BAB 3
METODE PENELITIAN

Penelitian ini merupakan studi eksperimen yang melakukan akuisisi dengan mengadopsi standar ACPO dan SNI ISO/IEC 27037:2014 untuk mengumpulkan dan menganalisis bukti digital dalam ekosistem *smart home*. Pendekatan yang digunakan dalam penelitian ini menggabungkan metode forensik *hybrid* yang terbagi dalam beberapa tahap utama, yaitu identifikasi, pengumpulan, akuisisi, preservasi, dan analisis.

3.1 Alat dan Bahan Penelitian

a. Alat Penelitian

1. BARDI *Smart* IP Camera *Outdoor* PTZ

   Smart CCTV ini menjadi objek utama dalam penelitian ini karena dapat menyimpan rekaman video ke dalam SD *card* dan mengirimkan video ke server *cloud* milik Tuya. *Smart* CCTV ini juga mendukung deteksi gerak, notifikasi dan kontrol melalui *smartphone.*

2. *Smartphone* Xiaomi (*rooted*)

   Smartphone ini digunakan untuk menjalankan aplikasi Tuya App yang berfungsi sebagai pengendali utama *smart* CCTV. *Smartphone* ini sudah dalam keadaan *rooted* sehingga memungkinkan peneliti melakukan akuisisi penuh direktori internal aplikasi dengan tujuan untuk menemukan artefak seperti *database*.db dan *log* aktivitas yang menyimpan data koneksi dan riwayat kontrol perangkat.

3. Raspberry Pi 4

   Raspberry Pi 4 ini digunakan sebagai aplikasi *Home Assistant* yaitu sistem *open source* untuk mengelola perangkat *smart home* dan digunakan untuk memonitor serta mengendalikan perangkat *smart* CCTV yang terintegrasi melalui Tuya *cloud.*

4. SD Card V-Gen 126 GB

   Digunakan sebagai media penyimpanan untuk BARDI *Smart* IP *Camera Outdoor* PTZ. SD *card* ini akan diakuisisi dan dianalisis menggunakan *tools* forensik untuk mendapatkan bukti digital.

5. SD Card SanDisk Ultra 16 GB

   Digunakan sebagai sistem operasi *Home Assistant* serta menyimpan *log* perangkat, konfigurasi, dan artefak digital lain. SD *card* ini juga akan diakuisisi dan dianalisis menggunakan *tools* forensik untuk mendapatkan bukti digital.

b. Bahan Penelitian

Bahan yang digunakan untuk melakukan akuisisi dan analisis barang bukti digital pada penelitian ini seperti *software* dan *hardware* yang mendukung dalam proses investigasi barang bukti digital seperti pada Tabel 3.1.

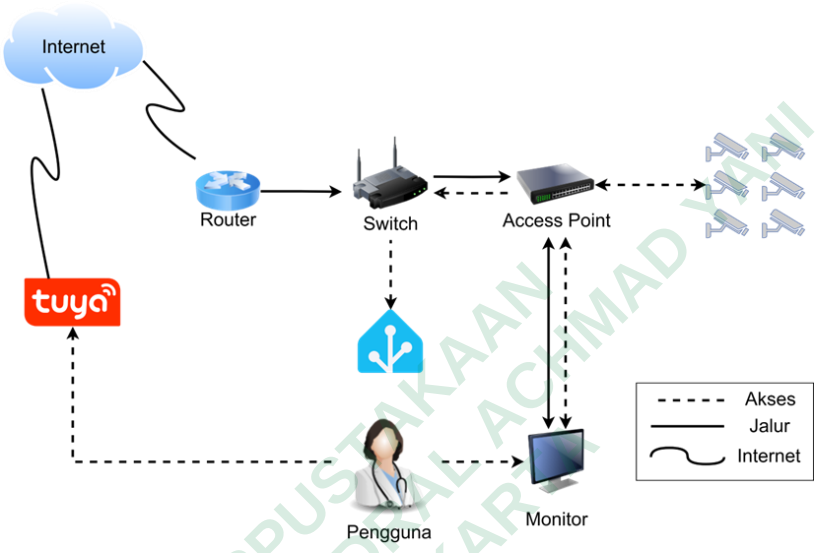
Tabel 3.1 Bahan Penelitian

No	Nama	Jenis	Keterangan
1	*Guymager*	*Software* forensik	Untuk membuat *image disk*.
2	*Android Debug Bridge* (ADB)	*Tools* android	Untuk melakukan akuisisi pada *smartphone.*
3	Sqlite *Viewer*	*Software database*	Untuk melihat dan menganalisis isi *database*.
4	Autopsy	*Software* forensik	Untuk melakukan analisis barang bukti digital
5	FTK Imager	*Software* forensik	Untuk melakukan analisis barang bukti digital

