Passware Kit Forensic 2021

Quick Start Guide

This guide covers:

- Detecting encrypted files and containers
- Recovering a file password
- Using the Dictionary Manager tool
- Customizing password recovery settings
- Extracting passwords from a memory image
- Decrypting a Keychain
- Decrypting a VeraCrypt container

Last updated: April 2021

Before You Begin

To get started with this guide, please follow the steps below:

1. Install Passware Kit Forensic 2021

Passware customers can download the software from Passware Account. If you do not own a Passware Kit license yet, please download Passware Kit Forensic Demo and review the list of limitations below.

2. Check for updates

Select "Check for Updates…" from the Help menu or download the latest version from Passware Account.

3. Get sample files

Download files.

Passware Kit Forensic Demo version limitations:

- Recovers either the first 3 letters of passwords or passwords containing no more than 3 characters
- Allows each of the attacks to run for up to 1 minute
- 64 MB limitation for VeraCrypt volume size

Passware Tip: *Contact Sales Team to get a fully functional time-limited evaluation version of Passware Kit Forensic (available to Law Enforcement only).*

System Requirements

PC platforms: Microsoft Windows Vista, Server 2003/2008/2012/2016/2019, or Windows 7/8.x/10 (64-bit only).
macOS: Mojave, Catalina, Big Sur.

- 1 GHz processor (2.4 GHz recommended)
- 1 GB of RAM (4 GB recommended)
- 1 GB of free hard disk space (more if you use custom dictionaries). For hardware acceleration on some strong file types, it is recommended to have 2 x (RAM + GPUs RAM) of free disk space for paging file.

GPU: GPU (Graphics Processing Unit) cards allow users to accelerate password recovery by up to 400 times compared to CPU-only systems. Passware Kit supports almost all types of NVIDIA (GTX, Tesla) and AMD GPUs.
Follow the link to get more information on hardware system and GPU recommendations.

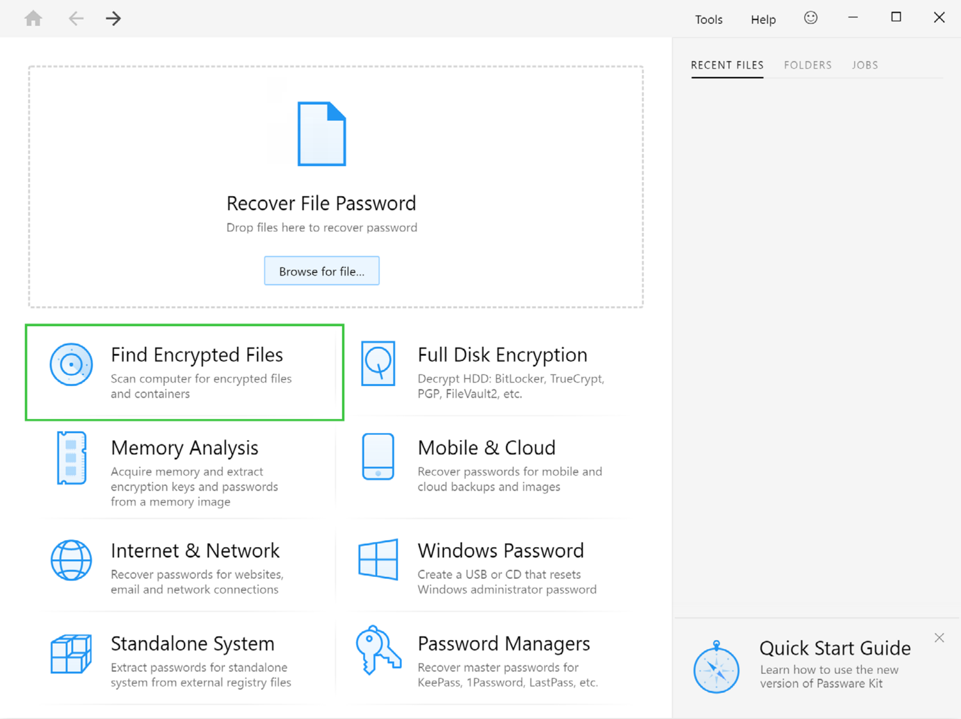
Passware Tip: *Passware Kit for Mac is a beta version. This beta is available for free to all Passware Kit Forensic customers with an active SMS subscription.*

Contents

Task 1

Detecting encrypted files and containers

1. On the Start page, click **Find Encrypted Files**:



Recover File Password
Drop files here to recover password

Find Encrypted Files
Scan computer for encrypted files and containers

Full Disk Encryption
Decrypt HDD: BitLocker, TrueCrypt, PGP, FileVault2, etc.

Memory Analysis
Acquire memory and extract encryption keys and passwords from a memory image

Mobile & Cloud
Recover passwords for mobile and cloud backups and images

Internet & Network
Recover passwords for websites, email and network connections

Windows Password
Create a USB or CD that resets Windows administrator password

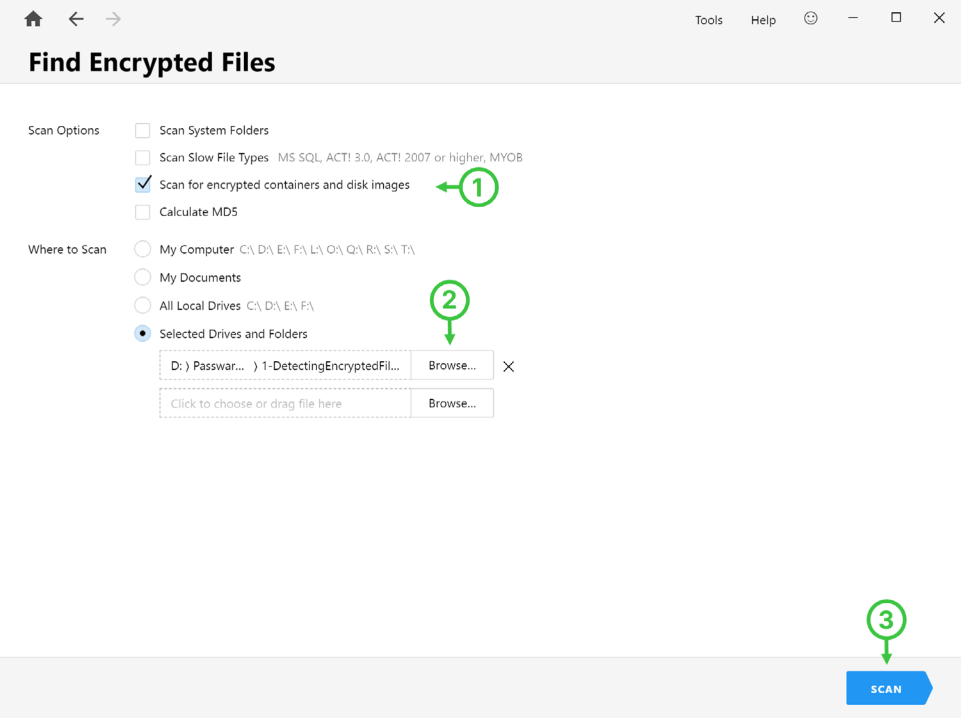
Standalone System
Extract passwords for standalone system from external registry files

Password Managers
Recover master passwords for KeePass, 1Password, LastPass, etc.

Quick Start Guide
Learn how to use the new version of Passware Kit

2. Enable the checkbox **Scan for encrypted containers and disk images,** click **Browse** and select the folder **1-DetectingEncryptedFiles** to scan:

Click **Scan**.

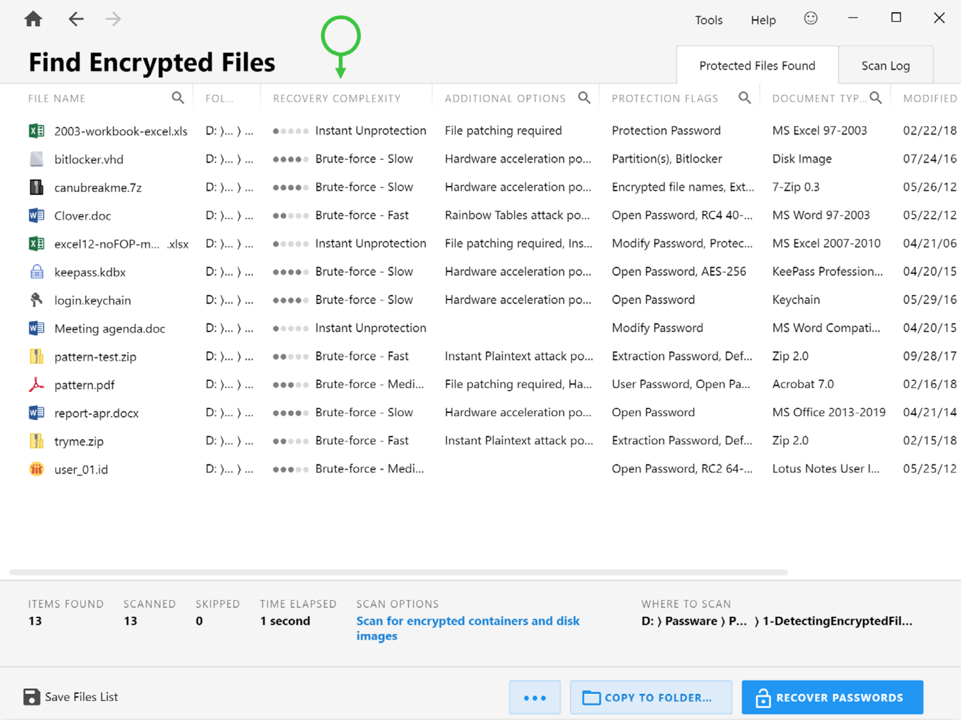


Find Encrypted Files

Scan Options
□ Scan System Folders
□ Scan Slow File Types MS SQL, ACT! 3.0, ACT! 2007 or higher, MYOB
☑ Scan for encrypted containers and disk images
□ Calculate MD5

Where to Scan
○ My Computer C:\ D:\ E:\ F:\ L:\ O:\ Q:\ R:\ S:\ T:\
○ My Documents
○ All Local Drives C:\ D:\ E:\ F:\
● Selected Drives and Folders
D: ⟩ Passwar... ⟩ 1-DetectingEncryptedFil...
Click to choose or drag file here

3. Passware Kit lists the encrypted files along with the detailed information about them, such as **Recovery Complexity, Protection Flags, Date Modified,** etc. Click **Recovery Complexity** to sort the files by the encryption strength.



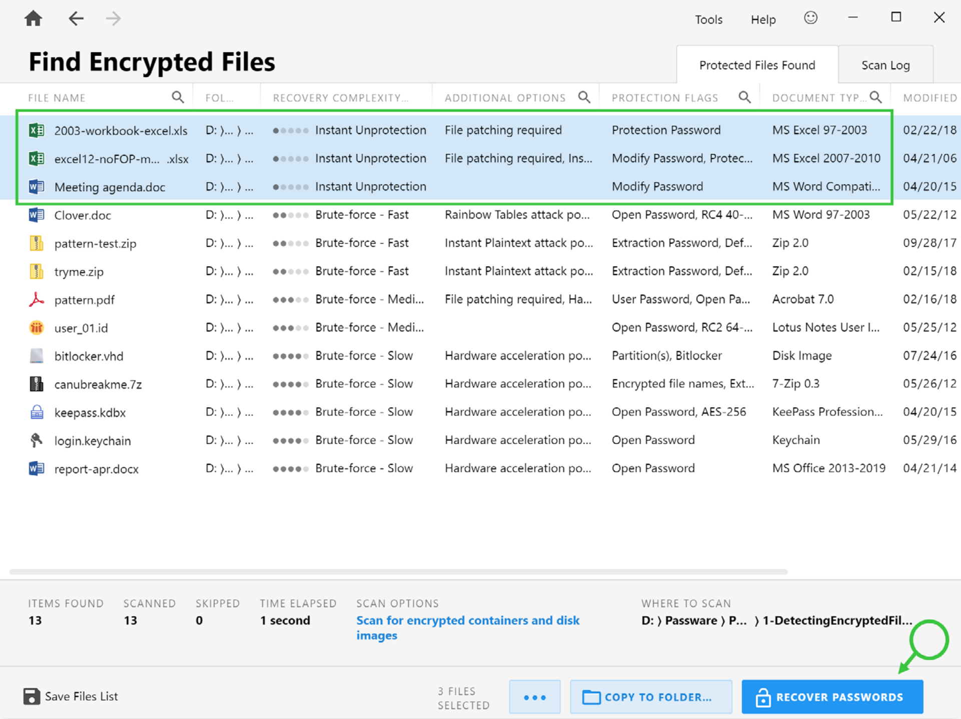
Find Encrypted Files

FILE NAME	FOL...	RECOVERY COMPLEXITY	ADDITIONAL OPTIONS	PROTECTION FLAGS	DOCUMENT TYP...	MODIFIED
2003-workbook-excel.xls	D: ⟩... ⟩ ...	●○○○○ Instant Unprotection	File patching required	Protection Password	MS Excel 97-2003	02/22/18
bitlocker.vhd	D: ⟩... ⟩ ...	●●●●○ Brute-force - Slow	Hardware acceleration po...	Partition(s), Bitlocker	Disk Image	07/24/16
canubreakme.7z	D: ⟩... ⟩ ...	●●●●○ Brute-force - Slow	Hardware acceleration po...	Encrypted file names, Ext...	7-Zip 0.3	05/26/12
Clover.doc	D: ⟩... ⟩ ...	●●○○○ Brute-force - Fast	Rainbow Tables attack po...	Open Password, RC4 40-...	MS Word 97-2003	05/22/12
excel12-noFOP-m... .xlsx	D: ⟩... ⟩ ...	●○○○○ Instant Unprotection	File patching required, Ins...	Modify Password, Protec...	MS Excel 2007-2010	04/21/06
keepass.kdbx	D: ⟩... ⟩ ...	●●●●○ Brute-force - Slow	Hardware acceleration po...	Open Password, AES-256	KeePass Profession...	04/20/15
login.keychain	D: ⟩... ⟩ ...	●●●●○ Brute-force - Slow	Hardware acceleration po...	Open Password	Keychain	05/29/16
Meeting agenda.doc	D: ⟩... ⟩ ...	●○○○○ Instant Unprotection		Modify Password	MS Word Compati...	04/20/15
pattern-test.zip	D: ⟩... ⟩ ...	●●○○○ Brute-force - Fast	Instant Plaintext attack po...	Extraction Password, Def...	Zip 2.0	09/28/17
pattern.pdf	D: ⟩... ⟩ ...	●●●○○ Brute-force - Medi...	File patching required, Ha...	User Password, Open Pa...	Acrobat 7.0	02/16/18
report-apr.docx	D: ⟩... ⟩ ...	●●●●○ Brute-force - Slow	Hardware acceleration po...	Open Password	MS Office 2013-2019	04/21/14
tryme.zip	D: ⟩... ⟩ ...	●●○○○ Brute-force - Fast	Instant Plaintext attack po...	Extraction Password, Def...	Zip 2.0	02/15/18
user_01.id	D: ⟩... ⟩ ...	●●●○○ Brute-force - Medi...		Open Password, RC2 64-...	Lotus Notes User I...	05/25/12

ITEMS FOUND	SCANNED	SKIPPED	TIME ELAPSED	SCAN OPTIONS	WHERE TO SCAN
13	13	0	1 second	Scan for encrypted containers and disk images	D: ⟩ Passware ⟩ P... ⟩ 1-DetectingEncryptedFil...

Passware Tip: *Do not lose the results of the search. Use the* ***Save Files List*** *option to save the list of found encrypted items into* ***Passware Job File*** *(*.pwjf). To load the list back, choose* ***JOBS*** *in the right panel on the* ***Start Page****. Click* ***Open Job*** *and browse for the saved* ***Passware Job File****.*

4. Optionally: Select the files (use **Ctrl-click** to select dedicated files or **Shift-click** to select multiple items at once) that you want to decrypt, starting from files with **Instant Unprotection** complexity and moving on to files with stronger encryption, such as archives or containers. Click **Recover Passwords** to proceed with password recovery and decryption in batch mode.



