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

BootCamp Keselamatan Maklumat
24 September 2020

AGENDA

1. MENGENAI SME
2. FUNGSI MYDFLAB
3. WAY FOREWARD

SME
PENGURUSAN KESELAMATAN MAKLUMAT

Kemajuan Kerja – Laluan Pakar Bidang Khusus (SME)

Rujukan :(Pekeliling Perkhidmatan Bilangan 1 Tahun 2019)

PERSEDIAAN SME:

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

UPDATE SPK

https://spk.mampu.gov.my

Penempatan

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

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
JUMLAH		**100**

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 IS0/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

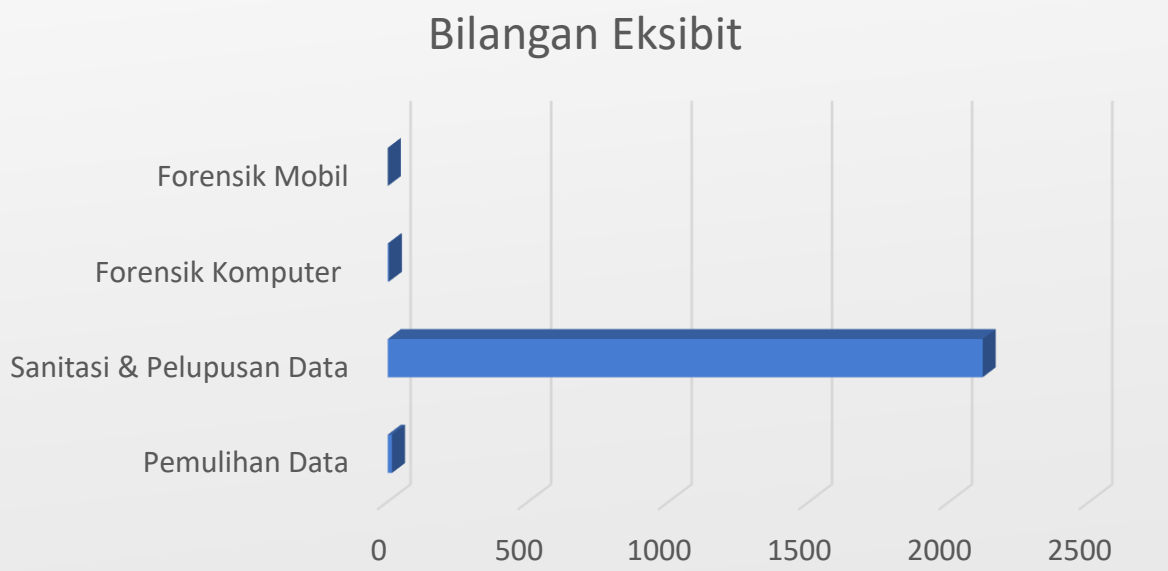
MALAYSIA GOVERNMENT DIGITAL FORENSIC LAB (MYDFLAB)

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

1	2	3	4
			
Forensik Komputer	**Forensik Mudah Alih**	**Sanitasi& Pelupusan Data**	**Pemulihan Data**
FTK	XRY	BLANCCO	ATOLA INSIGHT
AXIOM		SUPER-DUPER	R-STUDIO
		VOOM-3P	PC-3000
		ATOLA RECYCLER	

Status Pelaksanaan Sehingga Ogos 2020:

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



	Pemulihan Data	Sanitasi & Pelupusan Data	Forensik Komputer	Forensik Mobil
Bilangan Eksibit	15	2119	4	0

