BIOS UEFI en GPT

Keith Merrington

Inhoud

- Opstarten
- PC-firmware
  - BIOS/UEFI
  - BIOS updaten
- Schijforganisatie
  - MBR/GPT
- EFI
  - Toegang
  - En wat meer

PC Firmware

- Er zijn momenteel twee hoofdtypen firmware in IBM-compatibele pc's:

  BIOS - Basic Input Output System (1981)

  UEFI - Unified Extensible Firmware Interface (2005/2015)

  zie - https://www.intel.com/content/dam/www/public/us/en/zip/efi-1-10-update.zip

- Er is echter nog een ander type firmware, namelijk de open source firmware "Coreboot".

  zie https://doc.coreboot.org/

- Deze presentatie gaat alleen over BIOS en UEFI.

PC Firmware

- BIOS en UEFI zijn twee zeer verschillende systemen, hoewel ze in principe dezelfde functie hebben.
- Hoewel UEFI veel nieuwer is en een andere opstartmodus heeft, ondersteunt (bijna altijd) het nog steeds de oude BIOS-opstartmodus. Deze modus kan Legacy, BIOS-modus, CSM (Compatibility Support Module) of iets dergelijks worden genoemd.

* Mac-computers maken ook gebruik van UEFI.

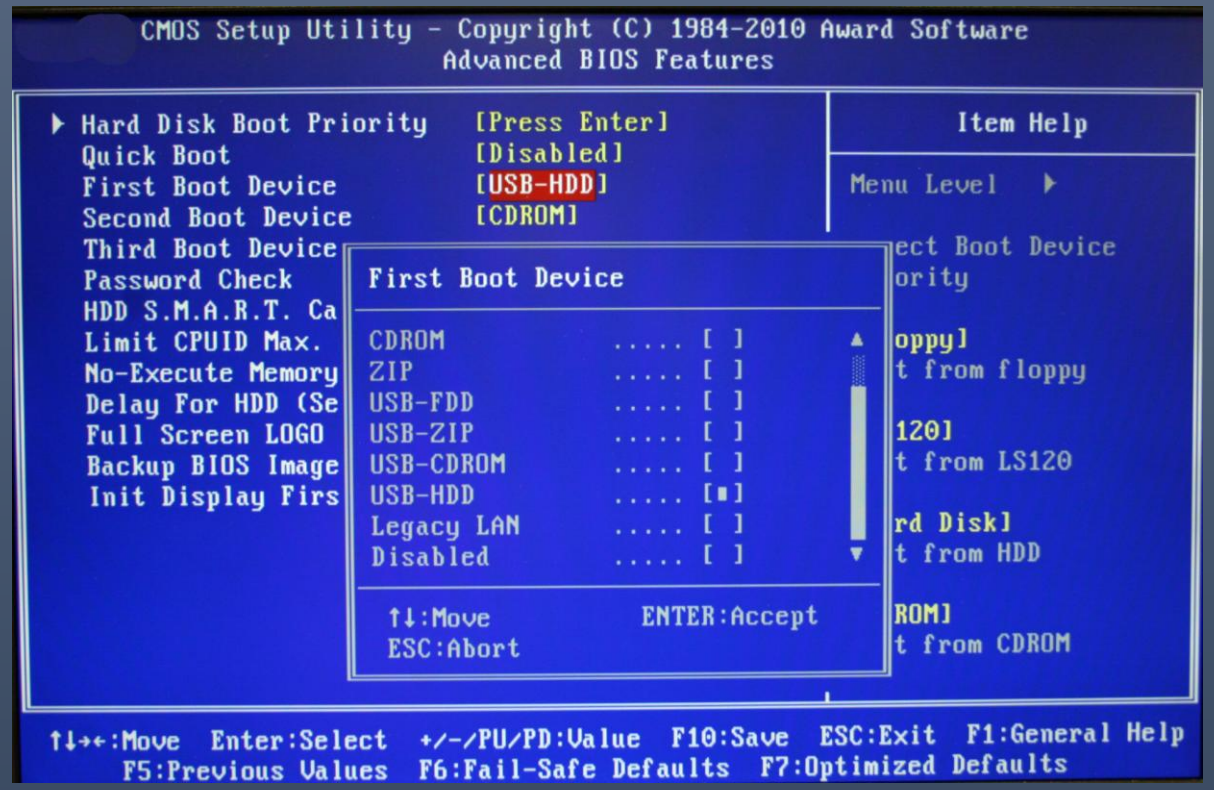
PC Firmware

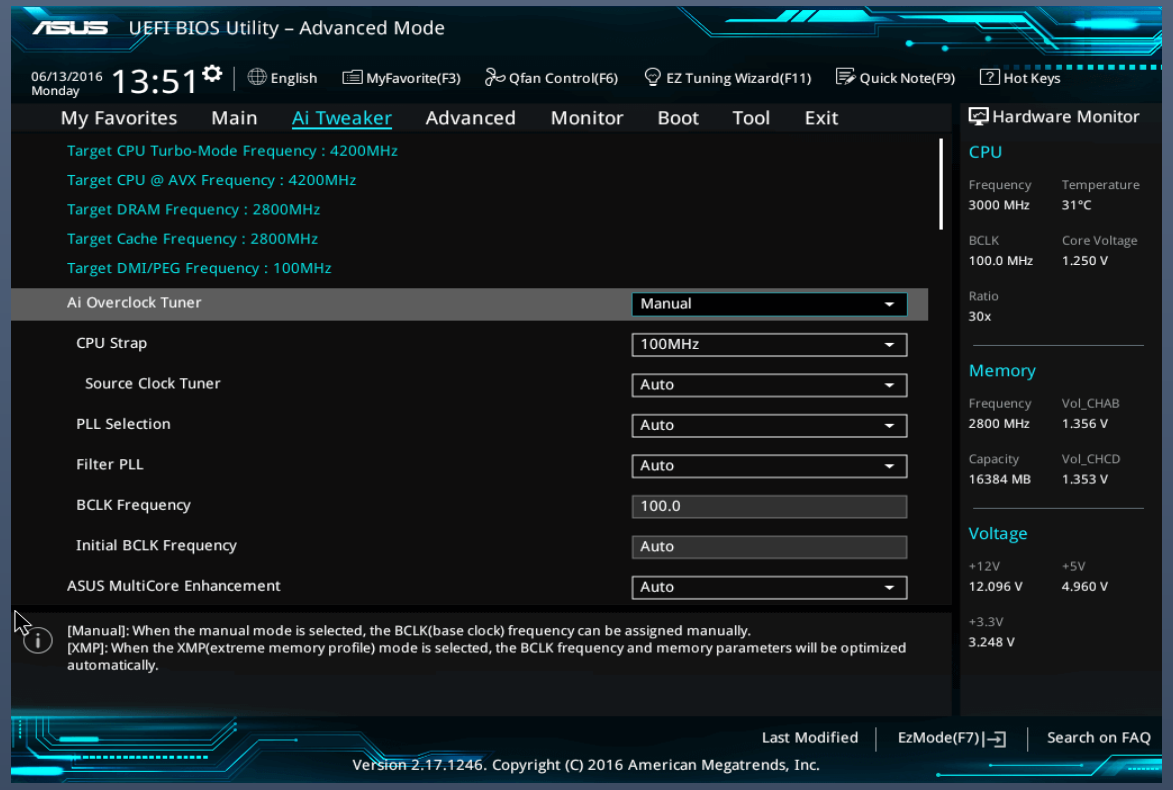
- UEFI biedt meer functies en voordelen, zoals snellere opstarttijden, betere beveiliging, ondersteuning voor grotere schijven (GPT) en een grafische gebruikersinterface. UEFI is vaak rechtstreeks toegankelijk vanuit het besturingssysteem, BIOS niet.
- Sommige besturingssystemen (versies) werken alleen met UEFI!
- Andere kunnen dat niet.
- Sommige werken met beide!

PC Firmware

- Legacy BIOS is de oude modus die gebruikmaakt van een 16-bits code en een beperkt aantal opties heeft, maar nog steeds wordt gebruikt (OS/2, Windows 7, Win 95, ME..).

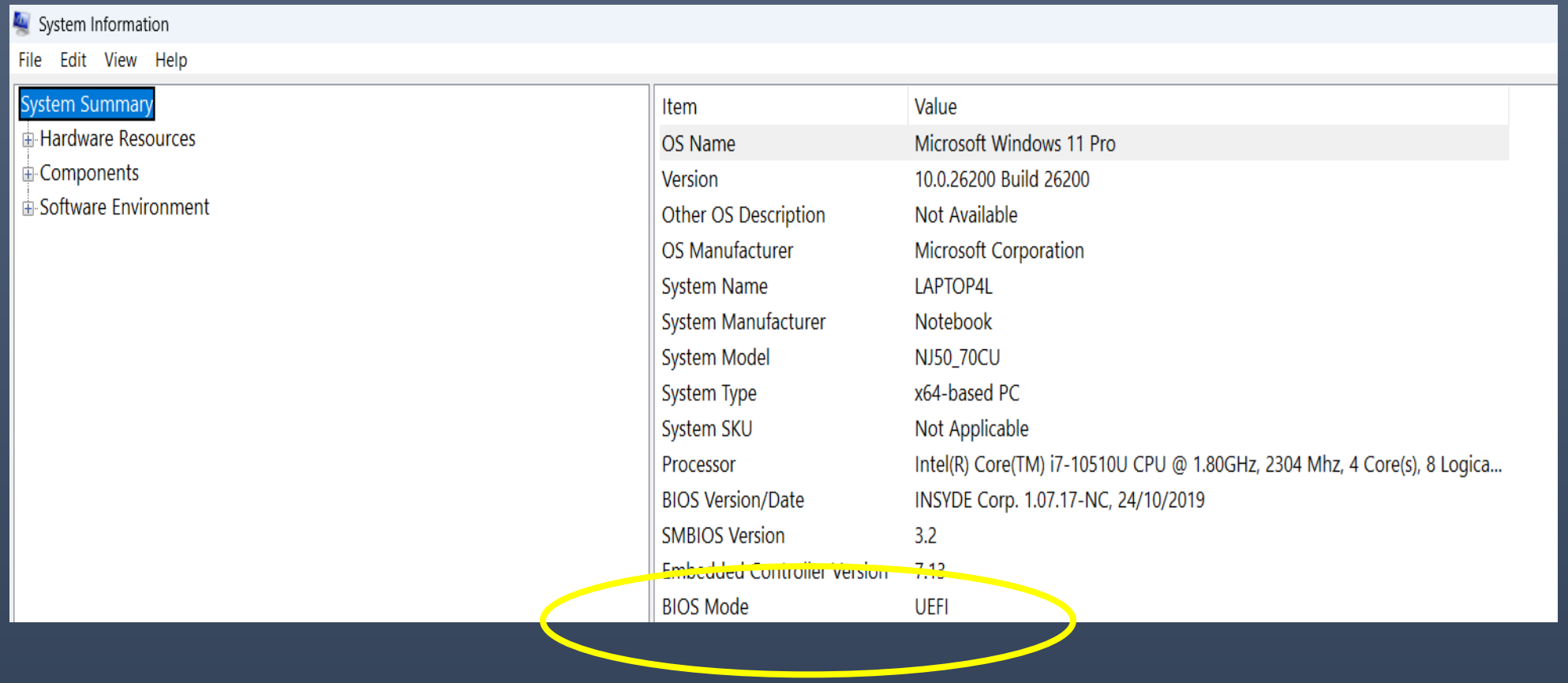
BIOS/UEFI


CMOS Setup Utility - Copyright (C) 1984-2010 Award Software
Advanced BIOS Features
Hard Disk Boot Priority [Press Enter]
Quick Boot [Disabled]
First Boot Device [USB-HDD]
Second Boot Device [CDROM]
Third Boot Device
Password Check
HDD S.M.A.R.T. Ca
Limit CPUID Max.
No-Execute Memory
Delay For HDD (Se
Full Screen LOGO
Backup BIOS Image
Init Display Firs
Item Help
Menu Level
First Boot Device
CDROM ..... [ ]
ZIP ..... [ ]
USB-FDD ..... [ ]
USB-ZIP ..... [ ]
USB-CDROM ..... [ ]
USB-HDD ..... [■]
Legacy LAN ..... [ ]
Disabled ..... [ ]
↑↓:Move ENTER:Accept
ESC:Abort
↑↓→←:Move Enter:Select +/-/PU/PD:Value F10:Save ESC:Exit F1:General Help
F5:Previous Values F6:Fail-Safe Defaults F7:Optimized Defaults


UEFI BIOS Utility – Advanced Mode
06/13/2016 Monday 13:51
English
MyFavorite(F3)
Qfan Control(F6)
EZ Tuning Wizard(F11)
Quick Note(F9)
Hot Keys
My Favorites Main Ai Tweaker Advanced Monitor Boot Tool Exit
Target CPU Turbo-Mode Frequency : 4200MHz
Target CPU @ AVX Frequency : 4200MHz
Target DRAM Frequency : 2800MHz
Target Cache Frequency : 2800MHz
Target DMI/PEG Frequency : 100MHz
Ai Overclock Tuner Manual
CPU Strap 100MHz
Source Clock Tuner Auto
PLL Selection Auto
Filter PLL Auto
BCLK Frequency 100.0
Initial BCLK Frequency Auto
ASUS MultiCore Enhancement Auto
[Manual]: When the manual mode is selected, the BCLK(base clock) frequency can be assigned manually.
[XMP]: When the XMP(extreme memory profile) mode is selected, the BCLK frequency and memory parameters will be optimized automatically.
Hardware Monitor
CPU
Frequency 3000 MHz
Temperature 31°C
BCLK 100.0 MHz
Core Voltage 1.250 V
Ratio 30x
Memory
Frequency 2800 MHz
Vol_CHAB 1.356 V
Capacity 16384 MB
Vol_CHCD 1.353 V
Voltage
+12V 12.096 V
+5V 4.960 V
+3.3V 3.248 V
Last Modified
EzMode(F7)
Search on FAQ
Version 2.17.1246. Copyright (C) 2016 American Megatrends, Inc.

Bios of UEFI

- In Windows, gebruik msinfo32 (typ in zoekpictogram in de taakbalk)



Bios - waarom

- Een BIOS (Basic Input/Output System) is nodig omdat het de eerste software is die draait bij het opstarten.
- Dit is essentieel voor de communicatie tussen hardware en het besturingssysteem.
- Het bepalen vanaf welke schijf op te starten. Zonder BIOS start je pc niet op en kunnen componenten niet met elkaar praten, waardoor het systeem onbruikbaar wordt.

