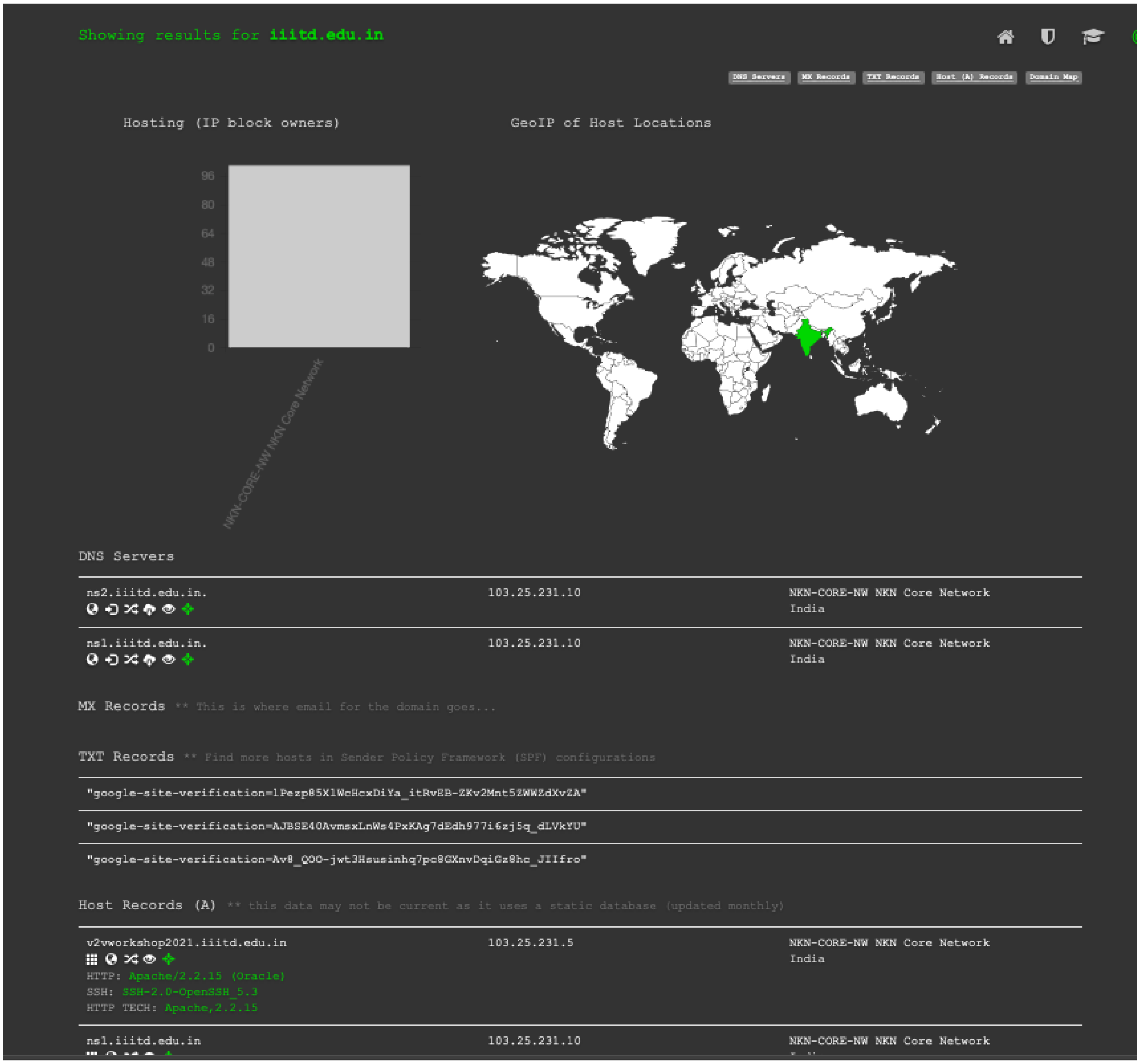
FCS ASSIGNMENT 1

Report for Question 3

For this question, I explored dnsdumpster and crt.sh. Dnsdumpster showed the public IP addresses of the various subdomains of iiitd.edu.in. It also showed DNS mappings of the domains, geographic location of the hosts, details of ISP, details of servers, trace path, hosts sharing the same IPs.



Showing results for **iiitd.edu.in**

DNS Servers

ns2.iiitd.edu.in.	103.25.231.10	NKN-CORE-NW NKN Core Network India
ns1.iiitd.edu.in.	103.25.231.10	NKN-CORE-NW NKN Core Network India

MX Records ** This is where email for the domain goes...

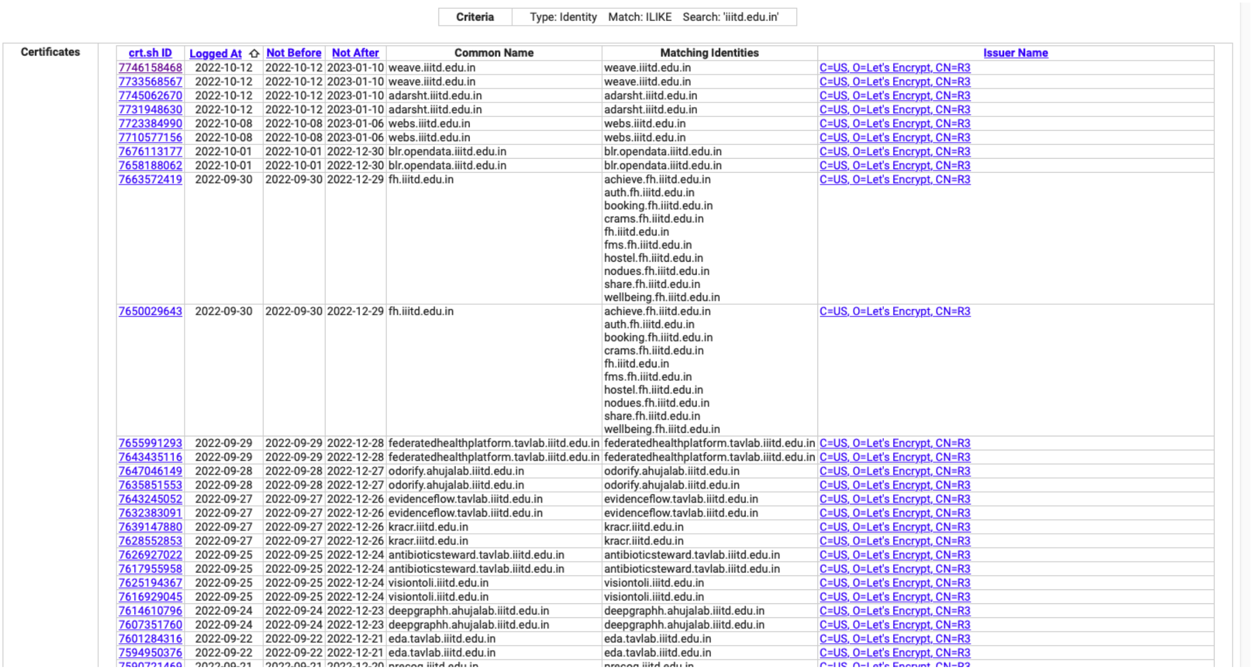
TXT Records ** Find more hosts in Sender Policy Framework (SPF) configurations

```
"google-site-verification=1Pezp85X1WcHcxDiYa_itRvEB-ZKv2Mnt5ZWWZdXvZA"
"google-site-verification=AJBSE40AvmsxLnWs4PxKAg7dEdh977i6zj5q_dLVkYU"
"google-site-verification=Av8_QOO-jwt3Hsusinhq7pc8GXnvDqiGz8hc_JIIfro"
```

Host Records (A) ** this data may not be current as it uses a static database (updated monthly)

v2vworkshop2021.iiitd.edu.in HTTP: Apache/2.2.15 (Oracle) SSH: SSH-2.0-OpenSSH_5.3 HTTP TECH: Apache,2.2.15	103.25.231.5	NKN-CORE-NW NKN Core Network India
ns1.iiitd.edu.in	103.25.231.10	NKN-CORE-NW NKN Core Network

I also explored crt.sh which showed details of the certificates, the certificates itself, the issuer(CA) and details of the CA.

