Lab 07 – Decoding GSM Data

**Find a paging request for a mobile device, show the TMSIS that is being paged.**

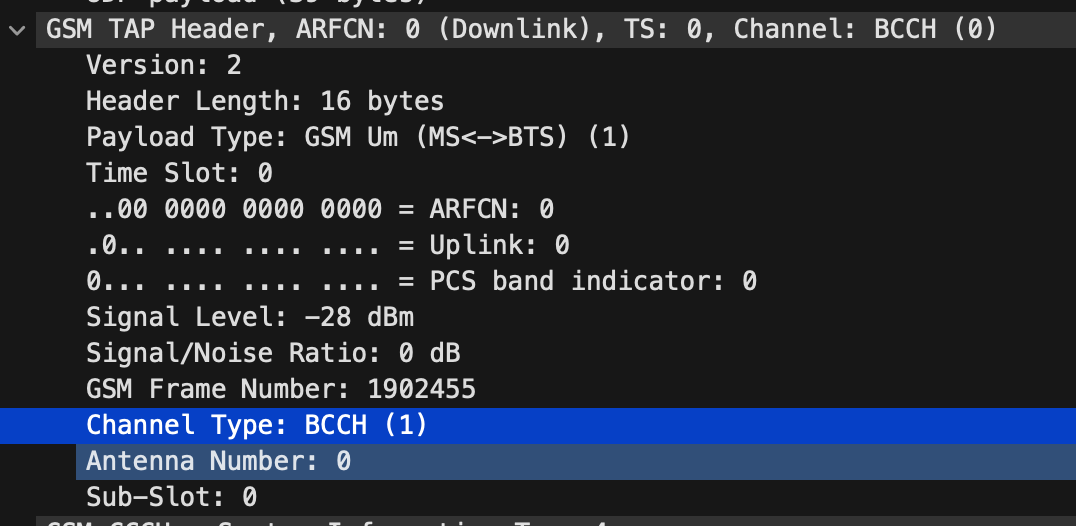
Text

Description automatically generated

TMSI/IMSI = 3322628238

**What frequency and ARFCN is this network operating on? Show a screenshot that clearly shows you found the correct type of BCCH with this info. Describe the ARFCN’s and what their actual frequencies would be. (ARFCN zero is NOT correct!). These values may be easiest found in the BCCH.**

Referencing this… <https://www.rfwireless-world.com/Tutorials/gsm-radio-frequency-planning.html>

****

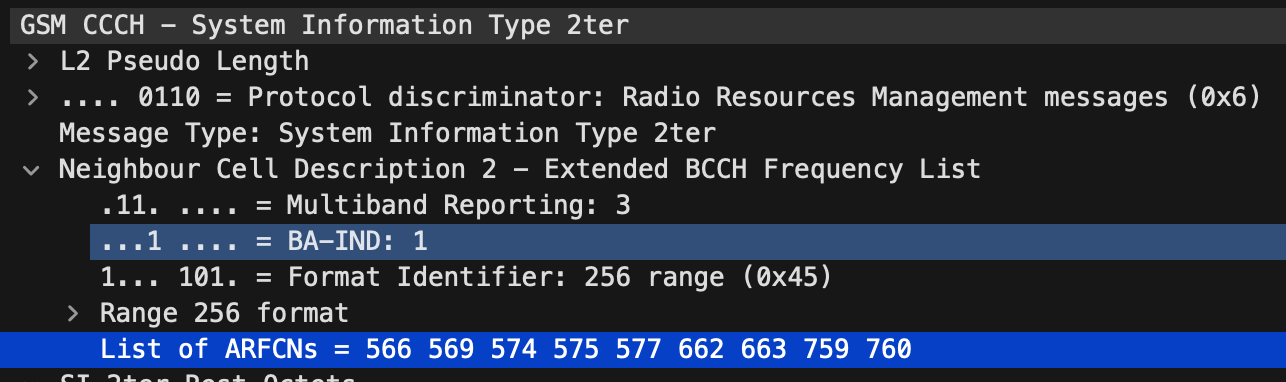
ARFCN is operating on BCCH (0) and the frequency should be something like….

890 + 0.2 \* n + 45 (for downlink), where n is the BCCH channel number

890 + 0.2 \* 1 = 890.0+45 = 935.0 MHz (?)