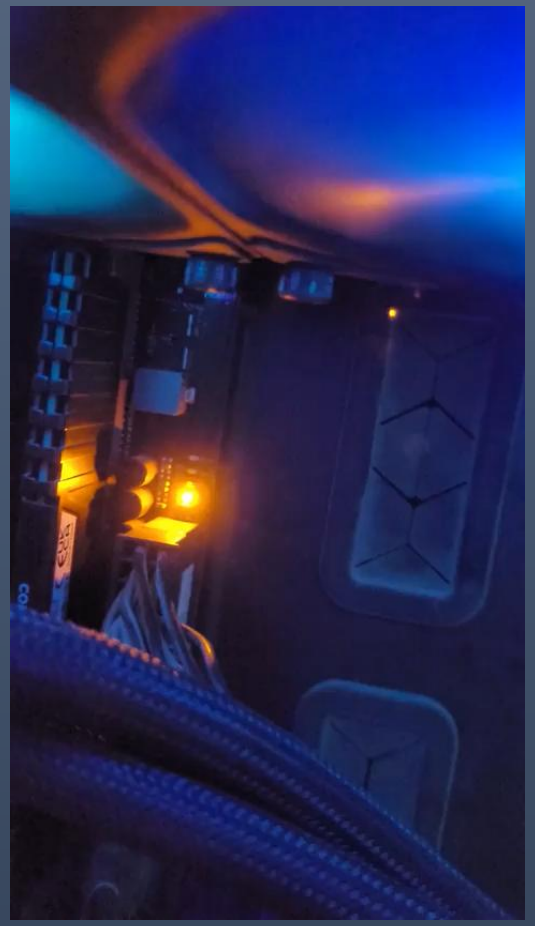
Bios - Belangrijkste functies

- Hardware-initialisatie: Controleert of CPU, videokaart, geheugen en moederbord werken POST. (Power On Self Test).
- Fouten worden aangegeven door LED’s en beeps.
- Verschillende BIOS-fabrikanten (zoals Award en AMI) gebruiken unieke codes, dus tel de pieptonen en raadpleeg de handleiding van uw moederbord.

POST – Piepcodes

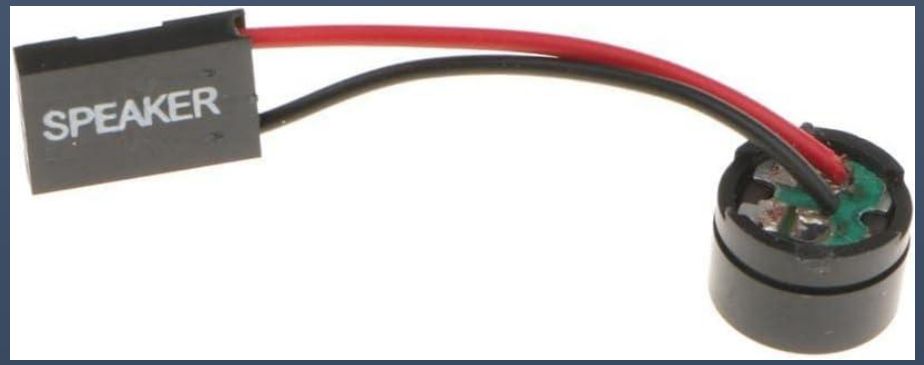
- Eén korte piep: Alles is in orde! De POST is geslaagd en de computer start normaal op.
- Twee korte pieptonen: Een niet-fatale fout, mogelijk een klein probleem zoals een vastzittende toets of een CMOS-fout, maar het systeem kan nog steeds opstarten.
- Eén lange, twee korte: Wijst meestal op een defecte of probleem met de videokaart.
- Eén lange, drie korte: Wijst vaak op een defecte toetsenbordcontroller.
- Continue pieptonen (lang/kort): Kunnen duiden op kritieke problemen, vaak met het geheugen (RAM) of het moederbord self.

POST - Problemen



Geen Buzzer!

- Tegenwoordig hebben de meeste Laptops en Pc's geen buzzer of luidspreker. Dan wordt bij een POST fout geen geluid gehoord.
- Bij een Pc is het is makkelijk genoeg om een buzzer toe te voegen.
- Er is bijna altijd een aansluiting op de moederboard en een beeper toevoegen is snel gedaan



Amazon.nl

Zalati Buzzer Beeper Computer Motherboard Desktop PC Generic BIOS Internal Speaker € 3,99

Bios - Belangrijkste functies

- Boot (Opstarten):
  - Boot Order/Priority: Bepaalt de volgorde waarin de pc naar opstartbare apparaten zoekt (USB, SSD, HDD, Netwerk).
  - Pas op bij sommige BIOS ’en moet het USB ingestoken worden om überhaupt het in het boot lijst te laten verschijnen!
  - UEFI/Legacy Mode: Kiezen tussen de moderne UEFI of de oudere BIOS-modus (UEFI is meestal aanbevolen).
  - Secure Boot: Een beveiligingsfunctie die onbevoegde software blokkeert tijdens het opstarten (belangrijk voor Windows 11).

Bios - Belangrijkste functies

- System Configuration (Systeemconfiguratie):
  - System Time/Date: Instellen van de klok en datum.
  - SATA Configuratie: Instellen van SATA-poorten (AHCI/IDE modus).
  - Nooit veranderen voor een drive dat al in gebruik is, omdat het drive daarna kan niet benaderde worden!
  - USB Configuratie: Beheer van USB-poorten.
- Advanced (Geavanceerd):
  - CPU Configuration: Overklokken, C-states, Hyper-Threading.
  - Memory (RAM): XMP (Intel) of DOCP/A-XMP (AMD) profielen om RAM op de geadverteerde snelheid te laten draaien.

Bios - Belangrijkste functies

- Security (Beveiliging):
  - Passwords: BIOS-wachtwoord instellen.
  - TPM (Trusted Platform Module): Voor versleuteling en beveiliging, vaak nodig voor Windows 11.
- Monitor/Hw Monitor:
  - Fan Control: Snelheden van ventilatoren instellen.
  - Temperatuur/Voltage: Lezen van systeemtemperaturen, voltages en fan-snelheden.

Bios - Veelgebruikte Functietoetsen:

- F1/F2/Del/Esc: Om de BIOS/UEFI binnen te gaan.
- F9: Laden van standaardinstellingen.
- F10: Opslaan en afsluiten.

BIOS - leveranciers

- Oorspronkelijk was de BIOS van IBM
- Daarna verschillende bedrijven, zoals **Compaq, Phoenix Technologies,** AMI hebben via reverse engineering nagemaakt om compatibele systemen te creëren.
- UEFI een open standaard die wordt beheerd door een consortium van bedrijven
- American Megatrends (AMI), Phoenix Technologies, and Insyde Software leveren hun BIOS aan diverse moederboard leveranciers.
- Als voorbeeld ASROCK gebruikt een aangepast versie van of AMI en soms Phoenix Technologies,.

Booting/Opstarten

- Opstarten is het proces waarbij een besturingssysteem wordt geladen. Dit proces begint wanneer we de computer aanzetten (met de aan/uit-knop of via een softwarecommando) en eindigt wanneer het besturingssysteem in het geheugen is geladen.
- Wanneer we de computer aanzetten, is er geen programma in het geheugen (RAM) van de computer. Dan zoekt de CPU naar een ander programma. Dit is in de EEPROM die zich op het moederbord bevindt. Door dit programma uit te voeren wordt de opstartprocedure gestart.
- Het opstartprogramma leest vervolgens de schijf om het opstartprogramma te laden en uit te voeren.

Booting

- Het opstartprogramma (of boot loader) laadt vervolgens het betreffende besturingssysteem en draagt de controle over aan het besturingssysteem.
- Er is geen fundamenteel verschil tussen een pc met een BIOS-systeem en een pc met een UEFI-systeem
- Het enige verschil zit hem in de manier waarop deze twee systemen dit doen
  - Maar meer later

Bios - Waarom updaten?

- Ondersteuning voor nieuwe hardware (bv. nieuwere CPU's).
- Oplossen van bugs en beveiligingsproblemen.
- Verbeteren van systeemprestaties en compatibiliteit.

BIOS updaten via Windows of DOS?

- De BIOS (of UEFI) updaten kan op twee manieren; via Windows of via DOS.
- Indien het update proces om wat voor reden dan ook wordt onderbroken zal uw moederbord niet meer functioneren. Dit is alleen te herstellen door de fabrikant, met uitzondering van dure moederborden met een reserve BIOS (dual BIOS).
- Vandaar dat u beter nooit via Windows kunt updaten!

Hoe

- Plaats de bestanden op een USB stick. Meestal zijn er enkele bestanden. Het belangrijkste bestand is het BIOS image. Dit bestand heeft een onbekende extensie en zal enkele megabytes groot zijn.
- Soms is het nodig de USB stick “bootable” te maken maar alle moderne moederborden kunnen een USB stick herkennen in de BIOS zonder speciale handelingen. Indien er alleen één .exe bestand wordt geleverd, voer dan dit bestand uit om de USB stick geschikt te maken.

Hoe

- Start de computer op in de BIOS mode.
- Dit wordt gedaan door tijdens het opstarten van de computer de juiste functie toets in te drukken.
- Druk tijdens het opstarten herhaaldelijk op de BIOS toets om in de BIOS te komen (meestal Delete F2 of F8).
- As U ziet het Windows logo dan was u te traag of gebruikte u de verkeerde toets.
- In het BIOS zoek naar de update functionaliteit. Deze bevat vaak het woord flash. Zo gebruikt MSI M-Flash. Asus heeft EZ Flash. Gigabyte heeft Q-Flash.

Een moederbord flashen zonder CPU

- Sommige moederborden kan zonder een CPU geflashed worden!
- Functies zoals **BIOS Flashback** (ASUS, MSI, ASRock) of **Q-Flash Plus** (Gigabyte).
- Op deze moederborden is een special USB-poorten en knoppen.
- Het moederbord heeft alleen een ATX-voeding en een USB-stick met de juiste BIOS-file nodig hebt

PC Firmware

- Om op te starten, leest de firmware de bootloader van de schijf. Hoe dit gebeurt, hangt af van de schijflay-out, waarvan er twee zijn:

MBR - Master Boot Record

GPT - De GUID (Globally Unique Identifier) Partition Table

- BIOS heeft alleen toegang tot MBR, maar UEFI heeft toegang tot beide.

MBR – een besturingssysteem opstarten

- Als de handtekening niet wordt gevonden, probeert het de volgende schijf, enzovoort. Wanneer deze wordt gevonden, draagt het BIOS de controle over aan deze eerste fase van de bootloader. Met andere woorden, de opcode op geheugenadres 0x7C00 in DRAM wordt uitgevoerd.
- De communicatie tussen het besturingssysteem en het BIOS verloopt via interrupts.

MBR – opstarten

- Bij sommige besturingssysteem, wanneer het BIOS-modus wordt gebruikt bij het opstarten, wordt de bootloader sterk afhankelijk van een aantal functies die door het BIOS zelf worden geleverd, voornamelijk de interrupts, int 10 (videodiensten) en int 13 (low-level schijfdiensten).
- Deze diensten worden gebruikt totdat de benodigde stuurprogramma's zijn geladen en beschikbaar zijn. Daarna zijn de BIOS-functies niet langer nodig.

BIOS Interrupts

Interrupt Vector	Beschrijving
05h	Shift-Print screen / BOUND-fout.
08h	Real-time klokonderbreking.
09h	Toetsenbordonderbreking.
10h	Videodiensten - Videomodus, Cursor Vorm/positie, Videomodus ophalen, Paletregisters (EGA, VGA, SVGA) .....
11h	Geeft apparatuur lijst weer
12h	Geeft conventionele geheugengrootte terug
13h	Low Level Disk Services
14h	Seriële poortdiensten
15h	Diverse systeemservices
16h	Toetsenborddiensten
17h	Printerservices

Interrupt Vector	Beschrijving
18h	Cassette BASIC uitvoeren:
19h	Laad het besturingssysteem.
1Ah	Real Time Klok-services
1Ah	PCI-services
1Bh	Ctrl-Break-handler
1Ch	Timer tick-handler
1Dh	Niet aanroepen;
1Eh	Niet aan te roepen;
1Fh	Niet aan te roepen;
41h	Adresaanwijzer: FDPT = Parameter tabel vaste schijf (1e harde schijf)
46h	Adresaanwijzer: FDPT = vaste schijf Parametertabel (2e harde schijf)
4Ah	Opgeroepen door RC voor alarm

UEFI – een besturingssysteem opstarten

- UEFI scant eerst naar beschikbare opstartvermeldingen in het NVRAM, waaronder besturingssystemen die op verschillende schijven of partities zijn geïnstalleerd.
- Vervolgens gebruikt het de standaardvermelding om de gewenste opstartoptie te selecteren uit de geselecteerde map van de speciale GPT EFI-partitie.
- Wanneer het systeem opstart met behulp van UEFI, start het ook op in Real Mode (16 bits), waarna de UEFI een rudimentair besturingssysteem op het platform bouwt om 32/64-bits Protected Mode mogelijk te maken.
- De communicatie tussen het besturingssysteem en UEFI verloopt via UEFI-services, niet via interrupts!

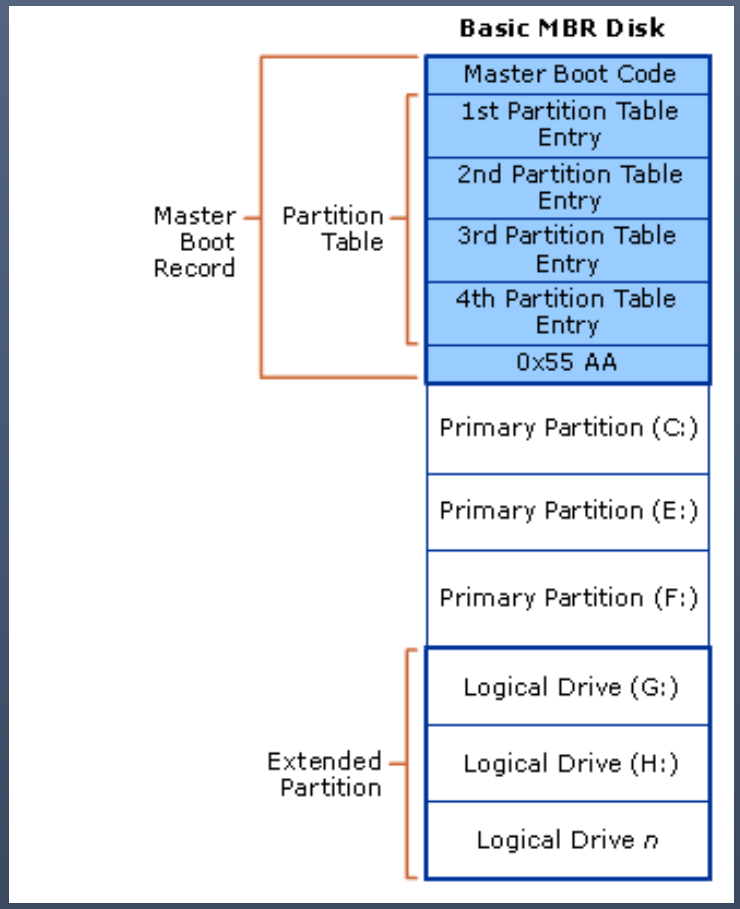
Schijforganisatie

- Er zijn twee methoden voor schijforganisatie voor opstartbare apparaten:

  - MBR – Master Boot Record
    - Dit is een methode waarbij de eerste sector van een gepartitioneerd of niet-gepartitioneerd medium (volume boot record) machinecode bevat voor het opstarten van programma's.
    - Voor gepartitioneerde media bevat de MBR de informatie over hoe de sectoren (ook wel "blokken" genoemd) van de schijf zijn verdeeld in partities.
  - GPT - GUID (Globally Unique Identifier) Partitie Tabel
    - Dit is de moderne versie van schijfpartitionering, gemaakt om de tekortkomingen van MBR-partitionering te verhelpen.

