REPOSITOR, Vol. 2, No. 5, Mei 2020, Pp. 583-590
ISSN : 2714-7975
E-ISSN : 2716-1382

Investigasi Dini Contact Tracing Pasien Menggunakan Pendekatan Standarisasi Forensik Digital

Dedy Hariyadi*
Universitas Jenderal Achmad Yani Yogyakarta
dedy@unjaya.ac.id

Abstrak

Pertumbuhan penderita Covid-19 terjadi peningkatan yang sangat cepat. Investigasi dini yang direkomendasikan oleh World Health Organization (WHO) diantaranya melakukan contact tracing. Senada dengan pertumbuhan ponsel cerdas juga cukup meningkat, menurut hasil survei di Indonesia penggunaan internetnya banyak melalui ponsel cerdas. Hal ini tidak menutup kemungkinan penderita Covid-19 memiliki ponsel cerdas yang terhubung ke internet. Ponsel cerdas memiliki fitur untuk mencatat sebuah aktivitas berpergian dari satu lokasi ke lokasi lainnya. Fitur ini jika diaktifkan oleh penggunanya maka sangat bermanfaat untuk mengetahui riwayat berpergian. Untuk mendapat informasi berupa riwayat berpergian perlu menggunakan pendekatan Forensik Digital yang telah miliki prinsip dasar dan teknik yang berfungsi menjaga integritas suatu informasi dari sebuah perangkat seperti ponsel cerdas. Informasi ataupun artefak yang ditemukan oleh analis forensik digital hanya disajikan kepada pihak yang berwenang untuk diolah dan dimanfaatkan sesuai dengan kebutuhan. Pada penelitian ini informasi yang disajikan adalah hasil analisis riwayat berpergian berupa lokasi-lokasi yang pernah dikunjungi oleh penderita.

Kata Kunci: *Covid-19, Forensik Digital, Ponsel Cerdas, Location History, Takeout*

Abstract

The growth of people with Covid-19 is increasing very fast. Early investigations recommended by the World Health Organization (WHO) include contact tracing. In line with the growth of smartphones, it is also quite increasing, according to the results of a survey in Indonesia using a lot of internet via smartphones. This does not rule out Covid-19 sufferers have a smartphone connected to the internet. Smartphones have a feature to record a travel activity from one location to another. This feature, if activated by its user, is very useful for knowing travel history. To get information in the form of travel history, it is necessary to use a Digital Forensic approach that already has basic principles and techniques that function to maintain the integrity of information from a device such as a smartphone. Information or artifacts found by digital forensic analysts are only presented to authorized parties to be processed and utilized as needed. In this study, the information presented is the result of an analysis of travel history in the form of locations that have been visited by sufferers.

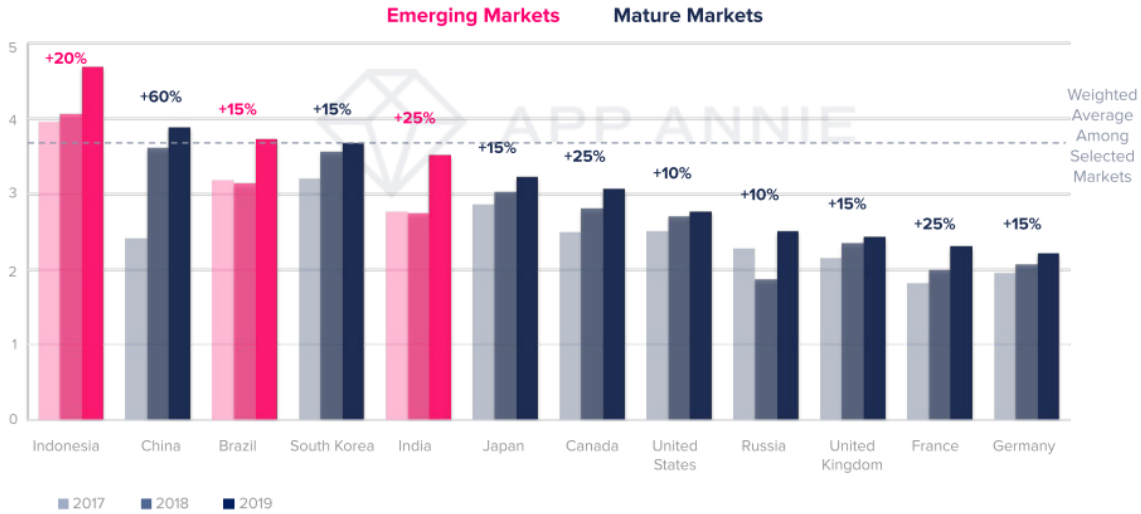
Keywords: *Covid-19, Digital Forensics, Smartphones, Location History, Takeout*

