Mind the Gap Persona

Josh Anderson

Work & Education

- Beginner Network Analyst at the Counterterrorism Tradecraft Support Office
- Student in after-hours for a degree in Data Science

About Me

Age: 21 Years Old

Favorite Song: Light On - Maggie Rogers

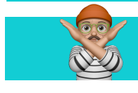
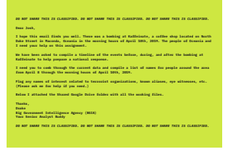
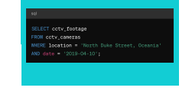
Favorite Movie: Perks of Being a Wallflower

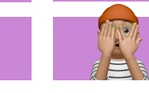
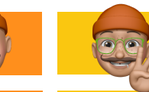
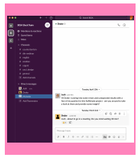
Favorite Color: Ticonderoga Wood Pencil Yellow

Zodiac Sign: Cancer (June)

Pain Points

- Limited knowledge of global telecommunications
- All knowledge has been acquired through just-in-time training events.
- Cannot visualize where the query went wrong

Time	8:00 A.M	9:00 A.M	10:00 A.M	11:00 A.M	12:00 P.M
Overview	Email & Review Assignments		Craft & Execute Queries		
Context	Josh begins his day.		QUERY A / QUERY B / QUERY C / Complete at the end of each Query		
Activities	Josh pours his cup of coffee when Drake, a Senior Analyst he is paired with, walks in and asks Josh to check his email when he returns to his desk.	Josh gets to his desk and is shocked by the 13 emails in his inbox. He makes note in his to-do list to check those later. He checks the email from Drake with his project assignment and the shared Drive folder.	Josh reviews his assignment and uses it to create a rough timeline in Google Docs of the events of April 10th. Josh makes sure to include gaps in the timeline in order to understand what he is searching for.	Then Josh opens a new software PowerGREP & decides to run a query searching for all data points that took place on the day of April 10th. / Josh references his notes from training on how to convert timestamps into epoch format so he can find all events happening on April 10th to help build his timeline. Josh sends the query in PowerGREP. / He runs a second query in BleepingComputer to look at the CCTVs on the buildings in the vicinity of Kaffeinate to get more information about who all was around the building on April 10th. / Josh also wants to analyze eyewitness account data, but he realizes it is in varying formats that can't be interpreted by one tool. / Josh manually inputs the eyewitness account data he has gathered from social media, NextDoor, and news reports into Google Sheets to cross analyze with the reviews from Kaffienate. / He cleans and imports this data from his Google Sheet into Knime with his completed query form. / Josh makes a note in his Google Doc of what he has done so far then takes a lunch break while his queries are running.	Out for Lunch
General Location	Office Kitchen	Josh's Desk	Josh's Desk		
Tech & Software	Coffee Machine iPhone Email	Monitor Email Google Drive	Monitor Email Google Docs Reliable News Sources	PowerGREP Data File / PowerGREP Data File Google Docs + Drive Epoch Converter / BleepingComputer Data File CCTV Camera Map Wifi Enabled Electronic Cameras / Google Sheets Social Media Credible News Reports Nextdoor Data Sheet / Google Sheets Knime / Google Docs	
Emotions					
Painpoints	Socialization before coffee	Multiple priorities Multiple sources for information Volume of email and requests	Doesn't know where to start There is a fair amount of context missing	Doesn't know most efficient way to query Intimidating dataset New and unfamiliar tool / Multiple tabs open Multiple softwares running at once / Data formats vary Multiple softwares running Overwhelming / Manually searching and inputting data Intimidating dataset Stressed / Difficult to consolidate information Extra steps to clean & manipulate the data Data is subject to human error / Documentation amount Long wait time for results	
Gainpoints		The highest priority task is laid out for Josh	Project assignment matches skill level	Learning new skills and tools / Feels confident in the tool and query / Josh is relieved he thought of eyewitnesses / Finishes cleaning data Has 15 minutes until lunch / Lunchtime	
Data			Josh's Timeline	Searching for April 10th (1554900000000) 00:00:00-24:00:00 (1554868800 - 1554955200) / Searching CCTV Footage  / Timeframe of Interest (April 8th - April 10th) / Cross analyze names from April 8th (1554699600) to the morning of April 10th (1554900000000) to gathered data. / Documentation includes query syntax, softwares used, and Josh's anticipated results.	

