**MODUL I**

**CABLING**

1. **TUJUAN**
2. Mampu membuat susunan konfigurasi T568A dan T568B untuk kabel *Unshielded Twisted Pair* (UTP).
3. Mampu memasang kabel UTP pada konektor *Registered Jack* 45 (RJ-45).
4. Mampu membuat kabel UTP jenis *Straight-Through dan Cross-Over*.
5. Memberi pemahaman bagaimana mengkonfigurasikan jaringan dengan protokol TCP/IP dan melakukan *sharing resources*.
6. Mampu memahami konsep PDU *layer* 2 dan *layer* 3.
7. Mampu menganalisa paket *layer* 2 dan *layer* 3 menggunakan *Wireshark*.
8. **DASAR TEORI**
   * 1. Kabel UTP

Kabel UTP (*Unshielded Twisted Pair*) adalah kabel yang terdiri dari 4 pasang dan dipilih sedemikian rupa. Memiliki 4 warna yaitu coklat, *orange*, hijau, dan biru. Adapun pasangannya ada yang berwarna putih atau campuran, misalnya kabel coklat putih dan sebagainya. *Twisted Pair Cable* ini terbagi kedalam 2 jenis diantaranya, *Shielded* dan *Unshielded*. *Shielded* adalah jenis dari kabel UTP yang memiliki selubung pembungkus, sedangkan *unshielded* adalah jenis yang tidak mempunyai selubung pembungkus. Untuk koneksinya kabel jenis ini memakai konektor RJ-45 atau RJ-11[1].

Fungsi kabel UTP yaitu digunakan sebagai kabel jaringan LAN (*Local Area Network*) pada sistem jaringan komputer, dan biasanya kabel UTP mempunyai impedansi kurang lebih 100 ohm, serta dibagi menjadi beberapa kategori berdasarkan kemampuannya sebagai penghantar data[1].

Kategori atau jenis kabel UTP:

1. CAT 1 – Kabel UTP *Category* 1 [Cat1] adalah jenis kabel UTP dengan kualitas transmisi yang terendah, di desain untuk mendukung komunikasi suara analog saja.
2. CAT 2 – Kabel UTP *Category* 2 [Cat2] adalah jenis kabel UTP yang memiliki kualitas transmisi yang lebih baik dibandingkan dengan kabel UTP Cat1, jenis atau kategori ini di desain untuk mendukung komunikasi data dan juga suara digital. Kabel ini bisa mentransmisikan data sampai 4 megabit/detik.
3. CAT 3 – Kabel UTP *Category* 3 [Cat3] adalah kabel UTP dengan kualitas transmisi yang lebih baik dibandingkan dengan kabel UTP *Category* 2, jenis atau kategori ini di desain untuk mendukung komunikasi data dan suara pada kecepatan hingga 10 megabit per detik.
4. CAT 4 – Kabel UTP *Category* 4 [Cat4] adalah suatu jenis kabel UTP dengan kualitas transmisi yang jauh lebih lebih baik jika dibandingkan dengan kabel UTP *Category* 3 (Cat3) atau sebelumnya, di desain untuk mendukung komunikasi data dan juga suara sampai kecepatan 16 megabit/detik.
5. CAT 5 – Kabel UTP *Category* 5 [Cat5] adalah suatu jenis kabel UTP dengan kualitas transmisi yang lebih baik jika dibandingkan dengan kabel UTP *Category* 4 (Cat4) atau yang sebelumnya, di desain untuk mendukung komunikasi data dan komunikasi suara pada kecepatan sampai 100 megabit/detik.
6. CAT 6 – Kabel UTP *Category* 6 [Cat6] adalah jenis standar kabel UTP dengan sertifikasi resmi paling tinggi.
7. CAT 7 – Kabel UTP *Category* 7 [Cat7] adalah jenis kabel premium yang sangat cocok sekali sebagai media yang high traffic berbagai macam aplikasi dalam 1 kabel (single cable). Maksimum data yang terkirim sampai 10 Gbit/detik, dengan frekuensi 1000 Mhz[2].

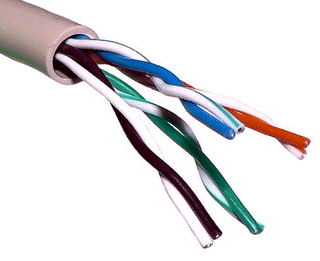
Pada umumnya jenis kabel yang banyak digunakan untuk membentuk sebuah jaringan komputer adalah kabel *Unshielded Twisted Pair* (UTP) kategori 5. Kabel ini dikoneksikan memakai konektor RJ-45, untuk dipasangkan pada LAN *card* yang dimiliki PC ataupun Switch/Hub. Kabel UTP kategori 5 yaitu satu kabel yang berisi delapan, masing-masing pasang di pelintir untuk mengurangi induksi.

Dalam kabel UTP kategori 5, urutan pengkabelannya yang *standart* berupa:

Tabel 1.1Susunan kabel *standart*

|  |  |  |
| --- | --- | --- |
| **PIN** | **Warna Kabel** | **Signal** |
| 1 | Putih *Orange* | Transmit (-) |
| 2 | *Orange* | Transmit (+) |
| 3 | Putih Hijau | *Receive* (-) |
| 4 | Biru | Tidak digunakan |
| 5 | Putih Biru | Tidak digunakan |
| 6 | Hijau | *Receive* (+) |
| 7 | Putih Cokelat | Tidak digunakan |
| 8 | Cokelat | Tidak digunakan |

Dalam pemakaian sehari-hari, kabel UTP sudah sangat baik digunakan sebagai kabel jaringan komputer misalnya dalam kegunaan ruang kantor atau dalam sistem jaringan suatu perusahaan. Mengenai beberapa kelemahan dan kekurangan kabel UTP yang tidak tahan terhadap medan elektromagnetik dan kerusakan benturan benda keras, masih bisa diatasi dengan memasang pelindung luar misalnya seperti pipa plastic[3].

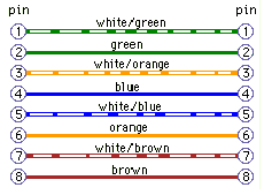


**Gambar 1.1** Kabel UTP

Untuk pemasangan kabel UTP, terdapat dua jenis pemasangan kabel UTP yang umum digunakan pada jaringan komputer terutama LAN, yaitu *Straight Through Cable* dan *Cross Over Cable*.

* + - * 1. *Straight Through Cable*

Kabel *Straight* adalah istilah untuk kabel yang menggunakan standar yang sama pada kedua ujung kabelnya, bisa EIA/TIA 568A atau EIA/TIA 568B pada kedua ujung kabel. Sederhananya, urutan warna pada kedua ujung kabel sama. Pada kabel *Straight*, pin 1 di salah satu ujung kabel terhubung ke pin 1 pada ujung lainnya, pin 2 terhubung ke pin 2 di ujung lainnya, dan seterusnya.

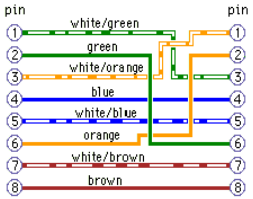


**Gambar 1.2** Susunan kabel *straight*

Contoh penggunaan kabel *Straight* adalah sebagai berikut :

1. Menghubungkan antara PC dengan Switch.
2. Menghubungkan PC dengan LAN pada modem *cable*/DSL.
3. Menghubungkan *Router* dengan LAN pada modem *cable*/DSL.
4. Menghubungkan Switch ke Router.
5. Menghubungkan Hub ke Router.[2]
   * + - 1. *Cross Over Cable*

Untuk tipe *Cross* digunakan untuk menyambungkan langsung antar dua PC, atau yang umumnya digunakan untuk menyambungkan antar Hub. (Misalnya karena colokan di Hubnya kurang).



**Gambar 1.3** Susunan kabel *cover*

Contoh penggunaan kabel *Cover* adalah sebagai berikut :

1. [Menghubungkan 2 buah PC secara langsung](http://www.catatanteknisi.com/2011/09/menghubungkan-2-komputer-dengan-kabel.html).
2. Menghubungkan 2 buah Switch.
3. Menghubungkan 2 buah Hub.
4. Menghubungkan Switch dengan Hub.
5. Menghubungkan PC dengan Router[2].
   * 1. Protokol ARP

Protokol ARP atau *Address* *Resolution* *Protocol* merupakan sebuah protokol yang bertanggung jawab mencari tau *MacAddress* atau alamat *hardware* dari suatu *Host* yang tergabung dalam sebuah jaringan LAN dengan memanfaatkan atau berdasarkan IP *Address* yang terkonfigurasi pada *Host* yang bersangkutan[3].

