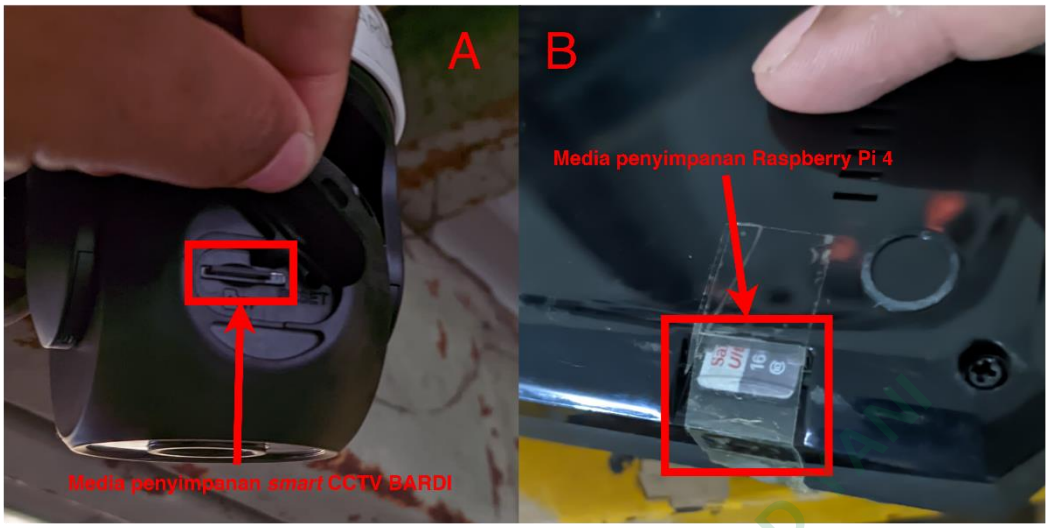
BAB 4
HASIL PENELITIAN

4.1 Pembahasan

4.1.1 Identifikasi

Sebelum melakukan proses identifikasi, peneliti menyusun dan menyerahkan surat izin penelitian dengan nomor surat B/024/TEKNO-FTTI-UNJAYA/II/2025 yang terlampir pada Lampiran 1, sebagai bentuk legalitas administratif yang menggantikan surat perintah penggeledahan. Tahap identifikasi merupakan tahapan awal dalam penelitian ini yang bertujuan untuk menentukan sumber barang bukti dan jenis media penyimpanan yang digunakan pada setiap barang bukti elektronik. Sebelum menentukan metode akuisisi di tahap selanjutnya. Dalam penelitian ini terdapat 3 perangkat yang teridentifikasi menjadi barang bukti yaitu BARDI *smart* IP *Camera Outdoor*, Raspberry Pi 4, dan *Smartphone* Xiaomi 5s Plus (*rooted),* seperti pada Gambar 3.4 bagian (C), (D) dan (E).

Proses identifikasi dilanjutkan dengan pemeriksaan fisik perangkat untuk memastikan setiap perangkat memiliki media penyimpanan eksternal atau tidak. Setelah dilakukan pemeriksaan fisik terhadap barang bukti elektronik, ditemukan sebuah SD *card* dengan kapasitas 126 GB dalam BARDI *Smart* IP *Camera Outdoor* PTZ sebagai media penyimpanan lokal yang memungkinkan SD *card* ini mengandung data rekaman video dalam format tertentu, SD *card* ini menjadi satu-satunya sumber data dari BARDI *smart* IP *Camera Outdoor* PTZ ini. Kemudian ada Raspberry Pi 4 yang terpasang *Home Assistant* digunakan sebagai pengendalian perangkat dan terhubung secara lokal. Pemeriksaan secara fisik juga dilakukan dan ditemukan sebuah SD *card* dengan kapasitas 16 GB yang digunakan sebagai *booting* dan penyimpanan *log* sistem *Home Assistant* yang memungkinkan menyimpan informasi seperti jejak digital aktivitas *streaming*, deteksi perangkat, hingga *metadata* koneksi ke *cloud*. Gambar 4.1 A menunjukan bahwa terdapat media penyimpanan dalam BARDI *Smart* IP *Camera Outdoor* PTZ dan B media penyimpanan Raspberry Pi 4.



Gambar 4.1 Media Penyimpanan Barang Bukti Elektronik

Barang bukti elektronik selanjutnya berupa *smartphone* Xiaomi 5s Plus pada Gambar 3.4 (E) yang terpasang aplikasi Tuya App dengan kondisi *smartphone* sudah *rooted,* agar memudahkan dalam melakukan pengambilan informasi. Hasil identifikasi pada *smartphone* Xiaomi 5s Plus berupa spesifikasi dari perangkat tersebut seperti pada Tabel 4.1.

Tabel 4.1 Spesifikasi *Smartphone* Xiaomi 5s Plus

Spesifikasi *smartphone* Xiaomi 5s Plus	
Device name	Mi Phone
Model number	Mi 5s Plus
Android Version	8.0.0
MIUI Version	MIUI Global 10.2
CPU	Quad-Core Max 2.35GHz
RAM	4.00 GB
Penyimpanan internal	64.00 GB
Penyimpanan eksternal	Tidak ditemukan
Karnel version	3.18.71 -perf-gd30d7f9
IMEI1	863818037511202
IMEI2	863818037511210

4.1.2 Pengumpulan

Pada tahap pengumpulan ini penulis mengumpulkan media penyimpanan yang sudah teridentifikasi pada tahap sebelumnya, seperti pada barang bukti BARDI *Smart* IP *Camera Outdoor* PTZ dan Raspberry Pi 4. Penulis mengamankan barang bukti elektronik fisik SD *card* berkapasitas 126 GB dan 16 GB pada tanggal 25 April 2025 untuk dilakukan akuisisi di laboratorium forensik. Proses ini dilakukan dengan sangat hati-hati agar tidak terjadi perubahan dan menghindari kerusakan pada media penyimpanan tersebut. Proses pengumpulan ini dilakukan dalam lingkungan yang terkendali dengan mematikan aliran listrik terlebih dahulu kemudian melepas media penyimpanannya. Setelah didapatkan SD *card* ini diidentifikasi kembali dan ditemukan kode pada media penyimpanan seperti pada Gambar 3.4 (A) merupakan kode dari SD *card* BARDI *Smart* IP *Camera Outdoor* PTZ sedangkan Gambar 3.4 (B) merupakan kode dari SD *card* Raspberry Pi 4. Lebih spesifiknya pada Tabel 4.2. Kedua SD *card* ini kemudian disimpan dalam sebuah kotak untuk selanjutnya dilakukan akuisisi.

Tabel 4.2 Kode SD *Card* Media Penyimpanan

No	Barang Bukti	Kode
1.	SD *Card* V-Gen 126 GB	A1 A1957748
2.	SD *Card* Sandisk 16 GB	9443DRDTE068

Berbeda dengan BARDI *smart* IP *Camera Outdoor* dan Raspberry Pi 4 yang memiliki media penyimpanan fisik berupa SD *card*, sehingga penulis hanya mengamankan media penyimpanannya saja. Di sini penulis mengamankan fisik *Smartphone* Xiaomi 5s Plus dikarenakan tidak memiliki media penyimpanan eksternal dan hanya mempunyai media penyimpanan internal. Selain itu *Smartphone* Xiaomi 5s Plus ini sudah dalam keadaan *rooted* maka memungkinkan untuk dilakukan akuisisi secara *logical* dengan cara mengakses secara langsung ke direktori Tuya App menggunakan ADB shell.

4.1.3 Akuisisi

Setelah proses pengumpulan dilakukan, tahap berikutnya melakukan akuisisi pada media penyimpanan dari masing-masing barang bukti elektronik yang telah didapatkan pada proses pengumpulan. Proses ini dilakukan pada tanggal 25-26 April 2025, proses akuisisi ini merupakan proses *imaging* dan ekstraksi dari barang bukti elektronik yang telah didapatkan dan disesuaikan berdasarkan jenis perangkat dan media penyimpannya. Proses akuisisi ini dilakukan sesuai dengan standar ACPO dan SNI ISO/IEC 27037:2014. Dalam penelitian ini penulis melakukan 2 metode akuisisi di antaranya, *physical* untuk SD *card* dari BARDI *smart* IP *Camera Outdoor* PTZ dan Raspberry Pi 4, serta *logical* untuk data aplikasi Tuya App pada *smartphone* Xiaomi 5s Plus. Ringkasan akuisisi barang bukti elektronik pada Tabel 4.3.

