SKRIPSI

PENERAPAN METODE *RESPONE POLICY ZONE* (RPZ) PADA DNS *FILTERING SLAVE TRUST* POSITIF KEMENTERIAN KOMINFO RI (Studi Kasus : Universitas Pakuan)

Disusun Oleh :
Azi Heris Saputra
065120138

PROGRAM STUDI ILMU KOMPUTER
FAKULTAS MATEMATIKA DAN ILMU PENGETAHUAN ALAM
UNIVERSITAS PAKUAN
BOGOR
2024

SKRIPSI

PENERAPAN METODE *RESPONE POLICY ZONE* (RPZ) PADA DNS *FILTERING SLAVE TRUST* POSITIF KEMENTERIAN KOMINFO RI (Studi Kasus : Universitas Pakuan)

Diajukan sebagai salah satu syarat untuk memperoleh
Gelar Sarjana Komputer Jurusan Ilmu Komputer
Fakultas Matematika dan Ilmu Pengetahuan Alam

Disusun Oleh :
Azi Heris Saputra
065120138

PROGRAM STUDI ILMU KOMPUTER
FAKULTAS MATEMATIKA DAN ILMU PENGETAHUAN ALAM
UNIVERSITAS PAKUAN
BOGOR
2024

HALAMAN KREASI/PERSEMBAHAN

“Aku tidak peduli akan jadi apa aku di masa depan. Apakah aku akan berhasil ataupun gagal. Tapi yang pasti, apa yang aku lakukan sekarang akan membentukku di masa depan." **(Uzumaki Naruto)**

“Maka sesungguhnya bersama kesulitan ada kemudahan. Sesungguhnya bersama kesulitan ada kemudahan. Maka apabila engkau telah selesai (dari sesuatu urusan), tetaplah bekerja keras (untuk urusan yang lain). Dan hanya kepada Tuhanmulah engkau berharap." **(QS. Al-Insyirah: 6-8)**

Skripsi ini Kupersembahkan untuk :

1. Allah SWT yang memberikan selalu kemudahan dan keberkahan untuk menyusun skripsi ini serta cahaya dalam kehidupan saya selama ini;
2. Ayah (Heru Elfianto) dan Ibu (Ismiati) tersayang, atas segala doa, dukungan serta kasih sayang yang tidak bisa diungkapkan dengan kata-kata;
3. Pakde (Agik Suprayogi) dan Bude (Sri Kayati) atas doa dan dukungannya selama ini menjadi wali saya dari kecil dan menjadi orang tua saya selama ini;
4. Adik saya (Deva) yang selalu memberikan dukungannya
5. Saudara-saudara saya yang selalu memberikan motivasi selama ini;
6. Keluarga besar PUTIK yang memberikan dukungan, motivasi serta dorongan untuk membuat skripsi ini;
7. Aries Maesya, M.Kom. selaku pembimbing utama yang telah memberikan dorongan moral dan motivasi kepada penulis;
8. Victor Ilyas Sugara., M.Kom selaku pembimbing pendamping yang telah memberikan bimbingan, semangat dan motivasi;
9. Dosen-dosenku di Ilmu computer FMIPA UNPAK yang selalu memberikan dukungan dan bimbingannya;
10. Sahabat saya (Yoga dan Karmila) yang selalu menjadi tempat untuk keluh kesan dalam menghadapi skripsi ini;
11. Calon istri yang InsyaAllah akan menjadi ibu dari anak-anak saya kelak yang selalu memberikan dukungan dalam mengerjakan laporan skripsi ini;
12. Teman-temen di kelas Ilkom-O (NR) Angkatan 2020;

HALAMAN PENGESAHAN

Judul : Penerapan Metode *Respone Policy Zone* (RPZ) Pada DNS *Filtering Slave Trust* Positif Kementrian KOMINFO RI
Nama : Azi Heris Saputra
Npm : 065120138

Mengesahkan,

Pembimbing Pendamping Program Studi Ilmu Komputer FMIPA-UNPAK	Pembimbing Utama Program Studi Ilmu Komputer FMIPA-UNPAK
Victor Ilyas Sugara, M.Kom.	**Aries Maesya, M.Kom.**

Mengetahui,

Ketua Program Studi Ilmu Komputer FMIPA- UNPAK	Dekan FMIPA-UNPAK
Arie Qur'ania, M.Kom.	**Asep Denih, S.Kom., M.Sc., Ph.D.**

PERNYATAAN KEASLIAN KARYA TULISAN SKRIPSI

Dengan ini saya,

Nama	: Azi Heris Saputra
NPM	: 065120138
Program Studi	: Ilmu Komputer
Fakultas	: Matematika dan Ilmu Pengetahuan Alam

Menyatakan bahwa skripsi yang berjudul **"Penerapan Metode *Respone Policy Zone*(RPZ) Pada DNS *Filtering Slave Trust* Positif Kementrian KOMINFO RI"**. Sejauh yang saya ketahui, karya tulis ini bukan merupakan karya tulis yang pernah dipulbikasikan atau sudah pernah dipakai untuk medapatkan gelar sarjana di Universitas lain, kecuali pada bagian-bagian Dimana sumber informasinya dicantumkan dengan cara referensi yang semestetinya.

Demikian pernyataan ini saya buat dengan sebenar-benarnya. Apabila kelak dikemudian hari terdapat gugatan, penulis bersedia dikenakan sanksi sesuai dengan peraturan yang berlaku.

Bogor, 24 Mei 2024

Azi Heris Saputra
065120138

PERNYATAAN PELIMPAHAN SKRIPSI DAN SUMBER INFORMASI SERTA PELIMPAHAN HAK CIPTA

Saya yang bertanda tangan dibawah ini :

Nama	: Azi Heris Saputra
NPM	: 065120138
Judul Skripsi	: Penerapan Metode *Respone Policy Zone* (RPZ) Pada DNS *Filtering Slave Trust* Positif Kementrian KOMINFO RI

Dengan ini saya menyatakan bahwa Paten dan Hak Cipta dari produk Skripsi dan Tugas Akhir diatas adalah benar karya saya dengan arahan dari komisi pembimbing dan belum diajukan dalam bentuk apapun kepada perguruan tinggi manapun. Sumber informasi yang berasal atau dikutip dari karya yang diterbitkan maupun tidak diterbitkan dari penulis lain telah disebutkan dalam teks dan dicantumkan dalam Daftar Pustaka dibagian akhir skripsi ini.

Dengan ini saya melimpahkan paten, hak cipta dari karya tulis saya kepada Universitas Pakuan.

Bogor, 20 Mei 2024

Azi Heris Saputra
065120138

RIWAYAT HIDUP

Azi Heris Saputra, dilahirkan di Bogor pada tanggal 04 Oktober 1998, dari pasangan Bapak Heru Elfianto dan Ibu Ismiati sebagai anak pertama dari 2 bersaudara. Penulis memulai Pendidikan di Sekolah Dasar yang bertempat di SND Babakan Dramaga 1, kemudian pada tahun 2010 peneliti melanjutkan Pendidikan di SMPN 7 Kota Bogor dan tamat pada tahun 2013, kemudian melanjutkan Sekolah Menengah Kejuruan di SMK INFORMAIKA PESAT Kota Bogor dan selesai pada tahun 2016. Pada tahun 2020 peneliti melanjutkan Pendidikan di perguruan tinggi, tepatnya di Universitas Pakuan Kota Bogor (UNPAK) pada Program Studi Ilmu Komputer, Fakultas Matematika dan Ilmu Pengetahuan Alam (FMIPA). Pada bulan Mei 2024 Peneliti menyelesaikan kuliah strata satu (S1), dengan judul penelitian " Penerapan Metode *Respone Policy Zone* (RPZ) pada DNS *Filtering Slave Trust* Positif Kementrian Kominfo RI".

RINGKASAN

Azi Heris Saputra 2024, Penerapan Metode *Respone Policy Zone* (RPZ) pada DNS *Filtering Slave Trust* Positif Kementrian Kominfo RI **"**Implementation of the Respone Policy Zone (RPZ) Method in Positive DNS Filtering Slave Trust Minustry of Society and Information of the RI ". Dibawah bimbingan Aries Maesya, M.Kom dan Victor Ilyas Sugara, M.Kom.

Penerapan DNS *Trust* Positif di lingkungan Universitas Pakuan memerlukan pendekatan yang lebih terarah dan efektif. Dalam kasus ini, *Response Policy Zone* (RPZ) muncul sebagai metode yang dapat diterapkan untuk meningkatkan efisiensi dan akurasi dalam *filtering* DNS. RPZ memungkinkan penggunaan aturan-aturan yang telah ditetapkan sebelumnya untuk menentukan kebijakan respon terhadap alamat-alamat yang diketahui mengandung konten yang menjadi ancaman.Meskipun telah banyak digunakan di berbagai lingkungan, penerapan RPZ pada DNS *Filtering Slave Trust* Positif di Universitas Pakuan masih merupakan bidang yang belum sepenuhnya dimaksimalkan. Oleh karena itu, penelitian ini akan membahas tentang penerapan metode RPZ pada DNS *Filtering* di Universitas Pakuan, dengan fokus pada konsep DNS *Filtering Slave Trust* Positif. Penerapan Metode *Respone Policy Zone* (RPZ) pada DNS *Filtering Slave Trust* Positif Kementrian Kominfo RI telah melakukan pengujian menggunakan skala *Likert* medapatkan hasil 82,32% dari 362 responden yang terdiri dari mahasiswa, dosen dan karyawan. Jumlah Responden dari Mahasiswa sebanyak 253 responden, Dosen 48 responded, karyawan sebanyak 61 responden. Proses pengolahan kuesioner menggunakan skala *Likert* menunjukkan mayoritas responden memberikan penilaian efektif terhadap langkah-langkah tersebut.

Kata Kunci : *Respone Policy Zone* (RPZ), DNS *Server*, *Trust* Positif.

KATA PENGANTAR

Puji syukur kehadiran Allah SWT, karena rahmat dan hidayah nya penulis dapat menyelesaikan penelitian ini yang berjudul :"**Penerapan Metode *Respone Policy Zone* (RPZ) Pada DNS *Filtering Slave Trust* Positif Kementrian Kominfo RI**". Penulisan tugas akhir ini merupakan salah satu syarat memperoleh gelar Sarjana Komputer di Program Studi Ilmu Komputer FMIPA UNPAK Bogor.

Dalam penulisan penelitian ini, penulis dengan senang hati ingin mengucapkan terima kasih yang sebesar-besarnya kepada :

1. Aries Maesya, M.Kom. selaku pembimbing utama yang telah memberikan dorongan moral dan motivasi kepada penulis.
2. Victor Ilyas Sugara., M.Kom selaku pembimbing pendamping yang telah memberikan bimbingan, semangat dan motivasi.
3. Arie Qur'ania, M.Kom., Ketua Program Studi Ilmu Komputer yang telah memberikan dorongan moral dan motivasi kepada penulis.
4. Tim Putik Universitas Pakuan yang selalu memberi dukungan penuh untuk dalam proses penelitian ini.
5. Keluarga saya yang selalu memberikan dukungan dan doannya agar cepat menyelesaikan penelitian ini.

Menyadari keterbatasan waktu dan kemampuan dalam penulisan penelitian ini masih jauh dari sempurna. Oleh karena itu, segala kritik dan saran yang membangun akan diterima dengan senang hati. Mudah-mudahan Allah SWT akan membalas semua kebaikan kepada semua pihak yang membantu. Akhir kata, semoga laporan ini dapat bermanfaat bagi kita semua. Amin.

Bogor, 20 Mei 2024

Azi Heris Saputra

DAFTAR ISI

DAFTAR GAMBAR

DAFTAR TABEL

DAFTAR LAMPIRAN

BAB I
PENDAHULUAN

1.1 Latar Belakang

Dalam era digital yang berkembang pesat, akses internet telah menjadi kebutuhan pokok dalam kehidupan sehari-hari. Namun, bersamaan dengan kemudahan akses tersebut, muncul pula berbagai tantangan terkait dengan konten yang tidak layak, konten berbahaya, dan konten yang merugikan. Di tengah dinamika ini, pengamanan dan pengendalian akses internet menjadi krusial, terutama di lingkungan lembaga Pendidikan Universitas Pakuan. Kementerian Komunikasi dan Informatika Republik Indonesia (KEMINFO RI) memiliki tanggung jawab untuk mengawasi dan mengendalikan konten internet yang beredar di Indonesia. Salah satu inisiatif yang telah diterapkan adalah DNS *Trust* Positif, yang bertujuan untuk memblokir akses ke konten yang merugikan, termasuk konten pornografi, hoax, SARA, dan pelanggaran hak cipta.

Situs negatif saat ini sudah semakin menyebar luas di lingkungan Universitas Pakuan. Setiap hari tercatat ribuan akses masuk ke halaman situs negatif, hal ini sesuai dengan peraturan Menteri Komunikasi dan Informatika Republik Indonesia Nomor 19 Tahun 2014 Pasal 8 Ayat (1). "Penanganan Situs Internet Bermuatan Negatif". Dengan adanya peraturan ini diharapkan dapat menjahui masyarakat dari dampak negatif internet.

Penerapan DNS *Trust* Positif di lingkungan Universitas Pakuan memerlukan pendekatan yang lebih terarah dan efektif. Dalam kasus ini, *Response Policy Zone* (RPZ) muncul sebagai metode yang dapat diterapkan untuk meningkatkan efisiensi dan akurasi dalam *filtering* DNS. RPZ memungkinkan penggunaan aturan-aturan yang telah ditetapkan sebelumnya untuk menentukan kebijakan respon terhadap alamat-alamat yang diketahui mengandung konten yang menjadi ancaman.

Meskipun telah banyak digunakan di berbagai lingkungan, penerapan RPZ pada DNS *Filtering Slave Trust* Positif di Universitas Pakuan masih merupakan bidang yang belum sepenuhnya dimaksimalkan. Oleh karena itu, penelitian ini akan membahas tentang penerapan metode RPZ pada DNS *Filtering* di Universitas Pakuan, dengan fokus pada konsep DNS *Filtering Slave Trust* Positif.

Terkait Permasalahan tersebut, beberapa peneliti telah melakukan penelitian seperti (Muhlison et al 2015) yang berjudul Analisis dan Implementasi DNS *Server* sebagai *Filtering* Konten Negatif Menggunakan Metode RPZ (*Response Policy Zone*) di PT. TIME EXCELINDO dengan tujuan penelitian ini dapat membebaskan *Client* dari proses filtering sehingga beberapa *Client* dapat terbebas dari proses filtering dengan bantuan router. Sedangkan penelitian (Firmasnyah et al 2019) dengan judul *Filtering Domain Name Server* (DNS) untuk membangun Internet Sehat Menggunakan Routerboard Mikrotik, tujuan penelitian untuk semua *Client* yang terkoneksi kedalam jaringan internet yang mendapatkan akses jika tersambung dengan DNS yang telah ditentukan, hal ini bertujuan untuk membatasi dan meminimalisir penggunakan Open DNS untuk mengakses situs-situs negatif.

Berdasarkan penelitian terdahulu terdapat beberapa masalah diantaranya *software* DNS *Recursive* hanya sebatas tempat cache DNS sementara, oleh karena itu *software* ini sulit untuk di kembangkan dalam hal penyimpanan *cache* DNS lebih lama lagi. Penerapan DNS *Trust* Positif di Universitas Pakuan meningkatkan efisiensi dan akurasi dalam *filtering* DNS.

Studi kasus ini bertujuan untuk memberikan pemahaman yang lebih mendalam tentang bagaimana penerapan DNS *Server* dengan metode RPZ yang menjadi *Slave* dari DNS *Trust* Positif Kementerian Komunikasi dan Informatika RI dapat membantu Universitas Pakuan dalam memblokir konten-konten negatif yang tidak diinginkan, seperti pornografi, *hoaks*, konten berbahaya, dan pelanggaran hak cipta. Diharapkan penelitian ini dapat memberikan kontribusi praktis dalam meningkatkan keamanan dan kenyamanan akses internet di lingkungan pendidikan, khususnya Universitas Pakuan.

1.2 Tujuan

Penelitian ini betujuan untuk penerapan Metode *Respone Policy Zone* (RPZ) pada DNS *Filtering Slave Trust* Positif Kementrian Kominfo RI solusi untuk menangani masalah terkait dengan konten yang tidak layak, konten berbahaya, dan konten yang merugikan.

1.3 Ruang Lingkup

Penelitian ini memiliki ruang lingkup untuk penerapan metode *Respone Policy Zone* (RPZ) pada DNS *Filtering Slave Trust* Positif Kementerian Kominfo RI sebagai berikut :

1. Penerapan metode *Respone Policy Zone* (RPZ) pada DNS *Filtering Slave Trust* Positif Kementerian Kominfo RI ini menggunakan Linux Ubuntu *Server* 22.04 LTS.
2. Aplikasi yang digunakan untuk penerapan metode *Respone Policy Zone* (RPZ) pada DNS *Filtering Slave Trust* Positif Kementerian Kominfo RI menggunakan aplikasi BIND9.
3. Metode yang akan digunakan dalam penelitian ini yaitu Metode *Respone Policy Zone* (RPZ) pada aplikasi BIND9
4. Penerapan metode *Respone Policy Zone* (RPZ) pada DNS *Filtering Slave Trust* Positif Kementerian Kominfo RI mencakup jaringan internet Universitas Pakuan
5. Sinkronisasi *Trust* Positif Kementerian Kominfo RI dengan DNS *Server* Universitas Pakuan.

1.4 Manfaat

Penelitian ini diantaranya dapat memberikan manfaat bagi Universitas Pakuan dalam penerapan metode *Respone Policy Zone* (RPZ) serta menjaga keamanan dan kenyamanan dalam menggunakan jaringan internet di lingkungan Unpak :

1. Penerapan metode RPZ pada DNS *Filtering Slave Trust* Positif di Universitas Pakuan akan meningkatkan kualitas layanan internet yang disediakan oleh universitas. Dengan memblokir konten-konten negatif yang sudah diregulasikan oleh Kominfo dan Pemerintah.
2. Merupakan solusi teknologi yang efektif dalam mengontrol akses ke konten negatif secara otomatis dan terstruktur melalui jaringan internet dengan metode *Respone Policy Zone* (RPZ).

