UJIAN AKHIR SEMESTER

MATAKULIAH DIGITAL FORENSIK

KELAS A

Muhammad Amanda Maulana Malik Ibrahim

212410102035

PROGRAM STUDI TEKNOLOGI INFORMASI

FAKULTAS ILMU KOMPUTER

UNIVERSITAS JEMBER

2025

1. Tantangan Hukum dan Teknis dalam Akuisis Data Cloud & IoT
    - Tantangan hukum dalam lingkungan forensik modern, para penyidik tidak akan menemui kasus dengan bukti yang tersembunyi dalam perangkat fisik tersangka, namun bukti tersebut biasanya di pindah ke layanan cloud atau disimpan pada network. Secara hukum, hambatan terbesar muncul dari masalah yuridiksi atau pengadilan. Pada perangkat fisik. Penyidik cukup meyita laptop atau ponsel pelaku dan melakukan forensik secara langsung pada perangkat. Namun ketika data disimpan pada cloud, data tidak memiliki lokasi tetap, dan data tersebut di Kelola serta dijaga oleh perusahaan internal yang menyediakan layanan tersebut, yang pastinya mereka memiliki peraturan dan regulasi internal tersendiri.

      Misalkan pelaku meyimpan transaksi lognya di thailand, backupnya disimpan di malaysia, dan copy-annya disimpan di kamboja, para penyidik harus melakukan proses hukum lintas negara seperti **Mutual Legal Assistance Treaty** (MLAT) atau proses kerjasama yang dilakukan oleh berbagai negara untuk memerangi kejahatan transnasional dan tantangan transnasional lainnya dengan meningkatkan kerja sama dalam penegakan hukum dan bantuan hukum timbal balik dalam masalah pidana. (Sumber:https://asean.org/our-communities/asean-political-security-community/rules-based-people-oriented-people-centred/treaty-on-mutual-legal-assistance-in-criminal-matters/).
      Proses ini membutuhkan waktu dan birokrasi yang lama dan ketat serta dilakukan dengan dasar hukum yang kuat.

      Lanjut membahas dari sisi Chain of Custoy (CoC). Dalam forensik tradisional, penguasaan bukti harus jelas (meyita perangkat, imaging, documentation, menjaga bukti untuk dihadirkan di pengadilan. Namun pada kasus cloud dan Iot, penyidik tidak memiliki kontrol langsung terhadap server fisik. Pengambilan data harus didampingin oleh penyedia layanan Cloud melalui API atau dashboard internal mereka. Akibatnya proses CoC menjadi anjang karena melibatkan pihak ketiga. Dari sisi teknikal, akuisisi hardware tidak dapat dilakukan bit-by-bit karena tersimpan pada server cloud yang bersifat virtual dan terdistribusi. Selain itu,

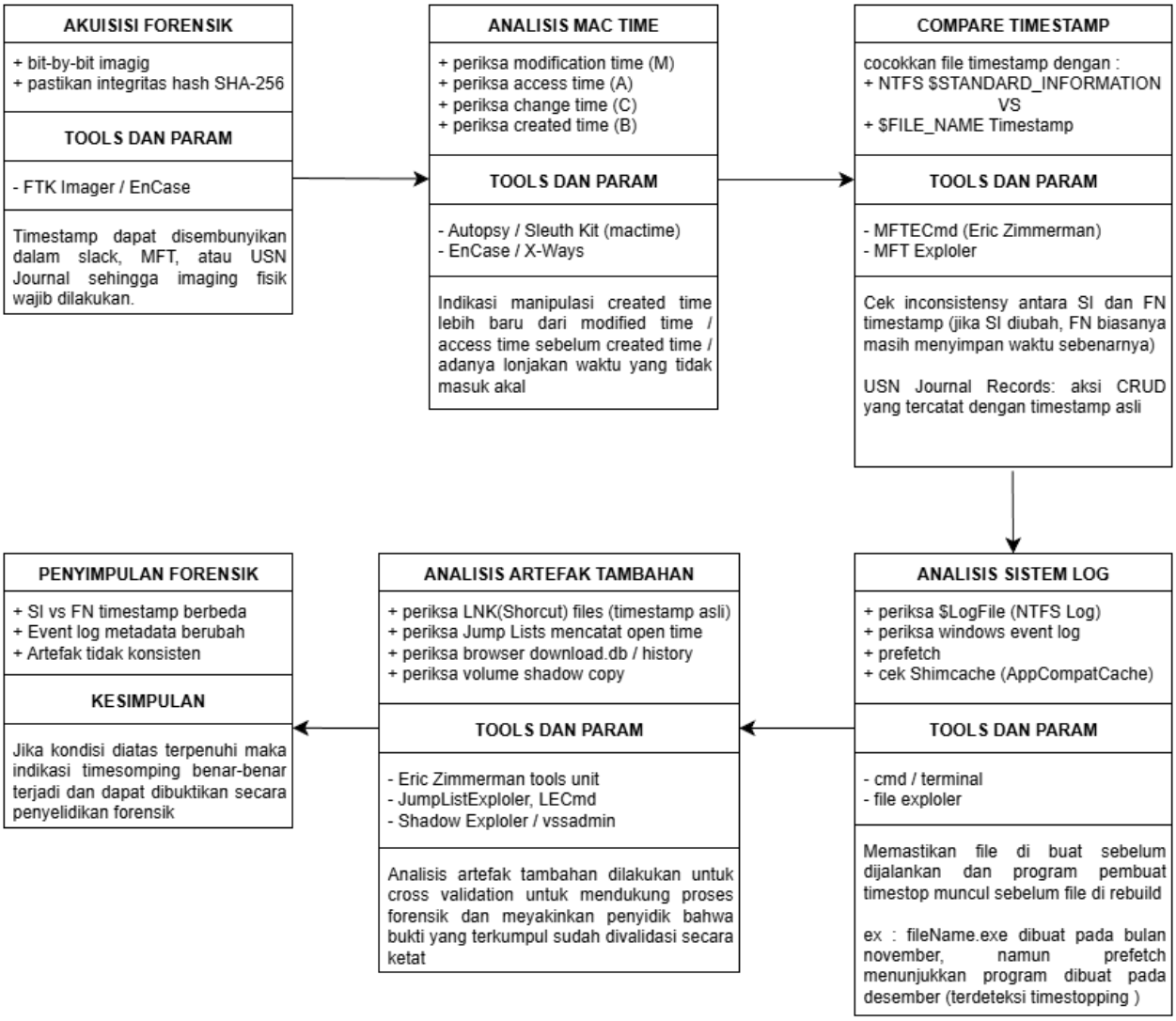
arsitektur Cloud dan IoT bersifat dinamis (proses Create Read Update dan Delete data dilakukan otomatis) dan juga berdasarkan sepengetahuan saya, file yang tersimpan di cctv itu bersifat sementara / temporary yang bisa di akses dalam beberapa rentang waktu saja, sehingga akuisisi akan lebih kompleks dan harus cepat.

