Task-7

Footprinting and Reconnaissance on Websites

(using osnit framework/nslookup.io)

**What is footprinting and how does it work?**

Footprinting is an ethical hacking technique used to gather as much data as possible about a specific targeted computer system, an infrastructure and networks to identify opportunities to penetrate them. It is one of the best methods of finding vulnerabilities.

The process of cybersecurity footprinting involves profiling organizations and collecting data about the network, host, employees and third-party partners. This information includes the OS used by the organization, firewalls, network maps, IP addresses, domain name system information, security configurations of the target machine, URLs, virtual private networks, staff IDs, email addresses and phone numbers.

* There are two types of footprinting in ethical hacking:

1)active footprinting

2)passive footprinting

**What is active footprinting?**

Active footprinting describes the process of using tools and techniques, like using the traceroute commands or a ping sweep -- Internet Control Message Protocol sweep -- to collect data about a specific target. This often triggers the target's intrusion detection system (IDS). It takes a certain level of stealth and creativity to evade detection successfully.

**What is passive footprinting?**

As the name implies, passive footprinting involves collecting data about a specific target using innocuous methods, like performing a Google search, looking through Archive.org, using NeoTrace, browsing through employees' social media profiles, looking at job sites and using Whois, a website that provides the domain names and associated networks fora specific organization. It is a stealthier approach to footprinting because it does not trigger the target's IDS.

## **What Is Reconnaissance?**

Footprinting is a part of a larger process known as reconnaissance. Reconnaissance is the information-gathering stage of ethical hacking, where you collect data about the target system. This data can include anything from network infrastructure to employee contact details. The goal of reconnaissance is to identify as many potential attack vectors as possible.

Data collected from reconnaissance may include:

* **Security policies** - Knowing an organization’s security policies can help you find weaknesses in their system.
* **Network infrastructure** - A hacker needs to know what type of network the target is using (e.g., LAN, WAN, MAN), as well as the IP address range and subnet mask.
* **Employee contact details** - Email addresses, phone numbers, and social media accounts can be used to launch social engineering attacks.
* **Host information** - Information about specific hosts, such as operating system type and version, can be used to find vulnerabilities.

Website footprinting and Reconnaissance can be done by DNS lookup/Osint framework

Now I’m using Osint framework for footprinting a website by domain name

**OSINT is short for open-source intelligence framework** that focuses on gathering information about the target available over the internet.

This framework helps security researchers for performing automated footprinting and reconnaissance, OSINT research, and intelligence gathering.

OSINT framework focuses on gathering information from free tools and resources. Still, some sites included might require registration or offer more data in exchange for money, but OSINT will provide at least a portion of the available information for no cost.

This framework has a simple web interface that contains the list of OSINT tools arranged in a category with a tree structure on the web interface

