

Forensic Investigation of Any Mobile Phone with MOBILedit Forensic

November 2, 2015 By Raj Chandel

With MOBILedit Forensic you can view, search or retrieve all data from a phone with only a few clicks. This data includes call history, phonebook, text messages, multimedia messages, files, calendars, notes, reminders and raw application data. It will also retrieve all phone information such as IMEI, operating systems, firmware including SIM details (IMSI), ICCID and location area information. Where possible MOBILedit Forensic is also able to retrieve deleted data from phones and bypass the passcode, PIN and phone backup encryption.

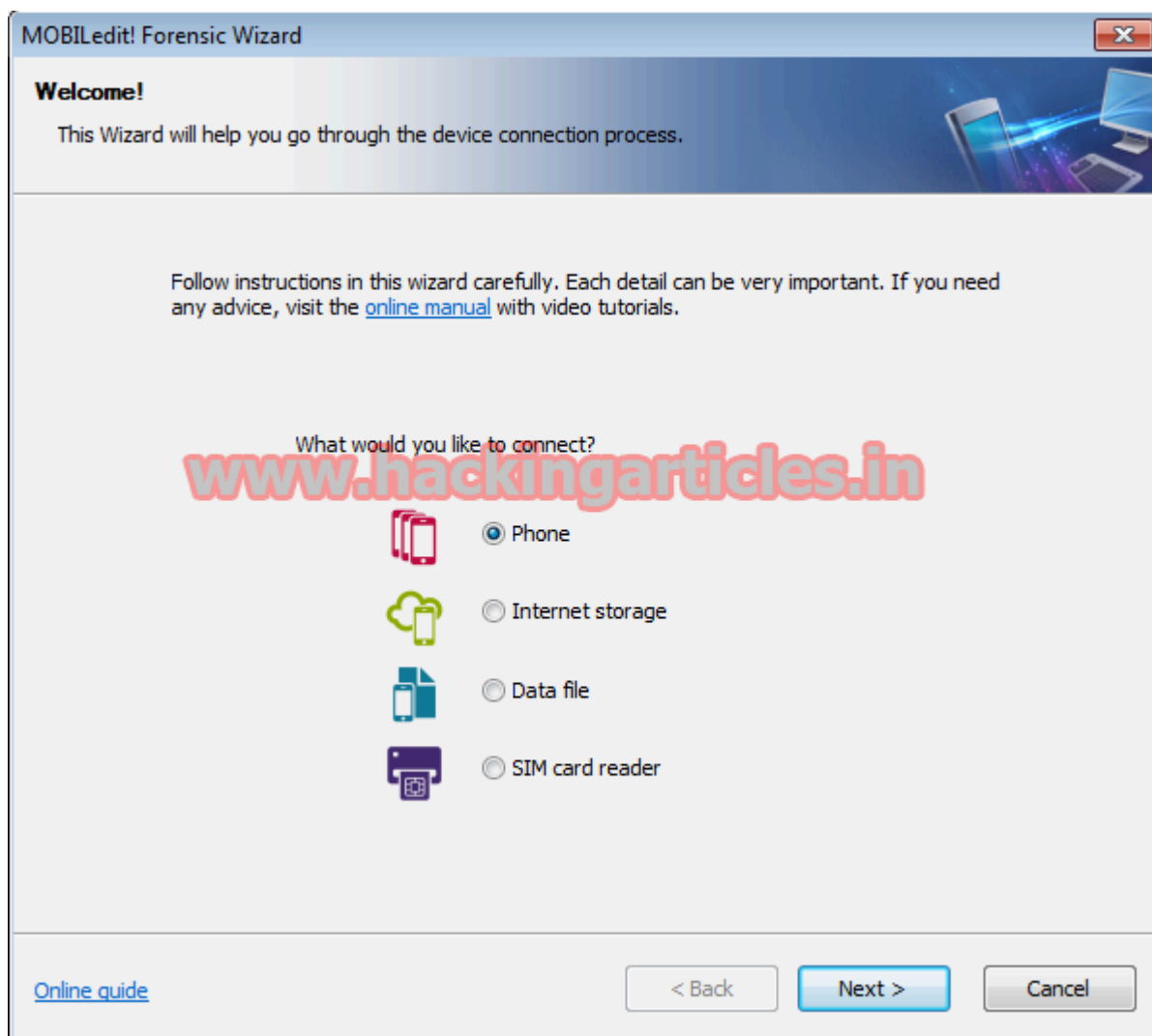
Note: USB Debugging must be enabled.

Download the MOBILedit! Forensic from [here](#) & Install on your PC. Now Click on MOBILedit! Forensic.

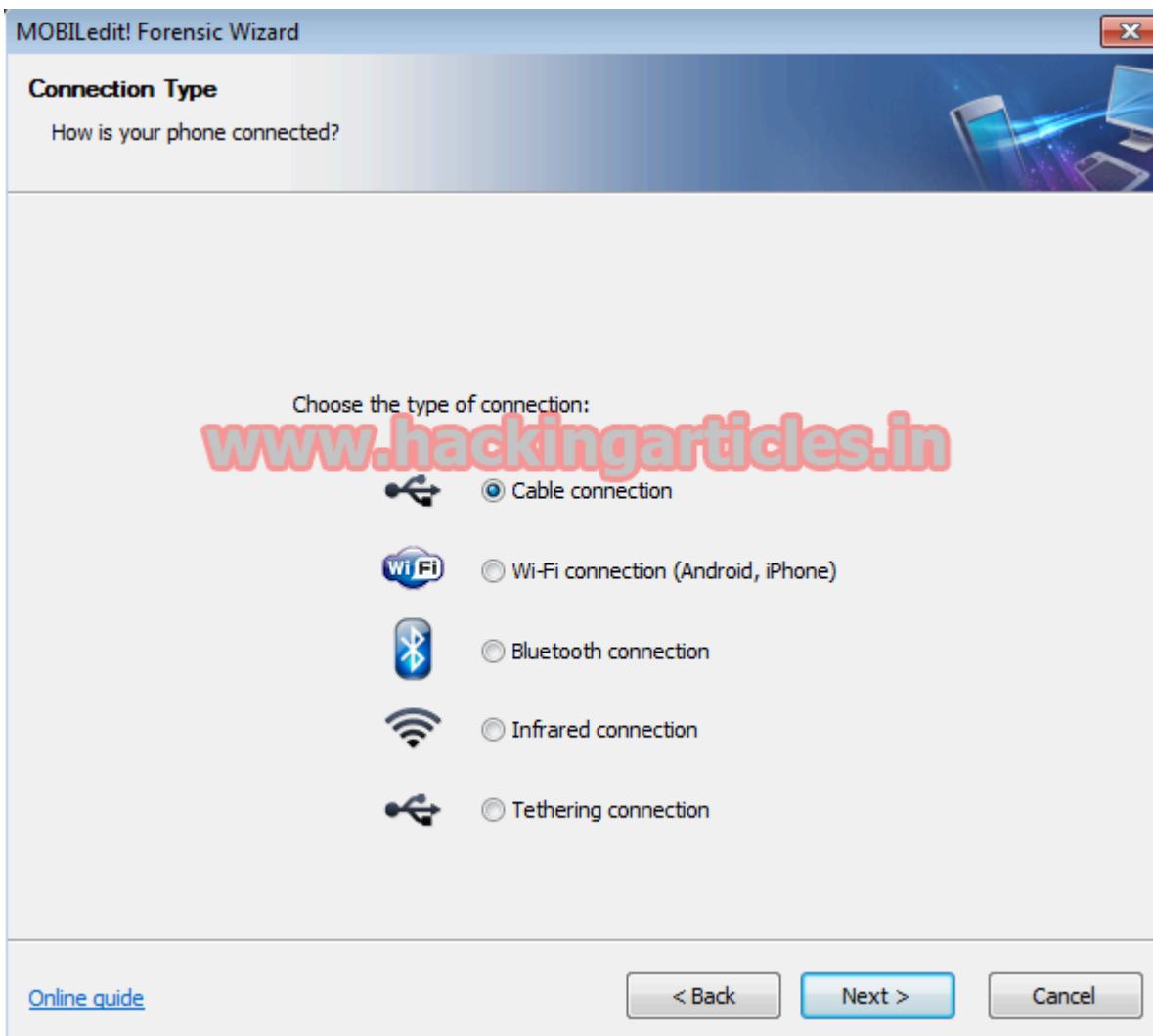
Click on Connect Option. MOBILEedit! Forensic Wizard will run and ask for Phone, Data file or SIM Card.

