

ÇEVİRİMDİŞİ PAROLA KIRMA SALDIRILARI

DÜZGÜN KÜÇÜK

İçindeki Saldırı Türler

Kişiyeye Özel Parola Listesi, Kaba Kuvvet, Rainbow Table

1) KİŞİYE ÖZEL PAROLA LİSTESİ

I. Parola Listesinin Oluşturulması

Kullanılan Araç: Cupp Tool

- Cupp aracı komut satırında çalışmaktadır. Bu aracın amacı hedef kişiye özel olarak parola listesi üretmektir.

Kullanımı:

```
[mazlum@mazlum-virtualbox]--(/TOOLS/cupp)
$python cupp.py -i

cupp.py!
# Common
# User
# Passwords
# Profiler

[ Muris Kurgas | j0rgan@remote-exploit.org ]
[ Mebus | https://github.com/Mebus/ ]

[+] Insert the information about the victim to make a dictionary
[+] If you don't know all the info, just hit enter when asked! ;)

> First Name: düzgün
> Surname: küçük
> Nickname:
> Birthdate (DDMMYYYY): 10102010

> Partners) name:
> Partners) nickname:
> Partners) birthdate (DDMMYYYY):

> Child's name:
> Child's nickname:
> Child's birthdate (DDMMYYYY):

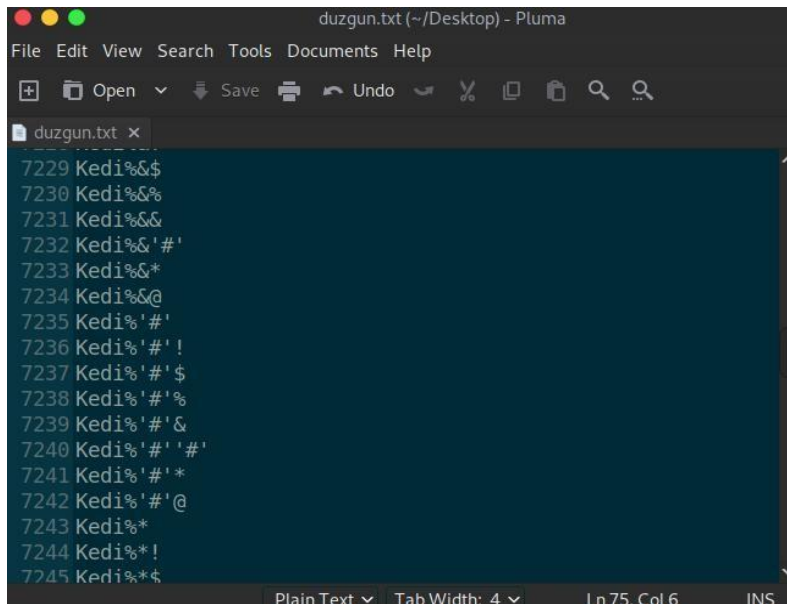
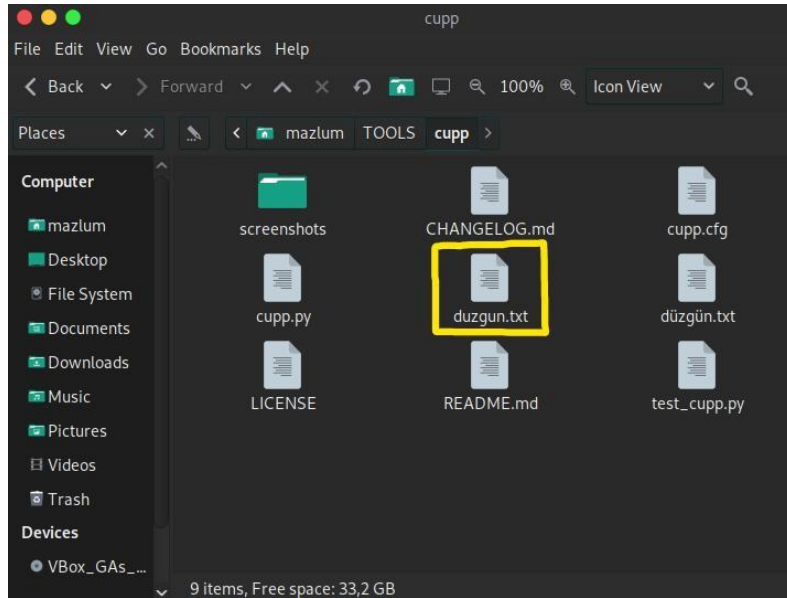
> Pet's name: kedi
> Company name: ABM
```

- Aracın yüklendiği klasöre gidip **python3 cupp -i** komutuyla araç çalıştırılır.
- Aracın girdileri üstte bulunan ekran görüntüsünde görünmektedir.

```
> Do you want to add some key words about the victim? Y/[N]: y
> Please enter the words, separated by comma. [i.e. hacker,juice,black], spaces will be removed: duzgun, Besiktas, 1903, Elazığ, Elazığ23
> Do you want to add special chars at the end of words? Y/[N]: y
> Do you want to add some random numbers at the end of words? Y/[N]:y
> Leet mode? (i.e. leet = 1337) Y/[N]: y

[+] Now making a dictionary...
[+] Sorting list and removing duplicates...
[+] Saving dictionary to duzgun.txt, counting 15866 words.
> Hyperspeed Print? (Y/n) : n
[+] Now load your pistolero with duzgun.txt and shoot! Good luck!
mazlum@mazlum-virtualbox [-~/TOOLS/cupp]
```

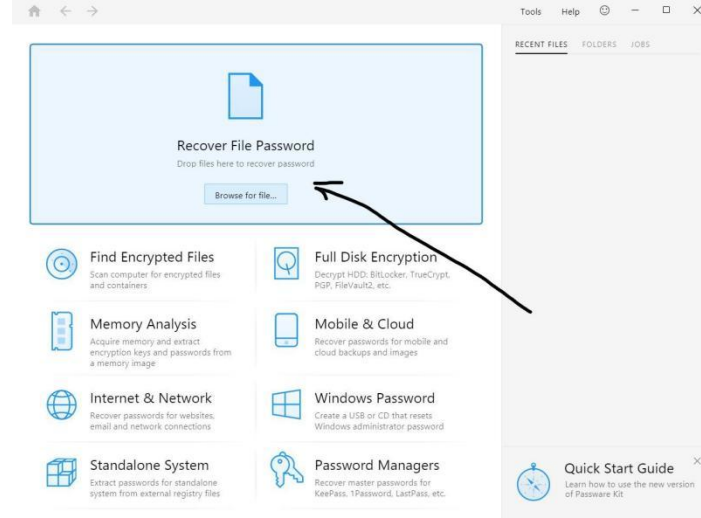
- Ana girdilerden sonra araç bize daha ayrıntılı ayarlar yapma imkanı da sunmaktadır.
- 5. satırda bulunan “leet mode” harflere benzeyen rakamların benzetildikleri harfler yerine kullanılmasıdır. Örnek: ARABA = 4R4B4
- Tüm ayarları yaptıktan sonra 15866 paroladan oluşan duzgun adında bir liste verdi. Liste aracın bulunduğu dizine kaydedilmektedir.



