



# **PERKONGSIAN ILMU Kemajuan Kerjaya – Laluan Pakar Bidang Khusus (SME)**

**BootCamp Keselamatan Maklumat  
24 September 2020**

**JABATAN PERKAMPUSAN**



# AGENDA



**1** **MENGENAI SME**

**2** **FUNGSI MYDFLAB**

**3** **WAY FOREWARD**



# SME

## PENGURUSAN KESELAMATAN MAKLUMAT

Kemajuan Kerja – Lalan Pakar Bidang Khusus (SME)

Rujukan : ([Pekeliling Perkhidmatan Bilangan 1 Tahun 2019](#) )

### PERSEDIAAN SME:

- ✓ Minat
- ✓ Rutin kerja
- ✓ Latihan/kursus/seminar/bengkel
- ✓ Penglibatan projek
- ✓ Pensijilan

1. KESELAMATAN DAN PERLINDUNGAN MAKLUMAT (ms 22-24)
2. PENGURUSAN INSIDEN DAN FORENSIK (ms 25-27)
3. PENILAIAN TADBIR URUS DAN AUDIT KESELAMATAN MAKLUMAT (ms 28-30)

SSA

**UPDATE SPK**

<https://spk.mampu.gov.my>

Penempatan

BIL	DIMENSI SME	MARKAH PENUH
I	Kelayakan Profesional	10
II	Penulisan/Penerbitan/Pembentangan	15
III	Khidmat Nasihat	10
IV	Penglibatan Projek	30
V	Khidmat Perundingan	30
VI	Mentoring	5
<b>JUMLAH</b>		<b>100</b>



Penilaian	Wajaran			
	Tahap 1 Gred 48	Tahap 2 Gred 52	Tahap 3 Gred 54	Tahap 4 JUSA C
LNPT	80%	60%	40%	20%
SSA	20%	40%	60%	80%



# MALAYSIA GOVERNMENT DIGITAL FORENSIC LAB (MYDFLAB)



MyDFLAB merupakan salah satu skop di dalam projek *Cyber Security Development Project* (CSDeP) dengan kerjasama CyberSecurityMalaysia (CSM).  
(26 Ogos 2016 – 25 Ogos 2018)

Malaysian Digital Forensic Lab (MyDFLAB) MAMPU telah dirasmikan pada **6 Disember 2016** oleh Yang Berbahagia Datuk Joseph Entulu Belaun, mantan Menteri di Jabatan Perdana Menteri pada ketika itu.

**Mengurangkan kos, perkhidmatan ini boleh menggunakan peralatan secara percuma di MyDFLab**

**Mengukuhkan keupayaan dan kepakaran pasukan Government Computer Emergency Response Team (GCERT) dan CERT bagi agensi dalam bidang forensik digital**

## OBJEKTIF PEMBANGUNAN MYDFLAB

Perkhidmatan pengendalian kes sanitasi dan pemulihan data serta forensik komputer dan mobil. kepada agensi sektor awam

Menjalankan kajian bagi penyelesaian masalah yang melibatkan pemulihan data dan sanitasi data.

## KRITERIA PEMBANGUNAN MYDFLAB

Memenuhi keperluan makmal forensik digital berdasarkan standard ISO/IEC 17025

Memenuhi keperluan minimum spesifikasi perkakasan/perisian dan sistem pengurusan kualiti makmal forensik yang dibekalkan.

**1 Polisi | 4 Prosedur | 5 SOP**

**31 Perisian | 34 Perkakasan**



# PERKHIDMATAN MALAYSIA GOVERNMENT DIGITAL FORENSIC LAB (MYDFLAB)



Penyediaan perkhidmatan dan kemudahan forensik digital secara berpusat kepada semua agensi Sektor Awam merangkumi:

## Status Pelaksanaan Sehingga Ogos 2020:

2020 : 26 Eksibit  
 2019 : 857 Eksibit  
 2018 : 795 Eksibit  
 2017 : 457 Eksibit  
 2016 : 3 Eksibit



