Supplemental to the 304th MI Bn Periodic Newsletter
Sample Overview: al Qaida-Like Mobile Discussions & Potential Creative Uses
By 304th MI Bn OSINT Team
October 16, 2008
This is a draft FOUO product

The above examples of Nokia Map Functions are displayed in a Pro Islamic State of Iraq (al Qaida) Discussion thread at http://www.muslm.net/vb/showthread.php?p=1797473 with software description and download instructions. Posting date March 24, 2008.

Overview

Terrorists and persons sympathetic to terrorism recommend a variety of different mobile to web technologies, software, and Voice over Internet Protocol (VoIP)[1] for their mobile phone use. Some of the tactics are old, some of the tactics are still emerging, and some tactics may emerge from hacker, activist, and criminal non-terrorist use. This paper briefly covers a few examples of terrorist use and potential use of mobile to web and web to mobile technologies and tactics from an open source perspective. The paper includes the following five topics: *Pro Terrorist Propaganda Mobile Interfaces*, *Mobile Phone GPS for Movements, Ops, Targeting, and Exploitation*, *The Mobile Phone as a Surveillance Tool*, *Voice Changers for Terrorist Phone Calls*, a *Red Teaming Perspective on the Potential Terrorist Use of Twitter*, and a sample of software that is recommended on one pro terrorist website for mobile phone activities. There are numerous possibilities that are not covered in this paper due to time and research constraints. For example, Google Earth, Mobile GPS Mashups[2] and Mobile Phone Number Spoofing techniques are not addressed in this paper but are certainly worth Open Source Intelligence (OSINT) consideration and probably deserve a paper (if not a book) unto itself.

Please note the following caveats to this article. The first limitation is the discussed technologies were not independently verified in a red teaming scenario, so it is unclear whether some of the discussed tactics and methodologies would actually work. For example, extremist suggestions to include integrating a mobile phone camera into a missile warhead seem highly improbable. Second, a majority of the information was extracted from al Qaida-like websites from uncollaborated postings made by terrorists, persons sympathetic to terrorism, or honey pots[3]. Third, the research used to generate this paper was conducted from open sources only and has not been compared and/or contrasted with information in non-open source (classified) venues. Fourth, each topic is merely an introduction into the subject and deserves further research and contemplation. Fifth, the author is not a linguist, but used rudimentary Arabic language skills and the Google translating tool to extract website context. Finally, the potential for use of certain web to mobile technologies and tactics is dependent upon the mobile service available in different states and regions. For example, terrorists could theoretically use Twitter social networking in the U.S. as an operation tool. However, it is unclear whether that same theoretical use would be available to terrorists in other countries and to what extent.

What did become clear from conducting research on this topic is that there are numerous different tactics, tools, and software services that can be used by terrorists to conduct activities that go well beyond the original intent of the mobile phone voice communications and that these burgeoning capabilities are available for OSINT exploitation. Further, there may be a possibility to profile a portion of particular cyber

---

[1] Prior August 2007 304th MI Bn OSINT Team Research Article "Terrorist and Extremist Use of Voice Over Internet Protocol" is available on the 304th MI Bn OSINT Team INTELINK U page at https://www.intelink.gov/inteldocs/view.php?fDocumentId=10699 (If you do not have access to INTELINK U and would like a copy of this newsletter please e-mail [redacted])

[2] http://sea-eyes.com/vb/t3306.html

[3] Honey Pot is defined as something (example a website) that is set up in order to allure select audience members so that they may be tracked and monitored.

terrorist-like groups and their audiences based on the particular set of software and phones that the group recommends from OSINT exploitation.

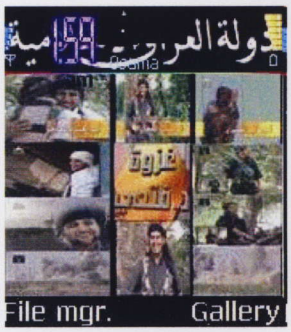
Table of Contents

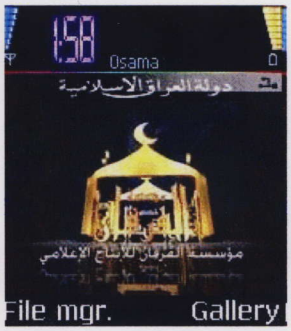
Pro Terrorist Propaganda Cell Phone Interfaces