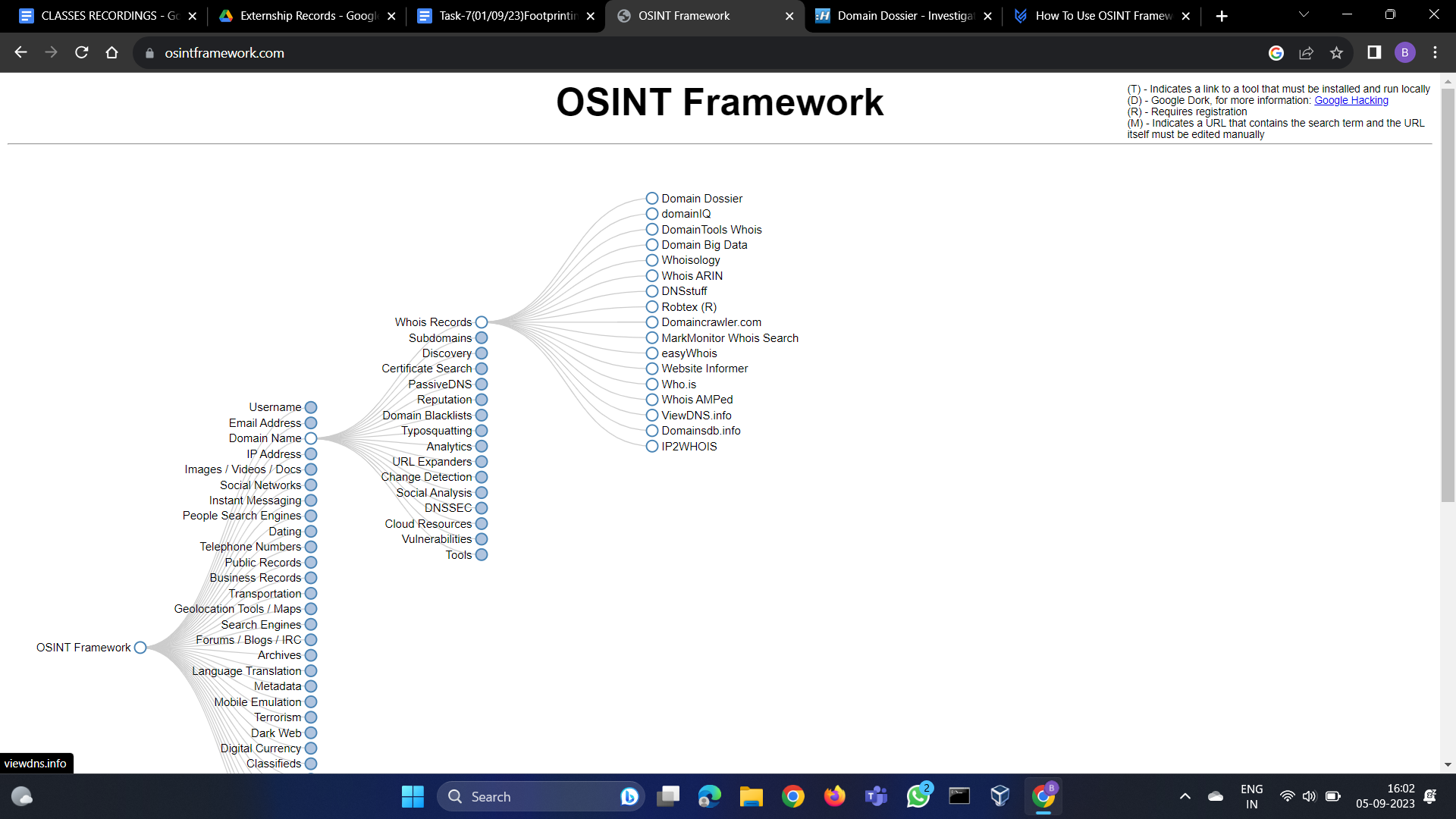
Indicators in the OSINT Framework

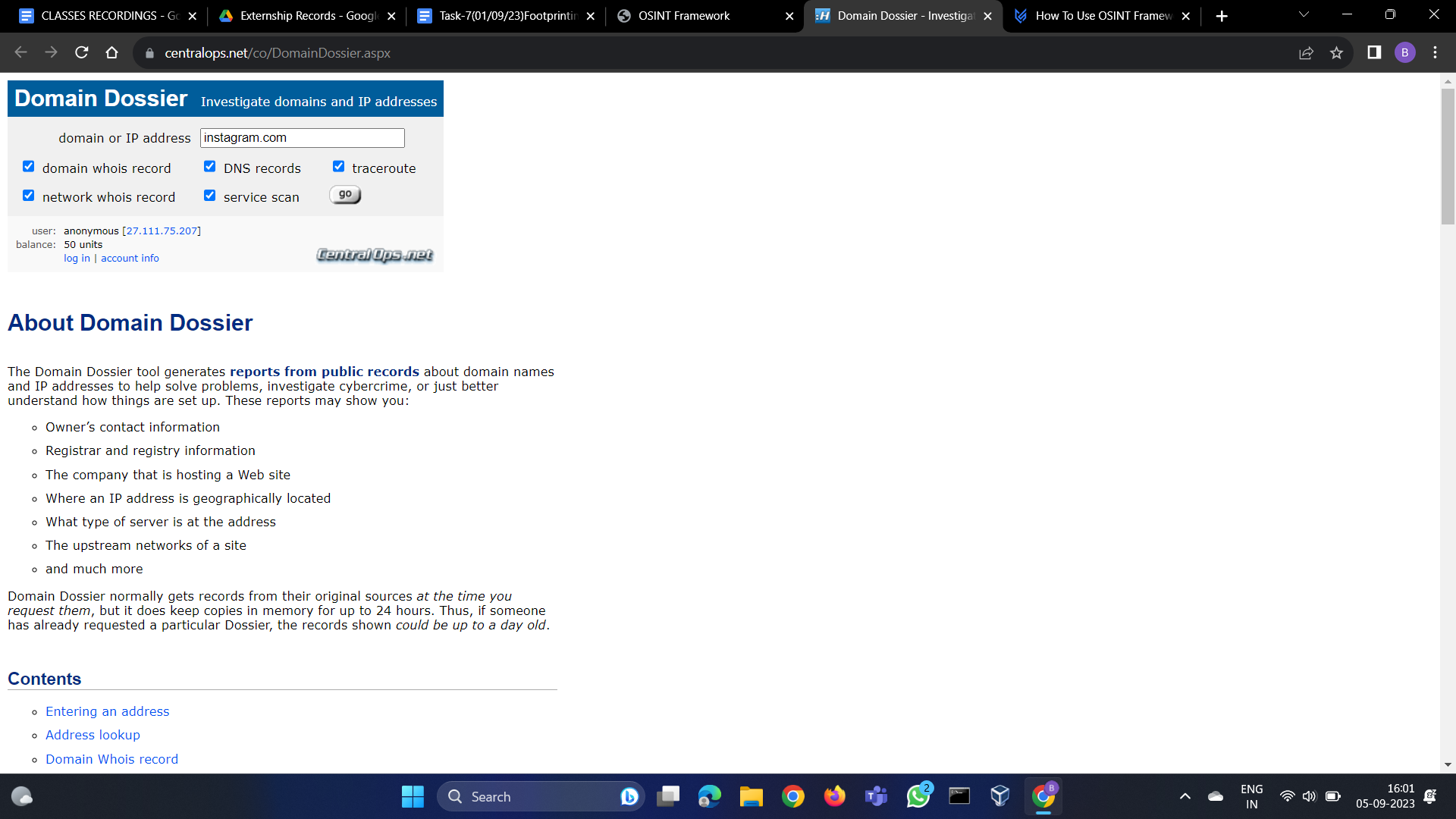
(T) – Indicates a link to a tool that must be installed and run locally

(D) – Google Dork, for more information: click here

(R) – Requires registration

(M) – indicates a URL that contains the search term and the URL itself must be edited manually





Here we found many things about the website domain,DNS records,networks by using them we can predicate the how the infrastructure made ,how to find ways to intrude to the network,where we can find the vulnerabilities to exploit using them when if were hacking

Report of the domain using domain dossier link

<https://centralops.net/co/DomainDossier.aspx?addr=instagram.com&dom_whois=true&dom_dns=true&traceroute=true&net_whois=true&svc_scan=true>

### **Address lookup**

| canonical name | [**instagram.com**](http://www.instagram.com/)**.** |
| --- | --- |
| aliases |  |
| addresses | **157.240.221.174**  **2a03:2880:f258:e0:face:b00c:0:4420** |

### **Domain Whois record**

Queried **whois.internic.net** with "**dom instagram.com**"...

