Shri G. S. Institute of Technology & Science,

Indore,Department of Computer Engineering

Subject: Information and Network Security

Session: December – May 2021

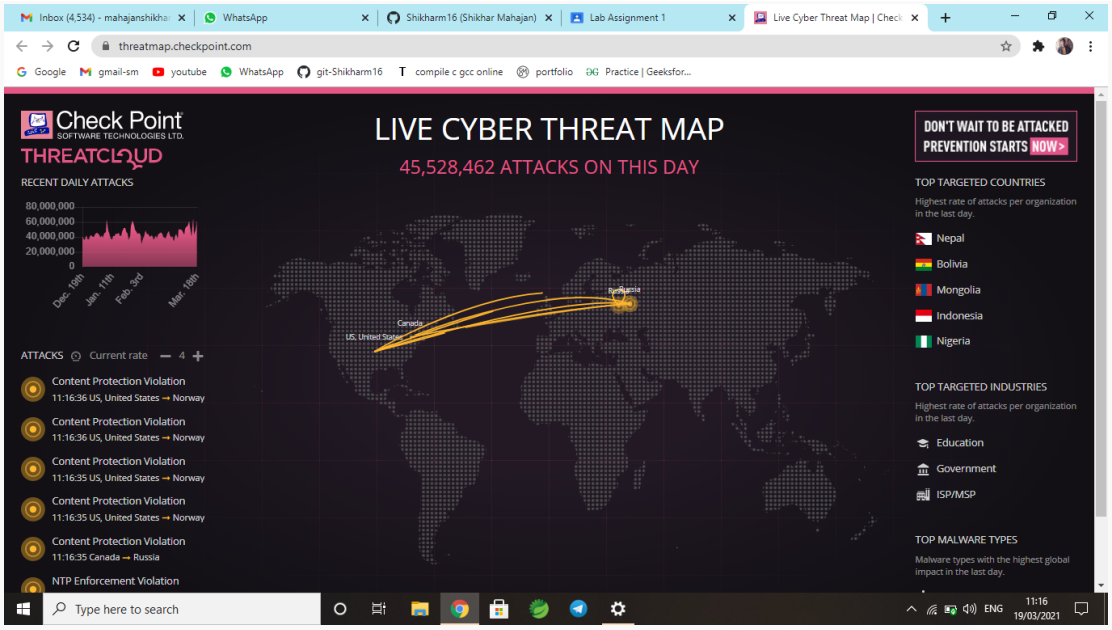
Lab Assignment

Submitted To:
Veerendra Shrivastava
Soma Saha

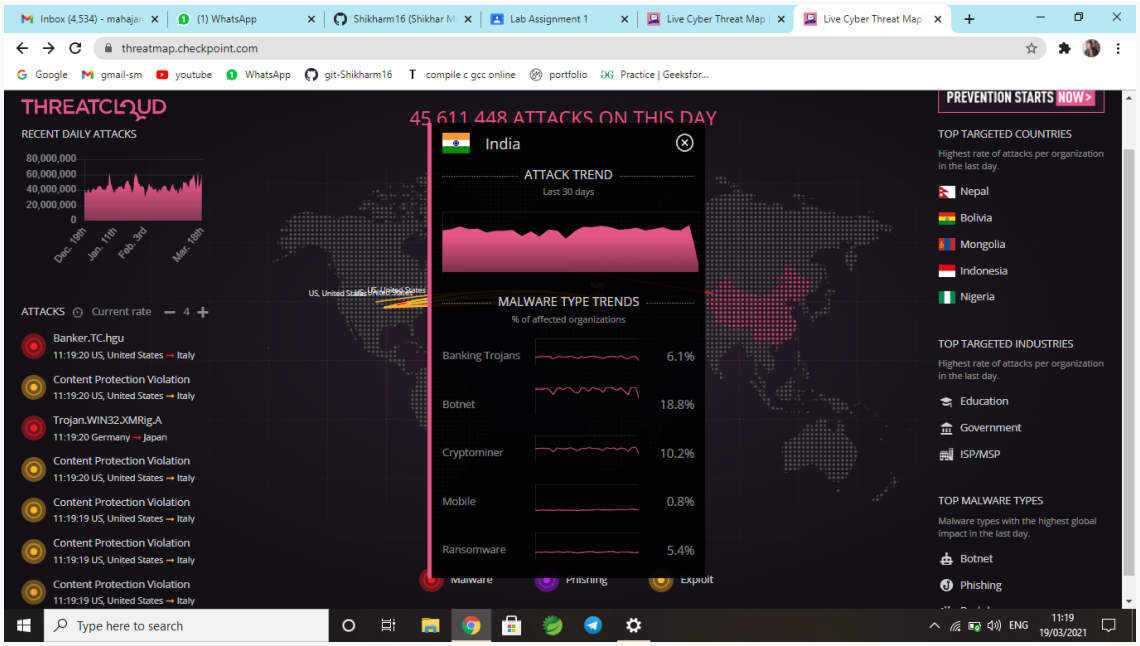
Submitted By:
Shikhar Mahajan
0801CS171077

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.

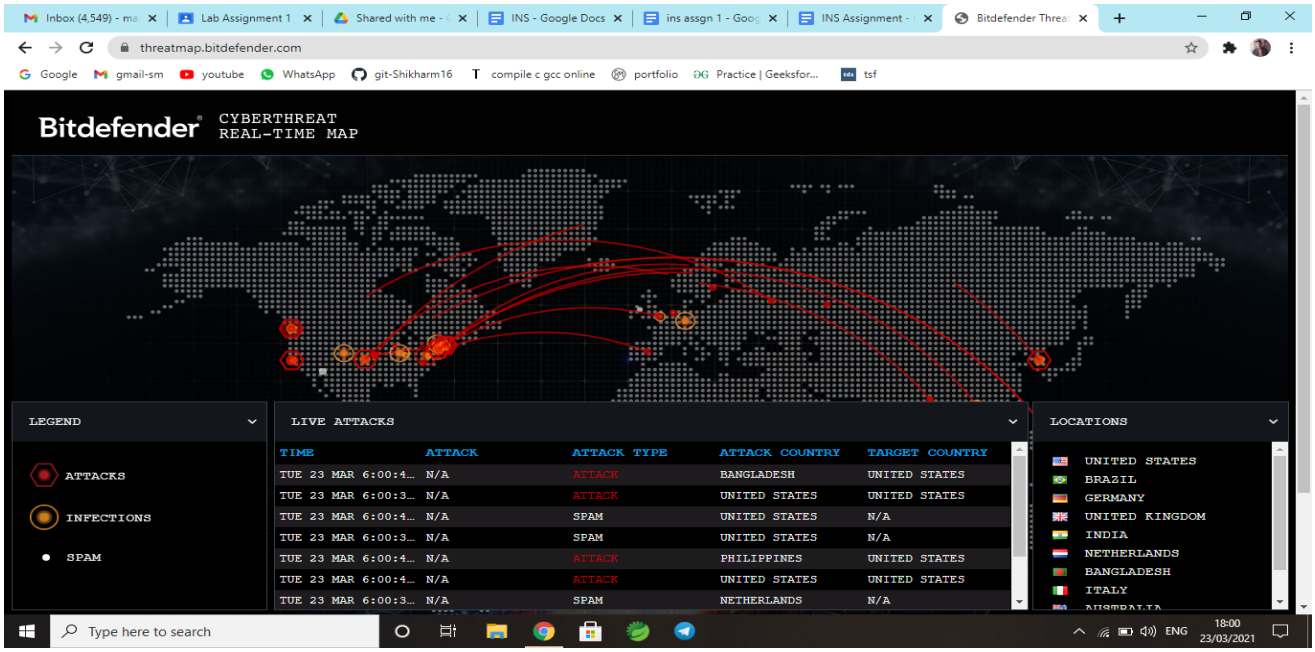
When a hacker hits a Norse sensor, the hacker believes that it has breached a system. Instead, Norse collected information about the hacker's toolkit, including his or her IP address. This information then manifested as data on the cyber attack map.

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.

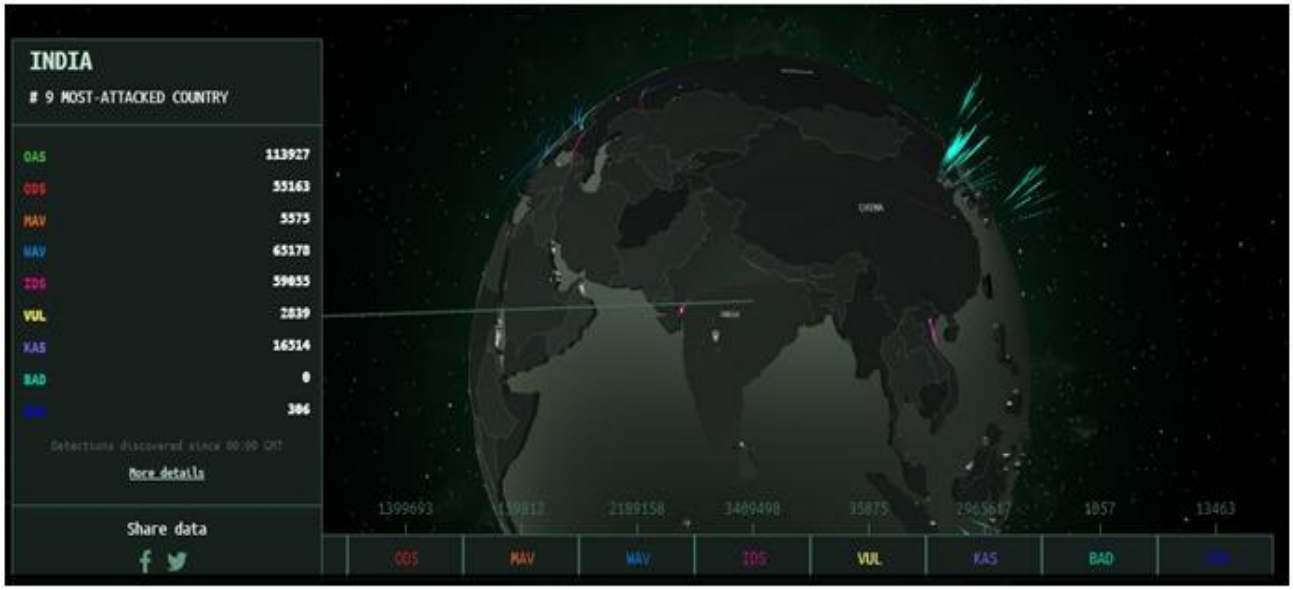
IV. Write the name of any five websites which is similar to the thread cloud and attach their screenshots.

Websites similar to ThreatCloud are:

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


Bitdefender CYBERTHREAT REAL-TIME MAP
threatmap.bitdefender.com
LEGEND
ATTACKS
INFECTIONS
SPAM
LIVE ATTACKS
TIME ATTACK ATTACK TYPE ATTACK COUNTRY TARGET COUNTRY
TUE 23 MAR 6:00:4... N/A ATTACK BANGLADESH UNITED STATES
TUE 23 MAR 6:00:3... N/A ATTACK UNITED STATES UNITED STATES
TUE 23 MAR 6:00:4... N/A SPAM UNITED STATES N/A
TUE 23 MAR 6:00:3... N/A SPAM UNITED STATES N/A
TUE 23 MAR 6:00:4... N/A ATTACK PHILIPPINES UNITED STATES
TUE 23 MAR 6:00:4... N/A ATTACK UNITED STATES UNITED STATES
TUE 23 MAR 6:00:3... N/A SPAM NETHERLANDS N/A
LOCATIONS
UNITED STATES
BRAZIL
GERMANY
UNITED KINGDOM
INDIA
NETHERLANDS
BANGLADESH
ITALY
Type here to search
ENG
18:00
23/03/2021

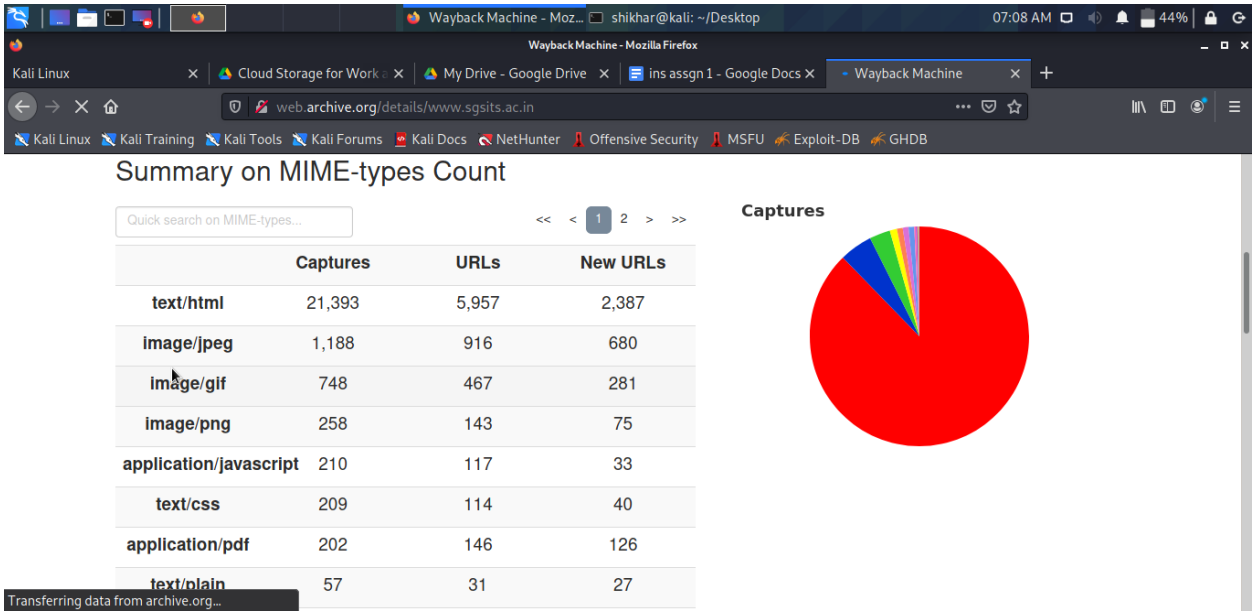

[X] NEW ATTACK: FROM [GERMANY] TO [COLOMBIA]
[X] NEW ATTACK: FROM [ALGERIA] TO [UNITED STATES]
[X] NEW ATTACK: FROM [UNITED KINGDOM] TO [UNITED STATES]
[X] NEW ATTACK: FROM [NETHERLANDS] TO [UNITED STATES]
FIREEYE CYBER THREAT MAP
APT
UNITED STATES
Backdoor.APT.LV
UNITED KINGDOM
GERMANY
ALGERIA
TOP 5 REPORTED INDUSTRIES
FINANCIAL SERVICES
SERVICES/CONSULTING
TELECOM
MANUFACTURING