1. Pendahuluan

Epidemiologi merupakan ilmu yang mempelajari tentang distribusi, frekuensi, dan faktor-faktor yang mempengaruhi penyebaran suatu penyakit pada suatu kelompok orang [1]. Terdapat beberapa faktor yang mempengaruhi distribusi penyakit yaitu: waktu, orang, dan tempat. Dalam mengidentifikasi sebaran penyakit dapat ditinjau dari aspek tempat dengan batasan tertentu seperti batas alam atau batas administrasi pemerintah. Contoh batas alam seperti sungai dan gunung, sedangkan batas administrasi dapat menggunakan batas wilayah yang telah ditetapkan oleh pemerintah seperti desa, kecamatan, kabupaten, kota, dan provinsi [2]. Sedangkan sebaran penyakit yang telah melewati batas beberapa negara atau sebaran yang sangat luas dan telah menjangkit ke banyak orang disebut pandemi [3].

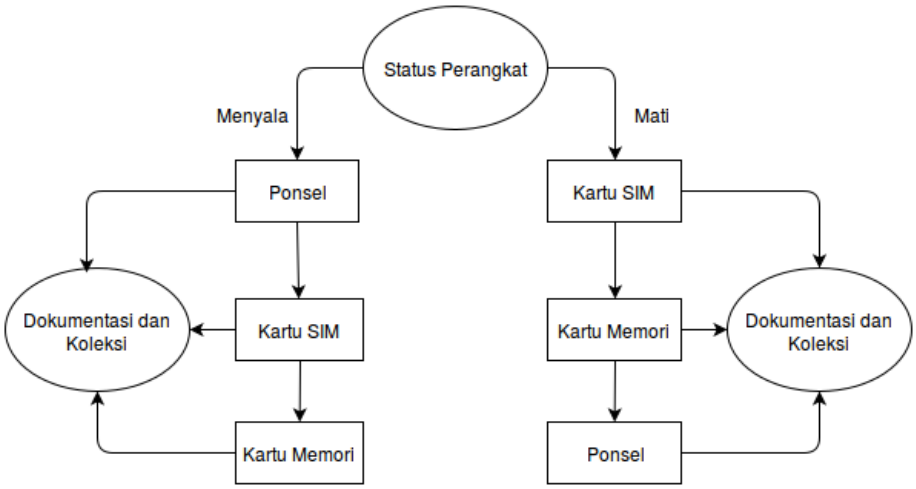
World Health Organization (WHO) memberikan panduan invesitigasi dini terkait tanggap darurat dari penyebaran *Novel Coronavirus* (2019-nCoV) dalam upaya penyempurnaan rekomendasi, pencirian epidemiologi, memahami penyebaran, tingkat keparahan, spektrum penyakit, dampak ke masyarakat, dan pemodelan tindakan pencegahan. Salah satu pemodelan

untuk melakukan tindakan pencegahan adalah mengetahui riwayat kontak pasien saat berpergian [4]. Selanjutnya 2019-nCoV disebut *Novel Corona Diseases* atau Covid-19. Penggunaan internet pada ponsel cerdas baik secara global [5] maupun nasional [6] menunjukan nilai yang cukup besar, yaitu diatas 90%. Bahkan Indonesia merupakan negara terbanyak yang menggunakan ponsel cerdas dalam sehari. Tren penggunaan ponsel cerdas bersistem operasi Android dari tahun 2017 selalu menunjukan peningkatan sampai tahun 2019, seperti tampak pada **Error! Reference source not found.** [7]. Oleh sebab itu untuk mengetahui riwayat berpergian seorang pasien dapat menggunakan pendekatan forensik digital dengan melakukan penelusuran dan analisis akun Google.



