ANALISIS FORENSIK KOMPUTER PADA LALU LINTAS JARINGAN

Samuel A. Mandowen[1]
[1] Prodi Sistem Informasi Jurusan Matematika FMIPA Universitas Cenderawasih, Jayapura

ABSTRACT

The purpose of this research is to analyze and report the contents of a network-captured file (nitroba.pcap.zip), which is an archive containing network based activities monitored and logged in Nitroba University network using network forensics tool called Wireshark. The network capture file downloaded from file share website/repository of Queensland University of Technology (QUT) Brisbane, Australia. This network-captured file contains activities may against cyber laws. In addition, this file was extracted to nitroba.pcap file on a local hard drive before carrying out forensic analysis. The network reported that there were activities by an individual sending harassing email to Lily Tuckrige. The message contains an IP address 140.247.62.34 in the message full headers and IP address points to Nitroba University dorm room. The analysis attempts to reconstruct the structure of the network, identify key players in the network and determine all activities leading to and occurring during the reported malicious activity. The analysis was carried out mainly using network forensic tools such as Wireshark v1.10.2 and NetworkMiner v1.5. The analysis of a network capture file nitroba.pcap resulted in the recovery of a number of value evidences. Final computer forensics investigation resulted in three main key findings and six item of supporting evidences from the analysis. Two items of the evidence containing the same message sent to Lily Tuckrige. One HTTP packet indicated the suspect's email address, namely jcoachj@gmail.com and six packets contain hostile messages. All the items of the evidence traced from IP address 192.168.15.4 and proved that Johnny Coach, one of Lily Tuckrige's students was the person who sent the harassing emails.

Keywords : Computer Forensics, Network Traffic.

PENDAHULUAN

World Wide Web (WWW) dan Internet telah mempermudah communikasi keseluruh belahan dunia dan memungkinkan setiap orang dapat berinteraksi secara langsung.Namun, teknologi Internet ini juga memungkinkan terjadinya tindakan-tindakan criminal pada dunia Internet atau cybercrime, misalkan pengiriman pesan-pesan ancaman atau intimidasi kepada orang-rang yang tidak bersalah. Penelitian-penelitian terkait teknologi informasi dan komputer (TIK) menunjukkan bahwa jumlah pengguna internet semakin meningkat, demikian pula jumlah aktifitas illegal, yakni, pencurian data, identitas seseorang, dan lain-lain meningkat secara eksponensial (Meghanathan, Allan dan Moore, 2009).

Forensik komputer bertujuan untuk melakukan pengumpulan dan analisis data yang diperoleh dari sistem komputer, jaringan komputer, arus komunikasi menggunakan kabel maupun tanpa kabel (*wired and wireless*) dan media-media penyimpan data dengan cara yang dapat diterima di pengadilan (Kessler, cited in Meghanathan, Allan dan Moore, 2009).

Dibandingkan dengan forensik komputer, dimana bukti-bukti biasanya disimpan dalam media penyimpan data, sedangkan data yang diperoleh pada jaringan adalah sangat *volatile* atau sudah untuk diprediksi. Para penyidik hanya dapat melakukan pengujian dan analisis jika filter packet dan *intrusion detection system* di set up pada jaringan komputer untuk mengantisipasi jika pelanggaran-pelanggaran pada jaringan komputer.

Image file yang digunakan sebagai contoh kasus dalam penelitian ini diperoleh pada repository website Queensland University of Technology (QUT) Brisbane , Australia, yakni nitroba.pcap.zip. *Image file* ini di monitoring dan direkam menggunakan aplikasi jaringan yaitu Wireshark yang pada port Ethernet pada jaringan *computer University Nitroba*. Paket jaringan yang direkam tersebut mengandung aktifitas-aktifitas

* *Alamat korespondensi* :
Kampus Uncen Waena, Jurusan Matematika, Program Studi Sistem Informasi, Jayapura
e-mail: kandera.awin@gmail.com

yang di kategorikan melanggar hukum atau sering disebut *cybercrime*.

