Digital Forensics Glossary

This document is designed to cover acronyms and terms used in the Incident Response domain of the Blue Team Level 1 certification training course.

This document is TLP:White, and can be shared without breaching the Terms and Conditions of the BTL1 course.

Learn more about Blue Team Level 1 and purchase the certification here – https://securityblue.team/why-btl1/

IOC // Indicator of Compromise – Intelligence gathered from malicious activity, intrusions, or incidents. An example would be a piece of malware that was observed in an attack against an organization. The file hashes and file name can be shared with other organizations so they can add it to blocklists or perform threat exposure checks.

TTP // Tools, Techniques, and Procedures – MITRE have defined over 240 unique tactics used by adversaries, known as TTPs. You can find them here, each with detailed descriptions, and the threat actors that have been known to use them.

PCAP // Packet Capture – A file that contains stored information of network traffic that has been captured by a network monitoring tool, such as Wireshark. PCAP files can also be imported by files for network analysis purposes, such as Wireshark or TCPDump.

HDD // Hard Disk Drive – A hard disk drive is an electro-mechanical data storage device that uses one or more rotating platters coated with magnetic material, allowing data to be written and read from the device.

SSD // Solid State Disk Drive – A SSD is a solid-state storage device that uses circuit assemblies to store data persistently, typically using flash memory, as opposed to a spinning magnetic disk as used by hard disk drives.

USB Drive // Universal Serial Bus Drive – A USB is a portable small-scale storage device that includes flash memory. These are typically used to transport files from one system to another without needing network connectivity.

ACPO // Association of Chief Police Officers – ACPO provides a set of guidelines for computer-based evidence, containing 4 main principles. These help to guide law enforcement and digital forensic experts when conducting investigations to ensure the evidence is valid and can be submitted in court for legal proceedings.

KAPE // Kroll Artifact Parser and Extractor – KAPE is used for fast acquisition of digital evidence and files that may be interesting to a forensic examiner. The operator is able to define the information they want to collect using modules, and KAPE will get to work, retrieving important information within minutes, while a complete forensic copy could take hours.

FTK Imager // Forensic Tool Kit Imager – A free tool that allows bit-by-bit disk drive images to be taken, disk images to be mounted in a read-only mode (software write-blocker), and analysis functionality to analyze disk images.

Write-Blocker // A software or hardware device that prevents one system from writing to another, ensuring that digital evidence isn't unintentionally tampered with. Typically used between a hard-drive that may contain digital evidence, and a forensic laptop or workstation that is taking a forensic copy of the data.

BHC // Browser History Capturer – A free tool that allows the operator to collect core files from mainstream web browsers, which can be manually reviewed, or imported into Browser History Viewer for analysis of web history.

BHV // Browser History Viewer – A free tool that allows the operator to capture some core browser files (it is better to use Browser History Capturer to collect files for analysis) and then provides analysis functionality, allowing for the inspection of long-term browser history, cached images and web pages.

/etc/passwd // Linux Passwd File – The passwd file, located at /etc/passwd contains information about all of the user accounts on a Linux system, including accounts used by service daemons, and user-created account. This can be combined with the associated shadow file to allow cracking of user passwords.

/etc/shadow // Linux Shadow File – The shadow file, located at /etc/shadow contains the encrypted passwords for all accounts on a linux system. This can be combined with the associated passwd file to allow cracking of user passwords.