

Laporan 10

Komputer dan Jaringan

Wireshark



Dosen Pengampu Mata Kuliah
Reesa Akbar

Muhammad Zulfi Aditya Saputra

D3 Teknik Elektronika A

2120500019

POLOTEKNIK ELEKTRONIKA NEGERI SURABAYA

2020/2021

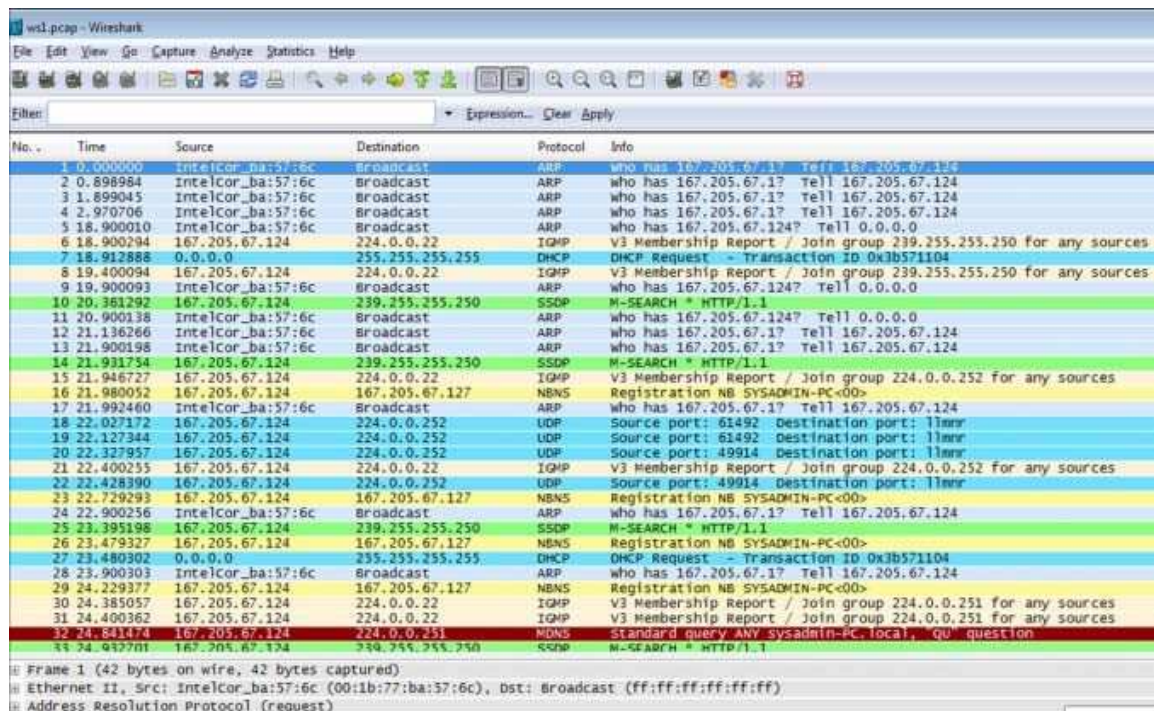
Wireshark

A. TUJUAN

1. Mengenalkan pada mahasiswa tentang konsep wireshark
2. Mahasiswa memahami konsep pengiriman dengan traceroute
3. Mahasiswa memahami proses fragmentasi

B. DASAR TEORI

Wireshark merupakan software untuk melakukan analisa lalu-lintas jaringan komputer, yang memiliki fungsi-fungsi yang amat berguna bagi profesional jaringan, administrator jaringan, peneliti, hingga pengembang piranti lunak jaringan. Wireshark dapat membaca data secara langsung dari Ethernet, Token-Ring, FDDI, serial (PPP and SLIP), 802.11 wireless LAN , dan koneksi ATM.



The screenshot shows the Wireshark interface with a list of captured packets. The columns are No., Time, Source, Destination, Protocol, and Info. The packets are numbered 1 through 34. The source and destination addresses are mostly 167.205.67.124 and 224.0.0.22. The protocols include ARP, IGMP, DHCP, NBNS, SSDP, and UDP. The info column provides details for each packet, such as 'who has 167.205.67.124' for ARP and 'V3 Membership Report' for IGMP.

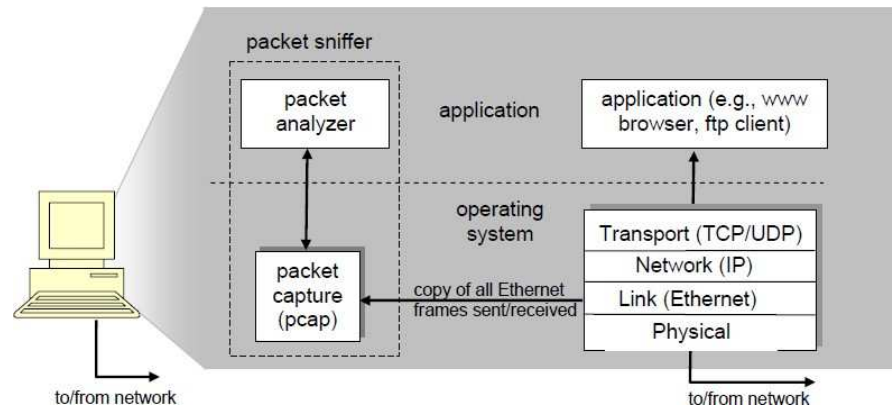
No.	Time	Source	Destination	Protocol	Info
1	0.000000	IntelCor_ba:57:6c	Broadcast	ARP	who has 167.205.67.124 Tell 167.205.67.124
2	0.898984	IntelCor_ba:57:6c	Broadcast	ARP	who has 167.205.67.124 Tell 167.205.67.124
3	1.899045	IntelCor_ba:57:6c	Broadcast	ARP	who has 167.205.67.124 Tell 167.205.67.124
4	2.970706	IntelCor_ba:57:6c	Broadcast	ARP	who has 167.205.67.124 Tell 167.205.67.124
5	18.900010	IntelCor_ba:57:6c	Broadcast	ARP	who has 167.205.67.124 Tell 167.205.67.124
6	18.900294	167.205.67.124	224.0.0.22	IGMP	V3 Membership Report / Join group 239.255.255.250 for any sources
7	18.912888	0.0.0.0	255.255.255.255	DHCP	DHCP Request - Transaction ID 0x3b571104
8	19.400094	167.205.67.124	224.0.0.22	IGMP	V3 Membership Report / Join group 239.255.255.250 for any sources
9	19.900093	IntelCor_ba:57:6c	Broadcast	ARP	who has 167.205.67.124 Tell 167.205.67.124
10	20.361292	167.205.67.124	239.255.255.250	SSDP	M-SEARCH * HTTP/1.1
11	20.900138	IntelCor_ba:57:6c	Broadcast	ARP	who has 167.205.67.124 Tell 167.205.67.124
12	21.136266	IntelCor_ba:57:6c	Broadcast	ARP	who has 167.205.67.124 Tell 167.205.67.124
13	21.900198	IntelCor_ba:57:6c	Broadcast	ARP	who has 167.205.67.124 Tell 167.205.67.124
14	21.931754	167.205.67.124	239.255.255.250	SSDP	M-SEARCH * HTTP/1.1
15	21.946727	167.205.67.124	224.0.0.22	IGMP	V3 Membership Report / Join group 224.0.0.252 for any sources
16	21.980052	167.205.67.124	167.205.67.127	NBNS	Registration NB SYSADMIN-PC<00>
17	21.992460	IntelCor_ba:57:6c	Broadcast	ARP	who has 167.205.67.124 Tell 167.205.67.124
18	22.027172	167.205.67.124	224.0.0.252	UDP	Source port: 61492 Destination port: 11mr
19	22.127344	167.205.67.124	224.0.0.252	UDP	Source port: 61492 Destination port: 11mr
20	22.327957	167.205.67.124	224.0.0.252	UDP	Source port: 49914 Destination port: 11mr
21	22.400255	167.205.67.124	224.0.0.22	IGMP	V3 Membership Report / Join group 224.0.0.252 for any sources
22	22.428390	167.205.67.124	224.0.0.252	UDP	Source port: 49914 Destination port: 11mr
23	22.729293	167.205.67.124	167.205.67.127	NBNS	Registration NB SYSADMIN-PC<00>
24	22.900256	IntelCor_ba:57:6c	Broadcast	ARP	who has 167.205.67.124 Tell 167.205.67.124
25	23.395198	167.205.67.124	239.255.255.250	SSDP	M-SEARCH * HTTP/1.1
26	23.479327	167.205.67.124	167.205.67.127	NBNS	Registration NB SYSADMIN-PC<00>
27	23.480302	0.0.0.0	255.255.255.255	DHCP	DHCP Request - Transaction ID 0x3b571104
28	23.900303	IntelCor_ba:57:6c	Broadcast	ARP	who has 167.205.67.124 Tell 167.205.67.124
29	24.229377	167.205.67.124	167.205.67.127	NBNS	Registration NB SYSADMIN-PC<00>
30	24.385057	167.205.67.124	224.0.0.22	IGMP	V3 Membership Report / Join group 224.0.0.251 for any sources
31	24.400362	167.205.67.124	224.0.0.22	IGMP	V3 Membership Report / Join group 224.0.0.251 for any sources
32	24.841474	167.205.67.124	224.0.0.251	NBNS	Standard query any sysadmin-pc.local, QID question
33	24.842701	167.205.67.124	239.255.255.250	SSDP	M-SEARCH * HTTP/1.1

