



FROM CURIOSITY TO CYBERSECURITY



NAVIGATING THE CYBER REALM

LAUNCHING KCSC - KUET CYBER SECURITY CLUB

**HAND IN HAND WITH SGIPC AND IN COLLABORATION WITH
HIDDEN INVESTIGATIONS**

DATE: 21 AUGUST, 2025



WHO AM I

Sakibul Ali Khan

- Founder & Lead, Hidden Investigations (est. 2022)
- Security Researcher, Yogosha Strike Force

Core Focus

- Offensive security, CTFs, Vulnerability research, Red teaming

Achievements & Awards

- 1st Runner-up – BlackHat USA CTF 2025
- 2nd Runner-up – BCS ICT Fest CTF 2025 (Bangladesh Computer Society)
- 7th place – Phoenix Summit CTF 2025 (Red Team Village/Threat Sim)

Vision

- “Learn together to build a skilled community.”



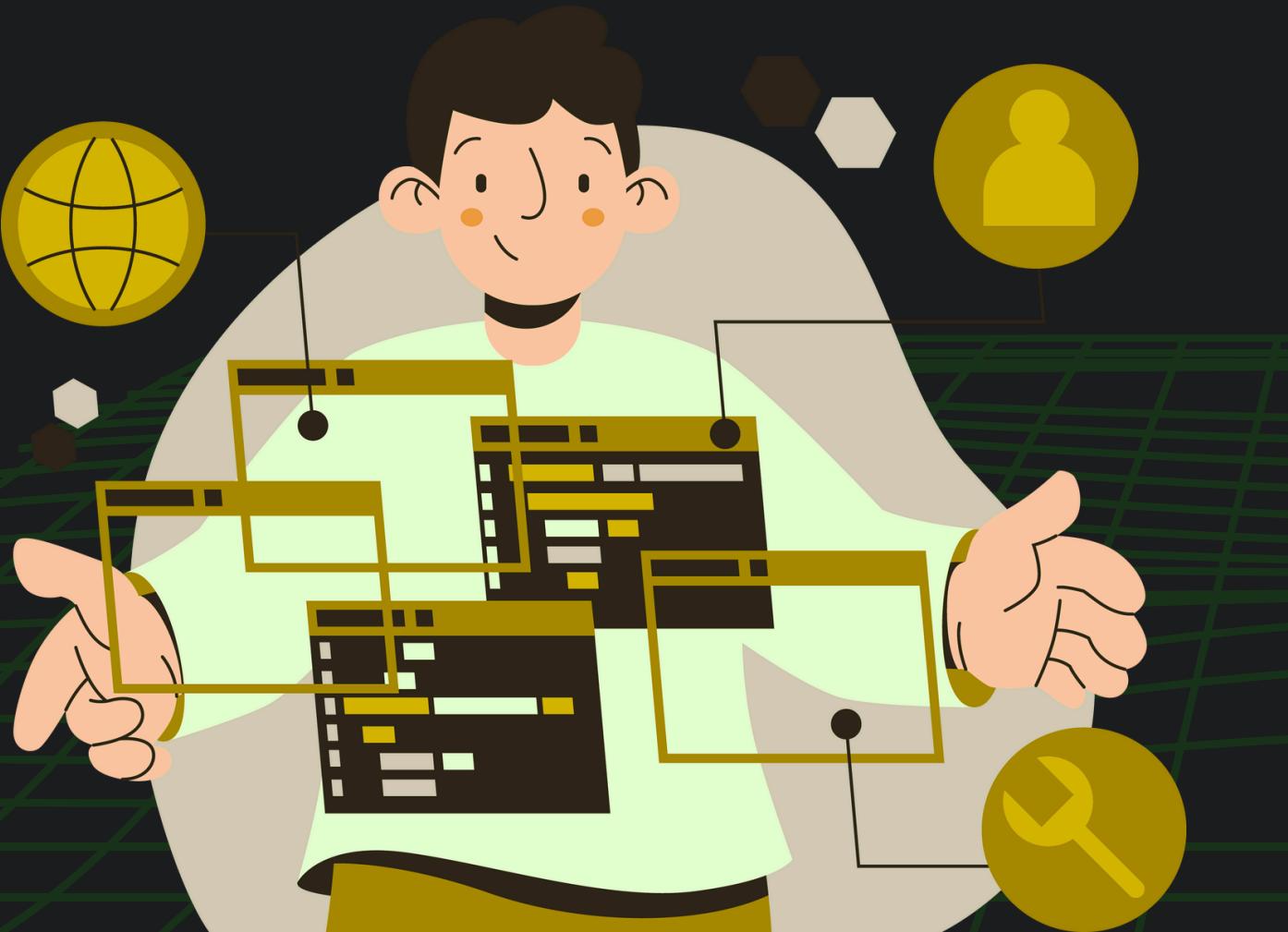
WHY CYBER SECURITY?



