Reconstruction en boîte noire d'accès à une carte SD

Xavier Mehrenberger & Raphaël Rigo

BeeRumP - 2017-06-22

AIRBUS GROUP

Idée

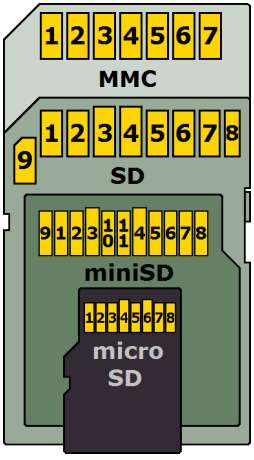
- Carte SD lue par un équipement
- Enregistrer les communication SD Card
- Décoder le protocole
- Déterminer quels fichiers ont été lus

Matériel de capture

Sparkfun SD/MMC breakout board – $10

Saleae Logic Pro 16 – $600
USB3, 16 canaux, 500MS/s

Pins



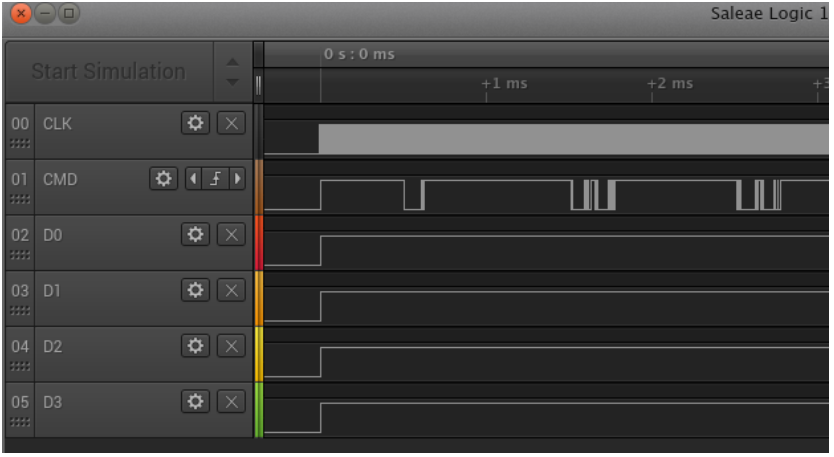
Pins :

- 1 : Card detect / DAT3 (data 3)
- 2 : CMD (commandes)
- 3 : VSS (masse)
- 4 : VCC (3.3v)
- 5 : CLK (horloge)
- 6 : VSS (masse)
- 7 : DAT0 (data 0)
- 8 : DAT1 (data 1)
- 9 : DAT2 (data 2)

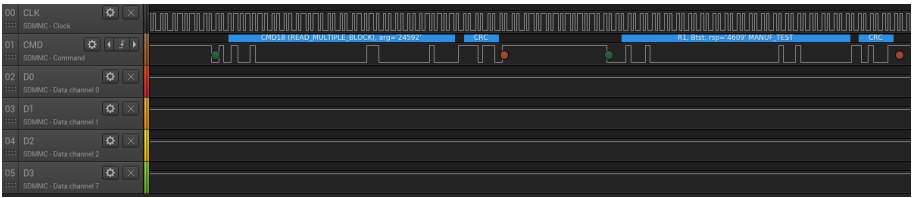
Modes :

- Single Bit
- 4 bits
- Single Data Rate / Double Data Rate
- . . .