Tabel 4.3 Ringkasan Akuisisi Barang Bukti Elektronik

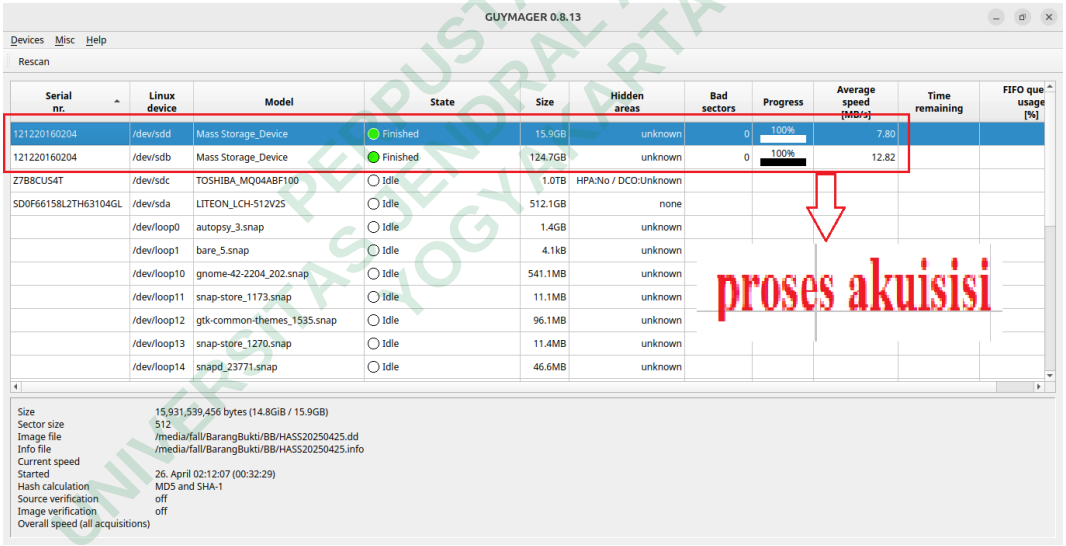
No	Barang Bukti Elektronik	Jenis Akuisisi	Tools	Hasil Output
1	SD *card* V-Gen 126 GB	*Physical*	Guymager	*Image*.dd
2	SD *card* Sandisk 16 GB	*Physical*	Guymager	*Image*.dd
3	*Smartphone* Xiaomi 5s Plus	*Logical*	Adb shell + Pull	Folder *databases*

4.1.4 Akuisisi *Pyhsical*

Metode ini merupakan proses penyalinan seluruh isi media penyimpanan dalam bentuk bit per bit tanpa memperhatikan sistem *file*, partisi, atau struktur datanya. Metode ini digunakan untuk melakukan pemulihan *file* yang telah terhapus, data tersembunyi, ruang *unallocated*, dan artefak yang tidak terlihat dalam sistem *file* biasa.

Dalam penelitian ini penulis melakukan akuisisi pada barang bukti elektronik berupa media penyimpanan eksternal SD *card* dari BARDI *smart* IP *Camera Outdoor* PTZ dan Raspberry Pi 4. Metode ini dipilih karena memberikan salinan data utuh termasuk artefak yang tidak terlihat dalam sistem, menghindari akses langsung yang dapat memodifikasi *metadata*, dan memberikan fleksibilitas dalam proses analisis. SD *card* tidak diakses secara langsung dalam di sistem operasi

Windows biasa, dalam melakukan proses akuisisi penulis menggunakan sistem operasi Linux Ubuntu 22.04 serta menggunakan *tools imaging* Guymager, karena mendukung akuisisi berbasis sektor, verifikasi hash *real-time*, dan fitur *write blocking* secara virtual. Langkah yang dilakukan proses akuisisi ini dengan cara memasangkan salah satu SD *card* ke USB *card reader* dan dihubungkan ke laptop. Kemudian jalankan Guymager, dalam penelitian ini penulis menyimpan hasil akuisisi pada sebuah *hard disk* berkapasitas 1 TB yang terbagi menjadi 4 patrisi dan masing-masing partisi mempunyai kapasitas 250 GB. Penulis memberi nama hasil akuisisi dengan format jenis barang bukti, tahun, bulan, dan tanggal yang disesuaikan pada saat melakukan akuisisi seperti, CCTV20250425 dan HASS20250425, aktifkan penghitungan hash MD5 dan SHA1 dan start *imaging*, tunggu hingga proses selesai seperti pada Gambar 4.2. Hasil akuisisi tersimpan dalam format .dd.



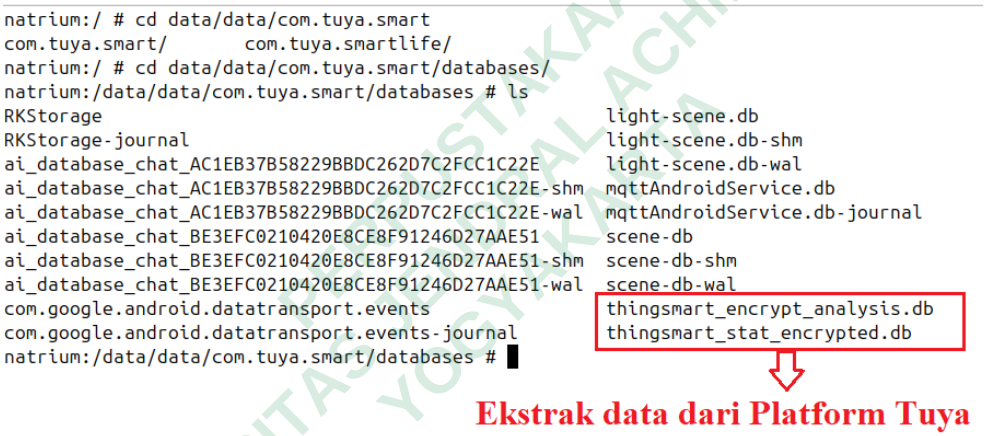
Gambar 4.2 Proses Akuisisi Media Penyimpanan Barang Bukti Elektronik.

4.1.5 Akuisisi *Logical*

Akuisisi *logical* dilakukan pada *smartphone* Xiaomi 5s Plus yang sudah dalam keadaan *rooted*, digunakan untuk menjalankan aplikasi Tuya App sebagai sistem pengendali *smart home*. Akuisisi *logical* ini merupakan proses penyalinan data yang tebaca dan dapat diakses, umumnya *file* konfigurasi, *database*, *log* aktivitas, dan arsip aplikasi. Metode *logical* ini dipilih karena *smartphone* Xiaomi

sudah dalam keadaan *rooted* sehingga memungkinkan untuk mendapatkan akses penuh ke direktori Tuya App.

Proses akuisisi ini dilakukan dengan mengaktifkan mode USB *debugging* pada perangkat dan menghubungkannya menggunakan kabel USB, untuk memastikan perangkat dikenali dengan perintah `adb devices` lalu jalankan perintah `adb devices, adb shell, su` kemudian masuk dalam direktori Tuya App yang terletak di /data/data/com.tuya.*smart*/databases/ dengan perintah `cd /data/data/com.tuya.smart/databases/` setelah masuk ke dalam direktori tersebut akan terdapat beberapa *file* konfigurasi, *databases* SQLite, dengan ekstensi .db. penulis mengambil beberapa *file* yang berkas dengan ekstensi .db seperti pada Gambar 4.3.



Gambar 4.3 *File* yang di Ekstrak dari Aplikasi Tuya App.