- CYBERCRIME IS A TRILLION-DOLLAR PROBLEM
- EVERY FIELD OF ENGINEERING NOW NEEDS SECURITY AWARENESS
- FROM PERSONAL DATA → NATIONAL SECURITY
- GROWING GLOBAL CAREER OPPORTUNITIES



CYBER SECURITY FIELDS



- Application Security (web, apps, APIs, bugs)
- Security Analyst (SOC Analyst)
- Forensics & Incident Response
- Cloud Security Specialist
- Corporate Security / Red Team (Attack) vs Blue Team (Defense)



SKILLS NEEDED TO START



- **BASICS** is everything
 - NETWORKING
 - LINUX & OTHER OS'S
 - PROGRAMMING
- **TOOLS** are a means to make the process faster by applying basic knowledge
 - BURP SUITE
 - WIRESHARK
 - CYBERCHEF
 - GHIDRA
- **MINDSET & ATTITUDE**
 - ASKING MORE QUESTIONS (HOW, WHY, WHAT IF)
 - SEARCHING FOR SOLUTIONS (PERSPECTIVE OF OTHERS)
 - PERSISTENCE
- **START SIMPLE, AS EXPERIENCE BUILDS UP OVER TIME**



MY JOURNEY (HIDDEN INVESTIGATIONS STORY)



- How I started (curiosity → hacking → learning)
- Challenges, failures, breakthroughs
- Building the Hidden Investigations Team
- Growing into a team with competitions, research & collabs
- Lessons I want KUET students to take away



CTFS: THE TRAINING GROUND



- WHAT IS A CTF? (QUICK DEFINITION)
- CATEGORIES (WEB, CRYPTO, FORENSICS, REVERSE, PWN, OSINT)
- WHY IMPORTANT: LEARN BY DOING, TEAMWORK, RECOGNITION
- WHERE TO PLAY: PICOCTF, HACKTHEBOX, CTFTIME



CAREER PATHWAYS IN CYBER SECURITY

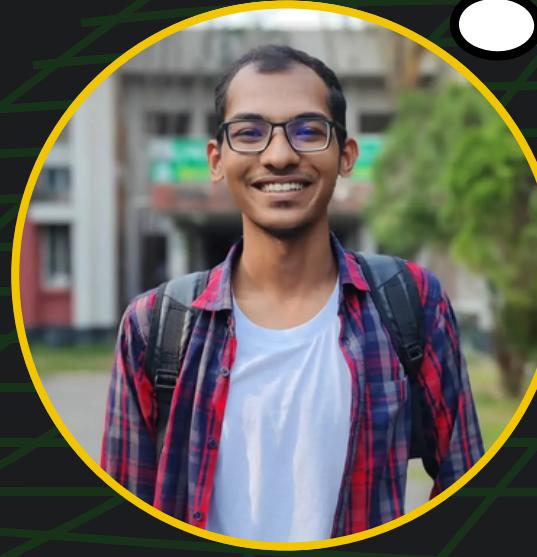


- Penetration Tester / Red Teamer
- Forensics & Incident Response
- Security Researcher
- Bug Bounty & Freelancing
- Academia & Research
- How CTFs + self-learning → career boost

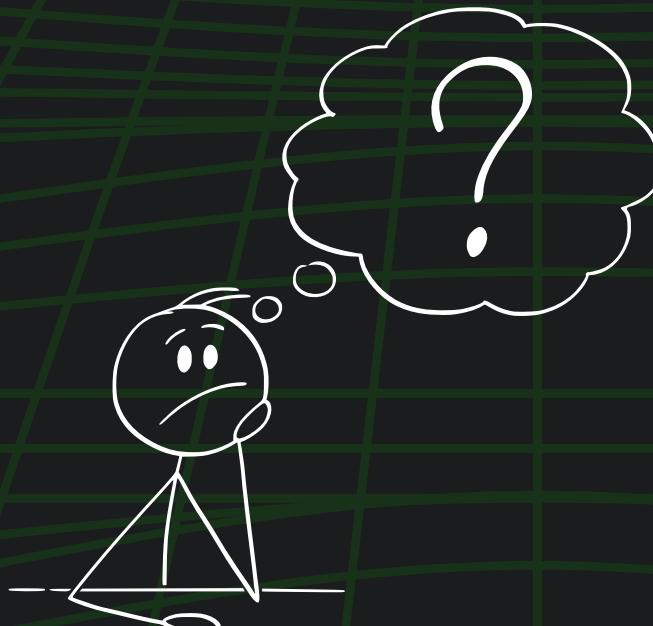


PRACTICAL DEMO

We found an image file, but something feels off. Its structure has been modified, and the message is hidden inside.