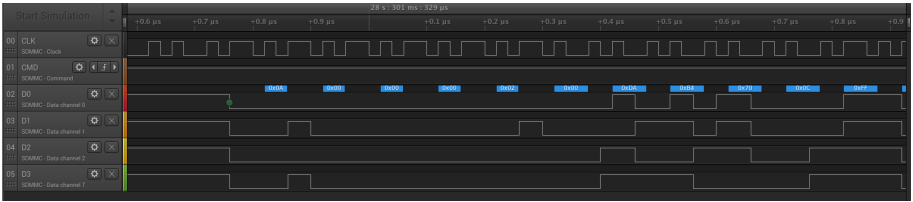
Saleae Logic Analyzer, sans décodeur



Résultat avec décodeur – commandes



Résultat avec décodeur – données



Protocole MMC – requête

- 1 ligne pour les commandes CMD (bi-directionnel)
- Commande envoyée par le lecteur

Protocole MMC – réponse

- Puis réponse de la carte - 7 formats de réponse possible

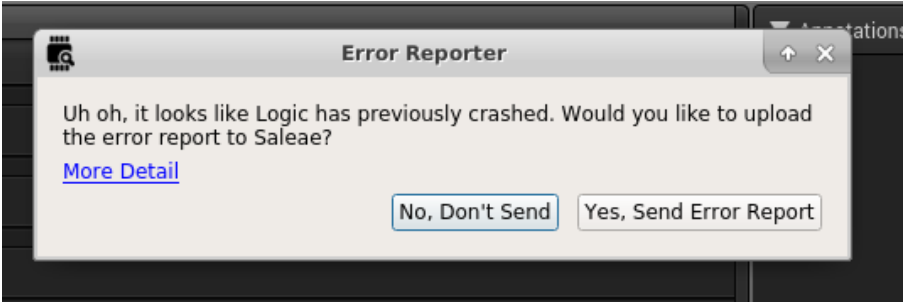
Protocole MMC – données

- 1, 4 ou 8 lignes de données (bi-directionnel)

Décodage du protocole

- Acquisition du signal avec `saleae`, export csv possible
- Option 1 : utiliser `sigrok` ?
  - \+ décodeur de (quelques) commandes existant, en python
  - \+ open source
  - \+ un peu documenté
  - – API d'accès aux données : fonction appelée pour chaque échantillon
- Option 2 : plugin `saleae`
  - \+ décodeur de commandes existant plus mature, en C++
  - \+ GUI : annotation sur les signaux, recherche
  - – documentation des APIs : partiel... il faut chasser les exemples
  - – pas de stagiaire à sacrifier pour que ça tombe en marche :-(
  - – pas open source : debug plus difficile

Crash


Error Reporter
Uh oh, it looks like Logic has previously crashed. Would you like to upload the error report to Saleae?
More Detail
No, Don't Send
Yes, Send Error Report

Difficultés

- API `saleae`
  - lire les valeurs
  - avancer jusqu'au prochain front d'horloge
  - $\Rightarrow$ pas de retour en arrière
- Interruption des transferts possible
- Transferts en parallèle des réponses
- Code existant : commandes uniquement
- 2 machines à état en parallèle : données, code
- Désynchronisation $\Rightarrow$ la suite est inutilisable
- 2 normes: SD, eMMC, assez similaires – lol

Reconstruction

- Sortie : fichier texte
  - commandes (ex. `READ_SINGLE_BLOCK`, `READ_MULTIPLE_BLOCK`)
  - arguments (ex. adresses)
  - données
- Reconstruction de l'image contenant les données lues

Analyse des accès aux fichier

- Quels fichiers ont été lus ?
- Utilisation d'un FS custom `https://github.com/phil777/fat-fuse`
- Contenu des fichiers : adresses physiques où chaque groupe de 8 octet est stocké
- $\Rightarrow$ on sait quels fichiers ont été lus

Timeline

- T : Audit d'un équipement
- T+X mois : release du code
- BeeRumP-1j : écriture des slides
- BeeRumP-1j : test anonymisé => fail
- BeeRumP-0j : test qui marche
- BeeRumP-6h : découverte du mode UHS-I – 200 MHz – fail
- BeeRumP : fin des slides ;)

Merci !

Merci

Questions ?

https://github.com/airbus-seclab/sdmmc-analyzer

Références

- [dirk] sdmmc-analyzer original code
  `https://github.com/dirker/sdmmc-analyzer`