

TRANSAKCJA PŁATNICZA

Małgorzata Wętkowska

Spis treści

- * Czym jest transakcja?
- * Karta płatnicza
- * Odczytanie danych z karty
- * Log transakcji

Czym jest transakcja?

- * Transakcja - zbiór operacji na bazie danych
- * Przelew - zabranie i dodanie pieniędzy z i do konta
- * 3 etapy:
 - Rozpoczęcie
 - Wykonanie
 - Zamknięcie

Karta płatnicza

*Magnetyczne

- kody kreskowe

*Elektroniczne

- pamięciowe stykowe
- procesorowe stykowe
- zbliżeniowe
- dualne



Odczytanie danych z karty

* Urządzenia

➤ Terminale płatnicze

* Aplikacje mobilne

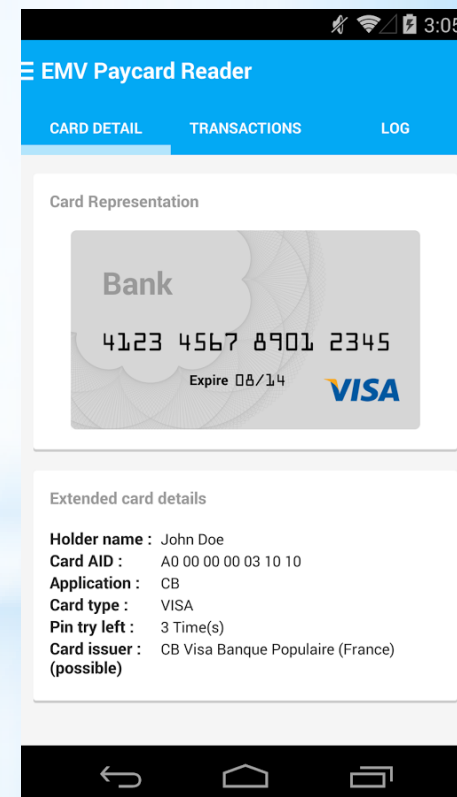
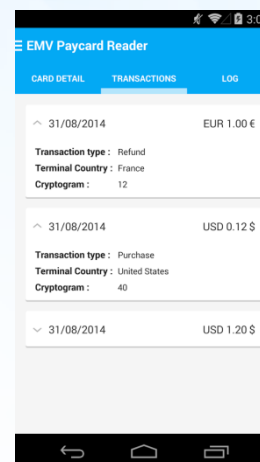
➤ Banking card reader NFC

