Syllabus
Gyanmanjari Institute of Technology
Semester-4 (B. Tech.)

Subject: Cyber Security – BET1CE14312

Type of course: Professional Elective Courses

Prerequisite: Basic knowledge of computer networks and operating systems, and familiarity with basic programming languages such as C, C++, and Python.

Rationale:

This course provides a comprehensive introduction to Cyber Security with a focus on modern defense techniques, ethical hacking fundamentals, and digital investigation skills. It covers core concepts such as threats, vulnerabilities, risk management, and security controls, along with the architecture of secure systems and networks. Students will learn about malware analysis, cryptography, secure communication, web application security, and network protection mechanisms.The course also includes hands-on experience with security tools for vulnerability assessment, penetration testing, incident response, and basic digital forensics. By the end of this course, learners will understand how to identify attacks, secure systems, investigate incidents, and implement security measures following industry best practices. This ensures strong theoretical knowledge and practical skills required for modern organizations, SOC environments, and cybersecurity roles.

Teaching and Examination Scheme:

Teaching Scheme			Credits	Examination Marks		Total Marks
CI	T	P	C	SEE	CCE	
2	0	2	3	100	50	150

Legends: CI-Class Room Instructions; T – Tutorial; P - Practical; C – Credit; SEE - Semester End Evaluation; CCE-Continuous and Comprehensive Evaluation.

Course Content:

Sr. No	Course Content	Hrs.	% Weightage
1	**Foundations of Cyber Security & Threat Landscape** ***Theory Topics:*** Introduction to Cyber Security, Information Security vs Cyber Security, Digital Assets, Threats, Vulnerabilities, Risks, CIA Triad (Confidentiality, Integrity, Availability), AAA Model, Security Controls (Administrative, Technical, Physical), Cyber Attack Lifecycle (Reconnaissance to Exploitation), Types of Attacks: Phishing, Malware, Password Attacks, Social Engineering, DoS/DDoS, Insider Threats, Introduction to Malware Types (Virus, Worm, Trojan, Ransomware), Basics of Security Tools: Antivirus, Firewall, IDS/IPS, Basic Awareness: Cyber Hygiene, Strong Passwords, Safe Browsing, Software Updates. ***Practical:*** 1. Basic System Information Enumeration — Use systeminfo, ipconfig/ifconfig, and uname commands to collect OS version, IP details, hardware info, and network configuration. 2. File & Directory Handling Commands — Use mkdir, ls/dir, copy/cp, move/mv, and del/rm to create, modify, move, and delete files/folders through the command line. 3. User & Permission Management — Configure user accounts, set passwords, and apply access rights using net user, useradd, chmod, and chown. 4. Process & Network Activity Monitoring — Identify running processes and active network ports using tasklist, ps -aux, netstat/ss, and htop. 5. Detect Basic Malware Indicators — Locate suspicious processes, services, and autorun entries using command-line inspection and system startup checks. 6. Perform Network Scanning – Use Nmap/Zenmap to discover active hosts, open ports, and basic network services for understanding network exposure 7. Assess System Security – Generate detailed system audit reports using WinAudit or Lynis to evaluate configuration weaknesses and security posture 8. Identify Malware Categories – Examine safe, static malware samples to understand characteristics and classify them into common malware types	18	20%

9. Test Password Strength – Use offline password checkers or John the Ripper to analyze password complexity and learn how weak passwords can be exploited
10. Observe Network Traffic – Capture and inspect packet flows using Wireshark to understand common protocols and recognize unusual network behavior
11. Apply Basic System Hardening – Configure firewall settings, manage User Account Control, and disable unnecessary services to enhance device security
12. Analyze System Logs – Explore Event Viewer or Linux log files to detect failed login attempts, warnings, and suspicious system events

Evaluation Method:

Sr. No.	Evaluation Methods	SEE	CCE
1	**Identifying System Weaknesses** Students will perform a compact security assessment on a given task and evaluate potential risk points. They are expected to interpret system exposure, observe system behavior, recognize suspicious elements, and provide a short rational conclusion on system safety and preventive improvements	20	
2	**Active Learning Assignment Secure Link & Email Inspection Task** To help students understand the basic concepts of identifying unsafe digital content through hands-on, inquiry-based activities that simulate real-world cyber threats. Students will examine sample emails and URLs, observe visible security indicators, analyze suspicious elements, and classify each item as safe or unsafe. They need to document their observations in a PDF format. and upload their completed inspection report on the GMIU Web Portal.		10
	Total	20	10

