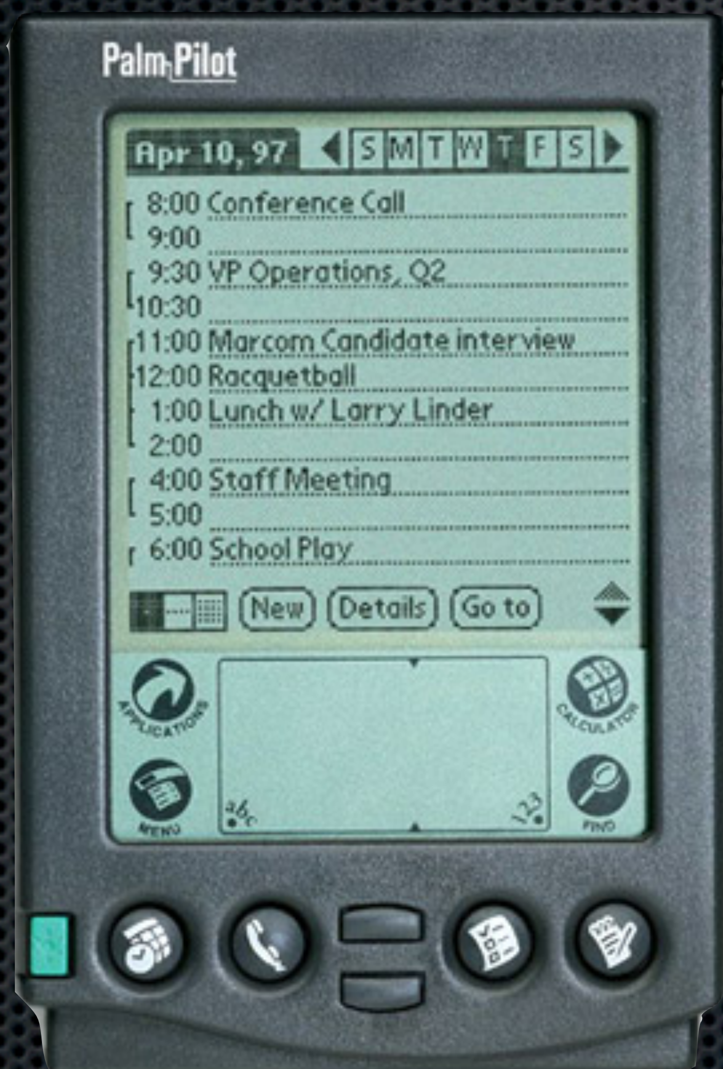


So what's next?

Power → Bios/UEFI → ?

MBR

GUID

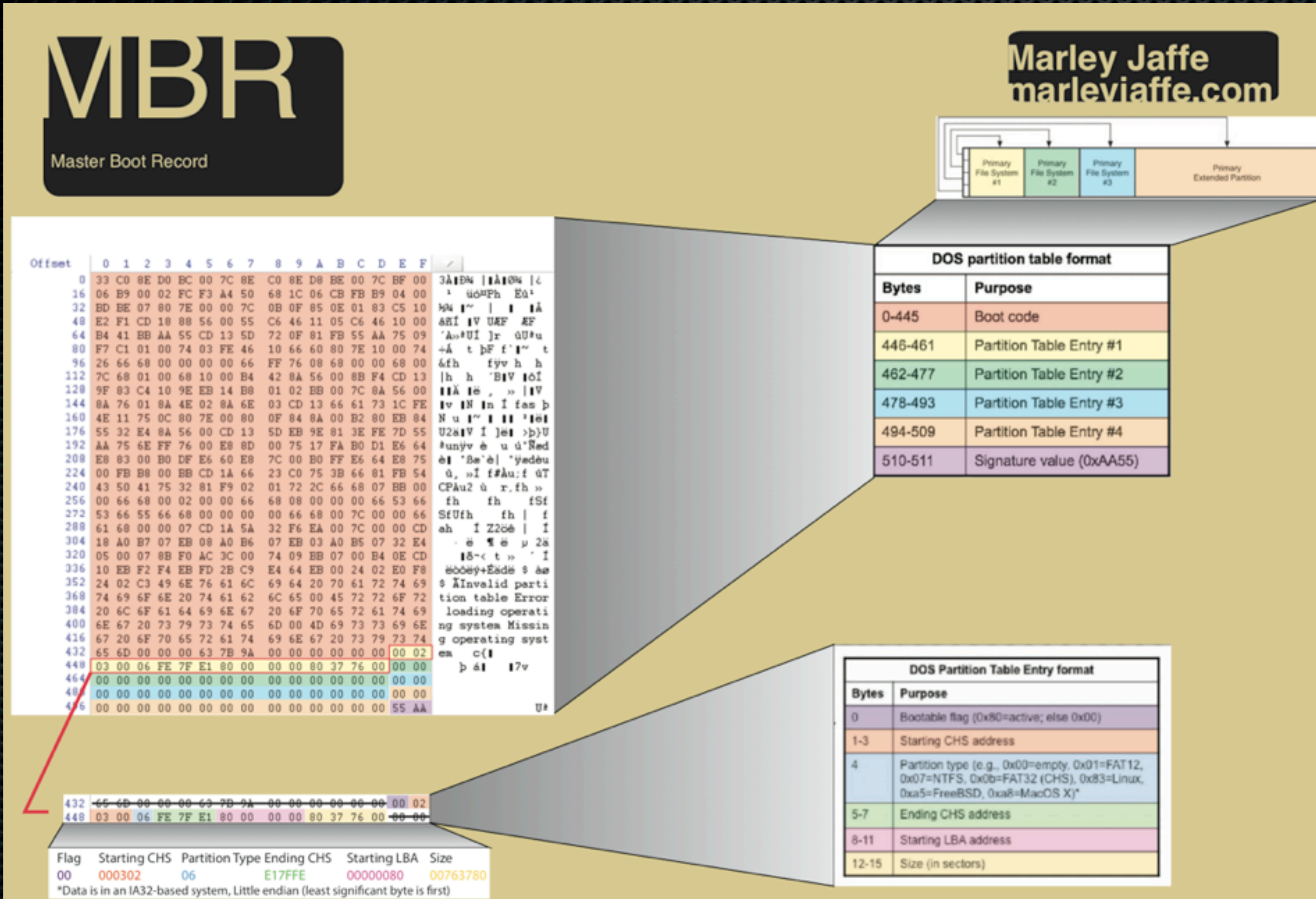


PalmPilot
Apr 10, 97
S M T W T F S
8:00 Conference Call
9:00
9:30 VP Operations, Q2
10:30
11:00 Marcom Candidate interview
12:00 Racquetball
1:00 Lunch w/ Larry Linder
2:00
4:00 Staff Meeting
5:00
6:00 School Play
New
Details
Go to

A quick aside...

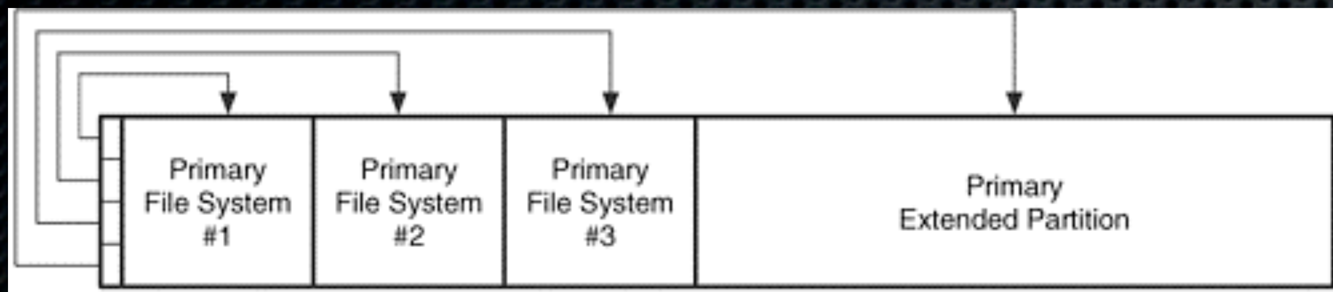
- Complied list of tools/scripts/resources for MBR/GPT analysis
  - http://www.jonrajewski.com/resources/
  - In the “Speaker Presentations” folder you will find
    - Evidence Files
    - MBR/GPT Resource
    - Presentation

“MBR/GPT Resource”



Sunday, May 19, 13

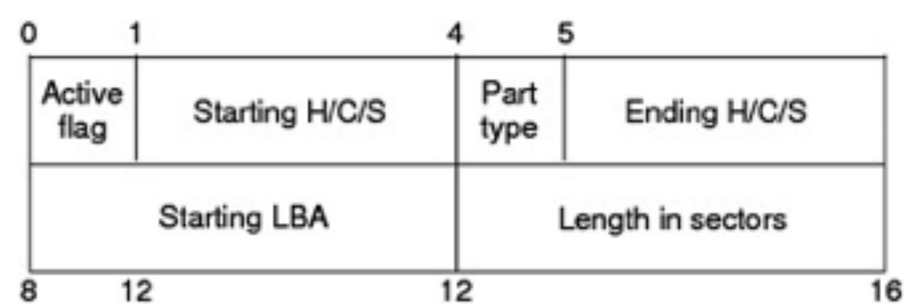
MBR



Partition Table

DOS partition table format	
Bytes	**Purpose**
0-445	Boot code
446-461	Partition Table Entry #1
462-477	Partition Table Entry #2
478-493	Partition Table Entry #3
494-509	Partition Table Entry #4
510-511	Signature value (0xAA55)

DOS Partition Table Entry format	
Bytes	**Purpose**
0	Bootable flag (0x80=active; else 0x00)
1-3	Starting CHS address
4	Partition type (e.g., 0x00=empty, 0x01=FAT12, 0x07=NTFS, 0x0b=FAT32 (CHS), 0x83=Linux, 0xa5=FreeBSD, 0xa8=MacOS X)*
5-7	Ending CHS address
8-11	Starting LBA address
12-15	Size (in sectors)



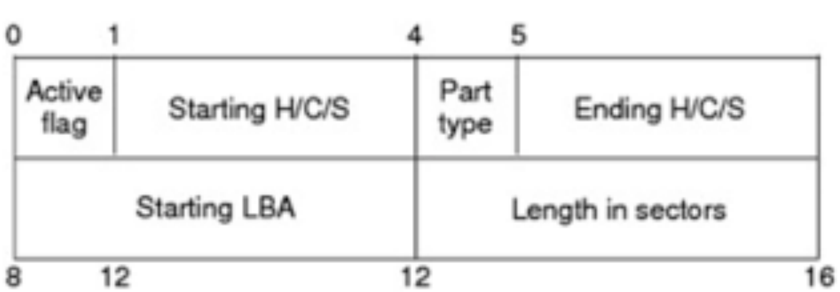
Offset	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	Access ▼
0000000000	33	C0	8E	D0	BC	00	7C	FB	50	07	50	1F	FC	BE	1B	7C	3À▮Ð¼ |ûP P ü¾ |
0000000010	BF	1B	06	50	57	B9	E5	01	F3	A4	CB	BD	BE	07	B1	04	¿ PW¹å ó¤Ë½¾ ±
0000000020	38	6E	00	7C	09	75	13	83	C5	10	E2	F4	CD	18	8B	F5	8n | u ▮Å âôÍ ▮õ
0000000030	83	C6	10	49	74	19	38	2C	74	F6	A0	B5	07	B4	07	8B	▮Æ It 8,tö µ ´ ▮
0000000040	F0	AC	3C	00	74	FC	BB	07	00	B4	0E	CD	10	EB	F2	88	ð¬< tü» ´ Í ëò▮
0000000050	4E	10	E8	46	00	73	2A	FE	46	10	80	7E	04	0B	74	0B	N èF s*þF ▮~ t
0000000060	80	7E	04	0C	74	05	A0	B6	07	75	D2	80	46	02	06	83	▮~ t ¶ uÒ▮F ▮
0000000070	46	08	06	83	56	0A	00	E8	21	00	73	05	A0	B6	07	EB	F ▮V è! s ¶ ë
0000000080	BC	81	3E	FE	7D	55	AA	74	0B	80	7E	10	00	74	C8	A0	¼▮>þ}Uªt ▮~ tÈ
0000000090	B7	07	EB	A9	8B	FC	1E	57	8B	F5	CB	BF	05	00	8A	56	· ë©▮ü W▮õË¿ ▮V
00000000A0	00	B4	08	CD	13	72	23	8A	C1	24	3F	98	8A	DE	8A	FC	´ Í r#▮Á$?▮▮Þ▮ü
00000000B0	43	F7	E3	8B	D1	86	D6	B1	06	D2	EE	42	F7	E2	39	56	C÷ã▮Ñ▮Ö± ÒîB÷â9V
00000000C0	0A	77	23	72	05	39	46	08	73	1C	B8	01	02	BB	00	7C	w#r 9F s ¸ » |
00000000D0	8B	4E	02	8B	56	00	CD	13	73	51	4F	74	4E	32	E4	8A	▮N ▮V Í sQOtN2ä▮
00000000E0	56	00	CD	13	EB	E4	8A	56	00	60	BB	AA	55	B4	41	CD	V Í ëä▮V `»ªU´AÍ
00000000F0	13	72	36	81	FB	55	AA	75	30	F6	C1	01	74	2B	61	60	r6▮ûUªu0öÁ t+a`
0000000100	6A	00	6A	00	FF	76	0A	FF	76	08	6A	00	68	00	7C	6A	j j ÿv ÿv j h |j
0000000110	01	6A	10	B4	42	8B	F4	CD	13	61	61	73	0E	4F	74	0B	j ´B▮ôÍ aas Ot
0000000120	32	E4	8A	56	00	CD	13	EB	D6	61	F9	C3	49	6E	76	61	2ä▮V Í ëÖaùÃInva
0000000130	6C	69	64	20	70	61	72	74	69	74	69	6F	6E	20	74	61	lid partition ta
0000000140	62	6C	65	00	45	72	72	6F	72	20	6C	6F	61	64	69	6E	ble Error loadin
0000000150	67	20	6F	70	65	72	61	74	69	6E	67	20	73	79	73	74	g operating syst
0000000160	65	6D	00	4D	69	73	73	69	6E	67	20	6F	70	65	72	61	em Missing opera
0000000170	74	69	6E	67	20	73	79	73	74	65	6D	00	00	00	00	00	ting system
0000000180	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
0000000190	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
00000001A0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
00000001B0	00	00	00	00	00	2C	44	63	16	23	AB	41	00	00	00	01	,Dc #«A
00000001C0	01	00	DE	FE	3F	05	3F	00	00	00	47	78	01	00	80	00	Þþ? ? Gx ▮
00000001D0	01	06	07	FE	FF	FF	86	78	01	00	7A	2D	4F	09	00	00	þÿÿ▮x z-O
00000001E0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
00000001F0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	55	AA	Uª