Investigasi ini menggunakan dua aplikasi utama yang sangat penting untuk melakukan analisis forensik pada jaringan komputer yaitu; Wireshark dan NetworkMiner. Dua aplikasi lain yang digunakan adalah HashCalc, digunakan untuk melakukan verifikasi integritas dari paket jaringan yang direkam pada jaringan dan Network location, yaitu aplikasi berbasis web yang digunakan untuk memetakan lokasi secara geografi dari alamat IP dimana kejahatan kriminal jaringan komputer tersebut terjadi.

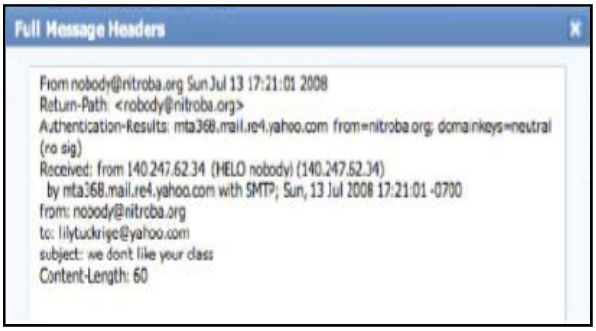
BAHAN PENELITIAN

Bahan yang digunakan penelitian ini adalah sebuah kasus yang terjadi pada Lily Tuckrige, seorang guru kimia pada Universitas Nitroba, dilaporkan bahwa terdapat pesan-pesan ancaman yang masuk ke alamat email pribadinya Lily Tuckrige, yaitu lilytuckrige@yahoo.com. Akibat dari pengiriman pesan ancaman ini yang dianggap melanggar hukum dalam dunia internet (cyber law), maka Lily Tuckrige memutuskan untuk melaporkan tindakan ancaman yang dilakukan terhadap dirinya dengan mengcapture isi dari pesan ancaman tersebut kepada Team Incident Response pada Universitas Nitroba untuk melakukan investigasi lanjutan terhadap kasus tesebut. Meresponi masalah ini, penyidik forensik jaringan meminta Lily Tuckrige melakukan screenshoot ulang pesan dengan full header. Pada full header pesan tersebut menunjukkan bahwa pesan tersebut diterima dari almt IP 140.247.62.34, dimana alamat IP tersebut merujuk salah satu kamar pada asrama Universitas Nitroba dan kamar tersebut di tempati oleh Alice, Babra dan Candice. Jaringan pada kamar tersebut memiliki 10 mbps Ethernet dan juga sebuat router Wi-Fi tanpa password yang diinstal oleh teman Babra. Selain ketiga orang yang menempati kamar pada asrama terebut ada juga beberapa siswa dari Lily Tuckrige yang mungkin juga bertanggung jawab atas pesan ancaman tersebut. Siswa-siswa yang ada pada kelas Lily Tuckrige adalah; Amy Smith, Tuck Gorge, Johnny Coach, Nancy Colburne, Esther Pringle, Jenny Kant, Burt Greedom, Ava Book, Jeremy Ledvkin, Tamara Perkins dan Asar Misrad.

Akibat dari pengiriman sejumlah pesan yang dikirim ke email yang sama milik Lily Tuckrige, maka Team Incident Response pada Universitas Nitroba memutuskan untuk memasang aplikasi jaringan pada port ethernet untuk mendeteksi dan merekam semua paket informasi yang melewati jaringan tersebut. Setelah menangkap semua paket pada traffik jaringan, para penyidik melakukan uji forensik dari aktifitas illegal tersebut dan mengungkapakan jika pelaku kriminal pada jaringan tersebut adalah salah satu dari mereka yang disebut di atas.

Bukti awal

Gambar 1 dan 2 menunjukkan isi dari pesan pelecehan atau ancaman yang dikirim oleh tersangka ke Lily Tuckrige, dosen kimia pada Universitas Nitroba.Hasil screenshot dari kedua pesan tersebut dikirim ke tema Incident Response untuk infestigasi forensic.Kedua bukti awal tersebut sangat penting bagi team investigasi lebih jauh dalam mengungkapkan pelaku. Gambar 1 menunjukkan header dari pesan pertama yang berisi pesan intimidasi dan informasi lain termasuk alamat IP (140.247.62.34) yang menunjukkan lokasi dimana pelaku melakukan aktifitas tersebut. Dalam beberapa hari kemudian pesan anonim lain dikirim ke alamat email Lily Tckrige yang mengandung pesan ancaman yang sama, lihat gambar 2.



