ITF+ Exam Glossary

Find more at BareMetalCyber.com

1. **Algorithm**
   An algorithm is a step-by-step set of instructions used to solve a problem or complete a task, often shown as logic or a flowchart. On the exam, it shows up when you must pick the correct order of actions or identify where a process breaks, especially in basic troubleshooting and programming concepts.

2. **Application (software)**
   An application is a program designed to help a user perform a specific task, like a browser, word processor, or email client. Exam questions often test whether you can distinguish applications from the operating system and utilities, and choose the right tool category for the scenario.

3. **Authentication**
   Authentication is the process of proving an identity, such as using a password, PIN, or biometric factor. On the exam, it commonly appears in security scenarios where you must separate “who you are” (authentication) from “what you’re allowed to do” (authorization).

4. **Backup**
   A backup is a stored copy of data that can be used to restore files after loss, corruption, or ransomware. Expect exam decisions about choosing an appropriate backup approach, and common confusion between “backup” and “archiving” or “syncing,” which are not the same thing.

5. **Bandwidth**
   Bandwidth is the maximum capacity of a network link to carry data over time (how much can fit through the “pipe”). On the exam, it matters when you diagnose slow connections or pick the best explanation for performance limits versus issues like latency or packet loss.

6. **Binary**
   Binary is a base-two number system that uses only zero and one to represent values. The exam uses it for foundational computing concepts, including data representation, storage sizing, and simple conversions or comparisons.

7. **BIOS/UEFI**
   BIOS (Basic Input/Output System) and UEFI (Unified Extensible Firmware Interface) are firmware interfaces that initialize hardware and start the boot process before the

operating system loads. Exam questions often test what these settings control (boot order, hardware configuration, security features) and where you would go to change them.

8. **Bit and Byte**
   A bit is the smallest unit of data (a zero or one), and a byte is typically eight bits and is a common unit for measuring file size and storage. On the exam, this distinction helps avoid classic traps like confusing network speeds (often bits per second) with file sizes (often bytes).

9. **Cloud computing**
   Cloud computing is using shared computing resources (like storage, applications, or virtual machines) delivered over a network instead of running everything locally. On the exam, it shows up when comparing local versus hosted options, understanding tradeoffs, and recognizing basic service models at a conceptual level.

10. **Confidentiality, Integrity, Availability (CIA) triad**
    The CIA triad is a foundational security model that frames protection goals: keeping data secret (confidentiality), correct (integrity), and usable when needed (availability). Exam questions often ask which part is being impacted in a scenario, such as unauthorized disclosure, tampering, or downtime.

11. **Cookie**
    A cookie is a small piece of data a website stores in a browser to remember state, such as a session sign-in or site preferences. On the exam, it often shows up in privacy and security scenarios where you must identify what enables tracking or session persistence and what risks exist if it is stolen.

12. **CPU (Central Processing Unit)**
    The CPU is the primary component that executes instructions and coordinates most processing tasks in a computer. Exam questions commonly test basic performance reasoning, such as what higher clock speed, more cores, or a CPU bottleneck implies in a simple scenario.

13. **Cyber hygiene**
    Cyber hygiene is the routine set of practices that reduce everyday security risk, like updating systems, using strong authentication, and backing up important data. On the exam, it appears as “best next step” choices where the safest baseline habit beats a flashy but irrelevant action.

14. **Database**
    A database is an organized collection of data designed for efficient storage,

retrieval, and management, often using tables and relationships. On the exam, it shows up when you need to pick the right way to store structured information and recognize basic database terms and purposes.

15. **Data type**
    A data type defines what kind of value a variable or field can hold, such as integer, string, or Boolean, and what operations make sense on it. Exam questions use this to test whether you can spot mismatches, like treating text as a number, or choosing the right field type in a simple database scenario.

16. **Default gateway**
    The default gateway is the router address a device uses to reach networks outside its local subnet. On the exam, it is a key troubleshooting clue when a device can reach local systems but cannot reach the internet or remote networks.

