Remik: Riset dan E-Jurnal Manajemen Informatika Komputer
Volume 7, Nomor 1, Januari 2023
http://doi.org/10.33395/remik.v7i1.12059
e-ISSN : 2541-1330
p-ISSN : 2541-1332

Implementasi Teknik Forensik dalam *Cybercrime* (*Carding*)

[1]*Qammaddin, [2]Sulfikar Sallu, [3]Ahmad Fathoni
[1, 2]Universitas Sembilanbelas November, [3]Universitas Islam Indonesia
[1, 2] Kolaka Sulawesi Tenggara Indonesia , [3] Yogyakarta Indonesia

*Penulis Korespondensi
Diajukan : 22/12/2022
Diterima : 06/01/2023
Dipublikasi : 06/01/2023

ABSTRAK
Cybercrime adalah istilah yang mengacu kepada aktivitas kejahatan dengan komputer atau jaringan komputer menjadi alat, sasaran atau tempat terjadinya kejahatan dunia maya antara lain adalah penipuan lelang secara online, pemalsuan cek, penipuan kartu kredit/carding, confidence fraud, penipuan identitas, pornografi anak dan sejenisnya. Tujuan penelitian agar dapat menemukan barang bukti digital yang dapat digunakan sebagai barang bukti. Metode penelitan yang digunakan adalah Pengumpulan Bukti Digital kejahatan. Hasil Barang bukti berupa carding ditemukan berupa phising email, invoice transaksi kartu kredit, percakapan IRC, log history, bookmark, Implikasi pengguna akan memiliki pemahaman yang mendalam terkait kejahatan dalam dunia maya.

Kata Kunci: *Cybercrime Carding*, Impelementasi Pencegahan Carding, Teknik Forensik.

I. PENDAHULUAN
Perkembangan teknologi informasi dan komputer (TIK) telah mengalami kemajuan yang sangat pesat, terutama sekali setelah diketemukannya teknologi yang menghubungkan antar komputer (networking) dan Internet. Namun demikian, berbagai kemajuan tersebut ternyata diikuti pula dengan berkembangnya sisi lain dari teknologi yang mengarah pada penggunaan komputer sebagai alat untuk melakukan berbagai modus kejahatan. Istilah ini kemudian dikenal dengan cybercrime. Komputer Forensik adalah (Moedjahedy, 2016) penyelidikan dan analisis komputer untuk menentukan potensi bukti legal. Berbeda dari pengertian forensik pada umumnya, komputer forensik dapat diartikan sebagai pengumpulan dan analisis data dari berbagai sumber daya komputer yang mencakup sistem komputer, jaringan komputer, jalur komunikasi, dan berbagai media penyimpanan yang layak untuk diajukan dalam sidang pengadilan.

Permasalahan yang diakibatkan oleh penggunaan komputer untuk kepentingan diatas telah mulai menimbulkan berbagai dampak negatif. Baik secara mikro yang dampaknya hanya pada tingkatan personal/perseorangan, maupun secara makro yang berdampak pada wilayah komunal, publik, serta memiliki efek domino yang luas. Untuk menangani permasalahan ini, maka di beberapa negara telah dibentuk unit khusus kepolisian yang berfungsi sebagai penindak kejahatan yang spesifik terkait dengan permasalahan *cybercrime*.

Masalahnya adalah banyaknya pengguna dalam dunia digital yang tertipu akibat tidak mengetahui informasi yang ada. Pelaku kejahatan kadang memanfaatkan data pengguna yang asli sehingga korban tidak merasakan kondisi tersebut. Pelaku kejahatan juga sering memanfaatkan keteledoran pengguna dalam menggunakan fasilitas jaringan dunia maya. Penelitian ini dilakukan untuk memberikan informasi yang positif kepada pengguna yang sering menggunakan teknologi dalam dunia maya untuk melakukan transaksi keuangan menggunakan kartu. Masalah yang akan dipecahkan adalah meminimalisasi kerugian yang ditimbulkan oleh penggunaan kartu oleh pelaku kejahatan dari pengguna komputer dalam dunia maya yang tidak mengetahui prosedur tersebut.

e-ISSN : 2541-1330
p-ISSN : 2541-1332

Mengapa Penting untuk dibahas karena Komputer forensik merupakan aktivitas yang berhubungan dengan pemeliharaan, identifikasi, pengambilan/penyaringan, dan dokumentasi bukti komputer dalam kejahatan komputer. komputer forensik juga merupakan kombinasi ilmu hukum dan pengetahuan komputer dalam mengumpulkan dan menganalisis data dari sistem komputer. Dalam suatu kasus hukum merupakan tugas ahli komputer forensik untuk menegakkan hukum dengan mengamankan barang bukti, rekonstruksi kejahatan, dan menjamin jika bukti yang dikumpulkan itu berguna di persidangan.

Cara mengatasi masalah dengan menganalisis kasus cybercrime dengan studi kasus berupa carding. Alasan Penelitian dilakukan karena di Indonesia ahlinya masih sangat jarang karena mungkin tidak terlalu banyak pakar teknologi informasi yang aware di bidang ini. Penelitian ber kontribusi dalam mengisi kesenjangan yang ada dengan memberikan konsep digital pada pengguna perangkat elektronik agar dapat mengetahui ciri dan karakter pelaku kejahatan digital, serta dapat terhindar dari berbagai penipun yang ada di dunia maya.

Metode Yang Akan digunakan Pengumpulan Bukti Digital kejahatan dengan memanfaaatkan seluruh data digital sebagai jejak pelaku kejahatan.

State of the art berbagai kasus yang ada diselesaikan dengan prosedur forensik sampai ke tahapan menjadi barang bukti yang sah.

Inovasi yang diusulkan menyelesaikan kasus cybercrime khususnya carding dengan teknik komputer forensik agar nantinya barang bukti dapat diterima sebagai barang bukti yang sah di pengadilan. Penelitian ini hanya menganalisis kasus cybercrime dengan studi carding, sebab di Indonesia sudah mulai menggunakan fasilitas kartu dalam transaksi di dunia maya

Tujuan mendalam agar dapat menemukan barang bukti digital yang dapat digunakan sebagai barang buktidengan menganalisis kasus cybercrime khususnya carding sesuai prosedur komputer forensik. Metode penelitan yang digunakan adalah Pengumpulan Bukti Digital kejahatan yang terjadi dalam dunia maya, dengan mengumpulkan jejak data digital yang dilakukan pelaku kejahatan terhadap korban.

Kemajuan teknologi dan informasi saat ini tidak hanya berdampak positif untuk kemajuan serta perkembangan peradaban manusia. Namun perkembangan pesat teknologi itu sendiri juga terlihat memiliki pengaruh negatif. Berbagai permasalahan yang timbul seiring perkembangan teknologi informasi dan komunikasi salah satunya adalah tindak kejahatan cybercrime.

II. STUDI LITERATUR

Tindak kejahatan komputer dan dunia maya yang terjadi saat ini semakin banyak jenisnya. Banyaknya tindak kejahatan dunia maya menyebabkan perlunya peranan seorang ahli dalam menyelesaikan tiap permasalahan yang ada. Dengan demikian topik penelitian ini menjadi sangat penting sebagai upaya untuk memperkenalkan kepada masyarakat ilmiah komputer di Indonesia prosedurprosedur untuk meyelesaikan tiap kasus kejahatan tersebut. Sejumlah peneliti sudah mengangkat isu-isu tersebut secara umum. (Das & Nayak, 2013) (UNESCO., 2022) membahas latar belakang serta metodologi yang digunakan dalam komputer forensik dan cara penggunaan beberapa tools komputer forensik terkait kejahatan dunia maya. Sementara (Madiyanto et al., 2017) (MUKTI, 2017) membahas tentang gambaran singkat terkait pengertian, metode dan implementasi proses forensik menggunakan sejumlah aplikasi yang tersedia.