FTK      XRY      BLANCCO      ATOLA INSIGHT

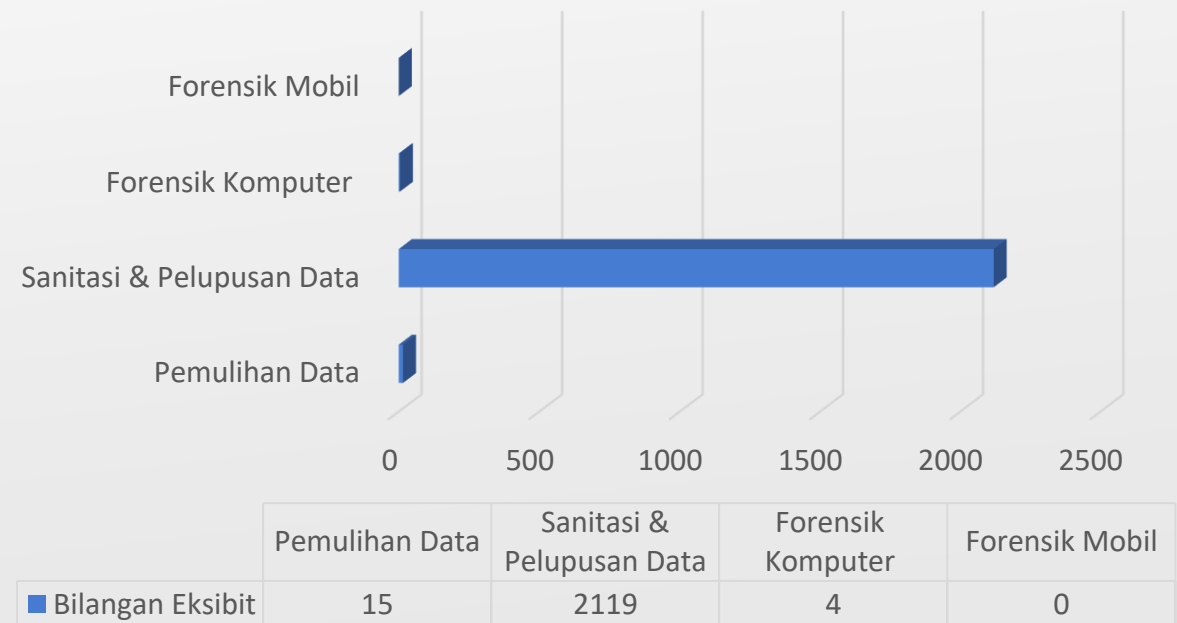
AXIOM      SUPER-DUPER      R-STUDIO



VOOM-3P      PC-3000

ATOLA RECYCLER

Bilangan Eksibit





# **LATAR BELAKANG PROJEK MALAYSIA GOVERNMENT DIGITAL FORENSIC LAB (MYDFLAB)**



## **PROJEK MALAYSIA GOVERNMENT DIGITAL FORENSIC LAB (MYDFLAB)**

Skop Utama Projek:

- i. Pembangunan Makmal Forensik Digital (MyDFLab);
- ii. Pembangunan Sistem Pengurusan Kes dan Kualiti (MyDFCaMS)
- iii. Perolehan Perisian
- iv. Perolehan Perkakasn Forensik



# CONTOH PENGGUNAAN BLANCCO DRIVE ERASER – ENTERPRISE EDITION

Notifications (0) Language: English Help Mampu\_Admin

blancco Management Console version: 5.5.0

Dashboard Reporting Users Licenses Support

Dashboard

+ [New dashboard](#)

### Dashboard :

#### Login details

Name: (Mampu\_Admin)  
Last login: 2020-07-15 09:56:57

**Completed erasures:**  
Since last login: 0

#### Import reports

You can quickly import reports by using the import widget. Click on the import button to open the report importing dialog:

[Import](#)

#### Available licenses

Product name	Available	Expiration date
Blancco Drive Eraser - Enterprise Edition	5979	2022-07-30 08:00