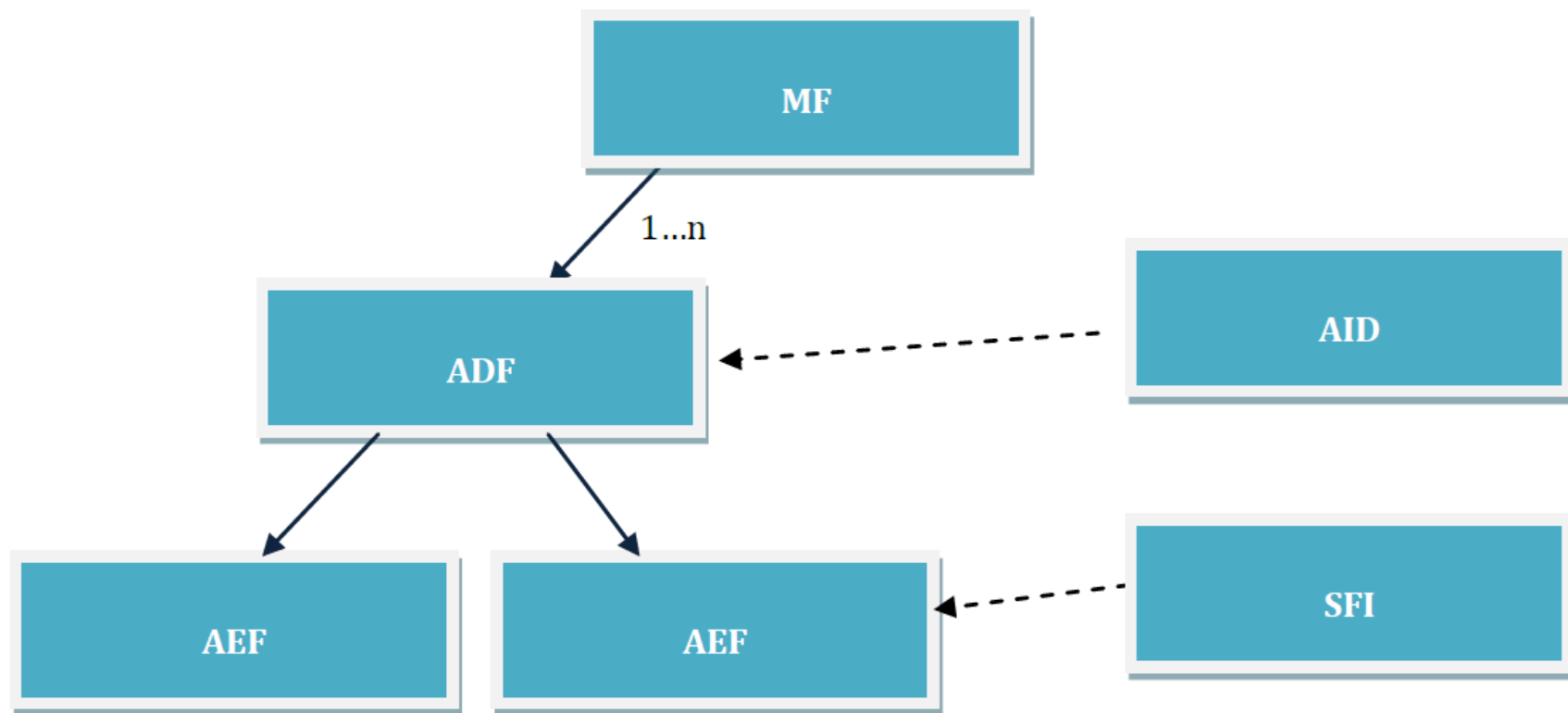
➤ Bankomat Card Infos

➤ CardTest

```
01:52:16.416: Er...
9F 4F - 1A bytes: Log Format
9F 27 (01 bytes) -> Cryptogram Information Data
9F 02 (06 bytes) -> Amount, Authorised (Numeric)
5F 2A (02 bytes) -> Transaction Currency Code
9A (03 bytes) -> Transaction Date
9F 36 (02 bytes) -> Application Transaction Counter (ATC)
9F 52 (06 bytes) -> Application Default Action (ADA)
DF 3E (01 bytes) -> [UNHANDLED TAG]
9F 21 (03 bytes) -> Transaction Time (HHMMSS)
9F 7C (14 bytes) -> Customer Exclusive Data
01:52:16.417: trying to read PIN retry counter from card...
01:52:16.418: sent: 80CA9F1700
01:52:16.428: received: 9F1701039000
01:52:16.429: status: 90 00 - success ->
01:52:16.429: Trying to decode response as BER-TLV..
01:52:16.430:
9F 17 - 01 bytes: Personal Identification Number (PIN) Try Counter
03 (BINARY)
01:52:16.430: -----
01:52:16.430: Current PIN retry counter: >>>>> 3 <<<<<
01:52:16.431: -----
```

```
CardTest
379*****006 AMERICAN EXPRESS
EXP 01/16
NEW TAG! ID=77 18 35 D7
Generic query worked.
-- [GENERIC QUERY RESULTS ]-----
Response Code: 9000
TAG: 6F LEN:26
[File Control Information (FCI) Template]
TAG: 84 LEN:14
[Dedicated File (DF) Name]
31 50 41 59 2e 53 59 53 1PAY.SYS
2e 44 44 46 30 31 .DDF01
TAG: A5 LEN:8
[File Control Information (FCI)
Proprietary Template]
TAG: 88 LEN:1
[Short File Identifier (SFI)]
01
TAG: 5F2D LEN:2
[Language Preference]
65 6e en
-- [sfi 1 blk 1 ]-----
Response Code: 9000
TAG: 70 LEN:33
[READ RECORD Response Message Template]
TAG: 61 LEN:31
[Application Template]
TAG: 4F LEN:8
```





Master File (MF) - posiada jeden lub więcej Application Definition Files (ADF). Wewnątrz ADF znajdują się Application Elementary Files (AEF), który zawierają niezbędne informacje.

