Incident Background

GAStech and the Protectors of Kronos

- GAStech (GT) is a company operating in the calm Island of Kronos. The company faces backlash from an environmental activist group called Protectors of Kronos (POK).
- Several key executives from GT go missing on January 20th, it is speculated that POK is behind their disappearances.
- Law enforcement provides data from the past two weeks preceding the incident (Jan 6th-19th) in order to investigate GT employees, to assist the investigations
- GT offers nice cars to employees which they use both for business and personal use, however, it secretly tracks the location of all cars. Truck drivers do not have business cars and only use trucks for business purposes. Cars are tracked while in use and are not shared.
- Personal/business credit/debit card data is also provided. The use of loyalty cards in the different business in town is also tracked.
- Datasets provided are: credit card, loyalty, gps data, car assignments, and geo-spatial data
- We're tasked to identify 12 suspicious events, support them with data, and answer:
    - What is the event?
    - Who was involved?
    - What locations did it happen?
    - When?
    - Why?
    - What is our confidence level?

UNIVERSITY of DENVER

DANIEL FELIX RITCHIE SCHOOL
OF ENGINEERING & COMPUTER SCIENCE

The Island of Kronos: City of Abila

What were the challenges?

- Datasets have different encodings.

- There are no primary keys in the data.

- Timestamps are not consistent, each dataset uses its unique type.

- Truck assignments are not tied to individuals.

- While GT secretly tracks employees, it's unknown if executives and/or security is aware of this fact, thus evading tracking.

- No distinction between personal and business purchases.