Select Phone Option. Click on Next.



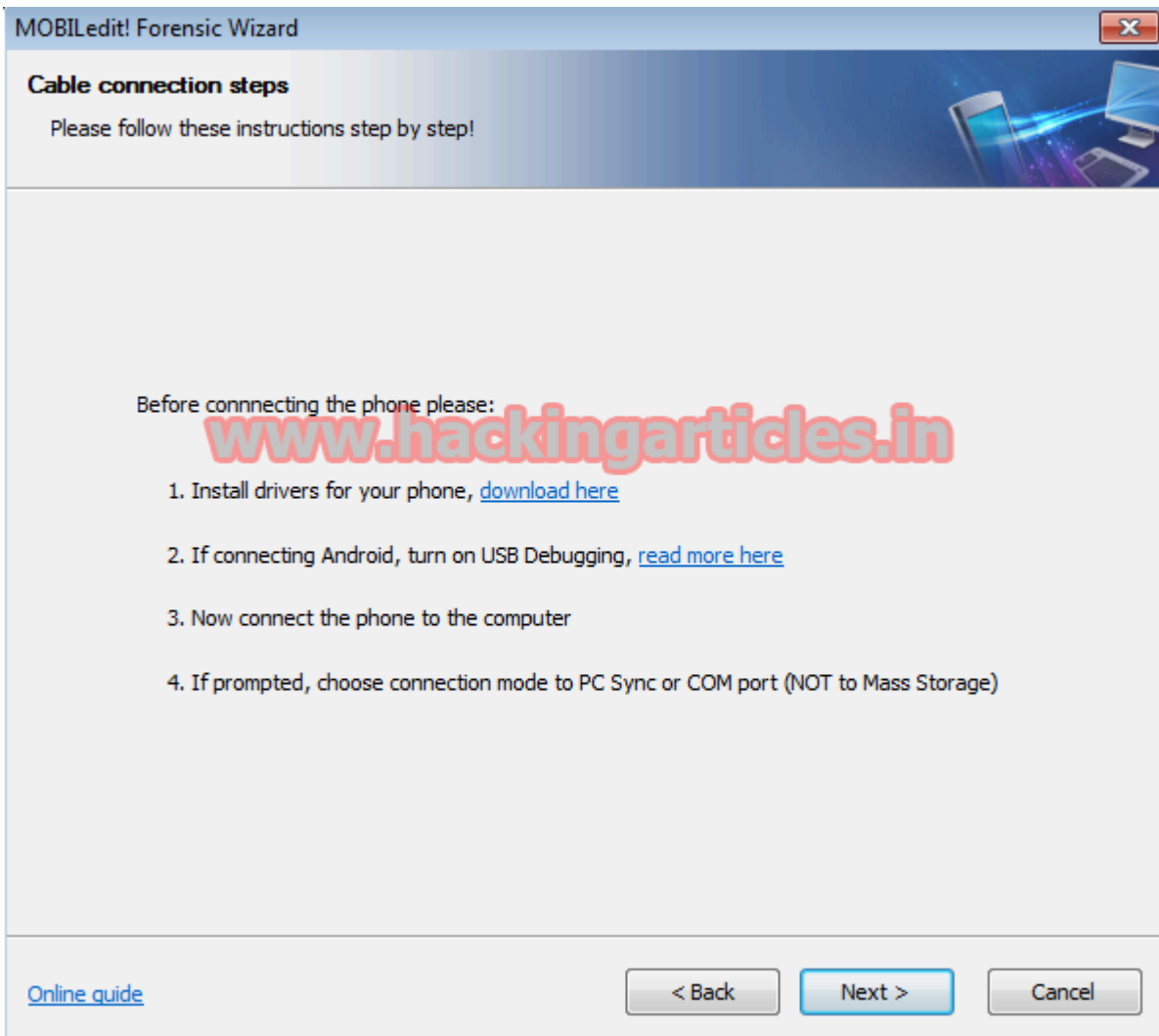


Now it will ask for type of connection. Select **Cable Connection**. And click on Next.

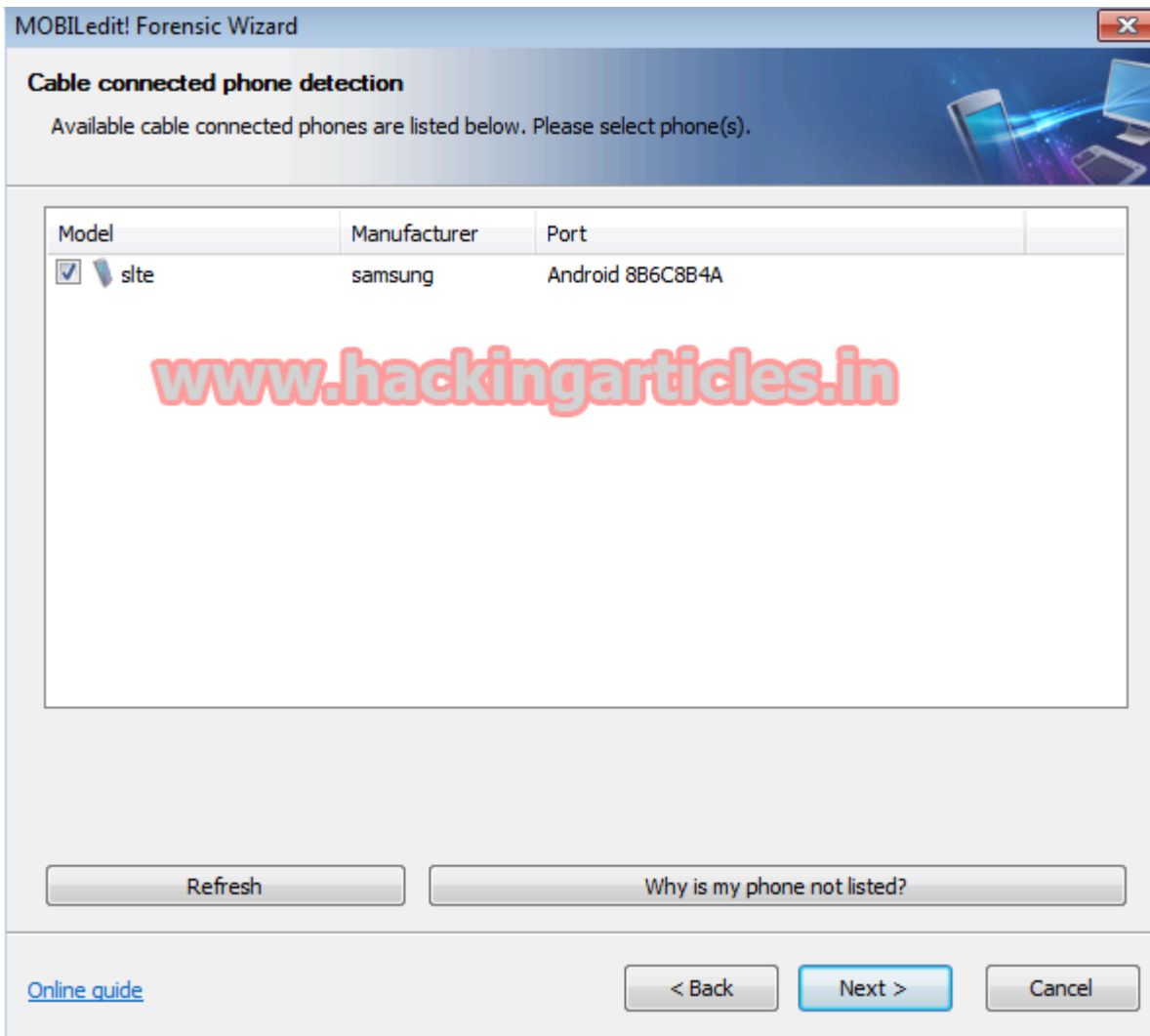


Now follow the instructions such as install Driver or turn on USB debugging if connecting Android.

Now connect the phone via data cable. If prompted choose connection mode to **PC Sync** or **COM port**. Click on **Next Option**.



