Cloud Forensics Challenges
Assessing Cloud Computing’s Impact on Digital Investigation

Dr. Keyun Ruan
NIST Cloud Forensic Science Working Group
10 Jan, 2012
Measuring the cost of cyber crime...
“We should spend less in anticipation of cybercrime (on antivirus, firewalls, etc.) and more in response, i.e., the prosaic business of hunting down cyber criminals and throwing them in jail.”

Source: Anderson et al. (2012) ‘Measuring the Cost of Cyber Crime’
What is Cloud Forensics?
• Law enforcement perspective
• Security perspective
• Traditional digital forensic challenges
• Digital forensics in the cloud ecosystem
Source: NIST 500-292 Cloud Computing Reference Architecture
• Split of control
• Segregation of duties
• Chain of dependencies
• Lack of transparency
Legal Challenges
• Multi Jurisdiction
• Multi Tenancy
• Data Ownership
• Privacy
• Service Level Agreement
Technical Challenges
• Hybrid forensic acquisition (live, virtual, large-scale, thin-client, thick-client, remote..)

• Evidence segregation

• Data location

• Time synchronization

• Log management

• Identity and anonymity

• Data recovery

• Proliferation of endpoints

• Encryption

• Interoperability

• ....
Survey on Cloud Forensics and Critical Criteria for Cloud Forensic Capability

• 257 respondents
• 32% of the respondents hold Bachelor (or Diploma) degrees, 41% of the respondents hold Master degrees, and 19% of the respondents hold Doctoral degrees.
• 15% of the respondents have 1-2 years of experience, 14% of the respondents have 3-4 years of experience, and 51% of the respondents have >5 years of experience.
• 76% of them claim to be “very familiar” or “familiar” with digital forensic tools.
Cloud Forensics Definitions

- A mixture of traditional computer forensics, small scale digital device forensics, and network forensics
  - Agree or Strongly Agree: 61%
  - Strongly Agree: 17%
  - Agree: 24%
  - Neutral: 44%

- An interdisciplinary area between digital forensics and cloud computing, although both definitions of digital forensics and cloud computing are still under discussion
  - Agree or Strongly Agree: 57%
  - Strongly Agree: 12%
  - Agree: 31%
  - Neutral: 45%

- An application of digital forensics in cloud computing
  - Agree or Strongly Agree: 61%
  - Strongly Agree: 11%
  - Agree: 26%
  - Neutral: 50%

- Cloud forensics is a brand new area
  - Agree or Strongly Agree: 42%
  - Strongly Agree: 12%
  - Agree: 30%
  - Neutral: 42%

- Cloud forensics is Internet forensics
  - Agree or Strongly Agree: 49%
  - Strongly Agree: 4%
  - Agree: 23%
  - Neutral: 72%

- Cloud forensics is network forensics
  - Agree or Strongly Agree: 56%
  - Strongly Agree: 8%
  - Agree: 28%
  - Neutral: 64%

- Cloud forensics is classical computer forensics
  - Agree or Strongly Agree: 48%
  - Strongly Agree: 3%
  - Agree: 26%
  - Neutral: 71%
Digital Forensics is: the use of scientifically derived and proven methods toward the preservation, collection, validation, identification, analysis, interpretation, documentation, and preservation of digital evidence derived from digital sources for the purpose of facilitating or furthering the reconstruction of events found to be criminal, or helping to anticipate unauthorized actions shown to be disruptive to planned operations. (DFRWS 2001)
Proposed definition: Cloud forensics is the application of digital forensic science in cloud computing environments. Technically, it consists of a hybrid forensic approach (e.g., remote, virtual, network, live, large-scale, thin-client, thick-client) towards the generation of digital evidence. Organizationally it involves interactions among cloud actors (i.e., cloud provider, cloud consumer, cloud broker, cloud carrier, cloud auditor) for the purpose of facilitating both internal and external investigations. Legally it often implies multi-jurisdictional and multi-tenant situations.
Significance of Cloud Forensics

Important component of cloud security
- Agree or Strongly Agree: 81%
- Strongly Agree: 32%
- Agree: 49%
- Neutral: 13%

As important as cloud security
- Agree or Strongly Agree: 78%
- Strongly Agree: 28%
- Agree: 50%
- Neutral: 18%

