# PENERAPAN CFTT UNTUK PENGUJIAN APLIKASI FORENSIK WEB BASED DENGAN FEDERATED TESTING

Yasir Muin
19917018

*Tesis diajukan sebagai syarat untuk meraih gelar Magister Komputer*
*Konsentrasi Forensika Digitali*
*Program Studi Informatika Program Magister*
*Fakultas Teknologi Industri*
*Universitas Islam Indonesia*
2021

**Lembar Pengesahan Pembimbing**

**Penerapan *CFTT* Untuk Pengujian Aplikasi Forensik Web Based Dengan *Federated Testing***

Yasir Muin
19917018

Yogyakarta, Juni , 2021

Pembimbing

| | |
|---|---|
| Dr. Yudi Prayudi S.Si., M.Kom | Fietyata Yuda S.Kom., M.Kom |

**Lembar Pengesahan Penguji**

**Penerapan *CFTT* Untuk Pengujian Aplikasi Forensik Web Baed Dengan *Federated Testing***

Yasir Muin
19917018

Yogyakarta, Juni, 2021

Tim Penguji,

Dr. Yudi Prayudi, S.Si., M.Kom
Ketua

Dr. Imam Riadi S.Pd., M.Kom
Anggota I

Rr. Ir. Bambang Sugiantoro S.Si., MT
Anggota II

Mengetahui,
Ketua Program Studi Informatika Program Magister
Universitas Islam Indonesia

Izzati Muhimmah, S.T., M.Sc., Ph.D.

## Abstrak

**Penerapan *CFTT* Untuk Pengujian Aplikasi Forensik Web Based Dengan *Federated Testing***

Perkembangan smartphone membuat aktivitas manusia lebih muda, dengan fitur-fitur yang diberikan, perkembangan tersebut tidak menutup kemungkinan kecanggihan fitur smartphone dimanfaatkan sebagai media komunikasi untuk mendukung bentuk aksi kejahatan. Proses investigasi forensik dalam penanganan barang bukti elektronik pada smartphone menjadi sebuah tantangan bagi ahli forensik karena perkembangan smartphone yang terus berkembang. permasalahan yang dihadapi oleh ahli forensik sulit menentukan tools forensik yang harus digunakan dalam penanganan barang bukti karena beberapa aplikasi yang dikembangan belum diuji dengan standar forensik. untuk itu dalam penelitian ini akan dilakukan pengujian aplikasi web-based berdasarkan *standar computer forensics tools testing* menggunakan aplikasi *federated testing*. pengujian ini dilakukan untuk mengevaluasi kelayakan aplikasi web-based dengan membandingkan data dari aplikasi web-based dan belkasoft yang didasarkan pada parameter CFTT. Hasil evaluasi diketahui bahwa aplikasi web-based masih lebih rendah dibandingkan dengan belkasoft pada aplikasi web-based parameter yang tidak bisa dihasilkan diantaranya data file, social media, location, dan mms, sedangkan pada aplikasi belkasoft semua parameter sesuai dengan parameter standar CFTT mampu di hasil oleh aplikasi tersebut, sehingga output dari pengujian ini dapat ditarik sebuah kesimpulan bahwa pada aplikasi web-based belum memenuhi standar secara fungsional kebutuhan yang digunakan, sehingga kedepannya perlu adanya penambahan terhadap beberapa kebutuhan yang mampu menambahkan parameter sesuai yang ada pada standar CFTT, sehingga semua kebutuhan yang ada pada standard tersebut bisa terpenuhi sesuai dengan yang diharapkan.



**Kata kunci**

Mobile Forensik Invetigasi, *CFTT; Federated Testing*, Aplikasi *Web Based Android analysis tools*.

**Abstract**

**CFTT Application for Forensic Web Based Application Testing with Federated Testing**

The evolutionary of smartphones and their technology simplify human activities, with the features provided, this development does not rule out the sophistication of smartphone features being used as a medium of communication to support forms of crime. The process of forensic investigations in handling electronic evidence on smartphones is a challenge for forensic experts because of the ever-growing development of smartphones. The problems faced by forensic experts are difficult to determine which forensic tools should be used in handling evidence because some of the applications developed have not been tested with forensic standards. For this reason, in this study, web-based application testing will be carried out based on computer forensics tool testing standards using federated testing applications. This test is carried out for the feasibility of web-based applications by comparing data from web-based applications and Belkasoft which are based on CFTT parameters. The results of the evaluation show that web-based applications are still lower than Belkasoft in web-based parameter applications that cannot be generated including data files, social media, location, and MMS, while in Belkasoft all parameters are in accordance with standard CFTT parameters that the application is able to produce. , so that the output of this test can be drawn a conclusion that the web-based application does not meet the functional standards of the requirements used, so that in the future it is necessary to add some requirements that are able to add parameters according to the CFTT standard, so that all the requirements that exist in the standard can be fulfilled as expected.

**Keywords**
*Mobile forensics investigation, CFTT, Federated Testing, Application Web Based Android Analysis Tools.*

## Pernyataan Keaslian Tulisan

Dengan ini saya menyatakan bahwa tesis ini merupakan tulisan asli dari penulis, dan tidak berisi material yang telah diterbitkan sebelumnya atau tulisan dari penulis lain terkecuali referensi atas material tersebut telah disebutkan dalam tesis. Apabila ada kontribusi dari penulis lain dalam tesis ini, maka penulis lain tersebut secara eksplisit telah disebutkan dalam tesis ini.

Dengan ini saya juga menyatakan bahwa segala kontribusi dari pihak lain terhadap tesis ini, termasuk bantuan analisis statistik, desain survei, analisis data, prosedur teknis yang bersifat signifikan, dan segala bentuk aktivitas penelitian yang dipergunakan atau dilaporkan dalam tesis ini telah secara eksplisit disebutkan dalam tesis ini.

Segala bentuk hak cipta yang terdapat dalam material dokumen tesis ini berada dalam kepemilikan pemilik hak cipta masing-masing. Apabila dibutuhkan, penulis juga telah mendapatkan izin dari pemilik hak cipta untuk menggunakan ulang materialnya dalam tesis ini.

Yogyakarta, Juni, 2021

Yasir Muin, S.T

## Daftar Publikasi

**Publikasi selama masa studi**

| Kontributor | Jenis Kontributor |
|---|---|
| Yasir Muin | Mendesain eksperimen (%)<br>Menulis *Paper* (%) |

**Publikasi yang menjadi bagian dari tesis**

Publikasi berikut menjadi bagian dari penulisan tesis ini

| Kontributor | Jenis Kontribusi |
|---|---|
| Yasir Muin | Mendesain eksperimen (x%)<br>Menulis *paper* (x%) |
| Yudi Prayudi | Mendesain eksperimen (x%) |
| Fietyata Yudha | Mendesain eksperimen (x%)<br>Menulis dan mengedit *paper* (x%) |

## Halaman Kontribusi

Penelitian ini tidak terlepas dari berbagai saran maupun bimbingan dari berbagai pihak, mulai dari pra penelitian, seminar proposal, seminar progress, hingga seminar pendadaran. Pihak-pihak tersebut, antara lain, Dr. Yudi Prayudi S.Si., M.kom dan Fietyata Yudha S.Kom., M.Kom

## Halaman Persembahan

Bismillahirrahmanirrahim.

Alhamdulillah, atas ridho Allah Subhanahu Wa Ta'ala karya ini Saya persembahakan kepada kedua malaikat tercinta yang selama ini telah mendukung, memberikan semangat dan motivasi dalam menyelesaikan pendidikan magister komputer saya ini, secara khususnya kepada:

1. Ayahanda (Muin Siraju) dan Ibunda (Djasia Togubu), yang selalu menjadi rumah tempat Saya kembali dalam keadaan sedih, susah maupun senang, yang menjadi alasan, motivasi serta sumber semangat dalam hidup saya. Teruntuk kedua orangtua yang selalu mematahkan statement saya ketika berkata "Saya tidak bisa" maka mereka dengan tegas berkata "Kamu pasti bisa!".
2. Saudaraku (Ikram Muin, Samira Muin, Salwa Muin, Namira Muin, dan Zulfikar Muin) Terima kasih atas semua bantuan dan do'a yang telah diberikan kepada saya selama menempu perkuliahan.

Teman-teman seperjuangan forensika digital angkatan 19 yang telah memberikan support selama menempuh pendidikan ini.

## Kata Pengantar

Assalamualaikum Wr. Wb.

Puji syukur penulis panjatkan kepada Allah SWT atas limpahan dan karunia yang diberikan kepada penulis sehingga dapat menyelesaikan laporan penelitian tesis dengan judul "Penerapan CFTT untuk pengujian aplikasi forensic dengan deferated testing". Adapun maksud dari penulisan laporan penelitian ini adalah sebagai persyaratan dalam mencapai jenjang pendidikan Magister Teknik Informatika konsentrasi Forensika Digital di Fakultas Teknologi Industri, Universitas Islam Indonesia. Dalam proses penyelesaian tesis ini penulis tidak dapat menyelesaikannya bila tidak ada turut serta pihak lain yang juga ikut membantu baik secara langsung maupun tidak langsung dalam menyelesaikan penelitian ini, untuk itu penulis ingin menyampaikan rasa terima kasih kepada beberapa pihak yang telah mendukung dalam penyusunan tesis ini, antara lain:

1. Bapak Fathul Wahid, S.T., M.Sc., Ph.D, selaku rektor Universitas Islam Indonesia yang memberikan kesempatan kepada penulis untuk menimbah ilmu di Universitas Islam Indonesia.
2. Bapak Prof. Hari Purnomo, M.T selaku Dekan Fakultas Teknologi Industri Universitas Islam Indonesia yang memberikan fasilitas dan bantuan untuk belajar.
3. Ibu Izzati Muhimmah, ST., M.Sc., Ph.D, selaku Ketua Program Studi Teknik Informatika Program Magister Fakultas Teknologi Industri, Universitas Islam Indonesia, yang selalu memberikan semangat kepada setiap mahasiswa agar segera menyelesaikan tesis.
4. Bapak Dr. Yudi Prayudi S.SI., M.Kom, dan Bapak Fietyata Yudha S.Kom.,M.Kom. selaku dosen pembimbing yang telah banyak meluangkan waktunya dalam memberikan berbagai saran selama proses bimbingan.
5. Seluruh Dosen, staff administrasi dan civitas Magister Teknik Informatika Universitas Islam Indonesia, baik secara langsung maupun tidak langsung telah membantu penulis selama masa studi penulis.
6. Seluruh keluarga baik Bapak, Ibu, dan Kakak yang telah mencurahkan segenap cinta, kasih sayang, perhatian dan dukungan baik moril maupun materil.
7. Rekan-rekan mahasiswa MTI khususnya konsentrasi Forensika Digital angkatan 19 yang selama ini berjuang bersama dan selalu memberikan semangat satu sama lain.
8. Mu'mina Kurniawati S.J. Kahar, S.Psi., M.Psi. yang turut membantu dan memberikan semangat dan motivasi dalam penyusunan laporan tesis.}

## Daftar Isi

## Daftar Tabel

## Daftar Gambar

## Glosarium

| | |
|---|---|
| akuisisi | - proses pengambilan atau proses ekstraksi data dari suatu perangkat. |
| Resource | - resource adalah sumber daya dari sebuah perangkat keras atau virtual sistem |
| Database | - kumpulan data yang disimpan secara sistematis di dalam sebuah sistem. |
| Mount | - proses di mana sistem operasi membuat file dan direktori pada perangkat penyimpanan tersedia untuk diakses pengguna melalui sistem file komputer. |
| pull data | - pull data adalah proses pemindahan data yang ada pada perintah android debugging system. |
| Debugging | - adalah ada salah satu opsi pengembanga yang ada pada fitur smartphone yang di bisa digunakan untuk mengakses perangkat |

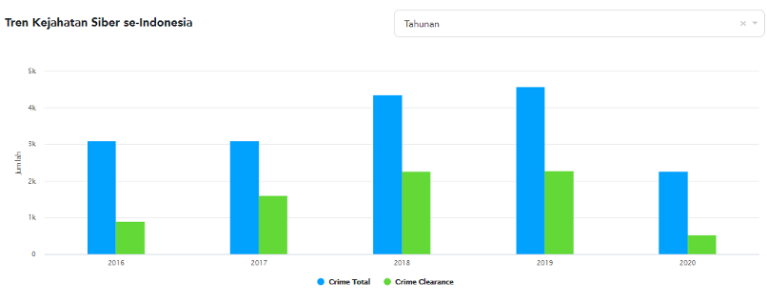
# BAB 1
# Pendahuluan

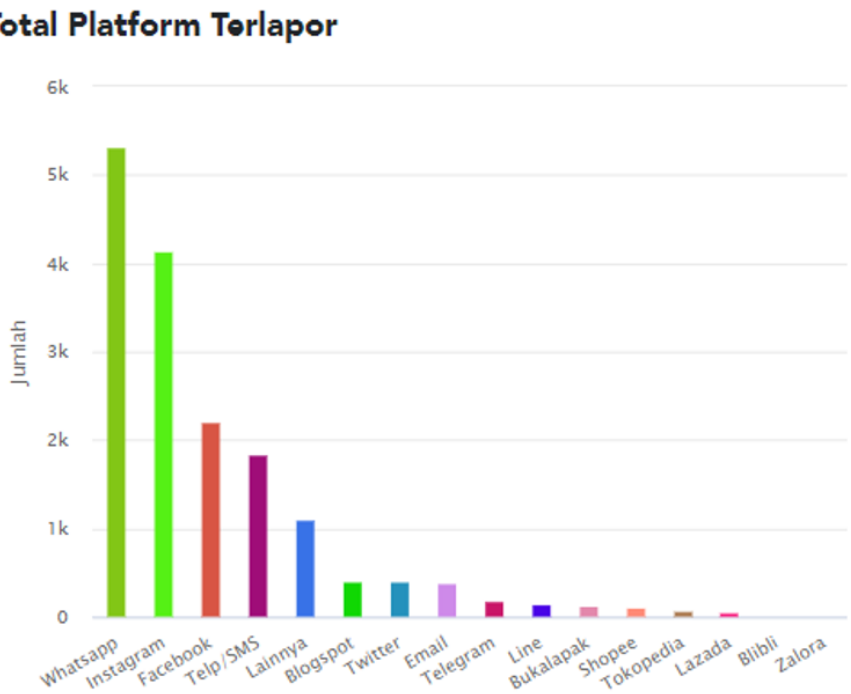
## 1.1 Latar Belakang

Keberadaan smartphone saat ini dianggap sangat membantu aktivitas manusia dalam melakukan pekerjaan sehari-hari. Berkembangnya fitur- fitur yang terdapat pada smartphone mempermudah para penggunanya melakukan aktivitas pekerjaan kantor, bisnis, e-banking, serta buat berhubungan dengan pengguna lain di media sosial. Pertumbuhan smartphone tidak cuma membagikan akibat positif namun dapat berakibat negatif kala pertumbuhan tersebut dimanfaatkan buat melaksanakan aksi kejahatan seperti pencurian data, penipuan atau tindak kejahatan lainnya yang memanfaatkan smartphone sebagai medianya (Riadi et al., 2019).

Berdasarkan data dari laporan newzoo, salah satu website yang melakukan perhitungan populasi penggunaan smartphone dan jumlah serangan penetrasi pada perangkat smartphone, pada tahun 2020 tercatat pengguna smartphone di Indonesia mencapai 160.232.000 juta dari 273.524.000 juta penduduk di Indonesia. Artinya, hampir 58% penduduk Indonesia menggunakan smartphone sebagai kebutuhan sehari-hari, sedangkan untuk kasus kejahatan yang terjadi pada perangkat smartphone tercatat sebanyak 58.6%. Hal ini menyebabkan hampir semua kasus yang terjadi baik konvensional maupun kasus berteknologi akan ditemukan barang bukti elektronik seperti smartphone, tablet dan lain-lain dari tangan tersangka (Newzoo, 2017).

Laporan dari direktorat tindak pidana siber bareskrim polri (dittipidsiber) menyatakan bahwa statistik peningkatan kejahatan siber setiap tahunnya mengalami peningkatan, mulai dari kasus yang berhasil ditangani sampai kasus yang dihentikan. Dittipidsiber merupakan satuan kerja yang bertugas membuat dan melaksanakan penegakan hukum terhadap kejahatan siber.






G ambar 1.1 Jumlah kasus dan platform pada *handphone* 2016 – 2020 (Polri, 2020).

Berdasarkan data pada gambar di atas, dapat diketahui bahwa jumlah kasus yang terjadi menggunakan *platform* yang berjalan pada perangkat *smartphone*. Hal ini tidak terlepas dari perkembangan teknologi *smartphone* dengan fitur-fitur seperti *chipset* dan sistem operasi yang disesuaikan dengan perkembangan zaman dan kebutuhan dari pengguna. Pada perangkat *smartphone, chipset* berkembang sangat cepat dan banyak varian atau produk. Macam-macam produk tersebut seperti mediatek, Samsung Exynos, Snapdragon, Nvidia Tegra, OMAP, PXA, Intel dan lain sebagainya. Selain chipset, pada *smartphone* juga terdapat sistem operasi yang banyak varian serta perkembangan versinya yang pesat. Android sistem operasi merupakan salah satunya.

Perkembangan teknologi *smartphone* menjadi tantangan bagi ahli forensik dan penegak hukum untuk melakukan akuisisi dan analisis terhadap barang bukti kejahatan yang dilakukan oleh pelaku. Bukti digital ini dapat berupa data yang ada pada *smartphone* seperti data kontak, *log* panggilan, pesan, video, gambar dan file dokumen yang akan dijadikan sebagai barang bukti dalam kasus persidangan. Informasi yang ditemukan dalam bukti tersebut dapat memberikan petunjuk tentang keberadaan dan aktivitas dari pelaku. Hal ini tentu perlu dipastikan validasi dari bukti tersebut karena berkaitan dengan putusan hukum yang akan ditentukan.

Akuisisi data dari perangkat digital telah menjadi bagian penting dari banyak investigasi kriminal. Banyak alat akuisisi yang dikembangkan oleh para *developer* dan ahli forensik untuk melakukan akuisis pada perangkat *smartphone*, namun penyelidik forensik terbaik pun mengakui bahwa akuisisi data dari perangkat seluler bisa jadi membosankan. Hal ini disebabkan banyaknya perbedaan jenis data dan format yang digunakan dari satu perangkat ke perangkat lainnya. Atas dasar permasalahan diatas maka perlu adanya evaluasi alat forensik yang efektif dalam melakukan penyelidikan di lapangan baik yang dilakukan oleh tim forensik maupun penyelidikan terhadap barang bukti *smartphone* android dan membuat spesifikasi yang berlaku umum dan memenuhi standar pengujian.

Standar pengujian telah banyak dikembangakan oleh organisasi internasioal salah satunya adalah organisasi *National Institute of Standard Technology* (*NIST*). Salah satu proyek yang dilakukan oleh *NIST* untuk pengujian alat komputer forensik adalah *CFTT (*C*omputer Forensic Tools Testing). CFTT* adalah sebuah metode untuk pengujian perangkat lunak komputer forensik yang dikembangkan secara umum seperti spesifikasi alat, prosedur pengujian, pengujian kriteria, pengujian set dan pengujian *hardware.* Proyek *Computer Forensic Tools Testing* di *NIST* adalah sebuah lembaga departemen perdagangan Amerika Serikat yang merancang dan memberikan ukuran jaminan untuk perangkat lunak yang digunakan oleh penegak hukum dalam penyelidikan komputer forensik, proyek ini didukung oleh kerja sama antara *NIST* dan *National Institute of Justice* (*NIJ*), organisasi penelitian, departemen kehakiman Amerika Serikat, dan Lembaga lainnya.

Pendekatan *CFTT* terhadap pengujian sebuah aplikasi adalah untuk menguji alat berdasarkan fungsionalitas yang didukungnya, pengujian ini dilakukan menggunakan aplikasi *federated testing,* dengan tujuan untuk menguji kelayakan aplikasi agar dapat dijadikan sebagai standarisasi aplikasi dalam melakukan investigasi yang dapat digunakan oleh seluruh komunitas forensik digital atau laboratorium forensik. *Federated testing* sendiri merupakan bagian pengembangan dari program *CFTT* yang menyediakan kebutuhan para penyidik dan laboratorium forensik digital dengan ruang uji, untuk pengujian alat dan laporan. *Federated testing* membantu penyidik forensik digital untuk menguji alat yang gunakan. Memungkinkan setiap lab, agensi, atau individu untuk menguji aplikasinya menggunakan metodologi pengujian yang sama seperti yang digunakan *CFTT*. *Output* dari proses ini adalah membuat laporan pengujian untuk alat tersebut. Laporan ini menghasilkan pengujian dalam format umum yang memudahkan setiap orang lain untuk memahami bagaimana aplikasi *web based android analysis tools* tersebut diuji dan bagaimana hasil pengujiannya. Sebelumnya aplikasi web-based ini belum dilakukan pengujian berdasarkan

standar forensik sehingga sangat berdapak terhadap setiap orang bila menggunakan aplikasi web-base dalam penangan kasus forensik, karena belum diketahui kemampuan-nya, untuk itu perlu dilakukan pengujian aplikasi web-based untuk mengetahui kemampuan dari aplikasi itu sendiri. Pengujian terhadap aplikasi *web based android analysis tools* didasarkan pada standarisasi CFTT sebagai pendekatan untuk mengetahui kemampuan aplikasi secara fungsional yang disesuaikan dengan laporan *federated testing*.

Berdasarkan uraian diatas, peneliti tertarik untuk melakukan pengujian aplikasi *web based android analysis tools,* untuk mengetahui kelayakan aplikasi dengan memverifikasi bahwa program yang diujikan mampu dijadikan sebagai standarisasi aplikasi dalam melakukan investigasi sesuai dengan standar *CFTT* dan dapat digunakan oleh seluruh komunitas forensik digital atau laboratorium forensik.

## 1.2 Rumusan Masalah

Berdasarkan latar belakang diatas maka rumusan masalah dalam penelitian ini adalah Mengimplementasikan pengujian CFTT untuk menetahui kemampuan aplikasi web-based dan memberikan rekomendasi perbaikan aplikasi web-based berdasarkan laporan pengujian dari CFTT?

## 1.3 Batasan Penelitian

Adapun batasan masalah dalam penelitian ini adalah pengujian hanya dilakukan pada aplikasi yang akan diuji berdasarkan aplikasi *federated testing* sesuai dengan standar CFTT.

## 1.4 Tujuan Penelitian

Adapun tujuan dalam penelitian ini adalah untuk mengimplementasikan pengujian CFTT untuk menetahui kemampuan aplikasi web-based dan memberikan rekomendasi perbaikan aplikasi web-based berdasarkan laporan pengujian dari CFTT.

## 1.5 Manfaat Penelitian

Adapun manfaat dalam penelitian ini adalah dapat memberikan rekomendasi terhadap aplikasi *web based android analysis tools* sehingga dapat digunakan oleh komunitas forensik atau laboratorium.

## 1.6 Literatur Review

Berikut tentang penelitian yang berkaitan dengan *Computer Forensic Tool Testing* (*CFTT*) antara lain:

Horsman, (2019) membahas keadaan pengujian alat forensik digital saat ini di 2018 bersama dengan kesulitan aplikasi pengujian yang cukup untuk digunakan dalam disiplin ini. Hasil selanjutnya pun investigasi menggunakan alat tersebut harus dapat diandalkan dan

dapat diulang sambil mendukung pendirian fakta, memungkinkan proses peradilan pidana kemampuan untuk mencerna setiap temuan selama proses menentukan rasa bersalah atau tidak bersalah. Kesalahan yang ada pada setiap tahap pemeriksaan dapat merusak keseluruhan investigasi, mengkompromikan hasil yang berpotensi sebagai bukti.

Guttman et al., (2014) dalam proyek *CFTT* telah menulis persyaratan alat, rencana pengujian dan pengujian alat forensik selama 10 tahun terakhir. Secara umum, hasilnya benar untuk kritis fungsi alat diminta untuk dilakukan. Beberapa kesalahan serius telah ditemukan, dan vendor alat mampu memperbaiki masalah dengan cepat. Sebagian besar masalah hanyalah perilaku unik yang bisa terjadi dihindari jika praktisi menyadarinya. Selama beberapa tahun ke depan *CFTT* akan berkembang menguji area fungsional lainnya seperti string mencari, perolehan memori langsung, alat triase dan ekstraksi email. Area lain akan coba dibuat metodologi pengujian *CFT* tersedia untuk forensic laboratorium dalam bentuk yang mudah bagi laboratorium untuk menguji alat forensik dengan cara yang umum dan untuk memfasilitasi berbagi hasil tes dan bahan tes.

Pan dan Batten (2009) menggunakan pendekatan pengujian untuk membandingkan kinerja alat forensik digital tanpa menggunakan peralatan canggih atau hanya menghabiskan banyak waktu. Hasil pengujian telah membuktikan validitas dan efektivitas metodologi. Selain itu, metode yang digunakan lebih efisien daripada yang lainnya. Metodologi yang digunakan sepenuhnya otomatis yang terkomputerisasi dapat dikembangkan untuk di masa depan. Prosedur yang dilakukan khusus untuk pengujian alat forensik digital karena memenuhi persyaratan keadilan dan kebutaan, dan dapat dijalankan, tanpa jeda, selama diperlukan untuk mencapai hasil yang akurat.

Roy et al., (2019) dalam penelitiannya mengambil bagian dalam pengembangan dan evaluasi kurikulum pada sebuah Universitas dengan memasukkan *National Institute Standar dan Teknologi (NIST) dengan* menetapkan *CFTT* sebagai standar untuk forensic digital. Tujuan proyek *CFTT* adalah untuk membangun metodologi untuk menguji perangkat lunak forensik komputer dengan pengembangan dari spesifikasi alat umum, prosedur pengujian, kriteria pengujian, pengujian set, dan uji perangkat keras.

Dalam penelitian ini akan dilakukan pengujian aplikasi *web based android analysis tools* dengan *federated testing* untuk menguji kelayakan aplikasi sesuai dengan satnarasi CFTT agar bisa di digunakan untuk investigasi forensik digital.

