Packet Analysis Report

What is the type of information that can be viewed? What do these mean? Here are some basic guidelines to assist you in understanding what the data means. Captured data from packet analysis can be used either directly or indirectly as evidence against a certain cybercrime based on information gathered from analysis.

Some sources of information that are forensic material are:

Source IP Address: Retrieves information of the user, cross checking this physically would allow the identification of which device is on this address.

Destination IP Address: Shows which target address that the person is searching/sending data to.

Port numbers: What kind of specific ports are being used and what type of malicious activity is done through open ports.

ICMP packets: Long ICMP packets shows that there might be some DoS(Denial of Service) attack.

TCP Sync ACK: Acknowledge flag for visualization of open ports.

Useful Tools

IP Address Lookup – Information on a specific public IP addresses.

Port Finder – Information on a specific TCP/UDP port.