

# Bharati Vidyapeeth Institute of Technology, Navi Mumbai

## Question Bank (K – Scheme)

### Unit Test-II

Program: - CM/IF6K

Semester: - IV

Course and code: - Emerging Trends in Computer Engineering and Information Technology (316313)

---

## Chapter 3 – Blockchain Technology

---

### (E) Blockchain Applications

1. Which industry uses blockchain for secure cross-border payments?

- (a) Healthcare (b) Finance (c) Supply Chain (d) Gaming

2. Blockchain improves supply chains by .....

- (a) Reducing transparency  
(b) Tracking products from origin to consumer  
(c) Hiding product details  
(d) Increasing fraud risk

3. In healthcare, blockchain helps by .....

- (a) Making all patient data public  
(b) Securely storing and sharing medical records  
(c) Slowing down data access  
(d) Reducing data collection

4. Blockchain offers gamers the ability to .....

- (a) Own in-game assets as NFTs  
(b) Cheat on games  
(c) Avoid transparency  
(d) Use centralized servers

5. Cross-border payments on blockchain are .....

- (a) Slow and costly  
(b) Faster and cheaper due to lack of intermediaries  
(c) Only for cryptocurrency  
(d) Not traceable

6. Which of the following Industry can use blockchain Technology?

- (a) Logistics and supply chain (b) Medical records (c) Financial Market (d) All of these

7. In supply chain applications, blockchain primarily helps by

- a) Reducing transparency  
b) Tracking products and ensuring authenticity  
c) Replacing sensors  
d) Removing cloud computing

8. A hospital wants to securely share patient records across multiple clinics while maintaining privacy. Which type of blockchain is most suitable?

- (a) Public Blockchain (b) Private Blockchain (c) Consortium Blockchain (d) Hybrid Blockchain

9. A gaming company wants to give players ownership of in-game assets through blockchain tokens that are tradable across platforms. Which application of blockchain does this represent?  
(a) Finance (b) Healthcare (c) **Gaming (NFTs / Digital Assets)** (d) Supply Chain
- 

**(F) Smart Contracts and Cryptocurrencies**

10. A smart contract is used to automatically release payment when goods are delivered in a supply chain. Which blockchain feature makes this possible?  
(a) Decentralization (b) Transparency (c) **Immutability and automation** (d) Cryptocurrency mining
11. Smart contracts \_\_\_\_\_  
(a) Require a lawyer to enforce  
(b) **Are self-executing contracts coded on blockchain**  
(c) Can be changed anytime by the creator  
(d) Need intermediaries
12. Which is a key feature of smart contracts?  
(a) **Autonomy and immutability**  
(b) Manual execution  
(c) Require human intervention  
(d) Can be erased easily
13. Bitcoin is .....  
(a) A centralized digital currency  
(b) **A cryptocurrency operating on blockchain**  
(c) A fiat currency  
(d) Not related to blockchain
14. Ethereum is known for .....  
(a) Only cryptocurrency transactions  
(b) **Enabling smart contract execution**  
(c) Being a private blockchain  
(d) Centralized control
15. Bitcoin and Ethereum are examples of:  
(a) Private Blockchains (b) **Public Blockchains** (c) Consortium Blockchains (d) Hybrid Blockchains
16. Bitcoin and Ethereum are examples of ?  
(a) Currency (b) **Cryptocurrency** (c) Cryptography (d) Algorithm
17. Which of the following is a popular cryptocurrency?  
(a) **Ethereum** (b) MySQL (c) Python (d) Hyperledger
18. Which blockchain is known for pioneering smart contracts?  
(a) Bitcoin (b) **Ethereum** (c) Litecoin (d) Dogecoin
19. A smart contract is  
(a) A physical contract stored digitally  
(b) **A self-executing program with the terms of the agreement coded**  
(c) A blockchain token  
(d) A database management system

20. "Smart contracts" are based on .....

- (a) "if/when...then" logic
  - (b) Manual approval process
  - (c) Paper documentation
  - (d) Third-party arbitration
- 

### (G) Blockchain Challenges

21. The biggest scalability challenge is .....

- (a) Slow transactions as network grows
- (b) Too much transparency
- (c) Lack of security
- (d) Too many users

22. Proof of Work consensus consumes .....

- (a) Minimal energy
- (b) High energy due to mining computations
- (c) No electricity
- (d) Renewable resources only

23. Regulatory uncertainty .....

- (a) Encourages rapid adoption
- (b) Hinders blockchain adoption globally
- (c) Is resolved everywhere
- (d) Does not affect blockchain

24. What is a "51% attack"?

- (a) When a single user controls over half of all mining power
- (b) More than half network uses blockchain
- (c) Over half transactions are instant
- (d) None of the above

25. Immutability challenges include .....

- (a) Inability to correct errors once stored
- (b) Data easily altered
- (c) Data deleted automatically
- (d) Frequent rollbacks

26. A privacy issue in public blockchains is .....

- (a) Complete anonymity
- (b) Exposure of transaction details publicly
- (c) Data encryption
- (d) Transparency for trusted users only

27. Which blockchain challenge is associated with high energy consumption due to mining?

- (a) Scalability (b) Security (c) Efficiency (d) Decentralization
- 

### (H) Additional Questions

28. What is tokenization in blockchain?

- (a) Converting assets into digital tokens for easier transfer
- (b) Hiding asset identity
- (c) Destroying digital records
- (d) Encrypting personal data only

