Discourse

22CS021/22IT021 - CYBER FORENSIC

1. Tool names are given, provide a appropriate objective and usage of the particular tools

S No	Tool Name	Objective	Usage
1	Network Miner		
2	Magnetic RAM capture		
3	Autopsy		
4	Wireshark		

2. Watermarking in cyber forensics is a technique used to embed hidden data within digital files (such as images, videos, documents, or audio) to ensure authenticity, traceability, and protection against tampering or unauthorized distribution.The encoding process of watermarking is given below.Watermarking involves embedding (encoding) hidden data (watermark) into a carrier signal (like an image, video, or audio). The decoding process extracts the watermark from the carrier.

i) Sketch the Encoding and Decoding process of watermarking technique.
ii) Illustrate an real time use case for the following watermarking techniques(Audio Watermarking, Blockchain-Based Watermarking, Fragile Watermarking, Text Watermarking, Robust Watermarking, image/Video Watermarking).

3. A small e-commerce website suddenly experiences unauthorized logins into its admin panel. The attacker gains access and steals customer data, including emails, phone numbers, and partial credit card details.
Identify the cyber-attacks that can happen in above scenario with appropriate and justify the same

4. TCP is used for secured data exchange which guarantee the data communication as the initial set up establishment is strong. Outline the three-way handshake and four-way handshake facilities in TCP.

5. Match the following table: Action and Impact of Cyber security

S.No	Steps	User Action	Cybersecurity Impact
1	Pop-up Appears(A1)	Abnormal system activity is noticed	Could be a malware-infected ad
2	User Clicks Pop-up (A2)	scan the system and remove malware	updating security patches
3	System Behavior Changes(A3)	abnormal system activity is noticed	Might install malware
4	Cybersecurity Response(A4)	User clicks without verifying	Indicates possible virus, spyware

6. A multinational company is setting up a secure office network to ensure high-speed connectivity, secure communication, and access control for its employees. The network should support wired and wireless connections, remote access, and data security to prevent cyber threats.

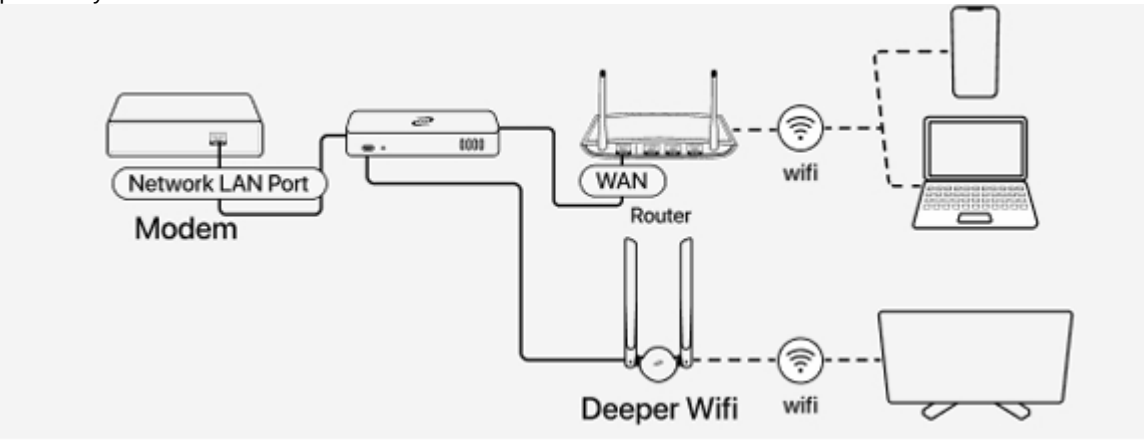


Fig: Network Configuration

When a cyber - crime investigation is taking place, identify the place where the data can be verified and investigated.

7. Hardware forensic tools are used in a theft investigation scene. These devices help in preventing data tampering, performing high-speed imaging, and creating forensic clones for offline analysis.

a) Find the missing elements in the table

A. Tool Name	B. Primary Function	C. Example Use-Case	D. Limitation
A1.Tableau TD3 Duplicator			
A2.Logicube Falcon			
A3.WiebeTech USB Write Blocker	Prevents writing to USB devices during analysis	Inspecting USB drives for stolen intellectual property without modifying drive contents.	Works only with USB devices

b) Provide a real time examples for the Hardware forensic tools in the column A.

