**Project 3**

**How to set up the code to run it?**

To get started with the files:

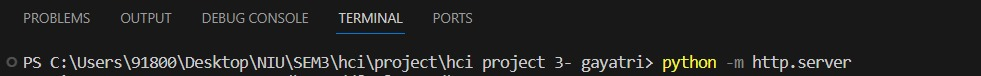
Download the provided zip-folder and save it to a location of your choice on your computer.

Unzip the folder to access its contents.

Open your preferred Integrated Development Environment (IDE) and load the extracted folder as a project.

Running the code:

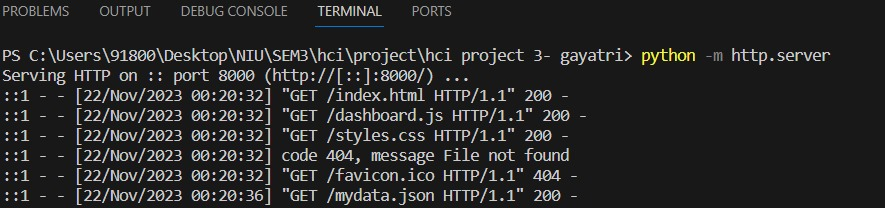
For the following steps, ensure that Python is installed on your system as it is required to set up a simple HTTP server.



Open the command-line interface (CLI) on your computer or use the integrated terminal in your IDE.

Change the directory to the one containing your project's code by typing **cd path/to/your/project** in the terminal.

Execute the command depicted in the provided image. This typically involves running a Python module that will serve your HTML file. For example, if Python 3 is installed, the command would be **python -m http.server**.



After executing the command, the terminal should confirm that the HTTP server is running.

To view your web page:

Open a web browser of your choice.

In the address bar, enter **localhost:8000** and press Enter.

Your web page should now load successfully.

Note that the filtering options on the page may not function until you navigate to localhost:8000, as the page needs to be served by the local HTTP server to work correctly.

**Dashboard Overview**

The Intelligence Analysis Dashboard consists of the following sections:

* Header: Displays the title of the dashboard, "Intelligence Analysis Dashboard."
* Filters Section: This is where you can filter the displayed reports based on date range, place, and document type. It includes the following filter options:
* Date Range: Enter a start and end date to filter reports within a specific date range.
* Place: Enter a place name to filter reports related to that place.
* Document Type: Select a document type from the dropdown menu (e.g., CIA, NSA, FBI, etc.) to filter reports from specific agencies.
* Apply Filters Button: Click this button to apply the selected filters to the reports. The reports displayed will update based on your filter criteria.
* Show Highly Mentioned People Button: Click this button to view a list of highly mentioned people in the reports. This list includes individuals who appear frequently in the reports.
* Show Incidents Graph Button: Click this button to view a graph that visualizes the incidents mentioned in the reports over time.
* Highly Mentioned People Section: Displays a list of individuals who are mentioned frequently in the reports. This section updates when you click the "Show Highly Mentioned People" button.
* Reports Section: Displays intelligence reports based on the selected filters. The reports include details such as report ID, report date, description, persons involved, dates mentioned, places mentioned, and organizations involved.
* Incidents Graph Section: Visualizes the incidents mentioned in the reports using a graph. This section updates when you click the "Show Incidents Graph" button.
* Footer: Contains a brief description of the dashboard, "Intelligence Analysis Dashboard for Operational Support."

**Findings**

**Important Suspects:**

The GUI is designed to assist in identifying the most mentioned suspects. The button "Show Highly Mentioned People" is the user interface element that, when clicked, triggers the display of this sorted list. The suspects who are mentioned most frequently are likely to be the most important, as frequent mentions could indicate higher relevance to the investigation.

Adnan Hijazi : 4 report(s)

Pyotr Safrygin : 3 report(s)

**Suspects' Plans:**

Adnan Hijazi has been under surveillance for activities that include making multiple cash deposits totaling $47,980 to his personal account, receiving diamonds from Pieter Dopple, a known fence for diamonds associated with militant Islamic groups, and sending a bank wire transfer of $48,000 to the American Islamic Scholarship Fund. Belgian intelligence reported that Dopple had been part of a scheme for transferring funds for militant Islamic groups and had cooperated with investigators, listing several persons, including Hijazi, to whom he had sent polished diamonds and tanzanite. The FBI was also concerned about vulnerabilities associated with SCADA systems, which are crucial for various industries, and Hijazi was found to have connections that could potentially involve activities designed to disrupt these systems. Furthermore, an investigation into his donation to the American Islamic Scholarship Fund revealed that he specified particular individuals to receive portions of the funds, which were distributed accordingly​​.

