Greening Digital Forensics: Opportunities and Challenges

Yap TzeTzuen, Ali Dehghantanha, Andy Seddon, and Seyed Hossein Mohtasebi

Asia Pacific University College of Technology and Innovation
Kuala Lumpur, Malaysia
ypjien@yahoo.com,{ali_dehqan,andy}@ucti.edu.my,
shmohtasebi@gmail.com

Abstract. Despite the fact that digital forensics involves strict procedures and principles, but as this paper presents, there are plenty of opportunities that can be practically employed in digital forensics to make this science greener. Virtualization can cost effectively reduce the number of workstations running forensic tools in the lab. Cloud computing not only facilitate managing and securing services but also decline the number of required network and cooling facilities. Forensic labs can also be optimized regarding environmental preservation. Using remote protocols and digitalizing paperwork procedures are environmentally helpful practices to accelerate investigation progress as well. Employing storage devices with optimal energy usage in digital forensics may highly reduce energy consumption. This paper studies established green technologies particularly in information technology field and suggests a framework for implementing compatible techniques in digital forensics to reduce greenhouse gas pollutants, limit carbon emissions, and preserve the environment.

Keywords: Green forensics, digital forensics, forensic lab.

1 Introduction

Recent years have witnessed a global intention of employing environmentally friendly products and technologies. Digital forensics, on the other hand, involves meticulous procedures, some deliberately redundant (e.g. duplicating data from digital evidence using different tools and storing several copies of that) to insure the accuracy of the investigation process. However a variety of green approaches and efforts might be adapted in digital forensics as well.This paper outlines the opportunities that can be taken for reducing environmental impacts of digital forensics in both forensic labs and crime scenes. It also encompasses challenges that confront with employing common green technologies in digital forensics. The remaining of this paper is organized as follows: Section 2 reviews virtualization and cloud computing, two notorious techniques being employed in green IT. It also delves into environmental conditions and electrical needs of forensics labs. Moreover, the section encompasses effective factors in energy consumption of storage devices. Section 3 proposes a framework for establishing the discussed methods in digital forensic labs. It also suggests some

V.V. Das, E. Ariwa, and S.B. Rahayu (Eds.): SPIT 2011, LNICST 62, pp. 114–119, 2012.

methods and techniques for implementing green digital forensic devices and forensic procedures. Section 4 analyses the proposed approach and the work is finally concluded in Section 5.

2 Literature Review

This section reviews the current state of the art of elements that affect greening digital forensics.

2.1 Virtualization

As stated in Gartner Data Center Conference, virtualization can promote hardware utilization by 5 to 20 times and enables organizations to decrease the number of servers and consequently reduce the power consumption [1].There are also some technologies can be employed for storage virtualization like IBM SAN Volume Controller (SVC) [2] that presents storage devices of a SAN coupled with a virtual pool as only one logical device[1].In addition to server virtualization that lowers costs, improves resource utilization, and increases availability, client virtualization can also be employed for the same benefits [1]. One of the challenges with regard to virtualization is any security threat that exploits a vulnerability of one of the running OSs may affect other OSs and services as well. Additionally, if a machine that provides several services, rather than one, goes down, then all services hosted on the machine will be shutting down [3]. Gartner has estimated that, by 2012, 60 percent of virtualized servers will be not as secure as physical machines that they have been replaced with [4]. Liu et al. [5] propose that a different IP is assigned to each virtual machine (VM) running on a machine. Each of VMs should be also separated from the rest using distinct virtual LANs (VLAN) and the only way a VM to connect to another VM should be through layer 3 network devices [5]. Using routers feature firewall for transmitting data between VLANs can minimize the risk of being infected by malicious software [5]. Even after applying this method still less network devices such as network interface controllers (NIC), cables, and switches are used [1].

2.2 Cloud Computing

Cloud computing optimizes and control resource usage by leveraging a measuring capability suitable for the type of service [6].Cloud computing environments are twofold, termed, public and private [7]. In public cloud computing environment, users communicate with servers using the Internet while private cloud computing environment is isolated from the outside world by means like firewall [7]. The common specification of two types is rather than equipping numerous workstations, strong servers with optimized configuration are run and managed.There are three types of cloud computing services as follows: (1) storage as a service, (2) processing as a service, and (3) software as a service [7]. In storage as a service as its name suggests, user stores their data in the cloud while in processing as a service user outsources intensive tasks to cloud [7]. Software as a service involves both of these

services and allows user to put all their tasks to cloud [7].Baliga et al. [7] compared these types with regard to transport, storage, and processing which their results is presented in Table 1.

