ASSIGNMENT NUMBER 01 FOOTPRINTING REPORT

BY ANKIT RAJ

SUBMITTED TO – MANOJ KUMAR SIR
mmahoj.manu26@gmail.com

TARGET – lnct.ac.in

STEPS & METHODS PERFORMED: -

1. REPORT ON WEBSITE TECHNOLOGY

2. REPORT ON SSL AND TLS CERTIFICATION

3. FINDING SUBDOMAINS

4. FINDING HIDDEN LINKS

5. CHECKING HEADERS SECURITY

6. FINDING BUFFER SIZE

7. FINDING HISTORY WITH archive.org

1. WEBSITE TECHNOLOGY

◪ Background

Site title	LNCT College | Top Engineering Colleges In Central India	**Date first seen**	September 2017
Site rank	614998	**Netcraft Risk Rating** ❓	1/10 ▬
Description	LNCT is one of the Top engineering college in Bhopal, MP and Central India. LNCT Synonymous with excellence in higher education with 28+...	**Primary language**	English

◪ Network

Site	https://lnct.ac.in ☒	**Domain**	lnct.ac.in
Netblock Owner	Amazon Data Services India	**Nameserver**	ns1.lnct.ac.in
Hosting company	Amazon - Asia Pacific (Mumbai) datacenter	**Domain registrar**	registry.in
Hosting country	🇮🇳 in ☒	**Nameserver organisation**	whois.registry.in
IPv4 address	3.7.218.202 (VirusTotal ☒)	**Organisation**	Lakshmi Narain College of Technology, Redacted For Privacy, Redacted For Privacy, REDACTED FOR PRIVACY, India
IPv4 autonomous systems	AS16509 ☒	**DNS admin**	info@arrowibc.com
IPv6 address	Not Present	**Top Level Domain**	India (.ac.in)
IPv6 autonomous systems	Not Present	**DNS Security Extensions**	unknown
Reverse DNS	ec2-3-7-218-202.ap-south-1.compute.amazonaws.com		

IP delegation

IPv4 address (3.7.218.202)

IP range	Country	Name	Description
`::ffff:0.0.0.0/96`	🇺🇸 United States	IANA-IPV4-MAPPED-ADDRESS	Internet Assigned Numbers Authority
↳ `3.0.0.0-3.255.255.255`	🇺🇸 United States	NET3	American Registry for Internet Numbers
↳ `3.0.0.0-3.127.255.255`	🇺🇸 United States	AT-88-Z	Amazon Technologies Inc.
↳ `3.6.0.0-3.7.255.255`	🇮🇳 India	AMAZON-BOM	Amazon Data Services India
↳ `3.7.218.202`	🇮🇳 India	AMAZON-BOM	Amazon Data Services India

◪ DMARC

DMARC (Domain-based Message Authentication, Reporting and Conformance) is a mechanism for domain owners to indicate how mail purporting to originate from their domain should be authenticated. It builds on SPF and DKIM, providing a method to set policy and to give reporting of failures. For more information please see **dmarc.org** ☒.

Raw DMARC record:

```
v=DMARC1; p=reject; rua=mailto:postmaster@lnct.ac.in, mailto:dmarc@lnct.ac.in
```

Tag	Field	Value
p=reject	Requested handling policy	Reject: emails that fail the DMARC mechanism check should be rejected. Rejection SHOULD occur during the SMTP transaction.
rua=mailto:postmaster@lnct.ac.in, mailto:dmarc@lnct.ac.in	Reporting URI(s) for aggregate data	postmaster@lnct.ac.in, Invalid (mailto:dmarc@lnct.ac.in)

⬛ Hosting History

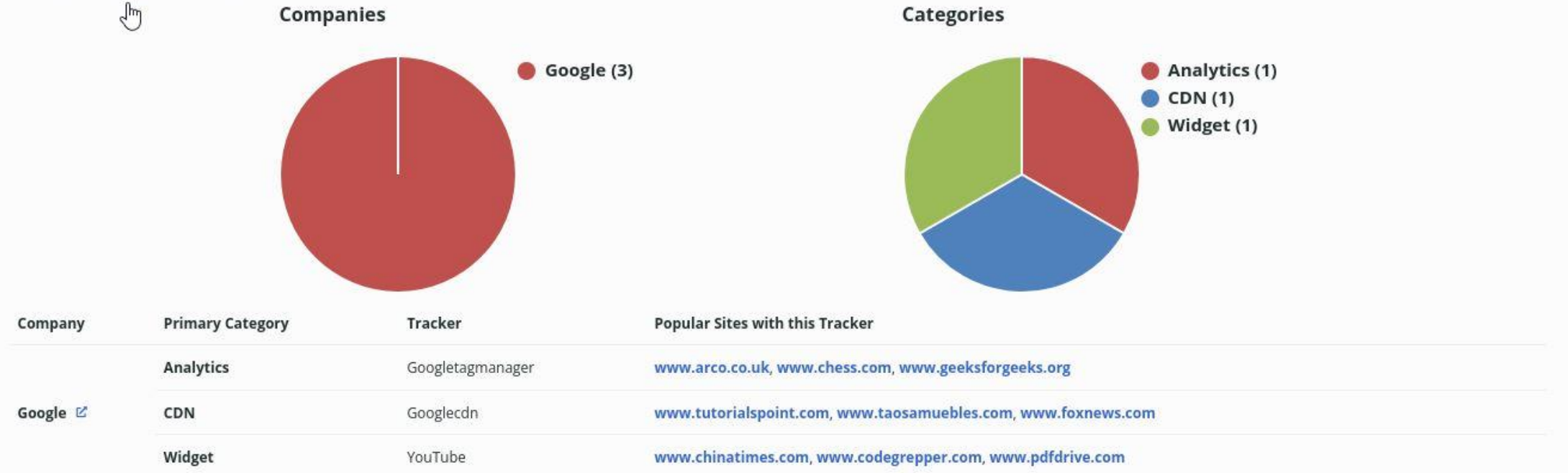| Netblock owner	IP address	OS	Web server	Last seen
▸ Amazon Data Services I...	3.7.218.202	Linux	nginx	23-Jun-2022
P.D.R Solutions FZC	216.10.242.46	Linux	Apache	22-Feb-2020

⬛ Sender Policy Framework

A host's Sender Policy Framework (SPF) describes who can send mail on its behalf. This is done by publishing an SPF record containing a series of **rules** ⬀. Each rule consists of a qualifier followed by a specification of which domains to apply this qualifier to. For more information please see **open-spf.org** ⬀.

Qualifier	Mechanism	Argument
+ (Pass)	a	
+ (Pass)	mx	
+ (Pass)	a	**ec2-3-7-218-202.ap-south-1.compute.amazonaws.com**
+ (Pass)	include	**_spf.google.com**
~ (SoftFail)	all	

⬛ Web Trackers

Web Trackers are third-party resources loaded onto a webpage. Trackable resources include social sharing widgets, javascript files, and images. These trackers can be used to monitor individual user behaviour across the web. Data derived from these trackers are primarily used for advertising or analytics purposes.

3 known trackers were identified.

Companies

Google (3)

Categories

Analytics (1)
CDN (1)
Widget (1)

Company	Primary Category	Tracker	Popular Sites with this Tracker
	Analytics	Googletagmanager	**www.arco.co.uk, www.chess.com, www.geeksforgeeks.org**
Google ⬀	**CDN**	Googlecdn	**www.tutorialspoint.com, www.taosamuebles.com, www.foxnews.com**
	Widget	YouTube	**www.chinatimes.com, www.codegrepper.com, www.pdfdrive.com**

⬛ Site Technology (fetched today)

Cloud & PaaS

Cloud computing is the use of computing resources (hardware and software) that are delivered as a service over a network (typically the Internet). Platform as a service (PaaS) is a category of cloud computing services that provide a computing platform and a solution stack as a service.

Technology	Description	Popular sites using this technology
Amazon Web Services - EC2 ⬀	Cloud computing service (Elastic Compute Cloud)	**www.epicgames.com, www.netflix.com, app.grammarly.com**

Server-Side

Includes all the main technologies that Netcraft detects as running on the server such as PHP.

Technology	Description	Popular sites using this technology
PHP ⬀	PHP is supported and/or running	**www.tutorialspoint.com, www.ghanaweb.com, arstechnica.com**
XML	*No description*	**www.ecosia.org, www.virustotal.com, gist.github.com**
SSL ⬀	A cryptographic protocol providing communication security over the Internet	
PHP Enabled ⬀	Server supports PHP	**www.sigmalive.com, www3.animeflv.net, www.northamericanweather.net**

Client-Side

Includes all the main technologies that run on the browser (such as JavaScript and Adobe Flash).

Technology	Description	Popular sites using this technology
Asynchronous Javascript	*No description*	www.paypal.com, www.foxnews.com, www.linkedin.com
JavaScript ⬈	Widely-supported programming language commonly used to power client-side dynamic content on websites	www.google.com, twitter.com, my308053-sso.crm.ondemand.com

Client-Side Scripting Frameworks

Frameworks or libraries allow for easier development of applications by providing an Application Program Interface (API) or a methodology to follow whilst developing.