3. Penerapan DNS *Slave* untuk *Filtering Slave Trust* Positif di Universitas Pakuan dengan DNS *Master* dari *Trust* Positif KOMINFO RI membuat konten-konten yang diblokir oleh KOMINFO RI akan selalu *update* secara otomatis pada DNS *server* Universitas Pakuan.
4. Menghindari *user* (Mahasiswa/Dosen/Staf) terkena *phising website* pada jaringan *local* maupun internasional.
5. Menghindari *user* (Mahasiswa/Dosen/ Staf) untuk melakukan akses pada situs atau website yang dinilai terindikasi memuat konten yang bersentimen Suku, Agama, Ras, dan Antar Golongan (SARA) hingga.
6. Menghindari ancaman *cyber* seperti penyebaran virus dan *malware* melalui situs atau website yang tidak terpercaya.

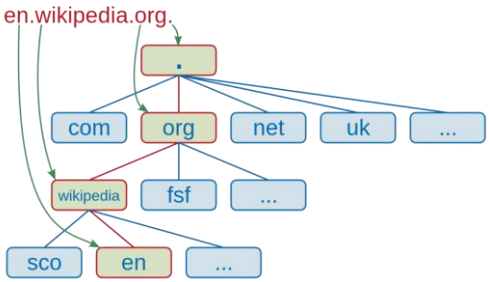
BAB II
TINJAUAN PUSTAKA

2.1 Landasan Teori

2.1.1 *Domain Name System* (DNS)

DNS adalah kependekan dari *Domain Name System* (DNS *server*), yaitu nama sebuah sistem database yang berguna untuk memenuhi kebutuhan komputer, layanan atau sumber daya yang terhubung ke dalam jaringan internet atau jaringan komputer pribadi. Atau definisi lainnya adalah merupakan sistem database yang terdistribusi, digunakan sebagai pencarian nama komputer di dalam jaringan yang menggunakan TCP/IP (*Transmission Control Protocol/Internet Protocol*). DNS memungkinkan nama suatu host pada jaringan komputer atau internet ditranslasikan menjadi *IP Address*, dan sebaliknya. (Nabil et al, 2019). Sistem ini bekerja seperti buku telepon untuk internet. Di mana nama *domain* mewakili nama website dan Alamat IP mewakili lokasi website di internet.

Prinsip dasar cara kerja DNS adalah mencocokkan nama komponen URL dengan komponen *IP Address*. Setiap URL dan *IP Address* memiliki bagian-bagian yang saling menjelaskan satu dengan yang lain. DNS *server* adalah bagian penting dari proses tersebut. Dapat dilihat pada Gambar 1.



Gambar 1. Model Tree *Domain*.

Pada gambar diatas perbedaannya, kode perpustakaan mulai dari depan. Sedangkan, kode pada DNS diurutkan dari belakang. Berikut penjelasan lengkapnya:

1. ***Root-Level Domain*** merupakan bagian tertinggi dari hirarki DNS. Biasanya ia berwujud tanda titik (.) di bagian paling belakang sebuah URL.
2. ***Top Level Domain*** adalah ekstensi yang berada di bagian depan *root-level domain*. Terdapat dua jenis TLD yang umumnya dipakai. Keduanya, yaitu *Generic Top-Level Domain* (GTLD) dan *Country Code Top Level Domain* (CCLTD).

GTLD biasanya menjelaskan sifat institusi dari pemilik web. Katakanlah, website untuk tujuan komersial biasanya memiliki ekstensi .COM. Lalu, .EDU untuk institusi pendidikan dan .GOV untuk lembaga pemerintahan.

Di sisi lain, CCLTD merupakan ekstensi yang menjelaskan asal negara dari pemilik situs. Misalnya, akhiran .ID untuk website Indonesia, .AU untuk Australia, .UK untuk Inggris, dan sebagainya.

1. ***Second Level Domain*** ialah nama lain untuk *domain* itu sendiri. Ia sering digunakan sebagai identitas institusi atau branding. Dalam kasus URL en.wikipedia.org, yang dimaksud SLD adalah wikipedia.

2. ***Third-Level Domain*** atau *subdomain* merupakan bagian dari *domain* utama yang berdiri sendiri. Apabila *domain* diibaratkan sebagai rumah, *subdomain* adalah salah satu ruang khusus di rumah itu sendiri.
3. ***Hostname*** atau bisa disebut juga dengan scheme. Ini merupakan bagian yang mengawali sebuah URL. Bagian ini menunjukkan sebuah fungsi dari sebuah website atau halamannya. Contoh paling banyak digunakan, yaitu HTTPS atau *Hypertext Transfer Protocol Secure*.

Ada beberapa jenis informasi yang bisa diminta dalam sistem DNS. Berikut adalah 10 DNS record yang paling sering dijumpai:

1. **A *Record*** atau *Address record* ─ menyimpan informasi soal *hostname*, *time to live* (TTL), dan *IPv4 Address*.
2. **AAA *Record*** ─ menyimpan informasi hostname dan hubungannya dengan *IPv6 address*.
3. **MX *Record*** ─ merekam *server* SMTP yang khusus digunakan untuk saling berkirim *email* di suatu *domain*.
4. **CNAME *Record*** ─ digunakan untuk me-redirect *domain* atau *subdomain* ke sebuah *IP Address*. Lewat fungsi satu ini, Anda tak perlu memperbarui DNS *record*.
5. **NS *Record*** ─ merujuk *subdomain* pada *authoritative name server* yang diinginkan. *Record* ini berguna jika *subdomain* Anda memiliki *hosting web* berbeda dengan *domain*.
6. **PTR *Record*** ─ memberikan izin pada DNS *resolver* untuk menyediakan informasi soal *IP Address* dan menampilkan *hostname* (*reverse DNS lookup*).
7. **CERT *Record*** ─ menyimpan sertifikat *enkripsi* atau sertifikat keamanan.
8. **SRV *Record*** ─ menyimpan informasi terkait lokasi komunikasi, semacam Priority, Name, Weight, Port, Points, dan TTL
9. **TXT *Record*** ─ membawa dan menyalurkan data yang hanya bisa dibaca oleh mesin.
10. **SOA *Record*** ─ bagian yang muncul di awal dokumen DNS *zone*. Bagian yang sama juga merujuk pada *Authoritative Name Server* serta informasi lengkap sebuah *domain*.

Ketika pengguna internet mengetikkan nama *domain* ke dalam *browser web*, *browser* akan mengirimkan permintaan DNS ke *server* DNS. *Server* DNS kemudian akan mencari alamat IP yang sesuai dengan nama *domain* tersebut. Jika alamat IP ditemukan, *server* DNS akan mengembalikannya ke *browser*.

Browser kemudian akan menggunakan alamat IP tersebut untuk terhubung ke website yang dituju. Berikut adalah beberapa komponen utama DNS :

1. **Nama *Domain***: Nama yang mudah diingat manusia yang digunakan untuk mewakili website.
2. **Alamat IP**: Alamat numerik yang digunakan oleh komputer untuk mengidentifikasi perangkat di internet.
3. ***Server* DNS**: *Server* yang menyimpan dan mengelola data DNS.
4. ***Record* DNS**: Data yang disimpan di *server* DNS, yang berisi informasi tentang nama *domain*, alamat IP, dan lainnya.

2.1.2 *Berkeley Internet Name Domain* (BIND9)

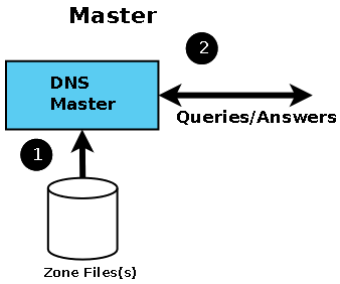
Berkeley Internet Name Domain (BIND9) adalah DNS *software* yang paling umum digunakan. BIND9 memiliki banyak fitur yang dapat membantu dalam membangun sebuah DNS *server*. Salah satu fitur BIND9 adalah Split DNS. BIND9

(Berkeley Internet Name Domain versi 9) menjadi perangkat lunak DNS *Server* yang paling banyak digunakan secara global, dengan kemampuan komprehensif yang dapat diterapkan pada berbagai sistem operasi, termasuk Linux. BIND9 mendukung berbagai jenis rekaman DNS, seperti A *record*, CNAME, MX, dan lainnya. (Pederson , 2023).

Pada konfigurasi ini BIND9 dapat difungsikan menjadi beberapa jenis tipe DNS Server yaitu :

1. ***Master (Primary) Name Servers***

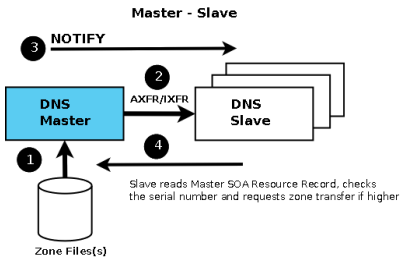
Master (Primary) adalah *name server* utama dari sebuah *domain*, *Name server* ini memuat informasi langsung mengenain *domain* tertentu yang langsung disimpan pada *server* dan diatur oleh *administrator*. Contohnya ns1.unpak.ac.id yang merupakan *primary server* dari *domain* unpak.ac.id maka setiap ada penambahan dan perubahan host di *domain* unpak.ac.id harus langsung *update* pada *zone file* db.unpak.ac.id Diagram DNS *Master* (*Primary*) dapat dilihat pada gambar 2.



Gambar 2. *Diagram DNS Master (Primary)*

2. ***Slave (Secondary) Name Servers***

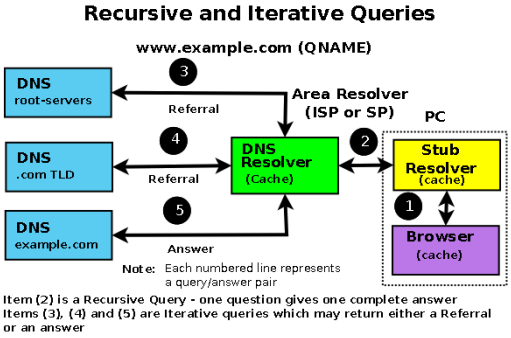
Slave (Secondary) Server adalah DNS *server* yang tidak memelihara langsung zona file dari suatu *domain. Secondary server* akan mengupdate *zona file* dari *primary server*. *Proses updating* secondary server dari *Master (primary) server* disebut *zona transfer*. *Secondary server* digunakan untuk mengurangi *traffic query* permintaan ke *Master (primary) server*. *Client* cukup mengirim *query* ke *secondary server*. Setiap ada perubahan pada *primary server* akan diupdate secara otomatis oleh *secondary server*. Sebuah DNS *server* dapat merupakan *primary server* dari beberapa *zona* sekaligus dan dapat juga merupakan *secondary server* dari beberapa *domain* sekaligus. Diagram DNS Slave (Secondary) dapat dilihat pada gambar 3.



Gambar 3. Diagram DNS *Slave (Secondary)*

3. *Caching Name Servers*

Caching Name Server yaitu *server* tidak mempunyai kewenangan terhadap *domain* tertentu, dia akan menjawab permintaan terhadap nama *domain* dari *nameserver* lain. Dengan menjalankan *Caching-only* DNS *Server* maka setiap permintaan dari pengguna akan diteruskan ke DNS *server root domain* (.) yang dapat diakses oleh DNS *server* tersebut. Diagram DNS Caching dapat dilihat pada gambar 4.



Gambar 4. Diagram DNS *Caching*

2.1.3 *Response Policy Zone* (RPZ)

Response Policy Zone adalah sebuah metode yang membuat *name server* administator memiliki hak untuk menentukan apa yang boleh dan tidak boleh, 19 apa yang diizinkan dan tidak diizinkan (Irawan et al, 2019). RPZ (*Response Policy Zone*) adalah sebuah metode yang diterapkan didalam sebuah DNS *Server*. Internet adalah sebuah tempat untuk menemukan segala informasi baik informasi positif dan negatif. Tanpa RPZ user dapat mengakses situs-situs negatif (Harsapranata, 2019). RPZ adalah fitur canggih dalam DNS yang memungkinkan administrator jaringan untuk mengontrol bagaimana nama *domain* diterjemahkan menjadi alamat IP. Fitur ini memberikan *fleksibilitas* dalam mengelola akses internet dengan cara:

1. Memblokir situs *web*: RPZ dapat digunakan untuk memblokir akses ke situs web tertentu, seperti situs web yang mengandung konten negatif atau berbahaya.
2. Mengalihkan *traffic*: RPZ dapat digunakan untuk mengalihkan *traffic* dari satu situs *web* ke situs *web* lain. Contohnya, ketika sebuah situs web sedang *down*, RPZ dapat mengalihkan *traffic* ke situs web alternatif.

2.1.4 *Trust* Positif

Trust Positif adalah sebuah gerakan yang digagas oleh Kementerian Komunikasi dan Informatika Republik Indonesia (Kominfo RI) untuk membangun ruang digital yang lebih positif dan bertanggung jawab di Indonesia. Gerakan ini diluncurkan pada tahun 2021 dengan tujuan untuk :

1. Meningkatkan literasi digital masyarakat.
2. Menangkal konten negatif di internet.
3. Mendorong penggunaan internet yang bertanggung jawab.

Sistem *TRUST* Positif menerapkan mekanisme kerja adanya *server* pusat yang akan menjadi acuan dan rujukan kepada seluruh layanan akses informasi publik (fasilitas bersama) serta menerima informasi – informasi atas fasilitas akses informasi public untuk menjadi alat analisa dan profiling penggunaan internet di Indonesia.

Sistem *TRUST* Positif bukan merupakan single *gateway* ataupun *traffic relay* untuk koneksi internet seluruh Indonesia. Masing – masing pengguna

menyediakan infrastruktur sesuai dengan kebutuhan masing – masing dan *TRUST* Positif akan berfungsi sebagai referensi atau rujukan database.Sampai dengan akhir tahun 2022, telah terdaftar 51.588 situs terkait pornografi, 156.975 situs dari perjudian, 32.432 situs penipuan online, serta 2005 situs dari pelanggaran ha katas kekayaan intelekual (HKI) tim *TRUST* Positif. Berikut adalah situs aduan konten negatif kominfo sebagai berikut :

1. Pornografi
2. Perjudian
3. *Radikalisme*
4. SARA
5. Kekerasan
6. Pornografi Anak
7. Penipuan
8. Pelanggaran Hak Cipta (HKI)

2.1.5 Ubuntu *Server*

Ubuntu adalah *distro* Linux turunan Debian yang dikembangkan dengan tujuan utama menjadi *distro* Linux *destop* yang mudah digunakan dengan rilis stabil setiap 6 bulan sekali. Ubuntu berasal dari kata dalam bahasa Afrika Kuno ubuntu yang maknanya kemanusiaan untuk semua (*humanity towards others*). (Nabil et al, 2019). Ubuntu *Server* adalah sistem operasi berbasis Linux yang dirancang untuk *server* dan *cloud*. Ubuntu *Server* adalah *open source software* yang tersedia secara gratis dan dapat digunakan untuk berbagai kebutuhan *server*, seperti :

1. *Web server*: Menyediakan layanan *web*.
2. *Mail server*: Menyediakan layanan *email*.
3. *Database server*: Menyediakan layanan *database*.
4. *File server*: Menyimpan *file* dan membagikannya ke pengguna lain.
5. *Application server*: Menjalankan aplikasi *server*.

2.1.6 *Local Area Network* (LAN)

LAN adalah singkatan dari *Local Area Network*. Jenis jaringan LAN ini sangat sering kita temui di warnet-warnet, kampus, sekolah ataupun perkantoran yang membutuhkan hubungan atau koneksi antar dua komputer atau lebih dalam satu ruangan. Jaringan LAN juga merupakan jaringan yang sangat di pengaruhi oleh topologi. (Rahmat, et al, 2022).

Local Area Network mempunyai ukuran terbatas, yang berarti bahwa waktu transmisi pada keadaan terburuknya terbatas dan dapat diketahui sebelumnya. Dengan mengetahui keterbatasanya menyebabkan adanya kemungkinan untuk menggunakan jenis desain tertentu hail ini juga memudahkan manajemen jaringan. (Ginta, et al 2013).

2.1.7 *Ping*

Ping artinya jeda waktu, nilai yang muncul pada *Ping* di tes kecepatan internet artinya jumlah jeda waktu yang dibutuhkan jaringan komputer atau gawai yang kita gunakan untuk mindahkan data. *Ping* merupakan salah satu program yang digunakan untuk mengecek komunikasi antar komputer dalam sebuah jaringan melalui protokol TCP/IP. *Ping* akan mengirimkan *Internet Control Message Protocol* (ICMP) *Echo Request messages* pada *IP Address* komputer yang dituju dan meminta respons dari komputer tersebut.

Ping adalah sebuah perintah komputer yang pertama kali dicetuskan pada tahun 1983 oleh Mike Muss. Awalnya, perintah ini dibuat dengan tujuan untuk melihat sumber masalah dari sebuah permasalahan komputer. Cara kerja *Ping* adalah dengan membuat perangkat *client* mengirim paket *ICMP_ECHO* dan beberapa data lain dalam suatu *host. Host* tujuan atau *server* akan memberi balasan dengan paket *ICMP_ECHOREPLAY* (Ardiansyah, 2017).

2.1.8 *Nslookup*

Nslookup adalah sebuah tool yang digunakan untuk mencari informasi tentang *Domain Name System* (DNS). Tool ini memungkinkan pengguna untuk:

1. Mencari alamat IP dari sebuah nama *domain*.
2. Mencari nama *domain* dari sebuah alamat IP.
3. Mencari informasi lain tentang DNS, seperti *record* MX dan CNAME.

NSLOOKUP tersedia di berbagai *platform* sistem operasi, seperti Windows, Linux, dan macOS.

2.1.9 Skala *Likert*

Skala *Likert* adalah suatu skala psikometrik yang umum digunakan dalam kuesioner, dan merupakan skala yang paling banyak digunakan dalam riset berupa survei. Ada dua bentuk pertanyaan yang menggunakan Likert yaitu pertanyaan positif untuk mengukur minat positif , dan bentuk pertanyaan negatif untuk mengukur minat negatif. Pertanyaan positif diberi skor 4, 3, 2, dan 1; sedangkan bentuk pertanyaan negatif diberi skor 1, 2, 3, dan 4. Bentuk jawaban skala Likert terdiri dari sangat setuju, setuju, tidak setuju, dan sangat tidak setuju (Taluke et al, 2019).