Dari sisi keamanan dan pencegahan tindak kejahatan dunia maya, (Shoukat et. al., 2018) (Suleiman et al., 2020) Memberikan gambaran bagaimana komputer forensik cocok sebagai elemen strategis dalam keamanan komputer secara keseluruhan organisasi. Sementara (Yar, 2012) (Manap et al., 2015) Membahas perkembangan identity teft yang merupakan bagian dari cybercrime dan cara memproteksi diri dan mencegah terjadinya tindakan tersebut. Untuk kalangan peneliti yang ada di Indonesia saat ini, isu-isu tentang komputer forensik yang dibahas secara khusus tampaknya belum terlalu banyak disentuh. Untuk itulah maka penelitian ini diajukan untuk mengangkat isu-isu seputar komputer forensic yang penangananya dilakukan secara khusus.

Cybercrime merupakan suatu tidakan kriminal yang dilakukan dengan

Remik: Riset dan E-Jurnal Manajemen Informatika Komputer
Volume 7, Nomor 1, Januari 2023
http://doi.org/10.33395/remik.v7i1.12059
e-ISSN : 2541-1330
p-ISSN : 2541-1332

menggunakan teknologi komputer sebagai alat kejahatan utama dan memanfaatkan perkembangan teknologi komputer khususnya Internet. Cybercrime didefinisikan sebagai perbuatan melanggar hukum yang memanfaatkan teknologi komputer yang berbasis pada kecanggihan perkembangan teknologi Internet (Deora & Chudasama, 2021) (Kadir et al., 2019)

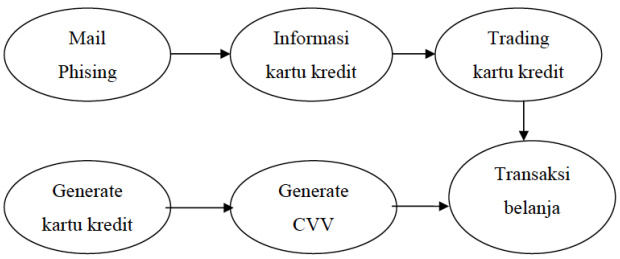
Cybercime sendiri memiliki beberapa karakteristik berdasarkan tindakan, sifat dan ruang lingkup kejahatannya. Berbeda dengan kejahatan lainnya, cybercrime dikelompokkan sesuai dengan karakteristik dari masing-masing kejahatannya. Dalam perkembangan kejahatan konvensional cybercrime dikenal dengan (Adoc.pub, 2020):

1. Kejahatan kerah biru
2. Kejahatan kerah putih

Semakin berkembang suatu teknologi komunikasi maka semakin meningkat pula tingkat kejahatan di dalamnya. Perkembangan dunia teknologi komunikasi dan Internet menyebabkan semakin banyak orang yang terkoneksi dengan Internet sehingga menimbulkan peluang munculnya berbagai jenis kejahatan komputer dengan beragam variasi kejahatannya. Dalam hal ini menurut Drs. Rusbagio Ishak (Kombes Pol/49120373), terdapat beberapa tendensi dari munculnya berbagai gejala kejahatan komputer :

1. Permasalahan finansial
   Cybercrime dapat menjadi alternatif baru untuk mendapatkan uang. Perilaku carding (penggunaan hak atas kartu kredit yang dilakukan tanpa seijin pihak yang sebenarnya mempunyai hak), melakuakan pengalihan rekening telepon dan fasilitas lainnya, adalah sebagian bentuk cybercrime dengan tendensi finansial.
2. Permasalahan terkait politik, militer dan sentimen nasionalisme
   Teknologi tingkat tinggi yang dimiliki oleh suatu negara pada umumnya menjadi lahan yang menarik bagi tiap negara untuk dijadikan ajang kompetisi dalam mengembangkan peralatan tempurnya, sehingga antar suatu negara terjadi persaingan yang dapat menyebabkan terjadinya tindak cybercrime yang digunakan untuk mendapatkan akses informasi antar negara pesaing.
3. Faktor kepuasan pelaku
   Pada tendensi ini terdapat masalah psikologis dari pelakunya. Dimana ada kecenderungan bahwa seseorang dengan kemampuan yang tinggi akan selalu merasa tertantang untuk menerobos berbagai sistem keamanan yang ketat. Dalam hal ini kepuasan batin menjadi orientasi utama bagi pelaku dibandingkan dengan tujuan finansial ataupun sifat sentimen.

Biasanya pelaku yang melakukan secara individual menggunakan tools (*card extrapolator*). Sedangkan yang dilakukan secara berkelompok biasanya bekerjasama dengan suatu usaha tertentu yang menggunakan kartu kredit dalam pembayarannya. Dimana pelaku menyimpan hasil inputan dari kartu kredit ke tempat penampungan lain secara ilegal. Adapun bentuk gambaran skenario carding pada kasus ini dapat dilihat pada gambar.1



Gambar 1. Gambaran Umum Skenario Kasus yang terjadi.

Dari gambaran skenario kasus di atas dapat dilihat urutan langkah kejahatan carding. Dalam skenario kasus ini detail tindakan pelaku carding dapat dilihat sebagai berikut:

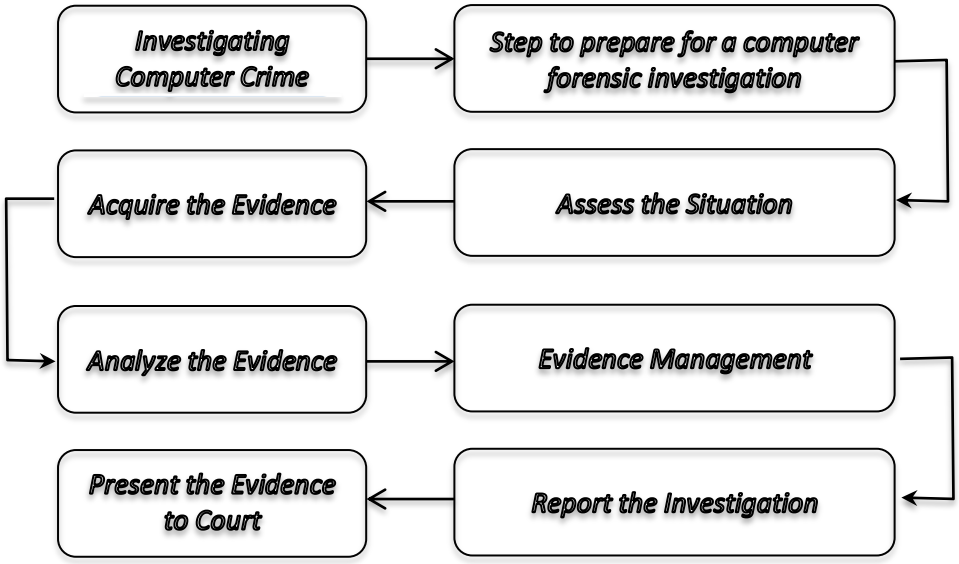
a) Pelaku carding menyebarkan mail phising untuk mendapatkan informasi kartu kredit dari pengguna layanan tersebut.
b) Pelaku juga menggunakan aplikasi *Credit Wizard* untuk mengenerate nomer kartu kedit.

