FORENSIK DIGITAL
{FORENSIK EMAIL}

Bahasan Meliputi:

- *Forensik Digital*
- *Forensik Email*
- *Akuisisi Email*
- *Analisis Email*
- *Studi Kasus*
- *Pelaporan*

Imam Riadi | Bashor Fauzan Muthohirin

Forensik Email

Imam Riadi | Bashor Fauzan Muthohirin

deandra kreatif

Forensik Email

Penulis: Dr. Imam Riadi | Bashor Fauzan Muthohirin
Proof: Diandra Kreatif
Layout: Diandra Kreatif
Cover: Diandra Kreatif

Diterbitkan melalui:
Diandra Kreatif (Kelompok Penerbit Diandra)
Jl. Melati No. 171
Sambilegi Baru Kidul, Maguwoharjo, Depok, Sleman, Yogyakarta
Telp. (0274) 2801996, Fax. (0274) 485222
E-mail: diandracreative@gmail.com
Fb. DiandraCreative SelfPublishing dan Percetakan
Instagram: diandraredaksi, diandracreative
www.diandracreative.com

Cetakan 2, Maret 2022
Yogyakarta, Diandra Kreatif 2022
xii + 55 hlm; 15,5 x 23 cm
ISBN:

Prakata

Perkembangan teknologi informasi dan komunikasi telah mengalami pertumbuhan sangat pesat seiring dengan era globalisasi yang menuntut percepatan arus informasi dan komunikasi. Kebutuhan informasi dan komunikasi merupakan kebutuhan utama masyarakat setelah kebutuhan primer. Salah satu perkembangan teknologi informasi dan komunikasi adalah electronic mail atau biasa disebut e-mail. E-mail merupakan salah satu alat yang digunakan untuk bertukar informasi, file, data, video, dan lain-lain. E-mail banyak digunakan dalam layanan bisnis dan personal, sehingga banyak dibutuhkan pengguna. Seiring dengan pertumbuhan teknologi, pertumbuhan kejahatan cyber juga ikut berkembang seperti penipuan e-mail, pemalsuan e-mail, e-mail fraud, dan lain-lain.

Buku ini memberikan landasan teori, metode, teknik, dan studi kasus untuk kalangan akademis dan profesional. Selain itu buku ini berfungsi sebagai buku teks, bahan ajar bagi pengguna pada bidang

teknik informatika, ilmu komputer, sistem informasi, dan sistem komputer.

Sebagai penutup,…

Buku ini jauh dari sempurna, saran dan pertanyaan dapat dilayangkan ke: imam.riadi@mti.uad.ac.id atau fauzan.bashor@gmail.com

Salam Hangat,

Daftar Isi

Daftar Gambar:

Bab 1
Forensicss Digital

Tujuan Instruksional Umum:

1. Mahasiswa/i mampu menjelaskan tentang *Forensik Digital.*

Tujuan Instruksional Khusus:

1. Mahasiswa/i mampu menjelaskan istilah standar dalam *Forensik Digital.*
2. Mahasiswa/i mampu memahami latar belakang, definisi, aplikasinya dan klasifikasi dalam *Forensik Digital.*
3. Mahasiswa/i dapat menjelajahi bidang investigatoran *Forensik Digital* yang sedang berkembang.

1.1. Pendahuluan

Korban melaporkan kepada pihak berwenang bahwa mereka mendapatkan *e-mail* yang sedikit aneh pada tanggal 11 November 2018. Pada *e-mail* tersebut korban akan mendapatkan hadiah berupa uang senilai Rp50 juta oleh salah satu PT. X yang memproduksi makanan siap saji yang terkenal di Indonesia. *E-mail* tersebut mengatasnamakan

HRD dari PT. X tersebut bahwa korban memenangkan kupon undian yang diundi setiap akhir pekan. Uang senilai Rp50 juta tersebut dapat diambil dengan syarat korban menghubungi nomor HP salah satu HRD di PT tersebut yaitu korban harus membayarkan biaya administrasi terlebih dahulu dengan maksud memperlancar pengiriman uang ke rekening korban, hal tersebut sangat aneh jika dilakukan oleh suatu perusahaan yang besar. Maka korban melaporkan hal tersebut kepada pihak yang berwajib untuk ditindak-lanjuti kebenaran akan *e-mail* yang dikirimkan. Kemudian pihak berwajib menindak-lanjuti laporan tersebut kemudian mengirim investigator ke tempat kejadian perkara. Melakukan akuisisi aktivitas log di dalam komputer investigator dan kemudian disimpan. Selanjutnya proses untuk mendapatkan barang bukti dari penipu, maka diperlukan proses investigasi pada *e-mail*.

1.2. Pengertian

Digital berasal dari kata Digitus, dalam bahasa Yunani berarti jari jemari. Apabila kita hitung jari jemari orang dewasa, maka berjumlah sepuluh (10). Nilai sepuluh tersebut terdiri dari 2 radix, yaitu 1 dan 0, oleh karena itu Digital merupakan penggambaran dari suatu keadaan bilangan yang terdiri dari angka 0 dan 1 atau *off* dan *on* (bilangan biner). Forensik (berasal dari bahasa Latin forensis yang berarti "dari luar", dan serumpun dengan kata forum yang berarti "tempat umum") adalah bidang ilmu pengetahuan yang digunakan untuk membantu proses penegakan keadilan melalui proses penerapan ilmu atau sains.

Menurut (Agarwal & Gupta, 2011) digital forensik adalah penggunaan ilmu dan metode untuk menemukan, mengumpulkan, mengamankan, menganalisis, menginterpretasi dan mempresentasikan barang bukti digital yang terkait dengan kasus yang terjadi untuk kepentingan rekonstruksi kejadian serta keabsahan proses peradilan.

Menurut ISACA (2015) digital forensik adalah proses mengidentifikasi, memelihara, menganalisis, dan menyajikan bukti digital dengan cara yang dapat diterima secara hukum dan dalam proses hukum apa pun (yaitu, pengadilan hukum).

Menurut Altheide & Carvey (2011) digital forensik merupakan penggunaan metode yang telah terbukti memperoleh pemeliharaan, pengumpulan, validasi, analisis identifikasi, interpretasi, dokumentasi, dan penyajian bukti digital yang berasal dari sumber digital untuk tujuan memfasilitasi atau melanjutkan rekonstruksi peristiwa yang ditemukan sebagai tindak kriminal, atau membantu mengantisipasi tindakan operasi yang terencana.

Menurut Zou, Huang, Lei, Zhou, & Zheng (2015) forensik digital diasosiasikan dalam banyak pikiran orang terutama dengan penyelidikan kesalahan. Namun, itu juga telah muncul dalam beberapa tahun terakhir sebagai sumber alat dan pendekatan yang menjanjikan untuk memfasilitasi pelestarian dan kurasi digital, khususnya untuk melindungi dan menyelidiki bukti kejahatan yang telah terjadi.

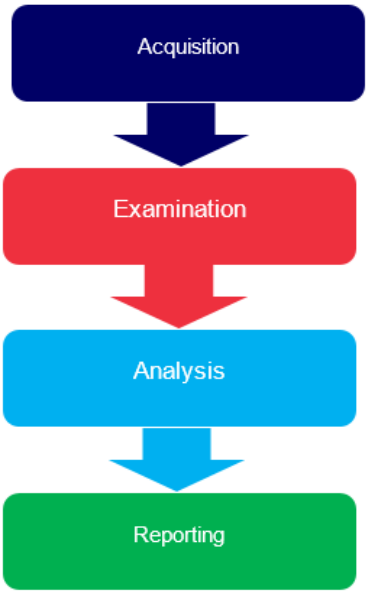
1.3. Metode Forensik

Proses untuk menemukan barang bukti digital, maka diperlukan metode agar dapat untuk menyelesaikannya. Terdapat beberapa metode forensik yang dapat digunakan seperti berikut :

1.0.1 *National Institute of Standards and Technology* (NIST)

NIST merupakan metode untuk melakukan analisis terhadap barang bukti digital atau untuk mendapatkan informasi dari bukti digital. NIST merupakan organisasi pemerintah di Amerika Serikat dengan misi mengembangkan dan mempromosikan penilaian, standar dan teknologi untuk meningkatkan fasilitas dan

kualitas kehidupan. Kegiatan utama adalah meneliti berbagai ilmu untuk mempromosikan dan meningkatkan infrastruktur teknologi. Berikut adalah tahapan 4 metode.



Gambar 1.1 Metode NIST

Berdasarkan gambar 1.1 merupakan tahapan proses investigasi digital forensik dari NIST, yang dimulai dari proses *akuisisi* barang bukti, *pengujian*, *pengujian* dan proses terakhir adalah *laporan* (Kent, Chevalier, Grance, & Dang, 2006; Umar, Riadi, & Muthohirin, 2018).

- ***Acquisition*** merupakan fase *acquisition* data yang terkait dengan peristiwa tertentu akan diidentifikasi, dikumpulkan, dan dilindungi.
- ***Examination*** merupakan fase pengujian alat dan teknik yang tepat untuk jenis data yang dikumpulkan selama fase pertama dilaksanakan untuk mengidentifikasi dan menganalisis

informasi yang relevan dari data yang diperoleh.

- ***Analysis*** merupakan fase yang paling penting dilakukan untuk menemukan bukti serangan. Seperti melakukan analisis log, analisis jaringan, dan analisis metode.
- ***Reporting*** merupakan fase terakhir melibatkan proses laporan dan praktik dalam konteks peristiwa saat ini untuk mengidentifikasi kekurangan kebijakan, kesalahan prosedural, dan masalah lain yang perlu diperbaiki.

NIST memiliki beberapa versi seperti *computer security, network security, information secerity,* dan lain-lain. Tabel 1.1 merupakan beberapa Metode NIST.

Tabel 1.1 NIST Network & Security

No	Nama	Tentang	Link
1.	NIST Interagency Report (IR) 7100	PDA *Forensics Tools*:An Overview and Analysis	https://csrc.nist.gov/publications
2.	NIST SP 800-31	Intrusion Detection Systems	https://csrc.nist.gov/publications
3.	NIST SP 800-44	Guidelines on Securing Public Web Servers	https://csrc.nist.gov/publications
4.	NIST SP 800-45	*Guidelines on Electronic Mail Security*	*https://csrc.nist.gov/publications*
5.	NIST SP 800-61	*Computer Security Incident Handling Guide*	*https://csrc.nist.gov/publications*
6.	NIST SP 800-72	Guidelines on PDA *Forensics*s	https://csrc.nist.gov/publications

7.	NIST SP 800-83	*Guide to Malware Incident Prevention and Handling*	https://csrc.nist.gov/*publications*
8.	NIST SP 800-160	Systems Security Engineering	https://csrc.nist.gov/publications
9.	NIST SP 800-190	application container security guide	https://csrc.nist.gov/publications

1.0.2 National Institute of Justice (NIJ)

Metode National Institute of Justice (NIJ) terbagi menjadi lima tahapan yakni *identification, collection*, *examination*, analysis, dan laporan (Mukasey, Sedgwick, & Hagy, 2001; Riadi, Rusydi, & Nasrulloh, 2017), secara lengkap dipaparkan sebagai berikut:

- ***Identification*** merupakan kegiatan pemilahan barang bukti tindak kejahatan digital dan pemilahan data-data untuk mendukung proses penyidikan dalam rangka pencarian barang bukti kejahatan digital. Pada tahap ini di dalamnya terdapat proses identifikasi, pelabelan, perekaman, untuk menjaga keutuhan barang bukti.
- ***Collection*** merupakan serangkaian kegiatan mengumpulkan data-data untuk mendukung proses penyidikan dalam rangka pencarian barang bukti kejahatan digital. Pada tahap ini di dalamnya terdapat proses pengambilan data dari sumber data yang relevan dan menjaga integritas barang bukti dari perubahan.
- ***Examination*** merupakan tahap pemeriksaan data yang dikumpulkan secara forensik baik secara otomatis atau manual, serta memastikan bahwa data yang didapat berupa *file* tersebut

asli sesuai dengan yang didapat pada tempat kejadian kejahatan komputer, untuk itu pada *file* digital perlu dilakukan identifikasi dan validasi *file* dengan teknik hashing.

- ***Analysis*** dilakukan setelah mendapatkan *file* atau data digital yang diinginkan dari proses pemeriksaan sebelumnya, selanjutnya data tersebut dianalisis secara detail dan komprehensif dengan metode yang dibenarkan secara teknik dan hukum untuk dapat membuktikan data tersebut. Hasil analisis terhadap data digital selanjutnya digunakan sebagai barang bukti digital serta dapat dipertanggungjawabkan secara ilmiah dan secara hukum.
- ***Reporting*** atau tahap pelaporan dilakukan setelah diperoleh barang bukti digital dari proses pemeriksaan dan dianalisis. Selanjutnya pada tahap ini dilakukan pelaporan hasil analisis yang meliputi penggambaran tindakan yang dilakukan, penjelasan mengenai *tool*, dan metode yang digunakan, penentuan tindakan pendukung yang dilakukan, dan memberikan rekomendasi untuk perbaikan kebijakan, metode, *tool*, atau aspek pendukung lainnya pada proses tindakan digital forensik.