Technology	Description	Popular sites using this technology
Underscore.js	*No description*	www.commbank.com.au, www.rbcroyalbank.com, www.cisco.com
Google Tag Manager ⬈	*No description*	www.chess.com, www.duolingo.com, www.researchgate.net
jQuery ⬈	A JavaScript library used to simplify the client-side scripting of HTML	www.msn.com, www.xnxx.com, www.cnblogs.com

Blog

Blog software is software designed to simplify creating and maintaining weblogs. They are specialized content management systems that support the authoring, editing, and publishing of blog posts and comments.

Technology	Description	Popular sites using this technology
WordPress Self-Hosted ⬈	Free and open source blogging tool and a content management system (CMS) based on PHP and MySQL (hosted independently)	www.myjoyonline.com, www.hackerrank.com, www.tecmint.com

PHP Application

PHP is an open source server-side scripting language designed for Web development to produce dynamic Web pages.

Technology	Description	Popular sites using this technology
WordPress ⬈	Free and open source blogging tool and a content management system (CMS) based on PHP and MySQL	jobs.lever.co, aules.edu.gva.es, lost-ark.maxroll.gg

RSS Feed

RSS Rich Site Summary is a family of web feed formats used to publish frequently updated works such as blog entries, news headlines, audio, and video in a standardized format.

Technology	Description	Popular sites using this technology
RSS ⬈	Standardized web feed format used to publish frequently updated works	www.theguardian.com, www.marca.com, www.geeksforgeeks.org

Web Stats

Web analytics is the measurement, collection, analysis and reporting of internet data for purposes of understanding and optimizing web usage.

Technology	Description	Popular sites using this technology
Google Webmaster Tools ⬈	Set of tools allowing webmasters to check indexing status and optimize visibility of their websites on Google	www.aliexpress.com, www.pinterest.com, www.disneyplus.com

Character Encoding

A character encoding system consists of a code that pairs each character from a given repertoire with something else such as a bit pattern, sequence of natural numbers, octets, or electrical pulses in order to facilitate the transmission of data (generally numbers or text) through telecommunication networks or for data storage.

Technology	Description	Popular sites using this technology
UTF8 ⬈	UCS Transformation Format 8 bit	

HTTP Compression

HTTP compression is a capability that can be built into web servers and web clients to make better use of available bandwidth, and provide greater transmission speeds between both.

Technology	Description	Popular sites using this technology
Gzip Content Encoding ☒	Gzip HTTP Compression protocol	www.seznam.cz, www.pole-emploi.fr, www.amazon.in

Doctype

A Document Type Declaration, or DOCTYPE, is an instruction that associates a particular SGML or XML document (for example, a webpage) with a Document Type Definition (DTD).

Technology	Description	Popular sites using this technology
HTML5 ☒	Latest revision of the HTML standard, the main markup language on the web	accounts.google.com, mail-redir.mention.com, outlook.live.com

HTML 5

HTML5 is a markup language for structuring and presenting content for the World Wide Web and a core technology of the Internet. It is the fifth revision of the HTML standard.

Technology	Description	Popular sites using this technology
Viewport meta tag	HTML5 tag usually used for mobile optimization	www.startpage.com, login.live.com, web.whatsapp.com
Canvas Tag	HTML5 canvas tag	www.hackthebox.com, www.abv.bg, www.abcbourse.com

CSS Usage

Cascading Style Sheets (CSS) is a style sheet language used for describing the presentation semantics (the look and formatting) of a document written in a markup language (such as XHTML).

Technology	Description	Popular sites using this technology
External ☒	Styles defined within an external CSS file	www.canva.com, www.instagram.com, www.deepl.com
CSS Media Query	*No description*	www.w3schools.com, www.facebook.com, www.twitch.tv

2. SSL & TLS CERTIFICATION

🔲 SSL/TLS

Assurance	Domain validation	Perfect Forward Secrecy	Yes
Common name	lnct.ac.in	Supported TLS Extensions	RFC8446 ⬀ supported versions, RFC8446 ⬀ key share, RFC4366 ⬀ server name, RFC7301 ⬀ application-layer protocol negotiation
Organisation	Not Present	Application-Layer Protocol Negotiation	h2
State	Not Present	Next Protocol Negotiation	Not Present
Country	Not Present	Issuing organisation	Let's Encrypt
Organisational unit	Not Present	Issuer common name	R3
Subject Alternative Name	*.lnct.ac.in, lnct.ac.in	Issuer unit	Not Present
Validity period	From Jun 7 2022 to Sep 5 2022 (2 months, 3 weeks, 6 days)	Issuer location	Not Present
Matches hostname	Yes	Issuer country	🇺🇸 US
Server	nginx	Issuer state	Not Present
Public key algorithm	rsaEncryption	Certificate Revocation Lists	Not Present
Protocol version	TLSv1.3	Certificate Hash	fJMO3tz4ehQEObtHrPtWVxsLwQ4
Public key length	2048	Public Key Hash	3bcac9be38a8f1e78328964333042aa5788466ad1b6bc07db960f9fa41e5f1f8
Certificate check	ok	OCSP servers	http://r3.o.lencr.org - 100% uptime in the past 24 hours 📈 Performance Graph
Signature algorithm	sha256WithRSAEncryption	OCSP stapling response	No response received
Serial number	0x036bcf4ac990f2cbe2c716a643eb897822c2		
Cipher	TLS_AES_256_GCM_SHA384		
Version number	0x02		

Certificate Transparency

Signed Certificate Timestamps (SCTs)

Source	Log	Timestamp	Signature Verification
Certificate	Cloudflare Nimbus 2022 QcjKsd8iRkoQxqE6CUKHXk4xixsD6+tLx2jwkGKWBvY=	2022-06-07 02:29:15	Success
Certificate	Google Argon 2022 KXm+8J450SHwVnOfY6V35b5XfZxgCvj5TV0mXCVdx4Q=	2022-06-07 02:29:15	Success

SSLv3/POODLE

This site does not support the SSL version 3 protocol.

More information about SSL version 3 and the POODLE vulnerability.

Heartbleed

The site did not offer the Heartbeat TLS extension prior to the Heartbleed disclosure, and so was not exploitable.

🔲 SSL Certificate Chain

Common name	ISRG Root X1
Organisational unit	Not Present
Organisation	Internet Security Research Group
Validity period	From 2015-06-04 to 2035-06-04

↓

Common name	R3
Organisational unit	Not Present
Organisation	Let's Encrypt
Validity period	From 2020-09-04 to 2025-09-15

Qualys ssl lab test report

SSL Report: Inct.ac.in (3.7.218.202)

Assessed on: Fri, 24 Jun 2022 18:16:34 UTC | Hide | Clear cache

Scan Another »

Summary

Overall Rating

B

Certificate
Protocol Support
Key Exchange
Cipher Strength

0   20   40   60   80   100

Visit our documentation page for more information, configuration guides, and books. Known issues are documented here.

This server supports TLS 1.0 and TLS 1.1. Grade capped to B. MORE INFO »

This site works only in browsers with SNI support.

This server supports TLS 1.3.

Certificate #1: RSA 2048 bits (SHA256withRSA)

Server Key and Certificate #1

Subject	Inct.ac.in Fingerprint SHA256: 1f4380b1a643fd94008baeaed6e6ad11570604366682f244d5ee95cb0fa4ebed6 Pin SHA256: O8rJvjio8eeDKJZDMwQqpXiEZq0ba8B9uWD5+kHI8fg=
Common names	Inct.ac.in
Alternative names	*.Inct.ac.in Inct.ac.in
Serial Number	036bcf4ac990f2cbe2c716a643eb897822c2
Valid from	Tue, 07 Jun 2022 01:29:14 UTC
Valid until	Mon, 05 Sep 2022 01:29:13 UTC (expires in 2 months and 10 days)
Key	RSA 2048 bits (e 65537)
Weak key (Debian)	No
Issuer	R3 AIA: http://r3.i.lencr.org/
Signature algorithm	SHA256withRSA
Extended Validation	No
Certificate Transparency	Yes (certificate)
OCSP Must Staple	No
Revocation information	OCSP OCSP: http://r3.o.lencr.org
Revocation status	Good (not revoked)
DNS CAA	No (more info)
Trusted	Yes Mozilla Apple Android Java Windows

Certification Paths

Path #1: Trusted

1	Sent by server	**lnct.ac.in** Fingerprint SHA256: 1f4380b1a643fd94008baeaed6e6ad1157060436682f244d5ee95cb0fa4ebed6 Pin SHA256: O8rJvjio8eeDKJZDMwQqpXiEZq0ba8B9uWD5+kHI8fg= RSA 2048 bits (e 65537) / SHA256withRSA
2	Sent by server	**R3** Fingerprint SHA256: 67add1166b020ae61b8f5fc96813c04c2aa589960796865572a3c7e737613dfd Pin SHA256: jQJTblh0grw0/1TkHSumWb+Fs0Ggogr621gT3PvPKG0= RSA 2048 bits (e 65537) / SHA256withRSA
3	In trust store	**ISRG Root X1** Self-signed Fingerprint SHA256: 96bcec06264976f37460779acf28c5a7cfe8a3c0aae11a8ffcee05c0bddf08c6 Pin SHA256: C5+lpZ7tcVwmwQIMcRtPbsQtWLABXhQzejna0wHFr8M= RSA 4096 bits (e 65537) / SHA256withRSA