II. Oluşturulan Parola Listesini Bir Programa Aktararak Saldırma

Kullanılan Program: Passware

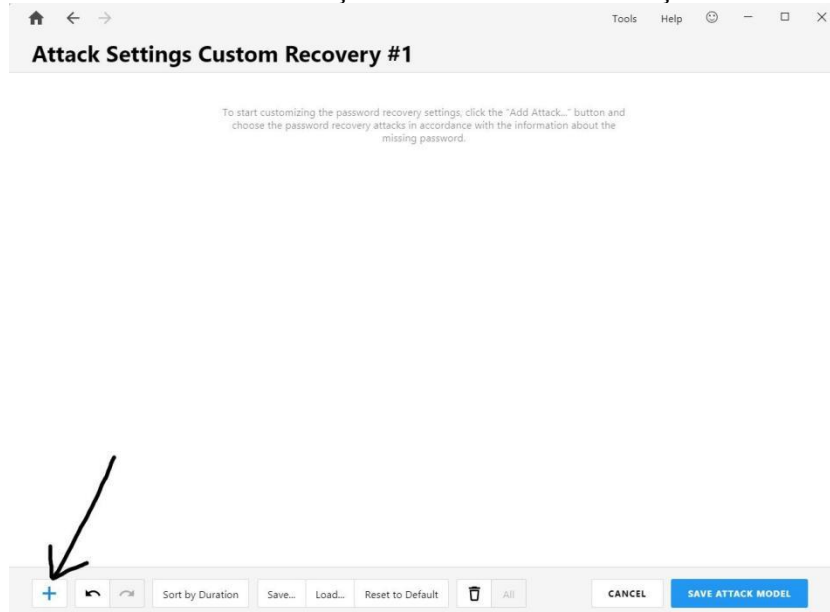
- Şifrelenmiş dosyayı belirtilen alana sürüklenebilir veya belirtilen alana tıklayıp açılan pencereden seçilebilir.



- Dosya seçildikten sonra önceden hazırladığımız listeyi eklemek için atarlara tıklamalıyız.



- Açılan bölüde saldırı eklemek için sol altta bulunan artı işaretine tıklanmalı.



- Açılan pencerede sözlük kısmına tıklayıp en altta bulunan seçenek seçilmeli.

BASIC ATTACKS

- Dictionary
- Xieve
- Brute-force
- Mask
- Known Password/Part
- Previous Passwords

GROUPS

- Join Attacks
- Append Attacks

New Dictionary Attack

Dictionary Attack checks thousands of words from dictionary files as possible passwords. Every word from the dictionary is tested in a variety of modifications according to the current attack settings.

SETTINGS

Length: 1 to 128 characters

Dictionary: English: 134,925 passwords

Pattern:

MODIFIERS

+ Change case

Substitute chars

Sample passwords: 3!42Å±9!!*! · 3!42Å±9_2001 · El42Å±9%*#! · ElazÅ±q_1990 · elazÅ±q_20...

Passwords to check: 134,925

Complexity: *****

CANCEL ADD ATTACK

- Karşımıza Programın kendi bünyesinde bulunan parolal isteleri geldi. Kendi listemizi eklemek için sol alttaki seçenek seçilmeli ve açılan pencereden dosya arama kısmına tıklayıp parola listesi seçilmeli.

Dictionary Manager

NAME	DESCRIPTION	SIZE
Dutch	Built-in Dutch dictionary	1013.0 KB
English	Built-in English dictionary	528.63 KB
Estonian	Built-in Estonian dictionary	537.45 KB
Finnish	Built-in Finnish dictionary	338.03 KB
French	Built-in French dictionary	453.17 KB
German	Built-in German dictionary	622.42 KB
Greek	Built-in Greek dictionary	1.07 MB
Irish	Built-in Irish dictionary	1.07 MB
Italian	Built-in Italian dictionary	711.35 KB
Polish	Built-in Polish dictionary	1.01 MB
Portuguese	Built-in Portuguese dictionary	288.53 KB
Romanian	Built-in Romanian dictionary	3.66 MB
Russian	Built-in Russian dictionary	526.86 KB
Slovenian	Built-in Slovenian dictionary	1.54 MB
Spanish	Built-in Spanish dictionary	833.43 KB
Swedish	Built-in Swedish dictionary	428.42 KB
ppr.dic	...	2.04 MB

Compile Dictionary from File

Source file: Click to choose or drag file here Browse...

☐ This file is a binary memory image

☐ Keep the original order of words

Skip words: ☐ shorter than 1 chars ☐ longer than 128 chars ☐ that aren't: English

NEXT

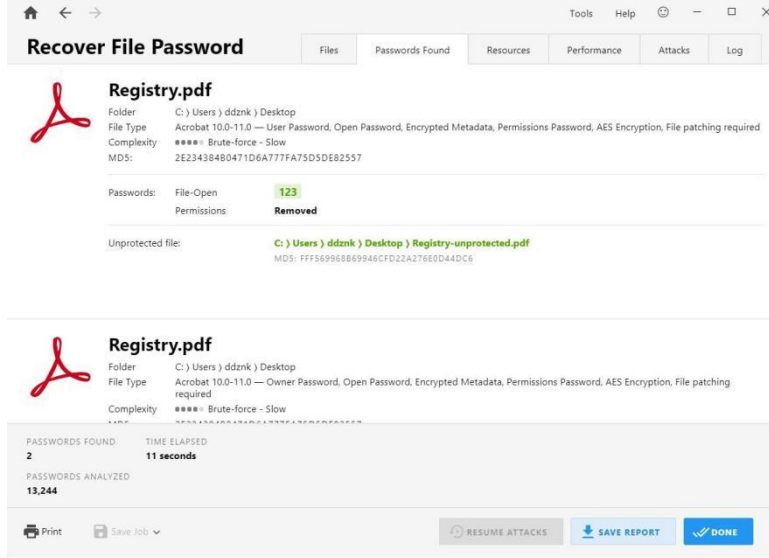
ADD DICTIONARY... *** DONE

- Geri geldiğimizde saldırı türleri arasına seçtiğimiz listenin dail olduğu görülmekte.

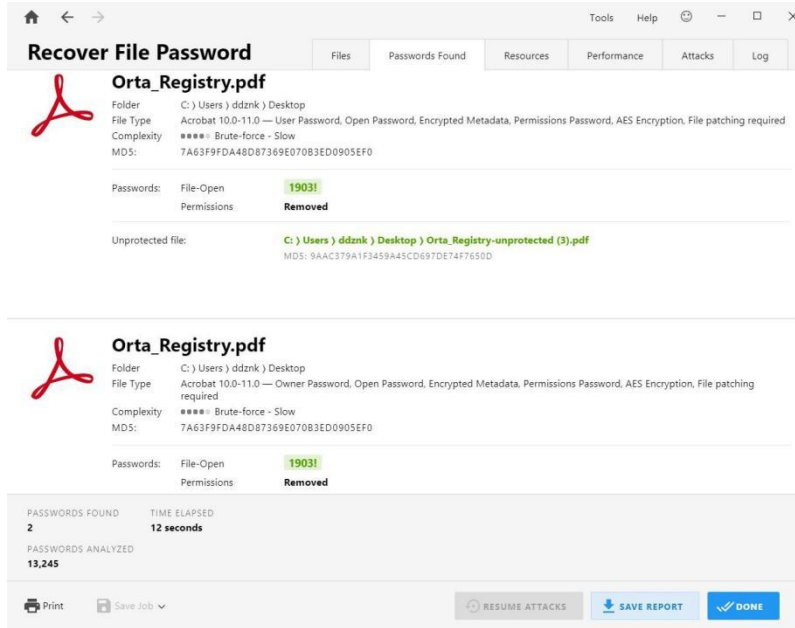


Örnekler:

A) Kolay Parola: 123



B) Orta Düzey Parola: 1903!