Tabel 1.1 Literatur review

| No. | Peneliti | Keywords | Ulasan Kritis | Pustaka |
|---|---|---|---|---|
| 1 | Horsman (2019) | Digital forensics Testing, Validation, Research Error-rate, Reliability | Melakukan pengujian alat forensic digital di tahun 2018. Forensik digital adalah disiplin yang memberikan pengambil keputusan pemahaman yang dapat diandalkan tentang jejak digital pada perangkat apa pun yang diselidiki, namun tidak dapat mengatakan dengan kepastian 100% bahwa alat yang digunakan untuk melakukan proses ini menghasilkan fakta yang akurat hasil dalam semua kasus. | Tool testing and reliability issues in the field of digital forensics |
| 2 | Guttman, Lyle dan Ayers (2014) | Ten Year of computer forensic, tools testing | Mengembangkan proyek CFTT telah menulis persyaratan alat, rencana pengujian dan pengujian alat forensik selama 10 tahun terakhir. Secara umum, hasilnya benar untuk kritis fungsi alat diminta untuk dilakukan. | Ten Years of Computer Forensic Tool Testing |
| 3 | Roy, Wu dan LaVenia (2019) | Digital Forensics (DF), curricula development NIST standards, Computer Forensics Tool Testing (CFTT), Hardware Write Blocker (HWB), Deleted File Recovery (DFR), Smart Phone Forensics | Mengembangkan dan mengevaluasi kurikulum pada sebuah Universitas dengan memasukkan National Institute Standar dan Teknologi (NIST) dengan menetapkan CFTT sebagai standar untuk forensic digital | Experience of Incorporating NIST Standards in a Digital Forensics Curricula |
| 4 | Pan dan Batten (2009) | Digital forensic tool testing Experimental errors Performance testing CFReDS project EESAG | Melakukan pengujian untuk membandingkan kinerja alat forensik digital tanpa menggunakan peralatan canggih. | Robust performance testing for digital forensic tools |

## 1.7 Metode Penelitian

Langkah-langkah yang ditempuh untuk melakukan penelitian ini adalah sebagai berikut:

## 1.8 Sistematika Penulisan

Untuk memberikan gambaran dan mempermudah dalam penyusunan penelitian ini, maka dibuat sistematika penulisan sebagai berikut:

**BAB I Pendahuluan**

Pendahuluan merupakan penghantar terhadap permasalahan yang akan dibahas. Didalamnya menguraikan tentang gambaran suatu penelitian yang terdiri dari latar belakang, rumusan masalah, batasan masalah, tujuan penelitian, manfaat penelitian, metodologi penelitian serta sistematika penulisan.

**BAB II Tinjauan Pustaka**

Pada Bab ini menjelaskan tentang teori-teori dasar yang digunakan untuk memecahkan masalah dalam penelitian ini. Teori yang berkaitan dengan penelitian yang sedang diteliti.

**BAB III Metodologi Penelitian**

Bab ini membahas tentang langkah-langkah penelitian, kebutuhan perangkat lunak, perangkat keras dan bahan penelitian yang digunakan serta perancangan antarmuka aplikasi yang akan dibuat.

**BAB IV Pembahasan**

Pada Bab ini membahas tentang hasil dan pembahasan, terkait dengan pembahasan penyelesaian masalah yang diangkat, penentuan hasil analisis dan evaluasi dari penelitian yang diangkat.

**BAB V Penutup**

Pada bab ini memuat kesimpulan akhir dari semua proses penelitian sampai kepada hasil implementasi metode dan saran yang perlu diperhatikan karena keterbatasan dalam mendapatkan materi yang dibuat selama melakukan penelitian dan rekomendasi yang dibuat untuk pengembangan penelitian selanjutnya.

# BAB 2
# Tinjauan Pustaka

## 1.1 Digital Forensik

Forensik digital telah didefinisikan sebagai penggunaan metode yang diturunkan dan terbukti secara ilmiah terhadap pelestarian, pengumpulan, validasi, identifikasi, analisis, interpretasi dan penyajian bukti digital yang berasal dari sumber digital dengan tujuan memfasilitasi atau melanjutkan rekonstruksi peristiwa yang ditemukan bersifat kriminal atau membantu mengantisipasi tindakan tidak sah yang terbukti mengganggu operasi yang direncanakan (Palmer, 2001). Menurut Marcella Jr. & Menendez, (2010), digital forensic adalah aktivitas yang berhubungan dengan pemeliharaan, identifikasi, pengambilan atau penyaringan, dan dokumentasi barang bukti digital dalam kejahatan komputer.

Forensika digital juga diartikan sebagai ilmu dan metode yang digunakan untuk menemukan, mengumpulkan, mengamankan, menganalisis, menginterpretasi dan mempresentasikan barang bukti digital yang terkait dengan kasus yang terjadi untuk kepentingan rekonstruksi kejadian serta keabsahan proses peradilan (Agarwal et al., 2011). Bagi Al- Azhar( 2012) forensika digital ialah aplikasi ilmu pengetahuan serta teknologi pc buat melaksanakan pengecekan serta analisis terhadap benda data elektronik serta objek, fakta digital dalam memandang keterkaitannya dengan kejahatan. Salah satu elemen penting dari forensik digital adalah kredibilitas bukti digital. Bukti digital termasuk computer bukti, audio digital, video digital, ponsel, mesin fax digital dll.

Bidang forensik digital telah menjadi hal yang lumrah karena semakin maraknya teknologi sejak akhir abad ke-20, dan relevansi yang tak terhindarkan dari teknologi ini dalam melakukan aktivitas kriminal. Dalam forensik tradisional, bukti biasanya berupa sesuatu yang dapat mengidentifikasi pelaku kejahatan, seperti rambut, darah atau sidik jari. Sebaliknya, forensik digital berurusan dengan file dan data dalam bentuk digital yang diambil dari perangkat digital. Forensik digital adalah istilah yang banyak digunakan, merujuk pada identifikasi, akuisisi, dan analisis bukti digital yang berasal dari lebih dari sekadar komputer, seperti ponsel cerdas, tablet, Perangkat Internet of Things, atau data yang disimpan di cloud (Du et al., 2017).

Menurut *National Institute of Standards and Technology* (NIST) ada empat tahapan dalam digital forensik (Karen Kent, Suzanne Chevalier, Tim Grance, 2006) yaitu *collection*, *examination*, *analysis* dan *reporting*.

1. *Collection* merupakan tahap pengumpulan data, yang selanjutnya akan diidentifikasi, pemberian label, perekaman data yang diperoleh dari sumber data yang relevan dan menggunakan prosedur yang sesuai sehingga integritas data dapat dipertanggung jawabkan.
2. *Examination* untuk melakukan pemeriksaan terhadap data yang telah dikumpulkan dengan menggunakan kombinasi metode otomatis dan manual, sehingga dapat menilai dan melakukan ekstraksi data dengan tetap menjaga integritas data.
3. *Analysis* menggunakan metode dan melakukan dokumentasi terhadap setiap langkah yang dilakukan, sehingga dapat memperoleh informasi yang berguna dan menjawab masalah-masalah dalam proses pemeriksaan dan pengumpulan data.
4. *Reporting* untuk melaporkan hasil dari analisa. tahapan ini meliputi sebagian prosedur antara lain uraian beragam informasi diperoleh, uraian dari tiap aksi yang dicoba, pemahaman beragam perkakas serta prosedur yang dicoba serta saran buat revisi dari proses forensik.


Gambar 2.1 Tahapan forensik digital menut *NIST*.

## 2.2 *Computer Forensics Tools testing* (CFTT)

*Program Computer Forensics Tool Testing* adalah proyek bersama dari *National Institute of Justice* (NIJ), *Department of Homeland Security* (DHS), dan *National Institute of Standards and Technology's* (NIST), *Office of Law Enforcement Support* (OLES) dan *Information Technology Laboratory* (ITL). CFTT didukung oleh organisasi lainnya, termasuk Biro Investigasi Federal, *Departemen AS Defense Cyber Crime Center*, Investigasi Kriminal Internal Revenue Service AS Divisi Program Kejahatan Elektronik, Biro Imigrasi dan Bea Cukai Penegakan dan Dinas Rahasia A.S. Perwakilan dari masing-masing instansi membentuk pengarah komite yang memberikan panduan proyek, dukungan teknis, dan memilih alat untuk pengujian (NIST, 2011).

Tujuan dari proyek *Computer Forensics Tool Testing* di N*ational Institute of Standards and Technology* (NIST) mengembangkan metodologi untuk menguji alat perangkat lunak forensik komputer dengan membuat spesifikasi alat umum, prosedur pengujian, kriteria pengujian, dan menguji kumpulan data. Hasilnya memberikan informasi yang diperlukan bagi pembuat alat untuk meningkatkan alat, bagi pengguna untuk membuat pilihan informasi tentang memperoleh dan menggunakan alat forensik komputer, dan bagi pihak yang berkepentingan untuk memahami kapabilitas alat tersebut. Pendekatan digunakan untuk menguji komputer alat forensik didasarkan pada metodologi internasional yang terkenal untuk pengujian kesesuaian dan pengujian kualitas (NIST, 2011).

Tujuan dari program CFTT adalah untuk memberikan jaminan yang terukur kepada praktisi, peneliti, dan pengguna lain yang berlaku bahwa alat yang digunakan dalam forensik komputer investigasi memberikan hasil yang akurat. Untuk mencapai hal ini diperlukan pengembangan spesifikasi dan metode pengujian untuk alat forensik komputer dan pengujian alat khusus selanjutnya terhadap spesifikasi tersebut. Tujuan kedua adalah memberikan bantuan dan sumber daya untuk praktisi forensik untuk melakukan pengujian alat forensik mereka sendiri. Ini dicapai dengan menyediakan persyaratan pengujian, rencana pengujian, perangkat pengujian dan data pengujian untuk penggunaan umum (NIST, 2011).

Metodologi pengujian yang dikembangkan oleh NIST didorong oleh fungsionalitas. Kegiatan investigasi forensik dipisahkan ke dalam fungsi atau kategori yang berbeda, seperti proteksi penulisan hard disk, pencitraan disk, pencarian string, dll. Metodologi pengujian kemudian dikembangkan untuk setiap kategori. Proses pengujian CFTT dipimpin oleh komite pengarah yang terdiri dari perwakilan komunitas penegak hukum. Komite pengarah memilih fungsi alat untuk pengembangan metode pengujian dan alat khusus untuk pengujian oleh anggota staf di CFTT. Setelah fungsi forensik dipilih, CFTT mengambil beberapa langkah persiapan untuk pengujian, yaitu:

### 2.2.1 Proses pengembangan spesifikasi

Setelah kategori alat dan setidaknya satu alat dipilih oleh komite pengarah proses pengembangan adalah sebagai berikut:

1. NIST dan staf penegak hukum mengembangkan dokumen persyaratan, pernyataan, dan kasus pengujian (disebut spesifikasi kategori alat).
2. Spesifikasi kategori alat diposting ke web untuk ditinjau sejawat oleh anggota komunitas forensik komputer dan untuk komentar publik oleh pihak lain yang berkepentingan.
3. Komentar dan umpan balik yang relevan dimasukkan ke dalam spesifikasi.

4. Lingkungan pengujian dirancang untuk kategori alat.

### 2.2.2 Proses Uji Alat

Setelah spesifikasi kategori dikembangkan dan alat yang dipilih, proses pengujian adalah sebagai berikut:

1. NIST memperoleh alat yang akan diuji.
2. NIST meninjau dokumentasi alat.
3. NIST memilih kasus pengujian yang relevan tergantung pada fitur yang didukung oleh alat.
4. NIST mengembangkan strategi pengujian.
5. NIST melakukan tes.
6. NIST menghasilkan laporan tes.
7. Komite Pengarah meninjau laporan pengujian.
8. Vendor meninjau laporan pengujian.
9. NIST memposting perangkat lunak dukungan ke web.
10. DHS memposting laporan tes ke web.

## 2.4 Federated Testing

*Federated testing* adalah perluasan dari Program *Computer Forensic Tool Testing* (CFTT) untuk menyediakan penyelidik dan lab forensik digital rangkaian pengujian untuk pengujian alat dan untuk mendukung laporan pengujian bersama. Tujuan dari *federated testing* adalah untuk membantu penyelidik forensik digital untuk menguji alat yang mereka gunakan di laboratorium mereka dan untuk memungkinkan berbagi hasil pengujian alat dalam komunitas forensik digital (NIST, 2011).

Berikut adalah rangkaian penginstalan untuk menguji alat menggunakan *federated* testing:

1. Unduh file .iso Linux langsung *federated testing* dan gunakan untuk membuat flash drive yang dapat di-boot atau DVD yang dapat di-boot. Seseorang dapat menggunakan alat Rufus untuk membuat flash drive yang dapat di-boot dari file iso.
2. Masukkan flash drive atau DVD yang dapat di-boot ke dalam workstation forensik dan boot ke situ.
3. Gunakan *interface* (*browser Web Firefox*) untuk memilih jenis alat yang ingin uji. Antarmuka pengguna akan memberitahu item apa yang perlu dimiliki untuk memulai.
4. Gunakan antarmuka untuk menghasilkan kasus pengujian untuk menguji alat dan ikuti petunjuk untuk menjalankan setiap pengujian.

5. Gunakan antarmuka untuk menghasilkan laporan pengujian untuk alat Anda.
6. Kirimkan laporan pengujian dan file log yang dibuat selama pengujian ke CFTT untuk dibagikan dengan komunitas forensik digital.

### 3.4 Bukti Digital

Bukti digital adalah informasi yang disimpan atau dikirim dalam bentuk biner yang dapat diandalkan di pengadilan. Fakta digital biasanya terpaut dengan kejahatan digital semacam kejahatan yang menggunakan sosial media selaku tempat mengimplemntasikan kejahatan, sehingga fakta digital digunakan buat menunjang dalam mengadili seluruh tipe kejahatan digital (Riadi et al., 2017). Bukti digital adalah semua jenis tipe data yang disimpan dan atau dikirimkan menggunakan komputer dimana suatu pelanggaran terjadi (Casey, 2011). Bukti digital tidak hanya meliputi bukti yang dihasilkan atau ditransmisikan melalui jaringan komputer saja, akan tetapi juga termasuk perangkat audio, video bahkan telepon seluler.

Bukti digital rapuh, mudah menguap, dan rentan jika tidak ditangani dengan benar. Segala macam perubahan yang mengandung bukti digital akan mengarah pada kesimpulan yang salah, atau bukti tersebut menjadi tidak berguna (Albanna & Riadi, 2017). Penetapan langkah-langkah perolehan alat bukti digital dilakukan dengan memperhatikan:

1. Media digital sebagai bukti.
2. Tata letak fisik media penyimpanan digital.
3. Integritas dan keaslian bukti digital.
4. Menggunakan Write-Protect, hashes, dan lainnya.
5. Akses ke bukti digital hanya diberikan untuk siapa.
6. Diberi otoritas dan tidak ada yang menggunakannya.
7. Perangkat elektromagnetik yang dekat dengan bukti digital.
8. Dokumentasi kondisi dan media.
9. Konfigurasi penyimpanan digital.
10. Penggunaan duplikat / pencitraan bukti digital prosedur dan perangkat data digital dibawah standar akuisisi forensik.
11. Dokumentasi informasi dan lakukan.
12. Konfigurasi pada perangkat digital.

### 2.5 Proses Mobile Forensik

Menurut (Kostadinov Dimitar, 2019) Proses forensik seluler bertujuan untuk memulihkan bukti digital atau data yang relevan dari perangkat seluler dengan cara yang akan mempertahankan bukti dalam kondisi baik secara forensik. Untuk mencapai itu, proses

forensik seluler perlu menetapkan aturan yang tepat yang akan mengisolasi, mengangkut, menyimpan untuk analisis dan bukti bukti digital yang aman berasal dari perangkat seluler. Biasanya, proses forensik seluler mirip dengan yang ada di cabang forensik digital lainnya. Namun demikian, orang harus tahu bahwa proses forensik seluler memiliki kekhasan tersendiri yang perlu dipertimbangkan. Mengikuti metodologi dan pedoman yang benar adalah prasy pra syuga penting untuk pemeriksaan perangkat seluler untuk menghasilkan hasil yang baik. Jelaskan langkah-langkah dalam proses proses mobile forensik.

1. Seizures

Forensik digital beroperasi dengan prinsip bahwa bukti harus selalu dilestarikan, diproses, dan diterima secara memadai di pengadilan. berbagai keputusan hukum yang dijalankan ssuai dengan pengambilalian perangkat seluler. Ada dua resiko besar mengenai fase proses forensik seluler ini: Aktivasi kunci (oleh pengguna / tersangka / pihak ketiga yang tidak disengaja) dan koneksi Jaringan / Seluler.

2. Akuisisi

Tujuan dari fase ini adalah untuk mengambil data dari perangkat seluler. Layar yang terkunci dapat dibuka dengan PIN, kata sandi, pola, mengumpulkan informasi dengan benar. Ada tantangan unik tertentu mengenai pengumpulan informasi dalam konteks teknologi seluler. Banyak perangkat seluler tidak dapat dikumpulkan dengan membuat image dan sebaliknya mungkin harus menjalani proses yang disebut akuisisi data, berbagai protokol untuk mengumpulkan data dari perangkat seluler karena spesifikasi desain tertentu hanya dapat memungkinkan satu jenis akuisisi.

3. Pemeriksaan dan analisis

Sebagai langkah pertama dari setiap penyelidikan digital yang melibatkan perangkat seluler, ahli forensik perlu mengidentifikasi:

- Jenis perangkat seluler – misalnya, GPS, smartphone, tablet, dll.
- Jenis jaringan – GSM, CDMA, dan TDMA.
- Carrier.
- Penyedia layanan (Reverse Search).

Pemeriksa mungkin perlu menggunakan banyak alat forensik untuk memperoleh dan menganalisis data yang berada di mesin. Karena keragaman perangkat seluler yang banyak, tidak ada solusi satu ukuran yang cocok untuk semua mengenai alat forensik seluler. Akibatnya, disarankan untuk menggunakan lebih dari satu alat untuk pemeriksaan. adalah beberapa produk perangkat lunak forensik populer yang memiliki kemampuan analitik

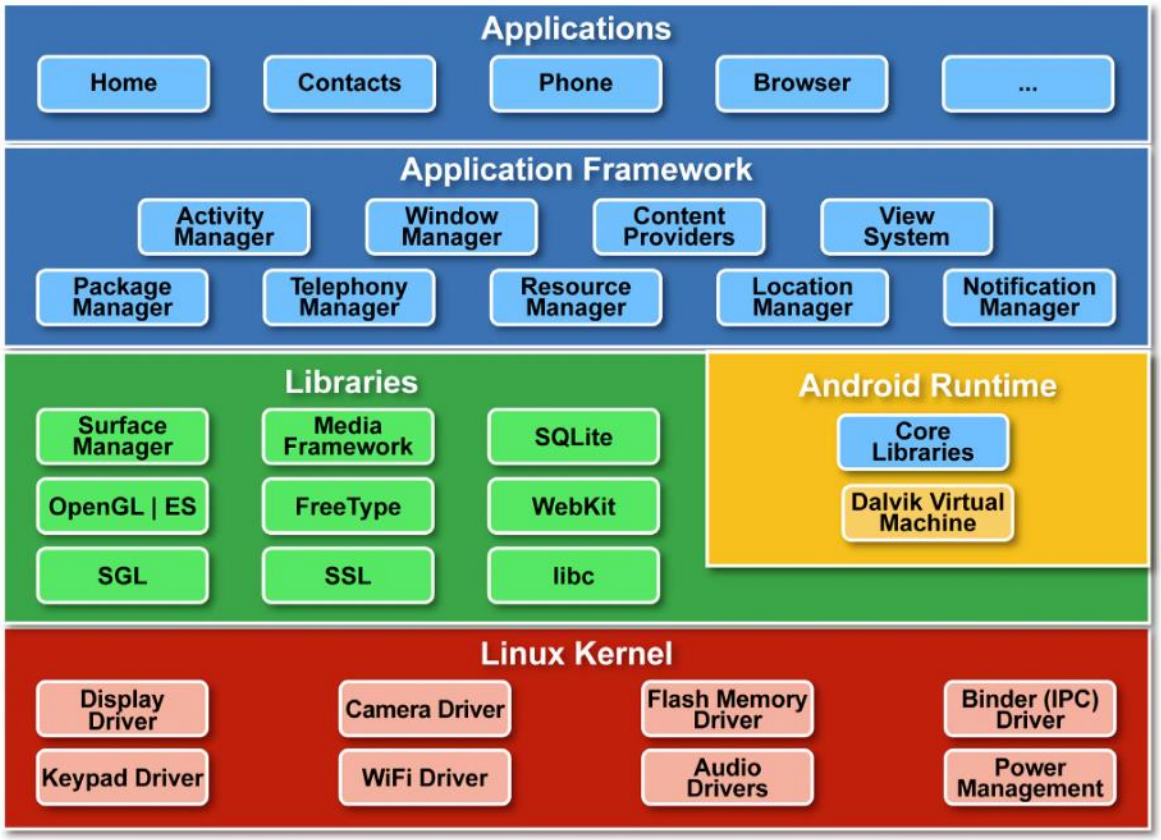
seperti accessData, sleuthkit, dan Encase. Analisis garis waktu dan tautan yang tersedia di banyak alat forensik seluler dapat mengikat masing-masing peristiwa paling signifikan, dari sudut pandang analis forensik. Semua informasi, bukti, dan temuan lain yang diekstraksi, dianalisis, dan didokumentasikan sepanjang penyelidikan harus disajikan kepada pemeriksa forensik lainnya atau pengadilan dengan cara yang jelas, ringkas, dan lengkap.

## 2.6 Forensik tools Testing

Mobile Forensik ialah bidang yang relatif baru di zona forensik digital, sehingga fitur lunak serta tool yang dapat digunakan buat mengambil informasi dari ponsel masih relatif baru. Tool ekstraksi dapat berbentuk hardware ataupun aplikasi bergantung kebutuhan pada informasi yang diekstrak dari fitur mobile. Tool yang ada kebanyakan merupakan tool komersial dan ada juga sedikit yang berupa tool open source, akan tetapi pengadaan tool-tool ini cukup sulit didapatkan terkait masalah privasi dan masalah keamanan serta biaya yang dibutuhkan (Madiyanto et al., 2017).

## 2.7 Android dan Arsitektur

Bagi Android merupakan tumpukan fitur lunak berbasis Linux sumber terbuka yang terbuat dari bermacam fitur serta aspek wujud.




Gambar 2.2 Architecture android.

1. Linux Kernel

Fondasi platform Android adalah kernel Linux. contoh, Android Runtime ( ART) tergantung pada kernel Linux buat fungsionalitas dasar semacam threading serta pengelolaan memori tingkatan rendah. Memakai kernel Linux membolehkan Android buat menggunakan fitur keamanan inti serta membolehkan produsen fitur buat meningkatkan driver fitur keras buat kernel yang lumayan diketahui.

2. Hardware Abstraction Layer (HAL)

Hardware Abstraction Layer (HAL) membagikan antarmuka standar yang menguak keahlian piranti keras. piranti kerangka kerja API Java yang lebih teratas. Perihal atas sebagian materi pustaka, tiap- tiap mempraktikkan antarmuka buat komponen fitur keras tertentu, semacam materi kamera ataupun bluetooth. Ketika API kerangka kerja melaksanakan panggilan buat mengakses perkakas, sistem Android muat materi pustaka buat komponen rkakas tersebut.

3. Android Runtime

Buat fitur yang melaksanakan Android tipe 5. 0( API tingkat 21) ataupun lebih besar, tiap aplikasi melaksanakan proses tiap- tiap sesi Android Runtime( ART). ART ditulis guna melaksanakan sebagian mesin virtual pada fitur bermemori rendah dengan mengeksekusi file DEX, format bytecode yang dirancang spesial buat Android yang dimaksimalkan buat footprint memori minimun. Membuat Kerangka aplikasi, misalnya Jack, mengumpulkan sumber Java ke bytecode DEX, yang bisa berjalan pada platform Android. Beberapa fitur utama Kompilasi mendahului waktu (AOT) dan tepat waktu (JIT), Pengumpulan sampah (GC) yang dioptimalkan, dan Dukungan debugging yang lebih baik, mencakup profiler penyampelan terpisah, pengecualian diagnostik mendetail serta laporan kehancuran atau keahlian buat pengaturan titik pantau guna memantau bidang tertentu.

4. Libraries C/C++

Banyak komponen dan layanan sistem Android inti seperti ART dan HAL dibuat dari kode bawaan yang memerlukan pustaka bawaan yang tertulis dalam C dan C++. Platform Android membolehkan kerangka kerja API Java tingkatkan guna sebagian pustaka bawaan pada aplikasi. Misalnya, bisa mengakses OpenGL ES lewat kerangka kerja API OpenGL Java Android guna meningkatkan suport buat menggambar serta memanipulasi grafik 2D dan 3D pada aplikasi.

5. Framework API Java

Keseluruhan rangkaian fitur pada Android OS tersedia untuk melalui API yang ditulis dalam bahasa Java. API ini membentuk elemen dasar yang harus buat aplikasi Android dengan

menyederhanakan konsumsi ulang, komponen dan layanan sistem modular, yang mencakup berikut ini:

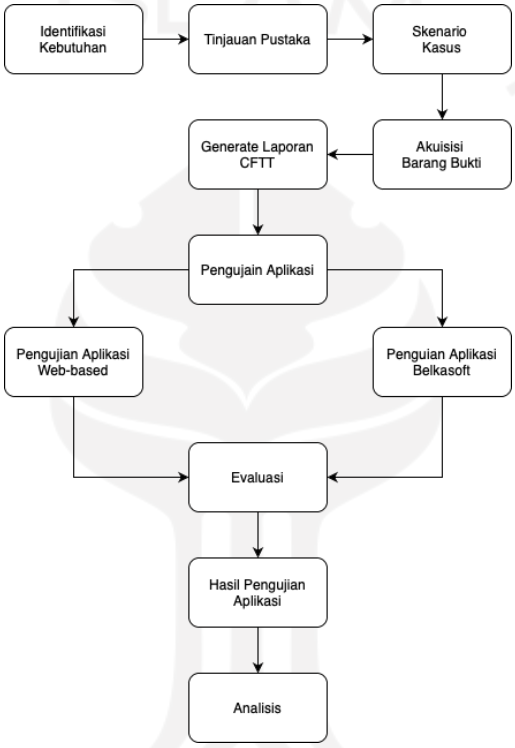
- Tampilan Sistem yang kaya dan luas dapat digunakan untuk membuat UI aplikasi, termasuk daftar, isi, kotak teks, tombol, dan bahkan browser web yang dapat disematkan.
- Pengelola Sumber Daya, memberikan akses ke sumber daya bukan kode seperti string yang dilokalkan, grafik, dan file layout.
- Pengelola Notifikasi yang mengaktifkan semua aplikasi guna menampilkan lansiran khusus pada bilah status.
- Pengelola Aktivitas yang mengelola siklus hidup aplikasi dan memberikan back-stack navigasi yang umum.
- Penyedia Materi yang memungkinkan aplikasi mengakses data dari aplikasi lainnya, seperti aplikasi Kontak, atau untuk berbagi data milik sendiri.

6. Aplikasi Sistem

Android dilengkapi dengan serangkaian aplikasi inti buat email, pesan SMS, kalender, menjelajahi internet, kontak dll. Aplikasi yang diiringi dengan platform tidak mempunyai status spesial pada aplikasi yang pengguna kepingin instal. Jadi, aplikasi pihak ketiga bisa jadi browser website utama, pengolah pesan sms ataupun apalagi keyboard utama (sebagian pengecualian berlaku, semacam aplikasi Settings sistem). Aplikasi sistem berperan selaku aplikasi buat pengguna serta membagikan kemahiran kunci yang bisa diakses oleh pengembang dari aplikasi mereka sendiri. Misalnya, jika aplikasi ingin mengirimkan pesan sms, tidak perlu membangun fungsi tersebut bisa juga menjalankan aplikasi sms mana saja yang telah diinstal guna mengirimkan pesan kepada penerima yang dicantumkan.

# BAB 3
# Metodologi

Bab ini menjelaskan desain dan metode yang digunakan dalam penelitian, tentang urutan langkah-langkah yang dibuat secara sistematis dan dapat dijadikan sebagai pedoman yang jelas dalam penyelesaian masalah. Adapun langkah-langkah pada penelitian ini dapat dilihat pada gambar 3.1.




Gambar 3.1 Alur penelitian.

