

## PRACTICAL: 7

### AIM:

Crack the Application Password using the following tools: Passware Password Recovery Kit Forensic, Advanced Archive Password Recovery, and Advanced PDF Password Recovery.

### THEORY:

#### Passware Password Recovery Kit Forensic:

The full password-protected electronic evidence finding solution, Passware Kit Forensic reports and decrypts every password-protected file on a computer. The software operates in batch mode to recover passwords and can identify more than 340 different file types.

Password managers, Apple iTunes Backup, Microsoft Office, PDF, Zip and RAR, QuickBooks, FileMaker, Lotus Notes, Bitcoin wallets, Mac OS X Keychain, Zip and RAR, and many other well-known Programmes.

APFS, Apple DMG, BitLocker, Dell, FileVault2, LUKS and LUKS2, McAfee, PGP, Symantec, TrueCrypt, and VeraCrypt disc images can have their passwords decrypted or recovered. allows for batch processing.

Analyzes live memory images and hibernation files and extracts encryption keys for hard disks and passwords for Windows & Mac accounts. Passware Bootable Memory Imager acquires memory of Windows, Linux, and Mac computers.

#### Advanced Archive Password Recovery:

Advanced Archive Password Recovery can unlock ZIP, 7Zip, and RAR archives that have been encrypted and were made with any version of major archivers. It can also retrieve protection passwords. Passwords for plain and self-extracting PKZip and WinZip, 7Zip, RAR, and WinRAR archives can be recovered automatically or with your help. Exploiting an implementation fault enables guaranteed unlocking of archives prepared with WinZip 8.0 and earlier in less than an hour.

The best-in-class performance in unlocking all sorts of archives is offered by Advanced Archive Password Recovery, which has perfect compatibility with all archive types, is aware of the flaws in certain types of protection, and knows which types of archives can be unlocked.

The only recovery tool that comes close to being fully universal is Advanced Archive Password Recovery, which supports a wide variety of compression and encryption algorithms, all versions of well-known archivers, and many archive formats.

Advanced Archive Password Recovery decrypts archives that have been compressed using a variety of techniques, including traditional Shrinking, Reducing, Imploding, and Tokenizing, as well as more contemporary Inflating, WavPack, BZip2, and PPMd.

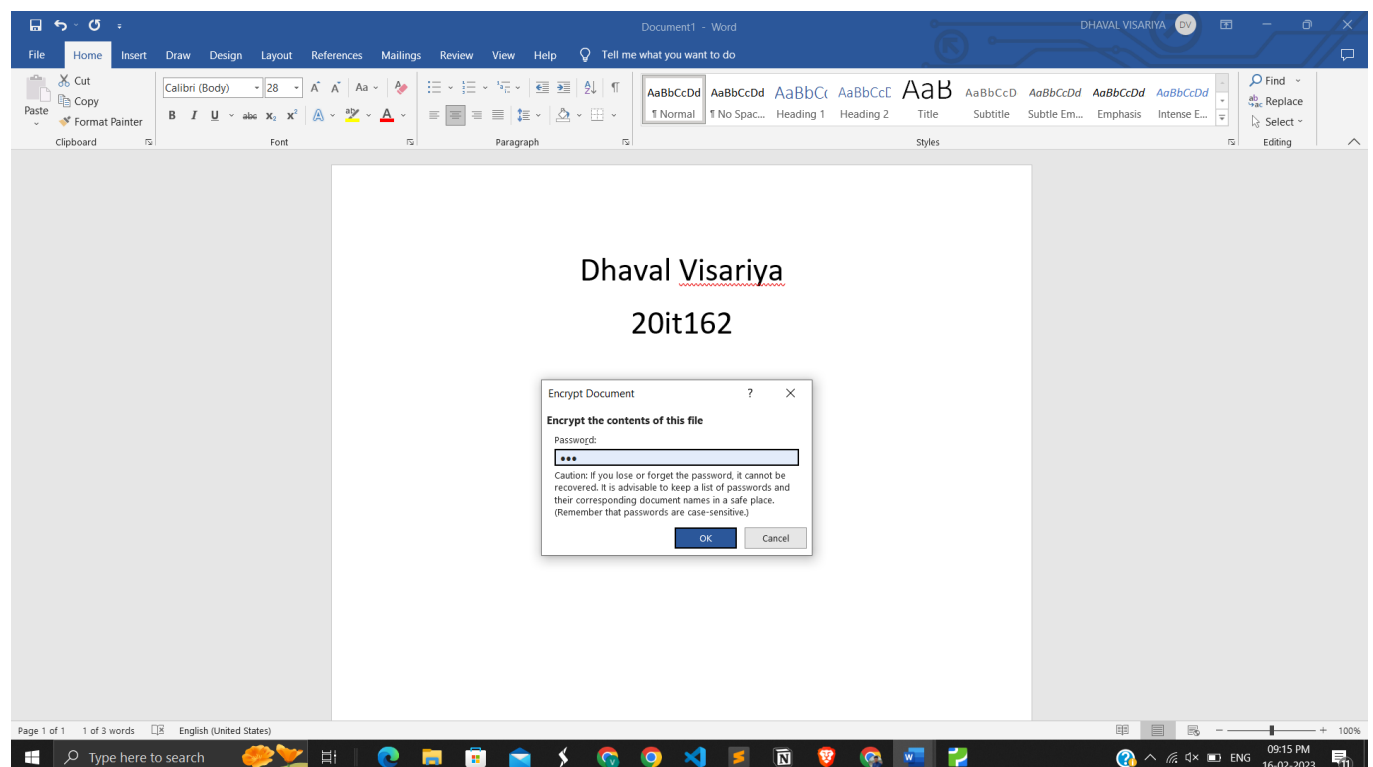
## Advanced PDF Password Recovery:

Unable to open a PDF file that has a password? By using an extremely sophisticated GPU-accelerated attack, "password to open" can be broken. Dictionary attacks and brute force can be easily used with Elcomsoft Advanced PDF Password Recovery. To cut down on the amount of passwords to try, combine masks, patterns, and rules. Modern high-performance video cards can be used to break PDF passwords more quickly than ever thanks to advanced GPU acceleration.

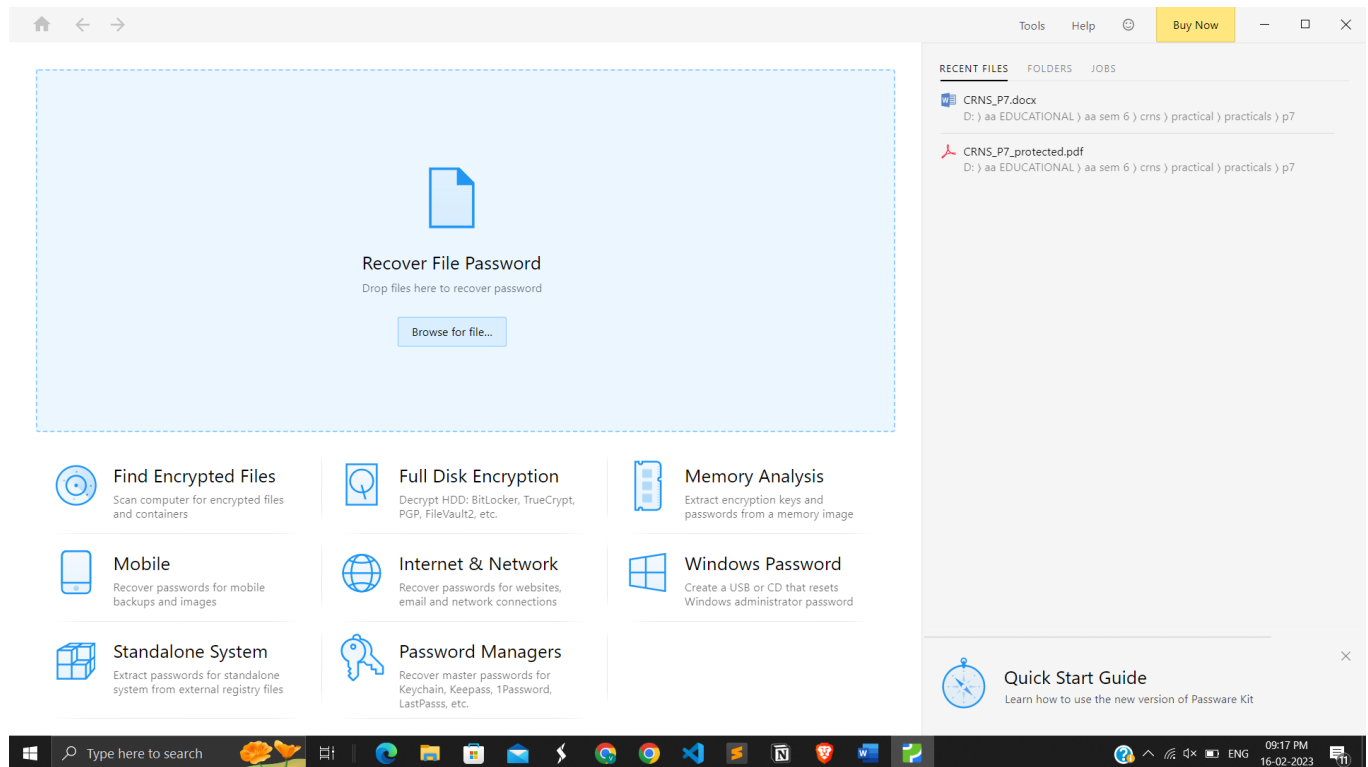
Password-protected PDF files can be accessed easily and quickly! By removing the printing, editing, and copying restrictions, you can instantly unlock restricted PDF documents if there is no "password to open" or if you know it. Advanced PDF Password Recovery will rapidly unlock or recover passwords that have been used to lock or protect PDF files made with any version of Adobe Acrobat or another PDF application. Advanced PDF Password Recovery employs a number of assaults on the PDF file document in order to discover the original password if the PDF is secured with a robust 128-bit or 256-bit key. However, even in that case, you still have options!

