Modul Pelatihan

JUNIOR CYBER SECURITY

Vocational School Graduate Academy
Digital Talent Scholarship
Tahun 2023

KATA PENGANTAR

Dunia saat ini berada pada era industri 4.0 yang lebih banyak menggunakan teknologi digital dan Indonesia telah mempersiapkan diri untuk masuk ke dalam tahap industri 4.0 tersebut melalui agenda percepatan transformasi digital. Salah satu langkah yang dilakukan dalam percepatan transformasi digital adalah penyiapan talenta digital. Laporan Bank Dunia tahun 2019 menyatakan bahwa Indonesia memiliki kekurangan 9 juta pekerja berketerampilan teknologi informasi dan komunikasi, sehingga perlu dilakukan penyiapan talenta digital untuk memenuhi kebutuhan tersebut dengan alokasi 600.000 orang setiap tahun. Upaya penyiapan talenta digital dilakukan oleh berbagai unsur baik pemerintah, institusi pendidikan, industri, komunitas masyarakat, maupun media publik.

Sejak tahun 2018, Kementerian Komunikasi dan Informatika melalui Badan Penelitian dan Pengembangan Sumber Daya Manusia menginisiasi Program Beasiswa Pelatihan Digital bernama *Digital Talent Scholarship* (DTS) yang telah berhasil dianugerahkan kepada lebih dari 300.000 penerima pelatihan bidang teknologi informasi dan komunikasi. Program *Digital Talent Scholarship* ini ditujukan untuk memberikan pelatihan dan sertifikasi berbagai tema pada bidang informatika, komunikasi, dan telekomunikasi, serta diharapkan melengkapi pemenuhan kebutuhan talenta digital Indonesia.

Program DTS tahun 2023 secara garis besar dibagi menjadi delapan akademi, salah satunya Vocational School Graduate Academy (VSGA). VSGA merupakan program pelatihan berbasis kompetensi kerja nasional bagi lulusan pendidikan vokasi SMK/sederajat dan diploma bidang *Science, Technology, Engineering, Mathematics* (STEM) yang belum mendapatkan pekerjaan atau sedang tidak bekerja. Tujuan Program VSGA adalah menyiapkan talenta digital dengan standar kompetensi sesuai Standar Kompetensi Kerja Nasional Indonesia (SKKNI). Oleh karena itu, penyusunan modul pelatihan untuk Program VSGA disusun dengan berbasis pada kompetensi (*Competency Based Training*). Kami berpesan agar modul pelatihan berbasis kompetensi yang telah disusun ini dapat menjadi referensi bagi peserta dan pengajar agar pelatihan berjalan efektif dan efisien.

Selamat mengikuti Pelatihan *Digital Talent Scholarship*, mari persiapkan diri kita menjadi talenta digital Indonesia yang kompeten.

Jakarta, April 2023
Kepala Badan Penelitian dan Pengembangan Sumber Daya Manusia
Kementerian Komunikasi dan Informatika Republik Indonesia

Dr. Hary Budiarto, M.Kom

Pendahuluan

Unit kompetensi ini berhubungan dengan pengetahuan, keterampilan, dan sikap kerja yang dibutuhkan dalam dalam menerapkan prinsip keamanan informasi pada transaksi elektronik untuk pencegahan, deteksi, dan pengelolaan ancaman keamanan siber.

A. Tujuan Umum

Setelah mempelajari modul ini peserta latih diharapkan mampu dalam menerapkan prinsip keamanan informasi pada transaksi elektronik dengan benar.

B. Tujuan Khusus

Adapun tujuan mempelajari unit kompetensi melalui buku modul alam mengumpulkan data ini guna memfasilitasi peserta latih sehingga pada akhir pelatihan diharapkan memiliki kemampuan sebagai berikut:

1. Mengidentifikasikan dan memenuhi kebutuhan terkait kerahasiaan, integritas, bukti dari pengguna dokumen kunci dan kontrak yang diakui.
2. Menetapkan aspek-aspek transaksi.
3. Melaksanakan dan memantau perlindungan keamanan untuk sistem infrastruktur dan penggunaan teknologi informasi sesuai dengan rencana implementasi dan prosedur operasi standar.

Latar belakang

Unit kompetensi ini berhubungan dengan pengetahuan, keterampilan, dan sikap kerja yang dibutuhkan dalam mengumpulkan data untuk data science. Penilaian dilakukan dengan mengacu kepada Kriteria Unjuk Kerja (KUK) dan dilaksanakan di Tempat Uji Kompetensi (TUK), ruang simulasi atau workshop dengan cara:

1.1 Lisan
1.2 Wawancara
1.3 Tes tertulis
1.4 Demonstrasi
1.5 Metode lain yang relevan.

Deskripsi Pelatihan

Materi Pelatihan ini memfasilitasi pembentukan kompetensi dalam menentukan kebutuhan teknis penerapan prinsip keamanan informasi pada transaksi elektronik.

Tujuan Pembelajaran

Setelah mengikuti pelatihan ini, peserta mampu menentukan kebutuhan teknis penerapan prinsip keamanan informasi pada transaksi elektronik.

Kompetensi Dasar

Mampu menentukan kebutuhan teknis penerapan prinsip keamanan informasi pada transaksi elektronik.

Indikator Hasil Belajar

Ketepatan dalam melakukan proses pengambilan data sesuai dengan tools yang telah disiapkan

INFORMASI PELATIHAN

INFORMASI PELATIHAN	
Akademi	VSGA untuk Junior Cyber Security
Mitra Pelatihan	
Tema Pelatihan	***Junior Cyber Security***
Sertifikasi	Sertifikasi kompetensi BNSP *Junior Cyber Security*
Deskripsi Pelatihan	Pelatihan ini menyiapkan peserta agar kompeten dalam melaksanakan pekerjaan *junior cyber security* yang dapat membantu pekerjaan praktisi *cyber security.* Kualifikasi pada jabatan ini menuntut seseorang memiliki kompetensi dalam menerapkan prinsip perlindungan informasi, menerapkan prinsip keamanan informasi untuk penggunaan jaringan internet, menerapkan prinsip keamanan informasi pada transaksi elektronik, melaksanakan kebijakan keamanan informasi, mengaplikasikan ketentuan/persyaratan keamanan informasi, mengelola log, dan menerapkan kontrol akses berdsarkan konsep/metodologi yang telah ditetapkan
Output Pelatihan	Setelah mengikuti pelatihan peserta akan mampu menganalisis dan memvisualisasikan data sehingga dapat digunakan dalam pengambilan keputusan
Durasi Pelatihan	24 JP (3 hari)
Jenis Pelatihan	**Luring */Offline* (40% Pengetahuan - 60% Praktek)**
Persyaratan Peserta	● Warga Negara Indonesia ● Usia Maksimal 29 Tahun pada saat mendaftar ● Lulus Pendidikan D3 Bidang TIK/SMK Bidang

INFORMASI PELATIHAN	
	(TKJ/TI/RPL) yang pernah bekerja minimal 3 tahun ● Belum Mendapatkan Pekerjaan Tetap/Pernah Bekerja tapi sedang tidak bekerja ● Lolos Seleksi Administrasi dan Tes Substansi
Persyaratan Sarana Peserta	Laptop/PC dengan spesifikasi: ● RAM minimal 4 GB ● 32/64-bit processor ● Operating System Windows 7,8,10, Linux, atau MAC OSX ● konektivitas WiFi ● Akses Internet Dedicated 256 kbps per peserta per perangkat
Kriteria Pengajar/*Trainer*/ Instruktur:	1. Minimal Lulusan S2 di bidang TIK; atau Memiliki kompetensi Okupasi Nasional "*Junior Cyber Security*". 2. Pengalaman Kerja diutamakan sebagai tenaga pengajar Pelatihan Bidang TIK minimal selama 2 tahun 3. Telah mengikuti pelatihan *training of trainner Junior Cyber Security*
Tim Penyusun:	1. Yan Hadynoer (BSSN) 2. Yoyok Darmanto (BSSN)

