Prosiding PKM-CSR, Vol. 4 (2021)
e-ISSN: 2655-3570

PENGENALAN *CYBER SECURITY* DALAM REVOUSI INDUSTRI 4.0 DAN MENYONGSONG ERA SOCIETY 5.0

Wahyu Tisno Atmojo[1], Master Edison Siregar[2], Kelly Kirsten Audrey[3]
[1]Program Studi Sistem Informasi, Universitas Pradita
[2] Program Studi Informatika, Universitas Pradita
[3] Program Studi Sistem Informasi, Universitas Pradita

wahyu.tisno@pradita.ac.id, edison.siregar@pradita.ac.id, kelly.kirsten@student.pradita.ac.id

Abstrak

Pengetahuan mengenai keamanan sistem informasi terutama keamanan dalam bertransaksi dalam internet mutlak diperlukan oleh masyarakat. Di masa pandemi seperti saat ini, transaksi melalui internet jauh meningkat. Hal tersebut disebabkan oleh adanya anjuran dari pemerintah bahwa semua kegiatan wajib dilakukan dari rumah. Dengan adanya jumlah transaksi melalui internet yang jauh meningkat, maka akan memunculkan peluang bagi orang yang tidak bertanggung jawab untuk "menyusupi" setiap transaksi yang kita lakukan. Lemahnya *password* yang kita gunakan kadangkala menjadi salah satu titik lemah kita dalam melakukan trasaksi di internet. Kadangkala kita merasa nyaman dengan penggunaan *password* sederhana yang kita gunakan. Hal tersebut tentu akan memudahkan penyusup untuk mengambil alih akun milik kita. Terdapat sebuah pendapat yang mengatakan bahwa kenyamanan berbanding terbalik dengan keamanan. Hal tersebut tentu saja merujuk kepada nyamanya kita dalam mengingat *password* transaksi akan berbading terbalik dengan tingkat keamanan akun kita. Untuk itulah diperlukan pemahaman mengenai pentingnya keamanan dalam berinternet bagi setiap lapisan masyarakat khususnya adalah peserta PkM ini. Metode pelaksanaan kegiatan ini adalah dengan bertatap muka secara langsung dengan menggunakan metode ceramah dan diskusi. Hasil kegiatan ini adalah meningkatnya pemahaman masyarakat terhadap pentingnya keamanan dalam berinternet.

Kata Kunci : Keamanan transaksi, Transaksi di Internet, Password yang lemah, Penyusup Transaksi

PENDAHULUAN

Penggunaan Internet dewasa ini menjadi kebutuhan wajib bagi setiap manusia terutama selama masa pandemi ini maka penggunaan internet untuk berbagai kebutuhan akan meningkat tajam. Hal tersebut dikarenakan semua lapisan masyarakat melakukan berbagai macam aktifitas dari rumah sehingga satu-satunya cara untuk dapat tetap bekerja adalah dengan melalui media internet. Hal tersebut juga mengikuti anjuran Pemerintah selama pandemic yang sering kita sebut dengan istilah PPKM (Pemberlakuan Pembatasan Kegiatan Kemasyarakatan) yang dikeluarkan oleh pemerintah dalam upaya mengurangi penyebaran virus covid 19. Hal tersebut tentu saja membuat semua perusahaan mewajibkan karyawanya melakukan pekerjaan dari rumah.

Dengan semua melakukan semua aktifitas melalui internet, maka muncul celah keamanan yang dapat dimanfaatkan oleh orang yang tidak bertanggung jawab untuk melakukan kejahatan melalui media interenet atau yang sering kita sebut dengan istilah kejahatan *cyber (Cyber Crime)*. *Cybercrime* dapat didefinisikan sebagai: "Pelanggaran yang dilakukan terhadap perorangan atau sekelompok individu dengan motif kriminal untuk secara sengaja menyakiti reputasi korban atau menyebabkan kerugian fisik atau mental atau kerugian kepada korban baik secara langsung maupun tidak langsung, menggunakan jaringan telekomunikasi modern seperti Internet (jaringan termasuk namun tidak terbatas pada ruang *Chat, email, notice boards* dan kelompok) dan telepon genggam (Bluetooth / SMS / MMS)" (Gani, 2018). *Cybercrime* merupakan sebiah ancaman nyata yang mau tidak mau harus kita hadapi di era industry 4.0 saat ini karena kebutuhan penggunaan internet yang sangat tinggi. Dalam aktifitas kita sehari-hari saat ini tidak bisa kita pisahkan dengan transaksi di internet, oleh karena itu pemahaman mengenai perlunya perlindungan data di internet sangat kita perlukan. Sampai dengan saat ini kita masih menganggap bahwa kejahatan dunia maya bukan merupakan sebuah ancaman, maka tidak mengherankan Ketika kita menemukan sebagaian orang yang menggunakan password akun email maupun akun social media menggunakan angka 1 sampai dengan 6. Hal tersebut tentu saja memudahkan orang lain yang tidak memiliki hak untuk masuk kedalam akun kita.