Pada gambar 3.1 menjelaskan terkait alur kerja penelitian yang digunakan untuk melakukan pengujian terhadap aplikasi web-based. Alur penelitian ini bertujuan untuk menguji aplikasi web-based dan belkasoft berdasarkan standar CFTT yang didasarkan pada laporan pengujian *deferated testing*. Hasil laporan pengujian kedua aplikasi akan dievaluasi dan membandingan kedua data dengan parameter yang ada pada standar CFTT, dari hasil evaluasi tersebut memperlihatkan kemampuan kedua aplikasi terhadap data yang dihasilkan.

## 3.1 Identifikasi Kebutuhan

Identifikasi kebutuhan merupakan tahapan yang menjelaskan tentang kebutuhan yang digunakan dalam penelitian. Pada tahap ini dilakukan *profiling* pada perangkat *smartphone* sebagai alat uji. Hasil tahapan ini digunakan untuk mengetahui dukungan alat forensik

terhadap *smartphone* dan mengetahui jumlah data yang digunakan untuk perbandingan data hasil akuisisi.

### 3.2 Tinjauan Pustaka

Tinjauan pustaka merupakan tahap untuk mengkaji dan mempelajari berbagai sumber literatur dan teori-teori yang mendukung tentang penelitian yang dilakukan. Sumber pembelajaran pada studi pustaka dapat bersumber dari jurnal, paper, artikel, buku-buku, website, dan sumber pembelajaran lainnya yang membahas berkaitan tentang, *computer forensics tools testing, federated testing,* dan validasi aplikasi forensik.

### 3.3 Skenario Kasus

Pada skenario kasus menjelaskan tentang bagaimana melakukan pengujian aplikasi web-based dan belkasoft yang didasarkan pada standar CFTT. pengujian ini lebih difokuskan pada aplikasi web-based karena aplikasi web-based merupakan aplikasi yang dikembangkan sendiri oleh mahasiswa universitas islam indonesia, yang akan diuji berdasarkan standar CFTT, sedangkan aplikasi belkasoft hanya digunakan sebagai perbandingan data untuk mengukur performa dari aplikasi web-based, hasil dari kedua pengujian ini kemudian dibandingkan dengan parameter yang ada pada standar CFTT untuk mengevaluasi parameter apa saja yang mampu dihasilkan oleh aplikasi web-based. Skenario dalam penelitian ini dimulai dari melakukan akuisisi data di perangkat *smartphone*, melakukan generet laporan standar CFTT pada aplikasi federated testing, sampai dengan proses pengujian aplikasi web-based dan belkasoft. pada skenario ini dibagi menjadi empat tahap yaitu:

1. Skenario pertama

Pada skenario pertama yaitu berkaitan dengan proses akuisisi perangkat *smartphone*. akuisisi ini bertujuan untuk membuat file image dari perangkat smartphone sesuai dengan prosedur forensik. file image tersebut akan digunakan sebagai bahan pengujian pada aplikasi web-based. perangkat yang digunakan dalam proses pembuatan file image adalah *smartphone* evercoss s50d. sebelum melakukan akuisisi dilakukan beberapa persiapan seperti rooting dan mengaktifkan fitur debugging di perangkat smartphone, selanjutnya melakukan proses akuisisi dengan menghubungkan kabel usb dari perangkat smartphone ke komputer, jika kedua perangkat berhasil terhubung, berikutnya melakukan proses akuisisi file image dari smartphone ke komputer menggunakan tools adb.

2. Skenario kedua

Pada skenario kedua adalah membuat laporan standar CFTT pada aplikasi federated testing. Pembuatan laporan tersebut dimulai dengan menginstal beberapa dependensi yang

dibutuhkan pada sistem operasi linux, federated testing ini berjalan pada sistem operasi linux, laporan standar ctff memberikan kebutuhan yang harus diterapkan pada setiap aplikasi forensik, pada kasus ini kebutuhan tersebut akan di implementasi pada aplikasi web-based dengan mengevaluasi apakah kebutuhan tersebut sudah bisa dipenuhi oleh aplikasi web-based atau tidak, hal ini akan terjawab ketika dilakukan pengujian aplikasi web-based. Untuk membuat laporan standar CFTT dapat mengakses halaman federated testing yang sudah diinstal sebelumnya, kemudian akan mendapatkan interface dari federated testing itu sendiri. Jelaskan pembuatan laporan CFTT berdasarkan langkah-langkah yang suda terdapat pada aplikasi tersebut, jika langkah-langkah tersebut berhasil maka akan secara otomatis aplikasi federated testing akan men generate sebuah laporan standar CFTT untuk diimplementasikan pada aplikasi web-based.

3. Skenario ketiga

Pada skenario ketiga adalah proses pengujian aplikasi. Pengujian dalam skenario ini dibagi menjadi dua yang pertama adalah skenario pengujian aplikasi web-based dan pengujian belkasoft, pengujian web-based dilakukan untuk menguji kemampuan dari aplikasi web-based berdasarkan aturan yang dijelaskan pada flowchart pada gambar 4.2 output dari hasil pengujian ini berupa data-data yang berkaitan dengan barang bukti digital pada perangkat smartphone. namun pada pengujian ini lebih ditekankan pada parameter yang didapatkan dari aplikasi web-based itu sendiri, yang mana parameter tersebut kemudian akan evaluasi berdasarkan parameter pada standar CFTT. Aplikasi *web based android analysis tools* ini berjalan pada sistem operasi linux ubuntu 18.04. proses awal dalam pengujian aplikasi ini adalah dengan menginstal beberapa dependensi yang dibutuhkan oleh aplikasi seperti python 2.7, python-pip, moka, biplist, magic dan cherrypy. setelah kebutuhan sudah terpenuhi maka selanjutnya menjalankan aplikasi dengan mengakses domain local server di web browser (localhost:8080) maka akan mendapatkan interface dari aplikasi *web based android analysis tools*. untuk proses pengujian aplikasi pertama-tama yang harus dilakukan adalah melakukan mount file image yang sudah diakuisisi sebelumnya ke direktori mounting, ini bertujuan agar aplikasi *web based android analysis tools* bisa membaca atau mengeksekusi file tersebut. yang kedua membuat sebuah new case pada aplikasi kemudian input beberapa field yang diminta seperti nama kasus, actor, komentar dan direktori file mount yang sudah dibuat sebelumnya. selanjutnya mengeksekusi dengan klik tombol proses maka aplikasi maka akan menampilkan hasil pengujian.

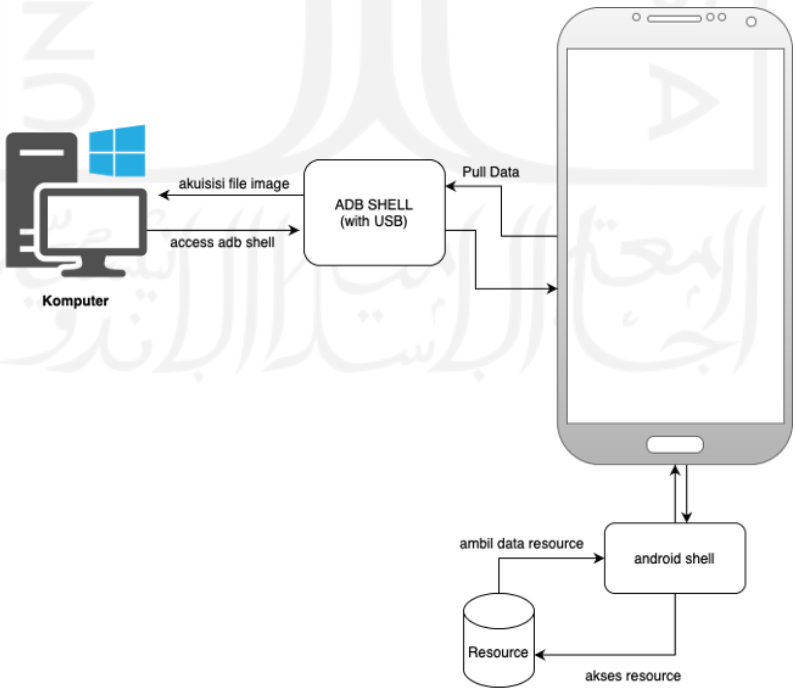
Sedangkan pengujian aplikasi belkasoft merupakan pengujian yang digunakan untuk mendukung pengujian aplikasi web-based yang hanya dilakukan untuk membandingkan

hasil dari pengujian web-based, pengujian tersebut bertujuan untuk menjawab apakah implementasikan CFTT pada aplikasi web-based sudah sesuai dengan parameter yang ada pada standar CFTT atau tidak berdasarkan hasil yang didapatkan dari pengujian. Proses pengujian aplikasi belkasoft akan dimulai dengan menginstal aplikasi pada sistem operasi windows, setelah sumua kebutuh berhasil dijalankan maka aplikasi dapat digunakan untuk melakukan pengujian barang bukti digital dengan memilih file yang akan dianalisis.

4. Evaluasi

Evaluasi merupakan bagian akhir yang memperlihatkan hasil pengujian aplikasi belkasoft dan aplikasi web-based dimana kedua hasil tersebut dievaluasi untuk mencari parameter apa saja yang tidak dihasilkan oleh aplikasi web-based. Karena kemampuan dari aplikasi rendah dibandingkan aplikasi belkasoft, sehingga perlu dievaluasi untuk mengetahui kemampuan terhadap aplikasi web-based. setelah mengetahui parameter yang dihasilkan oleh aplikasi web-based kemudian parameter tersebut akan disesuaikan dengan parameter dari standar CFTT. Parameter yang yang diukur dalam hasil pengujian kedua aplikasi adalah parameter call log, data file, network connection, sms message, browser/email data, address book entitas, data contact location data dan mms massage. data-data yang disebutkan merupakan fungsional kebutuhan standar CFTT yang mengharuskan setiap aplikasi forensik menerapkan kebutuhan tersebut.

## 3.4 Akuisisi Barang Bukti




Gambar 3.2 Akuisisi barang bukti smartphone.

Akuisisi barang bukti merupakan proses kloning atau imaging barang bukti digital dari perangkat *smartphone*. pada gambar di atas menjelaskan tentang simulasi atau alur kerja bagaimana melakukan akuisisi perangkat smartphone menggunakan android debugging bridge (ADB). untuk melakukan ekstraksi atau cloning data komputer akan mengakses adb shell yang terhubung melalui kabel usb ke perangkat smartphone kemudian pada android shell akan mengakses resource dari perangkat smartphone sesuai dengan perintah dan parameter yang digunakan pada adb shell, adb shell akan mengambil data dari resource smartphone dan mentransfer atau melakukan pull data ke adb shell dengan destinasi ke perangkat komputer, data yang ditransfer ke komputer ini berupa sebuah file image dengan format dd. file tersebut kemudian dijadikan sebagai bahan pengujian pada aplikasi *web based android analysis tools*.

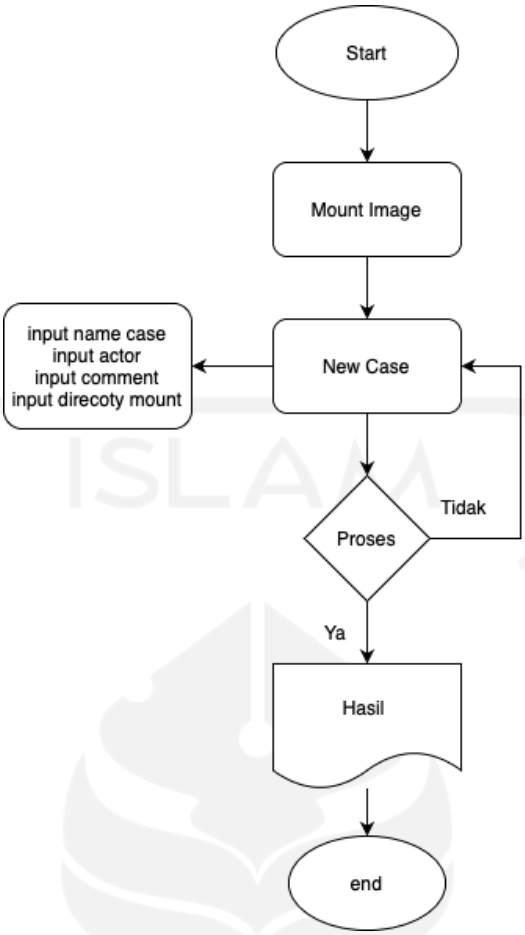
### 3.5 Geberate Standar CFTT

Generate parameter fungsional kebutuhan standar CFTT pada aplikasi federated testing untuk menghasilkan sebuah laporan umum yang menampilkan kebutuhan-kebutuhan yang direkomendasikan untuk diterapkan pada setiap aplikasi forensik, dalam kasus ini parameter pada CFTT ini akan diimplementasikan pada aplikasi web-based untuk mengevaluasi parameter apa saja yang bisa dihasilkan oleh aplikasi web-based sesuai dengan parameter yang ada pada standar CFTT. jika parameter dari hasil pengujian aplikasi web-based ini belum terpenuhi sesuai dengan yang ada di CFTT maka akan diberikan sebuah rekomendasi perbaikan aplikasi terhadap parameter tersebut, sehingga diharapkan aplikasi web-based ini bisa digunakan untuk keperluan mobile forensik.

### 3.6 Pengujian

Pengujian dilakukan secara bertahap dengan memastikan tiap tahap bekerja sesuai dengan yang diharapkan. Ada dua proses pengujian diantaranya:

1. forensik perangkat bergerak




Gambar 3.3 Alur aplikasi *web based android analysis tools*

Gambar 3.3 menjelaskan tentang alur proses pengujian aplikasi secara bertahap, dimulai dari proses mounting file image sampai dengan hasil pengujian aplikasi. Pengujian mobile forensik merupakan sebuah proses untuk menguji kemampuan aplikasi secara fungsional kebutuhan yang digunakannya. Kemudian hasil dari pengujian aplikasi ini akan dibandingkan dengan hasil dari pengujian aplikasi belkasoft yang mana pada hasil aplikasi web-based ini kemudian dievaluasi menggunakan pendekatan kebutuhan fungsional dari standar CFTT, pendekatan ini dilakukan untuk menganalisis kemampuan dari aplikasi web-based untuk meninjau apakah kebutan yang digunakan aplikasi web-based saat ini sudah sesuai dengan kebutuhan yang direkomendasikan oleh CFTT. sedangkan untuk perbandingan aplikasi belkasoft ini hanya menguatkan bahwa fungsional kebutuhan yang ada pada standar CFTT itu harus diterapkan pada aplikasi web-based, karena sebelumnya aplikasi belum diuji berdasarkan standar CFTT sehingga peneliti melakukan sebuah pengujian ini untuk mengevaluasi kemampuan dari aplikasi tersebut dan untuk memberikan rekomendasi terhadap pengembangan aplikasi. Sehingga output dari pengujian diharapkan aplikasi tersebut bisa digunakan oleh ahli forensik maupun laboratorium forensik dalam menangani sebuah kasus.

2. Pengujian Aplikasi Belkasoft

Pengujian aplikasi belkasoft merupakan sebuah proses yang dilakukan untuk mendukung pengujian aplikasi web-based dengan memberikan data hasil pengujian untuk membandingkan data tersebut dengan hasil pada aplikasi web-based berdasarkan standar CFTT. pengujian aplikasi belkasoft ini bertujuan untuk mendukung penerapan standar CFTT pada aplikasi web-based tentang bagaimana aplikasi tersebut di uji dan mengevaluasi hasil yang didapatkan dan ditinjau untuk pengembangan berikutnya, sehingga output pada aplikasi web-based ini bisa digunakan oleh ahli forensik dan laboratorium forensik

### 3.6 Evaluasi

Proses ini dilakukan untuk mengevaluasi hasil yang didapatkan dari aplikasi web-based dan aplikasi belkasoft dimana pada setiap aplikasi ini akan dilihat data apa saja yang dihasilkan oleh aplikasi kemudian mengevaluasi hasil yang didapatkan.

### 3.7 Hasil Pengujain Aplikasi

Pada tahap ini akan memberikan hasil pengujian aplikasi web-based dan aplikasi belkasoft dari hasil evaluasi. Hasil pengujian aplikasi tersebut menampilkan data yang mana setiap data yang didapatkan dari aplikasi web-based dan belkasoft ini diverifikasi dengan data parameter yang ada pada laporan standar CFTT, penerapan CFTT pada aplikasi web-based memperlihatkan hasil dari kedua aplikasi tersebut yang mana memiliki karakteristik tersendiri terhadap data yang dihasilkan.

### 3.8 Analisis

Analisis merupakan bagian dari prosedur pengujian aplikasi yang menganalisis hasil dari pengujian aplikasi dengan pendekatan standar CFTT. pengujian aplikasi web-based ini akan memberikan hasil laporan pengujian tentang parameter yang dihasilkan. Parameter tersebut akan disesuaikan dengan kebutuhan yang ada pada standar CFTT untuk mengevaluasi karakteristik data apa saja yang dihasilkan. Untuk memperkuat CFTT pada aplikasi web-based maka hasil pengujian aplikasi web-based akan dibandingkan lagi dengan pengujian belkasoft.

# BAB 4
# Hasil dan Pembahasan

Bab ini membahas hasil penelitian yang dijelaskan proses pengujian aplikasi mobile forensik berdasarkan diagram alur penelitian yang ada pada bab tiga, dimulai dari identifikasi perangkat, studi literatur, akuisisi data, pengujian damapi pada laporan pengujian. Penelitian ini dilakukan dengan dua tahap pengujian yaitu pengujian aplikasi *web based android analysis tools* dan pengujian aplikasi belkasoft menggunakan standar CFTT.

## 4.1 Identifikasi Perangkat

Identifikasi Perangkat merupakan langkah awal mengidentifikasi perangkat dan beberapa kebutuhan yang digunakan dalam pengujian aplikasi *web based android analysis tools*. Pada tahap ini dilakukan *profiling* pada perangkat *smartphone* sebagai alat uji. beberapa kebutuhan yang digunakan dalam pengujian baik itu perangkat keras maupun perangkat lunak sebagai berikut.

Tabel 4.1 Kebutuhan perangkat keras.

| No | Nama Perangkat Keras | Keterangan |
|---|---|---|
| 1 | Lenovo thinkpad<br>Prosesor i5<br>Ram 4 Gb | Digunakan untuk menginstal aplikasi web base |
| 2 | Lenovo Ideapad 330s<br>Prosesor i5<br>Ram 12 Gb | Digunakan untuk menginstal aplikasi federated testing |

Tabel 4.2 Kebutuhan perangkat lunak.

| No | Nama perangkat lunak | Keterangan |
|---|---|---|
| 1 | Linux Ubuntu 18.04 | Digunakan untuk menjalankan aplikasi web based |
| 2 | Windows 10 | Os Lenovo ideapad 330s |
| 3 | Linux ubuntu 14.04 | Os Federated Testing |
| 4 | Virtual Box | Digunakan untuk menginstal *federated testing* |

## 4.2 Akuisisi Data

Akuisisi merupakan proses untuk mendapatkan data, khususnya pada perangkat *smartphone* yang digunakan sebagai bahan pengujian. Ada tiga Teknik akuisisi yang biasa digunakan dalam proses pengumpulan bukti digital. diantaranya *physical extraction, logical extraction,* dan *file system extraction*. *Physical extraction* merupakan salinan bit by bit dari seluruh flash memori dari perangkat mobile dimana dengan teknik ini memungkinkan akuisisi secara utuh

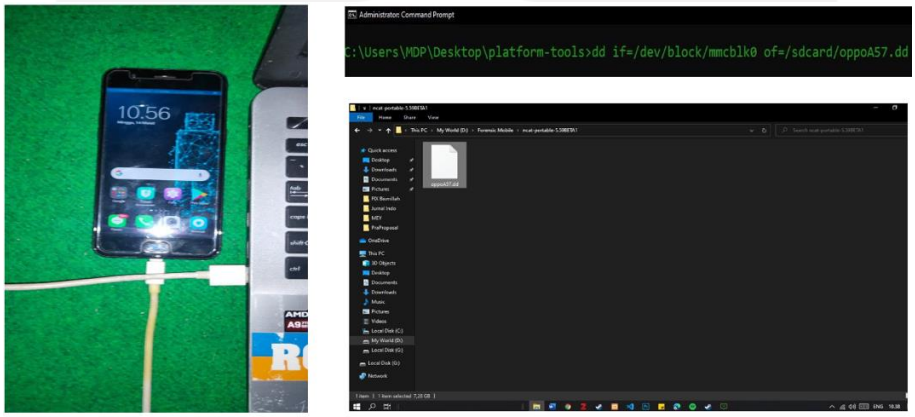
terhadap file yang disembunyikan atau terhapus. *Logical extraction* merupakan akuisisi dalam perangkat mobile dengan bit for bit pada logical storage yang mencakup file dan direktori yang berada pada logical storage (file system). Akuisisi ini memungkinkan struktur data system lebih mudah untuk di extract dan diatur. File System Extraction, berikutnya, ialah akuisisi terhadap file yang ada dalam memori fitur mobile dimana dengan metode ini membolehkan kita buat memperoleh akses seluruh file yang terdapat didalam memori fitur mobile( alokasi ruang), didalamnya terdapat foto, video, database file, sistem file serta log.

Proses pembuatan file image ini dilakukan menggunakan perangkat *smartphone* tipe oppo A57. Perangkat tersebut akan dilakukan rooting terlebih dahulu agar bisa mengakses semua *resource* yang ada pada perangkat. Setelah perangkat tersebut berhasil di root maka selanjutnya akan dilakukan proses imaging menggunakan beberapa tools seperti android debugging bridge (ADB), busybox, dan netcut.

Tabel 4.3 Tools akuisisi barang bukti.

| Nama Tools | Ket |
|---|---|
| Android Debugging Bridge (ADB) | Tools akuisisi |
| Busybox | Tools tambahan |
| Netcut | Tools Tambahan |

Langkah-langkah dalam pembuatan file image pada *smartphone* oppo a57 dimulai dengan mengaktifkan fitur *debugging* pada *smartphone*. Langkah selanjutnya adalah menyambungkan *smartphone* ke komputer melalui kabel USB. Setelah kedua perangkat berhasil dihubungkan maka selanjutnya membuat image file dengan perintah sebagai berikut sesuai dengan gambar 4.1.




Gambar 4.1 Perintah akuisi data *smartphone*.

Pada gambar 4.1 menjelaskan hasil proses akuisisi data *smartphone* oppo a57 dengan menggunakan beberapa perintah dan parameter untuk membuat sebuah file image

yang di ekstrak dari perangkat smartphone ke komputer. hasil ini kemudian dijadikan sebagai bahan pengujian aplikasi *web based android analysis tools*. dalam proses pengujian terdapat dua data yang akan digunakan sebagai bahan pengujian yaitu data dari smartphon oppo a57 dan data dari smartphon evercross, seperti yang ditunjukan pada gambar 4.2.

Tabel 4.4 File Image smartphone

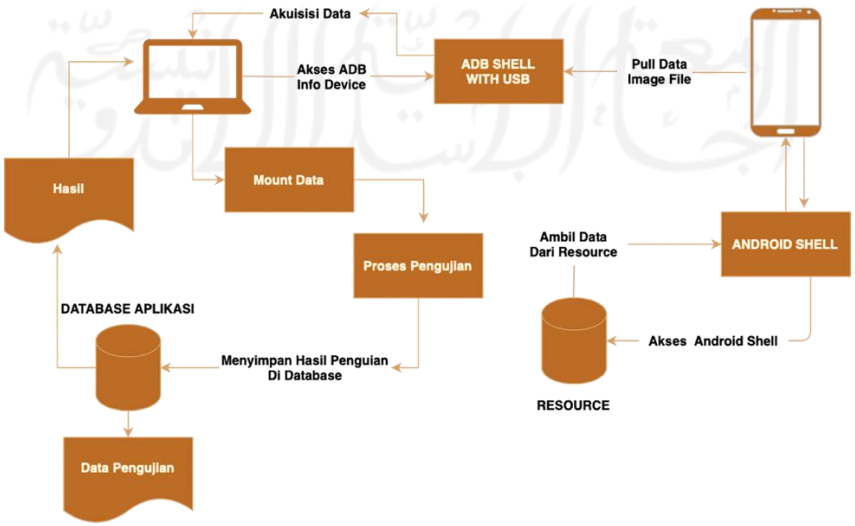
| Nama File Image | Keterangan |
|---|---|
| Oppo A57.dd | Akuisisi dari smartphone Oppo A57 |
| s50dv3.dd | Akuisisi dari smartphone Evercross s50 |

## 4.3 Pengujian

Pada proses pengujian merupakan bagian yang menjelaskan tentang tahapan proses pengujian. Ada dua tahapan pengujian aplikasi diantaranya pengujian web based android analysis tools dan pengujian mobile belkasoft kedua pengujian tersebut diuji berdasarkan standar CFTT yang mana setiap data dari hasil pengujian akan dibandingkan dengan parameter pada fungsional kebutuhan dari CFTT, output dari pengujian aplikasi web-based ini adalah untuk mengevaluasi dan merekomendasikan perbaikan jika terdapat parameter yang belum sesuai dengan standar CFTT, sehingga diharapkan bisa digunakan oleh ahli forensik dan laboratorium forensik.

### 4.3.1 Pengujian Forensik Perangkat Bergerak.

Gambaran umum proses pengujian aplikasi merupakan sebuah skema atau visualisasi yang dapat menggambarkan bagaimana proses pengujian aplikasi *web based android analysis tools* ini dilakukan di dalam sistem dan keterkaitan dengan entitas luarnya. Gambaran umum pengujian aplikasi *web based android analysis tools* dapat dilihat pada gambar 4.3.




Gambar 4.2 Workflow *web-based android analysis tools*.

Gambar 4.2 menggambarkan bagaimana aplikasi *web based android analysis tools* bekerja. Aplikasi berjalan pada perangkat komputer dengan sistem operasi linux ubuntu 18.4, dan untuk melakukan proses pengujian, dibutuhkan sebuah file image dari perangkat *smartphone* sebagai bahan pengujian aplikasi. Proses pembuatan file image suda di jelaskan pada poin akuisisi data.

1. Mount Data

Pada tahap ini merupakan proses untuk melakukan *mount* data dari file image yang sudah di akuisisi sebelumnya, tujuannya agar aplikasi *web based android analysis tools* ini dapat membaca dan mengeksekusi file image ke dalam aplikasi tersebut. proses *mount* data menggunakan perintah sebagai berikut, sesuai pada gambar 4.4.

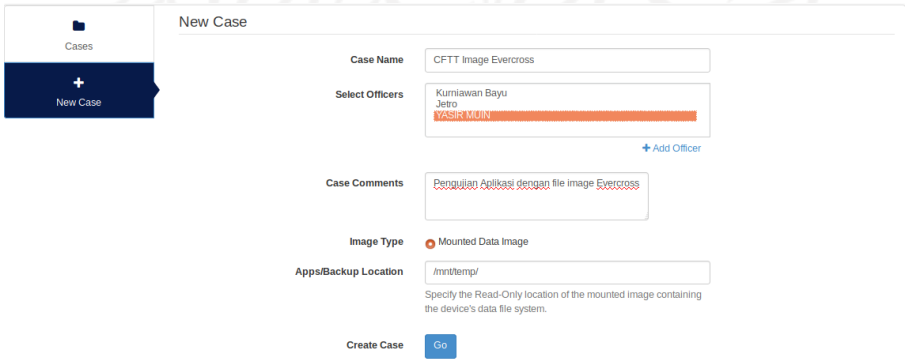
```
root@fd:/home/xcode/Documents# mount s50dv3.dd /mnt/temp/
root@fd:/home/xcode/Documents#
```

Gambar 4.3 Mount file image.