The mobile phone provides an active outlet for terrorist propaganda. Currently there are thousands of multimedia clips (audio, video, photo, Power Point, text, PDF) that may be up loaded to mobile phones from multiple websites and multimedia bunkers. In addition, mobile phone texting appears to be consistently and possibly increasingly popular among pro terrorist audiences (just as it is with non-terrorist audiences). Some terrorist organizations are further branded by a specific cell phone interface, which makes the actual phone a piece of propaganda. Following are two examples:

Army of the Mujahedeen Cell Phone Interface (Advertized Cell Phone Screen Appearance)

Islamic State of Iraq Cell Phone Interface (Advertized Cell Phone Screen Appearance)





The software for the above interfaces is advertized as being available for download on select extremist websites, such as tamkeen.iraqserve.com.

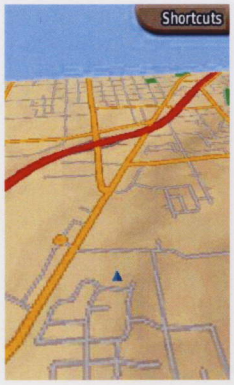
Source: Arabic Discussion Forum http://llyan.org/vb/showthread.php?t=5844 (From Google Search Result Description: "*Make your love for God, Eid and satisfaction and your obedience and Mwalatk and Zkirk and Islamic Jihad .... Sailing fast and easy navigation system with A-GPS maps and the application of Nokia Maps.*"

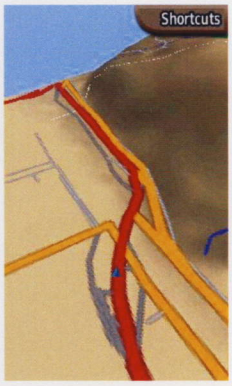
Compare the previous text with a vendor's write-up "*Sailing fast and easy navigation system with A-GPS and Nokia Maps application maps. Find your destination on foot or in the car with a compass for navigation Serra. Take pictures and video through the use of high-quality 3.2-megapixel camera with flash The advantage Panoramic 240 × 320QVGA See maps, pictures and videos on the screen QVGA stunning 2.4-inch size and the quality of 320 × 240 Browse the Internet, send e-mail your uploaded content quickly connect via high-speed 3.5G* "

Cell Phone GPS for Movements, Ops, Targeting & Exploitation

Nokia 6210 Navigator and other GPS cell phone services could be used by our adversaries for travel plans, surveillance and targeting.

Following is an example of one extremist discussion thread surrounding the use of Mobile Phone GPS (there are multiple postings on this issue which could be a paper unto itself.) On May 3, 2008 a discussion topic was posted in the pro terrorist forum *al Hebash* at www.alhesbah.net (now defunct) on the theoretical use of Nokia GPS for "Specialist use in Marksmanship, Border Crossings, and in Concealment of Supplies." The following three Graphics were associated with this posting.

