Cain and Abel

Cain and Abel is a password recovery and hacking tool that was primarily used for network sniffing, cracking password hashes, and recovering passwords stored in Windows systems. It was popular in the cybersecurity community for penetration testing and ethical hacking but was also misused for malicious purposes.

Key Features of Cain & Abel:

1. Network Sniffing – Captures network packets to extract passwords transmitted over protocols like FTP, HTTP, and SMB.
2. Password Cracking – Uses dictionary attacks, brute force attacks, and cryptanalysis techniques to crack password hashes.
3. ARP Poisoning – Performs Man-in-the-Middle (MITM) attacks to intercept and manipulate network traffic.
4. Decoding Stored Passwords – Retrieves stored passwords from Windows, including those from browsers and network authentication.
5. VoIP Sniffing – Captures and decodes VoIP conversations.
6. Hash Cracking – Cracks password hashes from various sources using rainbow tables and other techniques.

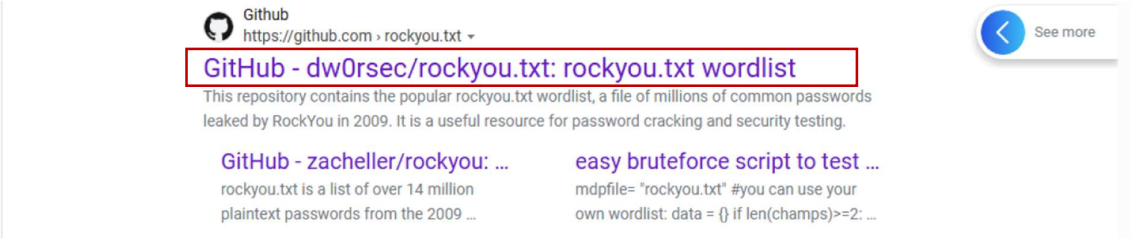
Cain & Abel has not been updated for many years, and it does not work properly on modern Windows systems due to security improvements. Additionally, most antivirus software flags it as malicious due to its hacking capabilities. I got it to run on windows 10 installed in VMware but had to shut down all the antivirus protection and firewall protection. So you shouldn't run it on your primary pc. Run it on a virtual machine.

Password Cracking

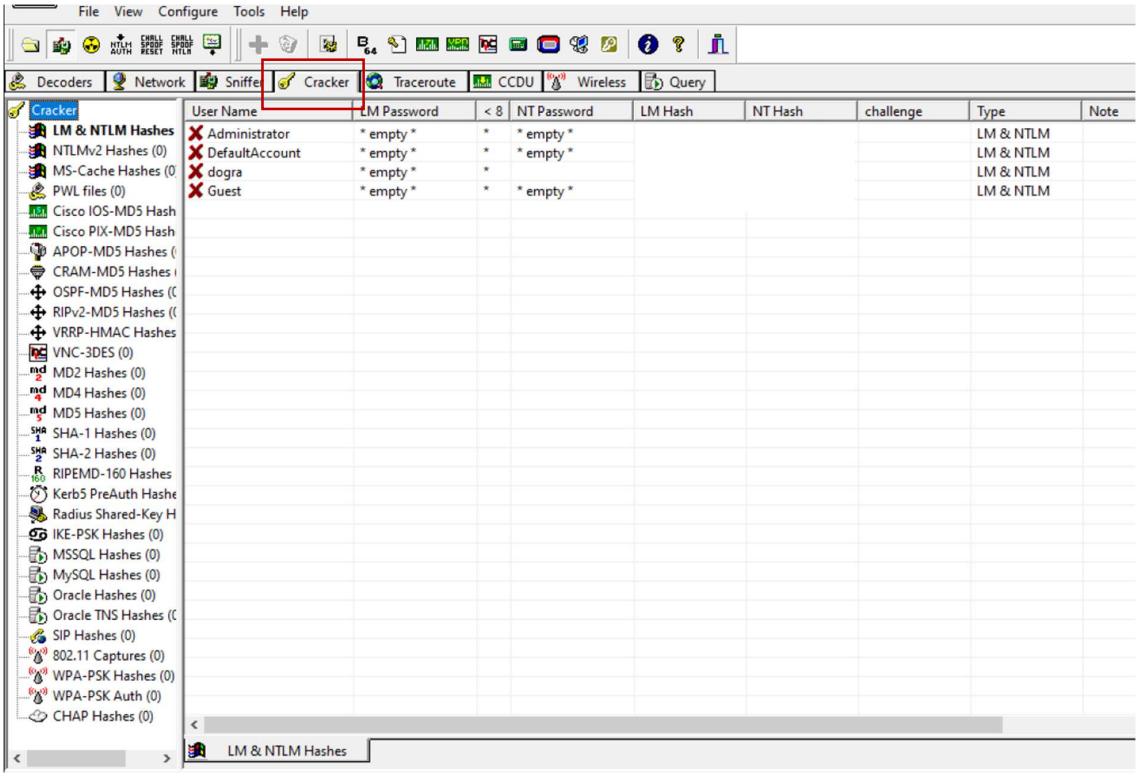
Cain & Abel supports multiple passwords cracking methods, including:

- Dictionary Attack (Uses wordlists of common passwords)
- Brute Force Attack (Tries all possible character combinations)
- Cryptanalysis (Uses precomputed hash tables like Rainbow Tables)

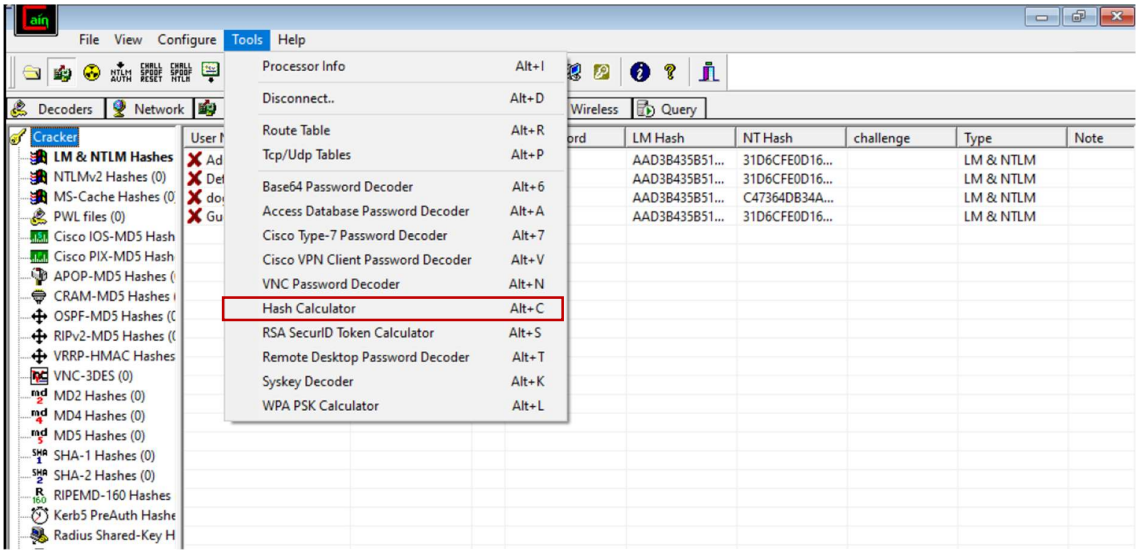
We will start with a dictionary attack. It uses a wordlist you can install rockyou.txt from GitHub and use it as a wordlist for your dictionary attack.



