

KRISHNA UNIVERSITY

BOARD OF STUDIES (BoS) – DEPARTMENT OF COMPUTER SCIENCE

MINUTES OF THE BOARD OF STUDIES MEETING

Date: Saturday, 22 August 2026

Time: 2:55 PM – 4:25 PM

Mode: Online through Google Meet

Members Present

S. No.	Name	Designation	Role
1	Prof. R. Kiran Kumar	Dept. of Computer Science, Krishna University	Chairman
2	Smt. P. Durga Bhavani	HOD, Dept. of Computer Science, Nalanda Degree College, Vijayawada	Member
3	Kondapalli Ramkumar	HOD, Dept. of Electronics and Internet of Things, Nalanda Degree College, Vijayawada	Member
4	Bommareddy Sudheer Reddy	Lecturer, Dept. of Computer Science, Nalanda Degree College & PG Centre, Vijayawada	Member
5	Prof. P. Suresh Varma	Dept. of CSE, Adikavi Nannaya University, Rajahmundry	Member
6	Dr. M.H.M. Krishna Prasad	Dept. of CSE, JNTUK, Kakinada	Member
7	Prof. D. Lalitha Bhaskari	Dept. of CS & Systems Engineering, Andhra University	Member
8	Assoc. Prof. M. Babu Reddy	HOD, Dept. of Computer Science, Krishna University	Member

Agenda

To discuss and approve the introduction of Machine Learning and Cyber Security as Minor papers.

Proceedings

The meeting commenced at **2:55 PM** with the Chairman welcoming all the members. The proposal for introducing **Machine Learning (ML)** and **Cyber Security** as Minor papers was placed before the Board for discussion.

The members discussed the proposed syllabus, course structure, credits, practical components, Course Outcomes, and industry relevance of the two Minor papers. The members also provided suggestions to make the courses practical, application-oriented, and aligned with current industry requirements.

Resolution

After detailed discussion, the **Board of Studies approved/recommended the introduction of the following as Minor papers:**

- 1. Machine Learning**
- 2. Cyber Security**

The Board recommended that the syllabus, Course Outcomes, credits, teaching scheme, and assessment pattern be finalized incorporating the suggestions of the members and submitted to the **competent academic authority for approval and implementation.**

Conclusion

The Chairman thanked all the members for their valuable suggestions and active participation. The meeting concluded with a vote of thanks.

Meeting ended at: 4:25 PM

Chairman, Board of Studies

Prof. R. Kiran Kumar

Signature: _____

BoS Coordinator / Head of the Department

Name: _____

Signature: _____

Handwritten signature in red ink, possibly reading "JL" or "JL" with a horizontal line.

Handwritten signature in blue ink, possibly reading "BSR" or "BSR" with a horizontal line.

Handwritten signature in black ink, possibly reading "JL" or "JL" with a horizontal line.

Handwritten signature in purple ink, possibly reading "K. Ankur" or "K. Ankur" with a horizontal line.

Handwritten signature in black ink, possibly reading "11" or "11" with a horizontal line.

**Model Syllabus for Cyber Security (Minor) in consonance with Curriculum
framework w.e.f. AY 2025-26**

COURSE STRUCTURE

Year	Semester	Course	Title of the Course	No. of Hrs /Week	No. of Credits
II	III	1	Computer Network and Security	3	3
			Computer Network and Security Lab	2	1
	IV	2	Introduction to Cyber Security	3	3
			Introduction to Cyber Security Lab	2	1
III	V	3	Information Security	3	3
			Information Security Lab	2	1
		4	Cryptography	3	3
			Cryptography Lab	2	1
	VI	5	Ethical Hacking	3	3
			Ethical Hacking Lab	2	1
		6	Digital Forensics and Incident Response	3	3
			Digital Forensics and Incident Response Lab	2	1

SEMESTER-III

COURSE 1: Computer Networks and Security

Theory

Credits: 3

3 hrs/week

UNIT I: Fundamentals of Computer Networks

Introduction to Computer Networks • Introduction to Computer Networks • Types of Computer Networks (LAN, MAN, WAN, PAN) • Network Topologies • Network Devices: Hub, Switch, Router, Modem, Access Point, Gateway • Transmission Media (Guided and Unguided)

UNIT II: Network Models and Communication Protocols

Network Models and Protocols • OSI Reference Model • TCP/IP Model • Comparison of OSI and TCP/IP Models • Data Encapsulation • Network Protocols • MAC Address and IP Address

