



FINFISHER™
EXCELLENCE IN
IT INVESTIGATION



FinSpyMobile 4.51

Release Notes



Copyright 2014 by FinFisher Labs GmbH, Germany
Date 2014-04-14

Release information

Version	Date	Author	Remarks
1.0	2012-02-11	mjm	Initial version
1.1	2012-02-15	lh	Updated and finalized for the v4.00 release
1.2	2012.06.18	Lh	Updated for the v4.10 release
1.3	2012.09.13	Lh	Update for the v4.20 release
1.4	2012.10.24	Lh	Update for the 4.20 hot fix
1.5	2013.02.26	Lh	Update for the 4.30 release
1.6	2013.02.28	Lh	Review and update the 4.30 release notes.
1.7	2013.04.24	Lh	FinSpy 4.31 Hot Fix Release
1.8	2013.09.02	Lh	FinSpy v4.40 Release
1.9	2014.04.14	Lh	FinSpy v4.51 Release



Table of Contents

1	OVERVIEW	4
2	SUPPORTED PLATFORMS	5
3	CHANGELOG	6
4	LIMITATIONS.....	7
4.1	PERMANENT LIMITATIONS.....	7
4.2	RELEASE LIMITATIONS	9

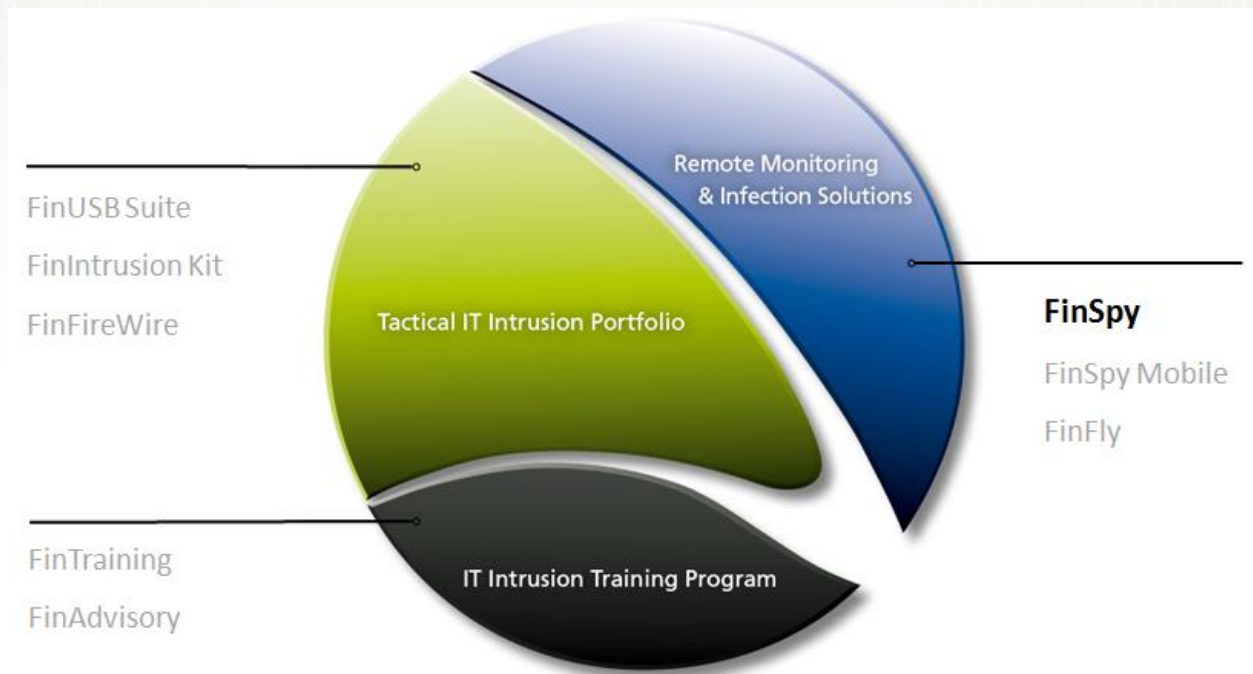


1 OVERVIEW

FinSpy Mobile is designed to help Law Enforcement and Intelligence Agencies to remotely monitor mobile phones and tablet devices and get full access to:







- **Communication:** Calls, SMS, MMS and more
- **Stored Data:** Address Book from Phone and SIM
- **Surveillance Devices:** Make silent Calls to remotely listen to the Microphone

