NAMA:BAGUS SAJIWO
NIM:1310651132
KELAS:B

The goal of access control is to allow authorized users to access the appropriate data and deny access to unauthorized users. Access control to protect against threats such as unauthorized access, inappropriate modification of data, and loss of confidentiality.

CORNERSTONE CONCEPT OF INFORMATION SECURITY

Before we could explain access control, we must define the concept of information runway secu-rity. These concepts provide the basis upon which the domain 10
General body of knowledge built
Confidentiality, integrity, and availability
secrecy

integrity and availability are the "CIA triad," the cornerstone con
except that information security. Triad, which is shown in, Forming three-legged Information security is built on top of the bench. Acronym sequence may change (some
more "AIC," perhaps to avoid a relationship with a particular intelligence agency), but
concepts that are important. This book will use "CIA" stands
Confidentiality trying to prevent the unauthorized disclosure of information: it makes
confidential data. In other words, confidentiality trying to prevent unauthorized access read
data. Examples of attacks would secrecy theft
Personally iden-
Information tifiable
(PII), such as credit card information
Integrity seeks to prevent unauthorized modification of information. In other words,
integrity trying to prevent unauthorized write access to the data integrity of trying to prevent the unauthorized modification of information. In other words, integrity trying to prevent unauthorized write access to data.

CRUNCH TIME

There are two types of integrity: the integrity of the data and the integrity of the system. Data integrity trying to
protecting information against unauthorized modification; the integrity of the system trying to protect the system, such as Windows server operating system in 2012, from unauthorized modification.
Availability Availability ensures that information is available when needed. The system should be used (provided) for normal business use. Examples of attacks against ketersediaanakan become Denial-of-Service
(DoS) attacks, which seek to deny service (or availabil-ity) of the system.

Identity and Authentication
Identity is the claim: if your name is "Person X," you identify yourself by saying "I People X. "Identities be weak because there is no evidence. You can also identify themselves by saying "I Person Y." Proving identity claims referred authentication: you authenticate the identity claim, usually by providing a piece of information
or an object that only you have, such as passwords or your passport.
A subject is an active entity in the system data. Most examples involve lessons accessing the data file. However, a computer program that is running is the subject as well.
a
the object is passive data into the system. Objects can range from database
to a text file. The important thing to remember about objects is that they are passive
in the system. They do not manipulate other objects.

Nondiscretionary access control
Role-Based Access Control
(RBAC) Defines how information is accessed on the system
based on the role of the subject. A role can be a nurse, backup administrator,
help desk technician, etc. The subjects are grouped into roles and each role has defined access permissions based on roles, not individuals.
RBAC is a nondiscretionary access control
because the rule-based access control,
then allow access). Other sites are prohibited and these rules apply throughout the all authenticated users.
Centralized access control
Centralized access control
concentrating in a single point of access control to logical

system or organization. inst
ead using local access control database system
authenticate through a third par
ty authentication server. Centralized access control
can be used to provide Single Sign-On (SSO), in which the subject can authenticate
once, and then access multiple systems. Centralized access control can be centralized
provides three "A" of the access control: Authentication, Authorization, and Accountability.

Access control list
Access control list
(ACL) is used across many IT security policies, procedures, and technology. Access control list is a list of objects; each entry describes the
subjects that can access the object. Subject attempts to access an object
which does not have a matching entry in the ACL will be rejected.
Access the procurement lifecycle
After proper access control model has been selected and used, the access pro-
the vision of the life cycle must be maintained and secured. While many organizations fol-
Low best practices for issuing access, many shortcomings formal process to ensure
lifetime is kept secure access as employees and contractors engaged in

That RADIUS Remote Authentication Dial-In User Service
(RADIUS) protocol is a third party
authentication system. RADIUS uses the User Datagram Protocol (UDP) port 1812
(Authentication) and 1813 (accounting).
RADIUS is considered a "AAA" system, which consists of three components:
authentication, authorization, and accounting. It authenticates credentials subjects
against the authentication database. This authority allows the user to specific users'
access to specific data objects. It accounts for each session by creating a data log
RADIUS entry for each connection made.
Diameter is RADIUS 'successor, is designed to provide enhanced Authentication,
Authorization, and Accounting (AAA) framework. RADIUS provides a limited
accountability and have problems with flexibility, scalability, reliability, and
security.
Diameter is more flexible, which enables support for remote users mobile phone,
for example.

TACACS.
System Terminal Access Controller Access Control
(TACACS) is a centralized access control system that requires users to send ID and static (reusable) password for authentication. TACACS uses UDP port 49 (and possibly also using TCP). Reusable passwords has security vulnerabilities: enhanced TACACS.

Compensation

QUICK FACTS

This type of access control can fall into one of three categories: administrative, technical, or
Physical.

1.
Administrative
(Also called a directive) controls implemented by creating and following organizational policies, procedures, or regulations. User training and awareness also fall into
this category.

2.
Technical
control is implemented using software, hardware, or firmware that limit
Logical access to the information technology system. Examples include firewalls, routers,
and encryption.

3.
Physical
control is implemented with a physical device, such as locks, fences, gates, and security guards.

Deterrent

Preventive control
prevents the action from occurring. This applies to any restrictions
Potential users, whether authorized or unauthorized, can be done. Examples of administrative prevention control is a pre-employment drug screening.
It is designed to prevent the organization from hiring an employee who uses illegal drugs.

Detective
Detective controls are idle control during or after a successful attack. Intrusion signal detection system after a successful attack, closed circuit television cameras (CCTV) which guards against an intruder alert, and building systems that are triggered alarm
by intruders are examples of detective controls.

Repair

Corrective control working with "fixing" broken systems or processes. Correction tive access control usually works hand in hand with the detective access controls. Antivirus has two components. First, run antivirus software scans and usability definition files to detect whether there is software that matches the virus list. If detects a virus, a corrective control takes over, putting suspicious software quarantine, or delete them from the system.

Recovery

After a security incident has occurred, control recovery may need to be taken in ordered to restore the function of the system and organization. Recovery means that the system must be restored: re-installed from the OS media or images, data is returned of backups, etc.