Gambar 1. Tampilan wireshark

Tools ini bisa menangkap paket-paket data/informasi yang berjalan dalam jaringan. Semua jenis paket informasi dalam berbagai format protokol pun akan dengan mudah ditangkap dan dianalisa. Karenanya tak jarang tool ini juga dapat dipakai untuk sniffing (memperoleh informasi penting seperti password email atau account lain) dengan

menangkap paket-paket yang berjalan di dalam jaringan dan menganalisisnya. Namun tools ini hanya bisa bekerja didalam dalam jaringan melalui LAN/Ethernet Card yang ada di PC

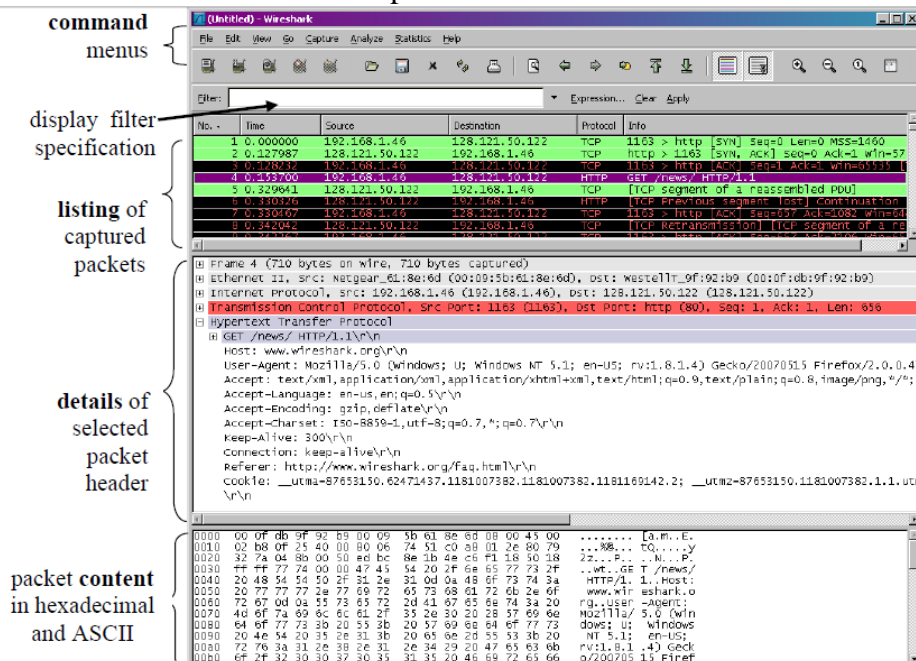
Untuk struktur dari packet sniffer terdiri dari 2 bagian yaitu packet analyzer pada layer application dan packet capture pada layer operating system (kernel).



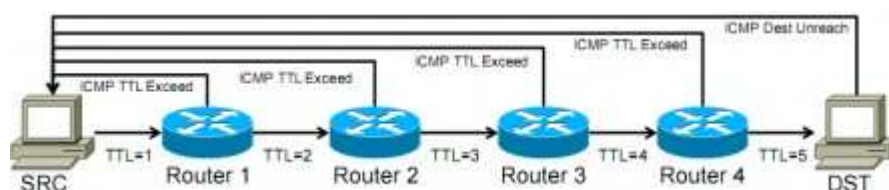
Gambar 2. Struktur Packet Sniffer

Struktur dari wireshark graphical user interface adalah sebagai berikut :

- Command menu
- Display filter specification : untuk memfilter packet data
- Listing of captured packets : paket data yang tertangkap oleh wireshark
- Details of selected packet header : data lengkap tentang header dari suatu packet
- Packet contents : isi dari suatu packet data



Gambar 3. Struktur Wireshark



Untuk mengetahui jalur yang ditempuh untuk mencapai suatu node, traceroute

mengirimkan 3 buah paket probe tipe UDP dari port sumber berbeda, dengan TTL bernilai 1. Saat paket tersebut mencapai router next-hop, TTL paket akan dikurangi satu sehingga menjadi 0, dan router next-hop akan menolak paket UDP tersebut sembari mengirimkan paket ICMP Time-to-Live Exceeded ke node asal traceroute tersebut. Dengan cara ini, pengirim traceroute tahu alamat IP pertama dari jalur yang ditempuh.