Fungsi Serta Peran dari Protokol ARP:

1. Peran protokol ARP ini sangat penting dalam jaringan, terutama mengenai komunikasi data yang terjadi dalam jaringan. Setiap *host* yang tergabung atau terhubung dalam sebuah jaringan LAN saling berkomunikasi menggunakan alamat fisik (*Mac Address*) dan tidak menggunakan alamat logis (IP *Address*).
2. Dikatakan pada poin nomor satu, bahwa setiap *Host* berkomunikasi menggunakan alamat fisik (*Mac* *Address*). Jadi, mau tidak mau setiap sebuah *Host* yang ingin berkomunikasi dengan *Host* lain harus mengetahui *Mac* *Address* yang dimiliki oleh *Host* tujuannya tersebut.
3. Lalu bagaimana sebuah *Host* bisa mendapatkan informasi mengenai *Mac* *Address* dari *Host* tujuannya? Jawabannya adalah pada tahapan transfer data. Sebelum sebuah data diberikan *Mac* *address*, terlebih dahulu data tersebut diberi alamat logis berupa IP *Address*. IP *address* yang ditambahkan ini merupakan IP *address* dari *Host* pengirim dan *Host* penerima.
4. Baru kemudian menentukan alamat fisik atau *Mac* *Address* dari *Host* tujuan. Nah, apabila belum diketahui alamat fisiknya, mau tidak mau harus dicari terlebih dahulu. Disinilah peran protokol ARP, dengan memanfaatkan informasi IP *address* *Host* tujuan yang ada, maka *Host* pengirim melakukan pencarian dengan menugaskan Protokol ARP[3].
   * 1. Protokol ICMP (*Internet Control Message Protocol*)

Protokol ICMP adalah protokol yang bertugas mengirimkan pesan-pesan kesalahan dan kondisi lain yang memerlukan perhatian khusus. Pesan/paket ICMP dikirim jika terjadi masalah pada *layer* [IP](http://www.transiskom.com/2011/02/pengertian-ip-internet-protocol.html) dan *layer* atasnya (TCP/UDP). Pada kondisi normal, protokol [IP](http://www.transiskom.com/2011/02/pengertian-ip-internet-protocol.html) berjalan dengan baik. Namun ada beberapa kondisi dimana koneksi [IP](http://www.transiskom.com/2011/02/pengertian-ip-internet-protocol.html) terganggu, misalnya karena *Router* *crash*, putusnya kabel, atau matinya *host* tujuan. Pada saat ini ICMP membantu menstabilkan kondisi [jaringan](http://www.transiskom.com/2010/06/jaringan-komputer.html), dengan memberikan pesan-pesan tertentu sebagai respons atas kondisi tertentu yang terjadi pada [jaringan](http://www.transiskom.com/2010/06/jaringan-komputer.html) tersebut[2].

Ada dua tipe pesan yang dapat dihasilkan ICMP:

1. ICMP *Error* *Message* (dihasilkan jika terjadi kesalahan [jaringan](http://www.transiskom.com/2010/06/jaringan-komputer.html)).
2. ICMP *Query* *Message* (dihasilkan jika pengirim paket mengirimkan informasi tertentu yang berkaitan dengan kondisi [jaringan](http://www.transiskom.com/2010/06/jaringan-komputer.html)[2].

ICMP *Error* *Message* dibagi menjadi beberapa jenis:

1. *Destination* *Unreachable*, dihasilkan oleh *router* jika pengirim paket mengalami kegagalan akibat masalah putusnya jalur baik secara fisik maupun *logic*. *Destination* *Unreacheable* dibagi lagi menjadi beberapa jenis:
2. *Network* *Unreacheable*, jika jaringan tujuan tidak dapat dihubungi.
3. *Host* *Unreacheable*, jika *host* tujuan tak bisa dihubungi.
4. *Protocol* *At* *Destination* *is* *Unreacheable*, jika di tujuan tak tersedia protokol tersebut.
5. *Destination* *Host* *is* *Unknown*, jika *host* tujuan tidak diketahui.
6. *Destination* *Network* *is* *Unknown*, jika *network* tujuan tidak diketahui.
7. *Time* *Exceeded*, dikirimkan jika isi *field* TTL dalam paket [IP](http://www.transiskom.com/2011/02/pengertian-ip-internet-protocol.html) sudah habis dan paket belum juga sampai ke tujuannya. Tiap kali sebuah paket [IP](http://www.transiskom.com/2011/02/pengertian-ip-internet-protocol.html) melewati satu *router*, nilai TTL dalam paket tsb, dikurangi satu. TTL ini diterapkan untuk mencegah timbulnya paket [IP](http://www.transiskom.com/2011/02/pengertian-ip-internet-protocol.html) yang terus menerus berputar-putar di *network* karena suatu kesalahan tertentu. Sehingga menghabiskan sumber daya yang ada.
8. *Parameter* *Problem*, paket ini dikirim jika terdapat kesalahan parameter pada *header* paket [IP](http://www.transiskom.com/2011/02/pengertian-ip-internet-protocol.html).
9. *Source* *Quench*, Paket ICMP ini dikirimkan jika *router* tujuan mengalami kongesti. Sebagai respons atas paket ini pihak pengirim paket harus memperlambat pengiriman paketnya.
10. *Redirect*, paket ini dikirimkan jika *router* merasa *host* mengirimkan paket [IP](http://www.transiskom.com/2011/02/pengertian-ip-internet-protocol.html) melalui *router* yang salah. Paket ini seharusnya dikirimkan melalui *router* lain[2].
    * 1. *Wireshark*

*Wireshark* merupakan *Network* *Protocol* *Analyzer*, juga termasuk salat satu *network* *analysis* *tool* atau *packet* *sniffer*. *Wireshark* mengizinkan pengguna mengamati data dari jaringan yang sedang beroperasi atau dari data yg ada di *disk*, dan langsung melihat / mensortir data yg tertangkap, mulai dari informasi singkat dan rincian bagi masing-masing paket termasuk juga *full header* & porsi data, sanggup diperoleh.

Wireshark mempunyai sekian banyak *feature* termasuk juga *display filter language* yg banyak & kebolehan me-reka ulang suatu aliran pada sesi TCP. Paket *sniffer* sendiri diartikan satu buah *tool* yg berkemampuan menahan dan melaksanakan pencatatan pada *traffic* data dalam jaringan.

Selagi berjalan aliran data dalam jaringgan, *packet sniffer* bisa menangkap *protocol* data unit (PDU), jalankan *decoding* juga analisis pada isi paket. *Wireshark* sebagai salah satu packet *sniffer* yg diprogram demikian supaya mengenali beragam macam protokol jaringan. *Wireshark* serta dapat menampilkan hasil enkapsulasi & *field* yg ada di dalam PDU[3].

1. **ALAT DAN BAHAN**
2. Komputer/Laptop
3. Kabel UTP
4. Konektor RJ-45
5. Tang *Crimping*
6. Software Wireshark
7. Gunting
8. Hub /Switch (*optional*)
9. LAN kabel tester (*optional*)
10. **PERMASALAHAN**

Adapun permasalahan dalam praktikum kali ini antara lain sebagai berikut:

1. Melakukan pembuatan dan pengujian kabel UTP dengan konfigurasi *cross-over* dan *straight-through.*
2. Menghubungkan 2 (dua) buah komputer menggunakan kabel UTP jenis *cross*.
3. Melakukan *setting* protokol TCP/IP.
4. *Testing* koneksi dua buah komputer dengan perintah *ping* dan tangkap proses yang terjadi menggunakan *Wireshark* kemudian melakukan analisa protokol Layer 2 (ARP) dan protokol Layer 3 (ICMP).
5. **LANGKAH PERCOBAAN**
6. Melakukan pembuatan dan pengujian kabel UTP dengan kombinasi *cross-over* dan *straight-through*

Dalam percobaan pertama ini praktikan mencoba untuk membuat sendiri kombinasi kabel UTP, mulai dari memotong kabel, menyiapkan konektor, melakukan proses c*rimping* serta menguji kabel dengan LAN-*tester*.

* 1. Konfigurasi *Cross*

Berikut adalah tabel konfigurasi *cross* di sisi pengirim dan di sisi penerima seperti yang tampak pada Tabel 1.2:

Tabel 1.2Konfigurasi *Cross*

|  |  |  |
| --- | --- | --- |
| **No** | **Pengirim** | **Penerima (cross)** |
| 1 | Putih orange | Putih hijau |
| 2 | Orange | Hijau |
| 3 | Putih hijau | Putih orange |
| 4 | Biru | Biru |
| 5 | Putih biru | Putih biru |
| 6 | Hijau | Orange |
| 7 | Putih coklat | Putih coklat |
| 8 | Coklat | Coklat |

Fungsi dari konfigurasi *cross* ini adalah untuk penggunaan kabel UTP dalam hal menghubungkan antara dua *device* yang sama atau mempunyai fungsi yang sama, misalkan PC ke PC atau *Router* ke *Router*.



**Gambar 1.4** Hasil pengujian kabel *cross* menggunakan LAN-*tester*

Dari **Gambar 1.4** terlihat saat dilakukan pengujian kabel dengan menggunakan *LAN-tester*, akan terlihat nyala lampu di kedua sisi pengirim dan penerima menyala dengan kondisi berbeda. Saat lampu 1 menyala pada sisi pengirim, pada sisi penerima menyala di lampu 3, saat lampu 2 menyala pada sisi pengirim, pada sisi penerima menyala di lampu 6. Sedangkan untuk lampu 4, 5, 7, 8 menyala secara bersamaan.

* 1. Konfigurasi *straight*

Berikut adalah tabel konfigurasi *straight* di sisi pengirim dan di sisi penerima seperti yang tampak pada Tabel 1.3:

Tabel 1.3Konfigurasi *Straight*

|  |  |  |
| --- | --- | --- |
| **Pin** | **Pengirim** | **Penerima** |
| 1 | Putih orange | Putih orange |
| 2 | Orange | Orange |
| 3 | Putih hijau | Putih hijau |
| 4 | Biru | Biru |
| 5 | Putih biru | Putih biru |
| 6 | Hijau | Hijau |
| 7 | Putih coklat | Putih coklat |
| 8 | Coklat | Coklat |

Fungsi dari konfigurasi *straight* ini adalah untuk penggunaan kabel UTP dalam hal menghubungkan antara dua *device* yang berbeda atau mempunyai fungsi yang berbeda, misalkan PC ke Hub/Switch.



