SECTION 6: FIRST HANDOUT

NOTE TO INSTRUCTOR: DO NOT HAND THIS OUT UNTIL THE BEGINNING OF THE EXERCISE AT THE FINAL SECTION

Password for evidence: DF1Rr0ck$

FOR585 Forensic Challenge: The Homicide of William O'Connor

In the evening hours of February 28, 2018 police arrived at the scene of a possible homicide of William O'Connor, who was found deceased with a gunshot wound in the chest. William was a thirty-nine year old male from Philadelphia, Pennsylvania who died under suspicious circumstances. Police seized Mr. O'Connor's mobile device (an Apple iPhone) as evidence at the scene. The device was locked, but the police were able to guess the password, as it was the victim's birthday. The police also recovered a piece of paper listing Mr. O'Connor's iCloud login information, which was used to obtain backup files from his iCloud account.

Following the media's reporting of Will's death, a woman named Grace Appster, came forward as a good Samaritan and potential witness. She told police that she had reason to believe William's wife Felicity could be responsible for his murder. Ms. Appster voluntarily consented to a search of her phone, and the police obtained an Android backup of her phone and a logical copy of the internal emulated media card from her Samsung Galaxy mobile device.

Shortly thereafter, police obtained a search warrant for the mobile device belonging to William's wife, Felicity O'Connor. Felicity handed her phone over to the police on March 12, 2018, explaining that she and Will recently separated. Felicity told police that and she was in Texas at the time he was murdered and couldn't have been responsible for his death. Felicity's alibi appears to be true. She was in fact in Texas when William died.

The police ask you to look into the electronic evidence from the three phones based upon Ms. Appster's claims, which also appear to be reliable.

The following evidence is presented to you as the digital examiner.

Will O'Connor
File system images of (1) Apple iPhone 6s – *PIN was 030177*
Cellebrite Physical Analyzer Advanced Logical Method 1 and 2 were utilized
The contents of an iCloud backup – *recovered from the iCloud account Williamoconnor1311@icloud.com*
If prompted for backup password = will

Felicity O'Connor
File system images of (1) Apple iPhone 5s
Cellebrite Physical Analyzer and AXIOM and were utilized

Grace Appster
Android backup (backup.ab) of (1) Samsung Galaxy S6 SM-G920A
Graces backup.ab password = 5555
Logical contents of emulated SD card from (1) Samsung device provided in FTK (*.ad) image files

The current search warrant enables you to examine data at rest and data extracted from the iCloud account tied to William O'Connor. Should your examination lead you to additional artifacts or data of interest, you may request subsequent search warrants from the Judge (i.e. Your FOR585 Instructor or SANS OnDemand SME). You must have valid reasons for wanting access, and you must provide specific information about what kind of information you are seeking or you will be turned away and told to keep digging.

Use the digital evidence to summarize the following:

- Identify a suspect(s) in the murder of William O'Connor
  - Provide sufficient details to support your findings
- Determine a possible motive for the killing
  - Provide sufficient details to support your findings
- Identify a timeline of events leading up to the murder
- Establish an approximate time of death
- Explain any anomalies in the evidence files you were originally presented to conduct your forensic analysis

PREPARE:

- A 10 minute PowerPoint Presentation showing the key facts you uncover and what they mean to the case.

- Each team will be allowed to opt out of presenting via silent ballot 1 hour minutes prior to presentations.

Each team will be allowed to vote on the best presentation - One vote per team. You cannot vote for yourself. The instructor has built in tie-breakers if needed. Keep in mind, you can be **disqualified**, if you act without proper authority. Just ask if you want to do something!

What to look for in the best presentations?

- Technical detail – not just pretty pictures
- Great explanations and graphics showing detail
- Presentation capability of the team

Do not award the vote to the most entertaining team, but the team that really gets the technical details and combines it with the overall best presentation style and explanations.