

SYNGRESS

上海交通大学图书馆



E1261391

DATA HIDING TECHNIQUES IN WINDOWS OS

A PRACTICAL APPROACH TO INVESTIGATION AND DEFENSE

Nihad Ahmad Hassan | Rami Hijazi

Data Hiding Techniques in Windows OS

A Practical Approach to Investigation and Defense

Nihad Ahmad Hassan

University of Greenwich
IT Security and Digital Forensics Consultant;
Founder of www.DarknessGate.com

Rami Hijazi

University of Liverpool
Information Security Consultant;
General Manager, MERICLER Inc.,
Candela Drive, Mississauga, Ontario, Canada

Helvi Salminen

Technical Editor



AMSTERDAM • BOSTON • HEIDELBERG • LONDON • NEW YORK • OXFORD • PARIS
SAN DIEGO • SAN FRANCISCO • SINGAPORE • SYDNEY • TOKYO

Syngress is an imprint of Elsevier

SYNGRESS

Syngress is an imprint of Elsevier
50 Hampshire Street, 5th Floor, Cambridge, MA 02139, United States

Copyright © 2017 Elsevier Inc. All rights reserved.

No part of this publication may be reproduced or transmitted in any form or by any means, electronic or mechanical, including photocopying, recording, or any information storage and retrieval system, without permission in writing from the publisher. Details on how to seek permission, further information about the Publisher's permissions policies and our arrangements with organizations such as the Copyright Clearance Center and the Copyright Licensing Agency, can be found at our website: www.elsevier.com/permissions.

This book and the individual contributions contained in it are protected under copyright by the Publisher (other than as may be noted herein).

Notices

Knowledge and best practice in this field are constantly changing. As new research and experience broaden our understanding, changes in research methods, professional practices, or medical treatment may become necessary.

Practitioners and researchers must always rely on their own experience and knowledge in evaluating and using any information, methods, compounds, or experiments described herein. In using such information or methods they should be mindful of their own safety and the safety of others, including parties for whom they have a professional responsibility.

To the fullest extent of the law, neither the Publisher nor the authors, contributors, or editors, assume any liability for any injury and/or damage to persons or property as a matter of products liability, negligence or otherwise, or from any use or operation of any methods, products, instructions, or ideas contained in the material herein.

Library of Congress Cataloging-in-Publication Data

A catalog record for this book is available from the Library of Congress

British Library Cataloguing-in-Publication Data

A catalogue record for this book is available from the British Library

ISBN: 978-0-12-804449-0

For information on all Syngress publications
visit our website at <https://www.elsevier.com/>

		Working together to grow libraries in developing countries
www.elsevier.com • www.bookaid.org		

Publisher: Todd Green

Acquisition Editor: Chris Katsaropoulos

Editorial Project Manager: Anna Valutkevich

Production Project Manager: Priya Kumaraguruparan

Designer: Mark Rogers

Typeset by TNQ Books and Journals

Data Hiding Techniques in Windows OS

**To my mom, Samiha, thank you for everything.
Without you, I'm nothing.**

Nihad A. Hassan

Biography

Nihad A. Hassan is an independent computer security and forensic consultant. He has been actively conducting research on computer forensic techniques for more than 8 years, focusing on techniques in Windows® OS, especially digital steganography techniques.

Nihad has completed numerous technical security consulting engagements involving security architectures, penetration testing, Windows® OS diagnostic reviews, disaster recovery planning, and computer crime investigation.

He has written thousands of pages of technical documentation for different global companies in the IT and cybersecurity fields in both Arabic and English. His writing style highlights information that is simplified and presented in an easy manner, which gives him an extensive reputation in this field.

Nihad believes that security concerns are best addressed by well-prepared and security-savvy individuals. Nihad also enjoys being involved in security training, education, and motivation. His current works are focused on network security, penetration testing, computer forensic and antiforensic techniques, and web security assessment. Nihad has a BSc honors degree in computer science from the University of Greenwich, United Kingdom.