Domain Name: INSTAGRAM.COM

Registry Domain ID: 121748357\_DOMAIN\_COM-VRSN

Registrar WHOIS Server: whois.registrarsafe.com

Registrar URL: http://www.registrarsafe.com

Updated Date: 2023-07-05T19:08:13Z

Creation Date: 2004-06-04T13:37:18Z

Registry Expiry Date: 2032-06-04T13:37:18Z

Registrar: RegistrarSafe, LLC

Registrar IANA ID: 3237

Registrar Abuse Contact Email: abusecomplaints@registrarsafe.com

Registrar Abuse Contact Phone: +1-650-308-7004

Domain Status: clientDeleteProhibited https://icann.org/epp#clientDeleteProhibited

Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited

Domain Status: clientUpdateProhibited https://icann.org/epp#clientUpdateProhibited

Domain Status: serverDeleteProhibited https://icann.org/epp#serverDeleteProhibited

Domain Status: serverTransferProhibited https://icann.org/epp#serverTransferProhibited

Domain Status: serverUpdateProhibited https://icann.org/epp#serverUpdateProhibited

Name Server: A.NS.INSTAGRAM.COM

Name Server: B.NS.INSTAGRAM.COM

Name Server: C.NS.INSTAGRAM.COM

Name Server: D.NS.INSTAGRAM.COM

DNSSEC: unsigned

URL of the ICANN Whois Inaccuracy Complaint Form: https://www.icann.org/wicf/

>>> Last update of whois database: 2023-09-04T15:08:42Z <<<

Queried **whois.registrarsafe.com** with "**instagram.com**"...

Domain Name: INSTAGRAM.COM

Registry Domain ID: 121748357\_DOMAIN\_COM-VRSN

Registrar WHOIS Server: whois.registrarsafe.com

Registrar URL: https://www.registrarsafe.com

Updated Date: 2023-07-05T19:08:13Z

Creation Date: 2004-06-04T13:37:18Z

Registrar Registration Expiration Date: 2032-06-04T13:37:18Z

Registrar: RegistrarSafe, LLC

Registrar IANA ID: 3237

Registrar Abuse Contact Email: abusecomplaints@registrarsafe.com

Registrar Abuse Contact Phone: +1.6503087004

Domain Status: clientDeleteProhibited https://www.icann.org/epp#clientDeleteProhibited

Domain Status: clientTransferProhibited https://www.icann.org/epp#clientTransferProhibited

Domain Status: clientUpdateProhibited https://www.icann.org/epp#clientUpdateProhibited

Domain Status: serverDeleteProhibited https://www.icann.org/epp#serverDeleteProhibited

Domain Status: serverTransferProhibited https://www.icann.org/epp#serverTransferProhibited

Domain Status: serverUpdateProhibited https://www.icann.org/epp#serverUpdateProhibited

Registry Registrant ID:

Registrant Name: Domain Admin

Registrant Organization: Instagram LLC

Registrant Street: 1601 Willow Rd

Registrant City: Menlo Park

Registrant State/Province: CA

Registrant Postal Code: 94025

Registrant Country: US

Registrant Phone: +1.6505434800

Registrant Phone Ext:

Registrant Fax:

Registrant Fax Ext:

Registrant Email: domain@fb.com

Registry Admin ID:

Admin Name: Domain Admin

Admin Organization: Instagram LLC

Admin Street: 1601 Willow Rd

Admin City: Menlo Park

Admin State/Province: CA

Admin Postal Code: 94025

Admin Country: US

Admin Phone: +1.6505434800

Admin Phone Ext:

Admin Fax:

Admin Fax Ext:

Admin Email: domain@fb.com

Registry Tech ID:

Tech Name: Domain Admin

Tech Organization: Instagram LLC

Tech Street: 1601 Willow Rd

Tech City: Menlo Park

Tech State/Province: CA

Tech Postal Code: 94025

Tech Country: US

Tech Phone: +1.6505434800

Tech Phone Ext:

Tech Fax:

Tech Fax Ext:

Tech Email: domain@fb.com

Name Server: C.NS.INSTAGRAM.COM

Name Server: B.NS.INSTAGRAM.COM

Name Server: D.NS.INSTAGRAM.COM

Name Server: A.NS.INSTAGRAM.COM

DNSSEC: unsigned

URL of the ICANN WHOIS Data Problem Reporting System: http://wdprs.internic.net/

>>> Last update of WHOIS database: 2023-09-04T15:08:55Z <<<

### **Network Whois record**

Queried **whois.arin.net** with "**n 157.240.221.174**"...

NetRange: 157.240.0.0 - 157.240.255.255

CIDR: 157.240.0.0/16

NetName: THEFA-3

NetHandle: NET-157-240-0-0-1

Parent: NET157 (NET-157-0-0-0-0)

NetType: Direct Allocation

OriginAS:

Organization: Facebook, Inc. (THEFA-3)

RegDate: 2015-05-14

Updated: 2021-12-14

Ref: https://rdap.arin.net/registry/ip/157.240.0.0

OrgName: Facebook, Inc.

OrgId: THEFA-3

Address: 1601 Willow Rd.