There will be a lack of awareness until a major critical incident happens
- Agree or Strongly Agree: 72%
- Strongly Agree: 31%
- Agree: 41%
- Neutral: 20%

Needs more funding and investment in R&D than it has got at the moment
- Agree or Strongly Agree: 77%
- Strongly Agree: 32%
- Agree: 45%
- Neutral: 21%
Cloud Forensics Usage

- Troubleshooting: 21%
- Log monitoring: 34%
- Due diligence: 40%
- Data and system recovery: 46%
- Regulatory compliance: 51%
- Investigations on digital crimes, civil cases, policy violations, etc.: 80%
- Others: 10%
Impact of cloud computing on digital forensics

46% of the respondents believe that “cloud computing makes forensics harder”
37% of the respondents believe that “cloud computing makes forensics easier”.

Comments on why “cloud computing makes forensics harder”:

• Reduced access to remote and distributed physical infrastructure and storage
• Lack of physical control and physical location of data
• Lack of standard interfaces
• Legal issues including multiple ownership, multiple jurisdictions, and multiple tenancies
• Lack of collaboration from the cloud provider(s)
• Evidence segregation
• Data recovery

Comments on why “cloud computing makes forensics easier”:

• Cloud investigations can leverage characteristics of cloud computing, e.g., computing power on demand, elasticity, distributed forensic processing, as well as scalable auditing, reporting, logging, imaging and testing. Forensic implementations in the Cloud can also be cheaper.
• Cloud investigations will be highly dependent on provider providing digital evidence through centralized administration and management, so there will be less work for the investigator/law enforcement side.
• Evidences in cloud environments are harder to destroy by the criminals as they maybe mirrored to multiple locations
Cloud Forensic Dimensions

• 80% of the respondents agree that there is a “technical” as well as “legal” dimension for cloud forensics
• 69% of the respondents agree that there is an “organizational/administrative dimension” for cloud forensics
• 43% of them agree that there is a “social dimension” for cloud forensics
• 14% of the respondents clicked “other” dimensions
• “Political” and “personal” dimensions have been mentioned in the comments
Challenges for Cloud Forensics

- Unification of log formats: 57% Significant or Very Significant, 46% Very Significant, 1% Significant, 1% Neutral
- Synchronization of timestamps: 59% Significant or Very Significant, 44% Very Significant, 5% Significant, 1% Neutral
- Different providers have different approaches to cloud computing: 67% Significant or Very Significant, 46% Very Significant, 6% Significant, 1% Neutral
- Limited investigator power given to the investigators or consulting firms to legally obtain data under respective jurisdictions in civil cases: 69% Significant or Very Significant, 39% Very Significant, 9% Significant, 1% Neutral
- Missing terms and conditions in SLA (Service Level Agreement) regarding investigations: 73% Significant or Very Significant, 50% Very Significant, 19% Significant, 2% Neutral
- Lack of legislative mechanism facilitating evidence retrieval involving confidential data: 75% Significant or Very Significant, 46% Very Significant, 16% Significant, 3% Neutral
- Lack of forensic expertise: 76% Significant or Very Significant, 40% Very Significant, 18% Significant, 1% Neutral
- Exponential increase of digital (mobile) devices accessing the Cloud: 77% Significant or Very Significant, 50% Very Significant, 20% Significant, 1% Neutral
- Segregation of forensic data in an infrastructure shared by multiple users (multitenant environment): 72% Significant or Very Significant, 39% Very Significant, 21% Significant, 3% Neutral
- Simple role management (e.g. admin, user) makes it difficult to categorize suspects: 51% Significant or Very Significant, 36% Very Significant, 16% Significant, 1% Neutral
- Lack of law/regulation and law advisory: 81% Significant or Very Significant, 47% Very Significant, 13% Significant, 1% Neutral
- Decreased access to and control over forensic data at all levels from customer side: 78% Significant or Very Significant, 42% Very Significant, 17% Significant, 2% Neutral
- Investigating external chain of dependencies of the cloud provider (e.g. a cloud provider can use the service from another provider): 80% Significant or Very Significant, 50% Very Significant, 30% Significant, 1% Neutral
- Lack of international collaboration and legislative mechanism in cross-nation data access and exchange: 85% Significant or Very Significant, 47% Very Significant, 38% Significant, 2% Neutral
- Jurisdiction: 90% Significant or Very Significant, 60% Very Significant, 20% Significant, 1% Neutral
- Ineffective encryption key management makes it easier to lose the ability to decrypt forensic data stored in the Cloud: 48% Significant or Very Significant, 44% Very Significant, 16% Significant, 2% Neutral
- Single points of failure: 38% Significant or Very Significant, 39% Very Significant, 25% Significant, 4% Neutral
Top Challenges (>75%)

