**Introduction**

Digital Forensics Department (DFD) has successfully gone through a challenging year 2012. This report will summarize second half year of 2012. As previous years, DFD is providing the services in computer forensic and data recovery areas for all Local Enforcement Agencies in Malaysia and other government agencies. The challenges that DFD faced are the increase number of cases referred to DFD. The numbers of exhibits and size or volume of the media are also another hurdle which we need to tackle.

**Digital Forensics and Data Recovery Statistics**

Summary of Digital Forensics cases received as shown in Graph 1 below:

![Graph 1:Digital Forensics cases received by month for 2012](image-url)
The graph is digital forensics cases received by month. Total cases referred to DFD is 661. From this 661, 550 is fallen under Digital Forensic, which represents 83.2% of the case. The highest month case received was on October with 73. Towards end of the year, only 15 cases. The possibilities of up and down of the graph are most agencies have their own labs and they manage to handle simple cases on their own. As a result, they only sent to us the complicated and difficult cases. Smuggle, Harrasment and Bribery are the three top case categories for this 2012 digital forensic statistic.

Summary of Data Recovery cases received as shown in Graph 2 below:

111 out of 661 cases received was Data Recovery. It represents 16.8% of total cases. Month of October shows the highest cases received with 21 cases. The lowest case received was recorded in month of March and August, which are 8 in total. Most the cases received through CyberClinic which is total up to 71. This Cyber Clinic was established to cater the demand from the public and will be the receiving and marketing arm for this data recovery service.
Digital Forensics Department Achievement in 2012

Section A: Services and Product Provided

a) Digital Forensics Service

Graph 3 below charted the total cases handled by DFD from year 2002 to 2012.

DFD has also involved in high profile cases with other agencies. The cases are:

i. Ops Rokok

This operation was held in three different locations, Pulau Langkawi, Pulau Labuan, and Klang Valley. Three teams from DFD were assigned to assist law enforcement agencies for this Ops Rokok. This operation is a collaboration between LHDN and Bank Negara Malaysia. DFD assist the LEA’s Investigation Officers in order to seize the digital evidence.
ii. **Ops Arak**
This operation was held in Miri, Sarawak. DFD was requested by Kastam Di-Raja Malaysia to assist in digital evidence seizure. Two premises were raided and various alcohol tonic brands were seized by the enforcement.

iii. **Ops Aeroplane Parts**
United State of America believed some companies in Malaysia involved in purchasing aeroplane parts from USA and sell them to Iran. DFD was requested by special task forces to join the operation and assist enforcement agency, SPRM on the digital evidence seizure.

iv. **Ops DurianTV**
Another major case that DFD involved at national level was Ops Durian. This operation took place in Pulau Pinang. Two teams were sent to assist local enforcements agencies which involved from two agencies, PDRM and MCMC.

b) **ASCLD/LAB-International Quality Management System (QMS)**
CyberSecurity Malaysia Digital Forensic Laboratories has been recognized by ASCLD/LAB as the first organization in Asia Pacific to receive ASCLD/LAB-International accreditation in the field of Computer & Multimedia Discipline. With this recognition, DFD can better assist Law Enforcement Agencies and report produced by analyst from DFD can be accepted in court.

In early 2012, one of our Regulatory Bodies (RBs) in Malaysia, Malaysian Communication and Multimedia Commission (MCMC) has engaged DFD to develop Digital Forensics Quality Management System (QMS) for their digital forensics laboratory in accordance to ASCLD/LAB-International and ISO/IEC 17025. Trainings were given to MCMC forensic members on the system implementation. DFD team was also assisted them to develop computerized QMS, which will help them to automate their documentation.

**Training Courses & Certification**
In 2012, DFD has provided training course to 6 different agencies. They were Bank Negara Malaysia (BNM), Lembaga Hasil Dalam Negeri (LHDN), Polis DiRaja Malaysia (PDRM), Selangor University (UNISEL), Kuala Lumpur University (UNIKL), and KPerak. Most of the participants successfully passed the examination and were given certification.
Research and Development Blueprint

DFD R&D Roadmap focuses on long term and short term research and development, plan to enhance the current services and operations. Furthermore, the roadmap is designed to ensure the sustainability of the CyberSecurity Malaysia’s Digital Forensic Department business via exploration of new knowledge and services through R&D efforts.

This is also an effort to ensure CyberSecurity Malaysia’s Digital Forensics Department contribution is continuously significance to the nation. DFD has played a very eloquent role in helping our country’s Law Enforcement Agencies (LEAs).

DFD has already on the move with the short term research plan via collaboration with the Fakulti Teknologi Sains dan Maklumat of Universiti Kebangsaan Malaysia in exploring face recognition for video forensics analysis. Both parties has jointly applied Exploratory Research Grant Schemes (ERGS) from Ministry of Higher Education (MoHE), in which grant tenure started since July 2011. This project is expected to be completed in June 2013. Apart from this collaboration, DFD has already on the planning for more research collaborations with the current collaborator and other IPTAs namely Universiti Tenaga Nasional (UNITEN), Universiti Teknologi Malaysia(UTM) and Universiti Teknologi Petronas(UTP).

A few critical research fields are already identified for the future collaborations as listed below:

i. Embedded device recovery and forensics
ii. Video and image forensics
iii. Audio forensics
iv. Biometrics forensics
v. Digital forensics SOP, methodology and innovations.

Based on the fields mentioned, the research topics selected for the undertaking are:

i. Forensic Data Analysis and Recovery from Embedded Device Flash Memory
ii. CCTV Surveillance Video Enhancement: Super-Resolution and Denoising via advanced image processing algorithms.
v. Audio Authentication: The Exploration of Electrical Network Frequency (ENF) in audio forensics.
vi. Biometrics Forensics: Suspects Biometrics Identification System via multimedia files forensics


c) Digital Forensics Portal

Digital Forensics Portal was launched in January 2012. This portal was developed for in-house portal used. It was established to provide the latest data related to cases conducted in forensic laboratories to all DFD members on their daily tasks. All information and inputs will be updated in real time and it will summarize all cases submitted by Investigation Officers (IOs). By having this portal, it has indirectly reduced the case processing time and increase operation productivity and efficiency.

Section B: Key activities and achievement.

a) Paper Publication

In November 2012, two (2) of our papers have been accepted in the Soft Computing and Pattern Recognition International Conference (SoCPaR, Brunei). The papers will be available in conference proceedings published by IEEE.

The papers were:


ii. Super Resolution Hybrid Methods for CCTV Forensics Interpretation.

b) Nomination by MOSTI

Digital Forensics Department has been nominated by MOSTI for the Prime Minister's Innovation Award, in the category of information technology. Nomination is based on the commitment, contribution and achievement shown by DFD toward the nation. Huge cost saving was reported during RMKe-9 by utilizing local expertise from DFD.
Conclusion

There are a lot of great achievements despite lots of challenges in this 2012. Number of case is increased while the number of staff was maintained. In view of more agencies referred to DFD, we can summarize that the relationship and trust with LEAs is good and healthy. Even though some of the agencies start to have their own forensic facilities, assistance from DFD is still needed especially when dealing with complicated and high-tech crimes. We wish to get more funding and mandate on this forensic area so that we can be the center of excellent in near future.