#### Consumed licenses

Product name	Consumed licenses
Blancco Drive Eraser - Enterprise Edition	21

Gambar 1: Dashboard Blancco Management Console



# CONTOH PENGGUNAAN BLANCCO DRIVE ERASER – ENTERPRISE EDITION

## Data Erasure Report



**Customer Details** Customer Name: testing

### Erasure Results

**Disk: 1 (1-1)** Vendor: **HGST** Model: **HTS725050A7E630** Serial: **RCF50ACE28TLYM**  
 Size: **500GB** Bus: **SATA** Sectors: **976773168**  
 HPA: **Doesn't exist** DCO: **Doesn't exist** Remapped Sector(s): **0**  
 Health Status: **good**

Remapped Sector(S) After Erasure: **0**

Start/End Time: **2020-07-14 08:52:16 (+0000) / 2020-07-14 10:21:05 (+0000)**  
 Duration: **01:28:49**  
 Method: **NIST 800-88 Clear**  
 Erasure Rounds: **1 (1 overwriting)**  
 Status: **Erased**

### Hardware Details

Manufacturer: **HP**  
 Chassis Type: **Notebook**  
 Model: **HP ProBook 430 G3**  
 Serial: **5CD6010PSK**  
 UUID: **317aab86-b40f-11e5-9467-08b0e602a021**  
 Asset Tag: **5CD6010PSK**  
 System SKU Number: **L6D84AV**  
 Processor: **GenuineIntel, Intel(R) Core(TM) i7-6500U CPU @ 2.50GHz, Cores: 2, Stepping: 3, Nominal speed: 2500MHz, Max speed: 3100MHz, External Clock: 100 MHz**

