

Nama : Asyrof Hafizh Maulana

---

### SECURE & UNSECURE PROTOCOL

1. Buktikan dengan cara melakukan network interception/penyadapan menggunakan aplikasi Wireshark bahwa protokol protokol dibawah ini disebut Aman atau Tidak Aman. Jelaskan dan tunjukkan masing masing screenshoot yang menunjukkan Aman atau kurang Amannya Protokol tersebut. Sebutkan juga port TCP/UDP default masing masing protocol tersebut jika ada.

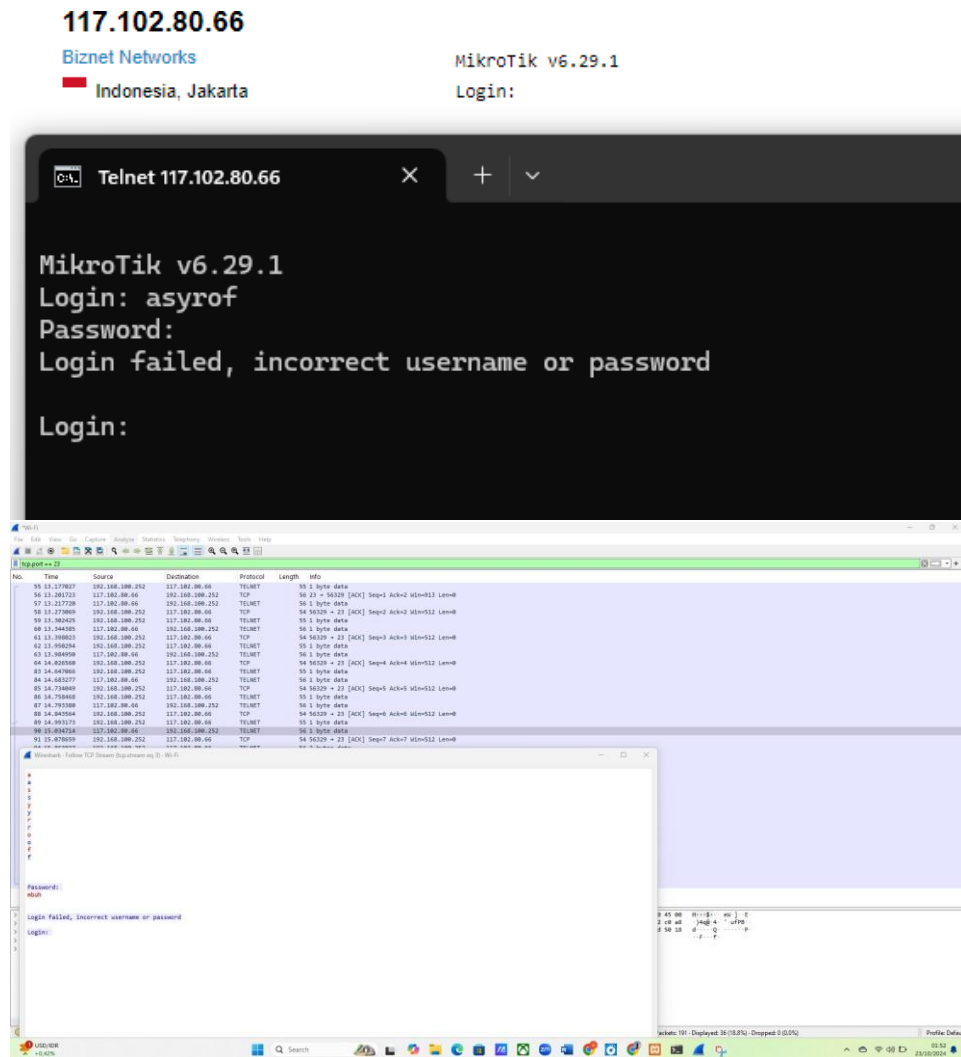
- a) Telnet vs SSH
- b) POP3 vs POP3s
- c) IMAP vs IMAPs
- d) HTTP vs HTTPS
- e) SMTP vs SMTPS
- f) FTP vs FTPS/SFTP
- g) LDAP vs LDAPs
- h) MYSQL
- i) POSTGRESQL
- j) DNS vs DNSSEC

Anda dapat terlebih dahulu menginstall service services tersebut, atau memanfaatkan services services yang sudah ada, atau anda temukan diinternet kemudian melakukan network interception/penyadapan komunikasi salah satu client ke services tersebut.

