CLOUD FORENSICS:
CHALLENGES & OPPORTUNITIES

Keyun Ruan, University College Dublin

About Me

- PhD candidate in Cloud Forensics, Center for Cyber Crime Investigation, University College Dublin
- Diploma in Art and Design, National College of Art and Design, Ireland
- Editor, **Cybercrime and Cloud Forensics: Applications for Investigation Processes** (to be published by IGI Global in 2012)
- RuanKeyun.com
- CloudForensicsResearch.org

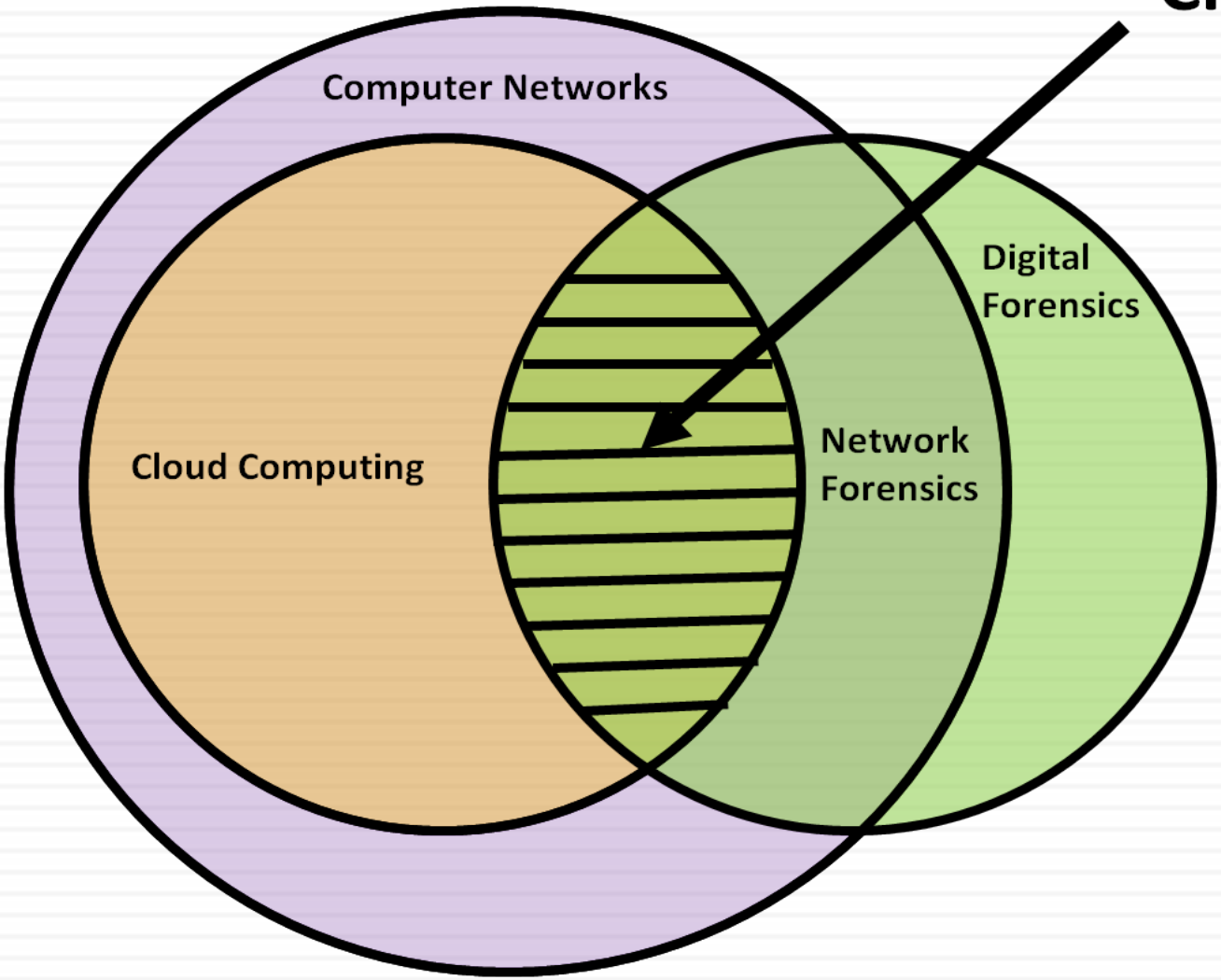
Cloud Forensics

What is Cloud Forensics

Usage of Cloud Forensics

The 3 Dimensions of Cloud Forensics

What is Cloud Forensics?



