

**PERBANDINGAN HASIL TOOL FORENSIK PADA FILE
SMARTPHONE ANDROID BACKUP DENGAN MENGGUNAKAN
METODE NIST**

SKRIPSI

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



diajukan oleh

PERMANA BANGUN PANGESTU

18.83.0329

Kepada

**PROGRAM SARJANA
PROGRAM STUDI TEKNIK KOMPUTER
FAKULTAS ILMU KOMPUTER
UNIVERSITAS AMIKOM YOGYAKARTA
YOGYAKARTA**

2022

**PERBANDINGAN HASIL TOOL FORENSIK PADA FILE
SMARTPHONE ANDROID BACKUP DENGAN MENGGUNAKAN
METODE NIST**

SKRIPSI

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



diajukan oleh

PERMANA BANGUN PANGESTU

18.83.0329

Kepada

**PROGRAM SARJANA
PROGRAM STUDI TEKNIK KOMPUTER
FAKULTAS ILMU KOMPUTER
UNIVERSITAS AMIKOM YOGYAKARTA
YOGYAKARTA**

HALAMAN PERSETUJUAN

SKRIPSI

**PERBANDINGAN HASIL TOOL FORENSIK PADA FILE SMARTPHONE
ANDROID BACKUP DENGAN MENGGUNAKAN METODE NIST**

yang disusun dan diajukan oleh

Permana Bangun Pangestu

18.83.0329

telah disetujui oleh Dosen Pembimbing Skripsi
pada tanggal 28 Maret 2022

Dosen Pembimbing,

Muhammad Kopravi, S.Kom., M.Eng

NIK. 190302454

HALAMAN PENGESAHAN
SKRIPSI

PERBANDINGAN HASIL TOOL FORENSIK PADA FILE SMARTPHONE
ANDROID BACKUP DENGAN MENGGUNAKAN METODE NIST

yang disusun dan diajukan oleh

Permana Bangun Pangestu

18.83.0329

Telah dipertahankan di depan Dewan Penguji
pada tanggal 21 Juli 2022

Susunan Dewan Penguji

Nama Penguji

Tanda Tangan

Senle Destya, M.Kom

NIK. 190302312

Andika Agus Slameto, M.Kom

NIK. 190302109

Muhammad Koprwl, S.Kom., M.Eng

NIK. 190302454

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. 190302096

HALAMAN PERNYATAAN KEASLIAN SKRIPSI

Yang bertandatangan di bawah ini,

Nama mahasiswa : Permana Bangun Pangestu
NIM : 18.83.0329

Menyatakan bahwa Skripsi dengan judul berikut:

PERBANDINGAN HASIL TOOL FORENSIK PADA FILE SMARTPHONE ANDROID BACKUP DENGAN MENGGUNAKAN METODE NIST

Dosen Pembimbing : Muhammad Kopravi, S.Kom., M.Eng

1. Karya tulis ini adalah benar-benar ASLI dan BELUM PERNAH diajukan untuk mendapatkan gelar akademik, baik di Universitas AMIKOM Yogyakarta maupun di Perguruan Tinggi lainnya.
2. Karya tulis ini merupakan gagasan, rumusan dan penelitian 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,



Permana Bangun Pangestu

HALAMAN PERSEMBAHAN

Bismillahirrahmanirrahim. Alhamdulillah hirabbil'amin, puji syukur saya panjatkan kepada Allah SWT, yang telah memberikan segala nikmat, karunia, kesehatan, petunjuk, kekuatan, dan perlindungan sehingga saya bisa menyelesaikan skripsi ini. Dengan rasa bangga dan bahagia, skripsi ini saya persembahkan kepada orang-orang yang selama ini telah mendukung, memberikan semangat dan motivasi dalam menyelesaikan pendidikan sarjana komputer saya ini, secara khusus kepada:

1. Bapak saya Sarengat, Ibu saya Pendah Saumi beserta keluarga besar saya yang selalu memotivasi, dan mendukung secara moril, material dan senantiasa sabar menasehati dan menyemangati saya.
2. Teman-teman lainnya yang selalu memberikan dukungan.
3. Semua orang yang telah membantu dan selalu memberikan saya motivasi untuk menyelesaikan skripsi ini.