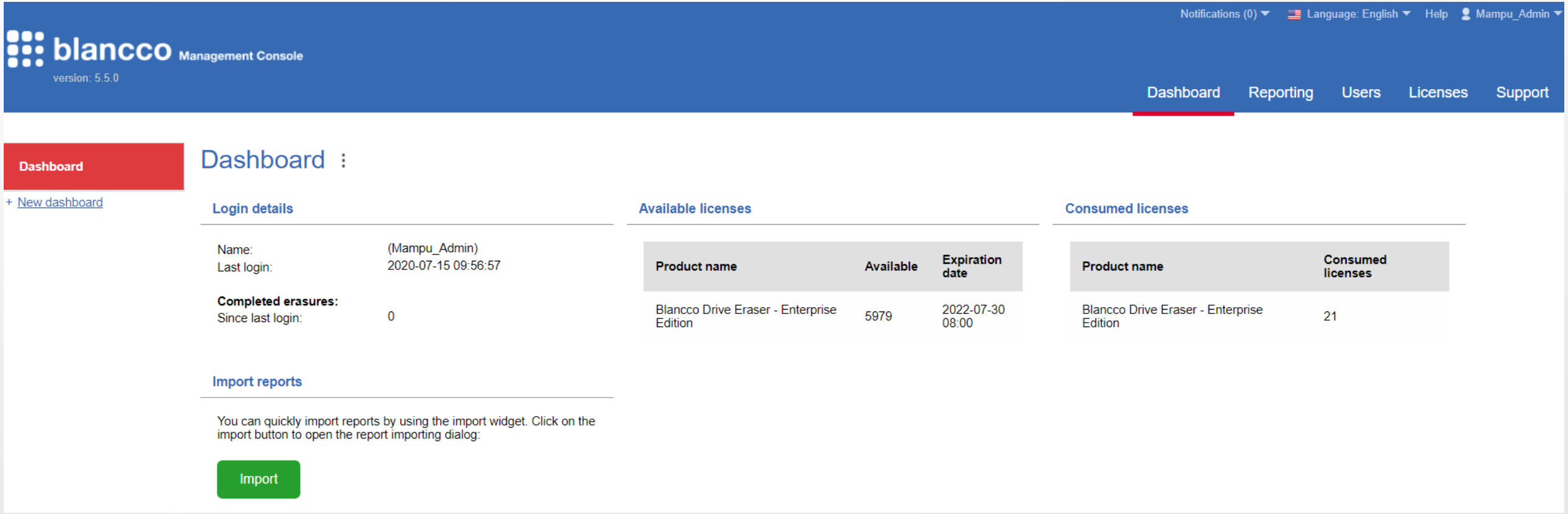
LATAR BELAKANG PROJEK

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



Gambar 1: Dashboard Blancco Management Console

CONTOH PENGGUNAAN

BLANCCO DRIVE ERASER – ENTERPRISE EDITION

Data Erasure Report

blancco

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

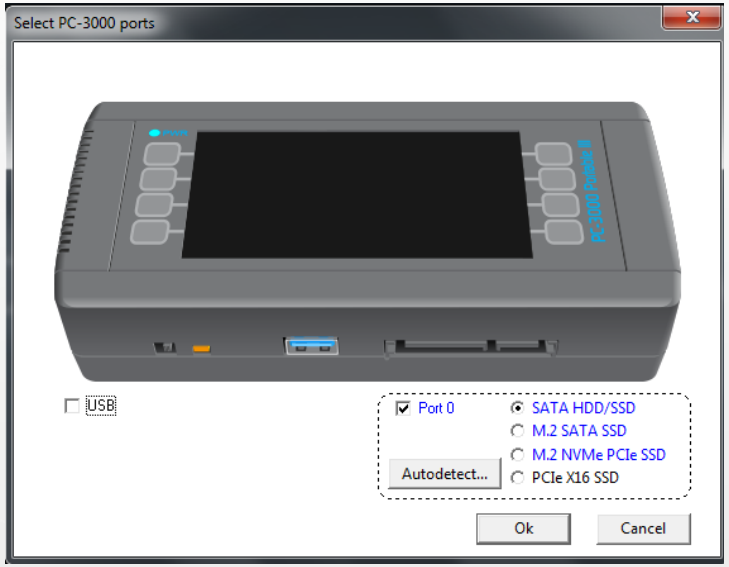
Digital Signature:

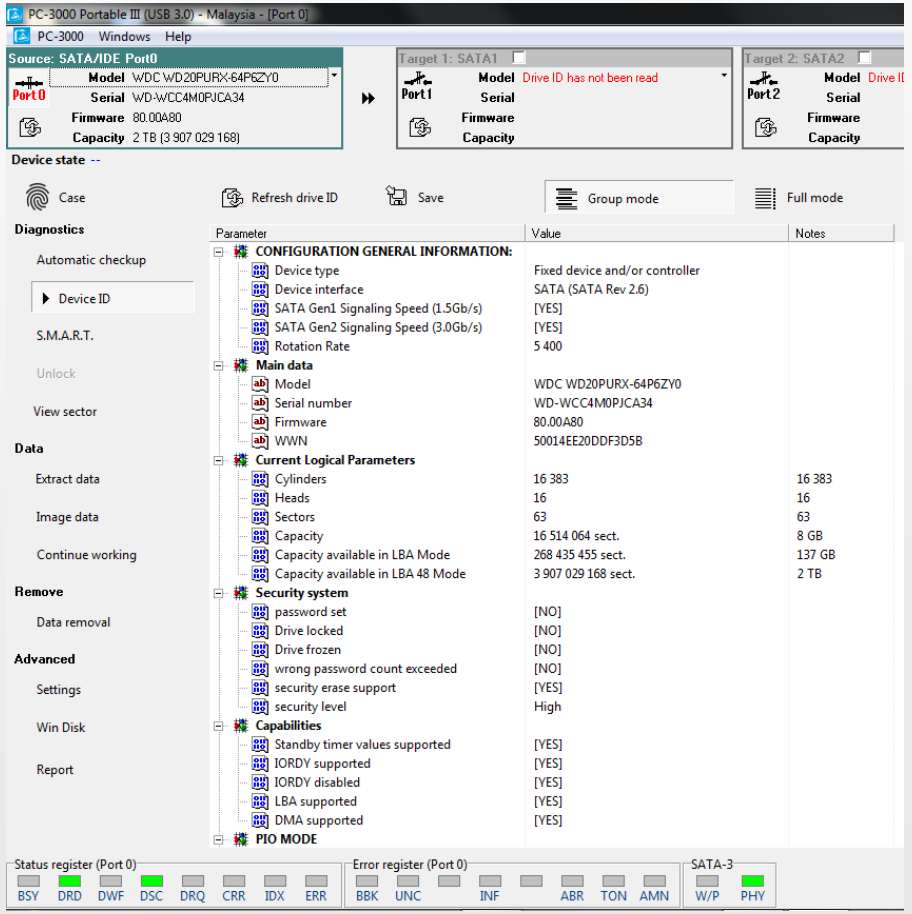
av0C+S6ItgkQIXYvBhJDLk+5J25mgz7uwnIZUkws2hdXmDDFtgMtApafm5CAtl3Rp8AOF5v4suXR03thlcGuieucTq3IAWtehGs76/iE5qaSHUttCyLtDipIIPGemPoJt6ponnA/ITNXJzelbfjMrxrF1sRbIfuOXfc1kCQJhW/y3i
+qqXYJNX7/AicogAlvG+A4VvHXq0YZyCnKR148CQq3q49RP0z4oL6XTVzmDbfmDtmywZ2WI8R9uJCQgnaNzeVJ1RFe+xrVjvco7OUGNRqj/UZOx1neFcHLUvxONbUz28Yq182LCD2NBWW0owqQfgayVzRxw8fbF9rnw4YQgg==