	Examination Style: **Identifying System Weaknesses (20 Marks)** Students will carry out a basic security evaluation of a provided system/machine to detect weak points and potential risks. The faculty will provide a prepared task or environment containing observable network behavior, configuration states, and possible security gaps for assessment. Students are expected to identify exposure, review system condition, and note signs of unsafe activity or weak protection. Finally, they will prepare a short conclusion and give explanation summarizing the vulnerabilities found along with simple, practical mitigation steps. **Secure Link & Email Inspection Task (10 Marks)** By the end of this activity, students will be able to identify key indicators of phishing and unsafe links, such as suspicious domains, misspelled URLs, fake HTTPS symbols, unusual attachments, and misleading sender details. They will learn to differentiate between genuine and fraudulent emails using basic techniques like URL hovering, sender verification, and checking HTTPS security. Students will open the faculty-provided folder containing sample emails and URLs, inspect each item for security cues, and decide whether it is safe or unsafe with a brief justification. After completing all samples, students will prepare a short inspection sheet in PDF format and upload it individually on the GMIU Web Portal.		
2	**Securing Systems, Networks, and Digital Identities** ***Theory Topics:*** Introduction to System & Network Security, Network Security Concepts, Secure Communication, Digital Identity & Access Management, Password & Credential Security, Endpoint & Device Security, Social Engineering & Human Attacks, Digital Footprint & Privacy Protection, Incident Response Basics. ***Practical:*** 13. Perform File Encryption – Use Windows EFS or 7-Zip AES-256 to encrypt files or folders and verify restricted access using a secondary user account. 14. Create a Secure Password Vault – Build a simple password vault using Excel or Google Sheets and protect the file using password	18	20%

	or encryption settings. 15. Check Browser Security Settings – Review HTTPS indicators, certificate details, cookie settings, site permissions, and tracking protection to generate a browser security checklist. 16. Configure a Basic Firewall Rule – Use Windows Defender Firewall to block a specific application or port and test the rule's effectiveness. 17. Apply File and Folder Permissions – Modify Read, Write, Modify, and Deny permissions using OS security settings and verify them through another user account. 18. Analyze Running System Processes – Use Task Manager or Process Explorer to identify unsafe, unknown, or unsigned system processes and document potential risks. 19. Perform Backup and Restore – Use Windows Backup or File History to back up important files and restore them to validate the backup process. 20. Inspect Browser Extensions – Review installed browser extensions or add-ons, check their permissions, and remove or disable any unsafe or unfamiliar ones. 21. Configure User Account Security – Create standard and administrator user accounts in Windows, apply login and password restrictions, and verify access control differences using both accounts. 22. Prepare a Report on Social Engineering Attacks – Study common social engineering techniques such as phishing, pretexting, and baiting, analyze real-world examples, and document prevention measures for individuals and organizations. 23. Enable Account Lockout Policy – Configure account lockout threshold using Local Security Policy, attempt multiple failed logins, and observe system lockout behavior and recovery. 24. Secure Removable Storage Devices – Restrict or allow USB storage access using Windows security or Group Policy settings and verify file transfer restrictions. 25. Prepare a Basic Incident Response Report – Document the steps involved in basic incident response including identification, containment, eradication, and recovery using a simple cyber incident scenario. 26. Design a Digital Footprint Awareness Poster – Create an educational poster explaining digital footprints, online privacy risks, and methods to control personal data exposure on the internet. 27. Verify Secure Communication (HTTPS & TLS) – Inspect HTTPS indicators, TLS version, encryption algorithms, and certificate chain in a web browser and compare secure and insecure websites.		

Evaluation Method:

Sr. No.	Evaluation Methods	SEE	CCE
1	**Endpoint Security Setup & Verification** Students will perform a complete endpoint security setup that includes enabling of the antivirus protection, configuring a firewall rule, applying device permission settings, and securing local user accounts. After the setup, they must verify the security posture by giving a viva of summarizing all applied controls.	20	
2	**Digital Security Practice Activity** Students perform a small but meaningful cybersecurity task such as creating a secure password vault, correcting a risky browser setting, configuring file permissions, or identifying a social engineering message. Students submit a short reflection describing the task, its importance, and the security improvement it provides.		10
	Total	20	10

Examination Style:

Endpoint Security Setup & Verification (20 Marks)
Students will secure a computer system by configuring essential endpoint protections such as antivirus settings, firewall rules, file permissions, and account security controls. After applying these configurations, students will verify their effectiveness by testing blocked applications, checking permission restrictions, and confirming active security features. A short report with screenshots and make whole task submitted as proof of successful endpoint security setup and verification with oral examination.