### Report Details

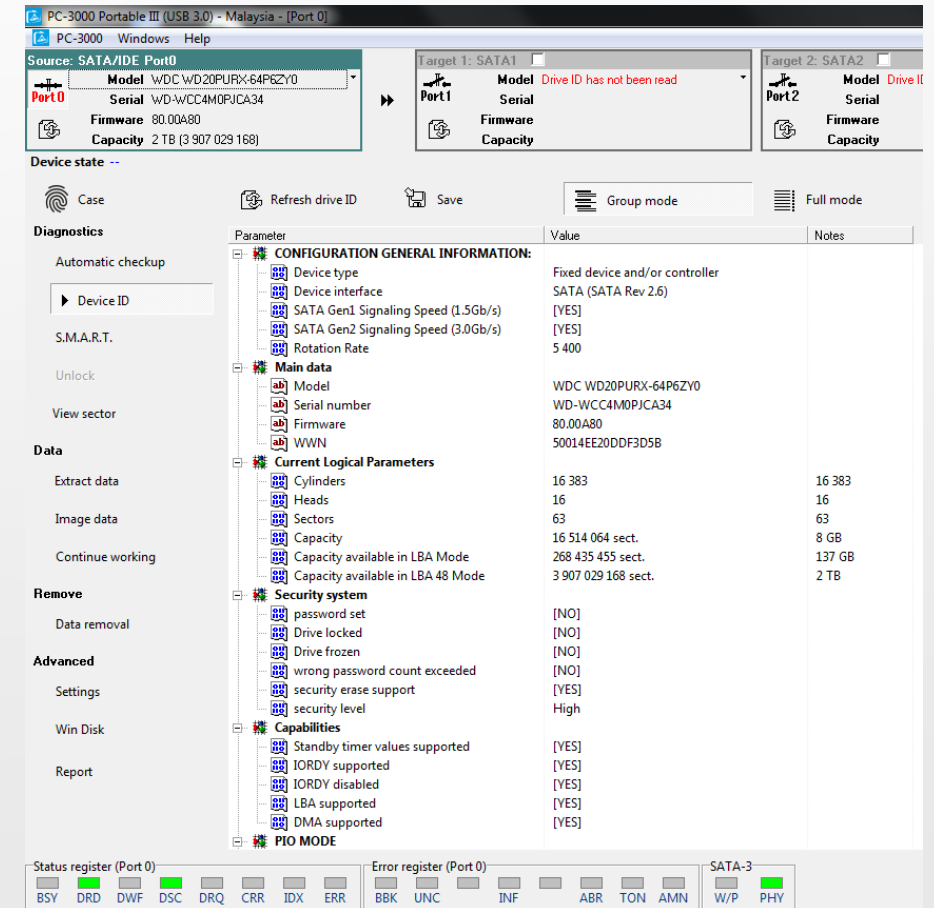
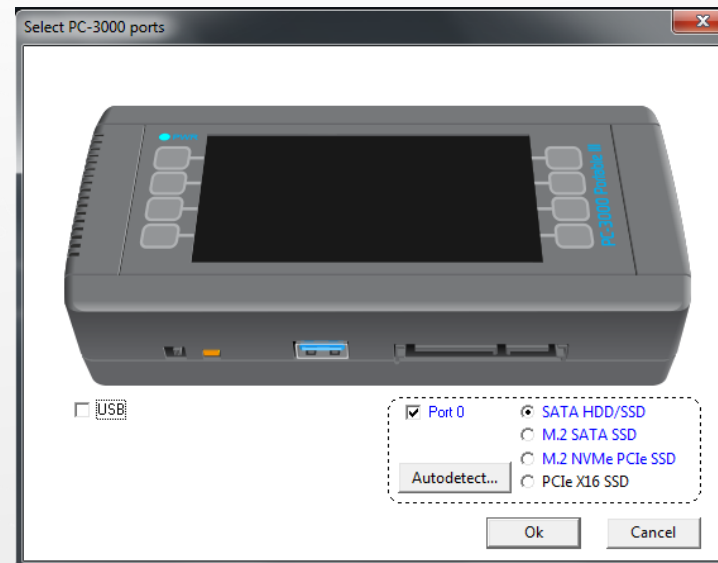
Report UUID: **15984753-e3f8-40b4-af7f-bf39db7c0a4c**  
 Report Date: **2020-07-14 09:59:30 (+0000)**  
 Software Version: **Blancco Drive Eraser 6.13.1**  
 Digital Signature:  
 av0C+S6ltgkQIXYvBhJDLk+5J25mgz7uwnlZUkws2hdXmDDFtgMtApafm5CAI#3Rp8AOF5v4suXR03thlcGuieucTq3IAWtehGs76/E5qaSHUttCyLiDipIIPGemPoJt6ponnA/ITNXJzelbfjMxrfF1sRbifuOXfc1kCQJhW/y3l+qqXYJNX7/AicogAivG+A4VvHXq0YZyCnKR148CQq3q49RP0z4oL6XTVzmDbfmDtrmywZ2Wi8R9uJCQgnaNzeVJ1RF6+xrVjvco7OUGNRqj/UZOx1neFcHLUvxONbUz28Yq182LCD2NBWW0owqQlgyVzRxx8fbF9mw4YOgg==

Gambar 1: Dashboard Blancco Management Console





# CONTOH PENGGUNAAN PC-3000 PORTABLE & DATA EXTRACTOR



Gambar 3: PC-3000 Portable & Data Extractor



# CONTOH PENGGUNAAN MAGNET AXIOM



**PROCESsing DETAILS**

**ADD KEYWORDS TO SEARCH**  
Provide the keywords and regular expressions that you want to include in your search. If a

**EVIDENCE SOURCES**

**SELECT EVIDENCE SOURCE**

COMPUTER MOBILE CLOUD

**ANALYZE EVIDENCE**

**SOURCES TO PROCESS**

Type	Image - location name	Evidence number	Search type	Start time	End time	Duration	Status
	PhysicalDrive0 ST4000DM000-1F2168 (3.64 TB) - Partitic	PhysicalDrive0 ST4000DM000-1	Full	9/3/2020 3:20:40 PM		0:10	Searching - 37%

**SEARCH IN PROGRESS**  
Time Elapsed: 0:19

**CURRENT SEARCH LOCATION**

PhysicalDrive0 ST4000DM000-1F2168 (3.64 TB) - Partition 1 (Microsoft FAT32, 500 MB) ESP Searching - Partition 1 (Microsoft FAT32, 500 MB) ESP

Search Definitions:

