# RALAYALA SEEMA UNIVERSITY KURNOOL SRI SANKARS DEGREE COLLEGE IN KURNOOL

A.Shaikshavali
Bsc microbiology
21367008001

# Project title:driven information gathering threat intellignece

- **□** Team ID: LTVIP2024TMID14080
- Team Size: 5
- Team Leader: Akthar Shaik Shavali
- Team member: Boggula Mani Kumar
- □ Team member: Darur Rajesh
- □ Team member: Gollakatikala Manohar
- Team member: Kalagondla Yella Raju

## index

### SNO TOPICNAME PAGE NO

- Osnit frame work into source key points
- 2. Osnit frame work on the tools for for dns information gathering
- 3. Dns for maping source for ruk website detalis analysis
- 4. Ruk webste details report for tools
- 5. Srv details and txt for records on the ruk website
- 6. Osnit frame work analysis
- 7. Information source intellignce
- 8. Ibomma website details analysis web cheker and them analysis
- 9. Tls security for issuses site feature
- 10. Website into web cheker.com target domain 1tamil.mv

- 5
- · 6
- 7
- **8**
- · 9
- **□** 10
- **□** 11
- **12**
- **1**3
- 14-15

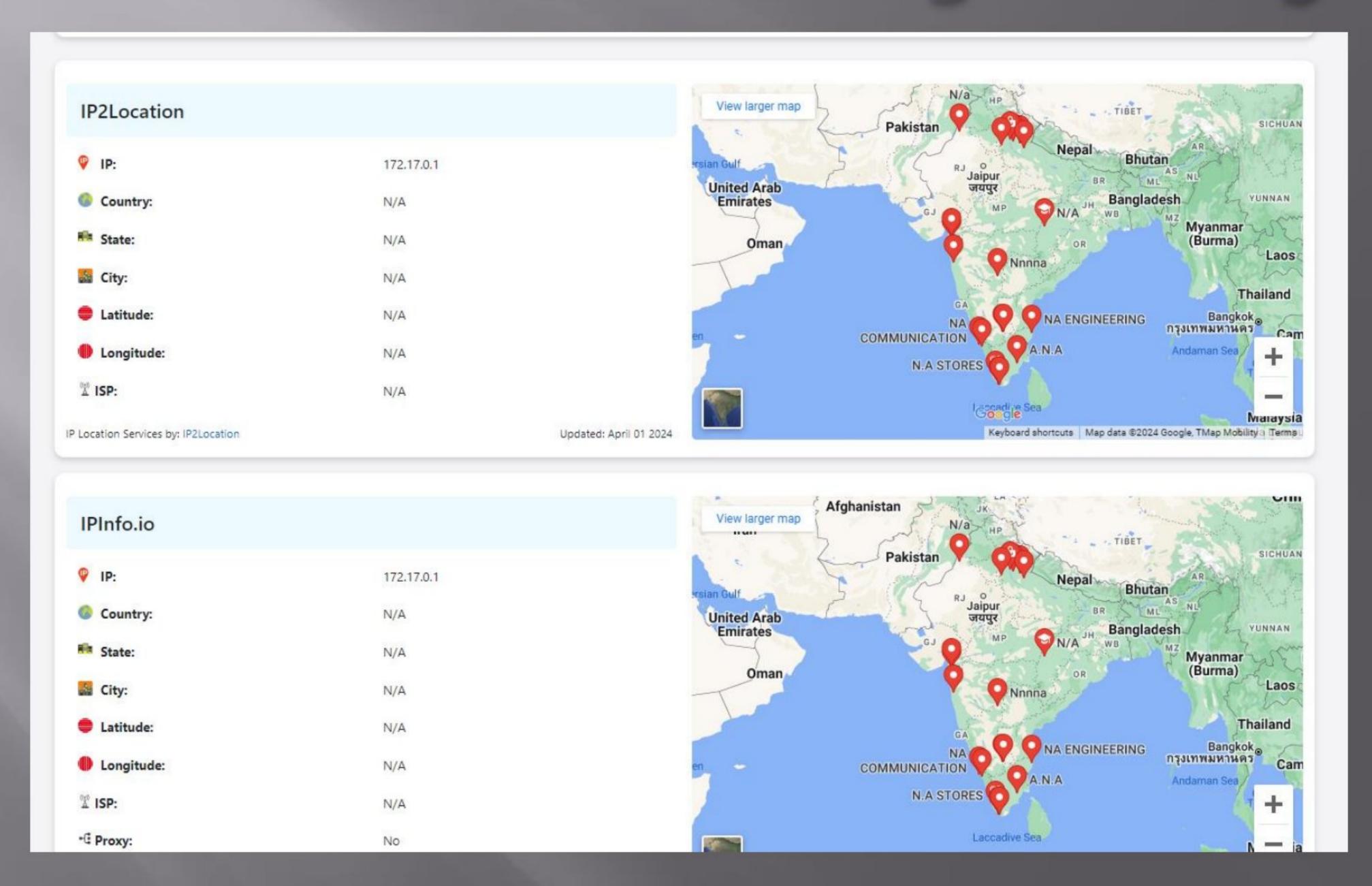
# DRIVEN INFORMATION GATHERING THREAT AND INTELLIGENCE

When we use osnit frame work on use service threat intelligence

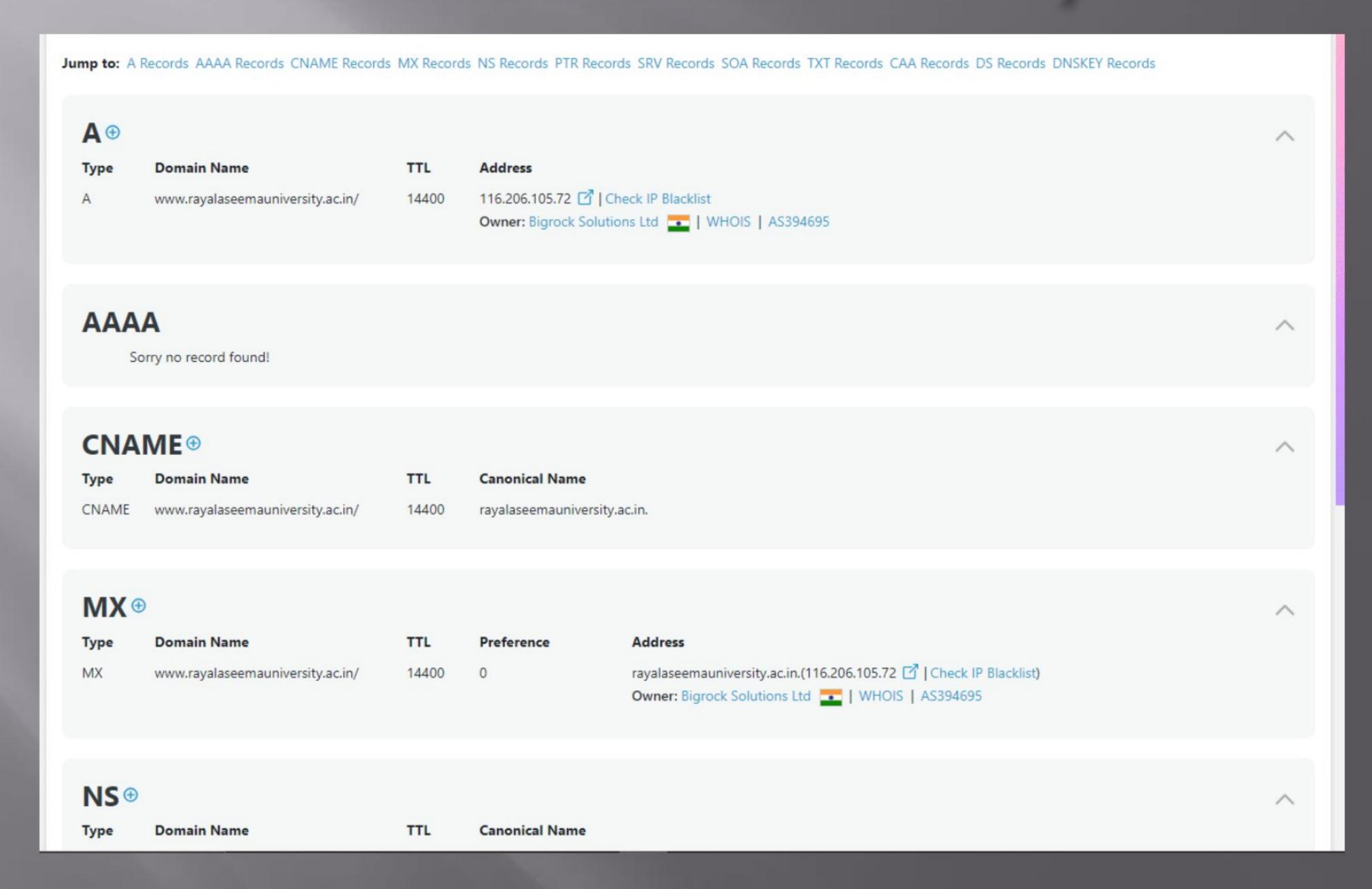
## Osnit frame work into source key points

