ÇEVRİMDIŞI PAROLA KIRMA SALDIRILARI

DÜZGÜN KÜÇÜK

İçindeki Saldırı Türleri

Kişiye Özel Parola Listesi, Kaba Kuvvet, Rainbow Table

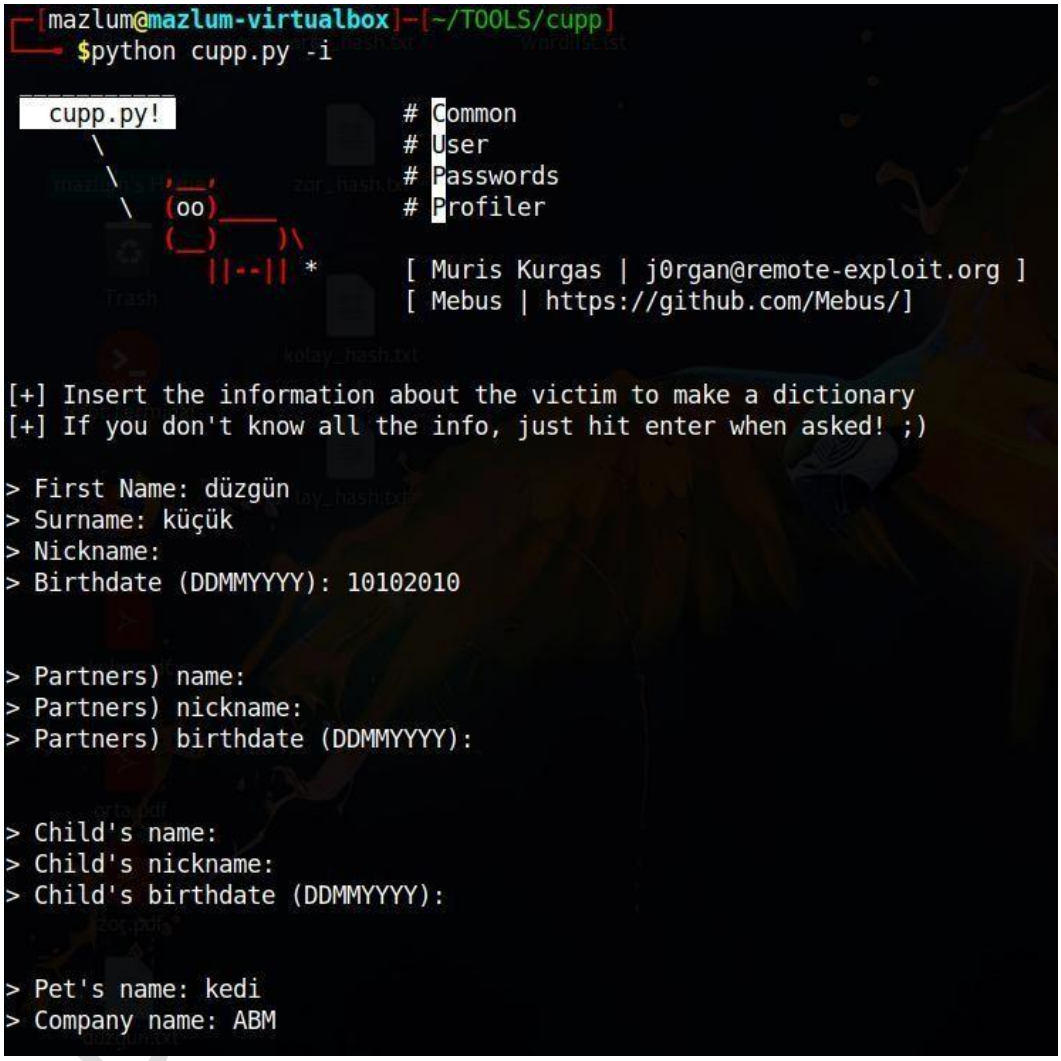
1) KİŞİYE ÖZEL PAROLA LİSTESİ

I. Parola Listesinin Oluşturulması

Kullanılan Araç: Cupp Tool

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

Kullanımı:



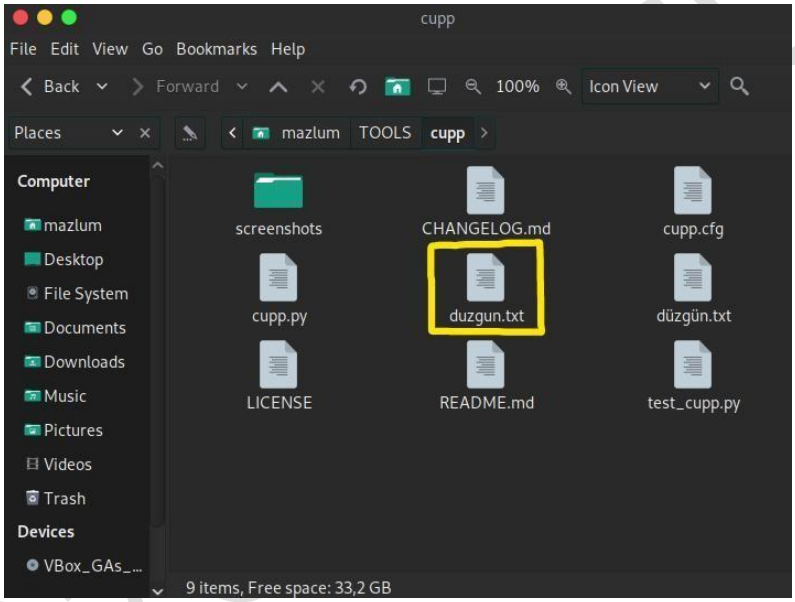
- Aracın yüklendiği klasöre gidip **python3 cupp -i** komutuyla araç çalıştırılır.
- Aracın girdileri üstte bulunan ekran görüntüsünde görünmektedir.

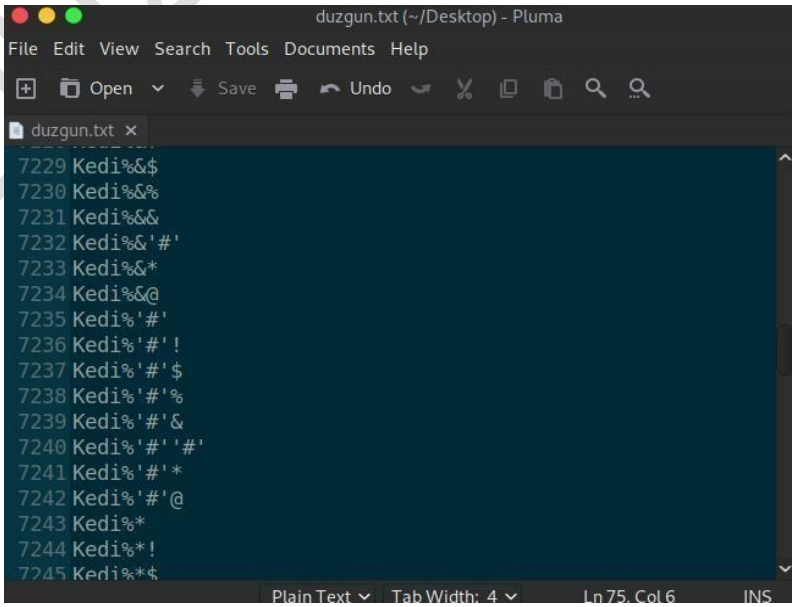
```
> Do you want to add some key words about the victim? Y/[N]: y
> Please enter the words, separated by comma. [i.e. hacker,juice,black], spaces will be removed: duzgun, Besiktas, 1903, Elazığ, Elazığ23_
> Do you want to add special chars at the end of words? Y/[N]: y
> Do you want to add some random 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 düzgün.txt, counting 15866 words.