1.0.3 Digital Forensicss Research Workshop (DFRWS)

Metode DFRWS membantu mendapatkan bukti dan mekanisme terpusat untuk merekam informasi yang dikumpulkan (Agarwal & Gupta, 2011):

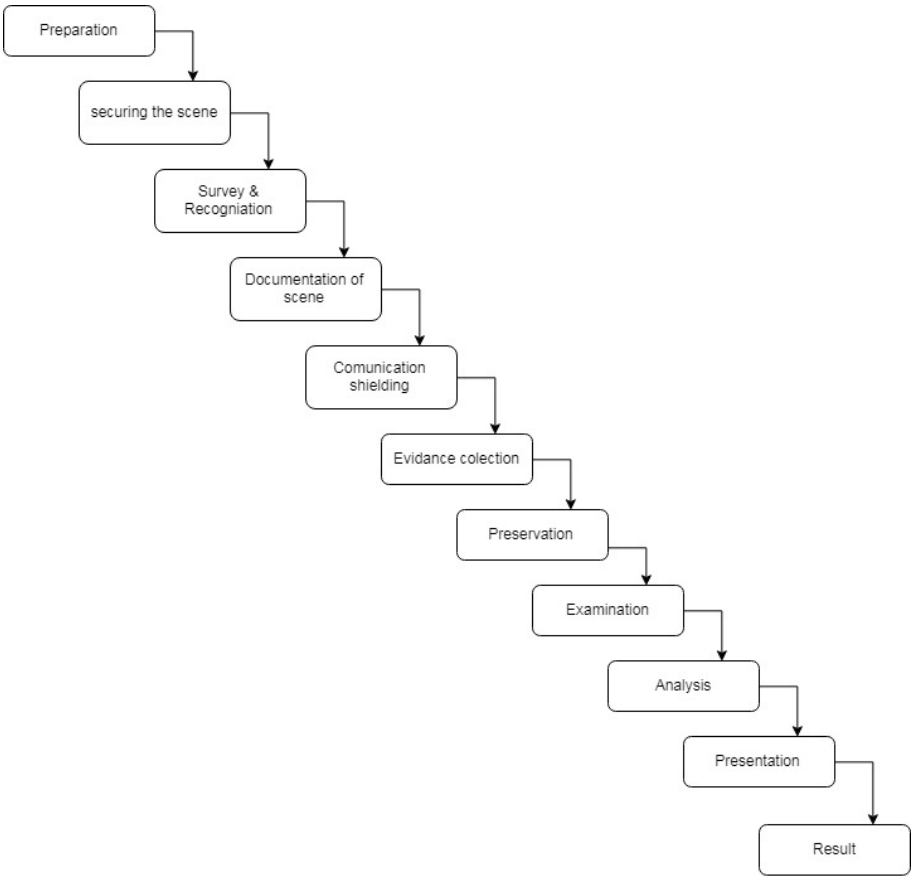
- ***Identification*** merupakan proses identifikasi, dilakukan untuk melakukan penentuan kebutuhan yang diperlukan pada penyelidikan dan pencarian bukti.
- ***Preservation*** merupakan pemeliharaan, dilakukan untuk menjaga bukti digital agar memastikan keaslian bukti dan membantah klaim bukti telah dilakukan sabotase.

- ***Collection*** merupakan proses pengumpulan, merupakan tahap untuk melakukan identifikasi bagian tertentu dari bukti digital dan melakukan identifikasi sumber data.
- ***Examination*** merupakan pemeriksaan, dilakukan untuk menentukan filterisasi data pada bagian tertentu dari sumber data, filterisasi data dilakukan dengan melakukan perubahan bentuk data namun tidak melakukan perubahan pada isi data karena keaslian data merupakan hal yang sangat penting.
- ***Analysis*** merupakan analisis, merupakan tahap untuk melakukan penentuan tentang di mana data tersebut dihasilkan, oleh siapa data tersebut dihasilkan, bagaimana data tersebut dihasilkan, dan kenapa data tersebut dihasilkan.
- ***Presentation*** merupakan presentasi, dilakukan dengan menyajikan informasi yang dihasilkan dari tahap analisis. Tahap presentasi dilakukan setelah diperoleh barang bukti digital dari proses pemeriksaan dan dianalisis. Selanjutnya pada tahap ini dilakukan pelaporan hasil analisis yang meliputi penggambaran tindakan yang dilakukan, penjelasan mengenai *tool*, dan metode yang digunakan, penentuan tindakan pendukung yang dilakukan, dan memberikan rekomendasi untuk perbaikan kebijakan, metode, *tool*, atau aspek pendukung lainnya pada proses tindakan digital forensik.

1.0.4 Systematic Digital Forensics Investigation Model (SRDFIM)

Merupakan salah satu metode forensik yang dapat digunakan, SRFDM di bangun berdasarkan *framework* yang diperlukan dalam dunia forensik dan berdasarkn *framework* forensik yang ada (M. M. Pollitt, 1995). Metode tersebut memiliki 11 step yang dilakukan dalam forensik, dimulai dari *preparation*, *securing the scene*, *survey and*

recogniation, *documentation of scene*, *comunication shielding*, *evidance colection*, *preservation*, *examination*, *analysis*, *presentation*, dan *result*. Gambar 1.2 merupakan proses tahapan proses SRDFIM.



Gambar 1.2 Metode SRDFIM

1.0.5 Integrated Digital Forensic Investigation Framework (IDFIF)

Integrated Digital Forensic Investigation Framework atau disingkat IDFIF merupakan *framework* yang telah dikembangkan sebagai standar metode penyelidikan (Ruuhwan, Riadi, & Prayudi,

2017). IDFIF memiliki 4 tahap yaitu *pre-process*, *proactive*, *reactive* dan *post*-proses.

- **Pre-proses** dalam proses ini terdapat 3 proses yaitu *notification*, *authorization,* dan *preparation*.
- **Proactive** dalam proses ini terdapat beberapa proses seperti *collection, crime scine investigation, presenation, analysis, preliminary report, securing the scene,* dan *detection of incident.*
- **Reactive** dalam proses ini terdapat beberapa proses seperti *identification, collection & Acquition, presenation, examination, analysis,* dan *presentation*.
- **Post-process** terdapat tiga proses terakhir yaitu *conclusion*, *recontruction*, dan *dissemination*.

1.0.6 Integrated E-mail Forensic Analysis Framework (IEFAF)

1.3.1. Static Forensicss

Static forensicss memiliki arti yang sama dengan forensik digital tradisional, *static forensicss* yaitu melakukan memeriksa duplikat yang disebut salinan disk untuk mengambil konten memori, seperti *file* yang dihapus, riwayat penelusuran *web*, fragmen *file*, koneksi jaringan, membuka *file*, riwayat *login* pengguna, dan lain-lain. Proses dalam membuat garis waktu yang memberikan pandangan yaitu statika parsial atau ringkasan tentang aktivitas yang dilakukan pada sistem korban sebelum mematikannya.

Analisis statis berbagai jenis perangkat lunak dan perangkat keras seperti Fundl, regcon untuk digunakan melakukan *dump* memori dan memilih data sebagai bahan pembuktian untuk dilakukan analisis dan laporan. Data forensik diperoleh dengan menggunakan berbagai jenis perangkat eksternal seperti USB, hardisk eksternal atau CD, dan DVD. Data tersebut dibawa ke

laboratorium forensik yang akan digunakan investigator untuk melakukan berbagai jenis operasi/langkah untuk menganalisis data forensik.

1.3.2. Live Forensicss

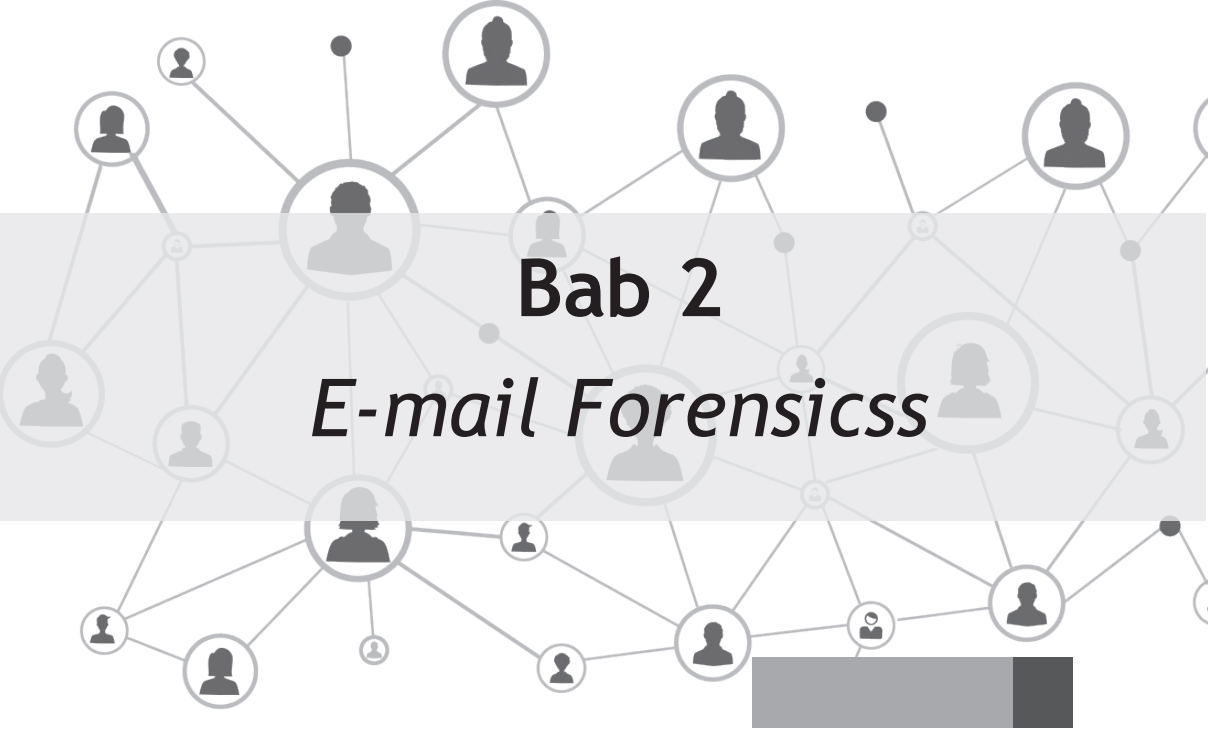
Live forensicss merupakan salah satu cara yang dapat digunakan untuk mendapatkan barang bukti secara langsung, informasi dikumpulkan, dianalisis, dan laporan dihasilkan. Sementara sistem yang digunakan tetap berfungsi, alat yang digunakan untuk melakukan analisis *live forensicss* dapat memberikan gambaran yang sangat jelas tentang pengetahuan seperti *dump* memori, proses yang berjalan, koneksi jaringan dan tidak terenkripsi. Versi *file* terenkripsi, sementara konten memori tersebut tidak dapat diperoleh dengan benar dalam analisis statis. Analisis *live forensicss* mampu memberikan konsistensi dan integritas data forensik. Informasi yang dikumpulkan dapat digunakan dengan berbagai cara untuk menghasilkan bukti forensik dan tindakan yang dilakukan oleh pengguna secara langsung.

1.4 Rangkuman

Digital *forensicss* adalah salah satu cabang ilmu forensik yang dapat digunakan untuk mendapatkan barang bukti pada pelaku kejahatan untuk melakukan identifikasi, menjaga keaslian, menganalisis, dan memberikan laporan.

1.5. Soal Latihan

1. Jelaskan secara singkat tentang arti istilah digital forensik.
2. Jelaskan secara singkat tentang pengertian digital forensik menurut Anda.
3. Jelaskan perbedaan *live forensicss* dan *static forensicss*.



Bab 2
E-mail Forensicss

Tujuan Instruksional Umum:

1. Mahasiswa/i mampu menjelaskan tentang *Forensik E-mail.*

Tujuan Instruksional Khusus:

1. Mahasiswa/i mampu menjelaskan istilah standar dalam *Forensik E-mail.*
2. Mahasiswa/i mampu memahami latar belakang, definisi, aplikasinya, dan klasifikasi dalam *Forensik E-mail.*
3. Mahasiswa/i dapat menjelajahi bidang investigatoran *Forensik E-mail* yang sedang berkembang.

2.1. Pengertian *E-mail*

Teknologi internet menyediakan banyak fasilitas dan kemudahan dalam berkomunikasi, dengan perkembangan teknologi informasi dan komunikasi khususnya di dunia internet, memungkinkan seseorang mengirim surat tanpa melalui kantor pos, yaitu melalui surat elektronik atau disebut dengan *e-mail*. *E-mail* merupakan gabungan dari 2 kata

yaitu "e" kepanjangan dari elektronik dan "*mail*" berasal dari serapan bahasa asing yang artinya *mail*/surel/ratel. Maka *e-mail* dapat diartikan *e-mail* adalah surat digital yang dapat dikirim menggunakan media internet yang tidak terhalang oleh ruang dan waktu. *E-mail* memiliki protokol dan standar yang sering dipakai dalam pengiriman dan pembacaan pesan, agar pesan tersebut sampai tujuan.