It will show the connected mobile. Check your Mobile model and click on **Next**.



To take the Backup, first of all enter Owner Name, Device Evidence Number and Owner Phone Number.

Click on **Browse** Option to select the path folder where backup data will be stored and click on **Next**.

MOBILedit! Forensic Wizard

Backup settings

Please set the following options for your backup.

Device Label:

Device Name: Device Evidence Number:

Owner Name: Owner Phone Number:

Phone Notes:

Device Capabilities

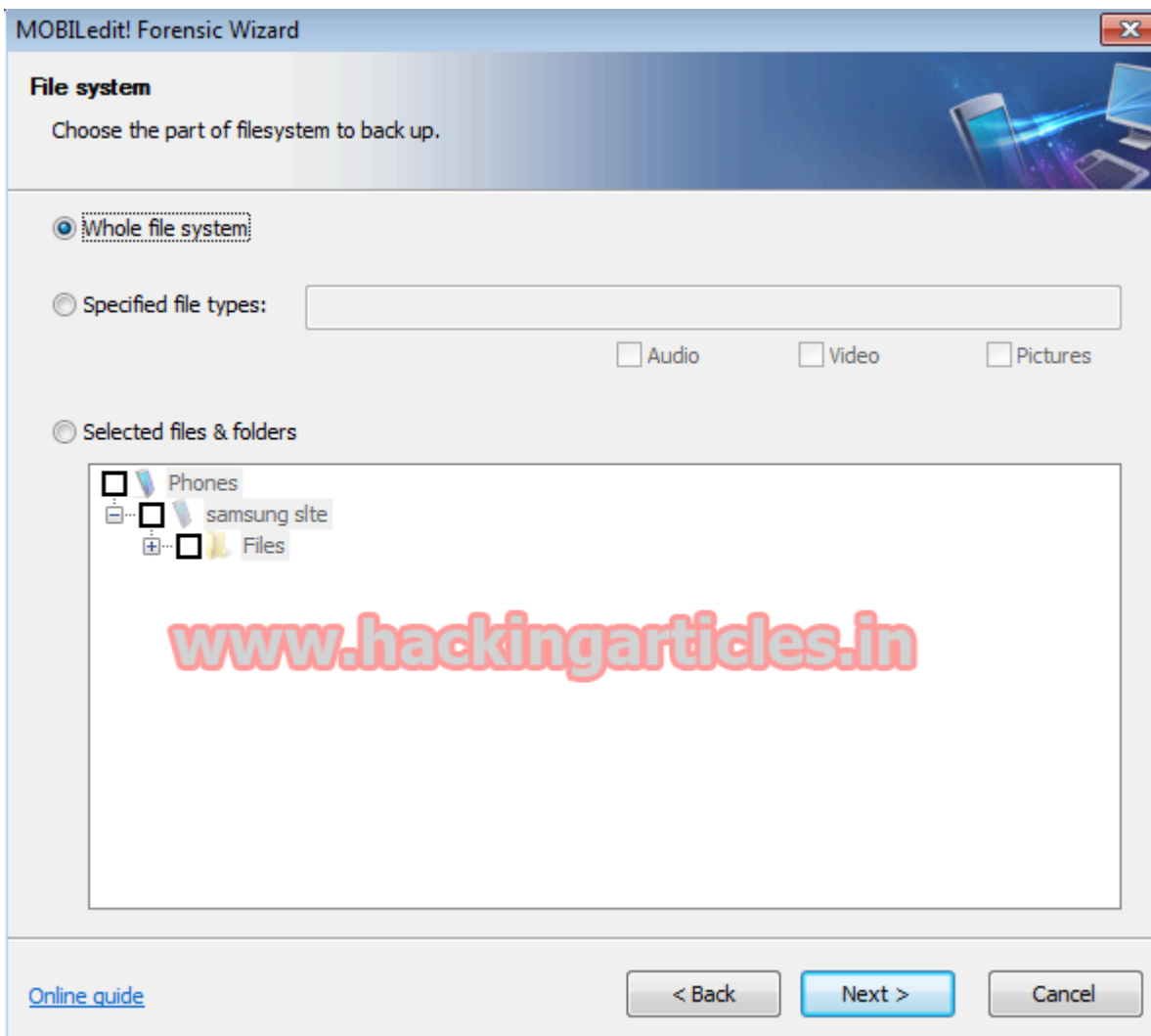
☒ Files

Communication Log Of Backup Operation

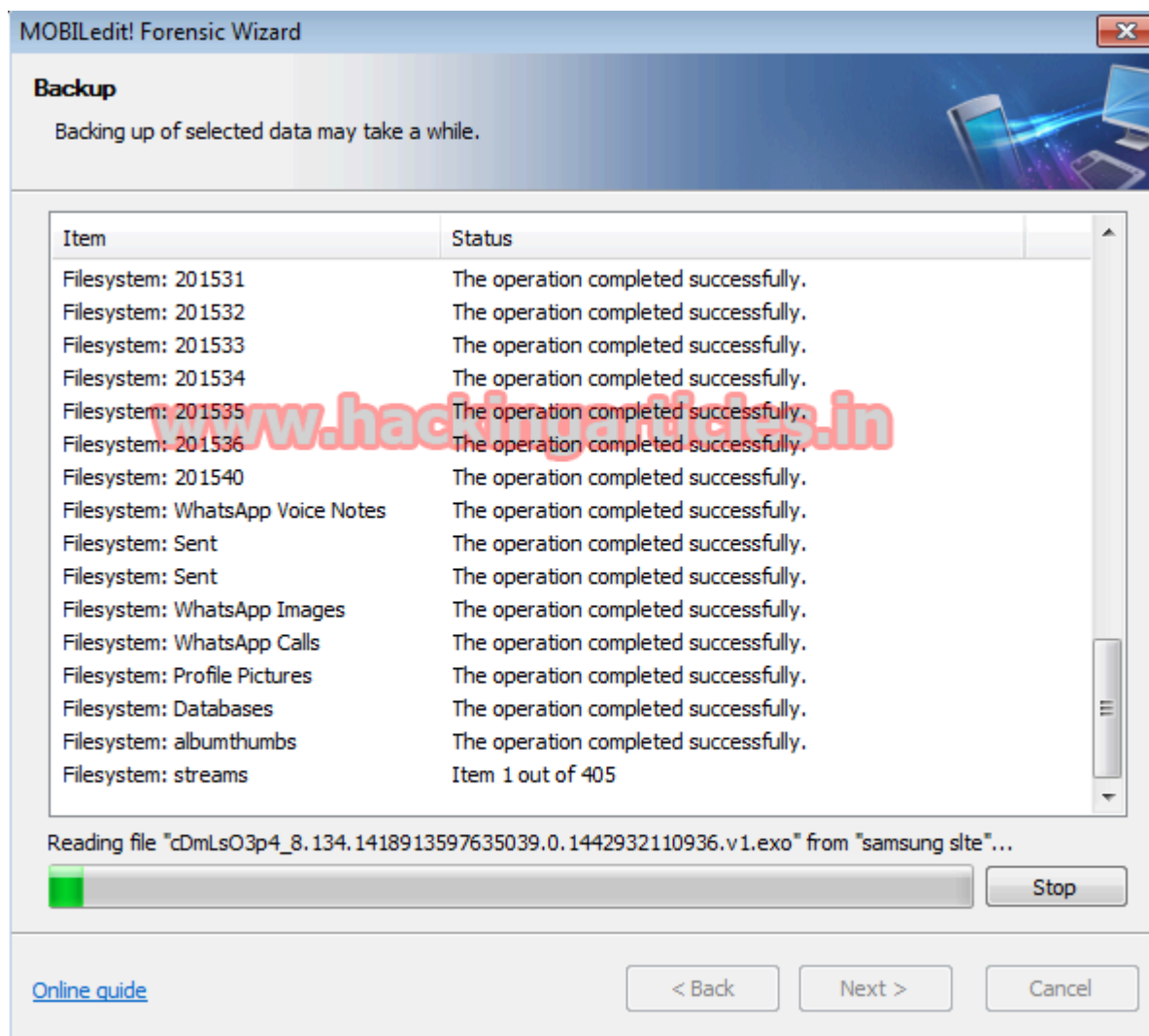
☒ Create:

[Online guide](#)

