Computer forenscis

Technology, Information Technology

Linux in Forensics Linux has various distributions that are very popular mainly because of the stability, better security and open source nature. The various Linux distributions are used for basic operations at home or professional services, for example; in forensic labs (Dixon). Linux has distinct advantages in a forensic lab setting; they are; availability and accessibility; the software is readily available on the internet. The source code is provided, and tools are carefully monitored for bugs. Efficiency; it allows much scripting and automation making it ideal for labs running more casework. Customization and optimization; the source code can be modified; therefore, the OS can be customized to suit the requirements of a particular lab. Support; its Adhoc support is excellent; mailing lists answer calls and provide assistance within minutes. It offers fast implementation of feature and patch requests.

Disadvantages; requires retraining, learning Linux takes time and effort, and the command line is not intuitive. Support; Linux offers no formal support organization. Support queries are direct to the community, and the answer quality varies considerably. Interoperating; interoperating with proprietary technologies is difficult, implementation takes time and may even be incomplete. Volunteer development effort; many projects are in perpetual development stage and may be edgy, poorly documented and abandoned (Wolfe).

In a forensic lab setting, both Linux and Windows have advantages and disadvantages. They are different but employ similar tools. The main difference is the approach taken in obtaining and interpreting the data. Recovery of data is crucial in forensics, and this is where Linux has an upper hand over Windows. Data on Linux is held for months even on heavily used systems. Linux file system avoids file fragmentation, and data remain clustered together. Deleted files are, therefore, easily recoverable on Linux than on Windows. Also, everything in Linux is noted as a file, and this translates to; any transaction occurring in Linux will leave traces (Grundy).

Works Cited

Dixon, P. D. An Overview of Computer Forensics. IEEE Potentials 24. 5 (2005): 7-10. Web.

Grundy, Barry J. The Law Enforcement and Forensic Examiners Introduction to Linux. A Practitioners Guide to Linux as a Computer Forensics Platform 3. 78 (2008): n. pag. Web. 16 Mar. 2015.

Wolfe, Dr. Henry B. Computer Forensics. Computers & Security 22. 1 (2003): 26-28. Web.