Ultra Compare Validation Lab

Kailey Cozart

Upload the answers to Canvas – Chapter 18 lab.

Lab – Students will be issued Samsung SCH-U365 Gusto II cell phones for this lab.

Create four separate folders titled, "Base Line Physical Exam, Final Physical Exam, Base line File System Exam, and Final File System Exam." Using UFED Touch or UFED 4 PC, conduct a Physical Exam – target the exam to extract to the Base Line Physical Exam folder.

Next, use UFED Touch or UFED 4 PC to conduct a File System exam. Target the exam to extract into the Base Line File System Exam folder. Now conduct a logical exam using Susteen. (Pull all supported data). When this is finished conduct another logical exam using UFED Touch or UFED 4 PC. It is not necessary to keep track of the output folders for your two logical exams– all that is important is that you perform two logical exams.

Next, conduct another physical exam using UFED Touch or UFED 4 PC. Target this exam to extract into the Final Physical Exam folder.

Lastly, conduct another UFED Touch or UFED 4 PC file system extraction. Target this exam to extract into the Final File System Exam folder. Go into the two File System exam folders – Base Line File System Exam and Final File System Exam. YOU MUST UNZIP THE ZIPPED FILE SYSTEM BEFORE COMPARING. Unzip each to the same folder location.
Use Ultra Compare Binary (Fast) settings to compare the base line binary against the final binary. Make sure you import the correct files (flash). Answer these questions:

1) How many bytes are different (total number)? **3,650,193**

2) How many bytes are exact? **134,761,839**

3) Use the Find Differences arrow. There is only one or two differences between the base line and final binary. **False**

Exit out of the binary so that you have a blank area. Now utilize the two way file compare. Bring in the base line unzipped file system and the final unzipped file system exams. Compare these files. Note the red star areas of change in a side by side comparison. (QCP Dump)

4) What is the total size differences showing on the entire file systems? Write down the sizes:

Total for base line FS **1,183,240** Total for final FS **1,183,286**

Double click on areas where you see the red star noted differences. Examine all the differences that have been found by Ultra Compare.

5) List some areas on your file system where you noted changes:

FUMO.tre in fota (folder);

1881, 945, and 925_1 in num(folder) which is in nvm (folder);

RG3.reg in Registry (folder);

sysinfo.j (file)

6) Now exam the containers (folders) that hold the SMS, MMS, call history, images, etc. Do you see any (red star) changes within these typical areas of user stored data? Please explain in your own words what this validation has shown you about connecting various tools to phones? **There aren't any changes in folders with user stored data. This shows that, while changes have been made to the binary of the phone, no evidential files have been altered. (Our validation has verified that no evidential files have been changed.)**