Digital Forensics – CyberCSI

Prepared by: Aswami Fadillah Mohd Ariffin ; Nor Zarina Zainal Abidin
Author email address: aswami@cybersecurity.my ; zarina@cybersecurity.my
Department: Digital Forensic Department
Extension: 6933; 6946
Submission Date: 08th March 2010

1.0 Introduction

2009 has been a very challenging year for Digital Forensics Department (DFD) with the increase of cases from year to year. It is challenging due to the fact that all cases being handled by us were unique in a sense and we need to deal with different type of technologies. As such DFD has to be prepared in any circumstance and with this we are providing a full fledge Digital Forensic Services to all Law Enforcement Agencies (LEAs) including Regulatory Bodies (RBs) with Standard Operating Procedure (SOP) in accordance to ASCLD/LAB-International (an ISO 17025 and American Society of Crime Lab Directors Standard dedicated to promoting excellence in forensic science through leadership and innovation).

As the vision of DFD of CyberSecurity Malaysia in the Ninth Malaysia Plan is "To be a National Centre of Reference and Excellence in Digital Forensics with ASCLD/LAB-International Accreditation", our commitment and passion have been soaring in every each year in assisting the country LEAs and RBs. This vision has keep us on the toe and with the closing of all cases including expert testimonies given by our dedicated analysts we deemed year 2009 was another successful year for the department. Nonetheless, DFD will always strive to provide the best Digital Forensics Service not only in the country but also at international level and our priority will always be to the Malaysia LEAs and RBs.

2.0 DFD Activities

2.1 Statistic of cases

In 2009, DFD has managed to successfully analyze a total of 374 cases. These cases were referred to us by various LEAs and RBs such as PDRM, KDRM, MCMC, SSM, SC, KPDNKK, SPRM, MINDEF and others (refer Figure 1). Thus so far, from year 2002 to 2009, DFD has assisted our LEAs and RBs with 1186 cases with a broad case background (refer Figure 2) including 50 onsite investigations this year alone.

As shows in Figure 2, harassment is the highest cases received by DFD in year 2009. Harassment can be divided into three types of cases which are threat, blackmail and sexual harassment. The second highest category is financial fraud where almost of the cases came from pyramid and investment scheme.

Illegal business, game piracy and copyright falls under 'Others' category and has recorded 18% of the cases. Document falsification or forgery of documents such as passport and form stated only 11% on the statistic. Sedition, internet scam, physical attack, gambling and robbery stated the low percentage (below 10%) where DFD only received 16 cases of sedition, 16 cases of internet scam, 8 cases of physical attack and 2 cases for both gambling and robbery.

