Examples of using qtools

In this document, we will collect examples of various practical problems that can be solved with the help of the qtools package

Modem IMEI Replacement Procedure

The IMEI of the modem is stored in the nvram 0x226 cell. The problem is that this cell has a write-once attribute. That is, it is registered once at the factory, and all further attempts to write it are stupidly ignored, even without reporting an error. But, of course, we will always find a way around all of this. To do this, you will have to roughly repeat the path that nvram and EFS take at the factory. The following example is for the ZTE MF823/825 modem. For other modems, the procedure may be slightly different. In particular, the config file is used only by ZTE modems.
The sequence of actions will be as follows:

1. Drain all nvram cells from the modem:

```
./qnvram -ri
```

2. Merge the config file from the modem (for ZTE modems that use this file):

```
./qefs -gf confg
```

3. Switch the modem to the boot mode and load NPRG into it, for example (for ZTE823):

```
./qcommand -e -c"c 3a"
./qdload -i loaders/NPRG9x15p.bin
```

Specific commands depend on the chipset and modem model.

4. Clean up the EFS partition. To do this, look at its initial block and size via qrflash, and then clear it via qwdirect:

```
./qrflash -s@ -m
./qwdirect -b<start> -c<len>
```

5. Reboot the modem by pulling it out and USB and plugging it back in.
6. Enter the IMEI you need:

```
./qnvram -j 834001432784560
```

7. Put the rest of the nvram cells back in place:

```
/qnvram -wa
```

8. Put the config file back in place if it was in the modem:

```
./qefs -wf config /
```

That's all. If the modem is in factory mode (with ttyUSB ports), then put it into working mode with at+zcdrun=f, and reboot it.