INFORMASI PEMBELAJARAN

RENCANA PELATIHAN		
Pertemuan	**Topik**	**Aktivitas**
Hari 1	● Pembukaan dan Penjelasan Rencana Pembelajaran ● Pre test	Pemaparan materi, diskusi dan *hands-on lab live class* 1 JP
	Pengantar *Junior Cyber Security* (Posisi dan peran *junior cyber security)*	Pemaparan materi, diskusi dan *hands-on lab live class* 1 JP
	Persiapan alat bantu (tools) pelatihan - Python (Jupiter) kenalkan dengan yang online; numpy, pandas, matplotl, seaborn, folium	Pemaparan materi, diskusi dan *hands-on lab live class* 1 JP

	- MySql (XAMPP)	
	Menerapkan prinsip perlindungan informasi 1. Mendefinisikan prosedur keamanan informasi yang tepat untuk tiap klasifikasi 2. Mengidentifikasi kelemahan dari informasi dalam sistem komunikasi bisnis 3. Menerapkan akses kontrol lingkungan Komputasi yang sesuai 4. Mematuhi dan melaksanakan petunjuk yang terdapat pada dokumen yang diterbitkan khusus oleh pemerintah atau badan-badan resmi terkait untuk mengelola sistem operasi 5. Mengumpulkan dan memelihara data yang diperlukan untuk memenuhi persyaratan pelaporan keamanan sistem.	Pemaparan materi, diskusi dan *hands-on lab live class* 2 JP
	Menerapkan prinsip keamanan informasi untuk penggunaan jaringan internet 1. Mematuhi dan menerapkan kebijakan dan prosedur keamanan informasi yang terkait dengan penggunaan jaringan internet 2. Mengidentifikasi tipe kelemahan dan jenisjenis serangan dalam jaringan internet 3. Mengaplikasikan penggunaan jaringan internet secara aman	Pemaparan materi, diskusi dan *hands-on lab live class* 3 JP
Hari 2	**Menerapkan prinsip keamanan informasi pada transaksi elektronik** 1. Mengidentifikasikan dan memenuhi kebutuhan terkait kerahasiaan, integritas, bukti dari pengguna dokumen kunci dan kontrak yang diakui 2. Menetapkan aspek-aspek transaksi 3. Melaksanakan dan memantau perlindungan keamanan untuk sistem infrastruktur dan penggunaan teknologi informasi sesuai dengan	Pemaparan materi, diskusi dan *hands-on lab live class* 3 JP

	rencana implementasi dan prosedur operasi standar	
	Melaksanakan kebijakan keamanan informasi 1. Mengidentifikasi aset penting dalam organisasi 2. Memproteksi aset penting dalam organisasi 3. Melakukan pemantauan terhadap aktivitas yang rentan ancaman	Pemaparan materi, diskusi dan *hands-on lab live class* 2 JP
	Mengaplikasikan ketentuan/persyaratan keamanan informasi 1. Mengaplikasikan persyaratan untuk program yang spesifik untuk keamanan lingkungan komputasi guna mengidentifikasi kelemahan/kerentanan 2. Menyediakan masukan tentang hal yang terkait dengan persyaratan keamanan untuk dimasukkan dalam laporan pekerjaan dan dokumen-dokumen pengadaan terkait 3. Mengumpulkan dan memelihara data yang diperlukan untuk memenuhi persyaratan pelaporan keamanan sistem 4. Mengindentifikasikan persyaratan keamanan dalam prosedur operasi di lingkungan komputasi 5. Menyusun persyaratan keamanan untuk perangkat keras, piranti lunak, dan penggunaan layanan yang spesifik untuk program keamanan jaringan 6. Mengevaluasi dan/atau menyetujui persyaratan keamanan yang relevanterhadap kemampuan teknologi informasi yang baru	Pemaparan materi, diskusi dan *hands-on lab live class* 3 JP

Hari 3	**Mengelola *log*** 1. Menetapkan kebijakan pencatatan *log* untuk menyertakan peristiwa penting 2. Melakukan kontrol berkas *log* terhadap kemungkinan diubah atau dihapus 3. Melakukan kontrol tempat menyimpan media file pencatatan terhadap kemungkinan penuh sehingga terjadi kegagalan ketika mencatat kejadian yang terjadi	Pemaparan materi, diskusi dan *hands-on lab live class* 4 JP
	Menerapkan kontrol akses berdsarkan konsep/metodologi yang telah ditetapkan 1. Menerapkan kontrol akses lingkungan komputasi yang sesuai 2. Melaksanakan kebijakan organisasi dan kebijakan *password* organisasi 3. Mengelola akun hak jaringan dan hak akses ke sistem jaringan dan infrastrukturnya 4. Mengimplementasikan peringatan secara online untuk menginformasikan para pengguna atas peraturan akses dari seluruh infrastruktur dan penggunaan sistem teknologi informasi 5. Menyusun prosedur untuk memastikan pengguna sistem menyadari tanggung jawab keamanan mereka sebelum memberikan akses ke sistem informasi organisasi 6. Melakukan kontrol dan pengawasan pada setiap pengguna yang memiliki akses khusus menjalankan fungsi keamanan agar menerima pelatihan keamanan dasar dan berkelanjutan serta mendapatkan sertifikasi yang sesuai untuk melaksanakan tugas keamanan	Pemaparan materi, diskusi dan *hands-on lab live class* 4 JP

Materi Pokok
1. Mengidentifikasikan dan memenuhi kebutuhan terkait kerahasiaan, integritas, bukti dari pengguna dokumen kunci dan kontrak yang diakui. 2. Menetapkan aspek-aspek transaksi. 3. Melaksanakan dan memantau perlindungan keamanan untuk sistem infrastruktur dan penggunaan teknologi informasi sesuai dengan rencana implementasi dan prosedur operasi standar.

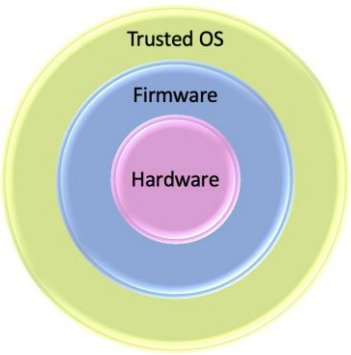
Sub Materi Pokok
1.1. Prosedur Keamanan Sistem Operasi, Perangkat TI, dan Aplikasi 1.2. Pencatatan *Log* Aplikasi dalam Transaksi Elektronik 2.1 Keabsahan Transaksi Elektronik 2.2 Keamanan Jalur Komunikasi pada Transaksi Elektronik 2.3 Protokol Keamanan Transaksi Elektronik 3.1. Pemantauan Keamanan Transaksi Elektronik. 3.2. Analisa Hasil Pemantauan Keamanan Transaksi Elektronik

1. MENGIDENTIFIKASIKAN DAN MEMENUHI KEBUTUHAN TERKAIT KERAHASIAAN, INTEGRITAS, BUKTI DARI PENGGUNA DOKUMEN KUNCI DAN KONTRAK YANG DIAKUI

1.1 Prosedur Keamanan Sistem Operasi, Perangkat TI, dan Aplikasi

a. Keamanan Sistem Operasi

Sistem operasi (OS) merupakan program yang dimuat ke dalam perangkat komputasi untuk mengelola sumber daya perangkat, seperti CPU, *memory*, *storage*, I/O *device*, dan *network*. Sistem operasi yang banyak dikenal adalah Windows, UNIX, iOS, Android, Symbian dan lainnya. Bukan tanpa celah, masing-masing OS juga memiliki kerentanan yang dapat dimanfaatkan untuk dieksploitasi oleh pihak penyerang. Pihak penyedia OS terus melakukan perbaikan dan pembaharuan terhadap OS-nya untuk menutup celah keamanan yang muncul.



