CyberSecurity dan Forensik Digital e-ISSN: 2615-8442
Vol. 3, No. 1, Mei 2020, hlm. 33-38

PENDEKATAN DD SEBAGAI SALAH SATU TEKNIK AKUISISI PERANGKAT ANDROID

Fietyata Yudha[1], Erika Ramadhani[2] , Fayruz Rahma[3] , Waldi Nur Hamzah[4]

[1,2,3,4]Jurusan Informatika, Universitas Islam Indonesia
Email: [1]yudha@uii.ac.id, [2]erika@uii.ac.id, [2]fayruz.rahma@uii.ac.id, [4]13523267@students.uii.ac.id

Abstrak

Teknologi perangkat bergerak berkembang pesat melampaui perkembangan perangkat-perangkat pendahulunya. Meningkatnya penggunaan perangkat bergerak berimplikasi pada perkembangan kejahatan komputer maupun siber. Kejahatan komputer maupun siber bergeser memanfaatkan perangkat bergerak sebagai target ataupun alat bantu melancarkan kejahatan. Meningkatnya kejahatan yang memanfaatkan perangkat bergerak sebagai target maupun alat bantu kejahatan mengharuskan penyidik forensik membuat sebuah model baru dalam proses penyelidikan forensik pada perangkat bergerak. Akuisisi merupakan tahapan forensik yang cukup memiliki perbedaan di antara beberapa perangkat komputer. Pada beberapa aplikasi akuisisi perangkat bergerak yang sudah ada sebelumnya, akuisisi perangkat bergerak disebut dengan istilah ekstraksi. Penelitian ini membahas tentang pendekatan teknik DD pada perangkat bergerak berbasis Android sebagai salah satu teknik dalam melakukan ekstraksi barang bukti yang berbentuk perangkat bergerak. Ekstraksi hanya bisa dilakukan dengan perangkat bergerak dalam kondisi *root* dan juga pada mode *custom recovery*. Berdasarkan eksperimen yang sudah dilakukan, hasil ekstraksi menggunakan teknik DD berhasil melakukan akuisisi seluruh sistem berkas yang ada pada perangkat bergerak berbasis Android yang dijadikan sampel uji dengan persentase ukuran hasil ekstraksi di atas 99% jika dibandingkan dengan ukuran asli penyimpanan perangkat tersebut. Hal ini menunjukkan bahwa hasil dari proses akuisisi dengan metode ini menghasilkan hasil yang hampir identik.

Kata kunci: *Akuisisi, Android, ekstraksi, Forensik Digital*

DD APPROACH AS ONE OF THE ANDROID ACQUISITION TECHNIQUES

Abstract

Mobile device technology is growing up rapidly beyond the development of its predecessor devices. Mobile devices usage is increasing and has implications for the development of computer system and cybercrime. Modern cybercrime has shifted to mobile devices. Mobile devices become targets or tools to launch cybercrime. The increase in cybercrime that uses mobile devices as targets or launches cybercrime is the reason why forensic investigators are required to create a new model in the process of forensic investigations on mobile devices. The acquisition of mobile devices is one of the digital forensics stages that use different technique compared to other types of computer devices. In some pre-existing mobile device acquisition implementation, the term of extraction used to describe the acquisition process. This study discusses the DD approach on Android-based mobile devices as one of the techniques in acquiring evidence in mobile devices. The acquisition can be done with a mobile device in the root condition or custom recovery mode. Based on experiments that have been carried out, the extraction results using DD technique succeeded in acquiring the entire file system on an Android-based mobile device that was used as a test sample. The extraction size is above 99,99 percent compared to the original size of the storage device. This shows that the acquisition process using this method produces almost identical results.