Remik: Riset dan E-Jurnal Manajemen Informatika Komputer
Volume 7, Nomor 1, Januari 2023
http://doi.org/10.33395/remik.v7i1.12059
e-ISSN : 2541-1330
p-ISSN : 2541-1332

c) Dari nomer kartu kredit yang telah didapat dari hasil generate, pelaku kemudian menggunakan aplikasi IRC untuk mendapatkan CVV dari nomer kartu kredit tersebut.
d) Pelaku melakukan transaksi mejual kartu kredit yang telah didapat melalui iRC.
e) Setelah memiliki informasi kartu kredit pelaku menggunakannya secara pribadi untuk belanja online membeli buku di *amazon.com* dengan menggunakan *web browser Mozilla* Firefox.
f) Setelah transaksi terjadi pelaku mendapatkan email notifikasi dari amazon.com dan kemudian pelaku menyimpan invoice transaksi pada laptop.

III. METODE

Meningkatnya populasi orang yang terkoneksi dengan Internet akan menjadi peluang bagi munculnya kejahatan komputer dengan beragam variasi kejahatannya. Di antara sebagian besar kasus yang terjadi terdapat kasus yang memiliki tendensi berupa permasalahan finansial dan kepuasan. Perilaku carding merupakan suatu tindakan yang termotivasi terhadap masalah finansial, dimana pelaku menggunakan kemampuannya untuk mengakses secara ilegal terhadap kartu kredit orang lain untuk digunakan secara pribadi. Kasus carding dapat dilakukan secara individual maupun berkelompok.



Gambar 1 Prosedur Komputer Forensik (Hacker, 2022)

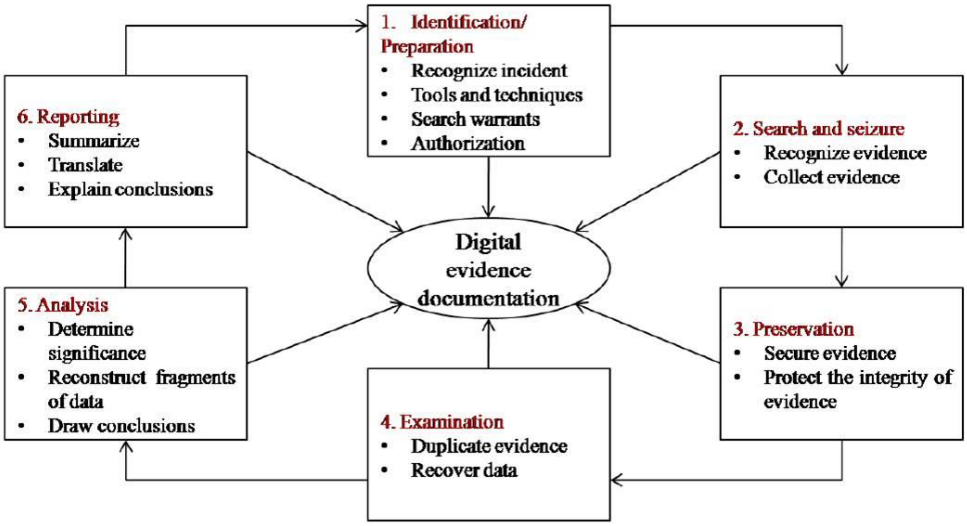
Penjelasasan:

1. *Investigating* computer crime adalah proses yang dilakukan dalam rangka Menyelidiki kejahatan komputer yang dapat dilakukan oleh user secara langsung maupun robot yang juga dibuat oleh user. Pada bagian ini komputer akan merekam seluruh rekam jejak digital yang terjadi. Hal ini biasa dilakukan oleh Penyidik Forensik Digital yaitu seseorang yang memiliki keinginan untuk mengikuti bukti dan memecahkan kejahatan secara virtual
2. *Steps to prepare for a computer forensic isvestigation* adalah proses atau langkah-langkah untuk mempersiapkan penyelidikan forensik komputer, pada bagian ini terdapat 5 langkah yang dilakukan: (Norwich University Online, 2017)
   a. Pengembangan Kebijakan dan Prosedur
   b. Penilaian Bukti
   c. Evidence Examination
   d. Pendokumentasian dan
   e. Pelaporan
3. *Asses the situation* adalah proses dalam Menilai situasi baik fisik maupun digital.
4. *Acquire the evidence* adalah proses lanjutan dari langkah sebelumnya untuk mendapatkan barang bukti, barang bukti tersebut berupa rekam jejak digital yang berhasil ditelusuri

Remik: Riset dan E-Jurnal Manajemen Informatika Komputer
Volume 7, Nomor 1, Januari 2023
http://doi.org/10.33395/remik.v7i1.12059
e-ISSN : 2541-1330
p-ISSN : 2541-1332

berdasarkan kondisi yang ada.

5. *Analyze the evidence* adalah proses lanjutan yang telah memperoleh barang bukti tahap ini merupakan bagian yang sangat penting yaitu Analisis bukti adalah proses yang memberikan kesempatan untuk mengontekstualisasikan dan menjelaskan bukti bagi raring lain. Analisis data mungkin memberi tahu orang mengapa bukti itu penting, apa artinya, atau bagaimana kaitannya dengan gagasan lain.(Team, 2022)
6. *Evidence Management* adalah proses kelanjutan dari analisis bukti, tahap ini merupakan tahapan dalam manajemen bukti yang akan mendeskripsikan seluruh bukti yang ada dan dikaitkan dengan bukti lain yang sesuai masalah. Bukti sangat penting dalam setiap kasus peradilan pidana, termasuk untuk tindakan teroris. Bukti dapat berupa lisan (pernyataan saksi), fisik (sidik jari atau pecahan peluru) atau elektronik (email dan pesan teks). Mengidentifikasi, mengumpulkan, mendokumentasikan, melestarikan, dan menyajikan jenis bukti yang berbeda ini dengan benar seringkali sulit dan menantang.(Nations, 2022)
7. *Report the Investigation* adalah tahapan yang memberikan laporan investigasi dari pekerjaan yang dilakukan.
8. *Present the Evidence to Court* merupakan tahap yang akan menyampaikan Bukti ke Pengadilan.



Gambar 2. Metodologi Komputer Forensik (*Beginners*, 2022)

Proses forensik digital ditunjukkan pada gambar berikut. Fase siklus hidup forensik adalah:
1. Persiapan dan identifikasi
2. Pengumpulan dan pencatatan
3. Menyimpan dan mengangkut
4. Pemeriksaan/penyidikan
5. Analisis, interpretasi, dan atribusi
6. Pelaporan
7. Bersaksi

Penjelasan.

1. Mempersiapkan Bukti dan Mengidentifikasi Bukti (Steegh, 2020) (Griffith, 2017)
   Untuk diproses dan dianalisis, bukti harus diidentifikasi terlebih dahulu. Ada kemungkinan bahwa bukti dapat diabaikan dan tidak diidentifikasi sama sekali. Urutan peristiwa di komputer mungkin termasuk interaksi antara:
   a. File yang berbeda
   b. File dan sistem file
   c. Proses dan file
   d. File log

   Dalam kasus jaringan, interaksi dapat terjadi antar perangkat dalam organisasi atau di

e-ISSN : 2541-1330
p-ISSN : 2541-1332

seluruh dunia (Internet). Jika bukti tidak pernah diidentifikasi relevan, mungkin tidak akan pernah dikumpulkan dan diproses.

