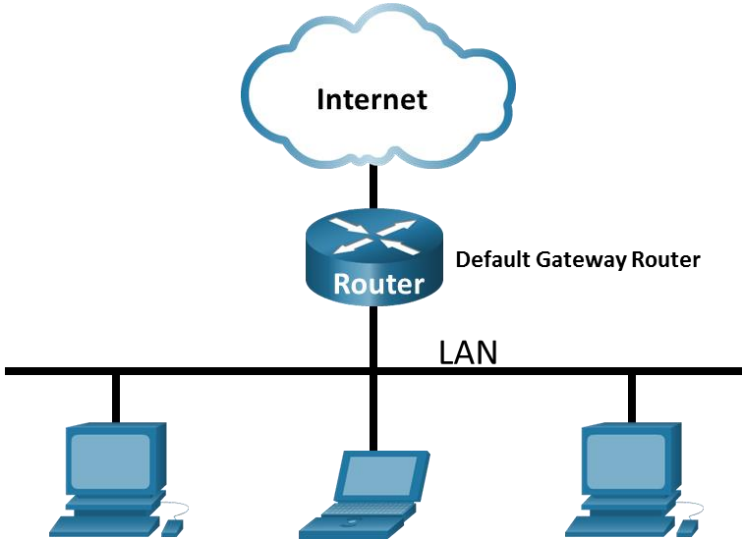
3. Wireshark: Memantau Lalulintas Jaringan

Topologi



Tujuan

- Latihan 1: Download dan Install Wireshark
- Latihan 2: Menangkap dan menganalisis data ICMP lokal dalam Wireshark
- Latihan 3: Menangkap dan menganalisis data ICMP remote dalam Wireshark

Skenario

Wireshark merupakan suatu software *protocol analyzer*, atau aplikasi "packet sniffer", digunakan untuk keperluan network troubleshooting, analisis, pengembangan software dan protokol, dan pendidikan. Karena data stream bergerak maju dan mundur di dalam jaringan, sniffer "menangkap" setiap *protocol data unit* (PDU) dan dapat mendecode dan menganalisis isinya sesuai dengan RFC yang bersesuaian, atau spesifikasi lain.

Wireshark adalah perkakas yang sangat berguna bagi siapapun yang bekerja dengan jaringan dan dapat digunakan pada sebagian besar praktikum kuliah jaringan komputer (*networking*) untuk analisis data dan *troubleshooting*. Aktifitas praktikum kali ini menyediakan instruksi untuk mendownload dan menginstal Wireshark. Selain itu, anda juga akan menggunakan Wireshark untuk menangkap paket data ICMP IP adress dan MAC address frame Ethernet.

Kebutuhan Perangkat

- 1 PC (Windows dengan akses internet)
- PC tambahan di dalam suatu *local-area network* (LAN) akan digunakan untuk membalas (reply) permintaan ping

Wireshark telah menjadi program packet-sniffer standard industri yang digunakan oleh insinyur jaringan. Software *open source* ini tersedia untuk banyak sistem

operasi, ternasuk Windows, Mac, dan Linux. Dalam praktikum ini, anda akan mendownload dan menginstal software Wireshark pada PC yang digunakan.

Catatan: Sebelum mendownload Wireshark, bersama Asisten praktikum, pastikan kebijakan mengenai download dan install software dari lab yang digunakan.

Pemanfaatan suatu packet sniffer seperti Wireshark dapat dianggap sebagai *breach of the security policy* dari kampus. Dianjurkan anda telah memperoleh ijin sebelum menjalankan Wireshark untuk kegiatan lab ini. Jika penggunaan packet sniffer seperti Wireshark merupakan masalah maka asisten praktikum boleh menugaskan kegiatan praktik ini sebagai tugas rumah atau memperlihatkan suatu demonstrasi *walk-through*.

Latihan 1: Download dan Install Wireshark

Langkah 1: Download Wireshark.

1. Wireshark dapat didownload dari **www.wireshark.org**.
2. Pilih versi software yang diperlukan berdasarkan pada arsitektur dan sistem operasi PC. Sebagai contoh, jika anda memiliki PC 64-bit yang menjalankan Windows, maka pilihlah **Windows Installer (64-bit)**.

   Setelah membuat pilihan, download dapat dimulai. Lokasi penyimpanan dari file yang terdownload tergantung pada browser dan sistem operasiyang digunakan. Pada pengguna Windows, lokasi defaultnya adalah folder **Downloads**.

