P-ISSN : 2598-5094
E-ISSN : 2656-1999

TIBANNDARU

Jurnal Ilmu Perpustakaan dan Informasi

Volume 4 Nomor 1 April 2020

TIBANNDARU

JURNAL ILMU PERPUSTAKAAN DAN INFORMASI

HALAMAN PENANGGUNG JAWAB

Terbit setiap : April dan Oktober

Alamat Sekretaris/Redaksi

Jurusan Ilmu Perpustakaan
Fakultas Ilmu Sosial dan Ilmu Politik Universitas Wijaya Kusuma Surabaya.
Jl. Dukuh Kupang XXV/54 Surabaya Telp. (031) 5677577. Website: jipfisip.uwks.ac.id.
Email: JIPFisip.@uwks.ac.id.

TIBANNDARU

JURNAL ILMU PERPUSTAKAAN DAN INFORMASI

DAFTAR ISI

Sekapur Sirih

Alhamdulillah puji syukur kehadirat Allah SWT yang telah melimpahkan segala rahmat-Nya sehingga pada bulan April tahun 2020 ini Jurusan Ilmu Perpustakaan Fakultas Ilmu Sosial dan Ilmu Politik Universitas Wijaya Kusuma Surabaya dapat menerbitkan Jurnal Tibanndaru: Ilmu Perpustakaan dan Informasi Volume 4 Nomor 1 April 2020.

Dengan terbitnya Jurnal Tibanndaru: Ilmu Perpustakaan dan Informasi Volume 4 Nomor 1 April 2020, besar harapan kami bawasanya Jurnal ini menjadi salah satu media kreativitas bagi pustakawan, dosen ilmu perpustakaan dan informasi untuk mengeksekusi cakrawala pengetahuannya dalam betuk penulisan karya ilmiah. Semakin banyak pustakawan, dosen ilmu perpustakaan dan informasi, dan pemerhati kepustakawanan yang produktif dengan menulis karya ilmiah maka akan menjadi sebuah keniscayaan sebuah eksitensi profesi ini dalam menyumbang gagasan keilmuan untuk kemajuan peradaban berbangsa dan bernegara.

Semoga Jurnal Jurnal Tibanndaru: Ilmu Perpustakaan dan Informasi Volume 4 Nomor 1 April 2020 ini benar-benar bermanfaat dan berguna bagi pengembangan ilmu pengetahuan khususnya ilmu perpustakaan dan informasi. Kami mengucapkan terimakasih yang setinggi-tingginya terhadap semua pihak yang terlibat dalam penulisan Jurnal Tibanndaru: Ilmu Perpustakaan dan Informasi Volume 4 Nomor 1 April 2020 ini baik dari penulis maupun penerbit. Kami (Tim dan Penulis) tentunya banyak kekurangan oleh karena itu saran dan kritik yang membangun sangat kami harapkan.

Tim Redaksi

Representasi *Social Engineering* Dalam Tindak Kejahatan Dunia Maya (Analisis Semiotika Pada Film Firewall)

[1]**Imas Rahmadhtul Hidayah**
[1]Badan Perpustakaan Universitas 17 Agustus 1945 Surabaya
[1]*e-mail: imasrahma@untag-sby.ac.id*

ABSTRAK

Pada era teknologi saat ini, informasi direpresentasikan sebagai asset yang berharga bagi setiap individu maupun organisasi. Terdapat tiga komponen penting dalam keamanan informasi (1) manusia (2) proses (3) teknologi. Bagi pelaku kejahatan dunia maya akan mencari celah dalam ketiga komponen tersebut, tak jarang komponen manusia menjadi targetnya. Dari permasalah yang diatas, peneliti tertarik untuk melakukan kajian dengan menempatkan film Firewall sebagai objek penelitian. Film tersebut menarik karena merupakan salah satu film bergenre *action thriller* yang bertema *cybercrime* pada perbankan. Melalui film tersebut, peneliti akan mengkaji terkait representasi *social engineering* dalam *cybercrime* menggunakan metode analisis semiotik yang dikembangkan oleh Roland Barthes. Hasil menunjukkan bahwa representasi *social engineering* yang tercermin yaitu *reverse social engineering* berbasis interaksi sosial. Makna yang tersirat dalam film Firewall yaitu dalam melindungi informasi perusahaan harus memperhatikan tiga komponen di atas karena pada dasarnya serangan dari dalam sama bahayanya dari serangan luar.

Kata Kunci: *Social Engineering, Dunia Maya, Film*

ABSTRACT

In the current technological era, information is represented as a valuable asset for every individual or organization. There are three important components in information security such as ; (1) human; (2) process; and (3) technology. For perpetrators of cybercrime will look for gaps in the three components, not infrequently the human component becomes the target. From the above problems, researchers are interested in conducting studies by placing the film Firewall as research objects. The film is interesting because it's one of the action-thriller films with a cybercrime theme in banking. Through the film, researchers will examine the related representation of social engineering in cybercrime using the semiotic analysis method developed by Roland Barthes. The results show that social engineering representation is reflected in reverse social engineering based on social interaction. The implicit meaning in the Firewall film that is protecting company information must pay attention to the three components above because attacks from the inside are just as dangerous from outside attacks.

Keywords: *Social Engineering, Cyber World, Film*

A. PENDAHULUAN

Hadirnya teknologi informasi dan komunikasi membawa perubahan besar dalam kehidupan manusia. Semakin canggihnya sebuah teknologi, maka akan semakin berkembang pula kemampuan serta rasa keingintahuan manusia untuk menguasai teknologi tersebut. Fenomena kejahatan dunia maya berkembang sejalan dengan perkembangan tingkat peradaban manusia. Istilah kejahatan dunia maya (*cybercrime*) muncul sebab adanya tindak penyalahgunaan teknologi informasi dengan memanfaatkan kecanggihan

internet. *Cybercrime* merupakan istilah yang digunakan untuk tindak kejahatan yang menggunakan jaringan komputer dengan menyalahgunakan teknologi digital sebagai alat kejahatan utamanya. *Cybercrime* tidak lepas dari permasalahan sistem keamanan jaringan, bila dikaitkan dengan informasi sebagai asset maka informasi memerlukan kehandalan dalam penerapan keamanan jaringan. Hadnagy (2011) mengatakan bahwa keamanan ibarat sebuah *puzzle* dengan dua sisi, pada bagian internal keamanan tersebut terlihat aman dan terjamin namun pada bagian eksternal ditemukan banyak ancaman seperti pencurian, peretasan, dan pengacau yang mencari celah *puzzle* tersebut.