8. Identify the correct statement about firewall

Statement1: A firewall is used to monitor and control incoming and outgoing network traffic based on security rules.
Statement2: The firewall and the intrusion detection system both are different.
Statement3: Firewall is a software.
Statement4: Firewall is a paid service.
Statement5: The firewall helps in filtering the network packets by following the access control list.
Statement6: Firewalls can prevent only specific types of cyberattacks.

9. HTML elements are used to create E-Commerce website. Read the implementation and identify the tool and identify the HTML tags and provide an example one is done for you

S No	Implementation	HTML Elements	Example
1	Organizes products into different sections like Electronics, Clothing, and Books	<section>	<section> Electronics </section>
2	Used to display the website logo, search bar		
3	Allowing users to navigate between categories.		
4	Used to structure the primary content		
5	Displays individual product descriptions		

10. The e-mail investigation process is given below
Step 1: Collect the sender information
Step 2: Get the E-mail header Information
Step 3:
Step 4:
Identify the missing steps in the Email investigation process and also determine the steps contribute to the data preservation phase in a cyber-crime investigation

11. Injection Attack is initiated by an attacker to hack the secured credentials. Predict the steps of the attack by referring to the figure given below.

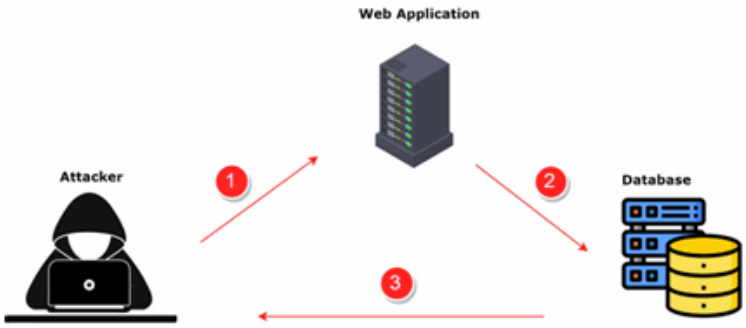
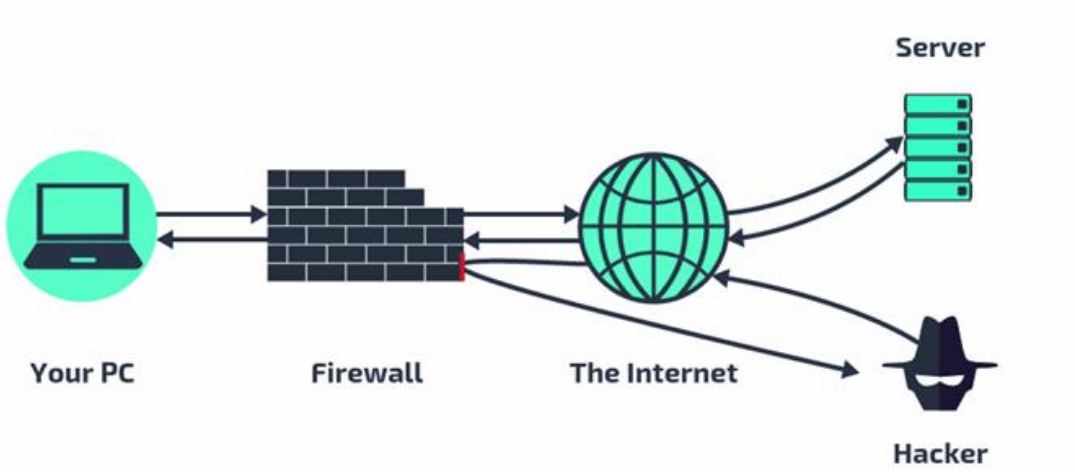


Figure:Injection Attack in Web application

12. A senior accountant in a large corporation receives an email claiming to be from the CEO, urgently requesting login credentials to approve a critical financial transaction. Believing the email to be legitimate, the accountant provides the credentials, unknowingly giving attackers access to their account. The attackers use the compromised email to send fraudulent instructions to the finance team, authorizing a significant fund transfer to a fake account. This breach leads to financial loss, operational disruption, and reputational damage for the company. Investigations reveal the attack was a phishing scheme targeting high level employ.

i) The consequences are like direct financial loss, operational disruption, and reputational damage so Identify a way to prevent this E Mail Spoofing.
ii) Outline the whole process, how would be this Email spoofing occurs in a attacker.

13. A firewall is a component that monitor the network and examine the abnormal activities. A firewall setup for a network is given below



i) Refer the figure given and predict the location of the firewall where it is placed.
ii) In which way Firewall protects the open ports in the environment.
iii) Infer the placement of the firewall in the given network setup and analyze how it ensures real-time protection against potential security threats.

