Stratosphere Research Laboratory | GSoC Proposal

Improvement of Slips web interface

Table of contents:

ABSTRACT

Slips is a behavioral intrusion prevention system that uses machine learning to detect malicious behaviors in network traffic. Slips focus on targeted attacks, detection of command and control channels, and providing a good visualization for the analyst. It can analyze network traffic in real-time, network captures such as pcap files, and network flows produced by Suricata, Zeek/Bro, and Argus. Slips processes the input data, analyzes it, and highlights suspicious behavior that needs the analyst's attention.

Slips is full of features and crazy ideas, detection methods, databases, machine learning and many many more (including a P2P detection system!). So get to know the project, try it, and come up with your own ideas.

Proposed lists of topics that could be included:

- Adapting the web interface to show all the information Slips has on each profile (connections, attacks, detections, etc.)
- Manage the complete configuration of slips from the web.
- Add graphs for continuous visualization of traffic
- Add explanations for alerts, evidence, and flows.

ABOUT ME

Full name	Shubhangi Choudhary
Discord username	Shubhangi#7161
Primary spoken language	English
University	Indian Institute of Technology (BHU), Varanasi
Course Major	Electrical Engineering
GitHub	https://github.com/shubhangi013
LinkedIn	https://www.linkedin.com/in/shubhangi-choudhary-32a347205/
Contact No	+91-7895870753

Slack handle	Shubhangi
Primary email	shubhangi.student.eee20@itbhu.ac.in
Secondary email	choudharyshubhangi13@gmail.com
Project Interested in	Slips

I'm Shubhangi, an Electrical Engineering undergraduate at IIT (BHU), Varanasi. I am an avid developer and love playing CTFs. I started out with development on May '21 with the basics. Later, over the months, I explored various technologies. Via a course I undertook, I practiced the MERN stack and by being a part of the website teams of various college bodies and hackathons, I got my hands dirty on other technologies, like Django, Vue.js, Angular, etc.

I am currently the secretary of the Club of Programmers, IIT (BHU), the programming society of my university - IIT (BHU) Varanasi

It was the power of Stratosphere's robust architecture fueled my interest in this project. I started contributing to several open source projects in June'21.

MY CODING SKILLS

I have been interested in programming since my first semester itself.

Relevant Courses:

1. Computer Programming in C (CSO 101)
2. Information Security (CSE 530)
3. Deep Learning: a hands-on Introduction offered by the University of Genoa

I started out in competitive programming wherein I used to code in **C++ and C**.Consequently, I got fascinated with CTFs and Machine Learning, for which I had to use **Python3**. Eventually, I ended up developing an interest in Software Development. Starting off with basics (**HTML, CSS, and JavScript**), I later moved to frameworks and technologies built around **Node.js**. I have recently been practicing Rust by following the

rustbook. Following are the frameworks, technologies, and languages I've used, apart from the aforementioned:

1. React
2. MongoDB
3. Express.js
4. Node.js
5. Django
6. Angular
7. TypeScript
8. Next.js
9. Rust
10. Flask

Here you can find all the projects I've been working on and contributing to:https://github.com/shubhangi013

I am a quick learner and very keen on expanding my horizons to newer technologies. If the project requires a skill I need to learn, I will give my 100% to practicing it.

MY BACKGROUND ON THE FOLLOWING TOPICS: SECURITY, NETWORKS, MACHINE LEARNING

Security and Networks : I have pursued a course on Information Security (CSE530) in my 5th Semester as an open elective and scored a decent grade ('A') in a class of around 100 students. The course revolved around learning about various cybersecurity attacks and frameworks used to prevent them. We learned about cryptography and other tools and techniques used to protect information. I also demonstrated a web injection attack during this class.

Machine Learning : I have completed the summer school on Deep Learning: a hands-on Introduction organized by University of Genoa, Italy in which I got accepted through an application submission. Currently, I am pursuing a course on Soft Computing (CSE458) which teaches us about various neural networks, genetic algorithms and the fuzzy set theory.

Besides the coursework, I have been attempting CTFs since my very first semester. The culmination of my love for development and security made me contribute at OWASP during my sophomore year.

PREVIOUS CONTRIBUTIONS / OPEN SOURCE DEVELOPMENT EXPERIENCE

I've been contributing to open-source since June'21 and was gravitated towards OWASP because of the way security and open-source were both being addressed at the same place in an active community. I have contributed to both the GUI and CLI parts of the project. I've also enhanced the documentation. I have also contributed to PublicLab and many other organizations with a vast range of technologies.