Dalam keamanan informasi, terdapat tiga hal yang menjadi komponen utama keamanan informasi yaitu (1) manusia (2) proses (3) teknologi (Andress dalam Rafizan, 2011). Ketiga aspek tersebut merupakan satu kesatuan dalam membangun sistem keamanan jaringan informasi. Seringkali yang kita ketahui, *hacker* hanya melakukan penyerangan langsung terhadap teknologi namun pada praktiknya bagi para *hacker* manusia merupakan komponen terlemah diantara ketiga komponen tersebut. Pada kasus pembobolan rekening bank yang menimpa Ilham Bintang seorang wartawan senior, salah satu diantara para pelaku merupakan karyawan bank tersebut yang menjual data nasabah bank ke sindikat *hacker*. Melansir dari CNN Indonesia, oknum karyawan tersebut memberikan kesaksian bahwa motif tindakan tersebut atas dasar keinginannya untuk memperoleh penghasilan lebih demi memenuhi tuntutan perekonomiannya. Bagi pelaku kejahatan dunia maya, melihat celah pada komponen manusia merupakan sebuah teknik dalam melakukan tindakan *hacking. Social engineering* atau rekayasa sosial didefinisikan sebagai suatu tindakan memanipulasi seseorang dengan cara melakukan suatu tindakan tertentu atau mencari kelemahan target agar dapat memperoleh informasi, akses, dan mendorong target untuk melakukan aksinya.

Film merupakan salah satu bentuk elektronik media komunikasi massa berupa audio visual yang menampilkan teks, bunyi, gambar, dan kombinasinya. Sebuah film dapat membangun emosi dan perasaan serta perspektif penonton terkait suatu hal. Film dapat digunakan sebagai sarana edukasi yang memberikan wawasan serta pengalaman bagi perkembangan jiwa dan pola pikir pemirsanya. Untuk memberikan edukasi secara sederhana, ringan, mudah diterima serta berbobot dapat dikomunikasikan dalam bentuk film.

Dalam mengkomunikasikan teknik-teknik penyerangan yang dilakukan oleh *hacker*, seorang sutradara Richard Loncraine membuat karya film yang berjudul Firewall. Film tersebut sangat menarik dengan mengangkat tema kejahatan teknologi informasi yang dilakukan oleh seorang karyawan sebuah bank dengan motif untuk menyelamatkan keluarganya dari otak pelaku kejahatan. Pada film Firewall terdapat *plot-twist* dimana yang berkarakter protagonis melakukan tindak kejahatan yang tidak disangka. Sebagaimana yang telah dipaparkan di atas, dalam sebuah film

terdapat makna dan pesan moral yang ditanamkan untuk pemirsa. Makna tersebut dapat disampaikan melalui elemen gambar, gerak, dan suara. Maka pertanyaan penelitian ini adalah bagaimana representasi *social engineering* dalam *cybercrime* pada film Firewall?.

Tujuan penelitian ini untuk mendeskripsikan makna visualisasi *cybercrime* melalui makna denotasi, konotasi, dan mitos pada film Firewall dengan pengungkapan tanda-tanda verbal dan non-verbal dalam teks film menggunakan analisis semitoka Roland Barthes. Dari penelitian ini diharapkan dapat menambah wawasan serta pengetahuan terhadap tindakan *cybercrime* sehingga dapat membuat strategi pengawasan sistem keamanan informasi.

B. METODE PENELITIAN

Penelitian ini menggunakan metode penelitian kualitatif bersifat deskriptif dengan mengumpulkan data-data berupa kata-kata dan gambar. Analisis teks dilakukan dengan analisis semiotika yang mengungkapkan makna dalam sebuah tanda dengan metode pengumpulan data auditif, tekstual, audiovisual, artefak, dan perilaku sosial (Hoed, 2014 dalam Fasah, 2018). Secara umum, semiotika merupakan sebuah ilmu yang mempelajari tanda. Termasuk dalam kajian seni rupa dan media rekam, semiotika dapat digunakan untuk melakukan pembacaan tanda-tanda sehingga dapat menemukan pesan, makna, dan kekuatan bahasa visual suatu karya seni. Dari tanda visual yang muncul akan dianalisis melalui makna denotasi, konotasi, dan mitos pada film Firewall dengan pengungkapan tanda-tanda verbal dan non-verbal dalam teks film.

Dalam pengumpulan data, penelitian ini menggunakan dilakukan dengan cara mengkategorikan teks atau simbol yang berkaitan dengan *social engineering* dalam *cybercrime* pada film Firewall sebagai data primer atau level teks dan level konteks sebagai data sekunder. Teknik analisis data menggunakan (1) level teks dengan analisis semiotika Roland Barthes, teori representasi dan teori *cybercrime* untuk menganalisis teks visual yang ditampilkan pada film Firewall. (2) Level konteks berisi data literature yang berkaitan dengan *social engineering* dan *cybercrime* digunakan untuk memahami makna yang ada. Untuk menafsirkan makna, peneliti menggunakan paradigma interpretatif. Paradigma merupakan suatu prinsip dasar pada diri seseorang tentang suatu pandangan dan membentuk cara pandang terhadap suatu hal.

C. TINJAUAN PUSTAKA

Representasi

The Shorter Oxford English Dictionary (dalam Hall, 1997) mengatakan bahwa kata representasi berkaitan dengan (1) *To represent something is to describe to depict it, to call it up in the mind by description or portrayal or imagination.* (2) *To represent also means to symbolize, stand for, to be a specimen of, or to substitute for.* Menurut Hall, representasi merupakan suatu produksi terkait sebuah makna atau konsep dalam pikiran individu melalui bahasa. Terdapat dua proses dalam representasi (Hall, 1997) yaitu representasi mental dan bahasa. Representasi mental merupakan suatu konsep abstrak yang berada dalam

pikiran masing-masing individu (peta konseptual). Bahasa memiliki peran penting untuk merekonstruksi makna/peta konseptual tersebut ke dalam bahasa yang lazim agar dapat terhubung dengan konsep dan ide tentang suatu hal dengan tanda dari simbol-simbol tertentu. Representasi dalam media diartikan sebagai penunjukan seseorang, kelompok, gagasan atau pendapat tertentu ditampilkan dalam pemberitaan.

Terdapat tiga pendekatan terhadap representasi menurut Hall (1997), sebagai berikut :

1. Reflektif, berkaitan dengan pandangan atau pemaknaan tentang representasi terhadap masyarakat sosial.
2. Intensional, berkaitan terhadap pandangan *creator/producer* representasi tersebut.
3. Konstruksionis, berkaitan dengan bagaimana representasi dibuat melalui bahasa, termasuk kode-kode visual.

