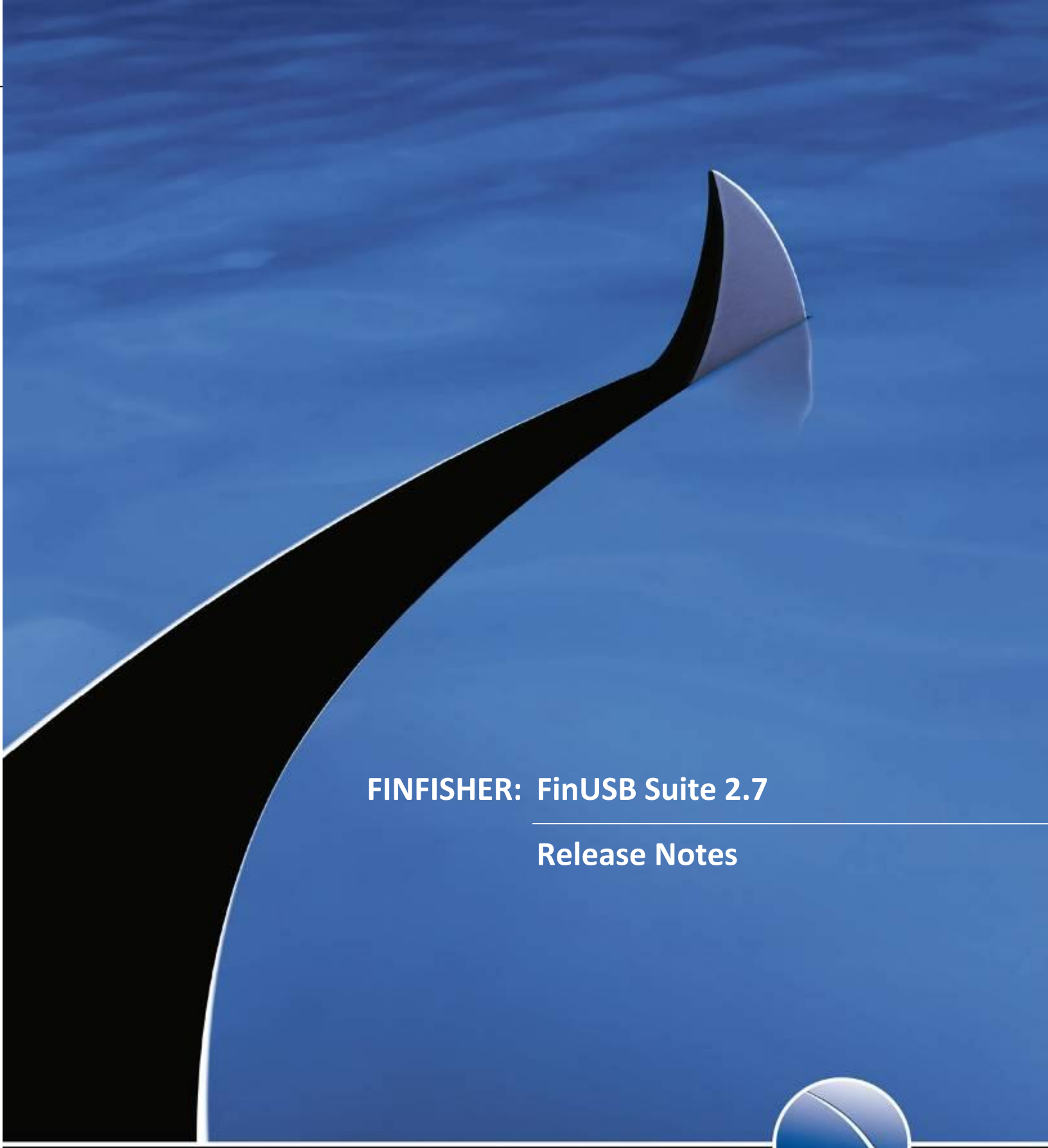


FINFISHER: FinUSB Suite 2.7

Release Notes

FINFISHER
IT INTRUSION

WWW.GAMMAGROUP.COM

Date 2010-09-28

Release information

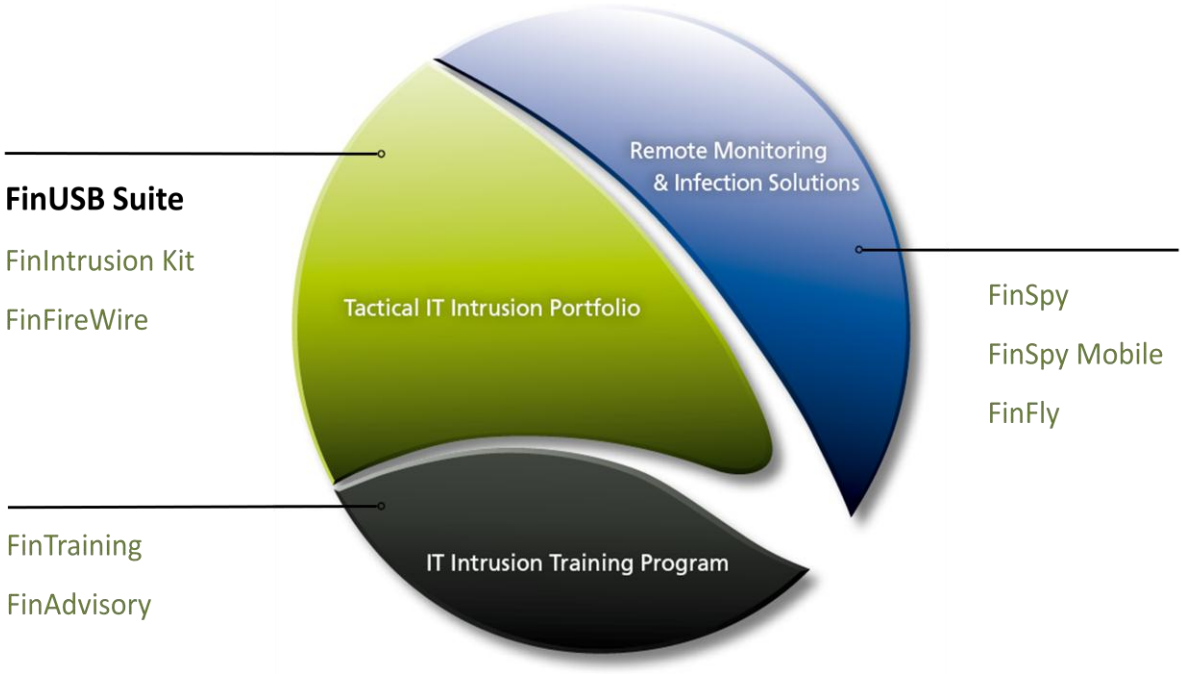
Version	Date	Author	Remarks
1.0	2010-05-27	ah	Initial version
1.1	2010-05-31	ht	Add changelog
1.2	2010-06-28	ht	New format
1.3	2010-09-20	am	Update document for version 2.7
1.4	2010-09-28	mjm	Review

Table of Content

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: 2.7		
Component	**Change**	**Description**
Dongle System	Added support for searching on R***emovable Devices***	If you select the location “All disks” in the generic file search tab, all local disks **and** removable devices will be scanned
Dongle System	Added support for searching the ***Temporary Directory***	This feature gathers all selected file types from the user’s temporary directory
Dongle System	Added support for gathering ***Opera Passwords***	This feature decrypts the content of the Opera web browser password file and displays the list of all web site passwords stored in this file
Dongle System	***USB Devices and History*** functionality	This feature shows all USB devices connected to the target, as well as all USB devices that were previously used
Dongle System	***Search Queries History*** functionality	This feature scans the cache and history files of the target Web browser, and locate all search queries that were made with the most popular search engines (e.g. Google, Yahoo and MSN) and with popular social networking sites (e.g. Twitter, Facebook, MySpace)
Headquarter	Modified the ***Generic Files Search*** section	The GUI mask offers a new predefined search location named “Temporary Directory”. The search can be tuned for several file types
Headquarter	Modified the ***Configure Dongle*** dialog	Added configuration controls in order to support the new features: “Opera Passwords”, “USB Devices” and “Search Queries History”

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
Auto-Remove FinUSB Dongle	Dongle light does not switch off on Windows Vista
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	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
Data Gathering Network	Known Wireless LAN WEP and WPA keys – no support for Windows 2000
Data Gathering Network	Installed Windows Updates/Hotfixes – no support for Windows Vista and Windows 7

GAMMA INTERNATIONAL
United Kingdom

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

info@gammagroup.com

WWW.GAMMAGROUP.COM