Hands-On quiz 9. Mobile Artifacts - Android

PURPOSE

- To understand mobile artifacts.
- To understand the connection between the examination and the investigation.

INSTRUctions

On your **host** machine, open your examination notes to continue updating them.

Throughout these instructions, you will be asked to take screenshots or answer questions (see sample below). Record this in your examination notes, which you will submit in Canvas.

Question # - This is a sample.

It is quite easy to get lost in the evidence and spend more time than needed. Concentrate on following the lab instructions. Nothing is hidden, and the labs are not graded based on how much 'stuff' you find. We are not trying to 'solve' a mystery but learn about forensics. We will be using the same case for multiple labs.

Exercise Prep

Please read carefully; this hands-on quiz is different than previous quizzes.

You will want to record the details of the answers below and the files in your examination notes, along with screenshots, for later reference.

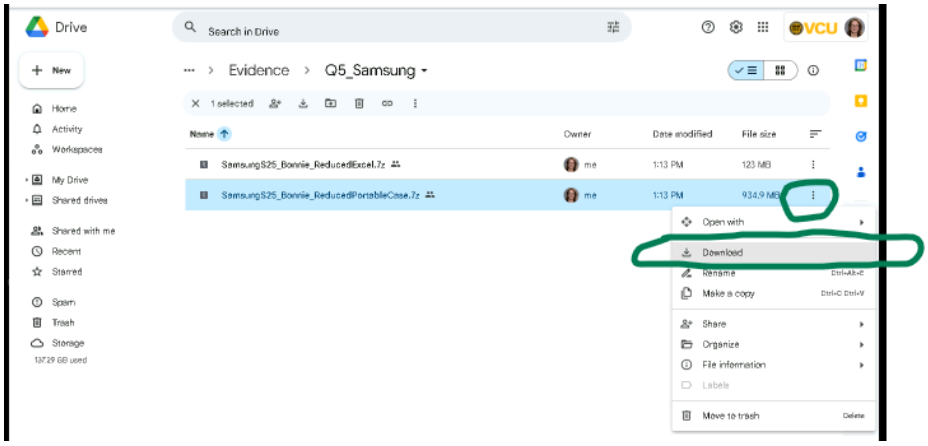
You will be briefing the investigator next Tuesday in class with the answers you find.

Once you have read through all the questions and finished the exercise preparation in the Virginia Cyber Range, start a 60-minute timer when indicated by the following instructions. Spend no more than 60 minutes looking for the answers in the data. (This is to simulate real life. We often have limited time to review data in critical incidents before the investigators want answers.) **It is also realistic that the investigator may be asking a question that does not have an answer in the data. These instructions and questions will differ from those in previous labs. This is intended to simulate the investigator's perspective and how they might ask questions.**

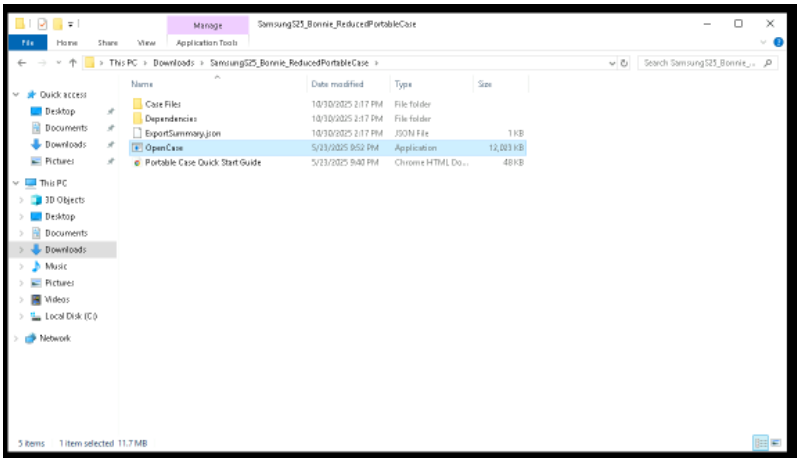
Do not open the Canvas Hands-On Quiz 9 until you are instructed to do so.

1. Go to the Virginia Cyberrange and open the **FRSC Treasure Island IP – Mobile Artifacts 10/22** environment.

2. Open **Chrome** type **my.vcu.edu** in the address bar and hit enter.
3. Login and access the Course Google Drive by selecting Student Email and log in. Then click the 9 dot menu, select Drive and Shared with Me.
4. Go to FRSC_525_DigitalForensics_Fall2025.
5. Go to InCyberRange > Evidence > Q5_Samsung and download SamsungS25_Bonnie_ReducedPortableCase.7z into your VM by click on the 3 dot menu and selecting download.



