

**Analisis Mobile Forensic Fitur Privacy pada Smartphone Android
Menggunakan Metode NIST (*National Institute of Standard and
Technology*)**

SKRIPSI

Program Studi S1 Teknik komputer



diajukan oleh

SITI ALFIANA

18.83.0229

Kepada

PROGRAM SARJANA

PROGRAM STUDI TEKNIK KOMPUTER

FAKULTAS ILMU KOMPUTER

UNIVERSITAS AMIKOM YOGYAKARTA

YOGYAKARTA

2022

**Analisis Mobile Forensic Fitur Privacy pada Smartphone Android
Menggunakan Metode NIST (*National Institute of Standard and
Technology*)**

SKRIPSI

untuk memenuhi salah satu syarat mencapai derajat Sarjana
Program Studi Teknik Komputer



diajukan oleh
SITI ALFIANA
18.83.0229

Kepada
PROGRAM SARJANA
PROGRAM STUDI TEKNIK KOMPUTER
FAKULTAS ILMU KOMPUTER
UNIVERSITAS AMIKOM YOGYAKARTA
YOGYAKARTA
2022

HALAMAN PERSETUJUAN

SKRIPSI

**Analisis Mobile Forensic Fitur Privacy pada Smartphone Android
Menggunakan Metode NIST (*National Institute of Standard and
Technology*)**

yang disusun dan diajukan oleh

Siti Alfiana

18.83.0229

telah disetujui oleh Dosen Pembimbing Skripsi
pada tanggal 21 Juli 2022

Dosen Pembimbing,

ii

Banu Santoso, S.T.,M.Eng

NIK. 190302327

HALAMAN PENGESAHAN

SKRIPSI

**Analisis Mobile Forensic Fitur Privacy pada Smartphone Android
Menggunakan Metode NIST (*National Institute of Standard and
Technology*)**

yang disusun dan diajukan oleh

Siti Alfiana

18.83.0229

Telah dipertahankan di depan Dewan Penguji
pada tanggal 21 Juli 2022

Susunan Dewan Penguji

Nama Penguji

Tanda Tangan

Rini Indrayani, ST, M.Eng
NIK. 190302417

Lukman, M.Kom
NIK. 190302xxx

Banu Santoso, S.T., M.Eng
NIK. 190302327

Skripsi ini telah diterima sebagai salah satu persyaratan
untuk memperoleh gelar Sarjana Komputer
Tanggal 21 Juli 2022

DEKAN FAKULTAS ILMU KOMPUTER

Hanif Al Fatta, S.Kom., M.Kom.
NIK. 19030209

HALAMAN PERNYATAAN KEASLIAN SKRIPSI

Yang bertandatangan di bawah ini,

Nama mahasiswa : Siti Affiana
NIM : 18.83.0229

Menyatakan bahwa Skripsi dengan judul berikut:

Analisis Mobile Forensic Fitur Privacy pada Smartphone Android Menggunakan Metode NIST (National Institute of Standard and Technology)

Dosen Pembimbing : Bani Sartoso, S.T., M.Eng.

1. Karya tulis ini adalah benar-benar ASLI dan BELUM PERNAM diajukan untuk mendapatkan gelar akademik, baik di Universitas AMIKOM Yogyakarta maupun di Perguruan Tinggi lainnya.
2. Karya tulis ini merupakan gagasan, rancangan dan penulisan SAYA sendiri, tanpa bantuan pihak lain kecuali arahan dari Dosen Pembimbing.
3. Dalam karya tulis ini tidak terdapat karya atau pendapat orang lain, kecuali secara tertulis dengan jelas dicantumkan sebagai acuan dalam naskah dengan disebutkan nama pengarang dan disebutkan dalam Daftar Pustaka pada karya tulis ini.
4. Perangkat lunak yang digunakan dalam penelitian ini sepenuhnya menjadi tanggung jawab SAYA, bukan tanggung jawab Universitas AMIKOM Yogyakarta.
5. Pernyataan ini SAYA buat dengan sesungguhnya, apabila di kemudian hari terdapat penyimpangan dan ketidakbenaran dalam pernyataan ini, maka SAYA bersedia menerima SANKSI AKADEMIK dengan pencabutan gelar yang sudah diperoleh, serta sanksi lainnya sesuai dengan norma yang berlaku di Perguruan Tinggi.

