SECTION 6: SOLUTIONS

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

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, AXIOM and Oxygen 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.

Executive Summary of Major Findings for the Homicide of William O'Connor

As requested by the Philadelphia Police Department Homicide division, an examination of William O'Connor's iPhone and iCloud data has been completed. Will's wife, Felicity, handed over her iPhone for examination and Grace Appster provided her Android for examination. The purpose of this investigation was to gain any leads or identify who murdered William O'Connor in his home on the night of February 28, 2018 and a motive, if possible.

Additional evidence that would have been granted for examination upon request:

1. Cloud data for Felicity O'Connor – Note: She and Will shared an iCloud account for quite some time. The police pulled her data at the same time as Will's, but you had to ask for it. This will show all of her activity since she wiped her iPhone prior to turning it into the police.
   A. iCloud
      https://for585.com/felicity
      Password: WPSEopFqeYYw

   B. Felicity Gmail - felicityocon@gmail.com
      Password: z8PrC8EhxdMM
      https://for585.com/felicity2

2. Cloud data for Grace Appster- Facebook data
   https://for585.com/grace
   Password: CzhrpXGtyoLb

3. The BlackBerry 10 backup for Paul Lazarro - once extracted **backup password is Lazarro1!** and the email associated with the backup is **hurtz4real@yahoo.com**
   https://for585.com/paul
   Password: w9nzu6w7uVzS

The evidence found on the devices prove the following:

- Will and Grace meet at a work happy hour in Bethesda, Md. They were both invited and did not know each other prior to that night.

- Will starts a relationship with Grace and plans to leave his wife.

- Felicity, Will's wife, catches wind of his infidelity because they share an iCloud account and she is getting his texts and copies of his photos!

- Will takes Grace on a trip to Dallas where he tells her his wife will be moved out and gone when he gets home.

- Felicity finds Paul Lazarro on Facebook and on VampireFreaks.com. He agrees to help her with any troubles she has.

- Felicity begs Will to change his mind and then hires Paul to kill Will.

- Felicity goes to Texas to stay with a friend and to create her alibi.

- Paul confirms with Felicity that she wants Will to be murdered via VampireFreaks and she responds to “do it ASAP”

- Will is murdered by Paul Lazarro on Feb 28, 2018. Paul connects to their Wi-Fi, offers to take a photo and leaves the scene.

- Grace was on the phone with Will when Paul arrived but she couldn’t hear anything. Thus, when she saw Will was murdered on the News she reached out to police.