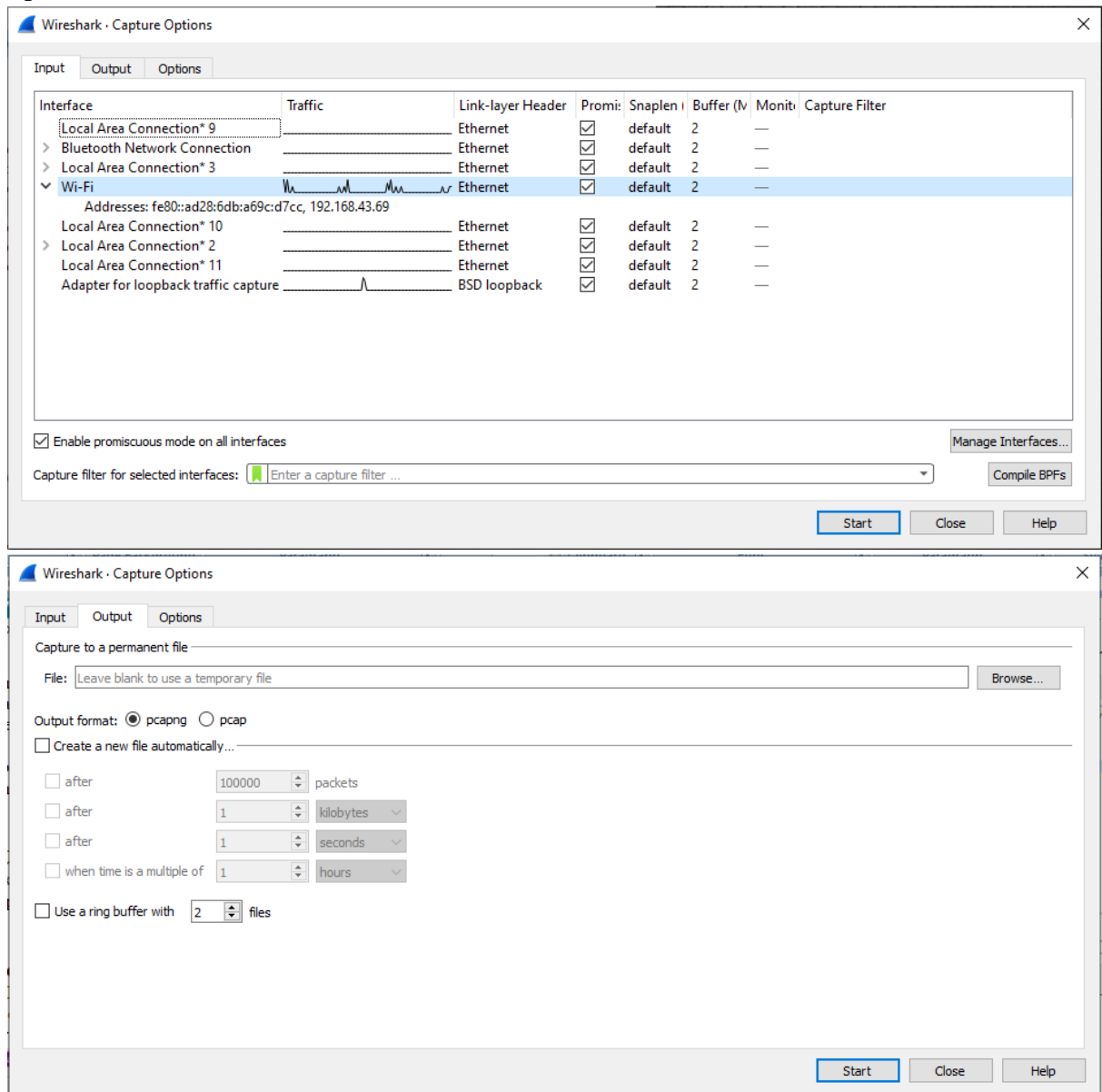
C. TUGAS PENDAHULUAN

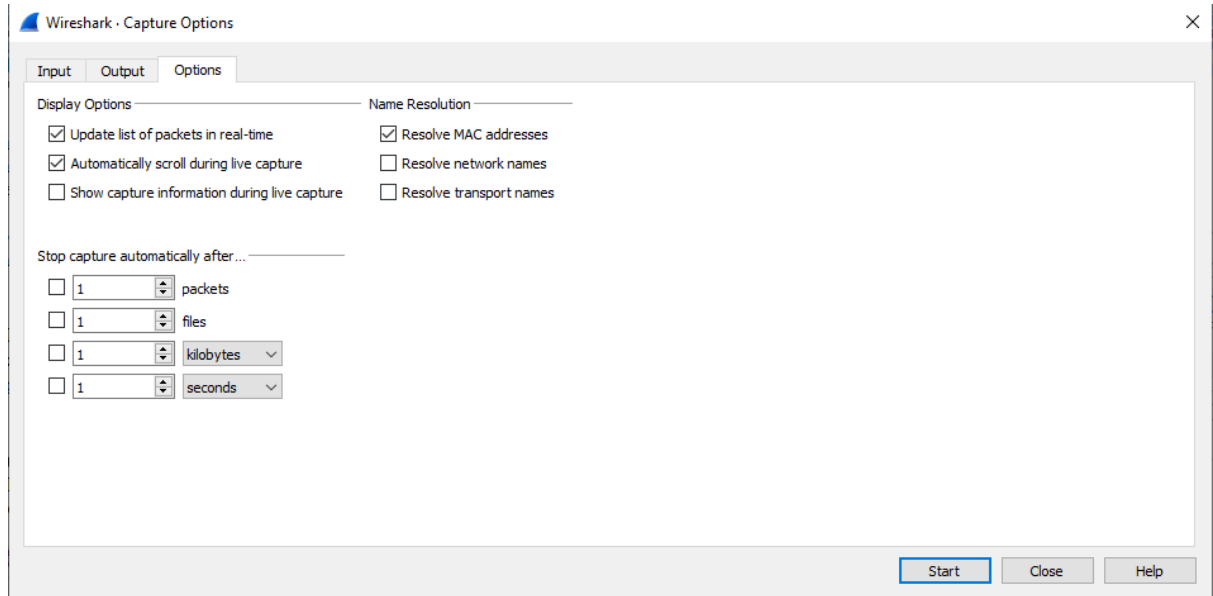
Mendownload paket wireshark dan pingplotter

