Large Scale Cloud Forensics

Edward L. Haletky

AstroArch Consulting, Inc.

Sam Curry

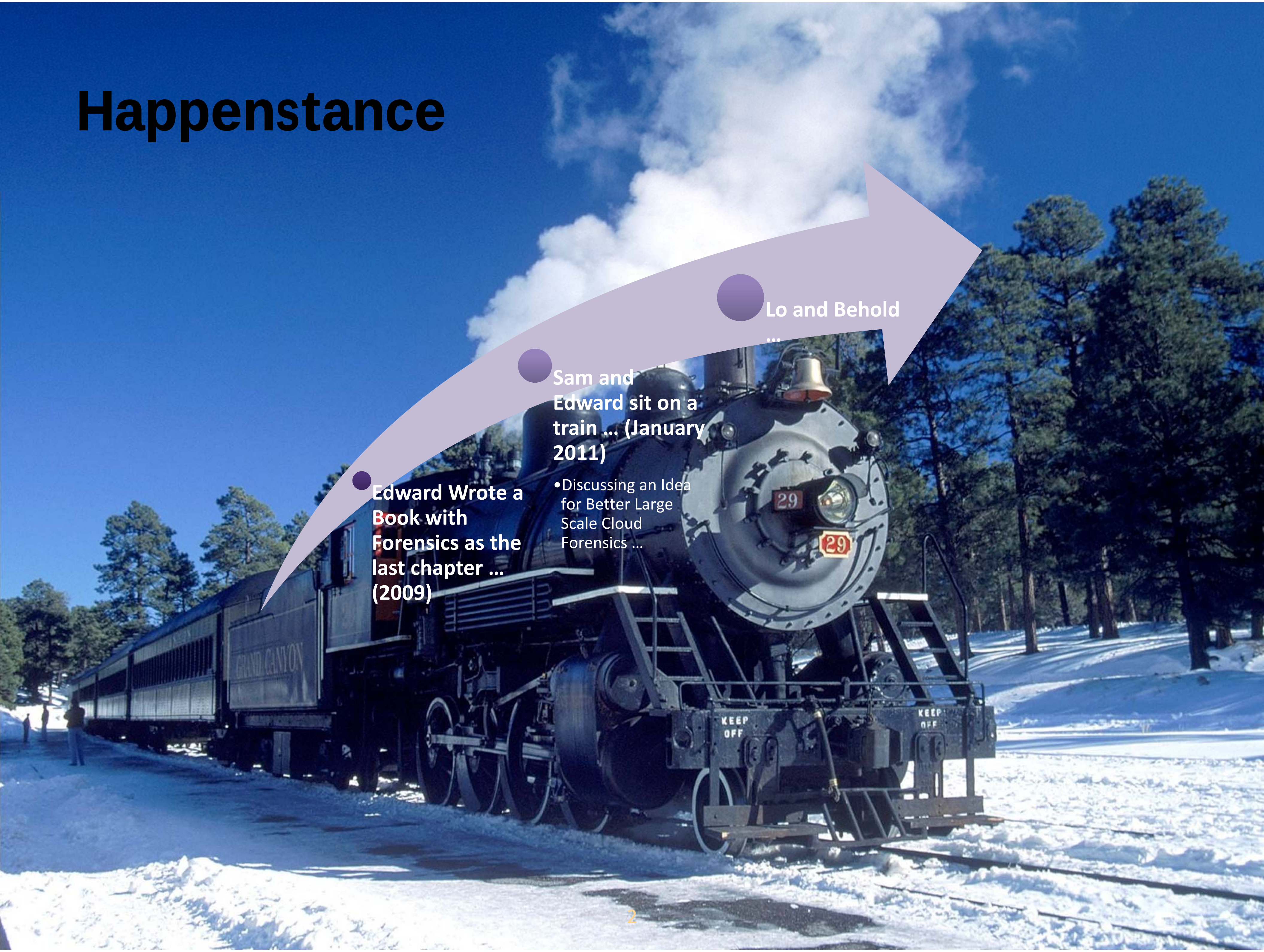
RSA, The Security Division of EMC

Session ID: STAR-302

Session Classification: Advanced

RSACONFERENCE2012

Happenstance



Edward Wrote a Book with Forensics as the last chapter … (2009)