UNIT III: IP Addressing and Network Services

IP Addressing and Internet Services • IPv4 Addressing • Public and Private IP Addresses • Subnet Mask (Basic Concepts) • DNS (Domain Name System) • DHCP (Dynamic Host Configuration Protocol) • NAT (Network Address Translation)

UNIT IV: Internet Protocols and Communication Security

Internet Protocols and Network Security • HTTP and HTTPS • FTP and SFTP • SMTP, POP3, and IMAP • SSH and Telnet • VPN (Introduction) • Common Port Numbers: 20, 21, 22, 23, 25, 53, 80, 110, 143, 443

UNIT V: Network Security Fundamentals

Network Security Fundamentals • Firewalls • Antivirus Software • Intrusion Detection System (IDS) • Intrusion Prevention System (IPS) • Proxy Server • Secure Wi-Fi Practices • Basic Network Troubleshooting

TEXT BOOK:

1. **William Stallings** – *Network Security Essentials: Applications and Standards*, 7th Edition, Pearson.
2. **Behrouz A. Forouzan** – *Data Communications and Networking*, 5th Edition, McGraw Hill.

SEMESTER-III

COURSE 1: Computer Networks and Security LAB

Practical

Credits: 2

2 hrs/week

List of Experiments:

1. Identify networking devices and create a simple LAN in Cisco Packet Tracer.
2. Study OSI/TCP-IP models using Packet Tracer simulations.
3. Configure IPv4 addressing and test connectivity with ping.
4. Capture HTTP, DNS, and ICMP traffic using Wireshark.
5. Configure Windows Firewall and perform basic network troubleshooting.

SEMESTER-IV

COURSE 2: INTRODUCTION TO CYBER SECURITY

Theory

Credits: 3

3 hrs/week

Unit 1. Cyberspace and Internet Fundamentals:

Cyber Space Cyberspace: Definition, Architecture and Regulation; Overview of Web technology; Internet: Advent of internet, World Wide Web, Internet infrastructure for data transfer and governance.

Unit 2. Cyber Crimes and Cyber Threats:

Cyber Crimes History & Development, Classification of cybercrimes- Cyber Terrorism, Cyber Threats, Cyber Stalking, Pornography, Child Pornography, Hacking, Viruses, Worms, Trojans, Malware, Scareware, Adware, Command and Control, Botnet, Cyber Trespass, Cyber Theft, Cyber Fraud, Password Cracking, Malware, Hunk Mail, Steganography, Cyber Terrorism, Cyber Warfare, Phishing. Impact of cybercrimes- Effect of cybercrimes on society, Cybercrimes against people, property, business and nation. Evaluation of cybercrimes, Definition of cyber criminals, Trends in cybercrime across India & the world.

Unit 3. Cyber Security Fundamentals:

Need and Importance, Overview, Cybersecurity Domains and Growth, The Cybersecurity Cube - Three Dimensions, CIA Triad, Confidentiality, The Principle of Confidentiality, Protecting Data Privacy, Controlling Access-Laws and Liability; Data Integrity: Principle, Need and Integrity Checks, Availability, The Principle of Availability, Ensuring Availability.

Unit 4. Social Media Security:

Social Media and Security Social networks: Introduction and Overview, Opportunities, Pitfalls; Social media: Types, Platforms, Monitoring, Hashtag, Viral content, Marketing, Privacy, Challenges, Security issues, Flagging and reporting of inappropriate content, Laws regarding posting of inappropriate content, Best practices, Case studies.

Unit 5. E-Commerce and Digital Payment Security:

E-Commerce and Digital Payments E- Commerce: Definition, Components, Security Elements, Threats, Security best practices. Digital payments: Introduction, Components, Modes (Banking Cards, Unified Payment Interface (UPI), e-Wallets, Unstructured Supplementary Service Data (USSD), Aadhar enabled payments), Frauds and Preventive measures. RBI guidelines on digital payments and customer protection in unauthorized banking transactions. Relevant provisions of Payment Settlement Act, 2007.

