twitter.com/b4l1c

Is it possible to identify someone on Twitter?

I did some research on this topic and I have realized that there is a way to get user's credentials to some extend. This method is theoretically very suitable for the brute-force logic. I have been using it for nearly for 1 year and generally I got positive results.

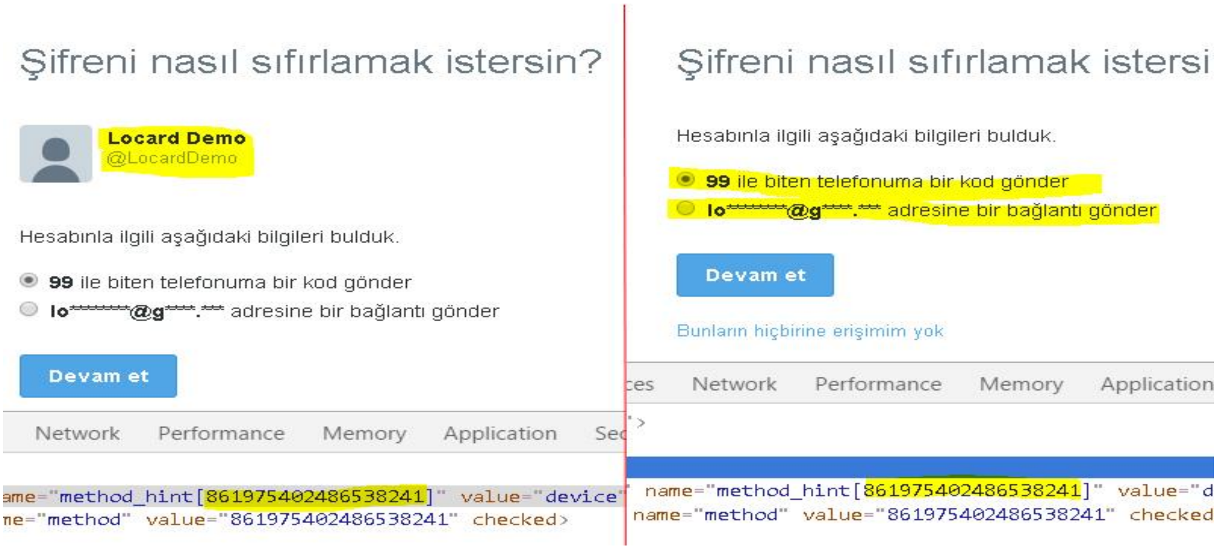
Please note that Twitter users must have added a phone number to their Twitter accounts for us to be able to find users with this method.

Forgot my Username & Password?

If you come to the "Password Reset" section on Twitter and click on the "Search" button with your Username information, Twitter gives us the associated account information for this Username. These include the "Phone Number" and "E-mail" addresses which are masked. The most important value which Twitter gives us as a masked is the method_hind parameter that is between the last 2 digit of the "Phone Number" and the source code.

The Method_Hind parameter has a static id value and masking the user information in this area still allows us to overcome the "privacy policy" definitions in "Search" operation with "Phone Number".

Why do we exceed Privacy Policy definitions? First of all, we have to pay attention to this difference. When we come to Password Reset section and search for "Username", we are given "Username" information visible, whereas "Phone Number" and "E-mail" details are masked. What happens if we come to the "Password Reset" section and click on "Search" button after typing "E-mail" or "Phone Number" instead of Username?
This time it does not give us the related "Username" information, otherwise we can easily associate this information with the accounts. At the very moment, Method_Hint parametre does the trick for us. The fact that the Method_Hint parameter has a static id value breaks the "Privacy Policy" because when you click on "Search" button with the username, we get the same "Method_Hind" id that we obtained when we search for the "Phone Number". By this means, we can associate the accounts with Method_Hind id.



Şifreni nasıl sıfırlamak istersin?

Locard Demo
@LocardDemo

Hesabınla ilgili aşağıdaki bilgileri bulduk.

● 99 ile biten telefonuma bir kod gönder
○ lo********@g****.*** adresine bir bağlantı gönder

```
ame="method_hint[861975402486538241]" value="device"
ne="method" value="861975402486538241" checked>
```

Şifreni nasıl sıfırlamak istersi

Hesabınla ilgili aşağıdaki bilgileri bulduk.