C) Zor Parola: B351k745!

The screenshot displays the 'Recover File Password' application window. The interface includes a top navigation bar with 'Tools', 'Help', and window controls. Below this is a tabbed interface with 'Files', 'Passwords Found', 'Resources', 'Performance', 'Attacks', and 'Log'. The 'Files' tab is active, showing details for 'Zor-Registry.pdf'. The file is located at 'C:\Users\ddznk\Desktop' and is an 'Acrobat 10.0-11.0' PDF. The complexity is 'Brute-force - Slow'. The MD5 hash is 'A14737E8AE8C7D85A41315E4681C064D'. The 'Passwords' section shows 'File-Open' with the password 'B351k745!' and 'Permissions' as 'Removed'. Below this, the 'Unprotected file' is listed as 'C:\Users\ddznk\Desktop\Zor-Registry-unprotected.pdf' with MD5 'B4A7E086A289D732477C430B9A005D5F'. A second instance of the file details is shown below. At the bottom, a summary section indicates 'PASSWORDS FOUND: 2', 'TIME ELAPSED: 15 seconds', and 'PASSWORDS ANALYZED: 17,468'. The bottom bar contains 'Print', 'Save Job', 'RESUME ATTACKS', 'SAVE REPORT', and 'DONE' buttons.

Recover File Password

Zor-Registry.pdf

Folder: C:\Users\ddznk\Desktop
File Type: Acrobat 10.0-11.0 — User Password, Open Password, Encrypted Metadata, Permissions Password, AES Encryption, File patching required
Complexity: Brute-force - Slow
MD5: A14737E8AE8C7D85A41315E4681C064D

Passwords: File-Open: **B351k745!**
Permissions: **Removed**

Unprotected file: **C:\Users\ddznk\Desktop\Zor-Registry-unprotected.pdf**
MD5: B4A7E086A289D732477C430B9A005D5F

Zor-Registry.pdf

Folder: C:\Users\ddznk\Desktop
File Type: Acrobat 10.0-11.0 — Owner Password, Open Password, Encrypted Metadata, Permissions Password, AES Encryption, File patching required
Complexity: Brute-force - Slow
MD5: A14737E8AE8C7D85A41315E4681C064D

Passwords: File-Open: **B351k745!**
Permissions: **Removed**

PASSWORDS FOUND: 2
TIME ELAPSED: 15 seconds
PASSWORDS ANALYZED: 17,468

Print Save Job RESUME ATTACKS SAVE REPORT DONE

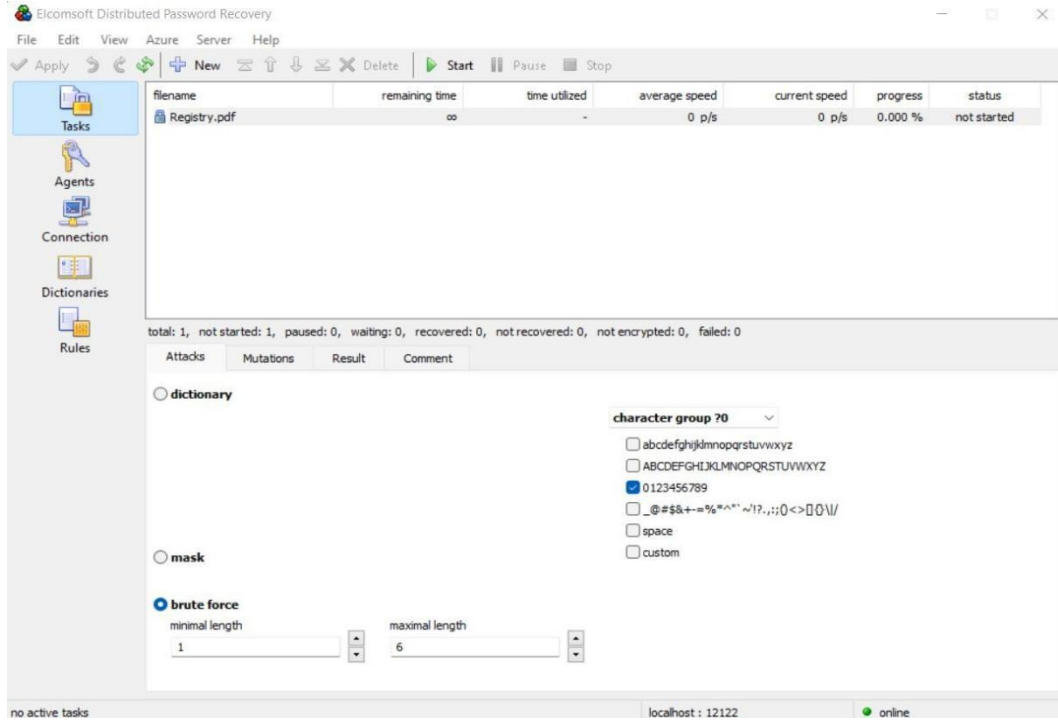
1) BRUTE FORCE

Deneme yanılma yoluyla belirlenen parola kombinasyonlarının teket teker şifrelenmiş dosya üzerinden denenmesidir.

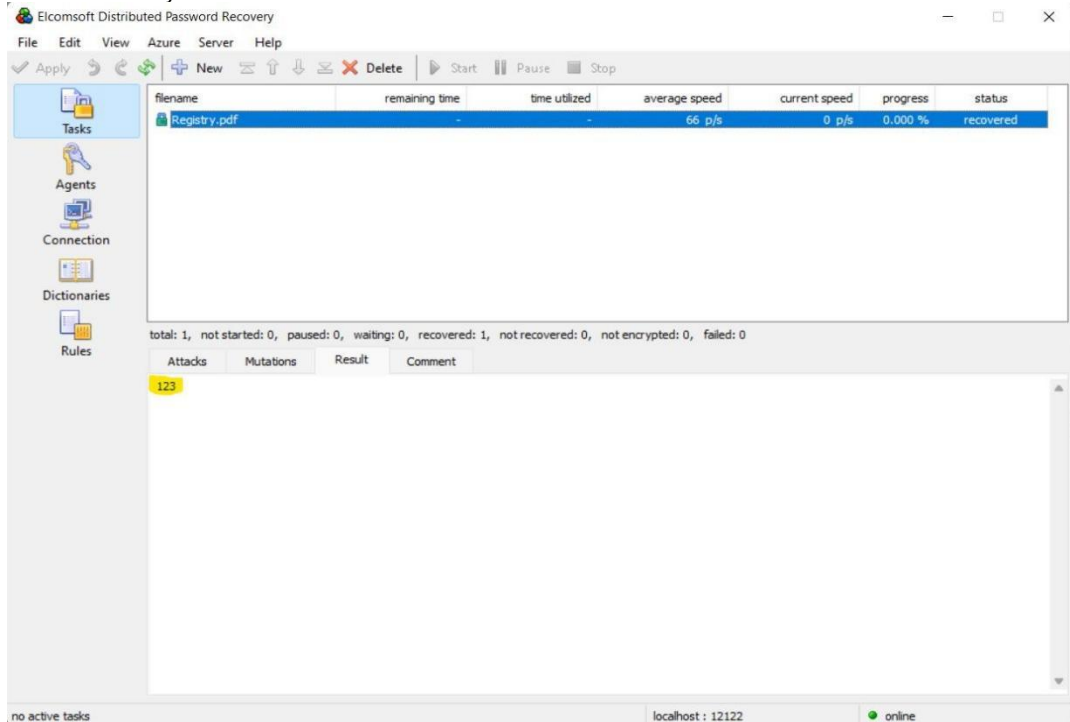
Örnekler:

A) Kolay Parola: 123

Kullanılan Program: Elcomsoft Distributed Password Recovery



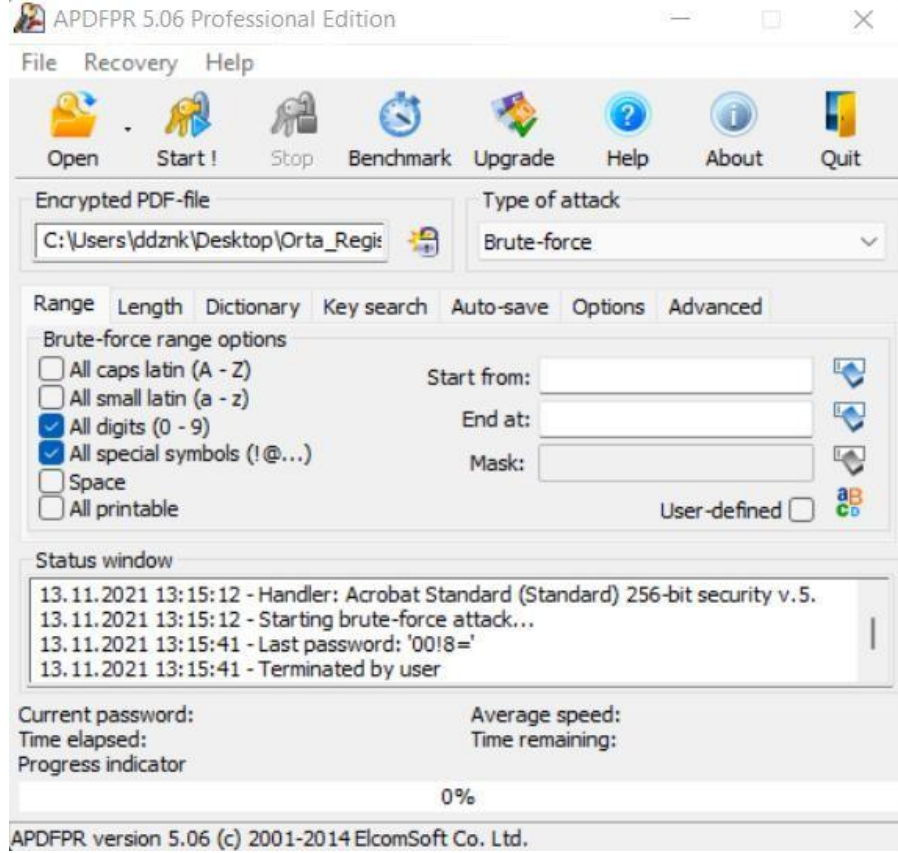
- Program menüsünün üst bölümünde “New” yazan kısma tıklayarak şifrelenmiş dosya programa eklenmektedir.
- Programın alt menüsünden “Attacks” kısmında saldırıyı düzenlemek için parola uzunluğu, parolaya dahil edilmesi istenilen karakterler ve saldırı tipi gibi ayarlar yapılabilir.
- İstenilen ayarlar yapıldıktan sonra üst kısımda bulunan “Start” butonuna tıklayıp saldırı başlatılabilir.



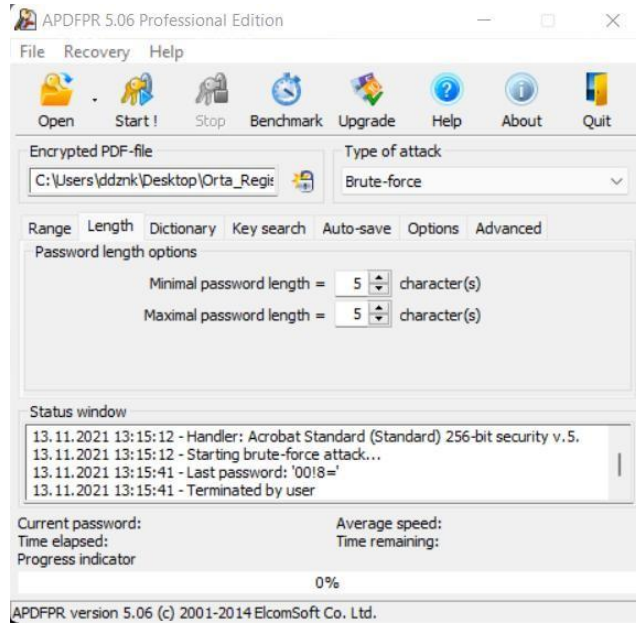
- Saldırı başarılı olduktan sonra “Result” kısmında bulunan parola değeri görünmektedir.

B) Orta Düzey Parola: 1903!

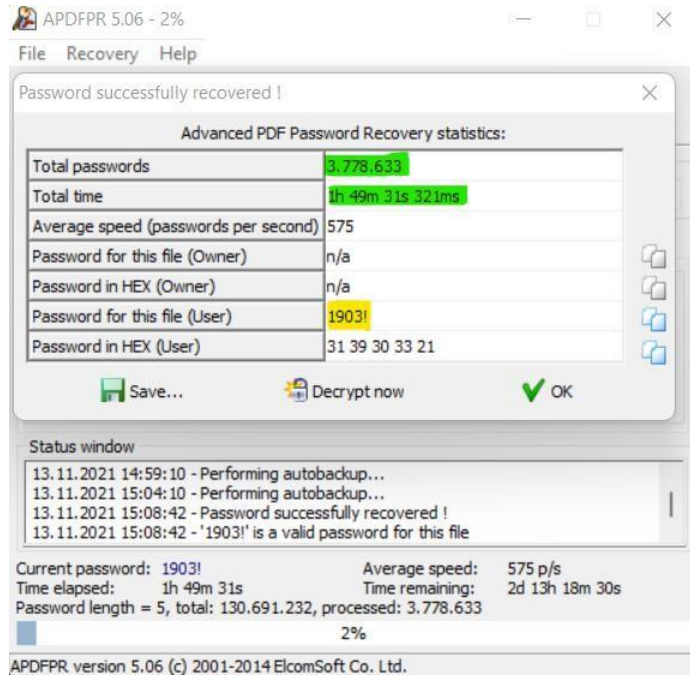
Kullanılan Program: Elcomsoft Advanced PDF Password Recovery



- Program menüsünün “Open” yazan kısmından şifrelenmiş dosya programa eklenmektedir.
- Programın “Range” yazan bölümünden saldırı için eklenecek karakterler, saldırının başlama noktası, saldırının bitiş noktası, maskeleyme ayarları yapılmaktadır.
- Programın “Length” bölümünden saldırıda kullanılacak parolaların uzunluğu belirlenebilir.