- Dalam perangkat fisik, proses validasi dilakukan dengan cara yang mudah (menyalin bit-by-bit dari harddisk untuk di cocokkan dengan sumber aslinya), sehingga selama bukti konsisten / bentuknya tidak berubah maka dianggap autentik. Namun pada layanan cloud, penyidik tidak memiliki akses langsung ke penyimpanan fisik, sehingga proses validasi menggunakan API yang disediakan oleh pemilik layanan Cloud. Banyak layanan Cloud yang menyediakan checksum hash seperti ETag pada AWS S3 atau Content-MD5 pada Azure yang berfungsi untuk memastikan keautentikan bukti. Para penyidik bisa menghitung hash dari Salinan yang di dapat dari proses call API dan membandingkannya dengan hash yang diberikan oleh penyedia layanan. Jika sama maka datanya autentik.

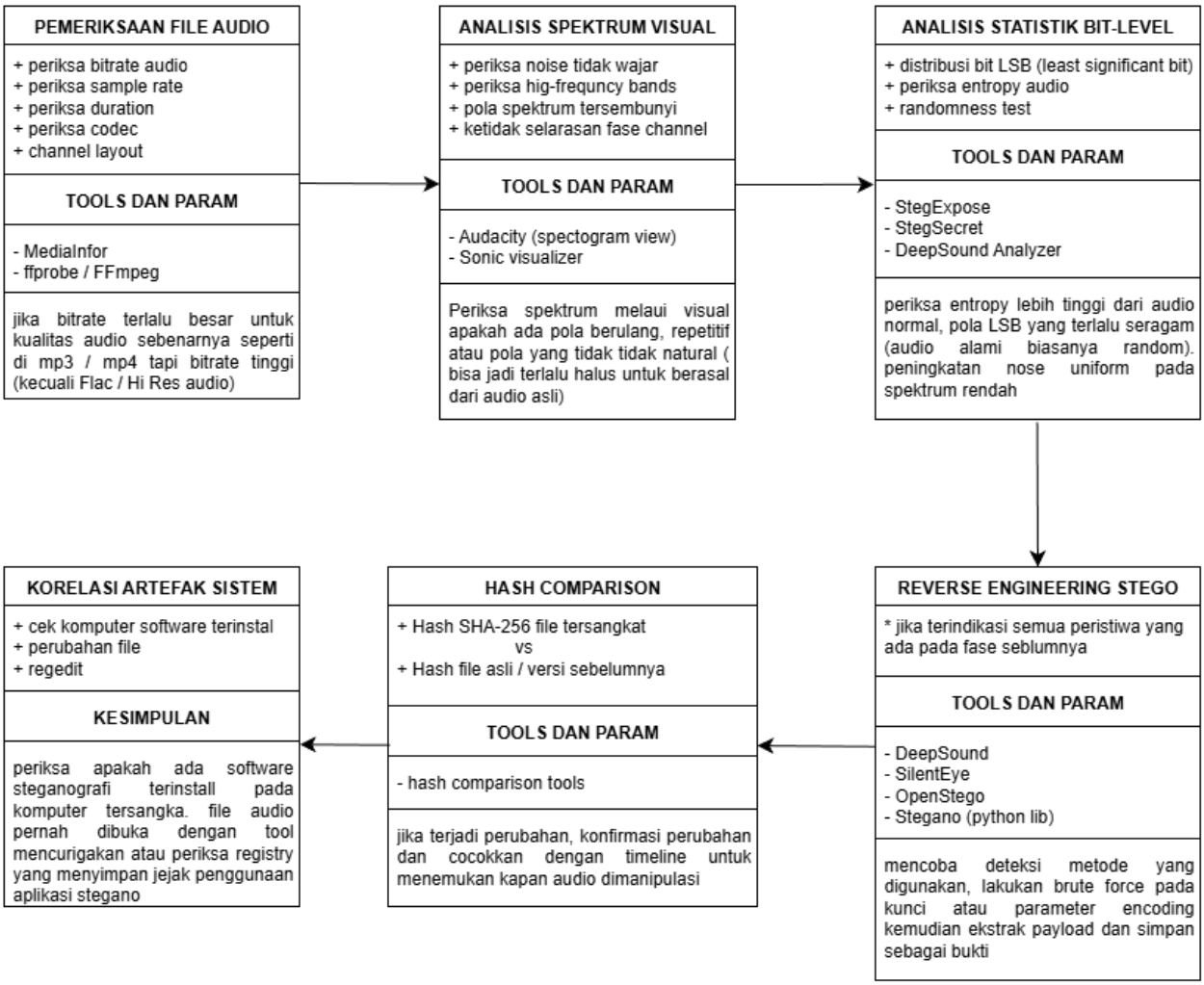
  Beberapa penyedia cloud juga menyediakan log audit yang bersifat immutable (tidak bisa diubah), yang setiap entri log dilindungi oleh digital signature. Dengan melakukan verifikasi terhadap signature tersebut, penyidik dapat memastikan bahwa data tidak dimodifikasi. Untuk memperkuat validasi, penyidik juga kaan mencatat timestamp, nama akun yang dipakai, dan spesifikasi API yang di call. Dukomentasi kemudian dimasukkan ke CoC sebagai bukti bahawa sleuruh proses didokumentasikan, bersifat transparan dan terkontrol.

  Dengan melakukan hal tersebut, metode akuisis dan validasinya berbeda antara perangkat fisik dan Cloud, standar keamanan tetap dapat dipenuhi melalui kombinasi mekanisme hashing, digital signatur serta dokumentasi CoC.

2. Workflow Deteksi Timestomping (Manipulasi Metadata Waktu File) dan audio steganography akan di ilustrasikan pada gambar dibawah.



Gambar 1. Workflow forensik timestomping



Gambar 2. Workflow forensik audio steganography

3. Penanganan temuan berdasarkan kode etik dalam konteks UU perlindungan data pribadi (UU No.27 tahun 2022), investigator hanya berwenang untuk mengakses data sejauh relevansi dengan tujuan investigasi dan dilarang memproses, membaca, mengubah atau menyalin serta menganalisis secara mendalam pada data pribadi yang tidak ada akitannya dengna kasus tersangka. Data pribadi sensitive seperti rekam medis termasuk data pribadi yang dilindungi lebih ketat menurut UU PDP (pada dasarnya seorang investigator memiliki akses teknis, namun ia tidak memiliki hak hukum untuk mengakses data lebih dari kebutuhan investigasi.