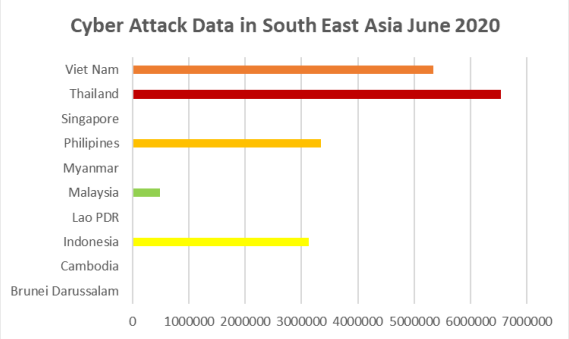
Keywords: *acquisition, Android, digital forensics, extraction*

1. PENDAHULUAN

Evolusi teknologi di dunia semakin memudahkan umat manusia dalam menjalankan kehidupannya. Teknologi semakin berkembang seiring perkembangan kehidupan manusia. Salah satu teknologi yang berkembang cukup pesat adalah teknologi perangkat bergerak. Berbagai jenis penyedia perangkat bergerak tersebar di seluruh dunia dengan berbagai macam fitur yang mereka tawarkan. Perkembangan teknologi perangkat bergerak bahkan telah melampaui perkembangan perangkat komputer personal ataupun komputer jinjing. Data yang dihimpun oleh Muller (2020), 96% populasi penduduk dewasa Indonesia telah memiliki perangkat bergerak pada kuartal ke-3 tahun 2019. Di

sisi lain, Kemp (2020) mengungkapkan bahwa jumlah perangkat bergerak di Indonesia lebih besar jika dibandingkan dengan jumlah populasi masyarakat Indonesia: jumlah perangkat bergerak yang terhubung pada jaringan di wilayah Indonesia adalah 338,2 juta atau sekitar 124% dari total populasi masyarakat Indonesia.

Perkembangan teknologi perangkat bergerak juga diikuti dengan perkembangan sistem operasi yang berjalan pada perangkat bergerak. Dua raksasa sistem operasi perangkat bergerak saat ini tengah menguasai pasaran, yaitu Android dan IOS. Android menguasai lebih dari 93,74% pasar sistem operasi perangkat bergerak Muller (2020b).Perkembangan perangkat bergerak juga diikuti dengan bergesernya tindak kejahatan siber maupun kejahatan berbantukan teknologi siber. Indonesia menempati peringkat keempat sebagai negara dengan jumlah serangan siber terbanyak di Asia Tenggara pada Juni 2020, setelah Filipina, seperti yang ditunjukkan pada Gambar 1 (Akamai, 2020). Kejahatan modern mulai memanfaatkan perangkat bergerak sebagai target maupun alat bantu dalam melancarkan kejahatan. Peningkatan kejahatan siber berbantukan perangkat bergerak sehingga diperlukan metode-metode untuk melakukan proses penyelidikan pada perangkat bergerak.



Gambar 1. Serangan Siber di Asia Tenggara (Akamai, 2020)

Pada proses investigasi forensik digital, tahapan akuisisi pada metodologi forensik digital memegang peranan penting dalam penanganan kasus kejahatan komputer. Kesalahan yang terjadi pada proses akuisisi akan berpengaruh terhadap keseluruhan kasus yang ditangani, bahkan bisa menyebabkan barang bukti tidak bisa digunakan untuk melakukan pembuktian di persidangan. Maka, diperlukan proses penanganan khusus pada tahapan akuisisi ini. Akuisisi pada perangkat bergerak berbeda dengan akuisisi yang dilakukan pada perangkat komputer atau pun penyimpanan komputer. Pada perangkat komputer atau penyimpanan perangkat komputer, proses akuisisi biasa disebut dengan proses *imaging*. Fakta di lapangan menunjukkan beberapa penyedia layanan perangkat akuisisi forensik pada perangkat bergerak menggunakan istilah ekstraksi guna menyebut proses akuisisi pada perangkat bergerak.