Pentingnya pemahaman masyarakat mengenai keamanan dalam berinternet atau sering disebut dengan istilah *cyber security* sangat diperlukan untuk mengetahui ancaman apa saja yang mungkin ditimbulkan dan baaimana cara mengatasai ancaman tersebut. *Cyber security* adalah kumpulan alat, kebijakan, konsep keamanan, perlindungan keamanan, pedoman, pendekatan manajemen risiko, tindakan, pelatihan, praktik terbaik, jaminan dan teknologi yang dapat digunakan untuk melindungi lingkungan *cyber* dan organisasi dan aset pengguna.(Ardiyanti, 2016). Dengan memahami ancaman yang ditimbulkan, maka masyarakat juga dituntut untuk mengetahui bagaimana cara menganmankan data-data di internet dan potensi keamanan dalam melakukan transaksi di internet dapat di minimalkan atau bahkan dihilangkan. Pengetahuan menenai ancaman-ancaman yang mungkin terjadi dalam melakukan transaksi sering disebut dengan pengetahuan internet atau biasa juga disebut dengan *Internet Knowledge*. Pengetahuan terhadap internet (*internet knowledge*) dapat mengarah pada karakteristik individu yang berkembang seiring berjalannya waktu. Perkembangan tersebut terjadi karena individu telah memiliki pengalaman dalam menyelesaikan tugas atau kegiatannya yang melalui penggunaan internet. Sebagai contoh pelaku UMKM yang memanfaatkan internet baik melalui *handphone* atau komputer yang terkoneksi online untuk memesan bahan mentah dari pemasok, menghubungi pelanggan yang melakukan pembelian produk UMKM, dan menginformasikan produk-produk terbaru UMKM kepada pelanggan atau konsumennya. Istilah pengetahuan terhadap internet adalah segala hal yang dipahami oleh orang-orang termasuk juga hal-hal yang dapat dilakukan oleh mereka dalam menggunakan internet. (Nugrahani, Ardiyanto, & Sulkhanul Umam, 2019).

Sistem keamanan informasi (*information security)* memiliki empat tujuan yang sangat mendasar adalah: a). Kerahasiaan (*Confidentiality*). Informasi pada sistem komputer terjamin kerahasiaannya, hanya dapat diakses oleh pihak-pihak yang diotorisasi, keutuhan serta konsistensi data pada sistem tersebut tetap terjaga. Sehingga upaya orang-orang yang ingin mencuri informasi tersebut akan sia-sia. b). Ketersediaan (*Availability*). Menjamin pengguna yang sah untuk selalu dapat mengakses informasi dan sumberdaya yang diotorisasi. Untuk memastikan bahwa orang-orang yang memang berhak untuk mengakses informasi yang memang menjadi haknya. c). Integritas (*Integrity*) Menjamin konsistensi dan menjamin data tersebut sesuai dengan aslinya, sehingga upaya orang lain yang berusaha merubah data akan segera dapat diketahui. d). Penggunaan yang sah (*Legitimate Use*). Menjamin kepastian bahwa

sumberdaya tidak dapat digunakan oleh orang yang tidak berhak.(Paryati, 2008)

