

STUDI TINGKAT *PASSWORD POLICY* MAHASISWA PROGRAM STUDI
PENDIDIKAN TEKNIK INFORMATIKA, PENDIDIKAN BAHASA INGGRIS, DAN
PENDIDIKAN MATEMATIKA UNIVERSITAS NEGERI YOGYAKARTA

SKRIPSI

Diajukan kepada Fakultas Teknik
Universitas Negeri Yogyakarta
untuk Memenuhi Sebagian Persyaratan
Guna Memperoleh Gelar Sarjana Pendidikan



Oleh
Hermawan Adhi Saputra
NIM. 07520241041

PROGRAM STUDI PENDIDIKAN TEKNIK INFORMATIKA
FAKULTAS TEKNIK
UNIVERSITAS NEGERI YOGYAKARTA
2012

STUDI TINGKAT *PASSWORD POLICY* MAHASISWA PROGRAM STUDI
PENDIDIKAN TEKNIK INFORMATIKA, PENDIDIKAN BAHASA INGGRIS, DAN
PENDIDIKAN MATEMATIKA UNIVERSITAS NEGERI YOGYAKARTA

SKRIPSI

Diajukan kepada Fakultas Teknik
Universitas Negeri Yogyakarta
untuk Memenuhi Sebagian Persyaratan
Guna Memperoleh Gelar Sarjana Pendidikan

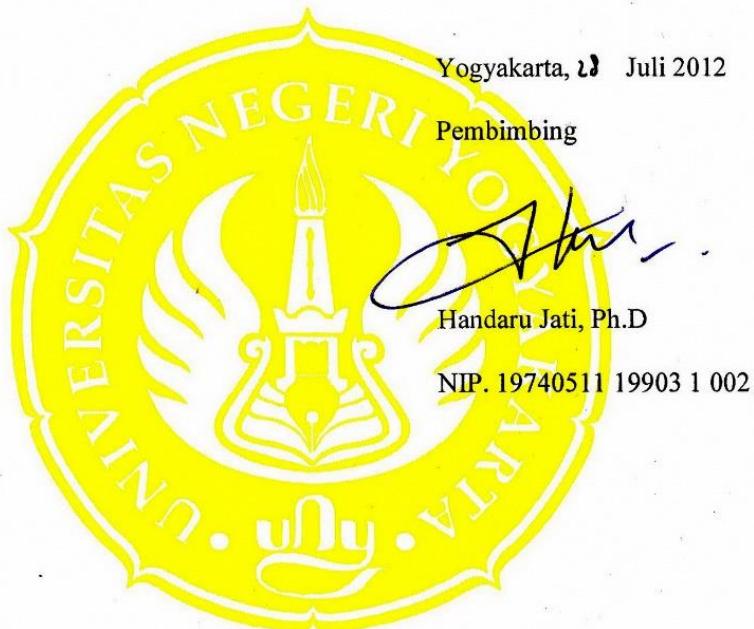


Oleh
Hermawan Adhi Saputra
NIM. 07520241041

PROGRAM STUDI PENDIDIKAN TEKNIK INFORMATIKA
FAKULTAS TEKNIK
UNIVERSITAS NEGERI YOGYAKARTA
2012

PERSETUJUAN

Skripsi yang berjudul “Studi *Password Policy* Mahasiswa Program Studi Pendidikan Teknik Informatika, Pendidikan Bahasa Inggris, dan Pendidikan Matematika Universitas Negeri Yogyakarta” ini telah disetujui oleh pembimbing untuk diujikan.



SURAT PERNYATAAN

Dengan ini saya menyatakan bahwa skripsi ini benar-benar karya saya sendiri. Sepanjang pengetahuan saya tidak terdapat karya atau pendapat yang ditulis atau diterbitkan orang lain kecuali sebagai acuan atau kutipan dengan mengikuti tata penulisan karya ilmiah yang telah lazim.

Tanda tangan dosen pengaji yang tertera dalam halaman pengesahan adalah asli. Jika tidak asli, saya siap menerima sanksi ditunda yudisium pada periode berikutnya.



NIM.07520241041

PENGESAHAN

Skripsi yang berjudul “Studi *Password Policy* Mahasiswa Program Studi Pendidikan Teknik Informatika, Pendidikan Bahasa Inggris, dan Pendidikan Matematika Universitas Negeri Yogyakarta” ini telah dipertahankan di depan Dewan Pengaji pada tanggal18 - 2 - 2013 dan dinyatakan lulus.

Nama	Jabatan	Tandatangan	Tanggal
Handaru Jati, Ph.D	Ketua Pengaji		18 - 2 - 2013
Dr. Ratna Wardani	Sekretaris Pengaji		18 - 2 - 2013
Adi Dewanto, M.Kom	Pengaji Utama		6 - 2 - 2013

DEWAN PENGUJI
UNIVERSITAS NEGERI YOGYAKARTA
Yogyakarta,
Dekan Fakultas Teknik,
Dr. Moch. Bruri Triyono
NIP. 19560216 198603 1 003




HALAMAN MOTTO

Tempat yang jauh tidak mudah dijangkau hanya dengan sekali langkah, namun dengan selangkah demi selangkah tempat tersebut akan mudah dijangkau

(anonim)

HALAMAN PERSEMPAHAN

*Julisan ini kupersembahkan untuk
kedua orangtuaku, kakakku, dan orang-orang tercinta di sepanjang hidupku*

ABSTRAK**STUDI TINGKAT *PASSWORD POLICY* MAHASISWA PROGRAM STUDI PENDIDIKAN TEKNIK INFORMATIKA, PENDIDIKAN BAHASA INGGRIS, DAN PENDIDIKAN MATEMATIKA UNIVERSITAS NEGERI YOGYAKARTA**

Oleh:

Hermawan Adhi Saputra

NIM. 07520241041

Kata sandi merupakan deretan karakter dalam komputer yang disusun guna memberikan hak atas suatu informasi. Terkadang kata sandi yang dipilih adalah kata sandi yang mudah ditebak seperti tanggal lahir, nama akrab atau bahkan sama dengan nama pengguna (*username*). Tujuan utama dilakukan penelitian ini adalah untuk mengetahui tingkat keamanan kata sandi yang digunakan mahasiswa UNY program studi mahasiswa Pendidikan Teknik Informatika dibanding mahasiswa Pendidikan Bahasa Inggris, dan Pendidikan Matematika. Hasil penelitian ini diharapkan dapat memberi wawasan bahwa pemilihan *password policy* yang aman memiliki kriteria tertentu.

Penelitian ini menggunakan angket tertutup sebagai media pengambilan data. Data yang terkumpul dianalisa secara deskriptif. Pendekatan yang dilakukan adalah kuantitatif. Tingkatan keamanan dikelompokkan menjadi 5 yaitu: sangat tidak aman, tidak aman, cukup aman, aman dan sangat aman. Lalu diuji untuk mengetahui seberapa signifikan tingkat *password policy* mahasiswa program studi Pendidikan Teknik Informatika, Pendidikan Bahasa Inggris, dan Pendidikan Matematika

Penelitian ini menunjukkan bahwa mahasiswa Pendidikan Teknik Informatika memiliki tingkat *password policy* paling tinggi yaitu 60,7% dari pada mahasiswa pendidikan Bahasa Inggris yaitu 59,6% dan dari mahasiswa Pendidikan Matematika 54,8%. Baik antara mahasiswa program studi Pendidikan Teknik Informatika, Pendidikan Bahasa Inggris, dan Pendidikan Matematika tidak memiliki perbedaan yang signifikan dalam pemilihan *password policy*.

Kata kunci: keamanan, kebijakan kata sandi

KATA PENGANTAR

Puji syukur *Alhamdulillah* kami panjatkan kehadirat Allah SWT karena hanya dengan kekuatan, kesabaran dan daya juang yang diberikan kepada penulis sehingga mampu menyelesaikan laporan hasil penelitian. Penulis menyadari bahwa dalam penulisan laporan ini tidak lepas dari bantuan berbagai pihak, oleh karena itu kami mengucapkan terima kasih yang tulus kepada

1. Prof. Dr. Rochmat Wahab, M.Pd., MA. Rektor Universitas Negeri Yogyakarta
2. Dr. Moch. Bruri Triyono, Dekan Fakultas Teknik Universitas Negeri Yogyakarta yang telah memberikan izin penelitian
3. Handaru Jati, Ph.D, Dosen Pembimbing yang dengan sabar memberikan bimbingan dan pengarahan selama penyusunan skripsi
4. Totok Sukardiyono, M.T., Dosen Pembimbing Akademik yang sabar memberikan dorongan
5. Bapak/ Ibu dosen Universitas Negeri Yogyakarta atas kemudahan yang telah diberikan
6. Bapak/ Ibu guru SMP N 1 Patuk Gunungkidul atas saran dan nasehatnya
7. Sahabat dan teman-temanku Prodi Pendidikan Teknik Informatika 2007
8. Pihak-pihak lain yang tidak bisa disebutkan satu persatu yang telah memberikan semangat dan dorongan.

Semoga semua amal baik mereka mendapat balasan Tuhan Yang Maha Kuasa.
Mudah-mudahan penelitian ini bermanfaat bagi kalangan semua pihak.

Yogyakarta, Juli 2012
Penulis

Hermawan Adhi Saputra

DAFTAR ISI

HALAMAN JUDUL.....	i
HALAMAN PERSETUJUAN.....	ii
HALAMAN PERNYATAAN	iii
HALAMAN PENGESAHAN.....	iv
HALAMAN MOTTO	v
HALAMAN PERSEMBAHAN	vi
ABSTRAK	vii
KATA PENGANTAR	viii
DAFTAR ISI.....	x
DAFTAR TABEL	xii
DAFTAR GAMBAR	xiii
DAFTAR RUMUS	xiv
DAFTAR LAMPIRAN.....	xv
BAB I PENDAHULUAN.....	1
A. Latar Belakang Masalah	1
B. Identifikasi masalah	4
C. Batasan masalah.....	5
D. Rumusan masalah	5
E. Tujuan Penelitian	6

F. Manfaat Penelitian	6
BAB II KAJIAN PUSTAKA	7
A. Kajian teoritik.....	7
B. Penelitian yang relevan	14
C. Kerangka berpikir.....	16
D. Hipotesis	16
BAB III METODE PENELITIAN.....	17
A. Desain penelitian.....	17
B. Populasi dan sampel.....	17
C. Instrumentasi	19
D. Teknik pengumpulan data.....	20
E. Validitas dan reabilitas instrumen penelitian.....	20
F. Teknik analisis data	21
BAB IV HASIL PENELITIAN DAN PEMBAHASAN.....	23
A. Hasil penelitian.....	23
B. Pembahasan	24
BAB V SIMPULAN DAN SARAN.....	28
A. Simpulan	28
B. Saran	28
DAFTAR PUSTAKA	30
LAMPIRAN-LAMPIRAN	32

DAFTAR TABEL

1. Hasil Percobaan Pertama Bruteforce Calculator Menggunakan Dua Jenis Karakter.....	15
2. Hasil Percobaan Kedua Bruteforce Calculator Menggunakan Dua Jenis Karakter.....	15
3. Kisi-Kisi Instrumen Penelitian.....	19
4. Tingkatan Keamanan <i>Password Policy</i>	22
5. Nilai Rata-Rata Akhir <i>Password Policy</i>	24
6. Perbandingan Tingkat <i>Password Policy</i> pada Layanan SIAKAD	24
7. Hasil Uji Beda Antar Prodi	27

DAFTAR GAMBAR

1. Grafik Jumlah Permintaan *Reset Password* 25

DAFTAR RUMUS

1. Nilai Akhir *Password Policy* 21

DAFTAR LAMPIRAN

1.	Angket penelitian	32
2.	Konversi nilai angket	34
3.	Surat izin kepada UPT puskom UNY	35
4.	Pengolahan data dengan statistik deskriptif dan pengujian normalitas	36
5.	Uji beda tingkat <i>Password Policy</i>	39
	A. Uji beda antara mahasiswa Pendidikan Bahasa Inggris, Pendidikan Matematika dan Pendidikan Teknik Informatika	39
	B. Uji beda antara mahasiswa Pendidikan Bahasa Inggris, dan Pendidikan Matematika.....	41
	C. Uji beda antara mahasiswa Pendidikan Matematika dan Pendidikan Teknik Informatika	43
	D. Uji beda antara mahasiswa Pendidikan Bahasa Inggris, dan Pendidikan Teknik Informatika	45
6.	Data hasil survey Mahasiswa Bahasa Inggris kategori umum.....	51
7.	Data hasil survey Mahasiswa Matematika kategori umum	52
8.	Data hasil survey Mahasiswa Pendidikan Teknik Informatika kategori umum	53
9.	Data hasil survey mahasiswa pendidikan bahasa inggris kategori siakad .	54
10.	Data hasil survey mahasiswa pendidikan matematika kategori siakad.....	55
11.	Data hasil survey mahasiswa pendidikan teknik informatika kategori Siakad.....	56
12.	Data hasil survey Mahasiswa Bahasa Inggris kategori keseluruhan.....	57
13.	Data hasil survey Mahasiswa Matematika kategori keseluruhan	58
14.	Data hasil survey Mahasiswa Pendidikan Teknik Informatika	

kategori keseluruhan	59
15. Data skor password policy	60
16. Data permintaan reset password dari UPT UNY	61
17. Berita terkait keamanan <i>password policy</i>	63

BAB I

PENDAHULUAN

A. Latar Belakang Masalah

Keamanan dalam berkomputer terkait dengan usaha manusia untuk mengamankan data atau informasi yang penting atau bernilai tinggi. Suatu data/ informasi bernilai tinggi bisa berupa data pribadi, data nilai mahasiswa, riwayat hidup, catatan kriminal. Semakin besar manfaat yang diperoleh semakin tinggi nilai informasi tersebut. Data dan informasi merupakan hal yang sangat berharga terutama jika data/ informasi tersebut menyangkut kepentingan bersama.

Prosedur keamanan komputer paling mudah dilaksanakan adalah dengan menggunakan kata sandi (*password*). Kata sandi merupakan aspek pertama dalam setiap keamanan komputer. Kata sandi biasa digunakan saat melakukan pengenalan *user* oleh sebuah sistem. Seperti pada saat kita masuk ke sistem operasi, masuk sebagai *administrator* di *webserver*, masuk layanan *email*, masuk layanan *chatting*, dan sebagainya. Diawal pembuatan *password* oleh *user*, biasanya sistem akan melakukan pengecekan apakah *password user* telah memenuhi beberapa *policy* dari *administrator*. Apabila *password* yang dipilih *user* tidak memenuhi syarat minimal maka sistem akan menolak *password* tersebut.

Sistem yang berinteraksi dengan *user* menggunakan *password* sangat banyak. Banyaknya kebutuhan akan *password* terkadang membuat *user* malas

untuk mengingat banyak *password* dan membuatnya semudah mungkin. Misalkan *login* layanan SIAKAD yang menggunakan id NIM dan *password* sama dengan NIM. Bagi pelaku yang paham akan informasi tersebut mungkin akan dengan mudah masuk dan mengganti informasi pemilik akun resmi seperti biodata, foto, dan *password* resmi. Bisa pula saat *user* layanan SIAKAD menggunakan *password* tanggal lahir, dan teman sekelasnya mengetahui hal tersebut. Teman sekelas tersebut hanya perlu mencoba satu kali dan langsung dapat mengakses SIAKAD korban.