Representasi media menurut David Croteau dan William Hoynes merupakan suatu hasil seleksi terhadap hal-hal yang berkaitan dengan kepentingan dan pencapaian tujuan komunikasi. Sedangkan Chris Barker mendefinisikan representasi sebagai konstruksi sosial yang mengharuskan untuk mengekplorasi pembentukan makna tekstual dan memahami cara makna tersebut dihasilkan pada berbagai konteks.

Dari definisi di atas dapat disimpulkan bahwa representasi merupakan penggambaran atau penunjukkan suatu hal tertentu yang ditampilkan dalam bentuk tertentu.

Teknologi Informasi

Dalam bahasa Yunani, kata teknologi berasal dari *techne* berarti keahlian dan *logia* berarti pengetahuan. Secara sempit, pengertian teknologi mengacu pada objek benda untuk memudahkan manusia dalam melakukan aktivitas (Rusman dkk, 2012 dalam Zulkarnaen, 2014). Sedangkan informasi merupakan sebuah data yang telah diolah sehingga dapat memberikan manfaat bagi penggunanya. Kata teknologi dan informasi mengalami perluasan makna seiring dengan berjalannya era globalisasi, apabila kedua kata tersebut dikaitkan bermakna bahwa teknologi informasi merupakan seperangkat alat yang digunakan untuk mencari, memproses, mengolah data sehingga menghasilkan sebuah informasi yang dapat disimpan, dikomunikasikan dan disebarluaskan.

Menurut Williams dan Sawyer (2003), teknologi informasi merupakan suatu teknologi yang menggabungkan komputasi dengan jalur komunikasi berkecepatan tinggi sebagai transmisi data, suara, dan video. Sedangkan Martin (1999) mengatakan bahwa teknologi informasi tidak terbatas pada teknologi komputer (perangkat keras dan perangkat lunak) guna memproses dan menyimpan informasi, melainkan mencakup teknologi komunikasi guna mengirimkan atau mendistribusikan informasi secara luas.

Keamanan Informasi

Informasi merupakan sebuah asset berharga bagi setiap individu maupun kelompok, organisasi maupun lembaga pemerintahan, sehingga penting untuk

menciptakan perlindungan informasi di tengah maraknya kejahatan dunia maya. Pencurian sebuah informasi rahasia akan menimbulkan kerugian serta berdampak pada bagi pelaku serta korban sasaran. Keamanan merupakan sebuah perlindungan dari oknum penjahat yang memiliki tujuan tertentu. Secara konvensional keamanan ibarat melakukan penjagaan pada sebuah perumahan elite, satpam ditugaskan untuk menjaga lingkungan tersebut agar tetap aman dari oknum penjahat. Sama halnya dengan sebuah sistem informasi, secara lebih modern dan digital, perusahaan membangun sebuah sistem keamanan berlapis dan beragam untuk menjaga informasi rahasia perusahaan.

Dalam sebuah sistem, tingkat keamanan adalah ukuran dari segitiga keamanan, fungsionalitas, dan kegunaan. Sistem dikatakan aman apabila sistem tersebut dapat memberikan perlindungan kuat dengan menawarkan semua layanan, fitur dan kegunaan bagi pengguna.

Terdapat tiga hal yang menjadi komponen utama dalam membangun keamanan informasi yaitu (Andress dalam Rafizan, 2011).

1. Proses, merupakan sebuah tahapan proses yang dijalankan dalam membentuk sebuah sistem keamanan berupa standar, prosedur, maupun kebijakan yang tertuang dalam dokumen resmi. Proses merupakan prioritas pertama yang harus diperhatikan untuk menjalankan sistem keamanan tersebut berdasar kebijakan.
2. Manusia, sistem dijalankan oleh penggunanya. Hal tersebut dianggap sebagai titik terlemah dalam sebuah sistem sehingga tak jarang *hacker* menjadikan manusia sebagai target sasaran utama. Selain teknologi, manusia merupakan prioritas kedua yang harus diperhatikan setelah proses.
3. Teknologi, dalam hal ini teknologi menjadi prioritas ketiga yang harus diperhatikan dengan membangun sistem keamanan berupa *firewall, anti-virus, anti-spam,* dan sistem keamanan jaringan lainnya sebagai upaya pencegahan penyerangan eksternal terhadap jaringan.

Kejahatan Dunia Maya

Munculnya teknologi informasi dibarengi dengan maraknya tindak kejahatan dunia maya. Istilah *cybercrime* muncul sebab adanya tindak penyalahgunaan teknologi informasi dengan memanfaatkan kecanggihan internet. Kejahatan dunia maya (*cybercrime)* merupakan istilah yang digunakan untuk tindak kejahatan yang menggunakan jaringan komputer dengan menyalahgunakan teknologi digital sebagai alat kejahatan utamanya. Tindakan kejahatan dunia maya tergolong sebagai tindak kriminal yang tidak dapat dilakukan oleh sembarang orang, pelaku kejahatan ini mempunyai kemampuan pada bidang teknologi. Istilah untuk orang yang melakukan tindakan *cybercrime* dikenal dengan sebutan *hacker.*

Para *hacker* atau oknum penjahat memanfaatkan celah keamanan pada sebuah jaringan untuk menyusup ke dalam jaringan tersebut. Berdasar jenis aktivitas yang dilakukan, *cybercrime* digolongkan dalam beberapa jenis sebagai berikut.

1. *Unauthorized access,* tindak penyusupan secara illegal ke dalam suatu sistem jaringan komputer, misalnya *probing* dan *port.*
2. *Illegal contents,* penyebaran data/informasi melalui internet yang tidak etis dan dianggap melanggar hokum sehingga mengganggu ketertiban umum.
3. Tindakan penyebaran virus yang dilakukan secara sengaja sehingga merusak data dalam komputer, umumnya dilakukan dengan menggunakan email.
4. Data *forgery,* kegiatan pemalsuan data penting yang tersedia di internet.
5. *Cyber espionage, sabotage and extortion. Cyber espionage* merupakan suatu kegiatan penyadapan sistem jaringan komputer sasaran dengan memanfaatkan jaringan internet. *Sabotage and extortion* merupakan tindak kriminal yang dilakukan dengan cara membuat kerusakan atau gangguan terhadap suatu data maupun sistem jaringan komputer yang terhubung dengan internet.
6. *Cyber stalking,* suatu kegiatan untuk melecehkan sasaran dengan memanfaatkan komputer. Kejahatan ini menyerupai terror dengan memanfaatkan media internet.
7. *Carding,* tindak kriminal yang dilakukan dengan cara mencuri nomor kartu kredit dan disalahgunakan dalam transaksi perdagangan elektronik.
8. *Hacking* dan *cracking,* tindak kejahatan yang dilakukan dengan cara pembajakan akun orang lain/situs website, penyebaran virus sehingga merusak data dalam komputer.
9. *Cybersquatting and typosquatting. Cybersquatting* merupakan kegiatan pendaftaran nama domain perusahaan/orang lain untuk ditransaksikan agar memperoleh keuntungan lebih besar. Sedangkan *typosquatting* merupakan kejahatan yang dilakuka dengan membuat domain yang mirip dengan domain orang lain.
10. *Hijacking,* kegiatan pembajakan karya orang lain, misalnya pembajakan perangkat lunak.
11. *Cyber terrorism,* tindak kriminal yang dilakukan dengan cara pengancaman terhadap orang lain/pemerintahan menggunakan alat teknologi informasi dan komunikasi.