6. Answer Download anyway to scan dialogue. Downloading may take 1-5 minutes, depending on connection speed.
7. Close Chrome.
8. Open **File Explorer > Downloads** and right-click on SamsungS25_Bonnie_ReducedPortableCase.7z, select 7-zip and Extract files.
9. Delete SamsungS25_Bonnie_ReducedPortableCase.7z (not the folder.)
10. Double-click on the SamsungS25_Bonnie_ReducedPortableCase folder.
11. Double-click on OpenCase and wait patiently while it opens.



12. Click View All Artifact categories.

Scenario UPdate

It is still 6/15/2025. Earlier today, you provided the investigator with information from Billie's iPhone, which enabled them to locate the woman Billie believed to be Ginnie Hawkins. Her real name is Anne Bonnie. The investigator got a search warrant for her phone. The Samsung phone was acquired and processed with Axiom. Anne is coming in with her lawyer for an interview in a few hours, and the investigator has some questions that they hope to get answers in order to structure their interview.

What we know:

- Billie's contact information is: Billieacebones@gmail.com, 8042003954
- Money Man (the loan shark)'s phone number on Billie's phone is +18046101513
- Ginnie's phone number from Billie's phone is +18045020058
- Lady was taken on 6/14/2025 from the dog park at Short Pump Park (37.6468387,-77.6136157)
- A Teach in Billie's Phone is at Telegram user Ateach2025

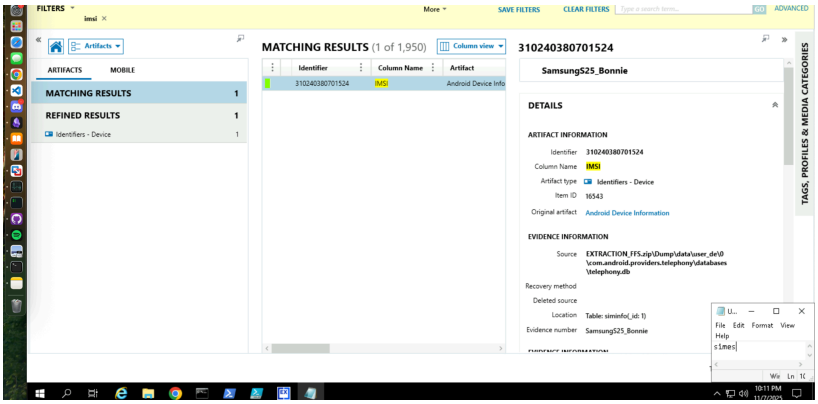
Investigators Questions

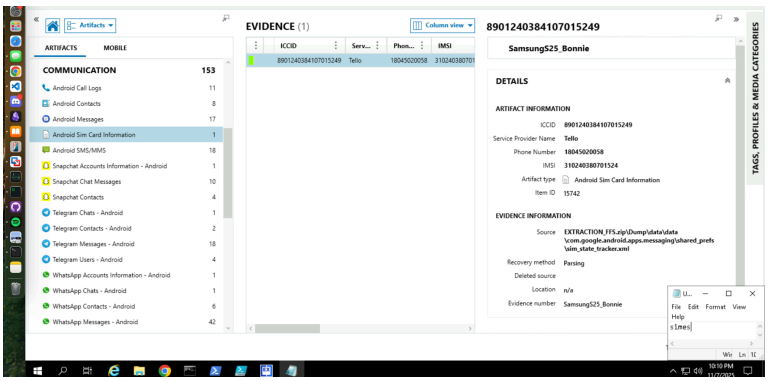
In real life, when a crisis occurs and multiple reviewers are examining the same data, they each focus on just a few key questions to ensure that all relevant questions are addressed. You are not expected to answer all the questions within 60 minutes. Answer what you can within the 60 minute period. When answering the questions below, use the following question order chart for your 60-minute review period. For example, Ashia would start at question 5, then proceed to question 6, and so on. Raymond would begin at question 15 and then proceed to question 16, and so on.

