e-stealth.com

ULTIMATE BLUETOOTH MOBILE PHONE SPY SOFTWARE

USER MANUAL

Note: we have provided instructions on a select contents of the entire suite and directions on installing on some of the industry's popular phones. Not all phones are listed. If you do not find your phone in this manual, we recommend that you search on the internet on how to install third-party software onto your phone.

Introduction

Bluejacking is the sending of unsolicited messages over Bluetooth to Bluetooth-enabled devices such as mobile phones, PDAs or laptop computers, sending a vCard which typically contains a message in the name field (i.e. for bluedating or bluechat) to another bluetooth enabled device via the OBEX protocol. Bluetooth has a very limited range, usually around 10 metres on mobile phones, but laptops can reach up to 100 metres with powerful transmitters. The name originated with a user named ajack on esato.com. Ajack was in a bank, searching for other BT enabled devices. When he found a Nokia 7650, he sent the owner a message saying "Buy Ericsson". He called it bluejacking, and it stuck ever since. Ajack together with Droll subsequently developed a utility for Symbian UIQ called SMan which was the first bluejacking software for a smartphone. Applications designed for Bluejacking such as the leader MobiLuck or recently Nokia Sensor are launching the MoSoSo (Mobile Social Software) Market.

Some people think that the term *bluejacking* comes from *Blue*tooth and hi*jacking*. While that certainly sounds logical, a bluejacker doesn't hijack anything: he or she merely uses a feature on the sender and the recipient's device. Both parties remain in absolute control over their devices, and a bluejacker will not be able to take over your phone or steal your personal information. It should be noted that "jack" on many college campuses means "to pull a prank"- to jack a dorm would be to pull a trick or prank them. This too may be the origins of bluejacking. Bluejacking is quite harmless, but because bluejacked people don't know what is

happening, they think their phone is malfunctioning. Usually, a bluejacker will only send a text message, but with modern phones it's possible to send images or sounds as well. Bluejacking has been used in guerrilla marketing campaigns to promote advergames. But with the increase in the availability of bluetooth enabled devices, these devices have become vulnerable to virus attacks and even complete takeover of devices through a trojan horse program.

Some People consider Bluebugging as a form of Bluesnarfing. But the nature is very different. Blue Bugging was invented in 2004, barely a year after bluesnarfing started. While bluesnarfing is about stealing files from a victim's device, blue snarfing does a very different job. It takes control of a victims mobile and commands it to do what the bluebugger wishes. To put it in real times, it means a bluebugger can take control of your phone, and use it to send a message or make a call.

While early bluebugging requires the bugger(literally) used a previously paired device, new tools in bluebugging have done away with that. Which means that anyone with the right knowledge and tool can take control of your phone.

Bluesnarfing is the theft of information from a wireless device through a Bluetooth connection, often between phones, desktops, laptops, and PDAs. This allows access to a calendar, contact list, emails and text messages. Bluesnarfing is much more serious in relation to Bluejacking, but both exploit others' Bluetooth connections without their knowledge. Any device with its Bluetooth connection turned on and set to "discoverable" (able to be found by other Bluetooth devices in range) can be attacked. By turning off this feature you can be protected from the possibility of being Bluesnarfed. Since it is an invasion of privacy, Bluesnarfing is illegal in many countries.

Installing JAR Files

To install .jar file in your mobile, you can either do it using your phone suite (eg. Nokia Suite on your PC, connected with your phone) or send the file to your phone (either through bluetooth, IR, or cable) and then install it. In some phones you may need to use also the corresponding .jad file. JAD files are included in the same folder for each application folder. Uploading both jad and jar files to your mobile should make the application(s) work. More instructions at the end of the document.

Bloover II

The phone must allow installations of JAVA files.