Table 1. High Energy Consumption in Cloud Computing with Regard to Cloud's Type

Factor	Software as Service	Storage as a Service	Processing as a Service
Transport	High frame rates	High download rate	Never
Storage	Never	Low download rate	-
Processing	Few users per server	High download rate	Medium to high encoding per week

Power Usage Effectiveness (PUE) and Data Center Infrastructure Efficiency (DCiE) are two metrics used for determining the energy efficiency of data centers, although they do not cover the whole scope of data center [1]. Equations (1) and (2), respectively, demonstrate how PUE and DCiE are calculated [8, 9].

$$PUE = \frac{\text{Total Facility Power}}{\text{IT Equipment Power}} \tag{1}$$

$$DCiE = \frac{\text{IT Equipment Power}}{\text{Total Facility Power}} \tag{2}$$

2.3 Environmental Conditions of the Lab

There are requirements specified for building and developing a digital forensic lab. These requirements and standards are stated in ASCLD/LAB and ISO/IEC 17025. One of the standards that the ASCLD/LAB requires for a laboratory to have is to provide a comfortable working environment for the employees [10]. One of the issues here is the cooling system in a lab. To save the cost of the electricity used by digital forensic lab, cooling fans or a good ventilation system is installed and can decline the waste of energy [1]. Unlike normal chemical lab systems can be designed to look alike of a normal office that has a low-velocity air handling system, resulting in substantial energy savings [11]. A proper energy saving lighting bulbs and tubes have the certification from the Energy Star program that promotes in protecting the environment and save money [17].

2.4 Storage Devices

Hard disk drives (HDD) are the most frequently used device being employed for storing data and HDD with high capacity typically use higher energy. There are models of HDDs in the market that use less energy and makes less heat. For instance, a Western Digital HDD consumes 5 watts less than a normal HDD [13]. Storage technologies like

NAND flash memory based SSD (Solid State Disk) in comparison with traditional HDDs waste less energy and at the same time provide more reliable services [14].Additionally, there are technologies which optimize power usage. MAID (Massive Array of Idle Disk) is an example that switches off idle HDDs [14, 15].

3 Proposed Approach

Our proposed framework is composed of four parts as follows as discussed in the rest of this section.

3.1 Virtualization and Consolidation

Installing multiple forensic tools with similar functionality on the same OS is deprecated [16]. The most elegant way to deal with these issues is employing VMs. Employing private cloud computing with optimal severs that provide services to multiple forensic investigators can significantly reduce the energy consumption.It also consolidates services and data and as a result it eases managing and securing them. As Table 1 demonstrates, in cloud computing energy consumption is dependent upon cloud type as well as the number of users. Since employing either virtualization or cloud computing will result in placing fundamental servers in data centers, improvement in cooling efficiency of data centers can conserve a considerable amount of energy.Metrics like PUE and DCiE can be employed for finding the efficiency of data centers.

3.2 Environmental Conditions of Lab

The heating, ventilation and air conditioning systems of a digital forensic lab can be designed similar of a normal office that requires low-velocity air system. Low-velocity air system consumes less amount of energy.Ventilation system can be installed for the digital forensic lab rather than using air conditioners, thus resulting in reducing the green house effect. Unlike air conditioning system, the usage of energy is lesser and there of no promoting of energy wastage by the ventilation system. Furthermore, to help in reducing the energy consumption of the lab, an energy saving lightning system should be installed. To maintain the energy consumption at a certain level and also to reduce the waste of energy on the digital forensic lab, energy recovery can be employed.

3.3 Storage Devices

Duplicating data stored on digital evidence and keeping several copies of them is an important stage in any digital forensics investigations. Therefore, using appropriate storage devices that consume less energy like modern HDDs and NAND flash memories can significantly reduce the overall power consumption in digital forensic investigations.Workstations connected to cloud environments do not need to have HDDs

with high capacity since HDDs with higher capacity consume more energy.Optimizing energy consumption using technologies like MAID is helpful for those servers of forensic lab that need large disk arrays.

3.4 Forensic Devices

Replacing energy sources of these devices with renewable energy sources can effectively reduce environmental impacts.Additionally, as far as possible instead of using hazardous materials, recyclable ones should be employed. Batteries are an exemplar of these materials.Equipping digital forensic devices like data acquisition tools with remote functionality can speed up the investigation process and at the same time it reduces unnecessary traveling.Many manual paperwork tasks such as chain of custody forms can be digitalized using mobile applications run on tablets or smartphones that are already carried by investigators.