Gambar 1. Header dari email yang menunjukkan pesan ancaman dari pelaku.

Gambar 2. Pesan anonim lain yang dikirim ke alamat email Lily Tuckrige

Verifikasi Paket Jaringan

File Image yang digunakan dalam analisis forensik ini direkm pada jaringan yang terdapat pada Universitas Nitroba. File paket jaringan tersebut memuat banyak paket data yang direkam dengan menggunakan aplikasi jaringan. Ferifikasi file image yang di rekam dikalkulasi menggunakan aplikasi HashCalc untuk memastikan integritas dari file image tersebut.

Tabel.1. Perbandingan Nilai Hash

Nilai hash asli yang ditunjukkan pada QUT Fileshare website	Hasil calculasi menggunakan HashCalc v2.02
nitroba.pcap.zip	**nitroba.pcap.zip**
MD5:A8904F79024119687	MD5:A8904F7902411968
BB4F788D460D0E0	7BB4F788D460D0E0
SHA1:	SHA1:
C85A1624B734E8B12EA38	C85A1624B734E8B12EA3
6CA8E2E5613EFA7A074	86CA8E2E5613EFA7A074
nitoba.pcap	**nitroba.pcap**
MD5:01961738FE44A6161	MD5:01961738FE44A616
8A52035D6775C47	18A52035D6775C47
SHA1:4FCC4EDF96895564	SHA1:4FCC4EDF9689556
0C7C713741524F4820375	40C7C713741524F482037
D1C	5D1C

Ringkasan Informasi Paket Jaringan

Hasil ekstrak dari file paket jaringan (nitroba.pcap) menunjukkan parameter-parameter forensik seperti ditunjukkan pada table 2. Informasi lain dari file pakaet jaringan yang di rekam tersebut dapat dilihat juga pada gambar 4, menggunakan aplikasi Wireshark.

Tabel 2. Ringkasan Informasi mengenai file rekaman pada jaringan

File: general information about the capture file	
Name:	nitroba.pcap
Length:	57,054,792 bytes
Format:	Whireshark/tcpdump/... - pcap
Encapsulation:	Ethernet
Packet size limit:	4,096 bytes
Time: the timestamps when the first and the last packet were captured (and the time between them).	
First Packet:	2008-07-22 11:51:07
Last Packet:	2008-07-22 16:13:47
Elapsed:	04:22:39
Capture : information from the time when the capture was done (only available if the packet datawas captured from the network and not loaded from a file).	
Interface:	Unknown
Dropped packets:	Unknown
Capture filter:	Unknown
Link type:	Ethernet
Packet size limit:	4096 bytes
Display: some display related information.	
Display filter:	None
Ignore packets:	0 (0.000%)
Traffic: some statistics of the network traffic	
Packets:	95,414
Between first & last packet:	15,759.951 sec
Average packets/sec:	6.054
Average packet size:	581.971 bytes
Bytes:	55,528,144
Average bytes/sec:	3,523.370
Average Mbit/sec:	0.028

METODE PENELITIAN

Aplikasi yang digunakan

Analisis konten dari paket jaringan ini menggunakan dua aplikasi utama untuk forensic jaringan, yaitu Wireshark dan NetworkMiner. Kedua aplikasi terebut dijalankan pada system operasi Windows 64 bit, 3.40GHz Intel ® Core ™ i7-3770 CPU dengan RAM 4 GB. Aplikasi lain yang digunakan dalam melakukan analisis forensik dari file image tersebut adalah HashCal untuk melakukan verifikasi checksum dari image file yang di peeroleh dari repository website QUT. Nettwork location, adalah aplikasi berbasis web pada google map juga digunakan untuk mencari lokasi secara geografi dari alamat jaringan dari IP 140.247.62.34.yang terdapat pada full header dari pesan email ancaman tersebut.

