



Dr. Vishwanath Karad

**MIT WORLD PEACE  
UNIVERSITY** | PUNE

TECHNOLOGY, RESEARCH, SOCIAL INNOVATION & PARTNERSHIPS

## **School of Computer Science and Engineering**

**Department of Computer Engineering and Technology**

**Third Year B. Tech. CSE (Cybersecurity and Forensics)**

### **Introductory Session**

### **(Basic Trends and Awareness in CyberSecurity)**

Organised By SoCSE (Dr. Vinayak Musale and Dr. Dhanashri Wategaokar)

<b>Name of Student</b>	<b>PRN</b>	<b>Official Email</b>
Dhiraj Rajput	1032230441	dhiraj.rajput@mitwpu.edu.in
Sushant Kumar	1032231329	sushant.kumar@mitwpu.edu.in
Ashish Sharma	1032231907	ashish.sharma@mitwpu.edu.in
Yashraj Narke	1032232513	yashraj.narke@mitwpu.edu.in
Nikhil Patil	1032232897	nikhil.patil1@mitwpu.edu.in
Prasanna Dhamal	1032230610	prasanna.dhamal@mitwpu.edu.in
Vishwesh Bhat	1032232281	vishwesh.bhat@mitwpu.edu.in
Yug Hiranandani	1032230871	hiranandani.vinodbhai@mitwpu.edu.in

# Introduction

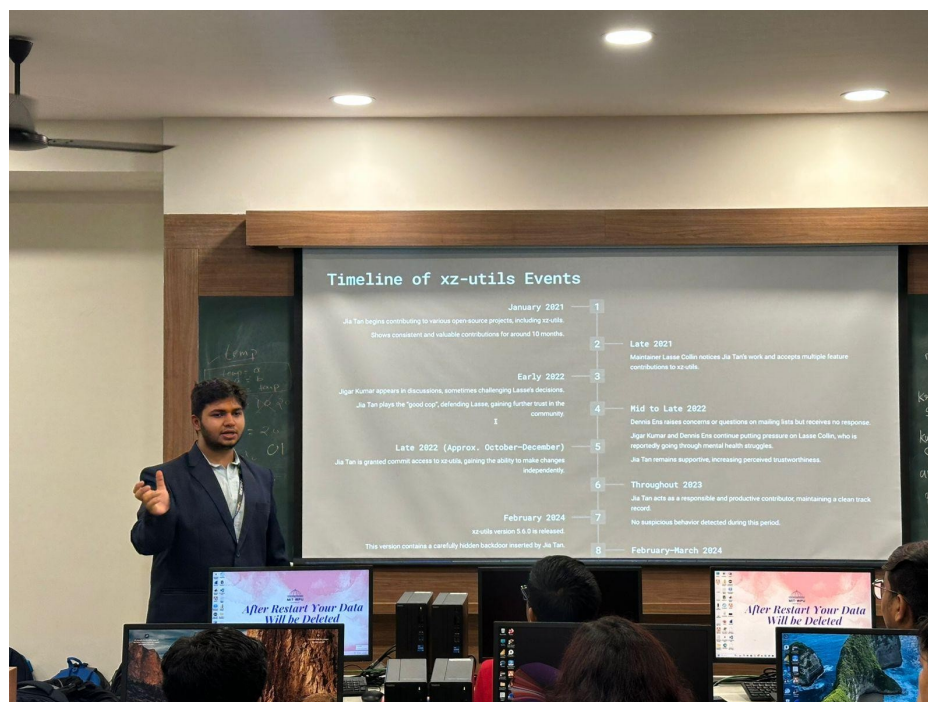
The cybersecurity awareness session aimed to educate attendees on the evolving threat landscape, common attack vectors, and the tools and platforms available for both protection and professional growth in the field. The session focused on practical demonstrations, real-life examples, and actionable guidance.

## Session Flow & Highlights -

### **1) Ashish Sharma – Introduction to Social Engineering and Academic Threats**

Ashish opened the session by discussing the psychological side of cyberattacks, especially social engineering. He highlighted how attackers target students and academic environments by using fake internship offers, scholarship scams, and phishing emails disguised as university communications.

His segment emphasized the importance of awareness and skepticism in today's digital world, particularly in academic settings.