2. Mengumpulkan dan Merekam Bukti Digital (Varol & Ülgen Sönmez, 2017) (*US Deputy Attorney General Eric H Holder Jr, 2000 Research by National Hitch Crime Unit (NHTCU), UK*, 1998)

   Bukti digital dapat dikumpulkan dari banyak sumber. Sumber yang jelas dapat berupa:

   Telepon genggam
   Kamera digital
   Hard drive
   CD
   perangkat memori USB

   Sumber yang tidak jelas dapat berupa:

   Pengaturan termometer digital
   Kotak hitam di dalam mobil
   RFID

   Perawatan yang tepat harus dilakukan saat menangani bukti digital karena dapat diubah dengan mudah. Setelah diubah, bukti tidak dapat dianalisis lebih lanjut. Hash kriptografi dapat dihitung untuk file bukti dan kemudian diperiksa apakah ada perubahan yang dilakukan pada file atau tidak. Terkadang bukti penting mungkin berada dalam memori yang mudah menguap. Mengumpulkan data volatil memerlukan keterampilan teknis khusus

3. Menyimpan dan Mengangkut Bukti Digital (Singh et al., 2022) (A Project Presented to the School of Science & Technology, 2014)

   Beberapa panduan penanganan barang bukti digital:

   a. Gambar media komputer menggunakan alat pemblokiran tulis untuk memastikan bahwa tidak ada data yang ditambahkan ke perangkat yang dicurigai
   b. Tetapkan dan pertahankan lacak balak
   c. Dokumentasikan semua yang telah dilakukan
   d. Hanya gunakan alat dan metode yang telah diuji dan dievaluasi untuk memvalidasi keakuratan dan keandalannya

   Harus berhati-hati agar bukti tidak pergi ke mana pun tanpa dilacak dengan benar. Hal-hal yang bisa salah dalam penyimpanan meliputi:

   Kadaluarsa dari waktu ke waktu (alami atau tidak alami)
   Perubahan lingkungan (langsung atau tidak langsung)
   Kebakaran
   Banjir
   Kehilangan daya ke baterai dan mekanisme pengawetan media lainnya

   Terkadang bukti harus dipindahkan dari satu tempat ke tempat lain baik secara fisik maupun melalui jaringan. Perhatian harus diambil bahwa bukti tidak berubah saat dalam perjalanan. Analisis umumnya dilakukan pada salinan bukti nyata. Jika ada perselisihan tentang salinannya, yang asli dapat diajukan ke pengadilan

4. Meneliti/Menyelidiki Bukti Digital (Horsman & Sunde, 2022) (Horsman & Sunde, 2022)

   Spesialis forensik harus memastikan bahwa dia memiliki otoritas hukum yang tepat untuk menyita, menyalin, dan memeriksa data. Sebagai aturan umum, seseorang tidak boleh memeriksa informasi digital kecuali seseorang memiliki kewenangan hukum untuk melakukannya. Investigasi forensik yang dilakukan pada data saat istirahat (hard disk) disebut analisis mati. Banyak serangan saat ini tidak meninggalkan jejak pada hard drive komputer. Penyerang hanya mengeksploitasi informasi di memori utama komputer. Melakukan investigasi forensik pada memori utama disebut analisis langsung. Terkadang kunci dekripsi mungkin hanya tersedia di RAM. Mematikan sistem akan menghapus kunci dekripsi. Proses pembuatan dan penggandaan yang tepat dari bukti asli disebut pencitraan. Beberapa alat yang dapat membuat seluruh gambar hard drive adalah:

   a. DCFLdd
   b. Iximager
   c. Guymager

   Drive asli dipindahkan ke penyimpanan aman untuk mencegah gangguan. Proses pencitraan diverifikasi dengan menggunakan SHA-1 atau algoritme hashing lainnya.

5. Analisis, Interpretasi dan Atribusi (Grigaliunas & Toldinas, 2020) (Hauger, 2018)

e-ISSN : 2541-1330
p-ISSN : 2541-1332

Dalam forensik digital, hanya beberapa urutan peristiwa yang dapat menghasilkan bukti. Tetapi kemungkinan jumlah urutannya sangat besar. Bukti digital harus dianalisis untuk menentukan jenis informasi yang tersimpan di dalamnya. Contoh alat forensik:

a. Forensics Tool Kit (FTK)
b. EnCase
c. Scalpel (file carving tool)
d. The Sleuth Kit (TSK)
e. *Autopsy*

Analisis forensik mencakup kegiatan berikut:

a. Tinjauan manual data di media
b. Inspeksi registri Windows
c. Menemukan dan memecahkan kata sandi
d. Melakukan pencarian kata kunci yang berhubungan dengan kejahatan
e. Mengekstrak email dan gambar

Jenis analisis digital:

a. Analisis media
b. Analisis manajemen media
c. Analisis sistem file
d. Analisis aplikasi
e. Analisis jaringan
f. Analisis gambar
g. Analisis video

6. Pelaporan (Zjalic, 2020) (Presiding et al., 2022)

Setelah analisis selesai, laporan dihasilkan. Laporan tersebut dapat dalam bentuk lisan atau dalam bentuk tertulis atau keduanya. Laporan tersebut berisi semua detail tentang bukti dalam langkah analisis, interpretasi, dan atribusi. Sebagai hasil dari temuan-temuan dalam fase ini, tuduhan-tuduhan tersebut harus dapat dikonfirmasi atau dibuang. Beberapa elemen umum dalam laporan adalah:

a. Identitas lembaga pelapor
b. Pengidentifikasi kasus atau nomor pengiriman
c. Penyidik kasus
d. Identitas pengirim
e. Tanggal penerimaan
f. Tanggal laporan
g. Daftar deskriptif barang yang diserahkan untuk pemeriksaan
h. Identitas dan tanda tangan pemeriksa
i. Deskripsi singkat tentang langkah-langkah yang diambil selama pemeriksaan
j. Hasil/kesimpulan

7. Saksi

Tahap ini melibatkan presentasi dan pemeriksaan silang saksi ahli. Saksi ahli dapat memberikan keterangan berupa:

a. Kesaksian didasarkan pada fakta atau data yang cukup
b. Kesaksian adalah produk dari prinsip dan metode yang dapat diandalkan
c. Saksi telah menerapkan prinsip dan metode secara handal terhadap fakta-fakta perkara

Para ahli dengan pengetahuan yang tidak memadai terkadang dihukum oleh pengadilan. Tindakan pencegahan yang harus diambil saat mengumpulkan bukti digital adalah:

a. Tidak ada tindakan yang diambil oleh lembaga penegak hukum atau agen mereka yang dapat mengubah bukti
b. Ketika seseorang mengakses data asli yang disimpan di komputer, orang tersebut harus kompeten untuk melakukannya
c. Uji coba audit atau catatan lain dari semua proses yang diterapkan pada bukti digital harus dibuat dan disimpan

Remik: Riset dan E-Jurnal Manajemen Informatika Komputer
Volume 7, Nomor 1, Januari 2023
http://doi.org/10.33395/remik.v7i1.12059
e-ISSN : 2541-1330
p-ISSN : 2541-1332