Sam and Edward sit on a train … (January 2011)

- Discussing an Idea for Better Large Scale Cloud Forensics …

Lo and Behold …

Problem Scenario

The Economist reported on July 6th, 2011, that arrests in Latvia triggered an FBI raid in Virginia

- Multiple Tenants Impacted
- Multiple Jurisdictions Involved

Touched Upon

- Continuity of Business
- “Legality” Issues (Boundaries => Tenants)
- Law Enforcement’s Civil Liability
- Effectiveness of Forensic Approach

Sledgehammer to drive in a Thumbtack

Formal Problem Statement

Given

- Large Scale
- Multi-Tenant
- Cloud

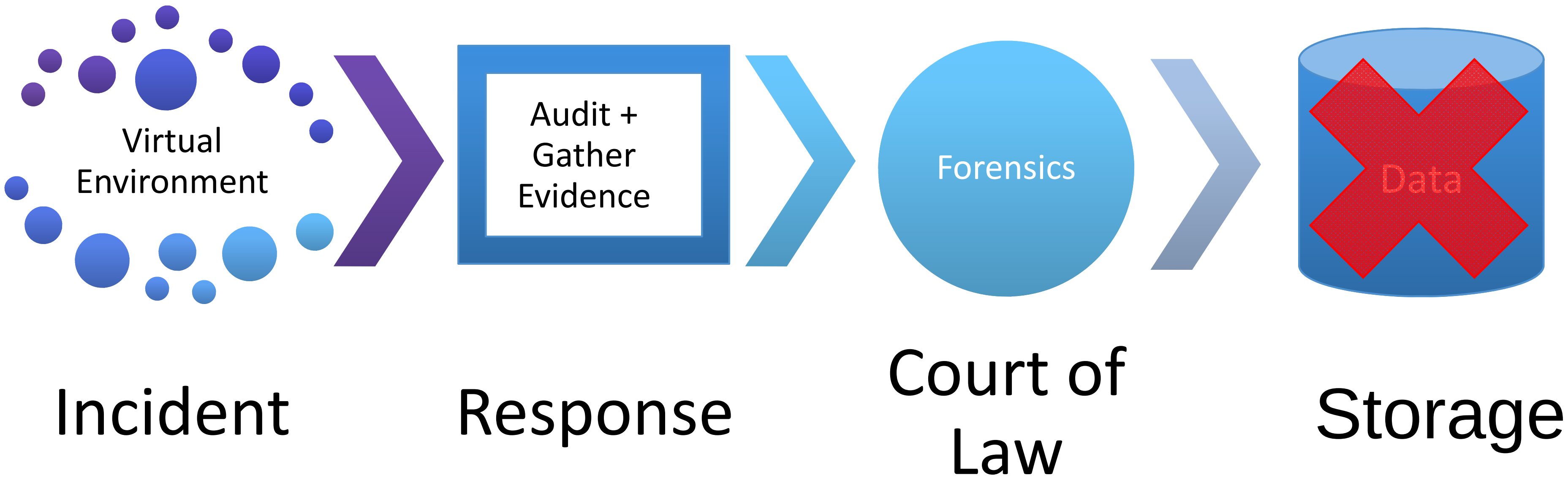
Required

- Acquire Data
- Perform Analysis
- Store Data

Solution Must Include

- Modern Methodology
- Improved Technology and Tools
- Improved Legal Framework

Challenges


Virtual
Environment
Audit +
Gather
Evidence
Forensics
Data
Incident
Response
Court of
Law
Storage

Why Care?