Penelitian ini mencoba melakukan teknik dd sebagai salah satu cara dalam melakukan proses akuisisi pada perangkat bergerak berbasis Android untuk mendapatkan keseluruhan media penyimpanan yang terdapat dalam perangkat bergerak tersebut dengan metode *rooting* Android dan Android *custom recovery*. Proses penelitian ini akan menjawab beberapa pertanyaan penting, antara lain: (1) Apakah teknik dd dapat digunakan untuk melakukan akuisisi data pada perangkat bergerak berbasis Android? (2) Metode apa saja yang dapat digunakan untuk melakukan teknik akuisisi dd pada perangkat bergerak berbasis Android? (3) Bagaimana hasil dari proses akuisisi dengan teknik dd yang dilakukan? dan (4) Apakah teknik ini bisa mendapatkan hasil yang identik dengan teknik akuisisi dd pada perangkat komputer biasa. Tujuan dari dilakukanya penelitian ini adalah untuk mengetahui bahwa teknik dd ini dapat digunakan untuk membantu kepentingan analisis dalam proses penyidikan forensik digital pada perangkat berbasis Android. Teknik ini bisa memberikan informasi lebih lengkap dibandingkan dengan informasi yang didapatkan dengan teknik akuisisi lainnya jika dilihat pada studi kasus komputer forensik.

2. PUSTAKA

2.1 Penelitian Sejenis

Penelitian yang dilakukan oleh Srivastava and Tapaswi (2015) memaparkan bahwa data pada media penyimpanan Android baik internal maupun eksternal tidak banyak berubah ketika dilakukan ekstraksi. Penelitian ini berfokus pada bagaimana data diekstraksi menggunakan metode *logical extraction*.

Yusoff et al., (2014) melalui penelitiannya menjelaskan mengenai metode dan teknik akuisisi data pada perangkat berbasis Firefox OS menggunakan kaidah forensika digital. Pada penelitian ini, dijelaskan mengenai tantangan, hambatan dan potensi forensik pada perangkat bergerak berbasis Firefox OS. Dalam penelitian ini juga digunakan metode *physical extraction* menggunakan UNIX dd.

Penelitian tentang akuisisi perangkat memori utama pada perangkat bergerak berbasis Android dilakuken oleh Yang et al. (2017). Penelitian ini dilakukan dengan melihat mulai banyaknya kasus kasus serangan *malware* pada perangkat bergerak. Peneliti mengajukan sebuah metode protokol *firmware update* untuk menggantikan teknik akuisisi memori utama konvensional pada perangkat bergerak berbasis Android yang sulit untuk dilakukan. Park, Jang and Park (2018) melakukan hal yang sama namun dengan perangkat yang berbeda. Mereka mengajukan metode yang sama namun untuk perangkat bergerak keluaran LG.

Sementara itu, Feng et al. (2018) meneliti metode ekstraksi logika pada perangkat bergerak berbasis Android. Metode ini dilakukan karena masifnya perkembangan perangkat bergerak berbasis

Android serta perkembangan pesat sistem operasi perangkat ini. Peneliti beralasan metode konvensional cukup sulit diimplementasikan pada perangkat-perangkat keluaran terbaru.

Berdasarkan penelitian yang sudah dilakukan oleh peneliti sebelumnya, implementasi teknik dd dalam proses akuisisi masih jarang dilakukan. Rata-rata penelitian yang berfokus pada perangkat bergerak berbasis Android menggunakan teknik *logical extraction* pada saat proses akuisisi barang bukti digital. Maka, penelitian yang akan dilakukan ini merupakan penelitian yang masih belum banyak dilaksanakan.

2.2 Forensik Perangkat Bergerak

Secara umum, forensik perangkat bergerak merupakan cabang dari keilmuan forensik digital di mana bidang ini berhubungan dengan proses pencarian barang bukti digital pada perangkat bergerak menggunakan teknik tertentu sesuai dengan kaidah forensik digital. Perangkat bergerak dapat dikatakan sebagai telepon seluler, namun dapat juga merujuk pada perangkat bergerak secara umum yang mempunyai kapabilitas telekomunikasi dan media penyimpanan internal, seperti tablet dan perangkat GPS. Namun, umumnya kata "perangkat bergerak" digunakan untuk merujuk pada telepon genggam. Telepon genggam pada umumnya dapat digunakan untuk menyimpan berbagai jenis informasi pribadi seperti informasi kontak, kalender, foto, catatan dan pesan singkat. Perangkat bergerak berbasis Android memungkinkan untuk menyimpan informasi lebih banyak, seperti video, surel, informasi dari perambah web, informasi lokasi, dan informasi dari aplikasi sosial media dan lain-lain.