Gambar 1: Dashboard Blancco Management Console

CONTOH PENGGUNAAN

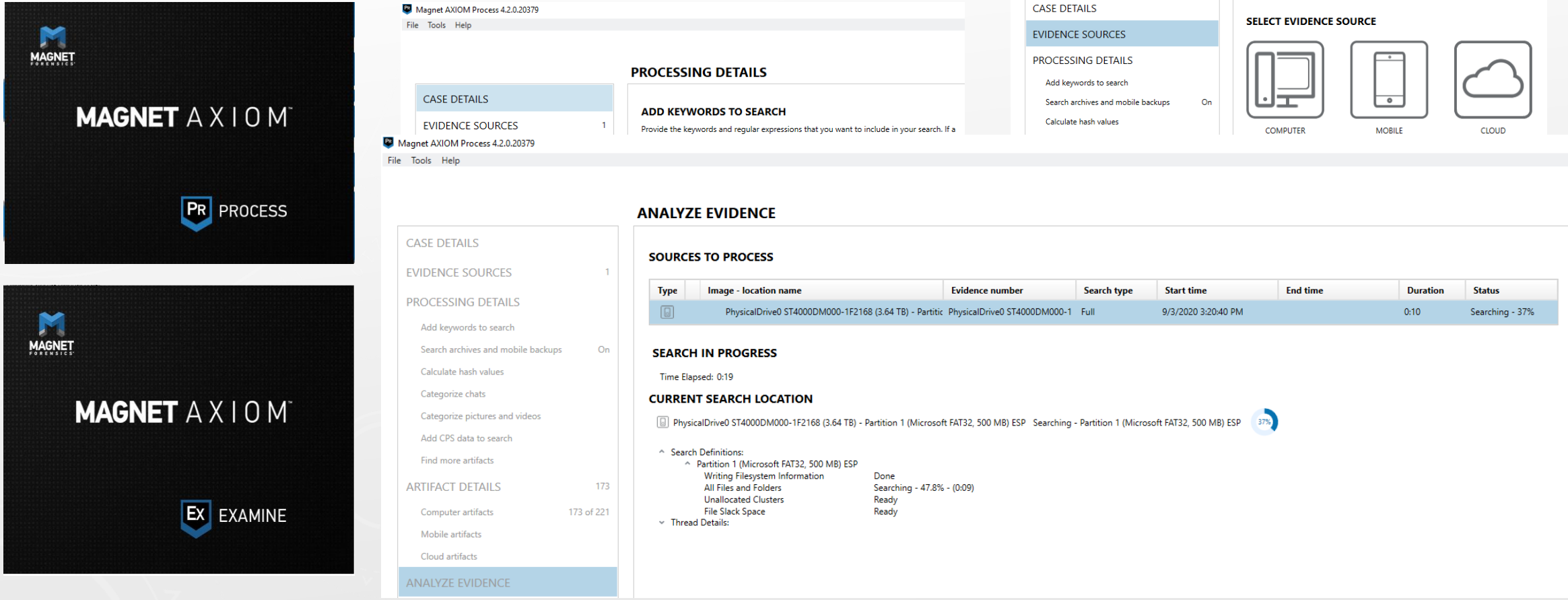
PC-3000 PORTABLE & DATA EXTRACTOR





Gambar 3: PC-3000 Portable & Data Extractor

