

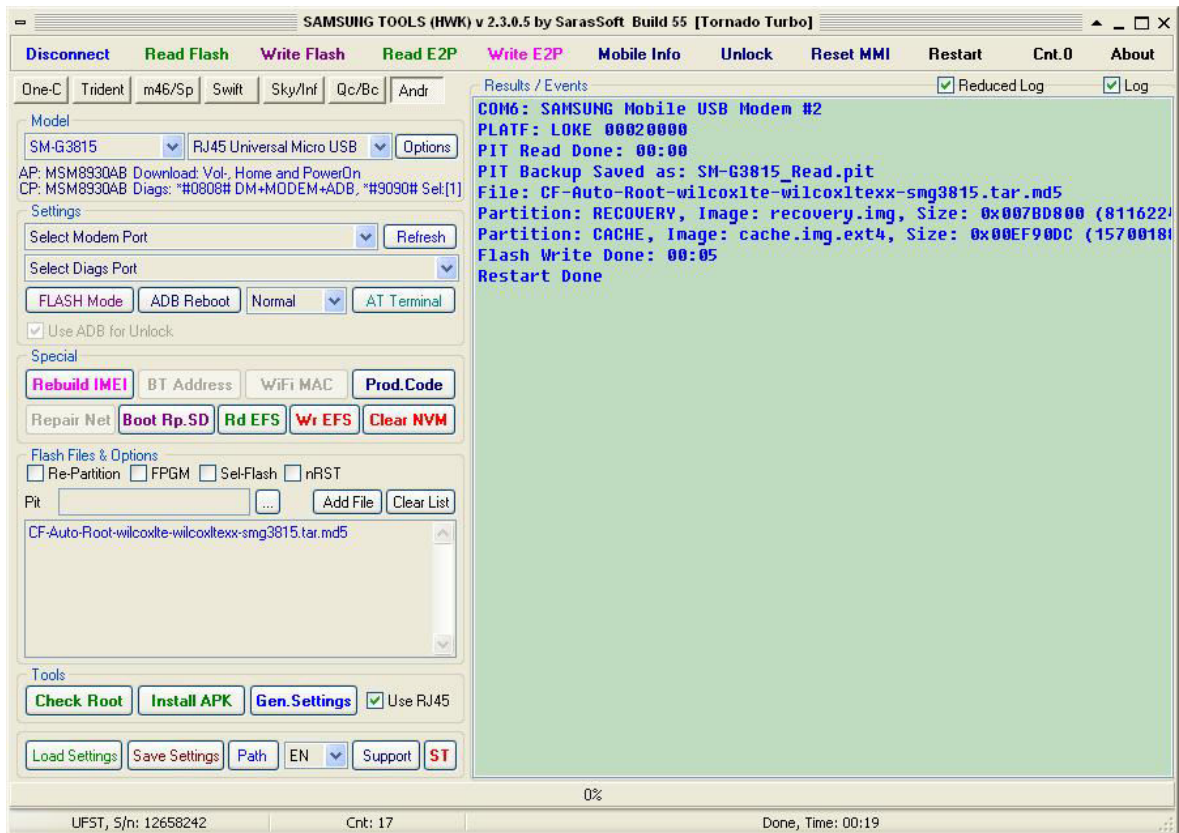
How to get a MSL Access on Qualcomm Platform Based Phones and Write Certification

