AUTO OSINT

Specification & Plan

Student - Liam Moore (C00196503)
Supervisor – Richard Butler

Introduction 2
Inspiration/Motivation 2
Tool Overview 3
User Groups/Audience 3
Deliverables 4
    Core Deliverables 4
    Non-Core Deliverables 5
Use Case Diagram 6
Use Cases 7
    Input Search Parameters 7
    Perform Search 7
    Copy/Export 7
    Enter New Input 7
Example GUI's 8
    Before a search 8
    After a search 9
Dataflow Diagrams 10
Non-Functional Requirements 12
    Functionality 12
    Usability 12
    Reliability 12
    Performance 12
    Security 12
    Supportability 12
Project Plan 13
    GANTT Chart 13
Table of Figures 15
References 15

Introduction

This document will outline the idea behind the Auto OSINT (Open-Source Intelligence) tool and explain why a tool like this can be used to help people spend less time copying and pasting information from between applications. We will learn about the project's main objective, who the tool is catered towards and how it will work. The tool will be created as a browser extension, in particular, a Google Chrome extension. The reason for this was to focus on making the project function as intended for what is probably the most used browser in the world. "As of August 2023, Google's Chrome accounted for 63.56 percent of the global web browser market share." The main target audience for this tool will be for anyone working in the Cyber Security area as my thought process around this was mostly influenced by my experience as a Cyber Security Analyst.

Inspiration/Motivation

The motivation behind the idea of my Auto OSINT tool came to me the more familiar I got with carrying out investigations. I would be utilising various OSINT tools to perhaps retrieve information on a particular IP address or hash value for example. I noticed that this could become very time consuming, especially if it must be done multiple times per investigation. What my Auto OSINT tool will achieve is lowering the total amount of time that is spent copying and pasting by simply providing a centralised tool that can carry out OSINT searches on the specified IP addresses or hashes and displaying the results back to the screen for the user to then use how they please for their investigations.

Tool Overview

The Auto OSINT tool is designed to aid in investigations and help Cyber Security Analysts to reduce the overall time they spend carrying out OSINT during investigations thus allowing more time for other aspects. This will give the user the option to either search OSINT sites for IP addresses or hash values based on what is needed for their investigation. An IP address is "an identifying number for network hardware connected to a network. Having an IP address allows a device to communicate with other devices over and IP based network like the internet." These IPs are used to identify certain devices in a network and during an investigation it is important to know the location and owner of an IP address. The same can be said for hash values, which "can be thought of as fingerprints for file. The contents of the files are processed through a cryptographic algorithm, and a unique numerical value – the hash value - is produced that identifies the contents of the file." Analysts use the hash values to identify the name of a file or to verify its legitimacy. OSINT sites such as Virus Total and Abused IPDB store information in these which is useful in the Cyber Security world.

For the Auto OSINT tool, the user inputs all information that is required into the interface. They can then select what OSINT sites they would like to take information from, this will produce a standard output from that site. Multiple sites can be chosen by the user to increase scope and obtain more information. There is a final option where the user can select "*produce full report"*. This is the option where the user can find out the most information. This allows for an in-depth report to be created on the target IP address or hash value. Once users have conducted and a search using the tool, they have the option to export the data received into either a .txt file or a .csv file.

This will fulfil the purpose of the tool in reducing the amount of time spent investigating.

User Groups/Audience

This tool will be aimed towards any cyber security professionals or companies. Although the main aim of my project is to free up more time during investigations it is not limited to such. Companies can use it for their own purposes outside of investigations such as conducting OSINT on themselves to see what information is available and how they can lower what is retrievable.

The tool is not just limited to those in the industry, but it can be used in education to aid students studying cybersecurity to learn what information can be obtained on the internet. While doing this, it can also teach students about which type of information is important when conducting investigations. Teachers and lecturers can highlight the importance of a good investigation and how it can benefit students when they enter the industry. While being a student at SETU for 4 years there has never been any classes or tutorials conducted that educate the students on this topic and I think that cybersecurity students would really benefit from this.

As this tool will be a Google Chrome extension, it will be available to any individual who uses Google Chrome. From my research I cannot find an equivalent extension on the Chrome

Store. From my experience using the CrowdStrike platform I know that there is a built option that searches a given hash value from an alert in Virus Total. Although this functionality exists within the platform it still brings the user to the site and does not really decrease the overall time on an investigation as users are still copying and pasting from only one source. The Auto OSINT extension also wins out on cost as having that functionality within CrowdStrike only comes if you have implemented it in your network which costs $8.99 per month per end device.

Deliverables

The deliverables are key in the successful creation and implementation of this tool. They are the goals that I strive to achieve in order to ensure that the tool functions and looks as it is expected. The deliverables are separated into core and non-core deliverables. Core deliverables are the primary objectives needed to be achieved in my tool. Non-core deliverables are the secondary objectives that are not vital to the operation of the tool.