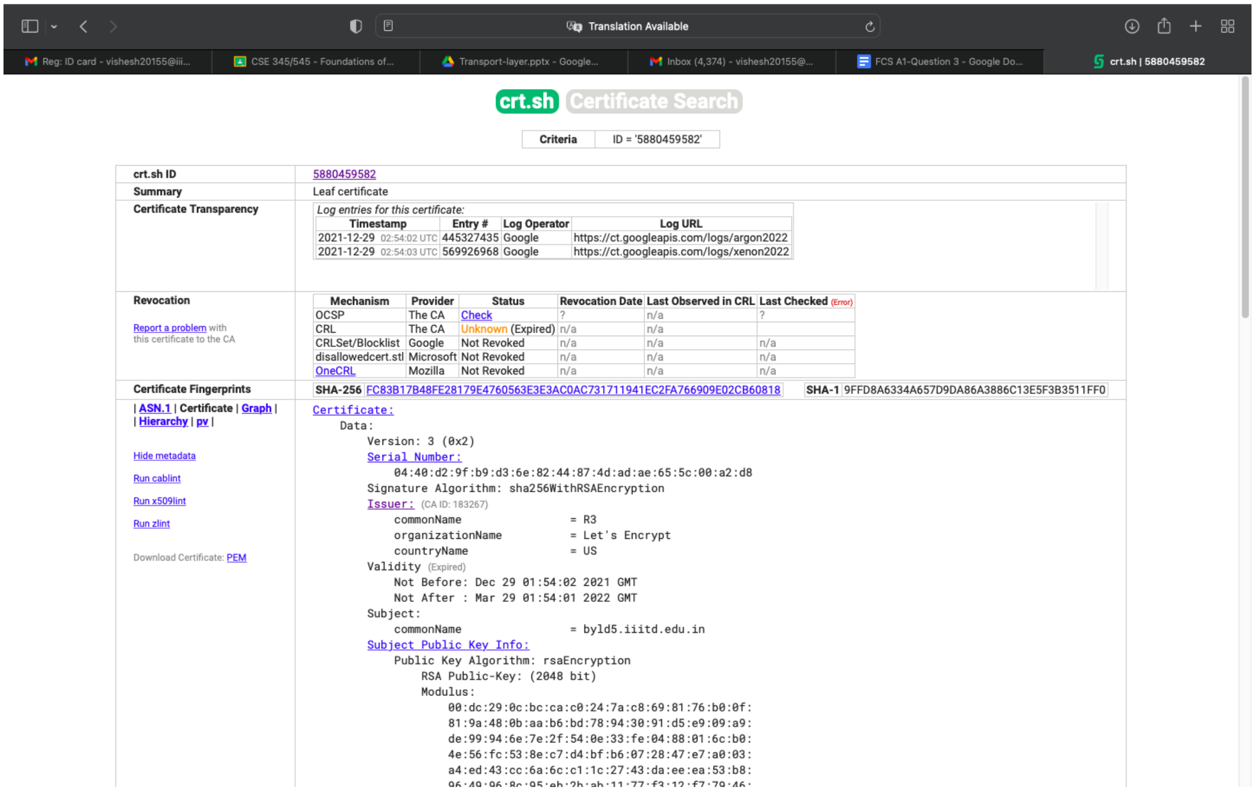


Criteria	Type: Identity Match: ILIKE Search: 'iiitd.edu.in'