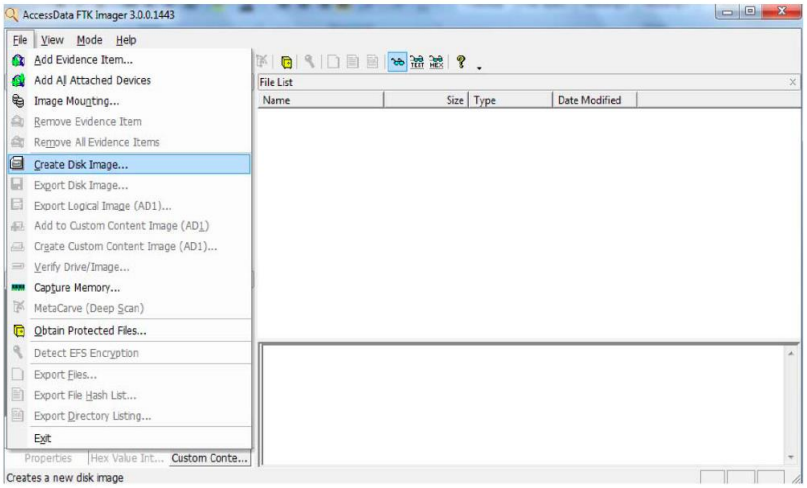
Penanggung jawab penyelidikan memiliki tanggung jawab keseluruhan untuk memastikan bahwa hukum dan ini dipatuhi

IV. HASIL DAN PEMBAHASAN

Perekaman Barang Bukti, dalam contoh kasus yang telah dibuat terdapat beberapa barang bukti yang dapat diimaging. Pada tahapan ini akan dilakukan imaging terhadap barang bukti yang telah ditemukan yaitu berupa sebuah komputer dan flashdisk. Untuk melakukan imaging maka akan digunakan FTK imager dan FTK untuk membuat image hardisk. Menggunakan FTK Imager adapun langkah – langkah pada FTK

Imager adalah sebagai berikut :

a. Setelah installasi FTK imager selesai, maka akan keluar tampilan awal FTK imager kemudian klik file > *Create Disk Image* > *Next*. Pada kasus ini akan dibuat image baru agar bisa dilakukan pengujian datmenggunakan FTK.

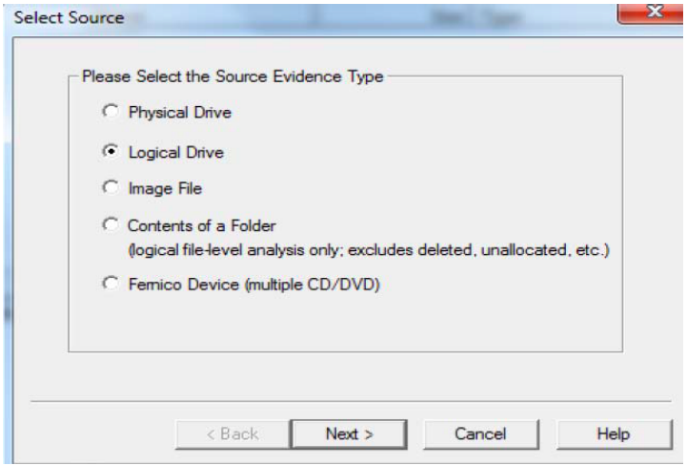


Gambar 3. Membuat *Disk Image*

b. Kemudian akan tampil halaman select source. Halaman ini dapat memilih untuk melakukan image terhadap type apa, pada kasus ini akan dipilih logical drive agar lebih mempermudah melakukan pengecekan pada setiap drive nya dan waktu yang dibutuhkan relatif lebih singkat. Untuk proses pemilihan source terlihat pada gambar 4 Ada beberapa pilihan source evidence type yaitu :

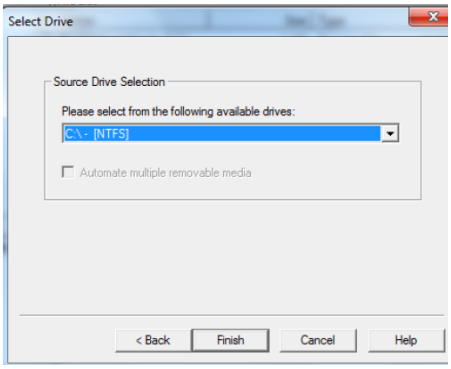
- *Physical Drive*, digunakan untuk membuat image disk secara keseluruhan.
- *Logical drive*, digunakan untuk membuat image partisi yang ingin dianalisis.
- *Image File*, digunakan untuk mengkonversi image.
- *Content of a folder*, untuk memilih file atau folder tertentu dan hanya untuk kebutuhan analisis saja.
- *fernico device*, digunakan untuk mengimage cd / dvd.

Remik: Riset dan E-Jurnal Manajemen Informatika Komputer
Volume 7, Nomor 1, Januari 2023
http://doi.org/10.33395/remik.v7i1.12059
e-ISSN : 2541-1330
p-ISSN : 2541-1332



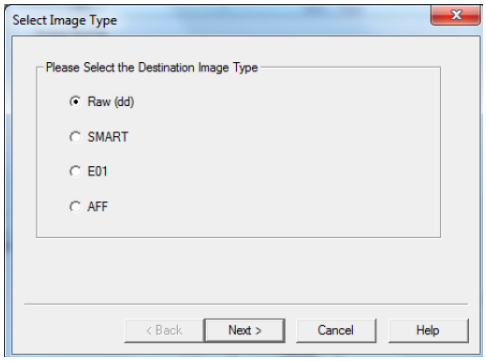
Gambar 4. Select Source

c. Selanjutnya pilih *drive* mana yang akan di *image* terlebih dahulu, misalnya memilih C :\[NTFS], yaitu local disk dari sistem operasi. Klik finish untuk mengakhiri. Proses Select Drive terlihat pada gambar 5 dibawah ini:



Gambar 5. *Select Drive*

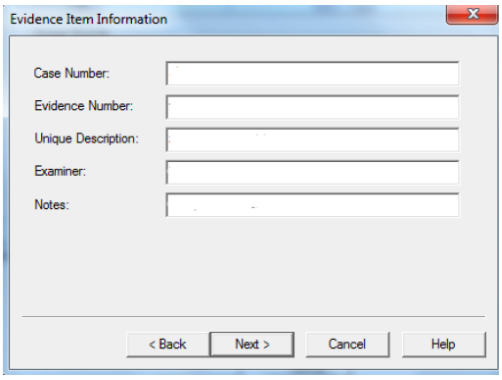
d. Selanjutnya akan diminta untuk menentukan image destination atau dimana *disk image* nya akan disimpan, klik add sehingga kemudian akan tampil halaman *select image type*, dan klik *next* untuk melanjutkan, untuk lebih jelasna dapat dilihat pada gambar 6 *Select Image Type*. Ada beberapa tipe image diantaranya :
   a. *Raw* (dd), merupakan data mentah atau yang belum diolah sama sekali.
   b. SMART
   c. E01
   d. AFF



Gambar 6. Select Image Type

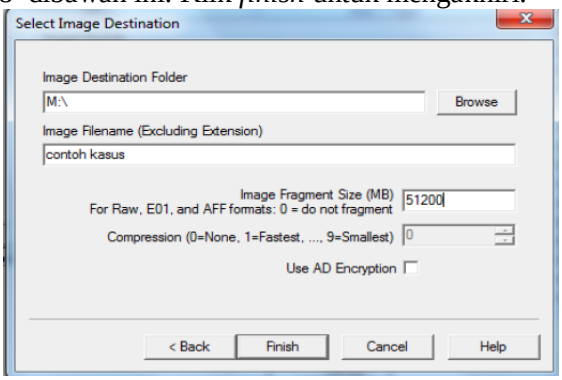
e. Selanjutnya akan diminta untuk mengisi informasi barang bukti, halaman ini digunakan untuk membuat nama file serta informasi mengenai barang bukti yang akan dibuat. Klik next untuk melanjutkan. Hal ini digambarkan pada gambar 7 berikut ini.