INDIA
9 MOST-ATTACKED COUNTRY
OAS 113927
ODS 55163
MAV 5575
NAV 65178
IDS 59055
VUL 2839
KAS 16514
BAD 0
306
More details
Share data
1399693
2189158
3409498
35875
1857
13463
ODS
MAV
NAV
IDS
VUL
KAS
BAD

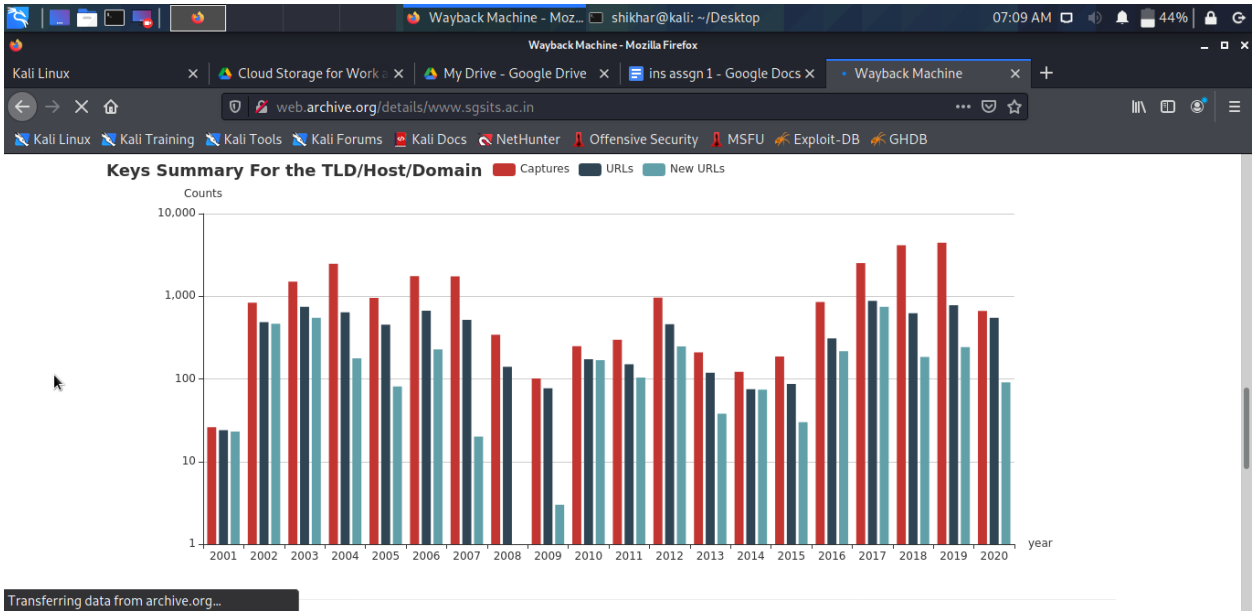

ATTACK
SEVERITY
LOCATION
Medium
Medium
High
High
Medium
High
High
High
Mexico
Argentina
United States
United States
China
United States
United States
Netherlands

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

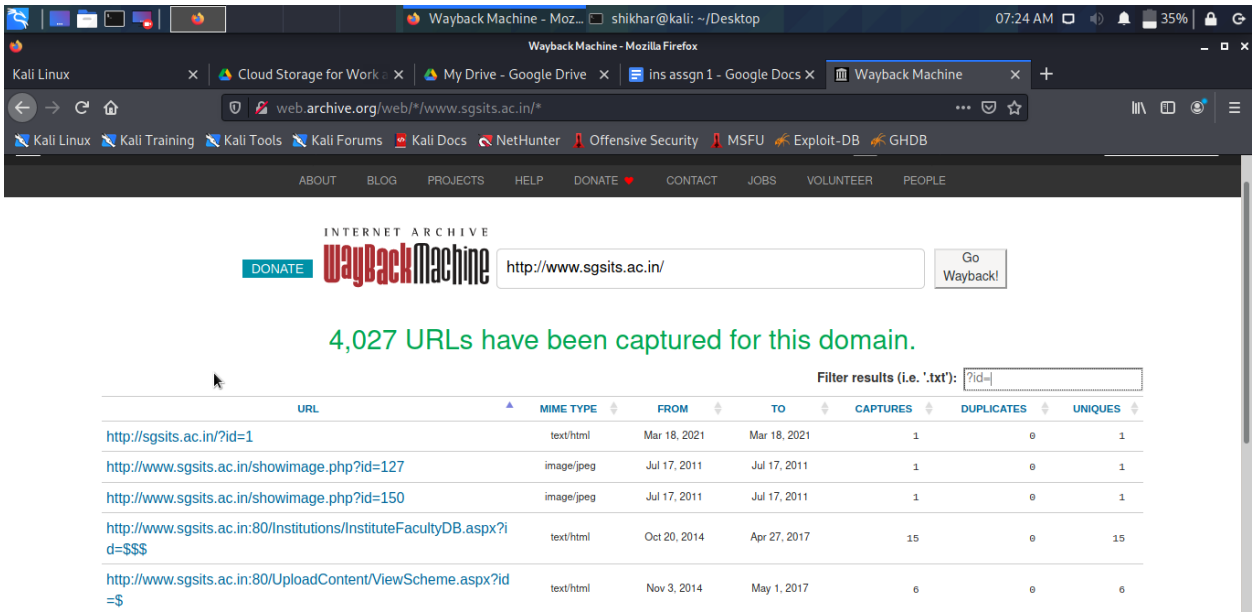
I. Search the target website on the wayback machine and count the number of captures with duration. Also attach the screenshot of your result.

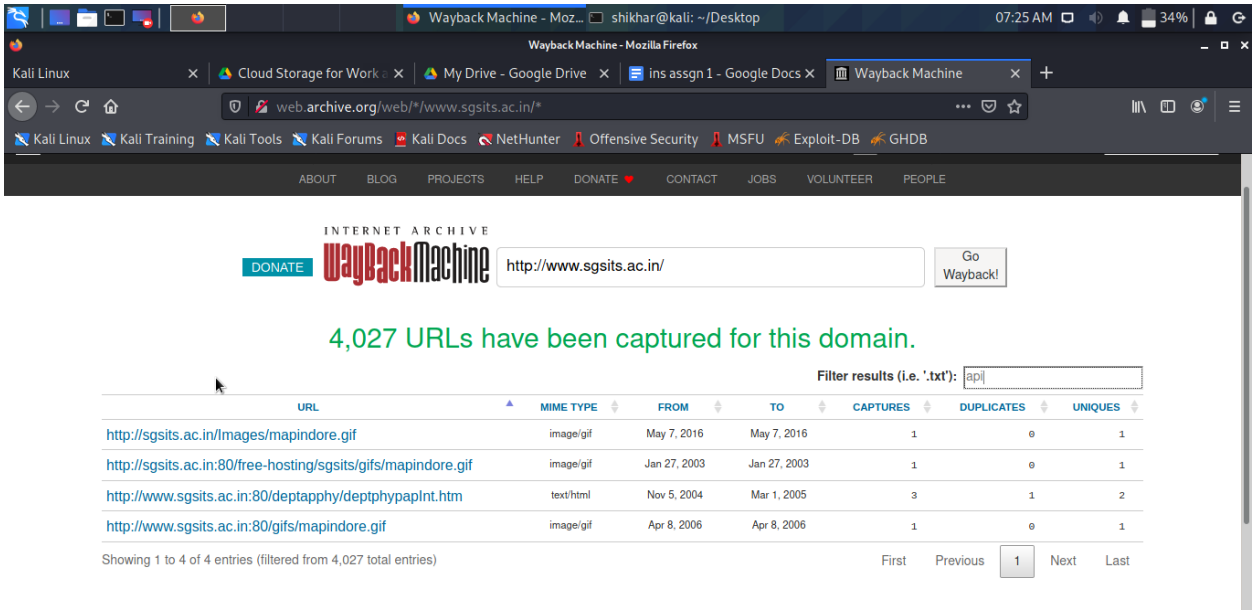


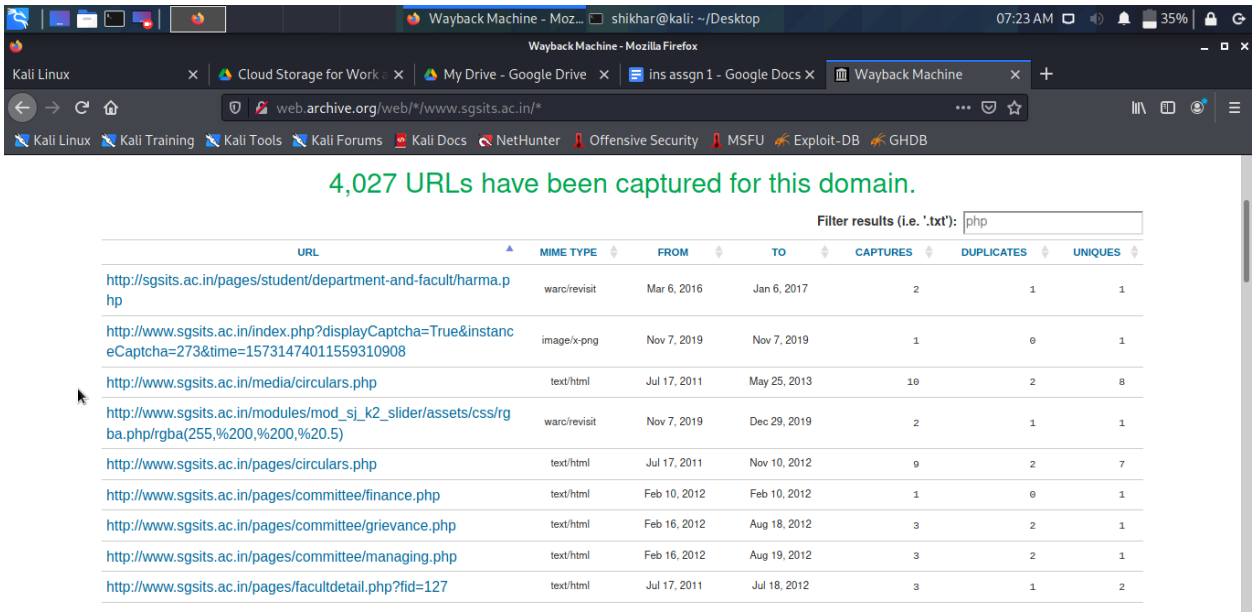
	Captures	URLs	New URLs
text/html	21,393	5,957	2,387
image/jpeg	1,188	916	680
image/gif	748	467	281
image/png	258	143	75
application/javascript	210	117	33
text/css	209	114	40
application/pdf	202	146	126
text/plain	57	31	27

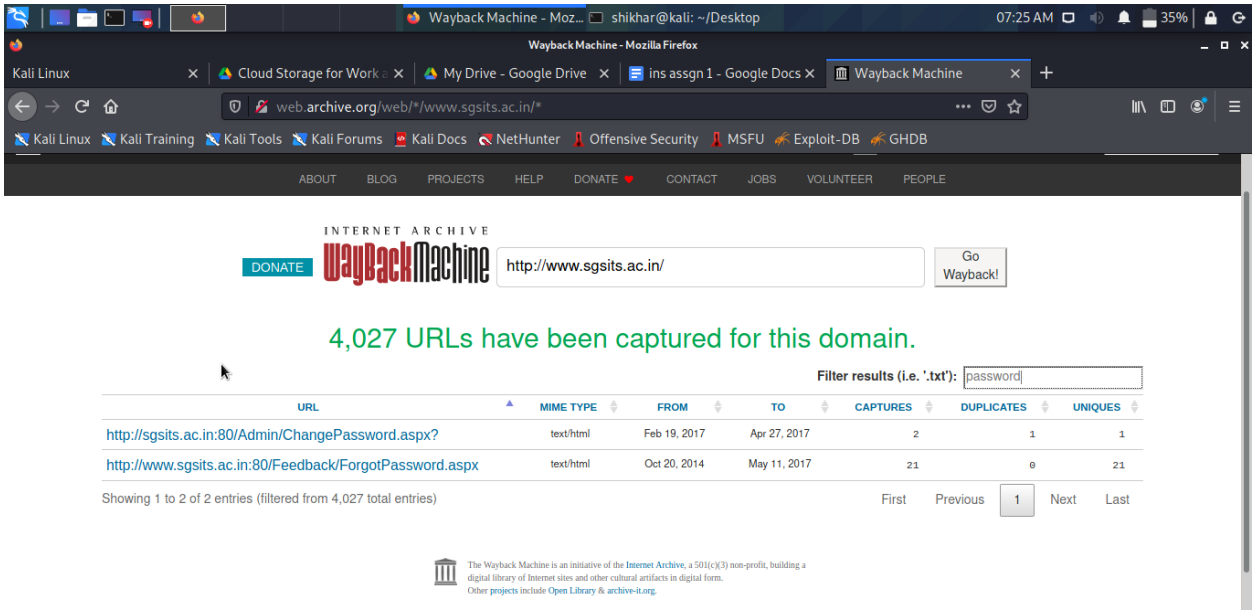


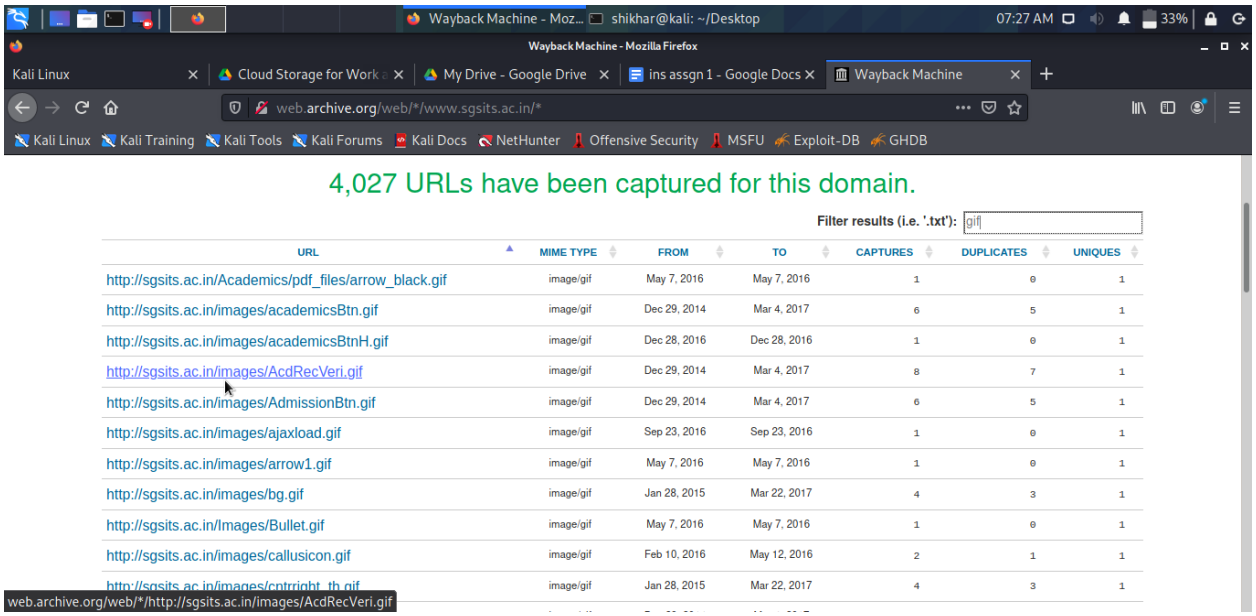
II. Try the following filters on the wayback machine for checking the vulnerabilities in the target website:?, ?id=, .zip, readme.php, readme.txt, .csv, password, /admin/, .js, /api/, .config, msg= etc. Also attach the screenshot for each filter and/or your result.




