**Assignment No.7**

**Title :** Password Cracking Using tool : John the Ripper

**( zip folder password cracking )**

**Step 1: Download John the Ripper Jumbo for Windows**

1. Go to the official download page:  
   👉 https://www.openwall.com/john/
2. Scroll down to the **"Windows binaries"** section.
3. Click the link:  
   🔗 John the Ripper 1.9.0-jumbo-1 for Windows (64-bit)  
   (This will download a ZIP file like john-1.9.0-jumbo-1-win64.zip)

**✅ Step 2: Extract the ZIP File**

1. Go to your **Downloads** folder.
2. Right-click the downloaded ZIP file (john-1.9.0-jumbo-1-win64.zip)
3. Select Extract All... → Choose a folder (or just extract to default).
4. It will create a folder like:

C:\Users\YourName\Downloads\john-1.9.0-jumbo-1-win64\

**Step 3 :** Create a Password-Protected ZIP File (Windows)

🔹 Step 1: Create a Sample Text File

Open Notepad

Write: This is a hello file

Save as: hello.txt (on Desktop or Downloads)

🔹 Step 2: Zip with Password (using 7-Zip)

Windows built-in ZIP doesn't support encryption, so use 7-Zip (free).

* Download 7-Zip (if not installed):

👉 https://www.7-zip.org/download.html

Create the ZIP with a password:

Right-click hello.txt

Click 7-Zip → Add to archive...

Choose:

Archive format: zip

Enter password: 54321 (or anything you want)

Encryption method: ZipCrypto (✅ simpler to crack)

Click OK

You now have a file like: **hello.zip** (with password)

Save this hello.zip file into the : **john-1.9.0-jumbo-1-win64/run/hello.zip**

**✅ Step 4: Locate the "run" Folder**

You can open Command Prompt directly in that folder:

Cmd

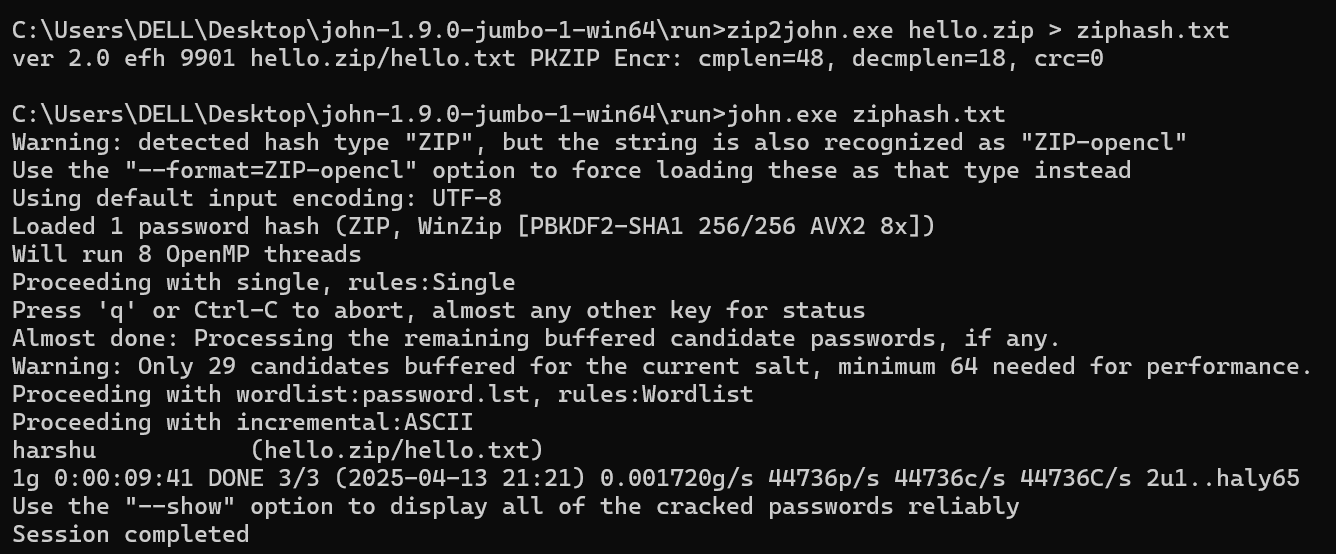
1. Open Command Prompt (Win + R, type cmd, press Enter)

**cd "C:\Users\YourName\Downloads\john-1.9.0-jumbo-1-win64\run"**

Step 5:Run the following command on the navigating directory

* **zip2john.exe secret.zip** > ziphash.txt (This extracts the hash into a file called ziphash.txt.)
* **john.exe ziphash.txt** (John will now try to crack the password using its built-in wordlist.)
* See the Cracked Password Once cracking is done, run:
* **john.exe --show ziphash.txt** ( hello.zip:$pkzip2$1\*2... → 54321)

**output :**



**Crack MD5 Hash with John the Ripper**

**Step 1: Prepare the Hash File**

1. Open **Notepad**.
2. Paste the following line:

* **user1:8a9eb6c3e80fbbcbf5fdf81576b7c4ab**
* **user2:63e4f94c3db440de94f104e7d0bedf7b**
* **user3:0091d2d7b1a72d5e3d21fa742538e17e**

1. Save it as:

* **hash.txt**

1. Place hash.txt inside the run folder of John the Ripper, for example:

* C:\Users\DELL\Downloads\john-1.9.0-jumbo-1-win64\run

**Step 2: Open Command Prompt**

1. Press Windows + R, type cmd, hit **Enter**.
2. Navigate to the John the Ripper "run" folder:

* **cd "C:\Users\DELL\Downloads\john-1.9.0-jumbo-1-win64\run"**

### Step 3: Crack the MD5 Hash

Run this command:

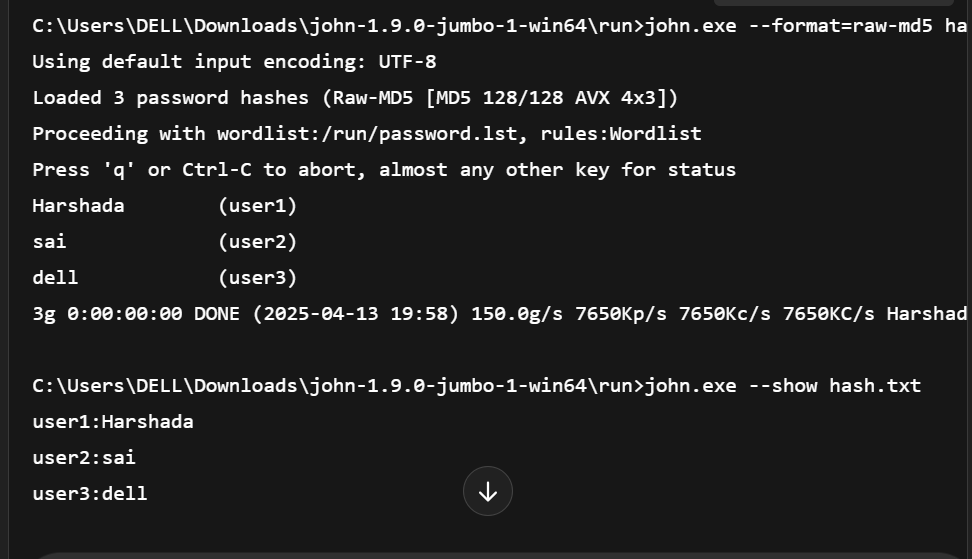
* **john.exe --format=raw-md5 hash.txt**

John will begin trying passwords to match the MD5 hash.

### View the Cracked Password

After it's done (or even during the process), run:

* **john.exe --show hash.txt**

****