● 99 ile biten telefonuma bir kod gönder
○ lo********@g****.*** adresine bir bağlantı gönder

Bunların hiçbirine erişimim yok

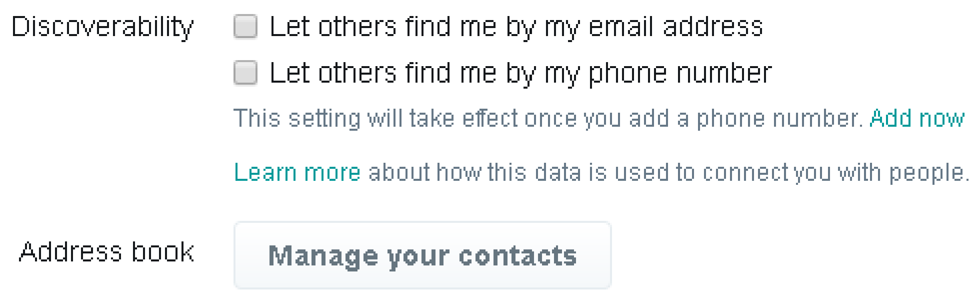
```
 name="method_hint[861975402486538241]" value="d
name="method" value="861975402486538241" checked
```

Hind id is obtained by entering "Username" on the left side and "Phone Number" information on the right side.

Note: It has come to our attention that Twitter has made some improvements to the "Password Reset" panel last a few years. I don't know if you ever noticed, around a year ago when we entered the "Password Reset" panel by Username or E-mail address, it was masking the Username part of your email address and gave us the rest of the domain information like @hotmail.com. Also, the first 4 and the last 2 digits of your phone number were shown but the middle part was masked. After these updates, they began to mask the first 4 digits of your phone number as well as the domain name which is the last part of your e-mail. By adding one more feature to their improvements, they are now also requesting the existing information to be able to perform in Password Reset panel. (Google has been using it for a long time, so you might noticed this). However, since this feature is not selected in the default settings, if the Twitter user does not enter the Settings section and activate this security measure, the protection does not work.

Twitter Import Contact

Twitter allows users to import "Contact List" via their e-mail account with the "Find Your Friends" feature. By using this feature, we can transfer all "Contacts" in our e-mail account to the "Contact List" section of my Twitter account. At this stage, we came across with another fiction mistake. Twitter users are presented with the "Discoverability" feature in their "Settings / Privacy" section, depending on their own choice. However, our selections in the "Discoverability" feature does not work in the "Manage your Contacts" section.



Discoverability

□ Let others find me by my email address

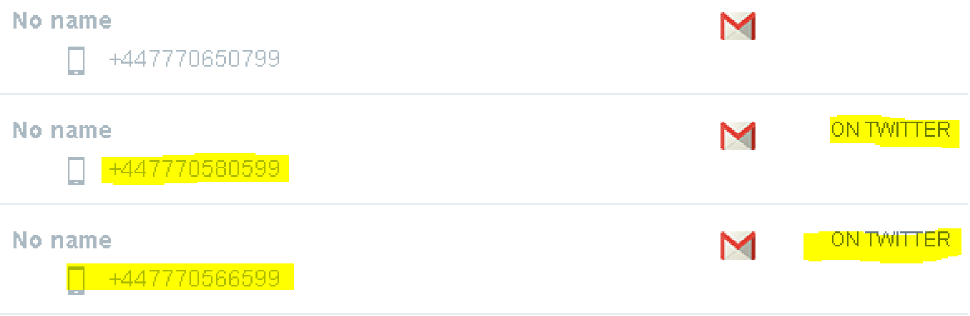
□ Let others find me by my phone number

This setting will take effect once you add a phone number. Add now

Learn more about how this data is used to connect you with people.

Address book

Even if these settings are not selected, if someone succeeds in adding you as a "Contact" to his/her Twitter account with your phone number, Twitter actually shares with us whether this number is on Twitter or not.



No name
+447770650799

No name
+447770580599
ON TWITTER

No name
+447770566599
ON TWITTER

What do we have?

With these findings we have obtained so far;

(1) We can find out whether there is a Twitter user with a "Phone Number" or not.
(2) We can find out the method_Hind id with a "Phone Number"

What do we have about the targeted account?

1. Username details
2. The last 2 digit of the "Phone Number"
3. Method_Hind id

Needs?

