Question: Your supervisor has asked you to list the acquisition tools avail...

Your supervisor has asked you to list the acquisition tools available on a forensic Linux Live CD. Download the current ISO version of Deft (www.deftlinux.net), CAINE (www.caine-live.net), Kali Linux (www.kali.org), or Penguin Sleuth (www.linux-forensics.com), and then create a bootable CD or DVD of it. Start it on your workstation and survey its tools. Then write a one to two-page report containing a brief description of each acquisition utility on the CD or DVD.

Expert Answer

Jagdish Dammala answered this
511 answers

Was this answer helpful? 2 0

ANSWER:-

These tools/utilities are can be stored in cd for kali linux

Binwalk tool:

Binwalk is a forensic tool in Kali that searches a specified binary image for executable code and files. It identifies all the files that are embedded inside any firmware image. It uses a very effective library known as “libmagic,” which sorts out magic signatures in Unix file utility.

Bulk extractor tool:

Bulk extractor tool extracts credit card numbers, URL links, email addresses, which are used as digital evidence. This tool lets you identify malware and intrusion attacks, identity investigations, cyber vulnerabilities, and password cracking. The specialty of this tool is that not only does it work with normal data, but it also works on compressed data and incomplete or damaged data.

HashDeep tool:

The hash deep tool is a modified version of the dc3dd hashing tool designed especially for digital forensics. This tool includes auto hashing of files, i.e., sha-1, sha-256, and 512, tiger, whirlpool, and md5. An error log file is auto written. Progress reports are generated with every output.

Magic rescue tool:

Magic rescue is a forensic tool that performs scanning operations on a blocked device. This tool uses magic bytes to extract all the known file types from the device. This opens devices for scanning and reading the file types and shows the possibility of recovering files deleted or corrupted partition. It can work with every file system.

Scalpel tool:

This forensic tool carves all the files and indexes those applications which run on Linux and windows. The scalpel tool supports multithreading execution on multiple core systems, which help in quick executions. File carving is performed in fragments such as regular expressions or binary strings.

Scrounge-NTFS tool:

This forensic utility helps in retrieving data from corrupted NTFS disks or partitions. It rescues data from a corrupted file system to a new working file system.

Guymager tool:

This forensic utility is used to acquire media for forensic imagery and has a graphical user interface. Due to its multi-threaded data processing and compression, it is a very fast tool. This tool also supports cloning. It generates flat, AFF, and EWF images. The UI is very easy to use.

Pdfid tool:

This forensic tool is used in pdf files. The tool scans pdf files for specific keywords, which allows you to identify executable codes when opened. This tool solves the basic problems associated with pdf files. The suspicious files are then analyzed with the pdf-parser tool.

Pdf-parser tool:

This tool is one of the most important forensic tools for pdf files. pdf-parser parses a pdf document and distinguishes the important elements utilized during its analysis, and this tool does not render that pdf document.

Peepdf tool:

A python tool that explores pdf documents to find whether it is harmless or destructive. It provides all the elements needed to perform pdf analysis in one single package. It shows suspicious entities and supports various encodings and filters. It can parse encrypted documents too.

Autopsy tool:

An autopsy is all one forensic utility for fast data recovery and hash filtering. This tool carves deleted files and media from unallocated space using PhotoRec. It can also extract EXIF extension multimedia. Autopsy scans for compromise indicator using STIX library. It is available in the command line as well as GUI interface.

img_cat tool:

img_cat tool gives the output content of an image file. The image files recovered will have meta-data and embedded data, which allows you to convert them into raw data. This raw data helps in piping the output to calculate the MD5 hash.

ICAT tool:

ICAT is a Sleuth Kit tool (TSK) that creates an output of a file based on its identifier or inode number. This forensic tool is ultra-fast, and it opens the named file images and copies it to standard output with a specific inode number. An inode is one of the data structures of the Linux system which stores data and information about a Linux file such as ownership, file size, and type, write and read permissions.

Srch_strings tool:

This tool looks for viable ASCII and Unicode strings inside binary data and then prints the offset string found in that data. srch_strings tool will extract and retrieve the strings present in a file and gives offset byte if called upon.

IT REALLY HELPS ME IF YOU UPVOTE.THANKYOU

Comment ❯

Questions viewed by other students

Q: Read the four detective reports and the combined affidavit and warrant for the M57 Patents case. Write a one- to two-page paper describing the evidence the police found and explaining whether they had enough information for the search warrant. Did the information justify taking all the computers and USB drives? Why or why not? Minimize 125.

A: See answer

Q: Cyber Law and Digital Forensics

A: See answer 100% (3 ratings)