Path #2: Not trusted (invalid certificate [Fingerprint SHA256: 0687260331a72403d909f105e69bcf0d32e1bd2493ffc6d9206d11bcd6770739])

1	Sent by server	**lnct.ac.in** Fingerprint SHA256: 1f4380b1a643fd94008baeaed6e6ad1157060436682f244d5ee95cb0fa4ebed6 Pin SHA256: O8rJvjio8eeDKJZDMwQqpXiEZq0ba8B9uWD5+kHI8fg= RSA 2048 bits (e 65537) / SHA256withRSA
2	Sent by server	**R3** Fingerprint SHA256: 67add1166b020ae61b8f5fc96813c04c2aa589960796865572a3c7e737613dfd Pin SHA256: jQJTblh0grw0/1TkHSumWb+Fs0Ggogr621gT3PvPKG0= RSA 2048 bits (e 65537) / SHA256withRSA
3	Sent by server	**ISRG Root X1** Fingerprint SHA256: 6d99fb265eb1c5b3744765fcbc648f3cd8e1bffafdc4c2f99b9d47cf7ff1c24f Pin SHA256: C5+lpZ7tcVwmwQIMcRtPbsQtWLABXhQzejna0wHFr8M= RSA 4096 bits (e 65537) / SHA256withRSA
4	In trust store	**DST Root CA X3** Self-signed Fingerprint SHA256: 0687260331a72403d909f105e69bcf0d32e1bd2493ffc6d9206d11bcd6770739 Pin SHA256: Vjs8r4z+80wjNcr1YKepWQboSIRi63WsWXhIMN+eWys= RSA 2048 bits (e 65537) / SHA1withRSA Valid until: Thu, 30 Sep 2021 14:01:15 UTC **EXPIRED** Weak or insecure signature, but no impact on root certificate

Certificate #2: RSA 2048 bits (SHA256withRSA) No SNI

Server Key and Certificate #1

Subject	Plesk Fingerprint SHA256: cec77202ec886e73b85ba867be2daa908b6f6e2be9f539570448030a7f43fa30 Pin SHA256: 7y0//v05mE/y68EI1jGGxS2LEBLtt60KE/fzsvgGMjE=
Common names	Plesk
Alternative names	- INVALID
Serial Number	5ec8d71e
Valid from	Sat, 23 May 2020 07:56:15 UTC
Valid until	Sun, 23 May 2021 07:56:15 UTC (expired 1 year and 1 month ago) EXPIRED
Key	RSA 2048 bits (e 65537)
Weak key (Debian)	No
Issuer	Plesk Self-signed
Signature algorithm	SHA256withRSA
Extended Validation	No
Certificate Transparency	No
OCSP Must Staple	No
Revocation information	None
Trusted	No NOT TRUSTED Mozilla Apple Android Java Windows

Additional Certificates (if supplied)

Certificates provided	1 (863 bytes)
Chain issues	None

Certification Paths

Mozilla Apple Android Java Windows

Path #1: Not trusted (path does not chain to a trusted anchor)

1	Sent by server Not in trust store	Plesk Self-signed Fingerprint SHA256: cec77202ec886e73b85ba867be2daa908b6f6e2be9f539570448030a7f43fa30 Pin SHA256: 7y0//v05mE/y68EI1jGGxS2LEBLtt60KE/fzsvgGMjE= RSA 2048 bits (e 65537) / SHA256withRSA Valid until: Sun, 23 May 2021 07:56:15 UTC EXPIRED

ROBOT (vulnerability)	No (more info)
Forward Secrecy	With modern browsers (more info)
ALPN	Yes h2 http/1.1
NPN	Yes h2 http/1.1
Session resumption (caching)	**No (IDs assigned but not accepted)**
Session resumption (tickets)	Yes
OCSP stapling	No
Strict Transport Security (HSTS)	No
HSTS Preloading	Not in: Chrome Edge Firefox IE
Public Key Pinning (HPKP)	No (more info)
Public Key Pinning Report-Only	No
Public Key Pinning (Static)	No (more info)
Long handshake intolerance	No
TLS extension intolerance	No
TLS version intolerance	No
Incorrect SNI alerts	No
Uses common DH primes	No, DHE suites not supported
DH public server param (Ys) reuse	No, DHE suites not supported
ECDH public server param reuse	No
Supported Named Groups	x25519, secp256r1, x448, secp521r1, secp384r1 (server preferred order)
SSL 2 handshake compatibility	Yes
0-RTT enabled	No

HTTP Requests

1 https://lnct.ac.in/ (HTTP/1.1 200 OK)

Miscellaneous

Test date	Sat, 25 Jun 2022 12:01:36 UTC
Test duration	221.969 seconds
HTTP status code	200
HTTP server signature	nginx
Server hostname	ec2-3-7-218-202.ap-south-1.compute.amazonaws.com

Configuration

Protocols

TLS 1.3	Yes
TLS 1.2	Yes*
TLS 1.1	Yes
TLS 1.0	Yes*
SSL 3	No
SSL 2	No

(*) Experimental: Server negotiated using No-SNI

Cipher Suites

TLS 1.3 (suites in server-preferred order) ⊟

TLS_AES_256_GCM_SHA384 (0x1302) ECDH x25519 (eq. 3072 bits RSA) FS	256
TLS_CHACHA20_POLY1305_SHA256 (0x1303) ECDH x25519 (eq. 3072 bits RSA) FS	256
TLS_AES_128_GCM_SHA256 (0x1301) ECDH x25519 (eq. 3072 bits RSA) FS	128

TLS 1.2 (suites in server-preferred order) ⊟

TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (0xc02f) ECDH x25519 (eq. 3072 bits RSA) FS	128
TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (0xc030) ECDH x25519 (eq. 3072 bits RSA) FS	256
TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256 (0xcca8) ECDH x25519 (eq. 3072 bits RSA) FS	256
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 (0xc027) ECDH x25519 (eq. 3072 bits RSA) FS WEAK	128
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 (0xc028) ECDH x25519 (eq. 3072 bits RSA) FS WEAK	256
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (0xc013) ECDH x25519 (eq. 3072 bits RSA) FS WEAK	128
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (0xc014) ECDH x25519 (eq. 3072 bits RSA) FS WEAK	256
TLS_ECDHE_RSA_WITH_ARIA_256_GCM_SHA384 (0xc061) ECDH x25519 (eq. 3072 bits RSA) FS	256
TLS_ECDHE_RSA_WITH_ARIA_128_GCM_SHA256 (0xc060) ECDH x25519 (eq. 3072 bits RSA) FS	128
TLS_ECDHE_RSA_WITH_CAMELLIA_256_CBC_SHA384 (0xc077) ECDH x25519 (eq. 3072 bits RSA) FS WEAK	256
TLS_ECDHE_RSA_WITH_CAMELLIA_128_CBC_SHA256 (0xc076) ECDH x25519 (eq. 3072 bits RSA) FS WEAK	128
TLS_RSA_WITH_AES_128_GCM_SHA256 (0x9c) WEAK	128
TLS_RSA_WITH_AES_256_GCM_SHA384 (0x9d) WEAK	256
TLS_RSA_WITH_AES_128_CBC_SHA256 (0x3c) WEAK	128

TLS_RSA_WITH_AES_256_CBC_SHA256 (0x3d) **WEAK**	256
TLS_RSA_WITH_AES_128_CBC_SHA (0x2f) **WEAK**	128
TLS_RSA_WITH_AES_256_CBC_SHA (0x35) **WEAK**	256
TLS_RSA_WITH_AES_256_CCM_8 (0xc0a1) **WEAK**	256
TLS_RSA_WITH_AES_256_CCM (0xc09d) **WEAK**	256
TLS_RSA_WITH_ARIA_256_GCM_SHA384 (0xc051) **WEAK**	256
TLS_RSA_WITH_AES_128_CCM_8 (0xc0a0) **WEAK**	128
TLS_RSA_WITH_AES_128_CCM (0xc09c) **WEAK**	128
TLS_RSA_WITH_ARIA_128_GCM_SHA256 (0xc050) **WEAK**	128
TLS_RSA_WITH_CAMELLIA_256_CBC_SHA256 (0xc0) **WEAK**	256
TLS_RSA_WITH_CAMELLIA_128_CBC_SHA256 (0xba) **WEAK**	128
TLS_RSA_WITH_CAMELLIA_256_CBC_SHA (0x84) **WEAK**	256
TLS_RSA_WITH_CAMELLIA_128_CBC_SHA (0x41) **WEAK**	128