> Hyperspeed Print? (Y/n) : n
[+] Now load your pistolero with düzgün.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 yarine kullanılmasıdır. Örnek: ARABA = 4R4B4

- Tüm ayarları yaptıktan sonra 15866 paroladan oluşan duzgun adında bir liste verdi. Liste aracın bulunduğu dizine kaydedilmektedir.

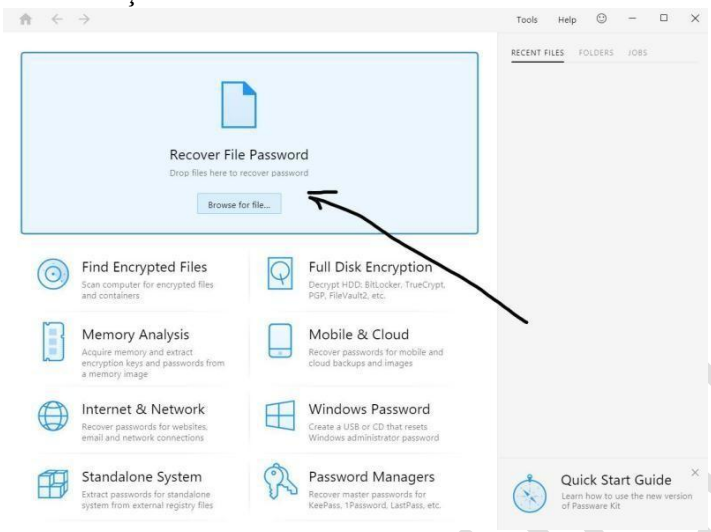




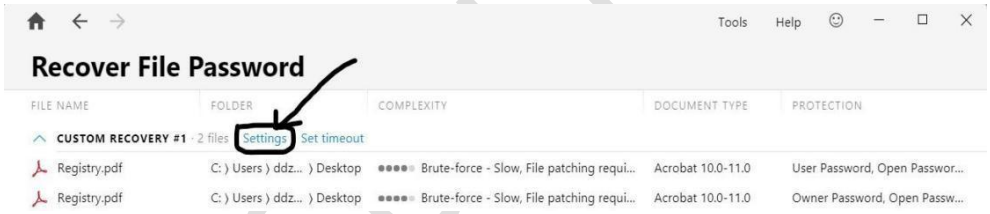
II. Oluşturulan Parola Listesini Bir Programa Aktararak Saldırma

Kullanılan Program: Passware

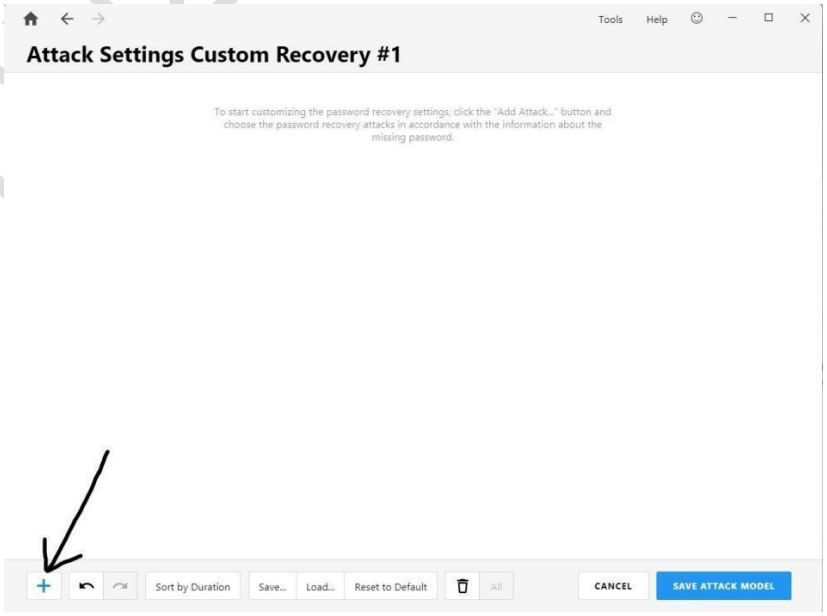
- Şifrelenmiş dosyayı belirtilen alana sürüklenebilir veya belirtilen alana tıklayıp açılan pencereden seçilebilir.



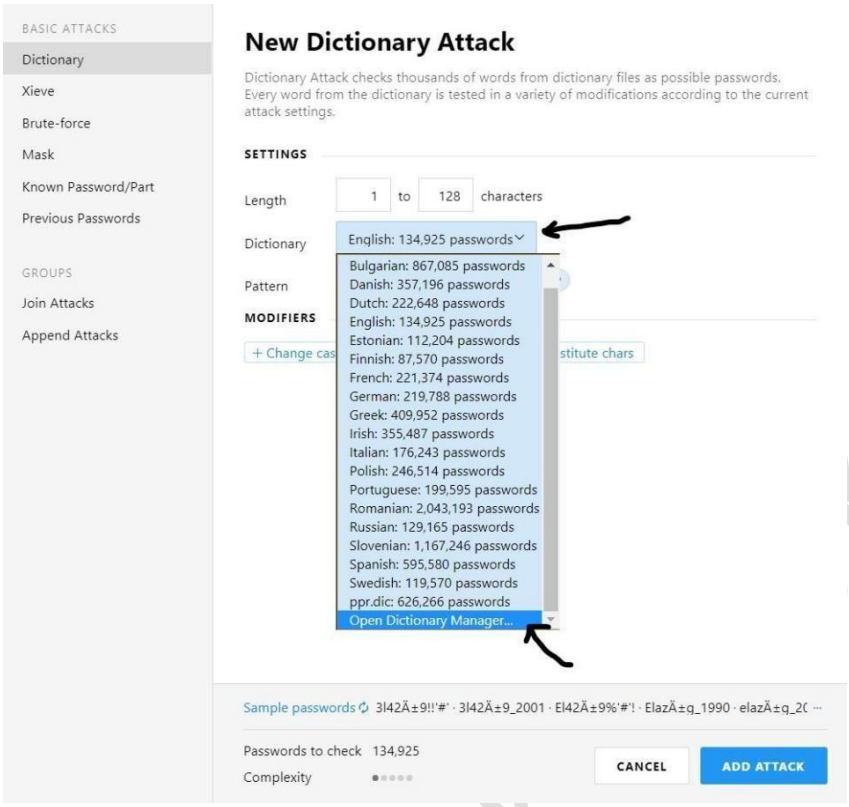
- Dosya seçildikten sonra önceden hazırladığımız listeyi eklemek için atarlara tıklamalıyız.



