TECNIA INSTITUTE OF ADVANCED STUDIES

NAAC GRADE "A" INSTITUTE (CYCLE-2)
Approved by AICTE, Ministry of Education Govt. of India,
Affiliated to G.G.S.I.P University & Recognized Under Sec. 2(f) of UGC Act 1956.
INSTITUTIONAL AREA, MADHUBAN CHOWK, ROHINI, DELHI-110085

CYBER SECURITY CLUB

Report (CYBER SECURITY AWARENESS PRESENTATION)

Event	PPT PRESENTATION
Type of Activity:	Ethical Hacking fundamentals
OBE Values	Innovation
Mulya Pravah	Dedication
Global Impact-UNSDG No.	SDG 9, SDG 16- **Industry, Innovation and Infrastructure & Peace, Justice and strong Institution.**
Objectives	1. To introduce students to the fundamentals of ethical hacking and cybersecurity. 2. To develop an understanding of ethical hacking methodologies and security testing. 3. To explain the importance of authorization, ethics and legal compliance while performing security testing. 4. To encourage students to explore careers and certifications in ethical hacking and cybersecurity. 5. To promote responsible and secure use of technology among college students.
Course Mapping	BCA 216T, BCA 220T, BCA 307T, MCA 253,BCA201,BCA301T
Course Outcome (CO)	Students will be able to identify common system, network and web application vulnerabilities using basic security assessment techniques. (CO2)
BT Level	BTL-3 (Apply)
Expected Outcomes	1. Students will be able to understand the fundamentals and phases of penetration testing. 2. Students will be able to identify common vulnerabilities in systems, networks and web applications. 3. Students will be able to apply appropriate techniques to reduce and mitigate identified security risks. 4. Students will be able to improve their readiness for further learning and careers in cybersecurity and ethical hacking.
In collaboration/association with	Domain Club: Cyber Security Club (DICT)
Name & Designation details of Resource Person- Internal Expert (LinkedIn Profile Link)	Dr. Sonal Jain, Assistant Professor (TIAS)
Name & Designation details of Resource Person- External Expert (Trained counseling expert(LinkedIn Profile Link)/	NA
Duration (Date & Time)	September 19, 2026
Mode (Offline/Hybrid)	Offline
Venue	COE-LAB, UG BUILDING, 2nd FLOOR, TIAS
No. of Internal Participants	20
No. of External Participants *[write NA if not applicable]*	0

No. of Institutions **Participated**	01
University Representation	NA
Awards/Recognition (if any) (Attach e-copy of Awards/Certificates)	E-Certificate

Innovation / Best Practice

The activity adopted a PPT presentation by establishing a best practice of learning the fundamental concept of ethical hacking.

Key innovative features include:

- Real world case studies included in PPT slides to connect theoretical concepts with practical cybersecurity incidents.
- Encourage adherence to industry standards and cybersecurity best practices.
- Promote ethical and responsible security testing with emphasis on legal authorization and cybersecurity ethics.
- Educate students about digital footprints, privacy and responsible online behaviour.
- Alignment of the activity with OBE – Innovation, Mulya Pravah – Dedication UNSDG 9,16–Industry, Innovation and Infrastructure & Peace, Justice and strong Institution.

Feedback:

Mode of feedback collection (form / oral / reflection / survey)	**Evidence to be maintained by the Event Coordinator:** • Attendance sheet • Event poster/flyer • Screenshots/photographs of the competition • Feedback form and responses
Key feedback highlights	**Students appreciated the opportunity to learn about ethical and responsible use of hacking techniques. The session encouraged students to explore further learning and career opportunities in cybersecurity. The event improved awareness of cybersecurity threats and safe online practices. Students gained a better understanding of ethical hacking and cybersecurity fundamentals.**
Suggestions for improvement (if any)	**NA**

