

ELECTRONIC EVIDENCE IN CRIMINAL INVESTIGATIONS

OAS-REMJA Working Group on Cybercrime Regional Workshop for South America
Santiago, Chile, 21 to 23 July 2009

Tuesday, 21 July

8:30 Arrival and registration

9:00 Opening session

Welcome and introduction by representatives of Chile, 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

Santiago Martín Acurio
Del Pino
Director Nacional de
Tecnologías de la
Información
Fiscalía General de
Ecuador

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 CSIRT
- 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

Victor Sanchez
*Senior Special Agent
 United States
 Immigration and
 Customs Enforcement*

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

Jaikumar Ramaswamy
*Trial Attorney
 United States
 Department of Justice*

16:30 Breakout group discussions: digital evidence and forming an investigation plan

17:30 Adjourn

Wednesday, 22 July

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

Santiago Acurio

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

10:30 Break

10:50 Collecting digital evidence: online investigations

Victor Sanchez

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

13:00 Lunch

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

Victor Sanchez

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**

Santiago Acurio

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, 23 July

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	Victor Sanchez
	<p>The ubiquitous mobile telephone can be a significant source of evidence</p> <ul style="list-style-type: none"> • Evidence residing on mobile phones • Searching and seizing mobile phones • Evidence held by service providers • Mobile phone location 	
12:00	User attribution	Jaikumar Ramaswamy
	<p>Investigators and prosecutors must show that the suspect used the computer</p> <ul style="list-style-type: none"> • 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 	
13:00	Lunch	
14:00	Applying law and regulation to collection of electronic evidence	Verónica Rosenblut Grodinsky <i>Abogado</i> <i>Unidad Especializada en Lavado de Dinero, Delitos Económicos y Crimen Organizado</i> <i>Fiscalía Nacional de Chile</i>
	<p>Chile's perspective on gathering electronic evidence</p> <ul style="list-style-type: none"> • Chile's general regulation on seizure and preservation of evidence • Seizure of electronic communications 	
15:00	Plenary discussion: putting it all together and preparing for trial	Jaikumar Ramaswamy
	<p>Participants and facilitators share their requirements, practices, and experiences for bringing an investigation to a conclusion, preparing for legal proceedings, and success at trial</p>	
15:40	Workshop wrap-up and feedback	
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

Michael Thomas: mthomas@oas.org

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