Student Name	**Question Order**
Marlon Adadey	1 > 2 > 3 > 4 > 5 > 6 > 7 > 8 > 9 > 10 > 11> 12> 13> 14 > 15 > 16 > 17 > 18 > 19 > 20
Kelvin Addo	2 > 3 > 4 > 5 > 6 > 7 > 8 > 9 > 10 > 11> 12> 13> 14 > 15 > 16 > 17 > 18 > 19 > 20 > 1
Savanah Allinson	3 > 4 > 5 > 6 > 7 > 8 > 9 > 10 > 11> 12> 13> 14 > 15 > 16 > 17 > 18 > 19 > 20 > 1 > 2
Juan Depazgonzalez	4 > 5 > 6 > 7 > 8 > 9 > 10 > 11> 12> 13> 14 > 15 > 16 > 17 > 18 > 19 > 20 > 1 > 2 > 3
Ashia Elliott	5 > 6 > 7 > 8 > 9 > 10 > 11> 12> 13> 14 > 15 > 16 > 17 > 18 > 19 > 20 > 1 > 2 > 3 > 4
Ebony Harris	6 > 7 > 8 > 9 > 10 > 11> 12> 13> 14 > 15 > 16 > 17 > 18 > 19 > 20 > 1 > 2 > 3 > 4 > 5
Jelani Howard	13> 14 > 15 > 16 > 17 > 18 > 19 > 20 > 1 > 2 > 3 > 4 > 5 > 6 > 7 > 8 > 9 > 10 > 11 > 12
Amanda Hurley	14 > 15 > 16 > 17 > 18 > 19 > 20 > 1 > 2 > 3 > 4 > 5 > 6 > 7 > 8 > 9 > 10 > 11 > 12 > 13
Raymond Jones	15 > 16 > 17 > 18 > 19 > 20 > 1 > 2 > 3 > 4 > 5 > 6 > 7 > 8 > 9 > 10 > 11 > 12 > 13 > 14

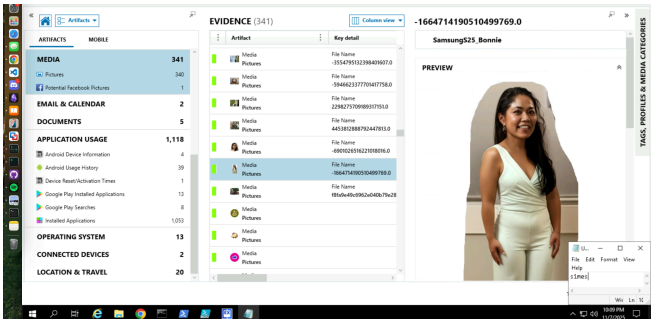
Gradi Kabasele	10 > 11> 12> 13> 14 > 15 > 16 > 17 > 18 > 19 > 20 > 1 > 2 > 3 > 4 > 5 > 6 > 7 > 8 > 9
Allen Lee	11> 12> 13> 14 > 15 > 16 > 17 > 18 > 19 > 20 > 1 > 2 > 3 > 4 > 5 > 6 > 7 > 8 > 9 > 10
Lauren Mack	16 > 15 > 14 > 13 > 12 > 11 > 10 > 9 > 8 > 7 > 6 > 5 > 4 > 3 > 2 > 1 > 20 > 19 > 18 > 17
Vrund Patel	17 > 16 > 15 > 14 > 13 > 12 > 11 > 10 > 9 > 8 > 7 > 6 > 5 > 4 > 3 > 2 > 1 > 20 > 19 > 18
Ian Richards	18 > 17 > 16 > 15 > 14 > 13 > 12 > 11 > 10 > 9 > 8 > 7 > 6 > 5 > 4 > 3 > 2 > 1 > 20 > 19
Shane Simes	19 > 18 > 17 > 16 > 15 > 14 > 13 > 12 > 11 > 10 > 9 > 8 > 7 > 6 > 5 > 4 > 3 > 2 > 1 > 20
Tyrus Somuah	20 > 19 > 18 > 17 > 16 > 15 > 14 > 13 > 12 > 11 > 10 > 9 > 8 > 7 > 6 > 5 > 4 > 3 > 2 > 1

Start the Timer and Answer these Questions

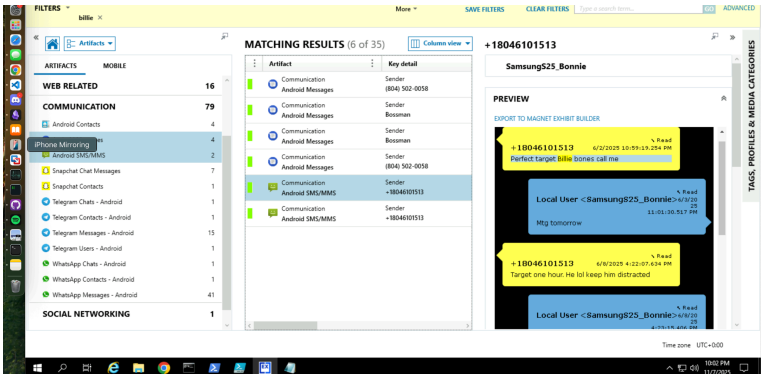
1. What is the subscriber ID for this phone?
    a. 310240380701524
    i. 