- Never worked with this type of data

- Geo-spatial files had errors

- Shapefiles had no POIs

- Tourist map did not contain all stops

- Too many POIs to manually tag

- GPS did not contain employe names or location names

UNIVERSITY of DENVER

DANIEL FELIX RITCHIE SCHOOL
OF ENGINEERING & COMPUTER SCIENCE

Time Breakdown
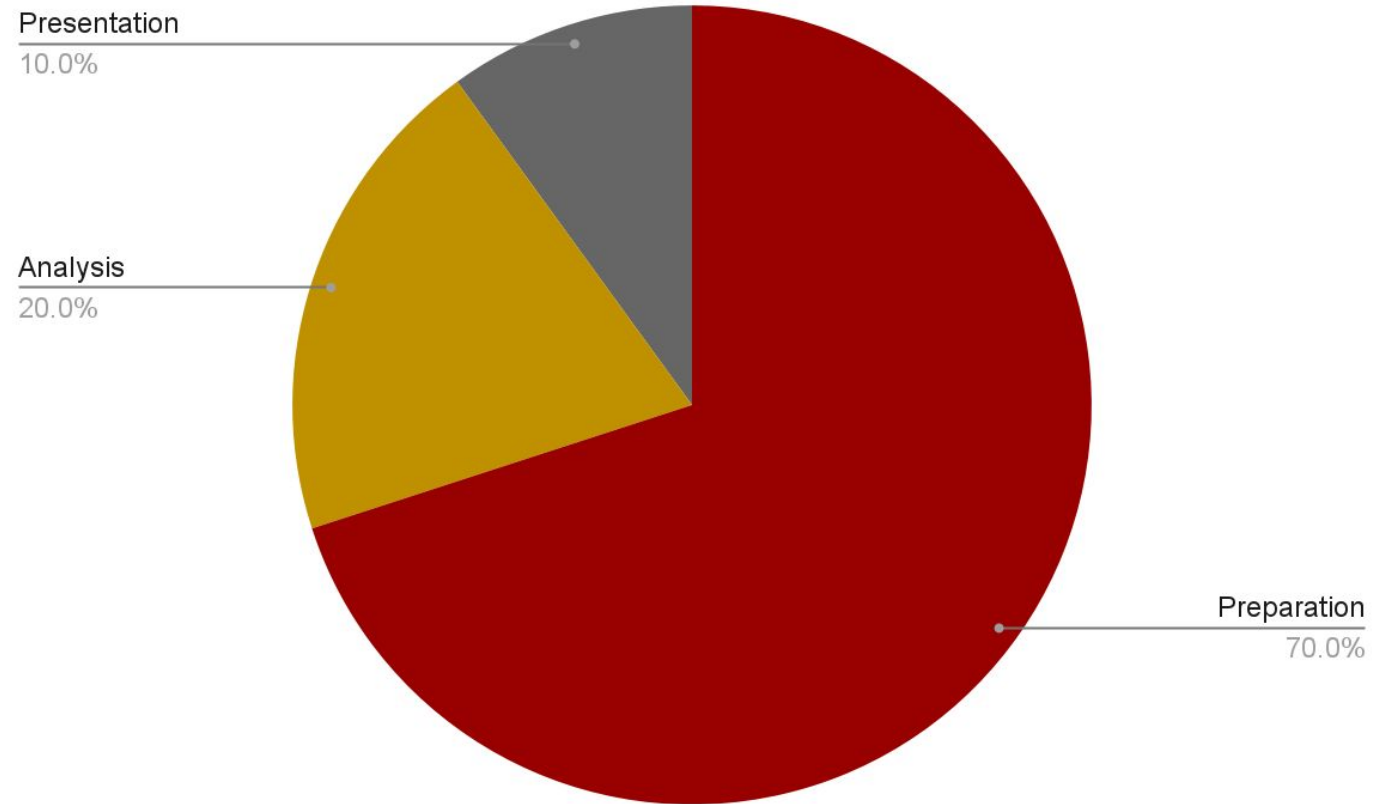
ABCD People Profiling

- There is a total of 44 employees to investigate, ~1500 credit card records, ~1400 loyalty transactions and staggering 685,000 GPS records to process.

- The data does not share a common key, a 1:1 relationship was established so that a common key could be generated and thus have the data easily referenceable across multiple data sets.

- Date/time values were also standardized across the board, missing information was often populated by inferring other datasets.

- After all that, individual analysis for each employee would be lengthy, a profiling routine was developed which ingests all data sets and reports and highlights patterns that warrant further investigation.

- Local Outlier Factor was the only model used in the profiling in order to highlight outlying credit card purchases which may not be easily identified.

People Profiling – Sample Report

- First name: Orhan
- Last name: Strum
- Title: SVP/COO

- Spending Pattern:
- Total spent: 2212.51
- Avg spent/day: 158.04
- Median purchase: 31.2
- Number of purchases: 34
- Average purchases/day: 2.43
- Top 3 days with most purchases:
-       count(*)   date
- 0   3   2014-01-18
- 1   3   2014-01-15
- 2   3   2014-01-13

- Top 15 purchases:

	timestamp	location	price	loyalty
0	2014-01-12 03:39:00	Kronos Mart	277.26	0
1	2014-01-18 15:40:00	Shoppers' Delight	258.33	1
2	2014-01-18 18:59:00	Albert's Fine Clothing	226.49	1
3	2014-01-19 12:41:00	Desafio Golf Course	150.07	1
4	2014-01-12 13:32:00	Ouzeri Elian	117.22	1
5	2014-01-18 13:04:00	Abila Zacharo	111.93	1
6	2014-01-08 13:21:00	Ouzeri Elian	109.73	0
7	2014-01-11 19:27:00	Albert's Fine Clothing	105.33	0
8	2014-01-13 21:27:00	Hippokampos	99.63	0
9	2014-01-14 12:00:00	Jack's Magical Beans	95.70	0

- Average purchase per location (top 10):

	location	avg(price)
0	Kronos Mart	277.26
1	Shoppers' Delight	258.33
2	Albert's Fine Clothing	165.91
3	Desafio Golf Course	150.07
4	Ouzeri Elian	113.475
5	Abila Zacharo	111.93
6	Hippokampos	37.34
7	Katerina's Café	33.39
8	Guy's Gyros	33.00
9	Jack's Magical Beans	31.42

- Loyalty Pattern:
- Number of loyalty purchases: 22

- Top 3 loyalty purchases:

	timestamp	location	price
0	2014-01-18 15:40:00	Shoppers' Delight	258.33
1	2014-01-18 18:59:00	Albert's Fine Clothing	226.49
2	2014-01-19 12:41:00	Desafio Golf Course	150.07