 # TLS 1.1 (suites in server-preferred order) ⊟

TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (0xc013) ECDH x25519 (eq. 3072 bits RSA) FS **WEAK**	128
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (0xc014) ECDH x25519 (eq. 3072 bits RSA) FS **WEAK**	256
TLS_RSA_WITH_AES_128_CBC_SHA (0x2f) **WEAK**	128
TLS_RSA_WITH_AES_256_CBC_SHA (0x35) **WEAK**	256
TLS_RSA_WITH_CAMELLIA_256_CBC_SHA (0x84) **WEAK**	256
TLS_RSA_WITH_CAMELLIA_128_CBC_SHA (0x41) **WEAK**	128

 # TLS 1.0 (suites in server-preferred order) ⊟

TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (0xc013) ECDH x25519 (eq. 3072 bits RSA) FS **WEAK**	128
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (0xc014) ECDH x25519 (eq. 3072 bits RSA) FS **WEAK**	256
TLS_RSA_WITH_AES_128_CBC_SHA (0x2f) **WEAK**	128
TLS_RSA_WITH_AES_256_CBC_SHA (0x35) **WEAK**	256
TLS_RSA_WITH_CAMELLIA_256_CBC_SHA (0x84) **WEAK**	256
TLS_RSA_WITH_CAMELLIA_128_CBC_SHA (0x41) **WEAK**	128

Handshake Simulation

Client	Cert	Protocol	Cipher Suite	
Android 2.3.7 No SNI [2]	Incorrect certificate because this client doesn't support SNI RSA 2048 (SHA256) | TLS 1.0 | TLS_RSA_WITH_AES_128_CBC_SHA			
Android 4.0.4	RSA 2048 (SHA256)	TLS 1.0	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA ECDH secp256r1 FS	
Android 4.1.1	RSA 2048 (SHA256)	TLS 1.0	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA ECDH secp256r1 FS	
Android 4.2.2	RSA 2048 (SHA256)	TLS 1.0	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA ECDH secp256r1 FS	
Android 4.3	RSA 2048 (SHA256)	TLS 1.0	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA ECDH secp256r1 FS	
Android 4.4.2	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 ECDH secp256r1 FS	
Android 5.0.0	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 ECDH secp256r1 FS	
Android 6.0	RSA 2048 (SHA256)	TLS 1.2 > http/1.1	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 ECDH secp256r1 FS	
Android 7.0	RSA 2048 (SHA256)	TLS 1.2 > h2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 ECDH x25519 FS	
Android 8.0	RSA 2048 (SHA256)	TLS 1.2 > h2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 ECDH x25519 FS	
Android 8.1	-	TLS 1.3	TLS_AES_256_GCM_SHA384 ECDH x25519 FS	
Android 9.0	-	TLS 1.3	TLS_AES_256_GCM_SHA384 ECDH x25519 FS	
Baidu Jan 2015	RSA 2048 (SHA256)	TLS 1.0	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA ECDH secp256r1 FS	
BingPreview Jan 2015	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 ECDH secp256r1 FS	
Chrome 49 / XP SP3	RSA 2048 (SHA256)	TLS 1.2 > h2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 ECDH secp256r1 FS	
Chrome 69 / Win 7 R	RSA 2048 (SHA256)	TLS 1.2 > h2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 ECDH x25519 FS	
Chrome 70 / Win 10	-	TLS 1.3	TLS_AES_256_GCM_SHA384 ECDH x25519 FS	
Chrome 80 / Win 10 R	-	TLS 1.3	TLS_AES_256_GCM_SHA384 ECDH x25519 FS	
Firefox 31.3.0 ESR / Win 7	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 ECDH secp256r1 FS	
Firefox 47 / Win 7 R	RSA 2048 (SHA256)	TLS 1.2 > h2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 ECDH secp256r1 FS	
Firefox 49 / XP SP3	RSA 2048 (SHA256)	TLS 1.2 > h2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 ECDH secp256r1 FS	
Firefox 62 / Win 7 R	RSA 2048 (SHA256)	TLS 1.2 > h2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 ECDH x25519 FS	
Firefox 73 / Win 10 R	-	TLS 1.3	TLS_AES_256_GCM_SHA384 ECDH x25519 FS	
Googlebot Feb 2018	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 ECDH x25519 FS	
IE 7 / Vista	RSA 2048 (SHA256)	TLS 1.0	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA ECDH secp256r1 FS	

Client	Cert	Protocol	Cipher Suite	
IE 7 / Vista	RSA 2048 (SHA256)	TLS 1.0	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA	ECDH secp256r1 FS
IE 8 / XP No FS [1] No SNI [2]	Server sent fatal alert: handshake_failure			
IE 8-10 / Win 7 R	RSA 2048 (SHA256)	TLS 1.0	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA	ECDH secp256r1 FS
IE 11 / Win 7 R	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256	ECDH secp256r1 FS
IE 11 / Win 8.1 R	RSA 2048 (SHA256)	TLS 1.2 > http/1.1	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256	ECDH secp256r1 FS
IE 10 / Win Phone 8.0	RSA 2048 (SHA256)	TLS 1.0	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA	ECDH secp256r1 FS
IE 11 / Win Phone 8.1 R	RSA 2048 (SHA256)	TLS 1.2 > http/1.1	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256	ECDH secp256r1 FS
IE 11 / Win Phone 8.1 Update R	RSA 2048 (SHA256)	TLS 1.2 > http/1.1	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256	ECDH secp256r1 FS
IE 11 / Win 10 R	RSA 2048 (SHA256)	TLS 1.2 > h2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	ECDH secp256r1 FS
Edge 15 / Win 10 R	RSA 2048 (SHA256)	TLS 1.2 > h2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	ECDH x25519 FS
Edge 16 / Win 10 R	RSA 2048 (SHA256)	TLS 1.2 > h2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	ECDH x25519 FS
Edge 18 / Win 10 R	RSA 2048 (SHA256)	TLS 1.2 > h2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	ECDH x25519 FS
Edge 13 / Win Phone 10 R	RSA 2048 (SHA256)	TLS 1.2 > h2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	ECDH secp256r1 FS
Java 6u45 No SNI [2]	Incorrect certificate because this client doesn't support SNI RSA 2048 (SHA256)	TLS 1.0	TLS_RSA_WITH_AES_128_CBC_SHA		
Java 7u25	RSA 2048 (SHA256)	TLS 1.0	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA	ECDH secp256r1 FS
Java 8u161	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	ECDH secp256r1 FS
Java 11.0.3	-	TLS 1.3	TLS_AES_256_GCM_SHA384	ECDH secp256r1 FS
Java 12.0.1	-	TLS 1.3	TLS_AES_256_GCM_SHA384	ECDH secp256r1 FS
OpenSSL 0.9.8y	RSA 2048 (SHA256)	TLS 1.0	TLS_RSA_WITH_AES_128_CBC_SHA No FS	
OpenSSL 1.0.1l R	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	ECDH secp256r1 FS
OpenSSL 1.0.2s R	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	ECDH secp256r1 FS
OpenSSL 1.1.0k R	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	ECDH x25519 FS
OpenSSL 1.1.1c R	-	TLS 1.3	TLS_AES_256_GCM_SHA384	ECDH x25519 FS
Safari 5.1.9 / OS X 10.6.8	RSA 2048 (SHA256)	TLS 1.0	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA	ECDH secp256r1 FS
Safari 6 / iOS 6.0.1	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256	ECDH secp256r1 FS
Safari 6.0.4 / OS X 10.8.4 R	RSA 2048 (SHA256)	TLS 1.0	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA	ECDH secp256r1 FS
Safari 7 / iOS 7.1 R	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256	ECDH secp256r1 FS
Safari 7 / OS X 10.9 R	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256	ECDH secp256r1 FS
Safari 8 / iOS 8.4 R	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256	ECDH secp256r1 FS
Safari 8 / OS X 10.10 R	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256	ECDH secp256r1 FS
Safari 9 / iOS 9 R	RSA 2048 (SHA256)	TLS 1.2 > h2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	ECDH secp256r1 FS
Safari 9 / OS X 10.11 R	RSA 2048 (SHA256)	TLS 1.2 > h2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	ECDH secp256r1 FS
Safari 10 / iOS 10 R	RSA 2048 (SHA256)	TLS 1.2 > h2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	ECDH secp256r1 FS
Safari 12.1.2 / MacOS 10.14.6 Beta R	-	TLS 1.3	TLS_AES_256_GCM_SHA384	ECDH x25519 FS
Safari 12.1.1 / iOS 12.3.1 R	-	TLS 1.3	TLS_AES_256_GCM_SHA384	ECDH x25519 FS
Apple ATS 9 / iOS 9 R	RSA 2048 (SHA256)	TLS 1.2 > h2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	ECDH secp256r1 FS
Yahoo Slurp Jan 2015	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	ECDH secp256r1 FS
YandexBot Jan 2015	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	ECDH secp256r1 FS

Not simulated clients (Protocol mismatch)   ⊟

IE 6 / XP No FS [1] No SNI [2]	Protocol mismatch (not simulated)

(1) Clients that do not support Forward Secrecy (FS) are excluded when determining support for it.

(2) No support for virtual SSL hosting (SNI). Connects to the default site if the server uses SNI.

(3) Only first connection attempt simulated. Browsers sometimes retry with a lower protocol version.

(R) Denotes a reference browser or client, with which we expect better effective security.

