Lab07- Decoding GSM Data

In this lab, you'll have the opportunity to explore a capture of GSM data using Wireshark. You'll find similarities to the terms we discuss in class to the values that are deep inside of the actual GSM frames.

Instructions

Using the Wireshark capture attached to the dropbox, answer the following questions:

1. Find a paging request for a mobile device, show the TMSIS that is being paged.
2. 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.
3. 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)
4. 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?
5. 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?
6. 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.
7. 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?
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).
9. Why are some PCH's blank, or contain no identity code? Why would GSM have an empty PCH?

What to Submit

Submit a single PDF that includes the answer to each question and a screenshot (if appropriate)!