- Partition 1 (Microsoft FAT32, 500 MB) ESP
  - Writing Filesystem Information Done
  - All Files and Folders Searching - 47.8% - (0:09)
  - Unallocated Clusters Ready
  - File Slack Space Ready
- Thread Details:

Gambar 4: MAGNET AXIOM



# CONTOH PENGGUNAAN R-STUDIO DATA RECOVERY

R-STUDIO Network Technician 8.13.176095 - Device View

Drive Create Tools View Help

Connect To Remote Refresh Open Drive Files Scan Open Image Create Image Create Region Create Virtual RAID Disconnect Options Stop

Device/Disk	Label	FS	Start
Local Computer			
ST4000DM000-1F2168 CC54	Z307SFZX	#0 RAID (1:0)	0 Bytes
Volume{1bc6cdd1-551e-4b11-adf0-785bc3d3ae6a}	ESP	FAT32	1 MB
Microsoft reserved partition			501 MB
C:	OS	NTFS	629 MB
E:	Storage	NTFS	1.24 TB
Empty Space19			3.63 TB
Volume{4cf31e7a-f69e-4582-9ef3-2fa55b224651}	WINRETOOLS	NTFS	3.63 TB
Volume{05d421f3-1a45-4a0b-904e-1bb331837987}	Image	NTFS	3.63 TB
D:			
Kingston DataTraveler 3.0	00000000000000	#1 USB (0:0)	0 Bytes
Partition1	BADRUL_V	FAT32	31.50 KB

Drive Create Tools View Help

Connect To Remote Refresh Open Drive Files Scan Open Image Create Image Create Region Create Virtual RAID Remove Stop

Device view

Device/Disk	Label	FS	Start	Size
Local Computer				
ST3320418ASCC44	9VMMRZKW	#0 SA...	0 Bytes	298.09 GB
Volume{445abf3b-13ef-...	System Reserved	NTFS	1 MB	100 MB
C:	System	NTFS	101 MB	121.97 GB
D:	Data	NTFS	122.07 GB	176.02 GB
PIONEERDVD-RW DVR-219...				
E:				
WDC WD75DA-00AWA11L07	7D577A141262	#1 USB	0 Bytes	6.99 GB
Empty Space12			512 Bytes	6.99 GB
Recognized1	External_USB	NTFS	1 MB	6.99 GB
Extra Found Files				
Recognized2		NTFS	63 KB	2.93 GB

Recognized partitions

Scan Information

WDC WD75DA-00AWA11L07 - 6.99 GB (7509196800 Bytes, 14666400 Sectors) 14550 Sectors per block

Log

Type	Date	Time	Text
System	10/31/2012	6:58:26 PM	Scanning drive WDC WD75DA-00AWA11L07 started
System	10/31/2012	7:05:10 PM	Scan has been completed for WDC WD75DA-00AWA11L07 in 6m 43s
System	10/31/2012	7:05:10 PM	Scanning drive WDC WD75DA-00AWA11L07 completed