Deterrent

Control preventer prevent users from performingactions on the system. Examples include "Beware of Dog" sign: thieves face two buildings, one with a guard dog and one without, are more likely to attack a building without a guard dog. Large fines for speeding are deterrent to drivers not to speed up. A policy of sanctions that make users understand that they will be fired if they were caught surfing Web sites is prevention of illicit or illegal.

Compensation

AN compensation control is an additional security controls put in place to compensate weaknesses in other controls.

METHOD OF AUTHENTICATION

A key concept to implement proper control access control authentication subjects in IT systems. Subject A first identify himself or himself; This identification can not be trusted. Subjects were then authenticate by promasi assurance that the identity of the claimed effect. AN

set credential
is the term used
for a combination of both user identification and authentication.

Type 2 authentication (something you have) requires users to have something, such as tokens, which proves they are authenticated users. Token is an object that helps prove the identity claim.
Synchronous dynamic tokens, using the time or counter to synchronize sign displayed
code with the code expected by the server authentication: the synchronized code.
Token-based dynamic synchronous time code display dynamic marks
change frequently, such as every 60 seconds. Dynamic code is only good for window. Authentication server know the serial number of each authorized
mark, the user it is associated with, and time. It can predict the dynamic code
each token uses three pieces of information.
Based-counter synchronous dynamic tok
ens using a simple counter: do expect tication Server authentication token code 1, and the user token displays the same way.
After use, the token displays a second token, and the server also expect
sign # 2

Asynchronous dynamic token, not synchronized with a central server. most
Various public is a challenge-response token. Challenge-response authentica- mark tion system generates a challenge or input to the mark. Then the user credentials ually entering information into the device along with their PIN, and devices generating output. This output is then sent to the system.

3 types of authentication (something you are) is biometrics, which uses physical acteristics
acteristics as a means of identification or authentication. Biometrics can be used to establish identity or to authenticate (prove a claim of identity).
For example, a
These facial recognition system can be used to determine the identity of an unknown
terrorists, and a fingerprint scanner can be used to authenticate the identity of the sub a
ject (who makes a claim of identity and then rubbing his finger to prove it).
Biometric registration and throughput
registration
describes the process of registration with biometric systems: creating

account for the first time. Users typically provide their name (identity), pass a word or PIN, and then provide biometric information, such as fingerprints on swiping
fingerprint reader or after a photo taken of their iris. Registration is a one-on-one a process that should take 2 minutes or less.

CRUNCH TIME

A false accept is worse than false rejects: most organizations would prefer to reject authentic
subject to receiving a fraud. Fars (Type II error) is worse than FRRS (Type I error). Twoisgreaterthanone, whichwillhelpyourememberthatFARisTypeII, whicharewersethan
Type I (FRRS)

Crossover Error Rate

The Crossover Error Rate (CER) describes the point at which the False Reject Rate (FRR) and False Accept Rate (FAR) is the same. CER also known as Equal error Rate (EER).

There are a number of types of biometric controls biometric controls in use today. Here are the main implemen- tations and their specific pros and cons associated with access control security.

fingerprint is the most widely used biometric controls available today. Smartcard can bring fingerprint information. Many US government office buildings rely on fingerprint authentication for physical access to facilities. Examples include smart keyboard, which requires the user to present the fingerprint to unlock the computer screen saver.

The data used to store the fingerprints of each person must be of a size small enough to be used for authentication. This data is a mathematical representation of a finger
print minutiae, the specific details of the mountains of finger swipes, which include whorls,
mountains, bifurcation, and others.

ACCESS CONTROL TECHNOLOGIES

There are several technologies that are used to implement access control.
Since every technology presented, it is important to identify what is unique about each
technical solutions.

Single sign-on

Single Sign-On (SSO) allows multiple systems to use a central authentication server

(US). This allows users to authenticate once and then access multiple, distinct systemic
tems. It also allows the security administrator to add, modify, or revoke user privileges
in one central system.

The main disadvantage to the SSO allows an attacker to gain access to
some sources after sacrificing any of the authentication methods, such as pass
said. SSO should always be used with multifactor authentication for this reason.

Federated identity management

Identity federation Management
(FIdM) applies Single Sign-On in the wider
scale: from cross-organization for Internet scale. Sometimes simply called
Identity Management (IDM). FIdM can use OpenID or SAML (Security Association
Markup Language).

Security Assessment is a holistic approach to assess the effectiveness of access
control. Instead of looking at the narrow penetration test or vulnerability assessment,
security assessment has a broader scope.

SUMMARY PURPOSE EXAM

If one thinks about the castle analogy to security, access control will ditch and
the walls of the fort. Access control ensures that the border protection mechanisms, in the second
logical and physical standpoint, guaranteed. The goal of access control is to allow
authorized users access to the appropriate data and deny access to unauthorized users-
This is also known as the subject of restricting access to objects. Although this task is
complex and involved one, it is possible to implement strong access control pro
gram without burdening users who rely on access to the system.

Protecting the CIA triad is another key aspect to implement access control.
Confidentiality, integrity, and availability is very important.