Wayback Machine - Moz... shikhar@kali: ~/Desktop
07:25 AM
34%
Wayback Machine - Mozilla Firefox
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
WayBackMachine
http://www.sgsits.ac.in/
Go Wayback!
4,027 URLs have been captured for this domain.
Filter results (i.e. '.txt'): api
URL MIME TYPE FROM TO CAPTURES DUPLICATES 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/deptapphy/deptphypapInt.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

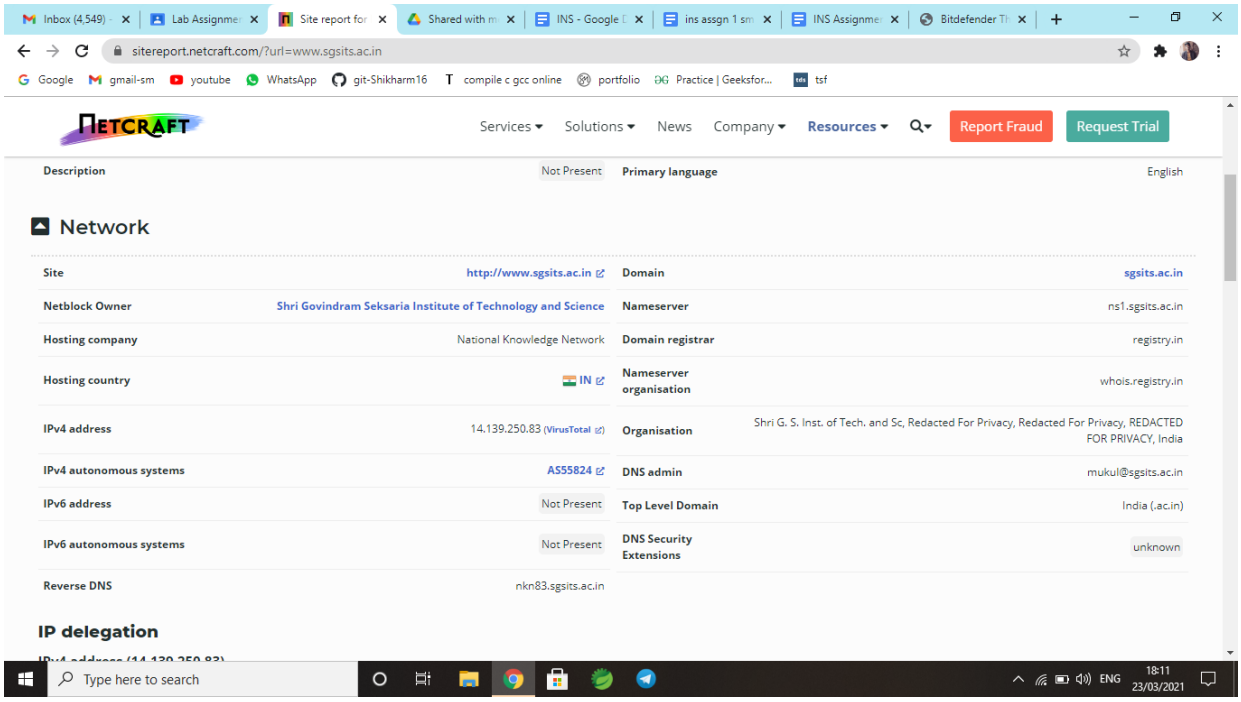

Wayback Machine - Moz... shikhar@kali: ~/Desktop
07:23 AM
35%
Wayback Machine - Mozilla Firefox
Kali Linux
Cloud Storage for Work
My Drive - Google Drive
ins assgn 1 - Google Docs
Wayback Machine
web.archive.org/web/*/www.sgsits.ac.in/*
Kali Linux Kali Training Kali Tools Kali Forums Kali Docs NetHunter Offensive Security MSFU Exploit-DB GHDB
4,027 URLs have been captured for this domain.
Filter results (i.e. '.txt'): php
URL MIME TYPE FROM TO CAPTURES DUPLICATES 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 - Moz... shikhar@kali: ~/Desktop
07:25 AM
Wayback Machine - Mozilla Firefox
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
WayBackMachine
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 DUPLICATES 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.

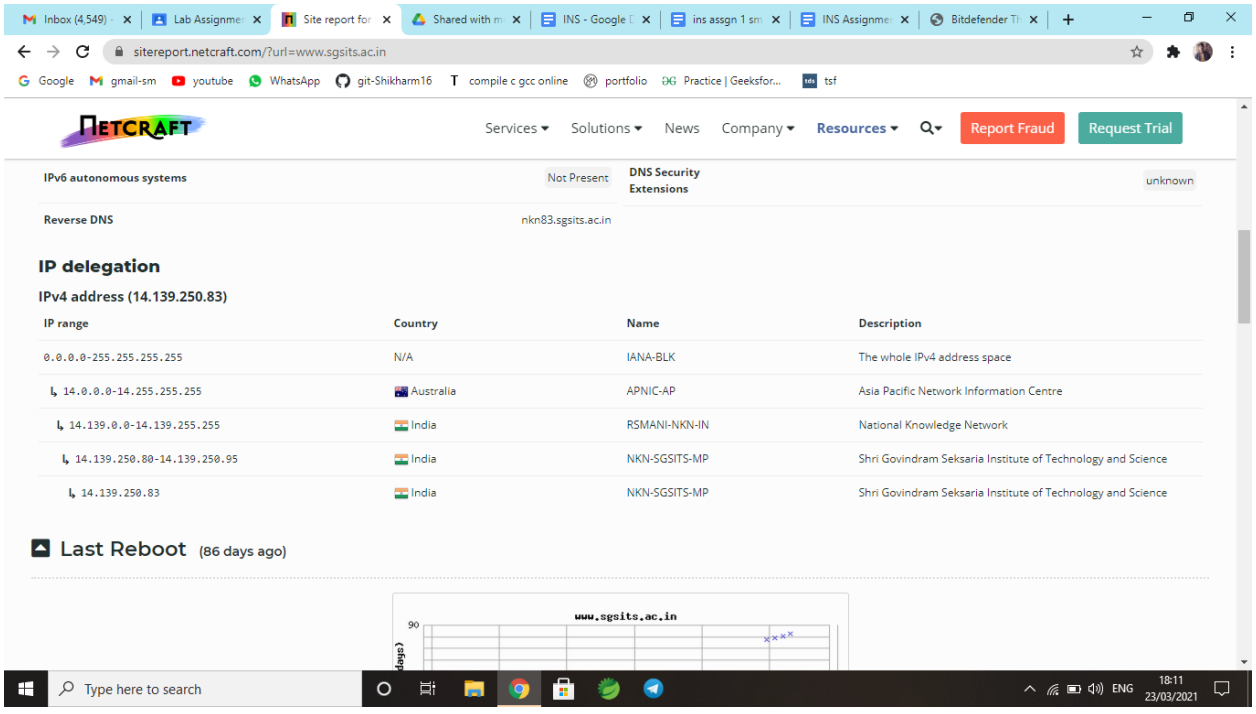

Wayback Machine - Moz... shikhar@kali: ~/Desktop
07:27 AM
Wayback Machine - Mozilla Firefox
Kali Linux
Cloud Storage for Work
My Drive - Google Drive
ins assgn 1 - Google Docs
Wayback Machine
web.archive.org/web/*/www.sgsits.ac.in/*
Kali Linux Kali Training Kali Tools Kali Forums Kali Docs NetHunter 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 DUPLICATES 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/cptrright_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 –

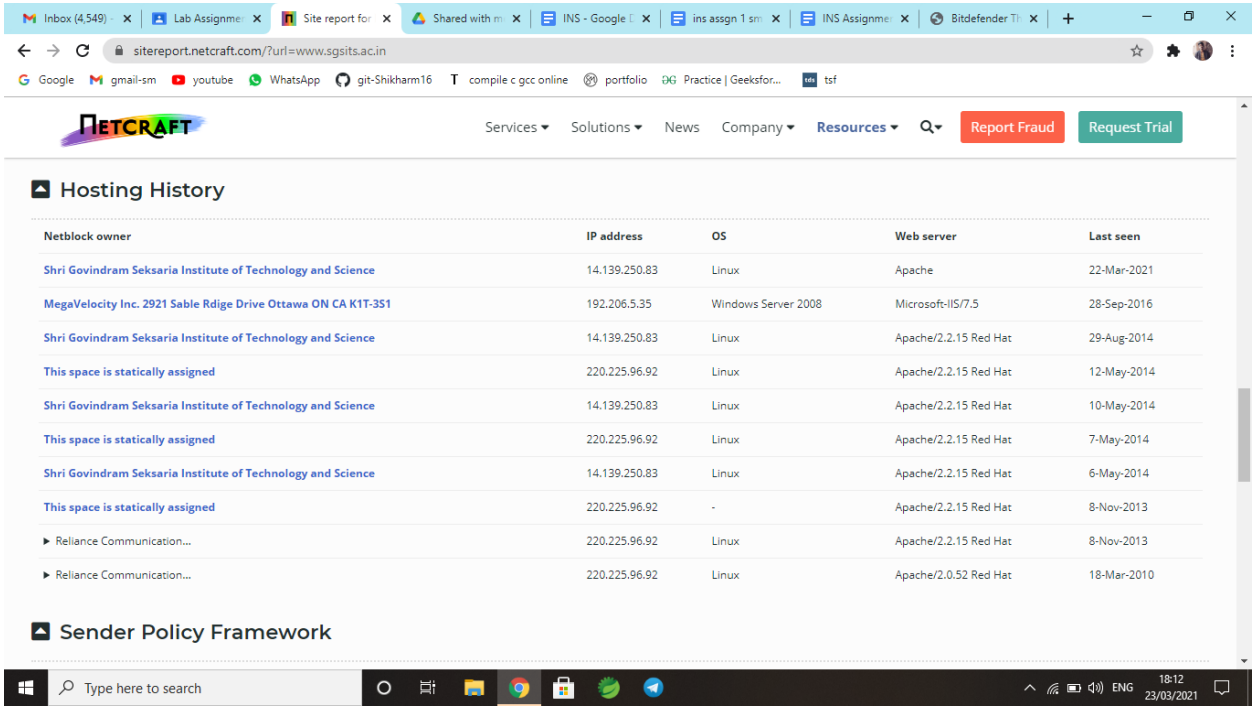
I. Write the names of various domains associated with the target website.



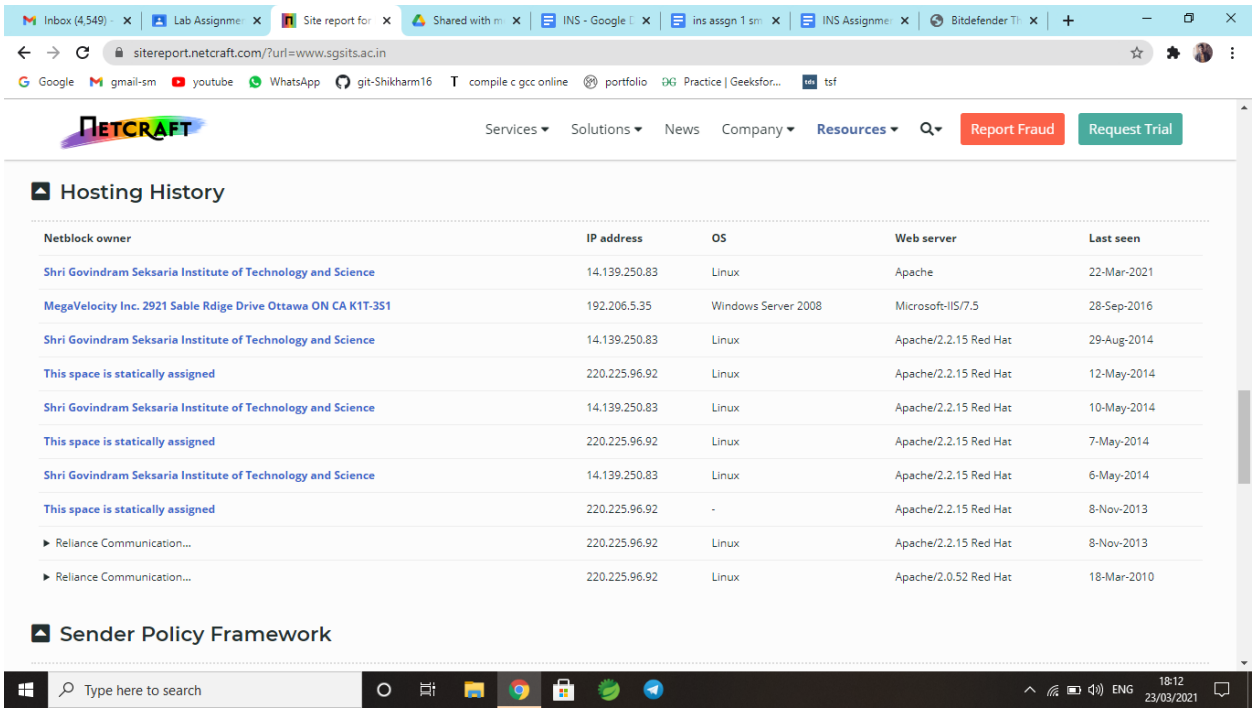
II. Write the IP version 4 and version 4 ranges associated with the target website.