1. Root Device, using Common Tools or special XXXX_ROOT.tar.md5 file flashing.

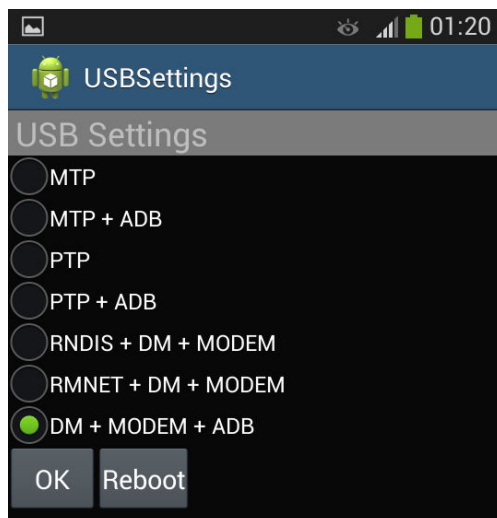
Add Exploit file to list **[Add File]**

Press **[Write Flash]** Button

Insert Cable to Switched Off Phone



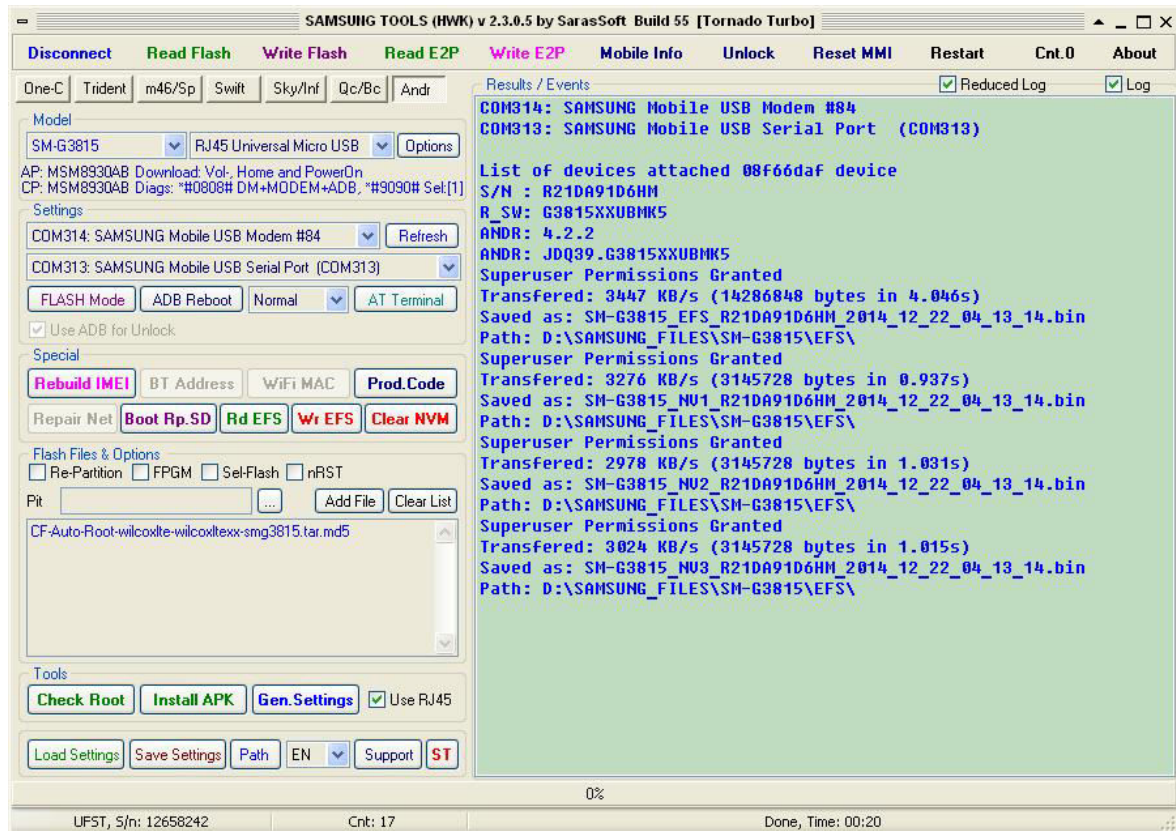
2. For new generation phones just Dial `*#0808#` and select DM + MODEM + ADB
It will turn on ADB on and set diags and modem ports to UFST friendly state



Press **[OK]** and wait till USB Ports Enumerated.

