



Hash Calculator

Generate MD5, SHA-1, SHA-256, SHA-384, SHA-512, or extract a crackable hash from a password-protected PDF



Text

File

NETWORKWALKS TRAINING ACADEMY

WAQAS KARIM CCIE

CYBERSECURITY & ETHICAL H.

Type or paste text. Hashes update as you type.

☐ Uppercase output

MD5

741b9d258280039a8a210bdb96f9f723

not secure

SHA-1

def99c402a83efe9d7aa66e4f0a73ea7ad6303ad

PASSWORD CRACKER

1 Extract the \$pdf\$ hash in the Hash Calculator 2 Paste it below
3 Run the attack, then open your PDF with the password

PDF HASH (\$pdf\$...)

```
[+] Trying: michelle X  
[-] Trying: trigger X  
[-] Trying: sunshine X  
[-] Trying: chocolate X  
[+] MATCH password1 ✓
```

Built-in list (100 passwords)

Upload wordlist (.txt)

Active: built-in list, 100 words

START CRACKING

PASSWORD CRACKED SUCCESSFULLY

password1

This is the PDF password. Open your PDF and enter it to unlock the file.

Copy password

PASSWORD CRACKING WITH NETWORKWALKS TOOLS

CYBERSECURITY & ETHICAL HACKING PROJECT TASKS



WEEK 3 | PROJECT MODULE 2

PASSWORD CRACKING WITH NETWORKWALKS TOOLS

Background

Password cracking is the process of recovering a password from stored data or a protected file. Security professionals use it to test how strong a password is and to show why weak passwords are risky. If a password is short or common, it can be found quickly, which proves the need for strong passwords.

Many files like PDF, ZIP, and Office documents can be locked with a password. When a file is locked, its password is stored in the form of a hash. A hash is a scrambled value that represents the password. To recover the password, we first take out this hash from the file, and then run it through a cracking tool that tries different words until it finds a match.

In this lab you will use two free online tools made by Networkwalks. First you will use the Hash Calculator to take the hash out of a locked PDF file. Then you will use the Password Cracker to find the real password from that hash. Both tools run in your web browser, so you do not need to install anything.

This lab helps you understand how password cracking works step by step and why strong passwords are important for protection.

Task

Crack the password of the attached PDF file (My Locked PDF1.pdf) using the Networkwalks Hash Calculator and Password Cracker tools on your Windows laptop.

Note: You can also do this lab on Kali Linux, as both tools run in any web browser.

