CyberCSI–Half Year 2011, Summary Report

Introduction

The Digital Forensics Department (hereinafter referred to as DFD) of CyberSecurity Malaysia has been gazetted under the Criminal Procedure Code (CPC) 399 on 23rd February 2009. This is the same gazette that was awarded to the Malaysian Chemistry Department on 3rd August 2004. According to the CPC, all reports and testimonials from DFD analysts are accepted by the Malaysia courts of law. DFD analysts has been tasked to assist law enforcement agencies (hereinafter referred to as LEA) in Malaysia (such as Royal Malaysian Police (PDRM), Malaysian Anti-Corruption Commission (MACC), Malaysian Communications and Multimedia Commission (MCMC) and the Securities Commission Malaysia) to analyse cases involving digital evidence.

This first half 2011 summary report provides an overview of activities undertaken by the DFD. These activities are related to case analysis received from the LEA and regulatory bodies (hereinafter referred to as RB) and trainings sessions and talks given to LEA, RB and public based organisations on digital forensics modules. The summary will also describe the number and types of cases handled by DFD in the first six (6) months of 2011.

Digital Forensics and Data Recovery Statistics

Digital Forensics Case Statistics

From January to June 2011, DFD handled 208 cases in digital forensic and 76 cases in data recovery. There was an increase trend compared to the same period in 2010, with a 29 percent increase in digital forensics and a 2.7 percent increase in data recovery. Digital Forensics inadvertently comprised cases concerning computer forensics, mobile forensics, audio forensics and video forensics submitted by LEA and RB.

The increased in numbers was contributed by wide usage of broadband in Malaysia where the utilisation of high-speed Internet networks is regarded increasingly more important for the development of the Malaysian society. Broadband services facilitate and are now necessary to maintain and increase the everyday quality of life, irrespective of living area.

Figure 1: Illustrates the cases received in Jan – Jun 2011 according to the scope of cases handled by DFD.

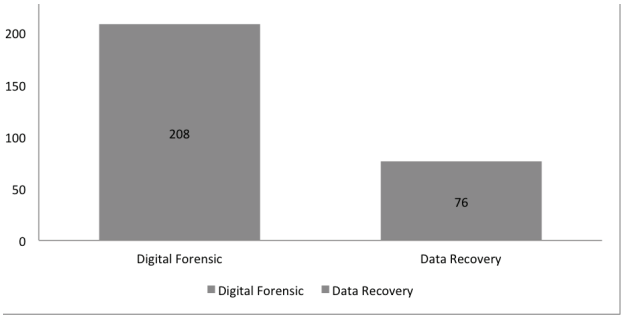


Figure 1: *Breakdown by Scope Classification in Jan-Jun 2011*

The chart in figure 2 shows the types of cases breakdown received by DFD in the period between Jan – Jun 2011. There are three (3) major cases that have been classified as of 'highest priority' which is Copyright, Bribery and CCTV/Video extraction. Other minor cases which also contributed to the statistics were Financial Fraud, Illegal Business, Harassment, Internet Scams, Document Falsification, Sedition and Internet Gambling.

