e-ISSN 2338-5197

Analisis Forensik pada *Web Phishing* Menggunakan Metode *National Institute Of Standards And Technology* (*NIST*)

Agil Nofiyan [a,1,*], Mushlihudin [b,2]

[a b] Program Studi Teknik Informatika, Fakultas Teknologi Industri, Universitas Ahmad Dahlan, Jalan Ringroad Selatan, Kragilan, Tamanan, Kec. Banguntapan, Bantul, Daerah Istimewa Yogyakarta (55191), Indonesia
[1] agil1500018271@webamil.uad.ac.id *; [2] mushlihudin@tif.uad.ac.id [3]
* Penulis Korespondensi

ABSTRAK

Komunikasi dan informasi menjadi kebutuhan yang sangat penting dan dapat menimbulkan masalah pada teknologi itu sendiri. Bentuk kejahatan *cybercrime* dengan teknik *phishing*, *phiser* memanipulasi *link* atau URL yang sengaja dilakukan untuk mendapatkan informasi penting dari seseorang atau kelompok. Teknik tersebut dengan menyisipkan *script* atau memanipulasi *website* dengan *protocols* HTTPS (*Hypertext Transfer Protocol Secure*) pada *website* yang digunakan oleh *phiser.* Hal tersebut untuk menarik perhatian korban mengakses URL atau situs yang *phiser* sebarkan melalui *email*. Maraknya pencurian *account* berbasis web *phishing* yang digunakan *phiser* atau pelaku dengan tujuan mengambil data yang *sensitive* pada *account* korban seperti *username* dan *password.*

Penggunaan metode *National Institute of Standards and Technology* (*NIST*) bertujuan untuk menganalisis proses investigasi atau forensik digital kasus *cybercrime* dan memunculkan barang bukti digital. Tahapan analisis berupa *Collection, Examination, Analysis* dan *Reporting*. Penggunaan *tools wireshark* untuk mencari barang bukti dan *tools hashcalc* untuk mengakuisisi barang bukti yang didapatkan. Hasil barang bukti digital tersebut dapat digunakan untuk proses penyelidikan mengungkap kejahatan digital.

Penelitian ini menganalisis serangan *web phishing* oleh *phiser* menggunakan *fitur fake login* dan didapatkan *file capture wireshark* dari web *phishing* dengan *protocols* HTTPS serta hasil analisis dari pendekripsian pada keamanan yang terdapat pada *protocols* HTTPS berupa URL *phishing*, DNS (*Domain Name System*) yang digunakan oleh pelaku, *IP address server*, *IP address destination*, identitas penyerang dan *email* dari informasi tindak kejahatan yang dilakukan *phiser* untuk mendapatkan *account valid* milik korbannya.

Kata Kunci : *Web Pishing*, digital forensik, *cybercrime, fake login, wireshark*

1. Pendahuluan

Perkembangan teknologi yang semakin pesat, dapat menimbulkan permasalahan bagi teknologi itu sendiri, hal tersebut menjadikan internet sebagai salah satu media yang dimanfaatkan untuk pencurian data oraganisasi, individu maupun pemerintahan. *Cybercrime* berdasarkan jenis aktivitas seperti *Unauthorized Acces* kejahatan yang dilakukan seseorang dengan memasuki sistem jaringan komputer tanpa izin dari pemilik sistem jaringan komputer yang dimasukinya, *Ilegal Contens* kejahatan dengan memasukan data atau informasi ke internet dan dianggap melanggar hukum, Penyebaran virus dengan sengaja seperti *Malware* dengan merusak *software*. *Carding* kejahatan untuk mencuri nomor kredit milik orang lain dan digunakan dalam transaksi perdangangan di internet [1]. Dalam hal ini phishing dikenal juga sebagai *carding* yaitu sebuah bentuk layanan menipu dengan menjanjikan keabsahan dan keamanan transfer data yang dilakukan. Penanganan pada kasus *cybercrime* tidak bisa hanya menggunakan bukti *screenshoot*, foto, maupun video karena bisa saja dapat dimanipulasi oleh pihak terkait, pada penelitian ini membutuhkan bukti lengkap terkait bukti digital seperti *link* atau URL, *Email*, *Domain*, *IP address*, dan identitas pelaku yang digunakan pelaku untuk memancing korban. Proses menemukan dan mengidentifikasi barang bukti digital membutuhkan proses yang panjang dan membutuhkan waktu untuk memperoleh data yang akurat [2]. Keamanan menjadi hal yang utama dalam perkembangan teknologi informasi dan dunia forensik, dengan perkembangan teknologi secara pesat berdampak pada kejahatan *cybercrime*. Namun bentuk kejahatan *cybercrime* dengan teknik *phishing*, *phiser* memanipulasi *link* atau URL yang sengaja

 e-ISSN 2338-5197

dilakukan untuk mendapatkan informasi penting dari seseorang atau kelompok. Teknik tersebut dengan menyisipkan *script* atau memanipulasi sebuah web dengan *protocols* HTTPS pada website yang digunakan oleh *phiser*. Hal tersebut untuk menarik perhatian korban mengakses URL atau situs yang *phiser* sebarkan melalui *email*. *Protocols* HTTPS mempunyai keamanan yang tinggi dengan cara mengenkripsi data menggunakan *algortihma* dari hal ini *phiser* memanfaatkan keamanan HTTPS untuk membuat web *phishing* dan juga meyakinkan korban bahwa web tersebut aman untuk digunakan. Pencurian *account* berbasis web *phishing* dengan *fake domain* yang digunakan *phiser* atau pelaku, dengan tujuan mengambil data yang *sensitive* pada *account* korban seperti *username* dan *password.* Oleh karena itu, pada penelitian ini ini peneliti membuat skenario kasus kejahatan web *phishing* dengan memanfaatkan *fitur login* dan *fake domain* bertujuan untuk menganalisis proses investigasi atau forensik digital kasus *cybercrime* serta memunculkan barang bukti meliputi DNS, *IP address server, IP address destination*, identitas penyerang, *email* korban dan *email* pelaku. Penyelidikan menggunakan tahapan dari metode *National Institute Of Standards And Technology* (*NIST*) dengan empat tahapan sebagai acuan analisis barang bukti yaitu *collection, examination, analiysis,* dan *reporting*.