Syarat untuk mengirim *e-mail* adalah memiliki alamat *e-mail*. Selain bertukar pesan *e-mail*, internet juga dapat berkirim dokumen, membuat blog, Facebook, Twitter, dan lain-lain. *Electronic mail* merupakan kegiatan yang paling sederhana di antara semua kegiatan di internet. *E-mail* didasarkan pada *file* ASCII (*American Standard Code For Information Interchange*) yakni teks sederhana yang dapat ditangani dengan program komunikasi dasar (Wijaya, 2009).

Pesan *e-mail* seluruhnya terdiri dari garis karakter ASCII. Setiap baris dapat berisi hingga 998 karakter dan diakhiri oleh karakter kontrol CR dan LF RFC 5322. Baris yang menyusun *header* muncul sebelum badan pesan. Garis kosong, yang hanya berisi karakter CR dan LF, menandai akhir dari *header*. Struktur *e-mail* terdiri dari dua bagian yaitu *header* yang memainkan peran yang sama dengan kop surat dalam surat biasa di dalamnya berisi metadata tentang pesan. Kedua yaitu *body* yang berisi pesan itu sendiri, terkadang pada *body* terdapat *signatur* (Didik & R, 2008).

2.2. Sejarah *E-mail*

Perjalanan perkembangan *e-mail* :

1961 MIT mendemonstrasikan Compatible Time-Sharing System (CTSS). Multiple user login ke IBM 7094 dari terminal dial-up, dan menyimpan *file* secara *online* ke disk. Memberikan bentuk baru untuk *user* dalam berbagi informasi.

1965 *multiple user* dari *time-sharing mainframe computer* dapat saling berkomunikasi.

1966 *e-mail* berkembang cepat menjadi *network e-mail*, mengizinkan *user* saling bertukar surat antarkomputer yang berbeda.

1969 jaringan komputer ARPANET memberikan kontribusi terhadap pengembangan *e-mail*. (Transfer antar system *e-mail* yang sukses).

1971 Ray Tomlinson memperkenalkan penggunaan tanda @ untuk memisahkan nama *user* dan komputer. ARPANET secara signifikan meningkatkan popularitas dari *e-mail*, dan membuatnya menjadi killer app dari ARPANET.

2.3. Format *E-mail*

E-mail terdiri dari 2 bagian :

Header — Terstruktur menjadi beberapa *fields* seperti *summary*, *sender*, *receiver*, dan informasi lain mengenai *e-mail* tersebut.

Body — isi surat sebagai teks yang tak terstruktur, juga berisi *signature block* di akhir.

Header E-mail mencakup setidaknya bidang-bidang berikut:

- Dari / dari: Alamat *e-mail*, dan secara opsional nama pengirim
- Kepada / kepada: Alamat *e-mail* [es], dan secara opsional nama [s] dari penerima pesan [s]
- Subjek: Ringkasan singkat isi pesan
- Tanggal: Waktu dan tanggal setempat saat pesan ditulis

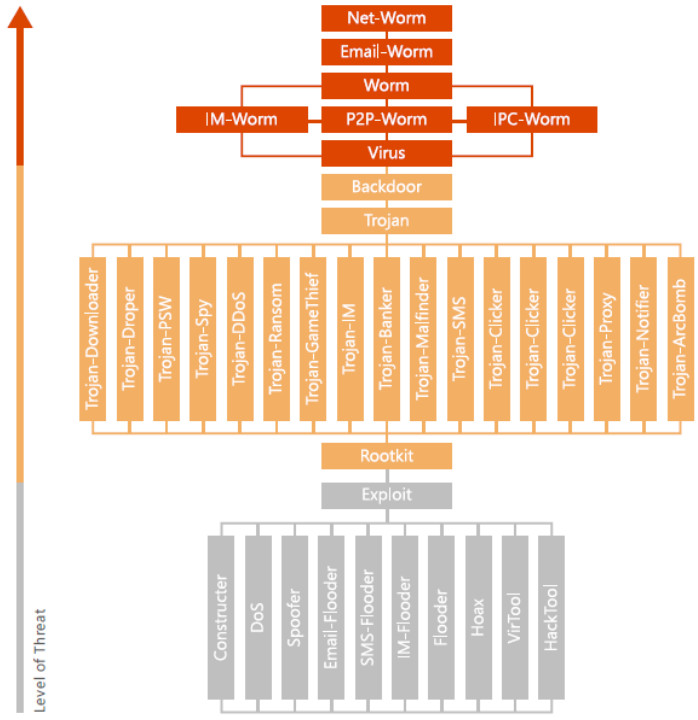
Bidang *header* umum lainnya meliputi:

- Tembusan: Salinan karbon
- Bcc: Blind Carbon Copy

- Diterima: Melacak informasi yang dihasilkan oleh server *e-mail* yang sebelumnya telah menangani pesan
- Content-Type: Informasi tentang bagaimana pesan harus ditampilkan
- Balas ke: Alamat yang harus digunakan untuk membalas pengirim.
- X-Face: Ikon kecil.

2.4. Ancaman *E-mail*

Terdapat beberapa ancaman yang digunakan *cyber crime* untuk menyerang pengguna *e-mail* salah satunya.



Gambar 2.1 Level Ancaman (State & Security, 2017)

Gambar 2.1 merupakan level ancaman yang dapat menyerang *e-mail*. Selain jenis ancaman *e-mail* dan motivasi peretas, memahami teknik penyebar penyerang adalah bagian besar dari strategi holistik. Penyerang mendapatkan akses ke target kredensial yang mereka inginkan dalam empat cara:

1. Bruch Force:

   Berulang kali mencoba kombinasi nama pengguna dan kata sandi menggunakan alat otomatis dan daftar kata kunci yang dikumpulkan selama riset *online* dari target.

2. Pasing Fraud (Penipuan):

   Menggunakan daftar kata kunci yang sama untuk menulis *e-mail* yang mengarahkan penerima untuk berinteraksi dengan lembaga keuangan terkenal, jejaring sosial, atau vendor dengan mengklik tautan.

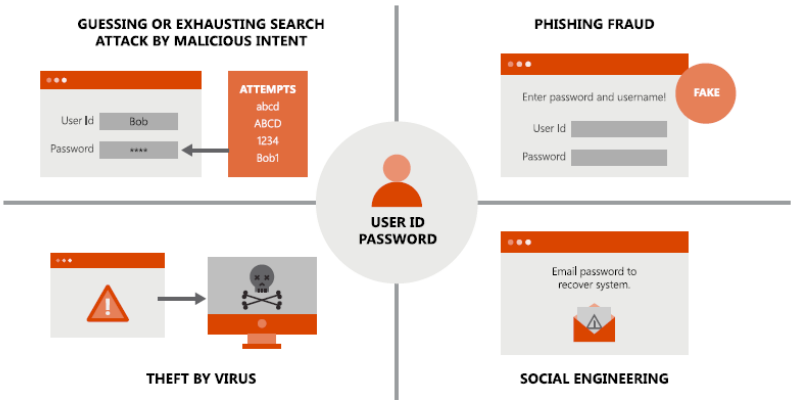
3. Serangan Virus:

   Menanamkan virus dalam *e-mail* untuk mengumpulkan informasi yang diperlukan di belakang layar atau memberikan akses jaringan yang memungkinkan pengumpulan data

4. Sosial Engginering:

   Menggunakan permintaan langsung yang disamarkan sebagai kontak tepercaya

Mari kita lihat masing-masing metode serangan ini secara lebih detail, menyoroti jenis ancaman yang digunakan di masing-masing metode serangan. Ingat bahwa penyerang adalah serbaguna, biasanya menggunakan berbagai metode dan kombinasi jenis ancaman

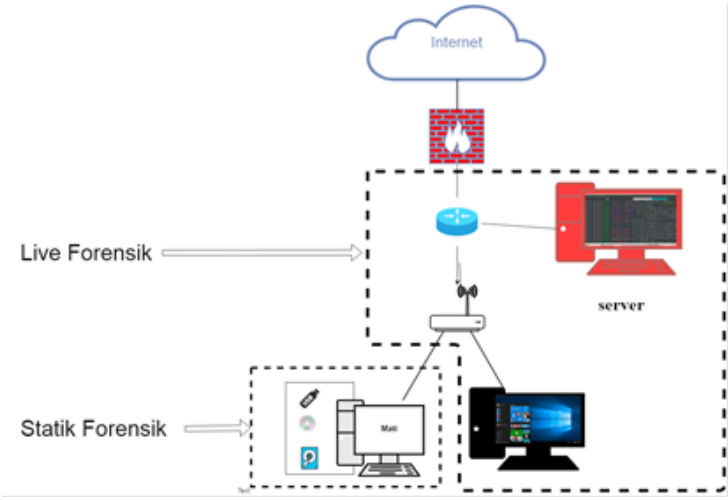


Gambar 2.2 Ancaman pada E-mail

Gambar 2.2 merupakan beberapa ancaman serangan yang dapat digunakan oleh pelaku kejahatan.

2.5. Rangkuman

E-mail merupakan salah satu cara yang dapat digunakan untuk bertukar informasi seperti data, tugas, dan lain-lain. *E-mail* terdiri atas 2 bagian, yaitu *header* dan *body*. *E-mail* tidak bia dianggap aman bagi pengguna, banyak kejahatan menggunakan media *e-mail* untuk menipu, memberi virus, dan lain-lain. Forensik pada *e-mail* dapat dilakukan dengan 2 cara yaitu dengan cara *live forensicss* dan *static forensicss*. Berikut ringkasan tentang *live forensicss* dan *static forensicss*.



Gambar 2.3 Statik dan Live forensicss

Gambar 2.3 Merupakan ruang lingkup analisis *live forensicss* dan *static forensicss*.

2.6. Soal Latihan

1. Jelaskan secara singkat tentang arti dari *e-mail* dan penggunaannya.
2. Jelaskan secara singkat ancaman yang dapat terjadi pada *e-mail*.
3. Jelaskan perbedaan *live forensicss* dan *static forensicss*.

Bab 3
Barang Bukti Digital

Tujuan Instruksional Umum:

1. Mahasiswa/i mampu menjelaskan tentang *Forensik E-mail.*

Tujuan Instruksional Khusus:

1. Mahasiswa/i mampu menjelaskan istilah standar dalam *Forensik E-mail.*
2. Mahasiswa/i mampu memahami latar belakang, definisi, aplikasinya, dan klasifikasi dalam *Forensik E-mail.*
3. Mahasiswa/i dapat menjelajahi bidang investigatoran *Forensik E-mail* yang sedang berkembang.

3.1. Pengertian

Pada kejahatan *cybercrime* akan meninggalkan barang bukti. Barang bukti kejahatan tersebut dapat diangkat menggunakan ilmu digital forensik. Digital forensik adalah penggunaan ilmu dan metode untuk menemukan, mengumpulkan, mengamankan, menganalisis, menginterpretasi, dan mempresentasikan barang bukti digital yang

terkait dengan kasus yang terjadi untuk kepentingan rekonstruksi kejadian serta keabsahan proses peradilan (Agarwal & Gupta, 2011). Barang bukti dapat berupa bukti digital dan elektronik. Bukti digital dapat dilihat ketika proses kejahatan berlangsung ataupun ketika bukti digital sudah disimpan, bukti digital dapat dilakukan penanganan khusus dengan ilmu digital forensik dengan menggunakan *tools* untuk memecahkan dan penarikan kesimpulan dari kasus kejahatan pada bukti digital yang didapatkan.

Hukum tentang kejahatan *cybercrime* diatur dalam undang-undang tentang ITE. Kejahatan ITE dapat dijerat hukum secara perdana maupun perdata sesuai tingkat kejahatan yang dilakukannya. Penangkap para pelaku *cybercrime* oleh pihak yang berwenang berdasarkan bukti-bukti kejahatan yang tersimpan di dalam *smartphone* sebagai barang bukti pada persidangan. Hampir semua pembuktian perkara pidana, selalu bersandar pada pemeriksaan alat bukti. Pembuktian dengan minimal dua alat bukti (Yahya, 2007).