Gambar 1. Survey Penggunaan Ponsel Cerdas Menurut App Annie

Akun Google yang digunakan pada ponsel cerdas bersistem operasi Android dapat dijadikan barang bukti digital untuk dikumpulkan dan dianalisis oleh analis forensik digital [8]. Prosedur mengamankan barang bukti elektronik berupa ponsel cerdas dibedakan menjadi dua yaitu ponsel dalam kondisi menyala dan ponsel dalam kondisi mati. Adapun tahapan akuisisi atau mengamankan barang bukti elektronik dan/atau digital dapat dilihat pada **Error! Reference source not found.** [9].



Gambar 2. Tahapan Akuisisi Ponsel

2. Metode Penelitian

Indonesia telah memiliki standarisasi terkait dengan forensik digital yang dikeluarkan oleh Badan Standarisasi Nasional, SNI ISO/IEC 27037:2014. Ruang lingkup standarisasi adalah

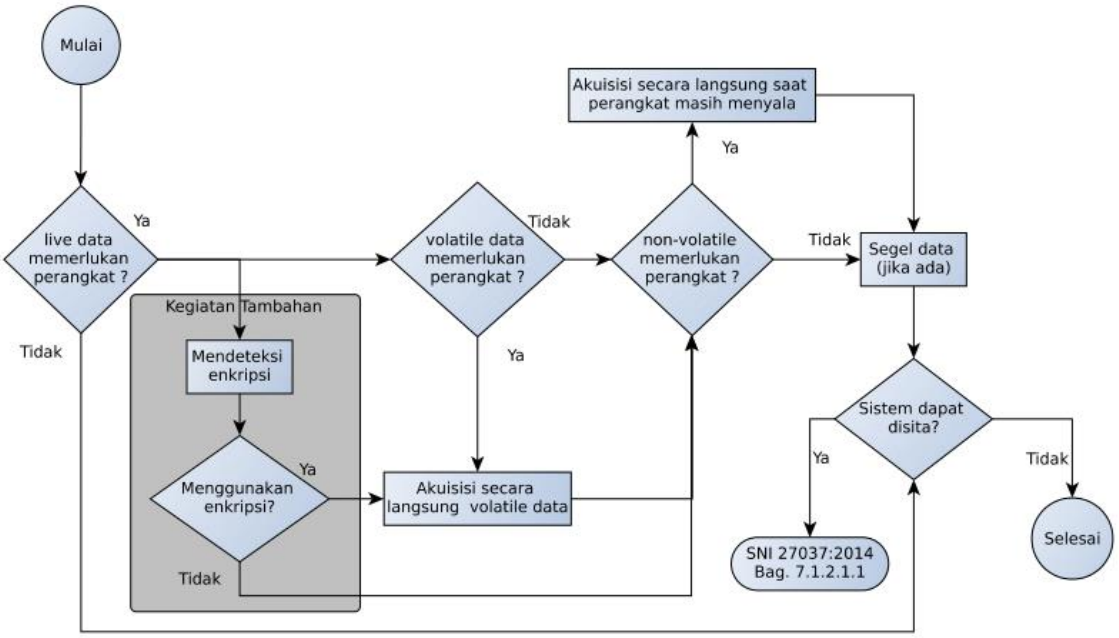
identifikasi, pengumpulan, akuisisi dan preservasi barang bukti elektronik dan/atau digital yang berpotensi. Pada penelitian ini berbasiskan SNI ISO/IEC 27037:2014 dalam mengumpulkan barang bukti elektronik dan/atau digital. Tidak hanya terkait perihal teknik pengumpulan barang bukti elektronik dan/atau digital saja. Namun, penelitian ini juga menekankan prinsip-prinsip forensik digital seperti [10]:

1. Meminimalkan penanganan secara langsung barang bukti elektronik dan/atau digital
2. Semua aktivitas harus didokumentasikan
3. Mematuhi peraturan dan perundangan yang berlaku
4. Tim forensik digital harus menjaga nama baiknya