Yogyakarta, 21 Juli 2022.

Yang Menyatakan,



Siti Affiana

HALAMAN PERSEMBAHAN

Segala puji bagi Allah SWT atas limpahan rahmat, hidayah dan karunia-Nya sehingga saya dapat menyelesaikan skripsi ini dengan lancar dan sebaik-baiknya. Skripsi ini saya persembahkan untuk :

1. Ibu saya tecinta Ibu Sarinten dan Bapak saya Partono keluarga saya tersayang yang selalu memberi support, selalu mendo'akan, memberika fasilitas yang saya butuhkan serta memberikan hasil kerja kersanya.
2. Bapak Banu Santoso, S.T., M.Eng selaku dosen pembimbing yang telah memberikan saya arahan serta bimbingan dalam menyelesaikan penyusunan Skripsi ini.
3. Kepada kerabat, semua teman dan sahabat yang selalu memberi support di saat saya berkeluh kesah dan membutuhkan.

KATA PENGANTAR

Puji dan syukur saya panjatkan kepada Tuhan Yang Maha Esa atas segala rahmat petunjuk serta pertolongan dan kekuatan yang di anugerahkan kepada penulis sehingga dapat menyelesaikan skripsi dengan judul “Analisis Mobile Forensic Fitur Privacy pada *Smartphone* Android Menggunakan Metode NIST (*National Institute of Standard and Technology*)”. Skripsi ini disusun sebagai syarat memperoleh gelar Sarjana Komputer pada program Studi S1 Teknik Komputer Fakultas Ilmu Komputer Universitas Amikom Yogyakarta.

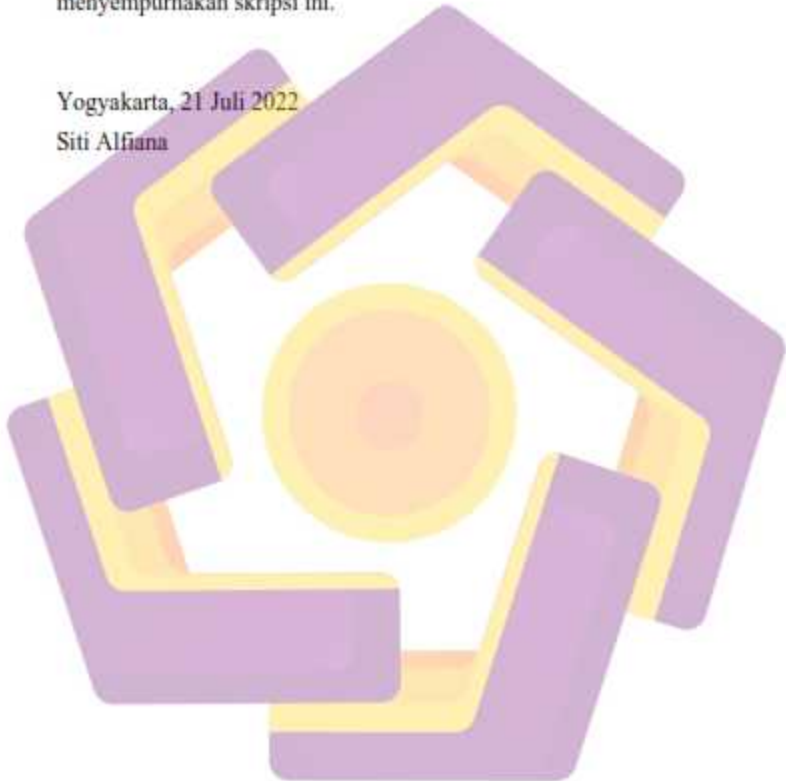
Di kesempatan ini penulis ingin menyampaikan banyak terimakasih kepada:

