USER'S

MANUAL

SymPA v 1.0

University of Málaga, Spain

November, 2008

Technical report ITI 07-2.

Authors: Almudena Díaz Zayas
             Pedro Merino Gómez

Revision Sheet

Release No.	Date	Revision Description
Rev. 0	11/09/07	First Release
Rev. 1	17/10/07	Bug fixed in figure 10
Rev. 2	12/10/2007	New release

USER'S MANUAL

TABLE OF CONTENTS

1.0   GENERAL INFORMATION

1.0   GENERAL INFORMATION

1.1   System Overview

SymPA is a protocol analyzer for mobile phones that allows all the incoming TCP/IP traffic to be captured without interfering with the normal performance of the terminal. The main design goals for this tool have been the following:

- To capture all incoming IP packets, while avoiding information overload.
- To perform efficient resource management, according to constraints on power processing and battery life of mobile devices.
- To include basic functions for network management such as ping, PDP (Packet Data Protocol) context info etc.
- To provide interfaces for processing captured information and exporting it to other environments.
- Analysis of security problems in mobile devices.
- Debugging of network protocols over cellular networks.
- Debugging of new protocols for new mobile services.
- Detection of bugs in network protocol implementations for mobile devices.
- Detection of irregular behavior of traditional protocols in mobile environments.

1.2   Points of Contact

www.lcc.uma.es/~pedro/mobile

1.3   Organization of the Manual

This document provides a user's guide for SymPA. It describes SymPA installation, basic usage and configuration.

2.0   SYSTEM SUMMARY

2.0 SYSTEM SUMMARY

SymPA mobile application enables traffic analysis and monitoring of mobile devices in real operating conditions. With this tool it is possible to sniff all of the IP traffic that other applications running on a mobile phone receive from GPRS/UMTS connections. This makes SymPA particularly suitable for studying the end-to-end performance of IP based protocols and for mobile peer-to-peer scenarios. In addition, the application provides useful information related to radio parameters and the state of the mobile device, which can be used to detect the cause of transmission problems.

From our point of view it is crucial to provide developers with tools similar to those used for local area networks such as ping, tracert, netstat, sniffers,…
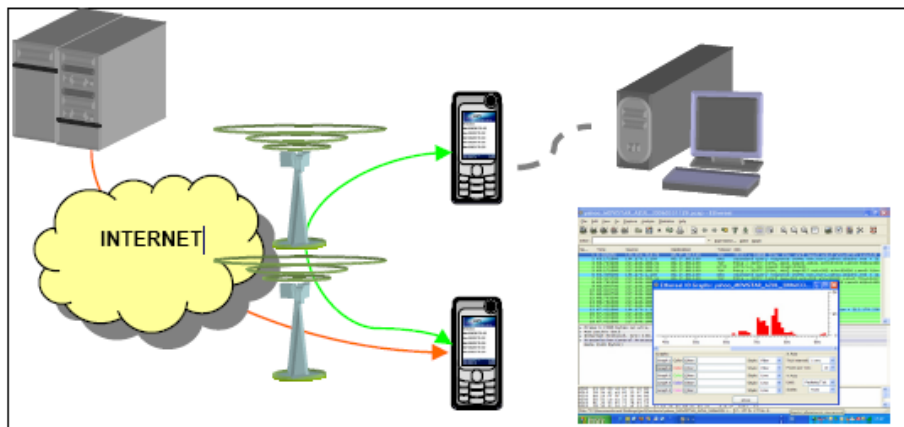

Figure 1. SymPA working diagram

2.1 Installation Guide

This release has been tested on Serie 60 devices with Symbian 9.x. Symbian 9.x tool version is now available but it needs to be signed. The following capabilities are necessary:
WRITEDEVICEDATA, NETWORKSERVICES, READDEVICEDATA AND NETWORKCONTROL.

For more information about the certificate you need to sign the application please visit www.symbiansigned.com

2.1.1 Installing SymPA on a Series 60 Smartphone using the Application Manager of the PC Suite

1. In the PC Suite Menu click on the "Install applications" option.
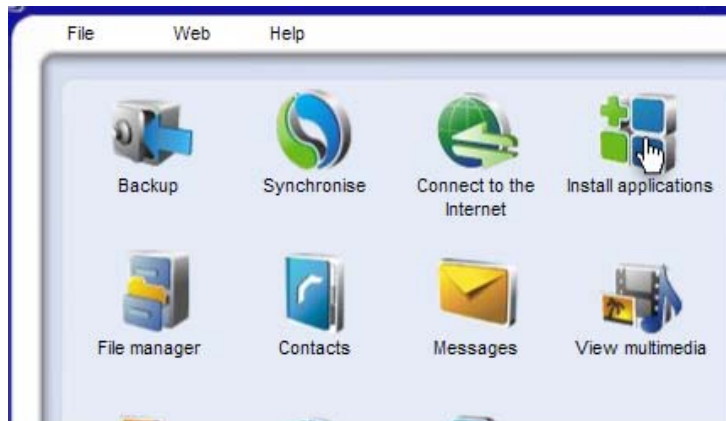

Figure 2. PC Suite Installation. Step 1

2. In the Applications installer on the left side, you can browse from "my computer" and select the .SIS file you wish to install.
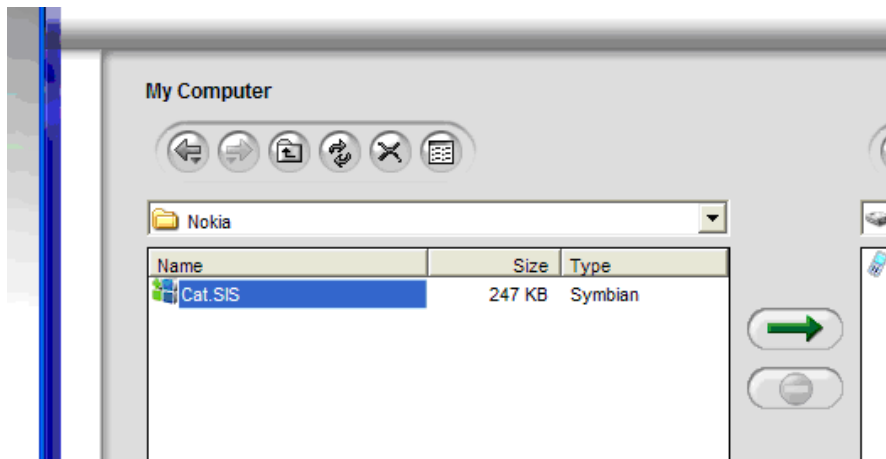