D. PERCOBAAN

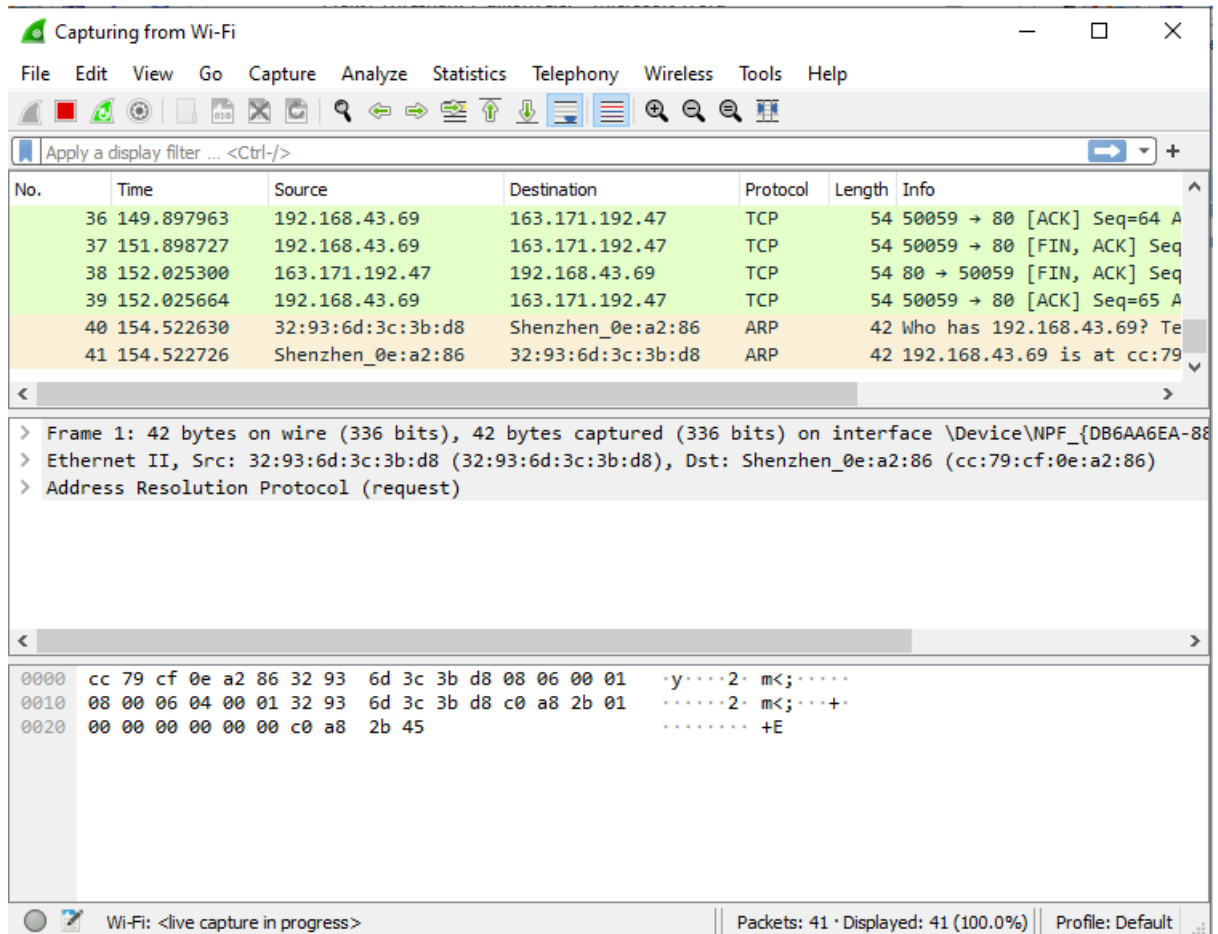
Pengenalan Wireshark

1. Bukalah wireshark. Dan mulai mengcapture paket data dengan memilih Capture | Options.

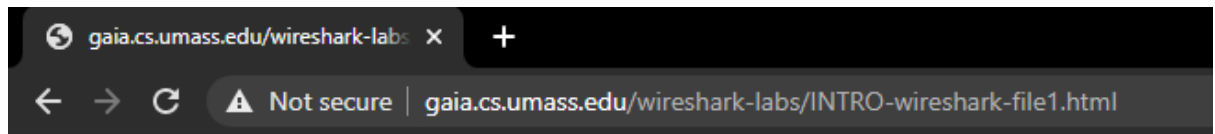




2. Memulai pengamatan dengan menekan tombol start.

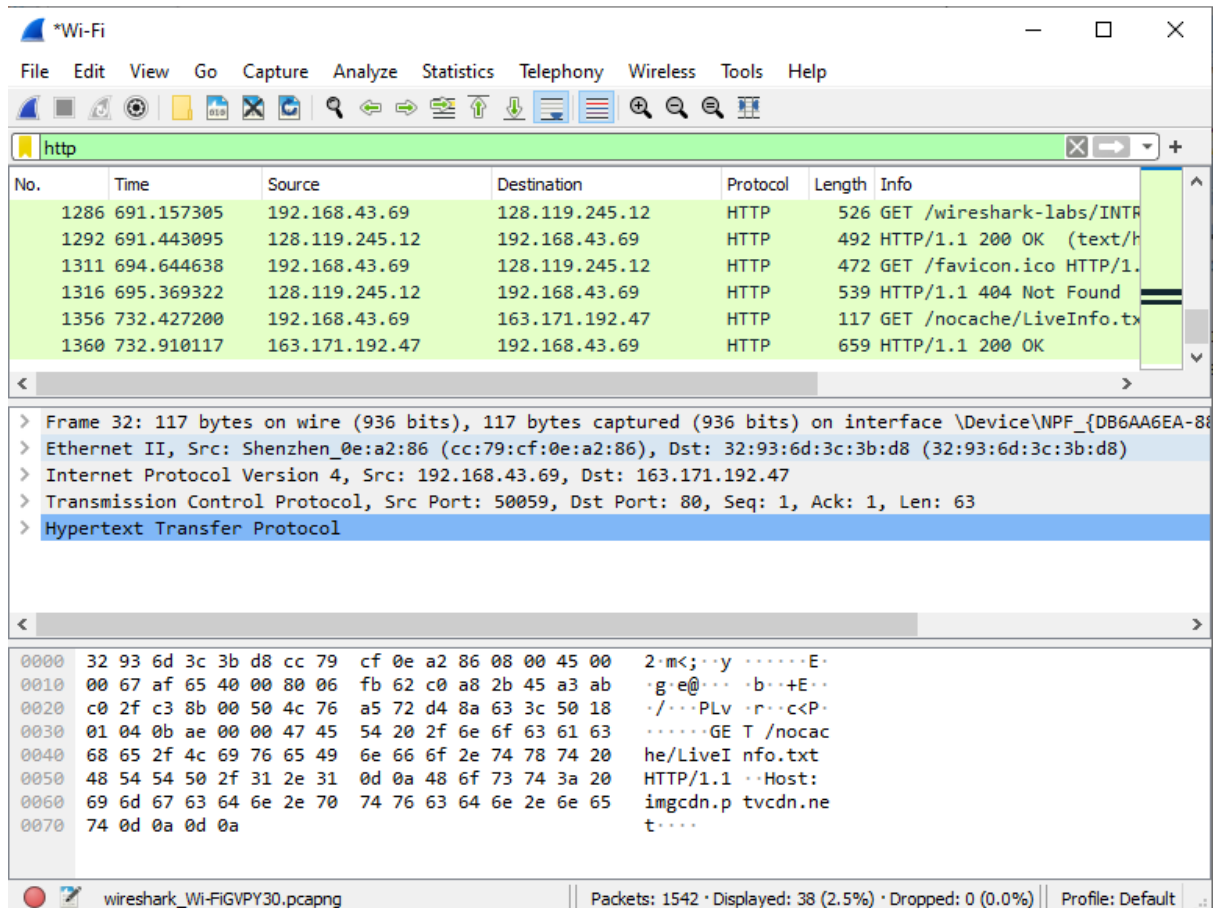


3. Saat wireshare jalan, melakukan koneksi ke :
<http://gaia.cs.umass.edu/wireshark-labs/INTRO-wireshark-file1.html>



Congratulations! You've downloaded the first Wireshark lab file!

