UNIVERSITAS
MUHAMMADIYAH
TASIKMALAYA

PEDOMAN KESELAMATAN
LABORATORIUM KOMPUTER

UMTAS	**PEDOMAN**	Nomor Dokumen : UMTAS-053-PED-003
		Tanggal Berlaku : 1 September 2019
	KESELAMATAN LABORATORIUM KOMPUTER	Revisi : R02
		Halaman : 1-16

LEMBAR PENGESAHAN

Disusun oleh :

NO.	NAMA	JABATAN	TANDA TANGAN	TANGGAL
1	Fahrurizal Muldiana, S.Kom	Kepala UPT Laboratorium Komputer		1 Agustus 2019

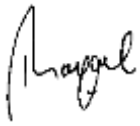
Diperiksa Oleh :

NO.	NAMA	JABATAN	TANDA TANGAN	TANGGAL
1.	Nia Restiana, M.Kep., Ns. Kep. Jiwa.	Wakil Rektor I		8 Agustus 2019
2.	Oni Sahroni, S.Sos., M.Si	Wakil Rektor 2		8 Agustus 2019

Disahkan Oleh :

NO.	NAMA	JABATAN	TANDA TANGAN	TANGGAL
1.	Dr. Ahmad Qonit AD., M.A.	Rektor		15 Agustus 2019

Dikendalikan Oleh:

NO.	NAMA	JABATAN	TANDA TANGAN	TANGGAL
1	Lilis Lismayanti, M.Kep.	Ketua Lembaga Penjaminan Mutu		15 Agustus 2019

VISI, MISI DAN TUJUAN
UNIVERSITAS MUHAMMADIYAH TASIKMALAYA

Sebagai Amal Usaha Persyarikatan Muhammadiyah, UMTAS membawa misi dan idiologi perjuangan Muhammadiyah untuk membentuk masyarakat Islam yang sebenar- benarnya dimana nilai-nilai Islam dijadikan panduan dalam pengembangan ilmu pengetahuan, teknologi, dan seni, dalam gerakan dakwah dantajdid untuk kemajuan bangsa.

UMTAS, mengemban Amanah dan mandat ini secara konsisten dan berkelanjutan, yang berbasis pada pelaksanakan Catur Dharma: bidang pendidikan, pengajaran, penelitian, pengabdian pada masyarakat, serta al-Islam dan Kemuhammadiyahan. UMTAS berkomitmen untuk menjamin keberlangsungan sistem pendidikan yang menyiapkan peserta didik menjadi cendekiawan muslim dan pemimpin bangsa yang bertakwa, berakhlak mulia, berilmu amaliah dan beramal ilmiah, yang memiliki keunggulan dalam keislaman, keilmuan, kepemimpinan, keahlian, kemandirian, dan profesionalisme.

1. VISI

Menjadi Universitas yang Unggul dan Islami dalam Pengembangan Ilmu Pengetahuan, Teknologi, dan Seni (IPTEKS) pada Tahun 2035.

2. MISI

a. Penyelenggaraan pendidikan dan pembelajaran yang unggul berdasarkan nilai-nilai Islam dan Kemuhammadiyahan dalam pengembangan IPTEKS;
b. Menyelenggarakan penelitian berdasarkan nilai-nilai Islam dan Kemuhammadiyahan yang berkontribusi pada pengembangan IPTEKS:
c. Menyelenggarakan pengabdian kepada masyarakat berlandaskan nilai-nilai Islam dan Kemuhammadiyahan untuk meningkatkan kesejahteraan masyarakat:
d. Menyelenggarakan pembinaan dengan pengembangan terhadap Sivitas Akademika berlandaskan nilai-nilai Islam dan Kemuhammadiyahan.

3. TUJUAN

a. Menghasilkan Sivitas Akademika yang mampu menguasai dan mengembangkan IPTEKS berlandaskan nilai-nilai Islam dan Kemuhammadiyahan.
b. Menghasilkan produk penelitian berlandaskan nilai-nilai Islam dan Kemuhammadiyahan yang berkontribusi pada perkembangan IPTEKS.
c. Menghasilkan produk pengabdian berlandaskan nilai-nilai Islam dan Kemuhammadiyahan untuk meningkatkan kesejahteraan masyarakat.
d. Menghasilkan Sivitas Akademika yang memiliki perilaku yang sesuai nilai-nilai Islam dan Kemuhammadiyahan.

