Miguel

Senior TDNA

SME in Zendian affairs

Miguel is a senior Target Digital Network analyst at BGIA. His daily work deals with understanding current intelligence topics worked by BGIA's Zendian Office as well as acquiring access to data to meet the **intelligence needs.**
His work can cover a wide range of data types and priorities frequently change as events occur. Miguel plans and oversees his team's activities, but is not a supervisor.

- Introverted — Extraverted
- Analytical — Creative
- Independant — Team player

Master of Science in Information Security | Joined BGIA 15 years ago | Python coding experience | Mentors Junior TDNAs

Legend
- Intentions
- Interface Actions
- Teammates' Actions
- Collaboration
- Tools and Query
- Definitions

Timeline

9 am	10 am	12 pm	3 pm
Reviewing Emails and Assessment	Craft & Execute Queries	Analyze Results	Document & Share Results

Actions

Reviewing Emails and Assessment (9 am)
- Leaves personal electronics
- Sits by his desk
- Logs in
- Check's his email
- Receives access from BGIA
- Creates an Agenda for the day
- Schedules meeting with the team
- Discuss analogies with the team about the observable evidence

Craft & Execute Queries (10 am)
- Opens analytical tools
- Finds packets of data
- Comes up with queries and runs them
- Checks on his teammates queries
- Suggests changes and mentors juniors
- Finds gaps in the data
- Runs faceted filtering searches
- Reviews tradecraft & compliance

Analyze Results (12 pm)
- Tradecraft lunch
- Triage the data for what is relevant
- Merge disparate data objects from other queries
- Collect team's findings
- Making sense of data
- Summarize data and explain its relevancy

Document & Share Results (3 pm)
- Copying and pasting results from various sources he visited this day
- Combining Data Summaries and requesting additional collections for next day
- Preparing summary and presentations for leadership
- Analyzing and incorporating feedback from previous briefings
- Briefing the leadership on the results of team's work

Taskflow

9 am

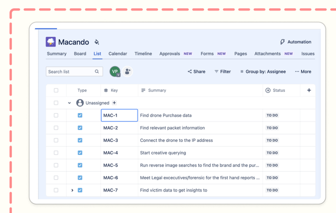
Logs in → Check's his email → Notified that a bombing as occurred at Macondo → BGIA grants access to network traffic datasets and communication records related to the Macondo bombing attack → Receives pictures of parts of a Drone and accurate location of the attack from BGIA

→ Realizes that he needs to use multiple sources and tools related to cellular and wifi Network traffic and geospatial and ONSIT tools around the area.

Agenda creation

Available Data	Data needed	Task Assignment fo...
Drone images	Drone purchase history	Junior TDNAs
CC TV footage	permissions and compliance issues regarding the communication data	Language analysts
Wifi_SSIDs	Communication reccords	Law enforcement department
Information from passerbys and first responders	Elecronic device activity	Reporters
	Sensor activity	Data analyst
	relevant articles about the info	

→ Opens Jira for work flow management



→ Schedules meetings around the day → First meeting begins → Discuss/brainstorm about the available information to connect the dots. Introduce the agenda for the day. → Agenda: Find drone network and the weapon used

10 am

Opens tools and tabs
- He opens wifi network data base
- ONSIT (sources open-source intelligence) Publicly available sources
- Image search t...
- Meighal open Xplico to find packets of relevant data
- Network traffic monitoring tool
- Uses image recognition to search places, people

→ Filter Packets (searching relevant packets of data from the internet/mobile service network used in that area to communicate)

Query
1. Purchase data of drone (from bombing date to a month)
2. Internet search for drone companies
3. Messages related to the criteria in wifi network: macondo_wifi
4. Voice detection speaking in Zandian language
5. Incoming International calls from Zandia to Cell Tower ID 43390

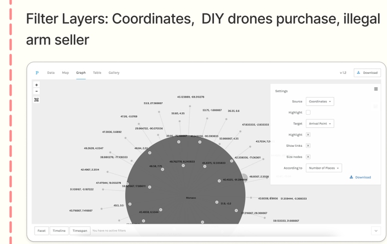
- Miguel sends Voice notes to language analyst
- Miguel send raw data to his team → TDNA juniors team mates a come up with queries to run to clean the broad data given them

```
In [ ]: sorted_df = df.sort_values(by='date', ascending=True)
```

TDNA juniors team mates reach back to Miguel for reviewing queries
- Michele, junior TDNA not being able to come up with efficient query and gets 0 → Miguel recommends him to check the BGIA Tradecraft Repository (TC Hub) and use "drone tutorial" k... → Michele searching for Trade Craft related to drone on TC Hub
- Josh finds a packets of data about buying DIY drone → Query: Search for DIY drones purchase data base from (from bombing date to a month)
- Susie finds a packets of data about making a IED → Query: Search for illegal arm seller who sells explosive

→ Junior TDNAs shares observable evidence data back to Miguel → Miguel runs a faceted filtering on packets to look for clues related to the bombing

Filter Layers: Coordinates, DIY drones purchase, illegal arm seller



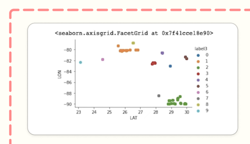
→ Miguel found gaps in the data, he realised that the Zandian might made procedural searches for building a drone or explosives

Query:
1. Youtube searches within the area for building a drone;
2. Youtube searches within the area for creating an explosive

