
Pelatihan Penggunaan Tool Manajemen Pemfilteran Konten Memblokir Akses Ke Web Dengan Cleanbrowsing

Helmi Kurniawan¹, Yusfrizal², Edy Victor Haryanto³, Muhammad Sadikin⁴

^{1,2,3,4}Universitas Potensi Utama

Jl. K.L. Yos Sudarso KM 6,5 No.3A Tanjung Mulia Medan

e-mail: ¹helmikurniawan77@gmail.com

Riwayat Artikel:

Dikirim : 09 Agustus 2023

Direvisi : 15 Agustus 2023

Diterima : 23 Agustus 2023

Abstrak: Sekolah merupakan tempat pembelajaran yang menggunakan internet, dimana guru dan siswa menggunakan internet untuk mencari bahan ajar atau mengunjungi situs tertentu, namun dalam mengunjungi situs web tersebut memiliki konten yang tidak pantas diakses siswa/i. Untuk dapat memfilter situs yang dibolehkan diakses atau tidak maka dibutuhkan sistem pemfilteran situs. Pemfilteran konten dapat digunakan untuk menyaring akses ke situs web atau email tertentu yang dianggap tidak aman. Langkah keamanan yang paling umum adalah ketika sekolah memfilter dan memblokir akses pengguna (siswa/i) ke platform media sosial tertentu. Adapun Metode pengabdian ini melatih guru dan siswa SMK PAB 5 Klambir lima dalam Penerapan pemfilteran konten dengan CleanBrowsing. Peserta kegiatan guru dan siswa berjumlah 25 orang, dimana sebagian besar guru dan siswa yaitu 60% telah berhasil mensetting cleanbrowsing, blok internet option dan membuat file profile bat. Peserta guru dan siswa yang mengikuti 100% merasa senang. Nilai hasil diperoleh dari angket yang diisi guru dan siswa.

Kata Kunci:

Pemfilteran Konten, Situs, Blokir, CleanBrowsing

Pendahuluan

Penggunaan Internet telah meningkat secara dramatis, karena kita semakin dekat dengan digitalisasi lengkap dari rutinitas sehari-hari kita. Semakin banyak orang menggunakan Internet, peretas dan penyerang semakin aktif, dan sistem jaringan kita menjadi lebih rentan terhadap serangan dunia maya. Pada dasarnya, keamanan jaringan diperlukan untuk menjalankan dua tugas: yang pertama adalah melindungi informasi dari akses yang tidak diinginkan, dan yang lainnya adalah mengamankan data yang disimpan di titik akhir seperti PC atau laptop tidak hanya untuk jaringan individual tetapi juga untuk jaringan bersama atau publik. jaringan domain. Penyaringan paket mengendalikan akses ke jaringan dengan memeriksa paket masuk dan keluar dan membiarkan mereka bergerak atau menghentikannya tergantung pada alamat IP sumber dan tujuan. Penyaringan paket adalah salah satu teknik untuk menerapkan firewall keamanan. Penyaringan paket adalah alat dan metode yang merupakan struktur bangunan mendasar dari keamanan jaringan. Ini adalah alat yang merupakan instrumen yang membantu dalam mencapai suatu fungsi. Ini adalah teknik karena merupakan pendekatan untuk menyelesaikan tugas. Pemfilteran konten adalah penggunaan program untuk menyaring

dan mengontrol akses konten melalui firewall mereka. Singkatnya, firewall filter konten bekerja untuk memblokir akses ke informasi yang dapat dianggap jahat atau berbahaya.

Di sekolah, firewall pemfilteran konten dapat digunakan untuk menyaring dan mengecualikan akses ke situs web atau email tertentu yang dianggap tidak aman, mencurigakan, atau tidak menyenangkan. Langkah keamanan yang paling umum adalah ketika sekolah memfilter dan memblokir akses pengguna (siswa/i) ke platform media sosial tertentu. Tapi itu bekerja di luar memblokir situs tertentu. sekolah juga dapat memblokir kata kunci dan istilah pencarian. Sistem pemfilteran konten jaringan membantu memastikan bahwa organisasi secara otomatis memperkuat keamanan mereka dan secara aktif menegakkan kebijakan perusahaan mereka seputar manajemen sistem informasi. Premis pemfilteran konten adalah memilih apa yang ada dan tidak dapat diakses di internet pengguna. Pelaksana sangat menekankan pada konten dewasa seperti pornografi dan memerangi kecanduan online terhadap perjudian, game, belanja online, dan sejumlah tantangan lain di era digital baru. Pemfilteran konten memungkinkan untuk memilih apa yang diizinkan untuk dilihat di jaringan rumah. Ini berlaku untuk semua perangkat yang terhubung ke router perangkat, tetapi juga dapat dikonfigurasi secara individual di perangkat. Dengan pemfilteran konten, orang tua dapat memilih apa yang ingin dan tidak ingin mereka izinkan di Wi-Fi rumah mereka. Ini meluas tidak hanya untuk keluarga, tetapi untuk siapa pun yang mengunjungi rumah.