3.2. Jenis-Jenis Bukti Digital

Barang bukti digital bersifat digital yang diekstrak dari barang bukti elektronik. Di dalam Undang-Undang No. 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik dikenal dengan istilah informasi elektronik dan dokumen elektronik. Berikut beberapa contoh barang bukti digital yaitu: *Logical file, Deleted File, Lost File, File slack, Log File, Encrypted File, Steganography file, Office file, Audio File, Video File, Image file, E-mail, User ID* dan *Password*, *Short Message Service (SMS), Multimedia Message Service (MMS), Call Logs.*

3.3. LOG

Log merupakan keamanan komputer berisi informasi tentang peristiwa yang terjadi dalam sistem dan jaringan organisasi. Log terdiri dari beberapa jenis seperti berikut (FC-Council, n.d.):

a. Operating system (OS)

Operating system log merupakan catatan pada sistem o*perating* untuk mengidentifikasi dan menyelidiki aktivitas mencurigakan yang melibatkan *host* tertentu, OS log yang mengandung sistem operasi seperti pada server, *workstation,* dan perangkat jaringan (Grance, Chevalier, Kent, & Dang, 2005).

b. Aplication System

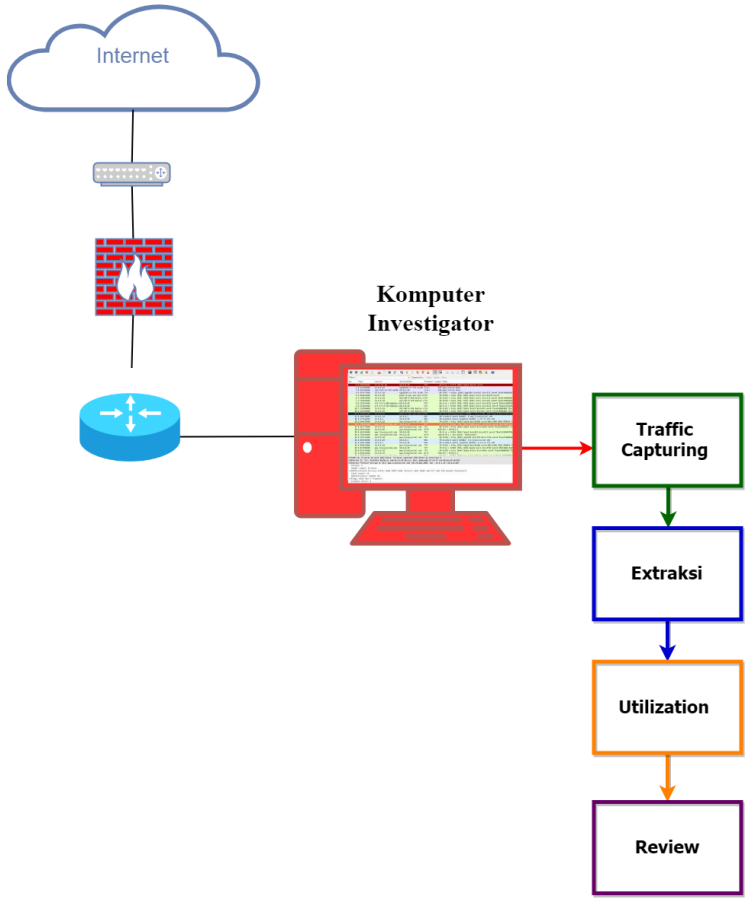
Log sistem aplikasi merupakan catatan perincian luas tentang karakteristik spesifik aktivitas aplikasi, dan sangat membantu dalam mengidentifikasi karakteristik serangan dari aplikasi yang kurang umum. Log aplikasi seperti log aplikasi yang berjalan pada sistem dan server seperti server *e-mail*, server database, dan lain-lain (FC-Council, n.d.).

c. *Security Software Log*

Log perangkat lunak keamanan berbasis jaringan dan *host*, seperti *anti malware software, intrusion detection and prevention system, remoteaccess software, webproxies, vulnerability management software, aothentication servers, router, firewalls, network quarantine servers* (FC-Council, n.d.).

3.4. Proses Mendapatkan Barang Bukti

Berikut yang digunakan untuk mendapatkan barang bukti adalah sebagai berikut.



Gambar 3.1 Skema Pengumpulan Barang Bukti

Gambar 4.1 merupakan skema yang digunakan untuk mendapatkan barang bukti digital dengan metode *live forensicss*. Proses *capturing* trafik jaringan dilakukan oleh komputer investigator dalam jaringan melalui perangkat *router*. Alat yang digunakan untuk *capturing* paket data

adalah *Wireshark* dan *Networkminer.* Setelah di-*capturing* kemudian dilakukan *Acquisition* pada trafik jaringan dan kemudian disimpan agar menghindari terjadinya perubahan informasi dalam proses analisis.

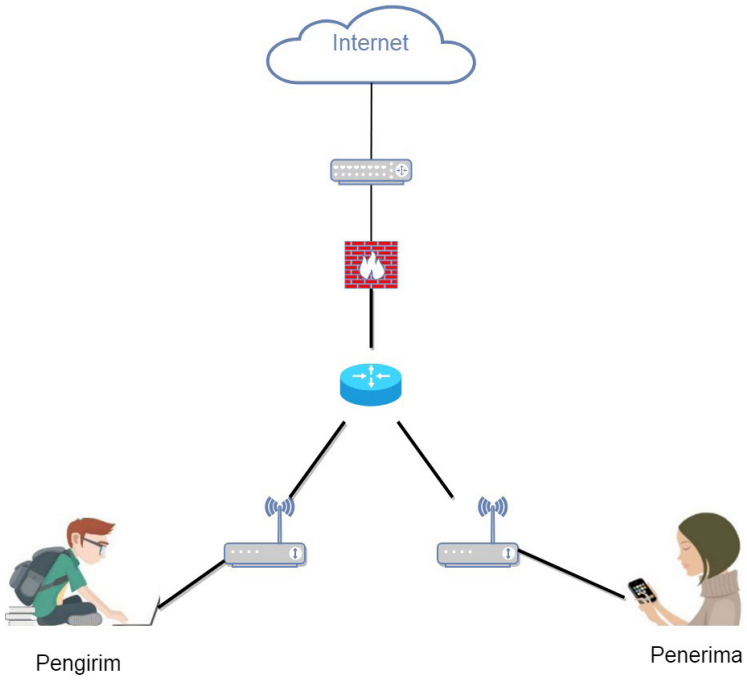
Setelah data disimpan maka dilakukan analisis guna untuk menemukan bukti kejahatan berdasarkan *IP Address*, *Timestamp*, *Port, MAC address*. Tahap selanjutnya adalah dilakukan proses validasi terhadap bukti digital yang ditemukan. Setelah dilakukan validasi maka dilakukan proses analisis dari barang bukti digital yang ditemukan.

3.4.1. *Acquisition*

Langkah awal dalam proses simulasi dengan melakukan *capturing* paket pada jaringan menggunakan *tools forensicss wireshark* dan *networkminer*. Proses pengumpulan data disajikan pada gambar 3.2.

3.4.2. Pengujian

Pengujian merupakan proses pengujian *tools* dangan metode *live forensicss* dan kemudian dijalankan untuk melakukan identifikasi informasi yang relevan dari data yang dikumpulkan sambil menjaga integritasnya. Pengujian ini menggunakan *tools forensicss Wireshark* dan *Networkminer* untuk melakukan *capturing* paket data yang melintas pada jaringan. Hasil *capturing* tersebut merupakan log yang akan digunakan untuk melakukan analisis paket. Gambar 3.2 merupakan proses pengirimanan *e-mail*.



Gambar 3.2 Proses Pengiriman E-mail

Gambar 3.2 merupakan tampilan proses pengiriman *e-mail* dari pelaku dan diterima oleh korban. Hasil pengujian tersebut melakukan proses filter untuk melihat paket *e-mail* yang melintas pada jaringan.

3.4.3. Analisis

Analisis merupakan proses analisis berdasarkan hasil pemeriksaan yang telah dilakukan. Pada proses analisis ini melakukan analisis terhadap log hasil *capturing tools wireshark* dan *networkminer* yang sudah disimpan. Hasil log yang dicari seperti *ip address*, *timestamp*, *port*, dan *mac address*. Analisis log dilakukan untuk analisis verifikasi data dengan menggunakan windump.

3.4.4. Laporan

Laporan merupakan tahap pelaporan tahap dokumentasi terhadap hasil investigatoran yang telah dilakukan selama analisis forensik berlangsung dengan menggunakan metode NIST. Proses pelaporan analisis didapat meliputi gambaran tindakan yang dilakukan, penjelasan mengenai alat dan prosedur yang dipilih, penentuan tindakan lain yang perlu dilakukan seperti pemeriksaan berdasarkan data tambahan, mengamankan celah yang teridentifikasi, meningkatkan kontrol keamanan yang ada, dan memberikan rekomendasi untuk perbaikan kebijakan, alat, prosedur, dan aspek lain dari proses forensik,

3.5. Rangkuman

Kejahatan yang dilakukan oleh *cybercrime* pasti akan meninggalkan barang bukti. Maka untuk mendapatkan barang bukti kita memerlukan alat yang mendapatkan barang bukti tersebut dan dapat menjaga keaslian dari barang bukti yang ditemukan. Barang bukti pada *file*, gambar, dokumen, pesan, *e-mail,* dan lain-lain.

3.6. Soal Latihan

1. Jelaskan apa yang dimaksud dengan *cybercrime* dan tujuannya.
2. Jelaskan dan sebutkan barang bukti yang dapat digunakan dalam persidangan.

Bab 4
Akuisisi *E-mail* sebagai Barang Bukti Digital

Tujuan Instruksional Umum:

1. Mahasiswa/i mampu menjelaskan tentang Akuisi *E-mail.*

Tujuan Instruksional Khusus:

1. Mahasiswa/i mampu menjelaskan langkah atau proses akusisi pada *E-mail*.
2. Mahasiswa/i mampu memahami latar belakang, definisi, aplikasinya dan klasifikasi dalam *Akuisis E-mail.*
3. Mahasiswa/i dapat menjelajahi bidang akusisi pada *E-mail* yang sedang berkembang.

4.1. *Preprocessing*

Preprocessing digunakan untuk melakukan *capturing* paket data yang melintas pada jaringan internet, maka diperlukan instal, dan konfigurasi *software* seperti *Wireshark* dan *Networkminer*.

4.2. Metode Akuisisi Barang Bukti

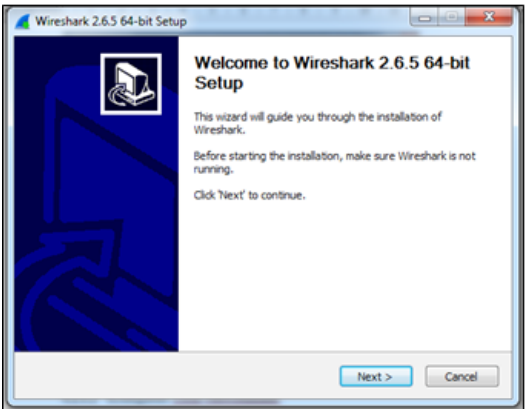
Pada proses akuisisi barang bukti alat yang diperlukan, akuisisi yang akan dilakukan pada investigatoran ini adalah melakukan akuisisi terhadap aktivitas atau log *e-mail* pada jaringan. Metode yang digunakan untuk mendaptkan log yaitu menggunakan *live forensicss*. Dan metode untuk mengumpulkan menggunakan metode *National Institute of Standards and Technology* (NIST).

4.3. Proses Akuisisi

Proses *Akuisition* ini adalah melakukan instalasi dan konfigurasi *tools* forensik seperti *wireshark*, *networkminer*, membuat akun *e-mail*, persiapan *smartphone* android.

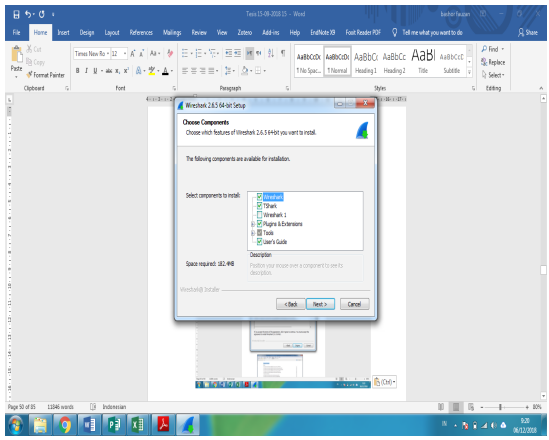
4.3.1. Instalasi *Wireshark*

Wireshark adalah program Network Protocol Analyzer yang berfungsi untuk menganalisis paket pada jaringan. Program ini dapat merekam semua paket yang lewat serta menyeleksi dan menampilkan data tersebut sedetail mungkin. Tahap-tahap proses instalasi aplikasi *wireshark* Gambar 4.3 tampilan halaman awal instalasi.



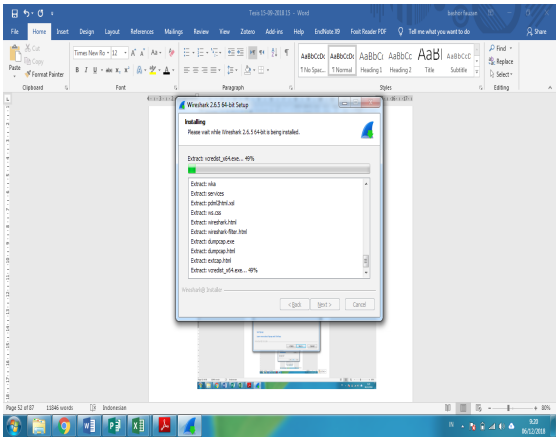
Gambar 4.1 Halaman Awal Instalasi Wireshark

Gambar 4.1 merupakan tahap untuk memilih komponen-komponen yang harus dipasang sesuai dengan versi yang akan diinstal.