Untuk menyalin data kedalam laptop gunakan perintah `cp -r /data/data/com.tuya.smart/databases /sdcard/databases_tuya` setelah itu `exit` untuk keluar dalam sesi adb shell, kemudian gunakan perintah `adb /sdcard/databases_tuya ~/Downloads/` untuk menyalin *file* tersebut ke folder *Downloads* dalam laptop.

4.1.6 Preservasi

Proses ini merupakan bagian penting dalam melakukan investigasi forensik digital, tujuannya untuk menjaga integritas, keaslian, dan keutuhan barang bukti digital pada saat melakukan akuisisi hingga analisis selesai dilakukan, serta

memastikan hasil akuisisi tidak mengalami perubahan dan sah saat digunakan dalam proses pembuktian hukum. Dalam penelitian ini preservasi dilakukan pada tiga jenis barang bukti digital hasil *physical imaging* dari media penyimpanan BARDI *smart* IP *Camera Outdoor* PTZ dan Raspberry Pi 4, serta *logical* akuisisi dari direktori aplikasi Tuya App.

Setiap *file* hasil akuisisi disimpan dalam sebuah *hardisk* yang berkapasitas 250 GB dan mendapatkan nilai hash MD5 dan SHA1 yang didapatkan setelah proses *imaging* selesai dan hasil ekstraksi pada direktori /data/data/com.tuya.*smart*/databases/ di aplikasi Tuya yang terpasang pada *smartphone* Xiaomi 5s Plus pun memiliki nilai hash. Nilai hash ini digunakan untuk mengverifikasi keaslian suatu *file*, jika terjadi perubahan nilai hash maka analisis dihentikan karena terjadi perubahan yang tidak sah pada saat melakukan analisis. Langkah awal dilakukan dengan menghitung nilai hash menggunakan nilai MD5 dan SHA1 seperti pada Tabel 4.4 yang memuat jenis *file*, format *file*, dan nilai hash setiap barang bukti digital yang didapatkan dari hasil akuisisi.

Tabel 4.4 Nilai Hash MD5 dan SHA1

Barang Bukti Digital	**Format *File***	**Hash MD5**	**Hash SHA1**
CCTV20250425.dd	.dd	6ba6c3e66703168a9198b7dff68b4e8d	a819cdd19fff1f5507d8e07210144648803b5402
HASS20250425.dd	.dd	d7bf2413734fab140c40333526f78b3f	050eb49a18ddc4783182d5a11834110bc861b051
thing*smart*_encrypt_analysis.db	.db	dd6d0316a508ff459ddf77bd70ac5cf4	1216dba2c3de8cbbec0c80d30d1d40b5aa7958a6
thing*smart*_stat_encrypted.db	.db	eed5d95470795ede094c1e8d5378b3c6	bc053ae95818caff073618a525b409bd32016192

4.1.7 Analisis

Proses analisis dilakukan ke barang bukti digital yang sudah didapatkan melalui proses akuisisi dengan tujuan untuk menemukan artefak digital yang relevan, baik berupa *file* yang sudah dihapus, konfigurasi sistem, atau *log* aktifitas. Proses ini menggunakan perangkat lunak forensik yang *open source* seperti Autopsy, FTK *Imager*, DMDE, Foremost, Photorec, Scalpel dan SQlite Viewer.

Dalam analisis ini diharapkan dapat menemukan barang bukti digital seperti gambar atau video yang dapat digunakan dalam persidangan nantinya.

a. Bardi *Smart* IP Camera Outdoor PTZ

Analisis hasil akuisisi SD *card* dari BARDI *smart* IP *Camera Outdoor* PTZ ini dilakukan dengan beberapa perangkat lunak forensik untuk mengidentifikasi artefak digital seperti rekaman video, gambar, atau *log* perangkat. Berdasarkan hasil analisis, ditemukan sturktur direktori dan *file*, Namun sebagian besar *file* .media atau .jpg yang ditemukan tidak dapat dibuka yang memungkinkan *file* tersebut mengalami kerusakan atau terenkripsi.

1. Autopsy

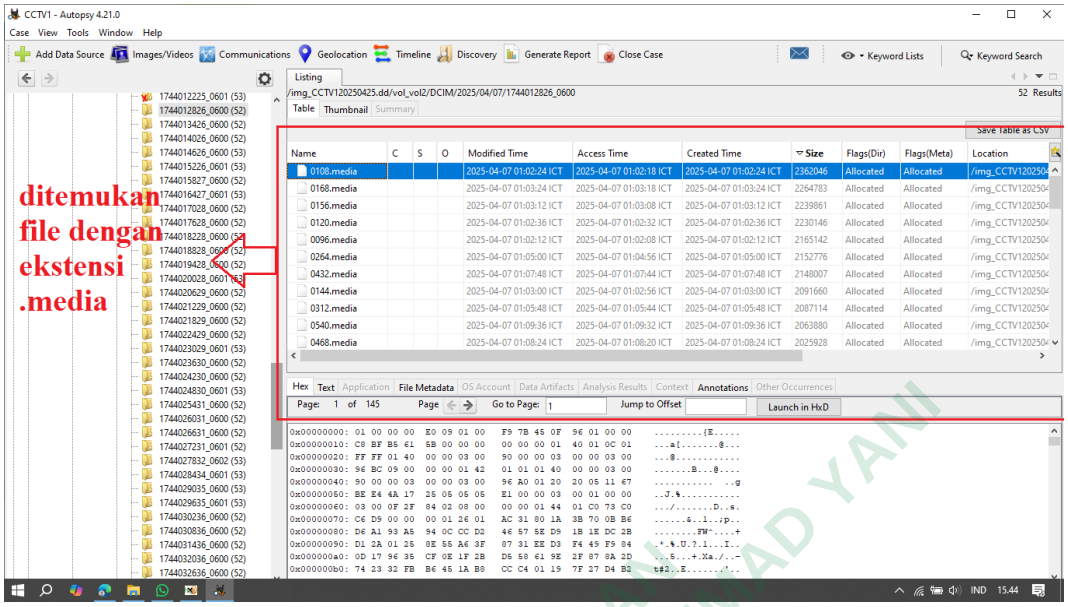
Analisis awal CCTV20250425.dd yang merupakan barang bukti digital hasil dari media penyimpanan BARDI *smart* IP *Camera Outdoor* PTZ menggunakan perangkat lunak Autopsy dengan versi 4.21.0. Hasil analisis dari barang bukti digital tersebut ditemukan beberapa artfak digital seperti /vol/ yang merupakan partisi utama dengan sistem *file* NTFS/exFAT, serta /.tuya.sd.test/ yang diduga merupakan bagian dari sistem konfigurasi atau pengujian dari aplikasi Tuya, ditemukan juga direktori /DCIM/ yang diduga sebagai penyimpanan foto atau video, lebih lengkapnya pada Tabel 4.5

Tabel 4.5 Artefak CCTV20250425.dd yang ditemukan Autopsy

No	Artefak	Keterangan
1	/vol/	Partisi utama dengan *file*system NTFS/exFAT
2	/.tuya.sd.test/	Kemungkinan berisi konfigurasi pengujian SD Card dari sistem Tuya
3	/DCIM/	Berisi folder penyimpanan BARDI *smart* CCTV berdasarkan tahun.
4	/DCIM/2025/	Berisi folder penyimpanan BARDI *smart* CCTV berdasarkan bulan.