Setelah tampilan pada browser keluar, stop wireshark, Chapture | Stop. Kemudian melakukan filter pada protokol agar protokol http saja yang ditampilkan.



4. Dari HTTP GET message diatas yang dikirim dari komputer anda ke gaia HTTP server. Amatilah data berikut pada informasi header packet dan juga content informasi yang dikandungnya :

- a. Ethernet frame


```

  Frame 32: 117 bytes on wire (936 bits), 117 bytes captured (936 bits) on interface \Device\NPF_{DB6AA6EA-88E9-44A9-B5CE-9A55E6A58A7D}, id 0
    Interface id: 0 (\Device\NPF_{DB6AA6EA-88E9-44A9-B5CE-9A55E6A58A7D})
      Interface name: \Device\NPF_{DB6AA6EA-88E9-44A9-B5CE-9A55E6A58A7D}
      Interface description: Wi-Fi
      Encapsulation type: Ethernet (1)
      Arrival Time: May 25, 2021 14:36:53.216631000 SE Asia Standard Time
      [Time shift for this packet: 0.000000000 seconds]
      Epoch Time: 1621928213.216631000 seconds
      [Time delta from previous captured frame: 0.001795000 seconds]
      [Time delta from previous displayed frame: 0.000000000 seconds]
      [Time since reference or first frame: 149.609703000 seconds]
      Frame Number: 32
      Frame Length: 117 bytes (936 bits)
      Capture Length: 117 bytes (936 bits)
      [Frame is marked: False]
      [Frame is ignored: False]
      [Protocols in frame: eth:ethertype:ip:tcp:http]
      [Coloring Rule Name: HTTP]
      [Coloring Rule String: http || tcp.port == 80 || http2]
    Ethernet II, Src: Shenzhen_0e:a2:86 (cc:79:cf:0e:a2:86), Dst: 32:93:6d:3c:3b:d8 (32:93:6d:3c:3b:d8)
      Destination: 32:93:6d:3c:3b:d8 (32:93:6d:3c:3b:d8)
        Address: 32:93:6d:3c:3b:d8 (32:93:6d:3c:3b:d8)
          .... 1. .... = LG bit: Locally administered address (this is NOT the factory default)
          .... 0 .... = IG bit: Individual address (unicast)
      Source: Shenzhen_0e:a2:86 (cc:79:cf:0e:a2:86)
        Address: Shenzhen_0e:a2:86 (cc:79:cf:0e:a2:86)
          .... 0. .... = LG bit: Globally unique address (factory default)
          .... 0 .... = IG bit: Individual address (unicast)
      Type: IPv4 (0x0800)

```

b. IP datagram

```

  Internet Protocol Version 4, Src: 192.168.43.69, Dst: 163.171.192.47
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
    Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
      0000 00.. = Differentiated Services Codepoint: Default (0)
      .... ..00 = Explicit Congestion Notification: Not ECN-Capable Transport (0)
    Total Length: 103
    Identification: 0xaf65 (44901)
    Flags: 0x40, Don't fragment
      0... .... = Reserved bit: Not set
      .1.. .... = Don't fragment: Set
      ..0. .... = More fragments: Not set
    Fragment Offset: 0
    Time to Live: 128
    Protocol: TCP (6)
    Header Checksum: 0xfb62 [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 192.168.43.69
    Destination Address: 163.171.192.47

```

c. TCP segment

```

Transmission Control Protocol, Src Port: 50059, Dst Port: 80, Seq: 1, Ack: 1, Len: 63
  Source Port: 50059
  Destination Port: 80
  [Stream index: 1]
  [TCP Segment Len: 63]
  Sequence Number: 1 (relative sequence number)
  Sequence Number (raw): 1282844018
  [Next Sequence Number: 64 (relative sequence number)]
  Acknowledgment Number: 1 (relative ack number)
  Acknowledgment number (raw): 3565839164
  0101 .... = Header Length: 20 bytes (5)
  Flags: 0x018 (PSH, ACK)
    000. .... = Reserved: Not set
    ...0 .... = Nonce: Not set
    .... 0... = Congestion Window Reduced (CWR): Not set
    .... .0.. = ECN-Echo: Not set
    .... ..0. = Urgent: Not set
    .... ...1 = Acknowledgment: Set
    .... .... 1... = Push: Set
    .... .... .0.. = Reset: Not set
    .... .... ..0. = Syn: Not set
    .... .... ...0 = Fin: Not set
    [TCP Flags: .....AP....]
  Window: 260
  [Calculated window size: 66560]
  [Window size scaling factor: 256]
  Checksum: 0x0bae [unverified]
  [Checksum Status: Unverified]
  Urgent Pointer: 0
  [SEQ/ACK analysis]
    [iRTT: 0.203085000 seconds]
    [Bytes in flight: 63]
    [Bytes sent since last PSH flag: 63]
  [Timestamps]
    [Time since first frame in this TCP stream: 0.204880000 seconds]
    [Time since previous frame in this TCP stream: 0.001795000 seconds]

```

d. HTTP message

```

Hypertext Transfer Protocol
  GET /nocache/LiveInfo.txt HTTP/1.1\r\n
    [Expert Info (Chat/Sequence): GET /nocache/LiveInfo.txt HTTP/1.1\r\n]
      [GET /nocache/LiveInfo.txt HTTP/1.1\r\n]
      [Severity level: Chat]
      [Group: Sequence]
    Request Method: GET
    Request URI: /nocache/LiveInfo.txt
    Request Version: HTTP/1.1
    Host: imgcdn.ptvcdn.net\r\n
    \r\n
    [Full request URI: http://imgcdn.ptvcdn.net/nocache/LiveInfo.txt]
    [HTTP request 1/1]
    [Response in frame: 35]