Gambar 1. Arsitektur OS

Berdasarkan fungsinya, OS menjadi wadah bagi komponen-komponen penyusun siistem elektronik, seperti aplikasi, *database*, *web server*, dan lain sebagainya. Celah keamanan pada OS, dapat berdampak pada timbulnya kerentanan sebuah sistem elektronik. Keamanan OS perlu dilakukan untuk menguatkan ketahanan OS terhadap ancaman dan serangan yang menyasar pada penggunaan OS. Terdapat beberapa teknik yang dapat digunakan, antara lain adalah:

- Menerapkan konfigurasi secara aman
- Menutup port jaringan yang tidak digunakan
- Menutup layanan yang tidak dipakai
- Mengelola akun OS (akun default lebih baik dihapus)
- Penggunaan akses kontrol berupa kredensial *password* yang aman
- Penggunaan TBC (*trusted computing base*)
- Melakukan pembaharuan konfigurasi keamanan secara berkala
- Memastikan OS *log* telah diaktifkan
- Menerapkan penggunaan *anti-malware*

b. Keamanan Perangkat TI

Selain perangkat yang menjalankan OS di dalamnya, juga terdapat perangkat TI yang menjalankan fungsi khusus dan spesifik yang tidak terlalu kompleks seperti perangkat PC atau *server*. Karakteristik perangkat TI tersebut umumnya memiliki fungsi spesifik, tidak menggunakan perangkat CPU, tetapi menggunakan mikrokontroler, dan tidak memiliki GUI (*graphical user interface*). Penerapan keamanan juga perlu diterapkan untuk perangkat-perangkat tersebut, agar tidak timbul celah keamanan baru pada perangkat tersebut yang nantinya menjadi satu kesatuan dengan sistem elektronik lainnya. Tabel berikut merupakan beberapa perangkat TI dan bagaimana implikasi keamanannya.

Tabel 1. Daftar Perangkat TI dan Keamanannya

Perangkat	Implikasi Keamanan
Wireless Device	Akses tidak sah dan manipulasi nilai input yang ditransmisikan melalui jaringan nirkabel
Display	Penggunaan secara tidak sah terhadap display input
External Storage	- Menjadi media penyebaran virus - Menjadi alternatif booting terhadap sistem operasi secara tidak sah
Scanner dan *Printer*	- Penggunaan secara tidak sah - Pencurian data dan informasi yang ditampung di dalam perangkat *scanner* dan *printer*
Camera dan *Microphone*	- Pencurian data secara tidak sah - Penggunaan secara tidak sah

Perangkat	Implikasi Keamanan
ICS/SCADA	Akses tidak sah ke dalam sistem yang mengakibatkan terambil alihnya dan terganggunya layanan industry
Microcontroller	Eksekusi program yang dijalankan tanpa pengamanan mengakibatkan eksekusi terhadap data sensitif dapat diakses secara tidak sah
Smart Devices dan *IoT*	Karakteristiknya yang selalu terhubung dengan jaringan, sehingga keamanan ada pada bagaimana pelindungan jalur komunikasi data yang digunakan di dalam lalu lintas jaringan

c. Keamanan Aplikasi

Aplikasi dikembangkan berdasarkan pada *software development life cycle* (SDLC) mulai dari perencanaan awal, penerapan, penggunaan sampai dengan pemusnahan. Masing-masing tahapan yang dijalankan memperhatikan bagaimana penerapan keamanan dapat disertakan, dengan tujuan agar aplikasi terbangun dalam lingkungan yang aman dan berjalan secara aman sebelum masuk tahap penggunaan. Keamanan aplikasi dapat diterapkan dengan beberapa teknik berikut:

- Keamanan pada integrasi antara aplikasi dengan OS
- Pembaharuan secara berkala (*versioning*) untuk mengenali dan menutup celah keamanan
- Penerapan teknik keamanan dalam penulisan kode sumber aplikasi (*secure coding*)
- Pengujian kode sumber sebelum dijalankan pada sistem produksi (*code test review*)
- Analisa keamanan terhadap kode sumber aplikasi (*static analysis*)

1.2 Pencatatan Log Aplikasi dalam Transaksi Elektronik

Penggunaan aplikasi merupakan bagian penting dalam operasi layanan bisnis. Pencatatan (*logging*) terhadap setiap kejadian atau aktifitas yang berjalan pada aplikasi menjadi penting untuk dilakukan sebagai bagian dalam pengelolaan log untuk menjaga agar aplikasi berjalan sesuai dengan perencanaan dan tetap aman. *Logging* aplikasi merupakan proses yang melakukan penyimpanan dan pencatatan setiap kejadian dan aktifitas yang berjalan di dalam aplikasi. Hasil dari pencatatan tersebut disimpan dalam bentuk *log* aplikasi. Informasi yang ada pada *log* aplikasi dapat dipergunakan untuk melakukan penilaian terhadap kemungkinan adanya anomali, ancaman, ataupun serangan yang menyasar pada keamanan aplikasi. Selain itu, log aplikasi juga dapat dimanfaatkan untuk proses investigasi apabila telah terjadi insiden keamanan pada aplikasi, seperti peretasan aplikasi, pencurian data, ataupun gangguan keamanan lainnya.

Tabel 2. Sumber *Log* Aplikasi

Log Source	Description
Client requests and server responses	• Server and client apps provide high-level data of request/response • Header data in web requests/responses
Account information	• Server apps may log account info • Can identify who uses account and app
Usage information	• Number of transactions and size of transactions can indicate threats
Significant operational events	• Startup, shutdown, app configuration changes • Can identify compromises and operational failure
HIDS/HIPS logs	• Can log anomalous app execution • Can check integrity of sensitive files for modification
Anti-malware logs	• Can provide similar insight into the behavior of malicious software

Log aplkasi memiliki karakteristik berbeda-beda sesuai dengan fungsi dan tujuan aplikasi yang dibangun. Selain itu, log aplikasi juga terpisah dan bukan bagian dari *log* milik OS. Data pada *log* aplikasi yang banyak dan bervariasi mengakibatkan kesulitan dalam mengenali dan analisa terhadapnya. Oleh sebab itu, penafsiran dan pemilihan data di dalam *log* aplikasi menjadi kunci dalam mengenali, mengidentifikasi, dan menganalisa kejadian-kejadian yang tergambar di dalam *log* aplikasi, khususnya yang berkaitan dengan bagaimana keamanan dalam penggunaan aplikasi. Tabel 2 merupakan beberapa parameter di dalam log aplikasi yang perlu diperhatikan dalam mendukung diterapkannya keamanan sebuah aplikasi.

Log aplikasi dalam transaksi elektronik dapat dijadikan bahan dalam pelaporan sebagai bentuk evaluasi terhadap keamanan transaksi elektronik. Berikut merupakan contoh laporan yang memperlihatkan log aplikasi dalam transaksi elektronik.