Terdapat juga beberapa kode etik forensik digital seperti (USFCE, ISC2, ACFE) yang mengharuskan untuk menjaga kerahasiaan absolut data sensitive yang tidak relevan, tidak mengungkapkan data, mendistribusikan data atau menceritakan temuan data sensitif kepada pihak manapun, serta tidak memindahkan data tersebut ke perangkat lainnya. Investigator dilarang untuk menjadikan data pribadi sebagai lampiran laporan, memeriksa isi data secara mendalam, menilai kehidupan pribadi karyawan berdasarkan temuan pada file tersebut.

Adapun beberapa Batasan wewenang investigator walaupun mereka di beri pekerjaan oleh perusahaan, investigaror bukanlah pemilik data, wewenangnya dibatasi oleh "Term of Engagement" atau ToE / surat penugasan yang biasanya menyebutkan ruang lingkup tentang perangkat apa yang boleh diperiksa, jenis data seperti apa yang relevan dan jelas dengan tujuan investigasi spesifik. UU PDPD dan prinsip legalitas juga berhubungan engnai wewenang investigator hanya boleh mengakses data yang diperlukan untuk mengungkap kecurangan. Untuk data sensistif tidak boleh dianalisis, tidak boleh digunakan sebagai bukti dan tidak boleh dilaporkan kecuali ada dasar hukum lain.

Sebagai investigator ketika menjumpai data pribadi yang tidak relevan mereka harus mendokumentiaskannya secara minimal saja (mencatat terdapat folder pribadi tidak relevan, tidak ada analisis lanjutan dan bukti tidak disentuh melebihi kebutuhan verifikasi minimal tanpa menyalin isisnya.) ketika ditemukan data sensitif yang tidak relevan maka segera hentikan ekplorasi di bagian tersebut untuk mematuhi data minimization, necessity dan privacy by design. Kemudian berikan tandan pada folder atau data sensitive yang tidak di analisis. Ketika dijumpai data sensitive tidak relevan laporkan pada supervisor atau data protection officer (DPO) perusahaan klien (bukan ke para petinggi perusahaan, karyawan lain apalagi disebarkan ke publik). Yang terakhir yaitu jaga kerahasiaan absolut (lakukan mengenkripsi data, minimalkan hak akses pada orang tertentu yang berwenang danberikan watermark atau tanda pada data sensitive yang tidak relevan agar tidak di buka sembarangan).

Adapun resiko yang harus ditanggung ketika investigator melanggar kode etik atau UU PDP antara lain dianggap melakukan pemrosesan data illegal, jika membocokrkan ke pada pihak yang tidak berwenang bisa dipidanakan. Karena sesuai dengan UU hal ini dianggap merusak integritas investigator, menciderai kepercayaan perusahaan dan berpotensi membatalkan hasil investigasi. Investigator forensik digital terikat oleh Batasan professional, hukum dan etika, meskipun ia memiliki akses teknis penuh ke perangkat karyawan, namun investigator tidak berhak memeriksa atau memproses data pribadi sensistif yang tidak relevan dengan kasus.

BAGIAN 1 INTEGRITAS DAN INFROMASI SISTEM

RINGKASAN EKSEKUTIF

Telah dilakukan pemeriksaan forensik digital terhadap disk image laptop milik **Jean**, karyawan M57 Patents, atas dugaan manipulasi data penggajian dan penyalahgunaan akses terhadap dokumen rahasia perusahaan. Laptop Jean (Lenovo IBM ThinkPad) telah diamankan dan citra disknya dibuat dalam format E01 (nps-2008-jean.E01).

TEMUAN POSITIF (DITEMUKAN):

a. Ditemukan file Excel **m57biz.xls** berisi data gaji lengkap dengan Social Security Numbers
b. Ditemukan komunikasi email yang mengindikasikan **serangan email spoofing**
c. Jean mengirimkan file m57biz.xls ke email eksternal **tuckgorger@gmail.com** pada 20 Juli 2008 pukul 08:28 GMT
d. Teridentifikasi **serangan phishing/spoofing** dimana hacker berpura-pura sebagai Alison

TEMUAN NEGATIF (TIDAK DITEMUKAN):

a. Tidak ada aplikasi steganografi atau enkripsi terinstal
b. Tidak ada riwayat browsing mencurigakan (fraud, job, competitor, dll)
c. Tidak ada indikasi file di-rename untuk menyembunyikan isi
d. Tidak ada penghapusan dokumen penting sebelum penyitaan
e. Tidak ada manipulasi timestamp file (timestomping)

TOOLS YANG DIGUNAKAN

Tools	Versi	Fungsi
FTK Imager	3.1.2.0	Hash verification, file export, preview file
Autopsy	4.22.1	Disk analysis, artifact extraction, timeline remodeling
Registry Exploler	1.2.0.0	Analisis windows registry file / hives
Ms Excel	2021	Review artifact file m57biz.xls
Ms Word	2021	Write forensic report

KESIMPULAN:

Jean **BUKAN** pelaku penggelapan data, melainkan **KORBAN** dari serangan social engineering (email spoofing/phishing). Jean secara tidak sengaja mengirimkan data sensitif perusahaan kepada hacker yang menyamar sebagai Alison (atasannya) melalui email palsu.

KORBAN SEBENARNYA:

- Jean: Korban social engineering, tidak memiliki niat jahat
- M57 Patents: Korban kebocoran data karyawan (gaji + SSN)
- Alison: Email-nya di-spoof oleh hacker, kemungkinan email forwarding atau account compromise

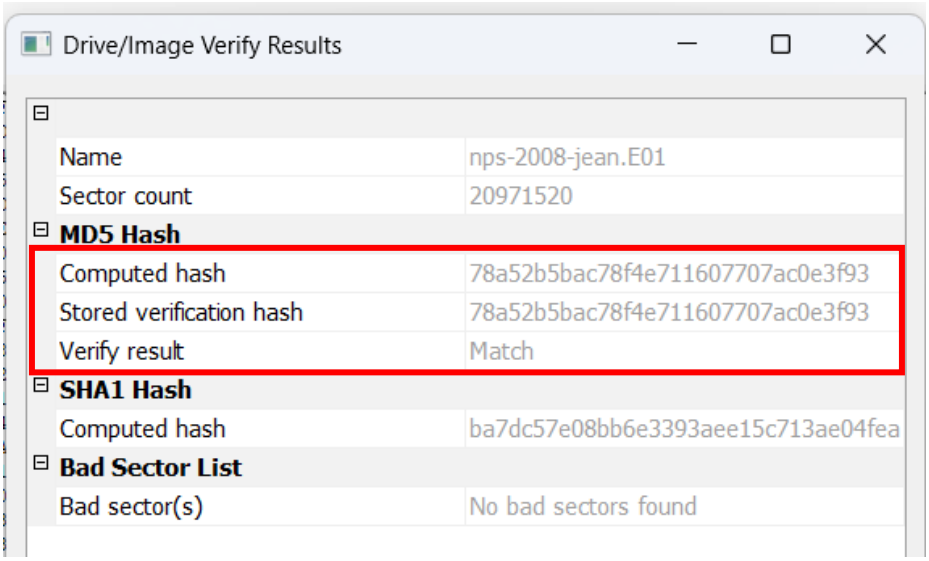
PELAKU:

Hacker dengan email tuckgorge@gmail.com yang melakukan spoofing terhadap identitas Alison

TAHAPAN FORENSIK

1. Verifikasi hash dari file image nps-2008-jean.e01 menggunakan FTK imager.

Proses compute hash menunjukkan bahwa hash MD5 antara computed hash dan stored verification hash sama, yang berarti file image.e01 tidak berubah atau tidak dimodifikasi ketika di download yang tertera pada gambar dibawah.