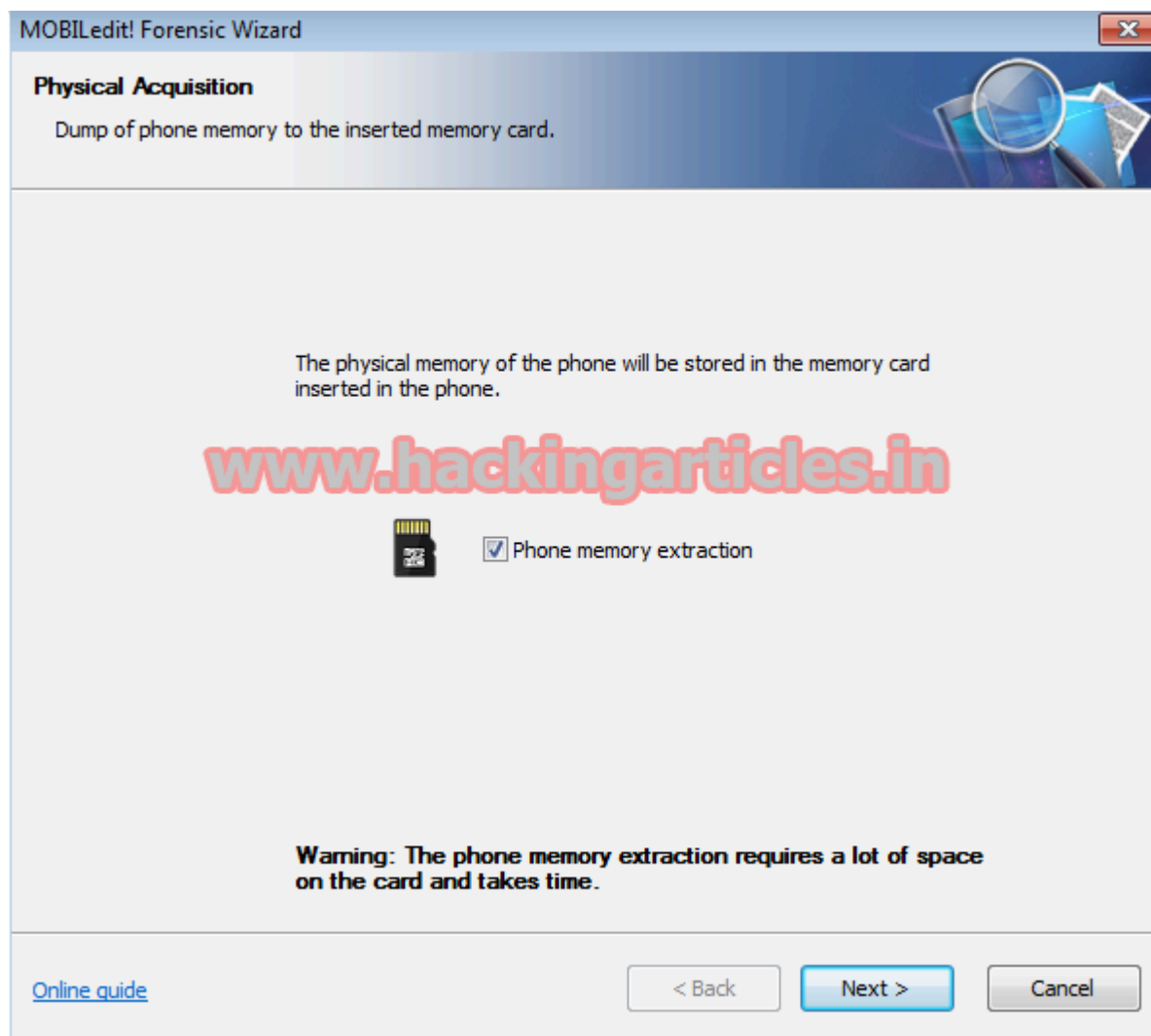
Now it will ask for part of file system to backup. Choose **Whole File System** or **Specified File Types** such as Audio, Video or pictures. Then Click on **Next**.



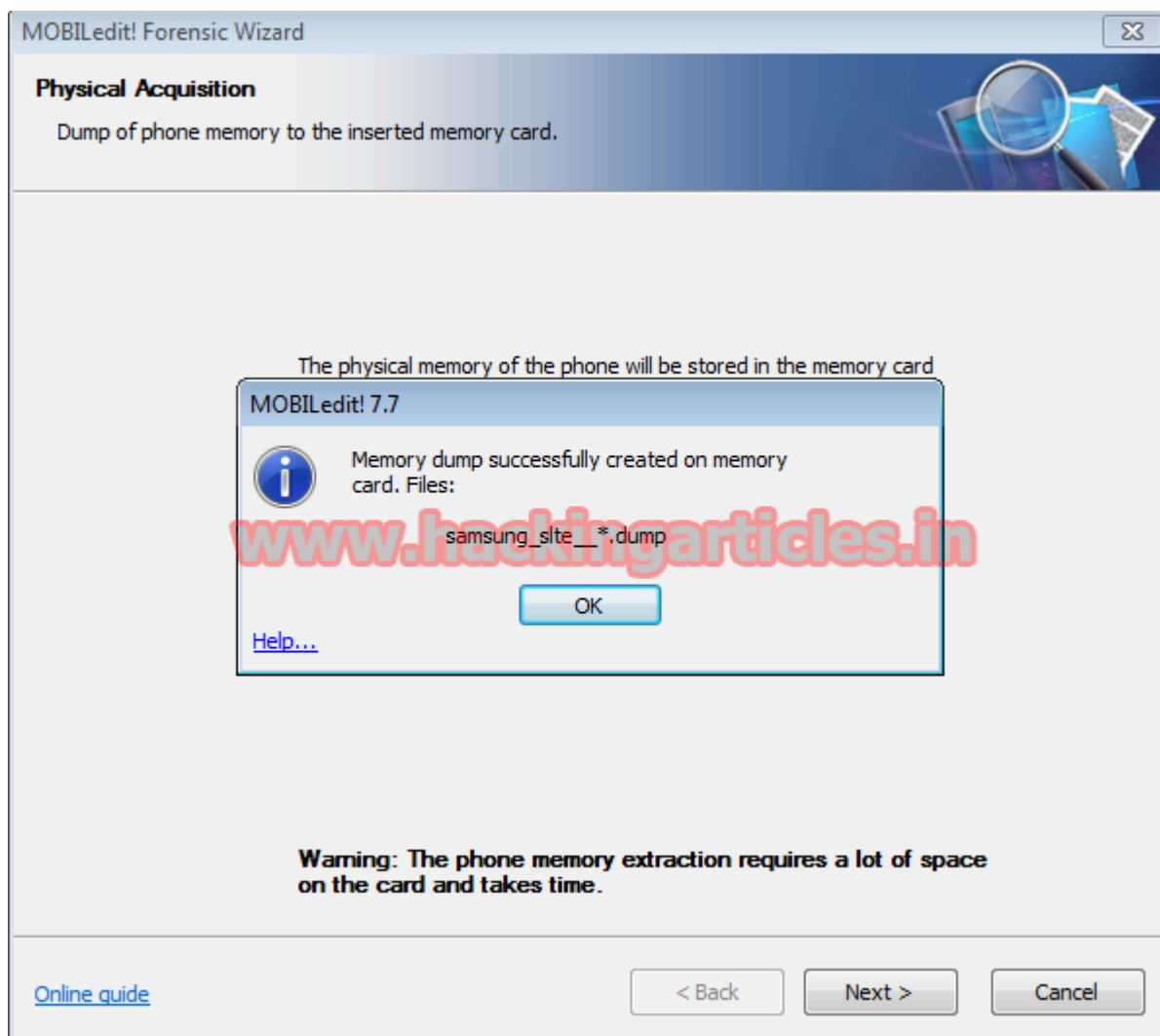
Now it will show the progress bar for Back Up and after completion click on **Next**.



