Forensik Komputer Studi Kasus: Universitas Klabat

Jimmy Moedjahedy
Jurusan Teknik Informatika, Universitas Klabat
e-mail: **jimmy@unklab.ac.id**

Abstrak

Forensik komputer adalah proses memeriksa media komputer seperti hard disk, disket, kaset, menggunakan metode-metode tertentu, dengan kata lain forensik komputer adalah proses mengumpulkan, menjaga, menganalisa dan penyajian bukti yang berkaitan dengan komputer. Jaringan komputer Universitas Klabat tidak luput dari serangan di jaringan, tujuan dari penelitian ini adalah untuk mengetahui seberapa sering sistem dan jaringan kampus diserang dengan melihat log di server, firewall, serta membuat penanganan dan juga deteksi secara dini tentang serangan ke jaringan. Hasil dari penelitian ini adalah ada beberapa pihak yang mencoba untuk mengakses server lewat autentikasi SSH yang ip publiknya berasal dari cina merupakan ip terbanyak, firewall juga diserang sebanyak 1840 kali, sehingga penulis mengimplentasi intrusion detection system dan intrusion prevention system diserver kampus untuk menangani dan mengumpulkan data yang lebih tentang serangan.
Kata kunci—forensik komputer, forensik jaringan, Universitas Klabat

Abstract

Computer forensics is the process of checking computer media such as hard disks, floppy disks, tape, using certain methods, in other words, computer forensics is the process of collecting, maintaining, analyzing and presenting evidence related to computers. Universitas Klabat computer network is not spared from the attack on the network, the aim of this study is to determine how often the system and campus networks are attacked by viewing the log in server, firewall, and make the handling as well as early detection of attacks to the network. The result of this research that there are those who tried to access the server using SSH and the most IP public were originated from China, the firewall also was attack 1840 times, so the author implemented intrusion detection systems and intrusion prevention systems in campus server to prevent and collect more data about the attack.

Keywords—*attendance system, scientific conference, web, barcode, spiral*

1. PENDAHULUAN

Perkembangan teknologi dan pertukaran dari media komunikasi dan informasi telah menciptakan suatu bentuk kejahatan baru yaitu kejahatan *cyber* dan kejahatan didunia komputer. Kejahatan didunia komputer secara tidak langsung memaksa para penegak hukum untuk membentuk suatu tim yang memiliki bidang keahlian khusus dalam menangani, mengumpulkan dan menganalisa barang bukti digital.[2]

Pada tahun 2004 di Indonesia, Dani Firman Syah atau yang lebih dikenal di dunia maya dengan nickname xnuxer berhasil membobol website KPU dan mengganti lambang-lambang partai. Proses penangkapan dimulai oleh polisi bersama tim asistensi dengan langkah pertama yaitu melihat log dari server yang ada di KPU, polisi menemukan nickname dani dan alamatnya yaitu Yogjakarta. Setelah itu polisi menyelidiki nicknamenya menggunakan *Internet Relay Chat* (IRC) , nicknamenya muncul disalah satu *Internet Protocol* (IP) warnet yang ada di Yogjakarta, polisi mencari warnet tersebut dan melihat log file kemudian menghubungi internet service provider. Salah satu IP public yang dipakai untuk masuk ke situs KPU adalah dari PT. Danareksa akhirnya polisi menyimpulkan bahwa pelakunya adalah Dani Firman dan bekerja di PT. Danareksa. Metode yang dipakai oleh polisi untuk menangkap Dani adalah forensik komputer. [3]

Forensik komputer adalah proses memeriksa media komputer seperti hard disk, disket, kaset, menggunakan metode-metode tertentu, dengan kata lain forensik komputer adalah proses mengumpulkan, menjaga, menganalisa dan penyajian bukti yang berkaitan dengan komputer. [1]

Forensik komputer merupakan proses memperoleh dan menganalisis informasi digital untuk digunakan sebagai bukti dalam kasus perdata, pidana, atau administrative.[2]

Komputer forensik sering juga disebut sebagai forensik digital, forensik teknologi informasi, atau data forensik yang merupakan proses investigasi di mana peneliti mengidentifikasi, menjaga, menganalisis bukti digital yang terdiri dari berbagai jenis. Bukti digital adalah data yang disimpan atau dikirimkan menggunakan komputer yang mendukung atau menyangkal teori bagaimana suatu pelanggaran terjadi. [4]

Seni forensik berasal dari dunia medis yaitu praktek kedokteran forensik yang sudah diakui sebagai spesialisasi medis pada akhir abad ke 18. Aktivitas forensic yang paling umum adalah otopsi atau pemeriksaan postmortem. Dari dasar itu ditemukan pula sidik jari yang digunakan dan diakui oleh semua pengadilan diseluruh dunia sebagai identitas diri yang sah. [5]