Langkah-langkah

Image file yang dizip, diekstrak menjadi nitroba.pacp kemudian diverifikasi dan dicocokan dengan nilai hash asli menggunakan HashCalc v2.02. Setelah itu, file nitroba.pcap dibuka menggunakan Wireshark v1.10.2 pada sistem operasi windows untuk dianalisis. Analisis awal file image yang telah diekstrak menunjukkan sejumlah paket data yang sangat banyak sehingga dilakukan filter untuk menjejaki trafik-trafik tertentu secara spesifik. Hal ini dilakukan dalam proses analisis forensik agar lebih fokus dan memudahkan pencarian aspek-aspek tertentu yang menunjukkan alamat IP yang menghasilkan paling banyak trafik untuk tipe-tipe file tertentu.

A. Filter dan Kata Kunci

Hasil ringkasan statistik dari file image (nitroba.pcap) berisi 95.414 paket data, maka teknik filter dan kata kunci yang sangat penting untuk digunakan untuk menghemat waktu dan mempermudah pekerjaan. Dalam melakukan analisis menggunakan aplkasi NetworkMiner, beberapa kata kunci penting yang digunakan untuk mencari paket-paket tertentu yang terdapat dalam nitroba.pcap file tersebut antara lain; nitroba, willselfdestruct, teaching, running dan lilytuckrige. Selain itu untuk melakukan filter dan menggunakan kata kunci untuk mencari paket data secara spesifik dapat dilakukan juga menggunakan aplikasi Wireshark, misalkan; ip.dst==192.168.15.4, ip.src==192.168.15.4, ip.addr==192.168.15.4, eth.src==00:17:f2:e2: c0:ce, frame contains teaching, frame contains lilytuckrige, dll. Dalam melakukan analisis menggunakan kedua aplikasi forensik jaringan, teknik filter dan kata kunci digunakan untuk menghemat waktu, memper-mudah pekerjaan dan mengidentifikasi paket data pada trafik jaringan yang dilakukan oleh pernye-rang yang ditargetkan.Tabel 3 menggambarkan beberapa teknik filter dan kata kunci menggunakan Wireshark v1.10.2. Kata kunci tersebut juga digunakan pada aplikasi NetworkMiner v1.5.

Tabel 3. Filter dan kata kunci yang digunakan

Filter	Deskripsi
ip.src==192.168.15.4	Menunjukkan trafik dari alamat IP192.168.15.4
ip.dst==192.168.15.4	Menunjukkan trafik dari alamat IP192.168.15.4
ip.addr==192.168.15.4	Menunjukkan trafik dari alamat IP192.168.15.4
eth.addr==00:17:f2:e2 :c0:ce	Menunjukkan trafik dari dan ke alamat Ethernet MAC 00:17:f2:e2:c0:ce
ip.src==192.168.15.4 and ip.dst==140.247. 62.34	Menunjukkan trafik dari alamat IP 192.168.15.4 ke alamat IP 140.247. 62.34
http	Hanya menunjukkan paket dengan protokol http
http contains “keyword”	Menunjukkan paket http dengan kata-kata yang lebih spesifik, antara lain nitroba, hide, willself-destruct, learning, tea-ching, harassing, anony-mous, lilytuckrige, Des-troyed, dll.
frame contains “keyword”	Filter menggunakan Wireshark untuk mencari paket yang mengandung nitroba, willselfdestruct, running, teaching, lily-tuckrige, Destroyed, hide, anonymous, nitroba dan kata kunci penting lainnya.
tcp contains “keyword”	Untuk mencari frames tertentu dengan kata-kata tertentu antara lain nitroba, hide, willselfdes-truct, learning, teaching, harassing, anonymous, lilytuckrige, Destroyed, dll.
http&&ip.src==192.168 .15.4	Hanya menunjukkan paket http yang berseumber dari alamat IP 192.168.15.4
eth.src==Apple_e2:c0: ce	Digunakan untuk menunjukkan paket yang bersumber dari nama mesin tersebut.
eth.src==00:17:f2:e2:c 0:ce	Digunakan untuk menunjukkan paket yang bersumber dar alamat MAC tersebut..

