

Practical Paranoia™ macOS 10.13

Security Essentials

- ✓ The Easiest
- ✓ Step-By-Step
- ✓ Most Comprehensive
- ✓ Guide To Securing Data and Communications
- ✓ On Your Home and Office macOS Computer

Marc L. Mintz, MBA-IT, ACTC, ACSP

TPP
The Practical Paranoid

Practical Paranoia: macOS 10.13 Security Essentials

Author: Marc Mintz

Copyright © 2016, 2017 by The Practical Paranoid, LLC.

Notice of Rights: All rights reserved. No part of this document may be reproduced or transmitted in any form by any means without the prior written permission of the author. For information on obtaining permission for reprints and excerpts, contact the author at marc@thepracticalparanoid.com, +1 888.504.5591.

Notice of Liability: The information in this document is presented on an *As Is* basis, without warranty. While every precaution has been taken in the preparation of this document, the author shall have no liability to any person or entity with respect to any loss or damage caused by or alleged to be caused directly or indirectly by the instructions contained in this document, or by the software and hardware products described within it. It is provided with the understanding that no professional relationship exists and no professional security or Information Technology services have been offered between the author or the publisher and the reader. If security or Information Technology expert assistance is required, the services of a professional person should be sought.

Trademarks: Many of the designations used by manufacturers and sellers to distinguish their products are claimed as trademarks. Where those designations appear in this book, and the author was aware of a trademark claim, the designations appear as requested by the owner of the trademark. All other product names and services identified in this document are used in editorial fashion only and for the benefit of such companies with no intention of infringement of trademark. No such use, or the use of the trade name, is intended to convey endorsement or other affiliation within this document.

Editions: v1.0 20170918 • v1.01 20170923 • v1.1 20171001

Cover design by Ed Brandt

ISBN-10: 1976513650

ISBN-13: 978-1976513657

Dedication

*To Candace,
without whose support and encouragement
this work would not be possible*

Contents At A Glance

Dedication.....	3
Contents At A Glance.....	5
Contents In Detail.....	7
1 Thank You for Studying Practical Paranoia!	19
2 Introduction	21
3 Data Loss.....	35
4 Passwords.....	65
5 System and Application Updates	107
6 User Accounts.....	121
7 Storage Device.....	153
8 Sleep and Screen Saver.....	165
9 Malware.....	171
10 Firewall.....	211
11 Firmware Password	223
12 Lost or Stolen Device	227
13 Local Network.....	251
14 Web Browsing.....	297
15 Email.....	379
16 Apple ID and iCloud.....	483
17 Documents	505
18 Voice, Video, and Instant Message Communications	555
19 Internet Activity.....	579
20 Social Media	635
21 When It Is Time to Say Goodbye	705
22 Miscellaneous.....	717
23 The Final Word.....	727
macOS 10.13 Security Checklist.....	729
Revision Log.....	735
Index	737
Mintz InfoTech, Inc. when, where, and how you want IT	743
Practical Paranoia Workshops & Books	744

Contents In Detail

Dedication.....	3
Contents At A Glance.....	5
Contents In Detail.....	7
1 Thank You for Studying Practical Paranoia!	19
2 Introduction	21
2.1 Who Should Study This Course.....	22
2.2 What is Unique About This Course and Book	23
2.3 Why Worry?	25
2.4 Reality Check	26
2.5 About the Author.....	28
2.6 Practical Paranoia Updates.....	29
2.7 Practical Paranoia Paperback Book Upgrades.....	30
2.8 Practical Paranoia Kindle Updates	31
2.9 Practical Paranoia Online Live Student Edition Updates	32
2.10 Notes for Instructors, Teachers, & Professors	33
2.11 Update Bounty.....	34
3 Data Loss.....	35
3.1 The Need for Backups	36
3.1.1 Assignment: Format the Backup Drive for Time Machine or Carbon Copy Cloner	40
3.1.2 Assignment: Configure Time Machine	43
3.1.3 Assignment: Integrity Test the Time Machine Backup.....	45
3.1.4 Assignment: Install and Configure Carbon Copy Cloner.....	47
3.1.5 Assignment: Test Run the First Clone Backup.....	54
3.1.6 Assignment: Encrypt the Clone Backup.....	57
3.1.7 Assignment: Integrity Test the Clone Backup	60
4 Passwords.....	65
4.1 The Great Awakening.....	66
4.2 Strong Passwords	67
4.2.1 Assignment: Create a Strong User Account Password.....	70
4.3 Keychain	75
4.3.1 Assignment: View an Existing Keychain Record	79

Contents In Detail

4.4	Challenge Questions	82
4.4.1	Assignment: Store Challenge Q&A in the Keychain	82
4.4.2	Assignment: Access Secure Data from Keychain	85
4.5	Harden the Keychain	88
4.5.1	Assignment: Harden the Keychain with a Different Password	89
4.5.2	Assignment: Harden the Keychain With a Timed Lock	91
4.6	Synchronize Keychain Across macOS and iOS Devices	94
4.6.1	Assignment: Activate iCloud Keychain Synchronization	94
4.7	LastPass	99
4.7.1	Assignment: Install LastPass	99
4.7.2	Assignment: Use LastPass to Save Website Authentication Credentials	103
4.7.3	Assignment: Use LastPass to Auto Fill Website Authentication ..	105
5	System and Application Updates	107
5.1	System Updates	108
5.1.1	Assignment: Configure Apple System and Application Update Schedule	109
5.2	Manage Application Updates With MacUpdate Desktop	112
5.2.1	Assignment: Install and Configure MacUpdate Desktop	112
5.2.2	Assignment: Application Updates with MacUpdate Desktop	117
5.3	Additional Reading	119
6	User Accounts	121
6.1	User Accounts	122
6.2	Never Log in As an Administrator	124
6.2.1	Assignment: Enable the Root User	124
6.2.2	Assignment: Login as the Root User	128
6.2.3	Assignment: Change the Root User Password	131
6.2.4	Assignment: Disable the Root User	132
6.2.5	Assignment: Create an Administrative User Account	132
6.2.6	Assignment: Change from Administrator to Standard User	134
6.3	Application Whitelisting and More with Parental Controls	136
6.3.1	Assignment: Configure a Managed with Parental Controls Account	137
6.3.2	Assignment: View Parental Controls Logs	148
6.4	Policy Banner	150
6.4.1	Assignment: Create a Policy Banner	150

Contents In Detail

7	Storage Device.....	153
7.1	Block Access to Storage Devices	154
7.1.1	Assignment: Disable USB, FireWire, and Thunderbolt Storage Device Access	154
7.1.2	Assignment: Enable USB, FireWire, and Thunderbolt Storage Device Access	155
7.2	FileVault 2 Full Disk Encryption	156
7.2.1	Assignment: Boot into Target Disk Mode.....	157
7.2.2	Assignment: Boot into Recovery HD Mode	157
7.2.3	Assignment: Boot into Single-User Mode.....	158
7.2.4	Assignment: Enable and Configure FileVault 2	158
7.3	FileVault Resistance to Brute Force Attack.....	162
7.4	Remotely Access and Reboot a FileVault Drive	163
7.4.1	Assignment: Temporarily Disable FileVault.....	163
8	Sleep and Screen Saver.....	165
8.1	Require Password After Sleep or Screen Saver	166
8.1.1	Assignment: Require Password After Sleep or Screen Saver	166
9	Malware.....	171
9.1	Anti-Malware.....	172
9.1.1	Assignment: Install and Configure Bitdefender (Home Users Only).....	176
9.1.2	Assignment: Install and Configure Bitdefender GravityZone Endpoint Security (Business Users)	192
9.2	Additional Reading.....	209
10	Firewall.....	211
10.1	Firewall	212
10.1.1	Assignment: Activate the Firewall.....	213
10.1.2	Assignment: Close Unnecessary Ports.....	216
11	Firmware Password	223
11.1	EFI Chip	224
11.1.1	Assignment: Create a Firmware Password.....	224
11.1.2	Assignment: Test the Firmware Password	225
11.1.3	Assignment: Remove the Firmware Password	225
12	Lost or Stolen Device	227
12.1	Find My Mac.....	228
12.1.1	Assignment: Activate and Configure Find My Mac	228

Contents In Detail

12.1.2	Assignment: Use Find My Mac From A Computer.....	234
12.1.3	Assignment: Use Find My Mac From An iPhone or iPad	238
12.2	Prey.....	241
12.2.1	Assignment: Enable the Guest User Account	241
12.2.2	Assignment: Create a Prey Account.....	242
12.2.3	Assignment: Install Prey	245
12.2.4	Assignment: Configure Prey	247
13	Local Network.....	251
13.1	Ethernet Broadcasting	252
13.2	Ethernet Insertion	253
13.3	Wi-Fi Encryption Protocols	254
13.4	Routers: An Overview	256
13.4.1	Assignment: Determine Your Wi-Fi Encryption Protocol.....	257
13.4.2	Assignment: Secure an Apple Airport Extreme Base Station	259
13.4.3	Assignment: Configure WPA2 On a Non-Apple Router.....	263
13.5	Use MAC Address to Limit Wi-Fi Access.....	267
13.5.1	Assignment: Restrict Access by MAC Address on an Apple Airport.....	267
13.5.2	Assignment: Restrict Access by MAC Address to A Non-Apple Router	275
13.6	Router Penetration.....	284
13.6.1	Assignment: Verify Apple Airport Port Security Configuration .	285
13.6.2	Assignment: Verify Non-Apple Airport Router Security Configuration	291
14	Web Browsing.....	297
14.1	HTTPS.....	298
14.1.1	Assignment: Install HTTPS Everywhere	300
14.2	Choose a Browser.....	304
14.3	Private Browsing	305
14.3.1	Assignment: Safari Private Browsing.....	305
14.3.2	Assignment: Firefox Private Browsing	307
14.3.3	Assignment: Google Chrome Incognito Mode	308
14.4	Secure Web Searches	310
14.4.1	Assignment: Make DuckDuckGo Your Safari Default Search Engine.....	310

Contents In Detail

14.4.2	Assignment: Make DuckDuckGo Your Firefox Default Search Engine.....	311
14.4.3	Assignment: Make DuckDuckGo Your Chrome Default Search Engine.....	312
14.5	Clear History.....	314
14.5.1	Assignment: Clear the Safari History.....	314
14.5.2	Assignment: Clear the Firefox Browsing History.....	315
14.5.3	Assignment: Clear the Chrome History	316
14.6	Browser Plug-Ins.....	318
14.6.1	Assignment: Install Traffilight Plug-In for Safari.....	318
14.6.2	Assignment: Install Traffilight Plug-In for Google Chrome	321
14.6.3	Assignment: Install Traffilight For Firefox	323
14.6.4	Assignment: Find and Remove Extensions from Safari.....	325
14.6.5	Assignment: Find and Remove Extensions from Google Chrome.....	326
14.6.6	Assignment: Find and Remove Add-Ons from Firefox	327
14.7	Fraudulent Websites.....	329
14.8	Do Not Track.....	333
14.8.1	Assignment: Secure Safari	334
14.8.2	Assignment: Secure Firefox.....	335
14.8.3	Assignment: Secure Chrome	338
14.8.4	Assignment: Install Ghostery for Safari.....	340
14.8.5	Assignment: Install Ghostery for Chrome	340
14.9	Adobe Flash and Java	345
14.9.1	Assignment: Configure Oracle Java For Automatic Updates.....	345
14.10	Web Scams.....	349
14.10.1	Recovering From A Web Scam.....	349
14.11	Tor 352	
14.11.1	Assignment: Install Tor for Anonymous Internet Browsing.....	354
14.11.2	Assignment: Configure Tor Preferences	364
14.12	Onion Sites and the Deep Web	375
14.13	Have I Been Pwned.....	376
14.13.1	Assignment: Searching With HaveIBeenPwned	376
14.13.2	Assignment: What To Do Now That You Have Been Breached .	378
15	Email.....	379
15.1	The Killer App.....	380

Contents In Detail

15.2	Phishing.....	381
15.3	Email Encryption Protocols.....	383
15.4	TLS and SSL With Mail App	384
15.4.1	Assignment: Configure Mail.app to Use TLS or SSL.....	384
15.5	HTTPS with Web Mail.....	389
15.5.1	Assignment: Configure Web Mail to Use HTTPS	389
15.6	End-To-End Secure Email With ProtonMail	390
15.6.1	Assignment: Create a ProtonMail Account	392
15.6.2	Assignment: Create and Send an Encrypted ProtonMail Email ..	396
15.6.3	Assignment: Receive and Respond to a ProtonMail Secure Email.....	400
15.7	End-To-End Secure Email With GNU Privacy Guard.....	405
15.7.1	Assignment: Install GPG and Generate a Public Key.....	406
15.7.2	Assignment: Add Other Email Addresses to a Public Key	412
15.7.3	Assignment: Install a Friend's Public Key.....	418
15.7.4	Assignment: Configure GPGMail Preferences.....	420
15.7.5	Assignment: Encrypt and Sign Files with GPGServices.....	422
15.7.6	Assignment: Send a GPG-Encrypted and Signed Email	426
15.7.7	Assignment: Receive a GPG-Encrypted and Signed Email.....	428
15.8	End-To-End Secure Email With S/MIME.....	431
15.8.1	Assignment: Acquire a Free Class 1 S/MIME Certificate	432
15.8.2	Assignment: Acquire A Class 3 S/MIME Certificate for Business Use	439
15.8.3	Assignment: Purchase a Class 3 S/MIME Certificate for Business Use	448
15.8.4	Assignment: Download and Install a Business S/MIME Certificate.....	459
15.8.5	Assignment: Exchange Public Keys with Others.....	463
15.8.6	Assignment: Send S/MIME Encrypted Email.....	466
15.9	Virtru Email Encryption	469
15.9.1	Create a Free Virtru for Gmail Account.....	471
15.9.2	Send Encrypted Gmail With Virtru	477
15.9.3	Receive and Reply to a Virtru-Encrypted Email	479
16	Apple ID and iCloud.....	483
16.1	Apple ID and iCloud	484
16.1.1	Assignment: Create an Apple ID.....	485

