Organizer:

CyberSecurity MALAYSIA

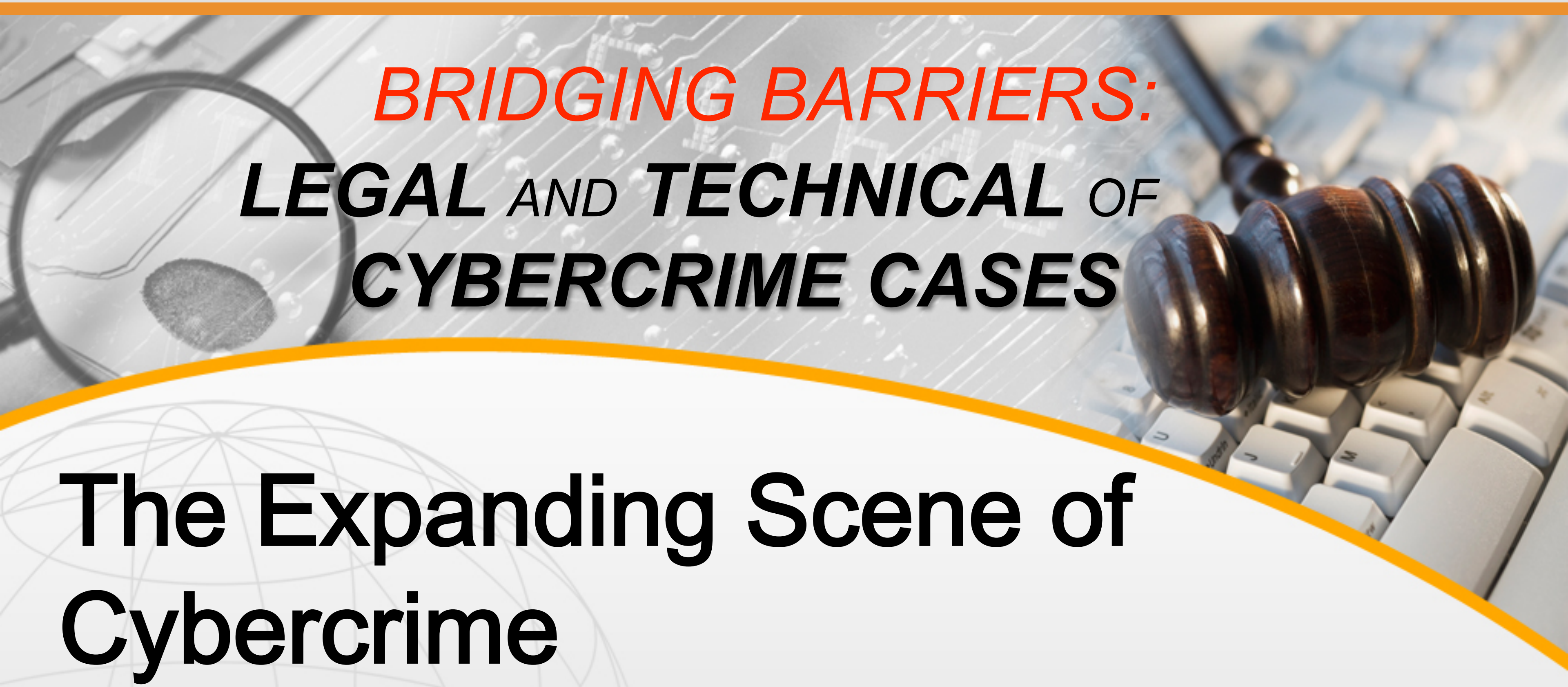
AGCSM

Endorsed by:

