silo
By Authentic8

FLASH REPORT

Using Genymotion’s Android Virtual Machine and Email Addresses for Social Media Account Discovery

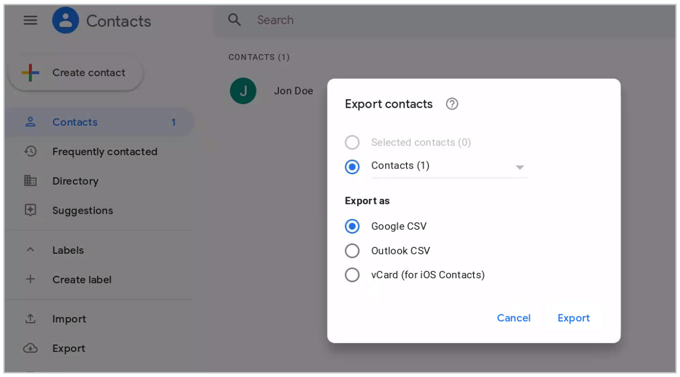
This paper describes how to leverage Genymotion’s Android virtual machine service and Google Contacts to identify social media accounts through the “suggested friends” function. The accounts discovered can be further exploited through other OSINT practices and ultimately incorporated into targeting and pattern of life analysis.

A user will need to identify an email database they wish to exploit. The email database covered in this workflow was discovered on https://ddosecrets.com/data/asia/ “Darkside of the Kremlin CSV Extracts”. The dataset contains information and email addresses for members of the Russian financial industry, oligarchy, and other spheres of influence. The file contains more data than just email addresses, therefore a regex command can be used to parse out the unwanted data, leaving the user with only the email addresses. The regex used to parse the Darkside of the Kremlin file (along with a text editor of choice):

```
\b[A-Z0-9._%+-]+@[A-Z0-9.-]+\.[A-Z]{2,}\b
```

Users can follow the next series of steps to identify social media accounts from the email dump.

1. After extracting emails from the file, a user must now create or log into a “burner” Gmail account to import the email addresses from the Darkside of the Kremlin file.
2. Once in Gmail, the user will need to create a dummy contact in Google Contacts. With the dummy contact created, export the contact as a CSV. This export will give the user the Google accepted CSV format for importing contacts.



Export contacts

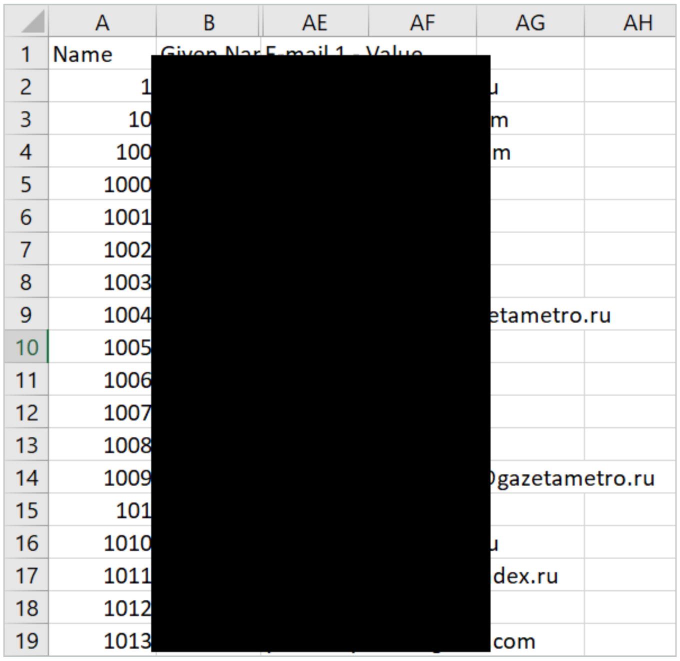
○ Selected contacts (0)
● Contacts (1)

Export as

● Google CSV
○ Outlook CSV
○ vCard (for iOS Contacts)

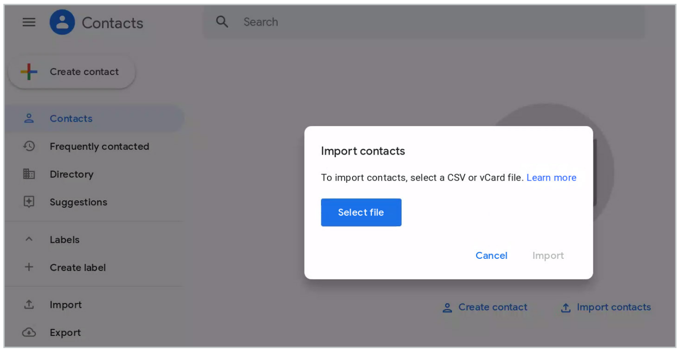
Cancel Export

3. The user must now delete the dummy contact from the Google CSV, and copy and paste the processed email addresses into it. Every email address must have a unique value for the first name field to import seamlessly into Google Contacts; a user should put 1,2,3 etc. in the “first name” field to meet this requirement. The ready-for-import CSV should look like the redacted image to the right.