Core Deliverables

Auto OSINT Tool:

The most integral part of the project is of course the tool itself. It is a fully functional Google Chrome extension that works seamlessly within the browser. Another appeal of the tool is the clean design of the tool which enhances the user experience while also ensuring that the tool is easy to navigate for the user. The interface is uncluttered and features an intuitive layout making it straight forward for the user to carry out their specific searches for investigations. Attention will also be paid to the extensions colour scheme, font styles, and graphics in order to ensure that the visual elements are not only aesthetically pleasing but would also contribute to a more efficient workflow.

Communication with OSINT sites:

Another important aspect of the project is the efficient communication with the OSINT sites and the integration of the APIs. This integration ensures that the data is extracted seamlessly from the OSINT sites and the results to be displayed neatly back to the user. Recognising that no system, even the most well-designed are not immune to issues, it will be important to implement correct error handling mechanisms. These are designed to manage any API failures providing informative error messages.

Information Collection:

It is vital to the user that the information extracted is valid and up to date. Ensuring that the tool extracts this information proves that the tool will be reliable and that the results will be accurate at the time of search.

Export/Copy Feature:

Another feature is the Export Button, designed for both user convenience and efficiency. With a single click, users can initiate data transfer, eliminating the need for complex procedures. To accommodate diverse data needs, the tool offers export options in formats two formats: CSV and txt. Upon successful export, a confirmation message appears, giving users the option to view or download the file. If an error occurs, a detailed message is generated to assist with troubleshooting.

Non-Core Deliverables

Broaden Search Horizons:

One feature that I would like to add is the ability to expand the search to various other sites. Although Virus Total and Abused IPDB are widely used in the industry for investigations, it will benefit the user greatly if there are more results to get a better understanding.

Produce Full Report:

Another feature I would like to integrate into the Auto OSINT tool is providing the user with the option to 'Produce a full report'. This option will provide the user with a comprehensive search of an IP or hash and report its findings. The key area I would have to ensure is correct is the authenticity of the information if a full report was selected. Verifying that the information is correct is the utmost importance.

Integration into other Browsers:

If time was not an issue, I would like to incorporate my tool into another browser such as Firefox. As stated earlier in this document, Google Chrome was the most popular browser, so it made sense to cater the creation of my tool to it.

Use Case Diagram

Use cases diagrams are used in system development to describe how a user uses and interacts with a system in real world examples. Use cases generally consist of an 'actor' which represents the user, the use case name which refers to the action the user can take while using the software. Below is a use case diagram showcasing the different actions a user can take against my Auto OSINT tool.