KATA PENGANTAR

Assalamual'aikum Warahmatullahi Wabarakatuh

Syukur Alhamdulillah, penulis panjatkan syukur kepada Allah SWT atas limpah dan karunia yang diberikan kepada penulis sehingga dapat menyelesaikan laporan skripsi dengan judul "Perbandingan Hasil Tool Forensik Pada File Smartphone Android Backup Dengan Menggunakan Metode NIST".

Penulisan skripsi ini merupakan salah satu syarat untuk mendapatkan gelar sarjana pada jurusan Teknik Komputer di Falkutas Ilmu Komputer, Universitas Amikom Yogyakarta. Segala usaha telah dilakukan untuk menyempurnakan skripsi ini. Namun, penulis menyadari dalam penulisan skripsi ini masih banyak ditemukan kekurangan dan kekhilafan. Maka dari itu kritik dan saran diharapkan penulis yang dapat menjadikan masukan guna perbaikan di masa yang akan datang sehingga skripsi ini dapat dikembangkan lebih lanjut.

Dalam menyusun laporan skripsi ini penulis menyadari adanya bantuan, bimbingan, doa serta nasihat dari berbagai pihak. Oleh karena itu dengan kesempatan ini izinkan penulis dengan rasa syukur dan kerendahan hati mengucapkan terimakasih kepada beberapa pihak:

1. Bapak Prof. Dr. M. Suyanto, MM., selaku Rektor Universitas Amikom Yogyakarta
2. Bapak Hanif Al Fatta, S.Kom., M.Kom, selaku Dekan Falkutas Ilmu Komputer Universitas Amikom Yogyakarta
3. Bapak Dony Ariyus, M.Kom, selaku Ketua Program Studi Teknik Komputer Universitas Amikom Yogyakarta
4. Bapak Muhammad Kopravi, S.Kom., M.Eng, selaku Dosen Pembimbing Skripsi yang telah meluangkan waktunya dalam memberikan saran selama proses bimbingan.
5. Serta semua pihak yang tidak dapat disebutkan satu per satu, yang telah banyak memberikan dukungan, motivasi, inspirasi dan membantu dalam proses menyelesaikan skripsi ini.

Semoga semua dukungan, bantuan dan bimbingan yang diberikan kepada penulis mendapat balasan dari Allah SWT. Akhir kata penulis mengucapkan terima kasih, semoga penyusunan skripsi ini dapat memberikan inspirasi maupun manfaat bagi pembaca, khususnya bagi mahasiswa/mahasiswi Universitas Amikom Yogyakarta.

Wassalamu'alaikum Warahmatullahi Wabarakatuh

Yogyakarta, 23 April 2022

Penulis



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 LAMBANG DAN SINGKATAN	xvi
DAFTAR ISTILAH	xvii
INTISARI	xviii
Abstract	xix
BAB I PENDAHULUAN	1
1.1 Latar Belakang Masalah	1
1.2 Perumusan masalah	3
1.3 Tujuan Penelitian	4
1.4 Batasan Masalah	4
1.5 Manfaat Penelitian	4
1.6 Sistematika penulisan	4
BAB II TINJAUAN PUSTAKA	6
2.1 <i>Literature Review</i>	6
2.2 Landasan Teori	10

2.2.1	Digital Forensik	10
2.2.2	<i>Mobile Forensic</i>	11
2.2.3	Smartphone	11
2.2.3.1	Android	11
2.2.4	Bukti Digital	12
2.2.5	MOBILedit	12
2.2.6	Magnet AXIOM	13
2.2.7	Oxygen Forensic	13
2.2.8	Belkasoft Evidence Center	13
2.2.9	Android Backup	14
2.2.10	<i>National Institute of Standards and Technology (NIST)</i>	14
BAB III METODOLOGI PENELITIAN		16
3.1	Alat dan Bahan	16
3.2	Langkah Penelitian	16
3.2.1	Perumusan masalah	17
3.2.2	Persiapan Penelitian	17
3.2.2.1	Persiapan Alat dan Bahan	17
3.2.2.2	Studi Literatur	18
3.2.2.3	Penyusunan dan Implementasi Skenario	18
3.2.3	Analisis <i>Mobile Forensik</i>	20
3.2.3.1	<i>Collection</i>	21
3.2.3.2	<i>Examination</i>	21
3.2.3.3	<i>Analysis</i>	21
3.2.3.4	<i>Reporting</i>	21
BAB IV HASIL DAN PEMBAHASAN		23

