Jurnal Teknologi Informasi dan Ilmu Komputer (JTIIK) DOI: 10.25126/jtiik.202072220
Vol. 7, No. 3, Juni 2020, hlm. 521-530 p-ISSN: 2355-7699
Akreditasi KEMENRISTEKDIKTI, No. 30/E/KPT/2018 e-ISSN: 2528-6579

ANALISIS FORENSIK ANDROID: ARTEFAK PADA APLIKASI PENYIMPANAN AWAN BOX

Gandeva Bayu Satrya*[1], A. Ahmad Nasrullah[2]

[1]Departemen Sains dan Terapan, Universitas Telkom, [2]Teknik Sistem, XtremaxTeknologi Indonesia
Email: [1]gbs@telkomuniversity.ac.id, [2]aanasrullah@gmail.com
*Penulis Korespondensi

(Naskah masuk: 16 Juli 2020, diterima untuk diterbitkan: 27 April 2020)

Abstrak

Sistem penyimpanan melalui *cloud* memiliki banyak keunggulan, seperti kemampuan akses dari lokasi manapun serta kemudahan penyimpanan pencadangan file pada komputer dan smartphone. Terdapat banyak pilihan layanan penyimpanan melalui *cloud*, seperti Dropbox, Microsoft OneDrive, Google Drive, dan Box. Dari beberapa jenis layanan peyimpanan tersebut Box adalah satu-satunya layanan penyimpanan *cloud* yang mampu menjamin tingkat reliability uptime hingga 99.9%. Awalnya, Box hanya ditujukan untuk kegiatan bisnis saja, namun sekarang Box dapat digunakan oleh pengguna secara umum. Selain memberikan pengaruh yang positif, pertumbuhan penggunaan teknologi layanan penyimpanan *cloud* juga telah memberikan peningkatan dalam peluang terjadinya kejahatan di dunia maya. Forensik digital merupakan solusi terbaru dalam mengamati keamanan sistem dan jaringan, sementara forensik bergerak adalah pengembangan forensik digital yang sepenuhnya difokuskan pada media smartphone. Forensik bergerak dapat dilakukan dalam dua sisi, yaitu server dan klien. Studi kasus dalam penelitian ini berfokus pada penggunaan smartphone Android yang terinstal Box sebagai layanan penyimpanan *cloud*. Sedangkan tujuan utama dari penelitian ini adalah untuk menyediakan sebuah metode forensik bergerak untuk menemukan artefak pada smartphone Android yang telah terinstal dengan aplikasi Box.

Kata kunci: *Forensik Android, forensik bergerak, forensik digital, artefak, penyimpanan awan, analisis Box*

ANDROID FORENSICS ANALYSIS: ARTIFACTS OF BOX CLOUD STORAGE

Abstract

Storing files in a cloud has many advantages, such as the ability to access them from any location and to keep backups of those files on computers and smartphones. There are many choices for cloud storage services, such as Dropbox, Microsoft OneDrive, Google Drive, and Box. Of these, Box is the only cloud storage service that guarantees uptime reliability 99.99% of the time. At first, Box was intended for business use only, but now it is also freely available for public use. Growth in cloud storage technology use has also resulted in increased opportunities for cybercrime to take place. Digital forensics is the latest solution for system and network security observers, while mobile forensics is a development of digital forensics that is fully focused on smartphone media. Mobile forensics can be performed on both the server and client sides. In this research, mobile forensics was performed on the client side. The case study in this paper focused on an Android operating system (OS) smartphone using Box cloud storage. The purpose of this study was to provide a mobile forensics method for finding artifacts on smartphones that have a Box application installed.

Keywords: *Android forensics, mobile forensics, digital forensics, artifacts, cloud storage, Box analysis.*

1. PENDAHULUAN

Modernisasi teknologi Internet kecepatan tinggi telah merubah gaya hidup kita secara signifikan. Tidak dapat disangkal bahwa Internet mampu mengunggah jutaan file, informasi, dan data secara global. Untuk membantu dalam memasok kebutuhan data penyimanan dalam jumlah besar besar , pengembang perangkat lunak Internet telah menyediakan penyimpanan cloud (Hossain et al., 2016)(Man et al., 2016). Penggunaan penyimpanan cloud diharapkan dapat membantu pengguna dalam mempermudah kegiatan *backup, accessibility*, dan *mobility* (Bocchi et al., 2017)(Akter et al., 2018). Penyimpanan *cloud* terdiri dari dua kategori: berbayar dan gratis. Pemilihan layanan penyimpanan *cloud* merupakan hal yang sulit untuk dilakukan. Hal

tersebut dikarenakan setiap aplikasi penyimpanan *cloud* memiliki kelebihan dan kekurangannya masing-masing. Sebagai contoh, sebuah layanan penyimpanan *cloud* mungkin menyediakan ruang data 5 GB tetapi menawarkan folder dan berbagi file di antara banyak pengguna secara bersamaan. Di sisi lain, mungkin juga terdapat layanan penyimpanan *cloud* lain yang menyediakan ruang data lebih besar, tetapi tidak bisa secara bersamaan berbagi folder dan file di antara banyak pengguna. Pada penelitian ini, analisis dan pengujian akan dilakukan pada layanan penyimpanan cloud dengan Box yang menjamin reliability hingga 99% (Box, 2019).

Peningkatan teknologi informasi juga secara tidak secara langsung memfasilitasi individu dan kelompok orang yang ingin melakukan kejahatan dunia maya (Holt et al., 2017)(Satrya & Shin, 2018). Sesuai dengan teori sistem keamanan jaringan, dapat dikatakan bahwa tidak ada sistem yang sepenuhnya aman. Cybercrime dapat terjadi kapan saja dan di mana saja. Cybercrime dapat didefinisikan sebagai pencurian informasi (Valjarevic & Venter, 2016)(Holt et al., 2017). Kejahatan dunia maya sangat difasilitasi oleh kecanggihan teknologi penyimpanan *cloud* dan kemudahan dalam penggunaannya. Laporan berita mencatat bahwa ada banyak perusahaan besar dan kecil yang telah mengalami kebocoran data penting dan rahasia. Jawaban untuk masalah ini adalah menggunakan forensik digital untuk membantu dalam mengidentifikasi pelaku yang melakukan kejahatan dunia maya.

Forensik digital adalah sebuah ilmu yang saat ini mampu meningkatkan ketertarikan antara hukum siber (cyberlaw), keamanan sistem, dan jaringan komputer (McKemmish, 2008)(Chen et al., 2019). Forensik digital telah mengalami pertumbuhan cukup cepat dan telah diterapkan ke dalam komputer, database, jaringan, internal memori, dan forensik bergerak. Forensik bergerak adalah cabang forensik digital yang berkembang pesat dan memiliki banyak sub-cabang sesuai dengan vendor perangkat seluler yang ada. Oleh karena itu, hal tersebut memberikan tantangan bagi peneliti untuk melakukan investigasi dan analisis pada perangkat seluler (Daryabar et al., 2016).