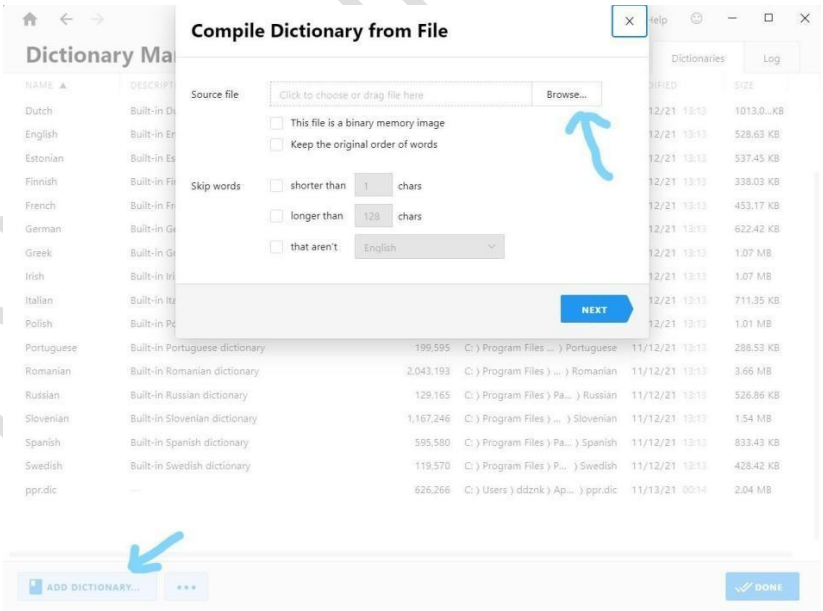
- Açılan bölüde saldırı eklemek için sol altta bulunan artı işeretine tıklanmalı.



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



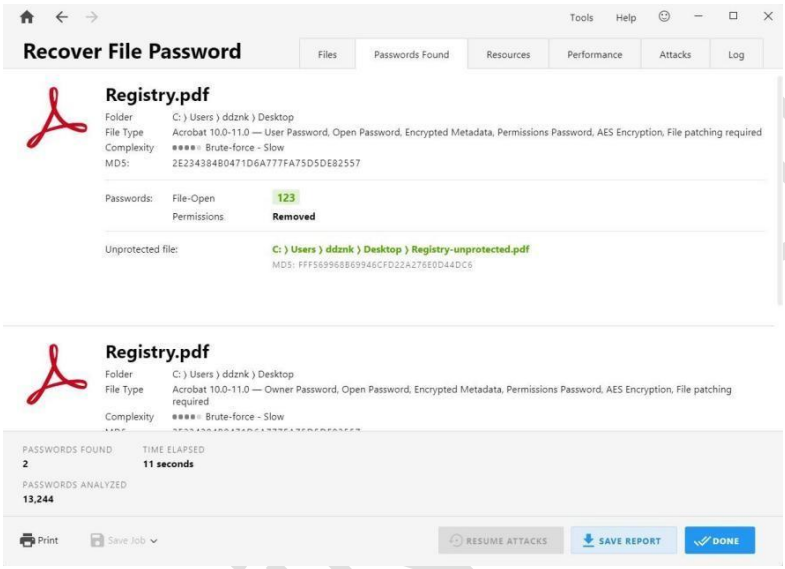
- Karşımıza Programın kendi bünyesinde bulunan parolal isteleri geldi. Kendi listemizi eklemek için sol alttaki seçenek seçilmeli ve açılan pencereden dosya arama kısmına tıklayıp parola listesi seçilmeli.



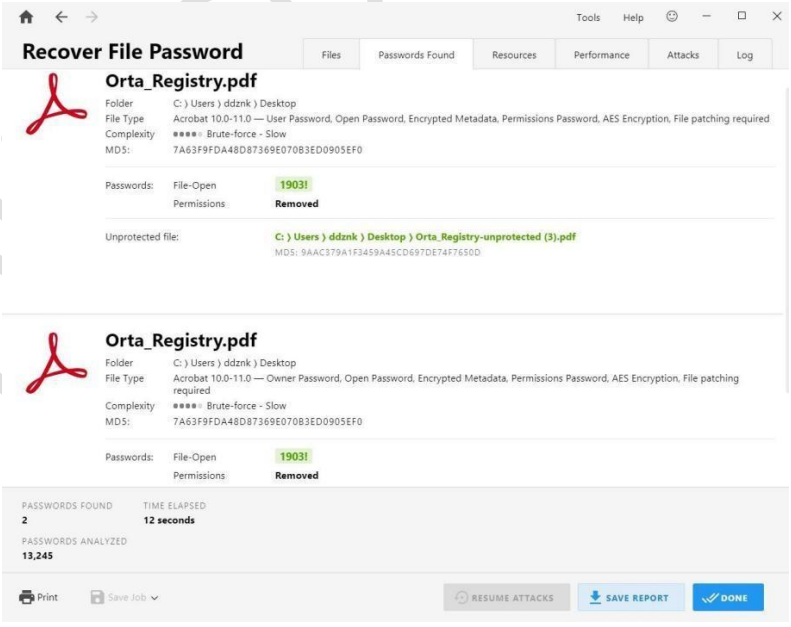
- Geri geldiğimizde saldırı türleri arasına seçtiğimiz listenin dail olduğu görülmekte.

Örnekler:

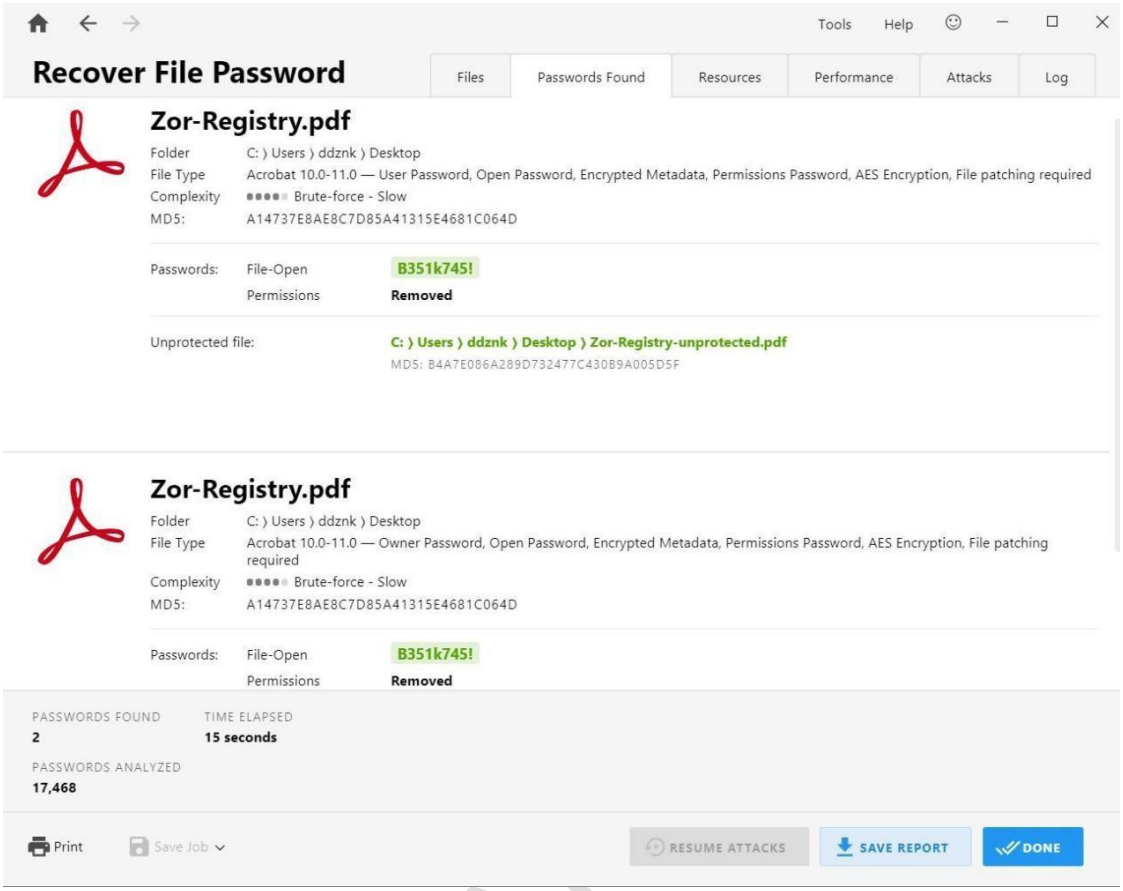
A) Kolay Parola: 123



B) Orta Düzey Parola: 1903!