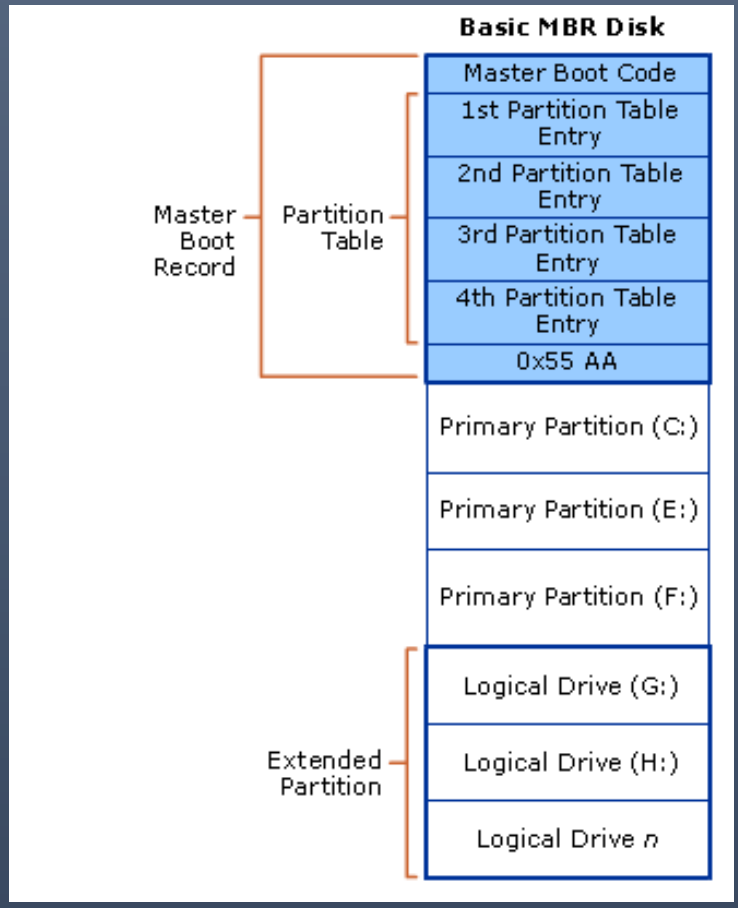
Schijforganisatie - MBR

- Een MBR-schijf heeft maximaal 4 primaire partities. Vaak wordt één primaire partitie, de zogenaamde uitgebreide partitie, onderverdeeld in een aantal logische partities
- In de allereerste sectoren van een MBR-schijf bevindt zich de opstartcode om het systeem op te starten. Het BIOS voert deze code uit, waardoor de specifieke opstartprocedure van het besturingssysteem wordt gestart Het volgende deel van de MBR zijn de partitietabellen



MBR

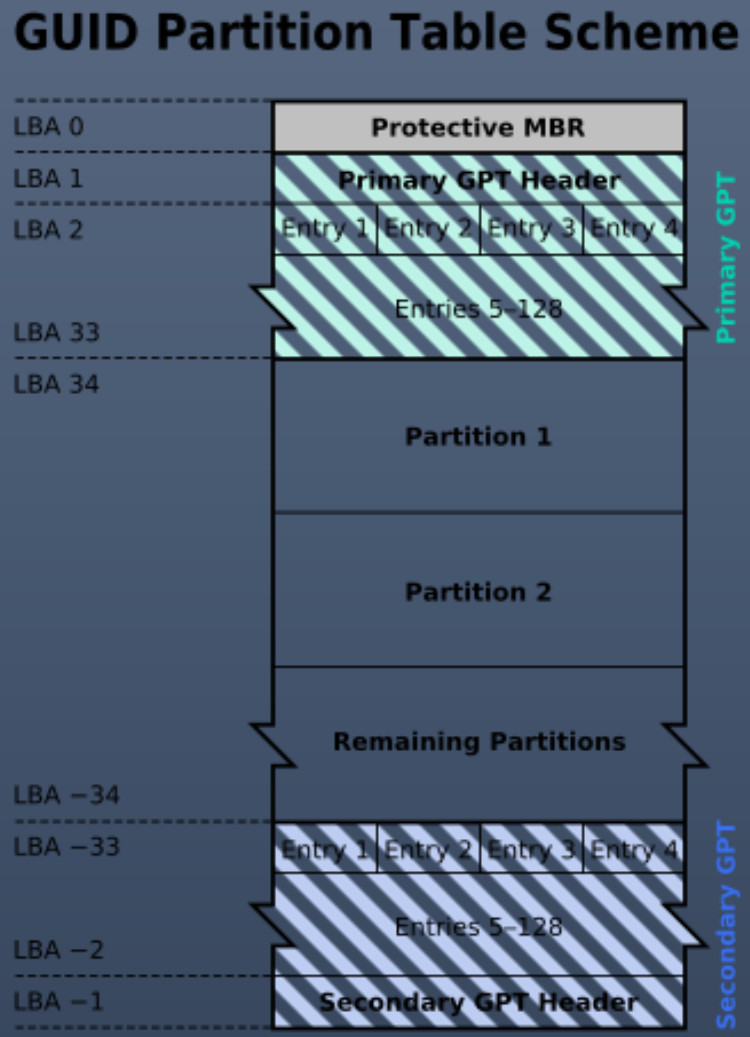
- Een MBR-schijf gebruikt 32 bits om het startpunt en de offset te beschrijven en heeft slechts toegang tot maximaal 2^{32} bytes, ongeveer 2,19 TB



Schijforganisatie - GPT

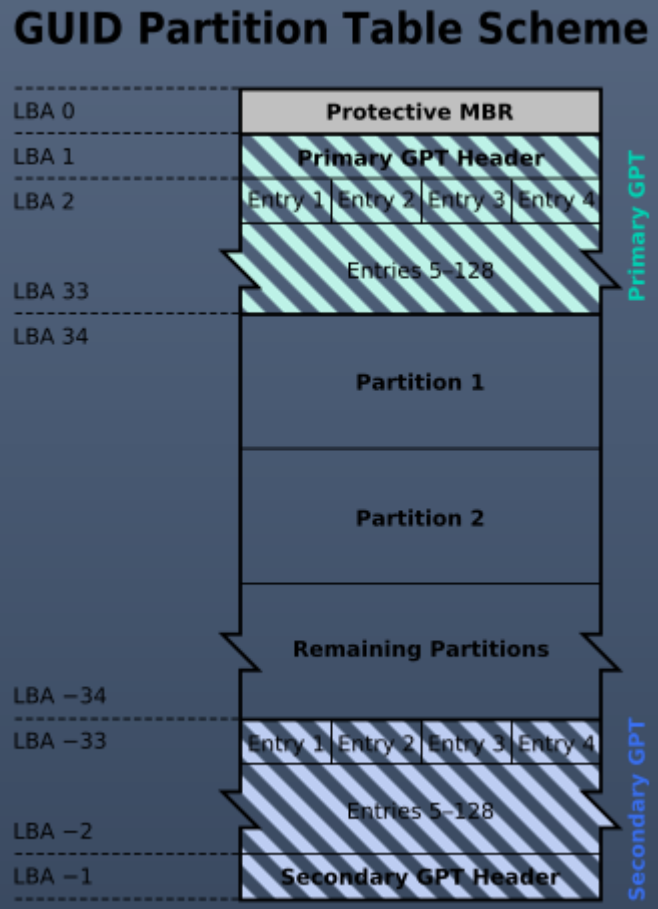
Een GPT-schijf bevat:

- Een beschermende MBR.
- Een primaire partitietabel
- Partitie-informatie
- Gegevenspartities.
- Een back-uppartitietabel



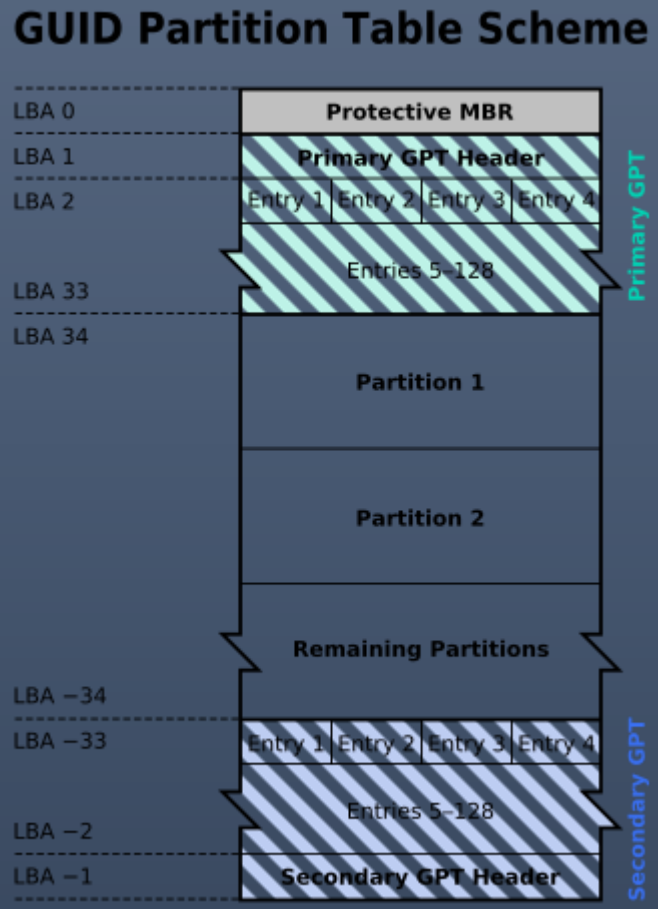
GPT – beschermende MBR

- Deze tabel bevat de beschermende MBR, GPT-header en partitietabel die het besturingssysteem helpen om informatie te laden en toegang te krijgen tot bestaande partitiegegevens.



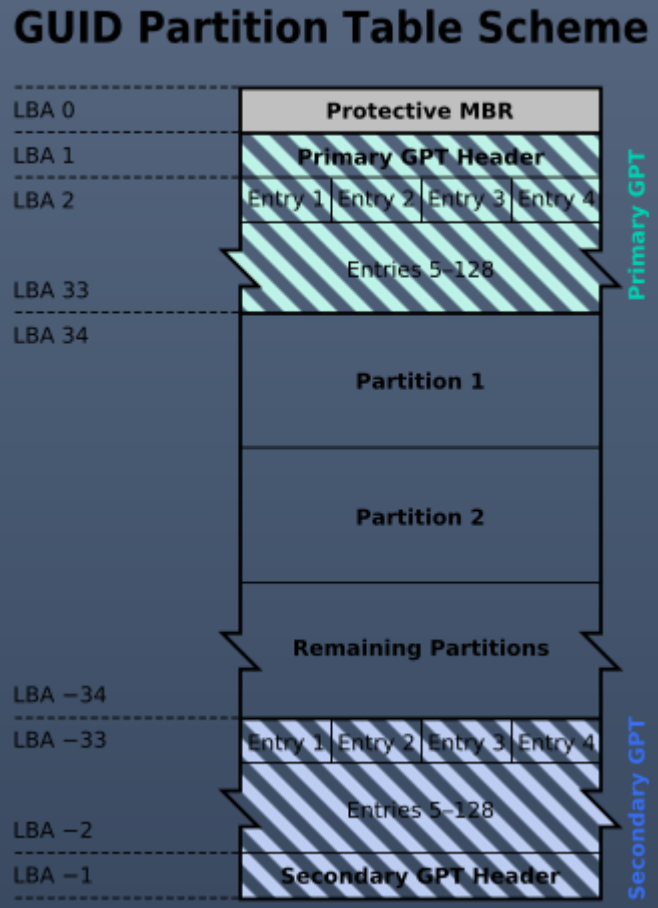
GPT - Primaire partitietabel:

- Deze tabel bevat de beschermende MBR, GPT-header en partitietabel die het besturingssysteem helpen om informatie te laden en toegang te krijgen tot bestaande partitiegegevens.



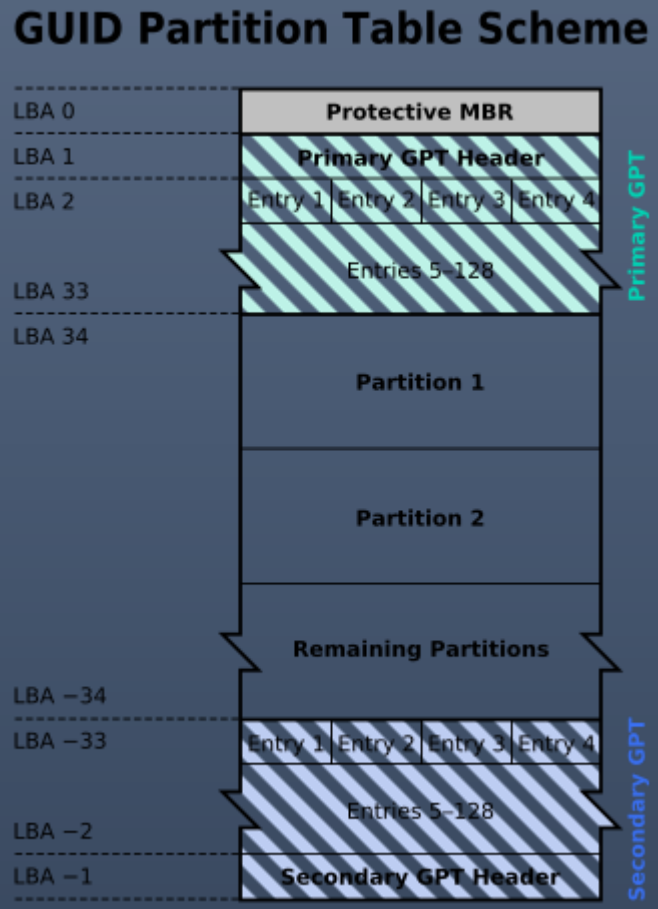
GPT - Normale gegevenspartities

- Dit is de fysieke locatie waar de GPT-schijf uw gegevens en persoonlijke bestanden opslaat (128 partities).
- De 128 partities zijn een de facto standaard (Microsoft), hoewel er in theorie een onbeperkt aantal partities mogelijk is.