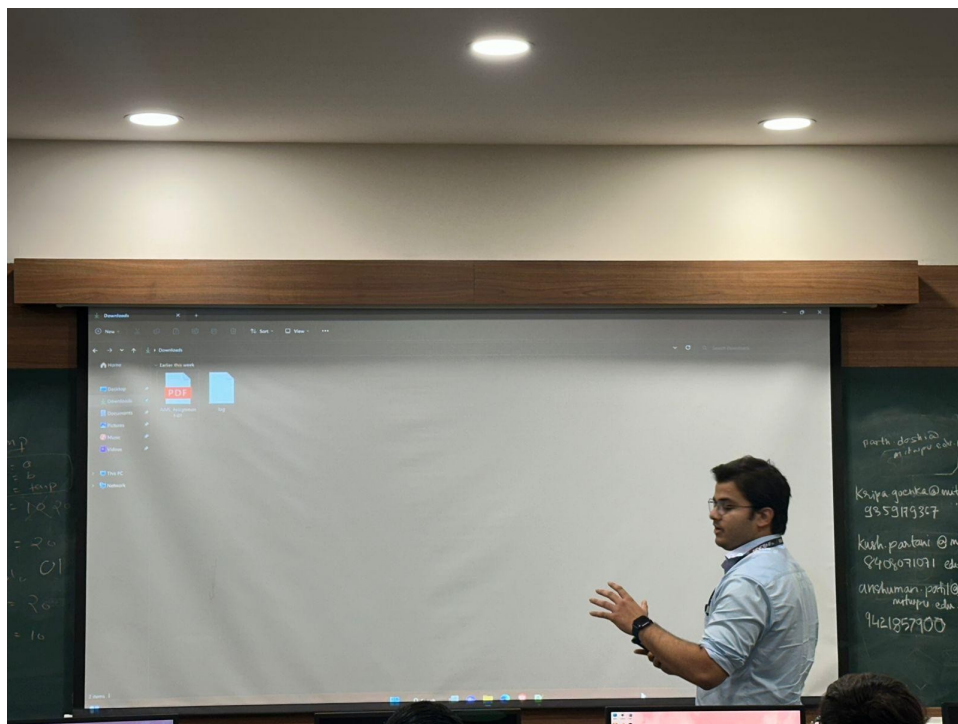
## 2) Sushant Kumar & Yashraj Narke – Remote Access Trojan (RAT) Demonstration

Together, Sushant and Yashraj gave an interactive demonstration of how Remote Access Trojans (RATs) are deployed and used by attackers to gain control of victim systems.

They simulated a common real-world attack scenario involving a disguised file and illustrated how quickly and silently a RAT can compromise a system.

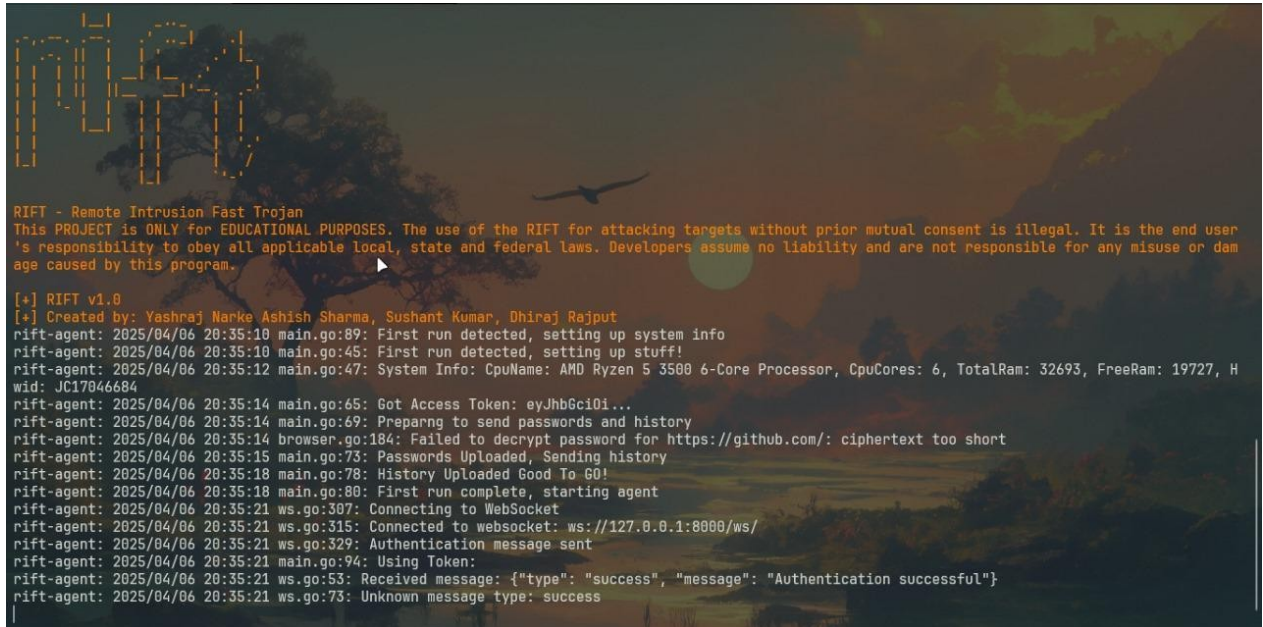
The key message: even a single cautious step—like avoiding unknown downloads—can prevent a major breach.

Their segment also tied the technical threat to broader human error, emphasizing a combination of technical knowledge and digital hygiene as the best defense.



