1. ***Describe the procedure of crime scene management***

i. Cordon Crime scene
ii. Establish approach way/walkthrough
iii. Take photographs
iv. Mark evidence
v. Conduct vaginal swab/check clothing for semen/check fingernails for scraped tissue
vi. Collect fingerprint of the victim, blood from the floor, windows
vii. Look for fingerprints in blood, on objects like an apple
viii. Send body for Post-Mortem
ix. Collect blood, apple pie, and other samples. Swab, remote, speed gun

2. ***Methods of disposal of unexploded explosives found in a case.***

<u>Explosives found in a case can be disposed of using the following methods:</u>

1. Detonation

2. Burning

3. Chemical decomposition

<u>Prohibited Methods:</u>

1. Abandoning

2. Burning

3. Dumping at sea

3. ***Disposal by detonation:***

Detonation can be done using:

a) Primary explosives
b) Military ordnances
c) Improvised Explosive Devices (IEDs)
d) Sensitive mixtures

4. ***What is an explosive?***

An explosive is a reactive substance that contains a great amount of potential energy that can produce an explosion if released suddenly, usually accompanied by the production of light, heat, sound, and pressure.

5. How many types of explosives are there?

Explosives are generally classified into two main types:

- High Explosives
- Low Explosives

6. Write 3 names and attributes of explosives:

1. TNT (Trinitrotoluene):

- Type: High Explosive
- Attributes: Stable and safe to handle, commonly used in military applications and demolition.

2. Nitroglycerin:

- Type: High Explosive
- Attributes: Highly sensitive to shock and temperature, used in dynamite and medical applications for heart conditions.

3. Black Powder:

- Type: Low Explosive
- Attributes: Composed of potassium nitrate, charcoal, and sulfur; used in fireworks, historical firearms, and as a propellant in various applications.

7. What is Human Trafficking?

Human trafficking means the act of selling, buying, recruiting, receiving, deporting, transferring, sending, confining, or harboring any person within or outside the territory of Bangladesh for purposes of sexual exploitation, labor exploitation, or any other form of exploitation or oppression. This is done through:

- Threat or use of force
- Deception or abuse of socio-economic, environmental, or other vulnerabilities
- Giving or receiving money or benefits to procure the consent of a person having control over the victim

<u>Salient Features of The Prevention & Suppression of Human Trafficking Act 2012:</u>

- Extra-territorial Application (Section 5): The law applies to offenses committed outside Bangladesh.
- Establishment of Anti-human Trafficking Offence Tribunals (Section 21): Special courts are established to handle human trafficking cases.
- Time Limit to Conclude the Trial (Section 21): Trials must be concluded within 180 working days; appeals within 10 working days.
- Trial in Camera (Section 25): Trials can be conducted privately to protect victims.
- Appointment of Interpreter (Section 26): An interpreter can be appointed if needed.
- Seizure, Freeze, Confiscation of Property, and Extra-territorial Injunction (Section 27): Authorities can seize and freeze properties involved in trafficking.
- Order of Compensation by Tribunal for Victims (Section 28): Victims can receive compensation.
- Admissibility of Foreign Documents/Written Proofs/Materials (Section 29): Foreign evidence is admissible.
- Admissibility of Electronic Proofs (Audio/Video) (Section 30): Electronic evidence is admissible.
- Government Responsibility to Identify and Rescue Victims (Section 32): The government is responsible for identifying and rescuing victims.
- Repatriation of Victims (Extradition Treaty) (Section 33): Victims can be repatriated based on treaties.
- Providing Information to Victims/Public Generally (Section 34): Information should be provided to victims and the public.
- Establishment of Protective Homes and Rehabilitation Centres (Section 35): Homes and centers for victims' protection and rehabilitation.
- Victim Protection, Rehabilitation, and Social Integration (Section 36): Ensuring victims' protection and social integration.
- Protection of Victims or Affected Persons and Witnesses in Criminal Trials (Section 37): Protecting victims and witnesses during trials.
- Publish/Telecast Victims/Family Members' Name and Address/Photo without Court Permission (Section 37-2): Prohibited without court permission.
- Protection of the Rights of Child Victims and Witnesses (Section 38): Special protection for child victims and witnesses.
- Financial Assistance to the Victim of Human Trafficking (Section 40): Financial support for victims.
- Formation of "Prevention of Human Trafficking Fund" (Section 42): Fund established for prevention and support.
- Joint or Mutual Legal Assistance and Cooperation to Suppress and Prevent Human Trafficking (Section 41): Encouraging international cooperation.