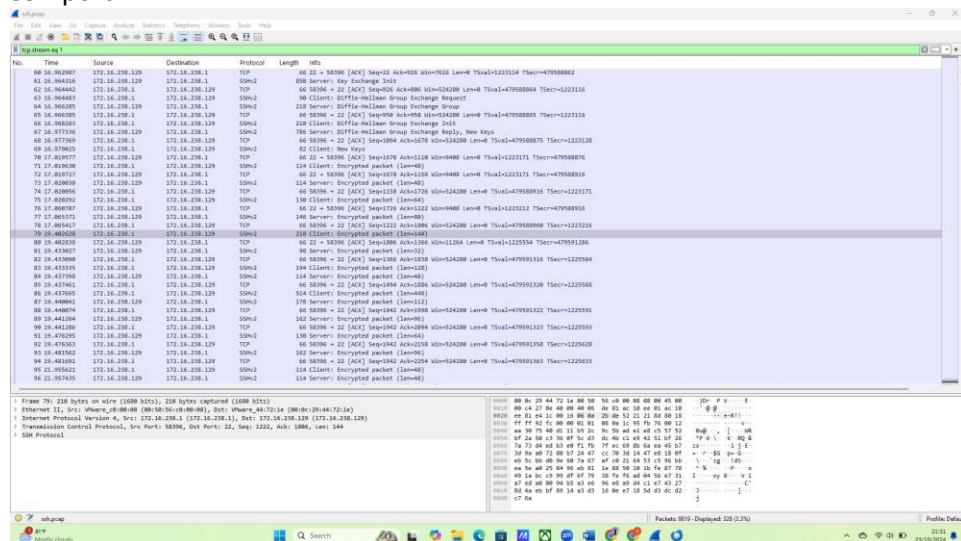
Jawab :

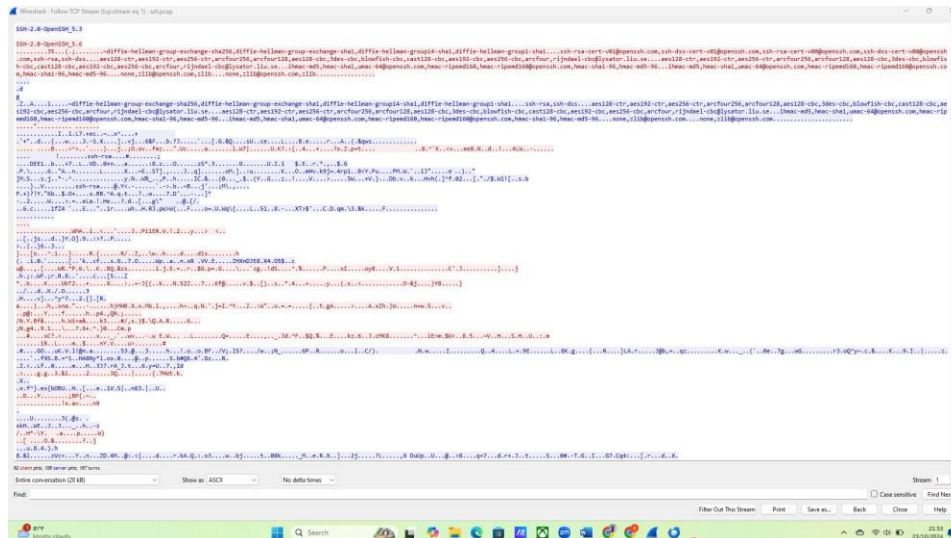
## a) Telnet vs SSH

Telnet port 23 :



SSH port 22 :