C) Zor Parola: B351k745!



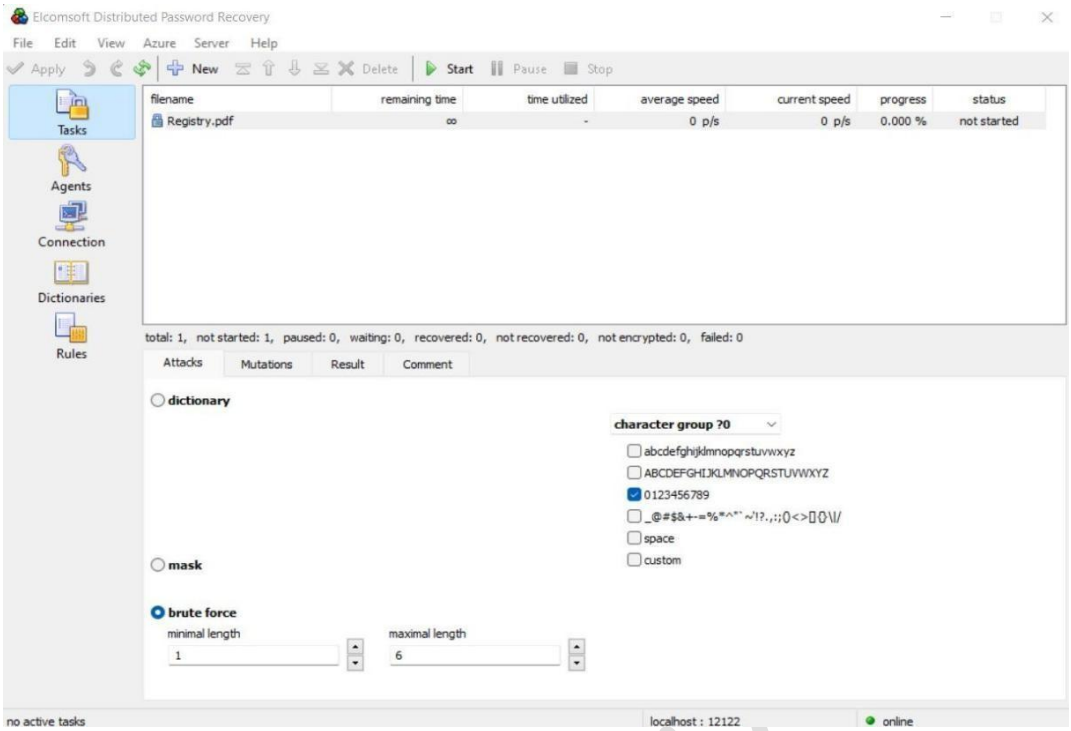
1) BRUTE FORCE

Deneme yanılma yoluyle belirlenen parola kombinasyonlarının teket teker şifrelenmiş dosya üzerinden denenmedsidir.

Örnekler:

A) Kolay Parola: 123

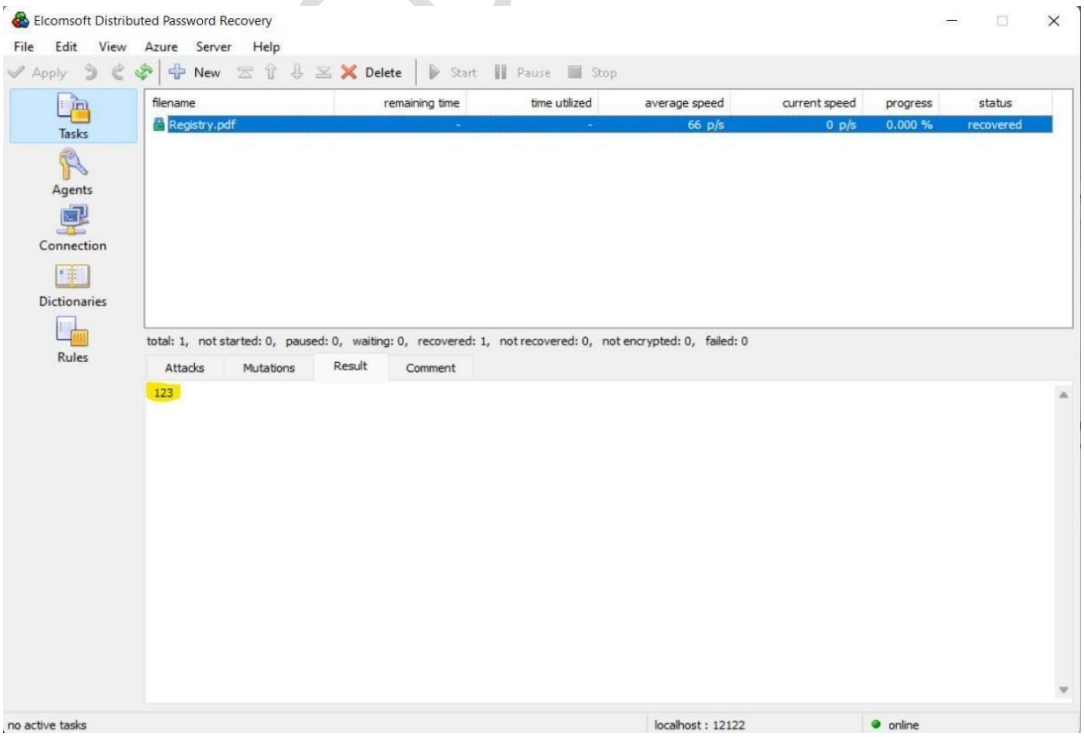
Kullanılan Program: Elcomsoft Distributed Password Recovery



- Program menüsünün üst bölümünde “New” yazan kısma tıklayarak şifrelenmiş dosya programa eklenmektedir.

- Programn alt menüsünden “Attacks” kısmında saldırıyı düzenlemek için parola uzunluğu, parolaya dahil edilmesi istenilen karakterler ve saldırı tipi gibi ayarlar yapılabilir.