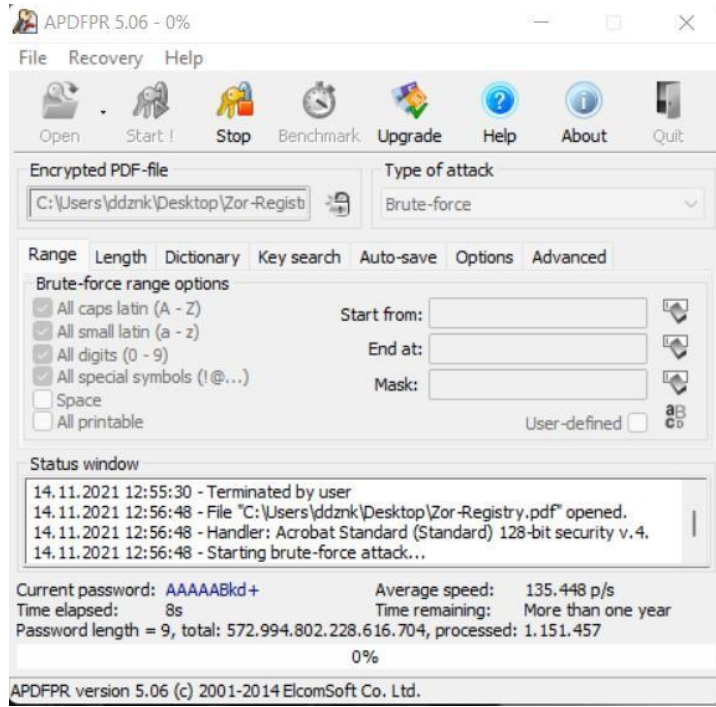


- Seçilen karakter uzayının büyüklüğüne ve parolada kullanılan karakter sayısına göre, parolanın kırılma süresi değişiklik göstermektedir. Ben parolayı kırarken sadece rakamlar ve özel karakterler kümesini seçtim. Max kırılma süresi 2 gün 15 saat civarı gösteriyordu ama benim parolamın başlangıç değeri “1” olduğu için 1 saat 49 dk gibi bir sürede bitti.

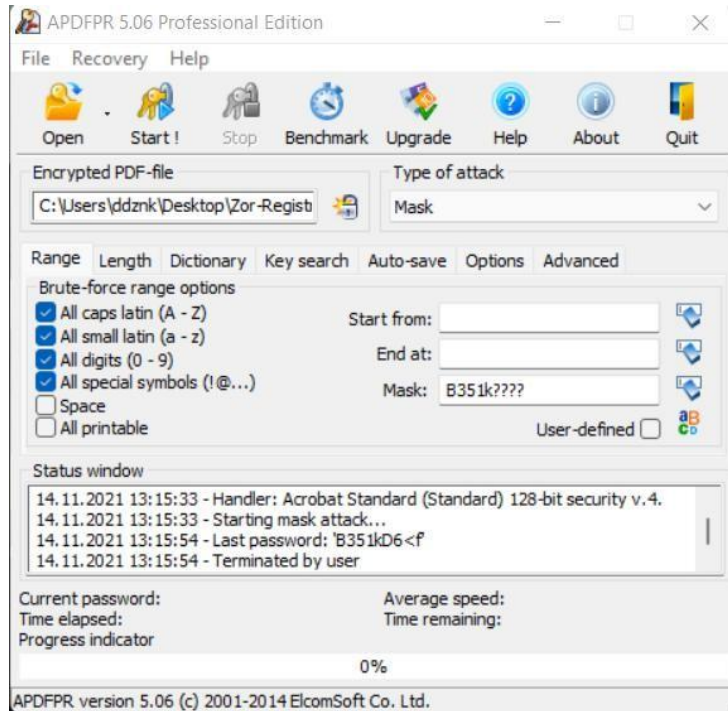


C) Zor Parola: B351k745!

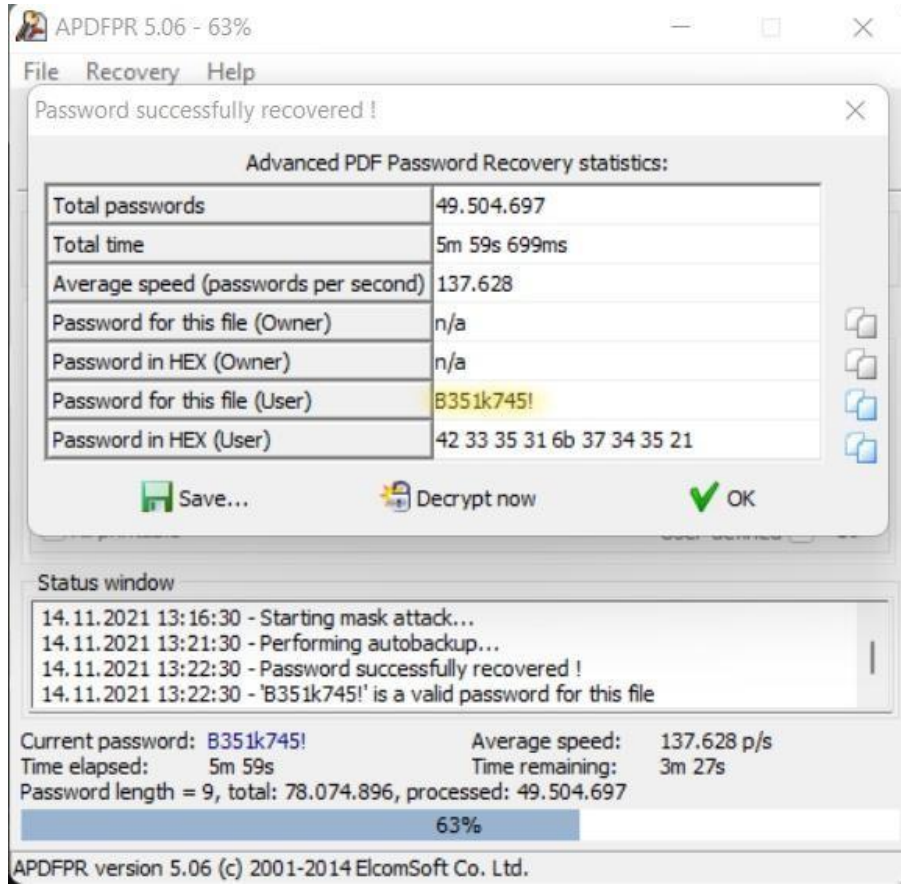
Not: Bu parolada büyük harf, küçük harf, rakam, özel karakter bulunmaktadır ve parola uzunluğu 9 karakter olduğu için tüm kümelerin seçilip karakter sayısını 9’a ayarladığımda parolanın kırılma süresi bir yıldan fazla olarak görüldü. Benim 1 yıl kadar bekleme gibi bir şansım olmadığı için “maskeleme” yöntemiyle parolayı kırdım.



Maskeleme: Eğer parolanın bazı karakterleri ve uzunluğu biliniyorsa bilinen karakterler yazılır, bilinmeyen karakterler yerine ise programın bilinmeyen karakter olarak atadığı karakterler yazılır. Bu bilinmeyen karakterler genellikle ? veya * karakterleridir.