4.1	Implementasi	23
4.1.1	<i>Collection</i> (Pengumpulan)	23
4.1.2	<i>Examination</i> (Pemeriksaan)	25
4.1.2.1	Magnet AXIOM	25
4.1.2.2	Oxygen Forensic	29
4.1.2.3	Belkasoft Evidence Center	31
4.2	Pengujian	35
4.2.1	Analysis	35
4.2.1.1	Magnet AXIOM	36
4.2.1.2	Oxygen Forensic	40
4.2.1.3	Belkasoft Evidence Center	43
4.2.2	Reporting	47
BAB V KESIMPULAN DAN SARAN		51
5.1	Kesimpulan	51
5.2	Saran	51
DAFTAR PUSTAKA		52

DAFTAR TABEL

Tabel 2. 1 Penelitian Terdahulu	6
Tabel 3. 1 Alat Dan Bahan Penelitian	16
Tabel 3. 2 Parameter Kinerja <i>Tools</i>	18
Tabel 4. 1 Perbandingan Ekstraksi <i>Tools</i> Magnet AXIOM, Oxygen Forensic, dan Belkasoft Evidence Center	35
Tabel 4. 2 Perbandingan Hasil Parameter	49

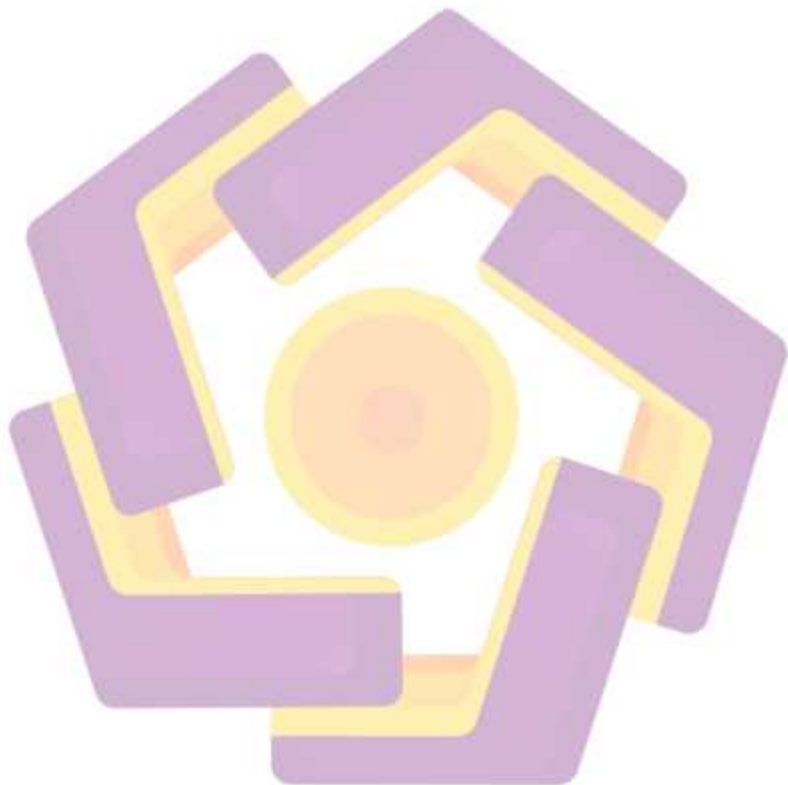


DAFTAR GAMBAR

Gambar 2. 1 Tahapan Metode NIST <i>Mobile Forensic</i>	14
Gambar 3. 1 Langkah Penelitian	17
Gambar 3. 2 Proses Menggunakan Metode NIST	22
Gambar 4. 1 Spesifikasi Smartphone Yang Digunakan Dalam Penelitian	23
Gambar 4. 2 Tampilan Fitur MOBILedit Enterprise	24
Gambar 4. 3 <i>File Android Backup</i> Hasil <i>Imaging</i>	25
Gambar 4. 4 Tampilan Detail Kasus Pada Magnet AXIOM	25
Gambar 4. 5 Memilih <i>File</i> Dan Folder Yang Akan Diekstraksi Pada Magnet AXIOM	26
