



OpenMF
Android Forensics Tool

OpenMF

Google Summer of Code 2021

Organisation: SCoRelab

Personal Details

- **Basic Details**

- **Name:** - Sachin Som
- **Nationality:** - Indian
- **Gender:** - Male
- **Time Zone:** - India(UTC +5.30)

- **Educational Details**

- **University:** - Arya college of Engineering & I.T.
- **Degree:** - Bachelor of Technology
- **Major:** - Electronics and Communication
- **SGPA:** - 9.4 (current)
- **Graduation year:** - 2022

- **Contact Details**

- **Email Address:** - sachinsom507@gmail.com
- **Phone Number:** - +91 8824634027
- **Gitter handle:** - sachinsom93

- **Social Media**

- **GitHub:** - [sachinsom93](https://github.com/sachinsom93)
- **LinkedIn:** - [sachinsom507](https://www.linkedin.com/in/sachinsom507)
- **Medium:** - [sachinsom507](https://medium.com/@sachinsom507)

About Me

1. Are you a SCoRe contributor/ Have you contributed to SCoRe before?

Yes, I am a Contributor to SCoRe lab projects. I have been contributing to SCoRe since January 2021. I have majorly contributed to OpenMF and Webiu Project. following are my contributions: -

Pull Requests:

[Merged] Added some APIs to listOfAPIs.md and Readme.md #83

(<https://www.github.com/scorelab/OpenMF/pull/83>)

[Merged] Refactored profile and getUser route #81

(<https://www.github.com/scorelab/OpenMF/pull/81>)

[Merged] Implemented frontend validation and toggle password checkbox #77

(<https://www.github.com/scorelab/OpenMF/pull/77>)

[Merged] [Backend] Created route for admin to add, update role, delete and view users route #76

(<https://www.github.com/scorelab/OpenMF/pull/76>)

[Merged] Created Unauthorized Handler #74

(<https://www.github.com/scorelab/OpenMF/pull/74>)

[Merged] fix: delete route #68

(<https://www.github.com/scorelab/OpenMF/pull/68>)

[Merged] Updated Readme for flask server #66

(<https://github.com/scorelab/OpenMF/pull/66>)

[Open] [Frontend] validated email before sending request to server #143

(<https://www.github.com/scorelab/OpenMF/pull/143>)

[Open] [Frontend] Implemented googleAuth and FaceBookAuth in frontend #135

(<https://www.github.com/scorelab/OpenMF/pull/135>)

[Open] [Frontend] Implemented managementRoute and extractorRoute #124

(<https://www.github.com/scorelab/OpenMF/pull/124>)

[Open] [Backend] Created 404 response handler #123

(<https://www.github.com/scorelab/OpenMF/pull/123>)

[Open] [Backend] Created update routes for name and password #107

(<https://www.github.com/scorelab/OpenMF/pull/107>)

[Open] Implemented a route for updating email address #99

(<https://www.github.com/scorelab/OpenMF/pull/99>)

[Open] [React] Created a frontend to create register admins #86

(<https://www.github.com/scorelab/OpenMF/pull/86>)

[Open] Added Gatsby-plugin-font awesome-CSS in package.json #50

(<https://www.github.com/scorelab/Webiu/pull/50>)

[Open] Added Null Check to Components #43

(<https://www.github.com/scorelab/Webiu/pull/43>)

[Open] Issue24 add logo #33

(<https://www.github.com/scorelab/Webiu/pull/33>)

[Open] Added A Loader component #31

(<https://www.github.com/scorelab/Webiu/pull/31>)

Issues:

[Closed] [Backend] Profile route should be flexible for admin and user both roles #80

(<https://github.com/scorelab/OpenMF/issues/80>)

[Closed] [Frontend] Add toggle password button in login screen #75

(<https://github.com/scorelab/OpenMF/issues/75>)

[Closed] [Backend] Unauthorized Handler is not defined for login required routes #73

(<https://github.com/scorelab/OpenMF/issues/73>)

[Closed] Delete route needs to change #67

(<https://github.com/scorelab/OpenMF/issues/67>)

[Closed] [Backend] Create route for admin to add users of different roles #61

(<https://github.com/scorelab/OpenMF/issues/61>)

[Closed] [frontend]: Creating a frontend for profile page #60

(<https://github.com/scorelab/OpenMF/issues/60>)

[Open] Create Dockerfiles for openMF modules #148

(<https://github.com/scorelab/OpenMF/issues/148>)

[Open] [Frontend] Need to validate email before sending request to server #142

(<https://github.com/scorelab/OpenMF/issues/142>)

[Open] [Frontend] Add password validation in frontend #139

(<https://github.com/scorelab/OpenMF/issues/139>)

[Open] Enable Sign In options with google and other options. #132

(<https://github.com/scorelab/OpenMF/issues/132>)

[Open] [Frontend] Enable lazy loading in React #130

(<https://github.com/scorelab/OpenMF/issues/130>)

[Open] [Frontend] create management and extractor specific route #122

(<https://github.com/scorelab/OpenMF/issues/122>)

[Open] [Backend] Create a 404 response from server #113

(<https://github.com/scorelab/OpenMF/issues/113>)

[Open] [Backend] Create a controller folder to put all route logics #108

(<https://github.com/scorelab/OpenMF/issues/108>)

[Open] [Backend] Implement route for updating password and name #100

(<https://github.com/scorelab/OpenMF/issues/100>)

[Open] [Backend] Update email route is missing #98

(<https://github.com/scorelab/OpenMF/issues/98>)

[Open] [Frontend] Register screen for admin #78

(<https://github.com/scorelab/OpenMF/issues/78>)

2. How can we reach you (e.g.: email) if we have questions about your application?

Email Address: - sachinsom507@gmail.com

Phone Number: - +91 8824634027

Gitter Handle: - sachinsom93

3. What is your GitHub username(s):

Username: - [sachinsom93](#)

Project Specific Questions

4. Which SCoRe GSoC project are you applying for (please submit separate applications for each project):

- I am applying for **OpenMF - Analytics API**.