2.1 SNI ISO/IEC 27037:2014

Untuk menghindari kebocoran data beberapa sistem telah menerapkan multi factor authetication yang melibatkan ponsel pemilik akun. Walaupun seseorang yang tidak berhak telah mengetahui username dan password tetap tidak dapat masuk ke sistem karena telah menerapkan *multi factor authentication* [11]. Oleh sebab itu tetap memerlukan ponsel dalam kondisi menyala untuk mendapatkan kode dari *multi factor authentication*. Pada SNI ISO/IEC 27037:2014 disarankan tahapan berikut sesuai pada alur **Error! Reference source not found.**:

1. Informasi yang didapatkan memerlukan akses ponsel jika menerapkan *multi factor authentication*.
2. Informasi yang didapatkan tidak bersifat *volatile*.
3. Informasi tersebut berupa kode *multi factor authentication* yang digunakan proses akuisisi.
4. Sehubungan ini bukan tindak kejahatan maka ponsel dapat dikembalikan ke pemilik.

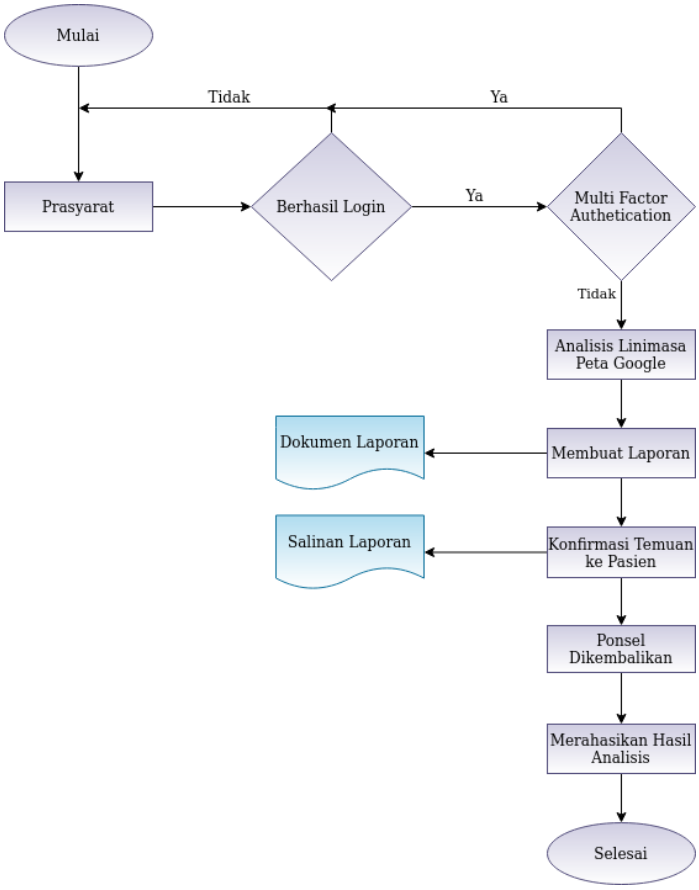


Gambar 3. Tahapan Akusisi Perangkat Dalam Kondisi Menyala

2.2 Alur Analisis

Berdasarkan **Error! Reference source not found.** maka diperlukan sebuah prasyarat dalam proses mendapatkan informasi dan analisis riwayat berpergian seorang pasien. Adapun prasyarat yang diperlukan diantaranya adalah surat persetujuan pemeriksaan dan ponsel cerdas telah diaktifkan *Location History*. Surat persetujuan pemeriksaan ini bersifat rahasia karena terdapat beberapa informasi penting seperti username dan password serta kode *multi factor authentication* jika ada. Tim analis melakukan analisis dan membuat laporan rangkap dua. Pihak pasien berhak mendapatkan hasil analisis dan mendapatkan ponsel kembali. Selain itu pihak yang berkepentingan wajib merahasikan informasi detil dan temuan terkait analisis riwayat berpegian pasien sesuai dengan prinsip forensik digital yang telah ditetapkan pada SNI ISO/IEC

27037:2014. Adapun alur analisis riwayat berpergian pasien yang menggunakan akun Google tampak pada **Error! Reference source not found.**.