Figure 2: Illustrates the breakdown of the types of cases received by DFD

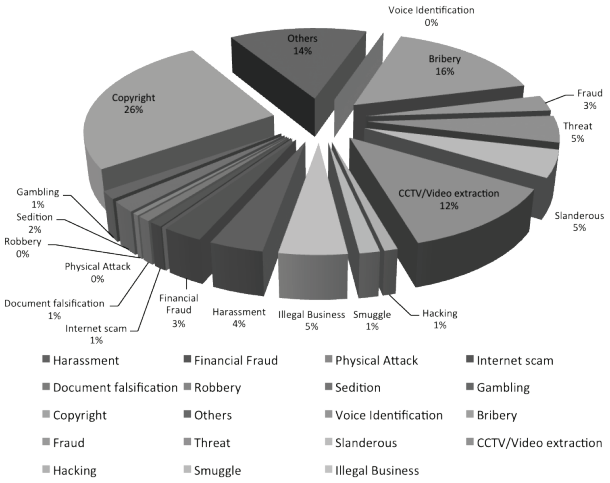


Figure 2: *Breakdown by Types of Digital Forensics Cases*

This period show a tremendous increase in copyright infringement cases of up to 26 percent, which comprised of 54 cases compared to 19 cases in 2010. Copyright infringement can be classified as plagiarism or piracy where it involves the "wrongful appropriation," "close imitation," or "purloining and publication" of another author's "language, thoughts, ideas, or expressions," and the representation of them as one's own original work. Most of the cases received from KPDNKK related to pirated songs, movies and books. Recently, DFD analysts were involved in analysing pirated software and computers seized by KPDNKK. At the same time, KPDNKK also requested DFD's assistance to join their raids, especially in cases that need technical processing at the crime scene itself.

Bribery cases were the second highest contributor to this year's numbers with 33 cases reported. While dealing with these type of cases, DFD provide support to LEA in analysing emails, text messages, multimedia messages, calls via electronic gadgets such as mobile phones, notebooks, hard disks and thumb drives that has been used as case evidences. DFD also forms one of the task force units for Ops 3B. During this operation, the DFD task force focuses solely on corruption and bribery elements within each case. This operation was lead by MACC (Malaysian Anti-Corruption Commission).

Other cases of concern are CCTV/Video extraction where 25 cases were reported in 2011. These are examples of CCTV cases analysis:

i. Video Authenticity - verify the genuineness and originality of video sources

ii. Video Content Analysis - analyse content in term of any object and activity recorded by CCTV systems

iii. Facial Identification - match CCTV footages with photos received

iv. Object Comparison - compare objects displayed on CCTV with objects received. Example: attire comparison

v. Video Frame Enhancement - improve quality of video frames

However, the success rates for CCTV cases depend on the quality of the devices itself. Currently, the majority of devices received were low in quality and this has impacted the findings as it is impossible to enhance poor quality video images. There should be an awareness campaign for the public to use more reliable devices and adopt strategic CCTV installations for their safety. DFD will also share with LEA and RB on the importance of this matter to ensure that investigation can be carried out smoothly.

Data Recovery Case Statistics

Data recovery is the process of salvaging data from damaged, failed, corrupted, or inaccessible secondary storage media when it cannot be accessed normally. Often, data are salvaged from storage mediums such as internal or external hard disk drives, solid state drives (SSD), USB flash drives, storage tapes, CDs, DVDs, RAID, and other electronics. Recovery may be required due

to physical damage to the storage device or logical damage to the file system that prevents it from being mounted by the host operating system.

Another scenario involves a disk-level failure, such as a compromised file system or disk partition or a hard disk failure. In any of these cases, the data cannot be easily read. Depending on the situation, solutions involve repairing the file system, partition table or master boot record, or utilising hard disk recovery techniques ranging from software-based recovery of corrupted data to hardware replacement on a physically damaged disk. If hard disk recovery is necessary, typically, the disk itself has failed permanently, and the focus is rather on a one-time recovery, salvaging whatever data that can be read.

In a third scenario, files have been "deleted" from a storage medium. Typically, deleted files are not erased immediately; instead, references to them in the directory structure are removed, and the space they occupy is made available for overwriting. In the meantime, the original file may be restored. Although there is some confusion over the term, "data recovery" may also be used in the context of forensic applications or espionage.

Figure 3: Illustrates the breakdown of cases received under Data Recovery (Jan-June 2011)

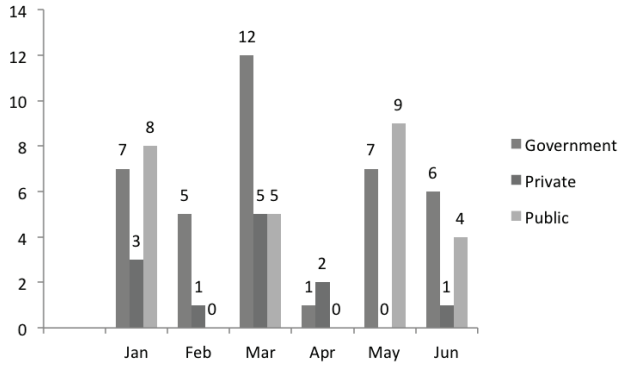


Figure 3: *Breakdown of cases received by Sector under Data Recovery (Jan-June 2011)*