1. Allah SWT karena atas rahmat-Nya, sehingga penulis dapat menyelesaikan Skripsi ini dengan lancar dan dengan sebaik-baiknya dan semoga dapat bermanfaat di kemudian hari.
2. Bapak Prof. Dr. M. Suyanto, M.M. selaku Rektor Universitas AMIKOM Yogyakarta
3. Bapak Dony Ariyus, M.Kom. selaku Ketua Program Studi S1 Teknik Komputer Universitas AMIKOM Yogyakarta
4. Bapak Banu Santoso, S.T., M.Eng selaku dosen pembimbing yang telah memberikan saya arahan dan meluangkan waktu untuk membimbing dalam menyelesaikan penyusunan Skripsi ini.
5. Segenap Dosen, Staff, dan Karyawan Universitas AMIKOM Yogyakarta yang telah memberikan ilmu kepada penulis di bangku perkuliahan dan juga membantu penulis dalam kelancaran administrasi sampai terselesaikannya Skripsi ini.
6. Orang tua, kerabat beserta keluarga besar yang selalu senantiasa mendoakan dan memberikan support penuh kepada penulis.
7. Serta seluruh pihak yang telah membantu dalam menyelesaikan penyusunan skripsi terutama kakak tingkat saya Amru Rizal S.kom yang telah banyak memberi saran masukan untuk skripsi saya, dan semua teman sahabat saya yang tidak dapat penulis sebutkan satu per satu.

Dalam penyusunan skripsi ini penulis menyadari masih jauh dari kata sempurna karena terbatasnya pengalaman dan pengetahuan penulis, Penulis mengharapkan skripsi ini kedepannya akan memberikan manfaat kepada pihak yang membutuhkan serta menjadi acuan dalam penelitian kedepannya. Penulis juga mengharapkan saran, kritik serta masukan yang dapat membantu menyempurnakan skripsi ini.

