Forensiccloud
An Architecture for Digital Forensic Analysis in the Cloud

Dr. David A. Dampier
Professor of Computer Science and Engineering
Director of the Distributed Analytics and Security Institute at Mississippi State University

Cody Miller
Research Associate, Distributed Analytics and Security Institute at Mississippi State University
Introduction

• The amount of data that needs to be processed during a examination continues to rise
• There is a backlog of cases and low priority cases may take months to process
• Rural departments may not have access to forensic workstations
Types of Clouds: Infrastructure as a Service

• Provisions for:
  • Processing Power
  • Storage Capacity
  • Network Capacity
  • Fundamental Computing Resources

• Consumer decides what software to run on the infrastructure provided.
  • Operating System
  • Applications
Types of Clouds: Platform as a Service

• Consumer runs applications either developed in house or purchased as they will

• No control over platform at all:
  • Operating System
  • Network
  • Servers
  • Storage
Types of Clouds: Software as a Service

- Everything runs in the cloud
- Software is made available in the cloud
- No control over resources
- Access through thin-client interface
Benefits of the Cloud

• On-demand self-service
• Broad network access
• Resource pooling
  • Funding
  • Infrastructure
• Rapid elasticity
• Measured service
Forensicloud

• Forensicloud is a cloud-based solution for performing digital forensic investigations with a limited technology investment on the client side.
• Forensicloud is a cross between an IaaS and SaaS
• Forensicloud is a hybrid cloud – only selected departments will have access to it
• All the investigator needs is a thin client to connect
• Virtual machines are used to provide investigators a secure environment in which to conduct an examination
Typical Forensics Process

1) Acquire the original and make copies for analysis
2) Authenticate the copies against the original
3) Analyze copy for evidence
   • In a cloud environment evidence must be transferred to the cloud first
     • Small amounts of data (reports, logs, etc) can be transferred to and from Forensicloud using the thin client.
     • Large amounts of data (evidence) will have to be transferred at the Forensicloud location
       • These drives could be shipped to the Forensicloud
       • Alternatively, the state could establish upload stations around the state with high speed internet connections
Forensicloud

• Virtualization is used to control and isolate the virtual machines

• Back end processing can be done on a simple set of cloud servers, or can include high performance clusters
  • *Recent Journal Publication:*

• A civilian version of the Forensicloud may be useful to attorneys
  • They would gain access to the tools and potential technical assistance from experts employed by the provider
Virtual Desktop Infrastructure

- Virtual desktop infrastructure (VDI) provides a method for investigators to access the virtual machine
- VDI provides both input (keyboard, mouse, etc.) and output (monitor, sound, etc.) for the virtual machine

[1]
Improvements to the Forensic process

• Allows a remote investigator to investigate evidence from any location with Internet access

• Forensic products are licensed for each virtual machine, which allows sharing of licenses
  • In a small state, you may only need 20 or so copies of commercial software for 100 or more departments

• Cloud resources can store and analyze a far greater amount of evidence than most local department forensic workstations can
Improvements (cont.)

• Forensicloud provides high user accountability because all actions are logged
• Forensicloud offers redundancy of data, which among other things provides data safekeeping
Vision for Forensicloud

• Small states like Mississippi and Alabama would likely have one cloud server

• Larger states might require multiple servers at different locations
  • However, these locations would be connected to each other

• This server would be available to every law enforcement agency in the state to conduct investigations on their own thin clients
Vision for Forensicscloud (cont.)

• Agencies would request accounts on the server for their cyber crime investigators, and the investigators would interact with the server.

• Investigators would conduct their investigation remotely. However, if they needed assistance, they can request access from state level investigators who could assist them.

• They could also turn over cases to the state or federal authorities much easier.
  • Access to a department’s case can be granted through the cloud to state or federal investigators.

• Additionally, read-only access can be granted to supervisors, prosecutors, etc., they can see the progress of the case, but not change anything.
Conclusions

- Cyber Investigators need a way to investigate computer evidence, but the equipment is expensive for smaller departments, especially when they may only have one or two cases a year
  - A reasonable lab costs a minimum of $10K to buy and then probably would have to be replaced completely in three to five years.
- A centralized source for hardware and software takes advantage of scale and resource sharing
Future Work

• Future prototypes will use an HPC cluster to process evidence

• More research needs to be done to determine better ways to transfer the evidence to the Forensicloud
Demonstration
Questions?

Dr. Dave Dampier
dampier@dasi.mssate.edu
662-325-0779

Cody Miller
miller@dasi.mssate.edu