Figure 3. PC Suite Installation. Step 2

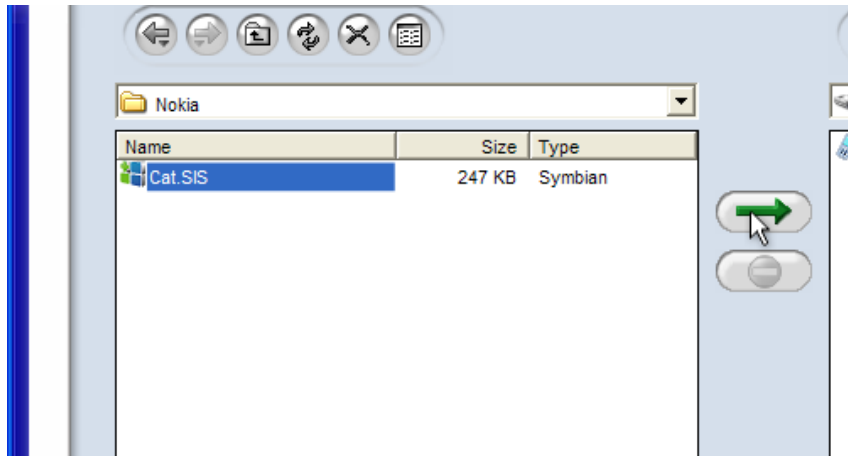3. Next click on the arrow pointing to the right

Figure 4. PC Suite Installation. Step 3

4. The application will be transferred to the mobile device and the installation will begin on the mobile phone.
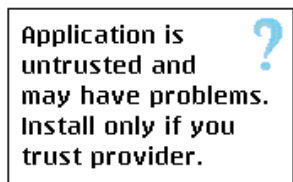

Figure 5. PC Suite Installation. Step 4

2.1.2 Installing SymPA via Infrared or Bluetooth

The installation file can be transferred to the mobile device via Infrared or Bluetooth. The .SIS file will be stored in the "Inbox" as a message and when the message is opened the installation starts.

2.1.3 Installing SymPA in the terminal

Figure 6. Terminal installation. Step 1
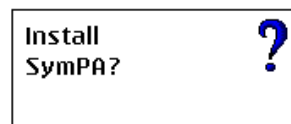
Figure 7. Terminal installation. Step 2

Figure 8. Terminal installation. Step 3

Figure 9. Terminal installation. Step 4

It is very important to install the application in the phone memory!!!

3.0   GETTING STARTED

3.0 GETTING STARTED

In this section menus available for using the application are described.

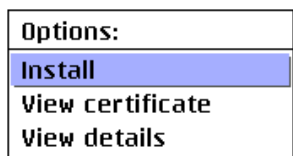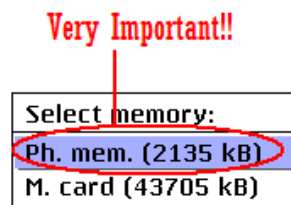## 3.1 System Menu

In the initial view of the application, at the top, cell information is shown. This information is updated every second. The information available is the following:

- **RAT (Radio Access Technologie)**
  Network Modes
  - o 0   Unknown
  - o 1   Unregistered
  - o 2   Gsm
  - o 3   Amps
  - o 4   Cdma95
  - o 5   Cdma2000
  - o 6   Wcdma
  - o 9   HDSPA **(New)**

Figure 10. Initial view

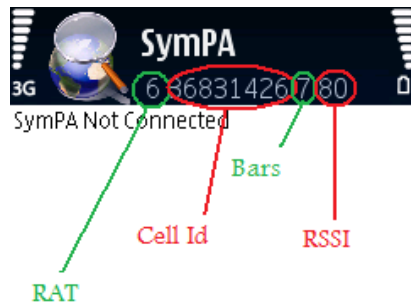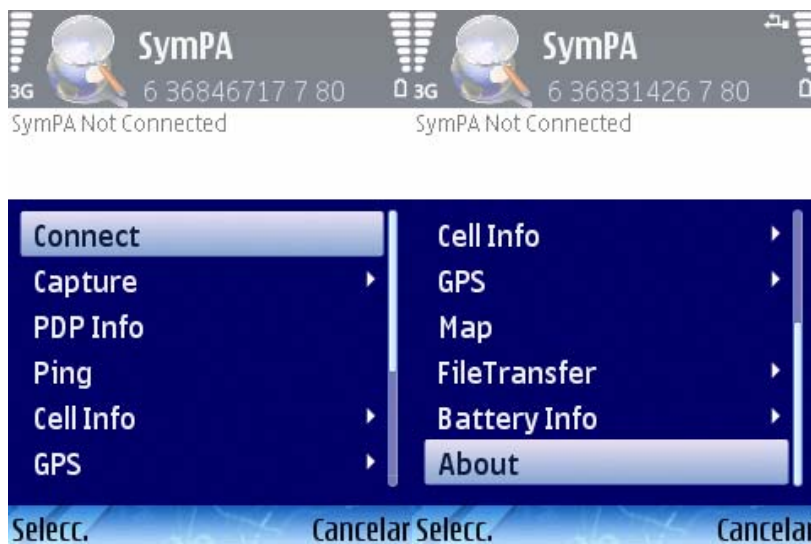Figure 11. Initial Menu

