Microsoft Philanthropies "Cyber Shiksha for Educators" Training Program

Comprehensive Report

Phase 1: September 23, 2024 – October 5, 2024

Phase 2: February 13, 2025 – February 20, 2025

Phase 3: February 24, 2025 – March 7, 2025

Microsoft Philanthropies "Cyber Shiksha for Educators" Training Program

The Microsoft Philanthropies "Cyber Shiksha for Educators" Training Program, implemented by ICT Academy, was successfully conducted at The ICFAI University, Jaipur. The program aimed to enhance cybersecurity awareness and skills among faculty members and students through a structured, multi-phase approach. Cybersecurity has become an essential domain in the digital era, necessitating initiatives like this to equip educators and students with the expertise required to mitigate cyber threats.

The purpose of the "Cyber Shiksha for Educators" training program was to strengthen cybersecurity education and awareness within the academic ecosystem. With rising cyber threats globally, it has become crucial for universities to equip faculty and students with industry-relevant cybersecurity skills. This program sought to create a sustainable learning environment where faculty members could train students in cybersecurity best practices, ensuring that future professionals are well-prepared to handle cyber risks.

Objectives of the Training Program

The primary goal of the initiative was to equip faculty members with comprehensive cybersecurity knowledge and effective teaching methodologies. Through this, the trained faculty could impart cybersecurity education to students, ensuring they were well-versed in risk management and industry best practices. Additionally, the program aimed to prepare a select group of students for advanced cybersecurity training under Microsoft trainers. The initiative sought to create a sustainable knowledge-sharing environment where trained faculty could continue to educate future students, reinforcing cybersecurity awareness and education over time.

Significance of the Training Program

Cybersecurity threats are growing exponentially, affecting individuals, businesses, and institutions. The importance of this program lies in its ability to enhance the cybersecurity capabilities of educators, who can further disseminate this critical knowledge to students. By embedding cybersecurity education into academic programs, universities can prepare students to enter the workforce with a strong foundation in cybersecurity principles. Additionally,

collaborations with industry leaders like Microsoft ensure that the curriculum remains relevant and aligned with industry standards.

Program Details

The 'Cyber Shiksha for Educators' program was a multi-phase training initiative that progressed from faculty training to student training and finally to an advanced training stage under the guidance of Microsoft experts. The training was conducted under the supervision of ICT Academy, with Mr. Avi Sharma as the primary contact person. Mr. Sarvesh Kumar served as the Single Point of Contact (SPOC) and a training coordinator, along with Mr. Abhinav Pandey, ensuring smooth implementation and coordination throughout the program

Training Program Breakdown

Phase 1: Faculty Training (September 23, 2024 – October 5, 2024)

In the first phase, faculty members underwent an intensive training session conducted by expert trainers from ICT Academy and Microsoft. The objective was to equip faculty with advanced cybersecurity knowledge and effective teaching methodologies. The training was conducted virtually for a total of 40 hours, with sessions scheduled from 10:00 AM to 12:30 PM and 1:30 PM to 3:00 PM. The faculty members who participated in this training were:

- Mr. Sarvesh Kumar
- Mr. Gopal Patidar
- Mr. Abhinav Pandey
- Ms. Aarti Jangid
- Mr. Bhavesh Shah
- Ms. Toshika Lata
- Mr. Shiwam Pratap Singh

A final assessment was conducted on October 22, 2024, to evaluate their learning outcomes.

Phase 2: Student Training by Trained Faculties (February 13, 2025 – February 20, 2025)

Following their training, the faculty members took on the role of trainers and trained 90 final-year BCA students in fundamental cybersecurity concepts. This phase was conducted on

campus, with a training duration of 30 hours spread across five days. Each day consisted of two sessions—one from 10:30 AM to 12:30 PM and another from 1:00 PM to 4:00 PM. The training was led by:

- Mr. Sarvesh Kumar
- Mr. Gopal Patidar
- Mr. Abhinav Pandey
- Ms. Aarti Jangid
- Ms. Toshika Lata

A post-assessment was conducted on February 22, 2025, to evaluate student performance. Out of the 90 students trained, 60 students qualified for the next phase of advanced cybersecurity training.

