SKRIPSI

PENGEMBANGAN PACKET FLOW PARSER UNTUK ANALISIS TRAFFIC PADA JARINGAN TERENKRIPSI

Disusun dan diajukan oleh:

Muhammad Anang Abrar

D121 20 1052

PROGRAM STUDI SARJANA TEKNIK INFORMATIKA

FAKULTAS TEKNIK

UNIVERSITAS HASANUDDIN

GOWA

2024

LEMBAR PENGESAHAN SKRIPSI

PENGEMBANGAN PACKET FLOW PARSER UNTUK ANALISIS TRAFFIC PADA JARINGAN TERENKRIPSI

Disusun dan diajukan oleh

Muhammad Anang Abrar
D121201052

Telah dipertahankan di hadapan Panitia Ujian yang dibentuk dalam rangka
Penyelesaian Studi Program Sarjana Program Studi Teknik Informatika
Fakultas Teknik Universitas Hasanuddin
Pada tanggal 30 Oktober 2024
dan dinyatakan telah memenuhi syarat kelulusan

Menyetujui,

Pembimbing Utama,

Dr. Eng. Muhammad Niswar, S.T., M.IT.
NIP 19730922 199903 1 001

Ketua Program Studi,

Prof. Dr. Ir. Indrabayu, S.T., M.T., M.Bus.Sys., IPM.ASEAN.Eng.
NIP 19750716 200212 1 004

PERNYATAAN KEASLIAN

Yang bertanda tangan di bawah ini :

Nama : Muhammad Anang Abrar

NIM : D121201052

Program Studi : Teknik Informatika

Jenjang : S1

Menyatakan dengan ini bahwa karya tulisan saya berjudul

Pengembangan Packet Flow Parser untuk Analisis Traffic pada Jaringan Terenkripsi

Adalah karya tulisan saya sendiri dan bukan merupakan pengambilan alihan tulisan orang lain dan bahwa skripsi yang saya tulis ini benar-benar merupakan hasil karya saya sendiri.

Semua informasi yang ditulis dalam skripsi yang berasal dari penulis lain telah diberi penghargaan, yakni dengan mengutip sumber dan tahun penerbitannya. Oleh karena itu semua tulisan dalam skripsi ini sepenuhnya menjadi tanggung jawab penulis. Apabila ada pihak manapun yang merasa ada kesamaan judul dan atau hasil temuan dalam skripsi ini maka penulis siap untuk diklarifikasi dan mempertanggungjawabkan segala resiko.

Segala data dan informasi yang diperoleh selama proses pembuatan skripsi, yang akan dipublikasi oleh Penulis di masa depan harus mendapat persetujuan dari Dosen Pembimbing.

Apabila di kemudian hari terbukti atau dapat dibuktikan bahwa sebagian atau keseluruhan isi skripsi ini hasil karya orang lain, maka saya bersedia menerima sanksi atas perbuatan tersebut.

Gowa, 30 Oktober 2024

Yang Menyatakan

Muhammad Anang Abrar

ABSTRAK

MUHAMMAD ANANG ABRAR. *Pengembangan Packet Flow Parser untuk Analisis Traffic Pada Jaringan Terenkripsi*(Dibimbing oleh Muhammad Niswar)

Flow merupakan informasi antara dua *endpoints* yang dihasilkan dengan mengumpulkan *packet* dari kedua *endpoints* tersebut. Informasi pada *flow* berupa fitur-fitur yang dapat digunakan untuk mengenali pola komunikasi dari dua endpoints. Melalui fitur-fitur ini, tingkat kerentanan dari *traffic* dapat deteksi. Metode pendeteksian ini menjadi lebih beguna apabila diaplikasikan pada *traffic* yang dienkripsi, dibanding, proses dekripsi *packet* secara utuh yang memakan biaya komputasi yang tinggi. Informasi pada fitur-fitur *flow* sangat cocok diaplikasikan pada model *machine learning.*Pada penelitian ini, penulis membuat sebuah alat yang dapat mengubah *packet* ke *flow* secara langsung tanpa terlebih dahulu mengumpulkan *packet*.

Penelitian ini bertujuan untuk membuat sebuah sistem yang dapat mengubah *packet* menjadi sebuah *flow* secara langsung dan menguji performa sistem yang telah dihasilkan.