	Digital Security Practice Activity (10 Marks) Students will complete one hands-on micro-activity where they perform a focused security action, such as Creating a secure password vault, removing risky browser extensions, securing file permissions, Detecting a fake message (social engineering simulation)		
3	**Fundamentals of Ethical Hacking and Vulnerability Assessment** ***Theory Topics:*** Introduction to Ethical Hacking and Security Testing, Phases of Ethical Hacking (Reconnaissance, Scanning, Enumeration, Exploitation, Reporting). Types of Reconnaissance: Passive & Active, Footprinting Techniques (Google Dorking, Social Enumeration), Introduction to Vulnerability Assessment, Common Vulnerabilities (Weak Credentials, Open Ports, Misconfigurations), Vulnerability Scoring Basics (CVSS), Web Application Vulnerabilities Overview (Broken Authentication, Injection, XSS, File Upload Issues, Security Misconfigurations), Network Vulnerabilities (Unsecured Services, Weak Firewalls, Insecure Protocols), Basics of Secure Architecture (Defense-in-Depth, Least Privilege, Zero Trust Principles), Introduction to SOC Monitoring and Log-Based Detection. ***Practical:*** 28. Perform Reconnaissance – Use OSINT tools (Whois, nslookup, and online footprinting tools) to gather public information about a test target. 29. Identify Open Ports and Services – Scan lab machines using Nmap to detect exposed ports and analyze potential weaknesses 30. Study Defense-in-Depth Using Architecture Diagrams – Analyze given system or network architecture diagrams and identify missing security layers using defense-in-depth principles(Draw.io (diagrams), OWASP Secure Architecture guidelin). 31. Enumerate System Information – Use tools like Netdiscover and SMB/FTP enumeration commands on safe lab systems. 32. Detect Common Web Vulnerabilities – Use DVWA or WebGoat (local offline installation) to practice identifying XSS, SQLi, and insecure inputs. 33. Analyze Vulnerability Reports – Use OpenVAS/Greenbone pre-generated reports to understand vulnerability severity and CVSS scoring. 34. Test Weak Credentials – Perform dictionary-based login testing on provided practice services with controlled, permitted credentials.	18	25%

35. Assess Network Weaknesses – Identify insecure services, outdated protocols, and weak configurations using Nmap scripts or built-in OS tools.
36. Document Findings – Prepare a short vulnerability report summarizing discovered issues and recommending basic fixes.
37. Analyze Google Dorking Risks – Identify exposed files, directories, or sensitive information using safe Google dorks on sample domains and document risks and mitigation techniques(Google Search (Dork queries), Exploit-DB Google Dork Database).

Evaluation Method:

Sr. No.	Evaluation Methods	SEE	CCE
1	**SecureScan Discovery Challenge** Students will learn how ethical hackers identify system weaknesses by performing basic reconnaissance and scanning tasks in a safe lab environment. They will spot vulnerabilities such as open ports and weak configurations, gaining a clear understanding of how attackers find entry points and how such issues can be prevented.	20	
2	**Active Learning Assignment System Weakness Evaluation Report** Students will review the results of a basic vulnerability scan or lab assessment and prepare a short report highlighting the weaknesses found, their possible impact, and simple recommended fixes. This task helps students practice documenting security issues clearly and understanding how vulnerabilities affect system safety.		10
	Total	20	10