Social Engineering

Dalam melakukan penyerangan, oknum penjahat melakukan berbagai teknik agar dapat mencapai tujuannya. Manusia dianggap komponen terlemah dalam sistem keamanan, untuk mendapatkan informasi dan akses tak jarang para *hacker* menggunakan teknik manipulasi terhadap seorang yang dapat memberinya akses. Dalam dunia *hacking,* teknik tersebut dikenal dengan istilah *social engineering* atau rekayasa sosial. *Social engineering* merupakan suatu seni manipulasi psikologis seseorang yang dilakukan oleh oknum penjahat (*hacker*) dengan tujuan agar orang tersebut memberikan informasi rahasia serta akses masuk. *Social engineering* merupakan suatu teknik pencurian data dan informasi rahasia dari seseorang dengan cara melakukan

pendekatan manusiawi melalui mekanisme interaksi sosial. Teknik ini dilakukan dengan cara mengeksploitasi kelemahan manusia. Sebagian besar perusahaan mengabaikan ancaman internal terhadap keamanan sistem, bagi oknum penjahat hal tersebut dimanfaatkan karena dianggap lebih mudah memanipulasi psikologis manusia daripada pekerjaan teknis yang menyerang teknologi dari sistem itu sendiri.

Menurut Dhull & Hooda (2016), teknik *social engineering* terbagi menjadi dua jenis sebagai berikut :

1. Berbasis interaksi sosial, artinya pelaku berhubungan langsung dengan sasarannya melalui interaksi sosial.
   - *Shoulder surfing,* dilakukan dengan cara berdiri bersebelahan dengan sasaran untuk mencuri data pribadi. Misalkan, menguntit PIN ATM sasaran.
   - *Hoaxing,* memberikan informasi palsu dengan cara meyakinkan sasaran sehingga sasaran percaya dan masuk ke dalam perangkap kejahatan.
   - *Tailgating,* pelaku mendapat akses masuk dengan cara menguntit individu yang mempunyai akses legal.
   - *Creating confusion,* pelaku menciptakan hal yang membingungkan dan mengambil kesempatan dalam situasi tersebut.
   - *Dumpster diving,* teknik ini dilakukan dengan cara mencari informasi sampah dokumen yang sudah dibuang.
   - *Impersonation,* teknik ini dilakukan dengan cara meniru identitas/melakukan penyamaran untuk mendapatkan akses legal ke sistem komputer atau jaringan.
   - *Reverse social engineering,* memanipulasi sasaran dengan cara menawarkan bantuan yang memberikan keuntungan bagi sasaran.
2. Berbasis interaksi komputer, artinya pelaku menggunakan komputer untuk mengumpulkan informasi yang diperlukan.
   - *Pop-up windows,* teknik ini dilakukan dengan cara memanfaatkan *pop-up windows* untuk mengelabui pengguna.
   - *Email attachment,* mengirimkan email yang dapat mengintai komputer sasaran.
   - *Phishing,* dilakukan dengan cara menipu untuk mendapatkan informasi pribadi milik sasaran. Biasanya dilakukan dengan cara mengirimkan email mengatasnamakan perusahaan yang berisi form data-data pribadi yang harus diisi.
   - *Brand Spoofing,* dilakukan dengan cara membuat situs palsu suatu merek ternama kemudian menyebarkannya secara acak untuk mendapat sasaran.
   - *Baiting,* dilakukan dengan cara memberikan umpan (dapat berupa perangkat atau lainnya) sehingga menarik perhatian sasaran untuk mengambil umpan tersebut dan dengan demikian pelaku dapat melakukan penyadapan/peretasan data rahasia.

Pola umum dilakukan oleh pelaku *social engineering* (Gartner dalam Rafizan, 2011), yaitu (1) pengumpulan informasi (2) mengembangkan relasi/hubungan (3) mengeksploitasi (3) eksekusi.

Semiotika

Secara umum, semiotika merupakan sebuah ilmu yang mempelajari tanda. Termasuk dalam kajian seni rupa dan media rekam, semiotika dapat digunakan untuk melakukan pembacaan tanda-tanda sehingga dapat menemukan pesan, makna, dan kekuatan bahasa visual suatu karya seni. Penganalisisan makna dalam sebuah film dapat dilakukan dengan metode-metode yang dikembangkan oleh para ahli. Penggunaan teori semiotika yang dikembangkan oleh Roland Barthes yang dikenal dengan istilah semiotika Barthesian sudah umum digunakan dalam penelitian budaya dan seni. Barthes membangun konsep-konsep dasar semiotika menjadi empat bagian, yaitu (1) Tanda : trikotomi tanda, penanda, dan petanda. (2) Sistem ganda : konotasi, metabahasa, dan mitos. (3) Hubungan tanda : hubungan simbolik, hubungan sintagmatik dan hubungan paradigmatik. (4) Bahasa : hubungan dialektis *langue/parole.* Konsep tersebut dibangun oleh Barthes atas dasar pengembangan konsep dasar semiotika Saussurean.

Penelitian Terkait

Hasil penelitian terdahulu menjadi referensi bagi penulis dalam penyusunan penelitian ini. Dalam penelitian tersebut terdapat kesamaan metode dan pendekatan penelitian yang digunakan.

1. Jurnal penelitian Rieka Mustika yang berjudul Representasi Nilai-Nilai Edukasi Pada Simbol dan Elemen Video Iklan Layanan Masyarakat Internet Sehat Aman (2017). Penelitian tersebut menggunakan pendekatan kualitatif yang bersifat deskriptif. Pengumpulan data penelitian dilakukan dengan dua unsur yaitu level teks dan level konteks. Level teks dianalisis menggunakan analisis semiotika Roland Barthes serta level konteks dilakukan dengan cara mengumpulkan literatur yang terkait dengan sosialisasi dan edukasi.
2. Skripsi Ayu Purwati Hastim yang berjudul Representasi Makna Film Surat Kecil Untuk Tuhan (Pendekatan Analisis Semiotika) pada tahun 2014. Penelitian tersebut berjenis kualitatif deskriptif dengan pendekatan analisis semiotika. Metode penelitian yang digunakan dalam analisis semiotik adalah interpretatif. Teknik analisis data yang digunakan menggunakan analisis semiotika model Charles Sanders Peirce untuk menganalisis struktur tanda (level sintagmatik) dan representasi makna (level paradigmatik) pada film.

