**409 GROUP WORK**

**QUESTION 3**

Five forensics tools suitable for live systems and network operations, discussing their configurations for these specific tasks are;

1. **WIRESHARK**

**Function:**

Network Traffic Capture and Analysis: Wireshark is a powerful open-source network protocol analyser. It allows users to capture and analyse network traffic in real-time. Wireshark can dissect and display the details of packets, making it invaluable for network troubleshooting, protocol analysis, and security monitoring.

**Configuration:**

Live Packet Capturing: Users can configure Wireshark to capture live network traffic. This involves selecting the network interface from which to capture packets. Configuration may include setting filters to capture specific types of traffic or specifying capture options such as packet size limits.

1. **VOLATILITY**

**Function:**

Memory Forensics: Volatility is an open-source memory forensics framework. It is used to analyse memory dumps of live systems, extracting information about running processes, network connections, and system state from volatile memory.

**Configuration:**

Memory Image and Profile Specification: To use Volatility, analysts typically provide a memory image file (captured from a live system) and specify the profile that corresponds to the operating system and version. Configuration involves selecting the appropriate plugins for analysis based on the type of information needed.

1. **LIVE RESPONSE COLLECTION (LRC) TOOLS (E.G., CROWDSTRIKE FALCON):**

**Function:**

Real-time Incident Response: LRC tools like CrowdStrike Falcon are designed for real-time incident handling and response. They provide capabilities for live forensics, threat detection, and response to security incidents.

**Configuration:**

Tool-Specific Configuration: The configuration of LRC tools varies depending on the specific tool used. Configuration options may include setting up real-time monitoring, defining response actions for different types of incidents, and configuring alerting mechanisms. Specific details depend on the features and capabilities of the chosen LRC tool.

1. **BRO (ZEEK):**

**Function:**

Network Analysis Framework: Bro, now known as Zeek, is a powerful network analysis framework. It captures, logs, and organizes network traffic, providing insights into network behavior. It goes beyond simple packet capture, enabling the creation of custom network policies and rules.

**Configuration:**

Defining Network Policies and Rules: Configuration involves specifying policies and rules to define what types of network activities should be monitored and logged. Users can customize Bro's behavior based on the specific network environment and security requirements.

1. **SNORT:**

**Function:**

Intrusion Detection System (IDS): Snort is an open-source intrusion detection system that monitors network traffic for suspicious activities or patterns indicative of a security threat. It can be deployed in real-time to detect and respond to potential intrusions.

**Configuration:**

Rules and Policies Setup: Configuration in Snort involves defining rules and policies to identify and respond to specific types of network traffic. Users configure rules to detect known attack patterns or unusual behavior. Additionally, configuration may include specifying response actions for detected threats.

**QUESTION 4**

Core forensic commands and their importance;

1. **DD (DISK DUMP):**

Importance: Creates forensic copies (images) of storage media for analysis without altering the original data.

1. **HASHDEEP:**

Importance: Computes hash values (MD5, SHA-1, SHA-256) to verify the integrity of files during forensic analysis.

1. **FILE:**

Importance: Determines file type and metadata, aiding in the identification of unknown files.

1. **STRINGS:**

Importance: Extracts readable text from binary files, helping to identify relevant information within them.

1. **GREP:**

Importance: Searches for specific patterns or keywords within files, facilitating the identification of relevant information.