

# **KEASLIAN PENGEMBALIAN DATA PADA FLASH DRIVE SEBAGAI BUKTI DIGITAL**

## **TUGAS AKHIR**

Disusun sebagai salah satu syarat untuk kelulusan Program Strata 1,  
di Program Studi Teknik Informatika, Universitas Pasundan Bandung

oleh :

Fadhilah Fil-Ardh  
NRP : 14.304.0020



**PROGRAM STUDI TEKNIK INFORMATIKA  
FAKULTAS TEKNIK  
UNIVERSITAS PASUNDAN BANDUNG  
OKTOBER 2019**

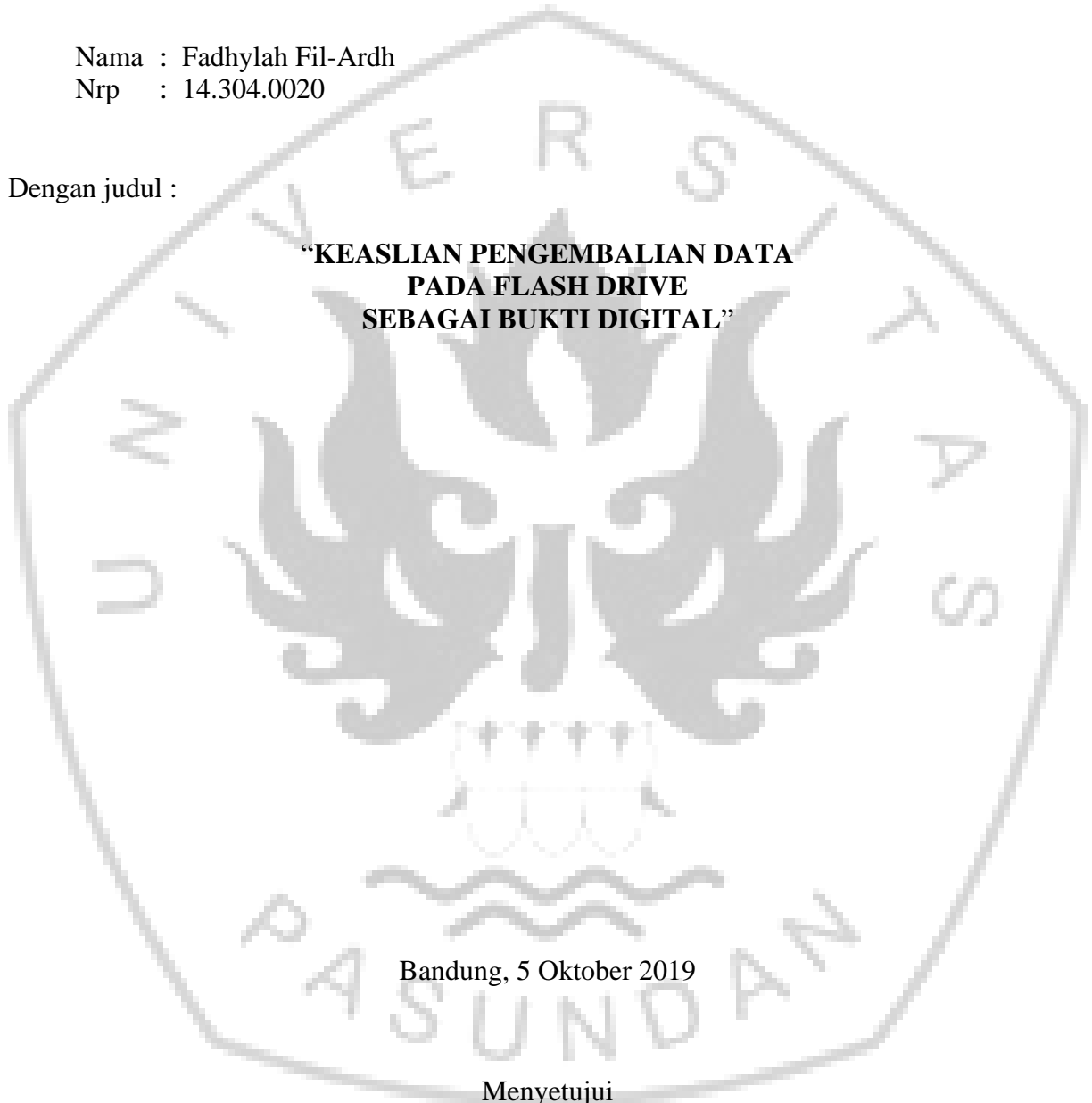
**LEMBAR PENGESAHAN  
LAPORAN TUGAS AKHIR**