Milon Das
Hidden Investigations



Heightened Secrets





PRACTICAL DEMO



WHAT IS STEGANOGRAPHY?

- STEGANOGRAPHY IS THE ART AND SCIENCE OF HIDING INFORMATION WITHIN OTHER FILES OR MEDIA IN A WAY THAT DOESN'T RAISE SUSPICION.

WHAT ARE JPG (OR JPEG) FILES?

- A JPG/JPEG IS A POPULAR IMAGE FORMAT USED ACROSS THE INTERNET, ESPECIALLY IN PHOTOGRAPHY.



PRACTICAL DEMO

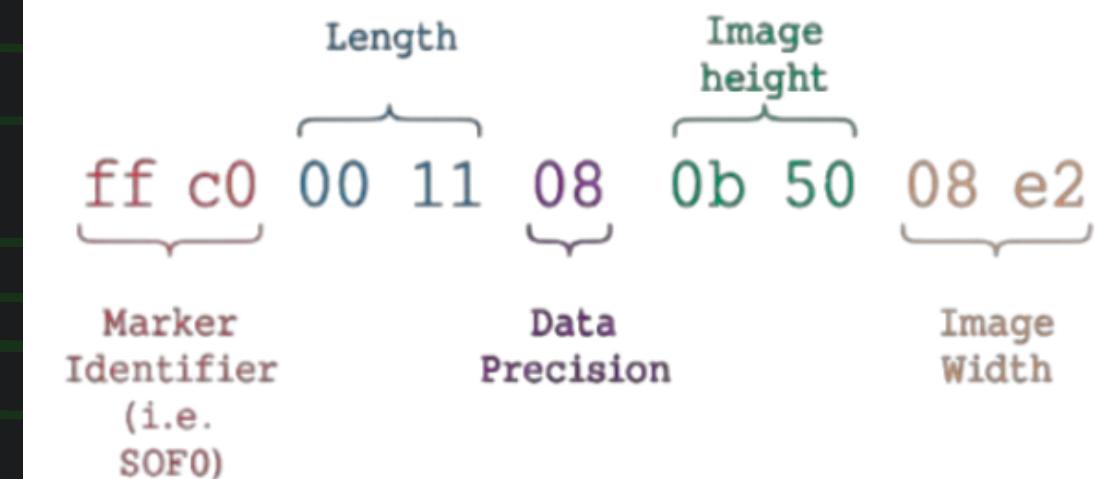
Short name	Bytes	Payload	Name
SOI	0xFF, 0xD8	none	Start Of Image
SOF0	0xFF, 0xC0	variable size	Start Of Frame (baseline DCT)
SOF2	0xFF, 0xC2	variable size	Start Of Frame (progressive DCT)
DHT	0xFF, 0xC4	variable size	Define Huffman Table(s)
DQT	0xFF, 0xDB	variable size	Define Quantization Table(s)
DRI	0xFF, 0xDD	4 bytes	Define Restart Interval
SOS	0xFF, 0xDA	variable size	Start Of Scan
RSTn	0xFF, 0xDn (n=0..7)	none	Restart
APPn	0xFF, 0xEn	variable size	Application-specific
COM	0xFF, 0xFE	variable size	Comment
EOI	0xFF, 0xD9	none	End Of Image

JPEG MARKERS (WIKIPEDIA REFERENCE)

- SOI = START OF IMAGE
- EOI = END OF IMAGE
- SOF = HOW THE PICTURE IS BUILT
- DQT/DHT = COMPRESSION DETAILS
- APP/COM = EXTRA INFO

SOF0 SEGMENT BREAKDOWN (JPEG HEADER EXAMPLE)