Offset	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0000000000	33	C0	8E	D0	BC	00	7C	FB	50	07	50	1F	FC	BE	1B	7C
0000000010	BF	1B	06	50	57	B9	E5	01	F3	A4	CB	BD	BE	07	B1	04
0000000020	38	6E	00	7C	09	75	13	83	C5	10	E2	F4	CD	18	8B	F5
0000000030	83	C6	10	49	74	19	38	2C	74	F6	A0	B5	07	B4	07	8B
0000000040	F0	AC	3C	00	74	FC	BB	07	00	B4	0E	CD	10	EB	F2	88
0000000050	4E	10	E8	46	00	73	2A	FE	46	10	80	7E	04	0B	74	0B
0000000060	80	7E	04	0C	74	05	A0	B6	07	75	D2	80	46	02	06	83
0000000070	46	08	06	83	56	0A	00	E8	21	00	73	05	A0	B6	07	EB
0000000080	BC	81	3E	FE	7D	55	AA	74	0B	80	7E	10	00	74	C8	A0
0000000090	B7	07	EB	A9	8B	FC	1E	57	8B	F5	CB	BF	05	00	8A	56
00000000A0	00	B4	08	CD	13	72	23	8A	C1	24	3F	98	8A	DE	8A	FC
00000000B0	43	F7	E3	8B	D1	86	D6	B1	06	D2	EE	42	F7	E2	39	56
00000000C0	0A	77	23	72	05	39	46	08	73	1C	B8	01	02	BB	00	7C
00000000D0	8B	4E	02	8B	56	00	CD	13	73	51	4F	74	4E	32	E4	8A
00000000E0	56	00	CD	13	EB	E4	8A	56	00	60	BB	AA	55	B4	41	CD
00000000F0	13	72	36	81	FB	55	AA	75	30	F6	C1	01	74	2B	61	60
0000000100	6A	00	6A	00	FF	76	0A	FF	76	08	6A	00	68	00	7C	6A
0000000110	01	6A	10	B4	42	8B	F4	CD	13	61	61	73	0E	4F	74	0B
0000000120	32	E4	8A	56	00	CD	13	EB	D6	61	F9	C3	49	6E	76	61
0000000130	6C	69	64	20	70	61	72	74	69	74	69	6F	6E	20	74	61
0000000140	62	6C	65	00	45	72	72	6F	72	20	6C	6F	61	64	69	6E
0000000150	67	20	6F	70	65	72	61	74	69	6E	67	20	73	79	73	74
0000000160	65	6D	00	4D	69	73	73	69	6E	67	20	6F	70	65	72	61
0000000170	74	69	6E	67	20	73	79	73	74	65	6D	00	00	00	00	00
0000000180	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
0000000190	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
00000001A0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
00000001B0	00	00	00	00	00	2C	44	63	16	23	AB	41	00	00	00	01
00000001C0	01	00	DE	FE	3F	05	3F	00	00	00	47	78	01	00	80	00
00000001D0	01	06	07	FE	FF	FF	86	78	01	00	7A	2D	4F	09	00	00
00000001E0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
00000001F0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	55	AA

Access

```
3À▌Ð¼ |ûP P ü¾ |
¿ PW¹å ó¤Ë½¾ ±
8n | u ▌Å âôÍ ▌õ
▌Æ It 8,tö µ ´ ▌
ð¬< tü» ´ Í ëò▌
N èF s*þF ▌~ t
▌~ t ¶ uÒ▌F ▌
F ▌V è! s ¶ ë
¼▌>þ}Uªt ▌~ tÈ
· ë©▌ü W▌õË¿ ▌V
´ Í r#▌Á$?▌▌Þ▌ü
C÷ã▌Ñ▌Ö± ÒîB÷â9V
w#r 9F s ¸ » |
▌N ▌V Í sQOtN2ä▌
V Í ëä▌V `»ªU´AÍ
r6▌ûUªu0öÁ t+a`
j j ÿv ÿv j h |j
j ´B▌ôÍ aas Ot
2ä▌V Í ëÖaùÃInva
lid partition ta
ble Error loadin
g operating syst
em Missing opera
ting system



,Dc #«A
Þþ? ? Gx ▌
þÿÿ▌x z-O

Uª
```

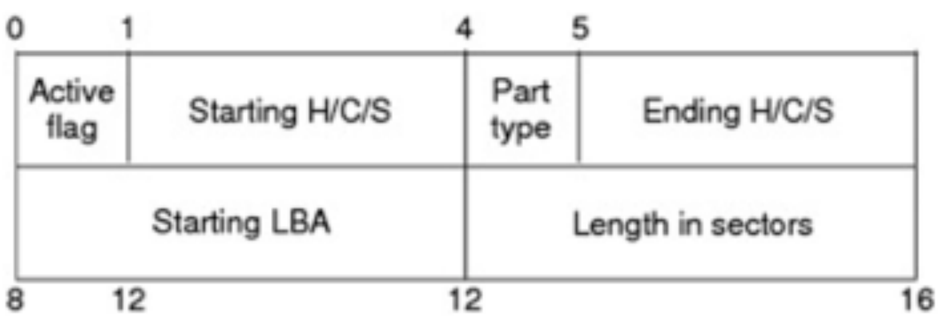
DOS Partition Table Entry format	
Bytes	**Purpose**
0	Bootable flag (0x80=active; else 0x00)
1-3	Starting CHS address
4	Partition type (e.g., 0x00=empty, 0x01=FAT12, 0x07=NTFS, 0x0b=FAT32 (CHS), 0x83=Linux, 0xa5=FreeBSD, 0xa8=MacOS X)*
5-7	Ending CHS address
8-11	Starting LBA address
12-15	Size (in sectors)



```
0001 0100 07fe 3f7f 3f00 0000 4160 1f00
8000 0180 83fe 3f8c 8060 1f00 cd2f 0300
0000 018d 83fe 3fcc 4d90 2200 40b0 0f00
0000 01cd 05fe ffff 8d40 3200 79eb 9604
```

* Data is in an IA32-based system – little-endian – least significant byte is first

DOS Partition Table Entry format	
Bytes	**Purpose**
0	Bootable flag (0x80=active; else 0x00)
1-3	Starting CHS address
4	Partition type (e.g., 0x00=empty, 0x01=FAT12, 0x07=NTFS, 0x0b=FAT32 (CHS), 0x83=Linux, 0xa5=FreeBSD, 0xa8=MacOS X)*
5-7	Ending CHS address
8-11	Starting LBA address
12-15	Size (in sectors)



	Flag	Type	Starting Sector	Size
1	0	07	0000003f	001F6041
2				
3				
4				

Adopted from Carrier

Partition	Flag	Type	Starting Sector	Size
1	00	07	0000003f (63)	001f6041(2056257)
2	80	83	001f6080 (2056320)	00032fcd(208845)
3	00	83	0022904d (2265165)	000fb040 (1028160)
4	00	05	0032408d (3293325)	0496eb79 (76999545)

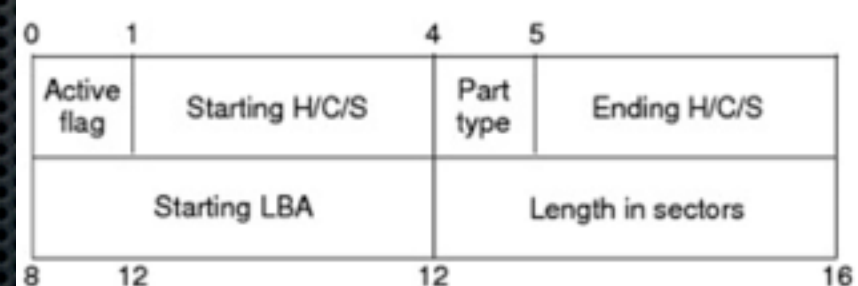
Adopted from Carrier

Let’s try it again!

How large is the first partition?
Sector size is 512 B

Offset	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	
0000000000	FA	33	C0	8E	D0	BC	00	7C	8B	F4	50	07	50	1F	FB	FC	ú3À▮Ð¼ |▮ôP P ûü
0000000016	BF	00	06	B9	00	01	F2	A5	EA	1D	06	00	00	BE	BE	07	¿ ¹ ò¥ê ¾¾
0000000032	B3	04	80	3C	80	74	0E	80	3C	00	75	1C	83	C6	10	FE	³ ▮<▮t ▮< u ▮Æ þ
0000000048	CB	75	EF	CD	18	8B	14	8B	4C	02	8B	EE	83	C6	10	FE	ËuïÍ ▮ ▮L ▮î▮Æ þ
0000000064	CB	74	1A	80	3C	00	74	F4	BE	8B	06	AC	3C	00	74	0B	Ët ▮< tô¾▮ ¬< t
0000000080	56	BB	07	00	B4	0E	CD	10	5E	EB	F0	EB	FE	BF	05	00	V» ´ Í ^ëðëþ¿
0000000096	BB	00	7C	B8	01	02	57	CD	13	5F	73	0C	33	C0	CD	13	» |¸ WÍ _s 3ÀÍ
0000000112	4F	75	ED	BE	A3	06	EB	D3	BE	C2	06	BF	FE	7D	81	3D	Ouí¾£ ëÓ¾Â ¿þ} =
0000000128	55	AA	75	C7	8B	F5	EA	00	7C	00	00	49	6E	76	61	6C	UªuÇ▮õê | Inval
0000000144	69	64	20	70	61	72	74	69	74	69	6F	6E	20	74	61	62	id partition tab
0000000160	6C	65	00	45	72	72	6F	72	20	6C	6F	61	64	69	6E	67	le Error loading
0000000176	20	6F	70	65	72	61	74	69	6E	67	20	73	79	73	74	65	operating syste
0000000192	6D	00	4D	69	73	73	69	6E	67	20	6F	70	65	72	61	74	m Missing operat
0000000208	69	6E	67	20	73	79	73	74	65	6D	00	00	00	00	00	00	ing system
0000000224	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
0000000240	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
0000000256	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
0000000272	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
0000000288	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
0000000304	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
0000000320	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
0000000336	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
0000000352	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
0000000368	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
0000000384	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
0000000400	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
0000000416	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
0000000432	00	00	00	00	00	00	00	00	E5	D4	03	00	00	00	80	01	åÔ ▮
0000000448	01	00	06	01	FF	FF	20	00	00	00	E0	93	3E	00	00	00	ÿÿ à▮>
0000000464	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
0000000480	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
0000000496	00	00	00	00	00	00	00	00	00	00	00	00	00	00	55	AA	Uª

DOS Partition Table Entry format	
Bytes	**Purpose**
0	Bootable flag (0x80=active; else 0x00)
1-3	Starting CHS address
4	Partition type (e.g., 0x00=empty, 0x01=FAT12, 0x07=NTFS, 0x0b=FAT32 (CHS), 0x83=Linux, 0xa5=FreeBSD, 0xa8=MacOS X)*
5-7	Ending CHS address
8-11	Starting LBA address
12-15	Size (in sectors)