Yogyakarta, 21 Juli 2022

Siti Alfiana

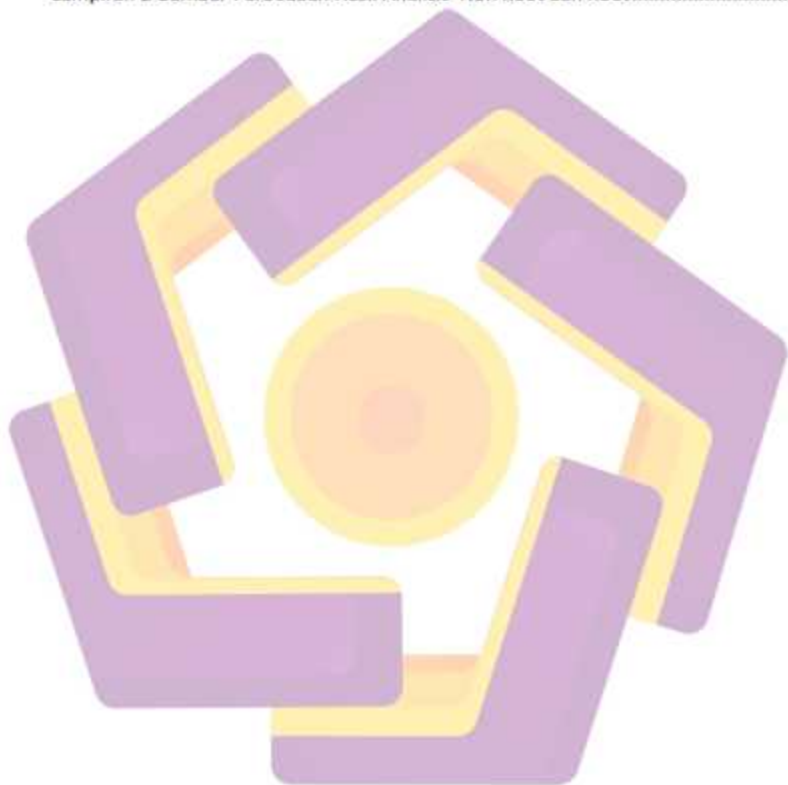


DAFTAR ISI

HALAMAN JUDUL.....	ii
HALAMAN PERSETUJUAN.....	iii
HALAMAN PENGESAHAN.....	iv
HALAMAN PERNYATAAN KEASLIAN SKRIPSI.....	v
HALAMAN PERSEMBAHAN.....	vi
KATA PENGANTAR.....	vii
DAFTAR ISI.....	ix
DAFTAR TABEL.....	xii
DAFTAR GAMBAR.....	xiii
DAFTAR IAMPIRAN.....	xvi
DAFTAR LAMBANG DAN SINGKATAN.....	xvii
DAFTAR ISTILAH.....	xviii
INTISARI.....	xx
ABSTRACT.....	xxi
BAB I PENDAHULUAN.....	1
1.1 Latar Belakang Masalah.....	1
1.2 Rumusan Masalah.....	2
1.3 Tujuan Penelitian.....	2
1.4 Batasan Masalah.....	3
1.5 Manfaat Penelitian.....	3
BAB II TINJAUAN PUSTAKA.....	5
2.1 Tinjauan Pustaka.....	5
2.2 Forensik Digital.....	9
2.3 Bukti Digital.....	10
2.4 Mobile Forensik.....	10
2.5 <i>Smartphone</i> (Android).....	11
2.6 Fitur Privat (Brankas Pribadi).....	12
2.7 WhatsApp.....	12
2.8 Standar Operasional Prosedur (SOP).....	13
2.9 National Institute of Standards and Technology (NIST).....	13
2.10 MOBILedit.....	14

2.11	Autopsy	15
BAB III METODOLOGI PENELITIAN.....		16
3.1	Gambaran Umum Penelitian	16
3.2	Metode Penelitian.....	16
3.2.1	Collection.....	17
3.2.2	Examination.....	17
3.2.3	Analysis.....	18
3.2.4	Reporting.....	18
3.3	Alat dan Bahan Penelitian	19
3.4	Tahap Persiapan Penelitian	20
3.5	Skenario Kasus.....	21
3.5.1	Eksperimen Skenario Pertama (Android Xiaomi non root)	22
3.5.2	Eksperimen Skenario Kedua, (Android Xiaomi root)	22
3.6	Alur Penelitian.....	22
BAB IV HASIL DAN PEMBAHASAN		24
4.1	Persiapan.....	24
4.1.1	Instalasi Tools pada Perangkat Investigator (peneliti)	24
4.1.2	Kondisi Objek Penelitian.....	26
4.2	Skenario Penelitian.....	26
4.2.1	Implementasi Skenario Pertama (Android Xiaomi non Root)	27
4.2.2	Implementasi Skenario Kedua (Android Xiaomi Root).....	31
4.3	Collection	35
4.3.1	Pengambilan Data dari Android (Xiaomi) non root.....	36
4.3.2	Pengambilan Data dari Android (Xiaomi) Root.....	40
4.4	Examination (Pengujian)	44
4.4.1	Hasil Implementasi Skenario Android non Root	44
4.4.2	Hasil Implementasi Skenario Android Root	47
4.5	Analysis (analisis).....	52
4.5.1	Analisa Skenario Pertama (Android Xiaomi non Root).....	52
4.5.2	Analisa Skenario Kedua (Android Xiaomi Root)	53
4.6	Reporting (Laporan akhir investigasi).....	55
4.6.1	Hasil kompirasi Android Xiaomi (Non root) dan Android Xiaomi (Root).....	55
BAB V KESIMPULAN DAN SARAN		59

5.1 Kesimpulan.....	59
5.2 Saran	59
DAFTAR PUSTAKA	61
LAMPIRAN.....	63
Lampiran 1 Gambar Perbedaan Hasil Imaging Android non Root dan Android Root ...	63
Lampiran 2 Gambar Perbedaan Hasil Analisis Non Root dan Root.....	64