5. What do you plan to accomplish over this summer for this project? (Please tell us

- What project you want to work on,
 - How you will approach that project portion (with your milestones))
- a. Project Introduction: -**
I want to work on the OpenMF project, OpenMF is an open-source forensic tool for Android smartphones that helps digital forensic investigators throughout the life cycle of digital forensic investigation. For e.g., let us say we have a crime scene in which we have captured some suspects and we have their mobile phones. If we want to extract all the data from their phones and see which of them are actually involved in the crime scene then we require

a software to perform this task and produce Meaningful evidence and Analysis report for every phone (Digital forensic case). The OpenMF project is a dedicated software to:

- a. Extract the relevant data
- b. Manage all the cases separately
- c. Produce Analysis report

This open-source project is an important tool for Digital forensic organization. At present OpenMF is only a command line tool but we are planning to make a complete web client with additional features like Admin, Management and Extractor. These roles will have different privileges to the tool and as a whole it will become a complete open-source forensic tool for Android smartphones which then can be used by any Digital forensic investigation organization.

b. Milestones: -

1. **OpenMF's admin section:** - Creating an admin dashboard for maintaining management section, extractor section and cases section.
2. **OpenMF's management section:** - Creating a management section for a management member to do analysis on extracted cases and to view all the other management members under one admin.
3. **OpenMF's extractor section:** - Creating an extractor section that would contain a list of active devices so that extractor can extract data from these devices and push them to the database.
4. **Cases Data Visualization:** - Analytics over the various data that are extracted by extractor should be available to the management member in the form of histograms, line graphs or pie charts. Like analysis over WhatsApp or Facebook data using data visualization tools.
5. **Implementing analysis on the Cases:** - Developing and creating various types of operation among cases. Like searching a word among all the cases, fetching all the cases that are extracted from a particular extractor user, ordering all the cases according to their extracted date or comparing two cases based on maximum repeated word.
6. Improving routing of the React App using react-router.
7. Updating project wiki and providing a video for complete setup and working of project.
8. Implementing various APIs related to cases, users etc.
9. Dockerizing OpenMF project for quick environment setup and reproductivity.

Extra Milestones:

- API documentation using Sphinx.
- Enabling Sockets to increase real time integration between admin, management and extractor section.
- Adding more ways to user authentication like authentication using GitHub, Facebook and Google.
- Converting this to a progressive web app with the help of service workers.
- Writing unit tests for React Components.
- Improving web performance.

6. If you have your own project to propose, please describe it here:

- NA

7. Projects related details. (Have you tried that project you selected from SCoRe project list? What problems, if any, were presented? What prevented you from getting the entire system up and running?)

- I didn't face any issue regarding setting up this project

8. List down any plans you have during this summer(over the time period of GSoC, such as classes, job, vacation plans, thesis, etc.)

- I don't have any specific plans for this summer, so I can properly work on this project. As I am enrolled in a B.Tech degree, I would have my end term exams from around the end of June. So, I would be a bit inactive during that time span.

9. Education:

- What year are you in school?
 - Currently, I am a 3rd year B.Tech undergraduate.
- What programming courses have you taken?
 - Training of Full Stack (MERN) course at grass solutions Jaipur.
 - Data structure and algorithms using Python (NPTEL course)
 - Complete TypeScript (Udemy course)
 - Data structure and algorithms self-Paced course(GeeksForGeeks)
 - Data Science using python (INeuron)
 - Statistics for machine learning(INeuron)
 - Microprocessors (NPTEL course)
- What is your major?
 - Electronics and communication(Batch 2022)
- Have you done group projects (programming or otherwise)?
 - [AVEO](#) : -
 - AVEO is an Angular web application which consumes the YouTube v3 Data API to create a minimal user-interface where YouTube videos can be viewed.
 - Tech Stack: - Angular at frontend, Node js for backend, MONGODB and YouTube V3 data API
 - I worked on the authentication part and at its frontend part.
 - Created some backend public and private APIs.
 - [WebMeet](#) : -
 - WebMeet is a web application, on which a user can create an account and then he can create separate rooms for video conferencing. WebMeet works on WebRTC that enables the user to communicate without any audio buffering.

- ii. Tech Stack: - Vanilla Js, Node js, socket.io for data communication between frontend and backend and webRTC for enabling real time video conferencing.
- iii. This project stood first at the [Game of codes](#) organized by Code Community of IIIT Una.
- **[SocialBud](#):** -
 - iv. A social media web app where users can create posts, delete posts, like or dislike posts, follow or unfollow to each other and many more.
 - v. Tech Stack: - React at frontend, Material UI for styling purpose, Node js for creating public and private APIs, context API for state management and MongoDB using mongoose.
- What was your primary contribution to/role in the group?
 - My primary role in the project was to work on the architecture of backend API endpoints, creating complex APIs according to the need of the project. I have also worked for the frontend portion of the projects. I am proficient with Node js, Flask, Django, frontend frameworks like Angular and React.

10. Do you have work experience in programming? Tell us about it.

- None

11. Do you have previous open source experience? Briefly describe what you have done ?

Yes, I am an Open Source Enthusiasts who worked with a couple of open source organisations and open source projects.

Following are my some of my open source contributions as an open source enthusiasts: -

1. Completed HacktoberFest 2020.
2. I have been selected as the top contributor in Game of Source (Game of Source was an open source contribution contest organised by GeeksForGeeks student partners).
3. Beside these I have contributed to many open Source projects.

12. Tell me one interesting fact about yourself.

- I love to learn new things.

Project Implementation: -

- **OpenMF's admin section**
 - Design and Implement Dashboard for admin section.
 - Creating different sections inside the admin section like management section, extractor section and cases section.
 - Integrating Flask backend to by REST API to enable admin for adding new management and extractor members.

- Fetching all the management, extractor members and cases that are related to an admin.
- Design and Implemented frontend design to view, update and deleting management, extractor members by an admin.
- Refer figure for these purposes.