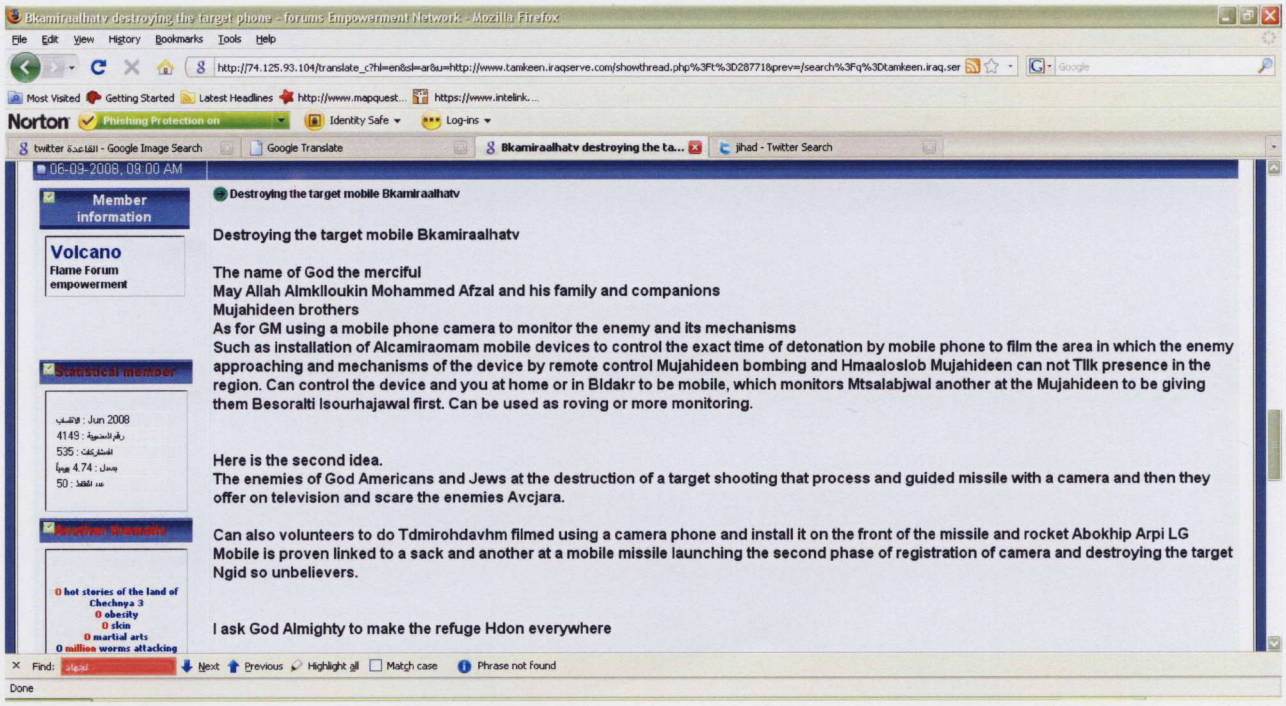




One response to the topic thread was that city images and pictures were not adequate because additional information, such as geo-coordinates, was needed for deserts and forests (non-urban areas). A later posting in the thread discussed the pros and cons of GPS under the title "*An Intensive Course in the Use of LG PSV GPS*" (Reference screen capture on next page) which briefly covered some of the benefits and detriments of using GPS. The article mentioned the use of geo coordinates for border crossings, item concealment, and for identifying enemy locations. The article also mentioned that GPS would be useful for identifying terrain and natural resources, such as water. In addition, the article mentioned that attained enemy GPS can be useful for information exploitation.

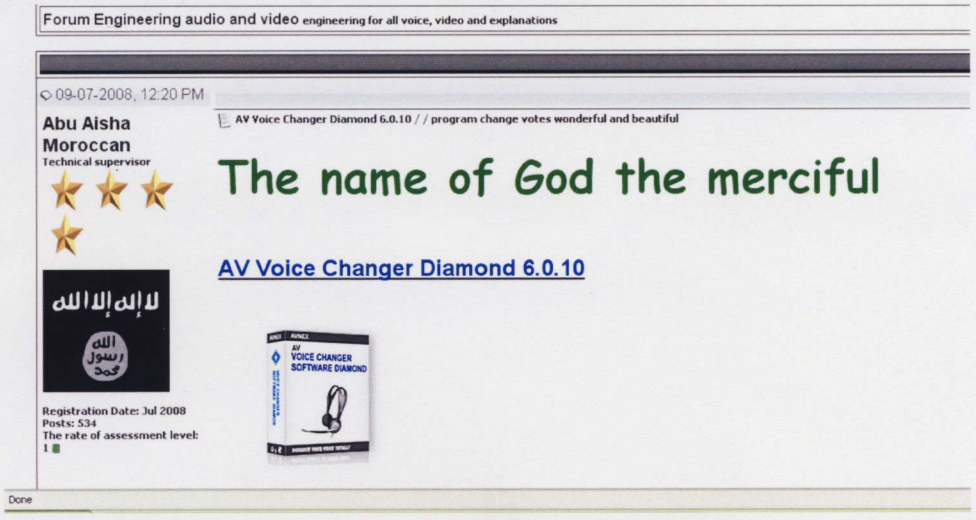
Mobile Phone Surveillance

On September 6, 2008 an individual using the pseudonym of "Volcano" provided a theoretical discussion in the Mujahedeen Army of Iraq Enabling Islamic Mobiles forum, www.tamkeen.iraqserve.com, on the use of mobile phones for target surveillance and attacks. Under the category of basic surveillance, "Volcano" recommended using the phone/video camera for monitoring enemy activities and operations in theater. Of unique interest is that "Volcano" posed several theoretical examples of how to use the mobile phone video and camera options in tandem with conducting attacks. For example, "Volcano" suggested that one could use the mobile phone for remote surveillance to tag the opportune time of attack. "Volcano" also hypothesized whether a mobile phone camera could be integrated into a missile head to film a target as it is being attacked. This recommendation probably would not work but provides insight into adversarial perspectives. (Reference the screen capture on the following page.)