2. What is the phone number for this phone?
    a. 18045020058
    i. 

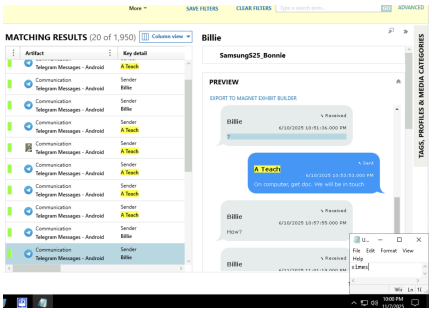
3. What is the service provider for this phone?
    a. Tello
4. What communication apps does Anne use?
    a. Snapchat, android message, Whatsapp, telegram
5. Is there any user attribution for Anne Bonnie, such as a picture or personal information?
    a. Yes

b. 

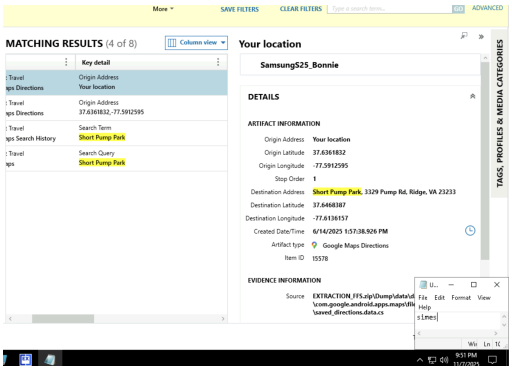
6. What accounts or IDs are on the phone for Anne Bonnie?
    a. annepieces8@gmail.com, A Bonnie (google account)
7. What accounts or IDs are on the phone for Ginnie Hawkins?
    a. hawkinsginnie97@outlook.com, ginnieh_dogluvr (snapchat), Ginnie (whatsapp)
8. Any communication with Bille Bones? If so, with what apps?
    a. Snapchat, telegram, whatsapp, android message

i. 

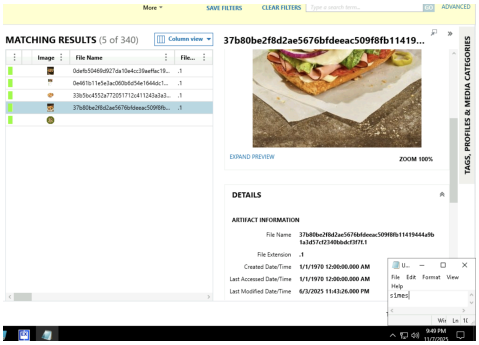
9. Any communication with A Teach? If so, with what apps?
    a. Telegram Messages showing sender is A Teach

i. 

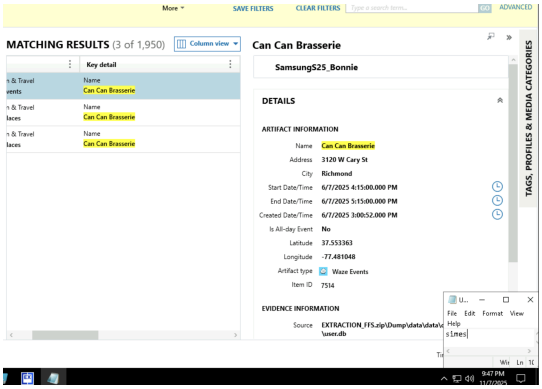
10. Any communication with John Silver? If so, with what apps?
    a. No Communication with John Silver
11. Any communication with Jack Rackam? Is so, with what apps?
    a. No Communication with jack rackam
12. Was Anne preparing to dognap a dog? If so, how?
    a. I don't see any proof of planning to dognap
13. Has this phone been at Short Pump Dog Park?
    a. Yes, 6/14/2025

i. 