Pada gambar 4.3 merupakan perintah untuk melakukan *mount* data dari file image s50dv3 ke direktori /mnt/temp/, pada perintah diatas terlihat bahwa proses *mount* berhasil dijalankan, maka semua data pada file s50dv3 ini akan dipindahkan ke direktori /mnt/temp/ sebagai hasil *mount*. Setelah proses *mount* berhasil maka selanjutnya masuk ke tahap berikutnya yaitu proses melakukan pengujian aplikasi *web based android analysis tools*.

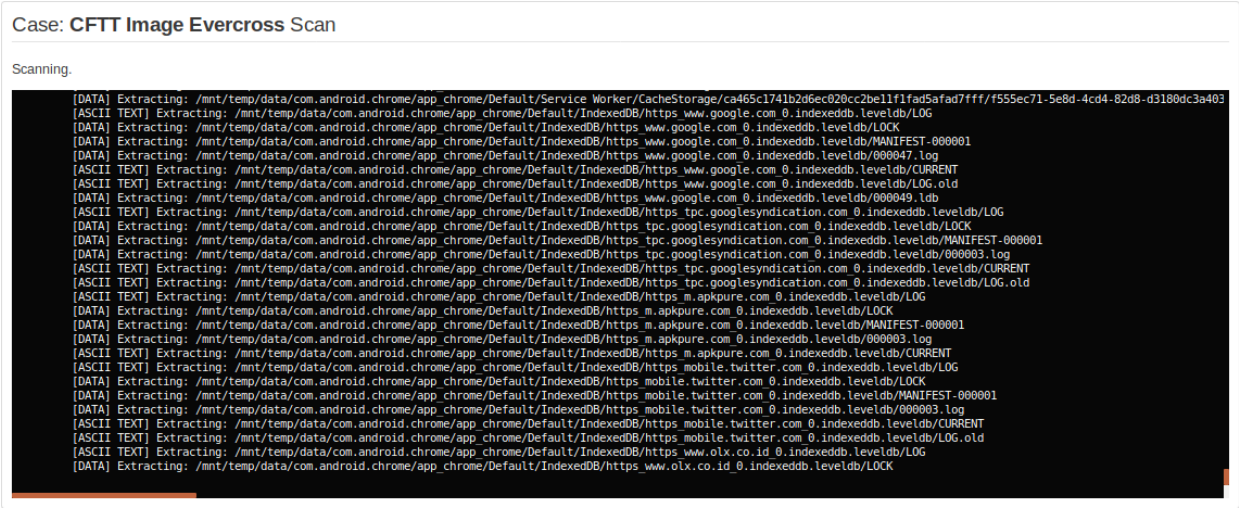
2. Proses Pengujian.

Pada tahap ini merupakan proses pengujian aplikasi *web based android analysis tools*, langkah awal dalam proses ini adalah pembuatan sebuah *new case* pada aplikasi, kemudian menginput beberapa *field* yang diminta seperti nama kasus, nama aktor, komentar pada kasus jika ingin ditambahkan, dan lokasi direktori *file image* yang di *mount* sebelumnya. untuk detailnya dapat dilihat pada gambar 4.4.




Gambar 4.4 *New case* pada aplikasi.

Setelah membuat *new case* pada aplikasi dengan menginput beberapa *field* yang ada pada gambar 4.5. data tersebut akan diproses setelah mengklik tombol proses pada *button* aplikasi. jika berhasil maka aplikasi akan *scanning* seluruh data *mount* yang ada pada direktori /mnt/temp/, dalam proses ini membutuhkan waktu beberapa menit untuk *scanning* data. kemudian akan ditampilkan pada halaman aplikasi. Sesuai pada gambar 4.5.




Gambar 4.5 Proses scanning data.

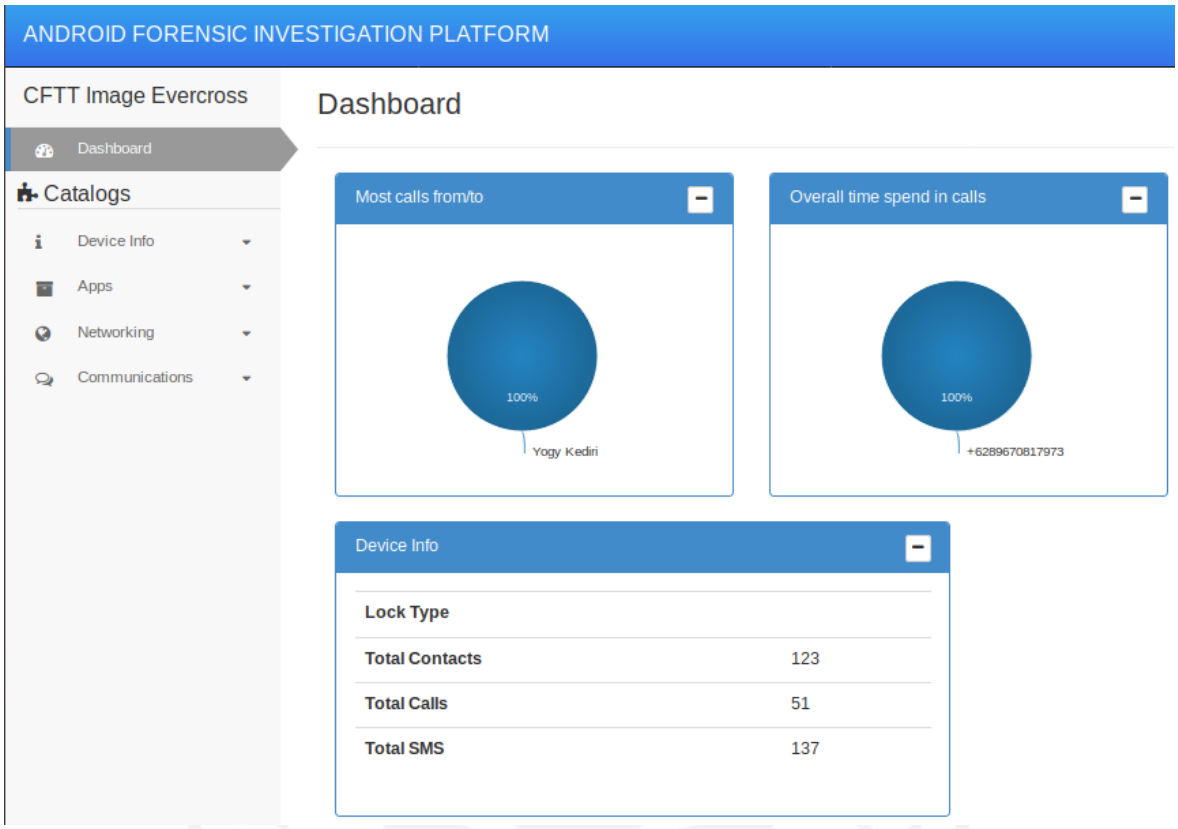
Setelah proses *scanning* selesai, maka hasil pengujian aplikasi akan ditambahkan pada halaman home aplikasi *web based android analysis tools* seperti pada gambar 4.6.


Gambar 4.6 Tambahkan *new case* pada aplikasi.

Pada gambar 4.7 merupakan hasil dari proses pengujian aplikasi yang dihasilkan dari data sebuah file akuisisi file image dari perangkat *smartphone*, untuk melihat hasil apa saja yang didapatkan oleh aplikasi yaitu dengan menekan tombol view seperti yang terlihat di gambar 4.6. hasil pengujian dikategorikan dalam beberapa kategori yaitu device info, apps, *networking* dan *communication* yang memuat data-data dari sebuah file image perangkat smartphone seperti berikut:

a. Halaman Dashboard

Pada halam dasbor ini menampilkan beberapa informasi grafik dan statistik dari seluruh yang dihasilkan, seperti pada gambar gambar 4.7.

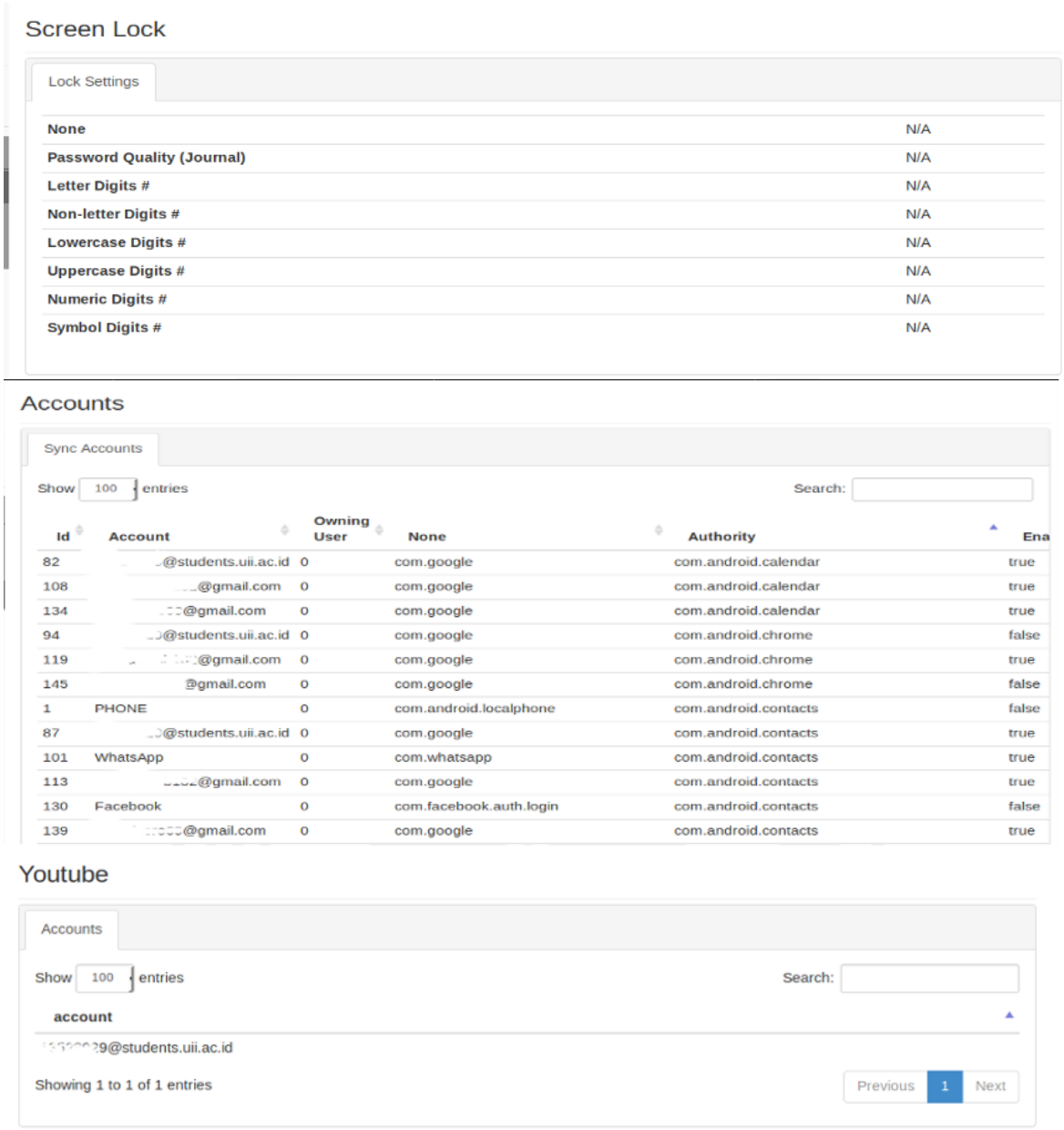



Gambar 4.7 Halaman dashboard.

Pada gambar 4.7 dapat dilihat bahwa hasil pengujian ditampilkan dalam bentuk grafik dan tabel, terdapat tiga poin di halaman utama yaitu *devices info, most call phone,* dan *overall time span in call*. Device info mencatat total kontak yang dihasilkan dari aplikasi sebanyak 129, total panggilan 51, dan total sms 137, sedangkan pada tampilan grafik dijelaskan pada *most call phone* atau panggilan yang paling sering atas nama yogi kediri dan pada *overall time span in call* atau panggilan yang paling lama tercatat adalah kontak +6289670817973.

b. Device Info

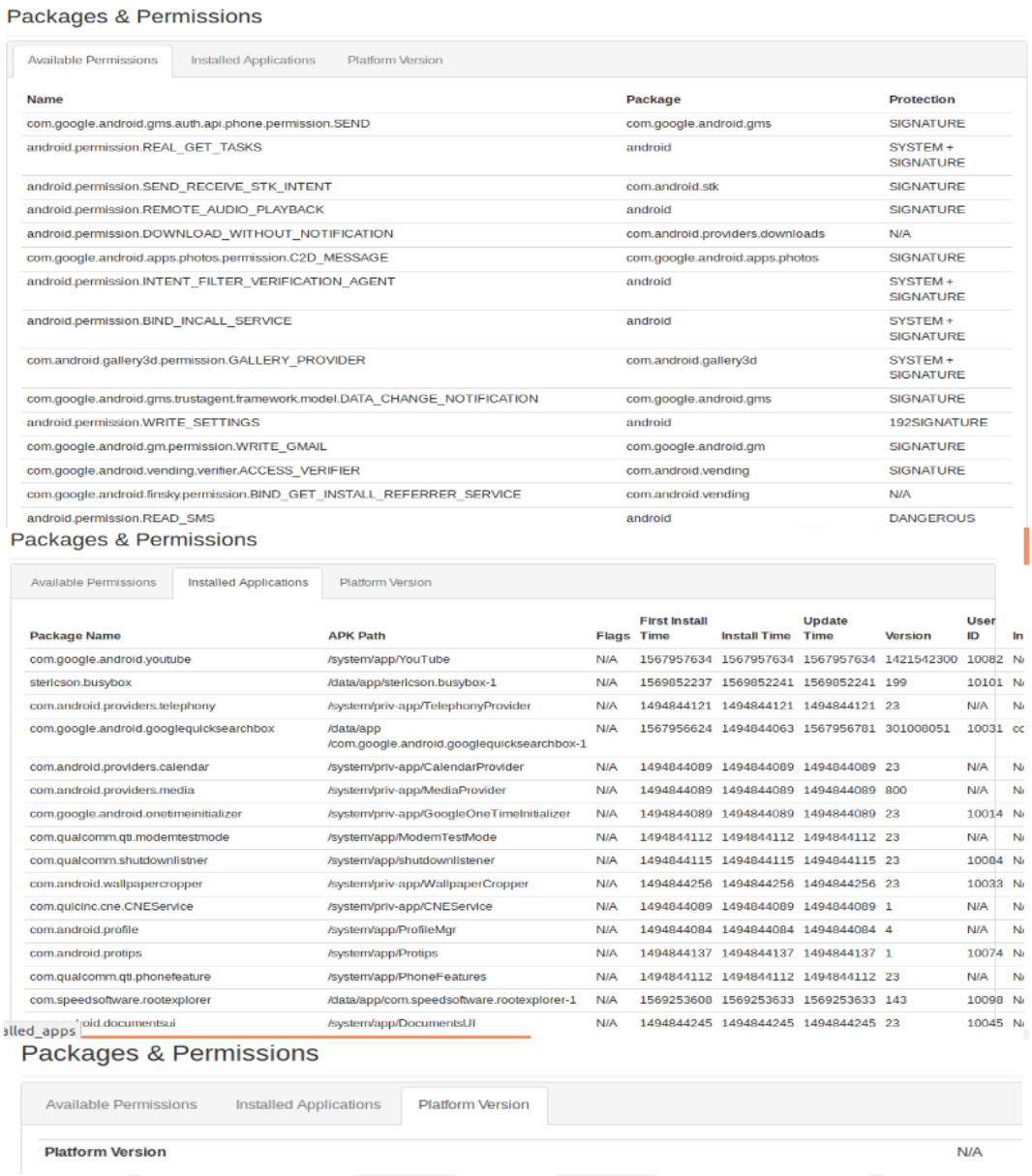
Pada device info menampilkan beberapa informasi seperti *screen lock*, youtube, dan *accounts*, setiap poin yang menyimpan informasi masing seperti yang ada pada poin *screen lock* ini, memyimpan informasi tentang *security quality (journal), letter digits, lowercase digits, numeric digits*, dan *symbol digits*. Pada point *youtube* menampilkan informasi tentang account youtube, dan terakhir pada poin accounts memuat informasi tentang akun-akun yang tersinkronisasi dengan aplikasi, semua informasi tersebut dapat dilihat pada gambar 4.8.




Gambar 4.8 Hasil dari device info.

c. Apps

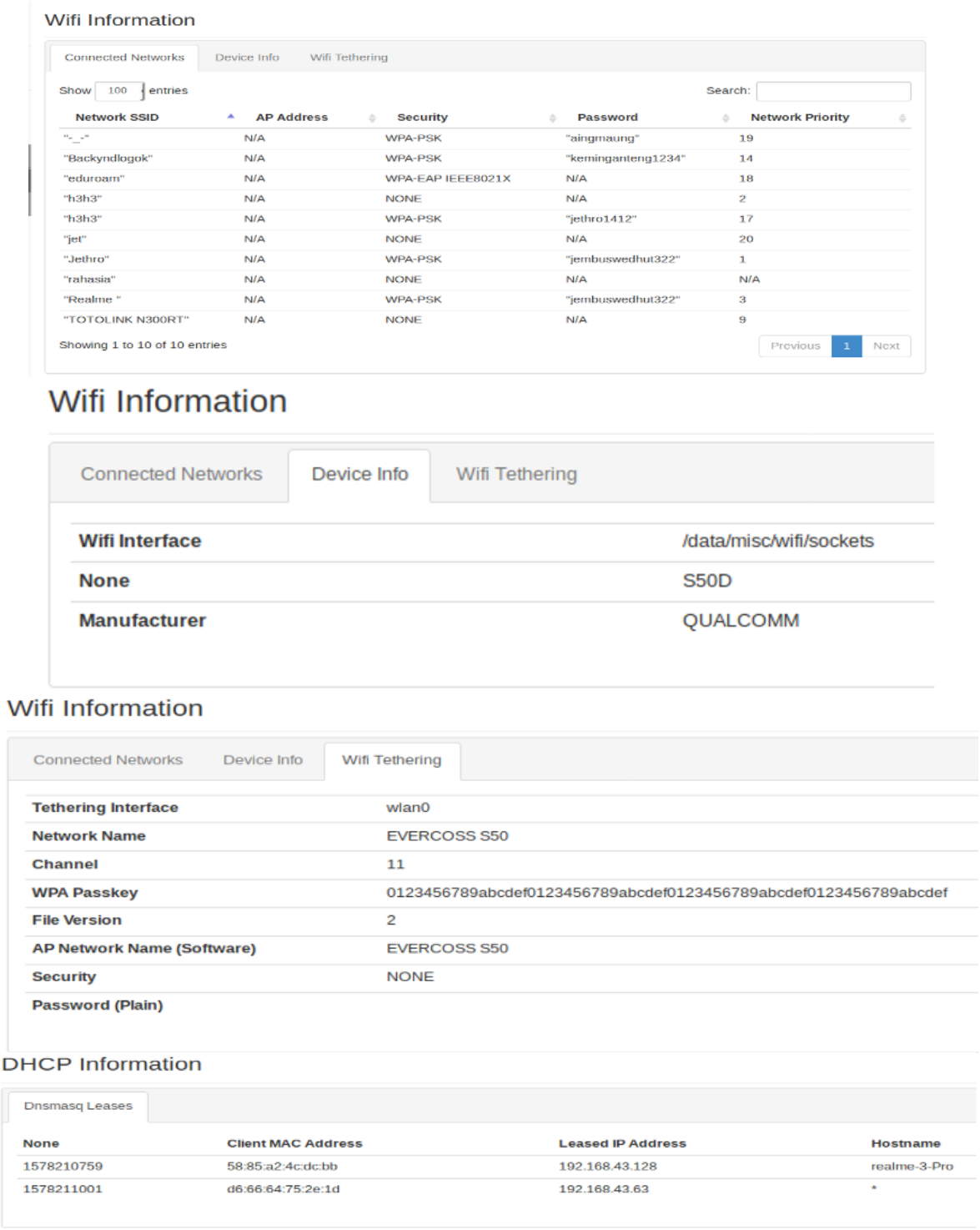
Pada kategori apps merupakan bagian aplikasi yang menyimpan informasi paket dan permission. Di dalam *packet* dan *permission* terdapat tiga kategori data diantaranya *available permission, instalasi aplikasi dan platform version*. Pada *available permission* ini menampilkan informasi tentang hak akses dari setiap paket dan aplikasi yang ada di *resource smartphone*, sedangkan pada *installation application* menampilkan seluruh informasi dari setiap aplikasi yang di install di dalam perangkat *smartphone*. Dan untuk *platform version* berisi informasi tentang versi dari *smartphone*, tetapi pada bagian aplikasi tidak dapat menampilkan versi dari aplikasi *smartphone*. Untuk lebih jelasnya dapat dilihat pada gambar 4.9.




Gambar 4.9 Hasil dari apps.

d. Networking

Pada bagian networking terdapat dua kategori yaitu *wifi information* dan *DHCP information*. Kedua kategori ini masing-masing menampilkan informasi terkait history dari perangkat smartphon yang konek ke jaringan komputer, data yang ditampilkan berupa informasi *SSID*, *security*, *password*, *mac address*, dan *ip address*. Seperti pada gambar 4.10.




Gambar 4.10 Hasil dari bagian network.

e. Communication

Pada bagian *communication* menampilkan informasi terkait dengan data panggilan telepon, internet chat, dan kontak, data panggilan telepon ada dua bagian yaitu informasi tentang history panggilan dan sms, sedangkan pada internet chat menampilkan informasi berupa chat

messenger facebook dan chat whatsapp, yang terakhir kontak, berisi informasi tentang kontak hp yang tercatat pada *smartphone*, dan kontak whatsapp. Seperti pada gambar 4.11.

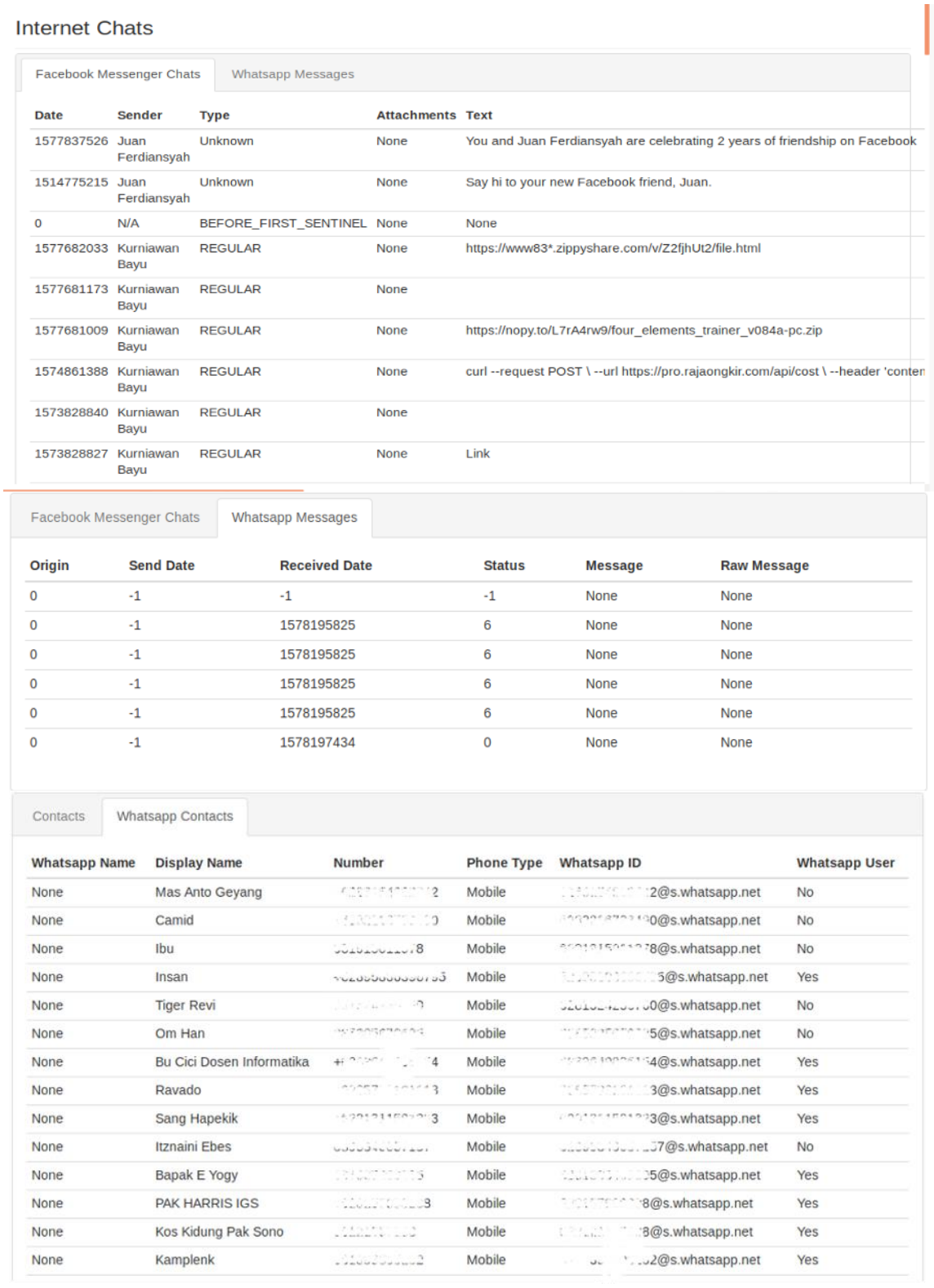
Telephony

Calls | SMS Messages

| Date | Type | Number | Contact | Duration (seconds) | Number Geolocation |
|---|---|---|---|---|---|
| 1570627201 | Incoming | [redacted] | None | 5 | Indonesia |
| 1570672659 | Missed | [redacted] | None | 0 | Greater Jakarta |
| 1570680297 | Missed | [redacted] | None | 0 | Greater Jakarta |
| 1571116537 | Missed | [redacted] | None | 0 | Indonesia |
| 1571287728 | Missed | [redacted] | None | 0 | Greater Jakarta |
| 1571404121 | Missed | [redacted] | None | 0 | Indonesia |
| 1571482905 | Missed | [redacted] | None | 0 | Indonesia |
| 1571483683 | Missed | [redacted] | None | 0 | Indonesia |
| 1572274205 | Missed | [redacted] | None | 0 | Indonesia |
| 1572580138 | Missed | [redacted] | None | 0 | New York |
| 1573370906 | Missed | [redacted] | Unknown | 0 | Indonesia |
| 1573387054 | Missed | [redacted] | Unknown | 0 | Indonesia |
| 1573537413 | Missed | [redacted] | None | 0 | Greater Jakarta |
| 1573636103 | Missed | [redacted] | None | 0 | Greater Jakarta |