## Frontend GUI Screenshots :

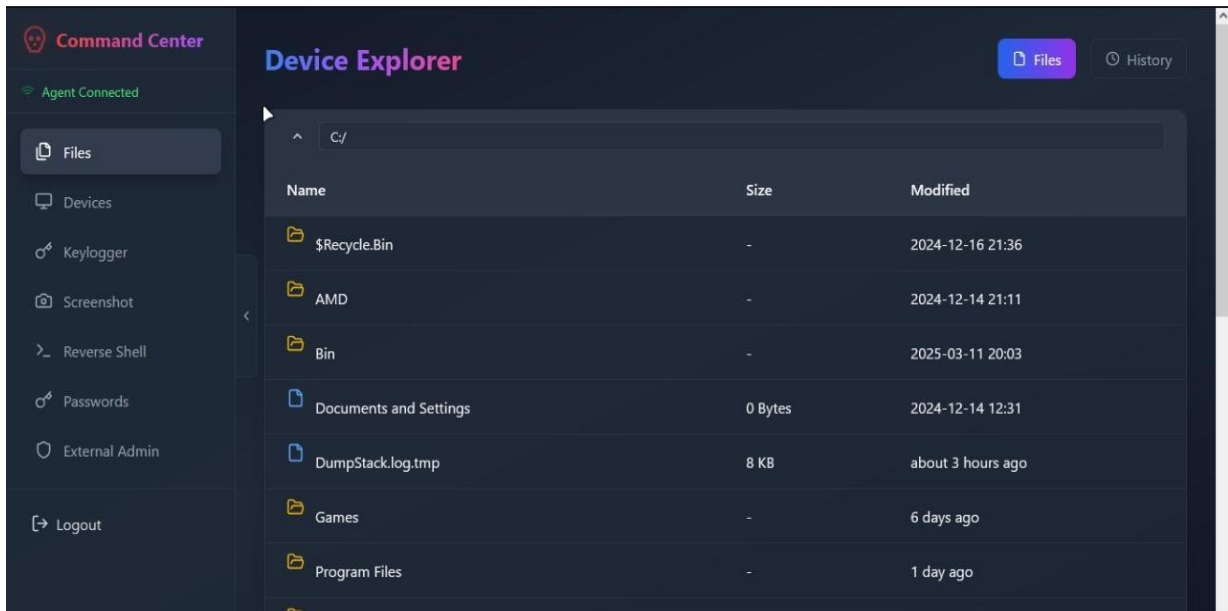
### Starting RIFT :



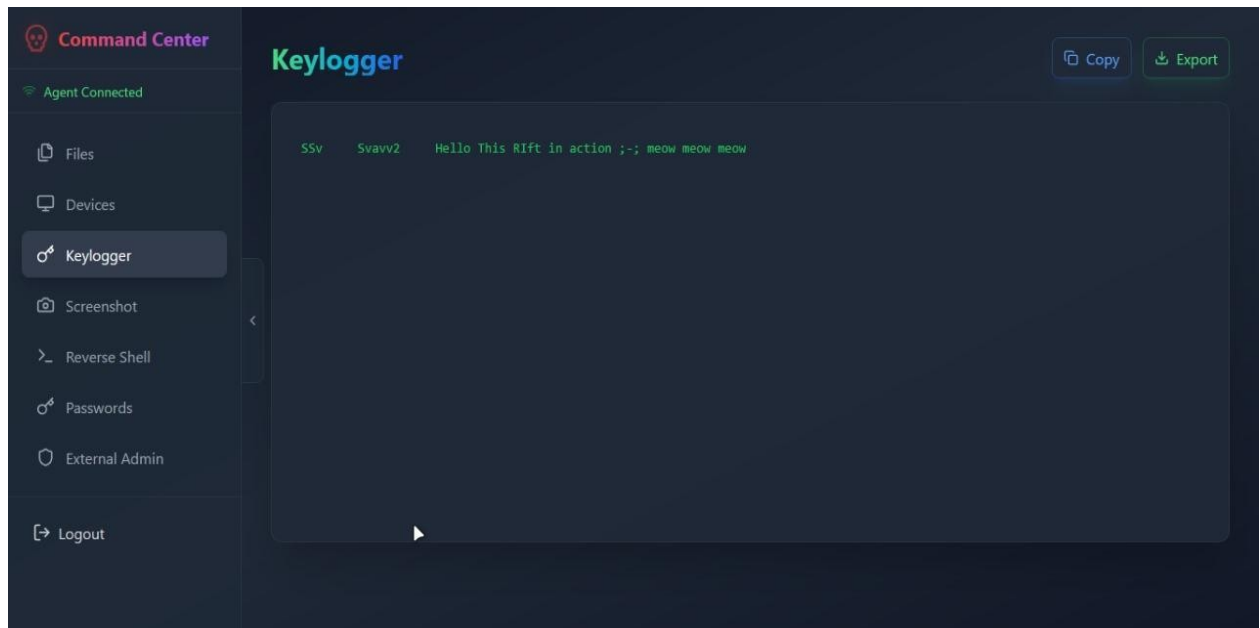
```
RIFT - Remote Intrusion Fast Trojan
This PROJECT is ONLY for EDUCATIONAL PURPOSES. The use of the RIFT for attacking targets without prior mutual consent is illegal. It is the end user
's responsibility to obey all applicable local, state and federal laws. Developers assume no liability and are not responsible for any misuse or dam
age caused by this program.

[+] RIFT v1.0
[+] Created by: Yashraj Narke Ashish Sharma, Sushant Kumar, Dhiraaj Rajput
rift-agent: 2025/04/06 20:35:10 main.go:89: First run detected, setting up system info
rift-agent: 2025/04/06 20:35:10 main.go:45: First run detected, setting up stuff!
rift-agent: 2025/04/06 20:35:12 main.go:47: System Info: CpuName: AMD Ryzen 5 3500 6-Core Processor, CpuCores: 6, TotalRam: 32693, FreeRam: 19727, H
wid: JC17046684
rift-agent: 2025/04/06 20:35:14 main.go:65: Got Access Token: eyJhbGciOiI...
rift-agent: 2025/04/06 20:35:14 main.go:69: Preparing to send passwords and history
rift-agent: 2025/04/06 20:35:14 browser.go:184: Failed to decrypt password for https://github.com/: ciphertext too short
rift-agent: 2025/04/06 20:35:15 main.go:73: Passwords Uploaded, Sending history
rift-agent: 2025/04/06 20:35:18 main.go:78: History Uploaded Good To GO!
rift-agent: 2025/04/06 20:35:18 main.go:80: First run complete, starting agent
rift-agent: 2025/04/06 20:35:21 ws.go:307: Connecting to WebSocket
rift-agent: 2025/04/06 20:35:21 ws.go:315: Connected to websocket: ws://127.0.0.1:8080/ws/
rift-agent: 2025/04/06 20:35:21 ws.go:329: Authentication message sent
rift-agent: 2025/04/06 20:35:21 main.go:94: Using Token:
rift-agent: 2025/04/06 20:35:21 ws.go:53: Received message: {"type": "success", "message": "Authentication successful"}
rift-agent: 2025/04/06 20:35:21 ws.go:73: Unknown message type: success
```