(All) We use defaults, but some platforms do not use their best protocols and features (e.g., Java 6 & 7, older IE).

(All) Certificate trust is not checked in handshake simulation, we only perform TLS handshake.

Protocol Details

DROWN	No, server keys and hostname not seen elsewhere with SSLv2 **(1) For a better understanding of this test, please read this longer explanation** (2) Key usage data kindly provided by the Censys network search engine; original DROWN website here (3) Censys data is only indicative of possible key and certificate reuse; possibly out-of-date and not complete
Secure Renegotiation	**Supported**
Secure Client-Initiated Renegotiation	No
Insecure Client-Initiated Renegotiation	No
BEAST attack	Not mitigated server-side (more info) TLS 1.0: 0xc013
POODLE (SSLv3)	No, SSL 3 not supported (more info)
POODLE (TLS)	No (more info)
Zombie POODLE	No (more info) TLS 1.2 : 0xc027
GOLDENDOODLE	No (more info) TLS 1.2 : 0xc027
OpenSSL 0-Length	No (more info) TLS 1.2 : 0xc027
Sleeping POODLE	No (more info) TLS 1.2 : 0xc027
Downgrade attack prevention	**Yes, TLS_FALLBACK_SCSV supported (more info)**
SSL/TLS compression	No
RC4	No
Heartbeat (extension)	No
Heartbleed (vulnerability)	No (more info)

ROBOT (vulnerability)	No (more info)
Forward Secrecy	With modern browsers (more info)
ALPN	Yes h2 http/1.1
NPN	Yes h2 http/1.1
Session resumption (caching)	No (IDs assigned but not accepted)
Session resumption (tickets)	Yes
OCSP stapling	No
Strict Transport Security (HSTS)	No
HSTS Preloading	Not in: Chrome Edge Firefox IE
Public Key Pinning (HPKP)	No (more info)
Public Key Pinning Report-Only	No
Public Key Pinning (Static)	No (more info)
Long handshake intolerance	No
TLS extension intolerance	No
TLS version intolerance	No
Incorrect SNI alerts	No
Uses common DH primes	No, DHE suites not supported
DH public server param (Ys) reuse	No, DHE suites not supported
ECDH public server param reuse	No
Supported Named Groups	x25519, secp256r1, x448, secp521r1, secp384r1 (server preferred order)
SSL 2 handshake compatibility	Yes
0-RTT enabled	No

HTTP Requests

1 https://lnct.ac.in/ (HTTP/1.1 200 OK)

Miscellaneous

Test date	Sat, 25 Jun 2022 12:01:36 UTC
Test duration	221.969 seconds
HTTP status code	200
HTTP server signature	nginx
Server hostname	ec2-3-7-218-202.ap-south-1.compute.amazonaws.com

3.<u>FINDING SUBDOMAINS</u>

Subdomain	IP address	OS	Server	Technology	Web Platform	Page Title
lnct.ac.in	3.7.218.202		nginx	PHP 7.3.33, PleskLin	WordPress 5.8.4	LNCT College | Top Engineering Colleges In Central India
ns1.lnct.ac.in	3.7.218.202		nginx	PHP		Plesk Obsidian 18.0.44
ns2.lnct.ac.in	3.7.218.202		nginx	PHP		Plesk Obsidian 18.0.44
ftp.lnct.ac.in	3.7.218.202		nginx	PHP		Plesk Obsidian 18.0.44
blog.lnct.ac.in	3.7.218.202		nginx	PHP 7.3.33, PleskLin	WordPress 5.7.6	LNCT Blog Post - LNCT Group Of Colleges
www.lnct.ac.in	3.7.218.202		nginx	PHP 7.3.33, PleskLin	WordPress 5.8.4	LNCT College | Top Engineering Colleges In Central India
mail.lnct.ac.in	3.7.218.202		nginx	PHP		Plesk Obsidian 18.0.44
conference.lnct.ac.in	3.7.218.202		nginx			International conference
webmail.lnct.ac.in	3.7.218.202		nginx	PHP 7.4.30		Roundcube Webmail :: Welcome to Roundcube Webmail

Subdomain	IP address	OS	Server	Technology	Web Platform	Page Title
portal.lnct.ac.in	103.85.92.198	Windows	Microsoft-IIS 8.5	ASP.NET		IIS Windows Server
erp.lnct.ac.in	103.134.249.220	Windows	Apache 2.4.51	PHP 7.3.33		403 Forbidden

Scan parameters

Domain:	lnct.ac.in
DNS records (NS, MX, TXT, AXFR):	On
DNS enumeration:	On
Certificate Transparency Logs:	Off
External APIs:	Off
Bing search:	Off
Google search:	Off
HTML links search :	Off
SSL search:	Off
Reverse DNS search:	Off
Smart DNS search:	Off
IP information:	False
Web technologies:	True
Include unresolved results:	False
DNS enumeration wordlist:	(1 words)

Scan information

Start time:	2022-06-23 19:11:28 UTC+03
Finish time:	2022-06-23 19:12:01 UTC+03
Scan duration:	33 sec

Subdomain	IP	Cloudflare
idealab.lnct.ac.in	3.7.218.202	
aic.lnct.ac.in	3.7.218.202	
grievance.lnct.ac.in	3.7.218.202	
jncterp1.lnct.ac.in	3.7.218.202	
fdp.lnct.ac.in	3.7.218.202	
blog.lnct.ac.in	3.7.218.202	
Idealab.lnct.ac.in	3.7.218.202	
admissions.lnct.ac.in	3.7.218.202	
hackathonclub.lnct.ac.in	3.7.218.202	
admission2021.lnct.ac.in	3.7.218.202	
covidhelp.lnct.ac.in	3.7.218.202	
ncc.lnct.ac.in	3.7.218.202	
rcds.lnct.ac.in	3.7.218.202	
lnctjbp.lnct.ac.in	3.7.218.202	
jnct.lnct.ac.in	3.7.218.202	
erp1.lnct.ac.in	103.85.92.220	
lncpbhopal.lnct.ac.in	3.7.218.202	
lnctbhopal.lnct.ac.in	3.7.218.202	
lnctindore.lnct.ac.in	3.7.218.202	
admissions2020.lnct.ac.in	3.7.218.202	
lnct.ac.in	3.7.218.202	
mail.lnct.ac.in	3.7.218.202	
www.lnct.ac.in	3.7.218.202	
lncte.lnct.ac.in	115.254.62.22	
jncterp.lnct.ac.in	103.85.93.99	
lncp.lnct.ac.in	115.254.62.21	
mca.lnct.ac.in	115.254.62.23	
lncts.lnct.ac.in	115.254.62.23	
mba.lnct.ac.in	115.254.62.23	
www.admissions2020.lnct.ac.in	3.7.218.202	
portal.lnct.ac.in	103.85.92.198	
erp.lnct.ac.in	103.134.249.220	
erp2.lnct.ac.in	103.85.92.197	
www.jnct.lnct.ac.in	3.7.218.202	
webmail.lnct.ac.in	3.7.218.202	
lnmc.lnct.ac.in	123.63.252.250	
erp.jnct.lnct.ac.in	none	
www.erp.jnct.lnct.ac.in	none	
www.lncte.lnct.ac.in	none	
www.jncterp.lnct.ac.in	none	
www.lncp.lnct.ac.in	none	
www.mca.lnct.ac.in	none	
www.lncts.lnct.ac.in	none	
www.mba.lnct.ac.in	none	
www.portal.lnct.ac.in	none	
lnct.lnct.ac.in	none	
www.lnct.lnct.ac.in	none	
www.erp.lnct.ac.in	none	
www.erp2.lnct.ac.in	none	
cpanel.lnct.ac.in	none	
webdisk.lnct.ac.in	none	
www.lnmc.lnct.ac.in	none	
lnnc.lnct.ac.in	none	
www.lnnc.lnct.ac.in	none	