D. HASIL DAN PEMBAHASAN

Analisis Temuan Data

Film Firewall dirilis pada 10 Februari 2006 bergenre *action thriller* yang disutradarai oleh Richard Loncraine. Naskah film berdurasi 105 menit ini ditulis oleh Joe Forte. Firewall dibintangi oleh Harrison Ford, Paul Bettany, Virginia Madsen, Carly Schroeder, Jimmy Bennet, Mary Lynn Rajskub, Robert Patrick, Robert Forster, Alan Arkin, Matthew Currie dan

lainnya. Para aktor dan aktris tersebut memiliki peran masing-masing, sebagai berikut sebagian nama tokoh yang terkait dalam pengungkapan pokok bahasan dalam film Firewall :

Tabel 1. Peran dan Penokohan

No.	Nama Tokoh	Peran	Keterangan
1.	Jack Stanfield	Kepala Sistem Keamanan Jaringan	Pemeran Utama
2.	Bill Cox	Pebisnis/Investor	Pemeran Utama
3.	Beth Stanfield	Istri Jack	Pemeran Pendukung
4.	Sarah Stanfield	Anak perempuan Jack	Pemeran Pendukung
5.	Andy Stanfield	Anak laki-laki Jack	Pemeran Pendukung
6.	Janet Stone	Resepsionis Jack	Pemeran Pendukung
7.	Harry Romano	Rekan kerja Jack	Pemeran Pendukung
8.	Liam	Kawanan Cox	Pemeran Pendukung
9.	Vel	Kawanan Cox (*hacker*)	Pemeran Pendukung
10.	Pim	Kawanan Cox	Pemeran Pendukung
11.	Willy	Kawanan Cox	Pemeran Pendukung
12.	Bobby	Staf Landrock Pacific Bank	Pemeran Pendukung

Fokus yang ditonjolkan dalam film ini adalah tindakan pencurian yang dilakukan dengan menggunakan jaringan komputer. Otak pelaku kejahatan memanfaatkan kelemahan sasaran agar dapat membekuk sasaran untuk turut serta membantu pelaku mendapatkan uang nasabah yang diinginkan.

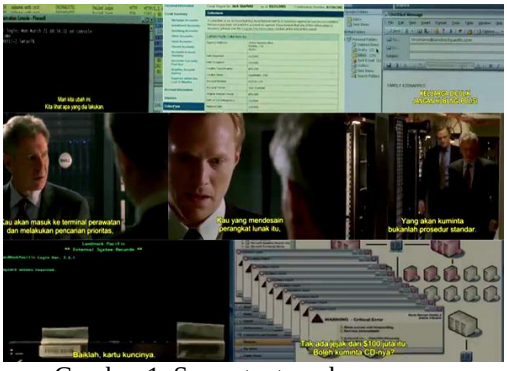
Dalam film Firewall, terdapat kejahatan dunia maya yang diilustrasikan dalam adegan-adegan diantaranya :

- C*yber terrorism,* menggunakan telepon genggam untuk menerima data foto penyanderaan keluarga Stanfield yang dikirimkan oleh salah seorang kawanan Cox.
- Intersepsi/penyadapan yang ditunjukkan dalam adegan pemasangan alat-alat penyadap seperti *wide lens* serta pemancar audio yang dilakukan oleh kawanan Cox kepada Jack.
- *Cracking* yang ditunjukkan dalam adegan peretasan akun email pribadi milik Jack Stanfield dilakukan oleh Vel (kawanan Cox).
- *Carding* ditunjukkan dalam adegan pengalihan uang digital dalam rekening nasabah Landrock Pacific Bank.
- *Unauthorized access* ditunjukkan dalam adegan penggunaan komputer server milik Bobby untuk mengakses sistem jaringan data nasabah secara illegal serta penyalahgunaan komputer untuk menghapus data arsip elektronik CCTV Landrock Pacific Bank.
- *Sabotage & extortion* ditunjukkan dalam adegan pelumpuhan seluruh sistem jaringan komputer dalam gedung Landrock Pacific Bank sehingga komputer tersebut tidak dapat berfungsi sebagaimana mestinya selama beberapa saat.

Analisis *screen shoots* pada film Firewall dilakukan untuk melakukan analisis teks dengan memperhatikan dimensi denotasi, konotasi dan mitos.

Untuk menafsirkan makna, peneliti menggunakan paradigma interpretatif.

- Scene tentang keamanan informasi



Gambar 1. Scene tentang keamanan informasi

Denotasi

1. Terdapat kata 'Firewall' yang diilustrasikan pada tampilan layar komputer.
2. Pada layar komputer menunjukkan saldo terhutang tokoh Jack.
3. Jack mengirimkan email untuk meminta bantuan.
4. Cox tidak dapat mengakses masuk data krusial nasabah sehingga meminta Stanfield melakukannya.
5. Jack merupakan ahli IT yang membangun sistem keamanan perusahaan tersebut.
6. Tindakan yang Cox minta kepada Jack bukanlah hal yang mudah dilakukan karena terdapat standar prosedur.
7. Untuk menjalankan perintah *maintenance,* membutuhkan kunci akses.
8. Pembersihan riwayat transfer data serta perusakan jaringan.

Konotasi

1. Firewall melambangkan suatu tembok pelindung, dalam bidang komputer diartikan sebagai sistem keamanan.
2. Melambangkan informasi pribadi yang terdapat dalam sistem informasi manajemen dapat diakses melalui jaringan yang terkoneksi.
3. Mengilustrasikan email sebagai bentuk media komunikasi digital yang terkoneksi dengan internet.
4. Data perusahaan yang bersifat krusial hanya dapat diakses oleh pihak yang berwenang.
5. Jack mempunyai akses masuk dengan mudah sebab *previllege* yang dimilikinya.
6. Ilustrasi ruang pangkalan data yang ditampilkan dalam keadaan sepi, sehingga memungkinkan terjadinya pencurian data dan informasi meskipun akses menuju ruangan tersebut dilengkapi dengan CCTV.
7. Kunci akses merupakan bagian dari sistem keamanan jaringan.
8. Mengilustrasikan bahwa tindakan kejahatan yang dilakukan sudah direncanakan secara matang sehingga tidak meninggalkan jejak kejahatan.