Telah diujikan dan dipertahankan dalam Sidang Sarjana Program Studi Teknik Informatika Universitas Pasundan Bandung, pada hari dan tanggal sidang sesuai berta acara sidang, tugas akhir dari :

Nama : Fadhylah Fil-Ardh  
Nrp : 14.304.0020

Dengan judul :

**“KEASLIAN PENGEMBALIAN DATA  
PADA FLASH DRIVE  
SEBAGAI BUKTI DIGITAL”**



Bandung, 5 Oktober 2019

Pembimbing Utama

Menyetujui

Pembimbing Pendamping

(Rita Rijayanti, ST., MT)

(Doddy Ferdiansyah, ST., MT)

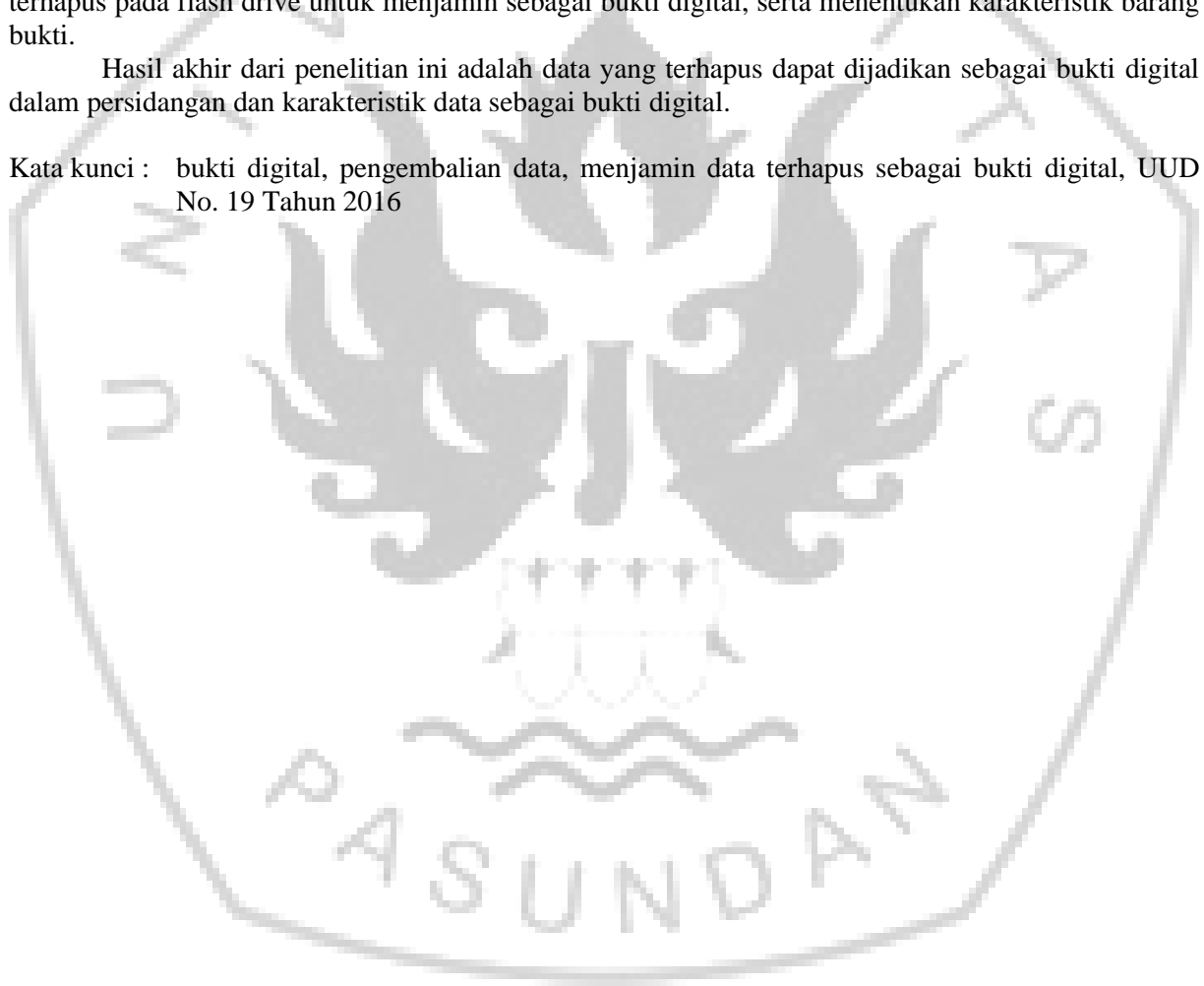
## ABSTRAK

Kehilangan data merupakan kejadian data yang diperlukan tidak dapat diakses karena terhapus, umumnya ketika data yang kita miliki tidak sengaja terhapus, flash drive yang bermasalah, dan tindakan yang disengaja untuk menghapus data. Kehilangan data merupakan kejadian yang serius, dimana data yang diperlukan tidak bisa diakses, karena tidak sengaja terhapus atau dihapus secara sengaja oleh seseorang. Data yang terhapus atau sengaja terhapus, dapat dijadikan sebagai bukti digital. Ini berlandaskan pada UUD Republik Indonesia tahun 2016, pada pasal 5 ayat 1 yang berbunyi “Bahwa keberadaan informasi Elektronik dan /atau Dokumen Elektronik mengikat dan diakui sebagai alat bukti yang sah untuk memberikan kepastian hukum terhadap Penyelenggaraan Sistem Elektronik dan Transaksi Elektronik, terutama dalam pembuktian dan hal yang berkaitan dengan perbuatan hukum yang dilakukan melalui Sistem Elektronik”. (UUD RI 2016)

Penelitian ini dilakukan untuk menjamin data terhapus dapat dijadikan sebagai bukti digital. Penelitian dilakukan dengan melakukan pengumpulan data dari flash drive, pengembalian data dan melakukan pengujian terhadap data yang terhapus, serta identifikasi data berdasarkan UUD No.19 Tahun 2016 pada pasal 5, 6 dan 16 ayat 1. Selanjutnya dilakukan analisis untuk menetapkan data terhapus pada flash drive untuk menjamin sebagai bukti digital, serta menentukan karakteristik barang bukti.

Hasil akhir dari penelitian ini adalah data yang terhapus dapat dijadikan sebagai bukti digital dalam persidangan dan karakteristik data sebagai bukti digital.

Kata kunci : bukti digital, pengembalian data, menjamin data terhapus sebagai bukti digital, UUD No. 19 Tahun 2016