Business

- Saves Money
- Less Operational Risk
- Less Liability Risk

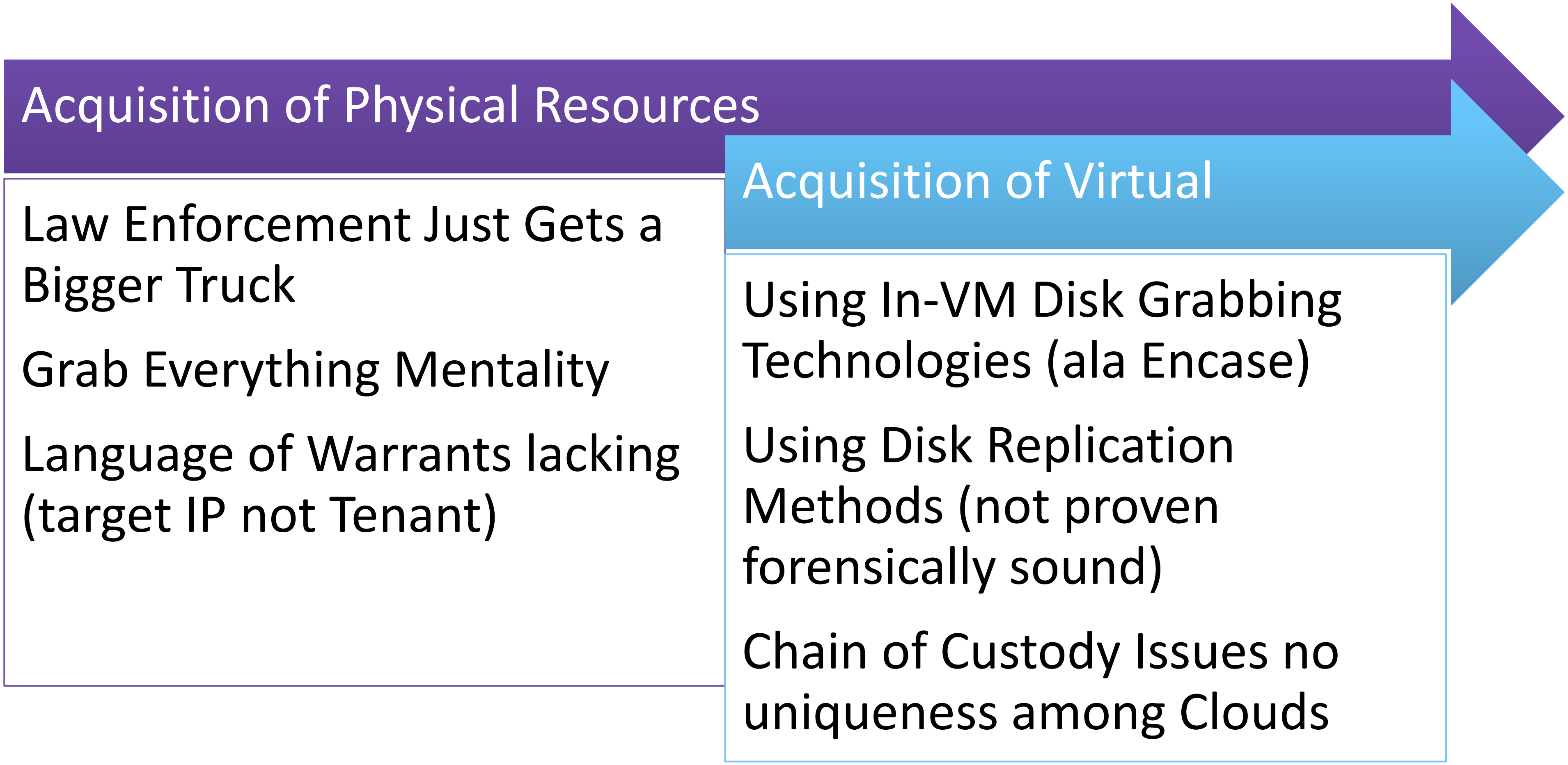
Law Enforcement

- Saves Money over Time
- Faster and Less Disruptive Acquisition
- Faster Investigations
- Less Error Prone Methodology

Forensic Scientists

- Advancing the State of the Art
- Less Time doing the Mundane

The State of Acquisition Today



Acquisition of Physical Resources

Law Enforcement Just Gets a Bigger Truck

Grab Everything Mentality

Language of Warrants lacking (target IP not Tenant)