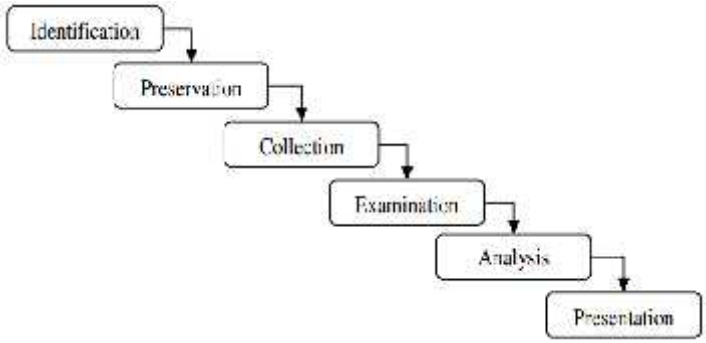
Universitas Klabat(UNKLAB) merupakan salah satu universitas swasta yang ada di Sulawesi Utara dibawah wilayah Kopertis IX yang berdiri pada tahun 1965. Sejak tahun 2002 UNKLAB telah memiliki dan menggunakan sistem informasi akademis untuk keperluan akademik baik mahasiswa maupun dilingkungan dosen dan juga keperluan administrasi. Selain Sistem Informasi Akademik, UNKLAB juga memiliki website sebagai sarana mendapatkan informasi tentang kampus mulai dari pendaftaran, kurikulum, biaya kuliah dan informasi lainnya yang berhubungan dengan akademik.

Dengan adanya sistem informasi dan website yang sudah online sejak tahun 2002 maka UNKLAB tidak luput dari serangan kejahatan internet, tujuan dari penelitian ini adalah untuk mengetahui seberapa sering serangan terjadi dan dan membuat penanganan serta deteksi secara dini jika ada serangan terhadap jaringan, sistem maupun website kampus.

2. METODE PENELITIAN

Model forensik yang digunakan dalam penelitian ini adalah *Digital Forensics Research Workshop (DFRWS)* Model.

Pada tahun 2001, Workshop DFRWS yang pertama mengusulkan proses investigasi forensik komputer yang terdiri dari 6 fase[8]



Gambar 1. DFRWS Model[8]

1. Fase Identifikasi (*Identification*)

Pada fase ini deteksi profil, sistem pemantauan, analisis audit, dilakukan. Dalam penelitian ini pada fase identifikasi dilakukan sistem pemantauan dengan mengaktifkan *log system, log authentication* dan *log firewall*.

2. Fase penjagaan (*Preservation*)

Fase ini melibatkan tugas-tugas seperti menyiapkan manajemen kasus yang tepat. Fase ini sangat penting untuk memastikan bahwa data yang dikumpulkan bebas dari kontaminasi. Pada fase ini dipastikan bahwa data yang diambil dari server farm UNKLAB dan tidak dimodifikasi oleh siapa pun agar supaya data yang diambil memang benar.

3. Fase Pengumpulan (*Collection*)

Pada fase ini data yang relevan sedang dikumpulkan berdasarkan metode yang disetujui dengan memanfaatkan berbagai teknik pemulihan. Dalam penelitian yang dilakukan, fase ini merupakan proses pengumpulan file-file berupa log dari server farm UNKLAB serta analisa sistem firewall.

4, 5. Fase pemeriksaan dan fase analisis (*examination and analysis*)

Dalam kedua fase ini , tugas-tugas seperti bukti tracing, validasi bukti, pemulihan data yang disembunyikan / dienkripsi,data mining, waktu,dilakukan. Proses analisis dan pemeriksaan dimulai difase

ini, dimana penulis akan membuat parsing dari log yang diambil serta menganalisis serangan yang terjadi, kapan diserang, IP dari mana yang menyerang.

6 . Fase dokumentasi (*Presentation*)

Fase ini merupakan fase akhir dan forensik komputer dimana hasil analisis sudah didapat dan penulis akan membuat kesimpulan dari hasil analisis dan memberi saran apa yang harus dilakukan untuk mengatasi serangan dan deteksi awal serangan.

2.1 Konsentrasi forensik komputer

Menurut Ramadhan [9], Semakin kompleksnya tindak kejahatan dalam bidang komputer membuat bidang ilmu komputer forensik melebarkan kajian ilmu forensik dari berbagai aspek. Maka dari itu perlu adanya pembagian konsentrasi ilmu dalam bidang komputer forensik tersebut, ini ditujukankan agar dalam melakukan investigasi untuk mengungkap kejahatan bahkan memulihkan sistem pasca kerusakan dapat dengan mudah dilakukan, karena sudah dibagi kedalam beberapa konsentrasi yakni :

1. Forensik Disk
2. Forensik Sistem
3. Forensik Jaringan
4. Forensik Internet

Forensik Disk, untuk konsentrasi ilmu yang satu ini sudah mulai berkembang, dimana forensik disk melibatkan berbagai media penyimpanan. Ilmu forensik yang satu ini sudah terdokumentasi dengan baik diberbagai literatur, bahkan profesional IT pun bisa menangani permasalahan forensik disk ini. Misalkan, mendapatkan file-file yang sudah terhapus, mengubah partisi harddisk, mencari jejak *bad sector*, memulihkan *registry windows* yang termodifikasi atau tersembunyi oleh virus dan lain sebagainya. Akan tetapi masih banyak professional IT yang belum mengetahui bahwasanya perilaku tersebut merupakan salah satu tindakan komputer forensik.

Forensik Sistem, metode ini tentunya dekat dengan sistem operasi, dan yang pastinya konsentrasi ilmu ini masih sulit untuk dikaji lebih dalam, ini dikarenakan banyaknya sistem operasi yang berkembang saat ini, dimana sistem operasi memiliki karakteristik dan perilaku yang berbeda, misalnya saja berbagai file sistem, maka dari itu metode forensik yang ada sekarang ini masih sulit untuk disama-ratakan. Kendalanya yakni software pendukung yang ada sekarang dimana sebagai *tool* untuk membedah sistem operasi masih ber-*platform windows*. Inilah yang menyebabkan masih perlunya pengembangan ilmu tersebut.

