Glossary terms from week 4

Terms and definitions from the certificate

Terms and definitions from Course 1, Week 4

Antivirus software: A software program used to prevent, detect, and eliminate malware and viruses

Database: An organized collection of information or data

Data point: A specific piece of information

Intrusion detection system (IDS): An application that monitors system activity and alerts on possible intrusions

Linux: An open-source operating system

Log: A record of events that occur within an organization’s systems

Network protocol analyzer (packet sniffer): A tool designed to capture and analyze data traffic within a network

Order of volatility: A sequence outlining the order of data that must be preserved from first to last

Programming: A process that can be used to create a specific set of instructions for a computer to execute tasks

Protecting and preserving evidence: The process of properly working with fragile and volatile digital evidence

Security information and event management (SIEM): An application that collects and analyzes log data to monitor critical activities in an organization

SQL (Structured Query Language): A programming language used to create, interact with, and request information from a database

---

Revision #1
Created 2023-06-03 02:49:47 UTC by naruzkurai
Updated 2023-06-03 04:51:01 UTC by naruzkurai