- **Cell Id**
    Cell Global Identifier

- **RSSI (- dBm)**
    Radio Signal Strength Indicator. Signal strength

- **Bars**
    Signal bars phone displays

3.1.0 Checking Connectivity (New)

Internet connectivity may be verified by establishing a TCP connection to any mobile or fixed device on the Internet. IP address associated to the connection is also provided.
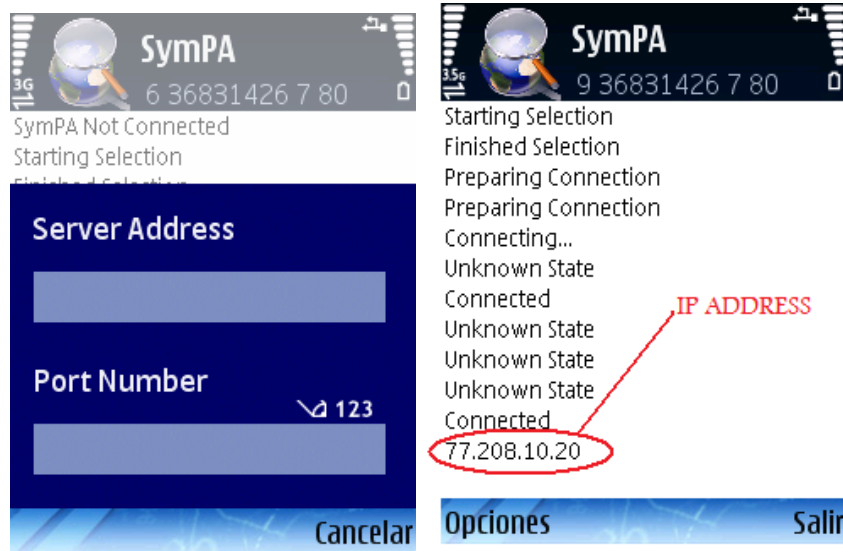
Figure 12. Checking connectivity

3.1.1 Capture

When SymPA is in capture mode, all IP packets reaching the mobile devices from data connections[1] are saved in a file in raw format. SymPA runs in the background without interfering with the performance of active applications. In parallel, network parameters can be observed periodically. When the capturing session finishes, capture is transformed to text2pcap input format. The lipcap format conversion tool is included in the free distribution of the Wireshark analyzer. The files can be transferred to a computer via USB, infrared or Bluetooth, depending on the terminal availability of these technologies. Lipcap files can be analyzed directly with Wireshark, taking advantage of the great variety of filtering options, statistical analysis and graph generation features of this application.

The capture functionality is launched from main menu "Capture/Start Capture" when the application capturing a "C" is shown in the navigation pane? (figure 14).

---

[1] GPRS, UMTS, HSDPA and WLAN data connections have been tested.

Figure 13. Capture Menu
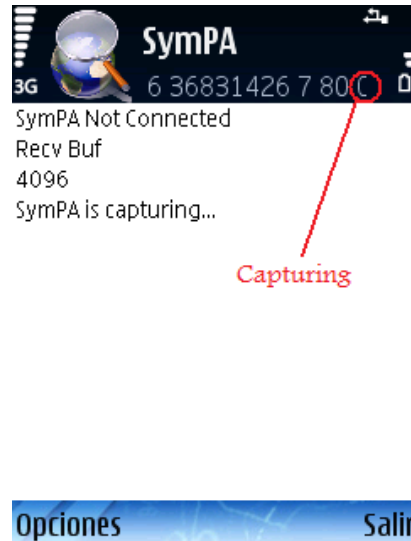

Figure 14. Capturing

Figure 15. Conversion Menu

Figure 16. File we want to convert

All the traffic captured is stored in a file located in the C:\ . The name of the file contains the date and time when the capture was initiated (figure 17). When it finishes, this file can be converted to the input format of text2cap tools using the conversion option shown in figure 15 and figure 16.
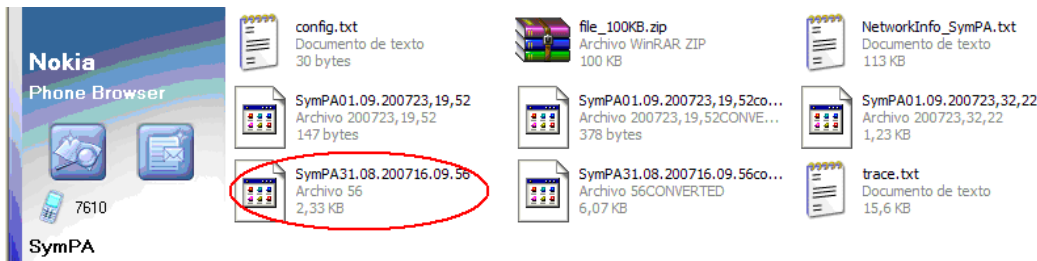
Figure 17. Capture File

The resulting file (figure 18) is transferred to the PC using a PC Suite or other technology such as Infrared or Bluetooth. Once the file is in the PC we can convert it to libpcap format so we can visualize it using a traditional Protocol Network Analyzer, such as Wireshark.
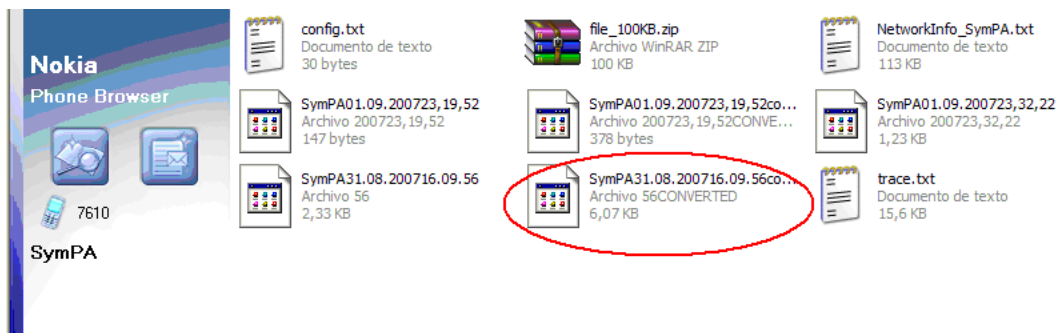