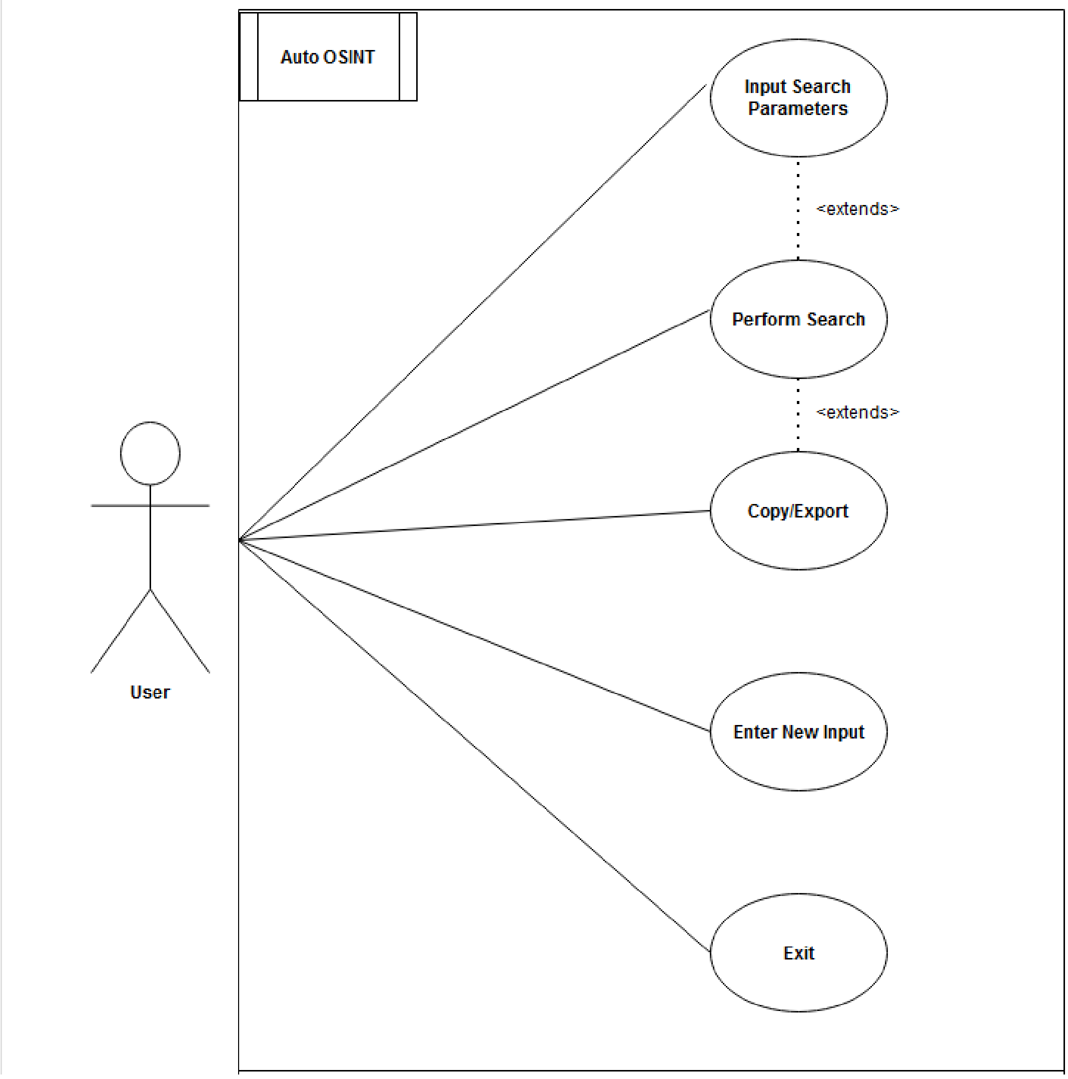


Figure 1 - Use Case Diagram

Use Cases

These describe how a person uses and interacts with the software or product to accomplish a task. The use cases below show each step a user takes when using the tool.

Input Search Parameters

Use case 1 highlights the first function that the user encounters, they are required to enter input to progress to the next function the tool provides.

Use Case 1	Input Search Parameters
Description	User enters search parameters.
Actor	User

Perform Search

Use case 2 provides us with the next step after the user inputs search parameters. This is where the search is set by the user. They can select here as to which OSINT site they want results from.

Use Case 2	Perform Search
Description	User clicks submit button to perform search
Actor	User
Trigger	User clicking submit
Precondition	User has entered search parameters

Copy/Export

Use case 3 is where the user has already performed a search and has results displayed back to the screen. They can decide to export or copy the results here.

Use Case 3	Copy/Export
Description	User copies or exports the results to txt or csv file
Actor	User
Trigger	User utilises the copy/export feature
Precondition	User has performed a search

Enter New Input

This is where the user can enter a new input if desired after they have performed an initial search.

Use Case 3	Enter New Input
Description	User copies or exports the results to txt or csv file
Actor	User
Trigger	User enters new search after initial search
Precondition	User has performed initial search

Example GUI's

Before a search

This is my idea on how the GUI could look before the user submits their search parameters. This is the screen that will greet users on start-up.