Figure 3 show breakdown of cases received by different sectors in 2011. It can be concluded that cases received from the government sector contributed to the highest majority with 38 cases, followed by public with 26 cases and private with 12 cases. The increase in the trend was also contributed by public awareness on the importance of data safety. They would prefer sending their devices to more trusted and reliable organisations with highly trained professionals who practices international standards of operations like DFD compared to other normal service providers. The wide usage of storage media such as hard disks and thumb drives by the public and organisations also contributed to this increase.

Others Activities

During this period, DFD conducted several training sessions and lectures, which involved participants from government bodies and enforcement authorities as well as local universities. The objectives of the training programmes were to share knowledge between DFD experts and participants so that both parties can benefit and discuss latest issues and technologies. The summaries obtained will be focussed on DFD's research and development and their collaboration with local higher institutions.

Talk

DFD has conducted several talks as requested by LEA, RB and institutions such as PDRM, Department of Pharmacy, Judicial and Legal Training Institute (ILKAP), Companies Commission of Malaysia (SSM), Royal Malaysian Customs Academy (AKMAL) and Universiti Teknologi Mara (UITM). Favourite topics requested by them are related to digital forensics and information security in Malaysia. The sessions create awareness on the importance of digital forensics to employees at these agencies

and the need to practice it daily. Besides training professionals at LEA, stakeholders and other government agencies, these sessions also help to ensure sustainability and effective dissemination of information and resources.

Training

Besides case investigation and talks, DFD also offer five (5) training modules to LEA and the public at large. These include:

i. Digital Forensics for Non IT Background
ii. Digital Forensics for First Responders
iii. Digital Forensics Investigation & Analysis
iv. Data Recovery (Advanced)
v. Forensics on Internet Applications (Advanced)

These courses are designed to expose digital forensic practitioners to forensic examinations and analyses based on specific interests. It is designed for those who would like to know how to solve unique forensic cases. At this moment, the agencies that have joined these training programmes are Telekom Malaysia, Ministry of Defence Malaysia (MINDEF) and the Arab Police Department.

Research and Development

Currently, the R&D of DFD collaborates with Universiti Kebangsaan Malaysia (UKM) in obtaining the Exploratory Research Grant Scheme (ERGS). The purpose of ERGS is to promote research and the early discovery of knowledge that can contribute to the increased level of intellectualism, the creation of new technologies and a dynamic cultural enrichment environment in line with Malaysia's national aspirations. DFD has also engaged two projects under Ministry of Science, Technology & Innovation, Malaysia called the E-Science Fund. The projects are Case Profiling, a collaboration with University Teknologi Malaysia (UTM) and Facial Recognition which is a collaboration with UKM. The projects will provide benefits to both parties in terms of acquiring knowledge and skills.

Four (4) DFD analysts presented papers at the International Conference on Pattern Analysis and Intelligent Robotics 2011 (ICPAIR 2011) International in Putrajaya on the 27th and 28th of June 2011. The presenters and their topics were as below:

i. Nazri Ahmad Zamani & Mohamad Zaharuddin Ahmad Darus - *"Multiple-Frames Super-Resolution for CCTV Forensics"*

ii. Sarah Khadijah Taylor & Mohd Izuan Effenddy Yusof - *"Forensic Acquisition on MP3 Forensics"*

Conclusion

This 1st half-year report shows increases of 31.7 percent from the last period in cases received by DFD. The cases reported to us during this period increased daily and it is believed the number will rise in the future. Thus, the field of digital forensics will continue to grow in line with current information technology developments which are in tandem with the awareness level of the masses on the use of technology. Therefore, training sessions, talks, and R&D are important elements to be balanced with new and growing information technology disciplines and cyber crimes. ■