B. Pemetaan Jaringan

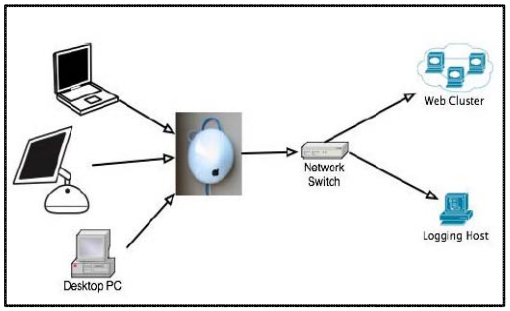
B.1. Lokasi Alamat IP 140.247.62.34

Sebagaimana terdapat pada full header pesan ancaman pada email Lily Tuckrige, menunjukkan bahwa pesan tersebut berasal dari alamat IP 140.247.62.34 yang menunjukkan salah satu kamar asrama pada Universitas Nitroba. Dengan menggunakan aplikasi berbasis web yakni; Netwok Location, maka alamat IP publik tersebut dapat dipetakan dan menunjukkan lokasi secara geografi dari jaringan alamat IP tersebut.

B.2. Topologi Jaringan

Topilogi jaringan mengindikasikan dimana pelaku mendapatkan akses internet dan mengirim pesan ancaman, lihat gambar 6.Berdasarkan full header dari pesan sersebut, alamat IP 140.247.62.34 adalah milik Universitas Nitroba,

dan lebih spesifik lagi adalah kamar dari asrama milik univeritas tersebut. Kamar tersebut dipasang sebuah router Wi-Fi produksi apple yang dapat diakses secara bebas tanpa menggunakan password.



Gambar 4. Topologi Jaringan dimana pelaku mendapatkan akses internet

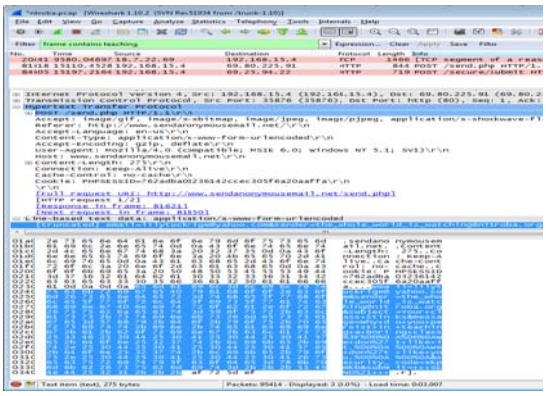
HASIL DAN PEMBAHASAN

Berdasar hasil analisis dan investigasi, ditemukan tiga bukti utama.Dua item dari bukti yang diperoleh sama peris dengan pesan ancaman yang dikirim ke alamat email milik Lily Tuckrige. Bukti lain yang dianggap sangat penting ditunjukkan pada gambar bukti ke-5 pada temuan ini. Semua bukti termasuk temuan yang tidak relevan diekstrak dan di analisa menggunakan Wireshark dan NetworkMiner.