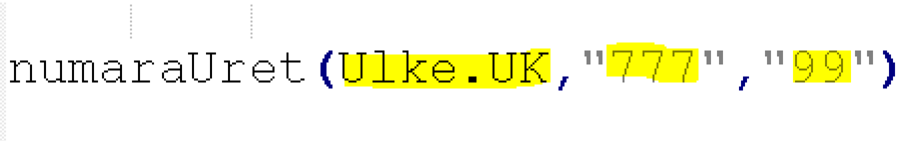
Identification of all "Phone Number" which ends with 99. One hundred thousand possibilities.

1 Gmail account -> To add 100 thousand possible phone numbers as Contact.
1 Twitter account-> To transfer contact lists in gmail account to Twitter account.

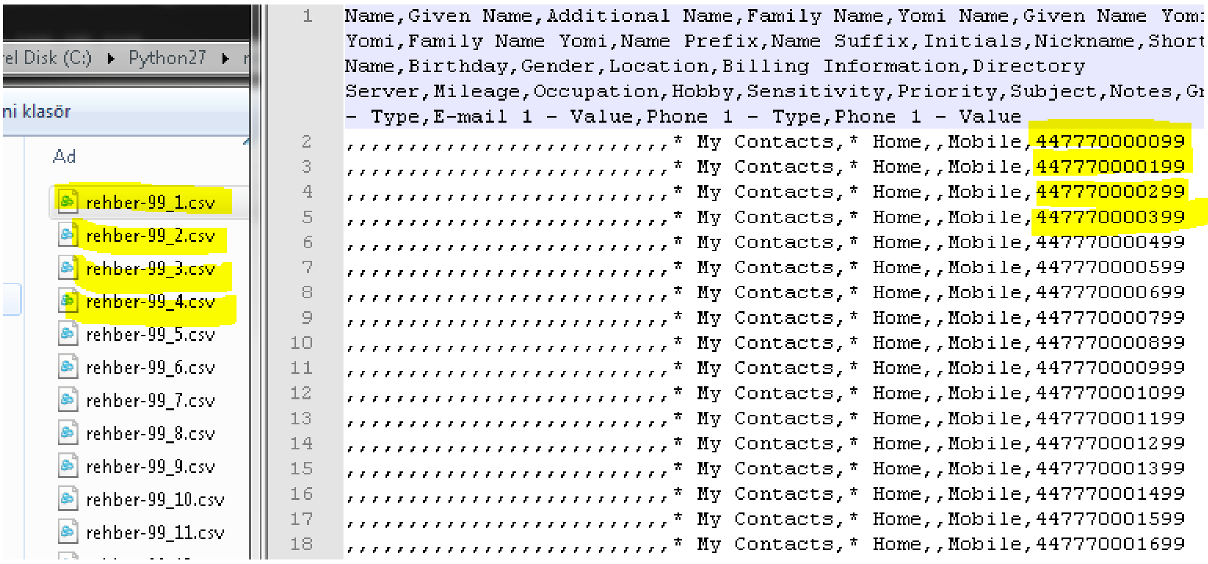
Phone Number Generator->https://github.com/ibrahimbalic/locarddemo/blob/master/telefon.py

Generating Phone Number

We are generating all "Phone Numbers" ending with 99 by the "phone.py" script I share from Github. Since I do not know the operator code of this PoC, I make 100 thousand directly with "777". Normally, we need to create separate lists for each operator.



```
numaraUret(Ulke.UK,"777","99")
```



