

Shri G. S. Institute of Technology & Science,

Indore, Department of Computer Engineering



Subject: Information and Network Security

Session: December – May 2021

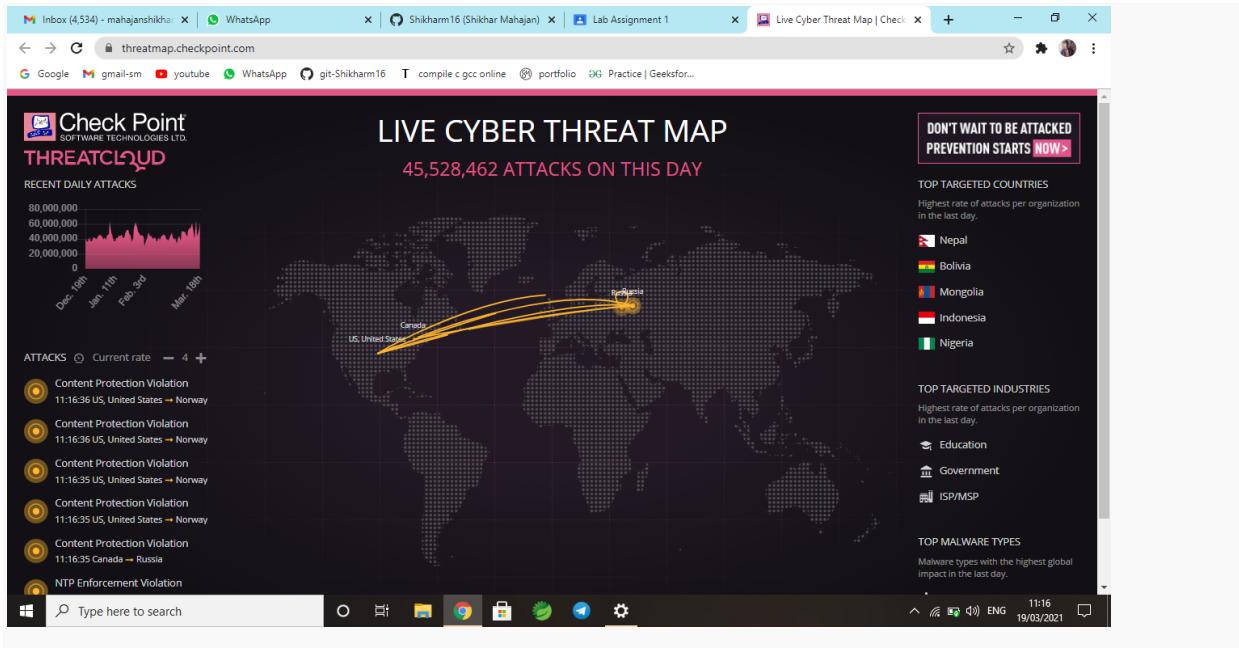
Lab Assignment

Submitted To:
Veerendra Shrivastava
Soma Saha

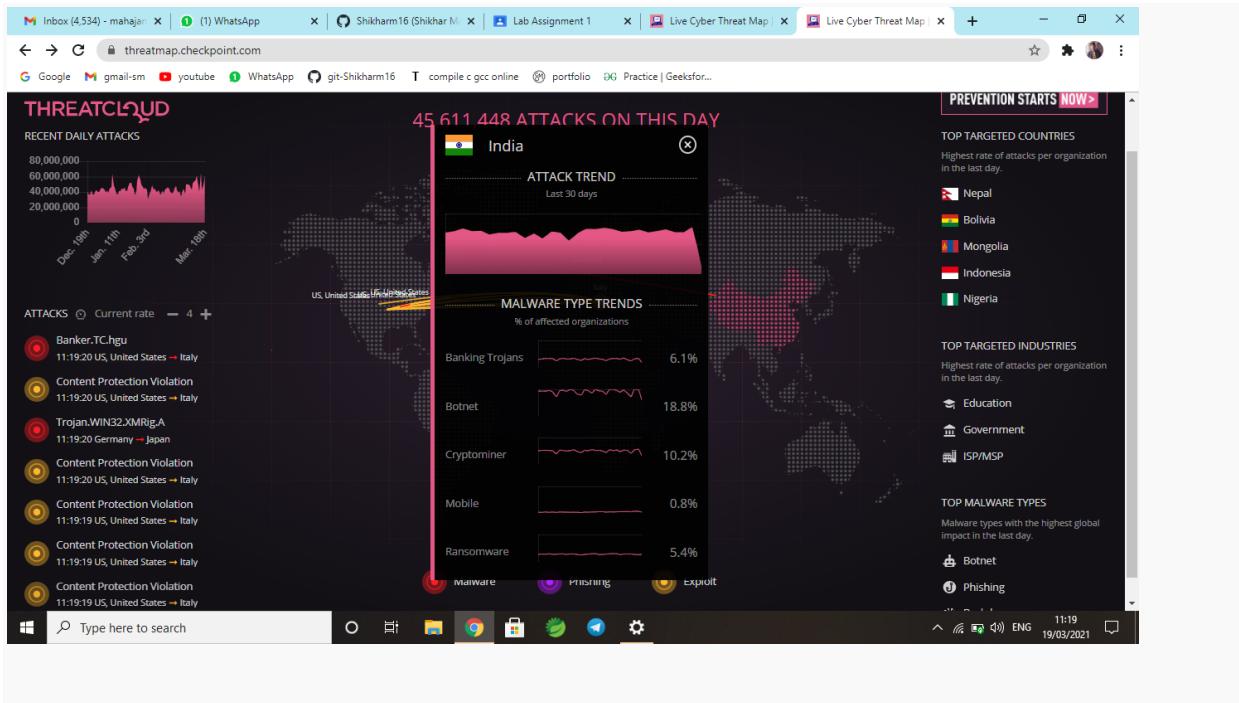
Submitted By:
Shikhar Mahajan
0801CS171077

Q1. Visit to the website <https://threatmap.checkpoint.com/> and answer the following Questions:

I. How many numbers of attacks are performed in all over the world when you visit this website? Attach the screenshot.



II. Write the various malware type trends in India in last 30 Days with percentage of affected organization?



III. Explain the working of a threat cloud map?

A cyber threat map, also known as a cyber attack map, is a real-time map of the computer security attacks that are going on at any given time. One of the most famous was released by the company Norse and went so viral, even among non-hackers, that it got its own story in Newsweek in 2015.

The map itself looks like a global game of laser tag. Beams of light, represented by different colors, shoot across a darkened screen showing where an attack comes from and where it is going. When it first caught the public eye, captivated audiences watched hackers wage cyber-war across hundreds and thousands of miles.

How Does A Cyber Threat Map Work?

If cyber attacks are sneaky mice – or, more appropriately, giant rats – then cyber attack maps work like the mousetrap.

Norse, for example, maintained a global threat intelligence network of more than 8 million sensors and “honeypots” in 47 countries across the world. These tools impersonated thousands of applications and devices that are common targets of hackers.

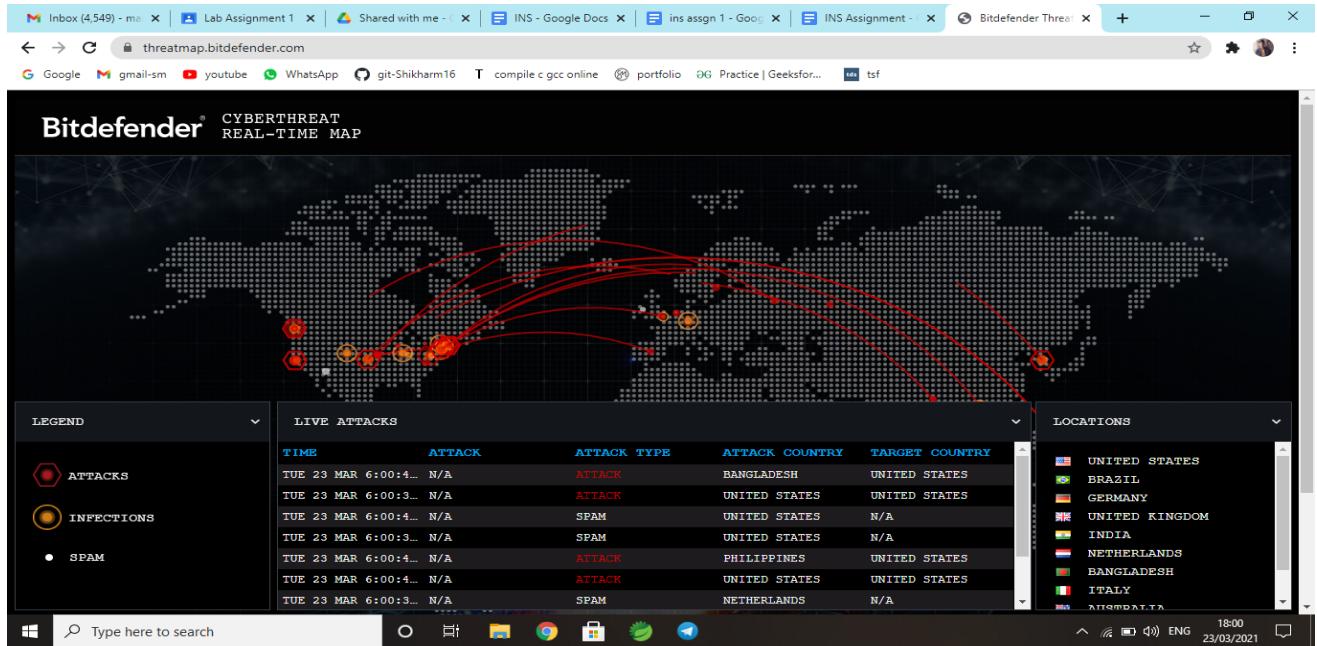
When a hacker hits a Norse sensor, the hacker believes that it has breached a system. Instead, Norse collected information about the hacker’s toolkit, including his or her IP address. This information then manifested as data on the cyber attack map.

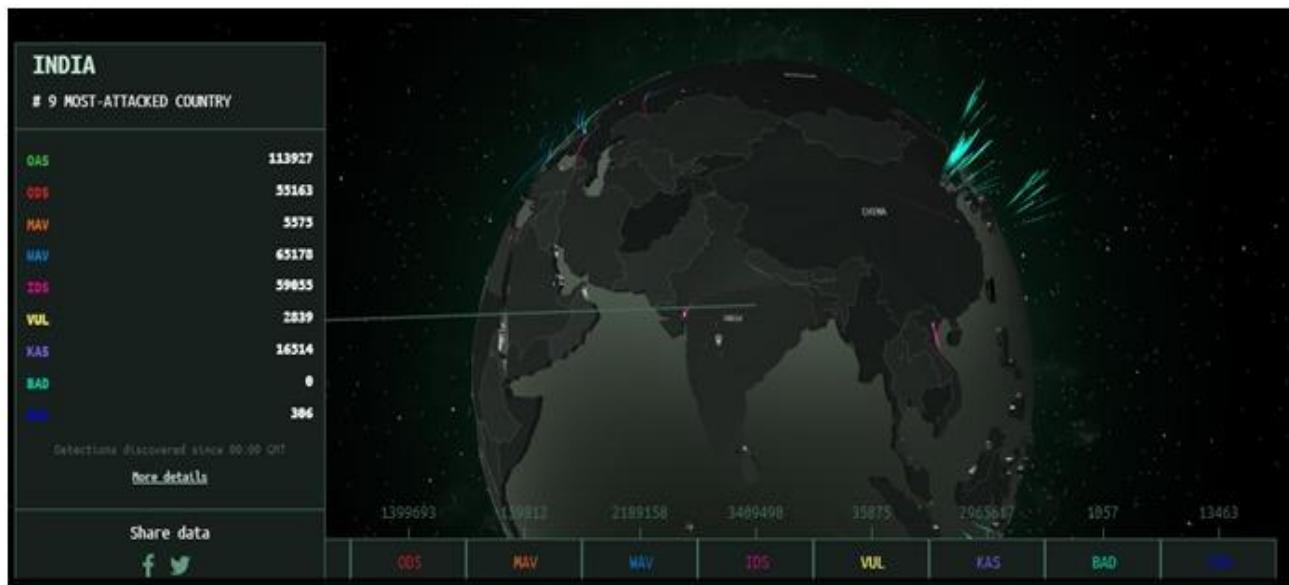
This model has continued past the demise of Norse to power live maps like Cyberthreat, ThreatCloud, and Fortinet. Some companies claim that these are real-time cyber attacks, but most are more like selections of recent attacks.