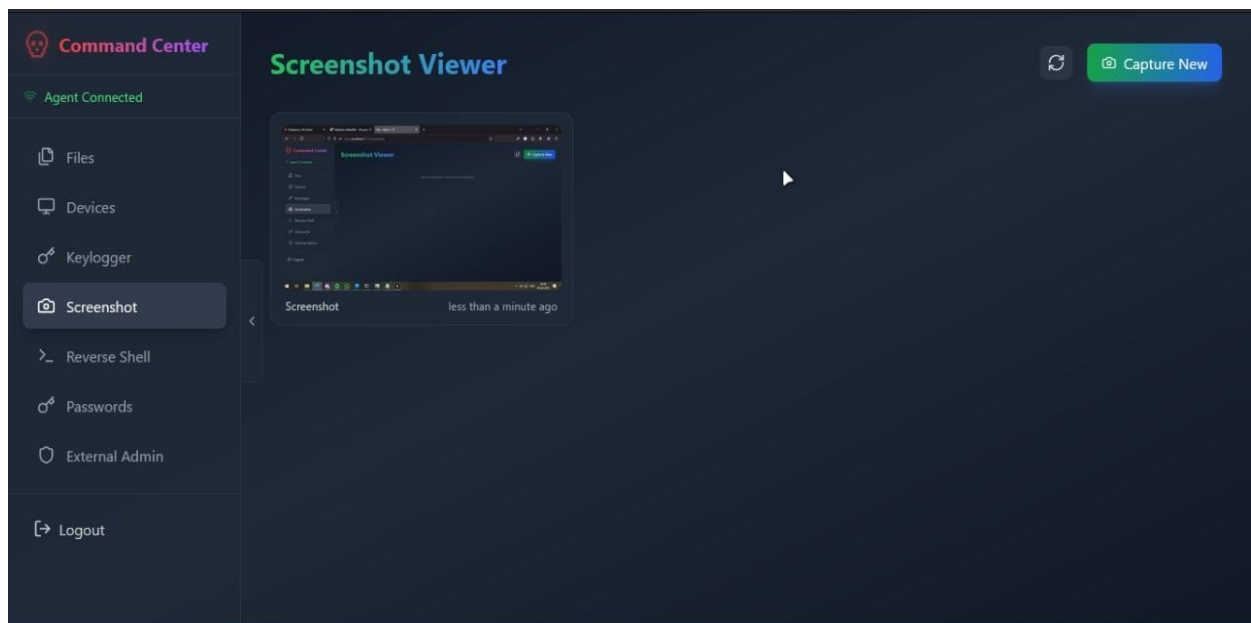
### Dashboard / Device Explorer :



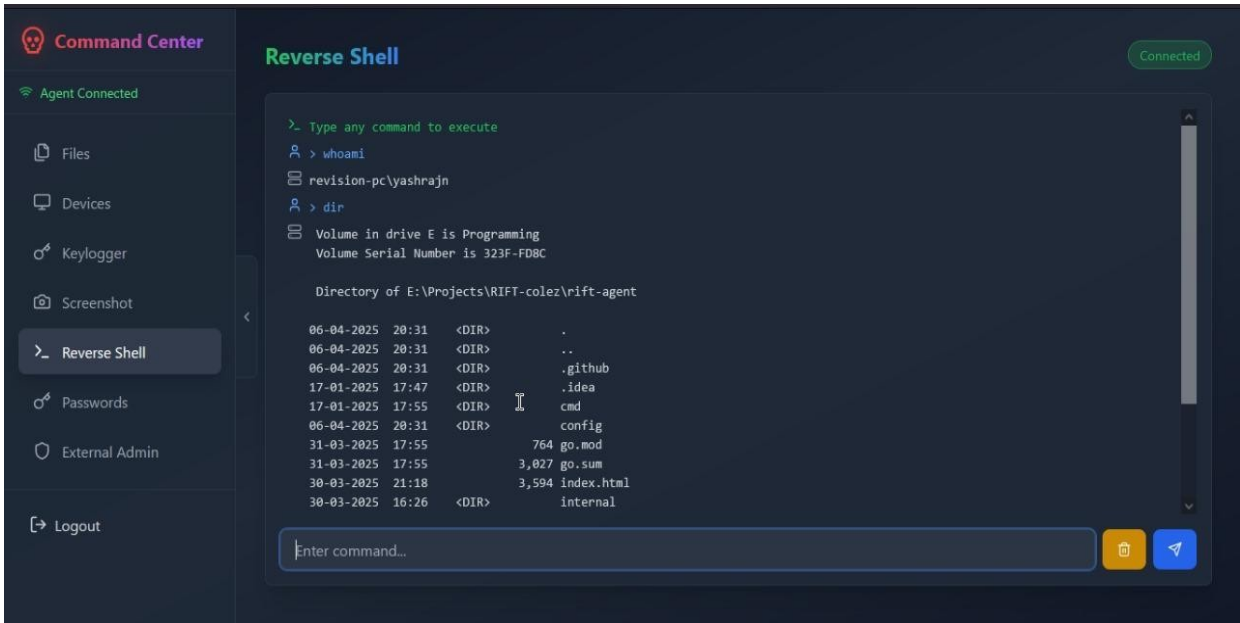
## Keylogger :



