USULAN PENELITIAN

DISERTASI DOKTOR

JUDUL :*USULAN DISERTASI*
PENGUSUL:

UNIVERSITAS KRISTEN SATYA WACANA

AGUSTUS, 2019

DAFTAR ISI

RINGKASAN

Kejahatan internet adalah aktivitas online ilegal yang dilakukan diinternet seperti website, chat rooms dan email. Semakin tingginya jumlah pemakai internet maka kejahatan yang terjadi akan juga semakin tinggi. Peran aktif dari berbagai pihak perlu dilakukan dalam mengungkapkan siapa pelaku aktivitas ini. Tingkat pengungkapan kasus kejahatan internet masih tergolong rendah. Minimnya atau hilangnya barang bukti *(Evidence)* secara digital menjadi salah satu faktor penyebabnya. Data log merupakan basis data dalam melakukan investigasi, ukuran data yang besar merupakan masalah tersendiri. Hasil penelitian menyebutkan dalam satu hari dengan jumlah host 300 komputer membutuhkan 1 TB *(terabyte*) untuk menyimpan data log. Padahal pelaporan terjadinya kejahatan internet sering sekali beberapa hari atau bulan kemudian, kepada pihak berwajib atau penegak hukum.

Analisa traceback merupakan teknik umum yang digunakan dalam proses rekonstruksi kejahatan internet (post mortem analysis). Analisa ini merupakan salah satu bagian dari proses network forensic. Kaidah forensik yang harus dicermati adalah menemukan sumber penyerang dengan tetap menjaga originalitas barang bukti. Untuk menjawab permasalahan diatas maka diusulkan sebuah metode yakni Payload Attribution. Metode ini merupakan suatu metode yang mengambil kutipan (excerpt) dari sebuah payload. Tujuan utama dari metode ini adalah mendapatkan ukuran media penyimpanan yang lebih efisien, dengan tetap menjaga originalitas barang bukti. Sehingga output yang diharapkan adalah barang bukti atau trafik yang efisien baik dari sisi media penyimpanan. Metode Winnowing Multi Hashing sebagai salah satu metode dalam payload attribution diharapkan dapat menjawab masalah dalam penelitian ini.

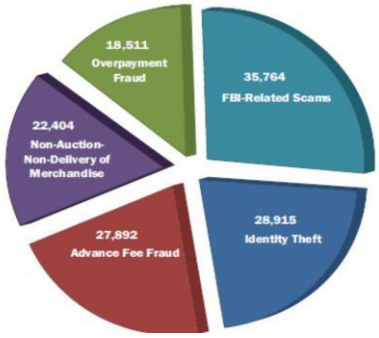
Kata Kunci : *Payload attribution , Winnowing Multi Hashing, , network forensic*

BAB 1. PENDAHULUAN

1.1 Latar Belakang

Gambar 1.1 Data tren kejahatan internet periode 2000 - 2012 (www.ic3.gov)

Dari jumlah komplain yang ada, dapat dikategorikan jumlah kasus yang masuk kategori lima besar pada tahun 2011 adalah seperti pada Gambar 1.2.



Gambar 1.2 Lima besar jenis kejahatan internet

Tabel 1.1 Properti Data Log

Dir	File	Registers	Entries	Time ranges
http	access_log	Requests to the web server.	3554	Jan 30 04:34:59 - Mar 17 11:38:27
	error_log	Errors and results of the requests.	3692	Jan 30 04:33:18 - Mar 17 11:38:27
	ssl_error_log	Errors in SSL connections.	374	Jan 30 04:33:18 - Mar 16 01:01:43
iptables	Iptablesyslog	Connection data flowing through the gateway.	179752	Feb 25 12:11:24 - Mar 31 23:57:48
snort	Snortsyslog	Alarms triggered by the NIDS snort.	69039	Feb 25 12:21:33 - Mar 31 23:49:38
syslog	Maillog	Mail traffic (smtp, pop3).	1172	Jan 30 04:19:27 - Mar 17 04:14:33
	Messages	General system messages.	1166	Jan 30 04:09:22 - Mar 17 13:06:36
	Secure	Login information (sshd,pop3).	1587	Jan 31 06:16:51 - Mar 17 12:59:00

1.2 Rumusan Masalah

Pada penelitian kali ini yang menjadi pokok permasalahan yang akan dibahas adalah :

1.
2.