Contents In Detail

16.1.2	Assignment: Enable 2-Factor Authentication	490
16.1.3	Sign in to Your iCloud Account	499
17	Documents	505
17.1	Document Security	506
17.2	Password Protect a Document Within Its Application	507
17.2.1	Assignment: Encrypt an MS Word Document.....	507
17.3	Encrypt a PDF Document.....	510
17.3.1	Assignment: Convert a Document to PDF for Password Protection.....	510
17.4	Encrypt a Folder for Only macOS Use.....	513
17.4.1	Assignment: Create an Encrypted Disk image	513
17.5	Encrypt A Folder for Cross Platform Use With Zip	517
17.5.1	Assignment: Encrypt A File or Folder Using Zip.....	517
17.5.2	Assignment: Open an Encrypted Zip Archive.....	523
17.6	Cross-Platform Disk Encryption	525
17.6.1	Assignment: Download and Install VeraCrypt	525
17.6.2	Assignment: Configure VeraCrypt.....	531
17.6.3	Assignment: Create a VeraCrypt Container	537
17.6.4	Assignment: Mount an Encrypted VeraCrypt Container	549
18	Voice, Video, and Instant Message Communications	555
18.1	Voice, Video, and Instant Messaging Communications	556
18.2	HIPAA Considerations	558
18.3	Wire	559
18.3.1	Assignment: Install Wire	559
18.3.2	Assignment: Invite People to Wire	564
18.3.3	Assignment: Import Contacts into Wire	569
18.3.4	Assignment: Secure Instant Message a Wire Friend.....	570
18.3.5	Assignment: Secure Voice Call with A Wire Friend.....	574
18.3.6	Assignment: Secure Video Conference with a Wire Friend	577
19	Internet Activity.....	579
19.1	Virtual Private Network.....	580
19.2	Gateway VPN	581
19.2.1	Assignment: Search for a VPN Host.....	585
19.3	Perfect-Privacy	587
19.3.1	Assignment: Create a Perfect-Privacy Account.....	587
19.3.2	Assignment: Configure IKEv2 VPN With Perfect-Privacy	595

Contents In Detail

19.3.3	Assignment: Advanced Perfect-Privacy Settings.....	600
19.4	Resolving Email Conflicts with VPN	604
19.5	Mesh VPN	605
19.6	LogMeIn Hamachi.....	606
19.6.1	Assignment: Create a LogMeIn Hamachi Account	606
19.6.2	Assignment: Add Users to a Hamachi VPN Network.....	619
19.6.3	Assignment: File Sharing Within a Hamachi VPN Network.....	629
19.6.4	Assignment: Screen Share Within Hamachi VPN	631
19.6.5	Assignment: Exit the Hamachi VPN Network	633
20	Social Media	635
20.1	What, me worry?	636
20.2	Protecting Your Privacy On Social Media.....	637
20.3	Facebook.....	638
20.3.1	Assignment: Facebook Security and Login	638
20.3.2	Assignment: Facebook Privacy Settings	644
20.3.3	Assignment: Timeline and Tagging Settings	647
20.3.4	Assignment: Facebook Manage Blocking.....	650
20.3.5	Assignment: Facebook Public Posts.....	652
20.3.6	Assignment: Facebook Apps	654
20.4	LinkedIn	664
20.4.1	Assignment: LinkedIn Account Security.....	664
20.4.2	Assignment: LinkedIn Privacy Settings	669
20.5	Google—More Than a Search Engine	681
20.5.1	Assignment: Manage Your Google Account Access and Security Settings	681
20.5.2	Assignment: Enable Google 2-Step Verification	698
21	When It Is Time to Say Goodbye	705
21.1	Preparing a Computer for Sale or Disposal.....	706
21.1.1	Assignment: Prepare Your Mac For Sale Or Disposal.....	706
21.1.2	Assignment: Secure Erase the Drive.....	710
21.1.3	Assignment: Install macOS 10.13	715
22	Miscellaneous.....	717
22.1	Date and Time Settings	718
22.1.1	Assignment: Configure Date & Time	719
22.2	Securing Hardware Components	721
22.3	National Institute of Standards and Technology (NIST)	723

Contents In Detail

22.3.1 NIST-Specific Security Settings	723
22.4 United States Computer Emergency Readiness Team (US-CERT).....	725
23 The Final Word.....	727
23.1 Additional Reading	728
macOS 10.13 Security Checklist.....	729
Revision Log.....	735
Index	737
Mintz InfoTech, Inc. when, where, and how you want IT	743
Practical Paranoia Workshops & Books	744

PRACTICAL PARANOIA MACOS 10.13 SECURITY ESSENTIALS

MARC L. MINTZ, MBA-IT, ACTC, ACSP

17 Documents

No matter how paranoid or conspiracy-minded you are, what the government is actually doing is worse than you imagine.

—William Blum¹, American author, and former State Department employee

What You Will Learn In This Chapter

- Password protect a document in its application
- Encrypt a PDF document
- Encrypt a folder for only macOS use
- Encrypt a folder for cross-platform use with zip
- Encrypt files or folders for cross-platform use with VeraCrypt

¹ https://en.wikiquote.org/wiki/William_Blum

17.1 Document Security

If your documents never leave your computer, and you have encrypted your storage devices using FileVault 2, there is no need to go the extra step to encrypt your documents. But should you ever need to email your sensitive data to someone else, or pass a sensitive document via any storage device, encrypting the document goes a long way to a good night of sleep.

There are several options to document encryption, each with its own benefits and drawbacks. We will discuss each here.

17.2 Password Protect a Document Within Its Application

A few applications are designed with document security in mind, and offer their own encryption scheme. Microsoft Office and Adobe Acrobat Pro are common examples.

Although Microsoft Office products make it an easy process to password protect your documents, prior to Office 2007 (Windows) and 2011 (Mac), it was an equally easy process to break the encryption. There are many freeware and commercial utilities that can bypass the password and open the document for reading in older versions.

Starting with Microsoft Office 2007 and 2011, Microsoft changed the encryption standard to use the secure AES-128² algorithm. Microsoft Office 2016 (Office 365) uses AES-256³. Assuming an adequate password length has been selected, it is estimated by some researchers that it would take millions of years to brute-force crack an AES-256 password with current computing power. For security during this lifetime (famous last words), the AES-256 encryption standard should be enough to protect your documents if an adequate password has been chosen.

17.2.1 Assignment: Encrypt an MS Word Document

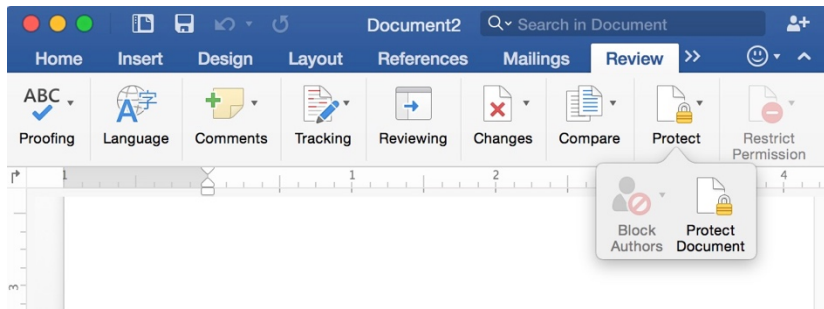
In this assignment, you encrypt a Microsoft Word 2016 (Office 365) file. Although this assignment uses a Word file, the process is identical for Excel and PowerPoint files.

- Prerequisite: Microsoft Word 2016 (365) installed and activated.
1. Open the target document in Microsoft Word.

² https://en.wikipedia.org/wiki/Advanced_Encryption_Standard

³ [https://technet.microsoft.com/en-us/library/cc179125%28v=office.16%29.aspx?f=255&MSPPError=-2147217396 - About](https://technet.microsoft.com/en-us/library/cc179125%28v=office.16%29.aspx?f=255&MSPPError=-2147217396-About)

2. Select *Review* tab > *Protect* > *Protect Document*.



3. The *Password Protect* dialog opens. You may set a separate password to *Open*, and to *Modify* this document. Enter a password for the desired function.
 - Note: Passwords for Microsoft Office products are limited to 15 characters.

Password Protect

Security

Set a password to open this document:

Password:

Set a password to modify this document:

Password:

☐ Read-only recommended

Protection

☐ Protect document for:

☒ Tracked changes

☐ Comments

☐ Read only

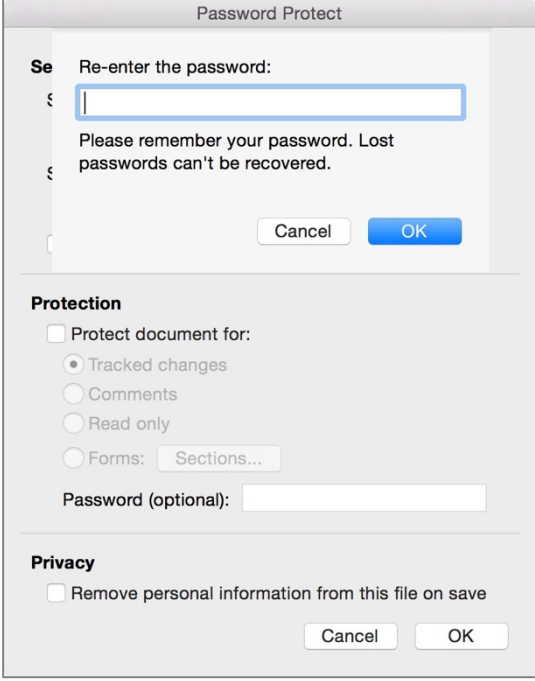
☐ Forms:

Password (optional):

Privacy

☐ Remove personal information from this file on save

4. Re-enter the password, and then click *OK*.



The screenshot shows a 'Password Protect' dialog box with a title bar. It is divided into three sections: a top section for password re-entry, a middle 'Protection' section, and a bottom 'Privacy' section. The top section has a label 'Re-enter the password:' followed by a text input field. Below the input field is a warning message: 'Please remember your password. Lost passwords can't be recovered.' At the bottom of this section are 'Cancel' and 'OK' buttons. The 'Protection' section has a checkbox 'Protect document for:' which is currently unchecked. Below it are four radio button options: 'Tracked changes' (selected), 'Comments', 'Read only', and 'Forms:'. The 'Forms:' option has a 'Sections...' button next to it. Below these is a 'Password (optional):' label followed by a text input field. The 'Privacy' section has a checkbox 'Remove personal information from this file on save' which is unchecked. At the bottom of the dialog are 'Cancel' and 'OK' buttons.

Re-enter the password:

Please remember your password. Lost passwords can't be recovered.

Cancel OK

Protection

☐ Protect document for:

- ☒ Tracked changes
- ☐ Comments
- ☐ Read only
- ☐ Forms: Sections...

Password (optional):

Privacy

☐ Remove personal information from this file on save

Cancel OK

5. Click the *OK* button at the bottom right of the *Password Protect* dialog. Your document is now protected.

17.3 Encrypt a PDF Document

As there are only a few applications that can encrypt their own documents, chances are you will be working with a file whose application cannot perform the encryption. macOS can “print” any document to pdf format, and in the process, add password-protected encryption to the pdf.

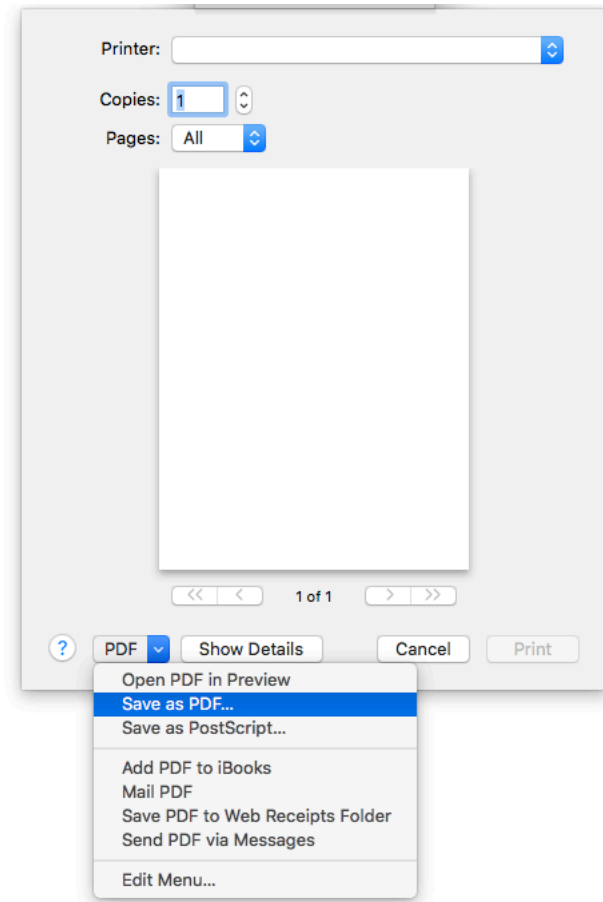
- As of macOS 10.12.3 (perhaps earlier) print to pdf services saves the file in Acrobat 7 format. This format uses AES-128 encryption, which is considered strong and may be used for HIPAA, SEC, legal, and other high-security needs.
- Earlier versions of macOS print to pdf services save the file in pdf version 1.4/Acrobat 5 format. This format uses RC4 128-bit encryption, which is considered weak, and should not be used for HIPAA, SEC, legal, or other high-security needs.
- Adobe Acrobat 7 and higher use AES 128-bit encryption. Adobe Acrobat 9 and higher use AES-256-bit encryption. These are considered secure, as long as strong passwords are used.

17.3.1 Assignment: Convert a Document to PDF for Password Protection

In this assignment, you convert a file into a PDF for encryption.

1. Open any printable document currently on your computer.
2. Select *File* menu > *Print*.

3. From the *Print* window, select the *PDF* button > *Save as PDF*.



4. In the window that opens, in the *Save As* field, name the pdf version of the document, and then select the *Security Options...* button.

Save As: Security Document.pdf

Tags:

Where: Documents

Title: test

Author: Marc Mintz

Subject:

Keywords:

Security Options...

Cancel Save

5. In the *PDF Security Options* window, enable the *Require password to open document* check box, enter a desired password in the *Password* and *Verify* fields, and then select the *OK* button.

PDF Security Options

☒ Require password to open document

Password:

Verify:

☐ Require password to copy text, images and other content

☐ Require password to print document

Password:

Verify:

Cancel OK

6. Quit the current document and application.

The pdf version of the document is now encrypted. If the original document is no longer needed, it may be trashed.

17.4 Encrypt a Folder for Only macOS Use

Perhaps you need to securely send an entire folder of files. An easy way to accomplish this is to use a utility to archive (compress to a single file) the files or folder, and have that same utility protect the archive with a password.