Phase 3: Advanced Cybersecurity Training (February 24, 2025 – March 7, 2025)

The final phase involved an advanced cybersecurity training session conducted by a Microsoft trainer, Mr. Pratik Agrawal. This phase focused on providing an in-depth understanding of cybersecurity threats, risk management strategies, ethical hacking, and security protocols. The training was conducted on campus over 70 hours, with daily sessions from 9:30 AM to 12:30 PM and 1:30 PM to 5:00 PM. The final assessment took place on March 7, 2025, marking the successful completion of the training program.

Benefits of the Training Program

Professional Gains for Faculty

- Gained advanced cybersecurity knowledge to integrate into their teaching curricula
- Enhanced academic and professional growth through industry exposure
- Strengthened teaching methodologies in cybersecurity topics

Opportunities for Students

- Hands-on training in cybersecurity, increasing employability
- Exposure to real-world cybersecurity challenges and best practices
- Specialized knowledge from Microsoft experts, opening career opportunities

Strategic Advantages for the Institution

- Strengthened reputation for high-quality cybersecurity education
- Enhanced collaboration opportunities with Microsoft and ICT Academy
- Increased awareness and preparedness against cyber threats

Impact of the Training Program

The training program significantly impacted both faculty and students. Faculty members acquired advanced cybersecurity knowledge, enabling them to integrate cybersecurity topics into their curriculum and effectively train students. Meanwhile, students received hands-on exposure to real-world cybersecurity challenges, enhancing their preparedness for careers in cybersecurity and IT industries.

Achievements and Success Stories

The program led to several key achievements. Faculty members improved their teaching capabilities by incorporating cybersecurity topics into their academic sessions. Students developed hands-on expertise in risk assessment, cyber threat detection, and ethical hacking principles. Out of the 90 students trained, 60 advanced to the specialized cybersecurity training under a Microsoft expert. The university also witnessed an increased awareness of cyber threats among students and faculty, fostering a culture of cybersecurity preparedness.

Incentive Structure

As part of the incentive structure for the training program, Microsoft processed a financial transfer to acknowledge the contributions of the participating faculty and institution. A total amount of ₹10,000 was transferred to the organization, reinforcing its commitment to cybersecurity education. Additionally, each faculty member involved in the training received an incentive of ₹4,000 as recognition for their dedication and efforts in facilitating the program. This initiative not only motivated faculty members but also encouraged greater participation in future training programs.

Conclusion

The successful completion of the Microsoft Philanthropies "Cyber Shiksha for Educators" Training Program represents a major milestone in the university's commitment to cybersecurity

education. This program not only elevated cybersecurity awareness among faculty members and students but also laid the foundation for future training initiatives. Moving forward, the university aims to integrate cybersecurity modules into its curriculum and encourage continuous skill development in the field.

Microsoft CyberShikshaa syllabus coverage (30 Hrs) — Stage - 2 — ACADEMY

Institution Name : The ICFAI University, Jaipur	Course Name : Cyber Security
Mentor Name 1 : Satyesh Kumar	Start Date : 13/02/25
Mentor Name 2 : Gopal Pathak	End Date : 20/02/25
	Batch No

Sno	Module	Topic	Subtopic	Methodology	Duration	Traning Date	Tranier Signature
1	System Fundamentals	Enterprise Architecture- 0	Introduction to Digital data, its types and information; Introduction to information system, Introduction to management information systems (MIS) and its functions;	Lecture	1	13/02/25	
2		Enterprise Architecture - 1	Introduction to Data Centre and its infrastructure; Security at Google data centre; Facebook data centre. Assignment : Green Data Center	Lecture	1	13/02/25	
3		Virtualization and its Components- 0	Introduction to virtualization, its benefits and virtual machines; Components of Virtual Machines, its hardware and its benefits;	Lecture	1	13/02/25	
4		Virtualization and its Components - 1	Application and Desktop Virtualization and their techniques; Assignment: Creating Virtual Machine on Oracle Virtual box;	Lecture, Demo, HandsOn	1	13/02/25	
5	Module Assignment				1		
6	Module Summary				1		
7	Formative Assessment-1				1		

