LAB 07 –DECODING GSM DATA

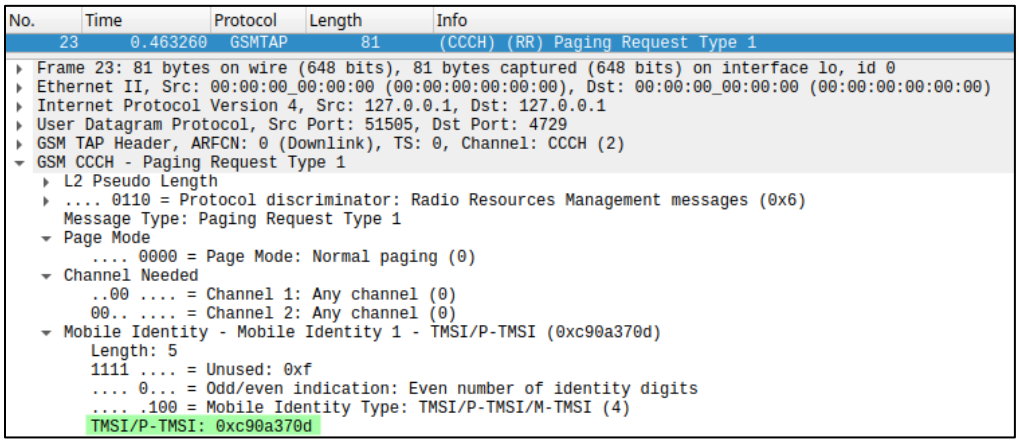
INSTRUCTIONS

In this lab, you will analyze a Wireshark capture of GSM data to explore various network parameters and protocols. Review the provided pcapng file and use the captured data to answer the questions provided. Upon completion, compile your observations into a single PDF report that includes the answer to each question and a screenshot (if applicable).

QUESTIONS

[1] FIND A PAGING REQUEST FOR A MOBILE DEVICE, SHOW THE TMSIS THAT IS BEING PAGED.

0xc90a370d



1.1 - *Wireshark Paging Request Type 1 Frame: TMSI/P-TMSI*

[2] WHAT FREQUENCY AND ARFCN IS THIS NETWORK OPERATING ON?

Include a screenshot showing you found the correct BCCH type and describe the ARFCN values along with what their actual frequencies would be. These values may be found easiest in the BCCH (ARFCN zero is NOT correct!).

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:

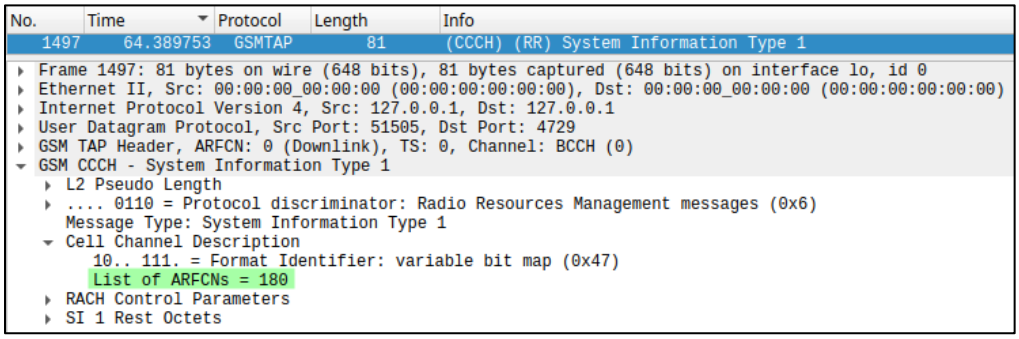
$$Uplink = 824.2 + 0.2 * (ARFCN - 128)$$
$$Downlink = 869.2 + 0.2 * (ARFCN - 128)$$

