Cellebrite

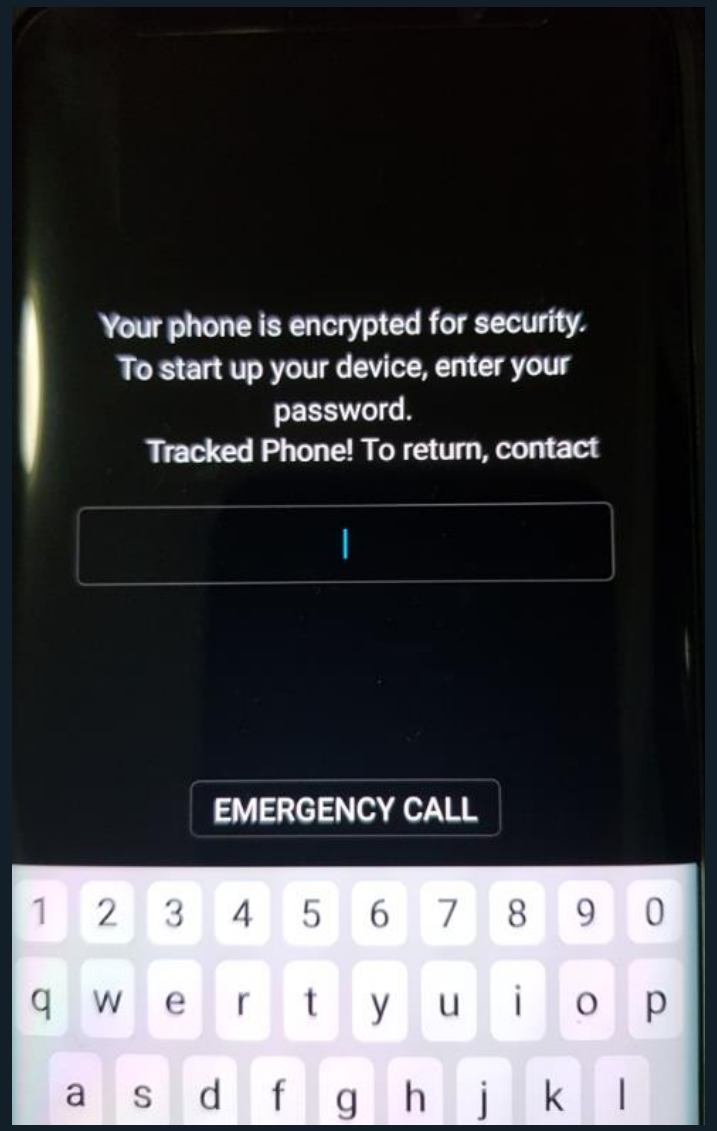
Android Encryption

Encryption – Unavoidable

What if I told you there is no spoon?

Basic terminology

- FDE / FBE
- Full File-System\Physical extraction
- Brute Force (unlock)
- After-First-Unlock (AFU)
- Before-First-Unlock (BFU)



Full Disk Encryption

Secure Boot ≠ Secure Startup

- Data is encrypted as a whole
- Introduced in Android 4.4 - enforced starting ~6.0
- Password to decrypt the data is "default_password"
- This is changed when the user enables Secure Startup
- A fully booted FDE Android's data is decrypted – even if it's protected by a screen lock

File Based Encryption – How does it differ?

- Each file has its own encryption key, making it very difficult for recovery of deleted files.
- Like FDE, FBE renders old physical extraction methods not viable (J-Tag, Chip-off, ISP)
- CAN’T have Secure Start up – but it doesn’t need it
- User passcode is directly tied to decrypting the User data (Credentials Encrypted Storage) that’s why you can’t just do a remove screen lock.
- Physical extractions are technically possible, but FFS used.