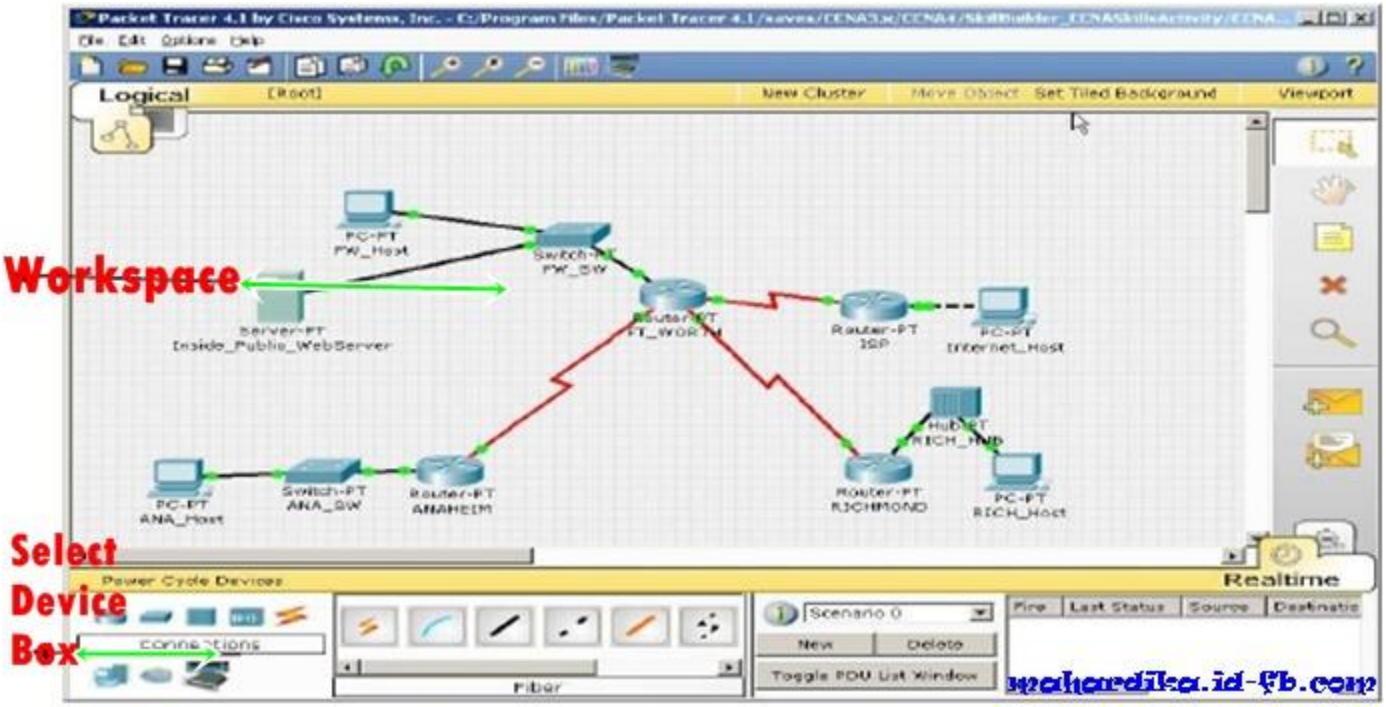
Maintain security during the CIA of the system means enact special procedures
to access the data. This procedure will change depending on the function
users require and sensitivity of the data that is stored on the system

No.2

Terdapat berbagai macam software yang dapat membantu kita dalam menganalisa ataupun mendisain jaringan komputer

A. Packet Tracer

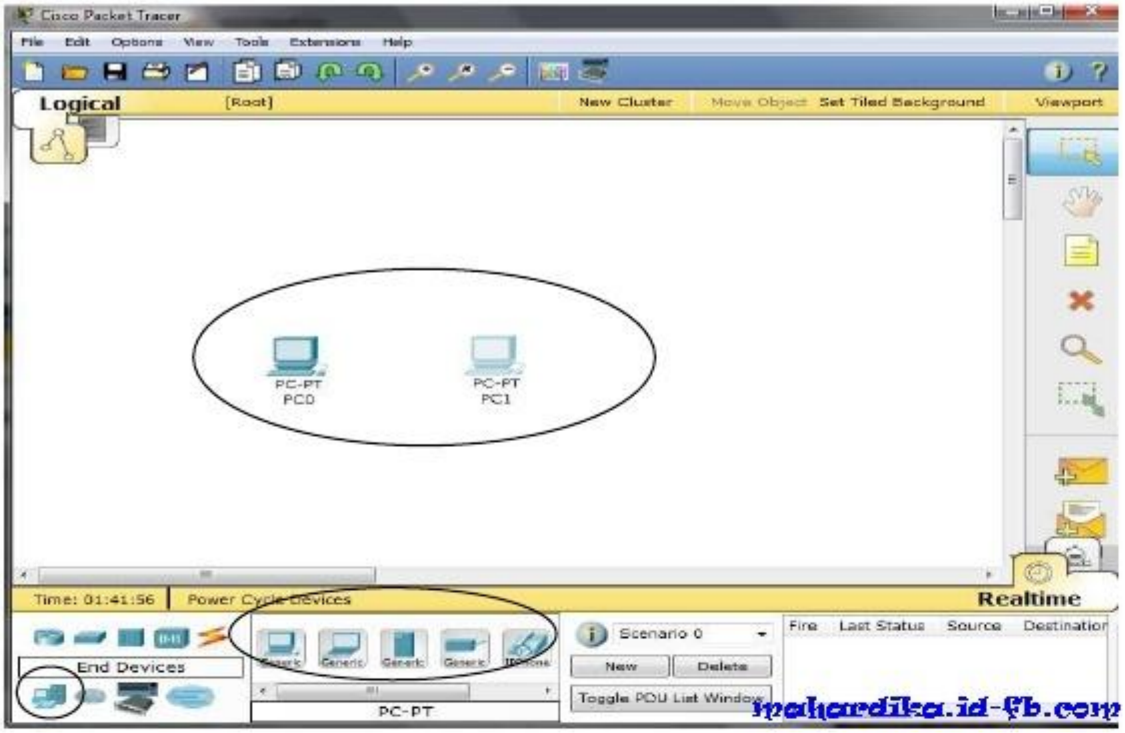
Packet tracer adalah sebuah simulator protocol jaringan yang dikembangkan oleh Cisco System. Paket Tracer dapat mensimulasikan berbagai macam protocol yg digunakan pada jaringan baik secara realtime maupun dengan mode simulasi.