Gambar 1. Verifikasi hash dengna FTK Imager

2. Identifikasi identitas sistem

- Apa sistem operesi (OS) laptop jean?

Value Name	Value Type	Data	Value Slack	Is Deleted
SubVersionNumber	RegSz			
CurrentBuild	RegSz	1.511.1 () (Obsolete data - do not use)	00-00-00-00	
InstallDate	RegDword	1210714172		
ProductName	RegSz	Microsoft Windows XP	00-00	
RegDone	RegSz			
RegisteredOrganization	RegSz			
RegisteredOwner	RegSz	Jean User		
SoftwareType	RegSz	SYSTEM	00-00-00-00-00-00	
CurrentVersion	RegSz	5.1	8-E4-01-00	
CurrentBuildNumber	RegSz	2600	01-00	
BuildLab	RegSz	2600.xpsp.080413-2111	30-00-33-00-2D-00-32-00-31-00-35-00-38-00...	
CurrentType	RegSz	Uniprocessor Free		
CSDVersion	RegSz	Service Pack 3	00-00-00-00-00-00	

Gambar 2. Data sistem operasi laptop Jean

Sistem operasi laptop Jean yakni Lenovo IBM ThinkPad menggunakan sistem operasi **Microsoft Windows XP versi 5.1** sesuai dengan keterangan hive registry yang diambil dari image file.e01 dengan path *root/WINDOWS/System32/config/SOFTWARE*

- Siapa nama User account utama yang terdaftar pada sistem?

Valid U...	Us...	I...	T...	Created On	Last Login Time	Last Password Chan...	L...	E...	User Name	Full Name	P...	Groups	Comment	U...	H...	I...	R...	A...	H...	P...	T...	N...	...	I...	...	S...	P...
☑	500	0	24	2008-05-13 22:20:14	2008-07-21 01:22:18	2008-05-13 22:23:39			Administrator			Administrators	Built-in account for administering the computer/domain					☐	☐	☐	☐	☑	☐	☐	☐	☐	☑
☑	501	0	0	2008-05-13 22:20:14					Guest			Guests	Built-in account for guest access to the computer/domain					☑	☐	☑	☐	☑	☐	☐	☐	☐	☑
☑	10...	0	0	2008-05-13 21:24:45		2008-05-13 21:24:45			HelpAssistant	Remote Desktop Help Assistant Account			Account for Providing Remote Assistance					☑	☐	☐	☐	☑	☐	☐	☐	☐	☑
☑	10...	0	0	2008-05-13 21:25:56		2008-05-13 21:25:56			SUPPORT_388945a0	CN=Microsoft Corporation,L=Redmond,S=Washington,C=US			This is a vendor's account for the Help and Support Service					☑	☐	☐	☐	☑	☐	☐	☐	☐	☑
☑	10...	0	0	2008-05-14 05:32:56					Kim	Kim		Administrators, Users						☐	☐	☐	☐	☑	☐	☐	☐	☐	☑
☑	10...	0	80	2008-05-14 05:33:08	2008-07-20 00:00:41				Jean	Jean		Administrators, Users						☐	☐	☐	☐	☑	☐	☐	☐	☐	☑
☑	10...	0	0	2008-05-14 05:34:03					Addison	Addison		Administrators, Users						☐	☐	☐	☐	☑	☐	☐	☐	☐	☑
☑	10...	0	0	2008-05-14 05:34:43					Abijah	Abijah		Administrators, Users						☐	☐	☐	☐	☑	☐	☐	☐	☐	☑
☑	10...	0	4	2008-05-14 05:34:54	2008-07-12 03:02:47				Devon	Devon		Administrators, Users						☐	☐	☐	☐	☑	☐	☐	☐	☐	☑
☑	10...	0	0	2008-05-14 05:35:35					Sacha	Sacha		Administrators, Users						☐	☐	☐	☐	☑	☐	☐	☐	☐	☑

Gambar 3. Data user account yang tersimpan

Berdasarkan temuan dari extract data file registry terdapat beberapa user account (administrator, guest, helpAssistant, support, Kim, Jean, Addison, Abijah, Devon dan Sacha), dalam kasusus ini yaitu Jean, memiliki user account dengan group administrator dan user, sehingga dia memiliki wewenang untuk mengakses file / mengeksekusi file pada komputer. File user account ditemukan pada path *root/WINDOWS/System32/config/SAM*

- Berapa timezone yang diatur pada laptop tersebut?

Value Name	Value Data	Value Data Raw
Bias	0	0
StandardName	GMT Standard Time	GMT Standard Time
StandardBias	0	0
StandardStart	Month 10, week of month 5, day of week 0, Hours:Minutes:Seconds:Milliseconds 2:0:0:0	00-00-0A-00-05-00-02-00-00-00-00-00-00-00-00-00
DaylightName	GMT Daylight Time	GMT Daylight Time
DaylightBias	-60	4294967236
DaylightStart	Month 3, week of month 5, day of week 0, Hours:Minutes:Seconds:Milliseconds 1:0:0:0	00-00-03-00-05-00-01-00-00-00-00-00-00-00-00-00
ActiveTimeBias	-60	4294967236

Gambar 4. Data timezone info

Isi data timezone info terdapat standartName GMT standart time, dengan Bias = 0 dan daylightBias = -60, hal ini memiliki arti bahwa timezone terdapat pada **GMT/UTC+0 (London, UK)** dengan dayligt -60 (**musim panas UTC+1**) sesuai dengan hasil value dari timezone info yang berlokasi pada *root/WINDOWS/System32/config/SYSTEM*

