CertStream User Guide

Welcome to CertStream! Choose a section from the table of contents below to find step-by-step guides on how to use CertStream.

Table of Contents

Introduction to CertStream

CertStream is an easy-to-deploy Python Script designed for Cybersecurity Researchers. It seamlessly captures newly-registered domains that matches your capture regexes.

The CertStream User Guide acquaints you with the application's functionality, enabling you to maximize its potential.

Key Features:

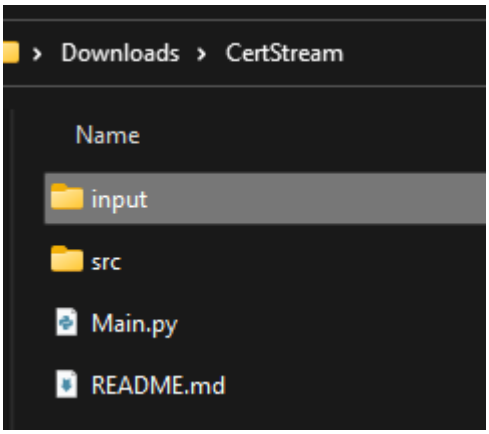
- Retrieve domains from Certificate Transparency's vast network of monitors.
- Filters for domains of interest with one or more capture regexes.
- Integrates seamlessly with Group IB's Digital Risk Protection Tools.
- Stores domains of interest into a SQLite database.

> 💡 CertStream only requires one command to start. CertStream is user-friendly!

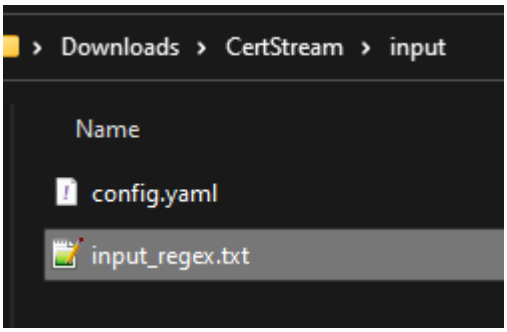
We are confident that CertStream will enhance your efficiency as Cybersecurity Researchers. Enjoy your experience with CertStream! 😀

Quick Start

1. Download `CertStream.zip` here, and extract `CertStream.zip` to any folder.



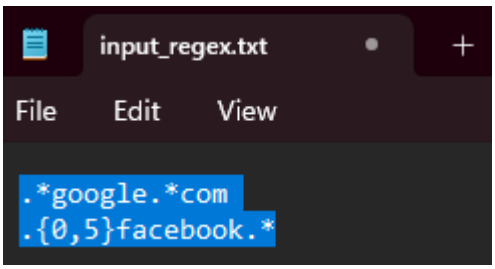
2. Open the `/input` folder, and edit `input_regex.txt` using any text editor.



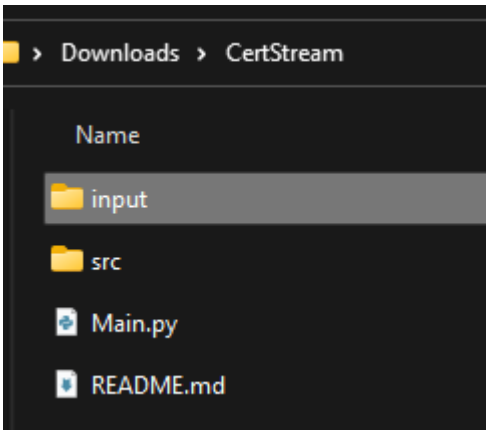
3. Add one or more regexes for CertStream to monitor, and save the file.

   CertStream will capture domains that matches any of the regexes.

   (e.g. The domain `google123.com` will be captured using the regexes below.)