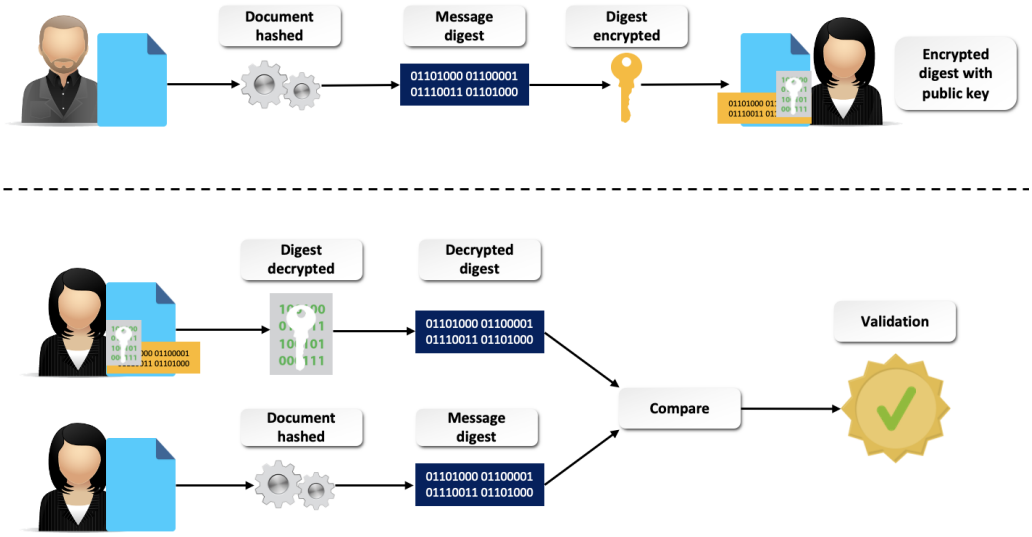
Report No:	**SISTEM LAYANAN 1**
Revision No:	
Date/Time:	
Author:	

Application Log				
No.	**Application**	**Connection**	**Throughput (Mbps)**	**Transaction (tps)**
1.	App1	362	14,60	182.820
2.	App2	128	325,39	63.840
3.	App3	14	2,51	82
4.	App4	2	2,50	43
…	…	…	…	124

2. MENETAPKAN ASPEK-ASPEK TRANSAKSI

2.1 Keabsahan Transaksi Elektronik

Salah satu keamanan di dalam transaksi elektronik adalah perlu dipastikan keabsahan objek, data, atau dokumen yang ditransaksikan. Dalam menjamin nilai keabsahan sebuah data, dapat dilakukan dengan penerapan fungsi tanda tangan digital (*digital signature*) sebagai sebuah terapan infrastruktur kunci publik (*public key infrastructure*) yang memiliki fungsi untuk validasi keabsahan sebuah objek, data ataupun dokumen elektronik.



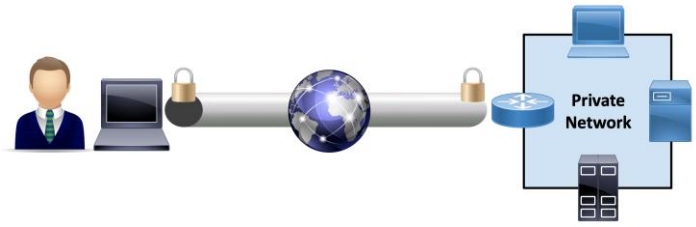
Gambar 2. Validasi Keabsahan menggunakan *Digital Signature*

2.2 Keamanan Jalur Komunikasi pada Transaksi Elektronik

Selain keamanan pada objek yang ditransaksikan pada sebuah transaksi elektronik, jalur komunikasi yang digunakan juga penting untuk diamankan dengan menggunakan teknik enkripsi yang dapat memberikan proteksi pada jalur komunikasi terhadap akses tidak sah ataupun tindakan lain, seperti pertasan dan pencurian data pada komunikasi transaksi elektronik. Enkripsi pada jalur komunikasi dapat dilakukan dengan menggunakan beberapa protocol keamanan yang ada di dalam jaringan, seperti TLS/SSL ataupun VPN.

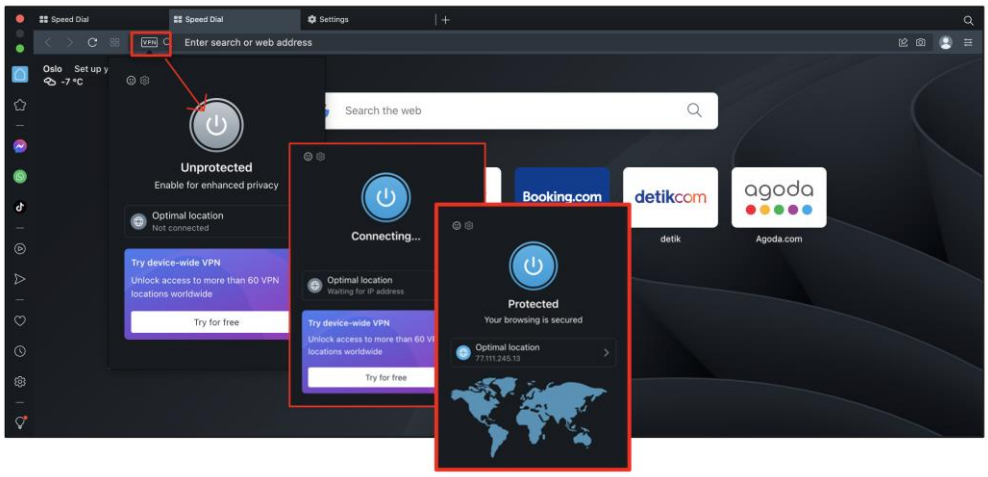
a. VPN

Sebuah metode yang digunakan untuk menghubungkan jaringan lokal/privat melewati jaringan internet. VPN berjalan sebagai sebuah protokol yang berfungsi dalam melakukan *tunneling* dan enkripsi jaringan.



Gambar 3. VPN

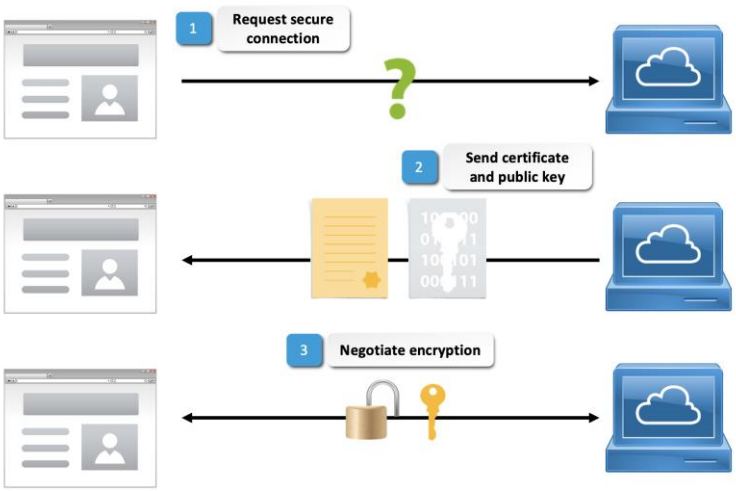
Salah satu aplikasi yang dapat digunakan untuk mendukung penggunaan VPN dalam transaksi elektronik adalah dengan menggunakan aplikasi Opera (VPN *browser*). Dengan penggunaan VPN *browser* ini, maka aktifitas yang dilakukan tidak bisa dilacak dan dipelajari, sehingga identitas alamat IP dapat disembunyikan sebagai bentuk keamanan dalam transaksi elektronik.