A. Menggunakan Aplikasi WireShark v1.10.2

A.1. Bukti-1

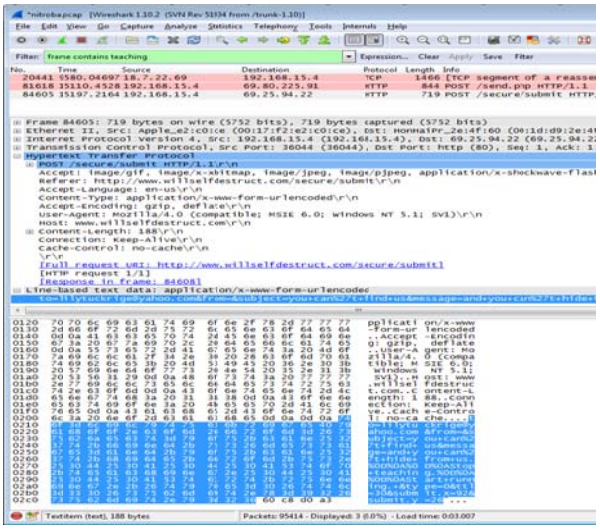
Untuk mengungkapkan pelaku yang dicurigaimengirim pesan ancaman ke Lily Tuckrige, pertama menggunakan kata kunci untuk mencari pesan tersebut. Teknik menggunakan kata kunci dan filter yang dilakukan menggunakan Wireshark adalah “frame contains teaching”, “tcp contains teaching”, “frame contains lilytuckrige”, “frame cointains running”, “frame contains Destroyed” dan kata kunci penting lainnya. Menggunakan filter “frame contains teaching” pada Wireshark menemukan satu bukti yang sangat krusial pada trafik http yang dikirim dan bersumber dari alamat IP 192.168.15.4 ke alamat IP tujuan 69.80.255.91. Isi dari paket data yang dikirim dari alamat IP tersebut memperlihatkan beberapa kata kunci seperti ditunjukkan pada table 3, antara lain; lilytuckrige, anonymous dan teaching. Dengan menggunakan kata kunci lilytuckrige mengindikasikan bahwa pelaku mengirim email ke lilytuckrige@yahoo.com melalui alamat web www.sendanonymousemail.net. Didalam paket tersebut juga terdapat kata kunci lain yang disoroti berwarna biru pada kolom kedua bagian bawah pada Gambar 5.



Gambar.5. Bukti ke-1, diekstrak menggunakan Wireshark v1.10.2

A.2. Bukti-2

Bukti kedua yang diperoleh pada file rekaman jaringan yang telah diekstrak dan dianalisa menggunakan Wireshark dengan menggunakan filter dan kata kunci yang sama menunjukkan bahwa sumber alamat IP yang sama 192.168.15.4 juga mengirim paket dengan kata kunci yang didaftarkan pada table 3. Paket yang dikirim ke alamat email lilytuckrige@yahoo.com melalui alamat web www.willselfdestruct.com mempunyai kesama-an pada pesan kedua yang dikirim ke email milik Lily Tuckrige.

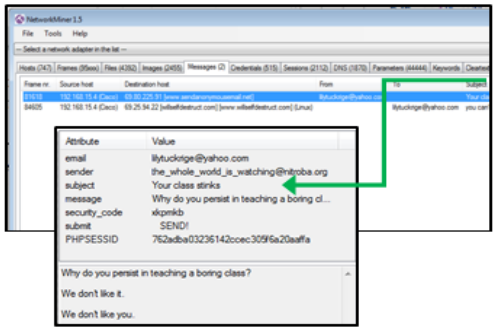


Gambar 6. Bukti ke-2, diekstrak menggunakan Wireshark v1.10.2

B. Menggunakan Aplikasi NetworkMiner v1.5

B.1. Bukti ke-3

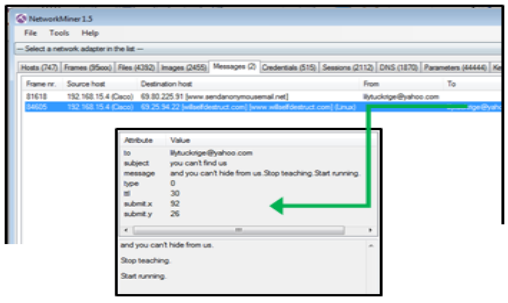
Bukti ke-3 dipeoleh menggunakan aplikasi NetworkMiner. Bandingkan dengan bukti-1 yang diekstrak menggunakan Wireshark, isi dari paket pada frame 81618 pada tab “Message” menunjukkan pesan yang sama persis dengan pesan yang ada pada email Lily Tuckrige. Menariknya, isi dari paket tersebut secara jelas menunjukkan isi dari pesan ancaman tersebut. ukti tersebut dapat dilihat pada colom timestamp pada gambar 7.