Third-Party Security Plug-ins and DRM: The use of Digital Rights Management (DRM) technology or any other third-party security plug-ins, such as FileOpen (FOPN fLock), is not supported by Advanced PDF Password Recovery.

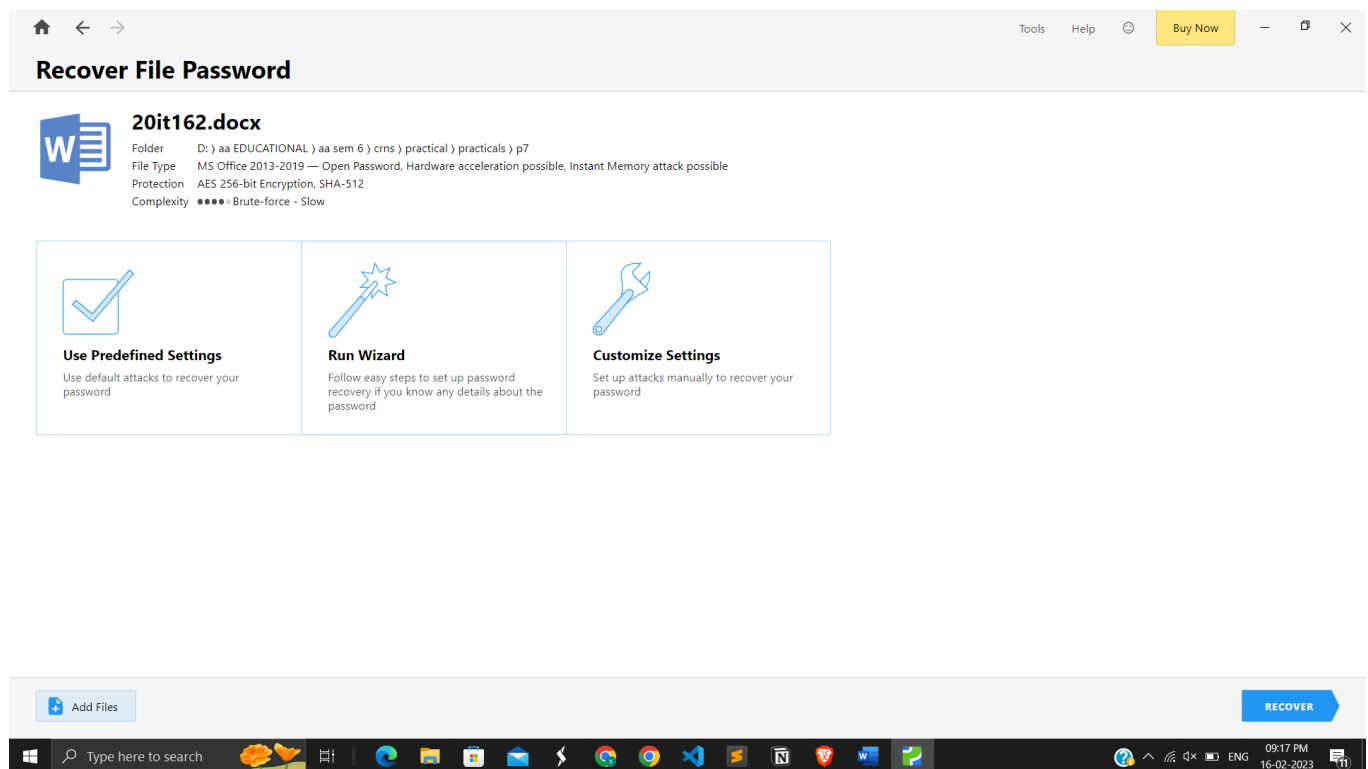
## OUTPUT:



Added password in word



### Interface of Passware Password Recovery Kit Forensic



### Three methods to get file password recovery

## Attacks Settings

Structure › Language › Length & Casing

Any information about the password helps to reduce the recovery time.