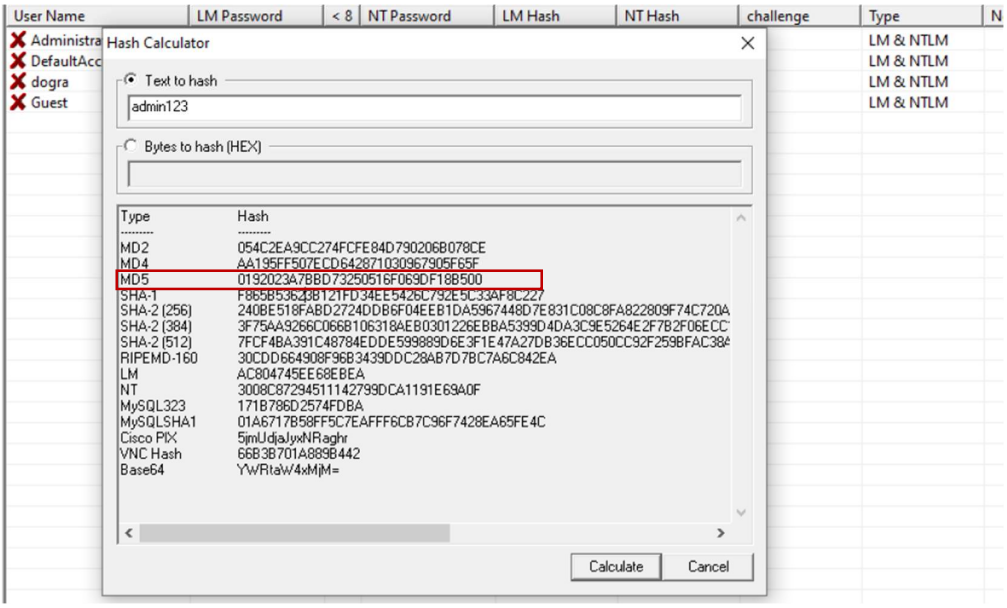
Start Cain and Abel and move to the Cracker tab. On the left hand side you will see all the available hashes that we can crack. Select any one of them.



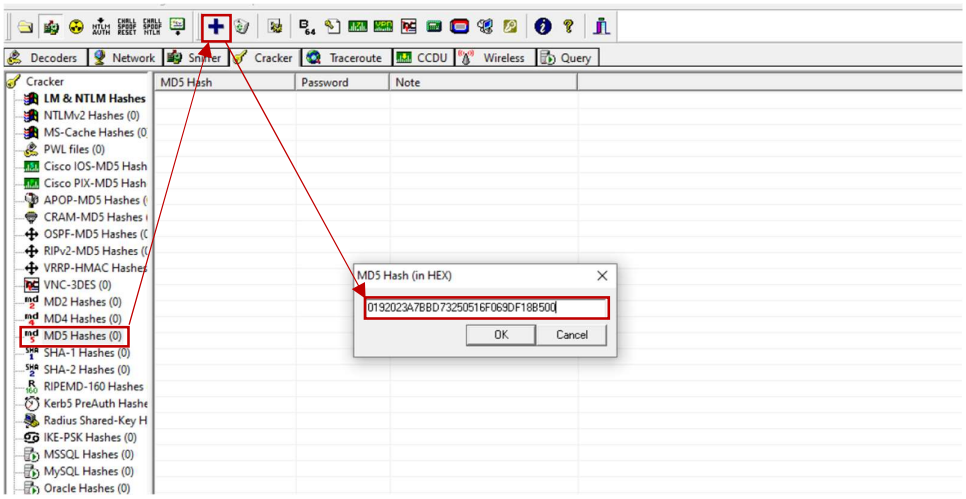
But first to break a hash we need one. You can create one for testing using cain and abel.



Step 1. In Tools select Hash Calculator and enter the text you want to hash. It will give you the hashed text using various hashing techniques. Copy any one of them you wish to crack. For this example, I have chosen the MD5 hash.



Step 2. On the left tab in Cracker Select MD5 hashes and then click on the add button to add the md5 hash you want to crack. Enter the md5 hash in the dialog box.