Gambar 7. Bukti ke-3, diekstrak menggunakan NetworkMiner v1.5

B.2. Bukti ke-4

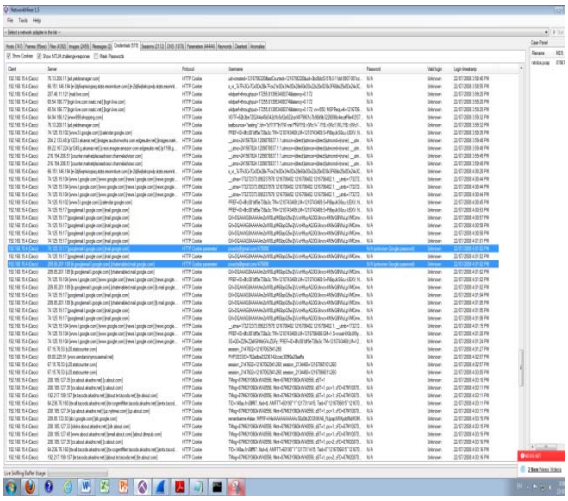
Sama hanya dengan melihat pada frame 84605 dari tab Message pada aplikasi NetworkMiner, bukti ke-4 menunjukkan karakteristik yang sama dan ditemukan pada bukti-2 yang ditunjukkan secara jelas pada isi paket tersebut.



Gambar 8. Bukti ke-4, diekstrak menggunakan NetworkMiner v1.5

B.3. Bukti ke-5

Bukti ke-5 jika dilihat pada tab “credential” aplikasi NetworkMiner, bukti kunci yang diperoleh adalah alamat email (jcoachj@gmail.com) yang adalah initial salah satu siswa yang terdaftar pada kelas yang diajarkan oleh Lily Tuckrige dengan nama lengkap Johnny Coach. Bukti ini diperkuat dengan mengidentifikasi alamat IP yang digunakan oleh pelaku untuk mengakses internet sama persis dengan alamt IP yang diperoleh pada bukti-bukti sebelumnya. Selain itu juga, pelaku menggunakan alamat email yang sama dengan sumber alamat IP yang sama untuk mengirim pada waktu yang sama.



Gambar 9. Bukti ke-5 paket HTTP yang menunjukkan alamt email jcoachj@gmail.com

C. Timeline

Table 3 menunjukkan urutan kejadian-kejadian yang teridentifikasi pada file rekaman jaringan tersebut. Kejadian-kejadian tersebut diurutkan berdasarkan konologis kejadian, memberikan waktu setiap kejadian terjadi, nomor frame dari setiap trafik, alamat IP klien, server dari alamat web, protocol, username, waktu login dan deskripsi dari setiap informasi yang dianggap relevan.

Selama investigasi forensik dilakukan untuk mengungkapkan pelaku pengiriman pesan ancaman tersebut, terdapat beberapa indikasi yang mengarah pada satu mesin apple dengan alamat IP 192.168.15.4 dan alamat MAC 00:17:f2:e2:c0:ce. Indikasi awal menunjukkan bahwa alat dengan alamat IP 192.168.15.4 menghasilkan sejumlah paket yang sangat besar pada file image rekaman jaringan tersebut. Dapat pula dilihat pada trafik paket HTTP yang melewati jaringan tersebut.Setelah mendapatkan beberapa bukti, upaya-upaya lanjutan dilakukan untuk menyelidiki lebih detail lagi dimana ditemukan juga bahwa terdapat dua system operasi yang aktif pada mesin tersebut menggunakan alamat IP 192.168.15.4.Salah satu mesin menggunkan

Windows NT 5.1 dan melakukan browsing menggunakan Mozila v4.Sistem Operasilainnya adalah Mac OSX_5_4, menggunakan Mozila v5.0 dan Safari v525.20.1 untuk aktifitas browsing.Informasi ini diperoleh dari paket HTTP dengan melihat pada “User Agent”.