KATA PENGANTAR

Buku keselamatan kerja laboratorium komputer dibuat untuk memberikan gambaran dan penjelasan tentang keselamatan dalam penggunaan Laboratorium, serta bahaya yang ditimbulkan dari kesalahan penggunaan laboratorium komputer di lingkungan Universitas Muhammadiyah Tasikmalaya (UMTAS).

Buku Pedoman keselamatan laboratorium komputer ini berisi prosedur pengendalian terhadap virus pada data, pengendalian bahaya kebakaran dan konsleting, serta konsleting air dan listrik pada penggunaan laboratorium komputer UMTAS.

Buku Pedoman ini diharapkan dapat bermanfaat bagi pengelola perencanaan program laboratorium komputer serta pimpinan unit kerja di lingkungan UMTAS.

Tasikmalaya, Agustus 2019
Penulis

Fahrurizal Muldiana, S.Kom.

DAFTAR ISI

KESELAMATAN KERJA DI LABORATORIUM KOMPUTER

I. Pendahuluan

Pengelolaan laboratorium yang terkait dengan keselamatan dan keamanan kerja (K3) merupakan bagian yang melekat dan tak terpisahkan dari semua kegiatan laboratorium. Orang yang bekerja di laboratorium, terutama dalam laboratorium, memiliki resiko terpapar dengan bahaya yang terkait dengan radiasi komputer, peralatan komputer dan segala kegiatan yang menyangkut tentang arus listrik.

Pada umumnya laboratorium di Perguruan Tinggi digunakan untuk melakukan aktivitas Catur Dharma Perguruan Tinggi, yaitu pendidikan; yang meliputi praktikum, penelitian mahasiswa dan demonstrasi; penelitian dosen, dan kegiatan pengabdian kepada masyarakat, dan Penguatan Al-Islam dan Kemuhammadiyahan yang bersumber pada Al Qur'an dan As Sunnah walaupun tidak menutup kemungkinan laboratorium tersebut digunakan juga sebagai laboratorium pengujian dan/atau kalibrasi. Oleh karena dalam laboratorium ini melibatkan banyak orang, maka resiko bahaya bekerja di laboratorium juga dapat melibatkan banyak orang.

Perguruan Tinggi memiliki tanggung jawab yang besar dalam menjaga keselamatan di laboratorium. Hendaknya tidak beranggapan bahwa para mahasiswa, teknisi/laboran atau dosen telah memiliki pengetahuan yang cukup tentang keamanan dan keselamatan kerja di laboratorium. Seyogjanya masalah keamanan dan keselamatan kerja di laboratorium diberikan perhatian dan penekanan yang cukup, sejalan dengan pelaksanaan kurikulum.

Perlu kiranya terus diupayakan pemberian informasi yang jelas, rinci dan menyeluruh tentang bahaya di laboratorium serta berupaya menciptakan keselamatan kerja di laboratorium. Untuk mahasiswa, informasi dapat diberikan dalam perkuliahan, sebelum praktikum dan/atau penelitian. Para dosen, teknisi/laboran atau karyawan lain dapat memperoleh informasi melalui penjelasan rutin oleh pihak yang berwenang, membaca buku, bahkan informasi tentang keamanan dan keselamatan laboratorium (*laboratory savety*) dapat dengan mudah diakses melalui *internet*.

II. Terminologi Istilah

Terminologi berikut akan digunakan dalam Panduan ini bagi menjelaskan mengenai keselamatan kerja dalam laboratorium komputer

2.1. *Server*

Server merujuk kepada komputer yang berupayaan tinggi yang berfungsi sebagai pelayan komunikasi data dalam sesuatu rangkaian jaringan komputer.

2.2. Sistem Operasi

Sistem operasi merujuk kepada *system* pengoperasian seperti Windows 95/98/7/8/10 bagi komputer *mikro* dan *NetWare*/ *Windows* NT pada *Server*.

2.3. Aplikasi

Aplikasi yang dijalankan pada laboratorium merujuk kepada aplikasi yang digunakan untuk proses belajar mengajar serta yang selalu digunakan seperti *spreadsheet* dan *word processing*, juga aplikasi yang dibangunkan bagi tujuan tertentu.