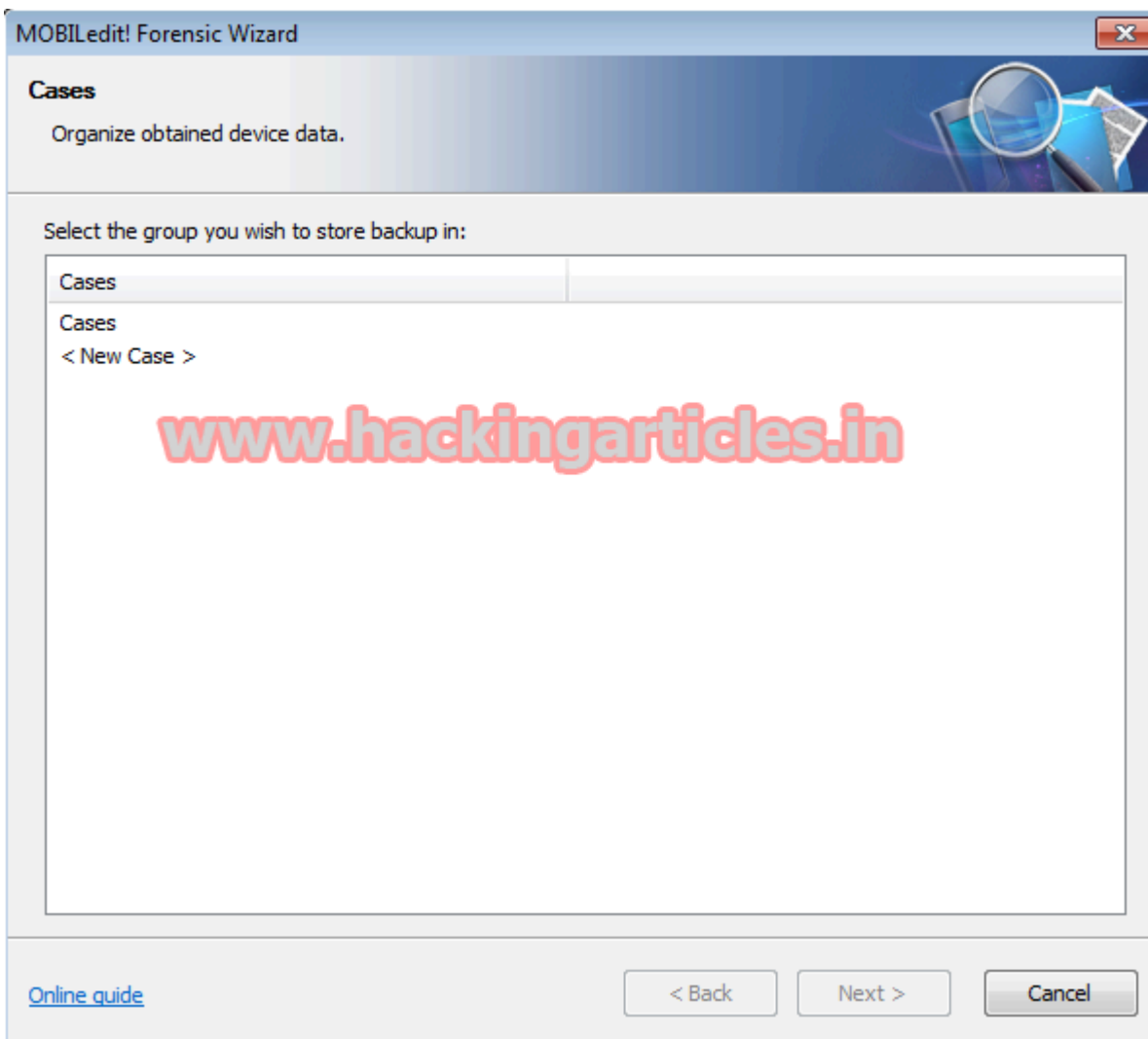
Now select the check box for **Phone memory extraction** and click on **Next**.



Now it will show the message for creation of memory dump on memory card file. Click on **Next**.



Now select the group....**Cases** to organize device data or click on <**New Case**> to create new case and click on **Next**.



If we have selected New Case Option, then it will ask for Case Number and investigator details .Enter Investigator Details and click on **Next**.

MOBILedit! Forensic Wizard

New case
Create a new case for obtained data.

Case Details

Label:

Number:

Investigator Details

Name:

E-mail:

Phone Number:

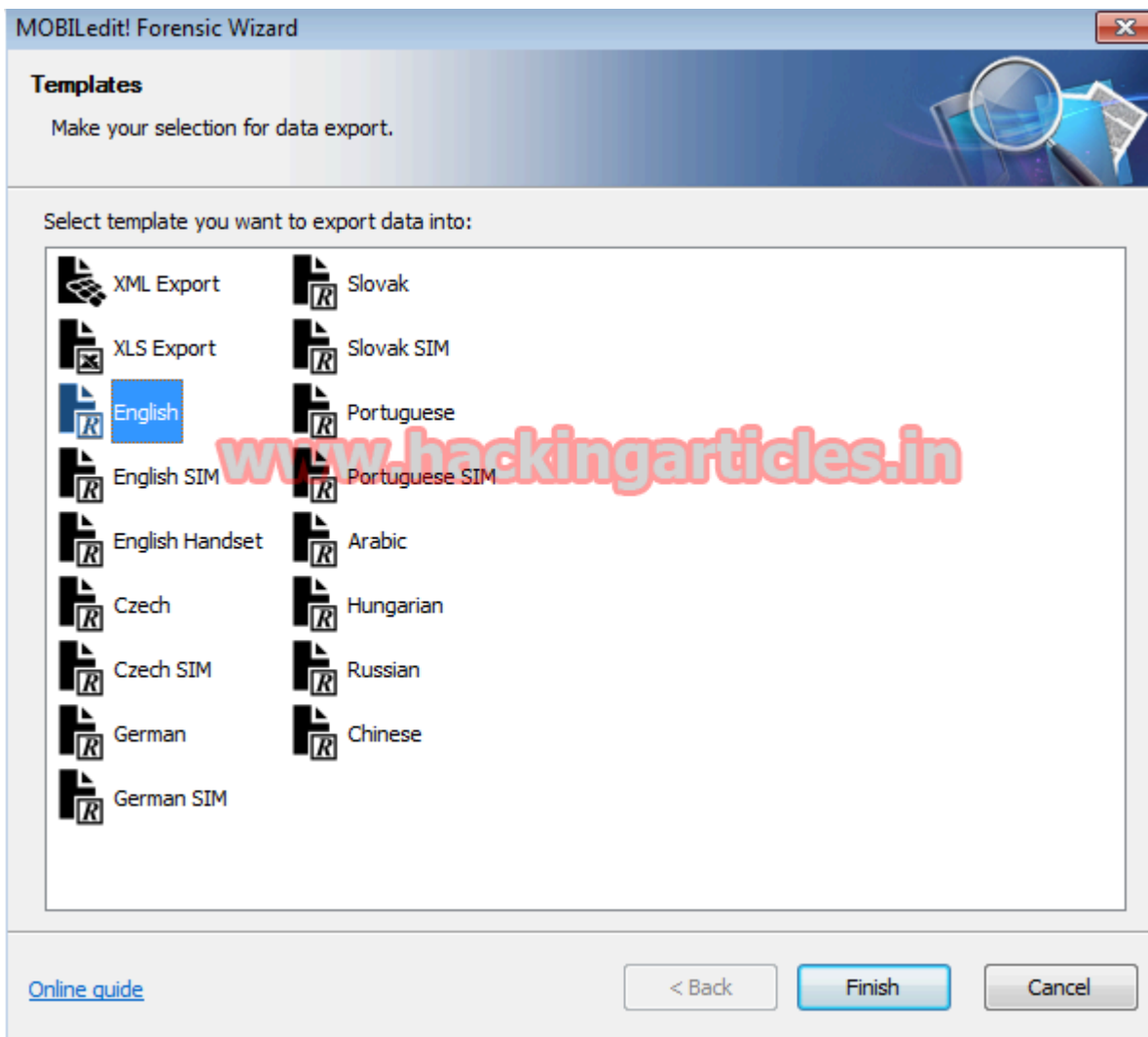
Notes

www.hackingarticles.in

[Online guide](#)