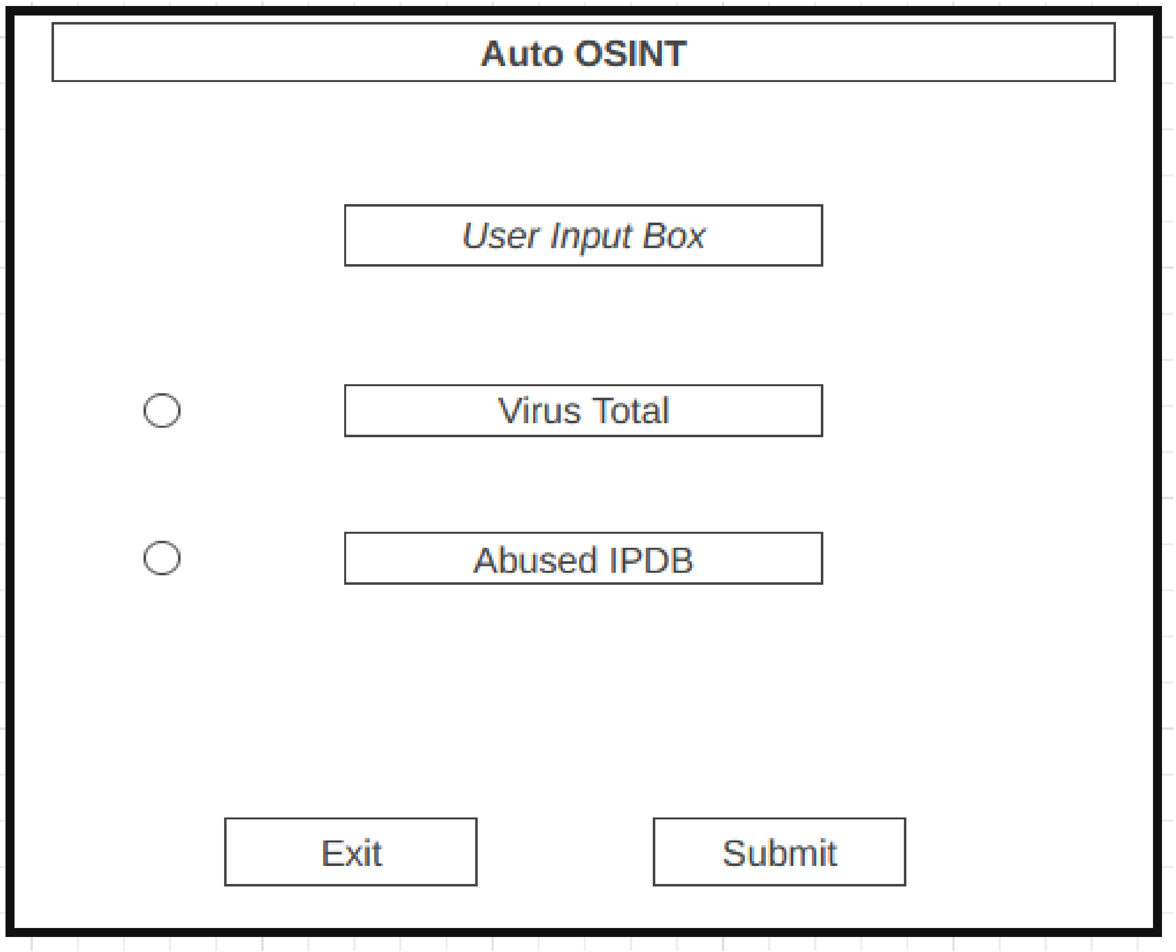
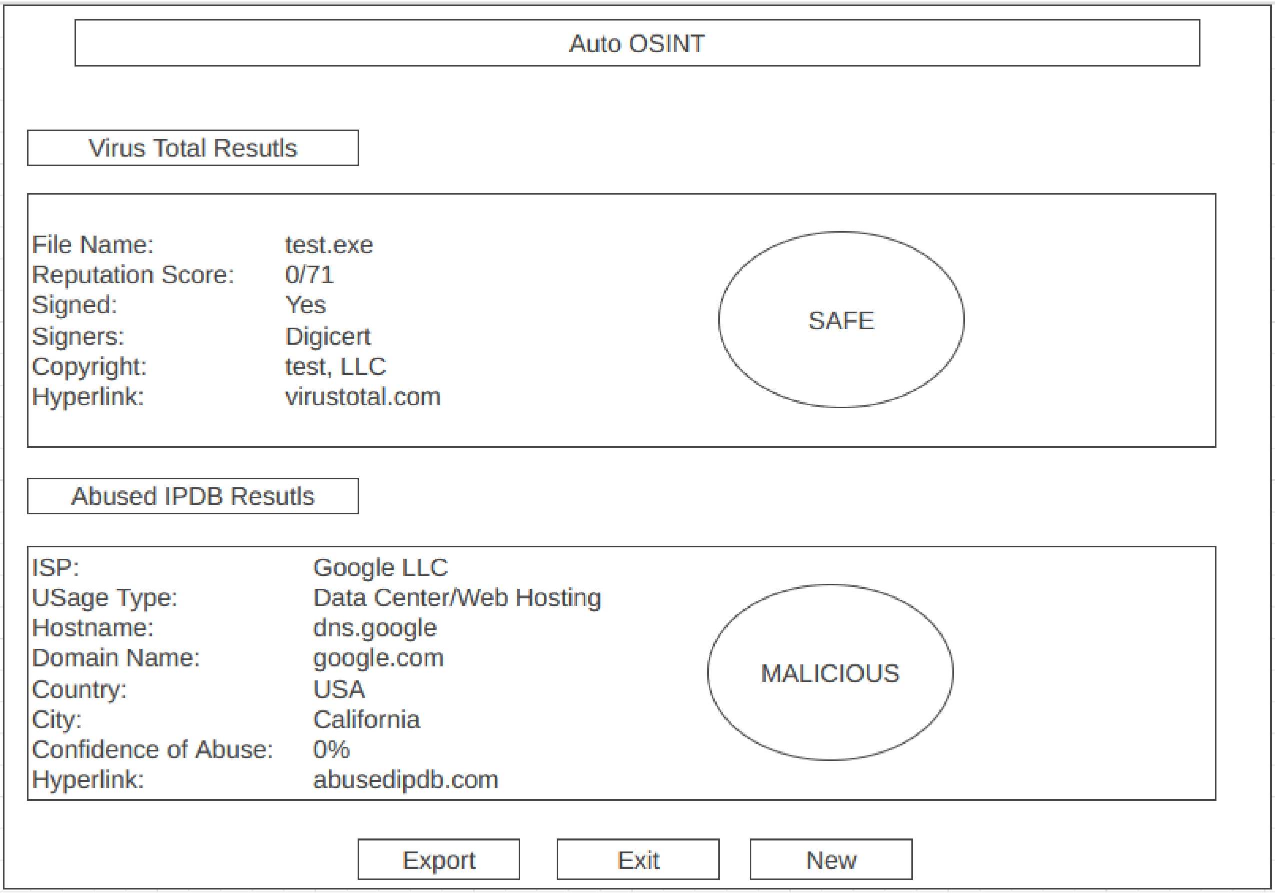


Figure 2- Sample GUI before user search is performed.

After a search

The following shows how the GUI will be displayed after the user has performed a search, As you can see, only the most important information is displayed at this stage and the export feature has been added.