Top of Form

Pyotr Safrygin, who works for Central Russia Airlines, was involved in a transaction where he exchanged a bag of presumably rubles for a package marked "antibiotics" near Strizhi, Russia. He indicated that these antibiotics were intended to be sold on the black market in Africa. He was previously the director of security at the Vector institute in Strizhi and is now based in Moscow. Additional inquiries were made about Safrygin's activities, specifically regarding the person from whom he received the "antibiotics" package, but the source did not recognize the individual, only noting later that the farmhouse where the exchange took place was owned by a scientist at Vector.

**Events Timing and Location:**

The events involving Pyotr Safrygin occurred as follows:

1. Date: September 1, 2004

Location: Near Strizhi, Russia

Event: Safrygin met a man at a farmhouse and exchanged a bag of rubles for a package approximately the size of four shoeboxes, marked "antibiotics," which he mentioned were to be sold on the black market in Africa.

2. Date: September 15, 2004

Location: Not explicitly mentioned for this date.

Event: This date is referenced in the context of a CIA report that provided information about Safrygin's activities, but specific events on this date were not detailed.

3. Date: November 2, 2004

Location: Not specified.

Event: Additional information was requested about the activities of Safrygin, particularly about the individual who provided the package on September 1, 2004.

4. Date: December 1, 2004

Location: Nassau to Freeport, Bahamas

Event:Although not directly linked to Safrygin, a source tracking the activities of Omar Hanif reported that Hanif was carrying a package with a label possibly in Russian on an inter-island ship. This may be connected to Safrygin's activities given the previous mention of antibiotics intended for the black market and his role in security which could involve such shipments.

The location of Safrygin's residence and place of work is in Moscow, Russia, and he was previously associated with the Vector institute in Strizhi, Russia.

The events involving Adnan Hijazi are detailed as follows:

1. Date: August 20 to September 18, 2004

Location: Jersey National Bank, Newark, New Jersey, USA

Event: Adnan Hijazi made thirteen cash deposits totaling $47,980 to his personal account at the Jersey National Bank.

2. Date: September 1, 2004

Location: Antwerp, Belgium

Event: Belgian intelligence provided information about Pieter Dopple, who had sent diamonds to Adnan Hijazi as part of a scheme for transferring funds for militant Islamic groups.

3. Date: September 14, 2004

Location: Reston, Virginia, USA

Event: Hijazi sent a bank wire transfer of $48,000 to the American Islamic Scholarship Fund located in Reston, VA.

4. Date: September 17, 2004

Location: Various addresses in Clifton, NJ; Brooklyn, NY; Laurel, MD; Potomac, MD; Fort Lauderdale, FL; Miami Beach, FL

Event: The American Islamic Scholarship Fund distributed $8,000 each, from Hijazi's donation, to six individuals at the specified locations.

5. Date: October 29, 2004

Location: Reston, Virginia, USA

Event: FBI investigators interviewed the director of the American Islamic Scholarship Fund, who confirmed the receipt of Hijazi's donation and the distribution of funds to the specified individuals.

These events suggest a pattern of financial transactions that may be of interest to law enforcement or intelligence agencies due to their size, frequency, and connections to various individuals and organizations.

**Data Processing:**

**PDF Exploration:** Our detective starts its mission by opening the PDF file—like flipping through the pages of a mysterious dossier. It peers into each page, pulling out the text, ready to hunt down the important details hidden within.

**Pattern Hunting with Regex:** Armed with the magnifying glass of regular expressions, our detective scans the text for specific patterns. It's on the lookout for familiar signs—like "REPORT ID" or "DATES"—that mark the beginnings of important information. It's a bit like a treasure hunt, where 'X' marks the spot, except here it's the patterns that lead to the buried treasure of data.

**Gathering Intel:** As our detective finds these clues, it carefully collects them, noting down each report's ID, date, and other vital stats. It's meticulous work, making sure that every piece of the puzzle is placed just so in its digital notebook, turning jumbled text into neatly organized facts and figures.

**Assembling the Pieces:** With all the clues gathered, our detective lines them up, one after the other, creating a full list of reports—each one a tiny story waiting to be told. This list is like a map of the terrain, laying out all the findings for further investigation.