2.4. *Virus*

Virus adalah subersif program komputer yang boleh mengakibatkan kerusakan atau terhapus data ada komputer dan memungkinkan menular pada operasi komputer lain.

2.5. Data

Data adalah semua informasi yang digunakan untuk menghasilkan sebuah informasi. Dalam hal ini data terdiri dari berbagai tingkatan. Tingakatan yang tertinggi adalah data tang bersifat rasia. Dan ini memerlukan suatu penggunaan *password* dalam menjalankannya.

III. Pengendalian Data

a. Akses terhadap data hanya akan diberikan bagi user tujuan spesifik atau kepada pengguna tertentu dan hanya akan diberikan atas dasar "Perlu Mengetahui" saja atau "*read only*".
b. Data tugas atau data administrasi yang akan dikirim menggunakan disket atau media elektronik yang telah bersih dari gangguan *virus*.
c. Penggunaan (*user-ID*) dan *password* dalam hal ini keduanya digunakan untuk menjaga akses keamaman data pada tiap-tiap komputer. Dalam hal ini baik *user ID* dan *password* harus mengikuti kaedah berikut :
    i. Setiap *user* diberikan *user ID* untuk menjaga kerahasiaan data pribadi masing-masing.
    ii. *Password* tidak boleh dicatat dalam kertas. Ini digunakan untuk menjaga validitas kerahasian kunci masuk ke data per *user*.
    iii. *Password* mempunyai kombinasi sekurang-kurangnya enam aksara.
    iv. Passowrd perlu ditukar sekurang-kurangnya setiap enam bulan.
    v. *Password* yang disimpan dalam komputer akan dikode (*encrypted*).
d. Melindungi perisian sistem dari *virus*, "*Trojan horses*" dan bom jangka. Untuk memastikan komputer dan rangkaian jaringan komputer yang disediakan tidak terganggu, semua sistem dilengkapkan dengan "*virus*- screening". Aplikasi ini digunakan untuk membatasi pihak ketiga atau dari lain-lain agensi atau sumber yang sekiranya akan merusak aplikasi komputer *local* dan di rangkaian jaringan komputer;

IV. Pengendalian Terhadap *Virus* Pada Data

Virus komputer bisa diartikan sebagai suatu program komputer biasa. Tetapi memiliki perbedaan yang mendasar dengan program-program lainnya, yaitu *virus* dibuat untuk menulari program-program lainnya, mengubah, memanipulasinya bahkan sampai merusaknya. Ada yang perlu dicatat disini, *virus* hanya akan menulari apabila program pemicu atau program yang telah terinfeksi tadi dieksekusi, disinilah perbedaannya dengan "*worm*".

4.1. Beberapa Cara Penyebaran *Virus*

Virus layaknya *virus* biologi harus memiliki media untuk dapat menyebar, *virus* komputer dapat menyebar ke berbagai komputer/mesin lainnya juga melalui berbagai media, diantaranya:

4.1.1. Media *Storage* R/W

Media penyimpanan *eksternal* dapat menjadi sasaran empuk bagi *virus* untuk dijadikan media. Baik sebagai tempat menetap ataupun sebagai media penyebarannya. Media yang bias melakukan operasi R/W (*Read* dan *Write*) sangat memungkinkan untuk ditumpangi *virus* dan dijadikan sebagai media penyebaran.

4.1.2. Jaringan (LAN, WAN,dsb)

Hubungan antara beberapa komputer secara langsung sangat memungkinkan suatu *virus* ikut berpindah saat terjadi pertukaran/ pengeksekusian *file* yang mengandung *virus*.

4.1.3. WWW (*internet*)

Sangat mungkin suatu situs sengaja ditanamkan suatu "*virus*" yang akan menginfeksi komputer-komputer yang mengaksesnya.

4.1.4. *Software* yang *Freeware*, *Shareware* atau Bajakan

Banyak sekali *virus* yang sengaja ditanamkan dalam suatu program yang disebarluaskan baik secara gratis, atau *trial version*.