Dampak dari pemilihan *password* yang mudah ditebak akan membuat pihak yang tidak memiliki hak dapat mengambil keuntungan. Beberapa situs berita di internet seperti terlampir di lampiran 17 menuliskan kejadian seputar keamanan *password* antara lain *Ternyata 63% Netter Malas Ganti Password, 20 Password paling buruk di 2011, Mayoritas password internet tidak aman, Separuh remaja internet mengumbar password di internet, Password dan ancaman yang dapat ditimbulkan, Ribuan pengguna Twitter jadi target pencurian password, Hasil survei: pengamanan password masih disepakati, dan 6.5 juta password linkedIn dibobol. Bagaimana password Anda?*. Kasus seperti ini tidak akan terjadi apabila pemilik data/ informasi tersebut membuat *password* yang kuat sesuai *policy* sistem.

Tebak-tebakan dalam *password* mungkin rasional jika dalam hitungan jari masih dimungkinkan menemukan *password*, namun untuk keperluan yang lebih ahli diperlukan teknik khusus. Para pakar komputer telah banyak

membuat *software* otomatis yang dapat memasukkan input berkali-kali untuk menebak sebuah *password* yang ada dalam sebuah sistem. Cara ini sering disebut dengan *bruteforce attack*, dengan kecepatan komputasi sebuah komputer yang semakin cepat dan efisien proses *bruteforce attack* mencoba setiap komposisi *password* dapat berjalan relatif lebih singkat. *Software* semacam ini untuk kalangan administrator digunakan untuk memulihkan *password* yang terlupa, namun ditangan *user* yang tidak benar *software* ini bisa jadi senjata untuk mendapatkan hak akses terhadap sebuah sistem. Untuk menghindari *bruteforce attack* tersebut penggunaan *password* yang kuat harus memiliki kebijakan (*policy*) yang jelas.

Mahasiswa program studi Pendidikan Teknik Informatika UNY merupakan calon guru bidang komputer. Seseorang yang memiliki kemampuan komputer dasar, jaringan, multimedia, pemrograman dan kemampuan komputer lainnya, termasuk keamanan berkomputer. Apabila dari calon guru tersebut saja tidak memiliki standar dalam pengamanan maka dikhawatirkan sifat tersebut akan menurun pada anak didiknya. Mahasiswa Pendidikan Bahasa Inggris dan Pendidikan Matematika dalam penelitian ini sebagai subjek orang awam yang tidak memiliki pengetahuan cukup tentang *password policy*. Mahasiswa Pendidikan Bahasa Inggris mewakili pula bidang bukan eksak dan mahasiswa Pendidikan Matematika mewakili bidang eksak, sehingga diharapkan penelitian ini dapat memberikan gambaran menyeluruh, bagaimana tingkat *password policy* nya?

Terkait dengan berita keamanan *password* maka peneliti mencoba mengaitkan dengan salah satu layanan UNY yaitu Sistem Akademik UNY (SIAKAD UNY). Setiap mahasiswa UNY pasti memiliki akses ke layanan SIAKAD. Setiap mahasiswa baru akan mendapatkan pelatihan ICT untuk memberikan bekal tentang layanan ini, dan pada pelatihan ini biasanya diberitahukan *username* dan *password* masing-masing mahasiswa. Jika tidak diganti *username* dan *password* menggunakan Nomor Induk Siswa (NIM). Mahasiswa tersebut juga bisa mengganti *password*. Tinggal memilih antara *password* yang mudah diingat atau mengganti *password* baru yang mungkin akan terlupa karena jarang diakses. Jika terjadi lupa *password* mahasiswa dapat menghubungi pusat layanan SIAKAD di PUSKOM untuk melakukan permintaan reset *password*. Tingkat kerumitan dalam pemilihan *password* apakah ada kaitanya dengan permintaan reset *password*.

B. Identifikasi masalah

Sesuai dengan kajian berbagai masalah yang relevan dan latar belakang masalah yang telah diuraikan, maka peneliti mengidentifikasi beberapa masalah terkait penelitian ini antara lain:

1. Tingkat *password policy* mahasiswa Pendidikan Bahasa Inggris, mahasiswa Pendidikan Matematika, dan mahasiswa Pendidikan Teknik Informatika UNY pada layanan SIAKAD.
2. Hubungan tingkat *password policy* terhadap kasus kehilangan *password*.

3. Perbedaan tingkat *password policy* pada mahasiswa Pendidikan Bahasa Inggris, mahasiswa Pendidikan Matematika, dan mahasiswa Pendidikan Teknik Informatika.

C. Batasan masalah

Peneliti merasa perlu untuk membatasi penelitian ini agar penelitian ini segera terlaksana sesuai kemampuan, waktu dan dana peneliti. Pembatasan ini tetap mempertimbangkan aspek metodologis tanpa mengorbankan kebermaknaan arti, konsep, atau judul yang diteliti. Oleh karena itu penelitian ini memiliki batasan masalah antara lain:

1. Penelitian hanya dilakukan pada komposisi *password*, tidak berkaitan dengan pengamanan dalam bentuk lain.
2. Penelitian hanya dilakukan pada mahasiswa Universitas Negeri Yogyakarta program studi
 - a. Pendidikan Bahasa Inggris
 - b. Pendidikan Matematika
 - c. Pendidikan Teknik Informatika

D. Rumusan masalah

1. Bagaimana tingkat *password policy* mahasiswa Pendidikan Bahasa Inggris, mahasiswa Pendidikan Matematika, dan mahasiswa Pendidikan Teknik Informatika pada layanan SIAKAD?

2. Apakah terdapat hubungan antara tingkat *password policy* dengan kasus kehilangan *password*?
3. Apakah terdapat perbedaan tingkat *password policy* pada mahasiswa Pendidikan Bahasa Inggris, mahasiswa Pendidikan Matematika, dan mahasiswa Pendidikan Teknik Informatika?

E. Tujuan Penelitian

Target penelitian yang akan dicapai merupakan penyelesaian rumusan masalah antara lain:

1. Mengetahui tingkat *password policy* mahasiswa Pendidikan Bahasa Inggris, mahasiswa Pendidikan Matematika, dan mahasiswa Pendidikan Teknik Informatika pada layanan SIAKAD.
2. Mengetahui ada tidaknya hubungan antara tingkat *password policy* dengan kasus kehilangan *password*
3. Apakah terdapat perbedaan tingkat *password policy* pada mahasiswa Pendidikan Bahasa Inggris, mahasiswa Pendidikan Matematika, dan mahasiswa Pendidikan Teknik Informatika

F. Manfaat Penelitian

Manfaat penelitian ini baik antara lain:

1. membuka wawasan tentang *password policy*, agar mahasiswa lebih memperhatikan *password policy*.

2. bagi admin SIAKAD agar menerapkan standar minimal dalam menggunakan *password*.
3. bagi mahasiswa Pendidikan Teknik Informatika UNY mengetahui tingkat keamanan *password*, sehingga dapat menggunakan password policy dengan benar.
4. bagi universitas penelitian mampu memberikan kontribusi pada ilmu pengetahuan bidang teknik Informatika
5. bagi penulis dapat mengaplikasikan ilmu yang didapat selama perkuliahan

BAB II

KAJIAN PUSTAKA

A. Kajian teoritik

1. Kata sandi (*password*)

Burnett menjelaskan bahwa, “*They (password) authenticate us to a machine to prove our identity—a secret that only we should know*” (Burnett, 2006:4). *Password* merupakan sederet karakter *string* (huruf, angka, dan simbol lain) milik *user* yang digunakan untuk mendapat akses legal terhadap suatu sistem atau terhadap suatu data (Kissell, 2011:134), sehingga dari kedua pendapat tersebut dapat disimpulkan bahwa *password* merupakan sederet karakter yang bersifat pribadi, digunakan untuk membuktikan kepemilikan sah atas suatu sistem.

2. *password policy*

Kurniawan menuliskan bahwa sekelompok aturan yang dibuat untuk meningkatkan keamanan informasi disebut *password policy* (Kurniawan, 2007:10). *Password policy* ini sering menjadi aturan agar memakai *password* yang kuat dan tepat dalam sebuah organisasi resmi.

Burnett mengungkapkan bahwa *password policy* diatur oleh *administrator* dalam sebuah organisasi yang membuat setiap *user* harus memenuhi standar pemilihan *password*, umumnya harus terdiri dari minimal 8 karakter dan memiliki kombinasi angka dan huruf (Burnett, 2006:61).

Password policy merupakan aturan yang dibuat khusus oleh regulasi sebuah organisasi sebagai bagian dari latihan kesadaran keamanan komputer atau *security awareness training*. Hal ini untuk meningkatkan keamanan data komputer organisasi. (http://en.wikipedia.org/wiki/Password_policy).

Password policy jika diliik dari pendapat tersebut dapat disimpulkan merupakan aturan yang dibuat oleh pihak *administrator* (penanggung jawab keamanan) dalam sebuah organisasi untuk menambah keamanan informasi. Dalam penelitian ini pihak yang memiliki hak dan penanggung jawab informasi adalah mahasiswa itu sendiri, selaku *administrator* dan *user*.

3. Standar *password policy*

Masing-masing perusahaan atau ahli memiliki *password policy* tersendiri. Antara lain

1. Microsoft

Dalam sebuah *online support* yang berjudul *Create strong passwords* (<http://www.microsoft.com/security/online-privacy/passwords-create.aspx>), menyebutkan hal-hal penting dalam menyusun *password* agar memiliki pengalaman transaksi *online* yang aman adalah sebagai berikut:

- 1) makin panjang dan komplek makin baik, gunakan
 - a) sekurang-kurangnya 14 karakter atau lebih

- b) variasikan karakter (huruf, tanda baca, simbol dan nomor)
 - c) seluruh tombol keyboard, tidak hanya huruf atau karakter yang sering dilihat atau digunakan
- 2) dapat diingat
- 3) ujilah *password* dengan *software* penguji *password*
- 4) jika *password* tersebut tercatat pastikan catatan tersebut berada di tempat aman dari pengintai
- 5) hal umum yang harus dihindari
 - a) kata yang ada dalam kamus bahasa apapun
 - b) kata yang dibalik, salah ejaan yang umum, dan singkatan
 - c) rentetan atau pengulangan karakter, seperti 123456, 77777, abcdefg, qwerty atau sejenisnya
 - d) informasi pribadi seperti nama, tanggal lahir, nomor SIM/ KTP/ *passport*, nomor telepon atau sejenisnya

2. *Google*

Menurut *gmail help* yang berjudul *Choosing a password and security question* (<http://mail.google.com/support/bin/answer.py?answer=29409> diakses tanggal 27 Maret 2011), google memberikan tips dalam memilih *password* yang baik agar akun *gmail* tetap aman antara lain

- 1) jangan menggunakan kata yang terdapat dalam kamus
- 2) sekurang-kurangnya terdiri dari 8 karakter

- 3) jangan gunakan *password* yang telah digunakan pada akun lain
- 4) jangan gunakan pola tertentu pada keyboard (asdf,qwerty) atau angka yang berurutan (123456)
- 5) gunakan akronim, tapi jangan yang umum seperti NASA atau SCUBA. Kombinasikan dengan nomor dan tanda baca.
- 6) gunakan tanda baca dan nomor, campurkan antara kapital(upper case) dan huruf kecil (lower case)
- 7) gunakan huruf pengganti yang mirip, seperti angka nol (zero) untuk huruf ‘O’ atau \$ untuk huruf ‘S’.
- 8) gunakan fonetis sebagai pengganti, seperti “luv 2 laf” untuk “love to lough”
- 9) jangan membuat *password* dengan hanya kombinasi huruf semua, nomor semua, atau bahkan huruf kecil semua
- 10) Jangan menggunakan karakter yang diulang (111111,aaaa)
- 11) jangan menggunakan contoh *password* yang ada pada tip dari google ini

Dalam lain kesempatan google juga memberikan tips memilih *password* secara cerdas antara lain

- 1) jangan menggunakan kembali (*reuse*) *password* untuk akun yang penting
- 2) gunakan campuran huruf, nomor dan simbol
- 3) buatlah *password* yang sulit ditebak, berdasar informasi pribadi

- 4) jika *password* tertulis dalam suatu media, simpanlah di tempat rahasia atau yang tidak mudah terlihat orang lain
- 5) pastikan pilihan pemulihan (*recovery option*) terbaru dan aman

3. imperva

imperva dalam salah satu *white paper* yang berjudul *Consumer Password Worst Practices* (http://www.imperva.com/docs/ WP_Consumer_Password_Worst_Practices.pdf) diakses tanggal 27 Februari 2011) menuliskan rekomendasi *password* sesuai standart NASA antara lain

- 1) sekurang-kurangnya 8 karakter
- 2) mengandung campuran empat tipe karakter berbeda : uppercase, lowercase, nomor, dan spesial karakter.
- 3) Jika hanya terdapat satu huruf atau spesial karakter, tidak boleh diletakkan diawal atau diakhir karakter *password*.
- 4) harus tidak berkaitan dengan nama, slang word (logat/ ucapan populer), kata yang ada di kamus, atau alamat email
- 5) gunakan *password* yang berbeda untuk semua situs
- 6) jangan percaya pihak ketiga siapapun itu
- 7) gunakan *passphrase*
- 8) ganti secara rutin *password*

4. Burnett dalam buku *Perfect Passwords: Selection, Protection, Authentication* menuliskan kriteria sebuah *password* bisa digolongkan kuat apabila memenuhi kriteria sebagai berikut (Burnett, 2006:136)
 - 1) lebih dari 15 karakter
 - 2) memiliki campuran huruf, nomor, dan simbol tanda baca
 - 3) terdiri dari minimal tiga informasi acak
 - 4) tidak mengandung informasi pribadi seperti tanggal lahir, nama pacar, nama hewan peliharaan, nomor keberuntungan dll
 - 5) jika *password* diketikan di google, tidak mendapatkan hasil
 - 6) hanya diketahui sendiri oleh pembuat *password*
 - 7) dapat diingat tanpa harus mencari
 - 8) bila tercatat disuatu tempat, tempat tersebut aman
 - 9) rutin diganti dalam jangka waktu kurang dari 6 bulan
 - 10) menggunakan satu *password* untuk satu tempat saja
 - 11) dapat diketikkan dengan cepat *password* tanpa kesalahan
5. Jubilee Enterprise dalam buku *Trik Mengamankan Password* (Jubilee Enterprise, 2010:2-10) menyebutkan trik-trik membuat *password* yang aman dan kuat antara lain
 - 1) Panjang *password* minimal 8 karakter
 - 2) Kombinasi antara huruf, angka dan simbol
 - 3) Kombinasi antara huruf kapital dan huruf kecil
 - 4) Jangan mengandung informasi pribadi

- 5) Menggunakan frase
- 6) Jangan menggunakan huruf atau angka secara berurutan
- 7) Hindari kata-kata dalam kamus
- 8) Jangan menggunakan username sebagai *password*

Dari beberapa pendapat ahli tersebut terdapat beberapa point yang sama atau mirip, dan saling melengkapi. Oleh karena itu dapat ditarik kesimpulan bahwa dalam membuat sebuah *password* yang kuat harus memenuhi beberapa kriteria. Kriteria *password* antara lain

1. terdiri dari minimal 8 karakter
2. terdiri dari campuran huruf, angka, simbol dan tanda baca
3. merupakan kombinasi huruf besar dan huruf kecil
4. tidak terdapat dalam kamus
5. tidak mengandung informasi pribadi
6. tidak ada orang lain yang diberitahu
7. bukan hanya perulangan karakter (11111, 9999)
8. bukan hanya rangkaian pola karakter (qwerty, asdf)
9. *password* yang tercatat disimpan ditempat yang aman
10. satu *password* hanya untuk satu akun
11. *password* tidak sama dengan *username*
12. rutin diganti

Keduabelas kriteria tersebut menjadi acuan standar dalam penelitian ini, sehingga *password* yang memenuhi 12 kriteria tersebut dianggap kuat/ aman.