City: Menlo Park

StateProv: CA

PostalCode: 94025

Country: US

RegDate: 2004-08-11

Updated: 2012-04-17

Ref: https://rdap.arin.net/registry/entity/THEFA-3

OrgTechHandle: OPERA82-ARIN

OrgTechName: Operations

OrgTechPhone: +1-650-543-4800

OrgTechEmail: domain@facebook.com

OrgTechRef: https://rdap.arin.net/registry/entity/OPERA82-ARIN

OrgAbuseHandle: OPERA82-ARIN

OrgAbuseName: Operations

OrgAbusePhone: +1-650-543-4800

OrgAbuseEmail: domain@facebook.com

OrgAbuseRef: https://rdap.arin.net/registry/entity/OPERA82-ARIN

### **DNS records**

| name | class | type | data | time to live | |
| --- | --- | --- | --- | --- | --- |
| instagram.com | IN | A | 157.240.251.174 | 102s | (00:01:42) |
| instagram.com | IN | AAAA | 2a03:2880:f258:e0:face:b00c:0:4420 | 102s | (00:01:42) |
| instagram.com | IN | NS | b.ns.instagram.com | 3600s | (01:00:00) |
| instagram.com | IN | NS | d.ns.instagram.com | 3600s | (01:00:00) |
| instagram.com | IN | NS | c.ns.instagram.com | 3600s | (01:00:00) |
| instagram.com | IN | NS | a.ns.instagram.com | 3600s | (01:00:00) |
| 174.221.240.157.in-addr.arpa | IN | HINFO | | CPU: | RFC 8482 | | --- | --- | | OS: |  | | 86400s | (1.00:00:00) |
| 240.157.in-addr.arpa | IN | HINFO | | CPU: | RFC 8482 | | --- | --- | | OS: |  | | 68675s | (19:04:35) |
| 240.157.in-addr.arpa | IN | NS | c.ns.facebook.com | 55811s | (15:30:11) |
| 240.157.in-addr.arpa | IN | NS | b.ns.facebook.com | 55811s | (15:30:11) |
| 240.157.in-addr.arpa | IN | NS | a.ns.facebook.com | 55811s | (15:30:11) |
| 240.157.in-addr.arpa | IN | NS | d.ns.facebook.com | 55811s | (15:30:11) |
| 0.2.4.4.0.0.0.0.c.0.0.b.e.c.a.f.0.e.0.0.8.5.2.f.0.8.8.2.3.0.a.2.ip6.arpa | IN | HINFO | | CPU: | RFC 8482 | | --- | --- | | OS: |  | | 86400s | (1.00:00:00) |
| 0.8.8.2.3.0.a.2.ip6.arpa | IN | HINFO | | CPU: | RFC 8482 | | --- | --- | | OS: |  | | 22878s | (06:21:18) |
| 0.8.8.2.3.0.a.2.ip6.arpa | IN | NS | b.ns.facebook.com | 26187s | (07:16:27) |
| 0.8.8.2.3.0.a.2.ip6.arpa | IN | NS | a.ns.facebook.com | 26187s | (07:16:27) |
| 0.8.8.2.3.0.a.2.ip6.arpa | IN | NS | d.ns.facebook.com | 26187s | (07:16:27) |
| 0.8.8.2.3.0.a.2.ip6.arpa | IN | NS | c.ns.facebook.com | 26187s | (07:16:27) |

### **Traceroute**

Tracing route to **instagram.com [157.240.221.174]**...

| hop | rtt | rtt | rtt |  | ip address | fully qualified domain name |
| --- | --- | --- | --- | --- | --- | --- |

| 1 | 2 | 1 | 1 |  | 169.254.158.58 |  |
| --- | --- | --- | --- | --- | --- | --- |

| 2 | 1 | 1 | 1 |  | 169.48.118.156 | ae103.ppr01.dal13.networklayer.com |
| --- | --- | --- | --- | --- | --- | --- |

| 3 | 0 | 0 | 0 |  | 169.48.118.136 | 88.76.30a9.ip4.static.sl-reverse.com |
| --- | --- | --- | --- | --- | --- | --- |

| 4 | 5 | 3 | \* |  | 169.45.18.42 | ae17.cbs02.dr01.dal04.networklayer.com |
| --- | --- | --- | --- | --- | --- | --- |

| 5 | 25 | \* | 26 |  | 169.45.18.5 | ae2.cbs01.eq01.chi01.networklayer.com |
| --- | --- | --- | --- | --- | --- | --- |

| 6 | \* | \* | 46 |  | 50.97.17.49 | ae0.cbs02.tl01.nyc01.networklayer.com |
| --- | --- | --- | --- | --- | --- | --- |

| 7 | 118 | \* | \* |  | 169.45.19.47 | ae1.cbs01.tg01.lon01.networklayer.com |
| --- | --- | --- | --- | --- | --- | --- |

| 8 | 111 | 111 | 111 |  | 169.45.18.13 | d.12.2da9.ip4.static.sl-reverse.com |
| --- | --- | --- | --- | --- | --- | --- |

| 9 | 113 | 113 | 114 |  | 195.66.239.19 |  |
| --- | --- | --- | --- | --- | --- | --- |

| 10 | 114 | 113 | 113 |  | 129.134.44.206 | po162.asw01.lhr3.tfbnw.net |
| --- | --- | --- | --- | --- | --- | --- |

| 11 | 118 | 114 | 114 |  | 129.134.57.126 | psw04.lhr8.tfbnw.net |
| --- | --- | --- | --- | --- | --- | --- |

| 12 | 112 | 111 | 111 |  | 173.252.67.157 |  |
| --- | --- | --- | --- | --- | --- | --- |

| 13 | 113 | 113 | 113 |  | 157.240.221.174 | instagram-p42-shv-01-lhr8.fbcdn.net |
| --- | --- | --- | --- | --- | --- | --- |