- Advisable to carry out a single attack each time (for example BLUEBUG with only sms, then phonebook later)
- Settings need to be specified each time you start Bloover
- Change your Bluetooth identifier before using this program, as the other party may see your name. Use space (" ") so you look invisible. Another trick is to call your phone "Security Settings: press 1234" so that the target phone user will think it comes from their own phone, and use 1234 also as passcode in case it is requested.
- The fixed numbers can be modified (see below)
- If you try the attack "initiate voice call" while being ***abroad*** you should not answer it if you have set your number, as you may be charged part of the call
- Try the attacks many time, they do not always work the first time
- TRY ONLY ONE ATTACK AT A TIME, EVERY ATTACK MUST START ONLY ONE FUNCTION (eg. bluebag only with sms, helomoto only with phonebook, etc.)
- Sometimes HELOMOTO freezes, therefore it is advisable to start the attack with BLUEBAG, this way it should not freeze
- It is advisable to install mobiluck (included in the package, only for Symbian phones), as it continuously updates regarding Bluetooth devices in the vicinities

Attacks

BLUEBUG

The attack bluebug uses AT command parser that sometimes is supplied as a hidden service and is exclusively for the earpieces. Bluebug allows to read and to write the contacts of the phonebook, to read and to send sms (to send sms may not be fully operational in the program), and to call a predetermined number with the targeted mobile phone.

HELOMOTO

Its attack is very similar to the one of the Bluebug. The vulnerable phones "trust" another mobile one that has tried (and not necessarily completed) a transfer OBEX PUSH. That allows a connection with the Headset profile of the mobile and so allows an unprotected access to the AT Command Parser. Recent versions of the motorola Vseries are subject to this attack.

BLUESNARF

The Bluesnarf attack is based on the profile OBEX Push. It is connected to most OPP services and demands names of known files from the Irmc lists instead of sending .vcf files as expected. It is possible to retrieve personal information like the phonebook, the calendar

and so on. This attack works, among other phones, on Nokia 6310i, 8910i, Sony Eircsson T610 to T68i.

BLUESNARF++

Bluesnarf ++ is an attack similar to the famous Bluesnarf. The main difference is that in Bluesnarf ++ the hacker can read or write without restrictions in the filesystem. Bluesnarf ++ gives full read and write access when connected to the OBEX Push profile, without the need of pairing devices. Here the hacker can see all system files (*ls* command) and can also delete them (*rm* comand). The accessible filesystem can include memory sticks or SD card.

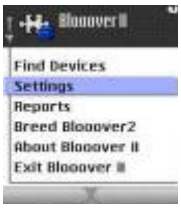
MALFORMED OBJECTS

This attack (malformed objects) is a disownment of the service used for attacking. Vulnerable mobile phones are forced to switch off when they receive "a malformed" business card for example. This causes instability of the phone parser and often causes unforeseeable behaviors (included crashing of the phone).

How to Start the Attacks

Start the program and search for devices:

After finding a device, go to options:



NOW WE CHOOSE an ATTACK

BLUEBUG:

ONLY ATTACK PHONEBOOK:

ONLY ATTACK SMS:

TO ONLY WRITE A CONTACT ON THE PHONEBOOK:

TO MODIFY CALL FORWARDING IN VICTIM's PHONE:

TO START A CALL FROM VICTIM's PHONE TOWARDS FIXED PHONE NUMBER:

HOW TO MODIFY THE FIXED PHONE NUMBERS OF THE PROGRAM:

In order to modify the number, it necessary to rename the bloover2.jar file in the computer to bloover2.zip, then go in org \ trifinite \ blooover2 extract the file e.class, copy it on the desktop, open it with a program like HHD Free Hex Editor (hexadecimal editor that can be found at http://www.jamsa.us/UserTools/free-hex-editor-neo.exe). Browse the file until you find the number and replace it with your desired destination number, overwriting exactly on the previous characters and keeping the total number length the same, and making sure that international prefix is also valid for your case. Once you are finished save the file, put the e.class file back into the bloover2.zip file, and rename the bloover2t.zip file back to bloover2.jar. Copy the jar file back into your mobile phone.

FTP_BT v1.08

Java based program.

If the language is not in English, then you need to do the following to change it into English:

go to Ftp_bt > Nastavenia > Jazyk > English and then restart the program.