Dostęp do ADF możliwy jest za pomocą Application Identifier (AID). Możliwe jest również wybranie AEF za pomocą Short File Identifier (SFI).

Banking Card Reader

CARD DETAIL

TRANSACTIONS

LOG

Card Representation



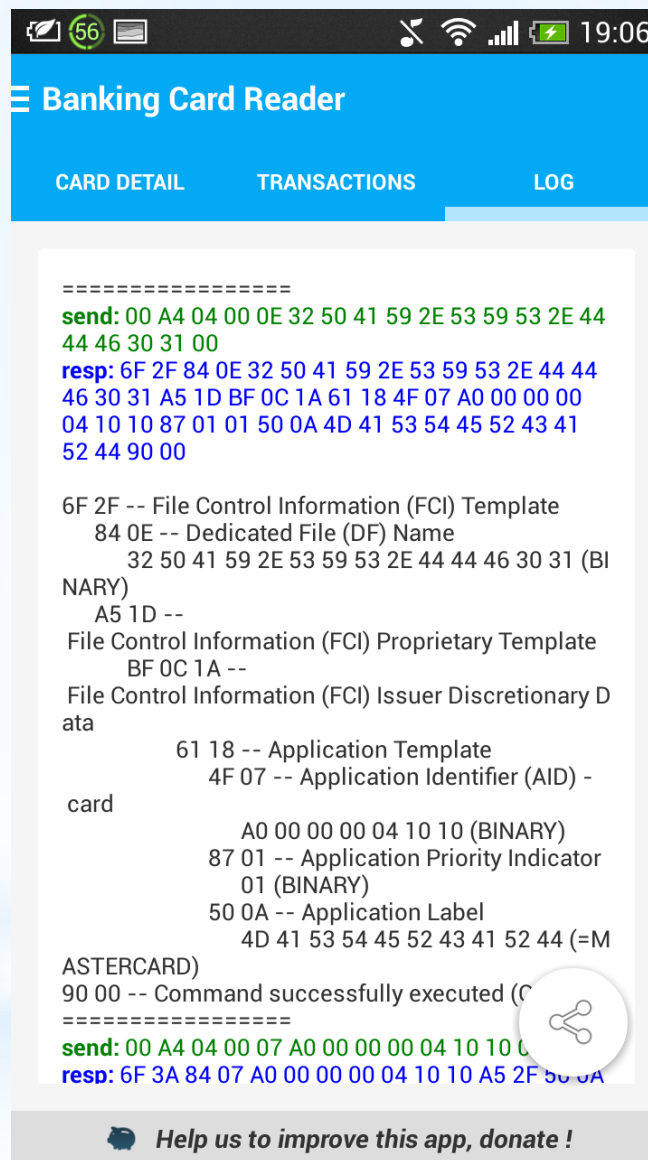
Extended card details

Card AID : A0 00 00 00 04 10 10
Application : MASTERCARD
Card type : Master card
Pin try left : 3 Time(s)
Card issuer : Mastercard international credit card, with
(possible) Moneo extension