IV. Write the name of any five websites which is similar to the threat cloud and attach their screenshots.

Websites similar to ThreatCloud are:

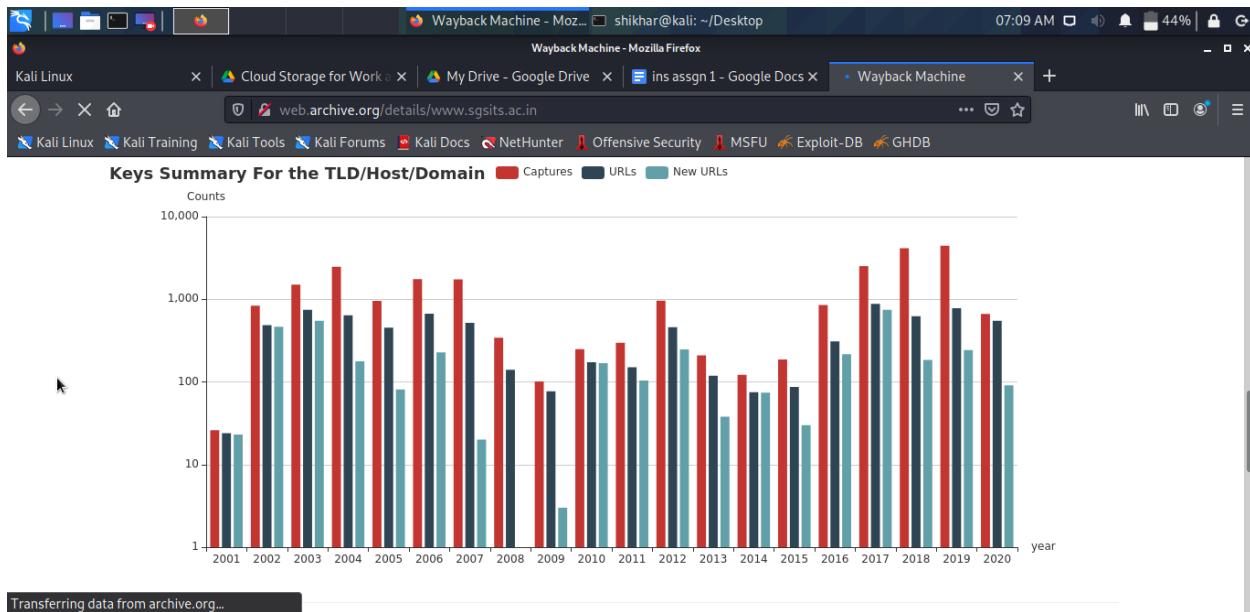
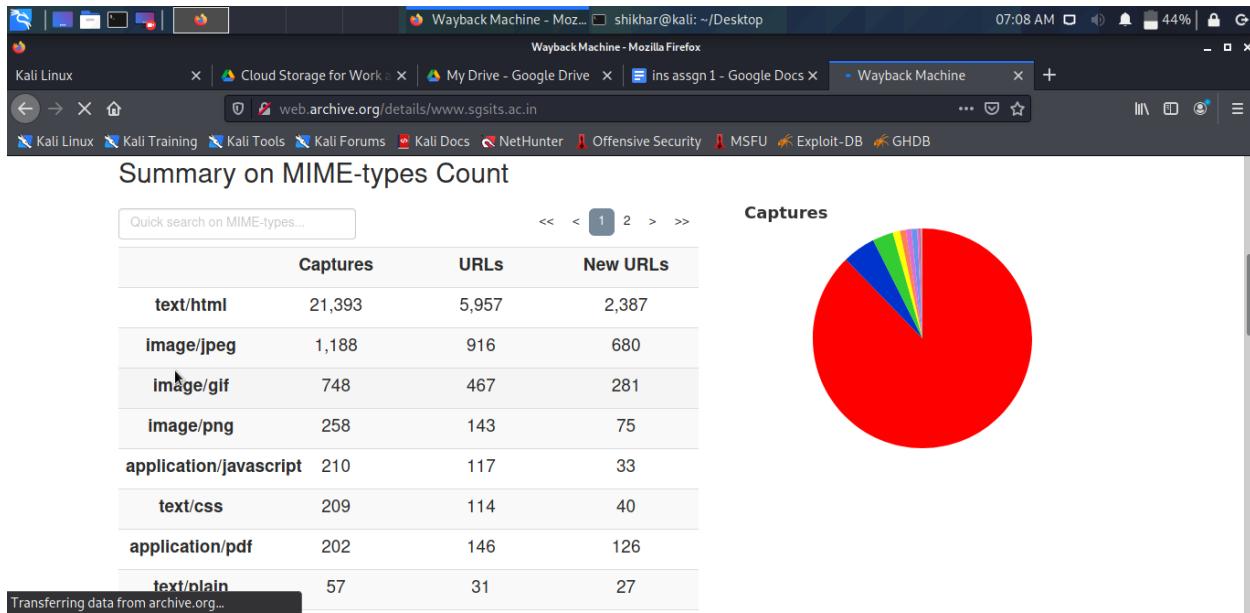
- CyberThreat by Kaspersky
- FireEye
- Fortinet
- Imperva
- Bitdefender
- SonicWall

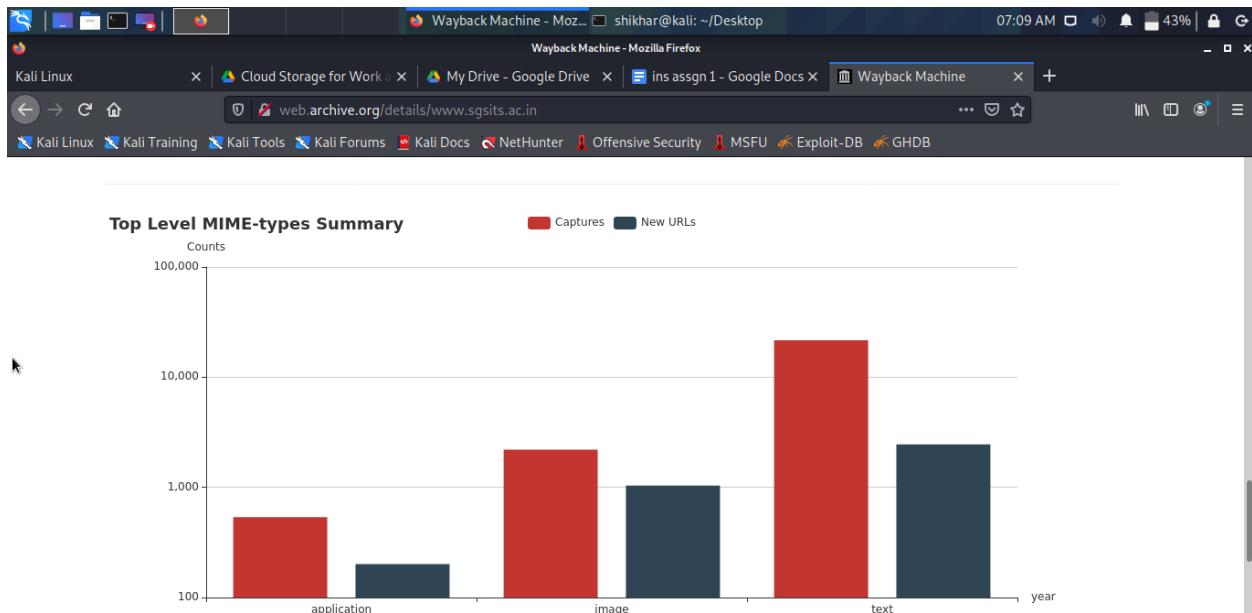




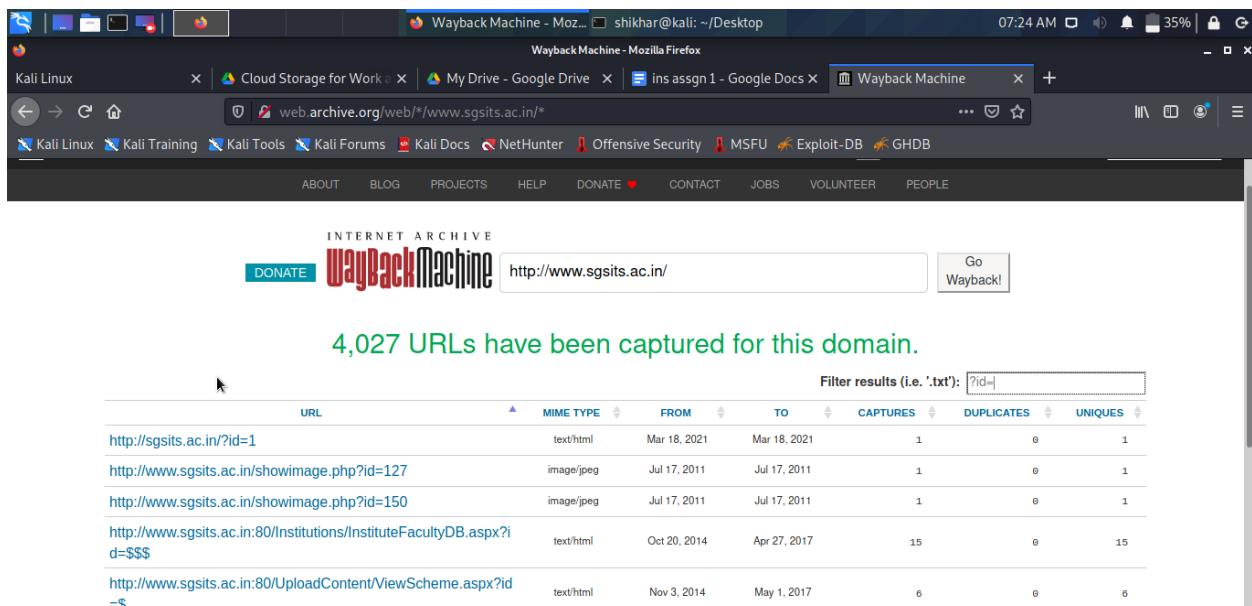
Q2. Visit to the website <https://web.archive.org/> and perform the following operation on the target website i.e. www.sgsits.ac.in -

I. Search the target website on the wayback machine and count the number of captures with duration. Also attach the screenshot of your result.





II. Try the following filters on the wayback machine for checking the vulnerabilities in the target website: ?, ?id=, .zip, readme.php, readme.txt, .csv, password, /admin/, .js, /api/, .config, msg= etc. Also attach the screenshot for each filter and/or your result.



Wayback Machine - Mozilla Firefox

shikhar@kali: ~/Desktop

7:25 AM 34% 34%

Kali Linux | Cloud Storage for Work | My Drive - Google Drive | ins assgn 1 - Google Docs | Wayback Machine | +

web.archive.org/web/*/www.sgsits.ac.in/*

Kali Linux Kali Training Kali Tools Kali Forums Kali Docs NetHunter Offensive Security MSFU Exploit-DB GHDB

ABOUT BLOG PROJECTS HELP DONATE CONTACT JOBS VOLUNTEER PEOPLE

INTERNET ARCHIVE

DONATE Wayback Machine http://www.sgsits.ac.in/ Go Wayback!

4,027 URLs have been captured for this domain.

Filter results (i.e. '.txt'): ap|

URL	MIME TYPE	FROM	TO	CAPTURES	DUPES	UNIQUES
http://sgsits.ac.in/Images/mapindore.gif	image/gif	May 7, 2016	May 7, 2016	1	0	1
http://sgsits.ac.in:80/free-hosting/sgsits/gifs/mapindore.gif	image/gif	Jan 27, 2003	Jan 27, 2003	1	0	1
http://www.sgsits.ac.in:80/deptappy/deptphpap1nt.htm	text/html	Nov 5, 2004	Mar 1, 2005	3	1	2
http://www.sgsits.ac.in:80/gifs/mapindore.gif	image/gif	Apr 8, 2006	Apr 8, 2006	1	0	1

Showing 1 to 4 of 4 entries (filtered from 4,027 total entries)

First Previous 1 Next Last

Wayback Machine - Mozilla Firefox

shikhar@kali: ~/Desktop

7:23 AM 35% 35%

Kali Linux | Cloud Storage for Work | My Drive - Google Drive | ins assgn 1 - Google Docs | Wayback Machine | +

web.archive.org/web/*/www.sgsits.ac.in/*

Kali Linux Kali Training Kali Tools Kali Forums Kali Docs NetHunter Offensive Security MSFU Exploit-DB GHDB

INTERNET ARCHIVE

4,027 URLs have been captured for this domain.