Proposed Designs for Admin Section:

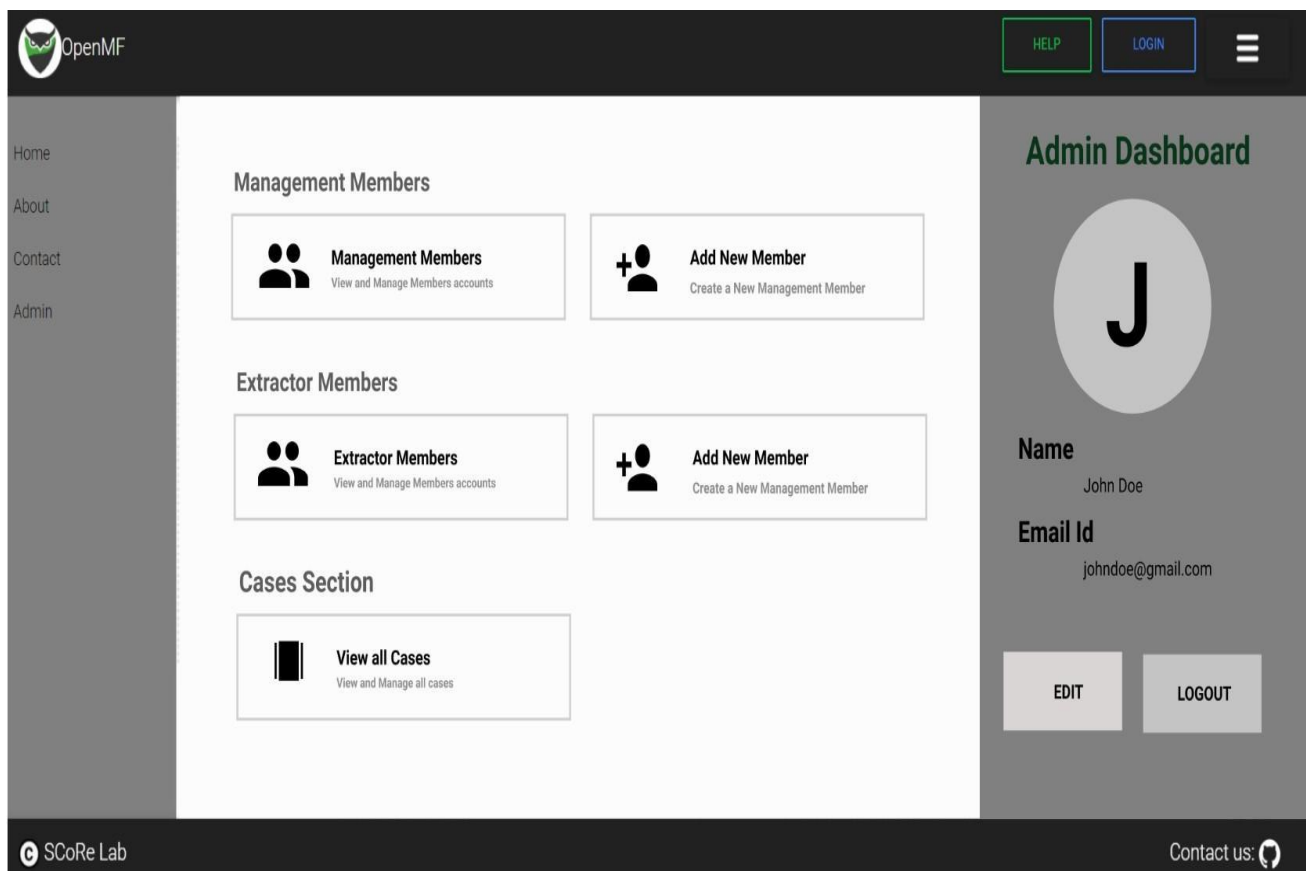
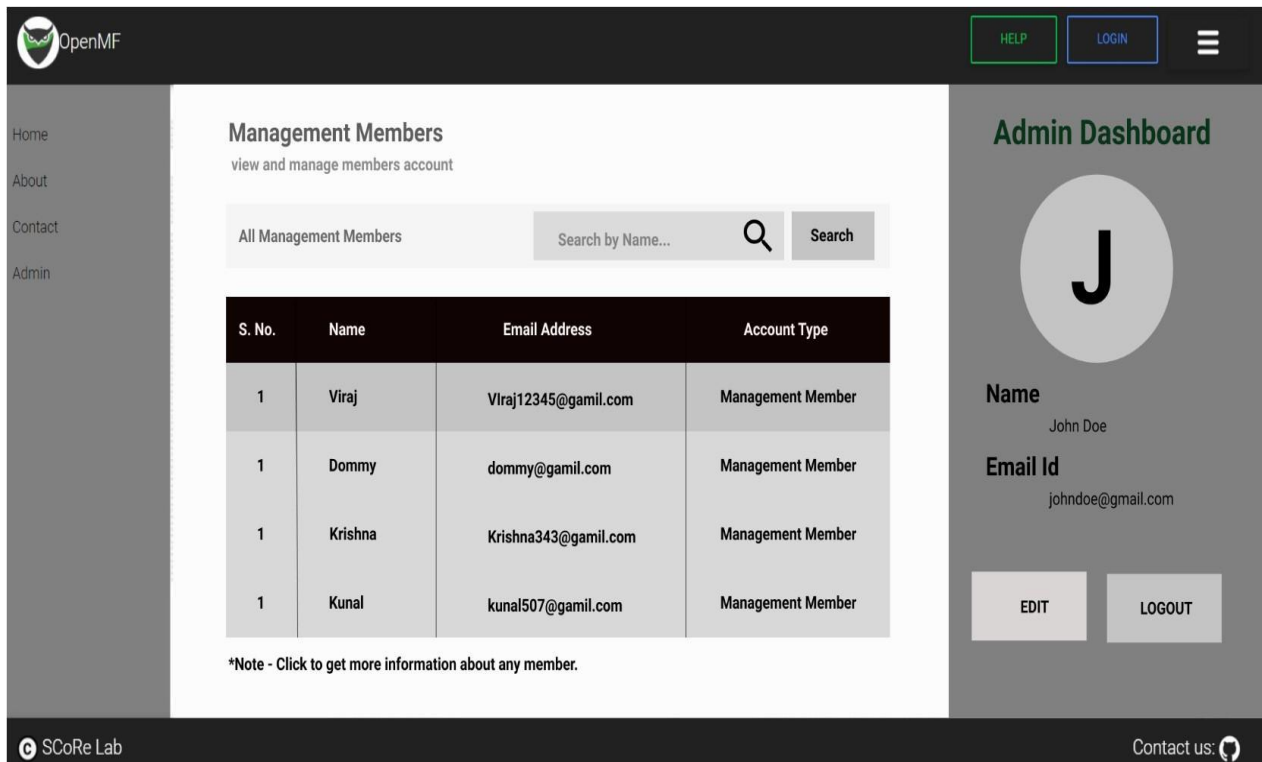


Figure 1: Admin Dashboard

(**Description for Figure 1:** - This page would help the admin to view all of the management, extractor members and cases also to add new members to the forensic organisation.)