3. Backup all Possible Partitions using [Rd EFS] Button

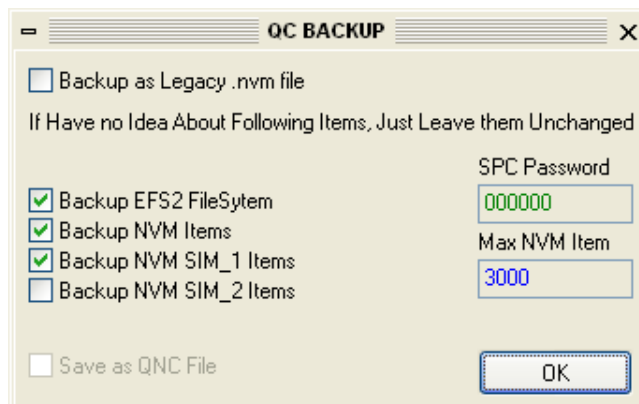
This will make a full Emergency Copy to Roll Back Your Phone to original state



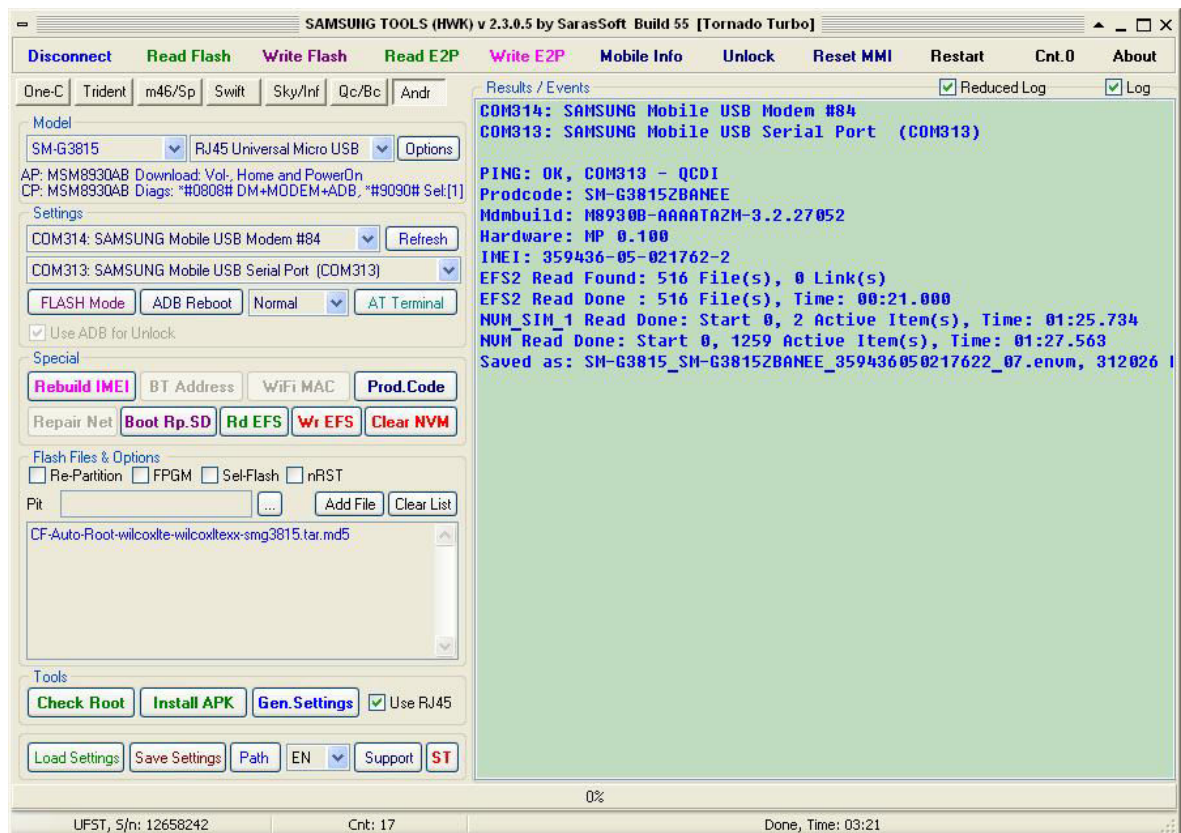
EFS is AP Embedded File System snapshot

NV1 ... _NV3_ is CP EFS2 File System Snapshots (Here have IMEI and Certificates, Radio Settings and other Vital Settings)

