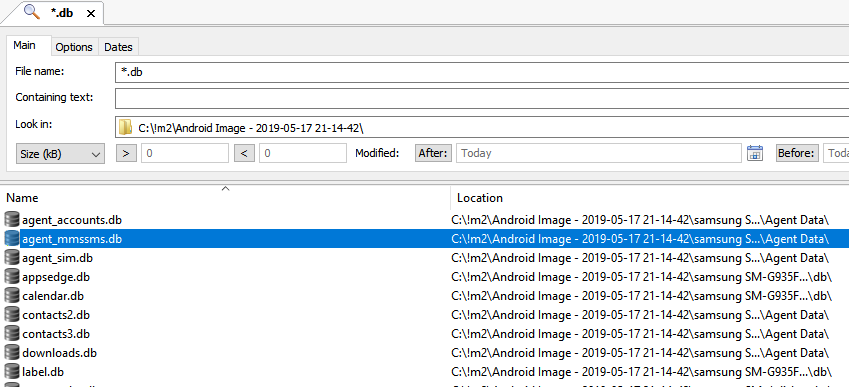
**Wykorzystanie skryptów Python’a do akwizycji SMS i MMS’ów z telefonu komórkowego Samsung z systemem operacyjnym Android 8.0**

Autor: C. Wawrentowicz

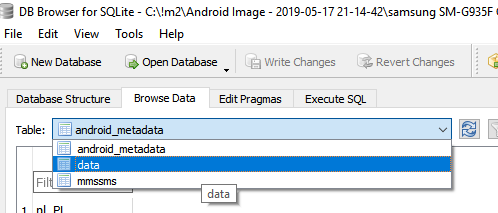
Data: 16.06.2019

Udostępnienie przez firmę Magnet darmowego programu „Magnet ACQUIRE” służącego do akwizycji danych m.in. z urządzeń mobilnych zainspirowało mnie do przeprowadzenia prób wykorzystania tego oprogramowania do pozyskania danych z telefonów komórkowych wyposażonych w system operacyjny Android. Do prób wykorzystałem model telefonu Samsunga z zainstalowanym systemem operacyjnych Androida 8.0.0, a celem było uzyskanie przejrzystego raportu z zawartością SMS i MMSów.

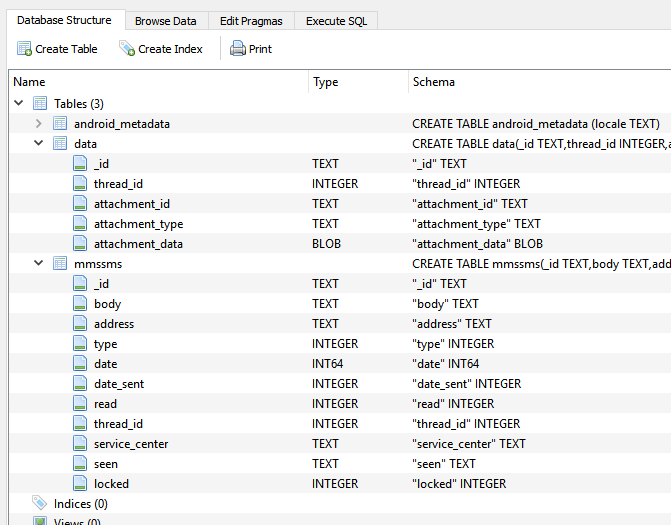
Po wykonaniu akwizycji danych programem „Magnet ACQUIRE” ich analizę rozpocząłem od wyszukania plików baz danych typu SQLite, które są standardowo używane do przechowywania danych w systemie Android. Do tego celu użyłem programu File Locator wyszukując plików z rozszerzeniem „.db”. Wśród znalezionych plików znajdował się m.in. plik o nazwie „agent\_mmssms.db”



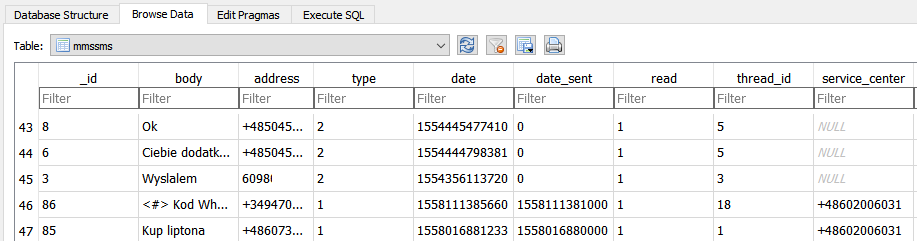
Zawartość tego pliku odczytałem za pomocą programu „DB Browser for SQLite”. Znajdowały się w nim trzy tabel, ale kluczowe znaczenie dla analizy miały dwie z nich: „data” i ”mmssms”