Investigation (Section 19):

- Investigation Officer (I/O): Must be at least of the rank of sub-inspector.
- Proactive Inquiry Before FIR: Investigation can start before an official report is filed.
- Investigation Period: 90 working days from the date of FIR or tribunal reference.
- Extension of Investigation: If needed, an extension of 30 more working days can be requested.
- Foreign Travel for Evidence: Investigation team can travel abroad with tribunal approval.
- Central Monitoring Cell: The government will establish a monitoring cell at the police headquarters.

<u>Preventive Search and Seizure (Section 20):</u>

- Authorization: A police officer, not below the rank of sub-inspector, authorized by a superior can conduct searches.
- Warrantless Search: Searches can be done without a warrant if there are reasonable grounds and in the presence of witnesses.
- Human Rights Respect: Searches should respect human rights and dignity; female officers should search women.
- Search Report: A report describing the reasons and results of the search must be prepared within 72 hours and sent to the tribunal.

8. What is social engineering? Types? Examples

Social engineering is a manipulation technique that exploits human error to gain private information, access, or valuables. In cybersecurity, it refers to tricking people into breaking normal security procedures.

Types of Social Engineering:

a) Phishing: Sending fraudulent messages that appear to come from a reputable source, typically via email, to steal sensitive data.
b) Pretexting: Creating a fabricated scenario to engage a target and extract information.
c) Baiting: Offering something enticing to the target (like free software) to get them to give up sensitive information or download malware.
d) Quid Pro Quo: Offering a service in exchange for information.
e) Tailgating/Piggybacking: Following someone into a restricted area without proper authentication.

Examples:

- Phishing: An email that looks like it's from your bank asking you to verify your account details.

- Pretexting: A caller pretending to be from IT support, asking for your login credentials to "fix" an issue.
- Baiting: A USB drive labeled "Confidential" left in a public place, which installs malware when inserted into a computer.

9. What is Crypto currency? Example

Crypto currency is a digital or virtual currency that uses cryptography for security. It is decentralized and typically based on blockchain technology, a distributed ledger enforced by a network of computers (nodes).

Example:

- Bitcoin (BTC): The first and most well-known Crypto currency, created by an anonymous person or group known as Satoshi Nakamoto.

10. What is a VPN? How does it work?

VPN (Virtual Private Network) is a service that encrypts your internet connection and hides your IP address, making your online actions virtually untraceable.

How it Works:

a) Encryption: Data sent and received is encrypted, making it unreadable to anyone who intercepts it.
b) IP Masking: Your real IP address is hidden, and you are assigned a new IP address from the VPN server.
c) Secure Connection: Establishes a secure and encrypted connection between your device and the VPN server.

11. Life cycle of social engineering

The life cycle of social engineering typically involves the following stages:

- Research: Gathering information about the target through social media, public records, or other resources.
- Hook: Engaging the target by creating a scenario or sending a message that prompts them to respond.
- Play: Executing the attack by manipulating the target to divulge information or perform an action.
- Exit: Closing the interaction without arousing suspicion, often after obtaining the desired information or access.

12. Sources of terrorist finance

Sources of terrorist finance can include:

- State Sponsorship: Financial support from sympathetic governments.
- Charities and Non-profits: Misuse of legitimate charities to funnel funds.
- Criminal Activities: Drug trafficking, smuggling, kidnapping for ransom, and other illegal activities.
- Business Ventures: Legitimate businesses used as fronts for funding.
- Donations: Contributions from individuals and organizations that support the cause.