DAFTAR TABEL

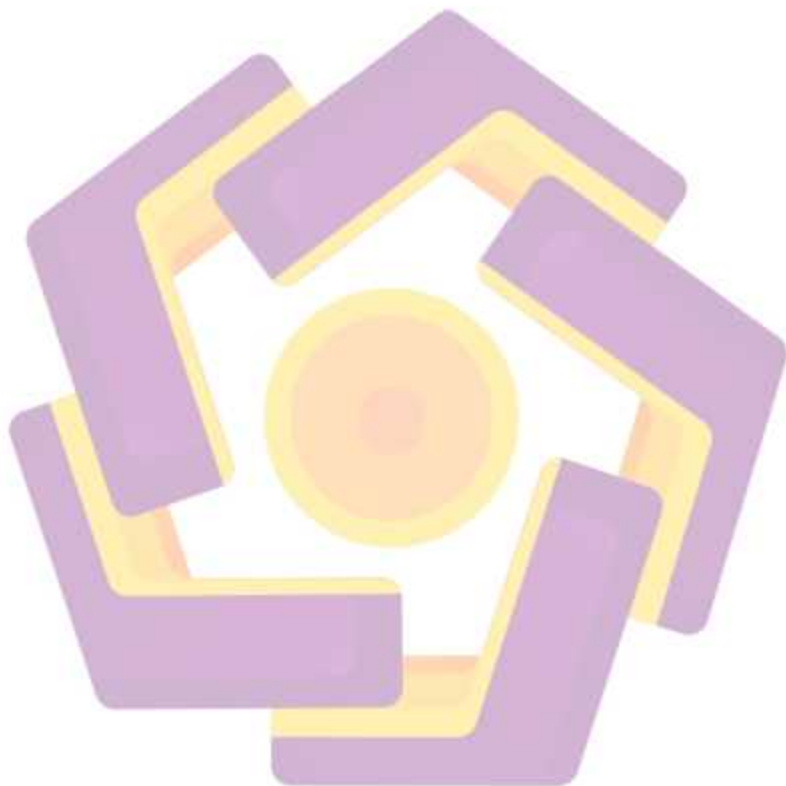
Tabel 2.1 Tinjauan Pustaka dan Penelitian Terdahulu.....	7
Tabel 3.1 Alat dan bahan penelitian.....	19
Tabel 4.1 Identitas Digital Evidence.....	26
Tabel 4.2 skenario yang digunakan.....	27
Tabel 4.3 Hasil Analisa Smartphone Android Xiaomi non Root	53
Tabel 4.4 Bukti Pendapatan Artefak lain selain Keempat File	53
Tabel 4.5 Hasil Analisis File Akuisisi Xiaomi Root yang Ditemukan	54
Tabel 4.6 Validasi Nilai Hash Hasil Akuisisi	54
Tabel 4.7 Bukti Log Aktivitas Private File yang Ditemukan	54
Tabel 4.8 Komparasi Hasil Analisis Rooted dan Non Rooted.....	56
Tabel 4.9 Persentase Perolehan Barang Bukti per File.....	56
Tabel 4.10 Persentase Perolehan Barang Bukti Digital Keseluruhan.....	57

DAFTAR GAMBAR

Gambar 2.1 Gambar Mobile Forensik Menggunakan Laptop	11
Gambar 2.2 Alur Kerangka Kerja NIST	14
Gambar 2.3 Dashboard Aplikasi Mobiledit	14
Gambar 2.4 Dashboard Aplikasi Autopsy	15
Gambar 3.1 Tahapan Metode National Institute of Standards and Technology	17
Gambar 3.2 Spesifikasi Smartphone Android yang Digunakan	20
Gambar 3.3 Tahapan Persiapan Penelitian	21
Gambar 3.4 Skenario private video pada Xiaomi non Root	22
Gambar 3.5 Skenario private video pada android Xiaomi	22
Gambar 3.6 Alur Penelitian	23
Gambar 4.1 Instalasi Tool MOBILedit pada Perangkat Penyelidik	25
Gambar 4.2 Proses Instalasi Autopsy	25
Gambar 4.3 Root pada Smartphone Android Xiaomi	26
Gambar 4.4 Penerimaan File dari WhatsApp	28
Gambar 4.5 Private File Video	28
Gambar 4.6 Private File Gambar	29
Gambar 4.7 Private File Dokumen	29
Gambar 4.8 Private File Musik	30
Gambar 4.9 File Tersimpan di Brankas Pribadi	30
Gambar 4.10 Memerlukan Kata Sandi atau Sidik Jari untuk Dapat Masuk	31
Gambar 4.11 Penerimaan File dari WhatsApp	32
Gambar 4.12 Penyembunyian File Video	32
Gambar 4.13 Penyembunyian File Gambar	33
Gambar 4.14 Penyembunyian File Dokumen	33
Gambar 4.15 Penyembunyian File Musik	34
Gambar 4.16 File Berhasi Diatur Private (tersembunyi)	34
Gambar 4.17 Harus Memasukan Kata Sandi untuk Dapat Masuk	35
Gambar 4.18 Proses pengambilan Data dari Android	36
Gambar 4.19 Pemilihan Tipe Smartphone	36

