



You have **2** free member-only stories left this month

 Sign in to Medium with Google ✕


 **Michael Mccann**  
michael.mmccann@gmail.com

Continue as Michael

To create your account, Google will share your name, email address, and profile picture with Medium. See Medium's [privacy policy](#) and [terms of service](#).

# More Proactive SIMs

AT&T inspired me to explore a little more.

 David Allen Burgess Follow

Nov 2, 2021 · 5 min read ★



After my encounter with proactive SMS from an AT&T SIM, I decided to start checking other SIMs as well. I know nearly all SIMs to see just how many SIMs actually use the SIMs I have.

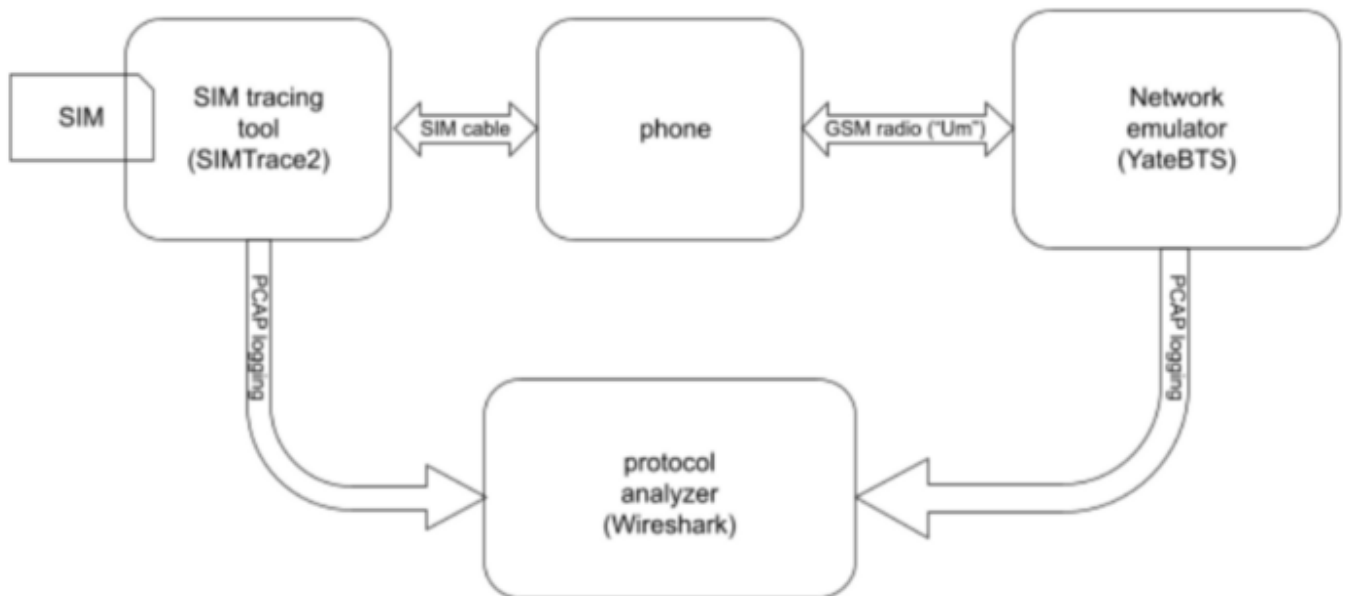
### The SIMs

In this first round, I am limiting my testing to SIMs that are used by large numbers of people.

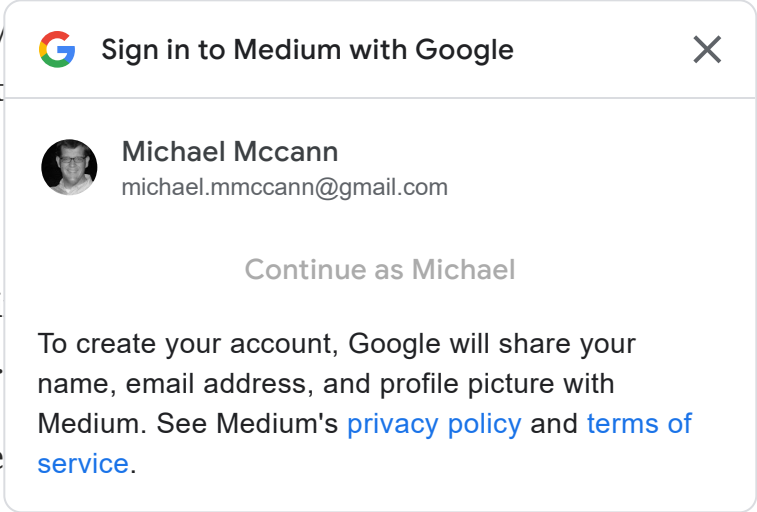
- AT&T (already covered but listed here)
- Verizon
- T-Mobile USA
- Vodafone Romania
- Orange Romania

