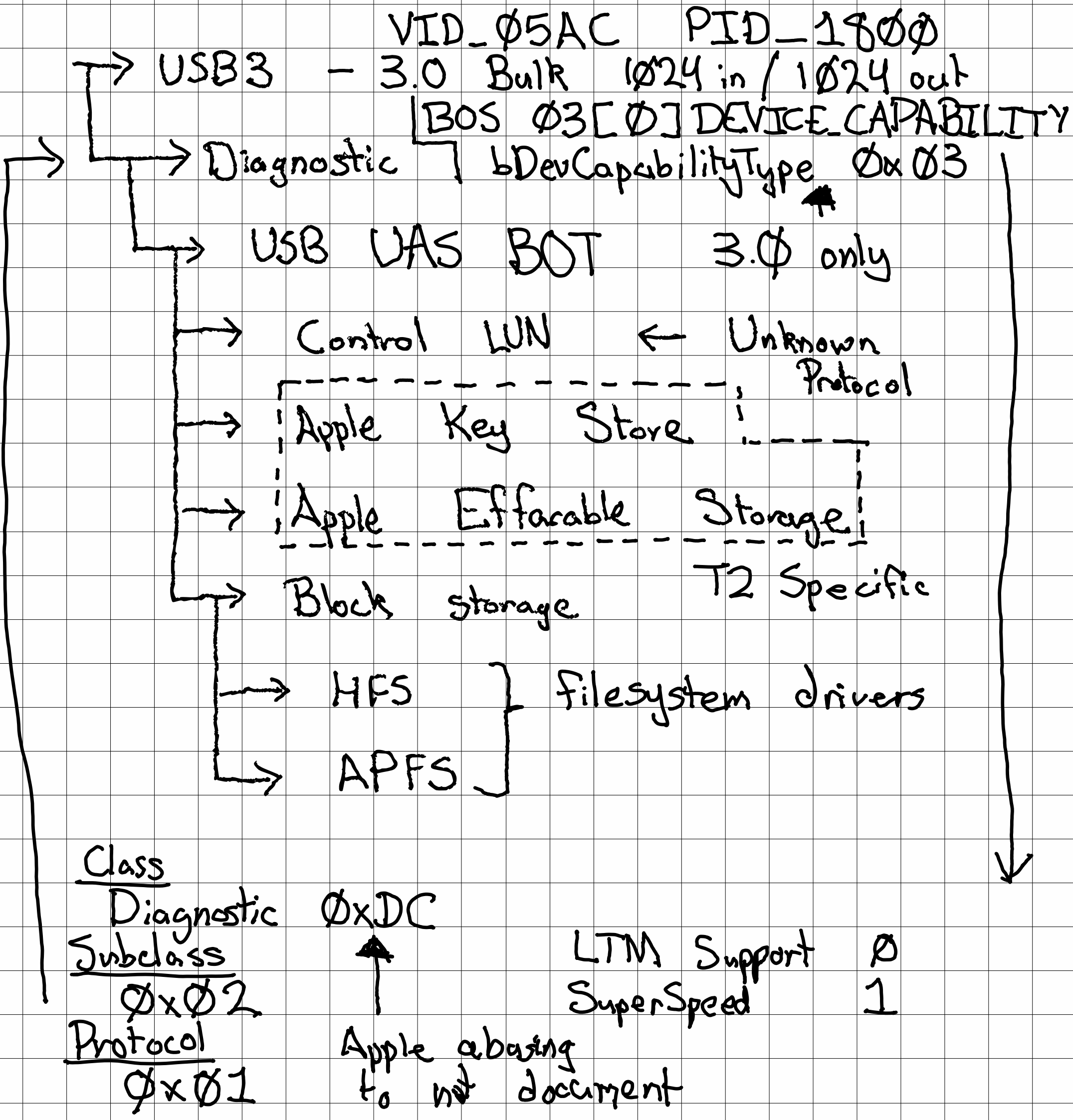
Apple Target Disk Mode on T1 and T2 machines