File-Based Encryption (aka “FBE”)

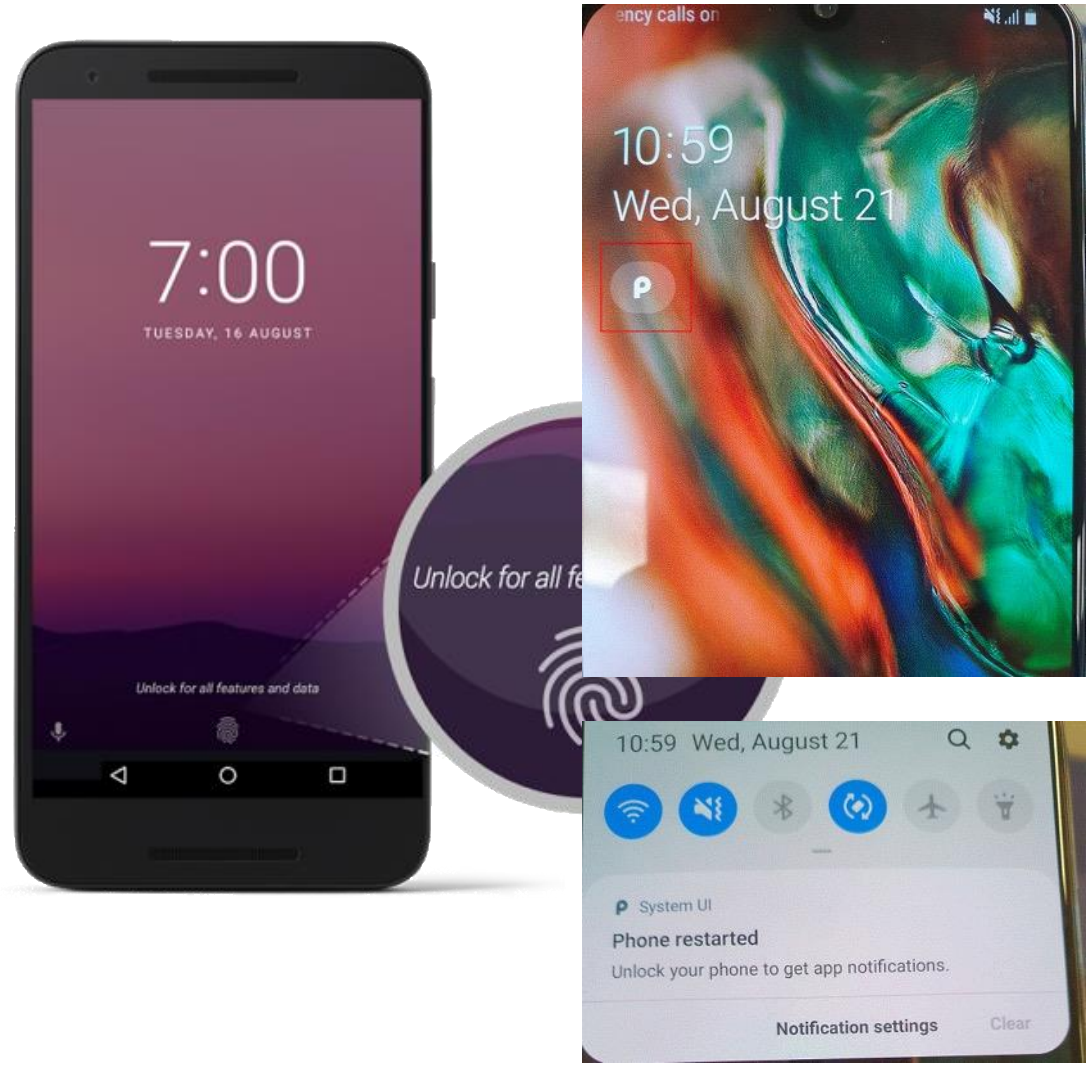
- Similar to the iOS model
- Device-Encrypted (DE) and Credential-Encrypted (CE)
  - Just like Secure Startup, the CE (most of the user data) is protected by the passcode (and hardware key)
- Starting with Android 7, OEMs can choose to release new devices as FDE or FBE.
- Notable FBE:
  - Google Pixel (October 2016)
  - New Huawei and Motorola phones since ~2018
  - Samsung – only in 2019! (S10 series and very recent models)

- Now any device with Android 10, you can assume its FBE.

How to identify File-Based Encryption?