The password is:

- ☒ One dictionary word apple
- ☐ More than one dictionary word greenapple
- ☐ One or more dictionary words combined with letters, numbers, or symbols apple!xyz or green123apple
- ☐ Non-dictionary, but similar to an English word softool or johnsapple
- ☐ Other
- ☐ I know nothing about the password

Basic attack settings

## Attacks Settings

Structure › Language › Type › Settings

- Password Type
- ☐ Contains letters only and resemble an English word i.e. softool  
\*Xieve attack can be applied to this part
  - ☒ Doesn't resemble an English word

# Attacks Settings

Structure > Language > Type > Settings

The length of this part of the password:

1

 to 

4

 characters

Known pattern (if any):

\*known parts can be separated with '\*' or '?', i.e., "\*p?e\*" will match both "apple" and "pie"\*

This part can use:

☐ Letters

☒ Numbers

☐ Symbols

☐ Space

Additional characters used:

Additional attack settings like only number, letters etc

Recover File Password

Files


Passwords Found

Resources

Performance

Attacks

Log



20it162.docx

Folder

D:\aa EDUCATIONAL \aa sem 6 \crns \practical \practicals \p7

File Type

MS Office 2013-2019 — Open Password, Hardware acceleration possible, Instant Memory attack possible

Protection

AES 256-bit Encryption, SHA-512

Complexity

■■■■ Brute-force - Slow

MD5

E29643D0E3496EB33FF107C13A295F18

Passwords:

File-Open

162

File-Modify

no password is set

PASSWORDS FOUND

1

TIME ELAPSED

6 seconds

PASSWORDS ANALYZED

4,395

Finally password crack 162

## Attacks Settings

[Structure](#) › [Language](#) › [Length & Words](#) › [Parts Settings](#) › [Part 1](#) › [Part 2](#) › [Part 3 Type](#) › [Part 3](#)

Any information about the password helps to reduce the recovery time.

The password is:

- ☐ One dictionary word apple
- ☐ More than one dictionary word greenapple
- ☒ One or more dictionary words combined with letters, numbers, or symbols apple!xyz or green123apple
- ☐ Non-dictionary, but similar to an English word softool or johnsapple
- ☐ Other
- ☐ I know nothing about the password

Made a second file in which password is it162 and have additional setting

## Attacks Settings

[Structure](#) › [Language](#) › [Length & Words](#) › [Parts Settings](#) › [Part 1](#) › [Part 2 Type](#) › [Part 2](#)

- Password structure:
- ☒ Dictionary + Non-dictionary apple123
  - ☐ Non-dictionary + Dictionary 123apple
  - ☐ Non-dictionary + Dictionary + Non-dictionary 123apple123
  - ☐ I don't know

- I know information about
- ☒ the first dictionary part
  - ☒ the first non-dictionary part

It consists of Dictionary + Non dictionary words so I choose it

Attacks Settings

Structure > Language > Length & Words > Parts Settings > Part 1 > Part 2 Type > Part 2

Set the password length:  to  characters

Known pattern (if any):

\*known parts can be separated with '\*' or '?', i.e., "\*p?e\*" will match both "apple" and "pie"

- How uppercase/lowercase letters are used in this part of the password:
- ☐ Original

aPPlE
- ☒ All lowercase
- apple
- ☐ All uppercase
- APPLE
- ☐ Normal casing
- Apple
- ☐ Toggle casing
- aPPLE
- ☐ Mixed casing
- ApPIE

