TAXII-STIX-APP

INTRODUCTION :

This web application fetches Threat Intelligence data from Open sources like HailATaxii through TAXII-Protocol. Taxii-Protocol uses Stix format to share the data. Stix is the format used by the Threat Intelligence sources to store and share information. Stix is widely accepted format for Threat Intelligence.

The data is requested through POST method to their respective endpoints and is in the form of raw XML format. The data is processed and converted to JSON format. This JSON data is then stored into a local database for further data processing, here we are using MapDB memory database. This data is stored in primary memory of the system in a structured HashMap.

The data consists of compromised IPs, Domains and URLs along with information on them. These are then categorised separately and stored in database with indexes as IP, Domain and URL. This data can be fetched from database when needed, once the data is stored in MapDB we need not to fetch again from open sources web.

To start the web app,

1. Build the project with Maven. War file is created in

   ```
   /out/arifact/"artifactname"/"artifactname".war
   ```

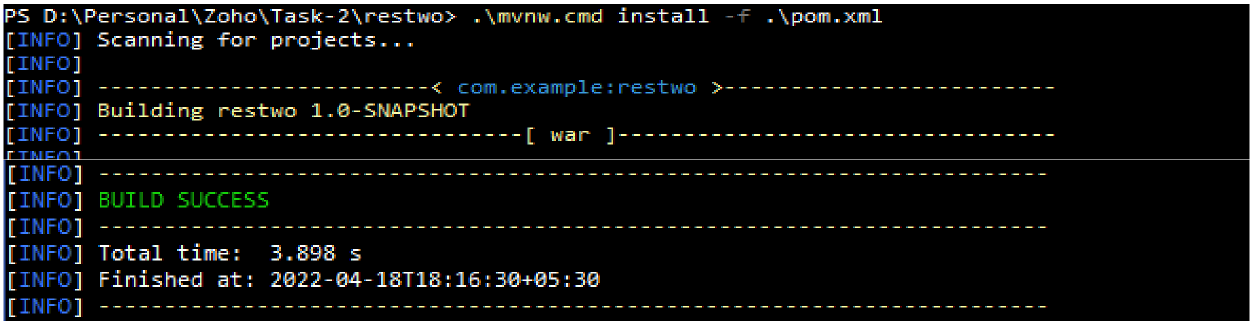
2. Copy the war file into Tomcat webapps folder

   ```
   %CATALINE_HOME%/webapps/
   ```

3. Start the Tomcat server. Startup script is in bin/ directory
   - `startup.bat` : for Windows
   - `startup.sh` : for Linux
4. Goto localhost:8080/"artifactname"/
5. End Points :
   - `api/url` : to fetch urls
   - `api/domain` : to fetch domains
   - `api/ip` : to fetch ips

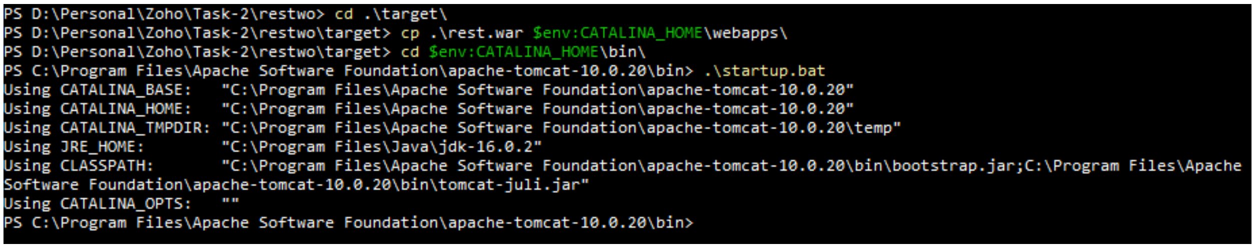
WORKING :

- Build the project to extract war file.



```
PS D:\Personal\Zoho\Task-2\restwo> .\mvnw.cmd install -f .\pom.xml
[INFO] Scanning for projects...
[INFO]
[INFO] --------------------------< com.example:restwo >--------------------------
[INFO] Building restwo 1.0-SNAPSHOT
[INFO] ----------------------------------[ war ]----------------------------------
[INFO]
[INFO] ------------------------------------------------------------------------
[INFO] BUILD SUCCESS
[INFO] ------------------------------------------------------------------------
[INFO] Total time:  3.898 s
[INFO] Finished at: 2022-04-18T18:16:30+05:30
[INFO] ------------------------------------------------------------------------
```