B. Penelitian yang relevan

Pada tahun 2007 dilakukan survey oleh Kurniawan dari ITB yang mengambil tempat Bandung. Survey ini mengambil sampel pelajar, mahasiswa/ mahasiswi, peneliti, wirausahawan, auditor, programmer, dosen, karyawan/ karyawati memperlihatkan bahwa 150 orang tersebut semuanya paham penggunaan *password*. Sebanyak 2% menggunakan spesial karakter, 14% menyatakan bahwa mereka menggunakan *case sensitif* pada komposisi *password*, 37% menggunakan numerik, dan 47% menggunakan alphabet saja.

Waktu yang diperlukan untuk melakukan *bruteforce attack* pada sebuah *password* dapat dihitung dengan *bruteforce calculator* yang dibuat *Mandylion Research Labs*. Kalkulator ini memperkirakan waktu yang dibutuhkan sebuah komputer dengan komputasi $2*(2^{33})$ kode/ jam untuk *cracking* sebuah *password* melalui banyaknya kemungkinan kombinasi karakter pembentuk *password*. Kurniawan pada tahun 2007 melakukan 2 percobaan dengan sampel *password* 6-10 karakter acak, memperoleh hasil hasil sebagai berikut

Tabel 1. Hasil Percobaan Pertama Bruteforce Calculator Menggunakan Dua Jenis Karakter (Kurniawan, 2007:25).

Jenis karakter				Total karakter	Banyak kombinasi	Waktu (jam)
Lower case	Upper case	Numeric	Spesial karakter			
4	-	2	-	6	45 juta	< 0,01
2	-	-	4	6	708 juta	0,02
-	-	4	3	7	327 juta	0,01
-	4	-	3	7	14 milyar	0,44
5	-	3	-	8	11 milyar	0,35
-	-	3	5	8	33 milyar	0,98
6	-	4	-	10	3 triliun	89,91

Tabel 2. Hasil Percobaan Kedua Bruteforce Calculator Menggunakan Dua Jenis Karakter (Kurniawan, 2007:25)

Jenis karakter				Total karakter	Banyak kombinasi	Waktu (jam)
Lower case	Upper case	Numeric	Spesial karakter			
4	-	1	1	6	146 juta	< 0,01
2	1	-	3	6	575 juta	0,02
2	-	2	4	8	46 milyar	1,36
2	-	4	2	8	70 milyar	2,06
5	1	4	-	10	3 triliun	89,91
3	3	2	2	10	31 triliun	920,64

Dari hasil percobaan dapat ditarik kesimpulan bahwa semakin panjang *password* maka semakin lama waktu yang diperlukan untuk melakukan *bruteforce attack*. Penggunaan spesial karakter juga akan membuat proses *bruteforce attack* semakin lama.

C. Kerangka berpikir

Password mempunyai peran penting dalam keamanan komputer. *Password* merupakan gerbang keamanan pertama dalam dunia komputer. Jika gerbang tersebut tidak memiliki keamanan yang baik maka pihak yang tidak memiliki hak akses dapat dengan mudah melewati gerbang tersebut. Pemilihan *password* yang baik dapat membantu meningkatkan keamanan suatu sistem. Namun tidak sedikit orang yang memilih *password* secara asal-asalan, sehingga dengan beberapa teknik tertentu *password* tersebut dapat ditebak oleh pihak yang tidak sah. Dari uraian di atas dapat diambil kesimpulan bahwa pemilihan *password* yang memiliki standar sangat penting.

D. Hipotesis

Ho : Tidak ada perbedaan tingkat *Password Policy* antara mahasiswa Pendidikan Bahasa Inggris, mahasiswa Pendidikan Matematika dan mahasiswa Pendidikan Teknik Informatika.

Ha : Ada perbedaan tingkat *Password Policy* antara mahasiswa Pendidikan Bahasa Inggris, mahasiswa Pendidikan Matematika dan mahasiswa Pendidikan Teknik Informatika.

BAB III

METODE PENELITIAN

A. Desain penelitian

Penelitian ini merupakan penelitian deskriptif dimana penelitian ini bertujuan untuk mendeskripsikan kejadian yang saat ini berlaku dan terdapat upaya mencatat, analisis dan menginterpretasikan kondisi sekarang ini. Penelitian ini mendeskripsikan informasi apa adanya sesuai variabel yang diteliti (Mardalis, 2007:26). Pendekatan yang digunakan adalah kuantitatif.

B. Populasi dan sampel

1. Populasi

Populasi merupakan semua objek atau subjek dipelajari untuk diambil kesimpulannya, populasi memiliki kualitas dan karakteristik tertentu yang ditentukan oleh peneliti. Populasi memiliki cakupan yang luas, bukan hanya orang, objek dan benda-benda saja, namun populasi mencakup sifat yang dimiliki oleh subjek/ objek (Sugiyono, 2011:80).

Populasi yang dipilih peneliti adalah mahasiswa Pendidikan Bahasa Inggris, mahasiswa Pendidikan Matematika, dan mahasiswa Pendidikan Teknik Informatika Universitas Negeri Yogyakarta. Mahasiswa Pendidikan Teknik Informatika mewakili populasi yang memiliki pengetahuan lebih mengenai *password policy*. Sedangkan mahasiswa Pendidikan Bahasa Inggris dan mahasiswa Pendidikan Matematika

mewakili populasi selain mahasiswa Pendidikan Teknik Informatika, populasi ini dianggap awam karena tidak mendalami *password policy*.

2. Cuplikan

Cuplikan atau sampel atau contoh, merupakan bagian dari populasi. Populasi ini diharapkan dapat mewakili karakteristik populasi (Sugiyono, 2011:81). Pengambilan cuplikan teknik *nonprobability sampling* kategori *sampling insidental*. Pada teknik ini tidak semua anggota cuplikan memiliki kesempatan yang sama, hanya siapa saja yang kebetulan ditemui itu sesuai kriteria penelitian maka dapat dijadikan sumber data (Sugiyono, 2011:85).

Jumlah cuplikan yang perlu diambil menurut L.R Gay seperti dikutip oleh Sarbiran untuk penelitian deskriptif adalah sebanyak 10% (Sarbiran, 2009:44). Nasution menuliskan bahwa sampel adalah sepersepuluh dari jumlah populasi atau jika populasi terlalu besar maka sampel akan lebih kecil dari sepersepuluh (Nasution, 2006:101). Hal yang turut menjadi pertimbangan dalam penentuan jumlah cuplikan adalah tujuan penelitian, pengetahuan tentang populasi, kesediaan, jumlah biaya, besar populasi, dan fasilitas. Roscoe dalam buku *Research Methods for Business* seperti dikutip oleh Sugiyono menyebutkan bahwa cuplikan sebanyak 30 sampai 500 layak digunakan dalam suatu penelitian (Sugiyono, 2011:91). Perincian cuplikan untuk mahasiswa Pendidikan Bahasa Inggris adalah 30,

cuplikan untuk mahasiswa Pendidikan Matematika sebanyak 30, dan cuplikan mahasiswa Pendidikan Teknik Informatika sebanyak 30.

C. Instrumentasi

Pada kajian teori telah dijelaskan beberapa pendapat ahli dan beberapa organisasi terkait kriteria standar *password* agar dapat disebut kuat. Kriteria tersebut diajukan acuan dalam membuat angket. Jika dirumuskan menjadi kisi-kisi angket seperti berikut:

Tabel 3. Kisi-Kisi Instrumen Penelitian

Nomor Kisi-kisi instrumen	Nomor butir soal
1	1, 13
2	2, 14
3	3, 15
4	4, 17
5	5, 16
6	6
7	7
8	8
9	9
10	10, 19
11	11, 18
12	12, 20

hasil penulisan angket dapat dilihat pada lampiran 1, lalu untuk cara konversi nilai bisa dilihat pada lampiran 2.

D. Teknik pengumpulan data

Pengumpulan data menggunakan angket tertutup, di dalamnya terdapat pilihan yang dapat dipilih responden. Kuisioner atau angket adalah teknik pengumpulan data melalui formulir yang berisi pertanyaan-pertanyaan yang diajukan untuk mendapatkan informasi yang diperlukan. Keuntungan dalam penggunaan angket tertutup antara lain hasilnya mudah diolah, responden tidak perlu banyak menulis karena jawaban sudah tersedia, pengisian angket dapat berjalan lebih cepat, dan lebih besar harapan angket akan dikembalikan (Nasution, 2006:103).

Angket yang telah dibuat oleh peneliti disebarluaskan secara *online* dengan *link* https://www.kwiksurveys.com/?s=ILLIJJ_304bd36f 1 Mei – 30 Juni 2011. Penyebaran *link* angket tersebut melalui *social media facebook*, dan *email*. Peneliti meminta bantuan pada teman-teman jurusan Pendidikan Bahasa Inggris, Pendidikan Matematika dan Pendidikan Teknik Informatika untuk saling menyebarkan sesama prodi. Angket tersebut sudah tertutup karena telah melewati batas waktu.

E. Validitas dan reliabilitas instrumen penelitian

Sarbiran menulis bahwa instrumen memiliki nilai validitas tinggi apabila instrumen tersebut mampu mengukur apa yang hendak diukur. Sebuah instrumen penelitian dikatakan memiliki validitas tinggi apabila alat tersebut memberikan hasil yang sesuai dengan maksud dilakukannya pengukuran (Sarbiran, 2009:60). Sutrisno Hadi seperti dikutip oleh Sugiyono menyebutkan

bahwa *construct validity* sama dengan *logical validity* atau *validity by definition*. Apabila definisi dari apa yang hendak diukur didasarkan pada teori-teori sudah benar, lalu teori-teori tersebut digunakan sebagai alat ukur maka hasil penelitian dari instrumen tersebut sudah dianggap valid (Sugiyono, 2011:123). Pada penelitian ini pembuatan instrumen didasarkan pada teori-teori yang sudah benar dan digunakan oleh beberapa sumber ahli oleh karena itu instrumen pada penelitian ini dianggap sah atau valid.

Instrumen yang menghasilkan data yang sama pada pengukuran objek yang sama walaupun dicoba beberapa kali berarti instrumen tersebut reliabel (Sugiyono, 2011:348). Seperti instrumen pada ilmu alam, misal penggaris, termometer, timbangan telah diakui validitas dan reliabilitasnya, karena sebelum dikeluarkan pabrik pasti instrumen tersebut telah diuji validitas dan reliabilitasnya berdasar teori yang ada. Instrumen yang digunakan pada penelitian ini dibuat berdasarkan pada teori-teori yang sudah banyak digunakan baik oleh perusahaan, ilmuan dan kalangan Pendidikan sehingga instrumen yang digunakan reliabel.

F. Teknik analisis data

Teknik analisis yang digunakan adalah statistik deskriptif. Statistik deskriptif adalah statistik yang digunakan untuk menganalisis data dengan cara mendeskripsikan atau menggambarkan keadaan objek atau subjek yang diteliti sesuai apa adanya (Sukardi, 2003: 157). Hasil perhitungan diperoleh

Respon didapat dari nilai akhir secara keseluruhan. Kriteria interpretasi tingkat *password policy* jika dibagi menjadi 5 golongan dapat dilihat di tabel 4

Tabel 4. Tingkatan Keamanan *Password Policy*

Rentang nilai (%)	Tingkat
> 80 – 100	Sangat aman
> 60 – 80	Aman
> 40 – 60	Cukup aman
> 20 – 40	Tidak aman
0 – 20	Sangat tidak aman

BAB IV

HASIL PENELITIAN DAN PEMBAHASAN

A. Hasil penelitian

Data penelitian yang diambil dapat dikelompokkan menjadi 3 kategori berdasar penggunaannya, yaitu

1. umum

Password yang biasa digunakan dalam berbagai kepentingan seperti *email*, *online forum*, keanggotaan *website*, *login* komputer. Pada angket kategori umum diwakili 12 pertanyaan, nomor 1 sampai 12.

2. SIAKAD

Sistem Akademik (SIAKAD) merupakan layanan milik Universitas Negeri Yogyakarta bagi mahasiswa untuk mengakses informasi akademik seperti melihat nilai mata kuliah, mengisi Kartu Rencana Studi (KRS), mendaftar yudisium, mendaftar wisuda. Pada kategori SIAKAD data yang diperoleh terbatas 6 pertanyaan, nomor 15 sampai 20.

3. keseluruhan

Merupakan nilai total 18 pertanyaan yang didalamnya terdapat kategori umum dan kategori SIAKAD. Dengan adanya kategori keseluruhan ini maka hasil survei dapat lebih mudah dibandingkan.

Dari hasil pengambilan data diperoleh data seperti pada lampiran 6 sampai dengan 16 jika dirangkum menjadi tabel 6

Tabel 5. Nilai Rata-Rata Akhir *Password Policy*

kategori	a. Pend. B. Inggris	b. Pend. Matematika	c. Pend. T. Informatika
umum	57,5% (cukup aman)	53,1% (cukup aman)	59,4% (cukup aman)
siakad	63,9% (aman)	57,8% (cukup aman)	63,9% (aman)
keseluruhan	59,6% (cukup aman)	54,8% (cukup aman)	60,7% (aman)

B. Pembahasan

Layanan SIAKAD UNY tidak memberi petunjuk dalam memilih *password* sehingga user bebas memilih *password*. Dari angket yang disebar diketahui perbandingan tingkat *password policy user* pada tabel 6

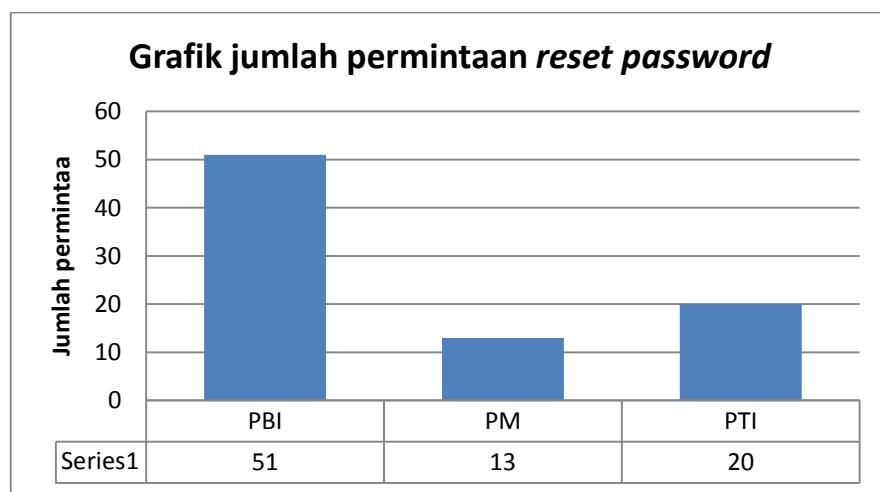
Tabel 6. Perbandingan Tingkat *Password Policy* pada Layanan SIAKAD

Mahasiswa Prodi	Tingkat <i>password policy SIAKAD</i> (%)
PBI	63,9
PM	57,8
PTI	63,9

Dari cuplikan yang diambil mahasiswa Pendidikan Teknik Informatika memiliki tingkat *password policy* yang sama tinggi dengan mahasiswa Pendidikan Bahasa Inggris yaitu 63,9% (aman), dan mahasiswa Pendidikan Matematika memiliki nilai lebih rendah dari keduanya yaitu 57,8% (cukup

aman). Hal ini berarti tidak ada tingkat *password policy* mahasiswa yang masuk dalam kategori sangat aman, sehingga rentang diakses orang lain.

