Forensics Investigation of Android Phone using Andriller

October 12, 2015 By Raj Chandel

Andriller – is software utility with a collection of forensic tools for smartphones. It performs read-only, forensically sound, non-destructive acquisition from Android devices. It has other features, such as powerful Lockscreen cracking for Pattern, PIN code, or Password; custom decoders for Apps data from Android (and some Apple iOS) databases for decoding communications. Extraction and decoders produce reports in HTML and Excel (.xlsx) formats.

Features

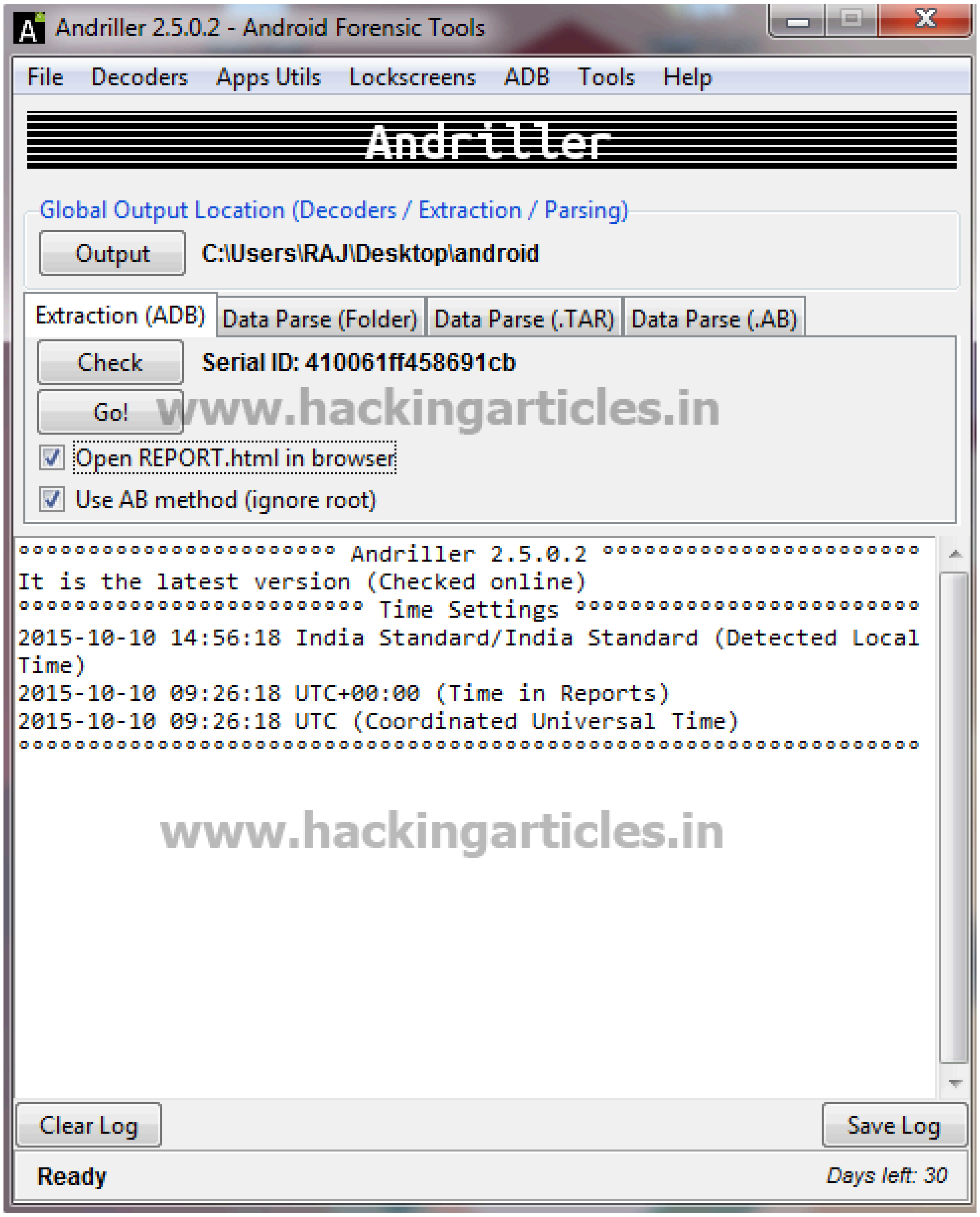
- Automated data extraction and decoding
- Data extraction of non-rooted without devices by Android Backup (Android versions 4.x)
- Data extraction with root permissions: root ADB daemon, CWM recovery mode, or SU binary (Superuser/SuperSU)
- Data parsing and decoding for Folder structure, Tarball files (from nanddroid backups), and Android Backup ('backup.ab' files)
- Selection of individual database decoders for Android and Apple
- Decryption of encrypted WhatsApp archived databases (msgstore.db.crypt, msgstore.db.crypt5, msgstore.db.crypt7, msgstore.db.crypt8)
- Lockscreen cracking for Pattern, PIN, Password
- Unpacking the Android backup files

First Download Andriller from **here** : and install in your Computer.

Now open the Andriller and select output folder. You will get a pop up and select your desired folder.

Now connect your Android phone with computer using Data cable. IN Andriller software click on Check option, if your Android phone is successfully connected with Andriller it will give a Serial ID.

Once you get Serial ID then select the check box which says **Open Report & Use AB method** and click on **GO.**



Global Output Location (Decoders / Extraction / Parsing)

C:\Users\RAJ\Desktop\android

Serial ID: 410061ff458691cb

☑ Open REPORT.html in browser

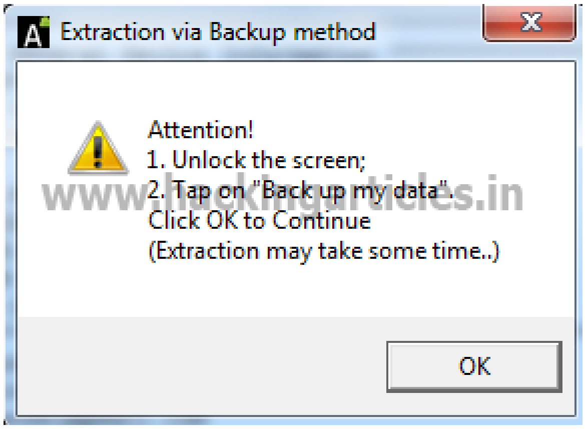
☑ Use AB method (ignore root)

```
°°°°°°°°°°°°°°°°°°°°°°° Andriller 2.5.0.2 °°°°°°°°°°°°°°°°°°°°°°°°
It is the latest version (Checked online)
°°°°°°°°°°°°°°°°°°°°°°°°° Time Settings °°°°°°°°°°°°°°°°°°°°°°°°°
2015-10-10 14:56:18 India Standard/India Standard (Detected Local
Time)
2015-10-10 09:26:18 UTC+00:00 (Time in Reports)
2015-10-10 09:26:18 UTC (Coordinated Universal Time)
°°°°°°°°°°°°°°°°°°°°°°°°°°°°°°°°°°°°°°°°°°°°°°°°°°°°°°°°°°°°°°°°°
```