**Gambar 1.5** Hasil pengujian kabel *Straight* menggunakan LAN-*tester*

Dari **Gambar 1.5** terlihat saat dilakukan pengujian kabel dengan menggunakan *LAN-tester,* akan terlihat nyala lampu di kedua sisi pengirim dan penerima menyala dengan cara bersamaan. Saat lampu 1 menyala pada sisi pengirim, pada sisi penerima menyala di lampu 1, saat lampu 2 menyala pada sisi pengirim, pada sisi penerima menyala di lampu 2. Begitu seterusnya hingga lampu ke 8.

Langkah-Langkah Pembuatan Kabel dengan Konfigurasi *Cross*/*Straight*:

Langkah 1:

Buang kulit pembungkus kabel UTP dan mengeluarkan 4 pasang kabel yang ada di dalamnya. Buanglah kulit sepanjang 3 cm dari ujung (**Gambar 1.6**).



**Gambar 1.6** Proses membuang pembungkus kabel

Langkah 2:

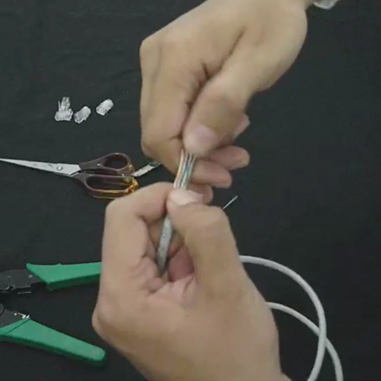
Setelah pembungkus kabel lepas, lalu urutkan kabel berdasarkan jenis yang diinginkan, baik jenis *straight* maupun *cross* *cable*. Contoh di bawah ini adalah mengurutkan jenis kabel *Straight* (**Gambar 1.7**).



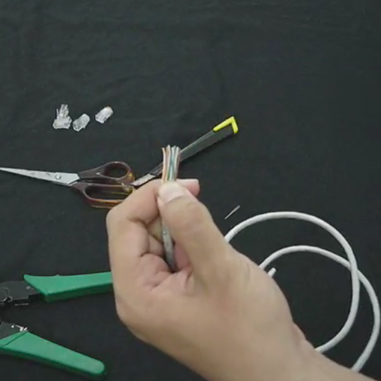
**Gambar 1.7** Proses mengurutkan jenis kabel

Langkah 3:

Setelah diurutkan, selanjutnya rapikan kabel tersebut (**Gambar 1.8** dan **Gambar 1.9**).



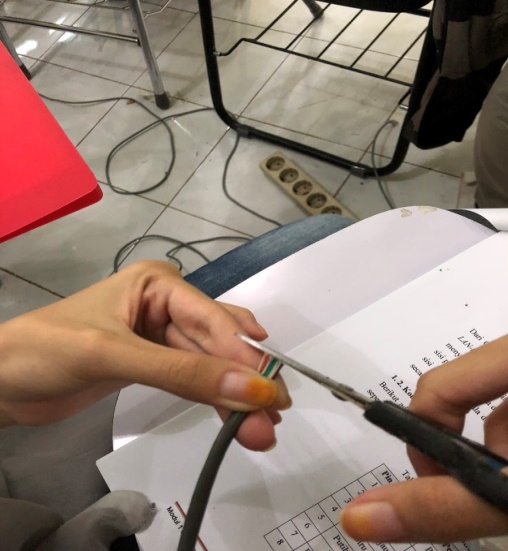
**Gambar 1.8** Proses merapikan kabel



**Gambar 1.9** Kabel yang telah rapi

Langkah 4:

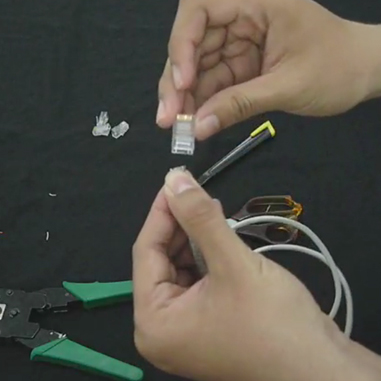
Ratakan ujung kabel dengan memotong menggunakan gunting (**Gambar 1.10**). Potong ujung kabel menggunakan gunting dan sisakan kabel sepanjang 2 cm dari ujung pembungkus yang telah kita potong tadi dengan *cutter*.



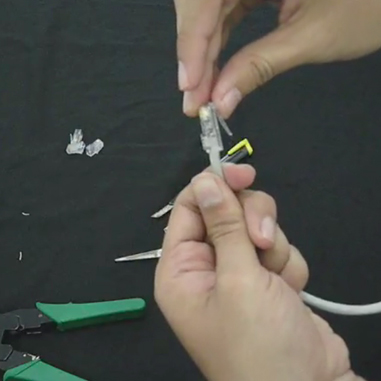
**Gambar 1.10** Proses meratakan ujung kabel

Langkah 5:

Masukkan ujung kabel ke dalam *Connector* RJ-45 dengan posisi *connector*-nya terbalik yaitu pengait RJ-45 di posisi bawah (**Gambar 1.11** dan **Gambar 1.12**).



**Gambar 1.11** Memasukkan ujung kabel ke dalam konektor RJ-45



**Gambar 1.12** Memasukkan ujung kabel ke dalam konektor RJ-45

Langkah 6:

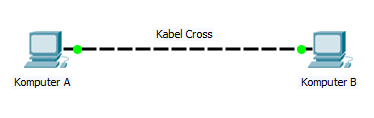
Tekan menggunakan *Crimping Tool* dengan kuat sampai ujung-ujung kabel dalamnya terluka dengan tembaga *Connector* RJ-45 seperti yang tampak pada **Gambar 1.13**.



**Gambar 1.13** Proses *crimping*

1. Menghubungkan 2 (dua) buah komputer menggunakan kabel *cross*

Pada percobaan ini praktikan menghubungkan antara 2 (dua) buah komputer sehingga kita membutuhkan kabel UTP dengan konfigurasi *cross*. Hal ini dilakukan karena perangkat yang disambung mempunyai fungsi yang sama dan apabila perangkat yang digunakan mempunyai fungsi yang berbeda maka digunakan konfigurasi *straight*. Pada praktikum hanya dilakukan koneksi antara 2 (dua) komputer sehingga digunakan konfigurasi *cross* seperti yang tampak pada **Gambar 1.14.**



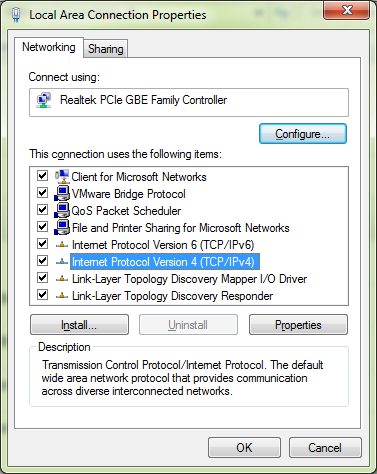
**Gambar 1.14** Dua buah komputer yang dihubungkan menggunakan kabel *cross*

1. Setting IP Address versi 4 (TCP/IPv4)

Setelah 2 (dua) buah komputer dihubungkan dengan kabel *cross*, agar komputer dapat saling berkomunikasi perlu dilakukan setting *IP address* pada jendela *Local Area Connection Properties* dalam sistem operasi Windowsdengan langkah sebagai berikut:

Langkah 1:

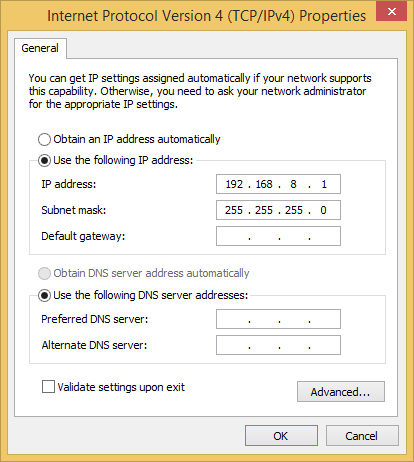
Klik “*Local Area Connection Properties*” kemudian pilih *tab* “*Networking*” dan klik dua kali pada pilihan “*Internet Protocol Version 4(TCP/ IPv4)*” seperti yang tampak pada **Gambar 1.15**.



**Gambar 1.15** Tampilan jendela *Local Area Connection* Properties

Langkah 2:

Pilih “*use the following IP address*”, lalu isikan secara manual IP yang akan digunakan pada field “*IP address*” dan masukkan *subnet* mask pada *field* “*Subnet mask*”. Untuk yang lain kosongkan saja, lalu klik “*OK*” seperti yang tampak pada **Gambar 1.16**.



**Gambar 1.16** Jendela *properties Internet Protocol* versi 4

Langkah 3:

Lakukan hal yang sama dengan komputer penerima dengan kondisi IP yang dimasukkan berada dalam kelas dan *subnet mask* yang sama. Misalkan untuk pengirim IP-nya “192.168.8.1*”* maka penerimanya “192.168.8.2*”,* sebagai contoh dengan *subnet mask* yang sama yaitu “255.255.255.0” maka kedua komputer akan berada dalam satu jaringan.