Figure 18. Converted File

```
05/05/200611:31:45,3437 000000 45 00 00 40 4d 88 40 00 2f 06 18 7c 96 d6 d6 1c d5 04 a3 bc 77 24 92 21 f8 df d4 8a 2k
05/05/200611:31:46,0625 000000 45 00 00 34 4d 89 40 00 2f 06 18 87 96 d6 d6 1c d5 04 a3 bc 77 24 92 21 f8 df d4 8b 2k
05/05/200611:31:46,3906 000000 45 00 00 de 4d 8a 40 00 2f 06 17 dc 96 d6 d6 1c d5 04 a3 bc 77 24 92 21 f8 df d4 8b 2k
05/05/200611:31:47,3906 000000 45 00 04 01 4d 8b 40 00 2f 06 14 b8 96 d6 d6 1c d5 04 a3 bc 77 24 92 21 f8 df d5 35 2k
05/05/200611:31:48,2812 000000 45 00 01 bc 4d 8c 40 00 2f 06 16 fc 96 d6 d6 1c d5 04 a3 bc 77 24 92 21 f8 df d9 02 2k
05/05/200611:31:49,3437 000000 45 00 01 bc 4d 8d 40 00 2f 06 16 fb 96 d6 d6 1c d5 04 a3 bc 77 24 92 21 f8 df da 8a 2k
05/05/200611:31:53,8437 000000 45 00 01 63 4d 94 40 00 2f 06 17 4d 96 d6 d6 1c d5 04 a3 bc 77 24 92 21 f8 df dc 12 2k
05/05/200611:31:54,4218 000000 45 00 01 2a 6d d3 00 00 6f 11 f7 3b 96 d6 d6 1c d5 04 a3 bc 1b 3a 1b 82 01 16 02 e1 8C
05/05/200611:31:54,4218 000000 45 00 00 70 6d d4 00 00 6f 11 f7 f4 96 d6 d6 1c d5 04 a3 bc 1b 3b 1b 83 00 5c 5f a0 8C
05/05/200611:31:54,4531 000000 45 00 01 b9 6d d5 00 00 6f 11 f6 aa 96 d6 d6 1c d5 04 a3 bc 1b 3a 1b 72 01 a5 34 75 8C
05/05/200611:31:54,5781 000000 45 00 00 70 6d d6 00 00 6f 11 f7 f2 96 d6 d6 1c d5 04 a3 bc 1b 3b 1b 73 00 5c bc 84 8C
05/05/200611:31:54,6875 000000 45 00 01 28 6d d8 00 00 6f 11 f7 38 96 d6 d6 1c d5 04 a3 bc 1b 3a 1b 82 01 14 3d 76 8C
05/05/200611:31:54,8281 000000 45 00 01 25 6d d9 00 00 6f 11 f7 3a 96 d6 d6 1c d5 04 a3 bc 1b 3a 1b 82 01 11 17 fb 8C
05/05/200611:31:55,0625 000000 45 00 01 32 6d da 00 00 6f 11 f7 2c 96 d6 d6 1c d5 04 a3 bc 1b 3a 1b 82 01 1e e9 57 8C
05/05/200611:31:55,6875 000000 45 00 04 c2 6d db 00 00 6f 11 f3 9b 96 d6 d6 1c d5 04 a3 bc 1b 3a 1b 72 04 ae db 68 8C
05/05/200611:31:56,2187 000000 45 00 01 29 6d df 00 00 6f 11 f7 30 96 d6 d6 1c d5 04 a3 bc 1b 3a 1b 82 01 15 e1 2d 8C
05/05/200611:31:56,2343 000000 45 00 03 66 6d dc 00 00 6f 11 f4 f6 96 d6 d6 1c d5 04 a3 bc 1b 3a 1b 72 03 52 eb ae 8C
05/05/200611:31:56,2812 000000 45 00 01 22 6d e0 00 00 6f 11 f7 36 96 d6 d6 1c d5 04 a3 bc 1b 3a 1b 82 01 0e bc 29 8C
05/05/200611:31:56,8281 000000 45 00 05 32 6d e1 00 00 6f 11 f3 25 96 d6 d6 1c d5 04 a3 bc 1b 3a 1b 72 05 1e e9 5e 8C
05/05/200611:31:56,9062 000000 45 00 00 c2 6d e2 00 00 6f 11 f7 94 96 d6 d6 1c d5 04 a3 bc 1b 3a 1b 72 00 ae ae 73 8C
05/05/200611:31:57,0000 000000 45 00 01 27 6d e3 00 00 6f 11 f7 2e 96 d6 d6 1c d5 04 a3 bc 1b 3a 1b 82 01 13 15 c0 8C
05/05/200611:31:57,1250 000000 45 00 01 27 6d e4 00 00 6f 11 f7 2d 96 d6 d6 1c d5 04 a3 bc 1b 3a 1b 82 01 13 3d f5 8C
05/05/200611:31:57,2500 000000 45 00 01 2a 6d e5 00 00 6f 11 f7 29 96 d6 d6 1c d5 04 a3 bc 1b 3a 1b 82 01 16 dd 70 8C
05/05/200611:31:57,6406 000000 45 00 03 fd 6d e6 00 00 6f 11 f4 55 96 d6 d6 1c d5 04 a3 bc 1b 3a 1b 72 03 e9 8d d3 8C
05/05/200611:31:57,9375 000000 45 00 03 81 6d e7 00 00 6f 11 f4 d0 96 d6 d6 1c d5 04 a3 bc 1b 3a 1b 72 03 6d 81 46 8C
05/05/200611:31:58,3125 000000 45 00 01 6a 6d e8 00 00 6f 11 f6 e6 96 d6 d6 1c d5 04 a3 bc 1b 3a 1b 82 01 56 d1 a2 8C
05/05/200611:31:58,5000 000000 45 00 01 48 6d e9 00 00 6f 11 f7 07 96 d6 d6 1c d5 04 a3 bc 1b 3a 1b 82 01 34 20 08 8C
05/05/200611:31:58,7812 000000 45 00 04 75 6d ea 00 00 6f 11 f3 d9 96 d6 d6 1c d5 04 a3 bc 1b 3a 1b 72 04 61 01 d6 8C
05/05/200611:31:59,1406 000000 45 00 02 db 6d eb 00 00 6f 11 f5 72 96 d6 d6 1c d5 04 a3 bc 1b 3a 1b 72 02 c7 dc 95 8C
05/05/200611:31:59,2656 000000 45 00 01 2f 6d ec 00 00 6f 11 f7 1d 96 d6 d6 1c d5 04 a3 bc 1b 3a 1b 82 01 1b 10 58 8C
05/05/200611:31:59,3906 000000 45 00 01 29 6d ed 00 00 6f 11 f7 22 96 d6 d6 1c d5 04 a3 bc 1b 3a 1b 82 01 15 49 66 8C
```

Figure 19. Converted File Format. Text2cap input

The file shown in figure 19 is the input of the text2cap tool provided with the Wireshark Protocol Analyzer. A .bat file example is available on the web site to use the text2cap utility, but before doing so, users need to check the time format which appears in the timestamps of a capture file as shown in figure 18 circled in red. This is because changes in the timestamp format depend on the internal configuration of the mobile device. The time format must be in 24h clock format and not pm/am format although this issue will be fixed in future releases to make the conversion seamless.