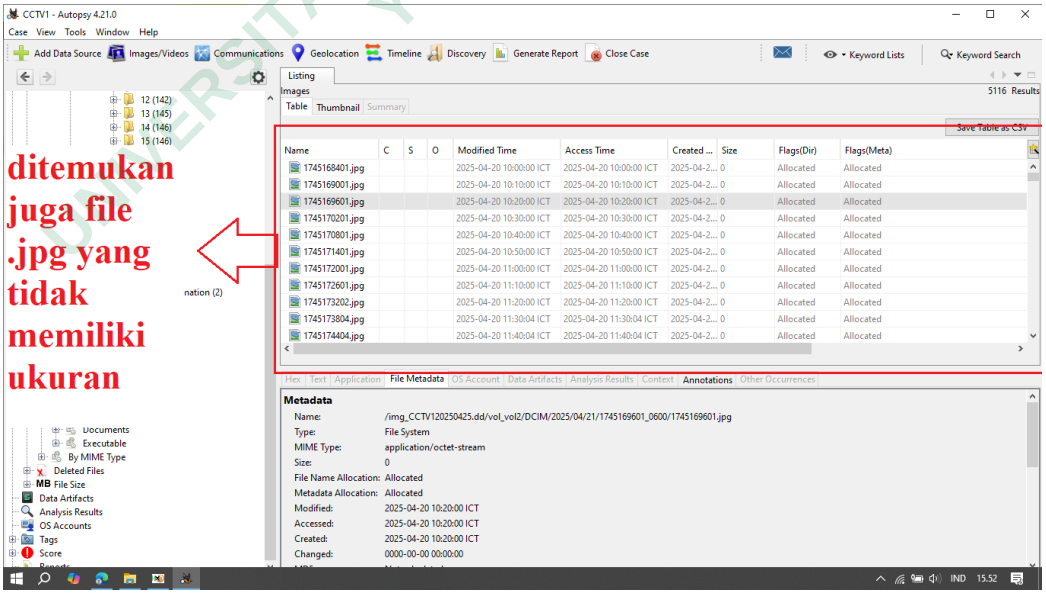
No	Artefak	Keterangan
5	/DCIM/2025/04/	Berisi folder penyimpanan BARDI *smart* CCTV berdasarkan tanggal.
6	/DCIM/2025/04/07/	Berisi folder penyimpanan BARDI *smart* CCTV berdasarkan jam dengan interfal 1 jam
7	/DCIM/2025/04/07/1744012826_0600/	Berisi *file* yang menyimpan hasil rekaman dari BARDI *smart* CCTV berupa .media dan tersimpan setiap 10 menit.
8	/DCIM/2025/04/21/1745169601_0600/	Ditemukan *file* dengan ekstensi .jpg, namun tidak memiliki ukuran dan tidak dapat dibuka.
9	*File* .media	Tanpa ekstensi umum seperti mov, mp4, dan jpg serta tidak dapat diputar.

Pada direktori /DCIM/2025/04/07/1744012826_0600 ditemukan *file* dengan ekstensi .media, *file* yang ditemukan tersebut mempunyai berbagai macam ukuran mulai dari 1075696 *byte* hingga 2362046 *byte*. Namun *file-file* dalam folder tersebut tidak memiliki ekstensi yang utuh seperti pada umumnya seperti .mp4, .jpg, .mov, atau *file-file* yang menunjukkan ekstensi gambar dan video. seperti pada Gambar 4.4.



Gambar 4.4 *File* Ekstensi .media.

File .media tersebut diekstrak dan diputar menggunakan media *player*, VLC dan beberapa pemutar video yang lain, hasilnya *file* .media tersebut tidak dapat diputar dengan keterangan *file* rusak. kemudian ditemukan juga beberapa *file* .jpg dalam direktori /DCIM/2025/04/21/1745169601_0600/ namun ukuran *file* .jpg tersebut tidak wajar, karena tidak memiliki ukuran *file* seperti pada Gambar 4.5.

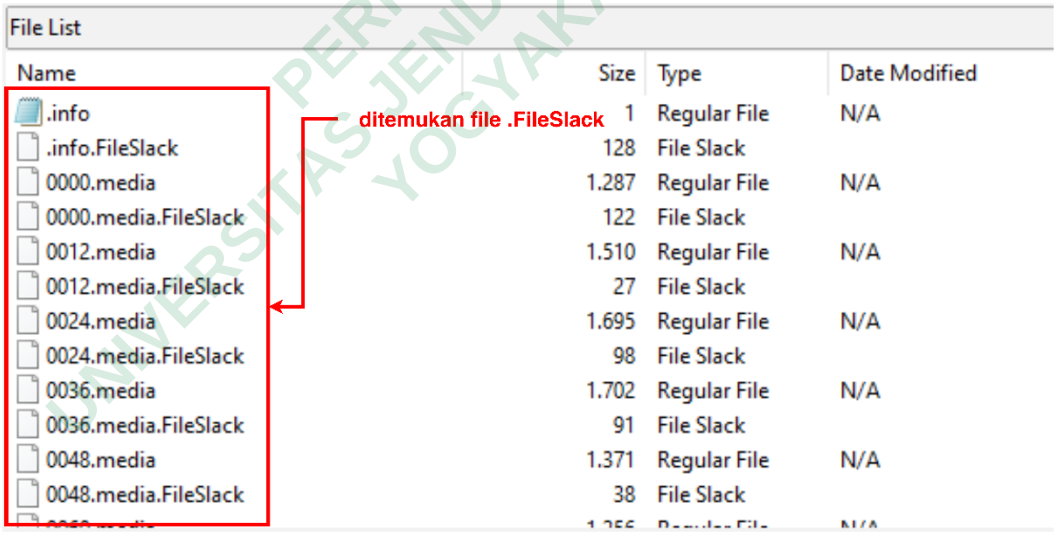


Gambar 4.5 Ditemukan *File* .jpg

Sama seperti *file* .media penulis kembali mengekstrak beberapa *file* .jpg untuk dilakukan percobaan membuka *file* .jpg. hasilnya sama seperti *file* .media, *file* .jpg dikatakan rusak dan tidak dapat dilihat/dibuka. Temuan ini mengindikasikan bahwa *file* tersebut telah dienkripsi menggunakan format *encoding proprietary* oleh sistem Tuya atau BARDI.

2. FTK Imager

Analisis lanjutan dilakukan menggunakan FTK Imager versi 4.7.1.2. Tujuannya sama seperti Autopsy untuk melihat dan memverifikasi direktori secara langsung. Analisis lanjutan menggunakan FTK *Imager* ini dilakukan untuk mengetahui apakah ada *file* yang tidak terdeteksi oleh Autopsy yang dilakukan sebelumnya. Hasilnya menunjukkan bahwa *file image* CCTV20250425.dd ini memiliki satu partisi dengan format *file* sistem exFAT, serta beberapa direktori yang sama seperti pada Tabel 4.5, termasuk direktori /.tuya.sd.test/ dan /DCIM/. Namun yang membedakan dalam FTK *Imager* ini ditemukan *file slack* Seperti pada Gambar 4.6



Gambar 4.6 Ditemukan Ekstensi .*File*Slack

3. DMDE

Penulis juga menggunakan DMDE untuk melakukan analisis lanjutan pada *image* CCTV20250425.dd. *tools* ini digunakan untuk melihat struktur media penyimpanan secara *low-lavel*, termasuk direktori tersembunyi dan *metadata* teknis lainnya yang mungkin tidak terbaca oleh Autopsy dan FTK *Imager*. Hasil

analisis menggunakan DMDE ini *menunjukkan* hal yang serupa seperti pada Tabel 4.4, *file* .media yang ditampilkan oleh DMDE juga tidak memiliki struktur yang umum. Tidak ditemukan juga metadata *file* seperti .mp4, .jpg, dan .mov. Hasil ini semakin memperkuat dugaan bahwa *file* .media disimpan dalam *proprietary encoding* atau terenkripsi oleh sistem Tuya atau Bardi sehingga tidak dapat dianalisis lebih lanjut tanpa proses *decoding* khusus.

4. Carving

Setalah dilakukan analisis menggunakan Autopsy, FTK *Imager* dan DMDE tetapi *file-file* tersebut tidak dapat diputar baik menggunakan VLC atau media *player* lain. Maka dari itu penulis melakukan analisis lanjutan berupa *file carving* dengan tujuan untuk mengidentifikasi *file* yang tersembunyi atau tehapus yang memungkinkan mendapat *fragmen file* dalam format .mp4, .avi, atau .264. serta melacak jejak struktur *file* yang tidak dikenali oleh *file* sistem utama, dalam melakukan *file carving* ini penulis menggunakan 3 *tools* seperti Foremost, Photorec, dan Sclapel. Hasil setelah dilakukan *carving* pada Tabel 4.6.

Tabel 4.6 Hasil Carving Foremost, Photorec, dan Scalpel.