1. Uji koneksi dengan perintah *ping* dan tangkap proses yang terjadi menggunakan software *Wireshark* kemudian lakukan analisa protokol Layer 2 (ARP) dan protokol Layer 3 (ICMP).
   1. Perintah *ping*

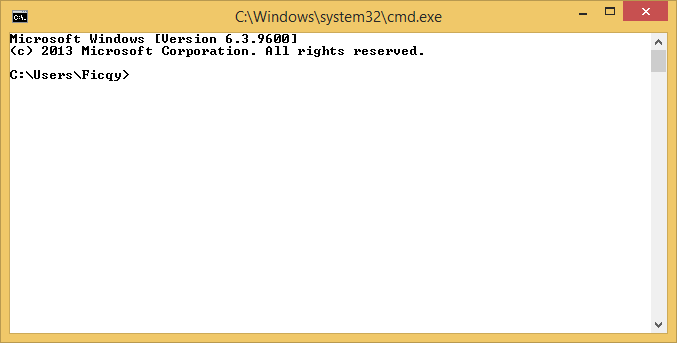
Untuk menguji apakah kedua komputer telah terkoneksi, maka lakukan perintah *ping* antar kedua komputer untuk proses uji koneksi.

Format perintah : “ping <IP Address komputer tujuan>”

Berikut langkah-langkahnya:

Langkah 1:

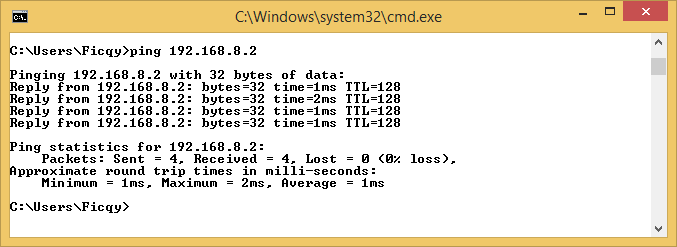
Buka *command prompt* atau *cmd* pada komputer 1 dengan mengetikkan “cmd” pada start menu kemudian tekan *enter* (**Gambar 1.17**).



**Gambar 1.17** Tampilan jendela *command prompt* pada Windows

Langkah 2:

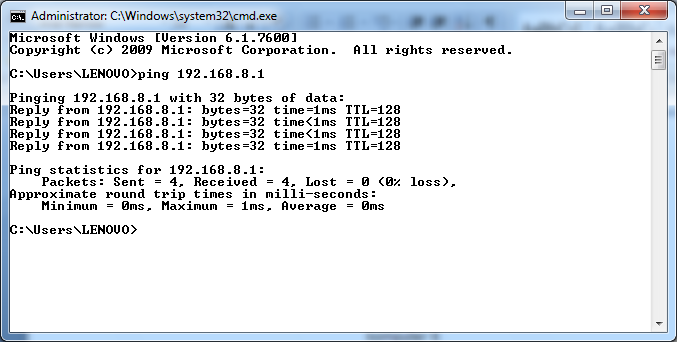
Ketik perintah “ping 192.168.8.2” untuk melakukan uji koneksi terhadap komputer tujuan. Akan ada pesan balasan “Reply from 192.168.8.2: bytes=32 time=1ms TTL=128” dst dari komputer tujuan seperti pada **Gambar 1.18**. Pesan tersebut mengindikasikan bahwa komputer 1 dan komputer 2 telah terjadi koneksi dan dapat saling bertukar data secara *point*-*to*-*point*.



**Gambar 1.18** Pesan balasan yang diterima oleh komputer 1

Langkah 3:

Pada komputer 2, ketikkan perintah “ping 192.168.8.1” dan akan ada pesan balasan seperti yang tampak pada **Gambar 1.19**.

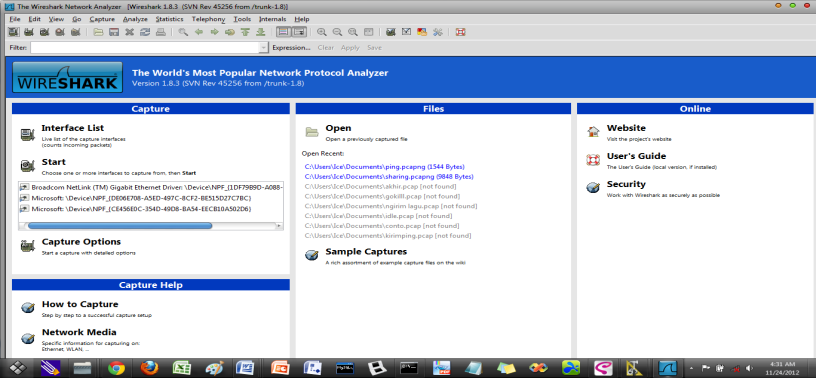


**Gambar 1.19** Pesan balasan pada komputer 2

Pada **Gambar 1.18** dan **Gambar 1.19** dapat dilihat ukuran tiap paket yang dikirimkan sebesar 32 *byte* dalam waktu 1 ms. *TTL (Time To Live)* mengindikasikan jumlah maksimum *hop* yang dilewati paket sebelum di-*drop* keluar jaringan. Pada proses *ping*, paket yang dikirimkan sejumlah 4 buah dan diterima 4 buah juga oleh host tujuan. *%loss* menunjukkan persentase paket yang dikirimkan dan diterima oleh *host*.

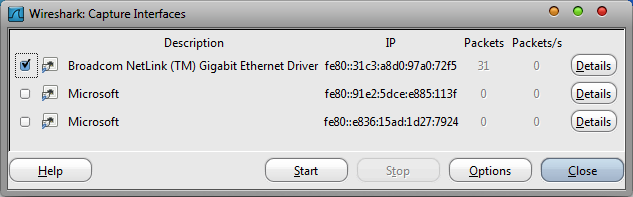
* 1. Analisa protokol Layer 2 (ARP – *Address Resolution Protokol*) dan protokol Layer 3 (ICMP) menggunakan *software Wireshark.*

Sebelum melakukan percobaan ini, lakukan instalasi *software* Wireshark di komputer Anda terlebih dahulu seperti yang tampak pada **Gambar 1.20**.



**Gambar 1.20** Tampilan jendela *software Wireshark*

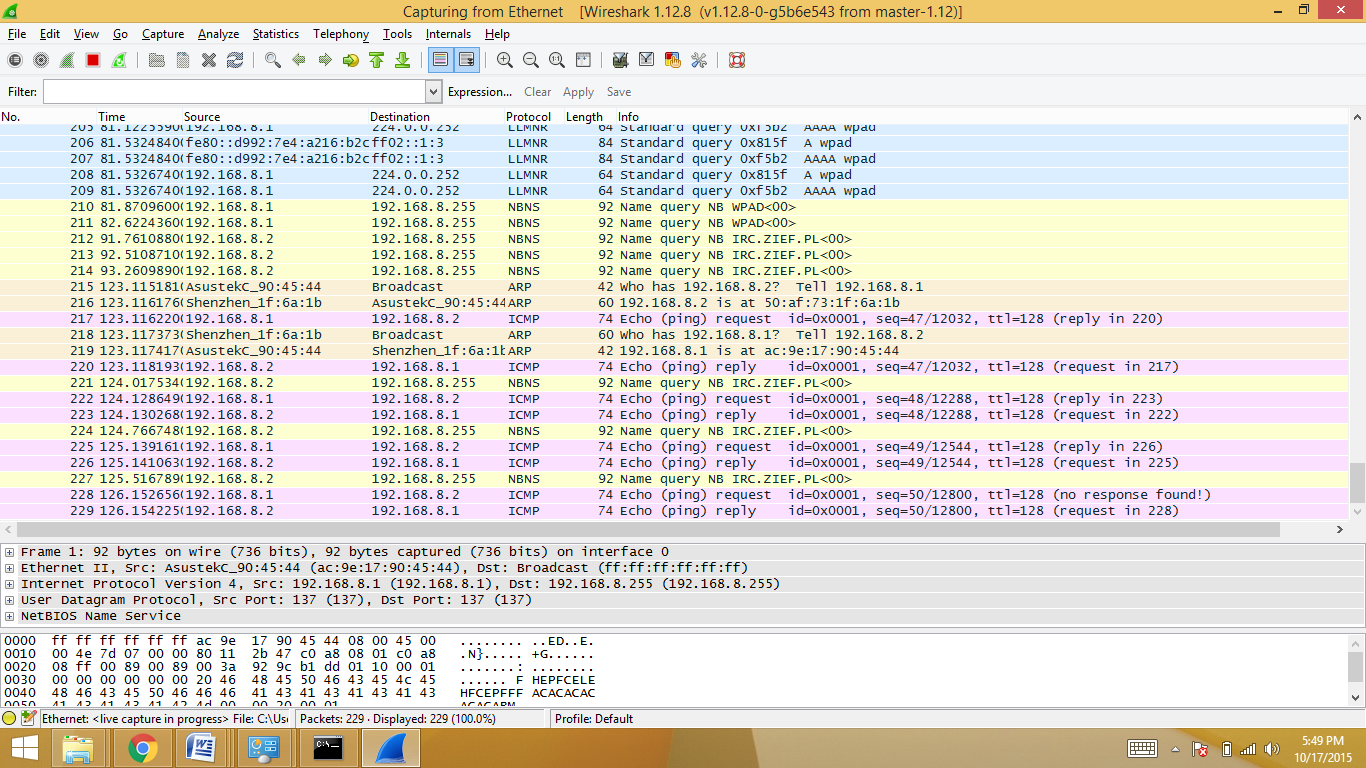
Kemudian geser *cursor* ke arah tab “*capture*” kemudian pilih “Interfaces”. Hentikan semua proses yang berjalan bila ada dengan memilih “stop” baru kemudian memilih koneksi yang akan dilakukan penganalisaan pada adapter *network* yang mana dengan mengklik tombol “start” seperti pada **Gambar 1.21.**