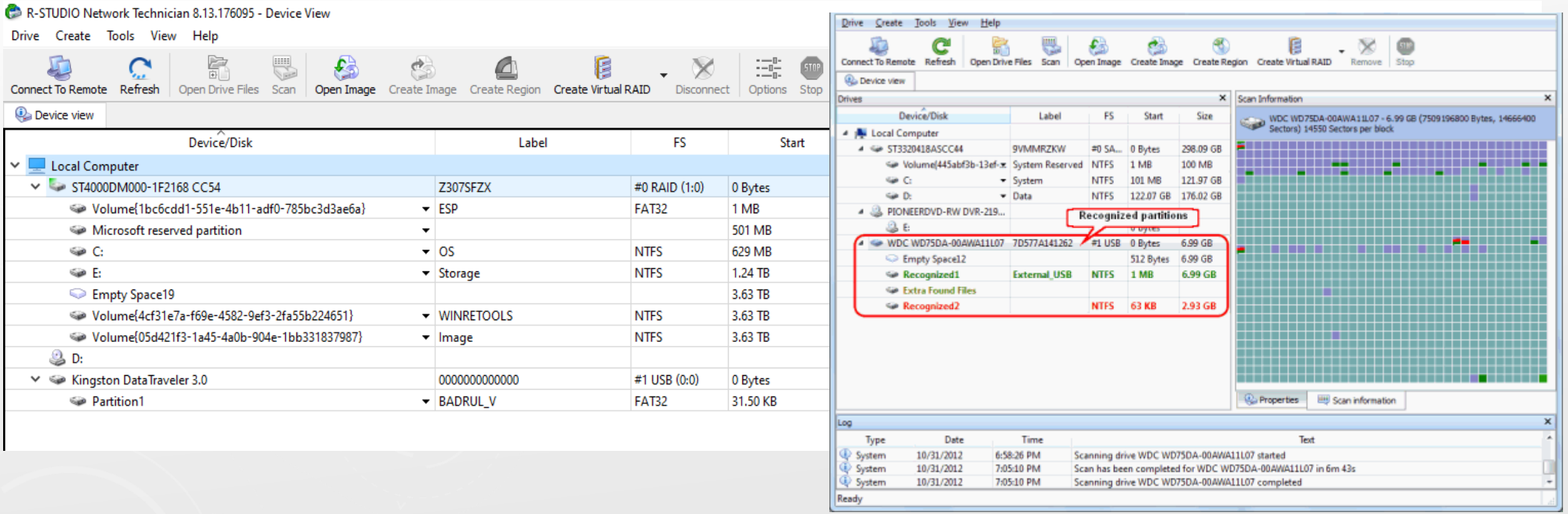
CONTOH PENGGUNAAN
MAGNET AXIOM



Gambar 4: MAGNET AXIOM

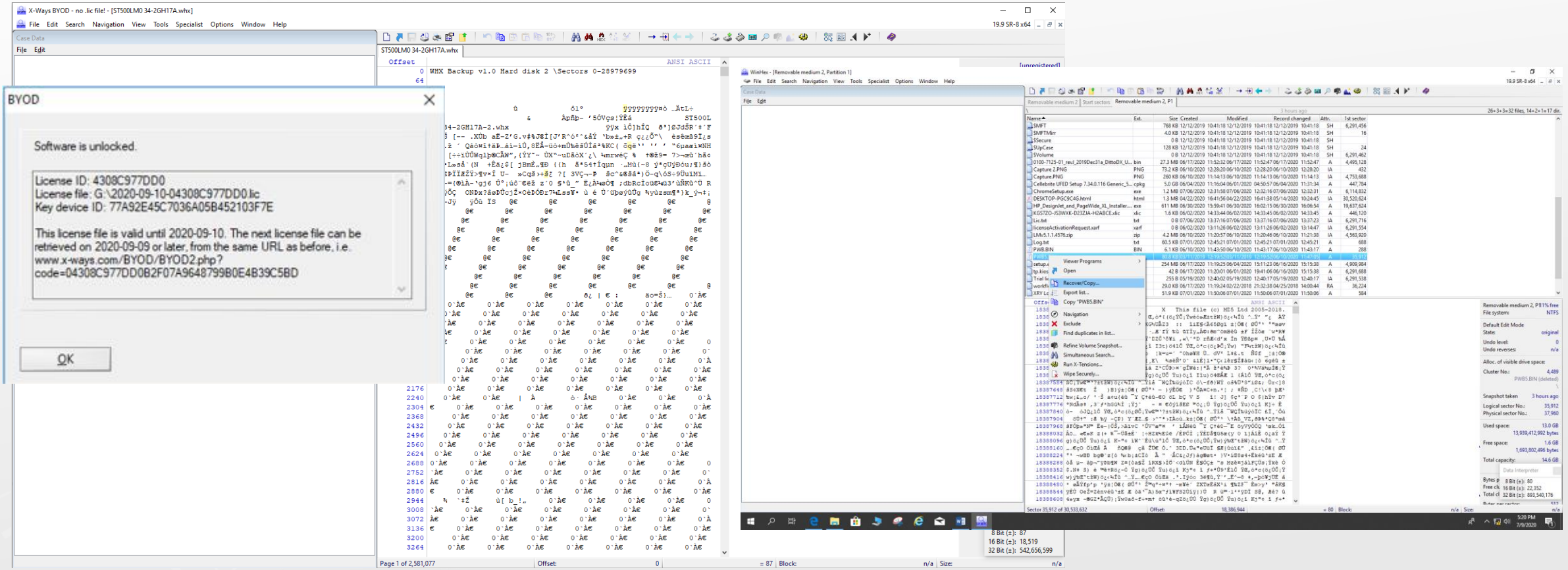
CONTOH PENGGUNAAN

R-STUDIO DATA RECOVERY



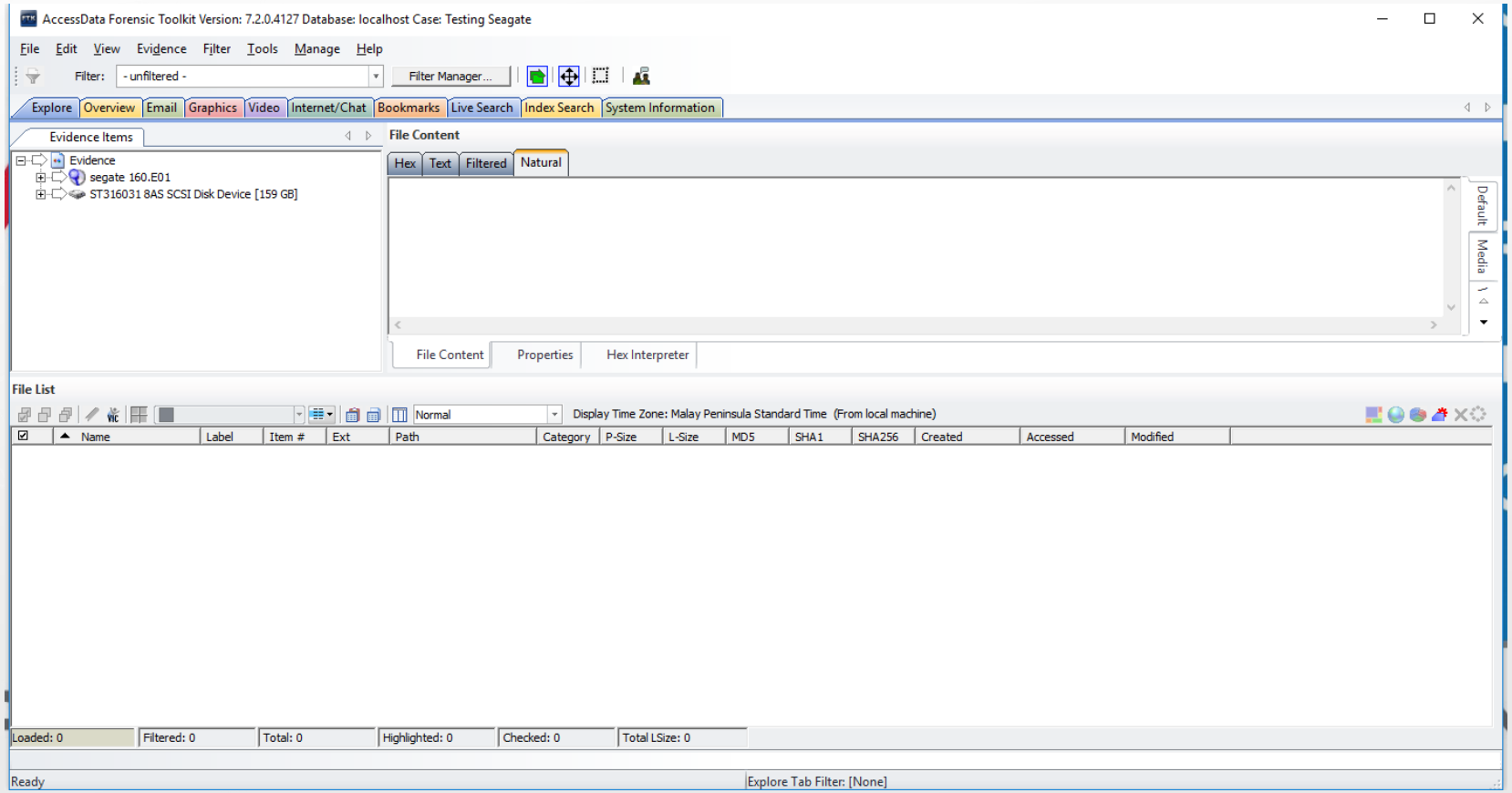