No	Nama	Jenis	Keterangan
6	Photorec	Data *recovery tools*	Untuk memulihkan *file* yang terhapus dari berbagai media penyimpanan
7	Scalpel	*File carving tools*	Untuk *recovery* data berdasarkan pola *header file*.
8	Foremost	*File carving tools*	Untuk mengekstraksi *file* dari *image disk* berdasarkan format *file*.
9	Binwalk	*Firmware analysis tools*	Untuk menganalisis *firmware,* mengekstrak data dari *binary file.*
10	Hex Editor	Editor biner	Untuk melihat dan mengubah *file* dalam format hexadecimal.
11	Laptop ThinkPad X260	Perangkat keras	Ram 8GB, Intel Core i5- 6300U, 477GB SSD, *Dual boot* Ubuntu-Windows (200GB Ubuntu).
12	*Card Reader*	Perangkat keras	Untuk membaca SD *card* saat proses *imaging*/ekstraksi data.
13	Kabel Data	Perangkat Keras	Untuk menghubungkan perangkat ke komputer saat proses akuisisi data.
14	*Hard Disk*	Media penyimpanan	Untuk menyimpan hasil akuisisi dari berbagai barang bukti elektronik
15	Ekosistem *Smart Home*	Sistem intergrasi	Jaringan perangkat pintar yang saling terhubung, dikontrol via aplikasi atau *voice assistant.*

Arsitektur ekosistem *smart home* yang telah dibuat dan digunakan dalam penelitian ini seperti pada Gambar 3.1 dan penjelasannya pada Tabel

3.2. Arsitektur ini dirancang untuk merepresentasikan sistem *smart home* yang terintegrasi dengan berbagai perangkat IoT dan semuanya dikendalikan melalui aplikasi Tuya. Sistem ini terdiri dari beberapa komponen utama. Masing-masing komponen memiliki peran spesifik dalam mendeteksi, mengirim, dan mengeksekusi perintah secara otomatis atau manual.



Gambar 3.1 Arsitektur Ekosistem *Smart Home* (Kusumaningrum dkk., 2024)

Tabel 3.2 Tabel Pengoperasian Ekosistem *Smart Home*

Komponen	**Fungsi**
ONT Modem	Menerima internet dari ISP dan mengubahnya menjadi sinyal digital.
Router	Mengelola lalu lintas jaringan, membagi IP, dan mengarahkan paket data.
Switch	Menyambungkan banyak perangkat secara fisik dalam jaringan lokal.
Access Point	Menyediakan akses jaringan nirkabel ke sensor atau perangkat lainnya.
Sensor	Mendeteksi kondisi atau aktivitas dan mengirimkannya ke sistem/server.
Monitor	Sistem pemantauan menampilkan hasil dari data sensor untuk pemantauan.

Pengguna	Mengamati dan mengendalikan sistem berdasarkan pengolahan *Home Assistant*

3.2 Jalan Penelitian

Penelitian fokus pada akuisisi perangkat *smart* CCTV yang terintegrasi dengan ekosistem *smart home*. Objek utama dalam penelitian ini di antaranya, perangkat *smart* CCTV, *Home Assistant*, dan aplikasi Tuya App. Metode standar yang digunakan dalam penelitian ini mengadopsi standar ACPO dan SNI ISO/IEC 27037:2014. Jalan penelitian ini dibagi menjadi 5 tahapan seperti pada Gambar 3.2.