Menurut data Unit Pusat Komputer (UPT) UNY setidaknya 1158 permintaan *reset password* dilakukan sejak Januari 2011 sampai 20 Juli 2011 (lihat lampiran 16), atau setidaknya 165 permintaan per bulan. Jika dirangkum seperti pada gambar berikut



Gambar 1. Grafik Jumlah Permintaan *Reset Password*

Ket:

PBI = mahasiswa Pendidikan Bahasa Inggris

PM = mahasiswa Pendidikan Matematika

PTI = mahasiswa Pendidikan Teknik Informatika.

Permintaan *reset password* oleh *user* ini biasa dikarenakan lupa *password*, atau karena *password* telah diganti orang lain. Pada tabel 6 menunjukkan bahwa mahasiswa PM yang memiliki tingkat *password policy* paling rendah, memiliki jumlah permintaan *reset password* paling sedikit dibanding mahasiswa PBI dan mahasiswa PTI, sehingga dapat

disimpulkan bahwa mahasiswa dengan tingkat *password policy* yang tinggi memiliki kecenderungan lupa *password* lebih tinggi juga.

Sesuai tabel 5 jika dikonversikan dengan tabel 4, sesuai persentase kesesuaian dengan standar yang digunakan maka mahasiswa Pendidikan Teknik Informatika memiliki tingkat *password policy* lebih tinggi (60,7% atau aman) dari mahasiswa Pendidikan Bahasa Inggris (59,6% atau cukup aman), dan dari mahasiswa Pendidikan Matematika (54,8% atau cukup aman). Untuk mengetahui ada tidaknya perbedaan *password policy* mahasiswa Pendidikan Bahasa Inggris, mahasiswa Pendidikan Matematika, dan mahasiswa Pendidikan Teknik Informatika menggunakan *one way ANOVA*. Namun sebelumnya data harus dipastikan berdistribusi normal. Pada lampiran 4, data yang diperoleh dari pengumpulan nilai memiliki distribusi data normal sehingga uji perbedaan dapat dilakukan. Dari perhitungan uji beda keseluruhan dan masing-masing seperti dilampirkan pada lampiran 5 didapat hasil seperti disajikan pada tabel 7, dengan demikian antara tingkat *password policy* mahasiswa Pendidikan Bahasa Inggris, Pendidikan Matematika, mahasiswa Pendidikan Teknik Informatika tidak ada perbedaan yang signifikan.

Tabel 7. Hasil Uji Beda Antar Prodi

Prodi		Hasil uji beda
Pend.Bahasa Inggris	Pend.Matematika	Tidak ada perbedaan
Pend.Matematika	Pend.T.Informatika	Tidak ada perbedaan
Pend.Bahasa Inggris	Pend.T.Informatika	Tidak ada perbedaan
Pend.Bahasa Inggris, Pend.Matematika, dan Pend.T.Informatika		Tidak ada perbedaan

Baik mahasiswa Pendidikan Bahasa Inggris, mahasiswa Pendidikan Matematika, dan mahasiswa Pendidikan Teknik Informatika tidak terdapat perbedaan yang signifikan. Hal ini berarti mahasiswa Pendidikan Teknik Informatika harus meningkatkan *password policy* nya, agar melebihi mahasiswa Pendidikan Bahasa Inggris dan mahasiswa Pendidikan Matematika. Bukan berarti Pendidikan Bahasa Inggris dan mahasiswa Pendidikan Matematika tidak harus meningkatkan *password policy* juga, tetapi karena Mahasiswa Teknik Pendidikan Informatika memiliki tanggungjawab lebih sebagai pendidik bidang komputer, dalam hal ini terutama *password policy*.

BAB V

SIMPULAN DAN SARAN

A. Simpulan

1. Pada layanan SIAKAD mahasiswa Pendidikan Teknik Informatika, Pendididikan Bahasa Inggris, dan mahasiswa Pendidikan Matematika belum masuk dalam kategori tingkat *password policy* sangat aman. Hal ini menimbulkan kerawanan keamanan data.
2. Ada kecenderungan mahasiswa dengan tingkat *password policy* yang tinggi memiliki tingkat lupa *password* lebih tinggi juga.
3. Berdasar nilai keseluruhan data yang diperoleh maka mahasiswa Pendidikan Teknik Informatika memiliki tingkat *password policy* lebih tinggi (60,7% atau aman) dari mahasiswa Pendidikan Bahasa Inggris (59,6% atau cukup aman), dan dari mahasiswa Pendidikan Matematika (54,8% atau cukup aman). Namun tidak terdapat perbedaan signifikan terhadap tingkat *password policy* pada mahasiswa Pendidikan Bahasa Inggris, mahasiswa Pendidikan Matematika, dan mahasiswa Pendidikan Teknik Informatika. Hal ini membuktikan bahwa masih perlunya peningkatan kesadaran *password policy* mahasiswa, terutama mahasiswa Pendidikan Teknik Informatika sebagai calon guru komputer.

B. Saran

1. Khusus untuk mahasiswa Pendidikan Teknik Informatika, harus meningkatkan standar *password policy* karena mahasiswa Pendidikan Teknik Informatika merupakan calon guru yang akan dijadikan contoh.

2. Untuk layanan SIAKAD, walaupun sampai saat ini belum ada kasus mengenai tindak kriminal karena kebobolan *password* setidaknya layanan SIAKAD harus menerapkan *password policy* pada mahasiswa dalam pemilihan *password* layanan SIAKAD.
3. Dikarenakan perkembangan ilmu pengetahuan dan teknologi yang begitu cepat, maka kriteria dalam pemilihan *password* yang kuat bisa saja bertambah seiring berjalannya waktu, sehingga jika penelitian ini diulang harus memperbarui landasan teori.
4. Penelitian ini bersifat kuantitatif sehingga semakin banyak cuplikan maka hasil penelitian akan semakin sesuai dengan kondisi lapangan. Untuk skala penelitian yang lebih besar, dan tidak mempermasalahkan biaya cuplikan yang diambil harus lebih banyak lagi.

DAFTAR PUSTAKA

Brannen, Julia. (2005). *Memadu Metode Penelitian Kualitatif dan Kuantitatif* cetakan keenam (Terjemahan Nuktah Artawie Kurde dkk.). Yogyakarta: Pustaka Pelajar Offset.

Burnett, Mark. (2006). *Perfect Passwords: Selection, Protection, Authentication*. Canada: Syngress Publishing, Inc.

Google Inc. (2011). *Choosing a password and security question*. Diperoleh dari <http://mail.google.com/support/bin/answer.py?answer=29409> diakses tanggal 27 Maret 2011.

Imperva Inc. (2010). *Consumer Password Worst Practices*. Diperoleh dari http://www.imperva.com/docs/WP_Consumer_Password_Worst_Practices.pdf diakses tanggal 27 Februari 2011.

Jubilee Enterprise. (2010). *Trik Mengamanakan Password*. Jakarta: Elex Media Komputindo.

Kissel, Richard (ed). (2011). “*Glossary of Key Information Security Terms*”. *National Institute of Standard and Technology (NIST)*. US Departement of Commerce.

Kurniawan. (2007). Studi tingkat keamanan password pada data, email, dan aplikasi. Tugas akhir, tidak dipublikasikan. Institut Teknologi Bandung.

Mandylion Research Labs. (2006). *BruteForce Attack Time Estimator*. Diperoleh dari <http://www.mandylionlabs.com/index15.htm> diakses tanggal 27 Februari 2011.

Mardalis. (2007). *Metode Penelitian : Suatu Pendekatan proposal Edisi 1, cetakan ke-9*. Jakarta: Bumi Aksara.

Microsoft Inc. (2011). *Create strong passwords*. Diperoleh dari <http://www.microsoft.com/security/online-privacy/passwords-create.aspx> diakses tanggal 27 Maret 2011.

_____. (2011). *Check your password—is it strong?* .Diperoleh dari <https://www.microsoft.com/security/pc-security/password-checker.aspx> diakses tanggal 27 Februari 2011.

Nasution S. (2006). *Metode research (Penelitian Ilmiah)* edisi kesatu cetakan kedelapan. Jakarta: Bumi Aksara.

Purwodarminto. (1989). *Ensiklopedi Nasional Indonesia*. Jakarta: Cipta Adi.

Sarbiran. (2009). *Metodologi Penelitian Pendidikan Kompetensi analisis dan Aplikasi Pendekatan Kuantitatif*. Materi Kuliah (tidak diterbitkan). Universitas Negeri Yogyakarta.

Suharsimi Arikunto. (1999). *Dasar-dasar Evaluasi Pendidikan*. Jakarta: Bumi Aksara.

Sugiyono. (2011). *Metode Penelitian Kuantitatif, Kualitatif dan R & D*. Bandung: CV. Alfabeta.

_____. (2011). *Statistika untuk Penelitian*. Bandung: CV. Alfabeta.

Sukardi. (2003). Metode Penelitian Pendidikan Kompetensi dan Praktiknya. Jakarta: Bumi Aksara.

Sutrisno Hadi. (1974). *Statistik*. Yogyakarta : Yayasan penerbit Fakultas Psikologi UGM.

Triton Prawira Budi. (2003). *SPSS 13.0 Terapan Riset Statistik*. Yogyakarta: Andi.

Wardani, I.G.A.K, dkk. (2009). *Teknik Menulis Karya Ilmiah*. Edisi 1. Jakarta: Universitas Terbuka.

Wikipedia.org. (2009). *Password policy*. Diperoleh dari http://en.wikipedia.org/wiki/Password_policy diakses tanggal 1 Januari 2011.

LAMPIRAN

Lampiran 1. Angket penelitian

Kuesioner Password Policy

Tujuan dari penelitian ini adalah meneliti kebiasaan penggunaan *password* (kata sandi) mahasiswa Universitas Negeri Yogyakarta Jurusan/ Program Studi:

- Pendidikan Bahasa Inggris,
- Pendidikan Matematika,
- dan Pendidikan Teknik Informatika.

Password yang dimaksud bisa berupa *password* email, *password login* komputer, *password* situs atau *password* forum *online*. Semua informasi yang terekam digunakan untuk kepentingan menyusun tugas akhir semata.

Pilihlah jawaban sesuai keadaan sebenarnya dengan memberi tanda (X)/ menulis pada tempat yang tersedia!

NIM : _____ (tidak wajib diisi)

Jurusan/ Program Studi :

- a. Pendidikan Bahasa Inggris
- b. Pendidikan Matematika
- c. Pendidikan Teknik Informatika

	Pertanyaan	Jawaban	
A. Password secara umum			
1. Apakah terdiri dari minimal 8 karakter?	Ya	Tidak	
2. Apakah terdiri dari kombinasi huruf, angka, dan simbol?	Ya	Tidak	
3. Apakah terdapat dalam kamus?	Ya	Tidak	
4. Apakah mengandung informasi pribadi?	Ya	Tidak	
5. Apakah merupakan perulangan karakter (contoh: 11111, 9999) ?	Ya	Tidak	
6. Apakah merupakan rentetan pola karakter pada <i>keyboard</i> (contoh: asdf, qwerty,12345)?	Ya	Tidak	

7. jika <i>password</i> terdokumentasi, apakah tempat dokumen tersebut bersifat rahasia (aman dari orang lain)?	Ya	Tidak
8. Apakah menggunakan kombinasi antara <i>uppercase</i> (huruf besar) dan <i>lowercase</i> (huruf kecil)?	Ya	Tidak
9. Apakah satu <i>password</i> hanya digunakan untuk satu <i>website</i> (atau satu <i>login</i>)?	Ya	Tidak
10. Apakah diperbaharui (diganti) secara rutin?	Ya	Tidak
11. Apakah ada orang lain yang diberitahu?	Ya	Tidak
12. Apakah <i>password</i> sama dengan <i>username</i> ?	Ya	Tidak
B. Password pada layanan siakad.uny.ac.id (SIAKAD)		
13. Berapa panjang karakter <i>password</i> SIAKAD Anda? 1,2,3,...13, atau ≥ 14		
14. Apa saja tipe karakter yang digunakan pada SIAKAD?	a. huruf besar (<i>uppercase</i>) b. huruf kecil (<i>lowercase</i>) c. angka d. simbol/ karakter spesial	
15. Apakah <i>password</i> SIAKAD Anda terdapat dalam kamus?	Ya	Tidak
16. Apakah <i>password</i> SIAKAD Anda merupakan perulangan karakter?	Ya	Tidak
17. Apakah <i>password</i> SIAKAD Anda mengandung informasi pribadi?	Ya	Tidak
18. Apakah ada orang lain yang diberitahu?	Ya	Tidak
19. Apakah <i>password</i> SIAKAD diperbaharui (diganti) secara rutin?	Ya	Tidak
20. Apakah <i>password</i> SIAKAD Anda sama dengan <i>username</i> nya?	Ya	Tidak

 Kepada Saudara/ i – ku

Terimakasih telah berpartisipasi dalam penelitian ini. Kami selaku peneliti mendoakan agar Saudara/i selalu sukses dan diberi kemudahan dalam segala hal. Aamiin

Hormat saya,
 hermawan adhi s.
hermawanadhis@gmail.com

Lampiran 2. Konversi nilai angket

Nomor pertanyaan	Pilihan jawaban	Konversi	
1	Ya/ Tidak	Ya = 1	Tidak = 0
2	Ya/ Tidak	Ya = 1	Tidak = 0
3	Ya/ Tidak	Ya = 0	Tidak = 1
4	Ya/ Tidak	Ya = 0	Tidak = 1
5	Ya/ Tidak	Ya = 0	Tidak = 1
6	Ya/ Tidak	Ya = 0	Tidak = 1
7	Ya/ Tidak	Ya = 1	Tidak = 0
8	Ya/ Tidak	Ya = 1	Tidak = 0
9	Ya/ Tidak	Ya = 1	Tidak = 0
10	Ya/ Tidak	Ya = 1	Tidak = 0
11	Ya/ Tidak	Ya = 0	Tidak = 1
12	Ya/ Tidak	Ya = 0	Tidak = 1
13	1,2,3,4,5,6,7,8,9,10, 11,12,13,>=14	Kurang dari 8 bernilai 0 Lebih dari atau sama dengan 8 bernilai 1	
14	a,b,c,d	14a = ab,abc,abd,abcd = 1	selain itu = 0
	ab,ac,bc,bd,cd	14b = acd,bcd,abcd = 1	selain itu = 0
	abc,abd,acd,bcd		
	abcd		
15	Ya/ Tidak	Ya = 0	Tidak = 1
16	Ya/ Tidak	Ya = 0	Tidak = 1
17	Ya/ Tidak	Ya = 0	Tidak = 1
18	Ya/ Tidak	Ya = 0	Tidak = 1
19	Ya/ Tidak	Ya = 1	Tidak = 0
20	Ya/ Tidak	Ya = 0	Tidak = 1

Lampiran 3. Surat izin kepada UPT puskom UNY

Hal : permohonan izin

Kepada

Yth. Kepala UPT Pusat Komputer UNY

Dengan hormat

Saya yang bertanda tangan di bawah ini

nama : Hermawan Adhi Saputra

NIM : 07520241041

program studi : Pendidikan Teknik Informatika

adalah mahasiswa UNY yang sedang melaksanakan tugas akhir berjudul *Studi tingkat Password Policy mahasiswa Universitas Negeri Yogyakarta*. Saya bermaksud mengajukan permohonan izin pengambilan statistik mahasiswa yang mengganti kata sandi (*password*) SIAKAD di UPT Puskom.