**Gambar 1.21** *Wireshark capture Interfaces*

Kemudian akan muncul tampilan seperti pada **Gambar 1.22** yang akan memuat aktivitas yang akan tercatat, meliputi :

1. *Time* : waktu dilakukannya proses
2. *Source* : sumber atau pengirim
3. *Destination* : tujuan atau penerima
4. *Protocol* : jenis *protocol* yang digunakan
5. *Length* : panjang data
6. *Info* : *info* mengenai proses komunikasi yang terjadi



**Gambar 1.22** Proses *capturing*

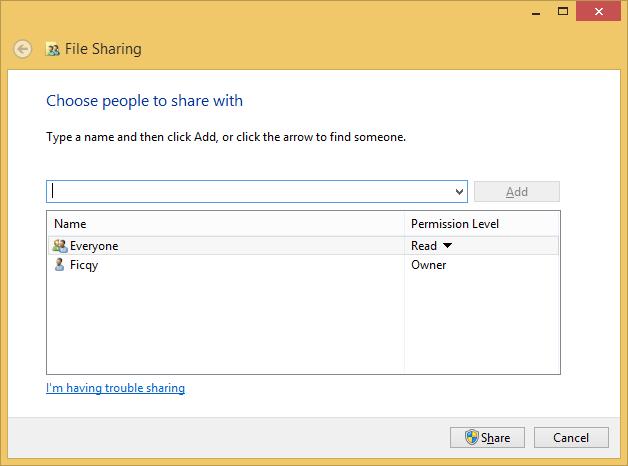
**Gambar 1.22** adalah contoh *capturing* proses *ping* dari IP “192.168.8.1” ke “192.168.8.2”. Pada dasarnya, program *ping* berfungsi mengirimkan paket *datagram* dengan protokol ICMP (*Internet Control Message Protocol*). Paket yang dikirimkan adalah *Echo (ping) request*. Bila pesan ini dibalas dengan paket *Echo (ping) reply* maka berarti *host* yang dituju sedang aktif. Dengan menggunakan program *wireshark* kita dapat mencuplik komunikasi yang terjadi pada saat perintah *ping* dijalankan.

Terdapat beberapa informasi yang dapat diambil dari **Gambar 1.22**. Terlihat alamat pengirim (192.168.8.1) dan alamat tujuan *ping* (192.168.8.2). Tampak pula 4 (empat) paket *ping* yang dikirimkan kesemuanya mendapat pesan balasan.

Untuk *ARP* dapat dilihat pada baris ke-1 dimana pada langkah ini komputer 1 dengan IP 192.168.8.1 dinyatakan sebagai si pengirim, yang menanyakan “who has 192.168.8.2? Tell 192.168.8.2” selanjutnya komputer 2 pada baris ke-2 dengan IP 192.168.8.2 menyatakan dirinya dengan menunjukan MAC *address Ethernet* card-nya yaitu pada keterangan “192.168.8.2 is at 54:a0:50:aa:bc:68”.

* 1. File Sharing

Selain dengan *ping* dapat juga dilakukan analisa dengan melakukan pengujian dengan pencuplikan proses *file sharing*. Yang harus dilakukan adalah sharing file dalam jaringan kemudian memberikan *checklist* pada “turn on file and printer sharing” agar file yang dishare dapat diakses. Kemudian komputer yang di *share file* tersebut mencoba mengcopy file nya dengan langkah sama seperti pada proses pencuplikkan *ping* maka akan diperoleh hasil seperti pada **Gambar 1.23**. Disini dilakukan pengujian dengan meng-*copy* file *tes.txt*.

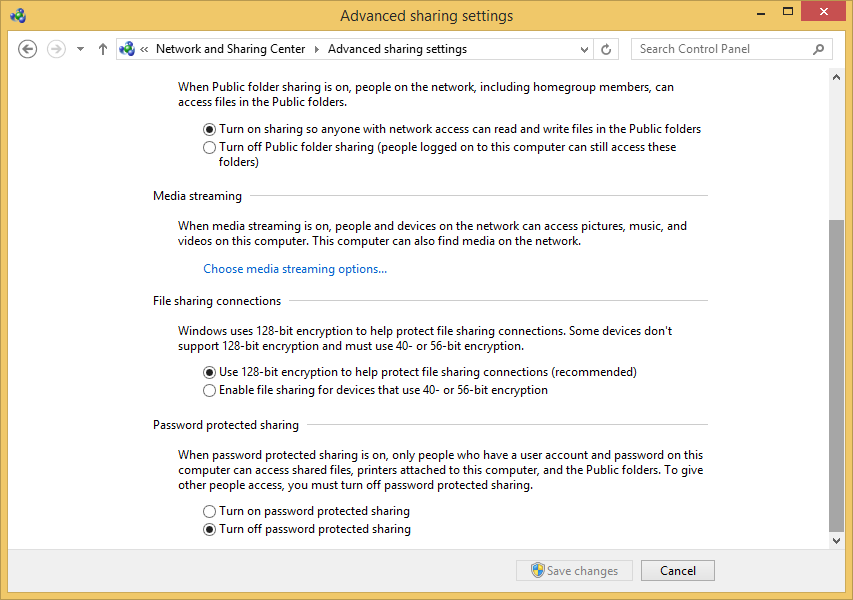


**Gambar 1.23** *File Sharing properties*

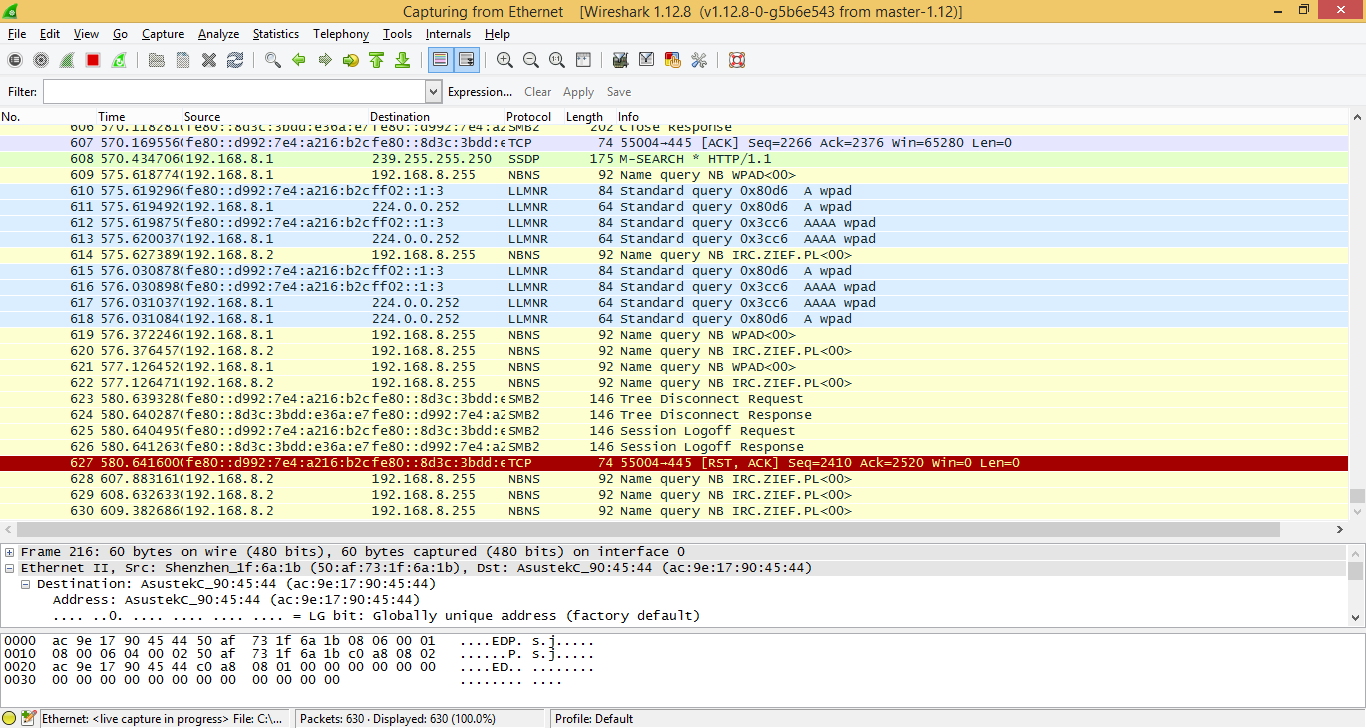
*Permission* pada *file sharing* dapat dilihat pada **Gambar 1.23**.

*Read* : *file* hanya dapat dilihat saja

*Write*/*read* : *file* hanya dapat dilihat dan di *edit*



**Gambar 1.24** Tampilan jendela *advanced sharing settings*



**Gambar 1.25** *Wireshark capturing process file sharing*

1. **HASIL DAN PEMBAHASAN**
   * + 1. Pembuatan kabel *Cross*

Dalam Konfigurasi *Cross-over* adalah suatu kabel yang digunakan pada saat ingin menghubungkan dua perangkat yang sama yaitu computer dengan komputer lainnya. Pengkabelan dengan konfigurasi *cross* dilakukan dengan cara memasang urutan warna kabel yang berbeda untuk kedua ujung kabel UTP, seperti pada Tabel 1.4dan Tabel1.5.