Sno	Module	Topic	Subtopic	Methodology	Duration	Traning Date	Tranier Signature
8	Need for Cyber Security	Overview of Cyber Security- 0	First Cyber Attack; Importance of Cyber Security; Human Firewal: An answer to your Cyber Security problem	Lecture	1	13/02/25	
9		Overview of Cyber Security - 1	Scope of Cyber Security; 5 laws of Cyber Security.	Lecture	1	14/02/25	
10		Types of cyber attacks	Types of cyber attacks	Lecture	1	14/02/25	
11		Ecosytem of Cyber Security	Cyber Security Framework; Attack Matrix and its features; Introduction of network security and recent developments; Types of Networks.	Lecture	1	14/02/25	
12	Module Assignment				1		
13	Module Summary				1		
14	Formative Assessment-2				1		
15		Fundamentals of Information Security - 0	Introduction to Information Security and its policies; CIA Triad-3 pillars of information security architecture;	Lecture	1	15/02/25	
16		Fundamentals of Information Security - 1	CIA components and its importance; Cyber security threats and best practices; Access controls and its types;	Lecture	1	15/02/25	
17		Fundamentals of Information Security - 2	Discretionary access control; Mandatory access control; Role based access control; Arbitrary based access control	Lecture	1	15/02/25	
18		Understanding Threats, Attack Categories and Hacking Process- 0	Active Reconnaissance; Types of Reconnaissance; Passive Reconnaissance; Types of Cyber Attack;	Lecture	1	15/02/25	
19		Understanding Threats, Attack Categories and Hacking Process- 1	Vulnerability Assessment and its features; Concept and types of Scanning Methodology; Penetration Tests	Lecture	1	15/02/25	

Sno	Module	Topic	Subtopic	Methodology	Duration	Traning Date	Tranier Signature
20	Introduction to Cyber Security	Understanding the Network Security- 0	Network Security Devices; Types of Network Securities; Network Access Control; Characteristics of Network Access Control;	Lecture	1	17/02/25	
21		Understanding the Network Security - 1	Application Security; Application Security Tools; Firewalls and its types; Introduce you virtual private network.	Lecture	1	17/02/25	
22		Understanding the Network Security - 2	Tunnelling protocol and types; IDS vs. IPS; IDS, IPS and their Types	Lecture	1	17/02/25	
23		Fundamentals of Web/Mobile Application Security- 0	ntroduction to Web Application Vulnerabilities; Basic Practices of Web Application Security; Common Cyberattacks on Web Applications; Mobile Application Vulnerabilities;	Lecture	1	18/02/25	
24		Fundamentals of Web/Mobile Application Security - 1	I Mobile Security Threats; Mobile Application Security; Fundamentals of Mobile Device Mangement; Overview of Mobile Device Management	Lecture	1	18/02/25	
25		Data Centre Security, Cloud Computing and Data Security- 0	Introduction to Cloud Computing and its types; Basics of Cloud Computing; cloud computing, its types, benefits and other considerations;	Lecture	1	18/02/25	
26		Data Centre Security, Cloud Computing and Data Security- 1	Types of Clouds and its different services; Cloud Computing Threats and Solutions; Clouds Computing – Threats and Vulnerabilities;	Lecture	1	20/02/25	

Modules - Stage 3:

Microsoft CyberShikshaa Stage 3 (70 Hrs) Session plan — Stage - 3

Institution Name: The Tafai University — Course Name: Cyber Security

Trainer Name: Tariq Ahmed — Start Date: 20-01-25

End Date: 07-03-25

Sno	Chapter	PlanCode	Subtopic	Methodology	Session_Hours (in minutes)	Skill_Type	Training Date	Trainer Signature
1	Network Security Threats and Countermeasures	Types of Firewall- 1	Firewall and its types; Types of Firewalls and its benefits	Lecture, Demo, Handson	60	Technical	24-01-25	
2	Network Security Threats and Countermeasures	Types of Firewall -2	Packet Filtering Firewall, Circuit-Level Gateway	Lecture	60	Technical	24-01-25	
3	Network Security Threats and Countermeasures	Types of Firewall -3	Application Firewall	Lecture	60	Technical	24-01-25	
4	Network Security Threats and Countermeasures	Inspection Techniques-1	Inspection Techniques; Stateful and Stateless Application	Lecture	60	Technical	24-01-25	
5	Network Security Threats and Countermeasures	Inspection Techniques-2	Stateful vs. Stateless Filtering Firewall	Lecture	60	Technical	24-01-25	
6	Network Security Threats and Countermeasures	Layers, Protocols and Ports- 1	Internet protocol; TCP Header; Transmission Control Protocol	Lecture	60	Technical	24-01-25	