Privileges given to admin of a forensic department:

- Can Update, delete and view management members.
- Can Update, delete and view extractor members.
- Can view all the extracted cases.



OpenMF HELP LOGIN

Home About Contact Admin

Management Members

view and manage members account

All Management Members Search by Name... Search

S. No.	Name	Email Address	Account Type
1	Viraj	Viraj12345@gamil.com	Management Member
1	Dommy	dommy@gamil.com	Management Member
1	Krishna	Krishna343@gamil.com	Management Member
1	Kunal	kunal507@gamil.com	Management Member

*Note - Click to get more information about any member.

Admin Dashboard

J

Name
John Doe

Email Id
johndoe@gmail.com

EDIT LOGOUT


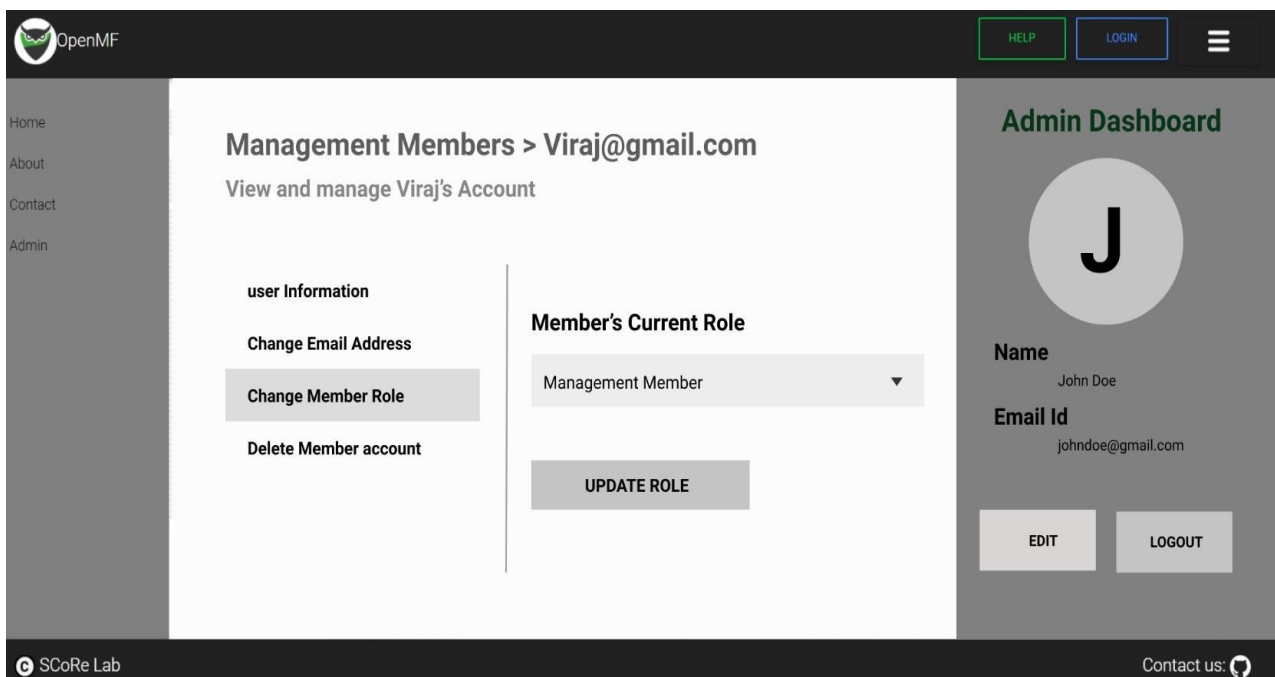
SCoRe Lab Contact us: 

Figure 2: Page to manage all the management members by admin

(Description for Figure 2: - When an admin clicks on Figure 1's "Management Members" then this page will visible that would help the admin to see all of the management member also the admin can click on any of the details to make a change to that member like role change, email change or to remove a member.)



OpenMF HELP LOGIN

Home About Contact Admin

Management Members > Viraj@gmail.com

View and manage Viraj's Account

user Information

Change Email Address

Change Member Role

Delete Member account

Member's Current Role

Management Member

UPDATE ROLE

Admin Dashboard

J

Name
John Doe

Email Id
johndoe@gmail.com

EDIT LOGOUT


SCoRe Lab Contact us: 

Figure 3: Page for changing role of a member

The screenshot shows the OpenMF Admin Dashboard. The top navigation bar includes the OpenMF logo, a HELP button, a LOGIN button, and a menu icon. The left sidebar contains links for Home, About, Contact, and Admin. The main content area is titled "Management Members > Viraj@gmail.com" and "View and manage Viraj's Account". It features a sidebar with options: user Information, Change Email Address, Change Member Role, and Delete Member account. The main content displays member details: Name (Viraj malhotra), Email Address (viraj@gmail.com), Account Type (Management Member), and Joined Date (12 August 2018). The right sidebar, titled "Admin Dashboard", shows a user profile for John Doe with a large 'J' avatar, Name (John Doe), Email Id (johndoe@gmail.com), and buttons for EDIT and LOGOUT. The footer includes the SCoRe Lab logo and a contact link.

OpenMF

HELP LOGIN

Home About Contact Admin

Management Members > Viraj@gmail.com

View and manage Viraj's Account

user Information

Change Email Address

Change Member Role

Delete Member account

Name Viraj malhotra

Email Address viraj@gmail.com

Account Type Management Member

Joined Date 12 August 2018

Admin Dashboard

J

Name John Doe

Email Id johndoe@gmail.com

EDIT LOGOUT

SCoRe Lab Contact us:

Figure 4: View Information of a member

This screenshot shows the same OpenMF Admin Dashboard as Figure 4, but with the "Change Email Address" option selected in the sidebar. The main content area now displays the "Member's Current Role" section, which includes a text input field containing "viraj@gmail.com" and an "UPDATE EMAIL" button. The rest of the interface, including the navigation bar, sidebar, and right-hand admin dashboard, remains identical to the previous figure.