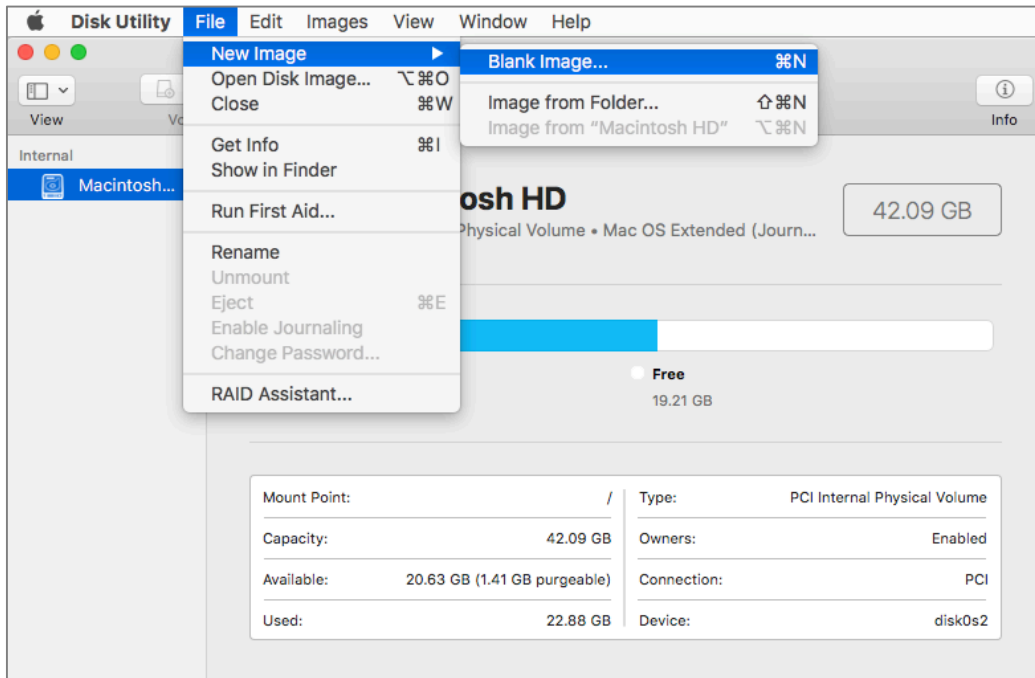
macOS has a built-in utility to do this for you—*Disk Utility*. The only downside is that the archives created with Disk Utility are only readable on another macOS/OS X computer—they are not cross-platform compatible. However, if your documents will be passed along only to others using macOS/OS X, it is an excellent tool.

17.4.1 Assignment: Create an Encrypted Disk image

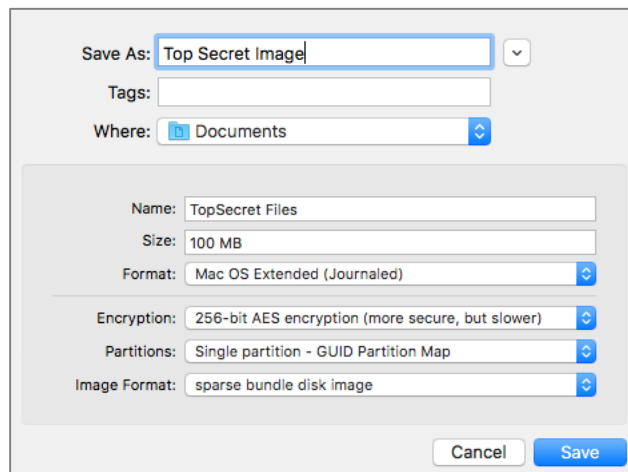
In this assignment you create an encrypted disk image to store sensitive files and folders.

1. Open Disk Utility, located in */Applications/Utilities*.

2. Select *Disk Utility* File menu > *New Image* > *Blank Image...*



3. Configure the *New Image* screen as below.



- *Save As:* The desired name for the archive that will hold all your files to be password protected.

- *Where:* Navigate to where you want the archive to be saved.
 - *Name:* Enter the name of the mounted disk image. To avoid confusion, this is normally named the same as the *Save As* field. For demonstration purposes, we are naming them differently in this example.
 - *Size:* This should be somewhat larger than the total size of files the archive will hold. It can be much larger, as the archive will compress out all unused space.
 - *Format: Mac OS Extended (Journaled).* This is the macOS standard format.
 - *Encryption:* 256-bit takes more time to encrypt and decrypt than 128-bit, but is also more secure. When selecting this option, you are prompted to provide a password. Enter your desired password, and then click *OK*.
 - *Partitions:* Single Partition, GUID Partition Map. This is the macOS standard.
 - *Image Format: Sparse Bundle Disk Image.* This is the format that will compress out all unused space.
4. Select the *Save* button.
 5. The archive is saved, and the Disk Image (the opened format of the archive) is displayed in the Finder Window Sidebar, and depending on your *Finder Preferences* menu > *General* > *Hard Disks*, may display as mounted on the Desktop. You now have an encrypted, password protected archive, but it's currently empty. Time to fill it.
 6. Locate the mounted disk image on the Desktop. In our example, it will be called *Top Secret Files*.
 7. Drag the various files and folder that you have targeted for password protection into the mounted image.
 8. Eject/unmount the mounted image. It will close, remove itself from the Desktop, leaving just the password protected archive in the location you specified in step 3 above (Desktop).

17 Documents

This archive may be securely passed to macOS/OS X users by any method. If they know the password, double-clicking the archive will mount the disk image to their Desktop, and they will have full read and write access to the documents inside.

17.5 Encrypt A Folder for Cross Platform Use With Zip

If you need to exchange a file or files with others and they do not use macOS/OS X, we can use the same strategy as we did with Disk Utility, but this time we need to password protect our archive in a format that is readable by any OS. Although there are over a dozen cross-platform compression formats, *zip* has become the most common standard.

Although macOS has the built-in ability to create zip archives, it uses the default format which lacks encryption. To encrypt our zip archives, you will need a 3rd-party utility. We recommend using *Keka* for macOS.

Once you have created an encrypted archive of your file or files, the archive can be uploaded to a file server, shared by email, or passed along via drive, disc, or thumb drive. As long as the other party knows the (strong) password, your data is safe from spying eyes.

- Note: The encryption protocol used in zip is considered weak, and should not be used for HIPAA, SEC, legal, or other high-security needs unless using a 3rd-party zip utility that provides AES 256-bit encryption. *WinZIP* is the industry leader for commercial software providing this level of zip security. *7-zip* is the industry leader for open source software with this level of zip security. *Keka* uses 7-zip as well as zip with AES 256.

17.5.1 Assignment: Encrypt A File or Folder Using Zip

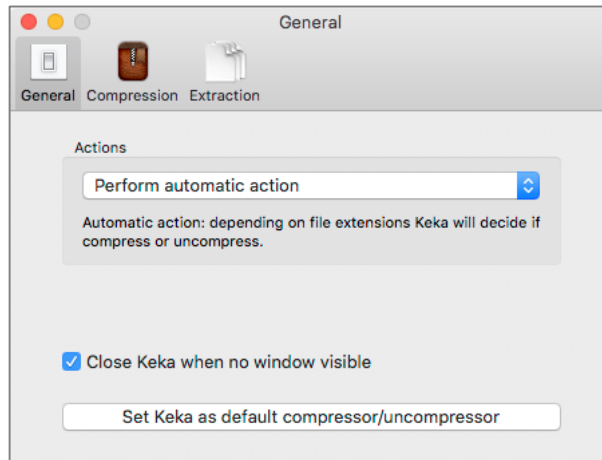
In this assignment, you encrypt a file using Keka. The same process can be used to encrypt a folder full of items.

- Note: Keka is available for free directly from the developer website, and for \$1.99 from the Apple App Store. There is currently no difference between the two products. Buying from the App Store supports development of Keka, and ensures your software is kept up to date.
1. Download Keka.
 - To download Keka from the developer site, open a browser to <https://www.kekaosx.com/>.

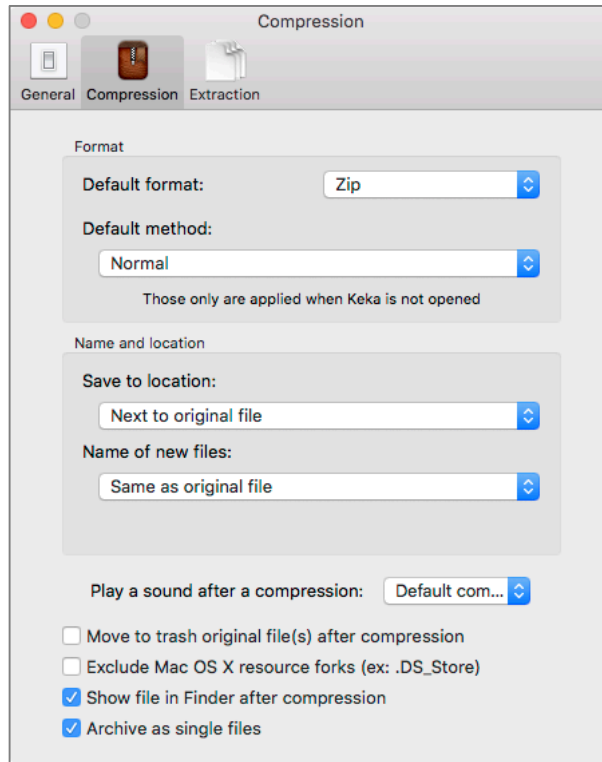
- To download from the Apple App Store, open the *App Store app*, search for *Keka*, and then download.

Configure Keka Preferences

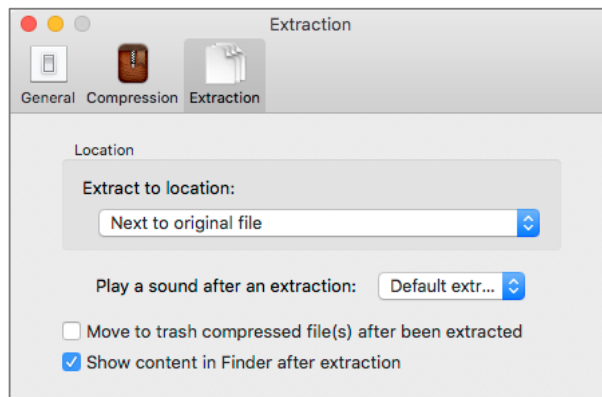
2. Select the *Keka* menu > *Preferences*.
3. Select the *General* tab, configure to your taste. Shown below are my preferences.



4. Select the *Compression* tab, configure to your taste. Shown below are my preferences.



5. Select the *Extraction* tab, configure to your taste. Shown below are my preferences.

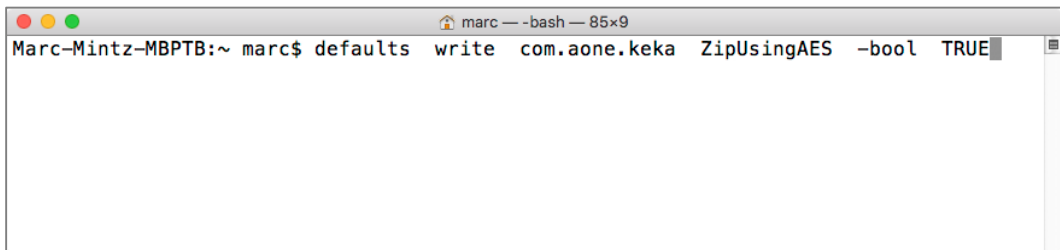


6. Close *Keka Preferences* window.
7. Quit *Keka*.

Enable AES 256-bit encryption

By default, Keka does not encrypt using AES 256. It is vital to your security and privacy that your documents have the highest level of protection, and AES 256 should be enabled

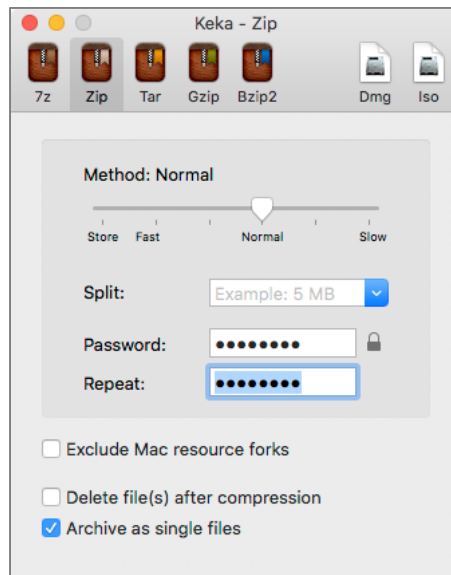
8. Open *Terminal*, located in */Applications/Utilities*. Terminal is the built-in utility that provides a Command Line Interface (CLI) for macOS.
9. In Terminal, enter:
`defaults write com.aone.keka ZipUsingAES -bool TRUE`



10. Tap the *Return* or *Enter* key.
11. Quit Terminal.

Compress and encrypt a file

12. Open *Keka*.
13. In the *Keka Main window* toolbar, select the *Zip* tab, and then verify the *Method* is set to *Normal*, *Archive as single files* is enabled, and then enter *password* in the *Password* and *Repeat* fields as the password for the file you will be encrypting.



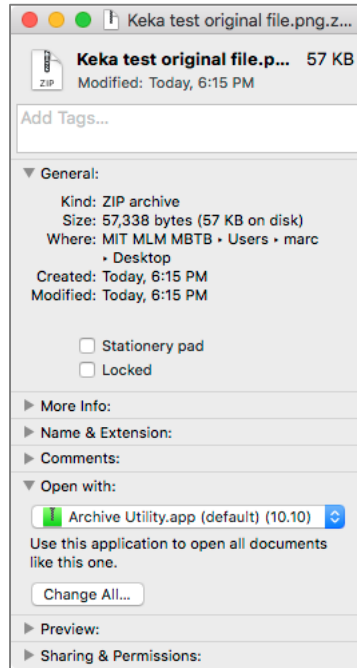
14. Locate a document file on your computer to be compressed and encrypted, and then drag and drop it onto the *Keka* Dock icon. For my example, the file is named *Keka test original file.png*.
15. A Finder window will open, displaying the new compressed and encrypted file, with the same name as the original, with a *.zip* file extension.

Set Keka as the default application to open zip files

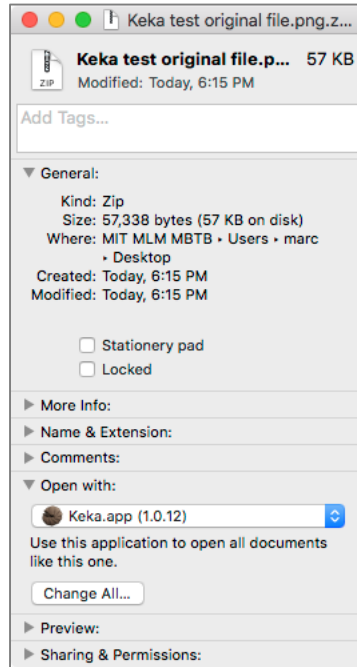
macOS 10.13 cannot recognize AES 256 encrypted files, but Keka can! To be able to open these files, macOS 10.13 must be trained to use Keka to open them, instead of the built-in default zip utility.

17 Documents

16. Single-click to select the encrypted zip file create a minute ago.
17. Select the *File* menu > *Get Info*.
18. If not currently visible, expand to view the *Open with* area. Note that the default *Archive Utility.app* is selected.



19. Click the *Archive Utility.app* pop-up menu, to select *Keka.app*



20. Click the *Change All...* button. From now on, all zip files will be opened with Keka.

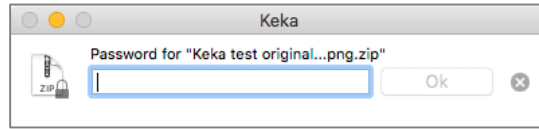
21. Close the *Get Info* window.