Gambar 4. 6 Memilih <i>Mobile</i> Artefak Pada Magnet AXIOM	27
Gambar 4. 7 Proses Ekstraksi Dengan <i>Tool</i> Magnet AXIOM	27
Gambar 4. 8 Waktu Proses Ekstraksi Pada Magnet AXIOM	28
Gambar 4. 9 Hasil Ekstraksi <i>File Android Backup</i> Dengan Magnet AXIOM	28
Gambar 4. 10 Tampilan Awal Pada Oxygen Forensic	29
Gambar 4. 11 Memilih <i>Import Backup</i> Pada Oxygen Forensic	29
Gambar 4. 12 Proses Ekstraksi Dengan <i>Tool</i> Oxygen Forensic	30
Gambar 4. 13 Waktu Proses Ekstraksi Pada Oxygen Forensic	30
Gambar 4. 14 Hasil Ekstraksi <i>File Android Backup</i> Dengan Oxygen Forensic	30
Gambar 4. 15 Direktori Penyimpanan Kasus Pada Belkasoft Evidence Center	31
Gambar 4. 16 Memilih Data Hasil <i>Imaging</i> Untuk Diekstraksi Pada Belkasoft Evidence Center	31
Gambar 4. 17 Memilih Jenis <i>Type</i> Data Sebelum Proses Ekstraksi Pada Belkasoft Evidence Center	32
Gambar 4. 18 Proses Ekstraksi Dengan <i>Tool</i> Belkasoft Evidence Center	32
Gambar 4. 19 Waktu Serta Proses Yang Gagal dan <i>Error</i> Dalam Ekstraksi Data 33	
Gambar 4. 20 Hasil Ekstraksi <i>File Android Backup</i> Dengan Belkasoft Evidence Center	33
Gambar 4. 21 Waktu Proses Ekstraksi <i>Mobile Forensic</i>	34
Gambar 4. 22 Jumlah Artefak Yang Ditemukan	34