4. Backup EFS2 + NVM to ENVM file using [Read E2P] button



This will Backup a Runtime EFS2 and NVM Items Copy, which will need it in Future to Restore Back Radio Settings.



Saved as: SM-G3815_SM-G3815ZBANEE_352309061266846_07.envm, 312026 byte(s)

Here are all readable CP EFS2 items Backup of Radio Strings (IMEI and Certification are not included)

.ENVM file have same functionality as .QCN files.

Note

If have damaged phone or done **[Clear NVM]** before, this Reading have no Sense!

Use in next steps Read Files from “Golden Phone” or download from Support Site!

As all things are now Backed up can feel safe to Destroy a phones Vital Data.

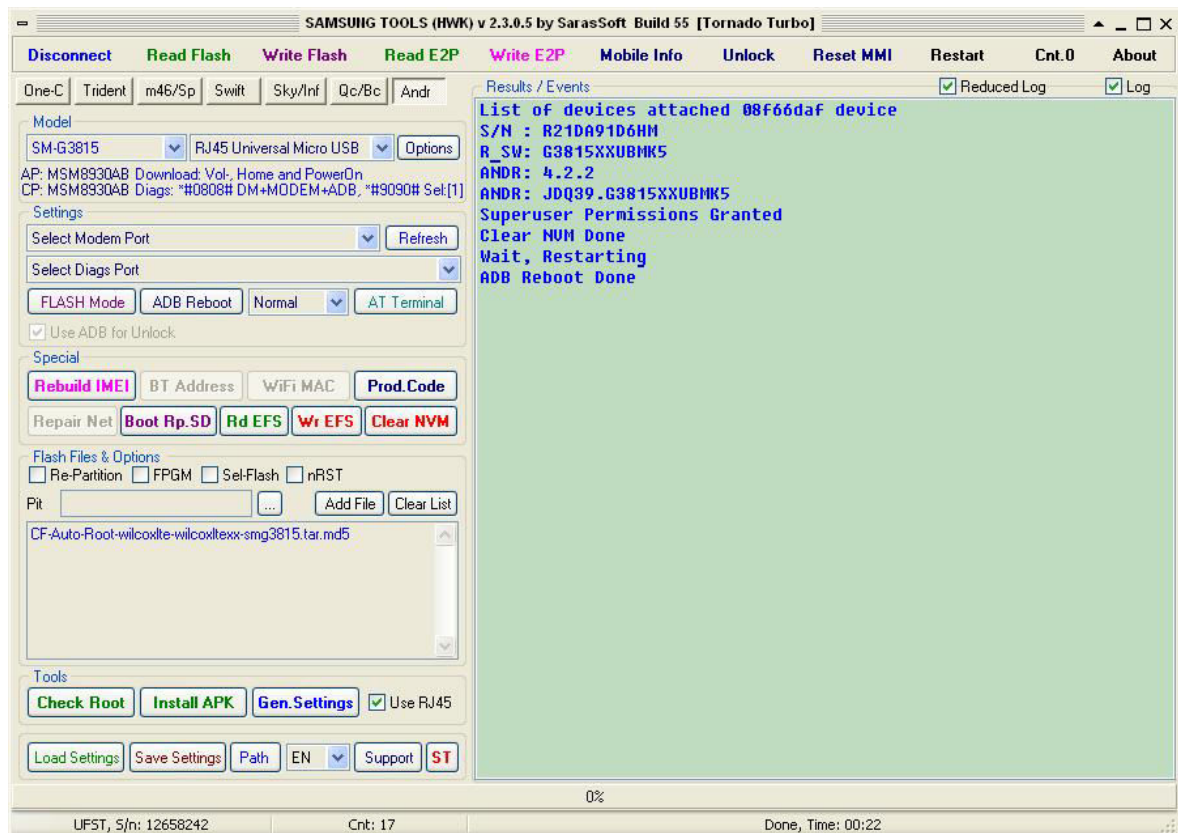
5. Press **[Clear NVM]** button