BAGIAN 2 ANALISIS AKTIVITAS PENGGUNA

3. Document analysis pada file image ditemukan beberapa file excel seperti pada gambar

Name	Created Date	Modified Date	Last Accessed Date	Size (KB)	File Path
excel.xls	5/14/2008 4:24:10 AM	8/23/2001 7:00:00 PM	5/14/2008 4:24:10 AM	8	\nps-2008-jean.E01\Device0\Root-F...
excel4.xls	5/14/2008 4:24:10 AM	8/23/2001 7:00:00 PM	5/14/2008 4:24:10 AM	4	\nps-2008-jean.E01\Device0\Root-F...
excel4.xls	5/14/2008 4:29:31 AM	8/23/2001 7:00:00 PM	5/14/2008 4:29:31 AM	4	\nps-2008-jean.E01\Device0\Root-F...
excel.xls	5/14/2008 4:29:31 AM	8/23/2001 7:00:00 PM	5/14/2008 4:29:31 AM	8	\nps-2008-jean.E01\Device0\Root-F...
excel4.xls	5/14/2008 4:30:10 AM	8/23/2001 7:00:00 PM	5/14/2008 4:30:10 AM	4	\nps-2008-jean.E01\Device0\Root-F...
excel.xls	5/14/2008 4:30:10 AM	8/23/2001 7:00:00 PM	5/14/2008 4:30:10 AM	8	\nps-2008-jean.E01\Device0\Root-F...
excel4.xls	7/6/2008 1:11:22 PM	8/23/2001 7:00:00 PM	7/6/2008 1:11:22 PM	4	\nps-2008-jean.E01\Device0\Root-F...
m57biz.xls	7/20/2008 8:28:03 AM	7/20/2008 8:28:03 AM	7/20/2008 8:28:03 AM	288	\nps-2008-jean.E01\Device0\Root-F...
EXCEL9.XLS	2/10/1999 2:41:18 PM	2/10/1999 2:41:18 PM	7/6/2008 2:21:30 PM	12	\nps-2008-jean.E01\Device0\Root-F...
SAMPLES.XLS	2/10/1999 2:42:00 PM	2/10/1999 2:42:00 PM	7/6/2008 2:21:30 PM	216	\nps-2008-jean.E01\Device0\Root-F...
SOLVSAMP.XLS	2/10/1999 2:42:04 PM	2/10/1999 2:42:04 PM	7/6/2008 2:21:30 PM	156	\nps-2008-jean.E01\Device0\Root-F...
excel4.xls	7/12/2008 10:02:48 AM	8/23/2001 7:00:00 PM	7/12/2008 10:02:48 AM	4	\nps-2008-jean.E01\Device0\Root-F...
excel.xls	7/12/2008 10:02:48 AM	8/23/2001 7:00:00 PM	7/12/2008 10:02:48 AM	8	\nps-2008-jean.E01\Device0\Root-F...

Gambar 5. Proses carving file excel

Setelah dilakukan pengecekan satu persatu, didapatkan file excel yang berisi data penggajian karyawan yaitu pada file excel bernama **m57biz.xls**. file excel terdapat pada user account Jean, yaitu pada path *root/Document%20and%20Settings/Jean/Desktop/m57biz.xls*.

Setelah proses analisis di **lakukan tidak ditemukan adanya indikasi penyembunyian file atau penggantian nama file**, karena ketika di periksa pada bagian createdDate, ModifiedDate dan LasTimeAcces **tidak ada perubahan** yang berarti file excel tersebut dibuat sekali dan dibuka sekali sesuai dengan timestamp yang disebutkan pada tiga indikator tersebut. Data sensitif terlihat pada file excel m57biz yaitu data SSN (Social security number) masing-masing karyawan.

Pengecekan seluruh excel telah dilakukan, namun Sebagian besar adalah file excel kosong dan ada beberapa yang corrupt, sehingga file m57biz.xls ditetapkan sebagai file excel yang mencurigakan. Berikut ini adalah isi dari file tertera pada gambar dibawah ini.

Name		Position	Salary	SSN (for background check)
Alison	Smith	President	$140,000	103-44-3134
Jean	Jones	CFO	$120,000	432-34-6432
Programmers:				
Bob	Blackman	Apps 1	90,000	493-46-3329
Carol	Canfred	Apps 2	110,000	894-33-4560
Dave	Daubert	Q&A	67,000	331-95-1020
Emmy	Arlington	Entry Level	57,000	404-98-4079
Marketing				
Gina	Tangers	Creative 1	80,000	980-97-3311
Harris	Jenkins	G & C	105,000	887-33-5532
BizDev				
Indy	Counterching	Outreach	240,000	123-45-6789
Annual Salaries			$1,009,000	
Benefits		30%	$302,700	
Total Salaries + Benefits			$1,311,700	
Monthly burn			$109,308.33	

Gambar 6. Isi file excel m57biz.xls

4. Pengecekan browsing history tidak ditemukan history usaha untuk menyembunyikan data dengan menggunakan keyword (encrypt, fraud, competitor, job). History terakhir browsing terlihat seperti jean sedang mencari hotel, tempat wisata, lirik lagu dan shopping pakaian yang tertera seperti gambar dibawah.

Source Name	S	C	O	Domain	Text	Program Name	Date Accessed	Data Source
places.sqlite				google.com	rose quartz chester	FireFox Analyzer	2008-07-21 06:48:37 GMT+07:00	nps-2008-jean.E01
places.sqlite				google.com	rose quartz chester	FireFox Analyzer	2008-07-21 06:47:27 GMT+07:00	nps-2008-jean.E01
places.sqlite				google.com	bailey creek cottages	FireFox Analyzer	2008-07-21 06:46:23 GMT+07:00	nps-2008-jean.E01
places.sqlite				google.com	mineral, ca hotels	FireFox Analyzer	2008-07-21 06:41:46 GMT+07:00	nps-2008-jean.E01
places.sqlite				google.com	CA lava park	FireFox Analyzer	2008-07-21 06:39:03 GMT+07:00	nps-2008-jean.E01
places.sqlite				google.com	CA lava fields	FireFox Analyzer	2008-07-21 06:38:43 GMT+07:00	nps-2008-jean.E01
places.sqlite				google.com	larry king ufo	FireFox Analyzer	2008-07-20 12:06:27 GMT+07:00	nps-2008-jean.E01
index.dat				google.com	lyrics "and ever will my love fo..	Internet Explorer ...	2008-07-17 17:26:00 GMT+07:00	nps-2008-jean.E01
index.dat				google.com	lyrics "and ever will my love fo..	Internet Explorer ...	2008-07-17 17:26:00 GMT+07:00	nps-2008-jean.E01
index.dat				google.com	lyrics "and ever will my love fo..	Internet Explorer ...	2008-07-17 17:26:00 GMT+07:00	nps-2008-jean.E01
index.dat				google.com	lyrics "you're the one I've waite.	Internet Explorer ...	2008-07-17 17:25:45 GMT+07:00	nps-2008-jean.E01
index.dat				google.com	lyrics "you're the one I've waite.	Internet Explorer ...	2008-07-17 17:25:45 GMT+07:00	nps-2008-jean.E01
index.dat				google.com	lyrics "you're the one I've waite.	Internet Explorer ...	2008-07-17 17:25:45 GMT+07:00	nps-2008-jean.E01
index.dat				yahoo.com	eb_clothng	Internet Explorer ...	2008-07-14 21:53:26 GMT+07:00	nps-2008-jean.E01
index.dat				yahoo.com	eb_clothng	Internet Explorer ...	2008-07-14 21:53:26 GMT+07:00	nps-2008-jean.E01