80 01 01 00 06 FF FF 20 00 00 00 E0 93 3E 00

Sunday, May 19, 13

Offset	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	
0000000000	FA	33	C0	8E	D0	BC	00	7C	8B	F4	50	07	50	1F	FB	FC	ú3À▮Ð¼ |▮ôP P ûü
0000000016	BF	00	06	B9	00	01	F2	A5	EA	1D	06	00	00	BE	BE	07	¿ ¹ ò¥ê ¾¾
0000000032	B3	04	80	3C	80	74	0E	80	3C	00	75	1C	83	C6	10	FE	³ ▮<▮t ▮< u ▮Æ þ
0000000048	CB	75	EF	CD	18	8B	14	8B	4C	02	8B	EE	83	C6	10	FE	ËuïÍ ▮ ▮L ▮î▮Æ þ
0000000064	CB	74	1A	80	3C	00	74	F4	BE	8B	06	AC	3C	00	74	0B	Ët ▮< tô¾▮ ¬< t
0000000080	56	BB	07	00	B4	0E	CD	10	5E	EB	F0	EB	FE	BF	05	00	V» ´ Í ^ëðëþ¿
0000000096	BB	00	7C	B8	01	02	57	CD	13	5F	73	0C	33	C0	CD	13	» |¸ WÍ _s 3ÀÍ
0000000112	4F	75	ED	BE	A3	06	EB	D3	BE	C2	06	BF	FE	7D	81	3D	Ouí¾£ ëÓ¾Â ¿þ} =
0000000128	55	AA	75	C7	8B	F5	EA	00	7C	00	00	49	6E	76	61	6C	Uªuǋõê | Inval
0000000144	69	64	20	70	61	72	74	69	74	69	6F	6E	20	74	61	62	id partition tab
0000000160	6C	65	00	45	72	72	6F	72	20	6C	6F	61	64	69	6E	67	le Error loading
0000000176	20	6F	70	65	72	61	74	69	6E	67	20	73	79	73	74	65	operating syste
0000000192	6D	00	4D	69	73	73	69	6E	67	20	6F	70	65	72	61	74	m Missing operat
0000000208	69	6E	67	20	73	79	73	74	65	6D	00	00	00	00	00	00	ing system
0000000224	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
0000000240	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
0000000256	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
0000000272	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
0000000288	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
0000000304	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
0000000320	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
0000000336	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
0000000352	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
0000000368	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
0000000384	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
0000000400	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
0000000416	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
0000000432	00	00	00	00	00	00	00	00	E5	D4	03	00	00	00	80	01	åÔ ▮
0000000448	01	00	06	01	FF	FF	20	00	00	00	E0	93	3E	00	00	00	ÿÿ à▮>
0000000464	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
0000000480	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
0000000496	00	00	00	00	00	00	00	00	00	00	00	00	00	00	55	AA	Uª

80 01 01 00 06 01 FF FF 20 00 00 00 E0 93 3E 00

0x003E93E0

4101088 sectors

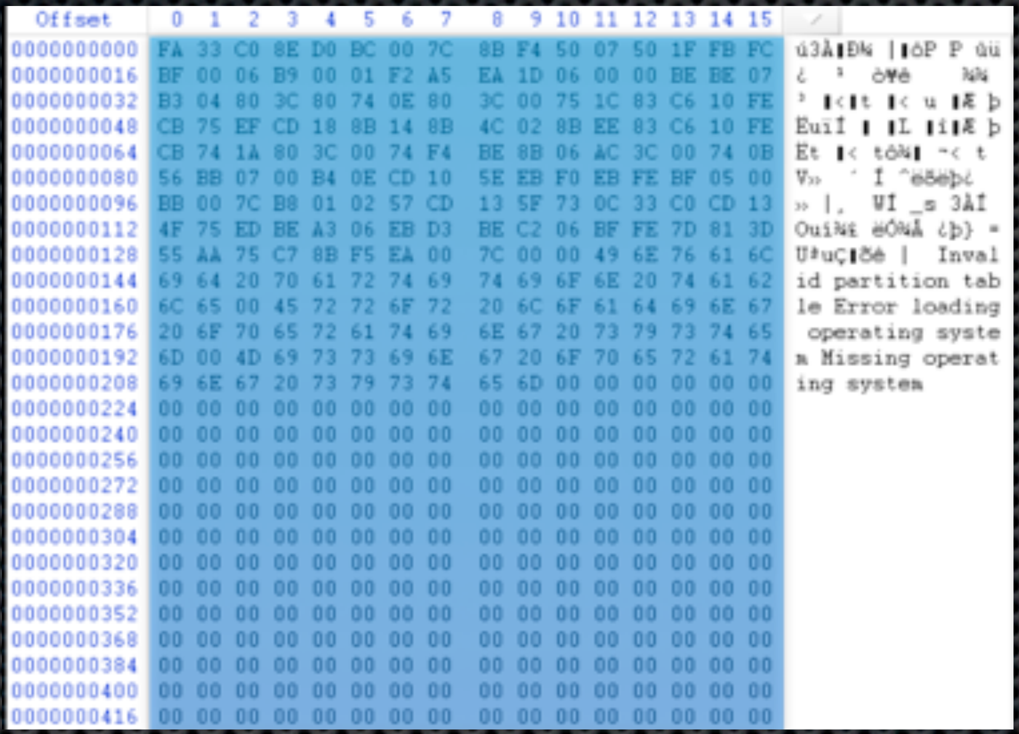
512 B per sector

1.95 GB in size

DOS partition table format	
Bytes	**Purpose**
0-445	Boot code
446-461	Partition Table Entry #1
462-477	Partition Table Entry #2
478-493	Partition Table Entry #3
494-509	Partition Table Entry #4
510-511	Signature value (0xAA55)

DOS Partition Table Entry format	
Bytes	**Purpose**
0	Bootable flag (0x80=active; else 0x00)
1-3	Starting CHS address
4	Partition type (e.g., 0x00=empty, 0x01=FAT12, 0x07=NTFS, 0x0b=FAT32 (CHS), 0x83=Linux, 0xa5=FreeBSD, 0xa8=MacOS X)*
5-7	Ending CHS address
8-11	Starting LBA address
12-15	Size (in sectors)

Can you parse the boot code?



- Jamie Levy - http://gleeda.blogspot.com/2012/04/mbr-parser.html
- https://raw.github.com/gleeda/misc-scripts/master/misc_python/mbr_parser.py

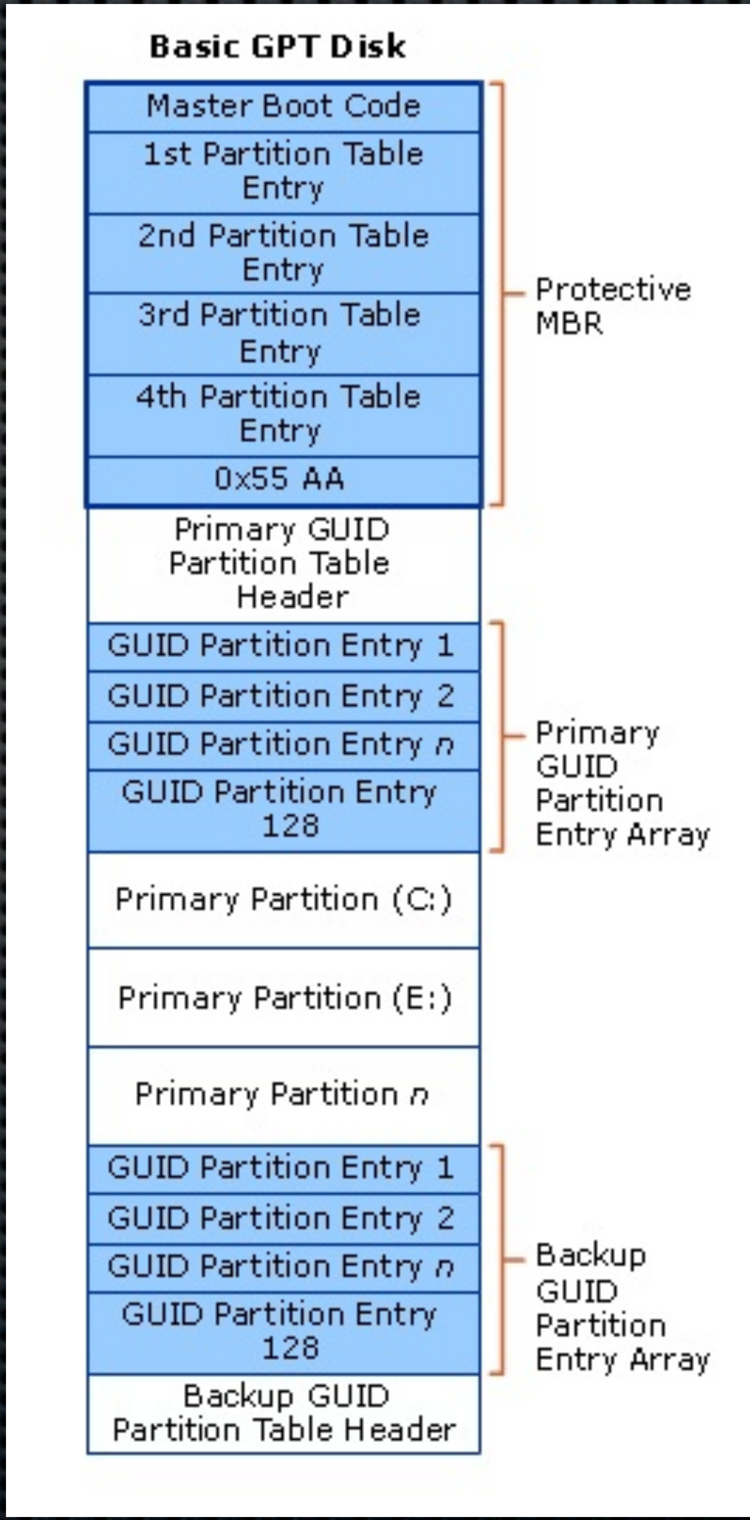
Any Questions on MBR?

Ohhhhhhhhh Yesssss!

It's time for some GPT

GPT Overview

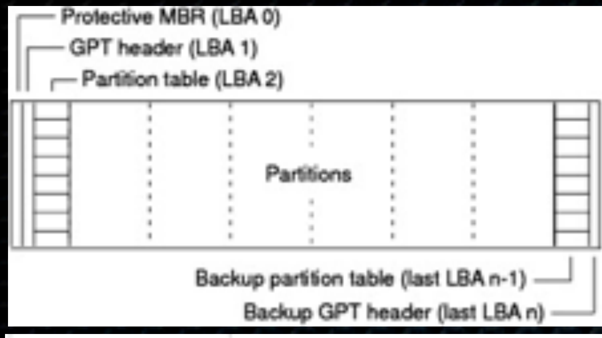
- Protective MBR
- Redundancy with integrity checking
- GUID is assigned to each partition

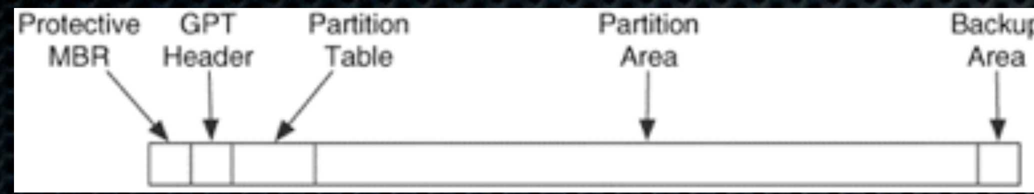


MBR/GPT comparison

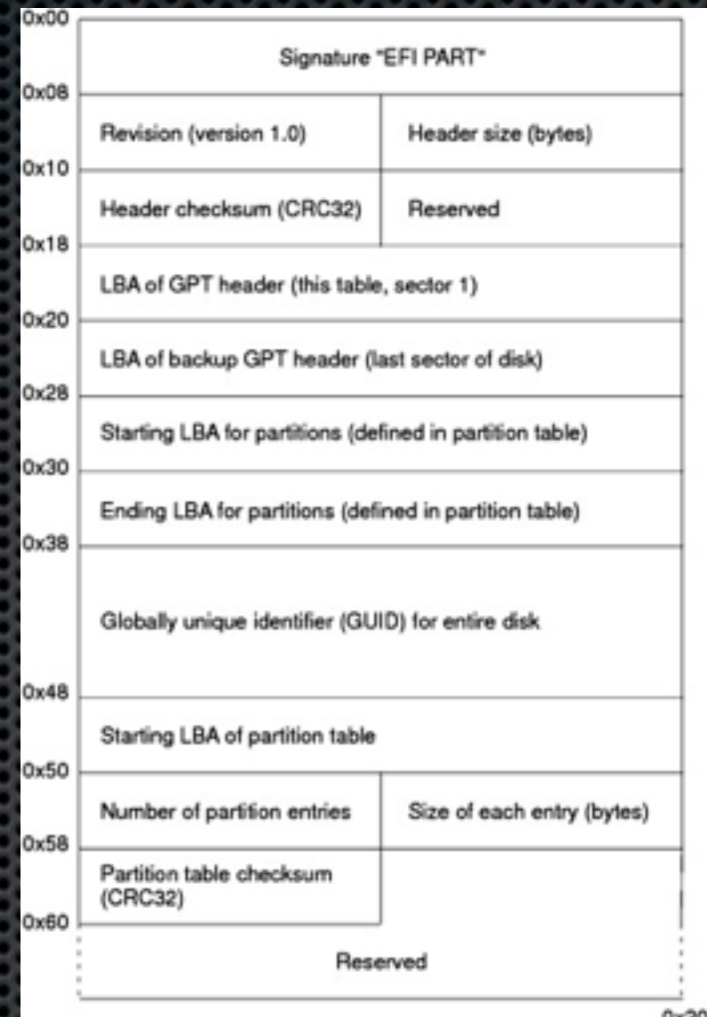
- 64 bits for LBA (GPT) vs. 32 bits
  - 4k clusters (9.4 ZB vs 8TiB)
- Supports 128 Partitions vs. 4 Primary
- Primary and backup partition table vs. Primary
- Uses CRC32 for integrity checking vs. None
- Each partition will have its own unique GUID vs. None
- Each partition will have its partition type GUID vs. None
- You can use 36 characters for a partition name vs. None

