UNIVERSITY OF PIRAEUS

Postgraduate Program “Techno-economic Management & Security in Digital Systems”

Department of Digital Systems

Design and implementation of an information system for extraction and processing security data of mobile networks

Georgios Paparis

Master Thesis

Piraeus, May 2013

UNIVERSITY OF PIRAEUS

Postgraduate Program “Techno-economic Management & Security in Digital Systems”

Department of Digital Systems

Design and implementation of an information system for extraction and processing security data of mobile networks

This Master Thesis was submitted by
Georgios Paparis

Evaluation Committee:

Christos Xenakis, Assistant Professor, Supervisor
Socrates Katsikas, Professor, Member
Konstantinos Lambrinoudakis, Associate Professor, Member

Accepted by: Panagiotis Demestichas, Professor
Director of Postgraduate Program

Piraeus, May 2013

Design and implementation of an information system for extraction and processing security data of mobile networks

Georgios Paparis
M.Sc. Thesis

Security of Digital Systems, University of Piraeus

Abstract

The increasing important role of smart phones in our life is a phenomenon. Smart phones handle more and more tasks like web-browsing, e-mailing and human entertainment. The people are addicted to their user. The popularity of them drives the attackers to implement advanced attack techniques against them. One of the best techniques to prevent some these advanced attack techniques is to ensure the security of mobile network. The communication in a mobile network does between mobile station and network. During of it, both components exchange important security data. In order to ensure and research the security of a mobile network, we designed and implemented an information system that monitors a mobile network. The information system is consists of an application that is running in a smart phone , named SIM Monitor, and an application that is running in a server, named SIM Analyzer. The purpose of SIM Monitor is to record security characteristics from network and SIM or USIM card of subscriber and the purpose of SIM Analyzer is to aggregate the above data and extract some important security information for network of subscriber. The extracted results provide the researcher to monitor the security characteristics of mobile network and find possible weak points of it.

Dedicated to my parents John and Anna and my sister Joanna.

Acknowledgements

I would like to thank all the people who contributed to the completion of this work. I am truly indebted and thankful to my professor Christos Xenakis for the inspiration and opportunities he has given me. His guidance and advice has been invaluable.

I would also like to thank Mr. Socrates Katsikas and Mr. Lambrinoudakis for accepting to join the evaluation committee of my work, as well as for their useful corrections to my work.

Furthermore, I am obliged to my colleague and research associate Dimitris Raptodimos for the excellent collaboration throughout the completion of this thesis.

Finally, I owe sincere thankfulness to my parents John and Anna and to my sister Joanna whose constant support and encouragement during difficult times enables me to achieve my goals and pursue my academic interests. I dedicate my thesis to them as a small token of my appreciation for all they have done for me.

Contents

1 Introduction

1.1 Introduction

Mobile phones play an important role in today's world and become an integral life of our daily life as one of the predominant means of communication. Smart phones handle more and more tasks like web-browsing, e-mailing, navigation and purchase stocks. The popularity of smart phones and the vast number of their applications makes them more attractive targets to attackers. Advanced attack techniques affect the communication of subscriber during the phase of authentication. In this thesis, it is designed and developed an information system that monitors a mobile network and researches the security of it. The system is consists of an application that is running in a smart phone (SIM Monitor) and an application that is running in a server (SIM Analyzer). The purpose of SIM Monitor is to record security characteristics from network and SIM or USIM card of subscriber. However, the purpose of SIM Analyzer is to aggregate the above data and extract some important security information for network of subscriber.

1.2 Structure of thesis

The remain of the thesis is organized as

In the chapter 2, SIM security is described. The file system of a SIM card is analyzed and the most important security contents of a SIM card are mentioned.

In the chapter 3, Network Security is described. It describes the steps of authentication and ciphering procedure in a GSM and UMTS network. It explains why the UMTS network is more secure than GMS network.

In the chapter 4, we describe the implemented Information System. We describe the architecture and we analyze the parts of it.

In the chapter 5, SIM Monitor is described. The first part of chapter is referred to AT Commands. It describes the types of AT Commands and gives a list of them. The second part is referred to operation of SIM Monitor.

In the chapter 6, SIM Analyzer is described. A detailed description of user interface helps the reader to become familiar with application. Also, it describes the architecture of application. Finally this chapter, it is referred to the developing tools and technologies that used for its design and implementation.

In the chapter 7, we describe extended work about the implementation of thesis.

Finally, in the chapter 8 we review the thesis.

2 SIM Security

SIM is an embedded system installed in a smartcard, also known as Integrated Circuit Card (ICC). SIM is contact smart card which is specified by ISO standard [13]. It contains a microprocessor, three types of memory, which are RAM, ROM and EEPROM. It is used for the secure storage of the International Module Subscriber Identity (IMSI) as well as an encryption keys that are used to verify the modules identity and secure the mobile communication as far as confidentiality and integrity are concerned. Furthermore, a SIM card contains the Integrated Circuit Card Identifier (ICCD), the Authentication Key (Ki), Location Area Identity (LAI) contacts and SMS messages. The above mentioned values are stored in special files in the SIM module called Elementary Files (EF).

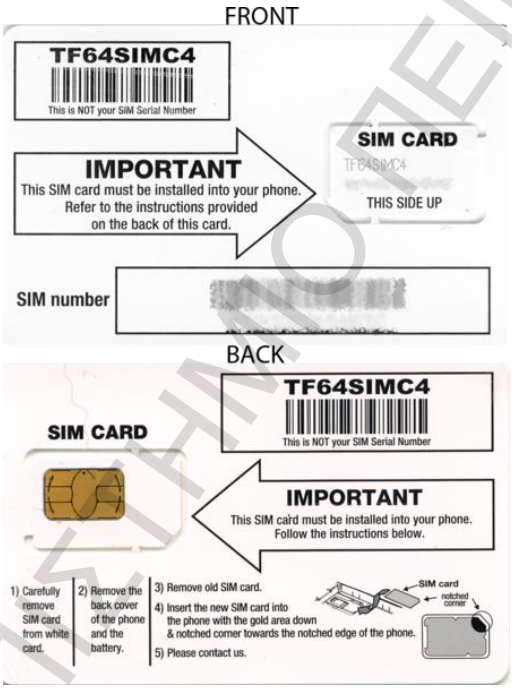

Figure 1: Both sides of a SIM card 1

2.1 SIM Memory Structure

The SIM memory structure is composed by directories and is very similar with the structure of a computer hard disk. The file system may be comprised of the following basic forms: a master file, a directory file and an elementary file [1].

The Master file (MF) is the root of file system. There is only one MF and it is analogous to the root directory in the Linux file system. The Master file contains dedicated and elementary files

Dedicated File (DF) is a subordinate directory to the Master File. It contains dedicated and elementary files.

Elementary File (EF) is a file that contains various types of formatted data. Data are structured as either a sequence of data bytes, a sequence of data bytes, a sequence of fixed size records or a fixed set of fixed size records used cyclically. More specifically

- **Transparent EF**: This file is organized as a sequence of bytes. It is possible to read all or only a subset if their contents by specifying a numeric interval.
- **Linear fixed EF**: The record is the atomic unit for this file. A record is a group of bytes that has a known coding. Every record of the same file represents the same kind of information. In a linear-fixed EF, all the records have the same length.
- **Cyclic EF**: It implements a circular buffer where the atomic unit of manipulation is the record. Therefore, the concepts of first and last are substituted by those of previous and next.

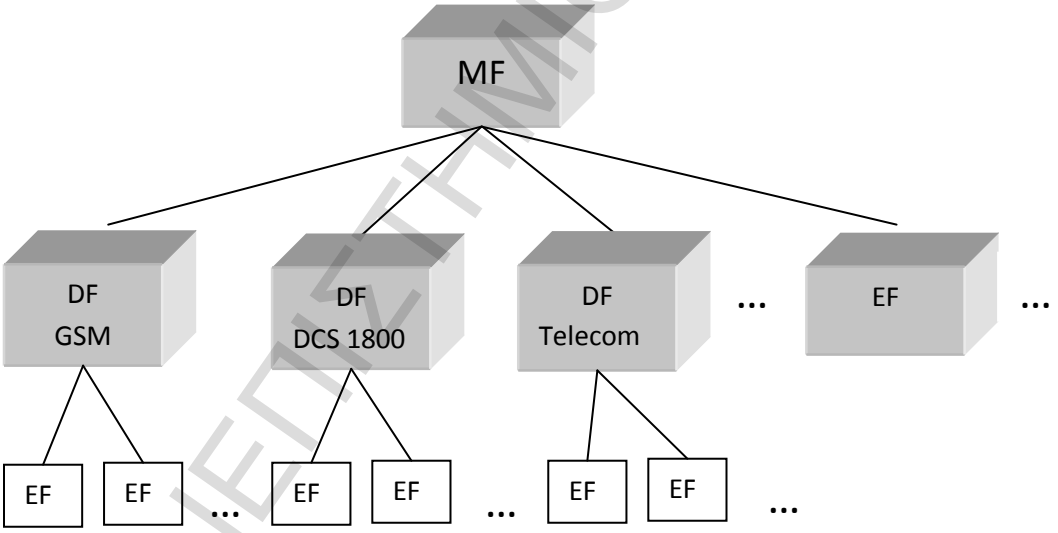

Figure 2: File System of SIM

There is also an important difference between these two types of files between DF and EF file. A Dedicated File contains a header, whereas an Elementary File contains a header and a body.

However, SIM includes numerous files to different purposes, the following are related to security and are the most important for the thesis:

1. **IMSI**: It is unique for a SIM/USIM card. It is used by the network for acquiring data for the specific subscriber. The IMSI value is sent as rarely as possible so that to prevent unwanted tracking and eavesdropping. Instead the value used is the Temporary Mobile Subscriber Identity (TMSI).
2. **Ciphering Mode:** When the ME and the network communicate through an encrypted channel the value is set to 1. When the communication is unencrypted the value is set to 0.
3. **Kc**: It is the ciphering key used by the SIM module. It is used for encrypting the voice communication between the ME and the network.
4. **KcGPRS:** Like Kc, it is used for the encrypted for the encryption of the GPRS data between the ME and the network.
5. **CK**: It is the ciphering key used by the USIM module. It is used for encrypting communication between the ME and the network.
6. **IK:** It is the integrity key used by the USIM module. It is used for ensuring integrity for the packets exchanged between the ME and the network.
7. **TMSI**: It is the identifier that is most commonly sent between the ME and the network. It is set by the network and only for the ME that are connected to a specific station. If the ME changes location and connects to a new station, the TMSI will be changed too.
8. **TMSI TIME**: It is the time interval between TMSI changes.
9. **LAI**: It is Location Area Information
10. **PTMSI**: It is the packet TMSI used for data packets.
11. **PTMSI SIGNATURE VALUE:** It ensures the integrity of PTMSI.
12. **RAI:** It is Routing Area Information.
13. **RAUS**: It is Routing Area Update Status.
14. **THRESHOLD**: It represents the time interval in which a key's update will take place.