2. Landasan Teori

2.1. Forensik Digital

Forensik digital merupakan bagian dari ilmu forensik yang meliputi pemulihan dan investigasi dari bahan yang ditemukan pada perangkat digital (*digital devices*), komputer (*host, server*), jaringan (*network*), dan aplikasi. Forensik digital merupakan ilmu yang masih baru dan dibutuhkan pemahaman dan kemampuan untuk menguasai ilmu ini [3]. Tahapan pada digital forensik digunakan untuk menjadi acuan menangani kasus tersebut, tahapannya sebagai berikut:

1. Identifikasi
   Dalam tahapan awal ini proses identifikasi pada barang bukti sangat penting untuk melakukan proses penyelidikan pada tahap berikutnya.
2. Pemeliharaan
   Pemeliharaan pada barang bukti digital harus dijaga dan terhindar dari kerusakan karena barang bukti hilang atau berubah membuat barang bukti tidak akan di akui di pengadilan
3. Analisis
   Tahapan ini bukti digital dilakukan pemeriksaan secara detail oleh penyidik untuk membuktikan kejahatan tersebut. Hasil analisis harus dipertanggunjawabkan didepan pengadilan dan secara keilmiahan.
4. Presentasi
   Presentasi dilakukan oleh penyidik dengan menyajikan dan menguraikan hasil dari barang bukti yang sudah di analisa, sehingga barang bukti tersebut membantu proses penyidikan untuk menemukan tersangka.

2.2. Komputer Forensik

Komputer forensik adalah bidang yang dapat membantu dalam upaya penegakan hukum terhadap kejahatan yang berhubungan dengan komputer langsung maupun tidak langsung dengan bantuan *software* yang digunakan untuk investigasi terhadap barang bukti yang ditemukan. Pentingnya ahli komputer forensik untuk pencarian dan menganalisa barang bukti pada kasus kejahatan di bidang komputer (*cybercrime*) [4].

2.3. *Website*

Website adalah halaman informasi yang menampilkan teks, data gambar diam atau gerak, data animasi, suara, video atau gabungan dari semuanya baik yang bersifat *statis* maupun *dinamis* yang membentuk satu rangkaian bangunan yang saling terkait dimana masing-masing dihubungkan dengan jaringan- jaringan halaman (*hyperlink*). Jaringan tersebut disediakan melalui jalur internet sehingga bisa di akses oleh pengguna internet di seluruh dunia. [5]. HTTP dan HTTPS adalah sebuah protokol untuk meminta atau menjawab antara client dan server, client HTTP meminta dengan membuat hubungan TCP/IP ke *port* 80 sedangkan HTTPS meminta dengan membuat hubungan *Secure Socket Layer* (SSL) atau *Transport Layer Security* (TLS) ke *port* 443. Perbedaaan HTTP dan

e-ISSN 2338-5197

HTTPS terdapat pada tingkat keamananya, pada protokol HTTP data yang dikirim ke server memiliki informasi kode yang menjelaskan dari permintaan data tersebut, setelah menerima kode, server akan menjawab atau mengirim kembali kode jawaban dari data tersebut, sedangkan protokol HTTPS data yang dikirim ke server akan terenkripsi disertai kunci publik, server bisa membaca permintaan data yang dienkripsi dan mendekripsi data dengan kunci publik. HTTPS di enkripsi dan dekripsi dari data yang diminta oleh pengguna dan data dikembalikan oleh server.[6]

2.4. *Cybercrime Phishing*

Phising adalah salah satu kejahatan yang paling cepat berkembang internet. Dimana *phiser* mengirim situs web yang terkait atau *email* secara acak untuk memancing penerima untuk membocorkan informasi pribadi, *email* yang digunakan seperti asli dari lembaga atau perusahaan layanan yang sah [7].

2.5. *National Intitute Of Standards And Technology* (*NIST*)

National Intitute Of Standards And Technology (*NIST*) adalah badan nasional *non-regulator* dari bagian administrasi teknologi Amerika Serikat. Misi dari badan ini adalah untuk mendorong dan membuat pengukuran, standar, dan teknologi untuk meningkatkan produktivitas, mendukung perdangangan, dan memperbaiki kaualitas hidup semua orang. Program *cybersecurity NIST* berupaya memungkinkan pengembangan lebih besar dan penerapan teknologi dan metodologi keamanan yang inovatif dan praktis untuk meningkatkan kemampuan negara mengatasi tantangan keamanan komputer dan informasi saat ini dan masa depan [8]. Tahapan pada metode *National Institute Of Standards And Technology (NIST)* dibawah ini tahapan yang dilakukan pada metode NIST, sebagai berikut:

1. *Collection* (Pengumpulan data)
   Pada tahapan ini yang dilakukan yaitu pengumpulan barang bukti dengan proses identifikasi, pengumpulan, pengambalian dan perekaman barang bukti.
2. *Examinarion* (Akuisisi data)
   Pada tahap ini hasil dari pengumpulan barang bukti dilakukan pengujian agar tidak ada perubahan informasi pada barang bukti.
3. *Analysis*
   Pada tahap ini barang bukti dilakukan pemeriksaan untuk mendapatkan bukti terkait dengan kasus tersebut.
4. *Reporting* (Pembuatan laporan)
   Pelaporan hasil investigasi yang didapatkan dari penyelidikan berisi tentang hasil analisa barang bukti sehingga bukti tersebut membantu proses penyidikan untuk menemukan tersangaka.

3. Metodologi

Pada penelitian ini untuk mengungkap bukti kejahatan *cybercrime* dengan objek penelitian ini adalah *fitur fake login* yang dimanfaatkan oleh *phiser* untuk ekspolitasi data *user* dengan mendapatkan informasi *username* dan *password* korban dengan menggunakan *email* sebagai media penyebaran URL *phishing*. Metode yang digunakan untuk mengungkap kejahatan adalah *National Institute Of Standards And Technology* (*NIST*).

