# ANALISIS FORENSIK WEB BROWSER PADA PERANGKAT ANDROID

Rahmat Inggi[*1], Heri Pebrianto Alam[2]
[1,2]Program Studi Sistem Informasi, STMIK Bina Bangsa Kendari
*e-mail: [*1]rahmatinggi35@gmail.com, [2]herifa95@gmail.com*

***Abstrak** Pada saat ini perkembangan teknologi sangat pesat, khususnya pada alat komunikasi Smartphone dengan sistem operasi Android. Dengan menggunakan Smartphone juga kita dapat dengan mudah mendapatkan sebuah informasi. Tetapi dengan teknologi yang semakin canggih masyarakat tidak hanya melakukan kegiatan yang positif namun ada juga yang melakukan kegiatan yang negatif. Web Browser merupakan aplikasi yang digunakan untuk mencari sebuah informasi, melakukan transaksi email, berkomunikasi dengan instant messenger atau jejaring sosial, berbelanja melalui situs Web e-commerce. Banyak terjadi tindak kejahatan melalui Web Browser ini salah satunya phising dimana pelaku melakukan penipuan dengan mengelabui korban seperti mengirim link palsu untuk mencuri data dari korbannya. Oleh karena itu dibutuhkan prosedur untuk menangani tindak kejahatan ini yaitu digital forensik. Tujuan dari penelitian ini untuk mengetahui proses investigasi forensik Web Browser serta mengetahui data apa saja yang dapat digunakan untuk menunjang bukti digital terhadapa kejahatan Web Browser khususnya Google Chrome pada perangkat Android. Metode yang digunakan pada penelitian ini adalah National Institute Of Justice (NIJ) dimulai dari tahapan persiapan, koleksi, pemeriksaan, analisis dan pelaporan. Hasil dari penelitian ini "Analisis Forensik Web Browser pada perangkat Android" terdapat beberapa barang bukti yang tersimpan didalam Web Browser Google Chrome yaitu Accounts, Bookmarks, Cookies, Cache, Document, E-mail, History, Images, Timestamps, Password, URL,Search History, dari beberapa bukti tersebut bisa dijadikan sebagai barang bukti di persidangan.***

***Kata Kunci :*** **Web Browser, Cybercrime, Digital Forensik, Android**

## I. PENDAHULUAN

Pada saat ini perkembangan teknologi sangat pesat, khususnya pada alat komunikasi Smartphone dengan sistem operasi Android. Penggunaan Smartphone juga kita dapat dengan mudah mendapatkan sebuah informasi. Tetapi dengan teknologi yang semakin canggih masyarakat tidak hanya melakukan kegiatan yang positif namun ada juga yang melakukan kegiatan yang negatif.

Di masa pandemi Covid-19 masyarakat cenderung lebih banyak mengandalkan internet ternyata turut berimbas pada kenaikan jumlah upaya serangan siber. Data dari Badan Siber dan Sandi Negara (BSSN), sepanjang bulan Januari hingga Agustus 2020, terdapat hampir 190 juta upaya serangan siber di Indonesia, naik lebih dari empat kali lipat dibanding periode yang sama tahun lalu yang tercatat di kisaran 39 juta. Upaya serangan siber terbanyak dicatat pada Agustus 2020, di mana BSSN mencatat jumlah serangan siber di kisaran 63 juta, jauh lebih tinggi dibandingkan Agustus 2019 yang hanya di kisaran 5 juta. Berdasarkan data tersebut, maka diperlukan suatu prosedur untuk menangani kejahatan pada dunia siber, salah satunya adalah digital forensik. Dalam mencari penanganan bukti secara umum berbeda dengan mencari bukti digital, Karena harus melalui beberapa prosedur-prosedur tertentu [1].

Forensik Smartphone Android telah berkembang dari waktu ke waktu, Beberapa kejahatan yang memanfaatkan kecanggihan dari Smartphone Android untuk melakukan kejahatan seperti phising, peretasan, perjudin, pornografi, korupsi, jaringan narkoba hingga kasus pembunuhan dsb. Salah satu kasus yang biasa terjadi yaitu phising dimana pelaku melakukan penipuan dengan mengelabui korban seperti mengirim link palsu, membuat Website bodong, dan sebagainya, tujuannya untuk mencuri data penting korban.