Band	Arfcn	Downlink (MHz)	Uplink (MHz)
850	180	879.6	834.6

2.1 - *GSM Band and ARFCN Frequencies Table [1]*

Band	Downlink (MHz)			Bandwidth (MHz)	Uplink (MHz)			Chanel number Arfcn	Duplex spacing (MHz)
	Low	Middle	High		Low	Middle	High		
450	460.6	**464**	467.4	6.8	450.6	**454**	457.4	259 - 293	10
480	489	**492.4**	495.8	6.8	479	**482.4**	485.8	306 - 340	10
380 T-GSM	390.2	**395**	399.8	9.6	380.2	**385**	389.8	Dynamic	10
410 T-GSM	420.2	**425**	429.8	9.6	410.2	**415**	419.8	Dynamic	10
810 T-GSM	851.2	**858.7**	866.2	15	806.2	**813.7**	821.2	Dynamic	45
750	747.2	**755.2**	763.2	16	777.2	**785.2**	793.2	Dynamic	-30
710	728.2	**737.2**	746.2	18	698.2	**707.2**	716.2	Dynamic	30
850	869.2	**881.5**	893.8	24.6	824.2	**836.5**	848.8	128 - 251	45
900 P	935.2	**947.5**	959.8	24.6	890.2	**902.5**	914.8	1 - 124	45
900 E	925.2	**942.5**	959.8	34.6	880.2	**897.5**	914.8	0 - 124 975 - 1023	45
900 R	921.2	**940.5**	959.8	38.6	876.2	**895.5**	914.8	0 - 124 955 - 1023	45
900 ER	918.2	**939**	959.8	41.6	873.2	**894**	914.8	0 - 124 940 - 1023	45
1900 PCS	1930.2	**1960**	1989.8	59.6	1850.2	**1880**	1909.8	512 - 810	80
1800 DCS	1805.2	**1842.5**	1879.8	74.6	1710.2	**1747.5**	1784.8	512 - 885	95

2.2 - *GSM/EDGE Frequency Band (45.005) Table: ARFCN Frequencies and Bands [1]*

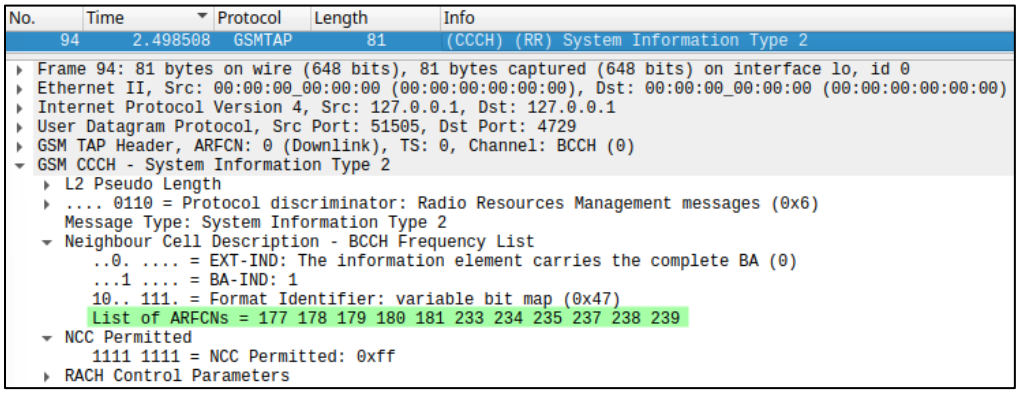


2.3 - *Wireshark System Information Type 1 Frame: Cell Channel Description*

[3] Find the neighboring ARFCN's broadcasted by the network.

The network broadcasts neighboring ARFCN's for handoff information. Find the data in the appropriate BCCH and include a screenshot. There are two available batches based on the BCCH and phone band capabilities; only one batch needs to be identified.