About application
Program to control and read information from other phone

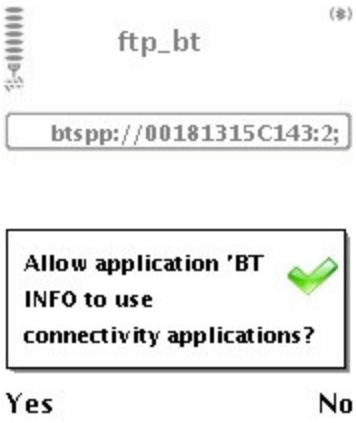
Newest version
1.08
Minimal requirements
MIDP 2.0
CLDC 1.0
JSR-82 Bluetooth **For full funcionality**
JSR-75 FileConnection
Port - IR0
Size
118822 B
More
Connect via BT/Irda
Reading SMS
Changing time/alarms
Pressing keys...
Languages in 1.08
Slovenčina
English
German
Russian
Greek

Success will depend on combination of perpetrator's phone and victim's phone. Pairing may be required on some models. If a code is asked then enter **0000**.

The program works best on SONY ERICSSON PHONES.

1)

2)



3)

4)

5)

Miyux

MiyuX is a tool that can browse and get files over Bluetooth. Works best on SE phones. These are the steps:

Steps:

1. Open Others (Not through MiyuX).
2. Create a folder Called Transferred Files.
3. Put a file in the folder what's saved on your memory card.
4. Run MiyuX.
5. Press 'more' then 'Incoming Path'
6. Open:
e:/
Then MSSEMC
Then Media Files
Then Others
Then Transferred Files
7. Press 'more' then 'Select'
(Now everything you transferred should be saved in Transferred Files and on your memory card)

STEPS:

1. press 'Scan'
2. select a device
3. a message will come up saying 'do you want to create a bluetooth connection' press 'yes'
4. a message will come up saying do you want to add 'device name' to your paired devices' press 'yes'
5. enter pin 0
6. message on other device will come up saying 'Your device name' wants to add you to paired devices' press 'ok'
7. enter pin 0
8. now press 'browse files' (Beta 5)
9. Now press these buttons via Keypad:

+// 0 - Properties
+// 1 - Create Folder
+// 2 - Up
+// 5 - Get
+// 8 - Down
+// c - Delete
+// Back

You may need to set the reading/writing java permissions, in order to avoid the continuous permission popup. The software to set this is in folder Miyux/ MobyToday_v10.zip. Instructions are contained inside.

BT_File_Explorer

Application for viewing and management of remote phones. Uses OBEX FTP. It requires CLDC 1.0, MIDP 1.0, JSR 82, JSR 75 in the host phone to work. To change into English, go to Jazyk - > Angličtina.

ISeeYourFiles

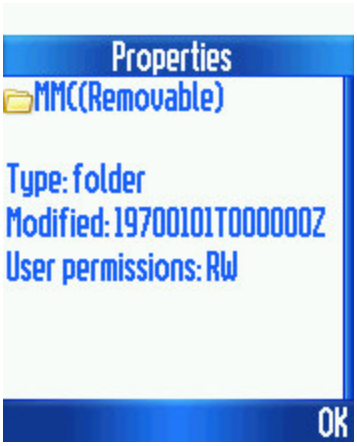
Midlet for viewing file system Bluetooth of devices. With its help it is possible to go on folders of other phones (and also computers, a handheld computer, etc.).

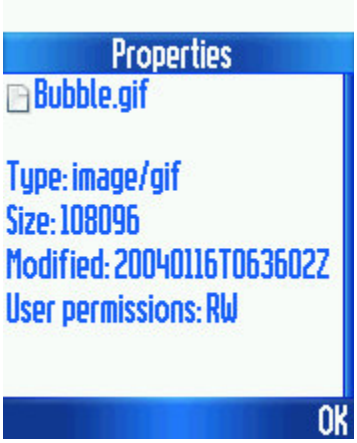
Will not work on E398/E1 phones!

Features:

1. Support JSR82 is necessary for midlet and realization of report OBEX File Transfer in the device to which connection is made.
2. At the first connection authorisation and input of a code on both phones is required.
3. At the first start midlet interrogation of names of all known devices will be made; it can take a lot of time, if the list big. If the device is inaccessible, its address will be displayed.