CyberCSI 3rd Quarter 2011Summary Report

Introduction

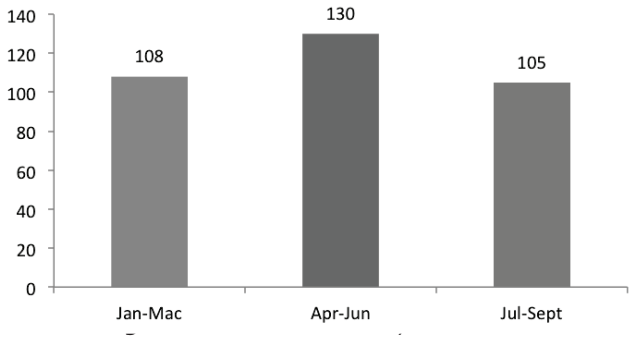
The CyberCSI Third Quarter Summary Report provides an overview of activities undertaken by the Digital Forensics Department (hereinafter referred to as DFD) of CyberSecurity Malaysia for the month of July, August and September in 2011. These activities are related to case analysis received from law enforcement agencies (hereinafter referred to as LEAs) and regulatory bodies (hereinafter referred to as RBs) such as Royal Malaysian Police (PDRM), Malaysian Anti-Corruption Commission (MACC), Malaysian Communications and Multimedia Commission (MCMC) and the Securities Commission Malaysia (SC). This summary will also highlight the training sessions and talks given to LEAs, RBs and public based organisations on modules encompassing digital forensics.

Digital Forensics and Data Recovery Statistics

Digital Forensics Case Statistics

From July to September 2011, DFD handled 105 cases in digital forensics. Digital Forensics cases comprised cases concerning computer forensics, mobile forensics, audio forensics and video or image forensics submitted by LEAs and RBs.

Figure 1: Illustrates cases on Digital Forensics received from July to September 2011.



The chart in Figure 2 shows the category breakdown of cases received by DFD in the period between July – September 2011. There are three (3) major categories that have been classified as of 'highest priority' which is Bribery, Illegal Business and CCTV/ Video Extraction. Other minor cases which also contributed to the statistics were Threat, Fraud, Smuggling, Harassment and Others.

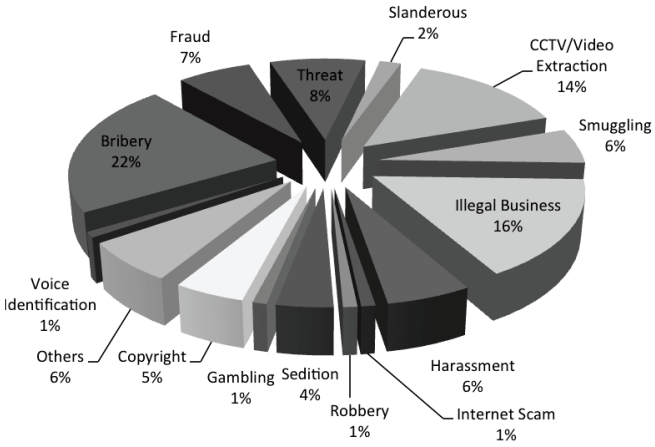


Figure 2: *Breakdown by Categories of Digital Forensics Cases*

Bribery cases were the highest contributor with 22 cases reported. When dealing with these types of cases, DFD provides support to LEAs by analysing emails, text messages, multimedia messages, calls via electronic gadgets such as mobile phones, notebooks, hard disks and thumb drives that were used as case evidences. DFD was also involved in the task force units consisting of various LEAs for *Ops* 3B. During this operation, the DFD teams focused solely on corruption and bribery elements within each case. This operation was led by BNM (Bank Negara Malaysia).

The Illegal Business category was at second place for this period with 16% share of the total cases recorded. This category showed an increase in its trend as compared to DFD's half year statistic (Jan-Jun) which was only at 5%.