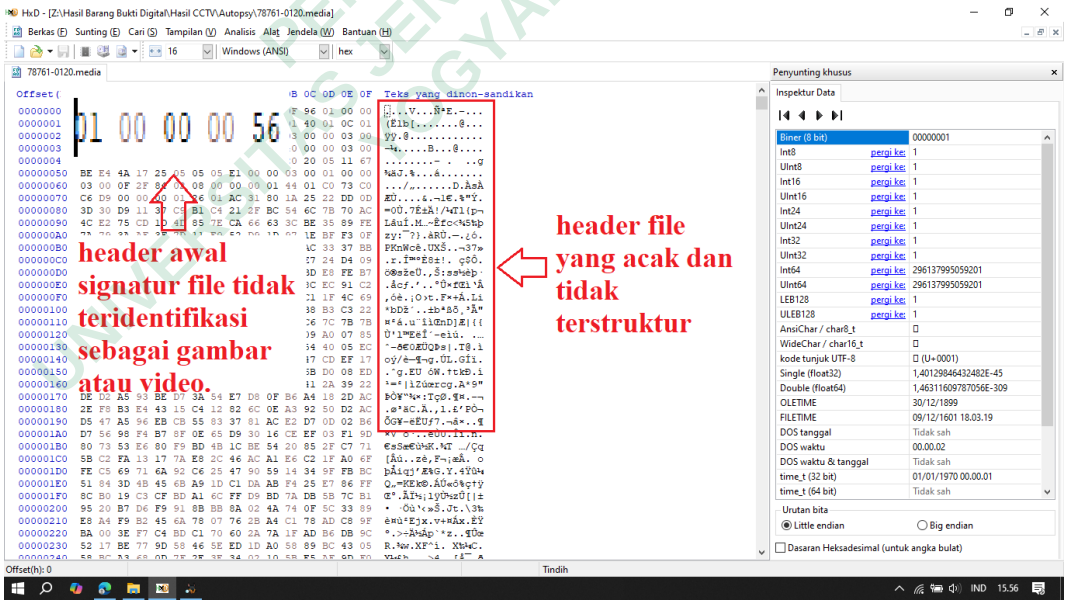
Tools	Nama File	Ukuran	Status	Keterangan
Foremost	04361247.mov	3,81 MB	Rusak	tidak dapat dibuka, tidak memiliki *header* video yang valid dan kemungkinan terenkripsi atau korup
Photorec	f132181496.swf	126 MB	Rusak	tidak dapat dibuka, tidak memiliki *header* video yang valid dan kemungkinan terenkripsi atau korup
Scalpel	00005485.mov	9,53 MB	Rusak	tidak dapat dibuka, tidak memiliki *header* video yang valid dan kemungkinan terenkripsi atau korup

Salah satu *file carving* yang didapat kemudian dibuka menggunakan *hexeditor* untuk memastikan apakah terdapat struktur *header* yang sesuai dengan *signature file* JPEG, MP4, MOV, dan AVI seperti Tabel 4.7.

Tabel 4.7 Jenis Signature *File* Sesuai Ekstensinya (*GCK File Signatures*, 2025).

Jenis	Signature *File*
JPEG	FF D8 FF E0
MP4	66 74 79 70 atau 69 73 6F 6D
MOV	6D 6F 6F 76
AVI	41 56 49 20 atau 4C 49 53 54

Hasilnya didapatkan *header* dan signature *file* yang acak dan tidak terstruktur. seperti pada Gambar 4.7 yang menunjukkan salah satu *file* hasil *carving*, kemudian dibuka menggunakan *hexeditor* untuk dianalisis lebih lanjut. Dugaan bahwa *file* telah dienkripsi oleh perangkat atau menggunakan format *encoding proprietary* semakin kuat karena *file* tersebut tidak memiliki *header* dan *signature* yang sesuai dengan format yang ada pada Tabel 4.7.



Gambar 4.7 *Header* dan Hex tidak Teridentifikasi.

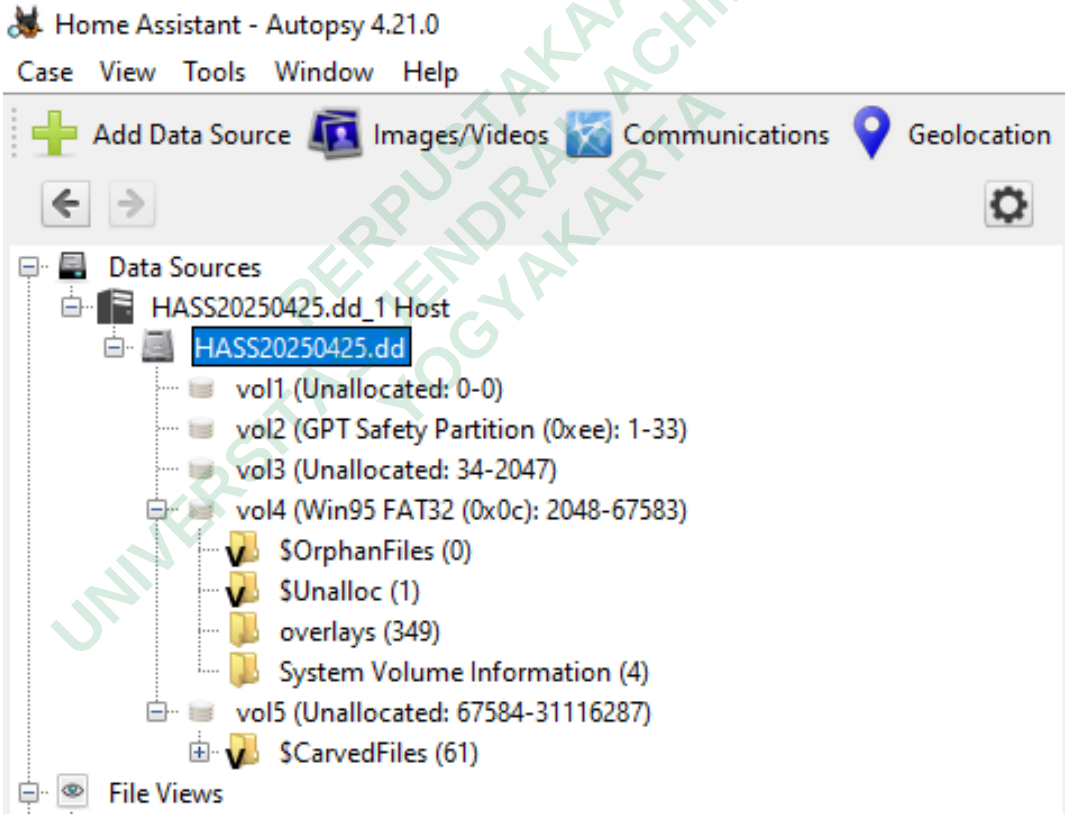
b. *Home Assistant*

Dari hasil analisis yang telah dilakukan menggunakan Autopsy, FTK *Imager*, dan DMDE tidak ditemukan *file* berupa video atau gambar dalam bentuk langsung

seperti .mp4 atau jpg yang tersimpan dalam *Home Assistant*. Hal ini mengindikasikan bahwa *Home Assistant* hanya bekerja sebagai pengendali perangkat BARDI *Smart* IP *Camera Outdoor* PTZ saja, sedangkan penyimpanan rekaman menggunakan *cloud* Tuya sepenuhnya.

1. Autopsy

Analisis awal HASS20250425.dd yang merupakan barang bukti digital hasil dari proses akuisisi media penyimpanan *Home Assistant* menggunakan perangkat lunak Autopsy versi 4.21.0. Analisis ini bertujuan untuk mengidentifikasi sistem *file*, partisi, dan artefak digital yang mungkin tersimpan dalam HASS20250425.dd. Setelah *file* HASS20250425.dd dibuka menggunakan Autopsy, terdapat 5 volume berbeda seperti pada Gambar 4.8.