Screenshots:


Properties
MMC(Removable)
Type: folder
Modified: 19700101T000000Z
User permissions: RW
OK


Properties
Bubble.gif
Type: image/gif
Size: 108096
Modified: 20040116T063602Z
User permissions: RW
OK

STMBlueS

STMBlueS is a great Bluetooth browser used to manage files from one mobile on another just like you do from your PC. This small application allows you to copy images, ring tones etc form one phone on another without installing any software on the target device.

FOR SAMSUNG users:

You need to upload also the corresponding JAD for each jar that you want to upload. Both files are included in each folder. Uploading both jad and jar files to your mobile should make the application(s) work.

USB CABLE via Phone (Samsung PC Studio)
1 - Connect phone to PC
2 - Run Samsung PC Studio if not running
3 - Open file manager (Click "Manage Files")
4 - Copy .jad and .jar to "Other Files" folder on phone.
5 - Disconnect phone and go to "Other Files", run .jad file and install game/app and run it.

If this fails, then follow these steps:

First of all you will need to obtain two programmes, SOFTICKPPP and JAVA UPLOADER...both can be found here:

http://www.mobileplaytime.co.uk/help/SoftickPPP221.exe
http://www.mobileplaytime.co.uk/help/Uploader.exe

Then you need to do the following:
Firstly go to applications/java world/options in the options menu go to the networksettings and fill in this:

APN : internet
username :
password :
proxy OFF
save settings.
Then install Softick PPP 2.21 but don't run it yet.
Connect your phone with the USB cable (check with studio from samsung if it is connected right)
Enable Serial Java download - #*536963#.
Then start softickppp (not active yet!) check in the settings if ss_mdm0 is enabled. Check it.
Set softick to Active.
Enter Serial Java menu #*5737425#, and choose PPP up and then USB.
Then load a JAD file in Uploader.exe
Then go in the menu to Serial Download.
It should work fine right now.
When finished, use the code #*536961# to avoid problems(DO THIS EVERY TIME YOUR PHONE CRASHES AND RESTARTS!!)
I have found that a program will upload every other time you go through the motions, on the second attempt the phone will switch itself off when you chose USB- not to worry, just enter the #*536961# code and start again...

If you STILL have problems uploading, instructions on how to install

JAR are explained in this website (for most D and E series). Use of Cable is recommended. Follow this guide:

http://www.mobileplayground.co.uk/d500gamesinstall.htm

FOR **E900**:

After copying the jar and jad files to the Other folder on your E900, to main display and type in *#9998*5282# then go to install midlet and the password is:235282 then find the .jad file and click install

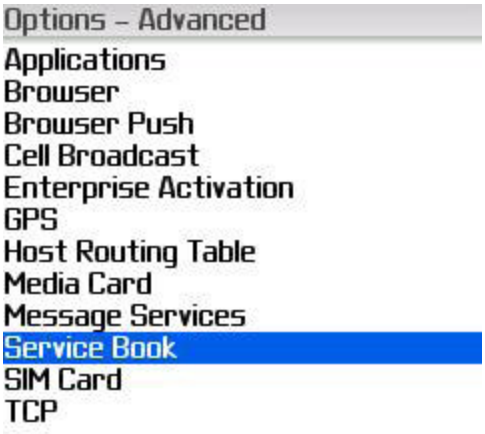
FOR Sony Ericsson users:

The best way of achieving this is to transfer the .jar and .jad files in mass storage mode into the 'other' folder on the memory card which the phone doesn't refuse; no 'operation failed' error. Then just install the .jad file from the file explorer.

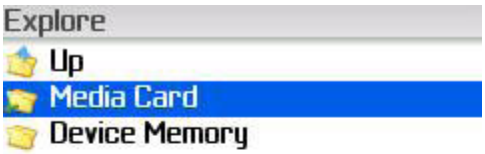
FOR Blackberry users:

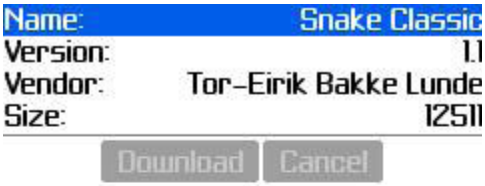
Connect the phone to your computer.
Go to: Options -> Advanced -> Media Card, press the menu key, choose "enable usb mass storage".