Forensik Jaringan, adalah suatu metode menangkap, menyimpan dan menganalisa data pengguna jaringan untuk menemukan sumber dari pelanggaran keamanan sistem atau masalah keamanan sistem informasi. Jika kita berbicara tentang bagian yang satu ini, pastinya ini melibatkan *OSI (Open System Interconnection) layer*, yang menjelaskan bagaimana komputer dapat berkomunikasi. Hal ini tidak hanya melibatkan suatu sistem jaringan LAN akan tetapi dapat mencakup ke dalam sebuah sistem jaringan yang lebih besar.

Forensik Internet, bidang ini lebih rumit lagi dari yang lainnya dikarenakan ada banyak komputer yang terhubung satu dengan yang lain dan penggunaannya dapat bersamaan tanpa memperhitungkan jarak sehingga dalam menelisik bagian ini membutuhkan teknik-teknik yang kompleks. Melalui forensik internet ini kita dapatmelacak siapa yang mengirim e-mail, kapan dikirim dan sedang berada di mana si pengirim, hal ini dapat dilakukan mengingat semakin banyaknya e-mail palsu yang meng-atasnamakan perusahaan tertentu dengan modus undian berhadiah yang akan merugikan si penerima e-mail, atau juga banyak e-mail yang bernada ancaman. Maka dari itu forensik internet menjadi suatu ilmu yang sangat menjanjikan dalam mengungkap fakta-fakta dan mengumpulkan bukti.

2.2 Tujuan dan metode forensik komputer

Tujuan dari forensik komputer adalah untuk memulihkan, menganalisa, dan menghadirkan segala sesuatu yang berhubungan dengan komputer yang bisa digunakan sebagai bukti dilembaga hukum dan pengadilan.[2]

Menurut [7] Pada dasarnya tidak ada suatu metodologi yang sama dalam pengambilan bukti pada data digital, karena setiap kasus adalah unik sehingga memerlukan penanganan yang berbeda. Walaupun demikian dalam memasuki wilayah hukum formal, tentu saja dibutuhkan suatu aturan formal yang dapat melegalkan suatu investigasi.

Untuk itu menurut *U.S. Department of Justice* ada tiga hal yang ditetapkan dalam memperoleh bukti digital:

1. Tindakan yang diambil untuk mengamankan dan mengumpulkan barang bukti digital tidak boleh mempengaruhi integritas data tersebut.
2. Seseorang yang melakukan pengujian terhadap data digital harus sudah terlatih.
3. Aktivitas yang berhubungan dengan pengambilan,pengujian, penyimpanan atau pentransferan barang bukti digital harus didokumentasikan dan dapat dilakukan pengujian ulang.

Selain itu terdapat pula beberapa panduan keprofesian yang diterima secara luas:

1. Pengujian forensik harus dilakukan secara menyeluruh. Pekerjaan menganalisa media dan melaporkan temuan tanpa adanya prasangka atau asumsi awal.
2. Integritas dari media asli harus dipelihara selama keseluruhan penyelidikan
3. Media yang digunakan pada pengujian forensic harus disterilisasi sebelum digunakan
4. Image bit dari media asli harus dibuat dan dipergunakan untuk analisa.

Dalam kaitan ini terdapat akronim PPAD pada Komputer forensik:

1. Memelihara (*Preserve*) data untuk menjamin data tidak berubah.
2. Melindungi (*Protect*) data untuk menjamin tidak ada yang mengakses barang bukti.
3. Melakukan analisis (*Analysis*) data menggunakan teknik forensik.
4. Mendokumentasikan (*Document*) semuanya, termasuk langkah-langkah yang dilakukan.

2.3 Tugas Forensik Komputer

Berikut adalah beberapa tugas pokok dari seorang ahli forensik[1]:

a. Penyitaan data
   Memeriksa dan menyalin dokumen atau data kompilasi yang mungkin mengandung bukti. Ahli forensik komputer yang harus melakukan ini dan menggunakan pengetahuan mereka tentang teknologi penympanan data untuk melacak bukti.

b. Duplikasi dan proteksi data
   Jika ada dua pihak yang saling memperebutkan data, maka ahli forensik harus menjaga data agar tidak dapat diubah dengan cara apapun, dan menduplikasi data tersebut serta tidak merugikan pihak yang mengajukan.
c. Pemulihan data
   Ahli forensik komputer harus dapat dengan aman memulihkan dan menganalisa bukti yang tidak dapat diakses lagi berdasarkan apa yang mereka pelajari secara mendalam mengenai teknologi penyimpanan dan media penyimpanan.
d. Pencarian dokumen
   Ahli forensic komputer harus dapat mencari lebih dari 20.000 dokumen elektrokronik dalam hitungan detik bukan dalam hitungan jam. Kecepatan dan efisiensi pencarian tersebut mengurangi proses pencarian yang rumit dan intrusif kepada semua pihak yang terlibat
e. Media Konversi
   Beberapa klien perlu mendapatkan dan menyelidiki data komputer yang tersimpan di perangkat lama dan tidak dapat dibaca. Ahli forensik komputer harus mengekstrak data yang relevan dari perangkat tersebut, mengubahnya menjadi format yang dapat dibaca, dan menempatkannya di media penyimpanan baru untuk analisis.
f. Saksi Ahli
   Ahli forensik komputer harus mampu menjelaskan proses teknis yang rumit sehingga mudah dipahami. Hal ini akan membantu hakim dan juri memahami bagaimana bukti komputer ditemukan, apa yang ada didalam barang bukti digital, dan bagaimana hal itu relevan dengan situasi.