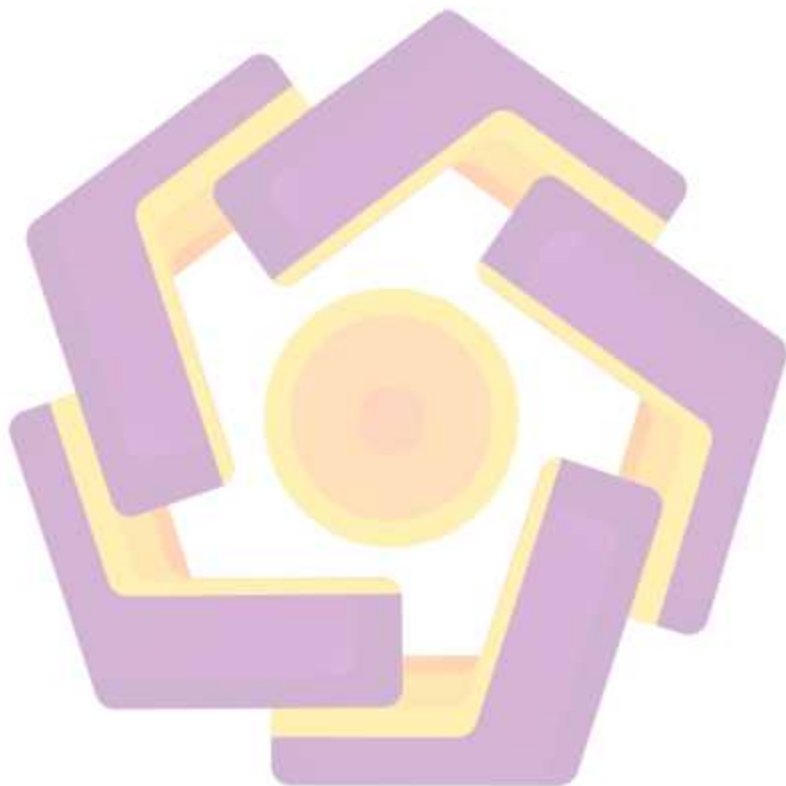
Gambar 4.20 Pemilihan tipe connection.....	37
Gambar 4.21 Petunjuk Pengaktifan Usb Debug	37
Gambar 4.22 Pengaturan Usb Debug.....	38
Gambar 4.23 Perangkat Berhasil Terkoneksi	38
Gambar 4.24 adalah Proses pada Saat Scan Smartphone Android Berlangsung...39	39
Gambar 4.25 Lokasi dari File yang Dilakukan Private.....	39
Gambar 4.26 Lokasi Folder yang Dilakukan Akuisisi.....	40
Gambar 4.27 Lokasi Folder yang Dilakukan Akuisisi.....	40
Gambar 4.28 Hasil Akuisisi.....	40
Gambar 4.29 Smartphone Android Xiaomi Berhasil Terdeteksi	41
Gambar 4.30 Data yang Berhasil Terdeteksi	41
Gambar 4.31 Data Cache yang Berhasil Terdeteksi	42
Gambar 4.32 Lokasi dari File yang Dilakukan Private.....	42
Gambar 4.33 Lokasi Aktifitas Private File yang Ditemukan.....	43
Gambar 4.34 Lokasi Keempat File yang Ditemukan.....	43
Gambar 4.35 File Akuisisi yang Didapatkan	43
Gambar 4.36 Analisis Akuisisi Menggunakan Autopsy	44
Gambar 4.37 File Private Music tidak Ditemukan	45
Gambar 4.38 File Private Dokumen tidak Ditemukan.....	45
Gambar 4.39 File Private Gambar tidak Ditemukan.....	46
Gambar 4.40 File Private Video tidak Ditemukan.....	46
Gambar 4.41 Log Aktivitas Privat File Tidak Terdeteksi.....	47
Gambar 4.42 Analisis Hasil Akuisisi Menggunakan Autopsy	47
Gambar 4.43 File Musik dapat Ditemukan.....	48
Gambar 4.44 File Gambar dapat Ditemukan	48
Gambar 4.45 File Video dapat Ditemukan	49
Gambar 4.46 File Dokumen dapat Ditemukan	49
Gambar 4.47 Log Aktivitas Private File Terdeteksi	50
Gambar 4.48 Hasil Akuisisi Pengujian ke Dua	50
Gambar 4.49 File Musik berhasil Terdeteksi.....	50
Gambar 4.50 File Dokumen Berhasil Terdeteksi.....	51