4 Analysis of Proposed Framework

Virtualization reducesrequired digital facilities in forensic labs. Since in cloud computing servers are consolidated in data centers rather than being distributed in different parts of organization's building, optimizing cooling systems and the structure of data center can noticeable decline energy consumption.There are also factors like licensing that needed to be taken into consideration.

Consuming less energy means promoting less burning of bio-fuel that produces carbon's footprint. By using computers that have low power consumption than the normal ones, the electricity usage in the lab should be reduced. It is noted that these low power consuming equipments can perform better than the normal ones. Since the low power consumption computers can perform in a better speed, there is possibility that the time duration of an examiner to investigate digital evidences can be shorten. Equipping mobile forensic devices with remote access and using secure protocols for transmitting data may reduce travelling of investigators. Instead of using papers for recording investigation process tablets can be used to facilitate investigation progress.

5 Conclusion and Future Work

The proposed framework in the paper may not be the best but in the future, there is always a better solution that can be adapted into the digital forensic lab for the purpose of being environment friendly and also promoting the idea of going green. Another suggestion to reduce carbon's footprint is to adapting green procedures in the digital forensic lab. Certain duration of time is needed for the employees in digital forensic lab to become accustomed to the new procedures. Outstanding results can be seen after that period of time which reduces greenhouse effect and promoting green digital forensics.

References

[1] Lamb, J.: The Greening of IT: How Companies Can Make a Difference for the Environment. IBM Press (2009)

[2] IBM System Storage SAN Volume Controller, http://www-03.ibm.com/systems/storage/software/virtualization/svc

[3] Gorge, M.: Are we being greenwashed to the detriment of our organisations' security? Computer Fraud & Security 2008(10), 14–18 (2008)

[4] Gartner Says 60 Percent of Virtualized Servers Will Be Less Secure Than the Physical Servers They Replace Through 2012 (2010), http://www.gartner.com/it/page.jsp?id=1322414

[5] Liu, J., Lai, W.: Security analysis of VLAN-based Virtual Desktop Infrastructure. In: International Conference on Educational and Network Technology (ICENT), pp. 301–304 (2010)

[6] Mell, P., Grance, T.: The NIST Definition of Cloud Computing (Draft), National Institute of Standards and Technology (2011)

[7] Baliga, J., Ayre, R.W., Hinton, K., Tucker, R.S.: Green Cloud Computing: Balancing Energy in Processing, Storage, and Transport. Proceedings of the IEEE 99(1), 149–167 (2011)

[8] PUE Data Center Efficiency Metric - Data Center Benchmarks and Certifications, http://www.digitalrealtytrust.com/pue-efficiency.aspx

[9] What is data center infrastructure efficiency (DCIE) (2008), http://searchdatacenter.techtarget.com/definition/data-center-infrastructure-efficiency-DCIE

[10] The American Society of Crime Laboratory Directors/Laboratory Accreditation Board (ASCLD/LAB) (2011), http://www.ascld-lab.org/forms/intlrequirements.html

[11] Digital Forensic Investigator News, http://www.dfinews.com/article/architectural-and-engineering-design-requirements-digital-forensic-facility?page=0,0

[12] Ken, M., Michael, C.: Sustainable 'Green' Forensic Laboratory Design, Forensic Magazine (2006), http://www.forensicmag.com/article/sustainable-green-forensic-laboratory-design

[13] Velte, T., Velte, A., Elsenpeter, R.: Green IT: Reduce Your Information System's Environmental Impact While Adding to the Bottom Line, 1st edn., pp. 51–53. McGraw-Hill Osborne Media (2008)

[14] Zhang, X., Zhao, X., Lin, Y., Zeng, L.: Key Technologies for Green Data Center. In: 2010 Third International Symposium on Information Processing (ISIP), pp. 477–480 (2010)

[15] Colarelli, D., Grunwald, D.: Massive Arrays of Idle Disks For Storage Archives. In: ACM/IEEE 2002 Conference, p. 47 (2002)

[16] Jansen, W., Ayers, R.: Guidelines on Cell Phone Forensics, National Institute of Standards and Technology (2007)

[17] Energy Star, http://www.energystar.gov/index.cfm?c=about.ab_index