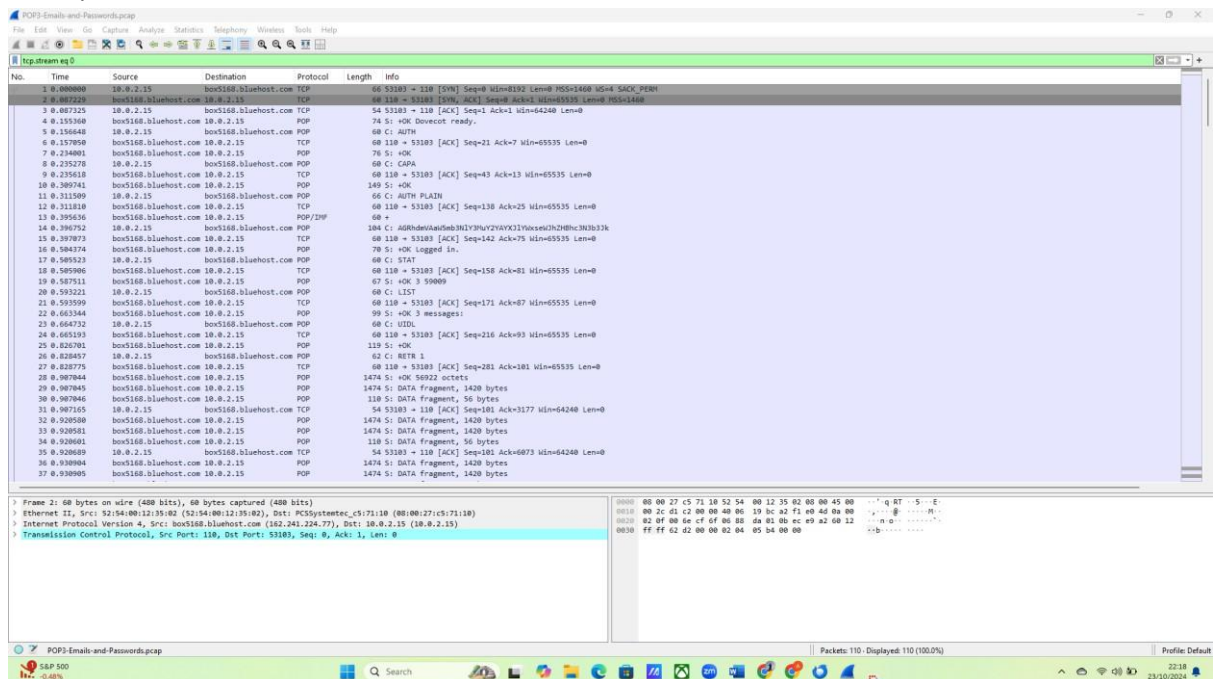


Penjelasan :

SSH jauh lebih aman dibandingkan Telnet dan merupakan pilihan yang direkomendasikan untuk mengakses sistem dan perangkat secara remote. Sebaliknya, Telnet sebaiknya dihindari untuk penggunaan yang sensitif karena kurangnya keamanan.

## b) POP3 vs POP3s

POP3 port 110 :



Penjelasan :

POP3S adalah versi aman dari POP3 yang mengenkripsi komunikasi antara klien dan server. Untuk pengguna yang mengutamakan keamanan, menggunakan POP3S sangat dianjurkan dibandingkan dengan POP3.

IMAP port 143 :

[illegible]

Penjelasan :

IMAPs adalah versi aman dari IMAP yang mengenkripsi komunikasi antara klien dan server.

Untuk pengguna yang mengutamakan keamanan saat mengakses email, menggunakan

IMAPs sangat dianjurkan dibandingkan dengan IMAP.

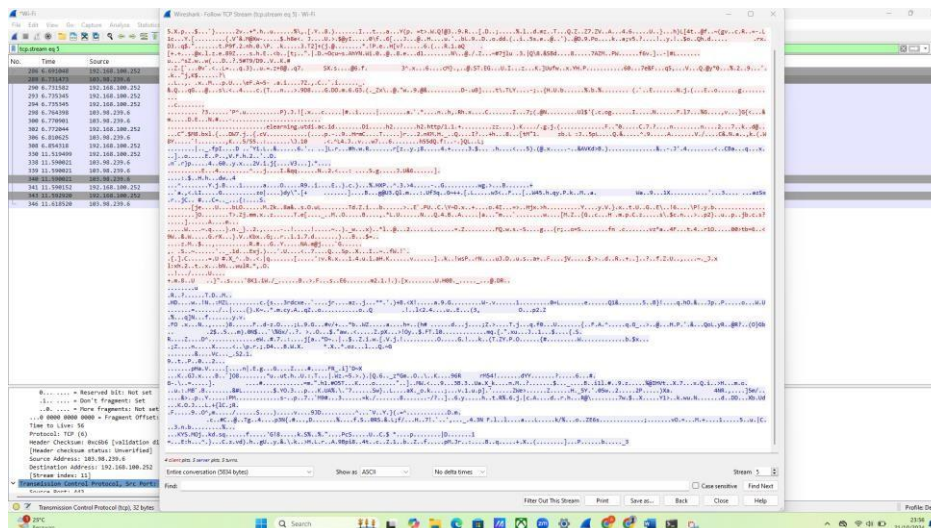
## d) HTTP vs HTTPS

HTTP port 80 :

