| | |
|---|---|
| **Name of organization supported** | **University of Colombo School of Computing (UCSC)** |
| **Project title** | **A Low Cost Digital Forensic Laboratory for a Developing Country** |
| **Dates covered by this report** | **30 June 2010** |
| **Country where the project has been implemented** | **Sri Lanka** |
| **Project leader name** | **Dr Kasun De Zoysa** |
| **Team members (list)** | Mr K. S. Goonatillake, (engineer)<br>Mr Kenneth M. Thilakarathna (Technical assistant/programmer)<br>Mr N. M. Laxman (Software Engineer/programmer)<br>Ms Yasantha Hettiarachchi (Research assistant/programmer) |
| **Submission date** | **9 July 2010** |

## Table of contents

## 1. Synthesis

Since 2003, the University of Colombo School of Computing (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. During the current project period, UCSC has received more than 100 new cases, which we were able to help solve using our Forensics Lab.

As a result of this project, University of Colombo School of Computing (UCSC) has formally requested the government of Sri Lanka to recognize the Center of Digital Forensic (CDF) at UCSC as the national investigation center for Computer Forensic Investigation. During the project period, we have purchased essential hardware and developed necessary software tools required for operations. The CDF consists of the necessary hardware, software, and established investigation methods to assist the police force with computer crimes in Sri Lanka.

This progress report mainly summarizes our activities during the reporting period. In order to keep the final report concise, the following supporting documents are included as separate documents.

- Three (3) Research papers
- The report on the technical training program
- The user manual of the software
- Teaching materials (Lecture notes, video demonstrations, case studies etc.)

In general, the current vision for the CDF at UCSC is to establish itself as a leading research and investigation center for digital forensic investigation in the South Asia region. As the first step towards our vision, we have now established the CDF at a national level. Research activities and a core training program will continue after the initial project period.

## 2. Development Problem

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. At UCSC, we have also developed software and relevant materials, as we have found that the existing forensic frameworks and toolkits are impractical in the Sri Lankan context.

Before the commencement of the project, we conducted an initial study and found that there was a need for this procedure to be modified to suit the current Sri Lankan legislative situation. In addition, the existing tools are not practical for use within our current communications infrastructure. Sri Lanka, as well as many other developing

countries, has limited ICT resources. As a result we have designed our own model that consists of four main phases:

1. Collection and preservation;
2. Examination and analysis;
3. Presentation and reporting; and
4. Returning evidence.

During the creation stag of this new model, we clearly defined the activities associated with each phase (see table 1).

| Phase | Activities |
|---|---|
| Collection and preservation | • Duplicate digital evidence using a standardized, accepted procedure<br>• Lossless compression of disk image/copy<br>• Data sampling & reduction of unwanted data<br>• Data recovery<br>• Ensure integrity, validity, and authenticity of digital evidence<br>• Case management<br>• Managing investigators |
| Examination and analysis | • Determine when, how and by whom the data was produced<br>• Validate and interpret significant data<br>• Extract hidden data and pattern matching<br>• Recognize obvious pieces of digital evidence<br>• Transform data into more manageable size for analysis<br>• Organize analysis results obtained physical and digital evidence<br>• Build a time line |
| Presentation and reporting | • Present information found in the analysis phase in graphs, etc.<br>• Clarify evidence and documents findings |
| Returning evidence | Manage the return of evidence and reports to the proper owner |

**Table 1: Activities done under each phase of the proposed model**

We have decided upon and prioritized the above activities in compliance with available resources and legislative boundaries that currently exist in Sri Lanka. After defining these activities, a software tool called the Forensic Investigation Tool for Developing Countries (FIT4D) was implemented. FIT4D software can be used to perform the activities listed in the above table. The user manual of the FIT4D software is included as a separate document for your reference (Please refer to FIT4D-User-Manual.pdf).

## 3. Project Process

As previously mentioned, we have started developing a new digital forensic framework with a software toolkit and a clear set of guidelines to accommodate any type of computer related crime in a developing country such as Sri Lanka. Our previous studies

identified that the extended DRFWS model proposed by Mark Reith, Client Carr, and Gregg Gunsch as the most compatible existing model to the procedure followed by the forensic experts in Sri Lanka.