This is an example of using the text2cap utility. The time format appearing in the converted file obtained from the SymPA tool should agree with that used in the call to the text2cap utility.

text2pcap.exe -l 12 -t %%d/%%m/%%Y%%H:%%M:%%S, %1 %1.pcap

3.1.2 PDP Context Info

This functionality has been tested over GSM, UMTS and HSDPA networks. Information provided can be divided into three categories:

3.2.2.1   Network Interface Information

Nifs Number of packet network interfaces.

Context Name Name of the context defined for the network interface.

Context Type
0 Unspecific context type
1 Internal created context
2 Externally created context

Nif Status Network Interface Status
0 Unknown
1 Not activated
2 Activating
3 Active
4 Deactivating
5 Suspended
6 Deleted

Figure 20. Network interface info

Context Number Number of contexts belonging to the network interface.

PDP Address PDP Address of network interface.

Conn Status Packet data connection status
0 Unattached

1 Attached to network but the packet data connection is inactive
2 Attached to network and the packet data connection is active
3 Attached to network but the packet data connection is suspended

3.1.2.2 Packet-switched Connection Context Information

Connection Speed Connection bandwidth in bits per second

Bytes Sent Number of bytes transmitted over the airlink since its activation

Overflow Sent Number of bytes overflow during the transmission

Bytes Received Number of bytes received

Overflow Recv Number of bytes overflow during reception
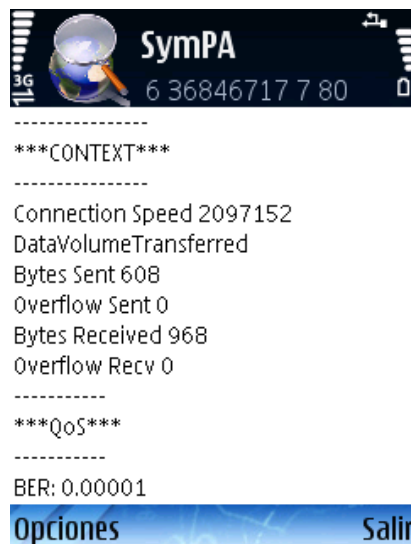
Figure 21. PDP Context Info

3.1.2.3 Negotiated values for GPRS/UMTS Rel99, UMTS Rel4 and HSDPA Rel 5 QoS profile

BER Negotiated target bit error rate

Deliver Erroneous SDU Negotiated target service data unit error ratio
- 1 Unspecific
- 2 Erroneous SDUs delivered. Error detection not considered

- o 4 Erroneous SDUs delivered plus error indication. Error detection used
- o 8 Erroneous SDUs discarded. Error detection used.

Deliver Order reqd Negotiated value for sequencial SDU delivery
- o 1 Unspecific
- o 2 Required to be in sequence
- o 4 Not Required to be in sequence

Guaranteed Bit Rate Downlink Downlink bitrate in kbps

Guaranteed Bit Rate Uplink Uplink bitrate in kbps

Max Rate downlink Maximum downlink bitrate negotiated in kbps

Max Rate Uplink Maximum uplink bitrate negotiated in kbps

Max SDU size Negotiated maximum SDU size (octets)

SDU error ratio Target SDU Error Ratio

Traffic class Negotiated traffic class

Traffic handling priority Negotiated traffic handling priority

Transfer delay Negotiated transfer delay (milliseconds)
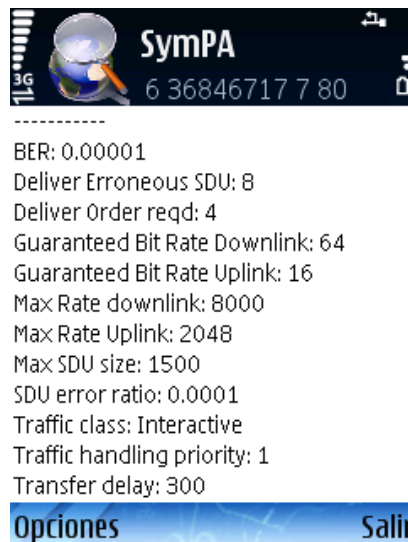
Figure 22. QoS Info

3.2.3 Ping

Traditional ping utility. Time is measured in microseconds. Provides an estimation of the round trip delay in connections.
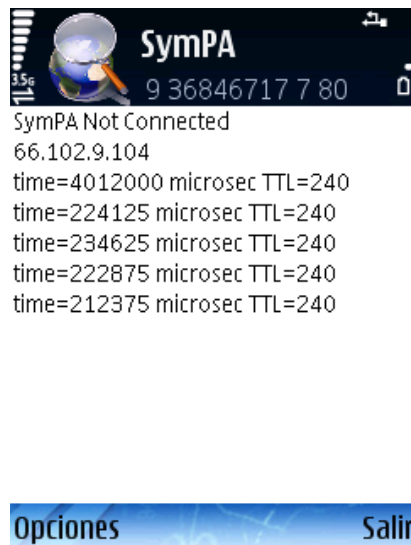
Figure 23. Ping

3.2.4 Mobile to Mobile File Transfer

This utility allows us to transfer a text file between two mobile devices using TCP sockets. The size of the file is fixed to 100kB, in future releases this value will be configurable.

Using this functionality, SymPA enables testing of mobile-to-mobile communications. In this way this tool allows the detection of anomalies and incorrect configurations in TCP implementations used in mobile terminals. These anomalies could appear due to degradation caused by factors which are only present in the mobile environment such as handover. This kind of scenario is therefore very difficult to reproduce. In this use case, it is especially important to use SymPA for real time monitoring.

Capturing the traffic between two mobile devices allows the mobile to mobile connection to be characterized.

3.2.4.1 Starting server side

This functionality is launched through the menu "File Transfer/FileTransfer/Start" as we can see in figure 24. Prior to this we need to open a PDP context. We can use the "Connect" option from the main menu to open a PDP context. The IP address provided will be used for establishing the connection from client side (Figure 25).