Menurut Forte and Donno (2010), prosedur umum dalam forensik perangkat bergerak dibagi menjadi lima tahapan, yaitu:

1. Persiapan penyidikan
2. Penyitaan dan isolasi barang bukti
3. Akuisisi data
   a. Akuisisi manual
   b. Akuisisi *logical*
   c. Akuisisi *filesystem*
   d. Akuisisi *physical*
4. Analisis dan pemeriksaan barang bukti
5. Pelaporan hasil dan dokumentasi barang bukti

Pada perangkat bergerak berbasis Android, diperlukan pendekatan khusus untuk melakukan proses forensik digital. Tetapi pada kenyataannya, saat proses penyidikan forensik digital untuk kasus yang melibatkan perangkat bergerak berbasis Android, belum dimungkinkan untuk menggunakan satu prosedur standar untuk semua kasus(Srivastava and Tapaswi, 2015).

2.1 Struktur Sistem Berkas Android

```
C:\WINDOWS\system32>adb -d shell
shell@virgo:/ $ su
root@virgo:/ # cat /proc/partitions
major minor  #blocks  name

   7        0      98304 loop0
 179        0   15388672 mmcblk0
 179        1       2031 mmcblk0p1
 179        2       1024 mmcblk0p2
 179        3       1024 mmcblk0p3
 179        4       1024 mmcblk0p4
 179        5       1024 mmcblk0p5
 179        6       1024 mmcblk0p6
 179        7       4096 mmcblk0p7
 179        8       5120 mmcblk0p8
 179        9       4096 mmcblk0p9
 179       10       8192 mmcblk0p10
 179       11      36864 mmcblk0p11
 179       12       1536 mmcblk0p12
 179       13       1536 mmcblk0p13
 179       14          1 mmcblk0p14
 179       15      62463 mmcblk0p15
 179       16       1536 mmcblk0p16
 179       17      31232 mmcblk0p17
 179       18      32768 mmcblk0p18
 179       19      32768 mmcblk0p19
 179       20      16384 mmcblk0p20
 179       21      16384 mmcblk0p21
 179       22     131072 mmcblk0p22
 179       23    1572864 mmcblk0p23
 179       24     393216 mmcblk0p24
 179       25   13029359 mmcblk0p25
 179       32       4096 mmcblk0rpmb
root@virgo:/ #
```

Gambar 2 Contoh Hasil Pemetaan Partisi Pada Perangkat Android

Struktur partisi pada perangkat berbasis Android umumnya berbeda-beda di setiap perangkatnya. Penyebab perbedaan ini antara lain tipe perangkat dan versi dari Android yang digunakan. Gambar 2 menunjukkan contoh partisi yang ada pada perangkat berbasis Android.

Menurut Hoog (2011), ada beberapa partisi yang umum ada pada perangkat berbasis Android, antara lain:

1. Bootloader
2. Boot
3. Recovery
4. Userdata
5. System
6. Cache

3. METODOLOGI

Dalam proses penelitian yang dilakukan, dibuat sebuah metode penelitian agar tujuan penelitian dapat tercapai. Kerangka tahapan penelitian dapat dilihat pada Gambar 3.

Studi literatur merupakan tahapan awal pada penelitian ini. Tahap ini bertujuan untuk memastikan bahwa hal yang akan dikerjakan merupakan hal yang relevan untuk dilaksanakan.