LAI and RAI value is not the same. A network supporting GPRS is divided into Routing Areas (RAs) [12]. Each RA is defined by the operator of the network and may contain one or several cells. A Location Area (LA) is a group of one or several RAs. The RA defines a paging area for GPRS, while the LA defines a paging area for incoming calls. When the network receives an incoming call for a mobile not localized at cell level but localized at RA level, it broadcasts a paging on every cell belonging to this RA.

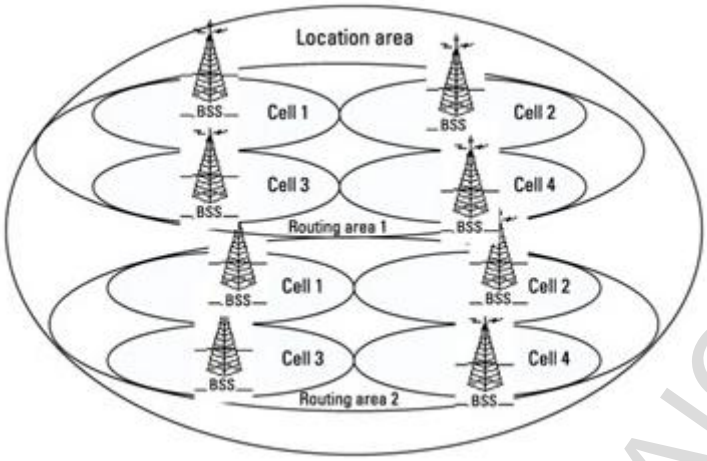

Figure 3: RA concept

When the ME moves to a new LA, it also moves to a new RA. Each RA is identified by Routing Area Identifier (RAI). The RAI consists of Location Area Identifier (LAI) and a Routing Area Code (RAC). The structure of RAI is

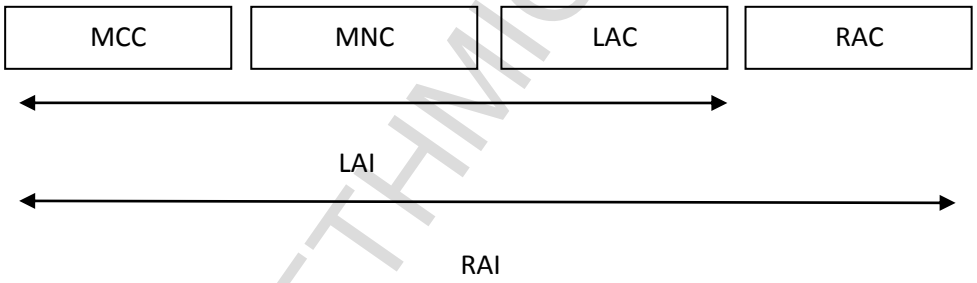

Figure 4: Structure of RAI

The LA is identified by Location Area Identifier (LAI). The LAI consists from the Mobile Country Code (MCC), the Mobile Network Code (MNC) and the Location Area Code (LAC). The RAI of each RA is broadcast on all cells belonging to this RA. The mobile station (MS) is able to detect a new RA by comparing the RAI it had previously saved with the one broadcast in the new cell, and then to signal to the network its RA change.

The basic issue is that when a Mobile Station (MS) detects a new LA or RA, it will signal to the network its LA and RA change.

2.2 Advantages of USIM

A SIM card is used to communicate on GSM network [14]. With the introduction of UMTS, it is recommended to use a SIM card to access UMTS network. The advantages of USIM [11] are the following:

- It is able to handle several mini applications, for example a contactless e-purse for the subway, a local service portal giving you access to your phone bill.
- A smart phone a USIM card can be used to make video calls. The basic requirement is the calling area is covered by 3G network.
- A new security algorithm is integrated. It allows protecting you from unauthorized access to your phone line.
- The data exchanges and calls are encrypted using keys computed by the USIM. These keys are stronger than those provided by SIMs.
- In USIM, the phonebook is bigger than SIM. It allows thousands of contacts instead of a maximum of 255 in a SIM. Also, each USIM contact is also richer, for instance it can contain email addresses, a second or third phone number.

3 Network Security

3.1 Mobile Network Technology

A brief description for each mobile network technology is appropriate when we deal with security of these systems.

GSM is an abbreviation of Global System for Mobile communication, known as Global Special Mobile [15]. It is mobile telephony that sets the standards on how mobile telecommunications work. GSM is a second generation (2G) telecommunications technology. GPRS supports data rates of max 14.4 kbit/sec. GSM is used mainly for telephony, but also for circuit switched and packet-switched data transmission. There are about 700 mobile networks that provide GMS services across more than 200 countries.

UMTS is an abbreviation of Universal Mobile Telecommunication System [16]. It is the third generation (3G) of mobile telecommunications technology. UMTS supports data rates of max 384kbit/sec. UMTS is the successor of GSM

GPRS is an abbreviation of General Packet Radio Service and is a service between UMTS and GSM networks of permanent connection to devices sustains and transmits data packets only when necessary [5]. It provides data rates of 56-114kbit/sec, in 2G systems. The 2G cellular technology combined with GPRS is described as 2.5G. It provides moderate-speed data transfer, by using unused time division multiple access (TDMA) channels.

A brief comparison of GSM and UMTS [6] is

- UMTS transfers data faster than GSM.
- GSM is 2G and 2.5G while UMTS is already 3G.
- UMTS is newer technology of GSM.
- GSM is based on TDMA while UMTS is mainly CDMA-based [18].

3.2 GSM Security

The first thing in the GSM Network Authentication must do is identify and authenticate the customer [3]. The steps in this procedure are

1. The Mobile Station requests access to the network.
2. The network and more specifically the Authentication Center (AuC) will use the IMSI to look up the Ki associated with that IMSI. The Ki is the individual subscriber authentication key. It is a 128-bit number that is paired with an IMSI when the SIM card is created. Also, the AuC will generate a 128-bit random number called the RAND. The network sends the RAND to the Mobile Station.

3. The SIM in the phone then uses the A3 Algorithm and the Individual Subscriber Authentication Key (Ki) to compute a Signed RESponse (SRES) and sends it back to the base station. The Ki is unique to every different SIM.
4. If the SRES matches the pre-computed value in the base station the user has authenticated to the network and next step takes place.
5. The SRES and the Ki are input parameters to A8 Algorithm. The purpose of the Algorithm is to compute a Session Key (Kc) and sends this to the base station.
6. The Kc is used along with the A5 algorithm to encrypt the data for over the air transmission.

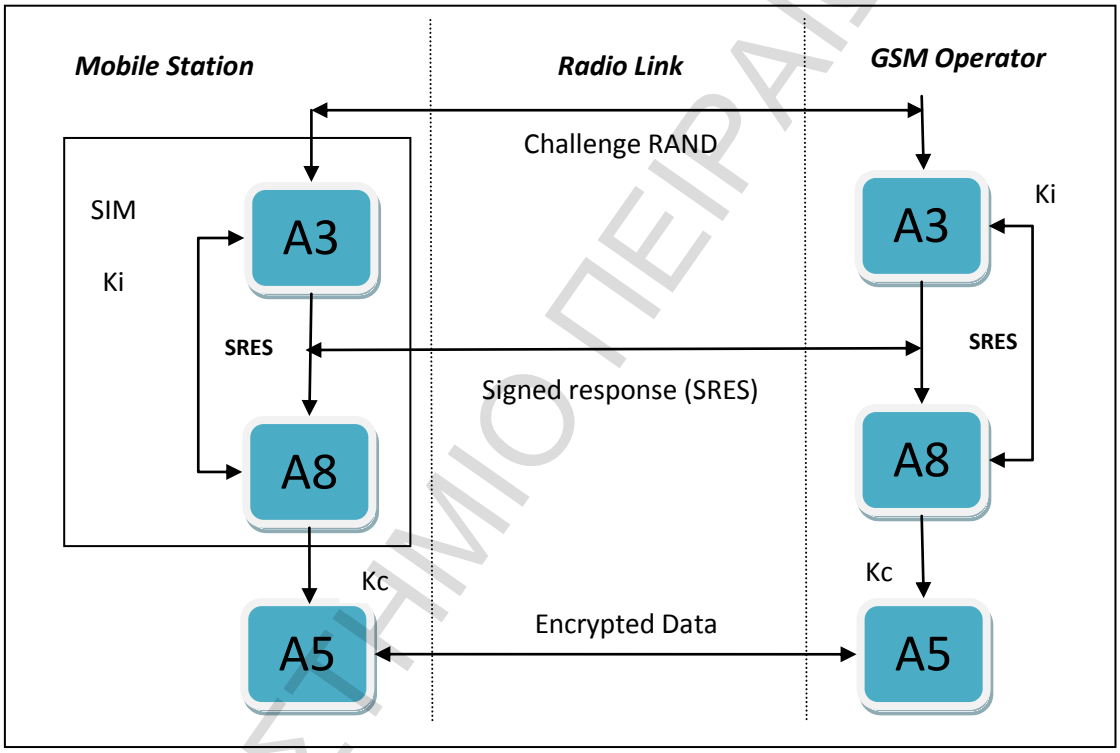

Figure 5: Authentication in GSM Network

3.2 UMTS Security

UMTS Security builds on the security of GSM. The proven GSM security features have inherited to UMTS, increasing the compatibility between the two protocols.

One of the main improved security mechanism is the mechanism of authentication in UMTS [3]. Unlike GSM, which has authentication of the user to the network only, UMTS uses mutual authentication which means the mobile user and the serving network authenticate each other. With this way, UMTS provides security against false base stations.

The steps of authentication are the following

1. The Mobile Station requests access to the network

2. The network receives the request and replies with a random value RAND and with an Authentication Token (AUTH). The AUTH contains a Message Authentication Code (MAC). The network sends the RAND to the Mobile Station
3. The Mobile Station calculates a new MAC called XMAC. It compared the XMAC and MAC. If they are equal the Mobile Station authenticates the network, otherwise it sends a failure message to the network.
4. The Mobile Station computes the SRES like the above step 3 of GSM Security. Once, SRES is computed, the Mobile Station sent it to the network.
5. The network compares the SRES with the XRES value calculated by itself. If the values are equal then the ME is authenticated to the UMTS network.