Ready

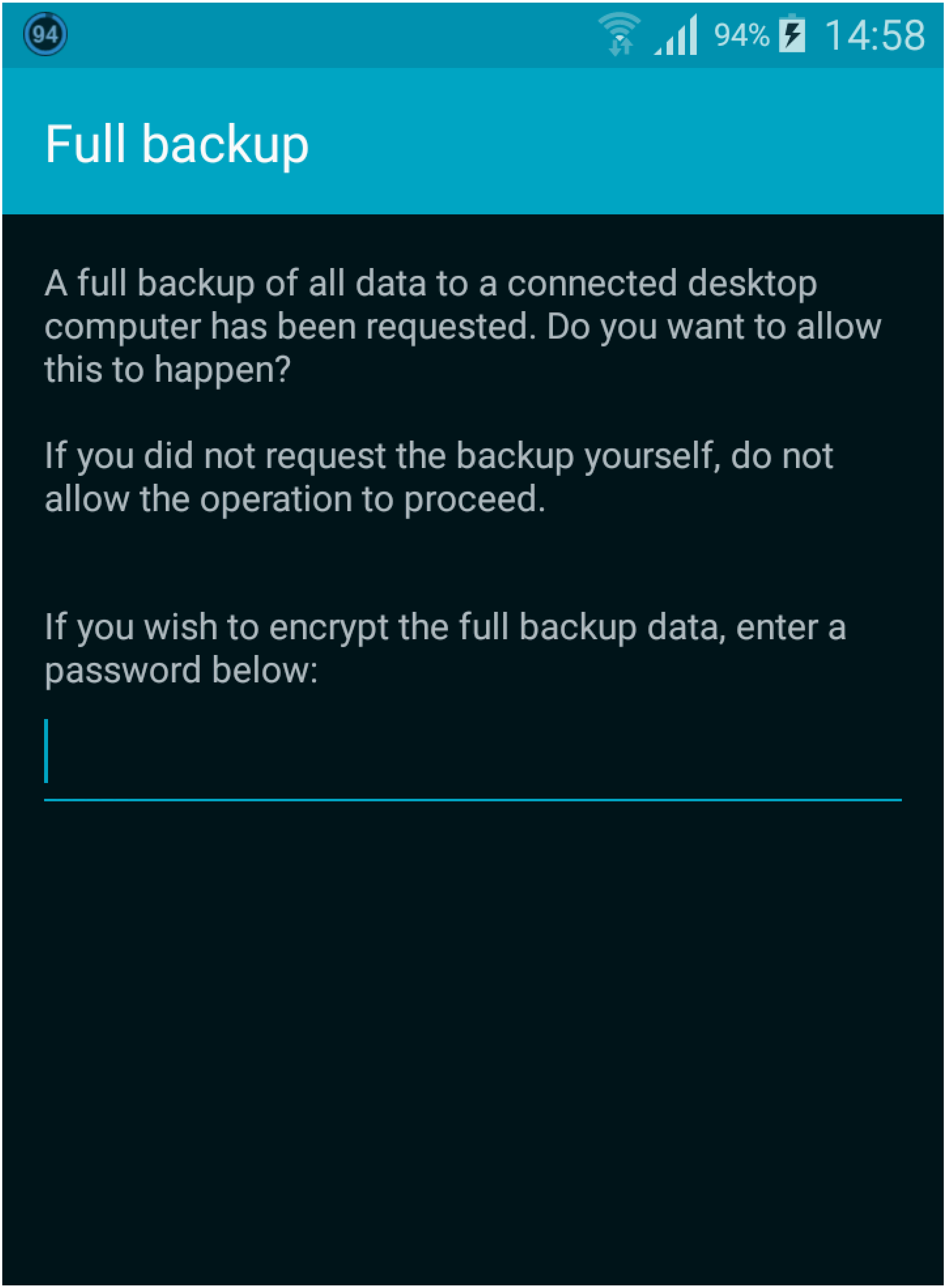
Days left: 30

Your will get a Pop up click ok.



Attention!
1. Unlock the screen;
2. Tap on "Back up my data".
Click OK to Continue
(Extraction may take some time..)

On your Android Phone you will get a screen says Full Back up , at the bottom right of your phone screen you will see **Back up my data** click on that.