Certificates

crt.sh ID	Logged At ⇧	Not Before	Not After	Common Name	Matching Identities	Issuer Name
7746158468	2022-10-12	2022-10-12	2023-01-10	weave.iiitd.edu.in	weave.iiitd.edu.in	C=US, O=Let's Encrypt, CN=R3
7733568567	2022-10-12	2022-10-12	2023-01-10	weave.iiitd.edu.in	weave.iiitd.edu.in	C=US, O=Let's Encrypt, CN=R3
7745062670	2022-10-12	2022-10-12	2023-01-10	adarsht.iiitd.edu.in	adarsht.iiitd.edu.in	C=US, O=Let's Encrypt, CN=R3
7731948630	2022-10-12	2022-10-12	2023-01-10	adarsht.iiitd.edu.in	adarsht.iiitd.edu.in	C=US, O=Let's Encrypt, CN=R3
7723384990	2022-10-08	2022-10-08	2023-01-06	webs.iiitd.edu.in	webs.iiitd.edu.in	C=US, O=Let's Encrypt, CN=R3
7710577156	2022-10-08	2022-10-08	2023-01-06	webs.iiitd.edu.in	webs.iiitd.edu.in	C=US, O=Let's Encrypt, CN=R3
7676113177	2022-10-01	2022-10-01	2022-12-30	blr.opendata.iiitd.edu.in	blr.opendata.iiitd.edu.in	C=US, O=Let's Encrypt, CN=R3
7658188062	2022-10-01	2022-10-01	2022-12-30	blr.opendata.iiitd.edu.in	blr.opendata.iiitd.edu.in	C=US, O=Let's Encrypt, CN=R3
7663572419	2022-09-30	2022-09-30	2022-12-29	fh.iiitd.edu.in	achieve.fh.iiitd.edu.in auth.fh.iiitd.edu.in booking.fh.iiitd.edu.in crams.fh.iiitd.edu.in fh.iiitd.edu.in fms.fh.iiitd.edu.in hostel.fh.iiitd.edu.in nodues.fh.iiitd.edu.in share.fh.iiitd.edu.in wellbeing.fh.iiitd.edu.in	C=US, O=Let's Encrypt, CN=R3
7650029643	2022-09-30	2022-09-30	2022-12-29	fh.iiitd.edu.in	achieve.fh.iiitd.edu.in auth.fh.iiitd.edu.in booking.fh.iiitd.edu.in crams.fh.iiitd.edu.in fh.iiitd.edu.in fms.fh.iiitd.edu.in hostel.fh.iiitd.edu.in nodues.fh.iiitd.edu.in share.fh.iiitd.edu.in wellbeing.fh.iiitd.edu.in	C=US, O=Let's Encrypt, CN=R3
7655991293	2022-09-29	2022-09-29	2022-12-28	federatedhealthplatform.tavlab.iiitd.edu.in	federatedhealthplatform.tavlab.iiitd.edu.in	C=US, O=Let's Encrypt, CN=R3
7643435116	2022-09-29	2022-09-29	2022-12-28	federatedhealthplatform.tavlab.iiitd.edu.in	federatedhealthplatform.tavlab.iiitd.edu.in	C=US, O=Let's Encrypt, CN=R3
7647046149	2022-09-28	2022-09-28	2022-12-27	odorify.ahujalab.iiitd.edu.in	odorify.ahujalab.iiitd.edu.in	C=US, O=Let's Encrypt, CN=R3
7635851553	2022-09-28	2022-09-28	2022-12-27	odorify.ahujalab.iiitd.edu.in	odorify.ahujalab.iiitd.edu.in	C=US, O=Let's Encrypt, CN=R3
7643245052	2022-09-27	2022-09-27	2022-12-26	evidenceflow.tavlab.iiitd.edu.in	evidenceflow.tavlab.iiitd.edu.in	C=US, O=Let's Encrypt, CN=R3
7632383091	2022-09-27	2022-09-27	2022-12-26	evidenceflow.tavlab.iiitd.edu.in	evidenceflow.tavlab.iiitd.edu.in	C=US, O=Let's Encrypt, CN=R3
7639147880	2022-09-27	2022-09-27	2022-12-26	kracr.iiitd.edu.in	kracr.iiitd.edu.in	C=US, O=Let's Encrypt, CN=R3
7628552853	2022-09-27	2022-09-27	2022-12-26	kracr.iiitd.edu.in	kracr.iiitd.edu.in	C=US, O=Let's Encrypt, CN=R3
7626927022	2022-09-25	2022-09-25	2022-12-24	antibioticsteward.tavlab.iiitd.edu.in	antibioticsteward.tavlab.iiitd.edu.in	C=US, O=Let's Encrypt, CN=R3
7617955958	2022-09-25	2022-09-25	2022-12-24	antibioticsteward.tavlab.iiitd.edu.in	antibioticsteward.tavlab.iiitd.edu.in	C=US, O=Let's Encrypt, CN=R3
7625194367	2022-09-25	2022-09-25	2022-12-24	visiontoli.iiitd.edu.in	visiontoli.iiitd.edu.in	C=US, O=Let's Encrypt, CN=R3
7616929045	2022-09-25	2022-09-25	2022-12-24	visiontoli.iiitd.edu.in	visiontoli.iiitd.edu.in	C=US, O=Let's Encrypt, CN=R3
7614610796	2022-09-24	2022-09-24	2022-12-23	deepgraphh.ahujalab.iiitd.edu.in	deepgraphh.ahujalab.iiitd.edu.in	C=US, O=Let's Encrypt, CN=R3
7607351760	2022-09-24	2022-09-24	2022-12-23	deepgraphh.ahujalab.iiitd.edu.in	deepgraphh.ahujalab.iiitd.edu.in	C=US, O=Let's Encrypt, CN=R3
7601284316	2022-09-22	2022-09-22	2022-12-21	eda.tavlab.iiitd.edu.in	eda.tavlab.iiitd.edu.in	C=US, O=Let's Encrypt, CN=R3
7594950376	2022-09-22	2022-09-22	2022-12-21	eda.tavlab.iiitd.edu.in	eda.tavlab.iiitd.edu.in	C=US, O=Let's Encrypt, CN=R3
7590721469	2022-09-21	2022-09-21	2022-12-20	precog.iiitd.edu.in	precog.iiitd.edu.in	C=US, O=Let's Encrypt, CN=R3

A few certificates' screenshots:


Translation Available
Reg: ID card - vishesh20155@iii...
CSE 345/545 - Foundations of...
Transport-layer.pptx - Google...
Inbox (4,374) - vishesh20155@...
FCS A1-Question 3 - Google Do...
crt.sh | 5880459582
crt.sh Certificate Search

Criteria	ID = '5880459582'

crt.sh ID	5880459582
Summary	Leaf certificate
Certificate Transparency	*Log entries for this certificate:*

Timestamp	Entry #	Log Operator	Log URL
2021-12-29 02:54:02 UTC	445327435	Google	https://ct.googleapis.com/logs/argon2022
2021-12-29 02:54:03 UTC	569926968	Google	https://ct.googleapis.com/logs/xenon2022

Revocation

Report a problem with this certificate to the CA

Mechanism	Provider	Status	Revocation Date	Last Observed in CRL	Last Checked (Error)
OCSP	The CA	Check	?	n/a	?
CRL	The CA	Unknown (Expired)	n/a	n/a	
CRLSet/Blocklist	Google	Not Revoked	n/a	n/a	n/a
disallowedcert.stl	Microsoft	Not Revoked	n/a	n/a	n/a
OneCRL	Mozilla	Not Revoked	n/a	n/a	n/a