2.1.10 Universitas Pakuan

Universitas Pakuan merupakan kelanjutan dari Universitas Bogor (Unbo) yang berkiprah selama hampir dua dekade sampai dengan tahun 1980. Beberapa perguruan tinggi swasta pada tahun 1977 berfusi dengan universitas ini yaitu Akademi Pariwisata, IKIP PGRI, Akademi Bahasa Asing, Akademi Sekretaris Manajemen Internasional dan Akademi Ilmu Agama Islam dengan badan penyelenggara Yayasan Perguruan Tinggi Bogor (YPTB). Logo Universitas Pakuan dapat dilihat pada gambar 5.

Gambar 5. Logo Universitas Pakuan

Visi :

"Universitas Pakuan menjadi Perguruan Tinggi yang Unggul, Mandiri, dan Berkarakter pada tahun 2038.

Misi :

1. Menyelenggarakan proses Pendidikan dan pengjaran yang unggul, untuk menghasilkan lulusan berdaya saing tinggi pada skala nasional, maupun internasional.
2. Menciptakan suasana akademik yang mengembangkan karakter kejujuran, kedispilinan, kemampuan bekerjasama, intergrasi,loyalitas, bertanggung jawab dan toleransi.
3. Menyelenggarakan penelitian dan pengembangan ilmu pengetahuan yang berorientasi pada publikasi ilmiah nasional, dan internasional bereputasi
4. Penyelenggarakan pengabdian pada Masyarakat berdasarkan yang beorientasi hasil-hasil penelitian, untuk mengingkatkan kualitas dan kesejahteraan Masyarakat Indonesia.
5. Menyelenggarakan proses Pendidikan yang bermutu dan dipercaya Masyarakat, dengan berpedoman pada sistem peminjaman mutu perguruan tinggi nasional, maupun internasional.

2.2 Penelitian Terdahulu

Dibawah ini merupakan penelitian terdahulu, Dimana para peneliti terdahulu telah melakukan analisa terlebih dahulu, agar dapat menyelesaikan suatu masalah yang dibutuhkan disebuah instansi.

1. Nama : Firmansyah, Rachmat Adi Purnama
   Judul : Filtering *Domain Name Server* (DNS) untuk Membangun Internet Sehat Menggunakan *Routerboard* Miktorik
   Tahun : 2019
   Isi : Semua *Client* yang terkoneksi kedalam jaringan internet yang mendapatkan akses jika tersambung dengan DNS yang telah ditentukan, hal ini bertujuan untuk membatasi dan meminimalisir penggunakan Open DNS untuk mengakses situs-situs negatif

2. Nama : Akhdan Nabil et all
   Judul : Konfigurasi DNS *Server* berbasis Linux Ubuntu dengan menggunakan RPZ di SIMAK Harapan Bersama Regal.
   Tahun : 2019
   Isi : *Optimalisasi* DNS *recursive* dapat membantu kinerja DNS lebih *responsive* dan memudahkan *monitoring* untuk *meminimalisir* kendala DNS saat digunakan, serta bisa membantu membatasi akses *client* terhadap situs-situs negatif.

3. Nama : Fahmi Faisan et al
   Judul : Implementasi DNS dari sudut pandang Efek *Cache* dan *Resolver* bersama untuk mengurangi beba pada sistem.
   Tahun : 2021
   Isi : *Resolver Local Full Service* dengan menggunakan Raspberry Pi menjadi solusi terbaik serta dapat menghemat waktu pencarian web *server* dan penyimpanannya ke *cache* dari *Resolver local full service* sebagai pembuatan *server lokal*.

4. Nama : Molvai Arman et al
   Judul : Pelatihan membangun *Server* DNS Lokal di SMK Negeri 1 Palembang
   Tahun : 2022
   Isi : Pengembangan yang bisa dilakukan yaitu pembuatan langsung DNS *Server* tanpa perlu menggunakan virtualisasi dengan menggunakan internet publik

5. Nama : Rian Hidayat el al
   Judul : *Optimalisasi* DNS *Recursive* untuk mempercepat pencarian informasi di internet PT. Parsaoran Global Datatrans
   Tahun : 2023
   Isi : Pengembangan yang bisa dilakukan dari penelitian ini yaitu bisa menggunakan *Software* BIND9 dengan cakupan konfigurasi DNS yang lebih luas agar kita bisa kembangan dalam optimalisasi DNS *Recursive*.

6. Nama : Dina Kartika et al
   Judul : Simulasi DNS *Server* dan *Server* dengan Sistem *Operasi* Debian pada Jaringan *Local Area Network*
   Tahun : 2023
   Isi : Pengujian menggunakan aplikasi *webstresstool* memberikan *respons* yang baik tanpa *eror* dengan spesifikasi *server prosesor* AMD A4-912 R3, RAM 4GB dan 250 GB HDD. rata-rata *respons time* untuk 10 *user* 77.3 ms, 20 *user* rata-rata 83 ms, 30 *user* rata-rata 227.13, 50 *user* 242.04 dan untuk 100 *user* mendapatkan hasil 521.01 ms

7. Nama : Azi Heris Saputra
   Judul : Penerapan Metode *Respone Policy Zone* (RPZ) Pada DNS *Filtering Slave Trust* Positif Kementrian Kominfo RI
   Tahun : 2024

   Isi : Kementerian Komunikasi dan Informatika RI dapat membantu Universitas Pakuan dalam memblokir konten-konten negatif yang tidak diinginkan, seperti pornografi, *hoaks*, konten berbahaya, dan pelanggaran hak cipta dengan menggunakan DNS *Server* dengan Metode RPZ

Penulis membuat Penerapan Metode *Respone Policy Zone* (RPZ) Pada DNS *Filtering Slave Trust* Positif Kementrian Kominfo RI. Berikut adalah tabel perbandingan terdapat pada Tabel 1 :

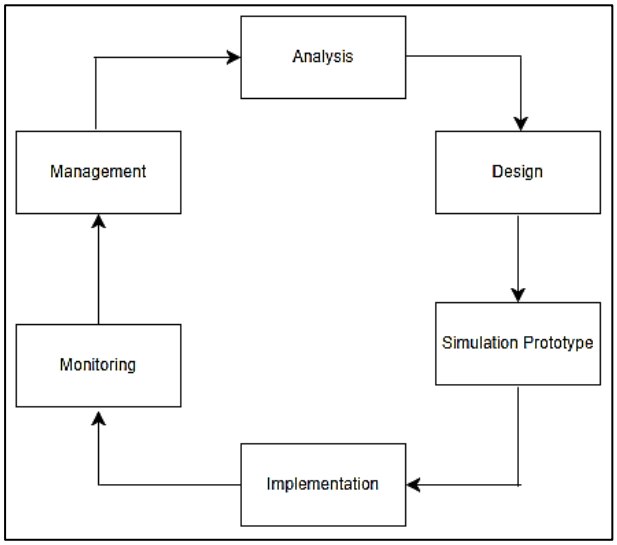
Tabel 1. Perbandingan Penelitian

No	Tahun	Penulis	Judul	Metode					
				DNS *Server*	OS Linux	Aplikasi BIND9	RPZ	IP *Public*	*Master-Slave*
1	2019	Nabil et al	Konfigurasi DNS *Server* Berbasis Linux Ubuntu dengan Menggunakan RPZ di SMK Harapan Bersama Tegal	√	√	√	√		
2	2019	Firmansyah, Purnama	*Filtering Domain Name Server* (DNS) untuk Membangun Internet Sehat Menggunakan *Routerboard* Mikrotik	√					
3	2021	Fauzan et al	Implementasi DNS dari Sudut Pandang Efek *Cache* dan *Resolver* Bersama untuk Mengurangi Beban Pada Sistem	√	√				
4	2022	Arman et al	Pelatihan Membangun *Server* DNS *Local* di SMK Negeri 1 Palembang	√	√	√			
5	2023	Hidayat et al	Optimalisasi Dns *Recursive* untuk Mempercepat Pencarian Informasi di Internet (Studi kasus : PT. Parsaoran Global Datatrans)	√	√				
6	2023	Kartika et al	Simulasi Dns *Server* dan *Web Server* dengan Sistem Operasi Debian Pada Jaringan *Local Area Network*	√	√	√			
7	2024	Azi Heris Saputra	Penerapan Metode *Respone Policy Zone* (RPZ) pada DNS *Filtering Slave Trust* Positif Kementrian Kominfo RI	√	√	√	√	√	√

BAB III
METODE PENELITIAN

3.1 Metode Penelitian

Metodologi penelitian ini dilakukan menggunakan metode analisis terhdapat kinerja suatu jaringan dengan menggunakan pendekatan metode NCLC (*Network Development Life Cyle)* dan Metode *Respone Policy Zone* (RPZ) pada DNS *Filtering Slave Trust* Positif Kementrian Kominfo RI. Metode NDLC yaitu : *Analysis*, *Design*, *Simulation*, *Implementatiom*, *Monitoring*, *Management*. NDLC merupakan suatu pendekatan proses dalam komunikasi data yang menggambarkan siklus yang awal dan akhirnya dalam membangun sebuah jaringan komputer. (Hafiz dan Kurnia. 2021). Metode NDLC (*Network Development Life Cycle*) dapat dilihat pada gambar 6.



Gambar 6. Metode NDLC (*Network Development Life Cycle*)

3.1.1 *Analysis*

Dari proses DNS *Filtering Slave Trust* Positif Kementrian Kominfo RI tahap awal ini dilakukan analisa kebutuhan, analisa permasalahan yang muncul, dan analisa penggunaan internet pada jaringan Universitas Pakuan. Metode yang digunakan dalam tahap ini diatanranya :

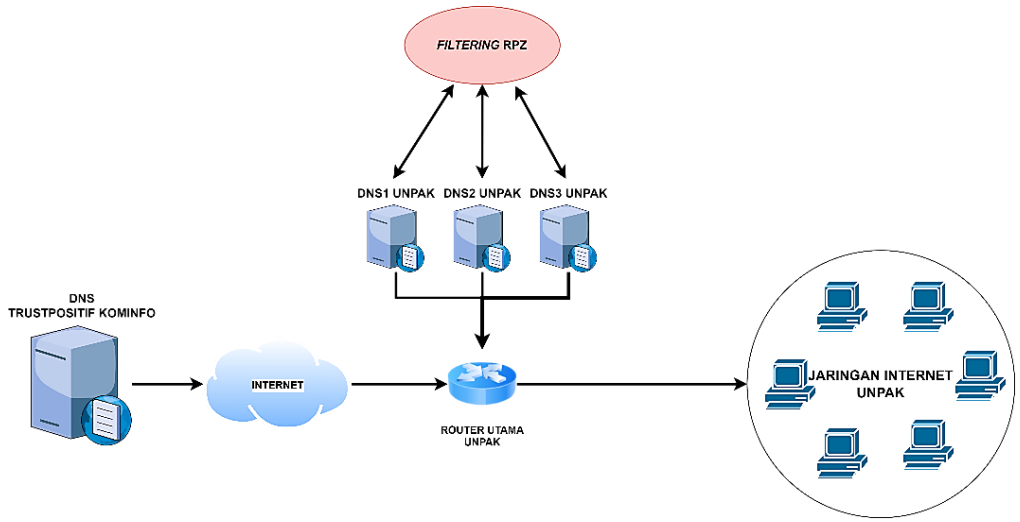
1. Pengecekan konten-konten yang diakses oleh pengguna internet pada jaringan Universitas pakuan yang dilakukan dengan mengecek *Query* DNS pada DNS *Server* yang sudah ada.
2. Membaca literatur penelitian sejenis, pada analiysis awal ini juga dilakukan dengan mencari jurnal-jurnal yang mungkin pernah dibuat sebelumnya.
3. Membaca panduan yang diberikan oleh Kominfo RI mengenai bagaimana penerapan *Trust* Positif pada aplikasi BIND9 dengan Metode *Respone Policy Zone* (RPZ)

Melalui analisis ini, diharapkan DNS *Filtering Slave Trust* Positif Kominfo RI menggunakan aplikasi BIND9 dengan Metode *Respone Policy Zone* (RPZ) dapat berhasil dilakukan pada jaringan internet Universitas Pakuan, sehingga dapat

membantu memblokir konten-konten negatif dan meningkatkan keamanan serta kenyamanan pengguna internet di kampus tersebut.

3.1.2 *Design*

Pada tahap desain, dibuatlah desain topologi pada jaringan internet di Universitas Pakuan yang akan dibangun menggunakan DNS *Server* dengan Metode *Respone Policy Zone* (RPZ). Desain topologi jaringan yang akan dibangun dapat dilihat pada gambar 7.



Gambar 7. Topologi Jaringan DNS *Server* RPZ

Pada topologi jaringan pada gambar 7 terdapat *router* utama sebagai pusat kendali internet pada jaringan Universitas Pakuan yang mengatur jalannya lalulintas internet dengan mendeklarasikan tiga DNS *Server* Universitas Pakuan sebagai DNS *server* untuk seluruh pengguna internet yang ada dibawah *router* utama Universitas Pakuan.Ketiga DNS *Server* Universitas Pakuan menggunakan *system* operasi Ubuntu *Server* 22.04 LTS dengan aplikasi BIND9 sebagai aplikasi DNS *Server* menggunakan Metode *Respone Policy Zone* (RPZ) sebagai *Filtering* konten negatif dengan konfigurasi DNS *Slave (Secondary)* dari DNS *Master (Primary) Trust* Positif Kominfo RI yang berada di luar jaringan internet Universitas Pakuan.Dengan konfigurasi DNS *Slave (Secondary)* pada ketiga DNS *Server* Universitas Pakuan, maka konten-konten yang difilter oleh DNS *Master (Primary) Trust* Positif Kominfo RI akan langsung trupdate pada ketiga DNS *Server* Universitas Pakuan.

3.1.3 *Simulation Prototype*

Simulasi Prototype akan dirancang untuk mengetahui keberhasilan dari rancangannya tersebut. Setelah ujicoba untuk mengiptimalkan hasil rancangan sebelum benar-benar diimplmentasikan pada jaringan.

3.1.4 *Implementation*

Implementasi semua yang telah direncanakan dan didesign sebelumnya. Implementasi merupaka tahapan yang sangat menentukan dari berhasil atau gagalnya sebuah project yang akan dibangun dan ditahap inilah akan diuji untuk menyelesaikan masalah teknis dan non teknis dilapangan. Ada beberapa masalah-masalah yang sering muncul diantaranya seperti berikut ini :

1. Jadwal yang tidak tepat karna adanya faktor-faktor penghambat

2. Peralatan pendukung dibutuhkan untuk manajemen *project* dan manajemen resiko untuk meminimalkan sekecil mungkin hambatan-hambatan yang ada.

3.1.5 *Monitoring*

Setelah melakukan DNS *Filtering Slave Trust* Positif Kementrian Kominfo RI pada jaringan internet Universitas Pakuan akan dilakukan pemantauan perkembangan dari apa yang telah diterapkan. Selama pemantauan akan di cek terus apakah terupdate konten-konten pada zone DNS *Trust* Positif DNS *Server* Universitas Pakuan.

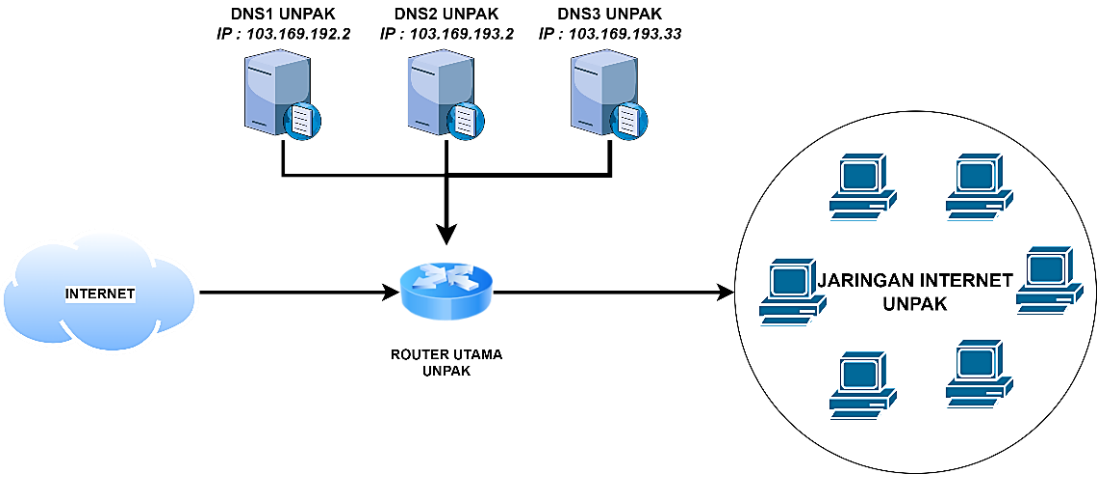
3.1.6 *Management*

Pada tahap ini salah satu yang menjadi perhatian khusus adalah masalah kebijakan, yaitu dalam hal aktivitas, pemeliharaan dan pengelolaan dikategorikan pada tahapan ini, melewati semua tahapan akan lebih mudah menentukan metode apa yang akan digunakan untuk memanajemen sistem kedepannya, setelah manajemen tahap pertama telah dilakukan dan mengetahui hasil akan lebih mudah memanajemen untuk menghadapai situasi yang terjadi nantinya.

