Wireshark & Capture Network.

WIRE SHARK

Contrail One

www.wireshark.com

PENGERTIAN

Wireshark: Network Protocol Analyzer Modern untuk Analisis dan Pemantauan Jaringan

Wireshark merupakan salah satu perangkat lunak analisis jaringan paling populer dan banyak digunakan oleh profesional IT di seluruh dunia. Aplikasi ini memberikan kemampuan untuk menangkap, membaca, dan menganalisis paket data secara rinci sehingga pengguna dapat memahami aktivitas yang terjadi di dalam jaringan komputer. menjelaskan sejarah, fungsi, cara kerja, manfaat, serta alasan mengapa Wireshark menjadi standar dalam dunia analisis jaringan modern.

SEJARAH WIRESHARK

Wireshark adalah aplikasi network protocol analyzer (alat untuk menganalisis paket jaringan) yang pertama kali dibuat oleh Gerald Combs pada tahun 1998.
Awalnya namanya Ethereal, lalu tahun 2006 berganti nama menjadi Wireshark karena masalah hak cipta pada nama sebelumnya.

Perkembangan pentingnya:

1998 → Gerald Combs membuat “Ethereal” dan dirilis sebagai open-source.

2006 → Berganti nama menjadi “Wireshark”, proyek makin besar dengan ribuan kontributor.

2008 → Dipakai secara resmi di banyak perusahaan IT & cybersecurity.

2015 → Wireshark 2.0 rilis dengan tampilan GUI baru

Sekarang → Jadi network analyzer paling populer di dunia, digunakan untuk edukasi, troubleshooting, sampai cybersecurity.

APA ITU WIRESHARK?

Wireshark adalah sebuah aplikasi open-source yang berfungsi sebagai network protocol analyzer, yaitu alat yang digunakan untuk menganalisis lalu lintas data (traffic) yang melewati jaringan komputer. Dengan Wireshark, kita dapat menangkap paket-paket data yang sedang dikirim dan diterima oleh perangkat, kemudian membaca isi dan struktur paket tersebut secara detail. Wireshark tidak hanya menampilkan data mentah, tetapi juga menerjemahkannya ke dalam bentuk yang lebih mudah dipahami. Inilah yang membuatnya sangat berguna untuk troubleshooting jaringan, pembelajaran protokol, hingga penelitian keamanan jaringan. Bahkan, Wireshark menjadi standar industri dan digunakan oleh perusahaan besar, lembaga pendidikan, hingga praktisi keamanan siber.

Wireshark memungkinkan pengguna melihat detail lengkap dari setiap paket, seperti:

- alamat IP sumber dan tujuan
- port yang digunakan
- jenis protokol (TCP, UDP, ICMP, DNS, HTTP, dll)
- ukuran paket
- waktu pengiriman
- proses handshake
- bahkan struktur internal protokol yang sedang berjalan

Fitur inti Wireshark yang paling penting adalah packet capturing, yaitu proses menangkap semua lalu lintas jaringan pada suatu interface (misalnya WiFi atau LAN). Semua paket tersebut kemudian ditampilkan dalam daftar dan bisa dibedah secara detail untuk memahami apa yang terjadi di jaringan.

Karena kemampuannya untuk meng-capture dan menganalisis secara mendalam, Wireshark banyak digunakan di bidang:

- troubleshooting jaringan (mencari error, delay, atau koneksi bermasalah)
- cybersecurity (mendeteksi aktivitas mencurigakan)
- administrasi jaringan
- pengembangan aplikasi yang memakai jaringan
- pendidikan, praktikum jaringan, dan riset teknis

Meskipun mampu menangkap paket, Wireshark tidak bisa melihat isi data yang terenkripsi, seperti pesan WhatsApp, banking, atau HTTPS, namun masih bisa melihat metadata seperti server tujuan dan protokol yang digunakan.

FUNGSI UTAMA WIRESHARK

Wireshark memiliki banyak fungsi penting yang membuatnya menjadi alat wajib bagi mahasiswa, admin jaringan, maupun analis keamanan. Fungsi utamanya adalah untuk menangkap paket data secara real-time dan menampilkan detail isi paket tersebut, termasuk alamat IP pengirim dan penerima, port komunikasi, protokol yang digunakan, ukuran paket, waktu pengiriman, dan berbagai informasi teknis lainnya. Selain itu, Wireshark juga membantu dalam troubleshooting jaringan, misalnya untuk mendeteksi penyebab jaringan lambat, adanya packet loss, atau kesalahan konfigurasi DNS. Dalam bidang keamanan, Wireshark digunakan untuk mendeteksi pola serangan, aktivitas mencurigakan, dan anomali data. Karena sifatnya yang fleksibel, Wireshark juga sering digunakan dalam dunia pendidikan untuk mempelajari protokol seperti TCP, UDP, HTTP, DNS, ARP, dan banyak lagi.