Immediately after boot, you can spot text along the lines of *“Unlock for all features and data”*

- This confirms FBE - only DE data is decrypted, CE is still encrypted!
- Wallpaper is visible*, but calls will come in with no contact names!
  - Don't believe us, try it...
- Recent exceptions to this rule

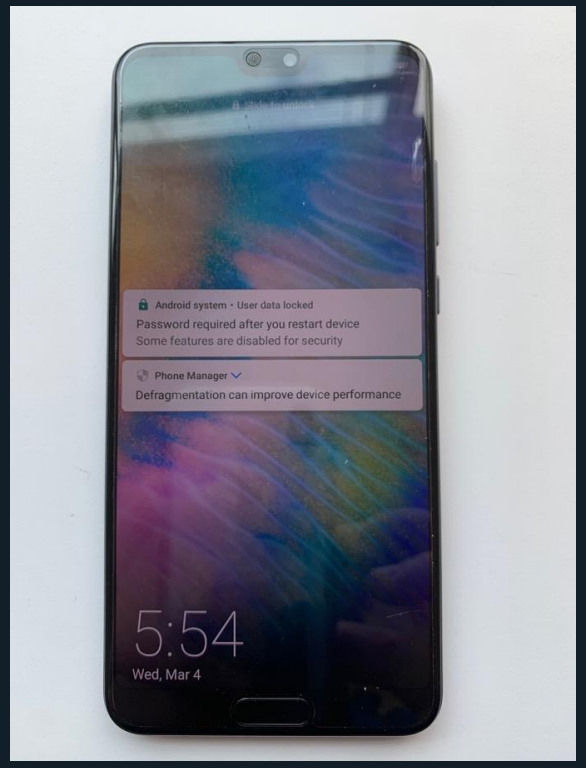


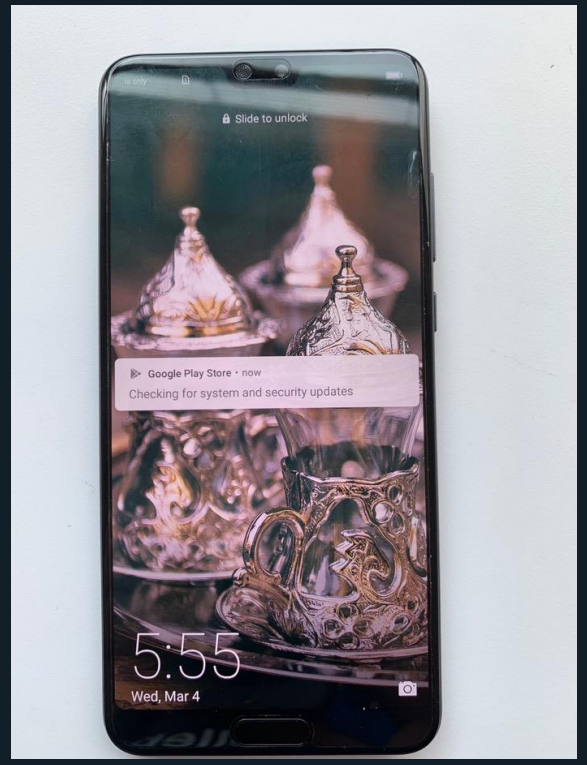
Cellebrite

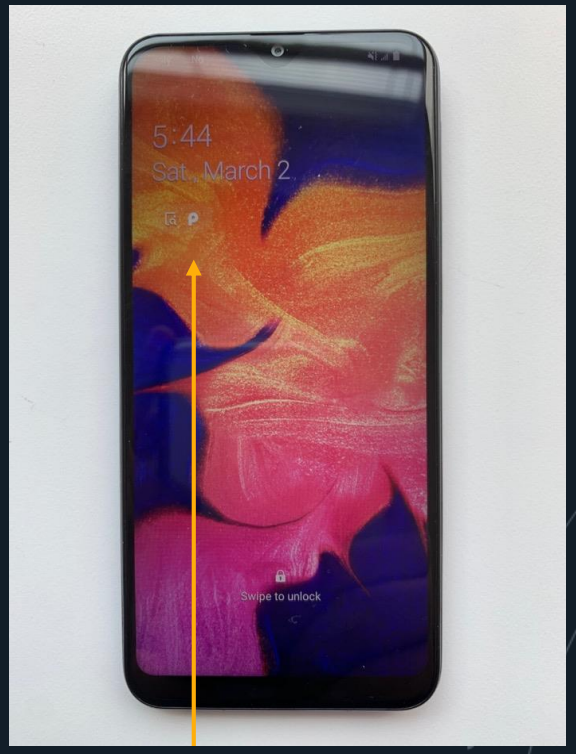
How do you identify what kind of phone you have?