File Name:	test.exe
Reputation Score:	0/71
Signed:	Yes
Signers:	Digicert
Copyright:	test, LLC
Hyperlink:	virustotal.com

ISP:	Google LLC
USage Type:	Data Center/Web Hosting
Hostname:	dns.google
Domain Name:	google.com
Country:	USA
City:	California
Confidence of Abuse:	0%
Hyperlink:	abusedipdb.com

Figure 3- GUI after user has performed search.

Dataflow Diagrams

Below I have included two data flow diagrams relating to the Auto OSINT tool. They show how the tool works and what occurs underneath the user interface that the user cannot see.

Dataflow diagram 1 shows how the tool communicates with the OSINT sites and shows how the data flows from start to finish when a user is utilising the tool.

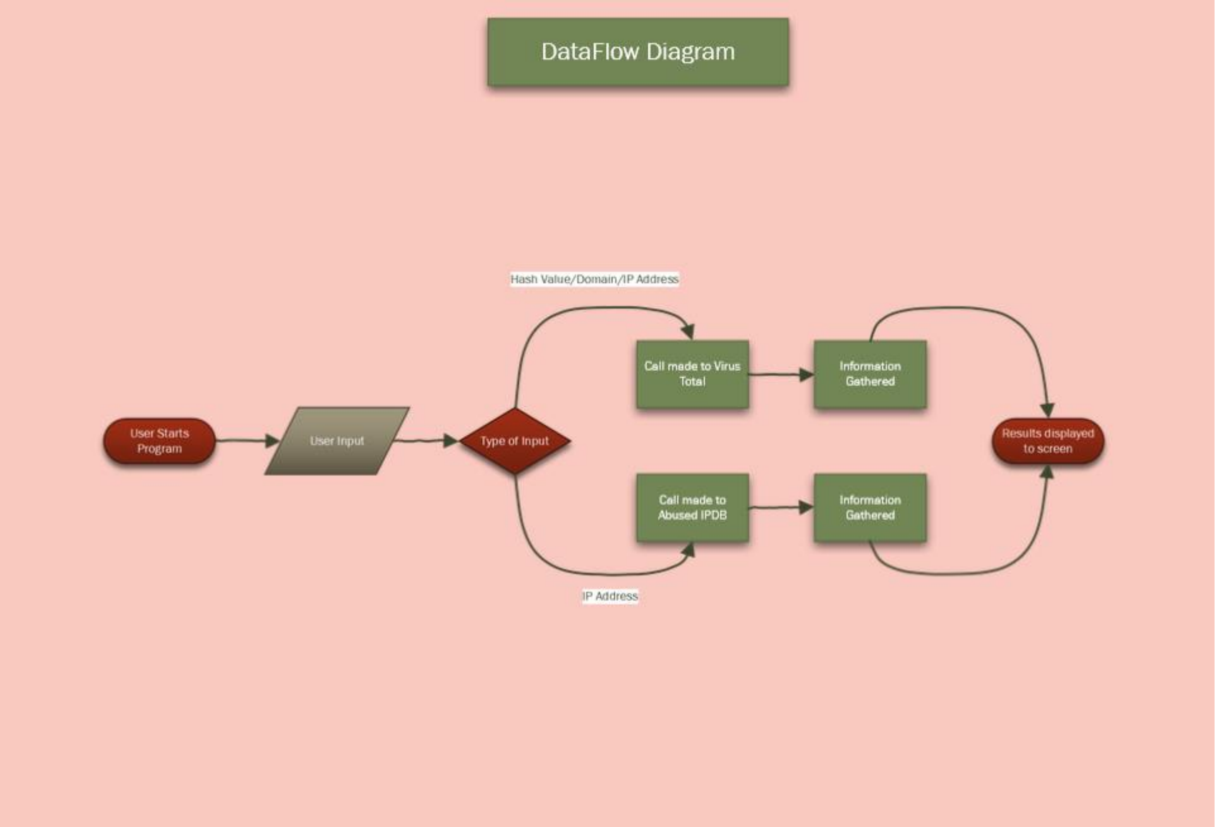
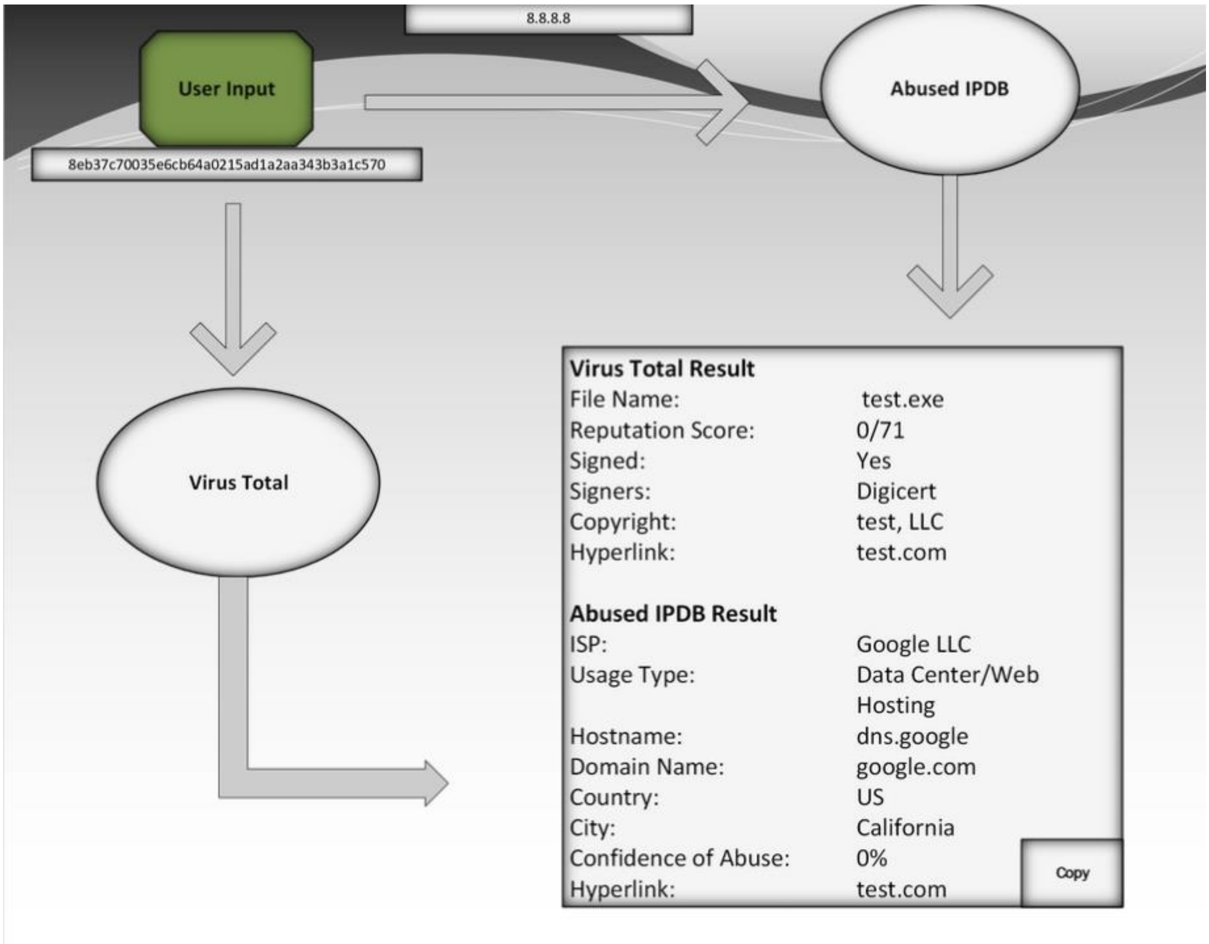