Mitos

Sebagai bagian dari bisnis, informasi merupakan asset berharga bagi perusahaan. Maka dari itu, setiap perusahaan hendaknya memiliki sistem keamanan yang dapat melindungi data dan informasi di dalamnya. Seperti penggunaan

firewall yang berfungsi sebagai usaha preventif bagi perusahaan untuk menjaga, memantau lalu lintas data dari serangan luar. Dalam perusahaan besar, tentunya memiliki sistem informasi manajemen yang berisi informasi terkait data pribadi pekerja sekaligus data perusahaan. Setiap komputer yang digunakan dalam perusahaan akan terhubung dalam sebuah jaringan. Email menjadi salah satu media yang digunakan oleh pelaku kejahatan untuk memperoleh informasi pribadi sasaran, selain itu pelaku kejahatan (*hacker*) mengirimkan data sebagai umpan kepada sasaran melalui email.

- Scene tentang transfer data dan informasi

Gambar 2. Scene tentang transfer data dan informasi

Denotasi

1. Vel memberikan bolpoin dan microphone kecil yang disematkan pada pakaian Jack.
2. Vel dapat memantau panggilan telepon Jack.
3. Jack merakit alat-alat yang dapat digunakan untuk memindahkan file secara terselubung (tanpa meninggalkan jejak)
4. Tampilan layar komputer yang menunjukkan data rekening nasabah.
5. Tampilan layar laptop yang menunjukkan proses penyusunan sejumlah uang yang akan ditransfer.
6. Tampilan layar laptop yang menunjukkan penyalinan data ke CD.
7. Penggunaan komputer tabung yang menampilkan data-data nasabah serta telepon genggam Bobby dalam genggaman Jack.

Konotasi

1. Pada bolpoin yang tersemat di pakaian Jack, terdapat kamera sehingga pemantau dapat melihat dimana arah Jack menghadap.
2. Microphone yang disematkan memiliki fungsi selayaknya panggilan telepon dalam keadaan on.
3. Seorang ahli keamanan jaringan tidak hanya menggeluti perangkat lunak, melainkan juga ahli dalam perakitan perangkat keras.
4. Tampilan background berwarna hitam dan tulisan berwarna terang identik dengan sistem *programing.*
5. Tampilan layar laptop menunjukkan sistem operasi windows tahun 2000’an.
6. CD memiliki fungsi sebagai alat penyimpanan eksternal.
7. Kecepatan transfer data yang ditampilkan dalam komputer tabung cukup cepat, hal tersebut diilustrasikan dengan adegan yang dilakukan pada ruang kerja Bobby tidak berlangsung lama.

Mitos

Kecanggihan teknologi menghasilkan

berbagai macam produk elektronik dengan fungsi masing-masing. Begitu pula dengan alat sadap yang dikemas seefisien mungkin serta memiliki kecanggihan tinggi sehingga keberadaannya tidak diketahui. Alat sadap berfungsi untuk memonitor sasaran dari jarak yang cukup dekat. Selain itu, produk teknologi informasi menghasilkan komputer dalam berbagai macam bentuk dengan fungsi yang sama, namun memiliki kelebihan serta kekurangan masing-masing.

- Scene latar tempat tindakan kejahatan dunia maya

Gambar 3. Scene latar tempat tindakan kejahatan dunia maya

Denotasi

Latar tempat yang dilakukan dalam melakukan aksi kejahatan dunia maya yaitu ruang kerja tokoh Jack, ruang pangkalan data, toilet, dan rumah tinggal keluarga Stanfield.

Konotasi

1. Ruang kerja Jack terkesan terbuka dengan kaca transparan sebagai penyekat. Ruang kerja tersebut menggambarkan kesan ramah serta dapat memantau/dipantau oleh karyawan lainnya. Pada sisi lainnya menghadap ke arah luar gedung sehingga terlihat gedung-gedung tinggi lainnya yang memberikan kesan hiburan ketika lelah bekerja.
2. Rumah tinggal Stanfield terkesan terbuka serta aestetik dengan banyak hiasan bunga hal tersebut memberikan kesan hangat dengan bunga yang melambangkan kasih sayang.
3. Ruang pangkalan data berisikan komputer-komputer server. Ruangan tersebut terlihat sepi yang menandakan bahwa tidak semua orang dapat masuk ke dalam tempat tersebut.
4. Toilet yang dominan dengan cat berwarna cokelat dapat menciptakan kesan sebagai tempat yang aman dari tekanan luar.

Mitos

Tempat-tempat tersebut dianggap sebagai tempat yang aman untuk melakukan aksi kejahatan. Namun meski demikian, tempat-tempat tersebut juga memiliki potensi untuk mengumpulkan bukti-bukti kejahatan karena pada dasarnya semua tempat di perusahaan tidak lepas dari pengawasan.

- Scene tentang hubungan sosial

Gambar 4. Scene tentang hubungan sosial

Denotasi

1. Suasana pagi di rumah tinggal Stanfield sungguh riuh dengan perdebatan kecil Sarah dan Andy. Beth merapikan pakaian Jack yang akan berangkat bekerja. Jack menyempatkan diri untuk memperbaiki mainan Andy kemudian berpamitan kepada Sarah dan Beth.
2. Tokoh Jack mengikuti rapat perusahaan dan meninggalkan ruangan sebelum rapat diselesaikan.
3. Harry dan Jack mengadakan pertemuan dengan Cox di sebuah restoran pada malam hari.

Konotasi

1. Pada rumah tinggal Stanfield, antara ruang tamu dan dapur tidak memiliki sekat sehingga memudahkan untuk berinteraksi ketika sedang melakukan aktivitas di masing-masing ruang. Hal tersebut melambangkan kesan hangat dan kekeluargaan. Selain itu pakaian berwarna biru yang dikenakan oleh Jack mengilustrasikan tokoh memiliki kepribadian melankolis.
2. Tokoh Jack mempunyai kuasa dan kedudukan penting dalam perusahaan tersebut, hal ini diilustrasikan pada pakaian berwarna biru yang dikenakan tokoh Jack yang memeberikan kesan professional dan melambangkan simbol kekuatan.
3. Pembicaraan kerjasama tidak hanya dilakukan di kantor maupun tempat privat lainnya, tetapi juga dapat dilakukan di ruang publik.

Mitos

Keluarga merupakan sebuah unit terkecil dalam masyarakat. Bagi setiap orang, keluarga merupakan sumber kebahagiaan yang harus dijaga hubungannya. Bagi pelaku kejahatan (*hacker*), Jack berpotensi untuk menjadi sasaran empuk dengan posisinya sebagai Kepala Keamanan Jaringan. Sehingga dengan memanfaatkan tipe kepribadian tokoh yang melankolis, akan mudah untuk memanipulasi psikologis sasaran.