BAB IV
PERANCANGAN DAN IMPLEMENTASI

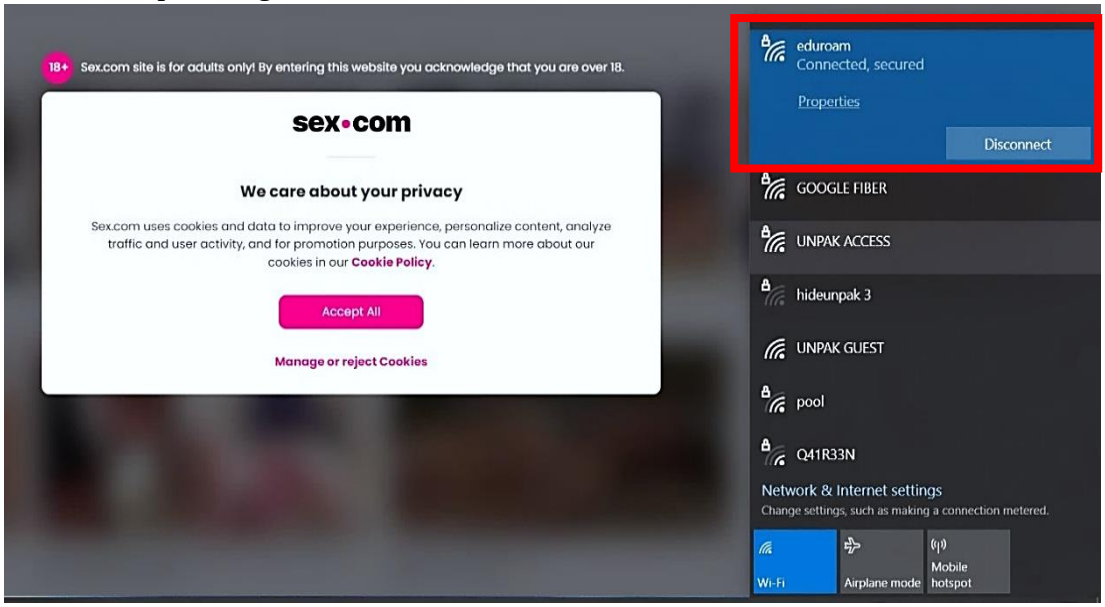
4.1 Tahap Analisis

Pada tahap analisis sistem ditemukan menganai masalah dalam penggunaan konten pada jaringan internet pada jaringan Universitas Pakuan, yang kemudian akan ditindak lanjut untuk mencari Solusi agar konten pada jaringan internet dapat memfilter konten negative yang ada pada jaringan internet pada jaringan Universitas Pakuan. Topologi jaringan yang sedang berjalan dapat dilihat pada gambar 8.



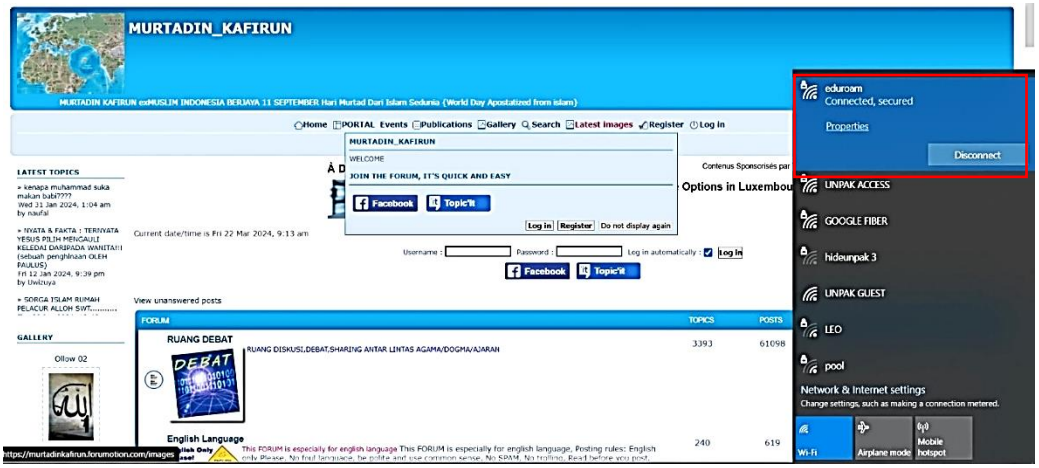
Gambar 8. Topologi Jaringan yang sedang berjalan

Topologi jaringan gambar 8 memiliki *router* utama sebagai pusat kendali internet Universitas Pakuan. *Router* ini mengatur lalulintas internet dengan tiga DNS *server* Unpak sebagai DNS *server* untuk pengguna internet di bawahnya. Namun, DNS Unpak belum bisa melakukan *filtering* konten negatif yang tersebar di internet UNPAK, seperti di gambar 9.



Gambar 9. Akses Konten Pornografi

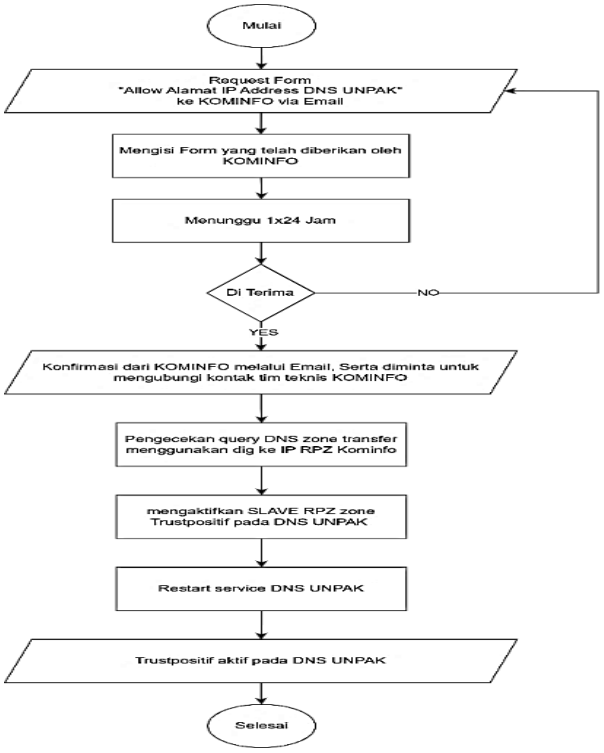
Pengguna internet di Universitas Pakuan dengan menggunakan jaringan WiFi eduroam masih bisa mengakses konten pornografi dan konten SARA yang mengandung konten negatif melalui *web browser*. Hal ini akan merugikan Universitas Pakuan karena internet di kampus harus sehat dan bersih dari konten-konten yang mengandung dengan konten negatif. Akses konten Sara pada gambar 10.



Gambar 10. Akses Konten SARA

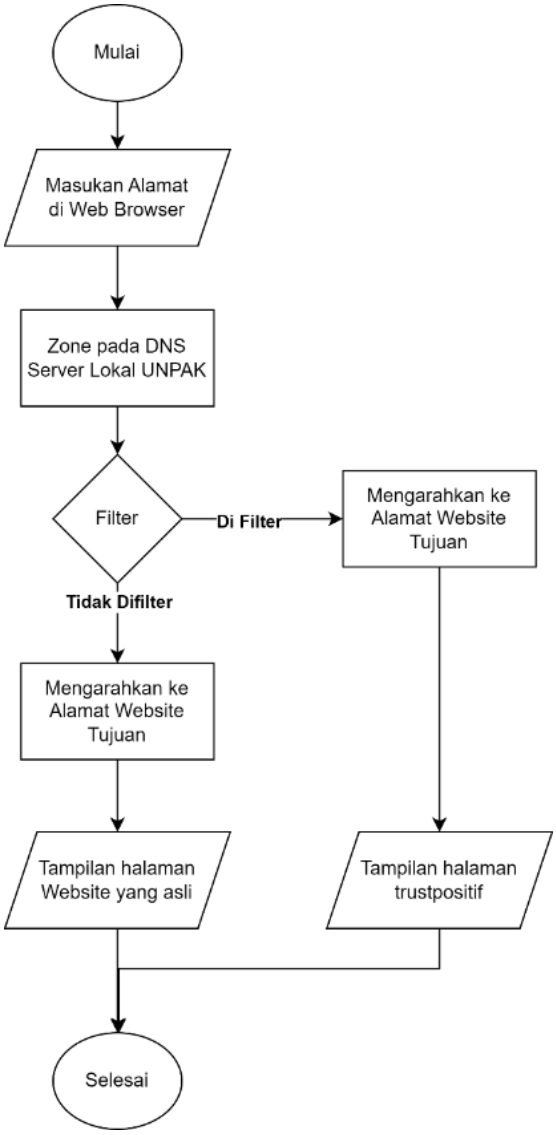
4.2 Tahap Desain

Dari tahap analisis tedapat masalah pada konten internet untuk pengguna internet di Universitas Pakuan, oleh karena itu dibuatlah rancangan desain yang akan dikembangkan untuk Penerapan Metode *Respone Policy Zone* (RPZ) Pada DNS *Filtering Slave Trust* Positif Kementerian KOMINFO RI di Universitas Pakuan. Flowchart Sinkronisasi dengan DNS UNPAK dapat dilihat pada gambar 11.



Gambar 11. Flowchart *Sinkronisasi* dengan DNS UNPAK

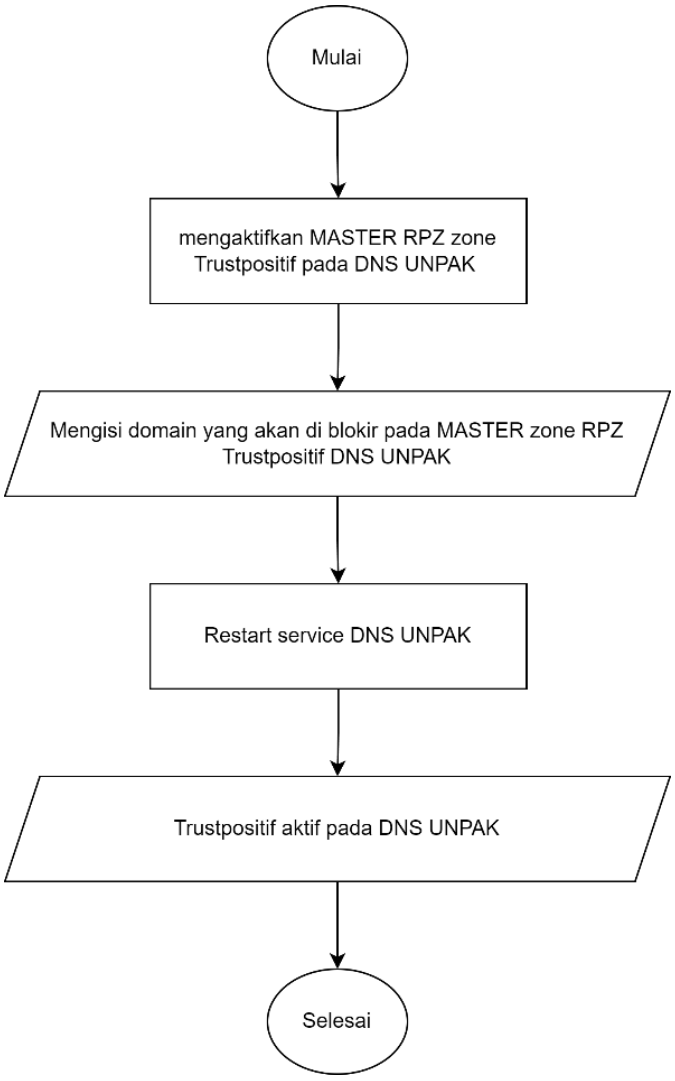
Gambar 11 menjelaskan bagaiman alur proses sinkronisasi DNS *Trust* positif Kominfo RI dengan DNS UNPAK, dimulai dari melakukan request form formulir untuk *Allow* Alamat IP *Address* DNS Universitas Pakuan ke DNS *Trust* positif Kominfo RI melalui *email* kemudian akan dibalas dan dikirimkan *link Form* untuk permohonan koneksi RPZ Kominfo untuk diisikan sesuai dengan data yang diperlukan, selanjutnya menunggu 1x24 jam dan dilanjutkan untuk konfirmasi ke tim teknis Kominfo RI, kemudian dilanjutkan untuk pengecekan pada DNS *server* Universitas Pakuan apakah sudah bisa *sinkron* atau tidak, setelah *sinkron* antara DNS *server* Universitas pakuan dan DNS *trust* positif Kominfo RI akan diaktifkan *zone slave trust* positif pada DNS *server* Universitas Pakuan, dan terakhir dilakukan *restrart service* DNS *Server* Universitas Pakuan kemudian *trust* positif akan aktif pada jaringan internet Universitas Pakuan. Flowchart Filtering DNS dengan Metode (RPZ) dapat dilihat pada gambar 12.



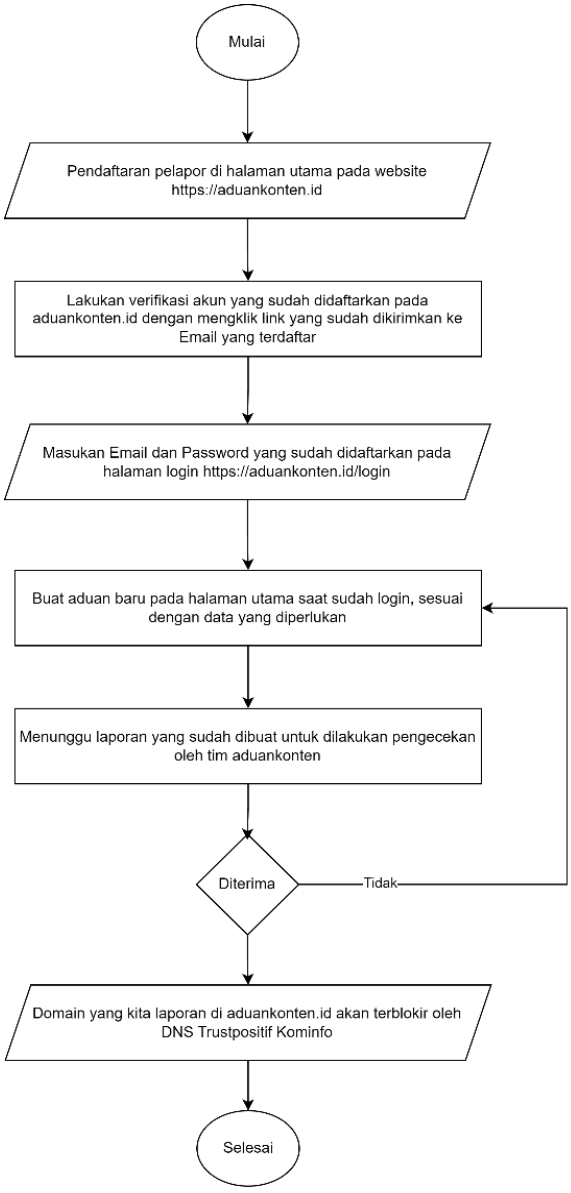
Gambar 12. *Flowchart Filtering* DNS dengan Metode (RPZ)

Gambar 12 menggambarkan alur bagaimana DNS *server* dengan menggunakan Metode *Respone Policy Zone* (RPZ) berkerja pada jaringan internet Universitas Pakuan sebagai *filtering* konten-konten negatif yang dimulai dari pengguna internet di Universitas Pakuan memasukan URL pada *browser* untuk mengakses situs tertentu, kemudian DNS *server* Universitas Pakuan akan mengecek apakah konten yang akan diakses oleh *client* itu mengandung konten negatif atau tidak , jika konten tersebut mengandung konten negatif maka akan dialihkan ketampilan *trust* positif Universitas Pakuan, tapi jika tidak mengandung konten negatif akan langsung dialihkan kehalaman asli dari URL yang dimasukan oleh *client*.

DNS *server* Universitas Pakuan menjadi DNS *Master trust* positif untuk *filtering* menggunakan metode RPZ yang dimulai dari mengaktifkan *Zone Master trust* positif pada DNS *server* Universitas Pakuan, dilanjutkan untuk mengisi *list domain* apa saja yang akan diblokir oleh DNS Universitas Pakuan, kemudian *restart service* DNS *server* Universitas Pakuan, dan DNS *Master trust* positif Universitas Pakuan akan aktif, *Flowchat* menjadi *Master Trust* Positif di DNS UNPAK pada gambar 13 .



Gambar 13. *Flowchart Master Trust* Positif di DNS UNPAK

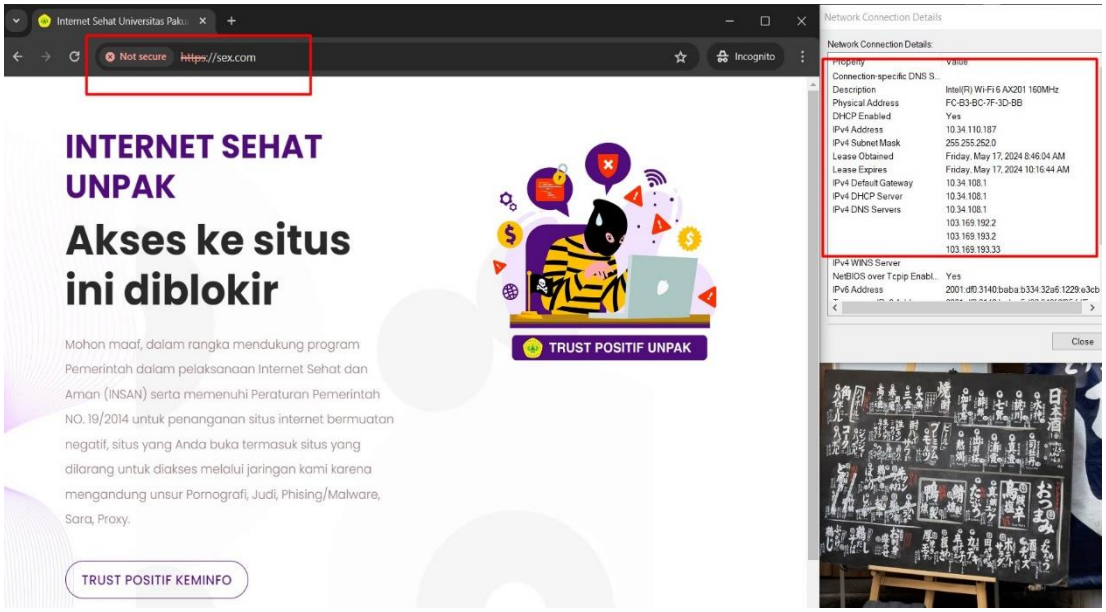


Gambar 14. *Flowchart* Domain yang akan diblokir melalui aduankonten

Gambar 14 menjelaskan bagaimana cara melaporkan *domain* yang mengandung konten negatif ke *trust* positif Kominfo RI agar dilakukan pemblokiran melalui *website* aduankonten.id dimulai dari pendaftaran akun untuk mengakses halaman *website* aduankonten.id, kemudian melakukan *verifikasi* akun yang didaftarkan dengan mengecek *email* yang terdaftar, lalu login ke *website* aduankonten.id untuk melaporkan domain yang akan diblokir, selanjurnya membuat laporan domain yang akan diblokir oleh *trust* positif Kominfo RI, didalam membuat laporan di aduankonten.id isikan data yang diperlukan untuk melakukan pelaporan pemblokiran domain yang mengandung konten negatif, selanjutnya menunggu proses oleh tim dari aduankonten.id, jika diterima laporan yang kita buat maka *domain* yang dilaporkan akan langsung terblokir oleh *trust* positif Kominfo RI.