Metode penelitian dilakukan dengan mensimulasikan transmisi *traffic* yang telah dikumpulkan sebagai dataset dengan kecepatan yang berbeda-beda. Dataset didapatkan dengan cara mengumpulkan *traffic* sintetis pada sebuah jaringan terisolasi. Kemudian, dilakukan pengambilan data performa sistem yang telah dibuat yang meliputi penggunaan sumber daya CPU, *memori* dan *flow* yang dihasilkan oleh sistem. Setelah itu, skenario yang sama diberlakukan pada alat Open Argus yang kemudian dilakukan perbandingan performa dan penggunaan sumber daya dari kedua alat tersebut.

Hasil penelitian menunjukkan adanya keunggulan pada alat yang telah dibuat pada sisi penggunaan memori yaitu 0.09% pada sistem yang telah dibuat dan 0.25% pada Open Argus. Hal ini disebabkan oleh perbedaan proses pengeluaran sebuah *flow* dari sistem yang dibuat.

Kata Kunci: Network Flow, Open Argus, Packet

ABSTRACT

MUHAMMAD ANANG ABRAR. *Development of Packet Flow Parser for Traffic Analysis in Encrypted Networks* (Supervised by Muhammad Niswar)

Flow is information between two endpoints that is generated by collecting packets from both endpoints. The information in the flow is in the form of features that can be used to recognize the communication pattern of two endpoints. Through these features, the vulnerability of the traffic can be detected. This detection method becomes more useful when applied to encrypted traffic, rather than the full packet decryption process which is computationally expensive. The information in the flow features is very suitable for application in *machine learning* models.In this research, the author created a tool that can convert packets to flow directly without first collecting packets.

This research aims to create a system that can convert packets into a flow directly and test the performance of the system that has been produced.

The research method is carried out by simulating the transmission of traffic that has been collected as a dataset at different speeds. The dataset is obtained by collecting synthetic traffic on an isolated network. Then, the performance data of the system that has been created is taken, which includes the use of CPU resources, memori and flow generated by the system. After that, the same scenario is applied to the Open Argus tool which is then compared to the performance and resource usage of the two tools.

The results showed an advantage in the tool that has been made in terms of memory usage, which is 0.09% in the system that has been made and 0.25% in Open Argus. This is due to the difference in the process of issuing a flow from the system created.

Keywords: Network Flow, Open Argus, Packet

DAFTAR ISI

DAFTAR GAMBAR

DAFTAR TABEL

DAFTAR LAMPIRAN

KATA PENGANTAR

Assalamualaikum Warahmatullahi Wabarakatuh.

Segala puji dan Syukur kami panjatkan kepadan Allah S.W.T. yang telah memberikan rahmat dan nikmat-Nya. Shalawat serta salam senantiasa tercurahkan kepada baginda Rasullullah *Shallallahu 'Alaihi Wa sallam*. *Alhamdulillahirabbil'aalamiin*, tugas akhir yang berjudul **"Pengembangan Packet Flow Parser untuk Analisis Traffic pada Jaringan Terenkripsi"** ini dapat diselesaikan sebagai salah satu syarat dalam menyelesaikan jenjang Strata-1 pada Departemen Teknik Informatika Fakultas Teknik Universitas Hasanuddin.

Dalam laporan penelitian ini disajikan hasil penelitian terkait judul yang telah diangkat dan telah melewati proses pencarian referensi dari penelitian penelitian terkait berupa jurnal, dokumentasi, maupun situs-situs di internet yang dapat membentuk hasil dari Tugas Akhir ini.

Penulis memahami secara penuh dan sadar bahwa tanpa bantuan dan bimbingan dari berbagai pihak mulai dari masa awal perkuliahan sampai dengan periode penyusunan tugas akhir, akan sangat sulit bagi penulis untuk dapat menyelesaikan Tugas Akhir ini. Sehingga penulis ingin menyampaikan ucapan terima kasih kepada sedalam-dalamnya kepada:

1) Allah *Subhanallahu Wa Ta'ala* atas semua nikmat, karunia dan pertolongan-Nya yang tak terhingga, yang telah diberikan kepada penulis disetiap jengkal proses pembuatan Tugas Akhir ini.
2) Syasmul Qamar dan Arsina Yusuf selaku orang tua penulis yang senantiasa memberikan dukungan, doa dan rasa percaya kepada kepada penulis sehingga penulis bisa mendapatkan kekuatan.
3) Ayusmar Ekananda, saudari penulis satu satunya yang telah memberikan dukungan moral dan material sehingga penulis dapat mengerjakan skripsi ini dengan lancar.
4) Bapak Dr. Eng. Muhammad Niswar, S.T., M.IT. selaku pembimbing yang telah memberikan inspirasi dan masukan kepada penulis selama melakukan penelitian.
5) Bapak Dr. Eng. Ady Wahyudi Paundu, S.T., M.T. dan Iqra Aswad, S.T., M.T. selaku dosen penguji yang telah memberikan masukan serta saran sehingga laporan skripsi ini dapat menjadi lebih baik.