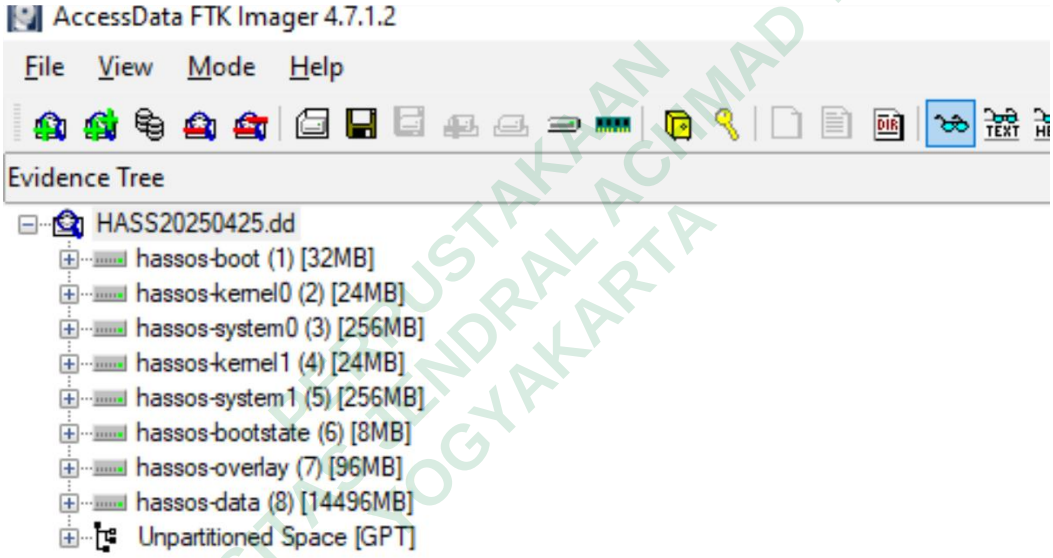
Gambar 4.8 Struktur partisi HASS20250425.dd yang ditemukan Autopsy.

Hasil ini memberikan informasi tentang partisi dan volume yang digunakan oleh *Home Assistant*. Ditemukan partisi FAT32 dan beberapa volume *unallocated*. Dalam temuan ini volume 4 teridentifikasi sebagai sistem *file* FAT32, namun dalam volume tersebut tidak ditemukan *file* yang dapat dijadikan

sebagai barang bukti potensial. Hasil ini mengindikasikan bahwa Autopsy tidak dapat mengekstrak partisi EXT4 yang digunakan oleh *Home Assistant*.

2. FTK *Imager*

Analisis lanjutan dilakukan menggunakan FTK Imager versi 4.7.1.2 diharapkan dapat menunjukkan hasil yang lebih komprehensif. Setelah *file* HASS20250425.dd dibuka, ditemukan 8 partisi pada HASS20250425.dd yang menunjukkan bahwa *Home Assistant* ini menggunakan sistem *multi* partisi seperti pada Gambar 4.9.



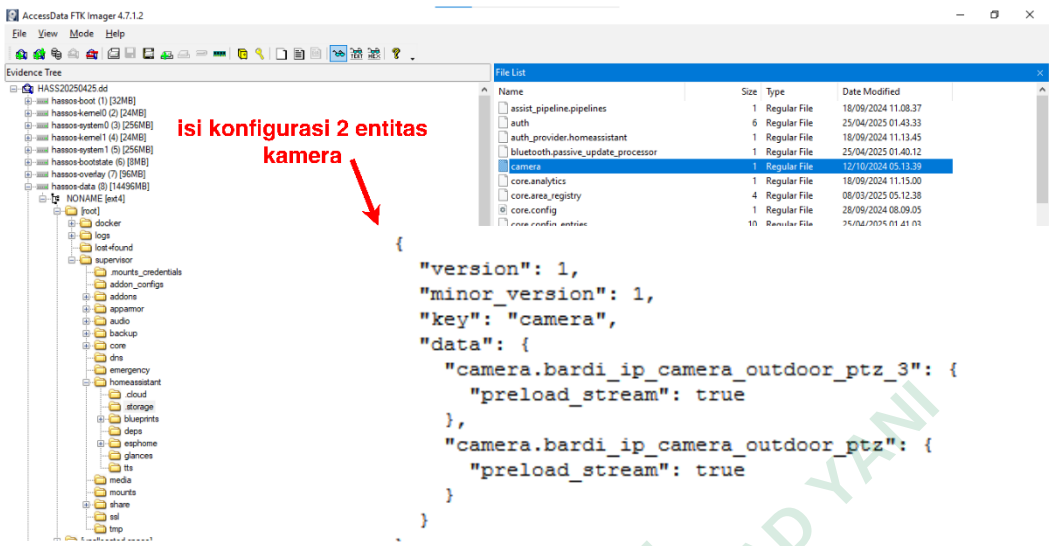
Gambar 4.9 Volume HASS20250425.dd yang ditemukan pada FTK *Imager*.

Dari 8 struktur partisi *Home Assistant* ini, penulis memfokuskan proses analisis pada partisi hassos-data karena memungkinkan menyimpan artefak digital yang relevan. Adapun keterangan pada tiap partisi pada Tabel 4.8.

Tabel 4.8 Struktur Partisi *Home Assistant* dari FTK *Imager*.

Partisi	Ukuran	Keterangan
Hassos-boot	32 MB	Berisi konfigurasi *booting* awal perangkat.
Hassos-karnel10	24 MB	*Karnel* pertama dari *Home Assistant*.
Hassos-system0	256 MB	Sistem utama *Home Assistant.*
Hassos-karnel11	24 MB	*Karnel* kedua untuk cadangan *failover*.
Hassos-system1	256 MB	*Root file* sistem sekunder untuk *update* OTA/*failback boot*.
Hassos-bootstate	8 MB	Menyimpan status terakhir *boot*.
Hassos-overlay	96 MB	Menyimpan perubahan sistem sementara.
Hassos-data	14, 496 MB	Menyimpan semua *file* konfigurasi, *file log*, *database*, dan integrasi.

Tujuan dari analisis ini untuk menemukan bukti digital terkait integrasi antara BARDI *smart* IP *Camera Outdoor* PTZ yang terintegrasi dengan *Home Assistant*, serta mengidentifikasi barang bukti yang potensial berupa video, foto, *log*, atau konfigurasi. Setelah struktur *file* dari *Home Assistant* diketahui, partisi dari hassos-data menjadi partisi yang paling memungkinkan menyimpan barang bukti potensial karena berisis *file* konfigurasi, *file log*, *database*dan integrasi. Setelah dilakukan penelusuran pada partisi hassos-data, ditemukan sebuah *file* dengan format .json pada direktori /*root*/supervisor/homeassistant/.storage/ yang berisi konfigurasi dua entitas kamera seperti pada Gambar 4.10.



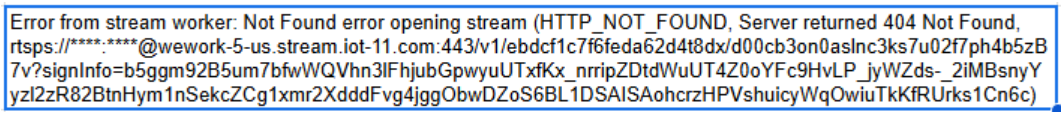
Gambar 4.10 Konfigurasi Entitas Kamera yang ditemukan FTK Imager.

Secara teknis hasil ini menunjukkan bahwa *Home Assistant* telah mengidentifikasi *streaming* untuk dua entitas kamera tersebut. Temuan ini menjadi indikator bahwa BARDI *smart* IP *Camera Outdoor* PTZ ini berhasil dihubungkan dan diketahui oleh *Home Assistant* meskipun belum terbukti menyimpan video secara lokal. Lebih detailnya pada Tabel 4.9.