Note: Disregard that the screenshots are set to other options, they are just indicative



At your computer you will get a Removable Disk at My computer, browse it. Now copy the downloaded JAR / JAD files into the memory card. Then disconnect the phone from the computer, at the phone press menu button and choose: Remove Media Card (at options, advanced, media card). Press menu again and choose "install Media card. Now you need to browse to your download files at your phone. Use media manager, browse to the JAR / JAD file, select it and you should get an install option.

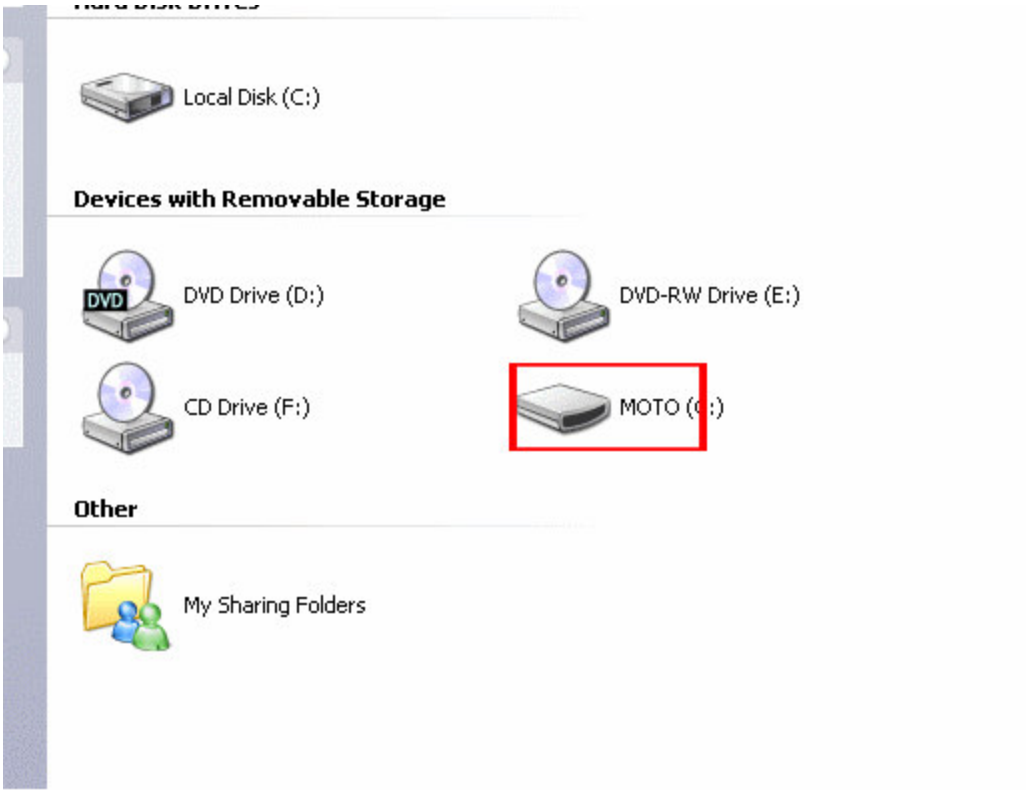




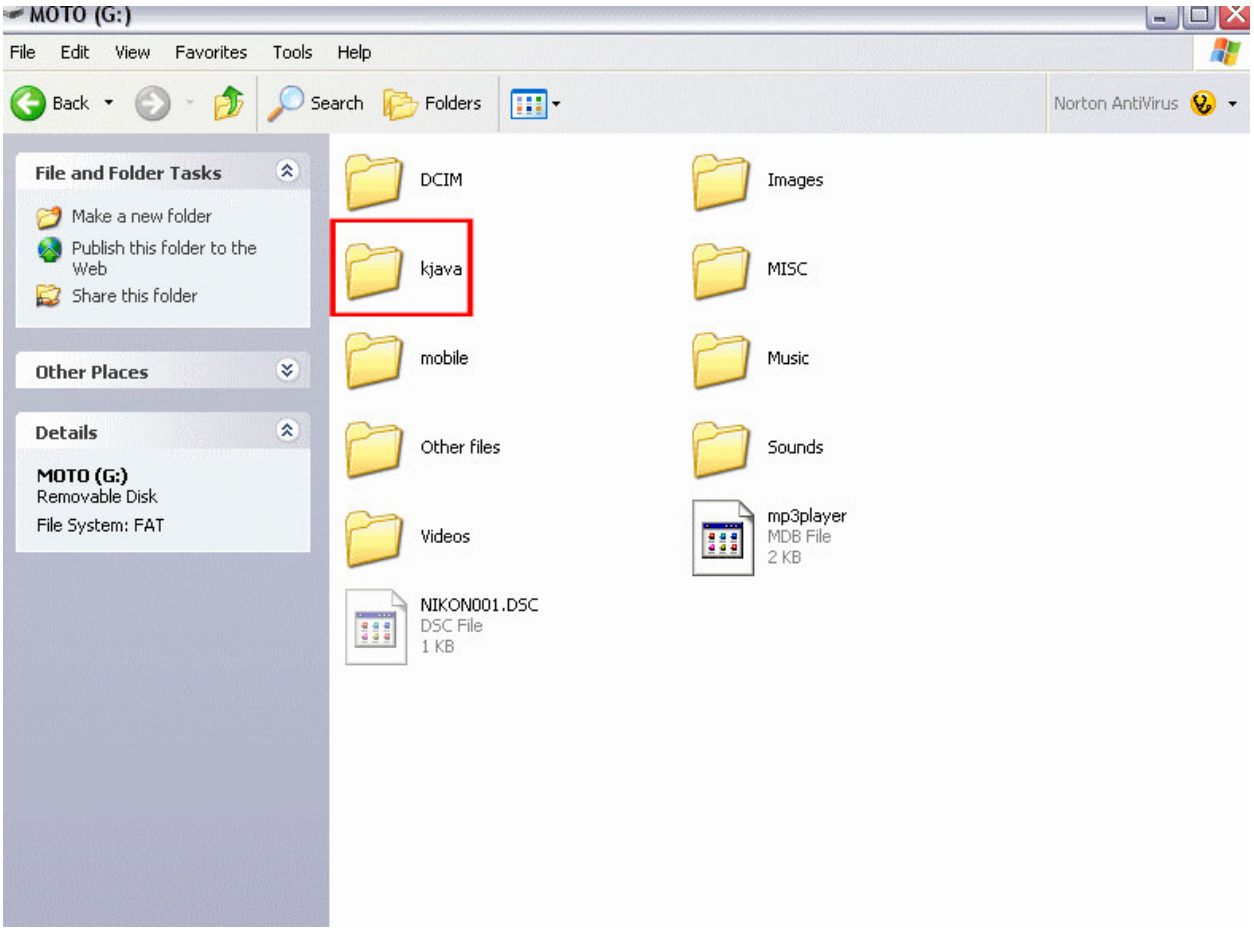
FOR MOTOROLA KRZR users:

You will need a memory card.
First off change the default connection on your phone to memory card.
settings/connection/usb settings/default connection/ change to memory card.