6) Prof. Dr. Ir. Indrabayu, ST., MT., M.Bus.Sys., IPM, ASEAN. Eng., selaku Ketua Departemen Teknik Informatika Fakultas Teknik Universitas Hasanuddin atas bantuan dan bimbingannya selama masa perkuliahan penulis.
7) Bapak Robert dan Ibu Yuanita serta segenap dosen dan staf Departemen Teknik Informatika Fakultas Teknik Universitas Hasanuddin yang telah membantu kelancaran penyelesaian tugas akhir penulis.
8) Kak Rayyan, kak Dita, Adit, Adetta, Fadhlu, kakak-kakak dan teman-teman dari lab CCIE yang menemani peneliti selama melakukan penelitian di dalam lab.
9) Nabila, Mia, Agunawan, Thoriq, Firman, Tasya, dan teman-teman REZOLVER'20 yang tidak dapat saya sebutkan semua, selaku orang orang yang telah membantu penulis dalam menyelesaikan masalah perkuliahan penulis.
10) Umrah sebagai orang yang selalu memberikan dukungan dan bantuan kepada penulis untuk menyelesaikan masalah yang dihadapi penulis.

Akhir kata, penulis berharap semoga Tuhan Yang Maha Esa membalas segala kebaikan dari segala pihak yang terlibat dan telah membantu penulis. Penulis menyadari masih terdapat banyak kekurangan pada penulisan Tugas Akhir ini. Oleh karena itu, penulis dengan senang hati menerima segala kritik dan masukan yang membangun untuk menjadikan Tugas Akhir lebih baik lagi. Semoga Tugas Akhir ini dapat memberikan manfaat dan menambah wawasan bagi semua pihak yang membacanya.

Gowa, 18 Oktober 2024

Muhammad Anang Abrar

BAB I
PENDAHULUAN

1.1. Latar Belakang

Internet telah menjadi pondasi yang mendasari segala aspek kehidupan manusia saat ini. Setiap detiknya jutaan sampai miliaran data dikirimkan ke internet. Seiring pesatnya akses internet, bahaya yang mengintai juga ikut meningkat dengan pesat. Pada tahun 2021 organisasi skala global menerima serangan siber setidaknya sekali dalam 14 detik. Hal ini didukung dengan pertumbuhan bahaya *malware* yang mencapai 1 miliar ancaman setiap harinya(Ogu et al., 2021). Dalam beberapa kasus, malware ditemukan memanfaatkan komunikasi TLS yang terenkripsi untuk menyerang kerentanan sebuah sistem (Kashyap et al., 2023). Maka dari itu untuk menghadapi masalah peningkatan serangan siber diperlukan tindakan pencegahan yang tangkas.

Salah satu solusi yang dapat digunakan sebagai langkah awal pencegahan serangan adalah IDS(Intrussion Detection System). IDS dapat digunakan untuk mengetahui perangkat atau jaringan yang mengalami serangan ataupun yang telah diserang. Pada level yang lebih tinggi, IDS bekerja dengan menangkap data, melakukan *preprocessing* dan kemudian menentukan seberapa mencurigakan sebuah *traffic* (Rodriguez et al., 2022). IDS dapat bekerja dengan cara yang berbeda beda tergantung jenisnya. Secara umum IDS terbagi atas 2 jenis berdasarkan cara analisisnya (Yang et al., 2022). Pertama, Packet-level IDS, bekerja dengan menganalisis *packet* yang diterima. Kedua, Flow-level IDS, bekerja dengan menganalisis *flow*, informasi yang diambil dari komunikasi antara 2 *endpoints*. Packet Flow/Traffic Flow didapatkan dari mengelompokkan *packet* berdasarkan 5 kriteria yaitu IP pengirim, IP penerima, Port pengirim, Port penerima dan protokol transport-nya (Rodriguez et al., 2022). Saat ini, riset Flow-based IDS merupakan topik yang lebih dominan jika dibandingkan dengan Packet-based IDS (Yang et al., 2022).