- Suspicious loyalty purchases:
- Unmatched!   Day: 2014-01-06 Jack's Magical Beans   7.84
- Unmatched!   Day: 2014-01-08 Ouzeri Elian   29.73
- Unmatched!   Day: 2014-01-13 Hippokampos   39.63
- Unmatched!   Day: 2014-01-14 Jack's Magical Beans   15.7
- Unmatched!   Day: 2014-01-15 Jack's Magical Beans   4.06
-   Matched!   Day: 2014-01-19 Ouzeri Elian   45.32   w/ Sven Flecha

- Driving Pattern:
- Distance driven: 212.09km
- Avg driven/day: 15.15km
- Breakdown per day:
- Distance driven on day 6 : 21.88km
- Distance driven on day 7 : 16.94km
- Distance driven on day 8 : 10.05km
- Distance driven on day 9 : 16.38km
- Distance driven on day 10 : 16.99km
- Distance driven on day 11 : 17.35km   (Weekend)
- Distance driven on day 12 : 9.41km   (Weekend)
- Distance driven on day 13 : 18.24km
- Distance driven on day 14 : 12.39km
- Distance driven on day 15 : 20.58km
- Distance driven on day 16 : 17.84km
- Distance driven on day 17 : 14.19km
- Distance driven on day 18 : 12.98km   (Weekend)
- Distance driven on day 19 : 6.82km   (Weekend)

Tool Building


- Found that the Abila Shape data exactly overlaid with the tourist map.
- Decided to use GPS file with Tourist Map for analysis.
- Added stop data to GPS by marking entry that had >5 minutes to the next stop.
- Added employee data to file.
- Truck data was missing so looked at truck routes and card purchases and assigned trucks based on those.
- Created 3 dashboards (plotly Dash) to explore GPS data
    - One by name, date, and time
    - One by employment type, date, and time
    - One by employee and shows all dates and routes
- Local Outlier Factor used to identify stops worth investigating in detail.
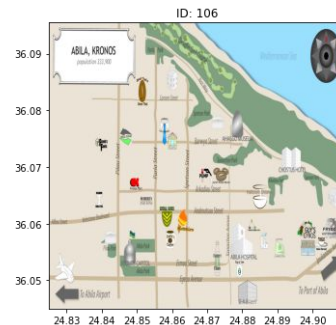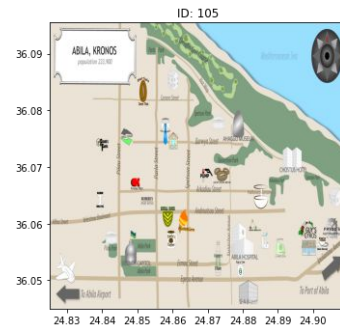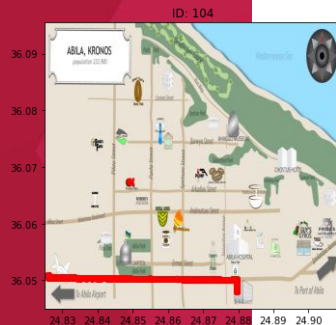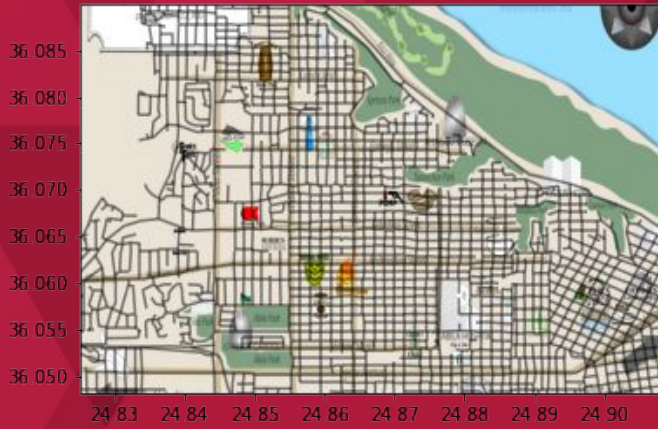
Dashboard Example
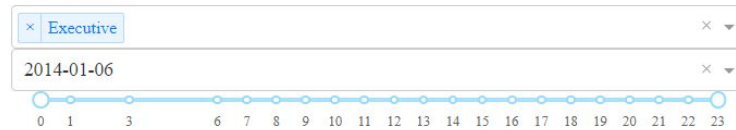
Routines and Events

Theory/Narrative

Through Analysis of Credit Card, Loyalty card data, we were able to paint a picture of the daily lives of the GAStech employees.