4.1.5. Attachment pada email, transfering *file*

Hampir semua jenis penyebaran *virus* akhir-akhir ini menggunakan email attachment dikarenakan semua pemakai jasa *internet* pastilah menggunakan email untuk berkomunikasi, *file-file* ini sengaja dibuat mencolok/menarik perhatian, bahkan seringkali memiliki *ekstensi* ganda pada penamaan *filenya*.

4.2. Komputer Terjangkit *Virus*

Komputer akan terjangkit *virus* bila :

a. Menggunakan komputer yang telah dijangkiti *virus* ke dalam jaringan;
b. Menggunakan media penyimpanan *eksternal* yang telah dijangkiti *virus*;
c. Menyalin kandungan media penyimpan *eksternal* yang telah dijangkiti *virus*.

4.3. Pencegahan *Virus* Komputer

a. "*Write protect*" pada media penyimpanan *eksternal* yang digunakan supaya penyalinan tidak dapat digunakan;
b. Jangan menyalin sembarang perisian data;
c. Senantiasa gunakan "*Scan Anti Virus*" untuk menghindari kehadiran *virus*;
d. Jauhkan program yang rusak dari *file* data ke dalam media penyimpanan *eksternal* yang berlainan;
e. Gunakan anti*virus* yang anda percayai dengan *update* terbaru. Tidak peduli apapun merknya asalkan selalu di*update*, dan auto-*protect* dinyalakan maka komputer akan terlindungi.
f. Selalu *scanning* semua media penyimpanan *eksternal* yang akan digunakan;
g. Jika terhubung langsung ke *Internet* kombinasikan anti*virus* anda dengan *Firewall*, *Anti-spamming*, dsb;
h. Selalu waspada terhadap *file-file* yang mencurigakan, contoh : *file* dengan 2 buah exstension atau *file executable* yang terlihat mencurigakan;
i. Untuk *software freeware+shareware*, ada baiknya anda mengambilnya dari situs resminya;
j. Semampunya hindari membeli barang bajakan, gunakan *software-software open source*.

4.4. Tindakan Penanggulangan *Virus* Komputer

Tindakan untuk menanggulangi, bila *virus* telah terjangkit. Bila data media *eksternal* :

a. "*Back-up*" semua data
b. Matikan *system*
c. Jalankan proses "*booting*" dengan menggunakan media *eksternal DOS* di "*writeprotected*" yang bersih dari serangan *virus*.
d. Gunakan program anti *virus* (dari media penyimpanan *eksternal*) untuk membuang *virus* pada media penyimpanan *eksternal* komputer yang dijangkiti tadi.

Bila di dalam komputer

a. Deteksi dan tentukan dimanakah kira-kira sumber *virus* tersebut apakah di media penyimpanan *eksternal*, jaringan, *email* dsb.
b. Jika ke jaringan maka ada baiknya anda mengisolasi komputer anda dulu (baik dengan melepas kabel atau *mendisable* sambungan *internet* dari *control panel*)
c. Identifikasi dan klasifikasikan jenis *virus* apa yang menyerang pc anda, dengan cara: Gejala yang timbul, misal : pesan, *file* yang *corrupt* atau hilang dsb
d. *Scan* dengan anti*virus*, jika terkena saat *auto-protect* berjalan berarti *virus definition* di dalam komputer tidak memiliki data *virus* ini, cobalah *update* secara manual atau *mendownload virus definitionnya* untuk

kemudian anda *install*. Jika *virus* tersebut memblok usaha anda untuk *mengupdate*, maka upayakan untuk menggunakan media lain (komputer) dengan anti*virus* yang memiliki *update* terbaru.

e. Bersihkan *virus* tersebut. Setelah berhasil mendeteksi dan mengenalinya maka usahakan segera untuk mencari *removal* atau cara- cara untuk memusnahkannya di situs-situs yang memberikan informasi perkembangan *virus* tersebut. Hal ini perlu dilakukan apabila anti*virus* dengan *update* terbaru anda tidak berhasil memusnahkannya.
f. Langkah terburuk. Jika semua hal diatas tidak berhasil adalah *memformat* ulang komputer
g. Tanda-tanda diserang *virus* :
   i. Program tidak dapat digunakan/dijalankan
   ii. Berlaku "*disc error*" (bila dalam media penyimpanan *eksternal*)
   iii. Kegagalan "*boot*" *system*
   iv. Sistem mengalami degradasi penggunaan.