Tabel 1.4Tabel konfigurasi UTP/RJ-45 pada pengirim.

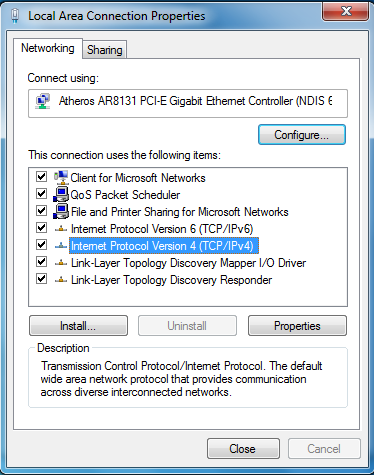
|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 |
| Putih orange | orange | Putih hijau | biru | Putih Biru | Hijau | Putih coklat | Coklat |

Tabel 1.5Tabel konfigurasi UTP/RJ-45 pada penerima.

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 |
| Putih hijau | hijau | Putih orange | biru | Putih Biru | orange | Putih coklat | coklat |

* + - 1. Menghubungkan 2 (dua) buah komputer menggunakan kabel *cross*

Dua buah komputer dapat dihubungkan dengan kabel UTP hanya jika kabel tersebut dikonfigurasi dengan menggunakan *cross-over*. Pada praktikum kali ini, dua buah komputer akan dihubungkan menggunakan kabel yang sudah dikonfigurasikan pada permasalahan nomor 1. Langkah pertama yang dilakukan, *setting* IP *address* dari komputer dengan membuka *network and sharing center,* klik *change adapter setting.* Kemudian pada halaman *control panel*, klik kanan pada *icon* *Ethernet* dan pilih *properties* maka akan tampil tampilan seperti gambar di bawah ini:

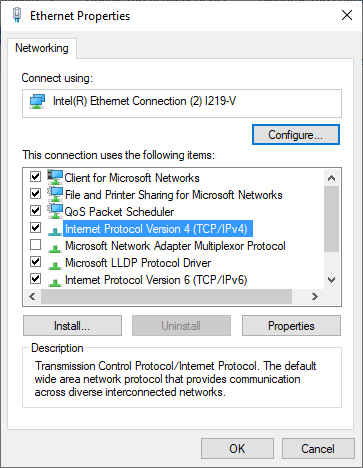


**Gambar 1.26** Tampilan jendela *Local Area Connection* *Properties*

* + - 1. *Setting* IP *Address versi* 4 (TCP/IPv4)

Setelah 2 (dua) buah komputer dihubungkan dengan kabel *cross*, agar komputer dapat saling berkomunikasi perlu dilakukan *setting* IP *address* pada jendela *Local Area Connection Properties* dalam sistem operasi *Windows*.

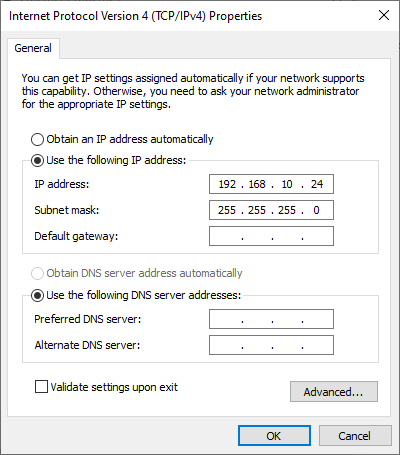
1. Pada *Local Area Connection Properties* kemudian pilih *tab* *Networking* dan klik dua kali pada pilihan *Internet Protocol Version 4(TCP/ IPv4)* seperti yang tampak pada **Gambar 1.27**.



**Gambar 1.27** Tampilan *properties* Ipv4

Pada tampilan tersebut, kemudian pilih *properties* dari *internet protocol version* 4 (TCP/IPv4). Setelah itu, akan muncul tampilan seperti **Gambar 1.27** yang menjadi halaman untuk melakukan perubahan IP *address* dari perangkat komputer.

Pilih *use the following IP address*, lalu masukan secara manual IP yang akan digunakan pada *field* IP *address* dan masukkan *subnet* *mask* pada *field* *Subnet mask*, klik *OK*.

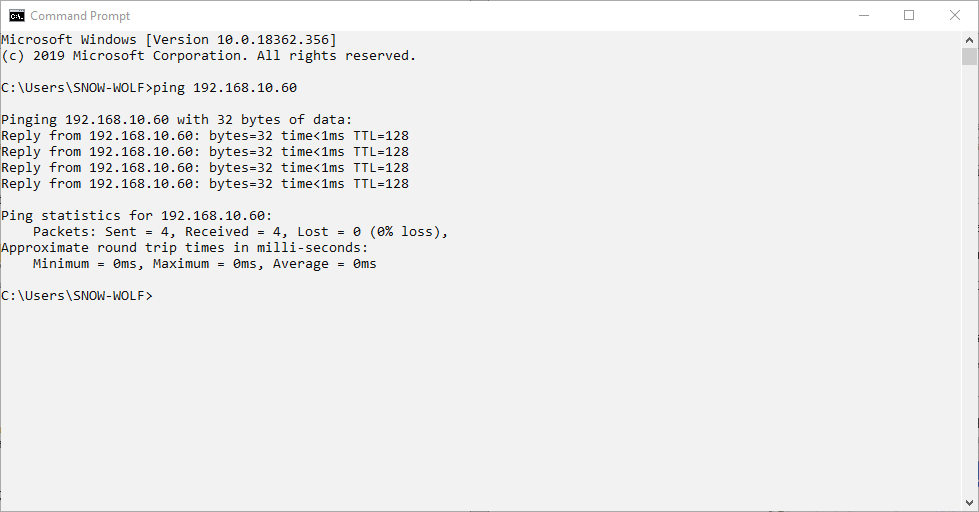


**Gambar 1.28** *Properties Internet Protocol versi* 4/IP *address* pengirim

Pada **Gambar 1.28** adalah IP address dari pengirim yaitu 192.168.10.24 di-*set*. Komputer pertama menggunakan IP *address* 192.168.10.24. Untuk menghubungkan kedua komputer, maka IP *address* dari komputer yang akan dihubungkan harus di-*set* dengan *network address* yang sama dengan komputer ini dengan host yang berbeda. IP *address* pada computer kedua yang lain di-*set* dengan 192.168.10.60.