GPT - Back-uppartitietabel

- Dit is het gebied waar de GPT-schijf de back-upinformatie voor de GPT-header en partitietabel bewaart. Het beschermt uw GPT-schijf effectief tegen verlies of beschadiging van de primaire partitietabel.



GUID Partitietabelkop (LBA 1)

Length	Contents	
8 bytes	Signature ("EFI PART", 45h 46h 49h 20h 50h 41h 52h 54h or 0x5452415020494645ULL[a] on little-endian machines)	
4 bytes	Revision number of header - 1.0 (00h 00h 01h 00h) for UEFI 2.10	
4 bytes	Header size in little endian (in bytes, usually 5Ch 00h 00h 00h or 92 bytes)	
4 bytes	CRC32 of header (offset +0 to +0x5b) in little endian, with this field zeroed during calculation	
4 bytes	Reserved; must be zero	
8 bytes	Current LBA (location of this header copy)	
8 bytes	Backup LBA (location of the other header copy)	
8 bytes	First usable LBA for partitions (primary partition table last LBA + 1)	
8 bytes	Last usable LBA (secondary partition table first LBA − 1)	
16 bytes	Disk GUID in mixed endian[12]	
8 bytes	Starting LBA of array of partition entries (usually 2 for compatibility)	
4 bytes	Number of partition entries in array	
4 bytes	Size of a single partition entry (usually 80h or 128)	
4 bytes	CRC32 of partition entries array in little endian	
*	Reserved; must be zeroes for the rest of the block (420 bytes for a sector size of 512 bytes; but can be more with larger sector sizes)	

Reference - https://en.wikipedia.org/wiki/GUID_Partition_Table

GUID-partitie-invoerformaat (LBA 2–33)

GUID partition entry format		
Offset	Length	Contents
0 (0x00)	16 bytes	Partition type GUID (mixed endian[12])
16 (0x10)	16 bytes	Unique partition GUID (mixed endian)
32 (0x20)	8 bytes	First LBA (little endian)
40 (0x28)	8 bytes	Last LBA (inclusive, usually odd)
48 (0x30)	8 bytes	Attribute flags (e.g. bit 60 denotes read-only)
56 (0x38)	72 bytes	Partition name (36 UTF-16LE code units)

90B6FF38-B98F-4358-A21F-48F35B4A8AD3
ArcaOS Type 1

36 Unicode tekens

Inclusief :
actieve vlag (voor legacy), alleen-lezen, schaduwkopie (van een andere partitie), verborgen, geen stationsletter (d.w.z. niet automatisch koppelen)

Reference - https://en.wikipedia.org/wiki/GUID_Partition_Table

GUID-partitietypetabel (gedeeltelijk)

Operating System	Partition type	Globally unique identifier (GUID)
…		
…		
Android 6.0+ ARM	Android Meta	19A710A2-B3CA-11E4-B026-10604B889DCF
	Android EXT	193D1EA4-B3CA-11E4-B075-10604B889DCF
Open Network Install Environment (ONIE)	Boot	7412F7D5-A156-4B13-81DC-867174929325
	Config	D4E6E2CD-4469-46F3-B5CB-1BFF57AFC149
PowerPC	PReP boot	9E1A2D38-C612-4316-AA26-8B49521E5A8B
freedesktop.org OSes (Linux, etc.)	Shared boot loader configuration[77]	BC13C2FF-59E6-4262-A352-B275FD6F7172
Atari TOS	Basic data partition (GEM, BGM, F32)	734E5AFE-F61A-11E6-BC64-92361F002671
VeraCrypt	Encrypted data partition	8C8F8EFF-AC95-4770-814A-21994F2DBC8F
OS/2	ArcaOS Type 1	90B6FF38-B98F-4358-A21F-48F35B4A8AD3
Storage Performance Development Kit (SPDK)	SPDK block device[78]	7C5222BD-8F5D-4087-9C00-BF9843C7B58C
barebox bootloader	barebox-state[79]	4778ED65-BF42-45FA-9C5B-287A1DC4AAB1
U-Boot bootloader	U-Boot environment[80][81]	3DE21764-95BD-54BD-A5C3-4ABE786F38A8
SoftRAID[citation needed]	SoftRAID_Status	B6FA30DA-92D2-4A9A-96F1-871EC6486200
	SoftRAID_Scratch	2E313465-19B9-463F-8126-8A7993773801
	SoftRAID_Volume	FA709C7E-65B1-4593-BFD5-E71D61DE9B02
	SoftRAID_Cache	BBBA6DF5-F46F-4A89-8F59-8765B2727503
Fuchsia standard partitions[82]	Bootloader (slot A/B/R)	FE8A2634-5E2E-46BA-99E3-3A192091A350
	Durable mutable encrypted system data	D9FD4535-106C-4CEC-8D37-DFC020CA87CB
	Durable mutable bootloader data (including	A409E16B-78AA-4ACC-995C-302352621A41
	Factory-provisioned read-only system data	F95D940E-CABA-4578-9B93-BB6C90F29D3E
	Factory-provisioned read-only bootloader data	10B8DBAA-D2BF-42A9-98C6-A7C5DB3701E7
…		

Reference - https://en.wikipedia.org/wiki/GUID_Partition_Table

GPT – Schijfgroottes

- Terwijl MBR 32 bits gebruikt om een blok te adresseren, gebruikt GPT 64 bits.
- Voor schijven met een sectoromvang van 512 bytes is de maximale grootte

  9,4 ZB

  = 9.400.000.000 TB

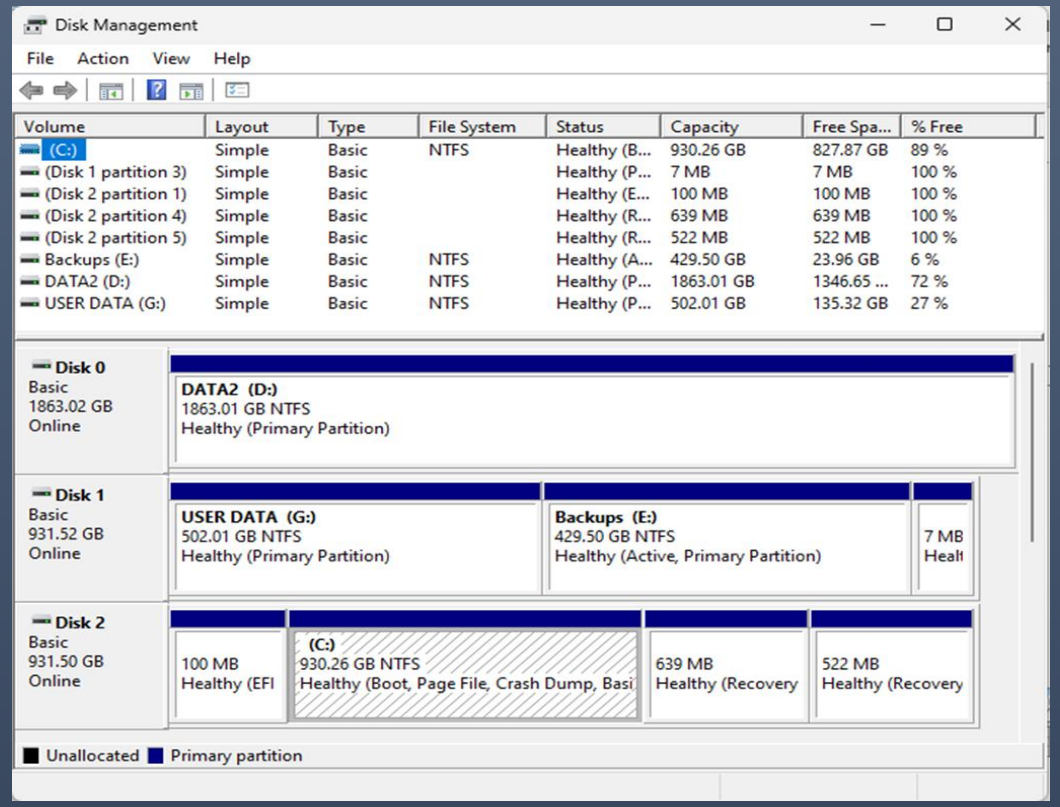
- 1 Zb = 10^{21} $bytes$

Schijforganisatie GPT – UUID

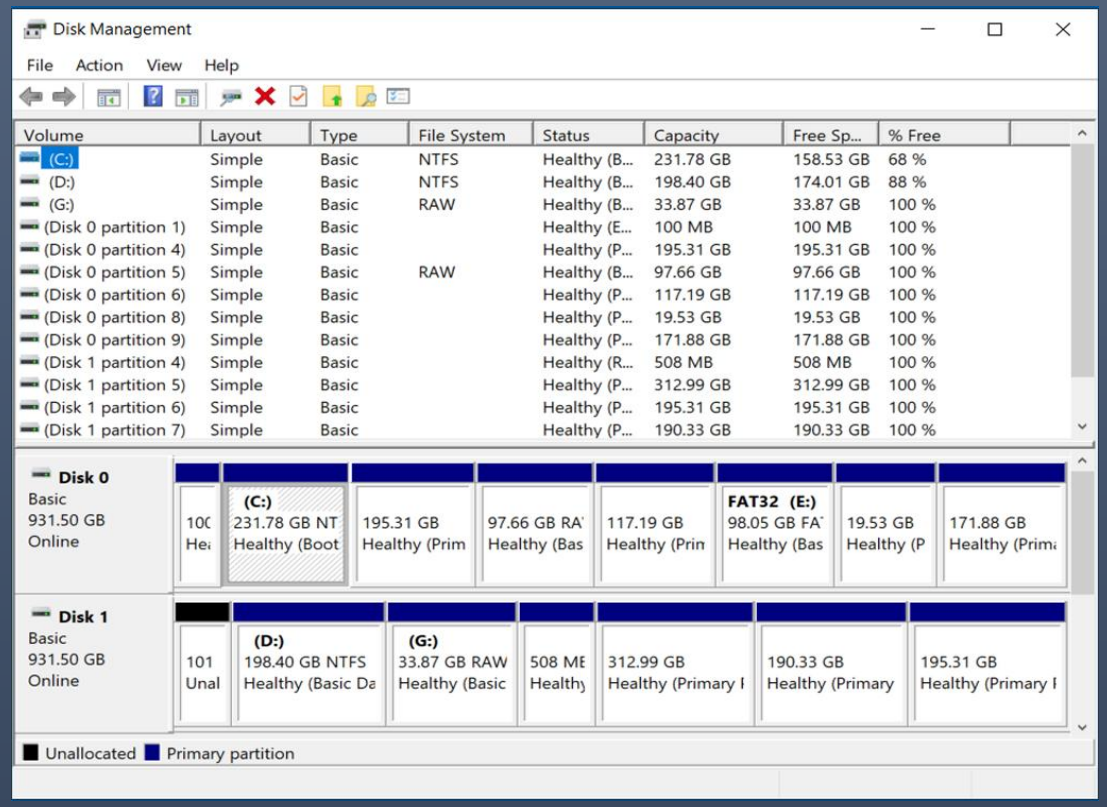
- UUID - Een UUID (Universal Unique Identifier) is een 128-bits waarde die wordt gebruikt om een object of entiteit uniek te identificeren. Afhankelijk van de specifieke mechanismen die worden gebruikt, is een UUID gegarandeerd verschillend, of in ieder geval zeer onwaarschijnlijk hetzelfde als enige andere UUID die tot het jaar 3400 na Christus wordt gegenereerd.
- Let op, voor schijven zijn er twee soorten
  - Schijf-UUID
  - Partitie-UUID

MBR/GFT Schijfindeling

MBR-schijfindeling



GPT-schijfindeling



EFI - De speciale GPT-partitie

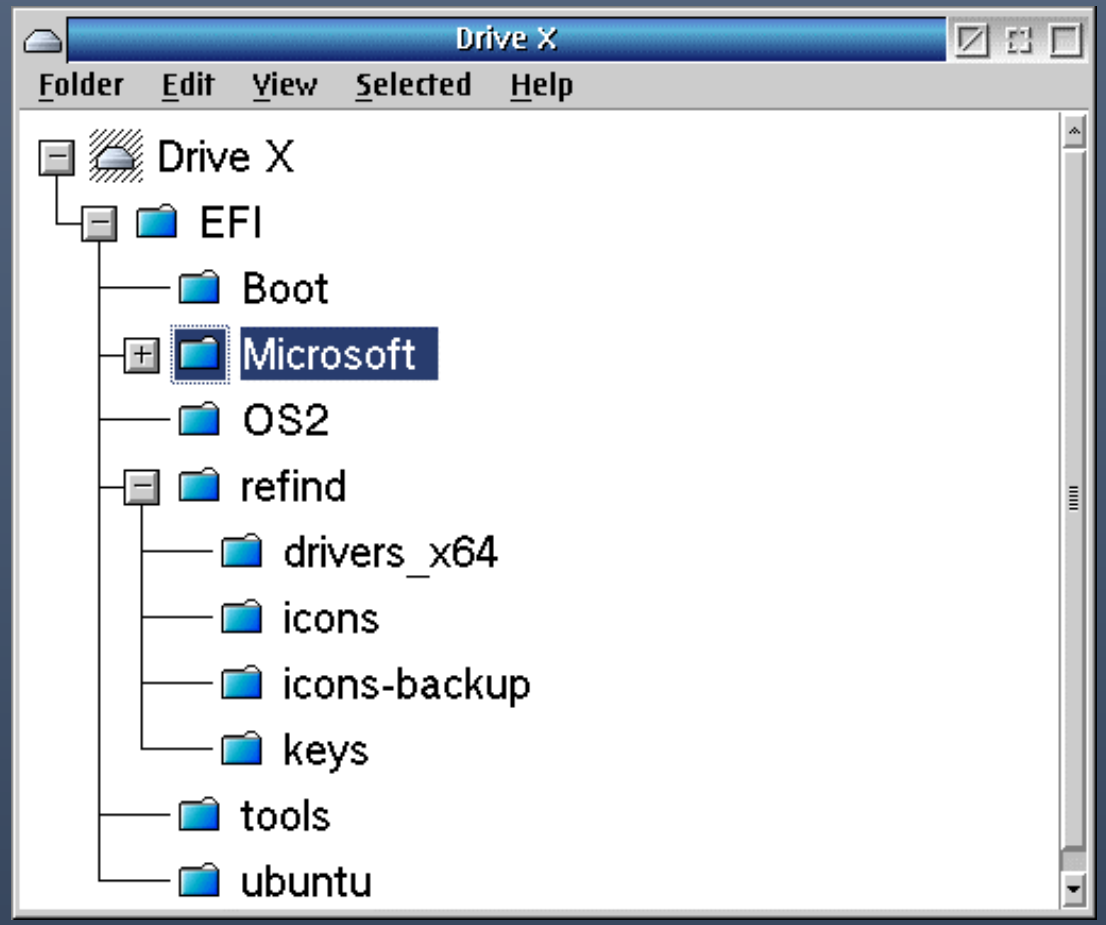
- Er is een speciale partitie op een GPT-schijf, de EFI-partitie (ook wel ESP genoemd).
- Dit is een OS-onafhankelijke partitie die fungeert als opslagplaats voor de UEFI-bootloaders, applicaties en stuurprogramma's en die is toegankelijk is voor de UEFI-firmware.
- Deze partitie is **verplicht** voor UEFI-opstarten.
- Dit is een FAT32-partitie met een grootte van ongeveer 100 MB, maar deze kan indien nodig groter (of kleiner) zijn.
- De inhoud van deze partitie is normaal gesproken niet zichtbaar, maar er zijn tools/opdrachten beschikbaar om deze te bekijken.