From the data gathered over two weeks, patterns emerge to give a suggestion to what happened to the missing executive.

From the discrepancies we believe the executives were kidnapped by a group of people working security for the company.

We have evidence to show that this was planned over the two week prior along with who is involved.

We also found other discrepancies to look into for a thorough investigation.
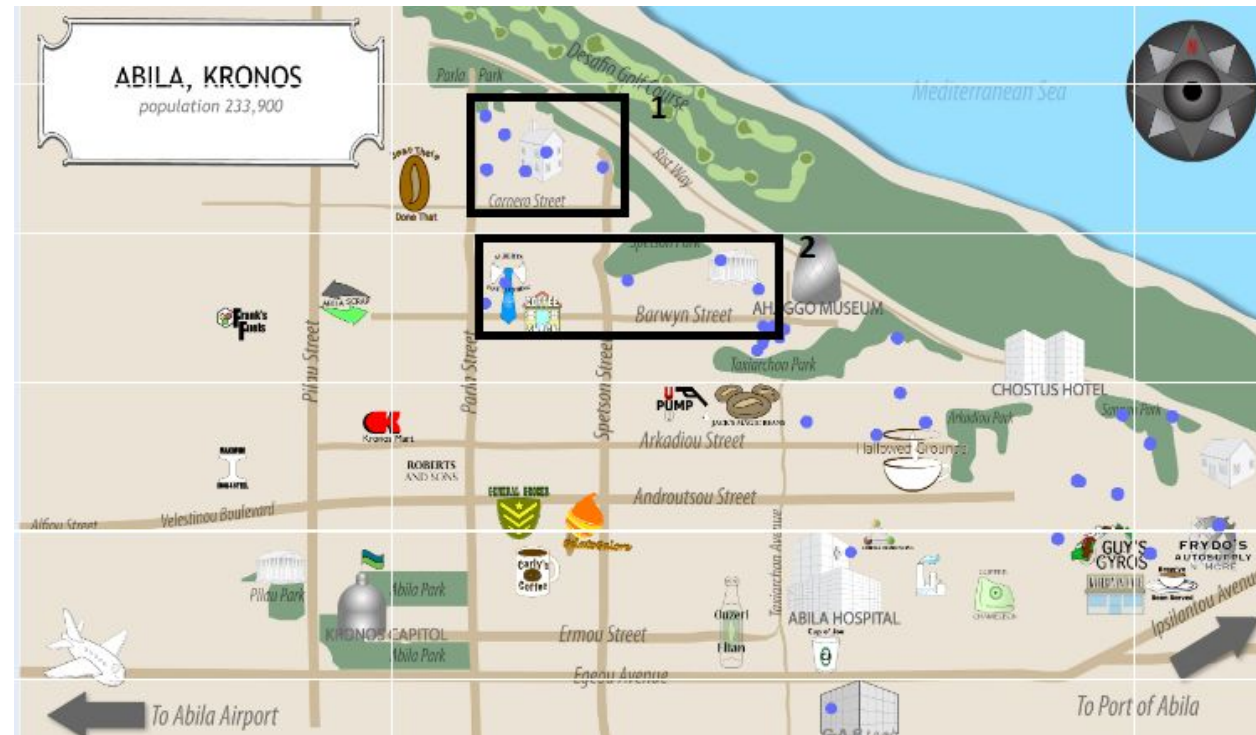
Where do they live?

- In general, employes live in the North East along the park areas
- 2 4 major areas
    - North of Canero St
    - Near Spetson Park and Taxiarchon Park
    - North of Hallowed Grounds
    - Near Guy's Gyros
  - In region 1 a majority of the Engineering team lives
  - In region 2 a majority of the Executives live

Daily Routines

Trucks
- Each truck as a set route
- Starts at the office, ends at the office

Employees
Weekdays
- Leave for work between 6-8
- Many will buy coffee
- Arrive at the office
- Leave to have lunch somewhere usually around 12
- Return to Office around 1
- After 5 Return home
- After hours shopping/food