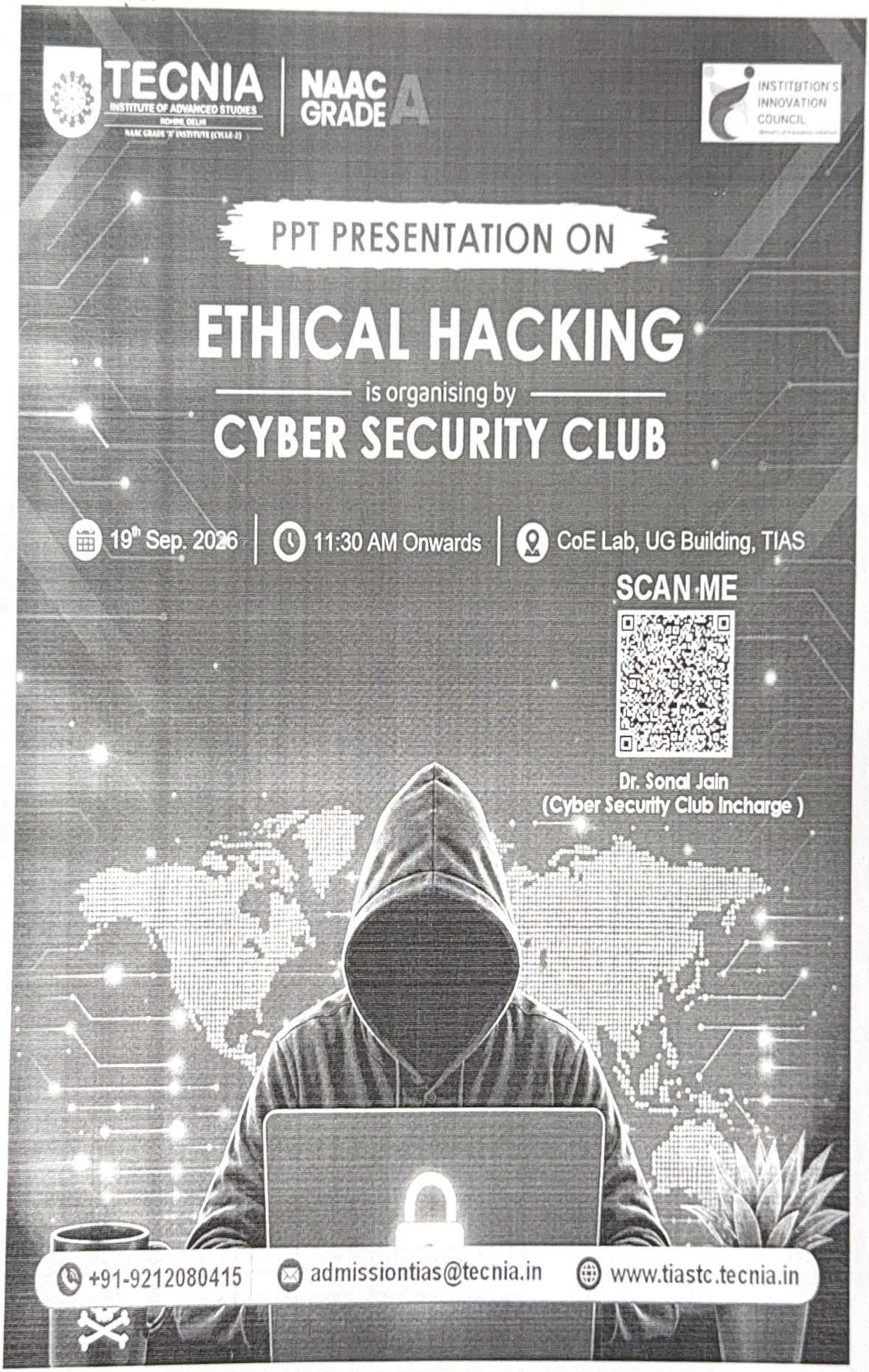
Conclusion:

The Ethical Hacking Fundamentals activity was informative and engaging. It helped students understand the basic concepts of cybersecurity and ethical hacking while emphasizing the importance of responsible and legal use of hacking techniques. The activity enhanced student's technical knowledge, cybersecurity awareness and interest in exploring future opportunities in the field of cybersecurity.

Media Coverage:

Social media link(s) (Mandatory)	https://www.instagram.com/tecniainstitute.ig/, https://in.linkedin.com/company/tecniainstitute, **https://www.facebook.com/Tecniaofficial/**
Print Media evidence (If any)	