Find Encrypted Files

FILE NAME	FOL...	RECOVERY COMPLEXITY...	ADDITIONAL OPTIONS	PROTECTION FLAGS	DOCUMENT TYP...	MODIFIED
2003-workbook-excel.xls	D: ⟩... ⟩ ...	●○○○○ Instant Unprotection	File patching required	Protection Password	MS Excel 97-2003	02/22/18
excel12-noFOP-m... .xlsx	D: ⟩... ⟩ ...	●○○○○ Instant Unprotection	File patching required, Ins...	Modify Password, Protec...	MS Excel 2007-2010	04/21/06
Meeting agenda.doc	D: ⟩... ⟩ ...	●○○○○ Instant Unprotection		Modify Password	MS Word Compati...	04/20/15
Clover.doc	D: ⟩... ⟩ ...	●●○○○ Brute-force - Fast	Rainbow Tables attack po...	Open Password, RC4 40-...	MS Word 97-2003	05/22/12
pattern-test.zip	D: ⟩... ⟩ ...	●●○○○ Brute-force - Fast	Instant Plaintext attack po...	Extraction Password, Def...	Zip 2.0	09/28/17
tryme.zip	D: ⟩... ⟩ ...	●●○○○ Brute-force - Fast	Instant Plaintext attack po...	Extraction Password, Def...	Zip 2.0	02/15/18
pattern.pdf	D: ⟩... ⟩ ...	●●●○○ Brute-force - Medi...	File patching required, Ha...	User Password, Open Pa...	Acrobat 7.0	02/16/18
user_01.id	D: ⟩... ⟩ ...	●●●○○ Brute-force - Medi...		Open Password, RC2 64-...	Lotus Notes User I...	05/25/12
bitlocker.vhd	D: ⟩... ⟩ ...	●●●●○ Brute-force - Slow	Hardware acceleration po...	Partition(s), Bitlocker	Disk Image	07/24/16
canubreakme.7z	D: ⟩... ⟩ ...	●●●●○ Brute-force - Slow	Hardware acceleration po...	Encrypted file names, Ext...	7-Zip 0.3	05/26/12
keepass.kdbx	D: ⟩... ⟩ ...	●●●●○ Brute-force - Slow	Hardware acceleration po...	Open Password, AES-256	KeePass Profession...	04/20/15
login.keychain	D: ⟩... ⟩ ...	●●●●○ Brute-force - Slow	Hardware acceleration po...	Open Password	Keychain	05/29/16
report-apr.docx	D: ⟩... ⟩ ...	●●●●○ Brute-force - Slow	Hardware acceleration po...	Open Password	MS Office 2013-2019	04/21/14

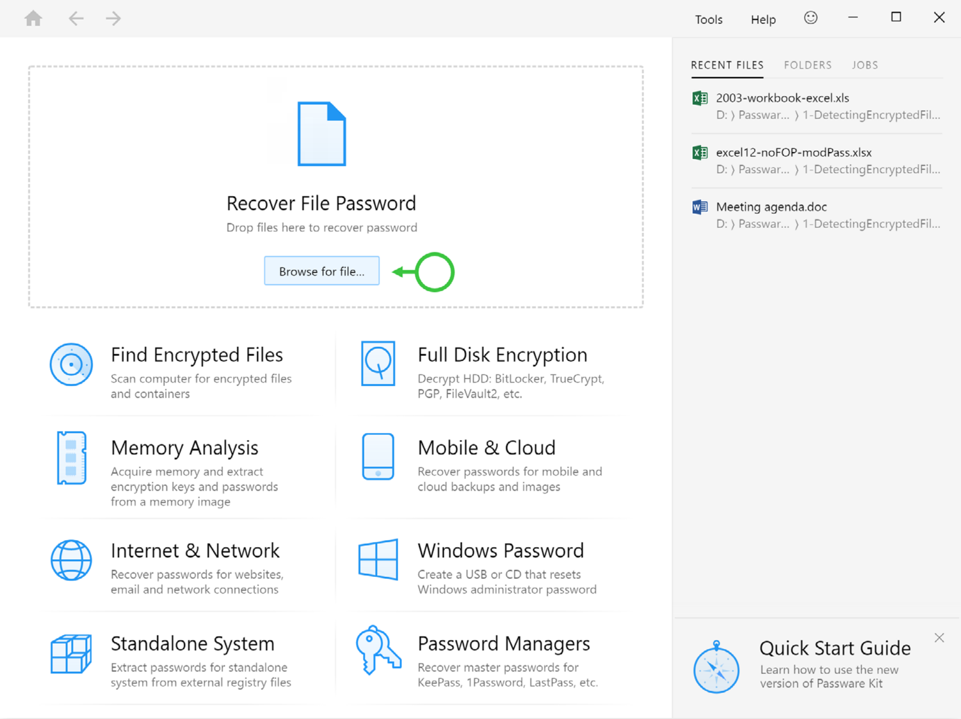
ITEMS FOUND	SCANNED	SKIPPED	TIME ELAPSED	SCAN OPTIONS	WHERE TO SCAN
13	13	0	1 second	Scan for encrypted containers and disk images	D: ⟩ Passware ⟩ P... ⟩ 1-DetectingEncryptedFil...

Passware Tip: *Check out 5 Tips for Discovering and Analyzing Encrypted Electronic Evidence.*

Task 2

Recovering a file password

1. On the Start page, click **Recover File Password**:



Recover File Password
Drop files here to recover password

Find Encrypted Files
Scan computer for encrypted files and containers

Full Disk Encryption
Decrypt HDD: BitLocker, TrueCrypt, PGP, FileVault2, etc.

Memory Analysis
Acquire memory and extract encryption keys and passwords from a memory image

Mobile & Cloud
Recover passwords for mobile and cloud backups and images

Internet & Network
Recover passwords for websites, email and network connections

Windows Password
Create a USB or CD that resets Windows administrator password

Standalone System
Extract passwords for standalone system from external registry files

Password Managers
Recover master passwords for KeePass, 1Password, LastPass, etc.

2003-workbook-excel.xls
D:) Passwar...) 1-DetectingEncryptedFil...

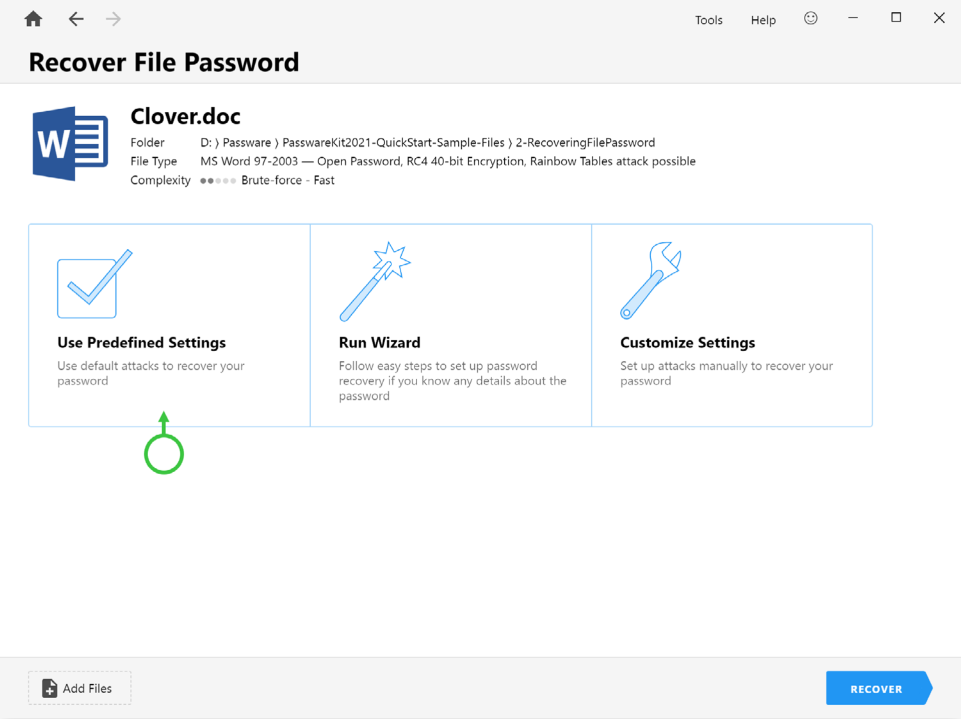
excel12-noFOP-modPass.xlsx
D:) Passwar...) 1-DetectingEncryptedFil...

Meeting agenda.doc
D:) Passwar...) 1-DetectingEncryptedFil...

Quick Start Guide
Learn how to use the new version of Passware Kit

2. Browse for the file **Clover.doc** from the **2-RecoveringFilePassword** folder and click **Open**.

3. Choose **Use Predefined Settings**:



Recover File Password

Clover.doc

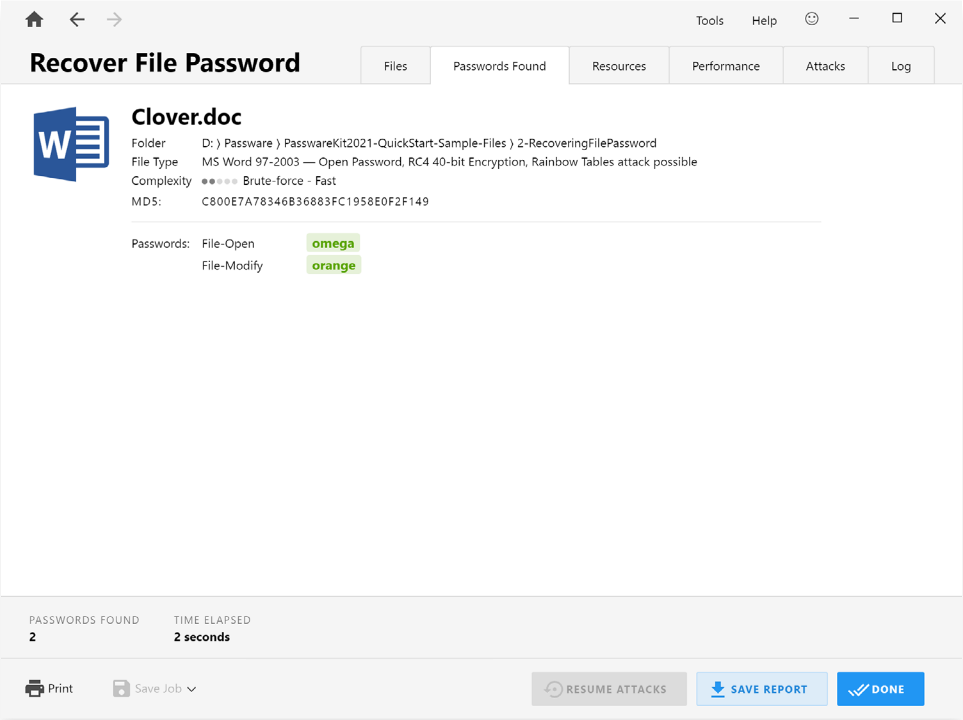
Folder D:) Passware) PasswareKit2021-QuickStart-Sample-Files) 2-RecoveringFilePassword
File Type MS Word 97-2003 — Open Password, RC4 40-bit Encryption, Rainbow Tables attack possible
Complexity ●●○○○ Brute-force - Fast

Use Predefined Settings
Use default attacks to recover your password

Run Wizard
Follow easy steps to set up password recovery if you know any details about the password

Customize Settings
Set up attacks manually to recover your password

4. Passware Kit applies its built-in English dictionary to the file and recovers the password:



Clover.doc

Folder D:) Passware) PasswareKit2021-QuickStart-Sample-Files) 2-RecoveringFilePassword
File Type MS Word 97-2003 — Open Password, RC4 40-bit Encryption, Rainbow Tables attack possible
Complexity ●●○○○ Brute-force - Fast
MD5: C800E7A78346B36883FC1958E0F2F149

Passwords: File-Open omega
File-Modify orange

PASSWORDS FOUND
2

TIME ELAPSED
2 seconds

Passware Tip: *Passware Kit provides comprehensive details on the recovery process. Check out all available tabs: Files, Resources, Performance, Attacks, and Log.*

Task 3

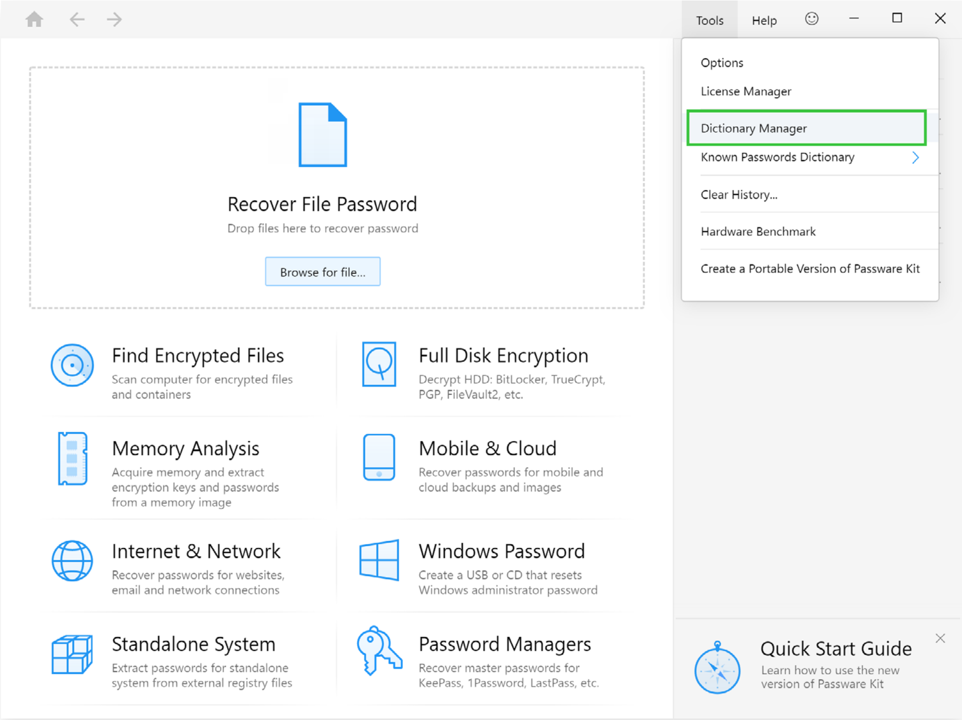
Using the Dictionary Manager tool

Dictionary Manager is a built-in tool for managing dictionaries and wordlists used by the Dictionary attack. The password for the file **Capital.zip** is a capital name. To recover this type of password, use the list of capitals as a custom dictionary file (**capitals-dictionary.txt** from the **3-UsingDictionaryManager** folder).

Such a list could be created manually as a text file or downloaded from wordlist resources. Learn more about dictionaries from Passware Knowledge Base.

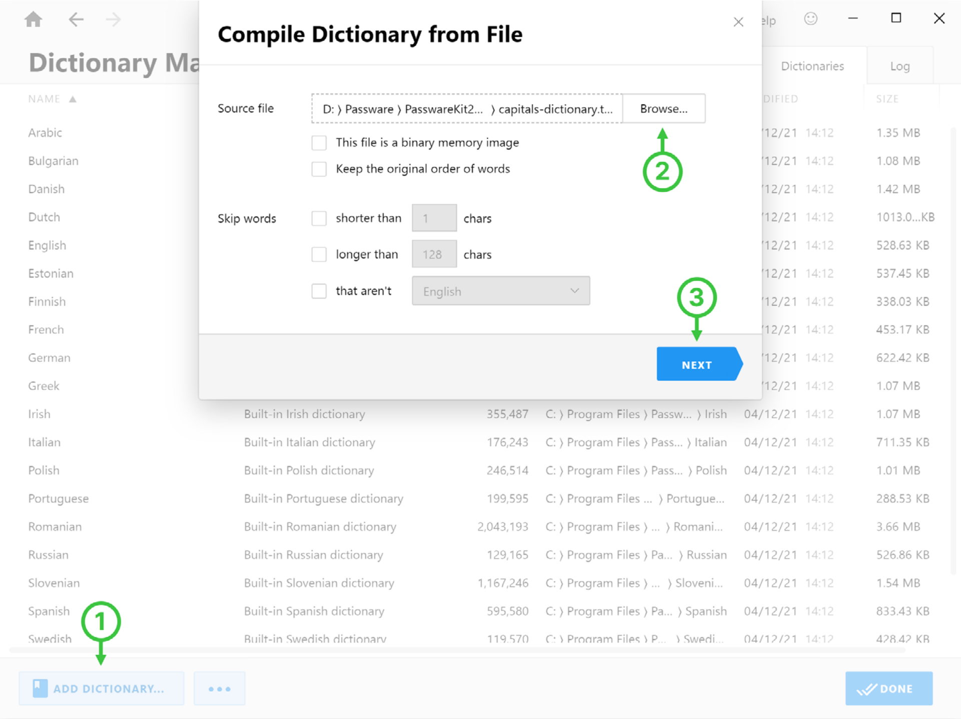
Passware Tip: *All Passware Kit Forensic customers have access to a selection of proprietary Passware dictionaries available at Passware Account on the "Free Dictionaries" tab.*

1. On the Start page, click **Tools** and select **Dictionary Manager**:


Tools
Help
Options
License Manager
Dictionary Manager
Known Passwords Dictionary
Clear History...
Hardware Benchmark
Create a Portable Version of Passware Kit
Recover File Password
Drop files here to recover password
Browse for file...
Find Encrypted Files
Scan computer for encrypted files and containers
Full Disk Encryption
Decrypt HDD: BitLocker, TrueCrypt, PGP, FileVault2, etc.
Memory Analysis
Acquire memory and extract encryption keys and passwords from a memory image
Mobile & Cloud
Recover passwords for mobile and cloud backups and images
Internet & Network
Recover passwords for websites, email and network connections
Windows Password
Create a USB or CD that resets Windows administrator password
Standalone System
Extract passwords for standalone system from external registry files
Password Managers
Recover master passwords for KeePass, 1Password, LastPass, etc.
Quick Start Guide
Learn how to use the new version of Passware Kit

2. In the **Dictionary Manager** window, click **Add Dictionary** and choose **Compile from File**.... Locate the file **capitals.txt** (a custom list of capitals, which is supposed to be used as a dictionary) and click **Next**.

Click **Compile** to proceed:



Compile Dictionary from File

Source file: D: ⟩ Passware ⟩ PasswareKit2... ⟩ capitals-dictionary.t... Browse...

