PRACTICAL: 7

AIM:

A digital forensics team is investigating a case involving encrypted files and documents critical to their investigation. The team must recover the passwords for various applications, including archived files and PDF documents, using tools like Passware Password Recovery Kit Forensic, Advanced Archive Password Recovery, and Advanced PDF Password Recovery. Recover application passwords using specialized tools to demonstrate password recovery techniques and evaluate the efficiency of each tool in real-world scenarios.

THEORY:

Passware Password Recovery Kit Forensic:

Passware is one of the most well-known tools used in digital forensics for password recovery. It supports a wide range of file formats, including encrypted Office documents (Word, Excel, PowerPoint), PDFs, and more. This tool uses several attack methods to recover passwords:

- **Brute-Force Attack**: This method attempts every possible combination of characters to find the correct password. It can be effective for short or simple passwords but is time-consuming for longer, complex passwords.
- **Dictionary Attack**: This attack uses a pre-compiled list of common passwords and attempts to match the password against entries in the list. It is faster than brute-force and works well when the password is a common word or phrase.
- **Mask Attack**: If the investigator has partial knowledge of the password (e.g., the password's length or the characters it contains), they can use a mask attack to limit the number of combinations attempted, significantly speeding up the process.

Passware is also capable of **GPU acceleration**, which allows the use of graphics cards (GPUs) to speed up password recovery, especially for more complex encryption.

Advanced Archive Password Recovery (AAPR):

AAPR specializes in recovering passwords from encrypted archive files, such as ZIP, RAR, and 7z formats. Archive files are often used for compressing multiple files into a single package, making them a common target in digital investigations.

- **Brute-Force Attack**: AAPR will try every possible combination of characters in an effort to find the password.
- **Dictionary Attack**: Similar to Passware, AAPR can use a wordlist to attempt known passwords, speeding up the recovery process for simple passwords.
- **Mask Attack**: If partial knowledge of the password is available (such as length or known characters), AAPR can use a mask attack to reduce the recovery time.

AAPR is particularly useful for encrypted archive files and can handle various compression formats. It is known for its speed and efficiency when compared to other password recovery tools.

Advanced PDF Password Recovery (APDFPR):

PDF documents are commonly used to store critical data, and they are often protected by passwords. APDFPR specializes in recovering passwords for encrypted PDF files. Similar to the other tools mentioned, it offers several attack methods:

- **Brute-Force Attack**: APDFPR attempts all possible combinations until the correct password is found.
- **Dictionary Attack**: The tool uses a wordlist of common passwords, which can be particularly effective if the password is a commonly used word or phrase.
- **Mask Attack**: If the investigator has knowledge about the length of the password or other patterns (such as specific characters), a mask attack can significantly reduce the time needed to crack the password.

APDFPR also supports the removal of **password restrictions** on PDF files, such as restrictions on printing or copying the document, even if the password to open the file is not recovered.

CODE:

N/A

OUTPUT:

Figure 1: Start Installing of Advanced Archive Password Recovery Setup

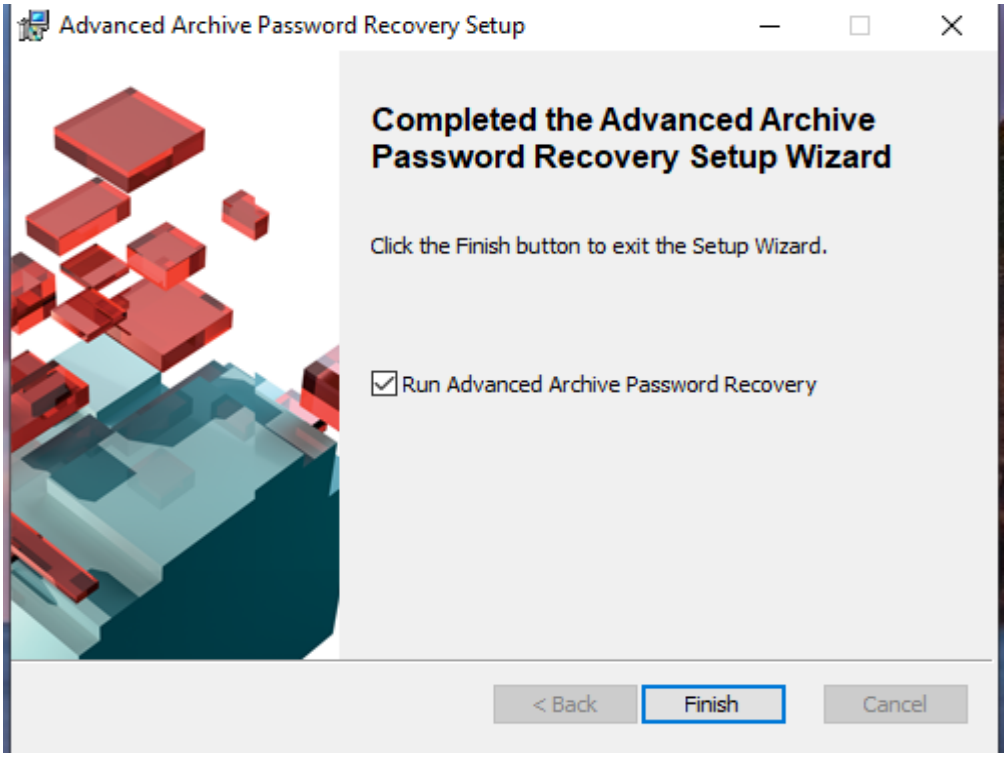

Figure 2: Complete Installing of Advanced Archive Password Recovery Setup

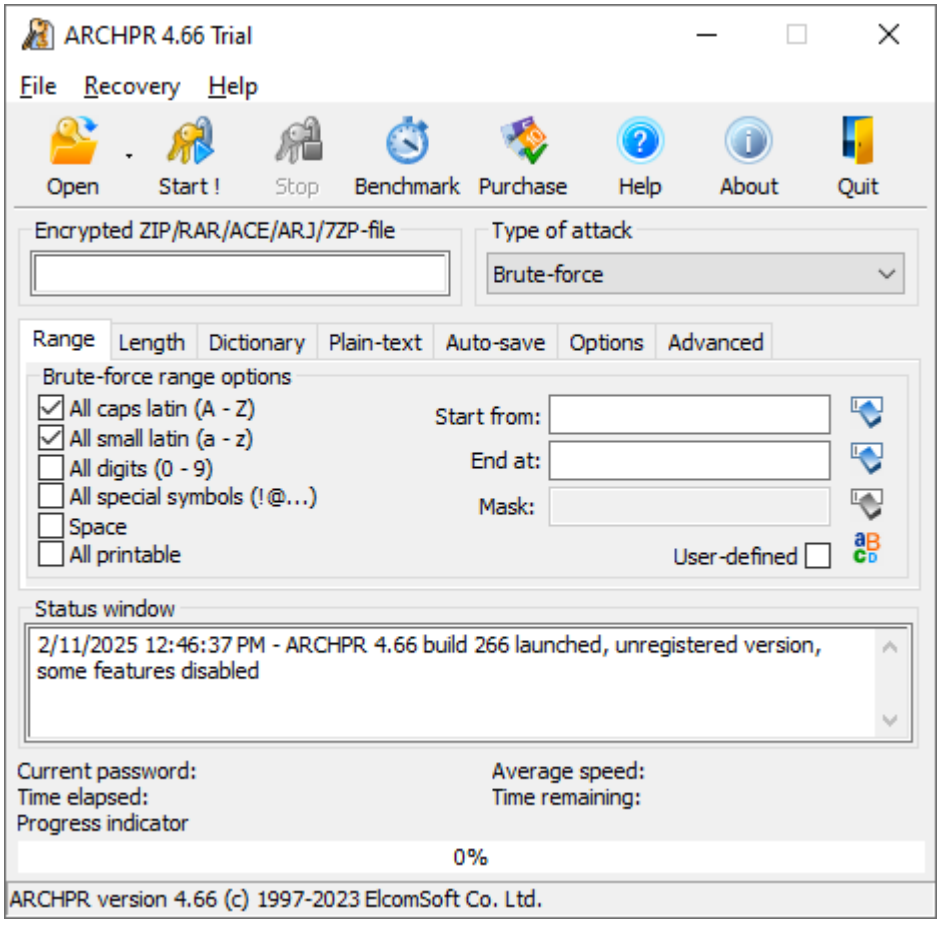

Figure 3: Open Advanced Archive Password Recovery Setup