Text Books:

1. Cyber Crime Impact in the New Millennium, by R. C Mishra , Auther Press. Edition 2010.
2. Cyber Security Understanding Cyber Crimes, Computer Forensics and Legal Perspectives by Sumit Belapure and Nina Godbole, Wiley India Pvt. Ltd. (First Edition, 2011) 3
3. Security in the Digital Age: Social Media Security Threats and Vulnerabilities by Henry A. Oliver, Create Space Independent Publishing Platform. (Pearson , 13th November, 2001)
4. Electronic Commerce by Elias M. Awad, Prentice Hall of India Pvt Ltd.
5. Cyber Laws: Intellectual Property & E-Commerce Security by Kumar K, Dominant Publishers.
6. Network Security Bible, Eric Cole, Ronald Krutz, James W. Conley, 2nd Edition, Wiley India Pvt. Ltd. 7. Fundamentals of Network Security by E. Maiwald, McGraw Hill.

SEMESTER-IV
COURSE 2 : INTRODUCTION TO CYBER SECURITY LAB

Practical

Credits: 2

2 hrs/week

List of Experiments:

1. VM Ware installations
2. Configuring security settings in Mobile Wallets and UPIs
3. Applying patches, fixing vulnerability (experiments)
4. Setting, configuring and managing three password policy in the computer (BIOS, Administrator and Standard User).
5. Setting and configuring two factor authentication in the Mobile phone.
6. Security patch management and updates in Computer and Mobiles.
7. Managing Application permissions in Mobile phone.
8. Installation and configuration of computer Anti-virus.
9. Installation and configuration of Computer Host Firewall.
10. Wi-Fi security management in computer and mobile.
11. Basic checklist, privacy and security settings for popular social media platforms.
12. Reporting and redressal mechanism for violations and misuse of social media platforms.
13. Windows memory acquisition using Dumpit Tool.

SEMESTER-V

COURSE 3: INFORMATION SECURITY

Theory

Credits: 3

3 hrs/week

UNIT I: Introduction to Information Security - Information Security concepts, CIA Triad, Information Assets, Threats, Vulnerabilities, Risk Assessment, Security Policies, ISO/IEC 27001 overview.

UNIT II: Access Control and Authentication

Identification, Authentication, Authorization, Access Control Models, Password Security, Multi-Factor Authentication (MFA), Biometrics.

UNIT III: Security Operations Center (SOC)

Introduction to SOC, Purpose and Importance, SOC Architecture, SOC Team Roles (L1, L2, L3 Analysts, Incident Responder, Threat Hunter, SOC Manager), Security Monitoring, Log Management, SIEM Basics, Threat Intelligence, Indicators of Compromise (IoCs), Alert Triage, Incident Detection, Security Reporting, Career Opportunities.

UNIT IV: Network and Web Security

Firewalls, IDS, IPS, VPN, HTTPS, Email Security, Wireless Security, Malware Protection, Secure Web Practices.

UNIT V: Incident Response and Security Management

Incident Response Lifecycle, Business Continuity, Disaster Recovery, Security Auditing, Digital Evidence, Cyber Laws, Future Trends in Information Security.

Textbooks:

1. Michael E. Whitman & Herbert J. Mattord - Principles of Information Security
2. Charles P. Pfleeger - Security in Computing
3. Nina Godbole & Sunit Belapure - Cyber Security
4. Chris Sanders - Blue Team Field Manual (Reference)

EC-Council - Certified SOC Analyst (CSA) Study Guide (Reference)

SEMESTER-V

COURSE 3: INFORMATION SECURITY

Practical

Credits: 2

2 hrs/week

List of Experiments:

1. Configure user accounts and password policies
2. Analyze Windows Event Viewer logs.
3. Explore Linux log files.
4. Perform basic network traffic analysis using Wireshark.
5. Study SIEM dashboards (demo)
6. Identify Indicators of Compromise (IoCs)
7. Prepare a basic incident response report
8. Configure Windows Firewall and review security events

SEMESTER-V

COURSE 4: CRYPTOGRAPHY

Theory

Credits: 3

3 hrs/week

UNIT I: Fundamentals of Cryptography

Introduction to Cryptography • Introduction to Cryptography • Need for Cryptography • History of Cryptography • Plaintext and Ciphertext • Encryption • Decryption • Cryptographic Goals: Confidentiality, Integrity, Authentication, Non-Repudiation

UNIT II: Classical Cryptographic Techniques

Classical Cryptography • Caesar Cipher • Monoalphabetic Cipher • Playfair Cipher • Vigenere Cipher • Rail Fence Cipher • Transposition Cipher

