Explaining iOS Devices Weaknesses

Dale Meredith
MCT | CEI | CEH | MCSA | MCSE
Cyber Security Expert

dalemeredith.com | Twitter: @dalemeredith | Linkedin: dalemeredith

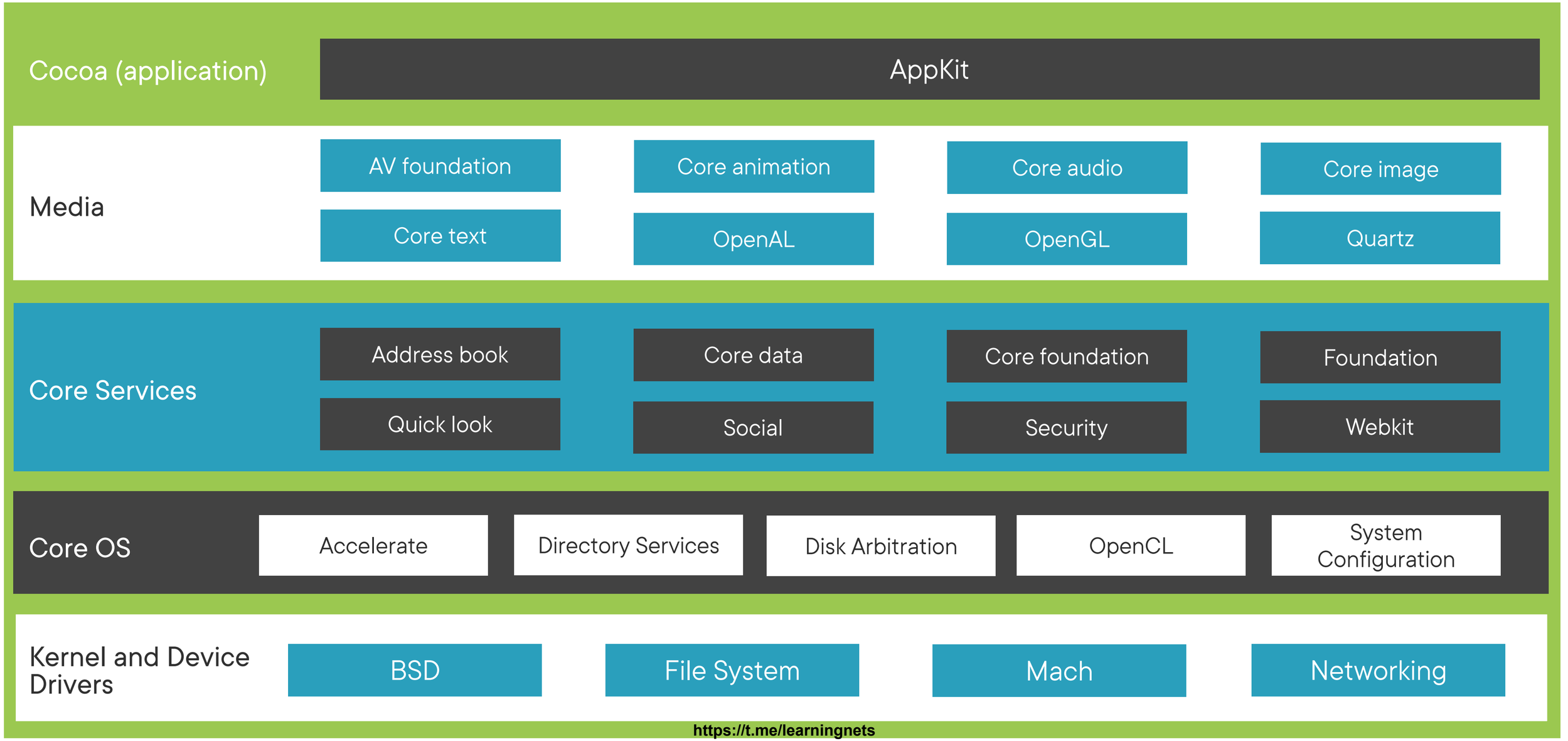
https://t.me/learningnets

“With enough time, nothing is unhackable.”