Gambar 4. Alur Analisis Riwayat Berpergian Pasien

3. Analisis dan Pembahasan

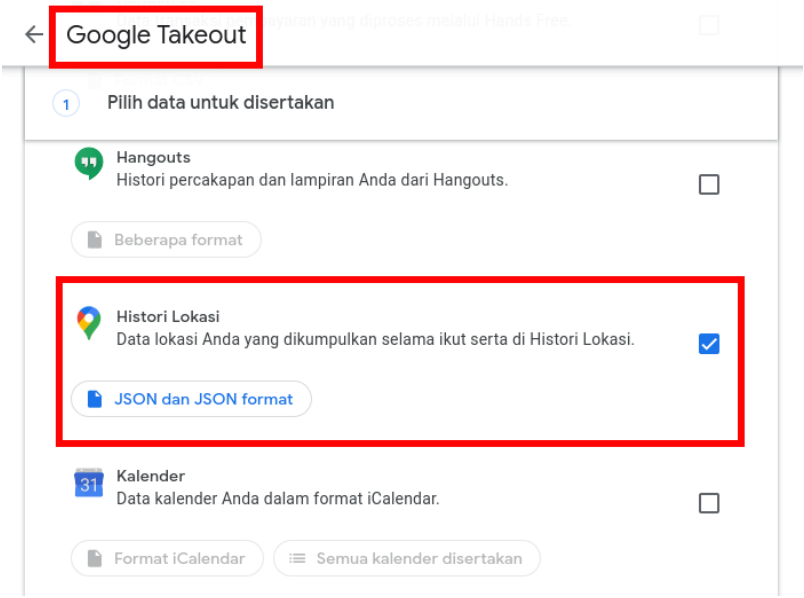
Setelah prasyarat telah dipenuhi oleh pihak yang berkepentingan diantaranya pasien, pihak berwenang, dan tim analis maka tahapan selanjutnya adalah melakukan pengumpulan barang bukti dan menganalisisnya. Pada penelitian ini mengikuti standarisasi dari National Institute of Standards Technology (NIST) dan mengikuti pedoman dari SNI ISO/IEC 27037:2014.

3.1. Pengumpulan Barang Bukti

Proses pengumpulan barang bukti mengikuti standarisasi forensik digital. Teknik akuisisi yang digunakan mengikuti standarisasi NIST Special Publication 800-101 yaitu ekstraksi barang bukti secara manual. Proses ekstrasi barang buktinya yaitu dengan cara mengakses akun surel gmail yang telah disampaikan pada prasyarat. Saat melakukan ekstraksi proses akuisisi direkam menggunakan kamera perekam [12]. Proses akuisisi menggunakan teknik ekstrkasi manual kurang lebih seperti tampak pada **Error! Reference source not found.**.

Gambar 5. Ekstraksi Barang Bukti Secara Manual

Dalam mengumpulkan barang bukti harus mengikuti kaidah yang telah tertuang pada SNI ISO/IEC 27037:2014 yaitu terkait syarat sebuah barang bukti digital. Syarat sebuah barang bukti yang berpotensi adalah relevan, reliabel, kecukupan [10]. Ketiga syarat tersebut dapat diketemukan saat melakukan penggeledahan akun Gmail yang menunjukan riwayat berpergian seseorang dalam bentuk peta dan berkas. json. Untuk mengekstraksi barang bukti digital berupa berkas json dapat mengunduhnya melalui sistem takeout milik Google yang diakses melalui halaman https://takeout.google.com/settings/takeout. Sehubungan kasusnya adalah riwayat berpergian maka mengekstraksi barang bukti yang relevan yaitu *Location History* seperti tampak pada **Error! Reference source not found.**. Waktu proses ekstraksi tergantung dari jumlah lokasi yang ditercatat oleh ponsel cerdas.