OpenMF

HELP LOGIN

Home About Contact Admin

Management Members > Viraj@gmail.com

View and manage Viraj's Account

user Information

Change Email Address

Change Member Role

Delete Member account

Member's Current Role

viraj@gmail.com

UPDATE EMAIL

Admin Dashboard

J

Name John Doe

Email Id johndoe@gmail.com

EDIT LOGOUT

SCoRe Lab Contact us:

Figure 5: Page for changing email of a member

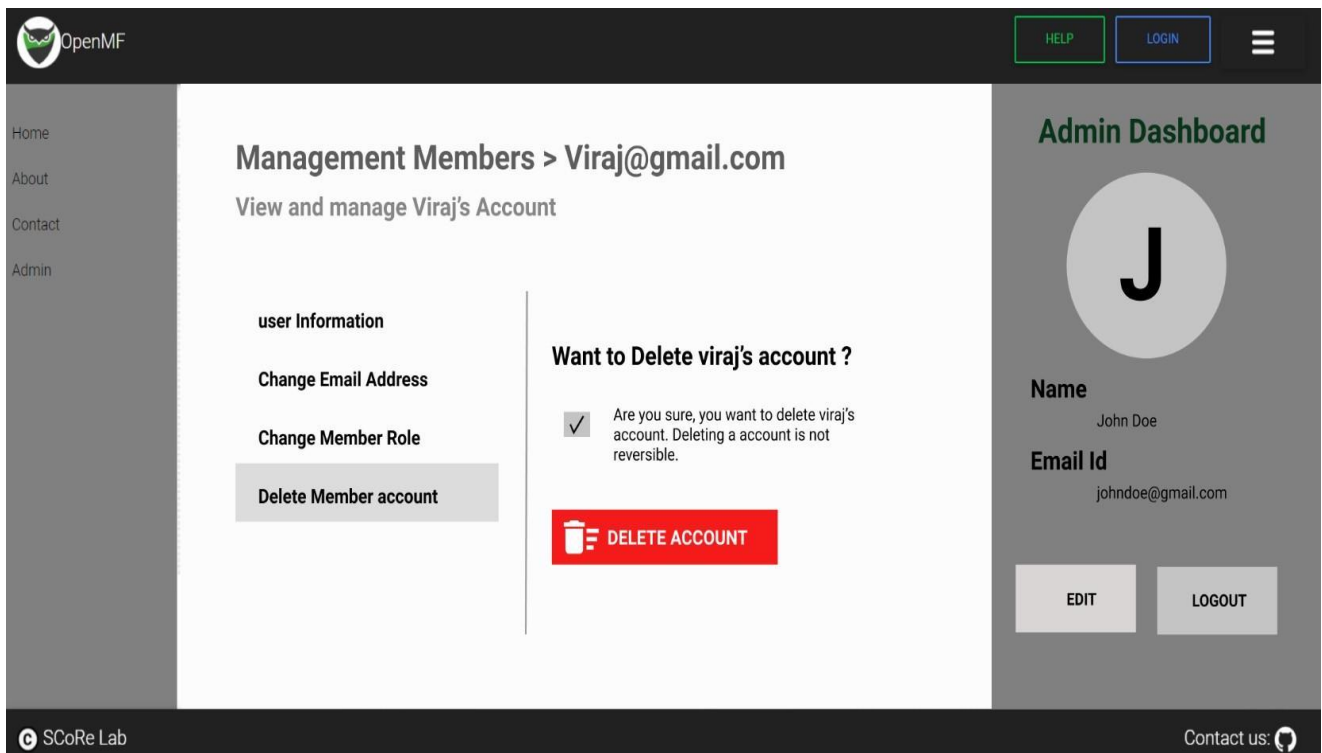


Figure 6: Page for deleting a member's account by admin

(Description for Figure 3, 4, 5 and 6: An admin has the privileges to View, changing email, updating role and Removing/Deleting a member's account.)

- **OpenMF's management dashboard: -**

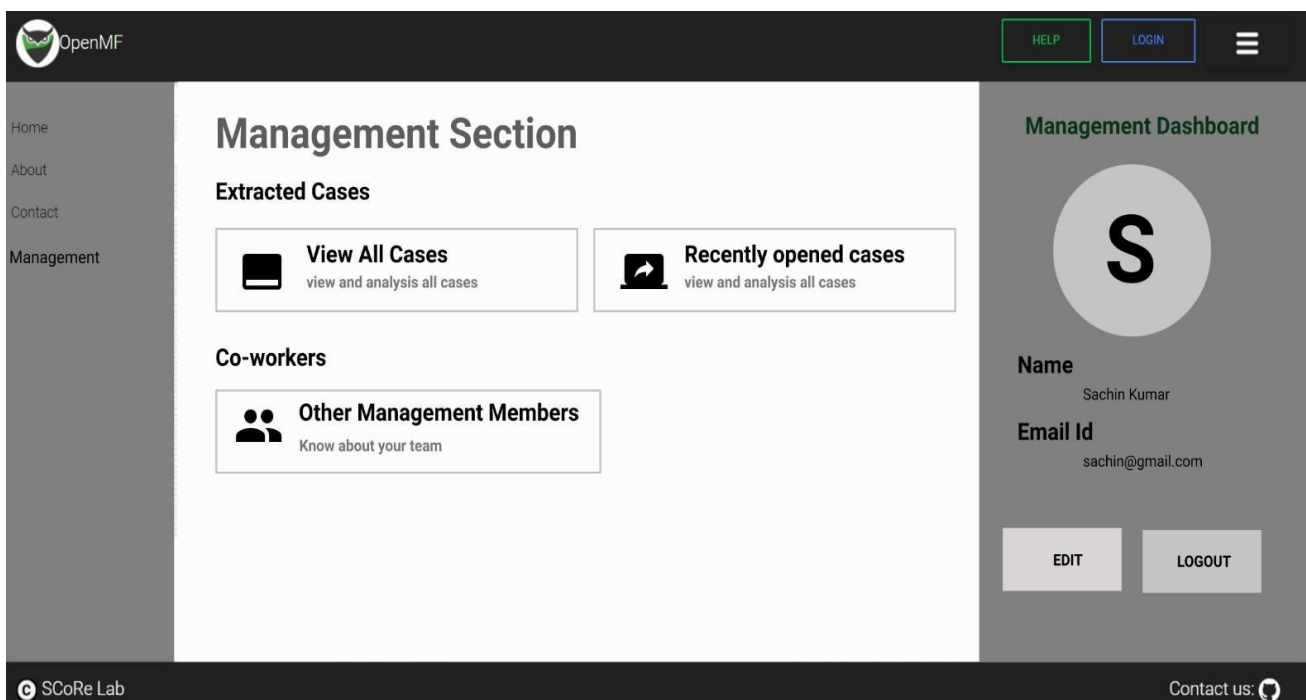


Figure 7: - Management section

(Description for figure 7: - Every management member has privileges for View and analyse each case, also a management member can View other management members who work under the same admin.)