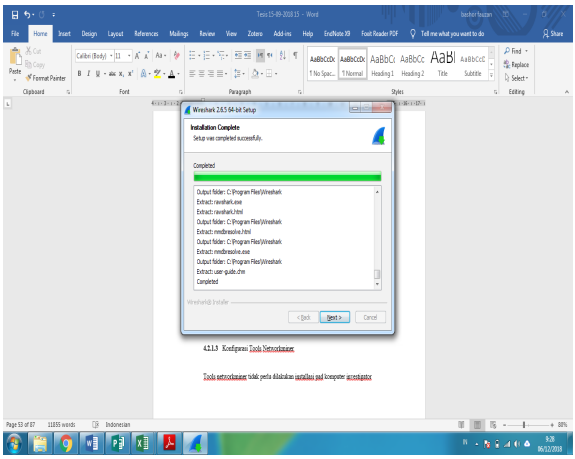
Gambar 4.2 Komponen–Komponen Wireshark

Gambar 4.2 memperlihatkan proses akhir pada instalasi *Wireshark* dan tunggu sampai proses mencapai 100%.



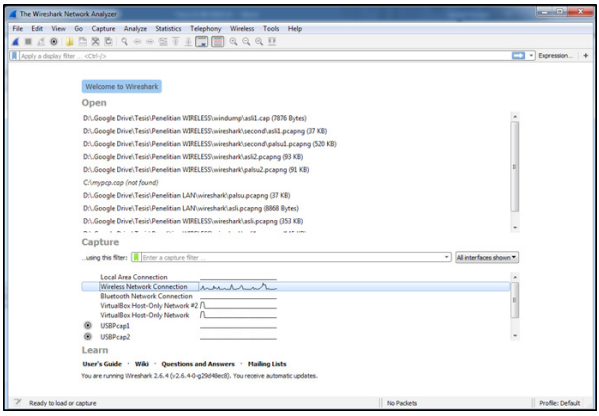
Gambar 4.3 Proses Akhir Instalasi Wireshark

Gambar 4.5 merupakan proses akhir pada proses instalasi *wireshark*. Tunggu hingga selesai maka akan muncul gambar 4.6.



Gambar 4.4 Tampilan Selesai Proses Instalasi

Gambar 4.4 merupakan tampilan sudah selesai melakukan instalasi dan sudah dapat digunakan. Dan akan tampil seperti gambar 4.6.

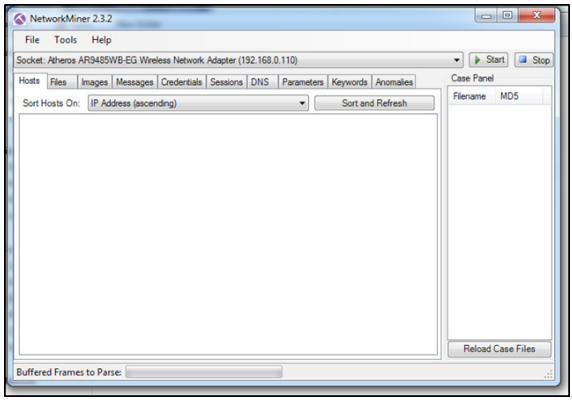


Gambar 4.5 Halaman Utama Aplikasi Wireshark

Gambar 4.6 merupakan tampilan utama *tools wireshark*. Kemudian untuk melakukan *capturing* perlu memilih jaringan yang akan digunakan. Pada investigatoran ini melakukan *capturing* paket yang melintas pada jaringan *wireless*.

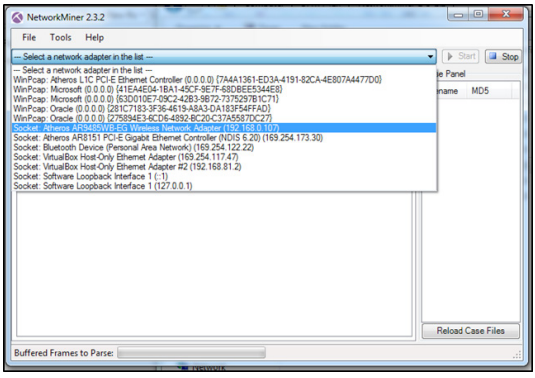
4.3.2. Instalasi *Networkminer*

Tools Networkminer tidak perlu dilakukan instalasi pada komputer investigator hanya perlu dijalankan. *Software Networkminer* yang diinstal juga pada sistem operasi windows 7 yang akan digunakan untuk *capturing* log dan analisis paket data yang melintas pada jaringan internet. *Networkminer* merupakan *tools forensics*s portable. Gambar 4.7 merupakan tampilan utama *Networkminer*.



Gambar 4.6 Halaman Utama *Networkminer*

Gambar 4.6 merupakan halaman utama pada *tool Networkminer*. Pada halaman utama terdapat menu-menu untuk melakukan analisis *network* forensik untuk mengawasi lalu lintas *network*.

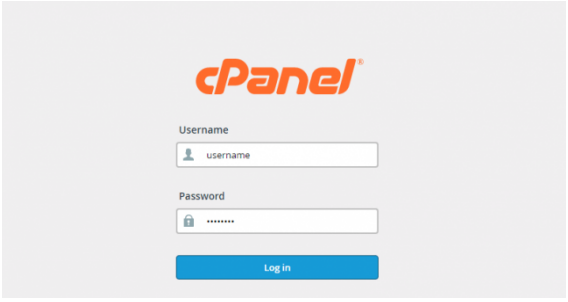


Gambar 4.7 Halaman Menu Analisis pada Networkminer

Gambar 4.7 merupakan Halaman Menu Analisis pada *Networkminer*. Kemudian dilakukan konfigurasi *network* apa yang akan digunakan. Pada kotak merah adalah jaringan yang akan saya *capture* aktivitas paket data pada jaringan.

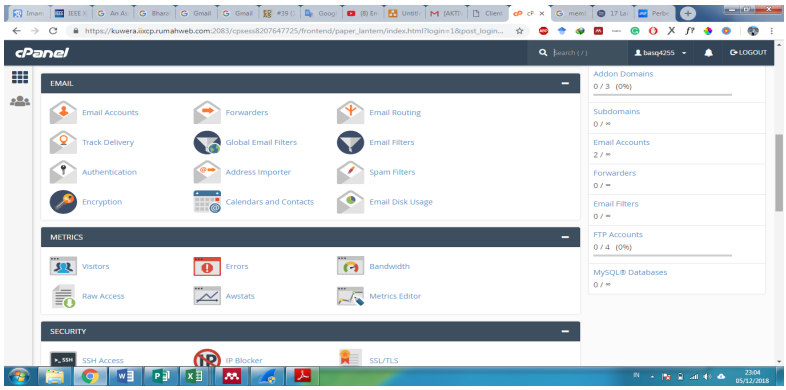
4.3.3. Konfigurasi *E-mail*

E-mail yang digunakan pada investigatoran ini adalah webmail dari *hosting* bashorfauzan.com. Pertama membuat nama *e-mail* pertama yaitu official@bashorfauzan.com yang akan digunakan sebagai penerima. Alamat kedua yang bertindak sebagai pengirim adalah akun *e-mail* support@bashorfauzan.com. Berikut adalah konfigurasi membuat *e-mail* akun *e-mail* yang akan digunakan. Berikut adalah proses konfigurasi *e-mail*.



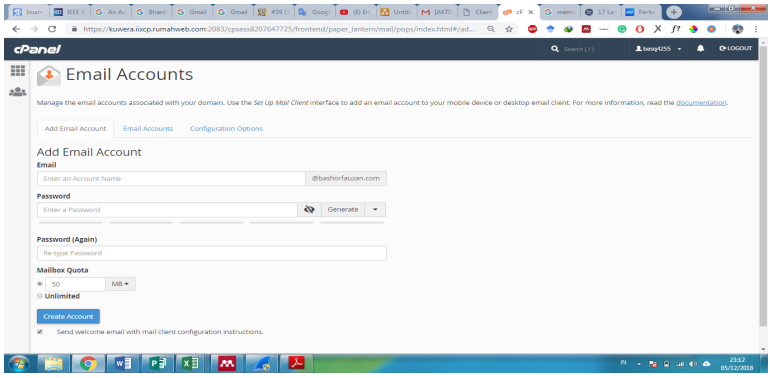
Gambar 4.8 Login ke cPanel

Gambar 4.9 merupakan tampilan login pada cpanel. Pada tampilan cpanel kita diminta untuk memasukkan *username* dan *password*. Jika sudah dimasukkan pilih tombol *log in*. Jika benar maka akan langsung masuk ke dalam menu utama cpanel. Seperti gambar 4.10.



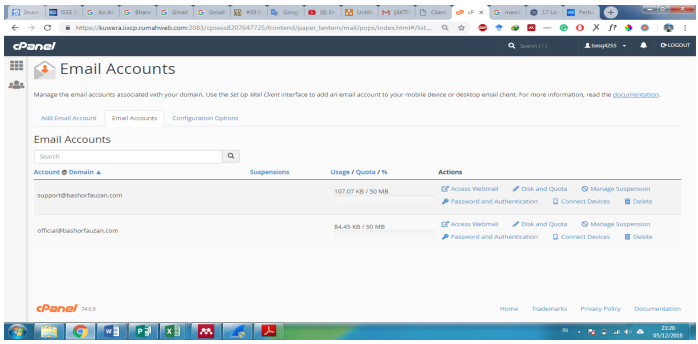
Gambar 4.9 Menu Utama cPanel

Gambar 4.10 merupakan tampilan menu utama pada cpanel setelah berhasil *login*. Pada menu utama cpanel terdapat ikon-ikon yang dapat mempermudah melakukan manajemen data *file* pada server. Selajutnya mencari ikon *mail account*, dapat dilihat pada gambar 4.10.



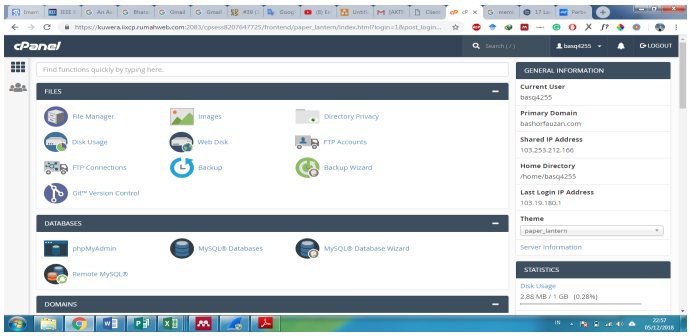
Gambar 4.10 Ikon E-mail

Gambar 4.10 merupakan tampilan ikon menu tentang manajemen *e-mail*. Pada kotak merah merupakan ikon *e-mail account* yang akan digunakan untuk membuat akun *e-mail* baru. Gambar 4.11 merupakan proses membuat akun *e-mail* baru.



Gambar 4.11 Membuat Akun *E-mail* Baru

Gambar 4.11 merupakan tampilan yang digunakan untuk membuat akun *e-mail* baru. Data yang harus dimasukkan adalah alamat akun *e-mail* baru, dapat dilihat pada kotak warna merah. Kemudian harus memasukkan sebanyak *password* 2 kali, dapat dilihat pada kotak warna biru. Setelah selesai dapat dilihat pada tab *E-mail Account*. Maka akan muncul seperti gambar 4.12.



Gambar 4.12 Merupakan Tampilan Akun E-mail

Gambar 4.12 merupakan tampilan akun *e-mail* yang telah berhasil dibuat, pertama akun *e-mail* dengan nama official@bashorfauzan.com dan akun support@bashorfauzan.com. Kedua akun *e-mail* tersebut akan digunakan untuk simulasi pengiriman *e-mail*.

4.1.4. *Smartphone*

Pada investigatoran ini menggunakan *smartphone* dengan sistem operasi android versi 8.0 atau Oreo. Dapat dilihat pada gambar berikut;

Gambar 4.13 Smartphone Android

Gambar 4.13 merupakan tampilan depan *smarphone* Xiomi Redmi S2. *Smartphone* ini akan digunakan untuk membuka *e-mail* yang dikirim seseorang.

4.4. Rangkuman

Alat dan bahan sangat diperlukan untuk melakukan proses forensik untuk mendapatkan barang bukti digital. Pada investigatoran ini menggunakan proses forensik berdasarkan metode NIST untuk mendapatkan barang bukti digital, dan mengunakan metode *live forensicss* untuk mendapatkan barang bukti.

4.5. Soal Latihan

1. Jelaskan dan sebutkan alat dan bahan yang digunakan.
2. Jelaskan proses akuisisi barang bukti menggunakan metode NIST.
3. Jelaskan barang bukti yang dapat ditemukan pada investigator.