 *Help us to improve this app, donate !*

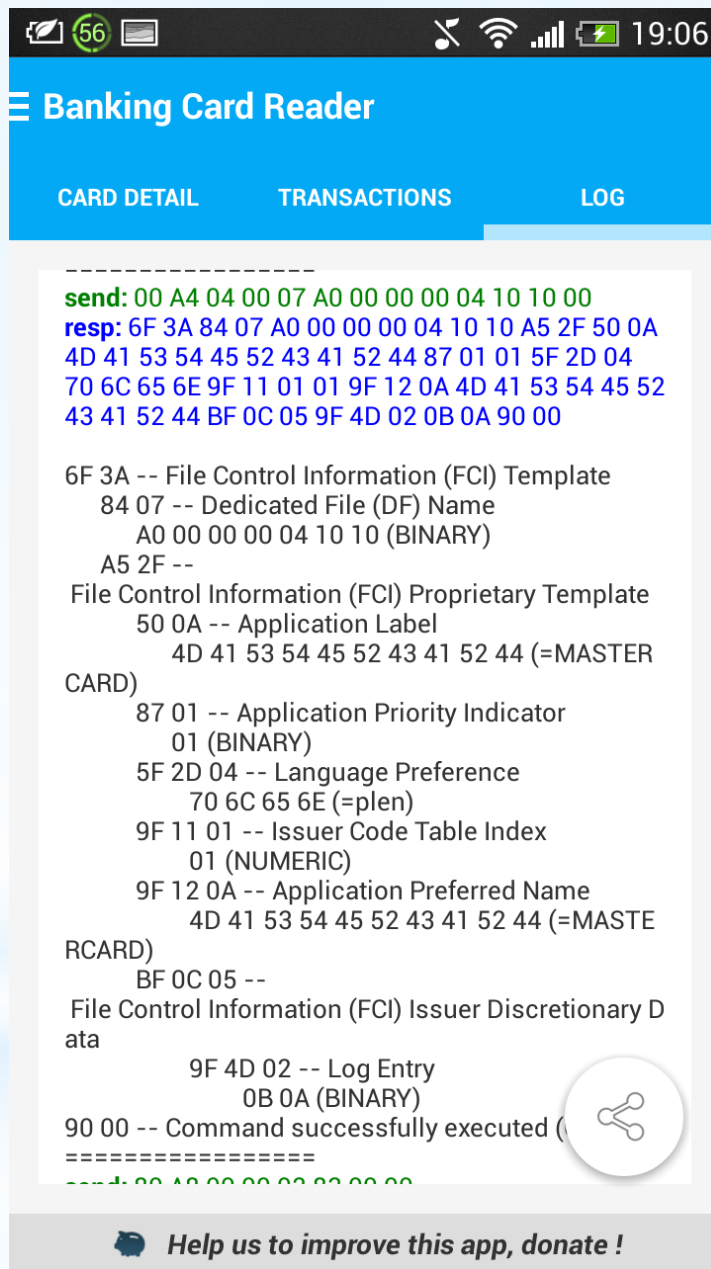
-Wysyłana jest komenda
SELECT FILE odczyt
danego folderu o
nazwie binarnej 32 50
41 59 2E 53 5953 2E 44
44 46 30 31 czyli PPSE -
Proximity Payment
System Environment

-PPSE - folder
zawierający listę
aplikacji obsługiwanych
przez interfejs
bezstykowy,
wywoływany jest za
pomocą polecenia
SELECT