Pull requests

Following are the pull requests I've opened in OWASP projects along with their status:

Pull requests	Description	Status
#87	Added user-friendly colors to the UI of PyGoat	Merged
#88	Revamped and improved the Login form's UI	Merged
#330	Added the correct commands for installation of SecureTea	Merged
#333	removed unnecessary conditional code and added the instruction to quit the application	Merged
#336	Corrected the warnings in the Python code on running SecureTea and corrected user guide's commands & improved GUI	Merged
#339	changed the color of the log-text.png as per the rest of the GUI	Merged
#345	Removed repetition of commands to setup the server log monitor	Merged
#354	Added instructions for setting up the web GUI for developers and corrected commands	Merged
#357	Added the login route to the register form	Open
#355	Corrected the CLI and the user image.	Open

Following are my contributions in PublicLab

Pull requests	Description	Status
#266	Aligned the images in the Readme to the center and added corresponding alt text	Merged
#268	remove the “thumbnail generation” code and corresponding stale code	Merged
#293	removed the unnecessary and vague logs	Merged
#326	as per this discussion, added the FTO template	Merged
#368	corrected the text in the quickstart moda	Merged

Following are my contributions in Slips:

Pull requests / issues	Description
#296	Added tooltips on table headers
#295	[webInterface] Add tooltips for new users
#294	Major overlap in the sidebar with the main window

Issues

I’ve opened the following issues:

Issues	Status
#329	Closed
#332	Closed
#338	Open

WHAT SCHOOL DO YOU ATTEND AND WHAT IS YOUR SPECIALTY/MAJOR AT THE SCHOOL?

I cleared the toughest undergraduate examination in India and the second toughest exam in the world , IIT JEE and got admission in IIT BHU in the department of Electrical Engineering. I am in the 6th semester of my 3rd year at the college. We are taught about control systems, power systems, modern day machines and digital and power electronics.

WHAT CITY/COUNTRY WILL YOU BE SPENDING THIS SUMMER IN? WHAT'S YOUR TIMEZONE?

I will most likely be spending my summer in two cities in India : Hyderabad and Varanasi. My time zone: India Standard Time,Time zone in India (GMT+5:30)

HOW MUCH TIME DO YOU EXPECT TO HAVE FOR THIS PROJECT?

I expect to devote a weekly 30-35 hrs to this project.

PLEASE LIST ALL JOBS, SUMMER CLASSES, VACATIONS, EXAMS, AND/OR OTHER COMMITMENTS THAT YOU'LL NEED TO WORK AROUND DURING GSOC.

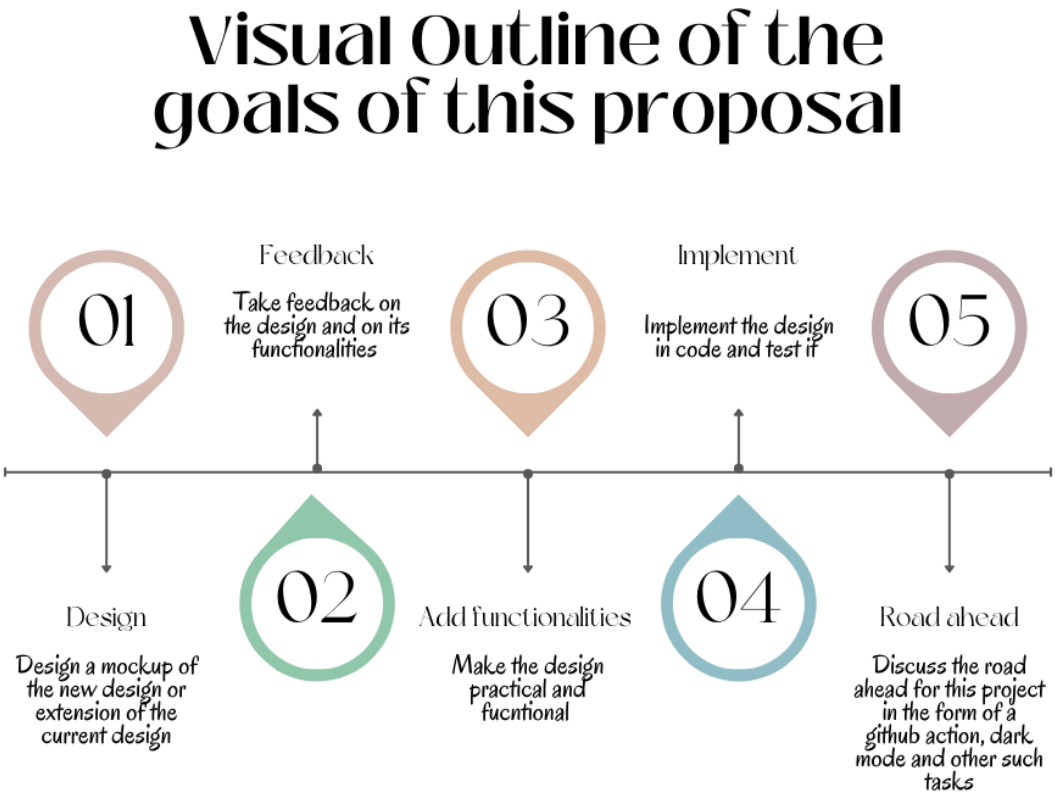
I will not be having any classes from May 10th 2023 to July 20th 2023. After that, I'll enter my 7th semester , the classes of which are hardly 4 hrs a day. So, I will be able to dedicate my time completely to my GSoC project.