Based on the statistics, there was a 20% reduction in numbers compared to previous quarters. This is might due to the establishment of digital forensics laboratory by some LEAs, for example PDRM's Forensic Cheras Facility and the MACC facility. When it involves high profile cases, these LEAs normally will be referred to by the DFD. In doing so, these LEAs can validate their findings by having a trusted second party to carry out the necessary analysis. This is also proof that the LEAs practises impartiality. Most of the LEAs and RBs were trained by DFD's professionals. This would indirectly strengthen the cooperation between the two sides enable the sharing of expertise in their respective fields. The establishment of digitals forensics labs by LEAs showed that our aim to empower our LEAs has started to produce results. DFD can now focus more on cases which requires more technical and advance technology. This type of cases needs more in-depth research since the criminals are more IT savvy and more up-to-date tools are used.

Data Recovery Case Statistics

Data recovery is the process of salvaging data from damaged, failed, corrupted, or inaccessible secondary storage media mediums when it cannot be accessed normally. Often, data is salvaged from storage mediums such as internal or external hard disk drives, solid state drives (SSD), USB flash drives, storage tapes, CDs, DVDs, Redundant Array of Independent (or Inexpensive) Disks (RAID), and other electronics storage mediums. Recovery may be required due to physical damage to the storage device or logical damage to the file system that prevents it from being mounted by the host operating system.

Another scenario involves a disk-level failure, such as a compromised file system or disk partition or a hard disk failure. In any of these cases, the data cannot be easily read. Depending on the situation, solutions involve repairing the file system, partition table or master boot record, or utilising hard disk recovery techniques ranging from software-based recovery of corrupted data to hardware replacement on a physically damaged disk. If hard disk recovery is necessary, typically, the disk itself has failed permanently and the focus is rather on a one-time recovery, salvaging whatever data that can be read.

In a third scenario, files have been "deleted" from a storage medium. Theoretically, deleted files are not erased immediately; instead, references to them in the directory structure are removed, and the space they occupy is made available for overwriting. In the meantime, the original file may be restored.

Figure 3 shows the breakdown of cases received under Data Recovery (Jul-September 2011) from Public, Private and Government Agencies in Quarter 3 of 2011.

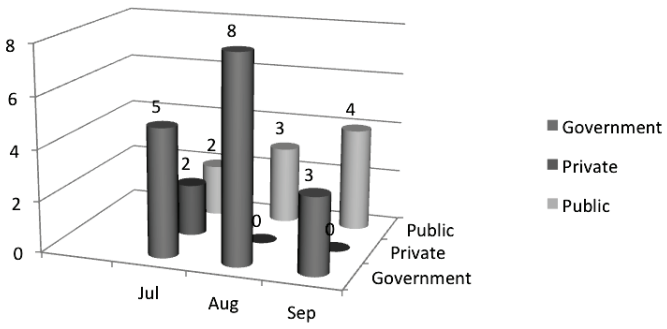


Figure 3: *Breakdown of cases received by Sector under Data Recovery (Jul-Sept 2011)*

It can be concluded that cases received from the government sector constituted the highest majority with 16 cases, followed by the public sector with nine cases and the private sector with two cases. Effective from October 2011, Data Recovery services will be taken over by CyberSecurity Clinics. CyberSecurity Clinic is another initiative by CyberSecurity Malaysia with the aim to help

Malaysians with the following objectives:

1. To provide an avenue for consumers to obtain assistance and to resolve issues in relation to cyber security, cyber safety and data privacy from a trusted service provider at a competitive price.
2. To serve as a citizen 'touch-point' and to demonstrate the government's commitment to the people by meeting and satisfying their needs.

Others Activities

During this period, DFD has conducted several training sessions and lectures, which involved participants from government bodies and enforcement authorities as well as local universities. The objectives of the training programmes were to share knowledge between DFD experts and participants so that both parties can benefit and discuss latest issues and technologies. The summaries obtained will focus on DFD's research and development and their collaboration with local higher institutions.