17.5.2 Assignment: Open an Encrypted Zip Archive

In this assignment, you open the encrypted zip archive created in the previous assignment.

- Prerequisite: Completion of the previous assignment. If performing this assignment on a different computer than the previous assignment, Keka must be installed.
1. Locate the encrypted zip archive created in the previous assignment.
 2. Double-click on the encrypted zip archive.

3. At the prompt, enter the password used to encrypt it.



4. The archive will open, saving the contents to the same folder as the zip file.

17.6 Cross-Platform Disk Encryption

Many in the IT security fields think the ultimate in document encryption comes with *VeraCrypt*⁴. VeraCrypt is free encryption software developed by *IDRIX*⁵, who specialize in security solutions. It is based on *TrueCrypt*⁶ that ceased development in 2014.

Although Linux, macOS/OS X, and Windows versions are available, no Android or iOS support is directly offered. Android users may create and decrypt, as well as read and write to TrueCrypt files using *EDS* (Encrypted Data Store), available from Google Play. iOS users may use *Disk Decipher*, available from the App Store, to create and decrypt, as well as read and write to TrueCrypt files.

VeraCrypt is a disk encryption utility, as opposed to file encryption. It creates an encrypted virtual disk, or as it is referred to by VeraCrypt, a container.

VeraCrypt presents a very high level of security, with a resultant greater complexity to the end-user. Given the speed of current systems and a strong password, data stored in a container may be considered immune from brute-force attacks.

As VeraCrypt creates a container, you can place anything within the container for secure storage. The container may reside only on the local drive, or be placed on a server for network access, or within a cloud storage solution (such as DropBox, Google Drive, etc.) to provide Internet access to files and folders, without the cloud provider (or hacker, malware, or government) being able to view the contents.

17.6.1 Assignment: Download and Install VeraCrypt

In this assignment, you install VeraCrypt.


1. Open a web browser to <https://www.veracrypt.fr/en/Downloads.html>

⁴ <http://veracrypt.codeplex.com>

⁵ <https://www.idrix.fr>

⁶ <http://en.wikipedia.org/wiki/TrueCrypt>

2. Click the Downloads tab (not the Downloads button). Selecting the tab allows you to select which version to download. Select *Mac OS X VeraCrypt*. The installer will download. We will come back to it after we install OSXFUSE.





[Home](#)
[Source Code](#)
[Downloads](#)
[Documentation](#)
[Donate](#)
[Forums](#)

Note to publishers: If you intend to host our files on your server, please instead consider linking to this page. It will help us prevent spreading of obsolete versions, which we believe is critical when security software is concerned. Thank you.

[Supported versions of operating systems](#)

PGP Public Key: https://www.idrix.fr/VeraCrypt/VeraCrypt_PGP_public_key.asc (ID=0x54DDD393, Fingerprint=993B7D7E8E413809828F0F29EB559C7C54DDD393)

Latest Stable Release - 1.21 (Sunday July 9, 2017)

-  **Windows:** [VeraCrypt Setup 1.21.exe \(28.2 MB\)](#) [\(PGP Signature\)](#)
-  **Mac OS X:** [VeraCrypt_1.21.dmg \(10.7 MB\)](#) [\(PGP Signature\)](#)
 - [OSXFUSE](#) 2.5 or later must be installed.

3. Once this begins downloading, select *OSXFUSE*. This takes you to <https://osxfuse.github.io>. From the sidebar > *Stable Releases*, select the most current version for macOS. The installer will download.



The screenshot shows the OSXFUSE website for macOS. At the top, there is a header with the FUSE logo (a blue square with the word 'FUSE' in white) and the text 'FUSE for macOS' and 'File system integration made easy'. Below the header, there are navigation links: 'Project on GitHub', 'Downloads', 'Wiki', 'Google Group', and 'Issue Tracker'. The main content area is divided into two columns. The left column has a section titled 'What is FUSE for macOS?' followed by a paragraph explaining that FUSE for macOS allows extending macOS's native file handling capabilities via third-party file systems. It is a successor to MacFUSE, which is no longer maintained. Below this is a section titled 'Features' with a paragraph explaining that installing the FUSE for macOS software package will let users use any third-party FUSE file system, with legacy MacFUSE file systems supported through an optional compatibility layer. The right column has a section titled 'Stable Releases' with two entries. The first entry is 'FUSE for macOS 3.6.3', which supports Mac OS X 10.5 or later on Intel or PowerPC, was released on 18 Jul 2017, and has been downloaded 94,667 times. The second entry is 'SSHFS 2.5.0', which also supports Mac OS X 10.5 or later on Intel or PowerPC, was released on 03 Feb 2014, and has been downloaded 548,898 times.

FUSE

FUSE for macOS

File system integration made easy

[Project on GitHub](#) [Downloads](#) [Wiki](#) [Google Group](#) [Issue Tracker](#)

What is FUSE for macOS?

FUSE for macOS allows you to extend macOS's native file handling capabilities via third-party file systems. It is a successor to [MacFUSE](#), which has been used as a software building block by dozens of products, but is no longer being maintained.

Features

As a user, installing the FUSE for macOS software package will let you use any third-party FUSE file system. Legacy MacFUSE file systems are supported through the optional MacFUSE compatibility layer.

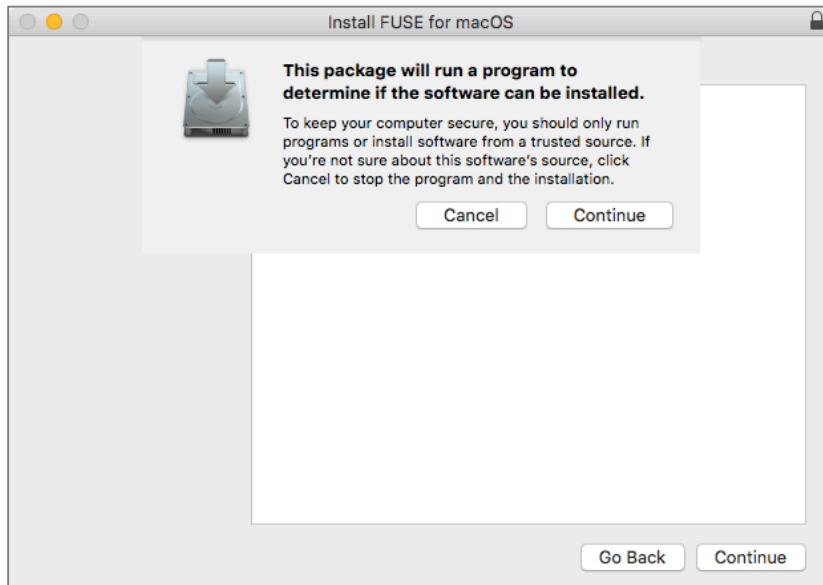
Stable Releases

	FUSE for macOS 3.6.3 Mac OS X 10.5 or later Intel or PowerPC Released on 18 Jul 2017 Downloaded 94,667 times
	SSHFS 2.5.0 Mac OS X 10.5 or later Intel or PowerPC Released on 03 Feb 2014 Downloaded 548,898 times

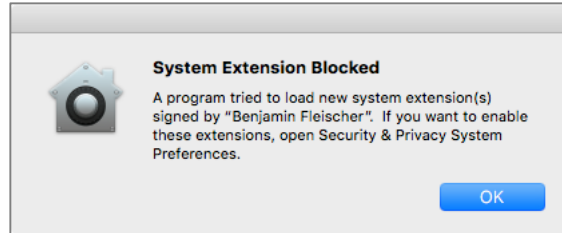
4. Locate the downloaded OSXFUSE installer (by default, located in your *Home Folder > Downloads*). Double-click to open the installer.



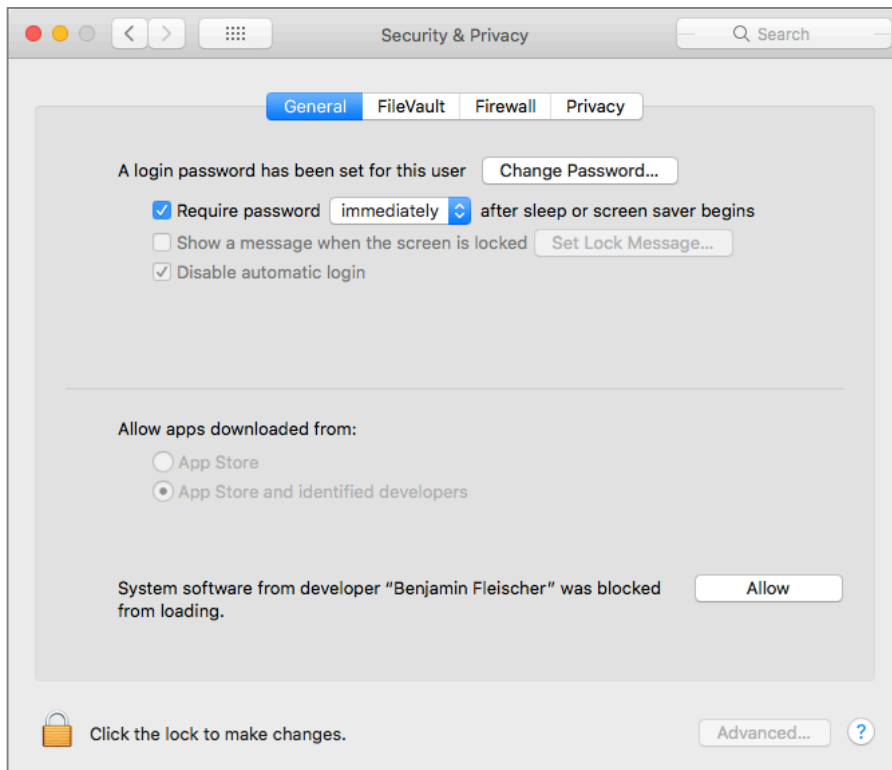
5. In the *Install FUSE for macOS* window, click the *Continue* button, and then follow the on-screen instructions to complete installation.



6. As of this writing, FUSE has not registered with Apple. At the end of the installation process, an alert will appear regarding blocking this installation. Click the *OK* button.



7. Following the instructions of the alert, open *Apple Menu > System Preferences > Security & Privacy > General*, and then click the *Allow* button. Installation of FUSE will complete. Close System Preferences. Click the *Close* button in the installer window.

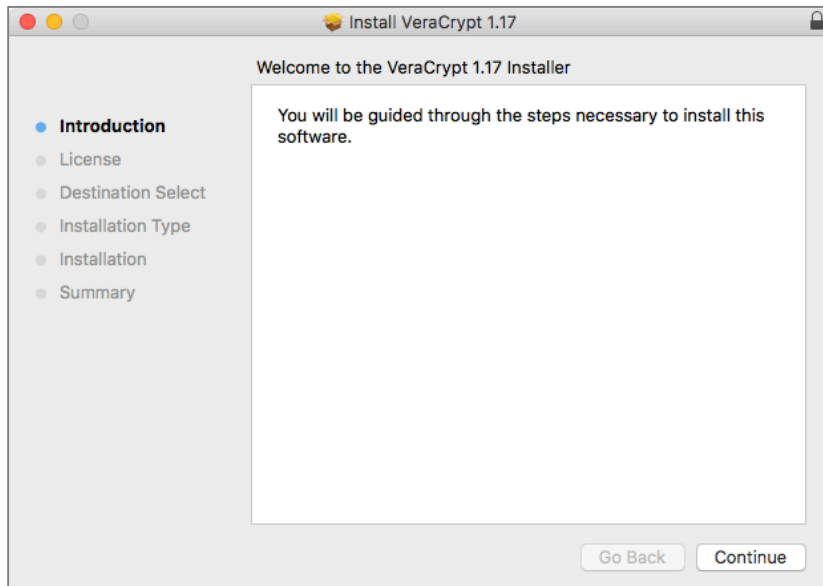


8. FUSE is now installed.

9. Locate the VeraCrypt installer (by default, in the *Home Folder > Downloads* folder). Double-click to launch the *VeraCrypt_Installer.pkg* inside of the mounted disk image.



10. The installer opens. Follow the on-screen instructions to complete the installation.



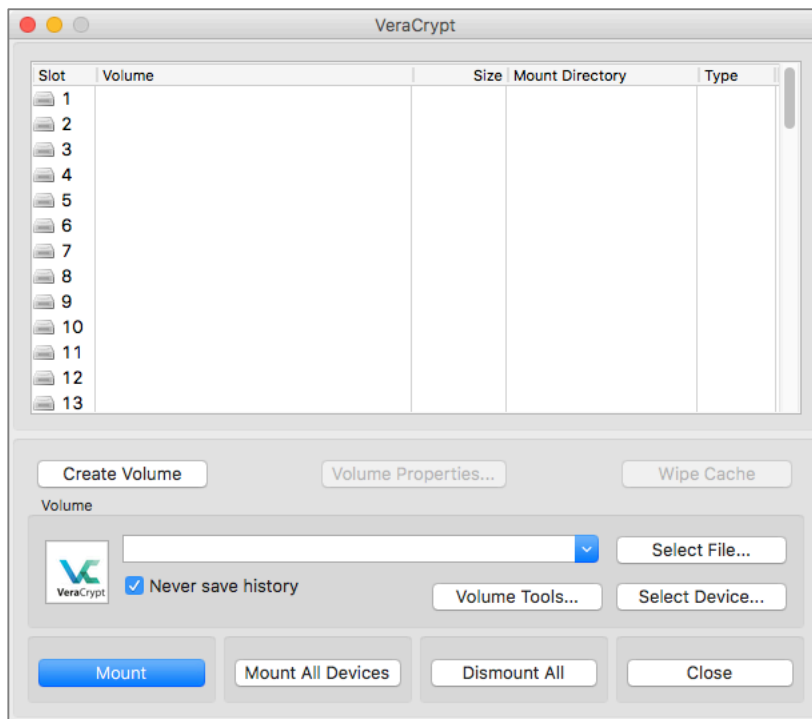
That's all there is to the installation.

