PERKHIDMATAN MyDFLab MAMPU

Datin Dr Siti Hanom binti Marjuni (hanom@mampu.gov.my)
Mohd Zabri Adil bin Talib (zabri@cybersecurity.my)

PENDAHULUAN

Sains forensik merupaka satu bidang sains yang menjalankan kajian ke atas penyiasatan sesuatu teori jenayah dengan mengaplikasikan ilmu sains seperti biologi, kimia, fizik dan teknologi maklumat. Proses siasatan teori jenayah ini pula perlulah mematuhi syarat dan sistem perundangan Malaysia. Forensik digital adalah istilah yang digunakan dalam mengaplikasikan sains teknologi maklumat dalam membantu penyiasatan jenayah digital, dimana keterangan dalam bentuk data digital yang diperolehi dalam peralatan elektronik digunakan dalam siasatan dan pembuktian kes di mahkamah.

Kaedah forensik ini penting terutamanya apabila keterangan tersebut diperolehi daripa eksibit yang bersifat tersembunyi dan tidak dapat dikenalpasti melalui pancaindera manusia. Contoh eksibit yang bersifat tersembunyi ini adalah seperti keterangan cap jari dan maklumat *Deoxyribonucleic acid* atau DNA. Kedua-dua contoh keterangan ini hanya boleh diperolehi dengan menggunakan teknik saintifik dan peralatan yang khusus.

Keterangan data digital juga berada dalam kategori eksibit yang bersifat tersembunyi. Terutamanya data digital yang telah dipadam dari sesebuah peralatan elektronik. Data digital yang telah

dipadamkan ini, hanya boleh diperolehi semula menggunakan teknik saintifik dan peralatan yang khusus dan digunakan dalam pembuktian kes pendakwaan di mahkamah.

Di Malaysia, aktiviti pencerobohan dan penggodaman computer,serangan virus, kecurian maklumat,pengintipan dan sebagainya semakin meningkat setiap hari. Berdasarkan statistic pada **Jadual 1**, pada tahun 2017 sebanyak 7,962 kes telah diterima oleh Malaysia Computer Emergency Response Team (MyCERT). Antaranya melibatkan kes seperti penipuan online, pencerobohan, percubaan pencerobohan, gangguan siber dan spam.

#	JAN	FEB	MAC	APR	MAY	JUN	JUL	AUG	SEP	OCT	NOV	DEC	TOTAL
Content Related	2	5	9	2	9	2	1	4	2	2	5	3	46
Malicious Codes	94	68	65	62	92	71	62	56	64	60	46	74	814
Denial of Service	11	0	3	3	1	3	8	6	2	2	1	0	40
Intrusion	98	201	148	101	138	284	146	363	181	121	119	111	2,011
Intrusion Attempt	39	19	32	41	22	8	37	31	8	9	11	9	266
Spam	26	38	24	30	31	32	36	30	29	26	17	25	344
Fraud	296	233	274	265	346	298	329	382	466	351	340	241	3,821
Vulnerabilities Report	5	2	8	3	1	4	2	11	6	10	5	3	60
Cyber Harassment	41	45	64	71	119	39	27	25	32	36	31	30	560
	612	611	627	578	759	741	648	908	790	617	575	496	7,962

Jadual 1: Statistik kes aduan insiden siber yang direkodkan oleh MyCERT

Dalam usaha untuk memantapkan penyelarasan dan pemantauan khususnya dari aspek keselamatan penggunaan ICT di sector awam, MAMPU telah melaksanakan Projek Pembangunan Keselamatan Siber Sektor Awam atau Cyber Security Development

Project (CSDeP). Salah satu sub projek di bawah CSDeP adalah membangunkan Makmal Forensik Digital yang dikenali sebagai MyDFLab.

OBJEKTIF PENUBUHAN MyDFLab

MyDFLab atau Malaysian Government Digital Forensics Lab merupakan satu inisiatif kerajaan untuk memantapkan dan memperkukuhkan keupayaan dan kepakaran pasukan GCERT (*Government Computer Emergecy Response Team* dan pasukan *Computer Computer Emergency Response Team* (CERT) di agensi-agensi sektor awam dalam bidang forensik digital. Keupayaan dan kepakaran ini penting bagi membolehkan pasukan GCERT dan CERT memberikan tindak balas terhadap insiden siber pada tahap yang terbaik.