**29. Which blockchain consensus reduces energy consumption compared to Proof of Work?**

- (a) **Proof of Stake**
- (b) Proof of Authority
- (c) Proof of Identity
- (d) Proof of Power

**30. Gas fees in Ethereum are used to .....**

- (a) **Pay transaction processing on blockchain**
- (b) Control user access
- (c) Reward users with tokens
- (d) None of the above

**31. Which layer of blockchain architecture is responsible for validating and recording transactions?**

- (a) Data Layer (b) Network Layer (c) **Consensus Layer** (d) Application Layer

**32. What is a dApp ?**

- (a) Type of Blockchain (b) A type of Cryptocurrency (c) **A decentralized Application** (d) Smart Contract

**33. How many layers are there in Blockchain architecture?**

- (a) 3 (b) 4 (c) **5** (d) 7

**34. Blockchain 2.0 is born in the year?**

- (a) 2009 (b) **2014** (c) 2017 (d) 2018

**35. \_\_\_\_\_ is used in peer to peer communications between the nodes that allow them to discover each other and get synchronized with another node.?**

- (a) Presentation Layer
- (b) Application Layer
- (c) **Propagation Layer**
- (d) Semantic Layer

---

## **Chapter 4 – Immersive Technology and Sustainable Computing**

---

### **(A) Immersive Technology**

#### **1. Immersive technology merges:**

- (a) **Hardware and software**
- (b) Physical and digital environments
- (c) Data and storage
- (d) Networks

#### **2. Main purpose of immersive technology is to:**

- (a) Replace physical systems
- (b) **Enhance user experience through engagement**
- (c) Reduce computer speed
- (d) Store more data

**3. Which technology completely replaces the real world with a simulated one?**

- (a) AR
- (b) VR**
- (c) MR
- (d) XR

**4. The device Essential for VR experience:**

- (a) Monitor
- (b) VR headset**
- (c) Smartphone
- (d) Keyboard

**5. Augmented Reality works by:**

- (a) Simulating only virtual worlds
- (b) Overlaying digital objects on real world**
- (c) Creating Sound-based simulations
- (d) Replacing human senses

**6. Mixed Reality (MR) is a combination of:**

- (a) AR and AI
- (b) VR and IoT
- (c) AR and VR**
- (d) None of these

**7. The term XR (Extended Reality) refers to:**

- (a) Only VR applications
- (b) Combination of VR, AR, MR**
- (c) Only AR applications
- (d) Gaming technology

**8. Haptic technology mainly stimulates which human sense:**

- (a) Hearing
- (b) Touch**
- (c) Vision
- (d) Smell

**9. A common example of AR in daily life is:**

- (a) Google Docs
- (b) Pokémon GO**
- (c) YouTube
- (d) PowerPoint

**10. Which Immersive technology allows users to interact with both real & digital objects in real time:**

- (a) AR
- (b) MR**
- (c) VR
- (d) XR

**11. The sense of "presence" in immersive technology means:**

- (a) The user is physically moving
- (b) The user feels part of the virtual world**
- (c) The user's device is on
- (d) None of these

**12. Which of the following is a wearable haptic device:**

- (a) VR headset
- (b) VR gloves**
- (c) Keyboard
- (d) Joystick

**13. Touchable haptics are commonly used in**

- (a) Smartphones and tablets**
- (b) Servers
- (c) VR helmets
- (d) Data centers

**14. Mid-air haptics deliver sensations using :**

- (a) Electricity
- (b) Ultrasound waves**
- (c) Heat sensors
- (d) Vibrations only

**15. Which immersive technology is most used for training pilots:**

- (a) AR
- (b) VR**
- (c) MR
- (d) XR

**16. Which technology provides 3D visual overlays on physical spaces:**

- (a) MR**
- (b) AR
- (c) VR
- (d) Haptic

**17. XR is best described as .....**

- (a) Software simulation
- (b) The umbrella term for AR, VR, MR**
- (c) Quantum device
- (d) Mechanical design tool

**18. Which industry was among the first to adopt immersive technology widely?**

- (a) Education
- (b) Gaming**
- (c) Manufacturing
- (d) Agriculture

**19. Immersive technologies engage which senses?**

- (a) **Sight and sound**
- (b) Taste and smell
- (c) Balance and touch
- (d) None

**20. Microsoft HoloLens is an example of .....**

- (a) VR device
  - (b) **MR device**
  - (c) AR device
  - (d) XR headset
- 

**(B)Applications of Immersive Technology**

**21. In education, immersive technology helps by .....**

- (a) Creating physical textbooks
- (b) **Enabling virtual field trips**
- (c) Replacing teachers
- (d) Reducing school hours

**22. Medical students use VR to .....**

- (a) Play games
- (b) **Practice surgery in virtual environments**
- (c) Write reports
- (d) Scan patient IDs

**23. AR can assist engineers by .....**

- (a) Reducing machine cost
- (b) **Overlaying design elements on real components**
- (c) Replacing hardware
- (d) Printing 3D models

**24. In real estate, VR enables .....**

- (a) Cost estimation
- (b) **Remote property tours**
- (c) Document management
- (d) Security scanning