Trace complete

### **Service scan**

| **FTP - 21** | Error: TimedOut |
| --- | --- |

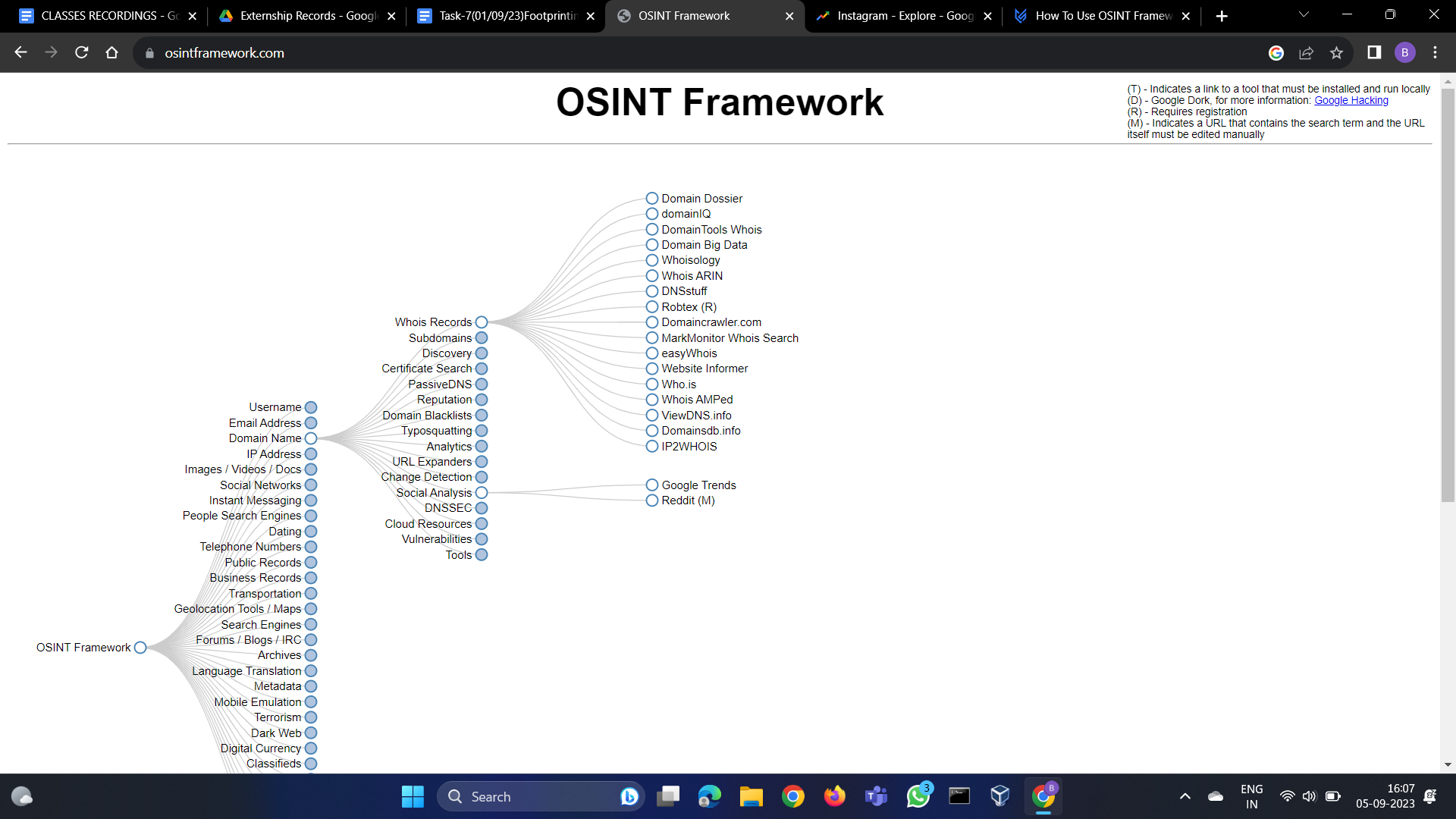
| **SMTP - 25** | Error: TimedOut |
| --- | --- |

| **HTTP - 80** | HTTP/1.1 301 Moved Permanently  Location: https://instagram.com/  Content-Type: text/plain  Server: proxygen-bolt  Date: Tue, 05 Sep 2023 10:33:22 GMT  Connection: close  Content-Length: 0 |
| --- | --- |

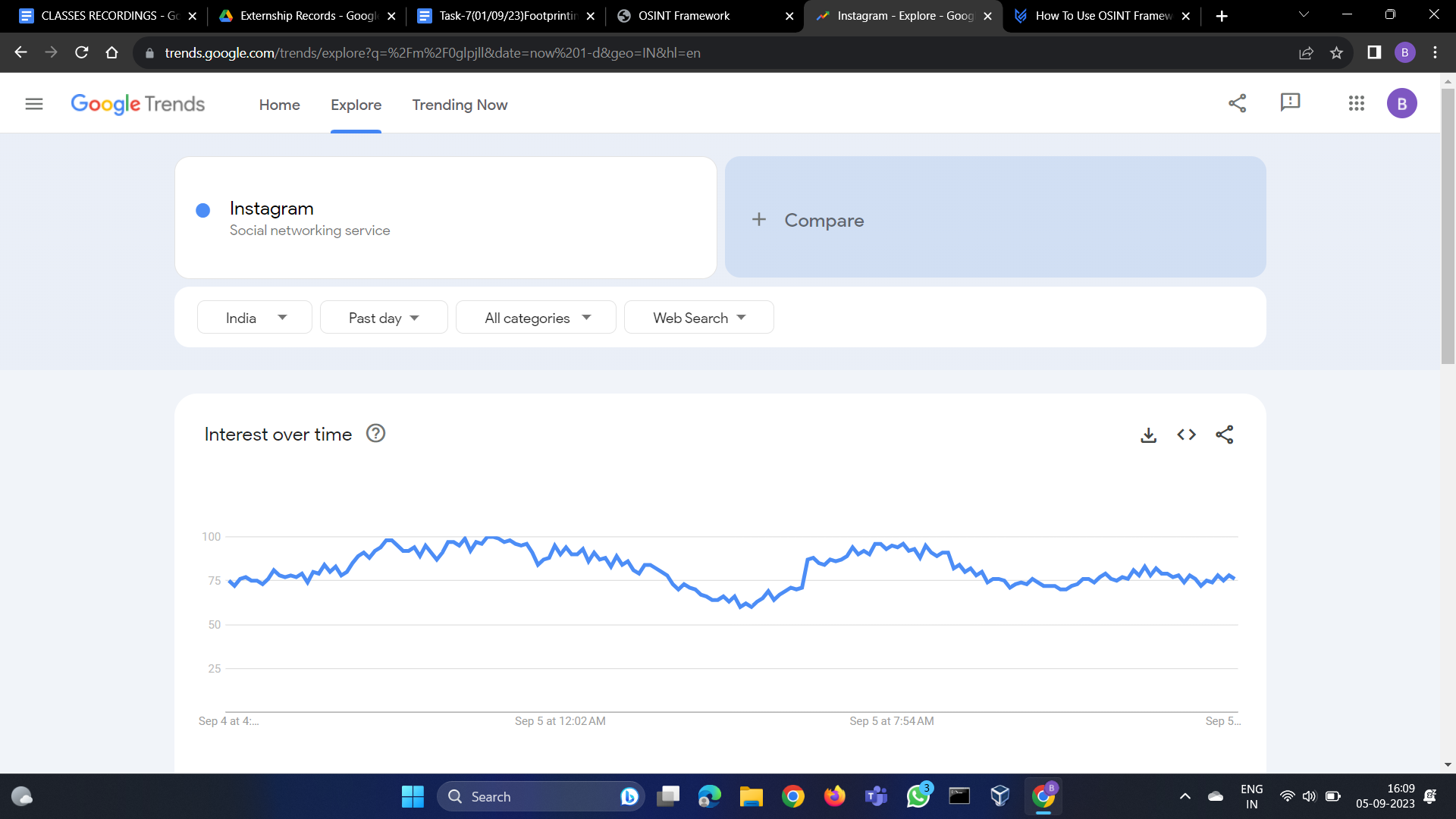
| **POP3 - 110** | Error: TimedOut |
| --- | --- |