Solution

STEP 1

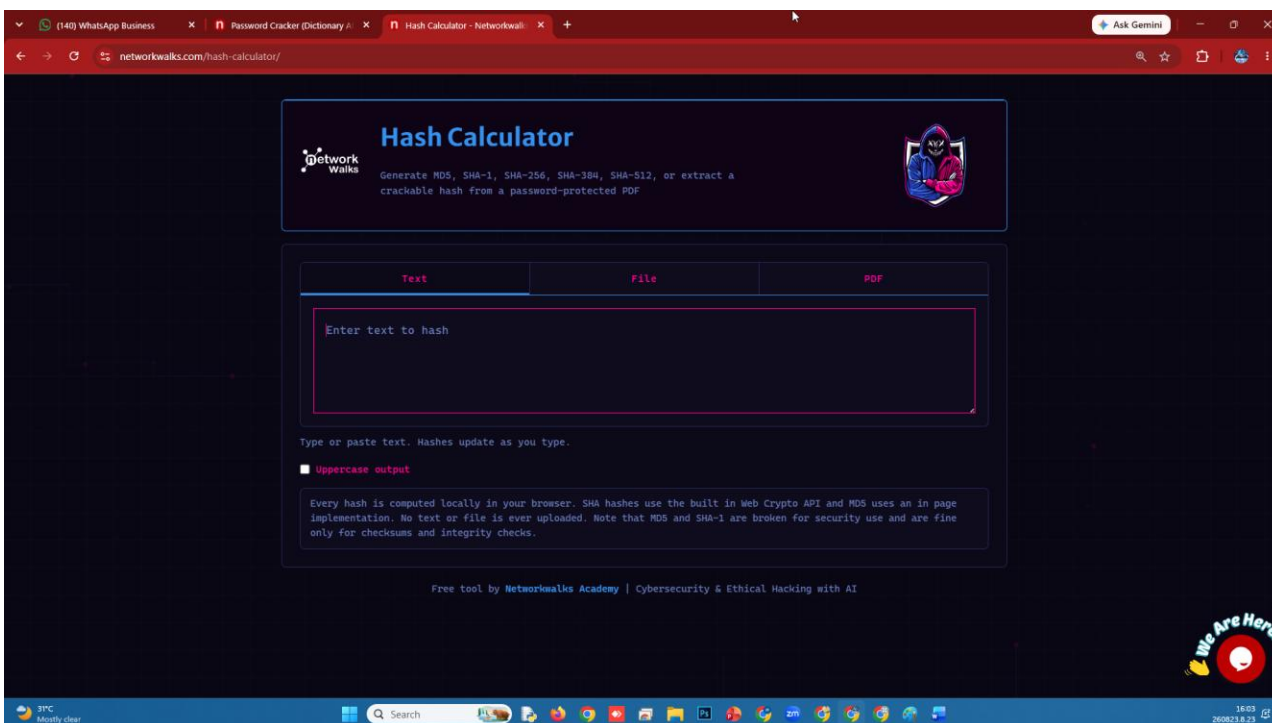
Download the encrypted PDF file (My Locked PDF1.pdf) to your laptop from the lab page:

<https://networkwalks.com/project-task-lab-password-cracking-with-networkwalks-tools/>

STEP 2

Open the Networkwalks Hash Calculator in your web browser:

<https://networkwalks.com/hash-calculator/>

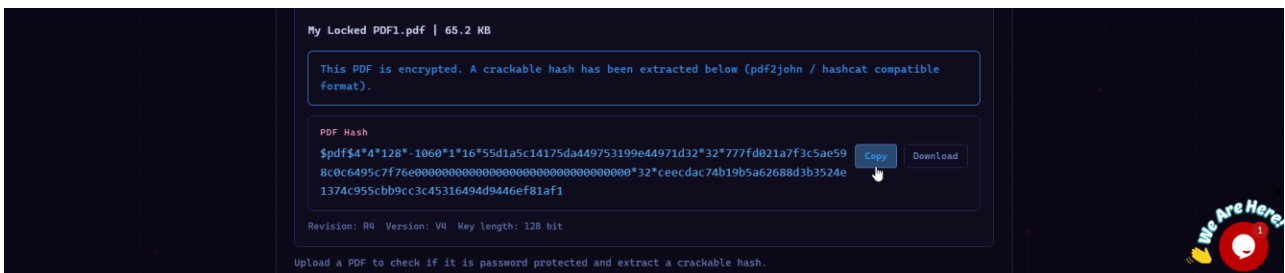


STEP 3

Upload the locked PDF file to the Hash Calculator. The tool will read the file and give you the hash value that starts with \$pdf\$...