I will be working on this project (hopefully :)) during my summer vacation.

I HAVE NOT APPLIED FOR ANY OTHER PROJECT UNDER GSoC'23

MY RESUME : click here

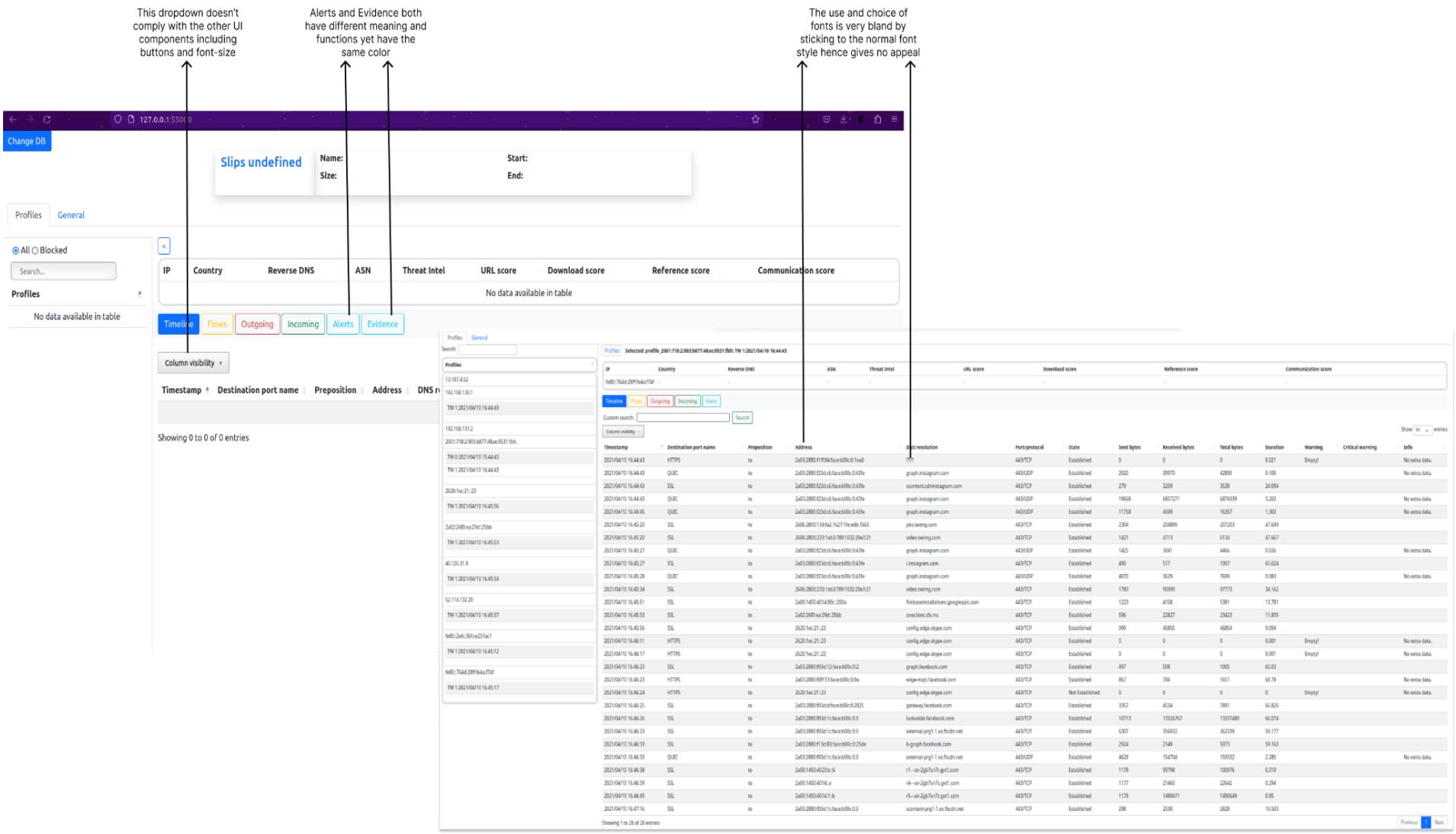