3.1. *Hardware* dan *Software* yang Digunakan

Penelitian ini dikerjakan menggunakan perangkat *hardware*, *software* dan beberapa web untuk menganalisa web *phishing*. Penelitian ini dilakukan dengan menggunakan 2 laptop kepemilikan yaitu milik investigator dan milik pelaku. Perangkat keras (*hardware*) dan perangkat lunak (*software*) yang digunakan investigator untuk menganalisis web *phising* seperti Tabel 1 sebagai berikut:

Tabel 1. Tabel Peralatan Investigator

 e-ISSN 2338-5197

Hardware	Software	Website
Processor Intel® Celeron® CPU N2840 @ 2.16GHz (2 CPUs), 2.16GHz	Sistem operasi windows 10 Pro 64-bit, x64 based processor	https://centralops.net (pencarian informasi tentang DNS)
Graphics Intel® HD Graphics	Wireshark-win64-3.0	
RAM 2GB	Hashcalc	
Harddisk 1 TB	Mozilla Firefox 71.0(32-bit)	

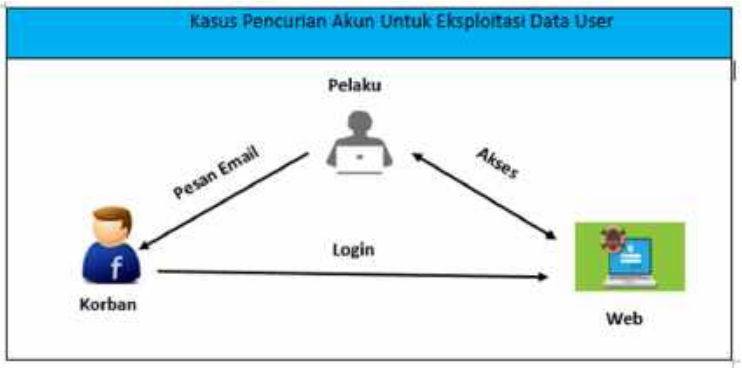
Perangkat keras (*hardware*) dan perangkat lunak (*software*) yang digunakan pelaku untuk merekontruksi serangan web *phishing* seperti ditampilkan pada Tabel 2.

Tabel 2. Tabel Peralatan Pelaku

Hardware	Software
Processor Intel® Core™ i7-7700 HQ CPU @ 2.80GHz, 2.80GHz	Sistem operasi windows 10 Pro 64-bit, x64 based processor
Graphics Intel® HD Graphics 630	Sublime Text 3
RAM 8 GB	Xampp versi 3.2.2
	Mozilla Firefox 71.0(64-bit)

3.2. Simulasi Kasus Kejahatan *Cybercrime*

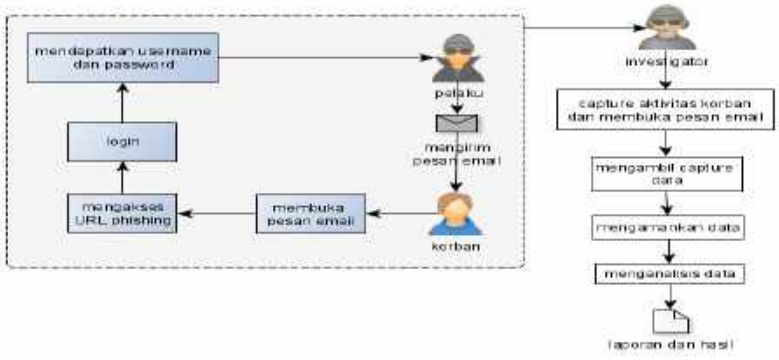
Simulasi kasus kejahatan *cybercrime* ini bertujuan untuk menjelaskan alur kejahatan *cybercime* yang dilakukan *phiser* seperti Gambar 1.



Gambar 1. Alur Proses Pencurian Akun

Pada tahapan ini akan dijelaskan alur pencurian *account* seperti Gambar 1 yang menjelaskan bagaimana pelaku mengirimkan *email* yang berisi URL *phishing* kemudian korban secara tidak sadar melakukan *login* menggunakan URL *phishing* tersebut, dari kejadian ini pelaku mendapatkan akses *account* korban. Berdasarkan simulasi kasus penulis mencoba membuktikan kejahatan tersebut, berdasarkan Gambar 2 mengimplementasikan alur lebih detail simulasi ulang kasus kejahatan dan pembuktian oleh investigator.

e-ISSN 2338-5197



Gambar 2. Rekontruksi Kejahatan dan Pembuktian oleh Investigator

Gambar 2 menampilkan rekontruksi kejahatan dan pembuktian yang dilakukan investigator dari barang bukti awal berupa pesan *email* korban yang berisikan URL *web phishing*. Investigator melakukan *capture* dengan membuka pesan *email*, mengakses URL *web phishing* dan mengisi *email* dan *password* pada *form fake login*. Investigator melakukan *capture* menggunakan *tools wireshark* untuk mendapatkan barang bukti dari *web phishing* serta mengakuisisi barang bukti agar tidak ada perubahan data dari barang bukti, *examination* atau pemeriksaan barang bukti dengan *tools hashcalc* untuk menguji nilai *hash* dari barang bukti terjadi perubahan atau tetap sama, analisis dilakukan untuk melakukan pencarian barang bukti dari hasil *capture* menggunakan *wireshark* dan melaporkan hasil barang bukti yang didapat dengan bahasa yang mudah dipahami.

3.3. *National Institute Of Standards And Technology* (*NIST*)

Pada penelitian ini mengacu dengan tahapan metode *National Institute Of Standards And Technology (NIST)* terdiri dari 4 tahapan yang dilakukan untuk melakukan proses investigasi sebagai berikut:

1. *Collection*

Tahapan yang dilakukan pada tahap ini yaitu pengumpulan data terkait kejahatan *phishing* dengan proses identifikasi, pengumpulan, pengambalian dan perekaman barang bukti. Pada tahapan penelitian ini proses awal melakukan *capturing* paket data pada website menggunakan *tools forensics wireshark,* kemudian paket data dilakukan akuisisi dan disimpan untuk menghindari terjadinya perubahan informasi pada paket data.

2. *Examination*

Proses pemeriksaan barang bukti untuk yang dikumpulkan menggunakan skenario. Proses pengujian barang bukti menggunakan *tool Hashcalc* untuk mendapatkan informasi dari *file hash* sama dengan nilai *file hash* pada *file capture.*

3. *Analysis*

Proses analisis yang dilakukan investigator pada barang bukti dari hasil pengumpulan data dan akuisisi pada tahap sebelumnya untuk memperoleh barang bukti yang terkait dengan kasus tersebut. Pemeriksaan meliputi bukti DNS yang digunakan oleh pelaku, *IP address server, IP address destination*, identitas penyerang, *email* korban dan pelaku.

4. *Reporting*

Proses pelaporan hasil investigasi dan data yang didapatkan dari penyelidikan. Laporan berisi tentang hasil identifikasi *capture* data dari barang bukti *URL phishing*. Laporan hasil analisis meliputi gambaran yang perlu dilakukan terkait kasus tersebut.