Filter results (i.e. '.txt'): php|

URL	MIME TYPE	FROM	TO	CAPTURES	DUPES	UNIQUES
http://sgsits.ac.in/pages/student/department-and-facult/harma.php	warc/revisit	Mar 6, 2016	Jan 6, 2017	2	1	1
http://www.sgsits.ac.in/index.php?displayCaptcha=True&instanceCaptcha=273&time=15731474011559310908	image/x-png	Nov 7, 2019	Nov 7, 2019	1	0	1
http://www.sgsits.ac.in/media/circulars.php	text/html	Jul 17, 2011	May 25, 2013	10	2	8
http://www.sgsits.ac.in/modules/mod_sj_k2_slider/assets/css/rgba.php?rgba(255,%200,%200,%20.5)	warc/revisit	Nov 7, 2019	Dec 29, 2019	2	1	1
http://www.sgsits.ac.in/pages/circulars.php	text/html	Jul 17, 2011	Nov 10, 2012	9	2	7
http://www.sgsits.ac.in/pages/committee/finance.php	text/html	Feb 10, 2012	Feb 10, 2012	1	0	1
http://www.sgsits.ac.in/pages/committee/grievance.php	text/html	Feb 16, 2012	Aug 18, 2012	3	2	1
http://www.sgsits.ac.in/pages/committee/managing.php	text/html	Feb 16, 2012	Aug 19, 2012	3	2	1
http://www.sgsits.ac.in/pages/facultdetail.php?fid=127	text/html	Jul 17, 2011	Jul 18, 2012	3	1	2

Wayback Machine - Mozilla Firefox

shikhar@kali: ~/Desktop

07:25 AM 35%

Kali Linux | Cloud Storage for Work | My Drive - Google Drive | ins assgn 1 - Google Docs | Wayback Machine | +

← → ⌛ ⌂ ⌂ web.archive.org/web/*www.sgsits.ac.in/*

Kali Linux Kali Training Kali Tools Kali Forums Kali Docs NetHunter Offensive Security MSFU Exploit-DB GHDB

ABOUT BLOG PROJECTS HELP DONATE CONTACT JOBS VOLUNTEER PEOPLE

INTERNET ARCHIVE

DONATE Wayback Machine http://www.sgsits.ac.in/ Go Wayback!

4,027 URLs have been captured for this domain.

Filter results (i.e. '.txt'): password

URL	MIME TYPE	FROM	TO	CAPTURES	DUPES	UNIQUES
http://sgsits.ac.in:80/Admin/ChangePassword.aspx?	text/html	Feb 19, 2017	Apr 27, 2017	2	1	1
http://www.sgsits.ac.in:80/Feedback/ForgotPassword.aspx	text/html	Oct 20, 2014	May 11, 2017	21	0	21

Showing 1 to 2 of 2 entries (filtered from 4,027 total entries)

First Previous 1 Next Last

The Wayback Machine is an initiative of the Internet Archive, a 501(c)(3) non-profit, building a digital library of Internet sites and other cultural artifacts in digital form. Other projects include Open Library & archive-it.org.

Wayback Machine - Mozilla Firefox

shikhar@kali: ~/Desktop

07:27 AM 33%

Kali Linux | Cloud Storage for Work | My Drive - Google Drive | ins assgn 1 - Google Docs | Wayback Machine | +

← → ⌛ ⌂ ⌂ web.archive.org/web/*www.sgsits.ac.in/*

Kali Linux Kali Training Kali Tools Kali Forums Kali Docs NetHunter Offensive Security MSFU Exploit-DB GHDB

4,027 URLs have been captured for this domain.

Filter results (i.e. '.txt'): gif

URL	MIME TYPE	FROM	TO	CAPTURES	DUPES	UNIQUES
http://sgsits.ac.in/Academics/pdf_files/arrow_black.gif	image/gif	May 7, 2016	May 7, 2016	1	0	1
http://sgsits.ac.in/images/academicsBtn.gif	image/gif	Dec 29, 2014	Mar 4, 2017	6	5	1
http://sgsits.ac.in/images/academicsBtnH.gif	image/gif	Dec 28, 2016	Dec 28, 2016	1	0	1
http://sgsits.ac.in/images/AcdRecVeri.gif	image/gif	Dec 29, 2014	Mar 4, 2017	8	7	1
http://sgsits.ac.in/images/AdmissionBtn.gif	image/gif	Dec 29, 2014	Mar 4, 2017	6	5	1
http://sgsits.ac.in/images/ajaxload.gif	image/gif	Sep 23, 2016	Sep 23, 2016	1	0	1
http://sgsits.ac.in/images/arrow1.gif	image/gif	May 7, 2016	May 7, 2016	1	0	1
http://sgsits.ac.in/images/bg.gif	image/gif	Jan 28, 2015	Mar 22, 2017	4	3	1
http://sgsits.ac.in/Images/Bullet.gif	image/gif	May 7, 2016	May 7, 2016	1	0	1
http://sgsits.ac.in/images/callusicon.gif	image/gif	Feb 10, 2016	May 12, 2016	2	1	1
http://sgsits.ac.in/images/cntrrihnt_th.gif	image/gif	Jan 28, 2015	Mar 22, 2017	4	3	1

web.archive.org/web/*http://sgsits.ac.in/images/AcdRecVeri.gif

Q3. Visit to the website <https://www.netcraft.com> and perform the following operation on the target website: www.sgsits.ac.in –

I. Write the names of various domains associated with the target website.

The screenshot shows the Netcraft Site Report for www.sgsits.ac.in. The 'Network' section displays the following information:

Site	Domain	Primary language
Netblock Owner	Shri Govindram Seksaria Institute of Technology and Science	Nameserver
Hosting company	National Knowledge Network	Domain registrar
Hosting country	IN	Nameserver organisation
IPv4 address	14.139.250.83 (VirusTotal)	Organisation Shri G. S. Inst. of Tech. and Sc, Redacted For Privacy, REDACTED FOR PRIVACY, India
IPv4 autonomous systems	AS55824	DNS admin
IPv6 address	Not Present	Top Level Domain
IPv6 autonomous systems	Not Present	DNS Security Extensions
Reverse DNS	nkn83.sgsits.ac.in	

IP delegation

IPv4 address (14.139.250.83)

IPv6 autonomous systems

Reverse DNS

II. Write the IP version 4 and version 4 ranges associated with the target website.

The screenshot shows the Netcraft Site Report for www.sgsits.ac.in. The 'IP delegation' section displays the following information:

IPv4 address (14.139.250.83)	Country	Name	Description
0.0.0.0-255.255.255.255	N/A	IANA-BLK	The whole IPv4 address space
↳ 14.0.0.0-14.255.255.255	Australia	APNIC-AP	Asia Pacific Network Information Centre
↳ 14.139.0.0-14.139.255.255	India	RSMANI-NKN-IN	National Knowledge Network
↳ 14.139.250.80-14.139.250.95	India	NKN-SGSITS-MP	Shri Govindram Seksaria Institute of Technology and Science
↳ 14.139.250.83	India	NKN-SGSITS-MP	Shri Govindram Seksaria Institute of Technology and Science

Last Reboot (86 days ago)

www.sgsits.ac.in

III. What is the name and location of the server of the target website?

Netblock owner

Netblock owner	IP address	OS	Web server	Last seen
Shri Govindram Seksaria Institute of Technology and Science	14.139.250.83	Linux	Apache	22-Mar-2021
MegaVelocity Inc. 2921 Sable Rdige Drive Ottawa ON CA K1T-3S1	192.206.5.35	Windows Server 2008	Microsoft-IIS/7.5	28-Sep-2016
Shri Govindram Seksaria Institute of Technology and Science	14.139.250.83	Linux	Apache/2.2.15 Red Hat	29-Aug-2014
This space is statically assigned	220.225.96.92	Linux	Apache/2.2.15 Red Hat	12-May-2014
Shri Govindram Seksaria Institute of Technology and Science	14.139.250.83	Linux	Apache/2.2.15 Red Hat	10-May-2014
This space is statically assigned	220.225.96.92	Linux	Apache/2.2.15 Red Hat	7-May-2014
Shri Govindram Seksaria Institute of Technology and Science	14.139.250.83	Linux	Apache/2.2.15 Red Hat	6-May-2014
This space is statically assigned	220.225.96.92	-	Apache/2.2.15 Red Hat	8-Nov-2013
► Reliance Communication...	220.225.96.92	Linux	Apache/2.2.15 Red Hat	8-Nov-2013
► Reliance Communication...	220.225.96.92	Linux	Apache/2.0.52 Red Hat	18-Mar-2010

Sender Policy Framework

IV. Can you detect the OS name? if yes then also write the name of the OS.

Netblock owner

Netblock owner	IP address	OS	Web server	Last seen
Shri Govindram Seksaria Institute of Technology and Science	14.139.250.83	Linux	Apache	22-Mar-2021
MegaVelocity Inc. 2921 Sable Rdige Drive Ottawa ON CA K1T-3S1	192.206.5.35	Windows Server 2008	Microsoft-IIS/7.5	28-Sep-2016
Shri Govindram Seksaria Institute of Technology and Science	14.139.250.83	Linux	Apache/2.2.15 Red Hat	29-Aug-2014
This space is statically assigned	220.225.96.92	Linux	Apache/2.2.15 Red Hat	12-May-2014
Shri Govindram Seksaria Institute of Technology and Science	14.139.250.83	Linux	Apache/2.2.15 Red Hat	10-May-2014
This space is statically assigned	220.225.96.92	Linux	Apache/2.2.15 Red Hat	7-May-2014
Shri Govindram Seksaria Institute of Technology and Science	14.139.250.83	Linux	Apache/2.2.15 Red Hat	6-May-2014
This space is statically assigned	220.225.96.92	-	Apache/2.2.15 Red Hat	8-Nov-2013
► Reliance Communication...	220.225.96.92	Linux	Apache/2.2.15 Red Hat	8-Nov-2013
► Reliance Communication...	220.225.96.92	Linux	Apache/2.0.52 Red Hat	18-Mar-2010

Sender Policy Framework

Q4. Visit to the website <https://builtwith.com> and perform the following operation on the target website: www.sgsits.ac.in –

I. Write the name of various technologies used in designing the target website.

SGSITS.AC.IN

Analytics and Tracking

	First Detected	Last Detected
Google Analytics	Jun 2017	Mar 2021
Google Universal Analytics	Jun 2017	Feb 2021

Widgets

	First Detected	Last Detected
Font Awesome	Jun 2017	Mar 2021
Google Font API	Jun 2017	Mar 2021
Google Code Prettify	Jun 2020	Jan 2021
COVID-19	Apr 2020	Apr 2020
Thawte Seal	Jan 2015	May 2017

Frameworks

	First Detected	Last Detected
PHP	Jul 2012	Mar 2021
ASP.NET	Oct 2014	Mar 2020
Shockwave Flash Embed	Jul 2012	May 2017
ASP.NET Ajax	Oct 2014	May 2017
ASP.NET 2.0	Oct 2014	May 2017
Adobe Dreamweaver	Oct 2014	May 2017
Visual Studio	Jul 2012	Jul 2013
Ruby on Rails	Jul 2012	Jul 2013

Content Delivery Network

	First Detected	Last Detected
Microsoft Ajax Content Delivery Network	Nov 2015	May 2017
AJAX Libraries API	Nov 2015	May 2017

Mobile

	First Detected	Last Detected
iPhone / Mobile Compatible	Jun 2017	Feb 2021
Viewport Meta	Jun 2017	Feb 2021
Apple Mobile Web App Capable	Jun 2017	Feb 2021

Content Management System

	First Detected	Last Detected
Joomla!	Jun 2020	Mar 2021
Open Source		
Visual Basic .NET	Jul 2012	Jul 2013

JavaScript Libraries and Functions

	First Detected	Last Detected
jQuery	Oct 2014	Mar 2021
JavaScript Library		

Technologies

- Hide Removed
- Hide Free
- Hide Established

sgsits.ac.in

sgsits.ac.in/*
Internal pages of sgsits.ac.in

mis.sgsits.ac.in

mail.sgsits.ac.in

moodle.sgsits.ac.in

Technology Spend

Very Low

Technology Spend is based on the sum of the average cost of the active premium paid-for technologies found across sgsits.ac.in.