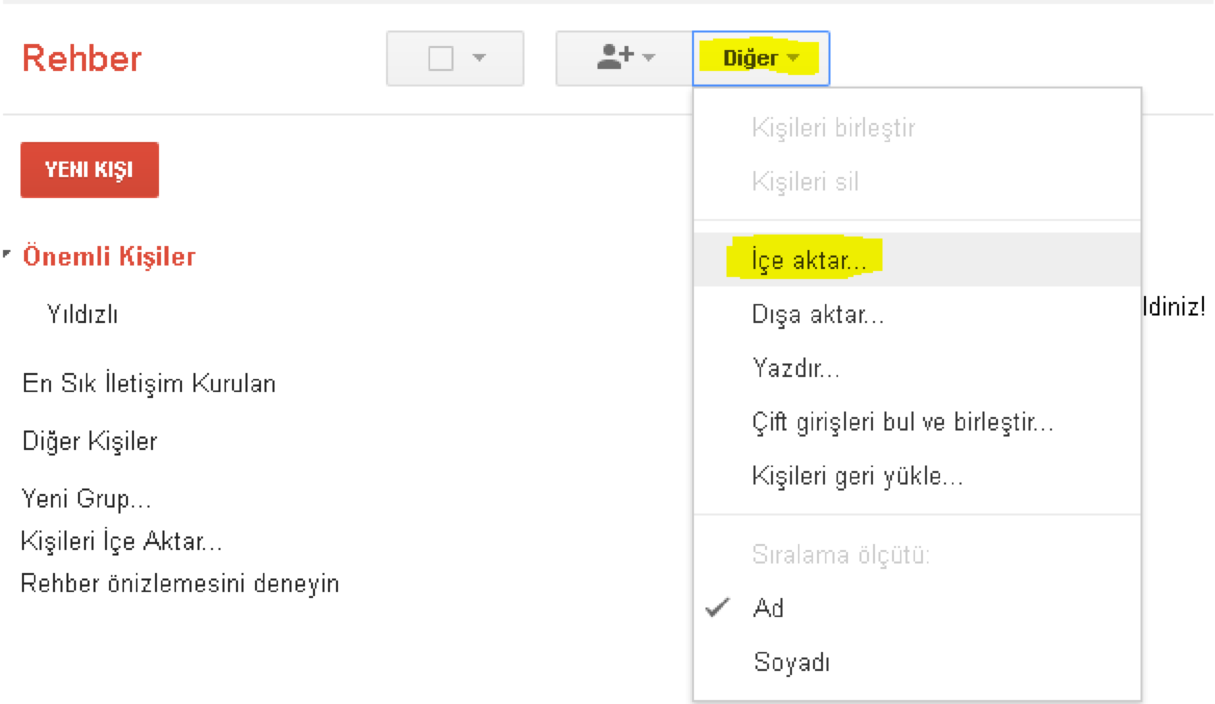
rehber-99_1.csv
rehber-99_2.csv
rehber-99_3.csv
rehber-99_4.csv
rehber-99_5.csv
rehber-99_6.csv
rehber-99_7.csv
rehber-99_8.csv
rehber-99_9.csv
rehber-99_10.csv
rehber-99_11.csv