Tabel 3. Timeline pelaku dengan alamat IP 192.168.15.4

Frame Number	Source IP address	Web address	Protocol	Username	Pswd	Valid Login	Login Timestamp	Description
72836	192.168.15.4	www.google. com	HTTP	-	-	-	22/07/2008 3:57:38 PM	Searching in Google: "How to annoy people"
75334	192.168.15.4	www.google. com	HTTP	-	-	-	22/07/2008 3:58:07 PM	Searching in Google: "I want to harass my teacher"
75924	192.168.15.4	answer.yahoo.com	HTTP	-	-	-	22/07/2008 3:58:32 PM	Searching in Google: "can I go to jail for harassing my teacher?"
	192.168.15.4	mail.google.com	HTTP	jcoachj@gmail.com	-	-	22/07/2008 4:01:02 PM	Logging with username jcoachj@gmail.com
81618	192.168.15.4	www.sendanonymousemail.net	HTTP	-	-	-	22/07/2008 4:02:57 PM	Sending email to : lilytuckrige@yahoo.com sender:the_whole_world_is_watching @nitroba.org subject: Your class stinks message:Why do you persist in teaching a boring class?, We don't like it, We don't like you.
84605	192.168.15.4	www.willselfdestruct.com	HTTP	-	-	-	22/07/2008 4:04:24 PM	sending email to : lilytuckrige@yahoo.com subject: you can't find us message: and you can't hide from us.Stop teaching., Start running.

KESIMPULAN

Dengan menggunakan aplikasi forensik jaringan, yakni Wireshark dan NetworkMiner dalam investigasi ini untuk mengekstrak dan menganalisa paket file yang direkam pada jaringan Universitas Nitroba akhirnya mendapatkan bukti yang jelas , beralasan dan pasti dan dapat digunakan untuk mengungkap pelaku pengiriman pesan ancaman tersebut. Semua bukti diperoleh secara langsung dari alamat IP 192.168.15.4 dengan alamat MAC 00:17:f2:e2:c0:ce. Dengan mempertimbangkan kronologis setiap kejadian dan melihat isi dari setiap paket yang ditelusuri dari alamat IP 192.168.15.4 menunjukkan bahwa Johnny Coach, salah satu siswa dari Lily Tuckrige adalah seseorang yang bertanggung jawab atas pesan ancaman tersebut. Alsan ini sangat masuk akan karena salah satu item dari bukti yang diperoleh menegaskan bahwa alamat IP 192.168.15.4 yang sama yang melakukan login ke alamat email atas namanya yaitu jcoachj@gmail.com. Ketika kesamaan bukti diperoleh, maka Johnny Coach harus ditahan dalam keterlibatannya sebagai pelaku pengiriman pesan ancaman dan dibawah untuk ditanyakan jika melakukan aktivitas-aktivitas yang mungkin sama dsebelumnya.

DAFTAR PUSTAKA

About Wireshark. Retrieved from: http://www.wireshark.org/about.html

Computer Forensics Glossary. Retrieved from: http://burgessforensics.com/glossary.php

Digital Forensics Glossary. Retrieved from: http://www.nij.gov/topics/forensics/evidence/digital/digital-glossary.htm

Glossary of Computer Forensics Terms. Retrieved from: http://www.pcrforensics.com/index.php?option=com_glossary&Itemid=132&task=list&glossid=1&letter=all&page=6

Meghanathan, N., Allam, S. R., Moore, L. A (2009).Tools and techniques for network forensics. Retrieved from: http://arxiv.org/ftp/arxiv/papers/1004/1004.0570.pdf

Offensive/harassing/menacing emails Retrieved from: http://www.police.qld.gov.au/programs/cscp/eCrime/offensive.htm

Sharma, V., (2012). 802.11 Sniffer Capture Analysis - Wireshark filtering. Retrieved from: https://supportforums.cisco.com/docs/DOC-24730

Solomon M. G., dkk. 2011. Computer Forensic, JumpStart. 2nd Edition. Wiley Publishing .

Use NetworkMiner to Analyse Network Traffic. Retrieved from: http://www.makeuseof.com/tag/monitor-network-watch-bandwidth-networkminer/

Wireshark User's Guide: Chapter 6. Working with captured packets. Retrieved from: http://www.wireshark.org/docs/wsug_html_chunked/ChWorkBuildDisplayFilterSection.html