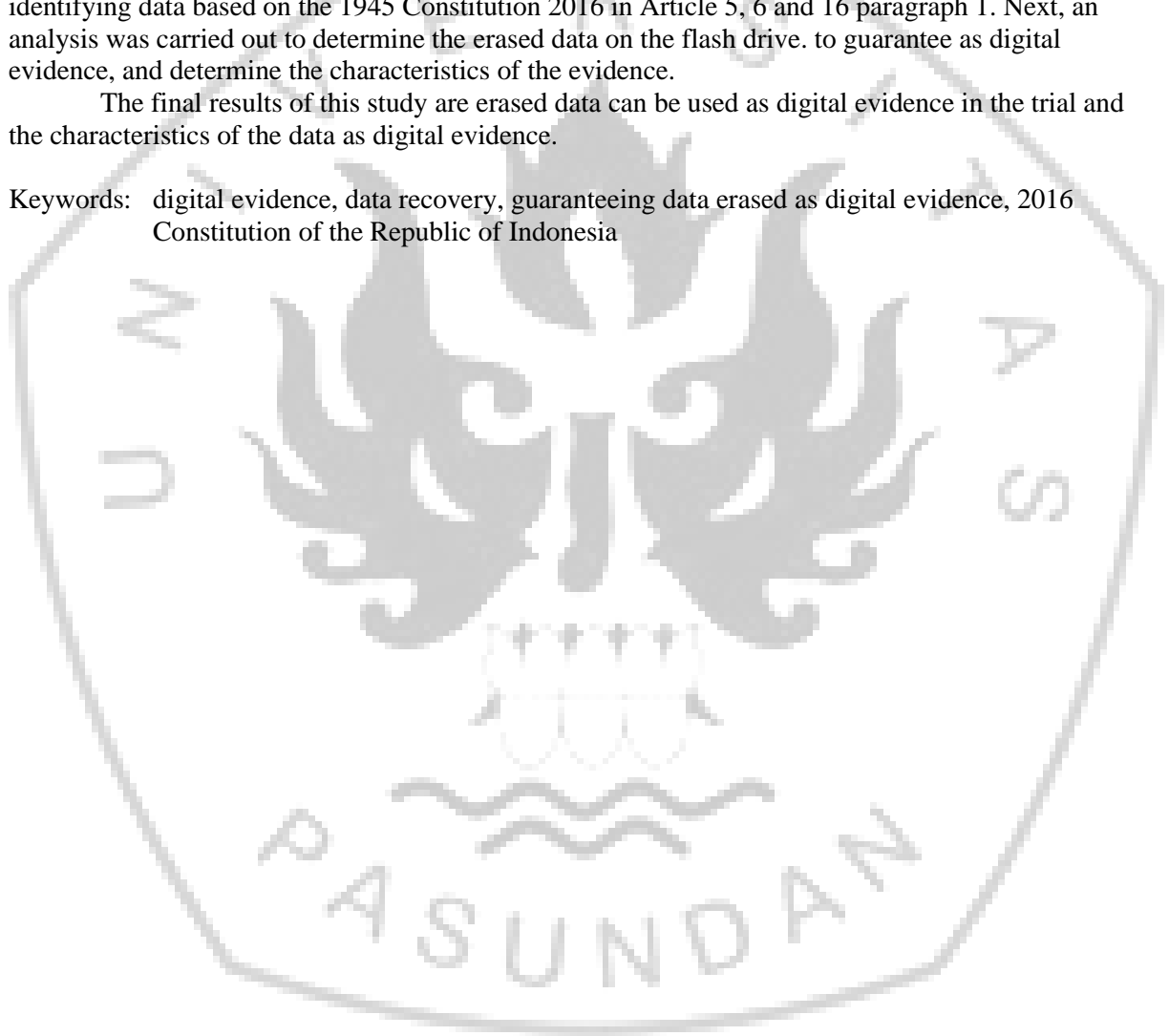
## ABSTRACT

Data loss is an event where the required data cannot be accessed because it is erased, generally when the data we have is accidentally deleted, the flash drive is in trouble, and the deliberate action to delete the data. Data loss is a serious event, where the required data cannot be accessed, because it was accidentally deleted or intentionally deleted by someone. Data that is erased or intentionally erased can be used as digital evidence. This is based on the 2016 Constitution of the Republic of Indonesia, in Article 5 paragraph 1 which reads "That the existence of Electronic Information and / or Electronic Documents is binding and is recognized as legal evidence to provide legal certainty for the Implementation of Electronic Systems and Electronic Transactions, especially in proving and matters relating to legal actions carried out through the Electronic System. " (Indonesian Constitution 2016)

This research was conducted to ensure erased data can be used as digital evidence. The study was conducted by collecting data from a flash drive, returning data and testing erased data, as well as identifying data based on the 1945 Constitution 2016 in Article 5, 6 and 16 paragraph 1. Next, an analysis was carried out to determine the erased data on the flash drive. to guarantee as digital evidence, and determine the characteristics of the evidence.

The final results of this study are erased data can be used as digital evidence in the trial and the characteristics of the data as digital evidence.

Keywords: digital evidence, data recovery, guaranteeing data erased as digital evidence, 2016 Constitution of the Republic of Indonesia