Location: Trace device and monitor locations





2 SUPPORTED PLATFORMS

	Platform	Supported Version	Latest Version on the Market
	Android	2.x.x, 3.x.x, 4.0.x, 4.1.x, 4.2.x, 4.4.x	4.4.x
	Blackberry	5.x, 6.x, 7.x	10.1
	iOS Untethered Jailbreak required	4.3.x, 5.x, 6.x, 7.0.x	7.1
	Symbian	Symbian ^3, Anna, Belle, S60 v5.x v3.x	Symbian ^3 Anna, Belle
	Windows Mobile	6.1, 6.5	6.5
	Windows Phone	Not Supported Yet	8



3 CHANGELOG

Version 4.51		
Component	Change	Description
FinSpy Mobile iOS Target	Target Generation/Installation (enhancement)	Support for iOS 7.0.x
FinSpy Mobile iOS Target	WhatsApp Module (bug fix)	WhatsApp changed the encryption technique of the database. The module was changed appropriately to support the new encryption.
FinSpy Mobile Android Platform	Target Generation/Installation (enhancement)	Support for Android 4.4.x
FinSpy Mobile Android Platform	Microphone Module (new data collection module)	A new live session data collection module which records and sends audio frames from the microphone to the Agent software. At the end of the live session a recording is generated and stored in the Master database for later access.
FinSpy Mobile Android Target	WhatsApp Module (bug fix)	WhatsApp changed the encryption technique of the database. The module was changed appropriately to support the new encryption.

4 LIMITATIONS

This chapter covers current known limitations within the FinSpy Mobile product.

4.1 Permanent Limitations

These are technical limitations of the FinSpy Mobile system that cannot be resolved.

Component	Operating System	Description
UMTS Modem	All	<p>The FinSpy Master Call Recording server only functions with the UMTS modem that is supplied during the delivery.</p> <p>If the provider network blocks the UMTS Modem from connecting and only allows own devices, they have to have one of the following chipsets:</p> <ul style="list-style-type: none"> ▪ HUAWEI E169 <p>If neither is possible, the following features will not be functional:</p> <ul style="list-style-type: none"> ▪ Spy Call ▪ Display of Phone Number ▪ Emergency Configuration ▪ Live Tracking <p>and the following features will not be functional if there is wifi or 3G connection:</p> <ul style="list-style-type: none"> ▪ Phone Call Interception
Provider Information	All	<p>It cannot be guaranteed that the Provider name is correctly displayed as the Provider database does not contain 100% of all providers world-wide.</p>
Phone Model	All	<p>It cannot be guaranteed that the Phone Model is correctly displayed as the Phone Model database does not contain 100% of all phone models on the market.</p>
Live Tracking	All	<p>It cannot be guaranteed that the exact GPS position of the device can be shown at all times as GPS might not be available and other Location sources like position of the base station will have to be used.</p>

		<p>When the Base-Station location has to be used, the distance to the real Targets position can be several kilometers.</p>
Battery Power	All	<p>Depending on the configuration, heart-beat intervals and live sessions, the battery of the phones will empty faster than usually.</p> <p>This is usually an insignificant percentage unless lots of Call Interception and Live Tracking is done.</p>
Feature Limitations	All	<p>We cannot guarantee that all features will work on all phone models and operating systems versions at all times as there are often significant modifications by vendor and providers.</p>
Phone Call Interception	All	<p>Live Phone Call recordings can only be done when the Provider allows conference calls for the Targets device.</p>
Spy Call & Phone Call Interception	All	<p>Due to different mobile platform versions, hardware configuration of the handsets, customization of the underlying systems operated by providers and the services provided by the mobile operators, the Spy Call and Phone Call Interception also known as Voice Features might now work reliably in all the possible combinations of the variables described above.</p>
Connectivity	All	<p>When the provider does not allow direct communication for installed applications and an APN has to be configured this might prevent FinSpy Mobile targets from communicating with the FinSpy Master server unless the APN is configured.</p> <p>A database exists with common APN configurations for various providers but this database does not cover 100% of all providers world-wide.</p>

		When the APN is not inside the database, it needs to be manually configured in the Target device to ensure the device can communicate with the server.
World Maps	All	It cannot be guarantee that the Location Maps cover 100% of the world and show all areas including new constructions and such correctly.
Covert Installation	All	Typically on all mobile operating systems, the user needs to allow 1 or more pop-ups before a new application is installed.

4.2 Release Limitations

These limitations are related to the current version of FinSpy Mobile and will be addressed in future releases.