After the initial study, we have decided to use a four-phase model, employing processes that suit Sri Lanka's legislative environment and available resources. Then the FIT4D software toolkit was developed to provide functionalities for each activity.

Before we start our own development, we have analyzed the features of existing software on the market. As many of the common digital forensic analysis tools such as Encase and FTK are developed with commercial interests, making these tools unaffordable for organizations in developing countries.

There are also open source software kits such as Sleuth Kit, Pyflag, and PTK. Unfortunately, PyFlag is not widely used because of its complexity and difficulty of deployment. At the time of writing this report, the PTK developers have decided to close their source code. After completing a survey on available commercial and open source software and their functionalities, we developed our own software based on Carrier's Sleuth Kit Library.

The first version of our software was released in January to the selected user community. We have incorporated the feedback from this user community into the first version of the public release. The first training program was conducted in January, and the separate report on the workshop is included (please refer the workshop_report.pdf file). During the training program, we have trained forensic investigators from various government authorities to use our software. We continuously receive their feedback about our software and incorporate that feedback into our development.

## 4. Principal Findings

The software toolkit, which is best fit to the current investigation procedure carried out by the forensic experts in Sri Lanka, was developed. Teaching materials were developed, and a training program was conducted. The first version of software tool was released to the public. However, the software should be expanded to include additional features in next few months.

Two research papers were published about our research and two public talks were delivered about the project at both local and international conferences. The other two research papers have been accepted for publication in August and September 2010. The current version of the software is available to download from the following link as a Live CD. Training materials and video about the software is also available at score.ucsc.lk/fit4d web site.

Our research activities will continue after the initial project period. We have planned to improve our investigation toolkit by including data mining and neural network technologies in coming months.

## 5. Fulfilment Of Objectives

In general, following table shows the overall progress of each activity:

| Activity | Status |
|---|---|
| Purchasing literature | Done |
| Training UCSC staff | Fundamental training was completed. Further training may be required for the sustainability of the project. |
| Developing a suitable investigation model | Done |
| Designing software architecture | Done |
| Developing the software | Done. Further customization is required based on user feedback. |
| Preparing the specification of equipment | Done |
| Installation of the equipment | All necessary equipment was purchased. Upgrade of the equipment may be required in future. |
| Initial tests of the equipment and tools | Done |
| Conducting special training programs | The initial training was conducted. |
| Publishing research papers | Two papers were published and two other papers are accepted for publication in August and September 2010. |

**Table 2: Status of each Activity**

We have realized that due to the large volume of hard disk capacity, data available for investigation will be huge and the keyword search may not be practical. Therefore, we will investigate new methodologies to categorize electronic evidence based on pattern recognition, neural networking and data mining techniques. In order to complete this task, research assistants attached to the project will continue their activities until December 2011.

## 6. Project design and implementation

As mentioned, we have developed an extension for the TSK suite (The Sleuth Kit) that provides advanced features. The software presents all the features already present in available forensic browsers, as well as new essential forensic features that carry on the whole digital investigation process. We provided anew graphical and highly professional interface based on Ajax technology; this is in addition to the functionalities available in existing tools. Our software offers numerous features such as disk imaging, new

searching techniques, new file analysis techniques, and image processing techniques of complex digital investigation cases.

We deployed the FIT4D system across a distribution model. This presents a lower risk, as opposed to storing all the evidence information in a central server. FIT4D system is run on top of a peer-to-peer Virtual Private Network (VPN), which assures privacy and data authenticity. Police stations and investigators are the two main parties involved in the FIT4D system. In the ideal situation, all the police stations would have FIT4D servers, where they can store evidence related to crimes they are handling. Another option is that the individual investigators have exclusive access to the FIT4D system. Each police station and respective investigators are connected to via VPN, where privacy of the data is ensured by the IPSec protocol. Although there is a risk of transmitting sensual data through public network, this has been identified as the most manageable solution because a developing country cannot afford the cost of building a separate private network to handle forensic information. Additionally, we propose that public key infrastructure is implemented to provide end-to-end security using digital certificates. This will ensure that all data transmitted through network are digitally signed.