## DAFTAR ISI

ABSTRAK .....	i
ABSTRACT .....	ii
DAFTAR ISI .....	iv
DAFTAR TABEL .....	vi
DAFTAR GAMBAR .....	vii
BAB I PENDAHULUAN .....	1-1
1.1 Latar Belakang .....	1-1
1.2 Identifikasi Masalah .....	1-1
1.3 Tujuan Tugas Akhir .....	1-1
1.4 Lingkup Tugas Akhir .....	1-1
1.5 Metodologi Pengerjaan Tugas Akhir .....	1-2
1.6 Sistematika Penulisan Tugas Akhir .....	1-3
BAB 2 LANDASAN TEORI .....	2-1
2.1 Teori pendukung .....	2-1
2.1.1 Komputer Forensik .....	2-1
2.1.2. Tujuan dan Fokus Komputer Forensik .....	2-1
2.1.2. Metode Komputer Forensik .....	2-2
2.1.3. Aspek Hukum pada Komputer Forensik.....	2-5
2.1.4. Bukti Digital .....	2-6
2.1.5. Karakteristik Bukti Digital .....	2-6
2.1.6. Recovery .....	2-8
2.1.7. Tahapan – Tahapan Recovery Data .....	2-8
2.1.8. Keamanan Informasi .....	2-10
2.1.9. Aspek Keamanan Informasi .....	2-10
2.1.10. Jenis-Jenis Ancaman Keamanan Informasi .....	2-10
2.1.11. Undang-Undang Republik Indonesia No 19 Tahun 2016 .....	2-11
2.1.12. TestDisk & PhotoRec .....	2-12
2.1.13. Fitur-Fitur TestDisk & PhotoRec .....	2-12
2.1.14. Perbedaan Dengan Forensik Software Winhex .....	2-13
2.2. Penelitian Terdahulu .....	2-13
BAB 3 SKEMA PENELITIAN .....	3-1
3.1 Alur Penyelesaian Tugas Akhir .....	3-1
3.2 Analisis Persoalan dan Manfaat Tugas Akhir .....	3-3
3.3 Kerangka Pemikiran Teoritis .....	3-3
BAB 4 ANALISIS DAN PENGUJIAN .....	4-1

4.1. Analisis Pengujian.....	4-1
4.1.1. Analisis Kebutuhan .....	4-1
4.1.2. Analisis Flash Drive .....	4-1
4.1.3. Analisis data terhapus .....	4-1
4.2. Pengujian.....	4-2
4.2.1. Skenario Pengujian .....	4-2
4.2.2. Flash drive dapat digunakan .....	4-2
4.2.3. Mengisi data pada flash drive .....	4-3
4.2.4. Menghapus data pada flash drive.....	4-3
4.2.5. Pengambilan data pada flash drive .....	4-3
4.2.6. Mengisi kembali flash drive .....	4-4
4.2.7. Mengakses Drive image.....	4-5
4.2.8. Pengembalian data .....	4-5
4.3. Identifikasi Data .....	4-6
4.3.1. Identifikasi data dikembalikan.....	4-6
4.1.2. Perbandingan data dikembalikan dengan data asli .....	4-7
4.4. Pembuatan Dokumentasi.....	4-7
4.4.1. Keutuhan dan Keaslian data .....	4-8
4.1.2. Karakteristik data.....	4-9
4.5. Hasil Pengujian .....	4-10
<b>BAB 5 KESIMPULAN DAN SARAN.....</b>	<b>5-1</b>
5.1. Kesimpulan .....	5-1
5.2. Saran .....	5-1
5.3. Rekomendasi .....	5-1
<b>DAFTAR PUSTAKA</b>	
<b>LAMPIRAN</b>	

# BAB 1

## Pendahuluan

Dalam bab ini membahas mengenai pendahuluan dari tugas akhir meliputi latar belakang, identifikasi masalah, tujuan tugas akhir, lingkup tugas akhir, metodologi penyelesaian tugas akhir dan sistematika penulisan tugas akhir.

### 1.1 Latar Belakang

Kehilangan data merupakan kejadian data yang diperlukan tidak dapat diakses karena terhapus, umumnya ketika data yang kita miliki tidak sengaja terhapus, *flash drive* yang bermasalah, dan tindakan yang disengaja untuk menghapus data. Biasanya data yang menjadi korban adalah data yang sangat penting dan memiliki nilai pada setiap individu.

Kehilangan data merupakan kejadian yang serius, dimana data yang diperlukan tidak bisa diakses, karena tidak sengaja terhapus atau dihapus secara sengaja oleh seseorang. Sebagai contoh, pengguna ingin mengakses sebuah data pada *flash drive* tetapi pengguna secara tidak sengaja menghapus data yang dimiliki, padahal pengguna sangat membutuhkan data tersebut. Akibatnya pengguna tidak bisa mengakses data yang ada pada *flash drive* karena terhapus. Adapun kasus menghapus data dengan sengaja untuk menghilangkan bukti hukum. Meskipun begitu, perlu adanya penanganan agar data yang diperlukan kembali seperti semula.