Demikian surat ini saya buat, atas izin yang diperoleh saya ucapan terimakasih.

Yogyakarta, Juli 2011

Mengetahui,

Dosen Pembimbing

Yang menyatakan,

Handaru Jati, Ph.D

NIP. 19740511 19903 1 002

Hermawan Adhi Saputra

NIM.07520241041

Lampiran 4. Pengolahan data dengan statistik deskriptif dan pengujian normalitas
 Langkah menyelesaikan masalah dengan SPSS:

1. Buat dua varibel data pada lembar kerja SPSS

- Variabel kedua : prodi

Tipe data: *numeric, width 8, desimal places : 0*

Value 3 yaitu 1(PB.Indonesia), 2(P.Matematika), 3(PT.Informatika)

- Variabel pertama : skor

Tipe data: *numeric, width 8, desimal places : 0*

2. Masukan data (lampiran 15) ke lembar data SPSS

3. Analisis dengan cara klik *Analyze > Descriptive Statistics > Explore*

4. Masukan variabel Skor ke kotak *Dependent List* dan Prodi ke kotak *Independent List*, kemudian klik *tab Plots*, beri tanda centang pada *Normality plot with tests*, klik *continue*, lalu klik *OK*

5. SPSS akan melakukan proses pengolahan dan hasilnya sebagai berikut

Case Processing Summary

Prodi	Cases						
	Valid		Missing		Total		
	N	Percent	N	Percent	N	Percent	
Skor	PB.Indonesia	30	100.0%	0	.0%	30	100.0%
	P.Matematika	30	100.0%	0	.0%	30	100.0%
	PT.Informatika	30	100.0%	0	.0%	30	100.0%

Descriptives

Prodi			Statistic	Std. Error
Skor	PB.Indonesia	Mean	59.2333	2.24616
		95% Confidence Interval for Mean		
		Lower Bound	54.6394	
		Upper Bound	63.8273	
		5% Trimmed Mean	59.0926	
		Median	61.0000	
		Variance	151.357	
		Std. Deviation	1.23027E1	
		Minimum	38.00	
		Maximum	83.00	

	Range	45.00	
	Interquartile Range	16.00	
	Skewness	.137	.427
	Kurtosis	-.374	.833
P.Matematika	Mean	54.4667	2.28726
	95% Confidence Interval for Mean	Lower Bound	49.7887
		Upper Bound	59.1446
	5% Trimmed Mean	54.4074	
	Median	55.0000	
	Variance	156.947	
	Std. Deviation	1.25279E1	
	Minimum	27.00	
	Maximum	83.00	
	Range	56.00	
	Interquartile Range	12.50	
	Skewness	-.029	.427
	Kurtosis	-.014	.833
PT.Informatika	Mean	60.2333	2.42624
	95% Confidence Interval for Mean	Lower Bound	55.2711
		Upper Bound	65.1955
	5% Trimmed Mean	60.6111	
	Median	66.0000	
	Variance	176.599	
	Std. Deviation	1.32891E1	
	Minimum	27.00	
	Maximum	83.00	
	Range	56.00	
	Interquartile Range	16.00	
	Skewness	-.537	.427
	Kurtosis	.212	.833

Tests of Normality

Prodi	Kolmogorov-Smirnov ^a	Shapiro-Wilk
-------	---------------------------------	--------------

		Statistic	df	Sig.	Statistic	df	Sig.
Skor	PB. Inggris	.110	30	.200*	.961	30	.326
	P. Matematika	.134	30	.176	.962	30	.345
	PT. Informatika	.201	30	.003	.940	30	.091

a. Lilliefors Significance Correction

*. This is a lower bound of the true significance.

Ket.

Mean : rata-rata skor *password policy*

Standard error : kesalahan standar untuk populasi yang diperkirakan dari sampel dengan menggunakan ukuran rata-rata.

Lower bound : nilai rata-rata setelah adanya pemotongan data terkecil 5% dan terbesar 5%. Hal ini dilakukan untuk menghilangkan data yang menimpang karena jauh dari rata-rata.

Median : titik tengah jika semua data diurutkan dan dibagi sama besar

Variance : varian data yang didapat dari kelipatan standar deviasi

Minimum : nilai skor terendah

Maximum : nilai skor tertinggi

Range : jarak data (data *maximum* dikurangi data *minimum*)

6. Cara menentukan apakah data berdistribusi normal atau tidak, maka dihitung *ratio skewness* dengan *standard error of skewness*. Jika *ratio skewness* antara -2 sampai 2 maka distribusi data normal.
 - Pada kelompok mahasiswa pendidikan bahasa inggris diperoleh *ratio skewness* dengan *standard error of skewness* atau $0,137/0,473 = 0,321$; sehingga data berdistribusi normal.
 - Pada kelompok mahasiswa pendidikan matematika diperoleh *ratio skewness* dengan *standard error of skewness* atau $-0,029/0,427 = -0,067$; sehingga data berdistribusi normal.
 - Pada kelompok mahasiswa pendidikan teknik informatika *ratio skewness* dengan *standard error of skewness* atau $-0,537/0,427 = -1,257$; sehingga data berdistribusi normal.

Lampiran 5.Uji beda tingkat *Password Policy*

Tabel Skor tingkat *Password Policy* masing-masing Prodi

No.Responden	Program Studi		
	Pend.Bahasa Inggris (a)	Pend.Matematika (b)	Pend.Teknik Informatika (c)
1	38,89	66,67	50,00
2	55,56	83,33	66,67
3	66,67	72,22	44,44
4	38,89	50,00	50,00
5	61,11	72,22	27,78
6	61,11	38,89	55,56
7	50,00	61,11	38,89
8	83,33	61,11	66,67
9	50,00	61,11	66,67
10	77,78	61,11	61,11
11	55,56	50,00	66,67
12	50,00	38,89	38,89
13	55,56	44,44	66,67
14	83,33	55,56	66,67
15	77,78	55,56	61,11
16	44,44	72,22	83,33
17	66,67	61,11	55,56
18	61,11	50,00	61,11
19	66,67	38,89	72,22
20	55,56	38,89	66,67
21	50,00	61,11	83,33
22	61,11	55,56	55,56
23	50,00	50,00	50,00
24	38,89	27,78	66,67
25	61,11	50,00	44,44
26	61,11	50,00	66,67
27	72,22	61,11	77,78
28	66,67	61,11	66,67
29	55,56	38,89	66,67
30	72,22	55,56	77,78

A. Uji beda antara mahasiswa Pendidikan Bahasa Inggris, Pendidikan Matematika dan Pendidikan Teknik Informatika

Langkah analisisnya:

1. Buatlah 2 variabel data pada lembar kerja variabel view SPSS

- a. Variabel pertama : prodi

Tipe data: numeric, desimal places : 0, measure : nominal

Values yaitu 1(PB. Inggris), 2(P. Matematika), 3(PT.informatika)

- b. Variabel kedua : skor

Tipe data: numeric, desimal places : 2, measure : scale

2. Masukan data ke *data view* SPSS
3. Analisis dengan cara *Analyze > Compare Means > One Way ANOVA*
4. Masukkan variabel Skor ke kotak *Dependent List* dan variabel Prodi ke kotak *Factor*. Pilih tombol *option* dan beri tanda cek pada *Descriptive* dan *Homogeneity of variance test*. Selanjutnya pilih tombol *continue*
5. Klik OK. Maka akan keluar output sebagai berikut

Descriptives

Skor								
	N	Mean	Std. Deviation	Std. Error	95% Confidence Interval for Mean		Minimum	Maximum
					Lower Bound	Upper Bound		
PB.inggris	30	59.6303	12.28725	2.24333	55.0422	64.2185	38.89	83.33
P.matematika	30	54.8150	12.35586	2.25586	50.2012	59.4288	27.78	83.33
PT.informatika	30	60.7420	13.28660	2.42579	55.7807	65.7033	27.78	83.33
Total	90	58.3958	12.77316	1.34641	55.7205	61.0711	27.78	83.33

Test of Homogeneity of Variances

Skor				
Levene Statistic	df1	df2	Sig.	
.096	2	87	.908	

ANOVA

Skor					
	Sum of Squares	df	Mean Square	F	Sig.
Between Groups	595.526	2	297.763	1.860	.162
Within Groups	13925.149	87	160.059		
Total	14520.674	89			

6. Analisis

Hipotesis

Ho Tidak ada perbedaan rata-rata Password Policy antara mahasiswa
 : Pendidikan Bahasa Inggris, mahasiswa Pendidikan Matematika
 dan mahasiswa Pendidikan Teknik Informatika

Ha Ada perbedaan rata-rata Password Policy antara mahasiswa
 : Pendidikan Bahasa Inggris, mahasiswa Pendidikan Matematika
 dan mahasiswa Pendidikan Teknik Informatika.

7. Dari output didapat nilai F hitung adalah 1,860 dan signifikansi 0,162

8. F tabel dicari pada signifikansi 0,05
 $df1$ (jumlah kelompok data-1)=1 dan $df2$ ($n-2$)=58. Hasil F tabel sebesar 4,007

9. Kriteria pengujian

- Jika F hitung $\leq F$ tabel, maka H_0 diterima
- Jika F hitung $> F$ tabel, maka H_0 ditolak

Berdasarkan signifikansi

- Jika signifikansi $> 0,05$ maka H_0 diterima
- Jika signifikansi $< 0,05$ maka H_0 ditolak

10. Karena F hitung $< F$ tabel ($1,860 < 4,007$) dan signifikansi $> 0,05$ ($0,162 > 0,05$) maka H_0 ditolak. Jadi, dapat disimpulkan bahwa tidak ada perbedaan rata-rata Password Policy antara mahasiswa Pendidikan Bahasa Inggris, mahasiswa Pendidikan Matematika dan mahasiswa Pendidikan Teknik Informatika.

B. Uji beda nilai *password policy* pada mahasiswa Pendidikan Bahasa Inggris dan mahasiswa Pendidikan Matematika

Langkah analisisnya:

1. Buatlah 2 variabel data pada lembar kerja variabel view SPSS
 - a. Variabel pertama : prodi

Tipe data: numeric, desimal places : 0, measure : nominal
 Values yaitu 1(PB. Inggris), 2(P. Matematika)

b. Variabel kedua : skor

Tipe data: numeric, desimal places : 2, measure : scale

2. Masukan data ke data view SPSS
3. Analisis dengan cara Analyze > Compare Means > One Way ANOVA
4. Masukkan variabel Skor ke kotak Dependent List dan variabel Prodi ke kotak Factor. Pilih tombol option dan beri tanda cek pada Descriptive dan Homogeneity of variance test. Selanjutnya pilih tombol continue
5. Klik OK. Maka akan keluar output sebagai berikut

Descriptives

Skor								
	N	Mean	Std. Deviation	Std. Error	95% Confidence Interval for Mean		Minimum	Maximum
					Lower Bound	Upper Bound		
PB. Inggris	30	59.6303	12.28725	2.24333	55.0422	64.2185	38.89	83.33
P. Matematika	30	54.8150	12.35586	2.25586	50.2012	59.4288	27.78	83.33
Total	60	57.2227	12.45567	1.60802	54.0050	60.4403	27.78	83.33

Test of Homogeneity of Variances

Skor				
	Levene Statistic	df1	df2	Sig.
	.000	1	58	1.000

ANOVA

Skor						
	Sum of Squares	df	Mean Square	F	Sig.	
Between Groups	347.812	1	347.812	2.291	.136	
Within Groups	8805.668	58	151.822			
Total	9153.479	59				

6. Analisis

Hipotesis

Ho : Tidak ada perbedaan rata-rata Password Policy antara mahasiswa Pendidikan Bahasa Inggris dan mahasiswa Pendidikan Matematika

Ha : Ada perbedaan rata-rata Password Policy antara mahasiswa Pendidikan Bahasa Inggris dan mahasiswa Pendidikan Matematika.

7. Dari output didapat nilai F hitung adalah 2,291 dan signifikansi 0,136

8. F tabel dicari pada signifikansi 0,05

df1 (jumlah kelompok data-1)=1 dan df2 (n-2)=58. Hasil F tabel sebesar 4,007

9. Kriteria pengujian

- Jika $F_{hitung} \leq F_{tabel}$, maka H_0 diterima
- Jika $F_{hitung} > F_{tabel}$, maka H_0 ditolak

Berdasar signifikansi

- Jika signifikansi $> 0,05$ maka H_0 diterima
- Jika signifikansi $< 0,05$ maka H_0 ditolak

10. Karena F hitung < F tabel ($2,291 < 4,007$) dan signifikansi > 0,05 ($0,136 > 0,05$) maka H_0 ditolak. Jadi, dapat disimpulkan bahwa tidak ada perbedaan rata-rata password policy antara mahasiswa Pendidikan Bahasa Inggris dengan mahasiswa Pendidikan Matematika.