Tabel 4.9 Entitas Kamera yang Diketahui *Home Assistant*

Artefak	Properti	Nilai	Direktori *File*
Camera.bardi_ip_*camera_outdoor*_PTZ	*Preload_stream*	*True*	/*root*/supervisor/homeassistant/.storage/camera
Camera.bardi_ip_*camera_outdoor*_PTZ_3	*Preload_stream*	*True*	/*root*/supervisor/homeassistant/.storage/camera

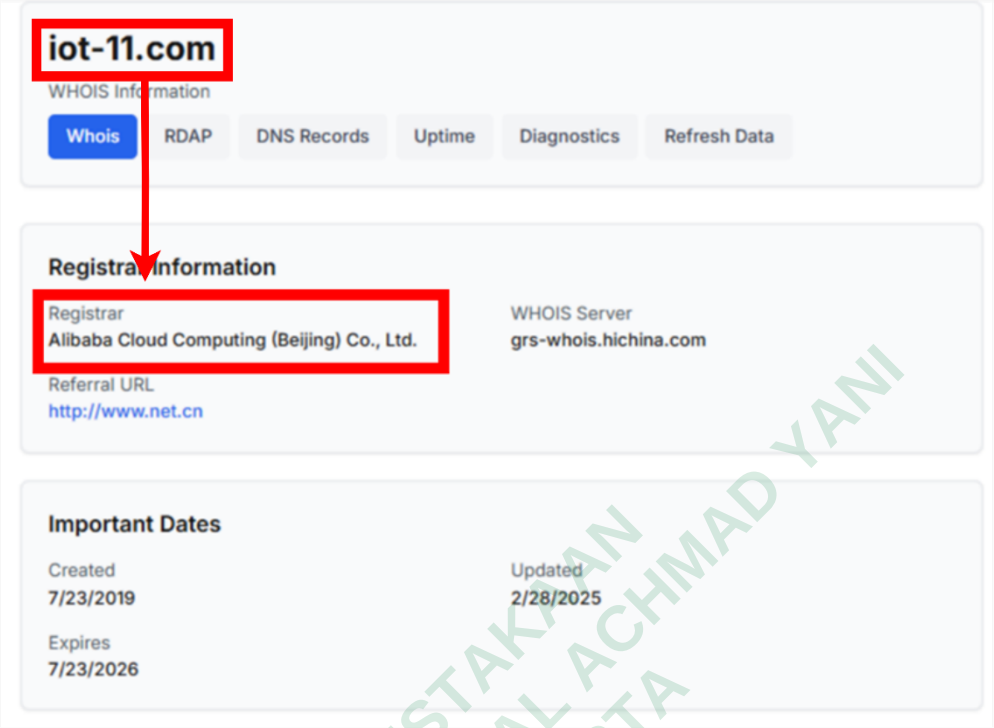
Selain *file* konfigurasi, pada direktori /supervisor/homeassistant/ ditemukan juga *file* home-assistant.*log*, *file log* ini berisi pesan *error* yang terjadi ketika *Home Assistant* mencoba mulai melakukan *stream* dari perangkat BARDI *Smart* IP *Camera Outdoor* PTZ. Pesan *error* ini berasal dari *stream_worker* yang mencatat kegagalan pada saat membuka *stream* melalui protokol RTSP (*Real Time Streaming Protocol*). *Log* yang ditemukan ini kemudian diekspor ke dalam *spreadsheet* untuk dianalisis lebih lanjut, hasilnya ditemukan domain wework-5-us.stream.iot.com dan muncul berulang, ini mengindikasikan bahwa kamera bergantung pada layanan *cloud*. seperti pada Gambar 4.11.



Gambar 4.11 Pesan *Error Stream* dari Entitas Kamera.

Penelusuran menggunakan WHOIS dilakukan setelah ditemukan domain wework-5-us.stream.iot-11.com, hasilnya menunjukkan bahwa domain ini milik *Amazon Technologies Inc.* dengan IP Address 52.12.191.236, seperti pada Gambar 4.12. Namun, domain iot-11.com dikelola oleh *Alibaba Cloud Computing Beijing Co., Ltd.*, seperti pada Gambar 4.13

Gambar 4.12 Penelusuran Domain wework-5-us.stream.iot-11.com.



Gambar 4.13 Penelusuran *Domain* iot-11.com.

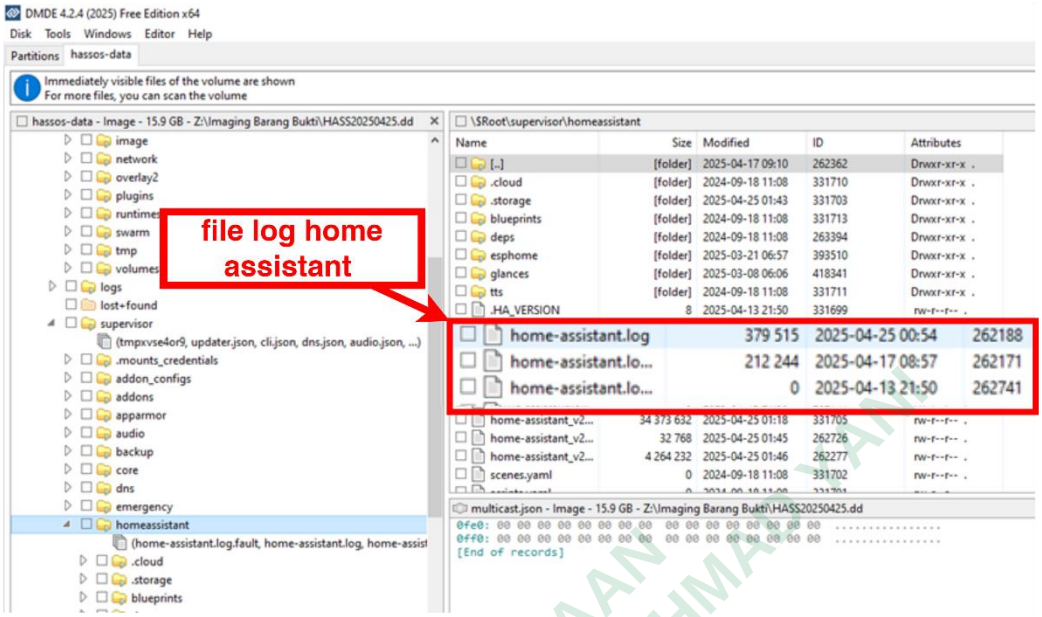
Hasil dari temuan FTK *Imager* ini menegaskan bahwa *Home Assistant* hanya berperan sebagai pengendali perangkat BARDI *Smart* IP *Camera Outdoor* PTZ tidak menyimpan hasil rekaman secara lokal dan mengandalkan *cloud* Tuya sepenuhnya sebagai media penyimpanan video.

3. DMDE

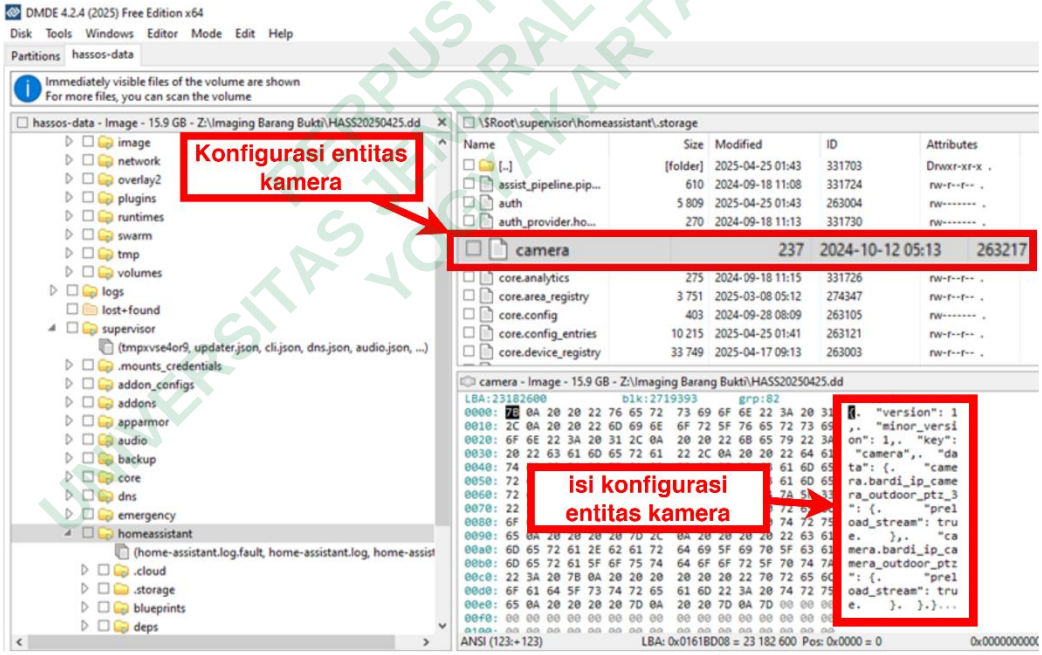
Analisis lanjutan *image* HASS20250425.dd dari hasil akuisisi media penyimpanan Raspberry Pi 4 yang menjalankan *Home Assistant* menggunakan perangkat lunak DMDE versi 4.2.4 yang merupakan alat forensik untuk melakukan penelusuran mendalam. Setelah *image* HASS20250425.dd dibuka menggunakan DMDE, ditemukan struktur partisi dari SD *card*, terdiri dari 8 partisi yang sama seperti hasil dari FTK *Imager* dan Tabel 4.7. Pada Gambar 4.14 merupakan hasil dari DMDE yang mendeteksi struktur *file* partisi.