Voice Changers for Terrorist Telephone Calls?

You may have seen it in a movie, the villain calling the victim with an altered voice to hide his/her identity. In the movies, that theme is fairly common; the question really is whether our adversaries will consider voice changing technology for use in future operations. The answer could be yes. On September 9, 2008 *Abu Aisha the Moroccan, Technical Supervisor*, of the *Technical Audio Discussion* of the *Ansar al Jihad* forum recommended voice changing software for making VOIP telephone calls. He mentioned that the software would be helpful for most VOIP services including Skype and Vonage. This recommendation was posted following public media reports of the Taliban using



SKYPE.[4] The timing was most likely coincidental and unrelated but the two concepts can complement one another. The Taliban and other like groups suspecting their VOIP communications are being be monitored could theoretically combine voice changing software with (or without) encryption and caller I.D. spoofing[5] in order to make basic detection more difficult. This tactic may or may not be effective to elude international intelligence agencies. However, it might be effective for calling in demands, interviews, and/or attack claims to media outlets. *Abu Aisha the Moroccan* specifically recommended *AV Voice Changer Diamond 6.0.10* off a freeware download page. Audio for Fun, http://www.audio4fun.com/voice-over.htm, describes the software package as:

> *"The latest edition in the VOICE CHANGER SOFTWARE series which is dedicated to voice changing and voice manipulating for online and local computer-based programs.*
>
> *The software is able to do a wide range of voice changing related tasks for many different purposes, such as voice-over and voice dubbing for audio/video clips, presentations, narrations, voice messages, voice mails, E-greeting cards, etc.; mimic the voice of any person, create animal sounds, change voices in songs, etc.*
>
> *This Diamond edition also presents a faster voice morphing algorithm, a professional looking interface, background effects library and numerous ready-to-use nickvoices. The many packages of parody voices will help users to talk in the voices of many Hollywood stars and other celebrities.*
>
> *Voice Changer Software Diamond works well with many common VoIP programs such as Net2Phone, SkypeOut, Vonage, etc., and many Instant Messenger programs such as Yahoo Messenger with Voice, Skype, Windows Live Messenger, AIM, etc.*
>
> *KEY FEATURES: Ready-to-use nickvoices, Parody Maker, Frequency Morpher, Audio Stream Recorder, Pitch and Timbre Morpher graph, Equalizers Background Effects.*
>
> *MAIN BENEFITS: Voice Changer Software Diamond is useful for users who want to be the Voice Master of Media in cyberspace. They can use it to have fun while chatting using instant messenger programs, do voice dubbing and voice-overs for their own video/audio clips, mimic the voice of their favorite Idol, and more."*

Terrorists may or may not be using Voice Changing software but it should be of open source interest that on line terrorists and/or terrorist enthusiasts are discussing it.

---

[4] Owen, Glen, "Taliban Using Skype Phones to Dodge MI6, UK Daily Mail, Sept. 13, 2008, http://www.dailymail.co.uk/news/worldnews/article-1055611/Taliban-using-Skype-phones-dodge-MI6.html?ITO=1490; Wylie, Pete, "Taliban VOIP Calls," Fierce VOIP, Sept. 15, http://www.fiercevoip.com/story/taliban-voip-calls/2008-09-15

[5] Spoofing is defined as using deception to create something that is fabricated or false, such as a false IP or telephone number.

Potential for Terrorist Use of Twitter: A Red Teaming Perspective

Example Iraq Tweets

"Less than 24 hrs before I head off for my vacation in Iraq and the kids are already making my wife miserable. Today is not going to be fun."

"Going to DFAC -- Dining Facility -- here at BIAP. Try to get on helicopter to Kalsu tonight."

"Put off at BIAP (Baghdad International Airport). Not sure why."

"Chillin in my tent at Baghdad International Airport (BIAP)."

"Drove off base today down Route Irish in an 'NTV and didn't get blown up...fun fun."

"Just picked my roomie up from BIAP, now it's ten 'til 2 in the morning, ugh."

"Today is my day off. 115 already in Camp Bucca, Iraq."

Example Afghanistan Tweets

"I'm in Bagram waiting for a flight to Camp Salerno by Kwost in the volatile east of Afghanistan near the Paki. border. Hot days/cold nights."