Create Notification

Add to Chrome

builtwith.com/detailed/sgsits.ac.in

jQuery migrate Compatibility

jQuery UI	Nov 2015	Feb 2021
jQuery Easing	Jun 2017	Feb 2021
jQuery prettyPhoto	Jun 2017	Feb 2021
jCarousel	Jun 2017	Feb 2021
Touchwipe	Jun 2017	Feb 2021
PrettyPrint	Jun 2017	Feb 2021
jQuery Mousewheel	Jun 2017	Feb 2021
Bootstrap.js	Oct 2017	Feb 2018
jQuery 1.7.2	Nov 2015	May 2017
Google Hosted Libraries	Nov 2015	May 2017
Google Hosted jQuery	Nov 2015	May 2017

Verified Link

Careers	Aug 2020	Feb 2021
Email Hosting Providers		
DKIM	Sep 2020	Feb 2021
SPF	Sep 2020	Feb 2021
Microsoft Exchange Online	May 2013	Aug 2013

Type here to search

18:50 23/03/2021

builtwith.com/detailed/sgsits.ac.in

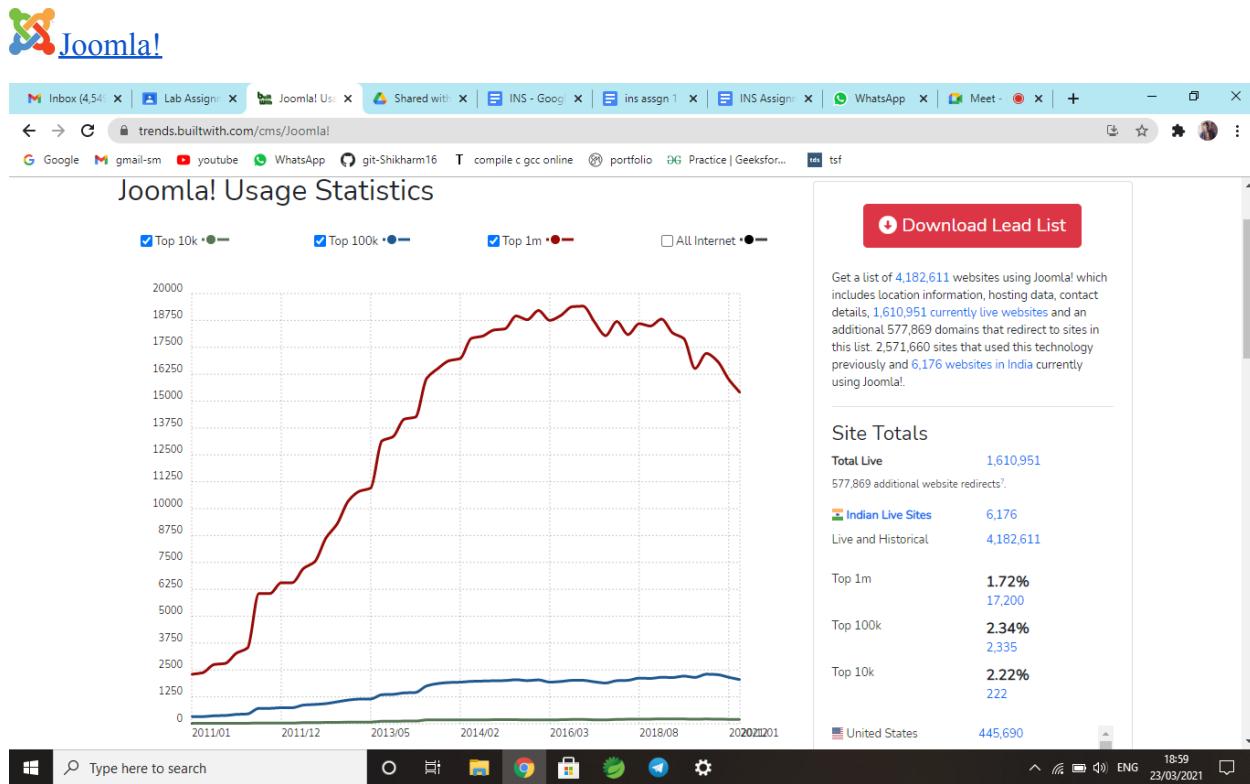
Business Email Hosting

SSL Certificates		
Common Name Invalid	Sep 2019	May 2020
Comodo PositiveSSL	Jan 2016	Feb 2020
Comodo SSL	Jan 2016	May 2016
Thawte SSL	Jan 2015	Dec 2015
Web Hosting Providers		
Swisscom	Jan 2019	Jan 2019
Dedicated Hosting	Mar 2016	Oct 2016
Web Servers		
Apache	Jul 2012	Mar 2021
IIS	Oct 2014	Mar 2020
IIS 7	Oct 2014	May 2017
Apache 2.2	Dec 2013	Dec 2016
Operating Systems and Servers		
CentOS	Nov 2016	Dec 2016
Red Hat Enterprise Linux	Jul 2012	Sep 2014
Syndication Techniques		
Atom	Jun 2017	Feb 2021
RSS	Jun 2017	Feb 2021

Type here to search

18:51 23/03/2021

II. Write the name of CMS used for designing the target website.



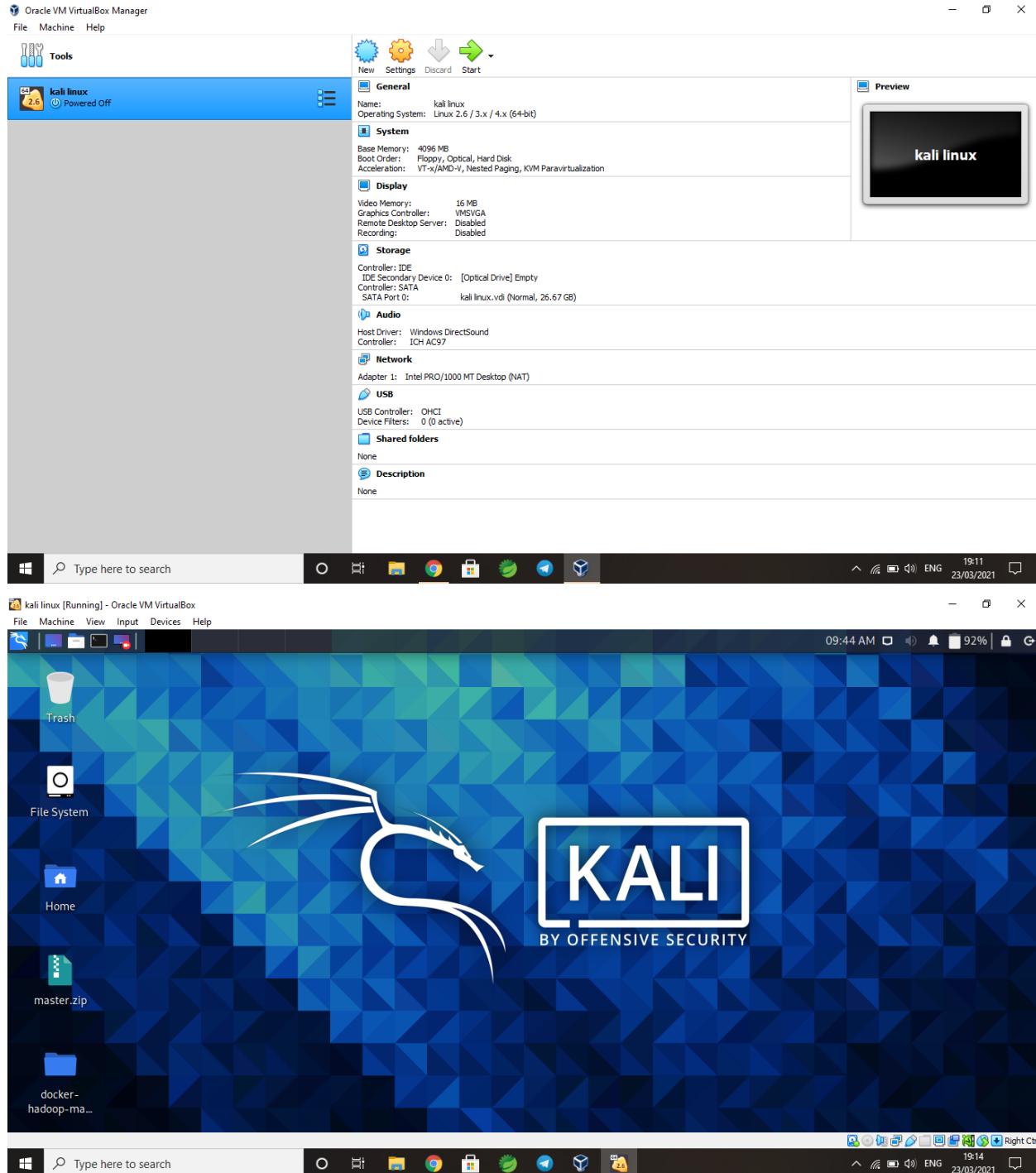
III. Write the description about the security certificates used in the target website.

Common Name Invalid
 Comodo PositiveSSL
 Comodo SSL
 Thawte SSL

IV. Write the name of other websites or tools which can be used for website technology lookup.

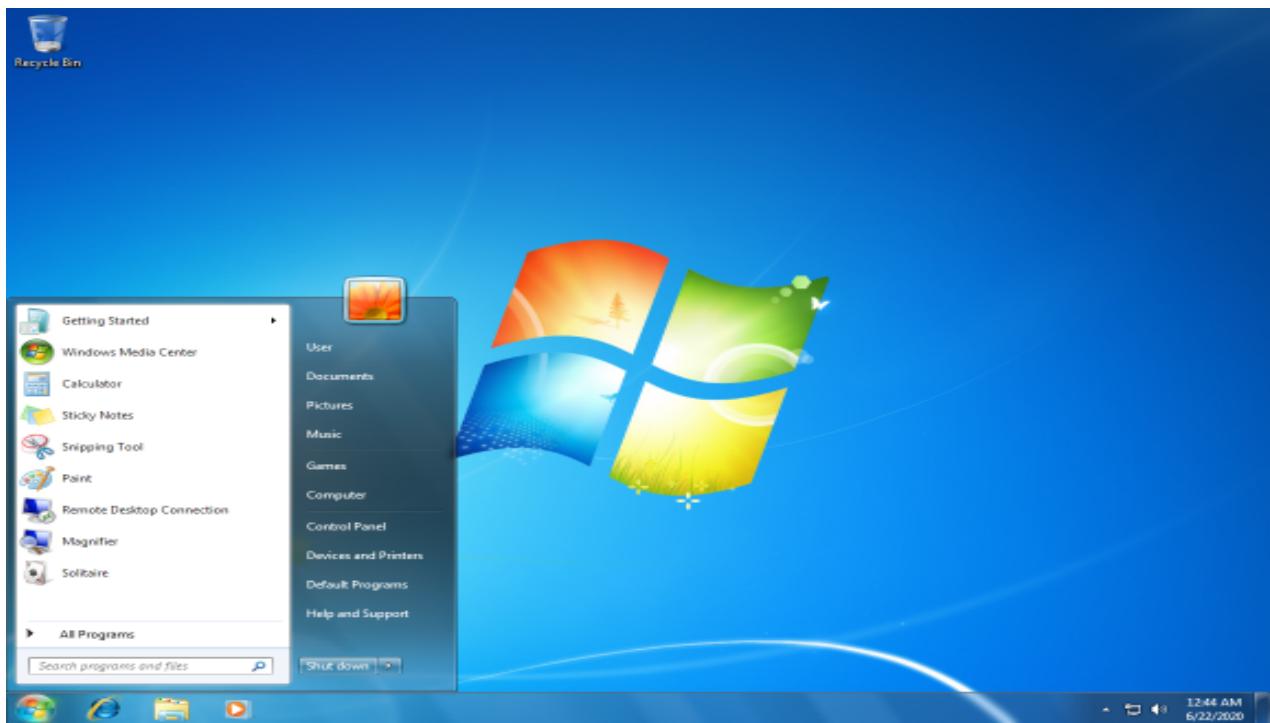
Top Alternatives to BuiltWith

- ZoomInfo.
- Leadfeeder.
- D&B Hoovers.
- Lusha.
- Lead411.
- Oceanos.
- VisitorTrack.
- Leadinfo.