12 pm

TRADECRAFT LUNCH
- Lunch but with talking about work related tasks and workflow in an informal setting
- Josh, junior TDNA, points out to how he wants to visualize the amount of drone purchases made in Oceania and Zendia within last month to compare aspects of both but is lacking skills to do so
- Miguel offers Josh to code a tool in JN that would easily visualize such graph for him
- Team is coming up with analogies to find alternative solutions
- Team is also discussing new standards and BGIA's tradecraft repository

→ Miguel shares all the found data to the data scientist → Data scientist tries to find specific data → Visualize and find clusters of data with purchases of commercial drone found



use chat for impromptu brainstorming sessions so they can share screens, copy and paste lead information, and discuss other anomalies that emerge during analysis

Clean Data → Zendian Groups / Weapons / Networks used to operate the drones

→ Miguel imports all the data files to the Jupiter notebook library and **performs technical analysis** to find more clustered data

Query: Find suspicious activity using wild card operator while filtering a cellular network related to an international call.

→ Miguel is using the Jupiter Notebook to build possible connections between those three categories → Miguel looks through his notes from the tradecraft lunch and **analogies** his team came up with helps him build new connections

- Miguel is using the JN to visualize data on Zendian groups. → Query: Search "drone" on Social Media and Map Review Platforms → Miguel notices that Google Maps reviews on bombed place led to 8 possibly suspicious comments → He reads through them and shares them with the team via chat for feedback → Data: comment left by Victor M. left on April 8th "Wanted to find a new place to fly my DJI Mavic Pro drone."
- Miguel is missing the information about the drone remains that was found on the location of the bombing so he is requesting additional info from his team that is working on researching zendian groups. → Miguel requests this query to be run tomorrow via the team chat
- Miguel conducts **packet capture** on the network to capture communication data between the drone and its operator, if controlled remotely. → Miguel finds out that one of the drone's remains required an additional expertise so the hardware could not be used to download datasets. → He reassigns this task to someone else on his team for tomorrow.

→ Miguel summarizes his findings

3 pm

Miguel refers back to his notes that document his and his teammates query and analysis process → Traces back all his steps throughout the day to document his steps in more detail → Miguel documents the framework of all his findings → He keeps in mind that he needs to explain the terms and simplify some vocabulary to make it accessible for other positions (Data Sources, Methodologies, Cleaning process, Tools used) → Miguel retraces missing data from the day and makes sure to note it for tomorrow's quarries/reassignment of the tasks → Miguel also highlights good practices and successes throughout the day for future references → He ensures that documentation aligns with industry best practices and compliance requirements. → Miguel also prepares a presentation on his team's findings for the briefing with the BGIA tomorrow morning → Miguel checks on his team last time for the day and adds notes for creating agenda tomorrow

Pain points

9 am
- Multiple priorities
- Infodumping with no categorization
- No prioritization
- No urgency warning on emails
- Chance of ignoring
- Emails are inaffective due to huge volumes
- Multiple sources for information
- Does not understand the starting point
- Time consuming
- Figuring out right medium to communicate
- Rapidly changing compliance requirements and data

10 am
- Junior TDNA may lack the pre requisite knowledge to search effectively and judge relevance which leads to zero results
- Time consuming
- Due diligence
- Only few set standardized Trustworthy tools
- A lot of time goes into investigate whether other tools & databases may return more efficient data
- Too much cognitive load associated with the task on
- Different components of the task (e.g., data sources, tools, technologies, processes, etc)
- Data science and analytics communication challenges
- Not being able to find relevant trade craft in repository
- Skill difference at entry level
- Makes mentoring more taxing
- Rapidly changing tools
- No recorded/online training modules or forums for new TDNA

12 pm
- Increased load on miguel to help juniors
- Unorganized tools and data
- Limitation of tools to visualization of data
- Different communication tools for different roles
- Time consuming
- Switching contexts too often
- Requires high concentration
- Load on working memory while using Multiple Tools
- Frustrations with the knowledge gaps

3 pm
- Manual and tidious process
- High Cognitive load to avoid Mistakes
- Time consuming
- Lots of retracing the steps
- Risk of errors
- Lack of version history
- Frustration in the amount of time needed to manual documenting the data they found

Gain Points

9 am
- Prioritize Information
- Effective communication between teams
- Efficiency Alert systems
- Quick communication on urgent information
- Efficiency in planning of agenda

10 am
- Data Organization
- Compliance warnings at different stages
- Effective Training/onboarding models catering to skill difference
- Solid Tradecraft system
- Standardized systems to avoid confusion
- efficient Tradecraft search

12 pm
- Good communication
- Visualizations helping data understanding
- Increased Adaptability and Flexibility
- Quick and effective sensemaking

3 pm
- Version history
- Accuacy and relyability
- Knowledge sharing
- Trust

Moods

Scale: Satisfaction, Confusion, Frustration

- Saturated morning: High volume of emails and high responsibility
- talking to his team (he loves them)
- Navigating between tabs and remembering yesterday's queries
- Heavy cognitive load and multitasking
- High concentration and hoping that no-one interrupts him
- Empowering time with the team and lunch
- Summarizing loads of data and finding out missing info
- Mentoring his team mates with their queries
- Sitting still and trying to remember the actions throughout the day
- Presenting results of his and team's work

Tools

9 am: Email, Chat, Workforce management tools, Jira

10 am: WireShark, Jupyter Notebook, Xplico, Bellingcat, BGIA Standards and Repository

12 pm: WireShark, Jupyter Notebook, Whiteboard for brainstorming, Chat, OneNote, Email

3 pm: OneNote, Jupyter Notebook, Jira, Chat, BGIA Standards and Repository