Ready

Gambar 4: R-Studio Data Recovery



# CONTOH PENGGUNAAN WINHEX SPECIALIST



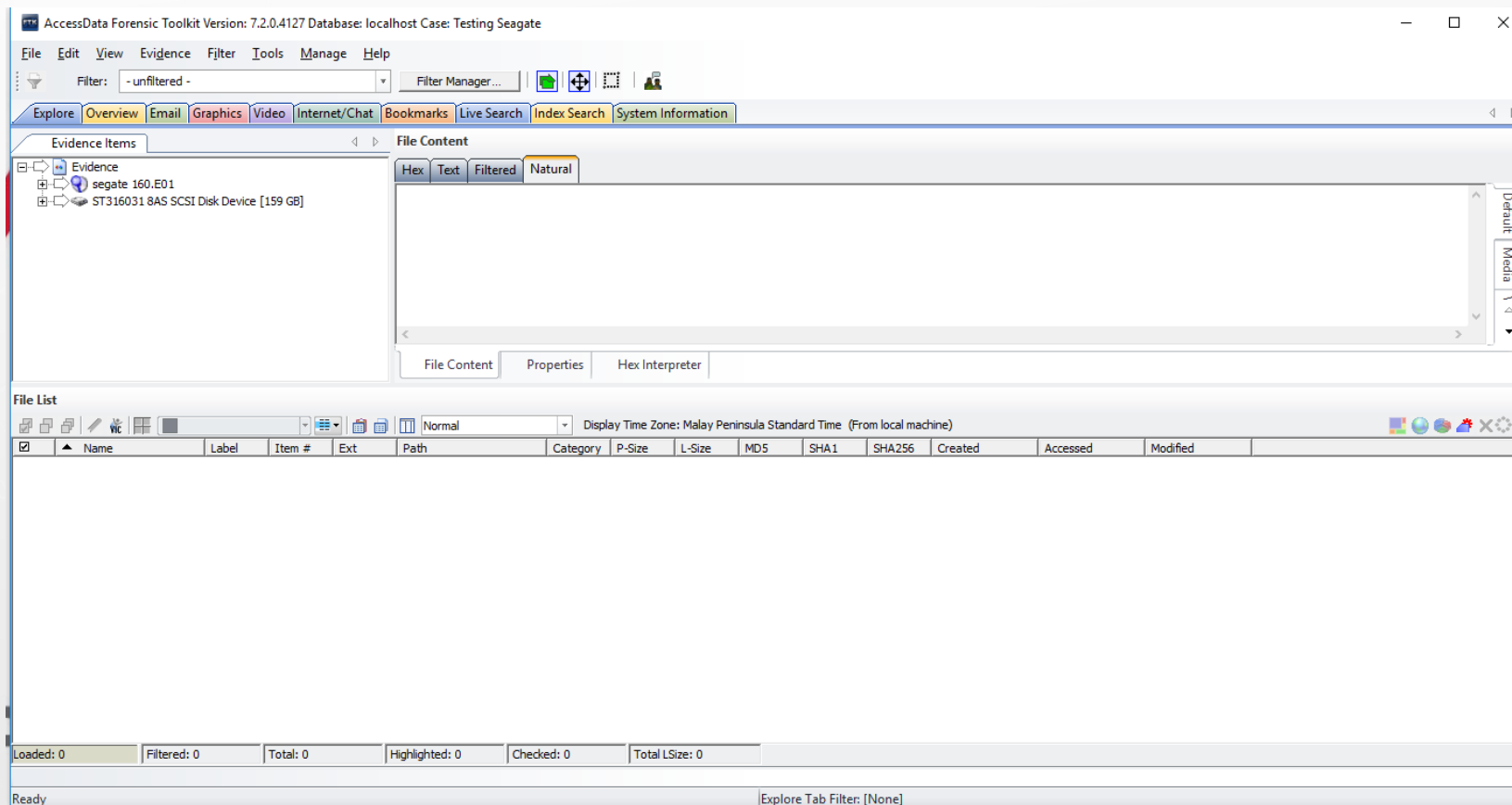
The screenshot displays the Winhex Specialist interface with several key components:

- BYOD License Dialog:** A window titled "BYOD" with the message "Software is unlocked." It displays license information:
  - License ID: 4308C977DD0
  - License file: G:\2020-09-10-04308C977DD0.lic
  - Key device ID: 77A92E45C7036A05B452103F7E
 Below this, it states: "This license file is valid until 2020-09-10. The next license file can be retrieved on 2020-09-09 or later, from the same URL as before, i.e. www.x-ways.com/BYOD/BYOD2.php?code=04308C977DD0B2F07A9648799B0E4B39C5BD"
- Hex Dump:** A large window showing a hex dump of data. The top part contains ASCII characters, including "WHX Backup v1.0 Hard disk 2 \Sectors 0-28979699". The bottom part shows a list of hex values (e.g., 2176, 2240, 2304) and their corresponding byte sequences.
- File Explorer:** A window showing the contents of a removable medium. It lists various files and folders, including:
  - SMET
  - SMFTr
  - Store
  - UpCase
  - Volume
  - 0100-725-01\_rev1\_2019Dec31a\_DittoDX.LI...bin
  - Capture.PNG
  - Capture.PNG
  - Colorbox UFSD Setup 7.34.0.116 Generic...\_cpk
  - ChromeSetup.exe
  - DESKTOP-PGCKG5.html
  - HP Desktop\_and Paperless\_XL\_installer...exe
  - K05720\_VS300X-D32JA-HDARCE.lic
  - Lic.txt
  - licenseactivationrequest.xml
  - LINKS147.zip
  - Log.txt
  - PWB5.BIN
  - Viewer Programs
  - Open
  - Recover/Copy...
  - Export list...
- System Information:** A small window in the bottom right corner shows system details:
  - 8 BR (s): 87
  - 16 BR (s): 18,519
  - 32 BR (s): 542,656,599