At present, we have deployed the prototype of the above proposed system in the laboratory. Therefore, investigators have to visit our laboratory and submit their digital evidence to the system. While developing the system we received feedback from field users and academic experts. Dr George R. S. Weir, from the Department of Computer and Information Sciences, University of Strathclyde (UK), works as our external research advisor. In last week of February, we gave Dr Weir and his graduate students at Strathclyde a demonstration of the FIT4D system and took their feedback. In mid-March, the demonstration was give to Asian open source community members at the Asia Open Source Software (AOSS) workshop (http://www.asia-oss.net/aoss25_mar10.htm) which was held in Singapore.

## 7. Project outputs and dissemination

The first version of the FIT4D software was released under a GPL license and documents were released under a Creative Common License. The software and documents are published on the score.ucsc.lk/fit4d/ web site.

After releasing the software, forensic investigation terminals were deployed at the laboratory and the first training workshop was conducted in January 2010. Twenty (20) participants from various government and private organizations attended the training workshop and a detailed report of this workshop is separately included. (Please refer workshop_report.pdf file).

The principal investigator, Dr Kasun De Zoysa, delivered two keynote addresses: one at the eAsia International Conference, December 2009 in Colombo Sri Lanka, and one at the Forensic Research Group Meeting at University of Strathclyde, February 2010 in

Glasgow, UK about the project outputs. The presentation slides are included as eAsiacrime.pdf file.

Two research papers were published at these international conferences. The electronic copies of these papers are separately included (please refer FIT4DPaper-CFET-2009.pdf and FIT4DPaper-CSSL-2009.pdf). Two other research papers have also been accepted for publication. Abstracts of these papers are included (please refer FIT4DPaper-CFET-2010.pdf and FIT4DPaper-CSSL-2010.pdf).

- Low Cost Forensic Tool for Analyzing Huge Data Sets in Digital Investigations, Yasantha N Hettiarachchi, T.N.K. De Zoysa, Keerthi Goonathillake, 4 International Conference on Cybercrime Forensics Education and Training, Canterbury Christ Church University, UK, 2-3 September, 2010
- Comparative Feature Analysis for "Forensic Investigation Toolkit for a Developing Country (FIT4D)", Yasantha N Hettiarachchi, Kasun De Zoysa, Keerthi Goonathillake, 28th National Information Technology Conference, The Computer Society of Sri Lanka, Sri Lanka, 11-12 August 2010
- FIT4D: A Forensic Investigation Toolkit for a Developing Country, Yasantha N Hettiarachchi, Kasun De Zoysa, Keerthi Goonathillake, 27th National Information Technology Conference, The Computer Society of Sri Lanka, Sri Lanka, 9-10 September 2009
- Developing a Forensic Software Toolkit for Sri Lanka, Yasantha N Hettiarachchi, T.N.K. De Zoysa, Keerthi Goonathillake, 3rd International Conference on Cybercrime Forensics Education and Training, Canterbury Christ Church University, UK, 1-2 September, 2009

Two senior lecturerers, Dr Kasun De Zoysa and Dr Laxman Jayarathne, attended a forensic training workshop and computer security conference, which were organized by the Open Web Security Application Project (OWSAP) in December 2009 in India. The knowledge gained from this international workshop was used at the training workshop held at the UCSC in January 2010.

In addition, at the postgraduate level, a forensic course will be introduced to the Master of Computer Security Program at UCSC in 2010-2011 (please refer MIS-Syllabus.pdf).

## 8. Capacity building

Two keynote addresses about the project outputs were delivered by the principle investigator Dr. Kasun De Zoysa at the eAsia International Conference, which was held in December 2009 in Colombo, Sri Lanka and Forensic Research Group Meeting at University of Strathclyde in February 2010 in Glasgow, UK. During the second week of march, the system was demonstrated to open source community in Asia at the Asia Open Source Software (AOSS) workshop (http://www.asia-oss.net/aoss25_mar10.htm)

which was held in Singapore.

The first training workshop was conducted in January 2010 and the second workshop is planed in March 2010. The course materials of the workshop is available to download and it can be used to conduct forensic training programs in the other countries.

Two(2) senior lectures, Dr. Kasun De Zoysa and Dr. Laxman Jayarathne attended a forensic training workshop and computer security conference which was organized by the Open Web Security Application Project (OWSAP) in December 2009 in India.