It Will Erase All Radio Settings, Network Settings, IMEI, Certificates and Will Reset MSL to 0000000000

This is exactly what we need, to access Security internals

But we have already saved All except Security on .ENVM file, so in next steps we will recover Radio Settings and Inject Own MSL security Objects.

It will make Clear Jobs and Restart a Phone, Don't Be Fast here, just wait until all is finished ...



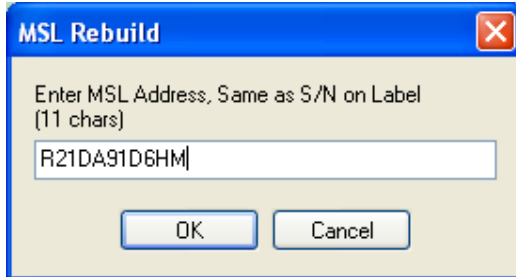
6. When Phone Booted Up and USB Ports Enumerated, just Press **[Gen.Settings]** Button

On Qualcomm Platform SoC's always must be ticked **[Use RJ45]** Option !

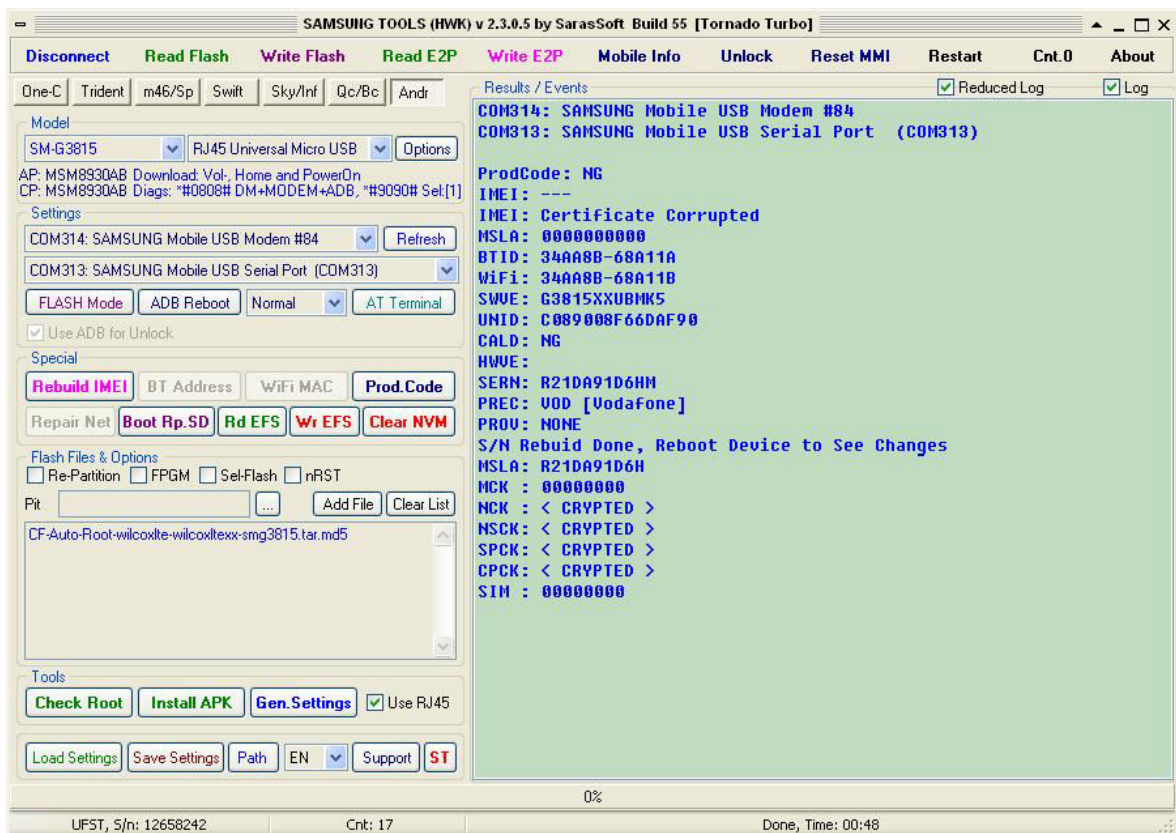
On Some new phones (SM-G530, SM-G800, SM-G850, SM-G901F, SM-N910) to have working UART (RJ45) Communications need Isolate Battery BSI pin