Gambar 4. Penggunaan VPN untuk keamanan transaksi elektronik

b. TLS/SSL

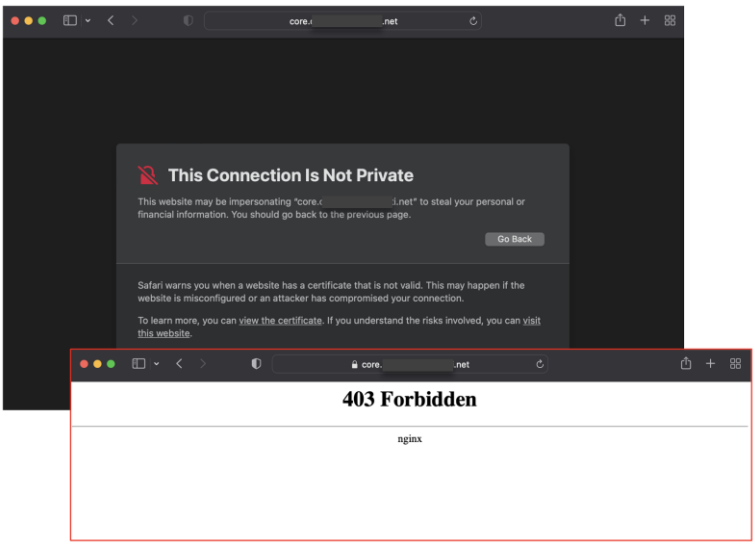
Protokol di dalam jaringan internet yang berfungsi sebagai protokol keamanan yang memanfaatkan sertifikat digital untuk otentikasi menggunakan enkripsi kunci publik. TLS/SSL melindungi komunikasi di dalam jaringan dari ancaman penyadapan informasi lalu lintas jaringan, dan ancaman modifikasi nilai data yang ditransmisikan melalui jaringan internet.



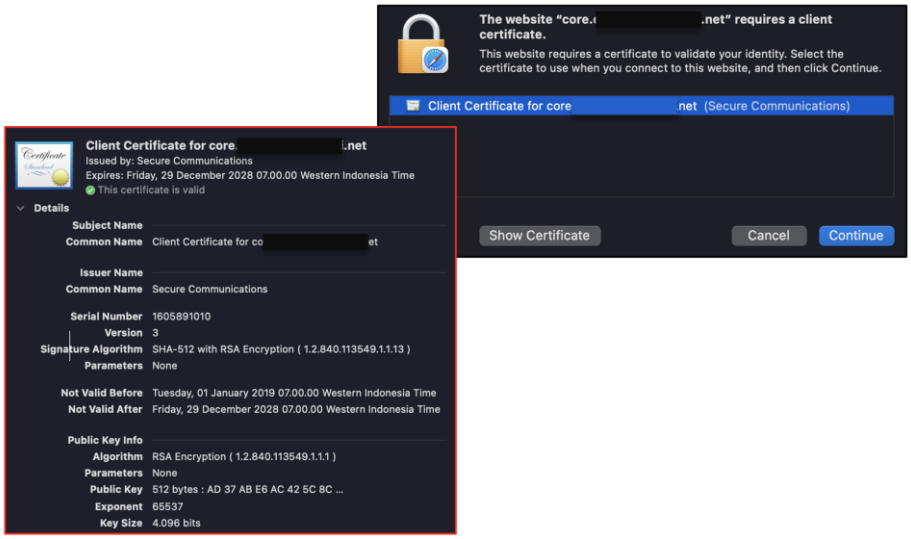
Gambar 5. TLS/SSL

Pemanfaatan sertifikat digital untuk keamanan transaksi elektronik dalam protokol TLS/SSL dapat dilihat pada skema berikut. Dicontohkan pada gambar (6-8) terdapat sebuah alamat situs yang diamankan transaksi elektroniknya

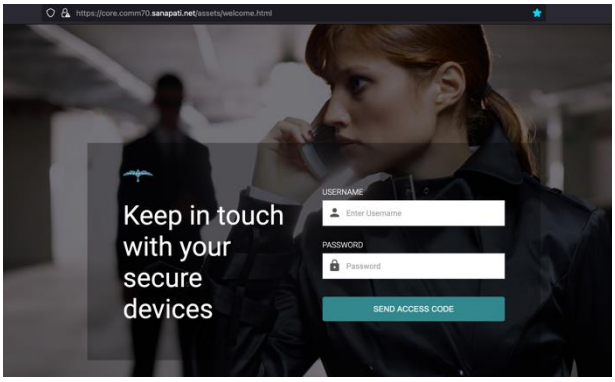
dengan TLS/SSL. Alamat situs tidak dapat diakses bagi siapa saja yang tidak memiliki sertifikat digital yang sesuai.



Gambar 6. Situs tidak dapat diakses apabila tidak memiliki sertifikat digital yang sesuai



Gambar 7. Penggunaan sertifikat digital yang sesuai



Gambar 8. Situs dapat diakses secara sah

2.3 Protokol Keamanan Transaksi Elektronik

TLS/SSL dan VPN sebagai protokol dasar untuk keamanan jalur komunikasi dapat diterapkan dan dipergunakan untuk protokol keamaan lainnya yang berada di pada lapis jaringan yang lebih tinggi. Terdapat protokol lainnya yang digunakan untuk keamanan transaksi elektronik yang mengkombinasikan protokol-protokol keamanan dasar. Protokol lainnya yang sudah banyak digunakan adalah protokol *Secure Electronic Transaction* (SET).

SET merupakan protokol yang digunakan untuk melayani pembayaran elektronik dengan penerapan teknologi enkripsi untuk keamanan transaksinya. Penggunaannya adalah untuk pemakaian kartu pembayaran (debit/kredit) melalui jaringan internet. SET diperkenalkan pada tahun 1996 dengan tujuan untuk melakukan pembayaran secara otomatis yang memungkinkan pengguna untuk menggunakan infrastruktur pembayaran menggunakan kartu pembayaran pada jaringan internet dalam mode yang lebih aman. Protokol SET ini menyediakan beberapa fungsi keamanan, seperti:

- Penyediaan saluran komunikasi yang aman dengan fungsi enkripsi antara pihak-pihak yang terlibat dalam transaksi pembayaran elektronik,
- Penyediaan validasi keabsahan transaksi dengan penerapan *digital signature*,
- Penyediaan keamanan privasi terhadap data dan informasi pribadi milik pihak-pihak yang terlibat dalam sistem pembayaran elektronik dengan menggunakan fungsi enkripsi.

Terdapat beberapa prasyarat yang harus dipenuhi untuk menjalankan protkol SET ini, salah satunya adalah menjaga kerahasiaan informasi pembayaran. Dengan fungsi enkripsi, maka kerahasiaan informasi transaksi dan pembayaran akan tetap terjaga. Bahkan pihak penerima pun tidak dapat melihat akun pembayar termasuk PIN, masa aktif , ataupun nilai CVV. Prasyarat tersebut diperlukan untuk meyakinkan kepada para pemegang kartu pembayaran bahwa informasi data yang ada pada akunnya tetap aman dan hanya bisa diakses oleh penerimanya. Selain itu, kerahasiaan juga akan sangat mengurangi risiko penipuan oleh salah satu pihak terutama pada pihak ketiga yang mungkin adalah pihak yang tidak bertanggung jawab.