Remik: Riset dan E-Jurnal Manajemen Informatika Komputer
Volume 7, Nomor 1, Januari 2023
http://doi.org/10.33395/remik.v7i1.12059
e-ISSN : 2541-1330
p-ISSN : 2541-1332



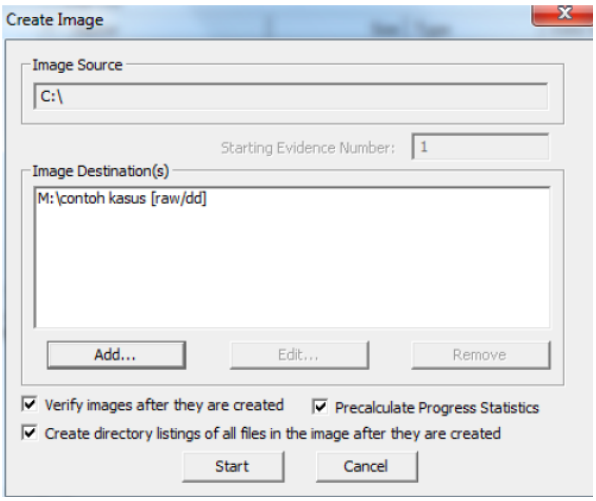
Gambar 7 *Evidence Item Information*

f. Selanjutnya akan diminta untuk menentukan dimana *image* akan disimpan, nama file image dan *image fragment size* atau ukuran *drive* yang akan di i*mage*. Seperti yang terlihat pada gambar 8 dibawah ini. Klik *finish* untuk mengakhiri.



Gambar 8. Select Image Destination

g. Setelah penambahan *image destination* selesai maka akan tampil halaman *Create Image* seperti pada gambar 9 berikut ini. Klik *Star*t untuk memulai proses imaging data dan *cancel* untuk membatalkan.



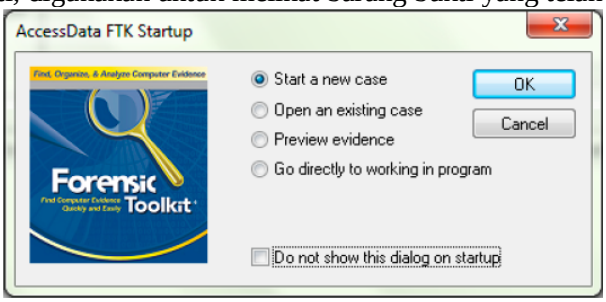
Gambar 9. *Create Image*

Setelah melalui tahapan imaging selanjutnya barang bukti yang telah dibuat image nya akan dianalisis dengan menggunakan *Forensic Toolkit*. Dalam kasus ini, *Forensic Toolkit* berperan untuk menemukan bukti yang mencakup dokumen, email dan baganbagan dari file sistem membuka program sebagai administrator (klik kanan dan pilih Run as Administrator), maka akan muncul beberapa opsi diantaranya :

a. *Start new case*, digunakan untuk membuat case baru dari image file yang ada.

Remik: Riset dan E-Jurnal Manajemen Informatika Komputer
Volume 7, Nomor 1, Januari 2023
http://doi.org/10.33395/remik.v7i1.12059
e-ISSN : 2541-1330
p-ISSN : 2541-1332

b. *Open an existing case*, digunakan untuk membuka kasus yang telah dibuat sebelumnya.
c. *Preview* barang bukti, digunakan untuk melihat barang bukti yang telah dibuat.



Gambar 10. *FTK startup*

Tampilan awal analisa dengan aplikasi RTK, pilih Start new case untuk dapat membuat kasus baru dari *image* yang telah dibuat.

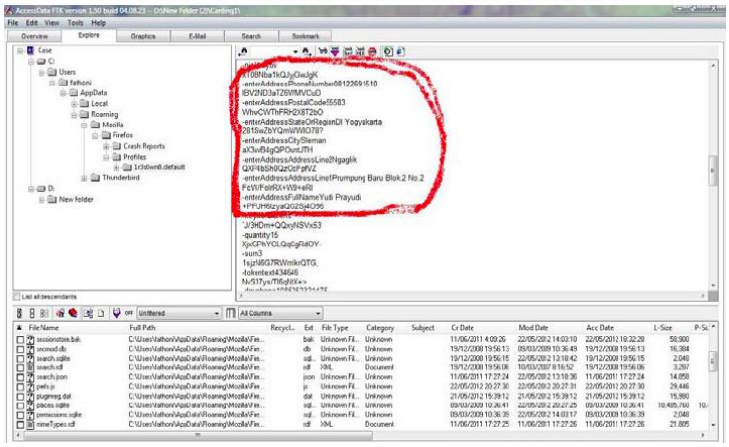
a. Ketika akan membuat case baru, maka akan tampil halaman *new case*, pada halaman ini akan diminta untuk mengisi informasi yang berkaitan dengan kasus ini, misal nama penyidik, nama kasus yang akan diselidiki, atribut-atribut lainnya mengenai kasus serta menentukan tempat yang akan menjadi folder penyimpanan kasus dan segala aktivitas yang berkaitan dengan penyidikan. Untuk informasi dalam penulisan laporan penyidikan FTK juga menyediakan form mengenai informasi penyidik.
b. Selama masa penyidikan yang menggunakan FTK, FTK akan membuat file bernama *ftk.log* yang akan mencatat aktivitas pada case. Dari *log* ini bisa menentukan *event* apa saja yang akan dicatat dengan member tanda check pada opsi yang sudah tertera.
c. Selanjutnya akan menentukan *option* untuk pemrosesan barang bukti, pilihlah proses yang relevan dengan barang bukti yang akan ditambah ke *case*. Contoh : jika *case* terutama memuat gambar maka tidak perlu melakukan index pada barang bukti, sedangkan bila kasus tidak memuat gambar maka tidak perlu menyimpan *thumbnail*.
d. *Refine case* memungkinkan untuk mengeliminate sejumlah data yang tidak terkait dari *case.* Tujuannya untuk menghemat waktu dan sumber data.
e. *refine index* membantu menentukan tipe data yang tidak ingin diindeks. *Index file* dibuat setelah pembuatan suatu case, tetapi pembuatan suatu bagian dari barang bukti bisa diindex kapan saja.
f. tampilan *window Add Evidence*. Pada halaman ini dapat menambah, mengurangi, mengelola informasi, serta parameter dari barang bukti. Adapun barang bukti yang dimaksud adalah barang bukti yang berhubungan dengan kasus (case).
g. Pilih file *image* yang ingin dicek atau diuji, kemudian perlu ditambahkan informasi mengenai barang bukti tersebut, seperti *evidence display name, evidence identification name/number* serta *comment*.
h. FTK akan memulai melakukan pengumpulan data dari file image agar bisa dibaca atau diuji mengenai case summary.