Talk

DFD has conducted several talks as requested by LEAs, RBs and other institutions such as Department of Pharmacy, *Judicial and Legal Training Institute* (ILKAP), Companies Commission of Malaysia (SSM), Royal Malaysian Customs Academy (AKMAL) and Universiti Teknologi Mara (UITM). Favourite topics requested were related to digital forensics and information security in Malaysia. The sessions aimed to create awareness on the importance of digital forensics to employees at these agencies and the need to practice it in their daily tasks. Besides training professionals at LEAs, stakeholders and other government agencies, these sessions also help to ensure sustainability and effective dissemination of information and resources.

Research and Development

Currently, the R&D Unit of DFD collaborates with Universiti Kebangsaan Malaysia (UKM) in obtaining the Exploratory Research Grant Scheme (ERGS). The purpose of ERGS is to promote research and the early discovery of knowledge that can contribute to an increase in the level of intellectualism, the creation of new technologies and a dynamic cultural enrichment environment in line with Malaysia's national aspirations.

One research was conducted in July 2011, named *"A 2.5D Facial Identification by Using Fuzzy Bees Algorithm for Video Forensics Analysis"*. The Process Flow for this research is as below:

3. Equipment Purchasing
4. Assembly and Test
5. Data Collection
6. Researching methodology for 2D and 3D face recognition
7. Project expected to be completed by August 2012

Conclusion

In conclusion, the field of digital forensics will continue to grow in line with current information technology developments which are in tandem with the awareness level of the masses on the use of such technology. The public, LEAs and RBs are now more aware on the increase in threats for cyber-crimes and that it requires more effort to combat them. Therefore, training sessions, talks and R&D are important elements to be balanced with new and growing information technology disciplines and cyber-crimes. ■

CyberCSI 4th Quarter 2011 Summary Report

Introduction

The CyberCSI's Fourth Quarter Summary Report provides an overview of activities undertaken by the Digital Forensics Department (hereinafter referred to as DFD) of CyberSecurity Malaysia for the month of October, November and December 2011. The activities for this quarter are more focused on ASCLD/LAB Accreditation and case analysis received from law enforcement agencies (hereinafter referred to as LEAs) and regulatory bodies (hereinafter referred to as RBs) such as Royal Malaysian Police (RMP), Malaysian Anti-Corruption Commission (MACC), Malaysian Communications and Multimedia Commission (MCMC) and the Securities Commission Malaysia (SC). This summary will also highlight the training sessions and talks given to LEAs, RBs and public based organisations on digital forensics modules.

The 1st Digital Forensic Laboratory Accredited With ASCLD/Lab in Asia

ASCLD/LAB was originally created as a committee of its mother organisation, the American Society of Crime Laboratory Directors (ASCLD) in 1998. It was created as a voluntary programme and remains one today. It offers voluntary accreditation to public and private crime laboratories in the United States and around the world. Accreditation is offered in forensic disciplines for which services are generally provided by forensic laboratories.

The American Society of Crime Laboratory Directors/Laboratory Accreditation Board (ASCLD/LAB) is the oldest and most well known crime/forensic laboratory accrediting body in the world. ASCLD/LAB has been accrediting crime laboratories since 1982 and currently accredits most federal, state and local crime laboratories in the United States including forensic laboratories in six other countries.

Before laboratories were accredited, ASCLD/LAB established four objectives for its programme. The four objectives have remained unchanged since the inception of the programme. ASCLD/LAB subsequently established a Quality Policy Statement and a Statement of Guiding Principles for Forensic Scientists and Forensic Laboratories.

The objectives of the ASCLD/LAB accreditation programme are:

1. To improve the quality of crime laboratory services provided to the criminal justice system.
2. To develop and maintain criteria which can be used by a crime laboratory to assess its level of performance and strengthen its operations
3. To provide an independent, impartial and objective system by which laboratories can benefit from a total operational review
4. To offer to the general public and to users laboratory services a means of identifying those laboratories which have demonstrated that they meet established standards

We are proud to announce that the Digital Forensics Lab of CyberSecurity Malaysia has officially received an accreditation from ASCLD International on 3rd November 2011. This is a direct recognisition of CyberSecurity Malaysia as the first organisation in Southeast Asia to obtain this certification. It is also an achievement to be proud of as DFD worked hard for three years to obtain the certificate. Some of the cases submitted by the LEAs for analysis will usually be brought to court for arbitration. Analysts involved will appear in court to testify on cases that have been analysed. This certificate is important as it is a measure of DFD credibility, which will be adopted by the courts later.