4. FINDING HIDDEN LINKS

Anchor Text [Sort By Anchor]	URL [Sort]
https://lnct.ac.in/lnct-group/	https://lnct.ac.in/lnct-group/
Our Vision | Mission	https://lnct.ac.in/our-vision-mission/
Trust	https://lnct.ac.in/trust/
Credo	https://lnct.ac.in/credo/
https://lnct.ac.in/our-leadership/	https://lnct.ac.in/our-leadership/
Management	https://lnct.ac.in/lnct-group-management/
OSD (OFFICER ON SPECIAL DUTY)	https://lnct.ac.in/osd-officer-on-special-duty/
PRINCIPAL/DIRECTOR/DEAN	https://lnct.ac.in/principal-director-dean/
Eminent Faculties	https://lnct.ac.in/eminent-faculties/
Advisor	https://lnct.ac.in/adviser/
https://lnct.ac.in/infrastructure/	https://lnct.ac.in/infrastructure/
AUDITORIUM	https://lnct.ac.in/lnct-auditorium/
SEMINAR HALL	https://lnct.ac.in/seminar-hall/
PEARSON VUE Select Center	https://lnct.ac.in/gmat-test-center/
Digital Library	https://lnct.ac.in/digital-library/
Digital Classrooms	https://lnct.ac.in/digital-classrooms/
Health Care	https://lnct.ac.in/health-care/
Hostels	https://lnct.ac.in/hostels/
Transportation	https://lnct.ac.in/transportation/
LNCT NISP	https://lnct.ac.in/lnct-isp/
https://lnct.ac.in/committees/	https://lnct.ac.in/committees/
DISCIPLINARY COMMITTEE	https://lnct.ac.in/disciplinary-committee/
Other Committees	https://lnct.ac.in/other-committees/
ANTI-RAGGING COMMITTEE	https://lnct.ac.in/anti-ragging-committee/
LNCT	https://lnct.ac.in/wp-content/uploads/2022/04/LNCT_ALL.pdf
LNCT Excellence	https://lnct.ac.in/wp-content/uploads/2022/04/LNCTE_ALL.pdf
https://lnct.ac.in/wp-content/uploads/2022/04/LNCTS_ALL.pdf	https://lnct.ac.in/wp-content/uploads/2022/04/LNCTS_ALL.pdf
LNCT Pharmacy	https://lnct.ac.in/wp-content/uploads/2022/04/LNCP_ALL.pdf
LNCT MBA	https://lnct.ac.in/wp-content/uploads/2022/04/MBA_ALL.pdf
LNCT MCA	https://lnct.ac.in/wp-content/uploads/2022/04/MCA_ALL.pdf
PMKVY Guidelines	https://lnct.ac.in/wp-content/uploads/2019/05/PMKVY.pdf
Aicte Mous	https://lnct.ac.in/aicte-mous/
AICTE Pragati	https://lnct.ac.in/aicte-pragati/
PMKVY Course Details	https://lnct.ac.in/wp-content/uploads/2021/06/PMKVYCD.jpg
Accreditation Status	https://lnct.ac.in/home-page/accreditation-status/
MOOC Courses With Credits for B.Tech (RGPV...	https://lnct.ac.in/wp-content/uploads/2019/12/MOOC-Courses-with-credits-for-B.Tech-RGPV-students.pd
Academic Calendar	https://lnct.ac.in/academic-calendar/
Shift 1	https://lnct.ac.in/wp-content/uploads/2021/11/Shift1.pdf
Shift 2	https://lnct.ac.in/wp-content/uploads/2021/11/Shift2.pdf
International Journal of LNCT	http://www.ijlnct.org/
Grievance Redressal	https://lnct.ac.in/grievance-redressal/
LNCT	https://lnct.ac.in/lnct-college/
https://lnct.ac.in/lnct-and-science/	https://lnct.ac.in/lnct-and-science/
LNCT Excellence	https://lnct.ac.in/lnct-excellence-college/
LNCT MBA	https://lnct.ac.in/lnct-mba/
LNCT MCA	https://lnct.ac.in/master-of-computer-application/
LNCT (Bhopal) Indore Campus	https://lnct.ac.in/lnct-bpl-indore-campus/
LNCT Vidyapeeth University	https://lnctvu.ac.in
LNCT Jabalpur	https://lnctuj.com/
JNCT Bhopal	https://jnctbhopal.ac.in
LNCT University	https://lnctu.ac.in/
Rishiraj College	https://lnctrishiraj.ac.in
CEC Bilaspur	https://cecbilaspur.ac.in/
LNCT Pharmacy	https://lnct.ac.in/lnct-pharmacy/
Civil Engineering	https://lnct.ac.in/civil-engineering/
Chemical Engineering	https://lnct.ac.in/chemical-engineering/
Electrical and Electronics Engineering	https://lnct.ac.in/electrical-and-electronics-engineering/
Mechanical Engineering	https://lnct.ac.in/mechanical-engineering/
Electrical Engineering	https://lnct.ac.in/electrical-engineering/
Electronics and Communication Engineering	https://lnct.ac.in/electronics-and-communication-engineering/
Computer Science Engineering	https://lnct.ac.in/computer-science-engineering/
Information Technology Engineering	https://lnct.ac.in/information-technology-engineering/
https://lnct.ac.in/department-of-humanities/	https://lnct.ac.in/department-of-humanities/
Department of Engineering Chemistry	https://lnct.ac.in/department-of-engineering-chemistry/
Department of Engineering Mathematics	https://lnct.ac.in/department-of-engineering-mathematics/
Department of Engineering Physics	https://lnct.ac.in/department-of-engineering-physics/
New Student Registration	http://portal1.lnct.ac.in/Accsoft2/studentonlinecounseling.aspx
Admission-process	https://lnct.ac.in/admission-process/

Admission-enquiry	https://lnct.ac.in/admission-enquiry/
https://lnct.ac.in/online-payment/	https://lnct.ac.in/online-payment/
Fee Refund Policy	https://lnct.ac.in/fee-refund-policy/
LNCT MODEL UNITED NATIONS 2022	https://lnct.ac.in/lnct-model-united-nations-2022/
Career Development Cell	https://lnct.ac.in/career-development-cell/
Regular Activities	https://lnct.ac.in/regular-activities/
Placement Records	https://lnct.ac.in/placement-records/
Industry Interaction	https://lnct.ac.in/industry-interaction/
CISCO Academy	https://lnct.ac.in/cisco-academy/
Achievements	https://lnct.ac.in/achievements/
Coursera For LNCT	https://lnct.ac.in/1st-premier-educational-group-in-central-india-to-provide-coursera-certificate-courses/
Student Testimonial	https://lnct.ac.in/student-testimonial/
Kalchuri-LNCT Group Incubation Centre	https://lnct.ac.in/kalchuri-lnct-group-incubation-centre/
Triumph	https://lnct.ac.in/triumph-2k19/
https://lnct.ac.in/wp-content/uploads/2021/06/Research-Development.pdf	https://lnct.ac.in/wp-content/uploads/2021/06/Research-Development.pdf
Hackathon Club	https://hackathonclub.lnct.ac.in/
LNCT Literary Club	https://lnct.ac.in/lnct-literary-club/
Quest Nature Club	https://lnct.ac.in/quest-nature-club/
LNCT Photography Club	https://lnct.ac.in/lnct-photography-club/
LNCT Music Club	https://lnct.ac.in/lnct-music-club/
LNCT Gender Club	https://lnct.ac.in/lnct-gender-club/
Testimonial	https://lnct.ac.in/testimonial/
Activity Classes	https://lnct.ac.in/activity-classes/
Curricular and Technical Events	https://lnct.ac.in/curricular-and-technical-events/
Sports	https://lnct.ac.in/sports/
NSS	https://lnct.ac.in/nss/
NCC	https://ncc.lnct.ac.in/
LNCT Radio	https://lnct.ac.in/lnct-radio/
Recent Events	https://lnct.ac.in/recent-events/
GALLERY	https://lnct.ac.in/gallery/
New Online Registration	https://lnct.ac.in/online-registration-fees-and-provisional-admission-fee-payment/
Student Login (ERP Accsoft)	http://portal1.lnct.ac.in/Accsoft2/studentLogin.aspx
Employee Login (College ERP)	https://lnct.ac.in/Divert.html
Online Payment	https://lnct.ac.in/pay-fees-online/
Hall Booking APP	https://drive.google.com/file/d/1aty953Y2JctgE0gledpXDuBwiGiRB_s9/view?usp=sharing
Agnipath Yogna	https://lnct.ac.in/wp-content/uploads/2022/06/Agnipath-yojna.jpg
CSR	https://lnct.ac.in/corporate-social-responsibility/
Alumni	http://www.lnctalumni.in/
Admission 2022	https://admissions.lnct.ac.in/
Voice of LNCT	https://lnct.ac.in/wp-content/uploads/2022/03/VOICE-OF-LNCT-small.pdf
LNCT Bhopal	http://lnctbhopal.in/
LNCP Bhopal	http://lncpbhopal.in/
Tie-Up	https://lnct.ac.in/wp-content/uploads/2021/04/Lakshmi-Narain-College-of-Technology-ISTE-Certificate.pd
LNCT Blog	https://blog.lnct.ac.in
https://lnct.ac.in/contact/	https://lnct.ac.in/contact/
Career	https://lnct.ac.in/career/
Lakshmi Narain College of Technology (LNCT)	https://lnct.ac.in/top-engineering-colleges-in-bhopal/
Civil Engineering	https://lnct.ac.in/category/civil-engineering/
Expert lecture was organised for the 2nd Semester...	https://lnct.ac.in/expert-lecture-was-organised-for-the-2nd-semester-students-of-civil-engineering-branch
LNCP celebrated International Day of Yoga	https://lnct.ac.in/lncp-celebrated-international-day-of-yoga/
Robotics Workshop	https://lnct.ac.in/robotics-workshop/
Exchange Program at Bahra University	https://lnct.ac.in/exchange-program-at-bahra-university/
Close Campus Drive by Vitamax Healthcare Pvt Ltd	https://lnct.ac.in/close-campus-drive-by-vitamax-healthcare-pvt-ltd/
Time Table For Diploma Engineering Examinations -...	https://lnct.ac.in/time-table-for-diploma-engineering-examinations-june-2022/
LNCP Organising a Session on Yoga for Humanity	https://lnct.ac.in/lncp-organising-a-session-on-yoga-for-humanity/
Seminar on Digital Banking and Financial Inclusion	https://lnct.ac.in/seminar-on-digital-banking-and-financial-inclusion/
RGPV , EXAMS. 2022 (Revised)	https://lnct.ac.in/rgpv-exams-2022-revised/
LNCT Group of Colleges Bhopal	https://lnct.ac.in
LNCT University Bhopal	https://lnctu.ac.in
CEC Bilaspur Campus	https://csebilaspur.ac.in
LNCT Jabalpur Campus	https://lnctuj.com
Industry Testimonials	https://lnct.ac.in/industry-testimonials/
EDIIC	LNCT University	https://ediic.lnctu.ac.in/
NIRF	https://lnct.ac.in/the-national-institutional-ranking-framework/