Selanjutnya akan dilakukan analisis forensik terhadap data-data yang telah di ekstract. Dengan analisis tersebut diharapkan dapat menemukan file-file yang berkaitan dengan kasus. Untuk menemukan barang bukti dari kasus yang sedang diselidiki seorang penyidik haruslah memahami konsep bukti yang dicari serta jenis dan tipe dari kejahatan yang sedang diselidiki. Untuk skenario kasus yang dibuat pada penelitian ini penyidikan berfokus untuk mencari barang bukti yang terkait berupa *Document, Email, Deleted Files, Data base, Other Thumbnail, Folder, Log History, Log* jaringan serta aplikasi yang

Remik: Riset dan E-Jurnal Manajemen Informatika Komputer
Volume 7, Nomor 1, Januari 2023
http://doi.org/10.33395/remik.v7i1.12059
e-ISSN : 2541-1330
p-ISSN : 2541-1332

mungkin digunakan oleh pelaku. Pada tahapan ini akan dimulai dari pencarian berupa *log history* pada *web browser* yang dilakukan oleh pelaku menggunakan komputernya. Log history *web browser* dapat ditemukan pada drive tertentu tempat instalasi aplikasi tersebut. *Web browser* yang sering digunakan antara lain google chrome dan mozilla *firefox*, pada *chrome log history*, *cache* dan *bookmar*k dapat ditemukan pada bagian direktori C:\Users\fathoni\AppData\Local\Google\Chrome\User Data\Default. Sedangkan pada mozilla firefox data-data yang berisi log history, bookmark dan cache dapat ditemukan pada direktori C:\Users\fathoni\AppData\Roaming\Mozilla\Firefox\Profiles\1r3s0wn8.default.

Dari Temuan sebelumnya yang berupa History dari web browser selanjutnya akan dilakukan pencarian informasi dari web browser tersebut. Pada kasus ini ditemukan beberapa inputan yang dilakukan oleh pelaku berupa session web browser yang terdapat pada direktori C:\Users\fathoni\AppData\Roaming\Mozilla\Firefox\Profiles\Ir3s0wn8.def ault\Sessionstore.bak. hasil temuan dapat dilihat pada gambar dibawah ini.



Gambar 11. Tampilan *Session*

Setelah mendapatkan data-data dan informasi dari *web browser* pelaku, selanjutnya akan diselidiki bagian yang memuat informasi berupa *E-mail*. Untuk melakukan pencarian berupa *E-mail* agar lebih mudah dapat dilakukan pencarian menggunakan tab E-mail. Pada tab *E-mail* dapat menemukan semua pesan masuk maupun keluar. Dari sini penyidik dapat melihat siapa pengirim email, siapa yang menerima email, kapan email tersebut dikirim serta header lengkap dari email tersebut. Pada kasus ini ditemukan bukti berupa email invoice hasil transaksi pelaku dan email yang digunakan pelaku untuk mendapatkan kartu kredit berupa *email phising*.

Penyidik dapat melakukan pencarian informasi berupa gambar. Untuk memudahkan pencarian maka terdapat tombol *Graphic* dan *Other Thumbnail*. Pada tombol tersebut penyidik dapat menemukan filefile yang telah disortir berupa image yang berekstensi jpeg, gif, png dan sebagainya. Pada kasus ini ditemukan screen shot hasil generate cvv yang dilakukan oleh pelaku menggunakan aplikasi *FNG AIO Geerator*.

Untuk menemukan file-file lain yang sulit dilihat di halaman *Overview* penyidik dapat mencoba untuk mencarinya pada *tab explore*. Pada halaman ini penyidik dapat melihat direktori pada barang bukti. Untuk mencari dokumen-dokumen terkait seperti *history*, *bookmark*, *cookies* dan sebagainya dapat dilakukan dengan mudah dengan cara mengakses direktori *Web Browser* yang digunakan pelaku. Dari sana dapat ditemukan situs apa saja yang pernah dikunjungi dan yang di bookmark oleh pelaku. Dari situ dapat dicari hal-hal terkait kasus misal, halaman situs jual beli *onlin*e yang diakses pelaku untuk menggunakan kartu kredit yang ia punya. Atau situs phising yang digunakan pelaku untuk mendapatkan informasi kartu kredit, serta dokumen yang tersimpan pada direktori pridadi pelaku.

Remik: Riset dan E-Jurnal Manajemen Informatika Komputer
Volume 7, Nomor 1, Januari 2023
http://doi.org/10.33395/remik.v7i1.12059
e-ISSN : 2541-1330
p-ISSN : 2541-1332

Untuk menemukan informasi berupa log percakapan yang dilakukan menggunakan IRC penyidik dapat melakukan pencarian pada direktori tempat instalasi aplikasi yang digunakan untuk melakukan *Relay Chatting* seperti aplikasi mIRC. Pada kasus ini ditemukan hasil percakapan pelaku berupa transaksi jual beli kartu kredit dan hasil generate CVV menggunakan mIRC. Hasil temuan terdapat pada direktori D:\New Folder\mIRC\log.

Setelah melakukan analisis dan pengecekan pada barang bukti yang telah ditemukan dan telah didapatkan hasil maka penyidik harus membuat laporan untuk kepentingan penyidikan di pengadilan. Laporan berisi rangkuman dari hasil investigasi, menyebutkan barang bukti secara spesifik dan pembuktiannya, dan kesimpulan yang jelas dan tidak bersifat ambigu.

Contoh Hasil

REPORT OF MEDIA ANALYSIS
MEMORANDUM FOR : Kepala Polisi
Investigator Fathoni
Jakal Street
SUBJECT : XYZ Forensics Analysis Report
SUBJECT : Lukman
Case Number : 001
1. Status : Closed
2. Summary of Finding :
• Ditemukan 1 file spreadsheet berisi daftar kartu kredit dan status jual beli.
• Ditemukan aplikasi card extrapolator.
• Ditemukan e-mail transaksi jual beli kartu kredit.
• Ditemukan ScreenShot Invoice yang diduga merupakan hasil dari transaksi pembelian online menggunakan kartu kredit.
• Ditemukan history dan bookmark situs phising yang digunakan untuk mendapatkan informasi kartu kredit.
• Ditemukan Log IRC berupa percakapan transaksi dan generate cvv.
3. Item Analyzed :
TAG NUMBER ITEM DESCRIPTION
012345 Sebuah Laptop
4. Details of Findings :
...

Kasus yang telah dibuat akan dipresentasikan teknik dan temuan ap saja yang telah didapatkan selama proses investigasi.

Teknik :
• Pelaku melakukan aktivitas penipuan untuk mendapatkan kartu kredit melalui IRC
• Pelaku juga melakukan aktivitas phising dengan berpura-pura sebagai perusahaan kartu kredit tersebut.
• Dari kartu kredit yang telah didapat pelaku mengenerate CVV dengan menggunakan cardwizard dan cardpro.
• CVV degenerate dengan menggunakan mIRC, cardwizard dan cardpro yang menggunakan MOD 10 Algorithm atau Luhn Algorithm.
• Kartu kredit digunakan pelaku untuk melakukan belanja secara online.
• Kartu kredit yang didapat diperjual belikan oleh pelaku.

Temuan :
• Ditemukan daftar kartu kredit yang dikumpulkan pelaku pada komputer yang menjadi barang bukti.

- Ditemukan aplikasi card extrapolator berupa : master4, cardpro, cardwizard.
- Ditemukan screenshot berupa invoice hasil transaksi.
- Ditemukan e-mail transaksi dan phising.
- Ditemukan history dan bookmark berupa situs phising dan situ belanja online.

V. KESIMPULAN

Untuk pencarian barang bukti carding, pada awalnya dapat difokuskan pencarian log aktivitas pada web browser dan untuk dapat menganalisis suatu barang bukti, seorang penyidik bukti digital harus paham akan konsep bukti itu sendiri, sistem operasi yang akan dicek serta paham akan konsep jaringan dan serangan serta Barang bukti carding yang ditemukan dalam penelitian ini berupa phising email, invoice transaksi kartu kredit, percakapan *IRC*, *log history*, *bookmark*, aplikasi terkait, dan sebagainya. Dengan menggunakan FTK akan menampilkan hampir seluruh data sehingga akan lebih mempermudah pencarian terhadap data yang telah dimanipulasi serta yang telah dihapus

VI. UCAPAN TERIMA KASIH

Kepoliisian Republik Indonesia, Khususnya Polda Yogyakarta yang telah memberikan kesemapatan pada peneliti.