Bab 5
Studi Kasus

Tujuan Instruksional Umum:

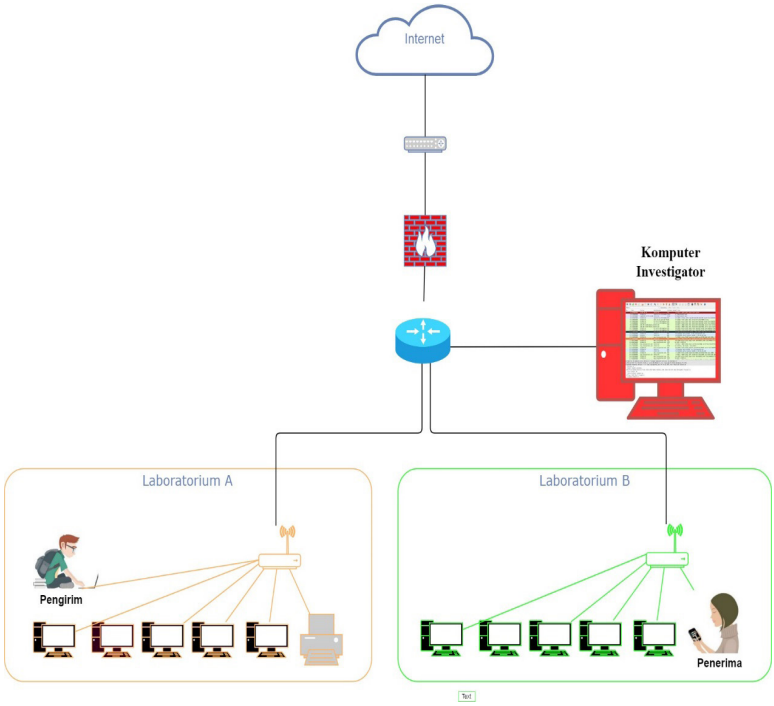
1. Mahasiswa/i mampu menjelaskan tentang penanganan kasus pada *E-mail*.

Tujuan Instruksional Khusus:

1. Mahasiswa/i mampu menjelaskan istilah kasus yang sedang terjadi pada kejahatan *E-mail*.
2. Mahasiswa/i mampu memahami latar belakang, definisi, masalah, dan barang bukti pada kejahatan *E-mail*.
3. Mahasiswa/i dapat menjelajahi kasus kejahatan email di lingkungan sekitar yang terus berkembang.

5.1. Skenario

Skenario yang akan digunakan pada investigatoran ini adalah melakukan pengiriman *e-mail*. Skenario ini dilakukan di lingkungan kampus Universitas Ahmad Dahlan. Skenario dapat dilihat pada gambar 5.1.



Gambar 5.1 Skenario Kasus

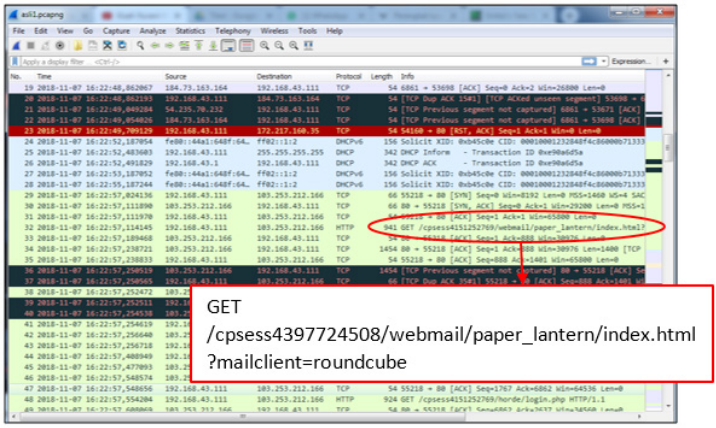
Gambar 5.1 merupakan proses simulasi yang dimulai dari penipu melakukan pengiriman *e-mail* kepada penerima. Jaringan yang digunakan adalah jaringan intranet dalam satu gedung. Kemudian masuk ke dalam server untuk di-*capture* paket yang melintas sebelum sampai pada penerima. Simulasi pengiriman *e-mail* dilakukan melalui jaringan pada laboratorium A dan diterima oleh pengguna pada jaringan laboratorium B.

5.2. *Examination E-mail Asli*

Examination ini dilakukan secara *live forensics*, skenario pertama investigatoran ini menggunakan *e-mail* asli yang dikirim oleh seseorang yang dapat dipertanggung-jawabkan. Berikut adalah tahap investigatoran:

5.2.1. *Examination* dengan *Wireshark*

*Tools forensic*s pertama pada proses *Examination* ini menggunakan *wireshark*. *Wireshark* merupakan alat yang mampu menangkap paket data yang melintas pada satu jaringan. Setelah dilakukan *capturing* maka dilakukan akuisisi log pada *wireshark*. Gambar 5.2 merupakan paket oleh yang berhasil di-*capturing wireshark*.



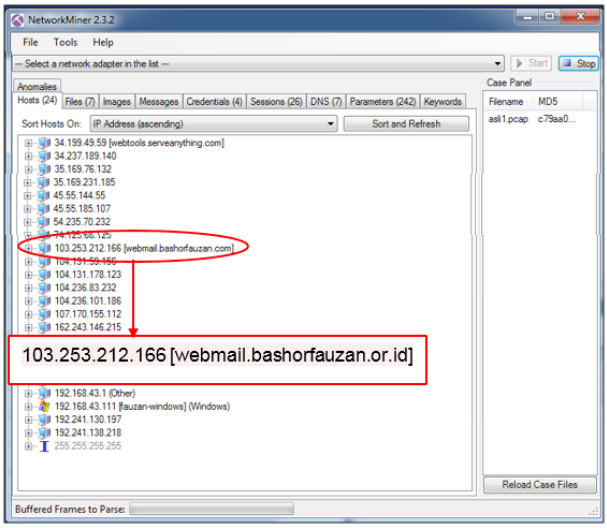
Gambar 5.2 Capturing E-mail Asli Wireshark

Gambar 5.2 merupakan proses *capturing* mengunakan *tools Wireshark*. Pada lingkaran merah merupakan hasil *capturing* paket yang berisi informasi webmail yang melintas pada jaringan. Ditemukan informasi berupa "GET/ cpsess4397724508/webmail/paper_lantern/ index.html?mailclient=roundcube" artinya bahwa *wireshark* berhasil dilakukan *capturing* paket *e-mail*.

5.2.2. *Examination* dengan *Networkminer*

Examination kedua yaitu menggunakan *tools Networkminer*. *Networkminer* memiliki kemampuan yang sama dengan *Wireshark* yaitu melakukan *capturing* paket data pada jaringan yang sedang berjalan. *Tool* ini mampu berjalan pada sistem operasi Windows 7 ultimate, berikut

adalah proses *Examination* menggunakan *Networkminer*. Gambar 5.3 merupakan hasil *capturing e-mail* asli.



Gambar 5.3 Capturing E-mail Asli Networkminer

Gambar 5.3 merupakan proses *capturing* menggunakan *tool Networkminer*. Pada lingkaran merah merupakan hasil *capturing* paket yang berisi informasi IP *Address* dan webmail yang didapatkan dari jaringan.

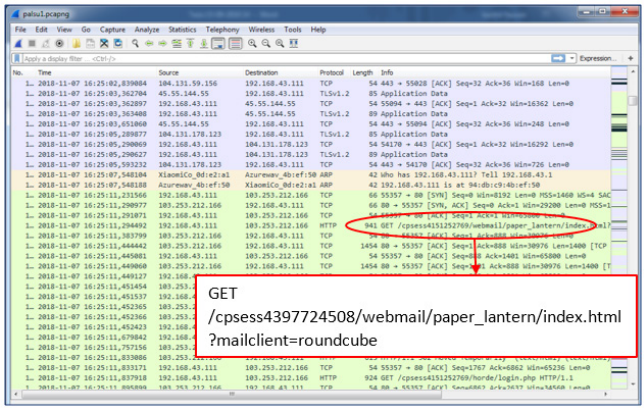
5.3. *Examination E-mail* Palsu

Examination kedua menggunakan *e-mail* palsu yang dikirim menggunakan webmail emkei.cz dan menggunakan alamat *e-mail* support@bashorfauzan.com.

5.3.1. *Examination* dengan *Wireshark*

Examination pada investigatoran yaitu melakukan pengiriman paket *e-mail* palsu kemudian dilakukan *capturing* menggunakan *wireshark*, paket yang dikirim dan diterima sangat banyak dalam

hitungan beberapa saat maka diperlukan *filtering* yang berguna untuk mempermudah mencari paket *e-mail* yang di-*capture*, berikut perintah filter yang digunakan adalah filter HTTP. Gambar 5.4 merupakan paket oleh yang berhasil di-*capturing wireshark*.

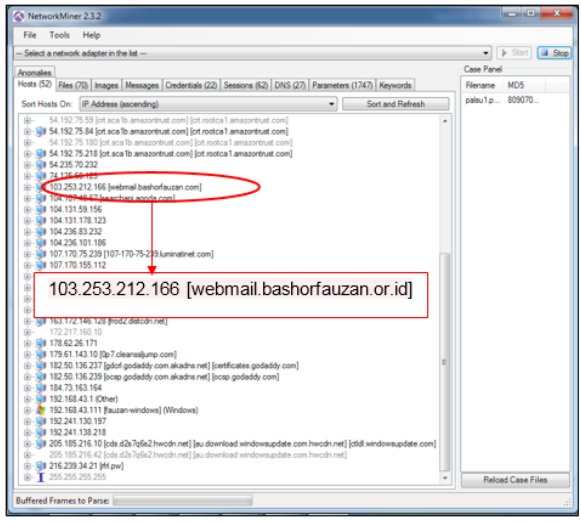


Gambar 5.4 Capturing E-mail Palsu Wireshark

Gambar 5.4 merupakan proses *capturing* menggunakan *tools Wireshark*. Pada lingkaran merah merupakan hasil *capturing* paket yang berisi informasi webmail yang melintas pada jaringan.

5.3.2. *Examination* dengan *Networkminer*

Examination kedua yaitu menggunakan *tools Networkminer*. *Networkminer* memiliki kemampuan yang sama dengan *Wireshark* yaitu melakukan *capturing* paket data pada jaringan yang sedang berjalan. *Tool* ini mampu berjalan pada sistem operasi Windows 7 ultimate, berikut adalah proses *Examination* menggunakan *Networkminer*.



Gambar 5.5 Capturing E-mail Palsu Networkminer

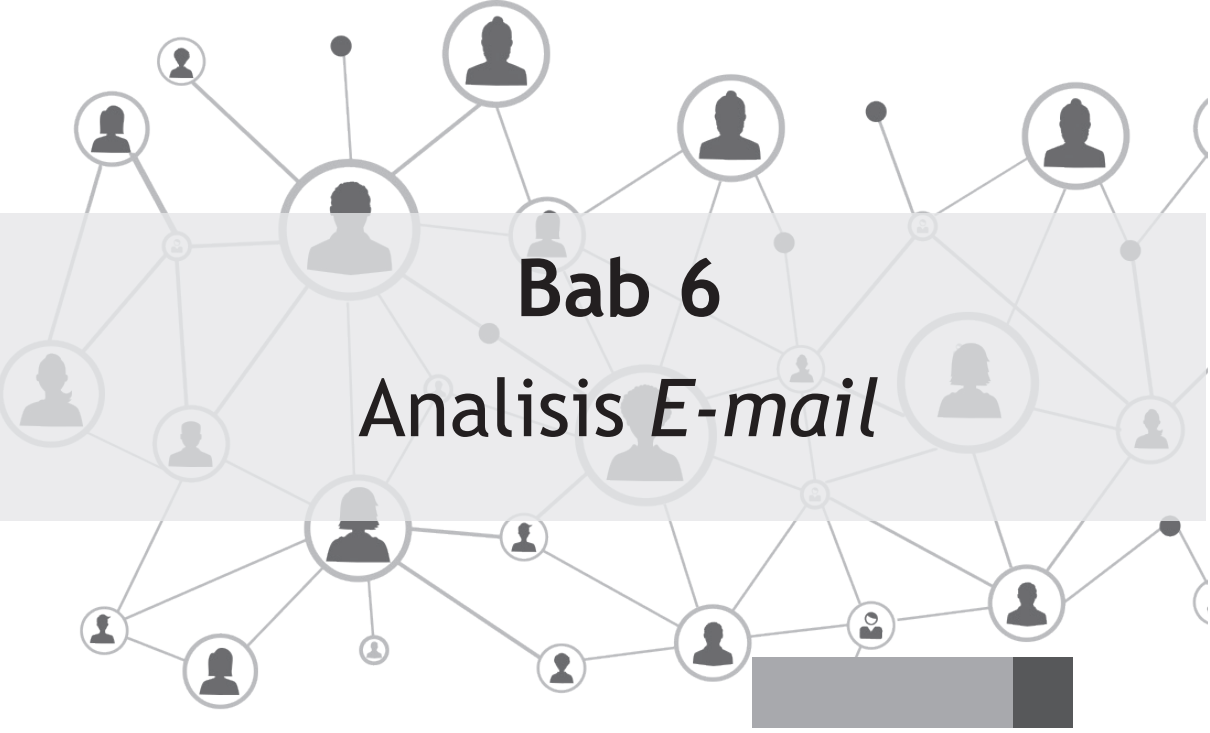
Gambar 5.5 merupakan proses *capturing* menggunakan *tools Networkminer*. Pada lingkaran merah merupakan hasil *capturing* paket yang berisi informasi IP *Address* dan webmail yang didapatkan dari jaringan.