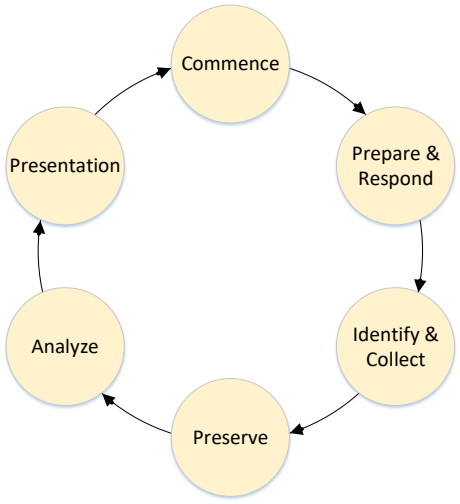
Secara umum, mayoritas pengguna smartphone saat ini adalah pengguna Android. Definisi dari forensik Android sama dengan forensik bergerak (dan hal tersebut merupakan dasar dari forensik digital): tahapannya adalah proses *identification*, *preservation*, *analysis*, dan *presentation* bukti digital pada perangkat seluler yang akan diterima oleh hukum. Fokus dari penelitian ini adalah untuk menganalisis dan menguji penyimpanan *cloud* dengan aplikasi Box pada dua vendor smartphone yang berbeda dan berbagai jenis sistem operasi Android (Chen et al., 2019)(Do et al., 2015). Forensik bergerak dilakukan dengan melakukan forensik digital secara offline dan online, seperti yang akan dilakukan di tempat kejadian perkara (TKP) dalam kasus kehidupan nyata.

Dengan mengadopsi prosedur forensik bergerak, penelitian terhadap penyimpanan awan pada aplikasi Box telah dilakukan dilakukan secara berurutan (McKemmish, 2008)(Daryabar et al., 2016)(Do et al., 2015). Scenario dalam penelitian ini akan dilakukan dalam dua langkah utama. Langkah pertama adalah melakukan 15 skenario pada smartphone pertama yang merupakan OPPO A37 smartphone (Android Lollipop). SHA-128 digunakan untuk memastikan bahwa metadata diambil pada rekam jejak yang dilakukan valid. Alasan dasar untuk menggunakan SHA-128 dalam proses akuisisi yang akan datang adalah bahwa MD5 yang tidak bisa lagi diandalkan. Analisis sementara yang diperoleh pada langkah pertama, lima belas skenario pengujian kemudian memberikan hasil yang sama pada smartphone kedua yaitu Samsung A7 smartphone (Android Nougat). Hal tersebut membuktikan bahwa metode yang digunakan oleh penulis untuk menemukan artefak dan data sisa *(remnant data)* mampu bekerja untuk berbagai vendor dan sistem operasi. Selain itu, hal tersebut juga dapat digunakan sebagai referensi bagi peneliti dan badan hukum dalam menyelesaikan kasus kejahatan dunia maya *(cybercrime)* yang terkait dengan aplikasi Box.

Tahapan selanjutnya dari penelitian ini disusun sebagai berikut. Bab 2 menjelaskan prosedur yang digunakan dalam penyelidikan. Tahapan ini dilakukan dengan kegiatan membandingkan metode secara rinci. Bab 3 menjelaskan hasil data yang diperoleh dari pengujian dan analisis. Bab 4 berisi diskusi dan ringkasan uji secara keseluruhan. Bab 5 menyajikan kesimpulan dan saran dari penelitian ini.

2. METODE PENELITIAN

USULAN METODOLOGI INVESTIGASI



Gambar 1. Digram usulan metodologi forensik

2.1. Commence

Tahapan ini merupakan tahapan dimana keseluruhan rencana telah dibuat (seperti yang

ditampilkan pada gambar 1 diatas), terdiri dari hal apa saja yang kemudian akan dilakukan pada penelitian (Maras et al., 2015)(McKemmish, 2008)(Pichan et al., 2015). Tahapan ini juga akan mengkonfirmasi kasus mana yang akan ditunjuk (dalam hal ini aplikasi Box) dan perangkat mana yang akan terlibat dalam penyelidikan.

Tujuan penelitian adalah untuk mengumpulkan dan menyusun bukti yang dapat disajikan di pengadilan. Ruang lingkup penelitian yang dilakukan adalah proses menemukan artefak dari semua aktivitas pengguna dalam aplikasi Box. Artefak merupakan tantangan bagi forensik investigator dalam menemukan barang bukti yaitu data informasi yang tersisa di smartphone atau komputer. Proses dalam menemukan artefak dilakukan pada aplikasi Box versi 4.28.2 yang diinstal pada sebuah smartphone OPPO A37. Setelah melakukan analisis pada Oppo A37, pengujian juga dilakukan pada smartphone Samsung A7 dengan cara yang sama seperti sebelumnya.

2.2. Prepare & Response

Untuk melakukan investigasi pada komputer dan smartphone, metode dan alat yang dilakukan tentu berbeda. Tahapan ini dilakukan untuk melakukuan penyelidikan dalam forensik digital secara tepat dan efektif. Hal ini sangat penting dilakukan dalam menentukan perangkat lunak mana yang akan digunakan beserta versinya. Pada tahapan ini, daftar perangkat lunak yang akan digunakan dalam forensik bergerak juga ikut ditentukan.

Perhatian lebih terhadap etika di dunia forensik digital yaitu menggunakan perangkat lunak yang dapat digunakan dan standar *(well-known)* di meja hukum *(court)*. Perangkat lunak yang digunakan pada penelitian ini adalah Android Lollipop 5.1.1, Android Nougat 7.0, aplikasi perangkat lunak Box versi 3.6.3, VRoot, Android Debug Bridge (ADB), Sqlite, SqliteBrowser, Busybox Pro v27, dan ES File Explore File Manager v3.2.3.5. Adapun perangkat kerasnya adalah Oppo A37, Samsung A7, dan Laptop Lenovo Y50-70 digunakan untuk proses akuisisi.

2.3. Identify & Collect

Tahapan ini berisi tentang tahapan dalam menentukan sumber penting dari bukti digital (seperti foto TKP, nama organisasi, log Internet, atau log smartphone). Proses identifikasi ini sangat berkaitan dengan kegiatan analisis barang bukti. Dengan kata lain, jika proses identifikasi dan proses pengumpulan tidak selesai, maka hasil yang didapatkan juga tidak lengkap dan tidak dapat diterima di meja hukum.