Calls | SMS Messages

| Message ID | Status | Type | Date Send | Local Date | From/To | Seen | Message |
|---|---|---|---|---|---|---|---|
| 1 | OK | Incoming | 1570703094 | 1570703097 | 111 | Yes | KUOTA makin BESAR, BAYAR mkn MURAH! 4GB CUMA 20rb utk 7hr. BALAS HP utk aktifkan. Nikmati 1GB +3GB jam1-12 skrg. BURUAAN sebelum PROMOnya HABIS! AS122 |
| 2 | OK | Incoming | 1570703094 | 1570703251 | 111 | Yes | KUOTA makin BESAR, BAYAR mkn MURAH! 4GB CUMA 20rb utk 7hr. BALAS HP utk aktifkan. Nikmati 1GB +3GB jam1-12 skrg. BURUAAN sebelum PROMOnya HABIS! AS122 |
| 3 | OK | Incoming | 1570707925 | 1570707927 | 123 | Yes | Paket MAU 2.5GB(.85+1.65)+25mnt 1hr gagal diperbarui karena pulsa tidak mencukupi. Segera isi pulsa dan cek paket menarik di *123# atau bima+, klik http://bit.ly/BIMA3 |
| 4 | OK | Incoming | 1570710636 | 1570710638 | 111 | Yes | 70 Menit BEBAS BICARA cuma 5rb! 20 Menit ke semua operator & 50 Menit ke sesama Tri. Balas AS utk beli. Cek Hot Sale di *123*4#. Kirim Pulsa & Paket di *323# |
| 5 | OK | Incoming | 1570753422 | 1570753423 | 111 | Yes | Kuota 3GB CUMA Rp 3,5rb siap bikin harimu jadi SERU! Balas AK untuk aktifkan. Nikmati 1GB +2GB (01-09) + 30mnt telp sesama Tri buat SEHARIAN. AS508 |
| 6 | OK | Incoming | 1570794326 | 1570794328 | 123 | Yes | Paket MAU 2.5GB(.85+1.65)+25mnt 1hr gagal diperbarui |



Internet Chats

Facebook Messenger Chats | Whatsapp Messages

| Date | Sender | Type | Attachments | Text |
|---|---|---|---|---|
| 1577837526 | Juan Ferdiansyah | Unknown | None | You and Juan Ferdiansyah are celebrating 2 years of friendship on Facebook |
| 1514775215 | Juan Ferdiansyah | Unknown | None | Say hi to your new Facebook friend, Juan. |
| 0 | N/A | BEFORE_FIRST_SENTINEL | None | None |
| 1577682033 | Kurniawan Bayu | REGULAR | None | https://www83*.zippyshare.com/v/Z2fjhUt2/file.html |
| 1577681173 | Kurniawan Bayu | REGULAR | None | |
| 1577681009 | Kurniawan Bayu | REGULAR | None | https://nopy.to/L7rA4rw9/four_elements_trainer_v084a-pc.zip |
| 1574861388 | Kurniawan Bayu | REGULAR | None | curl --request POST \ --url https://pro.rajaongkir.com/api/cost \ --header 'conten |
| 1573828840 | Kurniawan Bayu | REGULAR | None | |
| 1573828827 | Kurniawan Bayu | REGULAR | None | Link |

Facebook Messenger Chats | Whatsapp Messages

| Origin | Send Date | Received Date | Status | Message | Raw Message |
|---|---|---|---|---|---|
| 0 | -1 | -1 | -1 | None | None |
| 0 | -1 | 1578195825 | 6 | None | None |
| 0 | -1 | 1578195825 | 6 | None | None |
| 0 | -1 | 1578195825 | 6 | None | None |
| 0 | -1 | 1578195825 | 6 | None | None |
| 0 | -1 | 1578197434 | 0 | None | None |

Contacts | Whatsapp Contacts

| Whatsapp Name | Display Name | Number | Phone Type | Whatsapp ID | Whatsapp User |
|---|---|---|---|---|---|
| None | Mas Anto Geyang | | Mobile | 2@s.whatsapp.net | No |
| None | Camid | | Mobile | 0@s.whatsapp.net | No |
| None | Ibu | | Mobile | 8@s.whatsapp.net | No |
| None | Insan | | Mobile | 3@s.whatsapp.net | Yes |
| None | Tiger Revi | | Mobile | 0@s.whatsapp.net | No |
| None | Om Han | | Mobile | 5@s.whatsapp.net | No |
| None | Bu Cici Dosen Informatika | | Mobile | 4@s.whatsapp.net | Yes |
| None | Ravado | | Mobile | 3@s.whatsapp.net | Yes |
| None | Sang Hapekik | | Mobile | 3@s.whatsapp.net | Yes |
| None | Itznaini Ebes | | Mobile | 7@s.whatsapp.net | No |
| None | Bapak E Yogy | | Mobile | 5@s.whatsapp.net | Yes |
| None | PAK HARRIS IGS | | Mobile | 8@s.whatsapp.net | Yes |
| None | Kos Kidung Pak Sono | | Mobile | 3@s.whatsapp.net | Yes |
| None | Kamplenk | | Mobile | 2@s.whatsapp.net | Yes |

Gambar 4.11. Hasil dari bagian *communication*.

Hasil pengujian aplikasi *web based android analysis tools* menunjukan bahwa kemampuan aplikasi dalam melakukan proses investigasi forensik memberikan hasil laporan pengujian sesuai dengan rancangan sistem. secara fungsional, aplikasi ini mampu menghasilkan keluaran berupa data *contact*, *call log*, *network*, *application*, *account*, dan

*screenlock*. Dari hasil laporan pengujian terdapat beberapa data yang tidak dapat ditampilkan oleh sistem, seperti data *screenlock* dengan status N/A. yang dimaksud dengan status N/A yaitu aplikasi *web based android analysis tools* ini tidak dapat melakukan pengujian atau tidak suport terhadap hasil pengujian dari barang bukti digital. selain itu ada beberapa data yang tidak disupport di luar dari hasil pengujian seperti gambar, audio, dan video. Hal ini karena pembuatan aplikasi *web based android analysis tools* lebih difokuskan pada sisi aplikasi-nya sehingga data yang disebutkan seperti gambar dan lain-lain itu tidak termasuk dalam perancangan sistem. Hasil pengujian di atas dijabarkan pada tabel agar lebih muda dipahami, seperti pada tabel 4.5.

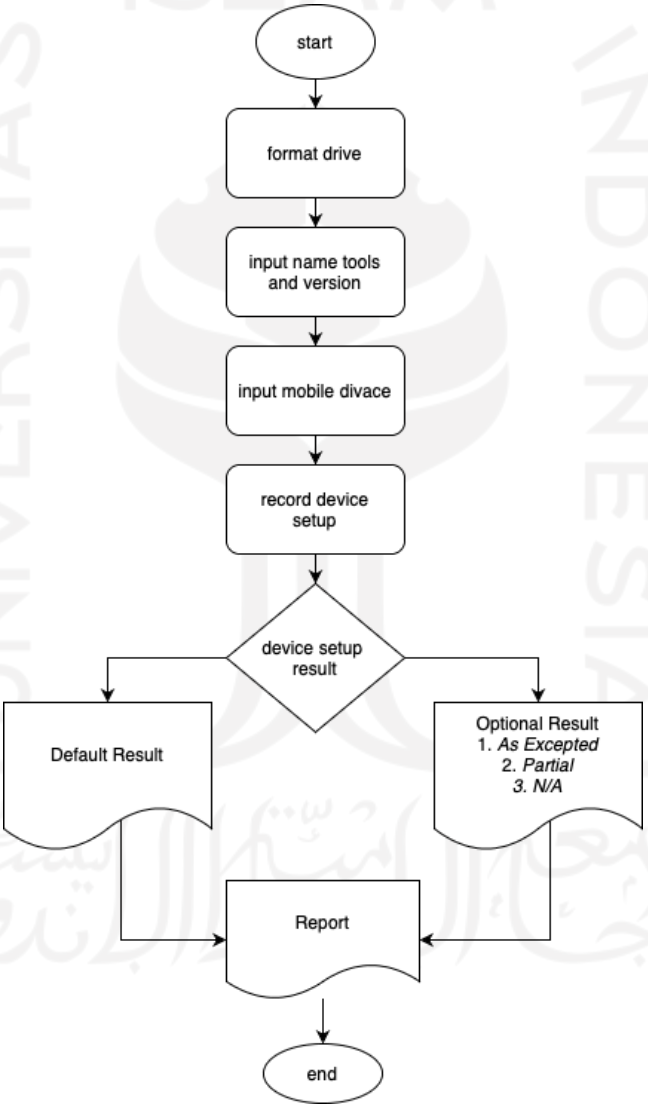
Tabel 4.5 Hasil pengujian dari aplikasi *web based android analysis tools*.

| **Data Objek** | | **Status** | **Keterangan** |
|---|---|---|---|
| Data Contact | Contact Telephone | *As Excepted* | Sesuai |
| | Contact Whatsapp | *Partial* | Sebagian data tidak didukung |
| Call Log | incoming | *As Excepted* | Sesuai |
| | Outgoing | | |
| | reject | | |
| Sosial Media data | Facebook messenger | *As Excepted* | Sesuai |
| | Whatsapp messenger | *Partial* | Sebagian data tidak didukung |
| Network connection | Network connection AP | *As Excepted* | Sesuai |
| | Device info | | |
| | Wifi tethering | | |
| Application | Available packet | *As Excepted* | Sesuai |
| | Application-install | | |
| | Platform Version | | |
| Account | Youtube Account | *As Excepted* | Sesuai |
| Screen Lock | Password quality | N/A | Tidak Support |
| | Numeric digit | | |
| | Symbol | | |

**Ket:**
***As Exceptio:*** aplikasi *web based android analysis tools* mampu memberikan hasil sesuai dengan yang diharapkan berdasarkan data yang ada pada barang bukti digital.
***Partial:*** aplikasi *web based android analysis tools* hanya mampu memberikan sebagian hasil beberapa data tidak bisa ditampilkan dari bukti digital.
**N/A*:*** aplikasi *web based android analysis tools* tidak support atau tidak bisa menghasil data dari barang bukti digital digital.

### 4.3.3 Pengujian *Federated Testing*

Pengujian *federated testing* merupakan salah satu program CFTT yang menyediakan fasilitas untuk menguji aplikasi atau tools forensik yang dibuat, hasil laporan pengujian dapat dibagikan ke komunitas forensik atau laboratorium forensik, untuk mendapatkan validasi terhadap aplikasi yang diuji harus melakukan dengan mengirimkan hasil laporan pengujian aplikasi ke CFTT untuk ditinjau dan diverifikasi agar bisa mendapatkan validasi atau standarisasi aplikasi tersebut. Proses pengujian *federated testing* memiliki alur kerja sebagai berikut.




Gambar 4.12 Alur pengujian *federated testing*.

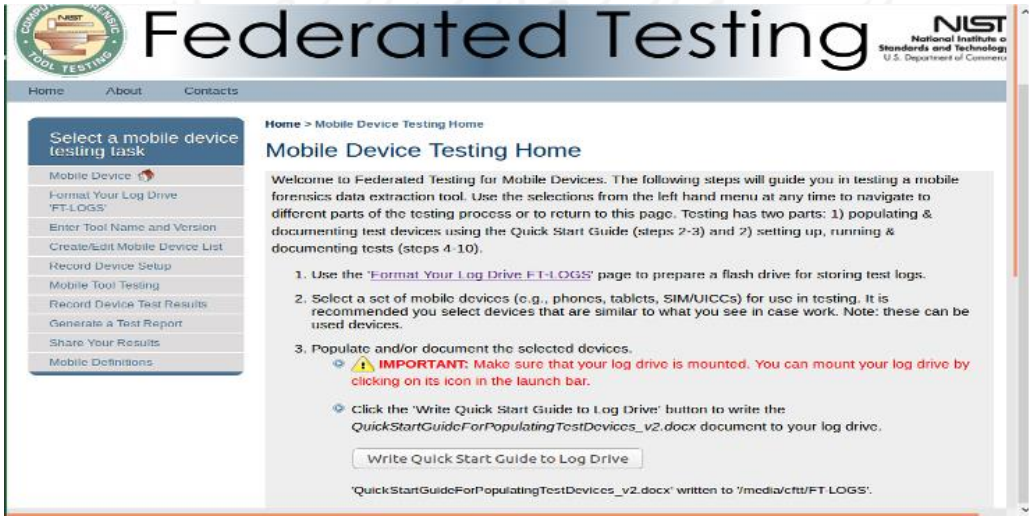
Gambar 4.12 merupakan penjelas tentang alur kerja dari pengujian *federated testing*. Dijelaskan bahwa pada alur kerja dimulai proses testing sampai dengan proses reporting:

1. Testing

Pada tahap testing merupakan tahapan awal yang menjelaskan bagaimana melakukan pengujian terhadap aplikasi yang akan diuji, proses pengujiannya sudah dijelaskan secara rinci tentang langkah-langkah pembuatan laporan pada halaman *federated testing*, langkah awal yang harus dilakukan untuk menjalankan aplikasi *federated testing* yang sudah di install pada sistem operasi linux, ketika sistem operasi linux dijalankan maka secara otomatis aplikasi *federated testing ini* akan dijalankan secara otomatis seperti pada gambar 4.13.


Gambar 4.13 *Interface federated testing*.

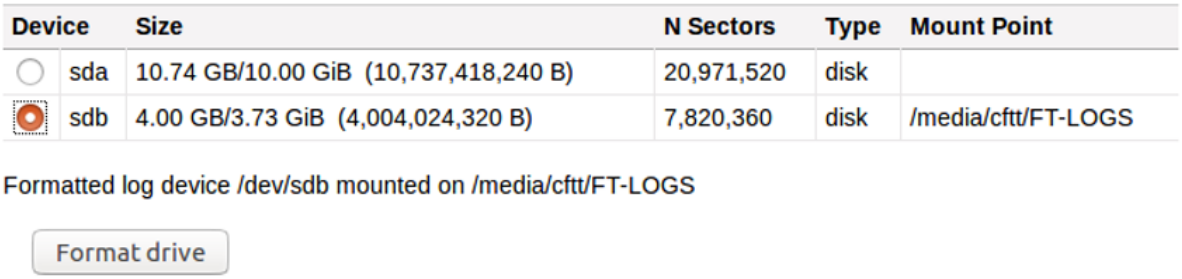
Pada gambar 4.13 merupakan tampilan *interface deferated* testing ketika pertama kali dijalankan. Dapat dilihat bahwa pada gambar tersebut ada beberapa fasilitas *federated testing* yang digunakan untuk menguji aplikasi seperti *disk image*, *write block*, *media preparation tool*, dan *mobile device tool*. selanjutnya masuk pada halaman mobile device tool maka akan terlihat langkah-langkah dalam pengujian aplikasi, seperti pada gambar 4.14.




Gambar 4.14 *Mobile device testing*.

a. Format drive

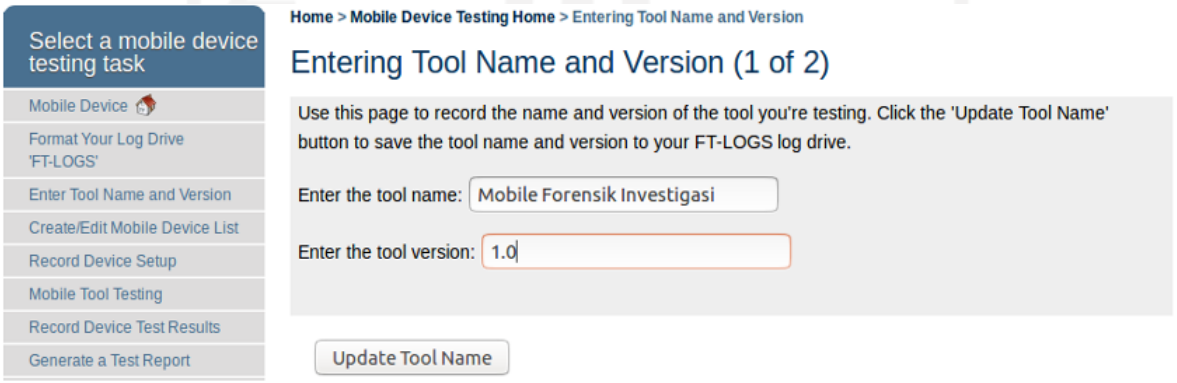
Pada halaman format drive dijelaskan bahwa pada pengujian aplikasi ini dibutuhkan sebuah perangkat *flashdisk*. *Flashdisk* ini digunakan untuk menyimpan aktivitas pengujian dan laporan hasil pengujian aplikasi. *Flashdisk* yang digunakan dalam kasus ini tipe kingston ukuran 4GB. ketika flash drive dicolokan ke komputer maka akan terbaca pada halaman web *federated testing*. Selanjutnya *flasdisk* tersebut harus di format terlebih dahulu sebelum melanjutkan ke proses berikutnya, seperti pada gambar 4.15.




Gambar 4.15 Format flash drive.

b. Tools name and version

*Tools name and version* adalah tahapan kedua yang digunakan untuk mencatat nama alat dan versi aplikasi yang akan diuji. Data ini akan disimpan ke dalam flash drive FT-LOGS sebagai dokumentasi ketika pembuatan reporting di akhir pengujian *federated testing*. Untuk pengisian nama dan versi aplikasi dapat dilihat pada gambar 4.16.

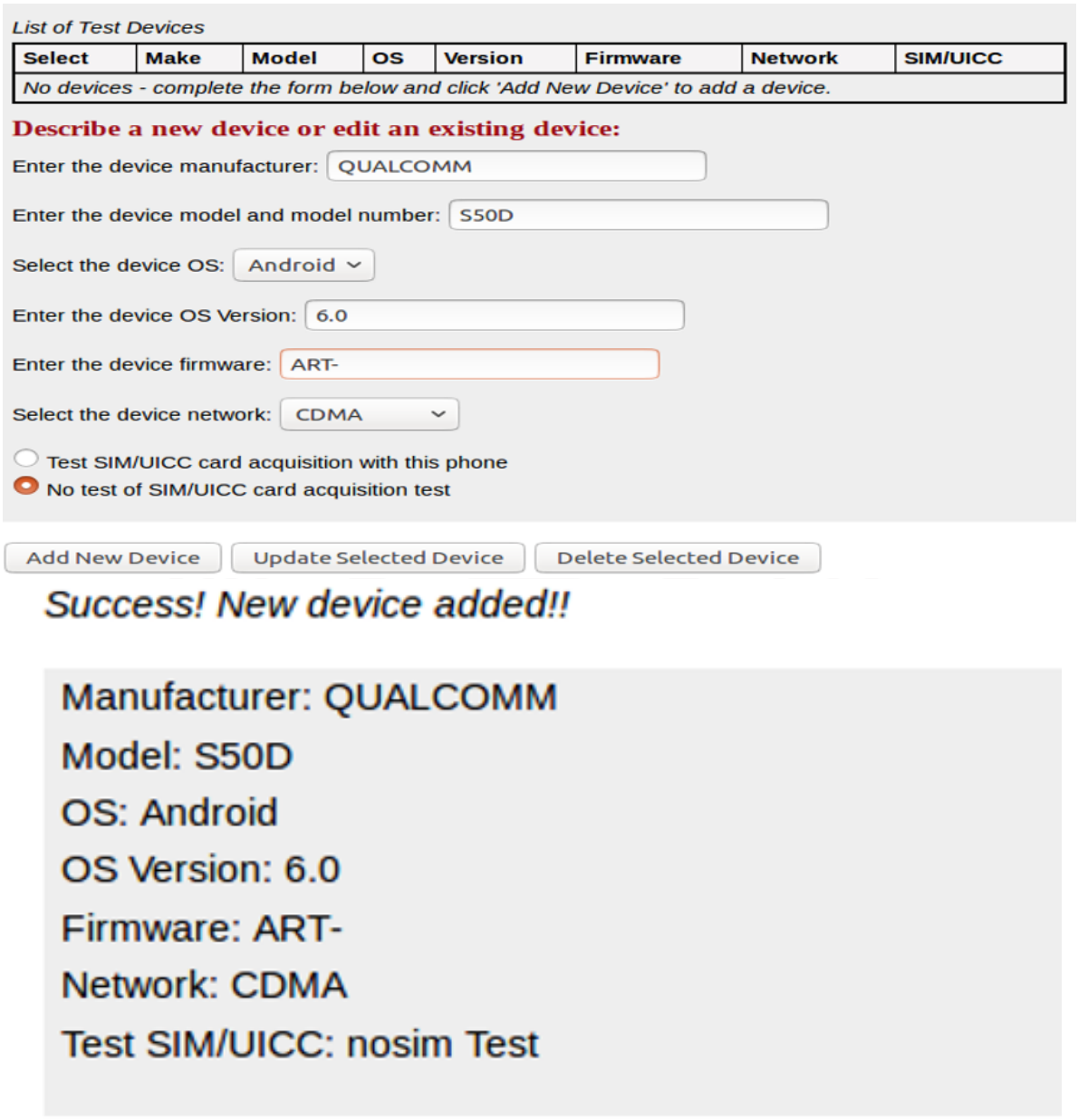



Gambar 4.16 Create name and version application.

c. Create Mobile Devices

Pada tahap *create mobile device* merupakan proses untuk menginput beberapa informasi tentang data smartphone. Data yang dimasukkan harus sesuai dengan data pada file image yang di akuisisi sebelumnya. Data *smartphone* yang dibutuhkan dalam penginputan mobile

device berupa *device manufacture, device model and model number, os version, Firmware, tipe network.* Seperti yang ditampilkan pada gambar 4.17.




Gambar 4.17 Create mobile device.

d. Record device setup

Pada *interface record Devices Setup* menampilkan informasi perangkat mobile yang telah dibuat sebelumnya pada tahap *create mobile device*. informasi ini akan di proses menghasil sebuah laporan umum dari *federated testing*. Laporan ini yang nanti akan dijadikan sebagai hasil evaluasi dari laporan pengujian aplikasi *web based android analysis tools*. Adapun hasil record devices dapat dilihat pada gambar 4.6.

Tabel 4.6 Hasil record device setup.

| Data Objek | | Status |
|---|---|---|
| Contact / Address Book Entitas | Regular length | Populated |
| | Maximum Length | |
| | Blank Name | |
| | Contact Group | |
| Calender, Memos | Regular length | Populated |
| | Sepesial Caracter | |
| | Delete Entry | |
| Data File | Audio | Populated |
| | Video | |
| | Document | |
| | Graphic | |
| Call Log | Incoming | Populated |
| | Outgoing | |
| | Missed | |
| SMS Massage | Incoming | Populated |
| | Outgoing | |
| MMS Massage | Incoming audio, video | Populated |
| | Outgoing audio, video | |
| Browser / Email Data | Visit Site | Populated |
| | Bookmark | |
| | Email | |
| Social Media | Facebook | Populated |
| | Instagram | |
| | Twitter | |

e. Record device test result

Pada halaman *record divisi test result* menampilkan informasi hasil record dari proses sebelumnya. Pada hasil laporan *record* terdapat opsional yang dapat pilih untuk menentukan hasil pengujian yang dapat disesuaikan dengan hasil pengujian aplikasi *web based android analysis tools*. Setelah menentukan opsi yang sudah ditentukan maka *federated testing* akan menghasilkan dua laporan yang berbeda yaitu laporan pertama menampilkan seluruh data di *federated testing* yang kedua menampilkan data yang ditentukan berdasarkan opsi yang dipilih. Seperti yang ditampilkan pada tabel 4.7.

Tabel 4.7 Record device test result.

| Result | Defenition |
|---|---|
| *As-expected* | aplikasi menghasilkan data sesuai yang di harapkan |
| *Partial* | aplikasi hanya mampu menghasilkan sebadian data |
| *Not As-expected* | aplikasi tidak menghasilkan data sesuai yang di harapkan |
| N/A | Tidak Suport |

| Entry | | Result | | | |
|---|---|---|---|---|---|
| | | *As-expected* | *Partial* | *Not as-expected* | N/A |
| Acquisition | *Acquisition All* | ✓ | | | |
| | *Disrupted* | | ✓ | | |
| Reporting | *Preview-Pane* | ✓ | | | |
| | *Generate Report* | ✓ | | | |
| Equipment/ user data | IMEI | | | | ✓ |
| | MEID/ESN | | | | ✓ |
| | MSISDN/MIN | | | | ✓ |
| Hashing | *Case File* | | | | ✓ |
| Case file data protection | *modify case data* | | | | ✓ |
| PIM Data | *Contact* | ✓ | | | |
| | *Calendar* | | | | ✓ |
| | *Memos/Notes* | | | | ✓ |
| Stand-alone data file | Audio | | | | ✓ |
| | Graphic | | | | ✓ |
| | Video | | | | ✓ |
| | Document | | | | ✓ |
| Call Log | Incoming | ✓ | | | |
| | Outgoing | ✓ | | | |
| | Missed | ✓ | | | |
| SMS Message | Incoming | ✓ | | | |
| | Outgoing | ✓ | | | |
| MMS Massage | Audio | | | | ✓ |
| | Graphic | | | | ✓ |
| | Video | | | | ✓ |
| Location | Coordinates | | | | ✓ |
| Browser/ Email Data | Visit Site | | | | ✓ |
| | Bookmark | | | | ✓ |
| | Email | ✓ | | | |
| Social Media | Facebook | ✓ | | | |
| | Twitter | | | | ✓ |
| | Instagram | | | | ✓ |
| | Linkedin | | | | ✓ |
| Other App | Application interes | ✓ | | | |
| Non latin character | reported in native | | | | ✓ |

2. Reporting

Pada halaman reporting merupakan tahapan terakhir dari proses pengujian yang menampilkan hasil laporan pengujian *federated testing*. Laporan yang dihasilkan terbagi menjadi dua tabel laporan yaitu tabel yang menampilkan seluruh informasi tentang hasil pengujian mobile forensik dan yang kedua tabel menampilkan hasil pengujian berdasarkan kebutuhan yang kita tentukan pada tahap sebelumnya.

a. Laporan umum *federated testing*

Tabel 4.8 Laporan umum *federated testing*

| **Data Objek** | | **Status** |
|---|---|---|
| Contact/ Address book entitas | Regular length | Populated |
| | Maximum Length | |
| | Blank Name | |
| | Contact Group | |
| Calender, Memos | Regular length | Populated |
| | Sepesial Caracter | |
| | Delete Entry | |
| Data File | Audio | Populated |
| | Video | |
| | Document | |
| | Graphic | |
| Call Log | Incoming | Populated |
| | Outgoing | |
| | Missed | |
| SMS Massage | Incoming | Populated |
| | Outgoing | |
| MMS Massage | Incoming audio, video | Populated |
| | Outgoing audio, video | |
| Browser / Email Data | Visit Site | Populated |
| | Bookmark | |
| | Email | |
| Social Media | Facebook | Populated |
| | instagram | |
| | twitter | |

b. Laporan yang diharapka dari *federated testing*

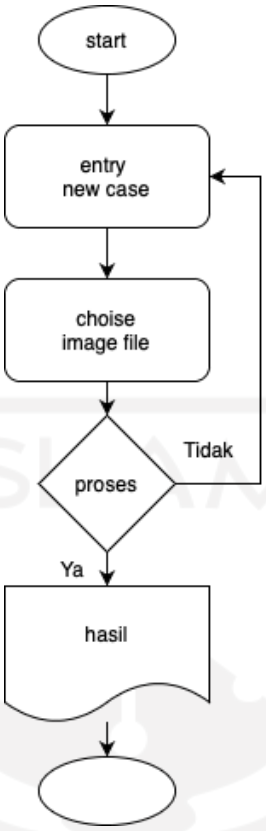
Tabel 4.9 Laporan umum *federated testing*.