PROPOSED CHANGES

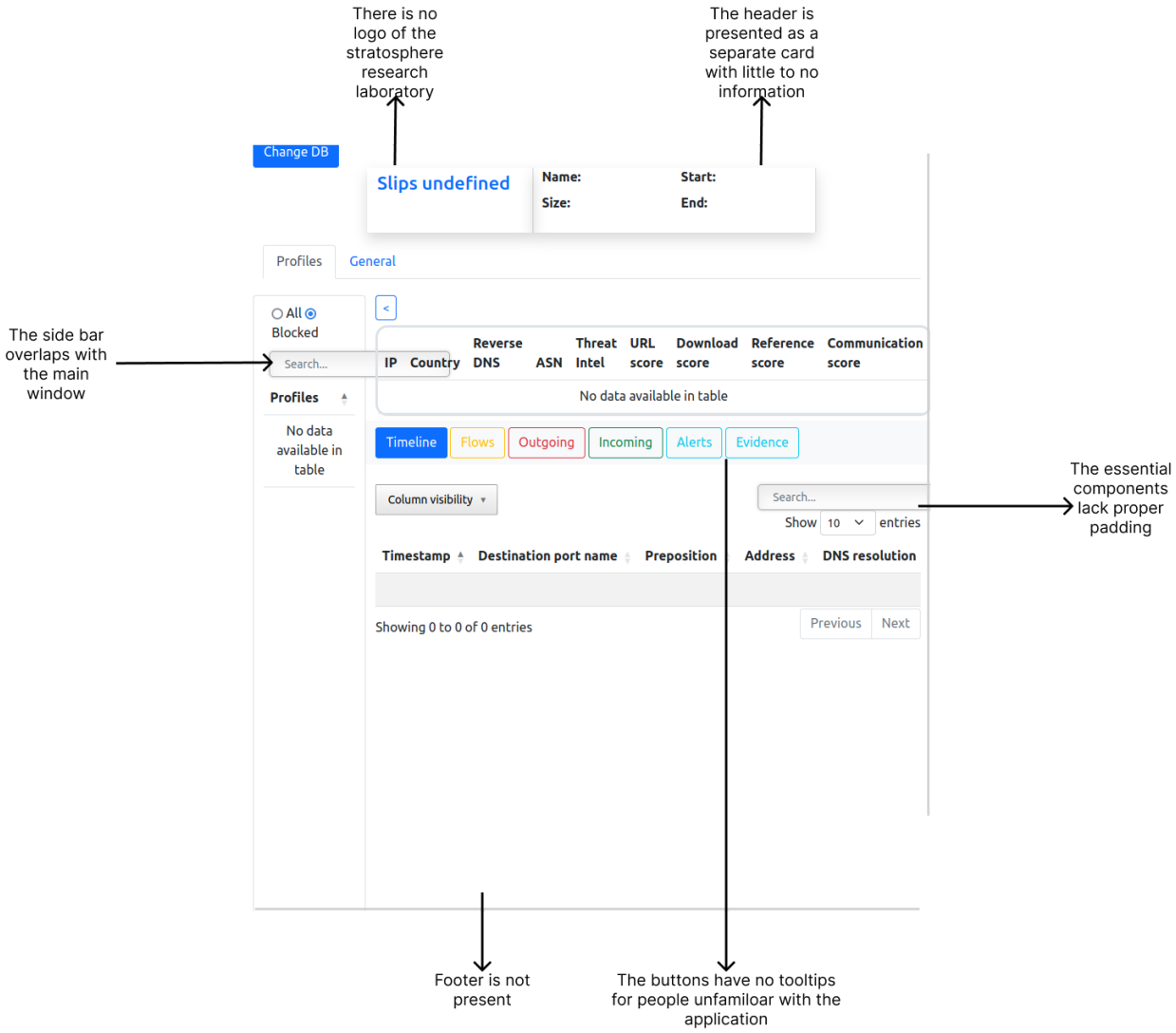


Web GUI

- **Problem:**

  The current GUI is just about functional and lacks a definite and uniform design.