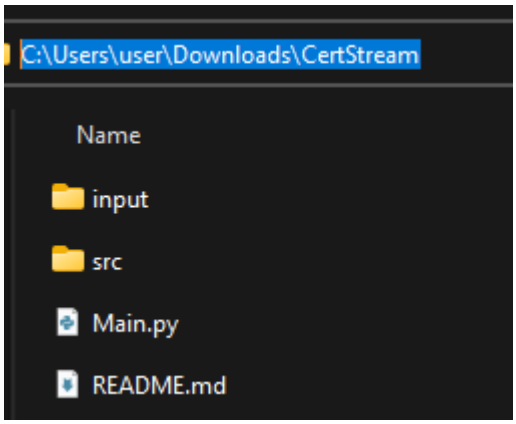


4. Navigate back to the previous folder.

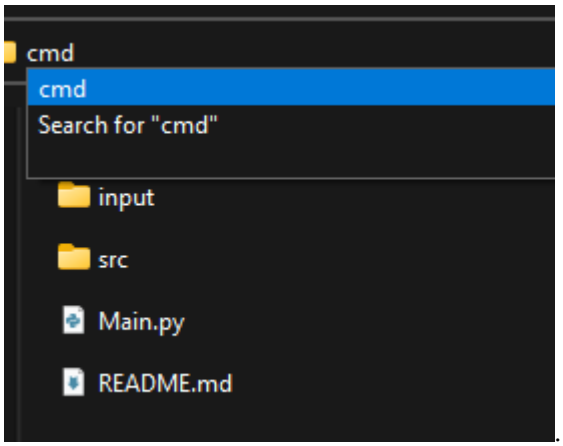


5. Open Command Prompt/Terminal on the home folder. For Windows users, follow the instructions below.

    1. Click on the address bar.



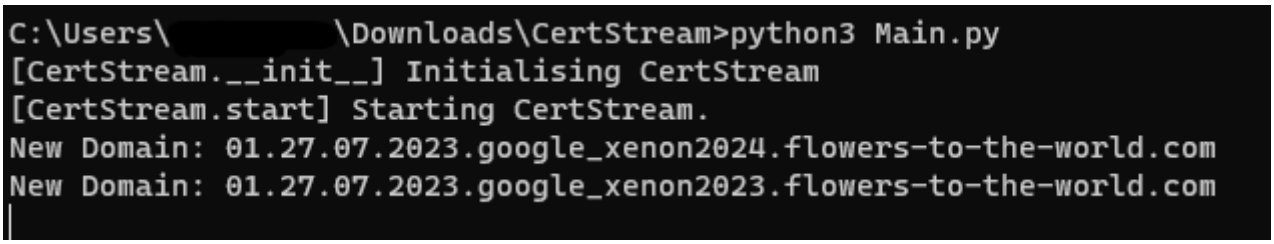
3. Type `cmd`, and press `Enter` to launch Command Prompt.



6. Copy each command below, and press `Enter` to start CertStream.

   CertStream will run indefinitely.

```
python3 -m pip install -r src/requirements.txt
python3 Main.py
```



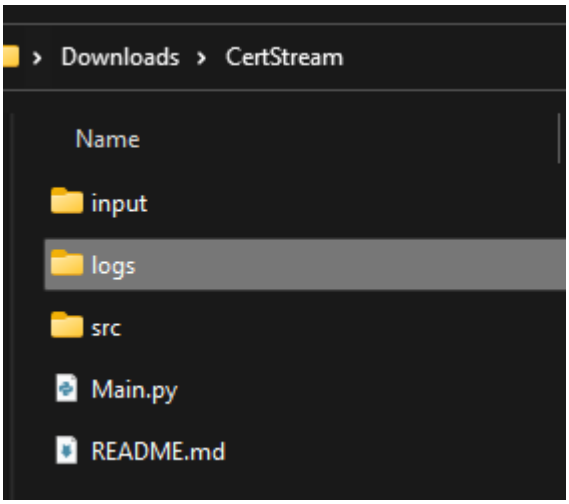
7. To stop CertStream, press CTRL+C (You may need to press a few times).

   Domains captured is exported to an output file.

> More time is needed for export when the number of domains stored is large.

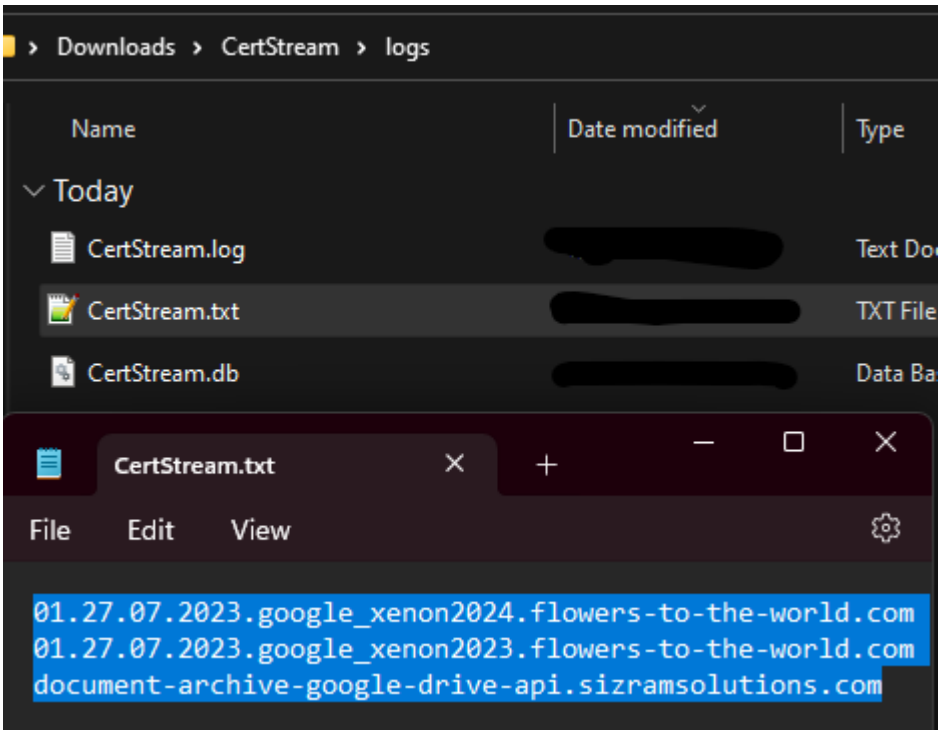
```
C:\Users\[redacted]\Downloads\CertStream>python3 Main.py
[CertStream.__init__] Initialising CertStream
[CertStream.start] Starting CertStream.
New Domain: 01.27.07.2023.google_xenon2024.flowers-to-the-world.com
New Domain: 01.27.07.2023.google_xenon2023.flowers-to-the-world.com
New Domain: 01.27.07.2023.google_xenon2023.flowers-to-the-world.com
New Domain: document-archive-google-drive-api.sizramsolutions.com
Listening Stopped. Please wait for the export.
CertStream Shutdown.

C:\Users\[redacted]\Downloads\CertStream>
```

8. Open the new `/logs` folder.



You will find the `CertStream.txt` output file.

9. Open `CertStream.txt` to view the captured domains.



Feedback

CertStream is a pilot program. Any feedback is appreciated while we develop CertStream. To deposit ideas and comments, create a new Issue on Github!

Authors

This User Guide is written by Choon Yong.