Weekends
- Store visits
- Lunch Visits
- Recreation

Event 1 – 10k Auto Supply Purchase

- While investigating the credit card transactions outliers, and the individual reports, the *single, biggest transaction* is made by **Lucas Alcazar** at the suspicious **Frydo's Auto Supply. *Ten thousand dollars***, and not a penny more.
- Lucas **was not physically present** at the auto supply shop around the time of the transaction, he was at a different business, corroborated by both his GPS data and a credit card transaction just a few minutes after:

  - *Day: 2014-01-13 19:20:00*
  - *Location: Frydos Auto Supply n' More*
  - *Price: 10000.0*

  - *Day: 2014-01-13 19:30:00*
  - *Location: Ouzeri Elian*
  - *Price: 28.75*

- This prompted investigating Lucas Alcazar's credit card transactions in more detail.
- **Loreto Bodrogi, Isia Vann** and **Inga Ferro** were at the auto shop during the time of the transaction.
- A purchase at U-Pump when he was not at this location. Minke Mies was at the gas station, at this time. This gives me compelling evidence that he was in possession of the card at that time.
- Suspects have passed the card around during meetings.
- His credit card was likely **cloned.** This is important to notice as his transactions may not always be his. And our suspects may be spending and hiding their tracks by using Lucas' card.

Event 2 – Executives Home's Surveillance

- Most home locations were easily referenceable by analyzing the daily routine maps and determining what were the likely locations of each employee homes as previously shown.
- All executives except the CEO live in the north area of Kronos, likely a nicer, expensive neighborhood (supported by museum + fine clothing store).
- CEO doesn't appear to live in Kronos, but came for a visit on the 17th throughout the 20th.
- All four residences were surveilled by a pair of individuals, on different days, likely taking turns, following the same pattern.
- **Isia Vann** arrived at **Ada Campo's** house at *23h Jan 6th* and left at *7h the next morning*. **Loreto Bodrogi** arrived at *3h on 7th*, and left with **Isia** at the same time.
- Both started their days and returned to a suspicious shop called **Frydo's Auto Supply**, making this place significant.
- On similar occasions, **Loreto** and **Minke Mies** surveilled **Orhan Strum's** house on the night of *Jan 8th–9th*.
- **Isia** and **Hennie Osvaldo** surveilled **Willem Vasco's** residence on the night of the *10th–11th*.
- Finally, **Minke** and **Hennie** surveilled **Ingrid Barranco's** home on the *13th–14th*.
- All suspects work for the security department.
- Some of them work with **perimeter control**.

Event 3 – Existence of Safehouses

- Throughout the two weeks of data, after surfacing the suspects from the home surveillances, following their tracking location with more attention, led us to find, what we believe to be, five separate safehouses, visited by different people, **mostly during their lunch breaks.**
- Those locations had no purchases made nor were visited by any other employees, making their locations likely a secret.
- Given that they were visited during (not exclusively) their lunch breaks, this could mean that they were performing a **dry-run** of the kidnapping, making sure they could drive from work, to the safehouses in a proper manner.

- Being that the day of the incident is a **Monday**, this would support the theory that the executives were kidnapped at their offices.
- Most safe houses are located near **Frydo's Auto Supply**, a place that will has been recognized as a suspicious location.
- Safe houses occasionally have multiple, suspect individuals visiting at the same time, likely for meetings.
- There are five executives in town on the night before the kidnappings, so that seems to be a convenient number of safehouses.

- **Minke Mies, Isia Vann, Loreto Bodrogi, Hennie Osvaldo and Inga Ferro**, the same people who scouted the execs are the employees seen at these locations, with **Inga** being the newest addition to the group (we already had suspicions on her for being at the Auto Supply shop during the fraudulent charge).
- Most of the trips in and out taken using secondary streets, likely to avoid being seen by the general public.
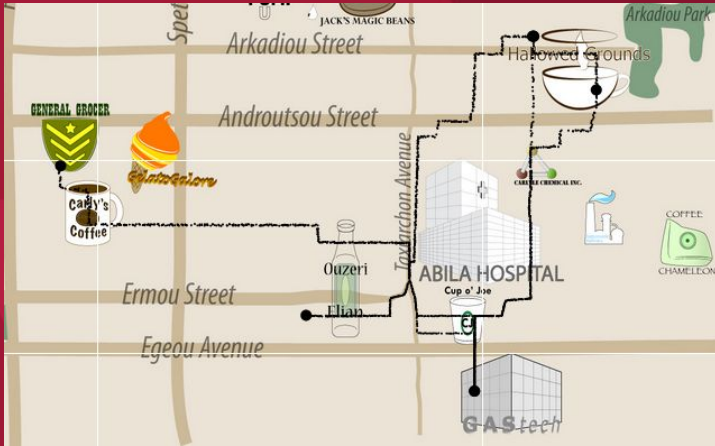