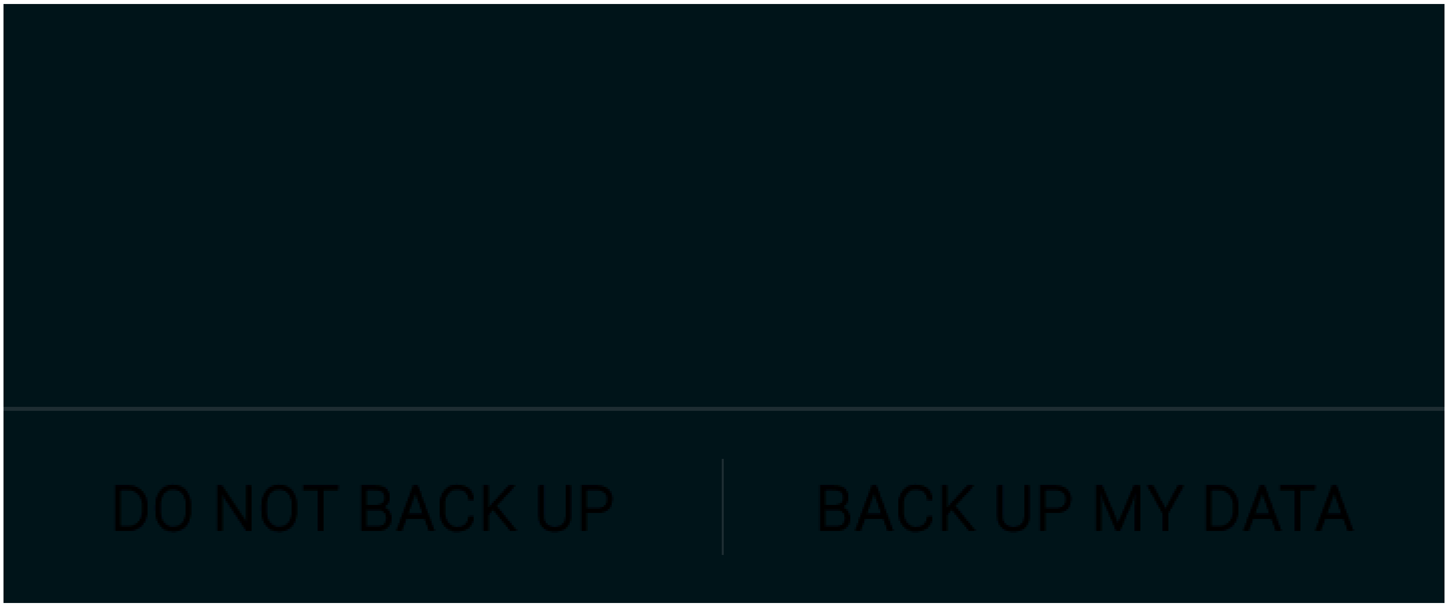


Full backup

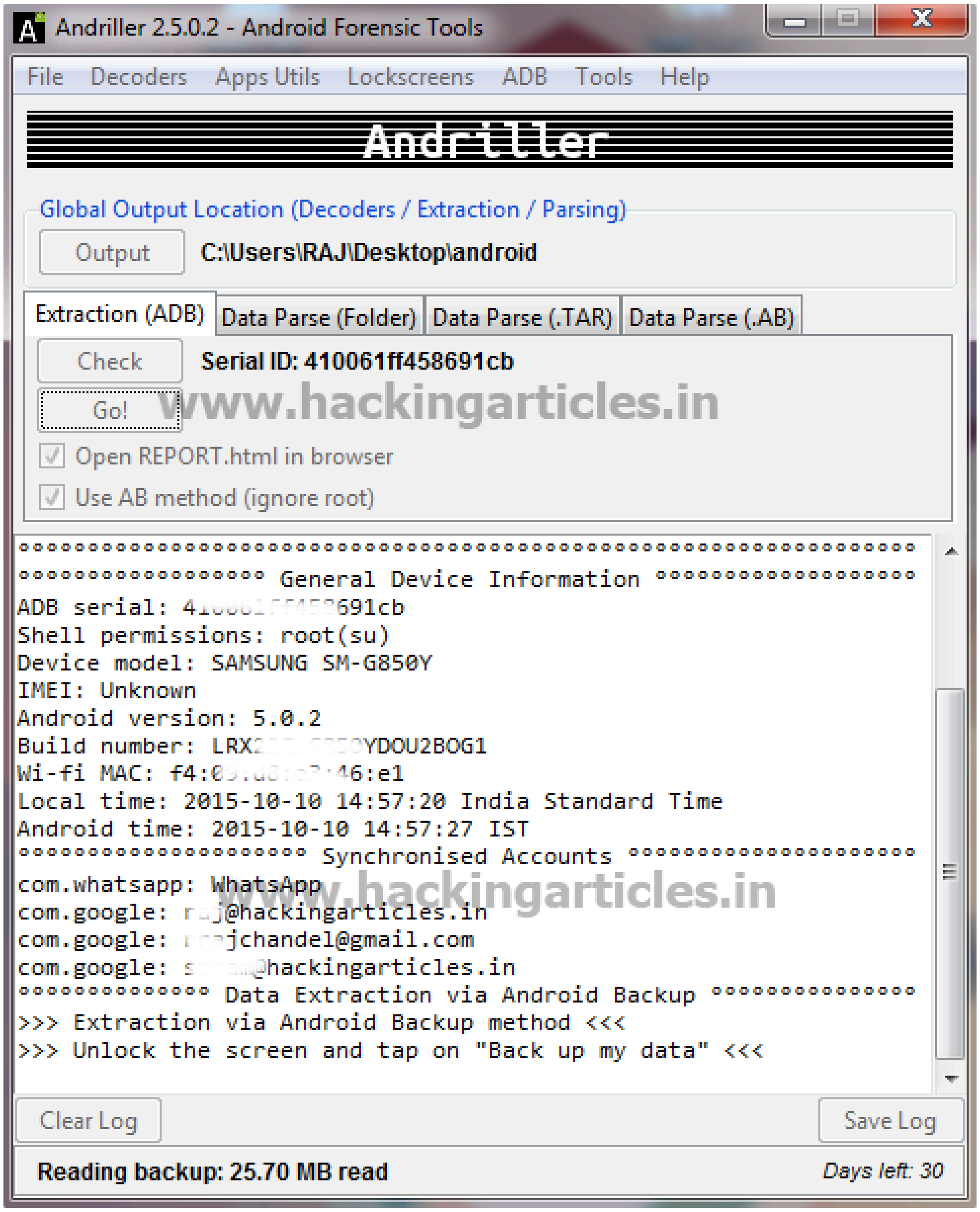
A full backup of all data to a connected desktop computer has been requested. Do you want to allow this to happen?

If you did not request the backup yourself, do not allow the operation to proceed.

If you wish to encrypt the full backup data, enter a password below:



Now Andriller will start taking the Back up of your phone and you can see the logs on Andriller as well.



Global Output Location (Decoders / Extraction / Parsing)