**25. AR marketing helps customers by .....**

- (a) Displaying product manuals
- (b) **Trying products virtually**
- (c) Increasing advertisements
- (d) None

**26. In tourism, immersive technology offers .....**

- (a) **Virtual previews of destinations**
- (b) Flight discounts
- (c) Paper tickets
- (d) Booking apps only

**27. The military uses VR and AR to .....**

- (a) Entertain troops
- (b) Conduct safe training simulations**
- (c) Build bases
- (d) None

**28. Healthcare uses VR for .....**

- (a) Music therapy
- (b) Pain management and mental health**
- (c) Billing
- (d) Insurance claims

**29. In architecture, immersive technology allows .....**

- (a) Viewing 3D models before construction**
- (b) Enhancing paper drawings
- (c) Speeding up cement drying
- (d) Painting walls

**30. AR glasses are used for .....**

- (a) Showing digital info in real-world view**
- (b) Listening to audio
- (c) Printing photos
- (d) Transferring files

---

**(C) Green Computing**

**31. Green computing promotes:**

- (a) Energy conservation**
- (b) Faster processors
- (c) Bigger servers
- (d) More power usage

**32. Green IT mainly focuses on:**

- (a) Recycling and reducing e-waste**
- (b) Expensive chips
- (c) Cloud gaming
- (d) Crypto mining

**33. Energy-efficient hardware helps by:**

- (a) Increasing electricity cost
- (b) Reducing power consumption**
- (c) Producing more heat
- (d) degrading performance

**34. Which of the following is a feature of Green Computing?**

- (a) High carbon footprint
- (b) Use of renewable energy in data centers**
- (c) Increasing e-waste
- (d) Faster clock speeds in processors

**35. Data centers improve cooling efficiency using .....**

- (a) **Hot aisle / cold aisle layout**
- (b) Random arrangement
- (c) Closed chambers
- (d) Heating ducts

**36. Liquid cooling in data centers is used for .....**

- (a) **Better heat transfer**
- (b) Soundproofing
- (c) Data encryption
- (d) Visual enhancement

**37. Virtualization helps green computing by .....**

- (a) **Reducing physical servers**
- (b) Increasing storage devices
- (c) Running fewer applications
- (d) Wasting resources

**38. Green computing is also called .....**

- (a) Cloud IT
- (b) **Green IT**
- (c) Smart IT
- (d) Energy IT

**39. Which of these is a benefit of green computing?**

- (a) **Cost savings**
- (b) High temperature
- (c) More pollution
- (d) Data loss

**40. A paperless office contributes to .....**

- (a) Waste generation
- (b) **Green computing**
- (c) Carbon increase
- (d) None

---

**(D) E-Waste Management and Recycling**

**41. The first stage in e-waste management is .....**

- (a) Sorting
- (b) **Collection**
- (c) Dismantling
- (d) Recycling

**42. Data destruction ensures .....**

- (a) File recovery
- (b) **Information security**
- (c) Power efficiency
- (d) Free software

**43. Shredding is done to .....**

- (a) Mix components
- (b) Break down parts for sorting**
- (c) Repair devices
- (d) None

**44. Magnetic separation removes .....**

- (a) Plastic
- (b) Steel and iron**
- (c) Copper
- (d) Glass

**45. Eddy current separation targets .....**

- (a) Non-ferrous metals**
- (b) Glass
- (c) Wood
- (d) Paper

**46. Water separation helps in separating .....**

- (a) Glass and plastics**
- (b) Metals
- (c) Chemicals
- (d) All materials

**47. Material recovery extracts .....**

- (a) Gold, copper, silver**
- (b) Plastic, paper, wood
- (c) Lead, mercury
- (d) Glass only

**48. Hazardous waste includes .....**

- (a) Plastic
- (b) Lead, mercury, cadmium**
- (c) Paper
- (d) Aluminum

**49. The purpose of e-waste recycling is to .....**

- (a) Produce more e-waste
- (b) Reduce environmental impact**
- (c) Generate new waste
- (d) Discard all materials

**50. Recovered materials are used to .....**

- (a) Create new electronic products**
  - (b) Build buildings
  - (c) Produce paper
  - (d) Make fuel
-

**(E)Quantum Computing**

**51. Quantum computing is based on .....**

- (a) **Quantum mechanics**
- (b) Classical physics
- (c) Thermodynamics
- (d) Nanotechnology

**52. The basic unit of quantum information is .....**

- (a) Bit
- (b) Byte
- (c) **Qubit**
- (d) Node

**53. Superposition allows a qubit to be .....**

- (a) 0 or 1
- (b) **0 and 1 simultaneously**
- (c) 2 only
- (d) None

**54. Entanglement means .....**

- (a) **Two qubits interact instantly**
- (b) Qubits separate
- (c) Bits collide
- (d) Data loss

**55. Quantum interference helps .....**

- (a) **Eliminate wrong solutions**
- (b) Store memory
- (c) Increase heat
- (d) Encrypt data

