

# RAYALASEEMA UNIVERSITY

# SRI SANKARA'S DEGREE COLLEGE,

# KURNOOL

G MANOHAR  
Bsc Microbiology  
21367008004

# Project Title : Driven Information Gathering and Threat Intelligence

- ▶ Team id : LTVIP2024TMID14080
- ▶ Team size : 05
- ▶ 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.	TOPIC NAME	PAGE NO.
1.	Osmit frame work into key points	- 5
2.	Osmit frame work on the tools for Dns information gathering	- 6
3.	Dns for mapping source for ruk website Details analysis	- 7
4.	Ruk website details report for tools	- 8
5.	Srv details and txt for records on the ruk website	- 9
6.	Osmit frame work analysis	- 10
7.	Information source intelligence	- 11
8.	Ibooma website details analysis web checker and them analysis	- 12
9.	Tls security for issueses site feature	- 13
10.	Website into web checker.com target domain 1tamil.mv	- 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.









# Dns for mapping source for ruk web site details analysis

**Jump to:** [A Records](#) [AAAA Records](#) [CNAME Records](#) [MX Records](#) [NS Records](#) [PTR Records](#) [SRV Records](#) [SOA Records](#) [TXT Records](#) [CAA Records](#) [DS Records](#) [DNSKEY Records](#)

A				
Type	Domain Name	TTL	Address	
A	www.rayalaseemauniversity.ac.in/	14400	116.206.105.72 <a href="#">Check IP Blacklist</a> Owner: <a href="#">Bigrock Solutions Ltd</a>  <a href="#">WHOIS</a>   <a href="#">AS394695</a>	

AAAA	
Sorry no record found!	

CNAME			
Type	Domain Name	TTL	Canonical Name
CNAME	www.rayalaseemauniversity.ac.in/	14400	rayalaseemauniversity.ac.in.

MX				
Type	Domain Name	TTL	Preference	Address
MX	www.rayalaseemauniversity.ac.in/	14400	0	rayalaseemauniversity.ac.in.(116.206.105.72 <a href="#">Check IP Blacklist</a> ) Owner: <a href="#">Bigrock Solutions Ltd</a>  <a href="#">WHOIS</a>   <a href="#">AS394695</a>

NS			
Type	Domain Name	TTL	Canonical Name



# Ruk website into report for domain

## MX Records

MX records for **www.rayalaseemauniversity.ac.in**:

Record	Type	Priority	Target	TTL
<a href="#">rayalaseemauniversity.ac.in</a>	MX	0	<a href="#">rayalaseemauniversity.ac.in</a>	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
<a href="#">rayalaseemauniversity.ac.in</a>	NS	<a href="#">ns2.cp-in-17.bigrockservers.com</a>	21600
<a href="#">rayalaseemauniversity.ac.in</a>	NS	<a href="#">ns1.cp-in-17.bigrockservers.com</a>	21600

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



# Srn 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	Type	Value	TTL
<a href="#">rayalaseemauniversity.ac.in</a>	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 →](#)



