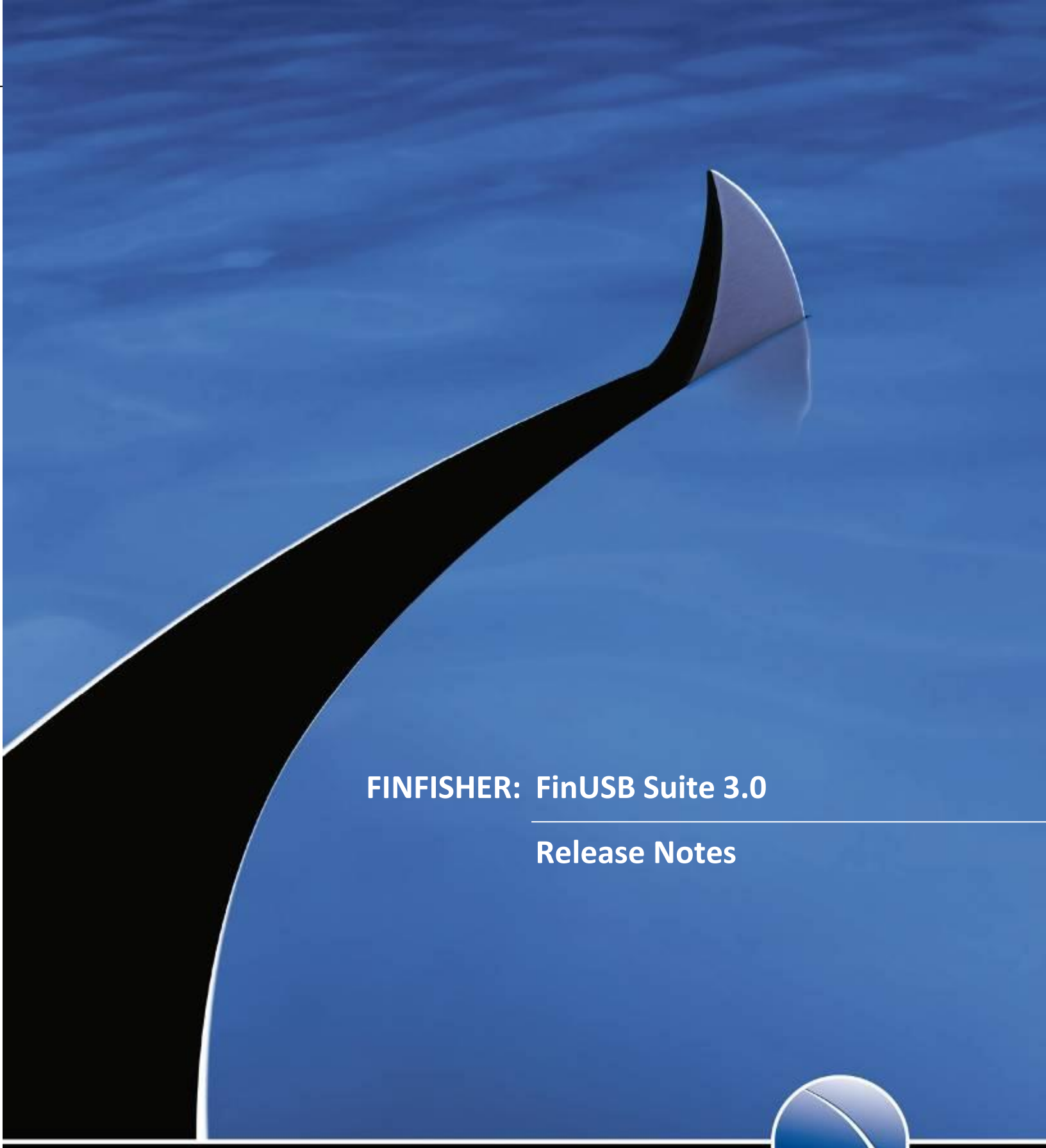


FINFISHER: FinUSB Suite 3.0

Release Notes

FINFISHER
IT INTRUSION

WWW.GAMMAGROUP.COM

Date 2011-05-20

Release information

Version	Date	Author	Remarks
1.0	2010-05-27	ah	Initial version
1.1	2010-05-31	ht	Added change log
1.2	2010-06-28	ht	New format
1.3	2010-09-20	am	Update document for version 2.7
1.4	2010-09-28	mjm	Review
1.5	2011-04-28	sb	Update document for version 3.0
1.6	2011-05-11	tm	Review