4 Information System

The Information System has the following architecture:

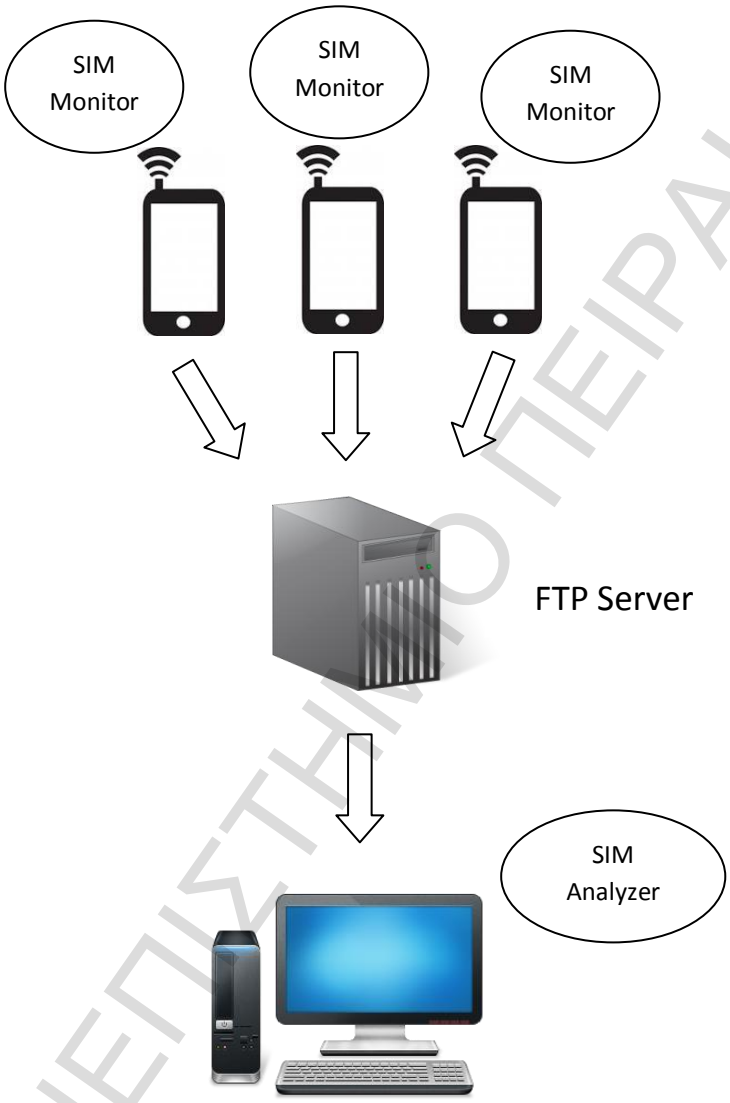

Figure 6: Architecture of Information System

A smart phone application - named **SIM Monitor** - is running in each smart phone. The application is developed for Android devices. Its purpose is to extract and record data at each user predefined time interval. The information related about the identity of subscriber, identity of network and security characteristics of Subscriber Identity Module (SIM).

The above data saved in the memory of smart phone. User can upload the data in the Secure **FTP server**.

The second most significant part of information system is a Windows Application, named **SIM Analyzer**. The SIM Analyzer gives the ability to user to download the data that are collected from smart phones and are saved in the SFTP server. The data are inserted in database of application so that user can extract useful results about security of mobile network. The extraction of results carried out with SQL queries in database of Desktop Application.

5 SIM Monitor

This chapter describes the operation and characteristics of SIM Monitor.

5.1 AT Commands

The extraction of security data from the Mobile Station based on AT commands. AT commands are instructions used to control a modem [10]. The group of commands is made of a set of shot text strings which combine together to form complete operational commands, for example dialing, terminating connections, changing parameters and extracting information of many sorts. The vast majority of modems use the Hayes commands. However, due to the large number of firmware and baseband devices, AT Commands are not supported completely in all devices. Furthermore, a baseband may support proprietary AT commands, available only for a specific device.

Every AT command line starts with “AT” or “at”. That’s why modem commands are called AT commands [4]. Many of the commands that are used to control wired dial-up modems, such as ATD (Dial), ATA (Answer). ATH (Hook control) and ATO (Return to online data state), are also supported by GSM/GPRS modems and mobile phones. However, GSM/GPRS modems and mobile phones support an AT command set that is specific to the GSM technology, which includes SMS-related commands like AT+CMGS (Send SMS message), AT+CMSS (Send SMS message from storage), AT+CMGL (List SMS messages) and AT+CMGR (Read SMS Messages).

The types of AT commands are: basic commands and extended commands.

Basic commands are AT commands that do not start with “+”. Some examples of basic commands are:

- ATD (Dial)
- ATA (Answer)
- ATH (Hook control) and
- ATO (Return to online data state)

Extended commands are AT commands that starts with “+”. Some examples of extended commands are:

- AT+CMGS (Send SMS message)
- AT+CMSS (Send SMS message from storage)
- AT+CMGL (List SMS messages)
- AT+CMGR (Read SMS messages)

The following tasks can be done using AT commands with a GSM/GPRS modem or mobile phone

- Get basic information about the mobile phone or GSM/GPRS modem.
    - AT+CGMI (Read the name of manufacturer)
    - AT+CGMM (Read the model number)
    - AT+CGSN (Read the IMEI)
    - AT+CGMR (Read the software version)
- Get basic information about the subscriber.
    - AT+CNUM (Read the MSISDN)

    - AT+CIMI (Read the International Mobile Subscriber Identity)
- Get the current status of the mobile phone or GSM/GPRS modem.
    - AT+CPAS (Read the activity status)
    - AT+CREG (Read the mobile network registration status)
    - AT+CSQ (Read radio signal strength)
    - AT+CBC (Read the battery charge level and battery charging status)
- Establish a data connection or voice connection to a remote modem (ATD, ATA)
- SMS
    - AT+CMGS / AT+CMSS (Send SMS messages)
    - AT+CMGR / AT+CMGL (Read SMS messages)
    - AT+CMGW (Write SMS messages)
    - AT+CMGD (Delete SMS messages)
    - AT+CNMI (Obtain notifications of newly received SMS messages)
- Check Phone Book Entries
    - AT+CBR (Read phone book entries)
    - AT+CPBW (Write phone book entries)
- Perform Security-related tasks
    - AT+CLCK (Open or close facility locks)
    - AT+CPWD (Change passwords)
- Control the presentation of results codes / error messages of AT commands.
    - AT+CMEE (Control whether to enable certain error messages)
    - AT+CMEE=1 (Enable to display in numeric format)
    - AT+CMEE=1 (Enable to display in verbose format)
- Get or change the configurations of the mobile phone or modem.
    - AT+COPS (Change the GSM Network)
    - AT+CBST (Change the bearer service type)
    - AT+CRLP (Change the radio link protocol parameters)
    - AT+CRLP (Change the SMS center address)
    - AT+CPMS (Change the storage of SMS messages)
- Save and restore configurations of the mobile phone or modem
    - AT+CSAS (Save settings related to SMS messaging)
    - AT+CRES (Restore settings related to SMS Messages)

The two following AT commands used in SIM Monitor in order to extract data related to SIM

- AT+CSIM (Generic SIM Access that sends commands to SIM card)
    - Command: +CSIM=<length>,<command>
    - Response:+ CSIM=<length>,<response>
    - The <length>field is the number of bytes the command consists of. The <command> field is populated with APDU commands that are sent to the SIM/USIM module. The <response> field is the data sent by the SIM/USIM module.
    - Examples
        - AT+CSIM=14,0, “A0A40000023F00” (Go to 3F00 directory)
        - AT+CSIM=14,0, “A0A40000027F20” (Go to 7F20 directory)
        - AT+CSIM=14,0, “A0A40000027F20” (Go to 7F20 directory)
        - AT+CSIM=10, “A0B0000009” (Go to 7F20 file)
- AT+CRSM (Restricted SIM Access)
    - Command:+CRSM=<command>[,<fileid>[,<P1>,<P2>,<P3>[,<data>[,<pathid>]]]]
    - Response: +CRSM: <sw1>,<sw2>[,<response>]

The <command> field is one of the following:

- 176 READ BINARY
- 178 READ RECORD
- 192 GET RESPONSE
- 214 UPDATE BINARY
- 220 UPDATE RECORD
- 242 STATUS
- 203 RETRIEVE DATA
- 219 SET DATA

- The <fileid> field is the integer of the file id. For example, the integer for file '6F08' is '28424'. The <P3> field is the number of bytes the response should have. If the <sw1> and <sw2> fields have values equal to "144" and"0" respectively, this means the command execution was successful.
- Examples
  - AT+CRSM=176,28448,0,0,9

5.2 Operation of SIM Monitor

The basic operation of SIM Monitor is a bash script. The basic script of smart phone sends a series of AT Commands to modem in order to extract important data from SIM card about security of Mobile Station and Mobile Network. The script is executed in each predefined time interval. The following figure explains the process, the modules that are participating and the information flow in SIM Monitor.

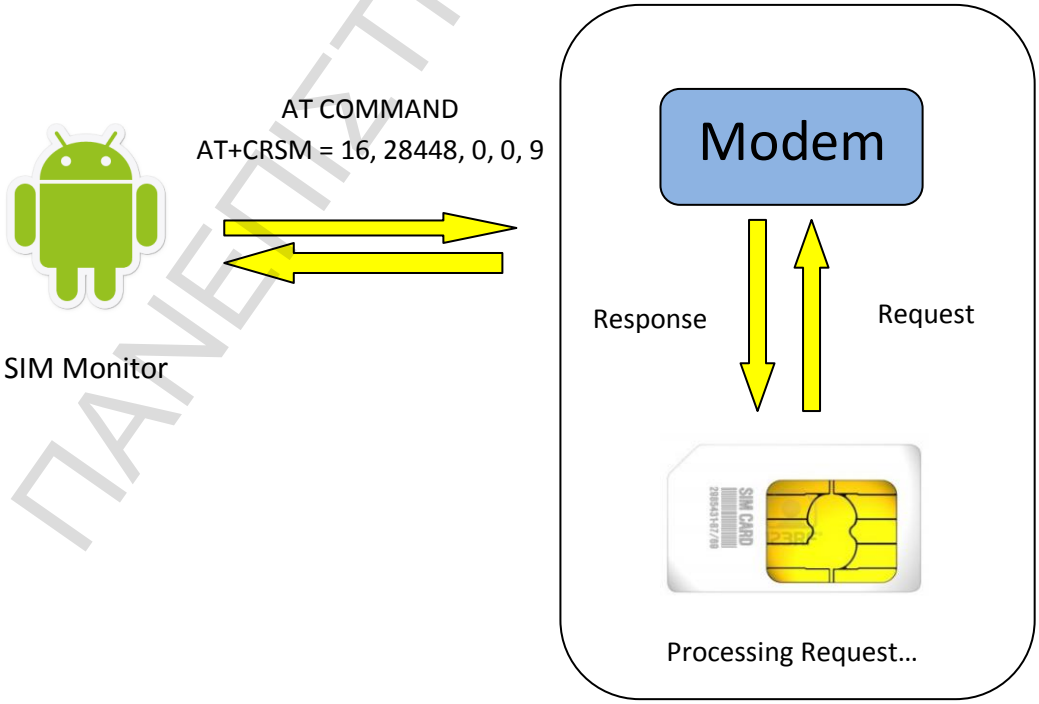

Figure 7: Process flow in a smart phone

The steps of the process in smart phone during SIM Monitor works are

1. The mobile station, specifically the modem, receives an AT Command. The AT Command is sent by the bash script that operates like daemon. The AT Command includes the file that will be read from the SIM/USIM card.
2. The modem performs a new response to the SIM/USIM card.
3. The command is received and processed by the SIM/USIM card in order to respond with the requested data. In this case, the data is the content of an EF file.
4. The generated response by SIM/USIM is forwarded to the modem. The value of the response is the value of the EF file.
5. The responses of the AT Commands are parsed from the SIM Monitor and saved in a file. The file is saved in the internal memory of smart phone.

