ELECTRONIC EVIDENCE IN CRIMINAL INVESTIGATIONS

OAS-REMJA Working Group on Cybercrime Regional Workshop for Central America
Panama City, Panama, 25 to 27 August 2009

Tuesday, 25 August

8:30	Arrival and registration	
9:00	**Opening session** Welcome and introduction by representatives of Panama, the United States, and the Organization of American States	
10:00	Break	
10:20	**Investigations involving computers and the Internet** Electronic evidence is likely to exist for most crimes • The nature and location of electronic evidence • An overview of investigations involving electronic evidence • Roles of investigators, analysts, and prosecutors • Basic training and equipment for police and investigators	Albert Rees *Trial Attorney* *United States Department of Justice*
11:00	**Plenary discussion: legal considerations for gathering electronic evidence** The law shapes the way that investigators gather evidence • Participants discuss their countries' laws and procedures for obtaining evidence and how this impacts gathering electronic evidence • Participants describe their countries' legal standards to successfully convict offenders using electronic evidence • All are encouraged to provide examples from their countries of successes and challenges in using electronic evidence in legal proceedings	
11:40	**Computers, networks, and the Internet** An introduction to computer systems and how the internet works • Creating and storing information • Moving information across the Internet; Internet protocol (IP) addresses • Internet applications: email and web browsers	Luis A. Gorgona S. *Deputy Director of Information Technology of the Presidential Ministry of Costa Rica*
13:00	Lunch	
14:00	**First response: before the police arrive** Much may have occurred before a crime involving computers or the Internet is reported to police • The role of the system administrator in incident response • The functions and role of the CSRIT • The goals of incident response • Assisting law enforcement in investigations	Luis A. Gorgona S. *Deputy Director of Information Technology of the Presidential Ministry of Costa Rica*

15:00	**First response: initial stages of the investigation** Investigators must respond promptly to identify and secure electronic evidence • Interviewing system administrators and other witnesses • Identifying sources of electronic and other evidence • Preserving electronic evidence • Integrating electronic and other evidence into the investigation • Case management and investigation plan	Matt Ralls *Special Agent* *United States* *Secret Service*
16:00	Break	
16:20	**Introduction to the case study** Participants will break into groups to apply principles presented in the workshop to a hypothetical case involving computers and the Internet	Michelle Kane *Trial Attorney* *United States* *Department of Justice*
16:30	**Breakout group discussions: digital evidence and forming an investigation plan**	
17:30	Adjourn	

Wednesday, 26 August

9:00	**Plenary discussion: first response actions and investigation plan** Participants report on their breakout group discussions, including conclusions, proposed actions, and unresolved issues	
9:30	**Collecting digital evidence: e-mail investigations** E-mail communications can be a source of evidence for any crime • The components of e-mail messages • E-mail headers and other metadata • Tracing e-mail • Working with service providers who hold data and records • International issues	To Be Determined
10:30	Break	
10:50	**Collecting digital evidence: online investigations** Individuals who use the Internet leave a trail of evidence that can be hard to follow, but valuable • Common applications: websites, IRC, IM, P2P, VOIP • Online reconnaissance • Encryption • Protecting the investigator's online identity • Working with service providers • International issues	Matt Ralls

13:00 Lunch

14:00 **Collecting digital evidence: computers, networks, and related items** Matt Ralls

Computers and other electronic devices may contain a wealth of information

- Searching for and seizing computers and related evidence
- Preparing for the search and seizure; reconnaissance and planning
- Securing the computer for analysis and data preservation
- Initial data collection – triage – volatile data collection
- Assistance from the forensic analyst and system administrator
- Imaging and preserving evidence
- Collecting and using non-electronic evidence

15:00 **Computer forensics** To Be Determined

An introduction for investigators and prosecutors on computer forensics and the evidence available through analysis

- Description of computer forensics
- What computer forensics can provide to the investigator and prosecutor; what it cannot provide
- Common techniques
- Working with the forensic analyst

16:00 Break

16:20 **Breakout group discussions: collecting digital evidence and creating a timeline**

17:30 Adjourn

Thursday, 27 August

9:00 **Plenary discussion: collecting digital evidence and creating a timeline**

Participants report on their breakout group discussions, including conclusions, proposed actions, and unresolved issues

9:30 **International cooperation** Albert Rees

The global nature of the Internet requires new thinking in international cooperation

- Applying principles of international legal assistance to electronic evidence
- The need for harmonized laws and procedures – Cybercrime Convention
- Data preservation and the 24/7 Network
- Some solutions; continuing problems

10:30 Break

10:50	**Mobile telephones as electronic evidence** The ubiquitous mobile telephone can be a significant source of evidence • Evidence residing on mobile phones • Searching and seizing mobile phones • Evidence held by service providers • Mobile phone location	Matt Ralls
12:00	**User attribution** Investigators and prosecutors must show that the suspect used the computer • Using electronic and other evidence to show that a person was using a computer at a particular time and place • Countering suspects' explanations as to why it was not them	Michelle Kane
13:00	Lunch	
14:00	**The OAS Working Group on Cybercrime** The OAS Working Group on Cybercrime is a group of government experts responsible for fostering international cooperation in the investigation and prosecution of cybercrime among the member states of the OAS	Rodrigo Cortés Legal Counsel Department of Legal Cooperation Secretariat for Legal Affairs of the OAS
14:30	**Plenary discussion: putting it all together and preparing for trial** Participants and facilitators share their requirements, practices, and experiences for bringing an investigation to a conclusion, preparing for legal proceedings, and success at trial	Michelle Kane
15:30	**Workshop wrap-up and feedback**	Albert Rees
16:00	**Closing**	
17:00	End of workshop	

For information about this workshop and other OAS-REMJA cybercrime programs:

Department of Legal Cooperation
Secretariat for Legal Affairs
Organization of American States

Rodrigo Cortés: rcortes@oas.org
+1 (202) 458-3395

www.oas.org/juridico/spanish/
www.oas.org/juridico/english/

Computer Crime and Intellectual Property Section
Criminal Division
United States Department of Justice

Albert Rees: albert.rees@usdoj.gov
Jaikumar Ramaswamy: jaikumar.ramaswamy@usdoj.gov
+1 (202) 514-1026
www.cybercrime.gov