Dengan adanya pandemic covid 19 saat ini, kenyataan yang harus kita hadapi adalah adanya peningkatan jumlah kejahatan dunia maya. Hal tersebut wajar karena hampir semua lapisan masyarakat pada saat pandemi mengunakan media interne untuk bekerja, belajar maupun melakukan berbagai macam transaksi baik perbankan maupun transaksi penjualan. Dari berita yang ditulis oleh media Indonesia, Penyebab meningkatnya kejahatan siber tersebut dikarenakan para penjahat siber memanfaatkan kecemasan yang disebabkan covid-19 untuk melakukan berbagai serangan, seperti malware pengumpulan data, ransomware, penipuan online, dan yang paling umum, yaitu phishing. Berdasarkan data dari Google, serangan phising yang memanfaatkan konten bertema covid-19 ini marak muncul sejak Januari 2020 dengan jumlah sekitar 149 ribu dan menjadi hampir dua kali lipat pada Februari, 293 ribu, dan pada Maret sudah mencapai 522 ribu. Data lain dari Trend Micro juga menunjukkan peningkatan yang serupa. Bahkan, pada Maret, jumlah *phising* menurut Trend Micro mencapai hampir sejuta kasus, dengan berbagai media penyaluran, semisal berkas dokumen, web palsu, dan yang paling banyak melalui e-mail. Data yang dapat dicuri tersebut kemudian digunakan untuk tujuan jahat yang berbeda, termasuk mengakses rekening bank dan memeras korban dalam pertukaran tebusan, seperti yang terjadi pada 2017 ketika banyak perusahaan terkena *ransomware Wannacry*. Sementara itu, di Indonesia, peningkatan serangan siber selama pandemi juga terjadi. Berdasarkan data yang dirilis Patrolisiber.id pada Januari hingga pertengahan Juni 2020, jumlah kejahatan siber yang dilaporkan ialah 2.259 kasus dengan 527 kasus selesai. *Platfrom* yang paling banyak digunakan untuk melakukan kejahatan tersebut ialah Whatsapp dengan 1.874 kasus, diikuti Instagram (1.781), dan Facebook (854).

Transformasi digital di tengah pandemi menghadirkan era baru yang dikenal dengan istilah kenormalan baru. Yaitu, era ketika segala bentuk aktivitas, seperti transaksi keuangan beralih ke digital. Keadaan ini memberikan konsekuensi logis akan meningkatnya ancaman serangan siber yang dapat menyusup ke dalam setiap aktivitas sosial tersebut melalui TIK. International Business Machines (IBM) memperlihatkan bahwa selama pandemi Covid-19, serangan siber global naik sebesar 6.000% (IBM 2020). Penjahat dunia maya terus mencari sektor serangan baru selama pandemi Covid-19. Social distancing yang dilakukan sebagai bentuk protokol kesehatan telah meningkatkan ketergantungan pada TIK, sehingga penjahat dunia maya dapat mengeksploitasi pandemi untuk memfasilitasi berbagai aktivitas kejahatannya, seperti mencoba mengambil alih platform konferensi video yang digunakan dalam rapat atau aktivitas pendidikan online, penipuan online, dan pencurian informasi data pribadi. (Wicaksana, Munandar, & Samputra, 2020).

Salah satu bentuk ancaman yang mungkin timbul dari kejahatan di internet adalah adanya manipulasi Dokumen Elektronik. Dokumen Elektronik adalah setiap Informasi Elektronik yang dibuat, diteruskan, dikirimkan, diterima, atau disimpan dalam bentuk analog, digital, elektromagnetik, optikal, atau sejenisnya, yang dapat dilihat, ditampilkan, dan/atau didengar melalui Komputer atau Sistem Elektronik, termasuk tetapi tidak terbatas pada tulisan, suara, gambar, peta, rancangan, foto atau sejenisnya, huruf, tanda, angka, Kode Akses, simbol atau perforasi yang memiliki makna atau arti atau dapat dipahami oleh orang yang mampu memahaminya. (Indonesia, 2016)

Dengan memperhatikan potensi keamanan yang ditimbulkan, maka diperlukan sosialisasi sebanyak-banyaknya kepada masayarakat untuk mengetahui potensi keamanan apa saja yang ditimbulkan dan bagaimana cara mengatasi ancaman tersebut. Maka kegiatan Pengabdian Kepada Masyarakat ini mengambil tema sosialiasi *cyber security* kepada masyarakat.