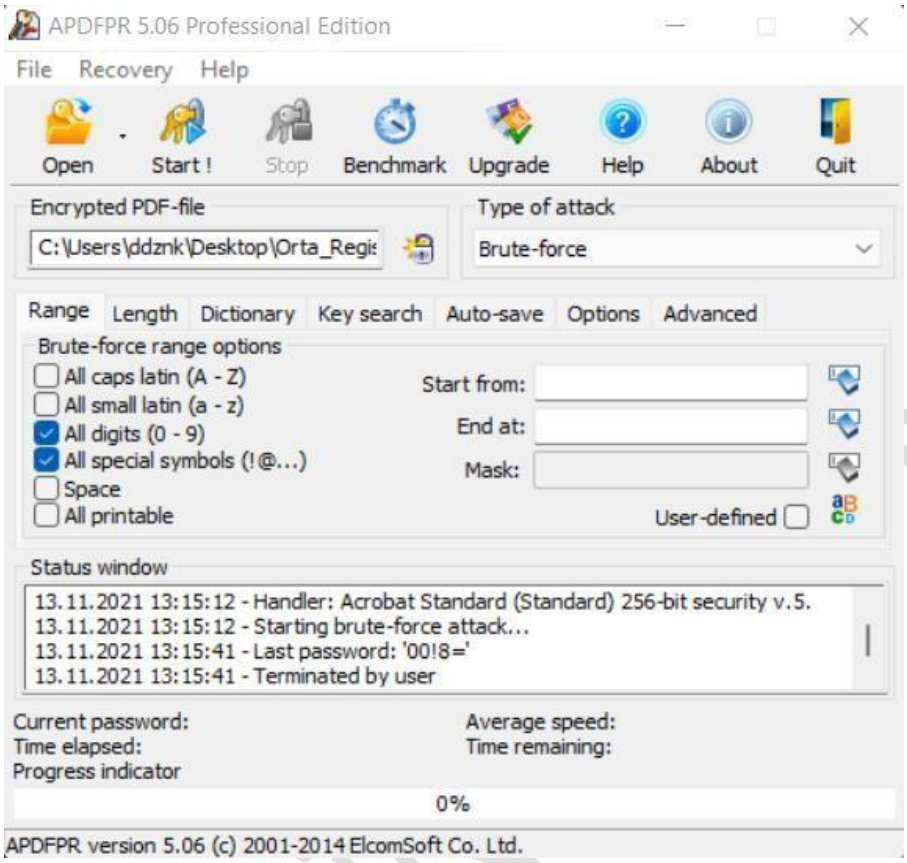
- İstenilen ayarlar yapıldıktan sonra üst kısımda bulunan “Start” butonuna tıklayıp saldırı başlatılıabilir.



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

B) Orta Düzey Parola: 1903!

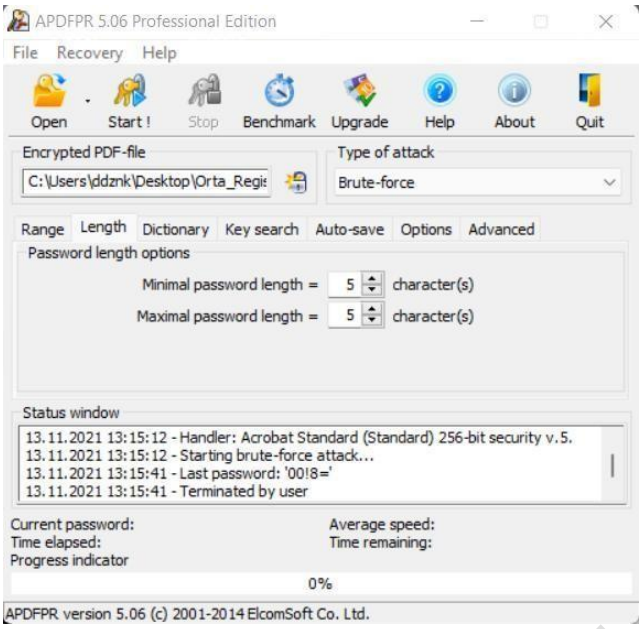
Kullanılan Program: Elcomsoft Advanced PDF Password Recovery



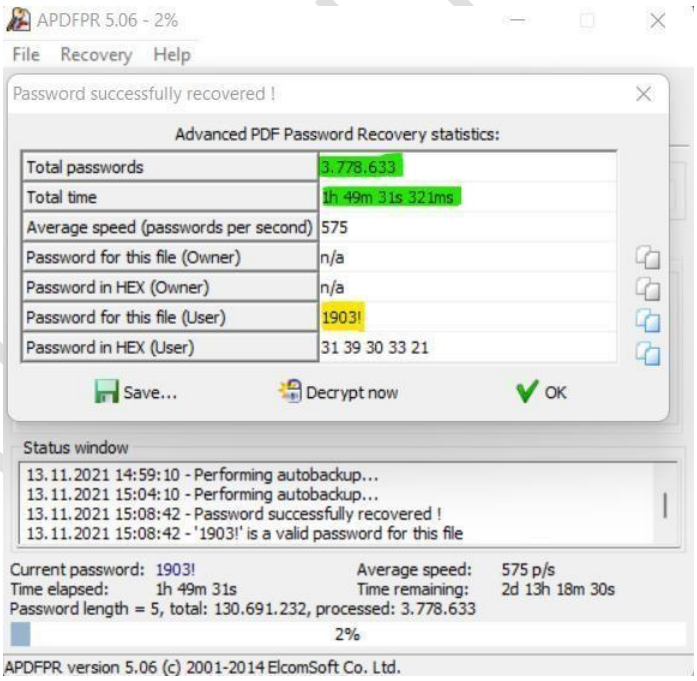
- Program menüsünün "Open" yazan kısmından şifrelenmiş dosya programa eklenmektedir.

- Programın "Range" yazan bölümünden saldırı için eklenecek karakterler, saldırının başlama noktası, saldırının bitiş noktası, maskeleme ayarları yapılmaktadır.

- Programın "Length" bölümünden saldırıda kullanılacak parolaların uzunluğu belirlenebilir.

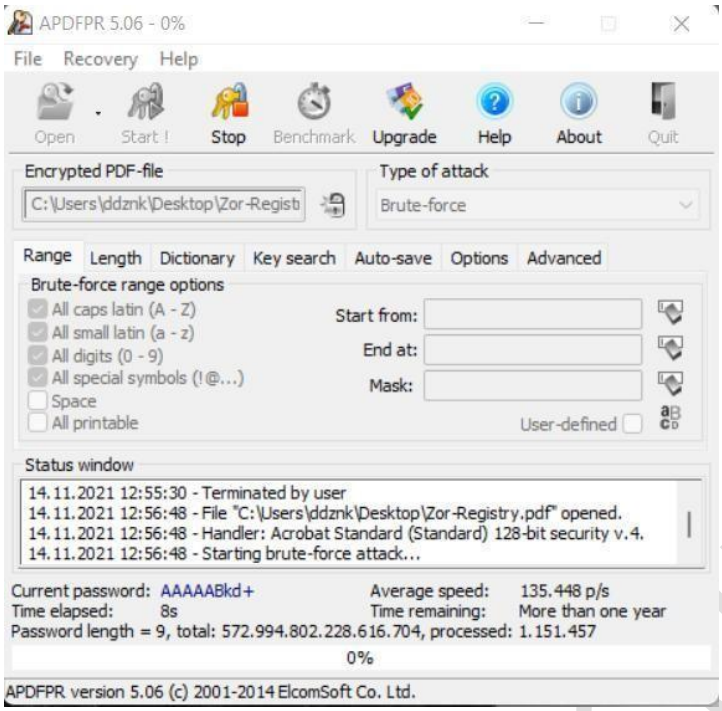


- Seçilen karakter uzayının büyüklüğüne ve parolada kullanılan karakter sayısına göre, parolanın kırılma süresi değişiklik göstermektedir. Ben parolayı kırarken sadece rakamlar ve özel karakterler kümesini seçtim. Max kırılma süresi 2 gün 15 saat civarı gösteriyordu ama penim parolamın başlangıç değeri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

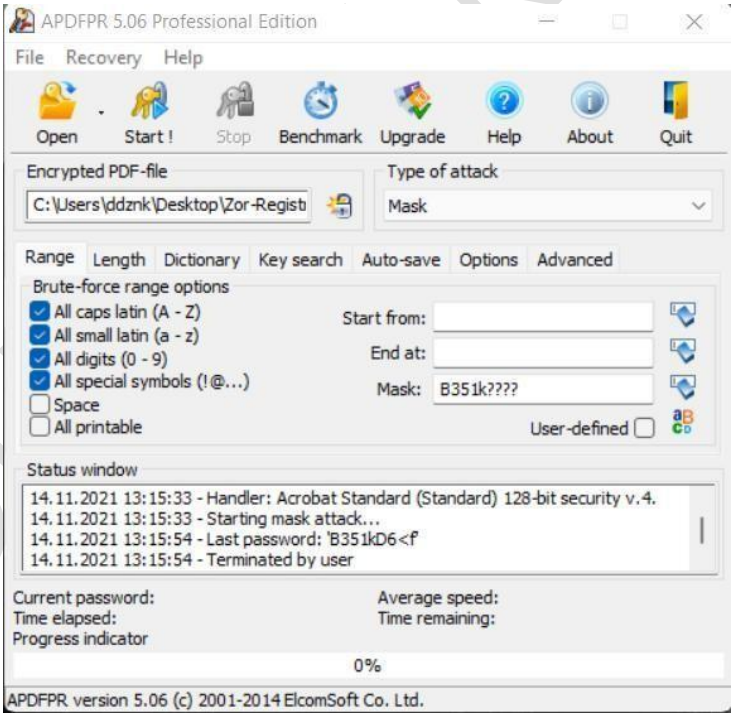


C) Zor Parola: B351k745!