C:\Users\RAJ\Desktop\android

Serial ID: 410061ff458691cb

☑ Open REPORT.html in browser

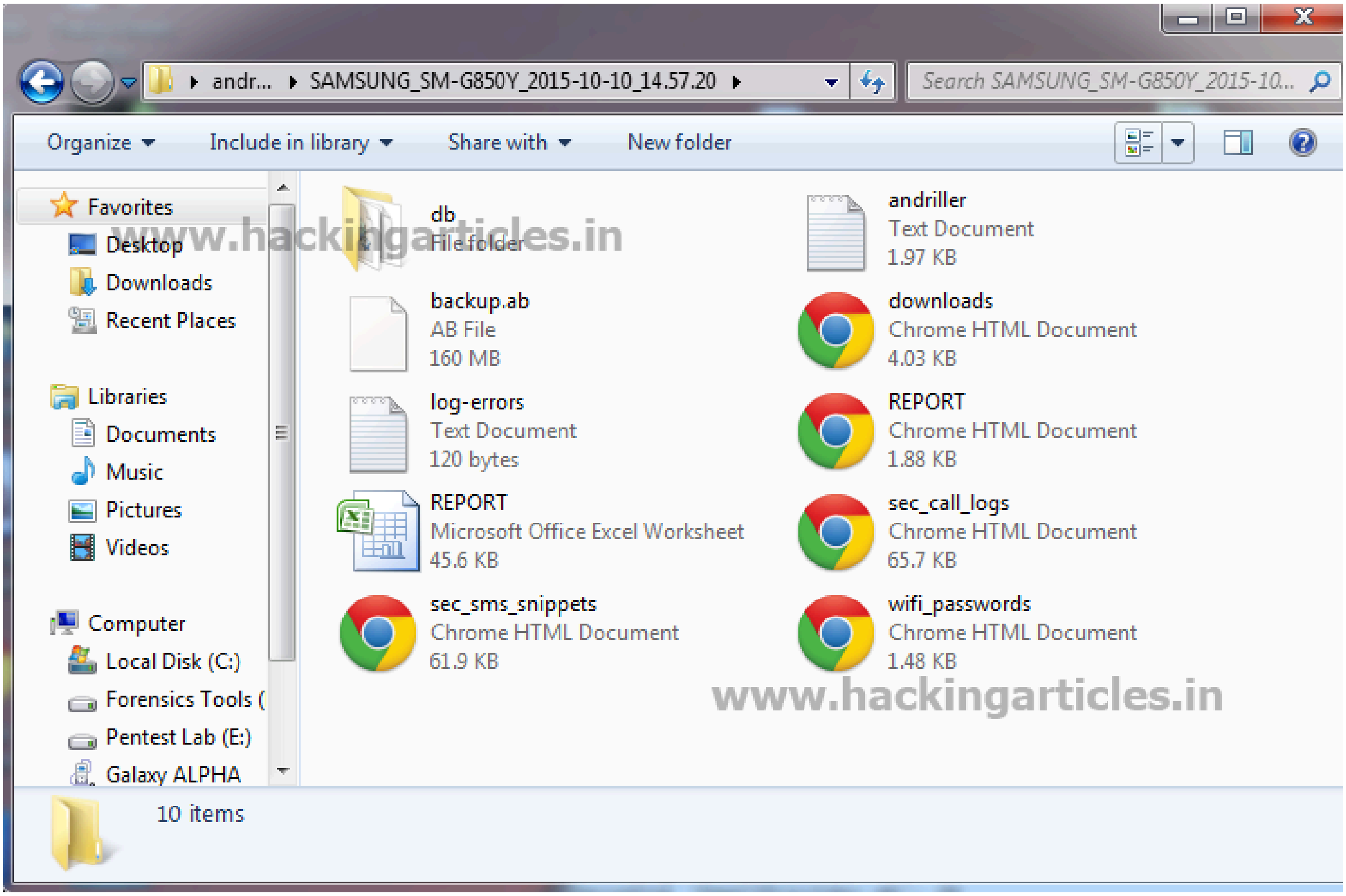
☑ Use AB method (ignore root)

```
°°°°°°°°°°°°°°°°°°°°°°°°°°°°°°°°°°°°°°°°°°°°°°°°°°°°°°°°°°°°°°°°°
°°°°°°°°°°°°°°°°°° General Device Information °°°°°°°°°°°°°°°°°°°
ADB serial: 41[redacted]691cb
Shell permissions: root(su)
Device model: SAMSUNG SM-G850Y
IMEI: Unknown
Android version: 5.0.2
Build number: LRX[redacted]YDOU2BOG1
Wi-fi MAC: f4:[redacted]46:e1
Local time: 2015-10-10 14:57:20 India Standard Time
Android time: 2015-10-10 14:57:27 IST
°°°°°°°°°°°°°°°°°°°°° Synchronised Accounts °°°°°°°°°°°°°°°°°°°°°
com.whatsapp: WhatsApp
com.google: r[redacted]j@hackingarticles.in
com.google: [redacted]jchandel@gmail.com
com.google: s[redacted]@hackingarticles.in
°°°°°°°°°°°°°° Data Extraction via Android Backup °°°°°°°°°°°°°°°
>>> Extraction via Android Backup method <<<
>>> Unlock the screen and tap on "Back up my data" <<<
```

Reading backup: 25.70 MB read

Days left: 30

Once the Backup is complete, you can see the complete data in the folder your selected.



db
File folder

andriller
Text Document
1.97 KB

backup.ab
AB File
160 MB

downloads
Chrome HTML Document
4.03 KB

log-errors
Text Document
120 bytes

REPORT
Chrome HTML Document
1.88 KB

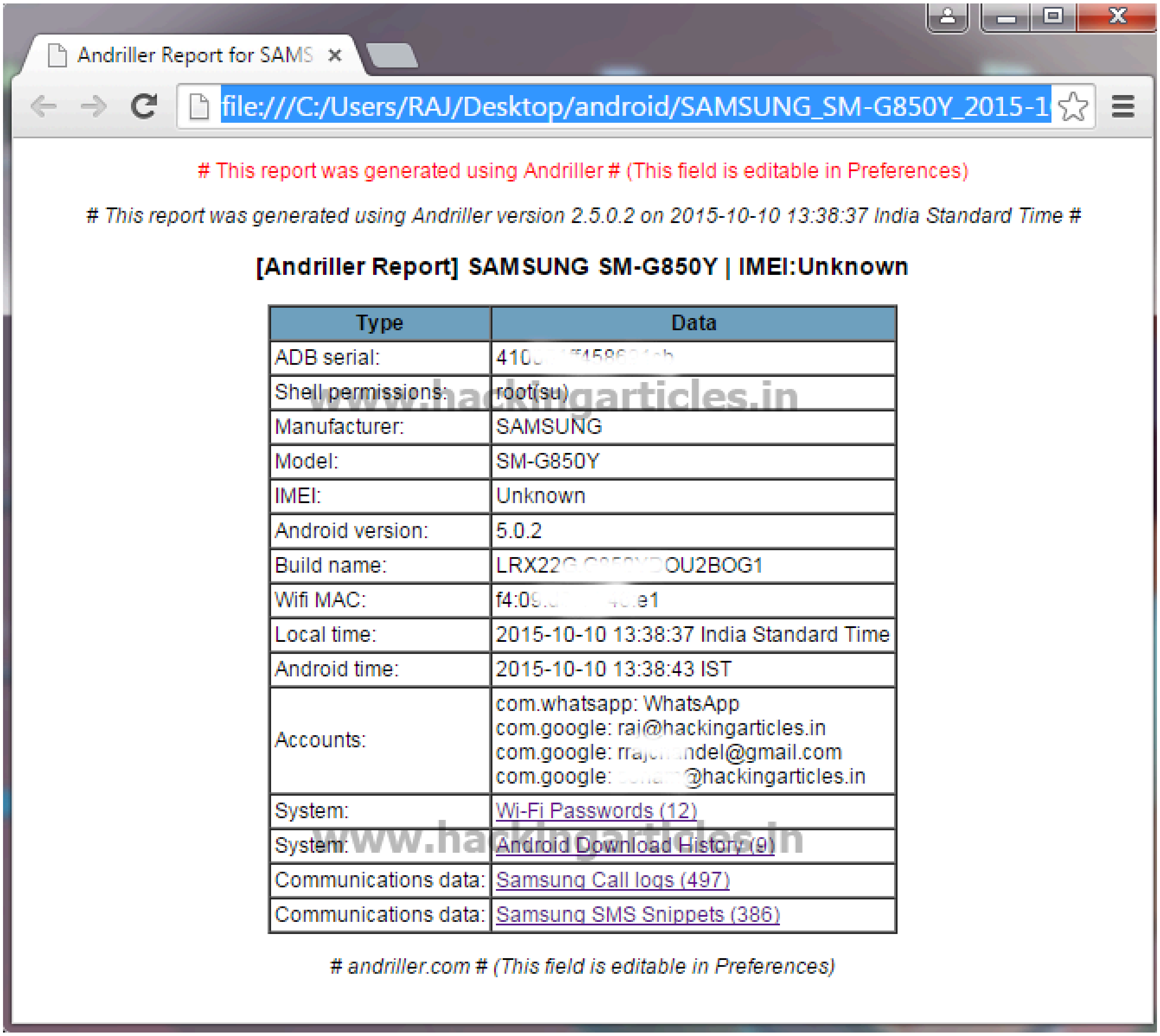
REPORT
Microsoft Office Excel Worksheet
45.6 KB

sec_call_logs
Chrome HTML Document
65.7 KB

sec_sms_snippets
Chrome HTML Document
61.9 KB

wifi_passwords
Chrome HTML Document
1.48 KB

You will see a pop up on your browser which will show you the complete phone report.