1.3 Ruang Lingkup Penelitian

Penelitian ini memiliki ruang lingkup sebagai berikut :

1.4 Manfaat Penelitian

1.5 Tujuan Khusus Penelitian

1.6 Urgensi Penelitian

1.7 Keterkaitan dengan Penelitian Disertasi

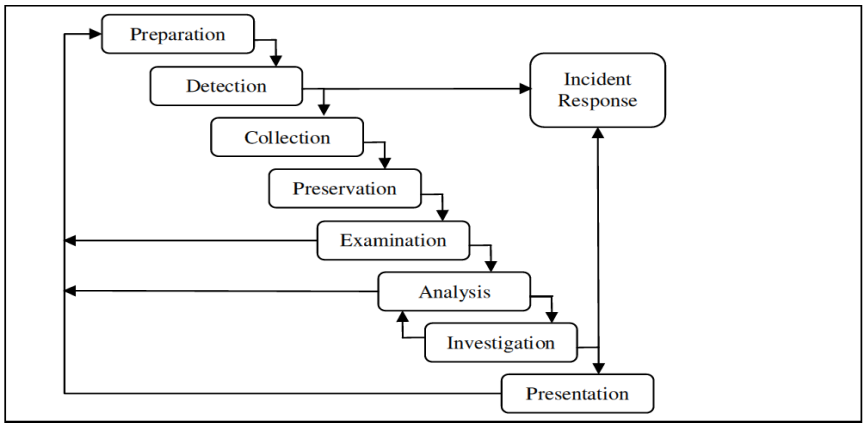
1.8 Kontribusi dalam Area Penelitian (Novelty)

1.9 Luaran Penelitian yang Diharapkan

.

BAB 2. TINJAUAN PUSTAKA

1.1 Bagian Pustaka



Gambar 2.1 Network forensik model generik (Yusoft dkk., 2011)

1.2 Payload Attribution System

1.3 Peta Jalan Penelitian

Peta jalan penelitian dengan tujuan akhir ada menemukan model rekonstruksi kejahatan internet dengan metode *newpayload attributtion*, seperti Gambar 2.5

Item	**2010 -2012**	**2013-2014**
Luaran penelitian		

Gambar 2.5 Roadmap Penelitian

Keterangan

	Sudah Dikerjakan
	Sedang Dikerjakan
	Belum dikerjakan

BAB III

METODOLOGI PENELITIAN

3.1 Tahapan Penelitian

Tahapan seperti pada Gambar

Gambar 3.1 Tahapan penelitian

3.2 Desain Penetian

3.3 Luaran Penelitian

3.4 Lokasi Penelitian

3.5 Indikator Capaian

3.6 Alat dan Bahan Penelitian

BAB 4 JADWAL PENELITIAN

.

4.1 Jadwal Penelitian

S=Semester

No	Kegiatan	Tahun											
		S1	S2										
1.													
2.													
3.													
4.													
5.													
6.													
7.													

DAFTAR PUSTAKA

Asia Pasific Computer Emergency Response Team (APCERT)., 2012, *APCERT Report Annual*, http://www.apcert.org

Almulhem, A. dan Issa, T., 2004, *Experience with Engineering a Network Forensics System*, ISOT Research Lab University of Victoria, Canada

Beverly, R., Simson, G. dan Greg, C., 2011, *Forensic carving of network packets and associated data structures*, Naval Postgraduate School Monterey, California, United States

Lampiran 1

Curriculum Vitae sertai foto berwarna 4x6 pojok kiri,
(lebih menekankan track record penelitian)

3	**PERJALANAN**					
	Kota/Tempat Tujuan	**Volume**		**Biaya satuan**		**Jumlah**
	Transport / akodomasi konsultasi ahli salatiga – Yogya	**3**	**kali**	**500,000**		**1,500,000**
	Transportasi /akodomasi kegiatan konsultasi salatiga –Jakarta	**2**	**kali**	**3,000,000**		**6,000,000**
						7,500,000
4	**LAIN-LAIN**					
	Biaya Seminar Nasional	**1**	**unit**	**2500000**		**2,500,000**
	Biaya Publikasi Internasional	**1**	**unit**	**5000000**		**5,000,000**
						7,500,000