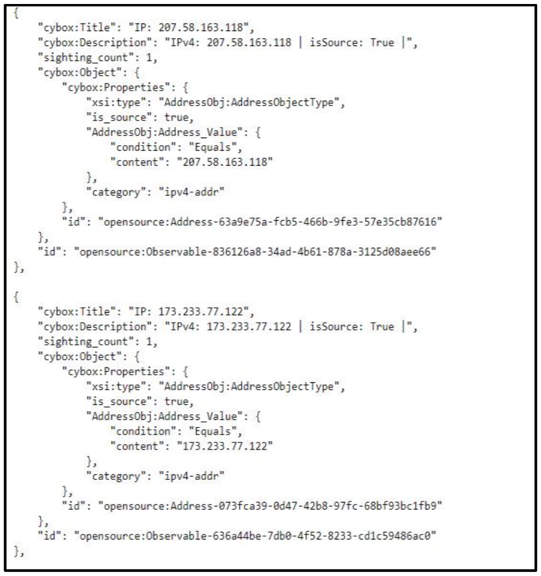
- target folder is created with war file in it. cd into target/ .
- copy the war file into $CATALINE_HOME/webapps/ directory.
- cd into $CATALINA_HOME/bin/ and start the TOMEE server by running the script startup.bat file.
- Loading data takes some time, after data is fetched it can be accessed from website.



```
PS D:\Personal\Zoho\Task-2\restwo> cd .\target\
PS D:\Personal\Zoho\Task-2\restwo\target> cp .\rest.war $env:CATALINA_HOME\webapps\
PS D:\Personal\Zoho\Task-2\restwo\target> cd $env:CATALINA_HOME\bin\
PS C:\Program Files\Apache Software Foundation\apache-tomcat-10.0.20\bin> .\startup.bat
Using CATALINA_BASE:   "C:\Program Files\Apache Software Foundation\apache-tomcat-10.0.20"
Using CATALINA_HOME:   "C:\Program Files\Apache Software Foundation\apache-tomcat-10.0.20"
Using CATALINA_TMPDIR: "C:\Program Files\Apache Software Foundation\apache-tomcat-10.0.20\temp"
Using JRE_HOME:        "C:\Program Files\Java\jdk-16.0.2"
Using CLASSPATH:       "C:\Program Files\Apache Software Foundation\apache-tomcat-10.0.20\bin\bootstrap.jar;C:\Program Files\Apache Software Foundation\apache-tomcat-10.0.20\bin\tomcat-juli.jar"
Using CATALINA_OPTS:   ""
PS C:\Program Files\Apache Software Foundation\apache-tomcat-10.0.20\bin>
```

- Go to http://localhost:8080/"filename". Homepage appears.

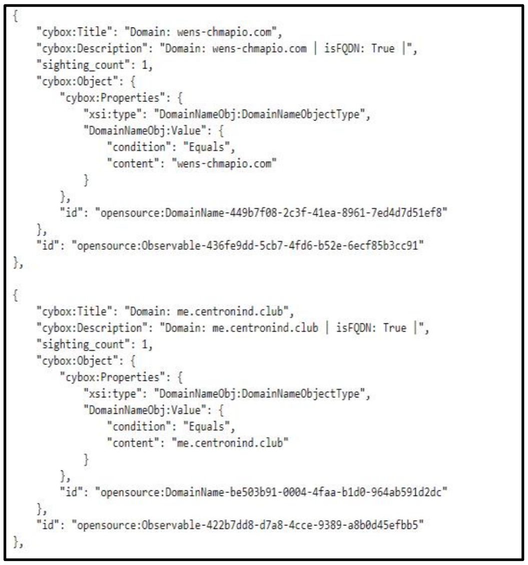
End Points :



```
{
    "cybox:Title": "IP: 207.58.163.118",
    "cybox:Description": "IPv4: 207.58.163.118 | isSource: True |",
    "sighting_count": 1,
    "cybox:Object": {
        "cybox:Properties": {
            "xsi:type": "AddressObj:AddressObjectType",
            "is_source": true,
            "AddressObj:Address_Value": {
                "condition": "Equals",
                "content": "207.58.163.118"
            },
            "category": "ipv4-addr"
        },
        "id": "opensource:Address-63a9e75a-fcb5-466b-9fe3-57e35cb87616"
    },
    "id": "opensource:Observable-836126a8-34ad-4b61-878a-3125d08aee66"
},

{
    "cybox:Title": "IP: 173.233.77.122",
    "cybox:Description": "IPv4: 173.233.77.122 | isSource: True |",
    "sighting_count": 1,
    "cybox:Object": {
        "cybox:Properties": {
            "xsi:type": "AddressObj:AddressObjectType",
            "is_source": true,
            "AddressObj:Address_Value": {
                "condition": "Equals",
                "content": "173.233.77.122"
            },
            "category": "ipv4-addr"
        },
        "id": "opensource:Address-073fca39-0d47-42b8-97fc-68bf93bc1fb9"
    },
    "id": "opensource:Observable-636a44be-7db0-4f52-8233-cd1c59486ac0"
},
```