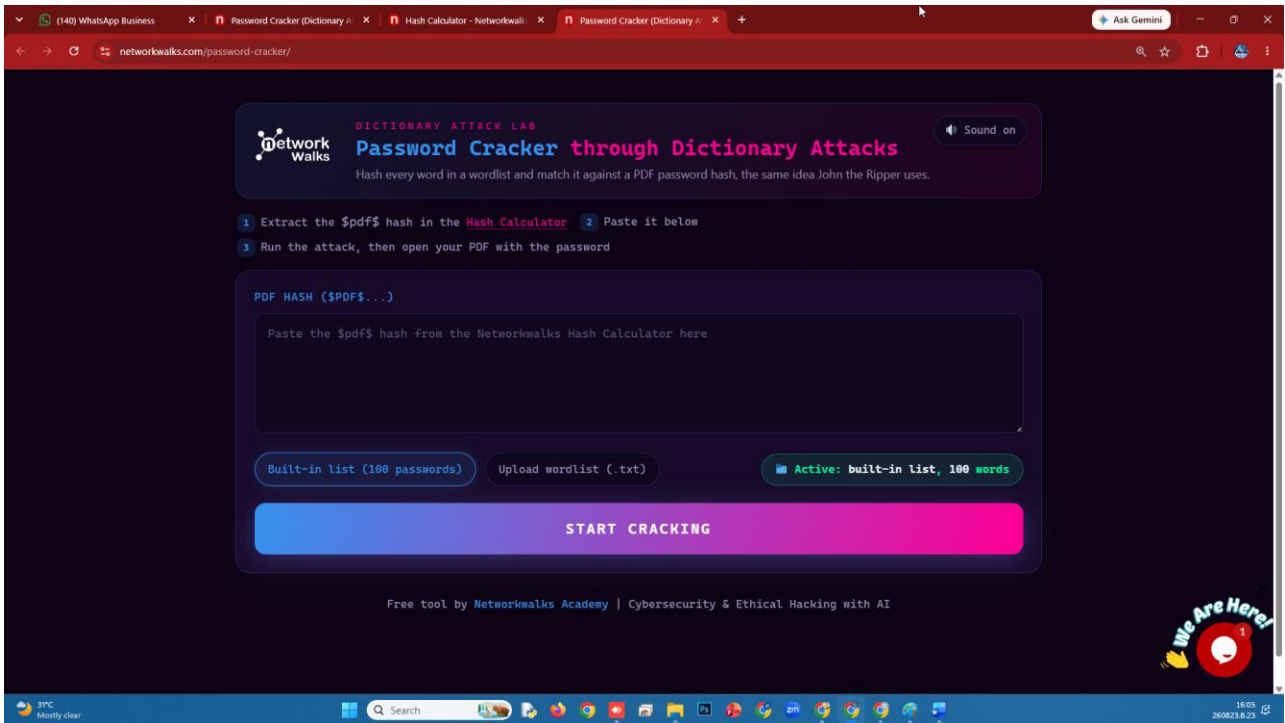
Copy the full hash value.

Note: Copy the complete hash starting from \$pdf\$. Do not