☐ Also try reversed words    apple -> elppa

Set a length and if I have any pattern

Attacks Settings

Structure > Language > Length & Words > Parts Settings > Part 1

Set the password length:  to  characters

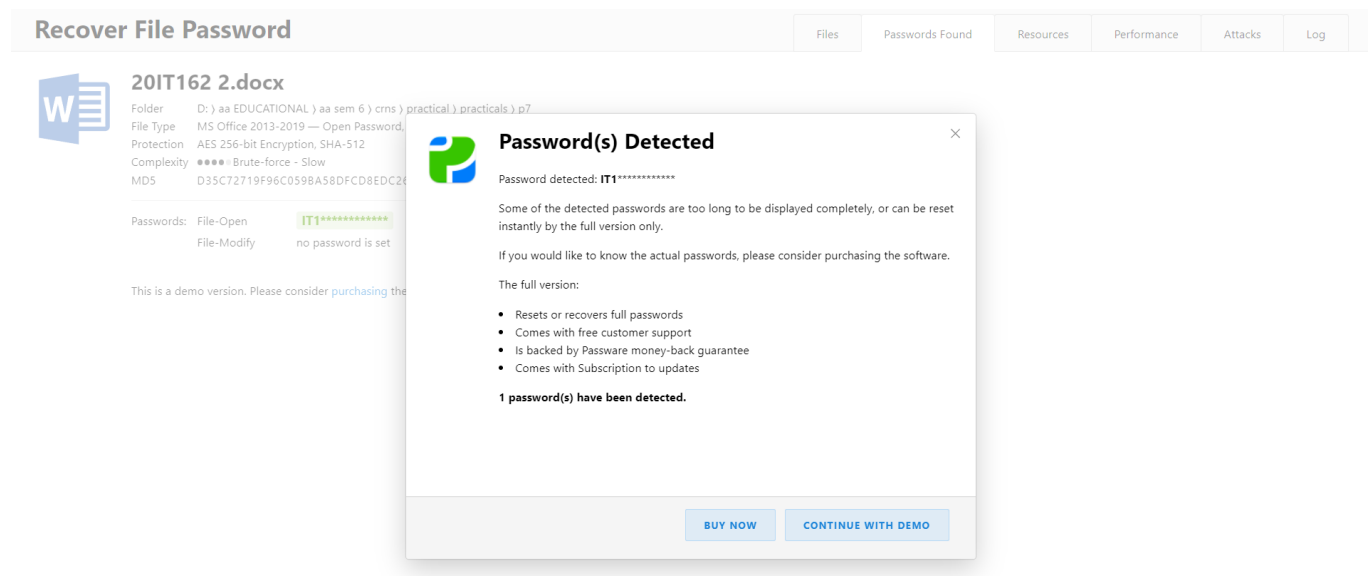
Known pattern (if any):

\*known parts can be separated with '\*' or '?', i.e., "\*p?e\*" will match both "apple" and "pie"

- How uppercase/lowercase letters are used in this part of the password:
- ☐ Original

aPPlE
- ☐ All lowercase
- apple
- ☒ All uppercase
- APPLE
- ☐ Normal casing
- Apple
- ☐ Toggle casing
- aPPLE
- ☐ Mixed casing
- ApPIE

☐ Also try reversed words    apple -> elppa



Finally it162 is also cracked

## LATEST APPLICATIONS:

**Passware Password Recovery Kit Forensic:** The software can recognise more than 340 distinct file types and recover passwords in batch mode.

Passware Kit Forensic includes over 30 password recovery tools, Encryption Analyzer Professional, Search Index Examiner, FireWire Memory Imager, and a Portable Version to provide immediate password recovery for any protected file detected on a PC or over the network while scanning.

**Advanced Archive Password Recovery** – It decrypts compressed archives created by a variety of methods, including the classic Shrinking, Reducing, Imploding, and Tokenizing as well as the more recent WavPack, BZip2, and PPMd.

**Advanced PDF Password Recovery - Third-Party Security Plug-ins and DRM:** The use of Digital Rights Management (DRM) technology or any other third-party security plug-ins, such as FileOpen (FOPN fLock), is not supported by Advanced PDF Password Recovery. With 256-bit AES encryption, Adobe Acrobat X PDF files are compatible with version 5.0, which also supports multicore and multi-processor systems and hardware acceleration with NVIDIA graphics cards

## LEARNING OUTCOME:

- In the task to get the password known the concept of constraints settings in passware software efficiently that we get the password easily.



- The kind of attacks we can make in the advanced pdf recovery like brute force attack and the plain text attack along with the detailed requirements of the variable.
- And the generation of the report of the document on which brute force attack is been executed helps to know about the location of the file along with the time required to find the correct password.

**REFERENCES:**

Passware Password Recovery Kit Forensic - <https://www.passware.com/kit-forensic/>

Tutorial - <https://www.youtube.com/watch?v=-kYx4VhFcvA>