- o Design and Implement Dashboard for management section.
- o Creating different sections inside the management dashboard like cases analytics section.
- o Fetching all the management members and cases to make it more user friendly.
- o Refer figure for these purposes.

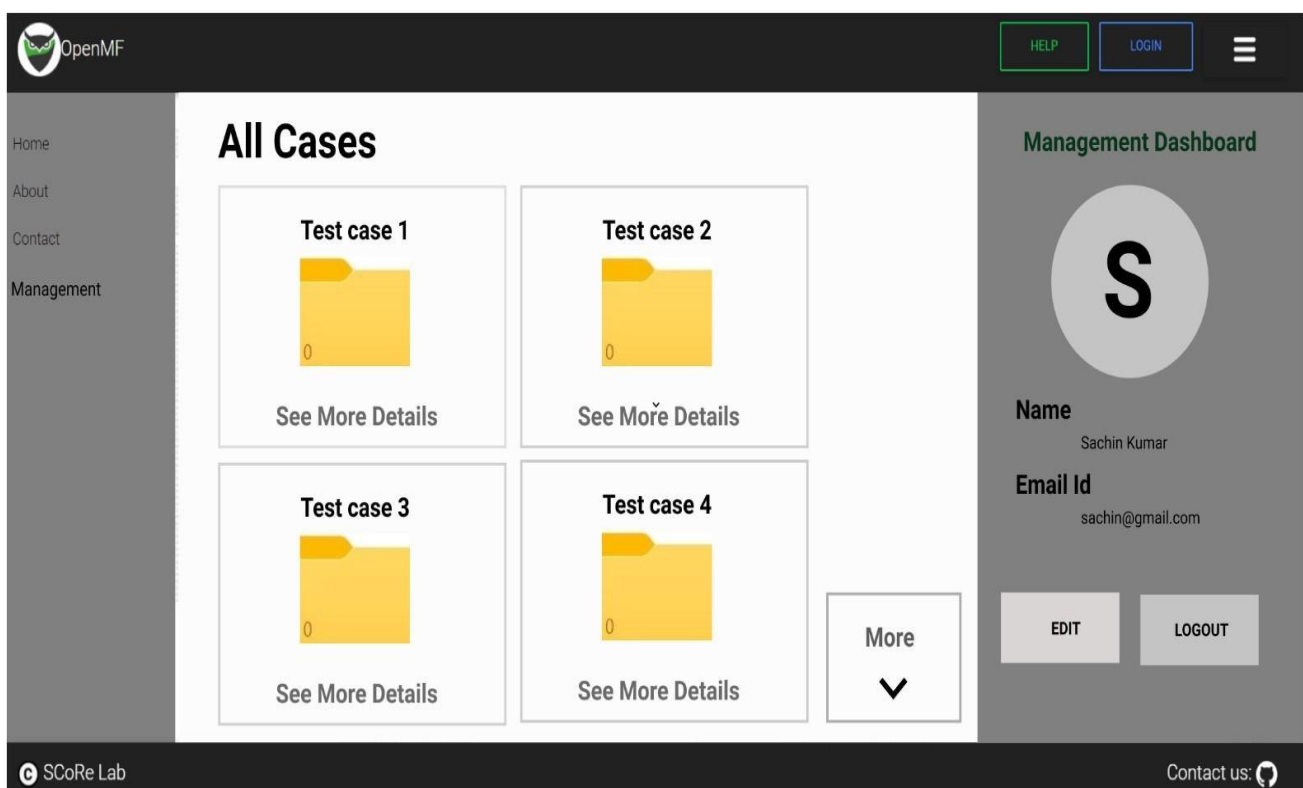


Figure 8: - Page to View all extracted case

- **OpenMF's Extractor dashboard: -**
 - o Design and Implement Dashboard for Extractor section.
 - o Integrating flask backend with extractor dashboard to list all the active devices.
 - o Creating a Data extraction option so that an extractor can extract data and push them to the database.
 - o Refer figure for these purposes.