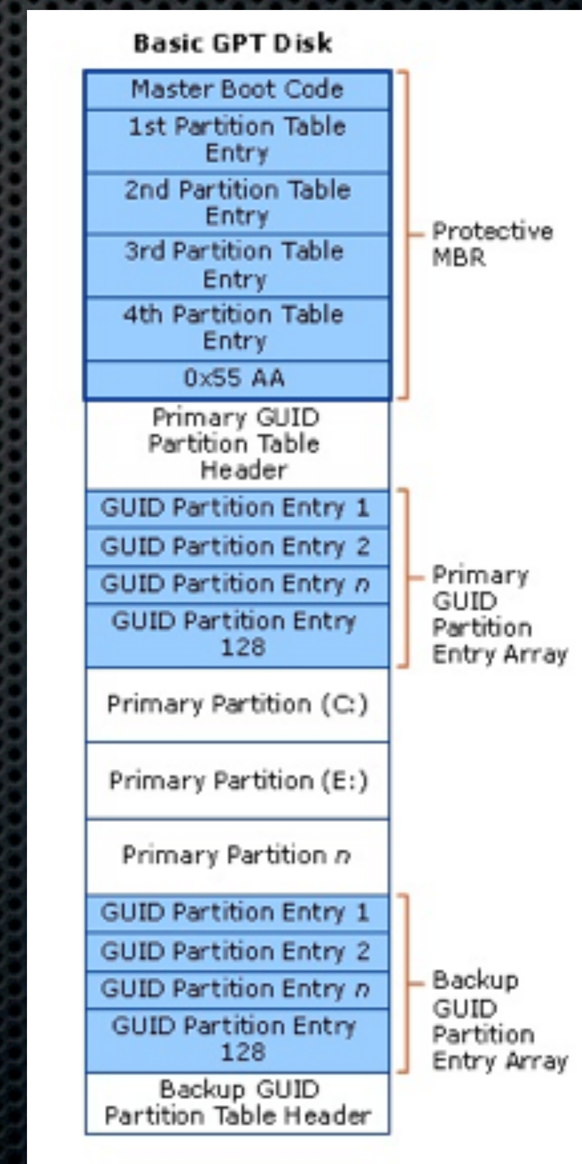
GUID





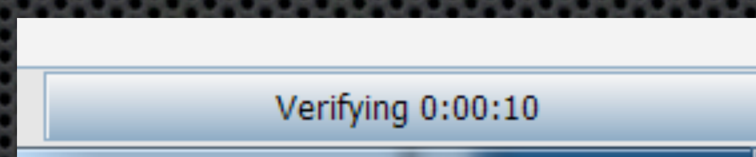
GUID partition table format		
Bytes	**Purpose**	**Description**
0-7	Signature value ("EFI PART")	Identifies EFI-compatible partition table header. This value must contain the ASCII string "EFI PART", encoded as the 64-bit constant 0x5452415020494645.
11	Version	The revision number for this header. This revision value is not related to the UEFI Specification version. This header is versionrevision value is not related to the UEFI 1.0, so the correct value is 0x0001000
12-15	Size of GPT header in bytes	Size in bytes of the GPT Header. The HeaderSize must be greater than 92 and must be less than or equal to the logical block size.
16-19	CRC32 checksum of GPT header	CRC32 checksum for the GPT Header structure. This value is computed by setting this field to 0, and computing the 32-bit CRC for HeaderSize bytes.
20-23	Reserved	Must be zero
24-31	LBA of current GPT header structure	The LBA that contains this data structure
32-39	LBA of the other GPT header structure	LBA address of the alternate LBA Header
40-47	LBA start of partition area	The first usable logical block that may be usedby a partition described by a GUID Partition Entry
48-55	LBA of end of partition area	The last usable logical block that may be used by a partition described by a GUID Partition Entry
56-71	Disk GUID	GUID that can be used to uniquely identify the Disk
72-79	LBA of start of the partition table	The starting LBA of the GUID Partition Entry
80-83	Number of entries in partition table	The number of Partition Entries in the GUID Partition Entry array
84-87	Size of each entry in partition table	The size, in bytes, of each the GUID Partition Entry structures in the GUID Partition Entry array. This field shall be set to a value of 128 x 2n where n is an integer greater than or equal to zero (e.g., 128, 256, 512, etc.). NOTE: Previous versions of this specification allowed any multiple of 8..
88-91	CRC checksum of partition table	Starts at "LBA start of the Partition Table" and is computed over a byte legnth of "Number of Partition Entries" * "Size of each entry in partition table"
92->end of sector	Reserved	The rest of the block is reserved by UEFI and must be zero

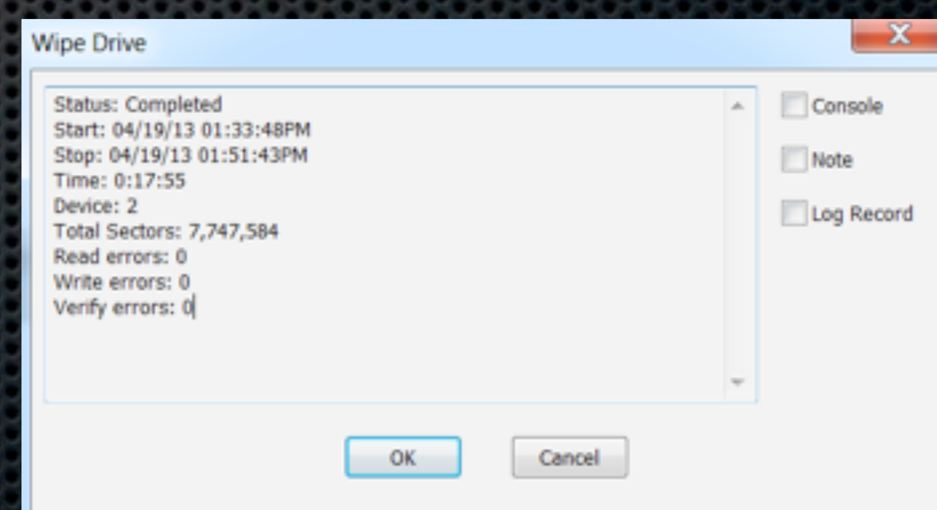




Check out the UEFI resource!

How do we create a GPT disk?

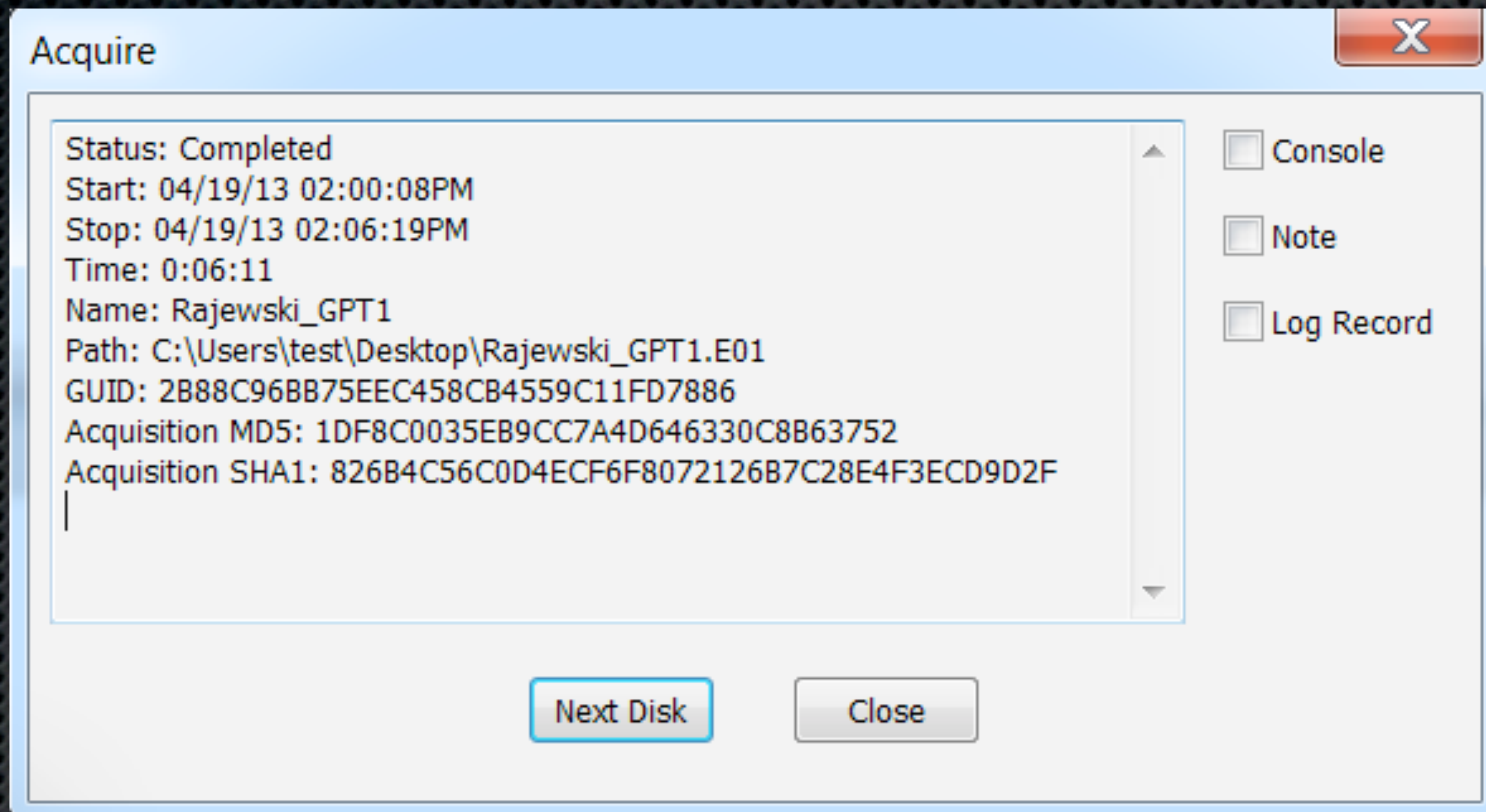


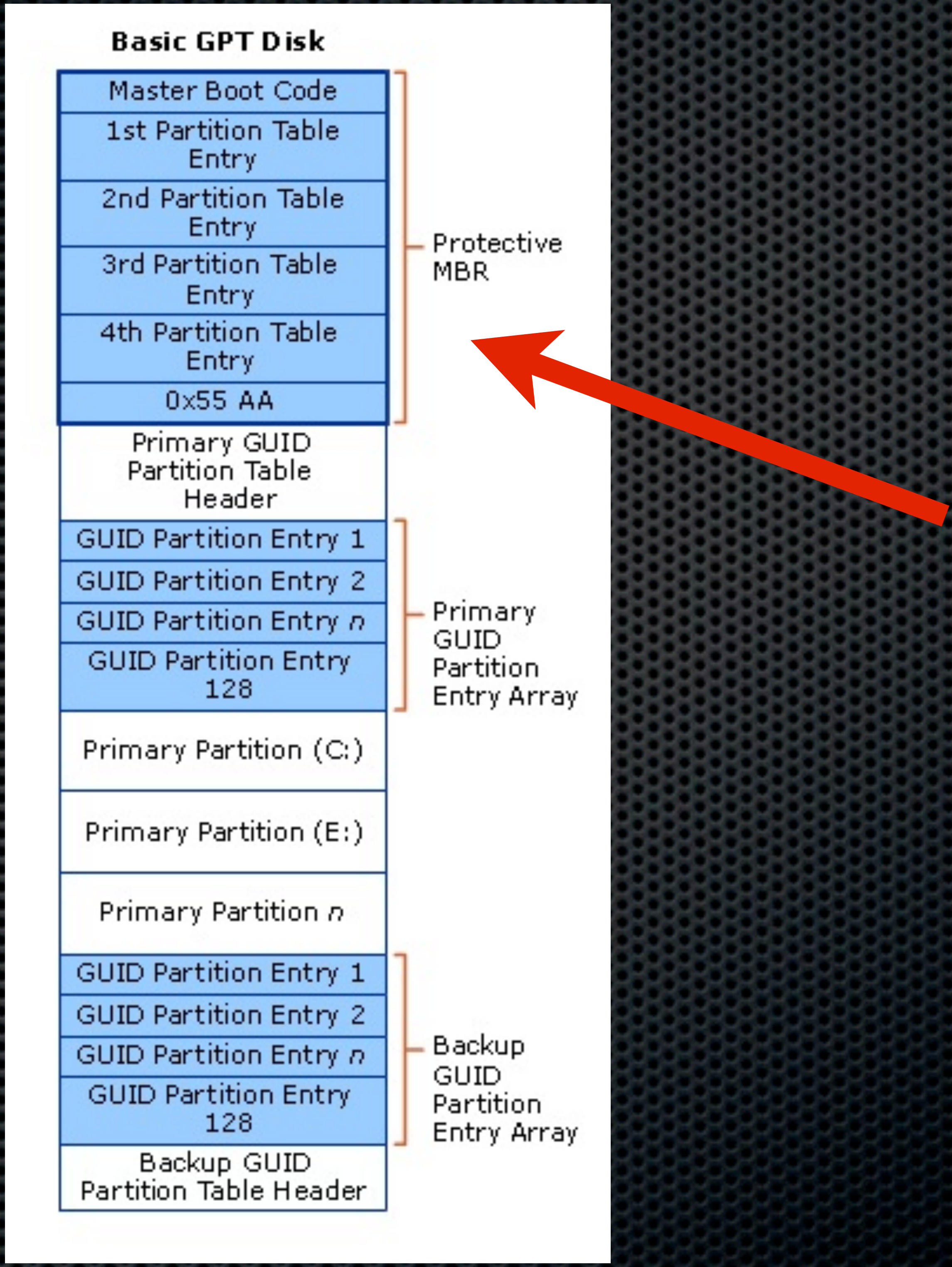


```
DISKPART> list disk

  Disk ###  Status         Size     Free     Dyn  Gpt
  --------  -------------  -------  -------  ---  ---
  Disk 0    Online           20 GB      0 B
  Disk 1    Online           60 GB      0 B        *
  Disk 2    Online         3783 MB      0 B
```