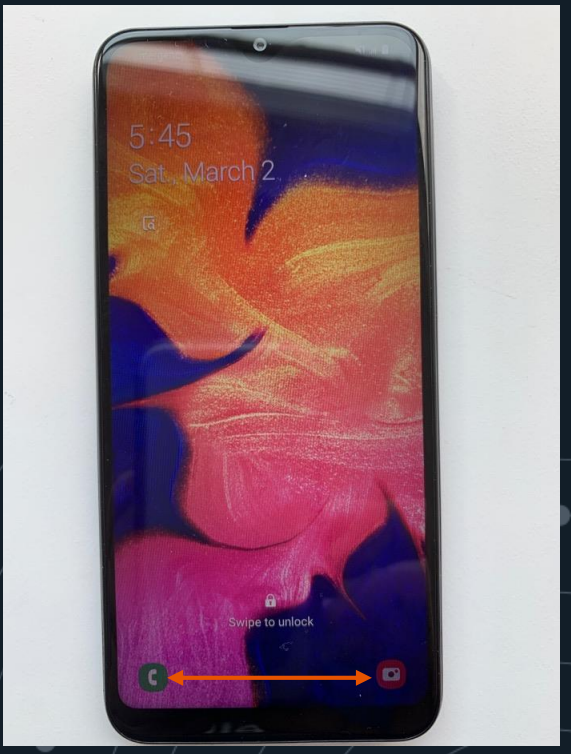
- Is it in AFU?
- If its cold, what do you see on the screen. Do you have any of the clues on the home screen?
- ADB SHELL and execute “getprop ro.crypto.type”
  - File = FBE
  - Block = FDE