Figure 24. Transfer File. Server Side. Step 1

Once the server opens a new socket and while it is waiting for external connections the message "Waiting for connections" is shown on the screen.

3.0 Getting Started
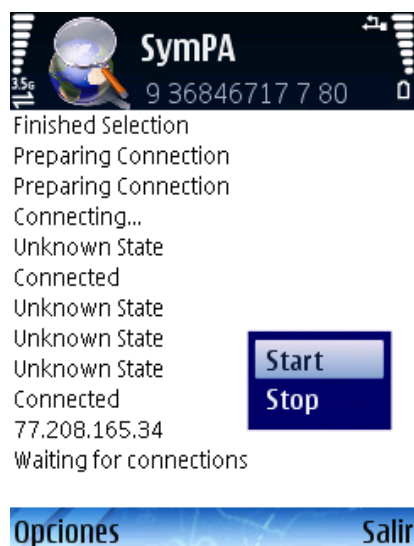
Figure 25. Transfer File. Server Side. Step 2
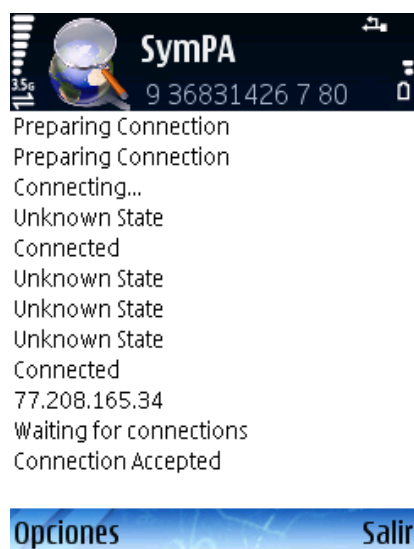
Figure 26. Transfer File. Server Side. Step 3

3.2.4.2 Starting client side

On the client side a dialog appears requesting an IP address (Figure 27). We should introduce the address shown on the server side. Then, we press the "OK" button and the connection is initiated.
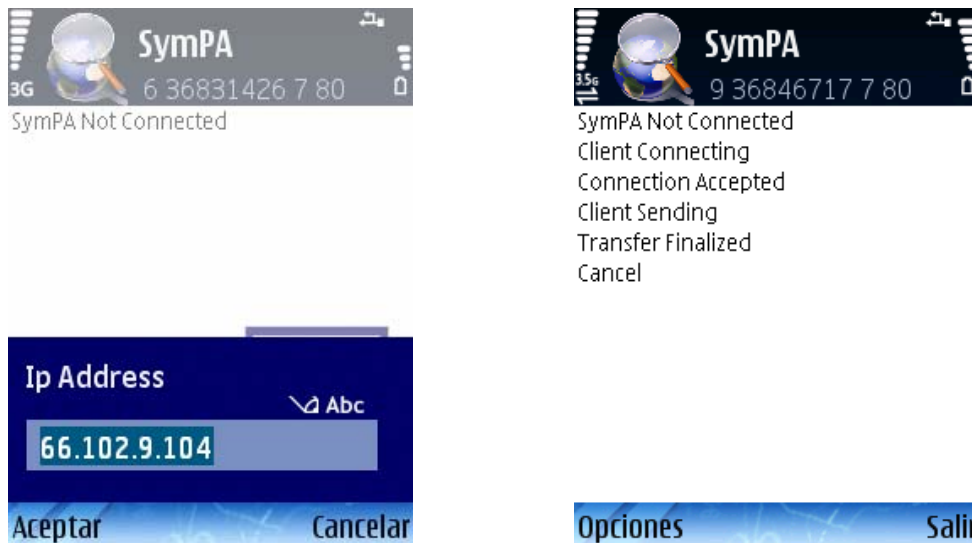
Figure 27. Transfer File. Client Side

3.2.5 Cell Info

The cell info utility offers two different options. The first option "Show Cell Info" shows the information about the cell where the mobile or device is located. The information available is the following:

CC (Country Code)
Network Identifier
Analog SID
CDMA SID
Tag (Network name)
Name (Network name)
Short Name (Network name)
Cell Identifier
LAC (Location Area Code)
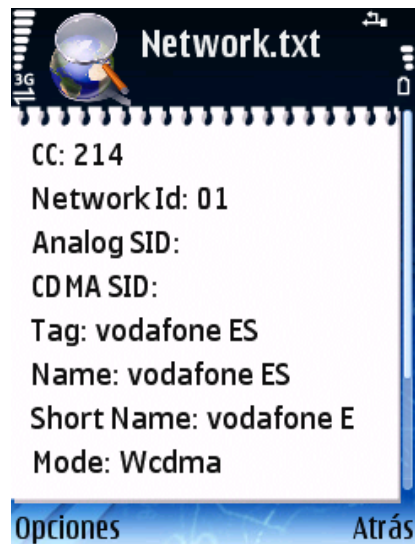
Figure 28. Network Info