List of ARFCNs = 177 178 179 180 181 233 234 235 237 238 239



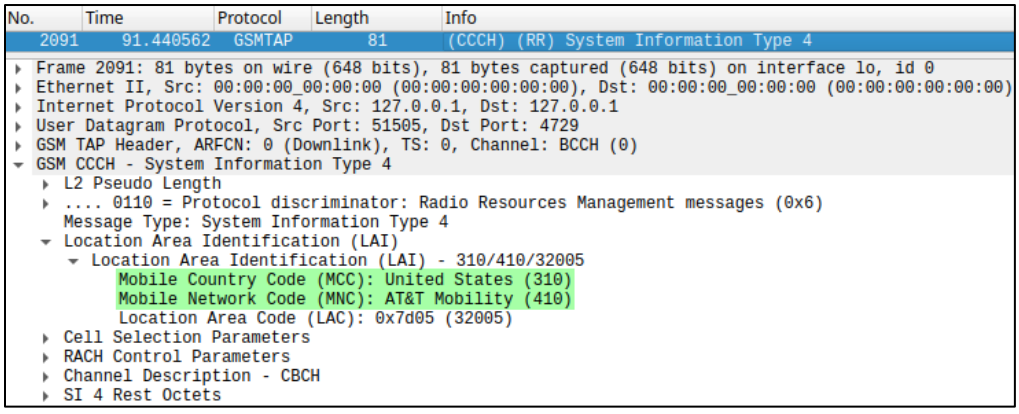
3.1 - *Wireshark System Information Type 2 Frame: Neighbor Cell Description*

[4] What network area identification parameters are available?

When searching through the BCCH's, you'll find one of the types that contains the network area identification parameters such as the MCC and MNC. Capture a screenshot showcasing the MCC/MNC details, describe them, and identify the associated carrier.

Mobile Country Code (MCC): United States (310)
Mobile Network Code (MNC): AT&T Mobility (410)

The Mobile Country Code (MCC) is a three-digit code assigned by the International Telecommunication Union (ITU) to uniquely identify a country. It is used as a reference to identify which country a mobile station (MS) is registered with. Alternatively, the Mobile Network Code (MNC) is a two- or three-digit code that identifies a specific mobile network within a country. [3]



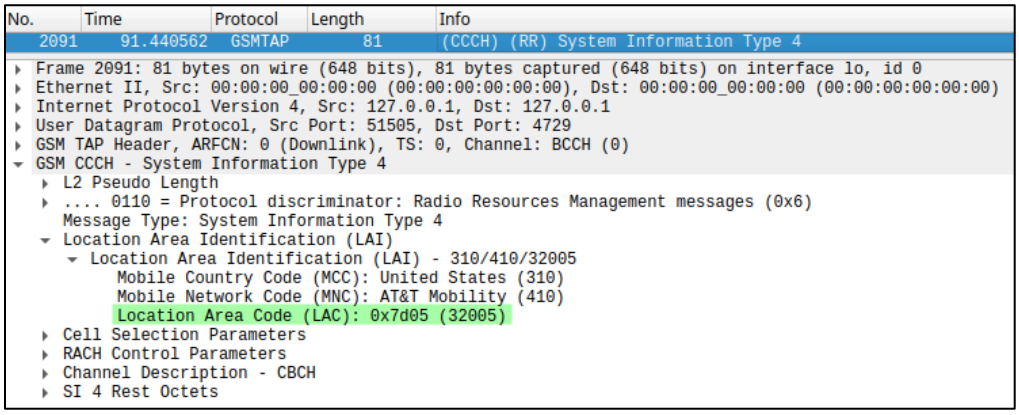
4.1 - *Wireshark System Information Type 4 Frame: MCC, MNC*

[5] What is the Location Area Code (LAC) broadcasted by the BCCH?

BCCH frames broadcast a Base Transceiver Station's (BTS) parameters, including the Location Area Code (LAC). When found, capture a screenshot displaying the LAC information and explain what LAC is.

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.