The screenshot displays a web browser window at the top showing the 'MONEY IT' login page. The page has a blue background with a circuit-like pattern. It contains fields for 'USERNAME' and 'PASSWORD', a red 'Login' button, and a link for 'Username and Password Login IT'. Below the browser, the Wireshark network protocol analyzer is open, showing a list of captured packets. Packet 101 is selected, showing its details in the 'Packet Details' pane. The 'Hypertext Transfer Protocol' section is expanded, revealing the full HTTP request. The request is a GET to 'http://monevit.diskominfotik.riau.go.id/' with various headers including 'Host', 'User-Agent', 'Accept', 'Referer', 'Accept-Encoding', 'Accept-Language', and 'Cookie'. The 'Follow HTTP Stream' pane at the bottom shows the raw HTTP data, including the status line '200 OK' and the HTML body content, which appears to be a redirecting page.







Penjelasan :

HTTPS adalah versi aman dari HTTP yang menggunakan enkripsi untuk melindungi data yang ditransfer antara klien dan server. Untuk situs web yang mengelola informasi sensitif, menggunakan HTTPS sangat dianjurkan untuk menjaga keamanan data pengguna.

## e) SMTP vs SMTPS

SMTP port 25 :

```

C:\WINDOWS\system32\cmd. X
220 mx.google.com ESMTP d9443c01a7336-20e7f0d2eb9s174998575ad.248 - gsmt
helloworld
502-5.5.1 Unrecognized command. For more information, go to
502 5.5.1 https://support.google.com/a/answer/3221692 d9443c01a7336-20e7f0d2eb9s174998575ad.248 - gsmt
cobasmt
502-5.5.1 Unrecognized command. For more information, go to
502 5.5.1 https://support.google.com/a/answer/3221692 d9443c01a7336-20e7f0d2eb9s174998575ad.248 - gsmt
cobalagi
502-5.5.1 Unrecognized command. For more information, go to
502 5.5.1 https://support.google.com/a/answer/3221692 d9443c01a7336-20e7f0d2eb9s174998575ad.248 - gsmt
test
502-5.5.1 Unrecognized command. For more information, go to
502 5.5.1 https://support.google.com/a/answer/3221692 d9443c01a7336-20e7f0d2eb9s174998575ad.248 - gsmt
aa
502-5.5.1 Unrecognized command. For more information, go to
502 5.5.1 https://support.google.com/a/answer/3221692 d9443c01a7336-20e7f0d2eb9s174998575ad.248 - gsmt
b
502-5.5.1 Unrecognized command. For more information, go to
502 5.5.1 https://support.google.com/a/answer/3221692 d9443c01a7336-20e7f0d2eb9s174998575ad.248 - gsmt
c
502-5.5.1 Unrecognized command. For more information, go to
502 5.5.1 https://support.google.com/a/answer/3221692 d9443c01a7336-20e7f0d2eb9s174998575ad.248 - gsmt
helo
501-5.5.4 Empty HELO/EHLO argument not allowed, closing connection.
501 5.5.4 https://support.google.com/mail/?p=helo d9443c01a7336-20e7f0d2eb9s174998575ad.248 - gsmt

Connection to host lost.
C:\Users\Asus TUF Gaming F15>

```





FTP port 20 :



FTP (File Transfer Protocol) adalah protokol untuk transfer file yang tidak menyediakan enkripsi, sehingga rentan terhadap penyadapan dan serangan; ini membuatnya tidak cocok untuk data sensitif. FTPS (FTP Secure) meningkatkan keamanan FTP dengan menggunakan SSL/TLS untuk mengenkripsi data yang ditransfer, beroperasi dalam dua mode (Explicit dan Implicit) dan menggunakan port 21 dan 990 untuk koneksi aman. SFTP (SSH File Transfer Protocol), di sisi lain, menggunakan SSH untuk mengamankan koneksi dan mengenkripsi semua data, serta memungkinkan pengelolaan file yang lebih baik dengan otentikasi yang kuat melalui kunci publik dan privat, beroperasi pada port 22. Meskipun FTP dapat digunakan untuk transfer file non-sensitif, FTPS dan SFTP sangat dianjurkan untuk komunikasi yang memerlukan perlindungan data, dengan SFTP sering dianggap lebih kuat dalam hal keamanan dan fungsionalitas, membuatnya pilihan ideal untuk transfer file yang aman di lingkungan yang berisiko.