Gambar 7. History browser

5. Pengecekan aplikasi yang terinstall tidak ditemukan aplikasi untuk melakukan enkripsi atau menyembunyikan file, aplikasi yang terinstall selayakanya aplikasi kantoran pada umumnya, untuk produktivitas dan multimedia.

software		0	ICW	2008-05-13 21:25:13 GMT+07:00	nps-2008-jean.E01
software		0	NetMeeting	2008-05-13 21:25:13 GMT+07:00	nps-2008-jean.E01
software		0	OutlookExpress	2008-05-13 21:25:13 GMT+07:00	nps-2008-jean.E01
software		0	DirectDrawEx	2008-05-13 21:25:11 GMT+07:00	nps-2008-jean.E01
software		0	Fontcore	2008-05-13 21:25:11 GMT+07:00	nps-2008-jean.E01
software		0	IE40	2008-05-13 21:25:11 GMT+07:00	nps-2008-jean.E01
software		0	IE4Data	2008-05-13 21:25:11 GMT+07:00	nps-2008-jean.E01
software		0	IE5BAKEX	2008-05-13 21:25:11 GMT+07:00	nps-2008-jean.E01
software		0	IEData	2008-05-13 21:25:11 GMT+07:00	nps-2008-jean.E01
software		0	MobileOptionPack	2008-05-13 21:25:11 GMT+07:00	nps-2008-jean.E01
software		0	SchedulingAgent	2008-05-13 21:25:11 GMT+07:00	nps-2008-jean.E01
software		0	Connection Manager	2008-05-13 21:23:57 GMT+07:00	nps-2008-jean.E01

Gambar 8. Daftar aplikasi yang terinstal

BAGIAN 3 PEMULIHAN DATA DAN FILE TERSEMBUNYI

6. Dokumen atau gambar yang dihapus **tidak ditemukan** file yang terkait dengan kasus Jean, Sebagian besar file yang dihapus merupakan file system atau file hasil generate sistem dan juga ada beberapa file log dan beberapa gambar yang korup seperti yang tertera pada gambar dibawah.

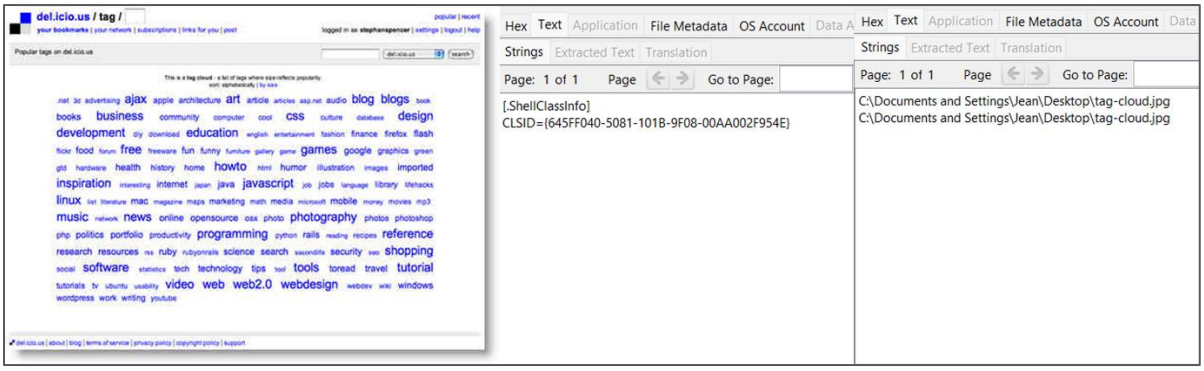
Name	S	C	O	Modified Time	Change Time	Access Time	Created Time	Size	Flags(Dir)	Flags(
Perflib_Perfdata_688.dat				2008-07-21 08:27:09 ...	2008-07-21 08:27:09 ...	2008-07-21 08:27:09 ...	2008-07-21 08:27:09 ...	16384	Unallocated	Unallc
XUL.mfl			1	2008-07-12 01:01:57 ...	2008-07-18 11:31:49 ...	2008-07-18 11:31:49 ...	2008-07-06 15:00:51 ...	928413	Unallocated	Alloca
change.log			1	2008-07-11 12:23:41 ...	2008-07-11 15:09:44 ...	2008-07-11 12:23:41 ...	2008-07-10 14:48:29 ...	84376	Unallocated	Alloca
change.log			1	2008-07-10 14:48:05 ...	2008-07-10 14:48:26 ...	2008-07-10 14:48:05 ...	2008-07-06 14:20:46 ...	23178	Unallocated	Alloca
change.log				2008-07-05 05:54:19 ...	2008-07-05 05:55:29 ...	2008-07-05 05:54:19 ...	2008-07-05 05:51:58 ...	32102	Unallocated	Alloca
change.log				2008-07-05 05:46:35 ...	2008-07-05 05:46:35 ...	2008-07-05 05:46:35 ...	2008-07-05 05:45:55 ...	119904	Unallocated	Alloca
change.log				2008-07-05 05:45:48 ...	2008-07-05 05:45:48 ...	2008-07-05 05:45:48 ...	2008-06-07 12:11:07 ...	119654	Unallocated	Alloca
change.log				2008-06-07 12:11:03 ...	2008-06-07 12:11:04 ...	2008-06-07 12:11:03 ...	2008-05-14 13:48:16 ...	240316	Unallocated	Alloca
change.log				2008-05-14 14:32:27 ...	2008-06-07 12:05:35 ...	2008-05-14 14:32:27 ...	2008-05-14 13:48:16 ...	560146	Unallocated	Alloca

Gambar 9. Daftar file yang dihapus

Pengecekan juga dilakukan pada recycle bin, dan ditemukan beberapa dokumen seperti gambar dan beberapa file, setelah di cek, file gambar tidak ada kaitannya dengan kasus, karena gambar hanya menunjukkan screenshot dari tag website yang lagi trending. Sementara itu untuk file info2 berisi path download dan file .ini hanya berisi shellclass info yang tidak ada kaitannya dengan kasus. Dokumen yang dihapus berada di recycle terdapat pada path *root/vol2/RECYCLER*