Unknown

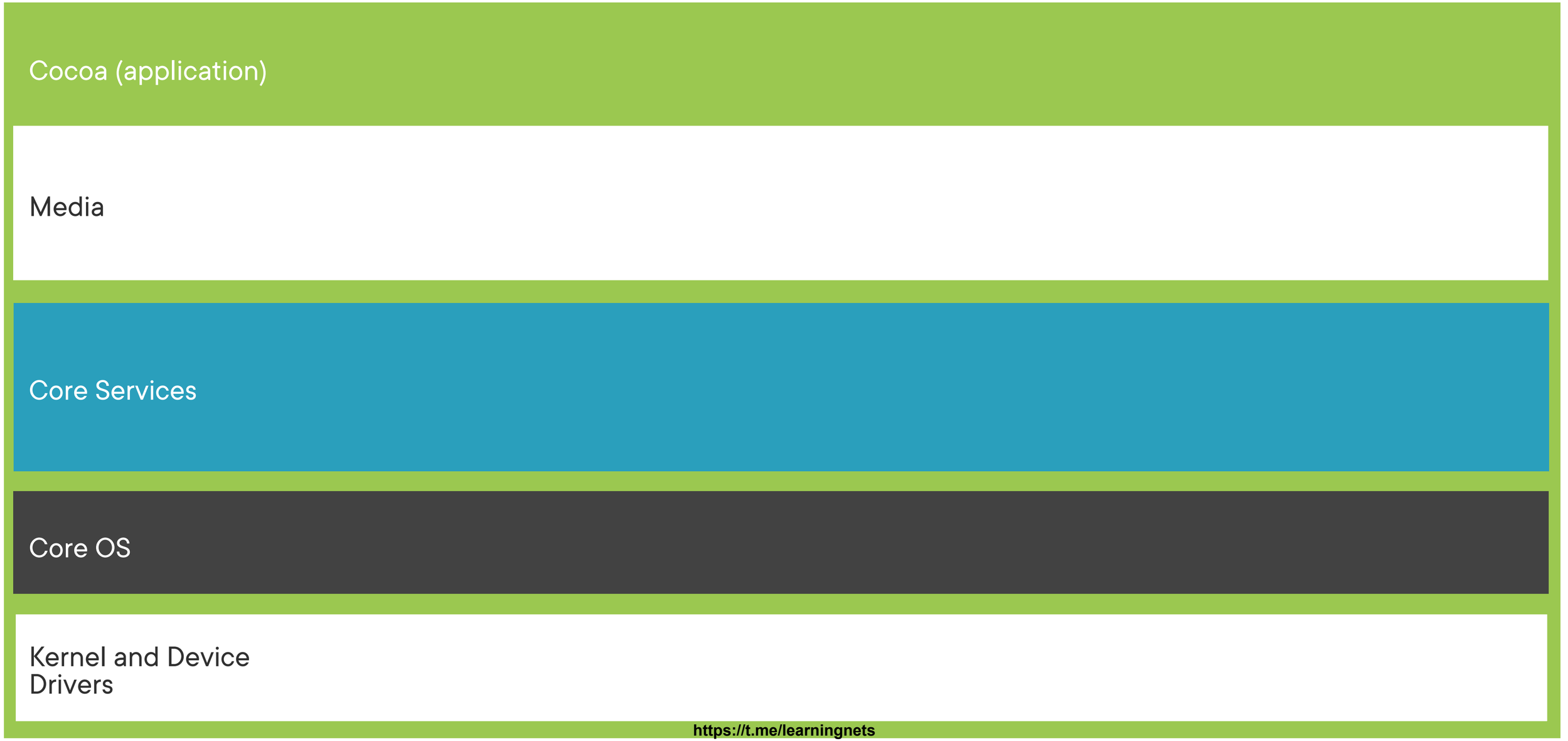
https://t.me/learningnets

Apple's Architecture



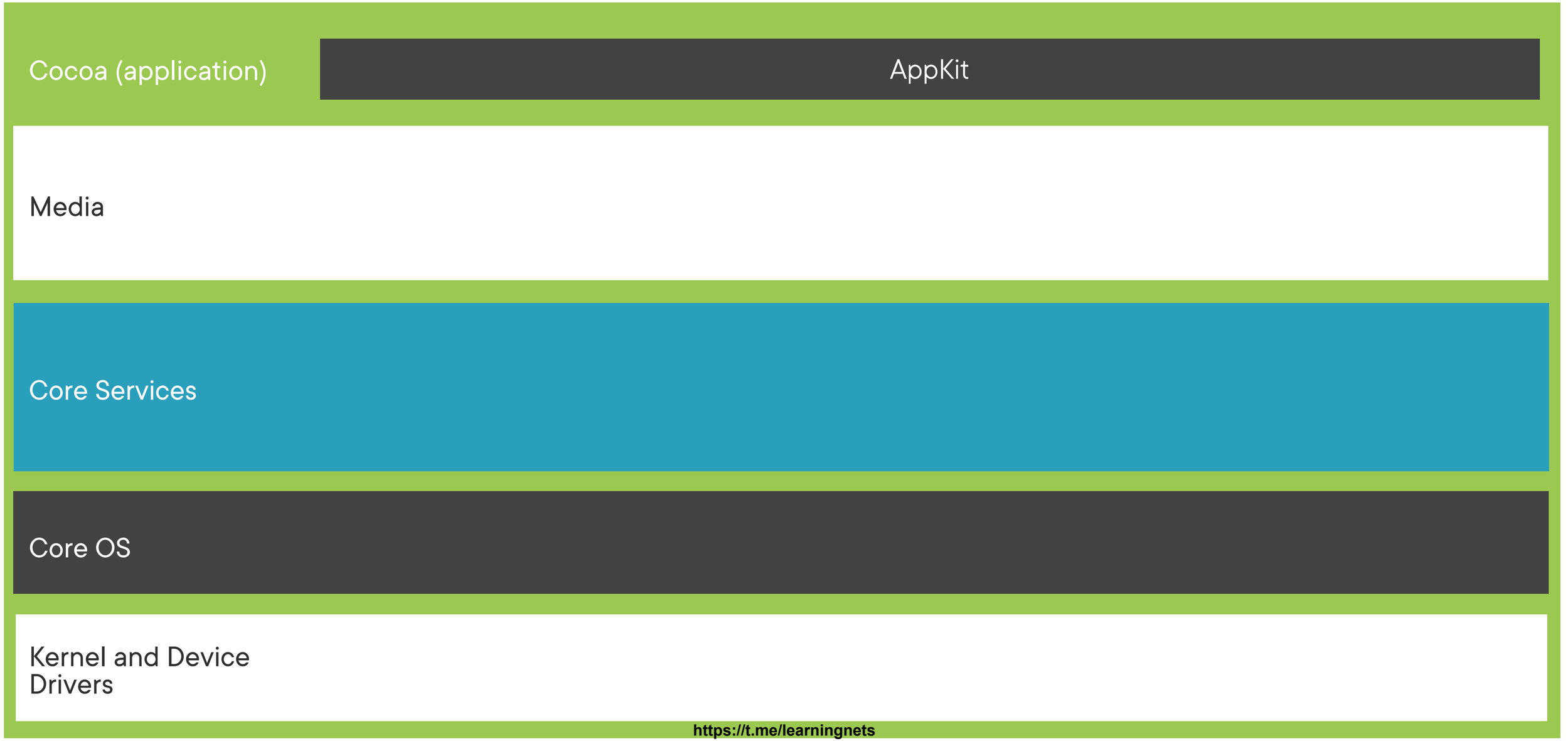
https://t.me/learningnets

Apple's Architecture