Figure 4 - Dataflow Diagram 1

Dataflow Diagram 2 shows how the tool operates when a user enters an IP address or a hash and where it communicates with the OSINT sites and how it displays the results back to the user.



Virus Total Result

File Name:	test.exe
Reputation Score:	0/71
Signed:	Yes
Signers:	Digicert
Copyright:	test, LLC
Hyperlink:	test.com

Abused IPDB Result

ISP:	Google LLC
Usage Type:	Data Center/Web Hosting
Hostname:	dns.google
Domain Name:	google.com
Country:	US
City:	California
Confidence of Abuse:	0%
Hyperlink:	test.com

Figure 5 - Dataflow Diagram 2

Non-Functional Requirements

Non function requirements are requirements that specifies the desired functionality, usability, reliability, performance, security, and scalability. These focus on how the system should work and its overall behaviour rather than the specific functions or features. Below are the non-functional requirements of the Auto OSINT tool.

Functionality

- The tool should be able to retrieve information from the relevant OSINT sites and display the results back to the user in a neat fashion.
- The tool should be capable to producing a report for the user when the user clicks the export button.

Usability

- The user interface should be intuitive and easy to understand. It should have a clean and uncluttered display that allows users of all technical levels to navigate without hesitation and use the tool to its full extent.

Reliability

- The tool should perform all the tasks it was designed or intended to do.
- Only reliable information should be obtained and displayed to the user.

Performance

- The tool should perform its tasks in a timely manner and not leave the user waiting for long periods of time.

Security

- The tool should be able to protect against unauthorised strings and characters to prevent any kind of attacks.