All of these SIMs were issued between 2014 and 2019.

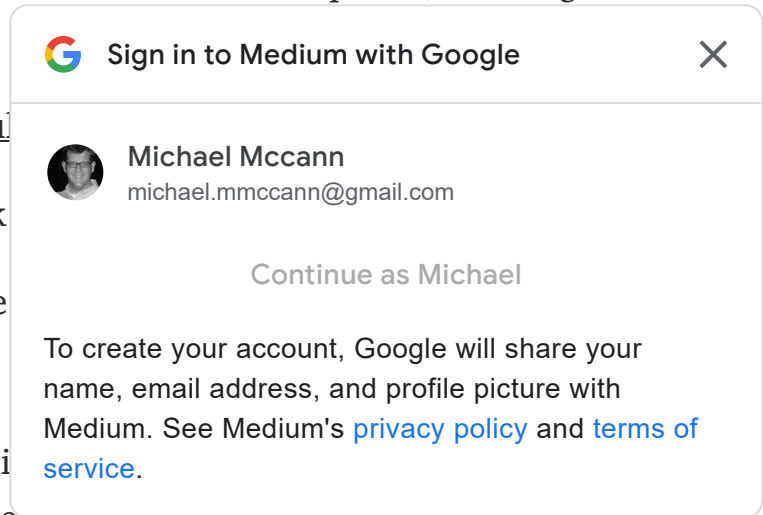
### The Test Bench



The test bench is the same as in the first article, repeated here for convenience:



- The [SIMTrace2](#) tool, which sits between the SIM and the phone, allowing us to sniff the communication between them.
- A host phone. I used an [Allview Sou](#)
- The [Legba Lab Kit](#), desktop network
- A generic smart card reader and the



## The Procedure

The purpose of the procedure is to monitor a phone to see what proactive features the SIM is using. To get the SIM to be active, we will use the Lab Kit to mimic the SIM's home network. Here are the steps:

1. The "SUT" is the "SIM Under Test".
2. Use PySim and the card reader to get the SUT's IMSI.
3. Use the first 5 or 6 digits of the IMSI to get the home network PLMN of the SUT.
4. Program the SUT's home network PLMN into the Lab Kit's GSM cell emulator.
5. Turn off the phone.
6. Install the SUT into the SIMTrace2 device.
7. Start a fresh capture in Wireshark.
8. Start the simtrace2-sniff program, with packets directed to your Wireshark host.
9. Power up the phone.
10. Usually, the phone will recognize its SIM's home PLMN and attach to the emulated network immediately. If not, select it manually.
11. Just let the phone sit for at least 5 minutes.
12. Make a short phone call.
13. Send an SMS to yourself.
14. Let the phone sit for another 5 minutes.

## 15. Check the Wireshark log for proactive operations.

For SIMs that are still valid and have coverage, you can skip Step #4.

## The Results

So, just to get it out of the way, here are

- Vodafone Romania

All the others were interesting.

All of the SIMs used a proactive supplementary services operation to change the call forwarding, but that does not count as “interesting”. I left an example [here](#) in Pastebin just in case anyone disagrees.