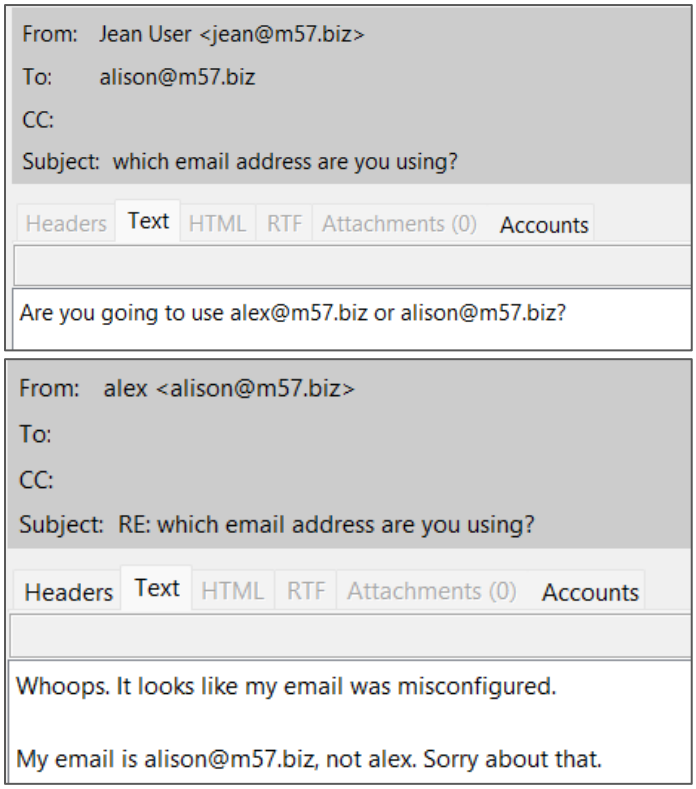
Name	S	C	O	Modified Time	Change Time	Access Time	Created Time	Location
Dc1.jpg				2008-07-11 13:25:19 GMT+07:00	2008-07-12 01:01:00 GMT+07:00	2008-07-12 01:00:37 GMT+07:00	2008-07-11 13:25:19 GMT+07:00	/img_nps-2008-jean.E01/vol_vol2/RECYCLER
desktop.ini				2008-07-12 01:00:56 GMT+07:00	2008-07-12 01:00:56 GMT+07:00	2008-07-12 01:00:56 GMT+07:00	2008-07-12 01:00:56 GMT+07:00	/img_nps-2008-jean.E01/vol_vol2/RECYCLER
[current folder]				2008-07-12 01:01:00 GMT+07:00	2008-07-12 01:01:00 GMT+07:00	2008-07-20 07:00:43 GMT+07:00	2008-07-12 01:00:56 GMT+07:00	/img_nps-2008-jean.E01/vol_vol2/RECYCLER
[parent folder]				2008-07-12 01:00:56 GMT+07:00	2008-07-12 01:00:56 GMT+07:00	2008-07-12 01:00:56 GMT+07:00	2008-07-12 01:00:56 GMT+07:00	/img_nps-2008-jean.E01/vol_vol2/RECYCLER
INFO2				2008-07-12 13:04:36 GMT+07:00	2008-07-12 13:04:36 GMT+07:00	2008-07-12 13:04:36 GMT+07:00	2008-07-12 01:00:56 GMT+07:00	/img_nps-2008-jean.E01/vol_vol2/RECYCLER

Gambar 10. File pada recycle bin



Gambar 11. Isi file yang dihapus di recycle bin

7. Pada komputer jean ditemukan beberapa email cache yang berisi percakapan antara jean dengan orang lain atau sistem, setelah di telurusi dan di baca secara runtut, ditemukan kebingungan antara Jean dengan Allison dan juga beberapa karyawan lain.

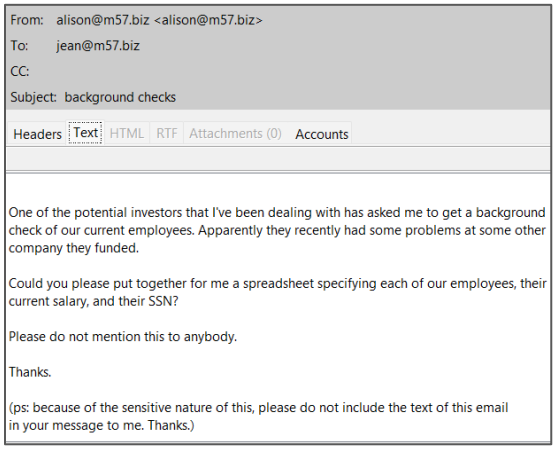


Keanehan dimulai ketika Jane menyadari bahwa Alison memiliki dua email perusahaan yaitu alex@m57.biz dan alison@m57.biz. Pada kejadian ini Jean memastikan bahwa Alison menggunakan yang mana.

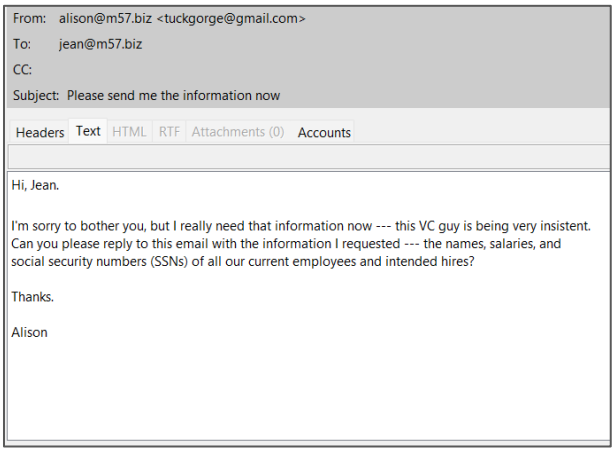
Alison mengkonfirmasi jika ia akan menggunakan alison@m57.biz. Namun setelah beberapa saat Alison mengkonfirmasi kembali bahwa dia salah me-konfigurasi email, dan mengonfirmasi kembali email yang digunakan adalah alison@m57.biz.

Gambar 12 & 13. Percakapan antara Jean dan Alison

Namun sebelum Alison mengkonfirmasi mana emailnya, dia memberi tahu Jean bahwa dia butuh **spreadsheet dari masing-masing karyawan termasuk gaji mereka dan Social Security Number mereka (SSN)**, yang mencurigakan adalah Alison tidak ingin siapapun tahu mengenai hal ini, dan Alison meminta untuk mengirimnya secara langsung via email (tanpa mereply email Alison).