- FF C0 → START OF FRAME (BASELINE DCT MARKER)
- 00 11 → SEGMENT LENGTH (17 BYTES)
- 08 → DATA PRECISION (8 BITS)
- 0B 50 → IMAGE HEIGHT = 2896 PX
- 08 E2 → IMAGE WIDTH = 2274 PX





QNA TIME

HIDDENINVESTIGATIONS.NET



HIDDEN INVESTIGATIONS



QUIZ TIME

At testmoz.com/14759746 pass: letmein



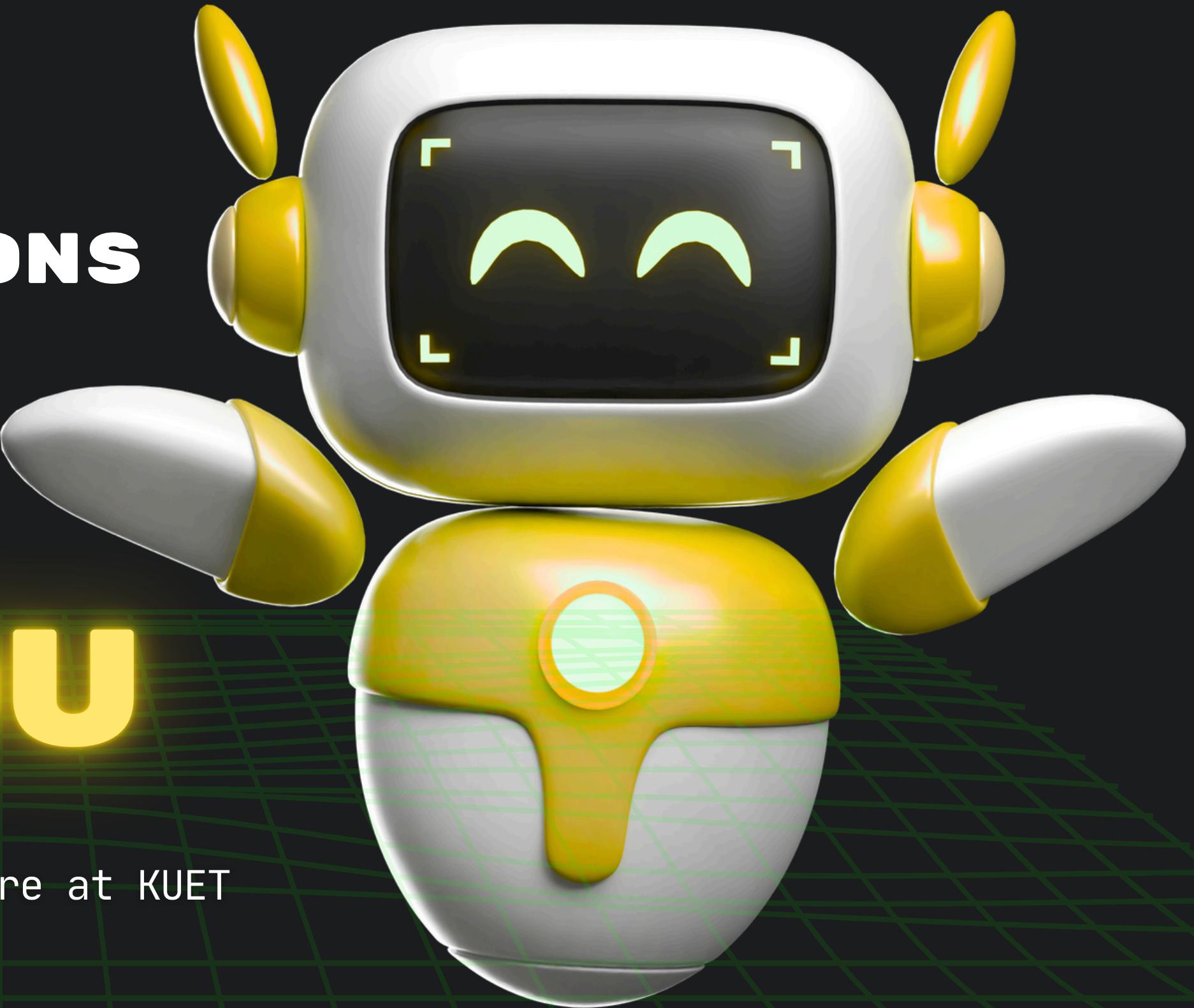
HIDDEN INVESTIGATIONS



YOUR CERTIFICATE
IS ON THE WAY



HIDDEN INVESTIGATIONS



THANK YOU

The future defenders & hackers can start right here at KUET