Handcarving Lab 3

Kailey Cozart

Students will need the following programs: FTK imager, MFI Hex Assistant, and VLC player. The files are on Canvas under Course Programs. The lab is worth 20 points. Submit the original questions with the answers. Go to: *Canvas – Files – Hand Carving Lab* and download the LG CDMA_VX8500 Chocolate Old.zip file and the Sanyo_CDMA_Sanyo_SCP-2700.zip file. Place both of them on your desktop in a folder. Use FTK Imager and add the folder (that contains these files) as evidence. The first 5 questions will use the VX8500 Chocolate. Navigate within the File System to the mms. Locate MMS1012770718.PDU. Using FTK hex view, determine what the attachment is. **Using techniques that are explained during lecture (as well as the manual);** Carve out the attachment and save it to your desktop – make certain that you include the correct file extension when saving it.

1) Download and use VLC to play the file (it is on Canvas if you can't locate it off the internet). Turn up the volume and listen to this entire file. At the end of the recording the person advises who wrote that recording. What is the name they reveal? (If you don't hear the name, you did not carve it correctly) **Hannah**
2) What is the phone number to this phone? (This may not be a normal "looking" number). **10000001682**
3) This MMS is missing one of the numbers needed in the message. Is it the sent "TO" or "FROM" number? **TO**
4) What is the exact TIME the message was sent or received (based off question 3), if it was Feb. 8th, 2012? **9:11 PM**
5) Look at MMS1012770753.PDU. Using the date and year from question 4, what time was this message was sent? **9:12 PM**

The last five questions use the Sanyo SCP 2700 file system: Navigate within the FS to *data/brew/camera/picturemail/00289.* Click on and view i939219983_0 (in hex view). Note: All your answers will be found in this file. Remember – not all dates and times will be in a format that you may have previously decoded. Make sure you try others (possible dates) using MFI Hex Assistant.

6) Carve out the attachment and save it. Describe *exactly* what the attachment is: **It looks like some kind of arm tattoo of a woman with a weird crown thing / facial markings.**
7) Is this a sent or received message? **Received**

8) Based on your previous answer, what was the time and date the message was either sent or received (whichever is your answer)? Provide the *actual values* that indicate this date/time: **37FB5C0F** (Warning: Be careful here, this needs to be what was used to decode in MFI Hex Assistant, you are not allowed to submit: Sat, 10 Oct 2009 20:26:20 GMT). Based on your *correct answer* above, why is the MFI Hex Assistant showing a different decoded hour? **Divergent Time Zones.**
9) What do you believe is the title of this message? **Goin on right now**
10) What is the nickname the sender or receiver has documented (for themselves) in this message? **Mexican Menace**