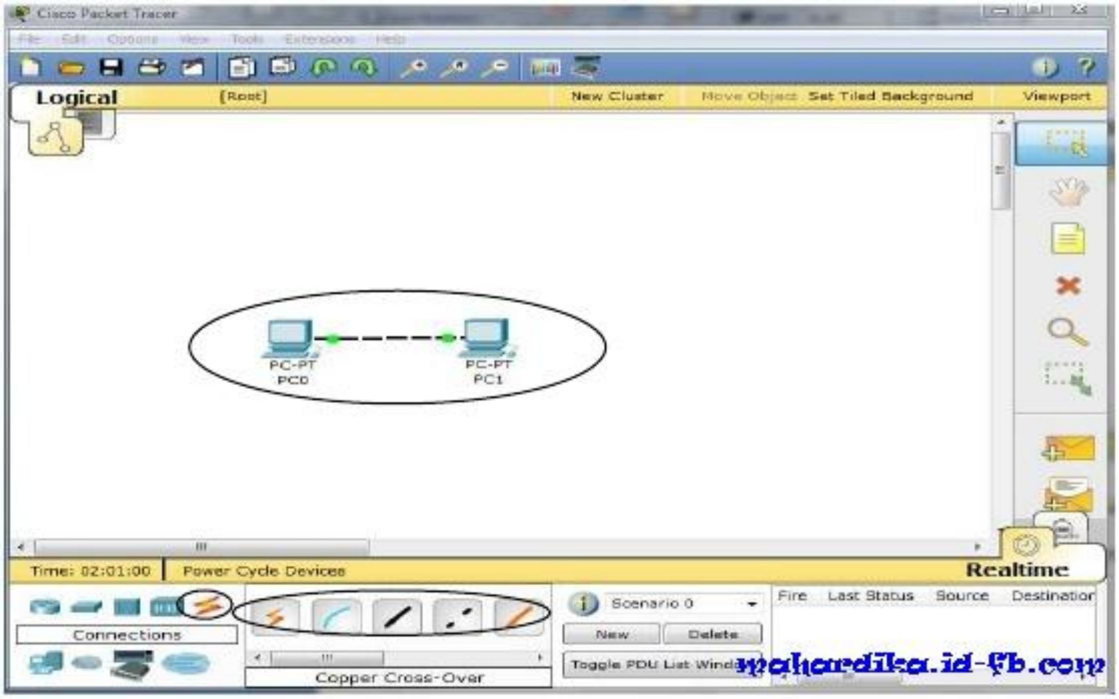
Gambar.1 Tampilan Packet Tracer

Membuat jaringan peer-to-peer menggunakan packet tracer :

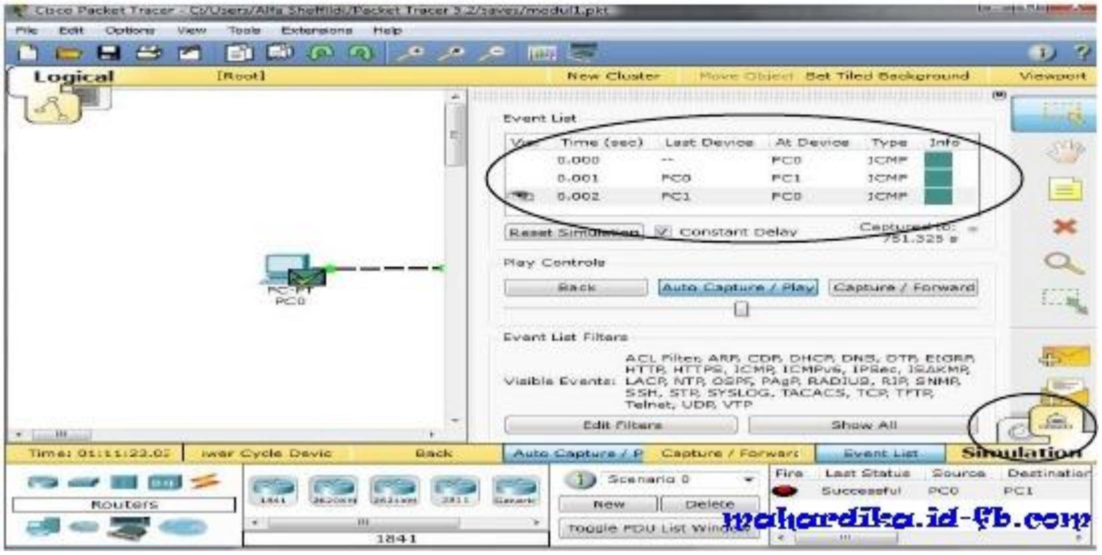
1.Ambil 2 buah PC dari select device box pada bagian end devices ke logical workspace seperti terlihat pada gambar dibawah ini :



2.Hubungkan 2 PC tadi dengan kabel yang sesuai (kabel cross) pada masing-masing port Ethernet



3.Selain mode realtime kita juga dapat memilih mode simulation, dimana pada saat kita melakukan perintah, kita dapat mengetahui prorokol yang digunakan dan apa yang sebenarnya terjadi pada setiap layer. Contohnya pada saat perintah ping pada gambar dibawah ini.



Cisco Packet Tracer - C:/Users/Alfa Sheffildi/Packet Tracer 5.2/saves/modul1.pkt

Event List

Vis.	Time (sec)	Last Device	At Device	Type	Info
	0.000	--	PC0	ICMP	🟩
	0.001	PC0	PC1	ICMP	🟩
	0.002	PC1	PC0	ICMP	🟩

☑ Constant Delay

Captured to: 751.325 s

Visible Events: ACL Filter, ARP, CDP, DHCP, DNS, DTP, EIGRP, HTTP, HTTPS, ICMP, ICMPv6, IPSec, ISAKMP, LACP, NTP, OSPF, PAgP, RADIUS, RIP, SNMP, SSH, STP, SYSLOG, TACACS, TCP, TFTP, Telnet, UDP, VTP