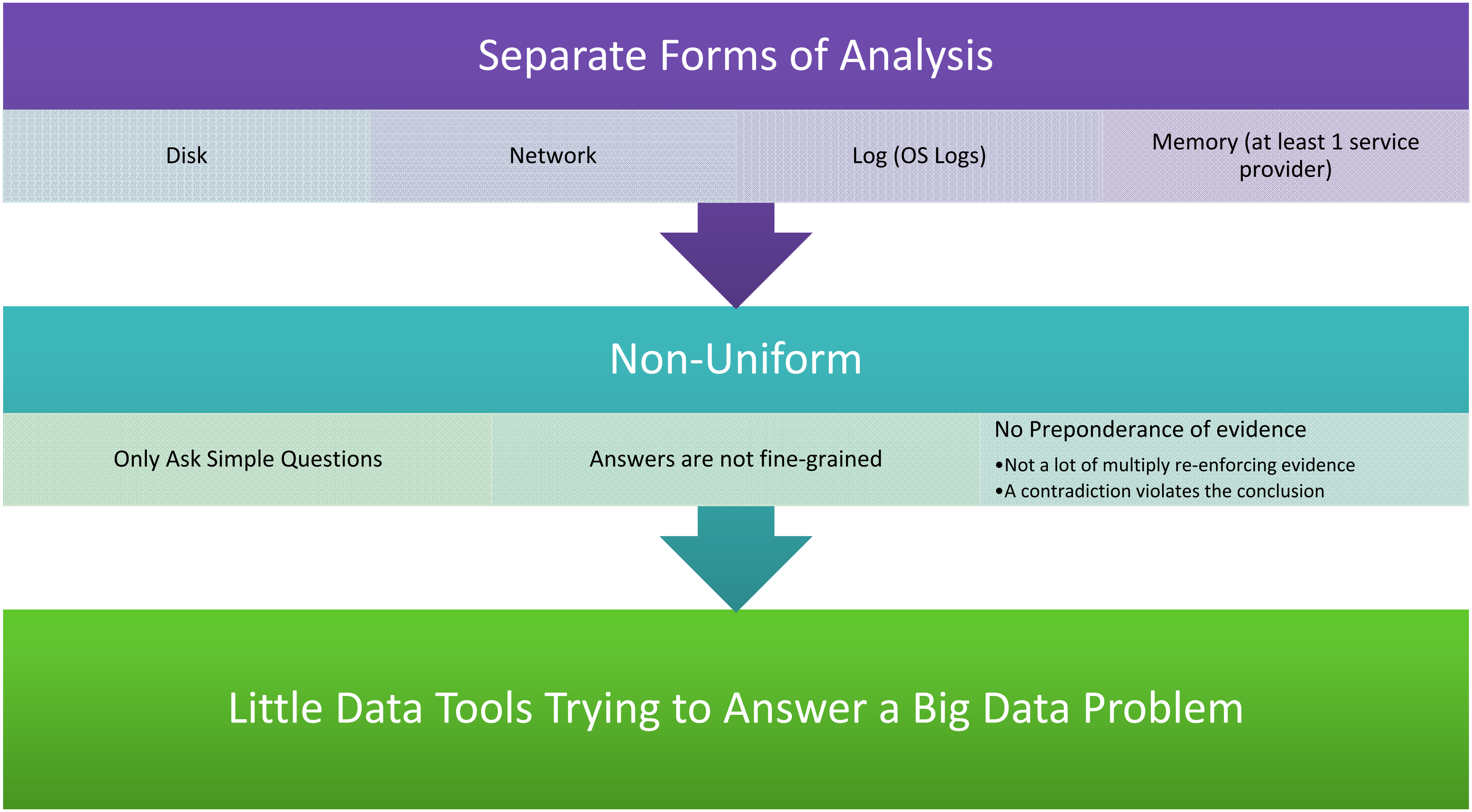
Acquisition of Virtual

Using In-VM Disk Grabbing Technologies (ala Encase)

Using Disk Replication Methods (not proven forensically sound)

Chain of Custody Issues no uniqueness among Clouds

State of Analysis Today



Separate Forms of Analysis

Disk	Network	Log (OS Logs)	Memory (at least 1 service provider)