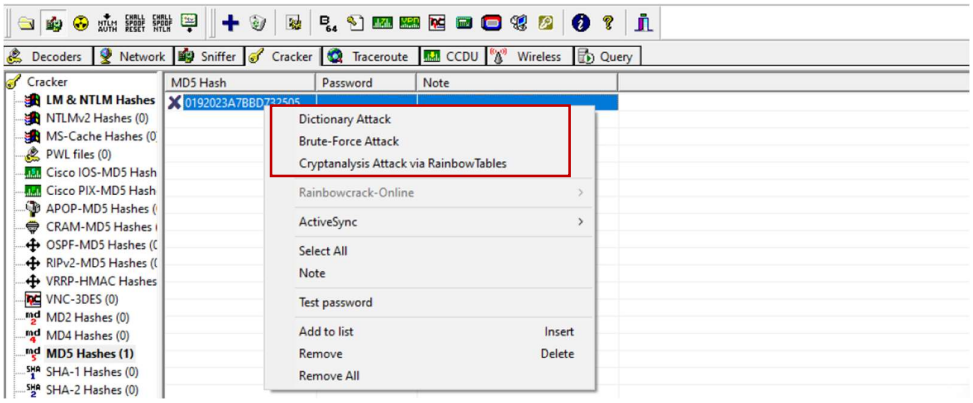


Step 3. The password will now be loaded on MD5. Right click on the hash and a dialog box will appear. You can select one of the three attacks.

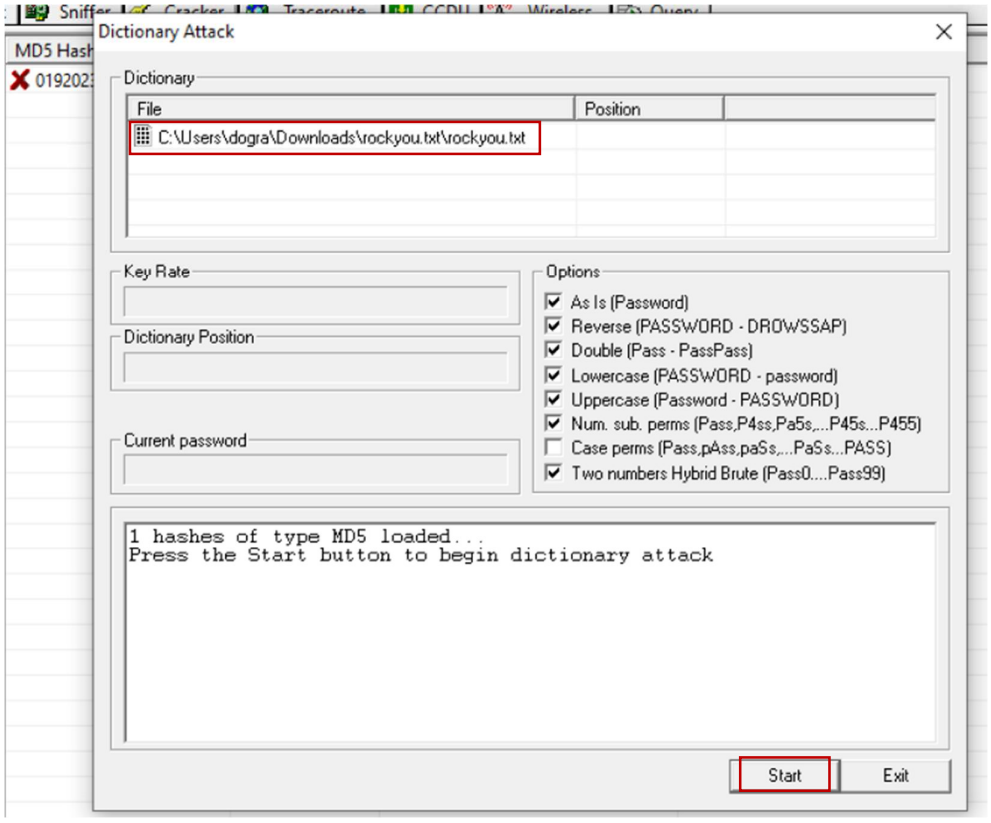
Dictionary Attack: A dictionary attack uses a predefined list of common passwords to guess the correct one. It is fast but ineffective against strong, unique passwords. Hackers rely on wordlists like "rockyou.txt" for cracking.

Brute Force Attack: A brute force attack systematically tries every possible character combination until the correct password is found. Though slow, it can eventually crack any password if given enough time and computing power.