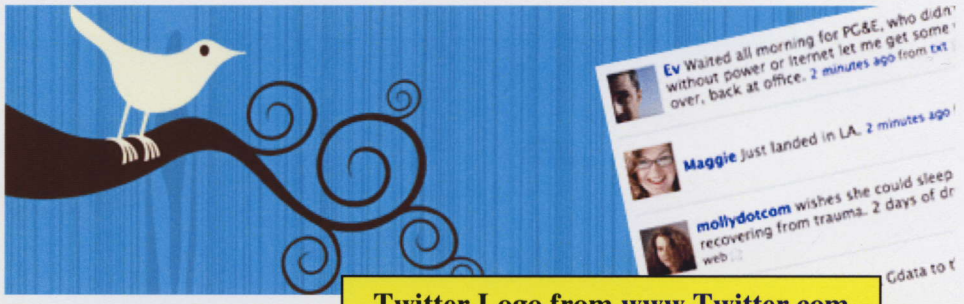
"Hi from Bagram air field; 20 minutes from now I'll hopefully board a flight to the Pakistan border."

"Flying to Bagram, Afghanistan in 12 hours. The journey is about to begin!"

Example Fort Huachuca Tweets

"Email I just got: "We are changing all of the PMs tasks at Ft. Huachuca. I hope this does not add a lot of extra work on your end." HA!"

"...is at Ft. Huachuca. It was great seeing him last night passing through Tucson International."



Twitter Logo from www.Twitter.com

Twitter is described as "a free Social Networking and Micro Blogging[6] service that lets members keep in touch with people using the web, their phone, or IM (instant messaging)."[7] Twitter is similar to other social networking sites in that it allows people to create a community of interest and/or group of online friends. Twitter launched in July 2006 and has become an increasingly popular networking venue over the past two years.[8] On September 26, 2008, there were **21,100,000** Google Hits for doing a search on Twitter.com, which was advertised on a multitude of different language web pages, including English, Arabic, Armenian, Simplified Chinese, Croatian, Czech, Indonesian, Korean, Thai, and other languages[9].

What makes Twitter unique is that the member can send Tweets (messages) near real time to Twitter cell phone

[6] Search Mobile Computing Online defines Micro Blogging as *"Microblogging is the practice of sending brief posts to a personal blog on a microblogging Web site, such as Twitter or Jaiku. Microposts can be made public on a Web site and/or distributed to a private group of subscribers. Subscribers can read microblog posts online or request that updates be delivered in real time to their desktop as an instant message or sent to a mobile device as an SMS text message."* http://searchmobilecomputing.techtarget.com/sDefinition/0,,sid40_gci1265620,00.html

[8] Crunch Base, "Twitter Company Profile," 2008, http://www.crunchbase.com/company/Twitter

[9] Google Search of Twitter.com, Sept. 27, 2008

groups and to their online Twitter social networking page. They can also Mashup their Tweets with a variety of other tools including geo coordinates and Google Maps or other electronic files/artifacts. Members can direct and re-direct audience members to other websites and locations from "Tweets" and can engage in rapid-fire group social interaction. For example, the earthquake that occurred in Los Angeles on July 29, 2008 was reported via a Twitter member approximately four minutes prior to the information being reported by the news and within minutes there were hundreds of Tweets from people experiencing the earthquake first hand.[10] Twitter has also become a social activism tool for socialists, human rights groups, communists, vegetarians, anarchists, religious communities, atheists, political enthusiasts, *hacktivists* and others to communicate with each other and to send messages to broader audiences.[11]

Twitter is already used by some members to post and/or support extremist ideologies and perspectives. For example, there are multiple pro and anti Hezbollah Tweets. In addition, extremist and terrorist use of Twitter could evolve over time to reflect tactics that are already evolving in use by *hacktivists* and activists for surveillance. This could theoretically be combined with targeting. Twitter was recently used as a counter-surveillance, command and control, and movement tool by activists at the Republican National Convention (RNC). The activists would Tweet each other and their Twitter pages to add information on what was happening with Law Enforcement near real time.