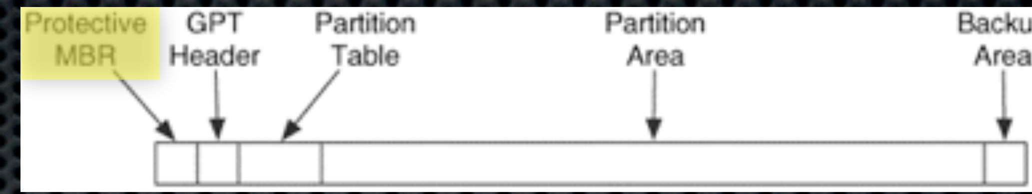
```
DISKPART> select disk 2

Disk 2 is now the selected disk.

DISKPART> clean

DiskPart succeeded in cleaning the disk.

DISKPART> convert gpt

DiskPart successfully converted the selected disk to GPT format.
```

If you want to follow along...




Basic GPT Disk
Master Boot Code
1st Partition Table Entry
2nd Partition Table Entry
3rd Partition Table Entry
4th Partition Table Entry
0x55 AA
Protective MBR
Primary GUID Partition Table Header
GUID Partition Entry 1
GUID Partition Entry 2
GUID Partition Entry n
GUID Partition Entry 128
Primary GUID Partition Entry Array
Primary Partition (C:)
Primary Partition (E:)
Primary Partition n
GUID Partition Entry 1
GUID Partition Entry 2
GUID Partition Entry n
GUID Partition Entry 128
Backup GUID Partition Entry Array
Backup GUID Partition Table Header

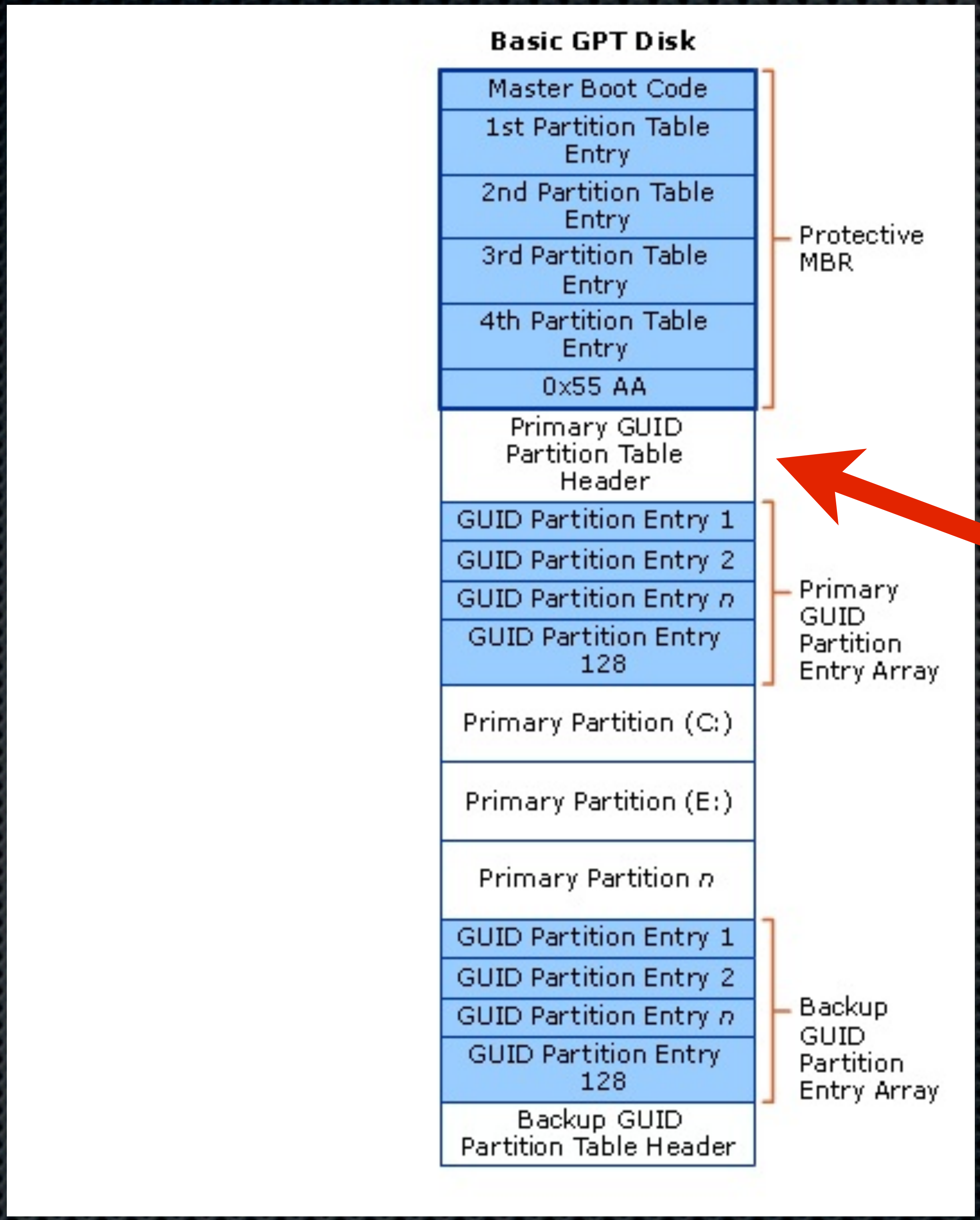
Protective MBR?



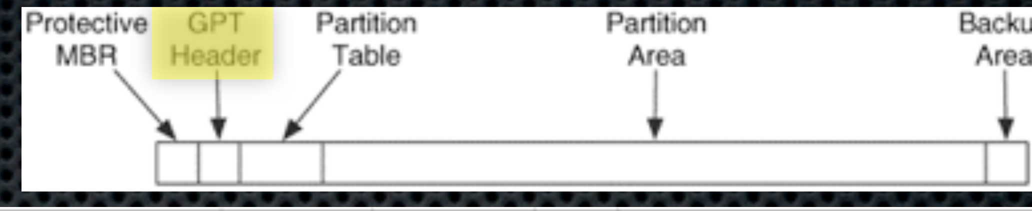
Offset	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	
0000000000	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
0000000016	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
0000000032	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
0000000048	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
0000000064	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
0000000080	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
0000000096	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
0000000112	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
0000000128	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
0000000144	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
0000000160	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
0000000176	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
0000000192	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
0000000208	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
0000000224	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
0000000240	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
0000000256	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
0000000272	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
0000000288	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
0000000304	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
0000000320	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
0000000336	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
0000000352	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
0000000368	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
0000000384	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
0000000400	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
0000000416	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
0000000432	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
0000000448	02	00	EE	FF	FF	FF	01	00	00	00	FF	FF	FF	FF	00	00	îÿÿÿ ÿÿÿÿ
0000000464	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
0000000480	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
0000000496	00	00	00	00	00	00	00	00	00	00	00	00	00	00	55	AA	Uª

GUID Protective MBR	
Bytes	**Description**
0-440	Unused by UEFI systems
440-443	Unused and set to Zero
444-445	Unused and set to Zero
446-509	MBR partition records that only have one entry pointing to the EFI Partition
510-511	Set to AA55
512	The rest of the logical block, if any, is reserved. Set to Zero

GUID protected MBR entry format	
Bytes	**Purpose**
0	Set to 0x00 to indicate a non-bootable partition. If set to any value other than 0x00 the behavior of this flag on non-UEFI systems is undefined. Must be ignored by UFI implementations
1-3	Set to 0x0002000, corresponding to the Starting LBA field
4	Partition type set to "EE" with indicates the EFI partition
5-7	Set to the CHS address of the last logical block on the disk. Set to 0xFFFFFF if it is not possible to represent the value in this field
8-11	Set to 0x00000001 (i.e., the LBA of the GPT Partition Header).
12-15	Set to the size of the disk minus one. Set to 0xFFFFFFFF if the size of the disk is too large to be represented in this field.


Basic GPT Disk
Master Boot Code
1st Partition Table Entry
2nd Partition Table Entry
3rd Partition Table Entry
4th Partition Table Entry
0x55 AA
Protective MBR
Primary GUID Partition Table Header
GUID Partition Entry 1
GUID Partition Entry 2
GUID Partition Entry n
GUID Partition Entry 128
Primary GUID Partition Entry Array
Primary Partition (C:)
Primary Partition (E:)
Primary Partition n
GUID Partition Entry 1
GUID Partition Entry 2
GUID Partition Entry n
GUID Partition Entry 128
Backup GUID Partition Entry Array
Backup GUID Partition Table Header

GPT Header



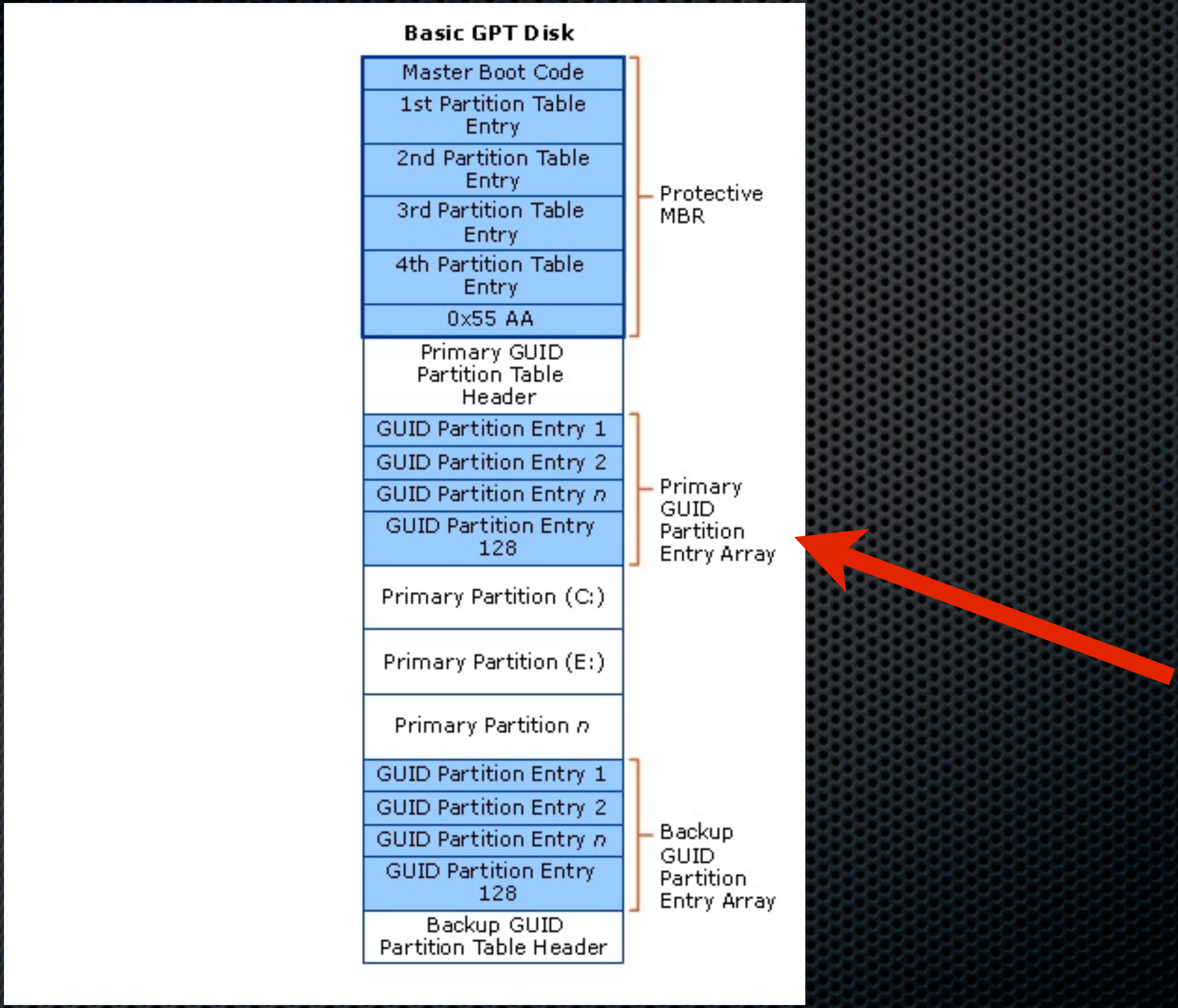

```
0000000512  45 46 49 20 50 41 52 54  00 00 01 00 5C 00 00 00  EFI PART    \
0000000528  A5 9C 63 D2 00 00 00 00  01 00 00 00 00 00 00 00  ¥▮cÒ
0000000544  FF 37 76 00 00 00 00 00  22 00 00 00 00 00 00 00  ÿ7v     "
0000000560  DE 37 76 00 00 00 00 00  85 71 29 4A 10 3C 80 4E  Þ7v     ▮q)J <▮N
0000000576  A8 24 C3 1D EA 93 72 08  02 00 00 00 00 00 00 00  ¨$Ã ê▮r
0000000592  80 00 00 00 80 00 00 00  86 D2 54 AB 00 00 00 00  €   €   ▮ÒT«
0000000608  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
0000000624  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
0000000640  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
0000000656  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
0000000672  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
0000000688  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
0000000704  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
0000000720  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
0000000736  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
0000000752  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
0000000768  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
0000000784  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
0000000800  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
0000000816  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
0000000832  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
0000000848  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
0000000864  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
0000000880  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
0000000896  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
0000000912  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
0000000928  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
0000000944  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
0000000960  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
0000000976  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
0000000992  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
0000001008  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
```