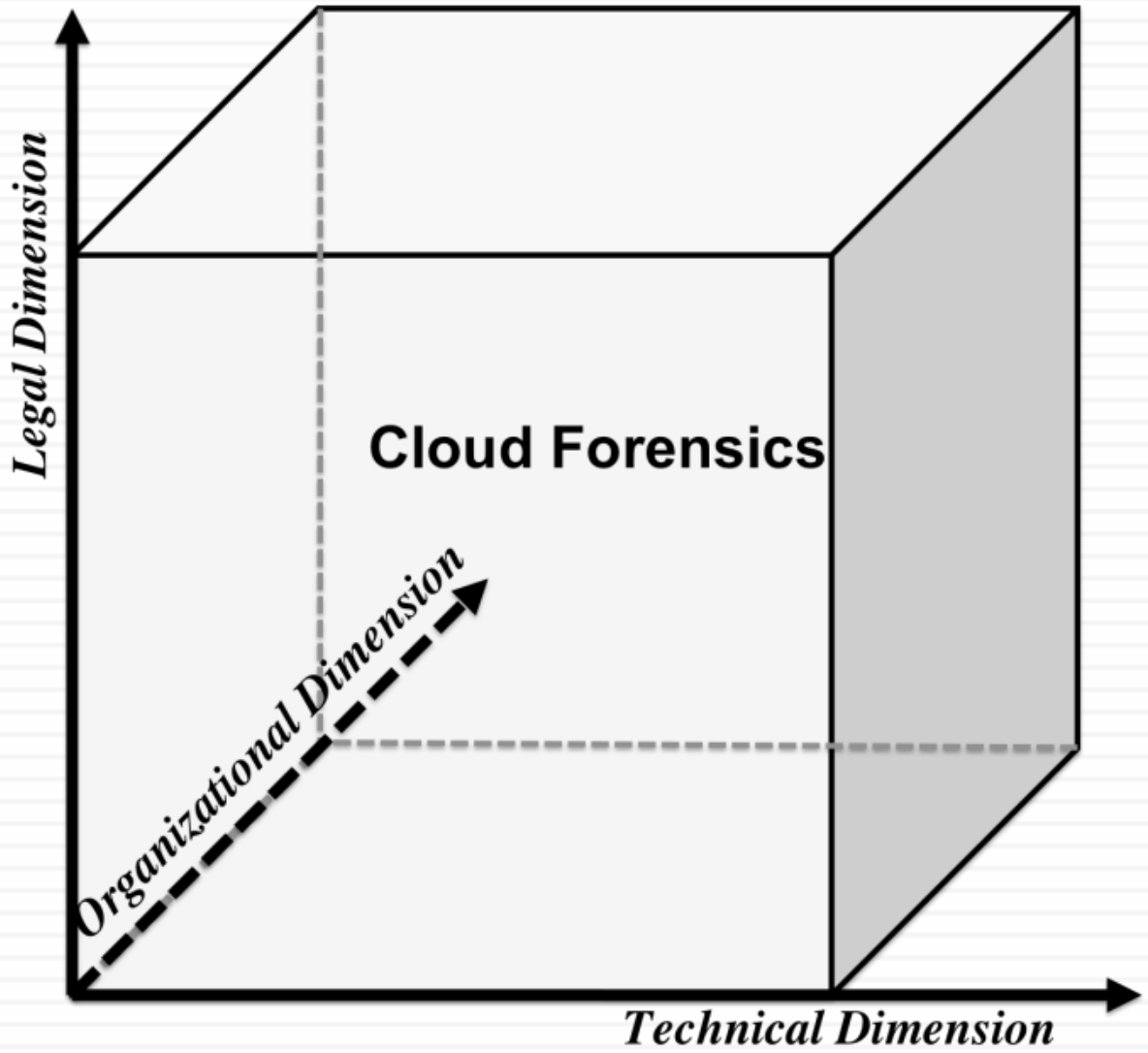
Cloud Forensics

1. Cross discipline between Cloud Computing and Digital Forensics
2. Subset of Network Forensics

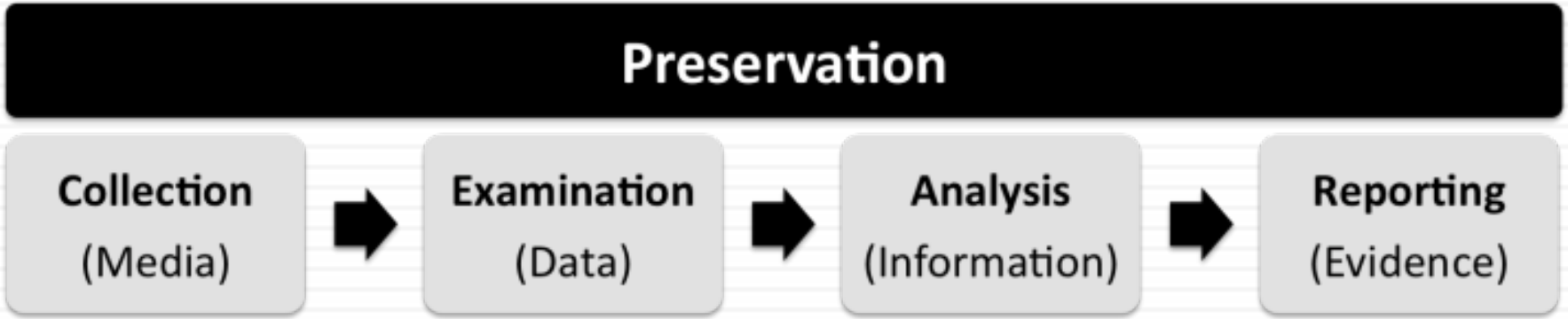
Usage of Cloud Forensics

- Investigation
- Troubleshooting
- Log monitoring
- Data and system recovery
- Due diligence/regulatory compliance