Berdasarkan penjelasan sebelumnya maka sudah tepatlah penerapan pemfilteran konten dalam proses belajar mengajar di lembaga pendidikan dan di rumah dengan aplikasi CleanBrowsing. Penerapan pemfilteran konten dengan CleanBrowsing yang dimaksud ini memblokir semua konten yang tidak pantas untuk siswa-siswi di sekolah. Misalnya, pemfilteran konten memblokir akses ke semua situs web dewasa, proksi, situs web konten campuran, situs phishing, dan menyetel mode aman untuk Youtube, Bing, dan Google. Aplikasi CleanBrowsing untuk Windows menampilkan tiga opsi – *custom filters*, *free family filters* and *free adult filter*. Kita dapat mengklik tombol di sebelah masing-masing filter untuk mengaktifkannya. Untuk mengaktifkan *custom filters*, maka harus membuat akun dengan *CleanBrowsing* dan mengatur filter di situs web perangkat siswa-siswa, lalu memposting tautan di aplikasi. CleanBrowsing memblokir DNS yang berisi situs web dewasa. Aplikasi ini adalah cara yang aman untuk menelusuri situs web tanpa menemukan konten yang tidak pantas di internet. Namun, aplikasi CleanBrowsing tidak tersedia di Google Play Store. Untuk mendapatkannya dengan membuka situs resmi CleanBrowsing dan mendownloadnya untuk versi gratis dan berbayar.

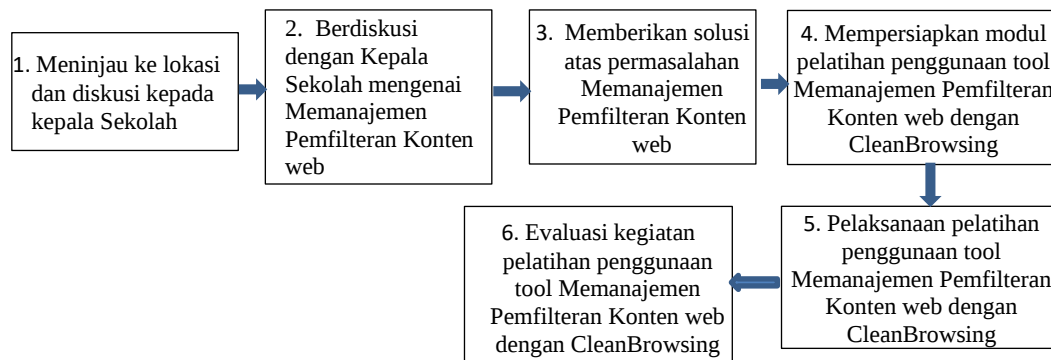
Dengan adanya pemfilteran konten dalam proses belajar mengajar yang sekarang ini, maka perlu dilakukan sebagai pengetahuan dan wawasan tentang penggunaan tool *CleanBrowsing* yang mendukung untuk sistem keamanan dalam jaringan internet dalam pembelajaran.

Berdasarkan uraian latar belakang di atas maka rumusan masalah pada kegiatan ini adalah:

- a. Bagaimana kondisi tingkat pemahaman IT siswa – siswa SMK PAB 5 Klambir Lima dalam manajemen pemfilteran konten memblokir akses ke semua situs web dengan CleanBrowsing?
- b. Bagaimana sistem keamanan yang digunakan pada jaringan komputer di SMK PAB 5 Klambir Lima?
- c. Bagaimana Penggunaan media CleanBrowsing yang digunakan sebagai media manajemen pemfilteran konten memblokir akses ke semua situs web?

Metode

Metode kegiatan abdimas dengan judul "Pelatihan Penggunaan Tool Manajemen pemfilteran konten memblokir akses ke web dengan CleanBrowsing " Hal ini dilakukan dengan tujuan agar guru dapat memahami materi pelatihan dengan baik dan dapat mempraktikkannya. Secara lengkap langkah-langkah pelaksanaan kegiatan pengabdian masyarakat terlihat pada Gambar 1.