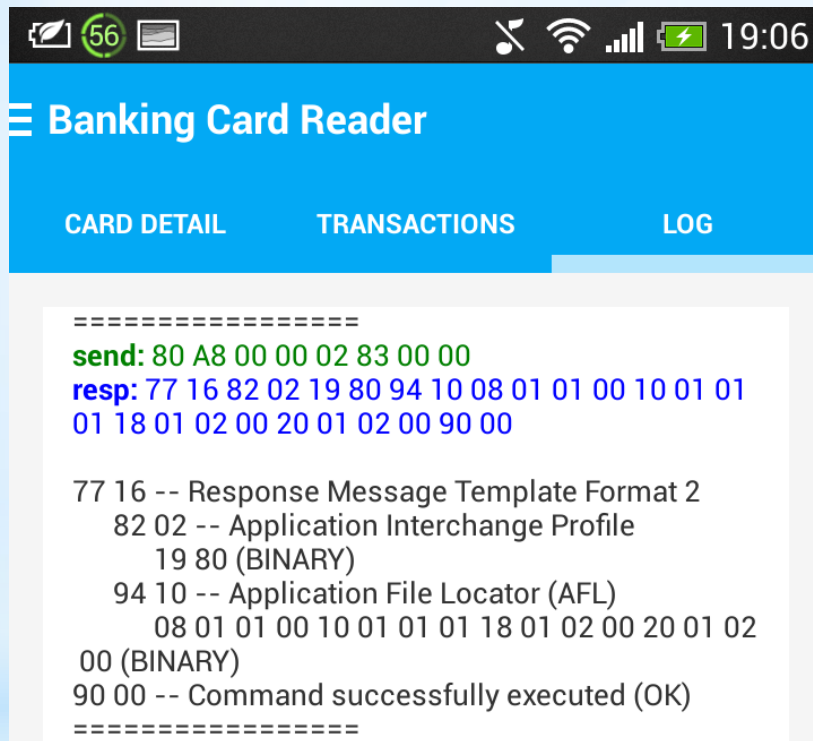
- W odpowiedzi
dostajemy informację
że w kolejnym kroku
należy wybrać folder o
binarnej nazwie A0 00
00 00 04 10 10 czyli
Application Identifier
MasterCard Credit,
etykieta aplikacji 4D 41
53 54 45 52 43 41 52
44 - CB MasterCard

-SELECT FILE A0 00
00 00 04 10 10 -
identyfikator karty
MasterCard



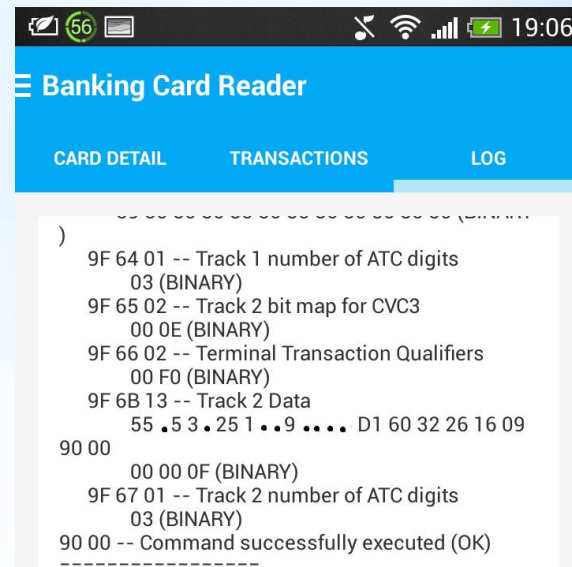
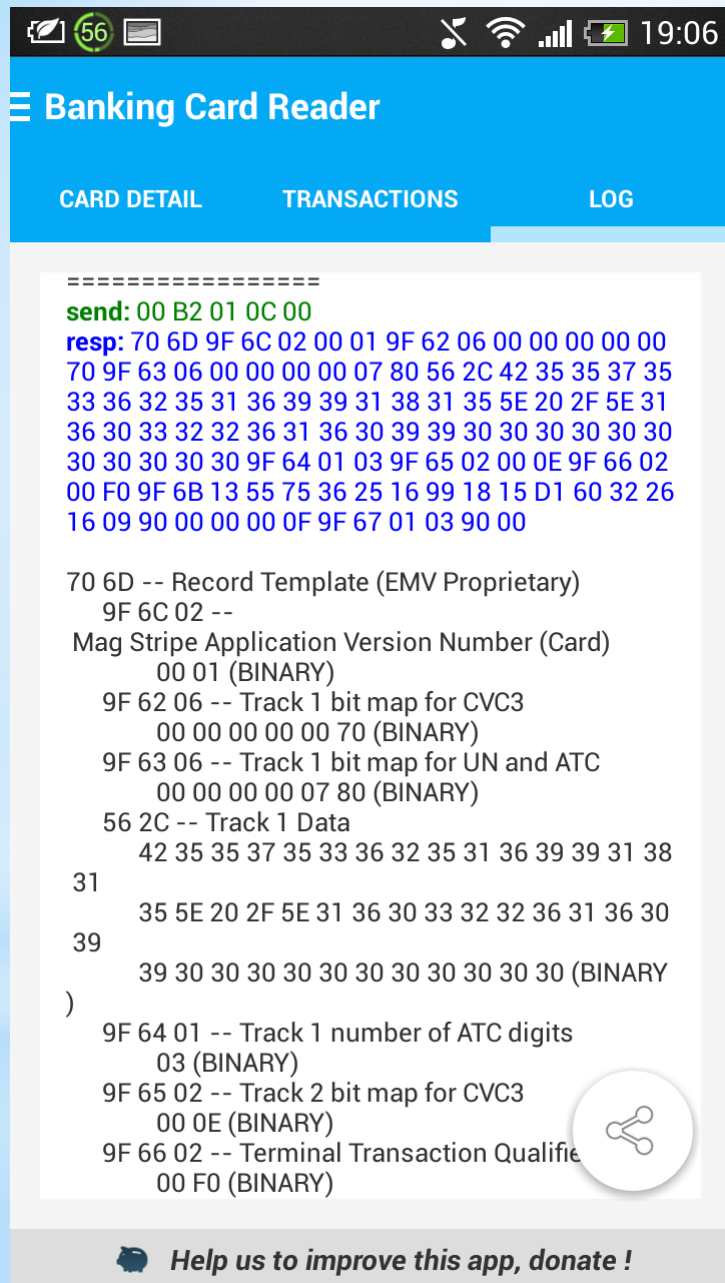
W odpowiedzi
otrzymujemy etykietę
aplikacji, preferencje
językowe.