FBE Devices Home Screen



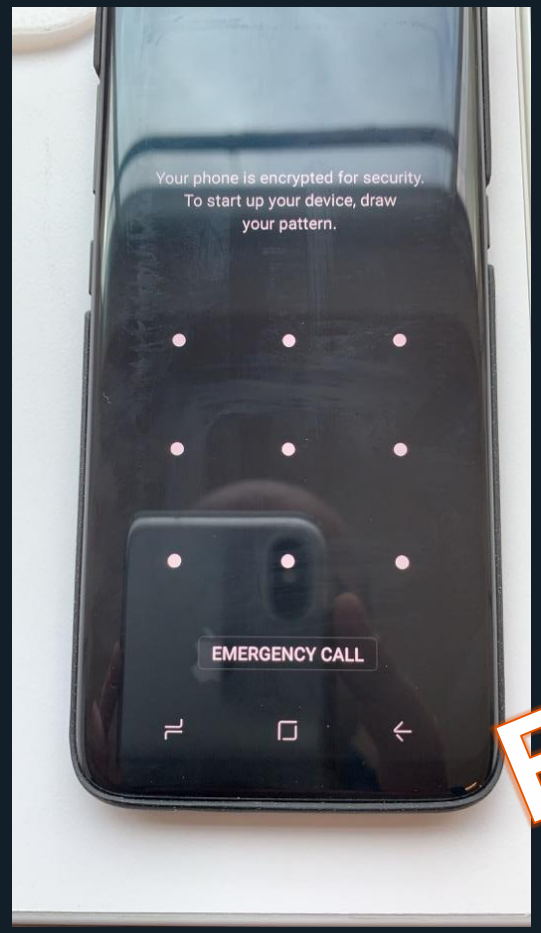


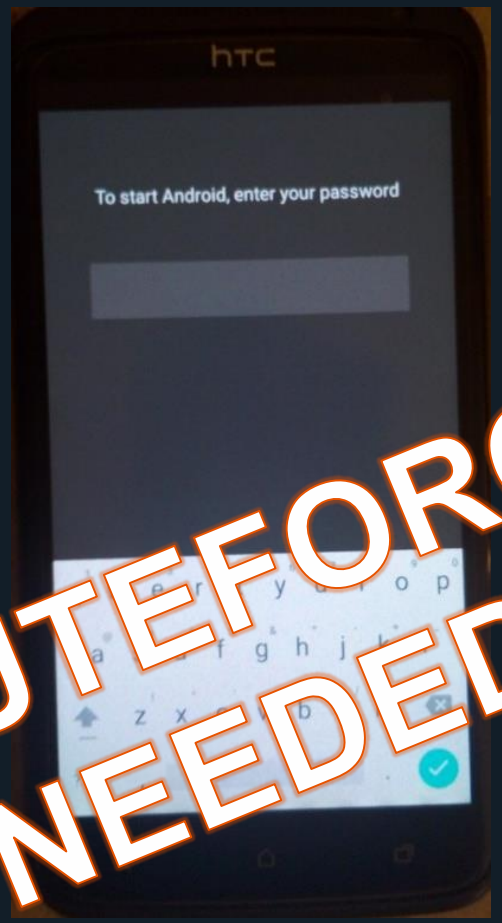




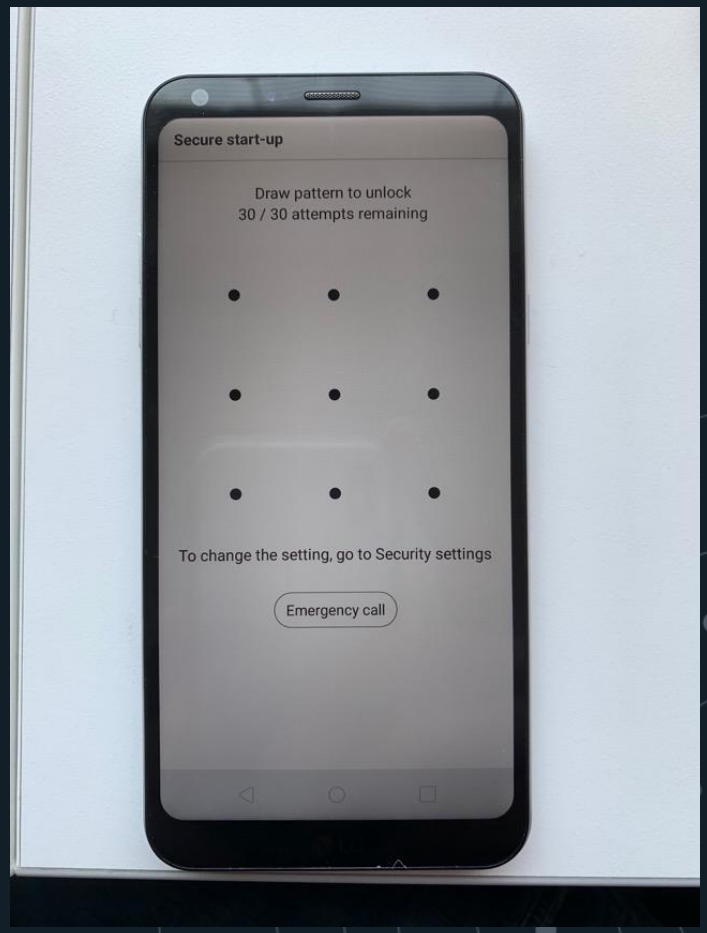
- Look for the visual cues on the home screen
- “P” for Samsung
- ”Some features are disabled for security”

Secure Start-Up





BRUTEFORCE NEEDED



When is Brute Force needed?

Cellebrite

Summary

Full Disk Encryption

- One key for entire memory
- Physical Extraction
- Can have Secure Startup
- When no Secure Start, bypass options available

File Based

- Full File System Extraction
- No Secure Start Up
- Each file has its own encryption key

AFU

The Encryption keys are loaded in RAM

Unlike in iOS there is no limitation to data being extracted.

Saves you the need to BruteForce passcodes

iOS extractions have some limitation; (native mail, health, and some other artifacts)

This will become more and more important going forward.. Keep devices alive.

BFU

The state of a device that has been restarted.