| **IMAP - 143** | Error: TimedOut |
| --- | --- |

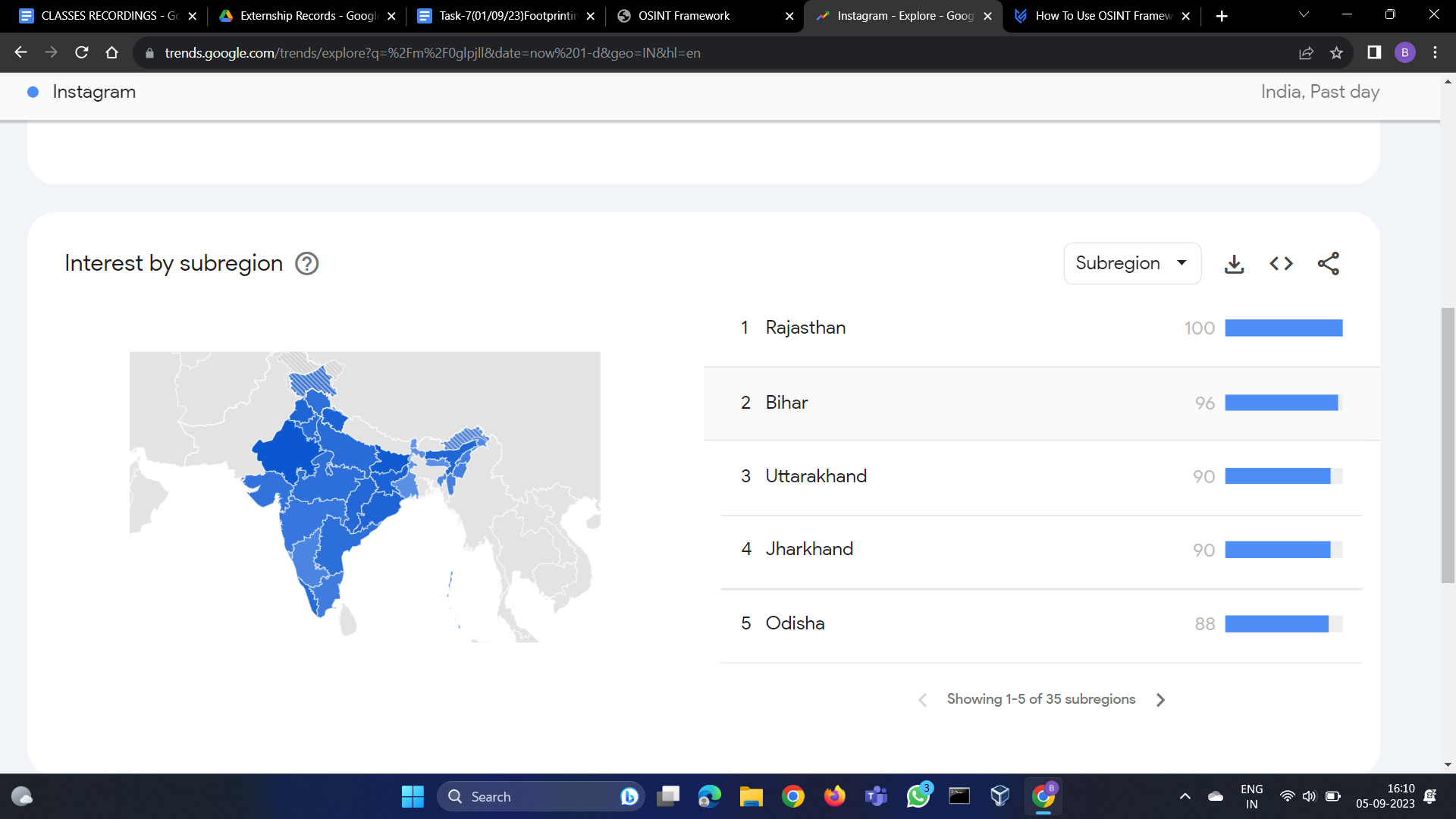
| **HTTPS - 443** | Error: The certificate key algorithm is not supported. |
| --- | --- |