17.6.2 Assignment: Configure VeraCrypt

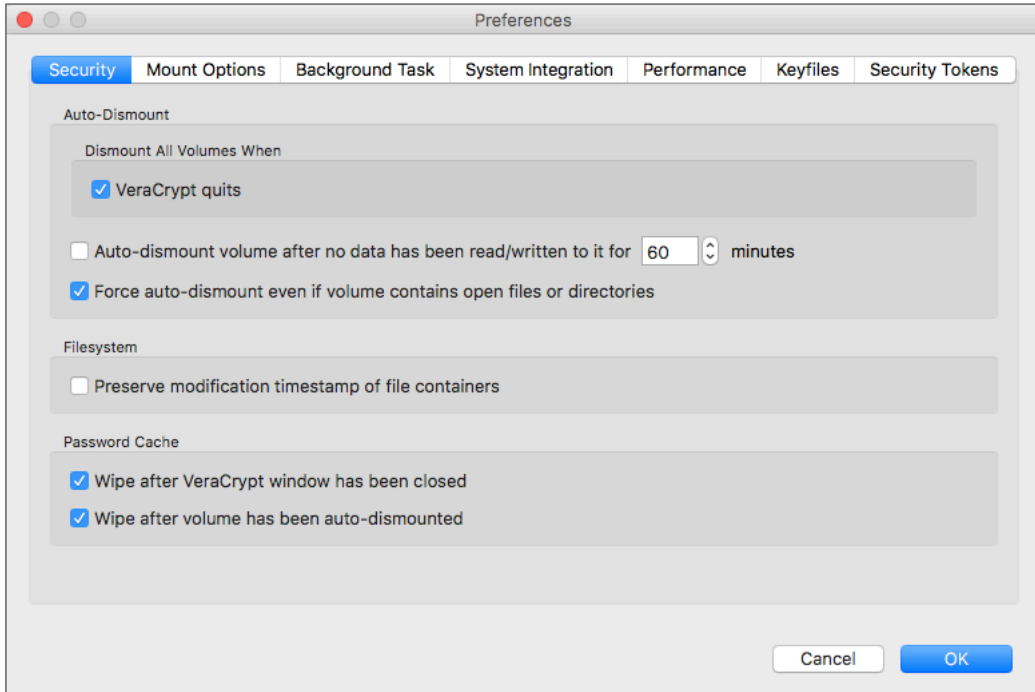
As with most applications, it helps to view and configure VeraCrypt preferences before using it.

In this assignment, you examine and configure VeraCrypt preferences.

1. Open VeraCrypt.

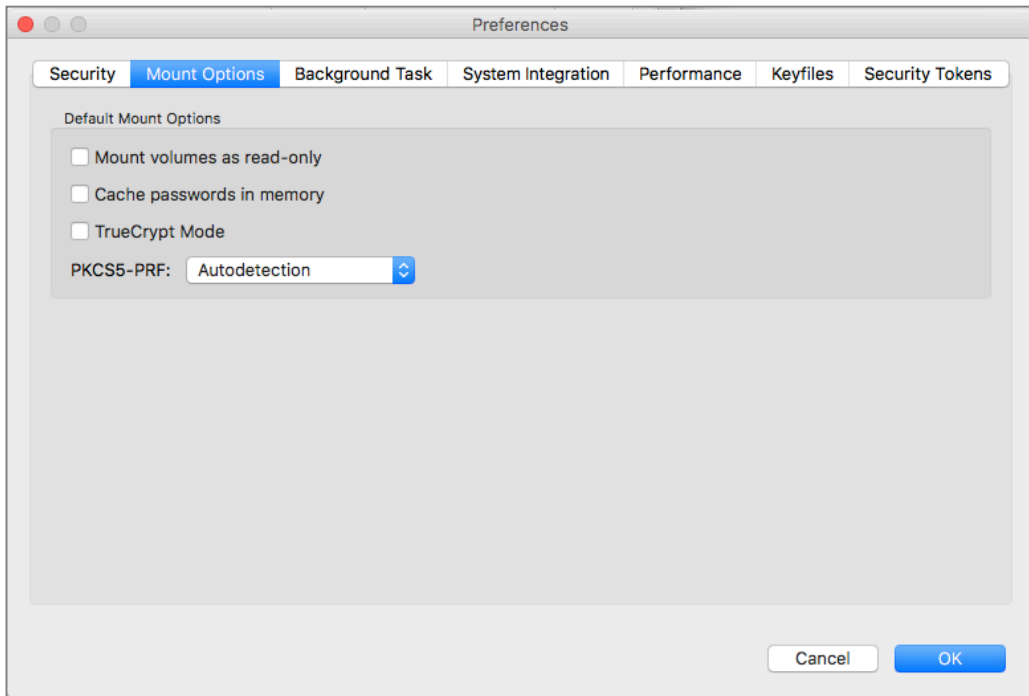


2. Select the *VeraCrypt* menu > *Preferences*. Select the *Security* tab. Most of the options may be configured to taste. The exception is *Preserve modification timestamp of file containers*, which should be *disabled* if the containers will be used with cloud-based file storage service (DropBox, Google Drive, SugarSync, etc.) as it will conflict with the service's ability to update the timestamp.

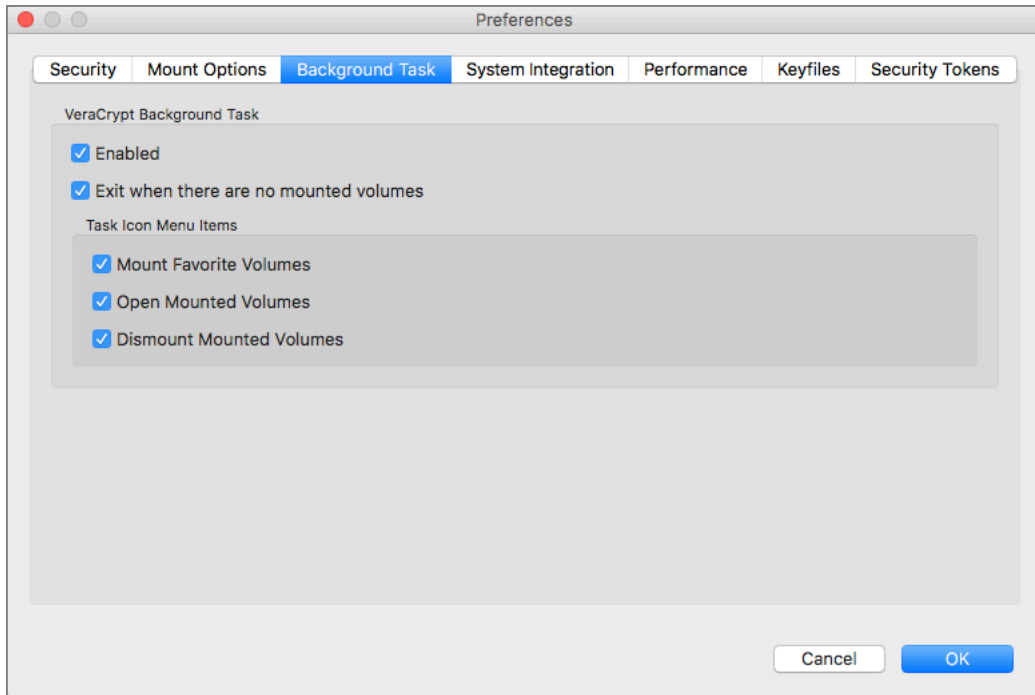


3. Select the *Mount Options* tab.

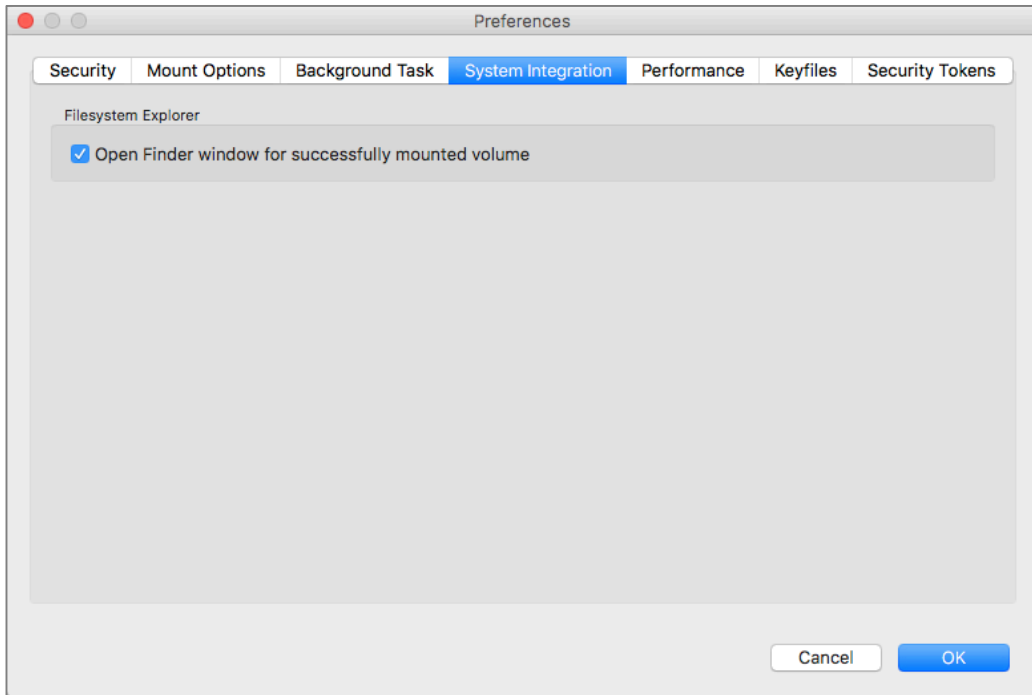
- *Mount volumes as read-only* if left unchecked will prevent accidental editing or deletion of the container contents.
- *Cache passwords in memory* if left unchecked will provide higher security against hackers gaining access to container passwords.
- *TrueCrypt Mode* option should be left unchecked unless you will be using software that can only work with the older TrueCrypt mode.



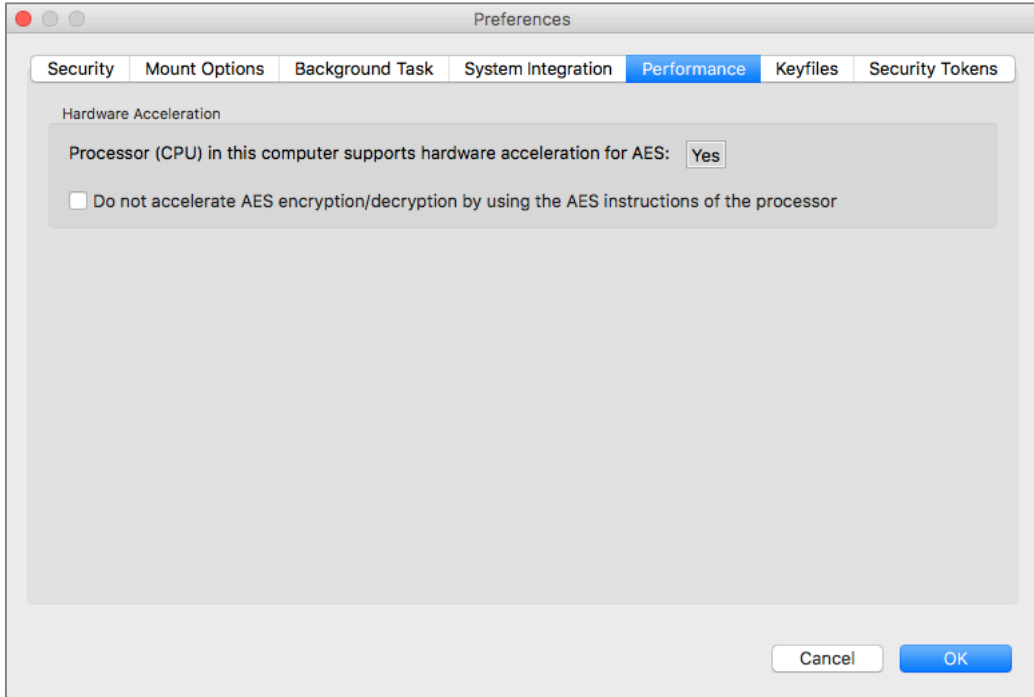
4. Select the *Background Task* tab. All options may be configured to taste. Listed below are my settings.



5. Select the *System Integration* tab. You may configure to taste. Listed below is my setting.



6. Select the *Performance* tab. If your computer supports hardware acceleration of AES encryption protocols, you probably want to leave the checkbox disabled. Doing so will improve encryption and decryption up to 4-fold.



7. The Keyfiles tab is an advanced option. Please see the VeraCrypt online documentation <https://veracrypt.codeplex.com/documentation> for additional information.
8. The *Security Tokens* tap is an advanced option. Please see the VeraCrypt online documentation <https://veracrypt.codeplex.com/documentation> for additional information.
9. Click the OK button to close the VeraCrypt Preferences window.

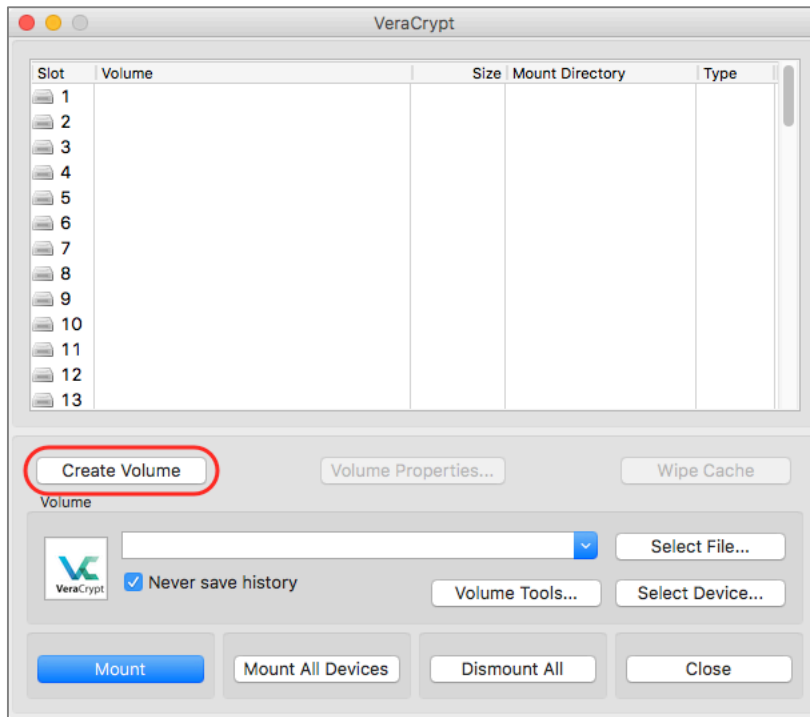
You are now ready to create your first encrypted VeraCrypt container!

17.6.3 Assignment: Create a VeraCrypt Container

Although we will cover the basics of using VeraCrypt, you may find it useful to dive deeper into the topic⁷.