The SIM Monitor follows the above procedure to extract important information security of the mobile network. It uses the corresponding AT command to access the value of the following variables: IMSI, Ciphering Mode, Kc, KcGPRS, CK, IK, TMSI, TMSI TIME, LAI, PTMSI, PTMSI SIGNATURE VALUE, RAI, RAUS and THRESHOLD. The data are saved temporarily in the internal memory of smart phone and the user can upload them in an SFTP Server.

Also, SIM Monitor offers the following options:

1. The user can change the time interval of script.
2. The user can upload the data to an SFTP Server.
3. The user can press a button and see the results of the script that executed that time.

6 SIM Analyzer

This chapter describes the operation and characteristics of SIM Analyzer.

6.1 Introduction

The main aim of SIM Analyzer is to extract results and some correlations from data that are collected from Smart phone application and are saved in SFTP Server. The data are inserted in database of application. The extraction of results carried out with SQL queries in database of SIM Analyzer.

The queries that are answered from the SIM Analyzer were

1. Identify the Network Operator?
2. The subscriber use SIM or USIM?
3. How often authentication is performed?
4. When a key changes the temporary identities change and vice versa?
5. When the user changes LAI or RAI, authentication is performed?
6. A key is reused?
7. A temporary identity is reused?
8. After how many calls-connections a key changes?
9. When the telephone is switched off and on the keys, identities change?
10. When a call or session takes place encryption is on or off?

6.2 Description

This section of thesis is an analytical description of the implemented SIM Analyzer.

The main form of SIM Analyzer is the following:

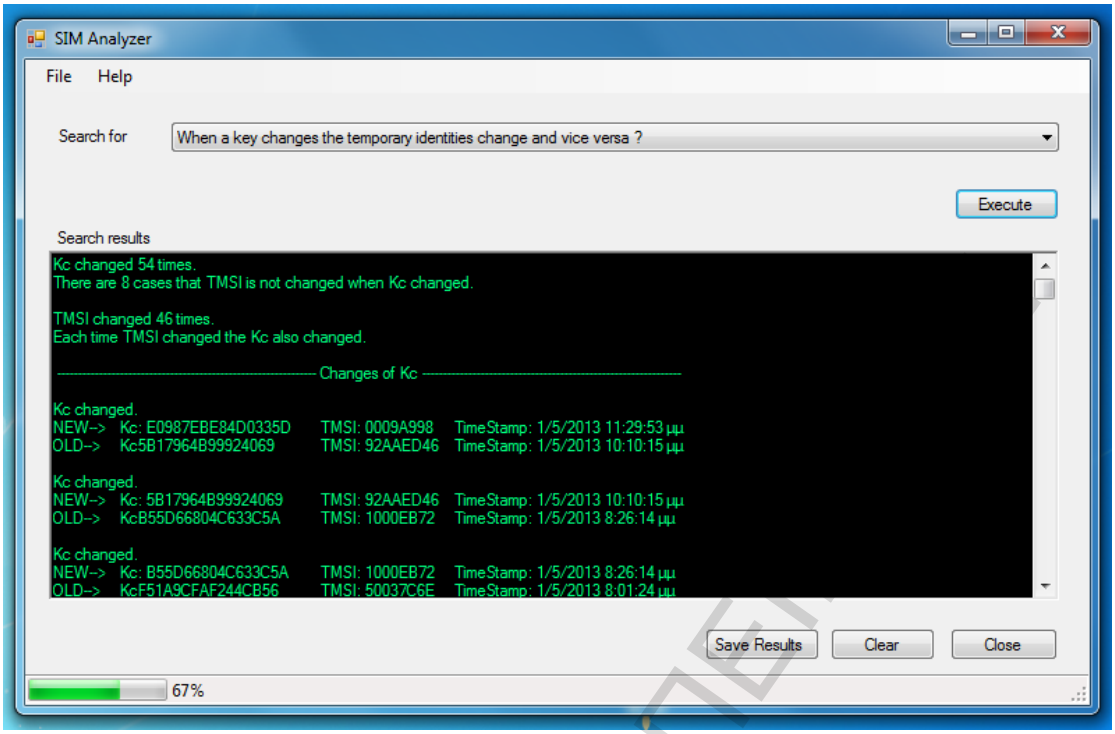

Figure 8: Main Form of SIM Analyzer

At the **top** of the application, there is a menu that provides some options to the user. Pressing the menu item “File”, the user can see the following menu items:

- **Download from the Server**
  This task downloads the data from the SFTP server that are collected from the various smart phones. The data are saved in a temporary local folder, called Temp.
- **Insert to the Database**
  This task inserts the above data in the database of SIM Analyzer.

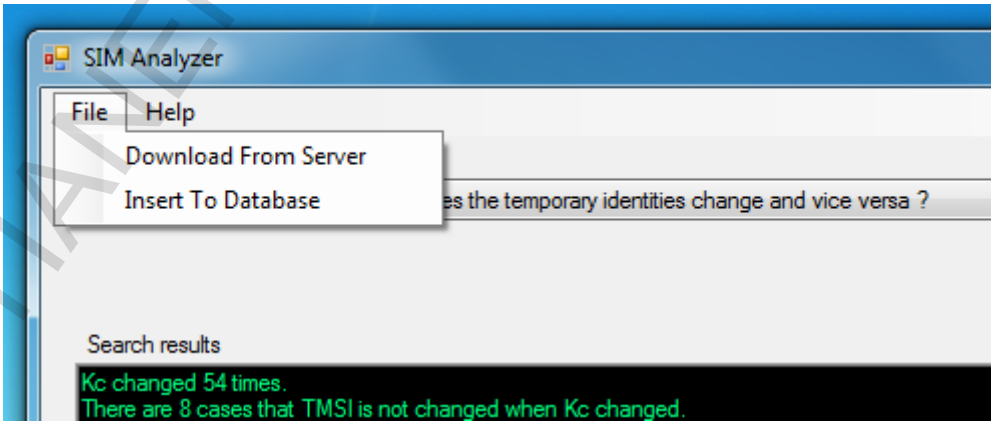

Figure 9: Menu options in SIM Analyzer

The **center** part of application consists from a drop down list control. The user can choose one of the queries that he wants to ask database.

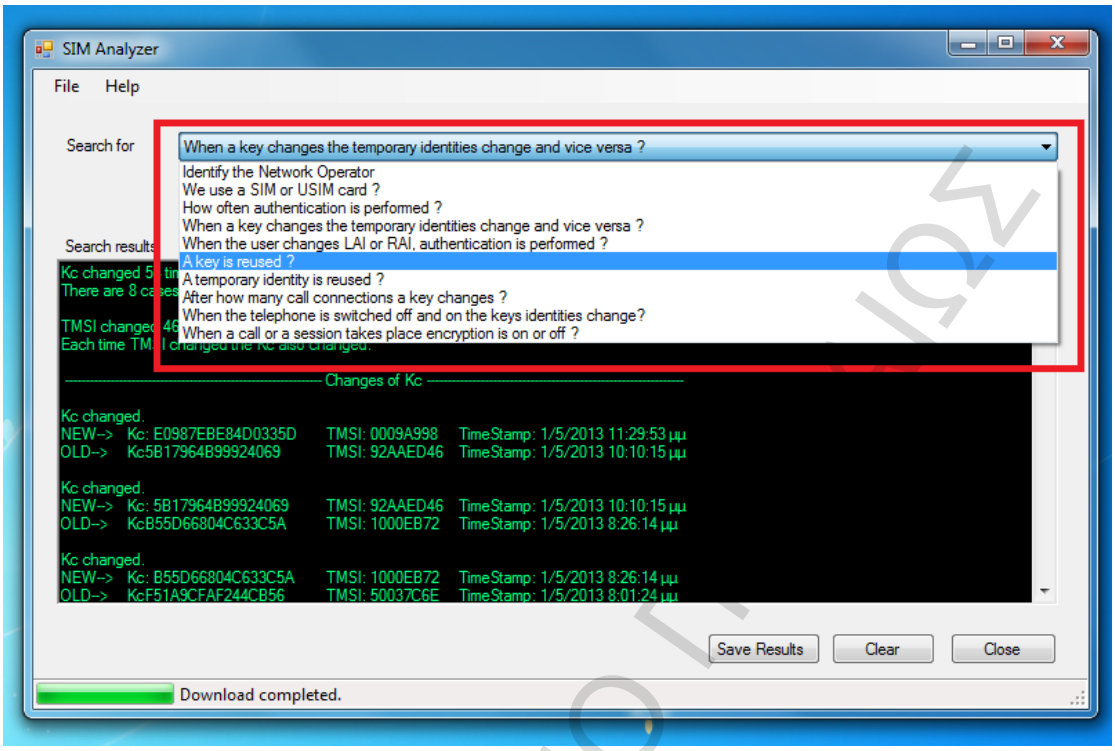

Figure 10: List of Queries in SIM Analyzer

After choosing the query, the user must press the button “Execute” so that the selected query extract results from the database.

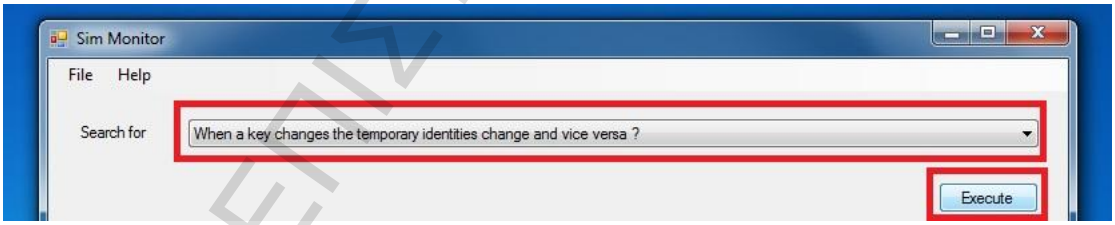

Figure 11: Execution of Selected Query

The results appeared to the black screen.