Q5. Perform the following operations:**I. Setup the following virtual machine in VirtualBox or VmWare environment:****1) Kali Linux**

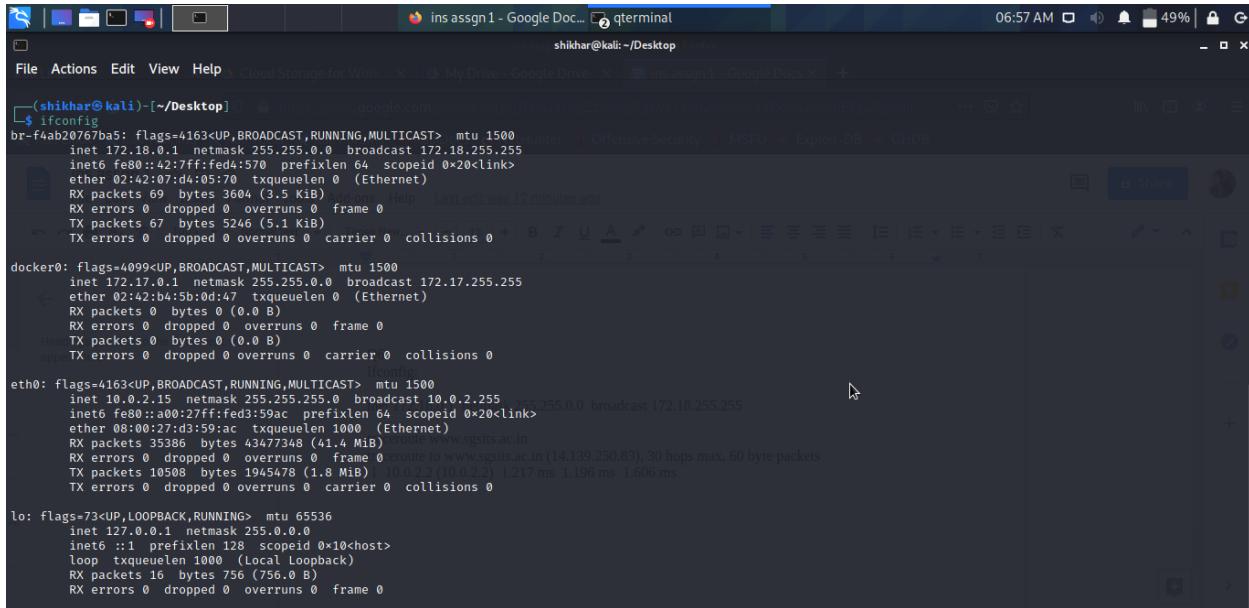
2) Metasploitable 2

3) Windows 7



Q6. Execute the following commands on/in the virtual machine:

I. Run the ifconfig in each of the virtual machine and write the IP, MAC and subnet mask details.



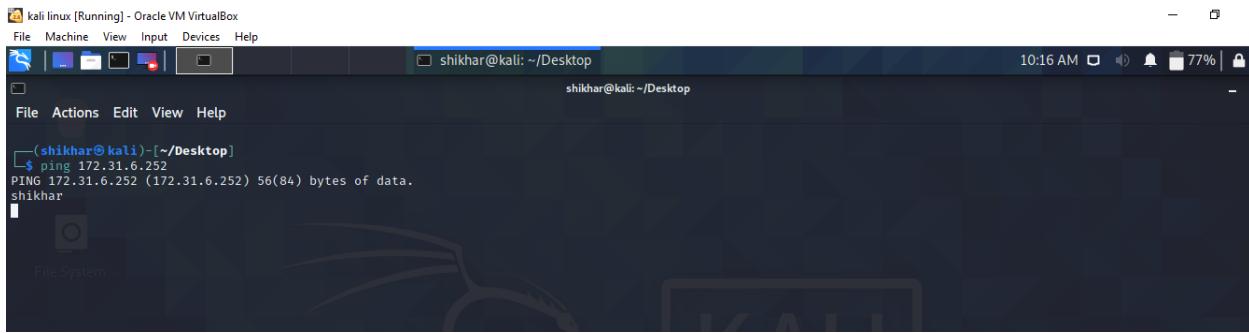
```
(shikhar㉿kali)-[~/Desktop]$ ifconfig
br-f4ab20767ba5: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 172.18.0.1 netmask 255.255.0.0 broadcast 172.18.255.255
        inet6 fe80::42:7ff:fed3:59ac prefixlen 64 scopeid 0x20<link>
            ether 02:42:07:d4:05:70 txqueuelen 0 (Ethernet)
                RX packets 69 bytes 3604 (3.5 Kib)
                RX errors 0 dropped 0 overruns 0 frame 0
                TX packets 67 bytes 5246 (5.1 Kib)
                TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

docker0: flags=4099<UP,BROADCAST,MULTICAST> mtu 1500
    inet 172.17.0.1 netmask 255.255.0.0 broadcast 172.17.255.255
        ether 02:42:b4:5b:0d:c7 txqueuelen 0 (Ethernet)
            RX packets 0 bytes 0 (0.0 B)
            RX errors 0 dropped 0 overruns 0 frame 0
            TX packets 0 bytes 0 (0.0 B)
            TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 10.0.2.15 netmask 255.255.255.0 broadcast 10.0.2.255
        inet6 fe80::4002:27ff:fed3:59ac prefixlen 64 scopeid 0x20<link>
            ether 08:00:27:d3:59:ac txqueuelen 1000 (Ethernet)
                RX packets 35386 bytes 43477348 (41.4 MiB)
                RX errors 0 dropped 0 overruns 0 frame 0
                TX packets 10508 bytes 1945478 (1.8 MiB)
                TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

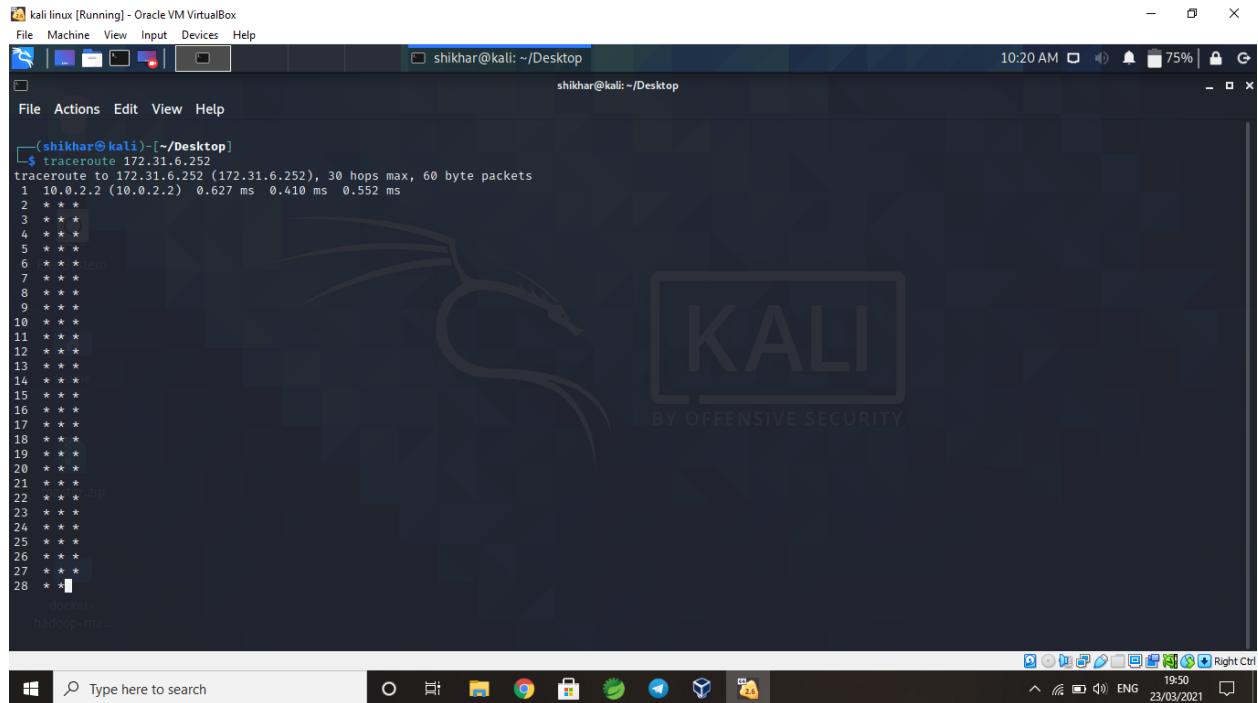
lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
    inet 127.0.0.1 netmask 255.0.0.0
        inet6 ::1 prefixlen 128 scopeid 0x10<host>
            loop txqueuelen 1000 (Local Loopback)
                RX packets 16 bytes 756 (756.0 B)
                RX errors 0 dropped 0 overruns 0 frame 0
```

II. Run the ping command in each of the virtual machines and ping to each other.



```
(shikhar㉿kali)-[~/Desktop]$ ping 172.31.6.252
PING 172.31.6.252 (172.31.6.252) 56(84) bytes of data.
shikhar
```

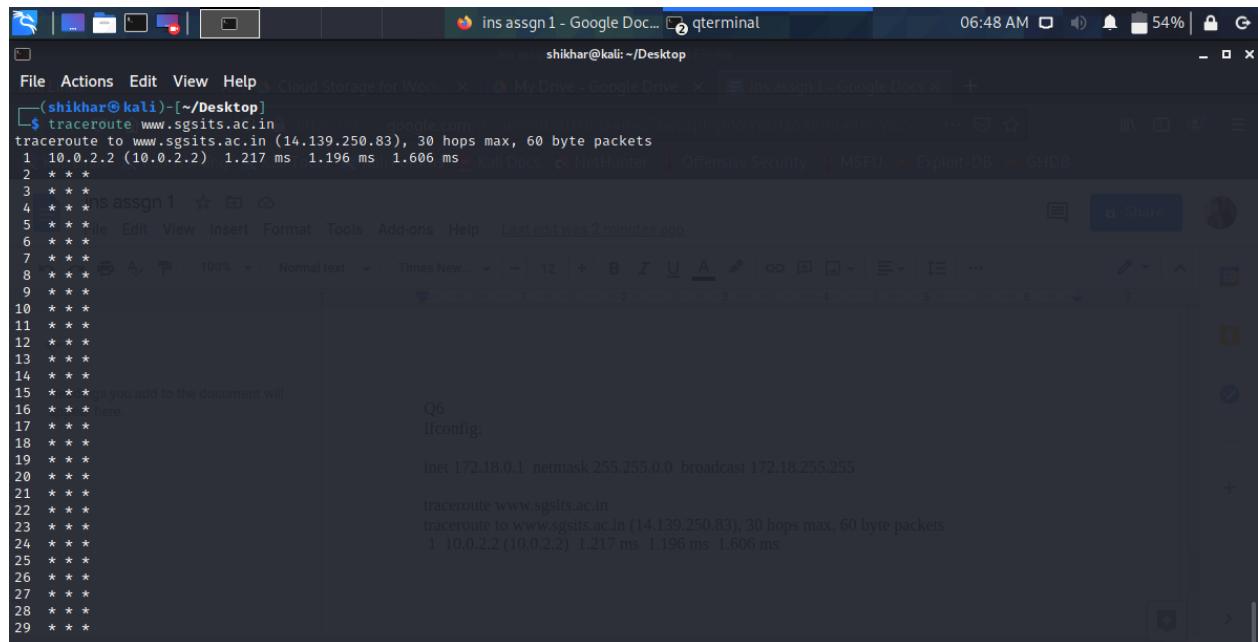
III. Run the traceroute command from one virtual machine to another virtual machine's IP and give the explanation of the output.