- Jurisdiction
- Lack of international collaboration and legislative mechanism in cross-nation data access and exchange
- Lack of law/regulation and law advisory
- Simple role management (e.g. admin, user) makes it difficult to categorize suspects
- Investigating external chain of dependencies of the cloud provider (e.g., a cloud provider can use the service from another provider)
- Decreased access to and control over forensic data at all levels from customer side
- Exponential increase of digital (mobile) devices accessing the cloud
Opportunities for Cloud Forensics

Dedicated forensic implementations are more cost-effective when applied on a larger scale and offered as part of the cloud infrastructure.

Establishment of a foundation of standards and policies for forensics that will evolve together with the technology.

Forensics-as-a-Service (using cloud computing to deliver forensic services).

The scalability and flexibility of the Cloud enables elastic and unlimited storage of logs and increases efficiency of indexing, searching and various queries of logs, etc.

Default technologies provided in the Cloud such as automatic MD5 checksums can improve the overall robustness of forensics in the Cloud.

There are more chances to find critical evidence left in the Cloud due to data abundance.

Agree or Strongly Agree | Strongly Agree | Agree | Neutral
Top Opportunities

• Establishment of a foundation of standards and policies for forensics that will evolve together with the technology
• Dedicated forensic implementations are more cost-effective when applied on a larger scale and offered as part of the cloud infrastructure
• Forensics-as-a-service (using cloud computing to deliver forensic services)
Parties to be Assessed for Cloud Forensic Capability

- Cloud end user: 36%
- Internet service provider: 38%
- Cloud consumer: 53%
- Cloud Service Provider: 78%
Critical Criteria for Cloud Forensic Capability

- A guideline on forensic reporting to ensure reporting follows consistent and standard format: 71%
- A guideline on internal collaboration between various functional teams in cases of investigation in the cloud organization: 80%
- A guideline on external collaboration between the cloud organization and other cloud organization(s), law enforcement, etc. in cases of investigation: 83%
- An agreement on the access and control over forensic data at all levels between cloud organizations: 73%
- An agreement on the division of responsibilities among all parties involved (cloud organizations, law enforcement, etc.) in cases of investigation: 76%
- Tools provided, techniques supported, access granted regarding forensic investigation should be included in the SLA (Service Level Agreement): 82%
- An agreement on the recording of the chain of custody among all parties in an investigation: 88%
- A policy in the cloud organization to reinforce proactive collection of forensic-relevant data in the Cloud: 84%
- A policy in the cloud organization to ensure all forensic procedures are performed in a standard fashion: 85%
- Legal experts in the cloud organization or externally assisting the cloud organization on multi-jurisdiction/multi-tenant issues regarding: 75%
- Forensic staff in the cloud organization provided with up-to-date training on cloud forensic knowledge: 83%
- A team of forensic staff in the cloud organization or externally assisting the cloud organization on forensic investigations in the Cloud: 84%
Conclusions

• The survey was circulated when cloud technology was still rapidly evolving, but a working definition of cloud forensics is proposed based on the analysis and discussions of survey results.
• Areas of critical importance for research and development are identified and agreed among respondents.
• Respondents have researched consensus that cloud forensics poses significant challenges to digital forensics, and a list of top challenges is concluded from the survey results.
• There is a need in the establishment of cloud forensic capabilities including a set of toolkits and procedures for cloud investigations, however, cloud forensics also brings opportunities especially in areas of standard acceleration, integrated forensic implementations, as well as Forensics-as-a-Service, which should not be neglected.
Thanks!

“The first requisite of civilization is that of justice.”

----- Sigmund Freud

Keyun Ruan
keyun.ruan@ucd.ie