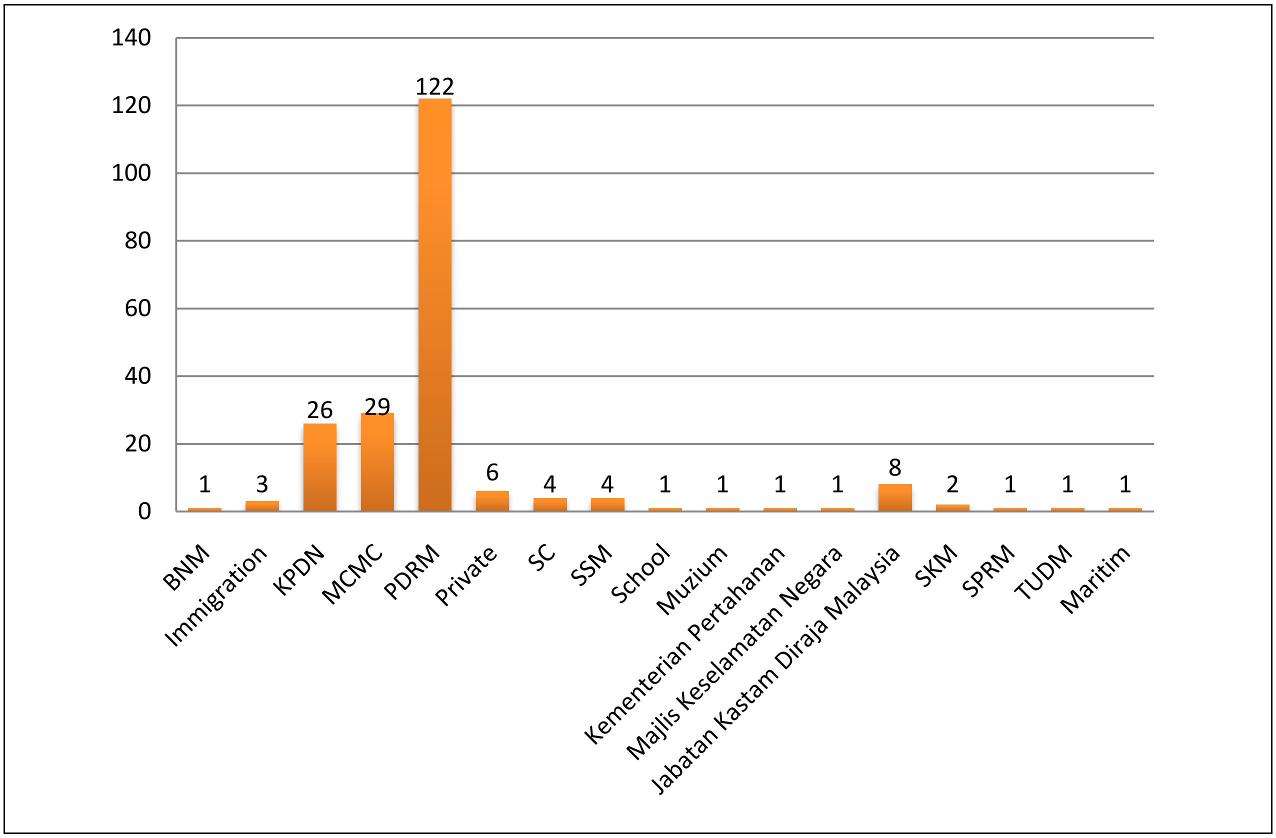

Figure 1: Total Cases Received by Agencies

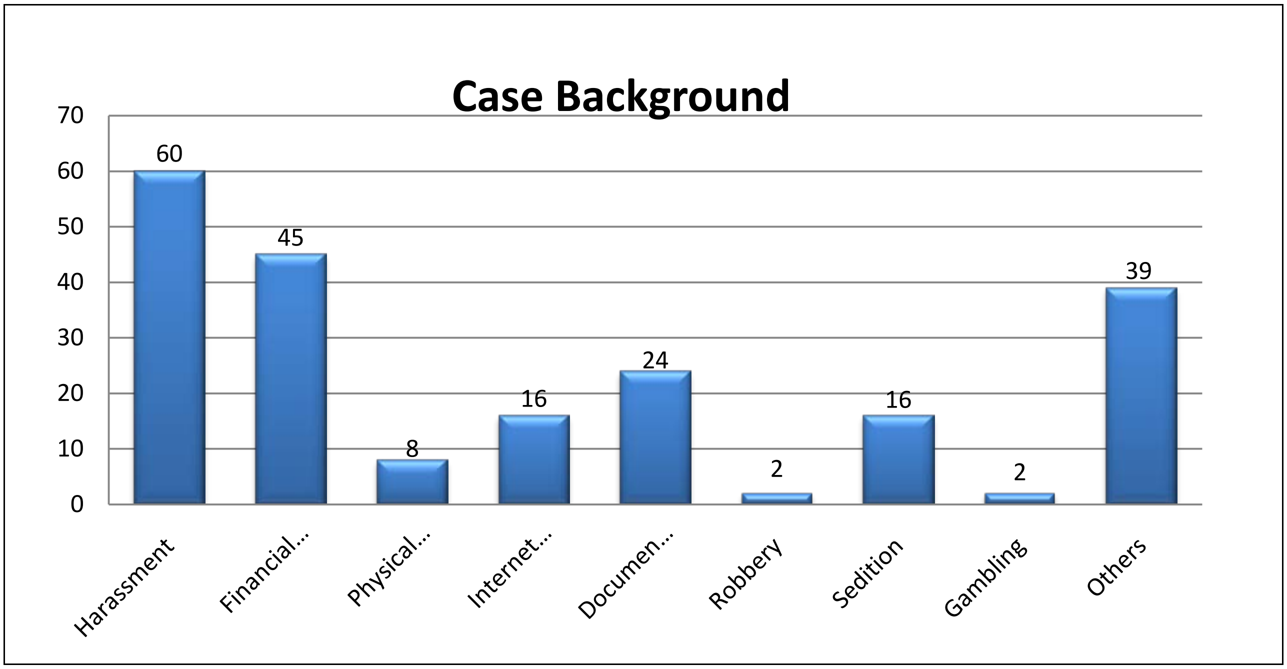

Figure 2: DFD Case Background

Figure 3 below, shows an increase of approximately 26% compared to the previous year. This increase in percentage has been a trend and DFD believe the number of digital cases will inevitably rise in the years to come. With this anticipation, our service is being recognized vital for the country and it has been part of the National Key Result Area (NKRA).