□ This file is a binary memory image

□ Keep the original order of words

Skip words:

□ shorter than 1 chars

□ longer than 128 chars

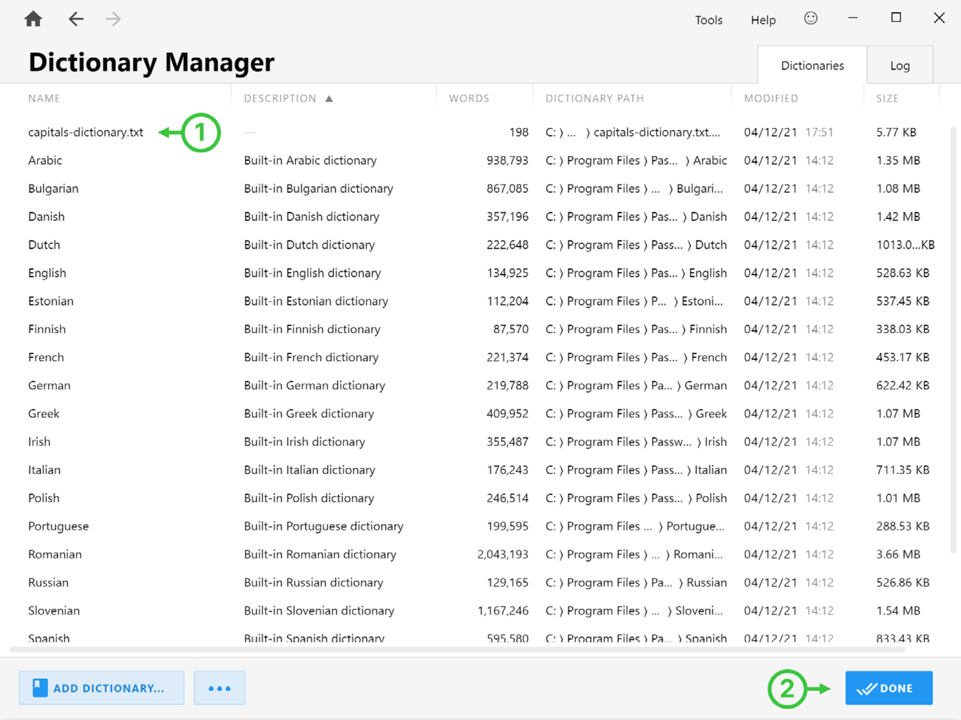
□ that aren't English

NAME ▲				…DIFIED	SIZE
Arabic				…12/21 14:12	1.35 MB
Bulgarian				…12/21 14:12	1.08 MB
Danish				…12/21 14:12	1.42 MB
Dutch				…12/21 14:12	1013.0...KB
English				…12/21 14:12	528.63 KB
Estonian				…12/21 14:12	537.45 KB
Finnish				…12/21 14:12	338.03 KB
French				…12/21 14:12	453.17 KB
German				…12/21 14:12	622.42 KB
Greek				…12/21 14:12	1.07 MB
Irish	Built-in Irish dictionary	355,487	C: ⟩ Program Files ⟩ Passw... ⟩ Irish	04/12/21 14:12	1.07 MB
Italian	Built-in Italian dictionary	176,243	C: ⟩ Program Files ⟩ Pass... ⟩ Italian	04/12/21 14:12	711.35 KB
Polish	Built-in Polish dictionary	246,514	C: ⟩ Program Files ⟩ Pass... ⟩ Polish	04/12/21 14:12	1.01 MB
Portuguese	Built-in Portuguese dictionary	199,595	C: ⟩ Program Files ... ⟩ Portugue...	04/12/21 14:12	288.53 KB
Romanian	Built-in Romanian dictionary	2,043,193	C: ⟩ Program Files ⟩ ... ⟩ Romani...	04/12/21 14:12	3.66 MB
Russian	Built-in Russian dictionary	129,165	C: ⟩ Program Files ⟩ Pa... ⟩ Russian	04/12/21 14:12	526.86 KB
Slovenian	Built-in Slovenian dictionary	1,167,246	C: ⟩ Program Files ⟩ ... ⟩ Sloveni...	04/12/21 14:12	1.54 MB
Spanish	Built-in Spanish dictionary	595,580	C: ⟩ Program Files ⟩ Pa... ⟩ Spanish	04/12/21 14:12	833.43 KB
Swedish	Built-in Swedish dictionary	119,570	C: ⟩ Program Files ⟩ P... ⟩ Swedi...	04/12/21 14:12	428.42 KB

Passware Tip: *Use the* ***Keep the original order of words*** *option to import password lists sorted by the frequency of use and length, not alphabetically.*

3. Passware Kit compiles the text file into a dictionary named **capitals-dictionary.txt**.

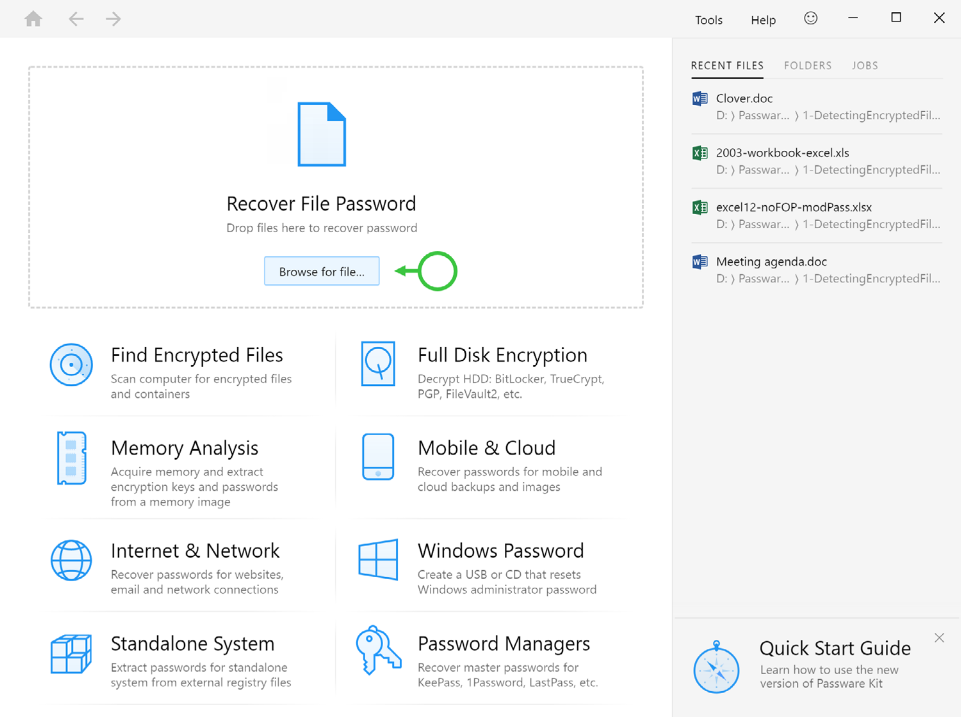
Click **Done**.



Dictionary Manager

NAME	DESCRIPTION ▲	WORDS	DICTIONARY PATH	MODIFIED	SIZE
capitals-dictionary.txt	—	198	C: ⟩ ... ⟩ capitals-dictionary.txt....	04/12/21 17:51	5.77 KB
Arabic	Built-in Arabic dictionary	938,793	C: ⟩ Program Files ⟩ Pas... ⟩ Arabic	04/12/21 14:12	1.35 MB
Bulgarian	Built-in Bulgarian dictionary	867,085	C: ⟩ Program Files ⟩ ... ⟩ Bulgari...	04/12/21 14:12	1.08 MB
Danish	Built-in Danish dictionary	357,196	C: ⟩ Program Files ⟩ Pas... ⟩ Danish	04/12/21 14:12	1.42 MB
Dutch	Built-in Dutch dictionary	222,648	C: ⟩ Program Files ⟩ Pass... ⟩ Dutch	04/12/21 14:12	1013.0...KB
English	Built-in English dictionary	134,925	C: ⟩ Program Files ⟩ Pas... ⟩ English	04/12/21 14:12	528.63 KB
Estonian	Built-in Estonian dictionary	112,204	C: ⟩ Program Files ⟩ P... ⟩ Estoni...	04/12/21 14:12	537.45 KB
Finnish	Built-in Finnish dictionary	87,570	C: ⟩ Program Files ⟩ Pas... ⟩ Finnish	04/12/21 14:12	338.03 KB
French	Built-in French dictionary	221,374	C: ⟩ Program Files ⟩ Pas... ⟩ French	04/12/21 14:12	453.17 KB
German	Built-in German dictionary	219,788	C: ⟩ Program Files ⟩ Pa... ⟩ German	04/12/21 14:12	622.42 KB
Greek	Built-in Greek dictionary	409,952	C: ⟩ Program Files ⟩ Pass... ⟩ Greek	04/12/21 14:12	1.07 MB
Irish	Built-in Irish dictionary	355,487	C: ⟩ Program Files ⟩ Passw... ⟩ Irish	04/12/21 14:12	1.07 MB
Italian	Built-in Italian dictionary	176,243	C: ⟩ Program Files ⟩ Pass... ⟩ Italian	04/12/21 14:12	711.35 KB
Polish	Built-in Polish dictionary	246,514	C: ⟩ Program Files ⟩ Pass... ⟩ Polish	04/12/21 14:12	1.01 MB
Portuguese	Built-in Portuguese dictionary	199,595	C: ⟩ Program Files ... ⟩ Portugue...	04/12/21 14:12	288.53 KB
Romanian	Built-in Romanian dictionary	2,043,193	C: ⟩ Program Files ⟩ ... ⟩ Romani...	04/12/21 14:12	3.66 MB
Russian	Built-in Russian dictionary	129,165	C: ⟩ Program Files ⟩ Pa... ⟩ Russian	04/12/21 14:12	526.86 KB
Slovenian	Built-in Slovenian dictionary	1,167,246	C: ⟩ Program Files ⟩ ... ⟩ Sloveni...	04/12/21 14:12	1.54 MB
Spanish	Built-in Spanish dictionary	595,580	C: ⟩ Program Files ⟩ Pa... ⟩ Spanish	04/12/21 14:12	833.43 KB

4. On the Start page, click **Recover File Password**:



Recover File Password

Drop files here to recover password

Browse for file...

RECENT FILES FOLDERS JOBS

Clover.doc
D: ⟩ Passwar... ⟩ 1-DetectingEncryptedFil...

2003-workbook-excel.xls
D: ⟩ Passwar... ⟩ 1-DetectingEncryptedFil...

excel12-noFOP-modPass.xlsx
D: ⟩ Passwar... ⟩ 1-DetectingEncryptedFil...

Meeting agenda.doc
D: ⟩ Passwar... ⟩ 1-DetectingEncryptedFil...

Find Encrypted Files
Scan computer for encrypted files and containers

Full Disk Encryption
Decrypt HDD: BitLocker, TrueCrypt, PGP, FileVault2, etc.

Memory Analysis
Acquire memory and extract encryption keys and passwords from a memory image

Mobile & Cloud
Recover passwords for mobile and cloud backups and images

Internet & Network
Recover passwords for websites, email and network connections

Windows Password
Create a USB or CD that resets Windows administrator password

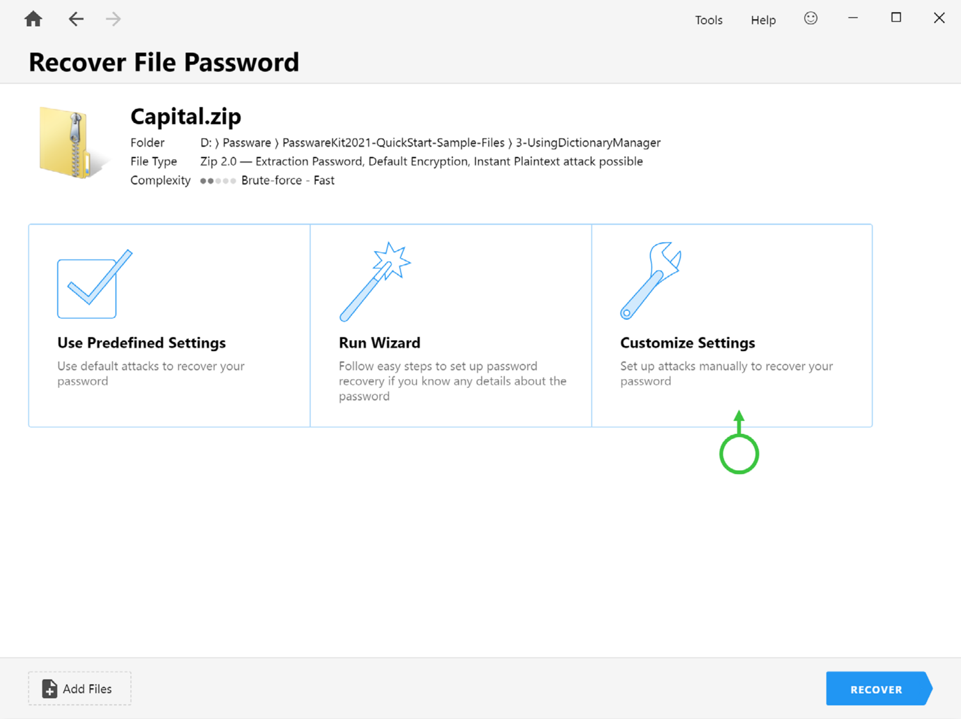
Standalone System
Extract passwords for standalone system from external registry files

Password Managers
Recover master passwords for KeePass, 1Password, LastPass, etc.

Quick Start Guide
Learn how to use the new version of Passware Kit

5. Locate the file **Capital.zip** from the **3-UsingDictionaryManager** folder and click **Open**.

6. Click **Customize Settings**:



Recover File Password

Capital.zip

Folder D: ⟩ Passware ⟩ PasswareKit2021-QuickStart-Sample-Files ⟩ 3-UsingDictionaryManager

File Type Zip 2.0 — Extraction Password, Default Encryption, Instant Plaintext attack possible

Complexity ●●○○○ Brute-force - Fast

Use Predefined Settings
Use default attacks to recover your password

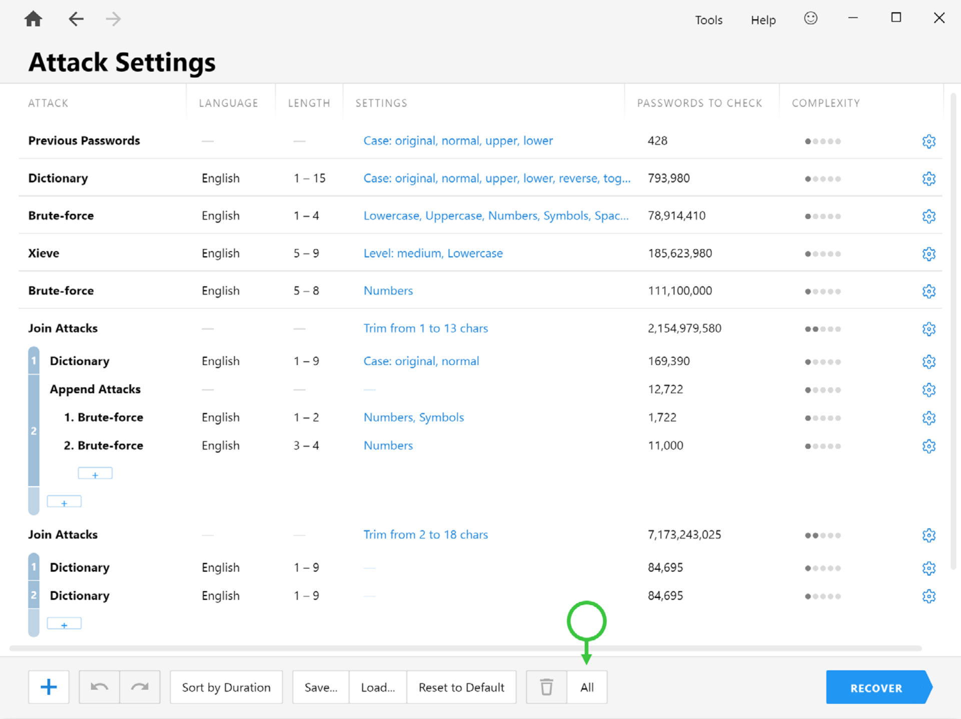
Run Wizard
Follow easy steps to set up password recovery if you know any details about the password

Customize Settings
Set up attacks manually to recover your password

Add Files

RECOVER

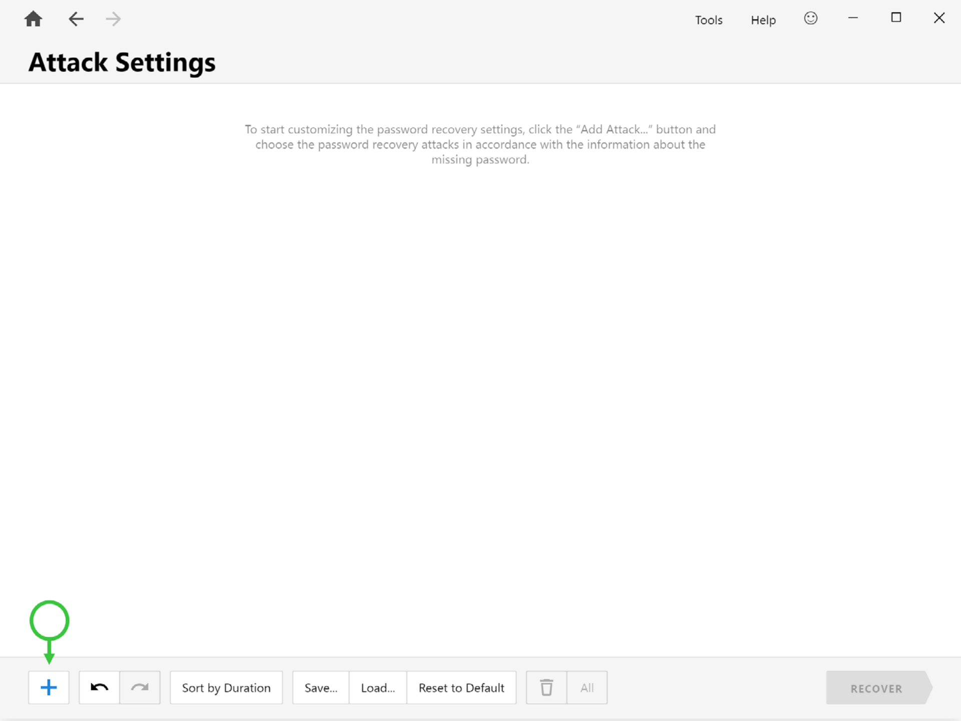
7. Passware Kit displays the settings of the default password recovery attacks. Click **All** to clear the list and start with your own settings:



Attack Settings

ATTACK	LANGUAGE	LENGTH	SETTINGS	PASSWORDS TO CHECK	COMPLEXITY
Previous Passwords	—	—	Case: original, normal, upper, lower	428	●○○○○
Dictionary	English	1 – 15	Case: original, normal, upper, lower, reverse, tog...	793,980	●○○○○
Brute-force	English	1 – 4	Lowercase, Uppercase, Numbers, Symbols, Spac...	78,914,410	●○○○○
Xieve	English	5 – 9	Level: medium, Lowercase	185,623,980	●○○○○
Brute-force	English	5 – 8	Numbers	111,100,000	●○○○○
Join Attacks	—	—	Trim from 1 to 13 chars	2,154,979,580	●●○○○
1 **Dictionary**	English	1 – 9	Case: original, normal	169,390	●○○○○
2 **Append Attacks**	—	—	—	12,722	●○○○○
1. Brute-force	English	1 – 2	Numbers, Symbols	1,722	●○○○○
2. Brute-force	English	3 – 4	Numbers	11,000	●○○○○
Join Attacks	—	—	Trim from 2 to 18 chars	7,173,243,025	●●○○○
1 **Dictionary**	English	1 – 9	—	84,695	●○○○○
2 **Dictionary**	English	1 – 9	—	84,695	●○○○○

8. Click **+**:

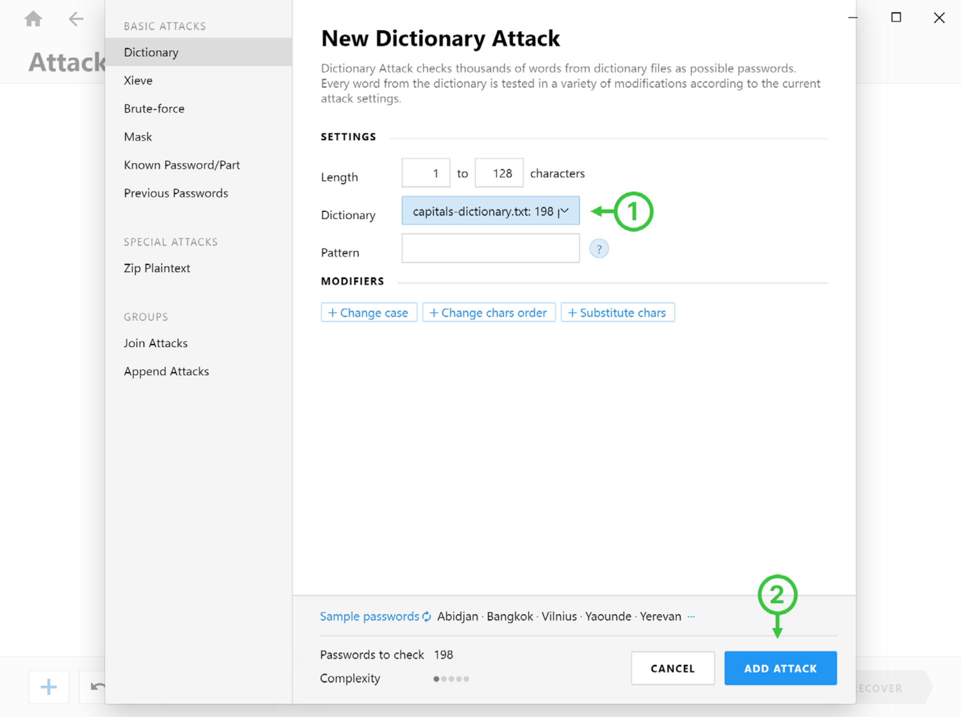


Attack Settings

To start customizing the password recovery settings, click the "Add Attack..." button and choose the password recovery attacks in accordance with the information about the missing password.

9. In the **New Dictionary Attack** settings, choose **capitals-dictionary.txt** from the **Dictionary** pull-down menu:

Click **Add Attack**.



New Dictionary Attack

Dictionary Attack checks thousands of words from dictionary files as possible passwords. Every word from the dictionary is tested in a variety of modifications according to the current attack settings.

SETTINGS

Length 1 to 128 characters

Dictionary capitals-dictionary.txt: 198

Pattern

MODIFIERS

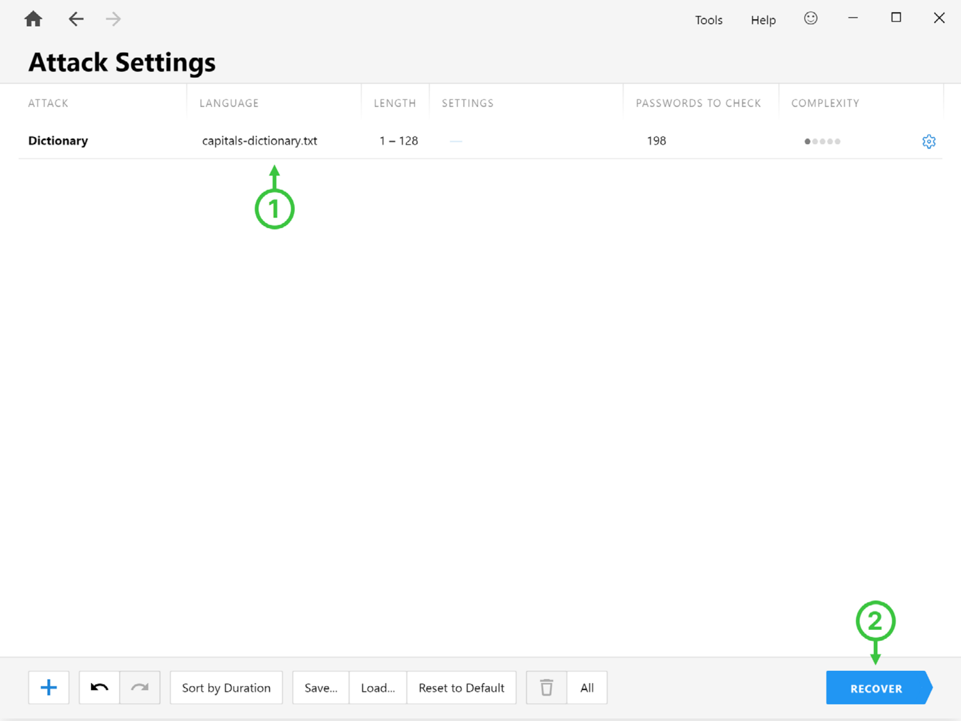
+ Change case + Change chars order + Substitute chars

Sample passwords Abidjan · Bangkok · Vilnius · Yaounde · Yerevan ···

Passwords to check 198

Complexity ●●●●●

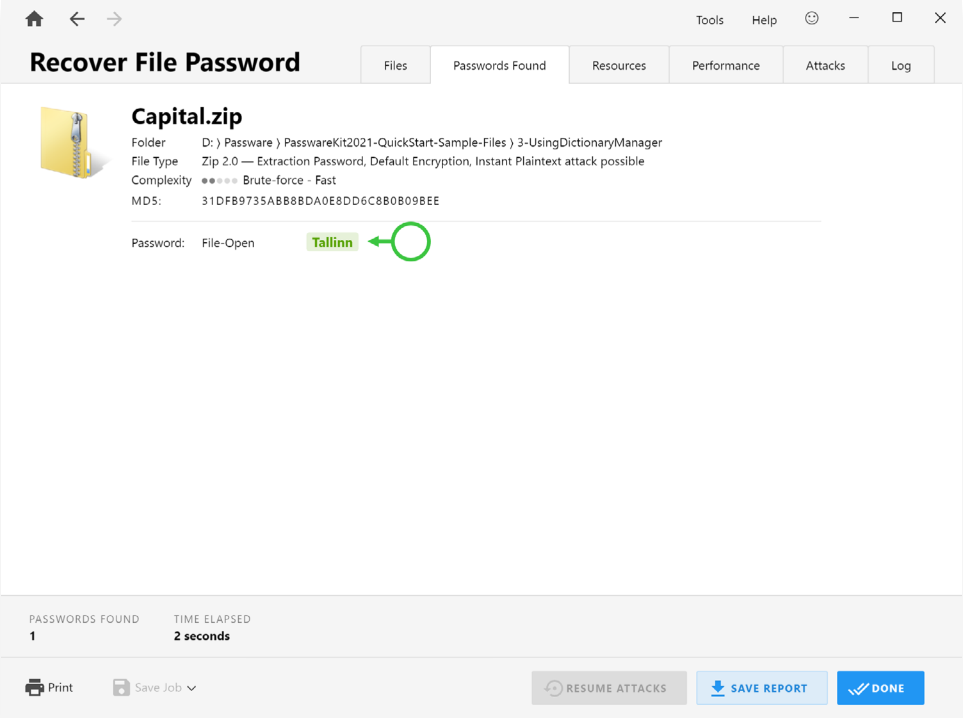
10. Click **Recover** to proceed with the custom settings:



Attack Settings

ATTACK	LANGUAGE	LENGTH	SETTINGS	PASSWORDS TO CHECK	COMPLEXITY
Dictionary	capitals-dictionary.txt	1 – 128	—	198	●●●●●

11. Passware Kit recovers the password for the file using the custom dictionary:



Capital.zip

Folder D:) Passware) PasswareKit2021-QuickStart-Sample-Files) 3-UsingDictionaryManager

File Type Zip 2.0 — Extraction Password, Default Encryption, Instant Plaintext attack possible

Complexity ●●○○○ Brute-force - Fast

MD5: 31DFB9735ABB8BDA0E8DD6C8B0B09BEE

Password: File-Open Tallinn

PASSWORDS FOUND 1

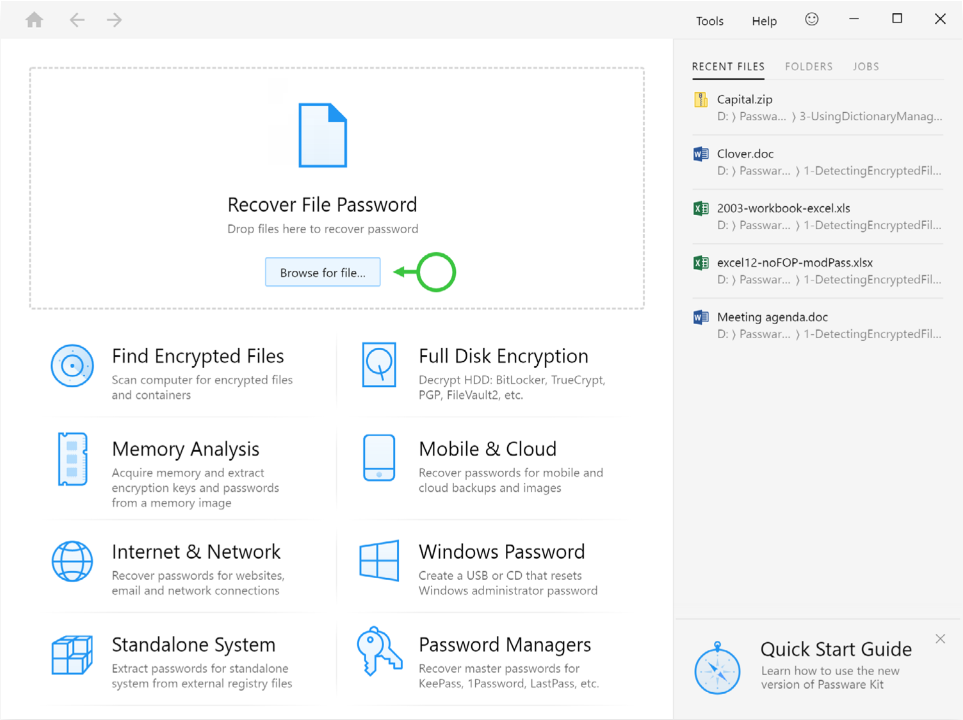
TIME ELAPSED 2 seconds

Task 4

Customizing password recovery settings

If a pattern for a password is known, it can be specified in Passware Kit settings. For example, the password for the file **placesihavebeen.zip** is a city name followed by a year, i.e. “London2015”, “Amsterdam2000”, etc. To recover this type of password, use a custom dictionary file from Task 3.

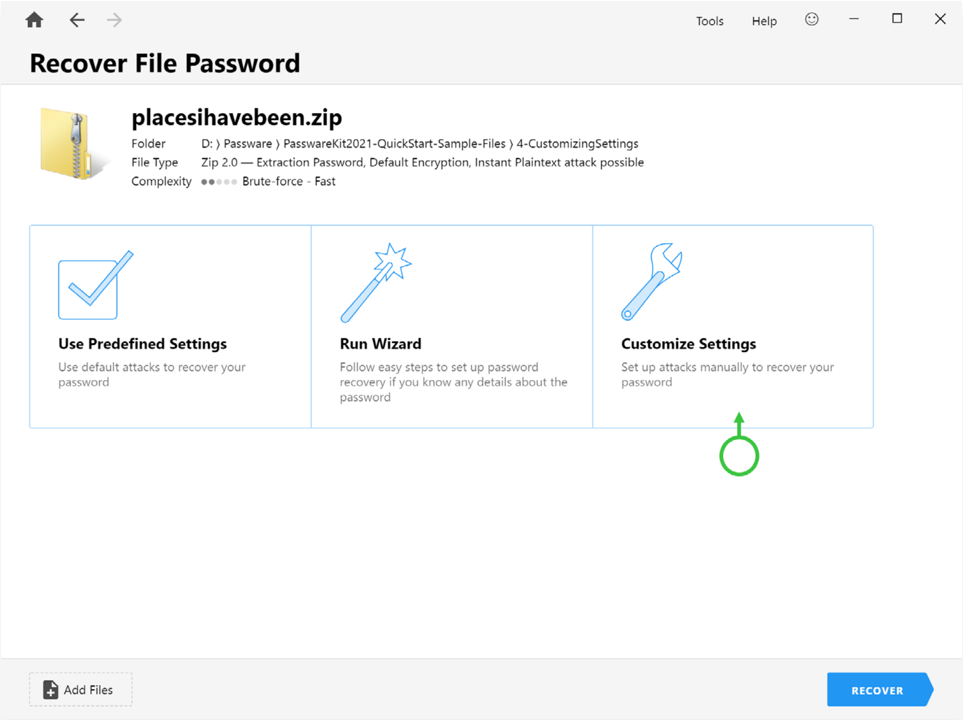
1. On the Start page, click **Recover File Password**:



Tools
Help
RECENT FILES
FOLDERS
JOBS
Capital.zip
D: ⟩ Passwa... ⟩ 3-UsingDictionaryManag...
Clover.doc
D: ⟩ Passwar... ⟩ 1-DetectingEncryptedFil...
2003-workbook-excel.xls
D: ⟩ Passwar... ⟩ 1-DetectingEncryptedFil...
excel12-noFOP-modPass.xlsx
D: ⟩ Passwar... ⟩ 1-DetectingEncryptedFil...
Meeting agenda.doc
D: ⟩ Passwar... ⟩ 1-DetectingEncryptedFil...
Recover File Password
Drop files here to recover password
Browse for file...
Find Encrypted Files
Scan computer for encrypted files and containers
Full Disk Encryption
Decrypt HDD: BitLocker, TrueCrypt, PGP, FileVault2, etc.
Memory Analysis
Acquire memory and extract encryption keys and passwords from a memory image
Mobile & Cloud
Recover passwords for mobile and cloud backups and images
Internet & Network
Recover passwords for websites, email and network connections
Windows Password
Create a USB or CD that resets Windows administrator password
Standalone System
Extract passwords for standalone system from external registry files
Password Managers
Recover master passwords for KeePass, 1Password, LastPass, etc.
Quick Start Guide
Learn how to use the new version of Passware Kit

2. Select the **placesihavebeen.zip** file from the **4-CustomizingSettings** folder and click Open.

Click **Customize Settings**:



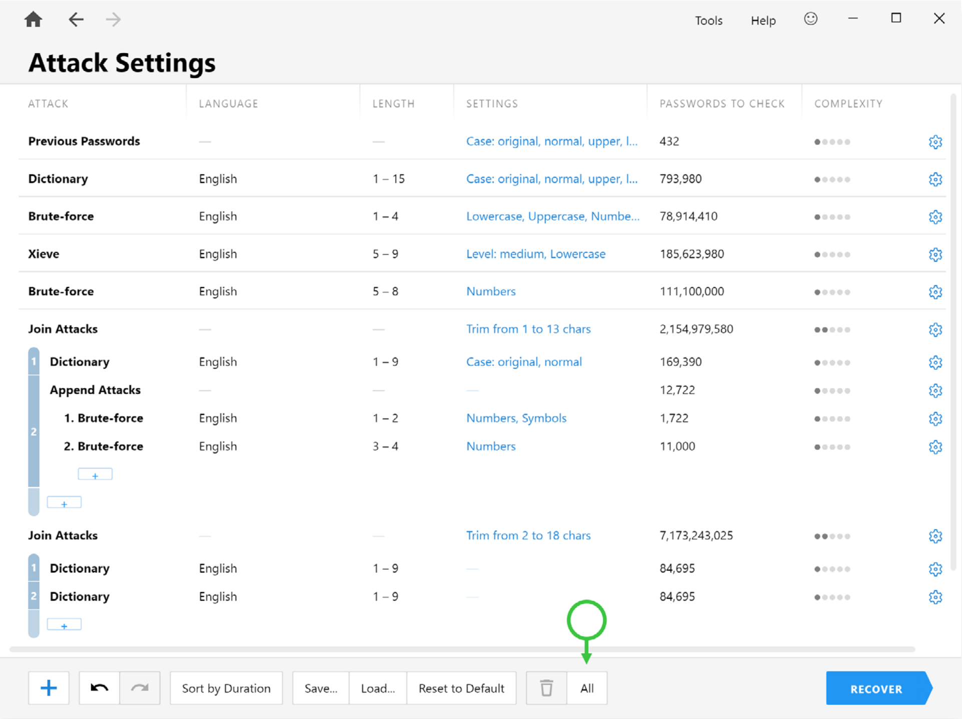
Recover File Password

placesihavebeen.zip

Folder	D: ⟩ Passware ⟩ PasswareKit2021-QuickStart-Sample-Files ⟩ 4-CustomizingSettings
File Type	Zip 2.0 — Extraction Password, Default Encryption, Instant Plaintext attack possible
Complexity	●●●●● Brute-force - Fast

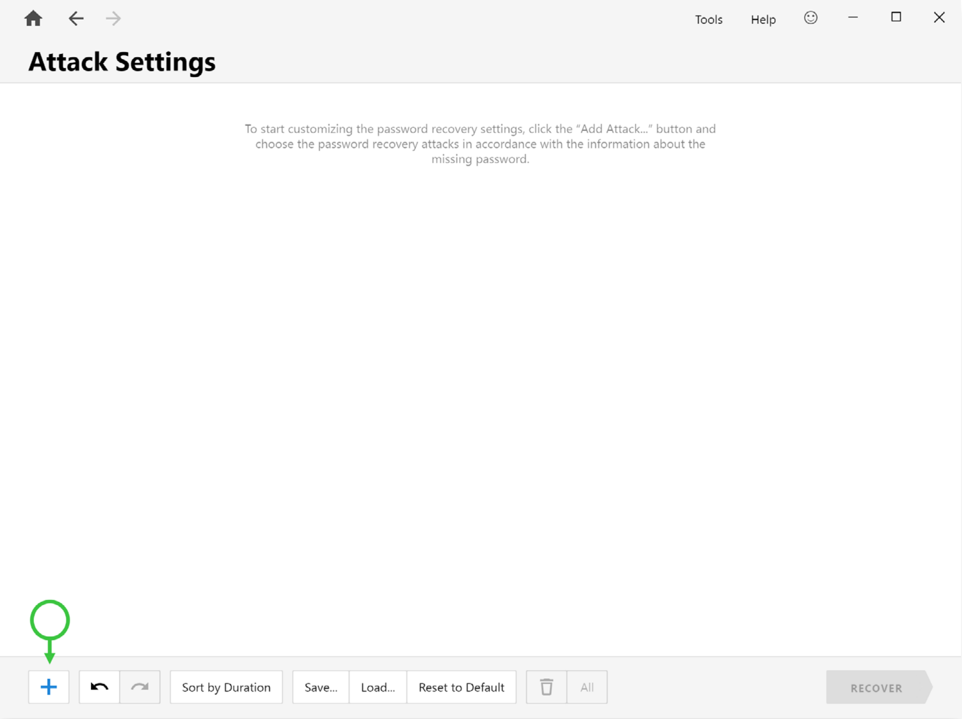
Tools
Help
Use Predefined Settings
Use default attacks to recover your password
Run Wizard
Follow easy steps to set up password recovery if you know any details about the password
Customize Settings
Set up attacks manually to recover your password
Add Files
RECOVER

3. Passware Kit displays the settings of the default password recovery attacks. Click **All** to clear the list and start with your own settings:



ATTACK	LANGUAGE	LENGTH	SETTINGS	PASSWORDS TO CHECK	COMPLEXITY
Previous Passwords	—	—	Case: original, normal, upper, l...	432	●○○○○
Dictionary	English	1 – 15	Case: original, normal, upper, l...	793,980	●○○○○
Brute-force	English	1 – 4	Lowercase, Uppercase, Numbe...	78,914,410	●○○○○
Xieve	English	5 – 9	Level: medium, Lowercase	185,623,980	●○○○○
Brute-force	English	5 – 8	Numbers	111,100,000	●○○○○
Join Attacks	—	—	Trim from 1 to 13 chars	2,154,979,580	●●○○○
Dictionary	English	1 – 9	Case: original, normal	169,390	●○○○○
Append Attacks	—	—	—	12,722	●○○○○
1. Brute-force	English	1 – 2	Numbers, Symbols	1,722	●○○○○
2. Brute-force	English	3 – 4	Numbers	11,000	●○○○○
Join Attacks	—	—	Trim from 2 to 18 chars	7,173,243,025	●●○○○
Dictionary	English	1 – 9	—	84,695	●○○○○
Dictionary	English	1 – 9	—	84,695	●○○○○

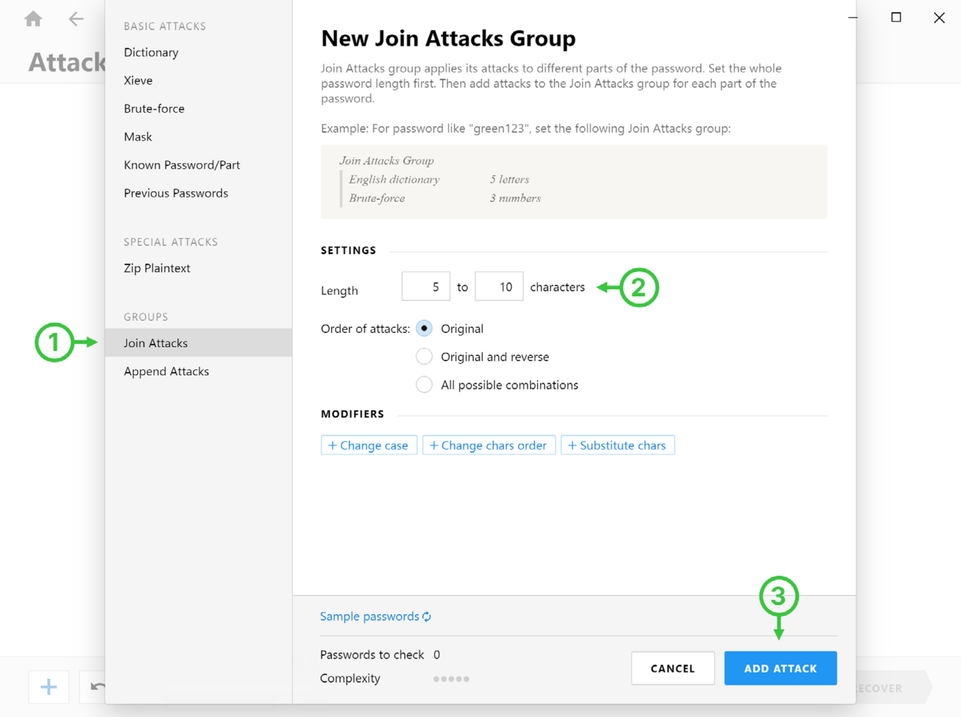
4. Click **+**:



To start customizing the password recovery settings, click the "Add Attack..." button and choose the password recovery attacks in accordance with the information about the missing password.

5. To specify the pattern **city + year**, click **Join Attacks**. You will need to join a **Dictionary** (city names) attack and a **Brute-force** attack (numbers) together. Specify the overall range of password **Length**, if known. In this example, the length is from 5 to 10 characters.

Click **Add Attack**:



New Join Attacks Group

Join Attacks group applies its attacks to different parts of the password. Set the whole password length first. Then add attacks to the Join Attacks group for each part of the password.

Example: For password like "green123", set the following Join Attacks group:

Join Attacks Group
English dictionary *5 letters*
Brute-force *3 numbers*

SETTINGS

Length 5 to 10 characters

Order of attacks: ● Original ○ Original and reverse ○ All possible combinations

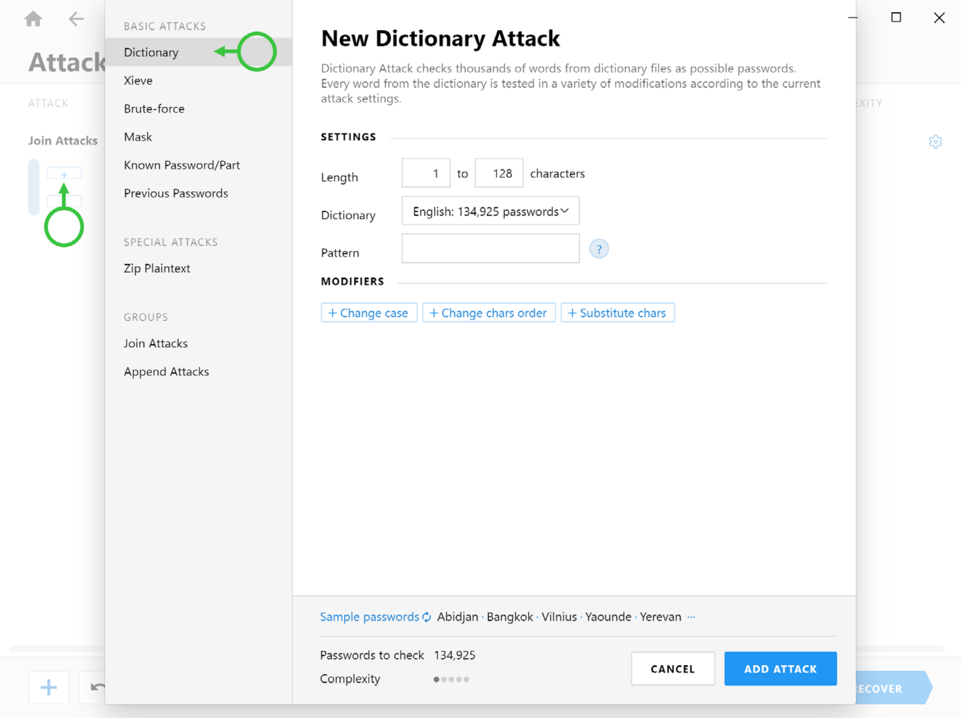
MODIFIERS

Sample passwords

Passwords to check 0

Complexity

6. Click **+** and choose a **Dictionary** attack:



New Dictionary Attack

Dictionary Attack checks thousands of words from dictionary files as possible passwords. Every word from the dictionary is tested in a variety of modifications according to the current attack settings.

SETTINGS

Length 1 to 128 characters

Dictionary English: 134,925 passwords

Pattern

MODIFIERS

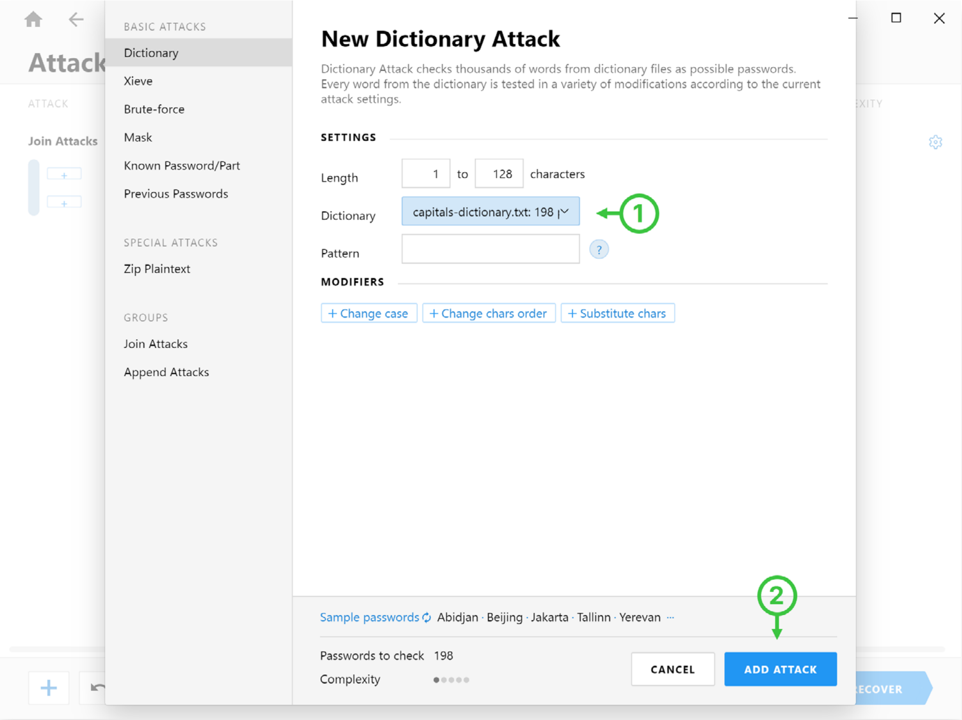
Sample passwords Abidjan · Bangkok · Vilnius · Yaounde · Yerevan ···

Passwords to check 134,925

Complexity

7. From the **Dictionary** pull-down menu, choose **capitals-dictionary.txt**, which was previously compiled in Task 3.

Click **Add Attack**:



New Dictionary Attack

Dictionary Attack checks thousands of words from dictionary files as possible passwords. Every word from the dictionary is tested in a variety of modifications according to the current attack settings.

SETTINGS

Length 1 to 128 characters

Dictionary capitals-dictionary.txt: 198

Pattern

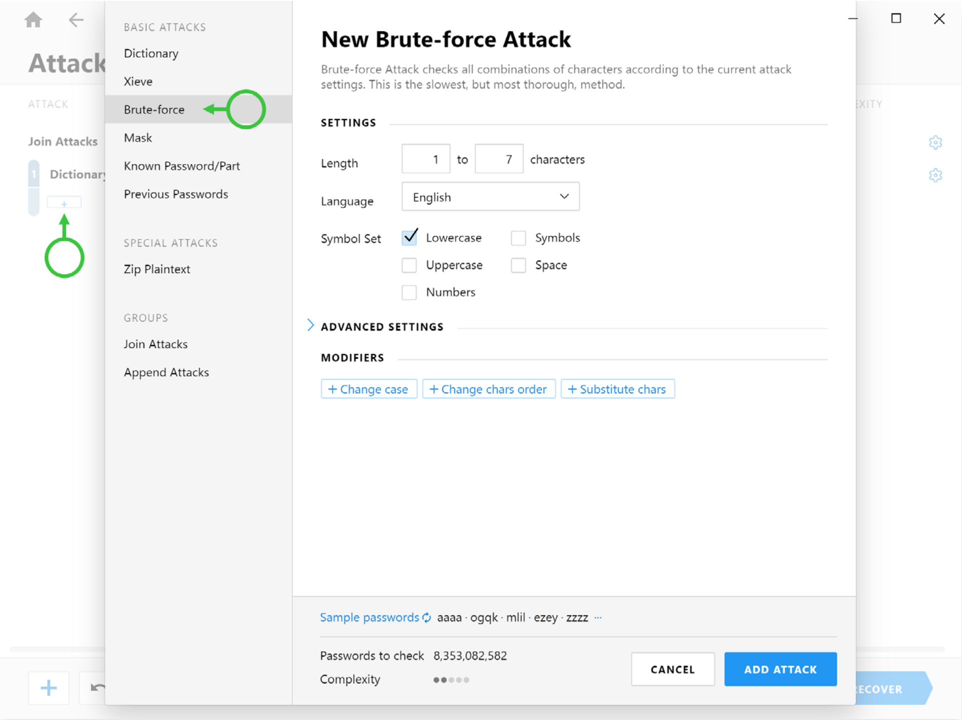
MODIFIERS

Sample passwords Abidjan · Beijing · Jakarta · Tallinn · Yerevan ···

Passwords to check 198

Complexity ●○○○○

8. Click **+** and choose a **Brute-force** attack:



New Brute-force Attack

Brute-force Attack checks all combinations of characters according to the current attack settings. This is the slowest, but most thorough, method.