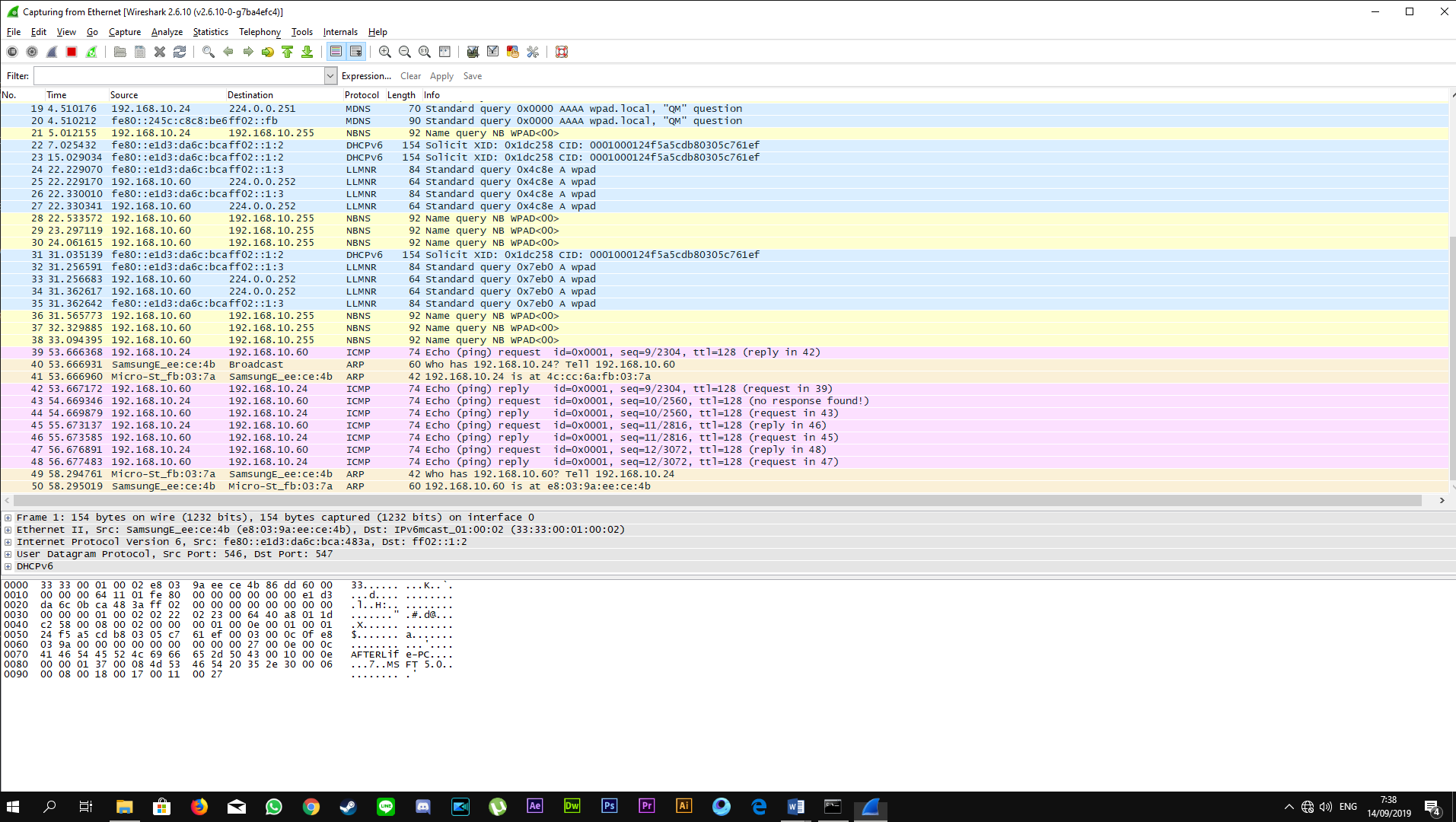
Perintah *ping*

Mengecek komputer yang telah terhubung melalui kabel kabel LAN dapat dilakukan dengan cara mengetik *ping* pada CMD (*command prompt*) dan masukkan IP *Address* dari komputer lain yang sedang terhubung. Lalu klik *enter* pada *keyboard*. *Ping* merupakan program yang dijalankan melalui CMD (*Command* *Prompt*) pada Windows. Fungsi perintah *ping* di CMD salah satunya untuk melakukan cek koneksi pada suatu *host*. Jika Anda menggunakan jaringan LAN, maka perintah ping akan diikuti dengan IP address milik komputer tujuan. IP *Address* 192.168.10.60 adalah IP *Address* yang dimiliki oleh komputer tujuan, sedangkan IP *Address* dari komputer asal adalah 192.168.10.24. Jika proses ping berhasil maka komputer tujuan akan mengirimkan balasan atau *reply. Reply from* berarti komputer tujuan memberikan balasan. *Bytes* merupakan *request packet* yang telah dikirimkan*. Time* menunjukkan waktu yang digunakan untuk mengirim dan menerima balasan. Sedangkan TTL merupakan nilai “*Time To Live”* yang mencegah adanya *circular routing* pada suatu jaringan.

****

**Gambar 1.29** Proses *ping* ke komputer lain

Pada komputer pengirim, ketikkan perintah *ping 192.168.10.60* dan akan ada pesan balasan. Pada **Gambar 1.29** dapat dilihat ukuran tiap paket yang dikirimkan sebesar 32 *byte* dalam waktu 1 ms. TTL *(Time To Live)* menandakan jumlah maksimum *hop* yang dilewati paket sebelum di-*drop* keluar jaringan. Pada proses *ping*, paket yang dikirimkan sejumlah 4 buah dan diterima 4 buah juga oleh host tujuan. 0*% loss* adalah persentase paket yang dikirimkan dan diterima oleh *host*.



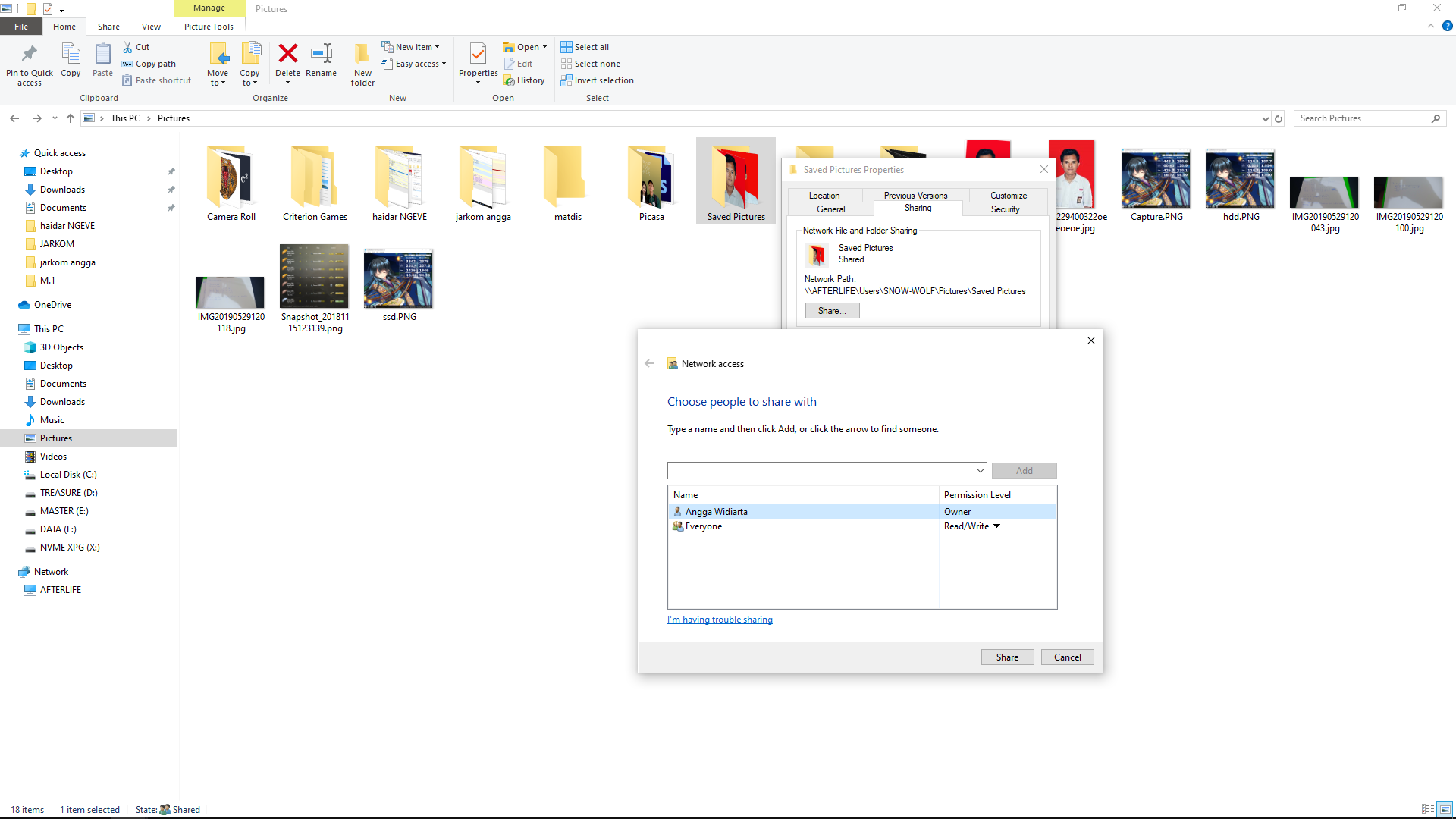
**Gambar 1.30** Tampilan Wireshark pada saat proses ping

Penggunaan program Wireshark untuk memonitor jaringan yang menghubungkan komputer satu dengan komputer lainnya. *Monitoring* untuk penggunaan kabel UTP *cross.*

**Gambar 1.30** menampilkan proses dari *ping* yang dilakukan pada CMD dan ditampilkan melalui Wireshark. PC asal memiliki IP *Address* 192.168.10.24 yang mengirim permintaan ketujuan (*destination*) IP *Address* 192.168.10.60. ICMP pada *ping* merupakan indikator untuk mengetahui berapa lama permintaan dan balasan yang telah dilakukan.

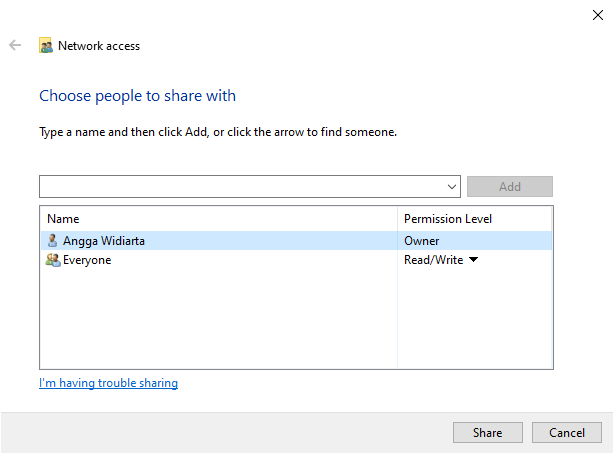
* + - 1. *File Sharing*

Adapun untuk langkah-langkah untuk berbagi *file* tersebut sebagai berikut:



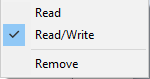
**Gambar 1.31** Langkah untuk melakukan *Sharing File*

Pengujian selanjutnya yaitu lakukan *sharing-file* menggunakan jaringan yang sudah dikonfigurasikan sebelumnya. *File* yang dapat di-*share* adalah *file* dalam bentuk *folder*. Untuk melakukan *sharing-file* adalah dengan meng-klik kanan pada *folder* yang diizinkan untuk di *sharing*. Kemudian arahkan kursor ke “*share with*” lalu pilih “*specify people*”. Setelah itu akan muncul tampilan



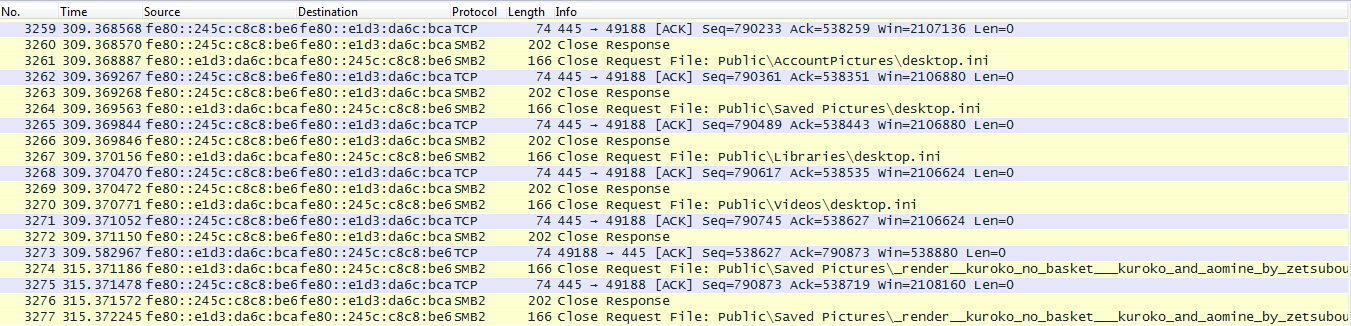
**Gambar 1.32** *File Sharing properties*

Kemudian pilih siapa saja yang dapat mengakses *file* yang telah di-*share*. Pilih *everyone* agar dapat bisa dilihat oleh yang saling terhubung.