UNIVERSITY *of* DENVER

DANIEL FELIX RITCHIE SCHOOL
OF ENGINEERING & COMPUTER SCIENCE
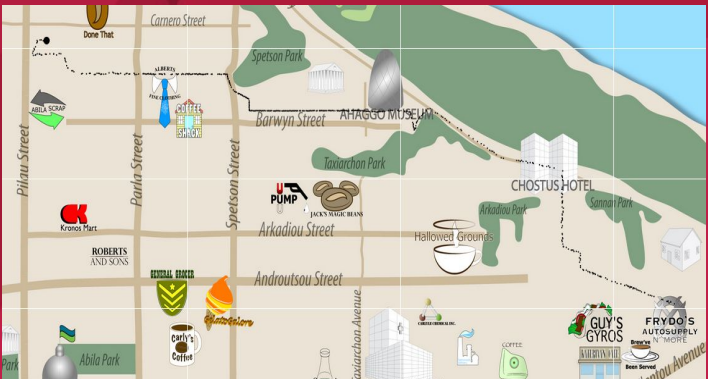
Event 4 – Lucas Alcazar Late Office Visits

- Employee **Lucas Alcazar,** who works at the IT Helpdesk, is seen on multiple occasions heading to GAStech during suspicious hours, outside his regular work schedule.
- His normal work schedule revolves around leaving his residence, NW of Hallowed ground at around 7h15, stopping for a coffee and going to work. Sometimes going out for small shopping during lunch break and heading back home around 17h30.
- However, on multiple occasions, **Lucas** can be seen going to the office at unusual times:

1. 1/6 he goes to the office at 22h15, returns the next morning 1/7 at 1h.
2. 1/8 Lucas again returns to the office at 21h30 and leaves 23h50 of the same day.
3. 1/15 again he heads to the office at around 22h45, and leaves on 1/16 shortly after midnight.
4. 1/7 he heads back to the office at 20h30 and leaves 22h40

- Being part of IT helpdesk, it may be that he went back to the office to put out some "fires". However, no other employees are seen at GT during this time.
- Maybe he was also working in production issues?
- We have no other reasons to suspect Lucas.

UNIVERSITY *of* DENVER
DANIEL FELIX RITCHIE SCHOOL
OF ENGINEERING & COMPUTER SCIENCE

Event 5 – Evening Gathering on 1/10/14

- On the evening of Friday, January 10th, a group of employees from the Engineering and IT teams gathered at the residence of Lars Azada. Attendees of this gathering included Lucas Alcazar, Felix Balas, Isak Baza, Linnea Bergen, Isande Borrasca, Nils Calixto, Axel Cazas, Gustav Cazar, Lidelse Dedos, Birgitta Frente, Vira Frente, Adra Nubarron, Marin Onda, and Brand Tempestad.

