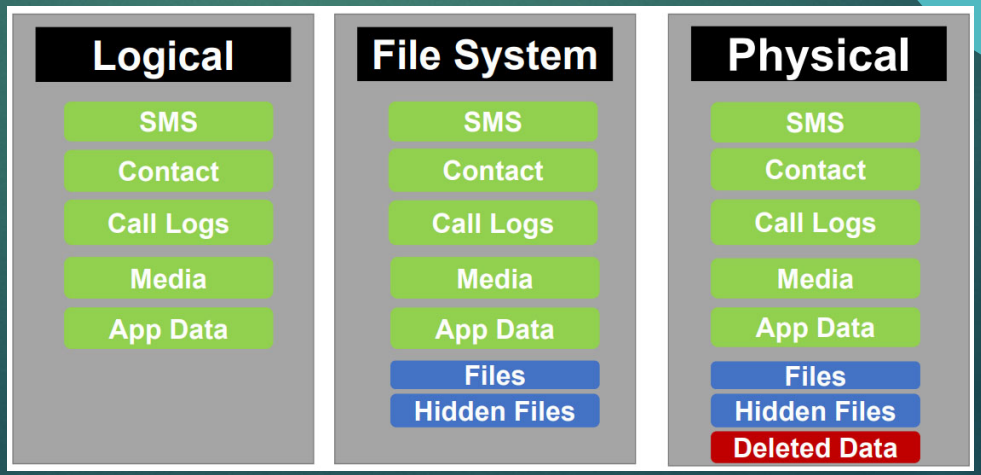
Where are we now… Week **15**

- We have 3 more lectures to be covered in this term:-
  - **Data Type (iOS) – week15**
  - Rooting & Jailbreaking – week16
  - Revision – week17
- We will do 1 more practical on Magnet Axiom.
- No more lab on week16. Please use the time to work on your assignment 2.
- 1 more assignment - Assignment 2. Due 16th Feb 2024.
- 1 revision on week17 and 1 final exam.

Week15 - **Data Type (iOS)**

- Seizure and Isolation – Some important things to do…
  - Take the picture of the mobile phone before starting any progress
  - Request for Passcode, SIM pin, iTunes backup password if possible
  - Search/request for the SIM
  - Change the setting, the Auto-lock feature to "never"
  - Perform isolation (Faraday bag)
  - Perform acquisition and follow by hashing