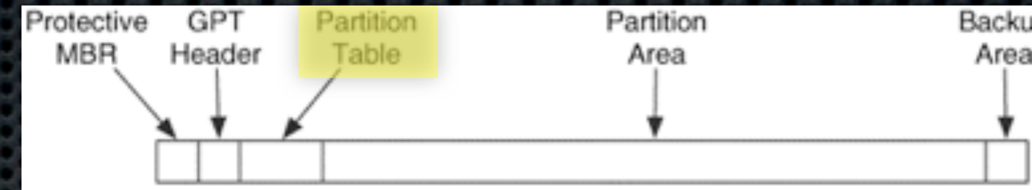
GPT Header

Mnemonic	Byte Offset	Byte Legnth	Bytes	Purpose
Signature	0	8	0-7	Identifies EFI-compatible partition table header. This value must contain the ASCII string "EFI PART", encoded as the 64-bit constant 0x5452415020494645
Revision	8	4	8-11	The revision number for this header. This revision value is not related to the UEFI Specification version. This header is version 1.0, so the correct value is 0x00010000.
Headersize	12	4	12-15	Size in bytes of the GPT Header. The HeaderSize must be greater than 92 and must be less than or equal to the logical block size.
HeaderCRC32	16	4	16-19	CRC32 checksum for the GPT Header structure. This value is computed by setting this field to 0, and computing the 32-bit CRC for HeaderSize bytes.
Reserved	20	4	20-23	Must be Zero
MyLBA	24	8	24-31	The LBA that contains this data structure.
AlternateLBA	32	8	32-39	LBA address of the alternate GPT Header.
FirstUsableLBA	40	8	40-47	The first usable logical block that may be used by a partition described by a GUID Partition Entry.
LastUsableLBA	48	8	48-55	The last usable logical block that may be used by a partition described by a GUID Partition Entry.
DiskGUID	56	16	56-71	GUID that can be used to uniquely identify the disk.
PartitionEntryLBA	72	8	72-79	The starting LBA of the GUID Partition Entry array.
NumberOfPartitionEntries	80	4	80-83	The number of Partition Entries in the GUID Partition Entry array.
SizeOfPartitionEntry	84	4	84-87	The size, in bytes, of each the GUID Partition Entry structures in the GUID Partition Entry array. This field shall be set to a value of 128 x 2n where n is an integer greater than or equal to zero (e.g., 128, 256, 512, etc.). NOTE: Previous versions of this specification allowed any multiple of 8..
PartitionEntryArrayCRC32	88	4	88-92	The CRC32 of the GUID Partition Entry array. Starts at PartitionEntryLBA and is computed over a byte length of NumberOfPartitionEntries * SizeOfPartitionEntry.
Reserved	92	Blocksize-92	92-	The rest of the block is reserved by UEFI andmust be zero.

Duplicate GUIDs?

- 2^122 [5]
    - 6 fixed bits
    - 122 random bits
- The odds of generated two identical GUIDs is 1 in 5,316,911,983,139,663,491,615,228,241,121,400,000
- So if you generate 1 million GUIDs on 1 million computers, the odds of generating a duplicate are: 1 in 5,316,911,983,139,663,491,615,228
- Take 1 billion GUIDs on 1 billion computers, odds of generating a dupe are: 1 in 5,316,911,983,139,663,491 (that's 5.3 quintillion).


Basic GPT Disk
Master Boot Code
1st Partition Table Entry
2nd Partition Table Entry
3rd Partition Table Entry
4th Partition Table Entry
0x55 AA
Protective MBR
Primary GUID Partition Table Header
GUID Partition Entry 1
GUID Partition Entry 2
GUID Partition Entry n
GUID Partition Entry 128
Primary GUID Partition Entry Array
Primary Partition (C:)
Primary Partition (E:)
Primary Partition n
GUID Partition Entry 1
GUID Partition Entry 2
GUID Partition Entry n
GUID Partition Entry 128
Backup GUID Partition Entry Array
Backup GUID Partition Table Header

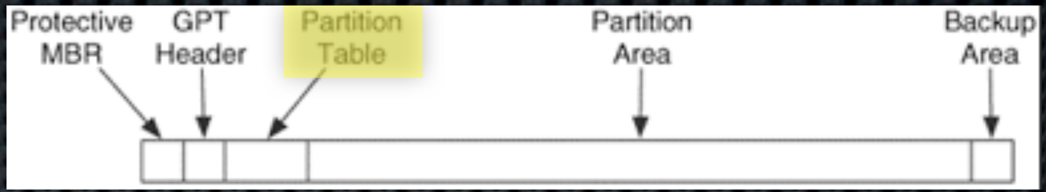


Partition Table

Offset	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	
0000001024	00	53	46	48	00	00	AA	11	AA	11	00	30	65	43	EC	AC	SFH ª ª 0eCì¬
0000001040	E8	A2	82	CA	5A	E7	32	4A	A8	E6	F8	65	BA	F2	74	63	è¢▮ÊZç2J¨æøeºòtc
0000001056	28	00	00	00	00	00	00	00	D7	93	3A	00	00	00	00	00	(×▮:
0000001072	00	00	00	00	00	00	00	00	44	00	46	00	53	00	35	00	D F S 5
0000001088	32	00	30	00	00	00	00	00	00	00	00	00	00	00	00	00	2 0
0000001104	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
0000001120	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
0000001136	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
0000001152	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
0000001168	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
0000001184	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
0000001200	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
0000001216	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
0000001232	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
0000001248	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
0000001264	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
0000001280	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
0000001296	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
0000001312	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
0000001328	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
0000001344	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
0000001360	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
0000001376	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
0000001392	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
0000001408	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
0000001424	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
0000001440	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
0000001456	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
0000001472	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
0000001488	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
0000001504	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
0000001520	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	

GPT Partition Entry

Mnemonic	Byte Offset	Byte Legnth	Bytes	Purpose
PartitionTypeGUID	0	16	0-15	Unique ID that defines the purpose and type of this Partition. A value of zero defines that this partition entry is not being used.
UniquePartitionGUID	16	16	16	GUID that is unique for every partition entry. Every partition ever created will have a unique GUID. This GUID must be assigned when the GPT Partition Entry is created. The GPT Partition Entry is created whenever the NumberOfPartitionEntries in the GPT Header is increased to include a larger rangeof addresses.
StartingLBA	32	8	32-39	Starting LBA of the partition defined by this entry.
EndingLBA	40	8	40-47	Ending LBA of the partition defined by this entry.
Attributes	48	8	48-55	Attribute bits, all bits reserved by UEFI
PartitionName	56	72	56-127	Null-terminated string containing a human-readable name of the partition.
Reserved	128	SizeOfPartition Entry - 128	32-39	The rest of the GPT Partition Entry, if any, is reserved by UEFI and must be zero.



Partition Table

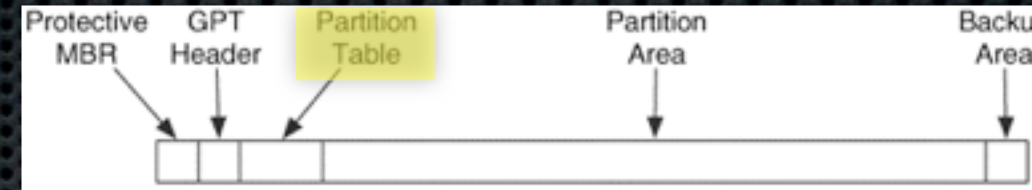
PartitionTypeGUID	0	16	0-15	Unique ID that defines the purpose and type of this Partition. A value of zero defines that this partition entry is not being used.

Table 18. Defined GPT Partition Entry - Partition Type GUIDs

Description	GUID Value
Unused Entry	00000000-0000-0000-0000-000000000000
EFI System Partition	C12A7328-F81F-11D2-BA4B-00A0C93EC93B
Partition containing a legacy MBR	024DEE41-33E7-11D3-9D69-0008C781F39F

http://en.wikipedia.org/wiki/GUID_Partition_Table

Partition Table



Attributes	48	8	48-55	Attribute bits, all bits reserved by UEFI

Defined GPT Partition Entry - Attributes		
Bits	**Name**	**Description**
Bit 0	Required Partition	If this bit is set, the partition is required for the platform to function. The owner/creator of the partition indicates that deletion or modification of the contents can result in loss of platform features or failure for the platform to boot or operate. The system cannot function normally if this partition is removed, and it should be considered part of the hardware of the system. Actions such as running diagnostics, system recovery, or even OS install or boot could potentially stop working if this partition is removed. Unless OS software or firmware recognizes this partition, it should never be removed or modified as the UEFI firmware or platform hardware may become non-functional.
Bit 1	No Block IO Protocol	If this bit is set, then firmware must not produce an EFI_BLOCK_IO_PROTOCOL device for this partition. By not producing an EFI_BLOCK_IO_PROTOCOL partition, file system mappings will not be created for this partition in UEFI.
Bit 2	Legacy BIOS Bootable	This bit is set aside by this specification to let systems with traditional PC-AT BIOS firmware implementations inform certain limited, special-purpose software running on these systems that a GPT partition may be bootable. For systems with firmware implementations conforming to this pecification, the UEFI boot manager (see chapter 3) must ignore this bit when selecting a UEFI compliant application, e.g., an OS loader (see 2.1.3). Therefore there is no need for this specification to define the exact meaning of this bit.
Bits 3-47		Undefined and must be zero. Reserved for expansion by future versions of the UEFI specification.
Bits 48-63		Reserved for GUID specific use. The use of these bits will vary depending on the PartitionTypeGUID. Only the owner of the PartitionTypeGUID is allowed to modify these bits. They must be preserved if Bits 0–47 are modified.

Partition Attributes

Bit	Description
Bit 0	Specifies that this partition is required for the platform to function. All original equipment manufacturer (OEM) partitions must have this bit set to protect the OEM partition from being overwritten by the disk tools supplied with Windows Server 2003.
Bit 60	Marks the partition as read-only. Used only for primary basic partitions of type
Bit 62	Marks the partition as hidden. Used only for primary basic partitions of type (VSS)
Bit 63	Prevents the system from assigning a default drive letter to the partition.

http://msdn.microsoft.com/en-us/library/aa381635(VS.85).aspx

So let's make this interesting...

Let's practice our skills!

Let's create multiple GPT Partitions on our thumb drive...

How would you create a GPT thumb drive with multiple partitions do this with Windows?

Using DISKPART to create multiple partitions on a thumb drive...