- Given the timing of this gathering, which occurred after work hours, it is likely that it was a social event, possibly an after-work party. It is worth noting that the event took place at Lars Azada's house, which may indicate that he was the host or organizer of the gathering.
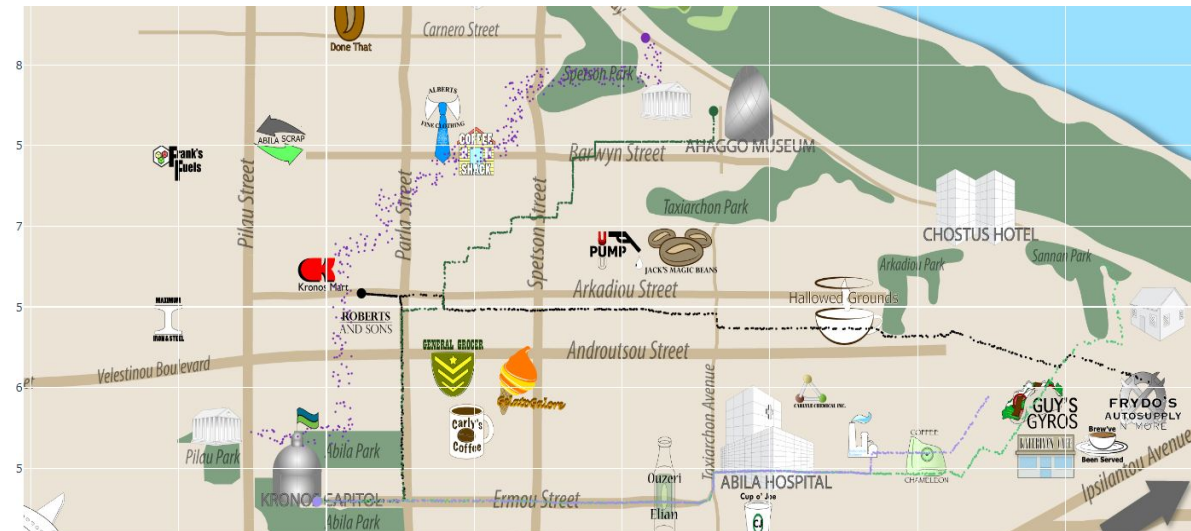
Event 6 – Lunch Gathering on 1/18

- During lunchtime, a group of employees from the Security and Engineering Departments of Kronos Capital were observed meeting at the premises. The attendees of this meeting were Kanon Herrero, Loreto Bodrigi, Edvard Vann, Elsa Orilla, and Adra Nubarron.

- It is noteworthy that Loreto Bodrogi made a stop at the Kronos Mart prior to arriving at the Capital. Additionally, it has been observed that Adra Nubarron did not have any GPS movement from the Capital until the following day. Further investigation may be needed to determine the reason for this occurrence.

Event 7 - GAStech CEO Visit to Kronos

- **Sten Sanjorge Jr.**, the President and CEO of GAStech is not seen in Kronos during the days preceding the kidnapping, that is until the morning of the 17th, when he is seen leaving Chostus Hotel in the morning.
- He either flew in an helicopter from the mainland to the Hotel (we can assume it has a heliport) or he simply flew in to the airport and took a cab to the hotel the night before.
- He has no credit card transactions before his arrival, meaning that the transactions captured in the report are for the island alone and would not cover transactions made outside its territory.
- The whereabouts of Sten on the days before his arrival remain a mystery.
- No suspicious individuals are found stopping at the hotel, either before or after Sten's arrival.

Event 8 – Executive Golfing

- Executives went Golfing on January 12th

- Executives and CEO went golfing again on the 19th

Event 9 – Relationships

-   **Isande Borrasca (SVP/CFO) and Brand Tempestad (Drill Technician) are likely having an affair.**

-   Based on the information provided from GPS tracking, it appears that Isande Borrasca and Brand Tempst have been meeting at the Chostus Hotel during lunch hours on multiple occasions, specifically on January 8th, 10th, 14th, and 17th. This suggests that there may be an ongoing romantic relationship between them. The fact that they are only seen together at the hotel and there positions, suggests they may be hiding this.

Event 10 – Relationships

- **Elsa Orilla and and Kanon Herroro are likely dating.**
- It has been observed through transaction data that **Elsa Orilla** (Drill Technician) and **Kanon Herroro** (Badging Office) have been meeting for lunch every day and sharing cars. Elsa drove on January 9th, 14th, and 17th, while Kanon drove on January 6th, 7th, 8th, 10th, 13th, 15th, and 16th.
- It is noteworthy that Kanon typically paid for these outings using a loyalty card, which may indicate that he has a stronger financial stake in the relationship. Based on these observations, it can be inferred that Elsa and Kanon are in a dating relationship.

timestamp_full	location	price	date	fullname
1/6/2014 13:27	Abila Zacharo	50.14	1/6/2014	Kanon Herrero
NaT	Abila Zacharo	50.14	1/6/2014	Elsa Orilla
1/7/2014 13:24	Kalami Kafenion	45.05	1/7/2014	Kanon Herrero
NaT	Kalami Kafenion	45.05	1/7/2014	Elsa Orilla
1/8/2014 13:38	Gelatogalore	50.36	1/8/2014	Kanon Herrero
NaT	Gelatogalore	50.36	1/8/2014	Elsa Orilla