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

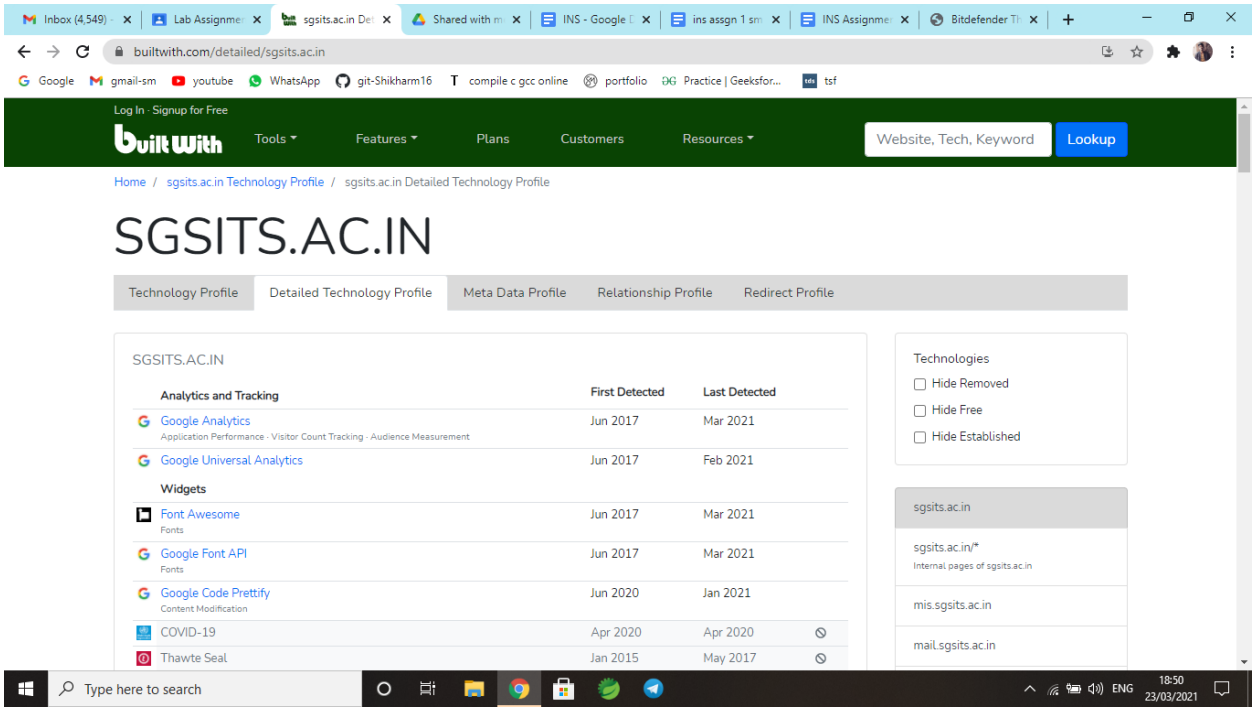


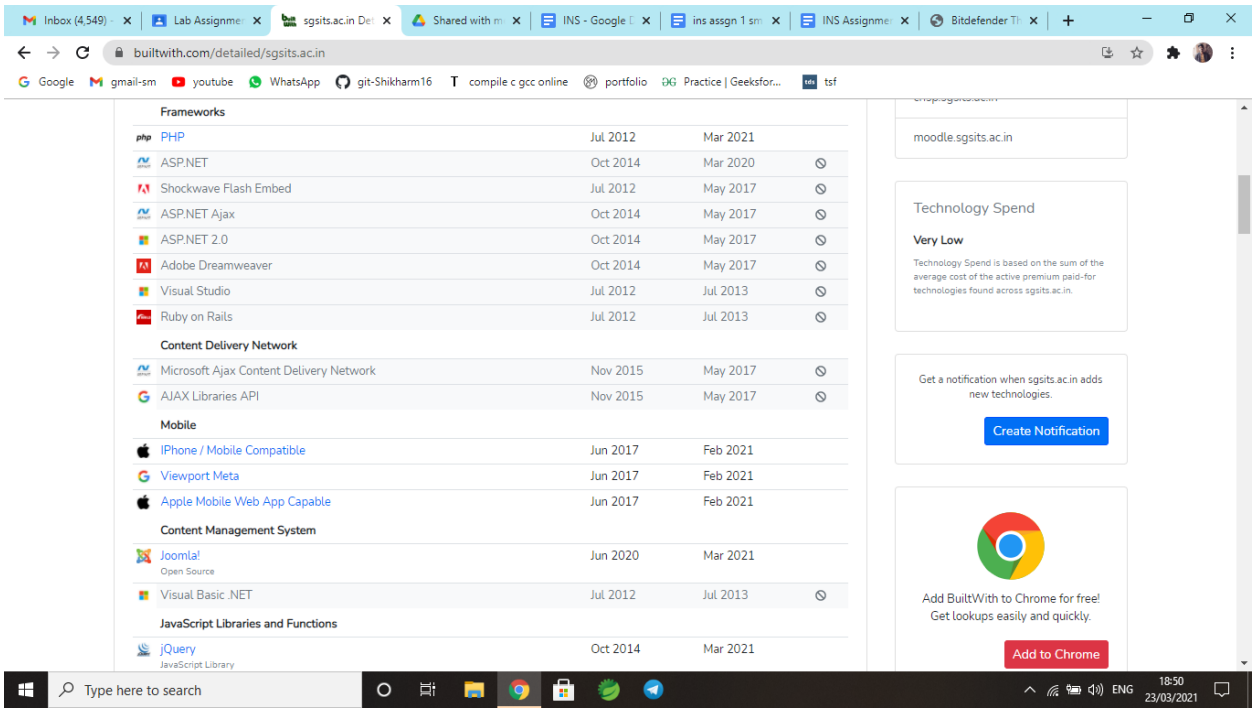
IV. Can you detect the OS name? if yes then also write the name of the OS.

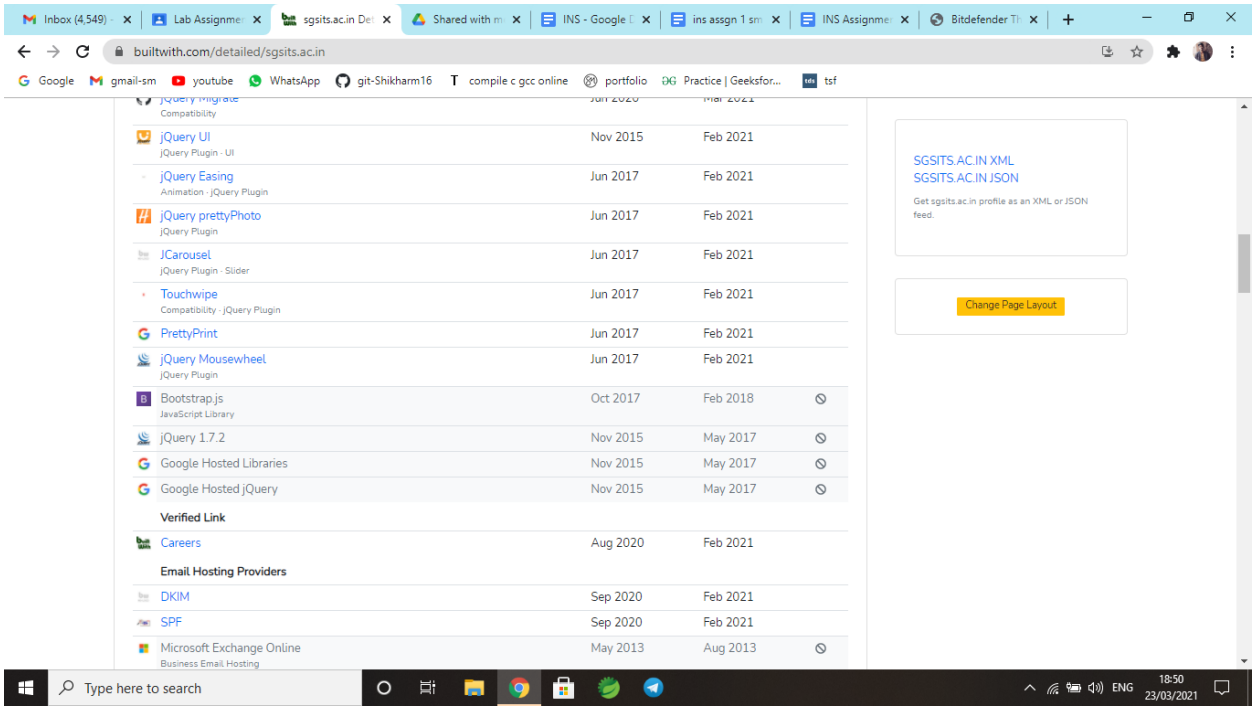


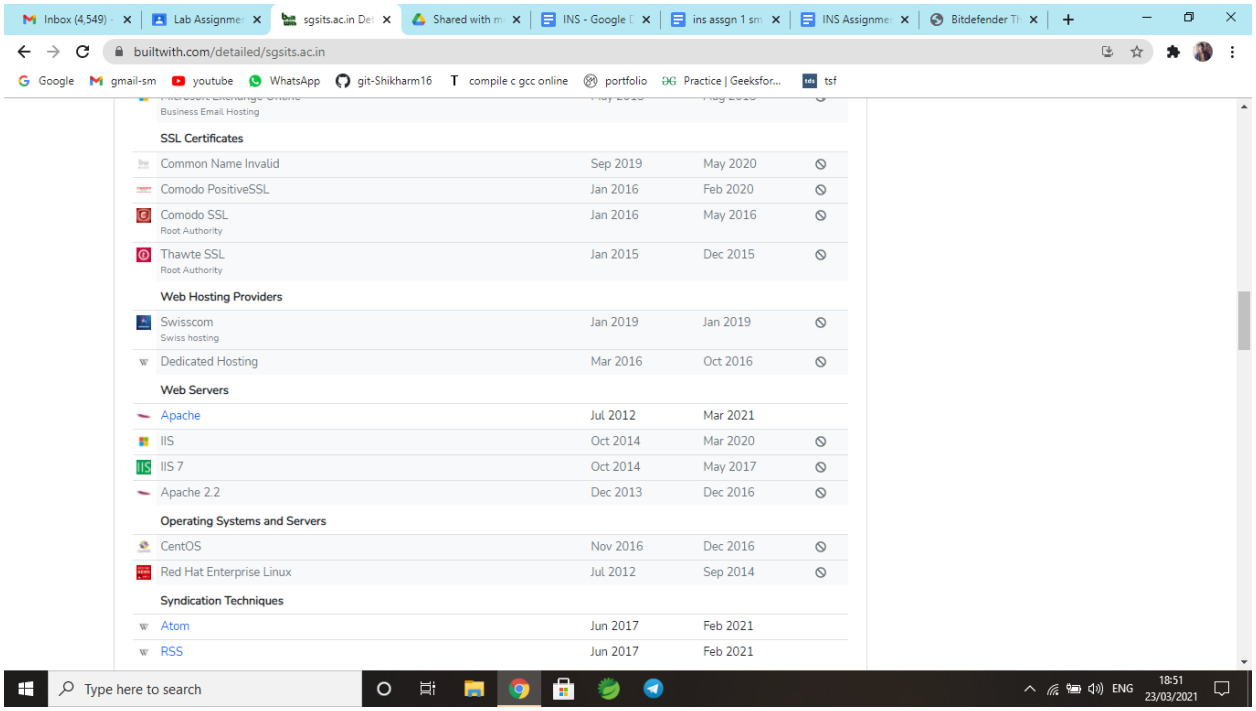
Q4. Visit to the website https://builtwith.com and perform the following operation on the target website: www.sgsits.ac.in –

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



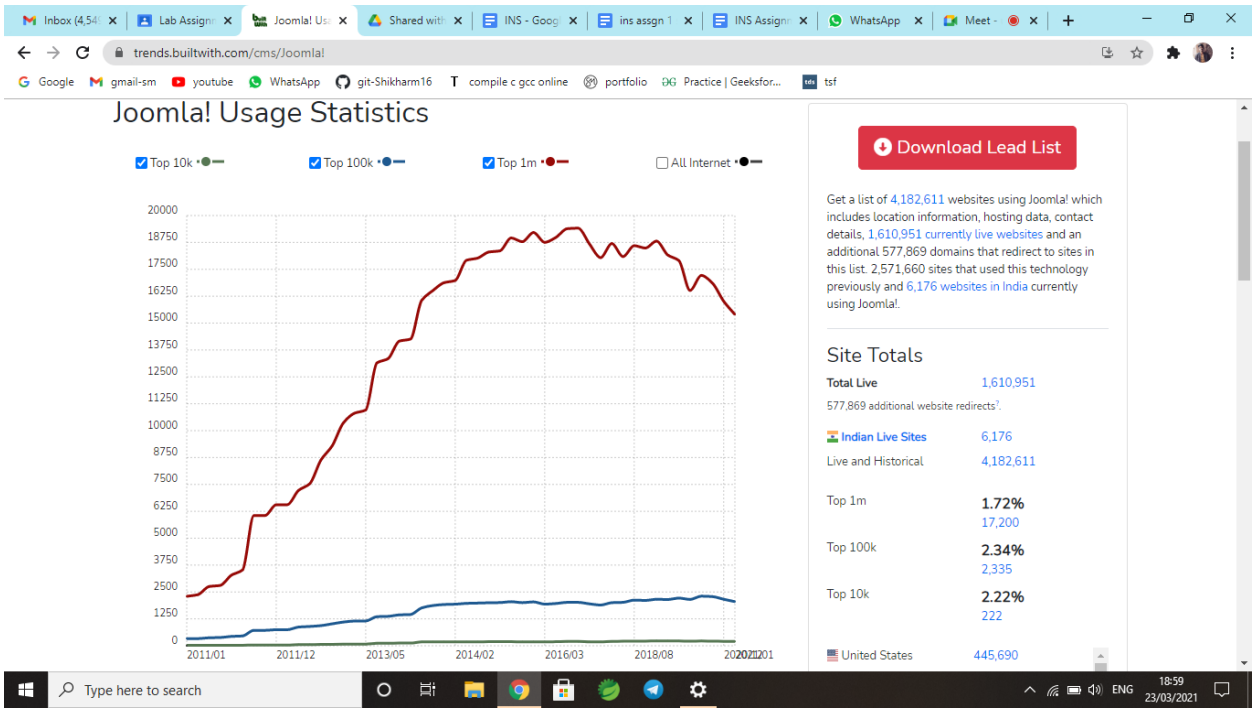



builtwith.com/detailed/sgsits.ac.in
jQuery UI Nov 2015 Feb 2021
jQuery Easing Jun 2017 Feb 2021
jQuery prettyPhoto Jun 2017 Feb 2021
JCarousel Jun 2017 Feb 2021
Touchwipe Jun 2017 Feb 2021
PrettyPrint Jun 2017 Feb 2021
jQuery Mousewheel Jun 2017 Feb 2021
Bootstrap.js Oct 2017 Feb 2018
jQuery 1.7.2 Nov 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
SGSITS.AC.IN XML
SGSITS.AC.IN JSON
Change Page Layout
Type here to search
ENG 18:50 23/03/2021


builtwith.com/detailed/sgsits.ac.in
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
ENG 18:51 23/03/2021

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

Joomla!