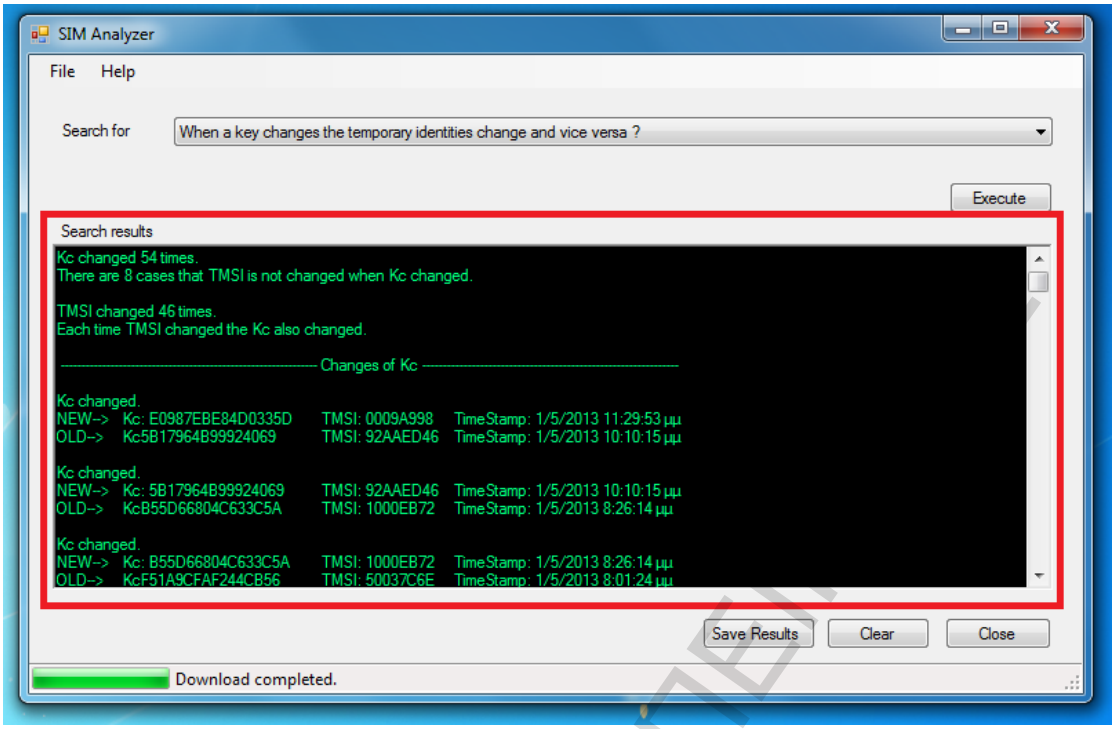

Figure 12: Results Area in SIM Monitor

At the **bottom** of the application, there are three buttons

- Save Results Button: The user can save the results in a file.
- Clear: The user can clear the black screen of the results.
- Close: The user can close the application.

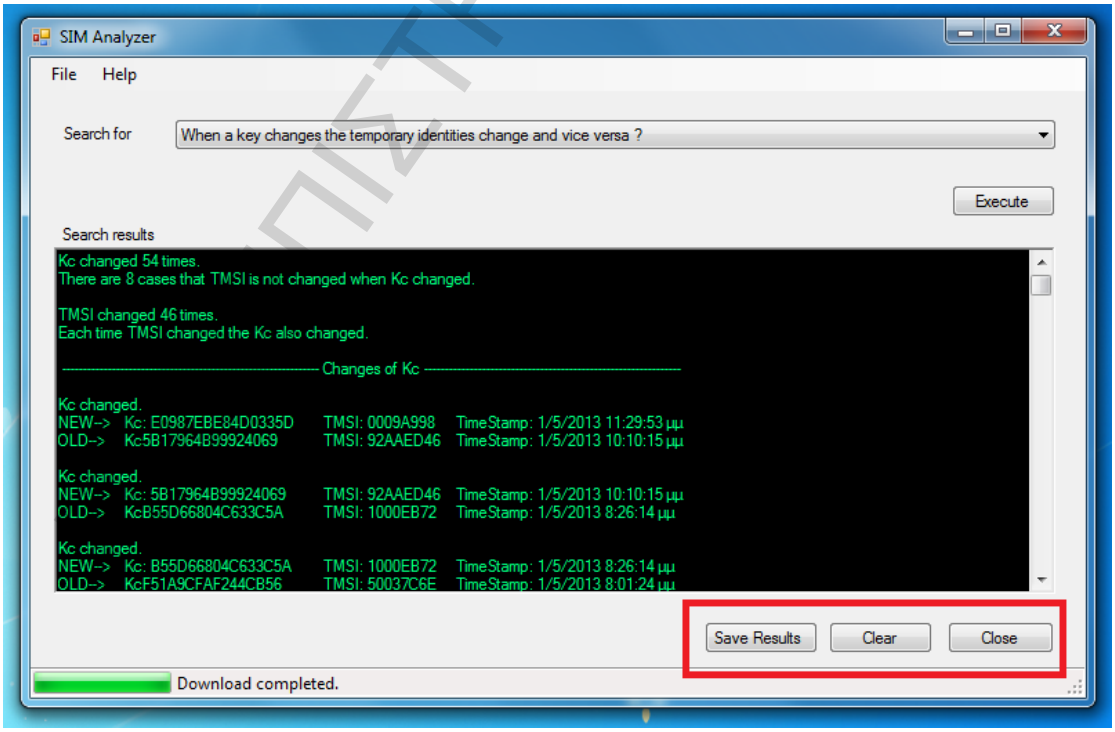

Figure 13: Bottom Area of SIM Monitor

The next section describes the results from the each query of SIM Analyzer. For each query, a screenshot of results is appeared. The data in database are almost 4000 records. They came from a Samsung Android smart phone. The dates of monitoring are between 30 April 2013 and 01 May 2013.

Query 1: Identify the Network Operator

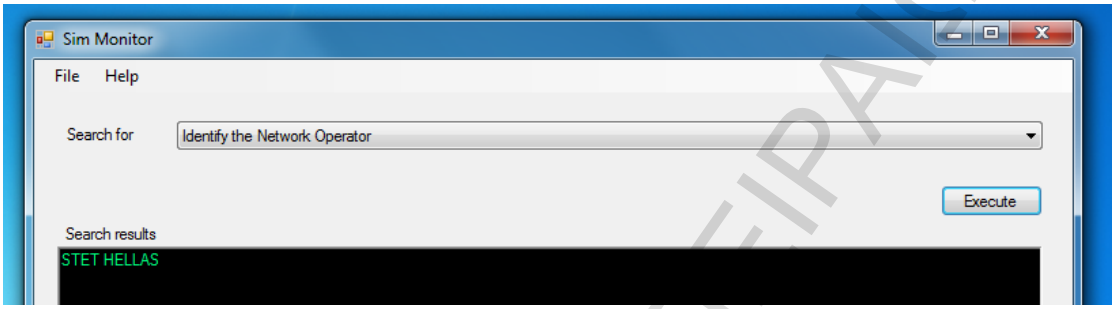

Figure 14: Results of "Identify the Network Operator"

This query returns the names of providers that inserted records in database have.

Query 2: The subscriber use SIM or USIM?

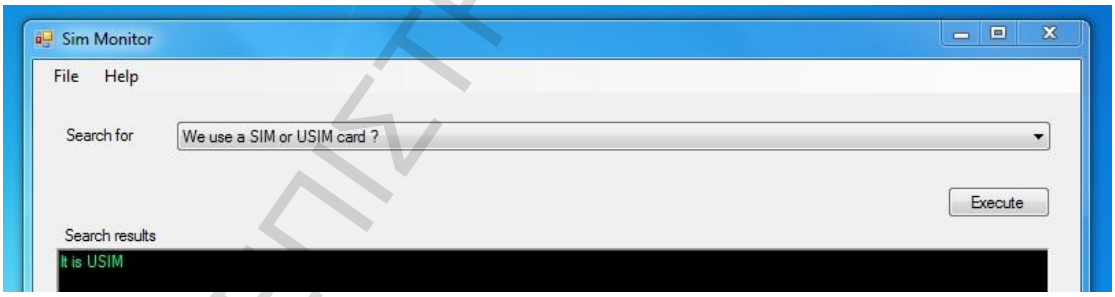

Figure 15: Results of "The subscriber use SIM or USIM?"

This query returns what kind of SIM used in the smart phones in which extract the data. The possible values of the types are SIM and USIM.

Query 3: How often authentication is performed?

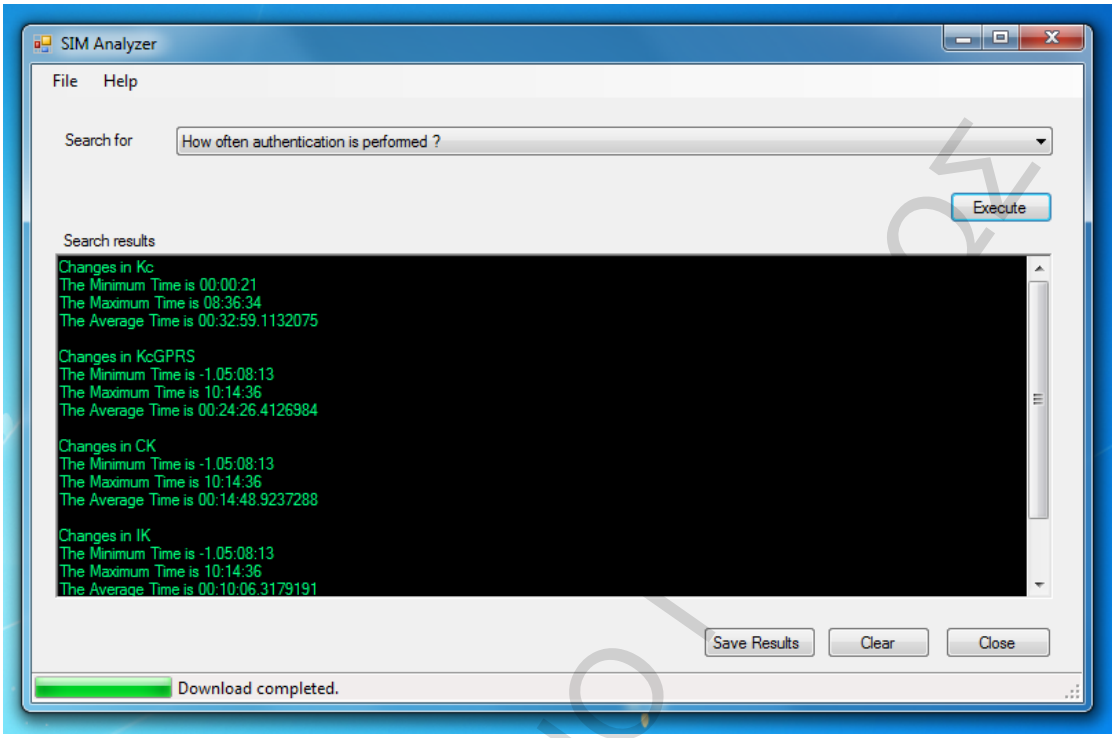

Figure 16: Results of "How often authentication is performed?"