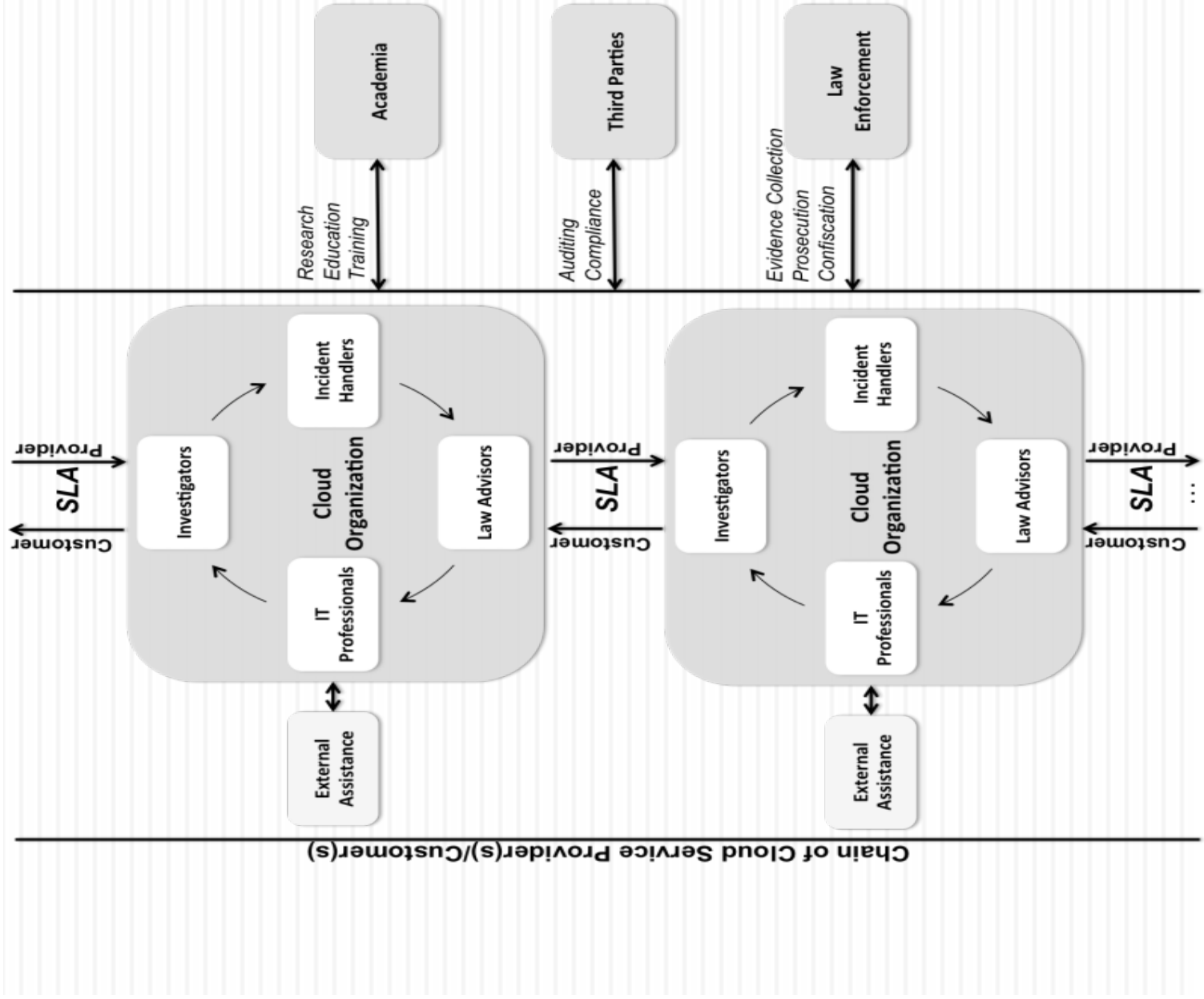
The 3 dimensions of Cloud Forensics



Technical Dimension



Organizational Dimension



Legal Dimension

- Multi-jurisdiction + Multi-tenancy
- SLA

Challenges

Technical Challenges

Organizational Challenges

Legal Challenges

Technical Challenges

Forensic Readiness

- Challenge No.1 Decreased Access
- Challenge No.2 Simple Identity Management Policies
- Challenge No.3 Ineffective Key Management

Technical Challenges

Challenges Unique to the Cloud

- Challenge No.4 Loss of Data Control
- Challenge No.5 Compartmentalization
- Challenge No.6 Resource Sharing
- Challenge No.7 Jurisdiction of Storage
- Challenge No.8 External Chain of Dependencies
- Challenge No.9 Single Point of Failure

Technical Challenges

Challenges exacerbated in the Cloud

- ***The velocity of attack factor*** *refers to the fact that the Cloud harness the power of thousands of compute nodes, combined with the homogeneity of the operating system employed by hosts, means the threats can be amplified quickly and easily*
- Challenge No.10 Synchronization of Timestamps
- Challenge No.11 Unification of Log Format
- Challenge No.12 Proliferation of Endpoints

Organizational Challenges

- Challenge No.13 Lack of forensic and law expertise
- Challenge No.14 Missing terms and conditions in SLA regarding forensic activities

Legal Challenges

- Challenge No.15 Multi-Jurisdiction
- Challenge No.16 Lack of mechanism for collaboration
- Challenge No.17 Lack of mechanism for evidence retrieval
- Challenge No.18 Launching cases of civil trail

Opportunities

Opportunities

- Opportunity No.1 Cost Effectiveness
- Opportunity No.2 Data Abundance
- Opportunity No.3 Overall Robustness
- Opportunity No.4 Scalability and Flexibility
- Opportunity No.5 Standards and Policies
- Opportunity No.6 Forensics-as-a-Service

Questions

Thank You!

keyun.ruan@ucd.ie

www.2centre.eu

cci.ucd.ie