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.

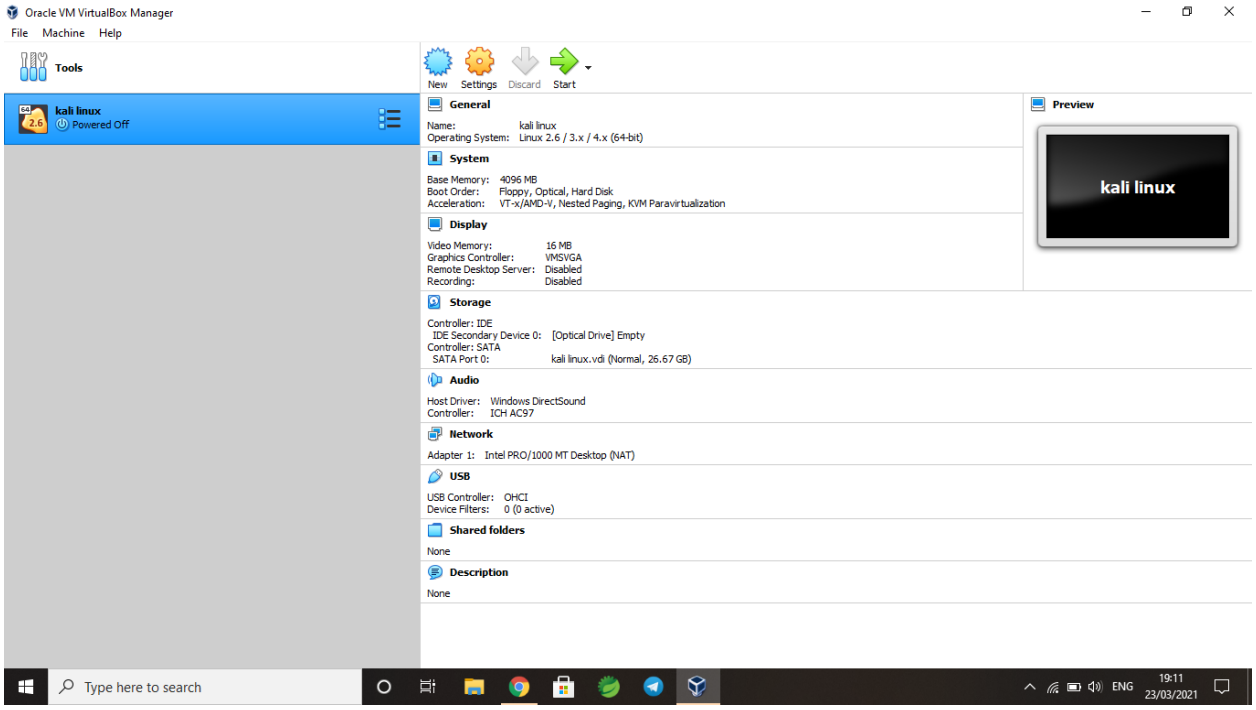
Top Alternatives to BuiltWith

- 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



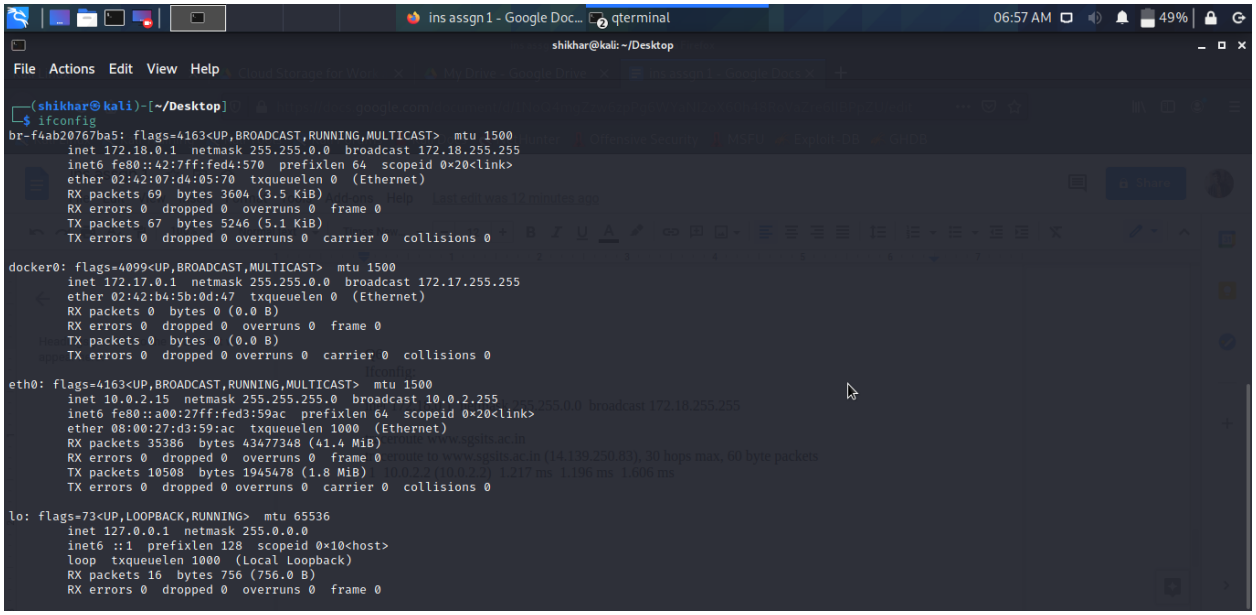
2) Metasploitable 2

```
 * Starting deferred execution scheduler atd                                [ OK ]
 * Starting periodic command scheduler crond                                [ OK ]
 * Starting Tomcat servlet engine tomcat5.5                                 [ OK ]
 * Starting web server apache2                                              [ OK ]
 * Running local boot scripts (/etc/rc.local)
nohup: appending output to `nohup.out'
nohup: appending output to `nohup.out'
                                                                           [ OK ]


Warning: Never expose this VM to an untrusted network!

Contact: msfdev[at]metasploit.com

Login with msfadmin/msfadmin to get started


metasploitable login:
```

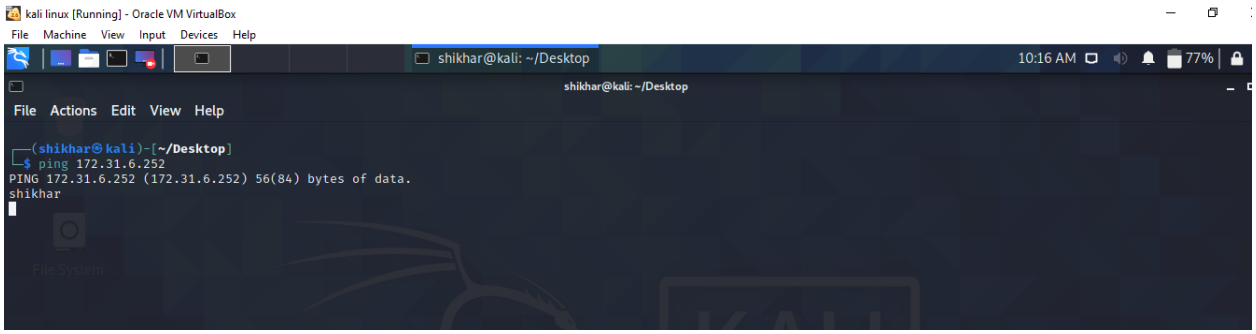
3) Windows 7

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

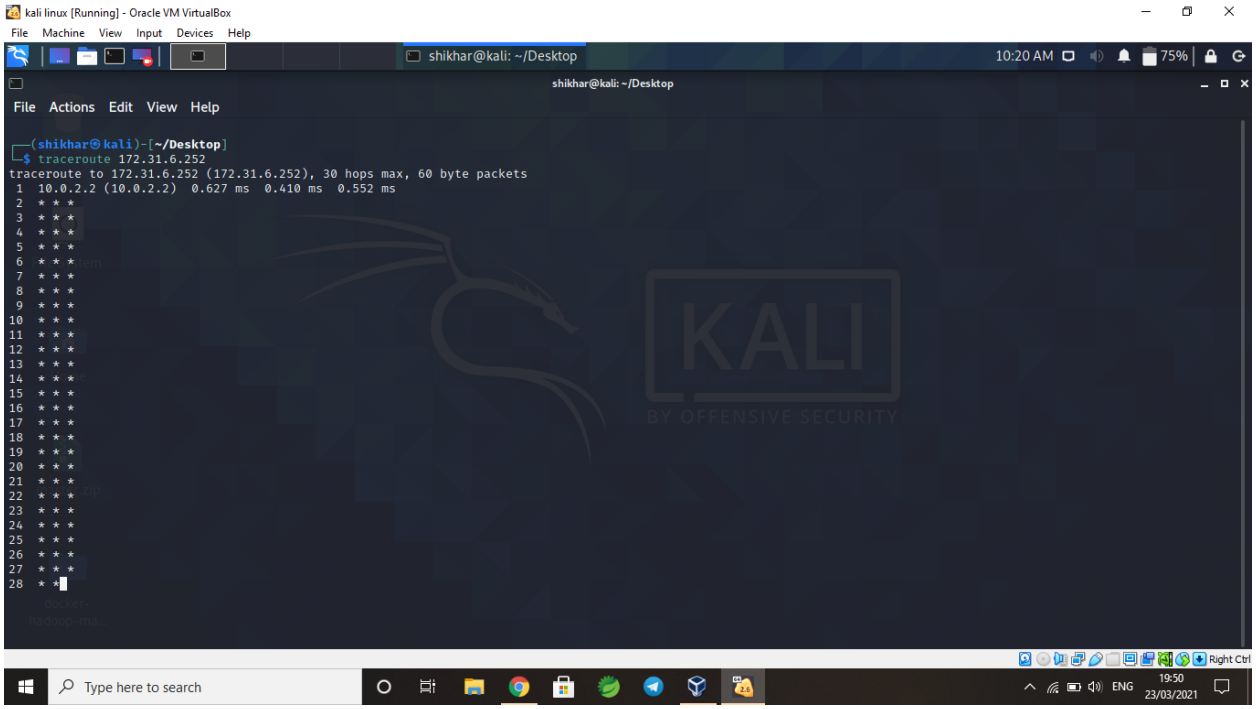
I. Run the ifconfig in each of the virtual machine and write the IP, MAC and subnet mask details.



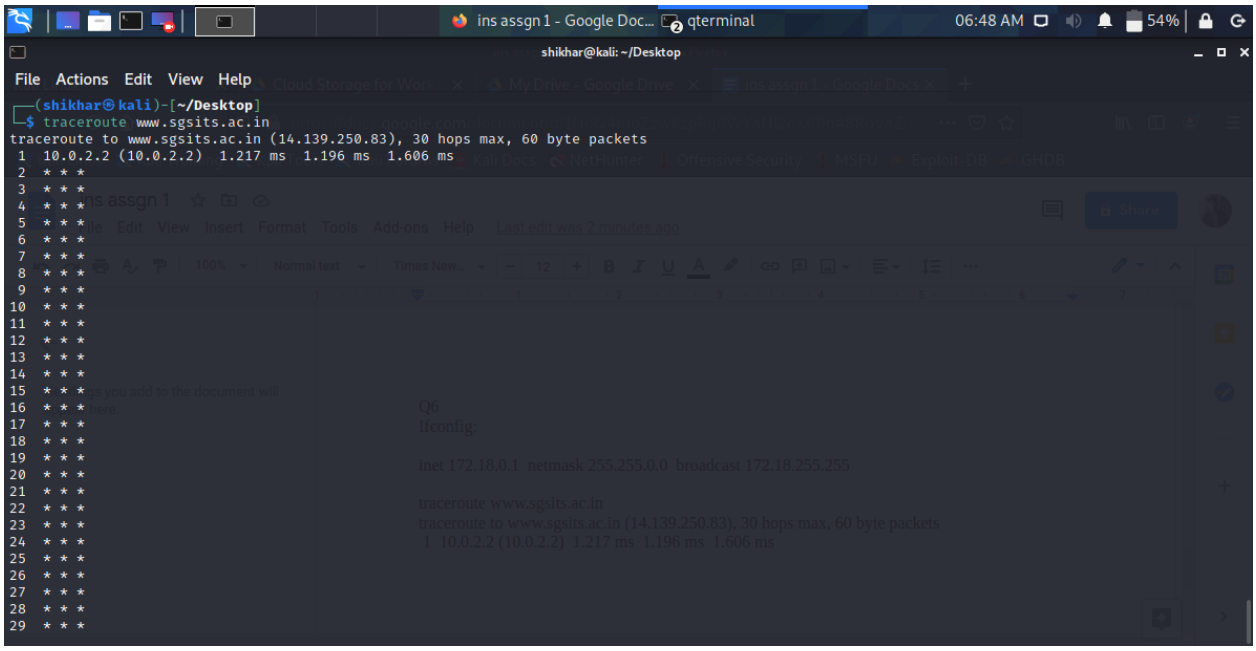
II. Run the ping command in each of the virtual machines and ping to each other.



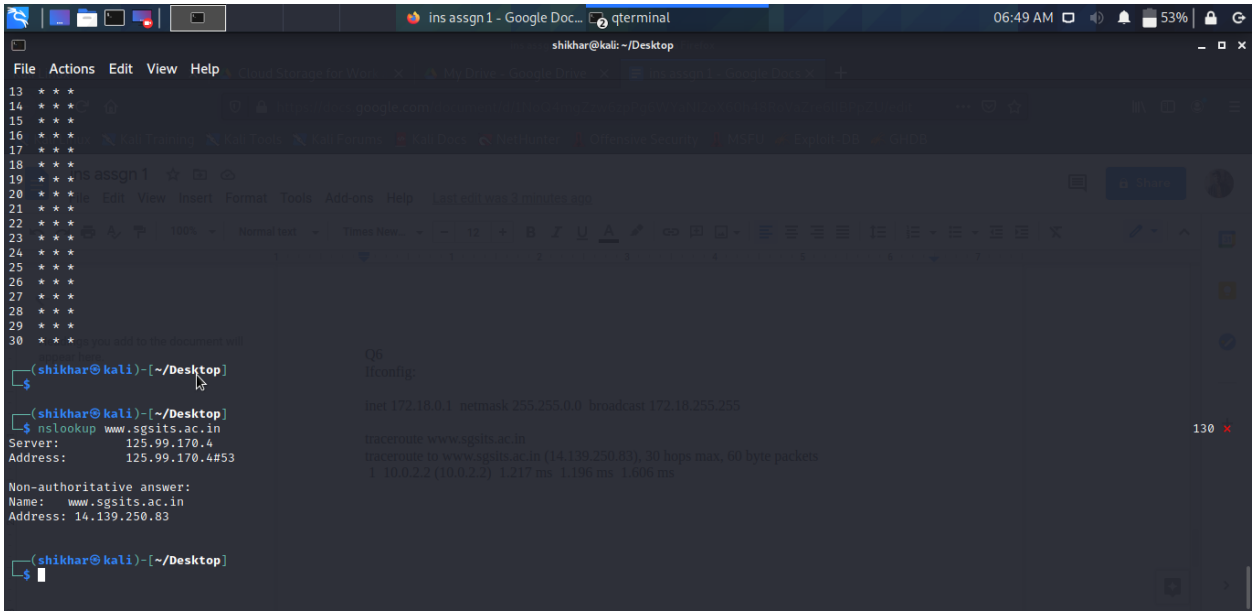
III. Run the traceroute command from one virtual machine to another virtual machine's IP and give the explanation of the output.