GET PROCESSING OPTIONS -
inicjuje transakcje w karcie



AIP wskazuje, jakie kroki przetwarzania (np weryfikacji posiadacza karty, uwierzytelnianie danych) są obsługiwane, a które powinny być stosowane do bieżącej transakcji.

AFL jest listą rekordów danych aplikacji znajdujących się na karcie, terminal będzie korzystać z AFL do odczytu danych z karty aplikacji. AFL również wskazuje, które, jeśli w ogóle, z rekordów danych powinny być wykorzystane przez terminal jako część danych wejściowych do procesu uwierzytelnienia danych.

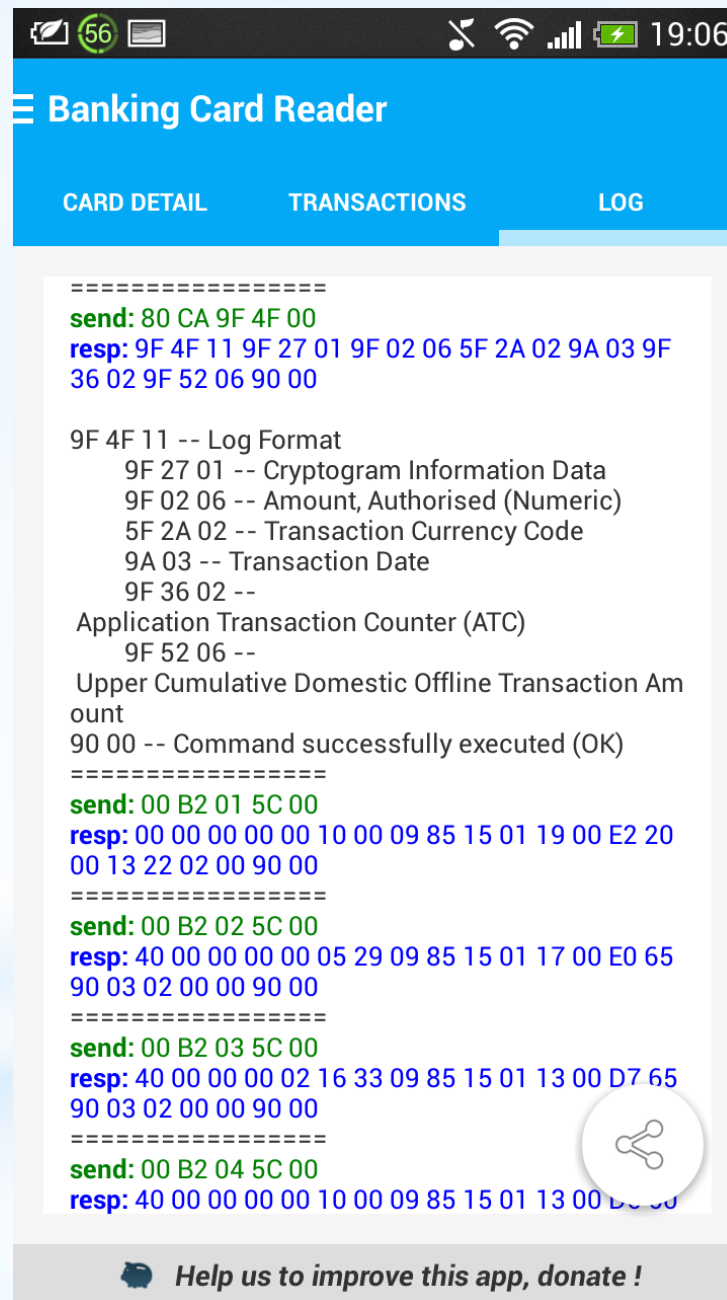


-READ RECORD przeczytanie rekordu od 1 do ostatniego

Ścieżka I- Imię i Nazwisko posiadacza karty, dane dotyczące kraju i banku wydającego kartę

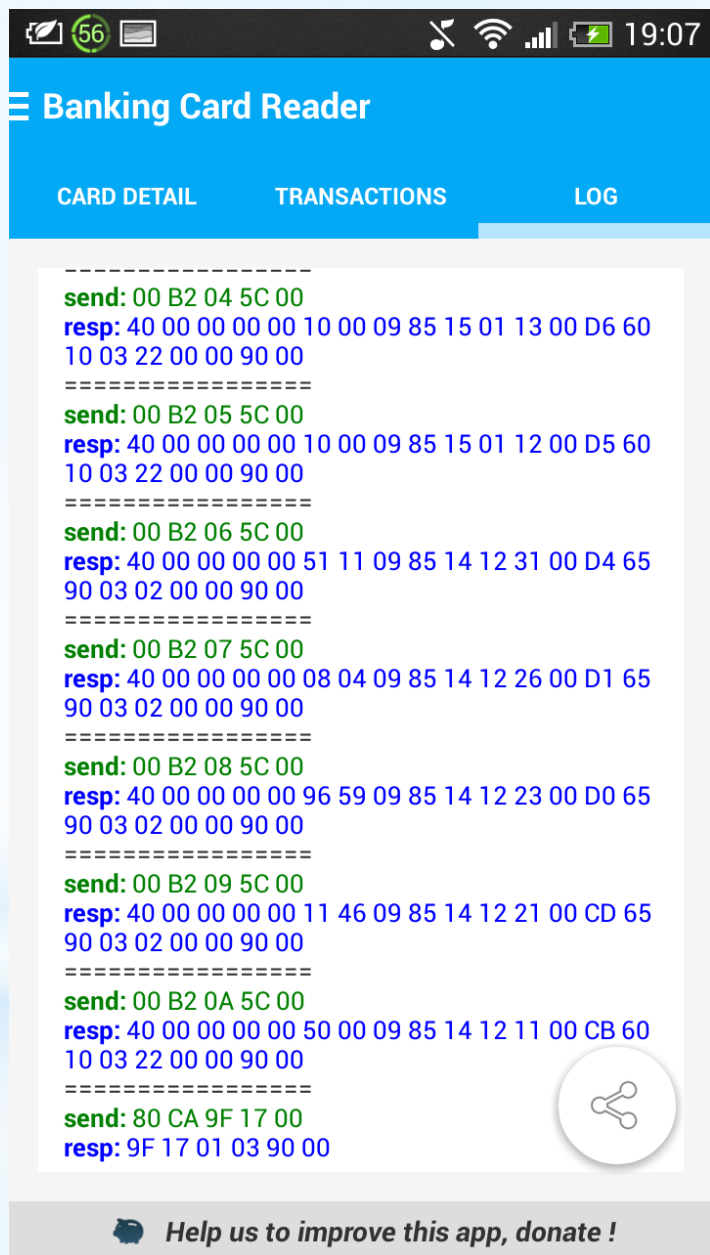
Ścieżka II - zawiera numer karty, datę ważności oraz kod serwisowy potrzebny do prawidłowego przeprowadzenia transakcji