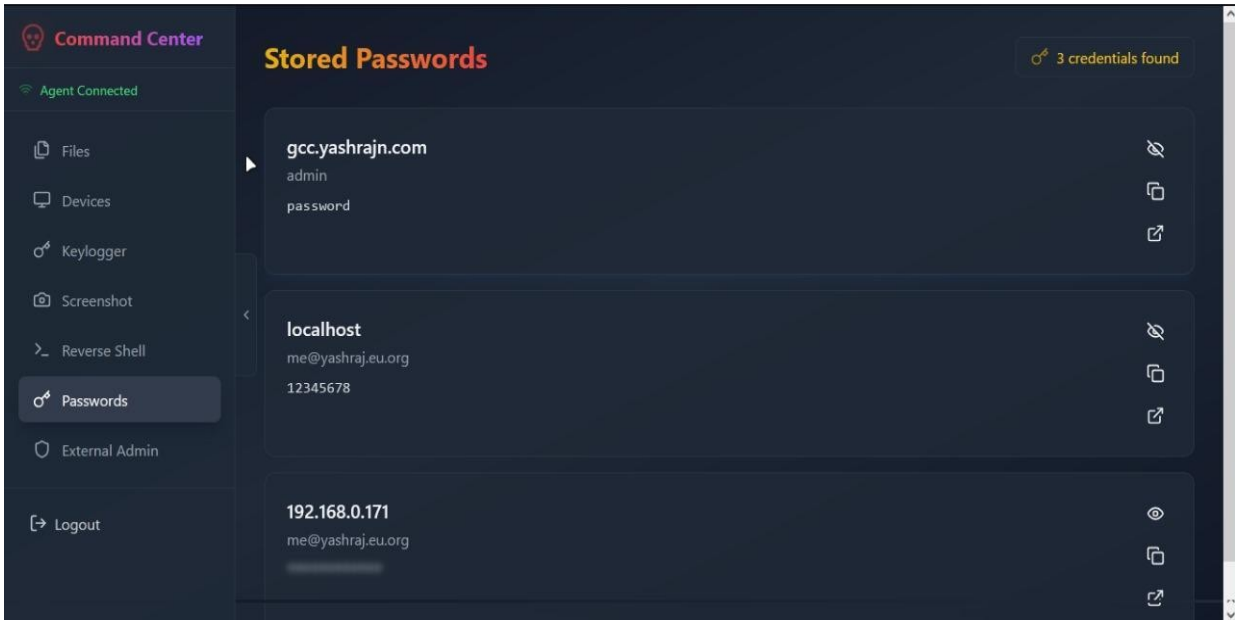
## Screenshot Viewer :



# Reverse Shell :



# Passwords :





### 3) Vishwesh Bhat – Phishing and Digital Awareness

Vishwesh presented various types of phishing attacks — including email, SMS, and voice phishing (vishing). He broke down how these threats trick users through urgency and social cues.

Participants were shown how to verify senders, spot malicious URLs, and report phishing attempts.

This segment reinforced how phishing often acts as the first step in malware or RAT deployment.

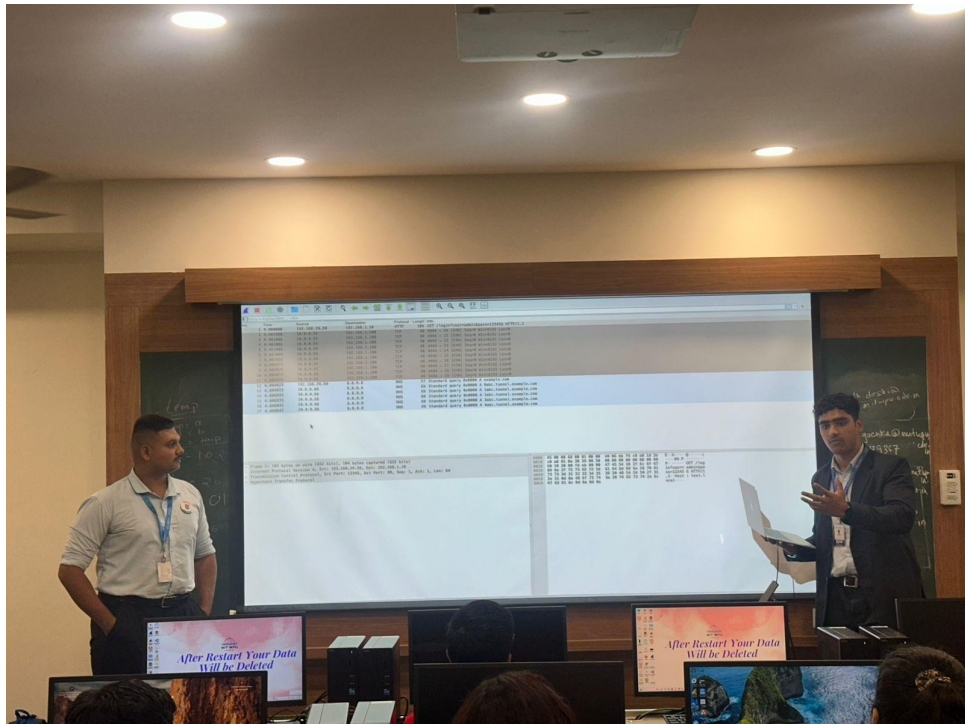


### 4) Nikhil Patil & Prasanna Dhamal – Tools & Bug Bounty

Nikhil and Prasanna introduced attendees to Wireshark, showcasing how network activity can be monitored and analyzed for suspicious traffic.