miss any part of it.



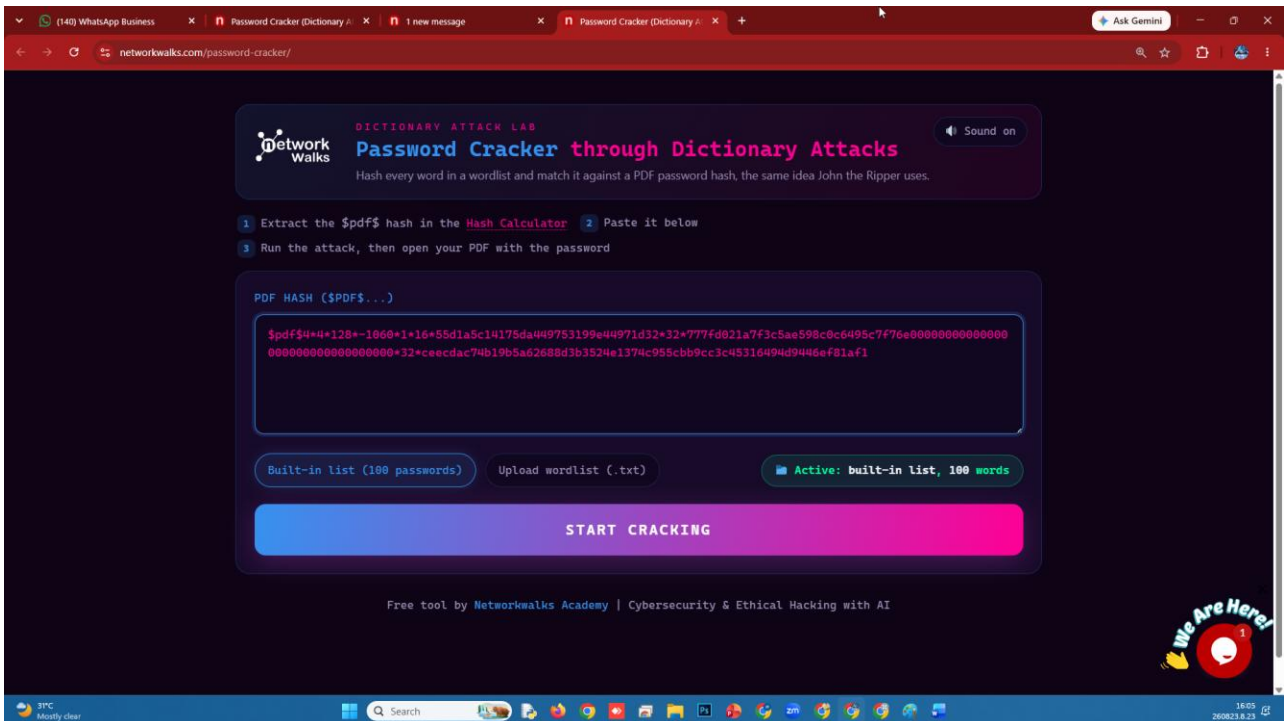
Open the Networkwalks Password Cracker in your web browser:

<https://networkwalks.com/password-cracker/>



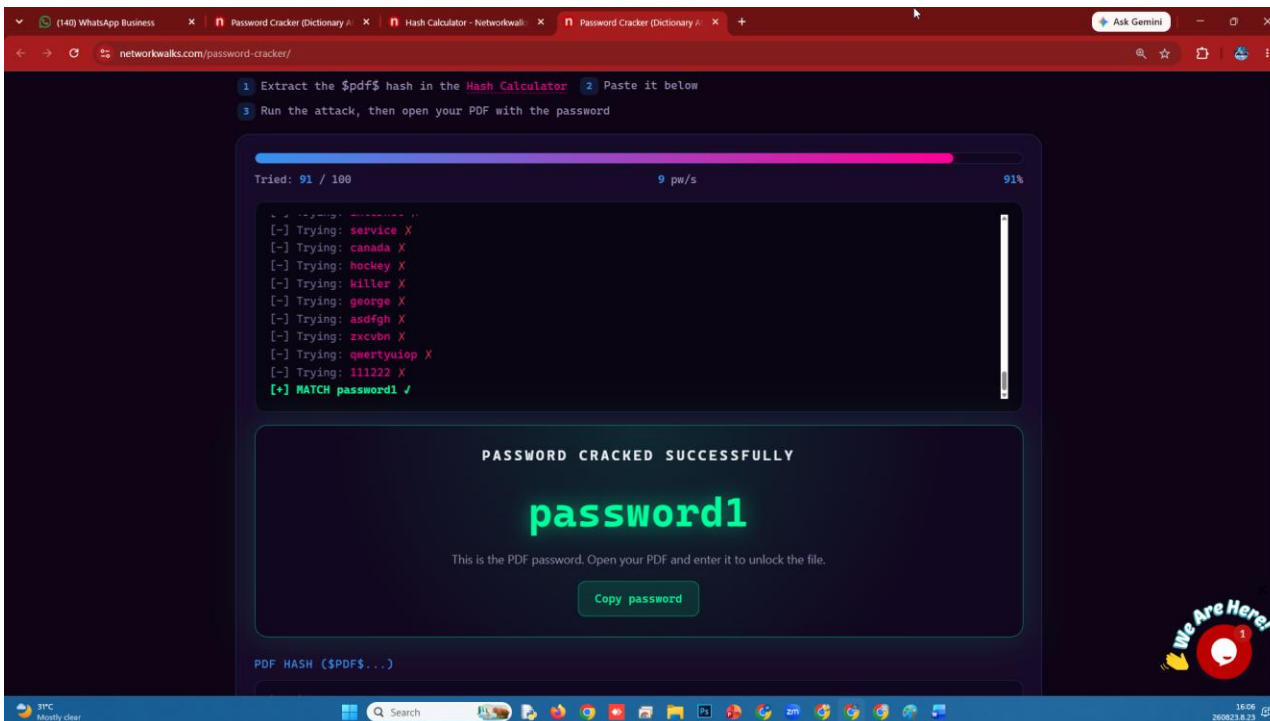
STEP 6

Paste the hash value into the Password Cracker and start the attack. The tool will try different passwords until it finds a match.



STEP 7

Wait for the tool to finish. The cracked password will be shown on the screen.

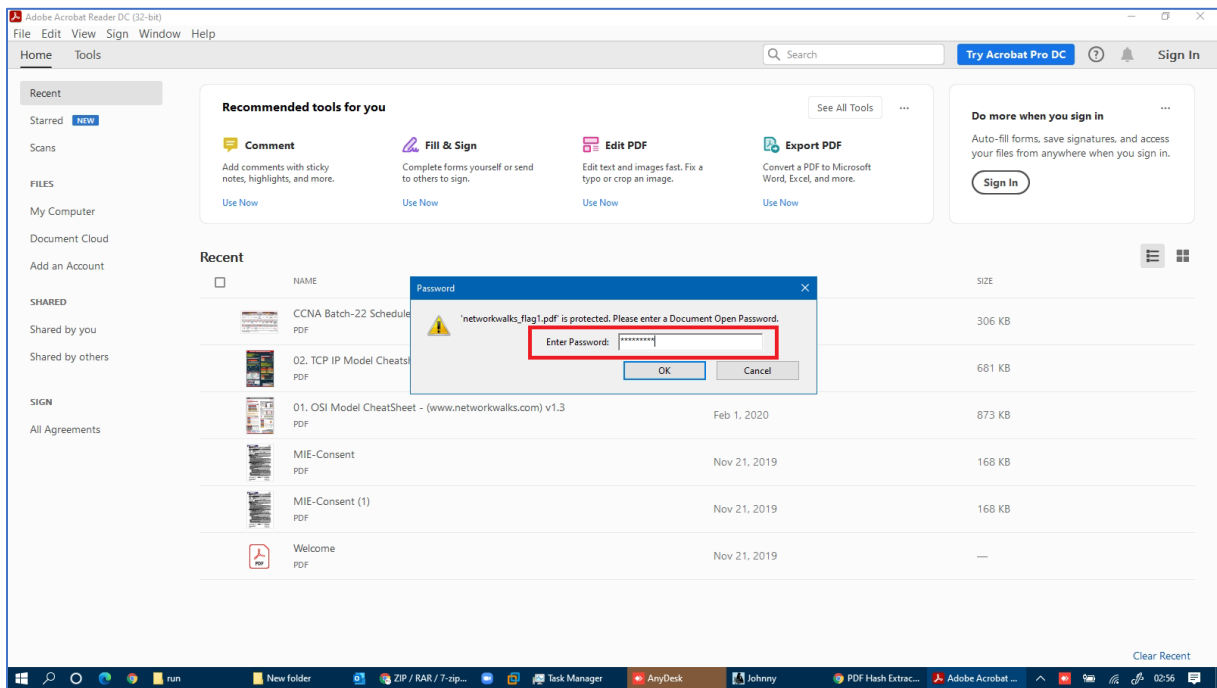


Note: The time taken depends on how simple or complex the password is.