# Osint frame work anaylsis for key points

## 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)

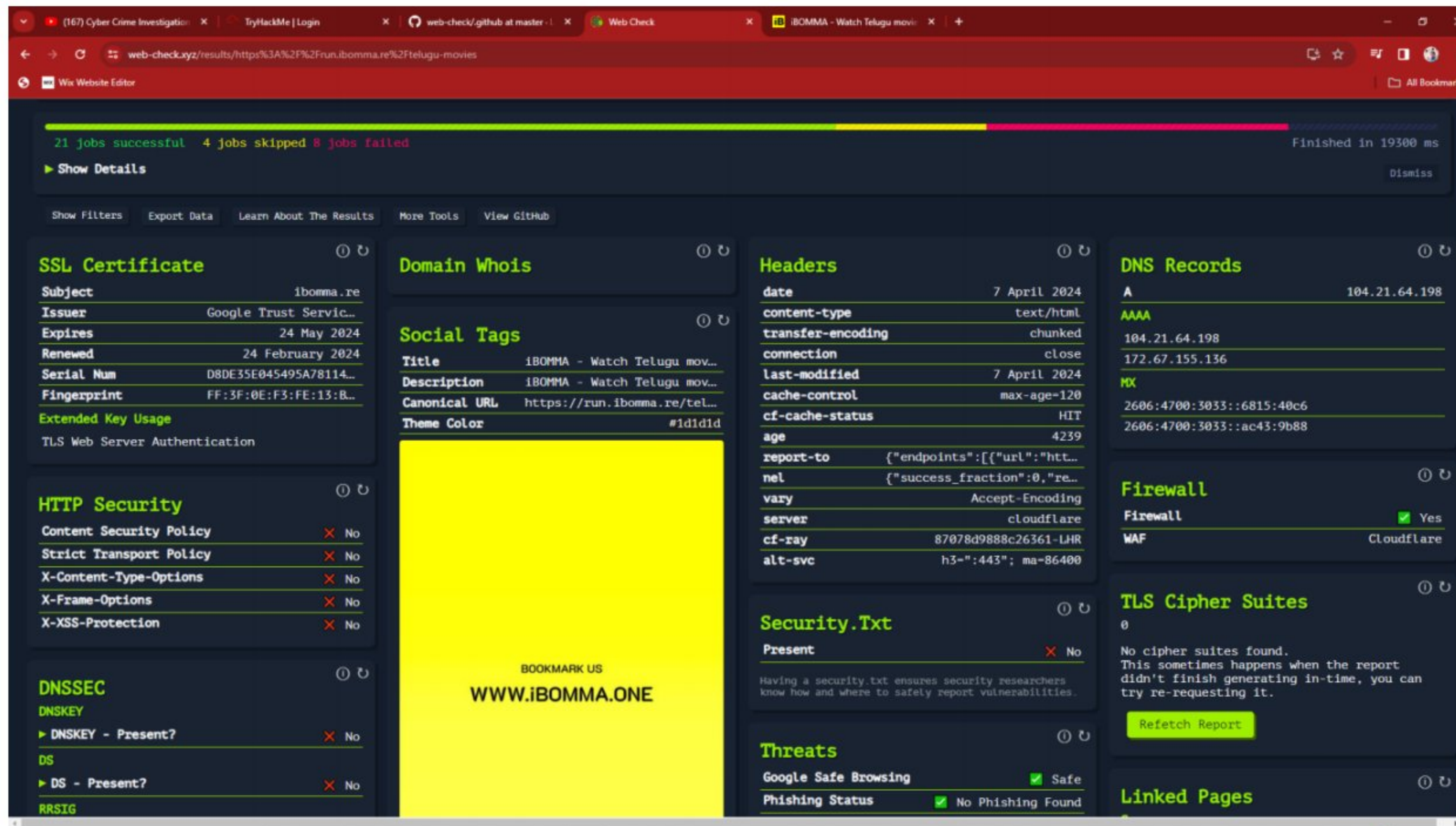
This refers to information gathered from contact with another individual. An example is having a one-on-one conversation with an employee (who could be a friend) of a rival company that was recently involved in a Cyber-attack whereby the individual outlines the methodologies of the **Advanced Persistent 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 analysis for webchecker.site in them analysis



The screenshot displays the webchecker.site interface for the domain **ibomma.re**. At the top, a status bar indicates "21 jobs successful", "4 jobs skipped", and "8 jobs failed", with a completion time of "Finished in 19300 ms". Below this, a navigation bar includes links for "Show Filters", "Export Data", "Learn About The Results", "More Tools", and "View Github".

The main content area is divided into several sections:

- SSL Certificate:** Shows details for **ibomma.re**, including the issuer (Google Trust Service), expiration date (24 May 2024), and fingerprint (FF:3F:0E:F3:FE:13:B...).
- Domain Whois:** Displays the title "IBOMMA - Watch Telugu mov...", description "IBOMMA - Watch Telugu mov...", canonical URL "https://run.ibomma.re/tel...", and theme color "#1d1d1d".
- Social Tags:** Shows the title "IBOMMA - Watch Telugu mov...", description "IBOMMA - Watch Telugu mov...", canonical URL "https://run.ibomma.re/tel...", and theme color "#1d1d1d".
- Headers:** Lists various headers such as **date** (7 April 2024), **content-type** (text/html), **transfer-encoding** (chunked), **connection** (close), **last-modified** (7 April 2024), **cache-control** (max-age=120), **cf-cache-status** (HIT), **age** (4239), **report-to**, **nel**, **vary** (Accept-Encoding), **server** (cloudflare), **cf-ray** (87078d9888c26361-LHR), and **alt-svc** (h3=":443"; ma=86400).
- DNS Records:** Shows records for **A** (104.21.64.198), **AAAA** (104.21.64.198, 172.67.155.136), and **MX** (2606:4700:3033::6815:40c6, 2606:4700:3033::ac43:9b88).
- HTTP Security:** Lists security features like **Content Security Policy**, **Strict Transport Policy**, **X-Content-Type-Options**, **X-Frame-Options**, and **X-XSS-Protection**, all marked as "No".
- DNSSEC:** Shows **DNSKEY** and **DS** records, both marked as "No".
- Security.Txt:** Indicates that a **security.txt** file is present.
- Threats:** Shows the **Google Safe Browsing** status as "Safe" and the **Phishing Status** as "No Phishing Found".
- Firewall:** Shows the **Firewall** status as "Yes" and the **WAF** (Web Application Firewall) as "Cloudflare".
- TLS Cipher Suites:** Indicates that no cipher suites were found.
- Linked Pages:** A section for linked pages.

The central part of the page features a large yellow banner with the text "BOOKMARK US" and "WWW.IBOMMA.ONE".



