

INVESTIGATING INTERNET CRIMES

OAS-REMJA Working Group on Cybercrime Regional Workshop for Central America
Digital Investigation Workshop
Lima, Peru, 31 August – 2 September 2010

Tuesday, 31 August

8:30 Arrival and registration

9:00 Opening session

Welcome and introduction by representatives of the United States, and the Organization of American States

10:00 Break

10:20 Large-scale crimes involving the Internet

The Internet has evolved into a useful tool for large-scale criminal activities

- Criminal uses for the Internet: crimes, communication, and more
- Criminal organizations and individuals who use the Internet
- Trends and new ways for Internet-based crime
- Government responses to Internet-based crime

Anthony Teelucksingh

Senior Counsel

United States

Department of Justice

11:20 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 applications

Michael Stawasz

Senior Counsel

United States

Department of Justice

13:00 Lunch

14:00 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

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

Sheila Cabrera

Special Agent

United States

Secret Service

16:00 Break

16:20 **Introduction to the group discussion problem**

Anthony Teelucksingh

Participants will break into groups to apply principles presented in the workshop to a hypothetical case involving computers and the Internet

16:30 **Breakout group discussions: first response and investigation plan**

17:30 Adjourn

Wednesday, 1 September

9:00 **Plenary discussion: first response and investigation plan**

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

9:30 **Collecting digital evidence: online investigations**

**Sheila Cabrera
Michael Stawasz**

Individuals who use the Internet leave a trail of evidence that can be hard to follow, but valuable

- Common applications: e-mail, websites, IRC, IM, P2P, VOIP
- Encryption
- Protecting the investigator's online identity
- Working with service providers
- International issues

10:30 Break

10:50 **Collecting digital evidence: online investigations -- continued**

13:00 Lunch

14:00 **Computer forensics**

Sheila Cabrera

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

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

15:00 **Mutual legal assistance: formal and informal measures**

Anthony Teelucksingh

The global nature of the Internet requires new thinking in mutual assistance

- 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

16:00 Break

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

17:30 Adjourn

Friday, 25 June

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 **Mutual legal assistance: practical considerations for improved cooperation**

Builds on the prior mutual legal assistance topic; sharing of electronic evidence between different countries occurs frequently

- Investigator to investigator sharing
- Working with service providers across borders
- OAS mutual legal assistance efforts
- Ideas for improved cooperation

PANEL:
Michael Stawasz
Sheila Cabrera
Invited Speakers

Anthony Teelucksingh,
 Moderator

10:30 Break

10:50 **Case study: [example of large scale fraud/theft by organized international criminals]** **United States**

12:00 **Case study** **Peru**

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

OAS
*Department of Legal
 Cooperation,
 Organization of
 American States
 Secretariat*

14:30 **Plenary discussion: putting it all together and getting to 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

15:30 **Workshop wrap-up and feedback**

16:00 **Closing**

17:00 End of workshop