A screenshot of a Kali Linux desktop environment. The terminal window shows the command `traceroute 172.31.6.252` being run, which traces the route to a host at 172.31.6.252 through various routers. The desktop background features the Kali logo.

```
(shikhar㉿kali)-[~/Desktop]
$ traceroute 172.31.6.252
traceroute to 172.31.6.252 (172.31.6.252), 30 hops max, 60 byte packets
1 10.0.2.2 (10.0.2.2) 0.627 ms 0.410 ms 0.552 ms
2 * * *
3 * * *
4 * * *
5 * * *
6 * * *
7 * * *
8 * * *
9 * * *
10 * * *
11 * * *
12 * * *
13 * * *
14 * * *
15 * * *
16 * * *
17 * * *
18 * * *
19 * * *
20 * * *
21 * * *
22 * * *
23 * * *
24 * * *
25 * * *
26 * * *
27 * * *
28 * * *
```

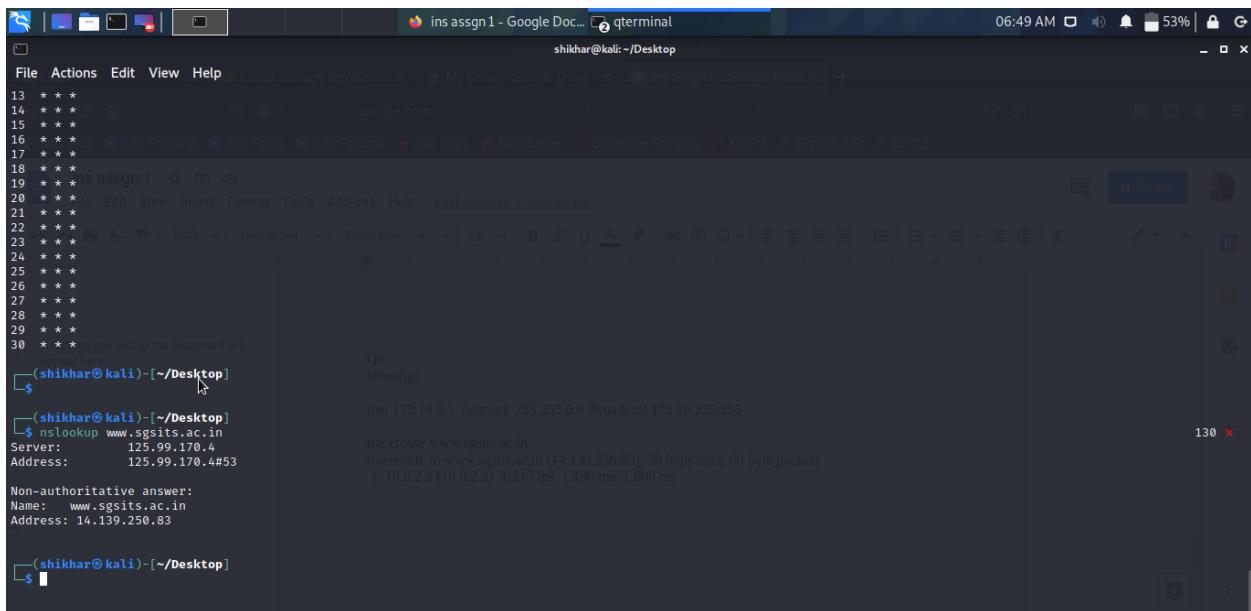
IV. Run the traceroute command for the target website i.e. www.sgsits.ac.in and give the explanation of the output.



A screenshot of a Kali Linux desktop environment. The terminal window shows the command `traceroute www.sgsits.ac.in` being run, which traces the route to the website www.sgsits.ac.in. The desktop background features the Kali logo.

```
(shikhar㉿kali)-[~/Desktop]
$ traceroute www.sgsits.ac.in
traceroute to www.sgsits.ac.in (14.139.250.83), 30 hops max, 60 byte packets
1 10.0.2.2 (10.0.2.2) 1.217 ms 1.196 ms 1.606 ms
2 * * *
3 * * *
4 * * *
5 * * * as you add to the document will
6 * * *
7 * * *
8 * * *
9 * * *
10 * * *
11 * * *
12 * * *
13 * * *
14 * * *
15 * * * here
16 * * *
17 * * *
18 * * *
19 * * *
20 * * *
21 * * *
22 * * *
23 * * *
24 * * *
25 * * *
26 * * *
27 * * *
28 * * *
29 * * *
```

V. Run the nslookup on the target website i.e. www.sgsits.ac.in and write the name/IP of the server, mail server, IP address of the target website etc.

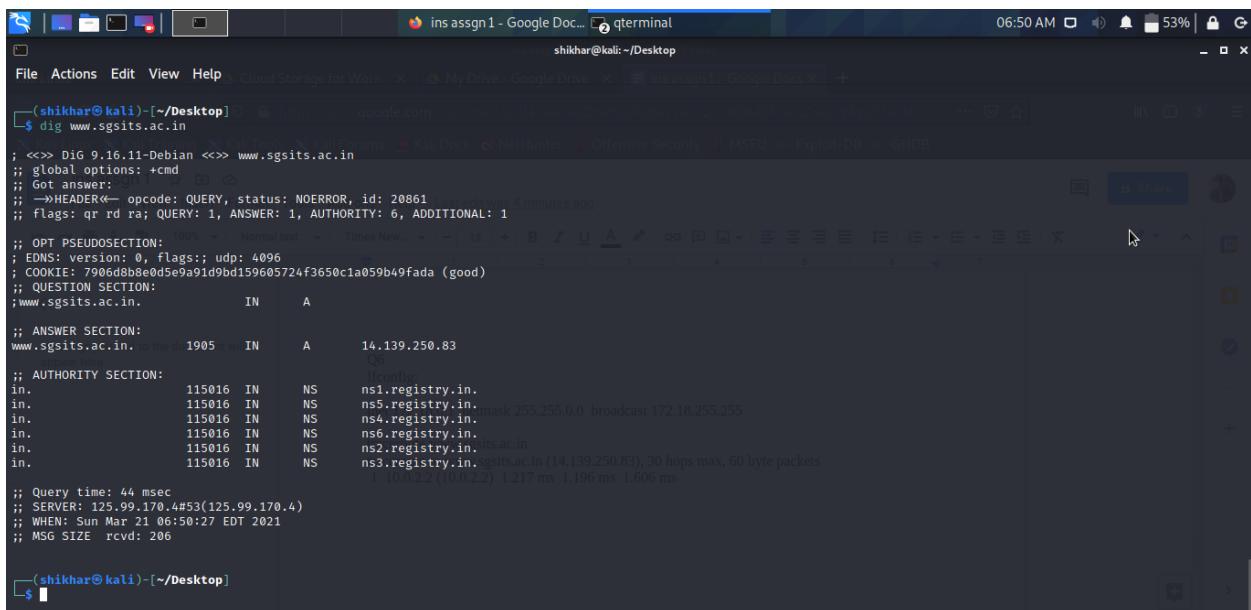


```

(shikhar㉿kali)-[~/Desktop]$ nslookup www.sgsits.ac.in
Server: 125.99.170.4#53
Address: 125.99.170.4#53

Non-authoritative answer:
Name: www.sgsits.ac.in
Address: 14.139.250.83
  
```

VI. Run the dig on the target website i.e. www.sgsits.ac.in and give the explanation of the output. Execute the dig command to get the name of the name servers and mail servers etc.



```

(shikhar㉿kali)-[~/Desktop]$ dig www.sgsits.ac.in
; <>>> DiG 9.16.11-Debian <>> www.sgsits.ac.in
;; global options: +cmd
;; Got answer:
;; ->HEADER<- opcode: QUERY, status: NOERROR, id: 20861
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 6, ADDITIONAL: 1
;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
; COOKIE: 7906db8e0d5e9a91d9bd159605724f3650c1a059b49fada (good)
;QUESTION SECTION:
www.sgsits.ac.in. IN A
;; ANSWER SECTION:
www.sgsits.ac.in. 1905 IN A 14.139.250.83
;; AUTHORITY SECTION:
in. 115016 IN NS ns1.registry.in.
in. 115016 IN NS ns5.registry.in.
in. 115016 IN NS ns4.registry.in.
in. 115016 IN NS ns6.registry.in.
in. 115016 IN NS ns2.registry.in.
in. 115016 IN NS ns3.registry.in.
  
```

VII. Run the netstat command and print the routing table of each of the virtual Machine.

```
(shikhar㉿kali)-[~/Desktop]
$ netstat -an
Active Internet connections (w/o servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
tcp   0      0      10.0.2.15:52314        bom07s26-in-f14.1:https ESTABLISHED
tcp   0      0      10.0.2.15:50596        bom12s12-in-f10.1:https ESTABLISHED
tcp   0      0      10.0.2.15:52074        bom07s25-in-f14.1:https ESTABLISHED
tcp   0      0      10.0.2.15:52168        74.125.24.189:https ESTABLISHED
tcp   0      0      10.0.2.15:33566        ec2-52-40-68-247:https ESTABLISHED
tcp   0      0      10.0.2.15:49716        bom12s14-in-f1.1e:https ESTABLISHED
tcp   0      0      10.0.2.15:38230        bom12s01-in-f3.1e:https ESTABLISHED
tcp   0      0      10.0.2.15:52364        bom07s30-in-f14.1:https ESTABLISHED
tcp   0      0      10.0.2.15:33162        bom12s10-in-f14.1:https ESTABLISHED
tcp   0      0      10.0.2.15:bootpc       10.0.2.2:bootps    ESTABLISHED
Active UNIX domain sockets (w/o servers)
Proto RefCnt Flags       Type            State           I-Node Path
unix  2      [ ]      DGRAM          0      20619  /run/user/1000/systemd/notify
unix  3      [ ]      DGRAM          1      12166  /run/systemd/notify
unix  2      [ ]      DGRAM          1      12182  /run/systemd/journal/syslog
unix  12     [ ]      DGRAM          1      12188  /run/systemd/journal/dev-log
unix  7      [ ]      DGRAM          1      12190  /run/systemd/journal/socket
unix  2      [ ]      DGRAM          1      14692  @00010
unix  3      [ ]      STREAM          CONNECTED    73879  /run/systemd/journal/stdout
unix  3      [ ]      STREAM          CONNECTED    23565  traceroute www.sgsits.ac.in (14.139.250.83), 30 hops max, 60 byte packets
unix  3      [ ]      STREAM          CONNECTED    21708  10.0.2.2 (10.0.2.2) 1.217 ms 1.196 ms 1.606 ms
unix  3      [ ]      STREAM          CONNECTED    20899
unix  3      [ ]      STREAM          CONNECTED    14109
unix  3      [ ]      STREAM          CONNECTED    42839
unix  3      [ ]      STREAM          CONNECTED    42791
unix  3      [ ]      DGRAM          20621
unix  3      [ ]      STREAM          CONNECTED    45284
unix  3      [ ]      STREAM          CONNECTED    23425  /run/user/1000/bus
unix  3      [ ]      STREAM          CONNECTED    23566
```

VIII. Run the arp command and give the explanation of the output.

```
(shikhar㉿kali)-[~/Desktop]
$ arp
Address      HWtype  HWaddress          Flags Mask Iface
172.18.0.5   ether   02:42:ac:12:00:05  C      br-f4ab20767ba5
172.18.0.2   ether   02:42:ac:12:00:02  C      br-f4ab20767ba5
172.18.0.6   assign1  ether   02:42:ac:12:00:06  C      br-f4ab20767ba5
172.18.0.3   Edit   View   ether   02:42:ac:12:00:03  C      Last edit was 7 minutes ago
172.18.0.4   ether   02:42:ac:12:00:04  C      br-f4ab20767ba5
10.0.2.2     ether   52:54:00:12:35:02  C      eth0

(shikhar㉿kali)-[~/Desktop]
$ 
$ 

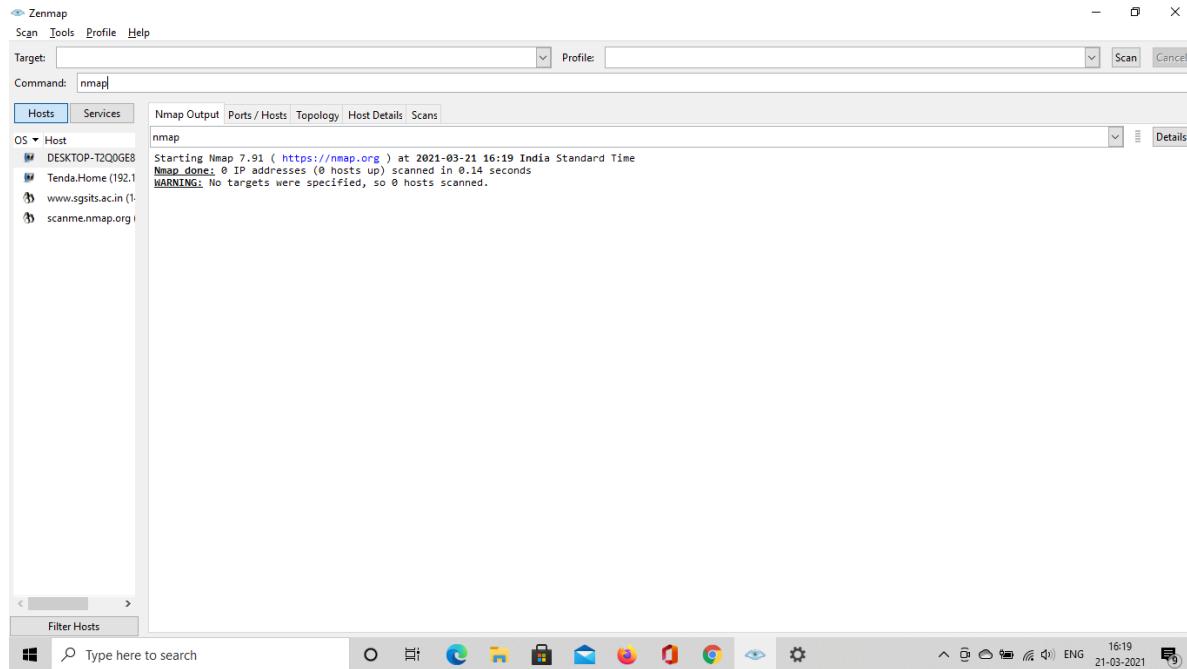
Headings you add to the document will appear here.

Q6
lconfig:
net 172.18.0.1 netmask 255.255.0.0 broadcast 172.18.255.255

traceroute www.sgsits.ac.in
traceroute to www.sgsits.ac.in (14.139.250.83), 30 hops max, 60 byte packets
1  10.0.2.2 (10.0.2.2) 1.217 ms 1.196 ms 1.606 ms
```