2.4. Preserve

Untuk penelitian yang mendalam, proses akusisi dan proses duplikasi sebaiknya dilakukan (Satrya et al., 2017). Hal tersebut dikarenakan hal terpenting dalam melakukan forensik bergerak adalah memastikan integritas dan keamanan data ketika proses akuisisi data dilakukan. Dengan keterbatasan waktu yang dimiliki oleh investigator sedangkan sistem operasi pada smartphone sedang bekerja, maka investigator harus melakukan proses akuisisi data secara langsung terhadap smartphone tersangka baik read-only memory (ROM) ataupun random-access memory (RAM). Dalam memastikan integritas hasil akuisisi dilakukan dengan mengambil nilai hash sebelum dan sesudah akuisisi menggunakan SHA-128. Keseluruhan proses penelitian ini telah melalui proses hashing. Pada kasus nyatanya, data asli hanya dapat diamati selama persidangan pidana siber *(cyberlaw)*. Proses duplikasi menghasilkan *image* yang identik dengan aslinya. Berikut ini adalah Algoritma 1 untuk melakukan proses akuisisi data pada aplikasi Box untuk semua kegiatan yang akan dilakukan:

Algoritma 1. Akuisisi database Box
1: **Initialize** inputData;
2: **Initialize** accData;
3: inputData find the "box" database;
4: **Save** inputData **to** "acqBox" database
5: db = query acqBox
6: **while** the db is not empty **do**
7: accData db;
8: **end while**

Untuk tahapan selanjutnya adalalah proses akusisi data yang secara langsung dilakukan. Urutan kegiatan yang dilakukan pada smartphone adalah *installing* Box, *signing up* pada Box, *logging in* ke Box, *uploading files* ke Box, *downloading files* dari Box, *opening files*, membuat *new folders* pada Box, membuat *new file*, *moving the file (move)*, *renaming the file (rename)*, *sharing files*, *deleting files*, *logging out* dari Box and *uninstalling* Box.

Tabel 1. Proses perbandingan dan data analisis pada Box

No	Nama Data	Data Pembanding	Data Dicari
1	Install	Signup	Perubahan pada signup
2	Signup	Logout	Perubahan pada logout
3	Logout	Login	Perubahan pada login
4	Login	Upload	Perubahan pada upload
5	Upload	Download	Perubahan pada download
6	Download	Operational file	Perubahan pada operational file
7	Operational file lama	Operational file baru	Perubahan pada operational file baru
8	Operational file	Uninstall	Perubahan pada uninstall

2.5. Analyze

Proses penyimpanan menghasilkan *image* dari data asli. *Image* ini akan digunakan untuk melakukan analisis. Penelitian ini menggunakan aplikasi Box yang diinstal pada Oppo dan Samsung smartphone, informasi yang diambil dari smartphone Android

adalah proses *install*, *signup*, *upload*, *download*, *logout*, *login*, operasi data file *(new files/new folder/rename/move/copy/share/delete)* dan *uninstall* aplikasi Box.

Tahap ini menjelaskan terhadap metode yang disarankan kepada peneliti atau investigator forensik dalam melakukan investigasi. Dengan membandingkan direktori dan basis data (database) dari satu aktivitas pengguna ke aktivitas sebelumnya, artefak dapat diidentifikasi. Pada Tabel 1 diatas terdapat perbandingan antara data yang diperoleh sebelum dan sesudah. Perubahan metadata dari file-file tersebut akan digunakan kembali dalam proses analisis yang lebih dalam.

2.6. Presentation

Tahapan selanjutnya adalah menghasilkan laporan yang benar dan dapat diterima berdasarkan hasil analisis yang diperoleh pada tahap sebelumnya untuk diberikan kepada pihak berwenang.

3. ANALISIS FORENSIK ANDROID

Pada tahapan ini, direktori dan database yang dibuat pada setiap aktivitas pengguna dibandingkan. Metode ini diharapkan dapat menemukan artefak yang terkait dengan kondisi tersebut berdasarkan hasil akuisisi. Analisis berikut menunjukkan artefak yang dibuat selama setiap aktivitas pengguna.

3.1. Analisis Data *Install*

Ketika aktivitas instalasi Box telah dilakukan, beberapa file baru dibuat. Salah satu yang perlu dipertimbangkan dari yang lain adalah file dengan direktori "data/app/com.box.android-1.apk". File ini adalah file .apk dari Box yang secara otomatis disimpan ketika instalasi dilakukan. Sebagaimana terlampir Tabel 2 di bawah ini, ada delapan file yang dibuat setelah penyimpanan *cloud* aplikasi Box telah diinstal. Karena itu, ketika delapan file tersebut ditemukan di smartphone selama proses investigasi, maka pengguna telah melakukan instalasi aplikasi Box pada smartphone.

Tabel 2. Rincian aktivitas installation pada Box

No	Direktori
1	data/dalvik-cache/data@app@com.box.android-1.apk@classes.dex
2	data/app/com.box.android-1.apk
3	data/app-lib/com.box.android-1/librdpdf.so
4	data/app-lib/com.box.android-1/libleveldb.so
5	data/data/com.box.android/files/gaClientId
6	data/data/com.box.android/shared_prefs/GLOBAL.xml
7	data/data/com.box.android/shared_prefs/device.xml
8	data/data/com.box.android/cache/com.android.opengl.shaders_cache

3.2. Analisis Data *Signup*

Ketika kegiatan signup dilakukan, file yang membutuhkan perhatian khusus adalah direktori "data/data/com.box.android/app_webview/". Namun, direktori ini juga muncul di aktifitas lain. Tidak ada informasi yang dapat diperoleh dari file lain di /app_webview/, jadi itu tidak bisa menjadi referensi untuk aktivitas signup. Dengan menggunakan ADB informasi signup dapat diperoleh. Hasil yang diperoleh dari log live forensik, menunjukkan pada thread "WebViewCallback:" dengan deskripsi di dalamnya sebagai "box show signup = true". Ini adalah bukti digital bahwa pengguna telah melakukan signup.

Tabel 3. Rincian log untuk aktivitas signup

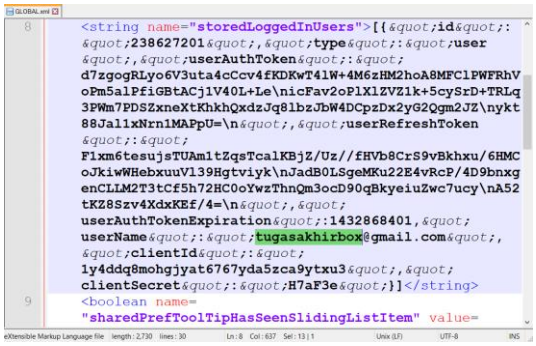
Logcat timestamp
01-29 16:41:01.589 6539 6539 D WebViewCallback:onLoadResource=https://app.box.com/api/oauth2/ authorize?response type=code&client id=1y4ddq8mohgjyat6767yda5zca9ytxu3&state=157ffdcee5cbc81a7f902a6bc035fa9014a68ff8ff66797351cef9ed9d5c5833&box show signup=true