13. Social media used by terrorists

Social media used by terrorists includes platforms like:

- Facebook: For spreading propaganda and recruiting followers.
- Twitter: For real-time communication and spreading messages.
- YouTube: For sharing videos of training, propaganda, and messages from leaders.
- Telegram: For secure communication and distributing information due to its encryption features.

14. Layers of the internet

Layers of the internet refer to the different levels that make up the internet structure:

- Surface Web: The part of the internet that is indexed by search engines and accessible to the general public.
- Deep Web: Parts of the internet not indexed by search engines, including databases, academic journals, and private networks.
- Dark Web: A small portion of the deep web that is intentionally hidden and accessible only through specific software like Tor, often associated with illegal activities.

****

15. What is the definition of caliber?

Answer: Caliber refers to the internal diameter of a gun barrel or the size of the bullet that fits into the barrel. It is usually measured in either inches or millimeters. For example, a 9mm caliber gun has a barrel that is 9 millimeters wide, and it uses bullets of the same size. Caliber is crucial in determining the power, range, and accuracy of a firearm, with larger calibers generally being more powerful.

16. What is CDR analysis, and why is it important?

Answer: CDR stands for Call Detail Record, which is a collection of data recorded by telecommunication companies that logs the details of phone calls, messages, and other communications. A CDR typically includes information such as the phone numbers involved in the communication, the time and date of the call, the duration of the call, and the location of the phones when the call was made.

Importance of CDR Analysis:

CDR analysis is vital in various contexts, especially in law enforcement and intelligence gathering. It helps investigators:

- Identify Communication Patterns: By analyzing who is communicating with whom, when, and how often, investigators can identify relationships and networks, which is crucial in criminal investigations.
- Track Movements: Since CDRs often include location data, they can help trace the movement of individuals over time.
- Corroborate Evidence: CDR analysis can corroborate other pieces of evidence in a case, providing a timeline of events or proving the presence of a suspect at a crime scene.
- Prevent Terrorism and Crime: By analyzing communication patterns, law enforcement agencies can preemptively identify and disrupt criminal or terrorist activities.

17. What are the sources of terrorist financing?

Answer: Terrorists fund their activities through various means, including:

- Donations from Supporters: Terrorists receive funds from individuals or organizations that support their cause. These donations can be small amounts from many people, often raised through social media or crowd funding platforms.
- Illegal Activities: Many terrorist groups engage in criminal activities to finance their operations. These can include drug trafficking, smuggling, kidnapping for ransom, and robbery.
- Exploitation of Resources: Some terrorist groups control territories where they exploit natural resources like oil, minerals, or timber, selling them on the black market to raise funds.
- Front Organizations: Terrorists often use seemingly legitimate businesses or charities as fronts to launder money and finance their operations without attracting attention.
- State Sponsorship: Some governments support terrorist groups for political reasons, providing them with money, weapons, or safe havens.

18. Why do terrorists use social media?

Answer: Terrorists use social media for several strategic reasons:

- Recruitment: Social media allows terrorists to reach a global audience, spreading their ideology and recruiting new members from around the world.
- Propaganda: They use platforms like Twitter, Facebook, and YouTube to share propaganda, videos, and messages to inspire or incite violence, and to demonstrate their power.
- Communication: Social media provides an easy and sometimes encrypted means of communication, enabling terrorists to coordinate attacks and share information with each other.
- Fundraising: Terrorist groups can solicit donations through social media, either directly or through disguised crowdfunding campaigns.
- Psychological Impact: By sharing videos or messages of terror attacks, they aim to create fear and uncertainty among the public and government.