2.4 Barang Bukti Digital

Bukti digital adalah informasi yang didapat dalam bentuk / format digital. Beberapa contoh bukti digital antara lain:

a. E-mail, alamat e-mail
b. File *wordprocessor/spreadsheet*
c. *Source code* perangkat lunak
d. File berbentuk image(.jpeg, .tip, dan sebagainya)

e. Web Browser bookmarks, cookies
f. Kalender, to-do list

Gambar 3. Barang bukti digital

Bukti digital tidak dapat langsung dijadikan barang bukti pada proses peradilan, karena menurut sifat alamiahnya bukti digital sangat tidak konsisten. Untuk menjamin bahwa bukti digital dapat dijadikan barang bukti dalam proses peradilan maka diperlukan sebuah standar data digital yang dapat dijadikan barang bukti dan metode standar dalam pemrosesan barang bukti sehingga bukti digital dapat dijamin keasliannya dan dapat dipertanggung jawabkan.
Berikut ini adalah aturan standar agar bukti dapat diterima dalam proses peradilan:

1. Dapat diterima, artinya data harus mampu diterima dan digunakan demi hukum, mulai dari kepentingan penyelidikan sampai dengan kepentingan pengadilan.
2. Asli, artinya bukti tersebut harus berhubungandengan kejadian / kasus yang terjadi dan bukan rekayasa.
   Lengkap, artinya bukti bisa dikatakan bagus dan lengkap jika di dalamnya terdapat banyak petunjukyang dapat membantu investigasi.
3. Dapat dipercaya, artinya bukti dapat mengatakan hal yang terjadi di belakangnya. Jika bukti tersebut dapat dipercaya, maka vproses investigasi akan lebih mudah.[6]

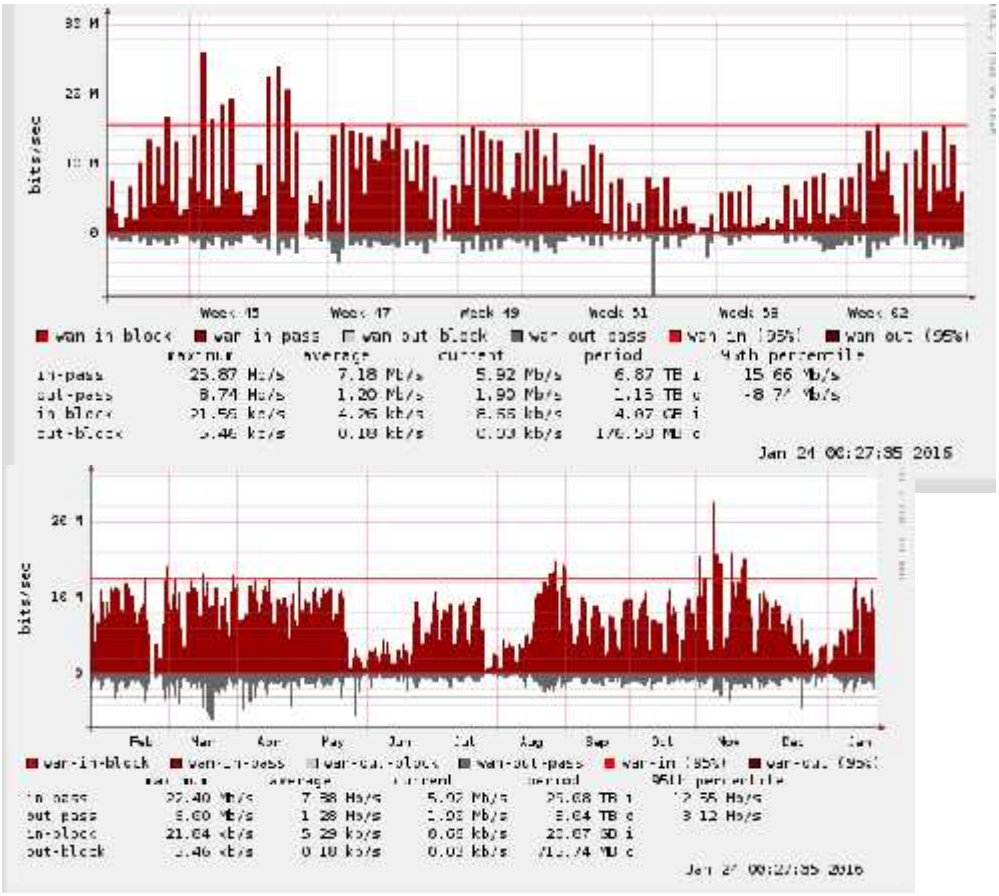
Digital evidence tersebar dalam berbagai media dan konteksnya, untuk itu diperlukan kejelian yang lebih daripada sekedar mengklasifikasikan data untuk tujuan forensik. Perlu diingat pula, semakin banyak *peripheral* atau *device* yang diintegrasikan dalam sistem komputer, tentu akan semakin kompleks dan melibatkan banyak pertimbangan untuk mengangkat digital evidence. Itu merupaka salah satu kendala dalam pengaksesan file-file yang akan dijadikan bukti-bukti.[9]
Berikut adalah kendala lain yang mungkin terjadi di lapangan pada saat investigasi untuk mengambil data :