Non-Uniform

Only Ask Simple Questions	Answers are not fine-grained	No Preponderance of evidence •Not a lot of multiply re-enforcing evidence •A contradiction violates the conclusion

Little Data Tools Trying to Answer a Big Data Problem

First Principles

Locard’s Priniciple

- Whenever a crime is committed there is an exchange of evidence between the criminal and the crime scene.
- 20th century this came to mean trace evidence
- In the Cloud, this implies electronic evidence

Uniqueness (Chain of Custody)

- Require Uniqueness Among Clouds
- How you process the, data affects the chain of custody
- Improve “Bagging and Tagging”

The Fourth Dimension (Time)

- Need a constant Time Source
- Can we find one outside the Target

Unique Identifier

Uniqueness is a Quality of the Following Objects:

- Virtual Disks
- Configuration Files
- Run-Time Files
- Log Files
- vNetwork Interfaces

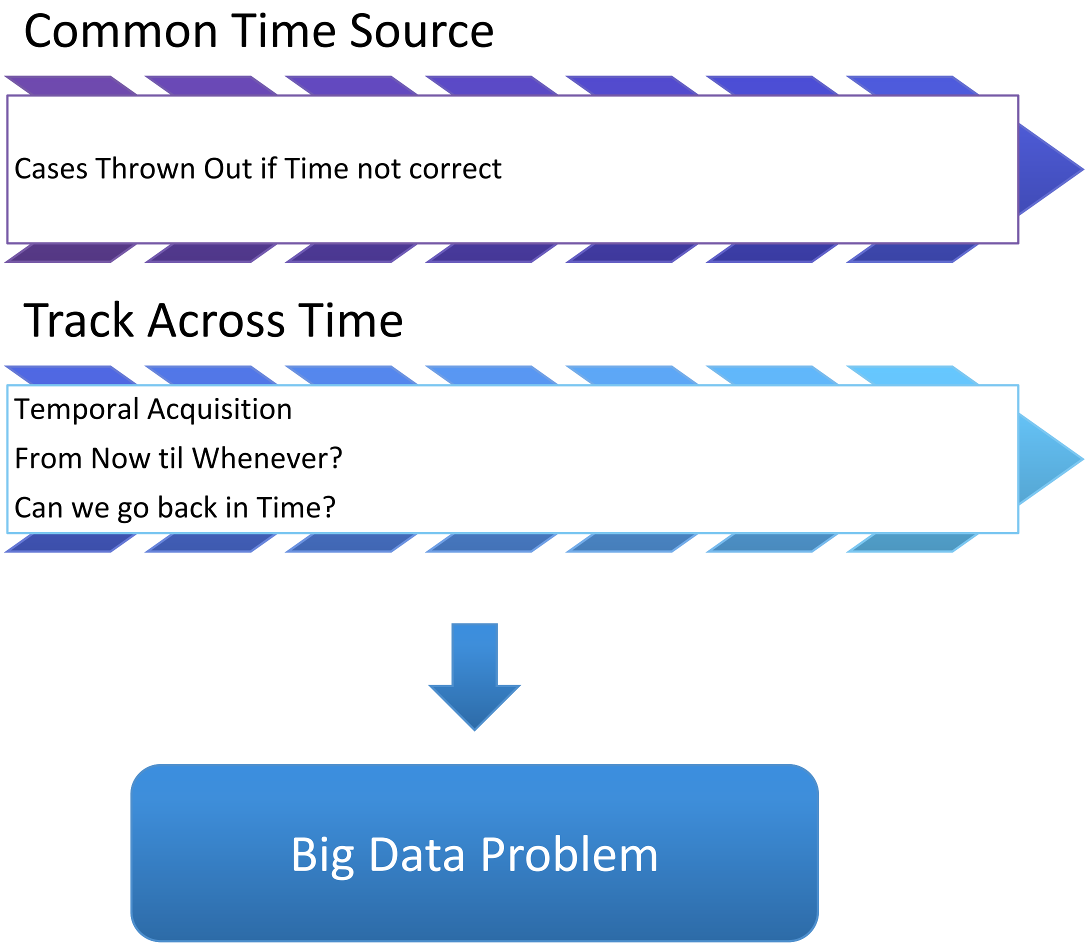
Uniqueness must be represented by an artifact that can be computed upon (search upon, quantify etc.)