- Scene tentang ancaman

Gambar 5. Scene tentang ancaman

Denotasi

1. Tokoh Jack mendapat tagihan hutang judi daring, ia meminta untuk memeriksa bukti-bukti.
2. Penyekapan keluarga Stanfield oleh kawanan penjahat di rumah tinggal Stanfield.
3. Cox mengetahui bahwa Andy memiliki alergi terhadap kacang.
4. Cox menekan Jack dengan sikapnya yang dingin namun mematikan.
5. Cox terlihat kesal sedangkan Jack dan Beth menunjukkan kekhawatiran.
6. Cox menatap Jack sebagai lawan bicaranya dengan tatapan tajam dan angkuh. Pada teks, Jack memohon

kepada Cox dan ia bersedia melakukan apapun yang diminta.

Konotasi

1. Penyangkalan yang dilakukan oleh Jack menunjukkan bahwa ia sangat yakin tidak melakukan apa yang dituduhkan.
2. Jack terlihat sangat menyayangi keluarganya dan menjadi pelindung bagi keluarganya.
3. Sarung tangan hitam yang dikenakan oleh Cox menunjukkan bahwa ia tidak ingin meninggalkan sidik jari pada barang-barang di rumah tinggal Stanfield.
4. Mengancam Jack dengan jarak yang cukup dekat menunjukkan kesan bahwa Cox ingin menampilkan pribadi/rekan kerja yang dekat dengan Jack mengingat ruang kerja Jack terkesan terbuka sehingga orang lain kemungkinan dapat melihat aktivitas yang dilakukan dalam ruang kerja Jack.
5. Ekspresi kesal Cox menunjukkan bahwa ia tidak main-main dengan ancamannya.
6. Jack berusaha untuk menyelamatkan keluarga meskipun ia harus menanggung resikonya.

Mitos

Penggunaan bukti seperti identitas diri serta surat-surat dapat meyakinkan orang lain. Penekanan ancaman melalui jalur hukum merupakan manipulasi psikologi dengan tujuan untuk menciptakan ketakutan serta kekhawatiran. Menciptakan kebingungan merupakan salah satu teknik yang digunakan oleh pelaku kejahatan untuk mengumpan sasaran. Teknik lain yang digunakan yaitu dengan mencari kelemahan sasaran. Ancaman menggunakan kelemahan sasaran yang berupa karakter *family man,* berimbas pada penyanderaan anggota keluarga. Sehingga pelaku kejahatan memanfaatkan hubungan kekeluargaan sebagai celah untuk mencapai tujuan yang diinginkan.

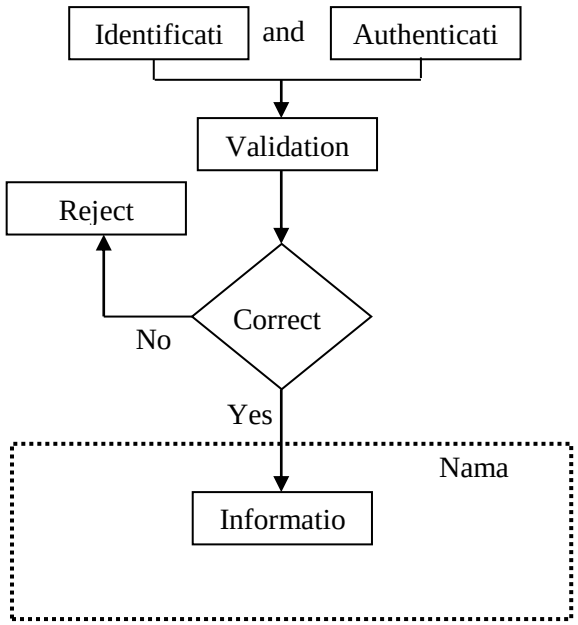
Representasi *Social Engineering* Dalam Tindak Kejahatan Dunia Maya

Pada scene-scene di atas merupakan analisis teks untuk mengetahui tindakan *social engineering* pada film Firewall. Selanjutnya akan dilakukan analisis konteks dengan cara menghubungkan makna yang tersirat di level teks dengan teori yang berkaitan. Representasi dalam media diartikan sebagai penunjukan seseorang, kelompok, gagasan atau pendapat tertentu ditampilkan dalam pemberitaan. Dari pendekatan terhadap representasi menurut Hall (1997), penelitian ini menggunakan pendekatan konstruksionis yang menaruh perhatian pada bagaimana representasi dibuat melalui bahasa, termasuk kode-kode visual.

Film Firewall implementasi kasus kejahatan dunia maya yang menggunakan teknik *social engineering* untuk mencapai tujuan yang diinginkan. Firewall memberikan edukasi kepada pemirsanya yang menganggkat studi kasus diimplementasikan oleh Sutradara dalam bentuk film. Dalam film tersebut, otak pelaku kejahatan yang melakukan *social engineering* tidak memiliki keahlian dalam

bidang *hacking*. Perilaku *social engineering* tidak hanya dilakukan oleh seorang *hacker*.

Menurut Rafizan (2011), berikut gambaran sederhana penerapan sistem keamanan dalam perusahaan.



Gambar 6. Gambaran sederhana sistem

Pada gambar tersebut menjelaskan bahwa untuk mengakses sebuah informasi perusahaan yang dilindungi sistem keamanan tahap pertama yang dilakukan yaitu validasi. Validasi dibutuhkan untuk mengidentifikasi data diri orang yang mengakses informasi tersebut, validasi biasanya dilakukan dengan menginputkan *username*. Pada kasus dalam film Firewall, validasi dilakukan dengan cara menempelkan kartu akses/identitas pada alat sejenis *fingerprint.* Selain berfungsi sebagai validasi, kartu akses tersebut juga berfungsi sebagai otetentifikasi (biasanya berupa *password*). Sehingga dengan adanya sistem keamanan tersebut, sistem akan memiliki *security log* sebagai bukti akses. Seorang *hacker* akan berusaha untuk mendapatkan *username* dan *password* agar dapat memiliki hak akses ke dalam sebuah server. *Hacker* atau pelaku kejahatan dunia maya memiliki teknik-teknik untuk melewati sistem keamanan agar memperoleh informasi penting salah satunya yaitu dengan teknik *social engineering.*

Representasi *social engineering* pada film Firewall apabila dikaitkan dengan pola umum bagaimana pelaku melakukan tindakan tersebut menurut Gartner (dalam Rafizan, 2011) tahap pertama yang dilakukan yaitu pengumpulan informasi, dilakukan dengan cara meretas akun pribadi sasaran yang tercatat dalam sistem informasi manajemen perusahaan selain itu pelaku juga melakukan peretasan terhadap email sasaran. Tahap kedua yaitu mengembangkan relasi, hal tersebut dilakukan pelaku dengan cara melakukan penyamaran menjadi ‘orang penting’ (pebisnis/investor) yang mendekati rekan sasaran untuk mendapat informasi tambahan sekaligus sebagai penghubung langsung dengan sasaran. Namun sayangnya, pada tahap ini pelaku tidak dapat meyakinkan sasaran sehingga pelaku melakukan rencana lainnya untuk mendapatkan sasaran. Pada tahap ketiga yaitu mengeksploitasi, artinya pelaku berusaha mendapatkan informasi-informasi penting yang diinginkan dari sasaran. Pada tahap ini pelaku melakukan cara paksa untuk menundukkan sasaran dengan cara memanfaatkan kelemahan sasaran sebagai

senjatanya. Tahap akhir yaitu eksekusi, pada tahap ini pelaku mencapai apa yang diinginkan yaitu menjadikan sasaran sebagai kunci akses.