UNIT III: Modern Cryptographic Algorithms

Modern Cryptography • Symmetric Key Cryptography • Asymmetric Key Cryptography • AES (Introduction) • DES (Introduction) • RSA (Introduction) • Key Management

UNIT IV: Hashing and Authentication

Hashing and Authentication • Hash Functions • MD5 • SHA Family • Message Authentication Codes (MAC) • Digital Signatures • Digital Certificates • Public Key Infrastructure (PKI)

UNIT V: Secure Communication and Applications

Secure Communication • SSL/TLS • HTTPS • VPN • Email Security • Secure File Transfer • Applications of Cryptography • Future Trends in Cryptography

TEXT BOOK:

1. **William Stallings** – *Cryptography and Network Security: Principles and Practice*, 8th Edition, Pearson.
2. **Behrouz A. Forouzan** – *Cryptography and Network Security*, McGraw Hill Education.

SEMESTER-V

COURSE 4: CRYPTOGRAPHY

Practical

Credits: 2

2 hrs/week

Details of Lab/Practical/Experiments/Tutorials syllabus:

1. Demonstrate plaintext, ciphertext, encryption
2. Demonstrate Decryption concepts.
3. Implement Caesar, Playfair
4. Implement Vigenere ciphers.
5. Demonstrate AES encryption
6. Generate RSA public/private keys.
7. Generate SHA-256 hashes, verify file integrity and demonstrate digital signatures.
8. Examine SSL/TLS certificates, verify HTTPS communication and develop a simple file encryption/decryption mini project.

COURSE 5: ETHICAL HACKING

Theory

Credits: 3

3 hrs/week

UNIT I: Fundamentals of Ethical Hacking

Introduction to Ethical Hacking • Introduction to Ethical Hacking • Information Gathering • Types of Hackers (White Hat, Black Hat, Grey Hat) • Ethical Hacking Methodology • Legal and Ethical Considerations • Cyber Security Standards and Best Practices

UNIT II: Footprinting and Reconnaissance

Footprinting and Scanning • Footprinting • Reconnaissance • Open Source Intelligence (OSINT) • Network Scanning • Port Scanning • Service Identification • Banner Grabbing (Introduction)

UNIT III: Vulnerability Assessment

Vulnerability Assessment • Vulnerability, Threat, and Risk • Vulnerability Assessment Process • Security Misconfigurations • Introduction to CVE and CVSS • Basic Security Auditing

UNIT IV: Ethical Hacking Tools

Security Tools • Kali Linux Overview • Nmap • Wireshark • Burp Suite Community Edition • Nikto (Introduction) • OWASP ZAP (Introduction)

UNIT V: Penetration Testing and Reporting

Reporting and Defensive Practices • Penetration Testing Life Cycle • Documentation and Report Writing • Responsible Disclosure • Security Recommendations • Cyber Hygiene • Case Studies of Cyber Incidents

TEXT BOOKS:

1. **Georgia Weidman** – *Penetration Testing: A Hands-On Introduction to Hacking*, No Starch Press.
2. **Michael T. Simpson & Scott T. Hoffman** – *Hands-On Ethical Hacking and Network Defense*, Cengage Learning.

COURSE 5: ETHICAL HACKING

Practical

Credits: 2

2 hrs/week

Experiments List

1. Install and Explore Kali Linux
2. Basic Network Scanning Using Nmap
3. Network Traffic Analysis Using Wireshark
4. Vulnerability Scanning Using OWASP ZAP (or Nikto)
5. Prepare a Basic Security Assessment Report

SEMESTER-VI

COURSE 6: DIGITAL FORENSICS

Theory

Credits: 3

3 hrs/week

UNIT I: Computer Forensics and Investigations

Computer Forensics and Investigations Computer Forensics: Introduction, Investigation Process, Systematic Approach. Data Recovery Workstations and Software. Investigator's Office and Laboratory: Forensics Lab Certification Requirements, Physical Requirements for a Computer Forensics Lab, Basic Forensic Workstation.

UNIT II: Data Acquisition

Data Acquisition Storage Formats for Digital Evidence, Acquisition Methods, Contingency Planning for Image Acquisitions, Validating Data Acquisition, RAID Data Acquisition, Acquisition Tools, Remote Network Acquisition Tools.

UNIT III : Digital Evidence Collection and Processing

Identifying, Processing Crime and Incident Scenes Digital Evidence: Search, Collection, Preparation, Isolation, Storage, Process, Verification, Documentation, Report, Archiving. Computer Forensics Tools: Evaluating Needs, Hardware & Software Tools.