- Type of Acquisition

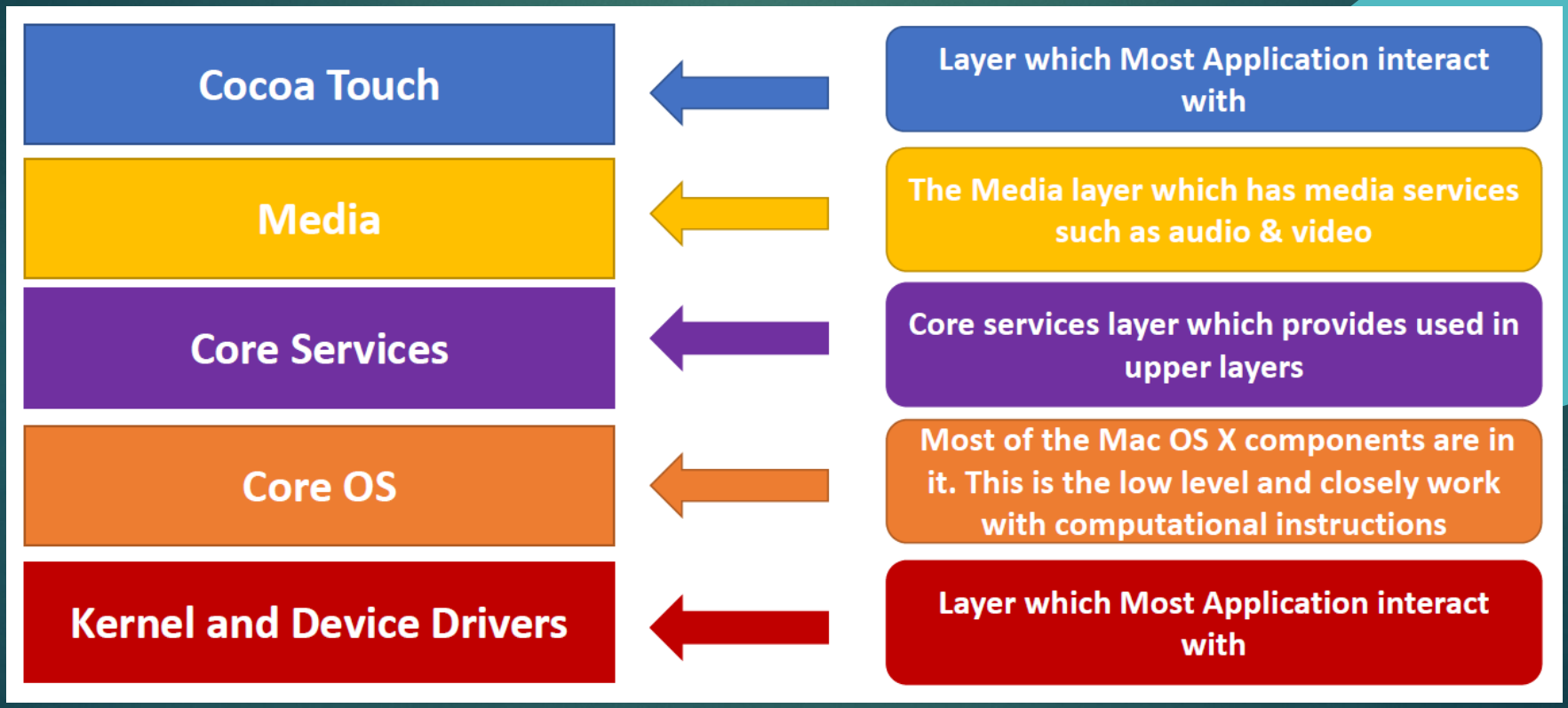


Week15 - **Data Type (iOS) Cont…**

- Jailbreaking
  - Jailbreaking allows the device owner to gain **full access** to the root of the operating system and access all the features
  - user could gain access to all partitions including file system with read-write permissions
  - Apple considers jailbreaking iOS to be a violation of its terms and conditions of use and advises customers that the practice exposes a phone to several risks, including:
    - Security vulnerabilities
    - Stability issues
    - Potential crashes and freezes
    - Shortened battery life