This query returns the minimum, the maximum and the average time of changes for each key. The keys of our research are Kc, KcGPRS, CK and IK. In the above example, we noticed that the Kc changes its value each 32 minutes and 59 seconds at average time. The minimum and the maximum time interval that the value of KcGPRS changed were 21 seconds and 8 hours, 36 minutes and 34 seconds, respectively.

Query 4: When a key changes the temporary identities change and vice versa?

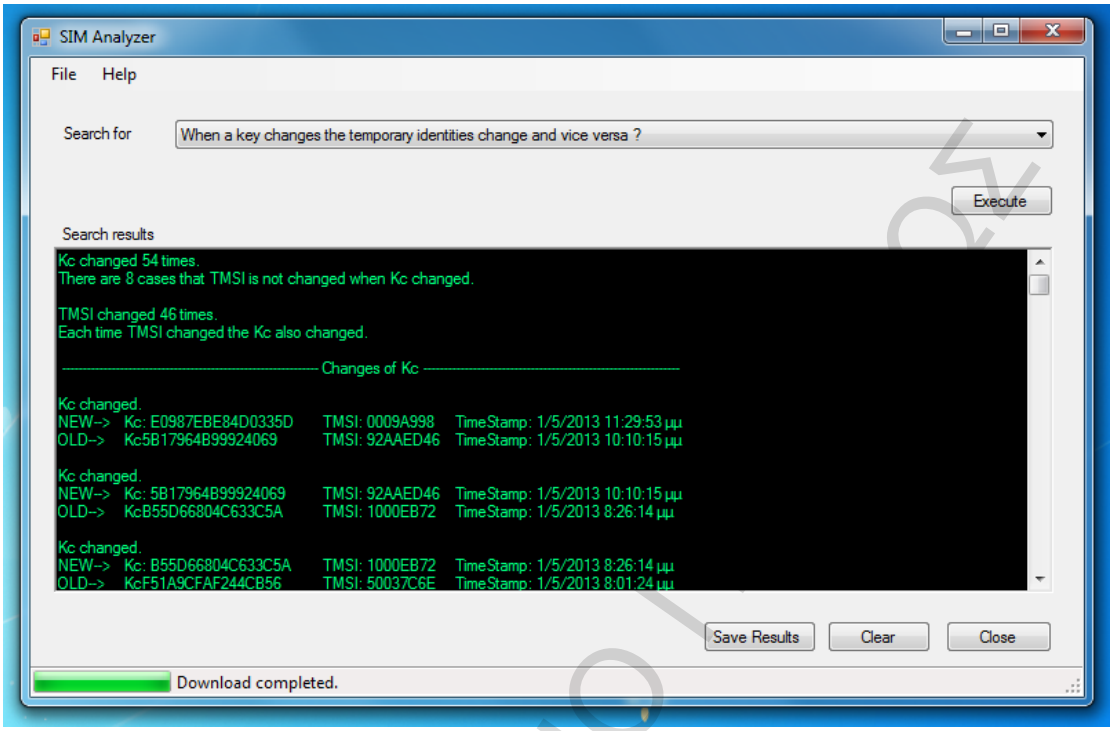

Figure 17: Results of "When a key changes the temporary identities change and vice versa?"

The query returns the following information about Kc

- The number of time that the value of Kc changed.
- The number of times that the value of TMSI changed, when the value of Kc changed.

Also, the query returns the following information about TMSI

- The number of time that the value of TMSI changed.
- The number of times that the value of Kc changed, when the value of TMSI changed.

Furthermore, the query returns all the changes of Kc. It is appeared the old and the new value of Kc, TMSI and the Time Stamp each time the value of Kc changes. The user of SIM Analyzer can observe the value of Keys in each change of Kc.

Finally, the query returns all the changes of TMSI. It is appeared the old and the new value of TMSI, Kc and the Time Stamp each time the value of TMSI changes. The user of SIM Analyzer can observe the value of Keys in each change of TMSI.

Query 5: When the user changes LAI or RAI, authentication is performed?

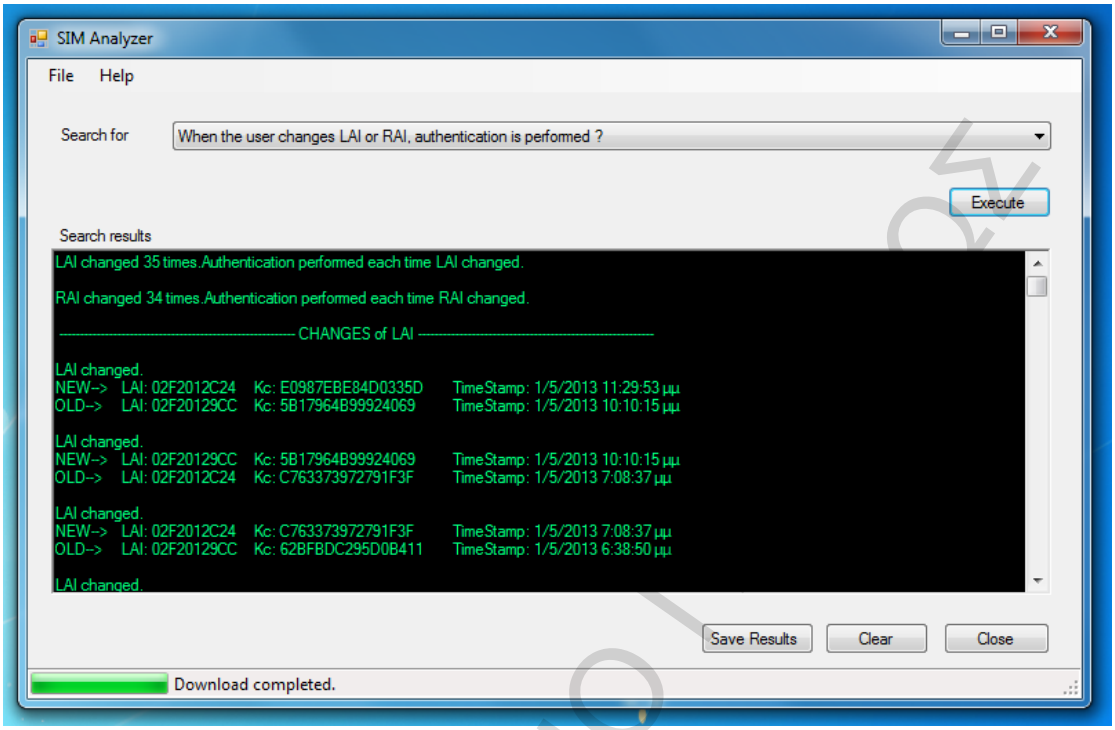

Figure 18: Result of "When the user changes LAI or RAI, authentication is performed?"

This query returns the number of times that the LAI changed and answers if the value of Kc changed during the change of LAI. Similarly, the query returns the number of times that the RAI changed and answers if the value of Kc changed during the change of RAI.

Also, the user of SIM Analyzer can observe all the changes of LAI and he can see the old and new value of LAI, Kc and Time Stamp for each change of LAI. Similarly, the user of SIM Analyzer can observe all the changes of RAI and he can see the old and new value of RAI, Kc and Time Stamp for each change of RAI.

Query 6: A key is reused?

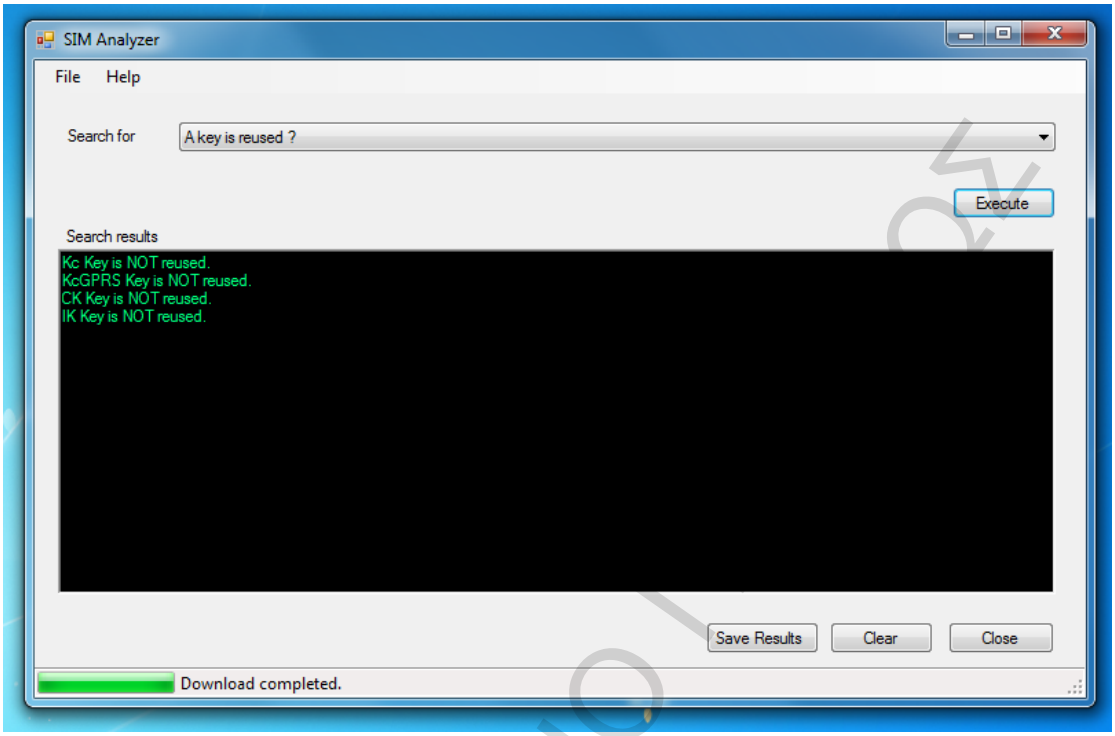

Figure 19: Results of "A key is reused?"

This query returns if the SIM reuse each one of the security keys (Kc, KcGPRS, CK, IK). It was expected that the mobile network will not reuse any of the security key.

Query 7: A temporary identity is reused?