Web Browser merupakan aplikasi yang digunakan untuk mencari sebuah informasi, melakukan transaksi email, berkomunikasi dengan instant messenger atau jejaring sosial, berbelanja melalui situs Web e-commerce. Dari data yang disajikan di atas Google Chrome merupakan Browser yang paling banyak digunakan di dunia, sebanyak 64,6% pengguna di internet dan pada tahun 2020 penggunaan Google Chrome meningkat 2% dari tahun sebelumnya, di posisi kedua Browser safari milik Apple dengan jumlah pengguna sebesar 17,84% dan mengalami peningkatan 11,098% dibanding tahun 2019, lalu Firefox berada di posisi ketiga dengan jumlah pengguna 4,22% turun 8,29% dibanding tahun 2019, Samsung internet berada di posisi selanjutnya dengan pengguna 3,35% turun 2,98 dari tahun sebelumnya, sementara Opera memliki pengguna 1,99% dan mengalami penurunan 29,14% dibanding tahun sebelumnya, di urutan keenam UC Browser memliki pengguna 1,74% pada tahun 2020 dan mengalami peningkatan 3,3% dari tahun sebelumnya, Microsoft Edge dengan jumlah pengguna

1,45% di tahun 2020, selanjutnya Browser Edge legacy memliki pengguna 1,38% pada tahun 2020 dan mengalami penuruan 55,07% dari tahun sebelumnya, kemudian internet explorer mengalami penurunan 65,92% menjadi 1,35% pada tahun 2020 [2].

Penelitian ini akan menganalisis pencarian bukti digital pada Web Browser Google Chrome pada perangkat Android. Dan penelitian ini diharapkan dapat membantu pihak yang berwajib untuk menemukan bukti forensik dalam menyelesaikan kasus-kasus cybercrime yang terjadi pada Web Browser khususnya Google Chrome

## II. LANDASAN TEORI

Penelitian ini menerapkan studi literatur untuk mencari data sekunder berupa teori dan penelitian sebelumnya yang berkaitan dengan penelitian ini. Data primer penelitian ini adalah data digital yang diperoleh dari simulasi skenario kasus yang kemudian data tersebut di proses menggunakan metode National Institute Of Justice (NIJ) Metode ini memiliki tahapan yang lebih baik dibandingkan dengan metode yang lainnya karena digunakan untuk memperoleh atau mendapatkan bukti digital.

Metode penelitian yang digunakan oleh peneliti berdasarkan pedoman forensik perangkat mobile yang dibuat oleh National Institute Of Justice (NIJ) dengan tahapan-tahapan sebagai berikut :


Gambar 1 Tahapan Forensik yang dikembangkan oleh NIJ

Tahap persiapan peneliti mengidentifikasi masalah dan mengumpulkan informasi-informasi tentang masalah yang sedang dihadapi. Dan mempersiapkan peralatan yang diperlukan dalam melakukan tugas penyelidikan. Tahap koleksi ini dilakukan pengumpulan data-data yang dapat mendukung proses penyidikan dalam mencari barang bukti kejahatan digital. dan didalam tahapan ini juga terdapat proses pengambilan data dari barang bukti serta menjaga integritas barang bukti dari perubahan. Tahap pemeriksaan, pada tahap ini memeriksa bukti secara digital yang diperoleh melalui proses forensik baik secara manual ataupun secara otomatis dan untuk memastikan barang bukti digital yang diperoleh adalah asli. Tahap Analisis setelah dilakukan tahapan pemeriksaan yang telah dilakukan, peneliti melalukan evaluasi dari setiap solusi agar dapat dilakukan pemecahan masalah. Tahap Laporan, peneliti melaporkan dari hasil uji coba yang meliputi penggambaran tindakan apa saja yang dilakukan dalam melakukan proses investigasi.[3].

## III. HASIL DAN PEMBAHASAN

### *3.1 Skenario Kasus*

Studi ini membuat studi kasus kejahatan siber yang dikenal sebagai "phishing," yang melibatkan menipu atau merayu korban untuk mengklik tautan dan memasukkan informasi sensitif seperti alamat email dan kata sandi mereka.