1. File terkompresi
2. Salah menamakan file secara disengaja atau tidak
3. Salah dalam memberikan file format, secara disengaja atau tidak
4. File yang diproteksi password
5. Hidden Files
6. File terenkripsi
7. Steganography

3. HASIL DAN PEMBAHASAN

Metode forensik yang dicoba di Universitas Klabat adalah forensik jaringan dimana akan dikumpulkan dan dianalisa data-data dari *server farm* yang ada di Network Operation Center (NOC) dari universitas.

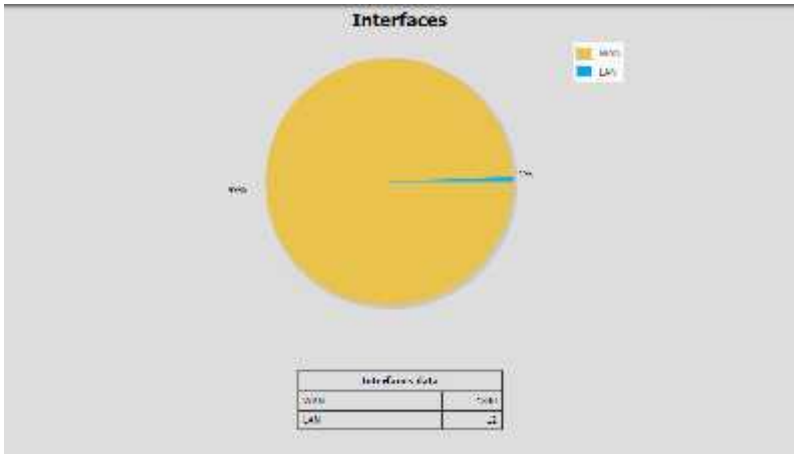
Berdasarkan data yang diambil, *traffic* jaringan di UNKLAB bisa dikatakan padat, karena besaran *bandwidth* yang disewa hanya 15 Mbps dan kalau dilihat dari grafik dibawah yaitu rata-rata traffic selama 3 bulan dan 1 tahun memiliki rata-rata kurang lebih 15 Mbps yang artinya pemakaian sudah pada puncaknya. Dari *traffic* ini bisa saja ada aktivitas serangan yang oleh penulis akan dianalisa dari file log yang ada.

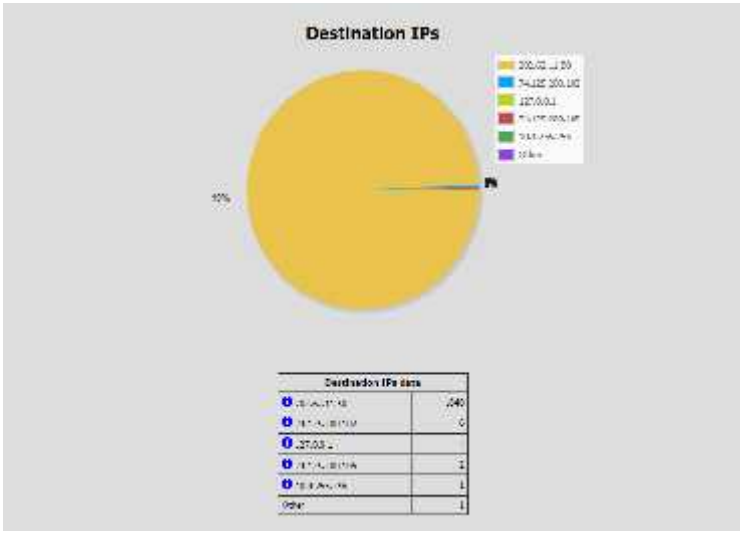


Gambar 4. Rata-rata traffic jaringan 3 bulan dan 1 tahun

3.1 Analisa hasil firewall

Berikut adalah *screen shot* yang diambil dari *firewall* yang telah diaktifkan dan diinstall oleh penulis di sistem operasi PFSENSE. Dari gambar dapat dilihat bahwa *interface* yang diserang kebanyakan adalah *interface* yang memiliki IP publik yaitu WAN dan penyerang berasal dari luar sebanyak 1840, dan *interace* LAN diserang oleh orang dalam sebanyak 12.