	Examination Style: **SecureScan Discovery Challenge (20 Marks)** Students will perform basic ethical hacking activities on a safe, controlled computer machine. They will carry out simple reconnaissance and scanning using approved tools to identify open ports, weak configurations, or exposed services. Students must explain how these weaknesses could be discovered by an attacker and suggest straightforward methods to prevent misuse. Their evaluation will be based on the accuracy of vulnerability identification, clarity of explanation, and understanding of how attackers locate system entry points. **System Weakness Evaluation Report (10 Marks)** Students will be given the output of a basic vulnerability scan or a preconfigured lab assessment. They must prepare a short and clear report that lists the detected weaknesses, explains the potential impact of each, and recommends simple fixes.This task evaluates the student's ability to interpret vulnerability findings, summarize risks, and document security issues in a structured manner. The report should be uploaded individually on the GMIU Web Portal.		
4	**Cyber Ethics, Legal Aspects & Smart Device Security** ***Theory Topics:*** Introduction to Cyber Ethics and Legal Frameworks, Overview of the IT Act 2000 and Its Amendments, Importance and Limitations of Cyber Law, Significance of Cyber Ethics in Modern Digital Culture, Cyberbullying and Online Harassment, Global Data Protection Principles (GDPR), Impact of Digital Forensics in Law Enforcement, Basics of Artificial Intelligence Ethics, Blockchain Ethics and Responsible Technology Use, Introduction to Smart Devices and IoT Ecosystem, Types of Smart Devices (Wearables, Smart Home Assistants, CCTV Cameras, Smart Appliances), Smart Device Operating Systems and Firmware Security, Secure Device Setup and Configuration (Strong Passwords, Biometric Locks, Auto-Updates), Application and Permission Management, Network Security for Smart Devices (Wi-Fi Security, Guest Network Usage), Secure Device Pairing (Bluetooth and NFC), Privacy Protection in Smart Devices (Camera, Microphone, Location), and Smart Home Security Concepts.	18	20%

***Practical*:**

38. Create a basic Privacy Notice for a sample mobile application, including data collection and user rights.
39. Explore & Extract EXIF Metadata – Extract metadata from a photo using an online EXIF viewer and identify details such as camera model, date, and GPS location.
40. Inspect a Website's Privacy Policy – Review the privacy policy of a popular websites and summarize what user data it collects and how it is used.
41. Trace a public blockchain transaction using a blockchain explorer and document the transaction details.
42. Identify and document sensors and connectivity modules present in any smart device (e.g., smartphone, smartwatch).
43. Perform secure device setup by configuring strong passwords, enabling auto-updates, and disabling unused features.
44. Inspect Wi-Fi network security settings and verify encryption (WPA2/WPA3) and password strength.
45. Design a simple smart home security architecture diagram showing devices and security measures
46. Evaluate an AI Tool for Ethical Concerns – Test an AI chatbot or generator with sample prompts and document any biased or inappropriate outputs.
47. Map Your Digital Footprint – Perform a self-check by searching your public online presence (name/email) and record what publicly available information appears.

Evaluation Method:

Sr. No.	Evaluation Methods	SEE	CCE
1	**Smart Device Security & Ethics Mini Practical** Students will perform a quick hands-on task—such as extracting EXIF data, tracing a blockchain transaction, creating a privacy notice, identifying smart device sensors, or checking basic security settings—and briefly explain the related security or ethics concept.	20	

	2	**IoT Home Security Blueprint:** Students draw(From Draw.io) a simple smart home diagram showing devices, network layout, and security measures (guest network, firewall, secure pairing).		10	
		Total	20	10	

Examination Style:

Smart Device Security & Ethics Mini Practical (20 Marks)
Students will complete a simple hands-on task from the practical list, such as extracting EXIF data, tracing a blockchain transaction, creating a short privacy notice, identifying sensors in a smart device, or checking basic security settings like Wi-Fi encryption or app permissions. They will perform the assigned task within a few minutes and briefly explain the security or ethical concept involved.

IoT Home Security Blueprint (10 Marks)
Students will design a simple smart home security diagram that shows how different smart devices (such as smart lights, smart TVs, cameras, assistants, and sensors) connect within a home network. The diagram should clearly indicate the main Wi-Fi network, a separate guest network for visitors or untrusted devices, and basic security measures like strong passwords, WPA2/WPA3 encryption, secure Bluetooth pairing, firewalls, and auto-updates. Students should label each device and highlight where security protections are applied, demonstrating a clear understanding of how to secure an IoT-enabled home environment.