They also discussed CV analysis tools and how professionals use these to detect malware behaviors.

The session concluded with an overview of bug bounty programs—their role in ethical hacking, financial rewards, and how beginners can get started.



Network traffic analysis tool interface showing a list of captured packets and details for a selected packet.

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	192.168.29.59	192.168.1.10	HTTP	104	GET /login?user=admin&pass=123456 HTTP/1.1

Frame 1: 104 bytes on wire (832 bits), 104 bytes captured (832 bits)

Internet Protocol Version 4, Src: 192.168.29.59, Dst: 192.168.1.10

Transmission Control Protocol, Src Port: 12345, Dst Port: 80, Seq: 1, Ack: 1, Len: 64

Hypertext Transfer Protocol

Raw data (hex and ASCII):

```
0000 45 00 00 68 00 01 00 00 40 06 da f9 c0 a8 1d 3b E..h.....@.....;
0010 c0 a8 01 0a 30 39 00 50 00 00 00 00 00 00 00 00 ...-09-P.....
0020 50 18 20 00 fd eb 00 00 47 45 54 20 2f 6c 6f 67 P..... GET /log
0030 69 6e 3f 75 73 65 72 3d 61 64 6d 69 6e 26 70 61 in?user= admin&pa
0040 73 73 3d 31 32 33 34 35 36 20 48 54 54 50 2f 31 ss=12345 6 HTTP/1
0050 2e 31 0d 0a 48 6f 73 74 3a 20 74 65 73 74 2e 6c .1-Host : test.l
0060 6f 63 61 6c 0d 0a ocal....
```

Protocol: Hypertext Transfer Protocol: Protocol

Packets: 17 · Displayed: 1 (5.9%)

Profile: Default



dns

No.	Time	Source	Destination	Protocol	Length	Info
1052	0.202146	10.0.0.66	8.8.8.8	DNS	56	Standard query 0x0000 A stealer.ru
1053	0.204636	10.0.0.66	8.8.8.8	DNS	57	Standard query 0x0000 A malware.bad
1054	0.204636	10.0.0.66	8.8.8.8	DNS	57	Standard query 0x0000 A fakebank.cn
1055	0.204636	10.0.0.66	8.8.8.8	DNS	56	Standard query 0x0000 A stealer.ru
1056	0.204636	10.0.0.66	8.8.8.8	DNS	59	Standard query 0x0000 A cmdcontrol.co
1057	0.204636	10.0.0.66	8.8.8.8	DNS	56	Standard query 0x0000 A stealer.ru
1058	0.204636	10.0.0.66	8.8.8.8	DNS	56	Standard query 0x0000 A stealer.ru
1059	0.204636	10.0.0.66	8.8.8.8	DNS	56	Standard query 0x0000 A stealer.ru
1060	0.204636	10.0.0.66	8.8.8.8	DNS	56	Standard query 0x0000 A stealer.ru
1061	0.207195	10.0.0.66	8.8.8.8	DNS	59	Standard query 0x0000 A cmdcontrol.co
1062	0.207195	10.0.0.66	8.8.8.8	DNS	57	Standard query 0x0000 A fakebank.cn
1063	0.207195	10.0.0.66	8.8.8.8	DNS	56	Standard query 0x0000 A stealer.ru
1064	0.207195	10.0.0.66	8.8.8.8	DNS	59	Standard query 0x0000 A cmdcontrol.co
1065	0.209213	10.0.0.66	8.8.8.8	DNS	59	Standard query 0x0000 A cmdcontrol.co
1066	0.209213	10.0.0.66	8.8.8.8	DNS	59	Standard query 0x0000 A cmdcontrol.co
1067	0.209213	10.0.0.66	8.8.8.8	DNS	57	Standard query 0x0000 A fakebank.cn
1068	0.209213	10.0.0.66	8.8.8.8	DNS	59	Standard query 0x0000 A cmdcontrol.co
1069	0.209213	10.0.0.66	8.8.8.8	DNS	57	Standard query 0x0000 A dropper.biz
1070	0.209213	10.0.0.66	8.8.8.8	DNS	59	Standard query 0x0000 A cmdcontrol.co
1071	0.211224	10.0.0.66	8.8.8.8	DNS	59	Standard query 0x0000 A cmdcontrol.co
1072	0.211224	10.0.0.66	8.8.8.8	DNS	56	Standard query 0x0000 A stealer.ru
1073	0.211224	10.0.0.66	8.8.8.8	DNS	57	Standard query 0x0000 A malware.bad

Frame 1052: 56 bytes on wire (448 bits), 56 bytes captured (448 bits)  
Internet Protocol Version 4, Src: 10.0.0.66, Dst: 8.8.8.8  
User Datagram Protocol, Src Port: 5566, Dst Port: 53  
Domain Name System (query)