Flow-based IDS bekerja dengan menerima *packet flow* kemudian menganalisis informasi yang didapatkan dari *packet flow* dari analisis tersebut dapat dihasilkan banyak atribut (Rodriguez et al., 2022). IDS konvensional bekerja dengan mencocokkan pola yang dihasilkan dari analisis *packet* ataupun *flow* yang telah diterima. Tidak adanya aturan universal yang dapat digunakan untuk mengkategorikan sebuah *traffic* berbahaya atau tidak membuat proses filter menjadi lebih sulit dilakukan. Perkembangan teknologi dan penerapan *machine learning* menjadi salah satu pendorong dominannya Flow-level IDS. Dari hasil analisis *traffic flow* tersebut dihasilkan banyak atribut yang dapat digunakan pada *machine learning* untuk penanganan lebih lanjut.

Masalah timbul pada proses pembacaan *packet flow* yang harus dianalisis oleh Flow-level IDS. Pada penelitian Rodriguez (2022) dan Ogu (2019) proses pengambilan *packet flow* dilakukan dengan mengubah file Packet Capture(.pcap) yang sebelumnya telah dikumpulkan. Proses ini masih membutuhkan waktu karena *packet* masih harus dikumpulkan kedalam file Packet Capture(.pcap) yang kemudian dianalisis menggunakan IDS seperti Zeek(dulunya bernama Bro), CICFlowmeter atau Netflow. Atribut yang didapatkan dari IDS akan dianalisis lebih lanjut misalnya pengklasifikasian *benign traffic* atau *attack/malicious traffic*.

Pada penelitian ini, penulis membuat sebuah sistem yang mengumpulkan *packet* dan mengubah *packet* tersebut menjadi *traffic flow*. Traffic *flow* ini akan dianalisis agar diperoleh atribut yang dapat dikelola lebih lanjut. Flow yang dihasilkan dapat disimpan kedalam teknologi *caching* sebagai candangan ataupun digunakan untuk keperluan lainnya seperti pengumpulan dataset.

1.2. Rumusan Masalah

Berdasarkan latar belakang tersebut, diperoleh beberapa masalah yang akan diangkat pada penelitian ini, yaitu:

a. Bagaimana membuat sebuah sistem Packet Flow Parser yang dapat mengubah *packet traffic* menjadi *packet flow*?

b. Bagaimana performa sistem Packet Flow Parser saat menangani *packet* pada kecepatan transmisi yang variatif?

1.3. Tujuan Penelitian

Berdasarkan rumusan masalah yang sebelumnya disebutkan, tujuan penelitian ini yaitu:

a. Membuat sebuah sistem Packet Flow Parser yang dapat mengubah *traffic packet* menjadi *packet flow*.
b. Mengetahui performa sistem Packet Flow Parser saat menangani *packet* pada kecepatan transmisi jumlah yang variatif.

1.4. Manfaat Penelitian

a. Bagi instansi, dihasilkan sebuah Packet Flow Parser yang relevan di ruang lingkup terkait yang dapat digunakan pada sistem IDS atau model klasifikasi.
b. Bagi pembaca umum, dapat mengetaui cara kerja sistem Packet Flow Parser untuk memperoleh data *traffic flow* dalam jaringan.
c. Bagi peneliti, dapat menjadi referensi penelitian selanjutnya.