Gambar 6. Mengekstraksi Location History

3.2. Analisis Barang Bukti

Hasil ekstrasi dari sistem Takeout Google berdasarkan History Location pertama kali diaktifkan sampai dengan saat ini. Jadi berkas yang dihimpun oleh pihak Google sangat besar. Rekomendasi untuk dilakukan kompresi dengan ekstensi berkas .tgz. Tabel 1 merupakan artefak dari *Location History* yang didapatkan dari sistem Takeout Google.

Tabel 1. Artefak Location History

No	Deskripsi	Tipe Berkas
1	Ringkasan riwayat perjalanan dari pertama kali mengaktifkan *Location History*.	Hypertext Markup Language (HTML), contoh: archive_browser.html

2	Riwayat perjalanan dari pertama kali mengaktifkan *Location History*.	JavaScript Object Notation (JSON), contoh: Histori Lokasi.json
3	Riwayat perjalanan dari pertama kali mengaktifkan *Location History* yang dikategorikan berdasarkan tahun.	JavaScript Object Notation (JSON), format: TAHUN_BULAN.json, contoh: 2020_MARCH.json

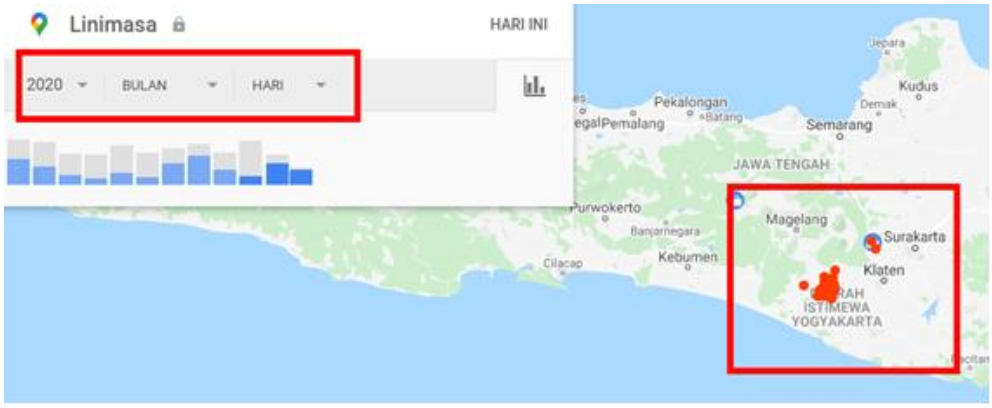
Artefak berupa berkas. json terdapat informasi diantaranya titik koordinat dengan format latitude dan longitude. Titik koordinat ini dapat menunjukan suatu lokasi yang dikunjungi, titik awal melakukan perjalanan, dan titik akhir dari perjalanan. Saat melakukan perjalanan terdapat beberapa aktivitas yang telah dikategorikan oleh Google diantaranya: mengendarai motor (motorcyling), penumpang (in passenger vehicle), berdiam diri (still), berjalan (walking), bersepeda (cycling), di dalam kapal (in ferry), berlari (running), di dalam pesawat (flying), di dalam bis (in bus), di dalam kereta bawah tanah (in subway), di dalam kereta (in train), berlayar (sailing), bermain ski (skiing), di dalam kendaraan (in vehicle), dan di dalam trem (in tram).

Catatan saat seseorang berkunjung ke suatu lokasi juga tercatat pada berkas. json. Adapun yang tercatat adalah latitude (latitudeE7), longitude (longitudeE7), alamat (address), nama lokasi (name), waktu berkunjung (startTimestampMs), dan waktu meninggalkan lokasi (endTimestampMs). Format waktu pada bagian durasi masih menggunakan Unix Timestamp, seperti tampak pada **Error! Reference source not found.**.