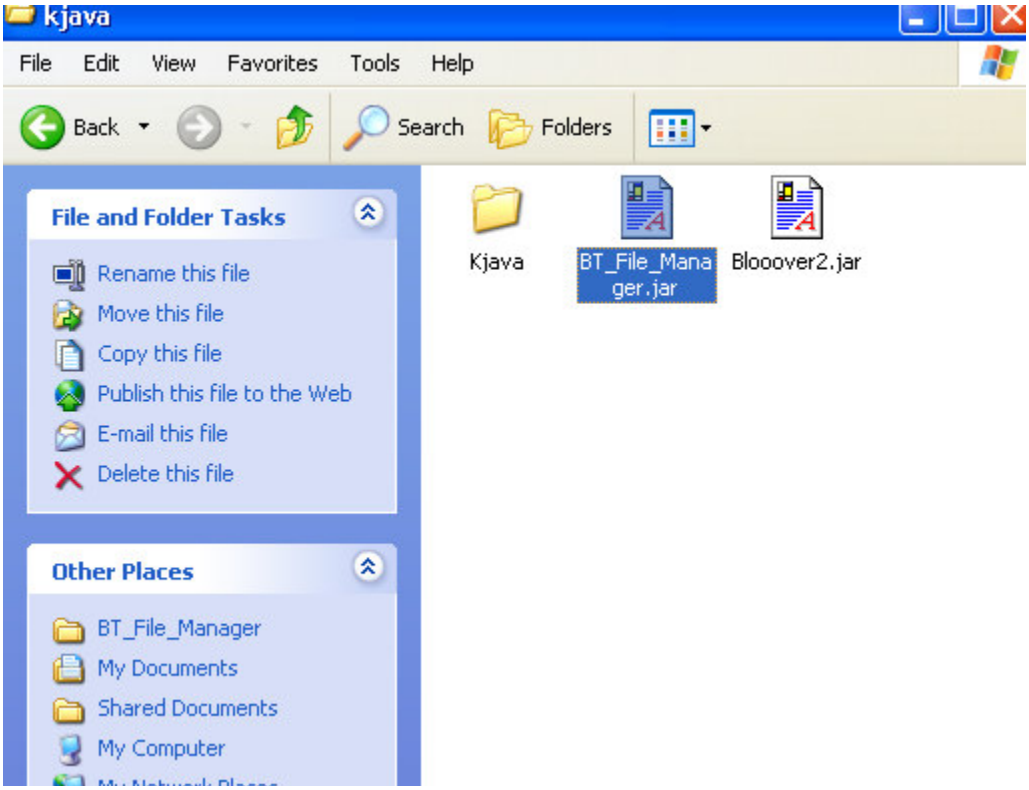
Now connect your k1 to your pc via data cable.
Goto my computer and your phone should show as a mass storage device.
Double click on your phone device



A load of folders will show up that are on your memory card.
Double click on the **kjava** folder.



Now all you have to do is drag and drop the jar files into the **kjava** folder. Two are shown as example



Now the applications are on your memory card, go into games/apps on your phone. Scroll down to install new. Click on the application you want to install, click options then install. Installation is now complete.

FOR MOTOROLA V3 users:

Using Bluetooth dongle:

Assuming you are using a Bluetooth dongle with your PC, this is the easiest way to transfer the files to your phone. These are the steps:

1. Have the phone OPEN
2. Drag and drop the jar/jad files from your PC to **OBEX object push folder** (**NOT** OBEX file transfer folder) in your mobile phone
3. When prompted, accept file transfer

If this doesn't work, you may want to switch your phone off and then back on.

Using USB Cable:

Download p2ktools and motorola drivers to get the program to work with your phone. Here is a link for both the program and drivers, scroll down the page until you find the programs:

http://www.fileden.com/files/2007/4/3/951585/P2KCommanderv3.3.zip

If you have problems with that one, try:

http://www.fileden.com/files/2007/4/3/951585/P2K-Tools-3.zip

http://www.fileden.com/files/2007/4/3/951585/P2K_Easy_Tool_v39.zip

1. Firstly, install motorola drivers, you have to do it about five times as there is a different driver each time you click on the file, so when it says installed, click on it again until they are all installed.

2. Now install P2KTools, once it is installed, link your phone to the computer with the data cable.

3. When you open P2ktools, click on "switch-to" in the top left hand corner and click p2kmode. Your phone will now link up and a little red light at the bottom of the screen will turn green.

4. Then click on the option "other features" and tick the box that says JavaApploader, then click "save options".

5.Turn off your phone then turn it back on and it will appear in the Java menu. Once this is done you need JARul from here:

http://www.fileden.com/files/2007/4/3/951585/JARul.zip

6. Install JARul

7. Go to your phone click on settings then Java settings and you should now see JavaApploader, click on it and it will then say insert cable.

8. Plug your USB cable into your phone and it will say JAVAuploader activated/ready.

9. Plug the data cable into the phone and then into your computer and then open JARuI and click on "open JAD"

10. Once you have chosen the JAD file for the application you want to upload, click on it so it opens in JARuI then click upload and it will go to your phone and then your phone will say Download.

Click on Download and the game will be installed onto phone. If JARuI doesnt work first time, change the COM3/COM4 setting in the top left hand corner of JARuI and it should work fine.