5.4. Rangkuman

Hasil dari kedua *tools* tersebut memiliki perbedaan, *tools Wireshark* berhasil mendapatkan IP *Address*, *port*, *timestamp,* dan MAC *Address*. Sedangkan *tool Networkminer* berhasil IP *Address*, *port*, dan *timestamp*.

5.5. Soal Latihan

1. Jelaskan secara singkat skenario yang digunakan pada simulasi.
2. Jelaskan hasil barang bukti *e-mail* asli dan palsu.
3. Jelaskan perbedaan hasil yang ditemukan *tool wireshark* dan *networkminer*.



Bab 6
Analisis *E-mail*

Tujuan Instruksional Umum:

1. Mahasiswa/i mampu menjelaskan tentang analisis E-*mail*.

Tujuan Instruksional Khusus:

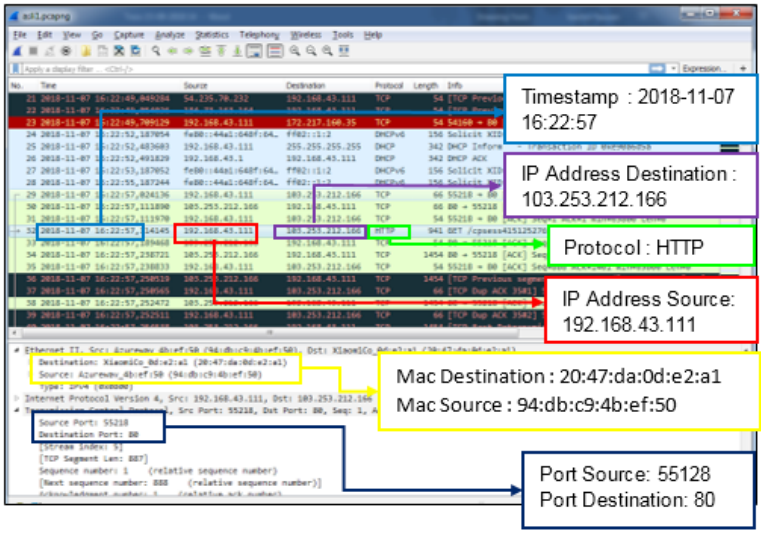
1. Mahasiswa/i mampu menjelaskan proses analisis pada *E-mail*.
2. Mahasiswa/i mampu memahami proses analisis pada email hingga mendaptkan barang butki yang sah.
3. Mahasiswa/i dapat menjelajahi bidang analisis email dan jenis-jenis kejahatan.

6.1. Analisis *E-mail* Asli

Tahap selajutnya adalah *analysis*, di mana tahap ini dilakukan untuk menganalisis hasil yang didapatkan oleh *tool forensicss Wireshark* dan *Networkminer*. *Analysis* dilakukan untuk memperoleh informasi yang berguna membahas pertanyaan-pertanyaan yang menjadi dorongan untuk melakukan pengumpulan dan pemeriksaan.

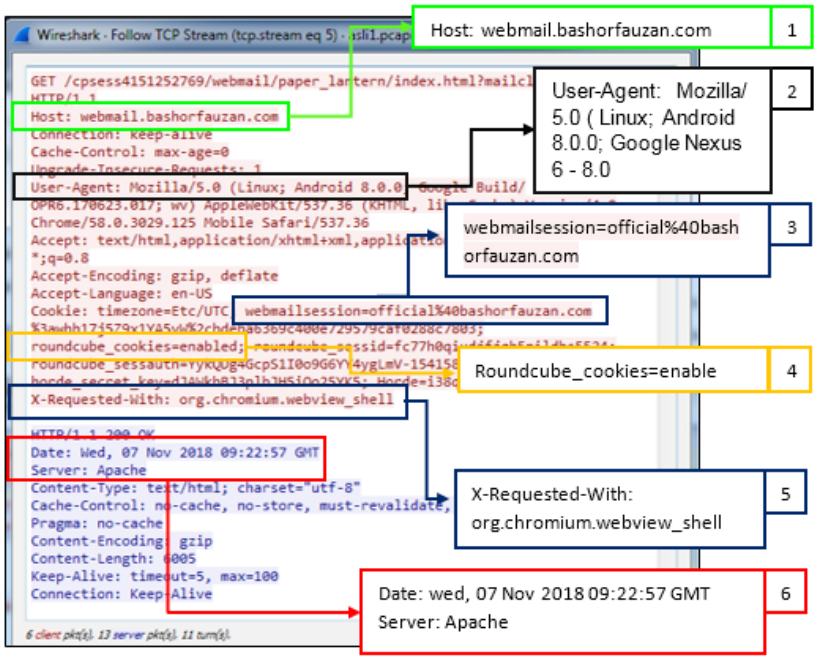
6.1.1. Analisis *Tools Wireshark*

Analisis pertama menggunakan *tools forensics Wireshark* dengan barang bukti yang telah diakuisisi. Analisis pertama menggunakan *Wireshark* ini untuk mendapatkan barang bukti paket data *e-mail* yang dikirim asli dari webmail support@bashorfauzan.com. Gambar 6.1 analisis paket data.



Gambar 6.1 *Capturing E-mail* Asli *Wireshark*

Gambar 6.1 merupakan hasil *capturing* pada layanan webmail. Terdapat beberapa barang bukti yang ditemukan seperti IP *Address source*, IP *Address destination*, protokol, MAC *address destination*, MAC *address source*, port *source,* dan *port destination*. Selain itu kita dapat melihat informasi lain yang didapatkan oleh *Wireshark* di dalam TCP *Stream*. TCP *Stream* merupakan kepanjangan dari Transmission Control Protocol. Pada TCP *Stream* memberikan informasi secara detail data yang di-*capturing*. Analisis dari TCP *Stream* dapat dilihat pada Gambar 6.2.



Gambar 6.2 Stream E-mail Asli

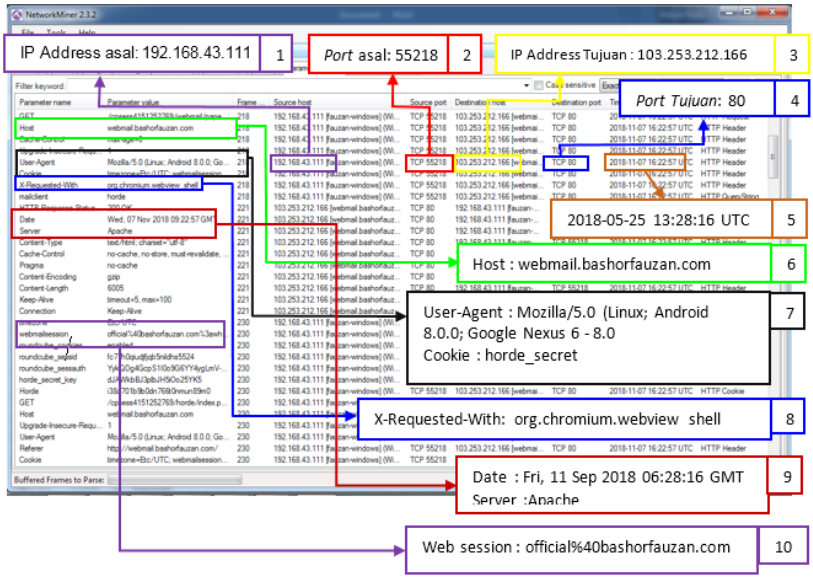
Gambar 6.2 merupakan isi dari TCP *Stream*, di dalam TCP *Stream* memberikan banyak informasi. Informasi yang dapat ditemukan pada TCP *Stream* adalah sebagai berikut:

1. Merupakan *host* webmail yang digunakan.
2. Merupakan informasi *smartphone* yang digunakan.
3. Akun *E-mail* yang digunakan untuk mengirim *e-mail*.
4. Merupakan *interface* yang digunakan untuk membuka *e-mail*
5. Merupakan *browser* yang digunakan untuk membuka *e-mail*.
6. Merupakan *timestamp* server dan server yang digunakan.

6.1.2. Analisis *Tools Networkminer*

Tahap pertama pada proses *analysis* mengunakan *Networkminer* adalah dengan melakukan analisis *e-mail* asli yang dikirim kemudian

dilakukan *capturing* menggunakan *Networkminer*. Gambar 6.3 merupakan hasil *analysis Networkminer*.



Gambar 6.3 Analisis Tool Networkminer

Gambar 6.3 merupakan hasil *Analysis E-mail* asli menggunakan *tools forensics Networkminer*. Terdapat beberapa barang bukti digital, berikut informasi yang dapat ditemukan :

1. Merupakan IP *Address source*.
2. Merupakan *port protocol source*.
3. Merupakan IP *Address destination*.
4. Merupakan *port protocol destination*.
5. Merupakan informasi *timestamp e-mail* diterima.
6. Merupakan *host* webmail yang digunakan.
7. Merupakan *smartphone* yang digunakan untuk membuka *e-mail* dan *interface* yang digunakan untuk membuka *e-mail*.

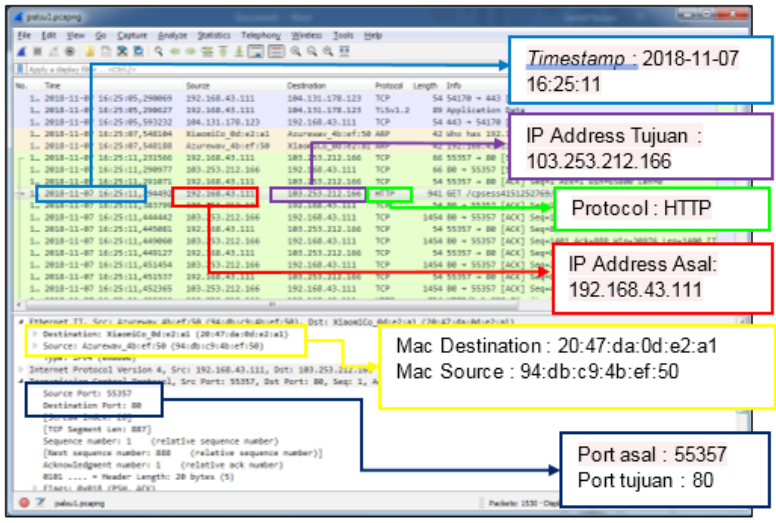
8. Merupakan *browser* digunakan untuk membuka *e-mail*.
9. Merupakan *timestamp* server *mail* dan server *e-mail*.
10. Merupakan *e-mail* yang digunakan untuk menerima *e-mail*.

6.2. Analisis *E-mail* Palsu

Analisis selanjutnya adalah hasil *capturing e-mail* palsu menggunakan *tools forensics Wireshark* dan *Networkminer*. *Analysis* dilakukan untuk memperoleh informasi yang berguna membahas pertanyaan-pertanyaan yang menjadi dorongan untuk melakukan pengumpulan dan pemeriksaan.

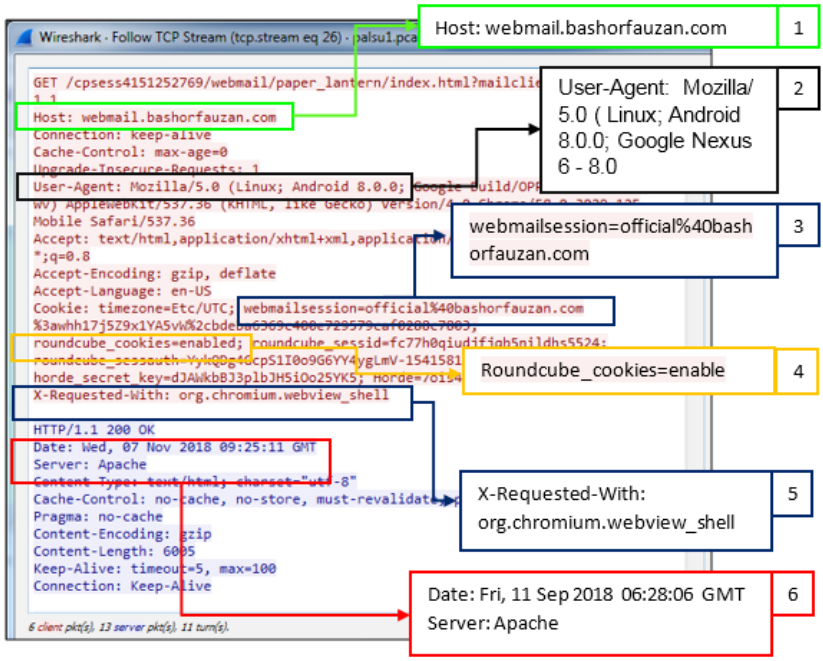
6.2.1. Analisis dengan *Wireshark*

Analisis kedua yaitu dengan menggunakan *e-mail* palsu menggunakan emki.kz yang dikirim mengunakan webmail support@ bashorfauzan.com. Gambar 6.4 merupakan hasil analisis.