UNIT IV: Forensic Analysis and Validation

Validating and Testing Forensics Forensic Analysis of Software and Validation: Data Analysis, Hiding techniques, Carving, Compression; Graphics file: Recognition, Location, Recovery, Live Memory Forensics (RAM)

UNIT V: Email Forensics and Investigation

Introduction to Email Investigation E-mail Investigations, Role of E- mail in Investigations, Role of Client and Server in E-mail, Email Crimes and Violations, E-mail Servers, Special E-mail Forensics Tools.

TEXT BOOK:

1. **Bill Nelson, Amelia Phillips & Christopher Steuart** – *Guide to Computer Forensics and Investigations*, 6th Edition, Cengage Learning.
1. **EC-Council** – *Computer Forensics: Investigating Network Intrusions and Cyber Crime*, Cengage Learning.

COURSE 6: DIGITAL FORENSICS

Practical

Credits: 2

2 hrs/week

List of Experiments

1. Disk Imaging (2 types)
2. FTK Imager
3. Cyber check suite and other forensic tools from CDAC
4. Forensic Imaging of Virtual Machines
5. Live Acquisition
6. Live Incident Response
7. Live Memory Forensics (Volatility framework)
8. Scalpel, Autopsy
9. Network Minor
10. Comparison of various software.

KRISHNA UNIVERSITY

B.SC Examinations Model Paper for Core Subjects

Semester : III

Paper Title : Computer Network and Security

Time: 3 Hours

Max. Marks: 70

Section – A (20 Marks)

Answer any FIVE questions. All questions carry equal marks.

5 × 4 = 20M

1. Define Hub, Router .
2. what are the advantages of networking.
3. Explain **MAC Address** with an example
4. What is encryption?
5. What is a **Subnet Mask**?
6. Define **HTTP**.
7. What is a **Firewall**
8. importance of **Antivirus Software**

Section – B (50 Marks)

Answer ALL questions. All questions carry equal marks.

5 × 10 = 50M

9. a) Define network. Explain types of networks .

b) Define topology. Explain different types of topologies with neat diagrams
10. a) Discuss about OSI Reference Model.

OR

- b) Explain the TCP/IP model and its layers.
- 11 . a) Explain **IPv4 addressing** in detail with suitable examples.

OR

- b) Explain **DNS** and describe how domain name resolution works. .

12 . a) Explain **FTP and SFTP** and differentiate between them.

OR

b) Explain **VPN**, its working and applications.

13. . a) Define **Network Security** and explain its importance.

OR

b) Discuss about **Network Troubleshooting**?

KRISHNA UNIVERSITY

B.SC Examinations Model Paper for Core Subjects

Semester : IV

Paper Title : Introduction to Cyber Security

Time: 3 Hours

Max. Marks: 70

Section – A (20 Marks)

Answer any FIVE questions. All questions carry equal marks

. 5 × 4 = 20M

1. Define WWW.
2. Define Cyber Crime
3. What is Phishing?
4. What is the CIA Triad?
5. What are Access Laws?
6. Explain about pitfalls
7. Explain components of E-Commerce.
8. What are e-Wallets

Section – B (50 Marks)

Answer ALL questions. All questions carry equal marks.

5 × 10 = 50M

9. a) Discuss Architecture, characteristics of CyberSpace.

OR

- b) Discuss the importance of Internet governance and regulation

10. a) Discuss about Cyber Threats.

OR

- b) Explain viruses.

11. a) Explain Need and Importance of Cyber Security.

OR

- b) Explain the principle of availability and its methods

12. a) Explain Social Media networks.

OR

b) Discuss the laws regarding posting inappropriate content on social media.

13. a) Explain digital payments and their major components.

OR

b) Explain the Payment and Settlement Systems Act, 2007 and its importance.

KRISHNA UNIVERSITY

B.SC Examinations Model Paper for Core Subjects

Semester : V

Paper Title : Information Security

Time: 3 Hours

Max. Marks: 70

Section – A (20 Marks)

Answer any FIVE questions. All questions carry equal marks.

5 × 4 = 20M

1. Define Information Security
2. what is Risk Assessment
3. What is Biometric Authentication
4. What is a SIEM?
5. Email Security
6. Define Incident Response.
7. What is IDS?
8. Differentiate between HTTP and HTTPS.