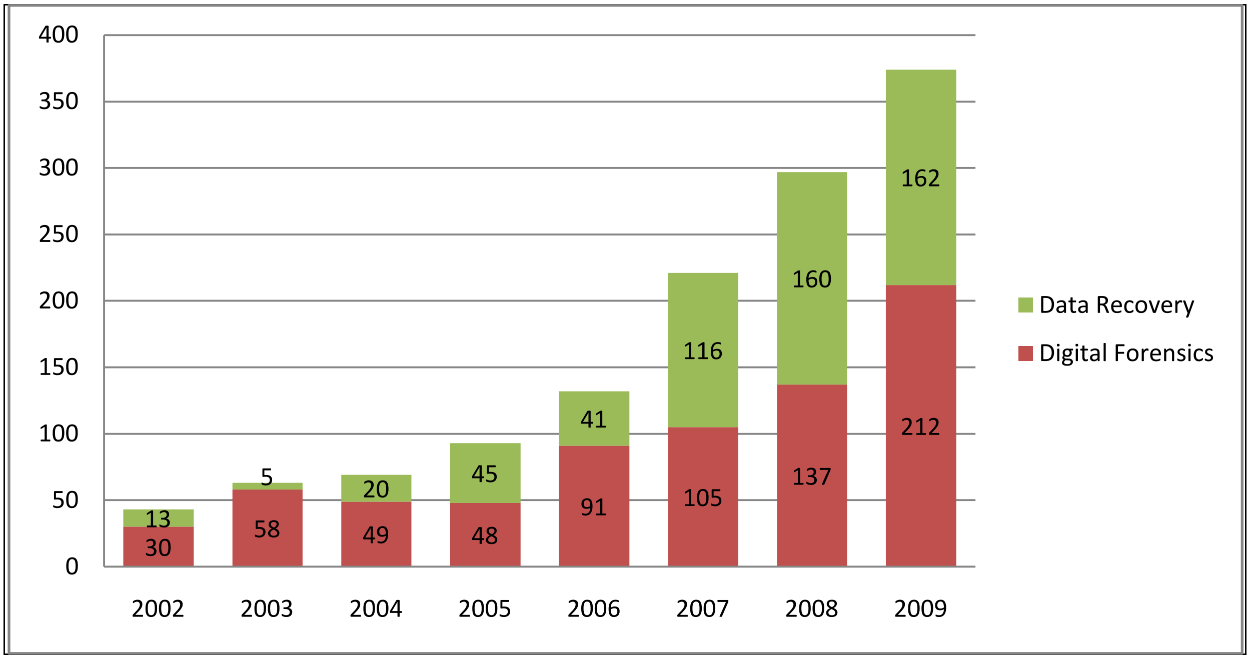

Figure 3: Yearly DFD Case Statistics

2.2 Talks & Knowledge Sharing

Below are some of the invitations (local and international) to speak at seminars, forum and workshop in Year 2009 where Digital Forensics analysts had participated:

- Talk on Digital Forensics at International Symposium and Cybercrime Response, Seoul, South Korea
- Talk on Digital Forensics at the OIC CERT Seminar, Kuala Lumpur
- KPDNKK Perlis Digital Forensics Workshop, Perlis
- Cyber Security Talk at Institution of Engineers, Putrajaya
- Talk on Prevention in Financial Crime & Bribery Forum, Kuala Lumpur
- Talk on Digital Forensics at International Symposium of Forensic Science & Health of Environment, Kuala Lumpur
- Talk on Digital Forensics for Legal Department of Lembaga Hasil Dalam Negeri Malaysia (LHDNM), Kuala Lumpur

Also, in Year 2009, DFD has successfully conducted one series of knowledge sharing in digital forensics at SecureAsia Conference brought by CyberSecurity Malaysia from 6 to 7 of July 2009. It has been attended by our so called Special Interest Group (SIG) mainly from the LEA and RBs to discuss on the issues in investigating cases that contains digital evidence and the way forward resolution. This SIG talk has also invited two digital forensic experts from Microsoft Asia and CEDAR Audio representatives as a speaker to add some new information related to digital forensics. In the same event, DFD has presented other topics such as “Quality Management in Digital Forensics Laboratory”, “Digital Media Investigation: The New Perspective” and “Lawful Interception: The Time Is Now!”

Apart from above, under the initiate of knowledge sharing, DFD has continuously participating in talk and lecture invitations to all interested parties from the government, non-profit organization and private sectors. DFD has also conducted digital forensic trainings to LEAs and RBs and one of the said training was Digital Forensics training for Certified Fraud Examiner (CFE) under the Central Bank of Malaysia (Bank Negara Malaysia).

2.3 Research & Development

Additionally, DFD is always committed in the area of Research & Development (R&D). After a rigorous research and development initiatives we have successfully produced and distributed to LEAs and RBs our 2nd version of Digital Forensics Live CD and Pocket Guide for Digital Forensics First Responders.

These products have all the essentials tools and information when conducting digital forensics investigation.

Through our R&D programs to create awareness and improvement in digital forensics investigation, as a result, there were several MoUs signed with local IPTS and IPTA. One example was collaboration with Management & Science University (MSU) on the Bachelor Degree curriculum in computer forensics. We also assisted other varsities and colleges such as UiTM, UUM, UTM, UKM, UIA, and UTP with course module development, part-time lecturing, student internship programs and supervising research programs at postgraduate level. This genuine endeavor is done in order to help producing more graduates in digital forensics expertise. Up to date we were informed that all the efforts have began to be fruitful where more students have enrolled in digital forensics related courses.

3.0 Conclusion

2009 has been another great year for us and we would like to use this achievement as a motivation for more successes especially in the Tenth Malaysia Plan. Most probably we will carry the same vision when we are into the Tenth Malaysia Plan as it has been proven noble. Last but not least, DFD will serve and strive continuously in looking and venturing ways to improve the service delivery processes for our stakeholders.