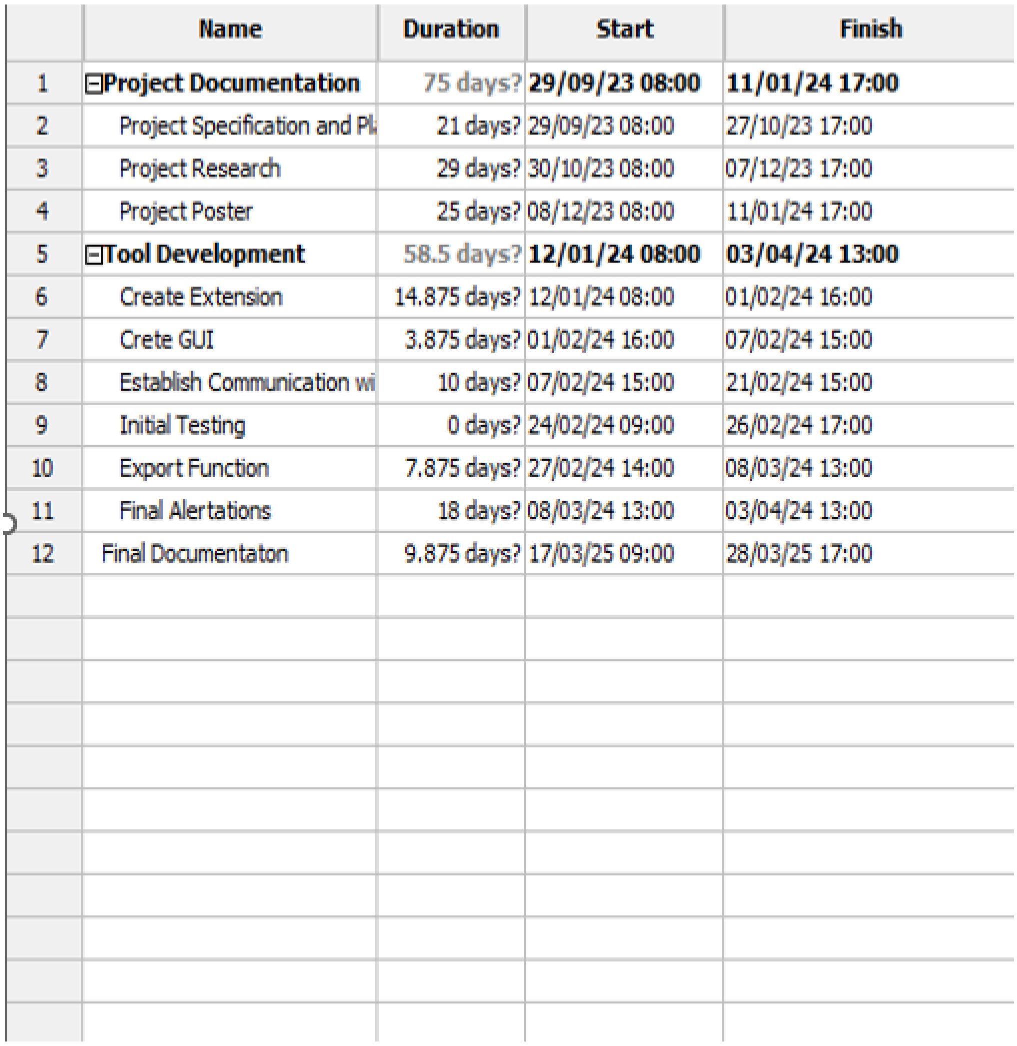
Supportability

- The tool will be supported for use on all Google Chrome browsers.

Project Plan

GANTT Chart

Below I have included a GANTT chart which shows approximate dates that I have set out for myself to have each of my functions set up and running. These are not final date and are open to change as I may run in to problems in some areas.



	Name	Duration	Start	Finish
1	**⊟Project Documentation**	75 days?	**29/09/23 08:00**	**11/01/24 17:00**
2	Project Specification and Pl	21 days?	29/09/23 08:00	27/10/23 17:00
3	Project Research	29 days?	30/10/23 08:00	07/12/23 17:00
4	Project Poster	25 days?	08/12/23 08:00	11/01/24 17:00
5	**⊟Tool Development**	58.5 days?	**12/01/24 08:00**	**03/04/24 13:00**
6	Create Extension	14.875 days?	12/01/24 08:00	01/02/24 16:00
7	Crete GUI	3.875 days?	01/02/24 16:00	07/02/24 15:00
8	Establish Communication wi	10 days?	07/02/24 15:00	21/02/24 15:00
9	Initial Testing	0 days?	24/02/24 09:00	26/02/24 17:00
10	Export Function	7.875 days?	27/02/24 14:00	08/03/24 13:00
11	Final Alertations	18 days?	08/03/24 13:00	03/04/24 13:00
12	Final Documentaton	9.875 days?	17/03/25 09:00	28/03/25 17:00

Figure 6 - Part 1 of GANTT chart showcasing important dates.