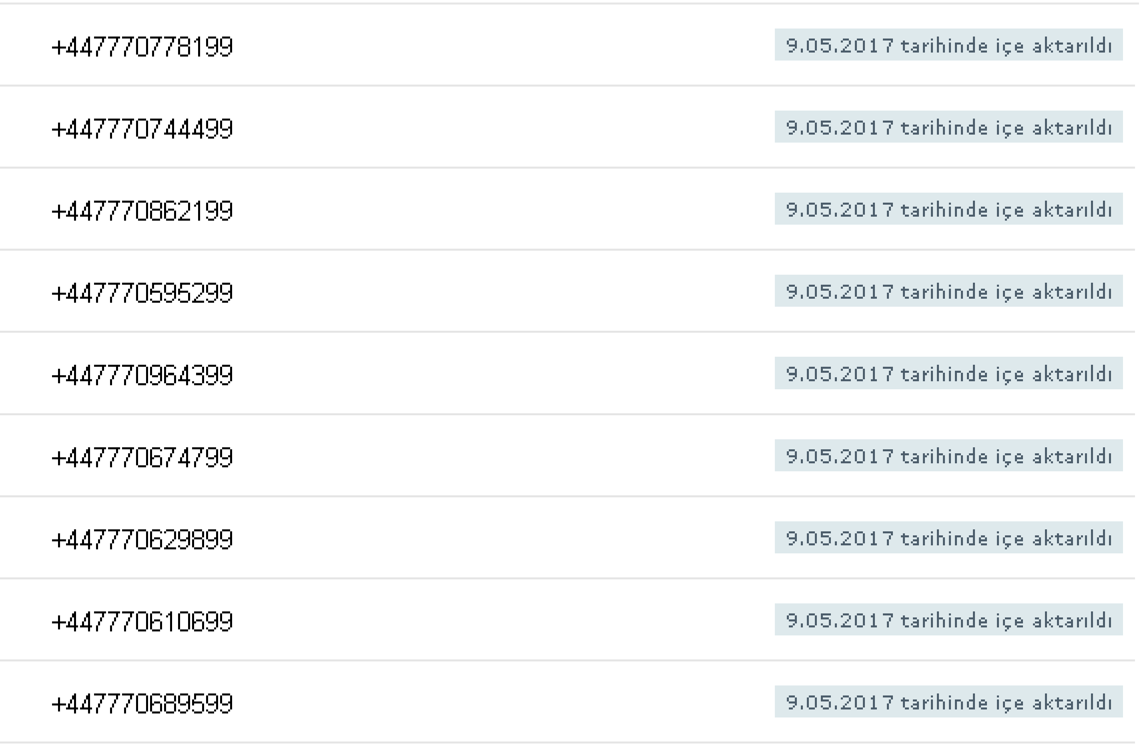
```
Name,Given Name,Additional Name,Family Name,Yomi Name,Given Name Yomi
Yomi,Family Name Yomi,Name Prefix,Name Suffix,Initials,Nickname,Short
Name,Birthday,Gender,Location,Billing Information,Directory
Server,Mileage,Occupation,Hobby,Sensitivity,Priority,Subject,Notes,Gr
- Type,E-mail 1 - Value,Phone 1 - Type,Phone 1 - Value
,,,,,,,,,,,,,,,,,,,,,,,,,* My Contacts,* Home,,Mobile,447770000099
,,,,,,,,,,,,,,,,,,,,,,,,,* My Contacts,* Home,,Mobile,447770000199
,,,,,,,,,,,,,,,,,,,,,,,,,* My Contacts,* Home,,Mobile,447770000299
,,,,,,,,,,,,,,,,,,,,,,,,,* My Contacts,* Home,,Mobile,447770000399
,,,,,,,,,,,,,,,,,,,,,,,,,* My Contacts,* Home,,Mobile,447770000499
,,,,,,,,,,,,,,,,,,,,,,,,,* My Contacts,* Home,,Mobile,447770000599
,,,,,,,,,,,,,,,,,,,,,,,,,* My Contacts,* Home,,Mobile,447770000699
,,,,,,,,,,,,,,,,,,,,,,,,,* My Contacts,* Home,,Mobile,447770000799
,,,,,,,,,,,,,,,,,,,,,,,,,* My Contacts,* Home,,Mobile,447770000899
,,,,,,,,,,,,,,,,,,,,,,,,,* My Contacts,* Home,,Mobile,447770000999
,,,,,,,,,,,,,,,,,,,,,,,,,* My Contacts,* Home,,Mobile,447770001099
,,,,,,,,,,,,,,,,,,,,,,,,,* My Contacts,* Home,,Mobile,447770001199
,,,,,,,,,,,,,,,,,,,,,,,,,* My Contacts,* Home,,Mobile,447770001299
,,,,,,,,,,,,,,,,,,,,,,,,,* My Contacts,* Home,,Mobile,447770001399
,,,,,,,,,,,,,,,,,,,,,,,,,* My Contacts,* Home,,Mobile,447770001499
,,,,,,,,,,,,,,,,,,,,,,,,,* My Contacts,* Home,,Mobile,447770001599
,,,,,,,,,,,,,,,,,,,,,,,,,* My Contacts,* Home,,Mobile,447770001699
```

If we edit and run the script according to ourselves, we create a directory named contact in the same directory, and it automatically prepares 5000 thousand listings in CVS format.

Importing Gmail Contacts

When you come to the Gmail contact panel, click on import button and upload the files one by one. After the selected files have been uploaded, we will see that the numbers are listed as follows.