17. **DHCP (Dynamic Host Configuration Protocol)**
    DHCP automatically assigns IP configuration settings like IP address, subnet mask, default gateway, and DNS servers to devices on a network. On the exam, it frequently appears in basic networking questions about why a device has the wrong address, an “APIPA” address, or inconsistent connectivity.

18. **DNS (Domain Name System)**
    DNS translates human-friendly names like example.com into IP addresses that computers use to connect. On the exam, it’s commonly tested through scenarios where a system can reach a site by IP but not by name, pointing to name-resolution problems.

19. **Driver (device driver)**
    A device driver is software that lets the operating system communicate correctly with specific hardware, like a printer, video card, or network adapter. On the exam, drivers show up in “new hardware not working” situations where installing, updating, or rolling back a driver is the best fix.

20. **Encryption**
    Encryption converts readable data into an unreadable form using a key so only authorized parties can recover the original content. On the exam, it is a core confidentiality control and is often contrasted with hashing, which is one-way and used for integrity checks rather than readable recovery.

21. **Firewall**
    A firewall is a security control that filters network traffic based on rules, allowing approved connections and blocking others. On the exam, it commonly appears in

troubleshooting and security scenarios where you must explain why traffic is failing or choose the best first control to reduce exposure.

22. **Folder (directory)**
    A folder, also called a directory, is a container used by an operating system to organize files in a hierarchy. Exam questions often test basic file-management concepts, such as paths, permissions, and the difference between moving, copying, and deleting data.

23. **FTP (File Transfer Protocol)**
    FTP is a protocol used to transfer files between systems over a network, traditionally without strong built-in encryption. On the exam, it often shows up as a “which is more secure” or “what’s appropriate for file transfer” decision, especially when compared to encrypted alternatives.

24. **Function**
    A function is a reusable block of code that performs a specific task and can be called by name, sometimes with inputs and outputs. On the exam, it appears in basic programming logic where you must recognize modularity, avoid repeated steps, and understand how inputs affect results.

25. **Hardware**
    Hardware refers to the physical components of a computer system, such as the CPU, RAM, storage, and peripherals. On the exam, it matters when you must choose the right component for a symptom, like distinguishing a storage issue from a memory issue.

26. **Hashing**
    Hashing is a one-way process that transforms data into a fixed-length value (a hash) that changes if the input changes. On the exam, hashing is mainly tied to integrity checks and password storage concepts, and it is a frequent confusion point with encryption, which is reversible with a key.

27. **HTML (Hypertext Markup Language)**
    HTML is the standard markup language used to structure content on web pages using elements like headings, paragraphs, and links. On the exam, it shows up as foundational web knowledge and helps you identify what controls page structure versus what controls styling or behavior.

28. **HTTPS (Hypertext Transfer Protocol Secure)**
    HTTPS is HTTP protected with encryption and authentication, typically using TLS, so data between the browser and site is harder to intercept or alter. On the exam, it

often appears in security decisions where you must pick the safer option for logins, forms, and sensitive browsing.

29. **IP address (Internet Protocol address)**
    An IP address is a numeric identifier assigned to a device on a network so it can send and receive data. On the exam, it is central to basic networking and troubleshooting, including recognizing private vs public addressing and why a device cannot reach other networks.

30. **ISP (Internet Service Provider)**
    An ISP is the company that provides internet connectivity services, often including routing, DNS options, and a modem or gateway device. On the exam, it comes up in boundary questions about what is inside the local network versus what is upstream, and when an outage is likely outside the user's control.

31. **Latency**
    Latency is the time it takes for data to travel from a sender to a receiver, often described as delay. On the exam, it helps you explain why a connection can have decent bandwidth but still feel slow, especially for real-time tasks like calls or gaming.

32. **Local Area Network (LAN)**
    A LAN is a network that connects devices within a limited area such as a home, office, or school. Exam questions often test whether you can distinguish a LAN from wider networks and identify common LAN components like switches and access points.

33. **Logical operator**
    A logical operator compares or combines conditions, such as AND, OR, and NOT, to produce a true or false result. On the exam, it appears in basic programming logic where you must determine how multiple conditions affect a decision path.