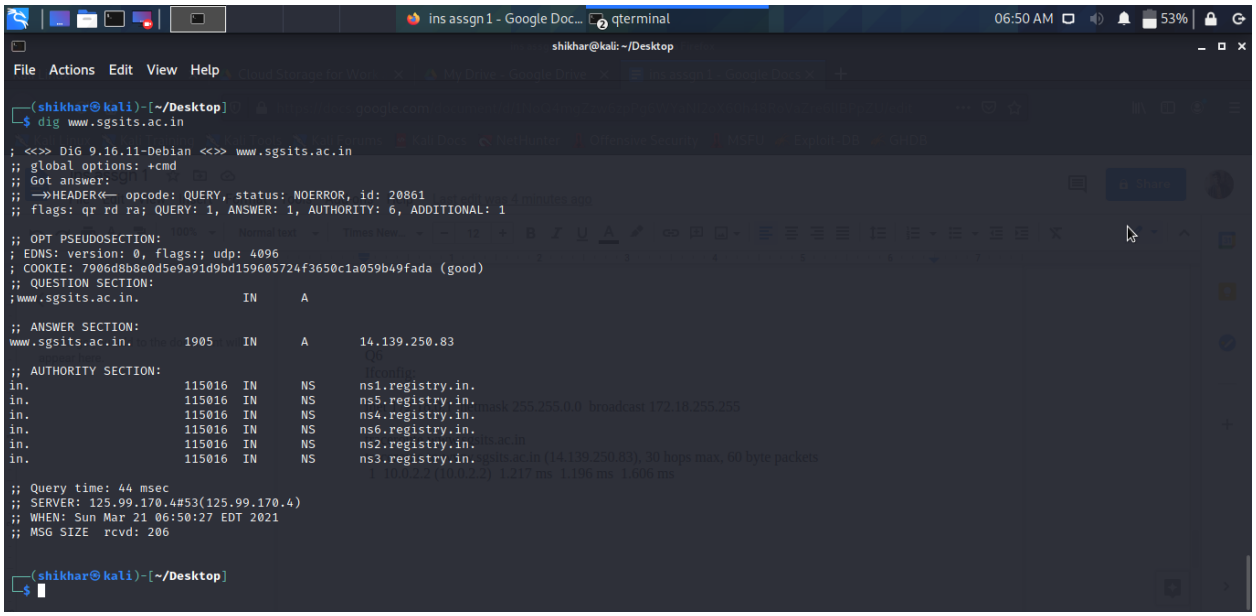
IV. Run the traceroute command for the target website i.e. www.sgsits.ac.in and give the explanation of the output.



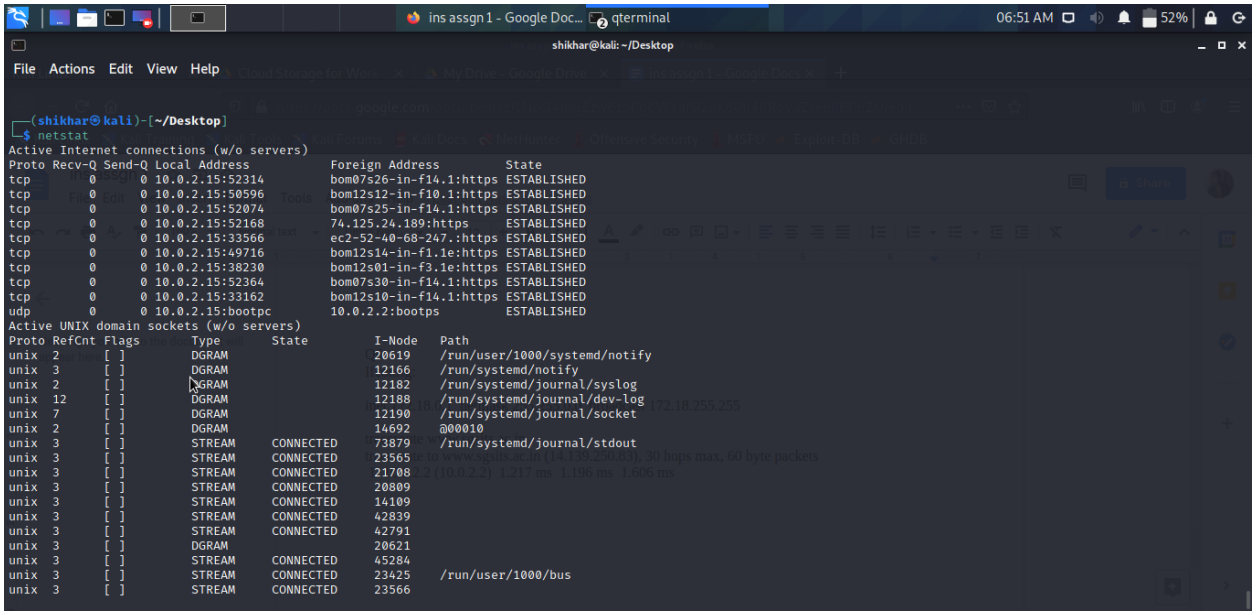
V. Run the nslookup on the target website i.e. www.sgsits.ac.in and write the name/IP of the server, mail server, IP address of the target website etc.



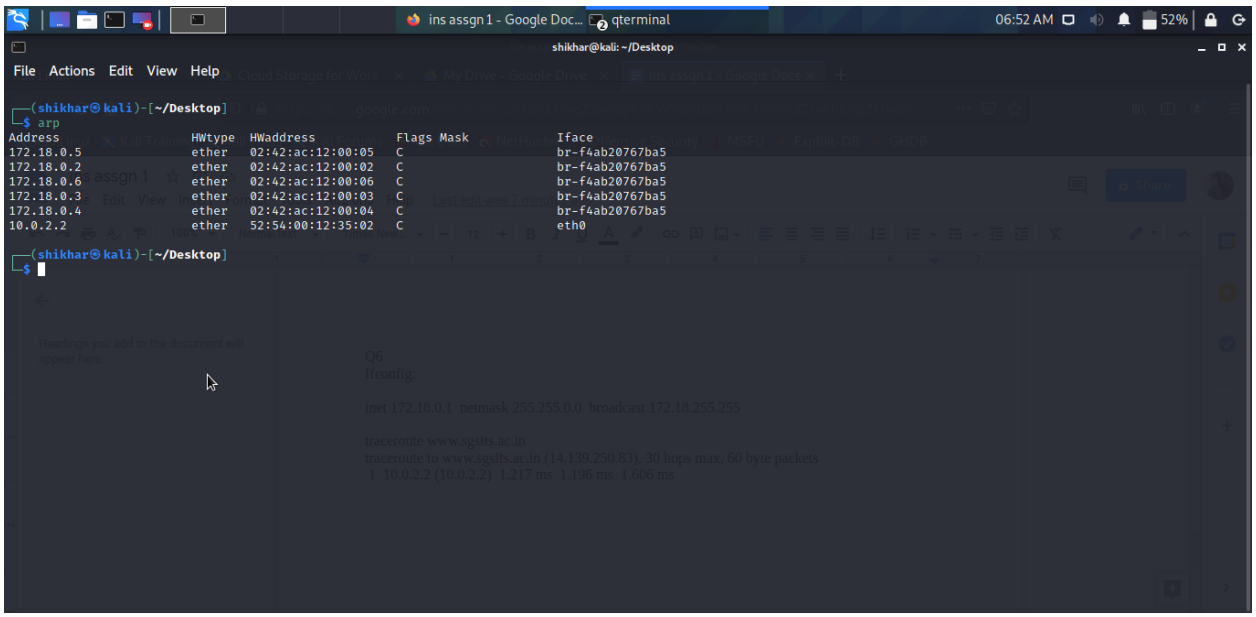
VI. Run the dig on the target website i.e. www.sgsits.ac.in and give the explanation of the output. Execute the dig command to get the name of the name servers and mail servers etc.



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

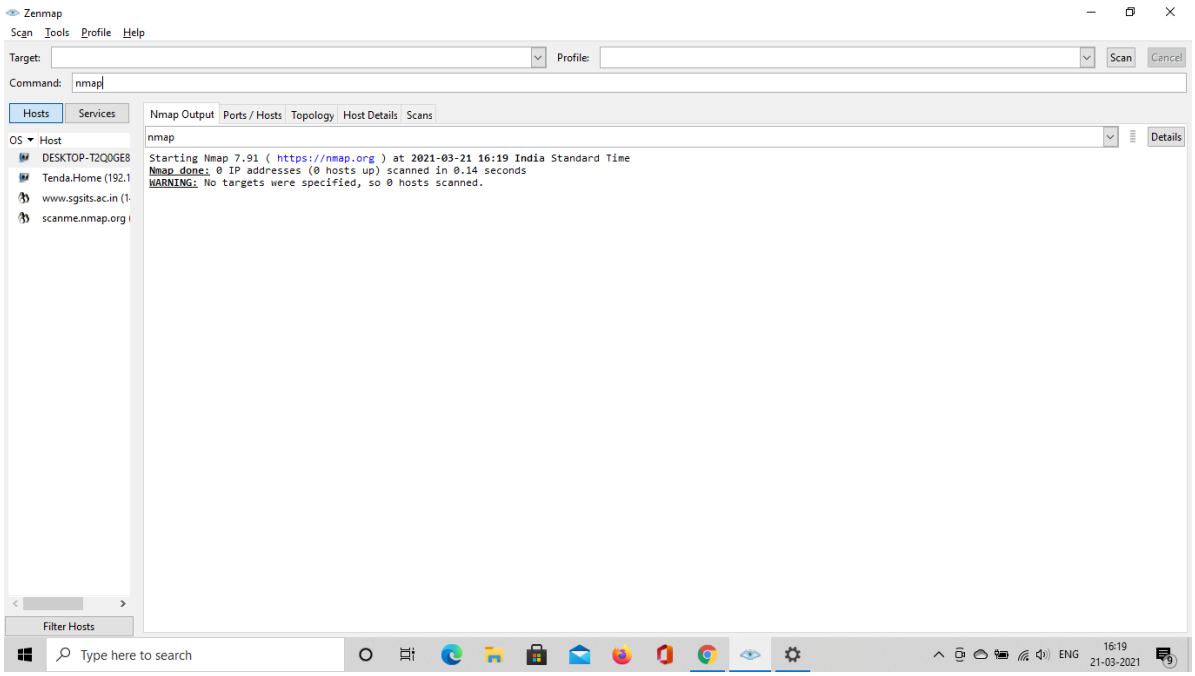


VIII. Run the arp command and give the explanation of the output.

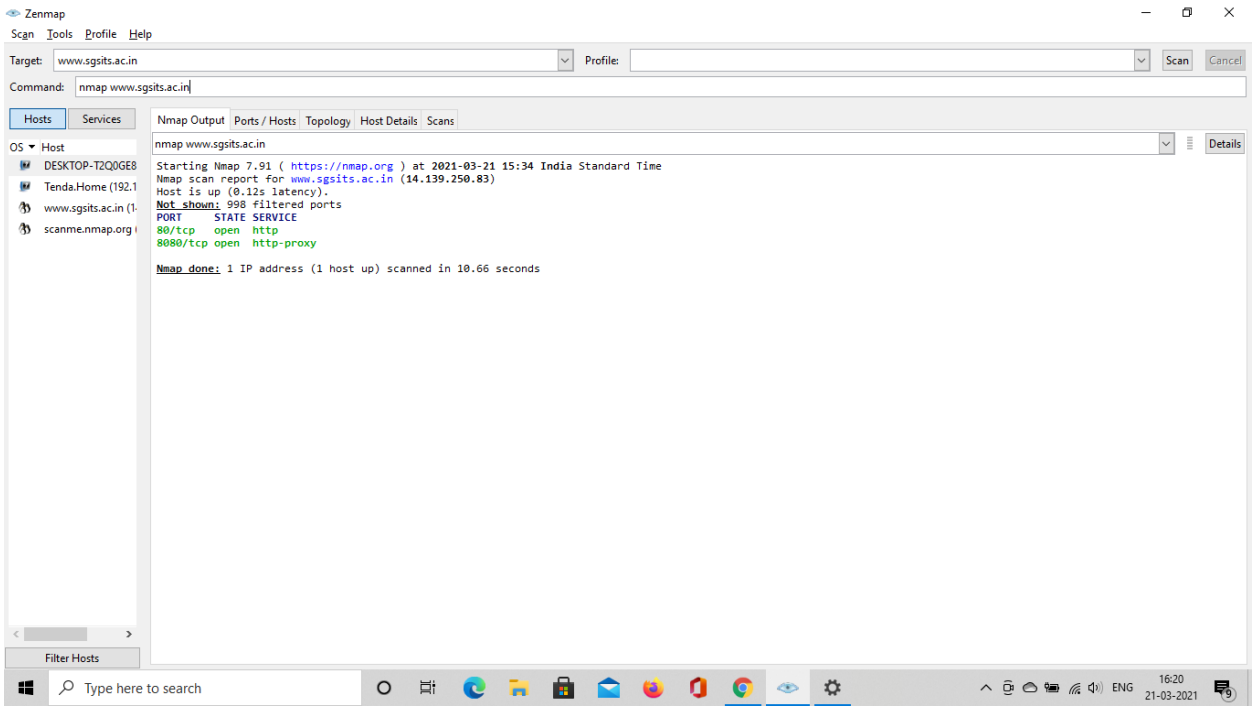


Q7. Execute the nmap command and answer the following questions:

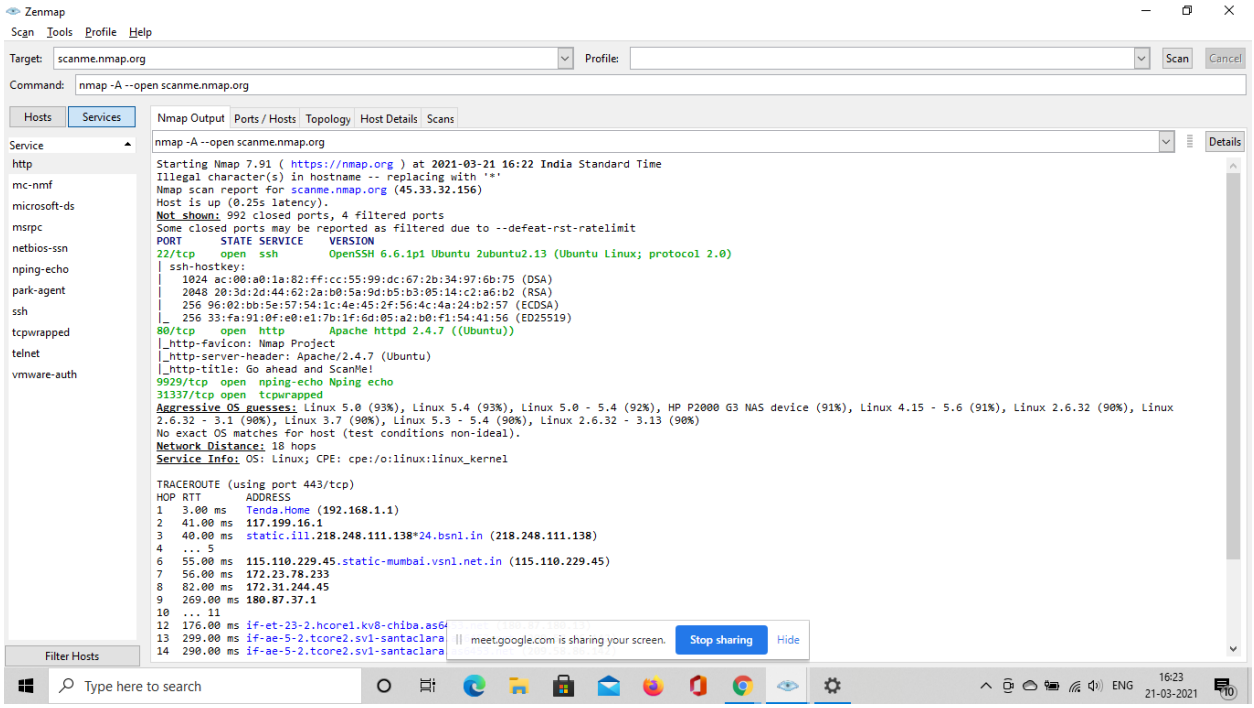
I. Execute the nmap on both the target machine i.e. windows & metasploitable 2 and give the explanation of the output.



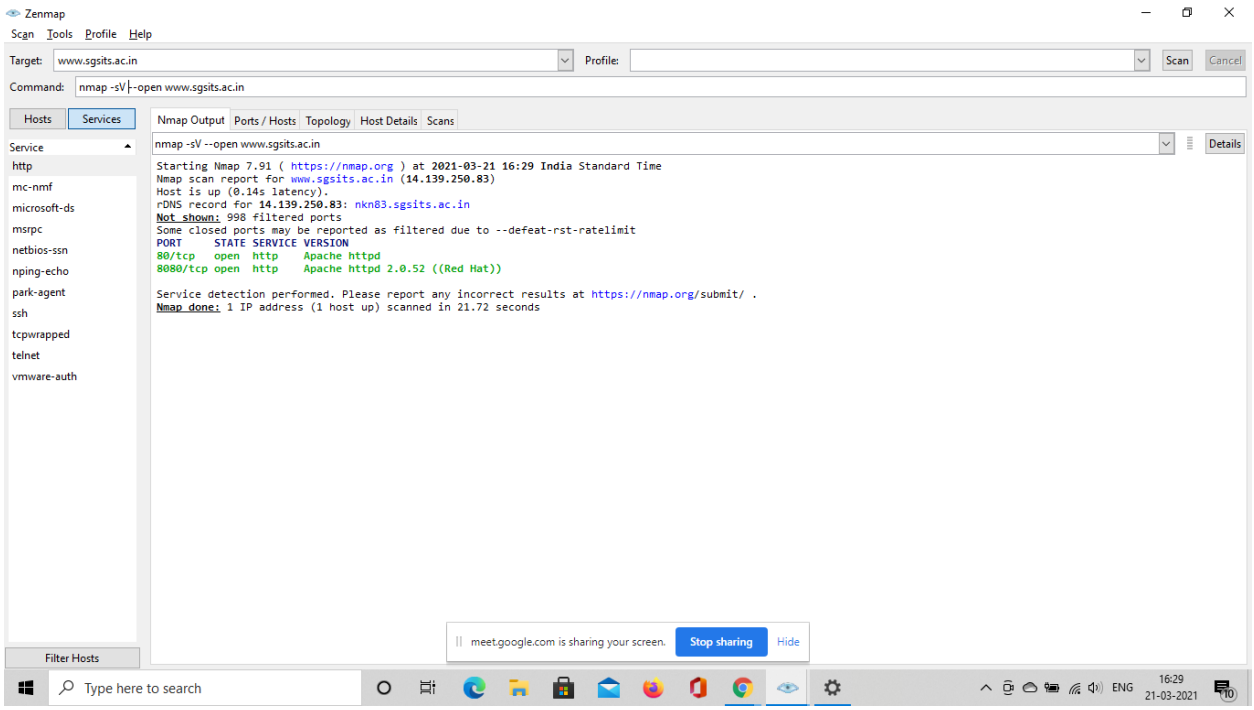
II. Execute the nmap on target website i.e. www.sgsits.ac.in and give the explanation of the Output.



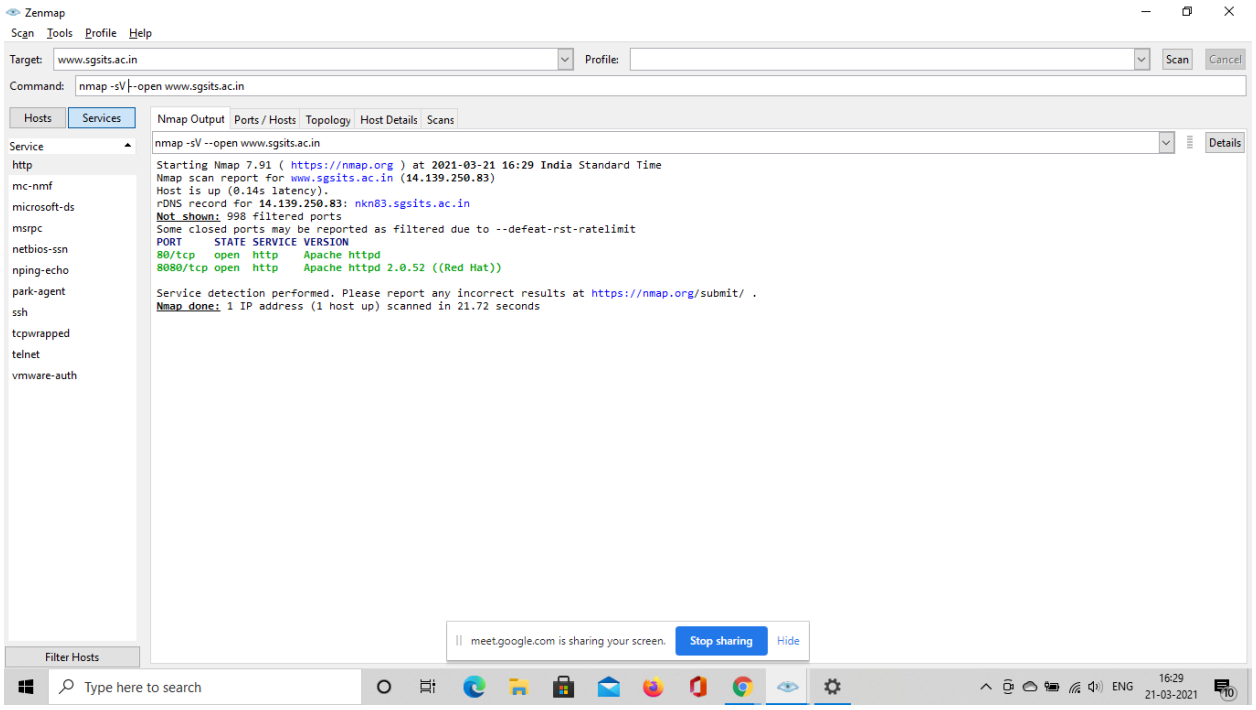
III. Execute the nmap on both the target machine i.e. windows & metasploitable 2 and display the open port in detail.

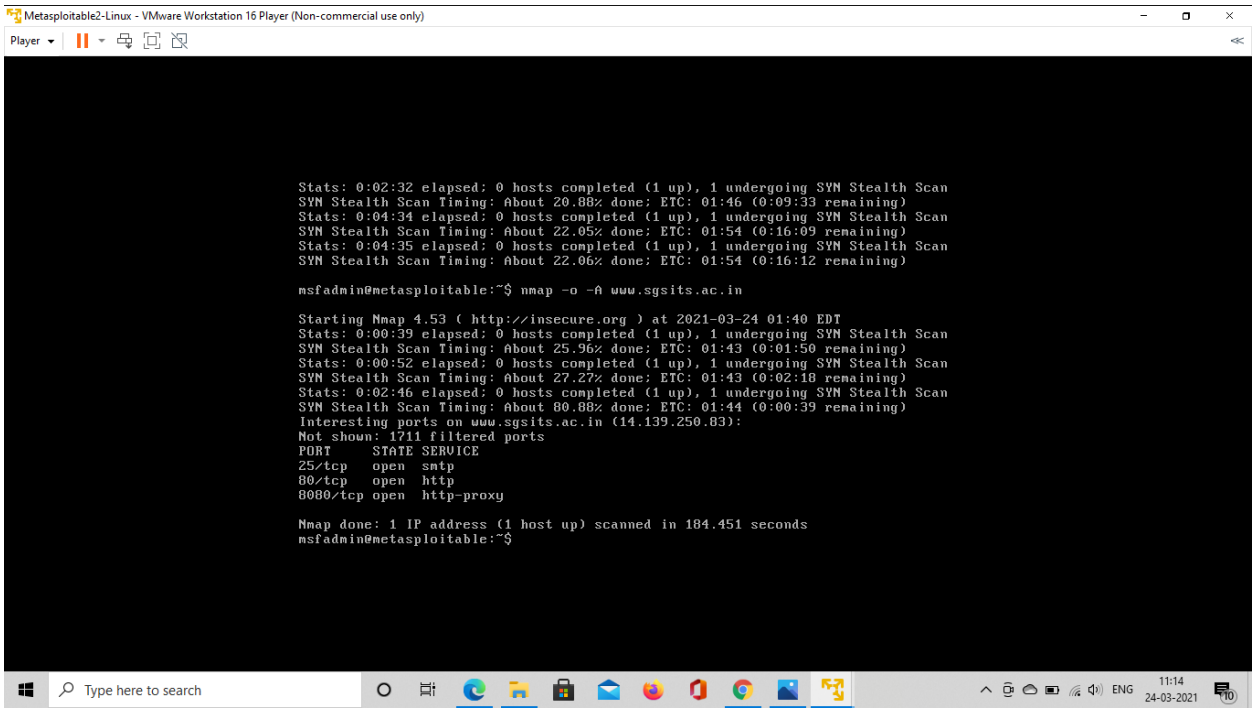


IV. Execute the nmap on both the target machine i.e. windows & metasploitable 2 and display the OS.

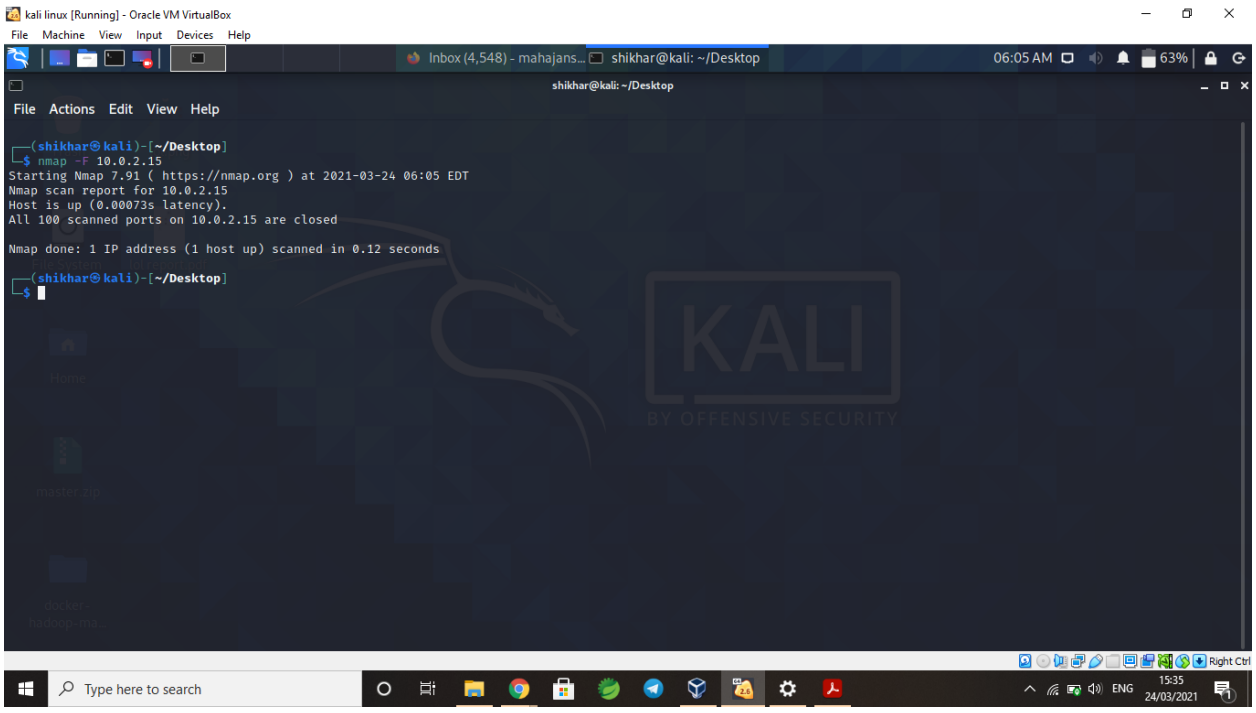


V. Execute the nmap on both the target machine i.e. windows & metasploitable 2 and display the services running on various open ports.