Gambar 1. Tahapan-tahapan Pengabdian kepada Masyarakat

Tahapan pelaksanaan kegiatan pengabdian kepada masyarakat di SMK PAB 5 Klambir Lima yaitu:

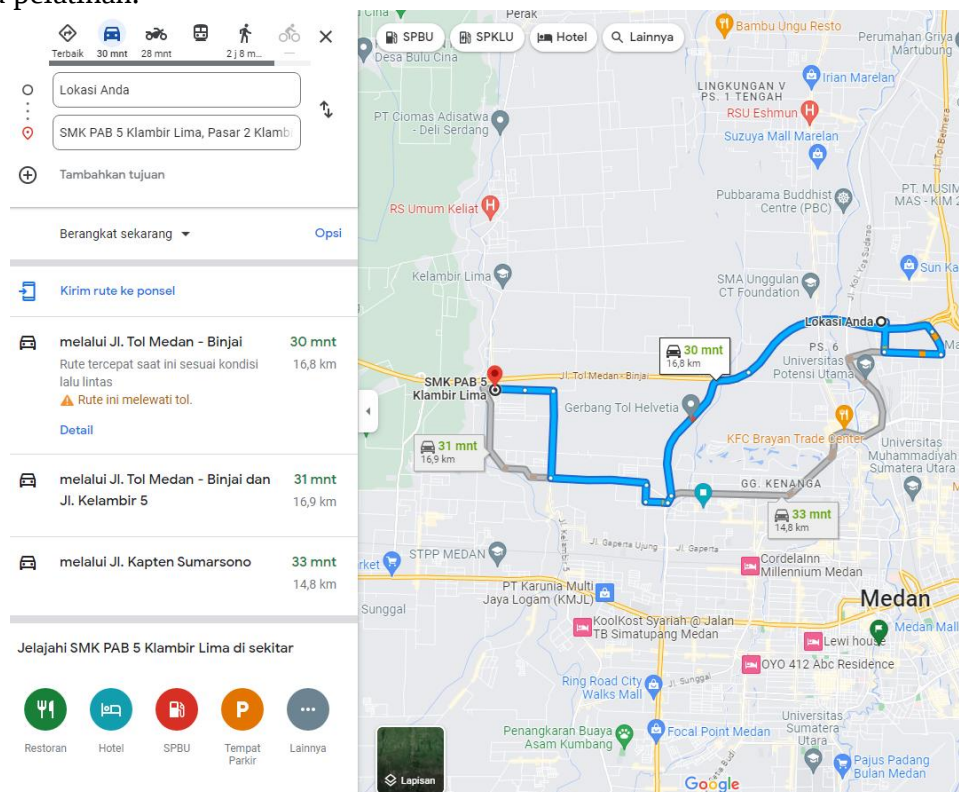
1. Menentukan dan menemukan tempat pengabdian kepada masyarakat (PkM) dengan mendapatkan persetujuan pihak sekolah SMK PAB 5 Klambir Lima perihal kegiatan PkM.
2. Melaksanakan Pertemuan dengan pihak sekolah mengenai bagaimana manajemen pemfilteran konten web yang diakses siswa oleh guru, terutama dalam menggunakan internet pada perangkatnya di SMK PAB 5 Klambir Lima.
3. Tim Pelaksana melakukan pelatihan manajemen pemfilteran konten web yang diakses siswa kepada guru-guru di SMK PAB 5 Klambir Lima berupa pelatihan penggunaan tool Penggunaan Tool Manajemen pemfilteran konten memblokir akses ke web dengan CleanBrowsing di internet.
4. Tim pelaksana mempersiapkan dan membuat modul pelatihan penggunaan tool Penggunaan Tool Manajemen pemfilteran konten memblokir akses ke web dengan CleanBrowsing serta bahan presentasi untuk disampaikan ke peserta pelatihan yaitu guru dan siswa.
5. Pada pelaksanaan pelatihan tim pelaksana mempresetansikan dan memberikan pendampingan kepada guru-guru dalam menggunakan dengan cleanbrowsing dari Internet untuk menyapaikan materi ajar secara online kepada siswa-siswa dalam Manajemen pemfilteran konten memblokir akses ke web dengan CleanBrowsing.
6. Setelah kegiatan selesai tim pelaksana Abdimas akan memberikan angket kepada guru-guru yang menjadi peserta pelatihan penggunaan tool Manajemen pemfilteran konten memblokir akses ke web dengan CleanBrowsing sebagai evaluasi hasil kegiatan yang telah dilaksanakan.