Gambar 4: R-Studio Data Recovery

CONTOH PENGGUNAAN WINHEX SPECIALIST



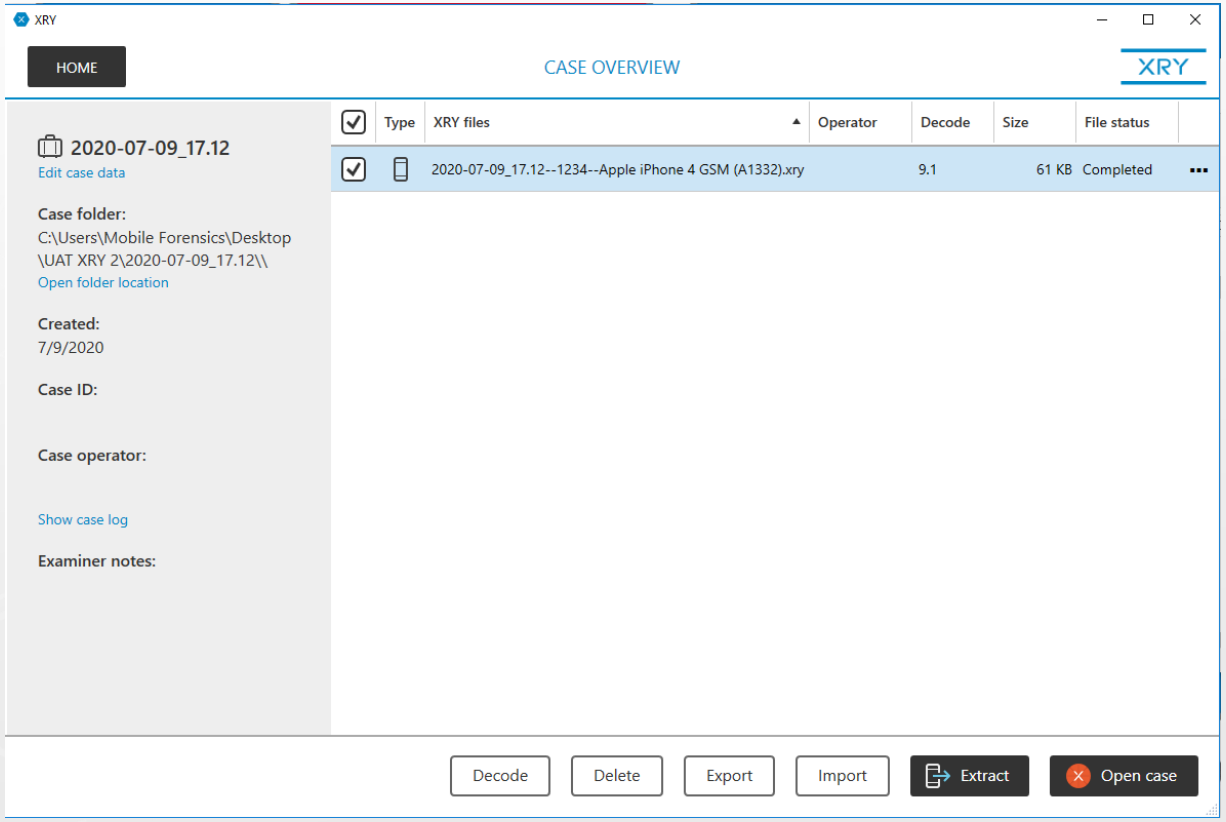
Gambar 4: Winhex Specialist

CONTOH PENGGUNAAN
FORENSIC TOOLKIT



Gambar 6: FORENSIC TOOLKIT