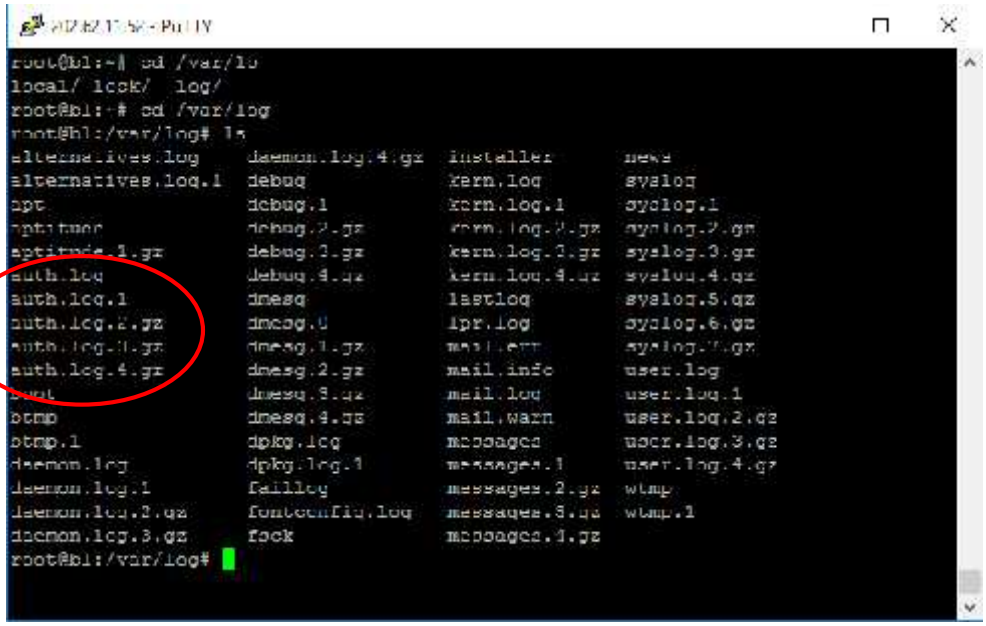




Gambar 4. IP yang diserang

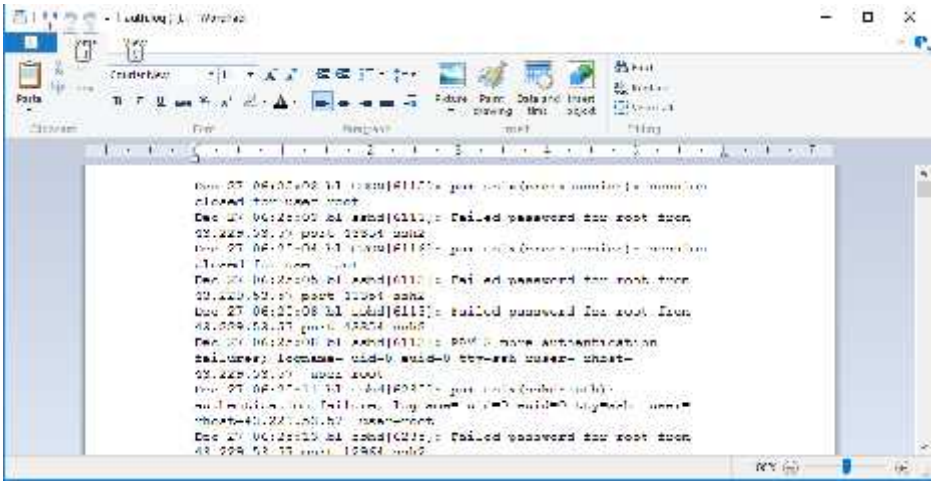
3.2Analisa Log Authentication

Yang dianalisa berikut adalah file *log authenticaton* seperti pada gambar dibawah ini:



Gambar 5. Letak file log authentication

Ketika kita membuka file *auth.log*, outputnya sulit untuk dianalisa dan ditabulasi satu persatu karena banyaknya keterangan, untuk itu agar supaya memudahkan proses tabulasi dan analisa digunakan metode *parsing*. *Parsing* log file yang digunakan bukan *script python*, tetapi menggunakan metode *command grep*.



Gambar 6. Isi file auth.log

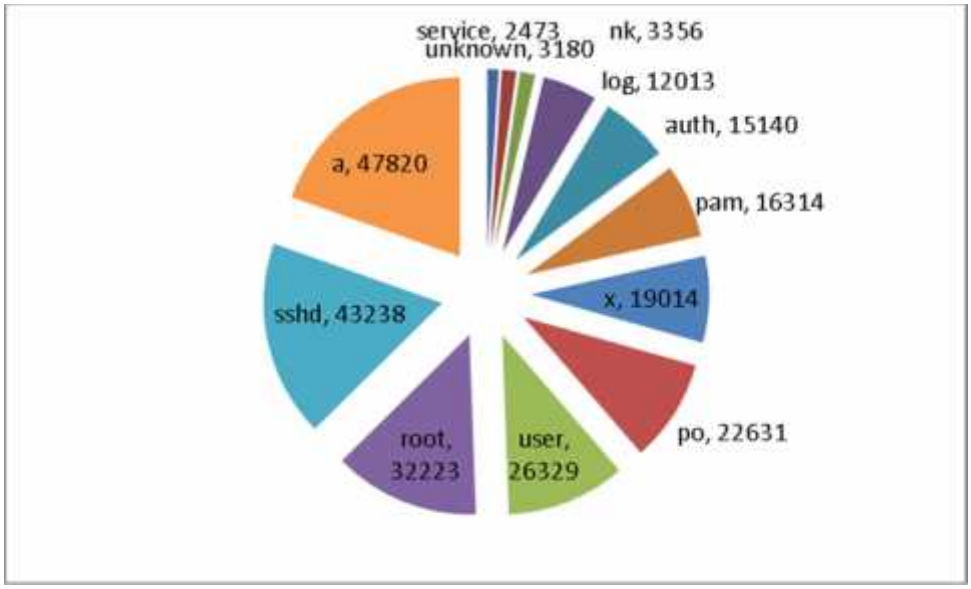
Untuk mengetahui user-user mana yang coba untuk mengakses sistem dengan cara memanfaatkan *service SSH* yang diaktifkan maka *command parsing* untuk memunculkannya adalah dengan menggunakan *command* ini:

```
grep -i "Failed password for invalid user" /var/log/auth.log |
  cut -d " " -f 11 |
  sort |
  uniq |
  while read name
  do
    grep "$name" /var/log/auth.log | wc -l | tr -d "\n"
    echo " $name"
  done | sort -n
```