Skenario kasus ini bermula pada saat pelaku mengirimkan sebuah link phising berupa link google form yang di dalamnya sudah di atur oleh pelaku agar bisa mengelabui korban. Lalu pelaku mengirim link tersebut melalui sebuah E-mail ke korban yang dituju, kemudian korban mengklik link tersebut dan di arahkan langsung ke Browser Google Chrome setelah itu korban menginputkan beberapa informasi ke dalam link tersebut berupa E-mail, Password, dan beberapa data penting lainnya. Setelah korban menginputkan beberapa informasi dari link phising tersebut, pelaku berhasil mendapatkan beberapa informasi korban yang kemudian digunakan pelaku untuk mencuri akun tersebut. Selanjutnya pihak yang berwenang mengamankan barang bukti yang ditemukan untuk dijadikan barang bukti di pengadilan, tujuan diamankan barang bukti adalah untuk menjaga keaslian dari barang bukti tersebut, lalu pihak berwenang memberikan barang bukti kepada investigator digital forensik untuk membantu proses pencarian barang bukti digital. Setelah menerima barang bukti dilakukan proses akuisisi data menggunakan tools forensik yang sudah disiapkan, selanjutnya dari proses akuisisi data didapatkan beberapa folder yang sudah di ekstraksi sehingga dilakukan proses analisis data menggunakan tools forensik yang bertujuan untuk menentukan bukti-bukti yang signifikan, Prosedur dokumentasi dan pelaporan harus dilengkapi dengan tepat, ringkas, dan jelas agar pihak-pihak yang berwenang dapat memahaminya.

Dan di bawah salah satu kode kriminal yang digunakan untuk menangkap pelaku phishing, pasal 378 tentang penipuan, beberapa penjahat dunia maya menggunakan taktik tipu daya untuk mendapatkan informasi dari korban mereka [4].

Dan para pelaku phising tunduk pada Pasal 51 UU ITE tentang manipulasi, yang menyatakan bahwa jika seseorang dengan sengaja melanggar hukum dengan mengubah, mengurangi, atau melakukan hal lain untuk

membuat data tampak asli, mereka dapat menerima hukuman maksimal 12 tahun penjara atau denda maksimal Rp 12 miliar. Dalam melakukan aksinya, mayoritas phisher memanipulasi untuk menipu korbannya [5].

*3.2 Investigasi Barang Bukti*

Teknik National Institute of Justice (NIJ) digunakan saat memeriksa bukti digital. Karena digunakan untuk mengumpulkan atau mendapatkan bukti digital, pendekatan ini memiliki tahapan-tahapan yang lebih unggul daripada cara-cara lainnya. Berikut adalah penjabarannya;

1. Persiapan

Untuk memudahkan dalam mencari bukti digital investigator menyiapkan Hardware yaitu Laptop dengan processor Intel Celeron N2840, RAM 8 GB,OS Windows 10 64 bit yang digunakan untuk menarik data, Kabel Connector Micro USB untuk menghubungkan laptop dan barang bukti yang akan di ekstraksi, dan Smartphone Android dengan sistem operasi Jelly Bean 4.2.2 digunakan sebagai barang bukti yang akan di ekstraksi untuk mencari bukti-bukti digital. Software atau tools yang digunakan investigator yaitu MOBILedit Forensics Express yang digunakan untuk melakukan proses ekstraksi data dari barang bukti dan Autopsy digunakan untuk proses analisis barang bukti digital, Aplikasi kingroot yang berfungsi untuk membuka hak akses pada Smartphone serta aplikasi Google Chrome yang digunakan sebagai Web Browser pada penelitian ini. Selanjutnya setelah menerima barang bukti dari pihak yang berwenang berupa Smartphone Android, investigator menyiapkan form permohonan pengujian dan Chain of Custody jadi form permohonan pengujian bertujuan untuk dasar dari investigasi untuk melakukan proses investigasi terhadap barang bukti yang diajukan, sedangkan Chain of Custody bertujuan untuk mencatat data personal penyidik sampai dengan konten barang bukti digital sesuai dengan mekanisme penyidikan. Kemudian dilakukan dokumentasi dari awal hingga bukti pelaporan yang dilengkapi oleh korban.