```

Pengamatan Traceroute IP

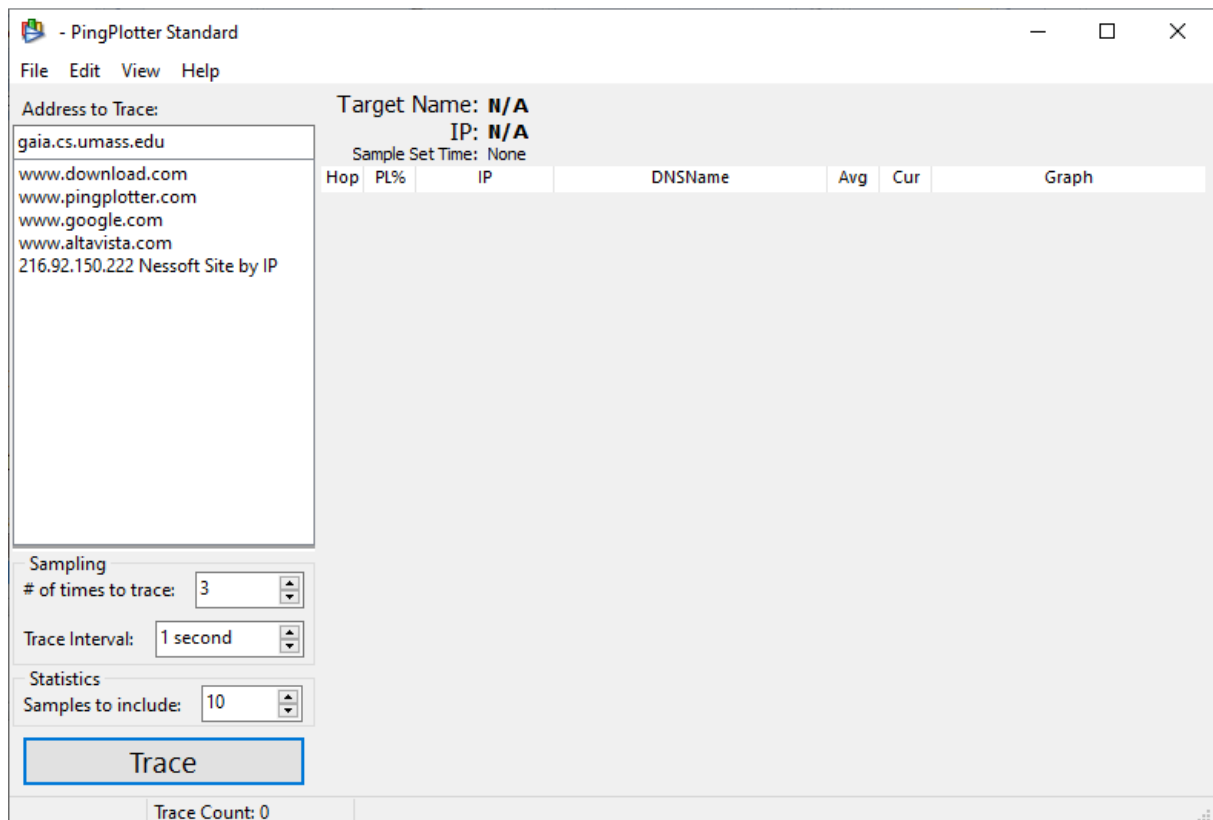
1. Download program pingplotter, dan gunakan dengan MS. Widows.