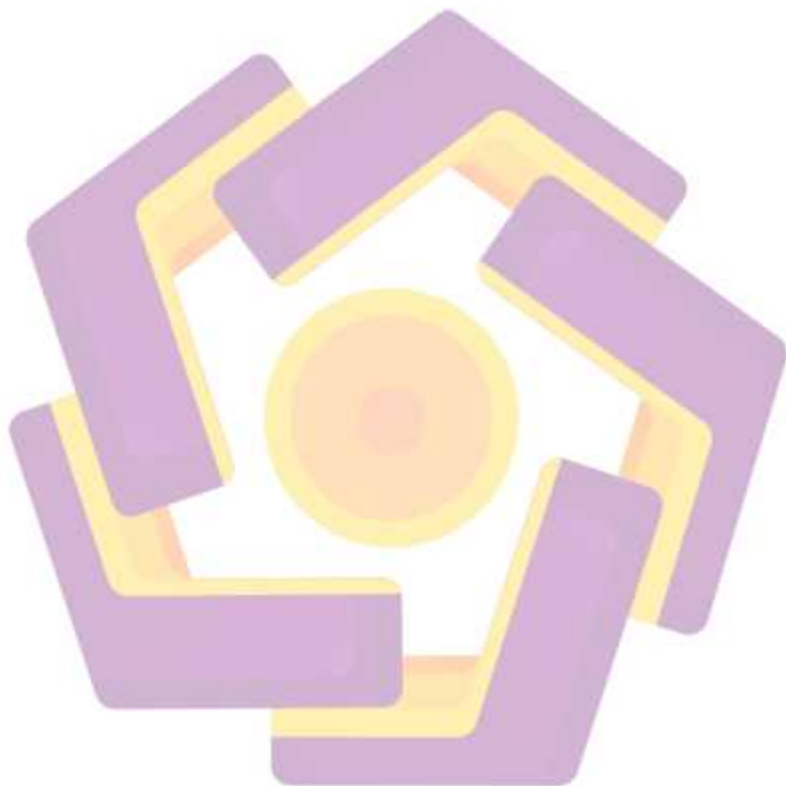
Gambar 4. 23 <i>Tool Magnet AXIOM Menampilkan Data Pendukung Artifact</i>	36
Gambar 4. 24 <i>Magnet AXIOM Dapat Menggabungkan Text Dengan Benar</i>	36
Gambar 4. 25 <i>Magnet AXIOM Tidak Memodifikasi Image File Dan Dapat Menampilkan Pesan</i>	37
Gambar 4. 26 <i>Magnet AXIOM Dapat Menampilkan PIM</i>	37
Gambar 4. 27 <i>Magnet AXIOM Dapat Menampilkan Audio, Dokumen, Gambar dan Video</i>	38
Gambar 4. 28 <i>Magnet AXIOM Dapat Menampilkan History Dan Bookmarks, Serta Geo-Location</i>	38
Gambar 4. 29 <i>Magnet AXIOM Dapat Menampilkan Data Email</i>	39
Gambar 4. 30 <i>Magnet AXIOM Dapat Menampilkan Data Aplikasi Media Sosial</i>	39
Gambar 4. 31 <i>Oxygen Forensic Dapat Mengekstraksi Data Pendukung Artifact</i>	40
Gambar 4. 32 <i>Oxygen Forensic Tidak Memodifikasi Image File Dan Dapat Menampilkan PIM</i>	40
Gambar 4. 33 <i>Oxygen Forensic Dapat Menampilkan Audio, Dokumen, Gambar dan Video</i>	41
Gambar 4. 34 <i>Oxygen Forensic Dapat Menampilkan History dan Bookmarks</i>	41
Gambar 4. 35 <i>Oxygen Forensic Dapat Menampilkan Email</i>	42
Gambar 4. 36 <i>Oxygen Forensic Dapat Menampilkan Geo-Location</i>	42
Gambar 4. 37 <i>Belkasoft Evidence Center Dapat Mengekstraksi Data Pendukung Artifact</i>	43
Gambar 4. 38 <i>Belkasoft Evidence Center Dapat Menggabungkan Text Dengan Benar</i>	43
Gambar 4. 39 <i>Belkasoft Evidence Center Tidak Memodifikasi Image File Dan Dapat Menampilkan Pesan</i>	44
Gambar 4. 40 <i>Belkasoft Evidence Center Dapat Menampilkan PIM</i>	44
Gambar 4. 41 <i>Belkasoft Evidence Center Dapat Menampilkan Audio, Dokumen, Gambar Dan Video</i>	45
Gambar 4. 42 <i>Belkasoft Evidence Center Dapat Menampilkan History Dan Bookmarks</i>	45

Gambar 4. 43 Belkasoft Evidence Center Dapat Menampilkan Email	46
Gambar 4. 44 Belkasoft Evidence Center Dapat Menampilkan <i>Geo-Location</i>	46
Gambar 4. 45 Hasil Kinerja <i>Tools Forensic</i>	47



