At Datarecovery.com, we frequently recover lost passwords for everything from Word documents and RAR files to encrypted Linux volumes (LUKS encryption) and Bitcoin wallets. Our customers often ask about our methods; do we simply try every possible password, or is there more to it?

To put it simply: There’s more to it. Password recovery services require a solid understanding of the various possible password cracking methods used in modern cryptography. Our engineers work with our clients to choose an appropriate methodology, then use dedicated equipment to complete the crack as efficiently as possible.

Some of the common password cracking methods used by software password cracker tools [such as hashcat](https://hashcat.net/hashcat/) are listed below. For more information or to discuss password recovery services, call 1-800-237-4200 to speak with a specialist.

**Brute-force attack –** A brute-force attack exhaustively tries every possible combination of letters, numbers, and symbols to crack a password. It’s the simplest way to crack a password, but also the most ineffective, since it wastes a lot of time making unlikely guesses.

Most types of encryption effectively prevent a brute-force attack by using hashing algorithms to slow down password entry. Longer passwords can also defeat this technique. For example, a brute-force attack might take 5 minutes to crack a 9-character password, but 9 hours for a 10-character password, 14 days for 11 characters, and 3.9 years for 12 characters.

While we have specialized hardware that allows for extremely fast brute-force cracking, this technique is rarely effective.

**Dictionary attack**– The name says it all: A dictionary attack enters every word in a dictionary as a password. This removes some of the randomness of a brute-force attack, reducing the amount of time needed to find the password—provided that the password is in the dictionary, of course.

Note that “dictionary” doesn’t literally refer to a simple English dictionary; the entries in a cryptography dictionary may include common substitutions (for instance, “4pple” for “apple”) and numeric entries.

A common example is a rainbow-table attack. A rainbow table is essentially a dictionary optimized for common hash values as well as passwords. A rainbow-table attack is, therefore, a dictionary attack, but with a specialized dictionary optimized for the cracking attempt.

**Combinator attack**– This attack appends dictionary entries to other dictionary entries. It’s effective because users often choose passphrases that combine a few common, easy-to-remember phrases, for instance “password123.”

Let’s say that the dictionary for a combinator attack has the words “dog” and “cat.” The combinator would try “dogcat” and “catdog” as possible passwords. A combinator attack can be extraordinarily effective at cracking user-generated passphrases, but it’s not too effective for cracking machine-created passphrases.

**Fingerprint attack**– This is a fairly new type of attack, and its method is fairly sophisticated. It breaks possible passphrases down into “fingerprints,” single- and multi-character combinations that a user might choose. For the word “dog,” the technique would create fingerprints including “d,” “o,” “g,” along with “do,” and “og.”

This can be an especially effective attack when a user remembers part of a password. However, due to its sophistication, it requires extraordinary computing power.

**Hybrid attack –**This is a blend of a dictionary and a brute-force attack. It makes a dictionary attack stronger by placing a string of brute-force characters to the beginning or end of the dictionary entries.

For instance, “software” might be appended with “software001,” “software002,” “001software” and so on.

**Mask attack –** Similar to a brute-force attack, but with rules to reduce the number of errant entries. It’s extremely useful if some of the characters are known, or if character types are known. For instance, if a user knows that his password has a capital letter at the beginning and three numbers at the end, the mask attack would be far more effective than a simple brute-force attack. The masks are often generated by the password cracker.

**Permutation attack –** A permutation attack uses a dictionary, but each entry in the dictionary also generates permutations of itself. For the word “dog,” a permutation attack would create the candidates “god,” “ogd,” “odg,” “gdo,” and “dgo.”

**PRINCE attack –**Stands for “PRobability INfinite Chained Elements.” The PRINCE attack uses an algorithm to try the most likely password candidates with a refined combinator attack. It creates chains of combined words by using a single dictionary.

**Rule-based attack –** As the name implies, a rule-based attack uses rules to eliminate possibilities. It’s one of the more complex types of attacks, but the possibilities are effectively endless. A password recovery engineer could create any criteria necessary to weed out unlike or impossible guesses.

**Table-Lookup attack –** Each word in a dictionary generates masks for a mask attack while creating new words by consulting a table. Simply put, it’s effective for guessing passwords when the user replaced one or more characters with numbers or symbols (for instance, “m$ney” instead of “money”).

**Toggle-Case attack –**This attack creates every possible case combination for each word in a dictionary. The password candidate “do” would also generate “Do” and “dO.”

If you’ve lost your password or if you need access to an encrypted file that you legally own, Datarecovery.com can help. Call us at 1-800-237-4200 to get started.