1.5. Ruang Lingkup

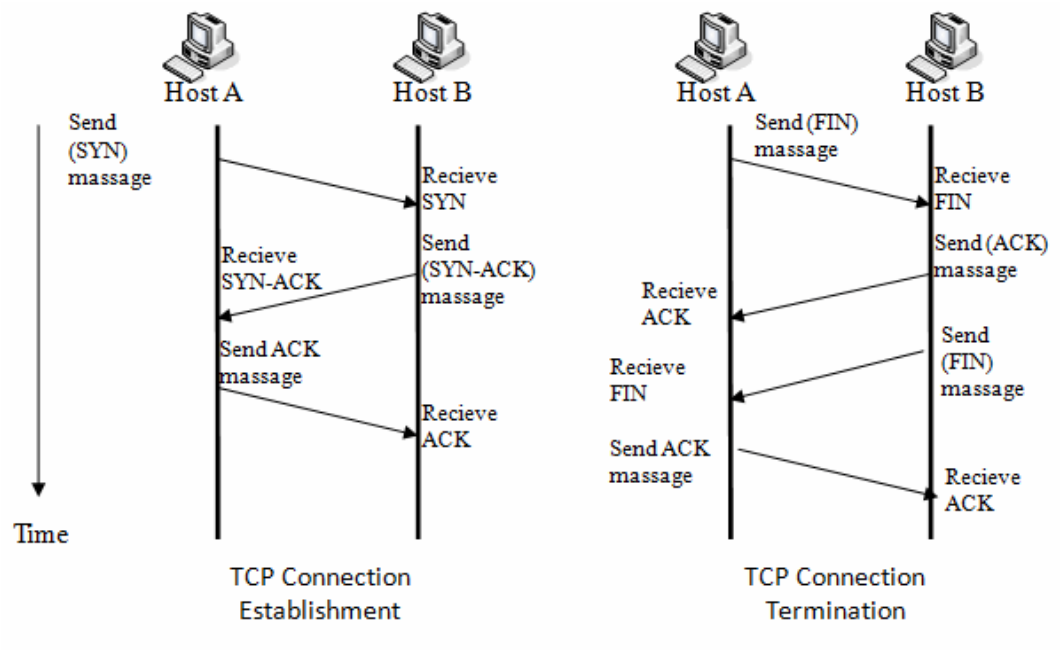
Batasan masalah dari penelitian ini antara lain:

a. Penelitian ini dilakukan menggunakan Jaringan Fakultas Teknik Universitas Hasanuddin sebagai object penelitian.
b. Performa sistem diukur berdasarkan parameter jumlah *packet* loss, penggunaan cpu dan penggunaan memori.

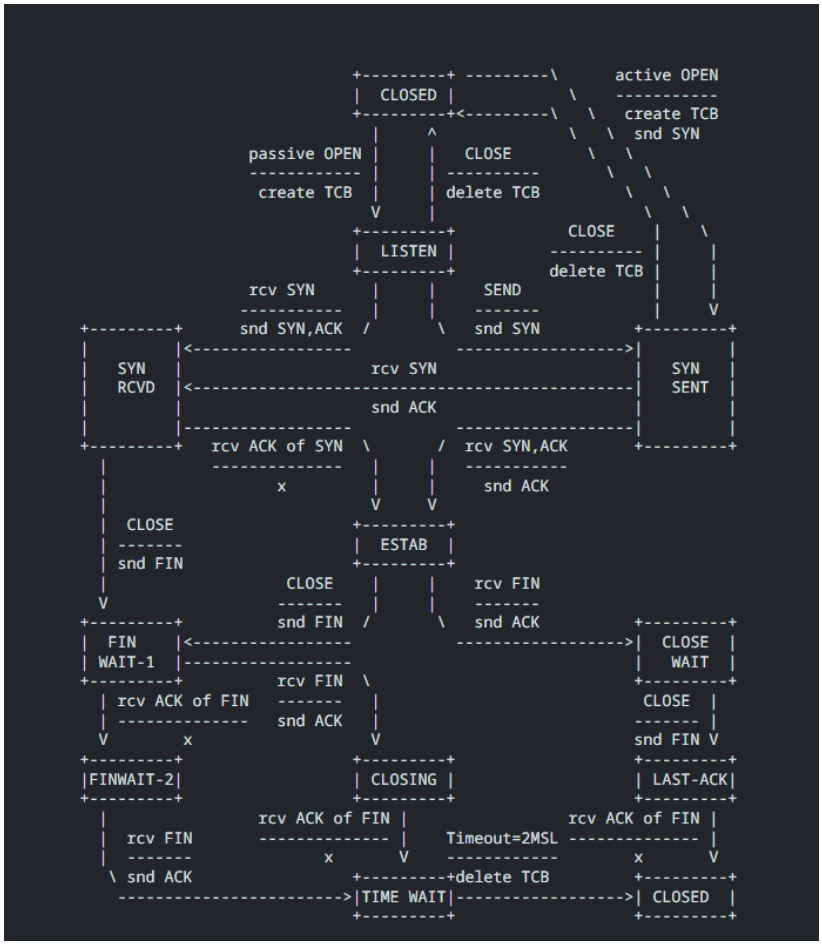
BAB II
TINJAUAN PUSTAKA

2.1. TCP Protocol

TCP(Transmission Control Protocol) pertama kali diperkenalkan oleh Cerf dan Kahn sebagai sebuah protokol yang dapat diandalkan untuk komunikasi antar host dalam jaringan komputer (Transmission Control Protocol, 1981). Protokol TCP digunakan pada arsitektur protokol berlapis dengan berada tepat diatas Internet Protocol(IP).