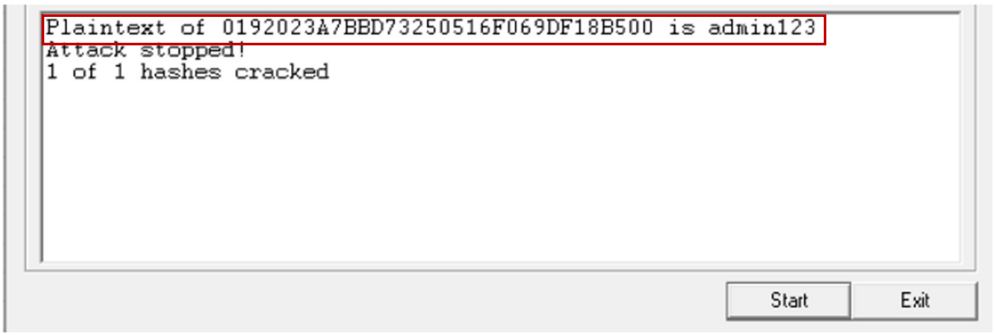
Cryptanalysis Attack: A cryptanalysis attack exploits weaknesses in encryption algorithms to reverse-engineer passwords instead of guessing them. Methods like rainbow tables allow rapid cracking of weakly hashed passwords without brute-force attempts.



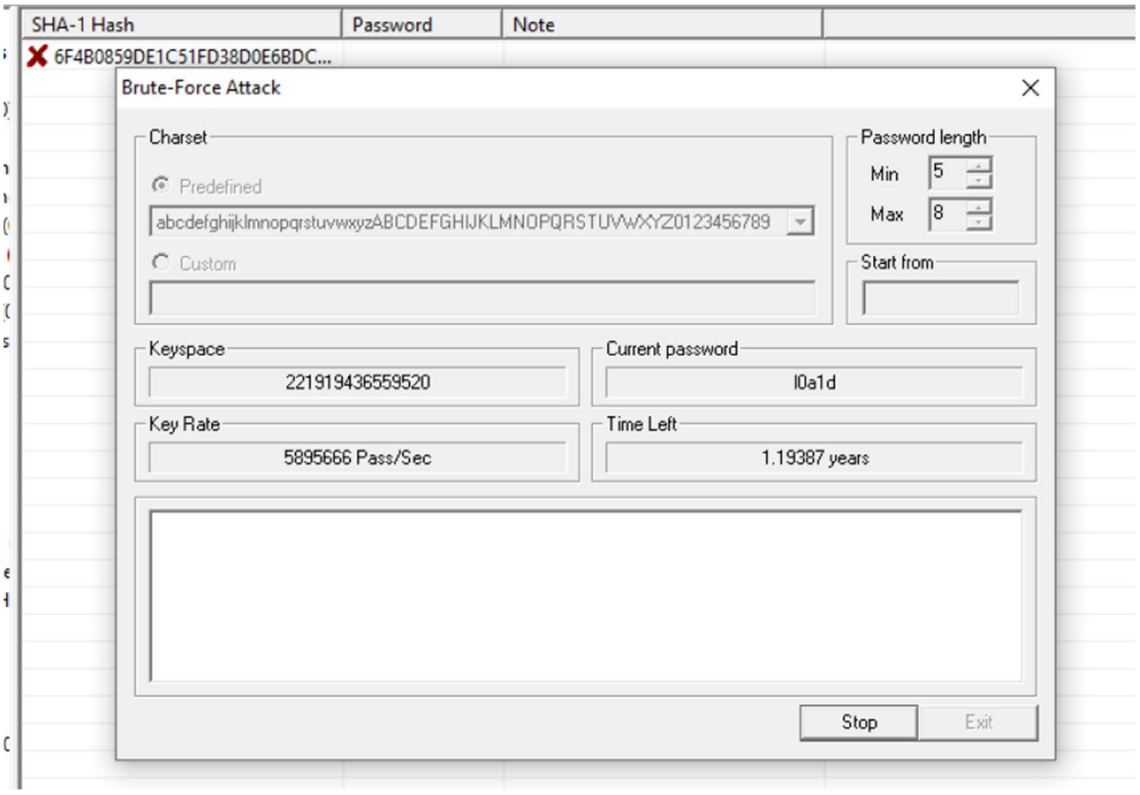
Step 4. We will start with the dictionary attack. Lets choose rockyou.txt as the wordlist for this attack and run it.