	A	B	AE	AF	AG	AH
1	Name	[redacted]	[redacted]	[redacted]		
2	1	[redacted]	[redacted]	[redacted]	[redacted]	
3	10	[redacted]	[redacted]	[redacted]	[redacted]	
4	100	[redacted]	[redacted]	[redacted]	[redacted]	
5	1000	[redacted]	[redacted]	[redacted]		
6	1001	[redacted]	[redacted]	[redacted]		
7	1002	[redacted]	[redacted]	[redacted]		
8	1003	[redacted]	[redacted]	[redacted]		
9	1004	[redacted]	[redacted]	[redacted]	[redacted]	
10	1005	[redacted]	[redacted]	[redacted]		
11	1006	[redacted]	[redacted]	[redacted]		
12	1007	[redacted]	[redacted]	[redacted]		
13	1008	[redacted]	[redacted]	[redacted]		
14	1009	[redacted]	[redacted]	[redacted]	[redacted]	
15	101	[redacted]	[redacted]	[redacted]		
16	1010	[redacted]	[redacted]	[redacted]	[redacted]	
17	1011	[redacted]	[redacted]	[redacted]	[redacted]	
18	1012	[redacted]	[redacted]	[redacted]		
19	1013	[redacted]	[redacted]	[redacted]	[redacted]	

4. A user can then import the CSV of contacts filled with Darkside of the Kremlin details.



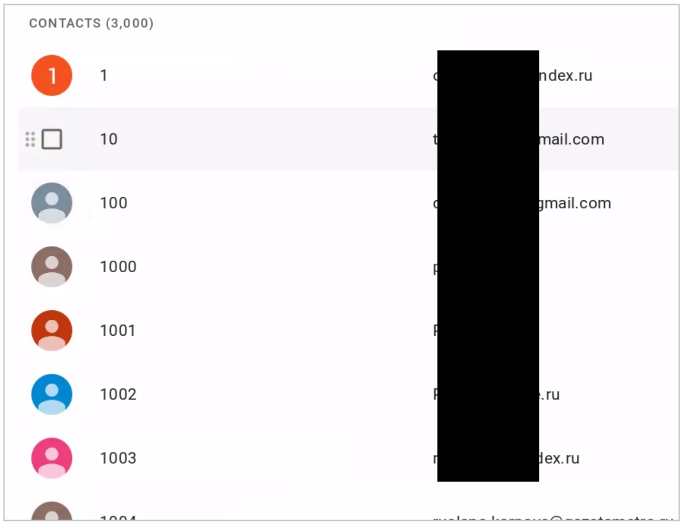
Import contacts

To import contacts, select a CSV or vCard file. Learn more

Select file

Cancel Import

5. Once the upload into Google Contacts is complete, the user should have a similar Contacts list as the redacted image to the right.

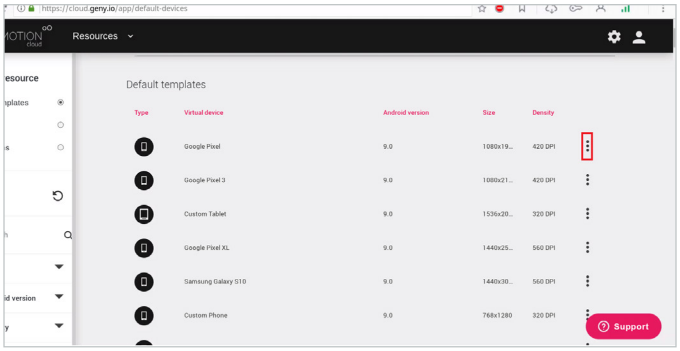

CONTACTS (3,000)

1	[redacted]
10	[redacted]
100	[redacted]
1000	[redacted]
1001	[redacted]
1002	[redacted]
1003	[redacted]

Using an Android VM from Genymotion

Users can now navigate to Genymotion (https://www.genymotion.com/), create an account, and sign in. The user will be signed into the cloud instance of Genymotion (https://cloud.geny.io) after validating the email address for their account. This service has an extensive trial period, then a paid subscription after the trial is over.