SETTINGS

Length 1 to 7 characters

Language English

Symbol Set ☑ Lowercase ☐ Symbols ☐ Uppercase ☐ Space ☐ Numbers

MODIFIERS

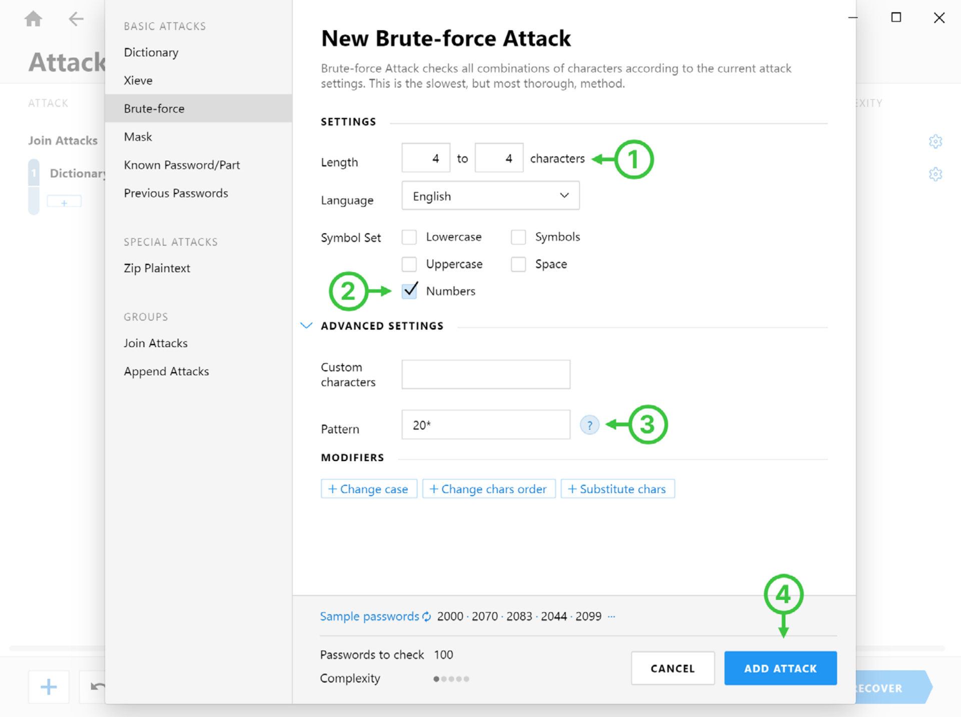
Sample passwords aaaa · ogqk · mlil · ezey · zzzz ···

Passwords to check 8,353,082,582

Complexity ●●○○○

9. In the **Brute-force** Attack settings, specify the length of the password part: For a year number, **Length** should be set from 4 to 4 characters. Specify the **Symbol Set**: enable the checkbox **Numbers** and disable all other checkboxes. In the **Advanced Settings** section, specify the **Pattern** of the password part: If it is a year of the current century, set the pattern to 20* (the password part will look like 2000, 2001, …, 2099).

Click **Add Attack**:



New Brute-force Attack

Brute-force Attack checks all combinations of characters according to the current attack settings. This is the slowest, but most thorough, method.

SETTINGS

Length 4 to 4 characters

Language English

Symbol Set □ Lowercase □ Symbols □ Uppercase □ Space ☑ Numbers

ADVANCED SETTINGS

Custom characters

Pattern 20*

MODIFIERS

+ Change case + Change chars order + Substitute chars

Sample passwords 2000 · 2070 · 2083 · 2044 · 2099 ···

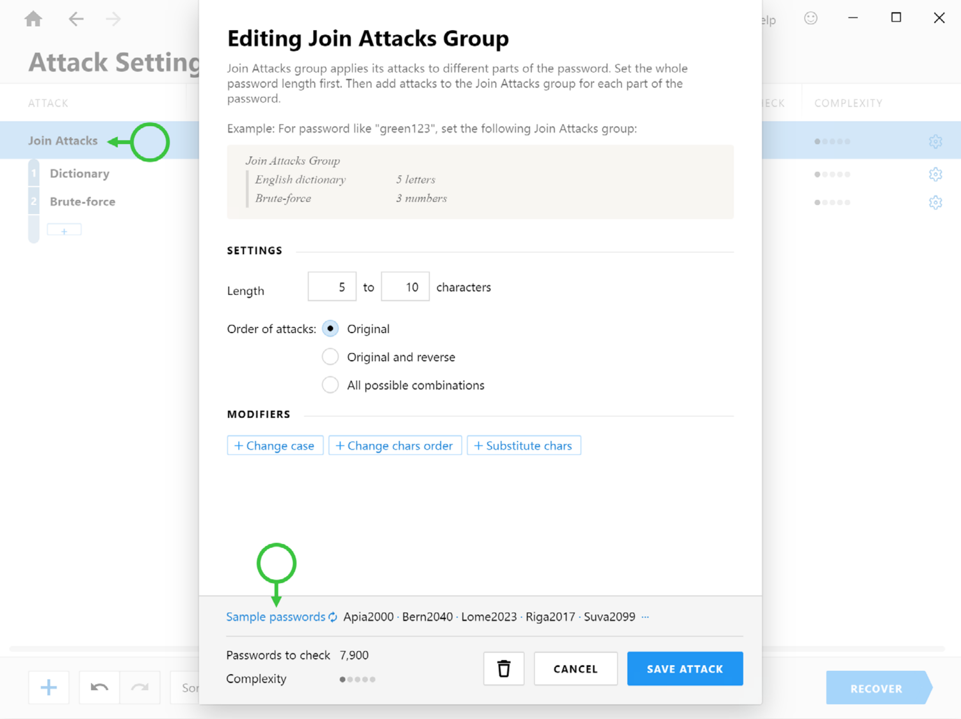
Passwords to check 100

Complexity ●○○○○

CANCEL ADD ATTACK

10. In the **Join Attacks** settings, click the **Sample passwords** link to see the passwords that are generated by the attack (a city name followed by a year):

Click **Save Attack**.



Editing Join Attacks Group

Join Attacks group applies its attacks to different parts of the password. Set the whole password length first. Then add attacks to the Join Attacks group for each part of the password.

Example: For password like "green123", set the following Join Attacks group:

Join Attacks Group
English dictionary *5 letters*
Brute-force *3 numbers*

SETTINGS

Length 5 to 10 characters

Order of attacks: ● Original ○ Original and reverse ○ All possible combinations

MODIFIERS

+ Change case + Change chars order + Substitute chars

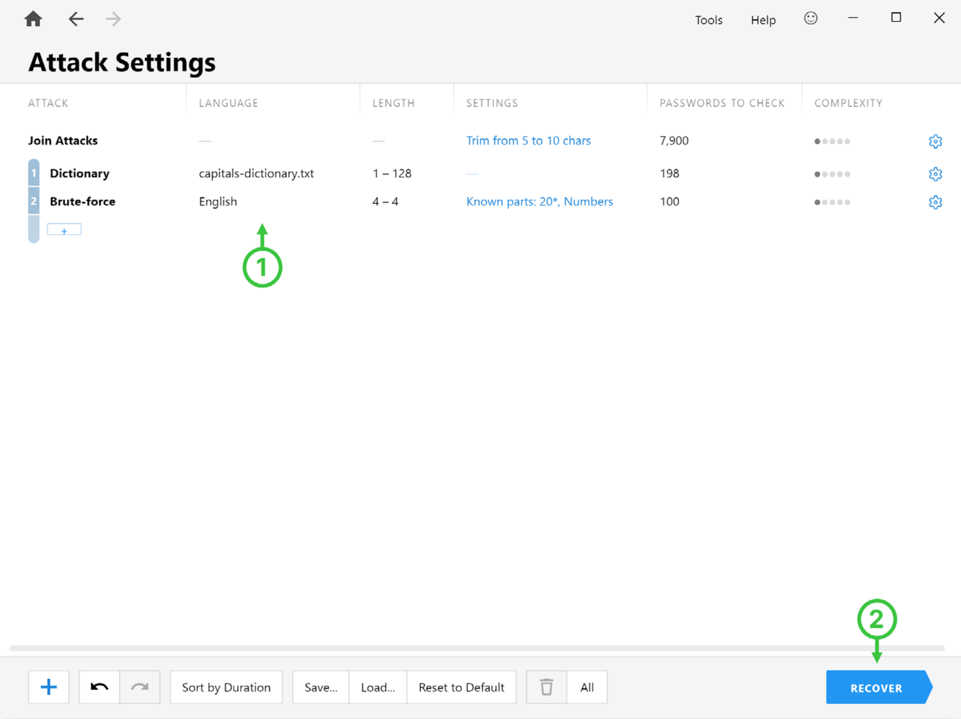
Sample passwords Apia2000 · Bern2040 · Lome2023 · Riga2017 · Suva2099 ···

Passwords to check 7,900

Complexity ●○○○○

CANCEL SAVE ATTACK

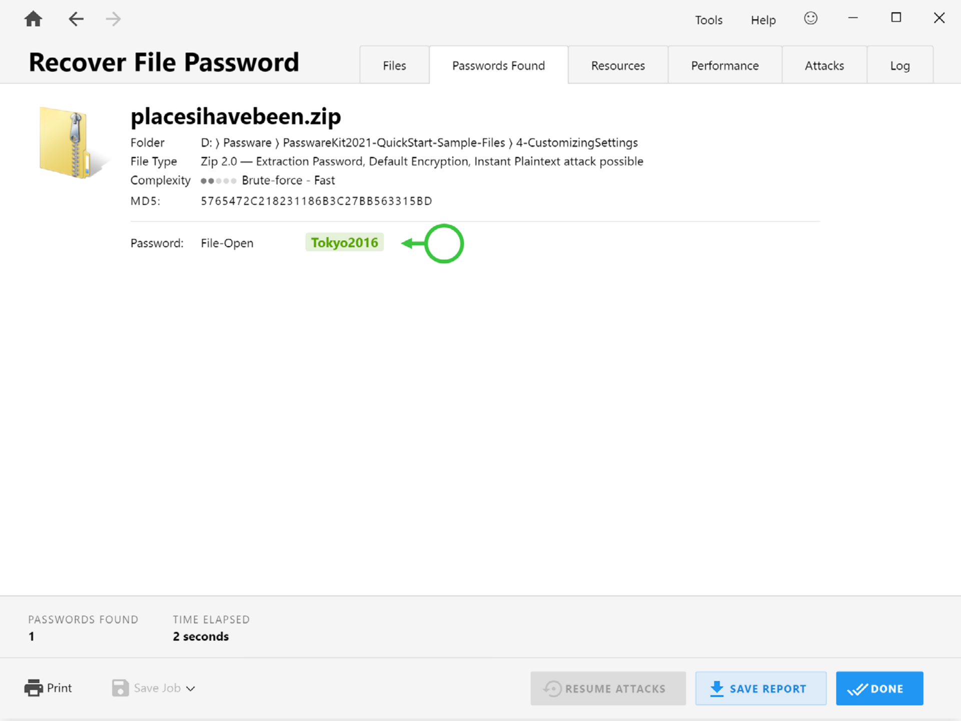
11. Click **Recover** to proceed with the custom settings:



Attack Settings

ATTACK	LANGUAGE	LENGTH	SETTINGS	PASSWORDS TO CHECK	COMPLEXITY
Join Attacks	—	—	Trim from 5 to 10 chars	7,900	●●●●●
1 Dictionary	capitals-dictionary.txt	1 – 128	—	198	●●●●●
2 Brute-force	English	4 – 4	Known parts: 20*, Numbers	100	●●●●●

12. Passware Kit recovers the password for the file using the custom settings:



Recover File Password

placesihavebeen.zip

Folder D:) Passware) PasswareKit2021-QuickStart-Sample-Files) 4-CustomizingSettings

File Type Zip 2.0 — Extraction Password, Default Encryption, Instant Plaintext attack possible

Complexity ●●●●● Brute-force - Fast

MD5: 5765472C218231186B3C27BB563315BD

Password: File-Open Tokyo2016

PASSWORDS FOUND 1

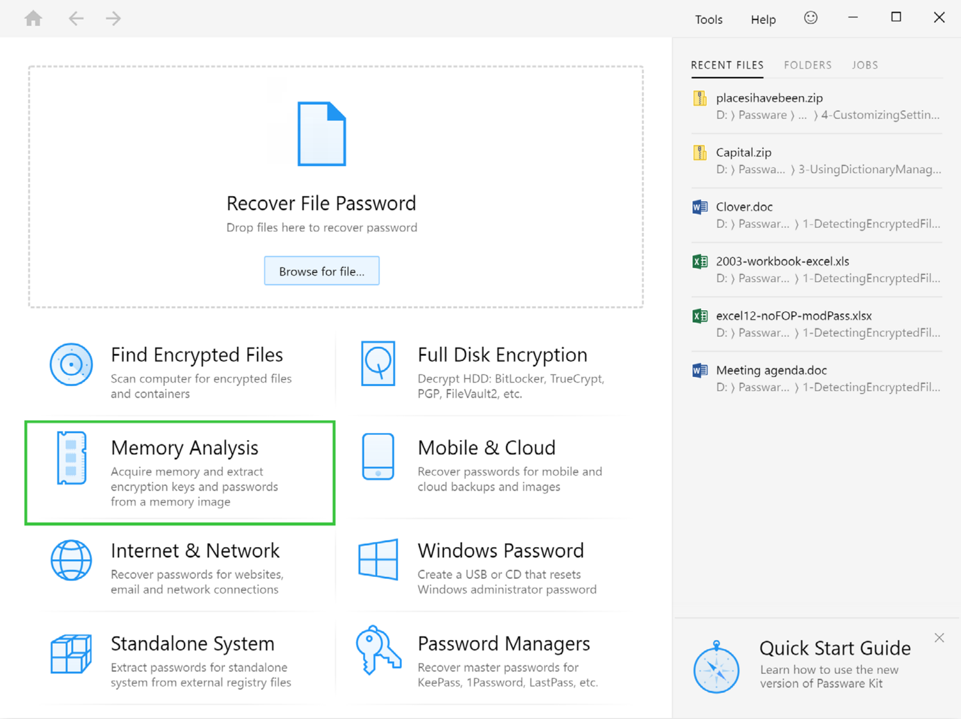
TIME ELAPSED 2 seconds

Passware Tip: *Follow the link for more information about Passware Kit password recovery settings to configure password candidates.*

Task 5

Extracting passwords from a memory image

1. On the Start page, click **Memory Analysis**:



Recover File Password

Drop files here to recover password

Browse for file...

Find Encrypted Files – Scan computer for encrypted files and containers

Full Disk Encryption – Decrypt HDD: BitLocker, TrueCrypt, PGP, FileVault2, etc.

Memory Analysis – Acquire memory and extract encryption keys and passwords from a memory image

Mobile & Cloud – Recover passwords for mobile and cloud backups and images

Internet & Network – Recover passwords for websites, email and network connections

Windows Password – Create a USB or CD that resets Windows administrator password

Standalone System – Extract passwords for standalone system from external registry files

Password Managers – Recover master passwords for KeePass, 1Password, LastPass, etc.

RECENT FILES FOLDERS JOBS

placesihavebeen.zip – D:) Passware) ...) 4-CustomizingSettin...

Capital.zip – D:) Passwa...) 3-UsingDictionaryManag...

Clover.doc – D:) Passwar...) 1-DetectingEncryptedFil...

2003-workbook-excel.xls – D:) Passwar...) 1-DetectingEncryptedFil...

excel12-noFOP-modPass.xlsx – D:) Passwar...) 1-DetectingEncryptedFil...

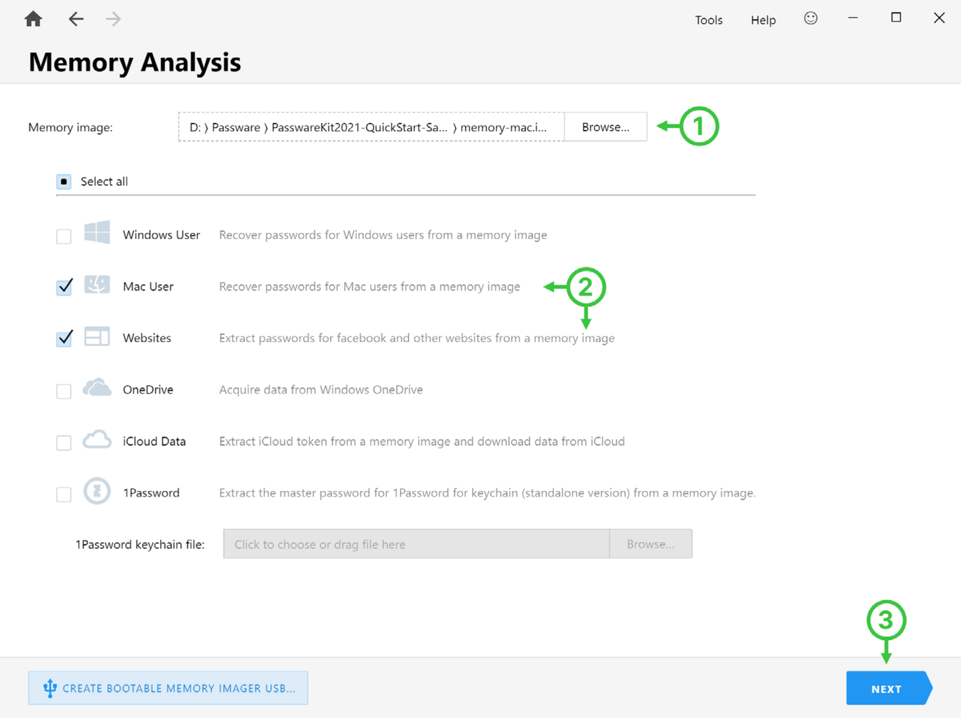
Meeting agenda.doc – D:) Passwar...) 1-DetectingEncryptedFil...

Quick Start Guide – Learn how to use the new version of Passware Kit

2. Click **Browse...** and locate the **memory-mac.img** file from the **5-ExtractingPasswordsFrom-MemoryImage** folder. Click **Open**.