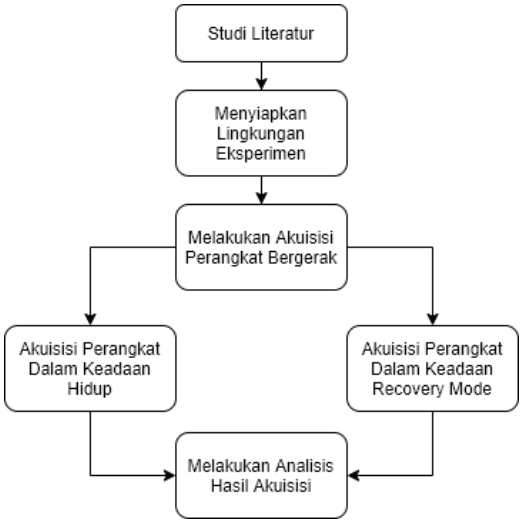
Proses eksperimen dilakukan dengan melakukan akuisisi terhadap sampel perangkat bergerak berbasis Android. Perangkat bergerak tersebut akan diakuisisi dengan menggunakan dua metode, yaitu: metode *rooting* dan metode *custom recovery*. Akuisisi akan dilakukan dengan teknik dd pada sistem operasi Linux.

Setelah proses akuisisi dilakukan, hasil yang didapatkan akan didokumentasikan untuk dilakukan analisis terhadap hasil tersebut. Adapun beberapa parameter yang akan dianalisis antara lain:

1. Jumlah Blok

2. Ukuran Penyimpanan (Byte)
3. Ukuran Hasil (Byte)
4. Persentase hasil
5. Jumlah Partisi Terakuisisi
6. Waktu Akuisisi (detik)
7. Kecepatan Rata-rata Transfer (MB/s)

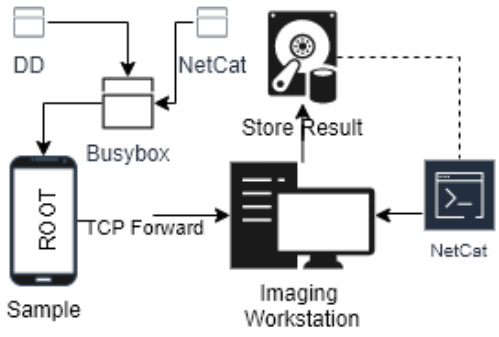
Parameter-parameter tersebut akan dibandingkan hasilnya antara proses akuisisi dengan metode *root* dan juga metode *custom recovery*.



Gambar 3. Metodologi Penelitian

4. PEMBAHASAN

Proses eksperimen dilakukan dengan menguji tiga sampel perangkat bergerak berbasis Android. Proses pertama yang dilakukan adalah persiapan lingkungan untuk melakukan akuisisi. Lingkungan akuisisi yang dimaksud adalah topologi yang akan diimplementasikan ketika melakukan proses akuisisi. Topologi lingkungan akuisisi dapat dilihat pada Gambar 4.



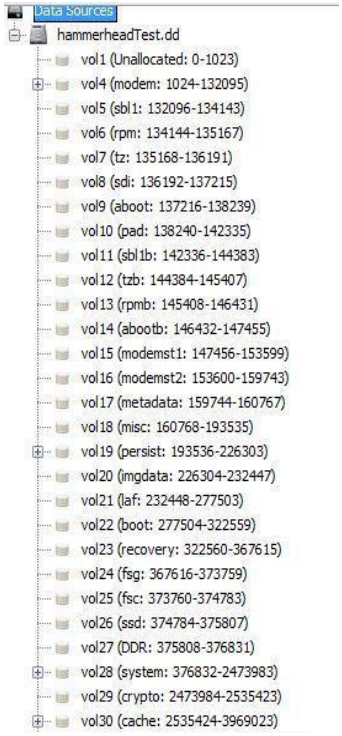
Gambar 4. Diagram Topologi Eksperimen

Sampel akan diakuisisi dengan menggunakan dua metode, yaitu: metode *root* dan metode *custom recovery*. Untuk menjalankan metode *root*, sampel harus sudah melalui proses *rooting* dan juga sudah terpasang *busybox* untuk mengakses beberapa perintah-perintah Linux lanjutan. Sementara itu, untuk menjalankan mode *custom recovery*, sampel terpasang ClockworkMod Recovery atau Team Win Recovery Project (TWRP).