- Parolanın ilk 5 karakterinin bilinip son 4 karakterinin bilinmediğini farzedip atağı başlattım.



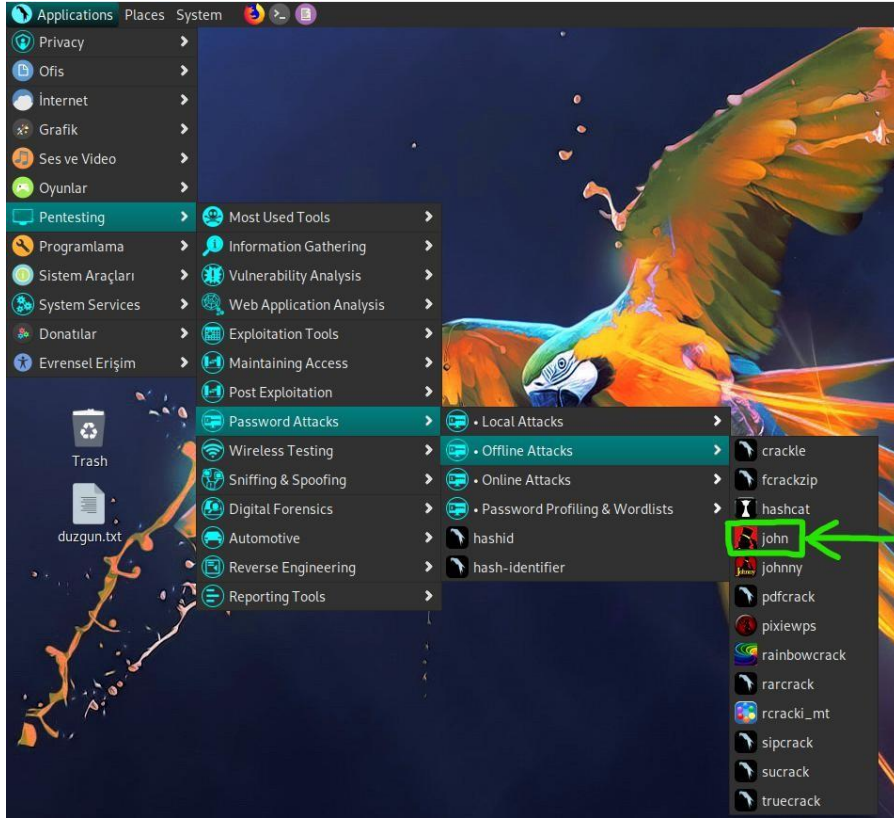
2) RAINBOW TABLE SALDIRISI

Rainbow Table Saldırısı: Bir tabloda parolaların düz halleri ve önceden hesaplanmış şifrelenmiş (hash alınmış) halleri bulunmaktadır. Saldırgan kırmak istediği hash değerini tabloda bulunan mevcut hash değerleri ile karşılaştırır ve eğer elindeki hash değeri ile tabloda bulunan herhangi bir hash değeri ile uyuşuyorsa o hash değerinin tablodaki karşılığı aranan paroladır.

I. Şifreli PDF Dosyasına Ait Hash Değerinin Hesaplanması

Kullanılan Program: John The Ripper

John The Ripper aracı komuta satırında çalışan bir araçtır ve çok fazla dosya yapısını desteklemektedir. Bu araç ile şifrelenmiş PDF dosyasının hash değeri alınabilmektedir.



- Kali Linux ve Parrot Linux içerisinde kendiliğinden kurulu olan bu araca Parrot üzerinden üst tarafta görülen şekilde erişmek mümkündür. Eğer bilgisayarda yüklü değilse GitHub üzerinden indirilebilir.
- Aracın desteklediği yapılar altta görüldüğü gibidir. Bize lazım olan **pdf2john.pl**'dir

```

(mazlum@mazlum-virtualbox) - [~/TOOLS/john/run]
$ls
1password2john.py      gelizjohn.py          office2john.py
7z2john.pl            genincstats.rb        openbsd_software2john.py
adxcsof2john.py       hccapx2john.py        openssl2john.py
aem2john.py           hexoraw.pl            oui.txt
aix2john.pl           htdigest2john.py     padlock2john.py
aix2john.py           hybrid.conf           pass_gen.pl
alnum.chr             ibmsscanner2john.py  password.lst
alnumspace.chr        ikescan2john.py      pcap2john.py
alpha.chr             ios7tojohn.pl         pdf2john.pl
andotp2john.py        itunes_backup2john.pl pem2john.py
androidbackup2john.py iwork2john.py         pfx2john.py
androidfde2john.py   john.bash_completion pgpdisk2john.py
ansible2john.py       john.conf             pgpsda2john.py
apex2john.py          john.zsh_completion  pgpwe2john.py
aplenotes2john.py    jtrconf.pm           pkcs12kdf.py
aruba2john.py         jtr_rulez.pm         potcheck.pl
ascii.chr             kdc2john.py          prosody2john.py
atmail2john.pl        keychain2john.py     pse2john.py
axcrypt2john.py       keyring2john.py      ps_token2john.py
benchmark-unify       keystore2john.py     pwsafe2john.py
bestcrypt2john.py     kirbi2john.py        radius2john.pl
bestcryptve2john.py  known_hosts2john.py  radius2john.py
bit-0039              korelogic.conf       regex_alphabets.conf
bitcoin2john.py       krb2john.py           relbench
bitshares2john.py    kwallet2john.py       repeats16.conf
bitwarden2john.py    lanman.chr            repeats32.conf
bks2john.py          lastpass2john.py     restic2john.py
blockchain2john.py   latin1.chr            rengen2rules.pl
ccache2john.py        ldif2john.pl          rules
cisco2john.pl         leet.pl              rulestack.pl
codepage.pl          lib                  sap2john.pl
cracf2john.py         libreoffice2john.py  sense2john.py
dashlane2john.py     lion2john-alt.pl     sha-dump.pl
deepsound2john.py    lion2john.pl          sha-test.pl
dictionary.rfc2865   lm_ascii.chr         signal2john.py
diqits.chr           lotus2john.py

```

```
$perl pdf2john.pl /home/mazlum/Desktop/kolay.pdf > /home/mazlum/Desktop/kolay_hash.txt
[mazlum@mazlum-virtualbox] ~/TOOLS/john/run
$perl pdf2john.pl /home/mazlum/Desktop/orta.pdf > /home/mazlum/Desktop/orta_hash.txt
[mazlum@mazlum-virtualbox] ~/TOOLS/john/run
$perl pdf2john.pl /home/mazlum/Desktop/zor.pdf > /home/mazlum/Desktop/zor_hash.txt
[mazlum@mazlum-virtualbox] ~/TOOLS/john/run
$
```

- Perl pdf2john.pl komutu sabit bir komuttur. “>” işaretinden önceki parametre şifreli dosyanın yolunu, sonraki parametre ise şifreli dosyadan elde edilen hash değerinin saklanacağı yeri göstermektedir.