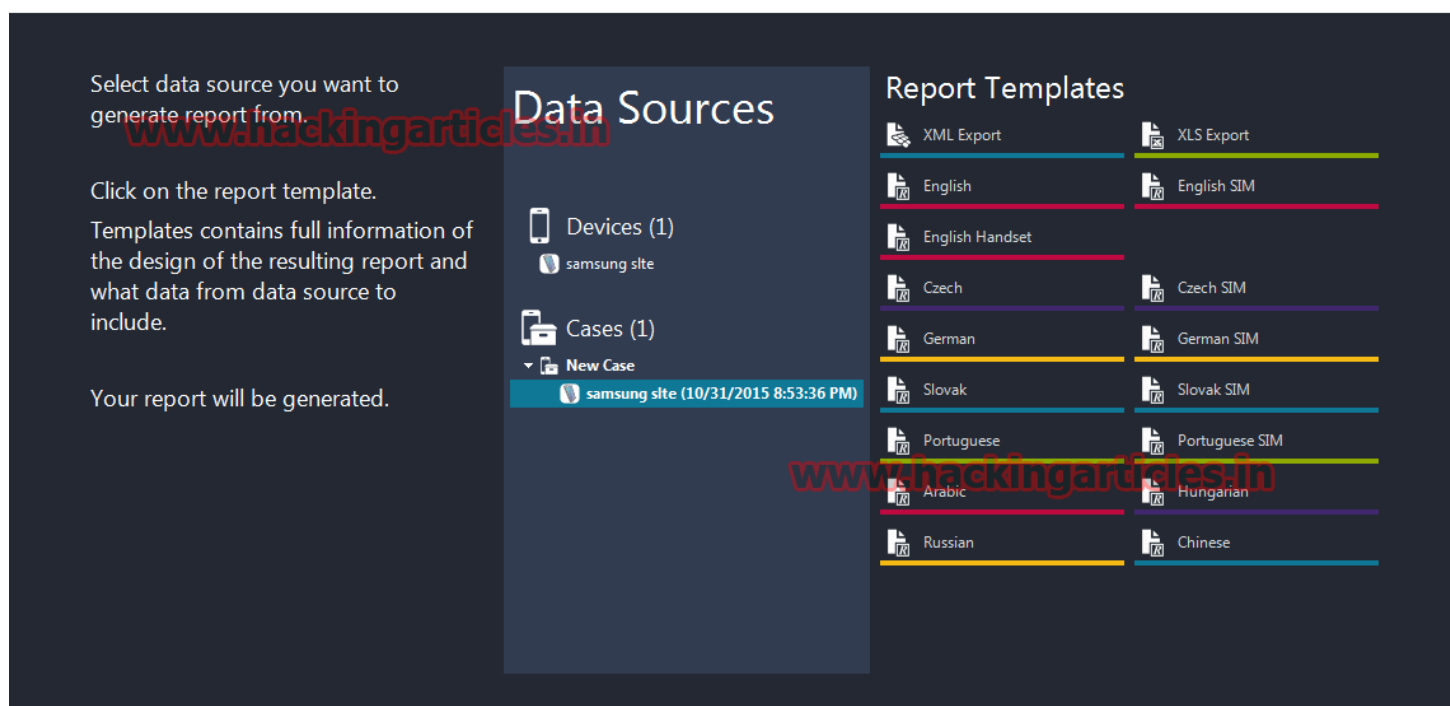
< Back Next > Cancel

Now select the Template for Data Export and Click on **Finish**.

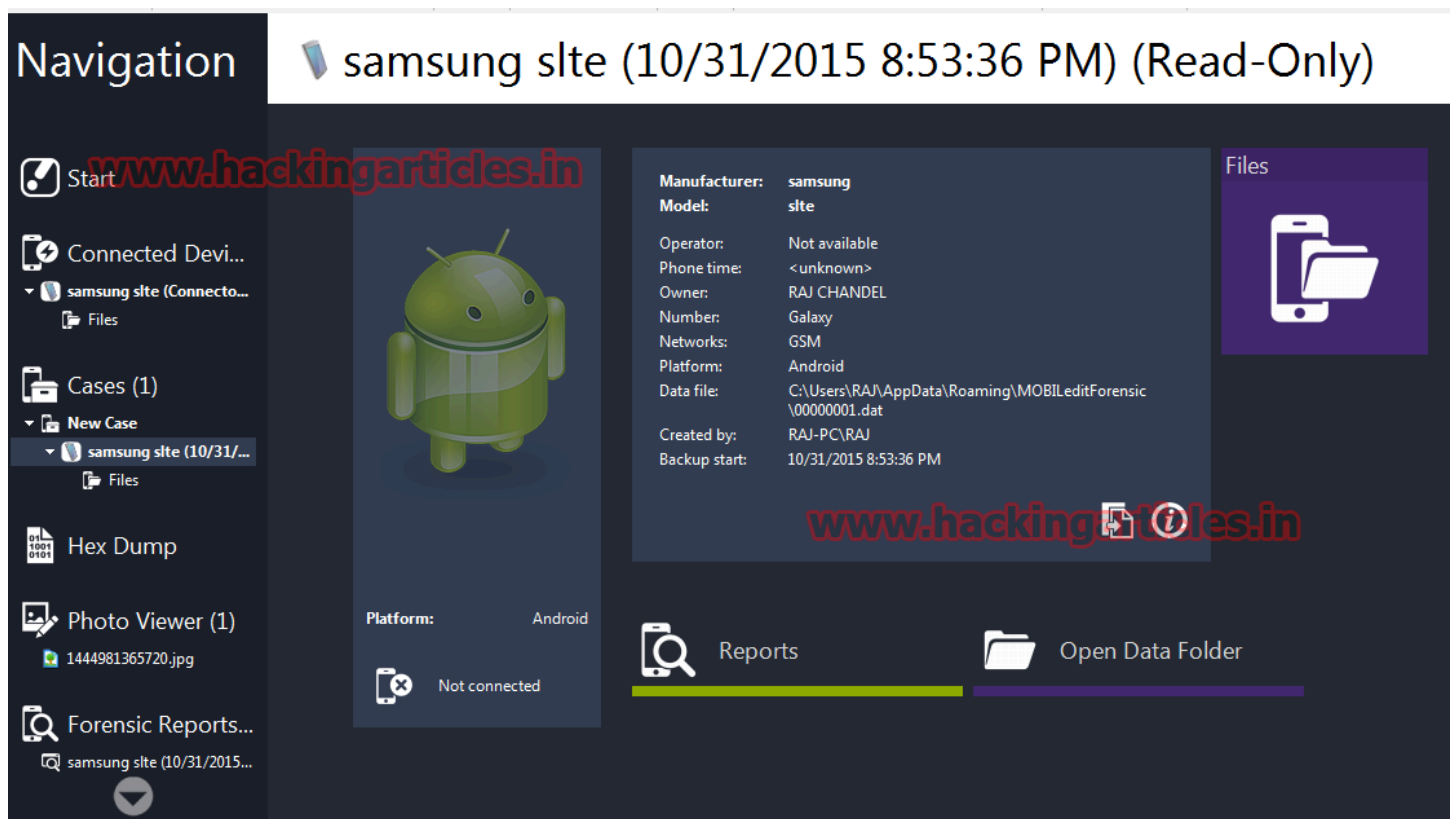


Now it will show the generated Forensic Report.

Forensic Reports



Select Connected Device Option.



Now it will generate a report with all the details such as Phone book, Call logs, messages, Files etc.

samsung SM-G850Y (Read-Only)



To get phone book details, select Phone book option

Navigation

Phonebook (510) - samsung SM-G850Y

www.hackingarticles.in

Start

Connected Device

samsung SM-G850Y (Re...

Phonebook

Call Logs

Messages

Application Data

Applications

Files

Media

User Files

Calendar

SIM card (Read-Only)

SIM Phonebook

Cases (2)

Hex Dump

All (510) Google (180) Phone... (47) SIM (233) WhatsApp (50)

Name | Sort by

Ankit...	Mobile Phone	95...	
anite...	E-mail	@ anit...	
Ang...	Mobile Phone	05...	
An...	Mobile Phone	0...	
Ank...	Mobile Phone	5...	
An...	Mobile Phone	9...	
An...	Mobile Phone	+91...	
an...	E-mail	@ ankit...	
	Web	http://www.go	
ankit...			

www.hackingarticles.in

Now you can select sub option such as WhatsApp to see WhatsApp Messages.

Navigation

Phonebook (510) - samsung SM-G850Y

www.hackingarticles.in

Start

Connected Devi...

samsung SM-G850Y (Re...