Date (mm/dd/yy)	Facts	Device/Cloud Owner (User)	Where/What	Notes
01/09/18	Will researches how to keep personal messages from showing up on iPad and family sharing information	Will	chrome history - Will's iPhone	Will and Felicity share his iCloud account which is making their phones "act funny" (syncing data to one another's device)
01/26/18	Felicity joins site "vampirefreaks.com"	Felicity	webkit data from Chrome	Oxygen works great for these as you can see all content
02/01/18	Will and Grace establish contact - Maryland	Will/Grace/Felicity (iCloud synced data)	Facebook	Possibly MD based on activity and map searches from Google Maps (Cloud data)
02/01/18	Will Googles Grace	Will	chrome history	
02/02/18	First contact between Grace and Felicity appears on Facebook as a feed comment, no response from Grace	Grace	Facebook (Cloud)	
02/03/18	Felicity starts questioning Will on Grace. He reassures her nothing is going on	Will/Felicity (cloud)	sms.db	
02/08/18	Will creates reminder searches for Flights, hotel and restuarants	Will	NoteStore.sqlite (iCloud Notes)	syncs to Felicity's device via iCloud
02/06/18	Felicity questions how Grace and Will know each other	Grace	Instagram (Cloud)	
02/08/18	Grace's first communication with Felicity	Grace	Instagram (Cloud)	
02/09/28	Grace searches how to lose a stalker and crazy ex wife	Grace	Ghostery	
02/10/18	Felicity friends Paul Lazarro on VampireFreaks	Paul/Felicity (Cloud)	webkit data from Chrome	Oxygen works great for these as you can see all content
02/12/18	Communication begins between Grace and Felicity through FB Messenger	Grace	Facebook Messenger (Cloud)	
02/14/18	Grace gets threatening message concerning will through FB Messenger	Grace	Facebook Messenger (Cloud)	
02/14/18	Felicity tells Paul via VampireFreaks that she thinks her husband will or already cheated on her and asks what she should do after stating "I hate her. If I can't have him I don't want anyone to."	Paul/Felicity (Cloud)	Felicity's cloud data or BB10 browser data	View in Hex if you can't see the conversations (data_3 Source file: /app/sys.browser.gYABgJYFHAzbeFMPCCpYWBtHAm0/appdata/data/webviews/cache/data_3) NOTE: also in data_1 and data_2
02/15/18	Grace searches for Google Allo help	Grace	Google Cloud Data Help	no Allo Application data found on device
02/17/18	Felicity begs Will to forgive her and he says he is leaving for Dallas	Will/Felicity (cloud)	sms.db	
02/17/18	Felicity starts to lean on Paul via VampireFreaks and he offers to "help solve her problem"	Felicity	Felicity's Google Cloud information	Gmail stored the messages
02/18/18	Felicty and Paul talk via Viber	Felicity	Felicity's Google Cloud information	Gmail stored the messages
02/18/18 - 02/24/18	Will and Grace together in Dallas	Will/Grace/Felicity (iCloud synced data)	calendar.db,Facebook Tags, EXIF data in JPGs confirms location, sms confirm they share a room	6528034772786952418.jpg
02/20/18	Will and Felicity argue via iMessage about "her"	Will/Felicity (cloud)	sms.db	Felicity gets this info from the shared iCloud syncing to her device
02/22/18	Grace and Will possibly getting married, mesage to Liz about Will and his wife being done.	Grace	GMail	
02/26/18	Will mentions divorce via iMessage to Felicity who won't respond to him	Will/Felicity (cloud)	sms.db	You see the response from Will's iCloud because Will and Felicity share an iCloud account at this point in time.
02/26/18	Grace continues to receive threatening messages from Felicity	Grace	Facebook Messenger (Cloud)	
02/27/18	Will tells Felicity to stop stalking grace	Will/Felicity (cloud)	sms.db	
02/28/18	Will conducts a Google search for "divorce attorneys in philadelphia"	Will	Safari history	found in BrowserState.db in tabs table
02/28/18	Grace logs into Amtrak - possible trip planning	Grace	Google Chrome (Cloud)	
02/28/18	Paul Lazarro (Hitman) arrives in PA and alerts Felicity that he has arrived and to say her final goodbyes	Paul/Felicity (Cloud)	Felicity's Google Cloud information	He arrives at 16:30 EST
02/28/18	Paul Lazarro (Hitman) confirms with Felicty that she wants to go through the "hit"	Paul/Felicity (Cloud)	Felicity's Google Cloud information	Gmail stored the messages
02/28/18	Felicity confirms and states "I'm not changing my mind. Do it ASAP"	Paul/Felicity (Cloud)	BlackBerry Broswer Cache	18:06 EST
02/28/18	Grace and Will are texting and then on a phone call. Grace hears a commotion	Grace/Will	Call logs and SMS	18:10 EST
02/28/18	Paul enters Will's house and shoots him, connects to the WiFi and reached out to Felicty telling her the "job is done"	Paul/Felicity (Cloud)	VampireFreaks.com via Chrome, WiFi	18:10 EST
02/28/18	Grace continuously reaches out to Will with no response		App data, Calls, SMS	
02/28/18	Paul sends Felicity a message on Vampire Freaks confirming that the job is done and thanks for the WiFi password and to send his money	Paul/Felicity (Cloud)	Felicity's Google Cloud information	Gmail stored the messages
03/01/18	Felicity wipes her iPhone and creates a new iCloud account	Felicity	database timestamps	Take note at lack of data!
03/01/18	Felicity gets an email confirming her Apple ID	Felicity (cloud)	Felicity's Google Cloud information	Gmail stored the messages
03/12/18	Felicity turns her device over to the police	Felicity	N/A	Data looks clean and she appears to be innocent