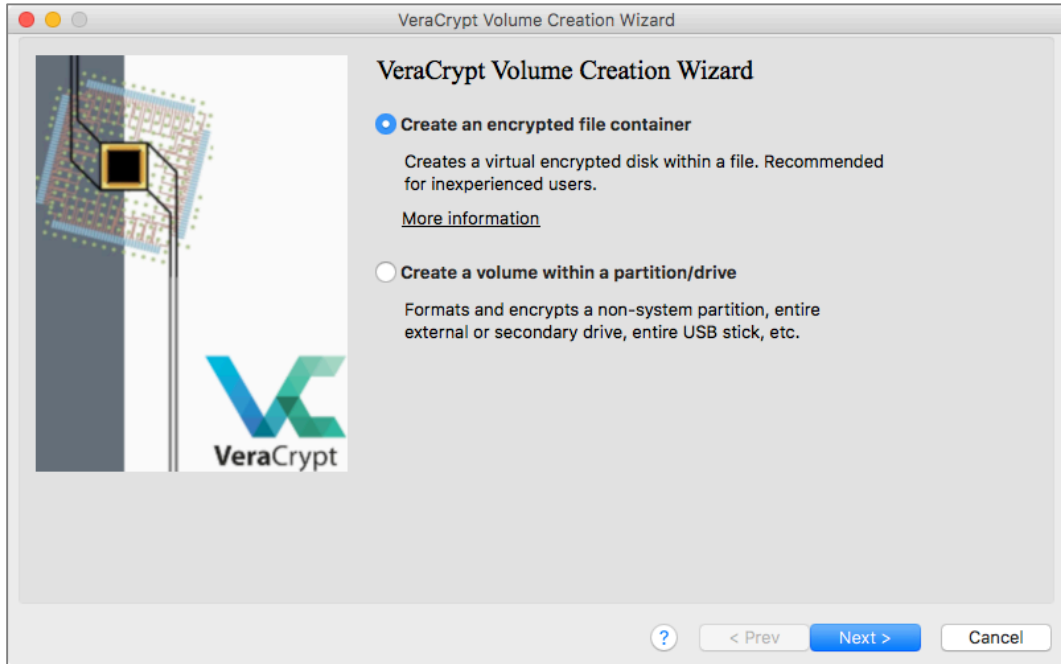
In this assignment, you create your first encrypted container

1. *Open* the *VeraCrypt* application, located in the */Applications* folder. Then select the *Create Volume* button.

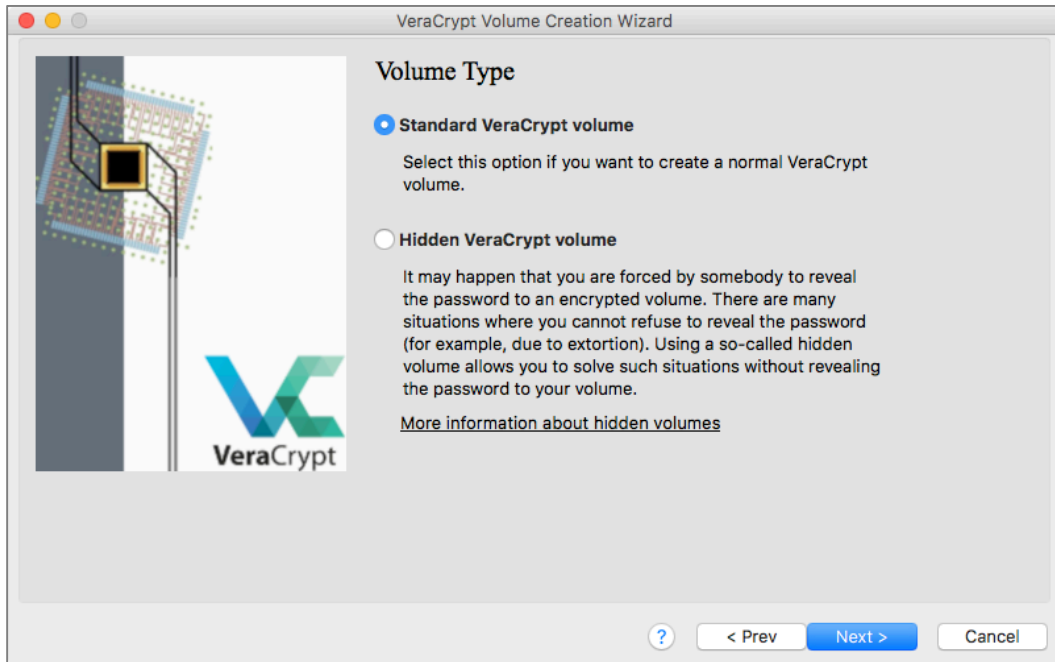


⁷ <https://veracrypt.codeplex.com/documentation>

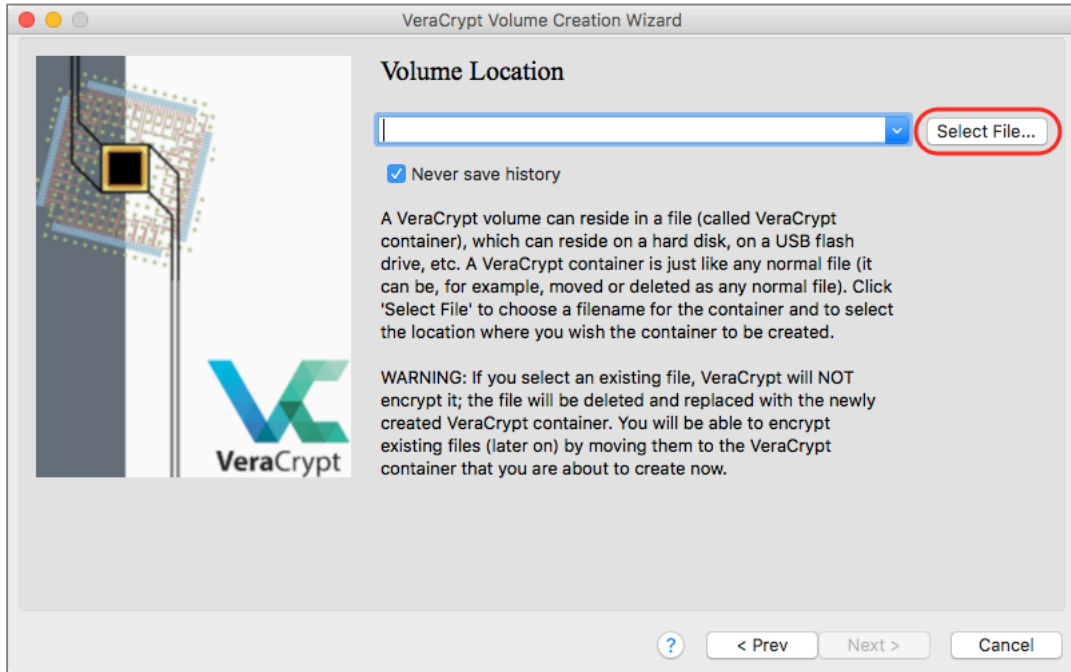
2. To create an encrypted container, at the *VeraCrypt Volume Creation Wizard*, select the *Create an encrypted file container* radio button, and then select the *Next>* button.



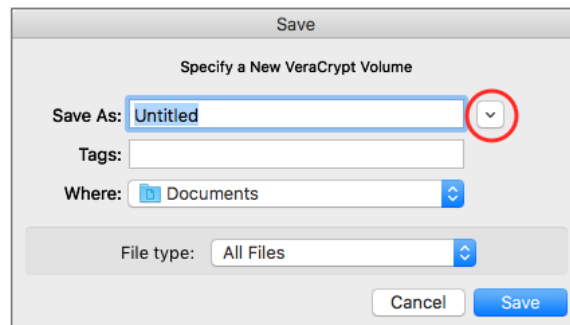
3. At the *Volume Type* window, select the *Standard VeraCrypt volume* radio button, and then select the *Next>* button.



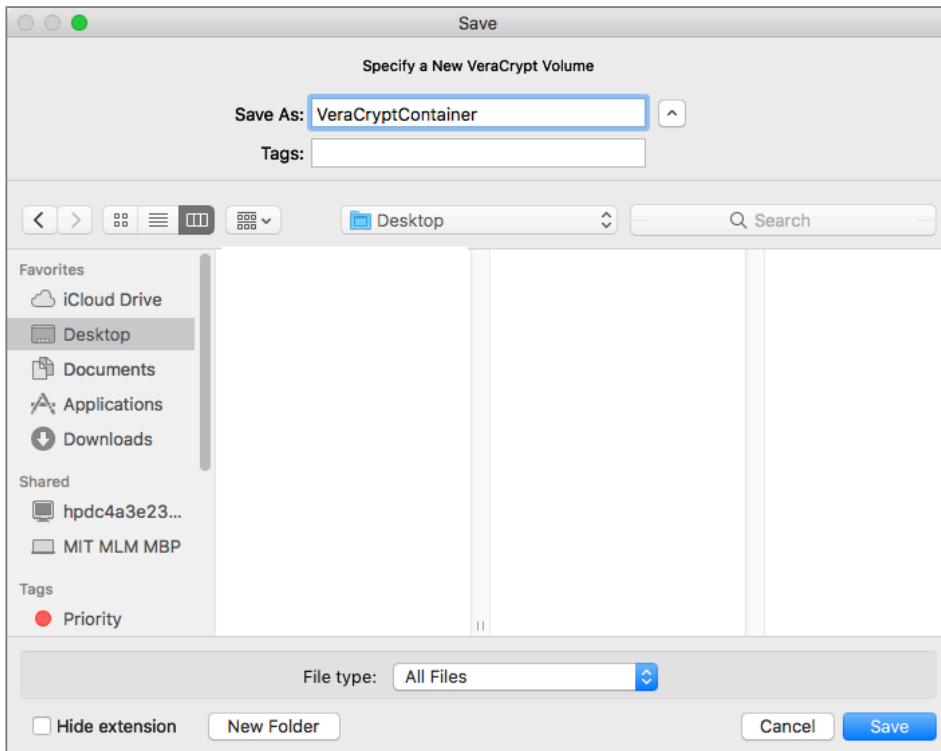
4. At the *Volume Location* window, select the *Select File...* button.



5. When the *Save* window appears, select the *Disclosure arrow* to the right of the *Save As* field. This will expand the window, making it easier to select where to save the container.



17 Documents

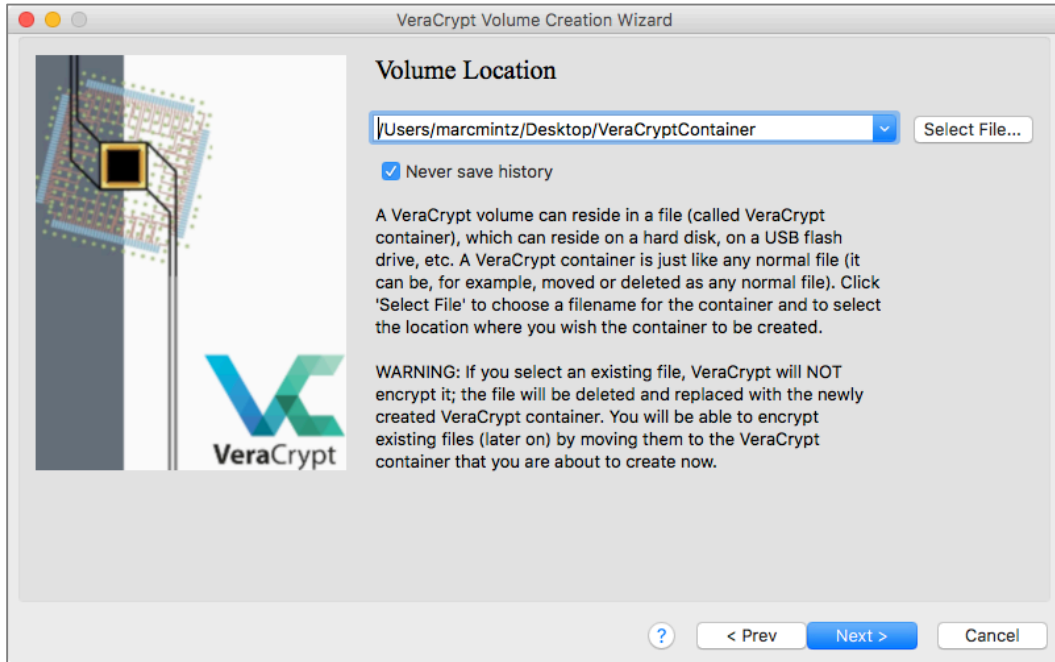


6. In the *Save As* field, enter a name for your container. For this assignment, use *VeraCryptContainer*.

Navigate to where you wish to save your container. For this assignment, use the *Desktop*.

7. Click the *Save* button.

8. When returned to the *Volume Location* window, select the *Next>* button.

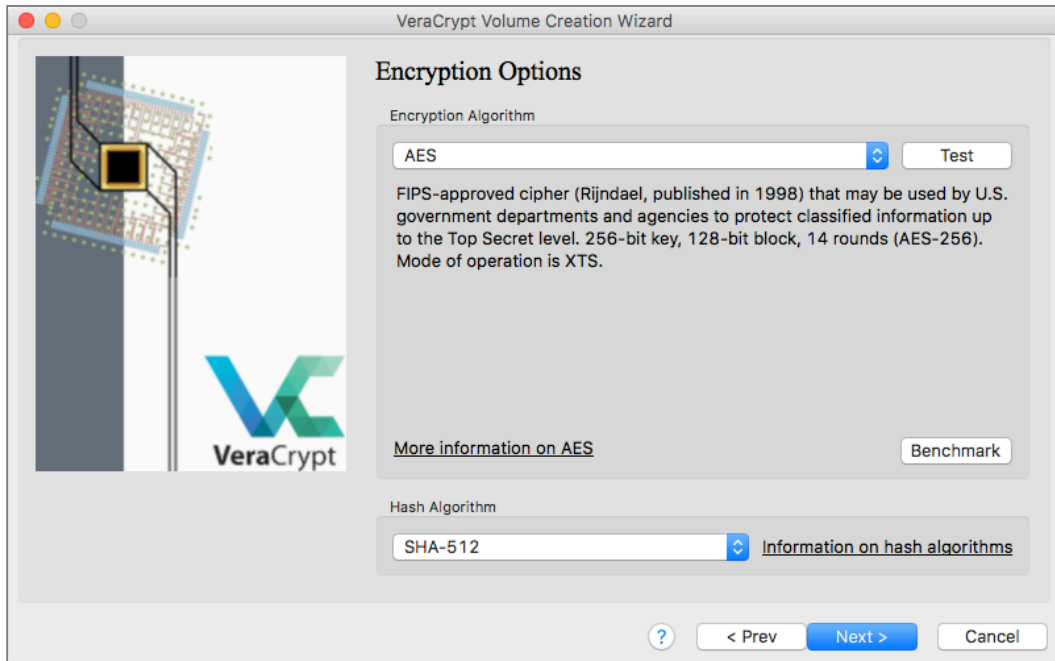


9. In the *Encryption Options* window, configure as below:

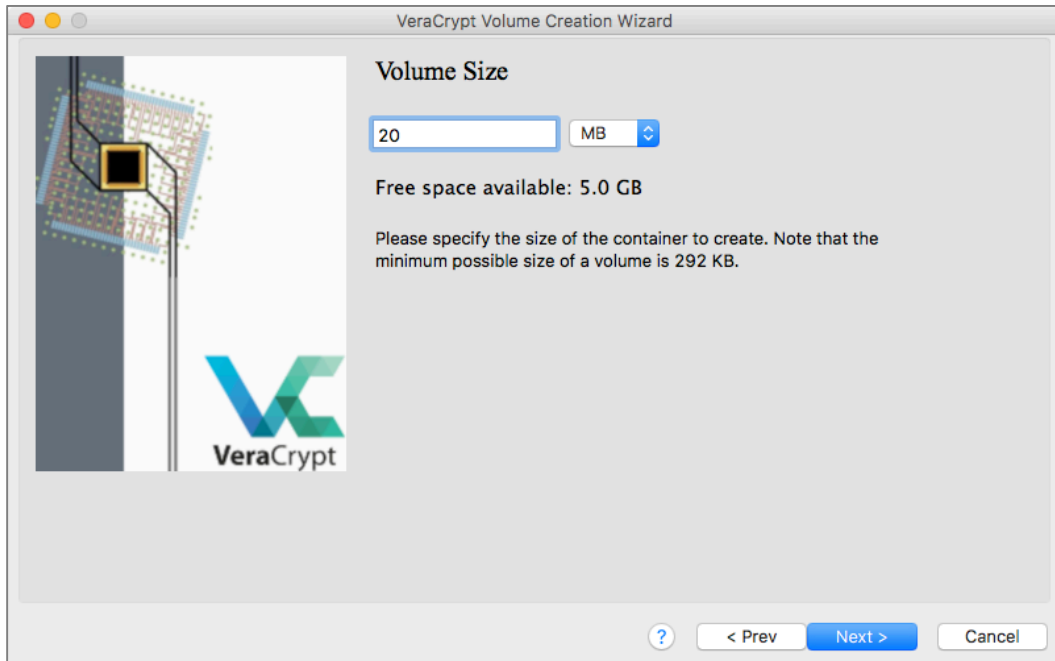
- From the *Encryption Algorithm* pop-up menu, select your desired option. *AES* is the industry standard, however, as the NSA and NIST were involved with its acceptance, some experts recommend selecting another option.
- From the *Hash Algorithm* pop-up menu, select the desired option. *SHA* was developed by the NSA, so some experts recommend selecting