Certificate Fingerprints

SHA-256	FC83B17B48FE28179E4760563E3E3AC0AC731711941EC2FA766909E02CB60818	SHA-1	9FFD8A6334A657D9DA86A3886C13E5F3B3511FF0

| ASN.1 | Certificate | Graph |
| Hierarchy | pv |

Hide metadata

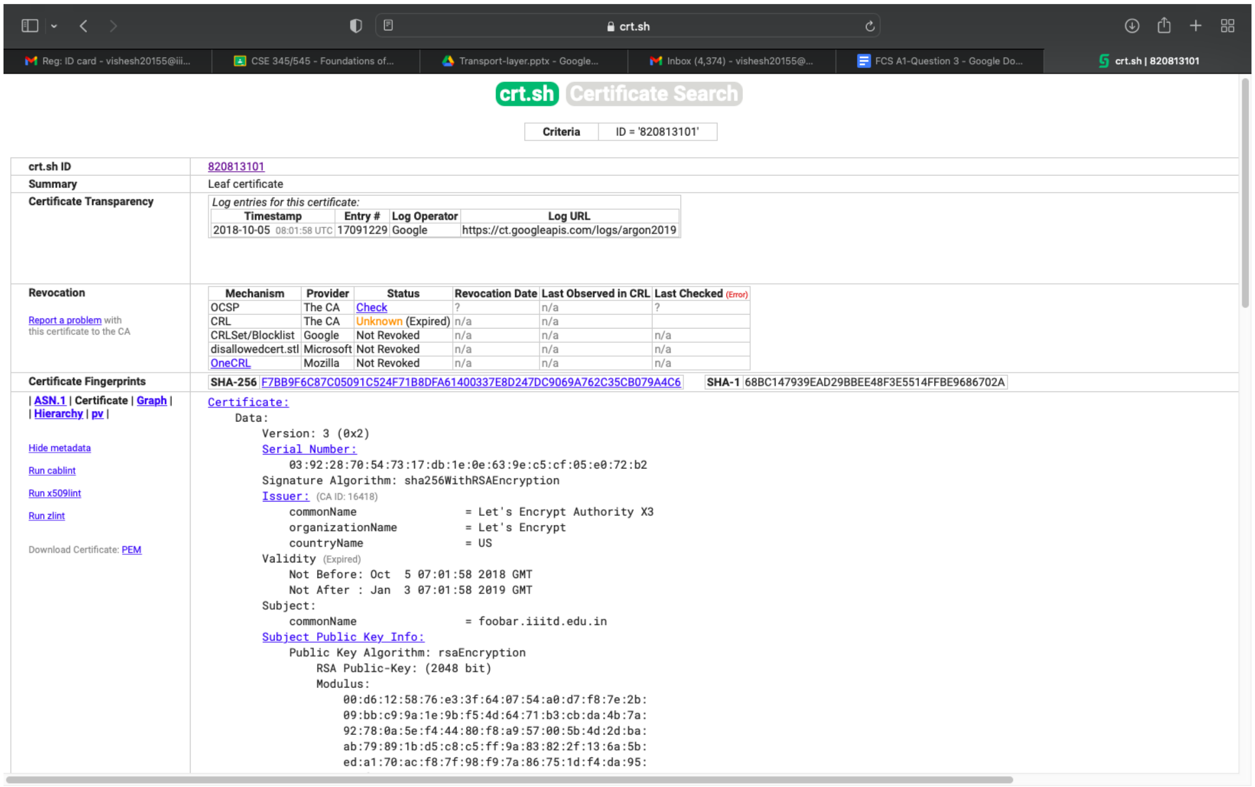
Run cablint

Run x509lint

Run zlint

Download Certificate: PEM

```
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number:
            04:40:d2:9f:b9:d3:6e:82:44:87:4d:ad:ae:65:5c:00:a2:d8
        Signature Algorithm: sha256WithRSAEncryption
        Issuer: (CA ID: 183267)
            commonName                = R3
            organizationName          = Let's Encrypt
            countryName               = US
        Validity (Expired)
            Not Before: Dec 29 01:54:02 2021 GMT
            Not After : Mar 29 01:54:01 2022 GMT
        Subject:
            commonName                = byld5.iiitd.edu.in
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                RSA Public-Key: (2048 bit)
                Modulus:
                    00:dc:29:0c:bc:ca:c0:24:7a:c8:69:81:76:b0:0f:
                    81:9a:48:0b:aa:b6:bd:78:94:30:91:d5:e9:09:a9:
                    de:99:94:6e:7e:2f:54:0e:33:fe:04:88:01:6c:b0:
                    4e:56:fc:53:8e:c7:d4:bf:b6:07:28:47:e7:a0:03:
                    a4:ed:43:cc:6a:6c:c1:1c:27:43:da:ee:ea:53:b8:
                    96:49:96:8c:95:eb:2b:ab:11:77:f3:12:f7:79:46:
```


crt.sh
Reg: ID card - vishesh20155@iii...
CSE 345/545 - Foundations of...
Transport-layer.pptx - Google...
Inbox (4,374) - vishesh20155@...
FCS A1-Question 3 - Google Do...
crt.sh | 820813101

crt.sh Certificate Search

Criteria	ID = '820813101'

crt.sh ID	820813101
Summary	Leaf certificate

Certificate Transparency

Log entries for this certificate:

Timestamp	Entry #	Log Operator	Log URL
2018-10-05 08:01:58 UTC	17091229	Google	https://ct.googleapis.com/logs/argon2019

Revocation

Report a problem with this certificate to the CA

Mechanism	Provider	Status	Revocation Date	Last Observed in CRL	Last Checked (Error)
OCSP	The CA	Check	?	n/a	?
CRL	The CA	Unknown (Expired)	n/a	n/a	
CRLSet/Blocklist	Google	Not Revoked	n/a	n/a	n/a
disallowedcert.stl	Microsoft	Not Revoked	n/a	n/a	n/a
OneCRL	Mozilla	Not Revoked	n/a	n/a	n/a

Certificate Fingerprints

SHA-256	F7BB9F6C87C05091C524F71B8DFA61400337E8D247DC9069A762C35CB079A4C6	SHA-1	68BC147939EAD29BBEE48F3E5514FFBE9686702A

| ASN.1 | Certificate | Graph |
| Hierarchy | pv |

Hide metadata

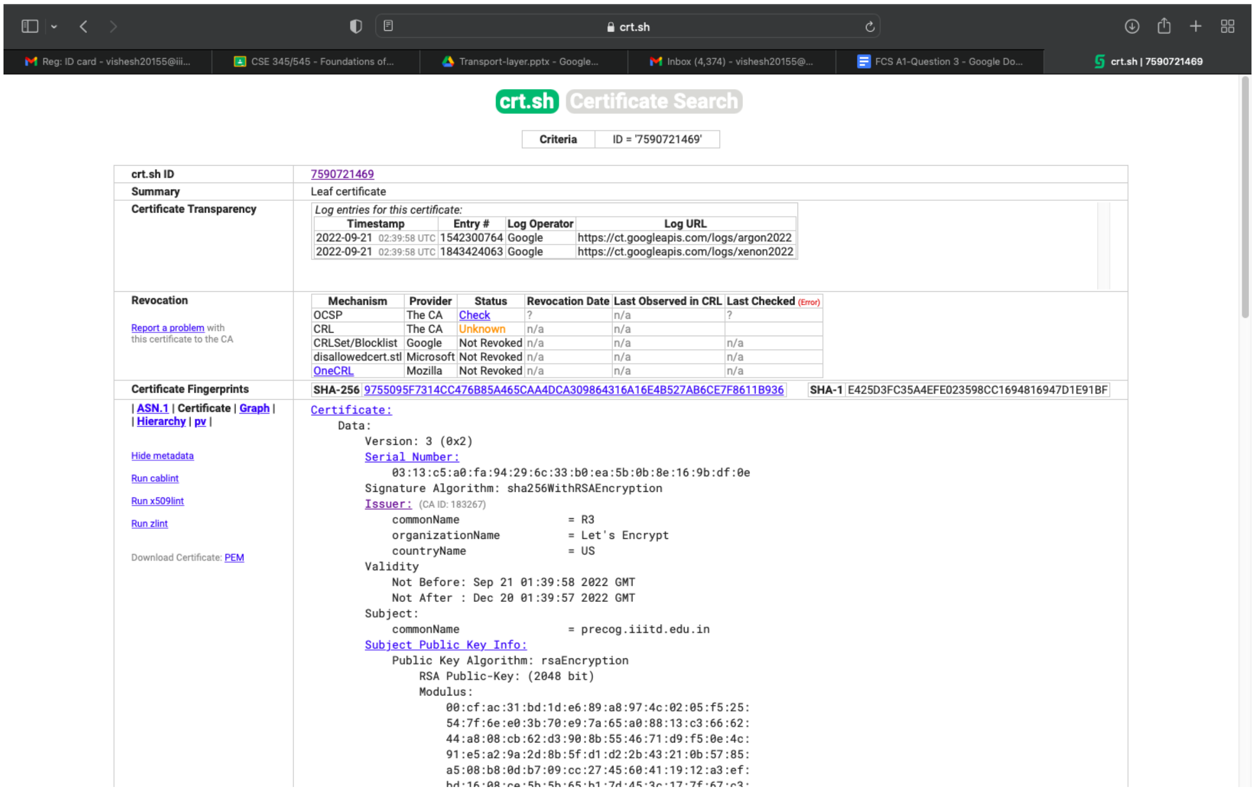
Run cablint

Run x509lint

Run zlint

Download Certificate: PEM

```
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number:
            03:92:28:70:54:73:17:db:1e:0e:63:9e:c5:cf:05:e0:72:b2
        Signature Algorithm: sha256WithRSAEncryption
        Issuer: (CA ID: 16418)
            commonName                = Let's Encrypt Authority X3
            organizationName          = Let's Encrypt
            countryName               = US
        Validity (Expired)
            Not Before: Oct  5 07:01:58 2018 GMT
            Not After : Jan  3 07:01:58 2019 GMT
        Subject:
            commonName                = foobar.iiitd.edu.in
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                RSA Public-Key: (2048 bit)
                Modulus:
                    00:d6:12:58:76:e3:3f:64:07:54:a0:d7:f8:7e:2b:
                    09:bb:c9:9a:1e:9b:f5:4d:64:71:b3:cb:da:4b:7a:
                    92:78:0a:5e:f4:44:80:f8:a9:57:00:5b:4d:2d:ba:
                    ab:79:89:1b:d5:c8:c5:ff:9a:83:82:2f:13:6a:5b:
                    ed:a1:70:ac:f8:7f:98:f9:7a:86:75:1d:f4:da:95:
```