Hasil dari *parsing log file auth.log* menunjukkan bahwa ada 403 user yang dicoba untuk masuk kedalam sistem melalui service SSH. Hasil yang ditunjukkan hanya diambil 12 nama user yang dicoba dengan jumlah percobaan ribuan kali.

Username	Jumlah Coba
service	2473
unknown	3180
nk	3356
log	12013
auth	15140
pam	16314
x	19014
po	22631
user	26329
root	32223
sshd	43238
a	47820

Tabel 1. Daftar 12 username yang dicoba oleh penyerang



Gambar 7. Chart jumlah username yang dicoba penyerang

Untuk melihat IP asal penyerang, *parsing command* yang digunakan adalah:

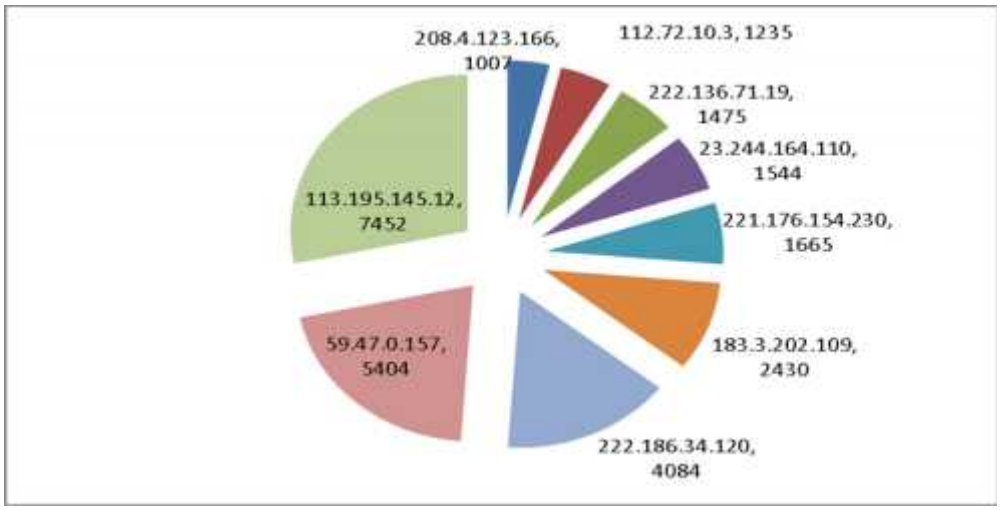
```
tmpfile=/tmp/breakinattempts.txt
zgrep -i "Failed password for root from" /var/log/auth.log* >$tmpfile
cat $tmpfile |
  cut -d " " -f 11 |
  sort |
  uniq |
  while read name
do
    cat $tmpfile |
      grep "$name" |
      wc -l |
      tr -d "\n"
  echo " $name"
done | sort -n
rm $tmpfile
```

Dari hasil *command parsing* untuk mengetahui IP asal penyerang ada 70 IP publik yang didapat dan hanya akan diambil 9 IP publik dengan percobaan ribuan kali.

Tabel 2. Asal IP Publik penyerang

IP Publik	**Jumlah Serangan**	**Negara Asal**
183.3.202.107	755	China
208.4.123.166	1007	Kansas, America
112.72.10.3	1235	Mongolia
222.136.71.19	1475	China
23.244.164.110	1544	California, America
221.176.154.230	1665	China

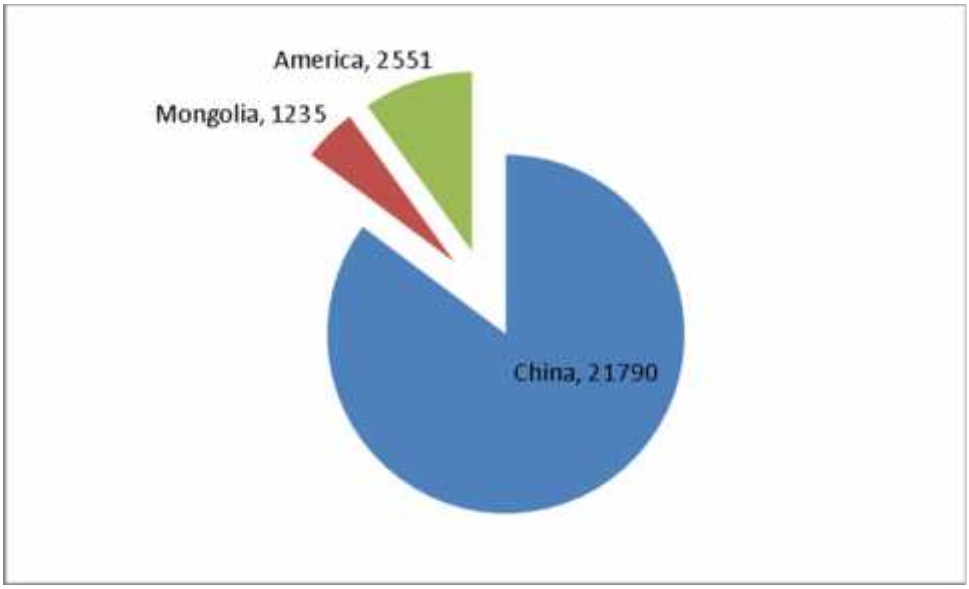
183.3.202.109	2430	China
222.186.34.120	4084	China
59.47.0.157	5404	China
113.195.145.12	7452	China