Basit Parolaya Ait Dosyasının Hash Değeri

```
Parrot Terminal
File Edit View Search Terminal Help
1 /home/mazlum/Desktop/kolay.pdf:$pdf$5*6*256*~4*1*16*097e41018f503ba046621dab^
02e39ded*48*f092c3a03052790a74bb53f5c7018751a33568208e8b5c67d36264bc23323812
5beda9f3e7ba603b204e4d2ccf4bde9d*48*8f3b843a2954c152c7c725af92b2d8830fa45656
8977910b24a192fb136f578fd16420cba46e5a4560eef30c23a7019e*32*9b73e830ea1b01cc
124b9d33419ca1905c2c4ccafd798ceb17a05896363a199e*32*865e8de958b9b3151a92880d
02e57a46c355074a97d3b55dcdb4fc7549824e78
```

Orta Düzey Parolaya Ait Dosyasının Hash Değeri

```
Parrot Terminal
File Edit View Search Terminal Help
1 /home/mazlum/Desktop/orta.pdf:$pdf$4*4*128*~4*1*16*6bacba384bc0e0087c7af2061^
2154fee*32*fc244e39d53b54783f434ea5fb8d043028bf4e5e4e758a4164004e56ffa0108*
32*c6d22afcb1d73776d95e0b2e51f8c1340b324e7e045b94392b457cc7adf41839
```

Zor Parolaya Ait Dosyasının Hash Değeri

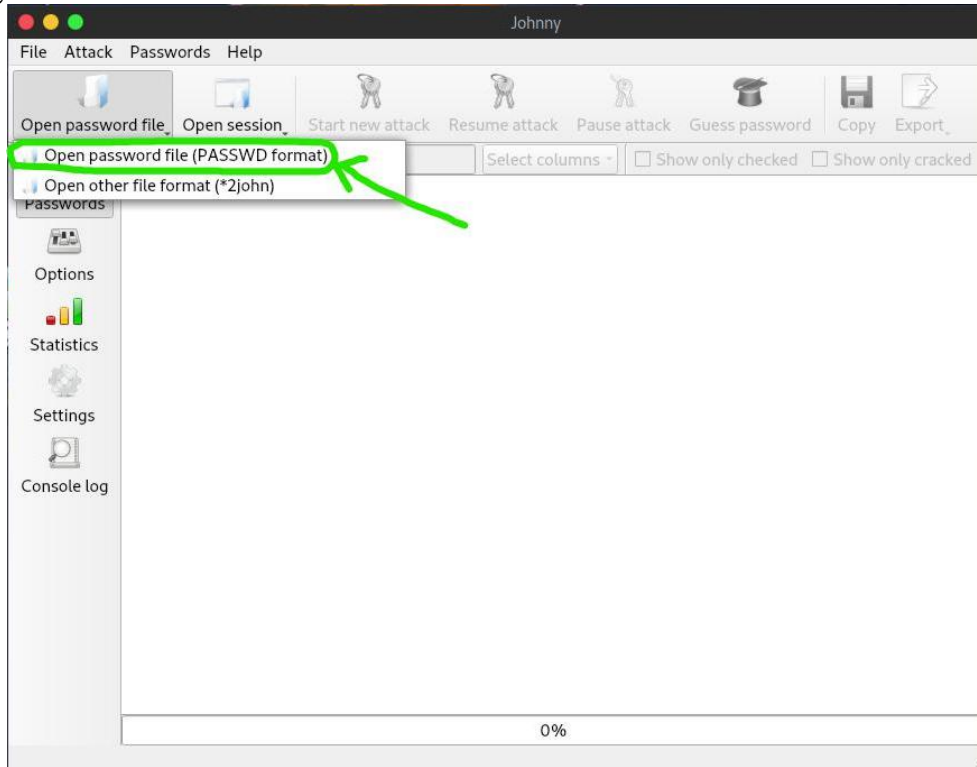
```
Parrot Terminal
File Edit View Search Terminal Help
1 /home/mazlum/Desktop/zor.pdf:$pdf$4*4*128*~4*1*16*d7638db8a34f25323871dd12bb^
938738*32*6f4a1d61675022290350f81b2169de1328bf4e5e4e758a4164004e56ffa0108*3
2*2ded03ffa3ab3bce941cc0007b89f00d59a676035adc8743a4e282acc38a09df
```

II. Hash Değerlerinin Kırılması

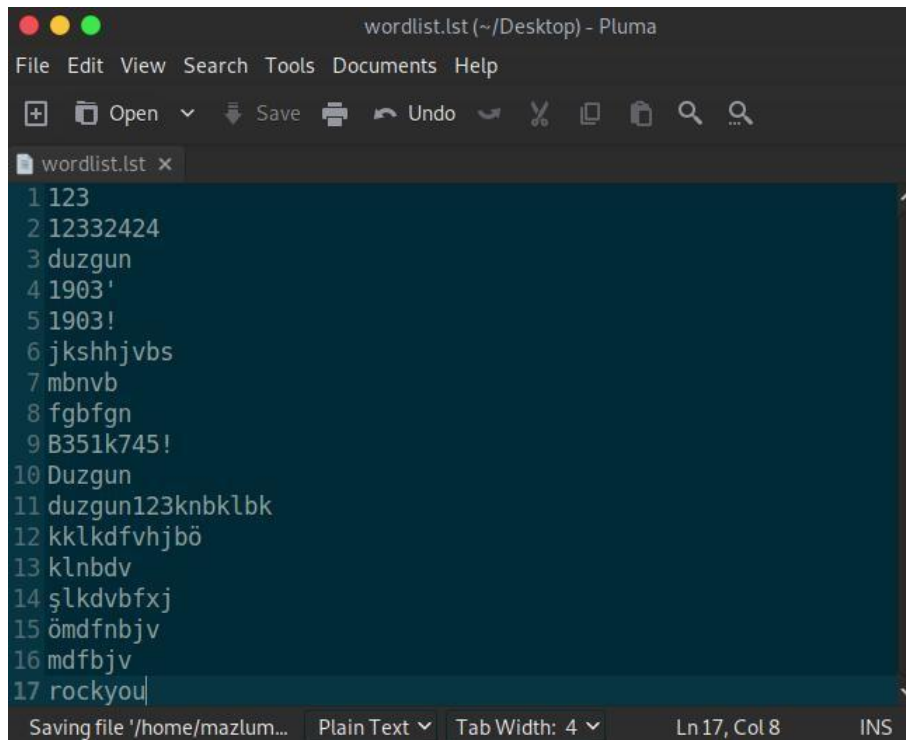
Kullanılan Program: Johnny

- Bu program John The Ripper aracının kullanıcı arayüze sahip halidir. Bu program üzerinden daha detaylı ve hızlı işlemler gerçekleştirilebilmektedir.

- Oluşturulan .txt dosyalarını programa eklemek için alt taraftaki görselde bulunan yol izlenmelidir.