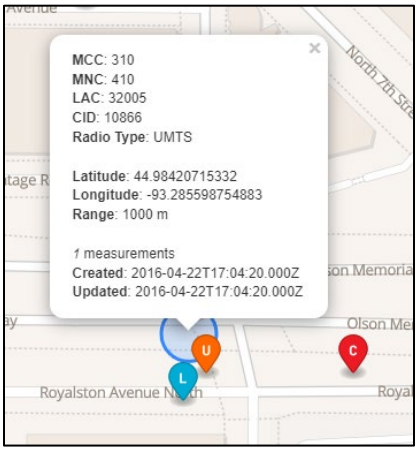


5.1 - *Wireshark System Information Type 4 Frame: LAC*

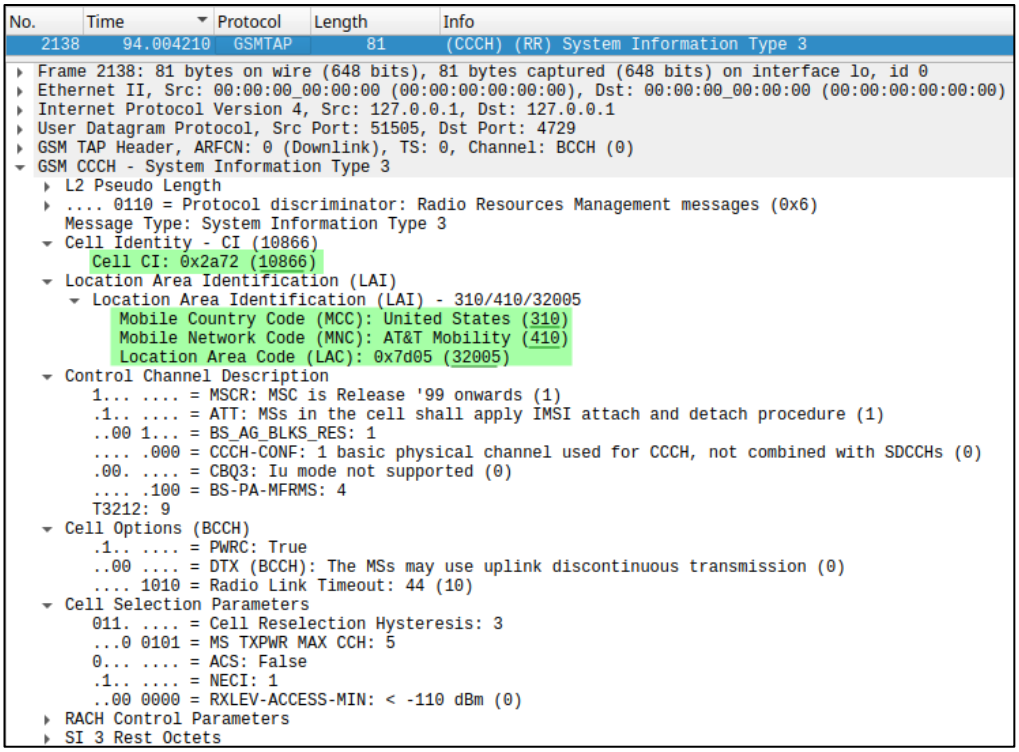
[6] What is the Cell Identity (CI) within the captured data?

In addition to a Location Area Code (LAC), the Cell Identity (CI) is an important value for determining the location of a Base Transceiver Station (BTS). While the Mobile Country Code (MCC) and Mobile Network Code (MNC) offer country and network identification, they usually do not pinpoint a specific region. As such, use the CI, along with the MCC, MNC, and LAC, to determine the city where the BTS is located. Multiple databases maintain records of these values for reference.

North Loop, Minneapolis, MN



6.1 - *OpenCellid: Cell Identity Inquiry*



6.2 - *Wireshark System Information Type 3 Frame: CI, MCC, MNC, LAC*

[7] What are the power parameters found in one of the BCCH's?

Power levels are critical in cellular networks to ensure proper signal transmission between the Mobile Stations (MS) and Base Transceiver Stations (BTS). The BCCH frames typically contain information about power parameters to ensure the MS hears the signal, receives a response, and one MS's signal doesn't overpower another's.

Cell Reselection Hysteresis (3)