| **Test-result internal memory acquisition** | | **Qualcomm S50D** |
|---|---|---|
| Acquisition | Acquire all | *As-expected* |
| | Disrupted | *partial* |
| Reporting | Preview-pane | *As-expected* |
| | General Report | *As-expected* |
| Equipment/ user data | IMEI | N/A |
| | MSISDN / MIN | N/A |
| PIM Data | Contact | N/A |
| | Calendar | N/A |
| | Memos | N/A |
| Stand Alone Data File | Audio | N/A |
| | Graphic | N/A |
| | Video | N/A |

| **Test-result internal memory acquisition** | | **Qualcomm S50D** |
|---|---|---|
| Call Data | Incoming | *As-expected* |
| | Outgoing | *As-expected* |
| | Missed | *As-expected* |
| Local Data<br>SMS Massage | Coordinates | N/A |
| | Incoming | *As-expected* |
| | Outgoing | *As-expected* |
| MMS Massage | Audio | N/A |
| | Graphic | N/A |
| | Video | N/A |
| Browser / Email Data | Visit Sites | N/A |
| | Bookmark | N//A |
| | Email | *As-expected* |
| Social Media Data | Facebook | *As-expected* |
| | Twitter | N/A |
| | Instagram | N/A |
| Other Application | Other-app interest | N/A |
| Non-Lite character | Reported in native format | N/A |
| Hashing | case File | N/A |
| Case file data protection | modify case data | N/A |

### 5.3.3 Pengujian Aplikasi Belkasoft

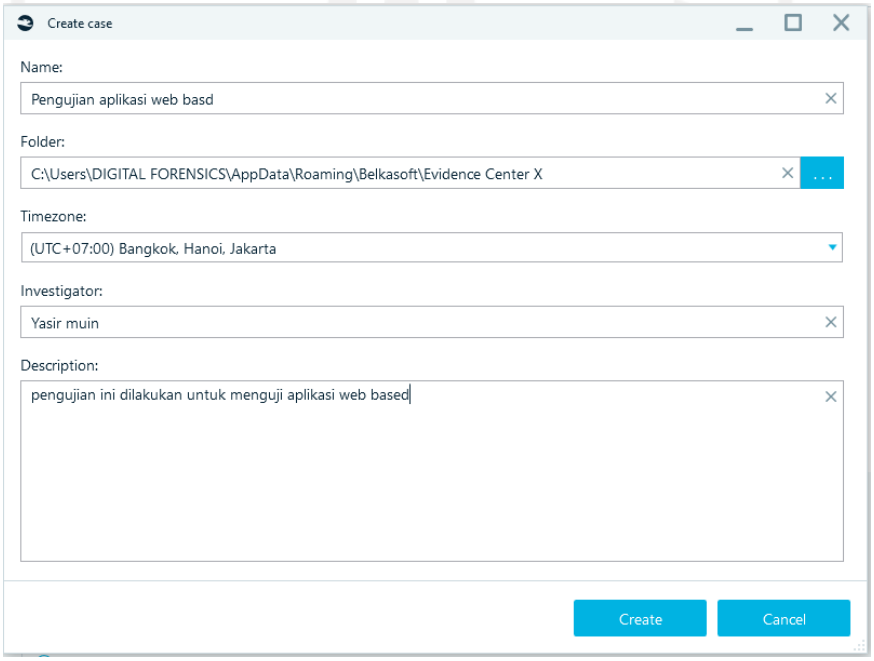
Aplikasi belkasoft merupakan salah satu perangkat lunak forensik digital yang banyak digunakan dalam investigasi forensik digital, karena memiliki kemampuan untuk memperoleh, mencari, menganalisis, menyimpan berbagai bukti digital yang ditemukan baik di dalam komputer maupun perangkat mobile. Belkasoft mampu melakukan ekstraksi bukti digital dari berbagai sumber dengan menganalisis hard drive, drive image cloud, memory dumps, iOS, Blackberry, android dan berbagai jenis platform lain. Belkasoft akan secara otomatis menganalisis sumber data dan memberikan artefak yang paling penting yang dapat digunakan penyidik untuk meninjau, memeriksa menganalisis atau membuat sebuah laporan (belkasoft). Namun pada penelitian ini akan dilakukan pengujian aplikasi tersebut berdasarkan standar CFTT yang nanti digunakan sebagai bahan perbandingan dari aplikasi *web-based*. Tujuannya untuk mengukur kelayakan aplikasi *web-based* apakah suda sesuai standar CFTT sesuai yang diharapkan. Proses pengujian akan dijelaskan berdasarkan alur kerja pada gambar 4.18.




Gambar 4.18 Alur pengujian aplikasi mobile forensik.

1. Create new case

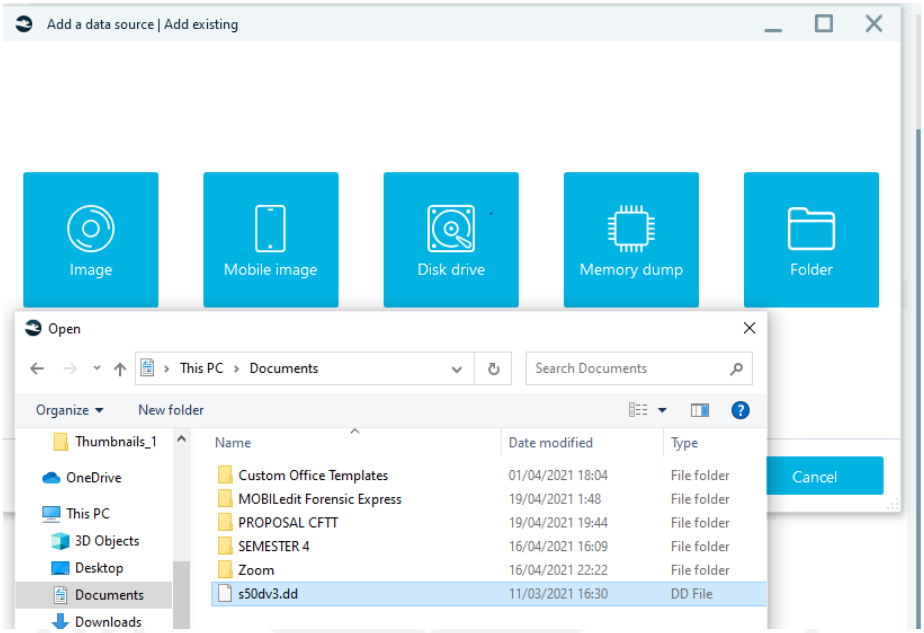
Pada bagian ini merupakan tahap untuk membuat kasus baru pada aplikasi belkasoft, dengan menginput beberapa parameter yang diminta seperti *case name investigation name*, dan *description*. Untuk lebih jelasnya dapat dilihat pada gambar 4.19.




Gambar 4.19 *Create new case*.

2. File image

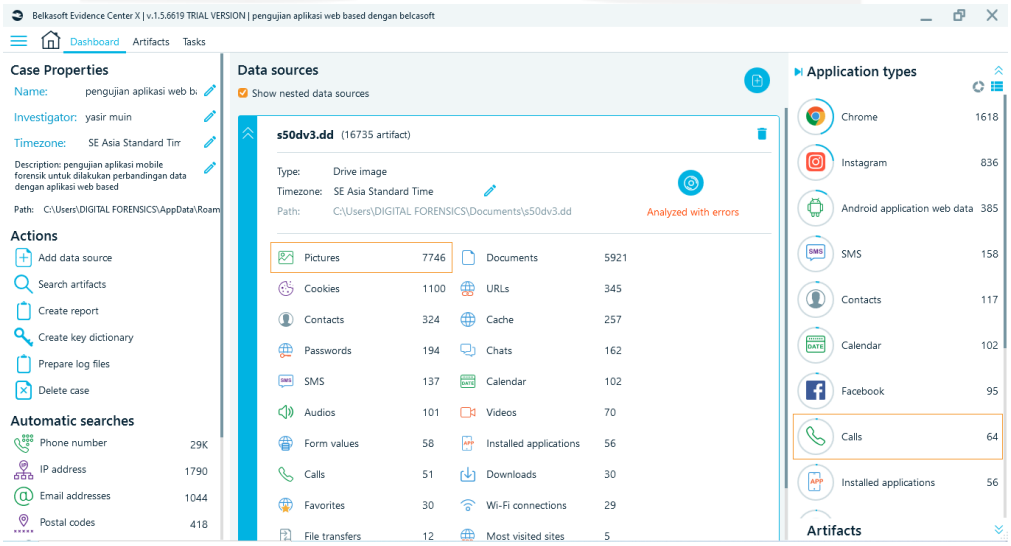
Pada tahap ini merupakan proses yang dilakukan untuk memanggil file image yang diakuisisi dari perangkat *smartphone* untuk diuji pada aplikasi belkasoft. File image yang digunakan saat pengujian aplikasi bigasoft sama dengan yang digunakan juga pada pengujian aplikasi *web based*. Proses pemanggilan file image dijelaskan pada gambar 4.20.




Gambar 4.20 Pemanggilan file image.

3. Hasil

Hasil merupakan tahap akhir yang menampilkan hasil pengujian aplikasi yang dianalisis dari sebuah barang bukti digital yang digunakan sebagai bahan pengujian aplikasi. Hasil yang didapatkan pada proses pengujian ini ditampilkan pada gambar 4.21.




Gambar 4.21. Hasil pengujian aplikasi belkasoft.

Pada gambar 4.2 menampilkan hasil yang di ditemukan dari analisis sebuah barang bukti elektronik *smartphone*. aplikasi belkasoft ini mampu menampilkan informasi yang lebih detail untuk barang bukti yang berhasil ditemukan. Untuk melihat dapa apa yang dihasilkan oleh aplikasi belkasoft akan ditampilkan pada tabel 4.10.

Tabel 4.10 Hasil pengujian aplikasi belkasoft

| **Data Objek** | | **Jumlah data** | **Status** |
|---|---|---|---|
| Contact / address book | contact | 324 | sesuai |
| Calender, memos | calender | 102 | sesuai |
| Data file | Audio | 101 | sesuai |
| | Video | 70 | sesuai |
| | Dokument | 5921 | sesuai |
| | picture | 7746 | sesuai |
| Call Log | Incoming | 51 | sesuai |
| | Outgoing | | sesuai |
| Sms | Incoming | 137 | sesuai |
| | outgoing | | sesuai |
| Browser email | Cache | 257 | sesuai |
| | Cookies | 1100 | sesuai |
| | Download | 30 | sesuai |
| | Favorites | 30 | sesuai |
| | Form values | 58 | sesuai |
| | Most visit site | 5 | sesuai |
| | Password | 194 | sesuai |
| | Session | 1 | sesuai |
| | Urls | 345 | sesuai |
| Social media | instagram | 836 | sesuai |
| | Facebook | 95 | sesuai |
| | whatsapp | 41 | sesuai |
| Location | Geolocation data | 4 | sesuai |
| Wifi Connection | Ip address | 1790 | sesuai |
| | Email address | 1044 | sesuai |
| | Postal codes | 418 | sesuai |
| | Mac address | 11 | sesuai |
| | ssid | 29 | sesuai |
| Application | Application-install | 56 | sesuai |

## 4.4 Evaluasi

Pada tahap ini merupakan proses untuk mengevaluasi data yang sudah diperoleh dari hasil pengujian aplikasi *web-based, federated testing,* dan *belkasoft*. Proses eveluasi ini dilakukan untuk mengetahui kelayakan aplikasi *web-based* apakah sudah memunuhi stnadar CFTT atau belum, yaitu dengan membandingakan data dari hasil laporan aplikasi *belkasoft* dan *federated testing.* Data evaluasi dapat dilihat pada tabel 4.11, 4.12 dan 4.13.

Tabel 4.11 Hasil pengujian aplikasi mobile forensik.

| **Data Objek** | | **Status** | **Keterangan** |
|---|---|---|---|
| Data Contact | Contact Telphone | *As Excepted* | Sesuai |
| | Contact Whatsapp | *Partial* | Sebagian data tidak didukung |
| Call Log | Incoming | *As Excepted*<br>*As Excepted* | sesuai<br>Sesuai |
| | Outgoing | *As Excepted* | |
| | Reject | *As Excepted* | |
| Sosial Media data | Facebook messenger | *As Excepted* | Sesuai |
| | Whatsapp messenger | *Partial* | Sebagian data tidak didukung |
| Network connection | Network connection AP | *As Excepted* | Sesuai |
| | Device info | *As Excepted* | Sesuai |
| | Wifi tethering | *As Excepted* | Sesuai |
| Application | Available packet | *As Excepted* | Sesuai |
| | Application-install | *As Excepted* | Sesuai |
| | Platform Version | *As Excepted* | Sesuai |
| Account | Youtube Account | *As Excepted* | Sesuai |
| Screen Lock | Password quality | N/A | Tidak Support |
| | Numeric digit | N/A | Tidak suport |
| | Symbol | N/A | Tidak suport |

Tabel 4.12 Hasil pengujian belkasoft

| **Data Objek** | | **Status** | **Keterangan** |
|---|---|---|---|
| Contact / address book | contact | *As Excepted* | sesuai |
| Calender, memos | calender | *As Excepted* | sesuai |
| Data file | Audio | *As Excepted* | sesuai |
| | Video | *As Excepted* | sesuai |
| | Dokument | *As Excepted* | sesuai |
| | picture | *As Excepted* | sesuai |

| Data Objek | | Status | Keterangan |
|---|---|---|---|
| Call Log | Incoming | *As Excepted* | sesuai |
| | Outgoing | *As Excepted* | sesuai |
| Sms Massage | Incoming | *As Excepted* | sesuai |
| | Outgoing | *As Excepted* | sesuai |
| Browser email | Cache | *As Excepted* | sesuai |
| | Cookies | *As Excepted* | sesuai |
| | Download | *As Excepted* | sesuai |
| | Favorites | *As Excepted* | sesuai |
| | Form values | *As Excepted* | sesuai |
| | Most visit site | *As Excepted* | sesuai |
| | Password | *As Excepted* | sesuai |
| | Session | *As Excepted* | sesuai |
| | Urls | *As Excepted* | sesuai |
| Social media | instagram | *As Excepted* | sesuai |
| | Facebook | *As Excepted* | sesuai |
| | whatsapp | *As Excepted* | sesuai |
| Location | Geolocation data | *As Excepted* | sesuai |
| Connection | Ip address | *As Excepted* | sesuai |
| | Email address | *As Excepted* | sesuai |
| | Postal codes | *As Excepted* | sesuai |
| | Mac address | *As Excepted* | sesuai |
| | ssid | *As Excepted* | sesuai |
| Application | Application-install | *As Excepted* | sesuai |

Tabel 4.13 Hasil pengujian federated testing.

| Data Objek | | Status |
|---|---|---|
| Contact / Address Book Entitas | Regular length | Populated |
| | Maximum Length | |
| | Blank Name | |
| | Contact Group | |
| Calender, Memos | Regular length | Populated |
| | Sepesial Caracter | |
| | Delete Entry | |
| Data File | Audio | Populated |
| | Video | |
| | Document | |
| | Graphic | |
| Call Log | Incoming | Populated |
| | Outgoing | |
| | Missed | |
| SMS Massage | Incoming | Populated |
| | Outgoing | |
| MMS Massage | Incoming audio, video | Populated |
| | Outgoing audio, video | |
| Browser / Email Data | Visit Site | Populated |
| | Bookmark | |
| | Email | |

| Data Objek | | Status |
|---|---|---|
| Social Media | Facebook | Populated |
| | Twitter | |
| | Instagram | |

Hasil evaluasi pengujian, diketahui bahwa setelah dilakukan perbandingan data antara hasil pengujian aplikasi *web-based* dan *belkasoft* berdasarkan standar *federated testing*, didapatkan pada aplikasi *web-based* masil lebih rendah dibandingkan dengan aplikasi *belkasoft* karena kemampuan aplikasi *web-based* ini hanya mampu memperoleh emat data yang sesuai dengan laporan *federated testing* diantaranya *call log, sms message, social media* untuk data lainnya belum di support oleh *web-based* itu sendiri. Sedangkan hasil pengujian *belkasoft* mampu menghasilkan semua data yang sesuai dengan laporan *federated* testing, diketahui bahwa aplikasi *belkasoft* ini merupakan salah aplikasi yang sangat *powerfull* yang banyak direkomendasi oleh ahli forensik karena kemampuan dan kemudahan sehingga banyak digunakan dalam investigasi forensik digital, aplikasi ini juga sudah diuji menggunakan standarisasi forensik sehingga data yang dihasil sesuai dengan laporan *federated testing*.

### 4.5 Hasil Pengujian Aplikasi

Reporting merupakan tahapan akhir yang menampilkan hasil laporan pengujian aplikasi *web based* dan *belkasoft* yang diuji berdasarkan standar CFTT. laporan pengujian tersebut menampilkan hasil perbandingan antara kedua aplikasi terkait kemampuan data yang diperoleh dari tiap aplikasi, hasil perbandingan dapat dilihat pada tabel 4.14.

Tabel 4.14 Hasil pengujian kedua aplikasi.

| No | Standar CFTT (Data Federated Testing) | | Pengujian Aplikasi | |
|---|---|---|---|---|
| | | | Web based | Belkasoft |
| 1 | Call Log | Incoming | ✓ | ✓ |
| | | Outgoing | ✓ | ✓ |
| | | Miss | ✓ | ✓ |
| 2 | Data File | Video | X | ✓ |
| | | Image | X | ✓ |
| | | Audio | X | ✓ |
| | | Document | X | ✓ |
| 3 | Network Connection | Network con | ✓ | ✓ |
| | | device info | ✓ | ✓ |
| | | wifi tethering | ✓ | ✓ |
| 4 | SMS Massage | Incoming | ✓ | ✓ |
| | | Outgoing | ✓ | ✓ |

| No | Standar CFTT (Data Federated Testing) | | Pengujian Aplikasi | |
|---|---|---|---|---|
| | | | Web based | Belkasoft |
| 5 | Browser / Email Data | Visited Sites | X | ✓ |
| | | Bookmark | X | ✓ |
| | | Email | ✓ | ✓ |
| 6 | Sosial Media | Facebook | ✓ | ✓ |
| | | Twitter | X | ✓ |
| | | Instagram | X | ✓ |
| 8 | Address Book Entitas | Regular length | X | ✓ |
| | | Special Character | X | ✓ |
| | | Blank Name | X | ✓ |
| | | Regular L email | X | ✓ |
| | | Regular L address | X | ✓ |
| | | Contact group | X | ✓ |
| 9 | Data Contact | Contact Phone | ✓ | ✓ |
| | | Contact Whatsapp | ✓ | ✓ |
| 11 | Location Data | GPS Coordinates | X | ✓ |
| | | Geo-Tagged Data | X | ✓ |
| 12 | MMS Massage | Incoming Audio | X | ✓ |
| | | Incoming Video | X | ✓ |
| | | Incoming Graphic | X | ✓ |
| | | Outgoing Audio | X | ✓ |
| | | Outgoing Video | X | ✓ |
| | | Outgoing Graphic | X | ✓ |

Berdasarkan tabel 4.7 memperlihatkan hasil pengujian dari aplikasi *web-based android analysis tools* dan *belkasoft* yang didasarkan pada standar forensik. Jika dilihat pada tabel tersebut hasil perbandingan data antara web-based dan belkasoft masih unggul belkasoft. Karena aplikasi belkasoft ini merupakan salah satu perkakas forensik yang suda menerapkan standar CFTT pada aplikasi tersebut, sehingga mampu menghasilkan data sesuai dengan *federated testing*, jadi bisa dikatakan bahwa aplikasi *belkasoft* sekarang fungsional memenuhi standar CFTT sehingga layak digunakan dalam proses investigasi forensik digital. Sedangkan data yang ditampilkan pada aplikasi *web-based* diketahui bahwa *tools* tersebut hanya mampu menghasilkan empat variabel data yang sesuai dengan laporan *federated testing*, beberapa data lainnya belum di support oleh aplikasi *web based*, hal ini disebabkan karena kebutuhan yang digunakan pada saat perancangan sistem *web-based* ini tidak disesuaikan dengan variabel data *federated testing* sehingga pada saat melakukan pengujian aplikasi, hasil yang didapatkan juga berbeda. Pengujian antara aplikasi *web-based* dan *belkasoft* juga ketika dibandingkan data dari kedua aplikasi tersebut terlihat bahwa

aplikasi *web-based* masih lebih rendah dibandingkan dengan aplikasi *belkasoft*, sehingga dapat disimpulkan bahwa aplikasi *web-based* belum mampu memenuhi standarisasi CFTT.

Hasil pada tabel tersebut juga menjelaskan tentang bagaimana data itu diperoleh, proses apa yang dilakukan oleh kedua aplikasi dalam memperoleh data, dan menjawab kenapa pada aplikasi *web-based* tidak mensupport data-data seperti yang dijelaskan diatas. Proses ini dijelaskan pada point berikut:

- **Call Data**: merupakan data yang berisi informasi tentang catatan atau history panggilan pada barang bukti digital, pada bagian ini kedua aplikasi tersebut memiliki kemampuan menampilkan call data, yang diperoleh dari direktori com.android.providers.
- **Data File**: merupakan data yang menampilkan informasi berupa data video, graphic, video, dan dokumen. Dapat dilihat pada tabel tersebut bahwa aplikasi *web-based* tidak mampu menghasilkan data tersebut, sedangkan pada aplikasi *belkasoft* berhasil menampilkan data file, data tersebut diperoleh dari direktori com.android.media dan com.android.graphic.
- **Network Connection**: merupakan bagian yang memuat tentang informasi dari histori aktivitas saat terkoneksi dengan internet pada perangkat smartphone. bagian ini merupakan fitur yang di support oleh aplikasi web based, sedangkan pada laporan federated testing fitur ini tidak terdapat fitur tersebut. untuk mengetahui bagaimana aplikasi web based menghasilkan data, yaitu dengan mengakses semua informasi tersebut pada direktori com.android.net.wifi. jika terdapat informasi pada direktori tersebut maka akan ditampilkan oleh aplikasi web based.
- **SMS Massage**: merupakan data yang berisi tentang informasi tentang pesan sms baik itu masuk maupun keluar, pada bagian ini kedua aplikasi masing-masing mampu menghasilkan data yang sama. pada hasil pengujian aplikasi web based aplikasi tersebut akan mencari data sms pada direktori smartphone yang berada class com.android.providers.telephony jika terdapat informasi tersebut maka akan ditampilkan pada aplikasi web based.
- **Browser / Email Data:** pada bagian ini data yang ditampilkan pada laporan federated testing berupa informasi visit site, bookmark dan data email, sedangkan pada hasil pengujian aplikasi web based hanya mampu menghasilkan data email, untuk data visit site dan bookmark tidak dapat ditampilkan oleh aplikasi tersebut. data email yang ditampilkan pada aplikasi web based tersebut dihasilkan dari direktori

com.android.chrome yang mana terdapat beberapa class di dalamnya salah satunya adalah data email.

- **Sosial Media:** pada bagian ini memuat informasi tentang platform data sosial media diantaranya facebook, instagram, twitter, dan linked yang ada pada laporan *federated testing*. sedangkan pada aplikasi web based sendiri hanya mampu menghasilkan informasi berupa data facebook yang ada pada perangkat smartphone. pada pengujian aplikasi web based ini menampilkan data facebook pada direktori com.android.facebook, com.android.instagram, com.android.twitter pada perangkat smartphone.
- **Application:** merupakan bagian yang berisi tentang paket-paket dan aplikasi yang diinstall pada perangkat smartphone. data ini hanya dihasilkan oleh aplikasi web based, pada laporan federated testing tidak terdapat data tersebut. untuk bisa menampilkan data-data tersebut aplikasi web based ini akan mengakses data tersebut pada direktori com.android.vending. dan ditampilkan pada aplikasi web based.
- **Address Book Entitas:** merupakan bagian yang memuat informasi berupa data spasial karakter dan beberapa reguler length lainnya, dat ini hanya ada pada laporan federated testing sedangkan pada aplikasi web based belum support data-data tersebut. ketika aplikasi web based saat diuji tidak bisa mengangkat data yang tersimpan pada barang bukti digital smartphone. sedangkan untuk aplikasi belkasoft berhasil memperoleh data tersebut yang didapat dari direktori com.android.providers.calendar
- **Data Contact:** merupakan bagian yang berisi tentang data kontak hp dan kontak whatsapp. data ini hanya dihasilkan oleh aplikasi web based, pada laporan federated testing tidak terdapat data tersebut. proses untuk bisa menampilkan data-data tersebut aplikasi web based adalah dengan mengakses data tersebut pada direktori msgstore.db.crypt dan com.android.whatsapp. yang kemudian ditampilkan pada aplikasi web based.
- **Account:** merupakan bagian yang berisi tentang data account youtube yang perna digunakan pada perangkat smartphone. data ini hanya dihasilkan oleh aplikasi web based saja, sedangkan pada laporan federated testing tidak terdapat data tersebut. proses untuk mengambil data account youtube pada perangkat smartphone maka aplikasi akan mengakses data tersebut pada direktori com.android.account yang ada pada perangkat smartphone. data tersebut kemudian ditampilkan di aplikasi web based.

- **Location Data:** merupakan informasi yang berisi tentang data GPS coordinates, pada bagian ini hanya terdapat pada laporan federated testing sedangkan untuk laporan dari aplikasi web based belum support terhadap data tersebut.
- **MMS Massage:** merupakan bagian yang yang memuat tentang data mmas massage seperti mms data audio, graphic, dan video. data ini hanya di support oleh laporan federated testing, untuk aplikasi web based saat ini belum suport data tersebut karena variabel yang digunakan pada saat membuat perancangan sistem hanya terbatas pada sebagian data.

## 4.6 Analisis

Berdasarkan hasil analisis pengujian kedua aplikasi dan beberapa sumber literature review lainnya yang menjelaskan tentang standarisasi terhadap sebuat tools forensik yang dibuat atau dikembangkan, mengharuskan setiap tools forensik harus menerapkan sebuah standar untuk memberikan jaminan terhadap aplikasi yang dibuatnya, sehingga dalam proses investigasi forensik baik itu akuisisi analisis dapat memberikan hasil atau bukti digital sesuai dengan yang diharapkan dan dapat diketahui juga kemampuan dari aplikasi tersebut. standarisasi juga memberikan sebuah jaminan terhadap kualitas sebuah aplikasi yang dapat diakui oleh sebuah organisasi atau komunitas forensik. Dari hasil Pengujian kedua aplikasi dapat diketahui bahwa kemampuan aplikasi memiliki perbedaan dari hasil yang diperoleh.

### 4.6.1 Belkasof

Berdasarkan hasil analisis pada pengujian aplikasi belkasoft bahwa sesuai dengan data yang dijelaskan pada tabel 4.14 merupakan hasil pengujian aplikasi yang mana ketika dilakukan perbandingan data dengan aplikasi web-based yang didasarkan pada laporan standar CFTT, didapatkan bahwa aplikasi belkasoft lebih memiliki performa yang sangat *powerfull* terhadap data-data yang dihasilkan dibandingkan dengan aplikasi web-based. Data-data tersebut ketika di sesuaikan dengan laporan standar CFTT, semua variabel yang ada pada laporan tersebut mempu dihasilkan oleh aplikasi belkasoft. aplikasi ini bisa menghasilkan data-data yang sesuai dengan standar CFTT, karena aplikasi tersebut ketika dikembangkan semua kebutuhan fungsional yang dipakai dalam pembuatan aplikasi ini menggunakan acuan dari standar forensik, sehingga hasil yang diperoleh juga sesuai dengan yang ada pada CFTT.