Q7. Execute the nmap command and answer the following questions:

I. Execute the nmap on both the target machine i.e. windows & metasploitable 2 and give the explanation of the output.



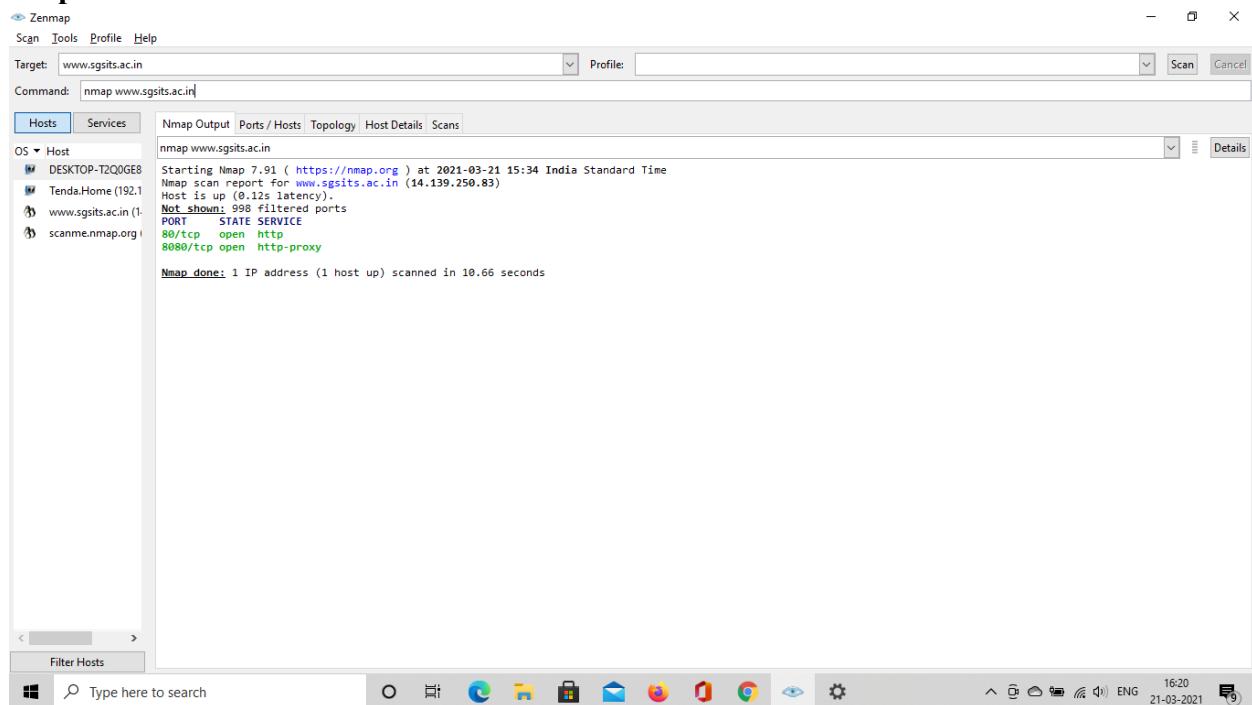
```

Zenmap
Scan Tools Profile Help
Target: [ ] Profile: [ ]
Command: nmap
Hosts Services Nmap Output Ports / Hosts Topology Host Details Scans
OS Host
DESKTOP-T2Q0GE8
Tenda.Home (192.1
www.sgsits.ac.in (1:
scanme.nmap.org

nmap
Starting Nmap 7.91 ( https://nmap.org ) at 2021-03-21 16:19 India Standard Time
Nmap done: 0 IP addresses (0 hosts up) scanned in 0.14 seconds
WARNING: No targets were specified, so 0 hosts scanned.

```

II. Execute the nmap on target website i.e. www.sgsits.ac.in and give the explanation of the Output.



```

Zenmap
Scan Tools Profile Help
Target: www.sgsits.ac.in Profile: [ ]
Command: nmap www.sgsits.ac.in
Hosts Services Nmap Output Ports / Hosts Topology Host Details Scans
OS Host
DESKTOP-T2Q0GE8
Tenda.Home (192.1
www.sgsits.ac.in (1:
scanme.nmap.org

nmap www.sgsits.ac.in
Starting Nmap 7.91 ( https://nmap.org ) at 2021-03-21 15:34 India Standard Time
Nmap scan report for www.sgsits.ac.in (14.139.250.83)
Host is up (0.12s latency).
Not shown: 998 filtered ports
PORT      STATE SERVICE
80/tcp    open  http
8080/tcp  open  http-proxy

Nmap done: 1 IP address (1 host up) scanned in 10.66 seconds

```

III. Execute the nmap on both the target machine i.e. windows & metasploitable 2 and display the open port in detail.

```

Starting Nmap 7.91 ( https://nmap.org ) at 2021-03-21 16:22 India Standard Time
Illegal character(s) in hostname -- replacing with '*'.
Nmap scan report for scanne.nmap.org (45.33.32.156)
Host is up (0.25s latency).
Not shown: 992 closed ports, 4 filtered ports
Some closed ports may be reported as filtered due to --defeat-rst-ratelimit
PORT      STATE SERVICE VERSION
22/tcp    open  ssh   OpenSSH 6.6.1p1 Ubuntu 2ubuntu2.13 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|_ 1024 ac:00:1a:82:ff:cc:55:99:dc:67:2b:34:97:6b:75 (DSA)
|_ 2048 20:3d:2d:44:62:2a:b0:5a:9d:b5:b3:05:14:c2:a6:b2 (RSA)
|_ 256 96:02:bb:5e:57:54:1c:4e:45:2:f5:56:4c:4a:24:b2:57 (ECDSA)
|_ 256 33:fa:91:0f:e0:e1:7b:1f:6d:05:a2:b0:f1:54:41:56 (ED25519)
80/tcp    open  http  Apache httpd 2.4.7 ((Ubuntu))
|_http-favicon: Nmap Project
|_http-server-header: Apache/2.4.7 (Ubuntu)
|_http-title: Go ahead and ScanMe!
|_http-user-agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/89.0.4369.90 Safari/537.36
|_http-ping: echo
31337/tcp open  tcpwrapped
Aggressive OS guesses: Linux 5.0 (93%), Linux 5.4 (93%), Linux 5.0 - 5.4 (93%), HP P2000 G3 NAS device (91%), Linux 4.15 - 5.6 (91%), Linux 2.6.32 (90%), Linux 2.6.32 - 3.1 (90%), Linux 3.7 (90%), Linux 5.3 - 5.4 (90%), Linux 2.6.32 - 3.13 (90%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 18 hops
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE (using port 443/tcp)
HOP RTT      ADDRESS
1  3.00 ms  Tenda.Home (192.168.1.1)
2  41.00 ms  117.199.16.1
3  40.00 ms  static.illi.218.248.111.138*24.bsnl.in (218.248.111.138)
4  ...      5
6  55.00 ms  115.110.229.45.static-mumbai.vsnl.net.in (115.110.229.45)
7  56.00 ms  172.23.78.233
8  82.00 ms  172.31.244.45
9  269.00 ms  180.87.37.1
10 ...     11
12 176.00 ms  if-et-23-2.hcore1.kv8-chiba.as64
13 299.00 ms  if-ae-5-2.tcore2.svl-santaclarra
14 290.00 ms  if-ae-5-2.tcore2.svl-santaclarra

```

IV. Execute the nmap on both the target machine i.e. windows & metasploitable 2 and display the OS.

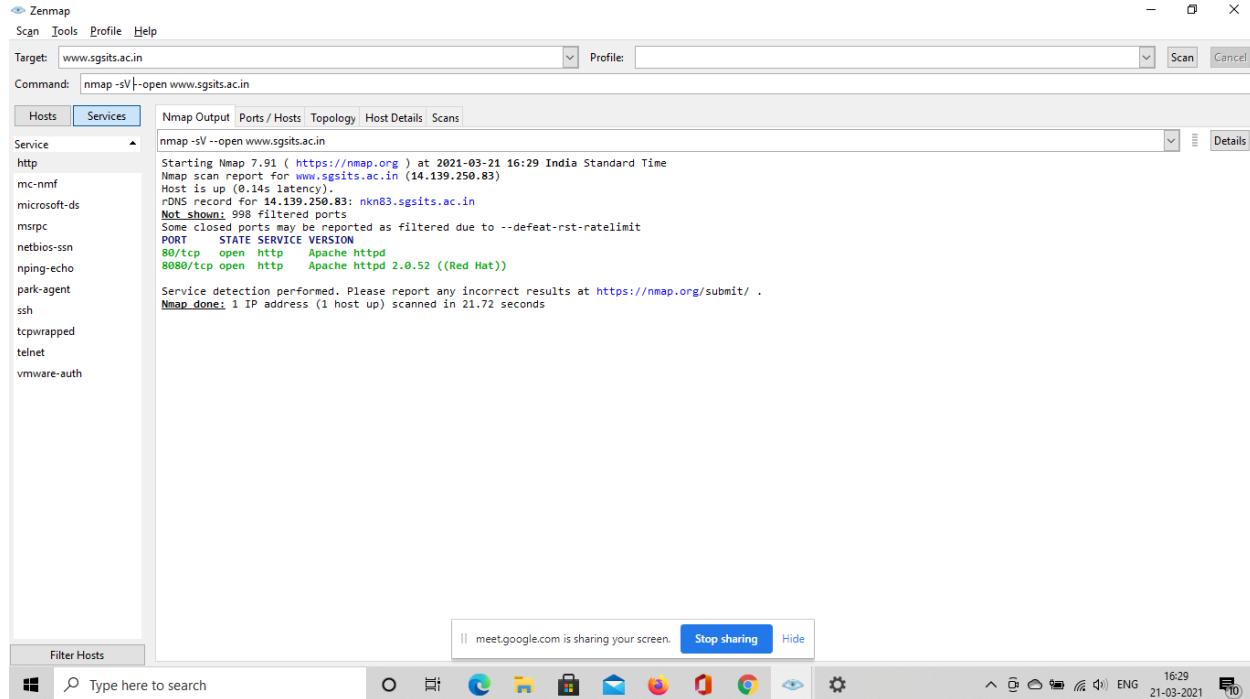
```

Starting Nmap 7.91 ( https://nmap.org ) at 2021-03-21 16:29 India Standard Time
Nmap scan report for www.sgsits.ac.in (14.139.250.83)
Host is up (0.14s latency).
rDNS record for 14.139.250.83: nkn83.sgsits.ac.in
Not shown: 998 filtered ports
Some closed ports may be reported as filtered due to --defeat-rst-ratelimit
PORT      STATE SERVICE VERSION
80/tcp    open  http  Apache httpd 2.0.52 ((Red Hat))
8080/tcp  open  http  Apache httpd 2.0.52 ((Red Hat))

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 21.72 seconds

```

V. Execute the nmap on both the target machine i.e. windows & metasploitable 2 and display the services running on various open ports.



```
Metasploitable2-Linux - VMware Workstation 16 Player (Non-commercial use only)
```

```
msfadmin@metasploitable:~$ nmap -o -A www.sgsits.ac.in
Starting Nmap 4.53 ( http://insecure.org ) at 2021-03-24 01:40 EDT
Stats: 0:02:32 elapsed: 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 20.88% done; ETC: 01:46 (0:09:33 remaining)
Stats: 0:04:33 elapsed: 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 22.05% done; ETC: 01:54 (0:16:09 remaining)
Stats: 0:04:35 elapsed: 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 22.06% done; ETC: 01:54 (0:16:12 remaining)

msfadmin@metasploitable:~$ nmap -o -A www.sgsits.ac.in
Starting Nmap 4.53 ( http://insecure.org ) at 2021-03-24 01:40 EDT
Stats: 0:00:39 elapsed: 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 25.96% done; ETC: 01:43 (0:01:50 remaining)
Stats: 0:00:52 elapsed: 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 27.27% done; ETC: 01:43 (0:02:18 remaining)
Stats: 0:02:46 elapsed: 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 80.88% done; ETC: 01:44 (0:00:39 remaining)
Interesting ports on www.sgsits.ac.in (14.139.250.83):
Not shown: 1711 filtered ports
PORT      STATE SERVICE
25/tcp    open  smtp
80/tcp    open  http
8080/tcp  open  http-proxy

Nmap done: 1 IP address (1 host up) scanned in 184.451 seconds
msfadmin@metasploitable:~$
```

VI. Execute the nmap in the given IP range and display the services running at specified ports i.e. port 80, 20, 21 etc. in that IP range.