So will see PopUp like this



Enter Here a Real Serial Number from Label, or enter any Valid Rxxxxxxxxx if not have label



After will Pop-Up **[General Settings]** Form

Which allows to Read/Write all Editable Values from/to Phone.

General Settings Editor

Nr	Item	Status	Read Values	New Values
1	Product Code		NG	NG
2	IMEI 1		---	---
3	IMEI 2		---	---
4	IMEI 3		---	---
5	Label Serial Nr		R21DA91D6HM	R21DA91D6HM
6	MSL Address		R21DA91D6H	R21DA91D6H
7	MSL Code	MSL Auth Ok		
8	BT Id		34AA8B-68A11A	34AA8B-68A11A
9	WiFi Id		34AA8B-68A11B	34AA8B-68A11B
10	Calibration Date		NG	NG
11	HW Version			
12	Locks			
13	Pre-Configuration		VOD	VOD
14	Certification 1		0266, 0000, NG_NONE, 1	
15	Certification 2			
16	Certification 3			

RJ45 (523k Micro USB Cable) G3815XXUBMK5 GEN: 1

Use **[Load Values]** if have saved before.

At first We need to write IMEI and Certification.

Use **[Write Cert]** Button, it will ask about a Certification File

General Settings Editor

Nr	Item	Status	Read Values	New Values
1	Product Code		SM-G3815ZBANEE	SM-G3815ZBANEE
2	IMEI 1	Update: Ok	359436-05-021762-2	359436-05-021762-2
3	IMEI 2		---	---
4	IMEI 3		---	---
5	Label Serial Nr		R21DA91D6HM	R21DA91D6HM
6	MSL Address		R21DA91D6H	R21DA91D6H
7	MSL Code	MSL Auth Ok	BDACA82AA1EACA0F44FE49DEEBB61065	
8	BT Id		34AA8B-68A11A	34AA8B-68A11A
9	WiFi Id		34AA8B-68A11B	34AA8B-68A11B
10	Calibration Date		2013-10-27	2013-10-27
11	HW Version		MP 0.100	MP 0.100
12	Locks			
13	Pre-Configuration		VOD	VOD
14	Certification 1	Update: Ok	0266, 0000, OK	
15	Certification 2			
16	Certification 3			

RJ45 (523k Micro USB Cable) G3815XXUBMK5 Modified: 2 Item(s), Restart Product ! GEN: 1

Now can Edit Other Fields in **[New Values]** Column and **[Write]** them

Also Here can use **[Save Values]** and **[Load values]** it will Save/Load Product Code WiFi address BT Address and other Model Specific values.

Here is also **[Init Locks]** button.