Tabel 4. File termodifikasi pada proses login

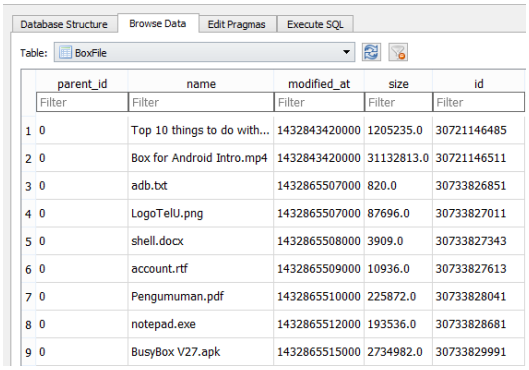
No	Direktori	Modifikasi
1	data/data/com.box.android/app_webview/Cache/the-real-index	Binary files /home/slave2/Downloads/TA/tmp/box/drsignup-all/the-real-index
2	data/data/com.box.android/app_webview/Cookies-journal	Binary files /home/slave2/Downloads/TA/tmp/box/drsignup-all/Cookies-journal
3	data/data/com.box.android/app_webview/Cookies	Binary files /home/slave2/Downloads/TA/tmp/box/drsignup-all/Cookies
4	data/data/com.box.android/shared_prefs/GLOBAL.xml	> <string name=shared_pref_key_remembered_user_name></string> <string name=storedLoggedInUsers>[]</string>stringname=storedLoggedInUsers>|<stringname=storedLoggedInUsers>[{"id":"238627201","type":"user","userAuthToken":"d7zgogRLyo6V3uta4cCcv4fKDKwT4lW+4M6zHM2hoA8MFClPWFRhVoPm5alPfiGBtACj1V40L+LeicFav2oPlXlZVZ1k+5cySrD+TRLq3PWm7PDSZxneXtKhkhQxdzJq8lbzJbW4DCpzDx2yG2Qgm2JZykt88Jal1xNrn1MAPpU=

3.3. Analisis Data *Login*

Ketika aktivitas login dilakukan, file dengan direktori "data/data/com.box.android/shared_prefs/GLOBAL.xml" ditampilkan (seperti ditunjukkan pada Gambar 2) informasi seperti nama pengguna yang digunakan oleh pengguna untuk login ke aplikasi Box. Ketika aktivitas login ke aplikasi Box dilakukan, terlihat ada empat file yang dimodifikasi. Seperti yang ditunjukkan pada tabel 4 di bawah ini, yang terpenting adalah direktori keempat yaitu /data/data/com.box.android/shared_prefs/GLOBAL.xml.



Gambar 2. File XML dari aktivitas login



Database Structure | Browse Data | Edit Pragmas | Execute SQL

Table: BoxFile

	parent_id	name	modified_at	size	id
	Filter	Filter	Filter	Filter	Filter
1	0	Top 10 things to do with...	1432843420000	1205235.0	30721146485
2	0	Box for Android Intro.mp4	1432843420000	31132813.0	30721146511
3	0	adb.txt	1432865507000	820.0	30733826851
4	0	LogoTelU.png	1432865507000	87696.0	30733827011
5	0	shell.docx	1432865508000	3909.0	30733827343
6	0	account.rtf	1432865509000	10936.0	30733827613
7	0	Pengumuman.pdf	1432865510000	225872.0	30733828041
8	0	notepad.exe	1432865512000	193536.0	30733828681
9	0	BusyBox V27.apk	1432865515000	2734982.0	30733829991

Gambar 3. File basis data dari aktivitas upload

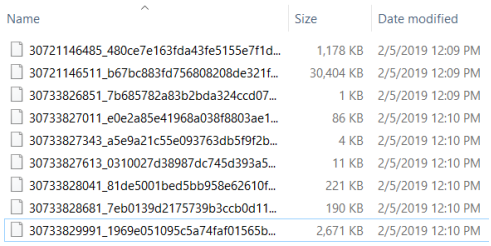
3.4. Analisis Data *Upload*

Setelah selesainya aktivitas upload yang dilakukan pengguna, file database dengan direktori "data/data/com.box.android/database/BoxSQLiteDB_ID" telah dimodifikasi dengan menambahkan beberapa nama file yang terkait dengan file yang di-upload di tabel Boxfile. Bagian yang dimodifikasi dalam database itu menggunakan format waktu UNIX seperti yang ditunjukkan pada Gambar 3. Untuk mendapatkan waktu kejadiannya dapat dilakukan dengan mengubahnya ke format yang umum yaitu *Greenwich Mean Time (GMT)*. Ketika file-file itu dibuka menggunakan SQLlite, file tersebut dapat dilihat dengan jelas apabila file telah di-upload oleh pengguna. Dari informasi ini, peneliti dapat mengidentifikasi nama file, waktu modifikasi, ukuran, dan fileID.

3.5. Analisis Data *Download*

Ketika aktivitas download dilakukan, beberapa file baru dibuat dalam direktori "mnt/shell /emulated/0/Android/data/com.box.android/ID/cache /dl_cache/". File-file ini adalah file yang telah di-download sebelumnya, tetapi telah dienkripsi oleh Box. Sebagai contoh setelah proses upload selesai, proses download dilakukan dengan mengunduh beberapa file tersebut. Sembilan dari banyak file yang terkait dengan aktivitas download telah ditunjukkan pada gambar 4. Dengan analisis yang lebih dalam, dua cara yang mungkin untuk mendapatkan nama file yang di-download ditemukan dalam bentuk teks biasa (tidak terenkripsi).

Cara pertama adalah menggunakan nama file di folder "dl cache". Setiap nama file memiliki struktur <file_id>_<encrypted_file_name>. File_id bisa cocok dengan kolom file_id dalam tabel BoxFile. Cara kedua adalah membuka database BoxSQLiteDB_238627201 menggunakan Hex Editor untuk memperkuat analisis pada langkah unduhan ini. Selain SQLite, Hex Editor digunakan untuk memperkuat analisis pada langkah unduhan ini. Dalam direktori \data\data\com.box.android\ database\BoxSQLiteDB_238627201 informasi tambahan ditemukan untuk artefak aktivitas download. Seperti sebelumnya dari proses pengunduhan dapat diperoleh dengan mengonversi format waktu UNIX menjadi data yang dapat dibaca manusia (atau GMT).

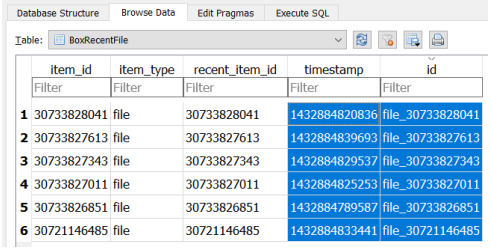


Name	Size	Date modified
30721146485_480ce7e163fda43fe5155e7f1d...	1,178 KB	2/5/2019 12:09 PM
30721146511_b67bc883fd756808208de321f...	30,404 KB	2/5/2019 12:09 PM
30733826851_7b685782a83b2bda324ccd07...	1 KB	2/5/2019 12:09 PM
30733827011_e0e2a85e41968a038f8803ae1...	86 KB	2/5/2019 12:10 PM
30733827343_a5e9a21c55e093763db5f9f2b...	4 KB	2/5/2019 12:10 PM
30733827613_0310027d38987dc745d393a5...	11 KB	2/5/2019 12:10 PM
30733828041_81de5001bed5bb958e62610f...	221 KB	2/5/2019 12:10 PM
30733828681_7eb0139d2175739b3ccb0d11...	190 KB	2/5/2019 12:10 PM
30733829991_1969e051095c5a74faf01565b...	2,671 KB	2/5/2019 12:10 PM