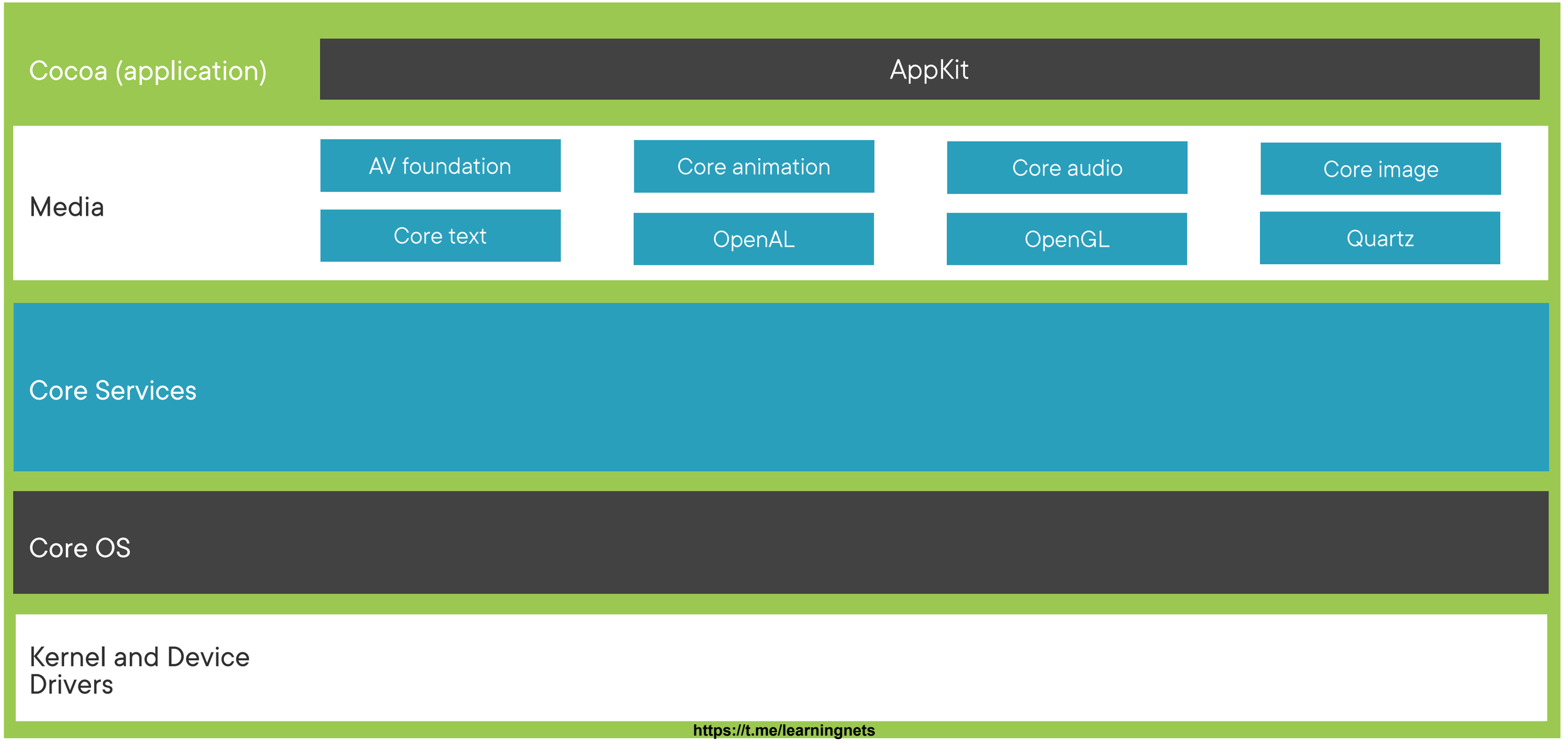
https://t.me/learningnets

Apple's Architecture



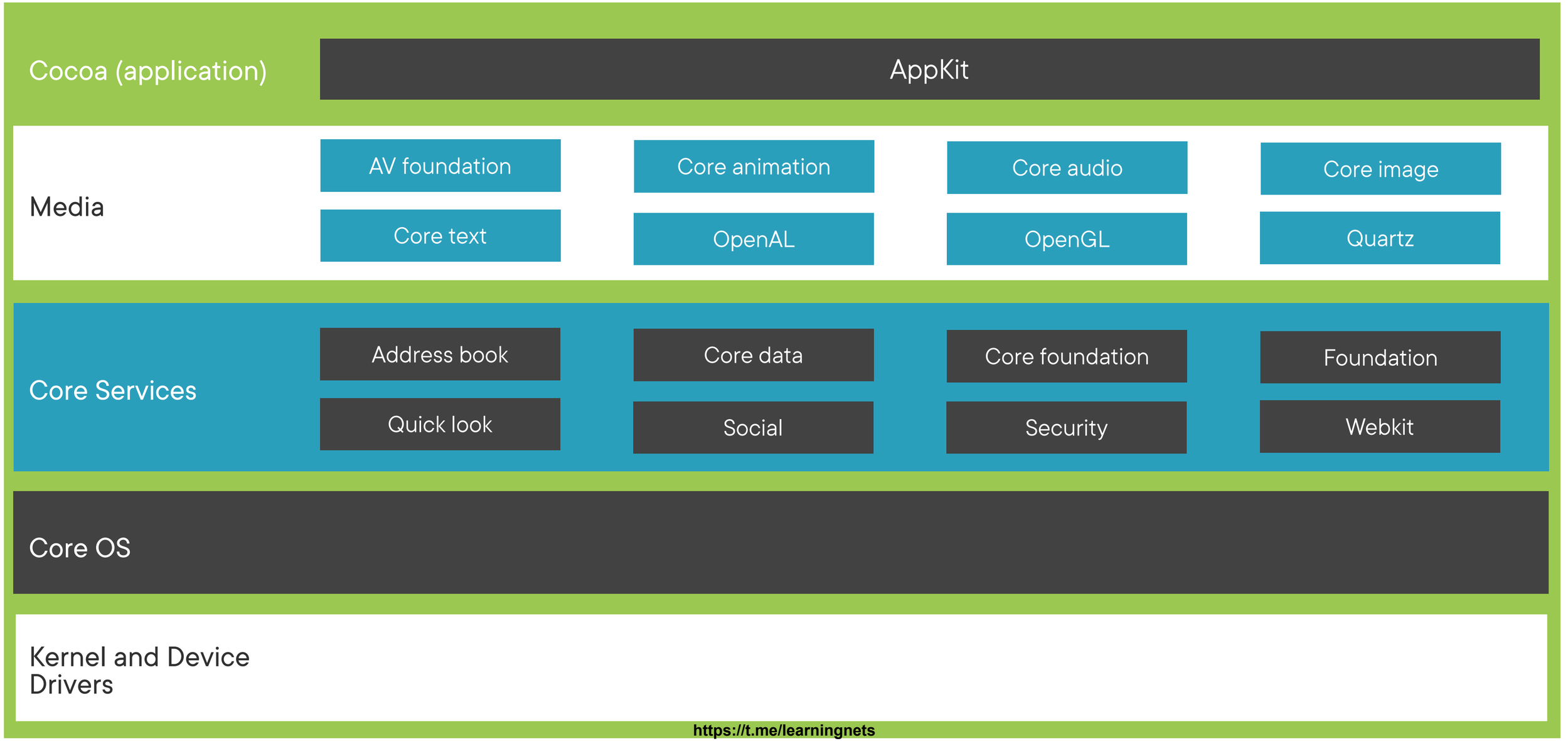
https://t.me/learningnets

Apple's Architecture