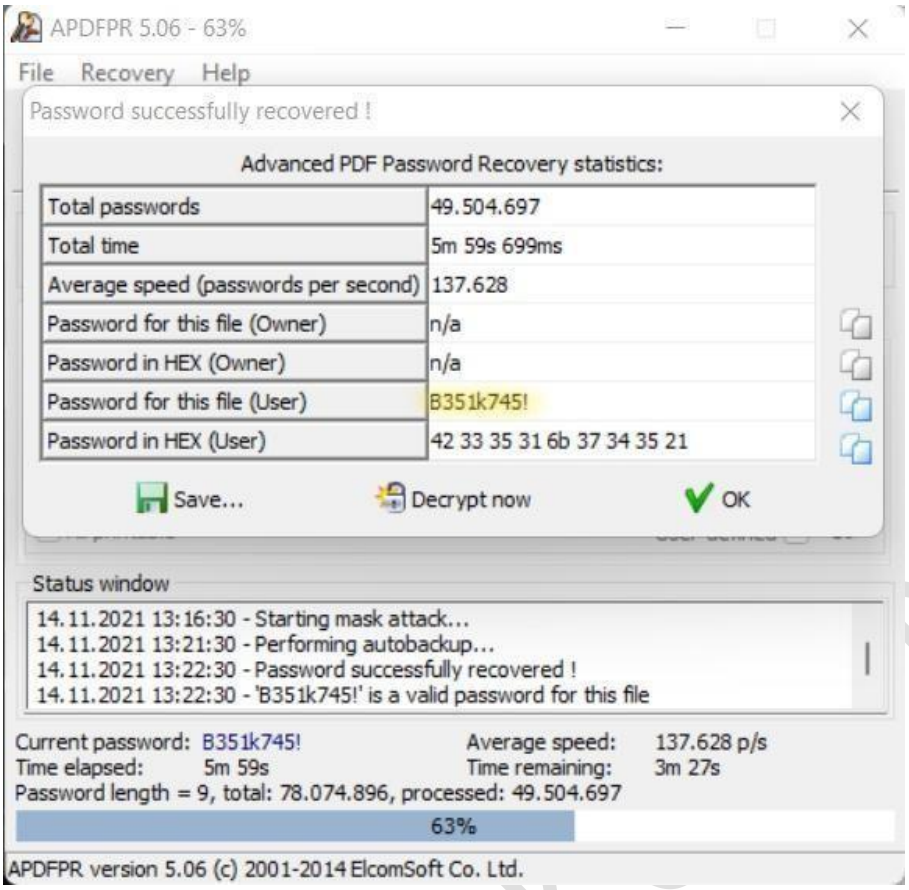
Not: Bu parolada büyük harf, küçük harf, rakam, özel karakter bulunmaktadır ve parola uzunluğu 9 karakter olduğu için tüm kümelerin seçilip karakter sayısını 9'a ayarladığımda parolanın kırılma süresi bir yıldan fazla olarak göründü. Benim 1 yıl kadar bekleme gibi bir şansım olmadığı için "maskeleme"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



Maskeleme: Eğer parolanın bağzı 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.



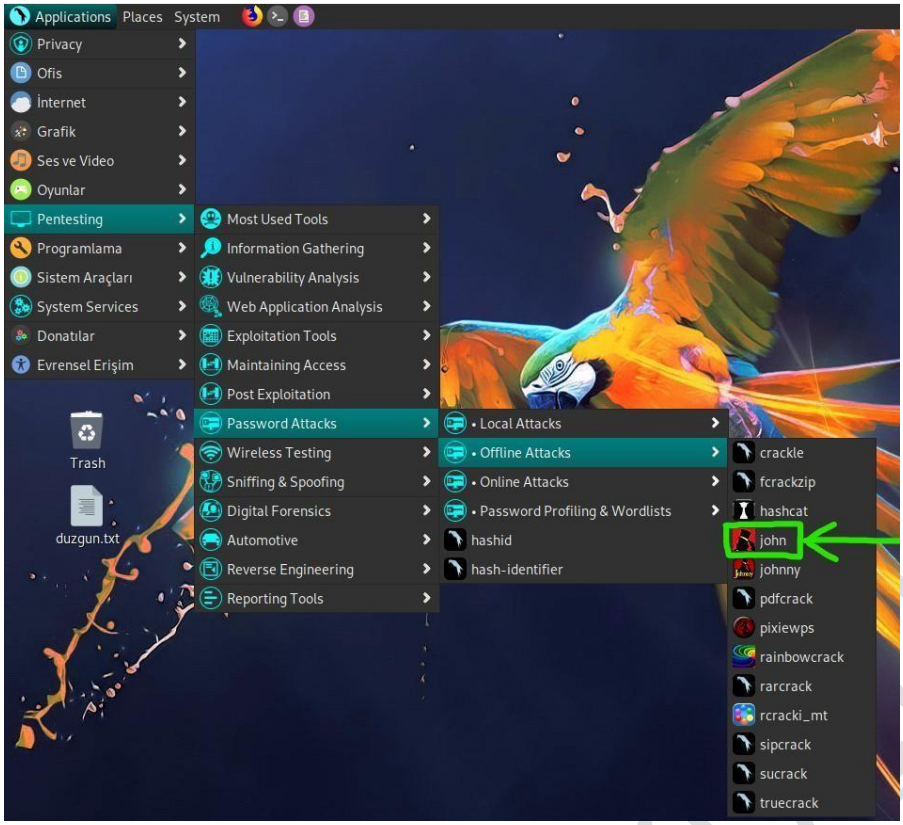
2) RAİNBOW TABLE SALDIRISI

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 herhengi bir hash değeri ile uyuşuyorsa o hash değerinin tablodaki karşılığı aranan paroladır.