The other function allows us to monitor the cell identifier and network mode. During the monitoring, cell information is stored every second in a file labeled NetworkInfo_SymPa.txt located in the C:\. The file format is shown in figure 30. While this mode is active, an "M" is shown in the navigation pane of the application (Figure 28).
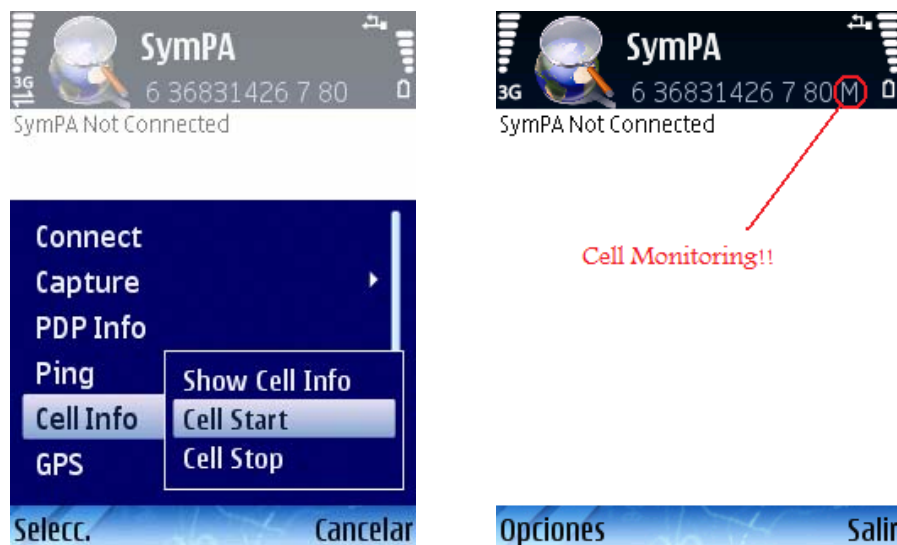
Figure 28. Network Monitoring
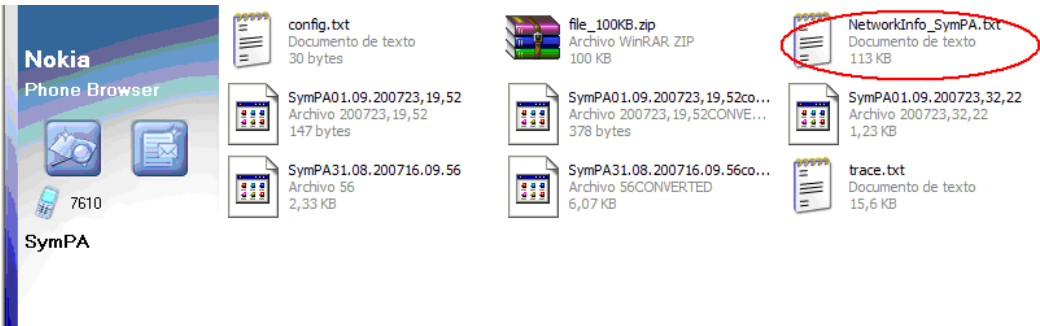
Figure 29. NetworkInfo_SymPA.txt

Figure 30. NetworkInfo_SymPA.txt file format

3.2.6 GPS Tracking (New)

GPS tracking functionality enables the monitoring of the speed of the mobile terminal as well as its position. The information is stored in a file name gps.txt, located in C:\. The format of this file is show in figure 32.
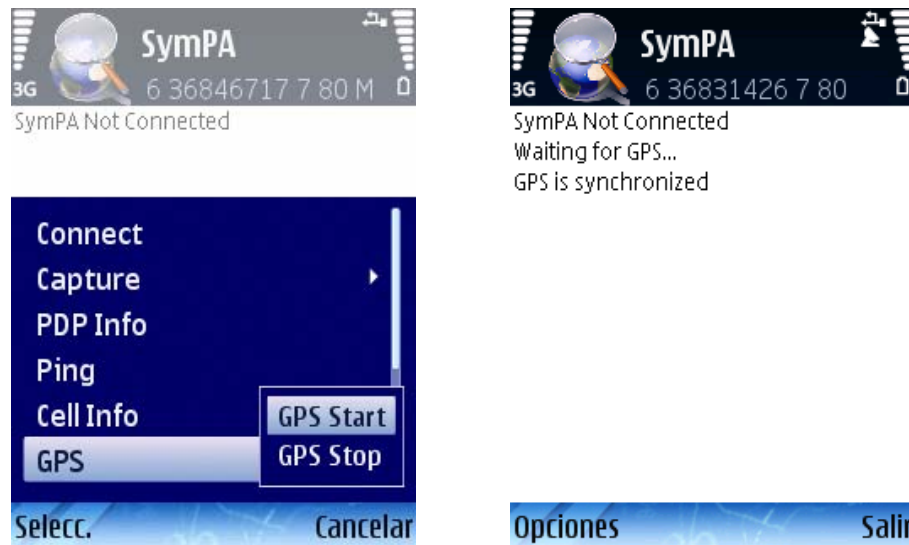

Figure 31. Gps tracking

Figure 32. Gps.txt

3.2.7 Localization (New)

This functionality allows visualizing directly on the mobile device a map of the area where the mobile device is located.
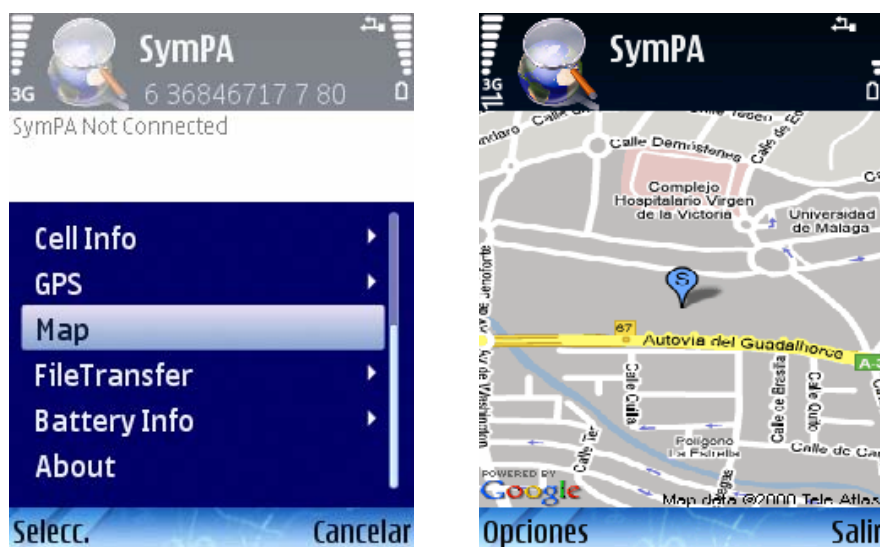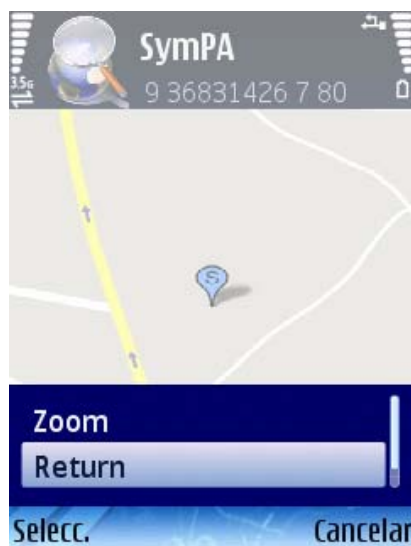