CARA KERJA WIRESHARK

Wireshark bekerja dengan cara:

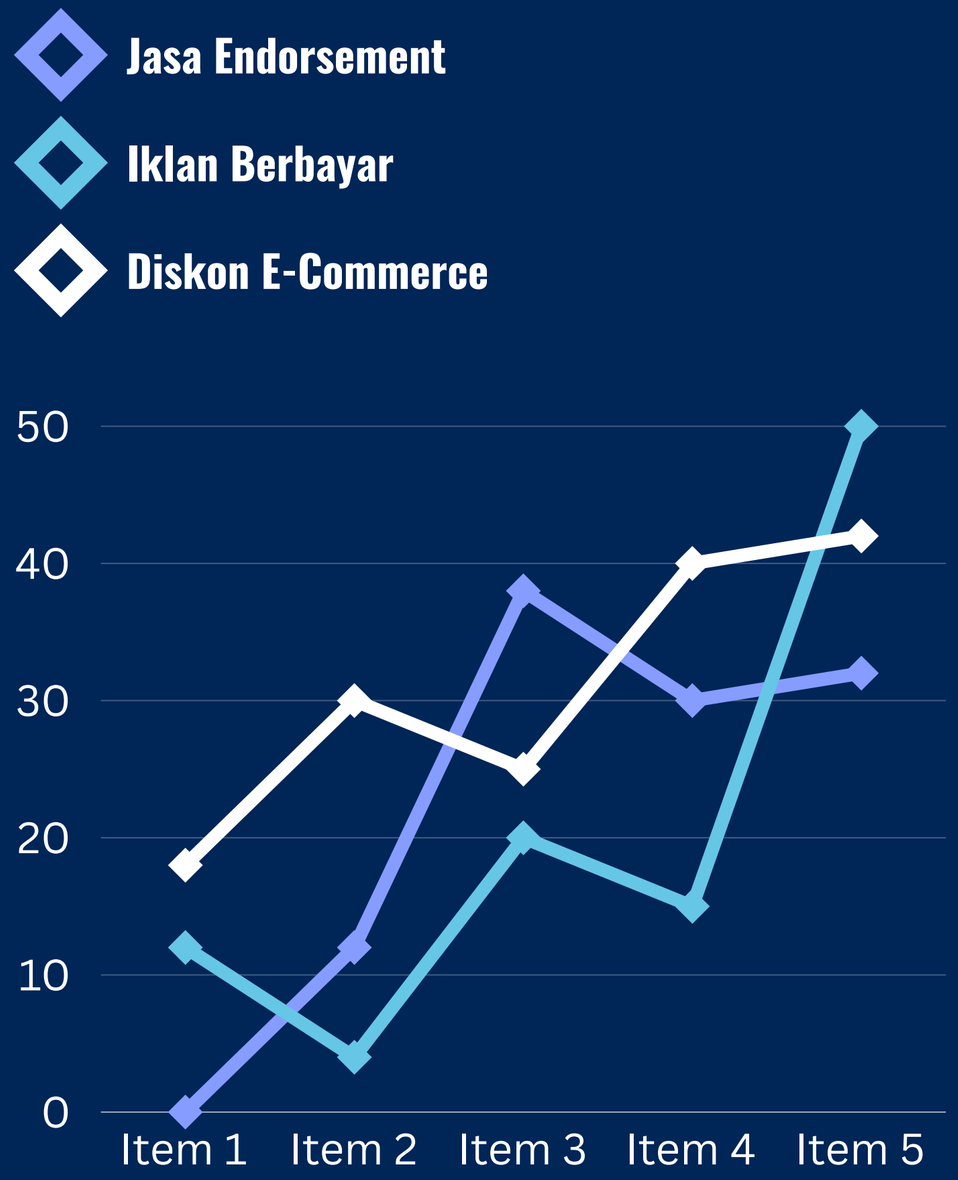
1. **Menangkap paket (packet capture) dari jaringan kamu.**
2. **Bisa dari:**
   - **WiFi**
   - **LAN**
   - **virtual network**
3. **Memecah paket menjadi informasi detail seperti:**
   - **IP sumber & tujuan**
   - **port**
   - **protokol (TCP, UDP, HTTP, DNS)**
   - **panjang paket**
   - **isi paket (jika tidak terenkripsi)**
4. **Menampilkan paket secara real-time dengan warna berb sesuai jenis protokol.**
5. **Merekam dan menyimpan hasil analisis dalam file .pcap.**

Catatan:

Untuk aplikasi yang terenkripsi (WhatsApp, Instagram, Banki Wireshark tidak bisa lihat isi chat, hanya melihat IP server & proto

FITUR UNGGULAN WIRESHARK

1. Real-time packet capture
2. Filter paket sangat detail (Display Filter)
3. Decode ratusan protokol
4. Follow TCP Stream untuk melihat percakapan koneksi
5. Coloring Rules (warna untuk setiap protokol)
6. Grafik I/O untuk melihat kecepatan traffic
7. Export data ke file .pcap, .csv, .txt



PROTOKOL YANG DI DUKUNG WIRESHARK

Wireshark mendukung lebih dari 2.000 protokol jaringan. Protokol-protokol tersebut mencakup protokol transport seperti TCP dan UDP, protokol jaringan seperti IP dan ICMP, protokol aplikasi seperti HTTP, HTTPS, SMTP, DNS, DHCP, FTP, hingga protokol keamanan seperti SSL/TLS. Bahkan protokol komunikasi modern seperti QUIC dan HTTP/2 juga telah didukung oleh Wireshark. Dengan kemampuan decoding protokol yang sangat luas, Wireshark dapat digunakan untuk menganalisis hampir semua jenis komunikasi jaringan modern. Namun demikian, protokol yang dienkripsi seperti WhatsApp, Instagram, dan aplikasi banking hanya dapat dianalisis sebagian karena isi datanya terlindungi oleh end-to-end encryption.