Kemudian berita acara penerimaan barang bukti dilakukan untuk mendapatkan hak atau izin dari penegak hukum untuk melakukan proses investigasi terhadap kasus yang ada.

2. Koleksi

Seperti yang ditunjukkan pada Gambar di bawah ini, investigator mengumpulkan bukti fisik berupa smartphone dan bukti elektronik berupa smartphone yang menjalankan sistem operasi Android yang akan digunakan untuk pengujian. Investigator juga menggunakan alat forensik untuk melakukan akuisisi data, khususnya MOBILedit Forensics Express dan Autopsy Tools untuk menganalisa file-file yang ditemukan pada disk dan mengembalikan file-file yang terhapus

3. Pemeriksaan

Karena MOBILedit Forensic Express mendukung sejumlah format gambar yang dapat digunakan oleh aplikasi forensik lainnya, maka MOBILedit Forensic Express dapat digunakan untuk menghasilkan cadangan data dan pencitraan sistem pada tahap analisis ini.

Saat menggunakan alat MOBILedit Forensic Express untuk pemeriksaan, barang bukti pertama harus terhubung ke komputer atau laptop sebelum alat ini akan secara otomatis terhubung ke Smartphone yang digunakan. Jika Smartphone terhubung dan terdeteksi oleh MOBILedit Forensic Express, proses akuisisi data kemudian dimulai, yang menyalin bukti digital dan mencatat aktivitas yang dilakuk

Setelah Smartphone sudah tersambung dan terdeteksi dilakukan proses ekstraksi dari aplikasi Google Chrome dengan mengklik Application analysis, yang bertujuan untuk melakukan ekstraksi hanya dengan memilih aplikasi tertentu saja, dan proses ekstraksi datanya lebih cepat sehingga memudahkan investigasi dalam proses ekstraksi data

Langkah selanjutnya yaitu melakukan proses ekstraksi pada aplikasi Google Chrome, kemampuan tool ini dalam membuat backup data cukup baik serta mampu membuat backup dengan ekstensi AB (Android Backup), img, zip, dan beberapa jenis ekstensi lain sehingga dapat dibuka dengan tool forensik lainnya.

Hasil dari proses ekstraksi ini berupa folder yang didalamnya berisi beberapa file yang akan dianalisis menggunakan tool autopsy untuk mendapatkan barang bukti digital

4. Analisis

Setelah prosedur ekstraksi menghasilkan file atau data digital, data tersebut akan diperiksa dengan cermat untuk memberikan bukti digital. Temuan penyelidikan ilmiah dan hukum dari bukti digital ini harus dipresentasikan di pengadilan. Perangkat lunak prosedur analisis ini menggunakan alat Autopsy. Antarmuka detektif kit, yang disebut autopsy, membuatnya lebih mudah bagi pengguna untuk memanfaatkan alat dan melakukan penyelidikan. Program ini dapat memeriksa sistem file NTFS, FAT, UFS1/2, dan EXT2/3 pada perangkat Windows dan UNIX. Program ini melakukan operasi seperti pencarian kata kunci, integritas gambar, manajemen kasus, dan hal-hal lainnya. Ini adalah layar pembuka aplikasi Autopsy pada Windows.

Pada saat membuka aplikasi adalah user harus mengisi beberapa form yaitu case information , form ini digunakan untuk menamai kasus dan mengatur letak penyimpanan bukti yang akan dianalisis , dan form optional information untuk mengurutkan kasus dan beberapa data dari investigator yang akan melakukan analisis.

Sementara formulir informasi opsional menjelaskan kasus dan penyelidik mana yang menggunakan aplikasi Autopsi untuk melakukan analisis, formulir informasi kasus menunjukkan kasus mana yang akan dianalisis dengan memasukkan nama kasus dan memilih direktori untuk menyimpan hasil kasus. Formulir ini memungkinkan pengambilan catatan analisis yang dapat dilacak.