(just saw the tool in the video… oh well, manual works too)

**The network broadcasts neighboring ARFCN’s. This is so your phone knows what bands it can handoff to that are nearby. Find the data in the appropriate BCCH and include a screenshot. (note, there are two different batches that were available, depending on which BCCH you look at and what band the phone is capable of, just include one)**



ARFCNs = 566, 569, 574, 575, 577, 662, 663, 759, 760

**When searching through the BCCH’s, you’ll find one of the types that contains the network area identification parameters. This includes our MCC and MNC! Take a screenshot that clearly shows you found the MCC/MNC. Describe them, who is the actual carrier?**

Text

Description automatically generated

MCC = United States (310)

MNC = T-Mobile (260)

Text

Description automatically generated

The device, or mobile identity, shows that the carrier is Telefonica UK Limited (10)

**BCCH’s are used to broadcast a BTS’s parameters. Inside of these frames, a Location Area Code can be found. Take a screenshot when you find one. Also answer: what is a LAC?**

Text

Description automatically generated

Location Area Code (LAC) is 0xfffe or 65534

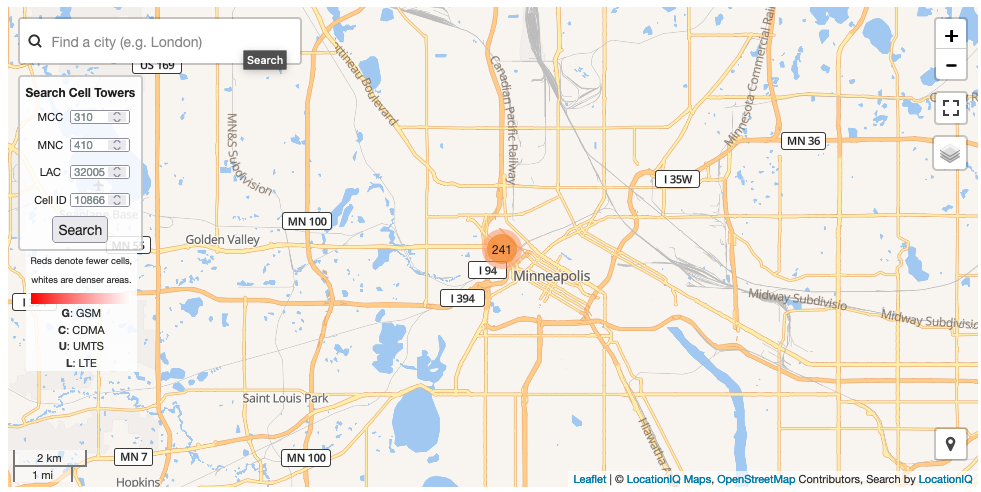
A cellular network is divided into several area’s and each location area consists of 1 to 65534 radio transmission cells. Each location area is uniquely identified by the location area code (LAC), a 16-bit number that forms part of the Location Area Identification (LAI).

**In addition to a LAC, the Cell Identity (CI) is an important value for determining the location of a BTS. Find the CI. Using the CI, MCC, MNC, and LAC, determine: what city is this BTS located in? There are many databases in existence that log these values. Remember: MCC/MNC won’t tell you a specific region typically.**

Graphical user interface, text

Description automatically generated

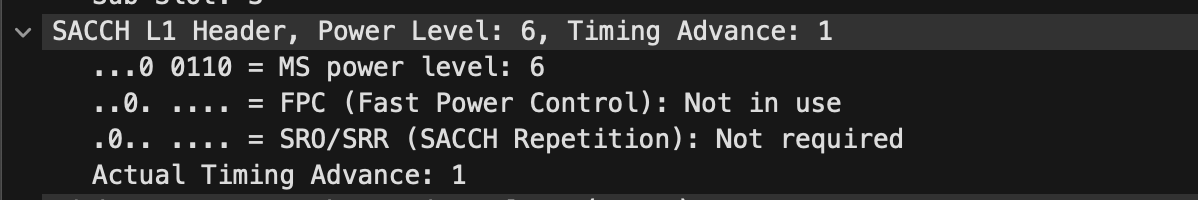
CI = 10866, MCC = United States (310), MNC = AT&T Mobility (410), LAC - 32005



Minneapolis, MN

**Power levels are very important in cellular networks, we want to make sure the MS hears our**

**signal and we want to make sure we can hear the MS’s replies back. We also want to ensure that one MS’s signal doesn’t overpower another MS’s signal. One of the BCCH’s should contain this information; what are the power parameters?**



Assuming these are the power parameters you meant, and not signal level/noise.

Text

Description automatically generated

From the OpenBTS manual.

**A few PCH’s exist. Paging requests are the network’s tool for waking a phone that’s camped and needs to do something. Some pages are very generic, but our capture has some that area**

**addressed to specific TMSIs. Take a screenshot showing that the TMSIS is broadcast out to the world in the clear (note, it’ll appear as a hexadecimal value).**

Text

Description automatically generated

TMSI = 3406566417

**Why are some PCH’s blank, or contain no identity code? Why would GSM have an empty PCH?**

Empty PCH’s can be used as a form of keep alive when the mobile terminal/adapter is not actively being used for data transmission (e.g. phone calls, downloading videos, etc…). AN empty PCH allows the device to save power but remain ready for use.

<https://patents.justia.com/patent/20140185512>