Materi pelatihan penggunaan tool manajemen pemfilteran konten web dengan CleanBrowsing meliputi:

1. Memberikan penjelasan mengenai Manajemen pemfilteran konten memblokir dengan CleanBrowsing di internet

2. Membuka CleanBrowsing melalui perangkat masing-masing
3. Membuat Manajemen pemfilteran konten memblokir dengan CleanBrowsing di internet pada web browser
4. Membagikan link CleanBrowsing yang dibuka oleh guru kepada whatsapp siswa-siswi
5. Menerangkan secara langsung melalui CleanBrowsing dengan family security.
6. Melakukan pembahasan Manajemen pemfilteran konten dan pemberian soal latihan kepada guru dan siswa secara online.

Kegiatan Pelaksanaan kegiatan pengabdian berlangsung pada hari Selasa, 19 Januari 2023 dari jam 09.30 s.d 17.00 WIB, dengan dihadiri 25 orang peserta di SMK PAB 5 Klambir Lima. Kegiatan berupa penyampaian materi dan praktek Manajemen pemfilteran konten memblokir akses ke web dengan CleanBrowsing. Setiap peserta melakukan praktek langsung setelah diberikan penjelasan oleh tim instruktur. Keberadaan SMK PAB 5 Klambir Lima yang terletak sekitar 16,5 km dari Universitas Potensi Utama. Keberhasilan kegiatan pengabdian kepada masyarakat di SMK PAB 5 Klambir Lima ukur melalui pemberian angket yang ke peserta pelatihan.



Gambar 2. Jarak Lokasi Universitas Potensi Utama ke SMK PAB 5 Klambir Lima

HASIL DAN PEMBAHASAN

Kegiatan pengabdian pada masyarakat ini dihadiri guru dan kepala SMK PAB 5 Klambir Lima yang memberikan fasilitas yang dibutuhkan dalam kegiatan yang dilaksanakan. Selain itu, kegiatan ini disambut dan dibuka oleh kepala sekolah SMK PAB 5 Klambir Lima dan ketua pelaksana Abdimas seperti terlihat pada Gambar 3.