4.5. Bagian yang diserang *virus*

Bagian komputer yang diserang *virus* antara lain :

a. Ke dalam *file* aplikasi
   i. *.EXE
   ii. *.COM
   iii. *.SYS
   iv. *.OVR
   v. dll
b. Ke dalam *"Memory";*
c. Ke ruang *"File Allocation Table (FAT)";*
d. Ke dalam *file* data
   i. *.DBF
   ii. *.WK?.
   iii. *.DOC
   iv. Dll

V. Pengendalian Bahaya Kebakaran dan Konsleting

5.1. Bahan-bahan mudah terbakar/Kebakaran

Kebakaran sebenarnya bukanlah proses yang terjadi tiba-tiba. Secara umum kebakaran terjadi jika dipenuhi unsur-unsur penyebabnya, yaitu:

i. bahan bakar,
ii. udara/oksigen, dan
iii. sumber penyalaan.

5.2. Penggolongan Api

Api dapat digolongkan menjadi lima kategori

a. Golongan A berasal dari bahan padat, misalnya batu bara, kayu, kertas, dan limbah padat. Peristiwa kebakaran yang cepat disebabkan senyawa

yang mudah menguap karena panas.

b. Golongan B berasal dari gas dan cairan yang dapat menghasilkan uap.
c. Golongan C berasal dari piranti listrik atau yang berdekatan dengan sumber atau sarana yang bermuatan atau berdaya listrik.
d. Golongan D berasal dari logam, misalnya magnesium, aluminium, titanium, natrium dan logam yang mudah teroksidasi. Temperatur pembakaran dan energi yang dihasilkan sangat tinggi dibandingkan golongan lain.
e. Golongan khusus, yaitu api yang ditimbulkan oleh senyawa oksidator atau campuran bahan bakar, misalnya senyawa atau bahan yang mudah terbakar akibat berhubungan dengan oksigen, hidrogen peroksida, dan sebagainya.

5.3. Penyebab Utama Kebakaran

Penyebab utama kebakaran antara lain :

a. Pemanasan yang tidak tepat, yaitu bila zat yang mudah terbakar dipanaskan tidak sebagaimana mestinya, tidak berhati-hati memakai penangas minyak, dan tidak memeriksa suhu minyak secara berkala.
b. Penyebaran uap dan gas-gas yang mudah terbakar, misalnya tidak melakukan pendingingan yang baik pada saat penyulingan, ada kebocoran zat, reaksi yang perlu dilakukan di ruang asam/ruang khusus, menuang sejumlah besar zat yang mudah terbakar, ceroboh/cairan mudah menguap berceceran, atau ventilasi ruang kurang baik.
c. Pecahnya wadah/botol zat yang mudah terbakar yang dipanaskan di atas logam.
d. Kelalaian penggunaan gas dan listrik, misalnya adanya kebocoran gas dan timbulnya loncatan api listrik karena hubungan singkat.
e. Personal yang kurang sadar/kurang hati-hati, misalnya merokok, membuang korek api, dan sebagainya.

5.4. Pencegahan Kebakaran

Pencegahan kebakaran antara lain :

a. Menyimpan bahan-bahan yang mudah terbakar di tempat yang aman dari sumber nyala api;
b. Bahan mudah bakar seperti kertas tidak boleh disimpan di ruang *server*;
c. Bekas sampah hendaklah diletakkan diluar ruang *server*;
d. semua alat-alat komputer perlu dimatikan apabila tidak digunakan
e. Gunakan wadah yang tepat untuk menyimpan atau menuang bahan cair yang mudah terbakar;
f. Jangan biarkan sampah (misalnya kertas yang tidak terpakai) menumpuk dan membakarnya di tempat sembarangan;
g. Semua pintu keluar bebas dari bahan-bahan yang mudah terbakar;
h. Pastikan bahwa kabel dan peralatan listrik tidak rusak;
i. Jangan memberi beban berlebih pada sirkuit listrik;
j. Buatlah peraturan dan tata tertib peringatan bahaya kebakaran dan

semua personal harus mematuhinya.

k. Usahakan tersedia peralatan pemadam kebakaran yang paling sesuai, dan pastikan penempatannya tepat dan baik, misalnya:
   i. mudah dijangkau,
   ii. mudah terlihat,
   iii. jarak yang tepat,
   iv. tidak terkunci,
   v. jangan dalam keadaan kosong.
l. Hindari kebiasaan buruk dan tidak pada tempatnya, khususnya di laboratorium; jangan merokok dan memasang alat pemanas di sekitar bahan- bahan yang mudah terbakar.