Data yang terhapus atau sengaja terhapus, dapat dijadikan sebagai bukti digital pada persidangan. Ini berlandaskan pada UUD Republik Indonesia tahun 2016, pada pasal 5 ayat 1 yang berbunyi “Bahwa keberadaan informasi Elektronik dan /atau Dokumen Elektronik mengikat dan diakui sebagai alat bukti yang sah untuk memberikan kepastian hukum terhadap Penyelenggaraan Sistem Elektronik dan Transaksi Elektronik, terutama dalam pembuktian dan hal yang berkaitan dengan perbuatan hukum yang dilakukan melalui Sistem Elektronik”.

Dalam dunia digital forensik terdapat cara untuk mengembalikan data yaitu *recovery*. *Recovery* adalah proses pengembalian data yang telah terhapus dari *flash drive*. dengan metode ini, data yang terhapus dapat dikembalikan dan dapat dijadikan sebagai barang bukti dalam persidangan.

Dalam tugas akhir yang akan dilakukan oleh penulis, akan membahas tentang bagaimana data yang terhapus dapat dijadikan sebagai barang bukti dalam persidangan.

### 1.2 Identifikasi Masalah

Berdasarkan latar belakang yang telah dipaparkan sebelumnya, maka permasalahan yang timbul pada tugas akhir ini adalah bagaimana data yang terhapus dapat dijadikan sebagai bukti digital ?

### 1.3. Tujuan Tugas Akhir

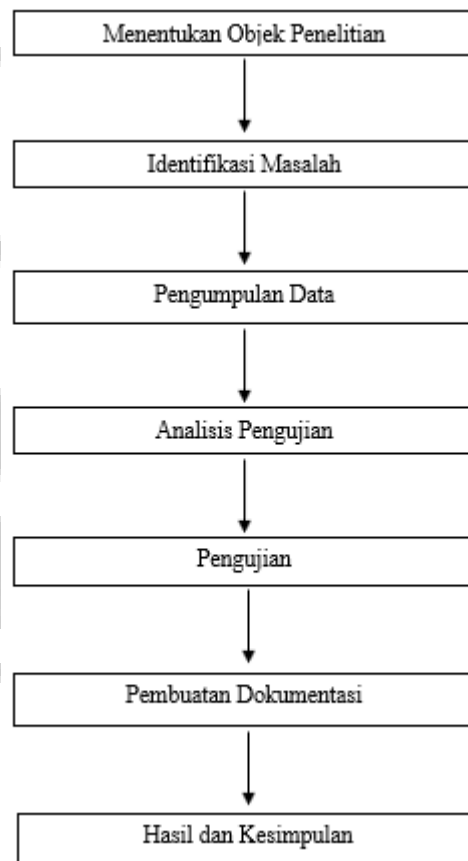
Tujuan tugas akhir ini adalah menjamin data yang terhapus sebagai bukti digital.

#### 1.4. Lingkup Tugas Akhir

Penyelesaian Tugas Akhir dibatasi sebagai berikut :

1. Menentukan karakteristik keaslian data yang dikembalikan sebagai bukti digital.
2. Data yang dikembalikan merupakan data yang berada pada *Flash Drive*.
3. Pengujian dilakukan menggunakan Software TestDisk.
4. Data yang dikembalikan akan dijadikan sebagai bukti digital yang mengacu pada UUD Republik Indonesia No. 19 Tahun 2016.

#### 1.5. Metodologi Pengerjaan Tugas Akhir



Gambar 1.1 Metode Penelitian

##### 1.5.1. Menentukan Objek Penelitian

Tahap ini menentukan objek yang akan diteliti saat melakukan penelitian.

##### 1.5.2. Identifikasi Masalah

Tahap ini setelah melakukan penentuan objek yang akan diteliti maka dilihat masalah yang terdapat dalam lingkup penelitian.

##### 1.5.3. Pengumpulan Data

Pengumpulan data dilakukan dengan cara melakukan tindakan pengambilan data pada *flash drive* melalui tahap *Disk Imaging*, yang kemudian akan diuji pada tahap pengujian.



#### 1.5.4. Analisis Pengujian

Tahap ini adalah analisis pengujian berdasarkan data yang telah dikumpulkan, analisis kebutuhan, ekstensi data, dan metode yang akan digunakan oleh penulis untuk diuji menggunakan kakas yang telah ditentukan.

#### 1.5.5. Pengujian

Tahap ini adalah pengujian data yang terhapus untuk mengetahui data yang terhapus sebagai barang bukti. Data yang terhapus juga akan diuji untuk mengetahui data yang terhapus dapat dijadikan sebagai bukti digital.