Langkah 2: Install Wireshark.

1. File yang sudah terdownload bernama **Wireshark-win64-x.x.x.exe**, dimana **x** merepresentasikan nomor versi jika anda mendownload versi 6 4bit. Double-click file tersebut agar proses instalasi mulai berjalan.

   Silakan memberikan respon sesuai dengan pesan keamanan yang tampil pada layar anda. Jika anda telah mempunyai salinan Wireshark pada PC, akan anda memperoleh pemberitahuan untuk meng-uninstall versi lama sebelum instalasi versi baru. Direkomendasikan anda menghapus versi lama sebelum menginstal versi lainnya. Klik **Yes** untuk meng-uninstall versi sebelumnya dari Wireshark.
2. Jika ini adalah kali pertama anda menginstal Wireshark, atau setelah proses uninstall selesai, anda akan menavigasi panduan Wireshark Setup. Klik **Next**.
   a. Tetap lanjutkan proses instalasi. Klik **I Agree** ketika jendela License Agreement tampil.
   b. Biarkan setingan default pada jendela Choose Components dan klik **Next**.
   c. Pilih opsi shortcut yang diinginkan dan klik **Next**.
   d. Anda dapat mengubah lokasi instalasi Wireshark, tetapi jika anda mempunyai ruang disk terbatas, direkomendasikan tetap memilih lokasi default. Klik **Next** untuk melanjutkan.
   e. Untuk menangkap data jaringan live, Npcap harus diinstal juga. Jika Npcap telah terinstal pada PC anda, kotak cek Install akan tidak dicentang. Jika versi Npcap yang terinstal lebih lama daripada versi yang hadir bersama dengan Wireshark, direkomendasikan anda mengjinkan versi lebih baru diinstalkan dengan men-klik kotak cek **Install Npcap x.x.x** (nomor versi). Klik **Next**.

f. **JANGAN** install USBPcap untuk menangkap trafik normal. **JANGAN memilih checkbox untuk menginstall USBPcap**. USBPcap bersifat eksperimental, dan dapat menyebabkan masalah USB pada PC Anda. Klik **Install** untuk melanjutkan.

   Wireshark memulai penyalinan file-file dan menampilkan status instalasinya.

g. Pada jendela terpisah, terimalah kesepakatan lisensi dalam Npcap Setup Wizard jika menginstal Npcap. Klik **I Agree**. Klik **Install** untuk segera menginstall Npcap. Klik **Next** untuk menyelesaikan instalasi Npcap dan klik **Finish** untuk keluar dari instalasi Npcap.

h. Klik **Next** pada saat instalasi Wireshark selesai.

i. Klik **Finish** untuk menuntaskan proses instalasi Wireshark. Reboot komputer jika diperlukan.

Latihan 2: Menangkap dan Menganalisis Data ICMP Lokal

Dalam latihan ini, anda akan melakukan ping PC pada LAN dan meng-capture *requests* dan *replies* (permintaan dan balasan) ICMP dalam Wireshark. Anda juga akan melihat frame-frame yang tertangkap untuk mengetahui informasi spesifik. Analisis ini akan membantu memastikan bagaimana header paket digunakan untuk men-transport-kan data ke tujuannya.

Langkah 1: Mengambil alamat antarmuka PC

Untuk kegiatan praktikum kali ini, anda perlu mengambil IP address PC dan alamat fisik dari *network interface card* (NIC)-nya yang dinamakan juga sebagai MAC address.

Buka jendela command prompt.

1. Dalam jendela command prompt, masukkan **ipconfig /all**, untuk mendapatkan IP address dari interface PC, deskripsinya, dan MAC (*physical*) address.

```
C:\Users\Student> ipconfig /all

Windows IP Configuration

   Host Name . . . . . . . . . . . . : DESKTOP-NB48BTC
   Primary Dns Suffix  . . . . . . . :
   Node Type . . . . . . . . . . . . : Hybrid
   IP Routing Enabled. . . . . . . . : No
   WINS Proxy Enabled. . . . . . . . : No

Ethernet adapter Ethernet:

   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . : Intel(R) 82577LM Gigabit Network Connection
   Physical Address. . . . . . . . . :00-26-B9-DD-00-91
   DHCP Enabled. . . . . . . . . . . : No
   Autoconfiguration Enabled . . . . : Yes
   Link-local IPv6 Address . . . . . : fe80::d809:d939:110f:1b7f%20(Preferred)
   IPv4 Address. . . . . . . . . . . : 192.168.1.147(Preferred)
```

```
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 192.168.1.1
<output omitted>
```

2. Tanyakan kepada anggota tim praktikum anda, berapa IP address dari PC mereka, berikan juga IP address PC anda kepada mereka. Jangan berikan MAC address anda sekarang!