C. Uji beda nilai *password policy* pada mahasiswa Pendidikan Matematika dan mahasiswa Pendidikan Teknik Informatika

Langkah analisisnya:

1. Buatlah 2 variabel data pada lembar kerja variabel view SPSS

a. Variabel pertama : prodi

Tipe data: numeric, desimal places : 0, measure : nominal

Values yaitu 2(P.Matematika), 3(PT.informatika)

b. Variabel kedua : skor

Tipe data: numeric, desimal places : 2, measure : scale

2. Masukan data ke data view SPSS
3. Analisis dengan cara Analyze > Compare Means > One Way ANOVA
4. Masukkan variabel Skor ke kotak Dependent List dan variabel Prodi ke kotak Factor. Pilih tombol option dan beri tanda cek pada Descriptive dan Homogeneity of variance test. Selanjutnya pilih tombol continue
5. Klik OK. Maka akan keluar output sebagai berikut

Descriptives								
Skor	N	Mean	Std. Deviation	Std. Error	95% Confidence Interval for Mean		Minimum	Maximum
					Lower Bound	Upper Bound		
P.matematika	30	54.8150	12.35586	2.25586	50.2012	59.4288	27.78	83.33
PT.informatika	30	60.7420	13.28660	2.42579	55.7807	65.7033	27.78	83.33
Total	60	57.7785	13.06682	1.68692	54.4030	61.1540	27.78	83.33

Test of Homogeneity of Variances

Skor				
Levene Statistic	df1	df2	Sig.	
.140	1	58	.710	

ANOVA

Skor	Sum of Squares	df	Mean Square	F	Sig.	
Between Groups	526.940	1	526.940	3.201	.079	
Within Groups	9546.831	58	164.601			
Total	10073.771	59				

6. Analisis

Hipotesis

Ho Tidak ada perbedaan rata-rata Password Policy antara mahasiswa
 : Pendidikan Matematika dan mahasiswa Pendidikan Teknik
 Informatika

Ha Ada perbedaan rata-rata Password Policy antara mahasiswa
 : Pendidikan Matematika dan mahasiswa Pendidikan Teknik
 Informatika

7. Dari output didapat nilai F hitung adalah 3,201 dan signifikansi 0,079

8. F tabel dicari pada signifikansi 0,05

df1 (jumlah kelompok data-1)=1 dan df2 (n-2)=58. Hasil F tabel sebesar 4,007

9. Kriteria pengujian

- Jika F hitung \leq F tabel, maka Ho diterima
- Jika F hitung $>$ F tabel, maka Ho ditolak

Berdasarkan signifikansi

- Jika signifikansi $>$ 0,05 maka Ho diterima
- Jika signifikansi $<$ 0,05 maka Ho ditolak

10. Karena F hitung $<$ F tabel ($3,201 < 4,007$) dan signifikansi $>$ 0,05 ($0,079 > 0,05$) maka Ho ditolak. Jadi, dapat disimpulkan bahwa tidak ada perbedaan rata-rata Password Policy antara mahasiswa Pendidikan Matematika dan mahasiswa Pendidikan Teknik Informatika.

D. Uji beda nilai *password policy* pada mahasiswa Pendidikan Bahasa Inggris dan mahasiswa Pendidikan Teknik Informatika

Langkah analisisnya:

1. Buatlah 2 variabel data pada lembar kerja variabel view SPSS

a. Variabel pertama : prodi

Tipe data: numeric, desimal places : 0, measure : nominal

Values yaitu 1(PB.inggris), 3(PT.informatika)

b. Variabel kedua : skor

Tipe data: numeric, desimal places : 2, measure : scale

2. Masukan data ke data view SPSS
3. Analisis dengan cara Analyze > Compare Means > One Way ANOVA
4. Masukkan variabel Skor ke kotak Dependent List dan variabel Prodi ke kotak Factor. Pilih tombol option dan beri tanda cek pada Descriptive dan Homogeneity of variance test. Selanjutnya pilih tombol continue
5. Klik OK. Maka akan keluar output sebagai berikut

Descriptives								
Skor	N	Mean	Std. Deviation	Std. Error	95% Confidence Interval for Mean		Minimum	Maximum
					Lower Bound	Upper Bound		
PB.inggris	30	59.6303	12.28725	2.24333	55.0422	64.2185	38.89	83.33
PT.informatika	30	60.7420	13.28660	2.42579	55.7807	65.7033	27.78	83.33
Total	60	60.1862	12.70015	1.63958	56.9054	63.4670	27.78	83.33

Test of Homogeneity of Variances

Skor	Levene Statistic	df1	df2	Sig.
	.142	1	58	.708

ANOVA

Skor	Sum of Squares	df	Mean Square	F	Sig.
Between Groups	18.537	1	18.537	.113	.738
Within Groups	9497.799	58	163.755		
Total	9516.336	59			

6. Analisis

Hipotesis

Ho Tidak ada perbedaan rata-rata Password Policy antara mahasiswa

: Pendidikan Bahasa Inggris dan mahasiswa Pendidikan Teknik
Informatika

Ha Ada perbedaan rata-rata Password Policy antara mahasiswa
 : Pendidikan Bahasa Inggris dan mahasiswa Pendidikan Teknik
 Informatika

7. Dari output didapat nilai F hitung adalah 0,113 dan signifikansi 0,738
8. F tabel dicari pada signifikansi 0,05
 $df1$ (jumlah kelompok data-1)=1 dan $df2$ ($n-2$)=58. Hasil F tabel sebesar 4,007
9. Kriteria pengujian
 - Jika F hitung $\leq F$ tabel, maka H_0 diterima
 - Jika F hitung $> F$ tabel, maka H_0 ditolakBerdasarkan signifikansi
 - Jika signifikansi $> 0,05$ maka H_0 diterima
 - Jika signifikansi $< 0,05$ maka H_0 ditolak
10. Karena F hitung $< F$ tabel ($0,113 < 4,007$) dan signifikansi $> 0,05$ ($0,738 > 0,05$) maka H_0 ditolak. Jadi, dapat disimpulkan bahwa tidak ada perbedaan rata-rata Password Policy antara mahasiswa Pendidikan Bahasa Inggris dan mahasiswa Pendidikan Teknik Informatika.

Lampiran 17. Berita terkait keamanan *password policy*

[ictwatch.com/internetsehat/2010/08/11/63-pengguna-internet-malas-mengganti-password/](http://www.ictwatch.com/internetsehat/2010/08/11/63-pengguna-internet-malas-mengganti-password/)

Ternyata 63% Netter Malas Ganti Password

August 11, 2010 in [a. Headline](#), [b. Berita & Fakta](#) by [Tim Internet Sehat](#)



(Internet Sehat) Sebuah survei mengungkapkan fakta yang mencengangkan tentang password, termasuk kebiasaan mengganti password, faktor yang dipertimbangkan ketika membuat password, dan nama atau kata yang digunakan saat membuat password.

Hasilnya, sebanyak 63 persen pengguna internet ternyata malas mengganti password alias tidak terlalu sering mengubah password, 17 persen mengaku menggantinya setiap kuartal, 9 persen menggantinya setiap tahun dan hanya 4 persen yang mengaku mengubah password minimal tiap bulan. Sisanya, tidak pernah mengganti password sama sekali.

Survei tersebut digelar secara online di internet oleh perusahaan keamanan dan antivirus Symantec, melalui blognya selama beberapa hari. Hasil survei (prosentase) tersebut terbilang cukup mengejutkan, mengingat saat ini kejahatan cyber semakin pandai memanfaatkan peluang dan gencar melakukan penyerangan lewat teknik rekayasa sosial ataupun jebakan lainnya.

<http://www.ictwatch.com/internetsehat/2010/08/11/63-pengguna-internet-malas-mengganti-password/>

[ictwatch.com/internetsehat/2011/11/25/25-password-paling-buruk-di-2011/](http://www.ictwatch.com/internetsehat/2011/11/25/25-password-paling-buruk-di-2011/)

25 Password Paling Buruk di 2011

November 25, 2011 in [a. Headline](#), [b. Berita & Fakta](#) by [Tim Internet Sehat](#)



Layaknya paspor, kita membutuhkan password agar bisa masuk ke sebuah layanan online entah itu *social media*, email atau layanan perbankan. Memakai password yang kuat dan sulit ditebak adalah syarat mutlak yang harus dimiliki jika ingin data-data aman saat berselancar di dunia maya.

Namun sayang, pengguna internet tampaknya tidak pernah belajar dari kasus-kasus pembobolan password yang banyak terjadi di internet belakangan ini. Mereka (pengguna internet-red) tetap saja memakai password yang mudah ditebak.

SplashData, developer software keamanan, mencoba men-generate daftar dari jutaan password yang dicuri dan diposting online oleh hacker. Hasilnya tidak mengherankan, password yang paling umum dipakai dan juga yang paling buruk termasuk "password", "123456" dan "qwerty" .

<http://www.ictwatch.com/internetsehat/2011/11/25/25-password-paling-buruk-di-2011/>

teknologi.inilah.com/read/detail/1849486/mayoritas-password-internet-tidak-aman

Mayoritas Password Internet Tidak Aman?



Oleh: Ahmad Taufiqqurakhman
Teknologi - Selasa, 10 April 2012 | 17:40 WIB

INILAH.COM, London - Mayoritas dari password internet tidak aman?

Setidaknya survei terbaru menyatakan hal tersebut.

Dengan banyaknya alamat *email*, situs jejaring sosial dan bank *online* saat ini, tentunya mengingat *password* satu persatu bakal menyulitkan seseorang. Demikian seperti dikutip dari [PocketLint](#).

Sebuah survei mengindikasikan bahwa lebih dari 70% dari pengguna internet cukup rentan terhadap serangan *hack*, mengingat mudahnya *password* mereka.

Berita Terkait

- [Inilah 10 Selebritis Teratas di Jejaring Sosial](#)
- [Video: Balotelli Belajar Bungkus Kado dari Tevez](#)
- [IE Masih Browser Terpopuler di Eropa](#)
- [Celah di Browser IE Bisa Lacak Pergerakan Mouse](#)
- [FB Lebih Membangun 'Ikatan' Ketimbang Twitter](#)

<http://teknologi.inilah.com/read/detail/1849486/mayoritas-password-internet-tidak-aman>

inet.detik.com/read/2010/09/27/155454/1449635/398/separuh-remaja-umbar-password-di-internet

Separuh Remaja Umbar Password di Internet

Fajar Widiantoro - detikinet



ilustrasi (ist)

Jakarta - Riset terbaru dari perusahaan antivirus AVG mengungkapkan, hampir separuh (39%) dari pengguna internet usia 18-25 tahun ternyata gemar berbagi *password* pribadi mereka. Kebiasaan tersebut biasa dilakukan dengan teman dekat atau anggota keluarga.

"Faktanya, kebanyakan pengguna internet usia muda memang mengamankan laptop atau PC mereka dengan *password*. Tapi yang dikhawatirkan di sini adalah empat dari sepuluh dari mereka gemar berbagi *password*," papar Tony Anscombe, juru bicara AVG.

Riset tersebut dilakukan sebagai bagian dari kampanye edukasi AVG, terkait masalah keamanan penggunaan jejaring sosial. Beberapa poin penting dari riset itu mengatakan bahwa wanita lebih sering berbagi *password* (42%), sementara pria hanya 28%.

<http://inet.detik.com/read/2010/09/27/155454/1449635/398/separuh-remaja-umbar-password-di-internet>

inet.detik.com/read/2010/09/30/113440/1452069/323/password-dan-ancaman-yang-bisa-ditimbulkannya/?i991

Password dan Ancaman yang Bisa Ditimbulkannya

Penulis: IGN Mantra - detikinet

Kamis, 30/09/2010 11:35 WIB



Ilustrasi (Ist.)

Jakarta - Password, apakah itu? Siapa yang tak mengenal password? Kebanyakan orang saat ini hanya menggunakanya sebagai formalitas tanpa tahu apa sebenarnya password, apa kegunaan, manfaat dan yang paling penting adalah bagaimana melindunginya.

Nah, soal kode-kode rahasia inilah yang akan dibahas penulis. Sehingga pembaca detikINET diharapkan dapat mengetahui apa sebenarnya password itu dan bagaimana cara mengelolanya.

Password adalah 'kata kunci', itu merupakan terjemahan bahasa Indonesia, gabungan dua kata 'pass' dan 'word'. Namun tak sesederhana itu, password berisi kode-kode tertentu yang disusun oleh pemiliknya baik oleh individu atau kelompok untuk melakukan sebuah autentikasi terhadap sistem yang berisi berbagai informasi.

<http://inet.detik.com/read/2010/09/30/113440/1452069/323/password-dan-ancaman-yang-bisa-ditimbulkannya/?i991102105>

inet.detik.com/read/2010/02/24/124651/1305820/323/ribuan-pengguna-twitter-jadi-target-pencurian-password

Ribuan Pengguna Twitter Jadi Target Pencurian Password

Ardhi Suryadhi - detikinet

Rabu, 24/02/2010 13:50 WIB



Ilustrasi (Ist.)

Singapura - Serangan cyber terhadap account Twitter terdeteksi dalam jumlah yang cukup besar. Para pelaku bermiat mencuri password (phishing) untuk kemudian membajak account di situs mikro blogging itu.

Menurut perusahaan sekuriti Sophos, serangan ini dimulai sejak Sabtu lalu. Hal itu diketahui setelah beberapa account Twitter memposting pesan yang disamaratakan dengan kata-kata humor. Padahal di balik itu, niat para peretas adalah untuk mencuri password pengguna Twitter.

Pesan tersebut beberapa di antaranya berbunyi, "Lol. this is me??", "lol , this is funny.", "Lol. this you???" and "ha ha, u look funny on here" dan ditambahi dengan suatu link.

Nah, link inilah yang akan menuntun pengguna yang tidak waspada ke situs login Twitter palsu. Dari situs palsu tersebut, password dan username pengguna Twitter akan dicuri.

<http://inet.detik.com/read/2010/02/24/124651/1305820/323/ribuan-pengguna-twitter-jadi-target-pencurian-password>

Hasil Survei: Pengamanan Password Masih Disepelekan

June 21, 2010 in [a. Headline](#), [b. Berita & Fakta](#) by [Tim Internet Sehat](#)



Sebuah hasil survei yang dirilis vendor anti-virus F-Secure menunjukkan, masih banyak pengguna teknologi yang belum mengindahkan imbauan untuk menggunakan password yang berbeda untuk masing-masing layanan yang diikutinya.

Perusahaan yang berkantor pusat di wilayah Skandinavia ini menyayangkan, meski banyak orang sudah membiasakan diri membuat password yang aman, tapi masih banyak juga yang mengandalkan satu password untuk semua kebutuhan mereka.

Dalam survei yang melibatkan 1500 pengguna internet di Jerman, Swedia dan Inggris, diketahui bahwa sekitar 20 persen responden mengaku bahwa mereka menggunakan password yang sama untuk semua layanan — mulai dari kartu kredit sampai online banking, dari akun e-mail sampai situs game.

<http://www.ictwatch.com/internetsehat/2010/06/21/hasil-survei-pengamanan-password-masih-disepelekan/>

6,5 Juta Password LinkedIn Dibabol. Bagaimana Password Anda?

June 7, 2012 in [a. Headline](#), [g. Privasi & Sekuriti](#) by [Tim Internet Sehat](#)



[Internet Sehat] Sebuah forum online Rusia melaporkan bahwa seorang hacker Rusia telah mencuri 6.458.020 password LinkedIn yang terenkripsi, dan memostingnya secara online tanpa username untuk membuktikan aksinya. Pihak LinkedIn sendiri sudah mengkonfirmasi bahwa sejumlah password telah berhasil dicuri, dan akan menghubungi user yang dirugikan untuk segera mengganti password mereka.

Walau username password tersebut tidak dipublikasikan oleh hacker, password itu sendiri dapat dimanfaatkan oleh pihak lain. Maka, bagi para user LinkedIn, sekuat apapun password Anda, disarankan untuk segera menggantinya.

Khawatir password LinkedIn Anda termasuk dalam 6,5 juta password yang diretas hacker Rusia itu? Firma manajemen password, LastPass, merilis sebuah tool aman yang dapat mengecek apakah password kita termasuk yang dicuri.