Step 5. Voila! The password is cracked and we have the plaintext now.



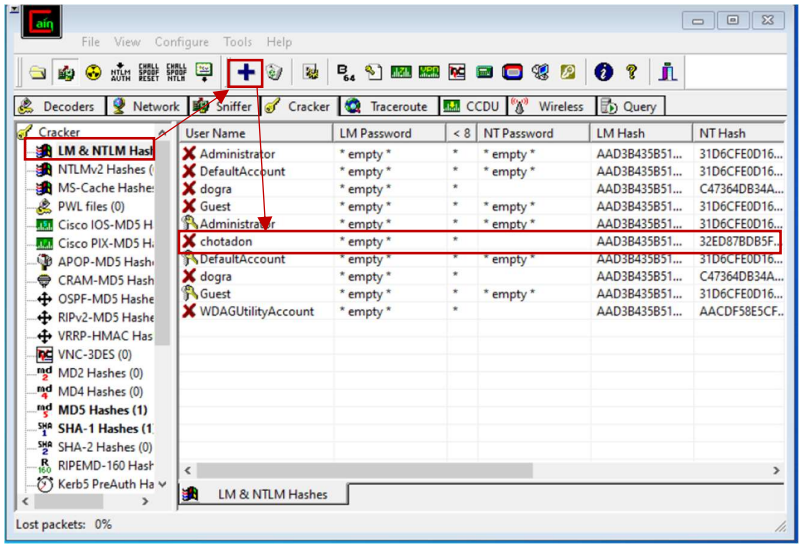
We can also run the Brute force and the cryptanalysis attack in the same manner.



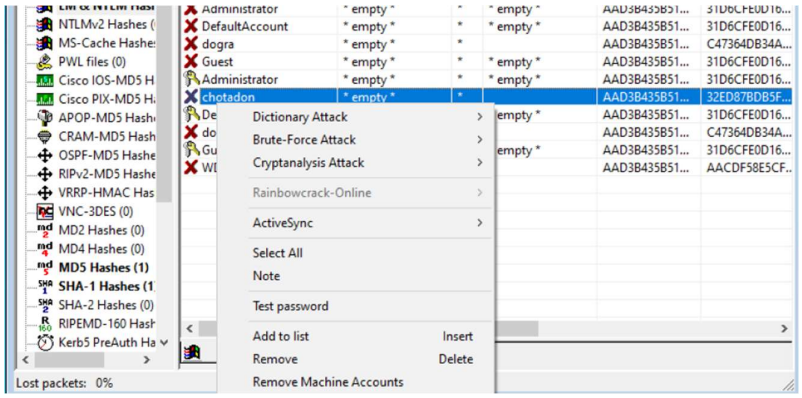
You can select different predefined as per the information we have gathered on the password. Lowercase, Uppercase, Numeric, Alphanumeric or combination of one or more or all. It also displays the current password, Key rate, Key space and Time left. Unfortunately, I can't wait 1.19 years to show you the cracked password.

NTLM Hashes

NTLM (NT LAN Manager) hashes are cryptographic representations of passwords used in Windows authentication. They are commonly found in legacy Windows environments and can be exploited if not properly secured. You can crack them by going to the NTLM hash in the cracker tab. Click on the add button and you can choose import hashes from the local system that means retrieving or loading cryptographic hash values (such as NTLM hashes) that are stored on a computer. After selecting that you will see all the available accounts on the local system. Empty here means a password has not been set for the account. A blank value means a password is associated with the account but has yet not been cracked. You can crack the password using the same steps as before.



For this example, we will be cracking password for the account chotadon. We will be using Brute force attack for this.



I chose numbers only in the predefined to reduce time. I already knew the password has only numbers in it. Voila! The password has been cracked.