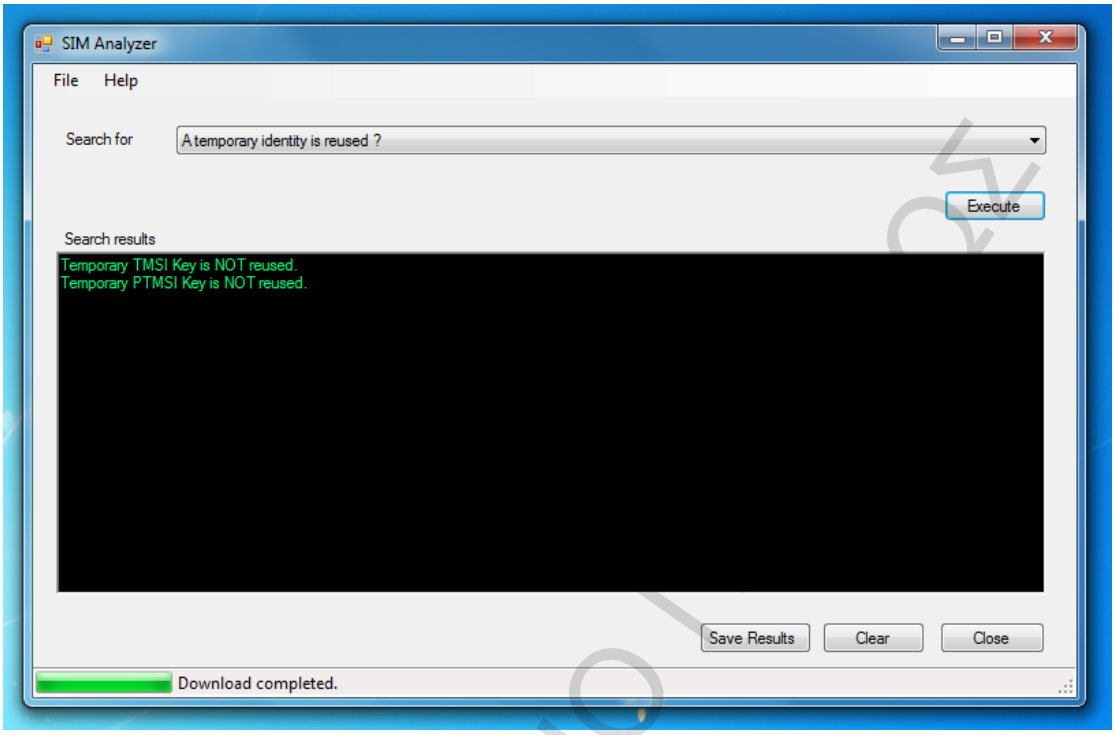

Figure 20: Results of "A temporary identity is reused?"

Similar to query 6, this query returns if the SIM reuse each one of the temporary security keys (TMSI, PTMSI). It was expected that the mobile network will not reuse any of the temporary security key.

Query 8: After how many calls-connections a key changes?

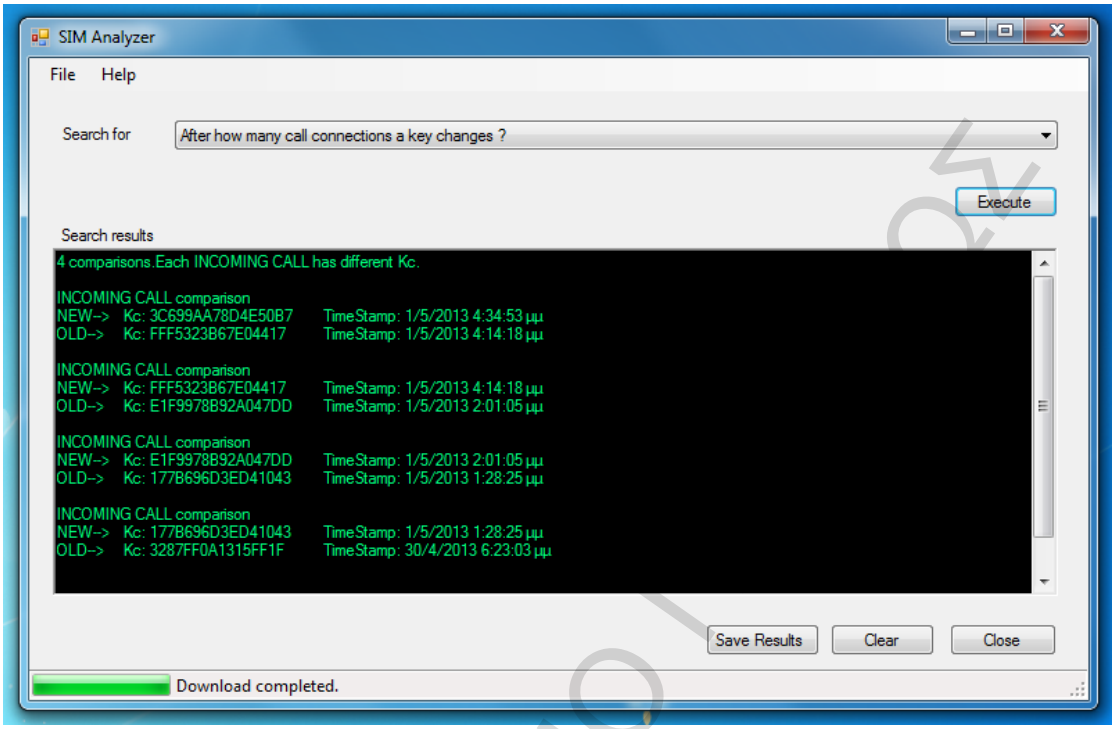

Figure 21: Results of "After how many calls-connections a key changes?"

This query examines if the value of Kc is similar or not in each calls connection. If it is similar it returns after how many call connections a key changed. However, it was observed that the value of Kc changed in each incoming call in our experiment.

Query 9: When the telephone is switched off and on the keys, identities change?

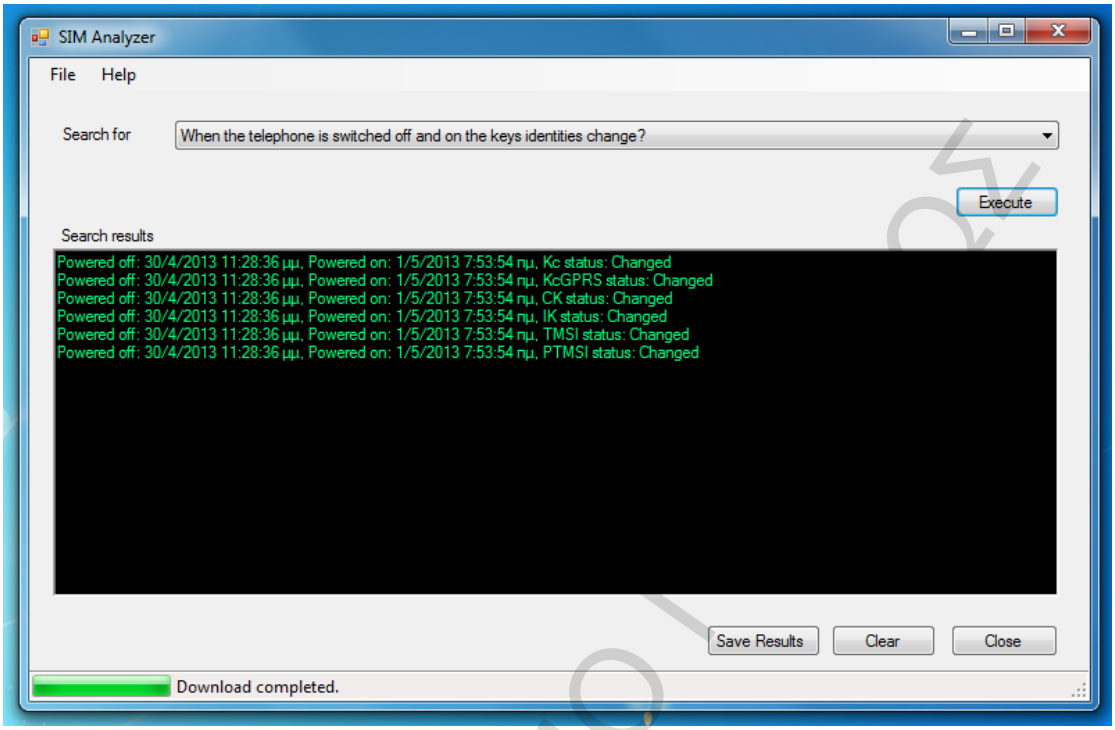

Figure 22: Results of "When the telephone is switched off and on the keys, identities change?"

The query returns the changes of keys (Kc, KcGPRS, CK, IK, TMSI and PTMIS) when the telephone is switched off and on. The above figure records one switch off and on. The user can observe the time that the phone is switched off, the time that the phone is switched on and if the value of the corresponding key is changed.

Query 10: When a call or session takes place encryption is on or off?

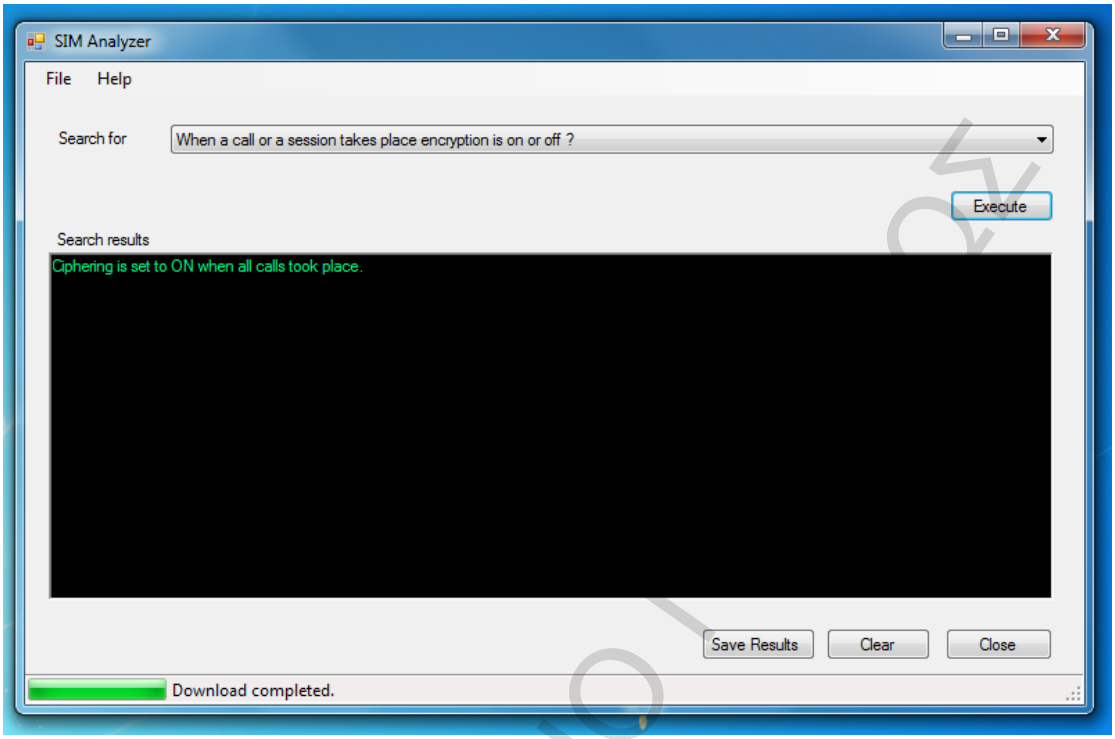

Figure 23: Results of "When a call or a session takes place encryption is on or off"

This query answers if there is encryption in an Incoming call or Outgoing call. According to the results of query, it was expected that during a call the encryption is ON.