STEP 8

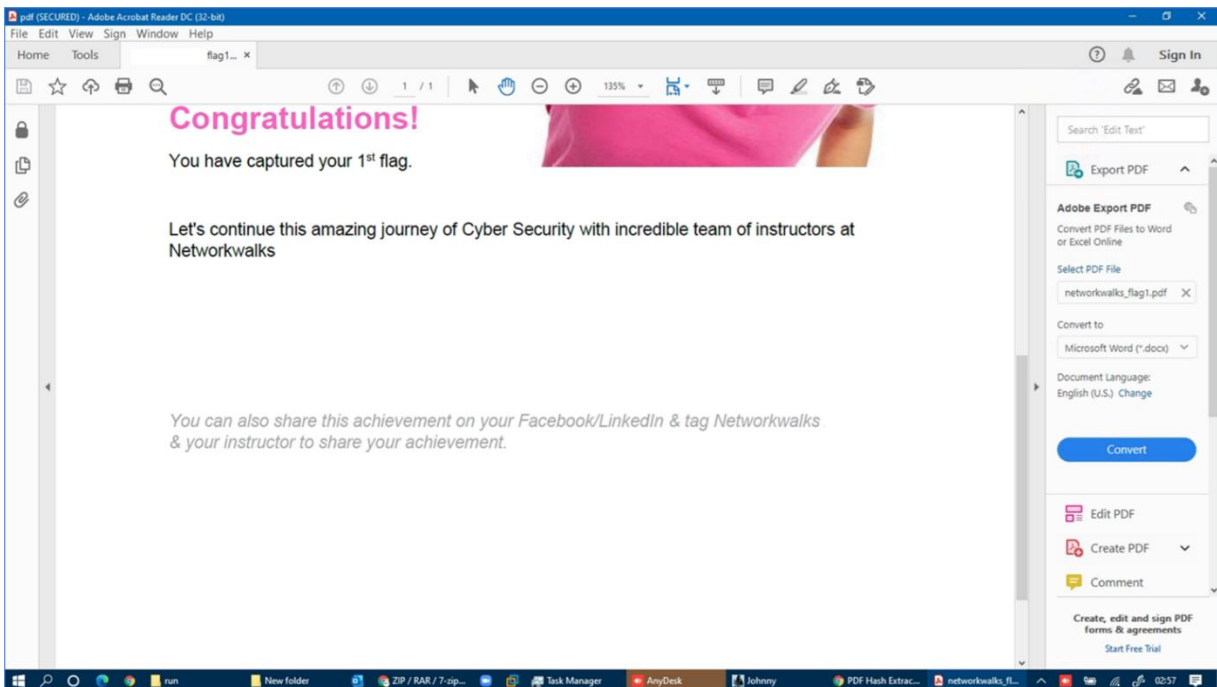
Open the locked PDF file and enter the cracked password.

Enter `password1` (which you have just cracked):



STEP 9

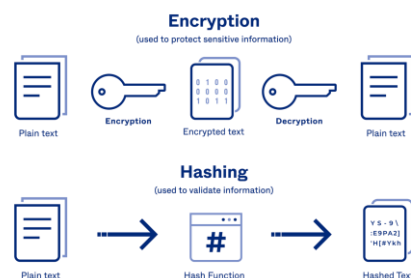
Your PDF file will open. You have completed the lab.



-End-

Extra References & tips

💡 Encryption is a two-way function; what is encrypted can be decrypted with the proper key. Hashing, however, is a one-way function that scrambles plain text to produce a unique message digest, as shown in below.



DO YOU KNOW?

Fact - A simple 8 character password using only lowercase letters can be cracked in minutes, while a strong 12 character mixed password can take many years

Fact - Over 24 billion username and password pairs are available on the dark web from past breaches

Fact - "123456" and "password" are still among the most used passwords in the world every year

Fact - 2025 - Global - A leak of around 183 million Gmail login details showed how old stolen passwords keep circulating for years



© All Rights are reserved, Networkwalks

Contact us today for your Cybersecurity & Network consultancy or your next training course & certification on Cisco CCNA, Cybersecurity, Ethical Hacking, Python programming, Linux & AI.

📞 +27 766 222 218 | +27 788 220 600

Leave your feedback at: info@networkwalks.com. Your technical questions, comments & suggestions are always Welcomed.
www.networkwalks.com