Andriller Report for SAMS
file:///C:/Users/RAJ/Desktop/android/SAMSUNG_SM-G850Y_2015-1

This report was generated using Andriller # (This field is editable in Preferences)

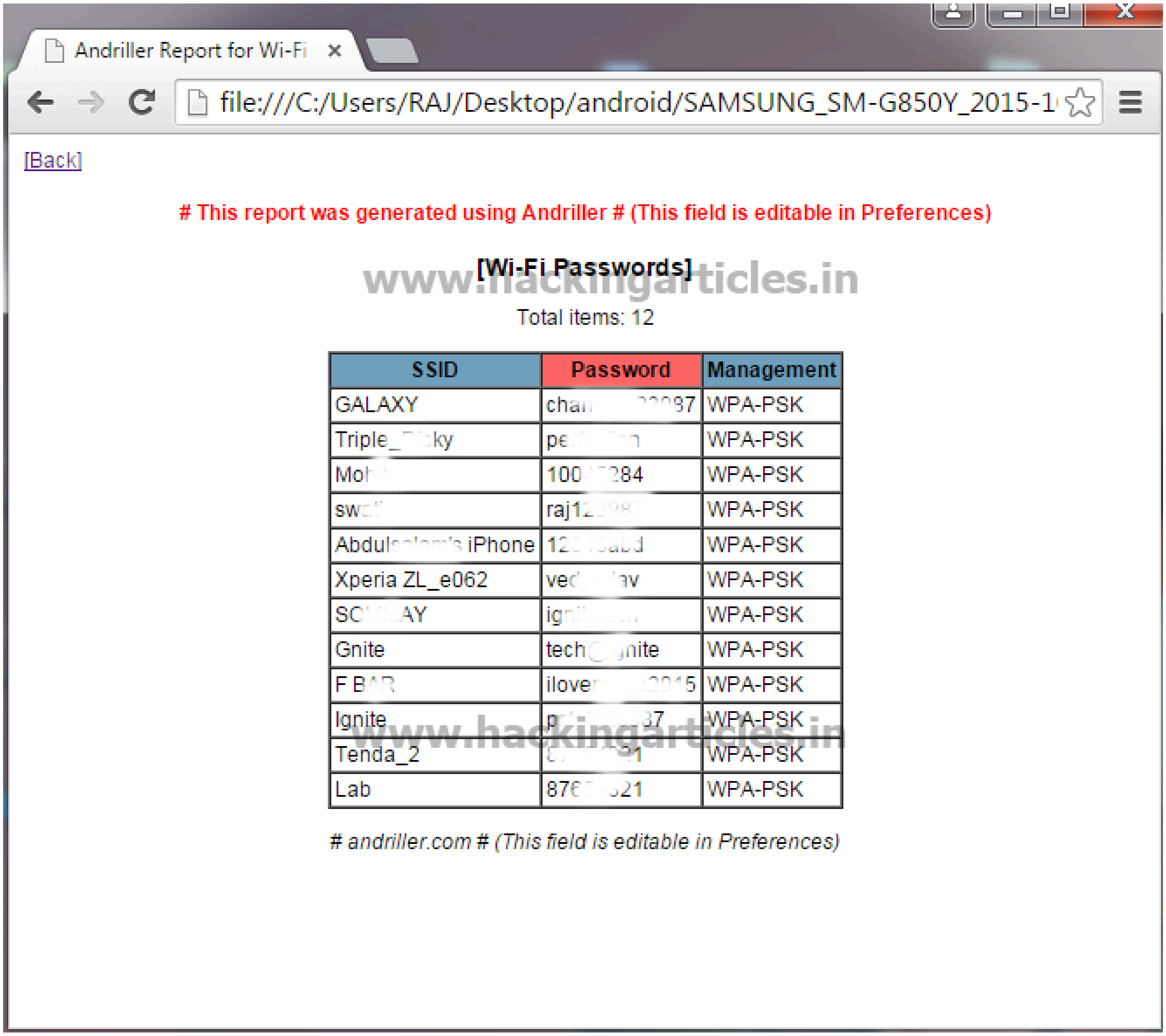
# This report was generated using Andriller version 2.5.0.2 on 2015-10-10 13:38:37 India Standard Time #

[Andriller Report] SAMSUNG SM-G850Y | IMEI:Unknown

Type	Data
ADB serial:	410[redacted]
Shell permissions:	root(su)
Manufacturer:	SAMSUNG
Model:	SM-G850Y
IMEI:	Unknown
Android version:	5.0.2
Build name:	LRX22G[redacted]OU2BOG1
Wifi MAC:	f4:09[redacted]e1
Local time:	2015-10-10 13:38:37 India Standard Time
Android time:	2015-10-10 13:38:43 IST
Accounts:	com.whatsapp: WhatsApp com.google: raj@hackingarticles.in com.google: rraj[redacted]ndel@gmail.com com.google: [redacted]@hackingarticles.in
System:	Wi-Fi Passwords (12)
System:	Android Download History (9)
Communications data:	Samsung Call logs (497)
Communications data:	Samsung SMS Snippets (386)

# andriller.com # (This field is editable in Preferences)

You can select any of the option to see the details as shown in the below image. Example select WiFi password, you will get all the details which is saved under this folder.