Gambar 3. 2 Jalan Penelitian

1. Identifikasi

   Pada tahap ini peneliti melakukan proses identifikasi terhadap perangkat dan media penyimpanan yang digunakan dalam ekosistem *smart home*. Identifikasi ini dilakukan untuk mengetahui jenis perangkat, jenis media penyimpanannya. Hasil dari identifikasi ini digunakan untuk menentukan metode akuisisi yang sesuai dengan jenis perangkat dan media penyimpanannya. Perangkat yang berhasil diidentifikasi pada Tabel 3.3

Tabel 3.3 Identifikasi Barang Bukti Elektronik

No	**Barang Bukti Elektronik**	**Jumlah**	**Penyimpanan**
1.	BARDI *Smart* IP *Camera Outdoor* PTZ	1	Eksternal
2.	*Smartphone* Xiaomi 5s Plus (*Rooted*)	1	Internal
3.	Raspberry Pi 4	1	Eksternal
4.	SD *Card*	2	-

2. Pengumpulan

Mengumpulkan media penyimpanan dari masing-masing barang bukti elektronik yang sudah teridentifikasi pada Tabel 3.3 sebelumnya. Setiap media penyimpanan dilepas dengan hati-hati agar tidak terjadi perubahan dan dapat dilakukan proses akuisisi.

Gambar 3.3 Barang Bukti Elektronik dan Media Penyimpanannya.

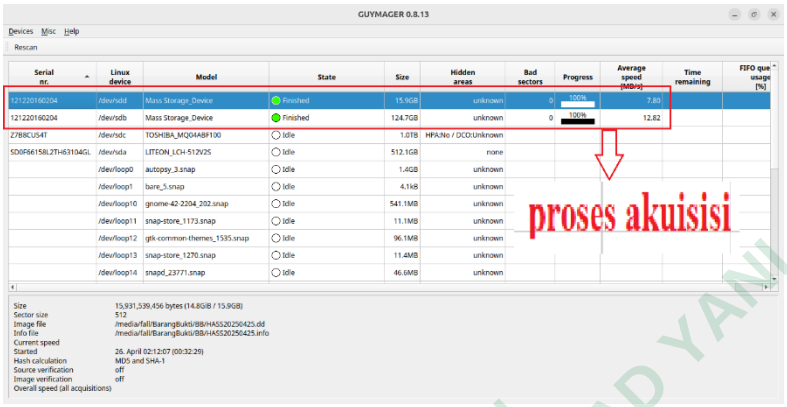
3. Akuisisi

Merupakan proses *imaging* dan ekstraksi dari barang bukti elektronik yang disesuaikan berdasarkan jenis perangkat dan media penyimpannya, metode ini digunakan untuk memaksimalkan ekstraksi dari berbagai perangkat tanpa merusak atau mengubah bukti digital yang asli. Metode akuisisi ini dibagi menjadi 2, di antaranya:

a. Akuisisi *Physical*

Melakukan akuisisi *physical* pada setiap penyimpanan eksternal yang ada di perangkat *smart* CCTV dan *Home Assistant* dengan menggunakan *Guymager* pada sistem operasi Linux. Proses ini bertujuan untuk mengambil isi penyimpanan secara *bit* per *bit* dalam bentuk *image file.* Hasil akuisisi *physical* ini disimpan dalam

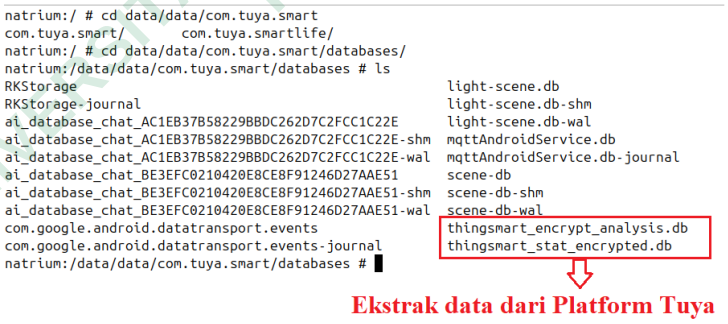
format .dd yang merupakan format citra *disk* mentah. seperti pada Gambar 3.5.



Gambar 3.4 Proses Imaging Penyimpanan *Smart Home* dan *Home Assistant.*

b. Akuisisi *Logical*

Melakukan akuisisi *logical* pada *smartphone* Xiaomi (*rooted)* yang terpasang aplikasi Tuya App. Akuisisi ini menggunakan ADB untuk mengekstrak direktori data aplikasi secara langsung dari sistem *file* android. *File* yang diambil berupa *database*dari aplikasi Tuya App seperti pada Gambar 3.6.