## g) LDAP vs LDAPS

LDAP port 389 :

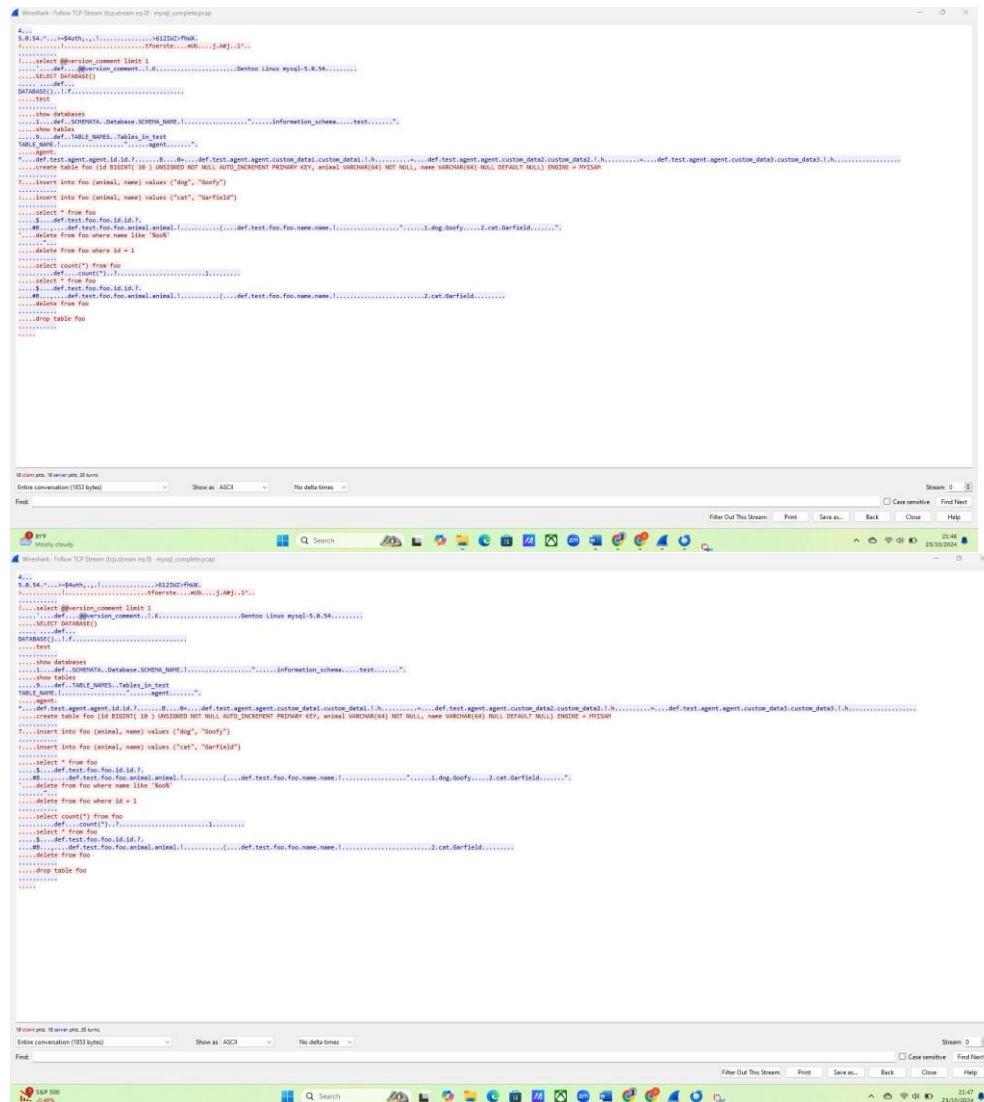
The image displays a Wireshark network traffic capture of an LDAP session on port 389. The top pane lists 36 packets, with the last packet (No. 36) selected. The middle pane shows the details of this packet, including Ethernet II (Type: IPv4), Internet Protocol Version 4 (Src: localhost:localdomain, Dst: localhost:localdomain), and Transmission Control Protocol (Src Port: 389, Dst Port: 389). The bottom pane shows the raw packet data in hexadecimal and ASCII. The packet is an LDAP message, specifically a search request, as indicated by the 'LDAP Search' entry in the details pane.

