**Lab 07 –Decoding GSM Data**

## Instructions

* 1. a

## Questions

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

* + 0xc90a370d
  + A screenshot of a computer

    Description automatically generated

### 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.

* + ARFCN: 180
  + Downlink Frequency: 879.6 MHz
  + Uplink Frequency: 834.6 MHz
  + The remaining ARFCNs within the band, ranging from 128 to 251, correspond to frequencies between 824.2 to 848.8 MHz for uplink and 869.2 MHz to 893.8 MHz for downlink. Their frequencies can be calculated using the following formulas:
  + Uplink = 824.2+0.2\*(ARFCN-128)
  + Downlink = 869.2+0.2\*(ARFCN-128)
  + <https://www.sqimway.com/gsm_band.php>
  + https://www.rfcafe.com/references/electrical/gsm-specs.htm
  + A close up of a text

    Description automatically generated
  + A screenshot of a data table

    Description automatically generated A screenshot of a computer

    Description automatically generated

### 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)

* + List of ARFCNs = 177 178 179 180 181 233 234 235 237 238 239
  + A screenshot of a computer

    Description automatically generated

### 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?

* + Mobile Country Code (MCC): United States (310)
  + Mobile Network Code (MNC): AT&T Mobility (410)
  + A screenshot of a computer

    Description automatically generated
  + A screenshot of a computer

    Description automatically generated

### 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?

* + Location Area Code (LAC): 0x7d05 (32005)
  + Location Area Code (LAC) is a unique reference point used to identify specific geographic areas within a network. Tracking changes in the LAC is important as it allows a mobile device to send a location update request if the mobile device moves to a new location.
  + A screenshot of a computer

    Description automatically generated

### 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.

* + North Loop, Minneapolis, MN
  + A screenshot of a map

    Description automatically generated
  + A screenshot of a computer

    Description automatically generated

### 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?

* + Cell Reselection Hysteresis (3):
    1. CRH sets a signal level (dB) difference threshold for when a mobile station (MS) should transition to a neighboring cell in another location. If the new cell has a stronger signal, and the difference in signal strengths surpasses the CRH threshold, it will transition to the new cell. The recommended default value of CRH is 4 dB.
    2. https://2g3g.blogspot.com/2009/10/4\_01.html
  + MS TXPWR MAX CCH (5):
    1. MS TXPWR MAX CCH represents the maximum transmit power level (in dBm) that the MS can use on the common control channels (CCH).
    2. https://www.sharetechnote.com/html/Handbook\_GSM\_SystemInformationType3.html
  + RXLEV-ACCESS-MIN (< -110 dBm):
    1. RXLEV-ACCESS-MIN refers to the minimum acceptable received signal level (dBm) required for MS access the network.
  + A screenshot of a computer

    Description automatically generated

### 8. 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).

* + TMSI/P-TMSI (0xc90a370d)
  + A screenshot of a computer

    Description automatically generated

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

* + In GSM networks, some Paging Channels (PCHs) may appear blank, or lack an identity code, due to attempts at optimizing MS idle state. Since a significant portion of a MS time is spent in "camping" mode, where it remains idle, it must continuously monitor the Common Control Channel (CCC) in order to detect any incoming signals or paging messages. While in this mode, the device synchronizes with the network's timing and periodically wakes up to check the Paging Channel (PCH) for incoming communication requests that contain its Temporary Mobile Subscriber Identities (TMSI). However, GSM networks sometimes transmit "empty page" signals, which contain no relevant information or identity codes. The purpose of these signals is to conserve power by allowing the MS to remain in sleep mode rather than processing unnecessary data.

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