- Eg Identification value

Rules of Unique Identifier

- No two objects, regardless of time or location, should have the same artifact
- Artifact Can be and should be used to describe relationships among objects
- Must Survive migration
  - Eg vMotion, Migration between clouds
- Ultimately Any of the Above objects without an ID is rogue

Time



Common Time Source

Cases Thrown Out if Time not correct

Track Across Time

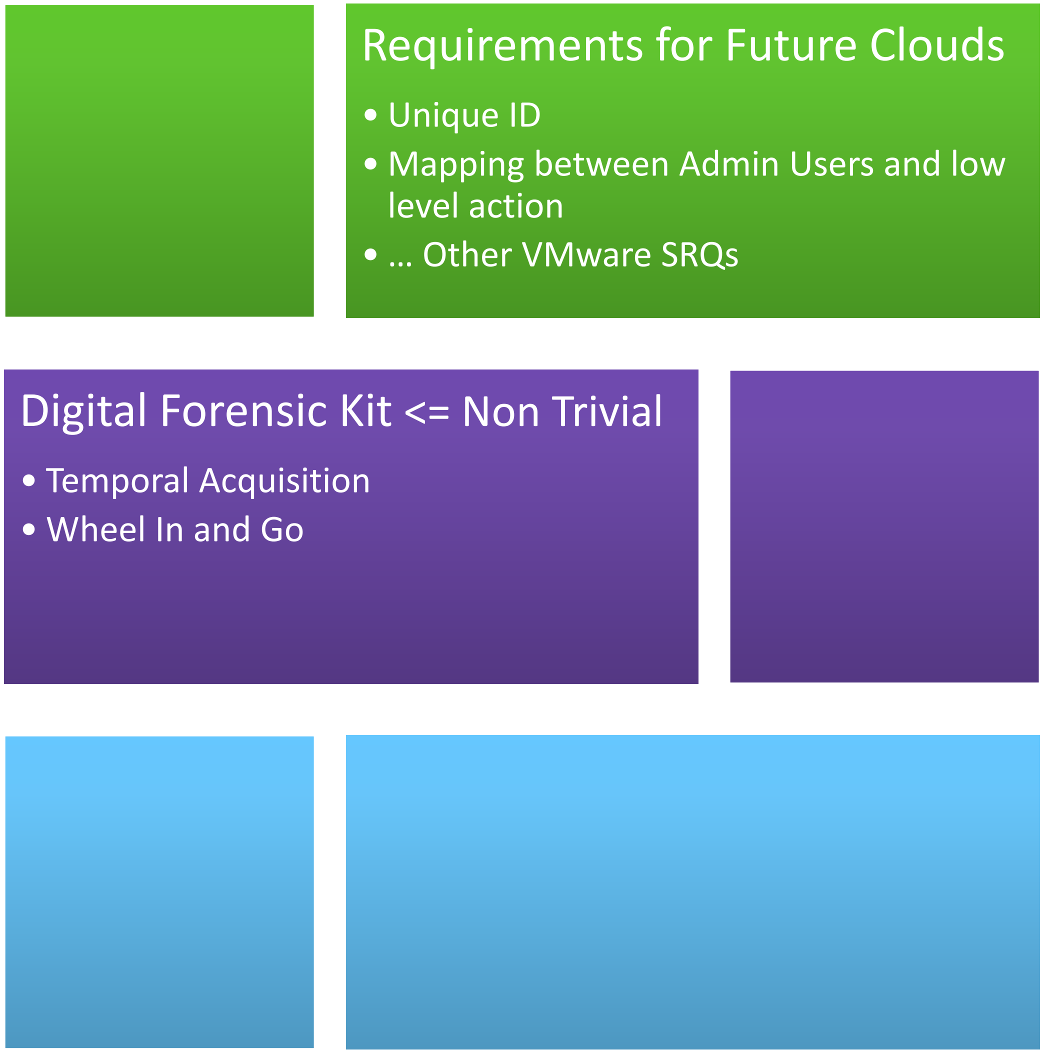
Temporal Acquisition

From Now til Whenever?