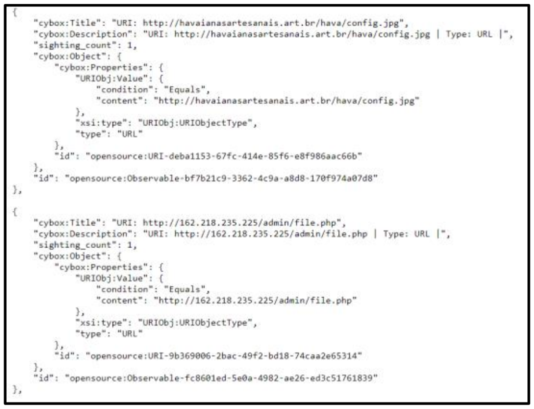
IP



```
{
    "cybox:Title": "Domain: wens-chmapio.com",
    "cybox:Description": "Domain: wens-chmapio.com | isFQDN: True |",
    "sighting_count": 1,
    "cybox:Object": {
        "cybox:Properties": {
            "xsi:type": "DomainNameObj:DomainNameObjectType",
            "DomainNameObj:Value": {
                "condition": "Equals",
                "content": "wens-chmapio.com"
            }
        },
        "id": "opensource:DomainName-449b7f08-2c3f-41ea-8961-7ed4d7d51ef8"
    },
    "id": "opensource:Observable-436fe9dd-5cb7-4fd6-b52e-6ecf85b3cc91"
},

{
    "cybox:Title": "Domain: me.centronind.club",
    "cybox:Description": "Domain: me.centronind.club | isFQDN: True |",
    "sighting_count": 1,
    "cybox:Object": {
        "cybox:Properties": {
            "xsi:type": "DomainNameObj:DomainNameObjectType",
            "DomainNameObj:Value": {
                "condition": "Equals",
                "content": "me.centronind.club"
            }
        },
        "id": "opensource:DomainName-be503b91-0004-4faa-b1d0-964ab591d2dc"
    },
    "id": "opensource:Observable-422b7dd8-d7a8-4cce-9389-a8b0d45efbb5"
},
```

Domain

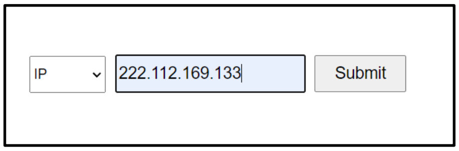


```
{
    "cybox:Title": "URI: http://havaianasartesanais.art.br/hava/config.jpg",
    "cybox:Description": "URI: http://havaianasartesanais.art.br/hava/config.jpg | Type: URL |",
    "sighting_count": 1,
    "cybox:Object": {
        "cybox:Properties": {
            "URIObj:Value": {
                "condition": "Equals",
                "content": "http://havaianasartesanais.art.br/hava/config.jpg"
            },
            "xsi:type": "URIObj:URIObjectType",
            "type": "URL"
        },
        "id": "opensource:URI-deba1153-67fc-414e-85f6-e8f986aac66b"
    },
    "id": "opensource:Observable-bf7b21c9-3362-4c9a-a8d8-170f974a07d8"
},

{
    "cybox:Title": "URI: http://162.218.235.225/admin/file.php",
    "cybox:Description": "URI: http://162.218.235.225/admin/file.php | Type: URL |",
    "sighting_count": 1,
    "cybox:Object": {
        "cybox:Properties": {
            "URIObj:Value": {
                "condition": "Equals",
                "content": "http://162.218.235.225/admin/file.php"
            },
            "xsi:type": "URIObj:URIObjectType",
            "type": "URL"
        },
        "id": "opensource:URI-9b369006-2bac-49f2-bd18-74caa2e65314"
    },
    "id": "opensource:Observable-fc8601ed-5e0a-4982-ae26-ed3c51761839"
},
```