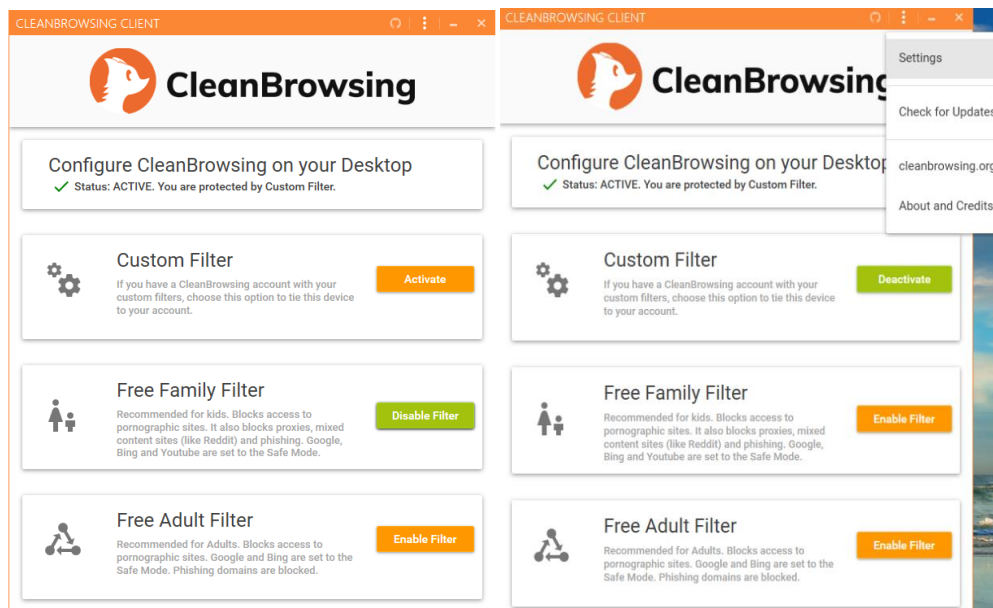


Gambar 3. Pelaksanaan Pengabdian kepada Masyarakat di SMK PAB 5 Klambir Lima

Adapun materi yang disampaikan pada kegiatan pengabdian kepada masyarakat terhadap guru dan siswa SMK PAB 5 Klambir Lima dalam pelatihan Memanajemen pemfilteran konten memblokir akses ke web dengan CleanBrowsing. CleanBrowsing adalah layanan pemfilteran konten berbasis DNS yang menyediakan cara bagi pengguna internet untuk memblokir akses ke jenis konten tertentu. Itu dirancang untuk menawarkan pengalaman menjelajah yang lebih aman dengan memfilter konten yang berpotensi berbahaya atau tidak pantas. CleanBrowsing beroperasi dengan bertindak sebagai perantara antara perangkat pengguna dan situs web yang akan dikunjungi. Saat akan mengonfigurasi perangkat atau jaringan untuk menggunakan server DNS CleanBrowsing, semua permintaan DNS pengguna (yang menerjemahkan nama domain seperti "www.example.com" menjadi alamat IP) dikirim melalui server CleanBrowsing. Aplikasi akan menganalisis permintaan dan memfilter konten apa pun yang termasuk dalam kategori yang telah di pilih untuk diblokir. Ada berbagai profil pemfilteran yang tersedia dengan CleanBrowsing, seperti Keluarga, Dewasa, dan Keamanan. Profil Keluarga dirancang untuk rumah tangga dengan anak-anak, memblokir akses ke konten dewasa, sedangkan profil Dewasa untuk orang dewasa yang ingin membatasi akses ke kategori tertentu. Profil Keamanan berfokus pada pemblokiran situs web jahat atau porno, judi dan perlindungan dari serangan phishing. Untuk menggunakan CleanBrowsing, pengguna perlu

mengonfigurasi perangkat atau jaringannya untuk menggunakan server DNS pengguna.

CleanBrowsing menawarkan layanan pemfilteran konten gratis. Layanan ini dapat dimanfaatkan dengan digunakan oleh setiap individu dan pemerintah kecil dan organisasi nirlaba tanpa biaya. Filter konten gratis ini menyediakan tiga filter berbeda yang dapat dikonfigurasi dengan cepat di lingkungan perangkat masing-masing. Layanan ini tidak menyertakan akun dengan CleanBrowsing, tidak memberi visibilitas tentang apa yang akan telusuri, dan disediakan apa adanya.



Gambar 4. Tampilan CleanBrowsing Pengguna dan Setting CleanBrowsing

Langkah 1 – Pilih perangkat Pengguna

Pilih perangkat yang ingin dilindungi. Temukan halaman Pengaturan Jaringan tempat server DNS dikonfigurasi (juga dikenal sebagai Server nama). Biasanya di bawah pengaturan Jaringan, Koneksi, WAN atau Wifi. Jika memerlukan detail lebih lanjut, CleanBrowsing memiliki panduan langkah demi langkah untuk perangkat berikut (CleanBrowsing menyertakan Aplikasi untuk beberapa di antaranya untuk menyederhanakan kebutuhan sistem perangkat): Mac, Linux, iPhone, Windows, Android.

Langkah 2 – Ubah Pengaturan DNS Pengguna

CleanBrowsing menawarkan 3 filter gratis (*Security, Adult and Family*), masing-masing dengan tingkat kontrol yang berbeda.

1. **Filter Family** : Memblokir akses ke semua situs dewasa, pornografi, dan eksplisit. Itu juga memblokir proxy dan domain VPN yang digunakan untuk mem-bypass filter. Situs konten campuran (seperti Reddit) juga diblokir. Google, Bing, dan Youtube diatur ke Safe Mode. Domain berbahaya dan Phishing diblokir. (mis., family -filter -dns.cleanbrowsing.org, 198.153.192.60)
2. **Filter Adult** : Memblokir akses ke semua situs dewasa, pornografi, dan eksplisit. Itu tidak memblokir proxy atau VPN, atau situs konten campuran. Situs seperti Reddit diizinkan. Google dan Bing diatur ke Safe Mode. Domain berbahaya dan Phishing diblokir. (misalnya, dewasa-filter-dns.cleanbrowsing.org, 198.153.192.50)

3. **Security Filter** : Memblokir akses ke phishing, spam, malware, dan domain berbahaya. Basis data domain berbahaya kami diperbarui setiap jam dan dianggap sebagai salah satu yang terbaik di industri. Perhatikan bahwa itu tidak memblokir konten dewasa. (mis., security-filter-dns.cleanbrowsing.org, 198.153.192.40)

Langkah 3 – Selesai

Jika ingin melindungi seluruh perangkat pengguna, pengguna dapat mengonfigurasi router pengguna untuk menggunakan server DNS yang sama yang disediakan pada langkah #2.