   Tutup jendela Command Prompt.

Langkah 2: Jalankan Wireshark dan Tangkap Data Jaringan

1. Jelajahlah Wireshark. Klik dua kali interface yang ingin mulai ditangkap paket datanya. Pastikan interface tersebut mempunyai lalulintas (trafik).
2. Informasi akan mulai memutar ke bawah bagian atas dalam Wireshark. Baris-baris data akan muncul dalam warna berbeda berdasarkan pada protokol.

   Informasi ini dapat bergulung dengan sangat cepat tergantung pada komunikasi apa yang terjadi antara PC dan LAN anda. Kita dapat menerapkan suatu filter untuk memudahkan menampilkan dan bekerja dengan data yang sedang ditangkap oleh Wireshark.

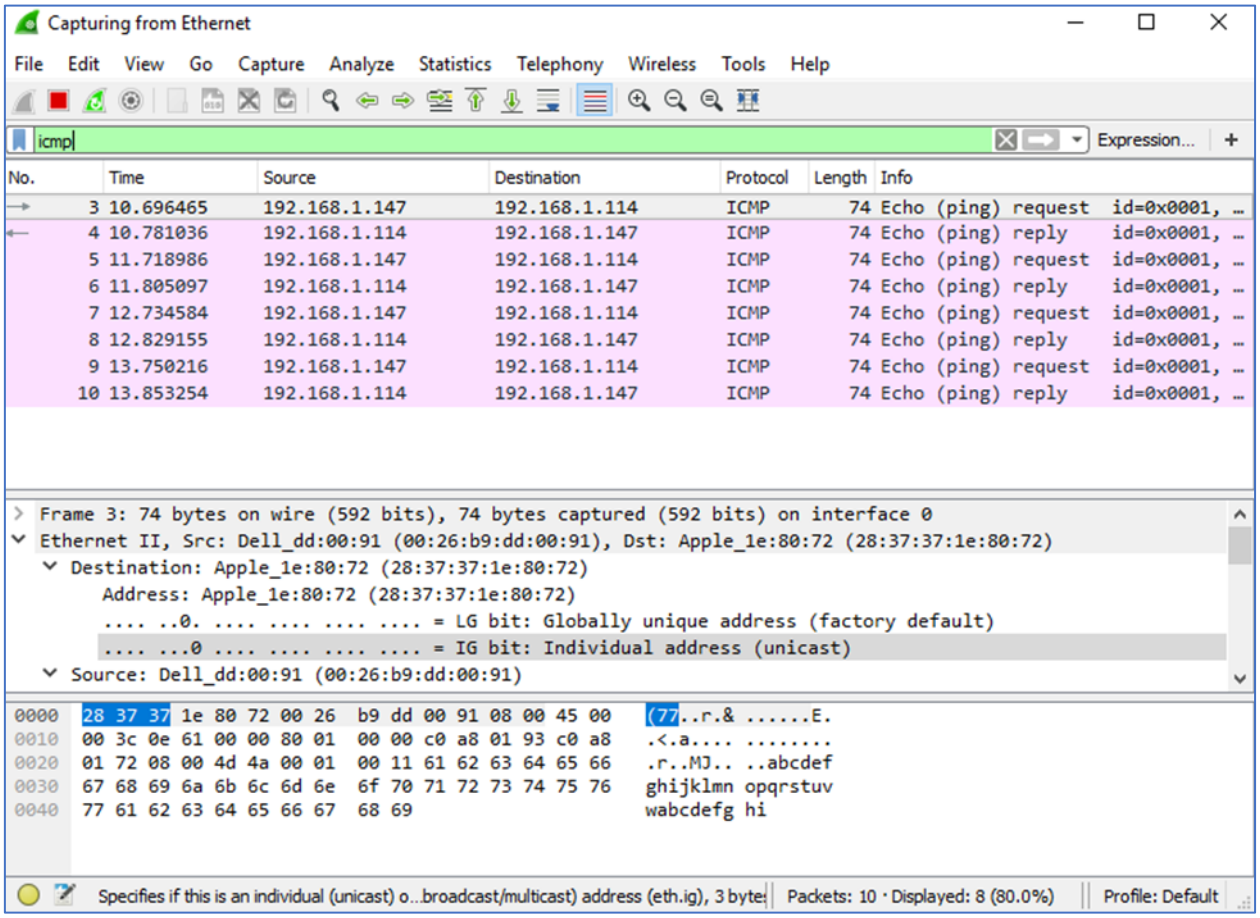
   Untuk praktikum kali ini, kita hanya fokus dalam menampilkan PDU ICMP (ping). Ketik **icmp** di dalam kotak **Filter** pada bagian atas Wireshark dan tekan **Enter,** atau klik tombol **Apply** (tanda paranh) untuk menampilkan hanya PDU ICMP (ping).
3. Filter ini menyebabkan semua data di dalam jendela atas tidak muncul, tetapi anda masih menangkap trafik pada interface tersebut. Beralihlah ke jendela command prompt dan jalankan perintah ping ke IP address yang telah diterima dari anggota tim tadi.

```
C:\> ping 192.168.1.114

Pinging 192.168.1.114 with 32 bytes of data:
Reply from 192.168.1.114: bytes=32 time<1ms TTL=128
Reply from 192.168.1.114: bytes=32 time<1ms TTL=128
Reply from 192.168.1.114: bytes=32 time<1ms TTL=128
Reply from 192.168.1.114: bytes=32 time<1ms TTL=128

Ping statistics for 192.168.1.114:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

Perhatikan, anda mulai melihat lagi data tampil pada jendela atas dari Wireshark.



Catatan: Jika PC dari tim anda tidak membalas (reply) ping anda, ini mungkin karena firewall PC dari anggota tim memblok request ini. Lihatlah Lampiran A: membolehkan trafik ICMP melewati Firewall untuk memperoleh informasi mengenai cara membuka akses ICMP melewati firewall menggunakan Windows.

4. Hentikan proses penangkapan data dengan klik icon **Stop Capture**.

Langkah 3: Memeriksa Data Rekaman

Dalam langkah 3 ini, periksalah data yang telah dibangkitkan oleh request ping dari PC anggota tim. Data Wireshark ditampilkan dalam 3 bagian: 1) bagian atas menampilkan daftar frame PDU yang ditangkap dengan suatu rangkuman dari informasi paket IP yang ditampilkan; 2) bagian tengah menampilkan daftar informasi PDU untuk frame yang terpilih pada bagian atas dan memisahkan frame PDU yang dicapture berdasarkan layer protokolnya; dan 3) bagian bawah menampilkan data mentah dari setiap layer. Data mentah ini ditampilkan dalam bentuk desimal dan heksadesimal.