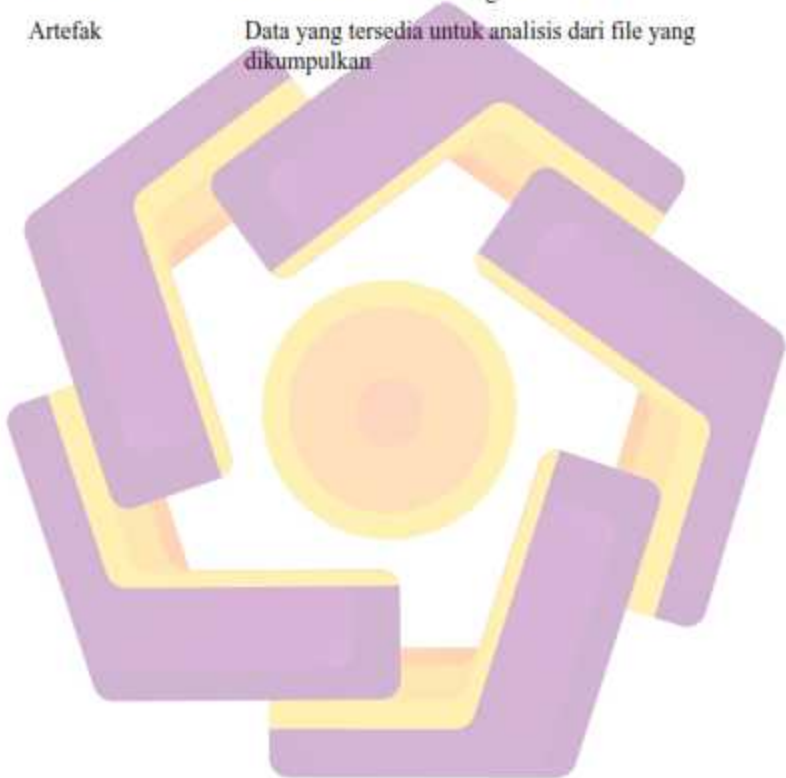
DAFTAR LAMBANG DAN SINGKATAN

Par	adalah angka indeks akurasi alat forensik
ar0	adalah jumlah variabel yang terdeteksi
arT	adalah keseluruhan variabel yang digunakan



DAFTAR ISTILAH

Examiner	Penguji, Pemeriksa
Imaging	Penciptaan gambar digital
Backup	Proses duplikasi atau menyalin data
Ekstraksi	Proses memilih atau mengambil data
Artefak	Data yang tersedia untuk analisis dari file yang dikumpulkan



INTISARI

Teknologi *smartphone* yang berkembang saat ini tidak hanya memberikan dampak positif namun juga bisa berdampak negatif jika digunakan untuk melakukan tindakan kejahatan atau bisa disebut *cybercrime*. Untuk melakukan investigasi tentunya diharapkan dapat memilih *tools* forensik yang tepat. Maka perlu dilakukan penelitian terhadap hasil analisis perbandingan kinerja *tools* forensik pada *file android backup smartphone*. Metode *National Institute of Standards and Technology* (NIST) digunakan dalam penelitian ini sebagai parameter dan untuk bukti digital yang diperoleh. Hasil ekstraksi *smartphone android OPPO A37f* dari *tools MOBILedit* didapatkan *file android backup* dan hasil analisa dari penggunaan *tools Magnet AXIOM* dengan tingkat akurasi data sebesar 39,3% dari variabel yang telah ditentukan, *Tools Oxygen Forensic* mendapatkan tingkat akurasi data sebesar 28,6% dari variabel yang telah ditentukan, dan *tools Belkasoft Evidence Center* mampu mendapatkan tingkat akurasi data sebesar 35,7% dari variabel yang telah ditentukan. Hasil dari penelitian ini dapat disimpulkan bahwa *tools Magnet Axiom* memiliki tingkat akurasi yang tinggi dibandingkan dengan *tools Oxygen Forensic* dan *Belkasoft Evidence Center* dalam mengekstrak data dari *file android backup smartphone*.

Kata kunci: *Tools Mobile Forensik, Smartphone, Android Backup, NIST*

Abstract

Smartphone technology that is currently developing not only has a positive impact but can also have a negative impact if it is used to commit crimes or can be called cybercrime. To conduct an investigation, of course, it is expected to choose the right forensic tools. So it is necessary to do research on the results of the comparative analysis of the performance of forensic tools on android smartphone backup files. The National Institute of Standards and Technology (NIST) method was used in this study as a parameter and for the digital evidence obtained. The results of the extraction of the *OPPO A37f* android smartphone from the *MOBILedit* tools obtained android backup files and the results of the analysis from the use of the *AXIOM Magnet* tools with a data accuracy rate of 39.3% from the predetermined variables, *Oxygen Forensic Tools* obtained a data accuracy rate of 28.6% from the variable that has been determined, and the *Belkasoft Evidence Center* tools are able to obtain a data accuracy rate of 35.7% of the predetermined variables. The results of this study can be concluded that the *Magnet Axiom* tool has a high level of accuracy compared to the *Oxygen Forensic* and *Belkasoft Evidence Center* tools in extracting data from android smartphone backup files.

Keyword: *Mobile Forensic Tools, Smartphone, Android Backup, NIST*