Figure 33. Map

Figure 34. Zoom functionality

3.2.8 Battery monitoring (New)

Battery monitoring functionality allows analyzing energy consumption using different radio access technologies, in different locations and in static or vehicular scenarios. Information collected is stored in a file named BatteryInfo_SymPA.txt , located in C:\. The format of this file is shown in figure 36.
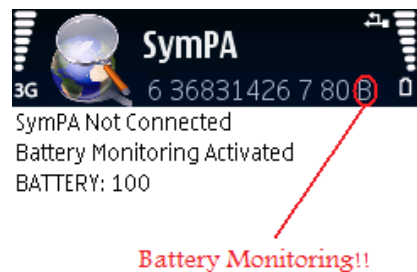

Figure 35. Battery Monitoring

Figure 36. BatteryInfo_SymPA.txt

3.2.9 Log file

A log file is stored in the SymPA directory with all the information shown on the screen of the mobile device. The log file is labeled "trace.txt".
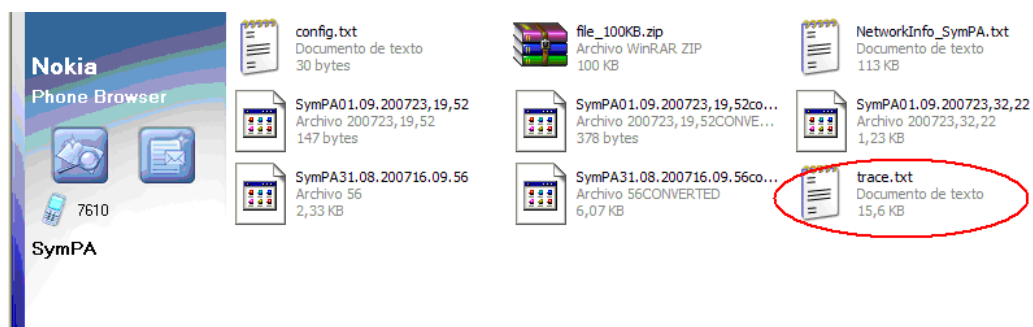

Figure 37. Log File

4.0   USE CASES

4.0   USE CASES

4.1 Live Capture

SymPA allows the capture of traffic received by third applications running on the mobile phone. The normal use of the tool is as follows. First of all, the SymPA tool needs to be launched and the capture mode should be activated. Then the application we want to analyze should be opened. This application will activate a PDP context and SymPA will capture all the traffic received through this context.

As we can see at figure 38 packet captured can be correlated with the rest of the information obtained with SymPA. In figure 38 we can see how a burst of packet losses takes place during a cell change.

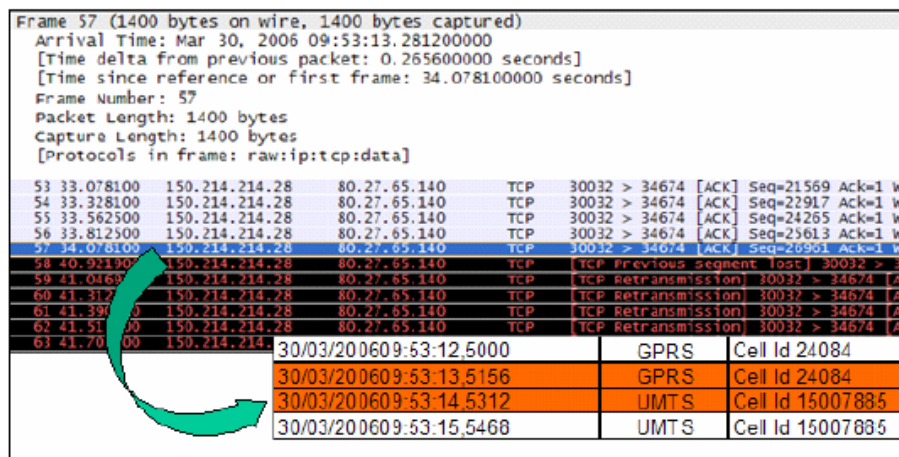

Figure 38. Live capture and cell monitoring

4.2 Info Maps

Cell monitoring and PDP context info functionalities can be used to obtain coverage maps, status maps, and quality of service maps of mobile networks, based on the cell identifier. GPS information have been incorporated to obtain and store data on the physical location of the cell, in order to establish geographical cell limits.

This point is very interesting in UMTS networks where the geographical area covered by a cell depends on the amount of traffic handled by the cell.

Con formato: Justificado

4.3 Experimental Results

This tool has been extensively tested in the performance analysis of video streaming service over cellular networks.

Experimental results can be found in our related works:

[1] A. Díaz-Zayas, P. Merino, L. Panizo, A.M. Recio, "Evaluating Video Streaming over GPRS/UMTS networks: A Practical Case", in IEEE 65th Vehicular Technology Conference VTC2007-Spring(VTC2007 Spring), 22 - 25 April 2007

[2] A. Díaz-Zayas, P. Merino, L. Panizo, A.M. Recio, ""Experimental analysis of peer-to-peer streaming in cellular networks", in IEEE 21st International Conference on Advanced Information Networking and Applications (AINA-07), May 21-23 2007

[3] A. D. Joseph, A. Díaz, P. Merino, F. J. Rivas, U. P. Kulkarni, J. V. Vadavi, G. S. Thyagaraju, S. M. Joshi, and A. R. Yardi, "Mobile and Ubiquitous Objects," IEEE Pervasive Computing, vol. 5, iss. 3, pp. 57–59, 2006.

[4] A. Díaz, P. Merino, and F. J. Rivas, "Performance Monitoring and Analysis of Wireless Communication Protocols for Mobile Devices," in Proc. 1st International Conference on Ubiquitous Computing: Applications, Technology and Social Issues (ICUC 2006), 2006, pp. 103–108.

[5] Almudena Díaz; Pedro Merino and F. Javier Rivas, Customer-centric measurements on mobile phones. In Proceedings on 12th IEEE International Symposium on Consumer Electronics. ICSE 2008. Vilamoura, Portugal. 14-16 April. págs. 4. IEEE Computer Society: Los Alamitos, CA, 2008.

[6] Almudena Díaz and Pedro Merino, Towards a lightweight middleware for mobile multimedia communications awareness. In Proceedings on Mobimedia 2008 MOBIMEDIA '08, July 7-9, 2008, Oulu, Finland