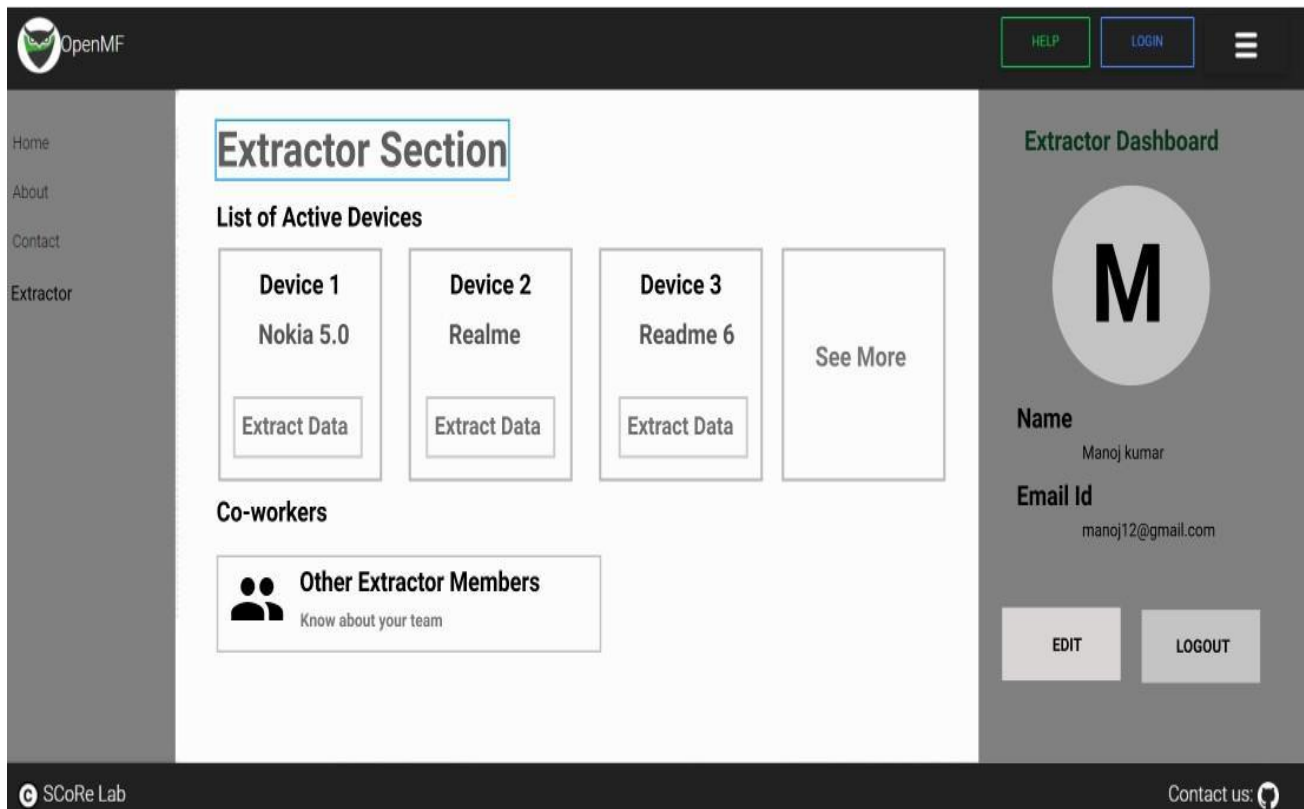


Figure 9: - Extractor section

(Description for Figure 9: - Extractor would have the privilege to View all the active devices, extracting data and to save them to the database.)

- **Implementing analysis on the Cases:** -
 1. Searching a word among all the cases: -
 - i. Creating a query that would give all the cases that would contain the searched word.
 - ii. Furthermore, sorting could be applied to the above output, to find the case that contains the maximum occurrence of the searched word.
 2. Sorting all the Cases: -
 - i. Sorting cases based on their extracted date, data size and starting alphabet.
 3. Listing All the Cases that are extracted between given dates.
 - i. For Example, if a management member wants to View a list of cases that were extracted between 1 January 2021 to 10 January 2021, then this query should return the cases that were extracted between specified dates.
 4. Comparing two cases: -
 - i. Creating a query that would take two case names as input and return the word that repeats the maximum number of times in them.
- **Refactoring React router:** -
 - o Connecting all the react components to a specific URL path using react-router and react-router-dom.
- **Creating REST APIs:** -

I am supposed to create some API and modify some of the existing APIs to make this project more user friendly. Some of them are following: -

S.NO.	API Route	Description
1.	user/delete/admin/{admin-id} → Method: DELETE → Login required → Only accessible by an admin	This route would be used to delete an admin's account. When an admin wants to delete an account, this route will first check whether the admin has any member or not. Because in the database, all the members contain a foreign key for referencing their admin email, so deleting directly an admin's account might generate storage problems.
2.	user/admin/deleted-users → Method: GET → Login required → Accessible by an admin	Response: List of all deleted users of an admin.
3.	cases/count/{admin-name} → Method: GET → Login required → Accessible by an admin and management members of a forensic organisation.	Response: count of extracted cases for a specific forensic organisation.
4.	cases/details/case-name/{folder-name} → Method: GET → Login required → Accessible by an admin and management members of a forensic organisation.	Response: Shows the details of a folder inside the management dashboard. Like extracted date, count of files, extracted member id and device name etc.
5.	cases/details/case-name/{folder-name}/{file-name} → Method: GET → Login required → Accessible by an admin and management members of a forensic organisation.	Response: Shows the details of a file inside the management dashboard. Like extracted date, extracted member id, device name and data size etc.
6.	cases/all-delete-cases → Method: GET → Login required → Accessible by an admin and management	Response: List all the deleted cases with details like case name, delete date and extracted member id

	member of a forensic organisation.	etc.
7.	extraction/cases/{extractor-id} → Method: GET → Login required → Accessible by extractor member and admin.	Response: Shows all the cases that are extracted by a specific extractor member.
8.	user/extractor/profile/{extractor-id} → Method: GET → Login required → Accessible by extractor member and admin.	Response: Shows all the profile details of an extractor that would be shown on the extractor dashboard and admin dashboard.

Note: - More APIs could be designed and developed during development period as per project requirements.

- **Case Analytics:** -

Data visualization provides us with a quick, clear understanding of the information. we can visualize large volumes of data in an understandable and coherent way, which in turn helps us comprehend the information and draw conclusions and insights. This helps us save time and lets us solve problems more efficiently.

Once the extractor extracts data from devices and pushes them to the database, the management member can analyse the cases based on various types of charts and graphs.

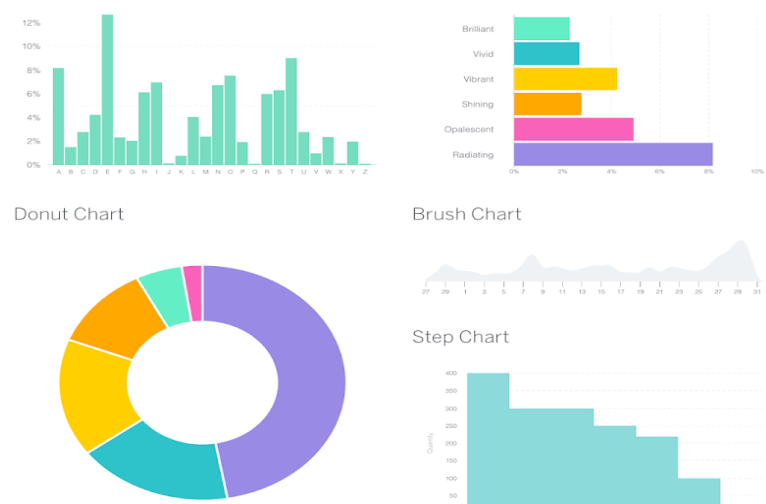


Figure 10: - charts supposed to create using d3.js for case analysis

I would implement this task of data visualization using D3.js library by drawing graphs like Pie Chart, Line graphs, Bar graphs etc.