Gambar 8. Chart IP Publik dan jumlan serangan

Negara Asal	**Jumlah Percobaan**
China	21790
Mongolia	1235
America	2551

Tabel 3. Jumlah serangan dari Negara asal



4. KESIMPULAN

Berdasarkan hasil yang didapat dengan menganalisa *firewall* yang dipasang penulis dimesin server dan *file log* yang diparsing menggunakan teknik *command grep*, ternyata ada banyak serangan didalam jaringan komputer kampus dibuktikan dengan adanya *log firewall* yang mendeteksi dan menghalangi sebanyak 1840 kali serangan. Selain itu juga percobaan untuk masuk ke sistem dengan memanfaatkan *service SSH* yang aktif. Ada 3 Negara yang melakukan percobaan *SSH* yang paling banyak, china sebanyak 21790 kali percobaan, Amerika sebanyak 2552 kali dan Mongolia sebanyak 1235 kali.

Penulis menyimpulkan dan telah melakukan implementasi:

1. Sebaiknya service SSH dimatikan, dan diaktifkan apabila administrator jaringan mau menggunakannya
2. Pemasangan *IDS (Intrusion Detection System)* dalam hal ini *snort* untuk deteksi yang lebih detail lagi mengenai jenis serangan seperti *Denial Of Service*, *SQL Injection*, dan lain-lain.
3. Pemasangan *IPS (Intrusion Prevention System)*
4. Setiap bulan administrator jaringan perlu membuat rekap dan analisa log, jika masih ada vulnerability dianalisa kembali apa yang perlu diperbaiki dari segi keamanan.

5. SARAN

Cakupan dari penelitian ini adalah secara umum mencari tahu seberapa banyak serangan dengan mencoba mengakses system lewat autentikasi dan mengaktifkan firewall serta *Intrusion Detection System*, untuk pengembangan dari penelitian ini lebih baik lagi kalau jenis serangan dibuat lebih spesifik seperti mendeteksi *SQL Injection*, *Denial of Service*, *rootkit*, dan jenis serangan lainnya yang dapat menggangu sistem yang ada.

UCAPAN TERIMA KASIH

Penulis mengucapkan terima kasih kepada Tuhan Yang Maha Kuasa atas penyertaanNya sehingga penelitian ini dapat diselesaikan. Terima kasih juga kepada Universitas Klabat khususnya Fakultas Ilmu Komputer yang telah membantu dan memberikan dukungan financial terhadap penulis dalam menyelesaikan.

DAFTAR PUSTAKA

[1] Vacca J. R, 2005, *Computer Fornensics-Computer Crime Scene Investigation*, Ed.2, Charles River Media, INC, Boston.

[2] Nelson B, Phillips A, Seuart C, 2010, *Guide to Computer Forensics and Investigations*, Ed.4, Cengage Learning, Boston.

[3] Moehiddin, I, Penangkapan Cracker situ KPU, perang masih berlangsung, https://ilhamqmoehiddin.wordpress.com/2010/02/07/penangkapan-cracker-situs-kpu-masih-berlangsung/, diakses tanggal 21 Januari 2016.

[4] Nena Lim , 2008, Escaping the Computer-Forensics Certification Maze: A Survery of Professional Certifications, *Communications of the Association for Information System (CAIS)*, vol 23 Article 30, hal 548-573.

[5] Berhgel Hal , 2003, The Discipline of Internet Forensics, *Communication of the ACM*, vol 46 No 8, hal 15-20.

[1] [6] Departemen Komunikasi dan Informatika, 2007, *Tutorial Interaktif Instalasi Komputer Forensik Menggunakan Aplikasi Open Source*, Ed.1, Direktorat Sistem Informasi, Perangkat Lunak dan Konten Direktorat Jenderal Aplikasi Telematika, Jakarta.

[7] Abdullah M. T, Mahmod R.,Ghani. A. A., Abdulah M. Z., Sultan A. B., 2008, Advances in Computer Forensics, *IJCSNS International Journal of Computer Science and Network Security*, vol 8 No 2, hal 215-219.

[8] Yusoff Y., Ismail R., Hassan Z., 2011, Common Phases of Computer Forensics Investigation Models, *International Journal of Computer Science & Information Techonolgy (IJCSIT)*, vol 3 No 3, hal 17-31.

[9] Ramadhan Z., 2011, Digital Forensik dan Penanganan Pasca Insiden, *Jurnal Ilmiah AbdiIlmu*, vol 4 No 1, hal 459-468.