14. A corporate cybersecurity team discovers unauthorized access to their internal file server. A forensic investigator is called in to collect and analyze the evidence. The following investigation practices are listed below.

Identify the invalid statements of Investigation Practices and justify the same.
1.Hash values are used to ensure that forensic images have been altered during acquisition.
2.It is not acceptable to analyze original evidence without creating a forensic image first.
3.Using a write blocker during evidence collection helps maintain the integrity of the original storage device.
4.Validating forensic data includes both verifying file integrity and ensuring the chain of custody is maintained.
5. Any hashing algorithm, including outdated ones like MD2, is not sufficient for legal forensic validation.
6.Digital evidence can be validated solely by checking the file size and timestamps
7.Comparing pre- and post-acquisition hashes is a standard method for verifying that no data was changed during imaging.
8.Validation of forensic data is mandatory if the evidence appears unaltered during manual inspection.

15. Consider the Wireshark output

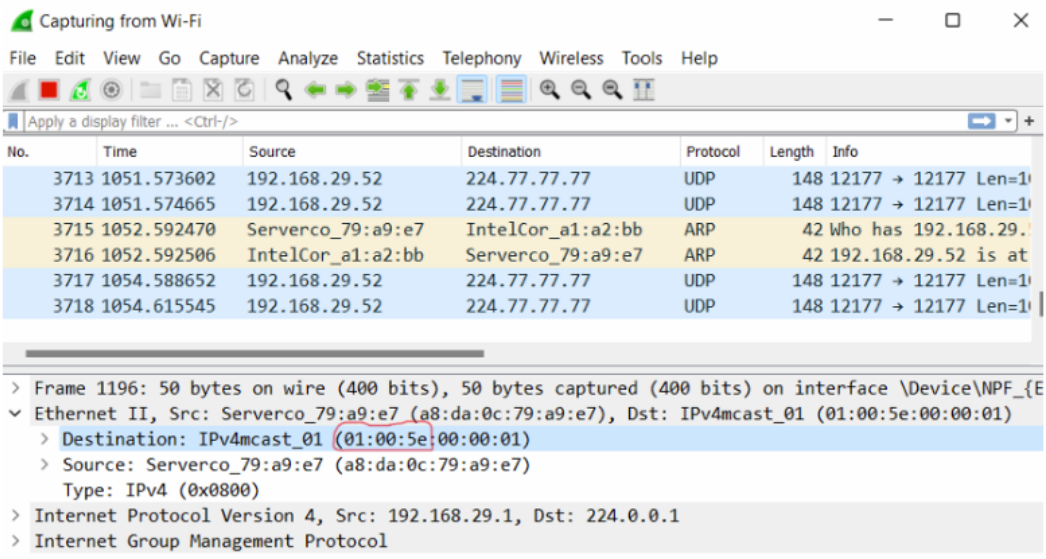


Fig:Wireshark

i) Predict the location where did the handsharking happens in the Wireshark output.
ii) Assertion (A): Network forensics helps in tracking and analyzing cyber threats by monitoring personal computer
Reasoning (R): Analyzing network logs and packet data, security teams can detect hacking attempts, data breaches, suspicious activities.
Identify the correct option and justify it.(2 marks)
a) Both A and R are true, and R is the correct explanation of A.
b) Both A and R are true, but R is not the correct explanation of A.
c) A is true, but R is false.
d) A is false, but R is true.

16. Investigating suspicious network traffic helps to detect unauthorized access and E-mail headers and metadata traces phishing attacks and fraud attempts in entire network.

IP addresses are stored in a particular database and predict the process how would the database helps in finding the threats.

17. A user visits an e-commerce website to buy a smartphone. The process involves multiple HTTP request/response cycles between the client (browser) and the web server.User receives an order confirmation, and the order is processed for shipping.HTTP status codes like 200 OK and 302 Redirect indicate a smooth transaction. If payment processing fails, the server returns HTTP 402 Payment Required or 500 Internal Server Error. If an item is out of stock, the server may return HTTP 404 Not Found or display an error message.

Consider the above scenario during checkout, after successful payment, the user is redirected to an order confirmation page with HTTP 302 Redirect, but the page fails to load due to a 500 Internal Server Error. Predict a method to resolve this issue.

18. Port number and Protocol name are given predict the purpose of protocol.

S No	Port number	Protocol name	Purpose of protocol
1	21	HTTP	?
2	25	FTP	?
3	53	SMTP	?
4	80	DNS	?