Sampel yang sudah terpasang *custom recovery* maupun *root* dan *busybox* akan menjalankan perintah Linux dd dan nc (Netcat). Perintah dd akan dijalankan pada perangkat sampel yang hasilnya akan dikirim ke jaringan dengan menggunakan metode TCP Forward. Hasil dari proses dd ini tidak disimpan di dalam perangkat sampel. *Imaging workstation* akan melakukan perekaman terhadap data yang dikirim melalui jaringan tersebut dengan menangkapnya menggunakan perintah nc. Kedua metode akuisisi yang dijalankan akan menggunakan teknik yang sama.

Dalam melakukan proses akuisisi perangkat sampel dengan metode *root*, perangkat sampel akan dinyalakan dan menjalankan metode isolasi dengan menggunakan mode pesawat. Penggunaan mode ini dimaksudkan agar pada saat proses akuisisi media penyimpanan tidak mengalami perubahan dikarenakan ada data baru yang masuk ke dalam perangkat sampel. Data baru yang dimaksud adalah data proses sinkronisasi yang dilakukan oleh perangkat sampel melalui jaringan, baik jaringan seluler maupun jaringan WiFi.

Sementara itu, proses akuisisi dengan metode *custom recovery* tidak perlu dilakukan isolasi karena sistem *custom recovery* merupakan salah satu alternatif menjalankan mode *recovery* pada perangkat Android. Mode *recovery* merupakan mode untuk memulihkan perangkat Android yang mengalami masalah. Mode recovery berbeda dengan mode normal karena mode *recovery* dijalankan pada partisi tersendiri, terpisah dari partisi sistem operasi.



Gambar 5. Contoh Hasil Akuisisi Dengan Pendekatan DD Pada Sampel

Proses akuisisi yang dilakukan akan menghasilkan berkas dengan ekstensi .dd. Gambar 5 merupakan salah satu contoh hasil akuisisi perangkat Android yang dibuka menggunakan aplikasi Autopsy Forensic.

Dari hasil analisis yang dilakukan, proses akuisisi dengan metode *root* dan juga metode *recovery* memiliki hasil yang identik seperti yang ditunjukkan pada Tabel 1. Perbedaan data yang terjadi hanya pada data waktu akuisisi. Akuisisi dengan metode *root* lebih lama jika dibandingkan dengan metode *custom recovery*. Selain itu, hasil eksperimen menunjukkan bahwa proses akuisisi dengan *custom recovery* saja sudah bisa mendapatkan data yang sama seperti ketika perangkat tersebut dilakukan *rooting*. Di sisi lain, hasil analisis menunjukkan bahwa data dari hasil proses akuisisi dengan menggunakan teknik dd ini tidak menghasilkan hasil yang identik dengan penyimpanan aslinya. Dari hasil analisis ukuran, masih terdapat 0.01% perbedaan ukuran antara media penyimpanan sumber dengan berkas hasil dari proses akuisisi. Hal ini perlu dilakukan kajian lebih lanjut.

Tabel 1. Hasil Pengujian Terhadap Sampel

Parameter	Sample 1		Sampel 2		Sampel 3
	Boot	Recovery mode	Boot	Recovery mode	Recovery mode
Akses Root	Ya	Ya	Ya	Ya	Ya
Isolasi	mode Pesawat	-	mode Pesawat	-	-
Jumlah Blok	7634952	7634952	30777378	30777378	30777378
Ukuran Penyimpanan(Byte)	3909095424	3909095424	15758017536	15758017536	15758017536
Ukuran Hasil(Byte)	3909091328	3909091328	15758000128	15758000128	15758000128
Persentase hasil	99,99%	99,99%	99,99%	99,99%	99,99%
Jumlah Partisi Terakuisisi	30	30	22	22	19
Waktu Akuisisi(Detik)	805.481	630.912256	4183.729	2680.600464	4424.978389
Kecepatan Rata-rata Transfer(MB/s)	4.62622279084832	5.90890407429334	3.59201085921196	5.60620659506086	3.39617477847077

5. KESIMPULAN DAN SARAN

Berdasarkan eksperimen yang sudah dilakukan dan juga melihat hasil yang didapatkan, dapat ditarik kesimpulan bahwa teknik DD dapat digunakan untuk melakukan akuisisi sistem berkas pada perangkat bergerak berbasis Android. Adapun teknik ini bisa dijalankan pada mode *root* dan juga mode *custom recovery*. Selain itu, hasil menunjukkan bahwa dengan metode *custom recovery* tanpa proses *rooting* akan mendapatkan hasil akuisisi yang identik dengan metode *rooting*.