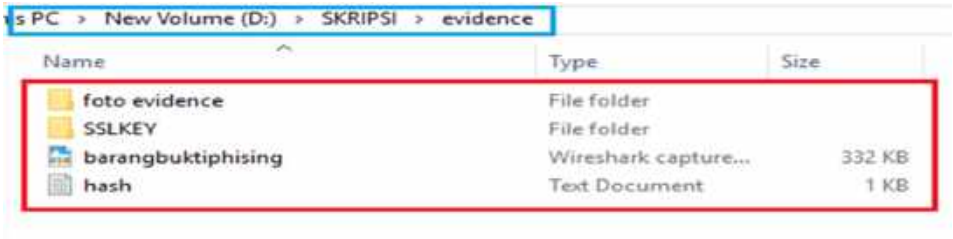
4. Hasil dan Pembahasan

4.1. *Collection*

Pada tahap pengumpulan data menggunakan *tools wireshark* untuk mengcapture saat korban mendapatkan *email* dari pelaku, korban mengakses *URL phishing* dan korban *login* dengan *username* dan *password* milik korban. Pada penelitian ini peneliti mengambil *file log* yang tersimpan untuk membantu investigasi. Dari aktivitas korban didapatkan *file* hasil *capture* (*.pcapng) dan nilai *hash*

e-ISSN 2338-5197

dari *file capture* serta didapatkan barang bukti tambahan dari folder SSLKEY dan folder foto evidence seperti ditampilkan pada Gambar 3.



Gambar 3. Isi Folder Evidence

Gambar 3 menampilkan 1 *file* hasil *capture* (*.pcapng) yang dilakukan pada tanggal 17 November 2019 dengan *file type* berupa *wireshark capture file*, folder foto evidence yang berisi *screenshoot* pesan *email* dari pelaku dan tampilan web *phishing*, folder SSLKEY yang berisi *file log* dari web *phishing* yang didapatkan dari tanggal 31 Oktober – 17 November 2019 dan diperoleh juga 1 *file* teks (*.txt) yang dibuat pada tanggal 19 November 2019.

4.2. *Examination*

Pada penelitian ini tahap akuisisi data dilakukan secara *offline* menggunakan *tools hashcalc* didapatkan nilai *hash* dari setiap *file* barang bukti seperti Tabel 3.

Tabel 3. Nilai *Hash File* dari Setiap *File* di Folder Evidence

File	Nilai Hash
Foto 1	1963ceb1e523b6a085580fec7a41327c
Foto 2	89de264bb94024bfa6b6ddadcfe9b744
Foto 3	7c471324ee91349ce94155e13b577255
Foto 4	139e63e9ee8106c9a713f93ab71d3d30
Foto 5	548b6db5ae8a527c9fa8f71f78df3b2a
Barangbuktiphising.pcapng	4b638e8f7dc62ee9a81abfcffc5678b3
SSLkeylog	0862d95d7b0a13ca2c4f1bcc7b10861c

Tabel 3 menampilkan informasi nilai *hash* dari setiap *file* di folder evidence yang tersimpan dalam *file* hash.txt. Nilai *hash* yang dibuat menggunakan *algorithma* MD5 dengan *tools hashcalc*.

4.3. *Analysis*

Pada penelitian ini tahap analisis data barang bukti pada *file capture* barangbuktiphising.pcapng menggunakan *tools wireshark* untuk menganalisis dan mendapatkan barang bukti. *File* sslkeylog.log merupakan *file log* dari web *phishing*. *File log* ini akan membantu untuk mendekripsi pada HTTP2, TLSv1.2 dan TCP yang terenkripsi namun tidak semua data *file capture* yang didapat terdekripsi karena keamanan pada HTTPS menggunakan SSL (*Secure Socket Layer*) atau TLS (*Transport Layer Security*). Paket data yang akan di analisis dipilih menggunakan teknik *filter* untuk mempercepat dan memudahkan identifikasi paket data. Beberapa kata kunci untuk mencari paket-paket tertentu yang berhubungan dengan *gmail* untuk mencari pesan *email*, DNS dan HTTP2. Selain itu melakukan filter menggunakan kata kunci untuk mencari data secara spesifik menggunakan aplikasi *wireshark* misalkan, *frame contains gmail* dengan *IP destianation* 74.125.24.19 maka *IP destianation* dijadikan kata kunci untuk mencari data yang berhubungan dengan pesan *email* pada paket data nomor 148, Kata kunci DNS (*Domain Name Server*) yang berhubungan dengan isi pesan dari *email* yaitu fucebook.xyz dengan *IP server* 103.28.12.100 yang juga menjadi kata kunci untuk mencari barang bukti yang berhubungan dengan *domain* fucebook.xyz, kemudian kata kunci http2.header yang

berhubungan dengan *header* dari web *phishing*. Tabel 4 menampilkan nomor paket data, teknik *filter* yang digunakan pada penelitian ini.

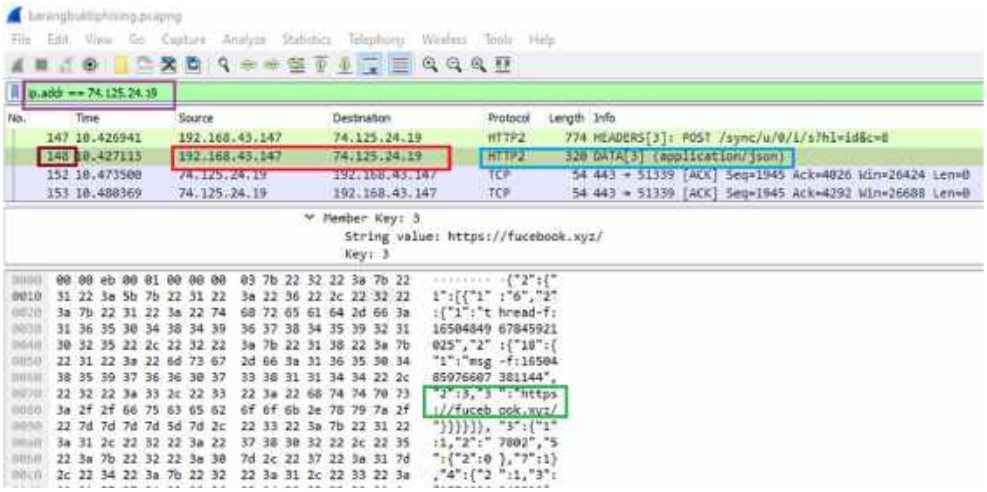
Tabel 4. Filterisasi yang digunakan di *tools wireshark*