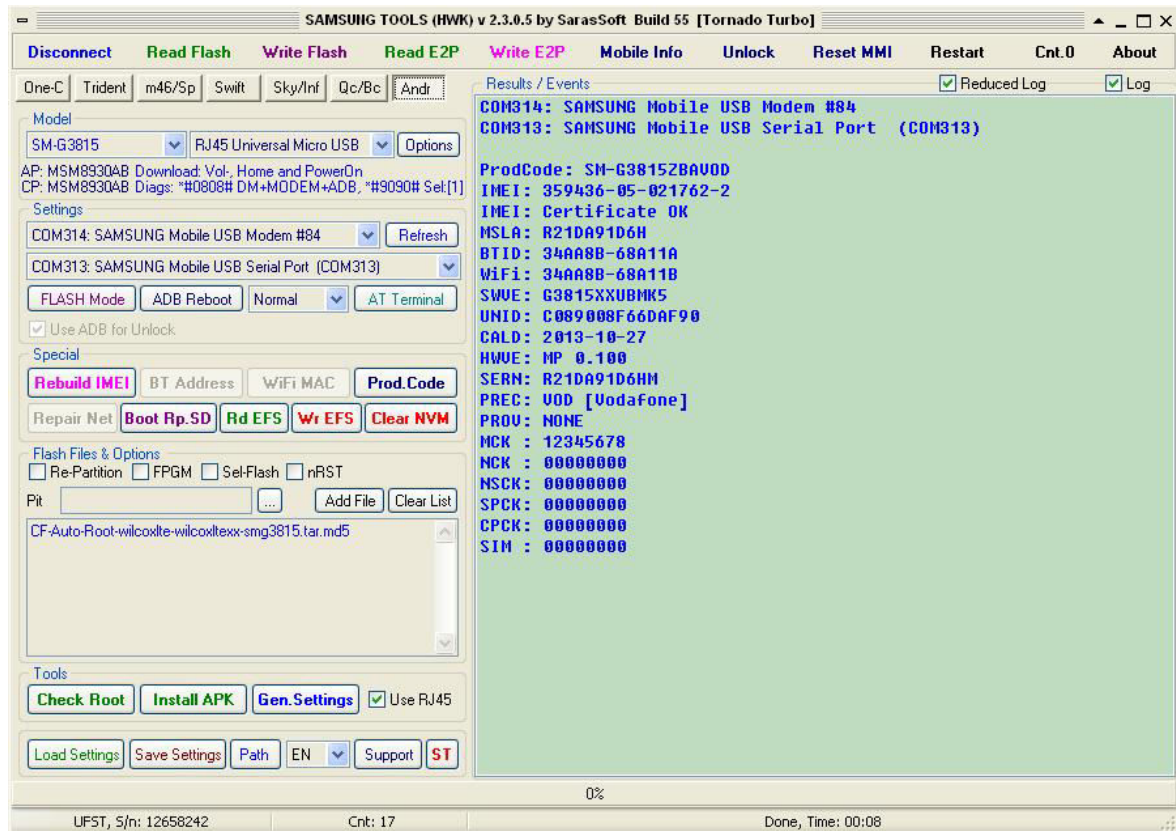
Note

As IMEI is Signed cannot Change IMEI value, can be only defined by the .CERT file

If see: **"Failed: WRITE SIGN Fail"** error in **[Status]** Column, must Restart Phone, because Modem is Stopped by Diags.