Inhoud van de EFI-partitie

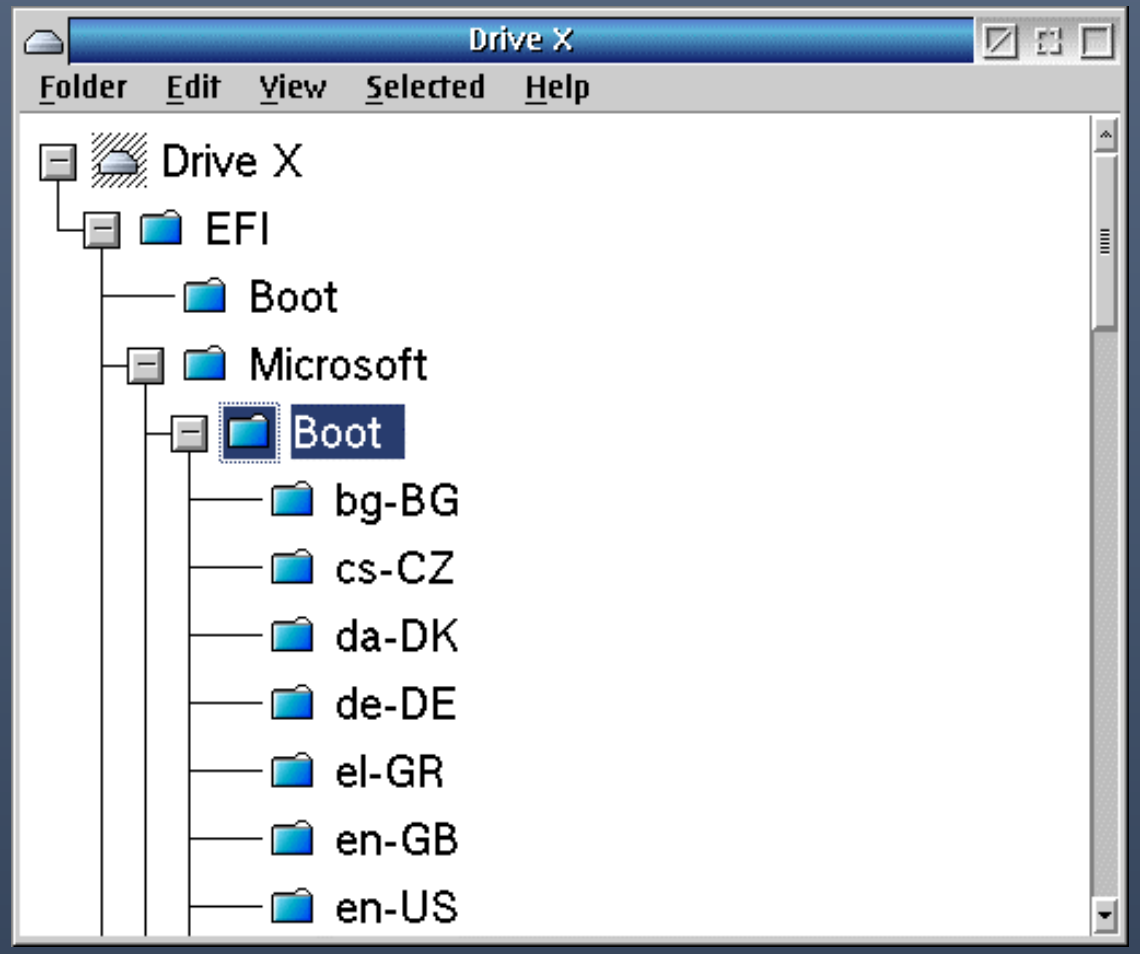
- De EFI-partitie bevat meestal een aantal mappen en submappen.
- De partitie slaat het opstartprogramma voor het besturingssysteem of de besturingssystemen op.
- Het kan ook speciale tools, programma's en opstartmanager(s) bevatten.

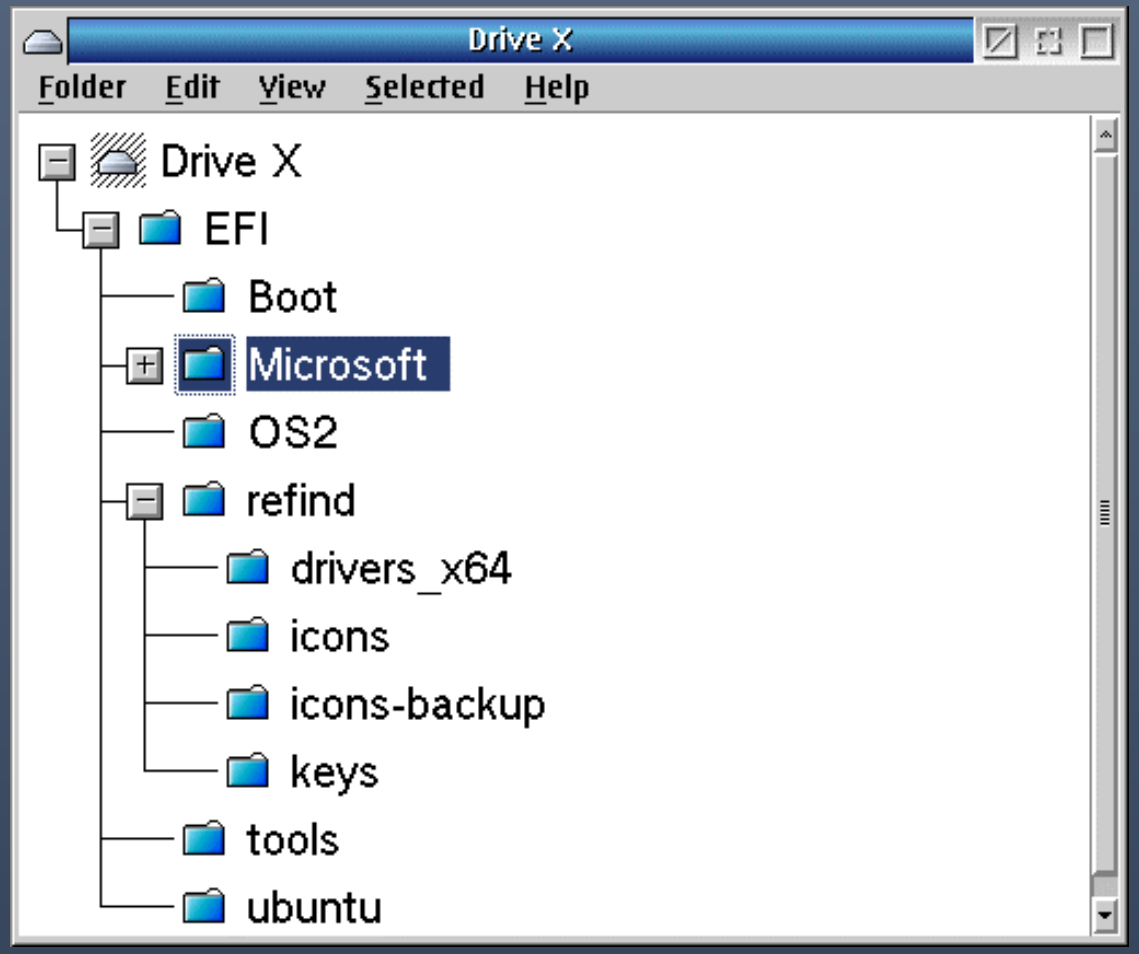
Inhoud van de EFI-partitie (voorbeeld)

- In dit voorbeeld bevat de EFI-partitie de mappen voor drie besturingssystemen
  - Microsoft (w10),
  - OS2 (ArcaOS)
  - Ubuntu.
- De partitie bevat ook de mappen van de opstartmanagers rEFind en AN Launcher
- Het bevat ook een map met hulpprogramma's



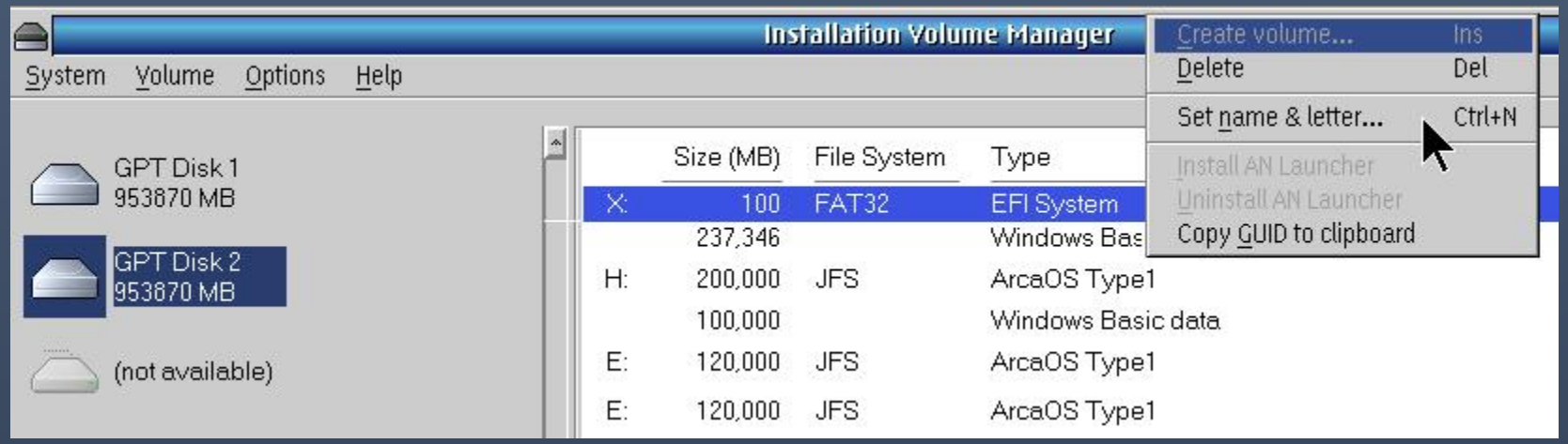
Inhoud van de EFI-partitie (voorbeeld)





De EFI-partitie bewerken/bekijken (ARCAOS (5.1))

- Selecteer Computer->Systeemconfiguratie ->
- Selecteer de partitie
- Opties -> naam en letter instellen
- Opslaan en afsluiten



De EFI-partitie bewerken/bekijken (Linux)

sudo fdisk -l (as root)

Device	Start	End	Sectors	Size	Type
/dev/sda1	2048	1128447	1126400	550M	EFI System
/dev/sda2	1128448	79626398	78497951	37.4G	Linux filesystem
/dev/sda3	79628288	85917854	6289567	3G	Linux swap

sudo mount /dev/sda1 /mnt

Ls –l

Nu kunt u uw favoriete editor gebruiken!

De EFI-partitie bewerken/bekijken (Linux)

sudo fdisk -l (as root)

Device	Start	End	Sectors	Size	Type
/dev/sda1	2048	1128447	1126400	550M	EFI System
/dev/sda2	1128448	79626398	78497951	37.4G	Linux filesystem
/dev/sda3	79628288	85917854	6289567	3G	Linux swap

sudo mount /dev/sda1 /mnt

Ls –l

Nu kunt u uw favoriete editor gebruiken!

De EFI-partitie bewerken/bekijken (Linux)

```
keith@keith-NJ50-70CU:/$ sudo ls -l /mnt/efi
total 6
drwx------ 2 root root 1024 mei 30  2021 Boot
drwx------ 4 root root 1024 mei 29  2021 Microsoft
drwx------ 2 root root 1024 sep 28  2021 OS2
drwx------ 6 root root 1024 dec 20 20:19 refind
drwx------ 2 root root 1024 jun 24  2021 tools
drwx------ 2 root root 1024 mei 30  2021 ubuntu
keith@keith-NJ50-70CU:/$
```

De EFI-partitie bewerken/bekijken (Windows)

Typ vanuit een verhoogde opdrachtprompt het volgende:

diskmgmt.msc (om de EFI-partitie te identificeren)

selecteer schijf 'n'

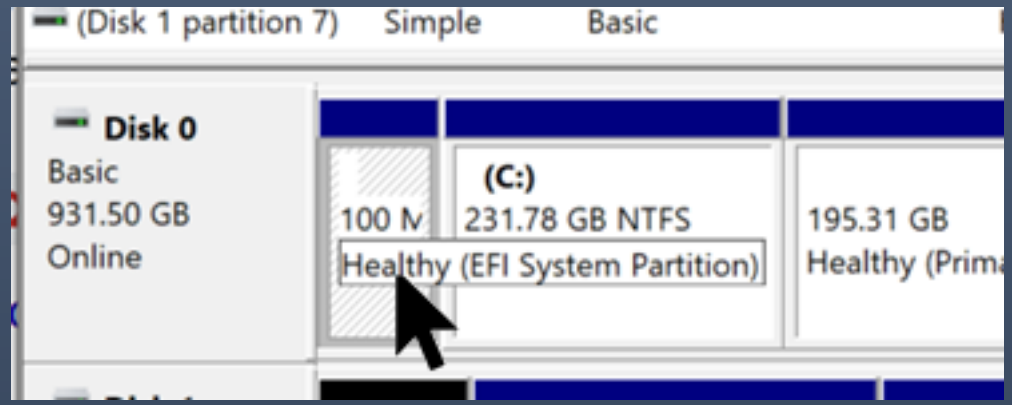
Partitie weergeven (om het partitienummer te verkrijgen)

selecteer partitie 'n'

letter toewijzen=X

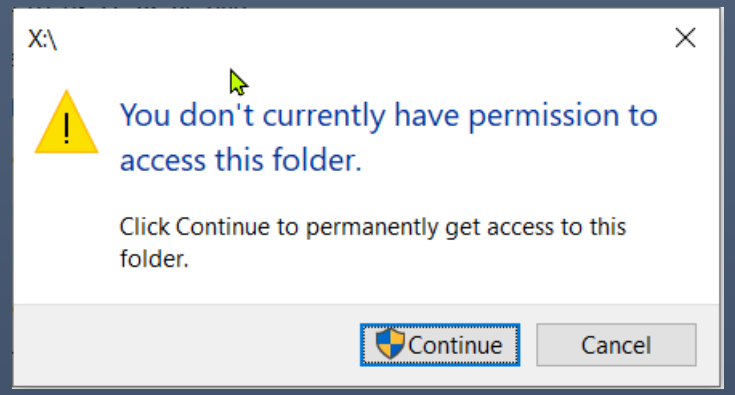
afsluiten

Notepad.exe (oude versie!)