I. Şifreli PDF Dosyasına Ait Hash Değerinin Hesaplanması

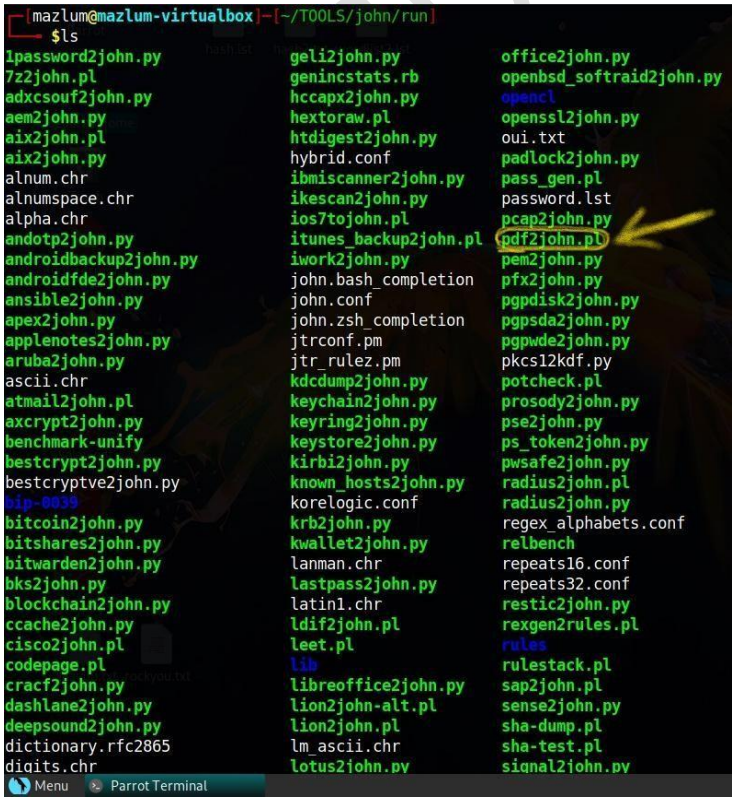
Kullanılan Program: John The Ripper

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 göründüğü gibidir. Bize lazım olan **pdf2john.pl**'dir



```
└─$perl pdf2john.pl  /home/mazlum/Desktop/kolay.pdf > /home/mazlum/Desktop/kolay_hash.txt
┌[mazlum@mazlum-virtualbox]-[~/TOOLS/john/run]
└─$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*fc244e39d53b54783f434ea5fb8d043028bf4e5e4e758a4164004e56fffa0108*
  32*c6d22afcb1d73776d95e0b2e51f8c1340b324e7e045b94392b457cc7adf41839
```

Zor Parolaya Ait Dosyasının Hash Değeri

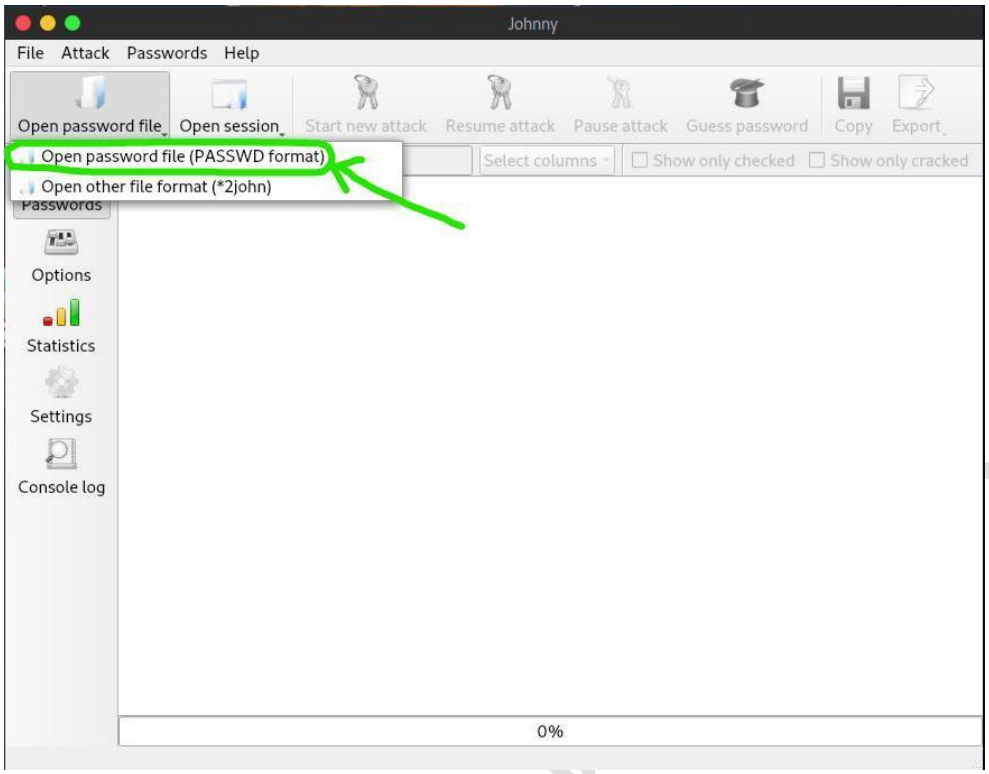
```
Parrot Terminal
File  Edit  View  Search  Terminal  Help
1 /home/mazlum/Desktop/zor.pdf:$pdf$4*4*128*-4*1*16*d7638db8a34f25323871dd12bb
  938738*32*6f4a1d61675022290350f81b2169de1328bf4e5e4e758a4164004e56fffa0108*3
  2*2ded03ffa3ab3bce941cc0007b89f00d59a676035adc8743a4e282acc38a09df
```

II. Hash Değerlerinin Kırılması

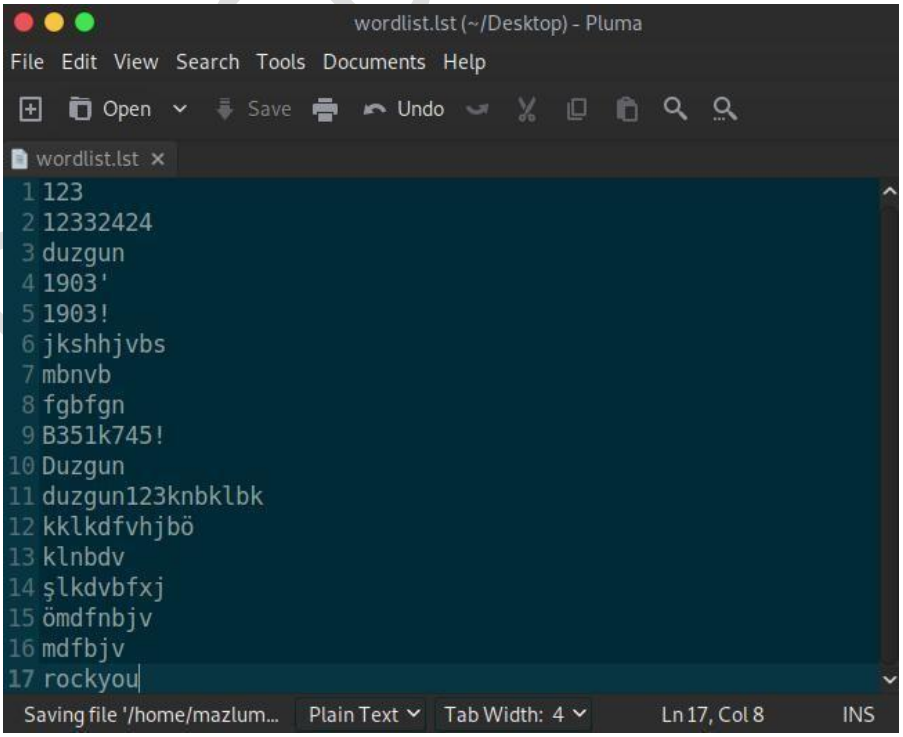
Kullanılan Program: Johnny

- 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.