Gambar 4.51 File gambar Berhasil Terdeteksi	51
Gambar 4.52 File Video Berhasil terdeteksi.....	52
Gambar 4.53 log Aktivitas Hiden Bertambah menjadi 8 File.....	52
Gambar 4.54 Persentase Perolehan Barang Bukti Digital per File	57



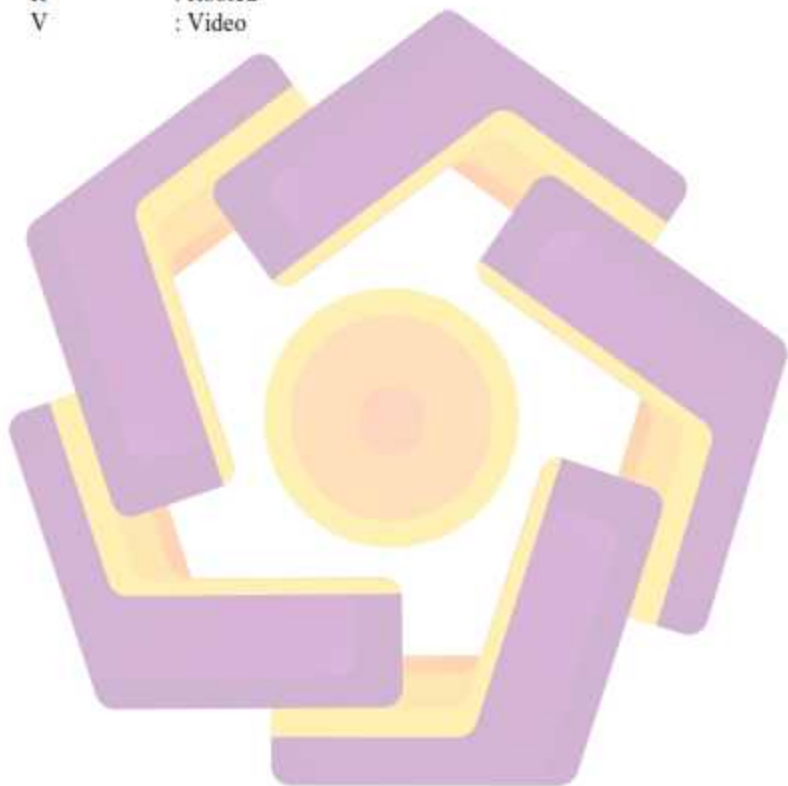
DAFTAR LAMPIRAN

- Lampiran 1. Gambar Perbedaan Hasil Imaging Android Non Root dan Root.....63
Lampiran 2. Gambar perbedaan Hasil Akuisis Non Root dan Root..... 64



DAFTAR LAMBANG DAN SINGKATAN

D	: Dokumen
G	: Gambar
M	: Musik
NR	: Non Rooted
R	: Rooted
V	: Video



DAFTAR ISTILAH

- Akuisasi : Proses pengambilan data dari barang bukti pelaku pada proses investigasi atau forensik untuk dilakukan analisis.
- Analisis : Kegiatan mengamati sebuah objek untuk menemukan kesimpulan
- Artefak : Sebuah barang bukti digital yang dicari
- Cache : Sebuah riwayat pada browser atau aplikasi yang digunakan untuk menyimpan informasi.
- Databases : Sebuah kumpulan data atau informasi yang tersimpan secara sistematis.
- Device : Perangkat pada sebuah teknologi yang digunakan untuk melakukan penyimpanan.
- Ekstraksi : Proses mengambil sebuah data dari sumber data agar dapat dibuka dan dilihat isinya di dalamnya.
- Hidden : Aktivitas untuk melakukan penyembunyian file agar file tersebut tidak dapat ditemukan atau ditampilkan pada default sistem
- History : Sebuah riwayat di masa lampau atau masa terdahulu yang pernah dilakukan.
- Identifikasi : Melakukan sebuah pencarian, mencari, mengumpulkan, meneliti, mencatat sebuah data yang dibutuhkan saat di lapangan.
- Imaging : Proses mencari atau memindai data untuk menemukan sebuah file atau barang bukti pada proses investigasi.
- Investigasi : Upaya untuk melakukan sebuah penyelidikan, penelitian, pencarian pemeriksaan dan pengumpulan informasi untuk mendapatkan sebuah data.
- Platform : Sebuah kombinasi antara sebuah perangkat lunak dan keras yang gunanya sebagai wadah atau tempat untuk memfasilitasi agar dapat bertukar informasi.