Sr#	URL	Anchor
1	https://lnct.ac.in	Image
2	https://lnct.ac.in/lnct-group/	LNCT-Group
3	https://lnct.ac.in/our-vision-mission/	Our Vision	Mission
4	https://lnct.ac.in/trust/	Trust
5	https://lnct.ac.in/credo/	Credo
6	https://lnct.ac.in/our-leadership/	Our Leadership

7	https://lnct.ac.in/lnct-group-management/	Management
8	https://lnct.ac.in/osd-officer-on-special-duty/	OSD (OFFICER ON SPECIAL DUTY)
9	https://lnct.ac.in/principal-director-dean/	PRINCIPAL/DIRECTOR/DEAN
10	https://lnct.ac.in/eminent-faculties/	Eminent Faculties
11	https://lnct.ac.in/adviser/	Advisor
12	https://lnct.ac.in/infrastructure/	Infrastructure
13	https://lnct.ac.in/lnct-auditorium/	AUDITORIUM
14	https://lnct.ac.in/seminar-hall/	SEMINAR HALL
15	https://lnct.ac.in/gmat-test-center/	PEARSON VUE Select Center
16	https://lnct.ac.in/digital-library/	Digital Library
17	https://lnct.ac.in/digital-classrooms/	Digital Classrooms
18	https://lnct.ac.in/health-care/	Health Care
19	https://lnct.ac.in/hostels/	Hostels
20	https://lnct.ac.in/transportation/	Transportation
21	https://lnct.ac.in/lnct-isp/	LNCT NISP
22	https://lnct.ac.in/committees/	Committees
23	https://lnct.ac.in/disciplinary-committee/	DISCIPLINARY COMMITTEE
24	https://lnct.ac.in/other-committees/	Other Committees
25	https://lnct.ac.in/anti-ragging-committee/	ANTI-RAGGING COMMITTEE
26	https://lnct.ac.in/wp-content/uploads/2022/04/LNCT_ALL.pdf	LNCT
27	https://lnct.ac.in/wp-content/uploads/2022/04/LNCTE_ALL.pdf	LNCT Excellence
28	https://lnct.ac.in/wp-content/uploads/2022/04/LNCTS_ALL.pdf	LNCT & Science
29	https://lnct.ac.in/wp-content/uploads/2022/04/LNCP_ALL.pdf	LNCT Pharmacy
30	https://lnct.ac.in/wp-content/uploads/2022/04/MBA_ALL.pdf	LNCT MBA
31	https://lnct.ac.in/wp-content/uploads/2022/04/MCA_ALL.pdf	LNCT MCA
32	https://lnct.ac.in/wp-content/uploads/2019/05/PMKVY.pdf	PMKVY Guidelines
33	https://lnct.ac.in/aicte-mous/	Aicte Mous
34	https://lnct.ac.in/aicte-pragati/	AICTE Pragati
35	https://lnct.ac.in/wp-content/uploads/2021/06/PMKVYCD.jpg	PMKVY Course Details
36	https://lnct.ac.in/home-page/accreditation-status/	Accreditation Status
37	https://lnct.ac.in/wp-content/uploads/2019/12/MOOC-Courses-with-credits-for-B.Tech-RGPV-students.pdf	MOOC Courses With Credits for B.Tech (RGPV Students)
38	https://lnct.ac.in/academic-calendar/	Academic Calendar
39	https://lnct.ac.in/wp-content/uploads/2021/11/Shift1.pdf	Shift 1
40	https://lnct.ac.in/wp-content/uploads/2021/11/Shift2.pdf	Shift 2
41	http://www.ijlnct.org/	International Journal of LNCT
42	https://lnct.ac.in/grievance-redressal/	Grievance Redressal
43	https://lnct.ac.in/lnct-college/	LNCT
44	https://lnct.ac.in/lnct-and-science/	LNCT & Science
45	https://lnct.ac.in/lnct-excellence-college/	LNCT Excellence
46	https://lnct.ac.in/lnct-mba/	LNCT MBA
47	https://lnct.ac.in/master-of-computer-application/	LNCT MCA
48	https://lnct.ac.in/lnct-bpl-indore-campus/	LNCT (Bhopal) Indore Campus
49	https://lnctvu.ac.in	LNCT Vidyapeeth University
50	https://lnctuj.com/	LNCT Jabalpur
51	https://jnctbhopal.ac.in	JNCT Bhopal
52	https://lnctu.ac.in/	LNCT University
53	https://lnctrishiraj.ac.in	Rishiraj College
54	https://cecbilaspur.ac.in/	CEC Bilaspur
55	https://lnct.ac.in/lnct-pharmacy/	LNCT Pharmacy
56	https://lnct.ac.in/civil-engineering/	Civil Engineering
57	https://lnct.ac.in/chemical-engineering/	Chemical Engineering
58	https://lnct.ac.in/electrical-and-electronics-engineering/	Electrical and Electronics Engineering
59	https://lnct.ac.in/mechanical-engineering/	Mechanical Engineering
60	https://lnct.ac.in/electrical-engineering/	Electrical Engineering
61	https://lnct.ac.in/electronics-and-communication-engineering/	Electronics and Communication Engineering
62	https://lnct.ac.in/computer-science-engineering/	Computer Science Engineering
63	https://lnct.ac.in/information-technology-engineering/	Information Technology Engineering
64	https://lnct.ac.in/department-of-humanities/	Department of Humanities
65	https://lnct.ac.in/department-of-engineering-chemistry/	Department of Engineering Chemistry
66	https://lnct.ac.in/department-of-engineering-mathematics/	Department of Engineering Mathematics
67	https://lnct.ac.in/department-of-engineering-physics/	Department of Engineering Physics
68	http://portal1.lnct.ac.in/Accsoft2/studentonlinecounseling.aspx	New Student Registration
69	https://lnct.ac.in/admission-process/	Admission-process
70	https://lnct.ac.in/admission-enquiry/	Admission-enquiry
71	https://lnct.ac.in/online-payment/	T & C Online Payment
72	https://lnct.ac.in/fee-refund-policy/	Fee Refund Policy