Paket Data	Filter	Dekripsi
Nomor 148	Ip.addr == 74.125.24.19	Menunjukan trafik dari alamat IP 74.125.24.19
Nomor 129	dns	Menunjukan paket dengan protokol DNS
Nomor 132	dns	Menunjukan paket dengan protokol DNS
Nomor 257	ip.addr == 103.28.12.100	Menunjukan trafik dari alamat IP 103.28.12.100
Nomor 259	ip.addr == 103.28.12.100	Menunjukan trafik dari alamat IP 103.28.12.100
Nomor 262	http2.header	Menunjukan paket dengan protokol http2.header
Nomor 275	http2.header	Menunjukan paket dengan protokol http2.header

Tabel 4 menampilkan *filter* atau kata kunci yang digunakan saat menganalisis paket data untuk mempermudah investigator saat menganalisis paket data yang tertangkap. Keterangan masing-masing nomor paket data akan dijelaskan lebih detail, meliputi:

1. Paket Data Nomor 148

Dari hasil analisa pada *IP* 74.125.24.19 merupakan *capture* isi pesan *email* URL web *phishing* yang dikirim pelaku kepada korban yang dikirim pada tanggal 17 November 2019, hasilnya seperti ditampilkan pada Gambar 4.



Gambar 4. Hasil *Capture* Isi pesan *email* dari paket data nomor 148

Gambar 4 menampilkan hasil *capture* pada paket nomor 148 dengan isi pesan *email* yaitu https://fucebook.xyz. Dari hasil *capture* pada paket nomor 148 dibandingakan dengan *file screenshot* foto 4 dari kotak masuk di *email* dindareni538@gmail.com seperti Gambar 5.

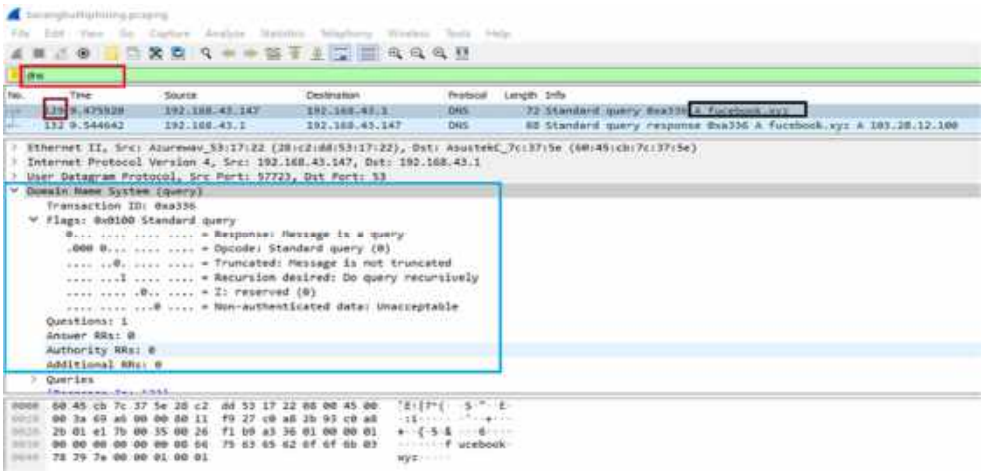
 e-ISSN 2338-5197

Gambar 5. Isi Pesan di *Email* dindareni538@gmail.com

Gambar 5 menunjukan isi pesan *email* dengan hasil *capture* sama yaitu https://fucebook.xyz yang merupakan URL *web phishing* dengan *subject* "Please, Sign In Your Account" dengan dalih agar korban melakukan *login* di URL tersebut, yang dikirimkan oleh pelaku dengan *email* rodalkul09@gmail.com kepada korban *email* dindareni538@gmail.com.

2. Paket Data Nomor 129

Paket data nomor 129 pada analisa *filterisasi* DNS merupakan sebuah *query request* kepada DNS *server* yang terdapat pada paket nomor 132 yang berarti *file* hasil *capture* ketika terjadi komunikasi menggunakan *protocol* DNS yang digunakan oleh pelaku untuk melakukan serangan *phishing*. Informasi detail setiap *query* hasilnya seperti Gambar 6.



Gambar 6. Informasi *Request Protocol* DNS

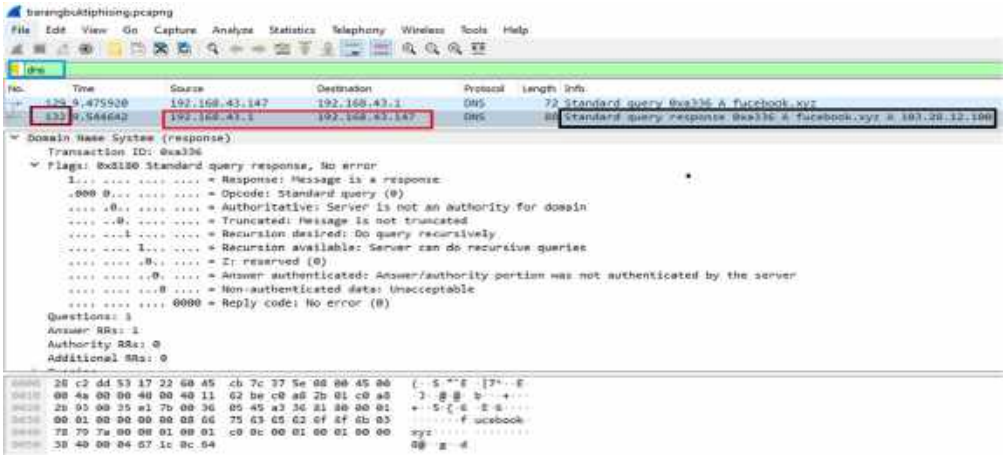
Gambar 6 menampilkan informasi format *header* paket data yang berisi *protocol* DNS. Aktifitas tersebut melakukan *query* terhadap *domain* fucebook.xyz. Analisa pada *query* sebagai tersebut:

a. *Flags* bernilai 0x100 yang memiliki arti:
   1) Tanggapan pesan bernilai 0 berupa *query*.
   2) *Opcode* menunjukan nilai 000 berupa *query*.
   3) Potongan pesan bernilai 0 artinya *not truncated*.
   4) Pengulangan bernilai 1 artinya *do query recursively*.
   5) Perlindungan bernilai 0 artinya Z *reserved.*
   6) Konfirmasi data bernilai 0 artinya *not authenticated* data.
b. *Questions* bernilai 1.
c. *Answer RRs* bernilai 0.
d. *Authority RRS* bernilai 0.
e. *Additional RRs* bernilai 0.