Time: 01:11:23.02

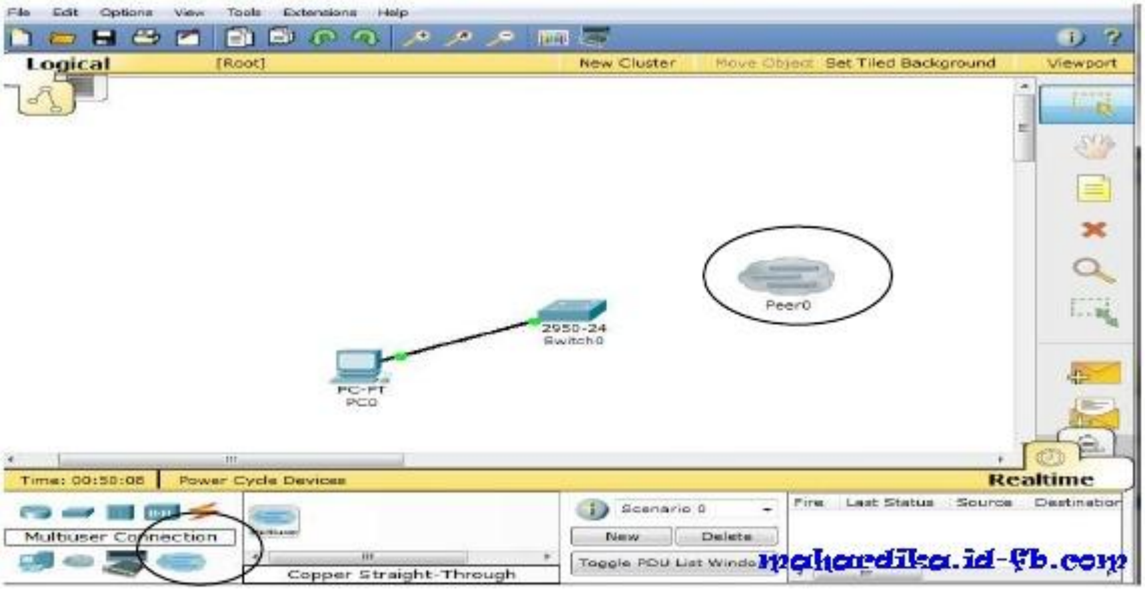
Scenario 0

Fire	Last Status	Source	Destination
●	Successful	PC0	PC1

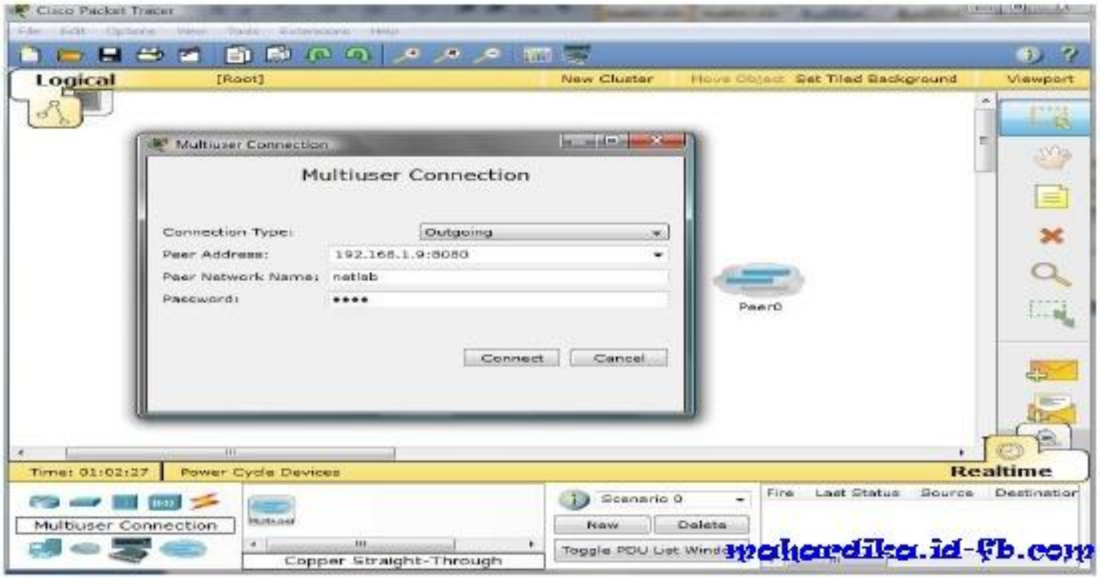
Membuat jaringan sederhana dengan menggunakan fitur multi user pada packet tracer :

Pada aplikasi packet tracer kita dimungkinkan untuk membuat simulasi jaringan gabungan antara simulasi jaringan menggunakan packet tracer di 2 atau lebih PC yang saling terhubung dalam satu network. Contoh penggunaan :

1.Buat jaringan sederhana lalu masukkan awan multiuser :



2.Klik pada awan multi user peer0, lalu set mode ke outgoing, dan ip address PC lain dimana terdapat simulasi jaringan yang akan dikoneksikan, set peer network name dan password
3.Tekan tombol connect da tunggu konfirmasi koneksi (mode incoming) di PC yang dituju muncul. Setelah terkoneksi, kita langsung dapat menjalankan 2 simulasi di PC yang berbeda.



Multiuser Connection

Connection Type: Outgoing
Peer Address: 192.168.1.9:8080
Peer Network Name: netlab
Password: ****