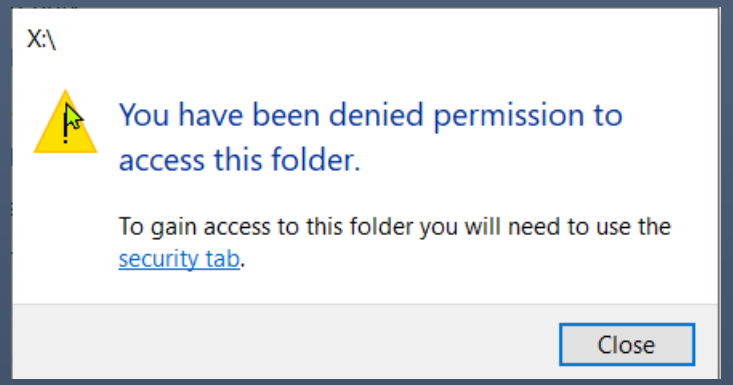


De EFI-partitie bewerken/bekijken (Windows)

Als u de bestandsverkenner gebruikt, krijgt u een foutmelding



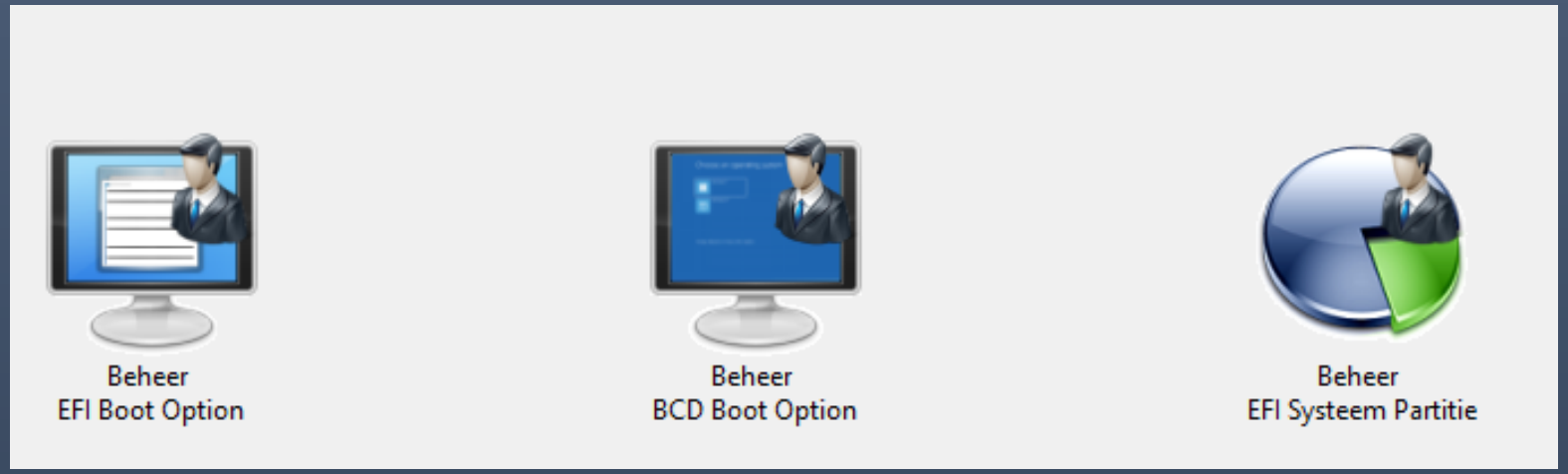
gevolgd door



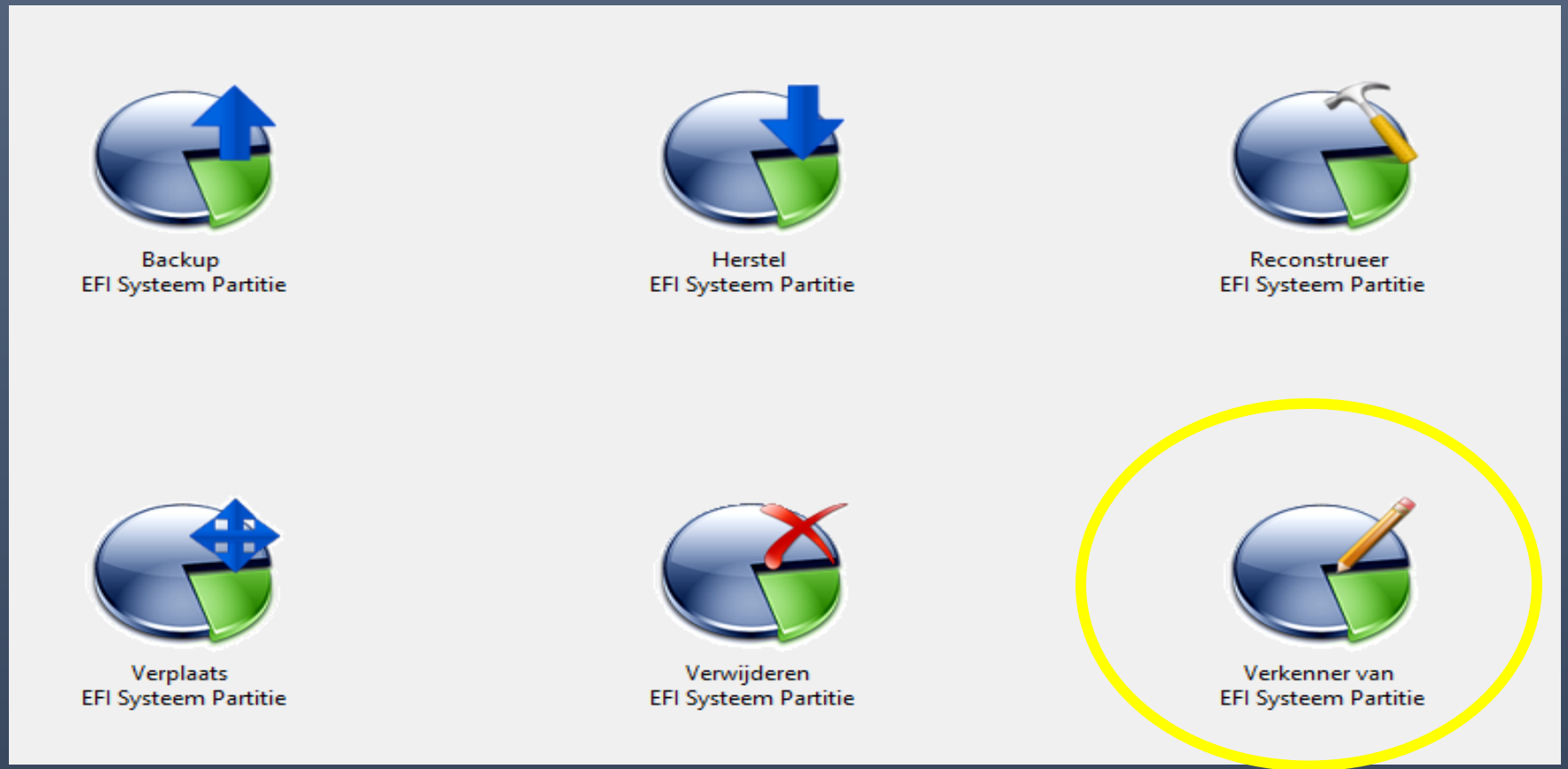
FAT32-partities hebben echter geen tabblad Beveiliging!

Het programma EasyUefi

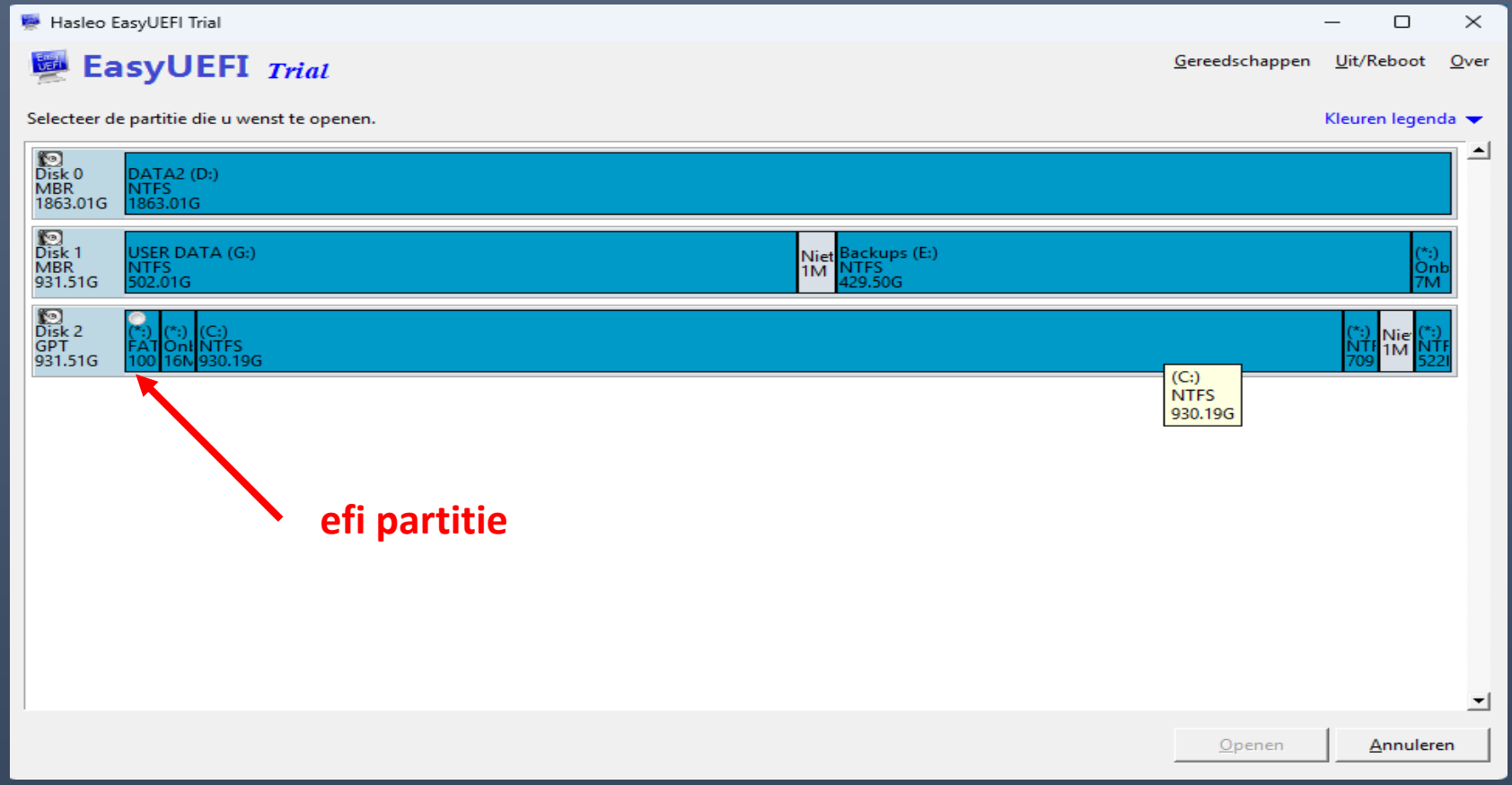
- Omdat het soms makkelijker kan is er het programma EasyUefi
- Is ook in het Nederlands
- Het programma is NIET gratis maar mag 14 dagen gebruikt worden



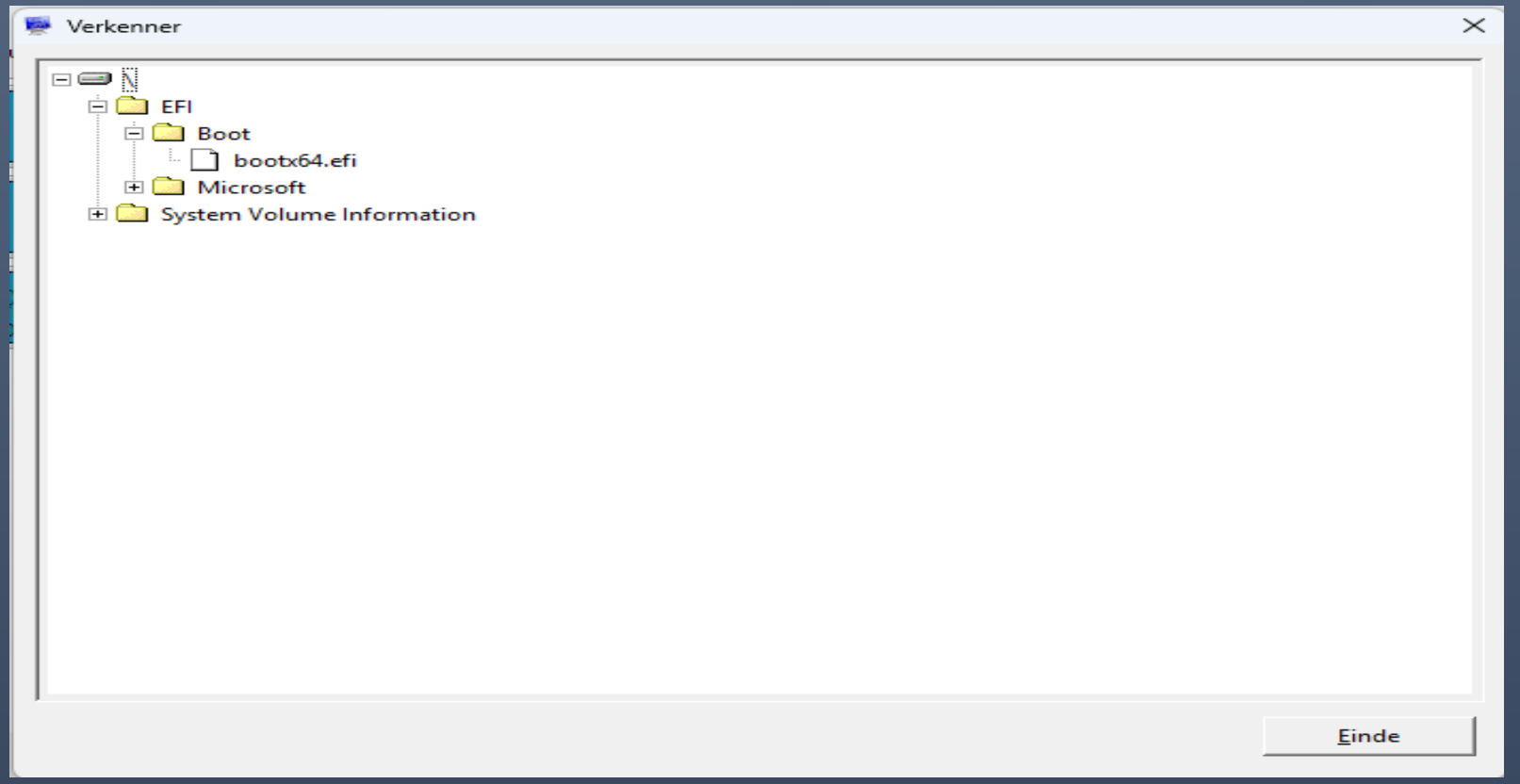
Via Verkenner van EFI



Verkenner van EFI – selecteer efi partitie



Verkenner van EFI



EFI – wat meer?