**56. Classical computers use .....**

- (a) Qubits
- (b) **Bits**
- (c) Gates only
- (d) Photons

**57. Quantum computers can solve problems .....**

- (a) Sequentially
- (b) **In parallel**
- (c) Randomly
- (d) Slowly

**58. Example of a quantum computer .....**

- (a) **IBM Quantum**
- (b) Dell Laptop
- (c) Raspberry Pi
- (d) Chromebook

**59. Quantum computing helps in .....**

- (a) **Drug discovery**
- (b) Game design
- (c) Web hosting
- (d) UI design

**60. Quantum Key Distribution (QKD) is used in .....**

- (a) **Cryptography**
- (b) AI
- (c) Robotics
- (d) Machine learning

**61. Google's quantum computer is called .....**

- (a) Titan
- (b) **Sycamore**
- (c) QuantumX
- (d) DeepMind

**62. Quantum computers process information using .....**

- (a) Classical gates
- (b) **Quantum gates**
- (c) Optical drives
- (d) CPUs

**63. Quantum computing benefits which field most?**

- (a) **Optimization**
- (b) Animation
- (c) Gaming
- (d) Cloud hosting

**64. Quantum computing is still in .....**

- (a) **Early development stage**
- (b) Full production
- (c) Decline
- (d) Decommissioning

**65. A key difference between classical and quantum computing is .....**

- (a) Speed of data transfer
- (b) **Representation of data (bits vs qubits)**
- (c) Screen resolution
- (d) Hardware design

**66. In quantum computing, probability is used for .....**

- (a) **Observing results**
- (b) Compressing data
- (c) Encrypting data
- (d) Deleting files

**67. Quantum algorithms are faster for .....**

- (a) Sorting
- (b) Factoring large numbers**
- (c) Simple addition
- (d) Text processing

**68. Which principle allows linked qubits to share information instantly?**

- (a) Superposition
- (b) Entanglement**
- (c) Holography
- (d) Refraction

**69. Which area can quantum computing revolutionize?**

- (a) Cybersecurity**
- (b) Photography
- (c) Social media
- (d) Printing

**70. The main challenge in building quantum computers is .....**

- (a) Data storage
- (b) Qubit stability and error correction**
- (c) Color display
- (d) User interface

---

**(F) Additional Questions**

**71. How does AR differ from VR?**

- (a) AR fully replaces the real world; VR only enhances it
- (b) AR enhances the real world with digital overlays, VR replaces the real world**
- (c) AR and VR are the same in terms of immersion
- (d) AR requires haptic suits while VR does not

**72. Why Mixed Reality (MR) is considered more advanced than AR?**

- (a) MR only works on smartphones
- (b) MR allows digital and physical objects to interact in real-time**
- (c) MR completely ignores the real environment
- (d) MR is only used in gaming

**73. Which application of immersive technology is best explained by “IKEA’s AR app to visualize furniture”?**

- (a) Tourism
- (b) Retail & E-commerce**
- (c) Entertainment
- (d) Healthcare

**74. Which of the following best explains server virtualization in Green Computing?**

- (a) Increasing the number of servers to balance workload
- (b) Using one physical server to host multiple virtual machines**
- (c) Reducing server speed to save energy

(d) Recycling old servers into new ones.

**75. Why is quantum superposition powerful?**

- (a) It reduces memory usage in computers
- (b) It allows a qubit to exist in multiple states at once**
- (c) It eliminates the need for quantum gates
- (d) It increases processor clock speeds

**76. A medical student practices surgery using a VR simulator before treating a real patient. This is an example of:**

- (a) Entertainment application of VR
- (b) Education & Training application of VR**
- (c) AR in healthcare
- (d) Haptic feedback technology

**77. A soldier trains in a VR battlefield before deployment. Which immersive technology application does this represent?**

- (a) Healthcare
- (b) Tourism
- (c) Defense & Military**
- (d) Sports & Fitness

**78. A smartphone provides vibration feedback when pressing a touchscreen button. This is an example of:**

- (a) Augmented Reality
- (b) Extended Reality
- (c) Haptic Technology**
- (d) Quantum Interference

**79. A data center reduces cooling costs by using free air cooling and liquid cooling. This demonstrates:**

- (a) Quantum computing optimization
- (b) E-waste management
- (c) Green Data Center Practices**
- (d) Mixed Reality in Industry

**80. A company wants to simulate new drug molecules to accelerate vaccine development. Which technology is most suitable?**

- (a) Virtual Reality
  - (b) Quantum Computing**
  - (c) Green Computing
  - (d) Mixed Reality
-

---

## Chapter 5 – Digital Forensics & Ethical Hacking

---

### (A) Digital Forensics

1. Digital Forensics is primarily concerned with .....

- (a) building computer systems
- (b) Preservation, identification, extraction, and documentation of computer evidence**
- (c) software development
- (d) network installation

2. ....is a branch of forensic science encompassing the recovery and investigation of material found in digital devices.