Gambar 6.4 Analisis E-mail palsu Wireshark

Gambar 6.4 merupakan hasil *capturing* pada layanan *e-mail* yang diakses menggunakan *smartphone* android, seperti *IP Address source*, *IP Address destination*, protokol, MAC *address destination*, MAC *address source*, *port source,* dan *port destination*. Selain itu kita dapat melihat informasi lain yang didapatkan oleh *Wireshark* di dalam TCP *Stream*. TCP *Stream* merupakan kepanjangan dari *Transmission control protocol.* Pada TCP *Stream* memberikan informasi secara detail data yang di-*capturing*. Analisis dari TCP *Stream* dapat dilihat pada Gambar 6.5.



Gambar 6.5 TCP Stream E-mail Asli

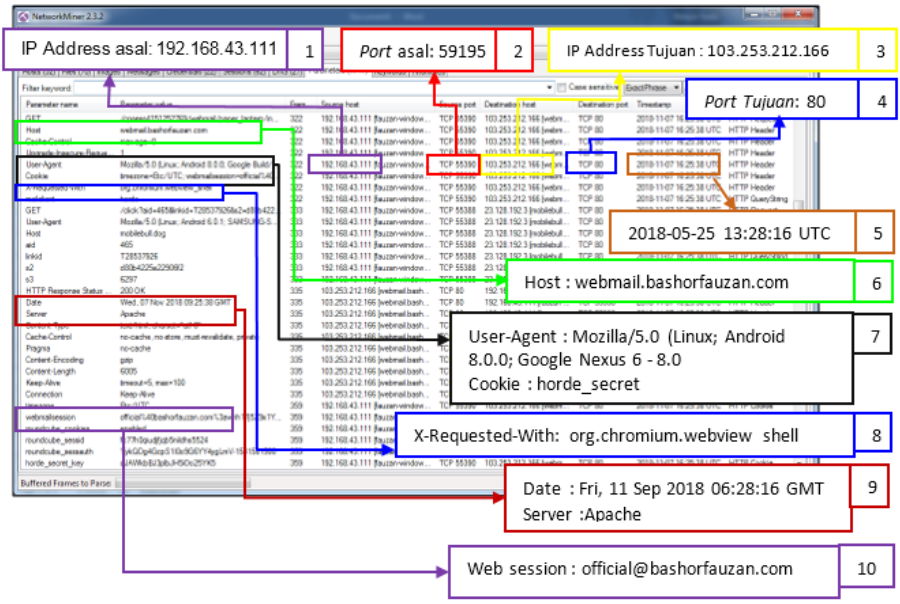
Gambar 6.5 merupakan isi dari TCP *Stream*, di dalam TCP *Stream* memberikan banyak informasi. Informasi yang dapat ditemukan pada TCP *Stream* adalah sebagai berikut:

1. Merupakan *host webmail* yang digunakan.
2. Merupakan informasi *smartphone* yang digunakan.

3. Akun *e-mail* yang digunakan untuk mengirim *e-mail*
4. Merupakan *interface* yang digunakan untuk membuka *e-mail*
5. Merupakan *browser* yang digunakan untuk membuka *e-mail*
6. Merupakan *timestamp* server dan server yang digunakan

6.2.2. Analisis dengan *Networkminer*

Tahap kedua pada proses *analysis* adalah menggunakan *networkminer*. *Networkminer* digunakan untuk melakukan analisis *e-mail* asli yang dikirim kemudian dilakukan *capturing* menggunakan *tool* forenik *Networkminer*. Gambar 6.6 merupakan hasil dari *analysis Networkminer*.



Gambar 6. 6 Analysis E-mail Palsu dengan Networkminer

Gambar 6.6 merupakan hasil *analysis e-mail* palsu dengan menggunakan *tools forensics Networkminer*. Terdapat beberapa barang bukti digital, berikut informasi yang dapat ditemukan :

1. Merupakan IP *Address source*.
2. Merupakan *port protocol source*.
3. Merupakan IP *Address destination*.
4. Merupakan *port protocol destination*.
5. Merupakan informasi *timestamp e-mail* diterima.
6. Merupakan *host* webmail yang digunakan.
7. Merupakan *smartphone* yang digunakan untuk membuka *e-mail* dan *interface* yang digunakan untuk membuka *e-mail*.
8. Merupakan *browser* yang digunakan untuk membuka *e-mail*.
9. Merupakan *timestamp* server *mail* dan server *e-mail*.
10. Merupakan *e-mail* yang digunakan untuk menerima *e-mail*.

6.3. Rangkuman

Hasil kedua *tools* tersebut memiliki perbedaan, barang bukti yang ditemukan. Setiap *tools* memiliki kemampuan mendapatkan barang bukti yang berbeda dari yang lain.

6.4. Latihan

1. Jelaskan secara singkat skenario yang digunakan pada simulasi.
2. Jelaskan hasil barang bukti *e-mail* asli dan palsu.
3. Jelaskan perbedaan hasil yang ditemukan *tools wireshark* dan *networkminer*.

Bab 7
Pelaporan

Tujuan Instruksional Umum:

1. Mahasiswa/i mampu menjelaskan laporan *E-mail.*

Tujuan Instruksional Khusus:

1. Mahasiswa/i mampu menjelaskan istilah standar dalam proses pelaporan *E-mail.*
2. Mahasiswa/i mampu memahami latar belakang, definisi, aplikasinya, dan tahap dalam pelaporan *E-mail.*
3. Mahasiswa/i dapat membuat laporan yang baik dan bernar sehingga dapat dipertanggung jawabkan.

7.1. Laporan *Wireshark*

Tahap akhir simulasi pertama adalah *laporan*. *Laporan* ini akan menampilkan hasil-hasil yang telah didapatkan oleh *tools forensics* yang digunakan dan telah dilakukan *analysis*.

Laporan pertama dari *tools forensics Wireshark*. Laporan ini bertujuan untuk mempermudah melihat laporan pada setiap tahapannya, *tools*

forensics Wireshark berhasil mendapatkan barang bukti digital seperti Tabel 7.1.

Tabel 7.1 Laporan Wireshark

No	Indikator	*Wireshark*	
		***E-mail* Asli**	***E-mail* Palsu**
1.	*IP Address source*	Ada	Ada
2.	*IP Address destination*	Ada	Ada
3.	Protokol	Ada	Ada
4.	MAC *address destination*	Ada	Ada
5.	MAC *address source*	Ada	Ada
6.	*Port Source*	Ada	Ada
7.	*Port Destination*	Ada	Ada
8.	Host *webmail*	Ada	Ada
9.	Informasi *smartphone* yang digunakan	Ada	Ada
10.	*Interface* yang digunakan untuk membuka *e-mail*	Ada	Ada
11.	Akun *e-mail* yang digunakan untuk mengirim *e-mail*	Ada	Ada
12.	*Browser* yang digunakan untuk membuka *e-mail*	Ada	Ada
13.	*Timestamp* pengirim	Ada	Ada
14.	Server *mail* yang digunakan	Ada	Ada

Tabel 7.1 merupakan barang bukti yang ditemukan oleh *tools forensics Wireshark* seperti IP *Address source*, IP *Address destination*, Protokol, MAC *address destination*, MAC *Address source*, *port source*, *port destination*, *host* webmail, informasi *smartphone* yang digunakan, *interface* yang digunakan untuk membuka *e-mail*, akun *e-mail* yang digunakan untuk mengirim *e-mail*, *browser* yang digunakan untuk membuka *e-mail*, *timestamp* pengirim dan server *mail* yang digunakan.

7.2. Laporan *Wireshark*

Laporan kedua dari *tools forensics Networkminer*. *Laporan* ini memiliki *destination* untuk melaporkan langkah-langkah yang telah dilakukan, berikut adalah hasil mendapatkan barang bukti digital seperti Tabel 7.2.

Tabel 7.2 Laporan Networkminer

No	Indikator	*Networkminer*	
		***E-mail* Asli**	***E-mail* Palsu**
1.	*IP Address source*	Ada	Ada
2.	*IP Address destination*	Ada	Ada
3.	Protokol	Ada	Ada
4.	*Port Source*	Ada	Ada
5.	*Port Destination*	Ada	Ada
6.	Host *webmail*	Ada	Ada
7.	Informasi *smartphone* yang digunakan	Ada	Ada
8.	*Interface* yang digunakan untuk membuka *e-mail*	Ada	Ada

9.	Akun *e-mail* yang digunakan untuk mengirim *e-mail*	Ada	Ada
10.	*Browser* yang digunakan untuk membuka *e-mail*	Ada	Ada
11.	*Timestamp* pengirim	Ada	Ada
12.	Server *mail* yang digunakan	Ada	Ada

Tabel 7.2 merupakan hasil yang didapatkan oleh *tools forensics Networkminer*. *Networkminer* berhasil mendapatkan 12 (Dua Belas) barang bukti seperti IP *Address source*, *port protocol source*, IP *Address destination*, *port protocol destination*, *timestamp e-mail* diterima, *host* webmail yang digunakan, *smartphone* yang digunakan untuk membuka *e-mail*, *interface* yang digunakan untuk membuka *e-mail*, *browser* yang digunakan untuk membuka *e-mail*, *timestamp* server *mail*, server *e-mail*, *e-mail* yang digunakan untuk menerima *e-mail.*

7.3. Rangkuman

Berdasarkan hasil analisis yang telah dilakukan *tools* forensik *wireshark* dan *networkminer* berhasil mendapatkan beberapa barang bukti digital, dapat dilihat pada Tabel 7.1 dan Tabel 7.2.

7.4. Soal Latihan

1. Jelaskan secara singkat fungsi laporan pada investigatoran ini.
2. Jelaskan perbedaan barang bukti dari *tools wireshark* dan *networkminer*.
3. Jelaskan perbedaan hasil Tabel 7.1 dan Tabel 7.2.

Daftar Pustaka

Agarwal, M., & Gupta, M. (2011). Systematic digital forensic investigation model. *IJCSS*, *5*(1), 118–131. Retrieved from http://www.cscjournals.org/csc/download/issuearchive/IJCSS/volume5/IJCSS_V5_I1.pdf#page=126

Didik, M., & R, W. (2008). Deteksi E-Mail Palsu Dengan Mempergunakan Header E-Mail. *Jurnal Teknologi*, *1*, 119–126. Retrieved from http://jurtek.akprind.ac.id/sites/default/files/119_126_ Didik.pdf

FC-Council. (n.d.). CHFI v8 Module 15 Log Capturing and Event Correlation.pdf.

Grance, T., Chevalier, S., Kent, K., & Dang, H. (2005). Guide to computer and network data analysis: Applying forensic techniques to incident response. *National Institute of Standards and Technology, Special Pub 800-86*, *86*, 800–86. Retrieved from http://scholar.google.com/scholar?hl=en&btnG=Search&q=intitle:Guide+to+Computer+and+Network+Data+Analysis:+Applying+Forensic+Techniques+to+Incident+Response#0

Kent, K., Chevalier, S., Grance, T., & Dang, H. (2006). Guide to integrating forensic techniques into incident response, (August). https://doi.org/10.6028/NIST.SP.800-86

M. M. Pollitt. (1995). Computer Forensics: An Approach to Evidence in Cyberspace. *The National Information Systems Security Conference*, (December), 487–491. https://doi.org/10.1016/S1361-3723(02)01110-7

Mukasey, M. B., Sedgwick, J. L., & Hagy, D. W. (2001). Guides Related to Collecting and Using Digital Evidence. Retrieved from http://www.iacpcybercenter.org/prosecutors/litigation-resources/

Riadi, I., Rusydi, U., & Nasrulloh, I. M. (2017). Analisis Forensik Bukti Digital Pada Frozen Solid State Drive Dengan Metode National Institute of Standards and Technology (Nist), *2*(2), 33–40. https://doi.org/10.21831/elinvo.v3i1.19308

Ruuhwan, R., Riadi, I., & Prayudi, Y. (2017). Evaluation of integrated digital forensics investigation framework for the investigation of smartphones using soft system methodology. *International Journal of Electrical and Computer Engineering*, *7*(5), 2806–2817. https://doi.org/10.11591/ijece.v7i5.pp2806-2817

State, T. C., & Security, E. (2017). The Current State of Email Security.

Umar, R., Riadi, I., & Muthohirin, B. fauzan. (2018). Acquisition Of Email Service Based Android, *3*(4). https://doi.org/http://dx.doi.org/10.22219/kinetik.v3i4.637

Wijaya, S. (2009). *Surat-surat Kesekretariatan: Panduan Praktis Menyusun Korespondensi Internal Perusahaan*. Pustaka Grhatama. Retrieved from http://onesearch.id/Record/IOS2750.9.393