Gambar 1 Pola Komunikasi TCP



Gambar 2 Pola State Komunikasi TCP

Komunikasi yang menggunakan protokol TCP dimulai oleh host A yang mengirim sebuah *packet* TCP dengan flag SYN yang akan dibalas oleh host B dengan SYN-ACK dan kemudian dibalas kembali oleh host A dengan ACK flag. Pola memulai komunikasi ini sering kali disebut sebagai three way handshake. Sementara itu, untuk mengakhiri komunikasi dengan benar dilakukan oleh host A yang mengirimkan *packet* dengan flag FIN yang kemudian dibalas oleh host B dengan FIN-ACK dan kemudian dibalas oleh host A dengan flag ACK kembali.

TCP tidak selalu menjamin komunikasi sukses dilakukan. Untuk mengatasi hal itu, TCP menggunakan flag RST untuk memberitahu bahwa komunikasi harus dibatalkan. Secara garis besar, flag RST dapat digunakan dalam beberapa kasus, yaitu:

a. Jika koneksi tidak berlangsung atau telah berada dalam CLOSED *state*.
b. Jika koneksi sedang berada dalam keadaan yang tidak tersinkronisasi (LISTEN, SYN-SENT, SYN-RECEIVED) dan menerima ACK *packet*.
c. Jika koneksi dalam keadaan tersinkronisasi(ESTABLISHED, FIN-WAIT-1, FIN-WAIT-2, CLOSE-WAIT, CLOSING, LAST-ACK, TIME-WAIT) dan menerima *segment* dengan nomor *sequence* yang *out-of-window* atau nomor *acknowledgment* yang tidak dapat diterima.

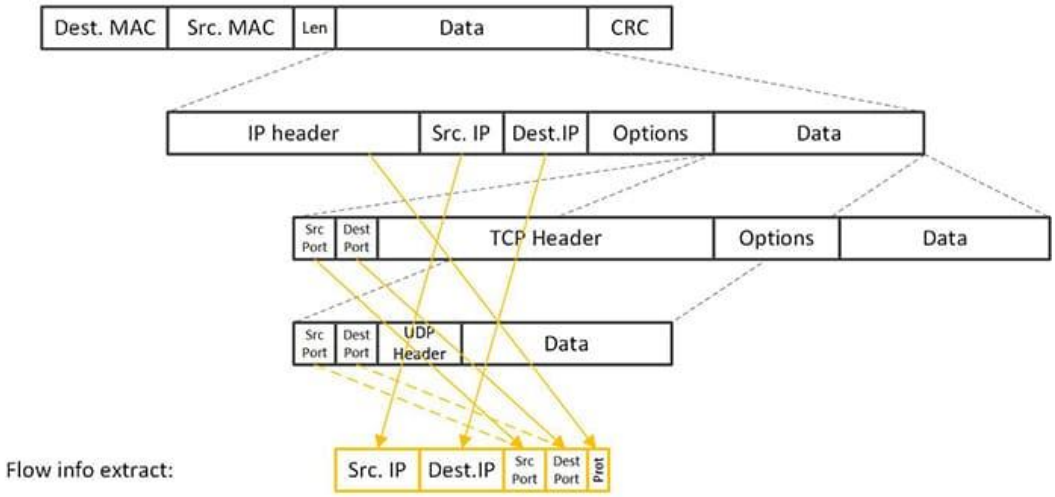
2.2. Transport Layer Security(TLS)

Transport Layer Security(TLS) merupakan protokol yang banyak digunakan untuk kriptografi untuk melindungi komunikasi web maupun surel. Protokol ini memungkinkan *client* dan *server* untuk mengautentikasi satu sama lain dengan kunci kriptografi. Protokol ini memberikan lapisan tambahan yang menyediakan kerahasiaan dan integritas (Dowling et al., 2021).

Informasi pada *payload* umumnya bersifat rahasia sehingga mengakses informasi pada *payload* akan menyalahi aturan privasi. Selain itu, proses dekripsi memerlukan tenaga komputasi yang cukup besar sehingga dapat menghambat proses analisis *packet*. Untuk itu, diperlukan metode lain untuk melakukan analisis ancaman pada jaringan. Salah satu solusi atas masalah ini adalah dengan melihat pola komunikasi pada *flow* jaringan.