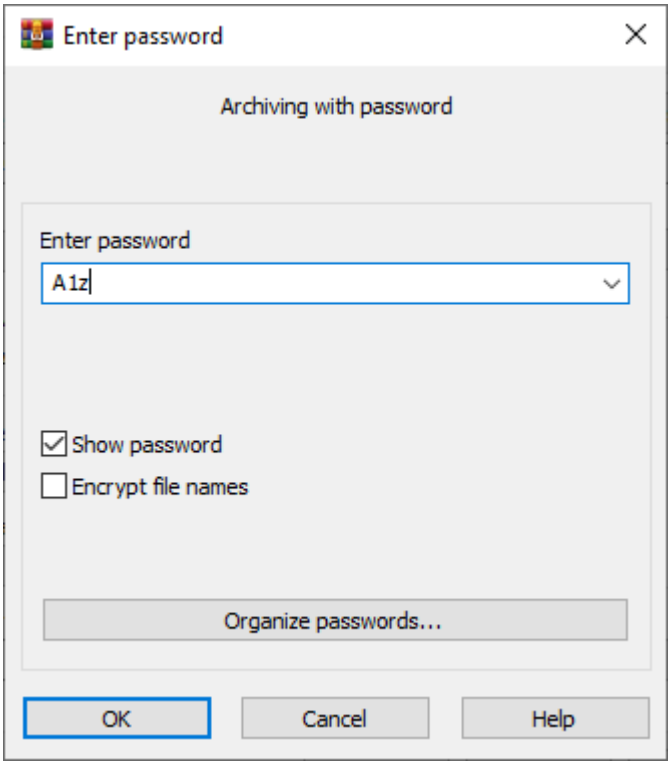

Figure 4:Set password to .rar file

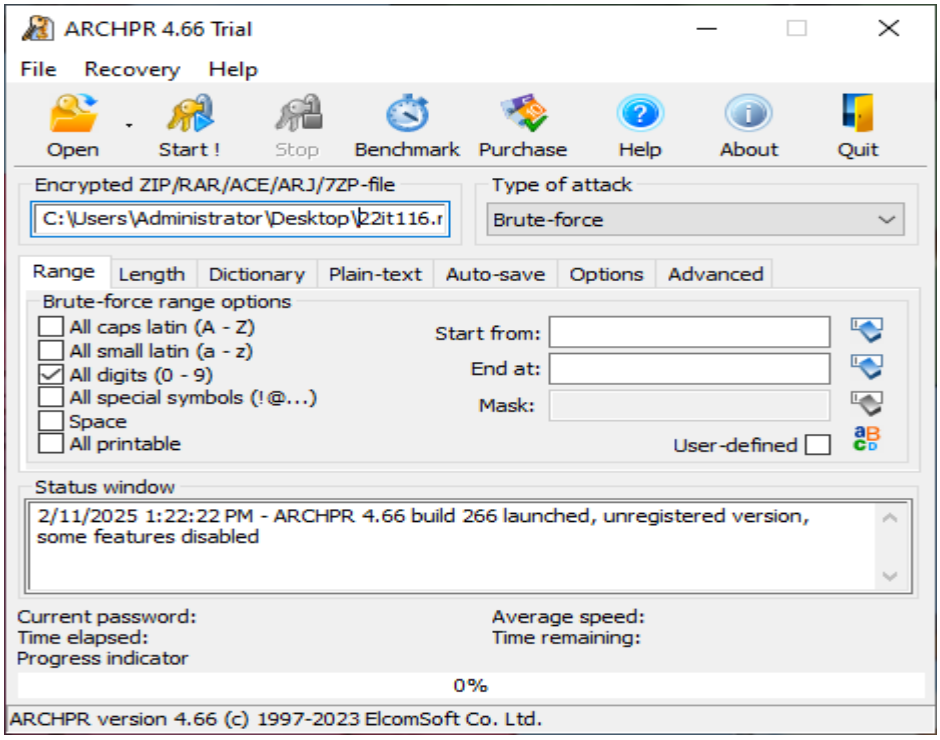

Figure 5:Set Encrypted .rar file to open it and set another parameter

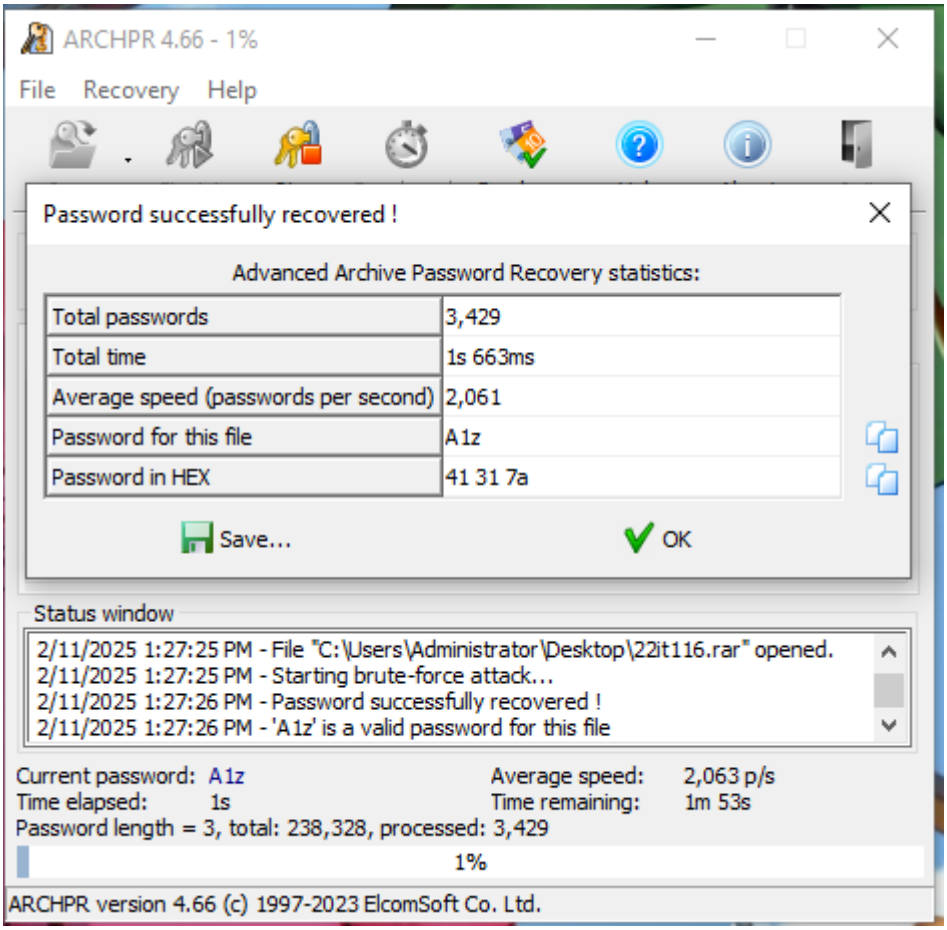

Figure 6: We got our password from Advanced Archive Password Recovery Setup