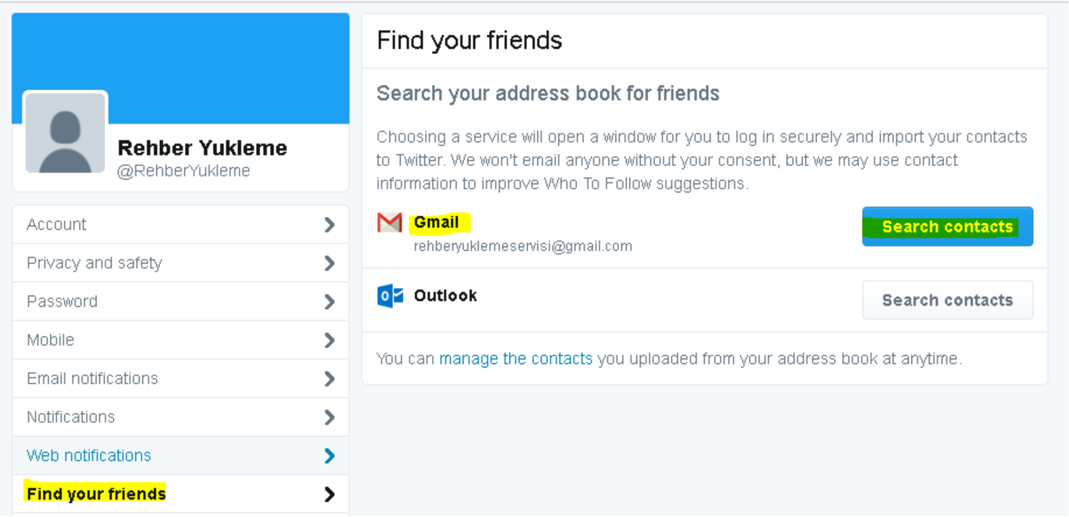


+447770778199	9.05.2017 tarihinde içe aktarıldı
+447770744499	9.05.2017 tarihinde içe aktarıldı
+447770862199	9.05.2017 tarihinde içe aktarıldı
+447770595299	9.05.2017 tarihinde içe aktarıldı
+447770964399	9.05.2017 tarihinde içe aktarıldı
+447770674799	9.05.2017 tarihinde içe aktarıldı
+447770629899	9.05.2017 tarihinde içe aktarıldı
+447770610699	9.05.2017 tarihinde içe aktarıldı
+447770689599	9.05.2017 tarihinde içe aktarıldı

Find your Friends with Twitter Gmail

Now it is time to transfer these numbers that we upload to our Gmail to our Twitter Contact List. To do that, we go to Settings / Find your friends section. https://twitter.com/who_to_follow/import

After this step we click on the Gmail Search contacts button.



Rehber Yukleme
@RehberYukleme

- Account
- Privacy and safety
- Password
- Mobile
- Email notifications
- Notifications
- Web notifications
- Find your friends

Find your friends

Search your address book for friends

Choosing a service will open a window for you to log in securely and import your contacts to Twitter. We won't email anyone without your consent, but we may use contact information to improve Who To Follow suggestions.

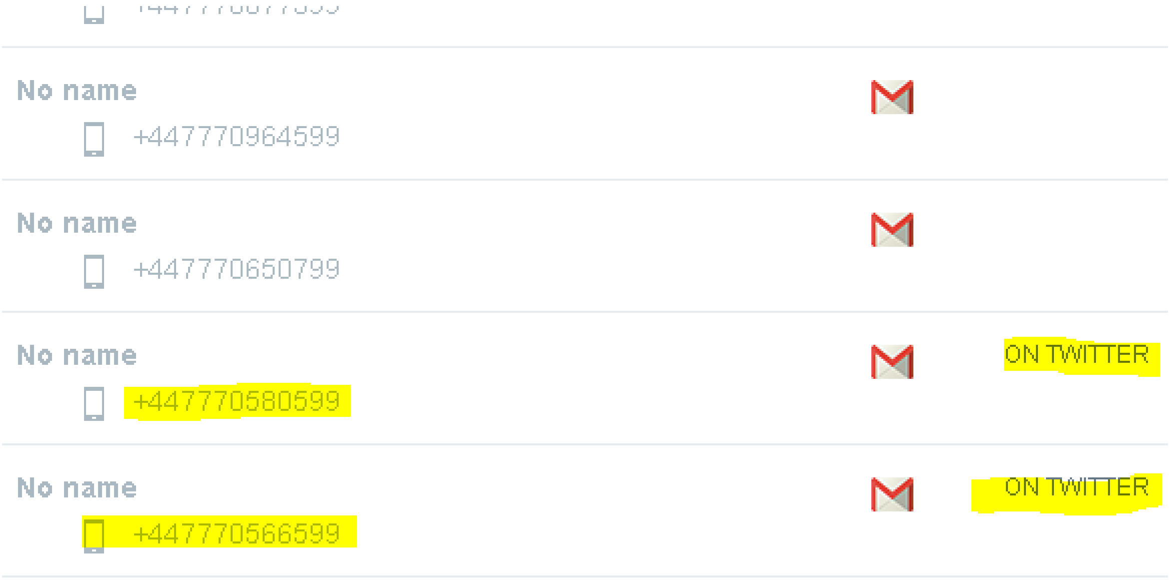
Gmail
rehberyuklemeservisi@gmail.com
Search contacts

Outlook
Search contacts

You can manage the contacts you uploaded from your address book at anytime.