- It seems like you're referring to the OSSTMM (Open Source Security Testing Methodology Manual) framework. Here are some key points about the OSSTMM framework:
- Comprehensive Methodology: OSSTMM is a comprehensive framework for security testing, providing guidelines, techniques, and methodologies for assessing the security posture of systems, networks, and applications.
- Open Source: As the name suggests, OSSTMM is an open-source framework, which means it is freely available for anyone to use, modify, and distribute.
- Risk-Based Approach: OSSTMM emphasizes a risk-based approach to security testing, focusing on identifying and prioritizing security risks based on their potential impact on the organization.
- Seven Sections: The OSSTMM framework is organized into seven main sections:
  - Information Security Foundation
  - Information Security Testing
  - Security Operations
  - Legalities
  - Data Destruction
  - Social Engineering
  - Tools
- Methodologies and Techniques: Within each section, OSSTMM provides detailed methodologies and techniques for conducting various types of security tests, including penetration testing, vulnerability assessment, security auditing, and social engineering assessments.

## Osnit frame work on the tools for dns information gathering



# Dns for maping source for ruk web site details analysis



## Ruk website into report for domain

#### MX Records

MX records for www.rayalaseemauniversity.ac.in:

Record	Туре	Priority	Target	TTL
rayalaseemauniversity.ac.in	MX	0	rayalaseemauniversity.ac.in.	14400

```
id 50240, opcode QUERY, rcode NOERROR, flags QR RD RA
;QUESTION
www.rayalaseemauniversity.ac.in. IN MX
; ANSWER
www.rayalaseemauniversity.ac.in. 14400 IN CNAME rayalaseemauniversity.ac.in.
rayalaseemauniversity.ac.in. 14400 IN MX 0 rayalaseemauniversity.ac.in.
; AUTHORITY
;ADDITIONAL
```

Show results globally →

#### **NS** Records

NS records for www.rayalaseemauniversity.ac.in:

Record	Type	Value	TTL
rayalaseemauniversity.ac.in	NS	ns2.cp-in-17.bigrockservers.com.	21600
rayalaseemauniversity.ac.in	NS	ns1.cp-in-17.bigrockservers.com.	21600

```
id 9613, opcode QUERY, rcode NOERROR, flags QR RD RA
;QUESTION
www.rayalaseemauniversity.ac.in. IN NS
; ANSWER
```

## Sry details and txt records on the ruk website

#### SRV Records

No SRV records found for www.rayalaseemauniversity.ac.in.

```
id 39154, opcode QUERY, rcode NOERROR, flags QR RD RA
;QUESTION
www.rayalaseemauniversity.ac.in. IN SRV
;ANSWER
www.rayalaseemauniversity.ac.in. 14400 IN CNAME rayalaseemauniversity.ac.in.
;AUTHORITY
rayalaseemauniversity.ac.in. 1800 IN SOA ns1.cp-in-17.bigrockservers.com. sales.bigrock.in. 2024022701 86400 7200 3600000 86400
;ADDITIONAL
```

Show results globally →

#### TXT Records

TXT records for www.rayalaseemauniversity.ac.in:

Record	Туре	Value	TTL
rayalaseemauniversity.ac.in	TXT	"v=spf1 ip4:116.206.105.72 +a +mx ~all"	14400

```
id 31031, opcode QUERY, rcode NOERROR, flags QR RD RA
;QUESTION
www.rayalaseemauniversity.ac.in. IN TXT
;ANSWER
www.rayalaseemauniversity.ac.in. 14400 IN CNAME rayalaseemauniversity.ac.in.
rayalaseemauniversity.ac.in. 14400 IN TXT "v=spf1 ip4:116.206.105.72 +a +mx ~all"
;AUTHORITY
;ADDITIONAL
```

Show results globally →

### Osnit frame work anaylsis for

#### Sources of Cyber Threat Intelligence

Cyber Threat Intelligence (CTI) refers to information gathered from collated data on present and potential threats. In order to gather information, there has to be sources to obtain them from. There are many sources of CTI and they can be categorised into one of the following:

#### Open-Source Intelligence (OSINT)

This refers to intelligence that has been made publicly available for use. This comprises of the resources found on the internet such as Social media (Facebook, Twitter, Instagram), Video sharing websites (YouTube) and other types of websites that provide information (Wikipedia, Pastebin, VirusTotal, Shodan, FireEye), Media like Newspapers and Magazines, and Professional/Academic publications that can be found at Libraries. This is the most commonly used source of CTI mainly because of vastness as well as being the only free source.

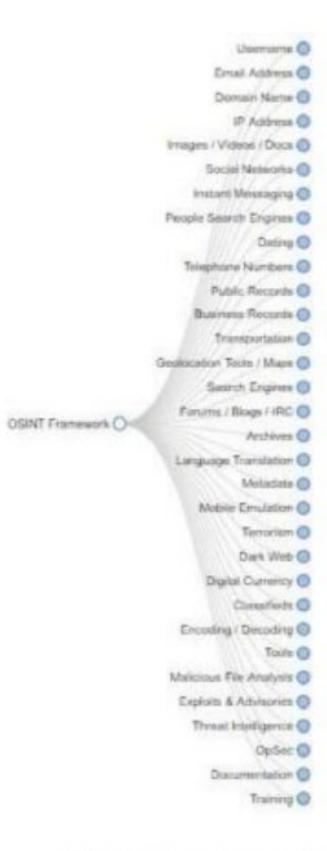


Figure showing the OSINT Framework [4]

## Information source intelligence

#### Commercial Vendors

The term refers to companies and businesses that specialize in everything Cyber Security and they provide services and information to other companies that require. The information obtained from or services rendered by these commercial vendors can be company specific, geographical location specific or cybercrime specific depending on the needs of the company hiring. However, as a result of the type of services rendered, there is a fee to be paid and depending on the reputation of the commercial vendor it could be very expensive. Symantec is currently one of the world's leading Cyber Security Vendors and they provide security for small, medium and enterprise businesses. Other Vendors include Blackberry, AT&T, Fortinet, Proofpoint.[5]

#### In-House Threat Intelligence

This is obtained when a company runs internal tests and diagnostics on its networks and systems to determine its security level. These tests could be in form of vulnerability tests to see if there are any vulnerabilities with regards to applications and servers connected to the company's network or monitoring of network activities to check for malicious activities. The results from these tests (also known as Security analytics) can be used to strengthen security levels. Company staff in charge of these tasks include incident response teams, security operations centre (SOC) personnel, and security analysts.[6]