More info can be found here:

http://www.somelifeblog.com/2007/01/motorola-razr-v3-how-to-charge-and.html

http://www.mediawink.com/Java-Cell-Phone-Application-Installation-Guide.html

FOR MOTOROLA Q users:

Method 1 (if it does not work, try method 2)

Steps:

1. Download JBed Midlet manager from

http://www.fileden.com/files/2007/4/3/951585/Jbed.zip

2. Unzip on your PC and transfer the .cab file to your Q. Install the cab file (or install them using ActiveSync). If you cannot install it, then probably your phone needs to be unlocked to allow installation of third party software. These are the steps to follow (**ONLY if you cannot install the cab file because it is not signed application)**:

- Download registry editor from

http://www.fileden.com/files/2007/4/3/951585/regeditSTG.zip

- Simply put the *.zip file with the regeditSTG.exe in it with ActiveSync into a folder on your phone (but not onto the memory card).
- Unzip the file with the *.zip program that comes with your phone.
  Now start regeditSTG.exe and change the following Registry Keys:
  HKEY_LOCAL_MACHINE\Security\Policies\Policies\00001001 = 2
  -> Change the value data from 2 to 1
  HKEY_LOCAL_MACHINE\Security\Policies\Policies\00001005 = 16
  -> Change the value data from 16 to 40
  HKEY_LOCAL_MACHINE\Security\Policies\Policies\00001017 = 128
  -> Change the value data from 128 to 144
  HKEY_LOCAL_MACHINE \Security\Policies\Policies
  -> Add new value "0000101b": Dword = 1

  After you have done all these steps close Regedit STG with the task manager (TaskMan) of your phone and reboot. That's it. Your phone is now totally application unlocked.

3. Copy the jad and jar files of Bluetooth hack to your Q using Activesync. Place it in the root directory of the Q.

4. Executing the jar file should fire up JBED.

Method 2

1. Download IBM J9 from here:
CLDC 1.1MIDP 2.0 for Windows Mobile 5.0 Smartphone Edition ARM

http://www.fileden.com/files/2007/4/3/951585/CLDC1.1MIDP2.0ARM.zip

Or:
CDC 1.1 Foundation 1.1 Personal Profile 1.1 for Windows Mobile 5

http://www.fileden.com/files/2007/4/3/951585/CDC1.1Foundation1.1.zip

Older versions:
CLDC 1.1 MIDP 2.0 for Windows Mobile 5

http://www.fileden.com/files/2007/4/3/951585/CLDC1.1MIDP2.0WM5.zip

CDC 1.0 Foundation 1.0 Personal Profile 1.0 for Windows Mobile 5

http://www.fileden.com/files/2007/4/3/951585/CDC1.0Foundation1.0.zip

2. Run the .exe file on your desktop.

3. Once the file finishes, go into the directory the installer created and unzip wemewm50-sp-arm-midp20_6.1.0.20060317-111429.zip (or corresponding).

4. Inside the unzipped folders are subfolders named "bin," "lib," "doc," and "examples" Copy All but "doc" to the Q using Activesync.

5. Using the file explorer, Resco Explorer, etc., run "emulator," which is inside the "bin" folder. Run it from your Q.

6. The program will install. Just keep hitting "yes."

7. Copy the jad and jar files to your Q using Activesync. Place it in the root directory of the Q.

10. Run "emulator." It gives you the option to install a MidLet. Choose to install the .jad that you desire to install.

FOR LG Chocolate users

First you should enable java content:

Go to program files/lgcontentsbank

Edit config.ini

Change EXIST_JAVA=N to EXIST_JAVA=Y

Then you have to create a folder called java under lgcontentsbank/contents

Copy your jar and jad files to this folder, now you must edit the jad file and add this line:

MIDletX-LG-Contents: KG800

Now use the LG contents bank application , select the java icon, your games/applications should be listed now, upload and enjoy.

On your chocolate go to the settings then to connectivity. it should give you 4 options:

1. Bluetooth
2. Modem
3. Network
4. GPRS attach

Select modem. it will ask you if you would like to activate it select yes. It should remain on the connectivity screen. connect your usb cable and go to the contents bank on your pc. Select connect. there should be an extra option. Select that and press connect it should connect. After that just select your file and click download it will ask what to name it and then it will download it.