When your list is successfully uploaded. We go to Settings/Privacy and Safety/Manage your contacts section.

When you come here, you get the following result



No name
+447770964599

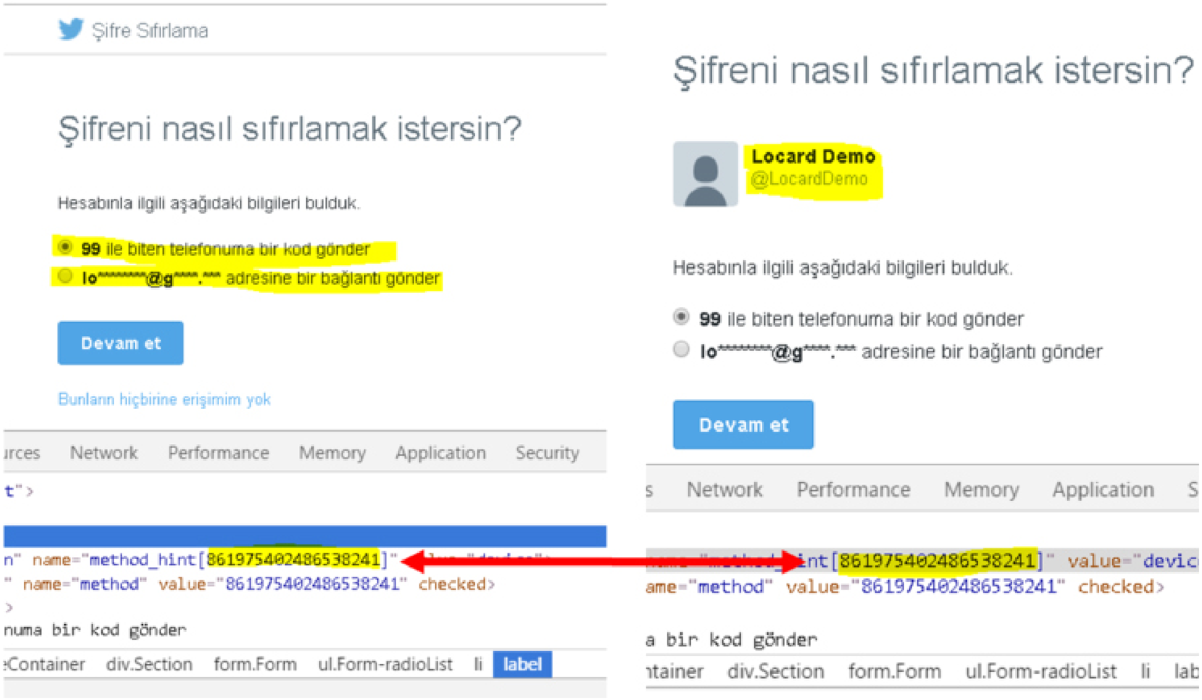
No name
+447770650799

No name
+447770580599
ON TWITTER

No name
+447770566599
ON TWITTER

As we can see here, the numbers that registered on Twitter has "on twitter" sign. We pick over this list to make a new list of people who are on Twitter. Then, we collect individual method_hind id from "Forgot Password?" section for these numbers and we are trying to determine the targeted account by comparing it with the method_hind id we have obtained.

Result?



Şifre Sıfırlama

Şifreni nasıl sıfırlamak istersin?

Hesabınla ilgili aşağıdaki bilgileri bulduk.

● **99** ile biten telefonuma bir kod gönder

○ **lo**********@g*****.***** adresine bir bağlantı gönder

Devam et

Bunların hiçbirine erişimim yok

```
t">

n" name="method_hint[861975402486538241]"
" name="method" value="861975402486538241" checked>
>
numa bir kod gönder
```

urces Network Performance Memory Application Security
:Container div.Section form.Form ul.Form-radioList li label

Şifreni nasıl sıfırlamak istersin?

Locard Demo
@LocardDemo

Hesabınla ilgili aşağıdaki bilgileri bulduk.

● **99** ile biten telefonuma bir kod gönder

○ **lo**********@g*****.***** adresine bir bağlantı gönder

Devam et

```
int[861975402486538241]" value="devic
ame="method" value="861975402486538241" checked>

a bir kod gönder
```

s Network Performance Memory Application S
ntainer div.Section form.Form ul.Form-radioList li lab

ibrahim@balicbilisim.com

www.ibrahimbalic.com

www.twitter.com/b4l1c