Can we go back in Time?

Big Data Problem

Tools Needed



Requirements for Future Clouds

- Unique ID
- Mapping between Admin Users and low level action
- … Other VMware SRQs

Digital Forensic Kit <= Non Trivial

- Temporal Acquisition
- Wheel In and Go

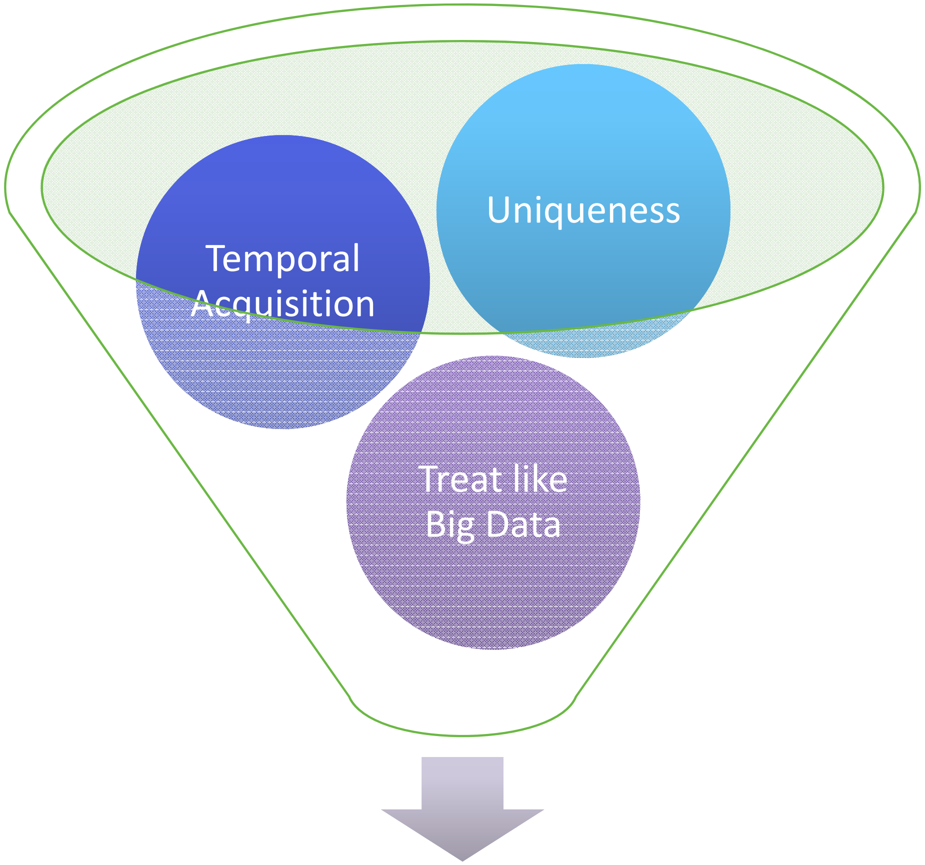
Modern Forensic Lab (Analysis 2.0)

Large Array of Storage

Systematic Way to Do Large Scale Repeatable Data Mining (HADOOP)

Knowing "How" to Inquire of the "Data" a Forensic Question regardless of Data "Type"

Conclusion



Large Scale Cloud Forensics

Research Needed

Prototype the Kit

Build Analysis Lab 2.0

- Improve Hadoop tools to import varied data formats

Use of Memory Images to Further Decryption

- Reduce reliance on Suspects to give keys

Cryptography

- Format Preserving Encryption

What Can I Do?

Architecture

- Preparation (Plan for Forensics)
- Modification (Change what you already have)
- Response (Improve Incident Response)

Talk to Legal and/or Public Policy Officer

- Review Your Current Approach
- Develop Organizational Policy

Resources Check

Pressure on Vendors (eg. Bug RSA)

Get Ready!

Open Q&A

What are YOUR comments and questions?

What we will do next year!

Take a train …

Please take a paper and send us feedback

elh@astroarch.com

sam.curry@rsa.com