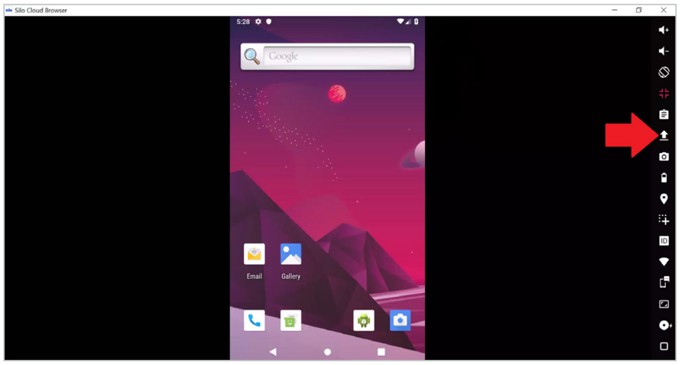
1. Once logged in, a user would launch a VM session, then click on the three vertical dots (see callout) for the desired device and click "Start".

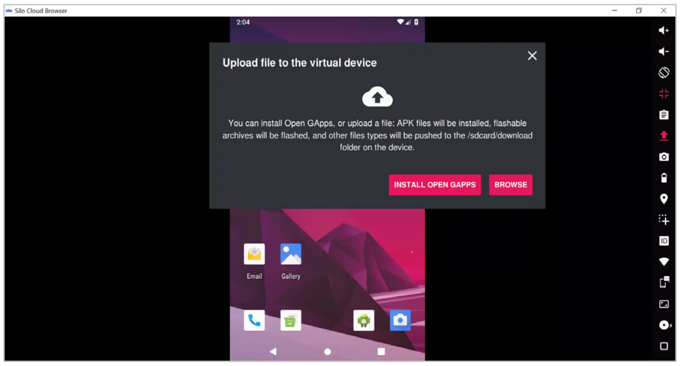


Default templates

Type	Virtual device	Android version	Size	Density
	Google Pixel	9.0	1080x19...	420 DPI
	Google Pixel 3	9.0	1080x21...	420 DPI
	Custom Tablet	9.0	1536x20...	320 DPI
	Google Pixel XL	9.0	1440x25...	560 DPI
	Samsung Galaxy S10	9.0	1440x30...	560 DPI
	Custom Phone	9.0	768x1280	320 DPI

2. Once in the Android VM, the user needs to "Install GApps". The GApps install will allow the user to access the Google Play Store and install the necessary apps to complete the workflow.

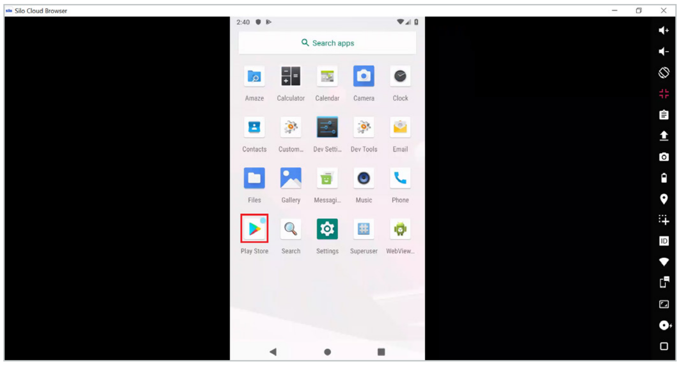




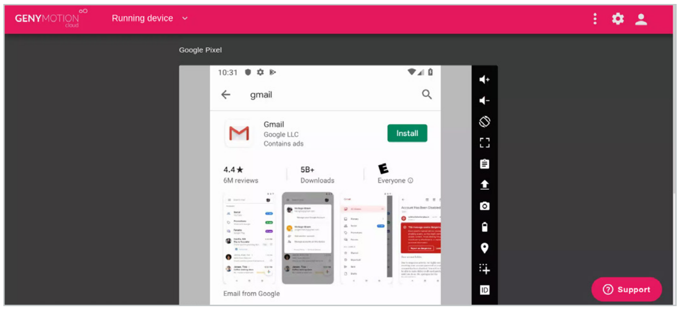
Upload file to the virtual device

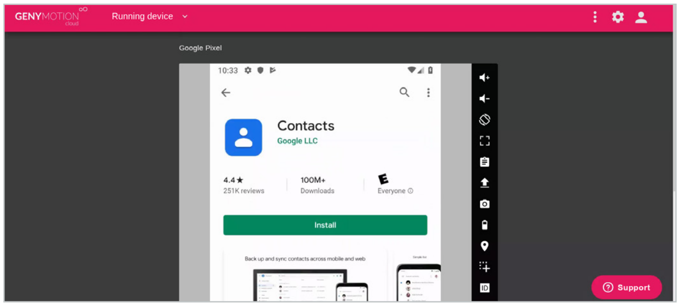
You can install Open GApps, or upload a file: APK files will be installed, flashable archives will be flashed, and other files types will be pushed to the /sdcard/download folder on the device.