The screenshot shows a Kali Linux desktop environment within Oracle VM VirtualBox. The terminal window displays the output of an nmap scan:

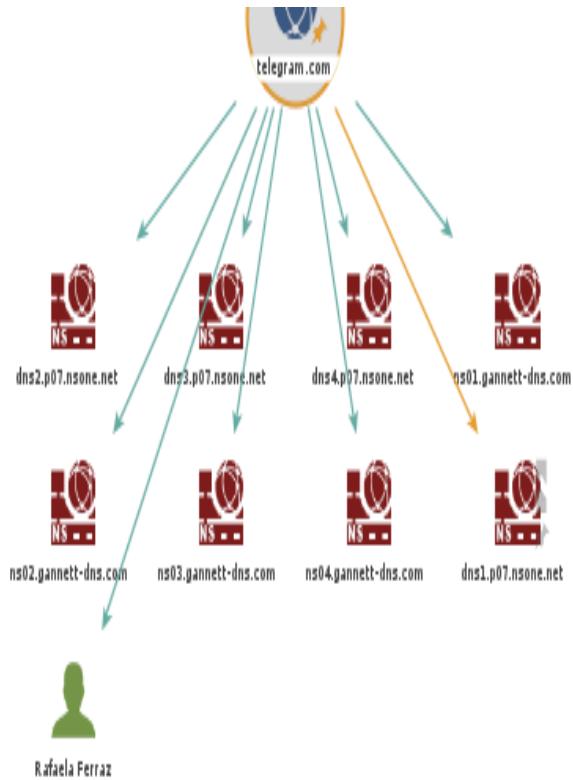
```
(shikhar㉿kali)-[~/Desktop]$ nmap -F 10.0.2.15
Starting Nmap 7.91 ( https://nmap.org ) at 2021-03-24 06:05 EDT
Nmap scan report for 10.0.2.15
Host is up (0.00073s latency).
All 100 scanned ports on 10.0.2.15 are closed

Nmap done: 1 IP address (1 host up) scanned in 0.12 seconds
```

The desktop background features the Kali logo. The taskbar at the bottom includes icons for various applications like a terminal, file manager, browser, and system settings.

Q8. Setup the Maltego application in Kali Linux and perform the following operations:

I. Select a target website/domain and perform the required transformation like email, phone no, name etc. transformations. Generate the report for all the transformation.



lol report.pdf - Adobe Acrobat Reader DC (32-bit)

File Edit View Sign Window Help

Home Tools lol report.pdf 2 / 6 66.7% Sign In

Search 'OCR'

Export PDF

Convert, edit and e-sign PDF forms & agreements

Free 7-Day Trial

1. Top 10 Entities

Total number of entities: 10
Total number of links: 9

Ranked by Incoming Links

Rank	Type	Value	Incoming links
1	NS Record	dns1.p07.nsone.net	1
2	NS Record	ns04.gannett-dns.com	1
3	NS Record	ns03.gannett-dns.com	1
4	NS Record	dns2.p07.nsone.net	1
5	NS Record	ns02.gannett-dns.com	1
6	NS Record	ns01.gannett-dns.com	1
7	NS Record	dns4.p07.nsone.net	1
8	Person	Rafaela Ferraz	1
9	NS Record	dns3.p07.nsone.net	1
10	Domain	telegram.com	0

Ranked by Outgoing Links

Rank	Type	Value	Outgoing links
1	Domain	telegram.com	9
2	NS Record	dns1.p07.nsone.net	0
3	NS Record	ns04.gannett-dns.com	0
4	NS Record	ns03.gannett-dns.com	0
5	NS Record	dns2.p07.nsone.net	0
6	NS Record	ns02.gannett-dns.com	0
7	NS Record	ns01.gannett-dns.com	0
8	NS Record	dns4.p07.nsone.net	0
9	Person	Rafaela Ferraz	0
10	NS Record	dns3.p07.nsone.net	0

Ranked by Total Links

Rank	Type	Value	Total links
1	Domain	telegram.com	9
2	NS Record	dns1.p07.nsone.net	1
3	NS Record	ns04.gannett-dns.com	1
4	NS Record	ns03.gannett-dns.com	1

lol report.pdf - Adobe Acrobat Reader DC (32-bit)

File Edit View Sign Window Help

Home Tools lol report.pdf 3 / 6 66.7% Sign In

Search 'OCR'

Export PDF

Convert, edit and e-sign PDF forms & agreements

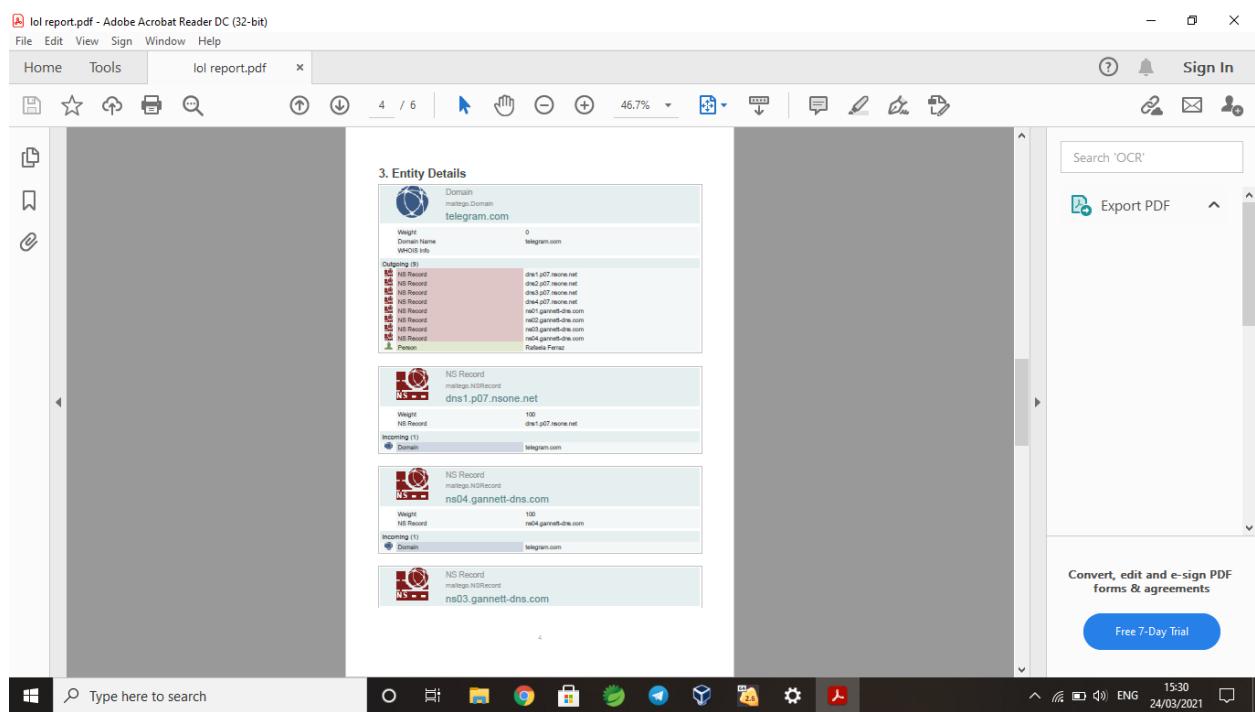
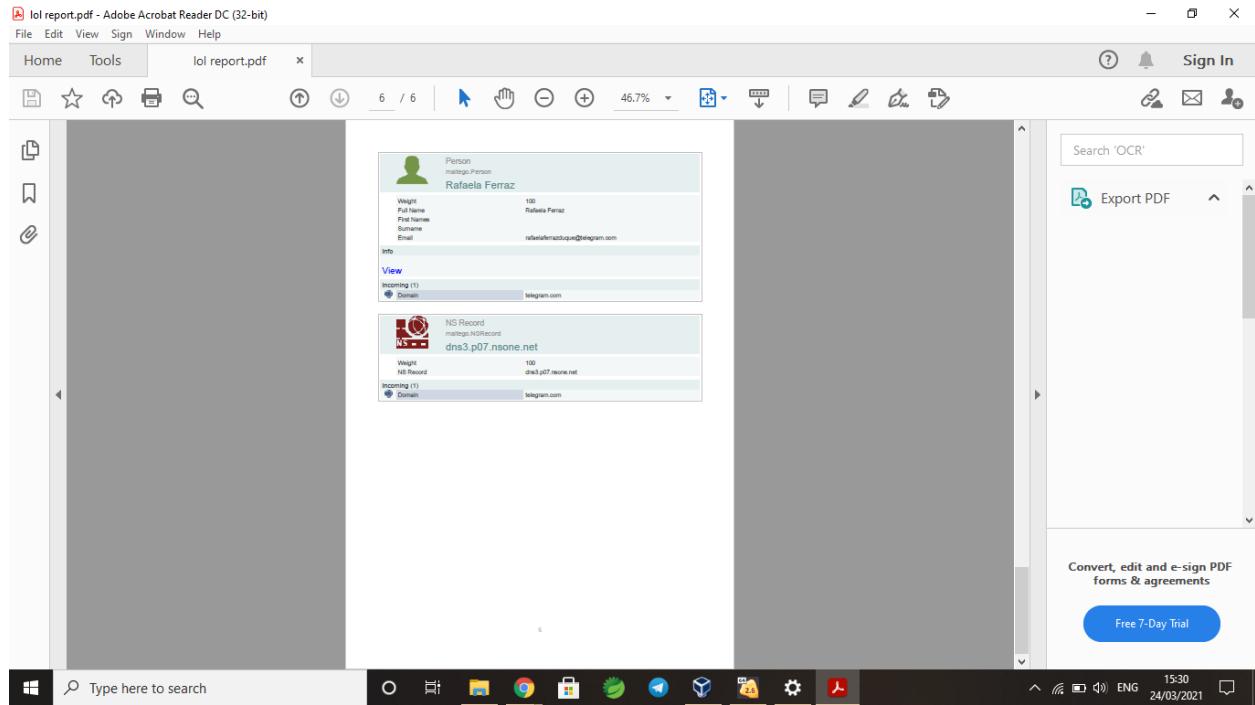
Free 7-Day Trial

2. Entities by Type

Domains (1)
telegram.com

NS Records (8)
dns1.p07.nsone.net
dns3.p07.nsone.net
ns01.gannett-dns.com
ns03.gannett-dns.com
dns2.p07.nsone.net
dns4.p07.nsone.net
ns02.gannett-dns.com
ns04.gannett-dns.com

People (1)
Rafaela Ferraz



III. List the name of any 5 general transformations which can be performed on a particular target to get the required information.

1. To DNS Name
2. To EmailAddress [Bing]
3. IPv4Address To Entities From WHOIS [IBM Watson]
4. To IP Address [DNS]
5. To Domain [Find other TLDs]