Whirlpool. For our example, we will use the industry standards—AES and SHA-512.

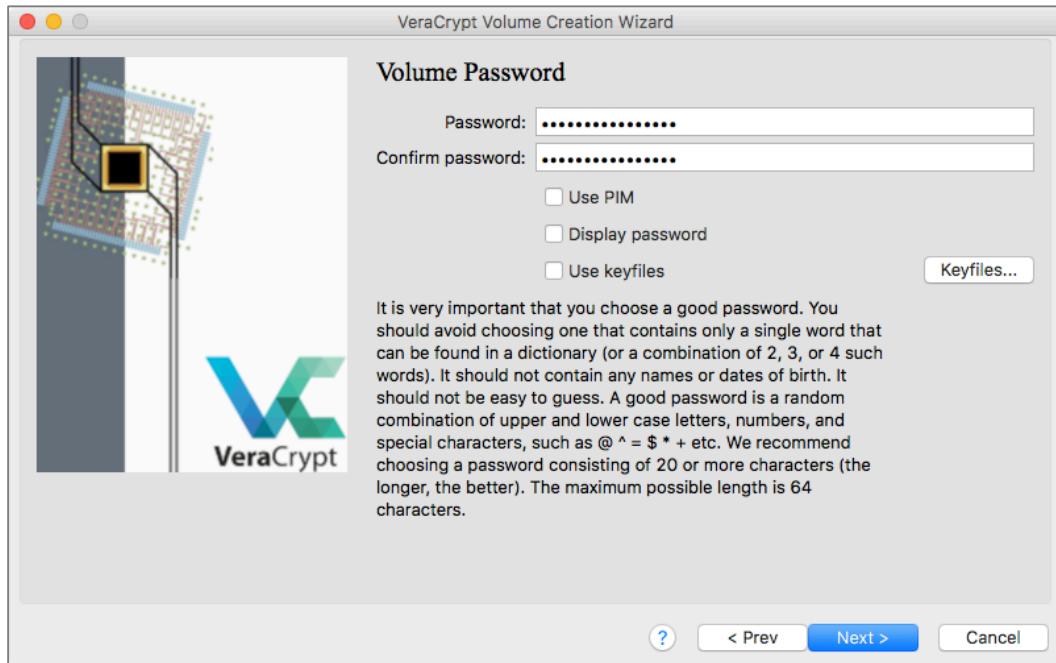
- Select the *Next>* button.



10. In the *Volume Size* window, set the size of your container. If you intend to email the container, keep in mind that each email provider has hard limits on the maximum file size that may be sent or received. If you intend to save the container to a storage device such as a thumb drive, keep in mind that a storage device needs approximately 20% free space for the directory and housekeeping needs. For this assignment, set *Volume Size* to 20MB, then select the *Next>* button.

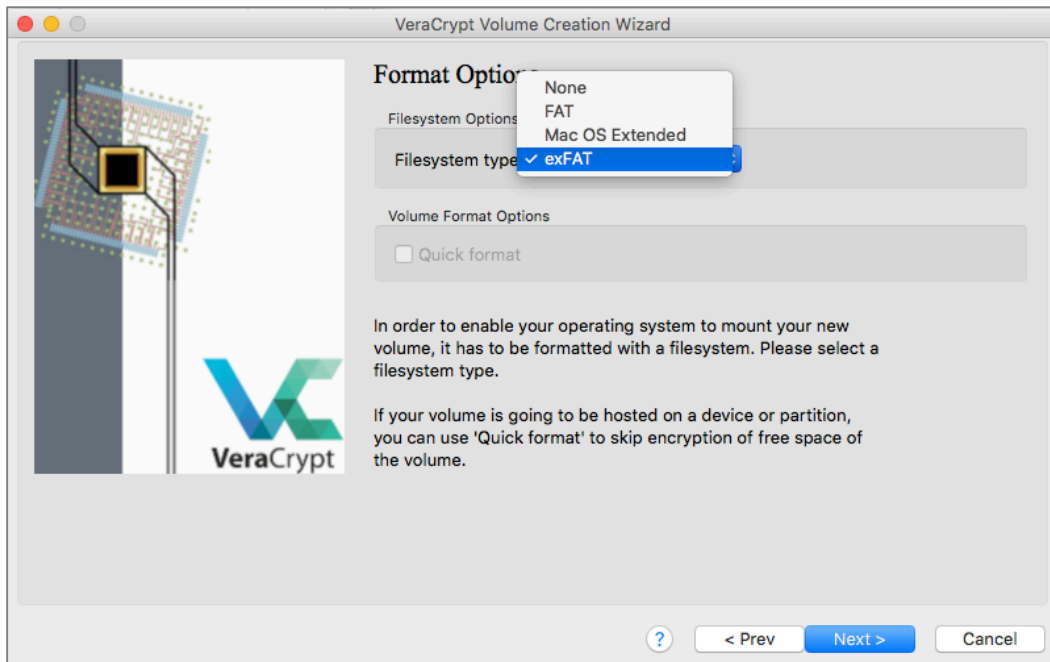


11. At the *Volume Password* window, in the *Password* and *Confirm Password* fields, enter a strong password for the container, and then select the *Next>* button.

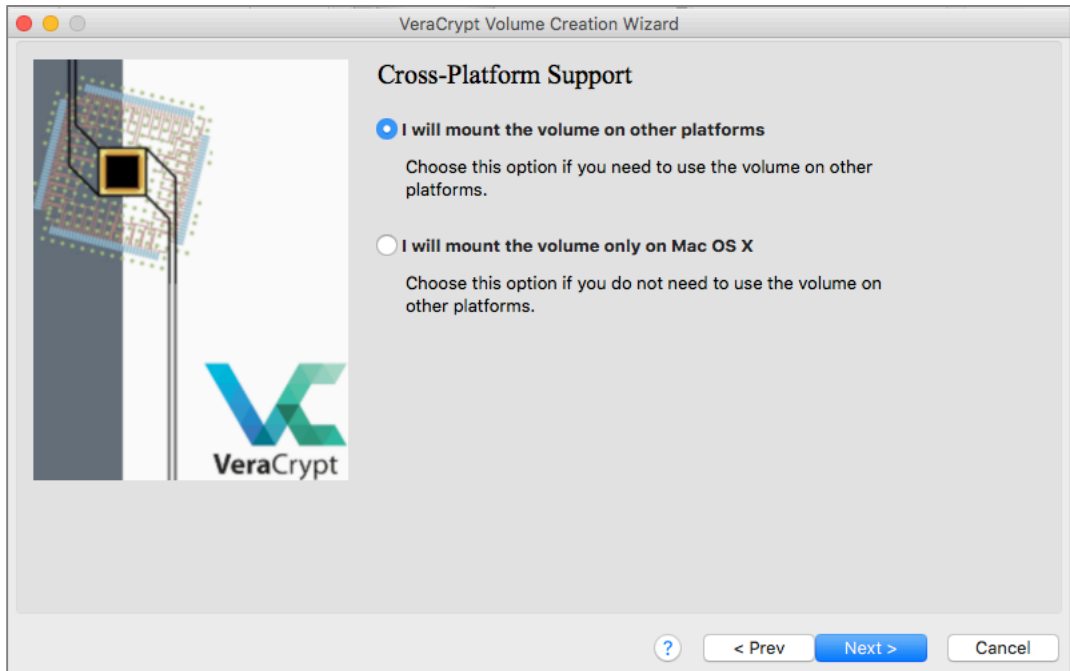


12. At the *Format Options* window, from the *Filesystem type* pop-up menu, select the desired option, and then select the *Next>* button. For this assignment, the *Filesystem type* is *exFAT*.

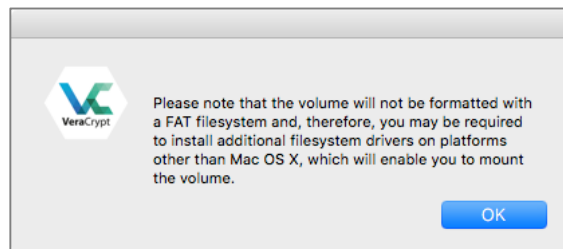
- *FAT* offers full compatibility for Linux and Windows use. macOS can read and write to FAT, but one should not hold macOS applications here as they may not function properly. It has a 4GB file size limit.
- *Mac OS Extended* offers full compatibility for macOS. Linux and Windows users are unable to read this format without the assistance of 3rd-party system add-ons. It has an 8EB file size limit.
- *exFAT* offers full compatibility with Windows and macOS, with modules available for Linux. It has a 16EB file size limit.



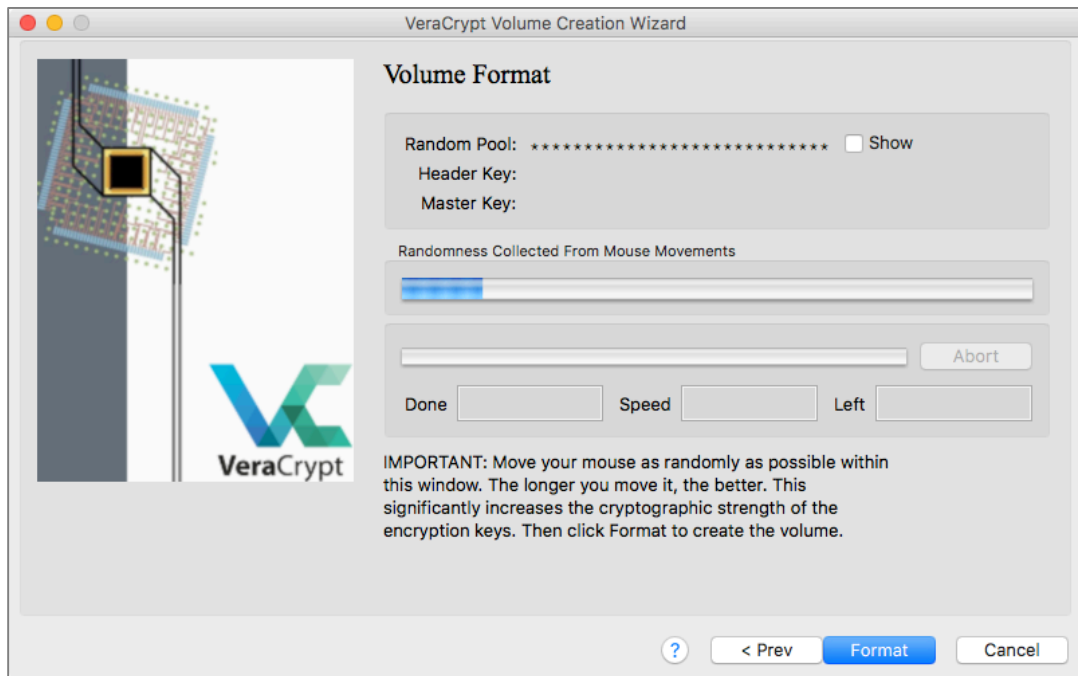
13. At the *Cross-Platform Support* window, select *I will mount the volume on other platforms*.



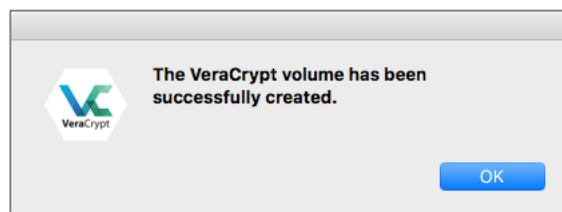
14. As we are selecting the exFAT volume structure, an alert will appear. Click *OK*.