4.3 Tahap *Simulation Prototype*

Pada tahap *Simulation Prototype*, tahapan sebelum implementasikan pada seluruh jaringan Universitas Pakuan dilakukan uji coba pada jaringan yang cakupannya kecil yaitu pada jaringan *Local Area Network* (LAN) di Pusat Teknologi Informasi dan Komunikasi (PUTIK) Universitas Pakuan selama 2 hari untuk lihat apakah ada masalah dalam penerapan *trust* positif atau tidak.



Gambar 15. Pengetesan Konten Negatif pada Jaringan di PUTIK

Pada gambar 15 dilakukan pengetesan untuk mengakses konten negatif di internet dengan menggunakan jaringan *Local Area Network* (LAN) di Pusat Teknologi Informasi dan Komunikasi (PUTIK) Universitas Pakuan. bisa dilihat saat kita akses konten yang mengandung konten negatif akan langsung dialihkan pada halaman *trust* positif Universitas Pakuan.

4.4 Implementation

Setelah dilakukan *Simulation Prototype* pada jaringan *Local Area Network* (LAN) di Pusat Teknologi Informasi dan Komunikasi (PUTIK) Universitas Pakuan yang cakupan jaringannya kecil dan berhasil melakukan *filtering* konten negatif selanjutnya adalah tahap *Implementation* ke seluruh jaringan Universitas Pakuan.

4.4.1 Permohonan Koneksi RPZ Kominfo

Langkah pertama sebelum dilakukan Penerapan Metode *Respone Policy Zone* (RPZ) Pada DNS *Filtering Slave Trust* Positif Kementrian Kominfo RI dengan mengirimkan permohonan *Allow* Alamat *IP Address* DNS *server* Universitas Pakuan melalu *email* pengendalianaptika@kominfo.go.id, untuk *email* dan balasan dari Kominfo RI bisa dilihat pada halaman lampiran 3.

4.4.2 Mengisi *Form* Permohonan Koneksi RPZ Kominfo

Langkah selanjutnya setelah megirimkan *email* ke Kominfo dan akan dibalas berserta *link* untuk mengisi *form* permohonan koneksi RPZ Kominfo yang akan diisikan sesuai data yang dibutuhkan dan menunggu 1x24 jam untuk dilakukan proses permohonan tersebut oleh tim Kominfo RI, untuk tampilan *Form* Permohonan Koneksi RPZ Kominfo bisa dilihat pada halaman lampiran 4.

4.4.3 Konfirmasi Ke Tim Teknis Kominfo RI

Setelah menunggu 1x24 dilanjutkan untuk konfirmasi untuk pengecekan apakah sudah diproses untuk permohonan koneksi RPZ Kominfo ke tim teknis Kominfo RI melalui nomer *Whatsapp* yang ada pada *email* balasan *email* sebelumnya, untuk tampilan konfirmasi ke tim teknis Kominfo RI melalui *Whatsapp* bisa dilihat pada halaman lampiran 5.

4.4.4 Pengecekan Query DNS *Trust* Positif Kominfo

Setelah menghubungi tim teknis Kominfo RI, akan disuruh untuk melakukan pemeriksaan *query* DNS *zone transfer* pada DNS *server trust* positif Kominfo RI, apakah sudah berhasil disinkronisasi dengan DNS *server* Universitas Pakuan, dengan masukan perintah seperti berikut :

 # dig AXFR @103.154.123.130 trustpositifkominfo +noidnout

Perintah diatas dilakukan pada DNS *Server* Universitas Pakuan yang menggunakan sistem operasi Ubuntu *Server* 22.04 LTS dengan aplikasi DNS *server* yaitu BIND9. Jika berhasil sinkron dengan DNS *Trust* positif Kominfo makan akan tampil informasi seperti pada gambar 16.

```
*.zoo.zone.trustpositifkominfo. 3600 IN CNAME   lamanlabuh.aduankonten.id.
rcz.ac.zw.trustpositifkominfo. 3600 IN  CNAME   lamanlabuh.aduankonten.id.
*.rcz.ac.zw.trustpositifkominfo. 3600 IN CNAME  lamanlabuh.aduankonten.id.
info.betting.co.zw.trustpositifkominfo. 3600 IN CNAME lamanlabuh.aduankonten.id.
*.info.betting.co.zw.trustpositifkominfo. 3600 IN CNAME lamanlabuh.aduankonten.id.
sbobet.\231\167\187\229\154\168.trustpositifkominfo. 3600 IN CNAME lamanlabuh.aduankonten.id.
*.sbobet.\231\167\187\229\154\168.trustpositifkominfo. 3600 IN CNAME lamanlabuh.aduankonten.id.
trustpositifkominfo.    900     IN      SOA     localhost. aduankonten.mail.kominfo.go.id. 24032201 120 60 2592000 900
;; Query time: 189769 msec
;; SERVER: 103.154.123.130#53(103.154.123.130) (TCP)
;; WHEN: Fri Mar 22 17:41:50 WIB 2024
;; XFR size: 5967389 records (messages 22701, bytes 130066942)

root@DNS1:/etc/bind#
```

Gambar 16. Proses Sinkron DNS *Server* UNPAK

Pada gambar 16 diatas bisa dilihat saat melakukan perintah # dig AXFR @103.154.123.130 trustpositifkominfo +noidnout di DNS *server* Universitas Pakuan akah muncul tampilan yang menandakan bawah DNS server *trust* positif Kominfo dan DNS *server* Universitas Pakuan berhasil sinkron.

4.4.5 Mengaktifkan *Zone Trust* Positif dan *Blacklist*

Setelah dipastikan sudah berhasil sinkron antara DNS *server trust* positif Kominfo dan DNS *server* Universitas Pakuan maka langkah selanjutnya yaitu mengaktifkan RPZ *zone trust* positif dan *Blacklist* pada DNS *server* Universitas Pakuan untuk menyimpan data konten negatif pada DNS *Server* UNPAK. Untuk *zone trust* positif dari Kominfo DNS *server* Universitas Pakuan akan menjadi DNS *Slave* untuk menyimpan salinan domain dari *server master* yaitu DNS *server trust* positif Kominfo, sedangankan *zone Blacklist* akan menjadi DNS *Master* bisa dilihat pada gambar 17.

```
zone "trustpositifkominfo"  {
        type slave;
        masters {
                103.154.123.130;
                139.255.196.202;
                };
        file "/etc/bind/rpz/db.trustpositifkominfo";
};

zone "blacklist" {
        type master;
        file "/etc/bind/rpz/blacklist.rpz";
};
```

Gambar 17. Penambahan *Zone* Pada DNS *Server* UNPAK

Pada gambar 17 untuk menambahkan *zone trust* positif dan *zone Blacklist* pada DNS *server* Universitas Pakuan di aplikasi BIND9 dapat dilakukan menambah *script* pada *file* /etc/bind/named.conf.local seperti pada gambar 17 dengan membuat *zone trust* positif dengan type *slave* yang tujuan *master* adalah *ip address* dari *master* DNS *server* trust positif Kominfo yaitu 103.154.123.130 dan 139.255.196.202 dengan tujuan file untuk menyimpan salinan domain *trust* positif dari DNS *server* Kominfo di /etc/bind/rpz/db.trustpositifkominfo dan *zone Blacklist* dengan type *master* dengan dengan tujuan file untuk menyimpan domain yang akan diblokir di /etc/bind/rpz/blacklist.rpz.

4.4.6 Mengaktifkan *Policy Trust* Positif

Setelah menambahkan *zone trust* positif di DNS *server* selanjutnya membuat *policy* untuk proses *filtering* domain pada DNS *server* Universitas Pakuan yang akan diblokir dari *list* domain yang didapatkan dari penambahan zone *trust* positif. Untuk menambahkan *policy* pada DNS *server* bisa dilihat pada gambar 18.

```
response-policy {
        zone "trustpositifkominfo" policy cname trustpositif.unpak.ac.id max-policy-ttl 30 log yes;
        zone "blacklist" max-policy-ttl 30 log yes;
}
```

Gambar 18. Penambahan *Policy* Pada DNS *Server* UNPAK

Pada gambar 18 untuk menambahkan *policy trust* positif pada DNS *server* Universitas Pakuan di aplikasi BIND9 dapat dilakukan menambah *script* pada *file* /etc/bind/named.conf.options seperti pada gambar 18 dengan menambahkan *response-policy* dengan tujuan *zone* dari yang sudah dibuat pada penambahan *zone* yaitu *zone* "trustpositifkominfo" dan *zone "blacklist",* untuk *zone* trustpositifkominfo diubah *record cname* yang *default* nya yaitu lamanlabuh.aduankonten.id menjadi trustpositif.unpak.ac.id. Dengan menambahkan *policy* pada DNS *server* maka secara otomatis list domain yang didapatkan dari Kominfo akan secara otomatis difilter berdasarkan zone yang sudah di dekelarasikan.

4.4.7 Menambahkan Domain secara manual pada DNS *Server* UNPAK

Untuk menambahkan domain yang akan diblokir secara manual pada DNS *server* Universitas Pakuan bisa dilihat pada gambar 19.

```
$TTL  604800
@       IN      SOA     blacklist. root.blacklist. (
                        13
                        604800
                        86400
                        2419200
                        604800 )

;;Masukan domain yang akan diblokir
gading69sip.com.blacklist.       IN      CNAME   trustpositif.unpak.ac.id.
```

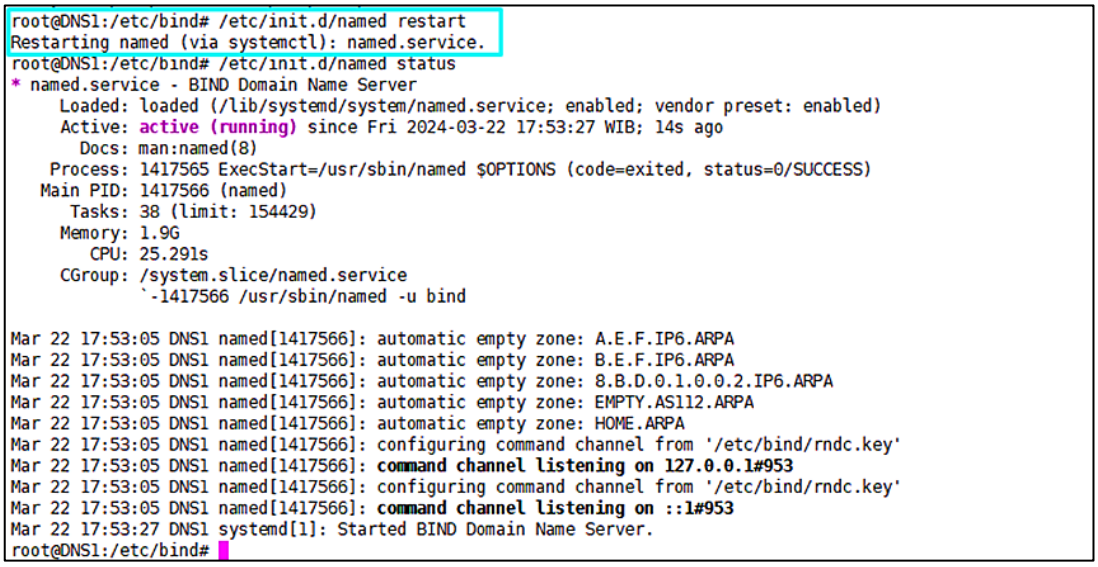
Gambar 19. Menambahkan Domain yang akan diblokir

Pada gambar 19 untuk menabahkan domain yang akan diblokir secara manual pada DNS server Universitas Pakuan di aplikasi BIND9 dapat dilakukan membuat *script* pada *file* /etc/bind/rpz/blacklist.rpz seperti pada gambar 19 dengan memasukan domain yang akan diblokir di paling bawah pada *script* contohnya yaitu

gading69sip.com ditambah dengan kata "*.blacklist*." menjadi "gading69sip.com.blacklist.", selanjutnya ditambah kata "IN" dengan format domain yaitu "CNAME" dan tujuan domainnya yaitu "trustpositif.unpak.ac.id".

4.4.8 *Restart Service* DNS S*erver* Universitas Pakuan

Setelah menambahkan *policy* di DNS *server* selanjutnya adalah *restart service* aplikasi BIND9 pada DNS *server* Universitas Pakuan untuk mengaktifkan *trust* positif yang sudah dikonfigurasikan. Untuk *restart* aplikasi BIND9 dengan memasukan perintah ***/etc/init.d/named restart*** seperti pada gambar 20.

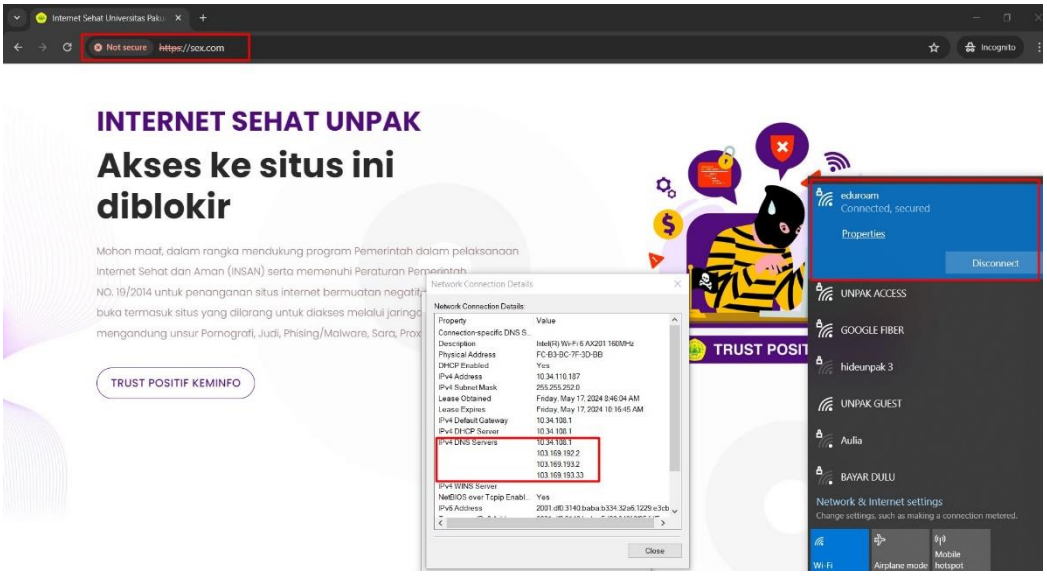


Gambar 20. *Restart* DNS *Server* UNPAK

BAB V
HASIL DAN PEMBAHASAN

5.1 Hasil

Pada bab ini akan membahas hasil Penerapan Metode *Respone Policy Zone* (RPZ) Pada DNS *Filtering Slave Trust* Positif KOMINFO RI berdasarkan analisis dan konfigurasi yang telah diuraikan pada bab 4. Untuk pengecekan konten pornografi dapat di lihat pada gambar 21 seperti berikut :



Gambar 21. Pengecekan Konten Pornografi DNS RPZ

Gambar 21 diatas bisa dilihat saat pengguna internet dengan menggunakan jaringan WiFi eduroam di lingkungan kampus Universitas Pakuan mengakses konten berbau pornografi yang berindikasi sebagai konten negatif akan langsung di blokir dan dialihkan kehalaman tampilan *trust* positif Universitas Pakuan, sebelumnya saat belum diterapkannya filtering dengan menggunakan DNS *server trust* positif masih bisa diakses tanpa terblokir. Seluruh pengguna internet Universitas Pakuan secara otomatis akan menggunakan 3 DNS *server* Universitas Pakuan dengan alamat IP *Address* yaitu 103.169.192.2, 103.169.193.2, dan 103.169.193.33 seperti pada gambar 21.