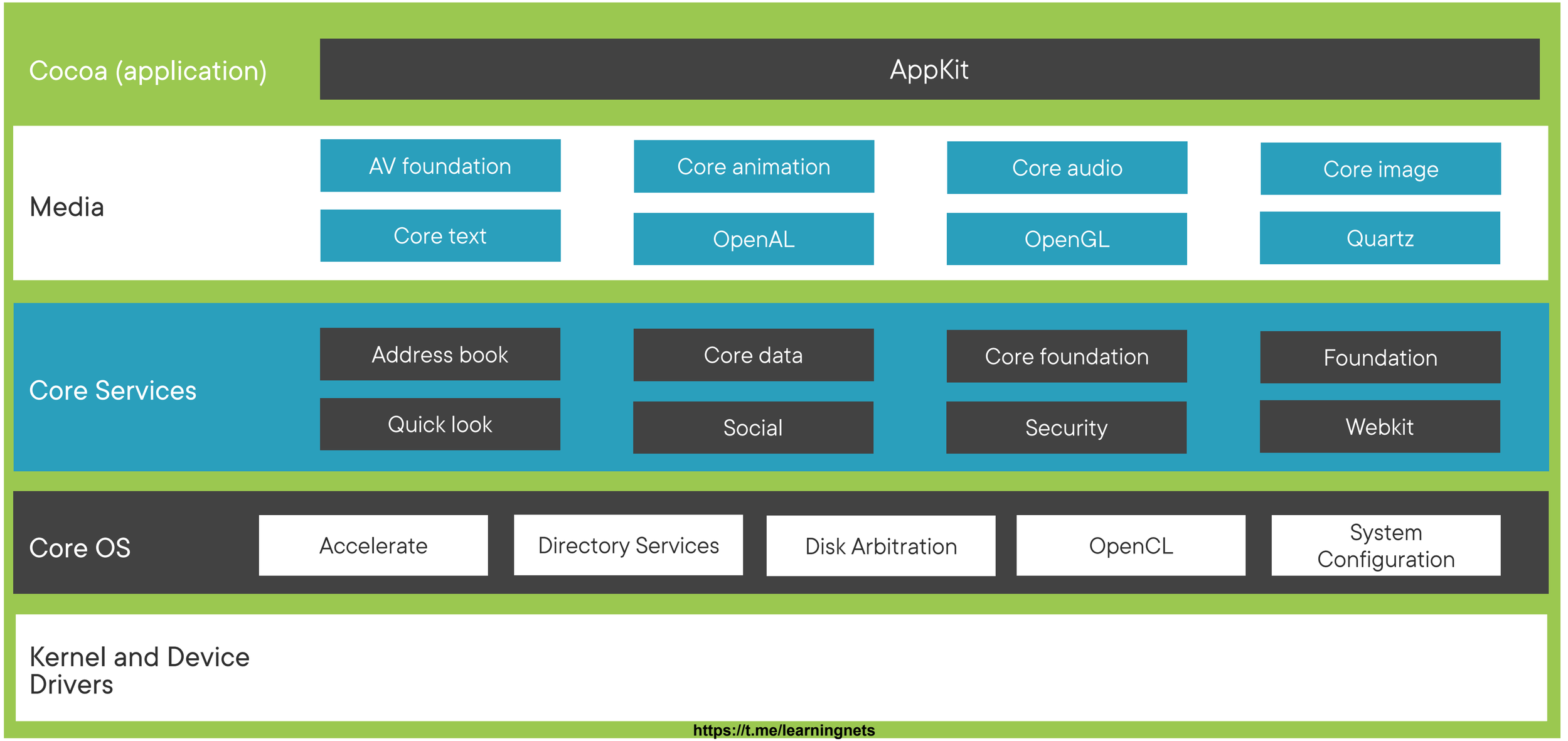
https://t.me/learningnets

Apple's Architecture



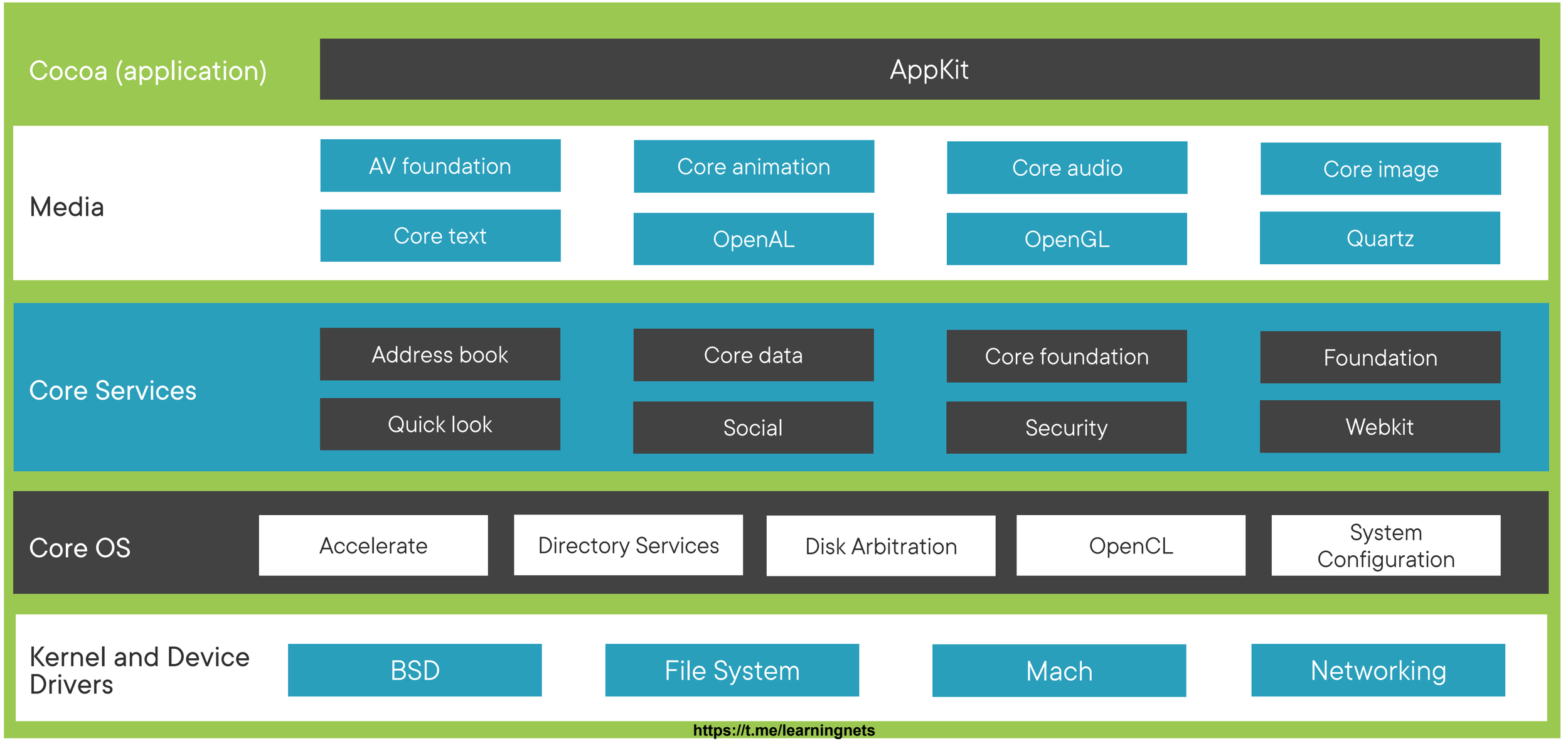
https://t.me/learningnets

Apple's Architecture



https://t.me/learningnets