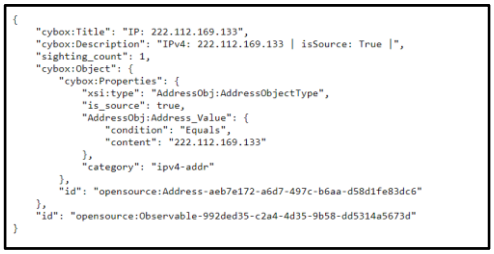
URL

Search



IP 222.112.169.133

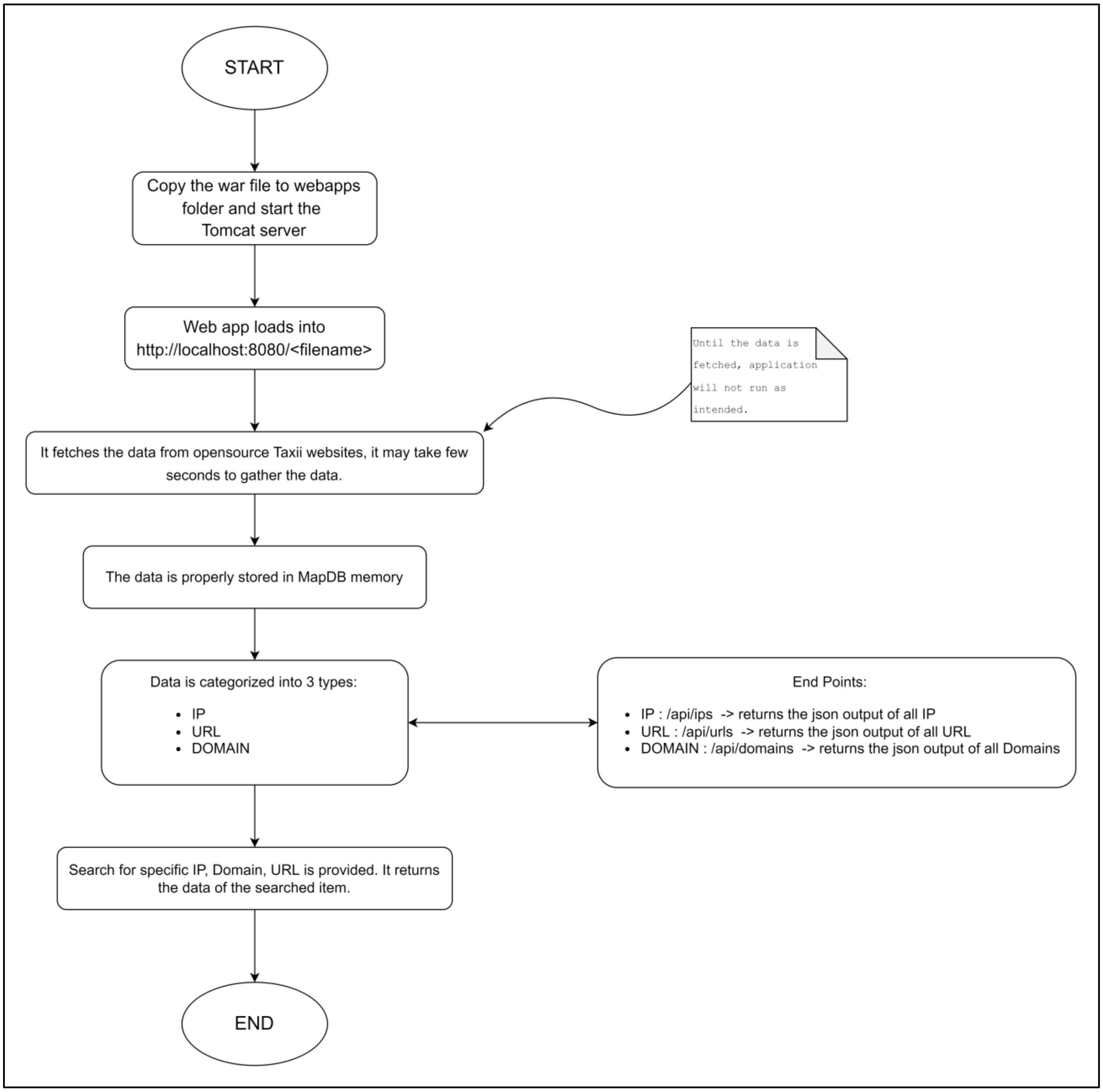
search



```
{
    "cybox:Title": "IP: 222.112.169.133",
    "cybox:Description": "IPv4: 222.112.169.133 | isSource: True |",
    "sighting_count": 1,
    "cybox:Object": {
        "cybox:Properties": {
            "xsi:type": "AddressObj:AddressObjectType",
            "is_source": true,
            "AddressObj:Address_Value": {
                "condition": "Equals",
                "content": "222.112.169.133"
            },
            "category": "ipv4-addr"
        },
        "id": "opensource:Address-aeb7e172-a6d7-497c-b6aa-d58d1fe83dc6"
    },
    "id": "opensource:Observable-992ded35-c2a4-4d35-9b58-dd5314a5673d"
}
```

result

Flow Chart :


START
Copy the war file to webapps folder and start the Tomcat server
Web app loads into http://localhost:8080/<filename>
Until the data is fetched, application will not run as intended.
It fetches the data from opensource Taxii websites, it may take few seconds to gather the data.
The data is properly stored in MapDB memory
Data is categorized into 3 types:
• IP
• URL
• DOMAIN
End Points:
• IP : /api/ips -> returns the json output of all IP
• URL : /api/urls -> returns the json output of all URL
• DOMAIN : /api/domains -> returns the json output of all Domains
Search for specific IP, Domain, URL is provided. It returns the data of the searched item.
END