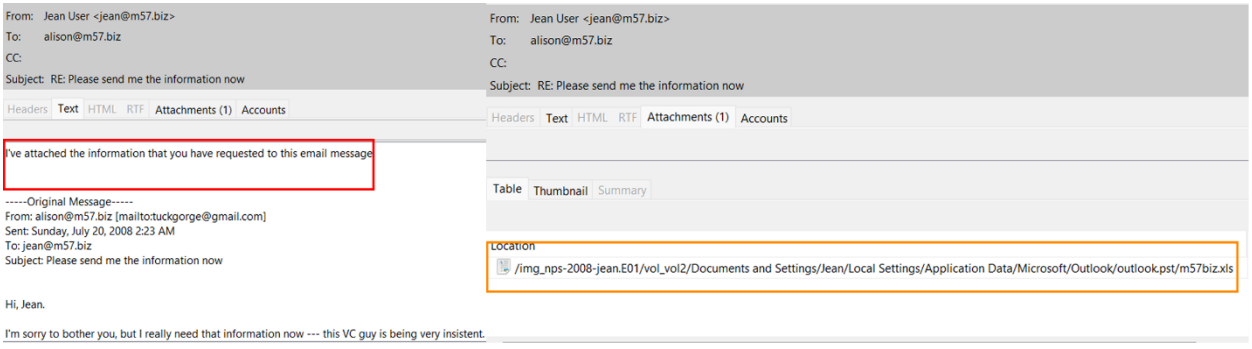


Gambar 14. Permintaan mencurigakan alison



Gambar 15. Permintaan email eksternal

Karena hacker menggunakaan teknik spoofing (peniruan) yang membuat seakan-akan pengirim dari permintaan tersebut adalah Alison yang tertera pada gambar 15.Jean pun menganggap pesan itu dari Alison, maka jean membuat spreadsheet m57biz.xls dan dikirmkan ke email eksternal (hacker) dengan melampirkan file spreadsheet tersebut yang tertera seperti gambar dibawah ini.



Gambar 16. Jean mengirim file spreadsheet ke email eksternal

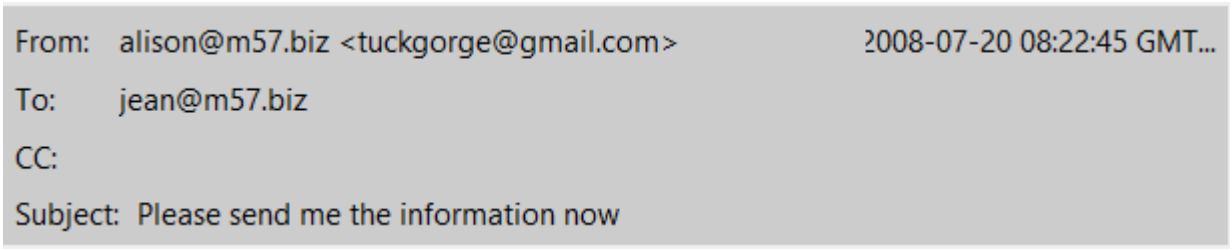
BAGIAN 4 KESIMPULAN DAN KRONOLOGI

REKONTRUKSI TIMELINE

Tanggal	Pukul	Peristiwa
20-07-2008	06:31	Jean meng-konfirmasi mana email yang benar-benar dipakai alison (alex@m57.biz atau alison@m57.biz)
20-07-2008	06:32	Hacker menginisiasi dengan menanyakan tentang proyek keuangan dengan subject “financial plans”
20-07-2008	06:32 – 06:33	Jean mendapat beberapa email spam (kemungkinan untuk mendistraksi jean)
20-07-2008	06:39	Alison meminta permintaan spreadsheet yang mencurigakan tentang data karyawan (salary, SSNs dll)
20-07-2008	06:44	Jean menanyakan kembali email mana yang digunakan alison
20-07-2008	06:44	Jean membalas pesan mencurigakan dari hacker (Alison) dan mengirim text “sure thing” ke email yang digunakan oleh Alison
20-07-2008	06:50	Alison dan Jean kebingungan tentang percakapan “sure thing” di email dan alison memutuskan untuk berhenti mencoba fitur di email
20-07-2008	08:22	Hacker mulai meminta spreadsheet yang berisi data sensitif karyawan perusahaan lewat email eksternal (tuckgorge@gmail.com)
20-07-2008	08:28	m57biz.xls dibuat oleh Jean
20-07-2008	08:28	Jean mengirim data ke hacker via email dan melampirkan file spreadsheet m57biz.xls ke tuckgorge@gmail.com
21-07-2008	06:47	Alison yang asli bertanya ke Jean karena ada yang tidak beres
21-07-2008	07:02	Bob si programmer menanyakan sesuatu terkait gaji Jean dan SSN Jean yang beredar diinternet
21-07-2008	07:11	Bob mengetahui bahwa ada kebocoran data sensitif perusahaan

Berdasarkan proses forensik yang dilakukan, **tidak ditemukan adanya indikasi penyembunyian data, enkripsi data atau penggelapan data oleh Jean**, Jean tidak melakukan Tindakan apapun

yan gmerugikan perusahaan, namun adanya indikasi bahwa Alison kemungkinan terkena serangan Phising, Spoofing dan Teknik email forwarding sehingga hacker mengetahui percakapannya dengan Jean, hal ini diperkuat dengan adanya misconfiguration pada email Alison (alex@m57 dan alison@m57), sehingga hacker melakukan spoofing (penipuan) dengan berpura-pura menjadi Alison dan meminta spreadsheet data sensitif karyawan perusahaan menggunakan email eksternal (tuckgorge@gmail.com).



Gambar 17. Email spoofing dari email eksternal

Berdasarkan keterangan email diatas, pengirim yang asli adalah email tuckgorge@gmail.com, namun hacker menuliskan alison@m57.biz sebagai nama pengirim. Jadi email yang dikirim oleh email eksternal (tuckgorge@gmail.ocm) tampak seolah-olah dikirim oleh Alison. Karena pada aplikasi email, yang ditampilkan pada layar adalah nama pengirim bukan elamat email pengirim.

SARAN DAN LANGKAH REKOMENDASI

1. Tidak menuntut Jean secara pidana
2. Memberikan teguran dan re-training untuk Jean (kelalaian prosedur)
3. Fokus investigasi kepada pelaku (hacker dengan email tuckgorge@gmail.com) dengan bantuan hukum
4. Memperbaiki kelemahan sistem keamananperusahaan yang memfasilitasi serangan ini seperti penambahan email authentication, DLP dan security awareness)
5. Menjadikan insiden ini sebagai pembelajaran untuk organisasi

Kasus ini adalah contoh dari beberapa kasus kategori “Organizational Security Failure” dimana individual negligence yaitu Jean diperbesar oleh system vulnerabilities, pada kasus ini yaitu email authentication lemah, no DLP, dan security training yang masih minim. Perusahaan diharapkan membangun security culture dan technical control yang solid agar kejadian seperti ini tidak terulang di masa yang akan datang.