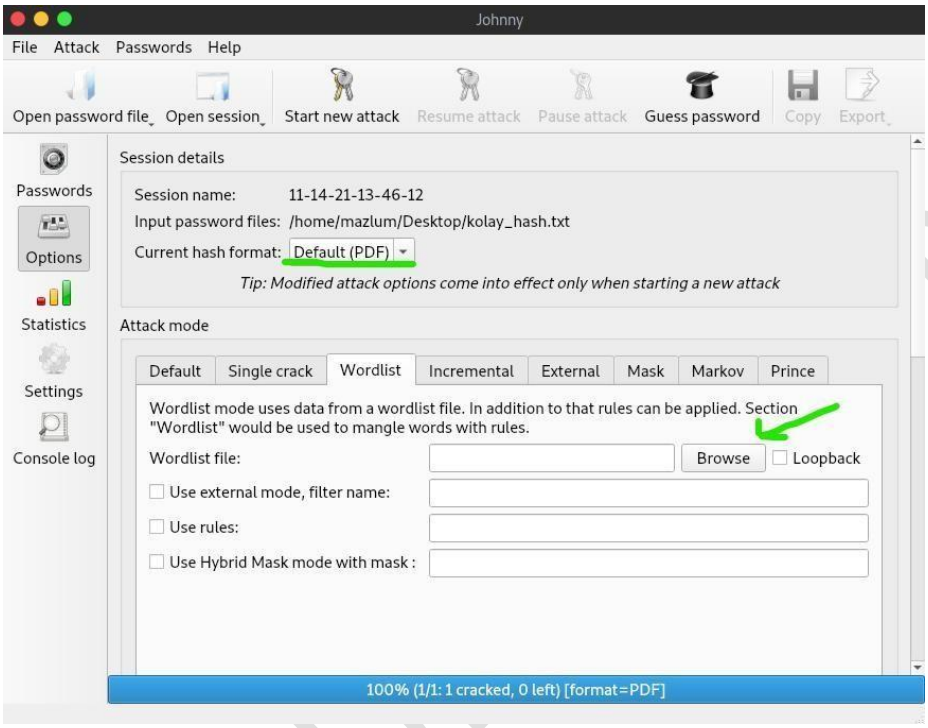
- Kırmak istediğimiz dosya yüklendikten sonra sıra önceden hazırladığımız parola listesini programa yüklemekte. **Bu program, listede bulunan şifrelenmemiş parolaları saldırı sırasında şifreleyip hedef hash değeri ile karşılaşırma özelliğine sahiptir. Bunun için oluşturduğum listeye parolaların hash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

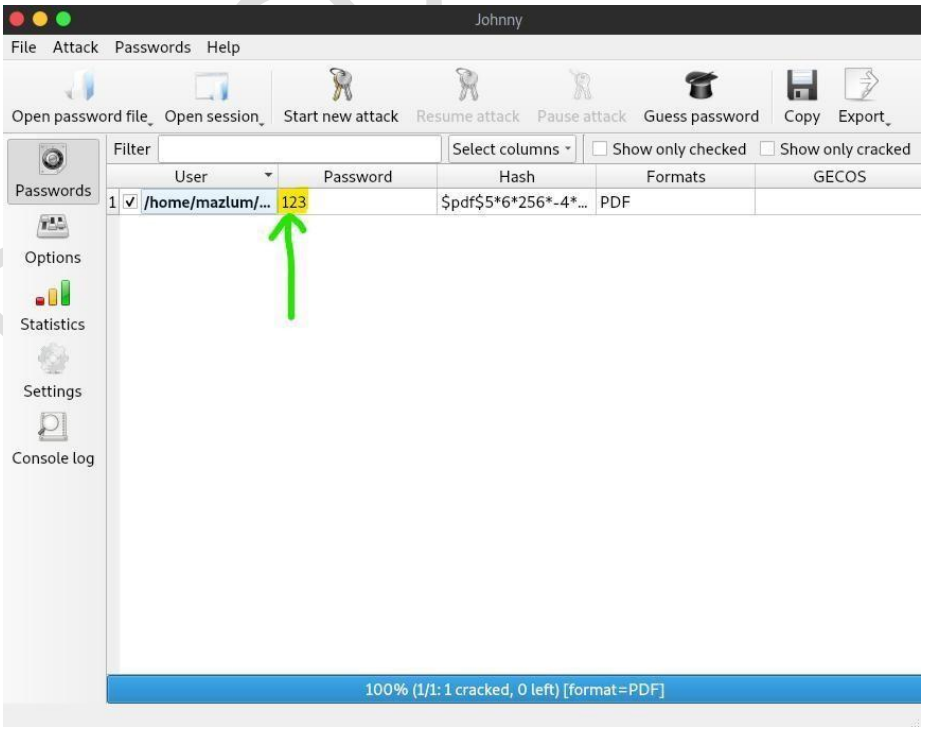


Örnekler:

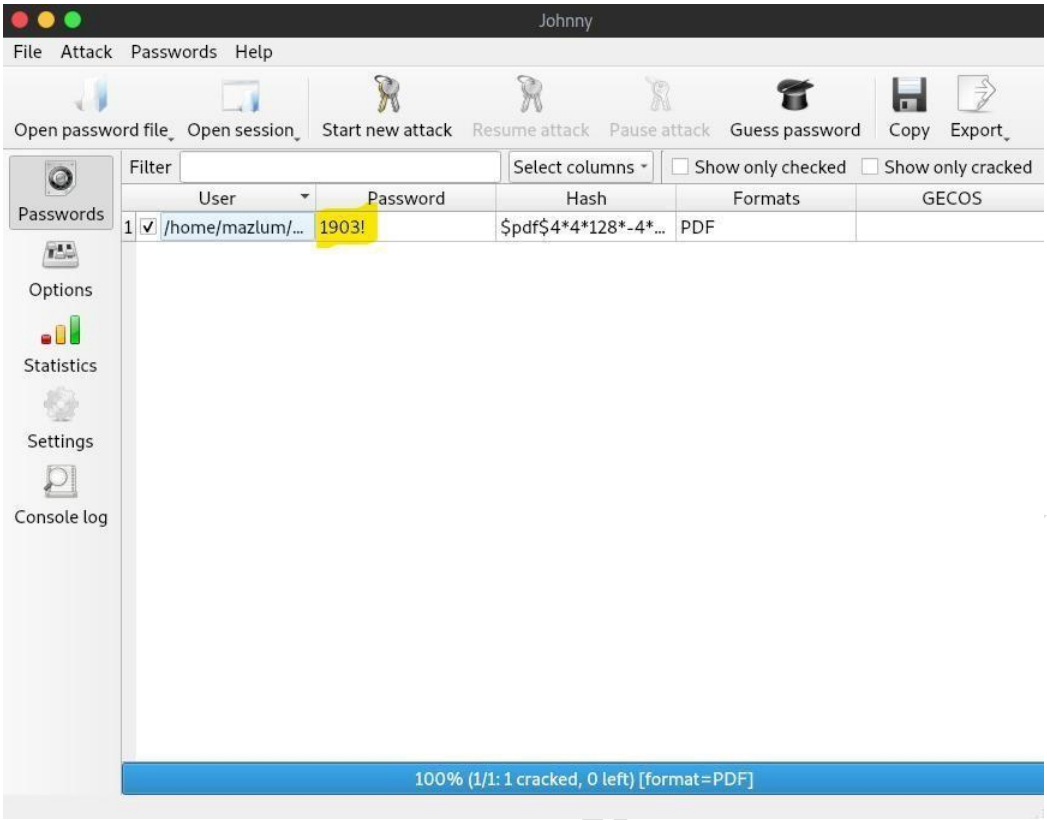
A) Kolay Parola: 123

- Programın seçenekler kısmında bulınan saldırı modu alanından oluşturulan parola listesi içeri aktarılabilir. Ayrıca, görülmektedir ki yüklenilen 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!