LastPass menjamin bahwa pihaknya tidak akan mencuri password kita. Caranya cukup sederhana, ketikkan password LinkedIn Anda di tool LastPass ([klik di sini](#)), lalu layanan ini akan melakukan pemeriksaan, dan mengirimkan hasilnya ke LastPass.Com.

<http://www.ictwatch.com/internetsehat/2012/06/07/password-linkedin-anda-dibabol-hacker/>

lampiran 6. Data hasil survei Mahasiswa Bahasa Inggris kategori umum

Nomor Responden	P												nilai awal X
	1	2	3	4	5	6	7	8	9	10	11	12	
1	0	1	0	0	1	1	1	0	0	0	0	1	5
2	1	0	0	0	1	1	1	0	0	0	1	1	6
3	0	0	1	0	1	1	1	0	0	1	1	1	7
4	0	0	1	0	1	1	0	0	0	0	0	1	4
5	1	0	1	0	1	1	1	0	0	0	1	1	7
6	1	0	1	0	1	1	0	0	1	0	0	1	6
7	1	0	0	1	1	1	0	0	0	0	1	1	6
8	1	1	1	1	1	1	1	0	0	0	1	1	9
9	0	0	1	1	1	1	0	0	0	0	1	1	6
10	0	1	1	1	1	1	0	0	1	1	1	1	9
11	0	1	1	0	1	1	1	0	1	0	0	1	7
12	1	1	0	0	1	1	1	0	0	0	0	1	6
13	1	0	0	1	1	1	0	0	0	0	1	1	6
14	1	1	1	1	1	1	1	0	0	0	1	1	9
15	0	1	1	1	1	1	1	0	1	0	1	1	9
16	0	1	0	0	0	1	1	0	0	0	1	1	5
17	1	1	1	0	0	1	1	0	1	0	1	1	8
18	1	0	1	0	1	1	1	0	0	0	1	1	7
19	1	1	1	0	1	1	1	0	0	0	1	1	8
20	1	1	0	0	1	1	1	0	0	0	1	1	7
21	1	0	1	0	1	1	1	0	0	0	1	1	7
22	0	1	1	1	1	1	1	0	0	0	0	1	7
23	0	1	1	0	0	1	1	1	0	0	0	1	6
24	1	0	0	0	1	1	1	0	0	0	0	1	5
25	1	0	1	0	1	1	0	0	0	0	1	1	6
26	1	0	1	0	1	0	1	0	1	0	1	1	7
27	1	1	1	0	1	1	1	0	1	0	1	1	9
28	1	1	1	0	1	1	1	0	1	0	0	1	8
29	1	0	1	1	1	1	0	0	0	0	0	1	6
30	1	1	1	0	1	1	1	0	1	1	0	1	9

Total nilai awal

207

Total nilai awal	207
Jumlah responden (n)	30
jumlah pertanyaan (P)	12

$$\text{nilai akhir} = (X / P) \times 100\%$$

Keterangan	X	nilai akhir (%)
nilai terendah	4	33,3
nilai tertinggi	9	75
nilai rata-rata	6,9	57,5

lampiran 7. Data hasil survey Mahasiswa Matematika kategori umum

Nomor Responden	P												nilai awal X
	1	2	3	4	5	6	7	8	9	10	11	12	
1	0	0	1	1	1	1	1	0	1	0	0	0	6
2	1	1	0	1	1	1	0	1	1	1	1	1	10
3	0	0	1	1	1	1	1	0	1	0	1	1	8
4	0	1	1	1	1	0	1	0	0	0	0	1	6
5	1	1	1	0	1	1	1	0	1	1	0	1	9
6	0	1	0	0	1	1	1	0	0	0	0	1	5
7	1	0	1	0	1	1	1	0	0	0	1	1	7
8	1	0	1	0	1	1	1	0	0	0	1	1	7
9	1	1	1	0	1	1	1	0	0	0	1	1	8
10	1	0	1	0	1	1	1	0	0	0	1	1	7
11	0	1	1	0	0	1	1	1	0	0	0	1	6
12	0	1	0	0	1	1	1	0	0	0	0	1	5
13	1	0	1	0	0	1	0	0	0	0	1	1	5
14	1	0	1	0	1	1	1	0	0	0	1	1	7
15	0	1	1	0	1	1	1	0	1	0	0	1	7
16	1	1	0	0	1	1	1	1	0	0	1	1	8
17	1	1	0	0	1	1	1	1	0	0	1	1	8
18	0	0	1	0	1	1	1	0	0	0	0	1	5
19	1	1	0	0	0	0	1	0	1	0	0	1	5
20	0	0	1	1	1	1	1	0	0	0	0	0	5
21	1	0	1	0	1	0	1	0	1	0	1	1	7
22	0	0	1	0	1	1	1	0	1	0	1	1	7
23	0	1	1	0	1	1	1	0	0	0	0	1	6
24	0	0	0	0	0	0	0	1	0	1	0	0	2
25	0	0	1	0	1	1	1	0	0	0	0	1	5
26	1	1	0	0	1	1	1	0	0	0	0	1	6
27	1	1	0	1	0	1	0	1	1	1	1	0	8
28	1	1	0	0	1	1	1	1	0	0	1	0	7
29	0	0	1	0	0	1	0	0	1	1	0	0	4
30	0	1	0	0	0	0	1	1	0	0	1	1	5
Total nilai awal												191	

Total nilai awal	191
Jumlah responden (n)	30
jumlah pertanyaan (P)	12

$$\text{nilai akhir} = (X / P) \times 100\%$$

Keterangan	X	nilai akhir (%)
nilai terendah	2	16,7
nilai tertinggi	10	83,3
nilai rata-rata	6,4	53,1

Lampiran 8. Data hasil survei Mahasiswa Pendidikan Teknik Informatika kategori umum

Nomor Responden	P												nilai awal X
	1	2	3	4	5	6	7	8	9	10	11	12	
1	1	1	0	0	1	1	1	0	0	0	1	1	7
2	0	0	1	1	1	1	1	0	1	0	1	1	8
3	1	0	0	1	0	0	1	0	0	0	0	1	4
4	1	1	0	0	1	0	1	1	0	0	1	1	7
5	0	0	0	1	0	0	1	0	0	0	0	1	3
6	1	1	0	1	1	1	1	0	1	0	0	1	8
7	1	1	1	0	0	1	1	0	0	0	0	0	5
8	0	1	0	1	1	1	1	1	0	0	1	1	8
9	1	1	0	1	1	1	1	0	1	0	1	1	9
10	1	1	0	1	1	1	1	0	0	0	1	1	8
11	0	1	0	1	1	1	1	0	0	0	1	1	7
12	1	0	0	0	1	0	0	0	1	0	0	1	4
13	1	1	0	0	1	1	1	1	0	0	1	1	8
14	0	1	1	1	1	1	0	0	0	0	1	1	7
15	0	1	1	0	1	1	1	0	1	0	1	1	8
16	1	1	1	1	1	1	1	1	0	0	1	1	10
17	1	0	1	1	1	1	0	0	0	0	0	1	6
18	1	0	1	1	1	1	1	0	0	0	1	1	8
19	1	0	0	0	1	1	1	1	1	0	1	1	8
20	0	1	1	1	1	0	1	1	0	0	0	1	7
21	1	1	1	0	1	1	1	1	0	1	1	1	10
22	1	0	1	0	1	1	1	1	0	0	0	1	7
23	1	0	1	0	1	1	0	0	0	0	1	1	6
24	1	1	1	1	1	1	1	0	0	0	0	1	8
25	1	0	1	0	1	1	1	0	0	0	0	1	6
26	1	1	1	1	1	1	1	0	0	0	0	1	8
27	1	0	1	1	1	1	0	0	0	1	1	1	8
28	0	0	1	0	1	1	1	0	0	0	1	1	6
29	1	0	0	1	1	1	1	0	0	0	0	1	6
30	1	1	1	0	1	1	1	0	1	0	1	1	9
Total nilai awal													214

Total nilai awal	214
Jumlah responden (n)	30
Jumlah pertanyaan (P)	12

$$\text{Nilai akhir} = (X / P) \times 100\%$$

Keterangan	X	Nilai akhir (%)
Nilai terendah	3	25
Nilai tertinggi	10	83,3
Nilai rata-rata	7,1	59,4

lampiran 9. Data hasil survei mahasiswa pendidikan bahasa inggris kategori siakad

No	Prodi	P						nilai awal
		15	16	17	18	19	20	
1	Pendidikan Bahasa Inggris (a)	0	1	0	0	0	1	2
2		1	1	0	1	0	1	4
3		1	1	0	1	1	1	5
4		1	1	0	0	0	1	3
5		1	1	0	1	0	1	4
6		1	1	1	1	0	1	5
7		0	1	1	0	0	1	3
8		1	1	1	1	1	1	6
9		1	1	0	0	1	0	3
10		0	1	1	1	1	1	5
11		1	1	0	0	0	1	3
12		0	1	0	1	0	1	3
13		0	1	1	1	0	1	4
14		1	1	1	1	1	1	6
15		1	1	1	1	0	1	5
16		1	0	1	0	0	1	3
17		1	0	1	1	0	1	4
18		1	1	1	1	0	0	4
19		1	1	0	1	0	1	4
20		0	1	0	1	0	1	3
21		0	1	0	0	0	1	2
22		1	1	1	0	0	1	4
23		1	0	0	1	0	1	3
24		0	1	0	0	0	1	2
25		1	1	0	1	1	1	5
26		1	1	0	1	0	1	4
27		1	1	0	0	1	1	4
28		1	1	0	0	1	1	4
29		1	1	1	0	0	1	4
30		1	1	0	0	1	1	4
							Total nilai awal	115

Total nilai awal	115
Jumlah responden (n)	30
Jumlah pertanyaan (P)	6

$$\text{nilai akhir} = (X / P) \times 100\%$$

Keterangan	X	nilai akhir (%)
nilai terendah	2	33,3
nilai tertinggi	6	100,0
nilai rata-rata	3,8	63,9

Lampiran 10. Data hasil survey mahasiswa pendidikan matematika kategori siakad

No	Prodi	P						nilai awal
		15	16	17	18	19	20	
1	Pendidikan Matematika (b)	1	1	1	1	1	1	6
2		1	1	1	1	0	1	5
3		1	1	1	1	0	1	5
4		1	1	0	0	0	1	3
5		1	1	0	0	0	1	3
6		0	1	0	0	0	1	2
7		1	1	0	1	0	1	4
8		1	1	1	1	0	0	4
9		0	1	0	1	0	1	3
10		1	1	1	0	0	1	4
11		1	1	0	0	0	1	3
12		0	1	0	0	0	1	2
13		1	1	0	0	0	1	3
14		0	1	1	0	0	1	3
15		1	0	1	0	0	1	3
16		1	1	1	1	0	1	5
17		1	1	0	1	0	0	3
18		0	1	0	1	1	1	4
19		1	0	0	0	0	1	2
20		1	0	0	0	1	0	2
21		1	1	0	1	0	1	4
22		0	1	0	1	0	1	3
23		1	1	0	0	0	1	3
24		1	0	1	1	0	0	3
25		0	1	0	1	1	1	4
26		1	0	0	1	1	0	3
27		1	0	0	1	0	1	3
28		1	1	0	1	0	1	4
29		0	1	0	1	1	0	3
30		1	1	1	0	1	1	5
Total nilai awal							104	

Total nilai awal	104
Jumlah responden (n)	30
Jumlah pertanyaan (P)	6

$$\text{nilai akhir} = (X / P) \times 100\%$$

Keterangan	X	nilai akhir (%)
nilai terendah	2	33,3
nilai tertinggi	6	100,0
nilai rata-rata	3,47	57,8

lampiran 11. Data hasil survey mahasiswa pendidikan teknik informatika kategori siakad

No	Prodi	P						nilai awal
		15	16	17	18	19	20	
1	Pendidikan Teknik Informatika (C)	1	1	0	0	0	0	2
2		0	1	1	1	0	1	4
3		1	1	1	0	0	1	4
4		1	0	0	0	0	1	2
5		1	0	1	0	1	0	3
6		1	0	1	0	0	0	2
7		1	0	0	1	0	0	2
8		1	1	0	1	0	1	4
9		0	1	1	1	0	0	3
10		1	1	1	0	0	0	3
11		1	1	1	1	0	1	5
12		1	1	0	1	0	0	3
13		1	1	0	1	0	1	4
14		1	1	1	1	0	1	5
15		1	1	0	1	0	0	3
16		1	1	1	1	0	1	5
17		1	1	0	1	0	1	4
18		1	1	0	0	0	1	3
19		1	1	1	1	0	1	5
20		1	1	1	1	0	1	5
21		1	1	1	1	0	1	5
22		1	1	0	0	0	1	3
23		0	1	0	1	0	1	3
24		1	1	1	0	0	1	4
25		1	1	0	0	0	0	2
26		0	1	1	1	0	1	4
27		1	1	1	1	1	1	6
28		1	1	1	1	1	1	6
29		1	1	1	1	1	1	6
30		1	1	0	1	1	1	5
Total nilai awal							115	

Total nilai awal	115
Jumlah responden (n)	30
Jumlah pertanyaan (P)	6

$$\text{nilai akhir} = (X / P) \times 100\%$$

Keterangan	X	nilai akhir (%)
nilai terendah	2	33,3
nilai tertinggi	6	100,0
nilai rata-rata	3,8	63,9

No	Prodi	P																		nilai awal
		1	2	3	4	5	6	7	8	9	10	11	12	15	16	17	18	19	20	X
1	Pendidikan Bahasa Inggris (a)	0	1	0	0	1	1	1	0	0	0	0	1	0	1	0	0	0	1	7
2		1	0	0	0	1	1	1	0	0	0	1	1	1	1	0	1	0	1	10
3		0	0	1	0	1	1	1	0	0	1	1	1	1	1	0	1	1	1	12
4		0	0	1	0	1	1	0	0	0	0	0	1	1	1	0	0	0	1	7
5		1	0	1	0	1	1	1	0	0	0	1	1	1	1	0	1	0	1	11
6		1	0	1	0	1	1	0	0	1	0	0	1	1	1	1	1	0	1	11
7		1	0	0	1	1	1	0	0	0	0	1	1	0	1	1	0	0	1	9
8		1	1	1	1	1	1	1	0	0	0	1	1	1	1	1	1	1	1	15
9		0	0	1	1	1	1	0	0	0	0	1	1	1	1	0	0	1	0	9
10		0	1	1	1	1	1	0	0	1	1	1	1	0	1	1	1	1	1	14
11		0	1	1	0	1	1	1	0	1	0	0	1	1	1	0	0	0	1	10
12		1	1	0	0	1	1	0	0	0	0	1	0	1	0	1	0	1	1	9
13		1	0	0	1	1	1	0	0	0	0	1	1	0	1	1	1	0	1	10
14		1	1	1	1	1	1	1	0	0	0	1	1	1	1	1	1	1	1	15
15		0	1	1	1	1	1	1	0	1	0	1	1	1	1	1	1	0	1	14
16		0	1	0	0	0	1	1	0	0	0	1	1	1	0	1	0	0	1	8
17		1	1	1	0	0	1	1	0	1	0	1	1	1	0	1	1	0	1	12
18		1	0	1	0	1	1	1	0	0	0	1	1	1	1	1	1	0	0	11
19		1	1	1	0	1	1	1	0	0	0	1	1	1	1	0	1	0	1	12
20		1	1	0	0	1	1	1	0	0	0	1	1	0	1	0	1	0	1	10
21		1	0	1	0	1	1	1	0	0	0	1	1	0	1	0	0	0	1	9
22		0	1	1	1	1	1	1	0	0	0	0	1	1	1	1	0	0	1	11
23		0	1	1	0	0	1	1	1	0	0	0	1	1	0	0	1	0	1	9
24		1	0	0	0	1	1	1	0	0	0	0	1	0	1	0	0	0	1	7
25		1	0	1	0	1	1	0	0	0	0	1	1	1	1	0	1	1	1	11
26		1	0	1	0	1	0	1	0	1	0	1	1	1	1	0	1	0	1	11
27		1	1	1	0	1	1	1	0	1	0	1	1	1	1	0	0	1	1	13
28		1	1	1	0	1	1	1	0	1	0	0	1	1	1	0	0	1	1	12
29		1	0	1	1	1	1	0	0	0	0	0	1	1	1	1	0	0	1	10
30		1	1	1	0	1	1	1	0	1	1	0	1	1	1	0	0	1	1	13
Total nilai awal																				322