You can reach Nihad through:

InfoSecurity blog	http://www.DarknessGate.com
Personal website	http://www.ThunderWeaver.com
Email	nihadhas@gmail.com



Rami Hijazi is the general manager of MERICLER Inc., an education and corporate training firm in Toronto, Canada. Rami is an experienced IT professional who lectures on a wide array of topics, including object-oriented programming, Java, eCommerce, Agile development, database design, and data handling analysis. Rami also works as consultant to Cyber Boundaries Inc., where he is involved in the design of encryption systems and wireless networks, intrusion detection, and data breach tracking, as well as providing planning and development advice for IT departments concerning contingency planning.



Helvi Salminen has worked full-time in information security since June of 1990. Prior to her security career, she had 12 years of experience in systems development. Helvi values lifelong learning and knowledge sharing, which she has practiced by studying and teaching in lifelong learning security education programs at Aalto University and by speaking at security conferences. She was awarded CISO of the year 2014 in Finland by the Finnish Information Security Association.

Preface

ABOUT THIS BOOK

In brief, this book presents a wide array of techniques that could be used to hide digital data under the Windows® OS, in addition to different steganographic techniques to conceal data in multimedia files. The book also presents different ways to investigate and explore hidden data inside digital files and the Windows® OS file structure.

The main focus of this book is teaching Windows® users how they can exploit data hiding techniques within Windows® OS and multimedia files to secure their data and communications. Today, the demand for privacy is a major concern for computer users. This book will help those users learn vast arrays of techniques to better secure their privacy by teaching them how to conceal their personal data. Users also learn how to use different cryptographic anonymity techniques to conceal their identity online.

Many books on data hiding techniques are available in the market. However, none of these books have a practical approach such as this one. The data hiding topic is usually approached in most books in an academic way with long math equations about how each hiding technique algorithm works behind the scene. These books are usually targeted for people who work in the academic arenas. We need a book that teaches professionals and end users alike how they can hide their data and discover the hidden ones using a variety of ways, under the most used operating system on earth, Windows®.

This book will entertain the reader by following a simple writing style. It focuses on approaching the data hiding topic practically and offers plenty of screen captures for each technique used. The book is written as a series of tutorials (you can consider it a cookbook full of delicious recipes, with each task (hence recipe) presenting a different hiding technique). Book contents are completely practical; a user can read a task and then implement it directly on his or her PC. Relevant theoretical information will be presented to enrich the user about terms used in each hiding technique, making this book quite informative for different user populations. Techniques discussed in this book cover all Windows® versions, from Windows® XP to Windows®10.

TARGET AUDIENCE

The topic of digital data hiding is quite stimulating. This book will be valuable for the following user groups:

1. Computer forensic investigators
2. Law enforcement officers and border protection agencies
3. Intelligence services staff
4. Human rights activists
5. Journalists
6. IT professionals
7. Computing and information technology students
8. Business managers in all industries
9. End users

Any computer user will benefit from this book! All people like to obscure their personal data using simple methods and they are eager to become more computer literate and able to override mass surveillance programs deployed by many governments to monitor online traffic. This book will explain these ideas in an easy-to-follow manner, making complex technical ideas easy to assimilate by nontechnical folks.

SUMMARY OF CONTENTS

In the following you will find a brief description about each chapter's contents.

Chapter 1, Introduction and Historical Background:

This chapter talks about the history of data hiding since old civilizations, and presents historical events related to this subject. This chapter begins by listing old cryptographic techniques used in ancient times to secure message transmission, and then discusses modern steganography and encryption techniques used in today's world.

Chapter 2, Data Hiding Using Simple Methods: In this chapter, we present many simple techniques that average computer users can use to hide their personal data. The techniques presented in this chapter can be used without using any third-party tool.