Andriller Report for Wi-Fi
file:///C:/Users/RAJ/Desktop/android/SAMSUNG_SM-G850Y_2015-1

[Back]

This report was generated using Andriller # (This field is editable in Preferences)

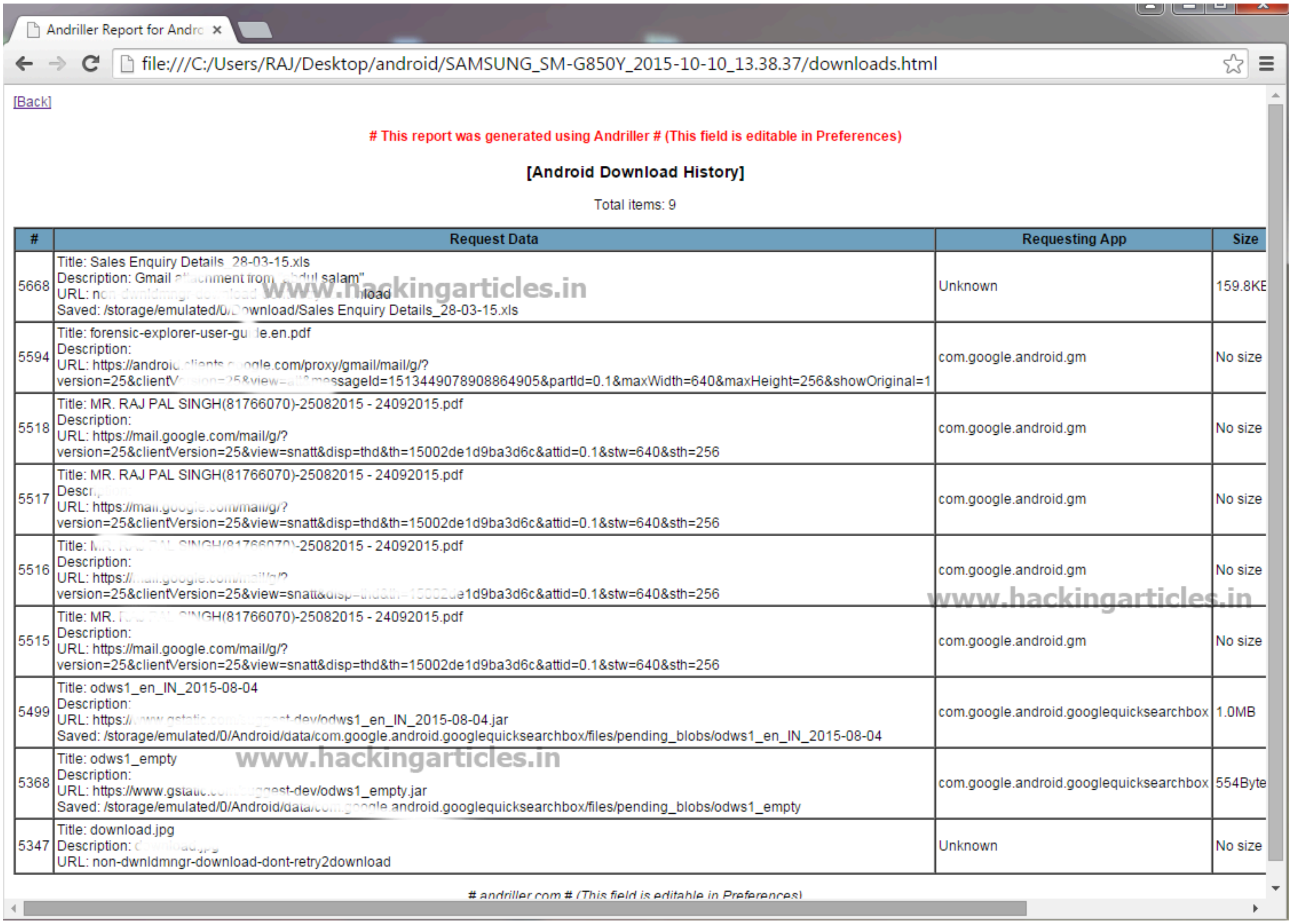
[Wi-Fi Passwords]

Total items: 12

SSID	Password	Management
GALAXY	chan[redacted]87	WPA-PSK
Triple_[redacted]ky	pe[redacted]	WPA-PSK
Moh[redacted]	100[redacted]284	WPA-PSK
sw[redacted]	raj12[redacted]	WPA-PSK
Abdul[redacted] iPhone	12[redacted]	WPA-PSK
Xperia ZL_e062	ved[redacted]av	WPA-PSK
SC[redacted]AY	ig[redacted]	WPA-PSK
Gnite	tech[redacted]nite	WPA-PSK
F B[redacted]R	ilove[redacted]15	WPA-PSK
Ignite	p[redacted]7	WPA-PSK
Tenda_2	[redacted]1	WPA-PSK
Lab	876[redacted]21	WPA-PSK

# andriller.com # (This field is editable in Preferences)

Same way select another option says Android Download history in this you will see all downloads.



Andriller Report for Andrc
file:///C:/Users/RAJ/Desktop/android/SAMSUNG_SM-G850Y_2015-10-10_13.38.37/downloads.html

[Back]

This report was generated using Andriller # (This field is editable in Preferences)

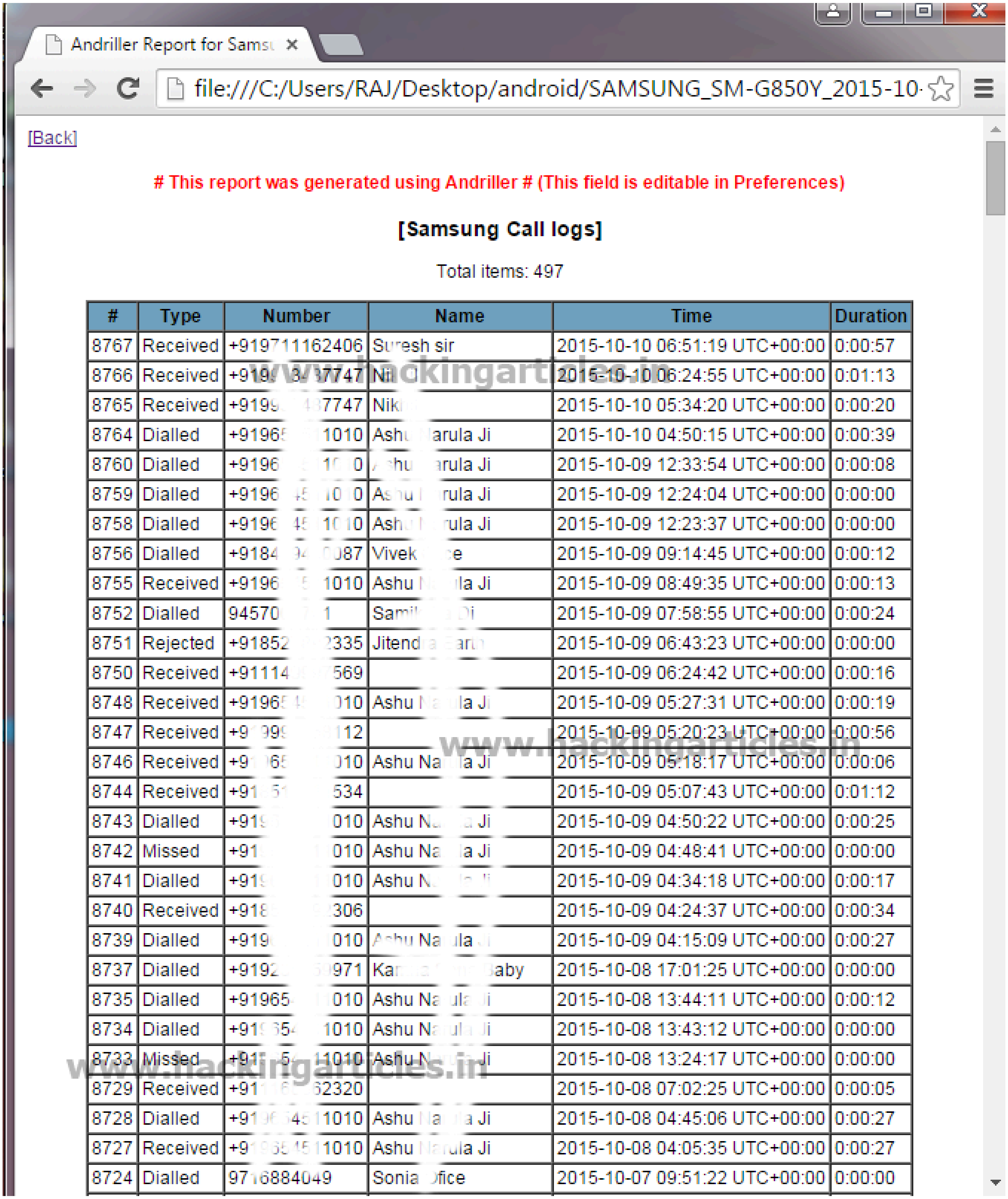
[Android Download History]