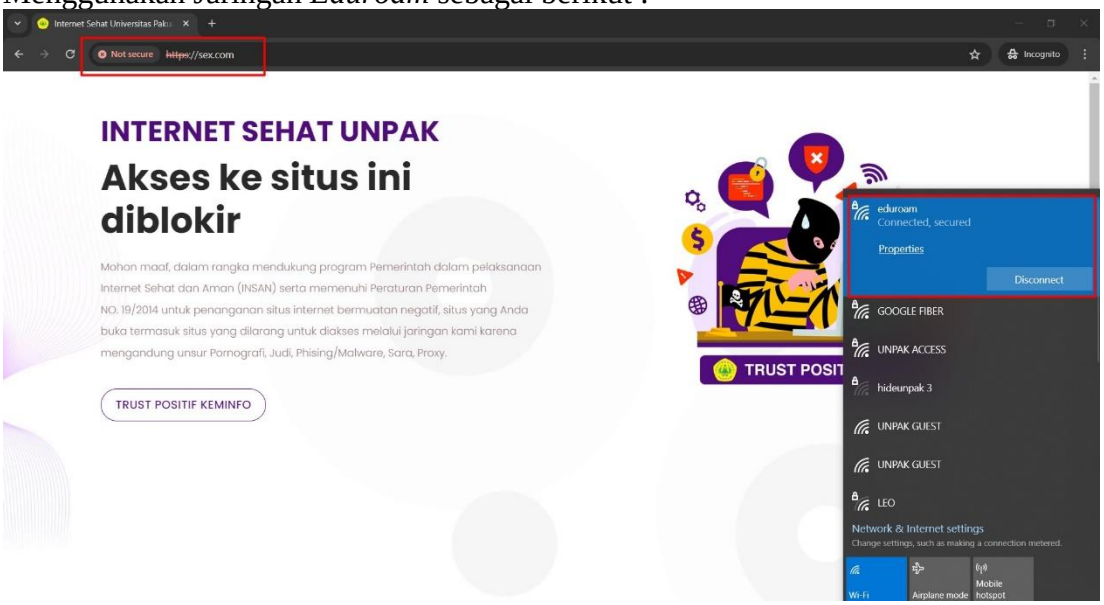
5.2 Tahap Pengujian

Tahap pengujian ini dilakukan untuk memastikan bahwa penerapan Metode *Respone Policy Zone* (RPZ) Pada DNS *Filtering Slave Trust* Positif KOMINFO RI berhasil memfilter konten-konten berbau dengan konten negatif. Pengujian ini dilakukan dengan cara seperti dibawah ini :

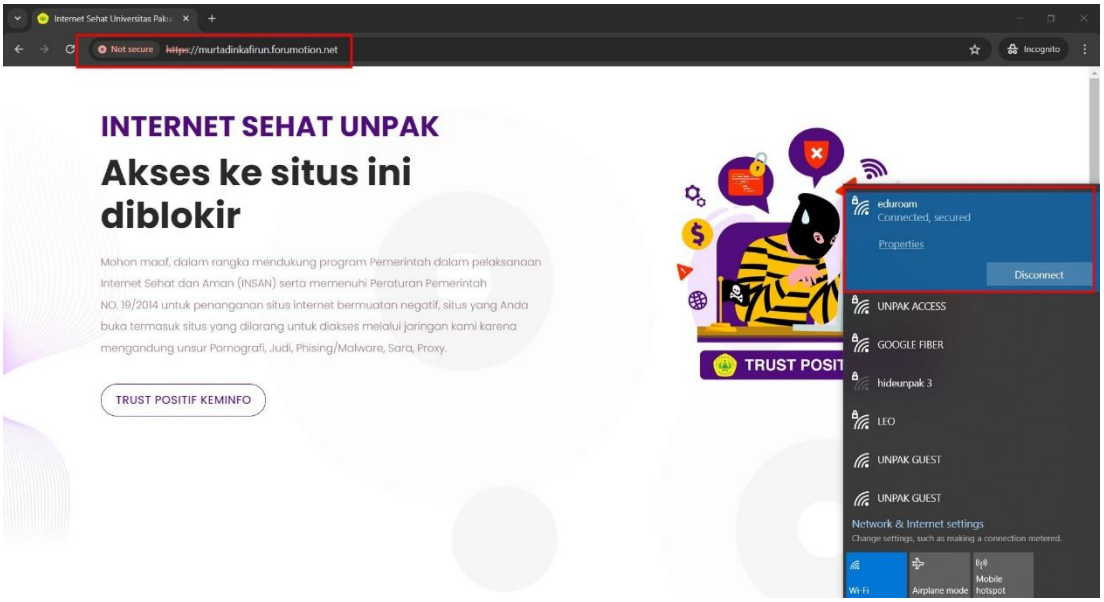
a. Uji Akses *Browser*
   Uji Akses *browser* dilakukan dengan mengakses langsung konten tersebut melalu aplikasi *browser* pengguna internet
b. Uji *Ping*
   Dengan menggunakan *ping*, akan diketahui berapa alamat *IP Address* yang merespon dari situs yang diuji coba.
c. Uji *Nslookup*
   Dengan *nslookup*, dapat diketahui berapa alamat IP dari sebuah nama domain.

5.2.1 Uji Akses *Browser*

Pada tahap ini pengguna internet di Universitas Pakuan akan mengakses konten dengan menggunakan aplikasi *browser* sebagai ujicoba untuk lebih memastikan lagi bahwa pemblokiran berhasil atau tidak. Seperti pada gambar 22 Uji Akses *Browser* Konten Pornografi dan gambar 23 Hasil Test Konten *Browser* SARA Menggunakan Jaringan *Eduroam* sebagai berikut :



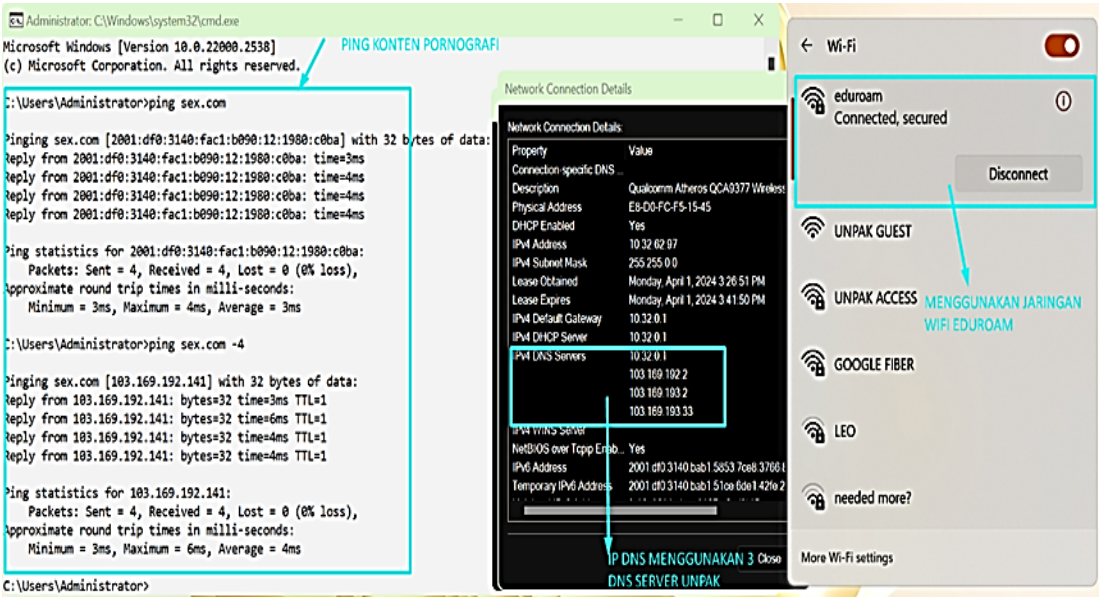
Gambar 22. Uji Akses *Browser* Konten Pornografi



Gambar 23. Hasil Test Konten *Browser* SARA

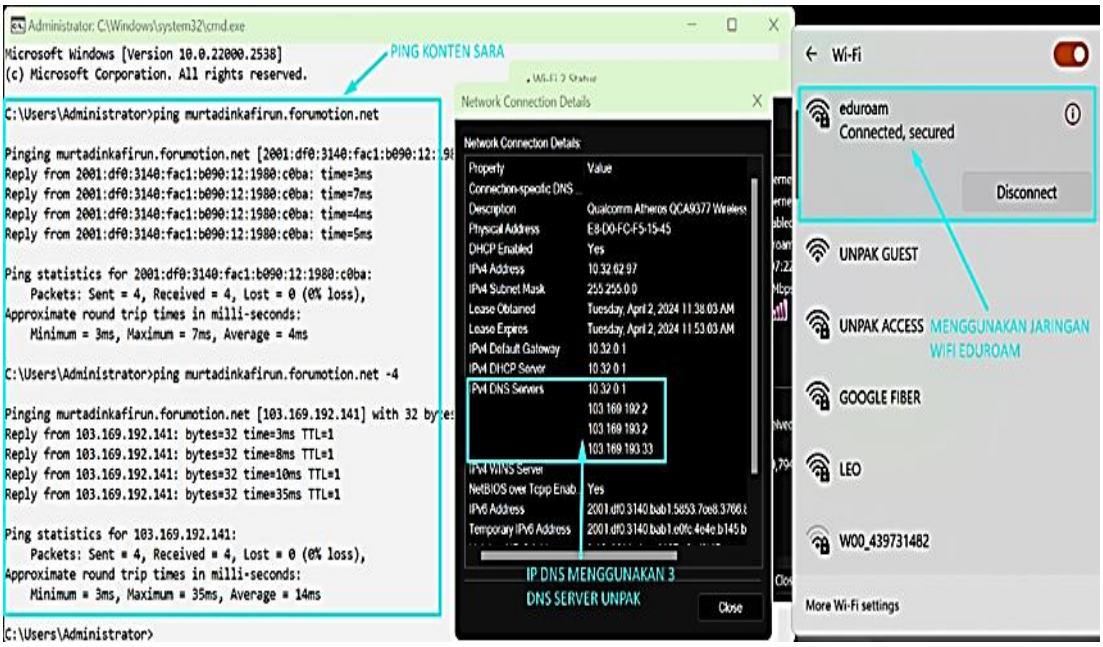
5.2.2 Uji *Ping*

Pada tahap ini pengguna internet di Universitas Pakuan melakukan *ping* menggunakan aplikasi *Command Prompt* (CMD) guna mengetahui respon alamat IP *Address* konten tersebut. Seperti pada gambar 24.



Gambar 24. Hasil Test Konten *Ping* Pornografi

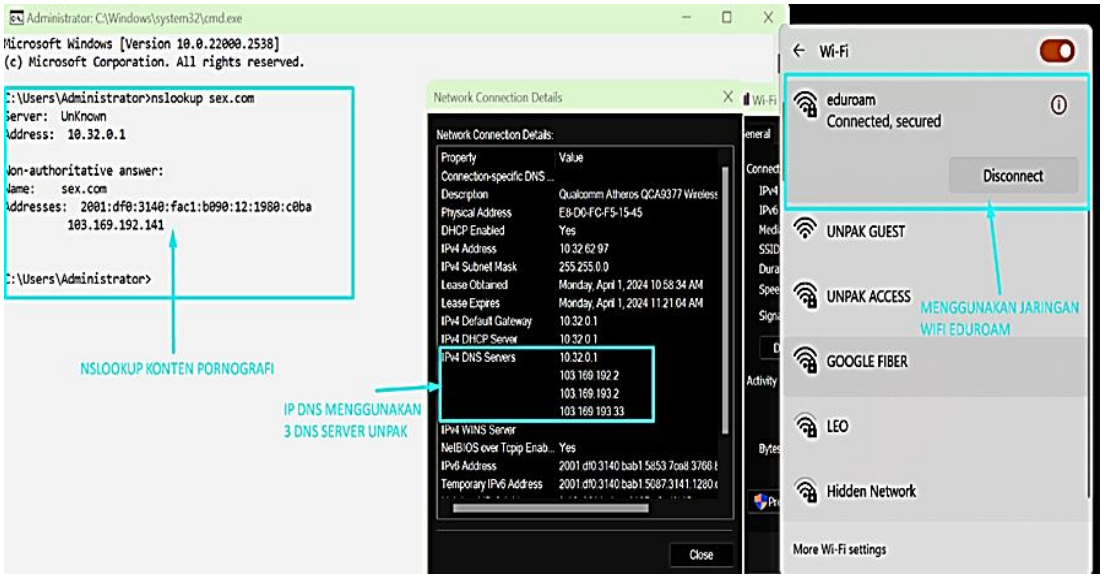
Hasil uji coba *ping* pada gambar 24 diatas menunjukan alamat IP Addres yang merespon konten dari sex.com yaitu adalah 2001:df0:3140:fac1:b090:12:1980:c0ba untuk alokasi IPv6 dan 103.169.192.141 untuk alokasi IPv4 sebagai alamat IP *Address* dari *trust* positif Universitas pakuan. dengan ujicoba *ping* seperti diatas maka secara otomatis konten dari sex.com akan langsung di alihkan ke alamat IP *Address* dari *trust* positif Universitas Pakuan. Hasil Test Konten *Ping* SARA Menggunakan Jaringan Eduroam dapat di lihat pada gambar 25.



Gambar 25. Hasil Test Konten *Ping* SARA

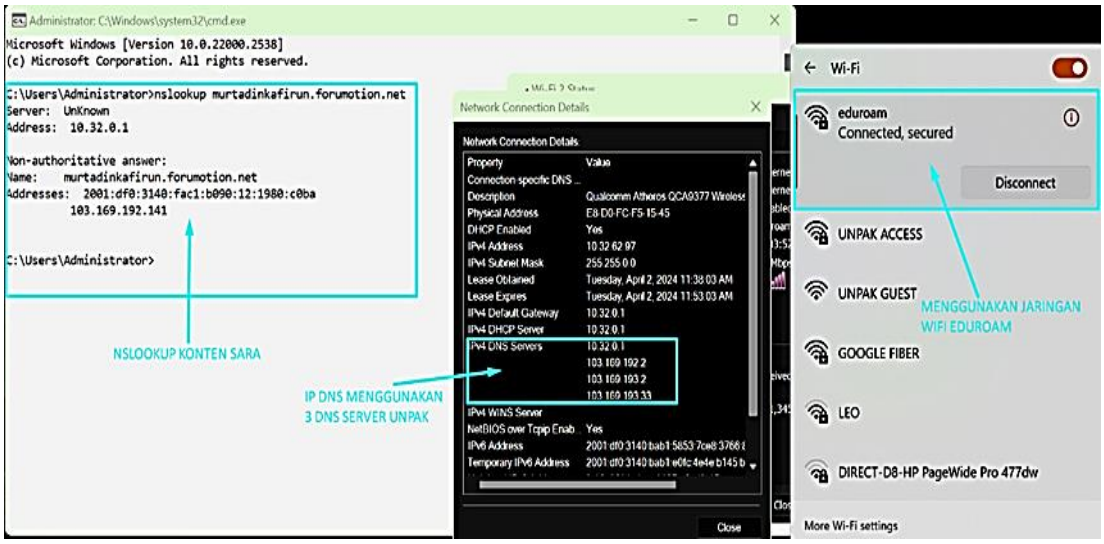
5.2.3 Uji *Nslookup*

Uji *Nslookup* Dengan tool *nslookup* pada aplikasi *Command Prompt* (CMD), dapat diketahui berapa alamat IP dari sebuah nama domain. Hasil uji coba *nslookup* menunjukkan alamat IPv4 dan IPv6 pada konten pornografi seperti pada gambar 26.



Gambar 26. Uji *Nslookup* Konten Pornografi

Hasil uji coba *nslookup* pada gambar 26 menunjukan alamat IP *Address* yang merespon konten dari sex.com yaitu adalah 2001:df0:3140:fac1:b090:12:1980:c0ba untuk alokasi IPv6 dan 103.169.192.141 untuk alokasi IPv4 sebagai alamat IP *Address* dari *trust* positif Universitas pakuan membuktikan bahwa situs tersebut berhasil di blokir. Begitu juga dengan hasil uji coba *nslookup* dengan konten SARA yaitu murtadinkafirun.forumotion.net dengan menggunakan Jaringan Eduroam akan secara otomatis dialihkan kealamat IP *Address* dari *trust* positif Universitas Pakuan yaitu 2001:df0:3140:fac1:b090:12:1980:c0ba untuk alokasi IPv6 dan 103.169.192.141 untuk alokasi IPv4 dapat di lihat pada gambar 27.



Gambar 27. Hasil Test Konten NSLookup SARA

Ketiga tahap pengujian ini dilakukan dari penerapan Metode Respone Policy Zone (RPZ) Pada DNS Filtering Slave Trust Positif KOMINFO RI berhasil dilakukan filtring konten-konten yang mengandung konten negatif dan secara otomatis akan langsung di alihkan ke trust positif Universitas Pakuan.

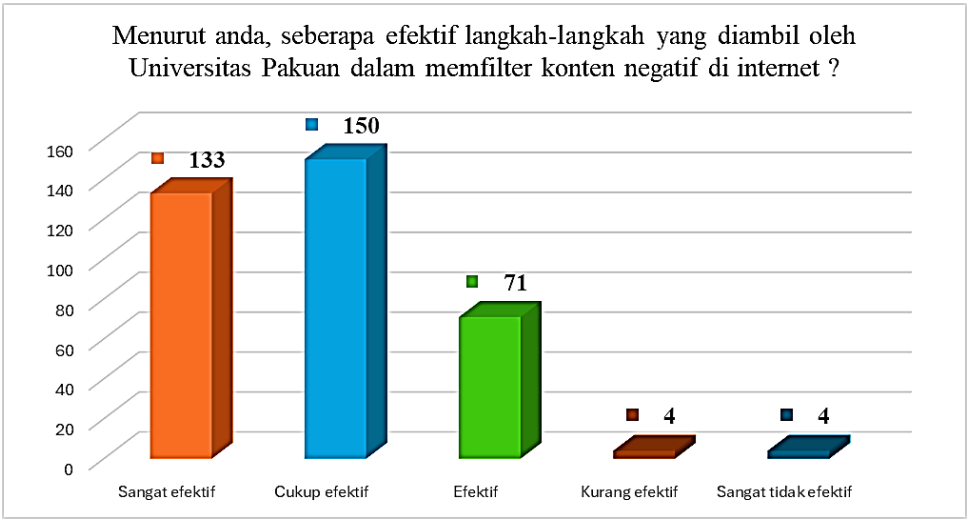
Tabel 2. Hasil Uji *Filtering*

Nama Situs	Parameter Uji		
	Akses *Browser*	***Ping***	***Nslookup***
sex.com	Ya	Ya	Ya
murtadinkafirun.forumotion.net	Ya	Ya	Ya

Dari table 2 hasil uji *Filtering* menggunakan parameter uji akses *browser*, *Ping*, dan *Nslookup* dengan konten yang mengandung *pornografi* yaitu sex.com dan konten yang mengandung SARA yaitu murtadinkafirun.forumotion.net menunjukan berhasil melakukan *filtering* terhadapat konten negatif.