Gambar 4. Block Internet Options (BIO) dan Akses Pusat Jaringan di Windows

CleanBrowsing memberikan instruksi terperinci di situs webnya untuk berbagai platform. Konfigurasi CleanBrowsing DNS untuk Pengguna Berbeda di Windows CleanBrowsing memberikan layanan pemfilteran konten berbasis DNS. Konfigurasi, bagaimanapun, seringkali bergantung pada pengguna layanan. Ini akan menunjukkan cara mengkonfigurasi DNS sesuai dengan pengguna tertentu. Ini akan dilakukan di tingkat perangkat, tetapi juga dapat direplikasi oleh administrator jaringan menggunakan Direktori Aktif dan GPO.[2][8][9] Untuk contoh kami menggunakan yang berikut ini:

1. Orang Tua : Ini akan menjadi pengguna administratif. Pengguna ini memiliki hak administratif penuh atas mesin dan tidak dapat membatasi pengguna administrator pada Windows.
2. Anak : Ini akan menjadi pengguna standar. Mereka dapat mengakses mesin, tetapi tidak memiliki hak administratif. Ini berarti admin dapat membatasi apa yang dapat dan tidak dapat dilakukan oleh pengguna.

Langkah-langkah spesifik untuk konfigurasi bergantung pada perangkat atau sistem operasi yang digunakan.

Langkah 1: Membuat Environment Variable

Environment Variable adalah pintasan yang memungkinkan pengguna menavigasi dengan cepat ke lokasi tertentu di mesin pengguna. Jalur Variabel Env : %script% C:\Windows\System32\Repl\Imports\Scripts. membuat direktori berikut: Repl\Imports\Scripts. Selanjutnya memilih lokasi ini berdasarkan rekomendasi Window tentang tempat skrip sistem seharusnya berada. (ref: <https://docs.microsoft.com/en-us/troubleshoot/windows-server/user-profiles-and-logon/assign-logon-script-profile-local->

user)

Langkah 2: Membuat Window Script untuk setiap Profile / DNS

Untuk membuatnya berfungsi, perlu membuat dua file Windows BAT. Setiap file BAT akan berisi instruksi khusus sesuai dengan profil yang digunakan. Setiap file bat masing-masing harus berisi informasi berikut:

A. Profil Orang Tua

:: Set Adult profile network settings

```
netsh interface ipv4 set dns "Wi-Fi" static 185.228.168.10 primary
```

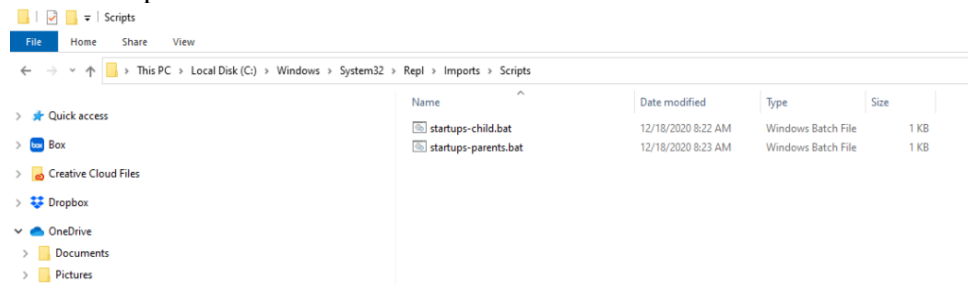
```
netsh interface ipv4 add dns "Wi-Fi" 185.228.169.11 index=2
```

B. Profil Anak

@echo off :: Set Child profile network settings

```
netsh interface ipv4 set dns "Wi-Fi" static 185.228.168.168 primary
```

```
netsh interface ipv4 add dns "Wi-Fi" 185.228.169.169 index=2
```



Gambar 5. File Profile parent.bat dan child.bat

Langkah 3: Buat Aturan untuk setiap Profil

Ada beberapa cara berbeda yang dapat dicoba. Pendekatan yang paling umum adalah memanggil skrip ini di "log on". Sayangnya, ada beberapa masalah User Access Control (UAC) dengan Windows yang ditemukan membuat ini tidak dapat diandalkan pada perangkat individual (tidak berlaku untuk pengguna AD / GPO). Untuk perorangan, disarankan untuk menggunakan fitur task scheduler sebagai solusi yang paling efektif.