METODE

Pengabdian kepada masyarakat (PkM) ini dilaksanakan selama 1 (satu) hari yaitu pada tanggal 4 Juni 2021, akan tetapi perencanaan dan persiapan telah dilakukan jauh-jauh hari sebelum pelaksanaan kegiatan. Tahap persiapan sampai dengan tahap pelaksanaan dilakukan kurang lebih 5 (lima) hari. Tahapan kegiatan ini terdiri dari 4 tahapan yaitu tahapan persiapan yang terdiri dari survey lokasi,

persiapan narasumber, persiapan materi dan persiapan akomodasi. Tahap pelaksanaan terdiri dari pelaksanaan seminar. Tahap evaluasi dilaksanakan dengan melakukan observasi dan evaluasi kegiatan terhadap narasumber. Serta terakhir adalah tahap pembuatan laporan dimana tahap ini berisi pembuatan laporan pelaksanaan sebagai bentuk pertanggung jawaban kegiatan yang dilaksanakan baik kepada Universitas Pradita maupun kepada instansi pengundang yaitu TNI dalam kegiatan TMMD ini. Adapun jadwal kegiatan secara terperinci dapat terlihat dalam Tabel 1 berikut.

Tabel 1. Jadwal Kegiatan

No	Jenis Kegiatan	Juni		Juli			
		3	4	1	2	3	4
1	Persiapan	■					
2	Pelaksanaan		■				
3	Evaluasi		■				
4	Pembuatan Laporan		■	■			
5	Penulisan jurnal				■	■	■

Peserta dari PkM ini adalah siswa/siswi SMP dengan jumlah peserta sebanyak 20 orang dan dilaksanakan di Lembaga Pemasyarakatan (LP) Kelas 1 Kabupaten Tangerang yang beralamat di Jalan Pancing Raya, Desa Taban, Kecamatan Jambe, Kabupaten Tangerang. Kegiatan ini dilakukan secara tatap muka langsung dengan menerapkan protokol Kesehatan secara ketat dengan melibatkan 2 (dua) dosen dari program studi Sistem Informasi. PkM ini merupakan rangkaian kegiatan TNI Manunggal Membangun Desa (TMMD) yang dilaksanakan oleh TNI dengan menggandeng berbagai institusi baik institusi Pendidikan maupun instassi pemerintahan dengan berbagai tema pengabdian yang berbeda-beda. Dan Universitas Pradita mendapatkan kesempatan untuk menjadi salah satu institusi yang berkolaborasi untuk melakukan penyuluhan-penyuluhan kepada masayarakat. Kegiatan ini di koordinasi oleh TNI sepenuhnya dan dari institusi hanya menyumbangkan pembicara untuk masing-masing kegiatan.

HASIL DAN PEMBAHASAN

Perguruan Tinggi yang mengusulkan program ini adalah Universitas Pradita melalui Program Studi Sistem Informasi. Program pengabdian masyarakat di Universitas Pradita berada di bawah koordinasi Lembaga Penelitian dan Pengabdian Masyarakat (LPPM). Kegiatan pengabdian pada masyarakat merupakan kegiatan rutin yang dilakukan oleh LPPM Universitas Pradta dengan menggandeng setiap Program Studi dalam pelaksanaanya. Sebagai sebuah lembaga yang menaungi seluruh kegiatan pengabdian masyarakat, LPPM Universitas Pradita telah melakukan berberapa cara untuk meningkatkan partisipasi dosen dalam mengajukan proposal pengabdian masyarakat baik yang didanai oleh DIKTI maupun oleh Internal Universitas Pradita dan dari dana pribadi. Dalam melaksanakan Kegiatan PkM ini, di ketuai oleh Wahyu Tisno Atmojo dan menggandeng anggota tim yaitu Master Edison Siregar yang merupakan dosen tetap program studi sistem Informasi.

Seluruh tim pelaksana kegiatan ini sedang dan telah melakukan berbagai program pengabdian masyarakat serta penelitian. Kegiatan pengabdian pada masyarakat yang telah dilakukan oleh tim pengusul antara lain adalah pembuatan website di Sekolah Alam Tangerang, Pembuatan Website desa Cikolelet dan berbagai bentuk kegiatan pengabdian kepada masyarakat yang lain. Dengan adanya *track record* kegiatan Pengabdian kepada Masyarakat tersebut maka dapat disimpulkan bahwa tim pelaksana sangat layak untuk melaksanakan kegiatan pengabdian kepada masyarakat dalam bentuk pemberian materi keamanan informasi kepada siswa/siswi SMP.