- (a) Analog forensic
- (b) Digital forensic**
- (c) Cyber forensic
- (d) Computer forensic

3. Digital forensics helps in .....

- (e) Breaking software licenses
- (f) Estimating potential impact of malicious activity**
- (g) Upgrading hardware
- (h) Designing new programming languages

4. Major goal of Digital Forensics is \_\_\_?

- (a) To duplicate original data and preserve original evidence.
- (b) Validation of digital information
- (c) Collection of digital evidence
- (d) All of above**

5. Which of the following is an objective of digital forensics?

- (a) Design UI for software
- (b) Recover, analyze, and preserve computer materials for legal proceedings**
- (c) Develop malware
- (d) Install operating systems

6. Investigator should follow following rule/rules?

- (a) Computer and data on it must be protected during acquisition of the media.
- (b) An examination should never be performed on the original media.
- (c) Both A & B**
- (d) A is true B is False

7. Which of the following is a core rule of digital forensics?

- (a) Work directly on the original evidence
- (b) Maintain integrity and create a forensically sound copy**
- (c) Ignore documentation
- (d) Skip chain of custody

**8. Forensic duplication is necessary because:**

- (a) To save storage space
- (b) To preserve the original evidence while performing analysis**
- (c) To speed up software installation
- (d) To format drives

**9. Which tool is widely used for forensic imaging?**

- (a) Wireshark
- (b) Encase**
- (c) MS-Excel
- (d) Notepad

**10. Forensic triage is performed to:**

- (a) Repair broken hardware
- (b) Quickly assess and prioritize evidence**
- (c) Encrypt files
- (d) Install antivirus software

**11. Metadata in digital evidence includes:**

- (a) Data about data (Creation time, author, last modified )**
- (b) File content only
- (c) File size Only
- (d) IP addresses only

**12. Imaging a storage device ensures .....**

- (a) Deletion of all files
- (b) An exact bit-by-bit copy of data**
- (c) Faster internet speed
- (d) Encryption of files

**13. Hashing in digital forensics is used to:**

- (a) Compress data
- (b) Verify integrity of digital evidence**
- (c) Encrypt emails
- (d) Convert files to PDFs

**14. Which model is used for real-time or live forensic analysis?**

- (a) DFRWS
- (b) Live Forensic Model**
- (c) IDIP
- (d) ADFM

**15. Foot printing in ethical hacking is done to...**

- (a) Plant malware
- (b) Gather preliminary information about the target**
- (c) delete user accounts
- (d) crack passwords only

**16. Scanning in hacking helps to:**

- (a) Exploit vulnerabilities
- (b) Identify open ports, services, and weak points**

- (c) Encrypt the network
- (d) Create a backup

**17. Enumeration phase involves:**

- (a) **Listing potential targets and system details**
- (b) Installing antivirus
- (c) Performing backups
- (d) Writing reports only

**18. Post-exploitation phase is for:**

- (a) Restoring system data
- (b) **Maintaining access, covering tracks, and extracting data**
- (c) Scanning the system
- (d) Running antivirus

**19. What is the first stage in digital forensics investigation?**

- (a) Analysis
- (b) Documentation
- (c) **Identification**
- (d) Presentation

**20. Which stage involves creating a forensic image of the digital evidence?**

- (a) Identification
- (b) **Preservation / Extraction**
- (c) Documentation
- (d) Presentation

**21. Which step of digital forensics focuses on freezing the crime scene digitally?**

- (a) Analysis
- (b) **Preservation**
- (c) Documentation
- (d) Collection

**22. Why is evidence preservation important in digital forensics?**

- (a) To compress data
- (b) **To maintain its integrity for legal acceptance**
- (c) To speed up recovery
- (d) To allow duplication

**23. The “Preservation” phase in any forensic model involves:**

- (a) **Collecting evidence and maintaining chain of custody**
- (b) Writing reports only
- (c) Installing software patches
- (d) Monitoring network traffic

**24. In digital forensics, \_\_\_\_\_ values are used to ensure data integrity.**

- (a) Checksum
- (b) **Hash**
- (c) Packet
- (d) Cipher

**25. Which of the following are sources of digital evidences?**

- (a) Internet based files
- (b) Stand-alone computers or devices
- (c) Mobile devices
- (d) All of the above**

**26. During evidence handling, why is a chain of custody important?**

- (a) To reduce paperwork
- (b) To prove evidence integrity and control**
- (c) To speed up the investigation
- (d) To delete irrelevant files

**27. What is/are the procedural steps to establish chain of Custody?**

- (a) Work with original evidence
- (b) Perform a hash test analysis**
- (c) Alter the state of evidence
- (d) Declare the confidential matters

**28. Why it is important to maintain the Chain of Custody?**

- (a) To preserve the integrity of the evidence
- (b) To prevent it from contamination
- (c) To maintain the state of evidence
- (d) All of the above**

**29. Write the Correct sequence steps of procedure to establish the Chain of Custody?**

- 1. Save the original materials**
- 2. Perform a hash test analysis to further authenticate the working clone**
- 3. Take screenshot of digital evidence content**
- 4. Inject bit by bit clone of digital evidence content into our forensic computers**

- (a) Sequence of Steps 1,2,3,4
- (b) Sequence of Steps 1,3,4,2**
- (c) Sequence of steps 2,3,4,1
- (d) Sequence of steps 3,4,1,2

**30. Volatile data in digital forensics refers to .....**

- (a) Hard disk data
- (b) Data in RAM that may be lost if not captured properly**
- (c) Data stored in external drives
- (d) Encrypted data only

---

**(B) Models of Digital Forensic Investigation**

**31. The DFRWS model was proposed in .....**

- (a) 1999
- (b) 2001**
- (c) 2005
- (d) 2010

**32. The DFRWS model belongs to-**

- (a) **Digital forensic investigation**
- (b) Operating system hacking
- (c) Web application development
- (d) Network protocol testing