Gambar 4.14 Struktur Partisi yang ditemukan DMDE.

Sama seperti pada FTK *Imager*, direktori hassos-data menjadi fokus utama karena diduga menyimpan *file* konfigurasi dan artefak digital dari *Home Assistant* dan juga karena partisi ini memiliki ukuran yang paling besar di antara partisi yang lain sekitar 15.2 GB. Setelah dilakukan penelusuran dalam partisi hassos-data ditemukan *file* home-assistant.*log* pada direktori /*root*/supervisor/homeassistant/ seperti pada Gambar 4.15. *File log* tersebut telah diidentifikasi sebagai barang bukti digital potensial dalam proses integrasi dan komunikasi antara *Home Assistant* dari perangkat BARDI *Smart* IP *Camera Outdoor* PTZ. Kemudian dalam direktori /*root*/supervisor/homeassistant/.storage/ ditemukan *file* camera yang berformat .json, seperti pada Gambar 4.16. sama dengan yang ditemukan di FTK *Imager*. Temuan ini menegaskan kembali bahwa *Home Assistant* mengenali dan mengaktifkan *stream* untuk perangkat BARDI *Smart* IP *Camera Outdoor* PTZ, meskipun tidak menyimpan video secara lokal.



Gambar 4.15 Temuan *File Log Home Assistant* dari DMDE



Gambar 4.16 Temuan Artefak Entitas Kamera dari DMDE

Hasil DMDE ini memperkuat temuan dari FTK *Imager*, bahwa *Home Assistant* menyimpan konfigurasi dan *log* sistem, namun tidak menyimpan *file* video atau foto secara lokal dan menegaskan bahwa sebagian besar komunikasi dan penyimpanan dilakukan melalui integrasi *cloud* milik Tuya.

c. Tuya App

Setelah melakukan akuisisi *logical* pada direktori /data/data/com.tuya.*smart*/databases/ yang kemungkinan menyimpan artefak digital dari aplikasi Tuya. Ditemukan beberapa *file* .db seperti pada Gambar 4.3 dan dilakukan analisis menggunakan *SQlite Viewer* pada setiap *file* .db yang ditemukan. Hasilnya seperti pada Tabel 4.10.

Tabel 4.10 Temuan *file* .db dari direktori databases aplikasi Tuya

Artefak	Direktori	Status	Temuan
mqttAndroidService.db	/data/data/com.tuya.*smart*/databases/	Terbaca	Terdapat tabel kosong
thing*smart*_encrypt_analysis.db	/data/data/com.tuya.*smart*/databases/	Terenkripsi	Kemungkinan berisi konfigurasi dan aktivitas perangkat terhubung
thing*smart*_stat_encrypted.db	/data/data/com.tuya.*smart*/databases/	Terenkripsi	Kemungkinan berisi statistik dan *log* perangkat yang terhubung

Pada saat MqttAndroidServices.db dibuka menggunakan *SQlite Viewer* ditemukan sebuah tabel dengan struktur kolom yang kemungkinan sering digunakan untuk komunikasi MQTT seperti pada Tabel 4.11, tabel pada MqttAndroidServices.db ini tidak memiliki data sama sekali, sehingga tidak menemukan informasi mengenai perintah atau komunikasi yang telah terjadi. Kemungkinan ini bisa terjadi disebabkan sinkronisasi melalui server *cloud* Tuya sehingga data tidak tersimpan.

Tabel 4.11 Struktur Tabel MqttAndroidService.db

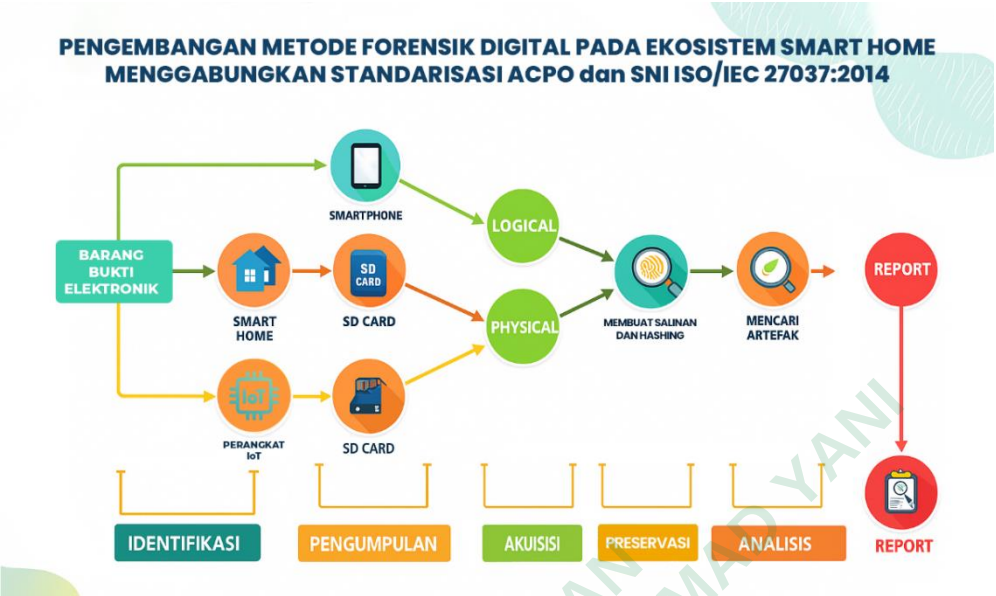
Nama	Tipe Data	Deskripsi
MessageId	Integer (Primary Key)	ID untuk setiap pesan MQTT.
ClientHandle	Text	Klien yang menangani pesan.

Nama	Tipe Data	Deskripsi
DestinationName	Text	Tujuan pesan yang diterima.
Payload	BLOB/Text	Isi pesan yang diterima.
Qos	Integer	Tingkat QoS dari pesan.
Mtimestamp	Integer	Timestamp waktu pesan diterima.

Sementara itu *file* *thingsmart*_encrpt_*analysis*.db dan *thingsmart_stat_encrypted*.db tidak dapat dibuka dikarenakan kedua *file* tersebut terenkripsi oleh aplikasi Tuya, kemungkinan kedua *file* tersebut berpotensi menyimpan data ataupun informasi.

4.2 Usulan Prosedur Forensik Digital

Penelitian ini menunjukkan bahwa proses investigasi dan analisis forensik digital pada ekosistem *smart home* dapat dilakukan dengan mengikuti tahapan identifikasi, pengumpulan, akuisisi, preservasi, analisis, dan pelaporan sesuai dengan standar ACPO dan SNI ISO/IEC 27037:2014. Secara keseluruhan penelitian ini mengembangkan metode forensik digital pada ekosistem *smart home*, seperti pada Gambar 4.17.



Gambar 4.17 Pengembangan Metode Forensik Digital pada Ekosistem *Smart Home*.