Chapter 3, Data Hiding Using Steganographic Techniques: In this chapter, we present different steganographic techniques to conceal our data in multimedia files. We demonstrate how we can use different tools and techniques to

conceal data inside e-documents, web files, images, and audio and video files. A brief discussion of how each technique works behind the scene is also included to make this chapter both informative and practical.

Chapter 4, Data Hiding Under Windows® OS File Structure: This is an advanced chapter that shows how we can exploit the Windows® OS NTFS file structure to conceal our data. Many data hiding techniques in this chapter can be performed without using third-party tools, mostly by exploiting Windows® OS's own files. This chapter gives insight on how hackers can use data hiding techniques to launch sophisticated attacks against computer systems and private networks.

Chapter 5, Data Hiding Using Encryption Techniques: This chapter presents different techniques to protect your private data using encryption. It covers encrypting a Windows® partition, data disk, and files in addition to emails, IMs, and VOIP calls. Attacks against full disk encryption and countermeasures also are described in this chapter. This chapter also covers using cryptographic anonymity techniques to anonymize your online communications, making them untraceable.

This chapter can be read alone; in fact, you can consider it as a minibook dedicated to teaching you practical tricks and guidelines for online risks and steps to protect yourself against cyberattacks through encryption and cryptographic anonymity tools.

Chapter 6, Data Hiding Forensics: This chapter is the reverse of Chapters 3 and 4 as it looks into how data hiding

forensics investigate different methods to detect concealed data in digital files and Windows® file structure. In addition to this the chapter illustrates how we can investigate Windows®-based machines to determine whether any steganography tools have been installed or used.

Chapter 7, Antiforensic Techniques: This chapter discusses techniques and gives advice on eliminating your tracks when using steganography tools to conceal secret data. It also presents ways to prevent general computer forensic tools from investigating and exploring your hidden data. This chapter is the reverse of , Chapter 6.

Chapter 8, Future Trends: We discuss future trends and advancements in digital data hiding and how new IT technology affects this subject.

COMMENTS AND QUESTIONS

To comment or ask technical questions about this book, send email to nihadhas@gmail.com.

We are going to publish a webpage for this book that lists additional references, tools, examples, and other information. You can access this page through the author's Info-Sec portal: <http://www.DarknessGate.com>.

For more information about Syngress books go to http://store.elsevier.com/Syngress/IMP_76/.

Acknowledgments

When I first thought about creating my first book, Rami Hijazi was the first person who came to my mind when seeking advice. I consider him the best man in the field. His precious feedback has always enlightened my road. Even after years of working together, I am constantly surprised by his amazing intelligence, innate humility, and genuine friendship. Looking forward to working with you again on another book, Rami!

It is with a deep sense of appreciation that I want to thank my technical reviewer Helvi Salminen. Helvi plays two roles in this book; first as a proposal reviewer she provided me with excellent feedback. The second role is of course reviewing this text technically. Without her excellent feedback and dedicated work, producing this text would have been difficult. Thank you very much, Helvi; I'm looking forward to working with you again on another book.

Book acquisition editor Chris Katsaropoulos, thank you for believing in my book's idea and for your moral encouragement before and during the writing process. Hope to work with you again.

Book Editorial Project Manager Anna Valutkevich, thank you for your diligent support during the writing process. You make authoring this book a joyful journey! Hope to work with you again, Anna!

Mary Ide, thank you very much for your feedback at the initial stage of book development. Your encouragement gave me a boost to proceed with this project.

Kandy Zabka, I highly appreciate your encouragement and practical advice on my book's proposal. Your initial feedback has guided my way all the way through the end.

I want to thank Jodi L. Colburn for her precious help at the start of my career as a computer security professional. I will always remember your encouragement and faithful advice.

I want to thank all the Syngress staff who worked behind the scenes to make this book possible and ready for launch. I hope you will continue your excellent job in creating highly valued computer security books. You are simply the best in this field.

Naturally, I'm saving the best for last. During this book I use many photos of a baby boy to describe digital steganographic techniques in images. These photos are of my brother's son Omran. I want to thank this little baby boy for adding a pleasant touch to the technical script. I hope he will become an author like his uncle when he grows up!