All you are going to get is data that is available to the device in encrypted state

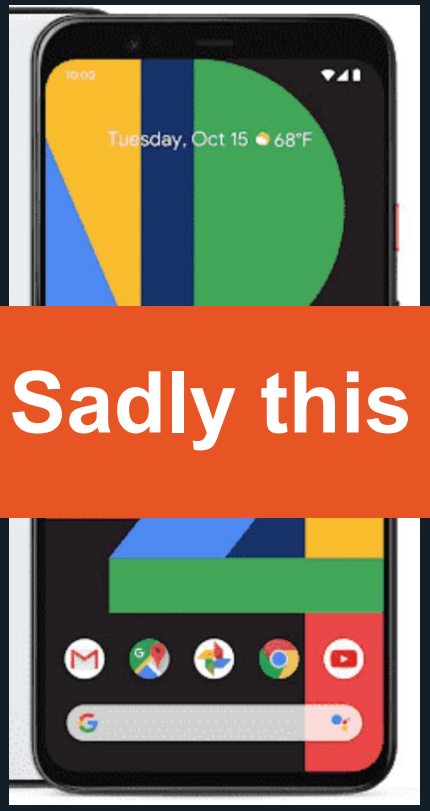
- maybe accounts.db
- some messages
- generally limited data

iOS seems to give more than Android in BFU

Cellebrite

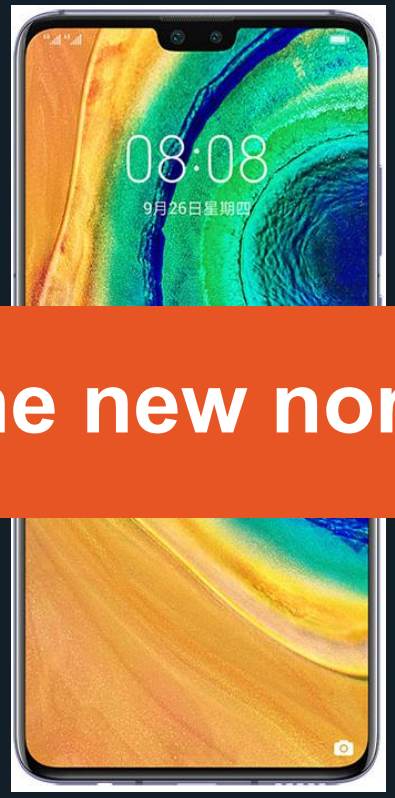
File Based Encrypted Devices

Google Pixel

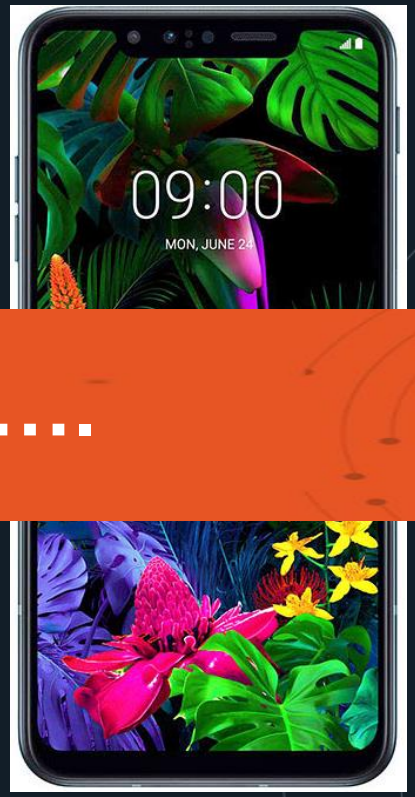