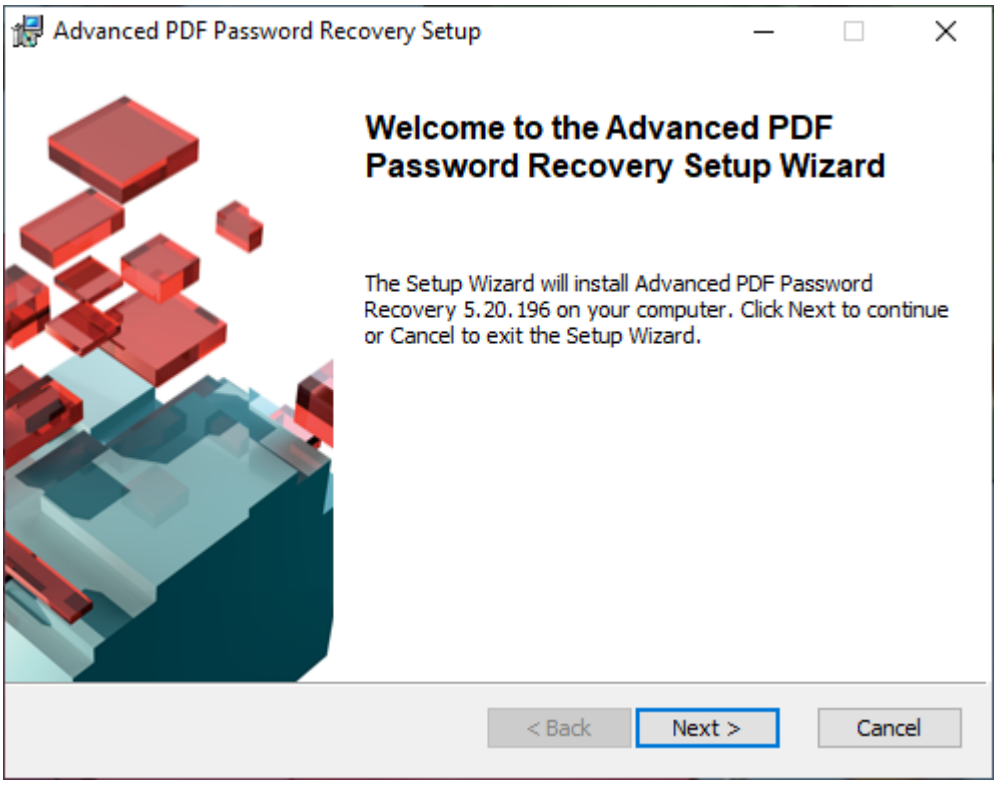

Figure 7: Start installing Advanced PDF Password Recovery Setup

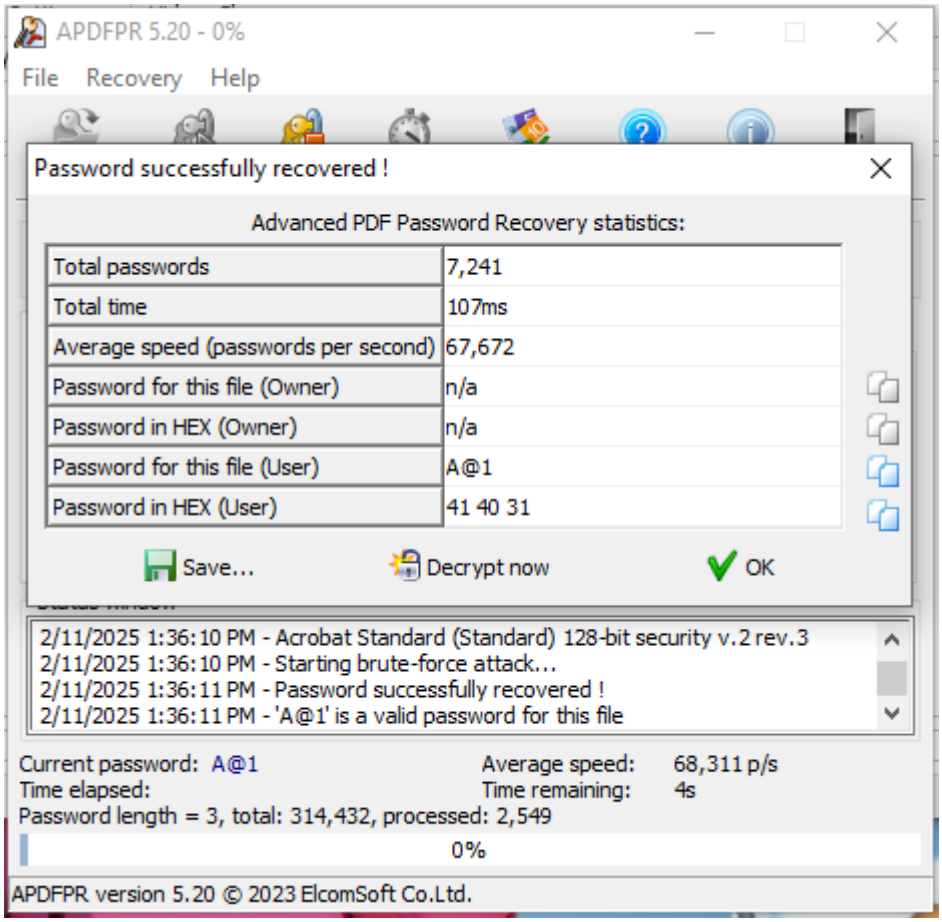

Figure 8:: We got our password from Advanced PDF Password Recovery

Figure 9:Start Passware Encryption Analyzer