Setelah melengkapi kedua formulir tersebut, lanjutkan ke tahap melakukan proses analisis dari file gambar yang dihasilkan oleh aplikasi. Tahap ini meliputi pemilihan file yang akan dianalisis dari proses ekstraksi penyimpanan, menentukan modul ingest untuk keperluan analisis data, dan menentukan data yang akan dianalisis dalam bentuk file yang telah diekstrak. Selain itu juga menampilkan sumber-sumber data yang telah diidentifikasi pada aplikasi Autopsy

File yang akan dianalisis adalah file logical yang dibuat selama proses ekstraksi data dari program Google Chrome. Akan ada kotak untuk memilih folder yang akan kita periksa setelah memilih opsi Logical Files. Formulir untuk mengambil folder yang dibuat selama prosedur ekstraksi dan dimasukkan ke dalam program autopsi untuk analisis. Setelah aplikasi autopsi memasukkan dan membaca data, aplikasi akan menampilkan formulir modul ingest dan memutuskan modul mana yang diperlukan untuk menganalisis data.

Selanjutnya adalah form untuk memilih modul ingest pada aplikasi autopsi. Tujuannya adalah untuk membagi data yang diperlukan untuk proses analisis file sehingga terorganisir dengan tepat dan investigator dapat menganalisisnya secara menyeluruh. Modul-modul ingest ini hadir dalam berbagai pilihan, yang masing-masing memiliki tujuan yang berbeda untuk analisis agar mudah dilakukan. dan setelah memilih modul ingest, program autopsi akan meluncurkan modul ingest yang dipilih dan membuka menu utama untuk menganalisis file penyimpanan yang dipilih. Selain itu, proses analisis dipecah menjadi beberapa komponen data tergantung pada tujuan modul ingest yang digunakan penyelidik untuk melihat data file yang telah dibaca dalam program autopsi dan menjadi sumber data. Hal yang dilakuykan ialah data source yang berhasil didapatkan oleh aplikasi autopsy dari folder ekstraksi yang dimasukan ke dalam aplikasi ini untuk dilakukan proses analisis terhadap folder tersebut, setelah masuk dan terbaca semua isi dari folder tersebut tersusun dengan teratur dan mudah untuk di analisis oleh investigator, dan folder hasil ekstraksi ini yaitu com.Android.chrome merupakan bahan analisis karena didalam folder tersebut terdapat data-data dari aplikasi Google Chrome. Setelah melakukan analisis data source, maka aplikasi ini memberikan fasilitas untuk melihat semua data-data.

Folder hasil ekstraksi aplikasi Google Chrome, yang berasal dari sumber data menyeluruh dan dipisahkan ke dalam berbagai komponen termasuk berdasarkan jenis file, file yang dihapus, dan ukuran file, dapat dilihat secara detail dengan kemampuan aplikasi otopsi. Data berdasarkan jenis file dibagi menjadi dua kategori, yaitu data berdasarkan ekstensi, yang menunjukkan semua data dengan format seperti gambar, video, audio, database, dokumen yang diperoleh melalui proses analisis sehingga dapat digunakan sebagai barang bukti, dan data berdasarkan jenis MIME, yang mencakup data seperti aplikasi, teks, dan jenis data lainnya.

Selanjutnya, data menunjukkan deleted files, yang menunjukkan data yang sudah dihapus dari sistem file, dan file size, yang menunjukkan jumlah data yang berhasil diperiksa. Langkah berikutnyamerupakan hasil dari konten yang tersimpan di dalam aplikasi Google Chrome seperti Web accounts, Web History, Web Bookmarks dan sebagaianya dari data ini didapatkan hasil rekam jejak digital dari penggunaan aplikasi Google Chrome yang kemudian dapat di ekstrak untuk menjadi sebuah barang bukti dalam kasus tindak kejahatan siber yaitu phising, dimana kita bisa melihat beberapa history pelaku dan akun korban yang didapatkan dari si pelaku kejahatan phising tersebut.

Dalam barang bukti yang investigator temukan dalam penelitian ini, yang berhubungan dengan kasus yang akan ditangani agar bisa dipertanggungjawabkan dengan kasus yang berjalan. Barang bukti pertama yang ditemukan setelah melakukan analisis adalah ada beberapa Accounts yang terdapat di dalam Google Chrome yang merupakan Accounts dari pelaku.

