isif asia

## fast facts

**Project:** A Low Cost Digital Forensic Laboratory for a Developing Country
**Lead Organization:** University of Colombo School of Computing (UCSC)
**Country:** Sri Lanka

## situation

As a result of the increase of computer crimes across the developed and developing world, a multitude of digital forensic investigation processes and models have been developed. These procedures have been developed to suit the specific needs of each country, region, or organization. Unfortunately, not all countries currently possess the tools necessary to investigate and actively pursue those who commit crimes online. In the case of Sri Lanka, there is a distinct need for a national investigation center for Computer Forensics, as current technologies are not applicable to the infrastructure.

## solution

A number of digital forensic investigation processes and models have been developed as a result of the increase of computer crimes across the developed and developing world. These procedures have been developed to suit the specific needs of each country, region, or organization. At University of Colombo School of Computing (UCSC), the project team has also developed software and relevant materials, as we have found that the existing forensic frameworks and toolkits are impractical in the Sri Lankan context.

Since 2003, UCSC has worked in collaboration with the Sri Lanka Police and the Criminal Investigation Department. To date, the UCSC has assisted in more than 200 court unique cases, employing several ad-hoc tools and forensic capabilities. During the current project period, UCSC has received more than 100 new cases, which they were able to help solve using their Forensics Lab. In general, the current vision for the Center of Digital Forensics (CDF) at UCSC is to establish itself as a leading research and investigation center for digital forensic investigation in the South Asia region.

This particular project began as an effort to develop a new digital forensic framework with a software toolkit and a clear set of guidelines to accommodate any type of computer-related crime in developing countries such as Sri Lanka. For this purpose, the Forensic Investigation Tool for Developing Countries (FIT4D) software toolkit provides functional solutions activity and employs a four-phase process designed to suit Sri Lanka's legislative environment and available resources.

FIT4D was developed as an extension for The Sleuth Kit, a library and collection of Unix-and-Windows-based tools and software designed to allow for the forensic analysis of computer systems. The software presents all the features already present in available forensic browsers, as well as new essential forensic features that support the whole digital investigation process. The team's FIT4D extension package includes not only an improved user interface, but includes several entirely new features such as disk imaging, new searching techniques, new file analysis techniques, and image processing techniques for complex digital investigation cases.

The FIT4D system operates on a peer-to-peer Virtual Private Network (VPN), which assures privacy and data authenticity. In an ideal situation, all police stations would have FIT4D servers, where they could store evidence related to crimes under investigation. As this is not currently feasible, there is an option to grant limited access to the FIT4D system and reap its benefits by connecting each police station and respective investigators via a virtual private network, or VPN. The privacy of the data is ensured by the Internet Protocol Security handling that is part of the server system. Although there is a risk of

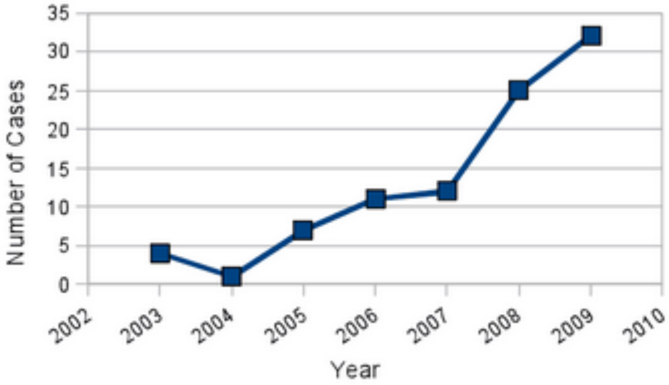
*This work has been developed with the support provided by the Information Society Innovation Fund (ISIF Asia) – 2013, licensed under the Creative Commons* Attribution.

transmitting sensitive data through public networks, this has been identified as the most manageable solution as most developing countries cannot afford the cost of building a separate private network to handle forensic information.

The first version of this software was released in January 2009 under a GPL license, and documents were released under a Creative Common License. The software and documents are published on the http://score.ucsc.lk/fit4d web site. The team has since incorporated the feedback from this first group of users into the updated version of the public release. The first training program was also conducted in January 2009, and allowed the team the opportunity to train forensic investigators from various government authorities in the use of their software.

## broader impact

Even though the team developed FIT4D for developing countries, it may be useful for developed countries as well. The team has received several inquiries regarding their work from universities and organizations in the UK. Other forensic teams in Sri Lanka have already begun to use the toolkit in their investigations, and The Sri Lanka Police and Defense Ministry has decided to include the software in their forensic laboratories.



Requests for support in investigating digital crime cases have grown consistently since the program's creation.

FIT4D research activities, results and training materials are published on the http://score.ucsc.lk/fit4d web site.

## project contact

Kasun De Zoysa
Email Address: kasun@ucsc.cmb.ac.lk
University of Colombo School of Computing (UCSC)
University of Colombo School of Computing
35 Reid Avenue,
Colombo, Sri Lanka
+94 11 2158973
www.ucsc.cmb.ac.lk