1. Klik frame PDU request ICMP pertama dalam bagian atas dari Wireshark. Perhatikan bahwa kolom **Source** mempunyai IP address PC anda, dan kolom **Destination** mengandung IP address dari PC anggota tim yang diping.

2. Dengan frame PDU ini masih terpilih dalam bagian atas, beralihlah ke bagian tengah. Klik tanda plus (+) agar baris Ethernet II menampilkan MAC address tujuan dan asal (*destination* dan *source*).

Pertanyaan

1. Apakah MAC address asal cocok dengan interface PC Anda?
2. Apakah MAC address tujuan dalam Wireshark cocok dengan MAC address anggota tim anda?
3. Bagaimana MAC address dari PC yang di-ping diperoleh oleh PC anda?

Catatan: Dalam contoh sebelumnya dari request ICMP yang telah dicapture, data ICMP dibungkus dalam PDU paket IPv4 (header IPv4) yang kemudian dibungkus dalam frame PDU Ethernet II (header Ethernet II) untuk transmisi pada LAN.

Latihan 3: Capture dan Analisis Data ICMP Jauh

Dalam latihan 3 ini, anda akan menjalankan perintah ping terhadap komputer jauh (remote host atau host di luar LAN) dan memeriksa data yang dibangkitkan dari ping tersebut. Anda kemudian akan menentukan apa perbedaan antara data ini dari data yang diperiksa dalam Latihan 2.

Langkah 1: Mulai menangkap data pada interface

1. Mulailah menangkap data lagi.
2. Suatu jendela meminta anda menyimpan data tangkapan sebelumnya sebelum memulai tangkapan lainnya. Tidak harus menyimpan data ini. Klik **Continue without Saving**.
3. Dengan capture aktif, ping tiga URL web site berikut dari jendela command prompt:
   - www.yahoo.com
   - www.cisco.com
   - www.google.com

   Catatan: Ketika anda mem-ping URL di atas, perhatikan bahwa Domain Name Server (DNS) mentranslasi URL ke IP address. Catat IP address yang diterima untuk setiap URL.
4. Anda dapat menghentikan penangkapan data dengan klik icon **Stop Capture**.

Langkah 2: Memeriksa dan menganalisis data dari remote host.

Silakan review data tangkapan dalam Wireshark dan periksa alamat IP dan MAC dari tiga lokasi yang telah diping.

Pertanyaan

1. IP address dari **www.yahoo.com**:
2. MAC address dari **www.yahoo.com**:
3. IP address dari **www.cisco.com**:

4. MAC address dari **www.cisco.com**:
5. IP address dari **www.google.com**:
6. MAC address dari **www.google.com**:
7. Apa yang penting dari informasi ini?
8. Bagaimana informasi ini berbeda dari informasi ping lokal yang anda terima dalam Latihan 2?