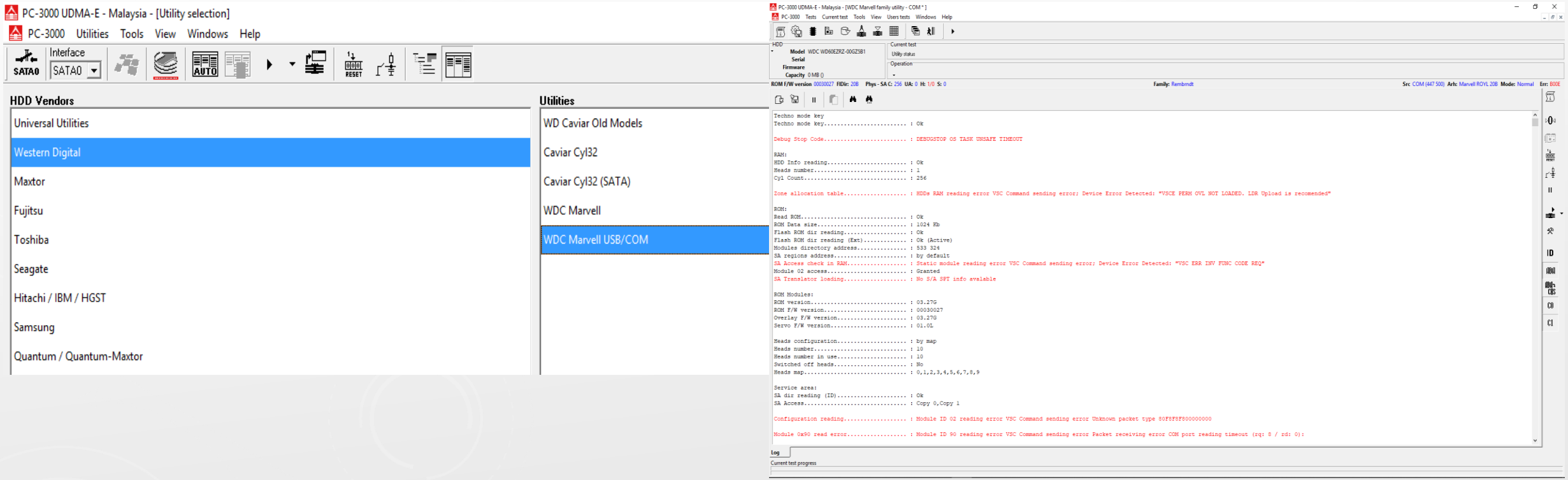
CONTOH PENGGUNAAN
XRY OFFICE



Gambar 7: XRY OFFICE

CONTOH PENGGUNAAN

PC-3000 UDMA & DATA EXTRACTOR



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