Seperti yang diketahui bahwa aplikasi belkasoft merupakan aplikasi profesional dengan performa yang baik, maka dalam kasus ini aplikasi tersebut hanya digunakan sebagai pendukung proses pengujian aplikasi web-based untuk mengetahui kemampuan aplikasi

tersebut terhadap parameter yang dihasilkan. Parameter yang dihasilkan aplikasi web-based ini yang kemudian akan dievaluasi untuk mencari parameter apa saja yang tidak sesuai dengan parameter yang ada di standar CFTT. hasil evaluasi memperlihatkan bahwa parameter yang belum bisa dihasilkan adalah parameter data file, mms message, data location, address book dan beberapa da lainnya. Kekurangan-kekurang dari aplikasi web-based yang menjadi rekomendasi untuk perbaikan kedepannya.

### 4.6.2 Web Based

Berdasarkan hasil analisa pengujian aplikasi web-base, sesuai dengan data yang ada pada tabel 4.14 dapat dilihat bahwa hasil yang diperoleh dari aplikasi web-based ini masih belum memberikan data secara menyeluruh jika ditinjau kembali berdasarkan variabel yang ada pada standar CFTT, data yang tidak dapat diperoleh seperti data video, gambar, document dan beberapa data social media instagram dan twitter ini merupakan data yang sangat penting yang perlu ada, karena data-data yang disebutkan diatas merupakan data sangat penting yang mana data tersebut kebanyakan didapatkan pada barang bukti yang ditemukan dalam kasus kejahatan. Setelah dilakukan analisis pada aplikasi web-based diketahui bahwa data yang tidak dapat dihasilkan dikarenakan, kemampuan aplikasi web-based yang secara fungsional pada script aplikasinya tidak ditambahkan fitur untuk melakukan tracking data file seperti file data (video, document, audio) sehingga ketika aplikasi dijalankan untuk melakukan analisis barang bukti digital secara otomatis untuk data tersebut tidak bisa diperoleh. untuk melengkapi kekurangan yang ada pada aplikasi web-based ini diharapkan kedepan adanya penelitian lanjutan yang dapat mengbangkan aplikasi web-based ini untuk melengkapi kebutuhan yang belum disuport saat ini, sebagai usulan untuk penembangan aplikasi kedepan harus memenuhi data-data yang dianggap sangat penting seperti:

1. Data file (document, audio, video) data ini harus mampu dihasilkan dengan melihat cara kerja aplikasi untuk mengambil data-date tersebut. Data ini secara default tersipan pada direktori com.android.media dan com.android.graphics.
2. Data social media (twitter, instagram dll) jika dilihat pada tabel 4.14 pada bagian social media hanya terdapat facebook yang bisa diperoleh oleh aplikasi web-based, kenapa tidak bisa mengangkat social media lainnya, karena dari posisi direktori antara facebook, instagram, dan twitter ini memiliki direktori yang berbeda sehingga secara otomatis aplikasi juga akan mengambil data sesuai dengan kebutuhannya.

Dari hasil analisis di atas sebenarnya masih ada beberapa data lain yang belum di support oleh aplikasi web-based, namun memberikan rekomendasi dua point karena point yang disebutkan diatas merupakan data yang penting didapatkan dalam proses investigasi

forensik. secara keseluruhan aplikasi ini bisa dikatakan belum memenuhi standar CFTT, karena dari segi fungsionalitas data yang digunakan juga masih rendah, ini diketahui setelah hasil pengujian yang membuktikan belum memenuhi standar, terkait dengan proses pelabelan bahwa aplikasi itu terstandarisasi atau tidak, melalui pratinjau dari pihak CFTT-nya. Dengan memberikan rekomendasi perbaikan aplikasi terhadap kebutuhan yang disebutkan pada hasil analisis diharapkan kedepan ada perbaikan aplikasi tersebut sehingga dapat digunakan oleh ahli forensik maupun laboratorium forensik terutama pada lingkungan akademik

.

# BAB 5
# Kesimpulan dan Saran

## Kesimpulan

Kesimpulan pada penelitian berhasil melakukan pengujian aplikasi *web based android analysis tools* dengan belkasoft berdasarkan standar CFTT, dengan hasil yang didapat dari aplikasi *web based* sebanyak tujuh variabel data yaitu *data contact, call log, social media, sms massage, network connected, application, account dan screen lock*. Setelah melakukan evaluasi dari hasil kedua aplikasi, didapatkan data yang sesuai dengan laporan *federated testing* hanya empat variabel data sesuai yaitu *call log, social media, sms massage* dan data *email*, adapun beberapa data yang belum di support aplikasi *web based* disebabkan karena kebutuhan yang digunakan pada saat perancangan sistem aplikasi *web based* tersebut tidak menggunakan fungsional kebutuhan CFTT, sehingga aplikasi tersebut belum mampu menghasilkan data secara menyeluruh.

Pengujian aplikasi belkasoft dalam kasus ini hanya digunakan sebagai alat pendukung pengujian aplikasi web-based untuk mengukur kemampuan aplikasi web-based terhadap data yang dihasilkan, hasil pengujian aplikasi web-based tidak bisa dibandingkan dengan belkasoft karena aplikasi belkasoft merupakan aplikasi profesional yang mana semua kebutuhan fungsionalnya sudah didasarkan pada standar forensik dan diuji secara profesional, sedangkan aplikasi web-based adalah aplikasi akademik yang dibuat dengan fungsional kebutuhannya dalam lingkup kecil sehingga parameter yang dihasilkan juga belum memenuhi standar secara fungsional kebutuhan. Untuk itu dilakukan pengujian aplikasi web-based untuk mengevaluasi parameter yang dihasilkan berdasarkan standar CFTT, dan memberikan rekomendasi perbaikan kedepannya, sehingga diharapkan bisa digunakan dalam keperluan forensik.

## Saran

Berdasarkan hasil pengujian sesuai dengan batasan masalah diatas bahwa dapat diketahui hasil pengujian aplikasi *web based android analysis tools* belum mampu menghasilkan data secara lengkap sesuai dengan parameter fungsional dari laporan *federated testing*, hal tersebut disebabkan karena kebutuhan yang digunakan pada perancangan sistem menggunakan fungsional kebutuhan secara independen sehingga berpengaruh terhadap hasil yang didaptkan, kekurangan dari aplikasi web-based terlihat setelah dilakukan perbandingan parameter dari perbandingan hasil dari belkasoft dan parameter fungsional pada CFTT.

Kekurangan pada aplikasi web-based tersebut diharapkan kedepannya bisa dikembangkan menggunakan parameter dari fungsional CFTT. sehingga aplikasi web-based bisa digunakan oleh ahli forensik atau laboratorium forensik dalam penanganan kasus mobile forensik. rekomendasi yang diberikan untuk perbaikan kedepan diantaranya:

1. Perbaikan terhadap parameter-parameter yang belum diperoleh dari aplikasi web-based sesuai parameter CFTT.
2. Mengklasifikasi data yang diperoleh sesuai dengan kategori.
3. Menambahkan fitur report pada aplikasi yang mampu *generate* laporan investigasi terhadap kasus yang ditangani.

# Daftar Pustaka


Agarwal, A., Gupta, M., Gupta, S., & Gupta, S. C. (2011). Systematic digital forensic investigation model. *International Journal of Computer Science and Security (IJCSS)*, *5*(1), 118–131. http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.227.8647&rep=rep1&type=pdf

Albanna, F., & Riadi, I. (2017). Forensic Analysis of Frozen Hard Drive Using Static Forensics Method. *International Journal of Computer Science and Information Security (IJCSIS)*, *15*(1).

Casey, E. (2011). *Digital Evidence and Computer Crime, Third Edition*. 840.

Du, X., Le-Khac, N. A., & Scanlon, M. (2017). Evaluation of digital forensic process models with respect to digital forensics as a service. *European Conference on Information Warfare and Security, ECCWS*, 573–581.

Guttman, B., Lyle, J. R., & Ayers, R. (2014). Ten years of computer forensic tool testing. *Digital Evidence and Electronic Signature Law Review*, *8*(0), 139–147. https://doi.org/10.14296/deeslr.v8i0.1963

Horsman, G. (2019). Tool testing and reliability issues in the field of digital forensics. *Digital Investigation*, *28*, 163–175. https://doi.org/10.1016/j.diin.2019.01.009

Karen Kent, Suzanne Chevalier, Tim Grance, H. D. (2006). Guide to integrating forensic techniques into incident response (NIST Special Publication 800-86). *NIST Special Publication, August*, 800–886. http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-86.pdf

Kostadinov Dimitar. (2019). *The Mobile Forensics Process: Steps & Types - Infosec Resources*. Infosec Resources. https://resources.infosecinstitute.com/topic/mobile-forensics-process-steps-types/

Madiyanto, S., Mubarok, H., & Widiyasono, N. (2017). Mobile Forensics Investigation Proses Investigasi Mobile Forensics Pada Smartphone Berbasis IOS. *Jurnal Rekayasa Sistem & Industri (JRSI)*, *4*(01), 93–98. https://doi.org/10.25124/jrsi.v4i01.149

Marcella Jr., A., & Menendez, D. (2010). Cyber Forensics. In *Cyber Forensics*. https://doi.org/10.1201/9780849383298

Newzoo. (2017). *Top Countries/Markets by Smartphone Penetration & Users | Newzoo*. https://newzoo.com/insights/rankings/top-countries-by-smartphone-penetration-and-

users/

NIST. (2011). Computer Forensics Tool Testing (CFTT) Project Overview. In *NIST*. https://www.nist.gov/itl/ssd/software-quality-group/computer-forensics-tool-testing-program-CFTT

Polri. (2020). *Patroli Siber*. https://patrolisiber.id/statistic

Riadi, I., Sunardi, S., & Sahiruddin, S. (2019). Analisis Forensik Recovery pada Smartphone Android Menggunakan Metode National Institute Of Justice (NIJ). *Jurnal Rekayasa Teknologi Informasi (JURTI)*, *3*(1), 87–95.

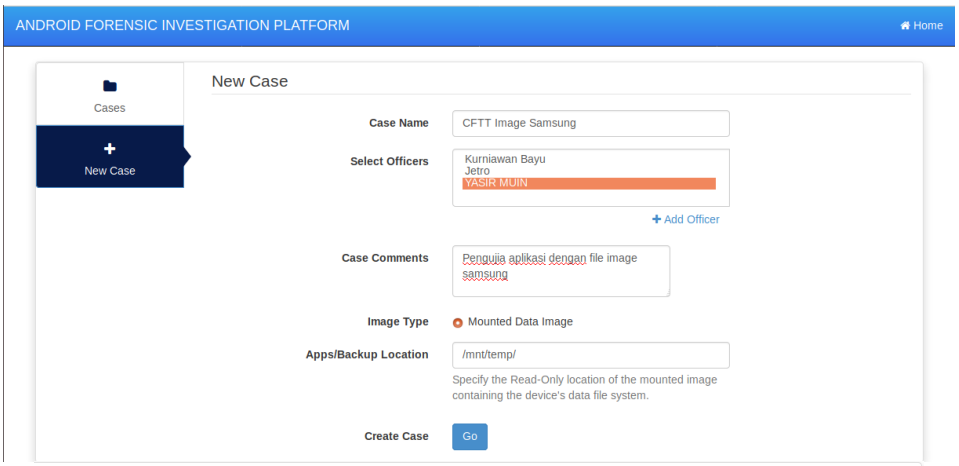
Riadi, I., Umar, R., & Firdonsyah, A. (2017). Identification Of Digital Evidence On Android's Blackberry Messenger Using NIST Mobile Forensic Method. *International Journal of Computer Science and Information Security*, *15*(5), 3–8.

Roy, S., Wu, Y., & LaVenia, K. N. (2019). Experience of incorporating NIST standards in a digital forensics curricula. *7th International Symposium on Digital Forensics and Security, ISDFS 2019*. https://doi.org/10.1109/ISDFS.2019.8757533

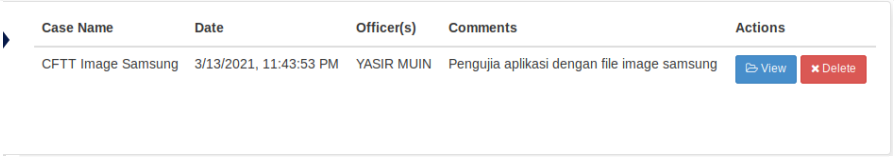
# LAMPIRAN A

Lampiran Hasil Pengujian Aplikasi *Web Based Android Analysis Tools*

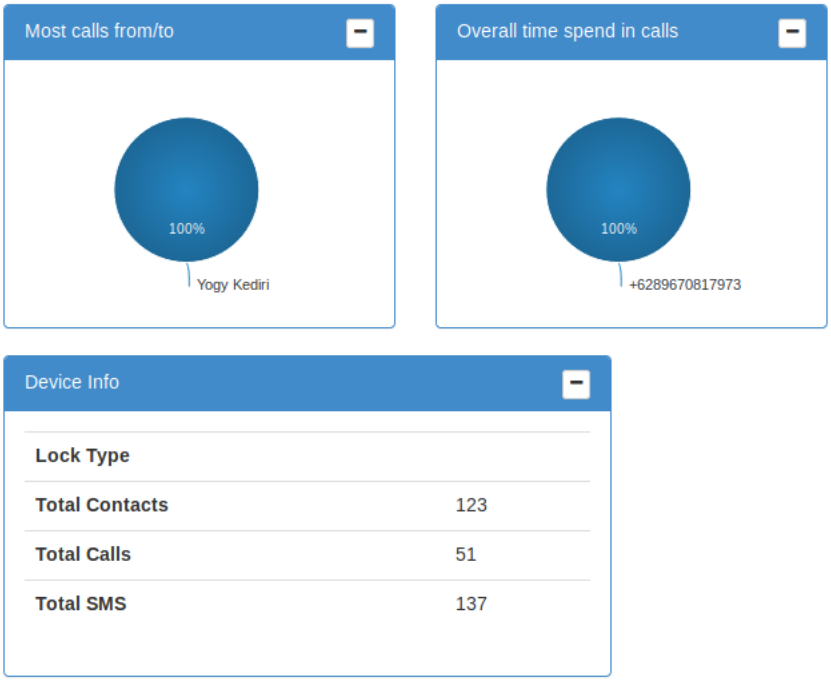
1



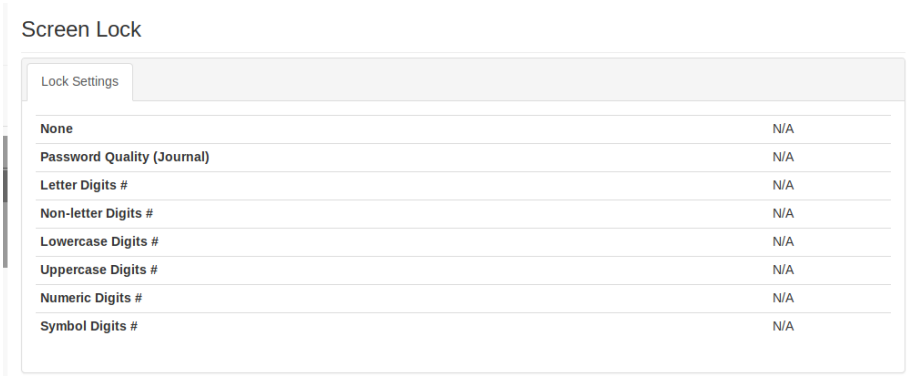

2




3




4



5

## Accounts

Sync Accounts

Show 100 entries Search:

| Id | Account | Owning User | None | Authority | Ena |
|---|---|---|---|---|---|
| 82 | _@students.uii.ac.id | 0 | com.google | com.android.calendar | true |
| 108 | _@gmail.com | 0 | com.google | com.android.calendar | true |
| 134 | _@gmail.com | 0 | com.google | com.android.calendar | true |
| 94 | _@students.uii.ac.id | 0 | com.google | com.android.chrome | false |
| 119 | _@gmail.com | 0 | com.google | com.android.chrome | true |
| 145 | @gmail.com | 0 | com.google | com.android.chrome | false |
| 1 | PHONE | 0 | com.android.localphone | com.android.contacts | false |
| 87 | _@students.uii.ac.id | 0 | com.google | com.android.contacts | true |
| 101 | WhatsApp | 0 | com.whatsapp | com.android.contacts | true |
| 113 | _@gmail.com | 0 | com.google | com.android.contacts | true |
| 130 | Facebook | 0 | com.facebook.auth.login | com.android.contacts | false |
| 139 | _@gmail.com | 0 | com.google | com.android.contacts | true |

6

## Youtube

Accounts

Show 100 entries Search:

| account |
|---|
| 29@students.uii.ac.id |

Showing 1 to 1 of 1 entries Previous 1 Next

7

## Packages & Permissions

Available Permissions | Installed Applications | Platform Version

| Name | Package | Protection |
|---|---|---|
| com.google.android.gms.auth.api.phone.permission.SEND | com.google.android.gms | SIGNATURE |
| android.permission.REAL_GET_TASKS | android | SYSTEM + SIGNATURE |
| android.permission.SEND_RECEIVE_STK_INTENT | com.android.stk | SIGNATURE |
| android.permission.REMOTE_AUDIO_PLAYBACK | android | SIGNATURE |
| android.permission.DOWNLOAD_WITHOUT_NOTIFICATION | com.android.providers.downloads | N/A |
| com.google.android.apps.photos.permission.C2D_MESSAGE | com.google.android.apps.photos | SIGNATURE |
| android.permission.INTENT_FILTER_VERIFICATION_AGENT | android | SYSTEM + SIGNATURE |
| android.permission.BIND_INCALL_SERVICE | android | SYSTEM + SIGNATURE |
| com.android.gallery3d.permission.GALLERY_PROVIDER | com.android.gallery3d | SYSTEM + SIGNATURE |
| com.google.android.gms.trustagent.framework.model.DATA_CHANGE_NOTIFICATION | com.google.android.gms | SIGNATURE |
| android.permission.WRITE_SETTINGS | android | 192SIGNATURE |
| com.google.android.gm.permission.WRITE_GMAIL | com.google.android.gm | SIGNATURE |
| com.google.android.vending.verifier.ACCESS_VERIFIER | com.android.vending | SIGNATURE |
| com.google.android.finsky.permission.BIND_GET_INSTALL_REFERRER_SERVICE | com.android.vending | N/A |
| android.permission.READ_SMS | android | DANGEROUS |

8

## Packages & Permissions

Available Permissions | Installed Applications | Platform Version

| Package Name | APK Path | Flags | First Install Time | Install Time | Update Time | Version | User ID | In |
|---|---|---|---|---|---|---|---|---|
| com.google.android.youtube | /system/app/YouTube | N/A | 1567957634 | 1567957634 | 1567957634 | 1421542300 | 10082 | N/ |
| stericson.busybox | /data/app/stericson.busybox-1 | N/A | 1569852237 | 1569852241 | 1569852241 | 199 | 10101 | N/ |
| com.android.providers.telephony | /system/priv-app/TelephonyProvider | N/A | 1494844121 | 1494844121 | 1494844121 | 23 | N/A | N/ |
| com.google.android.googlequicksearchbox | /data/app /com.google.android.googlequicksearchbox-1 | N/A | 1567956624 | 1494844063 | 1567956781 | 301008051 | 10031 | cc |
| com.android.providers.calendar | /system/priv-app/CalendarProvider | N/A | 1494844089 | 1494844089 | 1494844089 | 23 | N/A | N/ |
| com.android.providers.media | /system/priv-app/MediaProvider | N/A | 1494844089 | 1494844089 | 1494844089 | 800 | N/A | N/ |
| com.google.android.onetimeinitializer | /system/priv-app/GoogleOneTimeInitializer | N/A | 1494844089 | 1494844089 | 1494844089 | 23 | 10014 | N/ |
| com.qualcomm.qti.modemtestmode | /system/app/ModemTestMode | N/A | 1494844112 | 1494844112 | 1494844112 | 23 | N/A | N/ |
| com.qualcomm.shutdownlistner | /system/app/shutdownlistener | N/A | 1494844115 | 1494844115 | 1494844115 | 23 | 10084 | N/ |
| com.android.wallpapercropper | /system/priv-app/WallpaperCropper | N/A | 1494844256 | 1494844256 | 1494844256 | 23 | 10033 | N/ |
| com.quicinc.cne.CNEService | /system/priv-app/CNEService | N/A | 1494844089 | 1494844089 | 1494844089 | 1 | N/A | N/ |
| com.android.profile | /system/app/ProfileMgr | N/A | 1494844084 | 1494844084 | 1494844084 | 4 | N/A | N/ |
| com.android.protips | /system/app/Protips | N/A | 1494844137 | 1494844137 | 1494844137 | 1 | 10074 | N/ |
| com.qualcomm.qti.phonefeature | /system/app/PhoneFeatures | N/A | 1494844112 | 1494844112 | 1494844112 | 23 | N/A | N/ |
| com.speedsoftware.rootexplorer | /data/app/com.speedsoftware.rootexplorer-1 | N/A | 1569253608 | 1569253633 | 1569253633 | 143 | 10098 | N/ |
| alled_apps oid.documentsui | /system/app/DocumentsUI | N/A | 1494844245 | 1494844245 | 1494844245 | 23 | 10045 | N/ |

## Packages & Permissions

Available Permissions | Installed Applications | Platform Version

| Platform Version | N/A |
|---|---|

9

Wifi Information

Connected Networks | Device Info | Wifi Tethering

Show 100 entries Search:

| Network SSID | AP Address | Security | Password | Network Priority |
|---|---|---|---|---|
| "-_-" | N/A | WPA-PSK | "aingmaung" | 19 |
| "Backyndlogok" | N/A | WPA-PSK | "kemiganteng1234" | 14 |
| "eduroam" | N/A | WPA-EAP IEEE8021X | N/A | 18 |
| "h3h3" | N/A | NONE | N/A | 2 |
| "h3h3" | N/A | WPA-PSK | "jethro1412" | 17 |
| "jet" | N/A | NONE | N/A | 20 |
| "Jethro" | N/A | WPA-PSK | "jembuswedhut322" | 1 |
| "rahasia" | N/A | NONE | N/A | N/A |
| "Realme " | N/A | WPA-PSK | "jembuswedhut322" | 3 |
| "TOTOLINK N300RT" | N/A | NONE | N/A | 9 |

Showing 1 to 10 of 10 entries Previous 1 Next

10

Wifi Information

Connected Networks | Device Info | Wifi Tethering

| | |
|---|---|
| **Wifi Interface** | /data/misc/wifi/sockets |
| **None** | S50D |
| **Manufacturer** | QUALCOMM |

11

Wifi Information

Connected Networks | Device Info | Wifi Tethering

| | |
|---|---|
| **Tethering Interface** | wlan0 |
| **Network Name** | EVERCOSS S50 |
| **Channel** | 11 |
| **WPA Passkey** | 0123456789abcdef0123456789abcdef0123456789abcdef0123456789abcdef |
| **File Version** | 2 |
| **AP Network Name (Software)** | EVERCOSS S50 |
| **Security** | NONE |
| **Password (Plain)** | |

12

DHCP Information

Dnsmasq Leases

| None | Client MAC Address | Leased IP Address | Hostname |
|---|---|---|---|
| 1578210759 | 58:85:a2:4c:dc:bb | 192.168.43.128 | realme-3-Pro |
| 1578211001 | d6:66:64:75:2e:1d | 192.168.43.63 | * |

13

Telephony

Calls | SMS Messages

| Date | Type | Number | Contact | Duration (seconds) | Number Geolocation |
|---|---|---|---|---|---|
| 1570627201 | Incoming | [illegible] | None | 5 | Indonesia |
| 1570672659 | Missed | [illegible] | None | 0 | Greater Jakarta |
| 1570680297 | Missed | [illegible] | None | 0 | Greater Jakarta |
| 1571116537 | Missed | [illegible] | None | 0 | Indonesia |
| 1571287728 | Missed | [illegible] | None | 0 | Greater Jakarta |
| 1571404121 | Missed | [illegible] | None | 0 | Indonesia |
| 1571482905 | Missed | [illegible] | None | 0 | Indonesia |
| 1571483683 | Missed | [illegible] | None | 0 | Indonesia |
| 1572274205 | Missed | [illegible] | None | 0 | Indonesia |
| 1572580138 | Missed | [illegible] | None | 0 | New York |
| 1573370906 | Missed | [illegible] | Unknown | 0 | Indonesia |
| 1573387054 | Missed | [illegible] | Unknown | 0 | Indonesia |
| 1573537413 | Missed | [illegible] | None | 0 | Greater Jakarta |
| 1573636103 | Missed | [illegible] | None | 0 | Greater Jakarta |

14

Calls | SMS Messages

| Message ID | Status | Type | Date Send | Local Date | From/To | Seen | Message |
|---|---|---|---|---|---|---|---|
| 1 | OK | Incoming | 1570703094 | 1570703097 | 111 | Yes | KUOTA makin BESAR, BAYAR mkn MURAH! 4GB CUMA 20rb utk 7hr. BALAS HP utk aktifkan. Nikmati 1GB +3GB jam1-12 skrg. BURUAAN sebelum PROMOnya HABIS! AS122 |
| 2 | OK | Incoming | 1570703094 | 1570703251 | 111 | Yes | KUOTA makin BESAR, BAYAR mkn MURAH! 4GB CUMA 20rb utk 7hr. BALAS HP utk aktifkan. Nikmati 1GB +3GB jam1-12 skrg. BURUAAN sebelum PROMOnya HABIS! AS122 |
| 3 | OK | Incoming | 1570707925 | 1570707927 | 123 | Yes | Paket MAU 2.5GB(.85+1.65)+25mnt 1hr gagal diperbarui karena pulsa tidak mencukupi. Segera isi pulsa dan cek paket menarik di *123# atau bima+, klik http://bit.ly/BIMA3 |
| 4 | OK | Incoming | 1570710636 | 1570710638 | 111 | Yes | 70 Menit BEBAS BICARA cuma 5rb! 20 Menit ke semua operator & 50 Menit ke sesama Tri. Balas AS utk beli. Cek Hot Sale di *123*4#. Kirim Pulsa & Paket di *323# |
| 5 | OK | Incoming | 1570753422 | 1570753423 | 111 | Yes | Kuota 3GB CUMA Rp 3,5rb siap bikin harimu jadi SERU! Balas AK untuk aktifkan. Nikmati 1GB +2GB (01-09) + 30mnt telp sesama Tri buat SEHARIAN. AS508 |
| 6 | OK | Incoming | 1570794326 | 1570794328 | 123 | Yes | Paket MAU 2.5GB(.85+1.65)+25mnt 1hr gagal diperbarui |