KELEBIHAN WIRESHARK

1. Gratis dan open-source, dapat digunakan tanpa biaya dan terus berkembang oleh komunitas.
2. Fitur sangat lengkap dibanding analyzer lain, termasuk analisis paket real-time dengan detail mendalam.
3. Dipakai luas di industri dan kampus, menjadi standar untuk pembelajaran dan profesional jaringan
4. ribuan protokol, kompatibel dengan hampir semua jenis jaringan modern.
5. Mampu membaca traffic hingga isi paket, berguna untuk troubleshooting dan keamanan jaringan.
6. Memiliki plugin dan filter canggih, memudahkan pencarian paket tertentu dengan cepat.
7. Komunitas dan dokumentasi besar, banyak tutorial, forum, dan panduan belajar.
8. Komunitas dan dokumentasi besar, banyak tutorial, forum, dan panduan belajar.

KEKURANGAN WIRESHARK

Tidak bisa membaca data terenkripsi (WA, Banking, IG)

Wireshark hanya dapat menangkap dan menampilkan paket yang lewat di jaringan, tetapi tidak dapat membuka isi data jika telah dienkripsi menggunakan protokol seperti HTTPS, SSL/TLS, atau end-to-end encryption. Artinya, konten pesan atau data sensitif tidak dapat dilihat secara langsung, hanya metadata dan header tertentu saja.

Butuh skill untuk memahami protokol

Untuk memahami hasil analisis, pengguna harus mengerti konsep jaringan seperti TCP/IP, port, protokol, routing, dan istilah teknis lain. Tanpa pengetahuan tersebut, data yang ditampilkan akan sulit dimengerti dan tidak maksimal digunakan.

Bisa membebani CPU kalau traffic besar

Saat menganalisis jaringan besar atau menangkap paket dalam jumlah sangat banyak, Wireshark dapat memakan banyak sumber daya komputer sehingga membuat sistem menjadi lambat atau bahkan freeze jika hardware rendah.

Akses root/admin diperlukan

Untuk menangkap paket pada level rendah (low-level network access), Wireshark membutuhkan hak akses khusus seperti root (Linux) atau administrator (Windows). Tanpa izin ini, beberapa fitur tidak bisa berjalan.

Tidak mendeteksi serangan otomatis (bukan anti-malware)

Wireshark hanya menganalisis dan menampilkan paket, tetapi tidak secara otomatis mengidentifikasi atau memblokir ancaman keamanan seperti malware, DDoS, atau hacking. Pengguna harus menganalisis sendiri untuk menemukan indikasi serangan.

CONTOH PENGGUNAAN DI DUNIA NYATA

Perusahaan

Untuk mencari masalah jaringan kantor.

Cybersecurity

Untuk analisis malware & serangan jaringan.

Kampus

Untuk praktikum jaringan komputer.

Developer

Untuk debug komunikasi client-server.

Contoh penerapan Wireshark menunjukkan bahwa aplikasi ini bukan hanya untuk keperluan akademik, tetapi sudah menjadi alat utama dalam pekerjaan profesional. Mulai dari perusahaan, cybersecurity, hingga developer, semua memanfaatkan Wireshark untuk memahami alur komunikasi jaringan, mengatasi gangguan, dan memastikan keamanan sistem. Dengan demikian, penguasaan Wireshark memberikan nilai tambah besar untuk mahasiswa IT dan praktisi jaringan.

KESIMPULAN

Wireshark adalah alat analisis jaringan yang sangat lengkap dan memiliki peran penting dalam dunia teknologi informasi. Dari sejarahnya yang panjang, fungsinya yang sangat luas, hingga fitur-fiturnya yang mendalam, Wireshark terbukti menjadi alat terbaik untuk memahami lalu lintas jaringan. Aplikasi ini bermanfaat bagi mahasiswa, administrator jaringan, peneliti, hingga analis keamanan. Meskipun memiliki beberapa keterbatasan, terutama pada protokol yang terenkripsi, Wireshark tetap menjadi alat yang tak tergantikan dalam proses pembelajaran dan troubleshooting jaringan. Dengan menguasai Wireshark, kita dapat memahami bagaimana data bergerak, mengapa jaringan bisa bermasalah, dan bagaimana meningkatkan keamanan sistem.

TERIMA KASIH.