**Design and implementation of FROST: Digital forensic tools**

**for the OpenStack Cloud Computing Platform**

Josiah Dykstra\*, Alan T. Sherman

Cyber Defense Lab, Department of CSEE, University of Maryland, Baltimore County (UMBC), 1000 Hilltop Circle, Baltimore, MD 21250,

United States

**Abstract**

We describe the design, implementation, and evaluation of FROST dthree new forensic

tools for the OpenStack cloud platform. Our implementation for the OpenStack cloud

platform supports an Infrastructure-as-a-Service (IaaS) cloud and provides trustworthy

forensic acquisition of virtual disks, API logs, and guest firewall logs. Unlike traditional

acquisition tools, FROST works at the cloud management plane rather than interacting

with the operating system inside the guest virtual machines, thereby requiring no trust in

the guest machine. We assume trust in the cloud provider, but FROST overcomes nontrivial

challenges of remote evidence integrity by storing log data in hash trees and

returning evidence with cryptographic hashes. Our tools are user-driven, allowing customers,

forensic examiners, and law enforcement to conduct investigations without

necessitating interaction with the cloud provider. We demonstrate how FROST’s new

features enable forensic investigators to obtain forensically-sound data from OpenStack

clouds independent of provider interaction. Our preliminary evaluation indicates the

ability of our approach to scale in a dynamic cloud environment. The design supports an

extensible set of forensic objectives, including the future addition of other data preservation,

discovery, real-time monitoring, metrics, auditing, and acquisition capabilities.

ª 2013 Josiah Dykstra and Alan T. Sherman. Published by Elsevier Ltd. All rights reserved

Isi dari abstract diatas yaitu tentang bagaimana mendesain *Cloud Computing* Openstack dan tentang bagaimana cara menenmukan bukti-bukti digital dan akuisisi dari disk virtual dan pengimplementasi alat untuk melakukan digital forensik untuk platform Openstack dan alat bernama FROST ini dapat berinteraksi dengan sistem operasi pada mesin virtual tamu sehingga membutuhkan hak akses dari mesin virtual tamu dan dan disini kami sebagai designer digital forensic percaya dengan penyedia *cloud computing* alat forensik ini yaitu FROST menyediakan alat yang memungkinkan pelanngan melakukan pemerikasaan dan penyidikan tanpa memerlukan interaksi dengan provider penyedia *Cloud Computing* dan disini ditunjukkan bagaimana FROST yang abru dapat mengaktifkan fitur peneyelidik forensic untuk memperoleh data forensic dari Peneyedia Vloud Computing Openstack evaluasi awal ini menunjukkan kemampuan pendekatan untuk skala lingkungan *Cloud* Dinamis desain in mendukung extensible seperangkat tujuan dari digital forensik data, monitoring secara *real time*

**Sumber :**

Dysktra, Josiah. dan Sherman, Alan T. 2013. *Design and Implementation of FROST : Digital Forensic tools for the OpenStack Cloud Computing Platform* diambil dari <https://www.journals.elsevier.com/digital>-ivestigation