VID_Ø5AC PID_18ØØ

USB3 - 3.0 Bulk 1Ø24 in / 1Ø24 out

BOS Ø3[Ø] DEVICE_CAPABILITY

Diagnostic

bDevCapabilityType Øx Ø3

USB UAS BOT

3.Ø only

Control LUN ← Unknown Protocol

Apple Key Store

Apple Effacable Storage

T2 Specific

Block storage

HFS

APFS

filesystem drivers

Class

Diagnostic ØxDC

Subclass

ØxØ2

Protocol

ØxØ1

Apple abusing to not document

LTM Support Ø

SuperSpeed 1

```
+  IOSCSITargetDevice
   +  IOSCSIHierarchialLogicalUnit @ Ø
      +  AppleTDMControlLUN
   +  IOSCSIHierarchicalLogicalUnit @ 1
      +  AppleTDMAKSDriver ←┐
         +  AppleKeyStore   proxy
   +  IOSCSIHierarchicalLogicalUnit @ 2
      +  AppleTDMEffaceableNORDriver ← proxy
         +  AppleTDMNORFlashDevice
   +  IOSCSIHierarchicalLogicalUnit @ 3
      +  AppleTDMTypeØØ ← Block w/
                      ↓   AES-XTS
         +  AppleTDMBlockStorageServices
            +  IOBlockStorageDriver
               +  IOMedia
                  +  etc ...
```

Related Kernel Modules

+ AppleUSBTDM
+ AppleThunderbolt UTDM
+ AppleStorageDrivers
+ Apple KeyStore
+ Apple Hollywood ?
+ AppleFDEKeyStore
+ Apple Effaceable Storage
+ AppleEffacable NOR
+ IOUSBAttached SCSI
+ IOSCSIArchitectureModelFamily

AppleTDMControlLUN : Power Distribution

- GetAndSetPowerRequirements
- SetupBatteryStatusPolling
- Disable " "
- GetEVPDINQUIRYData
- SendControlRequest
- ReconditionTarget

AppleTDMAKSCommand (IOService*, unsigned short)

nabla-c0d3/iphone-dataprotection

AppleKeyStore.h

AppleTDMType00

- NVMeSecureErase
- GetIdentifyData
- DetermineDeviceCharacteristics
- DetermineMediaWriteProtectStatus
- GetAndPublishPageC0/2/3Data
-

LE uint32
↓

Negotiation :

H → T : "USBC", sequence =0, 31 bytes

uint16 uint16

receive_length send_length

T → H bytes

T → H uint8 uint8

"USBS", sequence , length

uint32 uint32 sint8

"USBC", sequence, receive_len, ep

USB Bulk Only Transport

no further analysis needed

Get LUNS   BE   uint32 length

response   BE   uint32 size
uint32

LUN[]
↑
8 byte

Inquiery Page code Ø

BE uint32 pages
byte[] page_id

ØSCØ   CØ   C1   C2   C3
↑
List of available vendor code pages to read

Serial Number? → $\boxed{83}$ ...

Changes as firmware reads values

Erase Routine

- Effacable Storage
  - Get geometry
  - Erase locker
- Disk, loop over bytes
  - Scsi erase / write nulls
- Open question. Disk controller firmware validity?
  + Store / Read test?
    - Random write, hash read?
    - Could still store malicious blocks in wear leaveling regions.
    - NVMe firmware upgrade procedure?
  - What other non-volitile storage exists?
    - Thunderbolt controller

iOS Key Wrapping

Each AP has burned in GID/UID

AppleKeyStore.kext handles the interfacing with the crypto engine

Recovery key provides the full key for extracting data

The T2 sits in the NVMe path on the PCIE bus, likely performing AES-GCM on the data

Interogitive: Is there value in file vault when a firmware password is stored and full secure boot is enabled?

Where is the firmware password stored?

↳ Disassemble app / get IOReg

What does the USB interface to the T2 look like? (network NCM?)