People First, Performance Now

MOSTI

Ministry od Science, Technology and Innovation



*BRIDGING BARRIERS:*

***LEGAL** AND **TECHNICAL** OF*

***CYBERCRIME CASES***

# The Expanding Scene of Cybercrime

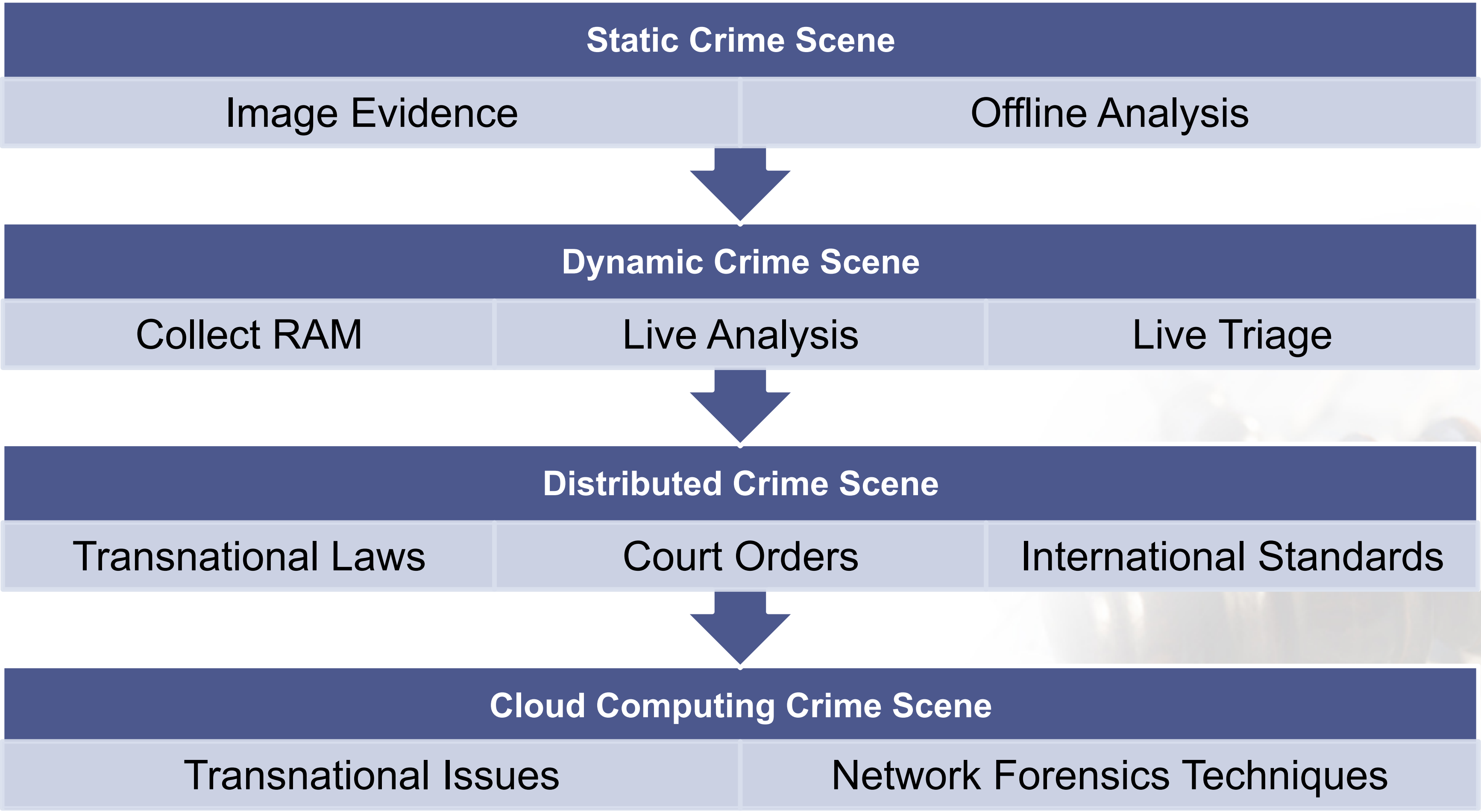
Steve Anson

5 July 2011

# Introduction

- US Department of State Antiterrorism Assistance Program
- Provides training and related assistance to law enforcement and security services worldwide
- Trained over 48,000 law enforcement officials from over 141 countries

# Digital Crime Scenes



**Static Crime Scene**

Image Evidence | Offline Analysis

**Dynamic Crime Scene**

Collect RAM | Live Analysis | Live Triage

**Distributed Crime Scene**

Transnational Laws | Court Orders | International Standards

**Cloud Computing Crime Scene**

Transnational Issues | Network Forensics Techniques

# Static Crime Scene

## The Good Old Days

# Static Crime Scene

- Scene Attributes:
  - Evidence Contained in Portable Devices
  - Evidence Stored on Non-Volatile Media
  - 25+ Years of Police Experience

# Static Crime Scene

- Response Techniques:
  - Power Off Devices
  - Collect Devices and Return to Lab
  - Image all Media in its Entirety
  - Offline Analysis of Data

# Dynamic Crime Scene

| | | |
|---|---|---|
| Larger RAM | Smarter Criminals | Encrypted Files |
| Encrypted Volumes | Critical Servers | Running Processes |
| Active Connections | Massive Data Sets | Complex RAIDs |

# Dynamic Crime Scene

- Scene Attributes:
  - Running Computers
  - Mission Critical Servers
  - RAM Containing Potential Evidence
  - Suspicion of Encryption
  - Huge Disk Storage

# Dynamic Crime Scene

- Response Techniques:
  - Live Collection of RAM
  - Logical Imaging of Relevant Evidence
  - Field Triage of Systems
  - Acquisition of Mounted Volumes

# Distributed Crime Scene

- Webmail
- Social Network Sites
- Transnational Evidence
- Hacking Cases
- Online Fraud
- Remote Storage
- Evidentiary Standards
- Cross Border Legal Differences

# Distributed Crime Scene

- Scene Attributes
  - – Evidence Held by Service Providers in Unknown Locations
  - – Evidence that Crosses International Borders
  - – Evidence in Remote Places that is Time Sensitive
  - – Need for Speed

# Distributed Crime Scene

- Response Techniques:
  - – Mutual Legal Assistance Treaties
  - – Court Orders for Data
  - – Multi-Jurisdiction Cases
  - – Questionable Access Methods
  - – ISO Compliant Evidence Processing

# Cloud Computing Crime Scene

- IaaS
- PaaS
- SaaS
- Cross Border Issues
- Unclear Location of Data
- No Physical Access to Machines
- Shared Computing Resources
- Data Privacy Concerns
- Distributed Storage

# Cloud Computing Crime Scene

- Scene Attributes
  - Distributed Evidence
  - Virtual Machines
  - Large, Shared Data Centers
  - Impossible to Seize and Image Everything
  - Cooperation with the Cloud Service Provider Needed

# Cloud Computing Crime Scene

- Response Techniques
  - Network Forensics Tools
  - Evidence Located Based on Access Rather than Device
  - Logical Image Acquisition
  - Collection and Analysis of Virtual Machines
  - Court Orders for Production of Data

# Summary

- Digital Crime Scenes are Increasingly Complex and Distributed
- Digital Forensics Techniques Must Evolve and Focus on “Best Evidence”
- International Standards (e.g. ISO 17025) Should be Adopted
- International Mutual Legal Assistance Must Be Improved