And Finally We can test, what we have done

By pressing [Gen.Settings] Button again

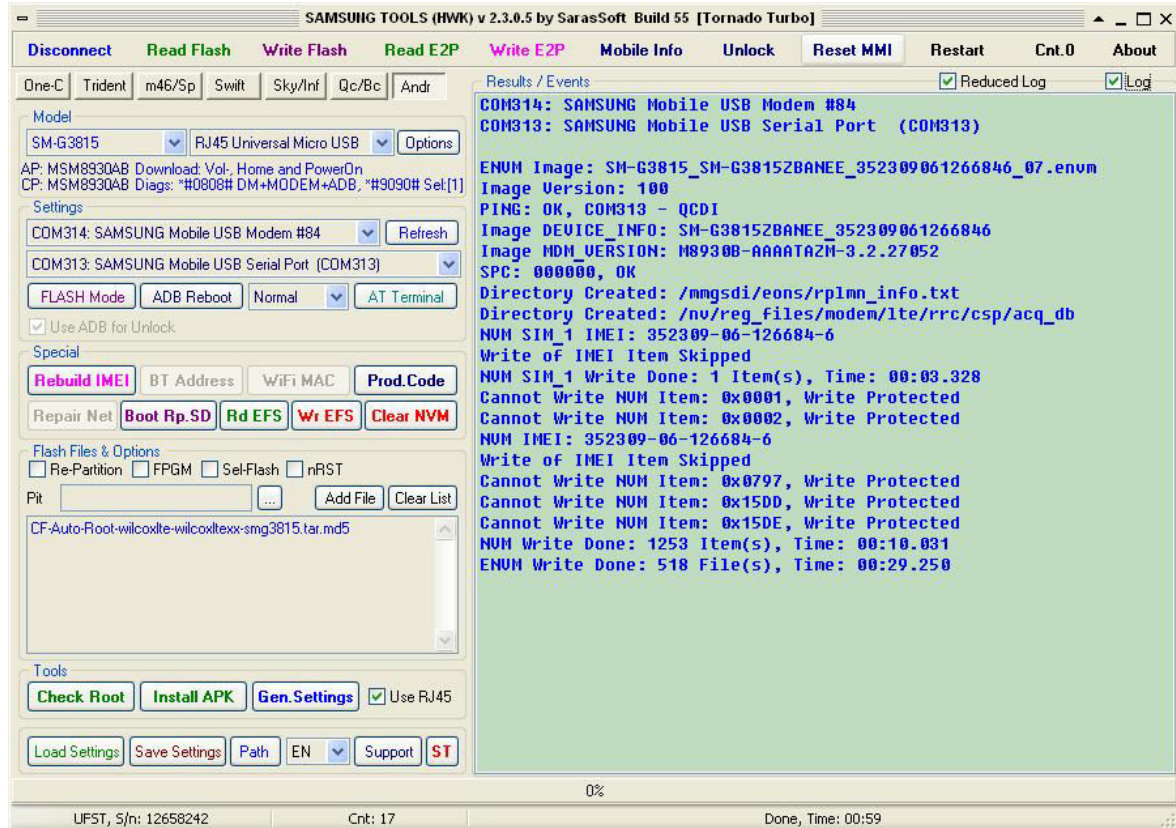


7. Now Let's Write Back the Radio Settings

Press **[Write E2P]** Button

and select SM-G3815_SM-G3815ZBANEE_352309061266846_07.envm file

When asked about Edit IMEI Number during write, Press **[Cancel]**



Do not worry about none written protected Items, it will not cause any Issues.

Restart Phone after write done, otherwise will not have Network because Modem is in "Radio Off" mode set by Diags.

To Restart Phone can use **[Restart]** Button.

As Once **[Clear NVM]** is Done and MSL is Rebuilt, MSL Values are Stored in Local Database.

So now can do all MSL Secured functions without **[Clear NVM]** or Root again:

Write other Certificate, Init Locks, Unlock...

Only Do not Forget Restart Phone after Used Diags Functions (**[Read E2P]**, **[Write E2P]**, **[Mobile Info]**) before use of **[Gen.Settings]**

All these Instructions are applicable for many similar phones:

GT-i9300i, GT-i9301i, GT-S7275, SM-G7102, SM-G7105, SM-G800H, SM-G900F, SM-N9005...

Only must have Certification file.

Our Certification files have SKID number at the end of Name, if this Number is match with phone number, can write certificate from other phone. SKID You will see when Doing **[Gen.Settings]** in **[Certification]** Row, **[Read Values]** Column. In Our Example SKID is 0266.

SKID Number's is also listed in Samsung_Android_Info.xps file.