crt.sh
Reg: ID card - vishesh20155@iii...
CSE 345/545 - Foundations of...
Transport-layer.pptx - Google...
Inbox (4,374) - vishesh20155@...
FCS A1-Question 3 - Google Do...
crt.sh | 7590721469

crt.sh Certificate Search

Criteria	ID = '7590721469'

crt.sh ID	7590721469
Summary	Leaf certificate

Certificate Transparency

Log entries for this certificate:

Timestamp	Entry #	Log Operator	Log URL
2022-09-21 02:39:58 UTC	1542300764	Google	https://ct.googleapis.com/logs/argon2022
2022-09-21 02:39:58 UTC	1843424063	Google	https://ct.googleapis.com/logs/xenon2022

Revocation

Report a problem with this certificate to the CA

Mechanism	Provider	Status	Revocation Date	Last Observed in CRL	Last Checked (Error)
OCSP	The CA	Check	?	n/a	?
CRL	The CA	Unknown	n/a	n/a	
CRLSet/Blocklist	Google	Not Revoked	n/a	n/a	n/a
disallowedcert.stl	Microsoft	Not Revoked	n/a	n/a	n/a
OneCRL	Mozilla	Not Revoked	n/a	n/a	n/a

Certificate Fingerprints

SHA-256	9755095F7314CC476B85A465CAA4DCA309864316A16E4B527AB6CE7F8611B936	SHA-1	E425D3FC35A4EFE023598CC1694816947D1E91BF

| ASN.1 | Certificate | Graph |
| Hierarchy | pv |

Hide metadata

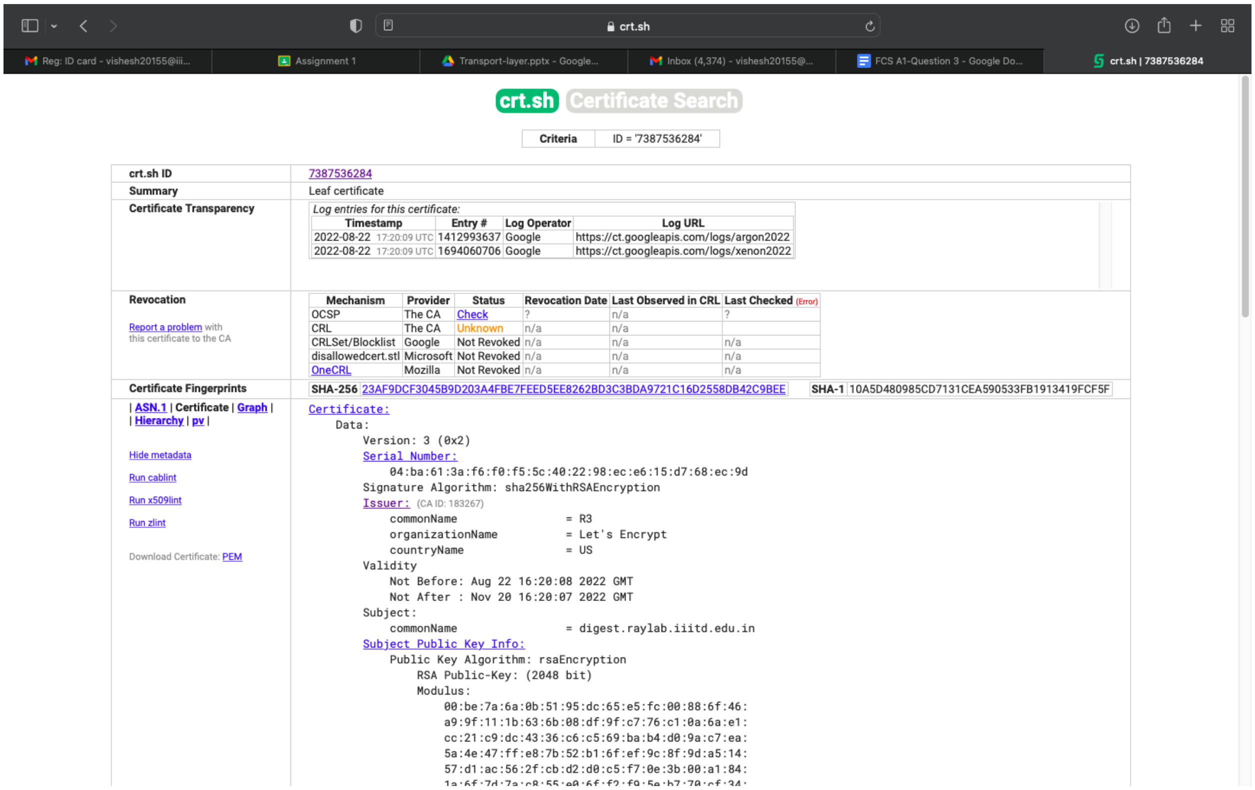
Run cablint

Run x509lint

Run zlint

Download Certificate: PEM

```
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number:
            03:13:c5:a0:fa:94:29:6c:33:b0:ea:5b:0b:8e:16:9b:df:0e
        Signature Algorithm: sha256WithRSAEncryption
        Issuer: (CA ID: 183267)
            commonName                = R3
            organizationName          = Let's Encrypt
            countryName               = US
        Validity
            Not Before: Sep 21 01:39:58 2022 GMT
            Not After : Dec 20 01:39:57 2022 GMT
        Subject:
            commonName                = precog.iiitd.edu.in
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                RSA Public-Key: (2048 bit)
                Modulus:
                    00:cf:ac:31:bd:1d:e6:89:a8:97:4c:02:05:f5:25:
                    54:7f:6e:e0:3b:70:e9:7a:65:a0:88:13:c3:66:62:
                    44:a8:08:cb:62:d3:90:8b:55:46:71:d9:f5:0e:4c:
                    91:e5:a2:9a:2d:8b:5f:d1:d2:2b:43:21:0b:57:85:
                    a5:08:b8:0d:b7:09:cc:27:45:60:41:19:12:a3:ef:
                    bd:16:08:ce:5b:5b:65:b1:7d:45:3c:17:7f:67:c3:
```


crt.sh
Reg: ID card - vishesh20155@iii...
Assignment 1
Transport-layer.pptx - Google...
Inbox (4,374) - vishesh20155@...
FCS A1-Question 3 - Google Do...
crt.sh | 7387536284

crt.sh Certificate Search

Criteria	ID = '7387536284'

crt.sh ID	7387536284
Summary	Leaf certificate
Certificate Transparency	*Log entries for this certificate:*