Total nilai awal	322
Jumlah responden (n)	30
jumlah pertanyaan (P)	18

$$\text{nilai akhir} = (X / P) \times 100\%$$

Keterangan	X	nilai akhir (%)
nilai terendah	7	33,3
nilai tertinggi	15	71,4
nilai rata-rata	10,7	59,6

No	Prodi	P																		nilai awal
		1	2	3	4	5	6	7	8	9	10	11	12	15	16	17	18	19	20	
1	Pendidikan Matematika (b)	0	0	1	1	1	1	1	0	1	0	0	0	1	1	1	1	1	1	12
2		1	1	0	1	1	1	0	1	1	1	1	1	1	1	1	1	0	1	15
3		0	0	1	1	1	1	1	0	1	0	1	1	1	1	1	1	0	1	13
4		0	1	1	1	1	0	1	0	0	0	0	1	1	1	0	0	0	1	9
5		1	1	1	0	1	1	1	0	1	1	0	1	1	1	0	0	1	1	13
6		0	1	0	0	1	1	1	0	0	0	0	1	0	1	0	0	0	1	7
7		1	0	1	0	1	1	1	0	0	0	1	1	1	1	0	1	0	1	11
8		1	0	1	0	1	1	1	0	0	0	1	1	1	1	1	1	0	0	11
9		1	1	1	0	1	1	1	0	0	0	1	1	0	1	0	1	0	1	11
10		1	0	1	0	1	1	1	0	0	0	1	1	1	1	1	0	0	1	11
11		0	1	1	0	0	1	1	1	0	0	0	1	1	1	0	0	0	1	9
12		0	1	0	0	1	1	1	0	0	0	0	1	0	1	0	0	0	1	7
13		1	0	1	0	0	1	0	0	0	0	1	1	1	1	0	0	0	1	8
14		1	0	1	0	1	1	1	0	0	0	1	1	0	1	1	0	0	1	10
15		0	1	1	0	1	1	0	1	0	0	1	1	0	1	0	0	0	1	10
16		1	1	0	0	1	1	1	1	0	0	1	1	1	1	1	1	0	1	13
17		1	1	0	0	1	1	1	1	0	0	1	1	1	1	1	0	1	0	11
18		0	0	1	0	1	1	1	0	0	0	0	1	0	1	0	1	1	1	9
19		1	1	0	0	0	0	1	0	1	0	0	1	1	0	0	0	0	1	7
20		0	0	1	1	1	1	0	0	0	0	0	1	0	0	0	0	1	0	7
21		1	0	1	0	1	0	1	0	1	0	1	1	1	1	0	1	0	1	11
22		0	0	1	0	1	1	1	0	1	0	1	1	0	1	0	1	0	1	10
23		0	1	1	0	1	1	1	0	0	0	0	1	1	1	0	0	0	1	9
24		0	0	0	0	0	0	0	1	0	1	0	0	1	0	1	1	0	0	5
25		0	0	1	0	1	1	1	0	0	0	0	1	0	1	0	1	1	1	9
26		1	1	0	0	1	1	1	0	0	0	0	1	1	0	0	0	1	1	9
27		1	1	0	1	0	1	0	1	1	1	1	0	0	0	0	1	0	1	11
28		1	1	0	0	1	1	1	1	0	0	1	0	1	1	0	1	0	1	11
29		0	0	1	0	0	1	0	0	1	1	0	0	0	1	0	1	1	0	7
30		0	1	0	0	0	0	1	1	0	0	1	1	1	1	1	0	1	1	10

Total nilai awal 296

Total nilai awal	296
Jumlah responden (n)	30
jumlah pertanyaan (P)	18

$$\text{nilai akhir} = (X / P) \times 100\%$$

Keterangan	X	nilai akhir (%)
nilai terendah	5	23,8
nilai tertinggi	15	71,4
nilai rata-rata	9,9	54,8

No	Prodi	P																		nilai awal
		1	2	3	4	5	6	7	8	9	10	11	12	15	16	17	18	19	20	
1	Pendidikan Teknik Informatika (c)	1	1	0	0	1	1	1	0	0	0	1	1	1	1	0	0	0	0	9
2		0	0	1	1	1	1	1	0	1	0	1	1	0	1	1	1	0	1	12
3		1	0	0	1	0	0	1	0	0	0	0	1	1	1	1	0	0	1	8
4		1	1	0	0	1	0	1	1	0	0	1	1	1	0	0	0	0	1	9
5		0	0	0	1	0	0	1	0	0	0	0	1	1	0	1	0	0	0	5
6		1	1	0	1	1	1	1	0	1	0	0	1	1	0	1	0	0	0	10
7		1	1	1	0	0	1	1	0	0	0	0	1	0	0	0	1	0	0	7
8		0	1	0	1	1	1	1	1	0	0	1	1	1	1	0	1	0	1	12
9		1	1	0	1	1	1	1	0	1	0	1	1	0	1	1	1	0	0	12
10		1	1	0	1	1	1	1	0	0	0	1	1	1	1	1	0	0	0	11
11		0	1	0	1	1	1	1	0	0	0	1	1	1	1	1	1	0	1	12
12		1	0	0	0	1	0	0	0	1	0	0	1	1	1	0	1	0	0	7
13		1	1	0	0	1	1	1	1	0	0	1	1	1	1	1	0	1	0	12
14		0	1	1	1	1	0	0	0	0	0	1	1	1	1	1	1	0	1	12
15		0	1	1	0	1	1	0	1	0	1	1	1	1	1	0	1	0	0	11
16		1	1	1	1	1	1	1	1	0	0	1	1	1	1	1	1	0	1	15
17		1	0	1	1	1	1	0	0	0	0	0	1	1	1	1	0	1	0	10
18		1	0	1	1	1	1	1	0	0	0	1	1	1	1	0	0	0	1	11
19		1	0	0	0	1	1	1	1	0	0	1	1	1	1	1	1	0	1	13
20		0	1	1	1	1	0	1	1	0	0	0	1	1	1	1	1	0	1	12
21		1	1	1	0	1	1	1	0	1	1	1	1	1	1	1	1	0	1	15
22		1	0	1	0	1	1	1	1	0	0	0	1	1	1	1	0	0	0	10
23		1	0	1	0	1	1	0	0	0	0	1	1	0	1	0	1	0	1	9
24		1	1	1	1	1	1	1	0	0	0	0	1	1	1	1	0	0	1	12
25		1	0	1	0	1	1	1	0	0	0	0	1	1	1	1	0	0	0	8
26		1	1	1	1	1	1	1	0	0	0	0	1	0	1	1	1	0	1	12
27		1	0	1	1	1	1	1	0	0	0	1	1	1	1	1	1	1	1	14
28		0	0	1	0	1	1	1	0	0	0	1	1	1	1	1	1	1	1	12
29		1	0	0	1	1	1	1	0	0	0	0	1	1	1	1	1	1	1	12
30		1	1	1	0	1	1	1	0	1	0	1	1	1	1	1	0	1	1	14

Total nilai awal 328

Total nilai awal	328
Jumlah responden (n)	30
jumlah pertanyaan (P)	18

nilai akhir = (X /P) x100%

Keterangan	X	nilai akhir (%)
nilai terendah	5	23,8
nilai tertinggi	15	71,4
nilai rata-rata	10,9	60,7

No.Responden	Program Studi		
	Pend.Bahasa Inggris	Pend.Matematika	Pend.Teknik Informatika
1	38,89	66,67	50,00
2	55,56	83,33	66,67
3	66,67	72,22	44,44
4	38,89	50,00	50,00
5	61,11	72,22	27,78
6	61,11	38,89	55,56
7	50,00	61,11	38,89
8	83,33	61,11	66,67
9	50,00	61,11	66,67
10	77,78	61,11	61,11
11	55,56	50,00	66,67
12	50,00	38,89	38,89
13	55,56	44,44	66,67
14	83,33	55,56	66,67
15	77,78	55,56	61,11
16	44,44	72,22	83,33
17	66,67	61,11	55,56
18	61,11	50,00	61,11
19	66,67	38,89	72,22
20	55,56	38,89	66,67
21	50,00	61,11	83,33
22	61,11	55,56	55,56
23	50,00	50,00	50,00
24	38,89	27,78	66,67
25	61,11	50,00	44,44
26	61,11	50,00	66,67
27	72,22	61,11	77,78
28	66,67	61,11	66,67
29	55,56	38,89	66,67
30	72,22	55,56	77,78

No	NIM	Nama	Fakultas	Prodi
1	6202241013	Dika Prahastiwi C.	FBS	PBI
2	6202244086	Muhammad Afif A	FBS	PBI
3	6202244090	INDRA DWI SETIAWAN	FBS	PBI
4	6202244090	INDRA DWI	FBS	PBI
5	7202241012	rika silvia	FBS	PBI
6	7202241031	erna sulistyani	FBS	PBI
7	7202244058	MUFARROHAH	FBS	PBI
8	7202244124	anita estiningsih	FBS	PBI
9	8202244003	riana novita	FBS	PBI
10	9202241057	Isa Anggit Prasetya	FBS	PBI
11	9202241057	ISA ANGGIT PRASETYA	FBS	PBI
12	9202241057	ISA ANGGIT PRASETYA	FBS	PBI
13	9202241075	DWI ASTUTI FEBRIAWATI	FBS	PBI
14	9202241085	Aprida Nur Riya Susanti	FBS	PBI
15	9202244016	IDHA KURNIASARI DEWI	FBS	PBI
16	9202244018	DEVI ANGGRAENI P	FBS	PBI
17	9202244018	DEVI ANGGRAENI PUSPITASARI	FBS	PBI
18	9202244026	Yosep Kusuma Wibawa	FBS	PBI
19	9202244031	KHOIRUL FAJARI MARWAN	FBS	PBI
20	9202244037	Fahmi dwi Prasetyo	FBS	PBI
21	9202244043	IKA KUSRIANI	FBS	PBI
22	10202241006	M.Arif Ridho	FBS	PBI
23	10202241014	Ahmad Fauji Ridwan	FBS	PBI
24	10202241015	TOMMY SAFARSYAH	FBS	PBI
25	10202241020	TITIK SULASMI	FBS	PBI
26	10202241029	Sita Arista Wulan Sari	FBS	PBI
27	10202241029	sita arista eulan sari	FBS	PBI
28	10202241029	Sita Arista Wulan Sari	FBS	PBI
29	10202241031	Suranti Tri Astuti	FBS	PBI
30	10202241031	SURANTI TRI ASTUTI	FBS	PBI
31	10202241031	Suranti Tri Astuti	FBS	PBI
32	10202241031	suranti tri astuti	FBS	PBI
33	10202241031	suranti tri astuti	FBS	PBI
34	10202241041	esthi nawangsasi	FBS	PBI
35	10202241054	RIZQIE OKTANTI T	FBS	PBI
36	10202241947	PRITA SARI MUSTIKA DEWI	FBS	PBI
37	10202244008	Muhammad Hafidz Ridlo	FBS	PBI
38	10202244008	Muhammad Hafidz Ridlo	FBS	PBI
39	10202244009	Bayu Pratomo	FBS	PBI
40	10202244013	WAHYU SETYAJI	FBS	PBI
41	10202244013	Wahyu Setyaji	FBS	PBI
42	10202244018	akhid nur yuono	FBS	PBI
43	10202244018	Akhid Nur Yuono	FBS	PBI
44	10202244020	delia trista nanda	FBS	PBI
45	10202244023	DWI MUFIT W	FBS	PBI
46	10202244038	khoirun nisak	FBS	PBI
47	10202244058	indah istiqomah ningtias	FBS	PBI
48	10202244075	Titin Suhartini Puspita Ningrum	FBS	PBI
49	10202244075	TITIN SUHARTINI P N	FBS	PBI
50	10202244079	puri destiar indreswari	FBS	PBI

No	NIM	Nama	Fakultas	Prodi
51	10202741009	ISSHA FIRMAN SUDRAJAT	FBS	PBI
52	5301244049	IBNU SUNDARU	FMIPA	PM
53	5301244049	IBNU SUNDARU	FMIPA	PM
54	5301244075	farida nursanti	FMIPA	PM
55	5301244098	NUR RAHMADIYATI	FMIPA	PM
56	7301241019	RATNA INDRAYANI	FMIPA	PM
57	8301244043	ANDRIANI SUZANA	FMIPA	PM
58	8301244043	ANDRIANI SUZANA	FMIPA	PM
59	9301241049	EKA BUDIHARTI	FMIPA	PM
60	9301244009	UMI BAROROH	FMIPA	PM
61	9301244042	Ade Tanty eMANINGRUM	FMIPA	PM
62	10301241006	LINDA LIANA	FMIPA	PM
63	10301241006	LINDA LIANA	FMIPA	PM
64	10301241018	FINKA FITRI ASTIKA	FMIPA	PM
65	9520244044	DHIAN SEPTIYANINGRUM	FT	PTI
66	9520244044	dhian septiyaningrum	FT	PTI
67	9520244068	BAIT SYAIFUL RIJAL	FT	PTI
68	9520244070	Dian Rakhmi Asyifa	FT	PTI
69	9520244070	Dian Rakhmi Asyifa	FT	PTI
70	9520244070	Dian Rakhmi Asyifa	FT	PTI
71	9520244072	DWI WISNU W	FT	PTI
72	9520244072	dwi wisnu widiyanto	FT	PTI
73	10520241001	Wasilatun	FT	PTI
74	10520241006	muhammad azyes h	FT	PTI
75	10520241027	zumrotul akamiyati	FT	PTI
76	10520241028	annisaul mahfudhoh	FT	PTI
77	10520241028	muh miftachus salam	FT	PTI
78	10520244009	eka nurrahmah	FT	PTI
79	10520244010	damar purba pamungkas	FT	PTI
80	10520244010	DAMAR PURBA PAMUNGKAS	FT	PTI
81	10520244017	nugroh agung pribadi	FT	PTI
82	10520244017	nugroh agung pribadi	FT	PTI
83	10520244043	Fahrian Syah Azhari	FT	PTI
84	10520244043	Fahrian Syah Azhari	FT	PTI