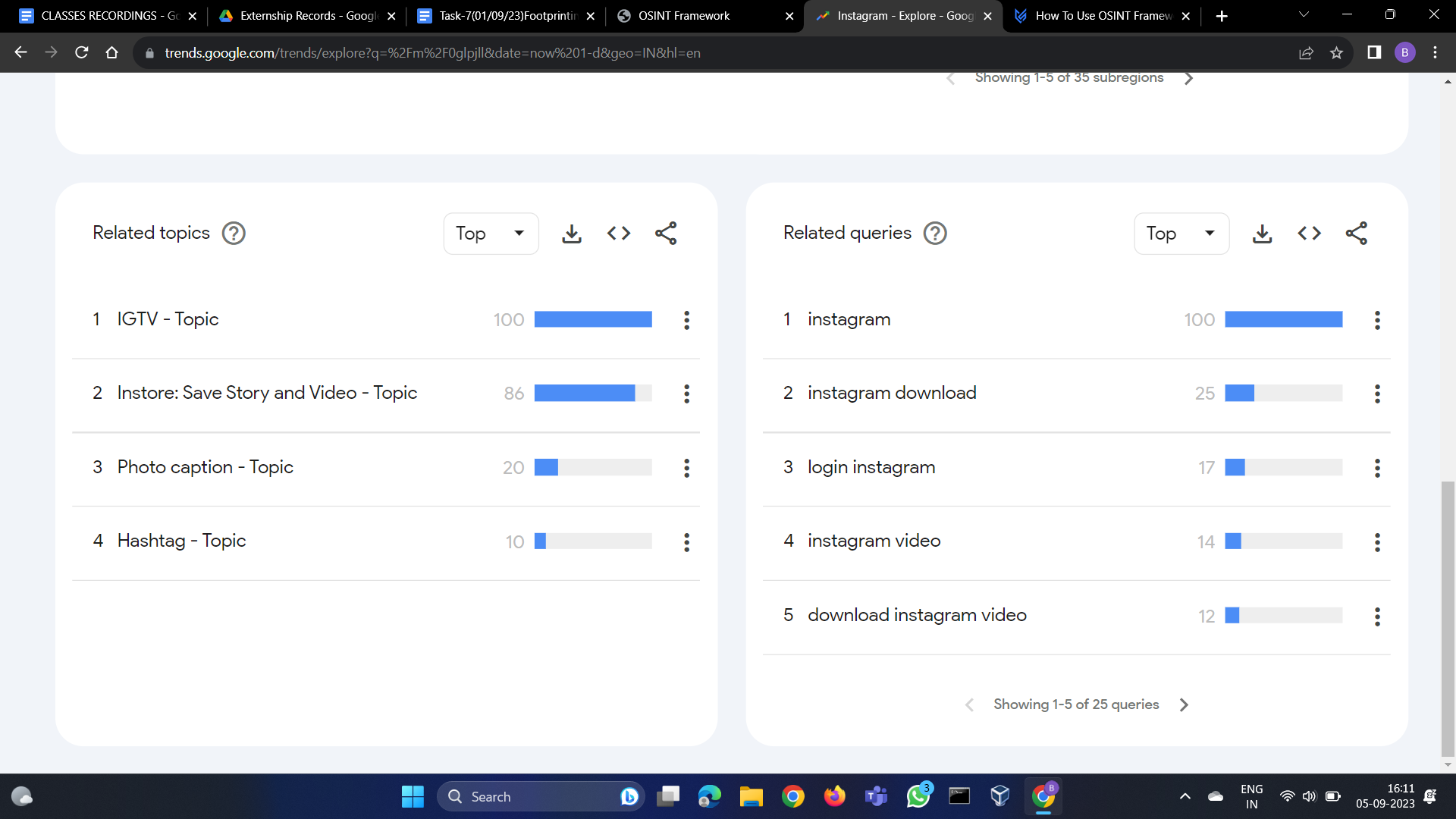
Lets move to next part like checking whether its has more users or not its analytics using google trends