MyDFLab telah dirasmikan pada 6 Disember 2016. Makmal yang terletak di Pusat Data Sektor Awam (PDSA) Cyberjaya ini menyediakan perkhidmatan berpusat untuk menerima laporan insiden keselamatan ICT dan membuat pelarasan tindakan pembetulan. Perkhidmatan yang ditawarkan oleh MyDFLab termasuklah:

a) Pemulihan data;
b) Sanitasi data;
c) Forensik komputer;
d) Forensik peranti mudah alih; dan
e) Penggunaan peralatan, latihan dan garis panduan kepada kementerian dan agensi kerajaan yang memerlukan dan

berminat untuk meningkatkan kapasiti dan proses pengendalian forensik komputer.

MyDFLab merupakan makmal forensik digital yang pertama seumpama dibangunkan di sektor awam. Pembangunan makmal ini mematuhi piawaian ISO/IEC 17025: 2005, iaitu memenuhi keperluan keseluruhan untuk makmal pengujian yang kompeten dan penentukuran. Makmal ini dilengkapi dengan peralatan khusus untuk menjalankan siasatan forensik digital. Sebagai contoh, *Forensic Toolkit*(FTK) dan *xry Mobile Forensics* digunakan dalam proses pemeriksaan dan analisis forensik digital. Terdapat juga peralatan lain seperti Ninja DEMI yang digunakan untuk memelihara data digital dari kerosakan, perubahan atau hilang.

Bagi tujuan pemuliharaan data pula, MyDFLab telah menyediakan peralatan yang dinamakan PC3000 UDMA dan clean booth. PC3000 UDMA mampu menjalankan diagnosis dan pemulihan data cakera keras berdasarkan antaramuka SATA (serial ATA) dan ATA (IDE) daripada pelbagai pembekal, kapasiti dan faktor bentuk manakala *clean booth* digunakan untuk memulihara data dalam persekitaran terkawal dan bebas habuk.

MyDFLab juga dilengkapi dengan peralatan forensik *hard disk crusher* yang digunakan semasa menjalankan sanitasi data secara fizikal untuk memastikan data-data sulit kerajaan dimusnahkan secara kekal mengikut piawaian antarabangsa yang telah ditetapkan.

PROGRAM LATIHAN TEKNIKAL FORENSIK DIGITAL

Sepanjang bulan September 2016 hinggabulan Februari 20i8 sebanyak 11 sesi latihan yang melibatkan latihan teknikal forensik digital, latihan penggunaan peralatan, pemeliharaan data, latihan penggunaan peralatan sanitasi telah pun dilaksanakan. Tujuan utama latihan-latihan ini adalah untuk memberi panduan kepada Pegawai GCERT dan CERT bagaimana menggunakan makmal dan peralatannya dengan cara yang betul.

Selain dari program latihan teknikal forensik digital, pasukan MyDFLab juga telah menghadiri Forensic Euro Expo 2017 yang telah diadakan pada 3 hingga 4 Mei 2017 bertempat di Olympia London. Ianya merupakan persidangan dan pameran antarabangsa yang membawa professional dan semua bidang sains forensik daripada pelbagai negara. Sepanjang persidangan tersebut peserta tidak melepaskan peluang untuk mendengar sendiri perbincangan dan sama-sama meneroka kemajuan terkini dalam teknologi forensik.

Pasukan juga telah diberi pendedahan mengenai teknologi dan pengurusan makmal menerusi beberapa aktiviti termasuklah lawatan strategic ke pusat keselamatan dan makmal forensik luar negara seperti National Cyber Security Center (NCSC) dan Metropolitan Police Service (MPS) Digital Forensics Lab, United Kingdom (UK) pada 5 Mei 2017. Lawatan ini bertujuan untuk memantapkan lagi pengetahuan terkini mengenai teknologi, operasi, pengurusan dan penyelidikan forensik digital bagi menyokong keselamatan ruang siber dan sistem perundangan

negara. Peluang ini juga dilihat sebagai medium untuk bertukar buah fikiran, pengalaman dan mengwujudkan kerjasama dengan pakar industri keselamatan siber.

Usaha ini amat penting dan sinonim dengan peranan MAMPU sebagai sebuah agensi perundingan dan penyelidikan yang unggul serta menjadi rujukan utama agensi-agensi di sektor awam. Secara tidak langsung ia juga dapat meningkatkan kredibiliti MAMPU sebagai Ketua Perkhidmatan ICT Kerajaan.

OPERASI MyDFLab

Penggunaan perkhidmatan MyDFLab telah pun dikuatkuasakan pada 17 Julai 2017 melalui surat arahan Ketua Pengarah MAMPU. Sejak penubuhannya, sebanyak lima (5) agensi iaitu Kementerian Perdadangan Antarabangsa dan Indurtri (MITI), MAMPU, Bahagian Permata, Jabatan Perdana Menteri, Kementerian Luar Negeri (KLN) dan Kementerian Pembangunan Wanita, Keluarga dan Masyarakat (KPWKM) telah memohon untuk mendapatkan perkhidmatan pemuluhan dan sanitasi data yang melibatkan sebanyak 388 unit cakera keras.