UNIVERSITY of DENVER

DANIEL FELIX RITCHIE SCHOOL OF ENGINEERING & COMPUTER SCIENCE

Event 11 – Truck Purchase Patterns

- Based on the available GPS data, it appears that the trucks followed normal routes, often traveling to and from the GAStech headquarters along these established paths.
- However, it is worth noting that while credit card and loyalty purchasing data was present at most stops, not all stops were associated with this information.
- In some cases, multiple stops made by the same truck did not have any associated purchase data.
  Further investigation may be necessary to determine the reasons for these discrepancies and whether they are of significance.

Event 12 - Irene Nant Inconsistent on 1/10/14

- Irene Nant was assigned to drive truck 107, which followed a normal route that included a stop at Carlyle Chemical. However, on January 10th, 2019, the truck assigned to her was being driven by someone else.
- Despite this, Irene was observed making a purchase at Carlyle Chemical on that day. It is noteworthy that truck 107 was located near Carlyle Chemical at the same time, driven by Claudio Hawelon.
- This raises the possibility that Irene may have ridden with Claudio or been involved with the truck in some way
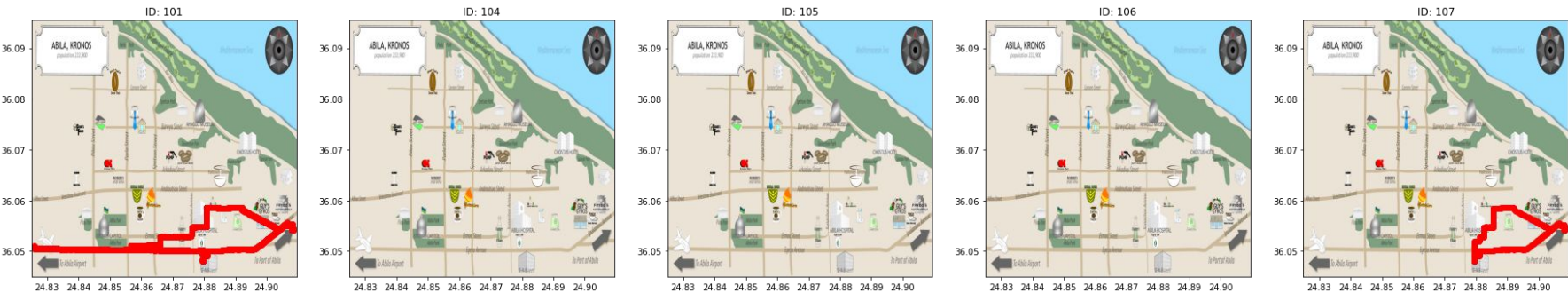

```
                       location              fullname        date  \
553           Nationwide Refinery    Cecilia Morluniau  2014-01-10
555   Stewart and Sons Fabrication   Cecilia Morluniau  2014-01-10
541                 Abila Airport      Claudio Hawelon  2014-01-10
551          Carlyle Chemical Inc.     Claudio Hawelon  2014-01-10
554           Nationwide Refinery      Claudio Hawelon  2014-01-10
568   Stewart and Sons Fabrication     Claudio Hawelon  2014-01-10
1658          Nationwide Refinery      Claudio Hawelon  2014-01-10
1659         Carlyle Chemical Inc.          Irene Nant  2014-01-10
```

Conclusions

We have evidence to suspect five employees

Minke Mies
Loreto Bodrogi
Isia Vann
Hennie Osvaldo
Inga Ferro

- Visited and test-drove from work to safe houses during work periods.
- Surveyed, the houses of all four GT executives who live on the island.
- Used a cloned card to raise funds (10k) to be used during the course of the previous weeks
- Drove around side streets when visiting suspicious places.
- Consistently met at the Auto Supply shop.
- All work with security, assuming to have advanced surveillance training.
- Aside from investigating the employees, it is our recommendation to survey the possible safehouses.
- Past histories and screening would be done to find out how these employees were able to get hired and coordinate.

Questions?