# Tls security for issuses site feture

The screenshot displays the web-check.xyz website interface, which provides a comprehensive analysis of a website's security and performance. The interface is organized into several sections:

- TLS Security Issues:** This section reports that no entries are available for analysis, suggesting a timing issue with the report generation. It includes a "Refetch Report" button.
- Crawl Rules:** A message indicates that this component errored unexpectedly, with a note that this usually happens if the server's response was not as expected. It also includes an "Error Details" link.
- Carbon Footprint:** This section provides environmental impact data: HTML Initial Size (134.39 bytes), CO2 for Initial Load (0.04481 grams), and Energy Usage for Load (0.0001014 KWg). A link to "websitecarbon.com" is provided for more information.
- HSTS Check:** The HSTS Enabled? status is "No", with a note that the site does not serve any HSTS headers.
- TLS Handshake Simulation:** Similar to the TLS Security Issues section, it reports no entries available for analysis and includes a "Refetch Report" button.
- Server Status:** The server is "Online", with a Status Code of 301 and a Response Time of 43ms.
- Redirects:** It shows that 3 redirects were followed when contacting the host, listing the sequence of URLs.
- Block Lists:** A list of various security and privacy tools (e.g., AdGuard, CleanBrowsing, CloudFlare, Comodo Secure, Google DNS, Neustar Family, Norton Family, OpenDNS, Quad9, Yandex Family, Yandex Safe) are shown, all with a status of "Not Blocked".
- Site Features:** This section lists various site features and their status: hosting (us-hosting: 2 Live, cloud-hosting: 1 Live, cloud-paas: 1 Live), widgets (1 Live), fonts (1 Live), javascript (javascript-library: 1 Live, jquery-plugin: 1 Live), and ui (1 Live). It also notes the last scan date: "Last scanned on 23 March 2024 at 00:30 pm".

At the bottom of the page, there are links to "View / Download Raw Data" and "Download Results", along with a "View Results" button.



# Website into webcheker 1tamil.mv after anaylsis and dns servers

The screenshot displays the web-checker tool interface, which provides a comprehensive analysis of the website 1tamil.mv. The tool is organized into several sections, each with a title and a list of details.

- Server Location:** City: MSA, Toronto, Ontario; Country: Canada; Timezone: America/Toronto; Languages: en-CA, fr-CA, iu; Currency: Dollar (CAD). A map shows the server location in North America.
- SSL Certificate:** Subject: 1tamil.mv.yt; Issuer: Google Trust Servic...; Expires: 4 July 2024; Renewed: 5 April 2024; Serial Num: 65C72601B2E4AF650DF...; Fingerprint: 57:2E:8A:86:FC:6F:8...; Extended Key Usage: TLS Web Server Authentication.
- Domain Whois:** DNS Records: A: 104.21.2.63; AAAA: 104.21.2.63, 172.67.128.214; MX: 2606:4700:3036::ac43:80d6, 2606:4700:3032::6815:23f.
- Server Info:** Organization: Cloudflare, Inc.; ASN Code: AS13335; Ports: 8080, 2082, 2083, 2053, 2086, ...; IP: 104.21.2.63; Type: cdn; Location: San Francisco, United Sta...
- Host Names:** Domains: stockholmquesthouse.com; Hosts: stockholmquesthouse.com.
- DNS Server:** DNS Server #1: IP Address: 104.21.2.63, DoH Support: No\*; DNS Server #2: IP Address: 172.67.128.214, DoH Support: No\*.
- Security.Txt:** Present: No. Having a security.txt ensures security researchers know how and where to safely report vulnerabilities.
- HSTS Check:** HSTS Enabled?: No. Site does not serve any HSTS headers.
- TLS Handshake Simulation:** No entries available to analyze. This sometimes happens when the report didn't finish generating in-time, you can try re-requesting it.
- Headers:** date: 7 April 2024; content-type: 1 August 2001; transfer-encoding: chunked; connection: close; set-cookie: ips4\_IPSSessionFront=ia2...; x-ips-loggedin: 1 January 2000; vary: Cookie, Accept-Encoding; x-xss-protection: 1 January 2000; x-frame-options: sameorigin; referrer-policy: strict-origin-when-cross-...; x-ips-cached-response: 7 April 2024; last-modified: 7 April 2024; expires: 7 April 2024; cache-control: max-age=30, public, s-max...; x-turbo-charged-by: LiteSpeed; cf-cache-status: DYNAMIC; report-to: {"endpoints":[{"url":"htt...}; nel: {"success\_fraction":0,"re...
- Cookies:** ips4\_IPSSessionFront: oqilmvsej62f35sula3bds5.
- HTTP Security:** Content Security Policy: No; Strict Transport Policy: No; X-Content-Type-Options: No.



# 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	<a href="#">104.21.0.0/20</a>	  <a href="#">AS13335 - Cloudflare, Inc.</a>
172.67.128.214	<a href="#">172.67.128.0/20</a>	  <a href="#">AS13335 - Cloudflare, Inc.</a>

### AAAA

AAAA	Prefix	ASN
2606:4700:3036::ac43:80d6	<a href="#">2606:4700:3036::/48</a>	  <a href="#">AS13335 - Cloudflare, Inc.</a>
2606:4700:3032::6815:23f	<a href="#">2606:4700:3032::/48</a>	  <a href="#">AS13335 - Cloudflare, Inc.</a>

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