Adapun saran untuk penelitian selanjutnya yang bisa dilakukan adalah dengan mengembangkan sebuah aplikasi yang dapat melakukan akuisisi perangkat bergerak berbasis Android dengan metode *rooting* maupun mode *custom recovery* sehingga dapat memudahkan penyidik forensik digital dalam melakukan proses penyidikan.

DAFTAR PUSTAKA

AKAMAI, 2020. Web Attack Visualization. [online] Web application attacks observed between Jun 18, 2020 to Jun 24, 2020 for All Industries. Available at: <https://www.akamai.com/us/en/resources/our-thinking/state-of-the-internet-report/web-attack-visualization.jsp> [Accessed 27 Jun. 2020].

FENG, P., LI, Q., ZHANG, P. AND CHEN, Z., 2018. Logical acquisition method based on data migration for Android mobile devices. Digital Investigation, [online] 26, pp.55–62.Available at:<https://doi.org/10.1016/j.diin.2018.05.003>.

FORTE, D. AND DONNO, A. DE, 2010. Chapter 10 - Mobile Network Investigations. In: E. Casey, C. Altheide, C. Daywalt, A. de Donno, D. Forte, J.O. Holley, A. Johnston, R. van der Knijff, A. Kokocinski, P.H. Luehr, T. Maguire, R.D. Pittman, C.W. Rose, J.J. Schwerha, D. Shaver and J.R.B.T.-H. of D.F. and I. Smith, eds. [online] San Diego: Academic Press.pp.517–557. Available at: <http://www.sciencedirect.com/science/article/pii/B9780123742674000100>.

HOOG, A., 2011. Android Forensic Techniques. In: Android Forensics, 1st ed. Syngress.pp.195–284.

KEMP, S., 2020. Digital 2020: Indonesia. [online] Global Digital Insights. Available at: <https://datareportal.com/reports/digital-2020-indonesia> [Accessed 14 Jun. 2020].

MULLER, J., 2020a. Indonesia: digital device ownership by device 2019 | Statista. [online] Statista Technology and Telecommunication. Available at: <https://www.statista.com/statistics/802628/digital-device-usage-among-adults-by-device-indonesia/> [Accessed 14 Jun. 2020].

MULLER, J., 2020b. Indonesia: mobile operating system market share 2019 | Statista. [online] Statista Technology and Telecommunication. Available at: <https://www.statista.com/statistics/262205/market-share-held-by-mobile-operating-systems-in-indonesia/> [Accessed 14 Jun. 2020].

PARK, J., JANG, Y.H. AND PARK, Y., 2018. New flash memory acquisition methods based on firmware update protocols for LG Android smartphones. Digital Investigation, [online] 25, pp.42–54. Available at: <https://doi.org/10.1016/j.diin.2018.04.002>.

SRIVASTAVA, H. AND TAPASWI, S., 2015. Logical acquisition and analysis of data from android mobile devices. Information and Computer Security, 23(5), pp.450–475.

YANG, S.J., CHOI, J.H., KIM, K.B., BHATIA, R., SALTAFORMAGGIO, B. AND XU, D., 2017. Live acquisition of main memory data from Android smartphones and smartwatches. Digital Investigation, [online] 23, pp.50–62. Available at: <https://doi.org/10.1016/j.diin.2017.09.003>.

YUSOFF, M.N., MAHMOD, R., ABDULLAH, M.T. AND DEHGHANTANHA, A., 2014. Mobile forensic data acquisition in Firefox OS. In: 2014 Third International Conference on Cyber Security, Cyber Warfare and Digital Forensic (CyberSec). pp.27–31.