Linux to the rescue!

```
root@bt:~# sudo fdisk -ls

Disk /dev/sda: 21.5 GB, 21474836480 bytes
255 heads, 63 sectors/track, 2610 cylinders
Units = cylinders of 16065 * 512 = 8225280 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes
Disk identifier: 0x000f1335

   Device Boot      Start         End      Blocks   Id  System
/dev/sda1   *           1        2497    20051968   83  Linux
/dev/sda2            2497        2611      916481    5  Extended
/dev/sda5            2497        2611      916480   82  Linux swap / Solaris

WARNING: GPT (GUID Partition Table) detected on '/dev/sdc'! The util fdisk doesn
't support GPT. Use GNU Parted.


Disk /dev/sdc: 3966 MB, 3966763008 bytes
256 heads, 63 sectors/track, 480 cylinders
Units = cylinders of 16128 * 512 = 8257536 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes
Disk identifier: 0x00000000

   Device Boot      Start         End      Blocks   Id  System
/dev/sdc1               1      266306  2147483647+  ee  GPT
Partition 1 has different physical/logical endings:
     phys=(1023, 255, 63) logical=(266305, 4, 4)
```

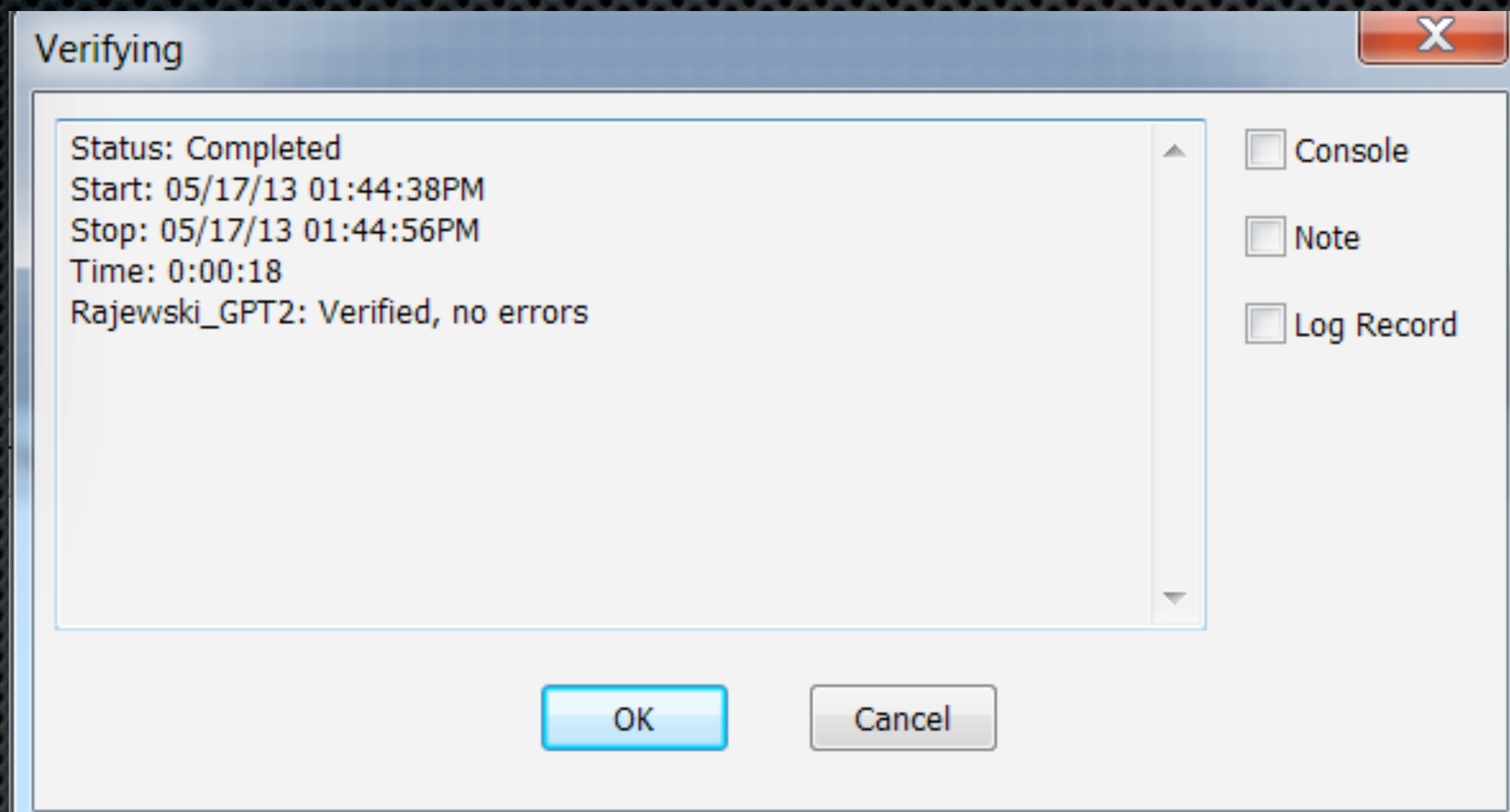
WARNING: GPT (GUID Partition Table) detected on '/dev/sdc'! The util fdisk doesn't support GPT. Use GNU Parted.

```
root@bt:~# sudo parted
GNU Parted 2.2
Using /dev/sda
Welcome to GNU Parted! Type 'help' to view a list of commands.
(parted) select /dev/sdc
Using /dev/sdc
```

```
(parted) mkpartfs logical fat32 462 662
WARNING: you are attempting to use parted to operate on (mkpartfs) a file system.
parted's file system manipulation code is not as robust as what you'll find in
dedicated, file-system-specific packages like e2fsprogs.  We recommend
you use parted only to manipulate partition tables, whenever possible.
Support for performing most operations on most types of file systems
will be removed in an upcoming release.
(parted) print
Model: Generic STORAGE DEVICE (scsi)
Disk /dev/sdc: 3967MB
Sector size (logical/physical): 512B/512B
Partition Table: gpt

Number  Start   End    Size   File system  Name                  Flags
 1      65.5kB  210MB  210MB  ntfs         Basic data partition
 2      261MB   461MB  200MB  fat32        logical
 3      461MB   662MB  200MB  fat32        logical
```

Image Source http://www.brenchelarmy.com/challenge.jpg

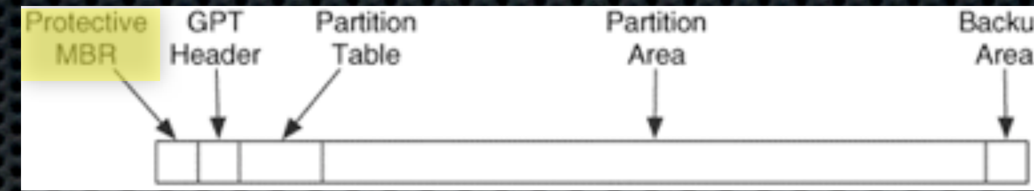
If you want to follow along...



“Rajewski_GPT2” Practice

- What can be discovered in the Protected MBR?
- How many partitions are on this GPT volume - list some details.
  - What is the “Starting LBA”
  - What is the “Ending LBA”
- What are the “Partition Names”

Protective MBR




```
Offset      0  1  2  3  4  5  6  7   8  9 10 11 12 13 14 15
0000000000 00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
0000000016 00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
0000000032 00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
0000000048 00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
0000000064 00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
0000000080 00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
0000000096 00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
0000000112 00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
0000000128 00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
0000000144 00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
0000000160 00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
0000000176 00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
0000000192 00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
0000000208 00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
0000000224 00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
0000000240 00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
0000000256 00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
0000000272 00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
0000000288 00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
0000000304 00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
0000000320 00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
0000000336 00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
0000000352 00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
0000000368 00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
0000000384 00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
0000000400 00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
0000000416 00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
0000000432 00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
0000000448 01 00 EE FE FF FF 01 00  00 00 FF 37 76 00 00 00   îþÿÿ    ÿ7v
0000000464 00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
0000000480 00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
0000000496 00 00 00 00 00 00 00 00  00 00 00 00 00 00 55 AA                 Uª
```

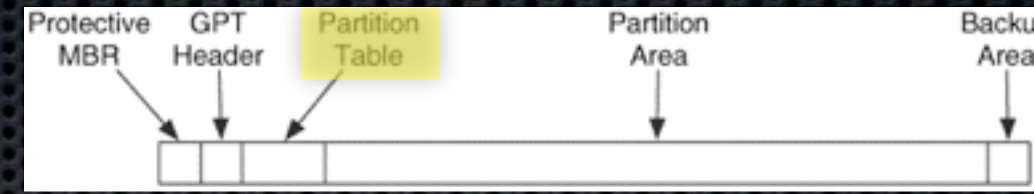
GUID Protective MBR

Bytes	Description
0-440	Unused by UEFI systems
440-443	Unused and set to Zero
444-445	Unused and set to Zero
446-509	MBR partition records that only have one entry pointing to the EFI Partition
510-511	Set to AA55
512	The rest of the logical block, if any, is reserved. Set to Zero

GUID protected MBR entry format

Bytes	Purpose
0	Set to 0x00 to indicate a non-bootable partition. If set to any value other than 0x00 the behavior of this flag on non-UEFI systems is undefined. Must be ignored by UFI implementations
1-3	Set to 0x0002000, corresponding to the Starting LBA field
4	Partition type set to "EE" with indicates the EFI partition
5-7	Set to the CHS address of the last logical block on the disk. Set to 0xFFFFFF if it is not possible to represent the value in this field
8-11	Set to 0x00000001 (i.e., the LBA of the GPT Partition Header).
12-15	Set to the size of the disk minus one. Set to 0xFFFFFFFF if the size of the disk is too large to be represented in this field.

Partition Table



Offset	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	
0000001024	A2	A0	D0	EB	E5	B9	33	44	87	C0	68	B6	B7	26	99	C7	¢ Ðëå¹3D▌Àh¶·&▌Ç
0000001040	3F	23	25	E4	2C	96	3E	49	9E	FA	73	70	56	EE	98	13	?#%ä,▌>I▌úspVî▌
0000001056	80	00	00	00	00	00	00	00	7F	40	06	00	00	00	00	00	▌ @
0000001072	00	00	00	00	00	00	00	00	42	00	61	00	73	00	69	00	B a s i
0000001088	63	00	20	00	64	00	61	00	74	00	61	00	20	00	70	00	c d a t a p
0000001104	61	00	72	00	74	00	69	00	74	00	69	00	6F	00	6E	00	a r t i t i o n
0000001120	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
0000001136	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
0000001152	A2	A0	D0	EB	E5	B9	33	44	87	C0	68	B6	B7	26	99	C7	¢ Ðëå¹3D▌Àh¶·&▌Ç
0000001168	A9	C7	D4	DF	12	CA	04	4A	8D	F0	CF	27	B5	D9	1F	C3	©ÇÔß Ê J ðÏ'µÙ Ã
0000001184	00	C8	07	00	00	00	00	00	FF	BF	0D	00	00	00	00	00	È ÿ¿
0000001200	00	00	00	00	00	00	00	00	46	00	41	00	54	00	5F	00	F A T _
0000001216	56	00	4F	00	4C	00	55	00	4D	00	45	00	00	00	00	00	V O L U M E
0000001232	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
0000001248	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
0000001264	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
0000001280	A2	A0	D0	EB	E5	B9	33	44	87	C0	68	B6	B7	26	99	C7	¢ Ðëå¹3D▌Àh¶·&▌Ç
0000001296	DF	58	F9	F8	3C	41	93	4C	A7	52	6F	3E	6C	76	3E	FA	ßXùø<A▌L§Ro>lv>ú
0000001312	00	C0	0D	00	00	00	00	00	FF	B7	13	00	00	00	00	00	À ÿ·
0000001328	00	00	00	00	00	00	00	00	46	00	41	00	54	00	32	00	F A T 2
0000001344	5F	00	56	00	4F	00	4C	00	55	00	4D	00	45	00	00	00	_ V O L U M E
0000001360	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
0000001376	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
0000001392	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
0000001408	A2	A0	D0	EB	E5	B9	33	44	87	C0	68	B6	B7	26	99	C7	¢ Ðëå¹3D▌Àh¶·&▌Ç
0000001424	51	D4	F7	60	17	FB	AF	4D	88	DA	0D	DF	70	C6	7F	C1	QÔ÷` û¯M▌Ú ßpÆ Á
0000001440	00	C0	13	00	00	00	00	00	FF	B7	19	00	00	00	00	00	À ÿ·
0000001456	00	00	00	00	00	00	00	00	46	00	41	00	54	00	33	00	F A T 3
0000001472	5F	00	56	00	4F	00	4C	00	55	00	4D	00	45	00	00	00	_ V O L U M E
0000001488	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
0000001504	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
0000001520	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
0000001536	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
0000001552	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
0000001568	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
0000001584	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
0000001600	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	

GPT Partition Entry

Mnemonic	Byte Offset	Byte Legnth	Bytes	Purpose
PartitionTypeGUID	0	16	0-15	Unique ID that defines the purpose and type of this Partition. A value of zero defines that this partition entry is not being used.
UniquePartitionGUID	16	16	16	GUID that is unique for every partition entry. Every partition ever created will have a unique GUID. This GUID must be assigned when the GPT Partition Entry is created. The GPT Partition Entry is created whenever the NumberOfPartitionEntries in the GPT Header is increased to include a larger rangeof addresses.
StartingLBA	32	8	32-39	Starting LBA of the partition defined by this entry.
EndingLBA	40	8	40-47	Ending LBA of the partition defined by this entry.
Attributes	48	8	48-55	Attribute bits, all bits reserved by UEFI
PartitionName	56	72	56-127	Null-terminated string containing a human-readable name of the partition.
Reserved	128	SizeOfPartition Entry - 128	32-39	The rest of the GPT Partition Entry, if any, is reserved by UEFI and must be zero.