0000 45 00 00 38 00 01 00 00 40 11 60 63 0a 00 00 42 E-8....@..c...B  
0010 08 08 08 08 15 be 00 35 00 24 14 35 00 00 01 00 .....5..\$5....  
0020 00 01 00 00 00 00 00 00 07 73 74 65 61 6c 65 72 .....ru.....stealer  
0030 02 72 75 00 00 01 00 01

Domain Name System: Protocol Packets: 2051 · Displayed: 200 (9.8%) Profile: Default

http

No.	Time	Source	Destination	Protocol	Length	Info
1030	0.198630	10.0.0.66	192.168.1.10	HTTP	152	GET /admin HTTP/1.1
1031	0.198632	10.0.0.66	192.168.1.10	HTTP	152	GET /admin HTTP/1.1
1032	0.198632	10.0.0.66	192.168.1.10	HTTP	152	GET /admin HTTP/1.1
1033	0.198632	10.0.0.66	192.168.1.10	HTTP	152	GET /admin HTTP/1.1
1034	0.198632	10.0.0.66	192.168.1.10	HTTP	152	GET /admin HTTP/1.1
1035	0.198632	10.0.0.66	192.168.1.10	HTTP	152	GET /admin HTTP/1.1
1036	0.198632	10.0.0.66	192.168.1.10	HTTP	152	GET /admin HTTP/1.1
1037	0.198632	10.0.0.66	192.168.1.10	HTTP	152	GET /admin HTTP/1.1
1038	0.198632	10.0.0.66	192.168.1.10	HTTP	152	GET /admin HTTP/1.1
1039	0.198632	10.0.0.66	192.168.1.10	HTTP	152	GET /admin HTTP/1.1
1040	0.200639	10.0.0.66	192.168.1.10	HTTP	152	GET /admin HTTP/1.1
1041	0.200639	10.0.0.66	192.168.1.10	HTTP	152	GET /admin HTTP/1.1
1042	0.200639	10.0.0.66	192.168.1.10	HTTP	152	GET /admin HTTP/1.1
1043	0.200639	10.0.0.66	192.168.1.10	HTTP	152	GET /admin HTTP/1.1
1044	0.200639	10.0.0.66	192.168.1.10	HTTP	152	GET /admin HTTP/1.1
1045	0.200639	10.0.0.66	192.168.1.10	HTTP	152	GET /admin HTTP/1.1
1046	0.202146	10.0.0.66	192.168.1.10	HTTP	152	GET /admin HTTP/1.1
1047	0.202146	10.0.0.66	192.168.1.10	HTTP	152	GET /admin HTTP/1.1
1048	0.202146	10.0.0.66	192.168.1.10	HTTP	152	GET /admin HTTP/1.1
1049	0.202146	10.0.0.66	192.168.1.10	HTTP	152	GET /admin HTTP/1.1
1050	0.202146	10.0.0.66	192.168.1.10	HTTP	152	GET /admin HTTP/1.1
1051	0.202146	10.0.0.66	192.168.1.10	HTTP	152	GET /admin HTTP/1.1

Frame 1051: 152 bytes on wire (1216 bits), 152 bytes captured (1216 bits)  
Internet Protocol Version 4, Src: 10.0.0.66, Dst: 192.168.1.10  
Transmission Control Protocol, Src Port: 12049, Dst Port: 80, Seq: 1, Ack: 1, Len: 112  
Hypertext Transfer Protocol  
GET /admin HTTP/1.1\r\nHost: vulnerable.site\r\nAuthorization: Basic dXNlcjpwYXNkd29yZA==\r\nCredentials: user:password  
User-Agent: ScapyTest\r\n\r\n[Full request URI: http://vulnerable.site/admin]

0000 45 00 00 98 00 01 00 00 40 06 ae 6b 0a 00 00 42 E-----@..k...B  
0010 c0 a8 01 0a 2f 11 00 50 00 00 00 00 00 00 00 00 .....P.....  
0020 50 18 20 00 5b c4 00 00 47 45 54 20 2f 61 64 6d P...[...GET /adm  
0030 69 6e 20 48 54 54 50 2f 31 2e 31 0d 0a 48 6f 73 In HTTP/1.1-Hos  
0040 79 3a 20 76 75 6c 6e 65 72 61 62 6c 65 2e 73 69 t: vulne rable.s  
0050 74 65 0d 0a 41 75 74 68 6f 72 69 7a 61 74 69 6f te..Auth orizatio  
0060 6e 3a 20 42 61 73 69 63 20 64 58 4e 6c 63 6a 70 n: Basic dXNlcjpw  
0070 77 59 58 4e 7a 64 32 39 79 5a 41 3d 3d 0d 0a 55 wYXNkd29 yZA==U  
0080 73 65 72 2d 41 67 65 6e 74 3a 20 53 63 61 70 79 ser-Agen t: Scapy  
0090 54 65 73 74 0d 0a 0d 0a Test....