34. **Malware**
    Malware is malicious software designed to harm systems, steal data, or disrupt operations, including viruses, worms, trojans, and ransomware. On the exam, it shows up in scenario questions where you identify likely causes, safe responses, and basic prevention methods.

35. **Multi-factor authentication (MFA)**
    MFA requires two or more different types of authentication factors, such as something you know (password) plus something you have (code) or something you

are (biometric). On the exam, it is a high-yield security control and is often tested through “best improvement” choices for account protection.

36. **Network switch**
    A network switch connects devices within a LAN and forwards traffic to the correct device using hardware addresses. On the exam, it helps you choose the right device for connecting multiple wired systems and avoid confusing switches with routers, which connect different networks.

37. **Operating system (OS)**
    An operating system is the core software that manages hardware resources and provides services for applications, such as file management and process control. On the exam, it appears in many basics questions about roles, updates, permissions, and what layer a problem likely belongs to.

38. **Patch management**
    Patch management is the process of acquiring, testing, and installing updates that fix bugs or security vulnerabilities. On the exam, it is a common security best practice and often appears as the most correct preventative action after identifying a vulnerability.

39. **Phishing**
    Phishing is a social engineering attack that tricks users into revealing sensitive information or installing malware, often via email, text, or fake websites. On the exam, it is frequently tested through recognition cues and correct response actions like reporting and not clicking suspicious links.

40. **RAM (Random Access Memory)**
    RAM is short-term working memory used by the system to run programs and hold active data temporarily. On the exam, it shows up in performance troubleshooting, such as identifying symptoms of low memory versus slow storage or a CPU bottleneck.

41. **Ransomware**
    Ransomware is a type of malware that encrypts files or locks systems and demands payment to restore access. On the exam, it typically appears in incident scenarios where the best answer emphasizes containment, recovery from backups, and reporting rather than paying the ransom.

42. **Router**
    A router connects different networks and directs traffic between them, such as between a home LAN and the internet. Exam questions often test whether you can

distinguish a router from a switch and recognize that routing decisions happen between networks, not just within one local segment.

43. **Social engineering**
    Social engineering is manipulating people into giving up information or performing unsafe actions, such as clicking a link or sharing credentials. On the exam, it is a high-yield concept because many scenarios are really about recognizing the human trick, not a technical failure.

44. **Software as a Service (SaaS)**
    SaaS is a cloud model where a complete application is delivered over the internet and managed by the provider, like web-based email or office tools. On the exam, it commonly shows up as a "who manages what" decision, where the provider handles most of the platform while the user organization still manages accounts and data use.

45. **Subnet mask**
    A subnet mask defines which part of an IP address is the network portion and which part identifies a device on that network. On the exam, it matters in basic network troubleshooting because an incorrect subnet mask can allow local communication to fail even when the IP address looks valid.

46. **TCP/IP (Transmission Control Protocol/Internet Protocol)**
    TCP/IP is the foundational suite of networking protocols used for addressing, routing, and reliable delivery of data across networks. On the exam, it appears as the basic "language" of networking, helping you reason about IP addressing, ports, and why connections succeed or fail.

47. **Troubleshooting methodology**
    A troubleshooting methodology is a structured approach to diagnosing and fixing problems, typically starting with identifying symptoms and testing likely causes in a controlled way. On the exam, it shows up as "best next step" questions where process discipline beats guessing or making multiple changes at once.

48. **URL (Uniform Resource Locator)**
    A URL is the address used to locate a resource on the web, including the protocol, domain, and path. On the exam, it often appears in web and security questions where you must spot suspicious domains, misleading links, or the difference between HTTP and HTTPS.

49. **Virtualization**
    Virtualization is using software to create virtual versions of resources, such as

running multiple virtual machines on one physical computer. On the exam, it helps explain efficient resource use and testing environments, and it can appear in comparisons between physical hardware and virtual systems.

50. **Wi-Fi**
    Wi-Fi is a wireless networking technology (typically using IEEE 802.11 standards) that connects devices to a LAN through a wireless access point. On the exam, it commonly appears in connectivity and security scenarios, including recognizing causes of weak signals and the need for secure wireless settings.