3. MELAKSANAKAN DAN MEMANTAU PERLINDUNGAN KEAMANAN UNTUK SISTEM INFRASTRUKTUR DAN PENGGUNAAN TEKNOLOGI INFORMASI SESUAI DENGAN RENCANA IMPLEMENTASI DAN PROSEDUR OPERASI STANDAR

3.1 Pemantauan Keamanan Transaksi Elektronik

Dalam operasional aplikasi atau sistem elektronik, terdapat informasi mengenai riwayat kejadian berkaitan dengan keamanan yang berlangsung selama berjalannya aplikasi. Setiap kejadian tersebut dicatat dan dikelola untuk menjadi bahan dalam pemantauan dan analisa keamanan secara *real-time*. Untuk menangani hal tersebut, terdapat sebuah teknologi yang dikenal dengan istilah *Security Information and Event Management* (SIEM). SIEM merupakan sebuah solusi keamanan yang dapat membantu pengelola sistem dalam mengenali celah dan ancaman keamanan yang berpotensi muncul sebelum serangan yang sesungguhnya terjadi. SIEM dapat memberitahukan adanya anomali dalam penggunaan aplikasi, dimana saat sekarang ini sudah semakin didukung dengan adanya teknologi *artificial intelligence* (AI) dalam melakukan pengenalan, deteksi dan juga analisa anomali keamanan. SIEM semakin berkembang menjadi lebih mutakhir dengan tambahan fungsi berupa *user and entity behaviour analysis* (UEBA) yang dapat mengelola ancaman keamanan terkini secara efisien.

SIEM menjalankan fungsinya dengan menerapkan beberapa tahapan langkah, mulai dari pengumpulan, agregasi,normalisasi, korelasi, sampai dengan analisa data. Walaupun sebagian besar SIEM memiliki kemampuan yang berbeda-beda, namun secara umum memiliki kegunaan yang sama, diantaranya adalah sebagai berikut:

- *Log Management*

  Data *log* dari komponen pendukung sistem elektronik, mulai dari perangkat *endpoint*, aplikasi, *database*, *server*, sampai dengan jaringan dikumpulkan dan dikelola secara terpusat.

- *Event Correlation and Analytic*

  Tahapan dalam melakukan analisa lanjutan terhadap korelasi kejadian dari data-data *log* yang berhasil dikumpulkan. Analisa ini dilakukan untuk mengidentifikasi dan memahami pola yang kompleks dari keseluruhan log yang terkumpul, sehingga dapat ditemukan dan diketahui kaitan dan korelasi antar kejadian untuk mengurangi potensi ancaman keamanan secara efektif dan efisien.

- *Incident Monitoring and Security Alerts*

  Dengan mengumpulkan log secara terpusat dan analisa korelasinya, maka memungkinkan SIEM dapat memantau insiden keamanan yang dapat terjadi pada perangkat ataupun aplikasi yang saling terhubung. Selain itu, pola perilaku anomali keamanan juga dapat dengan segera dideteksi dan diklasifikasikan secara *real-time*, sehingga tindakan mitigasi yang tepat dapat dengan segera diterapkan.

- *Compliance and Management Report*

  Secara utuh, SIEM juga dapat dijadikan sebagai sebuah referensi untuk melakukan verifikasi terhadap kepatuhan pada sebuah standar yang berlaku, seperti PCI_DSS, GDPR, HIPPA, SOX, dan lainnnya. Dengan fungsi ini, SIEM membantu pihak manajemen dalam menyusun dan menetapkan kebijakan yang berkaitan dengan keamanan untuk mengurangi risiko keamanan sejak dini.

Selain itu, SIEM juga memiliki kegunaan yang dimanfaatkan lainnya oleh pengelola aplikasi atau sistem transaksi elektronik, seperti deteksi serangan dan ancaman secara *real-time*, audit kepatuhan (menilai dan melaporkan), otomatisasi dengan fungsi AI, deteksi ancaman terkini (*insider attack*, *phishing*, *database injection*, DoS, peretasan dan pencurian data), mendukung investigasi forensik, dan melakukan pemantauan terhadap aktifitas pengguna dan aplikasi secara otomatis. Berikut merupakan contoh laporan yang memperlihatkan hasil pemantauan keamanan transaksi elektronik yang dapat dibuat.

Report No:	**SISTEM LAYANAN 1**
Revision No:	
Date/Time:	
Author:	

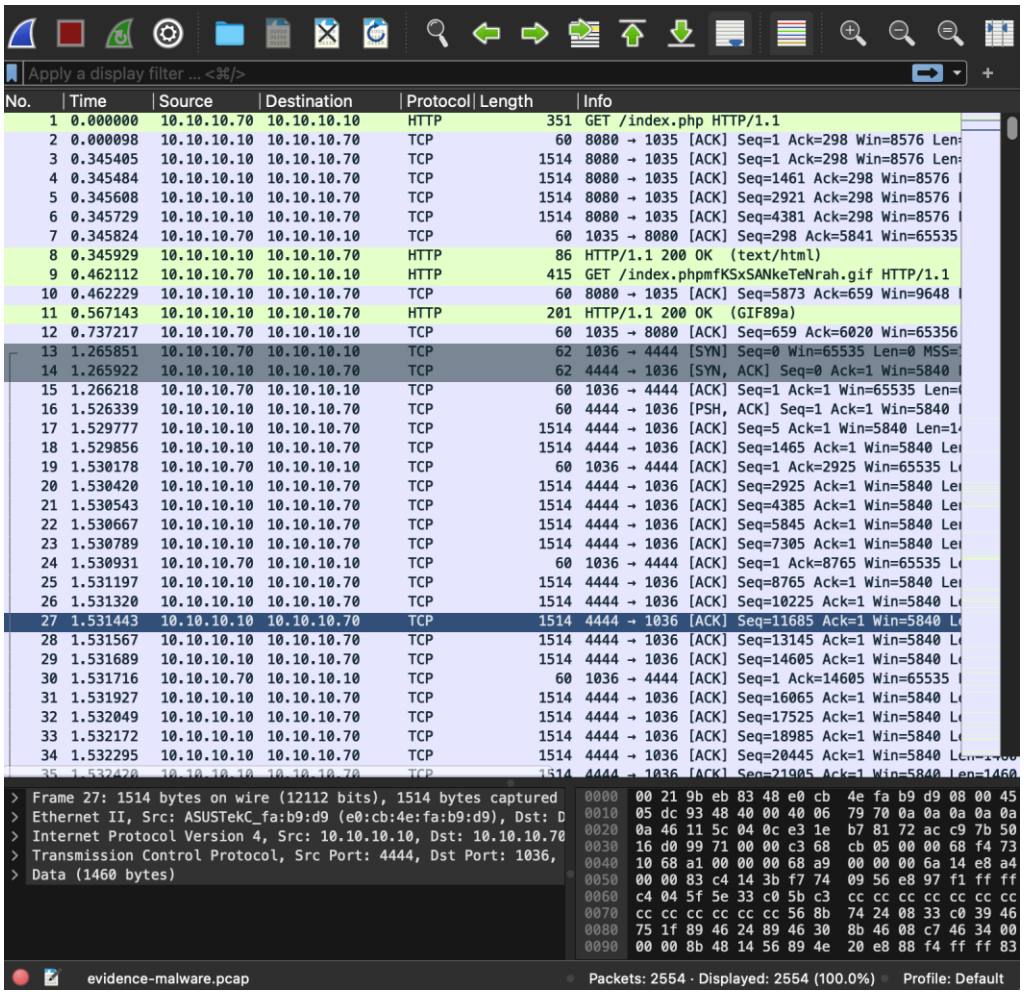
Security Monitoring							
No.	**Aplikasi**	**Severity**					
		Critical		**High**		**Medium**	
		Jumlah	**Status**	**Jumlah**	**Status**	**Jumlah**	**Status**
1.	App1	20	*blocked*	1	*queue*	0	-
2.	App2	5	*blocked*	32	*queue*	44	*forwarded*
3.	App3	13	*blocked*	22	*queue*	9	*forwarded*
4.	App4	…	…	…	…	…	…
…	…	…	…	…	…	…	…

3.2 Analisa Hasil Pemantauan Keamanan Transaksi Elektronik

Pemantauan, pengumpulan dan pemeriksaan terhadap riwayat kejadian (*log*) dilakukan, yang selanjutnya dilakukan analisa terhadap *log* tersebut. Analisa log bertujuan untuk memberikan gambaran utuh terhadap aktifitas sistem, melihat korelasi antar log, menjelaskan kejadian sesungguhnya apabila terdapat insiden keamanan di dalam sistem. Analisa log dapat dilakukan dengan menggunakan tools untuk membantu dan mempercepat dihasilkannya hasil analisa log yang komprehensif. Hasil analisa divisualisasikan dengan menggunakan aplikasi pendukung atau *tools* yang dapat dengan cepat memberikan korelasi dan gambaran mengenai kejadian yang terjadi, terkhusus yang berkaitan dengan aktifitas keamanan yang terjadi selama berjalannya aplikasi ataupun sistem elektronik.