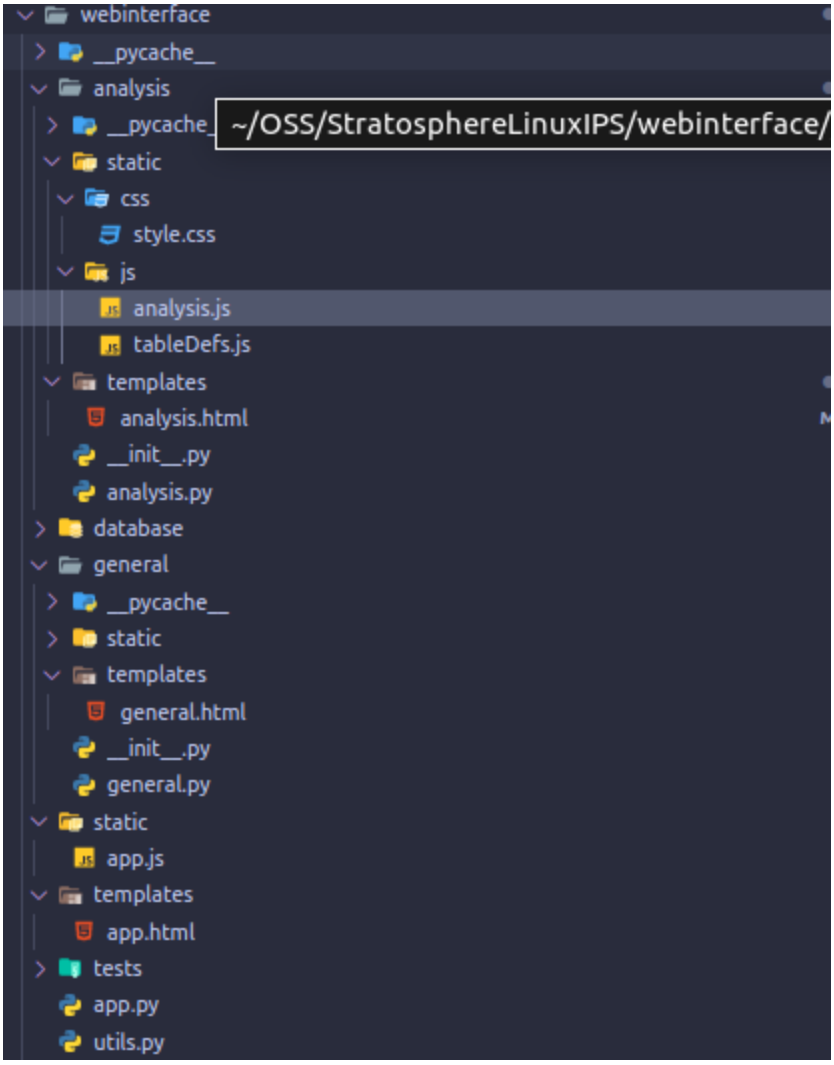

This dropdown doesn't comply with the other UI components including buttons and font-size
Alerts and Evidence both have different meaning and functions yet have the same color
The use and choice of fonts is very bland by sticking to the normal font style hence gives no appeal
127.0.0.1:55000
Change DB
Slips undefined
Name:
Size:
Start:
End:
Profiles
General
All
Blocked
Search...
Profiles
No data available in table
IP
Country
Reverse DNS
ASN
Threat Intel
URL score
Download score
Reference score
Communication score
No data available in table
Timeline
Flows
Outgoing
Incoming
Alerts
Evidence
Column visibility
Timestamp
Destination port name
Preposition
Address
Showing 0 to 0 of 0 entries



- **Tasks**

(I have added mockups and code implementation for some of the features.)

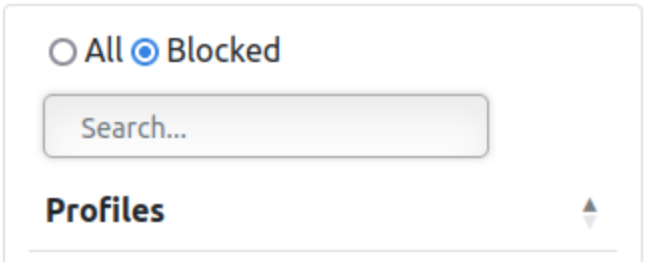
1. Better Display of time window numbers, start time, and end time



The above image is the folder structure for the files to be manipulated to implement the said tasks.

2. Showing all the info we have on each profile.
3. Show a list of Blocked Profiles in one place

   There exists a filter :



We can create a separate table or section to implement this further .