- Behalve bootloaders, zijn er ook programma's of tools, dat kan geladen en ook aangeroepen vanuit in het EFI partitie
- Het bekendste zijn:
  - EFI Shell – een primitief maar krachtige terminal programma
  - reFind – een boot selectie programma
  - MemTest – een geheugen test
  -
  -

Het EFI-Shell

- Het EFI-Shell is een opdrachtregelprogramma vergelijkbaar met de Linux-terminal.
- Na het opstarten wordt een lijst van (FAT32) partities weergegeven met hun kenmerken.
- Met het intypen van ‘help’ worden alle commando's met uitleg getoond. Met behulp van PgUp, PgDn kan het scherm ophoog of oplaag gescrold worden, zodat alle commando’s worden weergegeven.
- Met de cursor pijl omhoog wordt het eerder commando geselecteerd.
- Als een uitvoerbaar bestand wordt gebruik (xxxx.efi) wordt dat bestand uitgevoerd.
- Er is een script genoemd startup.nsh dat wordt automatisch opgestart wanneer het EFI shell wordt geladen

Het EFI-Shell

De commando's voor de EFI shell lijken op unix/linux of MSDOS commando's

- Bijvoorbeeld
  - ls maar met uitsluitend de opties –b –r -a
  - cd
  - mkdir
  - Echo
  - Cls (wis scheerm)
- Kleuren worden gebruikt om aan te geven wat voor type een bestand is. Blauw directories, groen uitvoerbaar, grijs alle andere bestanden.

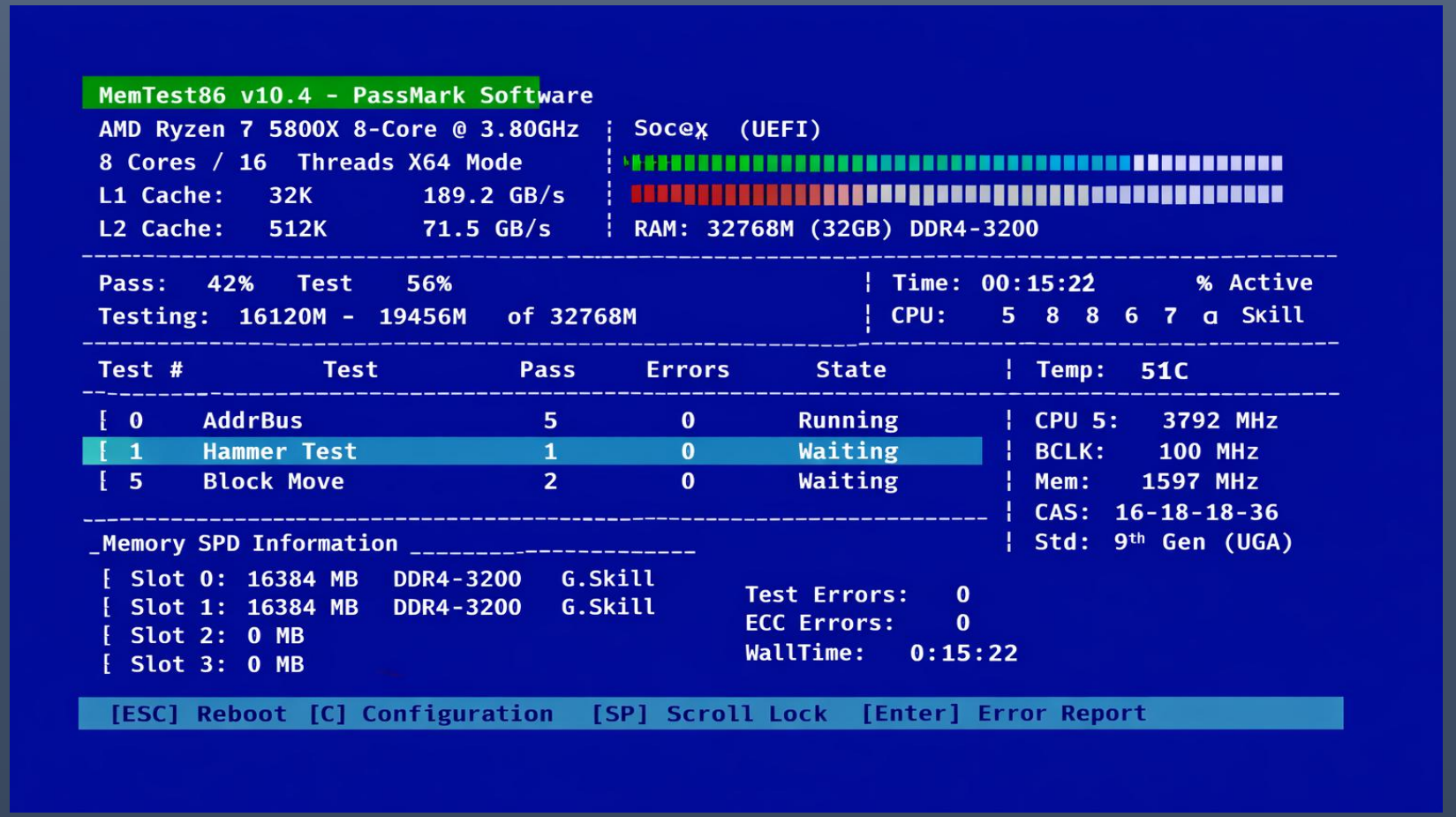
Het EFI-Shell – boot volgorde aanpassen

bcfg boot dump –b	*Dit geeft een lijst van bootable devices. Naar ‘Option’ is een getal waar 0 de eerste is*
bcfg boot mv 04 00	*Met dit commando wordt het bootable device 04 als eerste (00) geplaats en alle andere een positie later*

Het EFI-Shell – een OS selecteren

FS0:	*Selecteer de schijf waarop het Efi partite zich bevindt.*
ls	*Controleer dat de map EFI zich op deze schijf bevindt*
cd efi\Microsoft\Boot	*Ga naar de map van het boot lader*
Bootmgfw(.efi)	*Typ de naam van de lader app in*

Het Shell App memTest96 v10.4



Boot Managers

- De gemakkelijkste manier, als je wilt opstarten naar een ander besturingssysteem of zelfs een andere versie van hetzelfde systeem, is om een bootmanager te gebruiken.
- Bootmanagers zijn hoofdzakelijk in twee soorten die afhankelijk zijn van de firmware van de PC.

Boot Managers

- rEFInd - grafische UEFI bootmanager, boot :
    - WinNT/W10/W11, Linux, ArcaOS 5.1 (OS/2), BSD, MacOS ..
- AN Launcher - eenvoudige tekstuele UEFI bootmanager, start op:
    - WinNT/W10/W11, Linux , ArcaOS 5.1 (OS/2), MacOS

rEFInd

- rEFInd is een gratis (GNU licentie) programma ontwikkeld door Roderick W. Smith.
- Uitsluitend voor UEFI systemen
- Dynamische detectie van besturingssystemen.
- Aanpasbare OS-startopties.
- Grafische of tekstmodus. Het thema kan worden aangepast.
- Mac-specifieke functies, waaronder een spoofing-opstartproces
- Linux-specifieke functies, automatisch detecteren van de stubloader
- Ondersteuning voor “secure boot”

rEFInd

- Installatie in Linux (Ubuntu)
- Installatie in Windows (64bits)

rEFInd Installatie – Linux (Ubuntu)

Typ:

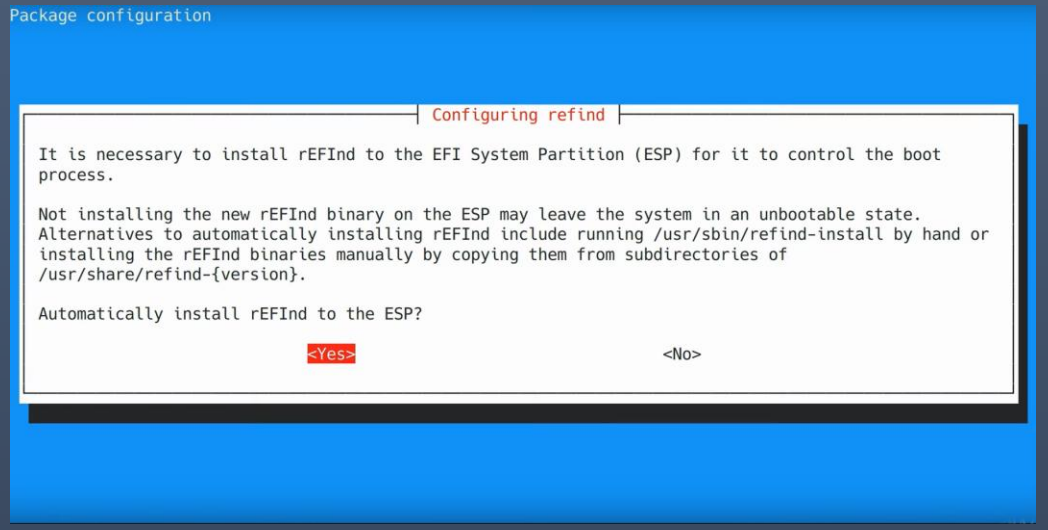
sudo apt-add-repository ppa:rodsmith/rEFInd

sudo apt-get update

sudo apt-get install rEFInd

At screen prompt select

Yes



- Computer afsluiten en opnieuw opstarten

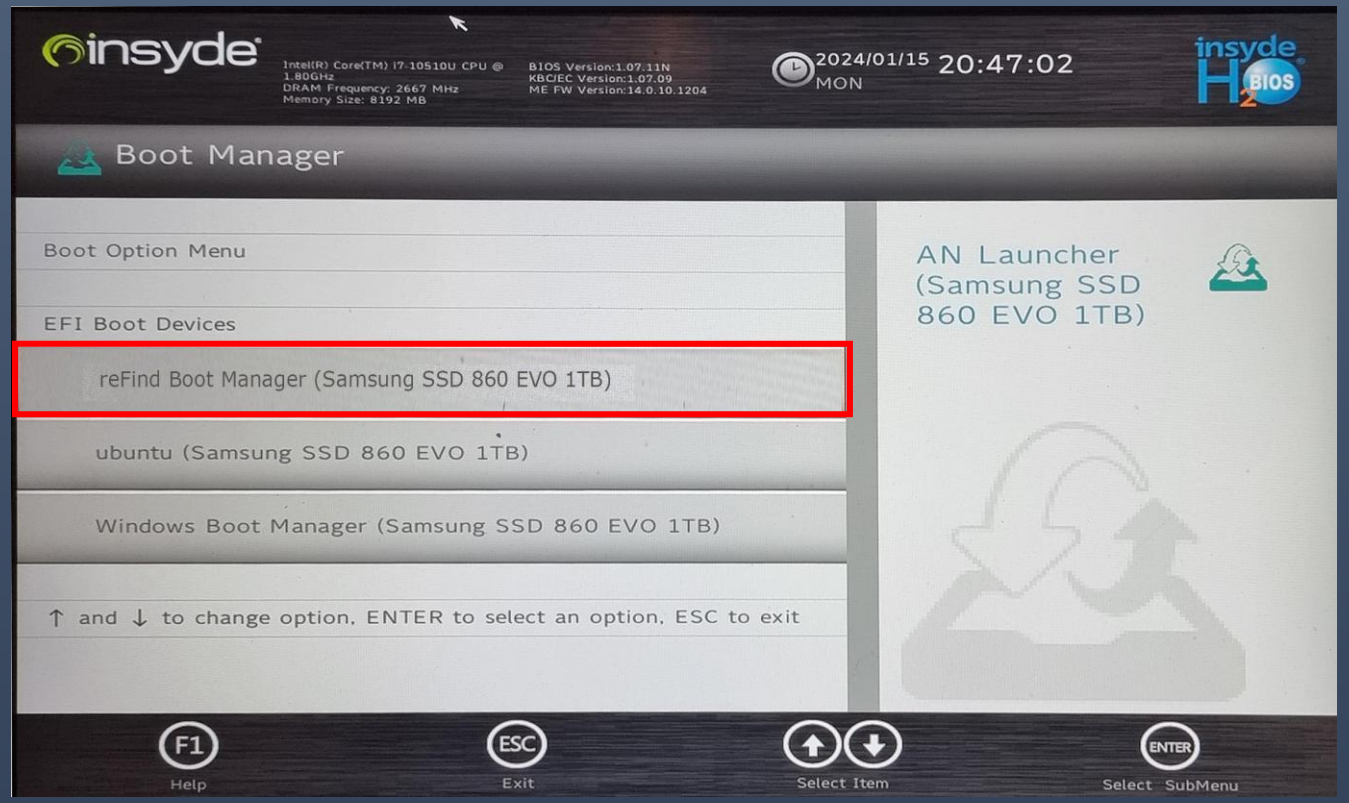
rEFInd Installatie – Linux (Ubuntu)

Het is mogelijk rEFInd ook met secure boot te installeren!