Phonebook

Call Logs

Messages

Application Data

Applications

Files

Media

User Files

Calendar

SIM card (Read-Only)

SIM Phonebook

Cases (2)

Hex Dump

All (510) Google (180) Phone... (47) SIM (233) WhatsApp (50)

















Name | Sort by

Mobile Phone	8958477110	
Ar...	Mobile Phone	
B...	air	
General	09770000070	
Ba...	F	
Mobile Phone	+91...	755
Bh...	ja	
Mobile Phone	+91...	133
B...		
Mobile Phone	99...	
M...	am	
Mobile Phone	09...	06
+91...	2	
Mobile Phone	+91...	
Co...	preme	
Mobile Phone	+91...	726
Des...		

www.hackingarticles.in

Click on Call Logs to see Missed Calls, Outgoing calls and Incoming calls.

Navigation

-  Start
-  Connected Devices
 -  **samsung SM-G850Y (Re...**
 -  Phonebook
 -  Call Logs
 -  Messages
 -  Application Data
 -  Applications
 -  Files
 -  Media
 -  User Files
 -  Calendar
 -  SIM card (Read-Only)
 -  SIM Phonebook
-  Cases (2)
-  Hex Dump

📞 Call Logs (65) - samsung SM-G850Y

Missed (65)			Outgoing		Incoming		www.hackingarticles.in	
<input type="checkbox"/>	Name	Number	Time					
<input type="checkbox"/>	Anil Rai	+91950044821	10/31/2015 12:30:05 PM					
<input type="checkbox"/>	Anil Rai	+91950044821	10/31/2015 12:04:26 PM					
<input type="checkbox"/>		+9111111111000	10/30/2015 4:09:13 PM					
<input type="checkbox"/>		+9111111111100	10/30/2015 2:12:24 PM					
<input type="checkbox"/>	K...	+9191111111171	10/29/2015 4:08:51 PM					
<input type="checkbox"/>	P...	+9101111111726	10/29/2015 1:25:21 PM					
<input type="checkbox"/>	P...	+9111111111726	10/29/2015 12:58:20 PM					
<input type="checkbox"/>	P...	+9111111111726	10/29/2015 12:57:17 PM					
<input type="checkbox"/>		+111111111163	10/27/2015 8:50:38 PM					
<input type="checkbox"/>		+9111111111100	10/27/2015 3:32:25 PM					
<input type="checkbox"/>		+9191111111118	10/27/2015 12:24:32 PM					
<input type="checkbox"/>	K...	+9111111111111	10/26/2015 11:41:04 PM					
<input type="checkbox"/>	M...	+9111111111103	10/26/2015 2:55:43 PM					
<input type="checkbox"/>	Dilip Kumar	+91111111111011	10/25/2015 8:46:45 PM					
<input type="checkbox"/>	P...	+9111111111111	10/25/2015 8:15:50 PM					

Now Click on Messages to see all received, sent and draft messages.

Navigation

Messages - samsung SM-G850Y

[illegible]

Click on Application Data to get all the details about content providers.

Navigation

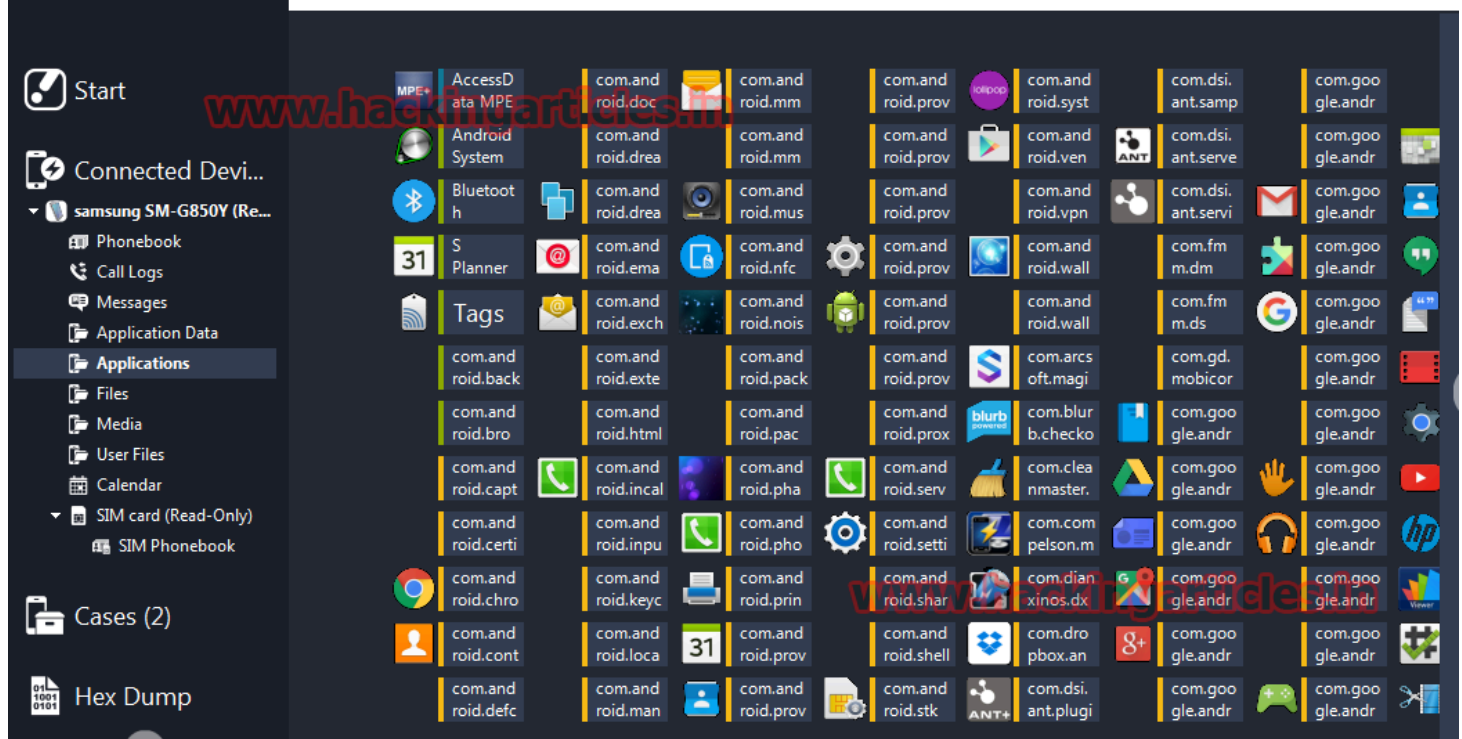
Content Providers - samsung SM-G850Y

File Name	Size	Created	Modified
Accounts.xml	< unknown >	< unknown >	< unknown >
Bookmarks.xml	< unknown >	< unknown >	< unknown >
CalendarAttendees.xml	< unknown >	< unknown >	< unknown >
CalendarEvents.xml	< unknown >	< unknown >	< unknown >
CalendarReminders.xml	< unknown >	< unknown >	< unknown >
Calendars.xml	< unknown >	< unknown >	< unknown >
Calls.xml	< unknown >	< unknown >	< unknown >
ContactsData.xml	< unknown >	< unknown >	< unknown >
ContactsException.xml	< unknown >	< unknown >	< unknown >
ContactsGroups.xml	< unknown >	< unknown >	< unknown >
ContactsRaw.xml	< unknown >	< unknown >	< unknown >
ContactsSettings.xml	< unknown >	< unknown >	< unknown >
ExternalAudio.xml	< unknown >	< unknown >	< unknown >
ExternalImages.xml	< unknown >	< unknown >	< unknown >
ExternalVideo.xml	< unknown >	< unknown >	< unknown >
index.xml	< unknown >	< unknown >	< unknown >
InternalAudio.xml	< unknown >	< unknown >	< unknown >
InternalImages.xml	< unknown >	< unknown >	< unknown >
InternalVideo.xml	< unknown >	< unknown >	< unknown >
Mms.xml	< unknown >	< unknown >	< unknown >
MmsAddr.xml	< unknown >	< unknown >	< unknown >
MmsPart.xml	< unknown >	< unknown >	< unknown >
Searches.xml	< unknown >	< unknown >	< unknown >
SimPb.xml	< unknown >	< unknown >	< unknown >
SimPbFixed.xml	< unknown >	< unknown >	< unknown >
SimPbOwn.xml	< unknown >	< unknown >	< unknown >
Sms.xml	< unknown >	< unknown >	< unknown >

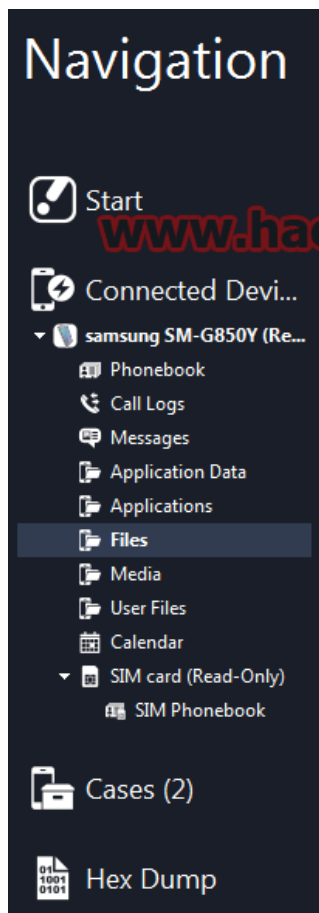
Click on Application to see all the installed Apps in Mobile.