Total items: 9

#	Request Data	Requesting App	Size
5668	Title: Sales Enquiry Details_28-03-15.xls Description: Gmail attachment from "abdul salam" URL: non-dwnldmngr-download-dont-retry2download Saved: /storage/emulated/0/Download/Sales Enquiry Details_28-03-15.xls	Unknown	159.8KE
5594	Title: forensic-explorer-user-guide.en.pdf Description: URL: https://android.clients.google.com/proxy/gmail/mail/g/? version=25&clientVersion=25&view=att&messageId=1513449078908864905&partId=0.1&maxWidth=640&maxHeight=256&showOriginal=1	com.google.android.gm	No size
5518	Title: MR. RAJ PAL SINGH(81766070)-25082015 - 24092015.pdf Description: URL: https://mail.google.com/mail/g/? version=25&clientVersion=25&view=snatt&disp=thd&th=15002de1d9ba3d6c&attid=0.1&stw=640&sth=256	com.google.android.gm	No size
5517	Title: MR. RAJ PAL SINGH(81766070)-25082015 - 24092015.pdf Description: URL: https://mail.google.com/mail/g/? version=25&clientVersion=25&view=snatt&disp=thd&th=15002de1d9ba3d6c&attid=0.1&stw=640&sth=256	com.google.android.gm	No size
5516	Title: MR. RAJ PAL SINGH(81766070)-25082015 - 24092015.pdf Description: URL: https://mail.google.com/mail/g/? version=25&clientVersion=25&view=snatt&disp=thd&th=15002de1d9ba3d6c&attid=0.1&stw=640&sth=256	com.google.android.gm	No size
5515	Title: MR. RAJ PAL SINGH(81766070)-25082015 - 24092015.pdf Description: URL: https://mail.google.com/mail/g/? version=25&clientVersion=25&view=snatt&disp=thd&th=15002de1d9ba3d6c&attid=0.1&stw=640&sth=256	com.google.android.gm	No size
5499	Title: odws1_en_IN_2015-08-04 Description: URL: https://www.gstatic.com/suggest-dev/odws1_en_IN_2015-08-04.jar Saved: /storage/emulated/0/Android/data/com.google.android.googlequicksearchbox/files/pending_blobs/odws1_en_IN_2015-08-04	com.google.android.googlequicksearchbox	1.0MB
5368	Title: odws1_empty Description: URL: https://www.gstatic.com/suggest-dev/odws1_empty.jar Saved: /storage/emulated/0/Android/data/com.google.android.googlequicksearchbox/files/pending_blobs/odws1_empty	com.google.android.googlequicksearchbox	554Byte
5347	Title: download.jpg Description: download.jpg URL: non-dwnldmngr-download-dont-retry2download	Unknown	No size

# andriller.com # (This field is editable in Preferences)

Same way select another option says Android Call logs in this you will see all Call details.



Andriller Report for Samsu
file:///C:/Users/RAJ/Desktop/android/SAMSUNG_SM-G850Y_2015-10-

[Back]

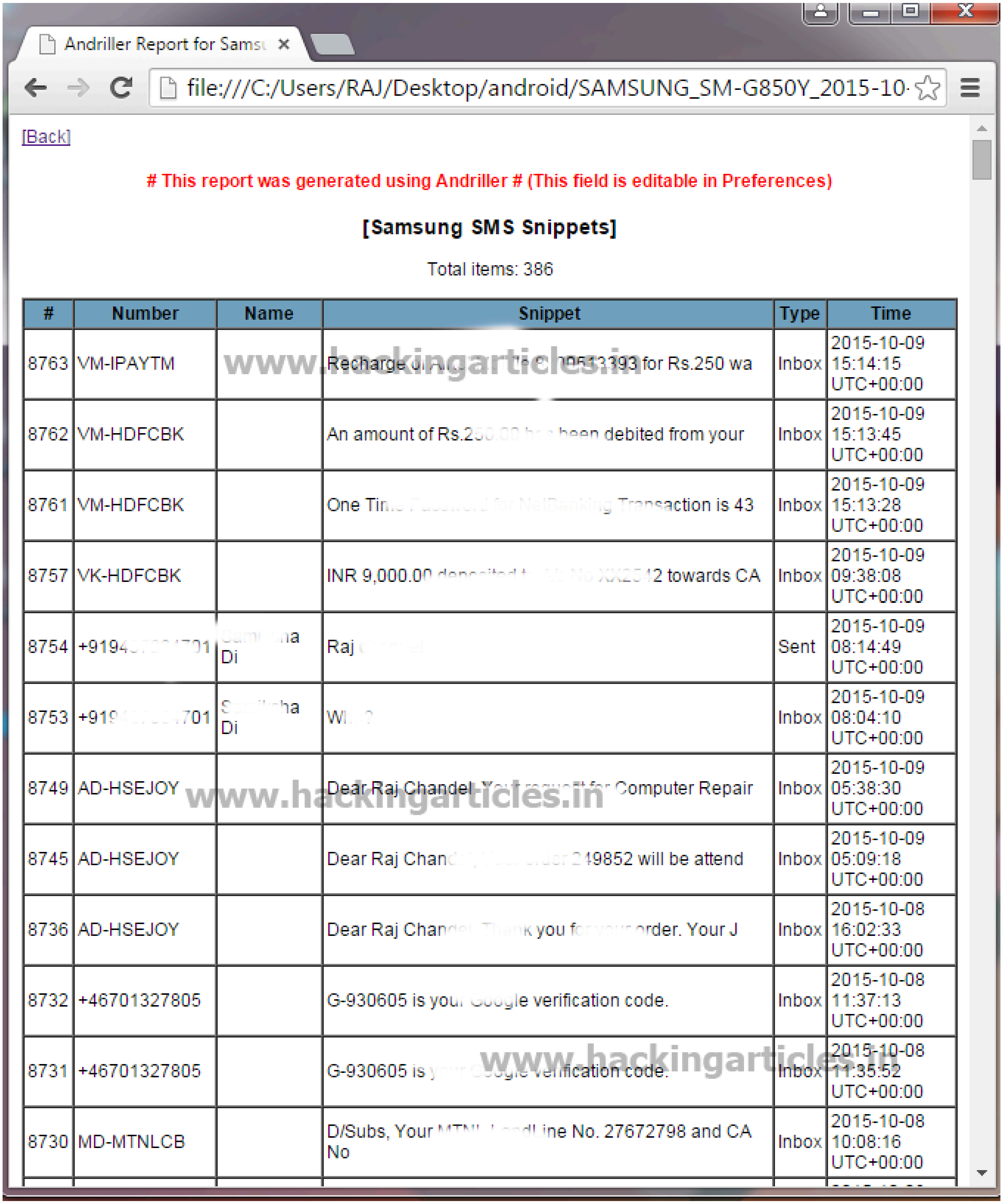
This report was generated using Andriller # (This field is editable in Preferences)

