Augury

User Guide

Team 07

Kaila Bryant

Ian Chorne

Nahod Habte

Liam Ison

Garrett McGuire

Date: (04/27/2025)

Department: CCSWE

Course: SWE 4724

Professor: Yan Huang

**Augury – IOC Intelligence**

***User Manual***

**Please refer to the project’s README if you need help getting the app running.  
Below is a guide for day-to-day use once everything is up and listening on its default ports.**

**1. What is Augury?**

Augury is a lightweight analyst console that:

1. Extracts Indicators of Compromise (IOCs) from free-form text.
2. Queries **Count FAKEula** (or your own tooling) for asset data, security logs, OIL (Observed-Indicator-List) sources, netflow, etc.
3. Displays everything in a tables with multiples tabs allowed for multiple searches.

**2. Performing Your First Search**

1. Paste *anything* containing IOCs (IPs, domains, hashes, URLs…) into the search bar.
2. Press **Enter** or click the search icon.
3. Augury will create a new **tab** named after the first IOC it extracted, pull back all related data, and render it in the **Table**.

**3. Working with Tabs**

1. To switch tabs click the tab you wish to go to.
2. If a new query is the same as a previous query it will just refresh that tab.
3. If a new query uses the same ioc as the tabs name it will append “(2)”, ”(3)”…
4. To close a tab click the “X” next to the tab name.

**4. Using the Table and it’s Links**

1. Every populated field can be copied, but many cells are **live links** that help you pivot into other tools or raw data:

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| | **Cell / Column** | **Destination** | **What you get** | | --- | --- | --- | |  |  |  | | **Look-Ups** quick list | Shodan, Censys, Spur, IP2Proxy, BGP View | Third Party links for that IOC. | | **CBR** | Carbon Black Response | Static & dynamic analysis plus host prevalence. | | **PDNS** | PDNSQuery | All PDNS data available on the API | | **GeoIP** | GeoIPQuery | Geographical data available on the API | | **LDAP** | Active Directiry Lookup | LDAP data available on the API | | **Binary** | **Carbon Black Response** binary page | CBR data associated with the binary hash provided | | **Security Log ▶ View OIL** | Security Logs found in OIL | Full event with surrounding context and JSON breadcrumbs. | |

1. Links will always open a new browser tab to ensure Augery workspace remains intact.

**5. Troubleshooting**

| **Symptom** | **Check** |
| --- | --- |
| **“Failed to fetch” in frontend** | **Backend not running, wrong port, or CORS header missing.** |
| **Blank table** | **Parser received an empty data[]; validate FAKEula response.** |
| **CORS pre-flight blocked** | **Backend must return Access-Control-Allow-Headers: \*.** |