6.4 Design and implementation

6.4.1 Architecture of SIM Analyzer

The implementation of SIM Analyzer is based on architecture of the above picture.

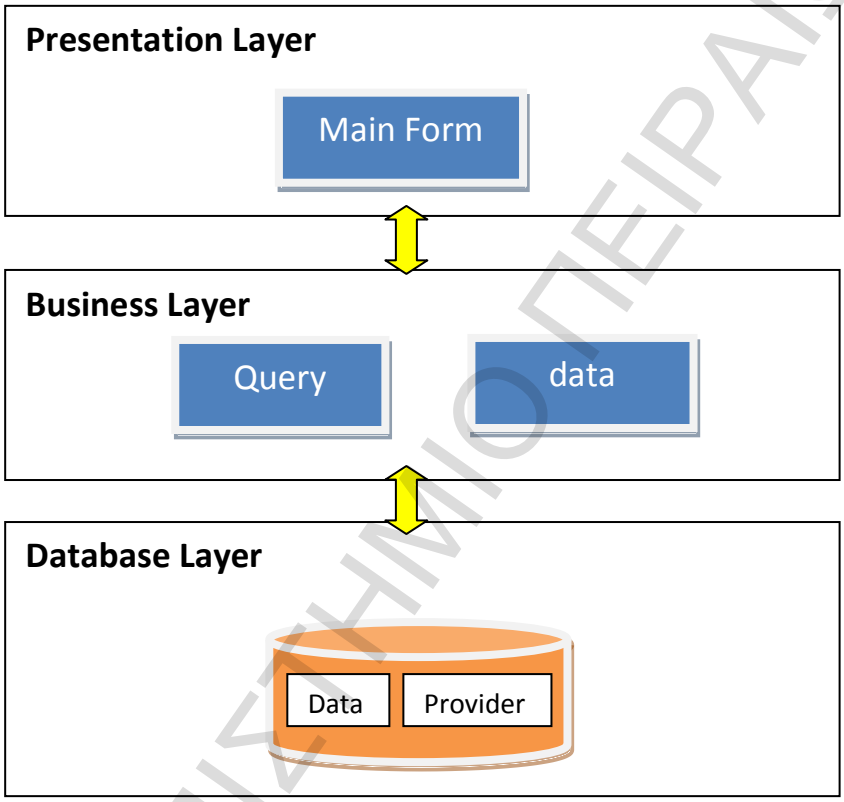

Figure 24: Architecture of SIM Analyzer

For the implementation of SIM Analyzer, the following tools are used.

- Visual Studio 2010 IDE
  The UI of SIM Analyzer and the business layer is developed at Visual Studio.
- MySQL version 5.6.
  The SIM Analyzer uses a MySQL Database. The MySQL Connection .NET version 6.6.5 is appropriate, so that SIM Analyzer can connect to MySQL database.

There are two tables in database.

- **Data**: is the basic table of database. It contains almost all the information of database. The columns of this table is

- **Id** is the unique number of each record in this table. It is primary key and it is increased by 1, each time that a new line is inserted.
- **Type** is the type of value that populates a specific row. The different types are: Ciphering Mode, Kc, KcGPRS, CK, IK, TMSI, TMSI TIME, LAI, PTMSI, PTMSI Signature Value, RAI, RAUS, THRESHOLD.
- **CellId** is the cell tower id and it is helpful for the security assessment of each tower individually.
- **EventType** is the type of status that smart phone is. The different types are: PERIODIC, INCOMING_CALL, SCREEN_ON, SCREEN_OFF, POWER_ON.
- **NetworkType** is the type of network that the smart phone is using. The different types are: UMTS, EDGE.
- **GpsLongitude** is the number that indicates how far north or south of the equator a place is located [8].
- **GpsLatitude** is the number that indicates how far east or west of the prime meridian a place is located. [8]
- **IsRoaming** is a Boolean value that indicates if or not the user of smart phone use network from another country.
- **Timestamp** is the timestamp of the current value. The structure is Year-Month-Day Hours:Minutes:Seconds Example is 2013-05-01 23:34:04.

- **Providers**
  - **Id** is the unique number of each provider. It is also the primary key of the table.
  - **Description** is the name of the provider.

It follows a small description of each tool that is used in implementation.

6.4.2 Visual Studio 2010

Visual Studio2010 is a complete set of development tools for building ASP.NET Web Applications, XML Web Services, desktop applications, and mobile applications [9]. Visual Basic, Visual C++ and Visual J# all use the same integrated development environment (IDE), which allows them to share tools and facilitates in the creation of mixed-language solution.

Windows Forms is for creating Microsoft Windows Application on the .NET Framework. This framework provides a clear, object-oriented, extensible set of classes that enables you to develop rich Windows applications. Additionally, Windows Forms can act as the local user interface in a multi-tier distributed solution.

.Net Framework is a multi-language environment for building environment, deploying and running XML Web Services and applications. It consists from these following parts:

- Common Language Runtime. The runtime has a role in both a component's runtime and development time experiences. While the component is running, the runtime is

responsible for managing memory allocation, starting up and stopping threads and processes, and processing, and enforcing security policy.

- Unified programming classes. It provides to developers a unified, object-oriented, hierarchical and extensible set of class libraries. It creates a common set of APIS across all programming languages; the common language runtime enables cross-language inheritance, error handling, and debugging.

6.4.3 MYSQL

MySQL is one of the most popular open source databases. It provides cost-effective delivery of reliable, high-performance and Scalable Web-Based and embedded database applications [9]. During implementation of the SIM Analyzer, MYSQL Workbench tool is used. It is a unified visual tool for database architects, developers and DBAs. It enables them to design, model and generate databases. It includes everything a data modeler needs for creating complex ER models, forward and reverse engineering. Additionally, it delivers key features for performing difficult change management and documentation tasks. Furthermore, it enables developers to create, execute and optimize SQL queries. The SQL Editor provides color syntax highlighting, reuse of SQL snippets, and execution history of SQL. Finally, the Object Browser provides instant access to database schema and objects.

7 Extended Work

As next step of this work, it will be to add more queries in SIM Analyzer. Some of them could be the following:

- How many of the operators are owned by Greek companies?
- How many of the operators are owned by foreign companies?
- How is the percentage of each type of SIM in general?
- How is the percentage or each type of SIM in each provider?
- How many changes of Key (Kc, KcGPRS, CK, IK) there are in time interval of 1 hour?
- How many changes of temporary Key (PTMSI, TMSI) there are in time interval of 1 hour?

Also, SIM Analyzer could give the ability to the user to extract results in XML format. The XML presentation of results enables the user to integrate the results to other systems or tools. So with this way, a quantitative and qualitative analysis of results of the queries would be possible and it could give more detailed correlations between data.

8 Conclusions

In this Master Thesis, we have presented an Information system that its aim is to monitor and analyze the security characteristics of a mobile network. It consists from two main applications, the SIM Monitor and the SIM Analyzer. SIM Monitor runs in Android Smartphone and its aim to collect data from the SIM or USIM card. The data related to security of mobile network like Keys, Temporary Keys and their correlations with current geographical position of mobile station. The SIM Analyzer takes the collection of data and extracts useful results about security of mobile network.

The analysis of the results shows that advanced security of mobile networks. More specifically, the results were

1. The value of Kc changes often.
2. When the value of Kc changes, the value of TMSI changes and vice versa.
3. Each time the user changes LAI or RAI, the value of Kc changes.
4. The value of Kc is not reused.
5. The value of TMSI is not reused.
6. The value of Kc changes in each INCOMING or OUTCOMING call.
7. The value of Kc changes in each switch off and on of mobile station.
8. All sessions of call were encrypted.

Last but not least, there are a plenty of queries that can be added to SIM Analyzer that will enhance the research in the area of security of mobile network.

9 References

1. **Sheng He Ruhr-University of Bochum,** SIM Card Security, http://www.emsec.rub.de/media/crypto/attachments/files/2011/04/sim_card_security.pdf
2. **Stellenbosch University,** Authentication and encryption, http://web.ee.sun.ac.za/~gshmaritz/gsmfordummies/encryption.shtml
3. **School of Computer Science And Statistics**, GSM and UMTS Security, http://ntrg.cs.tcd.ie/undergrad/4ba2.05/group7/
4. **European Telecommunication Standards Institute**, Digital cellular telecommunication system (Phase 2+); Specification of the Subscriber Identity Module
5. **4gltemall**, What is GSM, EDGE, GPRS, UMTS, 3G, HSDPA, HSDPA, HSUPA, LTE, http://www.4gltemall.com/blog/what-is-gsm-edge-gprs-umts-3g-hsdpa-hsupa-lte/
6. **Difference between Similar Terms and Objects**, Difference between GSM and UMTS, http://www.differencebetween.net/technology/difference-between-gsm-and-umts/
7. **Microsoft Developer Network,** Introducing to Visual Studio, http://msdn.microsoft.com/en-us/library/fx6bk1f4(v=vs.80).aspx
8. **Microsoft Developer Network,** About latitude and longitude, http://msdn.microsoft.com/en-us/library/aa578799.aspx
9. **MYSQL,** About MSQL, http://www.mysql.com/
10. **Developers Home,** AT Commands, http://www.developershome.com/sms/atCommandsIntro.asp
11. **Yahoo**, Difference between SIM and USIM card, http://answers.yahoo.com/question/index?qid=20070328135302AAqf6d8
12. **etutorials**, Overview of GPRS, http://etutorials.org/Mobile+devices/gprs+mobile+internet/Chapter+3+Overview+of+GPRS/Mobility/
13. **Wikipedia**, Subscriber Identity Module, http://en.wikipedia.org/wiki/SIM_card
14. **Wikipedia,** Universal Subscriber Identity Module, http://en.wikipedia.org/wiki/Universal_Subscriber_Identity_Module#USIM
15. **Wikipedia**, GSM**,** http://en.wikipedia.org/wiki/GSM
16. **Wikipedia**, UMTS, http://en.wikipedia.org/wiki/Universal_Mobile_Telecommunications_System
17. **Wikipedia,** General Packet Radio Service, http://en.wikipedia.org/wiki/General_Packet_Radio_Service
18. **Wikipedia,** Time Division multiple access, http://en.wikipedia.org/wiki/Time_division_multiple_access