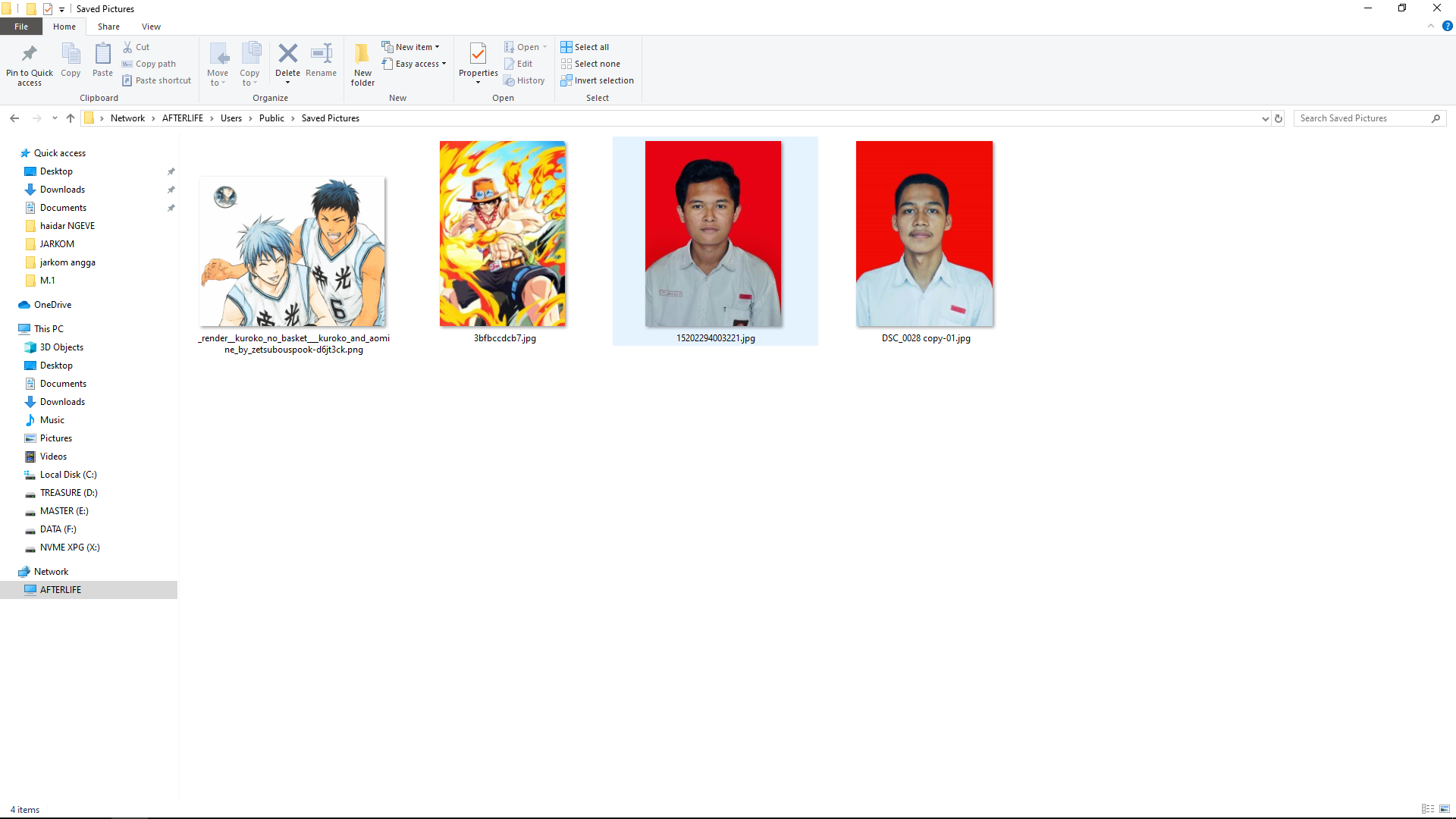
**Gambar 1.33** *Permission* pada file *sharing*

*Permission* pada *file sharing* dapat dilihat pada **Gambar 1.33** berfungsi agar *file* dapat dilihat. Dan *write/read* berfungsi agar file dapat dilihat dan di-*edit*.



**Gambar 1.34** *Wireshark capturing process file sharing*

**Gambar 1.34** merupakan tampilan alur data di Wireshark ketika *file* di-*share* dari suatu pengguna jaringan ke pengguna lain menggunakan kabel UTP *type cross.* Protokol yang digunakan yaitu protokol TCP, SMB2, DHCP. DHCP (*Dynamic Configuration Protocol*) adalah layanan yang secara otomatis memberikan nomor IP kepada komputer yang memintanya. Komputer yang memberikan nomor IP disebut sebagai DHCP *server*, sedangkan komputer yang meminta nomor IP disebut sebagai DHCP *client*. Dengan demikian *administrator* tidak lagi harus memberikan nomor IP secara manual pada saat konfigurasi TCP/IP, tapi cukup dengan memberikan referensi kepada DHCP *server*. *Transmission* *Control* *Protocol* (TCP) adalah suatu protokol yang berada di lapisan transport (baik itu dalam tujuh lapis model referensi OSI atau model DARPA) yang berorientasi sambungan (*connection-oriented*) dan dapat diandalkan (*reliable*). TCP dispesifikasikan dalam RFC 793. *Server* *Message* *Block* disingkat SMB adalah istilah Bahasa Inggris dalam teknologi informasi yang mengacu kepada protokol *client/server* yang ditujukan sebagai layanan untuk berbagi berkas (*file sharing*) di dalam sebuah jaringan. Protokol ini seringnya digunakan di dalam sistem operasi Microsoft Windows dan IBM OS/2. Sistem operasi berbasis UNIX juga dapat menggunakannya dengan tambahan perangkat lunak yang disebut dengan SAMBA. Fungsi dari SMB2 adalah untuk membuka dan menutup koneksi antara klien-klien SMB (yang disebut sebagai *redirector*) dan *server* SMB (komputer yang menjalankan *file and print services*) untuk mengizinkan klien agar dapat mengakses sumber daya di dalam jaringan, menemukan, membaca, dan menulisi berkas dalam sebuah *file server*, serta menemukan dan menggunakan alat pencetak yang digunakan bersamasama untuk mencetak secara jarak jauh. Pada pengiriman data menggunakan kabel UTP *cross*, pengiriman *segment* lebih sedikit.



**Gambar 1.35** Tampilan penerima file

Pada tampilan penerimaan *file* tidak jauh berbeda dengan pengiriman *file*.Dimana data yang di terima berada pada folder tempat data di kirim dan untuk proses pemeriksaan *file* yang di terima dilakukan pada *network* dan membuka *dekstop* yang terhubung dengan menggunakan kabel *cross* dan berada pada satu jaringan yang sama.

1. **KESIMPULAN**

Berdasarkan tujuan dan hasil pembahasan pada praktikum ini, dapat disimpulkan bahwa:

* + - 1. Konfigurasi kabel UTP menggunakan T-568A dan T-568B. T-568A yang perbedaannya terletak pada pengurutan warna kabel nomor urut 1, 2, 3, dan 6.
      2. Dalam pembuatan kabel UTP, digunakan konektor RJ-45 yang dikonfigurasi dengan aturan *straight-through* atau *cross-over*.
      3. Dalam konfigurasi jaringan dengan protokol TCP/IP perlu dilakukan konfigurasi IPv4 terlebih dahulu agar dapat menghubungkan dua buah komputer.
      4. Perintah *ping* yang dilakukan pada *command prompt* berguna untuk memastikan PC telah terkoneksi dengan PC lainnnya melalui kabel UTP.
      5. Pada TCP/IP, PDU *layer* 2 digunakan untuk *internet*, sedangkan PDU *layer 3* digunakan dalam proses transfer data.
      6. Pada Wireshark, perbedaan PDU *layer* 2 dan *layer* 3 terletak pada protokol yang digunakan, dimana pada *layer* 2 pada umumnya menggunakan protokol TCP/IP, sedangkan pada *layer* 3 menggunakan protokol TCP atau UDP.