Gambar 3.5 Proses Ekstraksi Tuya App menggunakan ABD.

4. Preservasi

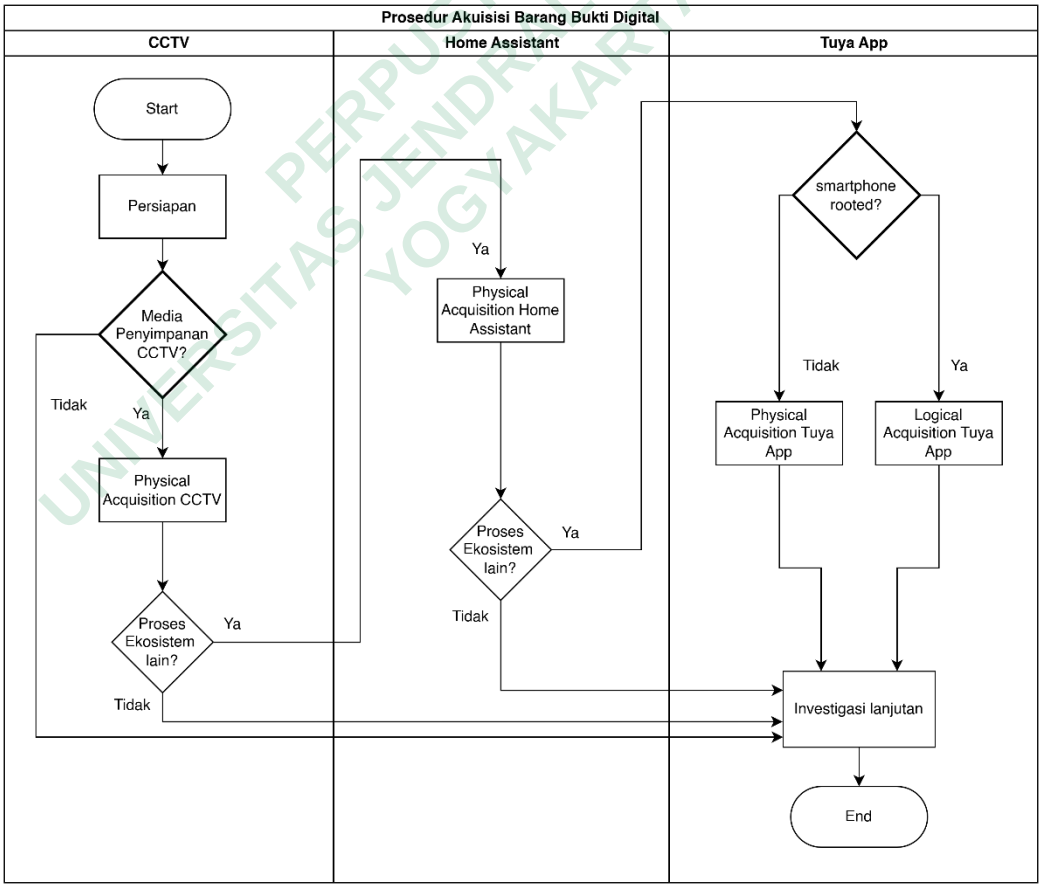
Pada tahap ini peneliti menyimpan hasil akuisisi ke media penyimpanan eksternal *(hard disk)* yang aman agar tidak terjadi perubahan pada barang bukti digital. Nilai hash MD5 dicatat agar menjamin bahwa integritas dan keaslian data tetap terjaga hingga tahap analisis.

5. Analisis

Pada tahap ini peneliti melakukan analisis dengan beberapa langkah, di antaranya:

a. Melakukan Analisis data dari hasil *imaging* SD *card smart* CCTV dan *Home Assistant* menggunakan Autopsy, FTK *Imager* dan DMDE.
b. Melakukan Analisis data *logical* yang telah diakuisisi dari aplikasi Tuya App.

Penelitian yang mengadopsi standar ACPO dan SNI ISO/IEC 27037:2014 ini membuat sebuah prosedur akuisisi barang bukti. Pada Gambar 3.7 menjelaskan prosedur akuisisi barang bukti yang digunakan dalam penelitian ini.



