As criminals take advantage of new technology, the ease of international travel and the anonymity of doing business in the virtual world, police and industry partners must adapt their responses to effectively confront this new and evolving type of crime.

In the past, when somebody robbed a bank, the pool of suspects was limited to the number of people with physical access to the bank. Today, when a bank is robbed digitally, anyone with a computer and an Internet connection could potentially be a suspect. In the virtual world, almost anyone could be connected to a crime and be able to erase traces of their activity in a way that is nearly impossible in the physical world.

Police can no longer simply connect the dots at a national level between the crime and the criminal, but trace a criminal through a complex series of networks, usually across jurisdictions. Digital forensics therefore becomes an essential part of an investigation, allowing police to trace, identify and build a case against a suspect.

The INTERPOL Global Complex for Innovation (IGCI), through its digital forensic laboratory, will build national digital forensic capacity, leveraging multistakeholder expertise, so that investigators are provided with practical technologies and skills to better coordinate and conduct transnational digital crime investigations.
Main activities

The IGCI will work with experts from across the public, private and academic communities to provide the tools, intelligence and digital forensic expertise required to more effectively combat cybercrime.

These activities will be concentrated within a digital forensic laboratory that will provide comprehensive support to national police worldwide.

CRIMEWARE ANALYSIS
The digital forensics laboratory will analyse malware and other related cybercrime tools (crimeware) identified by INTERPOL or submitted by a member country or partner organization. Malware analysis reports will be provided to member countries so that they may coordinate national responses and refocus their own resources. The digital forensics laboratory will also monitor botnets and analyse linkages of malicious activities in order to ultimately trace activities back the perpetrators.

MOBILE DEVICE FORENSICS
Massive numbers of new mobile devices are activated each year all over the world, increasing the need for channelling efforts and activities in the mobile forensic field. Various companies in the private sector provide training as well as the tools to empower officers in mobile forensics, as they understand the importance of retrieving and extracting digital evidence without tempering the data.

The IGCI will therefore leverage the expertise and tools of its private sector partners, which will be of great value to member countries in their investigations, evidence handling protocols and general understanding of the forensic data field.

The digital forensic lab will utilise the latest forensic techniques and solutions to assist member countries in the examination of digital devices to ensure that a systematic forensic examination is completed.

TESTING FORENSIC TOOLS
Further activities will aim to identify commercial and non-commercial digital forensic tools, developed by the private sector, academia and national research laboratories. It will subsequently drive, initiate and coordinate collaborative testing of these cutting-edge tools, as well as services and protocols, in order to push the frontiers of cybercrime fighting and advance the use of digital forensics at the national level.

We will also proactively engage strategic stakeholders, including research laboratories and institutions, academia, and the public and private sectors, to conceptualize and design state-of-the-art technological innovations that address current and future cybercrime activities.

DIGITAL FORENSIC TRAINING
The digital forensic lab will develop and provide career development trainings for examiners, investigators and other first responders to ensure they possess the latest knowledge of cybercrime trends, and the usage of digital forensic tools and techniques.

The digital forensic lab will offer training in computer, mobile and malware forensics as well as new digital forensic technology and techniques. It will also operate a knowledge bank of training materials to be accessed by member countries in order to facilitate information sharing and the development of best practices in cybersecurity capacity building.

Contact
INTERPOL General Secretariat
Global Complex for Innovation
200 quai Charles de Gaulle
69006 Lyon
France
Tel: +33 4 72 44 70 00
Fax: +33 4 72 44 71 63
www.interpol.int