3. Paket Data Nomor 132

Paket data nomor 132 pada analisa *filterisasi* DNS merupakan *respon* dari paket data nomor 129 kepada DNS *server* dan diperoleh hasil format *header* DNS seperti Gambar 7.

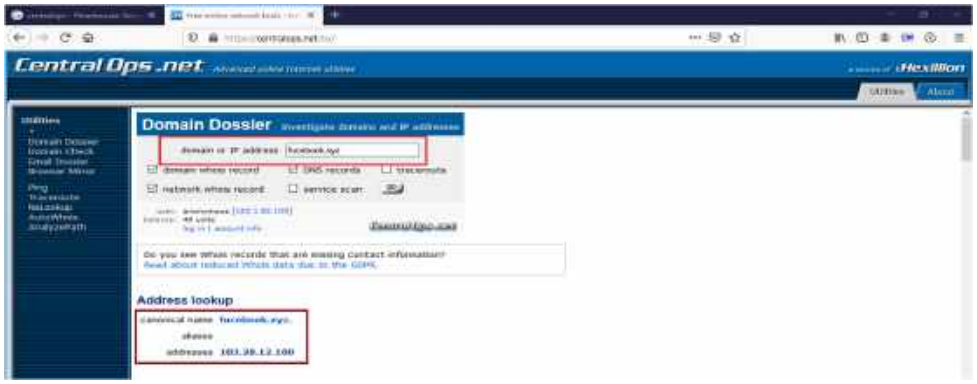
e-ISSN 2338-5197



Gambar 7. Informasi *Respon* DNS *Server*

Gambar 7 menampilkan informasi hasil *respon* paket data nomor 129 yang diketahui bahwa *respon* DNS *query* fucebook.xyz dengan IP *address source* 192.168.43.1 dan IP *address destination* 192.168.43.147. Hasil analisa *protocol* DNS yang digunakan pelaku dalam melakukan serangan di paket data nomor 132 disimpulkan merupakan paket data *protocol* DNS.

Setelah diketahui DNS dari *web phishing* tahap selanjutnya mencari informasi mengenai DNS tersebut menggunakan *website* https://centralops.net. Setelah mengakses *website* centralops.net memasukan *domain* fucebook.xyz pada kolom pencarian *domain*, maka diperoleh informasi DNS fucebook.xyz seperti Gambar 8.



Gambar 8. Informasi *IP Address Domain* fucebook.xyz

Gambar 8 menampilkan informasi IP *address domain* fucebook.xyz dengan IP *address server* 103.28.12.100. Informasi domain *whois record* yang berhubungan dengan *domain* fucebook.xyz dan diperoleh informasi lainnya meliputi:

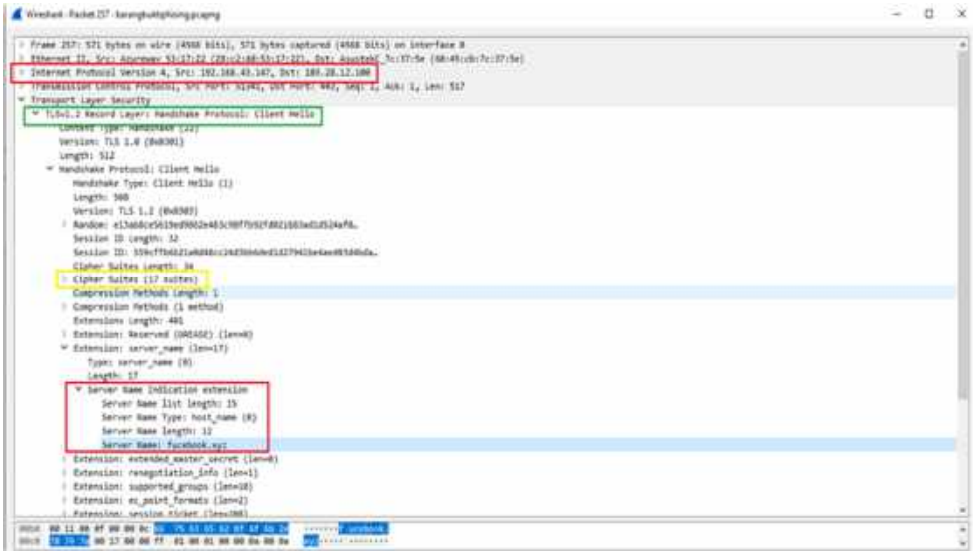
a. Nama domain : fucebook.xyz
b. Pembuatan domain : 30 oktober 2019
c. Organisasi pendaftar: fucebook
d. Provinsi pendaftar : Jawa Tengah
e. Negara pendaftar : Indonesia (ID)

4. Paket Data Nomor 257

Paket data nomor 257 pada analisa *filterisasi* ip.addr == 103.28.12.100 merupakan *record layer handshake protocol* “Client Hello” menggunakan *protocol* TLSv1.2 untuk komunikasi dengan

e-ISSN 2338-5197

membuat sambungan dari *client* dengan IP *address source* 192.168.43.147 ke *server* dengan IP *address destination* 103.28.12.100, seperti Gambar 9.