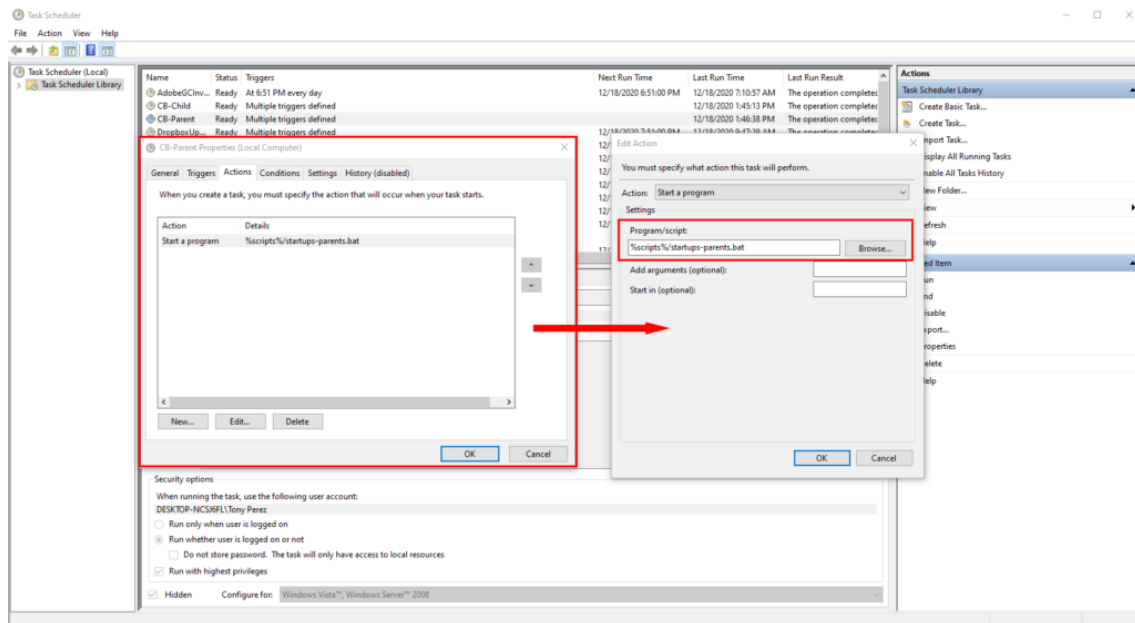
Buka task scheduler dengan mencarinya di windows. Opsi buat task akan membuka dialog baru.

1. Beri nama, untuk contoh ini kami menggunakan FP-Parent;
2. Di bawah Opsi Keamanan, pilih pengguna mana yang akan menjalankan skrip. Pastikan pengguna ini adalah administrator.
3. Pilih opsi yang bertuliskan "Run with highest privileges" ini sangat penting ketika dijalankan pada akun pengguna.

Langkah 4: Buat Task untuk Profil Anak

Setelah membuat Task untuk Profil Orang Tua, ulangi langkah-langkah untuk membuat tugas untuk Anak. Hal-hal penting yang harus diingat bersama anak adalah:

1. Gunakan file bat yang benar;
2. Pastikan Anda memilih pengguna yang benar di trigger;
3. Pastikan memilih pengguna yang tepat di pengaturan untuk menjalankan skrip;



Gambar 6. Tampilan menjalankan file Program Profile

Tabel 1. Tertib Acara Kegiatan Pelaksanaan Pengabdian Masyarakat

No	Waktu	Materi	Bentuk Kegiatan	Hasil
1	09.00-09.10 WIB	Melakukan Perkenalan Kepada Peserta	Ceramah	Peserta Mengenal Pemateri
2	09.10-09.25 WIB	Menjelaskan Bimtek Keamanan jaringan komputer	Ceramah, diskusi	Peserta Mengetahui Bimtek Manajemen pemfilteran konten
3	09.25-09.40 WIB	Mengatur konfigurasi jaringan internet	Ceramah, Praktek	Peserta mengkoneksikan laptop ke internet
4	09.40-11.10 WIB	Menjelaskan situs terpercaya untuk dapat diakses	Ceramah, Praktek, diskusi	Peserta Mengetahui situs terpercaya untuk bahan ajar dan pengetahuan
5	11.10-12.00 WIB	Soal Latihan download software Manajemen pemfilteran konten	Ceramah, Praktek, diskusi	Peserta dapat download software Manajemen pemfilteran konten
6	13.30-14.00 WIB	Menjelaskan situs yang boleh diakses dan tidak	Ceramah, Praktek, diskusi	Peserta Mengetahui situs boleh diakses dan tidak dari pemfilteran konten
7	14.00-14.30 WIB	Soal Latihan situs yang boleh diakses dan tidak	Ceramah, Praktek, diskusi	Peserta dapat menentukan situs yang boleh diakses dan tidak
8	14.30-15.00 WIB	Menjelaskan Manajemen pemfilteran konten dengan CleanBrowsing	Ceramah, Praktek, diskusi	Peserta Mengetahui Cara manajemen pemfilteran konten dengan CleanBrowsing
9	15.00-15.30 WIB	Soal Latihan media pemfilteran konten dengan CleanBrowsing	Ceramah, Praktek, diskusi	Peserta dapat pemfilteran konten dengan CleanBrowsing
10	15.30-16.00 WIB	Penutup	Ceramah	Peserta dapat pemfilteran konten dengan CleanBrowsing