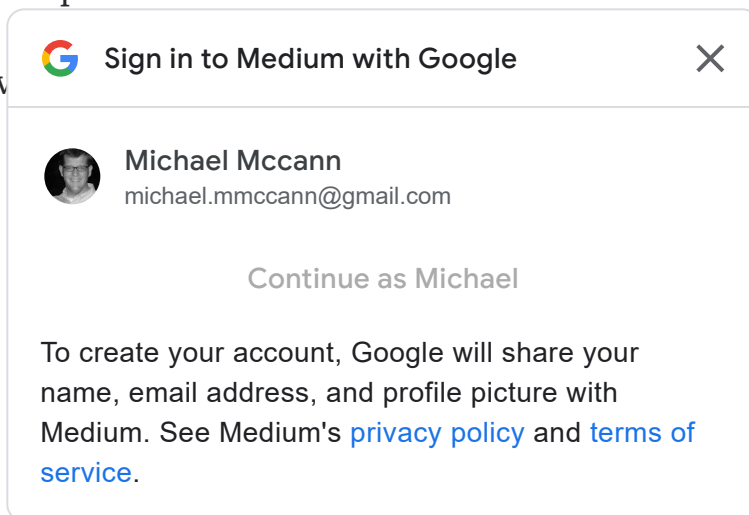
Now for the more interesting ones.

### AT&T

AT&T had a whole post to itself, but is summarized here for convenience. The AT&T SIMs that I have tested send an SMS to AT&T whenever they detect a change in the IMEISV. This IMEISV change is triggered by a baseband processor firmware update, or by moving the SIM to another phone. This type of SIM is covered in detail in the earlier article.

### Verizon

The Verizon SIMs that I tested attempt to open TCP/TP sessions on port 8443 at several IP addresses in the 63.55.x.x and 69.78.x.x blocks, using an APN called “vznadmin”. Since this is a special APN, it is not clear if these IP addresses are really public in this context, but if these IP addresses are public, WHOIS shows that they are owned by Verizon. Since none of these servers responded, I never got to see what the SIM was really trying, but I did see the TCP/IP SYN packets in the SMDCP layer of the Lab Kit, so, yes, the baseband processor really was trying to open these sessions. (Oh, you didn’t know that SIMs could open data sessions that are completely invisible to the application processor?) I saved an example of one of these SIM messages [here](#) on Pastebin.



## T-Mobile USA

This SIM sometimes uses proactive SMS server at ISDN address 122 . It is sent th +12063130004. The payload is binary- “Activate:dt=15”. (Normal text encoding ASCII. This is an M2M message.) An example, is available [here](#) on Pastebin.

## Orange Romania


This SIM tries to send a binary payload SMS to ISDN address 5692 through Orange Romania’s standard SMSC at +40744946000. There is a full example saved [here](#) on Pastebin What’s the content?


Straight outta Wireshark, we have:

1. 0060 XX XX XX 11 51 01 01 03 08 3a 25 76 03 08 91 23 ..;.Q.....: %v...#
2. 0070 06 04 0a 98 04 01 81 10 11 30 73 48 f5 05 09 08 .....0sH....
3. 0080 29 62 01 62 20 51 23 61 06 14 ff ff ff ff bf 4f )b.b Q#a.....O
4. 0090 80 ef 7f 00 80 0f 71 84 08 83 63 60 00 00 90 00 .....q...c` ....

Like the AT&T 2015 example, this message uses TLV formatting and most of the fields are obvious:

- 11 51 01: Header
- 03 08 3a 25 76 03 08 91 23 06 : field type 0x03, length 0x08, IMEI
- 04 0a 98 04 01 81 10 11 30 73 48 f5 : field type 0x04, length 0x0a, ICCID
- 05 09 08 29 62 01 62 20 51 23 61 : field type 0x05, length 0x09, IMSI
- 06 14 ff ff ff ff bf 4f 80 ef 7f 00 80 0f 71 84 08 83 63 60 00 00 : field type 0x06, length 0x14, probably a terminal profile
- 90 00: field type 0x09, length 0, unknown

 Sign in to Medium with Google
✕



**Michael Mccann**  
michael.mmccann@gmail.com

Continue as Michael

To create your account, Google will share your name, email address, and profile picture with Medium. See Medium's [privacy policy](#) and [terms of service](#).

## Conclusion

Of the five tier-1 SIMs I just have “laying messages or initiate connections through happening between the SIM and the base undetectable from the application process


I hope this is the start of a much larger world.


Cell Phones   Sim Card   Mobile Security

About   Write   Help   Legal

Get the Medium app



 Sign in to Medium with Google ✕

 **Michael Mccann**  
michael.mmccann@gmail.com

Continue as Michael

To create your account, Google will share your name, email address, and profile picture with Medium. See Medium's [privacy policy](#) and [terms of service](#).