Dit is mogelijk door gebruik te maken van een shim

rEFInd Installatie – Linux (Ubuntu)

Controleer na het opnieuw opstarten of de opstartoptie correct is ingesteld in de UEFI-bios



rEFInd Installatie – Windows 64bit (deel 1)

Download het zip bestand van rEFInd van sourceforge

http://www.sourceforge.net/projects/rEFInd/

Vanaf een opdrachtprompt met verhoogde bevoegdheid, typ :

diskmgmt.msc (om de EFI-partitie te identificeren)
select disk ‘n’
List partition (to get partition number)
select partition ‘n’
assign letter=X
exit

Het zip bestand uitpakken en kopieer het volledig rEFInd folder en inhoud, naar het efi folder zo dat een nieuwe folder \efi\rEFInd ontstaat.

rEFInd Installatie – Windows 64bit (deel 2)

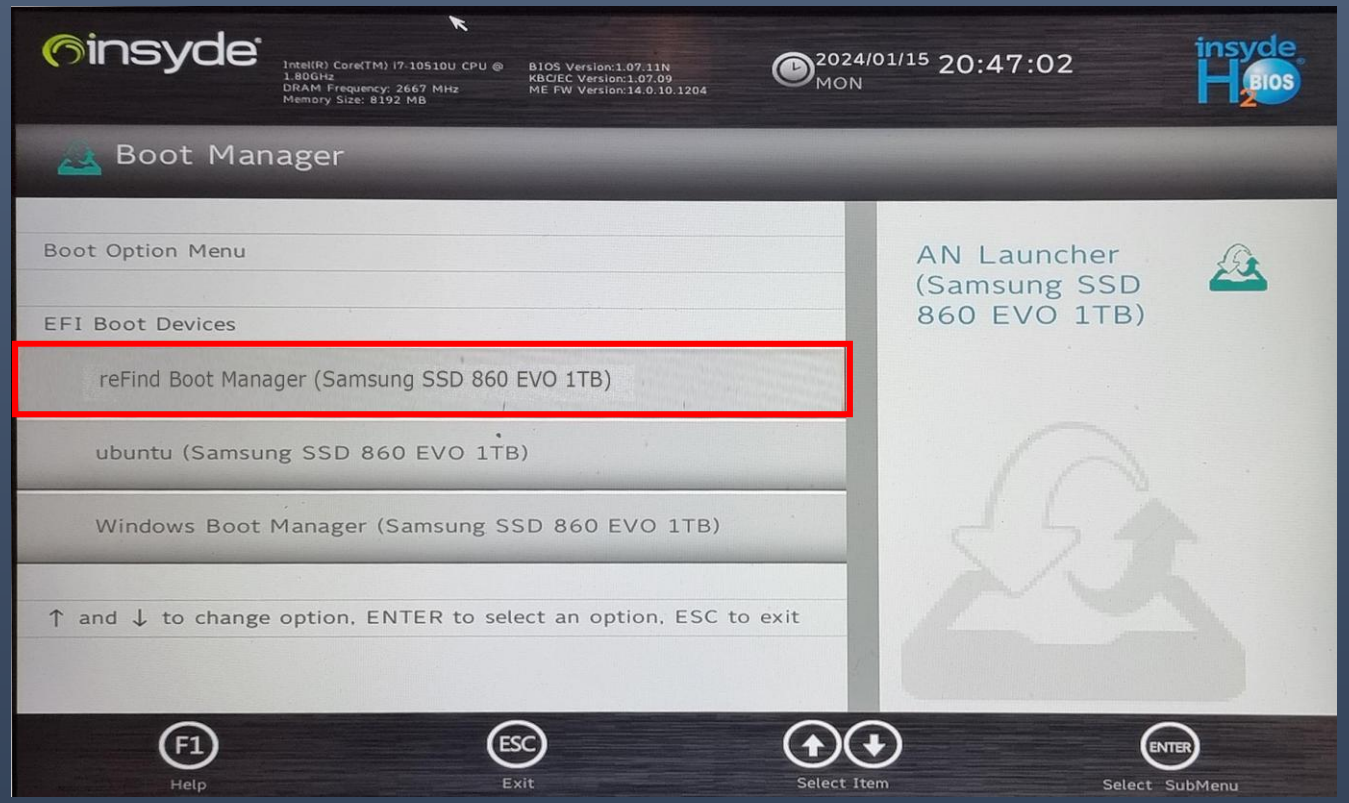
- In het folder “\efi\refind”, verwijder de folders: drivers_aa64 en drivers_ia32. Deze bestanden zijn allen nodig voor specifiek hardware.
- Om rEFInd in te stellen als het standaard EFI-opstartprogramma, typ vanaf een opdrachtprompt het volgende:

  bcdedit /set "{bootmgr}" path \EFI\rEFInd\rEFInd_x64.efi

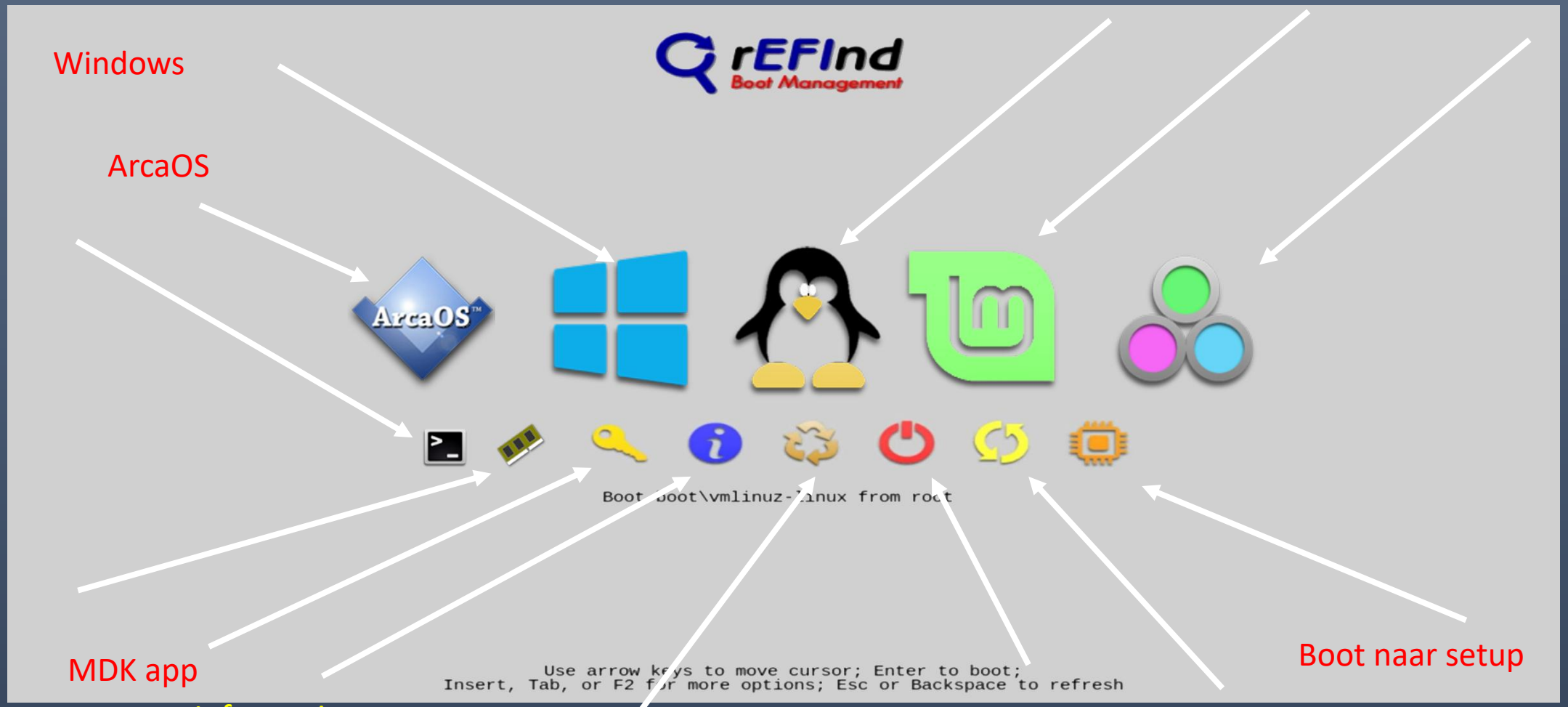
- Als je wilt, typ je bcdedit /set "{bootmgr}" beschrijving "rEFInd beschrijving“, om een eigen beschrijving in te stellen .
- Reboot system, en selecteer het UEFI BIOS.

rEFInd Installatie – Linux (Ubuntu)

Controleer na het opnieuw opstarten of de opstartoptie correct is ingesteld in de UEFI-bios



rEFInd Opstart scherm



Linux

Linux Mint

Onbekende OS

Windows

ArcaOS

Efi Shell

Efi Geheugen test

MDK app

Informatie

MDK app

Verborgen tabs

Uitzetten

Opnieuw opstarten

Boot naar setup

rEFInd configuratiebestand

rEFInd heeft een configuratie bestand (rEFInd. Conf) om:

- de muis in te schakelen
- het aanraakscherm te benutten
- de wachttimer in te stellen/uitzetten
- pictogram specificeren
- stanza's
- scherm resolutie
- en veel meer

rEFInd –voeg efi-shell toe aan het menu

- Het UEFI Shell kan eenvoudig toegevoegd worden aan het rEFInd startup menu.
- download het iso-bestand
- Vanuit het iso kopiëren het bestand ‘efi\boot\bootx64.efi’ naar het map \EFI \TOOLS met de naam shellx64.efi
- Computer afsluiten en opnieuw opstarten
- Nu is er in het EFI shell in het rEFInd menu

rEFInd - pictogrammen

- Alle pictogrammen die in rEFInd worden gebruik zijn terug te vinden in het map \efi\rEFInd\icons
- rEFInd gebruikt de naam van het submap om het icon te selecteren
  - UBUNTU
  - LINUX
  - LINUXMINT


os_ubuntul.png


os_linux.png


os_linuxmint.png

- Wanneer een OS niet wordt herkend wordt het ‘onbekende’ pictogram gebruikt.


os_unknown.png

- Door een pictogram toe te voegen met een naam die dezelfde is als die van een besturingssysteem, kan rEFInd dat pictogram weergeven

os_os2.png

rEFInd - pictogrammen

- rEFInd gebruikt pictogrammen met de volgende formaten
  - Apple's ICNS
  - Portable Network Graphics (PNG) format
  - bitmap image file (BMP) format
  - Joint Photographic Experts Group (JPEG) format

  PNG- en ICNS-bestanden werken het beste voor pictogrammen, omdat ze beide transparantie ondersteunen.

- rEFInd gebruik pictogrammen met de volgende afmetingen
  - OS pictogram 128x128 pixels
  - Tools 48x48 pixels (tweede rij)
  - Onderscheidingsteken 32x32 pixels

rEFInd handmatig aanpassen – stanza’s

- Voor meer controle over opties voor een menu-item wordt “Stanza’s gebruikt

- Menuentry "Ubuntu" {
- loader /EFI/ubuntu/grubx64.efi
- disabled
- }
- menuentry Arch {
- icon /EFI/rEFInd/icons/os_arch.png
- volume ARCHBOOT
- loader /vmlinuz-linux
- initrd /initramfs-linux.img
- options "root=/dev/sda3 ro"
- }

- menuentry "Windows via shell script" {
- icon \EFI\rEFInd\icons\os_win.png
- loader \EFI\tools\shell.efi
- options "fs0:\EFI\tools\launch_windows.nsh"
- }

Shell commands - 1

Command	Description
alias	Displays, creates, or deletes aliases (can alias commands, drives, and executables)
attrib [+|-][a|s|h|r] file di	Displays or changes the attributes of files or directories
bcfg	Manages the boot and driver options that are stored in NVRAM.
break	Executes a debugger break point
cd	Changes the directory
cls	Clears the screen and can change background color
comp file1 file2	Compares the contents of two files up to a maximum of 10 differences
connect	Binds an EFI driver to a device and starts the driver
cp [-r][-q] src file [dst]	Copies one or more files/directories to another location -r – Copies all recursively
date	Displays the current date or sets the date in the system
dblk	Displays the contents of blocks from a block device
devices	Displays the list of devices being managed by EFI drivers
devtree	Displays the tree of devices that follow the EFI Driver Model
dh	Displays the handles in the EFI environment
disconnect	Disconnects one or more drivers from a device
dmem	Displays the contents of memory
dmpstore	Displays all NVRAM variables
drivers	Displays the list of drivers that follow the EFI Driver Model
drvcfg	Invokes the Driver Configuration Protocol
drvdiag	Invokes the Driver Diagnostics Protocol
echo	Displays messages or turns command echoing on or off

Shell commands -2

Command	Description
edit	Edits an ASCII or UNICODE file in full screen
EfiCompress	Compresses a file
EfiDecompress	Decompresses a file
err	Displays or changes the error level
exit	Exits the EFI Shell
getmtc	Displays the current monotonic counter value
goto	Makes batch file execution jump to another location
guid	Displays all the GUIDs in the EFI environment
help [-b]	Displays commands list or verbose help of a command. –b – Displays one page at a time
hexedit	Edits with hex mode in full screen
load	Loads EFI drivers (e.g., Load ipmi.efi)
LoadBmp –w(seconds)	Displays a Bitmap file onto the screen
LoadPciRom	Loads a PCI Option ROM image from a file
ls [-b|-r|-a]	Display a list of files
map [-r|-v|-d]	Displays, resets, or deletes mappings with verbose option
memmap	Displays the memory map
mkdir dirname	Creates a directory at current location
mm	Displays or modifies MEM/IO/PCI
mode [row col]	Displays or changes console output
mount BlkDevice [sname]	Mounts a file system on a block device. The mounted names are lost at next map –r.
mv src dest	Moves one or more files/directories to destination
OpenInfo	Displays the protocols on a handle and the agents

Shell commands - 3

Command	Description
pause	Prints a message and suspends for keyboard input. Options are q to quit, any other key resume script.
pci	Displays PCI devices or PCI function configuration space
reconnect	Reconnects one or more drivers from a device
reset [-w|-s] [string]	Resets the system with warm reboot or complete shutdown. Can pass a string to the reset service.
rm [-q] file|dir	Deletes one or more files or directories -q – Does not prompt for a confirmation
set [-d|-v|-b] [sname [valu	Displays, deletes, changes, or creates environment variables
setsize	Sets the size of a file
stall	Stalls the processor for some microseconds
time	Displays the current time or sets the time of the system
touch [-r] filename	Sets the time and date of a file to the current time and date
type [-a|-u] file	Displays the contents of a file (ASCII or Unicode)
unload	Unloads a protocol image
ver	Displays the version information
vol [fs] [VolLabel]	Displays volume information of the file system

Referenties/downloads

- Partition styles

https://www.youtube.com/watch?v=hjyJUcxxw-I

- File Systems

https://www.youtube.com/watch?v=Q4QQIKUA_KI

- Disk formatting

https://www.youtube.com/watch?v=hjyJUcxxw-I

- Fat –Fat32 formats

https://www.youtube.com/watch?v=hv0grnkdiqs

Referenties/downloads

Bootloaders - vergelijking

https://en.wikipedia.org/wiki/Comparison_of_bootloaders

Airboot – binary

https://github.com/rousseaux/netlabs.air-boot/releases/download/v1.1.4RELEASE/AirBoot-v1.1.4-bin.zip

EFI Shell - binary

https://www.intel.com/content/dam/www/public/us/en/zip/efi-1-10-update.zip

Shell Commands

https://docstore.mik.ua/manuals/hp-ux/en/5991-1247B/ch04s13.html

Memory Test - efi

https://www.memtest.org/download/v7.00/mt86plus_7.00.binaries.zip

Bedankt