Operating System	Component	Description
All	Target Software	Full Anti-Virus/Anti-Spyware bypassing cannot be guaranteed due to regular changes in these products.
All	Mobile File Access Module	On 3G connections the Mobile File Access behaves unstable. The connection can be lost during the live session. The behavior is different from provider to provider.
Windows Mobile	Target Installation	The Target phone reboots after installation.
Windows Mobile	Target Deployment	WAP Push messages for remote installation are not supported.
Android	Target Installation	For Android 2.x platforms , after the installation of the Android target software is required a incoming/outgoing phone call or an

		incoming/outgoing SMS or the enabling/disabling of wifi/3g/Bluetooth to activate the target.
Android	Target Installation	For the Android 3.x and 4.x platforms , after the installation, an additional user interaction is required to launch the target software.
Android	SMS Communication	One of the Trojan communication channels is SMS. Due to the new security developments on Android 4.4.x the SMS sent by the master cannot be removed anymore and is visible in the incoming SMS' list.
Android	Target Removal	In the actual implementation is is not possible a complete auto removal of the target from a phone under surveillance. To completely remove the infection manual actions are required.
Android	Address Book Module	Custom fields in the address book are not recorded.
Android	Spy Call Module	The Spy Call Module is not supported on Android v2.3 and bigger.
Android	Phone Call Interception Module	Phone Call Interception Module is not supported under the Android Mobile Platform in the current version.
Android	Target Installation	The reinfection of an already infected Android target updates only the binaries. The configuration information of the existing Android infection is not overwritten with the configuration from the reinfection package.
Android	Mobile Device Camera	The Mobile Device Camera is supported only by 4.x Android Platforms. The feature is not supported on older versions of Android e.g. 2.x, 3.x.



iOS	Target Installation	The iOS target can be installed only under iOS jail broken devices.
iOS	Phone Call Interception Module	During the phone call interception if the phone processor is very busy there might be the possibility that a short ringing sound is produced.
iOS	Phone Call Interception Module	The Phone Call Interception is only possible if the Phone setting 'Call Waiting' is ON. If OFF, the conference call feature will not be active on the phone and as a consequence the Phone Call Interception will not be possible.
iOS	Spy Call Module	Spy call is possible only if the target phone is locked. If the user unlocks the phone, spy call is ended.
iOS	Email Module	The attachments can be collected and recorded only when the full email message is downloaded on the phone. By default the Mail application only downloads a small chunk of the email and the user has to manually download it.
iOS	Mobile File Access Module	The download/upload of large files is, in general, not recommended unless the device is connected to fast network (e.g. Wifi, 3G, LTE).
Blackberry	Installation	Upon installation a popup will be presented with all the rights the application needs. The user has to accept all the conditions to continue the FINSPY MOBILE Software installation
Blackberry	Visibility	When installed, the FinSpy Mobile Software will be visible in the installed applications list. When executed,

		will also be visible as a running process in the running processes list.
Blackberry	Communication	<p>The Blackberry FINSPY MOBILE Software is able to communication only using the HTTP protocol. The HTTP Tunneling feature has to be enabled on the Master and the port 80 should be opened on the Relays.</p> <p>If the time-based heartbeat is enabled, the heartbeat interval should not be set to less than 10 minutes especially on the old devices. In case of high heartbeat frequency the device might freeze and the heartbeats will not reach master with the desired frequency.</p>
Blackberry	Corrupted SMS Recordings	<p>The software might fail to interpret special character of any of the following languages correctly: Spanish language (Latin script), Portuguese language (Latin script), Turkish language (Latin script), Urdu language (Arabic and basic Latin scripts), Hindi language (Devenagari and basic Latin scripts), Bengali and Assamese languages (Bengali and basic Latin scripts), Punjabi language (Gurmukhī and basic Latin scripts), Gujarati language (Gujarati and basic Latin scripts), Oriya language (Oriya and basic Latin scripts), Tamil language (Tamil and basic Latin scripts), Telugu language (Telugu and basic Latin scripts), Kannada language (Kannada and basic Latin scripts) and Malayalam language (Malayalam and basic Latin scripts)</p> <p>Only the SMS' sent/received after the infection will be recorded.</p>
Blackberry	Address Book	Images stored with address book entries will not be recorded due to a critical problem in the vendor API.
BlackBerry	Blackberry Messenger	To record the Blackberry Messenger messages, after the infection the FINSPY MOBILE Software has to make some modification to the settings of the phone. These

