Large Scale Cloud Forensics

Edward L. Haletky

AstroArch Consulting, Inc.

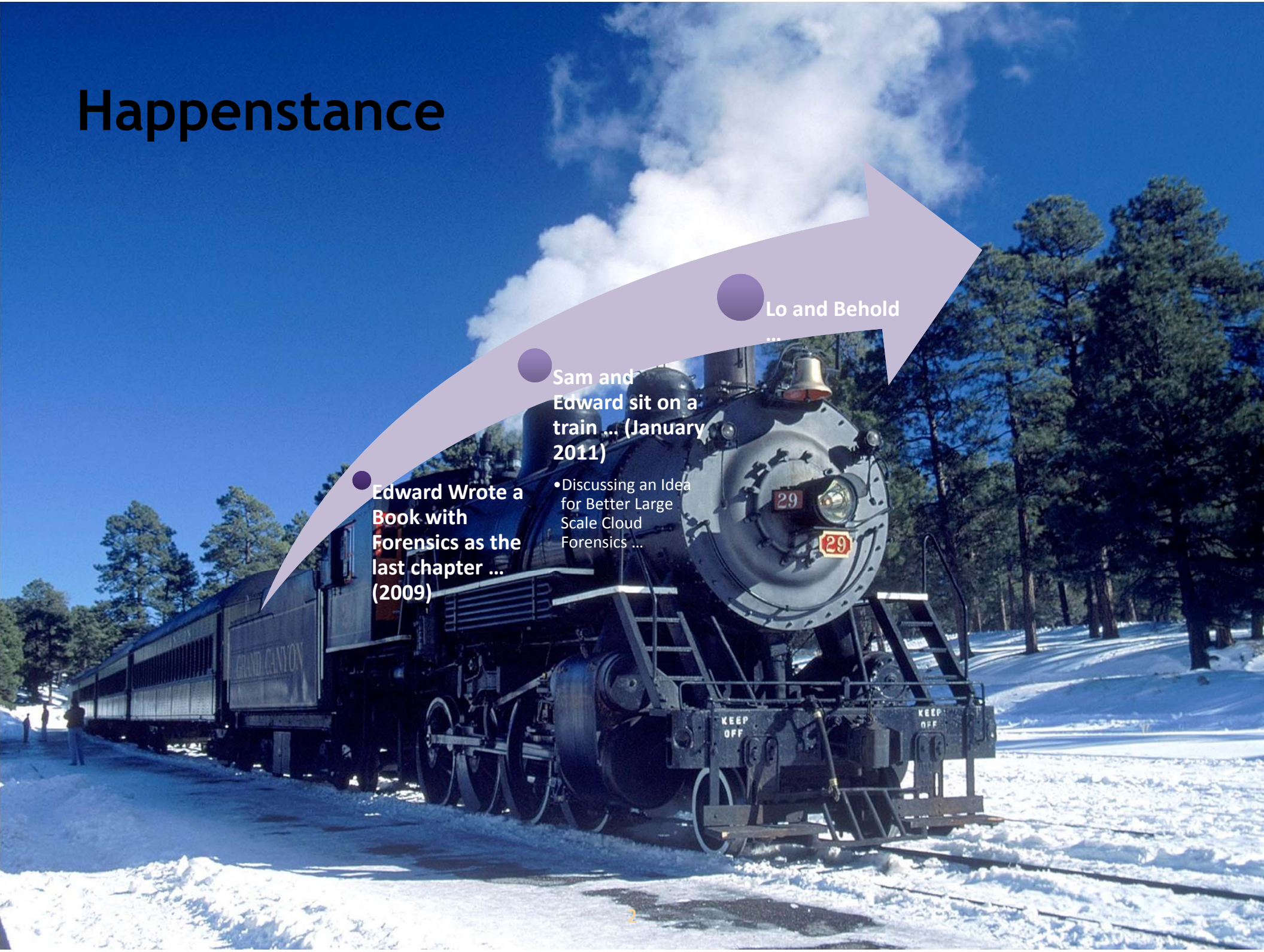
Sam Curry

RSA, The Security Division of EMC

Session ID: STAR-302

Session Classification: Advanced

Happenstance



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