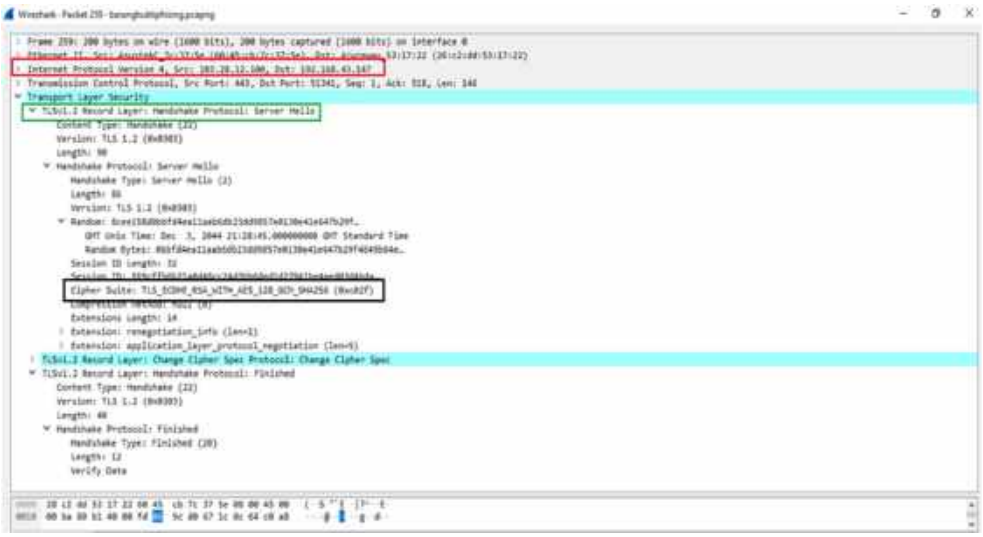
Gambar 9. Informasi *Record Layer Handshake Protocol* "Client Hello"

Gambar 9 menampilkan pengiriman paket data yang akan dikirim ke DNS dari IP *address source* 192.168.43.147 dengan mengirim permintaan *chIpher suites* sebanyak 17 *suites* yang akan di setujui salah satu *suites* oleh IP *address destination* 103.28.12.100 dengan nama *server* fucebook.xyz yang akan mengamankan komunikasi menggunakan *protocol* TLSv 1.2.

5. Paket Data Nomor 259

Paket data nomor 259 pada analisa *filterisasi* ip.addr == 103.28.12.100 merupakan *record layer handshake protocol* "Server Hello" menggunakan *protocol* TLSv1.2 untuk persetujuan komunikasi yang diminta *client* IP 192.168.43.147 pada paket data nomor 257 kepada *server* IP 103.28.12.100, seperti Gambar 10

.



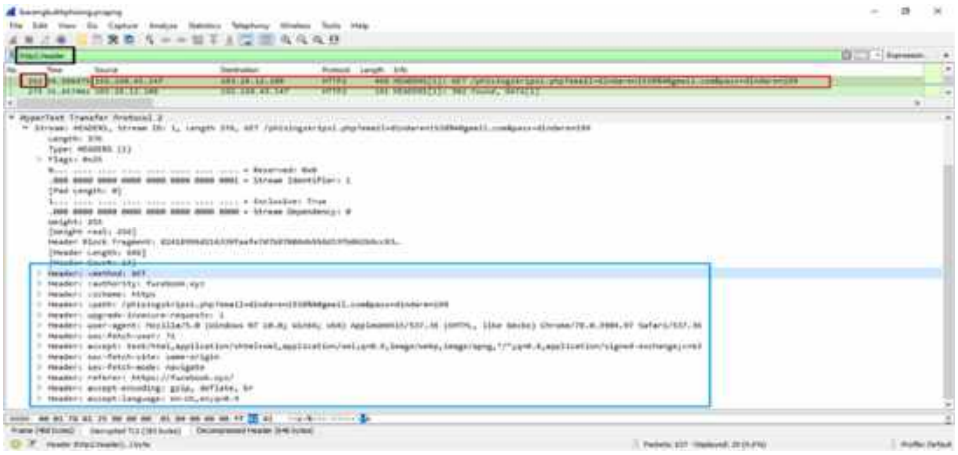
Gambar 10. Informasi *Record Layer Handshake Protocol "Server Hello*"

Gambar 10 menampilkan persetujuan komunikasi dari *server* dengan *IP* 103.28.12.100 kepada *clien* dengan *IP* 192.168.43.147 menggunakan *chiper suites* TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 yang bernilai 0xc02f.

e-ISSN 2338-5197

6. Paket Data Nomor 262

Paket data nomor 262 pada analisa *filterisasi* http2.header, terlihat IP 192.168.43.147 melakukan *request* ke IP 103.28.12.100, kemudian IP 192.168.43.147 diarahkan untuk mengakses website tersebut, seperti Gambar 11.

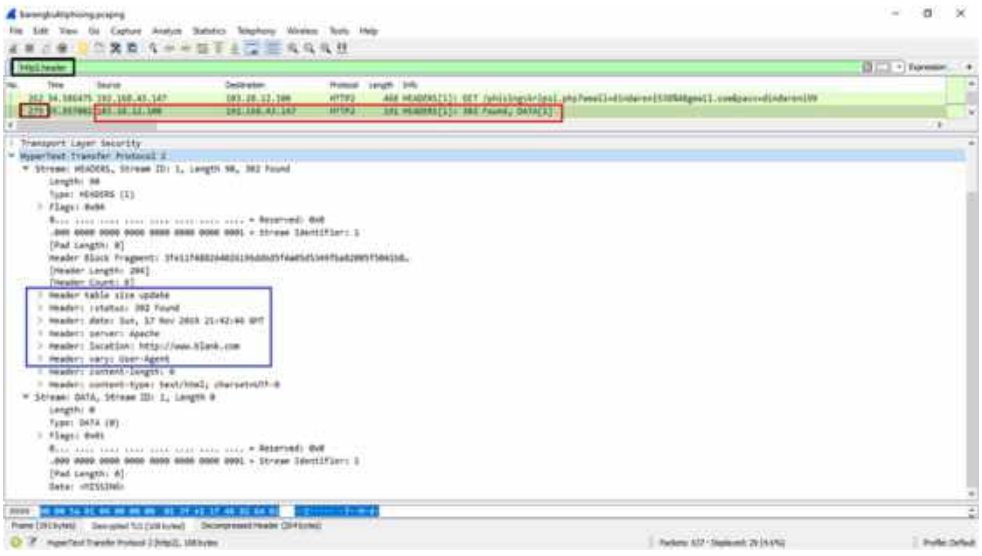


Gambar 11. Informasi *Protocol* HTTP2 di *header Web fucebook.xyz*

Gambar 11 menampilkan informasi dari *protocol* http2 pada *header* di web fucebook.xyz. Hasil analisis pada paket data nomor 262 di *form login* web fucebook.xyz, *method GET* merupakan *method* yang digunakan *phiser* di *form login* untuk pengiriman *input* data *email* dan *password*. Data yang dikirimkan *clien* dengan IP 192.168.43.147 akan melewati *path* atau *action* phisingskripsi.php ke *server* dengan IP *server* 103.28.12.100.