3. Enable checkboxes **Mac User** and **Websites**.

Click **Next**:



Memory Analysis

Memory image: D:) Passware) PasswareKit2021-QuickStart-Sa...) memory-mac.i... Browse...

■ Select all

☐ Windows User – Recover passwords for Windows users from a memory image

☑ Mac User – Recover passwords for Mac users from a memory image

☑ Websites – Extract passwords for facebook and other websites from a memory image

☐ OneDrive – Acquire data from Windows OneDrive

☐ iCloud Data – Extract iCloud token from a memory image and download data from iCloud

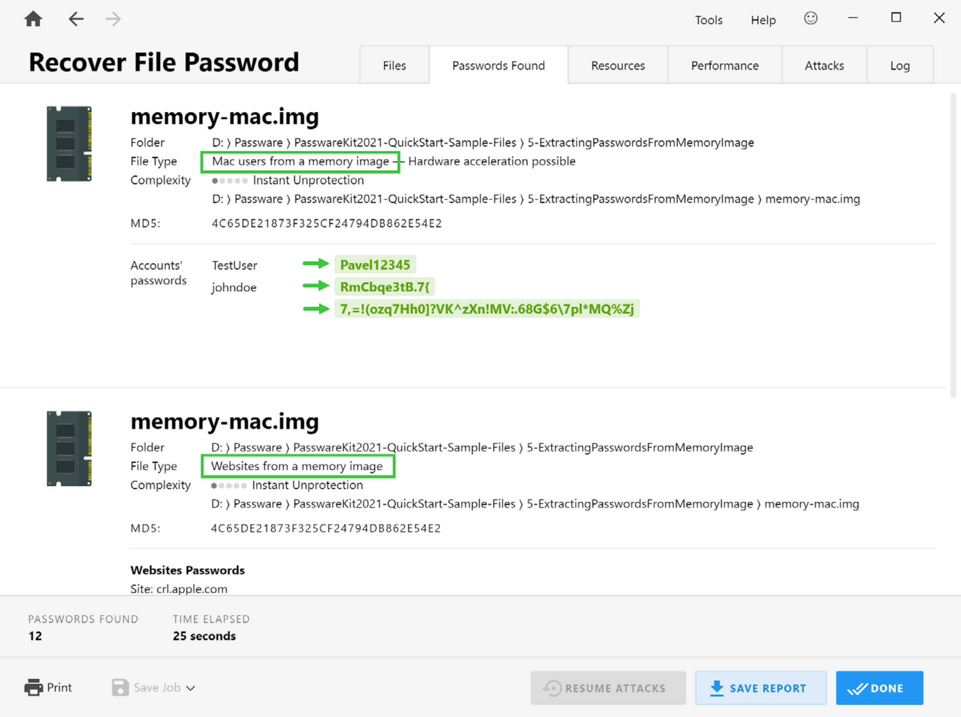
☐ 1Password – Extract the master password for 1Password for keychain (standalone version) from a memory image.

1Password keychain file: Click to choose or drag file here Browse...

CREATE BOOTABLE MEMORY IMAGER USB...

NEXT

4. Passware Kit extracts passwords for Mac users, as well as the list of open websites along with their login credentials:



Recover File Password

memory-mac.img

Folder D: ⟩ Passware ⟩ PasswareKit2021-QuickStart-Sample-Files ⟩ 5-ExtractingPasswordsFromMemoryImage
File Type Mac users from a memory image — Hardware acceleration possible
Complexity ●○○○○ Instant Unprotection
D: ⟩ Passware ⟩ PasswareKit2021-QuickStart-Sample-Files ⟩ 5-ExtractingPasswordsFromMemoryImage ⟩ memory-mac.img
MD5: 4C65DE21873F325CF24794DB862E54E2

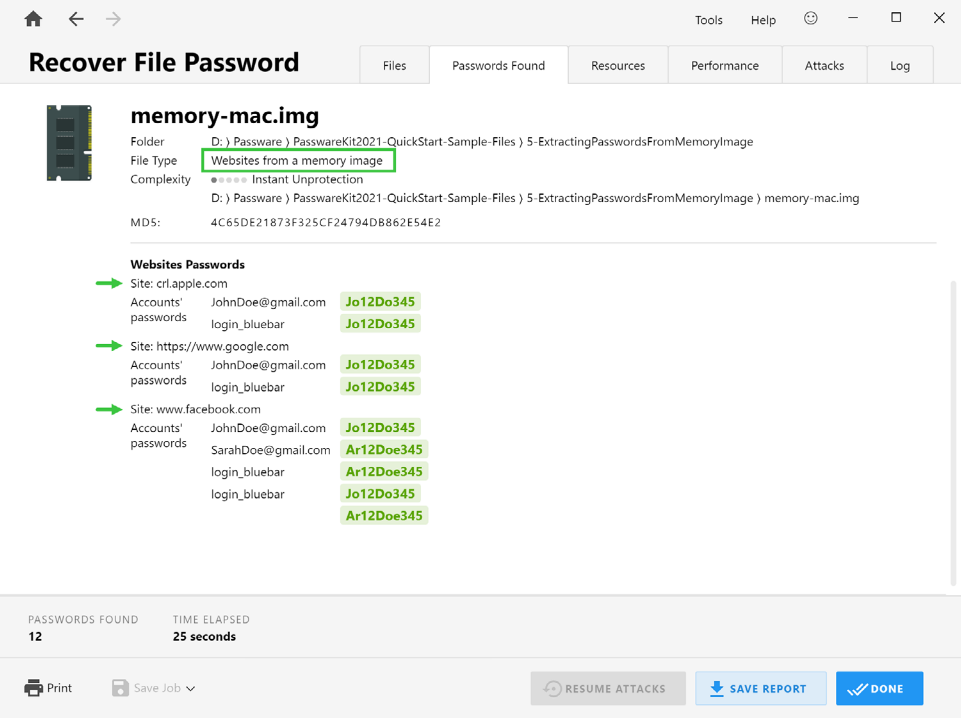
Accounts' passwords
TestUser → Pavel12345
johndoe → RmCbqe3tB.7{
→ 7,=!(ozq7Hh0]?VK^zXn!MV:.68G$6\7pl*MQ%Zj

memory-mac.img

Folder D: ⟩ Passware ⟩ PasswareKit2021-QuickStart-Sample-Files ⟩ 5-ExtractingPasswordsFromMemoryImage
File Type Websites from a memory image
Complexity ●○○○○ Instant Unprotection
D: ⟩ Passware ⟩ PasswareKit2021-QuickStart-Sample-Files ⟩ 5-ExtractingPasswordsFromMemoryImage ⟩ memory-mac.img
MD5: 4C65DE21873F325CF24794DB862E54E2

Websites Passwords
Site: crl.apple.com

PASSWORDS FOUND 12
TIME ELAPSED 25 seconds



Recover File Password

memory-mac.img

Folder D: ⟩ Passware ⟩ PasswareKit2021-QuickStart-Sample-Files ⟩ 5-ExtractingPasswordsFromMemoryImage
File Type Websites from a memory image
Complexity ●○○○○ Instant Unprotection
D: ⟩ Passware ⟩ PasswareKit2021-QuickStart-Sample-Files ⟩ 5-ExtractingPasswordsFromMemoryImage ⟩ memory-mac.img
MD5: 4C65DE21873F325CF24794DB862E54E2

Websites Passwords

→ Site: crl.apple.com
Accounts' passwords
JohnDoe@gmail.com Jo12Do345
login_bluebar Jo12Do345

→ Site: https://www.google.com
Accounts' passwords
JohnDoe@gmail.com Jo12Do345
login_bluebar Jo12Do345

→ Site: www.facebook.com
Accounts' passwords
JohnDoe@gmail.com Jo12Do345
SarahDoe@gmail.com Ar12Doe345
login_bluebar Ar12Doe345
login_bluebar Jo12Do345
Ar12Doe345

PASSWORDS FOUND 12
TIME ELAPSED 25 seconds

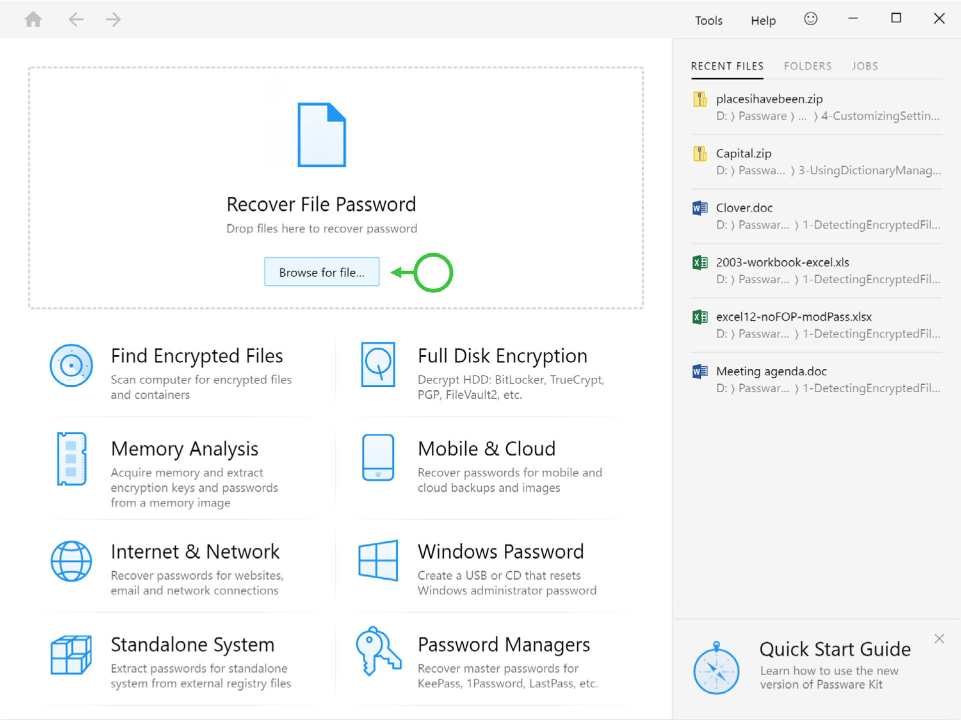
Passware Tip: *Check out 3 Steps to Acquire Memory and Bypass Encryption.*

Task 6

Decrypting a Keychain

By default, a Keychain password is the same as a Mac user password. Passware Kit leverages this feature to recover Keychain passwords with a **Previous Passwords** attack, which includes previously recovered passwords for Mac users (in Task 5). The previously recovered passwords are added automatically to the “Previous Passwords” dictionary to be reused for subsequent files.

1. On the Start page, click **Recover File Password**:



Recover File Password
Drop files here to recover password

Find Encrypted Files
Scan computer for encrypted files and containers

Full Disk Encryption
Decrypt HDD: BitLocker, TrueCrypt, PGP, FileVault2, etc.

Memory Analysis
Acquire memory and extract encryption keys and passwords from a memory image

Mobile & Cloud
Recover passwords for mobile and cloud backups and images

Internet & Network
Recover passwords for websites, email and network connections

Windows Password
Create a USB or CD that resets Windows administrator password

Standalone System
Extract passwords for standalone system from external registry files

Password Managers
Recover master passwords for KeePass, 1Password, LastPass, etc.

placesihavebeen.zip
D: 〉Passware 〉... 〉4-CustomizingSettin...

Capital.zip
D: 〉Passwa... 〉3-UsingDictionaryManag...

Clover.doc
D: 〉Passwar... 〉1-DetectingEncryptedFil...

2003-workbook-excel.xls
D: 〉Passwar... 〉1-DetectingEncryptedFil...

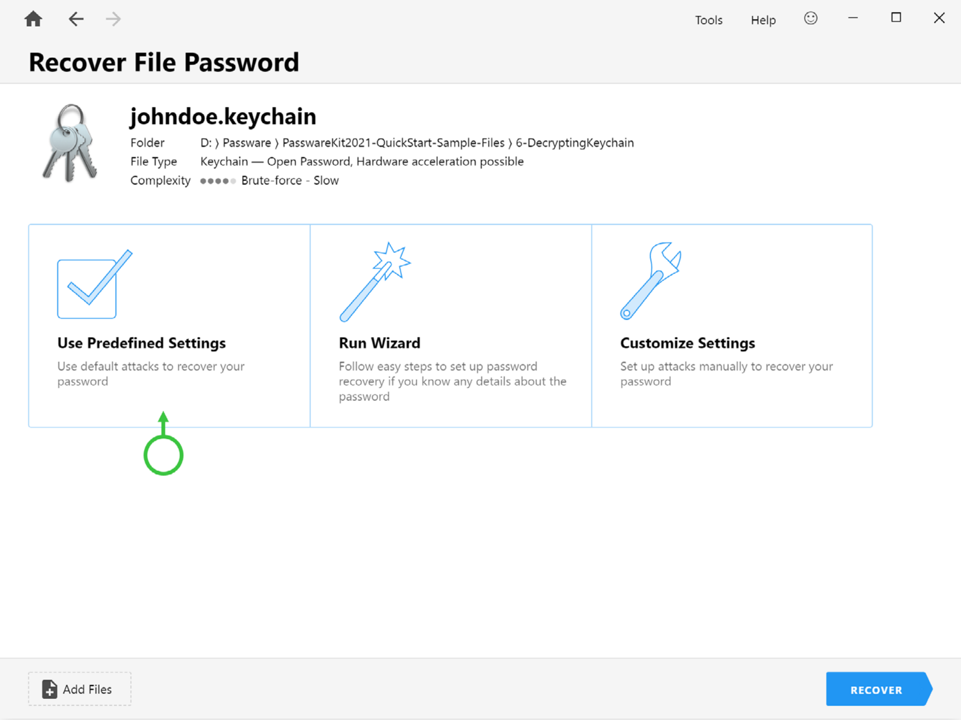
excel12-noFOP-modPass.xlsx
D: 〉Passwar... 〉1-DetectingEncryptedFil...

Meeting agenda.doc
D: 〉Passwar... 〉1-DetectingEncryptedFil...

Quick Start Guide
Learn how to use the new version of Passware Kit

2. Locate the **johndoe.keychain** file from the **6-DecryptingKeychain** folder and click **Open**.

3. Click **Use Predefined Settings**:



Recover File Password

johndoe.keychain

Folder D: ⟩ Passware ⟩ PasswareKit2021-QuickStart-Sample-Files ⟩ 6-DecryptingKeychain
File Type Keychain — Open Password, Hardware acceleration possible
Complexity ●●●●○ Brute-force - Slow

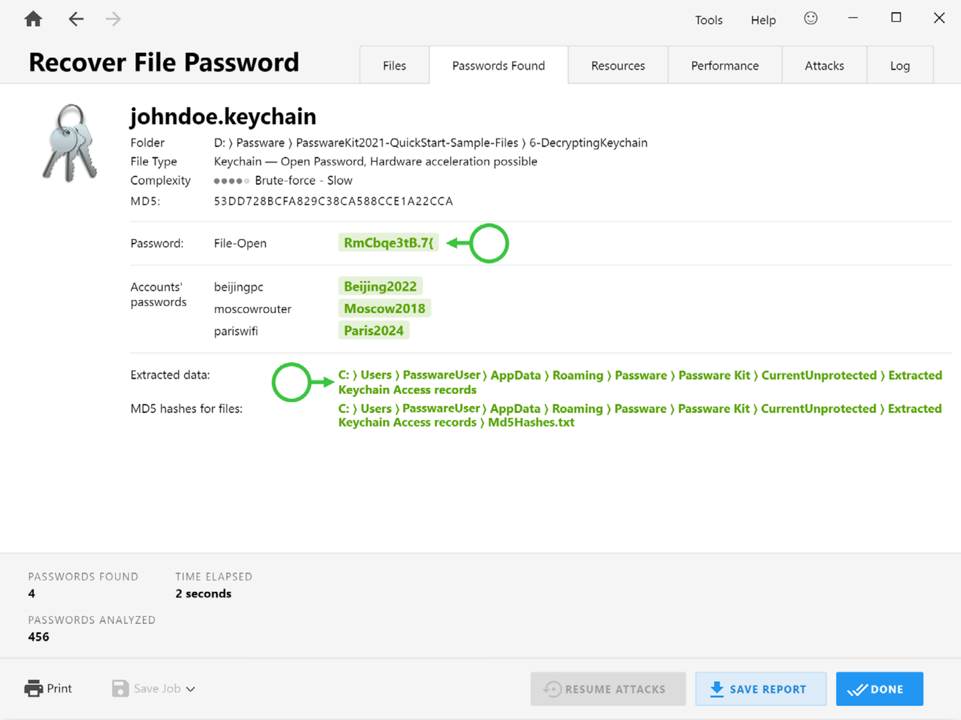
Use Predefined Settings
Use default attacks to recover your password

Run Wizard
Follow easy steps to set up password recovery if you know any details about the password

Customize Settings
Set up attacks manually to recover your password

Passware Tip: *The Login.keychain file is located at "~/<User>/Library/Keychains/" by default.*

4. Passware Kit runs default password recovery attacks, which include a **Previous Passwords** attack. The File-Open password is recovered in seconds and Passware Kit extracts all the login credentials and other data from the Keychain. It saves the records to a separate folder:



Recover File Password

johndoe.keychain

Folder D: ⟩ Passware ⟩ PasswareKit2021-QuickStart-Sample-Files ⟩ 6-DecryptingKeychain
File Type Keychain — Open Password, Hardware acceleration possible
Complexity ●●●●○ Brute-force - Slow
MD5: 53DD728BCFA829C38CA588CCE1A22CCA