Berdasarkan **Jadual 2**, semua kes yang melibatkan perkhidmatan sanitasi data Berjaya dijalankan. Proses sanitasi ini disertakan bersama sijil verifikasi bagi memastikan semua data telah dilupuskan. Bagi kes yang diterima daripada Kementerian Perdagangan Antarabangsa dan Industri, hasil diagnosis awal menunjukkan ketiga-tiga cakera keras yang dihantar mempunyai kerosakan fizikal. Kerosakan fizikal ini melibatkan bahagian *printed*

circuit board, yang mana alat ganti diperlukan untuk menjalankan proses pemulihan untuk menjalankan proses pemulihan data. Kes ini tidak berjaya diselesaikan kerana tiada alat ganti elektronik.

No	Nama Jabatan / Agensi Sektor Perkhidmatan Awam	Bil. Cakera Keras	Jenis Perkhidmatan
1	Kementerian Perdagangan Antarabangsa dan Industri (MITI)	3	Pemulihan data
2	MAMPU (DDMS)	236	Sanitasi data
3	Bahagian PERMATA Jabatan Perdana Menteri	2	Pemulihan dan sanitasi data
4	Kementerian Luar Negeri	146	Sanitasi data
5	Kementerian Pembangunan Wanita, Keluarga dan Masyarakat	1	Pemulihan data

Jadual 2: Statistik bilangan cakera keras dan jenis perkhidmatan oleh MyDFLab

CABARAN PERKHIDMATAN FORENSIK DIGITAL

Cabaran yang paling utama dalam bidang forensik digital adalah untuk menyesuaikan diri dengan teknologi terkini yang sentiasa berubah dan berkembang seiring dengan peredaran masa. Juruanalisa forensik digital perlu sentiasa berusaha meningkatkan pengetahuan mengenai teknologi maklumat merentas pelbagai peralatan elektronik seperti komputer, peralatan elektronik mudahalih, teknologi system pengoperasian komputer, sistem fail komputer, sistem GPS dan banyak lagi. Mereka juga perlu

menghadiri pelbagai kursus yang berkaitan secara berkala untuk meningkatkan kecekapan dan kekal kompeten.

Selain dari itu, peralatan anti forensik yang canggih juga semakin banyak dan mudah diperolehi. Peralatan anti forensik ini berkemampuan untuk memadam data secara kekal. Data digital yang dipadamkan menggunakan peralatan anti forensik ini tidak dapat dipulihkan semula walaupun dengan menggunakan peralatan forensik digital. Terdapat juga peralatan anti-forensik yang berkemampuan untuk eksploit data digital supaya si pelaku tidak boleh disabitkan dengan kesalahan jenayah tersebut.

Sesetengah alat ganti cakera keras sukar diperolehi dan kosnya juga tinggi. Sebagai contoh, dalam kes pemulihan data, kerosakan fizikal pada media storan digital memerlukan alat ganti lazim seperti *slider* dan *printed cuircuit board* mengikut pengeluar dan modelnya. Tanpa alat ganti yang sesuai, pemulihan data tidak dapat dijalankan.

KESIMPULAN

Secara keseluruhannya, penubuhan MyDFLab berjaya melengkapi serta meningkatkan keupayaan dan kepakaran pasukan GCERT dan CERT untuk menjalankan siasatan forensik digital dengan lebih cekap dan berkesan. Kini agensi kerajaan boleh mendapatkan perkhidmatan dan menghantar peranti mereka untuk mengembalikan data yang hilang, membuat pembersihan data atau sanitasi dan pemulihan data tanpa perlu merujuk kepada pakar luar negara. Secara langsung ia dapat mengurangkan kos kerajaan.

MAMPU akan terus memberikan tumpuan dalam pembangunan kompetensi dan kepakaran khususnya dalam bidang keselamatan dan pertahanan siber dalam usaha untuk melindungi ruang siber dari sebarang bentuk risiko yang boleh mengancam maklumat dan keselamatan negara.

Usaha ini juga dapat dilihat penting sebagai langkah untuk menyokong pembangunan dan memakmuran negara apatah lagi untuk menjadikan Malaysia sebagai hub ekonomi terbaik di rantau ASEAN dan menarik lebih ramai pelabur. Ini sudah pasti akan memberikan kesan yang besar ke atas ekonomi dan membawa banyak faedah kepada masyarakat di negara ini.

.