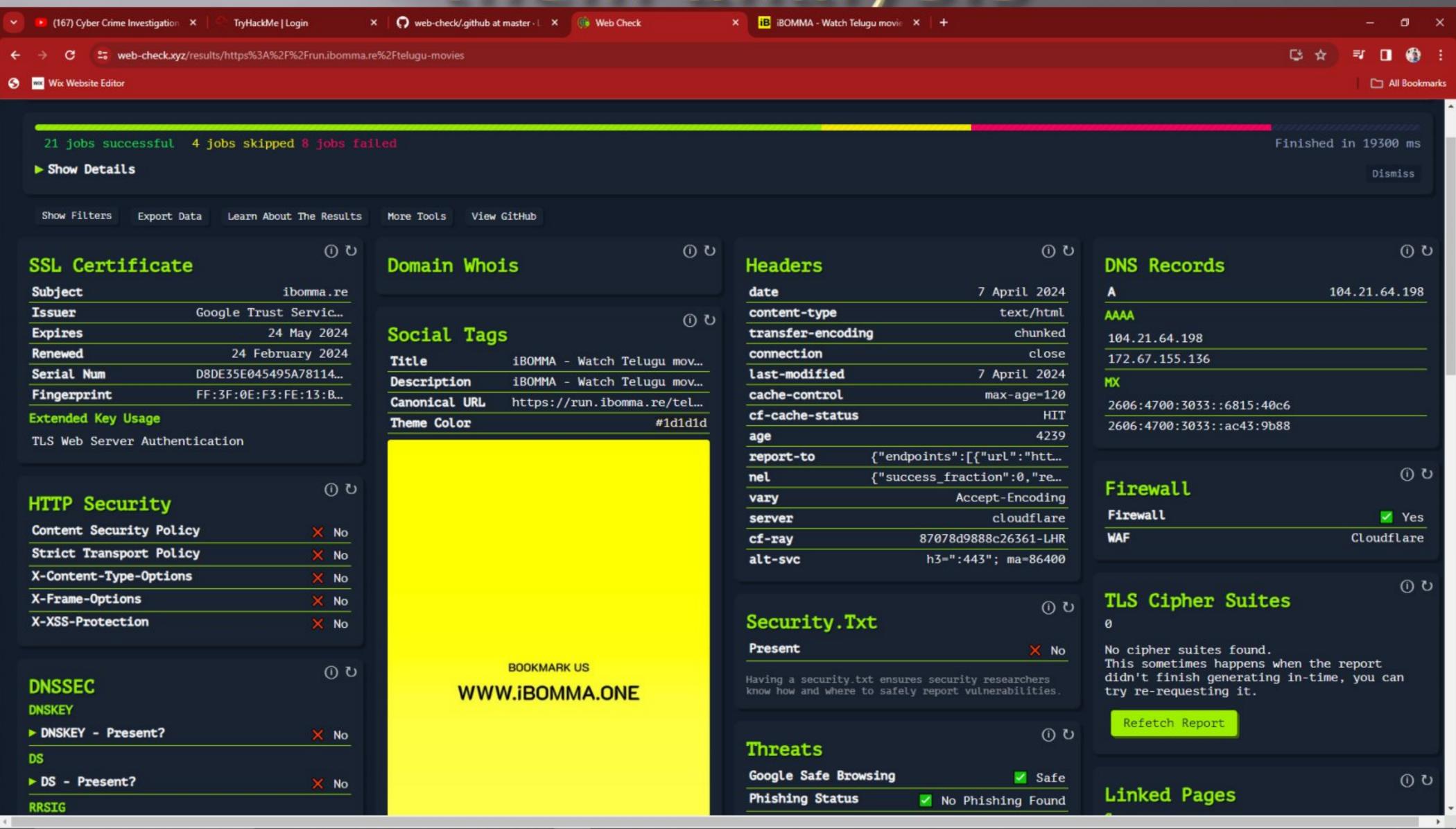
#### Human Intelligence (HUMINT)

This refers to information gathered from contact with another individual. An example is having a one-on-one conversation with an employee (who could be a friend) of a rival company that was recently involved in a Cyber-attack whereby the individual outlines the methodologies of the Advanced Persistent Threat (APT). Another example is attending a symposium/seminar whose subject matter could be an APT. The information obtained from both cases can be used to protect a company against that certain APT.

To ensure getting the information from the best source, the following should be considered:

- Are they updated regularly (monthly, yearly, or how)?
- How will the information be delivered to you?
- Which file formats is the information?
- Does the vendor provide alerts and reports? Will that be company specific or generic to everyone?