Gambar 3.6 Prosedur Akuisisi Barang Bukti

1. Persiapan Akuisisi

   Merancang teknik akuisisi berdasarkan karakteristik perangkat yang akan dianalisis. Persiapan ini juga mencakup pengecekan kondisi perangkat, dan menentukan metode akuisisi yang tepat.

2. Pemeriksaan Media Penyimpanan CCTV

   Setelah perangkat *smart* CCTV diamankan, dilakukan pemeriksaan apakah perangkat tersebut memiliki media penyimpanan eksternal, seperti kartu *micro* SD atau USB *storage*. Media eksternal ini menjadi sumber utama rekaman CCTV dan merupakan target akuisisi prioritas dalam proses ini.

3. Akuisisi Fisik dari CCTV

   Jika media penyimpanan ditemukan, maka dilakukan proses akuisisi fisik menggunakan metode *imaging* untuk menduplikasi isi media secara bit *level*. Proses ini dilakukan menggunakan *tools* seperti Guymager atau FTK *Imager*. Hasil akuisisi disimpan dalam format .dd dan dilakukan verifikasi hash.

4. Investigasi Lanjutan jika Tidak Ada Media

   Jika tidak ditemukan media penyimpanan pada perangkat CCTV, maka investigasi dilanjutkan di lab untuk menelusuri kemungkinan adanya penyimpanan berbasis *cloud* atau integrasi dengan sistem lain. Hal ini penting karena banyak perangkat IoT modern yang tidak menyimpan data lokal, melainkan mengalirkannya langsung ke server melalui internet.

5. Pemeriksaan Ekosistem Terkait (*Home Assistant*)

   Melakukan pengecekan terhadap ekosistem *smart home* yang mungkin terhubung dengan perangkat CCTV. Dalam penelitian ini, digunakan sistem *Home Assistant* yang berjalan di perangkat Raspberry Pi, yang memiliki potensi menyimpan *log*, konfigurasi, atau data rekaman terintegrasi.

6. Akuisisi Fisik dari *Home Assistant*

   Jika *Home Assistant* teridentifikasi memiliki media penyimpanan (biasanya *micro* SD card pada Raspberry Pi), maka dilakukan akuisisi fisik terhadap media tersebut. *Image*.dd dari media penyimpanan *Home Assistant*

diharapkan dapat menyimpan informasi penting seperti *log* koneksi perangkat CCTV, konfigurasi integrasi *cloud*, atau bukti aktivitas pengguna.

7. Investigasi Lanjutan jika Tidak Ada Media

   Jika media penyimpanan tidak ditemukan atau tidak dapat diakses, maka proses berlanjut ke tahap identifikasi perangkat atau aplikasi lain yang terhubung dengan CCTV, seperti aplikasi *mobile* yang digunakan oleh pengguna.

8. Pemeriksaan Aplikasi Tuya di *Smart*phone

   Langkah selanjutnya adalah menelusuri *smartphone* milik pemilik perangkat CCTV yang biasanya menjalankan aplikasi Tuya *Smart* sebagai pengontrol utama. Diperiksa apakah perangkat *smartphone* tersebut telah di *root*, karena status *root* menentukan metode akuisisi yang bisa dilakukan.

9. Akuisisi *Physical* atau *Logical* Tuya App (Jika *Rooted*)

   Jika perangkat telah di *root*, maka dimungkinkan melakukan akuisisi fisik maupun *logikal* terhadap direktori aplikasi Tuya, khususnya pada *path* /data/data/com.tuya.*smart*/. Pada direktori ini biasanya tersimpan *database*.db, konfigurasi pengguna, *log* koneksi, serta *token* autentikasi yang bisa menjadi bukti digital penting.

10. Akuisisi *Logikal* Terbatas (Jika Tidak *Rooted*)

    Jika perangkat belum di *root*, maka hanya dilakukan *logical acquisition* terbatas, seperti *backup* aplikasi, *file* APK, *metadata* yang bisa diakses publik, serta analisis terhadap *file log* sistem yang mencatat aktivitas Tuya App. Meskipun terbatas, proses ini tetap penting untuk menemukan korelasi antar perangkat.

11. Investigasi Lanjutan di Laboratorium

    Jika seluruh proses akuisisi dari semua perangkat tidak menghasilkan artefak digital yang jelas atau masih dalam bentuk terenkripsi/*proprietary*, maka dilakukan investigasi lanjutan di laboratorium forensik.