Timestamp	Entry #	Log Operator	Log URL
2022-08-22 17:20:09 UTC	1412993637	Google	https://ct.googleapis.com/logs/argon2022
2022-08-22 17:20:09 UTC	1694060706	Google	https://ct.googleapis.com/logs/xenon2022

Revocation

Report a problem with this certificate to the CA

Mechanism	Provider	Status	Revocation Date	Last Observed in CRL	Last Checked (Error)
OCSP	The CA	Check	?	n/a	?
CRL	The CA	Unknown	n/a	n/a	
CRLSet/Blocklist	Google	Not Revoked	n/a	n/a	n/a
disallowedcert.stl	Microsoft	Not Revoked	n/a	n/a	n/a
OneCRL	Mozilla	Not Revoked	n/a	n/a	n/a

Certificate Fingerprints

SHA-256	23AF9DCF3045B9D203A4FBE7FEED5EE8262BD3C3BDA9721C16D2558DB42C9BEE	SHA-1	10A5D480985CD7131CEA590533FB1913419FCF5F

| **ASN.1** | Certificate | **Graph** |
| **Hierarchy** | **pv** |

Hide metadata

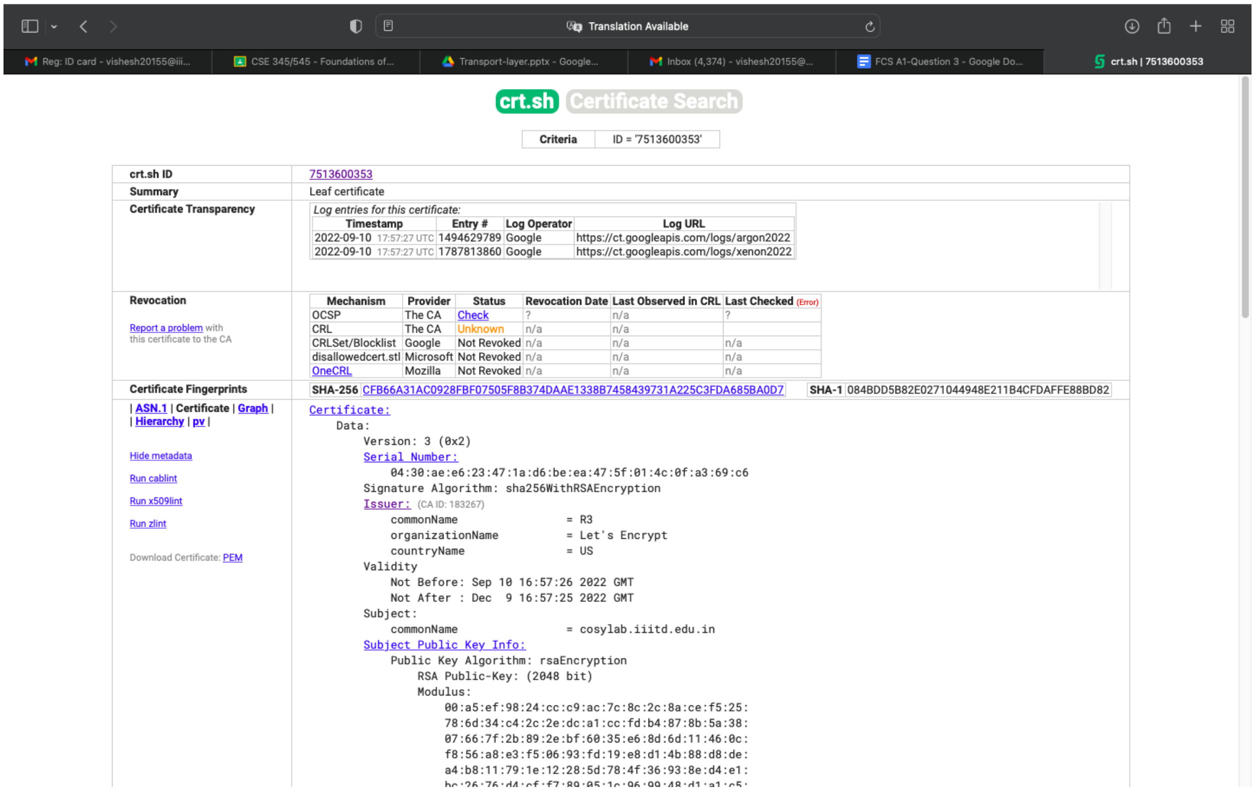
Run cablint

Run x509lint

Run zlint

Download Certificate: PEM

```
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number:
            04:ba:61:3a:f6:f0:f5:5c:40:22:98:ec:e6:15:d7:68:ec:9d
        Signature Algorithm: sha256WithRSAEncryption
        Issuer: (CA ID: 183267)
            commonName                = R3
            organizationName          = Let's Encrypt
            countryName               = US
        Validity
            Not Before: Aug 22 16:20:08 2022 GMT
            Not After : Nov 20 16:20:07 2022 GMT
        Subject:
            commonName                = digest.raylab.iiitd.edu.in
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                RSA Public-Key: (2048 bit)
                Modulus:
                    00:be:7a:6a:0b:51:95:dc:65:e5:fc:00:88:6f:46:
                    a9:9f:11:1b:63:6b:08:df:9f:c7:76:c1:0a:6a:e1:
                    cc:21:c9:dc:43:36:c6:c5:69:ba:b4:d0:9a:c7:ea:
                    5a:4e:47:ff:e8:7b:52:b1:6f:ef:9c:8f:9d:a5:14:
                    57:d1:ac:56:2f:cb:d2:d0:c5:f7:0e:3b:00:a1:84:
                    1a:6f:7d:7a:c8:55:e0:6f:f2:f9:5e:b7:70:cf:34:
```


Translation Available
Reg: ID card - vishesh20155@iii...
CSE 345/545 - Foundations of...
Transport-layer.pptx - Google...
Inbox (4,374) - vishesh20155@...
FCS A1-Question 3 - Google Do...
crt.sh | 7513600353

crt.sh Certificate Search

Criteria	ID = '7513600353'

crt.sh ID	7513600353
Summary	Leaf certificate
Certificate Transparency	*Log entries for this certificate:*

Timestamp	Entry #	Log Operator	Log URL
2022-09-10 17:57:27 UTC	1494629789	Google	https://ct.googleapis.com/logs/argon2022
2022-09-10 17:57:27 UTC	1787813860	Google	https://ct.googleapis.com/logs/xenon2022

Revocation

Report a problem with this certificate to the CA

Mechanism	Provider	Status	Revocation Date	Last Observed in CRL	Last Checked (Error)
OCSP	The CA	Check	?	n/a	?
CRL	The CA	Unknown	n/a	n/a	
CRLSet/Blocklist	Google	Not Revoked	n/a	n/a	n/a
disallowedcert.stl	Microsoft	Not Revoked	n/a	n/a	n/a
OneCRL	Mozilla	Not Revoked	n/a	n/a	n/a