7. Paket Data Nomor 275

Paket data nomor 275 pada analisa *filterisasi* http2.header, terlihat IP 103.28.12.100 melakukan *respon* ke IP 192.168.43.147, kemudian IP 103.28.12.100 memproses data yang di *input* ke DNS, seperti Gambar 12.



Gambar 12. Informasi *Respon* dari IP 103.28.12.100

Gambar 4.19 menampilkan *respon* dari IP 103.28.12.100 ke IP 192.168.43.147. Hasil analisa pada paket nomor 275 terdapat kode status 302 *found* yang berarti pengalihan dari *server* dengan IP

e-ISSN 2338-5197

103.28.12.100 ke *server* baru yang bernama http://www.blank.com dengan IP 199.59.242.153 dengan *server apache* dan aliran data bernilai 0.

4.4. *Reporting*

Tahap *reporting* pada penelitian ini melaporkan hasil analisis barang bukti yang berkaitan dengan laporan korban pada pencurian akun yang telah diskenariokan. Dari *file capture* barangbuktiphising.pcapng didapatkan hasil analisis. *Reporting* dari hasil analisis yang telah dilakukan dan disajikan dalam bentuk Tabel 5.

Tabel 5. *Reporting* Hasil Analisis *File Capture* barangbuktiphising.pcapng

Paket Data	Hasil
Paket Data Nomor 148	• Pesan e-mail • IP address source : 192.168.43.147 • IP address destination : 74.125.24.19 • IP: 209.85.220.65 • Mail from : Fucebook (rodalkul09@gmail.com) • Mail to : dindareni538@gmail.com • Subject : Please, Sign In Your Account • Isi pesan : https://fucebook.xyz
Paket Data Nomor 129 dan Paket Data Nomor 132	• Protocol DNS (Domain Name System) • Host Phishing : fucebook.xyz • IP Address Host Phishing : 103.28.12.100 • IP address source : 192.168.43.147 • IP address destination : 192.168.43.1 • Organisasi Pendaftar : fucebook • Provinsi Pendaftar : Jawa Tengah • Negara : Indonesia (ID) • Date : 30 Oktober 2019
Paket Data Nomor 257	• Protocol TLSv 1.2 • Handshake Protocol : Client Hello • Requests Server Name : fucebook.xyz • IP address source : 192.168.43.147 Request to IP address destination : 103.28.12.100 • Send Request Chiper Suites : (17 Suites) • Algorthma : brotli
Paket Data Nomor 259	• Protocols TLSv.12 • Handshake Protocol : Server Hello • Respon Server Name : fucebook.xyz • IP address source : 103.28.12.100 Respon to IP address destination : 192.168.43.147 • Chiper Suites yang dipilih Server : TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 yang bernilai 0xc02f.
Paket Data Nomor 262	• Protocol http2.header • IP address source : 192.168.43.147 • IP address destination : 103.28.12.100 • Authority : fucebook.xyz • Scheme : https • Method : GET • Path : phisingskripsi.php?email=dindareni538%40gmail.com&pass-dindareni99 • Referer : https://fucebook.xyz

Tabel 5. *Reporting* Hasil Analisis *File Capture* barangbuktiphising.pcapng (Lanjutan)

e-ISSN 2338-5197

Paket Data Nomor 275	• Protocol http2.header • IP address source : 103.28.12.100 Respon to IP address destination : 192.168.43.147 • Header Status : 302 Found (Pengalihan) • Date : 17 november 2019 • Server : Apache • Location : http://www.blank.com • IP Location : 199.59.242.153

5. Kesimpulan

Menghasilkan barang bukti dari implementasi tahapan metode *National Institute Of Standards And Technology (NIST)* yaitu *collection* (pengumpulan data) *file capture* barangbuktiphising.pcapng didapatkan dari proses rekontruksi serangan pada web *phishing*, *examination* (akuisisi data) pemeriksaan nilai *hash* MD5 pada barang bukti digital, *analysis* pada barang bukti *file capture* barangnbuktiphising.pcapng didapatkan tujuh paket data yang berhubungan dengan tindak kejahatan yang dilakukan *phiser*, *reporting* (pelaporan) melaporakan barang bukti berupa URL *phishing*, DNS yang digunakan oleh pelaku*, IP address server, IP address destination*, identitas penyerang dan *email* yang menghasilkan informasi tindak kejahatan yang dilakukan *phiser*. Hasil dari memecah *protocols* HTTPS secara keseluruhan dengan mendekripsi struktur lalu lintas pada *protocols* TLSv 1.2 untuk memudahkan investigator dalam menganalisis barang bukti digital. Pada saat investigasi deitemukan celah untuk mendekripsi *protocols* HTTPS yang digunakan web *phishing*.

Daftar Pustaka

[1] D. Andika, "Kejahatan Teknologi Informasi (Cybercrime)," 2017. [Online]. Available: https://www.it-jurnal.com/kejahatan-teknologi-informasi-cybercrime/.

[2] A. Ginanjar, N. Widiyasono, and R. Gunawan, "Web Phising Attack Analysis on E-Commerce Service Using Network Forensic Process Method," *J. Terap. Teknol. Inf.*, vol. 2, no. 2, pp. 59–69, 2019.

[3] B. Raharjo, "Sekilas mengenai forensik digital," *J. Sosioteknologi*, pp. 384–387, 2013.

[4] S. M. Wisnu Budi , Aan Widayat Kusban, Muhammad, "Analisis Computer Forensic Untuk Mendukung Proses Penyelidikan Dalam Kasus Kejahatan," p. 12, 2015.

[5] Hakim, "Pengertian Website Menurut Para Ahli | TipsSerbaSerbi." p. PENDIDIKAN, 2004.

[6] A. A. Zabar and F. Novianto, "Keamanan Http Dan Https Berbasis Web Menggunakan Sistem Operasi Kali Linux," *J. Ilm. Komput. dan Inform.*, vol. 69, no. 2, pp. 2089–9033, 2015.

[7] G. Liu, B. Qiu, and L. Wenyin, "Automatic detection of phishing target from phishing webpage," in *Proceedings - International Conference on Pattern Recognition*, 2010, no. August 2010, pp. 4153–4156.

[8] National Institute Of Standards And Technology U.S Departement of Commerce, "Cybersecurity | NIST," 2019. [Online]. Available: https://www.nist.gov/topics/cybersecurity. [Accessed: 22-May-2019].