fidélitas
Virtual

Computación Forense

Sistemas de Archivos

Clase 2a

Profesor: Ing. Alex Araya Rojas, MT

CISSP, CISM

Tipos de almacenamiento más conocidos

Magnéticos	Ópticos	Flash
• Alta capacidad de almacenamiento. • Disco cubierto por capa magnética. • Utilizan una cabeza mecánica para leer y escribir datos. • Disco Duro, disquete, cintas, etc.	• Discos recubiertos de material plástico. • Menor capacidad que un disco duro. • Por lo general son de lectura y una sola escritura. • CD-ROM, DVD, etc.	• Alta capacidad lectura y escritura. • Precio en bajada lo que aumenta su popularidad. • NVMe llega con fuerza a mejorar aún más a los SSD. • USB, Discos Estado Sólido.

Sistemas de archivos más comúnes

FAT / FAT32

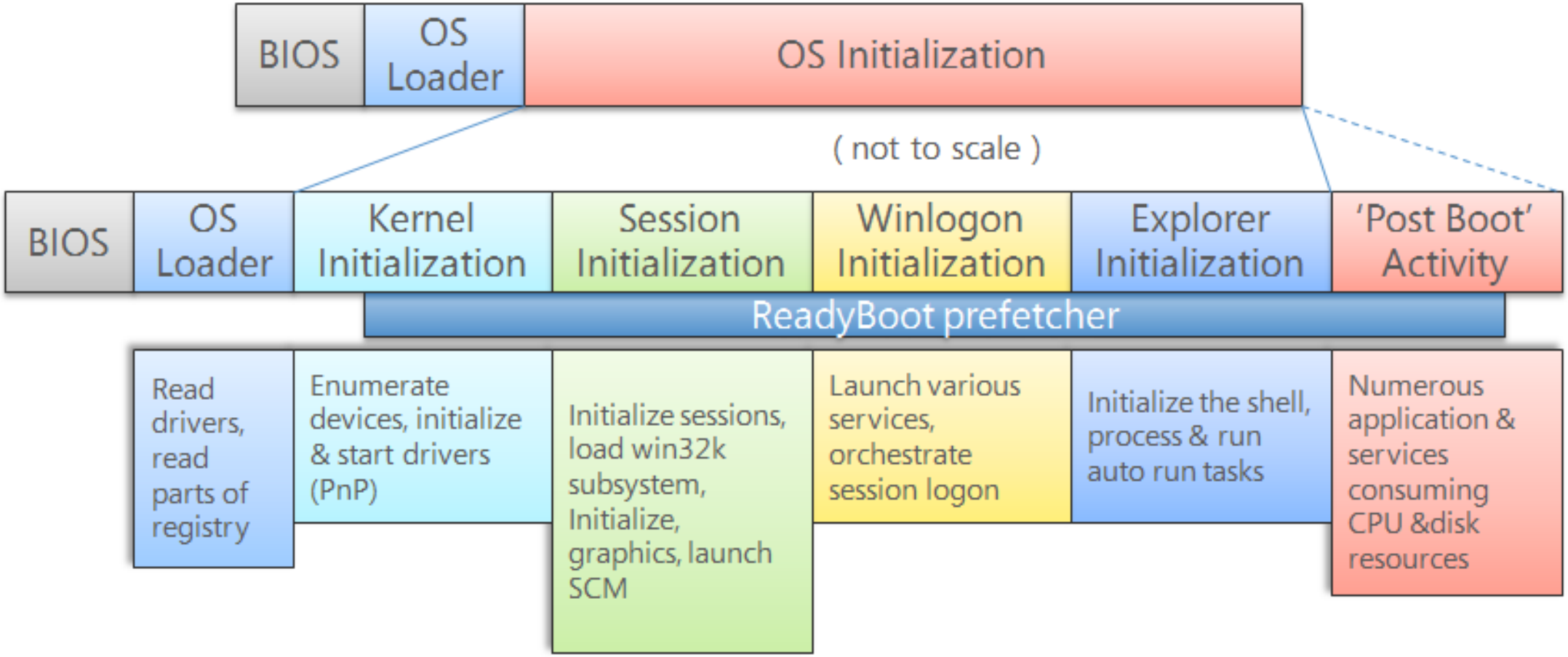
NTFS

EXT y sus versiones

EFS / HFS+

exFAT

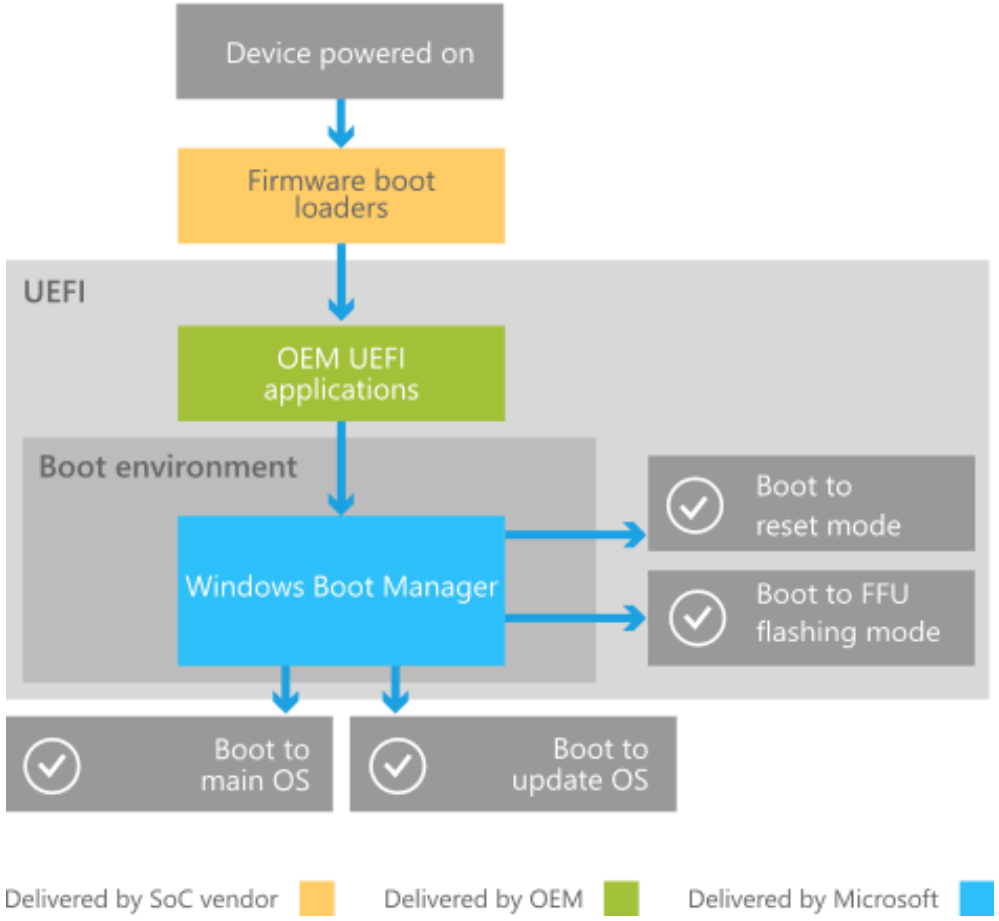
Proceso de arranque de Windows



UEFI vs BIOS

- Ambas son firmware, su función es la de controlar el hardware del equipo al encenderse.
- El BIOS (Basic Input Output System) fue creado en 1975 y su función principal es invocar al Sistema Operativo.
- La UEFI (Interfaz Unificada De Firmware Extensible), viene reemplazando la BIOS desde 2015.
- Velocidad, soporte a discos de mayor tamaño, actualizaciones simples, secure boot, ejecución de código a 32 y 64 bits sobre los 16 del BIOS, entre otras diferencias.