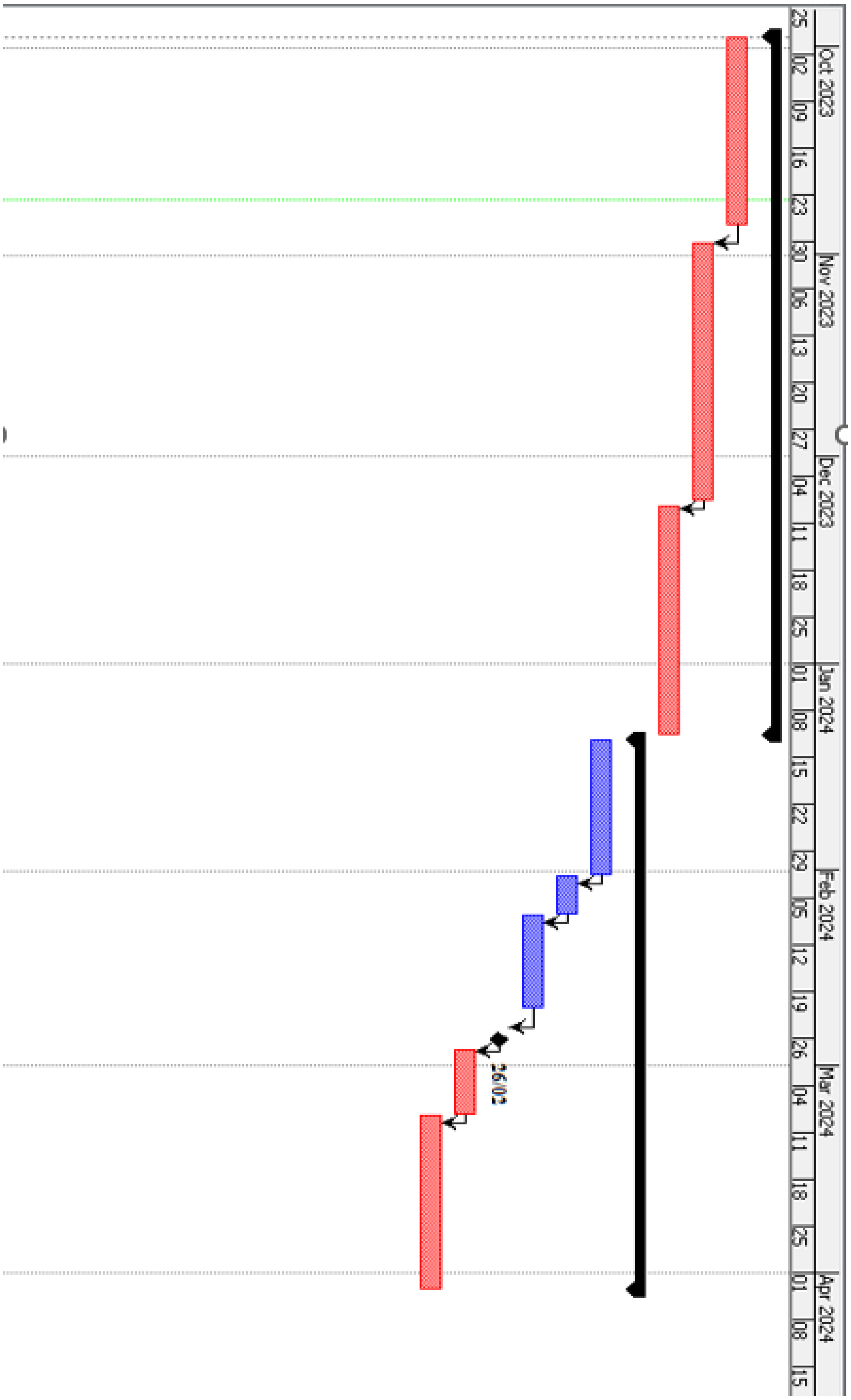


Figure 7 - Part 2 of GANTT chart.

Table of Figures

Figure 1 - Use Case Diagram 6
Figure 2- Sample GUI before user search is performed.......... 8
Figure 3- GUI after user has performed search. 9
Figure 4 - Dataflow Diagram 1 10
Figure 5 - Dataflow Diagram 2 11
Figure 6 - Part 1 of GANTT chart showcasing important dates. 13
Figure 7 - Part 2 of GANTT chart. 14

References

- Statista. (n.d.). *Most popular internet browser versions 2020*. [online] Available at: https://www.statista.com/statistics/268299/most-popular-internet-browsers/.

- Facebook, Twitter and LinkedIn (n.d.). *What Is an IP Address & What Are the Different Kinds of IP Addresses?* [online] Lifewire. Available at: https://www.lifewire.com/what-is-an-ip-address-2625920.

- Trendmicro.com. (2019). *Hash values - Definition - Trend Micro USA*. [online] Available at: https://www.trendmicro.com/vinfo/us/security/definition/hash-values.

- crowdstrike.co.uk. (n.d.). *FAQ: Falcon Prevent | Free Trial, Pricing, & More | CrowdStrike*. [online] Available at: https://www.crowdstrike.co.uk/products/endpoint-security/falcon-prevent-antivirus/faq/.

- Daly, N. (2022). *What Is a Use Case & How To Write One | Wrike*. [online] www.wrike.com. Available at: https://www.wrike.com/blog/what-is-a-use-case/.

- Scaled Agile Framework. (n.d.). *Nonfunctional Requirements*. [online] Available at: https://v5.scaledagileframework.com/nonfunctional-requirements/