5.2.4 Uji Validasi

Berdasarkan hasil uji validasi menggunakan kuesioner yang disebarkan kepada pengguna internet di Universitas Pakuan, didapatkan sebanyak 362 responden yang terdiri dari mahasiswa, dosen, dan karyawan. langkah-langkah yang diambil oleh universitas dalam memfilter konten negatif di internet dinilai secara positif. Proses pengolahan hasil kuesioner menggunakan perhitungan skala *Likert*, Skala Likert atau Likert Scale adalah skala penelitian yang digunakan untuk mengukur sikap dan pendapat. Dengan skala likert ini, responden diminta untuk melengkapi kuesioner yang mengharuskan mereka untuk menunjukkan tingkat persetujuannya terhadap serangkaian pertanyaan. di mana skor diberikan dari skala 1 hingga 5, menggambarkan penilaian mayoritas responden terhadap efektivitas langkah-langkah tersebut. Dari tabel hasil dibawah ini, terlihat bahwa skor rata-rata berada pada level "cukup efektif" hingga "sangat efektif", menunjukkan bahwa implementasi metode *Response Policy Zone* (RPZ) pada DNS *Filtering Slave Trust* Positif. memberikan kontribusi yang signifikan dalam mengurangi akses terhadap konten negatif. Untuk hasil diagram dari kuesioner bisa dilihat pada gambar 28.



Gambar 28. Diagram *Presentase Efektif* Dalam *Filter* Konten Negatif

Pengolahan hasil kuesioner dilakukan dengan menggunakan perhitungan skala *Likert,* Skor dibuat dari skala 1 sampai 5, untuk perhitungan dengan skala *Likert* bisa dilihat pada tabel 3.

Tabel 3. Hasil Kuisioner

Jawaban	Skor	Skor Maksimum (Skor*Jumlah Responden)
SE : Sangat Efektif	5	133
CE : Cukup Efektif	4	150
E : Efektif	3	71
KE : Kurang Efektif	2	4
STE : Sangat Tidak Efektif	1	4

Rumus : T x Pn
T = Total jumlah responden yang memilih
Pn = Pilih angka skor Likerts

1. Responden Sangat Efektif (5 Skor) : 133 * 5 = 665
2. Responden Cukup Efektif (4 Skor) : 150 * 4 = 600
3. Responden Efektif (3 Skor) : 71 * 3 = 213
4. Responden Kurang Efektif (2 Skor) : 4 * 2 = 8
5. Responden Sangat Tidak Efektif (1 Skor) : 4 * 1 = 4
6. Semua hasil dijumlahkan, total skor = 1.490

Interval Penilaian

1. *Index* 0% - 19.99% : Sangat Tidak Efektif
2. *Index* 20% - 39.99% : Kurang Efektif
3. *Index* 40% - 59.99% : Efektif
4. *Index* 60 % - 79.99% : Cukup Efektif
5. *Index* 80% - 100% : Sangat Efektif

Interpretasi Skor Perhitungan

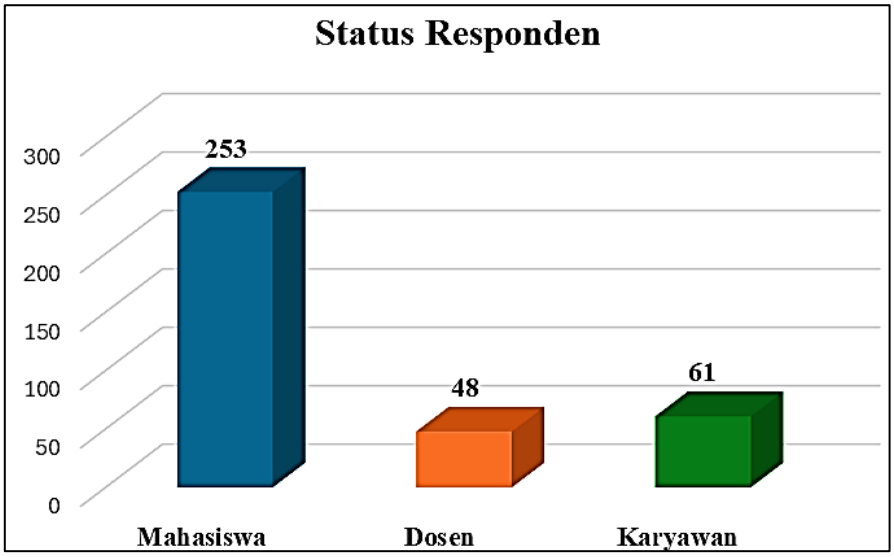
Agar mendapatkan nilai hasil interpretasi, terlebih dahulu harus diketahui skor tertinggi (x) dan skor terrendah (y) untuk item penilaian dengan rumus sebagai berikut :

Y : Skor tertinggi *likert* * Jumlah Responden
X : Skor terendah *likert* * Jumlah Responden
"Sangat Efektif " = 5 * 362 = 1.810
"Sangat Tidak Efektif " = 1 * 362 = 362

Rumus *Index* % = Total Skor / Y * 100

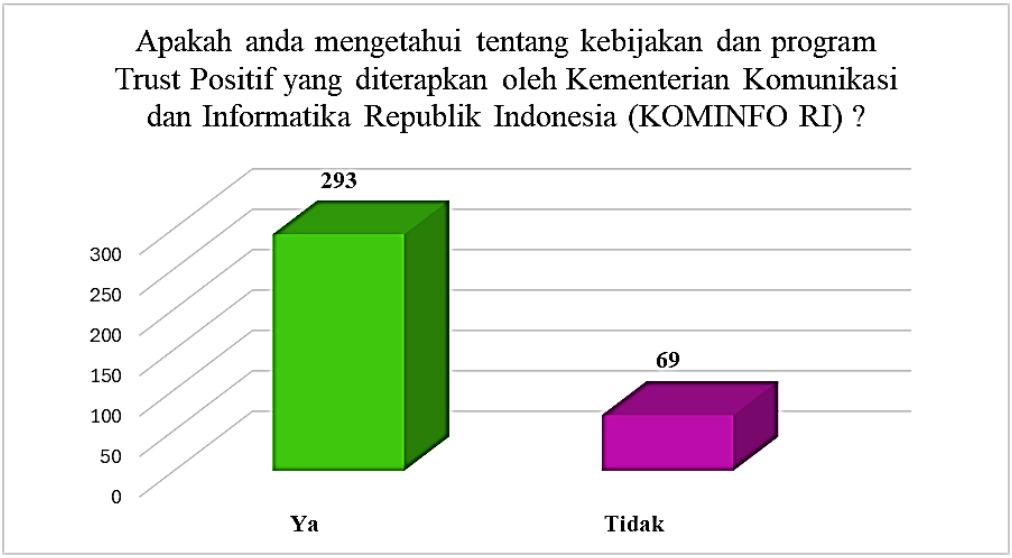
Rumus *Index* % = $\frac{1490}{1810}$ * 100 = **82.32%**

Hasil dari kuesioner menggunakan perhitungan skala *Likert* mendapatkan hasil 82.32% menujukan bawah interval penilaian berada pada *index* Sangat Efektif dalam memfilter konten negatif di internet Universitas Pakuan. Berdasarkan perolehan presentase kuesioner yang telah berpartisipasi untuk mengisi sebanyak 362 *response* terdiri dari mahasiswa, dosen, dan karyawan seperti pada gambar 29.



Gambar 29. Diagram *Presentase* Status *Responden*.

Pada gambar 29 diatas jumlah *responses* yang telah mengisi kuesioner sebagai uji validasi penerapan *trust* positif di Universitas Pakuan sebanyak 362 *response* yang terdiri dari Mahasiswa sebanyak 253 (69,9%), Dosen sebanyak 48 (13,3%) dan Karyawan sebanyak 61 (16,9%). Ada juga pertanyaan yang diajukan didalam kuesioner yang disebarkan disebarkan kepada pengguna internet di Universitas Pakuan, dengan pertanyaan untuk mengetahui seberapa banyak pengguna internet yang mengetahui tentang kebijakan dan program Trust Positif yang diterapkan oleh Kementerian Komunikasi dan Informatika Republik Indonesia, seperti gambar 30.



Gambar 30. Diagram *Presentase* tentang *Trust* Positif KOMINFO

Pada gambar 30 diatas adalah Diagram presentase seberapa banyak yang mengetahui tentang kebijakan dan program *Trust* Positif yang diterapkan oleh Kementerian Komunikasi dan Informatika Republik Indonesia di lingkungan Universitas Pakuan. Dari diagram presentase pada gambar 29 sebanyak 362 *response* yang mengetahui tentang kebijakan dan program *Trust* Positif oleh Kominfo yaitu sebanyak 293 (80,9%), sedangkan yang tidak mengetahui tentang kebijakan dan

program *Trust* Positif oleh Kominfo sebanyak 69 (19,1%). Kesimpulan yang bisa diambil dari Diagram presentase diatas bahwa banyak yang mengetahui tentang kebijakan dan program *Trust* Positif yang telah dibuat oleh Kominfo RI pada lingkungan Universitas Pakuan.

5.2.5 Uji Waktu *Resolve* Konten Negatif

Pengujian waktu *resolve* konten negatif untuk menguji waktu *resolve* DNS untuk konten negatif yang baru saja ditambahkan pada perangkat *smartphone, laptop,* dan PC di dalam jaringan Universitas Pakuan. DNS *Server* merupakan bagian kunci dalam *infrastruktur* internet yang mengonversi nama *domain* menjadi alamat IP *Address* yang terkait. Konten negatif merujuk pada domain yang diblokir oleh DNS Universitas Pakuan. Melalui pengumpulan data waktu *resolve* DNS dari berbagai perangkat di jaringan Universitas Pakuan, penelitian ini bertujuan untuk menganalisis efisiensi *resolve* DNS *Server* untuk konten negatif. Metode pengumpulan data melibatkan pengujian langsung dari perangkat yang terdaftar dalam jaringan Universitas Pakuan menggunakan perangkat lunak khusus. Seperti yang disajikan pada table 4.

Tabel 4. Pengujian waktu resolve perangkat

Data *Collectiong*	**Hari Libur**			**Hari Kerja**		
	Smartphone	**Laptop**	**Komputer**	***Smartphone***	**Laptop**	**Komputer**
Waktu *Capture* (Menit)	30	30	30	30	30	30
Rata rata DNS *Time Response*	9 ms	3 ms	2 ms	11 ms	5 ms	3 ms
Waktu *Resolve* Konten Baru (Menit)	4	2	1	6	3	1

Dari tabel 4 pengujian dilakukan selama 30 menit di waktu hari libur dan hari kerja pada perangkat yang terhubung pada jaringan internet Universitas Pakuan seperti yang tertera pada table 4 dapat disimpulkan perangkat komputer menunjukkan konsistensi dalam kinerja *resolve* DNS yang lebih baik dengan rata-rata response terhadapat DNS *Server* Universitas Pakuan pada hari libur sebesar 2 ms dan hari kerja sebesar 3 ms, diikuti oleh laptop pada hari libur sebesar 3 ms dan hari kerja sebesar 5 ms dan terakhir *smartphone* pada hari libur sebesar 9 ms dan hari kerja sebesar 11 ms. Waktu *resolve* konten baru cenderung lebih cepat pada komputer dibanding laptop dan *smartphone*. Faktor-faktor seperti beban jaringan dan aktivitas pengguna dapat memengaruhi kedua waktu tersebut. Pada hari libur, Komputer menunjukkan respon DNS dan *resolve* konten baru tercepat. Keseluruhan, Komputer lebih unggul dalam kinerja *resolve* DNS dan *resolve* konten baru, baik pada hari libur maupun hari kerja.

5.3 Pembahasan

Penerapan Metode *Respone Policy Zone* (RPZ) Pada DNS *Filtering Slave Trust* Positif Kementrian KOMINFO RI pada jaringan internet Universitas pakuan sangat efektif untuk memfilter konten-konten yang berbau dengan konten negatif seperti yang telah dilakukan pengujian konten negatif dengan uji akses *browser*, uji *ping*, dan uji *nslookup*. Dengan menggunakan DNS *Server* motode *Respone Policy*

Zone (RPZ) sangat efektif dan lebih dinamis dibanding dengan menggunakan *Firewall* di *Router* Mikrotik. Seperti yang disajikan tabel 5.

Tabel 5. Perbandingan Motede *Firewall* dan RPZ

Perbandingan	***Firewall* di *Router* MikroTik**	**DNS *Server* dengan Metode RPZ**
Jenis Blokir	Berbasis IP *Address* dan Nama *Domain*	Berbasis Nama *Domain*
Lokasi *Implementasi*	Pada *router* Mikrotik ditingkat jaringan	Pada *server* DNS di tingkat DNS
Jenis Lalu Lintas yang Dipengaruhi	Seluruh lalu lintas yang melewati *router*	Lalu lintas DNS yang diarahkan ke *server*
Fleksibilitas Manajemen	Perlu penyesuaian manual	Lebih dinamis, konfigurasi melalui rpz
Kesulitan *Implementasi*	Memerlukan pengetahuan konfigurasi *firewall*	Lebih mudah, konfigurasi di dns *server*
Skalabilitas	Terbatas oleh kapasitas dan Kinerja *Router*	Lebih *Skalabel* dengan Peningkatan *Server*
Sistem *Filtering*	Dialihkan ke alamat IP *Address* tujuan	Akan dilihkan ke *record cname* ke *domain* tertentu

Dari tabel 5 bisa disimpulkan bahwa pemblokiran menggunakan DNS *server* motode RPZ lebih unggul dari sisi *Flaksibilitas* dibanding menggunakan *Firewall* di *Router* Mikrotik karena karena DNS *server* motode RPZ memungkinkan pengelola jaringan untuk lebih mudah menyesuaikan dan mengelola daftar situs yang diblokir karena bisa di sinkronasikan dengan sumber yang lebih akurat contohnya disinkronasikan dengan DNS *server Trust* Positif Kominfo RI yang secara otomatis akan terupdate konten-konten sesuai dengan regulasi dari Kominfo RI. sedangkan jika menggunakan *Firewall* di *Router* Mikrotik harus mengubah *konfigurasi* setiap ada konten-konten yang baru pada *settingan firewall* di *router* MikroTik, yang bisa menjadi proses sangat rumit dibanding menggunkan DNS *server* motode RPZ.

BAB VI
KESIMPULAN DAN SARAN

6.1 Kesimpulan

Dengan menerapkan metode *Response Policy Zone* (RPZ) pada DNS *Filtering Slave Trust* Positif di jaringan internet Universitas Pakuan, hasil penelitian menunjukkan efektivitas dalam memfilter konten-konten negatif yang tidak layak, konten berbahaya, dan konten yang merugikan di internet. Pemanfaatan aplikasi BIND9 sebagai aplikasi DNS *Server*, serta metode *filtering* menggunakan *Response Policy Zone* (RPZ), telah terbukti sangat efektif dalam melakukan pemblokiran konten negatif. Dengan sebagai DNS *slave trust* positif dari Kementerian Kominfo RI, sistem dapat memantau konten-konten negatif secara terus-menerus dan memperbarui informasi secara otomatis. Implementasi ini memberikan kontribusi yang signifikan dalam menanggulangi konten berbahaya atau tidak diinginkan, serta menciptakan lingkungan internet yang sehat dan aman di Universitas Pakuan.

Berdasarkan Hasil penelitian dengan kuesioner menggunaka skala *Likert* medapatkan hasil 82,32% dari 362 responden yang terdiri dari mahasiswa, dosen dan karyawan. Jumlah Responden dari Mahasiswa sebanyak 253 responden, Dosen 48 responded, karyawan sebanyak 61 responden. Proses pengolahan kuesioner menggunakan skala *Likert* menunjukkan mayoritas responden memberikan penilaian efektif terhadap langkah-langkah tersebut. Interpretasi skor perhitungan menunjukkan bahwa presentase *interval* penilaian berada pada kategori "Sangat Efektif" mengindikasikan bahwa langkah-langkah tersebut berhasil dalam memfilter konten negatif di internet Universitas Pakuan. Dan didukung dengan pengujian waktu *resolve* terhadap konten-konten baru yang akan diblokir dapat disimpulakan bahwa perangkat komputer menunjukkan konsistensi dalam kinerja *resolve* DNS yang lebih baik, diikuti oleh laptop dan *smartphone*. Waktu resolusi konten baru cenderung lebih cepat pada Komputer. Faktor-faktor seperti beban jaringan dan aktivitas pengguna dapat memengaruhi kedua waktu tersebut, seperti pada hari libur akan lebih cepat dibanding hari kerja. Dengan demikian, penelitian ini memberikan rekomendasi yang penting untuk pengembangan sistem keamanan jaringan di lembaga pendidikan dan organisasi lainnya. Selain itu, hasil penelitian ini juga menyediakan landasan teoritis dan praktis yang berharga bagi penelitian lanjutan dalam bidang keamanan internet, membantu memperkuat infrastruktur keamanan *cyber* di berbagai sektor.

6.2 Saran

Saran dapat difokuskan pada pengembangan lebih lanjut terhadap sistem keamanan jaringan untuk DNS *server* yaitu dengan menggunakan perangkat *Firewall* sebagai perangkat yang berfokus untuk keamanan khususnya kemanan dari DNS *server* itu sendiri baik di dari luar jaringan maupun dari dalam jaringan di Universitas Pakuan. Karena keamanan untuk DNS *server* sangat penting guna menjaga kestabilan internet pada jaringan Universitas Pakuan.

DAFTAR PUSTAKA

Arman Molavi, Yohannes, & Muhammad Ezar Al Rivan. 2022. Pelatihan Membangun *Server* DNS *Local* di SMK Negeri 1 Palembang. VOL 2, NO. 1 TAHUN 2022.

Fauzan Fahmi, Catur Wirawan, & Muhammad Arief. 2021. Implementasi DNS dari Sudut pandangan Efek *Cache* dan *Resolver* Bersama untuk mengurangi beban pada Sistem. Vol.8, No.5 Oktober 2021.

Firmansyah, & Rachmat Adi Purnama. 2019. *Filtering Domain Name Sever* (DNS) untuk Membangun Internet Sehat menggunakan Routerboard Mikrotik. Volume VII, Nomor 1, Mei 2019.

Fujianto ahmad, & Indra Waspada. 2016. Rancang bangun sistem informasi pengelola DNS secara cepat studi kasus CV.Surya Putra Perkasa.

Harsapranata. 2019, "Analisa DNS yang dimanfaatkan dalam filterisasi *domain* di jaringan Lan menggunakan *Open Source*.," J. Ikra-ITH Inform., vol. 3, no. 88, pp. 20–29.

Hidayat Rian, Reza Aldiansyah, Dewa Agung, & Sutriyono. 2023. Optimalisasi DNS Recursive untuk mempercepat pevcarian informasi di internet studi kasus PT. Parsaoran Global Datatrans. *Volume* 1, No. 1, Juni 2023 ISSN 9999−9999 (media online).