Kemudian bukti selanjutnya ditemukan Bookmarks atau link sebuah Website yang tersimpan di Browser yang ditandai sebagai tautan yang sering dikunjungi. Pada Bookmarks ini pelaku menandai beberapa Website yang merupakan Web tentang cara membuat Web phising dan cara menghack sebuah E-mail.

Bukti selanjutnya yang didapatkan berupa Cookies yang tersimpan pada aplikasi Google Chrome, Cookies ini berfungsi agar Website mengetahui aktivitas apa yang telah dilakukan user pada waktu sebelumnya, Aktivitas yang dimaksud seperti mengklik sebuah tombol atau halaman yang sudah dibuka oleh user. Dari aktivitas penggunaan Google Chrome yang digunakan ada 286 Cookies yang ditemukan pada tahap analisis dan beberapa Cookies ini merupakan URL Google Form yang digunakan pelaku dalam membuat link phising tersebut.

Bukti Selanjutnya yang didapatkan dari proses analisis yaitu terdapat Cache dari Google Chrome yang tersimpan di dalam folder com.Android.chrome berupa data situs yang pernah di kunjungi pelaku yaitu Google form yang merupakan tempat membuat link phising tersebut. Selanjutnya bukti yang ditemukana ialah Email dan Password korban. Barang bukti berupa Email dan Password terdapat di folder download dimana pelaku mendownload hasil dari link phising yang berhasil di dapatkan dari korban.

Selanjutnya ditemukan History atau riwayat pencarian dari hasil analisis yang menampilkan beberapa jejak hasil kegiatan selama melakukan browsing di intenet melalui aplikasi Google Chrome, History yang ditemukan berupa pencarian Google form yang merupakan tempat pelaku membuat link phising tersebut. Didalam hasil analisis yang dilakukan pada aplikasi autopsy ini juga di temukan gambar atau file images yang mungkin bisa dijadikan sebagai barang bukti digital, yang tersimpan di dalam file types dengan format extension nya images.

Terdapat juga Timestamps atau stempel waktu berupa tanggal dan waktu yang tersimpan pada saat melakukan browsing di internet, Seperti pada saat mengakses sebuah situs maka tanggal dan waktu tersebut akan tersimpan otomatis pada aplikasi Google Chrome. Kemudian barang bukti yang ditemukan lagi terdapat di Web history Google Chrome berupa URL yang digunakan pelaku untuk melakukan tindak kejahatang phising, URL tersebut tersimpan di dalam history Google Chrome dan dari URL tersebut kita bisa menjadikan sebuah bukti digital dari pelaku dalam melakukan tindak kejahatan phising, Pelaku menggunakan link phising tersebut untuk dikirimkan ke korban untuk melakukan pencurian akun dan data-data penting lainnya.

Barang bukti selanjutnya yang bisa membuktikan kejahatan dari pelaku ialah ditemukan dokumen yang berisi tentang panduan bagaimana cara melakukan hacking, dimana pelaku mendownload dokumen tersebut melalui

Google Chrome dan tersimpan ke dalam perangkat yang digunakan pelaku. Selanjutnya ditemukan Search history atau riwayat penelusuran yaitu beberapa daftar dari sebuah laman Website yang pernah dikunjungi yang tersimpan didalam Browser Google Chrome.