VII. REFERENSI

A Project Presented to the School of Science & Technology, N. (2014). Digital Forensic : a Panacea for Evidence Preservation. *Nigerian National Open University*. https://www.academia.edu/31071732/DIGITAL_FORENSIC_A_PANACEA_FOR_EVIDENCE_PRESERVATION

Adoc.pub. (2020). *13 Cyber Crime _ Sebuah Evolusi Kejahatan Jenis kejahatan konvensional _ Kejahatan kerah biru (blue collar crime) Pencurian, penipuan, pembunuhan - PDF Free Download.pdf* (p. 15). https://adoc.pub/cyber-crime-sebuah-evolusi-kejahatan-jenis-kejahatan-konvens.html

Beginners, C. T. for. (2022). *Digital Forensics Life Cycle*. Digital Forensics Onlone.

Das, S., & Nayak, T. (2013). *I Mpact of C Yber C Rime : I Ssues and Challenges*. *6*(2), 142–153.

Deora, R. S., & Chudasama, D. M. (2021). Brief Study of Cybercrime on an Internet Information Systems Audits for eCommerce View project Grocery Deals View project. *Journal of Communication Engineering & Systems*, *11*(1), 1–6. https://doi.org/10.37591/JoCES

Griffith, R. (2017). Giving evidence in court. *British Journal of Nursing*, *26*(18), 1038–1039. https://doi.org/10.12968/bjon.2017.26.18.1038

Grigaliunas, Š., & Toldinas, J. (2020). Habits attribution and digital evidence object models based tool for cybercrime investigation. *Baltic Journal of Modern Computing*, *8*(2), 275–292. https://doi.org/10.22364/BJMC.2020.8.2.05

Hacker, C. E. (2022). *The All-New C | EHv12 with New Learning Framework : 1 . Learn 2 . Certify 3 . Engage 4 . Compete Who is a Certified Ethical Hacker ? C | EH Program Information 5 Phases of Ethical Hacking*. EC Council Cyber Security ExChange. https://www.eccouncil.org/cybersecurity-exchange/ethical-hacking/cehv12-new-learning-framework/

Hauger, W. K. (2018). Forensic Attribution Challenges During Forensic Examinations Of Databases by. *Faculty of Engineering, Built Environment and Information Technology*, *September*. https://repository.up.ac.za/bitstream/handle/2263/72738/Haunger_Forensic_2018.pdf?seque

nce=1&isAllowed=y

Horsman, G., & Sunde, N. (2022). Unboxing the digital forensic investigation process. *Science and Justice*, *62*(2), 171–180. https://doi.org/10.1016/j.scijus.2022.01.002

Kadir, N. K., Judhariksawan, J., & Maskun, M. (2019). Terrorism and Cyberspace: A Phenomenon of Cyber-Terrorism as Transnational Crimes. *FIAT JUSTISIA:Jurnal Ilmu Hukum*, *13*(4), 333. https://doi.org/10.25041/fiatjustisia.v13no4.1735

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

Manap, N. A., Abdul Rahim, A., & Taji, H. (2015). Cyberspace identity theft: An overview. *Mediterranean Journal of Social Sciences*, *6*(4S3), 290–299. https://doi.org/10.5901/mjss.2015.v6n4s3p290

Moedjahedy, J. (2016). Forensik komputer Studi Kasus: Universitas Klabat. *Jurnal Sistem Informasi Dan Teknologi Informasi (JUSITI)*, *5*(2), 95–106.

MUKTI, W. A. (2017). *ANALISA DAN PERBANDINGAN BUKTI FORENSIK APLIKASI MEDIA SOSIAL FACEBOOK DAN TWITTER PADA SMARTPHONE ANDROID* [UNIVERSITAS ISLAM NEGERI SYARIF HIDAYATULLAH]. https://repository.uinjkt.ac.id/dspace/bitstream/123456789/52787/1/WISNU ARI MUKTI-FST.pdf

Nations, U. (2022). *EVIDENCE MANAGEMENT*. Office on Drugs and Crime Online. https://www.unodc.org/unodc/en/terrorism/expertise/evidence-management.html

Norwich University Online. (2017). *5 Steps for Conducting Computer Forensics Investigations | Norwich University Online*. Information Security & Assurance. https://online.norwich.edu/academic-programs/resources/5-steps-for-conducting-computer-forensics-investigations

Presiding, S., The, J., Hon, R. T., Edis, S. A., Reporting, S. F., Judge, S. P., Forensic, S., Guidance, R., & Providers, F. S. (2022). *Streamlined Forensic Reporting (SFR) SFR FAQs*. Forensic Capability Network. https://www.fcn.police.uk/what-we-do/sfr

Shoukat et. al., S. (2018). Cyber Crime- Techniques, Prevention and Cyber Insurance. *International Journal of Computing and Network Technology*, *6*(1), 23–26. https://doi.org/10.12785/ijcnt/060103

Singh, A., Ikuesan, R. A., & Venter, H. (2022). Secure Storage Model for Digital Forensic Readiness. *IEEE Access*, *10*(January), 19469–19480. https://doi.org/10.1109/ACCESS.2022.3151403

Steegh, N. Ver. (2020). 10 Steps for Presenting Evidence in Court. *National Council Of Juvenile and Family Court Judges*, 16. https://www.ncjfcj.org/sites/default/files/NCJFCJ_SRL_10StepsEvidence_Final.pdf

Suleiman, M. M., Anas, A. A., Adamu, I., & Adam, S. M. (2020). Prevention & Detection Measures Against Cybercrimes Attack Department of Home & Rural Economics Department of Establishment , Central Administration School of Rural Technology and Entrepreneurship Development , Rano . Being A Paper To Be Presented At Its. *International Research Initiative Conference*, *1*(Kumar 2010), 13. https://www.academia.edu/44547837/Prevention_and_Detection_Measures_Against_Cyber crimes_Attack

e-ISSN : 2541-1330
p-ISSN : 2541-1332

Team, W. U. (2022). *Using evidence*. Academicguides Walden. https://doi.org/10.51952/9781447345527.ch012

UNESCO. (2022). *E4J University Module Series : Cybercrime Module 3 : Legal Frameworks and Human Rights The role of cybercrime law Substantive law*. United Nations Office on Drugs and Crime. https://www.unodc.org/e4j/en/cybercrime/module-3/key-issues/the-role-of-cybercrime-law.html

US Deputy Attorney General Eric H Holder Jr, 2000 Research by National Hitch Crime Unit (NHTCU), UK. (1998).

Varol, A., & Ülgen Sönmez, Y. (2017). Review of Evidence Collection and Protection Phases in Digital Forensics Process. *INTERNATIONAL JOURNAL OF INFORMATION SECURITY SCIENCE Y. Ülgen Sönmez et.Al*, *6*(4), 39–45. https://www.ijiss.org/ijiss/index.php/ijiss/article/view/267

Yar, M. (2012). Cybercrime and the Internet: An Introduction. *Cybercrime and Society*, *2022*, 1–20. https://doi.org/10.4135/9781446212196.n1

Zjalic, J. (2020). Forensic reporting. In *Digital Audio Forensics Fundamentals* (pp. 241–247). https://doi.org/10.4324/9780429292200-12