Digital Forensics and Data Recovery Statistics

Digital Forensics Case Statistics

From October to December 2011, DFD handled

99 cases in digital forensics. Digital Forensics cases comprised cases concerning computer forensics, mobile forensics, audio forensics and video or image forensics submitted by LEAs, RBs and Public.

Figure 1: Illustrates the Digital Forensics cases received from October to December 2011.

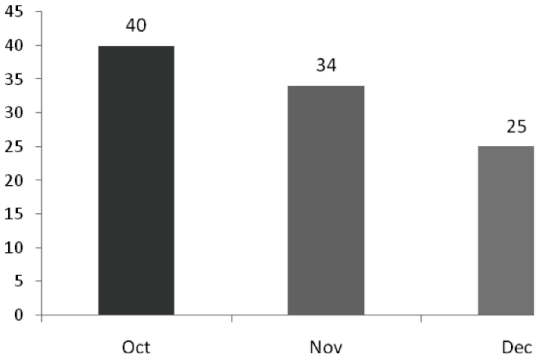


Figure 1: *Cases Breakdown from October to December 2011*

The chart below shows the categories of cases breakdown received by DFD in the period between October – December 2011. There are three (3) major categories that have been classified as of 'highest priority' which is Copyright, Bribery and CCTV/Video Extraction.

Figure 2: Illustrates the breakdown of the categories of cases received by DFD

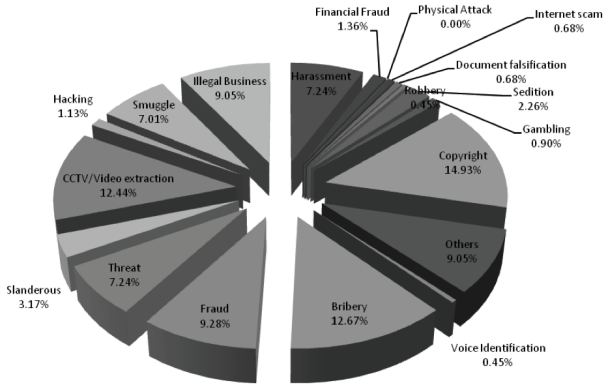


Figure 2: *Breakdown by Categories of Digital Forensics Cases (Oct-Dec 2011)*

Copyright cases were highest contributor with 14.93% cases reported. Infringement (or copyright violation) means the use of materials protected by copyright laws without the consent, it violates one of the original copyright owner's exclusive rights, such as the right to reproduce the copyrighted work or exercise, or create work products based on the copyrighted work.

From the point of law, piracy means copying activity, distribution and use of intellectual property products illegally without the permission of the copyright holder of the intellectual property. Piracy is an offence under the Copyright Act 1987. Intellectual property refers to any product and the work is registered copyright, such as books, music, film, television and radio broadcasts, computer software and industrial design. All intellectual property is protected by the Copyright Act 1987.

Piracy is rampant in Malaysia due to several factors:

1. Lack of awareness among consumers about intellectual property.
2. Pirated product prices far cheaper than genuine products.
3. Misuse of technology such as CD writers and DVD writers on the computer used for piracy.
4. Abuse of the Internet makes it a medium spread pirated products.

Bribery cases were the second highest contributor with 12.67% cases reported. When dealing with these type of cases, DFD provides support to LEAs by analysing emails, text messages, multimedia messages, calls via electronic gadgets such as mobile phones, notebooks, hard disks and thumb drives that has been used as case evidences. DFD also involved in the task force units with consists of various LEAs for Ops 3B. During this operation, the DFD teams focuses solely on corruption and bribery elements within each case. This operation was lead by BNM (Bank Negara Malaysia).