5. Laporan

Berdasarkan laporan dari Chain of Custody korban melaporkan tersangka dengan kasus tindak kejahatan phising melalui aplikasi Google Chrome pada perangkat Android pada tanggal 14 Agustus 2022 dan kemudian pihak investigator melakukan pengamanan serta mengumpulkan barang bukti berupa Smartphone Android dengan tipe Samsung GT-I9082 yang dicurigai dalam kasus ini dikediaman pelaku pada tanggal 18 Agustus 2022. Kemudian hasil yang ditemukan adalah pelaku terbukti bersalah atas perbuatannya sejak tanggal 21 Agustus 2022 sampai dengan di tangkapnya barang bukti pelaku dalam melakukan tindak kejahatan cybercrime yaitu melakukan tindak kejahatan phising untuk mendapatkan sebuah informasi dari korban. Untuk itu pelaku dikenakan pasal 378 KUHP tentang penipuan dan sebagian pelaku kejahatan cybercrime menggunakan trik kebohongan dalam mendapatkan sebuah informasi dari korban, dan pasal 51 (UU ITE) tentang manipulasi didalam pasal tersebut apabila seseorang sengaja melanggar hukum dengan cara-cara manipulasi, melakukan perubahan, pengurangan atau yang lainnya sehingga data tersebut seolah-olah asli. Selanjutnya investigator menyerahkan barang bukti pada pihak pengadilan untuk ditindak lanjuti dan bisa untuk dipertanggungjawabkan [6].

Hasil pengujian analisis Google Chrome pada perangkat Android

1. Accounts

Untuk bukti digital yang pertama yaitu Accounts dimana pada hasil analisis yang dilakukan terdapat beberapa Accounts yang tersimpan. Accounts tersebut merupakan milik pelaku yang digunakan untuk mengirimkan link phising tersebut ke korban.

2. Bookmarks

Bukti digital selanjutnya adalah Bookmarks yang tersimpan di Browser Google Chrome, yang ditandai dengan tautan yang sering dikunjungi dimana pelaku menandai beberapa website yang merupakan tentang cara membuat sebuah web phising dan cara menghack sebuah E-mail.

3. Cookies

Bukti selanjutnya ditemukan Cookies yang tersimpan pada aplikasi Google Chrome, terdapat beberapa aktivitas korban yang tersimpan seperti pada saat mengklik sebuah tombola atau halaman yang pernah dibuka oleh pelaku dan pada cookies ini ditemukan beberapa URL Google Form yang digunakan pelaku dalam membuat link phising.

4. Cache

Didapatkan juga Cache yang tersimpan pada aplikasi Google Chrome berupa situs yang dikunjungi oleh pelaku dimana pelaku mengunjungi situs Google Form yang digunakan pelaku untuk membuat link phising tersebut.

5. Document

Bukti selanjutnya ditemukan Dokumen yang didownload oleh pelaku, dimana isi dari dokumen tersebut merupakan panduan tentang bagaimana cara melakukan hacking. Dokumen ini tersimpan didalam folder Google Chrome pada perangkat yang digunakan oleh pelaku.

6. E-mail dan Password

Untuk bukti digital selanjutnya yang berhasil didapatkan adalah E-mail dan Password dari korban yang berhasil didapatkan melalui link phising tersebut. Pelaku mendownload phising tersebut yang kemudian hasil download tersebut tersimpan didalam folder com.android.chrome/live_external/files/Download/Untitled form.csv didalam folder tersebut terdapat sebuah file yang didalamnya terdapat E-mail dan password dari korban.

7. History

Bukti digital selanjutnya yang didapatkan yaitu History dari pelaku yang menampilkan beberapa riwayat pencarian atau jejak hasil kegiatan selama melakukan browsing pada aplikasi Google Chrome, Salah satu History yang didapatkan ialah berupa pencarian Google Form yang merupakan tempat pelaku membuat link phising tersebut.

8. Images

Dari proses analisis yang dilakukan ditemukan juga Images atau file gambar yang tersimpan di dalam folder aplikasi Google Chrome. yang bisa dijadikan salah satu bukti digital.

9. Timestamps

Terdapat juga Timestamps atau stempel waktu yang berupa tanggal dan waktu yang tersimpan pada saat melakukan browsing seperti mengakses sebuah situs maka tanggal dan waktu tersebut tersimpan otomatis pada aplikasi Google Chrome.

10. URL

Bukti digital selanjutnya didapatkan URL yang tersimpan didalam History Google Chrome,dimana link tersebut dikirimkan ke korban untuk melakukan tindakan kejahatan phising yang digunakan untuk mencuri akun dan data-data dari korban.