Penjelasan :

LDAP (Lightweight Directory Access Protocol) adalah protokol yang digunakan untuk mengakses dan mengelola informasi dalam direktori, seperti data pengguna dan grup, namun beroperasi tanpa enkripsi, sehingga membuatnya rentan terhadap penyadapan dan serangan yang dapat mengekspos informasi sensitif. Di sisi lain, LDAPS (LDAP Secure) meningkatkan keamanan dengan menggunakan SSL/TLS untuk mengenkripsi komunikasi antara klien dan server, yang melindungi data dan kredensial selama transfer. LDAP biasanya menggunakan port 389, sementara LDAPS menggunakan port 636 untuk komunikasi yang aman. Meskipun keduanya memiliki fungsi yang serupa, LDAPS sangat dianjurkan untuk aplikasi yang memerlukan perlindungan data tinggi, terutama dalam konteks akses informasi sensitif, karena menawarkan otentikasi yang lebih kuat dan perlindungan terhadap akses yang tidak sah. Dengan demikian, untuk organisasi yang berfokus pada keamanan, LDAPS adalah pilihan yang lebih baik daripada LDAP dalam pengelolaan dan akses informasi direktori.

## h) MYSQL

Mysql port 3306 :



```
4>
5.8.34>mysql -u root -p123456 -h 127.0.0.1
mysql: [Warning] Using a password on the command line interface can be insecure.
mysql>use agent;
mysql>create database agent;
mysql>show databases;
+-----+
| Database |
+-----+
| agent     |
+-----+
mysql>show tables;
+-----+
| Tables_in_agent |
+-----+
| agent            |
+-----+
mysql>create table agent (id int(11) unsigned not null auto_increment primary key, name varchar(64) not null, body varchar(256) not null default null) engine = InnoDB;
mysql>insert into agent (name, body) values ('dog', 'body');
mysql>insert into agent (name, body) values ('cat', 'body');
mysql>select * from agent;
+----+-----+-----+
| id  | name | body |
+----+-----+-----+
| 1   | dog  | body |
| 2   | cat  | body |
+----+-----+-----+
mysql>delete from agent where id = 1;
mysql>select count(*) from agent;
+-----+
| count(*) |
+-----+
| 1         |
+-----+
mysql>select * from agent;
+----+-----+-----+
| id  | name | body |
+----+-----+-----+
| 2   | cat  | body |
+----+-----+-----+
mysql>delete from agent where name like 'cat';
mysql>drop table agent;
mysql>
```

Penjelasan :

MySQL adalah sistem manajemen basis data relasional yang kuat dan fleksibel, ideal untuk berbagai aplikasi mulai dari pengembangan web hingga bisnis. Dengan fitur keamanan, kinerja tinggi, dan kemampuan untuk menangani data dalam jumlah besar, MySQL tetap menjadi salah satu pilihan utama untuk pengelolaan basis data di seluruh dunia. Keunggulan sumber terbuka dan dukungan komunitas yang luas membuat MySQL mudah diakses dan dikembangkan sesuai kebutuhan pengguna.

i) POSTGRESQL

Postgresql port 5432 :

File Edit View Go Capture Analyze Statistics Help

Log window (1)

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	10.0.0.1	10.0.0.2	TCP	70	53499 → 5432 [PSH] Seq=8 10405333 Len=8 Window=10800 Src=10.0.0.1 Dst=10.0.0.2 Seq=8 10405333 Len=8 Window=10800
2	0.000001	10.0.0.2	10.0.0.1	TCP	76	5432 → 53499 [PSH, ACK] Seq=8 10405333 Len=8 Window=10800 Src=10.0.0.2 Dst=10.0.0.1 Seq=8 10405333 Len=8 Window=10800
3	0.000002	10.0.0.1	10.0.0.2	TCP	66	53499 → 5432 [ACK] Seq=1 Ack=1 Win=12080 Len=8 TSize=787402152 TSecr=405053081
4	0.000003	10.0.0.1	10.0.0.2	PDQU	76	37
5	0.000002	10.0.0.1	10.0.0.2	TCP	66	5432 → 53499 [ACK] Seq=1 Ack=1 Win=12080 Len=8 TSize=405053086 TSecr=787402152
6	0.000012	10.0.0.1	10.0.0.2	TCP	66	53499 → 5432 [ACK] Seq=9 Ack=2 Win=12080 Len=8 TSize=787402156 TSecr=405053086
7	0.000010	10.0.0.1	10.0.0.2	PDQU	140	1
8	0.000011	10.0.0.1	10.0.0.2	TCP	76	48
9	0.000011	10.0.0.1	10.0.0.2	TCP	66	53499 → 5432 [ACK] Seq=3 Ack=13 Win=12080 Len=8 TSize=787402161 TSecr=405053081
10	0.000012	10.0.0.1	10.0.0.2	TCP	66	53499 → 5432 [PSH, ACK] Seq=3 Ack=13 Win=12080 Len=8 TSize=787402161 TSecr=405053081
11	0.000012	10.0.0.1	10.0.0.2	TCP	66	5432 → 53499 [PSH, ACK] Seq=4 Ack=13 Win=12080 Len=8 TSize=405053084 TSecr=787402161
12	0.000013	10.0.0.1	10.0.0.2	TCP	66	53499 → 5432 [ACK] Seq=4 Ack=13 Win=12080 Len=8 TSize=787402166 TSecr=405053084