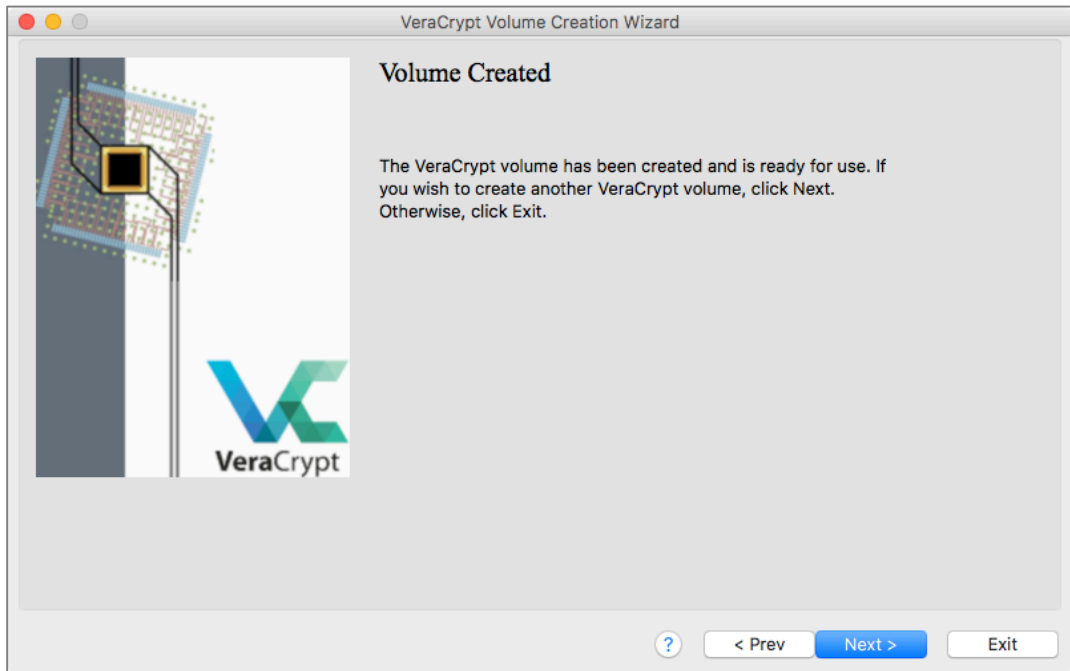
15. At the *Volume Format* window, move your cursor as randomly as possible within the window for at least 30 seconds, and then select the *Format* button.



16. Once the container encryption has completed, the *Success* alert appears. Select the *OK* button.



17. At the *Volume Created* window, select the *Exit>* button.



18. You will now find, at the location you specified earlier, the encrypted container.



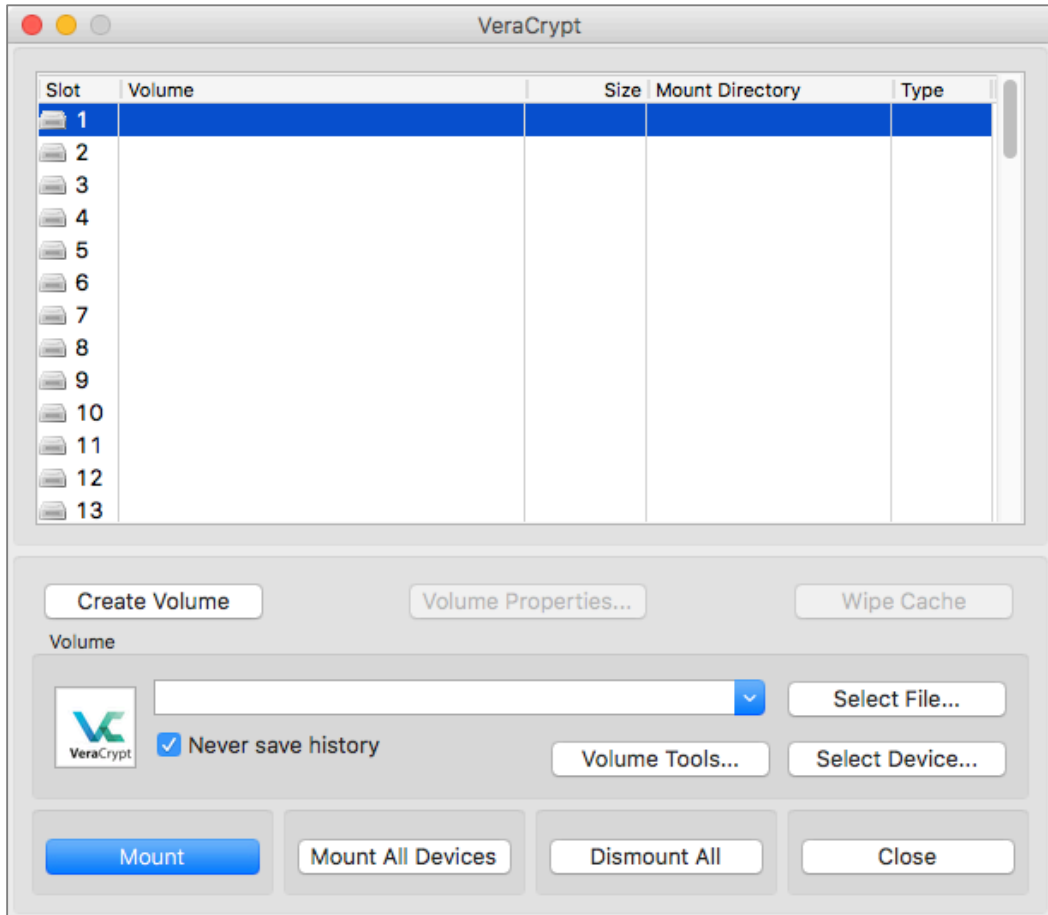
Congratulations, you have created your first truly spy-class encryption!

17.6.4 Assignment: Mount an Encrypted VeraCrypt Container

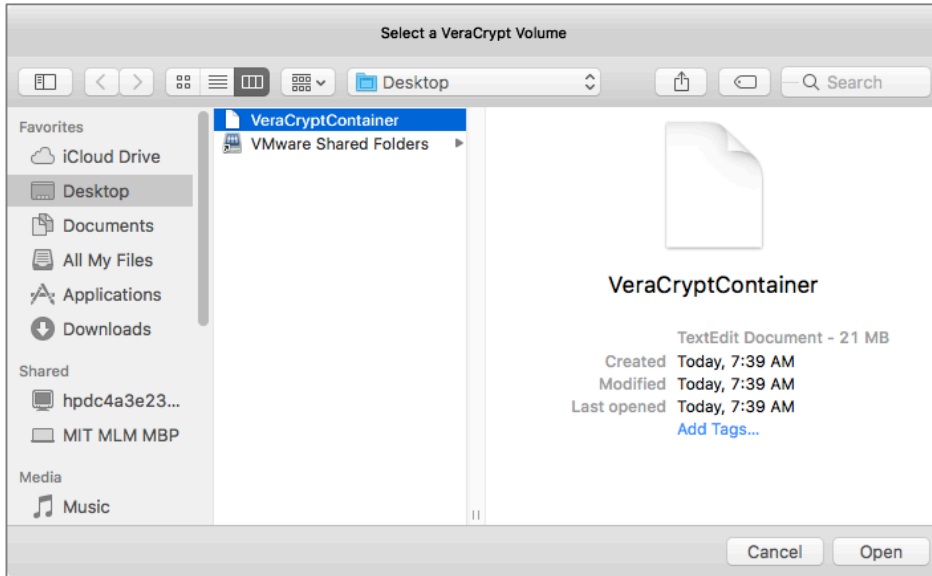
Once you have a VeraCrypt container, you eventually need to open it to read the contents, add to the container, or make edits to the files.

In this assignment, you will mount the VeraCrypt container, which gives you access to all its data.

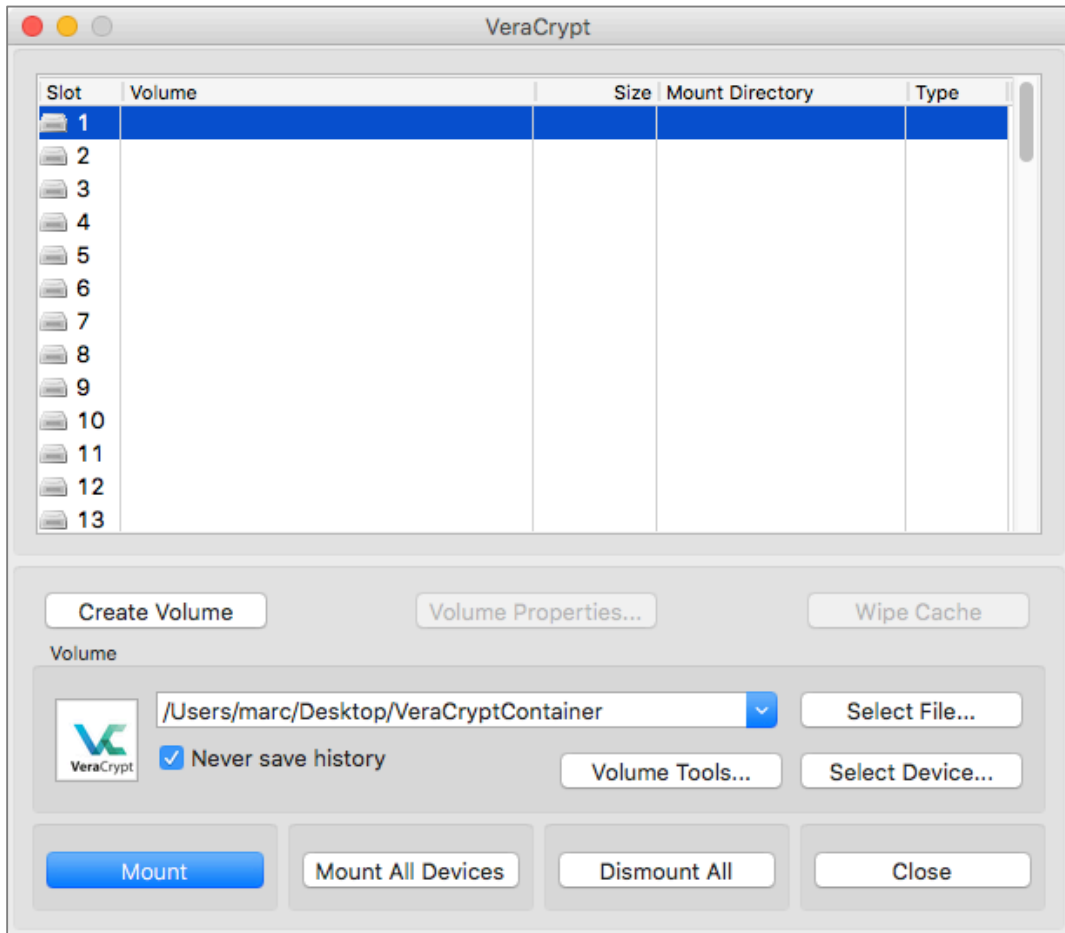
- Prerequisite: Completion of the previous assignment.
1. Open *VeraCrypt*, and then select one of the *Slot* numbers along the left side bar. This will become the temporary number of the VeraCrypt container to be mounted. Select the *Select File...* button.



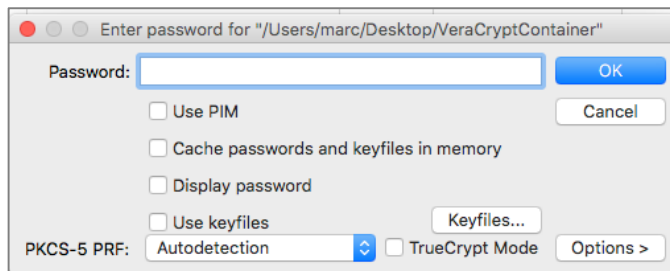
2. Select the *Select File...* button. The standard *Open* window appears. Navigate to the folder holding the target container. Select the container, and then select the *Open* button.



3. In the VeraCrypt window, select the *Mount* button.



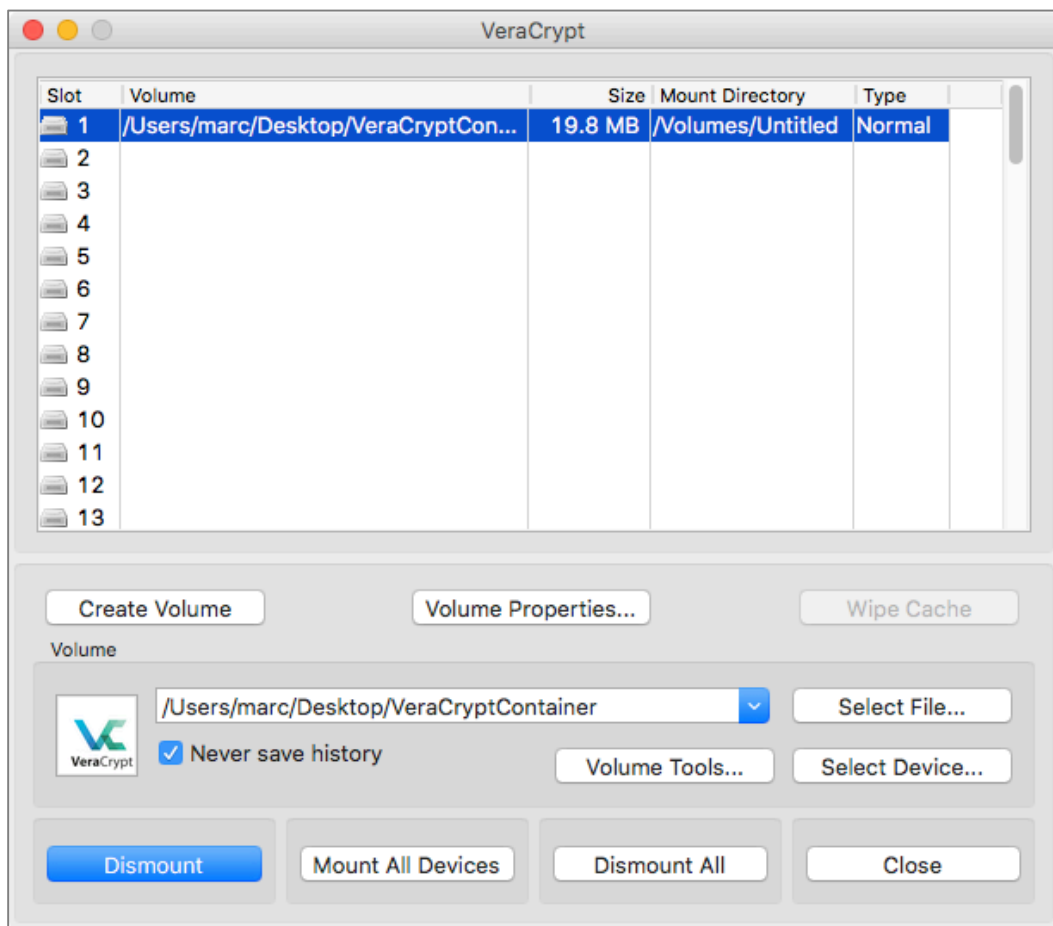
4. The *Enter password* window appears. Enter the password assigned to the container, and then select the *OK* button.



- On your Desktop, you will see the mounted volume, named *Untitled*. Double-click to open the volume.



- You may rename the mounted volume as you would any other item.
- You may drag and drop or save files and folder into the container.
- To unmount, return to the VeraCrypt window, and then select the *Dismount* button. The mounted volume will disappear from the Desktop.



OMG... You *really* are doing high-end security work now! This container may be copied to a thumb drive, optical disc, DropBox, Google Drive, or other Cloud-based storage, and remain secure.

Revision Log

20171001, v1.1

- Updated chapter *Documents > Encrypt A Folder for Cross Platform Use With Zip* to use Keka, instead of the depreciated macOS built-in tools.

20170923, v1.01

- Updated chapter *When It Is Time To Say Goodbye*

20170918, v1.0

- Initial release