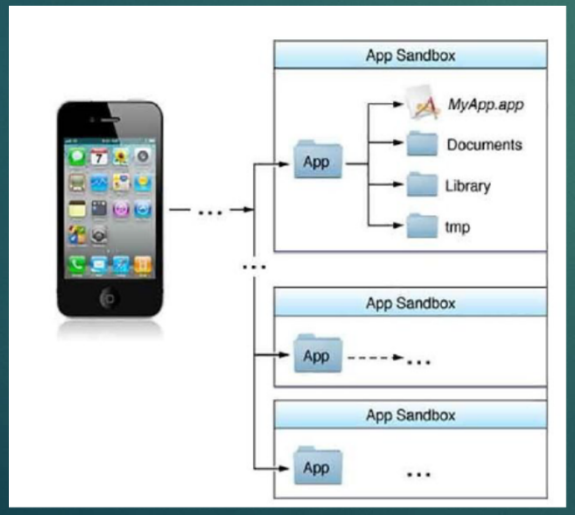
Week15 - **Data Type (iOS) Cont...**

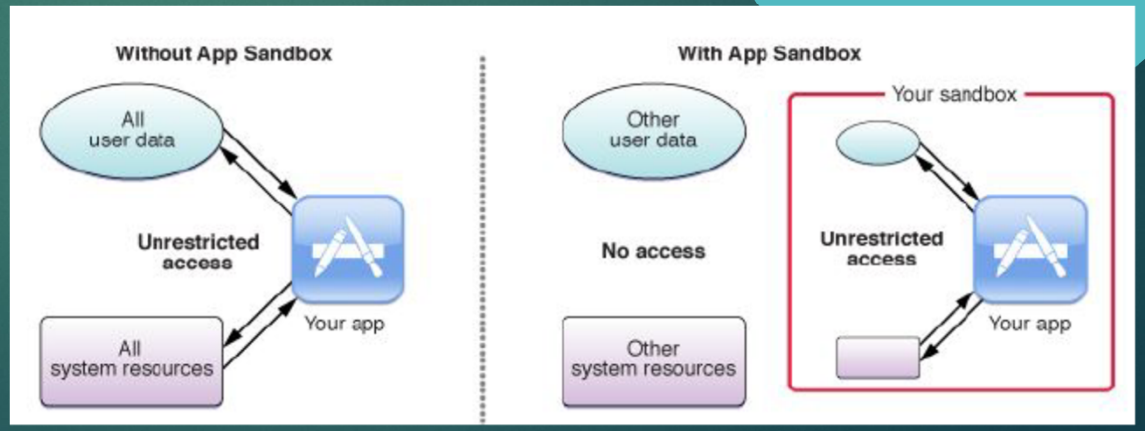
iOS Architecture



Week15 - **Data Type (iOS) Cont...**

- App Interaction with iOS
  - Sandboxing, a technology whose primary job is security and control
  - By enforcing a very strict set of rules on which apps can be installed on a device and exactly what they can do
  - Minimum set of privileges it needs to get its job done





Week15 - **Data Type (iOS) Cont...**

- iOS Standard Directories: Where Files Reside

Directory	Description
AppName.app	• This directory contains the app and all of its resources
Documents/	• This directory to store user-generated content which are Userdata
Documents/Inbox	• This directory to access files that your app was asked to open by outside entities. • Specifically, the Mail program places email attachments associated with your app in this directory
Library/	• The Library Directory Stores App-Specific Files such as data files, caches, resources, preferences
tmp/	• This directory to write temporary files that do not need to persist between launches of your app

Week15 - **Data Type (iOS) Cont…**

- **iOS Partitions**
  - An iOS device will have two (2) partitions:-
    - System partition
    - Data Partition

- **System Partition**
  - Firmware/OS partitions
  - Read only partition
  - Containing only system files, upgrade files and basic applications

- **Data Partition**
  - Contains user data
  - This partition will be the focus of most Investigation
  - It is Read/Write partition
  - This partition is where all iTunes applications will reside along with the user's profile data

Week15 - **Data Type (iOS) Cont...**

Data Structure and Artefacts

- Important artifacts which are generated by features of the system or interaction of the user with the device
- It is very necessary to understand how data are stored in device
- The iOS directory structure is **common across all iOS devices**
- The **folder structure resembles a UNIX layout** and there are several directories the examiner will immediately be interested in
- Some files will be stored in **text** format and easily readable
- Other files will be stored in **SQLite databases**, **XML files** or **binary** format

Note : Check out lecture notes iOS Forensic (Part 2) for more details.

Quiz Time (Data Type – iOS)…

1

1. Which of the following is not a step under the rule of Seizure and Isolation for iOS device?

- ○ Contact the owner of the iOS device.
- ○ Note location from where mobile has been collected.
- ○ Take picture of the location
- ○ Take picture of the mobile phone before any progress

2

1. What is purpose of a Sandbox in iOS device?

- ○ Provide security and control for iOS device
- ○ Provide user applications from App store
- ○ Provide user interface for user application
- ○ Provide path for iOS upgrade

1. Which of the following is not a motivation for Rooting/Jailbreaking?

- ○ Unlocking OS so that you can install unapproved app
- ○ Increase the value of your mobile phone
- ○ Remove unwanted bloatware
- ○ Increase available memory

Today's lab – Week 15

- **Need to do**:-
  - DFI Mobile Practical 3v6

- Image/Case files for the above exercises can be found in "Forensics 6" VM, "**Desktop/Magnet Case File/Practical_3_iOS_CaseFile**" folder on your VM's desktop.

- Submit you lab answers for DFI Mobile Practical 3v6 to "Brightspace ->Lab Exercise Submissions-> Week 15 Lab Submission".

- Continue to work on assignment 2 if got time…