Apple's Architecture

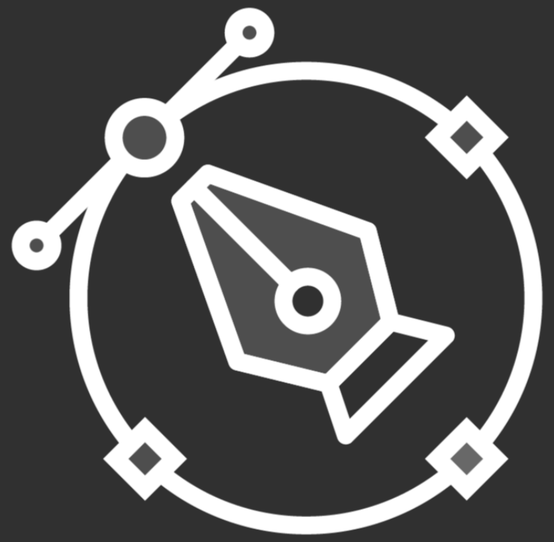


https://t.me/learningnets

Jailbreaking

https://t.me/learningnets

Jailbreaking vs. Rooting



Jailbreaking
Bends the rules

Rooting
Bends and breaks the rules

https://t.me/learningnets

Jailbreaking

Removes restrictions

Utilizes a custom kernel

Allows for customization

Goes against Apple’s terms and conditions

Enhances functionality

https://t.me/learningnets

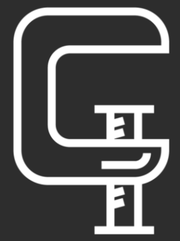
Jailbreaking eliminates sandbox restrictions, allowing malicious applications to access restricted resources and data.