Poster/Flyer



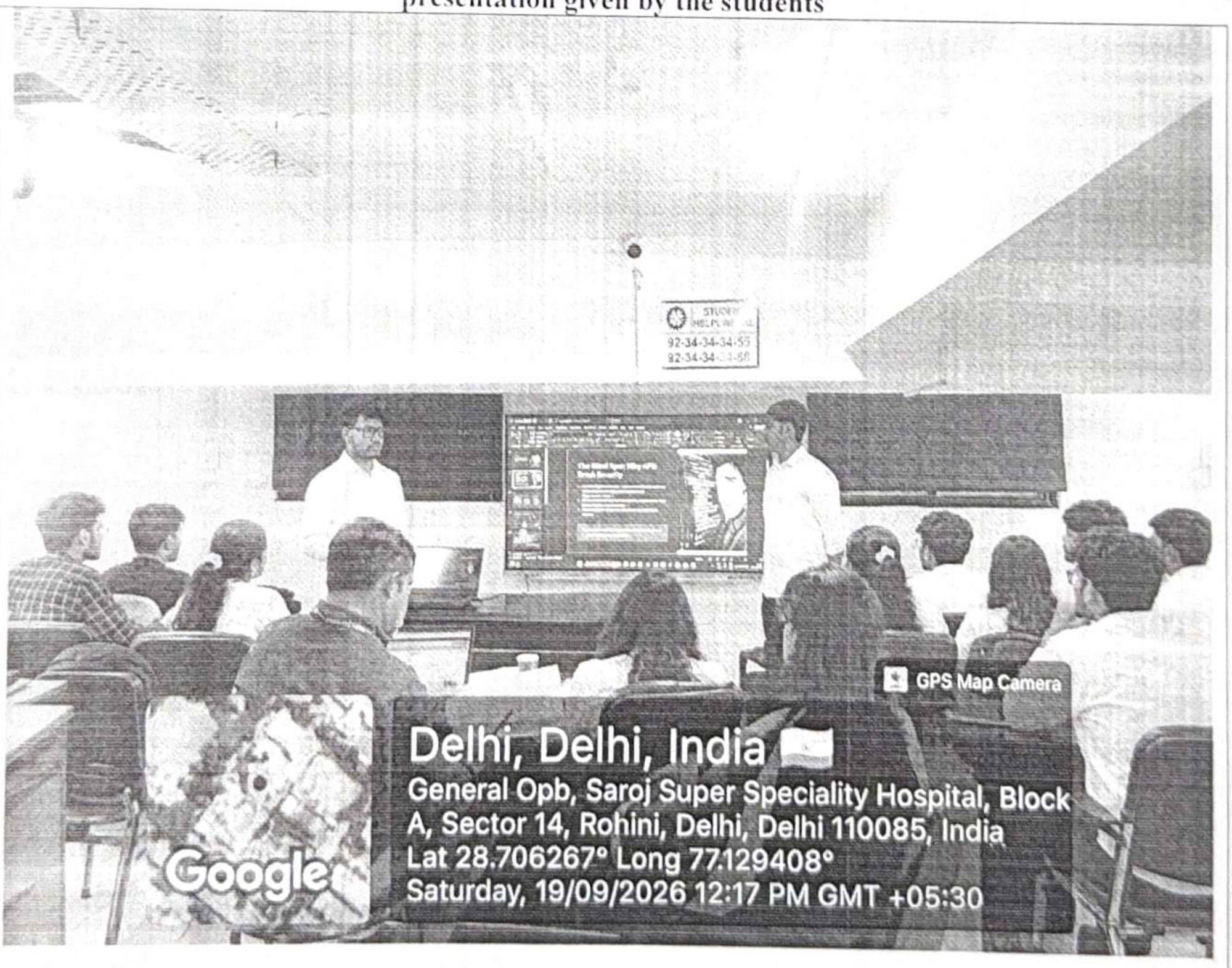
Between

Step-1: S

Geotag photos (with Caption):



presentation given by the students



Presentation given by the students

List of Participants (Attendance Sheet):

S.No.	Enrolment No.	Name of the Student	Prog & Year	Sign
1	08221302024	Mayank Mishra	BCA, Sem 3	
2	00521302024	Abhinav Ghildiyal	MCA, Sem 1	
3	03021302025	Nishika	BCA, Sem 3	
4	04321302024	Jatin	BCA, Sem 5	
5	04521302024	Lakshy Aggarwal	BCA, Sem 5	
6	03921302025	Ketna	BCA, Sem 3	
7	00417002025	Gazal bansal	BCA, Sem 3	
8	35921302024	Hardik	BCA, Sem 5	
9	36121302024	Prince	BCA, Sem 5	
10	00617002025	Alok Shukla	BCA, Sem 3	
11	02517002025	Mohd Ali	BCA, Sem 3	
12	03521302024	Himansh Bhagi	BCA, Sem 5	
13	0982130202	Mayank Sharma	BCA, Sem 5	
14	02121302024	Harshit Singh	BCA, Sem 5	
15	04121302024	Dhruv Behal	BCA, Sem 5	
16	01017002025	Kavya sharma	BCA, Sem 3	
17	02817002026	Himanshi Chauhan	BCA, Sem1	
18	01917004425	Maanas Sharma	MCA, Sem 3	
19	05021302024	Krish Khullar	BCA, Sem 5	

Event Coordinator/Club Incharge

Dr. Sonal Jain
Cyber Security Club Incharge

Dr. Ratandeep Kaur
Domain Club Head

Dr. Sushma Bahuguna
Asso. Dean, DICT
Asso. Dean, Dept. of Info. Comm. & Tech.
Tecnia Institute of Advanced Studies