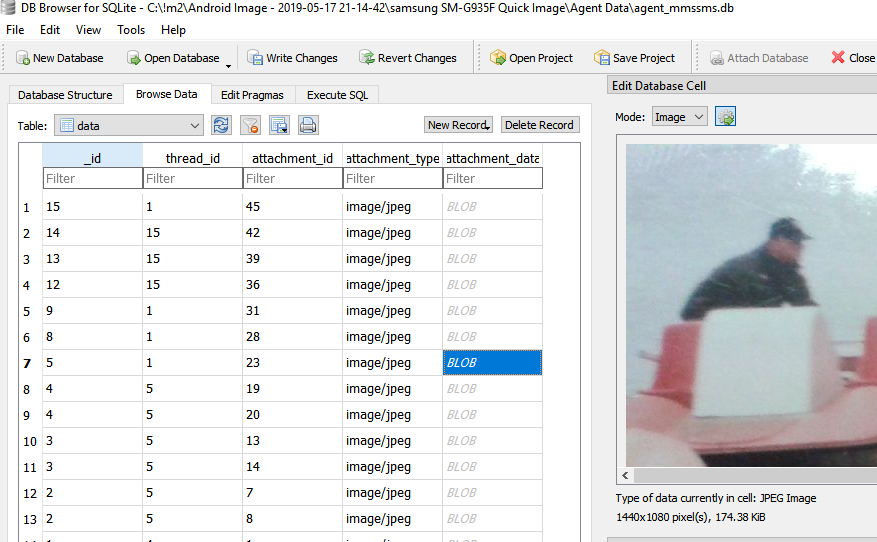


Rzut oka na ich strukturę pozwala stwierdzić, że w tabeli „mmssms” są przechowywane podstawowe dane z SMSów i MMSów, a w tabeli „data” załączniki do tych wiadomości (grafika w polach typu BLOB).

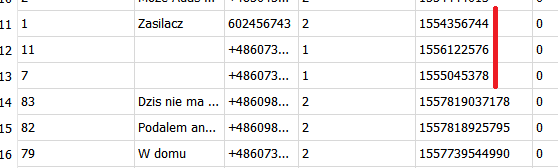


Przeglądając zawartość tabel „data” można zauważyć, że treść wiadomości jest przechowywana w polu „body”, numer telefonu w polu „address”, typ wiadomości wchodząca/ wychodząca w polu „type”, a data wiadomości w polu „date”. Wszystkie daty i czas są zapisane w formacie UNIX (czasu mierzący liczbę sekund od początku [1970](https://pl.wikipedia.org/wiki/1970) roku [UTC](https://pl.wikipedia.org/wiki/Uniwersalny_czas_koordynowany)).





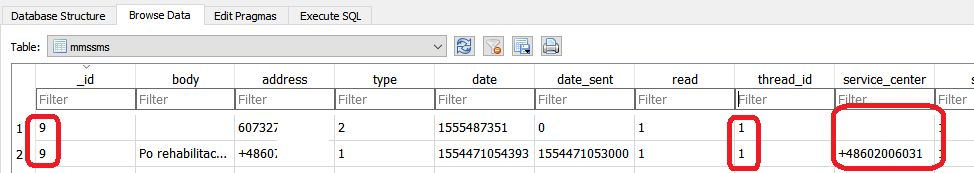
Analiza zapisu daty i czasu wykazała, że w przypadku gdy na końcu liczby reprezentującej datę i czas występowały trzy zera były one pomijane.



W związku z tym podczas konwersji daty i czasu na format „rrrr-dd-mm gg:mm:ss” należy sprawdzić ilość cyfr występujących w liczbie reprezentującej datę i czas i zależnie od otrzymanego wyniku wykonać odpowiednie wyliczenia w zapytaniu SQL.



Następnym przeanalizowałem sposób tworzenia relacji pomiędzy tabelami „data” i „mmssms”. Stwierdziłem, że tabele łączą się za pomocą klucza złożonego z dwóch pól: „\_id” oraz „thread\_id” jednak np. dla załącznika (tabela „data”) o wartościach \_id=9 i thread\_id=1 w tabeli „mmssms” odpowiadają dwa rekordy czyli wyglądało jakby te samo zdjęcie było wysłane dwukrotnie co w rzeczywistości nie miało miejsca. Dalsza analiza i porównanie wiadomości w telefonie komórkowym pozwoliło stwierdzić, że dodatkowym warunkiem łączącym rekordy w obu tabelach jest konieczność występowania numeru w polu „service\_center”.

v

Bazując na tych informacjach napisałem skrypt w Pythonie tworzący raport z treścią SMSów i MMSów w formacje HTML5