Network Analysis Tool

1.Network Analysis Tool

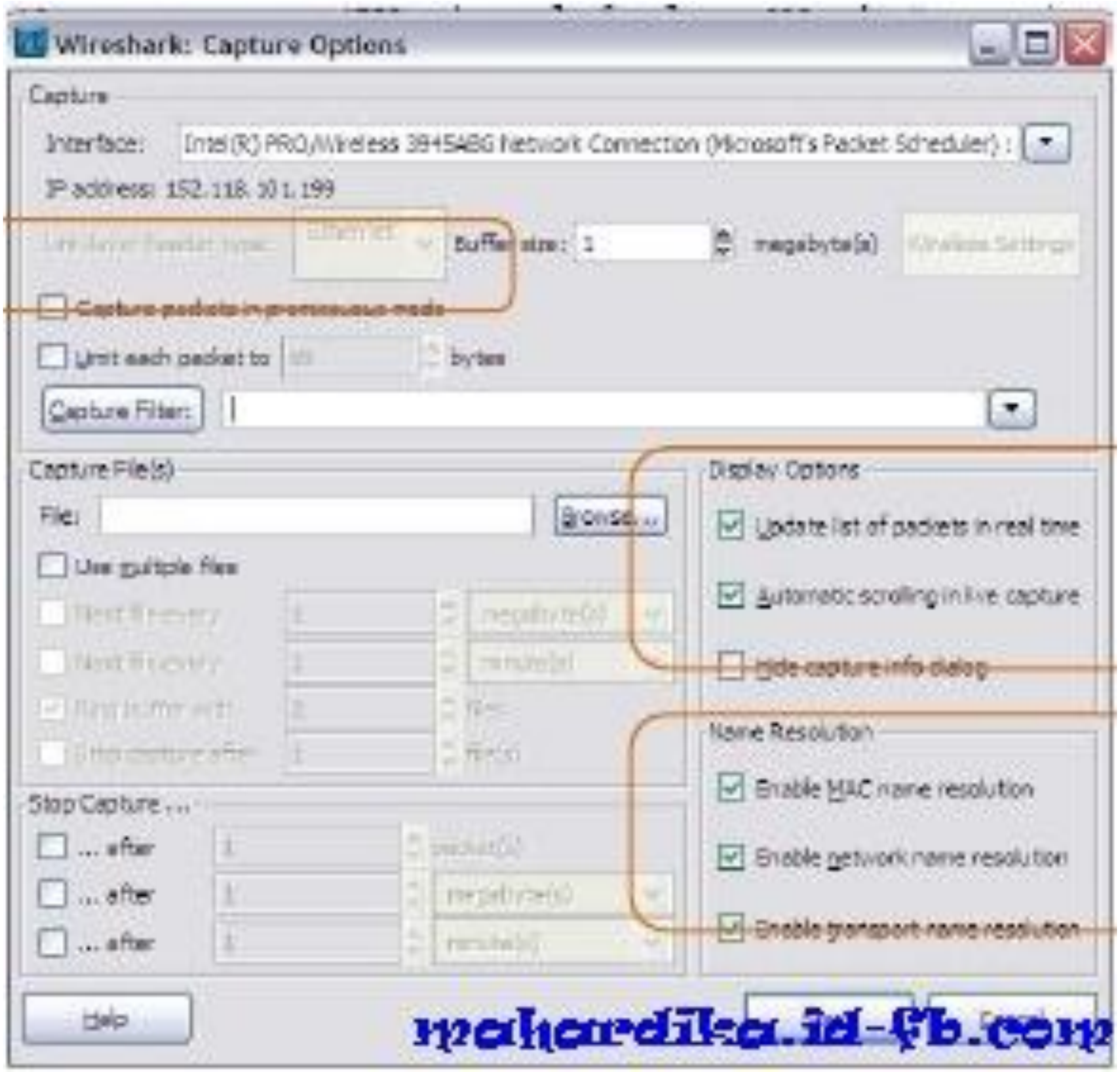
Wireshark merupakan salah satu network analysis tool, atau disebut juga dengan protocol analysis tool atau packet sniffer. Wireshark dapat digunakan untuk troubleshooting jaringan, analisis, pengembangan software dan protocol,serta untuk keperluan edukasi. Wireshark merupakan software gratis, sebelumnya,Wireshark dikenal dengan nama Ethereal.Packet sniffer sendiri diartikan sebagai sebuah program atau tool yang memiliki kemampuan untuk mencegat dan melakukan pencatatan terhadap traffic data dalam
jaringan. Selama terjadi aliran data dalam, packet sniffer dapat menangkap protocol data unit (PDU),melakukan dekoding serta melakukan analisis terhadap isi paket berdasarkan spesifikasi RFC atau spesifikasi-spesifikasi yang lain.Wireshark sebagai salah satu packet sniffer diprogram sedemikian rupa untuk mengenali berbagai macam protokol jaringan. Wireshark mampu menampilkan hasil enkapsulasi dan field yang ada dalam PDU.

Prosedur

Pada bagian ini akan diberikan bagaimana menggunakan Wireshark serta contoh melakukan capture PDU.

1)Jalankan Wireshark

2)Untuk melakukan capture dengan memilih pilihan yang tersedia, pilih menu
Capture > Options... akan tampil jendela semacam ini:



Wireshark: Capture Options

Capture

Interface: Intel(R) PRO/Wireless 3945ABG Network Connection (Microsoft's Packet Scheduler) :

IP address: 152.118.101.199

Buffer size: 1 megabyte(s)

□ Capture packets in promiscuous mode

□ Limit each packet to bytes

Capture File(s)

File:

□ Use multiple files

Stop Capture ...