Gambar 4. File basis data dari aktivitas download

3.6. Analisis Operasi *Open file*

Setelah aktivitas open file atau membuka berkas dilakukan, terbentuk berkas pada direktori "data/data/com.box.android/files/previews". Berkas-berkas tersebut memperlihatkan dari berkas yang telah dibuka secara langsung pada aplikasi Box. Berkas dalam format teks seperti .rtf, .docx dan lainnya akan diubah ke dalam bentuk .pdf sebelum berkas tersebut dapat ditampilkan. Terkait direktori "data/data/com.box.android/files/ previews", berkas ini juga ada di direktori "data/media/0/Android/data/com.box.android/ID/cache/previews" dan direktori "shell/emulated/0/Android/data/com.box.android/ID/cache/previews/". Tabel 5 menunjukkan berkas-berkas yang telah didapatkan dan dianalisis terkait aktivitas membuka berkas. Analisis yang lebih dalam mengenai aktivitas open file juga bisa didapatkan dengan membuka basis data BoxSQLiteDB_238627201 seperti yang ditunjukkan pada tabel 5. Format waktu UNIX dari berkas-berkas yang dibuka disimpan di tabel BoxRecentFile kolom timestamp. Berkas yang baru saja dibuka ditempatkan di bagian bawah tabel.



Database Structure | Browse Data | Edit Pragmas | Execute SQL

Table: BoxRecentFile

	item_id	item_type	recent_item_id	timestamp	id
	Filter	Filter	Filter	Filter	Filter
1	30733828041	file	30733828041	1432884820836	file_30733828041
2	30733827613	file	30733827613	1432884839693	file_30733827613
3	30733827343	file	30733827343	1432884829537	file_30733827343
4	30733827011	file	30733827011	1432884825253	file_30733827011
5	30733826851	file	30733826851	1432884789587	file_30733826851
6	30721146485	file	30721146485	1432884833441	file_30721146485

Gambar 5. File basis data dari aktivitas open file

3.7. Analisis Operasi *New folder*

Pada analisis ini, dilakukan aktivitas membuat new folder dengan nama TA1 dan TA2. Pada saat aktivitas ini terjadi, basis data "data/data/com.box.android/databases/BoxSQLiteDB_ID" diperbaharui dan ditambahkan data mengenai folder yang baru saja dibuat pada tabel BoxFolder seperti yang tertera pada Gambar 6. Metode ini dimaksudkan untuk membantu dalam mencari folder baru yang telah dibuat oleh pengguna. Posisi berkas yang baru pada basis data Box biasanya berada di bagian bawah atau diakhir dari direktori data/data/com.box.android/databases/BoxSQLiteDB_ID.

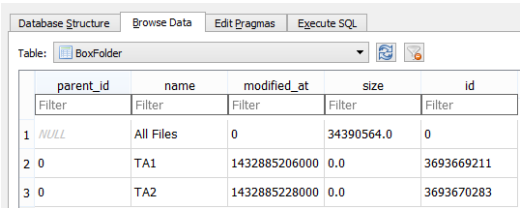


Table: BoxFolder

	parent_id	name	modified_at	size	id
1	NULL	All Files	0	34390564.0	0
2	0	TA1	1432885206000	0.0	3693669211
3	0	TA2	1432885228000	0.0	3693670283

Gambar 6. File basis data dari aktivitas new folder

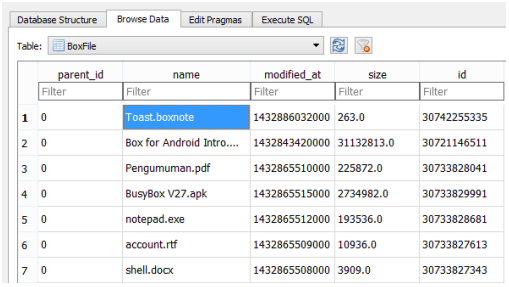


Table: BoxFile

	parent_id	name	modified_at	size	id
1	0	Toast.boxnote	1432886032000	263.0	30742255335
2	0	Box for Android Intro....	1432843420000	31132813.0	30721146511
3	0	Pengumuman.pdf	1432865510000	225872.0	30733828041
4	0	BusyBox V27.apk	1432865515000	2734982.0	30733829991
5	0	notepad.exe	1432865512000	193536.0	30733828681
6	0	account.rtf	1432865509000	10936.0	30733827613
7	0	shell.docx	1432865508000	3909.0	30733827343

Gambar 7. File basis data dari aktivitas new file

3.8. Analisis Operasi *New file*

Berkas baru (new file) yang dibuat langsung di aplikasi Box memiliki ekstensi *.boxnote*. Pada saat dilakukan aktivitas membuat berkas baru, basis data "data/data/com.box.android/databases/BoxSQLiteDB_ID" diperbaharui dengan data tambahan mengenai berkas yang baru saja dibuat pada tabel BoxFile seperti yang ada di Gambar 7.

3.9. Analisis Operasi *Move*

Performansi dari aktivitas memindahkan data (move), kolom parent_id pada table BoxFile dalam basis data "data/data/com.box.android/databases/BoxSQLiteDB_ID" akan diperbaharui berdasarkan folder id tempat berkas tersebut berada. Sebagai contoh dari aktivitas memindahkan data, sebuah berkas dipindahkan ke dalam dua folder yang berbeda. Misalnya, posisi berkas sebelumnya adalah /TA1/toast.boxnote dan akan dipindahkan ke dalam folder /TA2/. Selanjutnya, informasi yang ada pada basis data BoxSQLiteDB akan ikut berubah sesuai dengan ID parent yang baru seperti tertera pada Gambar 8.

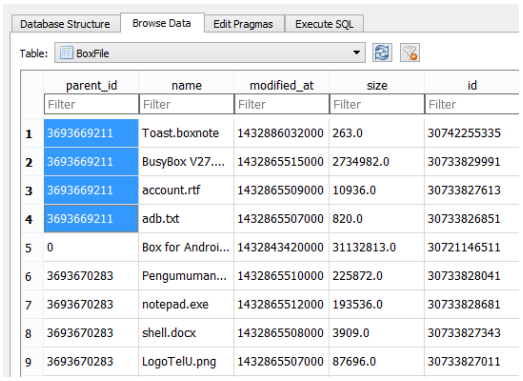


Table: BoxFile

	parent_id	name	modified_at	size	id
1	3693669211	Toast.boxnote	1432886032000	263.0	30742255335
2	3693669211	BusyBox V27....	1432865515000	2734982.0	30733829991
3	3693669211	account.rtf	1432865509000	10936.0	30733827613
4	3693669211	adb.txt	1432865507000	820.0	30733826851
5	0	Box for Androi...	1432843420000	31132813.0	30721146511
6	3693670283	Pengumuman...	1432865510000	225872.0	30733828041
7	3693670283	notepad.exe	1432865512000	193536.0	30733828681
8	3693670283	shell.docx	1432865508000	3909.0	30733827343
9	3693670283	LogoTelU.png	1432865507000	87696.0	30733827011