Certificate Fingerprints

SHA-256	CFB66A31AC0928FBF07505F8B374DAAE1338B7458439731A225C3FDA685BA0D7	SHA-1	084BDD5B82E0271044948E211B4CFDAFFE88BD82

| **ASN.1** | Certificate | **Graph** |
| **Hierarchy** | **pv** |

Hide metadata

Run cablint

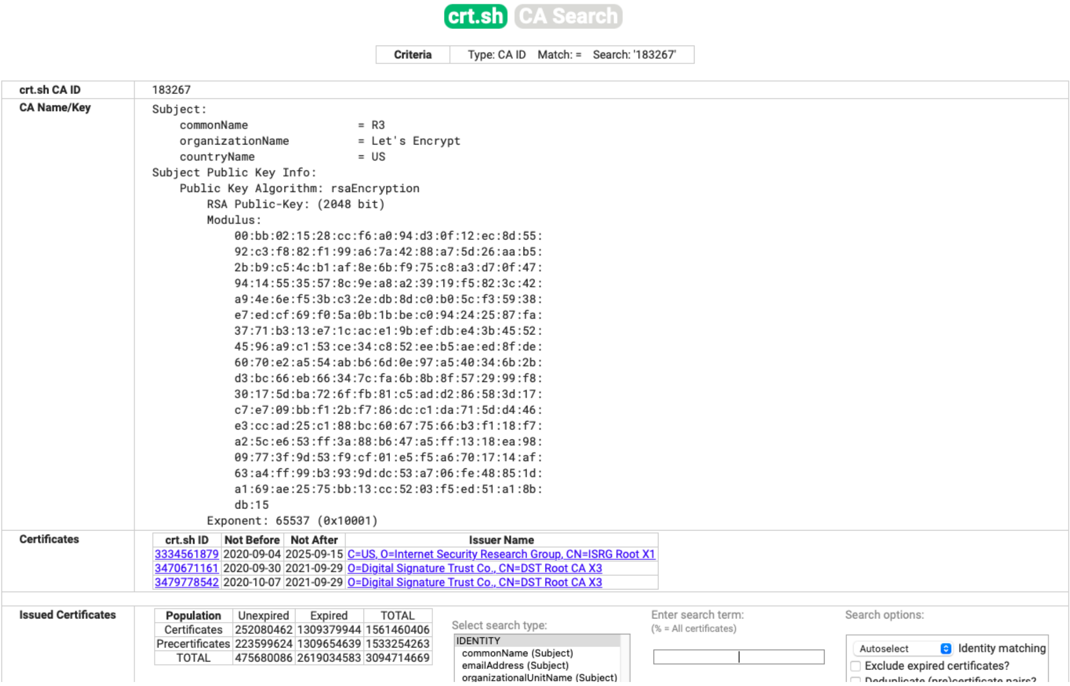
Run x509lint

Run zlint

Download Certificate: PEM

```
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number:
            04:30:ae:e6:23:47:1a:d6:be:ea:47:5f:01:4c:0f:a3:69:c6
        Signature Algorithm: sha256WithRSAEncryption
        Issuer: (CA ID: 183267)
            commonName                = R3
            organizationName          = Let's Encrypt
            countryName               = US
        Validity
            Not Before: Sep 10 16:57:26 2022 GMT
            Not After : Dec  9 16:57:25 2022 GMT
        Subject:
            commonName                = cosylab.iiitd.edu.in
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                RSA Public-Key: (2048 bit)
                Modulus:
                    00:a5:ef:98:24:cc:c9:ac:7c:8c:2c:8a:ce:f5:25:
                    78:6d:34:c4:2c:2e:dc:a1:cc:fd:b4:87:8b:5a:38:
                    07:66:7f:2b:89:2e:bf:60:35:e6:8d:6d:11:46:0c:
                    f8:56:a8:e3:f5:06:93:fd:19:e8:d1:4b:88:d8:de:
                    a4:b8:11:79:1e:12:28:5d:78:4f:36:93:8e:d4:e1:
                    bc:26:76:d4:cf:f7:89:05:1c:96:99:48:d1:a1:c5:
```

Screenshots of a few Issuer’s certificates:



Criteria	Type: CA ID Match: = Search: '183267'

crt.sh CA ID: 183267

CA Name/Key

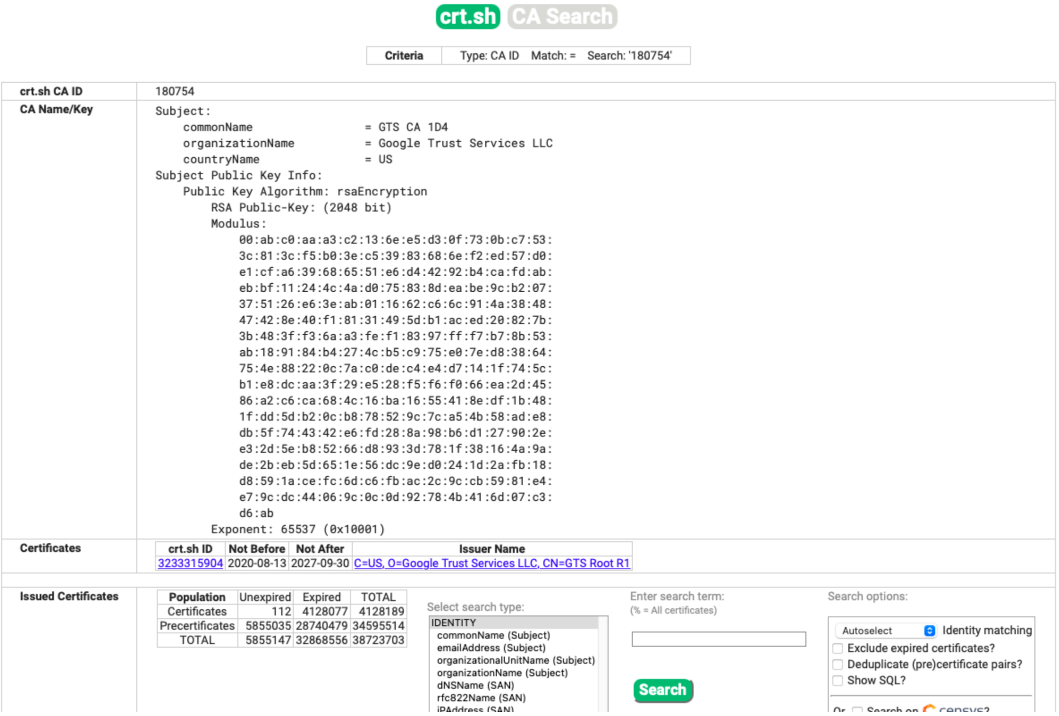
```
Subject:
    commonName                = R3
    organizationName          = Let's Encrypt
    countryName               = US
Subject Public Key Info:
    Public Key Algorithm: rsaEncryption
        RSA Public-Key: (2048 bit)
        Modulus:
            00:bb:02:15:28:cc:f6:a0:94:d3:0f:12:ec:8d:55:
            92:c3:f8:82:f1:99:a6:7a:42:88:a7:5d:26:aa:b5:
            2b:b9:c5:4c:b1:af:8e:6b:f9:75:c8:a3:d7:0f:47:
            94:14:55:35:57:8c:9e:a8:a2:39:19:f5:82:3c:42:
            a9:4e:6e:f5:3b:c3:2e:db:8d:c0:b0:5c:f3:59:38:
            e7:ed:cf:69:f0:5a:0b:1b:be:c0:94:24:25:87:fa:
            37:71:b3:13:e7:1c:ac:e1:9b:ef:db:e4:3b:45:52:
            45:96:a9:c1:53:ce:34:c8:52:ee:b5:ae:ed:8f:de:
            60:70:e2:a5:54:ab:b6:6d:0e:97:a5:40:34:6b:2b:
            d3:bc:66:eb:66:34:7c:fa:6b:8b:8f:57:29:99:f8:
            30:17:5d:ba:72:6f:fb:81:c5:ad:d2:86:58:3d:17:
            c7:e7:09:bb:f1:2b:f7:86:dc:c1:da:71:5d:d4:46:
            e3:cc:ad:25:c1:88:bc:60:67:75:66:b3:f1:18:f7:
            a2:5c:e6:53:ff:3a:88:b6:47:a5:ff:13:18:ea:98:
            09:77:3f:9d:53:f9:cf:01:e5:f5:a6:70:17:14:af:
            63:a4:ff:99:b3:93:9d:dc:53:a7:06:fe:48:85:1d:
            a1:69:ae:25:75:bb:13:cc:52:03:f5:ed:51:a1:8b:
            db:15
        Exponent: 65537 (0x10001)
```