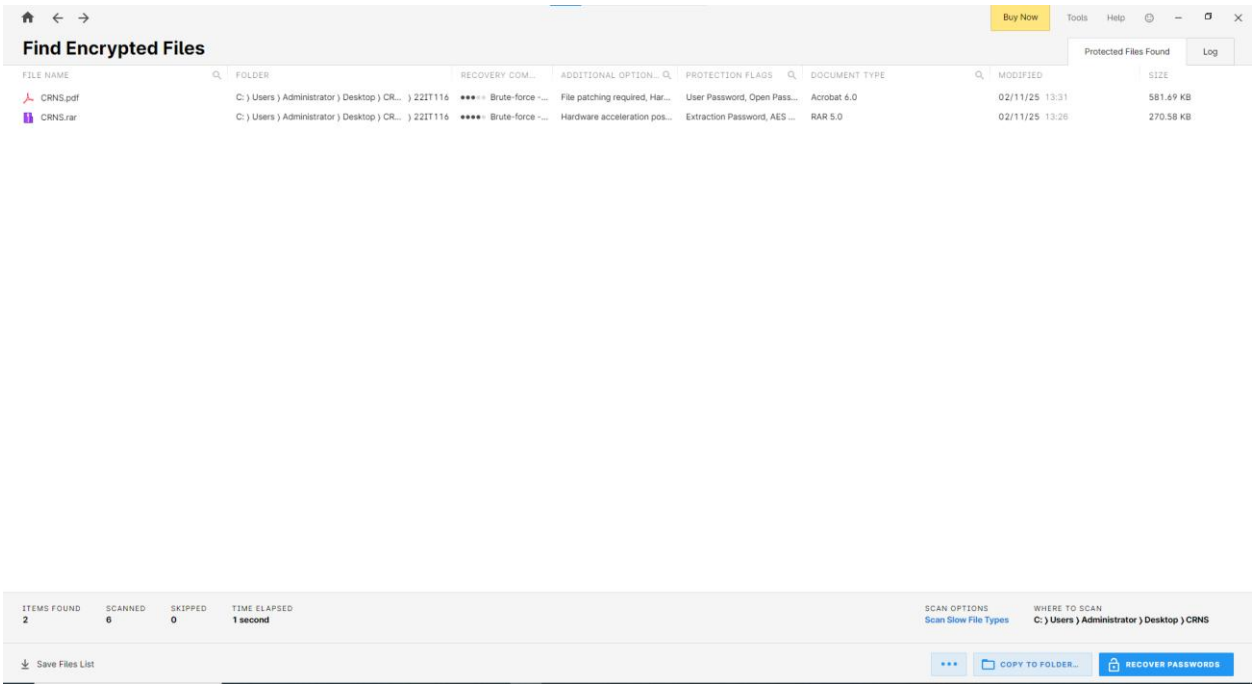

Figure 10:Scan encrypted files

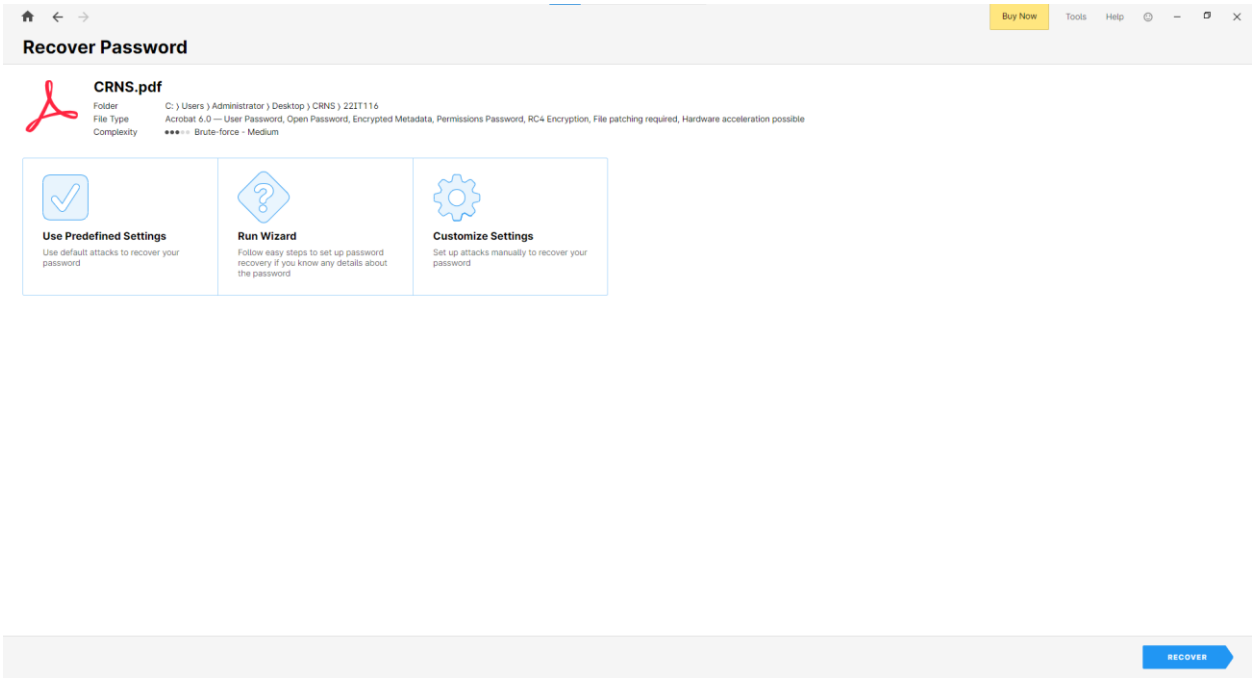

Figure 11:Click recover password for pdf file

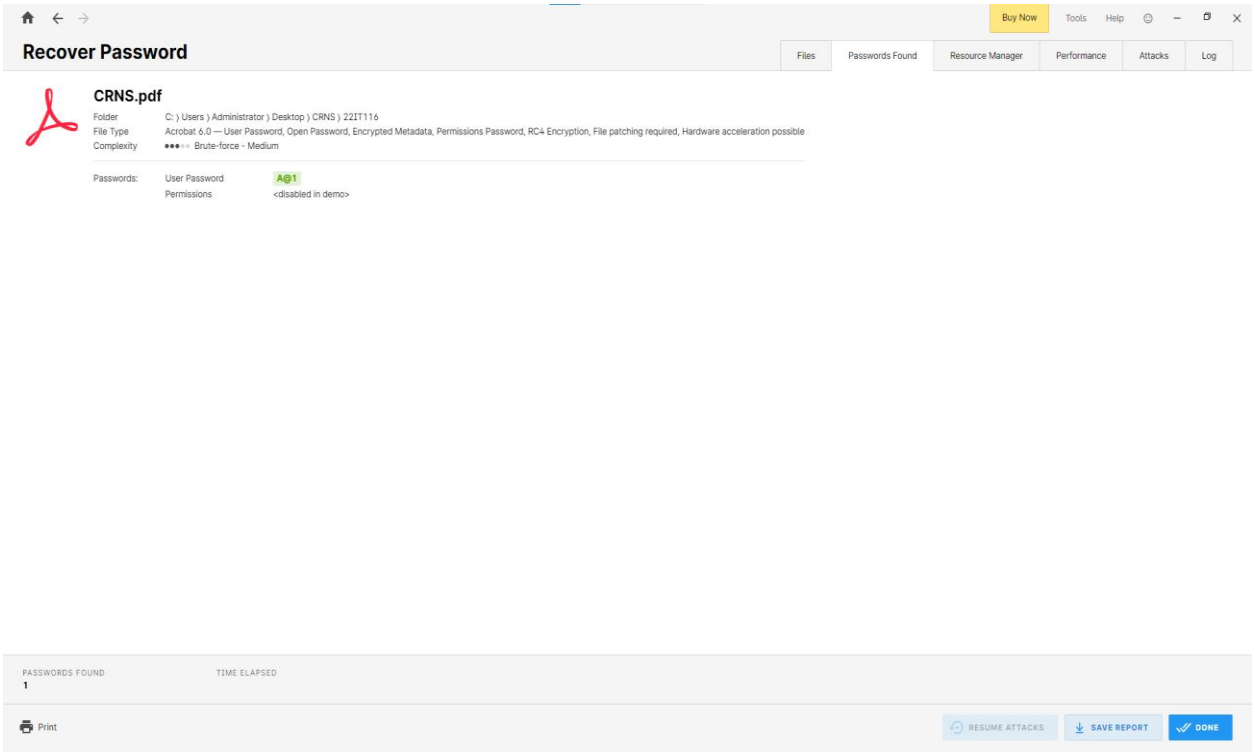

Figure 12: Apply Use Predefined Settings attack