4. Show the history of threat levels and confidence of each profile
5. If an IPv4 profile has an available IPv6 we should show it. and vice versa
6. Show the current threat level of each profile with graphs which can be implemented easily using Chart.js as follows

The code for which can be written as :

```
<div class="box" style="width: 600px; height: 800px; top: 20px;">
    <canvas id="lineChart"></canvas>
</div>
```

And a script file written as :

```
window.addEventListener('load', displayLineChart);

  function displayLineChart() {
      var chartDot = new Image();
      chartDot.src =
'https://cdn.icon-icons.com/icons2/1879/PNG/512/iconfinder-8-avatar-2
754583_120515.png';
      chartDot.width = 25;
      chartDot.height = 25;

      var ctx =
document.getElementById("lineChart").getContext("2d");
      var chart = new Chart(ctx, {
      type: 'line',
      responsive: false,

      // The data for our dataset
      data: {
            labels: ['Week1', 'Week2', 'Week3', 'Week4', 'Week5',
'Week6', 'Week7'],
            datasets: [
            {
            label: 'Threat',
            fill: false,
            backgroundColor: '#B1B695',
            borderColor: '#B1B695',
            data: [0, 15, 5, 2, 20, 25],
            pointStyle: chartDot,
            pointRadius: [0, 0, 0, 0, 0, 1]
            },
            {
            label: 'Alerts',
            fill: false,
            backgroundColor: '#9DB4C0',
            borderColor: '#9DB4C0',
            data: [0, 10, 3, 19, 25],
            pointStyle: chartDot,
            pointRadius: [0, 0, 0, 0, 1]
```

```
            }
        ]
        },

        options: {}
        });
    }
```

The dataset can obviously be stored overtime to present the information in the form of chart.

7. Show the user agent of each profile
8. Show the MAC of each profile
9. Live (Asynchronous) updating of the web view. (meaning that without refreshing the page, new info should be displayed)
10. Show slips logo somewhere
11. Showing about a profile
12. Progress bar

It can easily be implemented using bootstrap which has been used in the project through the simple code :

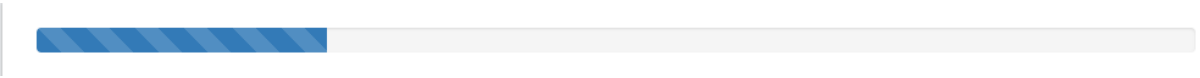
```
<div class="progress">
  <div class="progress-bar progress-bar-striped bg-warning
progress-bar-animated" role="progressbar" aria-valuenow="25"
style="width: 25%" aria-valuemin="0" ariavaluemax="100">
  </div>
</div>
```

And the following CSS :

```
.progress
{
  width: 50%;
  margin: 1.5em 0 0 2em;
  background: #999;
}
```

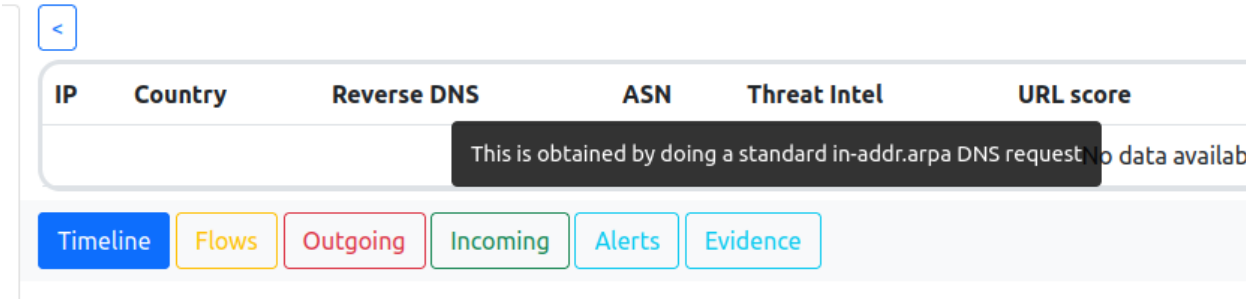
```
.progress-bar
{
  height: 40px;
  padding: 1em;
}
```

Which gives us the following output



We can also choose to animate the bar as per the CSS-framework we wish to work with.

13. We can also add tooltips to each button and table title such as:



Which has been added in the file

```
StratosphereLinuxIPS/webinterface/analysis/templates/analysis.html
```