**33. ADFM stands for.....?**

- (a) Analog Digital Forensic Model
- (b) **Abstract Digital Forensic Model**
- (c) Abstract Discrete Forensic Model
- (d) Analog Discrete Forensic Model

**34. EMCI means.....?**

- (a) **Extended Model for Cybercrime Investigation**
- (b) Electronic Model for Cybercrime Invention
- (c) Extended Mode for Cybercrime Investigation
- (d) Emergency Model for Cybercrime Investigation

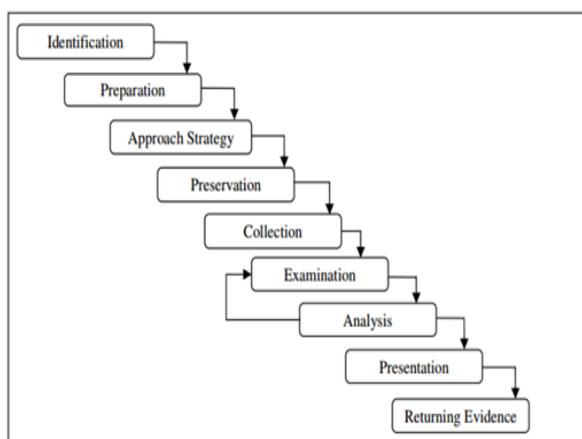
**35. UMDFPM stands for .....**

- (a) Unified Model of Digital Forensic Process
- (b) **UML Modeling of Digital Forensic Process Model**
- (c) Universal Method for Digital Police
- (d) Unified Module for Digital Protection

**36. Which model adds Preparation and Return of Evidence phases?**

- (a) DFRWS Model
- (b) **ADFM**
- (c) IDIP
- (d) EEDIP

**37. Identify Forensic Model in given fig?**



- (a) IDIP
- (b) EMCI
- (c) Waterfall
- (d) **ADFM**

**38. In ADFM, Which phase is used to provide summary and explanation of conclusion?**

- (a) Approach Strategy
- (b) Presentation**
- (c) Preservation
- (d) Analysis

**39. In ADFM model, The preparation of tools, techniques, search warrants are functions of which phase?**

- (a) Collection
- (b) Examination
- (c) Preservation
- (d) Preparation**

**40. The IDIP model integrates .....**

- (a) only digital evidence
- (b) Both digital and physical crime scene investigations**
- (c) only network attacks
- (d) only legal documentation

**41. Integrated Digital Investigation Process (IDIP) mainly focuses on-**

- (a) OS patching
- (b) Cloud backup
- (c) Data encryption
- (d) Linking physical and digital crimes**

**42. In IDIP Model, to provide mechanism to an incident to be detected and confirmed is purpose of which phase?**

- (a) Review phase
- (b) Physical crime investigation
- (c) Deployment phase**
- (d) Digital crime investigation.

**43. Which phase of IDIP model includes Detection & Notification Phase?**

- (a) Deployment Phase**
- (b) Physical Crime Investigation
- (c) Readiness
- (d) Review phase

**44. In IDIP Model, Which phase is used to put the pieces of digital puzzle together and developing investigative hypotheses.?**

- (a) Review phase
- (b) Presentation phase
- (c) Reconstruction phase**
- (d) Notification phase

**45. In IDIP, Digital crime investigation phase includes .....**

- (a) Survey phase
- (b) Documentation phase

- (c) Search and collection phase
- (d) All of above**

**46. In Digital Forensic, Planning, Transport of Evidence and Presentation of hypothesis are phases of .....model?**

- (a) ADFM
- (b) EMCI**
- (c) IDIP
- (d) None of these

**47. Hypothesis is the phase of which forensic model ?**

- (a) ADFM
- (b) EMCI**
- (c) IDIP
- (d) RoadMap

**48. Which model is suitable for multi-agency cybercrime cases requiring structured communication?**

- (a) DFRWS
- (b) Extended Model for Cybercrime Investigation**
- (c) ADFM
- (d) IDIP

**49. Which model focuses on end-to-end traceability and automated documentation?**

- (a) DFRWS Model
- (b) EEDIP**
- (c) UMDFPM
- (d) ADFM

**50. Which model emphasizes legal admissibility of evidence from start to end?**

- (a) DFRWS
- (b) ADFM
- (c) IDIP
- (d) EEDIP**

---

### **(C) Types of Hackers**

**51. Black-hat hacking is.....**

- (a) Legal tester of systems
- (b) Malicious hackers exploiting vulnerabilities for personal gain**
- (c) Students learning hacking
- (d) Cyber security officers

**52. Blue Hat hackers are usually:**

- (a) Internal corporate testers before software release**
- (b) Malicious hackers
- (c) Government hackers
- (d) Script kiddies

**53. Script kiddies are:**

- (a) Experienced hackers

- (b) **Unskilled attackers using pre-made tools.**
- (c) Government cybersecurity professionals
- (d) AI based attack tools

**54. Hacktivists are motivated by:**

- (a) Money
- (b) **Political or social causes**
- (c) Corporate espionage
- (d) Virus creation

**55. State-sponsored hackers are:**

- (a) Ethical testers
- (b) **Government-backed attackers for espionage or cyberwarfare**
- (c) Students learning hacking
- (d) Penetration testers.