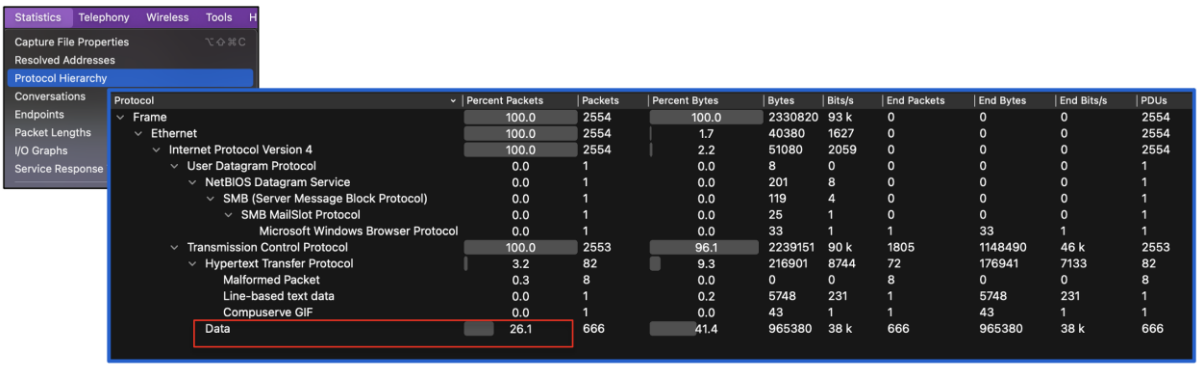
Pada contoh berikut, terdapat sebuah *log* transaksi elektronik yang diambil dari perangkat jaringan (**evidence.pcap**), kemudian *log* tersebut dilakukan analisa untuk memberikan kesimpulan mengenai hasil pemantauan keamanan transaksi elektronik. Analisa log dilakukan sesuai dengan tahapan berikut.

1) Log hasil pemanatauan transaksi elektronik diambil (**evidence.pcap**)
2) Jalankan aplikasi **Wireshark** untuk membantu dalam melakukan analisa log
3) Buka file **evidence.pcap** pada aplikasi **Wireshark**



Gambar 9. Log pada **evidence.pcap** yang dibuka pada aplikasi **Wireshark**

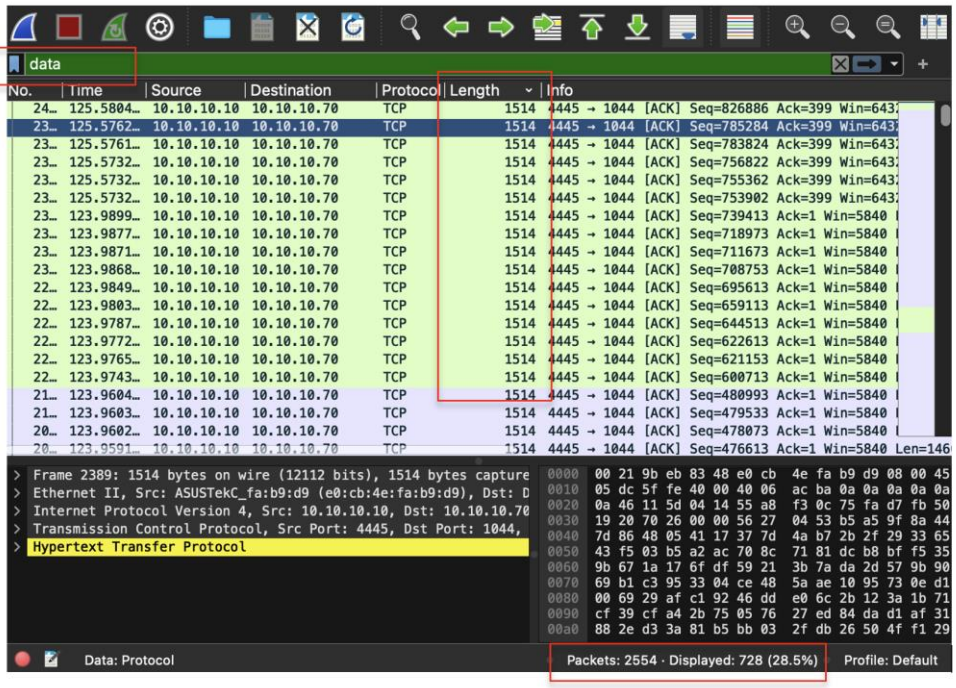
4) Lakukan analisa paket jaringan **evidence.pcap**
   - Pilih menu **Statistics** >> **Protocol Hiearchy**



Gambar 10. Komposisi penggunaan protokol pada *log* **evidence.pcap**

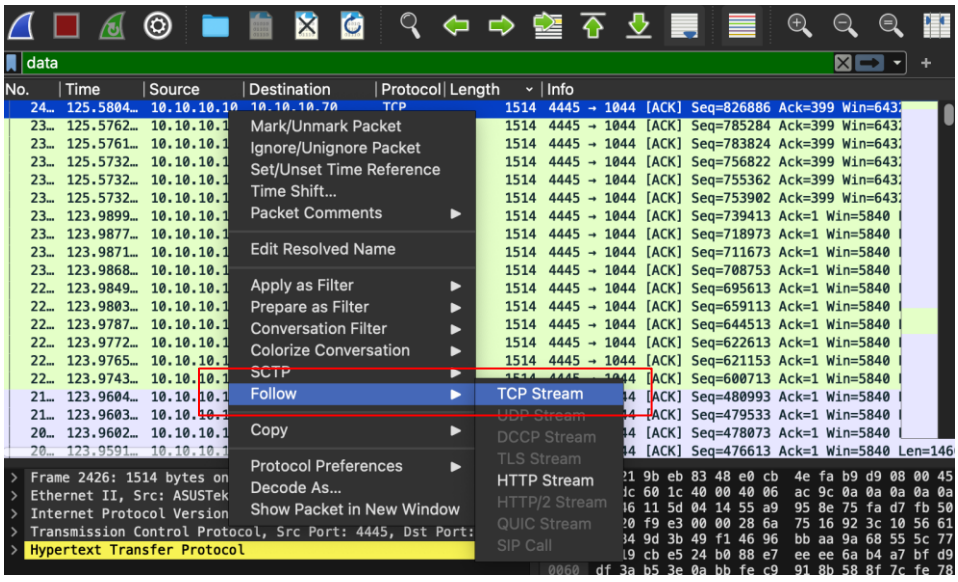
Didapatkan bahwa sejumlah 26% dari log **evidence.pcap** merupakan protokol **TCP** yang dimanfaatkan untuk komunikasi **Data**. Hal tersebut mengindikasikan bahwa terdapat data yang dikirim-terimakan pada transaksi elektronik tersebut.

- Lakukan pemilahan paket untuk menampilkan hanya yang berisikan komunikasi data, dengan cara menggunakan **keyword "Data"** dalam kolom **filter**.