Activist Use of Twitter for Law Enforcement Counter Surveillance and Movement Coordination at the most recent Republican National Convention (RNC)

The following sample Tweets were collected and posted in a Computer World article "Twitter Helps Republican Convention Protestors Organize, Elude Police," on September 8, 2008 (http://www.pcworld.idg.com.au/index.php/id;7484771):

- "Arrest teams are approaching seated protesters on Marion Bridge. Resisters are told they'll be met with force."
- "Protestors are now fighting back. First reports of violence now"
- "Western Ave. Bridge, west of capitol can be safely crossed."
- "City is on lockdown. Go to 14th and Jackson if you need help from tear gas pepper spray." (http://www.linuxworld.com.au/index.php/id;7484771)

There are multiple red-teaming examples that could be created surrounding potential adversarial use of Twitter. Following are three red team scenarios:

[10] Weaver, Matthew, "Did the Earth Tweet For You," UK Guardian Blog, July 30, 2008, http://www.guardian.co.uk/news/blog/2008/jul/30/laearthquakehitsrealitytv

[11] 304th MI Bn OSINT Team Review of Member Twitter Pages

Scenario 1:
Terrorist operative "A" uses Twitter with (or without) using a cell phone camera/video function to send back messages, and to receive messages, from the rest of his cell. Operative "A" also has a Google Maps Twitter Mash Up of where he is under a code word for other members of his cell (if they need more in-depth directions) posted on the WWW that can be viewed from their mobiles. Other members of his cell receive near real time updates (similar to the movement updates that were sent by activists at the RNC) on how, where, and the number of troops that are moving in order to conduct an ambush.

Scenario 2:
Terrorist operative "A" has a mobile phone for Tweet messaging and for taking images. Operative "A" also has a separate mobile phone that is actually an explosive device and/or a suicide vest for remote detonation. Terrorist operative "B" has the detonator and a mobile to view "A's" Tweets and images. This may allow "B" to select the precise moment of remote detonation based on near real time movement and imagery that is being sent by "A."

Scenario 3:
Cyber Terrorist operative "A" finds U.S. Army Smith's Twitter account. Operative "A" joins Smith's Tweets and begins to elicit information from Smith. This information is then used for a targeting package (targeting in this sense could be for identity theft, hacking, and/or physical.) This scenario is not new and has already been discussed for other social networking sites, such as My Space and/or Face Book.

Sample of other Mobile Phone Topics & Software Recommendations

Sample Source: The mobile phone technology forum in **www.tamkeen.iraqserve.com**

- Recommends and debates mobile phone brands (Samsung, Nokia, etc.)
- Propaganda multimedia downloads for the phone (videos, audio clips, text files, PDF, etc.)
- Mobile phone tips for surveillance activities
- Uses of SMS text messaging
- Windows Live Messenger for the mobile
- Free advanced mobile messages to your mobile from website Huda 76
- Mobile Phone GPS tracking options
- How to upload software updates
- Religious upload software, such as prayer times reminders
- Religious and ideological background wall paper
    - The Software package-Mobile Master Professional 7.0.1 Build 2699
- Xilisoft 3GP Video Converter
    - convert 3GP to avi or mpg, and vice versa, as well as 3gp mpg, mpeg2, mpeg4, wmv, mp4, 3gp, mov, rm, dv, yuv, h264 and MP3, WAV, AC3, WMA, m4a, ogg
- Ego Share Software (data recovery)
- How to maintain and crack mobile phone security codes
- How to make mobile software programs
- Discussions on how to protect and penetrate Blue Tooth technology
- PDA programs for the mobile phone (Some of the software downloads that were advertized are sub-listed below)
    - Best TaskMan v2.01

- emTube V1.06
- InstFast v0.01
- Islamic Organizer v2.00
- Blacklist v2.00
- ActiveFile v 1.25
- AnsweringMachine.v1.10
- rotateMe v2.0.5
- Symbian.Guru.BT.Guard.v1.00.S60v3.SymbianOS9.1.Unsigned.Arabic-ArabPDA
- Quick Office Premier Upgrade 4.5.25.0
- Tobias Stoger.S60Ticker.S60v3.SymbianOS9.1.Arabic-ArabPDA
- CorePlayer.v1.1.2
- FlashLite v3.0
- Mobiola Media Player v2.1
- AudioNotes.v1.31
- S60SpotOn v0.7
- Pocket.Quran.v0.96b
- Theme DIY v1.2
- FreeTones.v1.05.S60v3.SymbianOS9.1.Unsigned.Arabic
- SmartGuard v2.00
- Total recall (advertized for wire tapping)
- Best Dictaphone v1.0
- Opera v8.65 (search engine)
- KavMobile 6.1.8 (Antivirus)