Frame (152 bytes) Basic Credentials (13 bytes) Packets: 2051 · Displayed: 51 (2.5%) Profile: Default

```

Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.23s latency).
Not shown: 990 closed tcp ports (reset)
PORT      STATE SERVICE
22/tcp    open  ssh
80/tcp    open  http
1035/tcp   filtered multidropper
2010/tcp   filtered search
2601/tcp   filtered zebra
3880/tcp   filtered igrs
4444/tcp   filtered krb524
6543/tcp   filtered myhttv
9929/tcp   open  nping-echo
31337/tcp  open  Elite
OS fingerprint not ideal because: Didn't receive UDP response. Please try again with -sSU
No OS matches for host

OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 10.48 seconds
prasannadhamal@Prasannas-MacBook-Air ~ % clear

prasannadhamal@Prasannas-MacBook-Air ~ % sudo nmap -O scanme.nmap.org
Starting Nmap 7.97 ( https://nmap.org ) at 2025-07-31 21:59 +0530
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.26s latency).
Other addresses for scanme.nmap.org (not scanned): 2600:3c01::f03c:91ff:fe18:bb2f
Not shown: 996 closed tcp ports (reset)
PORT      STATE SERVICE
22/tcp    open  ssh
80/tcp    open  http
9929/tcp   open  nping-echo
31337/tcp  open  Elite
OS fingerprint not ideal because: Didn't receive UDP response. Please try again with -sSU
No OS matches for host

OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 13.49 seconds

```

## 5) Yug Hiranandani – Practice Platforms & CTF Learning

Yug presented on platforms like TryHackMe and Hack The Box, explaining their role in skill-building through real-world simulations and challenges.

He encouraged participants to regularly engage in CTFs and practice labs, noting how these platforms help bridge the gap between theory and practical expertise.

## 6) Dhiraj Rajput – Career Growth, Networking & Resume Building

Dhiraj closed the session with career-oriented insights on building a strong presence in the cybersecurity domain.

He shared tips on creating a compelling LinkedIn profile, maintaining a focused resume, and connecting with mentors and professionals.

He also demonstrated real student profiles as examples of how to represent achievements and technical growth effectively.

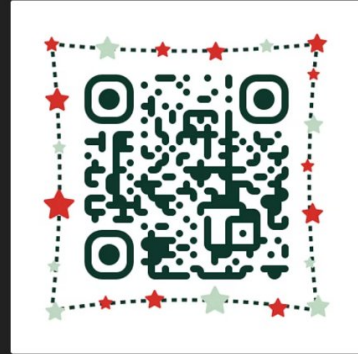
## Our LinkedIn



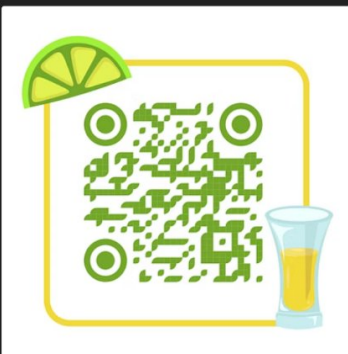
Sushant Kumar



Yashraj Narke



Ashish Sharma



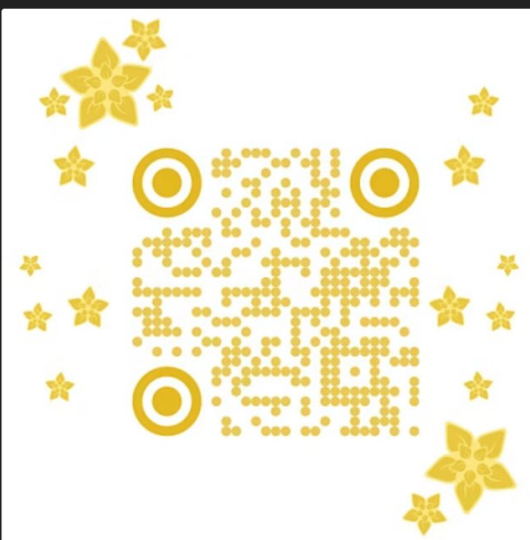
Vishwesh Bhat



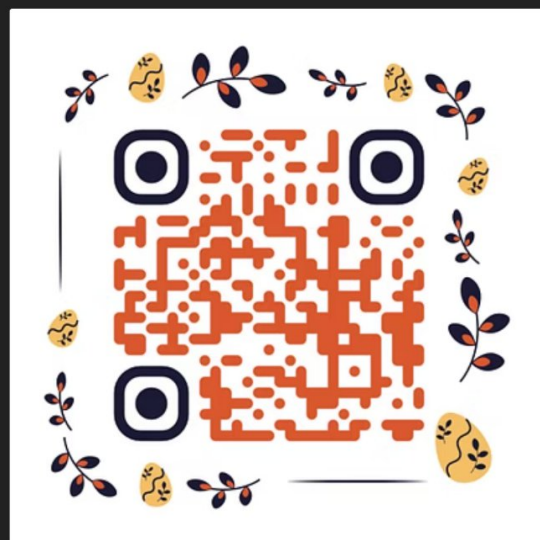
Dhiraj Rajput



Nikhil Patil



Yug Hiranandani



Prasanna Dhamal

## **Conclusion**

The session successfully combined awareness, technical demonstrations, and career insights to provide a 360-degree view of the current cybersecurity landscape.

Each speaker brought a unique perspective—from threats like phishing and RATs to the tools used to investigate them, and from ethical hacking platforms to career-building techniques.

Participants left better informed, more cautious, and motivated to pursue growth in the field of cybersecurity.

## **Presentation Link -**

<https://gamma.app/docs/Cybersecurity-Safety-Protecting-Yourself-in-the-Digital-Age-w6gkqohqn06uxs0?mode=doc>