Samsung Galaxy S10

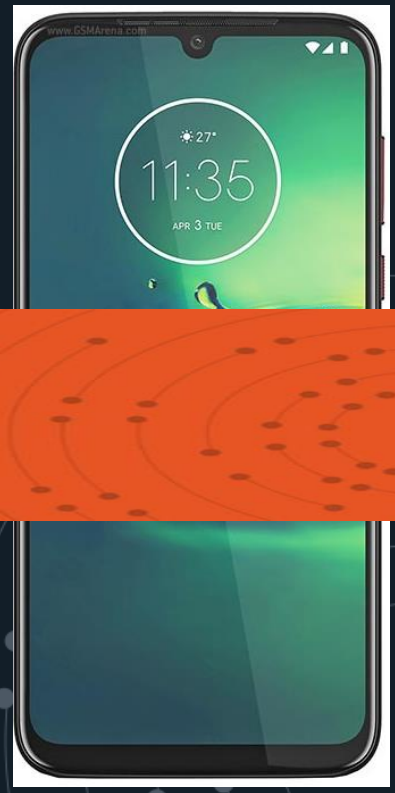
Huawei Mate 30



LG G8 ThinQ



Motorola G8 Plus

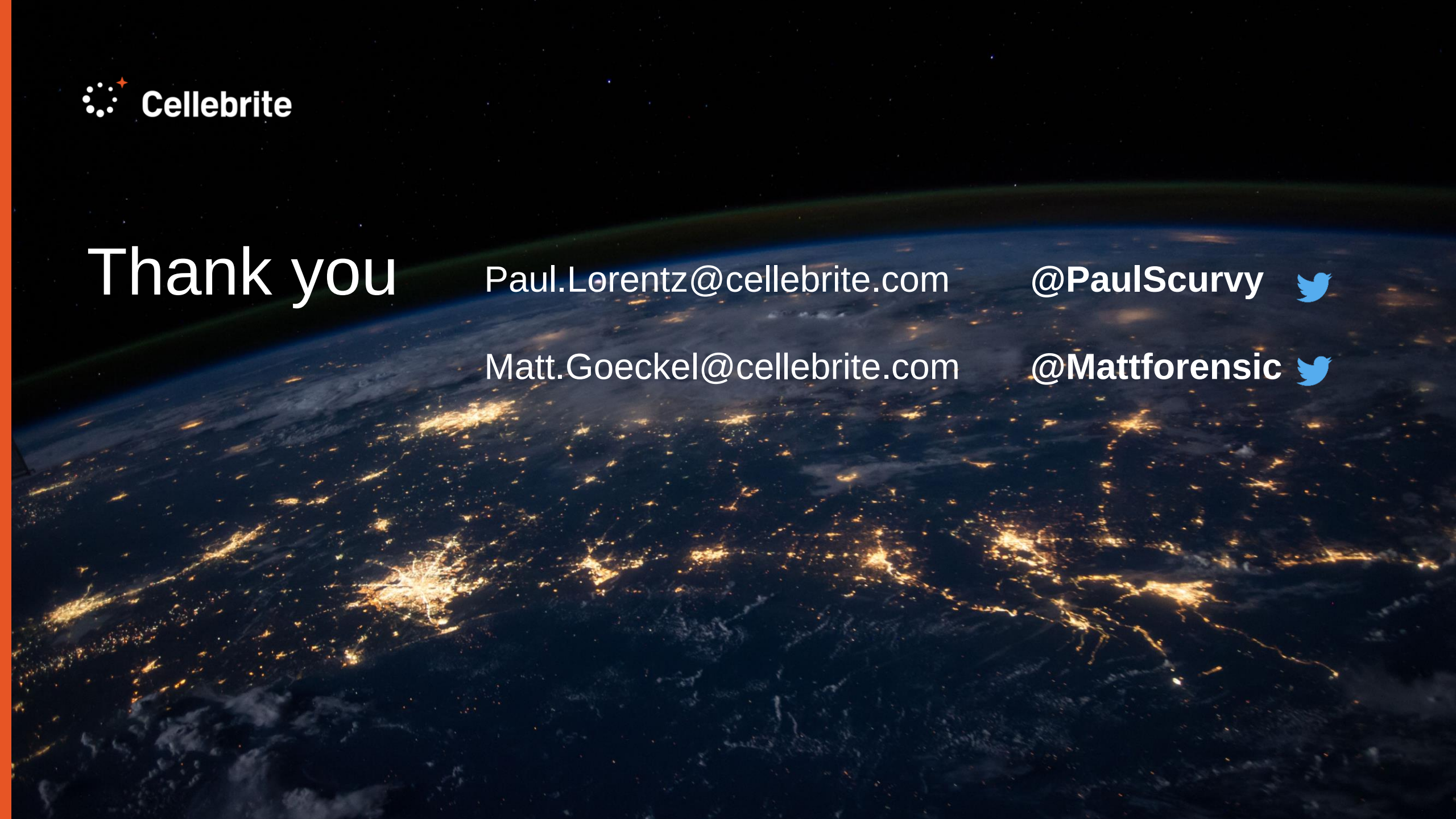


Sadly this is becoming the new norm….

Change is difficult, but should be expected.

But there’s always a way…..

Cellebrite


Cellebrite
Thank you
Paul.Lorentz@cellebrite.com
@PaulScurvy
Matt.Goeckel@cellebrite.com
@Mattforensic