Gambar 8. File basis data dari aktivitas move

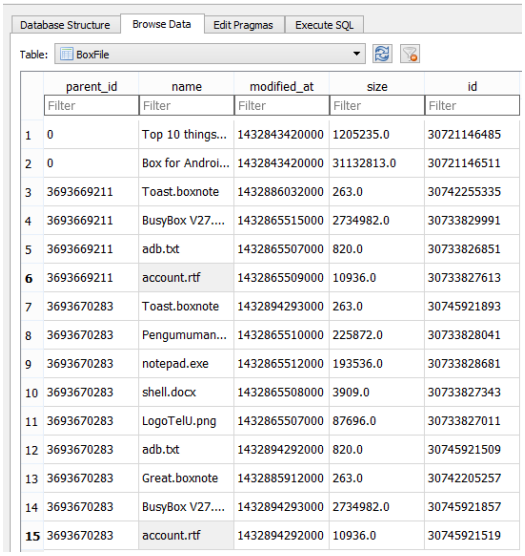


Table: BoxFile

	parent_id	name	modified_at	size	id
1	0	Top 10 things...	1432843420000	1205235.0	30721146485
2	0	Box for Androi...	1432843420000	31132813.0	30721146511
3	3693669211	Toast.boxnote	1432886032000	263.0	30742255335
4	3693669211	BusyBox V27....	1432865515000	2734982.0	30733829991
5	3693669211	adb.txt	1432865507000	820.0	30733826851
6	3693669211	account.rtf	1432865509000	10936.0	30733827613
7	3693670283	Toast.boxnote	1432894293000	263.0	30745921893
8	3693670283	Pengumuman...	1432865510000	225872.0	30733828041
9	3693670283	notepad.exe	1432865512000	193536.0	30733828681
10	3693670283	shell.docx	1432865508000	3909.0	30733827343
11	3693670283	LogoTelU.png	1432865507000	87696.0	30733827011
12	3693670283	adb.txt	1432894292000	820.0	30745921509
13	3693670283	Great.boxnote	1432885912000	263.0	30742205257
14	3693670283	BusyBox V27....	1432894293000	2734982.0	30745921857
15	3693670283	account.rtf	1432894292000	10936.0	30745921519

Gambar 9. File basis data dari aktivitas copy

3.10. Analisis Operasi *Copy*

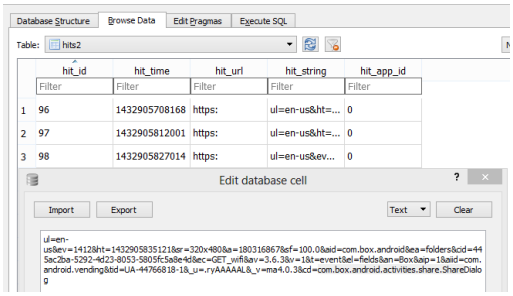
Pada saat aktivitas menggandakan berkas (copy) dilakukan, table BoxFile pada basis data "data/data/com.box.android/databases/BoxSQLiteDB_ID" juga diperbaharui dan ditambahkan data mengenai berkas yang telah digandakan. Jika hanya aktivitas copy yang dilakukan, maka parentID dan fileID akan berbeda tetapi ukuran besar berkas tetap sama seperti yang ditunjukkan di Gambar 9.

3.11. Analisis Operasi *Rename*

Ketika aktivitas mengubah nama (rename) dilakukan, beberapa kolom pada table BoxFile di basis data "data/data/com.box.android/databases/BoxSQLiteDB_ID" akan berubah sesuai degan perubahan-perubahan yang dilakukan. Sebagai contoh aktivitas yang dilakukan di skenario forensik Android ini adalah mengubah nama berkas dari shell.docx menjadi shiny.docx tetapi berkas tersebut tetap disimpan di folder yang sama.

3.12. Analisis Operasi *Share*

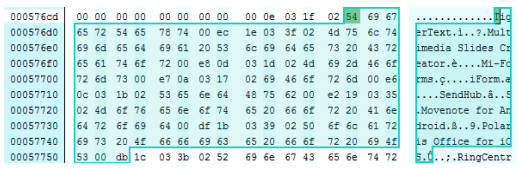
Pada saat dilakukan aktivitas membagikan berkas (share), maka tabel hits2 pada basis data "data/data/com.box.android/databases/google_analytics_v4.db" juga diperbaharui dengan "informasi data yang muncul" seperti yang digambarkan pada Gambar 10. Contoh dari aktivitas share adalah memberikan tautan dari berkas yang akan dibagikan. Disisi lain atau pengguna kedua yang diberikan akses, tautan tersebut diakses. Perubahan-perubahan akan terjadi pada basis data di tabel Box yang berada disisi pengguna yang memberikan akses. Maka dapat diperkirakan bahwa informasi mengenai siapa saja yang telah dibagikan akses ke berkas ini dapat diketahui dengan cepat pada proses investigasi.



Gambar 10. File basis data dari aktivitas share

3.13. Analisis Operasi *Delete*

Beberapa kolom di table BoxFile pada basis data "data/data/com.box.android/databases/BoxSQLiteDB_ID" berubah sesuai perubahan yang dibuat pada saat dilakukan aktivitas menghapus berkas (delete). Data dari berkas yang dihapus juga akan dihapus dari basis data. Sebagai contoh dari aktivitas delete, sebuah berkas akan dihapus dari direktori tertentu. Kemudian, informasi pada tabel basis data Box juga akan diubah menjadi NULL.



Gambar 11. File basis data dari aktivitas delete

Tabel 6 di bawah ini menunjukkan hasil catatan langsung selama proses penghapusan berkas. Salah satu persyaratan untuk *Android Live Log* adalah smartphone yang diambil dari tempat kejadian perkara tidak boleh dimatikan. Selain itu, masih ada metode lain yang bisa dilakukan yaitu dengan menggunakan Hex Editor untuk membuka basis data BoxSQLiteDB_ID. Berkas yang telah dihapus ditunjukkan sebagai sampah (trash) seperti pada Gambar 11. Jika pengguna tidak melakukan penghapusan secara permanen, berkas tersebut masih bisa ditemukan dan dikembalikan (hanya pada versi web) untuk digunakan sebagai bukti digital.