2. Setting dengan ketentuan :

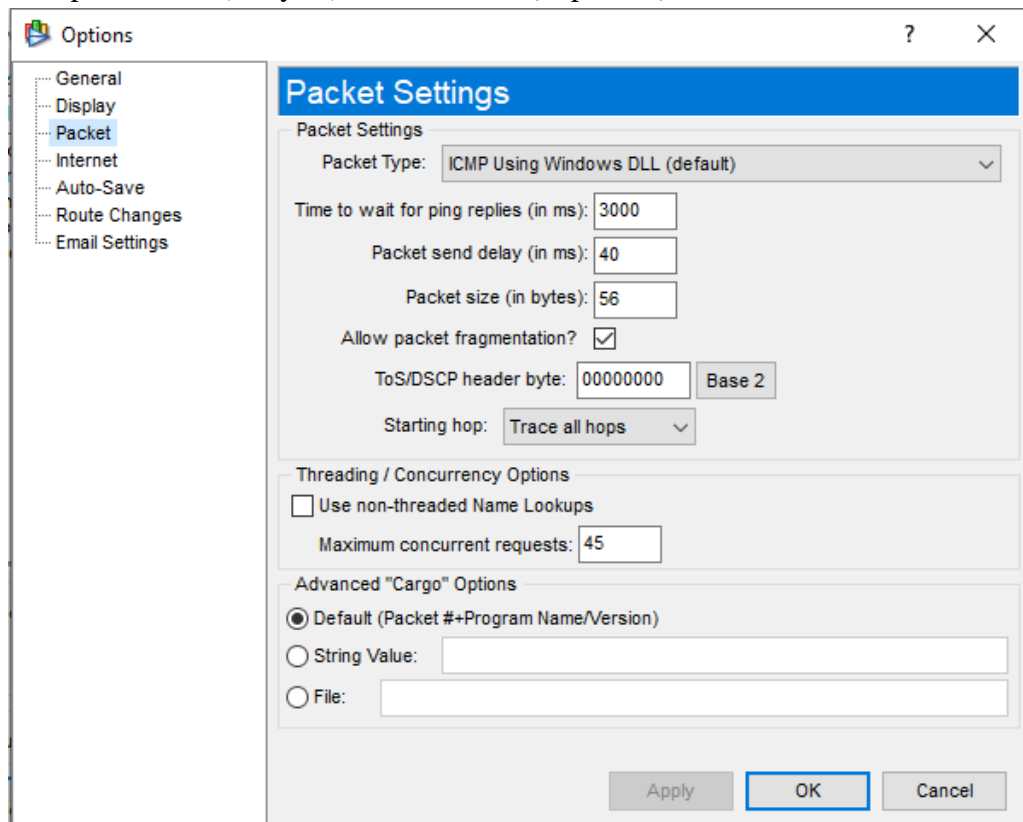
Address to trace : gaia.cs.umass.edu

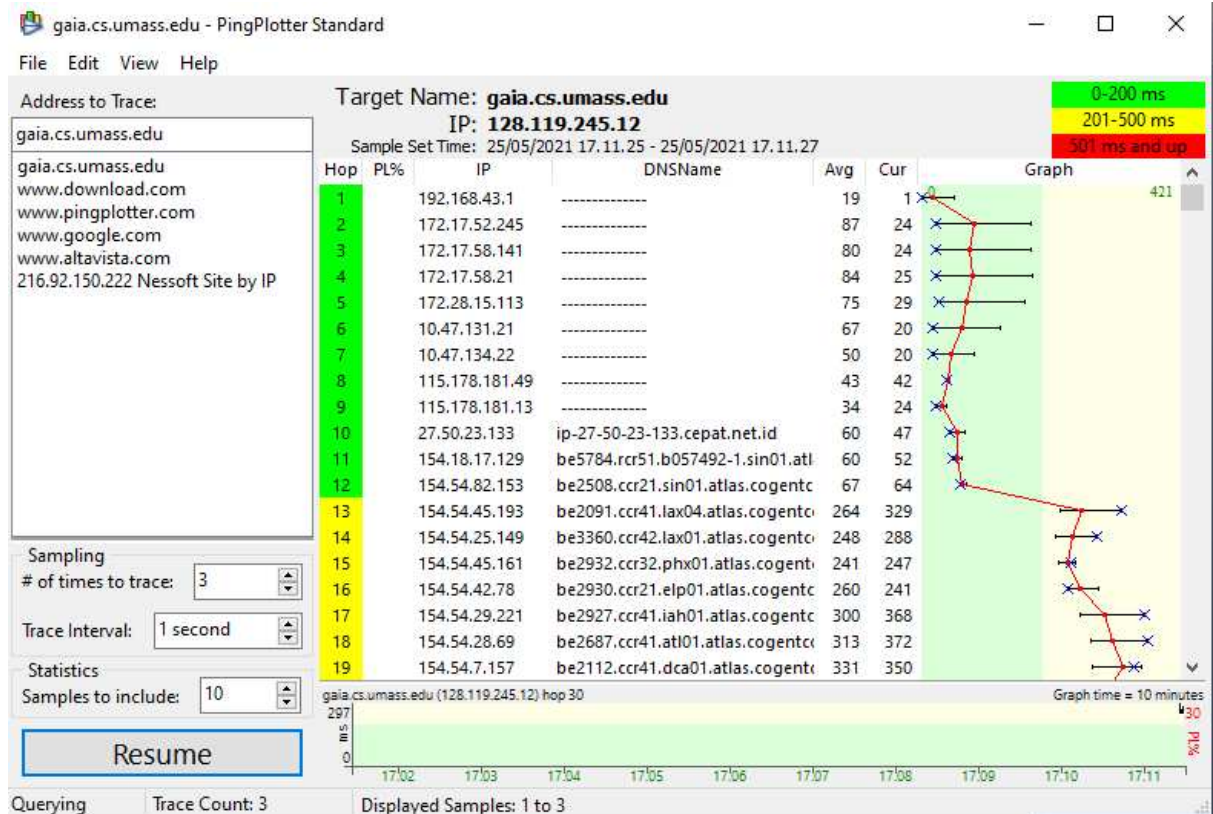
of time to trace : 3

Trace Interval : 1 second

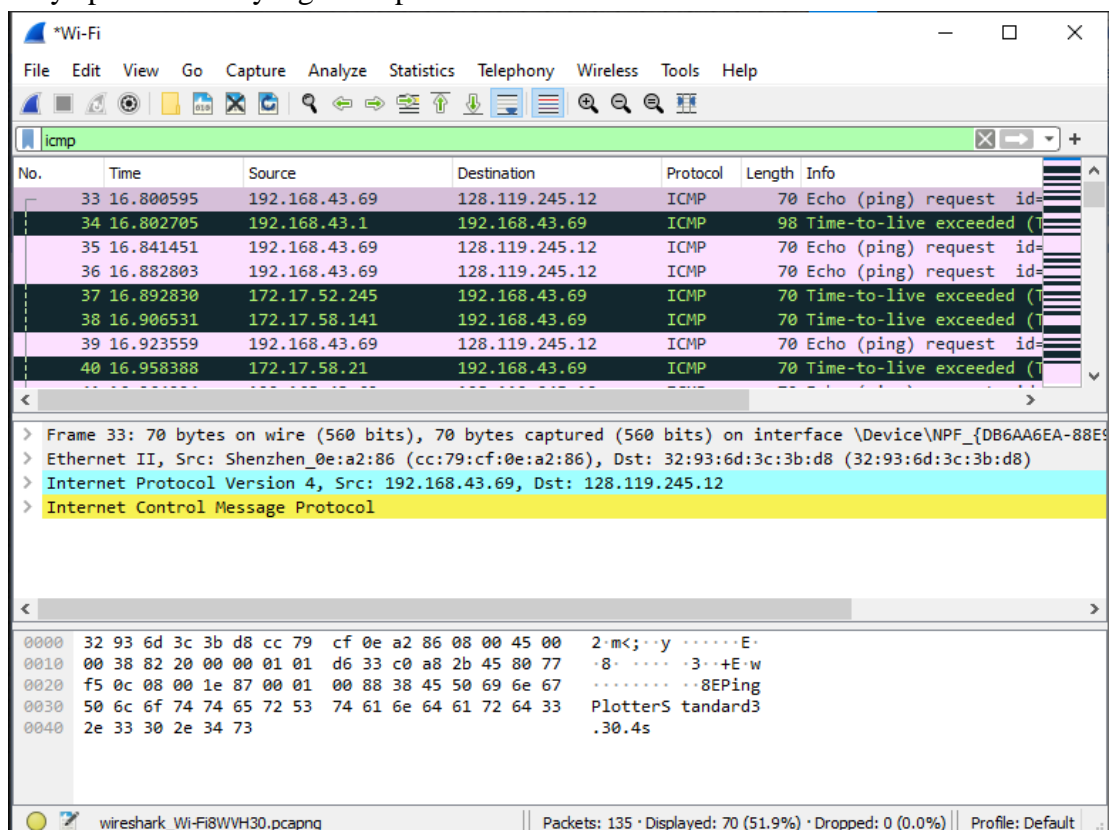


Atur packet size (in bytes) : 56, dari Edit | Options | Packet





3. Aktifkan wireshark untuk memulai mengcapture paket, dan tekan tombol trace pada pingplotter.
4. Matikan Matikan wireshark jika sudah selesai, lakukan filter paket ICMP agar hanya paket ICMP yang ditampilkan.