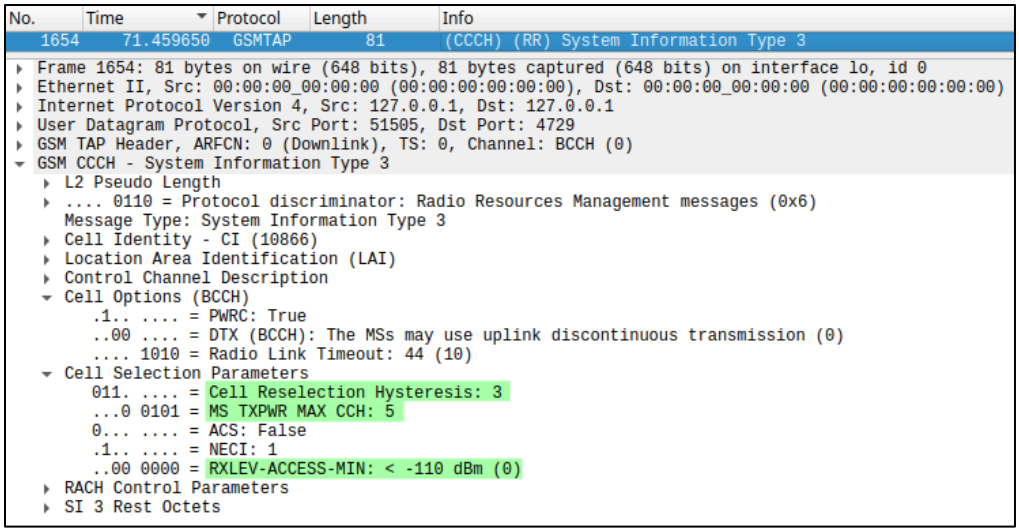
CRH sets a signal level (dB) difference threshold for when a mobile station (MS) should transition to a neighboring cell in another location. If the new cell has a stronger signal, and the difference in signal strengths surpasses the CRH threshold, it will transition to the new cell. The recommended default value of CRH is 4 dB. [5]

MS TXPWR MAX CCH (5)

MS TXPWR MAX CCH represents the maximum transmit power level (in dBm) that the MS can use on the common control channels (CCH). [6]

RXLEV-ACCESS-MIN (< -110 dBm)

RXLEV-ACCESS-MIN refers to the minimum acceptable received signal level (dBm) required for MS access the network. [5]

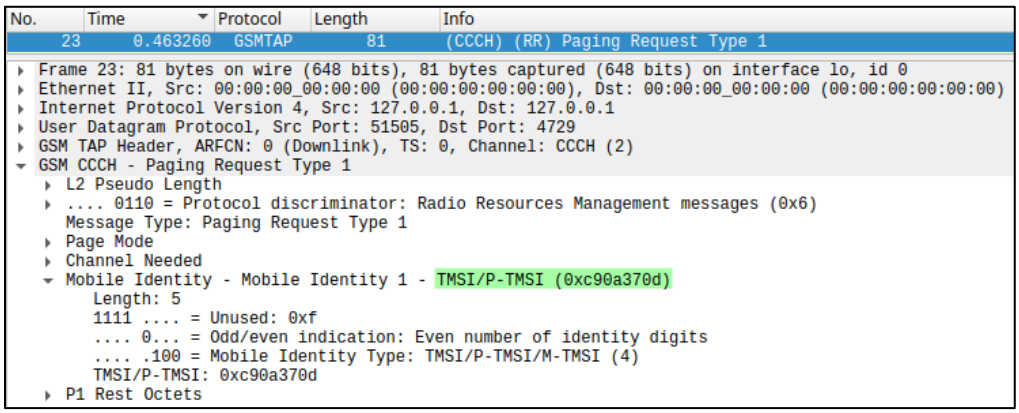


7.1 - *Wireshark System Information Type 3 Frame: Cell Selection Parameters*

[8] WHAT PCHS CAN BE LOCATED WITHIN THE CAPTURED DATA?

Paging requests are essential for waking a phone that has camped and needs to perform a task. While some pages are generic, our capture includes pages addressed to specific Temporary Mobile Subscriber Identities (TMSIs). Capture a screenshot demonstrating the broadcast of TMSIs – these will appear as hexadecimal values.

TMSI/P-TMSI (0xc90a370d)



8.1 - *Wireshark Paging Request Type 1 Frame: Mobile Identity*

[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. [7]

REFERENCES

[1] https://www.sqimway.com/gsm_band.php
[2] https://www.rfcafe.com/references/electrical/gsm-specs.htm
[3] https://teletopix.org/gsm/what-is-mnc-and-mcc-for-gsm/
[4] https://opencellid.org/#zoom=18&lat=44.984557&lon=-93.285374
[5] https://2g3g.blogspot.com/2009/10/4_01.html
[6] https://www.sharetechnote.com/html/Handbook_GSM_SystemInformationType3.html
[7] https://patents.justia.com/patent/20140185512