Hasil yang telah dicapai dalam kegiatan PKM ini adalah sebagai berikut: 1). Memberikan pemahaman kepada siswa/siswi tentang potensi serangan yang akan timbul dalam melakukan transaksi di internet dan bagaimana menanggulanginya. 2). Memberikan pemahaman kepada siswa/siswi bagaimana membuat

password yang baik dan benar.3). Memberikan pemahaman kepada siswa/siswi tentang bagaimana mempertahankan keutuhan data dalam transaksi di internet.

Kegiatan ini dilakukan dengan memberikan ceramah secara langsung mulai dari penyajian data tentang transaksi di internet, potensi kemananan yang mungkin ditimbulkan sampai dengan ancaman-ancaman yang ada serta bagaimana mengatasai ancaman tersebut serta bagaiaman cara mengamankan data dengan membuat password yang kuat yang tidak mudah untuk diidentifikasi oleh orang lain. Pembuatan password merupakan hal mutlah yang wajib dipahami. Nyamanya dalam penggunaan password sederhana adalah ancaman yang nyata Ketika kita melakukan transaksi di internet. Adanya anggapan bahwa kenyamanan berbanding terbalik dengaan tingkat keamanan haruslah menjadi perhatian yang besar, kadangkala kita nyaman dengan menggunakan password sederhana agar kita nyaman untuk melakukan transaksi, padahal dibalik kenyamanan dalam mengingat password tersebut terdapat bahaya kemanan data yang dapat digunakan oleh orang lain untuk memasuki system kita. Peningkatan serangan *cyber* dan pelanggaran data akhir-akhir ini menjadikan pemahaman keamanan online juga semakin meningkat. Salah satu informasi yang paling rentan untuk pengguna online adalah penggunaan password. Kesalahan paling umum yang dilakukan seseorang adalah memilih kata sandi yang lemah dan umum. Penulisan password yang paling mudah ditebak adalah '123456', 'password' dan '12345678'. Pembatasan penggunaan password yang berisi konteks informasi spesifik pengguna merupakan satu tantangan tersendiri, misalnya penyertaan nama pengguna, nama situs web, nama organisasi terkait, atau terminologi terkait lainnya kurang aman saat mengotentikasi pengguna di sistem terkait.(Komalasari, 2018). Adapun foto kegiatan penyampaian materi tersaji dalam gambar 1 berikut.

Gambar 1. Penyampaian materi oleh narasumber.

Peserta kegiatan berasal dari siswa/siwi SMP di sekitar wilayah LP yang terdiri dari 20 siswa dengan didampingi oleh guru. Peserta kegiatan diundang dan dikoordinasi oleh panitia acara TMMD yang berasal dari anggota TNI yang berdinas di Komando Distrik Militer (KODIM) 0510 dalam rangka rangkaian kegiatan TMMD ke 111 TA. 2021 yang berlangsung di Desa Jambe, Kecamatan Jambe yang dilaksanakan selama 1 (satu) bulan di mulai pada tanggal 15 Juni 2021 hingga 14 Juli 2021. Tigaraksa Adapun peserta kegiatan dapat dilihat dalam gambar 2 berikut.

Gambar 2. Peserta Kegiatan PkM

Peserta kegiatan adalah siswa/siswi SMP dengan mempertimbangkan bahwa siswa/siswi merupakan salah satu pengguna aktif internet yang merupakan pengguna internet dengan data terbanyak saat ini. Dengan adanya pemahaman tentang potensi keamanan, maka diharapkan siswa/siswi tersebut akan mampu untuk memberikan pemahaman kepada masyarakat di sektarnya mengenai materi yang telah didapatkan. Berdasarkan survei Asosiasi

Penyelenggara Jasa Internet Indonesia (APJII) tahun 2019-2020, penetrasi pengguna internet di Indonesia didominasi oleh kelompok usia 15-19 tahun (91 persen), disusul oleh kelompok usia 20-24 tahun (88,5 persen). Rata-rata pengguna mengakses internet untuk membuka sosial media (51,5 persen) dan berkomunikasi (32,9 persen). (Asosiasi Penyelenggara Jasa Internet Indonesia, 2020). Maka dengan menyasar kelompok usia 15 sampai dengan 19 tahun, diharapkan mereka akan menjadi agen perubahan untuk internet Indonesia yang lebih baik.