[Samsung Call logs]

Total items: 497

#	Type	Number	Name	Time	Duration
8767	Received	+919711162406	Suresh sir	2015-10-10 06:51:19 UTC+00:00	0:00:57
8766	Received	+919 3 37747	Ni	2015-10-10 06:24:55 UTC+00:00	0:01:13
8765	Received	+919 87747	Nik	2015-10-10 05:34:20 UTC+00:00	0:00:20
8764	Dialled	+91965 1010	Ashu arula Ji	2015-10-10 04:50:15 UTC+00:00	0:00:39
8760	Dialled	+9196 1 0	hu arula Ji	2015-10-09 12:33:54 UTC+00:00	0:00:08
8759	Dialled	+9196 5 10 0	A u rula Ji	2015-10-09 12:24:04 UTC+00:00	0:00:00
8758	Dialled	+9196 45 10 0	Ash rula Ji	2015-10-09 12:23:37 UTC+00:00	0:00:00
8756	Dialled	+9184 4 087	Vivek e	2015-10-09 09:14:45 UTC+00:00	0:00:12
8755	Received	+9196 1010	Ashu la Ji	2015-10-09 08:49:35 UTC+00:00	0:00:13
8752	Dialled	94570 7 1	Sami Di	2015-10-09 07:58:55 UTC+00:00	0:00:24
8751	Rejected	+91852 2335	Jitend arth	2015-10-09 06:43:23 UTC+00:00	0:00:00
8750	Received	+91114 569		2015-10-09 06:24:42 UTC+00:00	0:00:16
8748	Received	+9196 010	Ashu la Ji	2015-10-09 05:27:31 UTC+00:00	0:00:19
8747	Received	+9 99 112		2015-10-09 05:20:23 UTC+00:00	0:00:56
8746	Received	+9 65 010	Ashu Na la Ji	2015-10-09 05:18:17 UTC+00:00	0:00:06
8744	Received	+91 5 534		2015-10-09 05:07:43 UTC+00:00	0:01:12
8743	Dialled	+919 010	Ashu N Ji	2015-10-09 04:50:22 UTC+00:00	0:00:25
8742	Missed	+91 010	Ashu Na la Ji	2015-10-09 04:48:41 UTC+00:00	0:00:00
8741	Dialled	+919 010	Ashu N	2015-10-09 04:34:18 UTC+00:00	0:00:17
8740	Received	+918 306		2015-10-09 04:24:37 UTC+00:00	0:00:34
8739	Dialled	+919 010	hu Na ula	2015-10-09 04:15:09 UTC+00:00	0:00:27
8737	Dialled	+9192 971	Ka aby	2015-10-08 17:01:25 UTC+00:00	0:00:00
8735	Dialled	+91965 010	Ashu Na ul	2015-10-08 13:44:11 UTC+00:00	0:00:12
8734	Dialled	+91 54 1010	Ashu N ul	2015-10-08 13:43:12 UTC+00:00	0:00:00
8733	Missed	+91 5 11010	Ashu N Ji	2015-10-08 13:24:17 UTC+00:00	0:00:00
8729	Received	+91 62320		2015-10-08 07:02:25 UTC+00:00	0:00:05
8728	Dialled	+91 45 11010	Ashu a Ji	2015-10-08 04:45:06 UTC+00:00	0:00:27
8727	Received	+9 11010	Ashu ula Ji	2015-10-08 04:05:35 UTC+00:00	0:00:27
8724	Dialled	97 6884049	Sonia fice	2015-10-07 09:51:22 UTC+00:00	0:00:00

Same way select another option says SMS Snippets in this you will see all Overview.


Andriller Report for Samsu
file:///C:/Users/RAJ/Desktop/android/SAMSUNG_SM-G850Y_2015-10-

[Back]

This report was generated using Andriller # (This field is editable in Preferences)

[Samsung SMS Snippets]

Total items: 386

#	Number	Name	Snippet	Type	Time
8763	VM-IPAYTM		Recharge [redacted]9513393 for Rs.250 wa	Inbox	2015-10-09 15:14:15 UTC+00:00
8762	VM-HDFCBK		An amount of Rs.2[redacted] been debited from your	Inbox	2015-10-09 15:13:45 UTC+00:00
8761	VM-HDFCBK		One Ti[redacted] Transaction is 43	Inbox	2015-10-09 15:13:28 UTC+00:00
8757	VK-HDFCBK		INR 9,000.00 [redacted]2 towards CA	Inbox	2015-10-09 09:38:08 UTC+00:00
8754	+9194[redacted]701	[redacted]a Di	Raj [redacted]	Sent	2015-10-09 08:14:49 UTC+00:00
8753	+919[redacted]701	S[redacted]ha Di	Wh[redacted]	Inbox	2015-10-09 08:04:10 UTC+00:00
8749	AD-HSEJOY		Dear Raj Chandel [redacted] Computer Repair	Inbox	2015-10-09 05:38:30 UTC+00:00
8745	AD-HSEJOY		Dear Raj Chan[redacted]49852 will be attend	Inbox	2015-10-09 05:09:18 UTC+00:00
8736	AD-HSEJOY		Dear Raj Chan[redacted]k you f[redacted]order. Your J	Inbox	2015-10-08 16:02:33 UTC+00:00
8732	+46701327805		G-930605 is you[redacted]le verification code.	Inbox	2015-10-08 11:37:13 UTC+00:00
8731	+46701327805		G-930605 is y[redacted]verification code.	Inbox	2015-10-08 11:35:52 UTC+00:00
8730	MD-MTNLCB		D/Subs, Your MTN[redacted]dLine No. 27672798 and CA No	Inbox	2015-10-08 10:08:16 UTC+00:00