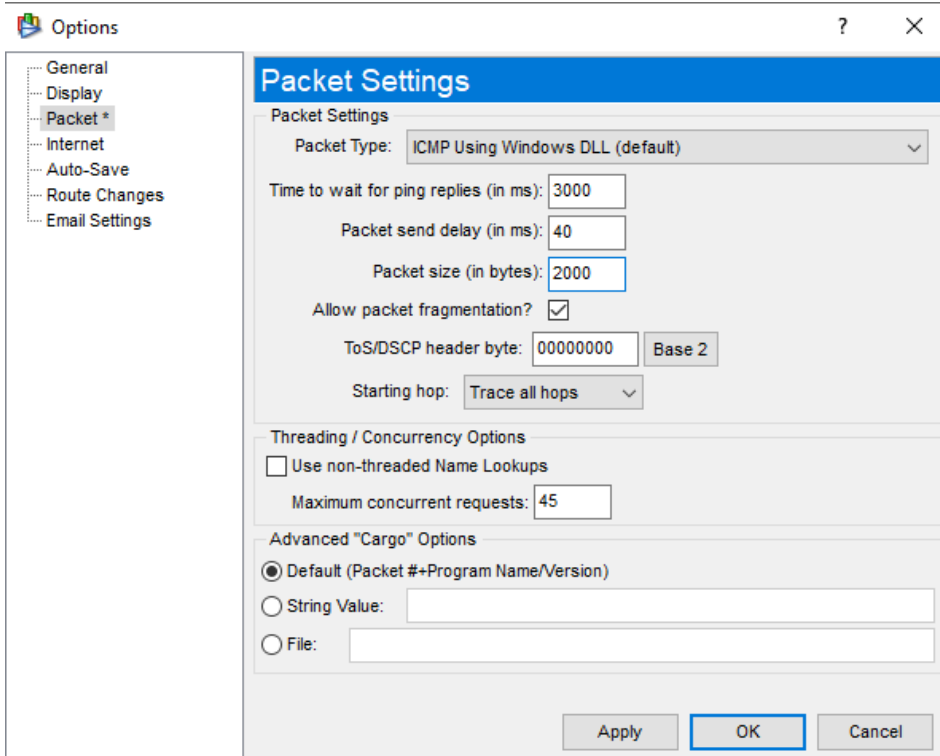


5. Pilih ICMP Echo Request message yang pertama yang dikirim oleh komputer anda, dan expand bagian paket Internet Protocol.

```
▼ Internet Protocol Version 4, Src: 192.168.43.69, Dst: 128.119.245.12
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
    ▼ Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
        0000 00.. = Differentiated Services Codepoint: Default (0)
        .... ..00 = Explicit Congestion Notification: Not ECN-Capable Transport (0)
    Total Length: 56
    Identification: 0x8220 (33312)
    ▼ Flags: 0x00
        0... .... = Reserved bit: Not set
        .0.. .... = Don't fragment: Not set
        ..0. .... = More fragments: Not set
    Fragment Offset: 0
    ▼ Time to Live: 1
        ▼ [Expert Info (Note/Sequence): "Time To Live" only 1]
            ["Time To Live" only 1]
            [Severity level: Note]
            [Group: Sequence]
        Protocol: ICMP (1)
        Header Checksum: 0xd633 [validation disabled]
        [Header checksum status: Unverified]
        Source Address: 192.168.43.69
        Destination Address: 128.119.245.12
```

Pengamatan Fragmentation

1. Mengulagi langkah B 1-4, dengan ukuran paket dirubah menjadi 2000



*Wi-Fi

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

icmp

No.	Time	Source	Destination	Protocol	Length	Info
8	30.222498	192.168.43.69	128.119.245.12	ICMP	534	Echo (ping) request id=
10	30.243540	192.168.43.69	128.119.245.12	ICMP	534	Echo (ping) request id=
11	30.244587	192.168.43.1	192.168.43.69	ICMP	590	Time-to-live exceeded (T
13	30.284121	192.168.43.69	128.119.245.12	ICMP	534	Echo (ping) request id=
15	30.325781	192.168.43.69	128.119.245.12	ICMP	534	Echo (ping) request id=
17	30.367348	192.168.43.69	128.119.245.12	ICMP	534	Echo (ping) request id=
19	30.489227	192.168.43.69	128.119.245.12	ICMP	534	Echo (ping) request id=
21	30.494607	192.168.43.69	128.119.245.12	ICMP	534	Echo (ping) request id=

> Frame 8: 534 bytes on wire (4272 bits), 534 bytes captured (4272 bits) on interface \Device\NPF_{DB6AA6E}

> Ethernet II, Src: Shenzhen_0e:a2:86 (cc:79:cf:0e:a2:86), Dst: 32:93:6d:3c:3b:d8 (32:93:6d:3c:3b:d8)

▼ Internet Protocol Version 4, Src: 192.168.43.69, Dst: 128.119.245.12

- 0100 = Version: 4
- 0101 = Header Length: 20 bytes (5)
- ▼ Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
 - 0000 00.. = Differentiated Services Codepoint: Default (0)

0000 32 93 6d 3c 3b d8 cc 79 cf 0e a2 86 08 00 45 00 2 m<;...yE

0010 02 08 82 43 00 b9 01 01 d3 87 c0 a8 2b 45 80 77 ...C.....+E.w

0020 f5 0c 33 2e 33 30 2e 34 73 31 31 45 50 69 6e 67 ..3.30.4 s11EPing

0030 50 6c 6f 74 74 65 72 53 74 61 6e 64 61 72 64 33 PlotterS tandard3

0040 2e 33 30 2e 34 73 31 31 45 50 69 6e 67 50 6c 6f .30.4s11 EPingPlo

0050 74 74 65 72 53 74 61 6e 64 61 72 64 33 2e 33 30 tterStan dard3.30

Frame (534 bytes) Reassembled IPv4 (1980 bytes)

Internet Control Message Protocol: Protocol | Packets: 92 · Displayed: 36 (39.1%) · Dropped: 0 (0.0%) | Profile: Default

▼ Internet Protocol Version 4, Src: 192.168.43.69, Dst: 128.119.245.12

- 0100 = Version: 4
- 0101 = Header Length: 20 bytes (5)
- ▼ Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
 - 0000 00.. = Differentiated Services Codepoint: Default (0)
 -00 = Explicit Congestion Notification: Not ECN-Capable Transport (0)
- Total Length: 520
- Identification: 0x8243 (33347)
- ▼ Flags: 0x00
 - 0... = Reserved bit: Not set
 - .0.. = Don't fragment: Not set
 - ..0. = More fragments: Not set
- Fragment Offset: 1480
- ▼ Time to Live: 1
 - ▼ [Expert Info (Note/Sequence): "Time To Live" only 1]
 - ["Time To Live" only 1]
 - [Severity level: Note]
 - [Group: Sequence]
 - Protocol: ICMP (1)
 - Header Checksum: 0xd387 [validation disabled]
 - [Header checksum status: Unverified]
 - Source Address: 192.168.43.69
 - Destination Address: 128.119.245.12
 - ▼ [2 IPv4 Fragments (1980 bytes): #7(1480), #8(500)]
 - [Frame: 7, payload: 0-1479 (1480 bytes)]
 - [Frame: 8, payload: 1480-1979 (500 bytes)]
 - [Fragment count: 2]
 - [Reassembled IPv4 length: 1980]
 - [Reassembled IPv4 data: 0800b30f000100ab31314550696e67506c6f747465725374616e64617264332e33302e34...]

E. KESIMPULAN

- Wireshark merupakan software untuk melakukan analisa lalu-lintas jaringan komputer, yang memiliki fungsi-fungsi yang amat berguna bagi profesional jaringan, administrator jaringan, peneliti, hingga pengembang piranti lunak jaringan. Wireshark dapat membaca data secara langsung dari Ethernet, Token-Ring, FDDI, serial (PPP and SLIP), 802.11 wireless LAN , dan koneksi ATM.
- PingPlotter Standard adalah utilitas sederhana yang menangani operasi ini dan memungkinkan Anda memonitor hasilnya melalui antarmuka nyaman yang dapat diakses untuk semua tipe pengguna. Hasilnya dapat diekspor ke berkas teks atau berkas gambar. Di antara berbagai parameter yang memungkinkan Anda mengonfigurasi tiap sesi, Anda dapat mengatur berapa kali tes dilakukan dan waktu jeda antara tes.