Frame 4: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on 0

Ethernet II, Src: Realtek-80:00:00:00:00:00, Dst: Realtek-08:00:27:00:00:00

Internet Protocol Version 4, Src: 10.0.0.1, Dst: 10.0.0.2

Transmission Control Protocol, Src Port: 53499, Dst Port: 5432, Seq: 3, Ack: 1, Len: 8

PostgreSQL

Type: S5 request

Length: 8

Request code: S5Request (30877385)

PostgresBackup.pcap

Search

Packets: 10 (100.0%)

Profile Default

```

1 0.000000 10.0.0.1 → 10.0.0.2 [PSH] Seq=8 10405333 Len=8 Window=10800 Src=10.0.0.1 Dst=10.0.0.2 Seq=8 10405333 Len=8 Window=10800
2 0.000001 10.0.0.2 → 10.0.0.1 [PSH, ACK] Seq=8 10405333 Len=8 Window=10800 Src=10.0.0.2 Dst=10.0.0.1 Seq=8 10405333 Len=8 Window=10800
3 0.000002 10.0.0.1 → 10.0.0.2 [ACK] Seq=1 Ack=1 Win=12080 Len=8 TSize=787402152 TSecr=405053081
4 0.000003 10.0.0.1 → 10.0.0.2 [PDQU] 76
5 0.000002 10.0.0.1 → 10.0.0.2 [ACK] Seq=1 Ack=1 Win=12080 Len=8 TSize=405053086 TSecr=787402152
6 0.000012 10.0.0.1 → 10.0.0.2 [ACK] Seq=9 Ack=2 Win=12080 Len=8 TSize=787402156 TSecr=405053086
7 0.000010 10.0.0.1 → 10.0.0.2 [PDQU] 140
8 0.000011 10.0.0.1 → 10.0.0.2 [ACK] Seq=3 Ack=13 Win=12080 Len=8 TSize=787402161 TSecr=405053081
9 0.000011 10.0.0.1 → 10.0.0.2 [PSH, ACK] Seq=3 Ack=13 Win=12080 Len=8 TSize=787402161 TSecr=405053081
10 0.000012 10.0.0.1 → 10.0.0.2 [PSH, ACK] Seq=4 Ack=13 Win=12080 Len=8 TSize=405053084 TSecr=787402161
11 0.000013 10.0.0.1 → 10.0.0.2 [ACK] Seq=4 Ack=13 Win=12080 Len=8 TSize=787402166 TSecr=405053084

```

2 items plus 2 more plus 3 items

Enter conversation (86 bytes)

Show as: ASCII

No delta time

Stream 0

Find

```

1 0.000000 10.0.0.1 → 10.0.0.2 [PSH] Seq=8 10405333 Len=8 Window=10800 Src=10.0.0.1 Dst=10.0.0.2 Seq=8 10405333 Len=8 Window=10800
2 0.000001 10.0.0.2 → 10.0.0.1 [PSH, ACK] Seq=8 10405333 Len=8 Window=10800 Src=10.0.0.2 Dst=10.0.0.1 Seq=8 10405333 Len=8 Window=10800
3 0.000002 10.0.0.1 → 10.0.0.2 [ACK] Seq=1 Ack=1 Win=12080 Len=8 TSize=787402152 TSecr=405053081
4 0.000003 10.0.0.1 → 10.0.0.2 [PDQU] 76
5 0.000002 10.0.0.1 → 10.0.0.2 [ACK] Seq=1 Ack=1 Win=12080 Len=8 TSize=405053086 TSecr=787402152
6 0.000012 10.0.0.1 → 10.0.0.2 [ACK] Seq=9 Ack=2 Win=12080 Len=8 TSize=787402156 TSecr=405053086
7 0.000010 10.0.0.1 → 10.0.0.2 [PDQU] 140
8 0.000011 10.0.0.1 → 10.0.0.2 [ACK] Seq=3 Ack=13 Win=12080 Len=8 TSize=787402161 TSecr=405053081
9 0.000011 10.0.0.1 → 10.0.0.2 [PSH, ACK] Seq=3 Ack=13 Win=12080 Len=8 TSize=787402161 TSecr=405053081
10 0.000012 10.0.0.1 → 10.0.0.2 [PSH, ACK] Seq=4 Ack=13 Win=12080 Len=8 TSize=405053084 TSecr=787402161
11 0.000013 10.0.0.1 → 10.0.0.2 [ACK] Seq=4 Ack=13 Win=12080 Len=8 TSize=787402166 TSecr=405053084