Lampiran 2

SURAT REKOMENDASI

Yang bertanda tangan dibawah ini :

Nama : Prof. Jazi Eko Istiyanto, M.Sc.,Ph.D

Adalah promotor dari mahasiswa Program Doktor Fakultas MIPA Program Studi Ilmu Komputer Universitas Gadjah Mada Yogyakarta atas nama :

Nama : Irwan Sembring

NIM : 09/291810/SPA/00238

Menerangkan bahwa mahasiswa tersebut telah diterima sebagai mahasiswa aktif Program Pasca Sarjana Fakultas MIPA (S3) mulai Tahun Akademik 2009/2010 dan sudah melaksanakan ujian komprehensif proposal dengan judul penelitian **"Rekonstruksi Kejahatan Internet Menggunakan Metode New Payload Atrribution".**

Dengan ini saya memberikan rekomendasi kepada mahasiswa yang bersangkutan untuk mengajukan Hibah Penelitian Disertasi Doktor Tahun Anggaran 2014.

Yogyakarta, 22 Agustus 2013

Wakil Dekan Akademik dan Kemahasiswaan
Fakultas MIPA UGM

Dr.Ing. Ari Setiawan, M.Si.

Promotor

Prof. Jazi Eko Istiyanto, M.Sc.,Ph.D

Lampiran 3

Ketersediaan Sarana dan Prasarana Penelitian

No	**Jenis Item**	Jumlah Kebutuhan	Tersedia	Belum Tersedia	Cara Mengatasi
1	Komputer analisa	4 Unit	4 unit		
2	Router cisco	4 Unit		4 unit	Sewa
3	Gateway	2 Unit	2 unit		
4	IP public	1 paket	1 unit		
5	Hosting			1 GB	Sewa
6	Akses Internet	2 MBPS /Unit	2 MBPS /Unit		
7	Intrusion Detection System	1 Unit	1 Unit		
8	Softaware database rules IDS berbasis payload	1 unit		1 unit	Beli

Lampiran 4. Biodata Pengusul/Peneliti

A.Identitas Diri

1	Nama	Irwan Sembiring,ST.,M.Kom
2	Jenis Kelamin	Laki-laki
3	Jabatan Fungsional	Lektor
4	NIP/NIK	0427
5	NIDN	0619097601
6	Tempat dan Tanggal Lahir	Kabanjahe 19 September 1976
7	Alamat Rumah	Perumahan Satya Asri 2 No 2 RT 4 RW 4 Blotongan –Salatiga, Jawa Tengah
8	No. Telepon/Faks/Hp	08562867047
9	Alamat Kantor	Fakultas Teknologi Informasi Universitas Kristen Satya Wacana, Jl. Diponegoro 52 – 60 Salatiga
10	No. Telepon/Faks	0298-321212 ext. 274/0298-83419240
11	Alamat e-mail	irwan@staff.uksw.edu
12	Lulusan yang telah dihasilkan	S-1 = 50 orang S-2 = 5 S-3= -
13	Mata kuliah yang diampu	1. E-business Security 2. Keemanan jaringan komputer 3. CNAP (Cisco Network Academy Proogram) 4. Business Inteligen 5. Jaringan Komputer

B. Riwayat Pendidikan

	S-1	S-2	S-3
Nama Perguruan Tinggi	UPN ” Veteran ” Yogyakarta	Universitas Gadjah Mada Yogyakarta	Universitas Gadjah Mada Yogyakarta
Bidang Ilmu	Teknik Informatika	Ilmu komputer	Ilmu Komputer /Network security
Tahun masuk/Lulus	1995/2001	2002/2004	2009/masih studi
Judul Skripsi/Thesis/Disertasi	Analisa Investasi menggunakan macro excel 2000	Analisa Ekonomi Dengan Metoda Information Economic Proyek E-Government Studi Kasus Kabupaten Selayar Sulawesi Selatan	Rekonstruksi Kejahatan Internet Menggunakan Metode New Payload Attrubution
Nama Pembimbing/Promotor	1.Drs. Janoe Hendarto,M.I.Kom 2.Frans Richard,ST.,M.Kom	Drs. Jazi Eko Istiyanto.,M.Sc.,P.hD	1.Prof. Jazi Eko Istiyanto.,M.Sc.,P.hD 2. Drs. Edi Winarko, M.Sc.,Ph.D. 3. Dr. Ahmad Ashari, M.Kom