CCTV/Video Extraction category was at third place for this period with 12.44% cases recorded. Here are examples of CCTV cases analysis:

1. Authenticity of video- verify sources of video either genuine or not.
2. Video content analysis- analyze the content in term of any object and activity recorded by CCTV system
3. Facial identification- match CCTV image with photo received
4. Object comparison-compare the object displayed on CCTV with object received.

Example: attire comparison

5. Video frame enhancement- improve the quality of video frame

However, the success rates for the CCTV cases are really depending on the devices quality itself. Currently, majority of the devices received were in low quality and this has impacted the findings as it's impossible to enhance the poor quality video images. There should be awareness to the public to use more reliable devices and strategic CCTV installation area for their safety. DFD will also share with LEA's and RB's on the importance of the matters to ensure investigation can be handled smoothly.

Data Recovery Case Statistics

Figure 3: Illustrates the breakdown of cases received under Data Recovery (Oct-Dec 2011)

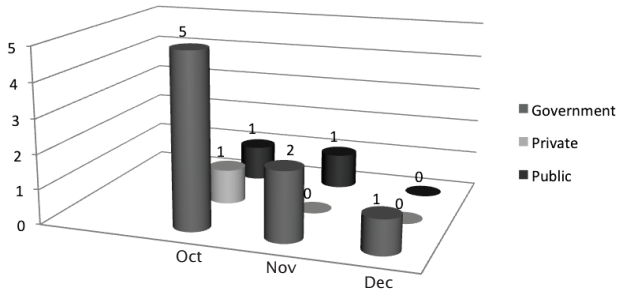


Figure 3: *Breakdown of cases received by Sector under Data Recovery (Oct-Dec 2011)*

Figure 3 show breakdown of cases received from Public, Private and Government Agencies in Quarter 4 of 2011. It can be concluded that cases received from the government sector contributed to the highest majority with 8 cases, followed by public with 2 cases and private with 1 case. Data Recovery cases reduce due to a few factors:

1. The service charges imposed for the data recovery services (starting Jan 2011)
2. Effective from October 2011, Data Recovery service taken over by CyberSecurity Clinics. The objectives of its setting up are:
   - To provide an avenue for consumers to obtain assistance and to resolve issues in relation to cyber security, cyber safety and data privacy from a trusted service provider at competitive cost
   - To serve as a citizen 'touch-point' and to demonstrate the government's commitment to the people by meeting their needs.
3. Outside competitors-the competitors might offer lower price to the public. Public also willing to take risk on data security. This might due to lack of awareness on security of data.

Talk and Training

For year 2011, DFD have been successfully conducted talks and trainings to the related parties such as government bodies and enforcement authorities as well as local universities. Not less than 20 trainings conducted which includes various topics on Digital Forensics area. For 2012 onwards, DFD will continue to serve in giving training to the LEAs and RBs in handling cybercrimes.

DFD offers five (5) trainings to the LEAs, RB, other institutions and public who interested on Digital Forensics such as:-

1. CSMDF Essentials Digital Forensic For Non-IT Background
2. CSMDF01 Digital Forensics for First Responder
3. CSMDF02 Digital Forensic Investigation & Analysis
4. CSMDF03 Data Recovery (Advanced)
5. CSMDF04 Forensics on Internet Application (Advanced)

Conclusion

In total, year 2011 have given many valuable experiences and challenges to the Digital Forensics Department through high profile cases and ordinary cases. Certainly the sweetest moment is when our lab have accredited by ASCLD / LAB (first accredited in Asian) and had successfully helping local authorities to solve their cases.

We foresee 2012 will be another challenging year for DFD. With very dynamic and active works in R&D and manufacturing for new digital equipments and applications, DFD will be exposing to more tough tasks to cope with. However with the enthusiasm and capability plus availability of the up-dated tools, all these challenges hope will make DFD be a better organisation. As always, we will continuously render our services to all our stakeholders.■