5.5. Pemadam kebakaran

Pemadam kebakaran disesuaikan dengan golongan api.

5.5.1. Air

Air digunakan untuk memadamkan api golongan A, tidak sesuai untuk golongan api lainnya.

5.5.2. CO_2

Gas CO_2 baik digunakan untuk memadamkan api golongan B dan C, khususnya untuk api yang ditimbulkan oleh listrik dan api yang melibatkan peralatan optik.

5.5.3. Bubuk Kering

Bubuk kering (biasanya natrium bikarbonat) dipakai untuk pemadaman api golongan A, B, dan C. Yang perlu diperhatikan adalah bahwa bubuk kering tersebut dapat merusak peralatan listrik dan optik.

5.5.4. Pemadam Halon

Halon (campuran karbon dan gas halogen), digunakan untuk pemadaman api golongan C, terutama untuk instalasi komputer atau instrumentasi, karena bahan tersebut tidak merusak sirkuit pada instrumen. Senyawa pemadam api logam, digunakan untuk pemadaman api golongan D. Campuran ini mengandung pasir, soda abu, grafit dan butiran plastik.

VI. Konsleting air dan listrik

Kebakaran dapat terjadi jika ada tiga unsur yaitu bahan yang mudah terbakar, oksigen dan percikan api. % lebih dari total kasus kebakaran disebabkan oleh listrik. Hal ini karena perlengkapan listrik yang digunakan tidak sesuai dengan prosedur yang benar dan standar yang ditetapkan oleh LMK (Lembaga Masalah Kelistrikan) PLN, rendahnya kualitas peralatan listrik dan kabel yang digunakan, serta intalasi yang asal-asalan dan tidak sesuai peraturan.

6.1. Pengertian Tentang Konsleting

Korseleting listrik (hubung singkat) terjadi karena adanya hubungan kawat positip dan kawat negatip yang beraliran listrik. Hal ini karena isolasi kabel rusak yang disebabkan gigitan binatang, sudah tua, mutu kabel jelek dan penampang kabel terlalu kecil yang tidak sesuai dengan beban listrik yang

mengalirinya. Kemudian di sekitar terjadinya percikan api isolasi kabel sudah mencapai titik bakar. Suhu isolasi kabel dapat mencapai titik bakar karena arus listrik yang lewat kabel jauh lebih besar dari kemampuan kabelnya. Misalnya kabel untuk ukuran 12 *ampere* dialiri arus listrik 16 *ampere*, karena kabel tersebut dipakai untuk menyambung banyak peralatan listrik akibatnya isolasi kabel menjadi panas.

Jika pada suhu isolasi yang sedang tinggi itu terjadi percikan api maka kemungkinan besar bahan isolasi akan terbakar. Percikan api terjadinya hanya satu kali karena sikring langsung bekerja memutuskan aliran, namun itu cukup untuk menyebabkan kebakaran dan kebakaran yang diakibatkan oleh percikan api akan tetap berlangsung karena karet isolasi yang sudah mencapai suhu bakar akan terbakat terus secara merembet.

Untuk bahan isolasi tertentu lelehan kabel terbakar yang jatuh tidak akan segera padam, tetapi masih menyala dengan waktu yang cukup untuk membakar, inilah salah satu kemungkinan penyebab kebakaran. Atau jika hubung singkat itu terjadi terlalu lama berati panasnya akan tinggi, kemudian dengan adanya udara yang mengandung oksigen dan ditambah lagi dengan adanya benda kering yang mudah terbakar maka menyebabkan timbulnya api. Api yang tidak bisa dikendalikan disebut kebakaran.