## 9. Project Management

Dr Kasun De Zoysa, senior lecturer at UCSC, works as the coordinator/advisor of the CDF4D research project. Mr K. S. Goonatillake, an engineer at UCSC, works as the advisor for the research project. Mr Kenneth Manjula Thilakarathna and Mr N. M. Laxaman are programmers and technical project managers. Ms Yasantha Hettiarachchi works as a Research Assistant and programmer.

## 10. Project Sustainability:

We have created a methodology for billing a nominal fee for each investigation. We project the CDF to begin generating its own income by 2011. In principal, this income will be used to maintain the CDF after the project period.

A Digital Forensic Investigation course is included in the planned Master of Science in Information Security program at UCSC. The syllabus of the proposed course and learning materials will be developed during project period. This new Master Degree will formally start in November 2010 and funds generated through this program will also be used to sustain the CDF at UCSC.

In addition to that, a new research proposal has been submitted to the European Union in January 2010 in collaboration with Stockholm University, Sweden.

## 10. Impact

The knowledge gained and software developed in this project directly contributed to the solving of 34 court cases in 2009. At the time of reporting, there are over 50 cases on the waiting list. Since all court cases are confidential we cannot reveal any details. The following table shows the receiving date of the some of the major cases, with the name of the majestic court and the digital media type. A quantified list of categories of these cases is illustrated in Figure 1.

| Date | Magistrate Court | Media |
|---|---|---|
| 7 Jan 2009 | Wattala | Memory,CD and Flash Drive |
| 15 Jan 2009 | Aluthkade | Laptop HD and Falsh Drive |
| 26 Jan 2009 | Colombo fort | Live computer System in a Bank |
| 27 Jan 2009 | Waunia | Back up Tape system of a Bank |
| 17 Feb 2009 | The Burea for the prevention of abuse of children & women | Computer HD |
| 19 Feb 2009 | Mathugama | Computer HD and Mobile Phone |
| 20 Feb 2009 | Matara | Digital Camera Chip |
| 24 Apr 2009 | Mount Lavinia | Computer HD |
| 5 May 2009 | Mahawa | Computer HD and Mobile Phone |
| 29 May 2009 | Colombo fort | Computer HD |
| 3 Jun 2009 | Colombo fort | Computer HD |
| 4 Jun 2009 | Walasmulla | Mobile Phone |
| 20 Jun 2009 | Colombo fort | Computer HD |
| 22 Jun 2009 | Colombo fort | Laptop HD and Computer HD |
| 29 Jun 2009 | Batticolo | Computer HD and Fake Visa Cards |
| 1 Jul 2009 | Colombo | Laptop HD |
| 10 Jul 2009 | Colombo fort | Computer HD |
| 20 Jul 2009 | Kurunegala | Computer HD and Flash Drive |
| 22 Jul 2009 | Mahawa | Flash Drive and Hard Disk |
| 24 Aug 2009 | Kaduwela | CTC Camera backup system |
| 25 Aug 2009 | Aluthkade | Mobile Phone |
| 25 Aug 2009 | Balangoda | Mobile Phone |
| 25 Aug 2009 | Child Protection Autority | Computer HD |
| 28 Aug 2009 | Kurunegala | Computer HD |
| 28 Sep 2009 | Colombo fort | Laptop HD |
| 1 Oct 2009 | Kurunegala | Laptop HD |
| 6 Oct 2009 | Colombo fort | computer HD and Laptop HD |
| 20 Oct 2009 | Colombo fort | Laptop HD |
| 23 Oct 2009 | Maligakanda | Live System at a System |
| 29 Oct 2009 | Aluthkade | Fake ATM Card , Laptop HD and ATM card printing system |
| 4 Nov 2009 | Mahawa | Computer HD |
| 5 Nov 2009 | Nugegoda | CD, Flash Drive,Memory Chip, Computer HD and Laptop HD |
| 24 Nov 2009 | Kegalle | CD and Mobile Phone |
| 4 Dec 2009 | Bambalapitiya Child Magistrate | Mobile Phone |