19. What are the challenges of counter-terrorism and the use of cyberspace?

Answer: Counter-terrorism in the context of cyberspace faces several challenges:

- Encryption: Terrorists often use encrypted communication tools, making it difficult for authorities to intercept and decode messages. This hinders the ability to monitor and prevent terrorist activities.
- Anonymity: The internet allows terrorists to operate anonymously, making it hard to trace their identities or locations. They can easily hide behind fake profiles or use the dark web.
- Speed of Information Spread: Information, including plans for attacks, can be spread quickly across the globe through the internet, making it challenging for authorities to respond in time.
- Radicalization: Cyberspace provides a platform for the rapid spread of extremist ideologies, leading to the radicalization of individuals without physical contact. This makes it difficult to detect and intervene before radicalization leads to violence.
- Resource Limitations: Law enforcement agencies may not have the resources, technology, or expertise to monitor all online activities, especially given the sheer volume of data generated daily.
- Legal and Ethical Issues: Monitoring cyberspace often raises legal and ethical concerns, such as the balance between privacy and security, which complicates counter-terrorism efforts.

20. Why can't the government trace the dark web?

Answer: The dark web is a part of the internet that is intentionally hidden and can only be accessed using special software like Tor (The Onion Router). It's designed to provide anonymity to its users through the following methods:

- Encryption: Communications on the dark web are heavily encrypted, meaning that even if data is intercepted, it is extremely difficult to read or understand.
- Anonymity: Users on the dark web use Tor or similar tools that hide their IP addresses, making it very difficult to trace their physical locations or identities.
- Decentralization: The dark web is decentralized, meaning there's no single server or point of control that can be targeted by authorities. It operates on a peer-to-peer network, where data is passed through multiple, random points, further masking its origin.
- Lack of Regulation: The dark web is not regulated by any government or organization, so traditional methods of surveillance and law enforcement are ineffective.

These features make it extremely challenging for governments to trace activities on the dark web, making it a haven for illegal activities like drug trafficking, illegal arms sales, and even terrorist communication.

21. What is social engineering? What are the types and examples?

Answer: Social engineering is a tactic used by attackers to manipulate people into giving up confidential information, such as passwords or bank details. Instead of hacking a computer system, the attacker "hacks" a person's trust by pretending to be someone trustworthy.

<u>Types of Social Engineering:</u>

- Phishing: Sending fake emails that appear to be from a legitimate source (like a bank) to trick people into providing sensitive information.

Example: An email claiming to be from your bank asks you to click on a link to verify your account details. The link leads to a fake website that steals your information.

- Pretexting: The attacker invents a story or pretext to obtain personal information.

Example: Someone calls pretending to be from the IT department, asking for your login details to fix a supposed issue.

- Baiting: Offering something enticing (like a free download or a USB drive left in a public place) to get someone to give up information or install malware.

Example: A USB drive labeled “Confidential” is left on the ground in a parking lot. When someone picks it up and plugs it into their computer, it installs malware.

- Tailgating: Gaining access to a restricted area by following someone who has legitimate access.

Example: An attacker waits by a secure door and follows an employee in when they open it, pretending to have forgotten their access card.

22. What is the life cycle of social engineering?

Answer: The life cycle of social engineering typically follows these stages:

- Research: The attacker gathers information about the target, such as personal details, habits, or relationships. This can involve studying social media profiles, company websites, or public records.
- Hook: The attacker establishes contact with the target, often by pretending to be someone trustworthy, like a colleague or a service provider. The goal is to gain the target’s trust.
- Play: The attacker exploits the relationship they’ve built to extract information or convince the target to take some action, like clicking a link or sharing a password.
- Exit: After achieving their goal, the attacker ends the interaction, often leaving no trace of their presence. The target may not realize they’ve been deceived until much later.

23. What is Crypto currency? Give an example.

Answer: Crypto currency is a type of digital or virtual currency that uses cryptography for security, making it difficult to counterfeit or double-spend. Crypto currencies operate on decentralized networks based on block chain technology, which is a distributed ledger enforced by a network of computers (nodes).

Example:

Bit coin: The first and most well-known Crypto currency, created in 2009 by an anonymous person (or group) known as Satoshi Nakamoto. Bitcoin allows for peer-to-peer transactions without the need for a central authority like a bank. Other examples of cryptocurrencies include Ethereum, Litecoin, and Ripple.

Crypto currencies are used for various purposes, including online purchases, investments, and as a means of transferring assets anonymously.