Certificates

crt.sh ID	Not Before	Not After	Issuer Name
3334561879	2020-09-04	2025-09-15	C=US, O=Internet Security Research Group, CN=ISRG Root X1
3470671161	2020-09-30	2021-09-29	O=Digital Signature Trust Co., CN=DST Root CA X3
3479778542	2020-10-07	2021-09-29	O=Digital Signature Trust Co., CN=DST Root CA X3

Issued Certificates

Population	Unexpired	Expired	TOTAL
Certificates	252080462	1309379944	1561460406
Precertificates	223599624	1309654639	1533254263
TOTAL	475680086	2619034583	3094714669



Criteria	Type: CA ID Match: = Search: '180754'

crt.sh CA ID: 180754

CA Name/Key

```
Subject:
    commonName                = GTS CA 1D4
    organizationName          = Google Trust Services LLC
    countryName               = US
Subject Public Key Info:
    Public Key Algorithm: rsaEncryption
        RSA Public-Key: (2048 bit)
        Modulus:
            00:ab:c0:aa:a3:c2:13:6e:e5:d3:0f:73:0b:c7:53:
            3c:81:3c:f5:b0:3e:c5:39:83:68:6e:f2:ed:57:d0:
            e1:cf:a6:39:68:65:51:e6:d4:42:92:b4:ca:fd:ab:
            eb:bf:11:24:4c:4a:d0:75:83:8d:ea:be:9c:b2:07:
            37:51:26:e6:3e:ab:01:16:62:c6:6c:91:4a:38:48:
            47:42:8e:40:f1:81:31:49:5d:b1:ac:ed:20:82:7b:
            3b:48:3f:f3:6a:a3:fe:f1:83:97:ff:f7:b7:8b:53:
            ab:18:91:84:b4:27:4c:b5:c9:75:e0:7e:d8:38:64:
            75:4e:88:22:0c:7a:c0:de:c4:e4:d7:14:1f:74:5c:
            b1:e8:dc:aa:3f:29:e5:28:f5:f6:f0:66:ea:2d:45:
            86:a2:c6:ca:68:4c:16:ba:16:55:41:8e:df:1b:48:
            1f:dd:5d:b2:0c:b8:78:52:9c:7c:a5:4b:58:ad:e8:
            db:5f:74:43:42:e6:fd:28:8a:98:b6:d1:27:90:2e:
            e3:2d:5e:b8:52:66:d8:93:3d:78:1f:38:16:4a:9a:
            de:2b:eb:5d:65:1e:56:dc:9e:d0:24:1d:2a:fb:18:
            d8:59:1a:ce:fc:6d:c6:fb:ac:2c:9c:cb:59:81:e4:
            e7:9c:dc:44:06:9c:0c:0d:92:78:4b:41:6d:07:c3:
            d6:ab
        Exponent: 65537 (0x10001)
```

Certificates

crt.sh ID	Not Before	Not After	Issuer Name
3233315904	2020-08-13	2027-09-30	C=US, O=Google Trust Services LLC, CN=GTS Root R1

Issued Certificates

Population	Unexpired	Expired	TOTAL
Certificates	112	4128077	4128189
Precertificates	5855035	28740479	34595514
TOTAL	5855147	32868556	38723703

Part a:

The private IP addresses of each of this subdomain were obtained using host (similar to ping or nslookup) command. When I was not connected to the IIITD network, ‘host’ command displayed the public IPs as shown in dnsdumpster. But after connecting to the IIITD network using VPN, the ‘host’ command showed private IPs of the domain.

All these private IPs are listed in the attached file Q3partA.txt.
Some of these are:

byld5.iiitd.edu.in:[1.1.1.121]
foobar.iiitd.edu.in:[1.1.1.116]
precog.iiitd.edu.in:[1.1.1.17]
digest.raylab.iiitd.edu.in:[192.168.30.176]
cosylab.iiitd.edu.in:[1.1.1.92]

Their certificates are attached above.

Part b:

This list was obtained by using host command for the subdomains by being inside the IIITD network.
The process for automating is as follows:
I downloaded the .xlsx file of all subdomains with their private IPs from dnsdumpster. Only subdomain name and IP columns were selected. I converted this into a CSV file. This CSV file, named Subdomains.csv is attached in the submission.
Inside the python program, I read this CSV file. Using this I ran a bash command for the host from within the python program. This was to get the private IPs. I appended all private IPs in the file private_ip.txt which gets created during runtime. Now these private IPs, along with their subdomains and corresponding public IPs are listed in a CSV file, ‘SubdomainMappings.csv’ which also is created in runtime. The subdomains and their corresponding private IPs are printed as well.

To get all this information, just run: `python 2020155_q3.py`.

Part c:

Although an attacker outside of IIITD cannot get access to the private IPs without having access to the internal IIITD network. But, with the private IPs, he can launch an attack at the IP protocol of the network layer if the IP layer isn’t secured with IPsec. He can modify the IP source IP addresses or destination IPs of the packets. He can also launch routing attacks. If an attacker gets access to the private IPs and somehow gets inside the IIITD network, he can cause a lot of trouble such as pinging the websites several times to puthem down. He can even access malicious sites, or launch a virus attack within IIITD. This will happen as he would have bypassed at least one layer of firewall.

The information, publicly available on dnsdumpster and crt.sh can be very useful for the attacker. ‘Dnsdumpster’ shows the entire mapping of all the subdomains in the network. This can help the attacker understand the entire network structure of an organization.

Hence whenever he would find a vulnerability, he can plan his attack well as he'll have the entire structure of the attack surface.

'crt.sh' has all the information about certificates, domain and subdomain names. This also gives the attacker information about network infrastructure. With the certificate information available publicly, the attacker can go through certificate transparency logs, which are also available publicly.

Using all this an attacker can pan out a DOS attack.

References:

https://blog.appsecco.com/certificate-transparency-part-3-the-dark-side-9d401809b025