Gambar 4: Winhex Specialist



# CONTOH PENGGUNAAN FORENSIC TOOLKIT



Gambar 6: FORENSIC TOOLKIT



# CONTOH PENGGUNAAN XRY OFFICE



The screenshot displays the XRY Office software interface. At the top, there is a navigation bar with a 'HOME' button and a 'CASE OVERVIEW' header. The main area is divided into a left sidebar and a central table. The sidebar contains case details for '2020-07-09\_17.12', including the folder path, creation date, and case ID. The central table lists the selected file with its type, operator, decode status, size, and file status. At the bottom, there is a toolbar with buttons for 'Decode', 'Delete', 'Export', 'Import', 'Extract', and 'Open case'.

<input checked="" type="checkbox"/>	Type	XRY files	Operator	Decode	Size	File status	
<input checked="" type="checkbox"/>		2020-07-09_17.12--1234--Apple iPhone 4 GSM (A1332).xry		9.1	61 KB	Completed	...

Gambar 7: XRY OFFICE



# CONTOH PENGGUNAAN PC-3000 UDMA & DATA EXTRACTOR



The screenshot displays the PC-3000 UDMA-E software interface. On the left, the 'HDD Vendors' list includes Universal Utilities, Western Digital, Maxtor, Fujitsu, Toshiba, Seagate, Hitachi / IBM / HGST, Samsung, and Quantum / Quantum-Maxtor. The 'Utilities' list on the right includes WD Caviar Old Models, Caviar Cyl32, Caviar Cyl32 (SATA), WDC Marvell, and WDC Marvell USB/COM. The main window shows a terminal output for a WDC Marvell USB/COM drive, displaying details such as Model WDC WD06ZFXZ-00G2S01, Serial, Firmware, Capacity 0 MB, and ROM F/W version 00030027. The terminal output includes various diagnostic messages and error reports, such as 'Zone allocation table: HDDs RAM reading error VSC Command sending error: Device Error Detected: \*VSC PERM OVL NOT LOADED. LDR Upload is recommended\*' and 'SA Access check in RAM: Static module reading error VSC Command sending error: Device Error Detected: \*VSC ERR INV FUNC CODE REQ\*'. The interface also shows a 'Log' button and 'Current test progress' indicator.

Gambar 9:PC-3000 UDMA & DATA EXTRACTOR



# WAY FORWARD

1

**Attachment programme di Makmal Forensik SKMM dan CSM  
- berpeluang mengikuti semua proses pengurusan insiden dan forensik**

- ✓ pengumpulan maklumat di lokasi
- ✓ Siasatan di lokasi
- ✓ Analisis dan forensik di Makmal Forensik
- ✓ Penulisan laporan
- ✓ Saksi di Mahkamah

2

**Garis Panduan Pengurusan Insiden dan Forensik Sektor Awam  
(rujukan pekeliling dan polisi sediaada)**





# TERIMA KASIH

[hanom@mampu.gov.my](mailto:hanom@mampu.gov.my)

**Maklumat yang dipaparkan dalam slaid ini adalah hak milik Unit  
Pemodenan Tadbiran  
dan Perancangan Pengurusan Malaysia (MAMPU)  
Jabatan Perdana Menteri  
Sebarang salinan hendaklah mendapat persetujuan dan kelulusan  
MAMPU**