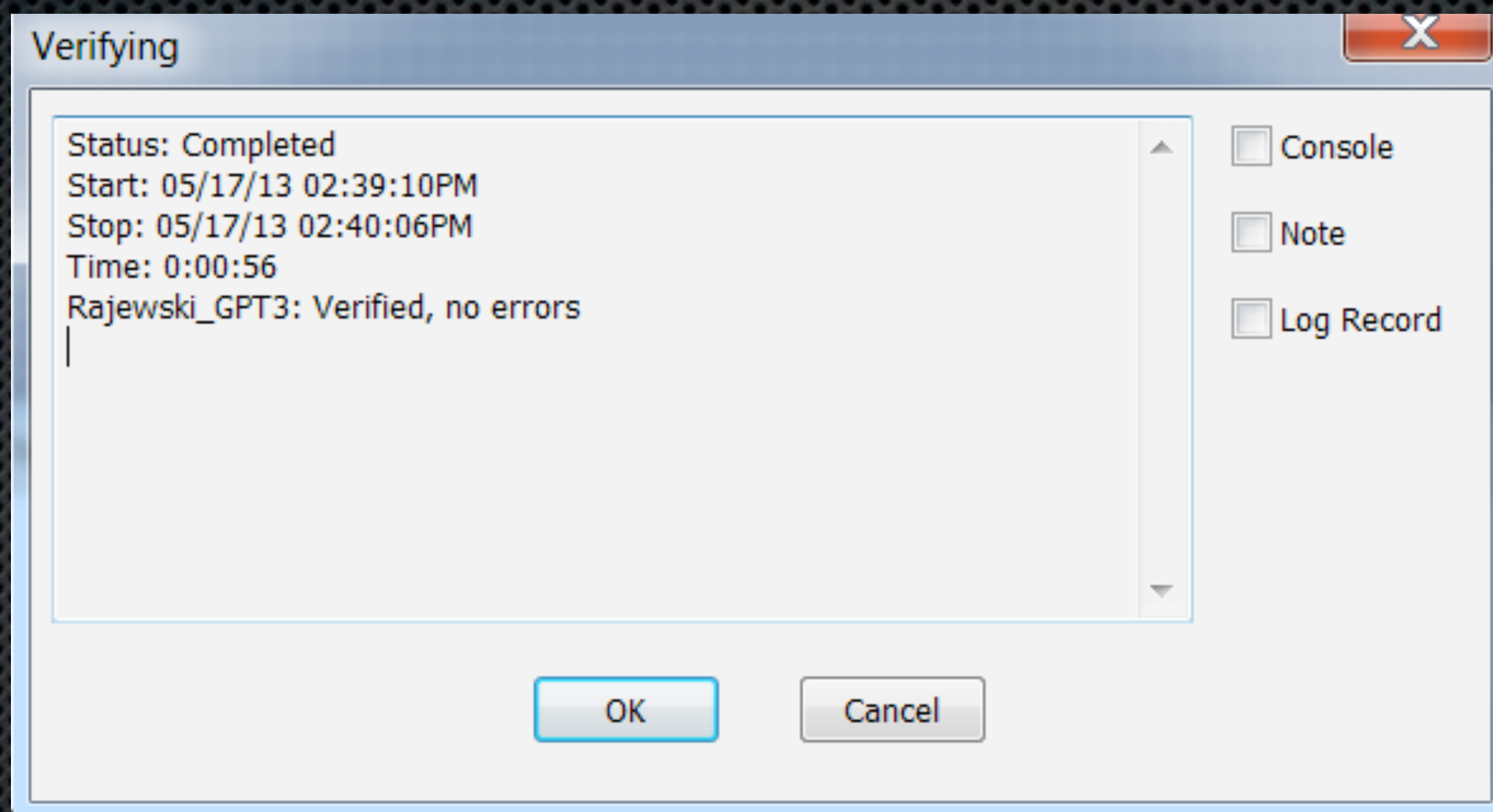
“Rajewski_GPT2” Practice

- What can be discovered in the Protected MBR?
  - Partition Type “EE” and the Start is LBA 1
- How many partitions are on this GPT volume - list some details.
  - 4 - GUID - All Linux - All have unique GUIDs
  - What is the “Starting LBAs” 80 (128), 07C800 (509952), 0DC000 (901120), 13C000 (1294336)
  - What is the “Ending LBAs” 06407f (409727), 0DBFFF (901119), 13B7FF (1292287), 19B7FF (1685503)
- What are the “Partition Names” - “Basic data Partition” “FAT_VOLUME” “FAT2_VOLUME” “FAT3_VOLUME”

How did you do?

The Final GPT Challenge!

Now let's try it one more time :)



"Rajewski_GPT2" Challenge

- What can be discovered in the Protected MBR?
- How many partitions are on this GPT volume - list some details.
  - What is the "Starting LBA"
  - What is the "Ending LBA"
- What can be discovered in the "Partition Tables"
  - Are you seeing the same results with your forensic tools?

Offset	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	
0000001024	28	73	2A	C1	1F	F8	D2	11	BA	4B	00	A0	C9	3E	C9	3B	(s*Á øÒ ºK É>É;
0000001040	9D	91	71	94	B5	D7	76	48	B1	45	F9	D3	75	FF	0C	58	‘q▮µ×vH±EùÓuÿ X
0000001056	28	00	00	00	00	00	00	00	27	40	06	00	00	00	00	00	('@
0000001072	00	00	00	00	00	00	00	00	45	00	46	00	49	00	20	00	E F I
0000001088	53	00	79	00	73	00	74	00	65	00	6D	00	20	00	50	00	S y s t e m P
0000001104	61	00	72	00	74	00	69	00	74	00	69	00	6F	00	6E	00	a r t i t i o n
0000001120	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
0000001136	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
0000001152	A2	A0	D0	EB	E5	B9	33	44	87	C0	68	B6	B7	26	99	C7	¢ Ðëå¹3D▮Àh¶·&▮Ç
0000001168	22	42	D7	47	80	A1	37	41	BD	0F	28	9C	96	8D	F1	FC	"B×G▮¡7A½ (▮▮ ñü
0000001184	00	48	06	00	00	00	00	00	FF	77	7D	00	00	00	00	00	H ÿw}
0000001200	00	00	00	00	00	00	00	00	49	00	4E	00	47	00	52	00	I N G R
0000001216	45	00	53	00	53	00	00	00	00	00	00	00	00	00	00	00	E S S
0000001232	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
0000001248	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
0000001264	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
0000001280	A2	A0	D0	EB	E5	B9	33	44	87	C0	68	B6	B7	26	99	C7	¢ Ðëå¹3D▮Àh¶·&▮Ç
0000001296	BF	84	D8	55	20	6B	93	46	BB	BE	E7	B5	FA	1F	82	09	¿▮ØU k▮F»¾çµú ▮
0000001312	00	78	7D	00	00	00	00	00	FF	6F	80	00	00	00	00	00	x} ÿo▮
0000001328	00	00	00	00	00	00	00	00	45	00	4E	00	4C	00	49	00	E N L I
0000001344	47	00	48	00	54	00	45	00	4E	00	45	00	44	00	00	00	G H T E N E D
0000001360	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
0000001376	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
0000001392	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
0000001408	A2	A0	D0	EB	E5	B9	33	44	87	C0	68	B6	B7	26	99	C7	¢ Ðëå¹3D▮Àh¶·&▮Ç
0000001424	E9	94	8D	A8	0D	30	91	4C	80	BB	05	1C	F9	48	EB	BC	é▮ ¨ 0‘L▮» ùHë¼
0000001440	00	70	80	00	00	00	00	00	FF	5F	86	00	00	00	00	00	p€ ÿ_▮
0000001456	00	00	00	00	00	00	00	00	43	00	68	00	61	00	6D	00	C h a m
0000001472	70	00	6C	00	61	00	69	00	6E	00	00	00	00	00	00	00	p l a i n
0000001488	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
0000001504	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
0000001520	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
0000001536	A2	A0	D0	EB	E5	B9	33	44	87	C0	68	B6	B7	26	99	C7	¢ Ðëå¹3D▮Àh¶·&▮Ç
0000001552	FA	83	CB	95	77	82	8A	4A	BB	85	0C	0F	B1	FA	CD	9E	ú▮Ë▮w▮▮J»▮ ±úÍ▮
0000001568	00	60	86	00	00	00	00	00	FF	F7	C1	00	00	00	00	00	`▮ ÿ÷Á
0000001584	00	00	00	00	00	00	00	00	43	00	4F	00	4C	00	4C	00	C O L L
0000001600	45	00	47	00	45	00	00	00	00	00	00	00	00	00	00	00	E G E
0000001616	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
0000001632	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
0000001648	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
0000001664	00	53	46	48	00	00	AA	11	AA	11	00	30	65	43	EC	AC	SFH ª ª 0eCì¬
0000001680	90	CB	17	42	DE	77	8D	46	84	9F	5B	B9	3B	C6	48	F7	Ë BÞw F▮▮[¹;ÆH÷
0000001696	00	F8	C1	00	00	00	00	00	D7	27	E3	00	00	00	00	00	øÁ ×'ã
0000001712	00	00	00	00	00	00	00	00	73	00	6E	00	6B	00	79	00	s n k y
0000001728	73	00	6E	00	6B	00	79	00	00	00	00	00	00	00	00	00	s n k y

```
0000001152  A2 A0 D0 EB E5 B9 33 44  87 C0 68 B6 B7 26 99 C7  ¢ Ðëå¹3D‖Àh¶·&‖Ç
0000001168  22 42 D7 47 80 A1 37 41  BD 0F 28 9C 96 8D F1 FC  "B×G‖¡7A½ (‖‖ ñü
0000001184  00 48 06 00 00 00 00 00  FF 77 7D 00 00 00 00 00   H       ÿw}
0000001200  00 00 00 00 00 00 00 00  49 00 4E 00 47 00 52 00          I N G R
0000001216  45 00 53 00 53 00 00 00  00 00 00 00 00 00 00 00  E S S
0000001232  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
0000001248  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
0000001264  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
```

- PartitionTypeGUID A2A0D0EBE5B9334487C068B6B72699C7 (Linux)
- UniquePartitionGUID 2242D74780A13741BD0F289C968DF1FC
- StartingLBA 0048060000000000
- EndingLBA FF777D0000000000
- Attributes 0000000000000000
- Partition Name 49004E004700520045005300530053 (INGRESS)
- Reserved

GPT Partition Entry				
Mnemonic	Byte Offset	Byte Legnth	Bytes	Purpose
PartitionTypeGUID	0	16	0-15	Unique ID that defines the purpose and type of this Partition. A value of zero defines that this partition entry is not being used.
UniquePartitionGUID	16	16	16	GUID that is unique for every partition entry. Every partition ever created will have a unique GUID. This GUID must be assigned when the GPT Partition Entry is created. The GPT Partition Entry is created whenever the NumberOfPartitionEntries in the GPT Header is increased to include a larger rangeof addresses.
StartingLBA	32	8	32-39	Starting LBA of the partition defined by this entry.
EndingLBA	40	8	40-47	Ending LBA of the partition defined by this entry.
Attributes	48	8	48-55	Attribute bits, all bits reserved by UEFI
PartitionName	56	72	56-127	Null-terminated string containing a human-readable name of the partition.
Reserved	128	SizeOfPartition Entry - 128	32-39	The rest of the GPT Partition Entry, if any, is reserved by UEFI and must be zero.

0000001664	00	53	46	48	00	00	AA	11	AA	11	00	30	65	43	EC	AC	SFH ª ª 0eCì¬
0000001680	90	CB	17	42	DE	77	8D	46	84	9F	5B	B9	3B	C6	48	F7	Ë BÞw F▌▌[¹;ÆH÷
0000001696	00	F8	C1	00	00	00	00	00	D7	27	E3	00	00	00	00	00	øÁ ×'ã
0000001712	00	00	00	00	00	00	00	00	73	00	6E	00	6B	00	79	00	s n k y
0000001728	73	00	6E	00	6B	00	79	00	00	00	00	00	00	00	00	00	s n k y

- PartitionTypeGUID 005346480000AA11AA1100306543ECAC (HFS)
- UniquePartitionGUID 90CB1742DE778D46849F5BB93BC648F7
- StartingLBA 00F8C10000000000
- EndingLBA D727E30000000000
- Attributes 0000000000000000
- Partition Name 73006E006B00790073006E006B0079 (snky snky)
- Reserved

Any Questions?

Thank you!

Jonathan T. Rajewski, MS, CCE, EnCe, CISSP, CFE
Assistant Professor, Digital Forensics, Champlain College
Director/Principal Investigator, Senator Patrick Leahy Center for Digital Investigation (LCDI)
Digital Forensic Examiner, Vermont Internet Crimes Task Force

Champlain College
West Hall
163 South Willard Street
Burlington, VT 05401
Office: +1 802-865-5460
Google Voice - +1 802-318-4804
Mobile - Available via request
Skype – jtrajewski

Jonrajewski.com/cyberblog

rajewski@champlain.edu
jtrajewski@gmail.com

PGP Public Key: Located on keyserver.pgp.com

Leahy Center for Digital Investigation
at CHAMPLAIN COLLEGE

Resources

- [1] http://www.zdnet.com/microsoft-windows-8-uefi-secure-boot-complaint-the-case-for-and-against-7000013248/
- [2] http://blog.hansenpartnership.com/owning-your-windows-8-uefi-platform/
- [3] http://blogs.msdn.com/b/b8/archive/2011/09/22/protecting-the-pre-os-environment-with-uefi.aspx
- [4] http://threatpost.com/ami-firmware-source-code-private-key-leaked-040513/
- [5] http://stackoverflow.com/questions/14074238/guid-uniqueness-on-different-machine