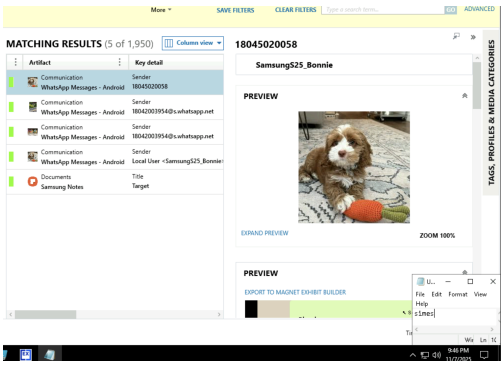
14. Has this phone been to Panera? If so, when and which one?
    a. Yes, 6/3/2025

i. 

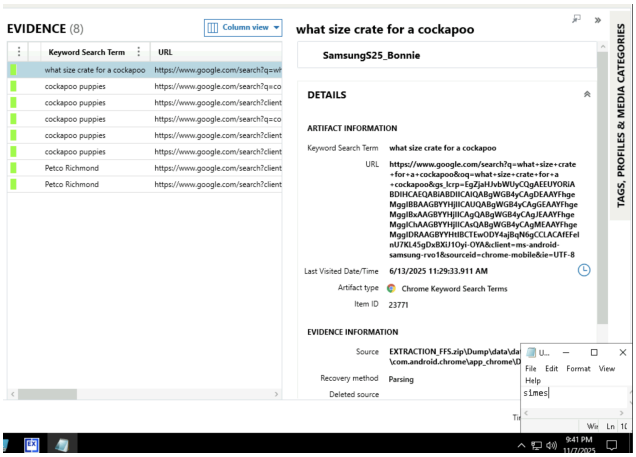
15. Has this phone been to Can Can Brasserie? If so, when?
    a. Yes, 6/7/2025

i. 

16. Any locations that could be searched for the dog Lady?
    a. Whatsapp and notes

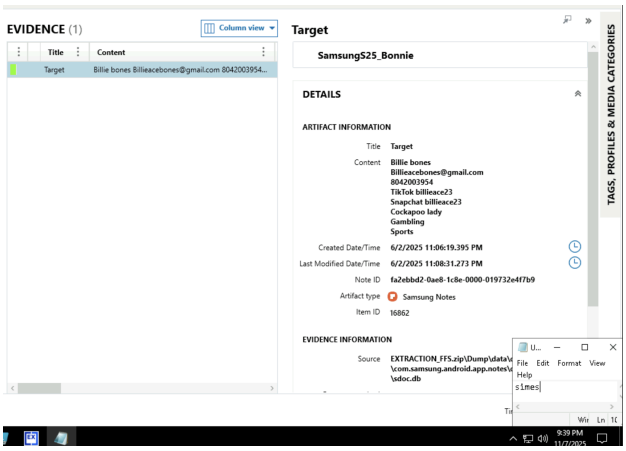
i. 

17. Any relevant web searches?
    a. Crate Sizes for a cockapoo



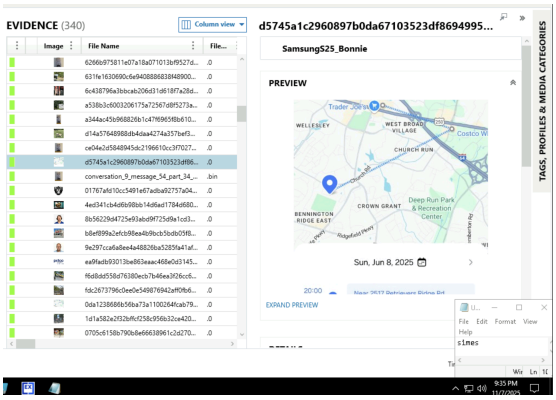
    i.

18. Any relevant notes or documents?
    a. Note saying billie is a target



    i.

19. Any relevant photos?
    a. Photos of Dogs
    b. Picture of dog kennel and receipt showing kennel and leash purchase
    c. Picture of Deep run rec center
    d. Picture of gps locations



    i.

20. Any home or work information for Anne Bonnie?

Submission

Now you can open the Hands-On Quiz 9 in Canvas.

Update your examination notes and report as appropriate. Bring the answers you have with you to class on 11/11, and we will discuss the case with the investigator.

Complete Hands-On Quiz 9 in Canvas by the due date.

Find Problems with the Lab?

Spelling? Something confusing? Instructors are human too.

If you found any problems with this lab, turn on Track Changes in this Word document. (***Review -> Track Changes***)

Make the changes.

Save the file with your last name at the end of the file name and email it to shaferk@vcu.edu.

You will receive extra participation points for the help.

And thank you!