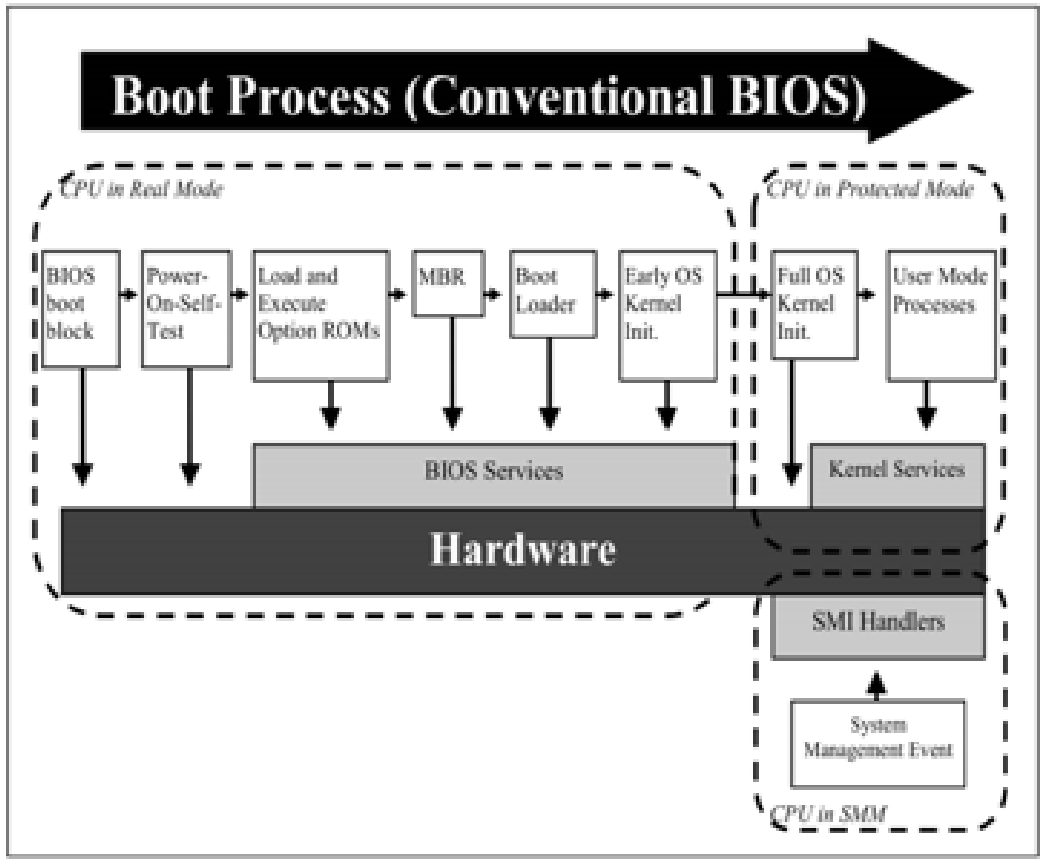
Proceso de arranque Windows UEFI

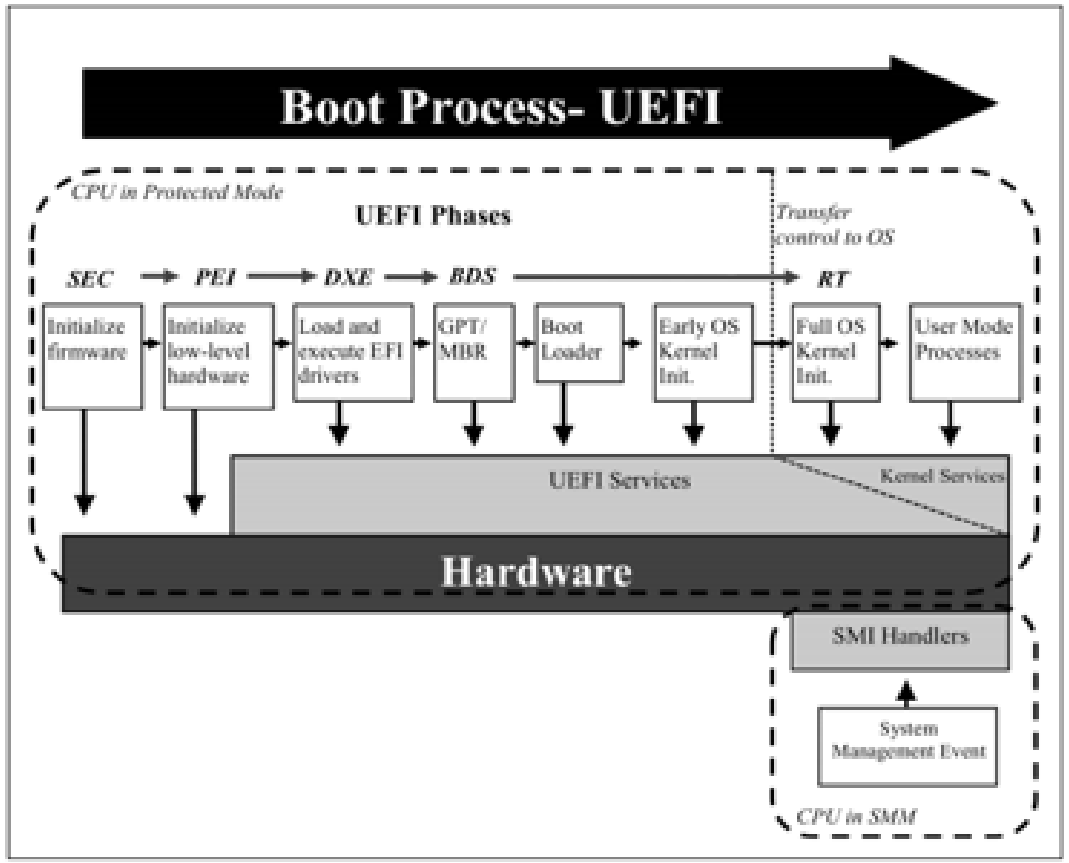


- Características como el Secure Boot no permite