Sno	Chapter	PlanCode	Subtopic	Methodology	Session Hours (In minutes)	Skill Type	Training Date	Trainer Signature
7	Network Security Threats and Countermeasures	Layers, Protocols and Ports- 2	User Datagram Protocol, Well known UDP and TCP Ports	Lecture	60	Technical	24-02-25	
8	Network Security Threats and Countermeasures	Layers, Protocols and Ports- 3	Client Server Model	Lecture	60	Technical	25-02-25	
9	Network Security Threats and Countermeasures	Layers, Protocols and Ports - 4	Internet Control Message Protocol; DNS and DHCP	Lecture	60	Technical	25-02-25	
10	Network Security Threats and Countermeasures	Layers, Protocols and Ports- 5	SSL and TSL; VPN and how it protects your IP address and privacy	Lecture	60	Technical	25-02-25	
11	Network Security Threats and Countermeasures	Firewall Features- 1	FortiManager and use cases; FortiAnalyzer and use cases	Lecture	60	Technical	25-02-25	
12	Network Security Threats and Countermeasures	Firewall Features- 2	Benefits of FortiManager; FortiManager Key Concepts	Lecture	60	Technical	25-02-25	
13	Network Security Threats and Countermeasures	Firewall Features- 3	Setting up FortiManager and its Considerations	Lecture	60	Technical	25-02-25	
14	Network Security Threats and Countermeasures	Firewall Features- 4	FortiAnalyzer Features; Forinet Use Cases and case studies of implementation	Lecture	60	Technical	25-02-25	

Sem	Chapter	Plan Code	Subtopic	Methodology	Session Hours Required	Skill Type	Description	Trainer Signature
17	Network Security Threats and Countermeasures	Network Level Attacks and Detection Techniques 1	Introduction to Fragment	Lecture, Demo, Hands-On	03	[illegible]	[illegible]	[illegible]
18	Network Security Threats and Countermeasures	Network Level Attacks and Detection Techniques 2	Understanding NMAP, OS Fingerprinting	Lecture, Demo, Hands-On	03	[illegible]	[illegible]	[illegible]
19	Network Security Threats and Countermeasures	Network Level Attacks and Detection Techniques 3	Non Cacheing and MAC attacks, ARP Poisoning	Lecture	03	Technical	[illegible]	[illegible]
20	Network Security Threats and Countermeasures	Network Level Attacks and Detection Techniques 4	Brute Force Attack	Lecture	03	Technical	[illegible]	[illegible]
21	Network Security Threats and Countermeasures	Security Recommendations, Countermeasures and Security Baseline 1	Overview of Security Baseline	Lecture	03	Technical	[illegible]	[illegible]
22	Network Security Threats and Countermeasures	Security Recommendations, Countermeasures and Security Baseline 2	HS Baseline Security Analysis	Lecture	03	Technical	[illegible]	[illegible]
23	Network Security Threats and Countermeasures	Security Recommendations, Countermeasures and Security Baseline 3	Protecting Networks against Advanced Evasion techniques	Lecture	03	Technical	[illegible]	[illegible]
24	Network Security Threats and Countermeasures	Security Recommendations, Countermeasures and Security Baseline 4	Firewall and IDS Forensic Security Logs and Checklist	Lecture	03	Technical	[illegible]	[illegible]

Sno	Chapter	PlanCode	Subtopic	Methodology	Session Hours (in minutes)	Skill Type	Running Date	Trainer Signature
23	Network Security Threats and Countermeasures	Network Analysis and Monitoring-1	Network Analysis, Identifier and view specific packets being sent and received on the network;	Lecture, Demo, HandsOn	60	Technical	23-03-25	
24	Network Security Threats and Countermeasures	Network Analysis and Monitoring-2	Security Configuration Checklist	Lecture	60	Technical	28-03-25	
25	Network Security Threats and Countermeasures	Network Analysis and Monitoring-3	Monitoring Network Bandwidth	Lecture, Demo, HandsOn	60	Technical	28-03-25	
26	Network Security Threats and Countermeasures	Network Analysis and Monitoring-4	Network Analyzers; Wireshark and its use cases	Lecture, Demo, HandsOn	60	Technical	28-03-25	
27	Network Security Threats and Countermeasures	Network Analysis and Monitoring-5	Wireshark Display Filters: Track network activity	Lecture, Demo, HandsOn	60	Technical	28-03-25	
28	Network Security Threats and Countermeasures	Network Analysis and Monitoring-6	View specific frame, tcp, ip and http	Lecture, Demo, HandsOn	60	Technical	28-03-25	
29	Module - 4 Revision				60	Technical	01-03-25	
30	Formative Assessment - 2				60	Technical	01-03-25	