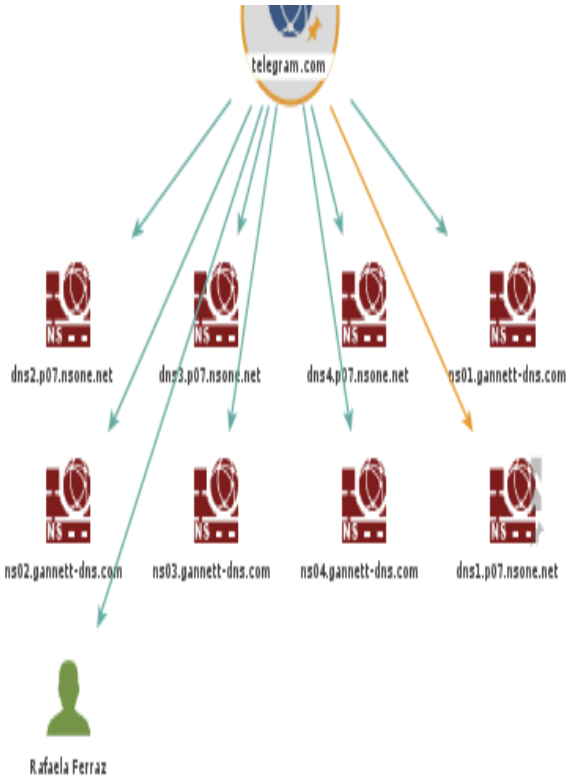


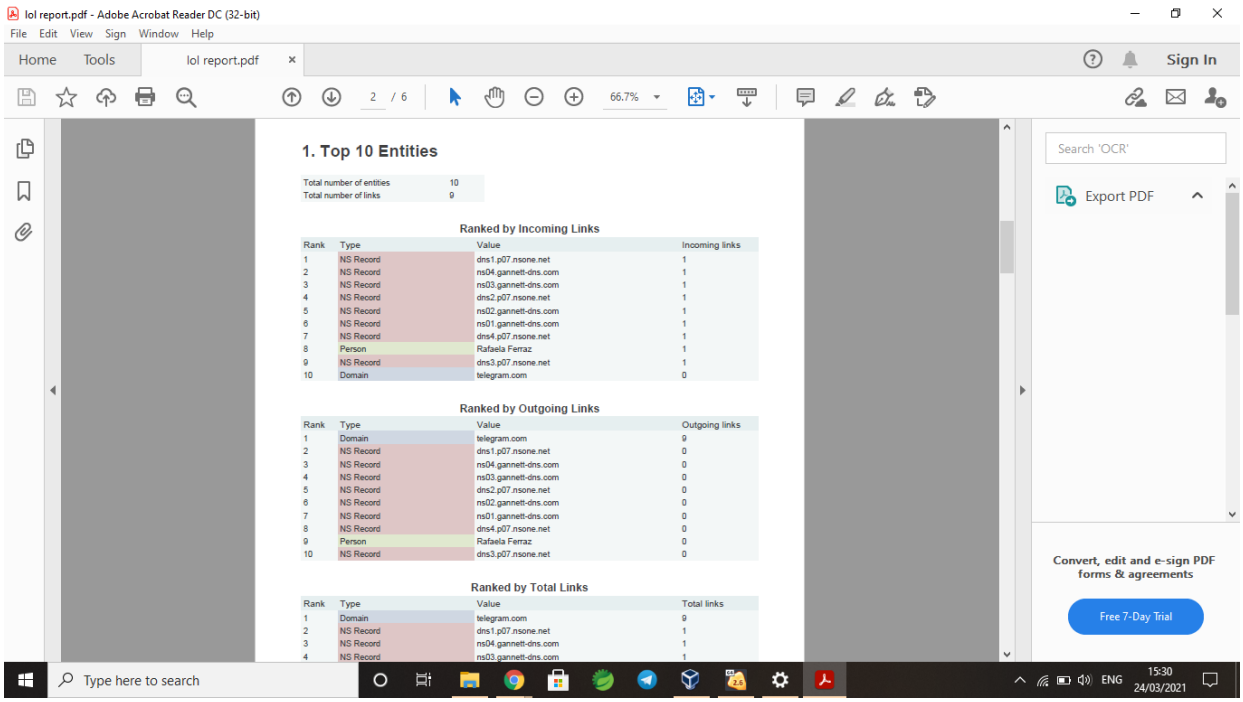
VI. Execute the nmap in the given IP range and display the services running at specified ports i.e. port 80, 20, 21 etc. in that IP range.

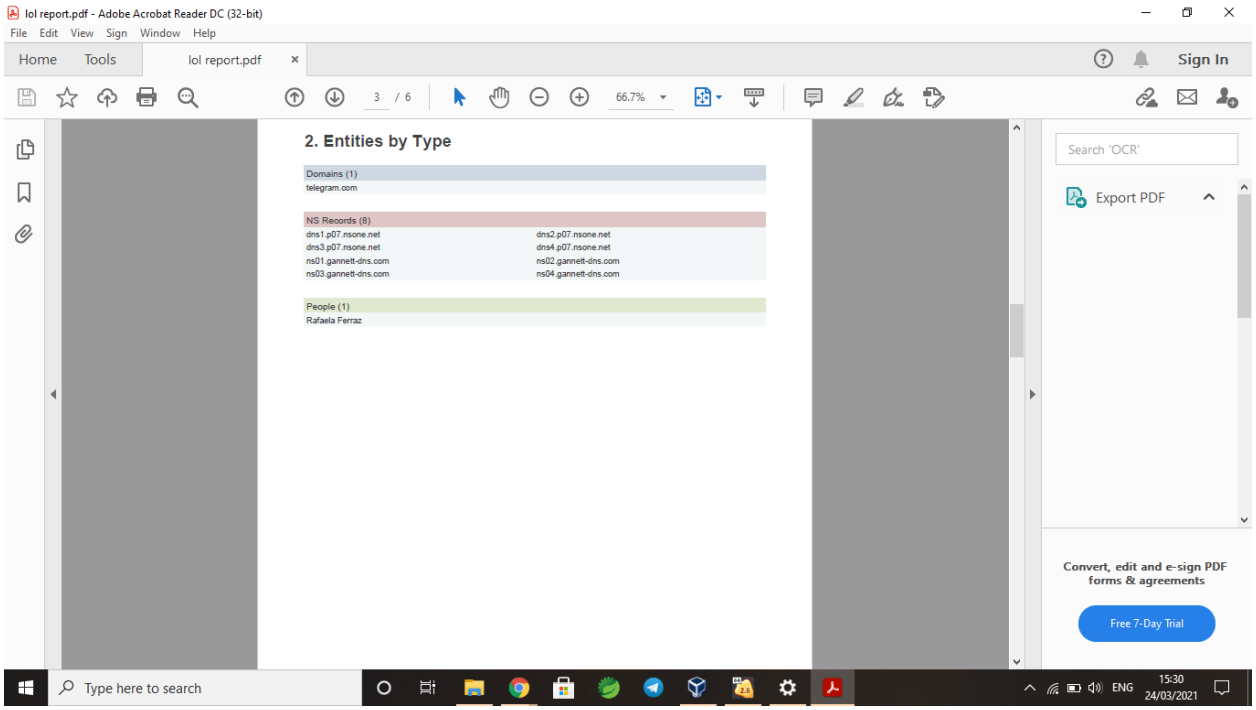


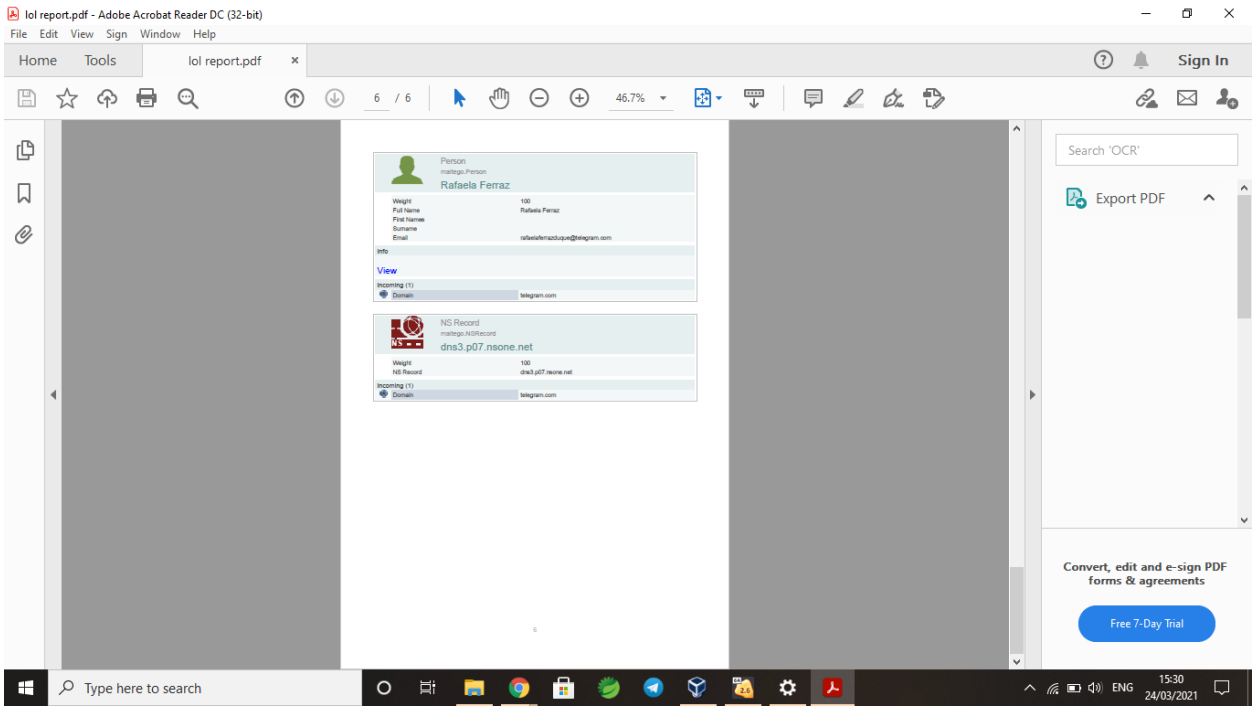
Q8. Setup the Maltego application in Kali Linux and perform the following operations:

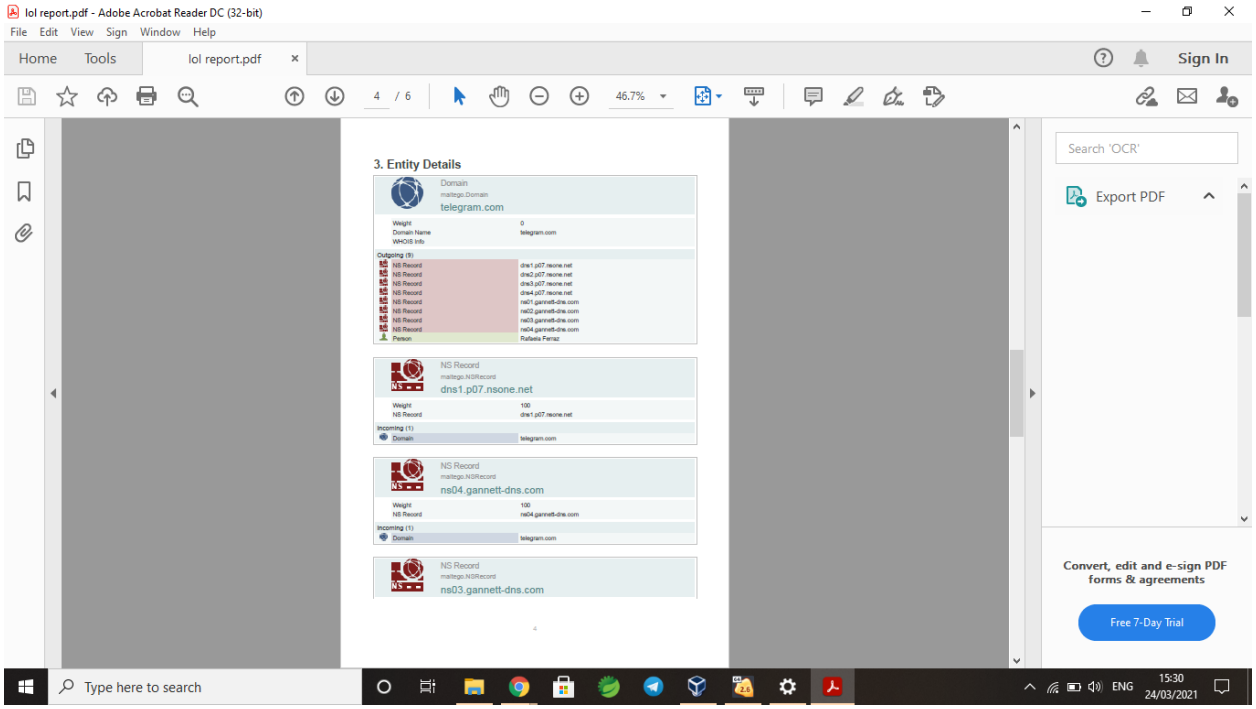
I. Select a target website/domain and perform the required transformation like email, phone no, name etc. transformations. Generate the report for all the transformation.




lol report.pdf - Adobe Acrobat Reader DC (32-bit)
File Edit View Sign Window Help
Home Tools lol report.pdf
Sign In
2 / 6
66.7%
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
Search 'OCR'
Export PDF
Convert, edit and e-sign PDF forms & agreements
Free 7-Day Trial
Type here to search
ENG 15:30 24/03/2021


lol report.pdf - Adobe Acrobat Reader DC (32-bit)
File Edit View Sign Window Help
Home Tools lol report.pdf
Sign In
3 / 6
66.7%
2. Entities by Type
Domains (1)
telegram.com
NS Records (8)
dns1.p07.nsone.net
dns2.p07.nsone.net
dns3.p07.nsone.net
dns4.p07.nsone.net
ns01.gannett-dns.com
ns02.gannett-dns.com
ns03.gannett-dns.com
ns04.gannett-dns.com
People (1)
Rafaela Ferraz
Search 'OCR'
Export PDF
Convert, edit and e-sign PDF forms & agreements
Free 7-Day Trial
Type here to search
ENG 15:30 24/03/2021


lol report.pdf - Adobe Acrobat Reader DC (32-bit)
File Edit View Sign Window Help
Home Tools lol report.pdf
Sign In
6 / 6
46.7%
Person
Rafaela Ferraz
View
NS Record
dns3.p07.nsone.net
Search 'OCR'
Export PDF
Convert, edit and e-sign PDF forms & agreements
Free 7-Day Trial
Type here to search
ENG
15:30
24/03/2021


lol report.pdf - Adobe Acrobat Reader DC (32-bit)
File Edit View Sign Window Help
Home Tools lol report.pdf
Sign In
4 / 6
46.7%
3. Entity Details
Domain
telegram.com
NS Record
dns1.p07.nsone.net
NS Record
ns04.gannett-dns.com
NS Record
ns03.gannett-dns.com
Search 'OCR'
Export PDF
Convert, edit and e-sign PDF forms & agreements
Free 7-Day Trial
Type here to search
ENG
15:30
24/03/2021

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]