la ejecución de Sistemas Operativos no certificados, pero puede desactivarse.

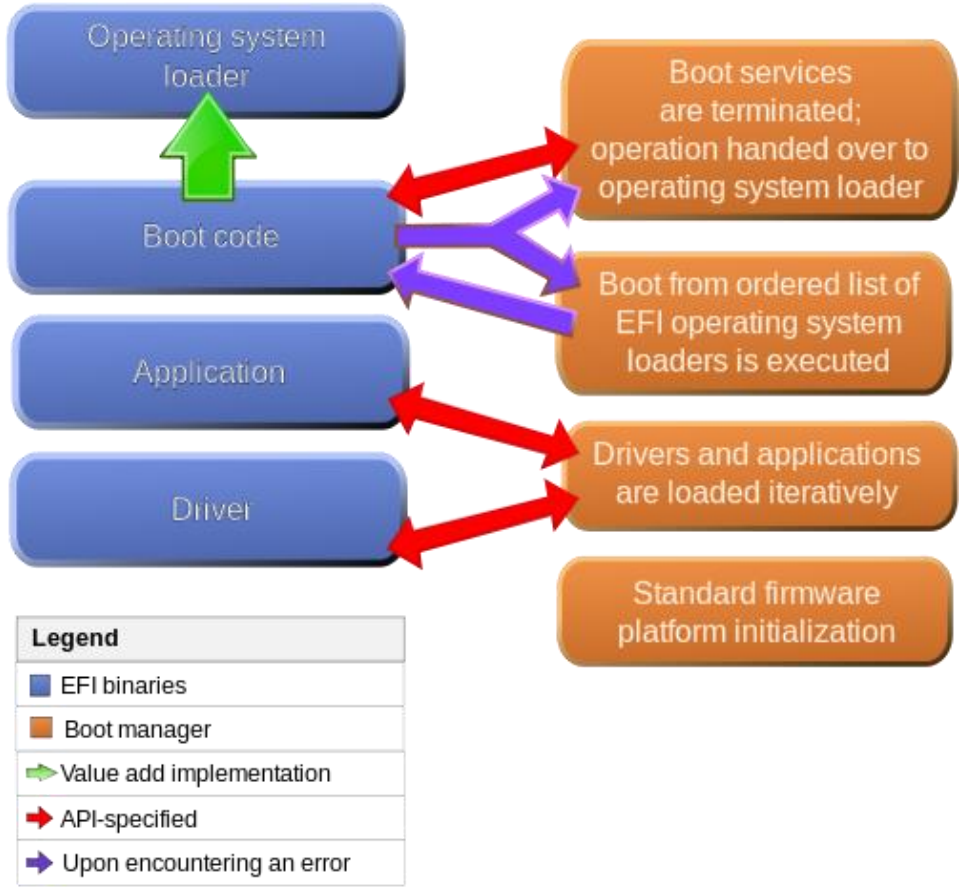
- Se empezó a utilizar desde Windows 8.