Nihad A. Hassan

Contents

Biography	xi	Renaming Files	27
Preface	xiii	Matching File Signatures and File Extensions	27
Acknowledgments	xv	Hiding Data in Compressed Files	28
		Hiding Data Through File Splitting	31
		Hiding Data in Microsoft® Office Documents	33
		Hidden Text	34
		Hidden Data Within Document Attributes (Metadata)	34
		White Font	35
		Hiding Data by Exploiting OLE Structured Storage	35
		Self-Encrypt MS Office® Document	37
		Hiding Inside MS Excel® Spreadsheet	38
		Data Hiding Inside Image Attributes (Image Metadata)	40
		Summary	43
		References	43
		Bibliography	43
1. Introduction and Historical Background		3. Data Hiding Using Steganographic Techniques	
Introduction	1	Introduction	45
Classical Cipher Types	2	Text Steganography	46
Substitution Cipher	2	Format-Based Steganography	46
Transposition Cipher	8	Random and Statistical Generation	47
Other Ciphers and Codes	9	Linguistic-Based Methods	48
Difference Between Substitution and Transposition Cipher	10	Hiding Inside MS Office® Documents Based on OOXML File Format	49
Practicing Old Ciphers Using Modern Computing	12	Webpage Text Steganography	64
Modern Cryptography Systems	12	Hiding Secret Messages Inside Twitter Updates	67
Secret Key Cryptography	13	Image Steganography	68
Public Key Cryptography	13	Digital Image Basic Concepts	69
Digital Signature	14	Image Steganographic Techniques	73
Cryptographic Hash Function	14	Digital Media Steganography Tools	81
Steganography	15	Data Hiding Inside Audio Files	81
What Is Steganography?	15	Audio Files Basic Concepts	82
Comparing Steganography and Cryptography	15	Audio Steganography Types	84
Steganography Types	15	Data Hiding Using Other Digital Media Types	90
Watermarking	20	Data Hiding Inside PDF Documents	91
Watermarking Types	20	Data Hiding Inside Program Binaries	94
Compare Steganography and Watermarking	21		
Anonymity	21		
Summary	21		
References	21		
Bibliography	22		
2. Data Hiding Using Simple Methods			
Introduction	23		
Bit-Shifting Data Hiding	23		
Hiding Data Inside Rich Text Format Documents	26		