73	https://lnct.ac.in/lnct-model-united-nations-2022/	LNCT MODEL UNITED NATIONS 2022
74	https://lnct.ac.in/career-development-cell/	Career Development Cell
75	https://lnct.ac.in/regular-activities/	Regular Activities
76	https://lnct.ac.in/placement-records/	Placement Records
77	https://lnct.ac.in/industry-interaction/	Industry Interaction
78	https://lnct.ac.in/cisco-academy/	CISCO Academy
79	https://lnct.ac.in/achievements/	Achievements
80	https://lnct.ac.in/1st-premier-educational-group-in-central-india-to-provide-coursera-certificate-courses/	Coursera For LNCT
81	https://lnct.ac.in/student-testimonial/	Student Testimonial
82	https://lnct.ac.in/kalchuri-lnct-group-incubation-centre/	Kalchuri-LNCT Group Incubation Centre
83	https://lnct.ac.in/triumph-2k19/	Triumph
84	https://lnct.ac.in/wp-content/uploads/2021/06/Research-Development.pdf	Research & Development
85	https://hackathonclub.lnct.ac.in/	Hackathon Club
86	https://lnct.ac.in/lnct-literary-club/	LNCT Literary Club
87	https://lnct.ac.in/quest-nature-club/	Quest Nature Club
88	https://lnct.ac.in/lnct-photography-club/	LNCT Photography Club
89	https://lnct.ac.in/lnct-music-club/	LNCT Music Club
90	https://lnct.ac.in/lnct-gender-club/	LNCT Gender Club
91	https://lnct.ac.in/testimonial/	Testimonial
92	https://lnct.ac.in/activity-classes/	Activity Classes
93	https://lnct.ac.in/curricular-and-technical-events/	Curricular and Technical Events
94	https://lnct.ac.in/sports/	Sports
95	https://lnct.ac.in/nss/	NSS
96	https://ncc.lnct.ac.in/	NCC
97	https://lnct.ac.in/lnct-radio/	LNCT Radio
98	https://lnct.ac.in/recent-events/	Recent Events
99	https://lnct.ac.in/gallery/	GALLERY
100	https://lnct.ac.in/online-registration-fees-and-provisional-admission-fee-payment/	New Online Registration
101	http://portal1.lnct.ac.in/Accsoft2/studentLogin.aspx	Student Login (ERP Accsoft)
102	https://lnct.ac.in/Divert.html	Employee Login (College ERP)
103	https://lnct.ac.in/pay-fees-online/	Online Payment
104	https://drive.google.com/file/d/1aty953Y2JctgE0gledpXDuBwiGiRB_s9/view?usp=sharing	Hall Booking APP
105	https://lnct.ac.in/wp-content/uploads/2022/06/Agnipath-yojna.jpg	Agnipath Yogna
106	https://lnct.ac.in/corporate-social-responsibility/	CSR
107	http://www.lnctalumni.in/	Alumni
108	https://admissions.lnct.ac.in/	Admission 2022
109	https://lnct.ac.in/wp-content/uploads/2022/03/VOICE-OF-LNCT-small.pdf	Voice of LNCT
110	http://lnctbhopal.in/	LNCT Bhopal
111	http://lncpbhopal.in/	LNCP Bhopal
112	https://lnct.ac.in/wp-content/uploads/2021/04/Lakshmi-Narain-College-of-Technology-ISTE-Certificate.pdf	Tie-Up
113	https://blog.lnct.ac.in	LNCT Blog
114	https://lnct.ac.in/contact/	CONTACT
115	https://lnct.ac.in/career/	Career
116	https://blog.lnct.ac.in/	Read LNCT Blog
117	https://lnct.ac.in/top-engineering-colleges-in-bhopal/	Lakshmi Narain College of Technology (LNCT)
118	http://lnct.ac.in/	Image
119	https://lnct.ac.in/category/civil-engineering/	Civil Engineering
120	https://lnct.ac.in/expert-lecture-was-organised-for-the-2nd-semester-students-of-civil-engineering-branch/	Expert lecture was organised for the 2nd Semester students of Civil branch
121	https://lnct.ac.in/2022/06/24/	
122	https://lnct.ac.in/lncp-celebrated-international-day-of-yoga/	LNCP celebrated International Day of Yoga
123	https://lnct.ac.in/author/admin/	admin
124	https://lnct.ac.in/2022/06/21/	
125	https://lnct.ac.in/robotics-workshop/	Robotics Workshop
126	https://lnct.ac.in/2022/06/20/	
127	https://lnct.ac.in/exchange-program-at-bahra-university/	Exchange Program at Bahra University
128	https://lnct.ac.in/close-campus-drive-by-vitamax-healthcare-pvt-ltd/	Close Campus Drive by Vitamax Healthcare Pvt Ltd
129	https://lnct.ac.in/time-table-for-diploma-engineering-examinations-june-2022/	Time Table For Diploma Engineering Examinations - June- 2022
130	https://lnct.ac.in/lncp-organising-a-session-on-yoga-for-humanity/	LNCP Organising a Session on Yoga for Humanity
131	https://lnct.ac.in/seminar-on-digital-banking-and-financial-inclusion/	Seminar on Digital Banking and Financial Inclusion
132	https://lnct.ac.in/2022/06/18/	
133	https://lnct.ac.in/rgpv-exams-2022-revised/	RGPV , EXAMS. 2022 (Revised)
134	https://lnct.ac.in/2022/06/17/	
135	https://lnctu.ac.in	LNCT University Bhopal
136	https://csebilaspur.ac.in	CEC Bilaspur Campus

137	https://lnctuj.com	LNCT Jabalpur Campus
138	https://www.facebook.com/LNCTGroupOfCollege	Facebook
139	https://twitter.com/grouplnct	Twitter
140	https://www.youtube.com/c/LnctBroadcastingChannel	Youtube
141	https://www.instagram.com/lnctgroupofcolleges/	Instagram
142	https://lnct.ac.in/industry-testimonials/	Industry Testimonials
143	https://ediic.lnctu.ac.in/	EDIIC	LNCT University
144	https://lnct.ac.in/the-national-institutional-ranking-framework/	NIRF

5. CHECKING HEADERS SECURITY

Security Report Summary

F

Site:	https://lnct.ac.in/
IP Address:	3.7.218.202
Report Time:	24 Jun 2022 17:57:36 UTC
Headers:	✖ Strict-Transport-Security ✖ Content-Security-Policy ✖ X-Frame-Options ✖ X-Content-Type-Options ✖ Referrer-Policy ✖ Permissions-Policy

Raw Headers

HTTP/2	200
server	nginx
date	Fri, 24 Jun 2022 17:57:35 GMT
content-type	text/html; charset=UTF-8
content-length	305810
vary	Accept-Encoding
x-powered-by	PHP/7.3.33
last-modified	Fri, 24 Jun 2022 15:19:01 GMT
vary	Accept-Encoding
x-powered-by	PleskLin

6. <u>BUFFER SIZE</u>

- The buffer size of the target lnct.ac.in is 1460 bytes.
- The tool used here to find the buffer size is "nping".
- It is used along with the "tcp" flag and "df" flag set which helps in sending the data using tcp protocol and "df" flag does not allows to fragment the data.
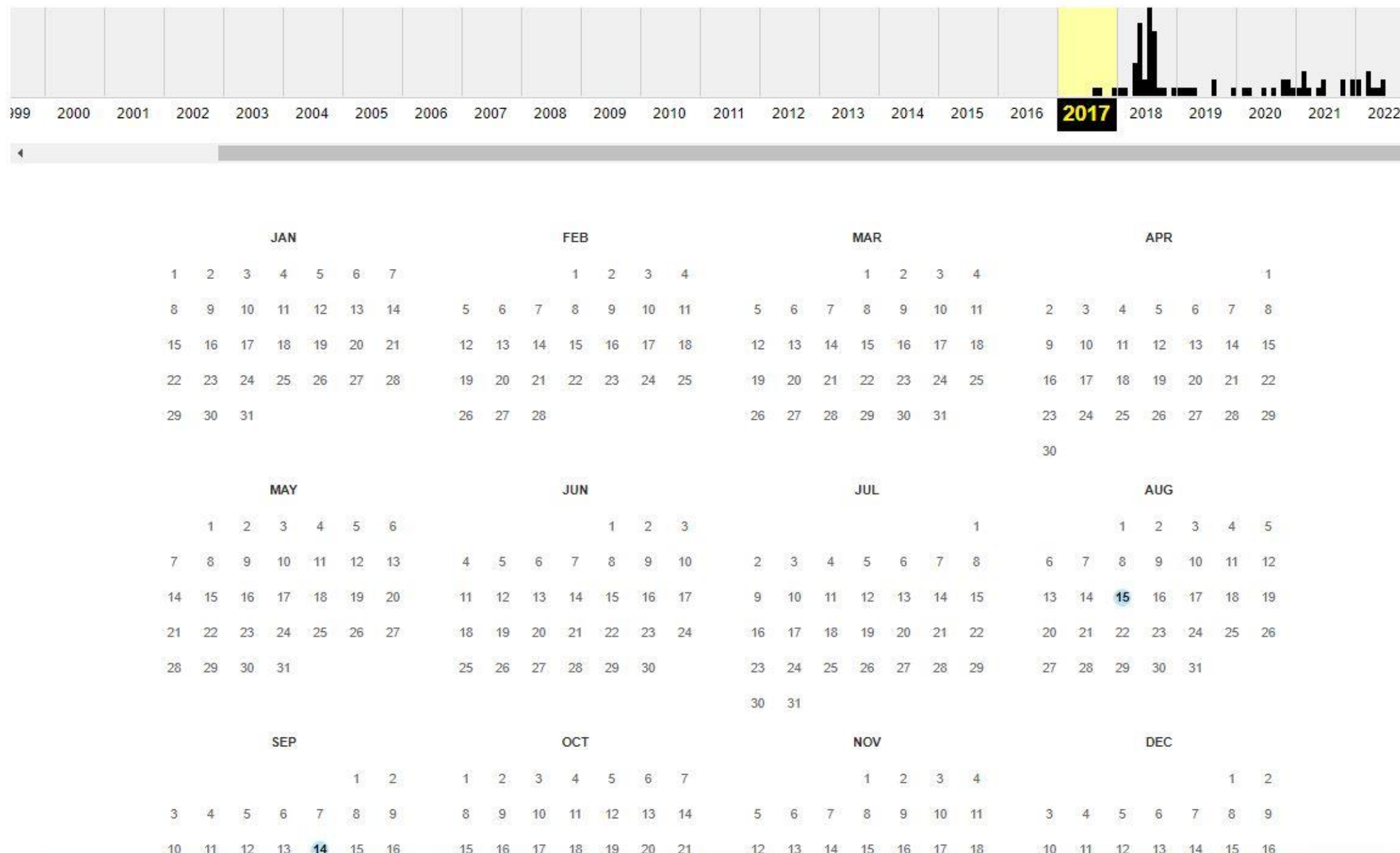- The screenshot of the operation performed is attached below:-

7. FINDING HISTORY WITH ARCHIVE.ORG

- **Various snapshots of our target is available on web.archive.org**
- **The first snapshot was created on August 15 2017.**
- **From that time a total of 79 snapshot was created between** August 15, 2017 **and** June 14, 2022.

END OF REPORT

THANK YOU