Chapter 9: Conclusion and Future Work

This thesis presented a study on applying digital forensics techniques in cloud computing environment for the investigation of cybercrimes in forensically sound and timely fashion. In this chapter, the work conclusion is introduced in Section 9.1 and the future research direction is presented in Section 9.2.

9.1 Conclusion

This work concerned with developing proficient digital forensic techniques for investigation of cybercrimes in cloud computing environment in forensically sound and timely manner. It is introduced research contributions in the field of cloud forensics. They can be summarized as follows:

- A literature review is done to explore and identify challenges and opportunities for performing digital forensics investigation in the cloud computing environment. The identification of cloud forensic challenges and opportunities such as secure and forensic analysis of cloud storage services, log data analysis, design cloud computing model to support digital forensics, design cloud-based forensic laboratory which helped us to accomplish and complete this research work.

- A cloud forensic approach based on data integrity checking for assisting and helping digital investigators is proposed for performing automatic digital forensics for box cloud storage as a case study. The experiment results showed that there are data artifacts that remain in the user machine that uses Windows 7 about using box cloud storage such as IP address, and user account information like a username. The proposed approach can potentially useful tool for performing cybercrimes investigation related to cloud storages.

- A forensic approach is introduced for analysis large size of log files to extract knowledge which can assist digital investigators and examiners during the investigation of cloud-based crimes that occurred through a particular time. In this approach, we used Apache Hadoop and Apache Spark for analysis web log data. Apache Hadoop for analysis of log data is used while an Apache Spark is used to provide batch and real-time analysis of
web server log data. In each approach, three different programs are implemented and tested on three different log files in size. Each program extracts the different type of information that can help digital investigators in reconstructing timeline related crimes that are occurred. The results show that Apache Hadoop and Apache Spark can be used as fast platforms for processing various large size of log files and extract beneficial information that can support digital investigators in analysis massive amount of cloud log data in a given frame time as well as reconstructed timeline related to incidents. Furthermore, the results can provision to reconstruct and generate a timeline related to historical past sequence events occurred during a crime as well as identify the malicious user’s IP address, date and time, with the number of access.

- A forensic approach is provided for investigation of cybercrimes in a private cloud environment. The proposed approach can help digital investigators and practitioners in acquisition and collection of digital evidence from the private cloud infrastructures especially virtual machine which is considered the essential element of virtualized cloud systems. In additions to can collect and extract information from the client device, hypervisor, and hypervisor management system to facilitate the investigation process in an effective manner. Also, presented a forensic methodology which can be used for investigating and analyzing virtual machine and its snapshots for assisting in the reconstruction of criminal activities which done using a virtual machine.

- An efficient forensic acquisition application called Hypervisor Forensic Acquisition Application (HFAA) is proposed for the acquisition of digital evidence clustered VMware ESXi servers. The design of proposed application can support to scale in a dynamic cloud computing environment where distributed clusters of hypervisors that share virtual machines and storage for providing better and on-demand services. This application aims to be utilized for extracting digital evidence from clustered VMware ESXi hypervisors for assisting the digital investigators in performing the digital investigation process. This application is an initial step for the digital investigators, practitioners, and researchers to develop new approaches and methods for evidence acquisition and extracting from clustered VMware ESXi hypervisors and hosted virtual machines in a forensically sound and timely manner. With some supplementary
development through adding new features to the proposed application, this can make it as a good tool to be used in cloud forensic area.

- A novel Cloud Forensics Investigation Model (CFIM) to investigate cybercrimes in the cloud environment is proposed. The proposed system is a smart system that is able to take a snapshot of the state of running virtual machine in virtual data center and send to Trusted Center Server (TCS) that monitor the status of the VMs as well as store snapshots of the virtual machines for sending them for Forensic Server (FS) up to require for performing forensics process. The proposed model supports a concept of Forensics as a Service (FaaS) that provide various benefits of conducting digital forensics through using Forensic Server on the cloud side. The implementation of the proposed model within cloud architecture can increase the probability of tracking malicious users in the cloud environment, determine weaknesses in cloud services such as a virtual machine for future use as well as support cloud forensics investigations.

A Cloud Forensic Laboratory (CFL) is introduced which is based on using cloud computing capabilities for investigation of cybercrimes that are a cloud or classical IT based. The proposed CFL can decrease the time that required to investigate cybercrimes in the cloud through using enormous capabilities of cloud computing. Finally, a forensic report can be generated about the committed crime for presenting it in a court of law as admissible proof. The proposed system can improve the investigation process by providing an environment for the digital investigators and experts to access various forensic tools and test environments remotely. Also, the proposed system can help the digital investigators and practitioners to perform the digital investigation process.

9.2 Open Problems and Future Work
The work carried out in this thesis leaves a number of open questions which are worth addressing in the future as follows:

- Design new hypervisor investigation procedures.
- Develop and design procedures and tools to segregate forensic data between multiple tenants in the cloud.
- Collaboration between international law enforcement agencies in cloud forensics.
- Providing proactive measures can significantly facilitate cloud forensic investigations.
- Providing changes in Service-Level Agreement (SLA) to support and facilitate forensic readiness in the cloud.
- Design and implement new methods to recover the deleted data, identify the ownership of the deleted data, and use the deleted data for event reconstruction in the cloud.
- Extending and modifying the current investigation tools to use them in the cloud computing environment.
- Developing new versions to perform more sophisticated forensic acquisition process on clustered VMware ESXi hypervisors as well as fixed the limitations mentioned above by adding more useful features.
- Implement the proposed cloud forensics model with OpenStack, which support different types of hypervisors such as Microsoft Hyper-V, Citrix XenServer, and Oracle VM. In addition, integrate an intrusion detection and prevention system to reduce digital forensics process cost and time.