Tabel 6. Rincian log untuk aktivitas delete

Logcat timestamp
05-29 11:11:34.929 1235 1246 D SystemAdController:Activity:ActivityInfo{427b1bd0com.box.android.activities.DeleteItemsActivity}is not the default one
05-29 11:11:34.930 738 1208 I ActivityManager: STARTu0{cmp=com.box.android/.activities.DeleteItems Activity (has extras)} from pid 27319
05-29 11:11:35.144 27319 27319 D ActivityThread: ACT-LAUNCH_ACTIVITY handled : 0 / ActivityRecord{427aaac8token=android.os.BinderProxy@431f06f8{com.box.android/com.box.android.activities.DeleteItemsActivity}}
05-29 11:11:35.211 738 756 I ActivityManager: [AppLaunch] Displayed Displayed com.box.android/.activities.DeleteItemsActivity: +263ms
05-29 11:11:35.212 738 756 D ActivityManager: AP_PROF:AppLaunch_LaunchTime:com.box.android/.activities.DeleteItemsActivity:263:6976134

Tabel 7. Rincian log untuk aktivitas logout

Logcat timestamp
01-26 16:28:35.196 23449 23699 I TableUtils: clearing table 'BoxFile' with 'DELETE FROM `BoxFile``
01-26 16:28:35.312 23449 23699 I TableUtils: clearing table 'BoxFolder' with 'DELETE FROM `BoxFolder``
01-26 16:28:35.334 23449 23699 I TableUtils: clearing table 'BoxComment' with 'DELETE FROM `BoxComment``
01-26 16:28:35.350 23449 23699 I TableUtils: clearing table 'BoxCollaboration' with 'DELETE FROM `BoxCollaboration``
01-26 16:28:35.367 23449 23699 I TableUtils: clearing table 'BoxUser' with 'DELETE FROM `BoxUser``
01-26 16:28:35.378 23449 23699 I TableUtils: clearing table 'BoxWebLink' with 'DELETE FROM `BoxWebLink``
01-26 16:28:35.399 23449 23699 I TableUtils: clearing table 'BoxRecentFile' with 'DELETE FROM `BoxRecentFile``
01-26 16:28:35.413 23449 23699 I TableUtils: clearing table 'BoxEvent' with 'DELETE FROM `BoxEvent``
01-26 16:28:35.431 23449 23699 I TableUtils: clearing table 'BoxOneCloudApp' with 'DELETE FROM `BoxOneCloudApp``
01-26 16:28:35.450 23449 23699 I TableUtils: clearing table 'BoxOneCloudAppCategory' with 'DELETE FROM `BoxOneCloudAppCategory``
01-26 16:28:35.466 23449 23699 I TableUtils: clearing table 'BoxOneCloudAppAction' with 'DELETE FROM `BoxOneCloudAppAction``
01-26 16:28:35.520 23449 23699 I TableUtils: clearing table 'BoxCollection' with 'DELETE FROM `BoxCollection``
01-26 16:28:35.534 23449 23699 I TableUtils: clearing table 'BoxCollectionItem' with 'DELETE FROM `BoxCollectionItem``

3.14. Analisis Data *Logout*

Pada saat dilakukan aktivitas logout (keluar), beberapa kolom pada tabel BoxFile di basis data "data/data/com.box.android/databases/BoxSQLiteDB_ID" akan dikosongkan. Sama seperti proses login (masuk), berkas dengan direktori data/data/com.box.android/shared_prefs/GLOBAL.xml dapat digunakan sebagai referensi dalam menentukan apakah pengguna sudah logout atau belum. Jika konten pada tabel basis data telah terhapus, maka berarti pengguna sudah keluar (logout).

Artefak tidak bisa ditemukan dengan mudah dalam proses investigasi. Salah satu pendekatan yang

bisa dilakukan untuk kasus seperti ini yaitu dengan menggunakan *Live Log Forensics* atau forensik secara langsung, dimana smartphone harus selalu tetap dinyalakan. Jika artefak dari aktivitas logout tidak bisa ditemukan, artefak tersebut bisa ditelusuri dari cache memori smartphone. Pada kasus ini, dilakukan pembacaan catatan aktivitas pada smartphone dengan menggunakan ADB seperti pada tabel 7. Dari data catatan tersebut, rangkaian *clearing table* didapatkan dari tiga belas tabel yaitu: *BoxFile*, *BoxFolder*, *BoxComment*, *BoxUser*, *BoxCollabaration*, *BoxWebLink*, *BoxOneCloudApp*, *BoxOneCloudAppAction*, *BoxEvent*, *BoxCollection*, dan *BoxCollectionItem.*

Tabel 8. Rincian aktivitas uninstall pada Box

No	Direktori
1	data/media/0/.boxinstall/abthreshold
2	data/media/0/.boxinstall/abpercentile
3	data/media/0/.box/install
4	mnt/shell/emulated/0/.boxinstall/abthreshold
5	mnt/shell/emulated/0/.boxinstall/abpercentile
6	mnt/shell/emulated/0/.box/install

Tabel 9. Rincian log untuk aktivitas uninstall

Logcat timestamp
01-27 16:31:07.818 1519 23963 D VoicemailCleanupService: Cleaning up data for package: com.box.android
01-27 16:31:10.688 12464 24009 D AccountUtils: Clearing selected account for com.box.android
01-27 16:31:10.761 23931 23931 I UninstallAppProgress: Finished uninstalling pkg: com.box.android

3.15. Analisis Data *Uninstall*

Jika aplikasi Box telah dihapus atau uninstall, data yang tersisa berkaitan dengan Box terdapat pada direktori "data/media/0/.boxinstall/". Langkah ini diharapkan dapat membantu dalam membuktikan bahwa pengguna (dalam hal ini yang merupakan tersangka) pernah melakukan install dan/atau uninstall aplikasi Box. Tabel dibawah ini merupakan berkas yang tersisa setelah proses uninstall. Jumlah berkas tersebut tidak dapat ditentukan secara pasti. Jumlahnya bisa berbeda untuk masing-masing akun, tetapi tidak akan berbeda jauh dari enam berkas pada Tabel 8 berikut ini. Kondisi ini sama dengan logout. Untuk melengkapi analisis ke lima belas ini, diperlukan forensik catatan aktivitas smartphone secara langsung (live activity phone log forensics). Forensik Android secara langsung memang cukup sulit karena diperlukan perlakuan khusus yaitu smartphone harus selalu dinyalakan. Hampir seluruh aktivitas yang telah dilakukan tercatat pada Logcat (versi Android). Dengan menggunakan ADB, catatan yang ada pada smartphone dapat dibaca dan diambil. Aktivitas uninstall terlihat dengan jelas pada logcat beserta waktu kejadiannya dengan tiga rangkaian berikut: *cleaning up the data for the package, clearing account forcom.box.android01-26 selected*, dan *finished uninstalling pkg*.

4. DISKUSI

Kesimpulan dapat ditarik dari tiga belas tahap analisis, sedangkan kesimpulan untuk dua analisis lainnya dianggap masih meragukan. Tiga belas tahap analisis tersebut ialah install, signup, login, upload, download, dan operasi berkas (open/new folder/new file/move/copy/rename/share/delete). Dua analisis lainnya ialah logout dan uninstall dimana metadata pada basis data yang ada tidak dapat ditemukan sama sekali. Metode alternatif untuk menemukan timestamp dan rangkaian aktivitas dari proses logout dan uninstall, termasuk juga kejadian apapun yang memungkinkan pada smartphone, adalah dengan melakukan log live forensic atau forensik catatan langsung.

Untuk menguji kebenaran dari artefak yang telah didapatkan, perlu dilakukan pengecekan terhadap aktivitas sebenarnya yang dilakukan oleh pengguna. Pengujian dilakukan dengan melakukan otentikasi terbalik terhadap hasil yang didapat. Proses pengujian ini dilakukan dengan menggunakan dua smartphone yang berbeda dengan satu responden individu untuk masing-masing smartphone.