Section – B (50 Marks)

Answer ALL questions. All questions carry equal marks.

5 × 10 = 50M

9. a) Explain **ISO/IEC 27001** and its role.

OR

- b) Discuss about Information Security concepts.

10. a) Explain Access Control Models.

OR

- b) Explain about Authentications.

11. a) Explain SOC Architecture with example.

OR

- b) Explain the career opportunities and skills required for working in a **Security Operations Center**.

12. a) Explain **Wireless Network Security** and the measures

OR

b) Discuss different types of malwares.

13. a) Explain Cyber Laws.

OR

b) Explain Disaster Recovery management.

KRISHNA UNIVERSITY

B.SC Examinations Model Paper for Core Subjects

Semester : V

Paper Title : Cryptography

Time: 3 Hours

Max. Marks: 70

Section – A (20 Marks)

Answer any FIVE questions. All questions carry equal marks.

$5 \times 4 = 20M$

- 1. Define Cryptography.**
- 2. History of Cryptography**
- 3. Define Caesar Cipher**
- 4. Define Transposition Cipher**
- 5. Explain RSA?**
- 6. Define Digital Signature**
- 7. Define SSL**
- 8. Define Public Key Infrastructure**

Section B

Answer the following questions

$5 * 10 = 50 M$

- 9. Explain about need for Cryptography**
(or)
- 10. Explain about Encryption and Decryption**
- 11. Explain about Monoalphabetic Cipher , Playfair Cipher**
(or)
- 12. Explain about Rail Fence Cipher & Transposition Cipher**
- 13. Explain about Symmetric Key Cryptography & Asymmetric Key Cryptography**
(or)
- 14. Explain about AES & DES**
- 15. Write about Hash functions with examples**
(or)
- 16. Explain about Message Authentication Codes (MAC)**
- 17. Explain about E-mail security**
(or)
- 18. Explain about future trends in Cryptography**

KRISHNA UNIVERSITY

B.SC Examinations Model Paper for Core Subjects

Semester : VI

Paper Title : ETHICAL HACKING

Time: 3 Hours

Max. Marks: 70

Section – A (20 Marks)

Answer any FIVE questions. All questions carry equal marks.

5 × 4 = 20M

- 1) Define Ethical Hacking
- 2) Write about types of Hackers
- 3) Define foot printing
- 4) Define Port scanning
- 5) Define security auditing
- 6) Define Nmap
- 7) Explain SPZAP
- 8) Define Cyber Hygiene

Section B

Answer the following questions

5 * 10 = 50 M

- 9 a). Explain about Ethical Hacking Methodology
OR
b). Explain about Legal and Ethical Considerations
- 10 a) .Explain about Open Source Intelligence (OSIN)
OR
b). Explain about Reconnaissance
- 11 a) Explain about Vulnerability Assessment
OR
b) Explain about Vulnerability Assessment Process
- 12 a) Explain about various security tools
OR

b) . Explain about Nikto

13 a) . Explain about Penetration Testing Life Cycle

OR

b) Explain about Security Recommendation

KRISHNA UNIVERSITY

B.SC Examinations Model Paper for Core Subjects

Semester : VI

Paper Title : Digital Forensics

Time: 3 Hours

Max. Marks: 70

Section –A (20 Marks)

Answer any Five questions. All questions carry equal marks.

5X4=20M

1. List the steps involved in an investigation process.
2. Define RAID.
3. What is documentation in evidence processing?
4. What are the common storage formats for digital evidence?
5. What is meant by isolation of evidence?
6. Name any two data hiding techniques
7. What is the role of an email server?
8. Define email forensics.

Section–B (50Marks)

Answer ALL Questions. All questions carry equal marks.

5 X 10 = 50M

9. a) Explain the systematic approach to computer forensics investigations.

OR

- b) Discuss the physical requirements for setting up a computer forensics lab

10. a) Explain the process of validating data acquisition.

OR

- b) Explain the different storage formats used for digital evidence.

11. a) Explain the steps involved in identifying and processing a crime scene

OR

- b) Explain the hardware and software tools used in computer forensics

12. a), Explain the concept of data carving and compression in forensic analysis

OR

b) Explain the recognition, location and recovery of graphics files

13. a) Explain the role of email in investigations with the email investigation process.

OR

b) Discuss the various email crimes and violations.