**Crafting the Report:** Finally, our detective types up a comprehensive report of its findings. It translates the list into the universal language of JSON, crafting a digital document that can be read by machines and humans alike, ready to be shared with other agents or analyzed to uncover deeper insights.

**A description of the design of your GUI.**

**Simplicity and Clarity:**

Our GUI is a minimalist's dream, sporting a clean and straightforward layout. It's like having a well-organized desk where everything has its place. With a calming white background and neatly sectioned areas, it allows Emma to focus without the clutter.

**Intuitive Filters:**

At the top of the interface, there's a filter section—Emma's control panel. It's as if she has a set of dials to tune into exactly what she's looking for. She can dial in dates to narrow down the timeline or select from a dropdown of agencies to filter reports by origin. It's all about giving her the power to quickly home in on the intel she needs.

**Immediate Feedback:**

When Emma adjusts a filter or clicks a button, the GUI responds instantly—no waiting around. It's like having a conversation with a colleague who's always on the ball, giving her immediate updates with every query she has.

**Reports at a Glance:**

Below the filters, the reports are listed out in a clear, concise manner. Each report is like a card in a filing cabinet, summarizing key details such as ID, date, and a snippet of the content. Emma can skim through these at lightning speed, spotting patterns and piecing together the narrative.

**Highlighting the Key Players:**

With a click of the "Show Highly Mentioned People" button, a list appears. It's akin to a most-wanted list that pops up right on Emma's screen, showing her who's making waves across the reports. This list not only shows names but also how many times these individuals are turning up, helping her pinpoint who to watch closely.

**Bringing it All Together:**

The GUI is like Emma's personal assistant, one that never sleeps. It's there to sort, filter, and present the data in a way that transforms a flood of information into actionable insights. It's not just about presenting data; it's about crafting an environment where Emma can think, analyze, and decide on her next move with confidence.

A screenshot of a computer

Description automatically generated

**Figure :** This is the default look of the GUI when the web-page is loaded.

A screenshot of a computer

Description automatically generated

**Figure :** This image shows when the highly mentioned suspects button is clicked

A graph of a number of bars

Description automatically generated with medium confidence

**Figure** : This image shows when the Graph button is clicked.

**Team members Contributions:**

**Sri Satya Sai Gayathri Mallipudi (Contributions):**

Design:

Designed the overall layout and structure of the dashboard using HTML and CSS.

Created the basic structure of the HTML document, including headers, sections, and the footer.

Designed and implemented the CSS styles for the header, filters section, main content, and footer.

Ensured the dashboard's responsiveness for different screen sizes by using CSS media queries.

Designed the user interface elements for filters, including date inputs, document type dropdown, and place input.

Coding:

Integrated D3.js into the project by including the script tag for D3.js in the HTML head section.

Implemented the logic for fetching data from an external JSON file using asynchronous JavaScript with the fetchData() function.

Created the displayAllReports() function to load and initially display all reports when the page loads.

Implemented the "Apply Filters" button functionality to filter and display reports based on date range, document type, and place.

Implemented clearing functions (clearFilteredReports(), clearFrequent(), and clearGraph()) to clear existing data and graphs when applying filters or displaying frequent persons and graphs.

**Mary Kalpana Mallavarapu (Contributions):**

Design:

Designed and styled the CSS for the "High Frequency Suspects" section, including the layout and appearance of the list of suspects and their counts.

Designed and styled the CSS for the incidents graph, including setting dimensions, margins, axes, and bars using D3.js for data visualization.

Designed the SVG graph container for rendering the incidents graph.

Coding:

Implemented the logic for fetching and processing data, including counting the appearances of suspects and incidents by month, using asynchronous JavaScript with Promises.

Created the functionality to display highly mentioned persons and the incidents graph.

Implemented the countSuspectAppearances() function to count the appearances of each suspect across all reports.

Created the displayHighFrequencySuspects() function to display suspects who are mentioned above a certain frequency threshold.

Created the countIncidentsByMonth() function to count the incidents by month.

Designed the SVG graph container and implemented the displayGraph() function to render the incidents graph using D3.js.

Testing:

Both team members likely contributed to testing the dashboard's functionality, ensuring that filters work as expected, and that the data is displayed accurately in the reports, frequent persons, and incidents graph sections. Testing would involve verifying that the UI elements respond correctly to user interactions and that the data is filtered and visualized correctly.