11. Search History

Bukti digital yang terakhir ditemukan Search history atau riwayat penelusuran yaitu beberapa daftar dari sebuah laman Website yang pernah dikunjungi yang tersimpan didalam Browser Google Chrome

## IV. KESIMPULAN DAN SARAN

### *1. Kesimpulan*

Berdasarkan penelitian ini yang berjudul "Analisis Forensik Web Browser Pada Perangkat Android" dapat disimpulkan bahwa :

1. Prosedur investigasi Web Browser Google Chrome pada perangkat Android menggunakan metode National Institute Of Justice (NIJ), dimulai dari tahapan persiapan, koleksi, pemeriksaan, analisis dan pelaporan. Dimana pada tahap persiapan peneliti mengidentifikasi masalah dan mengumpulkan informasi tentang masalah yang dihadapi serta mempersiapkan peralatan yang diperlukan untuk proses investigasi, kemudian Tahap koleksi merupakan tahap yang dilakukan untuk pengumpulan data yang dapat mendukung proses investigasi seperti Smartphone yang digunakan pelaku, Tahap pemeriksaan ini dilakukan proses ekstraksi data dari Smartphone yang digunakan pelaku

menggunakan tools MOBILedit Forensics Express dan dihasilkan folder hasil ekstraksi dari aplikasi Google Chrome, Kemudian tahap analisis tahapan ini merupakan proses pencarian bukti digital merupakan tools Autopsy, dan tahap pelaporan yaitu melaporkan hasil dari proses invetigasi yang dilakukan secara jelas.

2. Dari proses invetigasi barang bukti yang dilakukan terdapat beberapa bukti yang tersimpan didalam Web Browser Google Chrome yaitu Accounts, Bookmarks, Cookies, Cache, Document, E-mail, History, Images, Timestamps, Password, URL,Search History, dari beberapa bukti tersebut bisa dijadikan sebagai barang bukti di persidangan.

*2. Saran*

Dari penelitian ini, peneliti akan memberikan beberapa saran untuk penelitian selanjutnya yaitu:

1. Disarankan menggunakan metode forensik yang lain untuk melihat proses dari invetigasi yang dilakukan pada metode tersebut.
2. Disarankan untuk menggunakan aplikasi digital forensic yang lain untuk melakukan proses investigasi dan dijadikan perbandingan untuk hasil yang didapatkan.
3. Untuk penelitian selanjutnya disarankan menggunakan Smartphone dengan versi Android terbaru atau selain dari Smartphone Android yang digunakan pada penelitian ini

## DAFTAR PUSTAKA


[1] [1] Syafnidawaty, "Apa Itu Cyber Crime?," Raharja.Ac.Id, 2020. https://raharja.ac.id/2020/04/29/apa-itu-cyber-crime/ (accessed Nov. 16, 2021).

[2] [2] M. F. Sidiq and M. N. Faiz, "Review Tools Web Browser Forensics untuk Mendukung Pencarian Bukti Digital," J. Edukasi dan Penelit. Inform., vol. 5, no. 1, p. 67, 2019, doi: 10.26418/jp.v5i1.31430.

[3] [3] A. P. Kuncoro, "Pengembangan Mobile Forensics pada Aplikasi Mobile Banking Menggunakan Metode Static Forensic," 2017.

[4] [4] F. Mathilda, "Cyber Crime Dalam Sistem Hukum Indonesia Cyber Crime in Indonesia Law System," SIGMA-Mu - J. Publ. Has. Penelit. dan Gagasan Ilm. Multidisiplin, vol. 2, no. 2, pp. 34–45, 2012, [Online]. Available: https://jurnal.polban.ac.id/index.php/sigmamu/article/view/870

[5] [5] A. S. Gulo, S. Lasmadi, and K. Nawawi, "Cyber Crime dalam Bentuk Phising Berdasarkan Undang-Undang Informasi dan Transaksi Elektronik," PAMPAS J. Crim. Law, vol. 1, no. 2, pp. 68–81, 2021, doi: 10.22437/pampas.v1i2.9574.

[6] I. Riadi, A. Yudhana, and M. C. F. Putra, "Akuisisi Bukti Digital Pada Instagram Messenger Berbasis Android Menggunakan Metode National Institute Of Justice (NIJ)," J. Tek. Inform. dan Sist. Inf., vol. 4, no. 2, pp. 219–227, 2018.