**Table 3: Information about Court Cases**

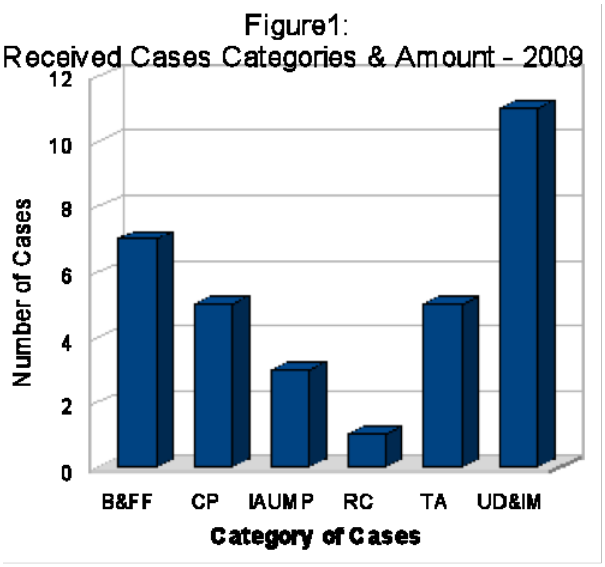
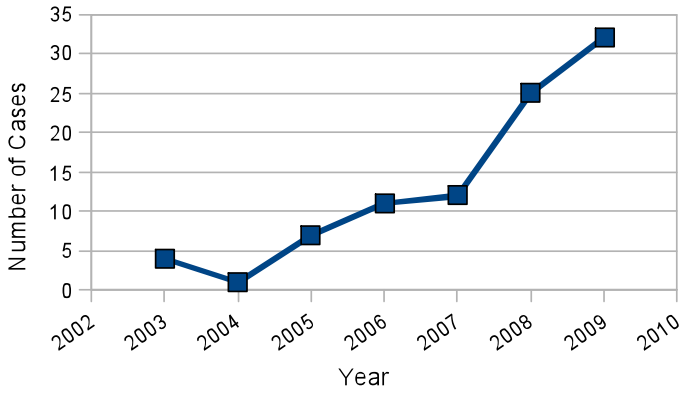



FIGURE 1 Legend

1. Banking and Finance Frauds *(B&FF)*
2. Child Pornography *(CP)*
3. Illegal Activities using Mobile Phones *(IAUMP)*
4. Terrorist Activities *(TA)*
5. Rape Cases *(RC)*
6. Unauthorized Document and Image Manipulations *(UD&IM)*

From 2009-2010, 47% of the court cases have been reported from Colombo district, and 43% were from outside the Western province. We also identified that the requests for support in finding evidence for digital crime cases have consistently increased during last few years (see the Figure 2).

Figure 2: Cases receiving progress




As depicted in Table 3, some of these cases are related to abuse directed at women and children. Therefore, we believe that output of this project has clear impact on the victims of the computer crimes in all social groups in all provinces in Sri Lanka.

## 11. Overall Assessment

In general, we have reached our goals within the given time frame (12 months). Having field investigators on the project team has given us valuable insight into the forensic industry. Even though we developed this software and documents for developing countries, it may be useful for developed countries as well. We have already received several inquiries regarding our work from universities and organizations in the UK.

We are pleased that the other forensic investigation organizations in Sri Lanka have started to use our software. The Sri Lanka Police and Defense Ministry will also use our software after they establish their forensic laboratories in mid-2010.

CDF will continue FIT4D research activities while conducting their investigations. Our achievements, research results, training materials, and activities are published on the score.ucsc.lk/fit4d web site.

## 12. Recommendations

We would like to recommend that ISIF provide a domain name for each project, in addition to the wiki page. For example, we would like to have fit4d.isif.asia as our official project web site. This would provide good visibility to our work, as well as ISIF, among the online community even after the project period has ended.

We suggest to simplify the technical reporting templates to cover only the following sections: 1) Introduction; 2) Project management; 3) Project process; 4) Fulfillment of objectives; 5) Project outputs and dissemination; 6) Impact; 7) Conclusion; 8) Recommendations.

ISIF funding program provides great opportunities to innovative Asian ICT researchers. The funding amount is sufficient to conduct quality work in a developing country. However, we recommend ISIF to consider a longer period for project implementation. This is specially relevant when project team are working to get a quality publication in competitive conferences and journals. In addition, formal financial procedures at the local institutes and the Asian countries may affect the process of fund transferring and purchasing equipments. Therefore, we would like to recommend a 24-month funding period instead of 12 months, with a budget of AUD 50,000.