2.3. Packet Flow

Packet Flow merupakan sebuah informasi yang dihasilkan dengan mengumpulkan setiap *packet* yang memilik kesamaan berdasarkan 5 atribut yaitu IP asal, port asal, IP tujuan, port tujuan dan protokol transportasi (Rodriguez et al., 2022). Informasi baru dapat dihasilkan dari *packet packet* yang telah dikumpulkan tersebut dengan mengamati pola dan kebiasaan dari komunikasi yang terjadi tanpa melihat isi *payload* dari *packet*.

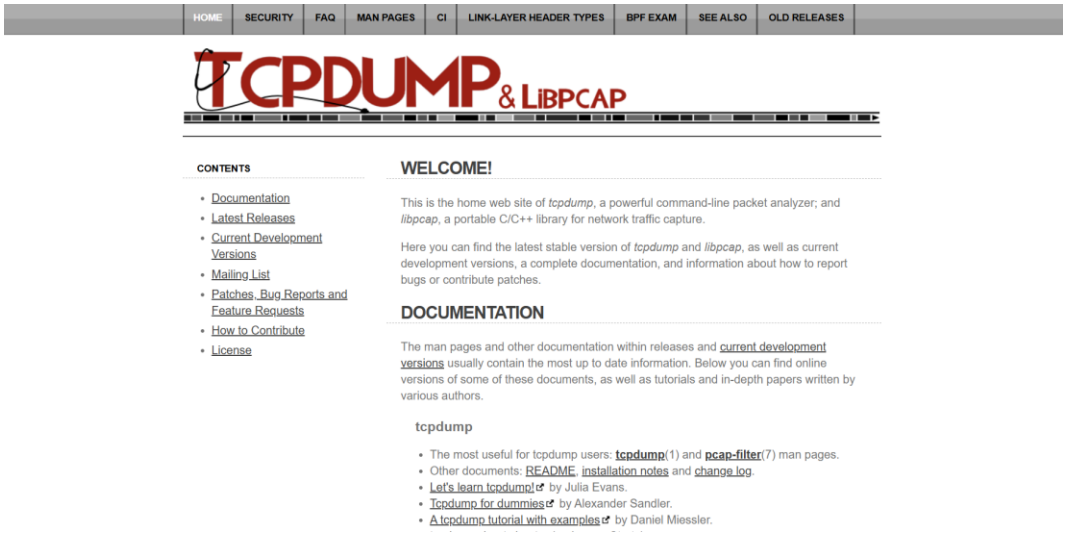


Gambar 3 Informasi pada *flow*

Gambar Menunjukkan skema informasi pada *packet* dengan memecahnya menjadi beberapa lapisan mulai dari lapisan Data Link, lapisan Network dan lapisan Communication. Informasi seperti IP asal, IP tujuan, port asal, port tujuan, dan protokol digunakan untuk mendefinisikan dan membedakan *flow* dengan satu sama lain(Rodriguez et al., 2022). Beberapa alat perangkat lunak yang berfungsi untuk menganalisis informasi dari kumpulan *packet* menjadi *flow* dapat menghasilkan informasi informasi tambahan seperti durasi komunikasi, total *byte* data yang ditukarkan selama komunikasi dan masih banyak lagi.

Informasi informasi yang diberikan *flow* dapat berbeda berdasarkan alat yang digunakan untuk mengekstrak informasi dari kumpulan *packet*. Salah satu alat yang dapat digunakan untuk mengekstrak informasi kumpulan *packet* dan mengubahnya menjadi *flow* adalah Zeek Flowmeter. Zeek Flowmeter dapat mengumpulkan sampai dengan 81 fitur. Beberapa diantaranya adalah durasi komunikasi yang dihitung dari nilai timestamp *packet* pertama pada *flow* masuk hingga *packet* terakhir dari *flow*, juga terdapat informasi seperti jumlah *packet* dan masih banyak lagi.