		<p>modifications are done with the first opportunity when the proper conditions are met; hence there is no deterministic point of time when the recordings start.</p> <p>Group chats are currently not supported.</p> <p>File transfers will only be reported but not recorded.</p>
Blackberry	Phone Call Interception Module	<p>During the phone call interception if the phone processor is very busy there might be the possibility that a short ringing sound is produced.</p>
Blackberry	Spy Call Module	<p>During the spy call live session if the phone processor is very busy there might be the possibility that a short ringing sound is produced.</p>
Blackberry	Mobile Email Messages Module	<p>The email attachments are not recorded.</p> <p>If no Email account configured during infection the phone needs to be restarted after the Email account was set up</p>
Blackberry	Mobile Screen Capture	<p>Screen captures can only be made with a delay of at least 90 seconds.</p> <p>When closing a screen capture session make sure to close it by closing the screen capture session window only. Do not use the stop button in the middle of the window.</p>
Blackberry	Mobile File Access	<p>Access to the blackberries file system is slow due to the underlying HTTP Protocol. Responses can unfortunately take up to 3 minutes.</p> <p>Any file uploaded to the device's internal memory must not exceed 2.86MB.</p> <p>The download/upload of large files is, in general, not recommended unless the device is connected to fast network (e.g. Wifi, 3G, LTE).</p> <p>When closing a screen capture session make sure to</p>



		close it by closing the screen capture session window only. Do not use the stop button in the middle of the window.
Symbian	Target Installation	Due to the fact that the 3.0 and 3.1 Symbian versions lack of some required services which are present in newer version of the Symbian systems a separate Trojan installer is generated for these old system versions.
Symbian	Email Module	Symbian S60 5.2 5.3 cannot generate email recordings.
Symbian	Target Installation	Symbian Trojan version will be displayed as 4.50 and not 4.51.



01010 0001110001 01000101 00001110001010001 10010001010 00000110010 0010001010 000011
10001 1100000111 10111000 11100000111101110 01101110001 11101001101 1101110001 111000
10110 0011111010 01101011 00011111010011010 10 11010110 00010111001 0011010110 000111
10011 1101000110 10111001 11101000110101110 11 01110011 11101101101 1101110011 111010
01110 00110 1000 01000111 000110 1000110001 10 10001110 00010110010 0010001110 000110
00001 11001 0101 11010000 111001 0101010100 01 10100001 11101010100 1110100001 111000
01100 00100 1000 01010110 000100 1000010101 00 101011100 00010010110 00101011100 000100
10101 11101 0111 10111010 111101 0111101110 01 01110101 11111001101 1101110101 111101
01011 01010 1100 10000101 101010 1100000001 11 00001011 10101100010 1100001011 101010
11001 1001 0111 10101100 1 1001 0111101011 01 01011001 1 101001011 1101011001 1 1001
0110 0110 001 01000011 0 0110 001010000 10 10000110 0 010110000 0010000110 0 0110
10000 0001 010 00111000 0 0001 010101110 00 01110000 0 000001101 0001110000 0 0001
11110 0110 010 01101111 0 0110 010011011 10 11011110 0 010111011 0011011110 0 0110
00011 101 101 10010001 1 101 101100100 11 00100011 1 101100100 1100100011 1 101
01100 010 000 0100011 0 010 000010001 00 10001100 0 010010010 0010001100 0 010
10001 100 111 11 11 0 1 100 111 11110 01 11110001 1 101011101 1111110001 1 1
01110 011 000 00 10 1 0 011 000 00101 10 00101110 0 010100110 0 0101110 0 011
10001 100 111 1 01 0 1 100 111 01010 01 01010001 1 101001001 1 1010001 1 100
01 11 1 1 100 1 00 1 1 1 100 10001 11 10001 11 1 1 1110010 1 0001 11 1 1 1
10 00 0 0 011 11 0 0 0 0 000 01110 00 01110 00 0 0 0001101 0 1110 00 0 0 0
0 10 0 1 000 00 0 0 1 000 1000 10 1000 10 0 0 01100 0 0 000 10 0 0 1
1 01 1 0 11 11 1 0 11 0111 01 0111 01 1 1 10011 1 1 111 01 1 1 0
0 10 0 1 00 00 0 1 0 01 1000 10 1000 10 0 0 1100 0 0 000 10 0 0 1
01 1 0 1 0 1 1 0 1 1 0 1 1 0 1 1 0 1 1 0 1 1 0 1 1 0
0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0
1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1
2 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0