C.Pengalaman Penelitian Dalam 5 Tahun Terakhir

No	Tahun	Judul Penelitian	Pendanaan	
			Sumber	Jumlah (Rp)
	2010	Pemetaan Pemadaman Listrik Berbasis SIG Menggunakan AJAX dan SVG	Program Penelitian Dosen Muda Dikti	8,5 juta

D.Pengalaman Penulisan Artikel Dalam Jurnal Dalam 5 Tahun Terakhir

No	Judul Artikel Ilmiah	Volume/No/Tahun	Nama Jurnal
1	Simulation of IP Traceback with Efficient Probabilistic Packet Marking Algorithm on Distributed Denial of Service Attacks	2/1/2011	IJITNA (International Journal of Information Technology and Network Application)
2.	Topology of Network Forensic with New Payload Attributtion Method	2/3/2011	IJITNA (International Journal of Information Technology and Network Application)

E. Pengalaman Penyampaian Makalah Secara Oral Pada Pertemuan Ilmiah/Seminar dalam 5 Tahun Terakhir

No	Nama Pertemuan Ilmiah/Seminar	Judul Artikel Ilmiah	Waktu dan Tempat
1	International Conference on Technology and Business (ICTBM)	Port Knocking and RSA Method on Iptables Firewall Implementation	Dubai 16-03-2010
2	International Conference on Technology and Business (ICTBM)	Data Authentication in Network Forensic Using MD5 and CRC32 Method	Dubai 16-03-2010

Semua data yang saya isikan dan tercantum dalam biodata ini adalah benar dan dapat dipertanggungjawabkan secara hukum. Apabila di kemudian hari ternyata dijumpai ketidak-sesuaian dengan kenyataan, saya sanggup menerima risikonya. Demikian biodata ini saya buat dengan sebenarnya untuk memenuhi salah satu persyaratan dalam pengajuan Hibah Penelitian Disertasi Doktor

Salatiga, 22 Agustus 2013

(Irwan Sembiring,ST..M.Kom)

Lampiran 5. Surat pernyataan pengusul/peneliti

LAMPIRAN 5.SuratPernyataanPengusul/Peneliti

SURAT PERNYATAAN

Yang bertandatangan di bawahini:

Nama	: IrwanSembiring
NIP / NIDN	: 0427/0619097601
Pangkat / Golongan	: Penata Tingkat I/III C
JabatanFungsional	: Lektor
Alamat	: Perum Satya Asri blok 2 no 2 Blotongan Salatiga

Dengan ini menyatakan bahwa proposal penelitian saya dengan judul : **"EFISIENSI MEDIA PENYIMPANAN DATA LOG MENGGUNAKAN METODE PAYLOAD ATTRIBUTION PADA REKONSTRUKSI KEJAHATAN INTERNET"**yang diusulkan dalam skim penelitian Hibah Disertasi Doktor untuk tahun anggaran 2014**bersifat original dan belum pernah dibiayai oleh lembaga / sumber dana lain**. Bilamana di kemudian hari ditemukan ketidak sesuaian dengan pernyataan ini, maka saya bersedia dituntut dan diproses sesuai dengan ketentuan yang berlaku dan mengembalikan seluruh biaya penelitian yang sudah diterima ke kas negara. Demikian pernyataan ini dibuat dengan sesungguhnya dan dengan sebenar-benarnya.

Salatiga, 22/08/2013

Yang menyatakan,

Mengetahui,

Pembantu Rektor V,

Bidang Penelitian dan Pengabdian Masyarakat,

(Prof. Ferdy S. Rondonuwu, SPd, M.Sc., Ph.D)

(Irwan Sembiring)