Summary	95	Other Security Distributions	138
References	95	Advice When Using Security	
Bibliography	95	Operating Systems	138
		Portable Stick Computer	140
4. Data Hiding Under Windows® OS File Structure		Disk Encryption	140
Introduction	97	Encrypting Partitions Using BitLocker	141
Data Hiding Using Alternate Data Stream	98	Creating Encrypted Vaults	145
What Is the New Technology File System?	98	Single File Encryption	159
What Is an Alternate Data Stream?	98	Cloud Storage Encryption	161
How Can We Use Alternate Data Streams to Hide Files?	98	Discussion of Security Level in Disk Encryption	162
Hiding Executable Code in Alternate Data Stream Files	100	Anonymize Your Location Online	169
Important Notes About Using Alternate Data Stream in Hiding Files	102	Using the TOR Browser	169
How to Delete Alternate Data Stream Files	104	Virtual Private Networks	176
Detecting Alternate Data Stream Files	104	SSH Tunneling	179
Data Hiding Using Stealth Alternate Data Stream	104	Using Proxy Server	179
Hiding Data Inside Windows®	106	Anonymous Search Engine	180
Restoration Points	106	Web Browser Privacy Add-Ons	181
Hiding Data Inside Windows® Registry	109	Secure Anonymous File Sharing	183
Hiding in a File's Slack Space	112	Encrypting Email Communications	185
Understanding Hard Disk Drives	112	Email Encryption Using Gpg4Win	186
File Allocation Table	114	Open PGP Encryption for Webmail	
Hidden Partitions	117	Using the Mailvelope Browser Extension	190
Hidden Partitions Under Windows® OS	118	Secure Web Mail Providers	192
Creating a Hidden Partition Within a USB Zip Drive	118	Encrypt Instant Messaging, Video Calls, and VOIP Sessions	195
Data Hiding Within Master File Table	123	What Are the Risks?	195
Data Hiding in Disk Bad Blocks	127	Off-the-Record-Messaging and Pidgin	195
Data Hiding Under Computer Hardware Level	128	A Secure Video Calling Service	
Data Hiding Inside Host Protected Area	129	Using Gruveo	198
Hiding Data in Device Configuration Overlay	130	A Secure Anonymous Calling Service	
Summary	131	Using GHOST CALL	199
References	131	Retroshare Secure Social Platform	199
Bibliography	132	TOR Messenger	199
		Complete Anonymous IM Using Ricochet	201
5. Data Hiding Using Encryption Techniques		Create and Maintain Secure Passwords	201
Introduction	134	Password Best Practice	201
Security Awareness Corners	134	Password Generation Tools	202
Human Security	134	Password-Saving Techniques	202
Device Security	134	Password Manager Tools	202
Message Security	135	Miscellaneous Security Hints and Best Practices	203
Network Security	135	Summary	204
Anonymous Operating System	135	References	204
Tails	135	Bibliography	205
Ubuntu Privacy Remix	137		
		6. Data Hiding Forensics	
		Introduction	207
		Understanding Computer Forensics	208
		Computer Forensic Process	208
		Differences Between Computer Forensics and Other Computing Domains	209
		The Need for Digital Evidence	209

Steganalysis	210	Registry Antiforensics	276
Steganalysis Methods	210	Disable Windows Hibernation	278
Destroying Hidden Data	211	Disable Windows Virtual Memory (Paging File)	278
Steganalysis of Digital Media Files	211	Disable System Restore Points and File History	280
Text Document Steganalysis	211	Disable Windows Thumbnail Cache	281
Image Forensics	214	Disable Windows Prefetch Feature	281
Audio Forensics	219	Disable Windows Logging	285
Video Forensics	219	Disable Windows® Password Hash Extraction	285
Digital Files Metadata Forensic	222	Clearing Digital Footprints	287
Windows Forensics	227	Live CDs and Bootable USB Tokens	287
Capture Volatile Memory	228	Virtual Machines	288
Capture Disk Drive	231	Using Portable Applications	289
Deleted Files Recovery	233	Direct Attack Against Forensic Software	289
Windows Registry Analysis	239	Summary	289
Forensic Analysis of Windows Prefetch Files	249	References	289
Windows Minidump Files Forensics	250	Bibliography	290
Windows Thumbnail Forensics	250		
File Signature Analysis	252	8. Future Trends	
File Attributes Analysis	252	Introduction	291
Discover Hidden Partitions	252	The Future of Encryption	292
Detect Alternative Data Streams	255	Data Stored in Cloud Computing	293
Investigating Windows Volume Shadow Copy	255	Virtualization Technology	293
Virtual Memory Analysis	257	Data Hiding in Enterprise Networks	294
Windows Password Cracking	259	Data Concealment	294
Host Protected Area and Device Configuration Relay Forensic	262	Data Leakage Prevention	295
Examining Encrypted Files	262	Streaming Protocols	295
Summary	264	Wireless Networks and Future Networking Protocols	296
References	265	Data Hiding in Mobile Devices	297
Bibliography	265	Anonymous Networks	297
		Summary	298
7. Antiforensic Techniques		References	298
Introduction	267	Bibliography	298
Antiforensics Goals	268		
Data Hiding General Advice	268	Index	299
Data Destruction	268		
Hard Disk Wiping	269		
Manipulating Digital File Metadata	272		
Windows Antiforensics Techniques	275		
Configure Windows for Better Privacy	275		
Disable Recycle Bin	276		