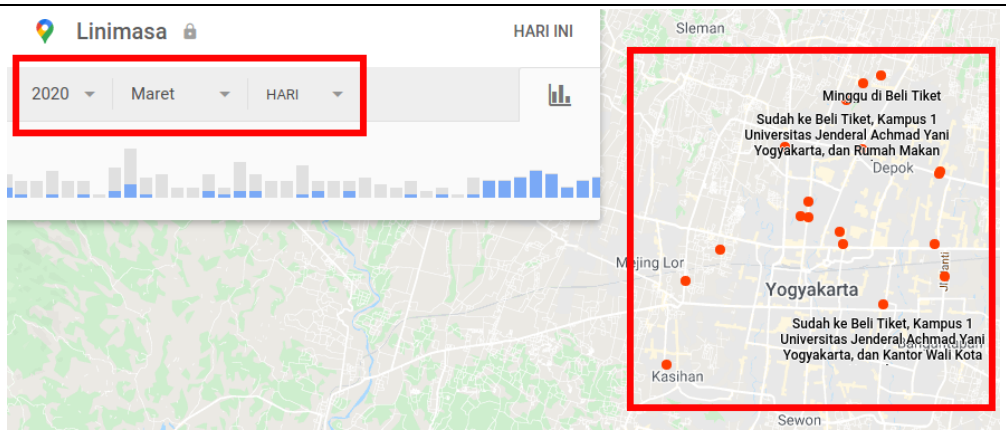

```
"placeVisit" : {
  "location" : {
    "latitudeE7" : -77837429,
    "longitudeE7" : 1103413049,
    "placeId" : "ChIJEchb6bNZei4R_H-jXKwA9Ws",
    "address" : "Jl. Tata Bumi\nArea Sawah\nBanyuraden\nKec. Gamping\nKabupaten Sleman\nDaerah Istimewa Yogyakarta 55293\nIndonesia",
    "name" : "Bakso & Mie Ayam Mas Joss 2",
    "locationConfidence" : 100.0
  },
  "duration" : {
    "startTimestampMs" : "1583124480000",
    "endTimestampMs" : "1583125746000"
  }
```


Gambar 7. Artefak Berkunjung ke Suatu Lokasi

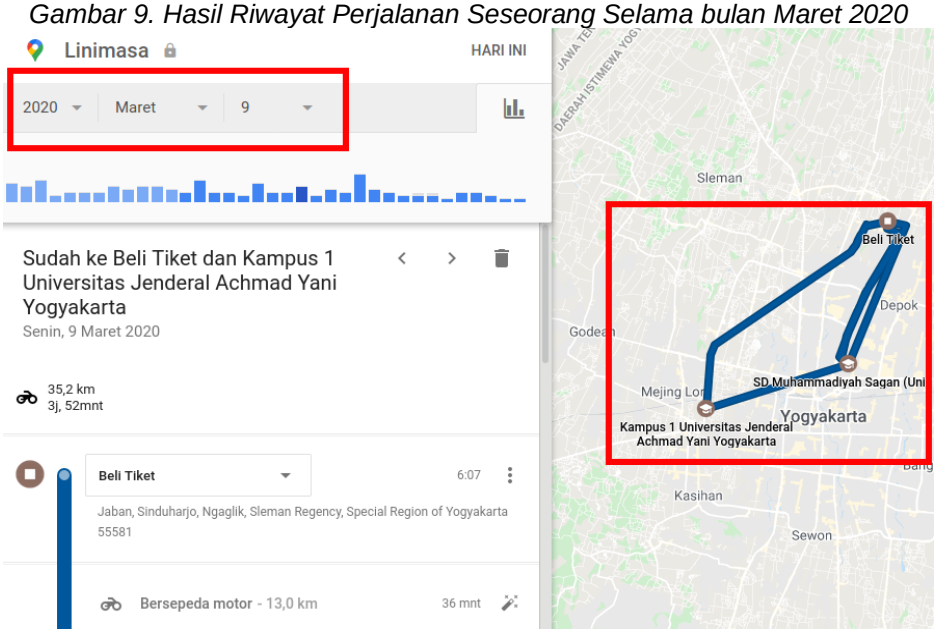
Pihak Google telah mempermudah analisis riwayat berpergian menggunakan layanan Google Map yang dapat diakses pada alamat https://www.google.com/maps/timeline. Pencarian riwayat dapat berdasarkan tahun, tahun-bulan, atau tahun-bulan-hari. **Error! Reference source not found.** menunjukan riwayat perjalanan selama tahun 2020, pada penelitian ini terhitung mulai bulan Januari sampai dengan Maret. Terlihat riwayat perjalanan lebih didominasi di wilayah Daerah Istimewa Yogyakarta. Peta yang disajikan pihak Google dapat diperbesar sesuai dengan kebutuhan. Hasil penelusuran riwayat perjalanan selama bulan Maret 2020 dapat dilihat pada **Error! Reference source not found.** sedangkan riwayat perjalanan selama sehari, sebagai contoh pada tanggal 9 Maret 2020 dapat dilihat pada **Error! Reference source not found.**.