2.4. Libpcap



Gambar 4 Halaman Beranda TCPDUMP

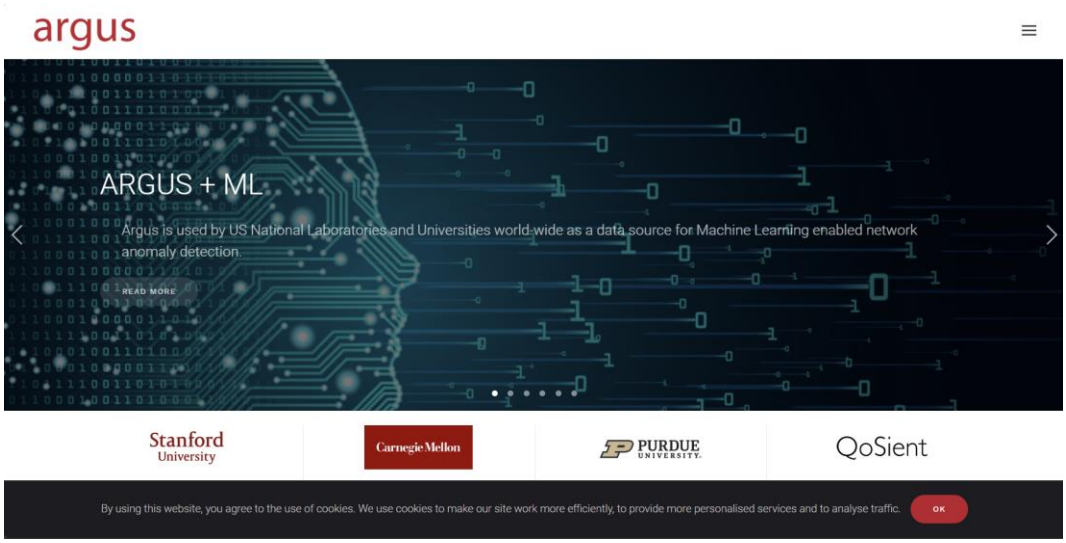
Libpcap merupakan pustaka *packet capture* yang dapat menangkap informasi *packet* pada jaringan yang digunakan pada platform berbasis Unix/Linux. Tcpdump yang merupakan salah satu alat monitor jaringan yang sering kali digunakan pada sistem operasi berbasis Unix/Linux dibuat menggunakan pustaka ini(Wei, 2019).

Libpcap bekerja dengan membuat RawSocket yang menangkap setiap *packet* yang datang. Packet ini diterima dari kartu jaringan yang telah dikonfigurasi ke mode *layer promiscuous* yang membuat kartu jaringan dapat menerima tiap *packet* pada jaringan *host*. Packet yang diterima akan disaring oleh BPF(berkeley *packet* filter) dan kemudian dikirim ke *buffer kernel* Linux(Zhang & Wang, 2019). Datanya kemudian dapat digunakan untuk pemrosesan lebih jauh dengan memindahkannya ke memori.

2.5. Tcpreplay

Tcpreplay adalah sebuah peralatan untuk menulis dan mentransmisikan ulang *packet* berdasarkan *packet* yang sebelumnya telah ditangkap dalam file berformat pcap. Tcpreplay bersifat gratis dan sumber terbuka. Tcpreplay dapat mengirim kembali *packet* dengan konfigurasi tertentu untuk mensimulasikan jaringan yang sebenarnya. Salah satu fungsionalitas Tcpreplay memungkinkan pengiriman *packet* dengan transmission rate yang berbeda beda (Masumi et al., 2021).

2.6. Open Argus



Gambar 5 Halaman Beranda Openargus

Open Argus adalah sebuah peralatan yang berfungsi untuk menganalisis trafik pada jaringan. Argus dikembangkan oleh Carnegie Mellon Software Engineering Institute dan dinyatakan sebagai proyek sumber terbuka sejak tahun 1996 dan didistribusikan di bawah lisensi publik GNU, meskipun hak atas produk dimiliki oleh 34 QoSient LLC. Argus dapat menganalisis *traffic* langsung melalui antarmuka jaringan dan juga dari file pcap(Peterson, 2021). Argus akan mengelola *packet* yang dianalisis dan mengelompokkannnya menjadi sebuah *flow*.

Flow menggambarkan skema komunikasi dan transaksi *packet* antara dua *endpoints* yang saling berkomunikasi. Informasi pada *packet* digunakan untuk menghasilkan informasi pada *flow*. Argus menghasilkan beberapa informasi pada *flow* seperti total data yang ditransfer, IP asal, IP tujuan, port asal, port tujuan, protokol, dan jumlah *packet* yang diterima.