Pada tahap diskusi presentation ini, dilakukan pelaporan dari hasil analisis yang telah didapatkan selama proses forensik Android. Hasil analisis tersebut ditunjukkan oleh Tabel 10. Tabel ini memberikan informasi dari 15 skenario yang telah didapatkan dan disimpulkan berdasarkan hasil uji pada kedua smartphone yang berbeda sistem operasi Android dan begitupun juga vendornya.

5. KESIMPULAN DAN SARAN

Investigasi pada aplikasi penyimpanan cloud Box memang cukup kompleks, tetapi dapat disederhanakan dibuktikan dengan investigasi forensik bergerak yang dilakukan dari sisi pengguna pada smartphone berbasis Android. Dari berbagai tahap forensik Android yang telah dilakukan, dibentuk sebuah rekomendasi sebagai panduan bagi investigator dalam melakukan pengujian pada penyimpanan awan Box. Metode perbandingan dan analisis yang diajukan dapat membantu proses investigasi untuk menemukan artefak yang bisa digunakan sebagai bukti digital. Setelah melakukan analisis dan pengujian pada dua smartphone yang berbeda, artefak yang ditemukan sama, dapat diterima dan diperhitungkan secara legal.

Penelitian selanjutnya masih diperlukan untuk berkas terenkripsi yang lebih condong ke area ilmu kriptografi dan juga untuk kasus-kasus dimana data sudah terhapus secara level memori internal. Adapun kasus lain dimana investigator mendapatkan smartphone dalam keadaan mati atau kondisi yang tidak layak, dengan kata lain adalah bagaimana proses memulihkan smartphone Android tersebut baik sistem operasinya ataupun datanya.

Tabel 10. Analisis hasil pengujian pada aplikasi Box

No	Aktivitas	Direktori	Informasi
1	Install	data/app/com.box.android-1.apk	-
2	Sign up	data/data/com.box.android/app_webview/	Informasi tanggal dan waktu menggunakan adb logcat
3	Login	data/data/com.box.android/ shared_prefs/GLOBAL.xml	Username yang digunakan saat login
4	Upload	data/data/com.box.android/databases/ BoxSQLiteDB_ID	Beberapa daftar file yang pernah diupload berikut dengan informasi waktunya
5	Download	mnt/shell/emulated/0/Android/data/ com.box.android/ID/cache/dl_cache/	Beberapa daftar file yang pernah didownload berikut dengan informasi waktunya
6	Open File	data/data/com.box.android/files/previews	Beberapa daftar file yang pernah dibuka berikut dengan informasi file extension
7	New Folder	data/data/com.box.android/databases/ BoxSQLiteDB_ID	Nama folder yang pernah dibuat berikut dengan informasi waktunya beserta sizenya
8	New File	data/data/com.box.android/databases/ BoxSQLiteDB_ID	Nama file yang pernah dibuat berikut dengan informasi waktunya beserta sizenya
9	Move	data/data/com.box.android/databases/ BoxSQLiteDB_ID	Nama file yang pernah dipindahkan berikut dengan informasi waktunya modifikasinya
10	Copy	data/data/com.box.android/databases/ BoxSQLiteDB_ID	Nama file yang pernah digandakan berikut dengan informasi waktunya modifikasinya beserta parentID yang baru
11	Rename	data/data/com.box.android/databases/ BoxSQLiteDB_ID	Nama file yang pernah digantikan namanya berikut dengan informasi waktunya modifikasinya
12	Share	data/data/com.box.android/databases/ google_analytics_v4.db	Nama file yang pernah dibagikan namanya berikut dengan informasi waktunya dan link yang akan dibagikan
13	Delete	data/data/com.box.android/databases/ BoxSQLiteDB_ID	Nama file yang pernah dihapus berikut dengan informasi waktunya dilakukannya
14	Logout	data/data/com.box.android/databases/ BoxSQLiteDB_ID	Informasi tanggal dan waktu menggunakan adb logcat
15	Uninstall	data/media/0/.boxinstall/	Informasi tanggal dan waktu menggunakan adb logcat

DAFTAR PUSTAKA

AKTER, M., GANI, A., RAHMAN, M. O., HASSAN, M. M., ALMOGREN, A. & AHMAD, S., 2018, Performance analysis of personal cloud storage services for mobile multimedia health record management, IEEE Access 6, 52625-52638.

BOCCHI, E., DRAGO, I. & MELLIA, M., 2017, Personal cloud storage benchmarks and comparison, IEEE Transactions on Cloud Computing 5(4), 751-764.

Box, 2019, Application [online], Tersedia di <https://app.box.com/apps> [Diakses 7 Juli 2019].

CHEN, L., TAKABI, H. & LE-KHAC, N.-A., 2019, Security, Privacy, and Digital Forensics in the Cloud, John Wiley & Sons.

DARYABAR, F., DEHGHANTANHA, A., ETEROVIC-SORIC, B. & CHOO, K.-K. R., 2016, Forensic investigation of onedrive, box, googledrive and dropbox applications on android and ios devices, Australian Journal of Forensic Sciences 48(6), 615-642.

DO, Q., MARTINI, B. & CHOO, K. R., 2015, A cloud-focused mobile forensics methodology, IEEE Cloud Computing 2(4), 60-65.

HOLT, T. J., BOSSLER, A. M. & SEIGFRIED-SPELLAR, K. C., 2017, Cybercrime and digital forensics: An introduction, Routledge.

HOSSAIN, A. R. M. R., ISLAM, G. I., SHAHINURZZAMAN, M. & HOSSAIN, M. A., 2016, In the cloud storage market how users are using it without hesitation (report 2016), International Journal of Computer (IJC) 21(1), 30-34.

MAN, Y., GAO, C., LYU, M. R. & JIANG, J., 2016, Experience report: Understanding cross-platform app issues from user reviews, in 2016 IEEE 27th International Symposium on Software Reliability Engineering (ISSRE), pp. 138-149.

MARAS, M.-H., 2015, Computer forensics, Jones and Bartlett Learning.

MCKEMMISH, R., 2008, When is digital evidence forensically sound?, In IFIP international conference on digital forensics, pp. 3-15. Springer.

PICHAN, A., LAZARESCU, M. & SOH, S. T., 2015, Cloud forensics: Technical challenges, solutions and comparative analysis, Digital investigation 13, 38-57.

SATRYA, G. B., NASRULLAH, A. A. & SHIN, S. Y., 2017, 'Identifying artefact on microsoft

onedrive client to support android forensics, International Journal of Electronic Security and Digital Forensics 9(3), 269-291.

SATRYA, G. B. & SHIN, S. Y., 2018, Proposed method for mobile forensics investigation analysis of remnant data on google drive client, Journal of Internet Technology 19(6), 1741-1751.

VALJAREVIC, A. & VENTER, H. S., 2016, Introduction of concurrent processes into the digital forensic investigation process, Australian Journal of Forensic Sciences 48(3), 339-357.