Salah satu materi yang dibahasa dalam kegiatan ini adalah bagaimana menjaga keutuhan data yang ada di internet agar data yang dikirimkan sama persis dengan data yang diterima. Adapun dokumentasi dari pemaparan materi tentang keutuhan data terlihat dalam gambar 3 berikut.

Gambar 3. Pemaparan Materi tentang Keutuhan Data

Selain materi mengenai keutuhan data, juga dijelaskan bagaimana cara membuat password yang baik dan benar. Penggunaan password yang lemah adalah salah satu titik yang berpotensi digunakan sebagai lubang kemanan untuk dijadikan sebagai titik serangan orang yang tidak bertanggung jawab untuk dapat masuk ke system kita.Adapun pemaparan materi tentang penggunaan *password* yang baik dan benar dapat dilihat dalam gambar 4 berikut.

Gambar 4. Pemaparan Materi tentang pembuatan *password* yang baik dan benar.

Dengan memberikan pemaparan materi tersebut, diharapkan generasi muda saat ini mengetahu potensi keamanan yang dapat ditimbulkan dan bagaimana mengatasi potensi kemanan tersebut serta diharapkan setelelah mendapatkan materi, siswa/siswi tersebut dapat menyebarkan informasi kepada masyarakat di sekitar mereka sehingga kelak mereka akan menjadi agen perubahan di masyarakat.

KESIMPULAN

Dari kegiatan PKM yang telah dilaksanakan, dapat ditarik kesimpulan bahwa: 1). Materi yang diberikan oleh pemateri cukup menarik bagi peserta, dibuktikan dengan banyaknya pertanyaan yang diberikan oleh peserta kepada narasumber. 2). Materi yang diberikan dapat membantu siswa/siswi memahami potensi-potensi serangan yang dilakukan oleh orang lain terhadap akun social media sehingga siswa/siswi akan dapat melakukan pengamanan terhadap data setelah mengetahui apa saja ancaman tersebut.

.

UCAPAN TERIMAKASIH

Ucapan terima kasih sebesar-besarnya diberikan kepada: 1). Komando Distrik Militer (KODIM) 0510 yang telah memberikan kesempatan kepada Universitas Pradita untuk menjadi salah satu institusi yang berperan dalam kegiatan TMMD. 2). LPPM Universitas Pradita yang telah

memberikan kesempatan kepada Program Studi Sistem Informasi untuk melakukan pengabdian kepada masyarakat.

.

REFERENSI

Ardiyanti, H. (2016). *Cyber-Security Dan Tantangan Pengembangannya Di Indonesia*. 95–110.

Asosiasi Penyelenggara Jasa Internet Indonesia. (2020). Laporan Survei Internet APJII 2019 – 2020. *Asosiasi Penyelenggara Jasa Internet Indonesia*, *2020*, 1–146. Retrieved from https://apjii.or.id/survei

Gani, A. G. (2018). Cybercrime (Kejahatan Berbasis Komputer). *Jurnal Sistem Informasi*, *5*(1), 16–29. Retrieved from http://journal.universitassuryadarma.ac.id/index.php/jsi/article/view/18

Indonesia, R. (2016). The Amendment of 11th Law of 2008 on Information and Electronic Transaction. *Journal of Chemical Information and Modeling*, *53*(9), 287.

Komalasari, R. (2018). Kesadaran Akan Keamanan Penggunaan Username Dan Password. *Tematik*, *5*(2), 56–67. https://doi.org/10.38204/tematik.v5i2.265

Nugrahani, T. S., Ardiyanto, F., & Sulkhanul Umam. (2019). *Manajemen Dewantara 1(2),25-37*. *3*(2), 203–213.

Paryati. (2008). Keamanan Sistem Informasi. *Seminar Nasional Informatika 2008 (SemnasIF 2008) UPN "Veteran" Yogyakarta, 24 Mei 2008*, *2008*(semnasIF), 379–386.

Wicaksana, R. H., Munandar, A. I., & Samputra, P. L. (2020). Studi Kebijakan Perlindungan Data Pribadi dengan Narrative Policy Framework: Kasus Serangan Siber Selama Pandemi COVID-19 A Narrative Policy …. *Jurnal IPTEK-KOM …*, *22*(2), 143–158. Retrieved from https://jurnal.kominfo.go.id/index.php/iptekkom/article/download/3505/1477

.