5	**Cybercrime: Illustrations, Examples and Mini Cases:** ***Theory Topics:*** Introduction, Kinds of Cyber Crime (Cyber staking, Software Privacy and Crime related to IPRs, Phishing, Denial of Service Attack(DoS), Identity Theft), Real-Life Example (Maharashtra Website Govt. Hacked, E-Mail Spoofing and Bombing, Indian Bank Fraud, Jamtara Scam, Mini Cases (The Zig-Zigler Case, Cyberpornography (Minor Case), Indian Online Gambling, Pune Citybank Call Center Fraud, NASSCOM vs. Ajay Sood etc.), Online Scams (Purchasing Goods and Services Scam, Lottery Scam, Charity Scam, Pet Scam, The Hitman Scam, Pyramid Scheme Scams etc.), Digital Signature and Digital signature Crime, Financial Fraud.	18	15%

Practical:

48. Analyze the headers of a suspicious email to detect spoofing or phishing attempts.
49. Create a fake login page offline and identify signs that indicate phishing.
50. Verify File Integrity Using Hashes – Generate MD5/SHA256 hashes for two files (genuine vs. modified) and compare them to detect tampering.
51. Create an Awareness Poster on Online Scams(PowerPoint) – Design an educational poster explaining common online scams (lottery, charity, pet, pyramid schemes) with prevention tips for the general public.
52. Analyze a Fake Digital Identity Profile with OSINT – Examine a sample social media or e-commerce profile provided by the faculty to identify indicators of identity theft, impersonation, or fake accounts and document warning signs.
53. Detect Online Payment Fraud Indicators – Analyze a simulated transaction receipt or bank alert message to identify red flags related to financial fraud such as mismatched URLs, unusual payment flow, or fake customer support numbers.
54. Simulate a DoS Indicator Check – Observe network slowdown patterns or blocked access on a controlled lab machine to understand symptoms of DoS attempts
55. Digitally sign a PDF and verify its authenticity.
56. Compare a genuine software installer and a pirated installer to detect suspicious modifications.
57. Categorize and analyze various online scam messages (lottery, charity, pet, pyramid schemes)
58. Analyze a Breach Case Study – Review a short real-life cybercrime incident summary provided by the faculty and identify the attack type, victim impact, and exploited vulnerability.
59. Perform WHOIS lookup and SSL check on a suspicious website to analyze trustworthiness.
60. Analyze SMS and Email Scam Indicators Using Online Analyzers – Examine suspicious SMS or email content to identify phishing patterns, shortened URLs, and scam keywords(VirusTotal (URL/Text scan), PhishTank (online), browser URL preview).

Evaluation Method:

Sr. No.	Evaluation Methods	SEE	CCE
1	**Cybercrime Forensic Analysis Challenge:** Students will perform one assigned forensic task—such as email header analysis, WHOIS lookup, EXIF extraction, the digital signature verification, or the scam message review—and present their findings & real time screen-shots with a structured tool vise explanation.	20	
2	**Active Learning Assignment Digital Crime Pattern Exploration** Students will explore a set of curated mini cybercrime scenarios provided by the faculty—such as financial fraud attempts, impersonation cases, ransomware notes, or phishing templates—and identify the crime type, the attacker's strategy, and the target's vulnerability. They will reflect on how the crime could have been prevented and submit a short write-up and make a case study pdf document with summarizing their understanding.		10
	Total	20	10

Examination Style:

Cybercrime Forensic Analysis Challenge (20 Marks)
Each student will perform one major cyber-forensic activity assigned by the examiner, such as analyzing an email header for spoofing, performing a WHOIS and SSL check on a suspicious website, extracting EXIF metadata from an image, verifying a digital signature on a PDF, or examining scam messages for fraud patterns. The student must carry out the steps accurately, interpret the findings, and provide a brief explanation or justification of the conclusions drawn based on the evidence collected. Students will give a short viva based on the task they performed.

	Digital Crime Pattern Exploration (10 Marks) The faculty will provide a curated set of short cybercrime scenarios—such as suspicious financial activity alerts, fake communication attempts, unusual login notifications, or misleading online messages. Students will study these scenarios, identify the type of cybercrime represented, interpret the attacker's likely method, and determine the weakness that allowed the incident to occur. They will prepare a brief explanation linking the clues to the crime type and suggest simple preventive measures. This activity emphasizes understanding crime patterns, attacker behavior, and basic defensive reasoning without requiring any technical tools.		

Suggested Specification Table:

Distribution of Marks (Revised Bloom's Taxonomy)						
Level	Remembrance (R)	Understanding (U)	Application (A)	Analyze (N)	Evaluate (E)	Create (C)
Weightage %	10%	25%	25%	20%	10%	10%

Note: This specification table shall be treated as a general guideline for students and teachers. The actual distribution of marks in the question paper may vary slightly from the above table.