Gambar 8. Hasil Riwayat Perjalanan Seseorang Selama Tahun 2020



Gambar 9. Hasil Riwayat Perjalanan Seseorang Selama bulan Maret 2020



Gambar 10. Hasil Riwayat Perjalanan Seseorang pada 9 Maret 2020

4. Kesimpulan

Pengguna ponsel cerdas bersistem operasi Android dan iOS yang memiliki akun Gmail jika telah mengaktifkan *Location History* maka dapat dilakukan analisis riwayat perjalanan. Analisis ini dapat digunakan untuk membantu untuk melakukan *tracing* orang dalam pengawas, pasien dalam pengawasan atau pasien positif Covid-19. Menganalisis dengan pendekatan forensik digital karena memiliki prinsip dan prosedur yang menjaga integritas sehingga mempermudah pihak-pihak yang berwenang untuk melakukan tindakan lebih.

Penelitian ini masih bersifat analisis dasar atas eksplorasi ponsel cerdas yang dimiliki orang dalam pengawas, pasien dalam pengawasan atau pasien positif Covid-19 saat melakukan perjalanan. Informasi riwayat kunjungan berupa peta belum maksimal sehingga perlu pendalaman lebih lanjut terkait dengan berkas yang diunduh melalui sistem Takeout. Berkas. json dapat dikembangkan lagi untuk penelitian selanjutnya yang digabungkan dengan berkas. json lainnya dari sistem Takeout orang dalam pengawas, pasien dalam pengawasan atau pasien positif Covid-19 sehingga menghasilkan analisis *tracing* yang lebih komprehensif.

Referensi

[1] Z. Ismah, *Dasar Epidemiologi*. Medan: Universitas Islam Negeri Medan, 2018.
[2] I. Dwiprahasto, “Epidemilogi,” in *Epidemiologi*, Magister Manajemen Rumah Sakit UGM.
[3] World Health Organization, “Pencegahan dan pengendalian infeksi saluran pernapasan akut (ISPA) yang cenderung menjadi epidemi dan pandemi di fasilitas pelayanan kesehatan,” Jenewa, 2007.

[4] World Health Organization, “Coronavirus disease (COVID-2019): Situation Reports - 8,” Jenewa, 2020.
[5] J. Mander dan V. Trifonova, “Device, GlobalWebIndex’s Flagship Report on Device Ownership and Usage,” 2019.
[6] Asosiasi Penyelenggara Jasa Internet Indonesia dan Asosiasi Penyelenggara Jasa Internet, “Penetrasi dan Perilaku Pengguna Internet Indonesia 2018,” Jakarta, 2019.
[7] App Annie, “State of Mobile 2020,” 2020.
[8] A. Edens, *Cell Phone Investigations: Search Warrants, Cell Sites and Evidence Recovery*. Police Publishing, 2014.
[9] L. Reiber, *Mobile Forensic Investigations: A Guide to Evidence Collection, Analysis, and Presentation*. Mc Graw Hill Education, 2016.
[10] Badan Standarisasi Nasional, “Teknologi Informasi - Teknik Keamanan-Pedoman Identifikasi, Pengumpulan, Akuisisi dan Preservasi Bukti Digital (SNI ISO/IEC 27037:2014),” Jakarta, 2014.
[11] A. Bissada dan A. Olmsted, “Mobile Multi-Factor Authentication,” in *2017 12th International Conference for Internet Technology and Secured Transactions, ICITST 2017*, 2018, hal. 210–211, doi: 10.23919/ICITST.2017.8356383.
[12] R. Ayers, S. Brothers, dan W. Jansen, “NIST Special Publication 800-101 Revision 1: Guidelines on Mobile Device Forensics,” Gaithersburg, MD, Mei 2014.