15

Internet Chats

Facebook Messenger Chats | Whatsapp Messages

| Date | Sender | Type | Attachments | Text |
|---|---|---|---|---|
| 1577837526 | Juan Ferdiansyah | Unknown | None | You and Juan Ferdiansyah are celebrating 2 years of friendship on Facebook |
| 1514775215 | Juan Ferdiansyah | Unknown | None | Say hi to your new Facebook friend, Juan. |
| 0 | N/A | BEFORE_FIRST_SENTINEL | None | None |
| 1577682033 | Kurniawan Bayu | REGULAR | None | https://www83*.zippyshare.com/v/Z2fjhUt2/file.html |
| 1577681173 | Kurniawan Bayu | REGULAR | None | |
| 1577681009 | Kurniawan Bayu | REGULAR | None | https://nopy.to/L7rA4rw9/four_elements_trainer_v084a-pc.zip |
| 1574861388 | Kurniawan Bayu | REGULAR | None | curl --request POST \ --url https://pro.rajaongkir.com/api/cost \ --header 'conter |
| 1573828840 | Kurniawan Bayu | REGULAR | None | |
| 1573828827 | Kurniawan Bayu | REGULAR | None | Link |

16

Facebook Messenger Chats | Whatsapp Messages

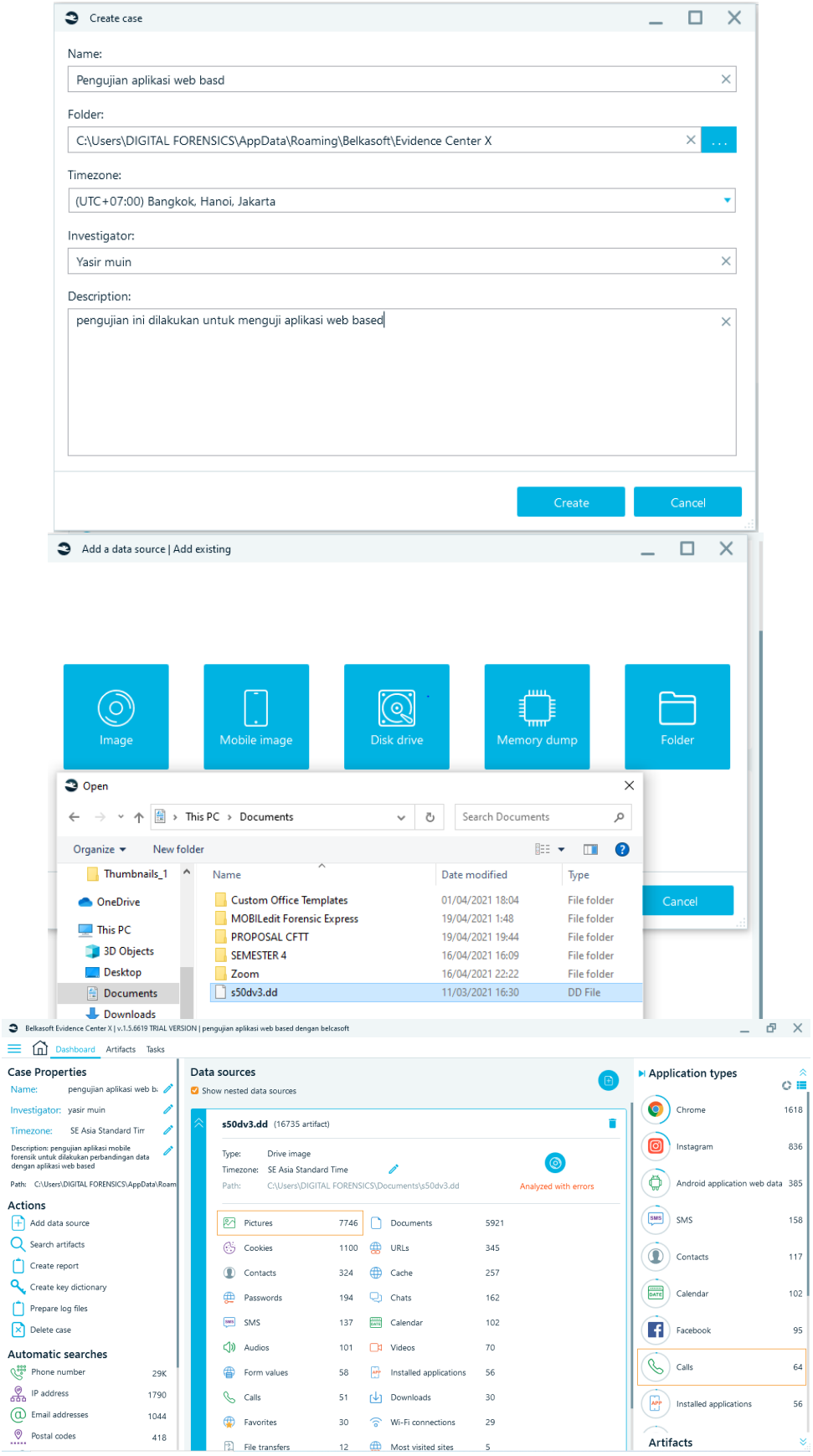
| Origin | Send Date | Received Date | Status | Message | Raw Message |
|---|---|---|---|---|---|
| 0 | -1 | -1 | -1 | None | None |
| 0 | -1 | 1578195825 | 6 | None | None |
| 0 | -1 | 1578195825 | 6 | None | None |
| 0 | -1 | 1578195825 | 6 | None | None |
| 0 | -1 | 1578195825 | 6 | None | None |
| 0 | -1 | 1578197434 | 0 | None | None |

17

Contacts | Whatsapp Contacts

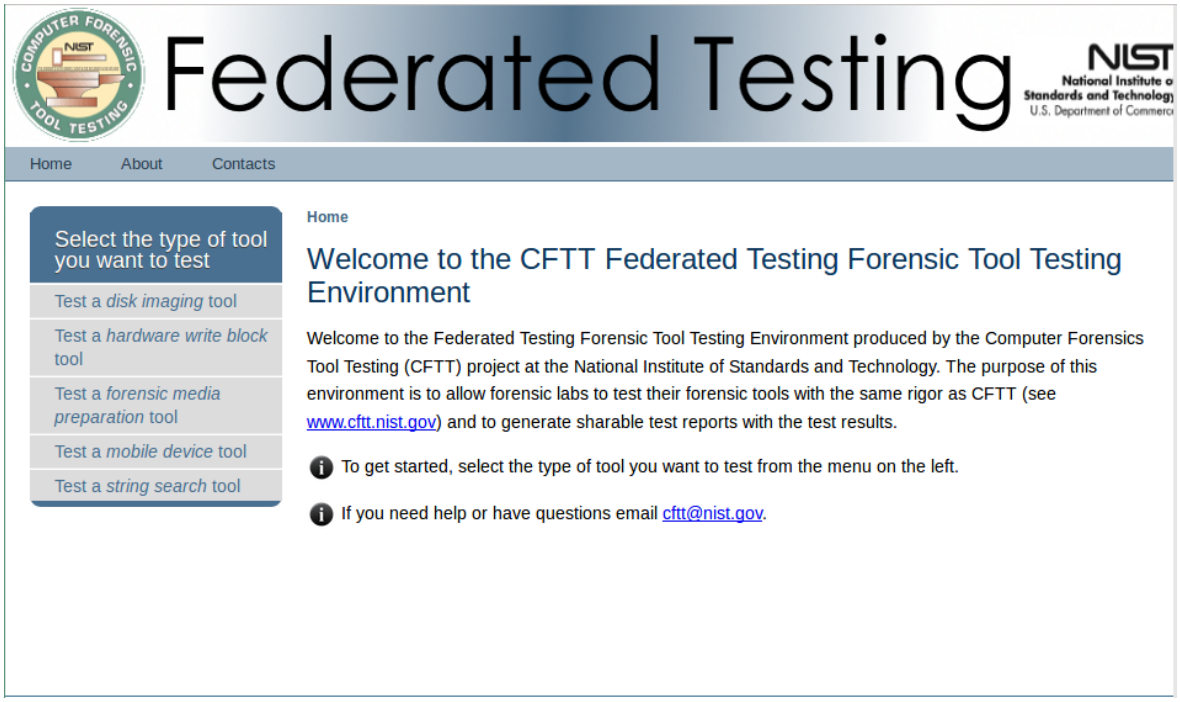
| Whatsapp Name | Display Name | Number | Phone Type | Whatsapp ID | Whatsapp User |
|---|---|---|---|---|---|
| None | Mas Anto Geyang | [redacted] | Mobile | [redacted]2@s.whatsapp.net | No |
| None | Camid | [redacted] | Mobile | [redacted]0@s.whatsapp.net | No |
| None | Ibu | [redacted] | Mobile | [redacted]8@s.whatsapp.net | No |
| None | Insan | [redacted] | Mobile | [redacted]5@s.whatsapp.net | Yes |
| None | Tiger Revi | [redacted] | Mobile | [redacted]0@s.whatsapp.net | No |
| None | Om Han | [redacted] | Mobile | [redacted]5@s.whatsapp.net | No |
| None | Bu Cici Dosen Informatika | [redacted] | Mobile | [redacted]4@s.whatsapp.net | Yes |
| None | Ravado | [redacted] | Mobile | [redacted]3@s.whatsapp.net | Yes |
| None | Sang Hapekik | [redacted] | Mobile | [redacted]3@s.whatsapp.net | Yes |
| None | Itznaini Ebes | [redacted] | Mobile | [redacted]57@s.whatsapp.net | No |
| None | Bapak E Yogy | [redacted] | Mobile | [redacted]5@s.whatsapp.net | Yes |
| None | PAK HARRIS IGS | [redacted] | Mobile | [redacted]8@s.whatsapp.net | Yes |
| None | Kos Kidung Pak Sono | [redacted] | Mobile | [redacted]8@s.whatsapp.net | Yes |
| None | Kamplenk | [redacted] | Mobile | [redacted]2@s.whatsapp.net | Yes |

Lampiran hasil pengujian aplikasi belkasoft

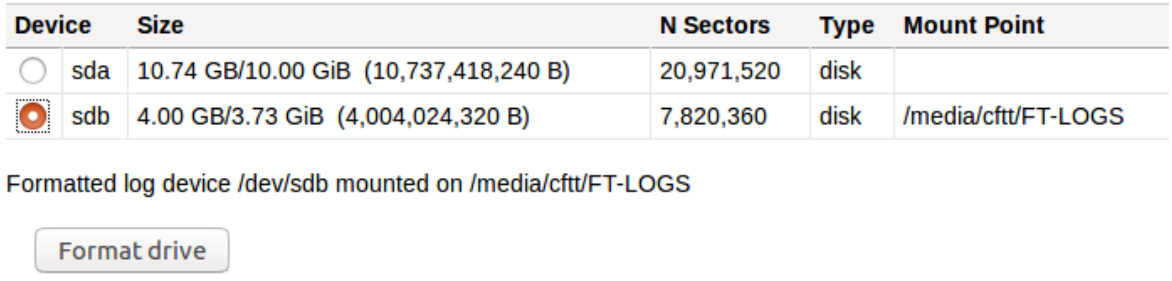


Lampiran Hasil Pengujian Aplikasi *Web Based Android Analysis Tools*

18




19

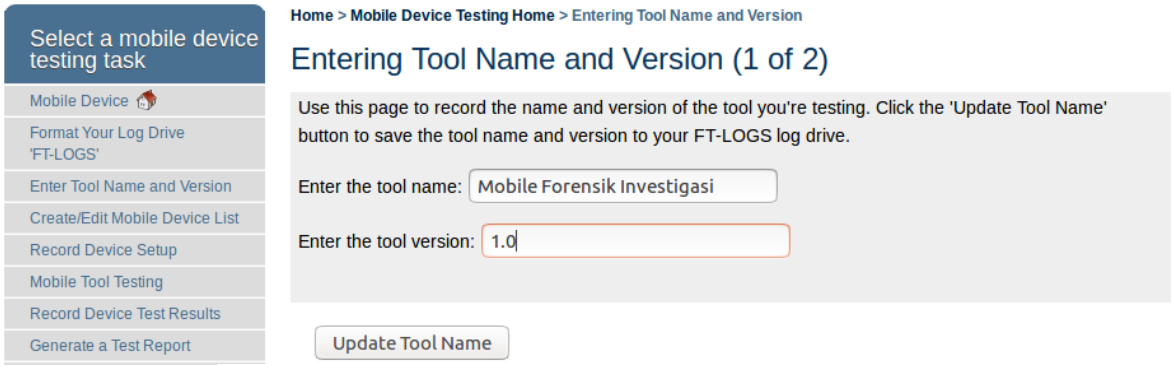


| Device | | Size | N Sectors | Type | Mount Point |
|---|---|---|---|---|---|
| ○ | sda | 10.74 GB/10.00 GiB (10,737,418,240 B) | 20,971,520 | disk | |
| ◉ | sdb | 4.00 GB/3.73 GiB (4,004,024,320 B) | 7,820,360 | disk | /media/cftt/FT-LOGS |

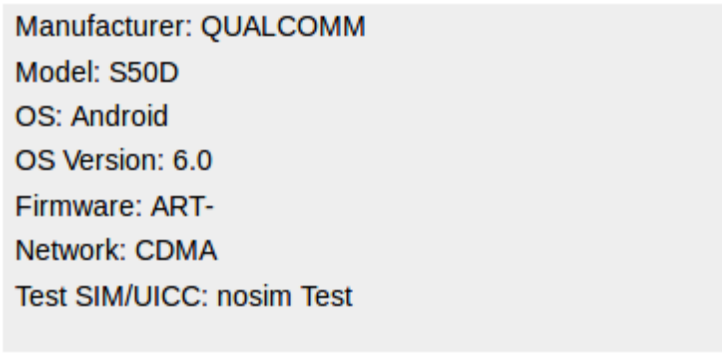
Formatted log device /dev/sdb mounted on /media/cftt/FT-LOGS

Format drive

20




21



22

*List of Test Devices*

| Select | Make | Model | OS | Version | Firmware | Network | SIM/UICC |
|---|---|---|---|---|---|---|---|
| *No devices - complete the form below and click 'Add New Device' to add a device.* | | | | | | | |

**Describe a new device or edit an existing device:**

Enter the device manufacturer: QUALCOMM

Enter the device model and model number: S50D

Select the device OS: Android

Enter the device OS Version: 6.0

Enter the device firmware: ART-

Select the device network: CDMA

- ○ Test SIM/UICC card acquisition with this phone
- ◉ No test of SIM/UICC card acquisition test

Add New Device | Update Selected Device | Delete Selected Device

**Selected Device:**

Manufacturer: *QUALCOMM*

Model: *S50D*

23

*Documenting Device Setup*

| Data Type | | Setup | |
|---|---|---|---|
| PIM Data: Contacts/Address Book Entries | Regular Length | ◉ Populated | ○ Omitted |
| | Maximum Length | ◉ Populated | ○ Omitted |
| | Special Character | ◉ Populated | ○ Omitted |
| | Blank Name | ◉ Populated | ○ Omitted |
| | Regular Length, email | ◉ Populated | ○ Omitted |
| | Regular Length, graphic | ◉ Populated | ○ Omitted |
| | Regular Length, Address | ◉ Populated | ○ Omitted |
| | Non-Latin Entry | ◉ Populated | ○ Omitted |
| | Contact Groups | ◉ Populated | ○ Omitted |
| | Deleted Entry | ◉ Populated | ○ Omitted |

24

| | | | |
|---|---|---|---|
| PIM Data: Calendar data, Memos | Regular Length | Populated | Omitted |
| | Maximum Length | Populated | Omitted |
| | Special Character | Populated | Omitted |
| | Blank Entry | Populated | Omitted |
| | Deleted Entry | Populated | Omitted |
| Stand-alone data files | Audio | Populated | Omitted |
| | Graphic | Populated | Omitted |
| | Video | Populated | Omitted |
| | Documents | Populated | Omitted |
| | Audio – Deleted | Populated | Omitted |
| | Graphic - Deleted | Populated | Omitted |
| | Video - Deleted | Populated | Omitted |
| | Documents - Deleted | Populated | Omitted |
| Call Logs | Incoming | Populated | Omitted |
| | Outgoing | Populated | Omitted |
| | Missed | Populated | Omitted |
| | Incoming – Deleted | Populated | Omitted |
| | Outgoing – Deleted | Populated | Omitted |
| | Missed - Deleted | Populated | Omitted |
| SMS/EMS Messages | Incoming SMS – Read | Populated | Omitted |
| | Incoming SMS – Unread | Populated | Omitted |
| | Incoming SMS – Deleted | Populated | Omitted |
| | Incoming EMS – Read | Populated | Omitted |
| | Incoming EMS – Unread | Populated | Omitted |
| | Incoming EMS – Deleted | Populated | Omitted |
| | Outgoing SMS | Populated | Omitted |
| | Outgoing Group SMS | Populated | Omitted |
| | Outgoing SMS – Deleted | Populated | Omitted |
| | Outgoing EMS | Populated | Omitted |
| | Outgoing Group EMS | Populated | Omitted |
| | Outgoing EMS – Deleted | Populated | Omitted |
| MMS Messages | Incoming Audio | Populated | Omitted |
| | Incoming Graphic | Populated | Omitted |
| | Incoming Video | Populated | Omitted |
| | Outgoing Audio | Populated | Omitted |
| | Outgoing Graphic | Populated | Omitted |
| | Outgoing Video | Populated | Omitted |
| Location Data | GPS Coordinates | Populated | Omitted |
| | Geo-tagged Data | Populated | Omitted |

| | | | |
|---|---|---|---|
| Browser/Email Data | Visited Sites | Populated | Omitted |
| | Bookmarks | Populated | Omitted |
| | Email | Populated | Omitted |
| Social Media Data | Application 1, e.g., Facebook | Populated | Omitted |
| | Application 2, e.g., Twitter | Populated | Omitted |
| | Application 3, e.g., LinkedIn | Populated | Omitted |
| | Application 4, e.g., Instagram | Populated | Omitted |
| Other Applications of Interest | Other Applications of Interest | Populated | Omitted |

*List of Test Devices*

| Select | Make | Model | OS | Version | Firmware | Network | SIM/UICC |
|---|---|---|---|---|---|---|---|
| | QUALCOMM | S50D | Android | 6.0 | ART- | CDMA | No SIM/UICC |

25

Continue

*Essential* and *Optional* Test Runs

| Fed Testing - Mobile | Acquire All | Connectivity | Case File/Data Protection | Hashing | SIM/UICC Authentication |
|---|---|---|---|---|---|
| *Essential* | x | | | | |
| *Optional* | | x | x | x | x |

26

*List of Test Devices*

| Select | Make | Model | OS | Version | Firmware | Network | SIM/UICC |
|---|---|---|---|---|---|---|---|
| | QUALCOMM | S50D | Android | 6.0 | ART- | CDMA | No SIM/UICC |

Continue

**Selected Device:**

Manufacturer: *QUALCOMM*

Model: *S50D*

*Results Key*

| Result | Definition |
|---|---|
| *As Expected* | The mobile forensic application returned expected test results – the tool acquired and reported data from the mobile device or SIM/UICC successfully. |
| *Partial* | The mobile forensic application returned some of data from the mobile device or SIM/UICC. |
| *Not as Expected* | The mobile forensic application failed to return expected test results – the tool did not acquire or report supported data from the mobile device or SIM/UICC successfully. |
| *N/A* | Not Applicable – the mobile forensic application is unable to perform the test or the tool does not provide support for the acquisition for a particular data element. |

27

28

## Device Test Results

*Documenting Device Test Results*

| Entry | | Result | | | |
|---|---|---|---|---|---|
| Acquisition | Acquire All | (●) As Expected | ( ) Partial | ( ) Not as Expected | ( ) N/A |
| | Disrupted | ( ) As Expected | (●) Partial | ( ) Not as Expected | ( ) N/A |
| | Notes: | | | | |
| Reporting | Preview-Pane | (●) As Expected | ( ) Partial | ( ) Not as Expected | ( ) N/A |
| | Generated Reports | (●) As Expected | ( ) Partial | ( ) Not as Expected | ( ) N/A |
| | Notes: | | | | |
| Equipment/User Data | IMEI | ( ) As Expected | ( ) Partial | ( ) Not as Expected | (●) N/A |
| | MEID/ESN | ( ) As Expected | ( ) Partial | ( ) Not as Expected | (●) N/A |
| | MSISDN/MIN | ( ) As Expected | ( ) Partial | ( ) Not as Expected | (●) N/A |
| | Notes: | | | | |
| PIM Data | Contacts | (●) As Expected | ( ) Partial | ( ) Not as Expected | ( ) N/A |
| | Calendar | ( ) As Expected | ( ) Partial | ( ) Not as Expected | (●) N/A |
| | Memos/Notes | ( ) As Expected | ( ) Partial | ( ) Not as Expected | (●) N/A |
| | Notes: | | | | |
| Stand-alone Data Files | Audio | ( ) As Expected | ( ) Partial | ( ) Not as Expected | (●) N/A |
| | Graphic | ( ) As Expected | ( ) Partial | ( ) Not as Expected | (●) N/A |
| | Video | ( ) As Expected | ( ) Partial | ( ) Not as Expected | (●) N/A |
| | Documents | ( ) As Expected | ( ) Partial | ( ) Not as Expected | (●) N/A |
| | Notes: | | | | |
| Call Logs | Incoming | (●) As Expected | ( ) Partial | ( ) Not as Expected | ( ) N/A |
| | Outgoing | (●) As Expected | ( ) Partial | ( ) Not as Expected | ( ) N/A |
| | Missed | (●) As Expected | ( ) Partial | ( ) Not as Expected | ( ) N/A |
| | Notes: | | | | |

| | | | | | |
|---|---|---|---|---|---|
| SMS/EMS Messages | Incoming | ◉ As Expected | ○ Partial | ○ Not as Expected | ○ N/A |
| | Outgoing | ◉ As Expected | ○ Partial | ○ Not as Expected | ○ N/A |
| | Notes: | | | | |
| MMS Messages | Audio | ○ As Expected | ○ Partial | ○ Not as Expected | ◉ N/A |
| | Graphic | ○ As Expected | ○ Partial | ○ Not as Expected | ◉ N/A |
| | Video | ○ As Expected | ○ Partial | ○ Not as Expected | ◉ N/A |
| | Notes: | | | | |
| Location Data | Coordinates/Geo-tagged | ○ As Expected | ○ Partial | ○ Not as Expected | ◉ N/A |
| | Notes: | | | | |
| Browser/Email Data | Visited Sites | ○ As Expected | ○ Partial | ○ Not as Expected | ◉ N/A |
| | Bookmarks | ○ As Expected | ○ Partial | ○ Not as Expected | ◉ N/A |
| | Email | ○ As Expected | ○ Partial | ○ Not as Expected | ◉ N/A |
| | Notes: | | | | |
| Social Media Data | Application 1, e.g., Facebook | ◉ As Expected | ○ Partial | ○ Not as Expected | ○ N/A |
| | Application 2, e.g., Twitter | ○ As Expected | ○ Partial | ○ Not as Expected | ◉ N/A |
| | Application 3, e.g., LinkedIn | ○ As Expected | ○ Partial | ○ Not as Expected | ◉ N/A |
| | Application 4, e.g., Instagram | ○ As Expected | ○ Partial | ○ Not as Expected | ◉ N/A |
| | Notes: | | | | |
| Other Applications of Interest | Other Applications of Interest | ◉ As Expected | ○ Partial | ○ Not as Expected | ○ N/A |
| | Notes: | | | | |
| Non-Latin Character | Reported in native format | ○ As Expected | ○ Partial | ○ Not as Expected | ◉ N/A |
| | Notes: | | | | |
| Hashing | Case File/ Individual Files | ○ As Expected | ○ Partial | ○ Not as Expected | ◉ N/A |
| | Notes: | | | | |
| Case File Data Protection | Modify Case Data | ○ As Expected | ○ Partial | ○ Not as Expected | ◉ N/A |
| | Notes: | | | | |

29

| Data Objects | | QUALCOMMS50D |
|---|---|---|
| PIM Data: Contacts/Address Book Entries | Regular Length | populated |
| | Maximum Length | populated |
| | Special Character | populated |
| | Blank Name | populated |
| | Regular Length, email | populated |
| | Regular Length, graphic | populated |
| | Regular Length, Address | populated |
| | Non-Latin Entry | populated |
| | Contact Groups | populated |
| | Deleted Entry | populated |
| PIM Data: Calendar, Memos | Regular Length | populated |
| | Maximum Length | populated |
| | Special Character | populated |
| | Blank Entry | populated |
| | Deleted Entry | populated |
| Stand-alone data files | Audio | populated |
| | Graphic | populated |
| | Video | populated |
| | Documents | populated |
| | Audio – Deleted | populated |
| | Graphic - Deleted | populated |
| | Video - Deleted | populated |
| | Documents - Deleted | populated |
| Call Logs | Incoming | populated |
| | Outgoing | populated |
| | Missed | populated |
| | Incoming – Deleted | populated |
| | Outgoing – Deleted | populated |
| | Missed - Deleted | populated |
| SMS/EMS Messages | Incoming SMS – Read | populated |
| | Incoming SMS – Unread | populated |
| | Incoming SMS – Deleted | populated |
| | Incoming EMS – Read | populated |
| | Incoming EMS – Unread | populated |
| | Incoming EMS – Deleted | populated |
| | Outgoing SMS | populated |
| | Outgoing Group SMS | populated |
| | Outgoing SMS – Deleted | populated |
| | Outgoing EMS | populated |
| | Outgoing Group EMS | populated |
| | Outgoing EMS – Deleted | populated |
| MMS Messages | Incoming Audio | populated |
| | Incoming Graphic | populated |
| | Incoming Video | populated |
| | Outgoing Audio | populated |
| | Outgoing Graphic | populated |
| | Outgoing Video | populated |
| Location Data | GPS Coordinates | populated |
| | Geo-tagged Data | populated |
| Browser/Email Data | Visited Sites | populated |
| | Bookmarks | populated |
| | Email | populated |
| Social Media Data | Application 1, e.g., Facebook | populated |
| | Application 2, e.g., Twitter | populated |
| | Application 3, e.g., LinkedIn | populated |
| | Application 4, e.g., Instagram | populated |
| Other Applications of Interest | Other Applications of Interest | populated |

| Test Results -- Internal Memory Acquisition | | QUALCOMMS50D |
|---|---|---|
| Acquisition | Acquire All | as expected |
| | Disrupted | partial |
| Reporting | Preview-Pane | as expected |
| | Generated Reports | as expected |
| Equipment/User Data | IMEI | N/A |
| | MEID/ESN | N/A |
| | MSISDN/MIN | N/A |
| PIM Data | Contacts | as expected |
| | Calendar | N/A |
| | Memos/Notes | N/A |
| Stand-alone Data Files | Audio | N/A |
| | Graphic | N/A |
| | Video | N/A |
| | Documents | N/A |
| Call Logs | Incoming | as expected |
| | Outgoing | as expected |
| | Missed | as expected |
| SMS/EMS Messages | Incoming | as expected |
| | Outgoing | as expected |
| MMS Messages | Audio | N/A |
| | Graphic | N/A |
| | Video | N/A |
| Location Data | Coordinates/Geo-tagged | N/A |
| Browser/Email Data | Visited Sites | N/A |
| | Bookmarks | N/A |
| | Email | N/A |
| Social Media Data | Application 1, e.g., Facebook | as expected |
| | Application 2, e.g., Twitter | N/A |
| | Application 3, e.g., LinkedIn | N/A |
| | Application 4, e.g., Instagram | N/A |
| Other Applications of Interest | Other Applications of Interest | as expected |
| Non-Latin Character | Reported in native format | N/A |
| Hashing | Case File/Individual Files | N/A |
| Case File Data Protection | Modify Case Data | N/A |