Ścieżka III - Istnieje i wykorzystywana jest do zapisywania informacji o banku, obecnie nie wykorzystywana.

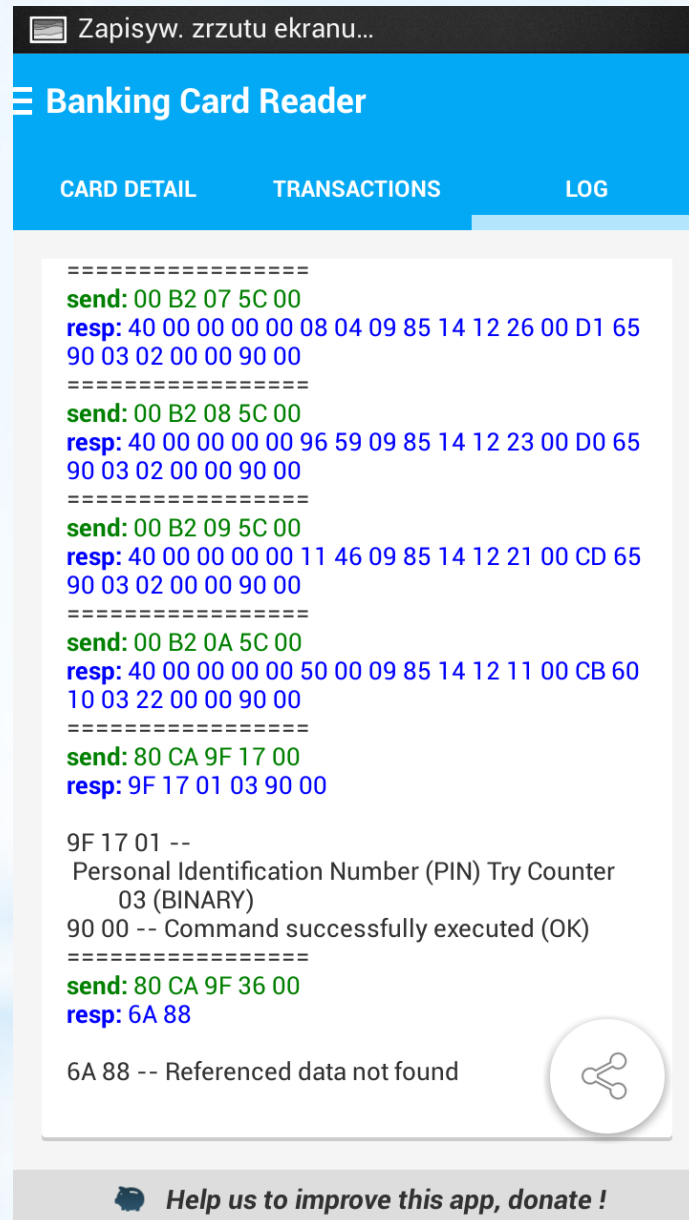


Komenda GET DATA służy do znalezienia formatu logu

W odpowiedzi na polecenie GET DATA - otrzymujemy informację o szyfrowaniu danych na karcie, autoryzowaną kwotę transakcji, datę transakcji oraz licznik transakcji



READ RECORD -
odczytuje rekordy
danych od 1 do
ostatniego,



Polecenie GET DATA 80
CA 9F 17 00
odpowiada za licznik
prób wpisania
błędnego kodu PIN

DZIĘKUJĘ ZA UWAGĘ