Representasi *social engineering* pada film Firewall jika dikaitkan dengan teknik *social engineering* milik Dhull & Hooda (2016), maka tindakan *social engineering* yang sangat tercermin menggunakan teknik *reverse social engineering* yang berbasis interaksi sosial. Melihat kedudukan sasaran dalam perusahaan, memanipulasi sasaran dengan menawarkan keuntungan akan lebih mudah dilakukan untuk meyakinkan serta membangun kepercayaan sebagai relasi yang dapat diandalkan. Selain itu, mengingat keluarga merupakan kelemahan yang diilustrasikan dalam film, maka dengan cara memberi keuntungan untuk membebaskan keluarganya dari penyanderaan membuat sasaran masuk ke dalam perangkap kejahatan.

E. KESIMPULAN

Setelah menyaksikan film tersebut, pemirsa dapat menyadari bahwa adanya teknologi juga membawa dampak buruk bagi kehidupan. Bagi perusahaan, dengan menyaksikan film tersebut dapat menjadi evaluasi terhadap sistem keamaan serta pentingnya menjaga informasi secara ketat. Makna yang terungkap melalui makna denotasi, konotasi, dan mitos pada film Firewall dalam teks mengunakan analisis semiotika Roland Barthes adalah *Hacker* tidak hanya melakukan penyerangan luar seperti melakukan penyebaran virus dan sejenisnya melainkan menggunakan teknik lain yang lebih ‘elegan’ dengan menyerang melalui jalur dalam (internal). Penyerang internal terkesan massif dan terstruktur, sehingga tidak terdeteksi oleh sistem keamanan (berbasis interaksi sosial).

Tercermin lima dari sepuluh representasi tindak kejahatan yang dilakukan dalam film Firewall. Tindakan tersebut memberikan kerugian bagi pelaku, korban, serta perusahaan terlihat pada akhir film yang menggambarkan peristiwa pembunuhan. Selain itu, tindakan *social engineering* dalam kasus film Firewall tidak dilakukan secara langsung oleh *hacker.* Pada film tersebut, peran *hacker* sebagai peran pendukung pelaku utama kejahatan yang membantu menangani peretasan, penyadapan, pengintaian, dan perusakan jaringan perusahaan.

DAFTAR PUSTAKA

Anggoro, A. R. (2016, Oktober 12). *Konsep-Konsep Dasar Semiotika Struktural Pada Momen Ilmiah Roland Barthes.* Retrieved Mei 03, 2020, from Repository ISI: http://repository.isi-ska.ac.id/32778/1/Albertus%20Rusputranto%20Ponco%20Anggoro%2C%20S.Sn.%2C%20M.Hum._Penelitian.pdf

Besar. (2016). *Kejahatan Dengan Menggunakan Sarana Teknologi Informasi*. Retrieved April 30, 2020, from Business Law Binus University: https://business-law.binus.ac.id/2016/07/31/kejahatan-dengan-menggunakan-sarana-teknologi-informasi/

CNN Indonesia. (2020, Februari 06). *Pembobolan Rekening Ilham Bintang, Data Dijual Orang Bank*. Retrieved Mei 06, 2020, from CNN Indonesia: https://m.cnnindonesia.com/nasional/20200205211241-12-472073/pembobolan-rekening-ilham-bintang-data-dijual-orang-bank

Dhull, R., & Hooda, S. S. (2016). Contrast Study of Social Engineering Techniques. *IOSR Journal of Computer Engineering, Volume 18*(Issue 4), 66-68.

Djanggih, H., & Qamar, N. (2018, June). Penerapan Teori-Teori Kriminologi Dalam Penanggulan Kejahatan Siber (Cyber Crime). *Pandecta, Volume 13*(Number 1), 10-23.

Fasah, A. P., & Laksmi. (2018). Representasi Profesionalisme Pustakawan Dalam Mengelola Perpustakaan Pada Film Pendek Project: Library. *Lentera Pustaka, Vol. 4*(No. 1), 1-6.

Forte, J. (Writer), & Loncraine, R. (Director). (2006). *Firewall* [Motion Picture].

Hadnagy, C. (2011). *Social Engineering: The Art of Human Hacking.* Indianapolis: Wiley Publishing, Inc.

Kelrey, A. R., & Muzaki, A. (2019, November). Pengaruh Ethical Hacking Bagi Keamanan Data Perusahaan. *CyberSecurity dan Forensik Digital, Vol. 2*(No. 2), 77-81.

Putra, A. M. (2015, Oktober 30). *Pengenalan Teknologi Informasi.* Retrieved Mei 06, 2020, from Sisfo ITP: https://sisfo.itp.ac.id/bahanajar/index.php?dir=Andi%20M%20Nur%20Putra/Pengantar%20Teknologi%20Informasi/&file=BAB%20I%20Pengenalan%20Teknologi%20Informasi.pdf

Rafizan, O. (2011). Analisis Penyerangan Social Engineering. *Masyarakat Telematika Dan Informasi : Jurnal Penelitian Teknologi Informasi dan Komunikasi, Vol. 2*(No. 2), 115-126.

Ramadhan, M. H. (2017, Agustus 11). *Representasi Visi dan Misi UIN Sunan Ampel Surabaya dalam Lirik Lagu Mars dan Himne : Analisis Semiotika Model Ferdinand de Saussure.* Retrieved Mei 06, 2020,

from Digital Library UIN Sunan Ampel: http://digilib.uinsby.ac.id/19237/

Zulkarnaen, M. J. (2015, April 06). *Efektivitas Penggunaan Teknologi Informasi dan Komunikasi Dalam Meningkatkan Prestasi Belajar Pendidikan Agama Islam Siswa Kelas X Teknik Komputer dan Informatika di SMK Negeri 3 Bojonegoro.* Retrieved Mei 03, 2020, from Digital Library UIN Sunan Ampel: http://digilib.uinsby.ac.id/1534/