Navigation

📁 Applications (286) - samsung SM-G850Y



Select Files Option to see all the details about system files in Mobile.



Files - samsung SM-G850Y

Files

File Name	Size	Created	Modified
default.prop	330 B	<unknown>	1/1/1970 5:30:00 AM
file_contexts	63.71 KB	<unknown>	1/1/1970 5:30:00 AM
fstab.goldfish	922 B	<unknown>	1/1/1970 5:30:00 AM
fstab.universal5430	2.24 KB	<unknown>	1/1/1970 5:30:00 AM
init	663.64 KB	<unknown>	1/1/1970 5:30:00 AM
init.baseband.rc	1.39 KB	<unknown>	1/1/1970 5:30:00 AM
init.container.rc	1.38 KB	<unknown>	1/1/1970 5:30:00 AM
init.envron.rc	1.50 KB	<unknown>	1/1/1970 5:30:00 AM
init.goldfish.rc	2.77 KB	<unknown>	1/1/1970 5:30:00 AM
init.rc	38.77 KB	<unknown>	1/1/1970 5:30:00 AM
init.trace.rc	1.88 KB	<unknown>	1/1/1970 5:30:00 AM
init.universal5430.rc	54.76 KB	<unknown>	1/1/1970 5:30:00 AM
init.universal5430.usb.rc	10.18 KB	<unknown>	1/1/1970 5:30:00 AM
init.usb.rc	3.79 KB	<unknown>	1/1/1970 5:30:00 AM
init.wifi.rc	2.96 KB	<unknown>	1/1/1970 5:30:00 AM
init.zygote32.rc	301 B	<unknown>	1/1/1970 5:30:00 AM
property_contexts	9.24 KB	<unknown>	1/1/1970 5:30:00 AM
publiccert.pem	1.47 KB	<unknown>	1/1/1970 5:30:00 AM
seapp_contexts	6.42 KB	<unknown>	1/1/1970 5:30:00 AM
sepolicy	382.51 KB	<unknown>	1/1/1970 5:30:00 AM
sepolicy_version	486 B	<unknown>	1/1/1970 5:30:00 AM
service_contexts	29.88 KB	<unknown>	1/1/1970 5:30:00 AM
ueventd.goldfish.rc	323 B	<unknown>	1/1/1970 5:30:00 AM
ueventd.rc	4.88 KB	<unknown>	1/1/1970 5:30:00 AM
ueventd.universal5430.rc	3.92 KB	<unknown>	1/1/1970 5:30:00 AM

Now Click on Media and select internal media or user media and then select pictures option to see Pictures.

Pictures - samsung SM-G850Y

Media		File Name	Created	Modified
Internal media	Alarms	20140629_221620.jpg	<unknown>	10/27/2015 5:27:24 PM
	Music	20150419_205246.jpg	<unknown>	10/27/2015 5:27:24 PM
	Pictures	20151012_192528.jpg	<unknown>	10/12/2015 1:55:28 PM
	Ringtones	20151016_130621.jpg	<unknown>	10/16/2015 7:36:21 AM
	Videos	20151028_223906.jpg	<unknown>	10/28/2015 5:09:06 PM
User Media	Alarms	20151029_163338.jpg	<unknown>	10/29/2015 11:03:38 AM
	Music	20151029_163520.jpg	<unknown>	10/29/2015 11:05:20 AM
	Pictures	20151029_234358.jpg	<unknown>	10/29/2015 6:13:58 PM
	Ringtones	20151029_234408.jpg	<unknown>	10/29/2015 6:14:08 PM
	Videos	20151029_234414.jpg	<unknown>	10/29/2015 6:14:14 PM
		20151030_190017.jpg	<unknown>	10/30/2015 1:30:17 PM
		20151030_190021.jpg	<unknown>	10/30/2015 1:30:21 PM
		20151030_190025.jpg	<unknown>	10/30/2015 1:30:25 PM
		20151030_190042.jpg	<unknown>	10/30/2015 1:30:42 PM
		20151030_190046.jpg	<unknown>	10/30/2015 1:30:46 PM
		20151030_190049.jpg	<unknown>	10/30/2015 1:30:49 PM
		20151030_212240.jpg	<unknown>	10/30/2015 3:52:40 PM
		20151030_212244.jpg	<unknown>	10/30/2015 3:52:44 PM
		20151030_220141.jpg	<unknown>	10/30/2015 4:31:41 PM
		20151030_220205.jpg	<unknown>	10/30/2015 4:32:05 PM
		20151030_220223.jpg	<unknown>	10/30/2015 4:32:23 PM
		20151030_220256.jpg	<unknown>	10/30/2015 4:32:56 PM
		20151030_220301.jpg	<unknown>	10/30/2015 4:33:01 PM
		20151030_220351.jpg	<unknown>	10/30/2015 4:33:51 PM
		20151030_220401.jpg	<unknown>	10/30/2015 4:34:01 PM
		20151030_220621.jpg	<unknown>	10/30/2015 4:36:21 PM
		20151030_220636.jpg	<unknown>	10/30/2015 4:36:36 PM
		20151030_221734.jpg	<unknown>	10/30/2015 4:47:34 PM

To view User's Files, Click on Option User Files.

Navigation

Start

Connected Device...

▼ **samsung SM-G850Y (Re...**

- Phonebook
- Call Logs
- Messages
- Application Data
- Applications
- Files
- Media
- User Files**
- Calendar
- ▼ SIM card (Read-Only)
 - SIM Phonebook

Cases (2)

Hex Dump

User Files - samsung SM-G850Y

File Name	Size	Created	Modified
.CM_Cloud	<folder>	<unknown>	<unknown>
.face	<folder>	<unknown>	<unknown>
.LAS	<folder>	<unknown>	<unknown>
.mmssyscache	<folder>	<unknown>	<unknown>
.PolarisViewer5	<folder>	<unknown>	<unknown>
.SPenSDK30	<folder>	<unknown>	<unknown>
.thumbnails	<folder>	<unknown>	<unknown>
airdroid	<folder>	<unknown>	<unknown>
Android	<folder>	<unknown>	<unknown>
androidlav	<folder>	<unknown>	<unknown>
BeamMemo	<folder>	<unknown>	<unknown>
CallRecordings	<folder>	<unknown>	<unknown>
cleanmaster	<folder>	<unknown>	<unknown>
CMLauncher	<folder>	<unknown>	<unknown>
com.facebook.orca	<folder>	<unknown>	<unknown>
data	<folder>	<unknown>	<unknown>
DCIM	<folder>	<unknown>	<unknown>
dianxin	<folder>	<unknown>	<unknown>
Download	<folder>	<unknown>	<unknown>
hariom pawar	<folder>	<unknown>	<unknown>
Hike	<folder>	<unknown>	<unknown>
media	<folder>	<unknown>	<unknown>
Music	<folder>	<unknown>	<unknown>
Pictures	<folder>	<unknown>	<unknown>
Playlists	<folder>	<unknown>	<unknown>
Pradhanmantri	<folder>	<unknown>	<unknown>
Ringtones	<folder>	<unknown>	<unknown>
SHAREit	<folder>	<unknown>	<unknown>
SmartVoiceRecorder	<folder>	<unknown>	<unknown>