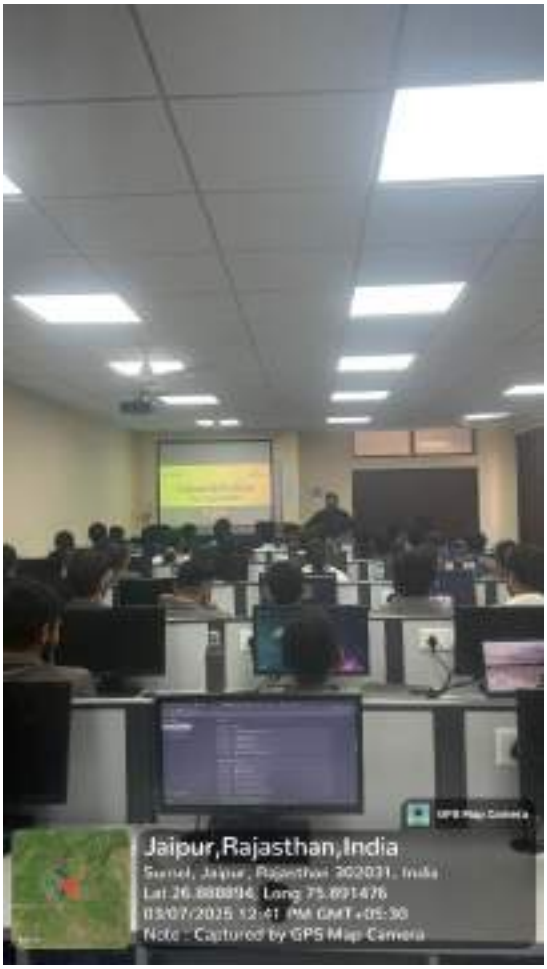
Sno	Chapter	PlanCode	Subtopic	Methodology	Session Hours (In minutes)	Skill Type	Scheduled Date	Trainer Signature
31	Cryptography	Introduction to Cryptography-1	Introduction to cryptography, Overview of cryptography	Lecture	60	Technical	[illegible]	
32	Cryptography	Introduction to Cryptography-2	Cryptography and Cryptanalysis, Types of cryptography	Lecture, Demo, HandsOn	60	Technical	[illegible]	
33	Cryptography	Introduction to Cryptography-3	Types of cryptography, Symmetric encryption, Asymmetric encryption, Hash Cryptography	Lecture, Demo, HandsOn	60	Technical	[illegible]	
34	Cryptography	Understanding Digital certificates and Signatures-1	Understanding digital certificates and signatures	Lecture, Demo, HandsOn	60	Technical	[illegible]	
35	Cryptography	Understanding Digital certificates and Signatures-2	Introduction to signatures	Lecture, Demo, HandsOn	60	Technical	[illegible]	
36	Cryptography	Understanding Digital certificates and Signatures-3	Introduction to digital certificates	Lecture	60	Technical	[illegible]	
37	Cryptography	Cryptographic attacks-1	Introduction to cryptographic attacks	Lecture	60	Technical	[illegible]	
38	Cryptography	Cryptographic attacks-2	Types of cryptographic attacks, Traditional cryptographic attacks.	Lecture	60	Technical	[illegible]	