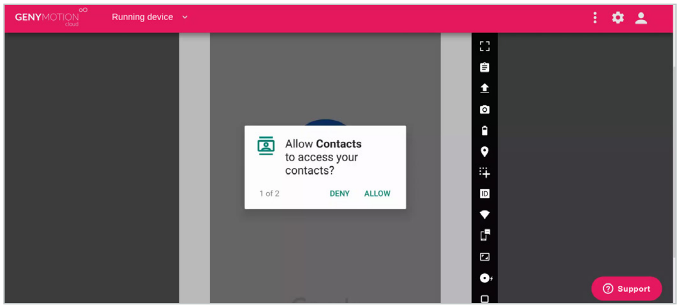
3. The user can now click and drag up from the bottom of the VM to access the Applications menu. Once in the menu, the user can click on "Play Store" and sign in with the burner Gmail account containing the uploaded email contacts.



4. Search Gmail and Google Contacts in the Play Store, install both apps, and ensure that the Google contacts are allowed to sync to your chosen device.

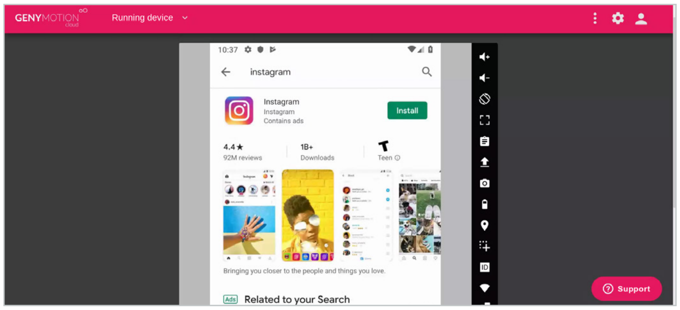






Allow **Contacts** to access your contacts?

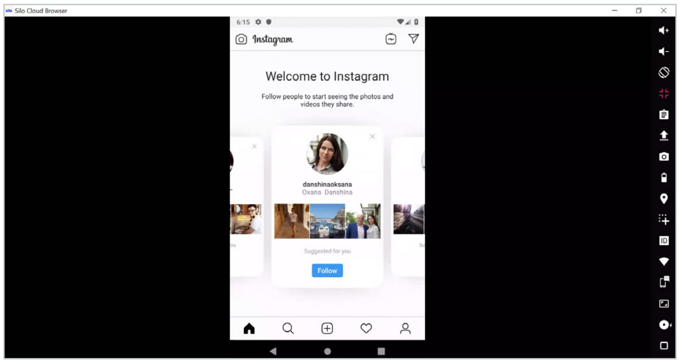
5. The user can now install social media apps via the Play Store. Instagram has been incorporated into this workflow, but a user can replicate it with other social media platforms, such as Facebook, Twitter, etc.



Bringing you closer to the people and things you love.

Related to your Search

6. The image to the right is of an Instagram account created in an VM instance with a burner Gmail address. Instagram provides suggestions for whom the user might want to follow. These suggestions appear because Google Contacts was synced with the device, allowing social media platforms to cross reference the uploaded emails from Google Contacts with, in this case, active Instagram accounts.



Welcome to Instagram

Follow people to start seeing the photos and videos they share.

silo
By Authentic8

CONNECT WITH US

+1 877-659-6535
www.Authentic8.com

PROTECT THE THINGS YOU CARE ABOUT FROM THE THINGS YOU CANNOT TRUST

Authentic8 enables anyone, anywhere, on any device to experience the web without risk. The Silo Web Isolation Platform by Authentic8 separates the things you care about like apps, data and devices, from the things you cannot trust like public websites, external users and unmanaged devices. Silo executes all web code in a secure, isolated environment that is managed by policy, to provide protection and oversight.

Today, the world's most at-risk organizations rely on Silo to deliver trust where it otherwise cannot be guaranteed.