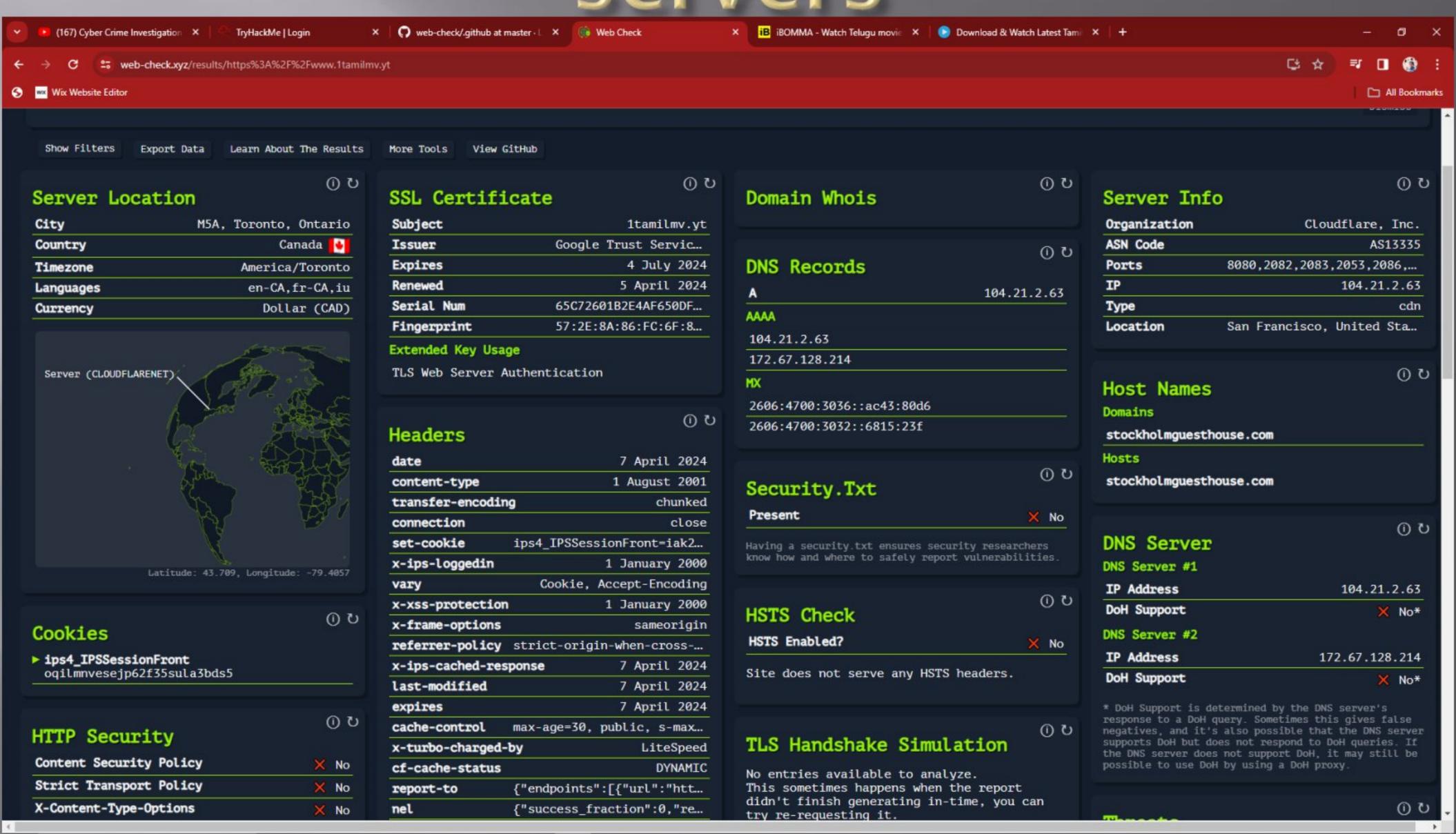
# Ibomma web site details anaylsis for webcheker.site in them analysis



## Tls security for issuses site feture



# Website into webcheker Itamil.mv after anaylsis and dns servers



# Dns to domain ip adderss for on tamil.mv scaning report

View

#### www.1tamilmv.yt

**DNS Results** 

#### A

A	Prefix	ASN	
104.21.2.63	104.21.0.0/20	AS13335 - Cloudflare, Inc.	
172.67.128.214	172.67.128.0/20	AS13335 - Cloudflare, Inc.	

#### AAAA

AAAA	Prefix	ASN	
2606:4700:3036::ac43:80d6	2606:4700:3036::/48	AS13335 - Cloudflare, Inc.	
2606:4700:3032::6815:23f	2606:4700:3032::/48	AS13335 - Cloudflare, Inc.	

Queried from the local bgp.tools unbound DNS instance. (lookup bgp.tools for source IPs)