Table of Content

1 Overview 4

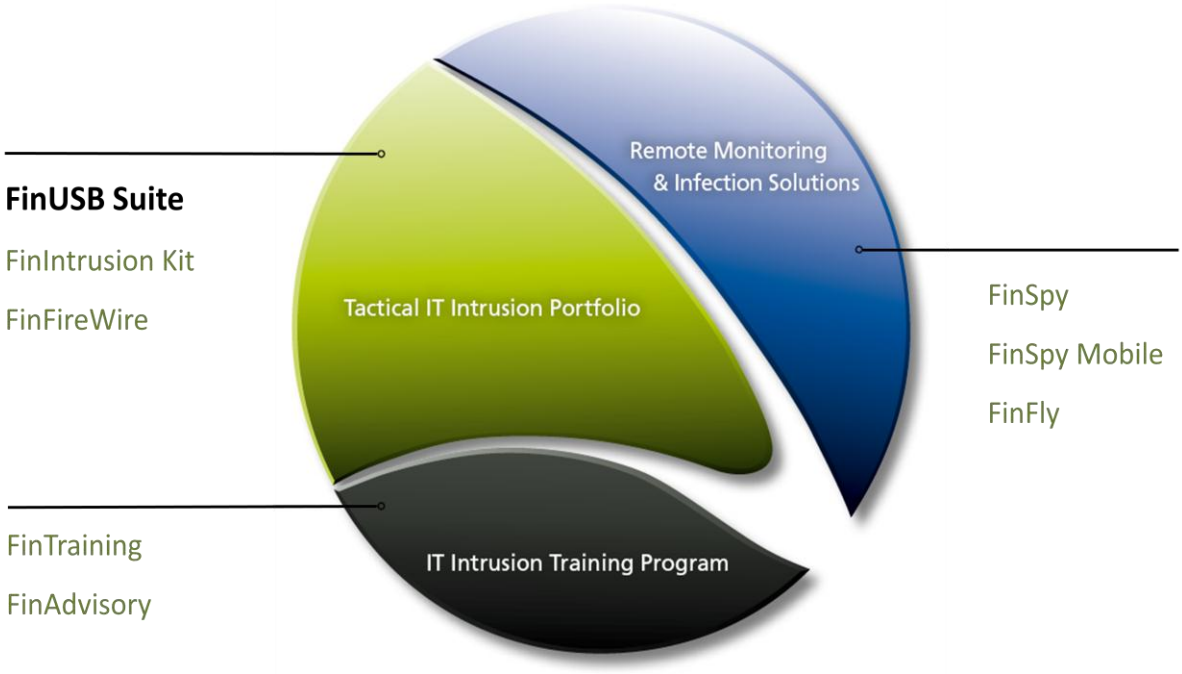
2 ChangeLog 5

3 Limitations 6

1 OVERVIEW

The *FinUSB Suite* is designed to help Law Enforcement and Intelligence Agencies to extract important information from a Target System with **little or no user intervention**.

The data is covertly extracted using special USB devices that automatically download configured data in the background while only the regular data is viewable by the Target.



2 CHANGELOG

Version: 3.0		
Component	**Change**	**Description**
Dongle System	Added support for collecting the ***Web Browser Stored Password***	This feature gathers passwords that are stored within common Browsers.
Dongle System	**Added support for 64bit systems**.	This feature enables the FinUSB Dongle to collect data also from 64bit systems.
Dongle System	***Google Chrome Cookies*** functionality	Collects all cookies from the Google Chrome browser
Headquarter	**Completely rewritten**	The GUI has been implemented completely new, using the GTK# toolkit and gtk-themes.
Headquarter	**Language Options** functionality	Added language support for several languages: German, Arabic, French, Spanish and Portuguese.

3 LIMITATIONS

This chapter covers current known limitations within the FinUSB Suite Software.

Feature	Description
FinUSB Generic	Full Anti-Virus/Anti-Spyware bypassing cannot be guaranteed due to regular changes in these products
FinUSB Generic	If the dongle removed while collecting data on 64 bit systems, the process won't exit and will hang.
Auto-Remove FinUSB Dongle	Dongle light does not switch off on Windows Vista
Auto-Remove FinUSB Dongle	Doesn't reliably work on 64bit platforms.
Windows Account Hashes	Only Windows 2000 > Service Pack 2 and Windows XP
Windows Logon Bypass	Reboot of Target System is required. The devices do not work if: • System boot is protected using a passphrase (BIOS) • Hard disk is prioritized at boot and BIOS access is protected by password • Hard disk is encrypted
Data Accessibility	The information the *FinUSB Dongle* is able to obtain is subject to the data being: • available on the Target System • accessible by the current User account
Automated Execution	In case the automated execution (see table) does not work, a manual start of the FinUSB Dongle software is required
Automated Execution, **Shortcut for Manual Start**	Targets that have the *Embassy Trust Suite* installed will require that the FinUSB Dongle software is started manually by running the ***LaunchU3.exe*** in the ***System*** folder.
Data Gathering Files	Only files smaller than 4GB will be gathered
Data Gathering Passwords	LSASecretsDump doesn't work on 64bit systems.
Data Gathering Passwords	Instant Messenger account – no support for Trillian on Windows 2000 and Windows 7
Data Gathering Passwords	Instant Messenger account – no support for GoogleTalk on

	Windows Vista
Data Gathering Passwords	Instant Messenger account – no support for Yahoo Messenger 8.x and Yahoo Mail! on Windows 2000, Windows XP, Windows Vista
Data Gathering Passwords	Email account configuration – no support for Windows Live Mail on Windows XP
Data Gathering Passwords	Network login passwords for remote computers that are stored locally- no support for Windows Vista and Windows 7, need to be system administrator on all systems.
Data Gathering Network	Known Wireless LAN WEP and WPA keys – no support for Windows 2000, need to be system administrator on all systems.
Data Gathering Network	Installed Windows Updates/Hotfixes – no support for Windows Vista and Windows 7
Software Update	Versions 2.6 and lower will not be removed on installing the newest Version
Report	Some Arabic/Chinese Characters are not displayed correctly in the Report (e.g. Windows updates description)

GAMMA INTERNATIONAL
United Kingdom

Tel: +44 - 1264 - 332 411
Fax: +44 - 1264 - 332 422

info@gammagroup.com

WWW.GAMMAGROUP.COM