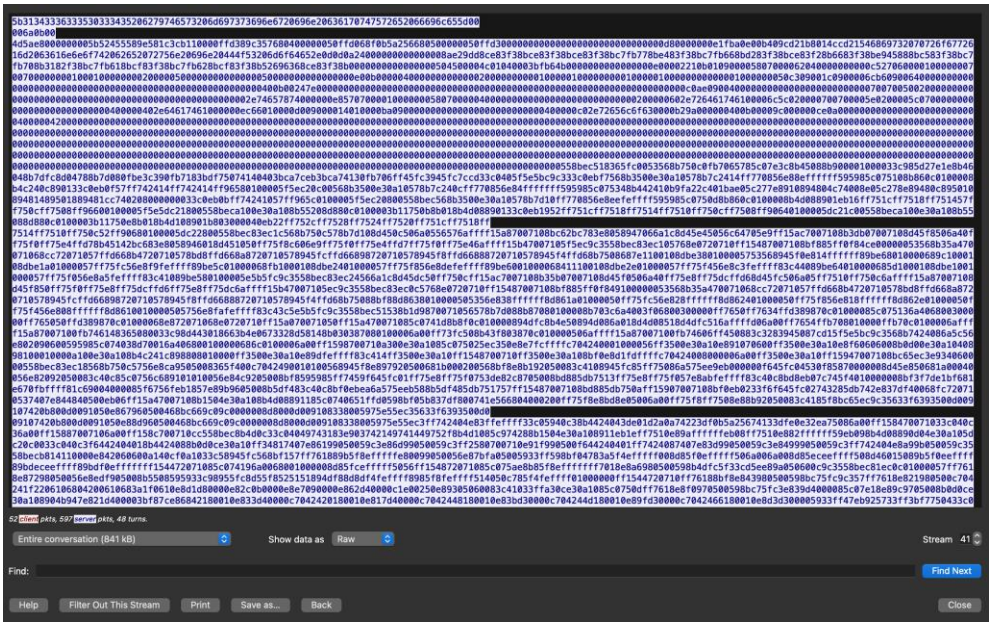
Gambar 11. Filter untuk protocol **Data**

- Lakukan ekstraksi paket dengan cara klik kanan pada salahs atu paket, kemudian pilih menu **Follow >> TCP Stream**



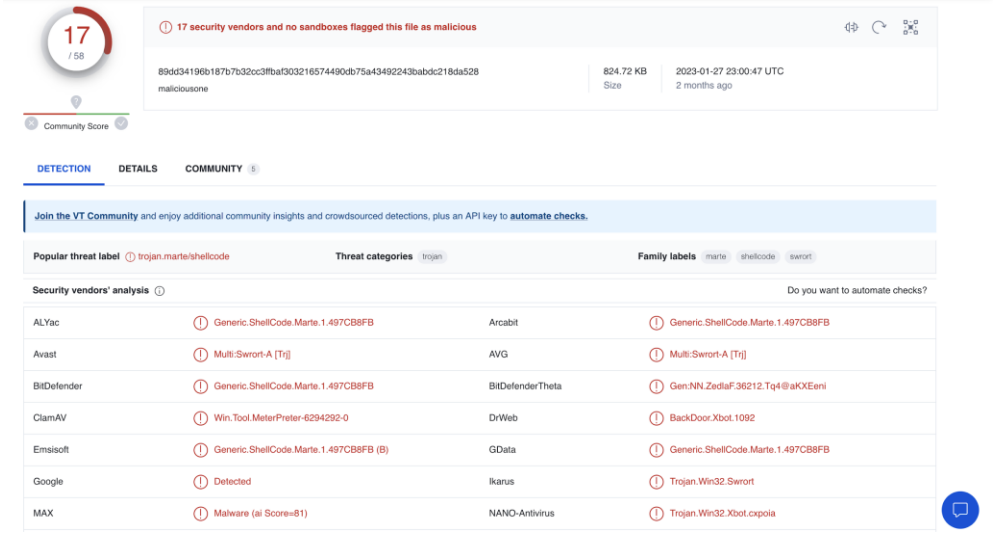
Gambar 12. Ekstraksi paket

- Setelah dilakukan ekstraksi paket, selanjutnya paket yang berisikan data tersebut ditampilkan dalam bentuk *raw file*
- *raw file* tersebut selanjutnya disimpan dalam bentuk sebuah file dengan cara memilih tombol **Save As** (simpan dengan nama file **FILE**)



Gambar 13. *raw file* hasil ekstraksi paket

- **FILE** yang berhasil disimpan merupakan data yang terdapat pada log **evidence.pcap**
- Perlu dilakukan analisa tambahan untuk mengetahui **FILE** tersebut lebih dalam
- Salah satunya dapat menggunakan pemindaian *file* terhadap anomali keamanan, yaitu aplikasi Virus Total
- Dari hasil pemindaian didapatkan bahwa ternyata FILE tersebut berisikan sejumlah *malware* dan *trojan*



Gambar 14. Hasil pemindaian **FILE** dengan **Virus Total**

5) Dokumentasikan dalam sebuah laporan hasil analisa *log* keamanan transaksi elektronik

Report No:	**SISTEM LAYANAN 1**
Revision No:	
Date/Time:	
Author:	

Security Monitoring Log Analysis

No	Date	Time	Events	Status	Officer	Notes
1.	29-04-2010	06:42:04	malware threats	closed	hadynoer	restoring system at the time before malware infected
...	...	...	...	...	...	...
...	...	...	...	...	...	...

Latihan 1

- Penggunaan VPN untuk keamanan transaksi elektronik

Latihan 2

- Penggunaan TLS/SSL untuk keamanan transaksi elektronik

Latihan 3

- Pencatatan log aplikasi transaksi elektronik
- Penyusunan laporan pemantauan keamanan transaksi elektronik
- Penyusunan analisa hasil pemantauan keamanan transaksi elektronik

A. Pengetahuan yang diperlukan untuk menerapkan prinsip keamanan informasi pada transaksi elektronik

1. Pengetahuan tentang aspek keamanan informasi (CIA triad)
2. Pengetahuan tentang ancaman pada penggunaan transaksi elektronik
3. pengetahuan tentang aplikasi pengamanan dalam penggunaan transaksi elektronik

B. Keterampilan yang diperlukan untuk menerapkan prinsip keamanan informasi pada transaksi elektronik

1. Kemampuan menjalankan program komputer sederhana untuk keamanan informasi
2. Kemampuan mengenali ancaman serangan pada transaksi elektronik

C. Sikap Kerja yang diperlukan untuk menerapkan prinsip keamanan informasi pada transaksi elektronik

1. Harus cermat dalam menjalankan program komputer untuk keamanan informasi
2. Harus cermat dalam menelaah log.
3. Memiliki *security awareness* (kesadaran akan ancaman keamanan informasi)
4. Teliti.

Tugas Dan Proyek Pelatihan
1. Kerjakan Latihan 1 sampai dengan latihan 3

Link Referensi Modul
https://www.virustotal.com (aplikasi pemindaian file)

Link Pertanyaan Modul

Bahan Tayang
Bisa berupa Link/ Screen Capture Slide pelatihan

Link room Pelatihan dan Jadwal live sesi bersama instruktur
Zoom, Meets

Penilaian
Komposisi penilaian Kuis 1 Mengumpulkan data: Nilai 10 (Range 0 -10)

Target Penyelesaian Modul
1hari/sampai 3 JP

KOMINFO digitalent

VSGA Vocational School Graduate Academy

2023

#JadiJagoanDigital

digitalent.kominfo.go.id