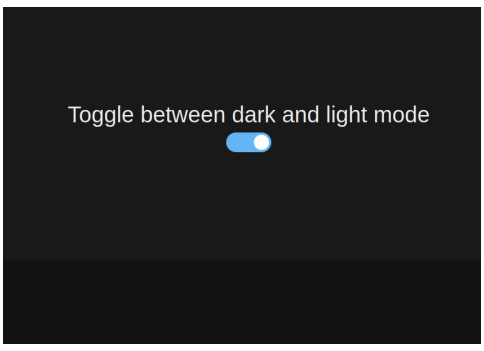
Through the following code

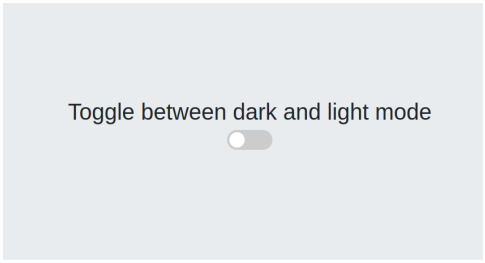
```
    <div class="row">
    <table id="table_ipinfo" class="table">
    <thead>
        <tr>
```

```
            <th>IP</th>
            <th>Country</th>
            <th data-toggle="tooltip" data-placement="top" title="This
is obtained by doing a standard in-addr.arpa DNS request">Reverse
DNS</th>
            <th>ASN</th>
            <th>Threat Intel</th>
            <th>URL score</th>
            <th>Download score</th>
            <th>Reference score</th>
            <th>Communication score</th>
            </tr>
      </thead>
      </table>
      </div>
```

14. List of loaded modules and disabled modules
15. Show current model status (are we in training or testing mode)
16. Show the current gateway's IP and MAC, an mark the gateway profile as 'Gateway'
17. Have a whitelist tab to show what IPs/domains/orgs are currently whitelisted
18. Add a dark mode to the application with a toggle switch

    A dark mode can be added which can be toggled using a switch





Implemented using bootstrap as the following lines of code :

```
<!DOCTYPE html>
<html lang="en">

<head>
  <meta charset="UTF-8">
  <meta name="viewport" content="width=device-width,
initial-scale=1.0">
  <meta http-equiv="X-UA-Compatible" content="ie=edge">
  <title>Toggle between dark and light mode</title>
  <link rel="stylesheet" href="./css/bootstrap.css">
  <link rel="stylesheet" href="./css/bootstrap-dark.css">
  <link rel="stylesheet"
href="https://cdnjs.cloudflare.com/ajax/libs/font-awesome/4.7.0/css/f
ont-awesome.min.css">

</head>
<body>
  <header>
  </header>
  <main role="main">

      <section class="jumbotron text-center">
      <div class="container d-flex align-items-center
justify-content-center flex-column" style='height:45vh;'>
      <h1 class="jumbotron-heading">Toggle between dark and light
mode</h1>
      <p>
            <label class="switch">
            <input type="checkbox" id='switch-theme'>
            <span class="slider round"></span>
            </label>
      </p>
      </div>
      </section>
  </main>

</body>
</html>
```

Styled with the following :

```
:root {
      --primary-dark:#121212 ;
      --color-dp0: #191919  ;
      --color-dp1: rgb(35,35,35) ;
      --color-dp2: rgb(38,38,38) ;
      --color-dp3: rgb(41,41,41) ;
      --color-dp4: rgb(42,42,42) ;
      --color-dp6: rgb(48,48,48) ;
      --color-dp8: rgb(49,49,49) ;
      --color-dp12: rgb(53,53,53) ;
      --color-dp16: rgb(56,56,56) ;
      --color-dp24: rgb(58,59,59) ;
      --color-text: #eee ;
      --color-text-secondary: #a0a0a0;
      --color-white: #fff;
      --color-blue-secondary: rgb(0, 99, 204);
      --color-blue-tertiary: rgb(0, 123, 255);
      --select-width: 80px;
      --select-height: 35px;
}
.switch {
      position: relative;
      display: inline-block;
      width: var(--select-width);
      height: var(--select-height);
      animation : moveUp .5s .5s;
      animation-fill-mode:backwards;
}
@keyframes moveUp {
      from {
      transform:translateY(30px);
      opacity:0;
      }
      to {
      transform:translateY(0px);
      opacity:1px;
      }
```

```css
}

.switch input {
 opacity: 0;
 width: 0;
 height: 0;
}
.slider {
 position: absolute;
 cursor: pointer;
 top: 0;
 left: 0;
 right: 0;
 bottom: 0;
 background-color: #ccc;
 -webkit-transition: .4s;
 transition: .4s;
}

.slider:before {
 position: absolute;
 content: "";
 height: calc(var(--select-height) - 2 * 4px );
 width: calc(var(--select-height) - 2 * 4px );
 left: 4px;
 bottom: 4px;
 background-color: white;
 -webkit-transition: .4s;
 transition: .4s;
}

input:checked + .slider {
 background-color: var(--color-dark-primary);
}

input:focus + .slider {
 box-shadow: 0 0 1px #2196F3;
}
```

```
input:checked + .slider:before {
 -webkit-transform: translateX( 45px );
 transform: translateX( 45px );
}

/* Rounded sliders */
.slider.round {
 border-radius: 34px;
}

.slider.round:before {
 border-radius: 50%;
}

html {
      scroll-behavior: smooth;
}
body {
      transition:.35s all ease-out;
}
[data-theme="dark"] .jumbotron
{
      background: var(--color-dp0) !important;
}

[data-theme="dark"] body{
      background-color: var(--primary-dark) !important;
      color: var(--color-text) !important;
}

[data-theme="dark"] .bg-light {
      background-color: var(--color-dp0) !important;
}

[data-theme="dark"] .bg-white {
      background-color: var(--color-dp0)  !important;
}

[data-theme="dark"] .bg-dark {
```

```
      background-color: var(--color-dp4) !important;
}

/* custom checkbox */

.btn-fixed--right-corner {
      position:fixed;
      bottom:25px;
      right:25px;
      width:45px;
      height:45px;
      font-size:1.8rem;
      font-weight:700;
      display:flex;
      align-items:center;
      justify-content:center;
}
```