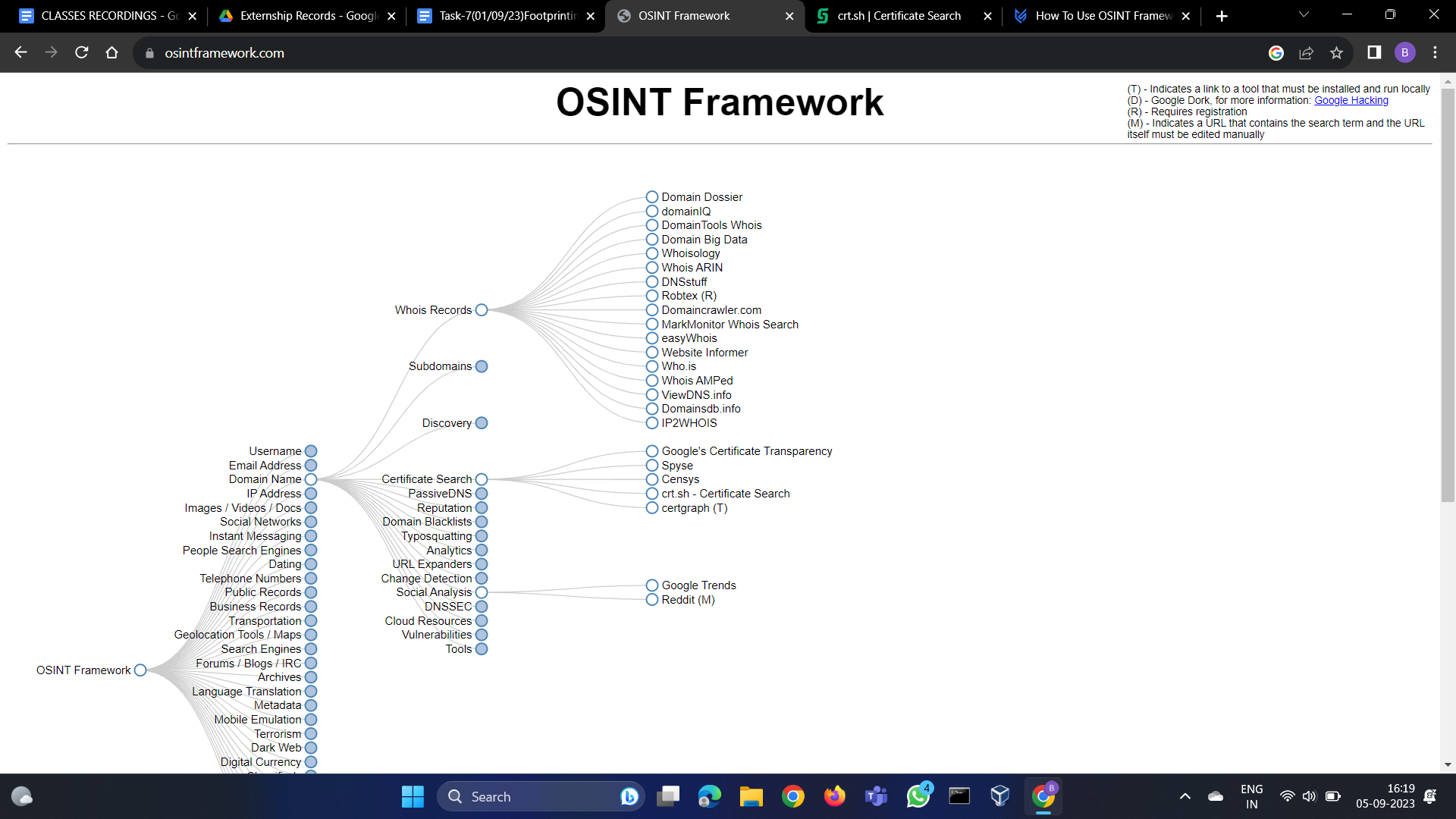


Now we can see that by subregion part which has more active users in the country (India).Here are the Top 5 states of active users

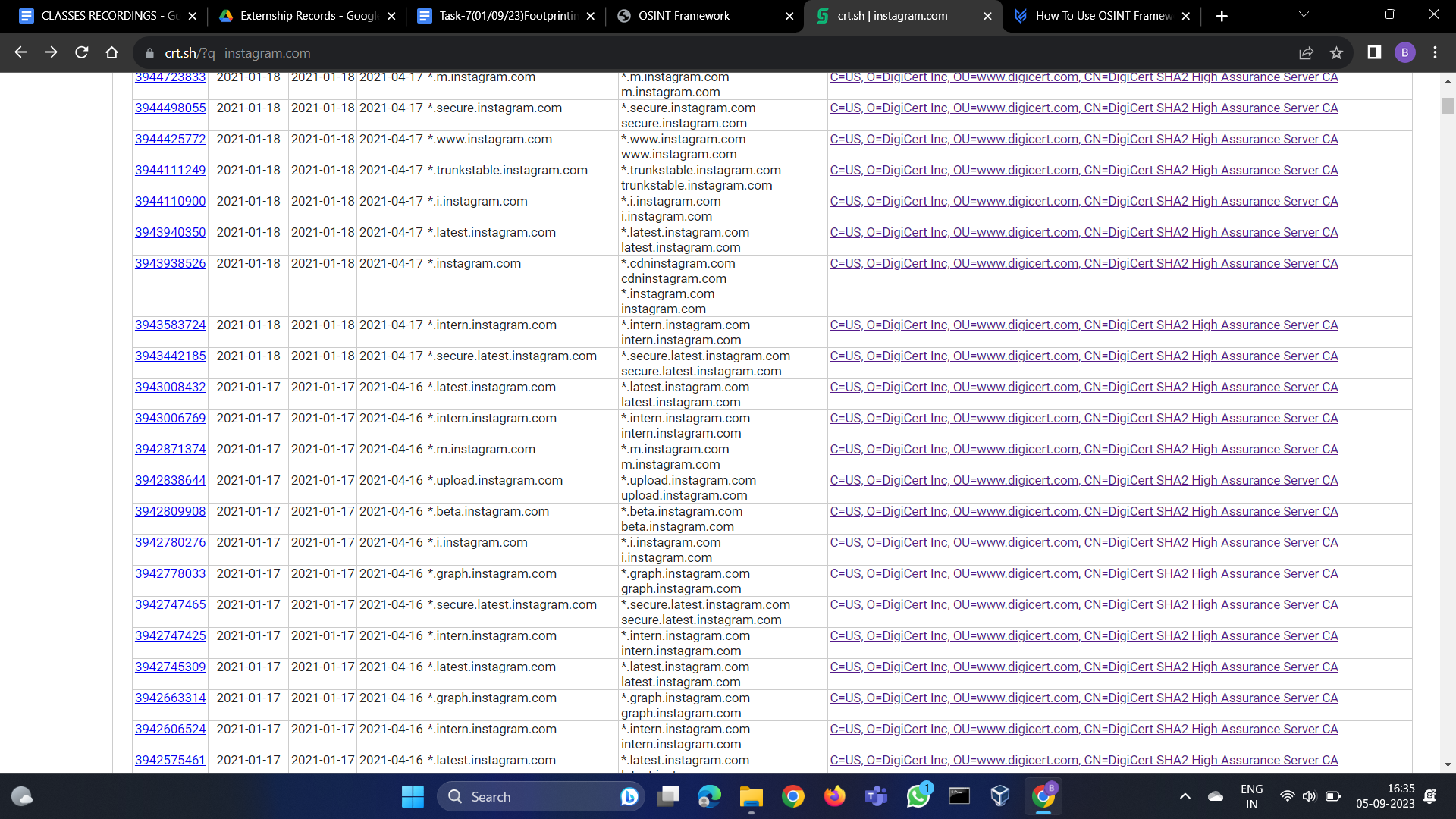


Next we can how many downloads ,login ,videos on instagram





Now seeing the certificates using crt.sh -Certificate search



Like the above we can footprint persons as well with the usernames ,etc

We can get everything from Osint framework for footprinting website,person,organization,domain ,ip address,etc