```

Penjelasan :

PostgreSQL adalah sistem manajemen basis data relasional yang kuat dan fleksibel, ideal untuk pengelolaan data yang kompleks dan canggih. Dengan dukungan untuk berbagai tipe data, kemampuan transaksi ACID, dan fitur ekstensibilitas yang kaya, PostgreSQL menjadi pilihan utama bagi pengembang yang mencari solusi basis data yang handal. Keunggulan open-source dan kemampuan untuk menyesuaikan fungsionalitas menjadikan PostgreSQL sebagai alat yang sangat bermanfaat untuk aplikasi yang memerlukan skalabilitas, keamanan, dan kinerja tinggi.

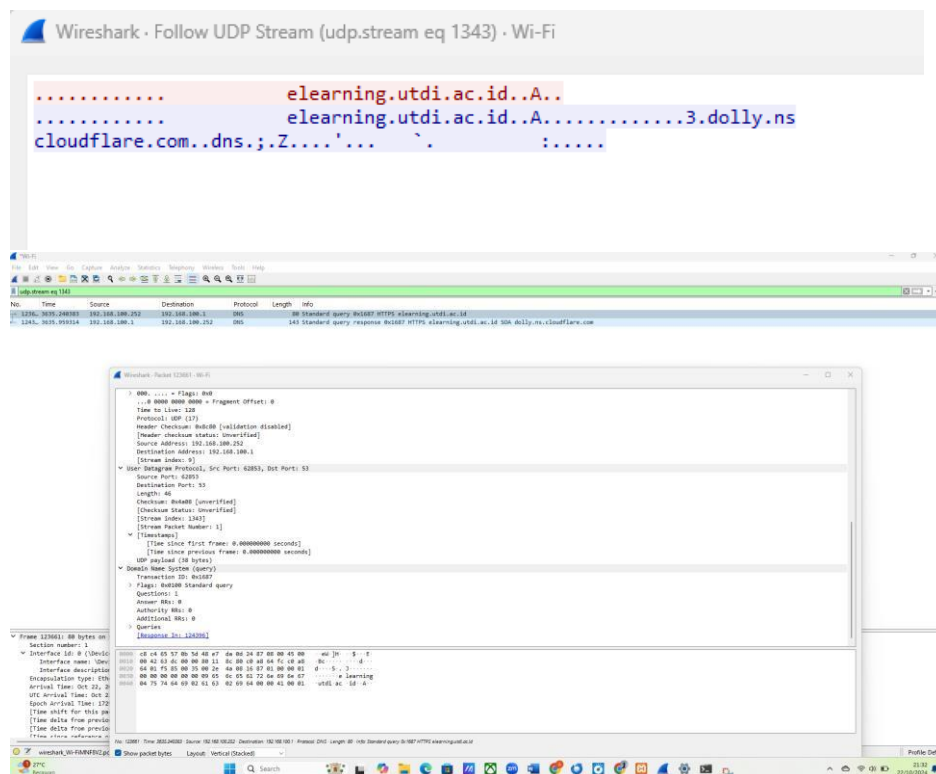
## j) DNS vs DNSSEC

DNS port 53 TCP :

```
C:\Users\Asus TUF Gaming F15>nslookup elearning.utdi.ac.id
Server:    UnKnown
Address:    192.168.100.1

Non-authoritative answer:
Name:      elearning.utdi.ac.id
Address:    103.98.239.6

C:\Users\Asus TUF Gaming F15>
```





[illegible]

Secara keseluruhan, DNS adalah komponen fundamental dari infrastruktur internet yang memungkinkan penerjemahan nama domain menjadi alamat IP, tetapi tidak menyediakan keamanan yang cukup. DNSSEC, di sisi lain, adalah ekstensi keamanan yang menambahkan lapisan perlindungan dengan menandatangani data DNS secara kriptografis, memastikan keaslian dan integritas informasi yang diterima. Dengan semakin meningkatnya ancaman terhadap sistem DNS, penerapan DNSSEC menjadi semakin penting untuk melindungi pengguna dan data mereka dari serangan berbahaya.