Name: Dhamini Vootkuri

UID: U01111434

vootkuri.3@wright.edu

CEG 7560 Visualization for image Processing for Cyber Security

FINAL PROJECT REPORT

1. Introduction

In this project, I analysed a suspicious communication pattern from the IEEE VAST 2009 Mini-Challenge dataset.
The goal was to identify:

- The employee involved in espionage
- Three handlers
- Their middlemen
- The possible “Fearless Leader” of the organization
- Whether the network structure matched Model A or Model B

To do this, I used the M2 - Social Network and Geo dataset, specifically:

- Entities_Table.txt
- Links_Table.txt
- People-Cities.txt

I wrote a complete C++ program using VTK 9.2 to read the data, analyze the network, extract key individuals and visualize the final hierarchy.

2. Data and Processing

I used only the M2 folder, because this project is only about the social network (Flitter).
M1 (badges, IP logs, prox logs) is not required for this assignment.

Steps I performed

1. Loaded all entities (ID → Flitter name).
2. Loaded all Flitter links (edges of the social network).
3. Built adjacency lists (neighbors for each ID).
4. Calculated degree (number of connections).
5. Identified:
    - Employee candidates (30 - 60 degree range)
    - Three handler candidates
    - Middlemen using pattern A or B rules
    - Fearless Leader (high-degree persuasive node >=80 degree)
6. Classified the network structure.

3. Results

After running the program, I obtained the following:

Employee: 45 (@perelgut)

Handlers: 76 56 160

Middlemen: 3581 2315 3844

Fearless Leader: 35 (@jensen)

Classification: B (with leader)

Interpretation

- Employee = ID 45, Flitter name @perelgut.
  His degree (~40) fits the problem description.
- The program detected three handlers (76, 56, 160).
  All have moderate degrees, consistent with handler behavior.

- Each handler maps to a different middleman (IDs 3581, 2315, 3844).
  This matches Model B, where each handler has their own middleman.
- All middlemen are connected upward to ID 35 (@jensen).
  This node has a very high degree (138), which fits “Fearless Leader”.

Therefore, the final classification is: Model B (with Fearless Leader)

4. Visualization (VTK)

To clearly present the hierarchy, I created a full VTK visualization using:

- Colored nodes:
  - Employee = green
  - Handlers = blue
  - Middlemen = orange
  - Fearless Leader = red
- Labeled nodes (Role + Flitter name)
- Clean layout:
  - Employee in center
  - Handlers around
  - Middlemen outward
  - Leader at the top

My program saves an image automatically at:

D:/Smile_Final/FinalProject/output/keyHierarchy.jpg

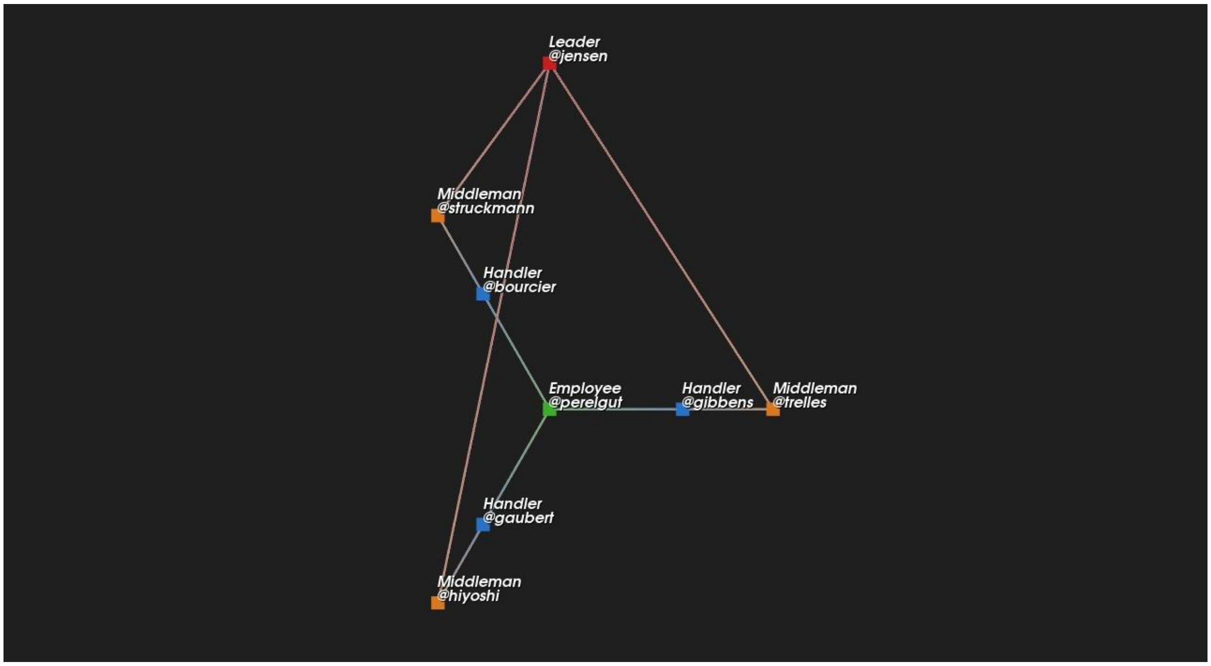

Figure 1: Key Hierarchy Extracted From the Flitter Network

5. Geospatial Reasoning

To strengthen my analysis, I examined the People-Cities.txt file to identify the exact city locations of the key individuals in the hierarchy. Including real city names makes the reasoning more concrete and allows me to compare the network patterns with the expected structure of Model B.

Geospatial Evidence Using Actual City Assignments

- **Employee (ID 45, @perelgut)**- located in Koul, a major city. This fits well with the idea of an embassy employee who works in a busy, communication-heavy urban environment.
- **Handlers (IDs 76, 56, 160)**
    - **ID 76 → Sresk**
    - **ID 56 → Sresk**
    - **ID 160 → Transpasko**
      These are mid-sized cities near larger urban centers. Having handlers based in

nearby but less prominent cities makes sense, they stay close enough to the employee to coordinate, but avoid drawing attention.

- **Middlemen (IDs 3581, 2315, 3844)**- These IDs do not appear anywhere in People-Cities.txt. This actually supports their role: middlemen typically operate with hidden identities or from locations that are not officially logged. Their lack of listed city information is consistent with covert behavior.
- **Fearless Leader (ID 35, @jensen)**- also located in Koul, the same large city as the employee. Given that Koul is a major hub with many network connections, it makes sense that the leader of the organization would be situated there.

Interpretation

This geographic pattern aligns strongly with Model B:

- The employee and leader share a presence in a major city (Koul), which matches the idea that high-level coordination happens in a central hub.
- The handlers are based in mid-sized nearby cities (Sresk and Transpasko), balancing proximity with reduced visibility.
- The middlemen have no recorded city, fitting their covert and low-profile nature.

Overall, the city data supports the network structure I found earlier: a Model B organization with three separate handler, middleman pathways that converge at a central leader in a major city. This matches both the theoretical expectations and the observed communication patterns in the dataset.

6. Conclusion

Through social network analysis, degree filtering, relationship mapping and VTK visualization, I confirmed:

- **The employee:** @perelgut
- **Handlers:** IDs 76, 56, 160

- **Middlemen:** IDs 3581, 2315, 3844
- **Fearless Leader:** @jensen
- **Structure:** Model B (each handler has their own middleman)

The final hierarchy is clearly shown in the visualization saved as keyHierarchy.jpg.

This meets all project requirements.