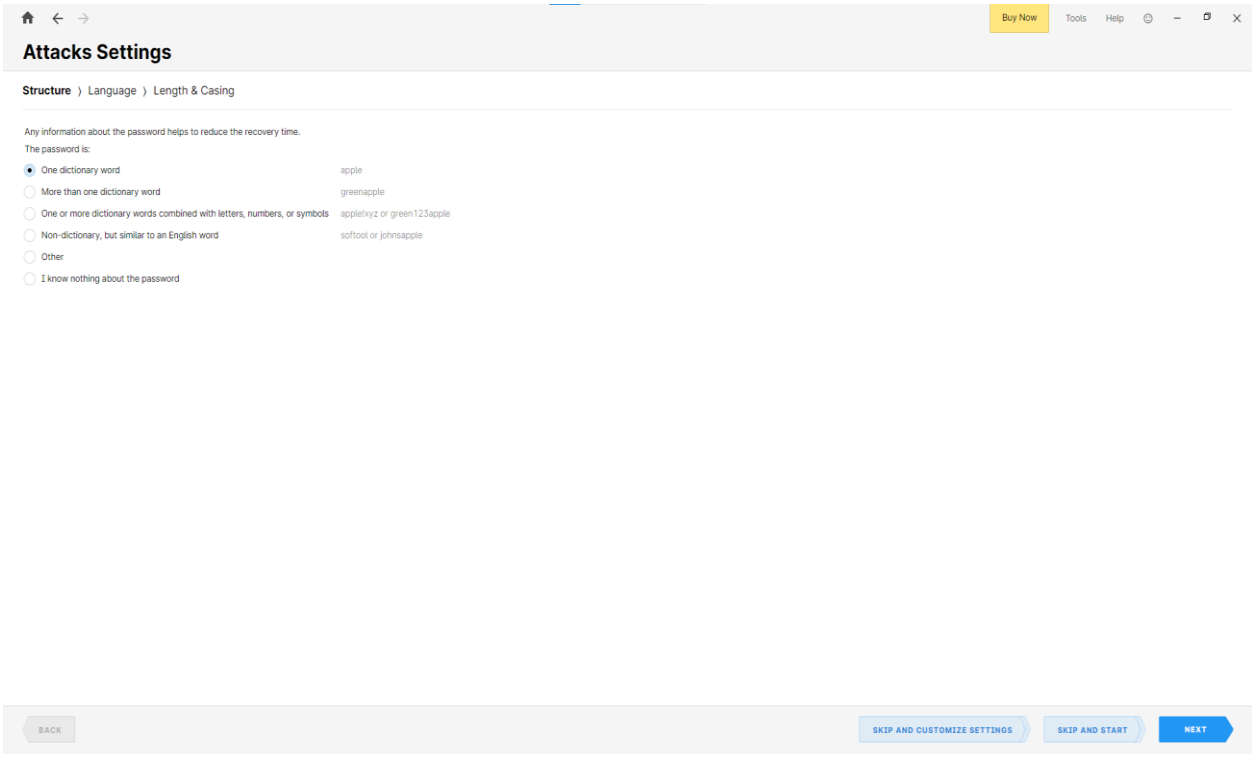

Figure 13:Apply Run Wizard

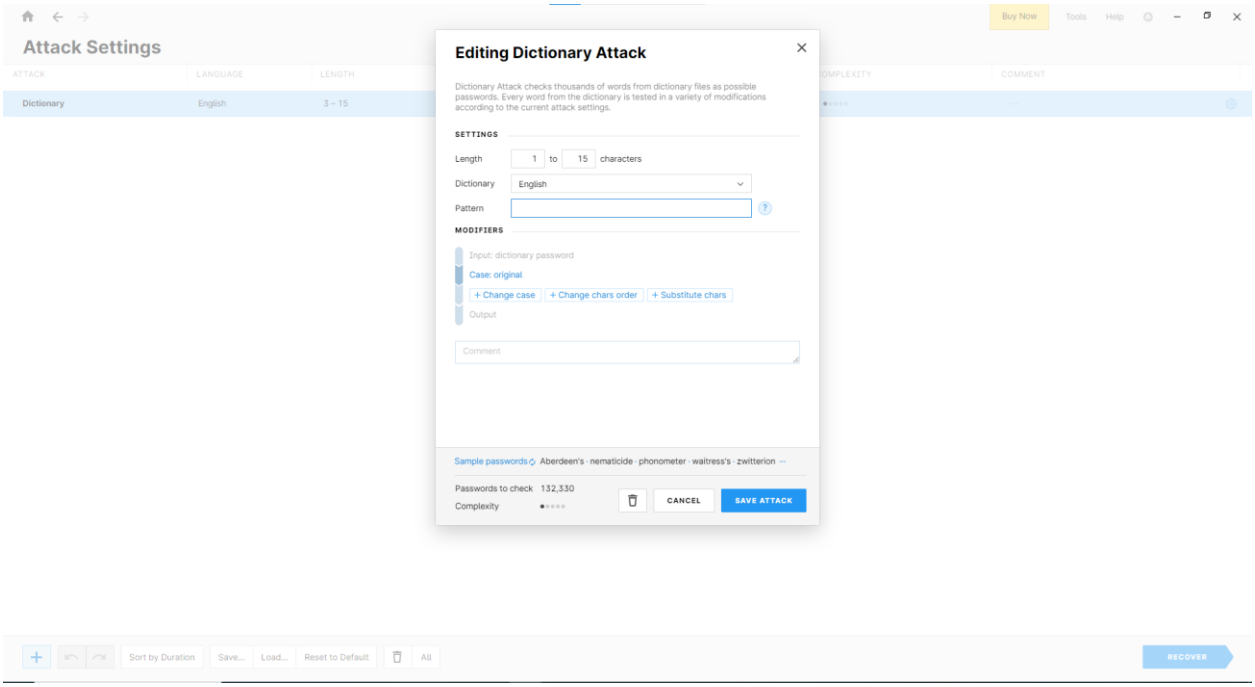

Figure 14:Apply Customize Settings

LATEST APPLICATIONS:

- Hashcat
- Passware Kit 2025 v1
- Kon-Boot
- Active@ Password Changer
- NirSoft Utilities

LEARNING OUTCOME:

In this practical, I gained a deeper understanding of different password recovery methods, including brute-force, dictionary, and mask attacks, and their effectiveness with various encrypted files. Using tools like Passware, AAPR, and APDFPR, I explored how each method performed depending on password complexity and file type.

REFERENCES:

1. Advanced PDF Password Recovery : https://www.elcomsoft.com/apdfpr.html
2. Advanced Archive Password Recovery: https://www.elcomsoft.com/archpr.html
3. Passware Password Recovery Kit Forensic: http://passware.com/
4. ChatGPT : https://chatgpt.com/