Hubung singkat yang terjadi ternyata bisa juga menyebabkan listrik yang mengalir semakin besar. Kemudian karena ada sikiring yang ditempatkan pada papan hubung bagi (PHB), di mana sikring itu berfungsi sebagai pemutus/pembatas arus maka kelebihan arus akan menyebabkan listrik padam sehingga keadaan menjadi aman. Dengan demikian hubung singkat bisa diamankan oleh sikring. Tapi jika sikring itu dililitkan kawat untuk mencegah agar tidak cepat putus berarti besarnya arus yang bisa memutus sikring menjadi besar akibatnya hubung singkat akan berlangsung lama hingga menimbulkan percikan api yang akan membakar isolasi akhirnya menimbulkan kebakaran. Sementara pembatas/pemutus arus itu terjadi pada saat daya listrik melebihi daya tersambung pada alat pengukur dan pembatas (APP).

APP itu sendiri merupakan batas tanggung jawab antara PLN dan pelanggan. Di mana sebelum masuk ke konsumen listrik itu melalui jaringan tegangan rendah (JTR), saluran masuk pelanggan (SMP) dan APP. Hal inilah yang merupakan tanggung jawab PLN, sedangkan setelah APP merupakan tanggung jawab pelanggan.

Dengan demikian kalau terjadi kebakaran akan diketahuilah siapa yang bertanggung jawab. Selain dari itu ada juga kebakaran karena listrik yang disebabkan karena telah terjadi kontak yang tidak sempurna yaitu kadang-kadang tersambung kadang-kadang tidak sehingga menimbulkan percikan api. Contohnya dapat dilihat pada saklar lampu pada malam hari sehingga ruangan menjadi gelap dan menimbulkan percikan api karena kontaknya sudah rusak akibatnya kotak kontak hangus terbakar. Jika kontak yang tidak sempurna dilewati oleh arus, maka lambat laun panas akan naik. Kemudian panas yang terjadi akan merambat memanaskan material sekitar termasuk

bahan isolasi. Jika bahan menjadi mudah terbakar karena suhunya tinggi maka percikan api akan sangat mudah menyebabkan kebakaran.

Kemungkinan lain penyebab kebakaran adalah keran putus tidak sempurna, sehingga aliran listrik kadang-kadang tersambung kadang-kadang tidak. Tapi hal ini sukar dideteksi karena secara pisik isolasi kabelnya masih terlihat utuh. Tapi sebenarnya di dalam isolasi ada kawat yang sudah putus tidak sempurna.

6.2. Penyebab Konsleting

Penyebab Konsleting antara lain adalah :

i. Kebakaran akibat konsleting itu bisa disebabkan oleh karena faktor human *error*.
ii. Awamnya pengguna laboratorium terhadap penggunaan listrik sehingga sering kali bertindak sembrono atau teledor dalam menggunakan listrik atau tidak mengikuti prosedur dan metode penggunaan listrik secara benar menurut aturan PLN, sehingga terjadilah kebakaran itu yang tidak sedikit kerugiannya.

6.3. Usaha Penanggulangan

Sedangkan usaha yang bisa dilakukan untuk menekan terjadinya kebakaran adalah dengan :

a. Di ruang server hendaklah dipastikan tidak berlaku limpahan air dari AC (*Air Conditioner*).
b. Suhu dan kelembapan diruang *Server* hendaklah diawasi dan dikawal
c. Meningkatkan kesadaran pengguna laboratorium komputer listrik untuk keperluan sehari-hari/proses belajar mengajar.
d. Seperti dalam membagi-bagi arus dengan menggunakan *stop* kontak bukannya dilakukan dengan semaunya tapi harus dilakukan sesuai peraturan supaya tidak menimbulkan kebakaran. Artinya jika jumlah steker yang dipasang pada suatu *stop* kontak melebihi batas maka akan menyebabkan kabel pada *stop* kontak itu menjadi panas. Jika panas itu terjadi dalam waktu yang relatif lama maka hal ini akan menyebabkan melelehnya terminal utama dan akhirnya secara pelan-pelan terjadilah hubung singkat. Kemudian dari panas itu munculah api yang akan merambat di sepanjang kabel dan jika *isolator* tidak mampu menahan panas maka akan terjadilah kebakaran.
e. Gunakanlah *stop* kontak sebagaimana mestinya. Dalam hal ini ada dua *stop* kontak; pertama *stop* kontak 200 Watt hanya digunakan untuk peralatan di bawah 500 - 1000 VA; ke dua jenis *stop* kontak tenaga yang digunakan untuk peralatan di atas 1000 VA.