Comparación BIOS vs UEFI

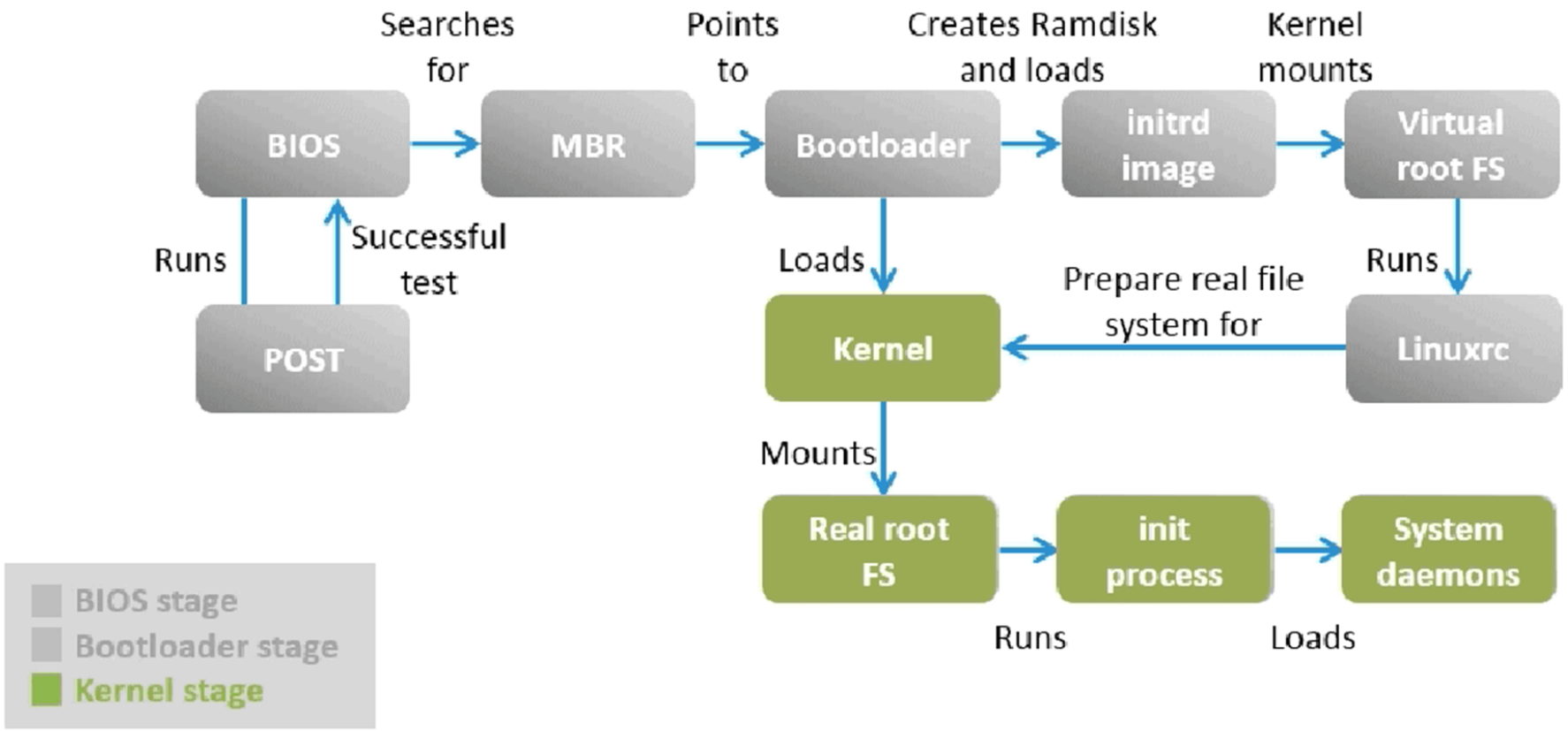




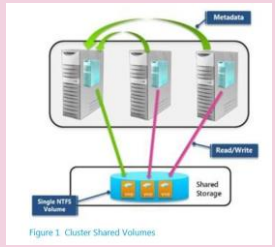
Proceso arranque en Mac OS



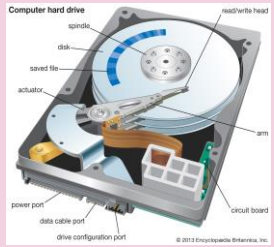
Proceso arranque en Linux



Tipos de Sistemas de archivos



File System Disco Compartido



File System Disco

File System Cinta

File System Red

File System Bases de Datos

Laboratorios

- En el laboratorio aprenderá a identificar los diferentes sistemas de archivos con herramientas forenses.

- Los espero en la próxima clase!!

fidélitas
Virtual

Gracias