Time	1:00 P.M	2:00 P.M	3:00 P.M	4:00 P.M	5:00 P.M	OFF DA CLOCK
Overview	Analyze Results			Modified Queries	Documentation & Share Results	Leaving Work
Context	When Josh returns from lunch, he sees that his queries have all finished.	Josh investigates the Knime error.	Finally, Drake comes over to Josh's desk and asks to review Josh's submitted queries in addition to his anticipated results.	Josh modifies and reruns his queries based on Drake's comments.	Josh summarizes his daily activities and findings for Drake in the shared project folder.	EOD
Activities	For Query A, Josh received too many results to sort through manually and make a conclusion. He realizes his syntax likely wasn't specific enough to get the data he really needed. / For Query B, Josh sees that his query has returned no results. He isn't sure if his query syntax was the problem, or if this is a collection gap. He makes a note to get a second opinion on his query from Drake. / For Query C, Knime returns an unexpected result. Josh remembers he made a note about multiple lines of data from NextDoor mentioning drone sightings, none of which came up in the query results.	Josh realizes he will need tradecraft help from Drake. / Before he goes to ask for help on Query A and B, Josh attempts to solve the problem for Query C on his own, investigating why his results didn't yield the expected outcomes. / After 30 minutes, Josh notices that Knime removed a couple hundred rows of data that it could not read and did not provide an error pop-up indicating such. / Josh wonders if he cleaned the data properly. He makes a note in Knime's note field and in his working Google Doc about the error. / Josh messages Drake on Slack to see if he is available to meet and look at Josh's specific problems. Drake asks if Josh can wait, as Drake is about to go into a meeting.	Drake finds a problem with Josh's syntax for Query A. Drake shows Josh how to improve his query filter to sort the data by timestamp in order to narrow his results. / For Query B, Drake finds no problems with Josh's syntax. He recommends executing a new query to determine if the CCTV footage actually exists, or if this is a collection gap. Josh makes a note of this so he doesn't forget. / For Query C, Drake agrees that Josh may have not cleaned the data properly. He recommends watching a BGIA training video to refresh Josh on this process. He tells Josh he may have to re-run Query C after cleaning the data a second time.	For Query A, Josh adds a filter to his query to look only for the timestamps of the gap areas in his current timeline. He makes a note of the modified query syntax and his anticipated results. / For Query B, Josh uses Power Bi, a new software. He starts a new query for CCTV Reports from April 8th - April 10th. It instantly pulls up a report. Josh takes notes. / For Query C, Josh looks over BGIA tradecraft and trainings to improve his syntax and refine his data cleaning process. He finds a common error, that the data didn't merge properly, he recompiles it and reruns the query. Josh takes notes.	Josh realizes it is almost time to leave for the day, so he begins documenting his findings, the queries he has left running, and gaps in data. / He saves and uploads this document to the relevant project website so his team can access it, and so he can remember where he left off tomorrow.	Josh packs his bag and heads to his car and plays Motion Sickness by Phoebe Bridgers
General Location	Josh's Desk			Josh's Desk	Josh's Desk	Josh's Car
Tech & Software	PowerGREP Data File Google Docs Google Drive / BleepingComputer Data File CCTV Camera Map Google Docs / Google Sheets Knime Google Docs	Google Docs Knime BGIA Tradecraft / Google Docs Knime / Google Docs Knime / Slack	PowerGREP Google Docs / Bleeping Computer Google Docs / Knime BGIA Tradecraft Google Docs	PowerGREP Google Docs / Power Bi CCTV Reports Google Docs / BGIA Tradecraft Knime Google Docs	Software Note Fields Google Docs Google Drive / Software Note Fields Google Docs Google Drive	
Emotions	 					
Painpoints	Results are overwhelming or confusing Unsure of proper querying syntax / No results Collection gap / Unexpected results Confusion / Imposter syndrome Feeling of inexperience becomes overwhelming / Intimidating dataset Manually combing through data/results / Time consuming Software removed data Malfunctioning error notification system / Anxious if he missed something Multiple note fields / Has to wait for help / Losing time for analysis Embarrassed for making a silly mistake / Collection gap Has to rewrite query Has to use a new software / Has a new task Repetition of time consuming steps Questions abilities			Repetition of time consuming steps / New software Difficult to find information / Repetition of time consuming steps	Contextualizing and communicating analysis	Emotionally worn out from the day.
Gainpoints	Was able to identify his mistake himself / Looks forward to collaborating with Drake / Communication allows for insight and perspective and resource sharing / Help is accessible easily / Query A Solution / Didn't make an error! Proper workflow process / Thankful there is a resource			Feels more confident about this query because of Drake's help / Closes a timeline gap. / Josh manages to fix the error he was having. Additional software experience.		Doesn't have class today and gets to go home and watch Shrinking.
Data	Query Results from PowerGREP Search Personal Documentation (Google Docs) / Query Results from BleepingComputer Personal Documentation (Google Docs) / Eye witness accounts, X Social Media, Google Sheet Personal Documentation (Google Docs)	BGIA Tradecraft Knime Results / Query Results from Knime Dataset Personal Documentation (Google Docs) / Personal Documentation (Google Docs) 	BGIA Tradecraft PowerGREP Software / Josh's Modified Query in BleepingComputer / Updated Query C with syntax for missing data error included:	Josh's Modified Query in BleepingComputer / Report states the cameras were down for maintenance from April 6th - April 11th, no feed was documented. Personal Documentation. / BGIA Tradecraft Personal Documentation	Personal Documentation / Personal Documentation, Shared Team Documentation	