25 guru dan siswa yang telah mengikuti pelatihan, menunjukkan bahwa 15 guru dan siswa

diantaranya sudah dapat menggunakan internet dan dapat setting Cleanbrowsing. 2 guru masih membutuhkan pendampingan dalam menggunakan internet dan akses blokir konten. Perbandingan kondisi peserta guru dan siswa sebelum dan setelah mengikuti kegiatan pelatihan pengabdian kepada masyarakat dapat dilihat pada tabel 2:

Tabel 2. Tingkat Pemahaman Materi Pelatihan Sebelum Setelah Pelatihan

Kondisi	Dapat berinternet dan tanpa blok	Dapat setting Cleanbrowsing	Perlu Pendampingan
Sebelum Kegiatan	20	0	5
Setelah Kegiatan	23	15	2

Berdasarkan Tabel 2 di atas menunjukkan bahwa pelatihan yang telah dilaksanakan sudah dapat membantu memberikan ketrampilan pada guru dan siswa berikut hasil evaluasi setelah pelaksanaan kegiatan adalah:

- Meningkatnya pengetahuan dan pemahaman guru dan siswa dalam keamanan dalam berinternet dan manajemen pemfilteran konten memblokir akses ke web dengan CleanBrowsing
- Meningkatnya keterampilan guru dan siswa dalam menggunakan fasilitas internet sebagai manajemen pemfilteran konten memblokir akses ke web dengan aman
- Meningkatnya keterampilan guru dan siswa pengetahuan dan pemahaman guru dan siswa dalam manajemen pemfilteran konten memblokir akses ke web melalui aplikasi teknologi.

Kesimpulan

Berdasarkan dari hasil kegiatan pengabdian kepada masyarakat ini dapat diberikan kesimpulan diantaranya:

- Peserta guru dan siswa yang ikut kegiatan berjumlah 25 peserta dan 15 peserta telah mampu manajemen pemfilteran konten memblokir akses ke web melalui CleanBrowsing.
- Berdasarkan angket yang di berikan ke guru dan siswa untuk di isi hasilnya menunjukkan bahwa 60% menyatakan paham untuk setting pemfilteran konten memblokir akses ke web melalui CleanBrowsing dan membedakan sumber situs yang aman atau tidak.
- Berdasarkan angket yang di berikan ke guru dan siswa untuk di isi hasilnya menunjukkan bahwa 92% menyatakan paham untuk Dapat berinternet dan tanpa blok akses situs web.
- Semua Peserta yaitu guru dan siswa yang mengikuti kegiatan pengabdian kepada masyarakat menyatakan senang sebanyak 100%

Daftar Referensi

- Asep, S. (2017). *Analisis Penggunaan Web Filter Menggunakan Fortigate*.
<https://cleanbrowsing.org/help/docs/setup-content-filtering-on-windows-with-cleanbrowsing/>.
 Akses 12 Desember 2022
- Hasibuan, M. S. (2018). Keylogger Pada Aspek Keamanan Komputer. *Jurnal Teknovasi: Jurnal Teknik Dan Inovasi*, 3(1), 8–15.

- Irzadi, W. (n.d.). *Analisis Dan Perancangan Sistem Keamanan Jaringan Wireless Berbasis Remote Authentication Dial In User Service (Radius) Server Di Badan Pengkajian Penerapan Teknologi*.
- Paulan, R., Herdiansyah, M. I., & Santi, R. (2012). Analisa Keamanan Jaringan Terhadap Ancaman Data Flooding Pada Badan Penanggulangan Bencana Daerah Prov. Sum-Sel. *Jurnal Mahasiswa TI S1*.
- Rahardjo, B. (2005). Keamanan sistem informasi berbasis internet. Bandung: PT. Insan Indonesia.
- Salsabila, Z. G. (2020). *Pengadaan Perangkat Security Untuk Bni Penjompongan Di PT. Swadharma Duta Data*.
- Simarmata, J., Romindo, R., Putra, S. H., Prasetyo, A., Siregar, M. N. H., Ardiana, D. P. Y., Chamidah, D., Purba, B., & Jamaludin, J. (2020). *Teknologi Informasi dan Sistem Informasi Manajemen*. Yayasan Kita Menulis.
- Wahyu, M. F. W. A. (2019). *LKP: Penerapan Firewall Menggunakan Fortigate di PT. PLN Rayon Taman Sidoarjo*. Universitas Dinamika.