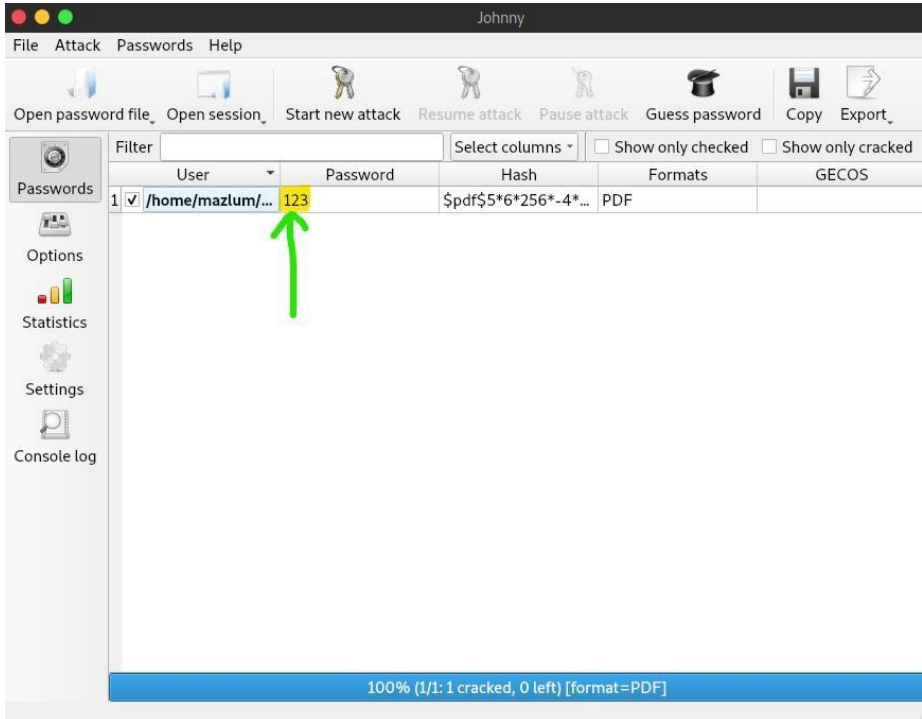
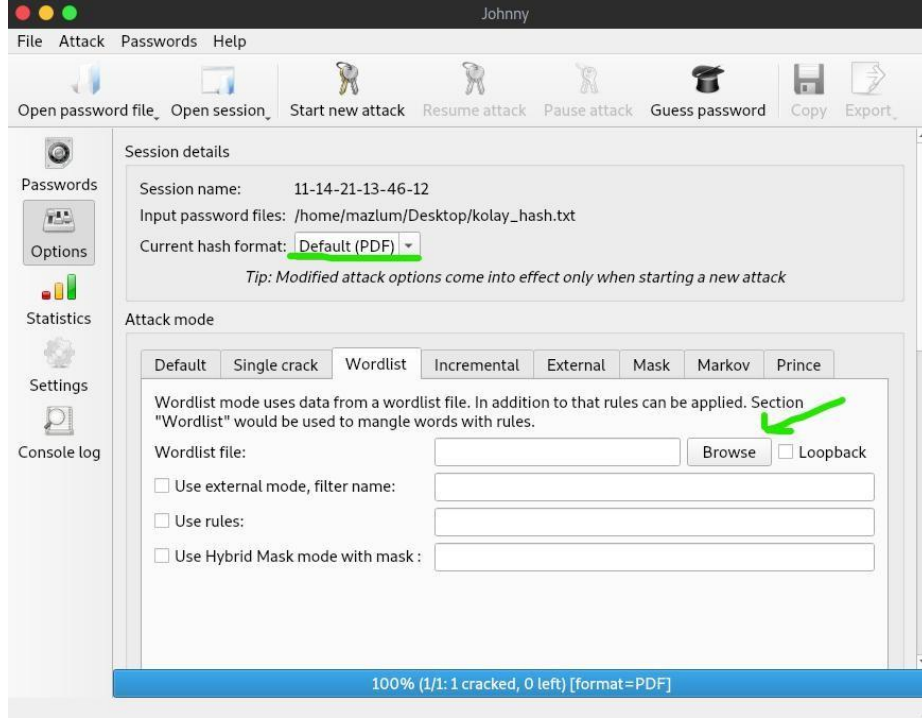
- Kırılmak istediğimiz dosya yüklendikten sonra sıra önceden hazırladığımız parola listesini programa yüklemekte. **Bu program, listede bulunan şifrelenmemiş parolaları saldırı sırasında şifreleyip hedef hash değeri ile karşılaştırma özelliğine sahiptir. Bunun için oluşturduğum listeye parolaların hash değerlerini eklemedim.**



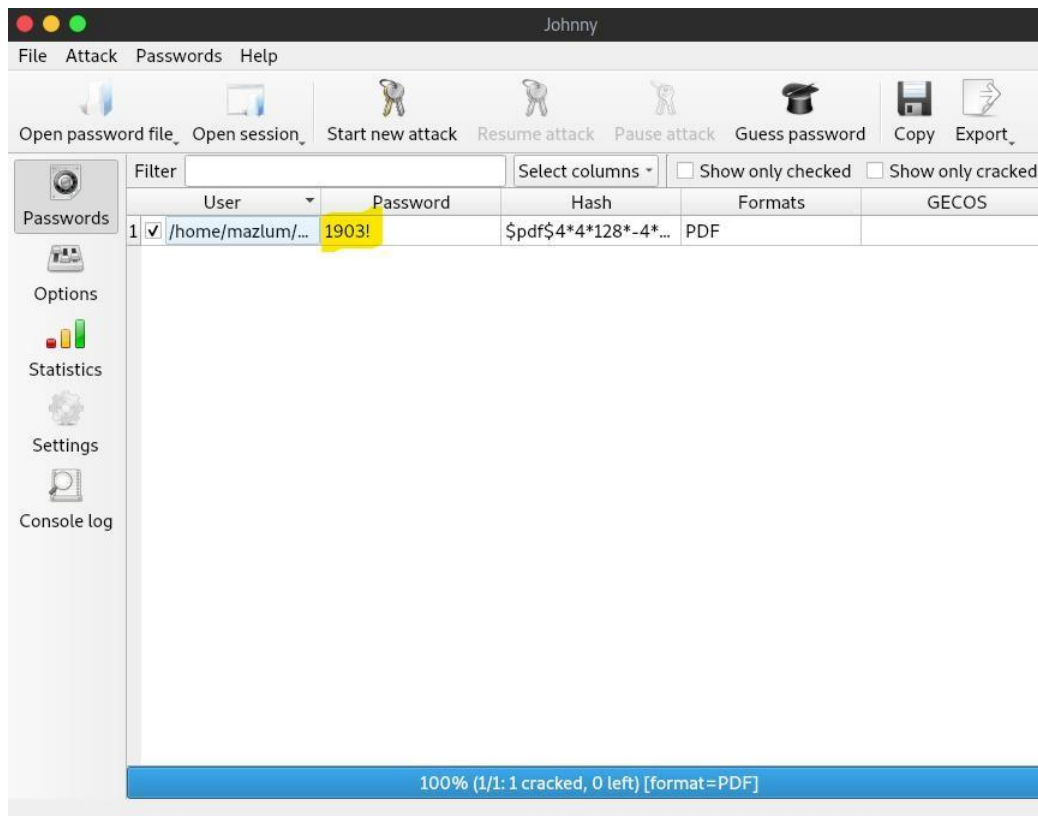
Örnekler:

A) Kolay Parola: 123

- Programın seçenekler kısmında bulunan saldırı modu alanından oluşturulan parola listesi içeri aktarılabilir. Ayrıca, görülmektedir ki yüklenen hash değerinin bir PDF dosyasına ait olduğu program tarafından anlaşılmış.
- Parola listesi programa aktarıldıktan sonra üst tarafta bulunan anahtar simgeli “yeni saldırı başlat” butonuna tıklayarak saldırı başlatılabilir.



B) Orta Düzey Parola: 1903!



D) Zor Parola: B351k745!