Kartika Dina, Riska, & Yessi Mardiana. 2023 Simulasi DNS *Server* dan *Web Server* dengan Sistem Operasi Debian pada Jaringan *Local Area Network*.

Kominfo. Sejarah kominfo.https://www.kominfo.go.id/profil diakses pada tanggal di 04 Maret 2024.

Irawan, Fatoni, 2019. "Internet Positif di Lingkup Perusahaan dengan Metode Response Policy Zone," J. Sist. dan Teknol. Inf., vol. 5, no. 2, p. 6.

Miftahur Rahman.2023. Implementasi *Web Content Filtering* pada Jaringan RT/RW Net Menggunakan Pi-Hole DNS *Server*. /Vol.7 No.1 / e-ISSN: 2549-2233 / p-ISSN: 2580-4952.

Muhlison Sani, & Kusnawi. 2015. Analisa dan Implementasi DNS *Server* sebagai *Filtering* Konten Negatif Menggunakan Motede RPZ (*Response Policy Zone*) di PT. Time Excelindo. Vol. 16 No. 1 Maret 2015, hlm 49-54.

Mulki Pederson, Nurul Fitria, Rizky Elinda, & Zuli Yanti. 2019. Implementasi DNS *Server* pada Sistem Operasi Ubuntu Menggunakan VirtualBox.

Nabil Akhdan, Much. Sobri Sungkar, & Rizal Nur Ependi.2019. Konfigurasi DNS *Server* Berbasis Linuk Ubuntu dengan menggunakan RPZ di SMK Harapan Bersama Tegal.

Niagahoster. Apa itu DNS? Pengertian, Fungsi, Cara Kerja, dan Cara Settingnya https://www.niagahoster.co.id/blog/apa-itu-dns/ diakses pada tanggal di 04 Maret 2024.

Subekti Zaenal Mutaqin, Hendra Setiawan, et al. 2020. Perancangan *Infrastruktur Domain Name Server Local* menggunakan Ubuntu *Server* 16.04 pada PT. XYZ. Vol: 8 no:2.2020.

Sulaksono Danang Haryo, Gusti Eka Yliastuti, Cintra Nurina & I Kadek Agus.2023. Impementasi *Domain Name Server* (DNS) *Spoofing* pada Jaringan Nirkabel. ISSN 2775-5126.

Taluke Dryon, Ricky S. M Lakat & Amanda Sembel. 2019. Analisis Preferensi Masyarakat dalam Pengelolaan Ekosistem Mangrove di Pesisir Pantai Kecamatan Loloda Kabupaten Halmahera Barat. ISSN 2442-3262.

Universitas Pakuan. Sejarah, visi dan misi https://www.unpak.ac.id/profil/tentang-kami/sejarah/ diakses pada tanggal di 04 Maret 2024.

Wijayanti Solikha Nova, Maylane Boni, & Roni Darpono. 2020. Rancang bangun DNS *Server* di SMK NU WAHID HASYIM TALANG menggunakan Linux Debian 7.

LAMPIRAN

Lampiran 1. *Email* Permintaan *List Domain Blacklist Trust* positif Kominfo

3/8/24, 10:30 AM Universitas Pakuan Mail - Re: Permintaan List Domain Blacklist Trustpositif Kominfo

Universitas Pakuan

Azi Heris Saputra <azi@unpak.ac.id>

Re: Permintaan List Domain Blacklist Trustpositif Kominfo

2 messages

Pengendalian Aptika <pengendalianaptika@mail.kominfo.go.id> Fri, Mar 8, 2024 at 9:30 AM
To: Azi Heris Saputra <azi@unpak.ac.id>

Kepada Yth. Bapak Azi Heris Saputra,

Silahkan mengisi form http://bit.ly/FormKoneksiRPZ, setelah 1x24 jam silahkan cek dengan melakukan transferzone ulang ke IP alternatif menggunakan perintah:
dig AXFR @103.154.123.130 trustpositifkominfo +noidnout

Untuk informasi lebih lanjut silahkan menghubungi CP Tim Teknis kami Bapak Okky Robiana Sulaeman di no. HP: 0856-9357-0901.

Demikian disampaikan, atas perhatiannya diucapkan terima kasih.

Direktorat Pengendalian Aplikasi Informatika
Direktorat Jenderal Aplikasi Informatika
Kementerian Komunikasi dan Informatika

From: "Azi Heris Saputra" <azi@unpak.ac.id>
To: pengendalianaptika@kominfo.go.id
Cc: helpdeskdomain@mail.kominfo.go.id, helpdesk@domain.go.id
Sent: Friday, March 8, 2024 8:20:42 AM
Subject: Permintaan List Domain Blacklist Trustpositif Kominfo

Dear Team Kominfo,

Selamat Sore, Saya Azi Admin Jaringan dari Universitas Pakuan Bogor, saya mau bertanya untuk mengenai List Domain yang di Blokir sama trustpositif Kominfo, kebetulan di kampus kami menggunakan DNS server sendiri dan kami sudah menjadi anggota APJII. maka dari itu kami mencari info mengenai List domain yang di Blacklist guna kami terapkan RPZ di DNS kami bisa memblokir domain yang tidak pantas sesuai dengan aturan Kominfo.

Terima kasih.

Best Regards,

Azi Heris Saputra | **Network Engineer**

a: Universitas Pakuan | Jl. Pakuan PO Box 452 Bogor 16143
Jawa Barat Indonesia
e: azi@unpak.ac.id | w: unpak.ac.id
m: + 62 857 7892 2135 | p: +62 251 8312 206

linkedin icon

DISCLAIMER: Perhatian e-Mail ini (termasuk seluruh lampirannya, bila ada) hanya ditunjukan kepada penerima yang tercantum di atas. Jika anda bukan penerima yang dituju, maka Anda tidak diperkenankan untuk menyimpan, menyebarkan, menggandakan, mendistribusikan, atau memanfaatkan e-Mail ini beserta seluruh lampirannya. Jika anda secara tidak sengaja menerima e-Mail ini, mohon kerjasamanya untuk segera memberitahukan ke alamat e-Mail pengirim serta menghapus e-Mail ini beserta seluruh lampirannya. Anda juga harus memeriksa e-Mail ini beserta lampirannya untuk keberadaan virus. Kami tidak bertanggung jawab atas kerugian yang di timbulkan oleh virus yang ditularkan melalui e-Mail ini.

Formulir permohonan koneksi RPZ Kominfo

Mohon diisi formulir ini bagi ISP yang akan melakukan sinkronisasi ke RPZ kominfo

azi@unpak.ac.id Switch account

Draft saved

* Indicates required question

Email *

azi@unpak.ac.id

Nama PT / Badan Usaha *

Nama PT / Badan Usaha

Universitas Pakuan

Brand ISP

Brand koneksi / Market brand dari ISP

Universitas Pakuan

Nama kontak *

Untuk kontak teknis kami sarankan adalah oprasional DNS server pada ISP

085778922135

Email kontak *

azi@unpak.ac.id

Nomor kontak (selular - WA) *

Nomor kontak selular yang dapat dikontak melalui WhatsApp messenger. No kontak ini akan dimasukkan dalam grup teknis sinkronisasi RPZ

085778922135

Data upstream NAP / ISP yang digunakan *

PT.Mora Telematika Indonesia

Alamat IP Publik DNS Server (Jika sudah ada)

RPZ sistem kominfo adalah sebuan DNS server yang berisi sebuah zone yang dapat direplikasi (transfer zone). Untuk dapat melakukan transfer zone, ISP harus terlebih dahulu meregister Source IP yang akan melakukan transfer ke sistem RPZ kominfo. Mohon memasukkan IP yang dimaksud ke dalam dform di bawah ini (maksimal 4 IP). Jika informasi ini belum ada, dapat disusulkan melalui Whatsapp Message ke sdr. Riko Rahmada

IP 1

103.169.192.2

IP 2

103.169.193.2

IP 3

103.169.193.33

IP 4

Your answer

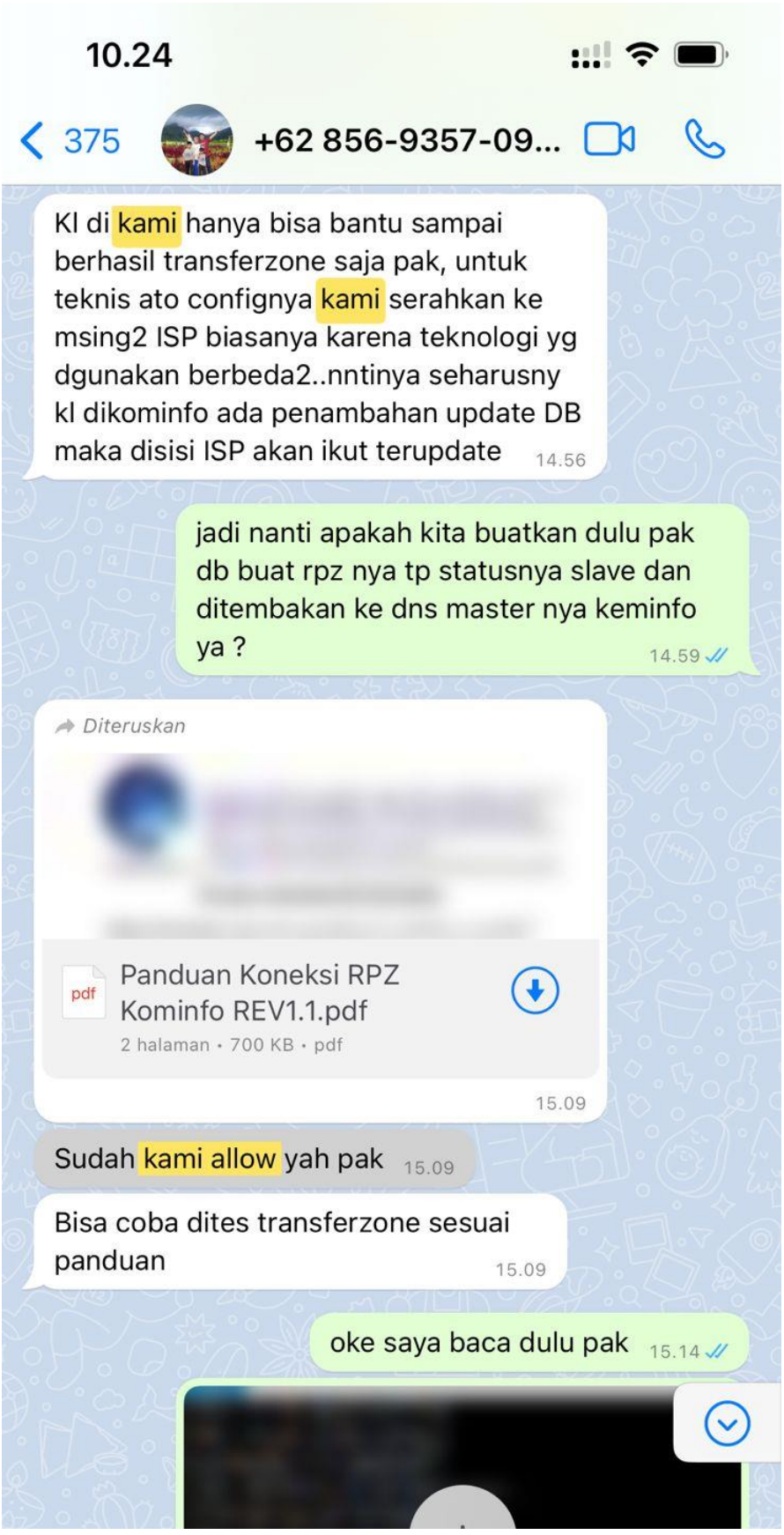
Submit Clear form

Never submit passwords through Google Forms.

This form was created outside of your domain. Report Abuse - Terms of Service - Privacy Policy

Google Forms

Lampiran 3. Konfirmasi Tim Teknis Kominfo



Lampiran 4. SK TUGAS AKHIR

YAYASAN PAKUAN SILIWANGI
Universitas Pakuan
FAKULTAS MATEMATIKA DAN ILMU PENGETAHUAN ALAM
Unggul, Mandiri & Berkarakter Dalam Bidang MIPA

KEPUTUSAN DEKAN
FAKULTAS MATEMATIKA DAN ILMU PENGETAHUAN ALAM
UNIVERSITAS PAKUAN
No. : 152/KEP/D/FMIPA-UP/III/2024

T E N T A N G

PENGANGKATAN PEMBIMBING TUGAS AKHIR
PADA PROGRAM STUDI ILMU KOMPUTER
FAKULTAS MATEMATIKA DAN ILMU PENGETAHUAN ALAM
UNIVERSITAS PAKUAN

DEKAN FAKULTAS MATEMATIKA DAN ILMU PENGETAHUAN ALAM
UNIVERSITAS PAKUAN,

Menimbang :
a. bahwa setiap mahasiswa tingkat akhir Program Strata Satu (S1) harus melaksanakan Tugas Akhir sebagaimana tercantum di dalam kurikulum setiap Program Studi di lingkungan Fakultas MIPA Universitas Pakuan.
b. bahwa untuk pelaksanaan Tugas Akhir diperlukan pengawasan dari pembimbing.
c. bahwa sehubungan dengan point a dan b di atas perlu dituangkan dalam suatu Keputusan Dekan.

Mengingat :
1. Undang-undang RI No.: 20 Tahun 2003 tentang Sistem Pendidikan Nasional.
2. Peraturan Pemerintah No.: 60 Tahun 1999 tentang Pendidikan Tinggi.
3. Statuta Universitas Pakuan Tahun 2022.
4. Surat Keputusan Rektor Nomor: 35/KEP/REK/VIII/2020 tanggal 03 Agustus 2020 tentang Pemberhentian Dekan dan Wakil Dekan Masa Bakti 2015-2020 serta Pengangkatan Dekan dan Wakil Dekan Masa Bakti 2020-2025 di lingkungan Universitas Pakuan.
5. Ketentuan Akademik yang tercantum dalam Buku Panduan Studi Fakultas MIPA, Universitas Pakuan Tahun 2023.

Memperhatikan : Usulan dari Ketua Program Studi Ilmu Komputer FMIPA UNPAK.

M E M U T U S K A N

Menetapkan :

Pertama : Mengangkat pembimbing yang namanya tersebut di bawah ini :
1. Pembimbing Utama : Aries Maesya, S.Kom., M.Kom.
2. Pembimbing Pendamping : Victor Ilyas Sugara, M.Kom.

Untuk membimbing dalam rangka melaksanakan tugas akhir bagi mahasiswa :

Nama	:	Azi Heris Saputra
NPM	:	065120138
Program Studi	:	Ilmu Komputer
Judul Skripsi	:	Penerapan Metode Response Policy Zone (RPZ) Pada DNS Filtering Slave Trust Positif Kementerian Kominfo RI

Jl. Pakuan P.O. Box 452, Bogor 16143, Telp./Fax. (0251) 8375547
Website : https://fmipa.unpak.ac.id

Kedua	:	Kepada para pembimbing diharapkan dapat menjalankan tugasnya sebagai pembimbing dengan sebaik-baiknya.
Ketiga	:	Dalam waktu 1 (satu) bulan setelah diterbitkannya SK ini, mahasiswa wajib melaksanakan Seminar Rencana Penelitian yang diselenggarakan oleh Program Studi Ilmu Komputer dengan dihadiri oleh Pembimbing dan Penguji.
Keempat	:	Dana untuk honorarium pembimbing dibebankan kepada mahasiswa yang ketentuannya diatur oleh Fakultas MIPA.
Kelima	:	Surat Keputusan ini berlaku untuk jangka waktu 1 (satu) tahun sejak tanggal ditetapkan sampai dengan mahasiswa tersebut Lulus Sidang/Ujian Skripsi, dengan ketentuan akan diadakan perubahan/perbaikan sebagaimana mestinya bila dikemudian hari terdapat kekeliruan dalam penetapannya.

Ditetapkan di : Bogor
Pada tanggal : 14 Maret 2024

Dekan,

Asep Denih, S,Kom., M.Sc., Ph.D.

Tembusan :
1. Yth. Ketua Program Studi Ilmu Komputer;
2. Yth. Aries Maesya, S.Kom., M.Kom.;
3. Yth. Victor Ilyas Sugara, M.Kom.;
4. Arsip.

Jl. Pakuan P.O. Box 452, Bogor 16143, Telp./Fax. (0251) 8375547
Website : https://fmipa.unpak.ac.id

Lampiran 5. Kartu Bimbingan Mahasiswa

Kartu Bimbingan Mahasiswa
Program Studi Ilmu Komputer FMIPA - UNPAK

Nama Mahasiswa : Azi Heris Saputra
NPM : 065120138
Judul Skripsi : Penerapan Metode Response Policy Zone (RPZ) Pada DNS Filtering Situs Judi Positif Kemenkominfo RI
Pembimbing Utama : Aries Maesya, M.Kom
Pembimbing Pendamping : Victor Ilyas S, M.Kom

No.	Hari, tanggal	Catatan	Tanda Tangan	
			Pembimbing Utama	Pembimbing Pendamping
1.	Kamis, 7 maret 2024	Bimbingan Proposal 1	1	
2.	Jumat, 8 maret 2024	Bimbingan Proposal 2		2
3.	Jumat, 15 maret 2024	Bimbingan Proposal 3	3	
4.	Minggu, 17 maret 2024	Zoom Pra Sidang Proposal		4
5.	Senin, 22 April 2024	Bimbingan Hasil 1	5	
6.	Kamis, 25 April 2024	Bimbingan Hasil 2		6
7.	Jumat, 3 Mei 2024	Bimbingan Sidang Hasil	7	
8.	Sabtu, 4 Mei 2024	Bimbingan Pra Sidang Hasil		8
9.	Sabtu, 11 Mei 2024	Bimbingan Skripsi 1	9	
10.	Senin, 13 Mei 2024	Bimbingan Skripsi 2		10
11.	Rabu, 15 Mei 2024	Bimbingan Pra Sidang Skripsi	11	
12.				12
13.			13	
14.				14
15.			15	
16.				16
17.			17	
18.				18