**56. Which hacker type acts legally to help organizations secure systems?**

- (a) Black Hat
- (b) **White Hat**
- (c) Grey Hat
- (d) Blue Hat

**57. Which hacker type may access systems without permission but without malicious intent?**

- (a) White Hat
- (b) **Grey Hat**
- (c) Red Hat
- (d) Green Hat

**58. A hacker who identifies and exploits weaknesses in telephones instead of computers is called as.....**

- (a) White hat hacker
- (b) Black hat hacker
- (c) **Phreaker**
- (d) Hacktivist

**59. The skilled criminal experts who write some of the hacking tools, including the scripts and other programs that the script kiddies and security professionals use are known as.....**

- (a) Hacktivist
- (b) **Criminal Hackers**
- (c) Script Kiddies
- (d) Security Researchers

**60. A Red Hat Hacker is known for .....**

- (a) creating malware for profit
- (b) **Aggressively stopping black hat hackers**
- (c) learning hacking as a beginner
- (d) ethical penetration testing

---

**(D) Ethical Hacking**

**61. Ethical hacking is .....**

- (a) Illegal hacking for personal gain
- (b) Authorized testing of systems to identify vulnerabilities**
- (c) Installing malware
- (d) Ignoring security measures

**62. Ethical Hacking is.....**

- (a) Identifying weakness in computer systems and/or computer networks and coming up with counter measures that protect the weaknesses.**
- (b) Identifying weakness in programmer and coming up with counter measures that protect the weaknesses.
- (c) Identifying weakness in only software and attacking the same.
- (d) Enforcing the weakness in computer systems.

**63. Using password cracking algorithm to gain access to a system is an example of .....**

- (a) Security auditing
- (b) Ethical hacking**
- (c) System engineering
- (d) Social engineering

**64. ....is performed with the target's permission in a professional setting.**

- (a) Ethical hacking**
- (b) Social engineering
- (c) System Engineering
- (d) Software Testing

**65. Sequential steps hackers uses are: \_\_, \_\_, \_\_, \_\_**

- A. Maintaining Access**
- B. Reconnaissance**
- C. Scanning**
- D. Gaining Access**

- (a) B, C, D, A**
- (b) B, A, C, D
- (c) A, B, C, D
- (d) D, C, B, A

**66. Phases of Ethical Hacking do NOT include .....**

- (a) Reconnaissance
- (b) Scanning
- (c) System destruction**
- (d) Reporting and analysis

**67. The intent of ethical hacking is.....**

- (a) To discover the hacker who hacks the secure systems.
- (b) To promote the malicious attacker's hack to better secure systems.
- (c) To discover vulnerabilities from a malicious attacker's viewpoint to better secure systems.**
- (d) To introduce vulnerabilities into better secure systems.

**68. The goal of ethical hacker is to hack a system in a.....**

- (a) Non-destructive fashion**
- (b) Destructive fashion
- (c) Highly destructive fashion
- (d) Corruptive fashion

**69. To catch a thief, think like a thief. That's the basis for.....**

- (a) Security testing
  - (b) Ethical hacking**
  - (c) Configuration testing
  - (d) Performance testing
- 

### **(E)Types of Hacking**

**70. What do the Cyberterrorists do?**

- (a) They are skilled criminal experts who write some of the hacking tools, including the scripts and other programs that the script kiddies and security professionals use.
- (b) They are highly technical and publicly known security experts who not only monitor and track computer, network, and application vulnerabilities but also write the tools and other code to exploit them.
- (c) Attack corporate or government computers and public utility infrastructures, such as power grids and air traffic control towers.**
- (d)They are computer novices who take advantage of the exploit tools, vulnerability scanners, and documentation available free on the Internet but who don't have any real

**71. ....is the art of exploiting the human elements to gain access to unauthorised resources**

- (a) Social Engineering.**
- (b) IT Engineering.
- (c) Software testing
- (d) Ethical Hacking.

**72. Which of the following is an AI-powered attack?**

- (a) Ransomware 2.0
- (b) Deepfake phishing**
- (c) OS downgrade attack
- (d) Firmware exploit

**73. Ransomware 2.0 is known for .....**

- (a) Encrypting files only
- (b) Encrypting and exfiltrating data for double / triple extortion**
- (c) Exploiting network devices
- (d) Downgrading OS

**74. IoT exploits typically involve .....**

- (a) Social engineering only
- (b) Insecure devices used for attacks or botnets**
- (c) Application layer bypass
- (d) Red Hat hacking

**75. Zero-day exploits are .....**

- (a) Known vulnerabilities with patches
- (b) Unknown vulnerabilities with no patches available**
- (c) OS downgrade techniques
- (d) Only web application issues

**76. Advanced WAF bypass attacks target .....**

- (a) Operating System
- (b) Web applications**
- (c) IoT devices
- (d) Firmware only

**77. Deep fake technology is associated with:**

- (a) Video/Audio manipulation**
- (b) Password cracking
- (c) Firmware upgrade
- (d) Hardware design