And made functional using the following script file :

```
const btn = document.getElementById('switch-theme');
localStorage.setItem('theme','light');
btn.addEventListener('click',(e)=>{
      let theme = localStorage.getItem('theme');
      console.log(theme);
      if(theme == 'light' || theme ==''){

document.documentElement.setAttribute('data-theme','dark');
            localStorage.setItem('theme','dark');
      }
      else {
            document.documentElement.removeAttribute('data-theme');
            localStorage.setItem('theme','light');
      }
})
```

19. Manage the configuration of slips from the web
    - Change the feeds : JA3 feeds, SSL feeds, TI feeds

- Whitelist
- Manage API keys: VT, riskIQ, slack bot token
- Warden.conf
- Slips.conf
- Local TI files

Documentation

- **Problem**

  The current documentation lacks the developer friendly instruction on how to contribute to the web interface of the application

- **Tasks**
  - Create an issue as well as pull request template specifically for the web interface and subsequently to contribute to the other parts of the application.
  - Update the contribution guidelines on https://stratosphere linuxips.readthedocs.io/en/develop/contributing.html and include on how to contribute to specific parts of the application.

Create a GitHub Action for the repository

- **Problem**

  The repository should be beginner-friendly and less intimidating for first-time users and contributors.

- **Tasks**

  Install and configure a GitHub action for the repository. If the need persists or is not fulfilled, create a GitHub action that encourages first-time contributors on their first issue or pull request.

TIMELINE

I will strictly adhere to the following timeline. The tasks would be completed before the deadline.

Time period	Tasks
Community Bonding Period	
May 4 - May 28	• Discuss and get pending pull requests merged • Discuss with the mentors on what communication medium would they prefer for updates regarding the project
Coding period begins	
May 29 -June 15	• Discuss the library/framework to be used for the web GUI • Decide on the color palette of the GUI • Start designing of the Figma mockup of the design
June 16- July 14	• Implement the palette along with redesigning other components like the footer • Deploy the GUI on a platform like netlify that supports continuous integration of fresh commits • Start implementing the other functional features like the progress bar and other such features
Phase-1 Evaluation (July 14)	
July 14- Aug 4	• Revamp the documentation and extend the current docs to deploy on Jekyll or integrate them into the documentation section of the website of the project • Implement the GUI changes in the main repository • Describe the function of each command • Update the documentation with the latest GIFs and Images
Aug 5- Aug 12	Buffer week to complete the pending tasks and get them reviewed and discuss the implementation of additional features like a dark mode
Aug 13- Aug 27	• Create a GitHub action or install and set up an existing one from the repository • Bug fixing and discussion around future utilities we can add to the application • Discussion around testing of the written code
Aug 28 - Sept 4	• Get pending pull requests merged

	• Discuss future scope of the application • Write a blog about my Summer of Code journey
Final Evaluation : August 28 - September 4, 2023	

WHY AM I THE RIGHT PERSON FOR THIS TASK?

By playing CTFs, I gained an understanding of how fascinating the realm of application security is. As a tech enthusiast, I've been playing around with various application security tools. When I found out about the open source opportunities in security applications, I decided to give back to all the developers who develop those tools by contributing to open-source projects.

I have obtained an understanding of the entire repository. I have experience of working in a team because of hackathons and projects I've contributed to. **I am currently the secretary of the Club of Programmers. As the secretary, I have led the 4 different verticals Software Development Group, Infosec , Competitive Programming and Machine Learning.** I've been working with Node.js for the last 2 years and have made projects in TypeScript. I'm practicing Angular as well and have good knowledge of various CSS frameworks. I have undertaken workshops and tutorials for the people venturing out into programming. I, therefore, have an understanding of what a beginner needs. I will utilize this while revamping the documentation.

POST GSoC

Post GSoC, I would be connected with the organization. I would keep contributing with the same zeal because the project is more than an organization to me.GSoC would be a perfect opportunity to learn more while giving back to the community. Post GSoC period would be equally motivating.