□ ... after 1

□ ... after 1

□ ... after 1

Display Options

☑ Update list of packets in real time

☑ Automatic scrolling in live capture

□ Hide capture info dialog

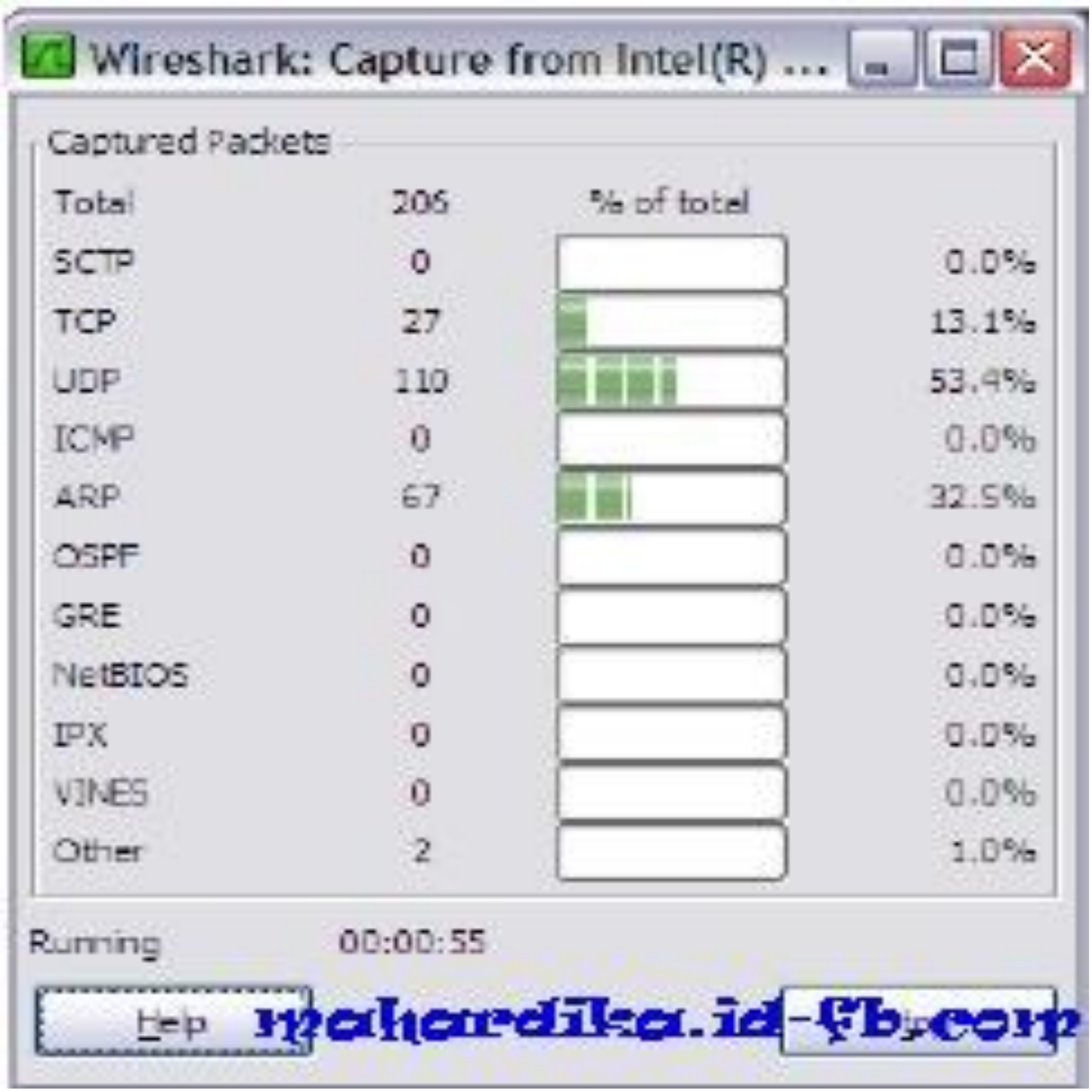
Name Resolution

☑ Enable MAC name resolution

☑ Enable network name resolution

☑ Enable transport name resolution

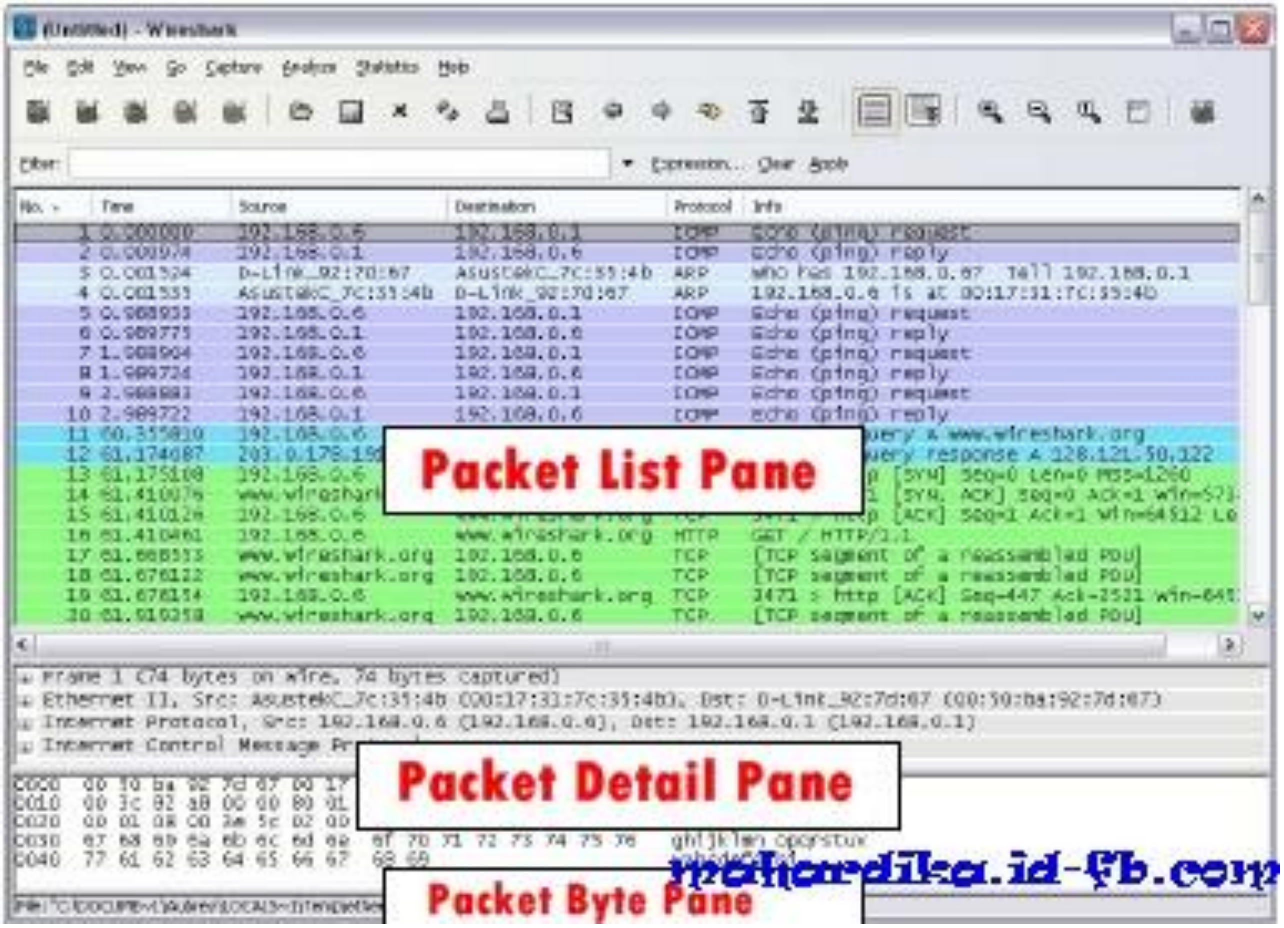
3.Pada jendela Capture Option, pilihlah interface Ethernet yang akan di-capture. Terlihat pada screenshot di atas terdapat 3 buah highlight. Highlight paling atas menunjukkan pilihan untuk melakukan capture pada Promiscuous Mode. Jika pilihan ini diaktifkan, maka Wireshark akan melakukan capture terhadap paket-paket yang ditujukan untuk komputer ini dan paket-paket yang terdeteksi oleh NIC dari komputer-komputer dalam satu segmen jaringan.Highlight kedua menunjukkan pilihan-pilihan untuk mengatur tampilan atau informasi yang akan ditampilkan oleh Wireshark. Jika pilihan hide capture dialog info dinonaktifkan, ketika kita memulai capture, Wireshark akan menampilkan jendela tambahan yang memberikan statistik persentase protokol yang ter-capture sebagai berikut:



Total	206	% of total	
SCTP	0		0.0%
TCP	27		13.1%
UDP	110		53.4%
ICMP	0		0.0%
ARP	67		32.5%
OSPF	0		0.0%
GRE	0		0.0%
NetBIOS	0		0.0%
IPX	0		0.0%
VINES	0		0.0%
Other	2		1.0%

Running 00:00:55

Highlight ketiga memberikan pilihan bahwa Wireshark akan menerjemahakan alamat jaringan dalam PDU menjadi nama.Mengaktifkan pilihan ini akan menambah PDU ekstra ke dalam data yang ter-capture.Jendela Wireshark terdiri atas tiga bagian, seperti ditunjukkan pada screenshot berikut:



```
No. -  Time       Source                Destination           Protocol  Info
    1 0.000000   192.168.0.6           192.168.0.1           ICMP      Echo (ping) request
    2 0.000974   192.168.0.1           192.168.0.6           ICMP      Echo (ping) reply
    3 0.001524   D-Link_92:7d:67       AsustekC_7c:35:4b     ARP       Who has 192.168.0.6?  Tell 192.168.0.1
    4 0.001535   AsustekC_7c:35:4b     D-Link_92:7d:67       ARP       192.168.0.6 is at 00:17:31:7c:35:4b
    5 0.988933   192.168.0.6           192.168.0.1           ICMP      Echo (ping) request
    6 0.989775   192.168.0.1           192.168.0.6           ICMP      Echo (ping) reply
    7 1.988904   192.168.0.6           192.168.0.1           ICMP      Echo (ping) request
    8 1.989724   192.168.0.1           192.168.0.6           ICMP      Echo (ping) reply
    9 2.988883   192.168.0.6           192.168.0.1           ICMP      Echo (ping) request
   10 2.989722   192.168.0.1           192.168.0.6           ICMP      Echo (ping) reply
   11 60.355810  192.168.0.6                                           uery A www.wireshark.org
   12 61.174087  203.0.178.19                                          uery response A 128.121.50.122
   13 61.175108  192.168.0.6                                           p [SYN] Seq=0 Len=0 MSS=1260
   14 61.410076  www.wireshark                                         1 [SYN, ACK] Seq=0 Ack=1 Win=573
   15 61.410128  192.168.0.6                                           p [ACK] Seq=1 Ack=1 Win=64512 Le
   16 61.410461  192.168.0.6           www.wireshark.org     HTTP      GET / HTTP/1.1
   17 61.668533  www.wireshark.org     192.168.0.6           TCP       [TCP segment of a reassembled PDU]
   18 61.676122  www.wireshark.org     192.168.0.6           TCP       [TCP segment of a reassembled PDU]
   19 61.676154  192.168.0.6           www.wireshark.org     TCP       3471 > http [ACK] Seq=447 Ack=2521 Win=645
   20 61.910258  www.wireshark.org     192.168.0.6           TCP       [TCP segment of a reassembled PDU]
```

```
+ Frame 1 (74 bytes on wire, 74 bytes captured)
+ Ethernet II, Src: AsustekC_7c:35:4b (00:17:31:7c:35:4b), Dst: D-Link_92:7d:67 (00:50:ba:92:7d:67)
+ Internet Protocol, Src: 192.168.0.6 (192.168.0.6), Dst: 192.168.0.1 (192.168.0.1)
+ Internet Control Message Pr
```

```
0000  00 50 ba 92 7d 67 00 17
0010  00 3c 82 a8 00 00 80 01
0020  00 01 08 00 3e 5c 02 00
0030  67 68 69 6a 6b 6c 6d 6e   6f 70 71 72 73 74 75 76   ghijklmn opqrstuv
0040  77 61 62 63 64 65 66 67   68 69                     wabcdefghi
```

Packet List Pane menampilkan ringkasan dari paket-paket yang tertangkap oleh Wireshark.Memilih salah satu paket yang tampil pada bagian ini akan memperlihatkan detail dari paket tersebut pada dua panel di bawahnya.Packet Detail Pane menampilkan detail dari paket yang dipiliha pada Packet List Pane.Packet Byte Pane menunjukkan isi data dari sebuah paket dalam heksadesimal serta menunjukkan detail dari field yang dipilih pada Packet Detail Pane.Untuk memulai proses capture, klik pada tombol Start.

4)Buka command prompt dengan cara klik Start > Run... > ketikkan cmd >
klik OK. Lakukan ping ke komputer sebelah anda dengan mengetikkan perintah ping IPkomputerDiSebelahAnda.

5)Aktivitas ping tersebut akan terekam oleh Wireshark, simpan hasil capture dengan memilih menu File > Save As... pada Wireshark.
6)Berdasarkan hasil capture Wireshark tersebut, isikan informasi yang diminta pada borang yang disediakan.