- **Dockerizing OpenMF Project: -**

I am willing to use Docker containers and build an image for this project. This would have many benefits. Then the project will be self-maintained and easy to set up regardless of the system dependencies. Once containerization, this project could easily be deployed to any platform, like Google Cloud Platform, AWS etc.

- **Updating Project Wiki and Providing Video for setup: -**

I am supposed to document the project setup for different sections of this project like React frontend, flask backend, project guide to use OpenMF and listing all the APIs that were used in this project. Also, creating a Video explaining the complete setup of this project and working of the project.

- **Improving web performance: -**

Web performance can be improved by various techniques. This could be seen in the given figure.

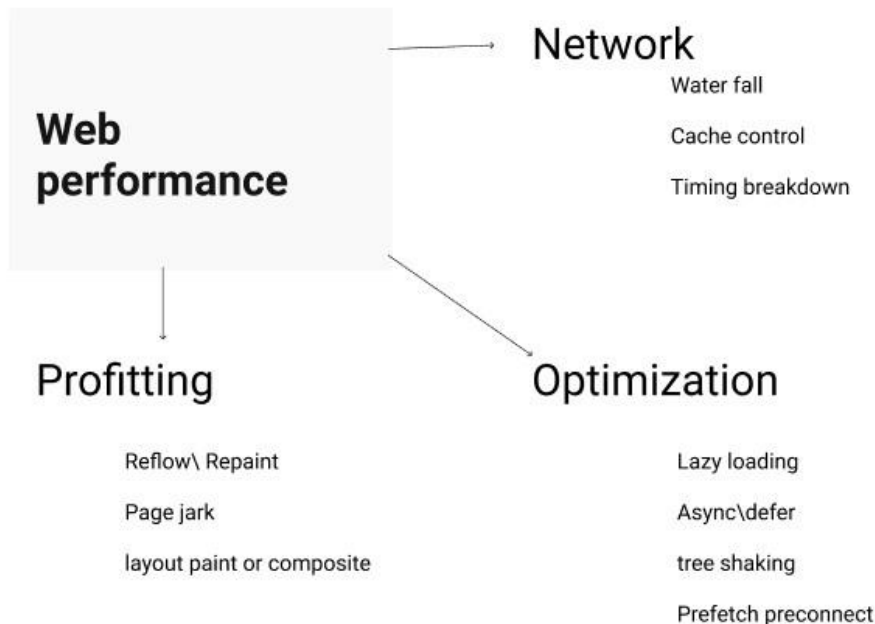


Figure 11 : - Web performance improving techniques

Project Tech stack: -

- React for Project Frontend.
- Flask for Creating REST APIs.
- SQLAlchemy.
- Styling components and material UI for styling purpose.
- Redux, Redux-Saga, Redux-toolkit for state management purposes.
- React-router and React-router-dom for Routing purpose.
- Python.
- Python-adb and adb-shell.

Timeline

Week	Time Period	Task
Community Bounding	May 17 to June 7	<ul style="list-style-type: none"> – Communicate with the mentors and know more about the project. – Getting each and every insight of the project to consolidate the whole development process. – Working some of the existing bugs or issues.
Week 1	June 7 to June 13	<ul style="list-style-type: none"> – Continue to refine the plans for the project's UI. – Complete the required Changes in UI based on mentor's feedback. – Writing My first blog for sharing experience regarding community bonding and GSOC's first week. – Finalizing UI for project's frontend.
Week 2	June 14 to June 20	<ul style="list-style-type: none"> – Start working on the Admin dashboard. – Creating react components for different sections of the admin dashboard. – React component for management section, extractor section and cases section in for admin dashboard. – Writing blog for week 2.
Week 3	June 21 to June 27	<ul style="list-style-type: none"> – Continue working on the admin dashboard. – Creating react components for View, update and delete management members and extractor members.

		<ul style="list-style-type: none"> – Implementing cases in the section inside the admin dashboard and integrating it with the flask backend. – Writing blog for week 3.
Week 4	June 28 to July 4	<ul style="list-style-type: none"> – Start implementing a dashboard for the management section. – Integrating extractor components to SQLAlchemy to push extracted data to the database. – Writing blog for week 4.
Week 5	July 5 to July 11	<ul style="list-style-type: none"> – Start implementing extractor member dashboard. – Preparing for first evaluation. – Writing blog for week 5.
First Evaluation (12 July to 16 July)		
Week 6	July 12 to July 18	<ul style="list-style-type: none"> – submitting Phase 1 evaluations. – Getting feedback regarding the project flow and doing the required changes. – Complete all the remaining work from week 1 to week 5. – Combining all the react components using react-router. – Writing blog for week 6.
Week 7	July 19 to July 25	<ul style="list-style-type: none"> – Developing and implementing SQL queries to do analysis among extracted cases. – Implementing some REST APIs in Flask related to cases. – Writing blog for week 7.
Week 8	July 26 to August 1	<ul style="list-style-type: none"> – Set up and Integrate Chart.js to React. – Creating various graphs to enable easy analysis over extracted cases in the management section. – Writing blog for week 8.
Week 9	August 2 to August 8	<ul style="list-style-type: none"> – Updating project wiki. – Dockerizing the whole project. – Writing blog for week 9.
Week 10	August 9 to August 15	<ul style="list-style-type: none"> – Getting feedback regarding the project flow and doing the required changes.

		<ul style="list-style-type: none">- Recording a video for project setup and working of the project.- Cleaning the code, clearing console errors or warnings.- Writing blog for week 10.
Final Week Submitting final work and final evaluation.		
		<ul style="list-style-type: none">- Continue to work on this project, finishing items that are in the extra milestones section.

References:

1. Scorelab official Website: - <https://scorelab.org/>
2. OpenMF GitHub link: - <https://github.com/scorelab/OpenMF>

End of Proposal