#### 1.5.6. Pembuatan dokumentasi

Tahap ini adalah pembuatan dokumentasi dari hasil pengujian yang telah dilakukan pada data yang dikembalikan

#### 1.5.7. Hasil dan Kesimpulan

Pada tahapan ini akan dirumuskan kesimpulan yang didapatkan berdasarkan hasil dari penerapan dan implementasi untuk mengembalikan data.

### 1.6. Sistematika Penulisan Tugas Akhir

Buku Tugas Akhir ditulis dengan mengikuti sistematika sebagai berikut :

#### **Bab 1 : Pendahuluan**

Pada bab ini berisi Latar belakang, Identifikasi Masalah, Tujuan Tugas Akhir, Lingkup Tugas Akhir, Metodologi Pengerjaan Tugas Akhir, dan Sistematika Tugas Akhir

#### **Bab 2 : Landasan Teori dan Penelitian Terdahulu**

Pada bab ini berisi Tinjauan pustaka atau Teori yang digunakan untuk membantu penyelesaian Tugas Akhir, Meliputi Komputer Forensik, Metode Komputer Forensik, Bukti Digital, *Recovery*, Keamanan Informasi, Aspek Hukum dari Komputer Forensik, Undang-Undang Republik Indonesia Nomor 19 Tahun 2016, Tools yang digunakan dan Penelitian Terdahulu.

#### **Bab 3 : Skema Penelitian**

Pada bab ini berisi kerangka tugas akhir berupa alur penyelesaian Tugas Akhir, dan Peta Analisis dan Solusi Tugas Akhir.

#### **Bab 4 : Analisis dan Pengujian**

Pada bab ini berisi tentang langkah-langkah analisis pengembalian data untuk mengetahui kebutuhan pengembalian data yang akan dilakukan. Pada bab ini juga menjelaskan tentang langkah-langkah pengujian pada studi kasus yang telah dianalisis untuk pengembalian data.



**Bab 5 : Hasil dan Kesimpulan**

Pada bab ini berisi tentang hasil dari pengembalian data, dan sebuah kesimpulan yang dapat diambil dari hasil penelitian.



## DAFTAR PUSTAKA

- [UUD16] Undang-Undang Republik Indonesia Nomor 19 Tahun 2016 Tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik, 2016
- [AND16] Andreas, Silalahi Vandi, Dr. Irawan Serimbing, ST., M.Kom., Analisis Digital Forensik Investigation pada Bukti Digital Steganography, 2016
- [EKO12] Eko Indjarti, Richardius, Forensik Komputer, 2012
- [VIL16] Vilda Rosalina, Andri Suhendarsah, M. Natsir, Analisis Data Recovery Menggunakan Software Forensik: Winhex and X-Ways Forensik, 2016
- [SAS09] Sanusi, Muzammil, Hard Disk, Teknologi, Troubleshooting, Data Recovery, 2009
- [HAR11] Hartono Anggit Dwi, Ema Utami, Hanifa Al Fatta, Penerapan Teknik Komputer Forensik untuk Pengembalian dan Penghapusan Berkas Digital
- [FAR] Farhat, ST., MMSI., MSC., Pengantar Forensik Teknologi Informasi “Tahapan Komputer Forensik
- [RIA18] Riadi, Imam, Rusydi Umar, Imam Mahfudl Nasrulloh, Analisis Forensik Digital pada Frozen Solid State Drive dengan Metode National Institute of Justice (NIJ), 2018
- [CAS11] Casey, Eoghan, Digital Evidence and Computer Crime, 2011
- [BIN15] Pengantar Keamanan Informasi, <https://mti.binus.ac.id/2015/04/02/pengantar-information-security/>, 2015
- [DOU01] Dougherty, James J., Computer Forensics, SANS Institute, 2001
- [DOL12] Dolphin data lab, Four phase Of Data Recovery, <https://www.dolphindatalab.com/the-four-phases-of-data-recovery/>, 2012
- [SID13] Sidik, Suryanto Dampak Undang-Undang Informasi dan Transaksi Elektronik (UUITE) Terhadap Perubahan Hukum dan Sosial Dalam Masyarakat, 2013
- [4N619] 4N6Labs, Karakteristik Barang Bukti Digital dan Jenis Data, <http://www.4n6labs.org/karakteristik-barang-bukti-forensics-digital-dan-jenis-data/>, 2019