https://t.me/learningnets

Jailbreaking Tools

Cydia

Yuxigon



Hexxa Plus

Sileo

ApricotiOS

Trimgo

https://t.me/learningnets

https://t.me/learningnets

Types of Jailbreaking

https://t.me/learningnets

Jailbreaking Techniques

Untethered jailbreak

Tethered jailbreak

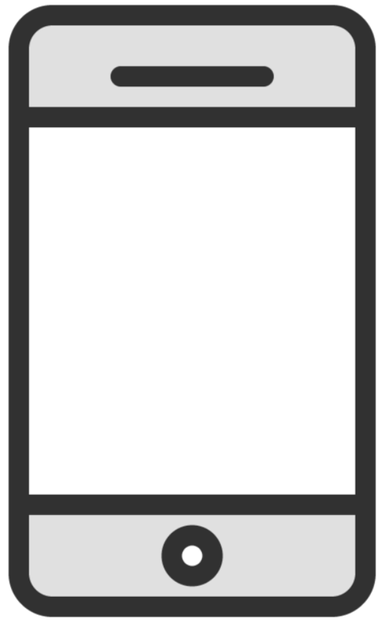
Semi-tethered jailbreak

Semi-untethered jailbreak

https://t.me/learningnets

Types of Jailbreaking

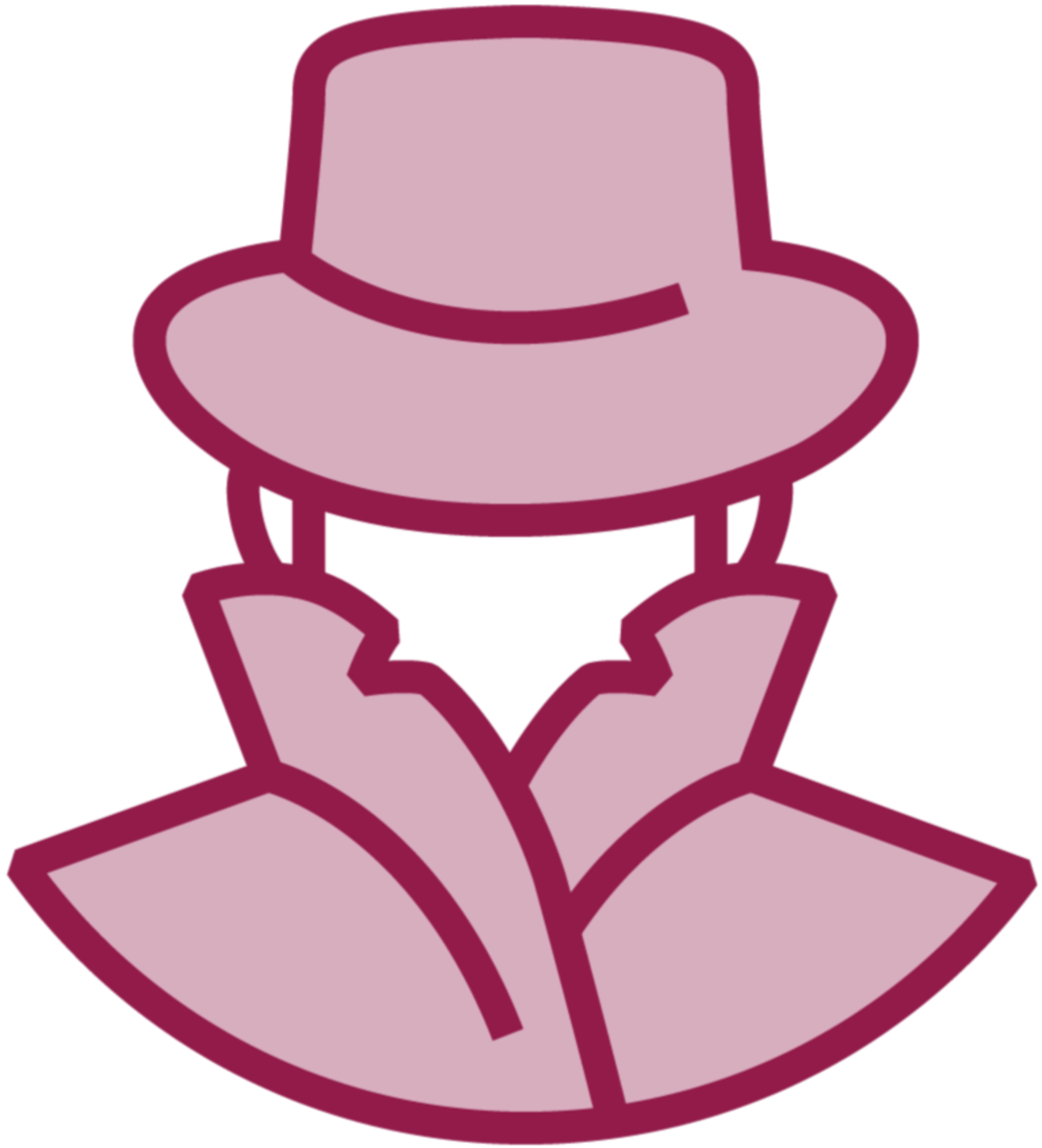
- **The userland exploit**
- **The iBoot exploit**
- **The Boot ROM exploit**



https://t.me/learningnets

Securing Apple's Platform

https://t.me/learningnets



https://t.me/learningnets

Passcode lock the device

Avoid sideloading apps

Disable Javascript and add-ons from your web browser

Avoid storing sensitive data on the device

Change the default root password

Configure ‘find my phone’ to wipe the device if lost or stolen

https://t.me/learningnets

Update, update, update

Disable iCloud services

Enable ‘ask to join networks’

Enable erase data after 10 attempts

Turn off Siri

Turn off voice dial

And more...

https://t.me/learningnets

Learning Check

https://t.me/learningnets

Learning Check

- Untethered jailbreak
- Media layer
- Userland
- Boot ROM exploits
- Tethered jailbreak

https://t.me/learningnets

Up Next:
Outlining Mobile Device Management (MDM)

https://t.me/learningnets