Password: File-Open **RmCbqe3tB.7{**

Accounts' passwords
beijingpc **Beijing2022**
moscowrouter **Moscow2018**
pariswifi **Paris2024**

Extracted data: **C: ⟩ Users ⟩ PasswareUser ⟩ AppData ⟩ Roaming ⟩ Passware ⟩ Passware Kit ⟩ CurrentUnprotected ⟩ Extracted Keychain Access records**

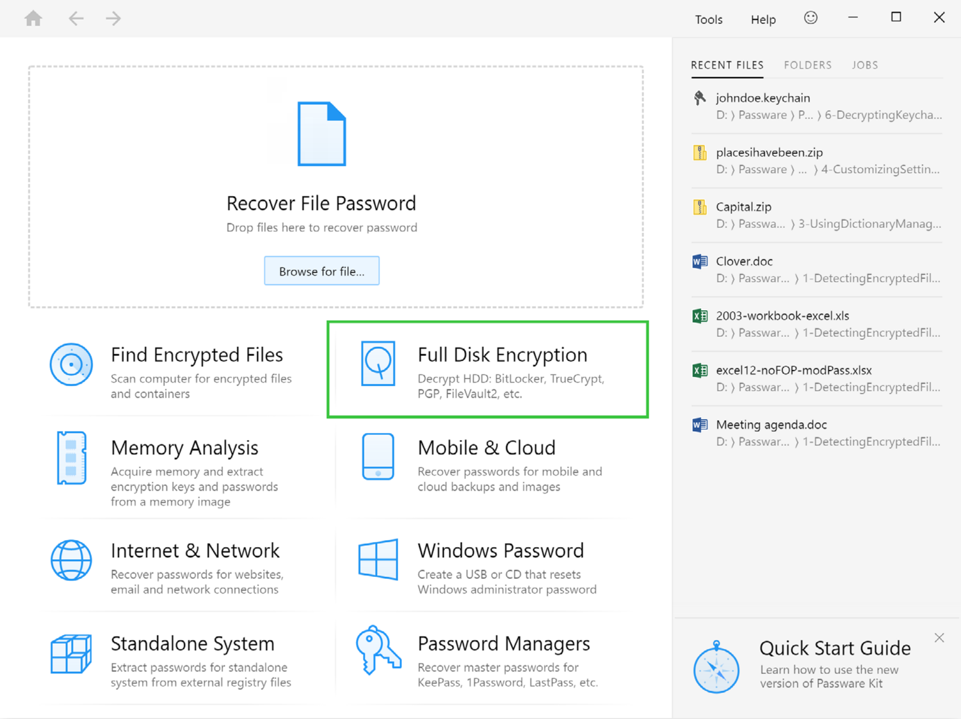
MD5 hashes for files: **C: ⟩ Users ⟩ PasswareUser ⟩ AppData ⟩ Roaming ⟩ Passware ⟩ Passware Kit ⟩ CurrentUnprotected ⟩ Extracted Keychain Access records ⟩ Md5Hashes.txt**

PASSWORDS FOUND 4
TIME ELAPSED 2 seconds
PASSWORDS ANALYZED 456

Task 7

Decrypting a VeraCrypt container

1. On the Start page, click **Full Disk Encryption**:



Recover File Password
Drop files here to recover password
Browse for file...

Find Encrypted Files
Scan computer for encrypted files and containers

Full Disk Encryption
Decrypt HDD: BitLocker, TrueCrypt, PGP, FileVault2, etc.

Memory Analysis
Acquire memory and extract encryption keys and passwords from a memory image

Mobile & Cloud
Recover passwords for mobile and cloud backups and images

Internet & Network
Recover passwords for websites, email and network connections

Windows Password
Create a USB or CD that resets Windows administrator password

Standalone System
Extract passwords for standalone system from external registry files

Password Managers
Recover master passwords for KeePass, 1Password, LastPass, etc.

RECENT FILES FOLDERS JOBS

johndoe.keychain
D:) Passware) P...) 6-DecryptingKeycha...

placesihavebeen.zip
D:) Passware) ...) 4-CustomizingSettin...

Capital.zip
D:) Passwa...) 3-UsingDictionaryManag...

Clover.doc
D:) Passwar...) 1-DetectingEncryptedFil...

2003-workbook-excel.xls
D:) Passwar...) 1-DetectingEncryptedFil...

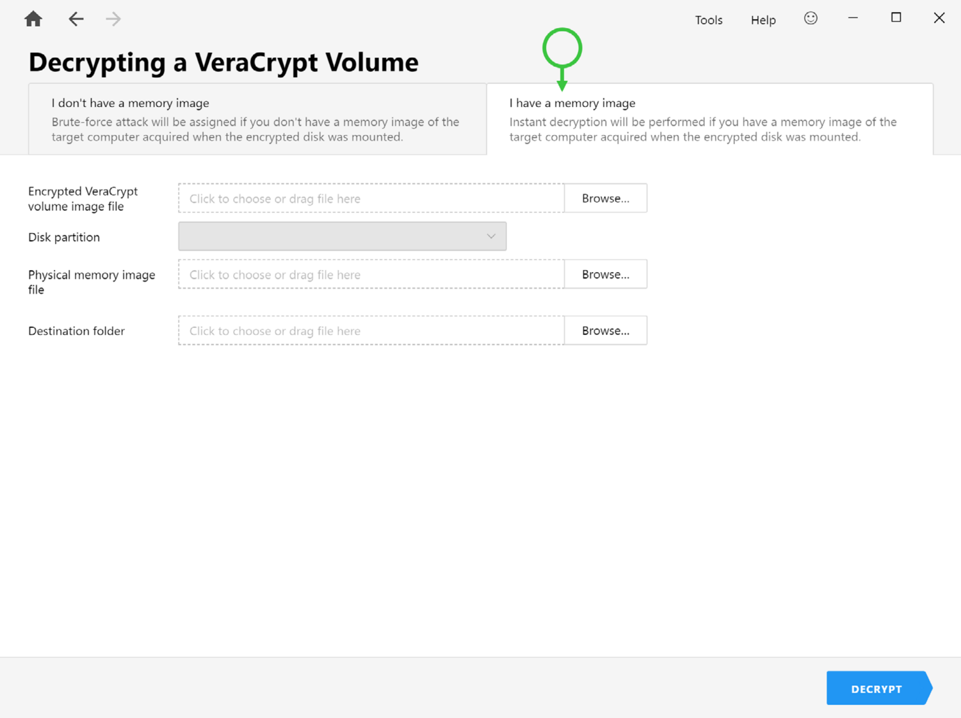
excel12-noFOP-modPass.xlsx
D:) Passwar...) 1-DetectingEncryptedFil...

Meeting agenda.doc
D:) Passwar...) 1-DetectingEncryptedFil...

Quick Start Guide
Learn how to use the new version of Passware Kit

2. Choose **VeraCrypt**.

3. Click the **I have a memory image** tab:



Decrypting a VeraCrypt Volume

I don't have a memory image
Brute-force attack will be assigned if you don't have a memory image of the target computer acquired when the encrypted disk was mounted.

I have a memory image
Instant decryption will be performed if you have a memory image of the target computer acquired when the encrypted disk was mounted.

Encrypted VeraCrypt volume image file: Click to choose or drag file here | Browse...

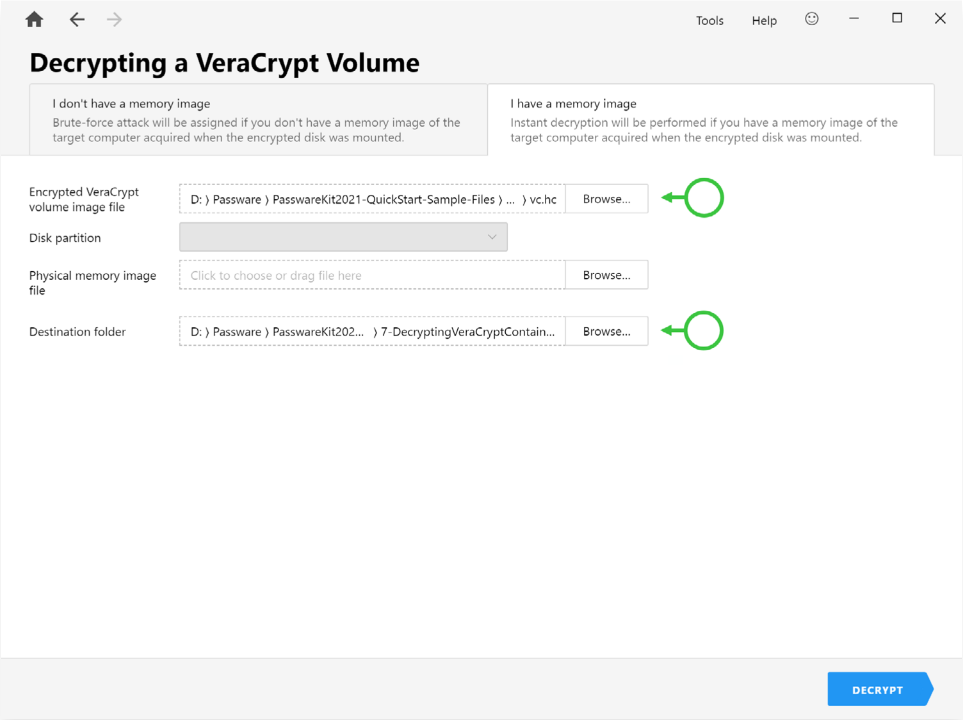
Disk partition

Physical memory image file: Click to choose or drag file here | Browse...

Destination folder: Click to choose or drag file here | Browse...

3. In the **Encrypted VeraCrypt volume image file** field, click **Browse**..., set **All files (*.*)** from the pull-down menu of the **File name** field, and locate file **vc.hc** from the **7-DecryptingVeraCryptContainer** folder:

The decrypted volume image will be saved in the **Destination folder** location.



Decrypting a VeraCrypt Volume

I don't have a memory image
Brute-force attack will be assigned if you don't have a memory image of the target computer acquired when the encrypted disk was mounted.

I have a memory image
Instant decryption will be performed if you have a memory image of the target computer acquired when the encrypted disk was mounted.

Encrypted VeraCrypt volume image file: D: ⟩ Passware ⟩ PasswareKit2021-QuickStart-Sample-Files ⟩ ... ⟩ vc.hc

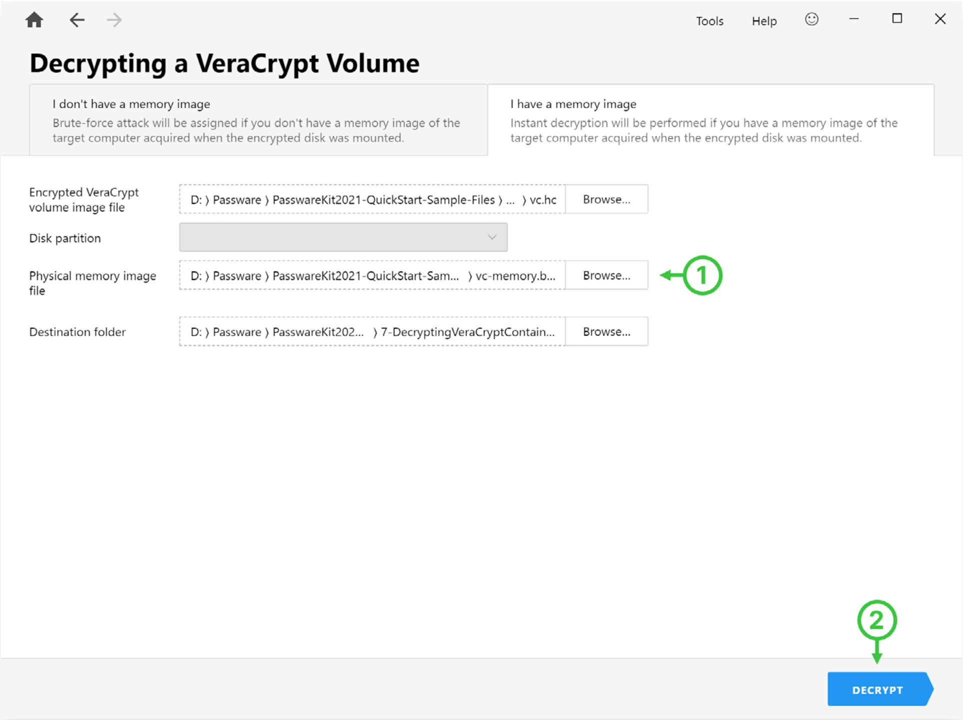
Disk partition:

Physical memory image file: Click to choose or drag file here

Destination folder: D: ⟩ Passware ⟩ PasswareKit202... ⟩ 7-DecryptingVeraCryptContain...

4. In the **Physical memory image file** field, click **Browse**... and locate the **vc-memory.bin** file.

Click **Decrypt**:



Decrypting a VeraCrypt Volume

I don't have a memory image
Brute-force attack will be assigned if you don't have a memory image of the target computer acquired when the encrypted disk was mounted.

I have a memory image
Instant decryption will be performed if you have a memory image of the target computer acquired when the encrypted disk was mounted.

Encrypted VeraCrypt volume image file: D: ⟩ Passware ⟩ PasswareKit2021-QuickStart-Sample-Files ⟩ ... ⟩ vc.hc

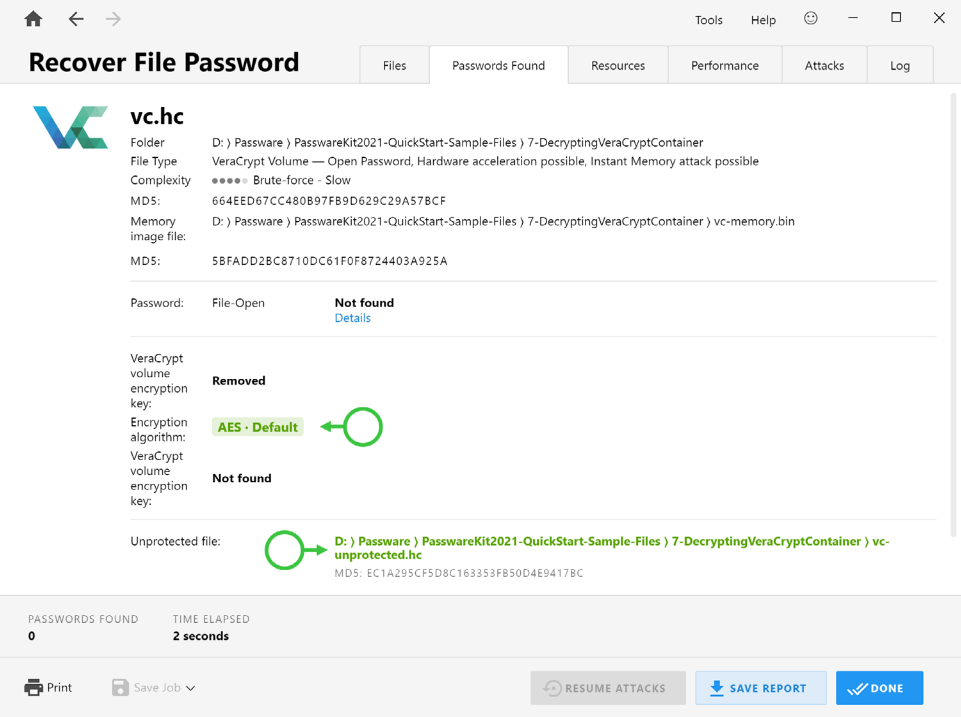
Disk partition:

Physical memory image file: D: ⟩ Passware ⟩ PasswareKit2021-QuickStart-Sam... ⟩ vc-memory.b...

Destination folder: D: ⟩ Passware ⟩ PasswareKit202... ⟩ 7-DecryptingVeraCryptContain...

5. Passware Kit extracts the VeraCrypt volume encryption key and uses it to decrypt the volume:

It also displays the encryption algorithm used to protect the container.



Recover File Password

vc.hc

Folder	D: 〉 Passware 〉 PasswareKit2021-QuickStart-Sample-Files 〉 7-DecryptingVeraCryptContainer
File Type	VeraCrypt Volume — Open Password, Hardware acceleration possible, Instant Memory attack possible
Complexity	●●●●● Brute-force - Slow
MD5:	664EED67CC480B97FB9D629C29A57BCF
Memory image file:	D: 〉 Passware 〉 PasswareKit2021-QuickStart-Sample-Files 〉 7-DecryptingVeraCryptContainer 〉 vc-memory.bin
MD5:	5BFADD2BC8710DC61F0F8724403A925A

Password: File-Open **Not found**
Details

VeraCrypt volume encryption key:	**Removed**
Encryption algorithm:	**AES · Default**
VeraCrypt volume encryption key:	**Not found**

Unprotected file: **D: 〉 Passware 〉 PasswareKit2021-QuickStart-Sample-Files 〉 7-DecryptingVeraCryptContainer 〉 vc-unprotected.hc**
MD5: EC1A295CF5D8C163353FB50D4E9417BC

PASSWORDS FOUND
0

TIME ELAPSED
2 seconds

Passware Tip: *More related articles [Tips for Efficient TrueCrypt/VeraCrypt Decryption] and [BitLocker Decryption Explained] from our blog.*

Congratulations!

You have successfully completed all the tasks!

Enroll on Passware Certified Examiner (PCE) Training now to become a certified decryption expert.

Questions?

Contact us for assistance.