9. Mengapa Wireshark menampilkan MAC address dari local host, tetapi tidak MAC address sebenarnya dari remote host?

Lampiran A: Membolehkan Trafik ICMP melewati Firewall

Jika anggota tim anda tidak dapat mem-ping PC anda, mungkin firewall mengunci request tersebut. Lampiran ini mendeskripsikan cara membuatu suatu rule (aturan) dalam firewall untuk mengijinkan request ping masuk ke dalam Windows. Bagian ini juga menjelaskan bagaimana mematikan aturan ICMP baru setelah anda menyelesaikan praktikum.

Latihan A1: Membuat rule *inbound* baru.

1. Beralihlah ke **Control Panel** dan klik pilihan **System and Security** dalam tampilkan Category.
2. Pada jendela **System and Security**, klik **Windows Defender Firewall** atau **Windows Firewall**.
3. Pada sisi kiri dari jendela **Windows Defender Firewall** atau **Windows Firewall**, klik **Advanced settings**.
4. Pada jendela **Advanced Security**, klik pilihan **Inbound Rules** pada *sidebar* kiri dan kemudian klik **New Rule…** pada *sidebar* kanan.
5. Ini menjalankan panduan **New Inbound Rule**. Pada layar **Rule Type**, klik pilihan **Custom** dan klik **Next**.
6. Pada sisi kiri, klik pilihan **Protocol and Ports** dan menggunakan menu drop-down **Protocol Type**, pilih **ICMPv4**, dan kemudian klik **Next**.
7. Pastikan bahwa **Any IP address** untuk kedua IP address *local* dan *remote* terpilih. Klik **Next** untuk melanjutkan.
8. Pilih **Allow the connection**. Klik **Next** untuk melanjutkan.
9. Secara default, rule ini berlaku untuk semua profil. Klik **Next** untuk melanjutkan.
10. Namakanlah rule ini dengan **Allow ICMP Requests**. Klik **Finish** untuk melanjutkan. Rule ini akan mengijinkan anggota tim anda menerima balasan ping dari PC anda.

Latihan A2: Mematikan atau Menghapus Rule.

Setelah menyelesaikan praktikum ini, anda ingin mematikan (disable) atau menghapus aturan yang baru dibuat dalam Latihan A1. Menggunakan opsi **Disable Rule** memungkinkan anda mengaktifkan kembali rule tersebut di kemudian hari. Penghapusan terhadap rule secara permanen menghapusnya dari daftar aguran masuk (*inbound rules*).

1. Pada jendela **Advanced Security**, klik **Inbound Rules** dalam panel kiri dan kemudian cari rule yang telah dibuat sebelumnya.
2. Klik kanan rule ICMP dan pilih **Disable Rule** jika diinginkan. Anda juga dapat memilih **Delete** jika ingin menghapusnya secara permanen. Jika anda memilih opsi ini, anda harus membuat ulang rule untuk mengijinkan balasan ICMP.