Sno	Chapter	PlanCode	Subtopic	Methodology	Session Hours (in minutes)	Task Type	Training Date	Trainer Signature
39	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]
[illegible]	Web Server & Application Security	Web Application Architecture-1	[illegible] Architecture	Lecture	[illegible]	Technical	[illegible]	[illegible]
41	Web Server & Application Security	Web Application Architecture-2	Web Application Basics	Lecture	60	Technical	[illegible]	[illegible]
42	Web Server & Application Security	Web Application Architecture-3	Full Stack Development with M.E.R.N stack	Lecture	60	Technical	[illegible]	[illegible]
43	Web Server & Application Security	Web Application Architecture-4	Working of DNS (Domain Name System)	Lecture	60	Technical	[illegible]	[illegible]
44	Web Server & Application Security	Web Application Architecture-5	Working of DNS and its vulnerabilities	Lecture	60	Technical	[illegible]	[illegible]
45	Web Server & Application Security	Vulnerabilities in Web Server and Applications-1	Web Server Vulnerabilities	Lecture	60	Technical	[illegible]	[illegible]
46	Web Server & Application Security	Vulnerabilities in Web Server and Applications-2	Web Application Security	Lecture	[illegible]	Technical	[illegible]	[illegible]

Sno	Chapter	PlanCode	Subtopic	Methodology	Duration (Hours (In minutes))	Skill Type	Training Date	Trainer Signature
47	Web Server & Application Security	Vulnerabilities in Web Server and Applications - 3	Technology Stack for Web Development	Lecture	60	Technical	[illegible]	[illegible]
48	Web Server & Application Security	Vulnerabilities in Web Server and Applications - 4	Web Application Attacks; Importance of Web Security	Lecture	60	Technical	04-03-25	[illegible]
49	Web Server & Application Security	Vulnerabilities in Web Server and Applications - 5	Web Application Framework	Lecture	60	Technical	04-03-25	[illegible]
50	Web Server & Application Security	Proxy Setup - 1	What is HTTPS?; Working of HTTP; Configuring Chrome to work with Burp;	Lecture	60	Technical	05-03-25	[illegible]
51	Web Server & Application Security	Proxy Setup - 2	HTTP Request Methods;	Lecture	60	Technical	05-03-25	[illegible]
52	Web Server & Application Security	Proxy Setup - 3	HTTP Crash Course & Exploitation;	Lecture	60	Technical	05-03-25	[illegible]
53	Web Server & Application Security	Proxy Setup - 4	HTTP Status Messages; HTTP - Responses	Lecture	60	Technical	05-03-25	[illegible]
54	Web Server & Application Security	Secure Coding Practices - 1	Secure Coding Techniques	Lecture	60	Technical	05-03-25	[illegible]

Sno	Chapter	PlanCode	Subtopic	Methodology	Session_Hours (In minutes)	Skill_Type	Training Date	Trainer Signature
55	Web Server & Application Security	Secure Coding Practices- 2	OWASP Secure Coding Practices	Lecture, Demo, HandsOn	60	Technical	05-03-25	
56	Web Server & Application Security	Secure Coding Practices- 3	Quick Reference Guide	Lecture	60	Technical	05-03-25	
57	Web Server & Application Security	Web Application Vulnerability Scanning Tools- 1	Burp Suite and its tools:	Lecture, Demo, HandsOn	60	Technical	06-03-25	
58	Web Server & Application Security	Web Application Vulnerability Scanning Tools- 2	Nikto and its features	Lecture, Demo, HandsOn	60	Technical	06-03-25	
59	Web Server & Application Security	Web Application Vulnerability Scanning Tools- 3	CMSeek, its features and detection tools;	Lecture, Demo, HandsOn	60	Technical	06-03-25	
60	Web Server & Application Security	Web Application Vulnerability Scanning Tools- 4	Practice: Web Application Vulnerability Scanning Tools.	Lecture, Demo, HandsOn	60	Technical	06-03-25	
61	Web Server & Application Security	Web Application Vulnerability Scanning Tools- 5	WPScan and its uses	Lecture, Demo, HandsOn	60	Technical	06-03-25	
62	Web Server & Application Security	Burp Suite Intruder/Repeater -1	Burp Repeater	Lecture, Demo, HandsOn	60	Technical	06-03-25	

Images from the event:




IcfaiTech
Jaipur,Rajasthan,India
Sumel, Jaipur, Rajasthan 302031, India
Lat 26.888689, Long 75.891799
03/07/2025 12:49 PM GMT+05:30
Note : Captured by GPS Map Camera


IcfaiTech
Jaipur,Rajasthan,India
Sumel, Jaipur, Rajasthan 302031, India
Lat 26.888707, Long 75.891810
03/07/2025 12:49 PM GMT+05:30
Note : Captured by GPS Map Camera