**78. AI-powered phishing scams belong to the category of \_\_\_\_\_ hacking.**

- (a) Application
- (b) Network**
- (c) Operating system
- (d) Firmware

**79. What is called when an unknown vulnerability is exploited before the vendor releases a patch.**

- (a) Zero-day exploits**
- (b) Ransomware
- (c) Deep fake misuse
- (d) Chain of custody error

**80. Phishing attacks aim to:**

- (a) Send spam
- (b) Trick users into revealing sensitive information**
- (c) Encrypt files
- (d) Scan network

**81. Ransomware attacks primarily involve:**

- (a) Stealing identities
- (b) Encrypting user data and demanding ransom**
- (c) Crashing websites
- (d) Spamming emails

**82. IoT botnets are used to:**

- (a) Launch DDoS attacks**
- (b) Encrypt files
- (c) Test network speed
- (d) Clean devices

**83. Malware is:**

- (a) Authorized software
- (b) Malicious software designed to disrupt or damage**

- (c) Antivirus software
- (d) Operating system upgrade

**84. Zero-day attacks are dangerous because:**

- (a) They use old vulnerabilities
- (b) **There is no patch available yet**
- (c) There are easy to prevent
- (d) They target only students

---

**(F) National Cyber Security Policy, IT Act and Cybercrime Prevention against Women and Children Scheme**

**85. National Cyber Security Policy (NCSP) 2013 aims to .....**

- (a) Increase internet speed in India
- (b) **Protect public and private infrastructure from cyber attacks**
- (c) Ban all social media
- (d) Create malware

**86. IT Act 2000 primarily deals with .....**

- (a) Hardware design
- (b) **Electronic records, digital signatures, and cybercrime**
- (c) Building networks
- (d) Installing OS updates

**87. In Section 65, Tampering with computer source documents leads to the penalty as :**

- (a) **Imprisonment up to three years, or/and with fine up to ₹200,000.**
- (b) Imprisonment up to three years, or/and with fine up to ₹100,000
- (c) Imprisonment up to three years, or/and with fine up to ₹500,000
- (d) Imprisonment up to life.

**88. The Digital Personal Data Protection Act (DPDP) 2023 ensures:**

- (a) Free access to all data.
- (b) Encourages phishing attacks.
- (c) **Lawful processing of personal data with consent**
- (d) Deletion of all user data automatically

**89. CCPWC Scheme (2018) focuses on:**

- (a) **Cybercrime prevention against women and children**
- (b) Reducing malware attacks
- (c) Ethical Hacking training only
- (d) IOT security

**90. Which section of IT Act 2000 deals with hacking and computer offenses**

- (a) Section 43
- (b) **Section 66**
- (c) Section 72A
- (d) Section 69

**91. The IT (Amendment) Act 2008 introduced:**

- (a) Only digital signatures
- (b) **Cybercrime provision including identity theft, phishing & cyber terrorism**
- (c) Internet connectivity rules

(d) Hardware standards

**92. Digital personal data protection Act (DPDP) 2023 replaced.....**

- (a) IT Act 2000 completely
- (b) **Some provisions related to personal data protection under IT Act**
- (c) Only Copyright law
- (d) Cybercrime section

**93. Cybercrime against women & children is covered under:**

- (a) IT Act Section 43
- (b) **IT Act 66A/66B & CCPWC Scheme**
- (c) DPDP Act only
- (d) NCSP only

**94. Law that mandates consent for collecting personal data?**

- (a) IT Act 2000
- (b) **DPDP Act 2023**
- (c) CCPWC Scheme
- (d) NCSP 2013

**95. NCSP 2013 was formulated by:**

- (a) UNESCO
- (b) **Government of India**
- (c) Private companies
- (d) Ethical hackers

**96. Which IT Act amendment introduced the Digital Personal Data Protection (DPDP) Act?**

- (a) 2000
- (b) 2008
- (c) **2023**
- (d) 2013

**97. Police investigating online child exploitation cases would rely on which scheme?**

- (a) NCSP 2013
- (b) IT Act 2000
- (c) **CCPWC 2018**
- (d) DPDP 2023

---

**(G) Additional Questions**

**98. A company discovers its employees are receiving AI-generated phishing emails, which type of hacking is this?**

- (a) OS hacking
- (b) Application hacking
- (c) **Network hacking**
- (d) Firmware hacking

**99. If an attacker uses a deep fake voice to trick a bank employee into transferring money, this attack can be classified as-**

- (a) Network phishing
- (b) **Social engineering with AI exploits**
- (c) Firmware attack
- (d) OS downgrade attack

**100. A forensic investigator is analyzing encrypted ransomware files. The encryption key was deleted by the attacker. To prove the case in court, which forensic step is most critical?**

- (a) Collection
- (b) Chain of custody
- (c) Preservation
- (d) Presentation**

**101. A financial company's servers are encrypted by a ransomware gang. Attackers demand cryptocurrency payment and threaten to leak confidential customer data if the ransom is not paid. Identify the type of hacking involved in this case.**

- (a) Application hacking
- (b) Network hacking – Ransomware 2.0**
- (c) Firmware exploits
- (d) OS downgrade attack

**102. A multinational company handling Indian citizen's personal data fails to comply with the DPDP Act 2023. Which risk do they face?**

- (a) Cyber forensic investigation
  - (b) Legal penalties and restrictions on data processing**
  - (c) Ethical hacking mandates
  - (d) NCSP 2013 enforcement
-