Course Outcome:

After learning the course, the students should be able to:	
CO1	Understand fundamental concepts of cyber security, threats, vulnerabilities, security principles, attack types, and basic cyber hygiene practices.
CO2	Apply system and network security techniques to protect digital identities, credentials, endpoints, communications, and respond to basic security incidents.
CO3	Assess systems and networks using ethical hacking and vulnerability assessment techniques to identify security weaknesses and interpret assessment results.
CO4	Evaluate cyber ethics, legal frameworks, and emerging technology ethics, and implement security and privacy measures for smart devices and IoT systems.
CO5	Examine real-life cybercrime cases and online scams to identify attack methods, impacts, legal aspects, and preventive measures.

Instructional Method:

The course delivery method will depend upon the requirement of content and needs of students. The teacher, in addition to conventional teaching methods by black board, may also use any tools such as demonstration, role play, Quiz, brainstorming, MOOCs etc.

From the content 10% topics are suggested for flipped mode instruction.
Students will use supplementary resources such as online videos, NPTEL/SWAYAM videos, e-courses, Virtual Laboratory.

The internal evaluation will be done on the basis of the Active Learning Assignment.
Practical/Viva examination will be conducted at the end of semester for evaluation of performance of students in the laboratory.

Reference Books:

[1] Cyber Security: Understanding Cyber Crimes, Computer Forensics and Legal Perspectives, Nina Godbole & Sunit Belapure, Wiley India.
[2] Computer Security: Principles and Practice, 4th Edition, William Stallings & Lawrie Brown, Pearson Education.
[3] The Web Application Hacker's Handbook: Finding and Exploiting Security Flaws, 2nd Edition, Dafydd Stuttard & Marcus Pinto, Wiley Publication.
[4] Information Security: Principles and Practice, 2nd Edition, Mark Stamp, Wiley India.
[5] CEH v11 – Certified Ethical Hacker Study Guide, Ric Messier / EC-Council, Wiley India.

Suggested Assessment Guidelines

Module 1: Foundations of Cyber Security & Threat Landscape

Identifying System Weaknesses (20 Marks)		
Criteria	**Description**	**Marks**
Observation & Detection	Identifies visible system issues or suspicious behavior.	5
Analysis of Weaknesses	Points out possible vulnerabilities or weak settings.	5
Security Reasoning	Explains why the issue is risky.	5
Mitigation Suggestions	Suggests simple preventive or corrective steps.	5
	Total	**20**

Module 2: Securing Systems, Networks, and Digital Identities

Endpoint Security Setup & Verification (20 Marks)		
Criteria	**Description**	**Marks**
Security Configuration	Correct firewall, permissions, and account controls.	5
Effectiveness Testing	Verifies protections through simple system checks.	5
Report Submission	Shows screenshots demonstrating applied settings.	5
Oral Examination	Briefly explains each security control.	5
	Total	**20**

Module 3: Fundamentals of Ethical Hacking and Vulnerability Assessment

Endpoint Security Setup & Verification (20 Marks)		
Criteria	**Description**	**Marks**
Scanning	Performs basic recon and port scanning.	5
Detection	Identification of weak configurations.	5
Attack View	Explains Exploitation works.	5
Prevention	Suggests simple fixes to secure the system.	5
	Total	**20**

Module 4: Cyber Ethics, Legal Aspects & Smart Device Security

Smart Device Security & Ethics Mini Practical (20 Marks)		
Criteria	**Description**	**Marks**
Task Execution	Correct Task.	5
Accuracy	key details (EXIF data, sensors, permissions, etc.).	5
Concept Understanding	Clear Explanation of the related security/ethical idea.	5
Clarity of Output	Correct Screenshots & Findings.	5
	Total	**20**

Module 5: Cybercrime: Illustrations, Examples and Mini Cases:

Cybercrime Forensic Analysis Challenge (20 Marks)		
Criteria	**Description**	**Marks**
Task Execution	RAW data (email header, WHOIS, EXIF, etc.).	5
Evidence Interpretation	Findings & crime indicators.	5
Conclusion Quality	Clear,justification based on collected evidence.	5
Viva Performance	Explanation of the whole analysis.	5
	Total	**20**