- Private : Adalah menyembunyikan atau tidak melakukan publikasi yang dilakukan agar orang lain tidak mengetahuinya dan hanya diri kita sendiri yang tau.
- Recovery : Sebuah tindakan mengembalikan file atau data yang terhapus, hilang, rusak, atau di keformat dari penyimpanan utama.
- Root : Kegiatan melakukan perizinan menggunakan aplikasi pihak ketiga pada ponsel pintar yang fungsinya adalah untuk mendapatkan kontrol yang lebih tinggi.



INTISARI

Pada era saat ini kemajuan dan perkembangan teknologi sangat cepat, diantaranya adalah teknologi ponsel salah satunya *smartphone* yang bertipe Android. *Smartphone* saat ini seperti sudah menjadi kebutuhan, kepentingan kita sehari-hari. *Smartphone* mempunyai banyak sekali *type*, merk dan tentunya dengan kapasitas dan fitur-fitur yang cukup memadai. Di dalam fitur terbaru *Smartphone* terdapat satu fitur penyembunyian file yaitu fitur privat yang tidak bisa di akses oleh sembarang orang dan di perlukan kata sandi atau sidik jari untuk dapat mengaksesnya. Implementasi kasusnya adalah penyembunyian sebuah file bukti digital dari Whatsapp yang berupa file video, audio, gambar, dan dokumen di fitur privat *smartphone* android Xiaomi (non root) android Xiaomi (root) yang akan dilakukan akuisisi menggunakan tools mobile forensic yaitu MOBILedit forensic menggunakan metode NIST (*National Institute of Standard and Technology*) yang mempunyai 4 tahapan *collection, examination, analysis dan reporting*. Hasil dari akuisisi *smartphone* android Xiaomi non root dan Xiaomi root dilakukan analisis menggunakan tools Autopsy. Dengan metode NIST di dapatkan sebuah data yang dapat dilakukan analisis yang memungkinkan didapatkan file tersembunyi tersebut, Presentase yang di dapatkan dari hasil analisis yang dilakukan pada akuisisi *smartphone* Android Xiaomi (non root) file privat 0 % atau tidak dapat ditemukan, sedangkan pada *smartphone* android Xiaomi (root) 100% dapat ditemukan yaitu file video dan file gambar, file dokumen, dan file musik. temuan ini dapat dijadikan sebagai barang bukti digital di tindak kejahatan yang memanfaatkan fitur privat pada fasilitas *smartphone* Android.

Kata kunci: Mobile Forensic, File Privat, Android, NIST

ABSTRACT

In the current era, technological progress and development is very fast, including mobile phone technology, one of which is an Android-type smartphone. Smartphones nowadays have become a necessity, our daily interests. Smartphones have various types, brands and of course with sufficient capacity and features. In the latest Smartphone features there is one file hiding feature, namely a private feature that cannot be accessed by just anyone and a password or fingerprint is required to access it. The implementation of the case is the hiding of a digital evidence file from Whatsapp in the form of video, audio, and video files, images, and documents on the private Xiaomi android smartphone feature (non-root) Xiaomi android (root) which will be acquired using mobile forensic tools, namely MOBILedit forensics using the NIST (National Institute of Standard and Technology) method which has 4 stages of collection, examination, analysis and reporting. The results of the acquisition of non-rooted and rooted Xiaomi android smartphones were analyzed using Autopsy tools. With the NIST method, we get a data that can be analyzed which allows the hidden file to be obtained, the percentage obtained from the results of the analysis carried out on the acquisition of Xiaomi Android smartphones (non root) private files are 0% or cannot be found, while on Xiaomi Android smartphones (root) 100% can be found i.e. video files and image files, document files; and music files. These findings can be used as digital evidence in crimes that use private features on Android smartphone facilities.

Keywords: *Mobile Forensic, Private Files, Android, NIST*