

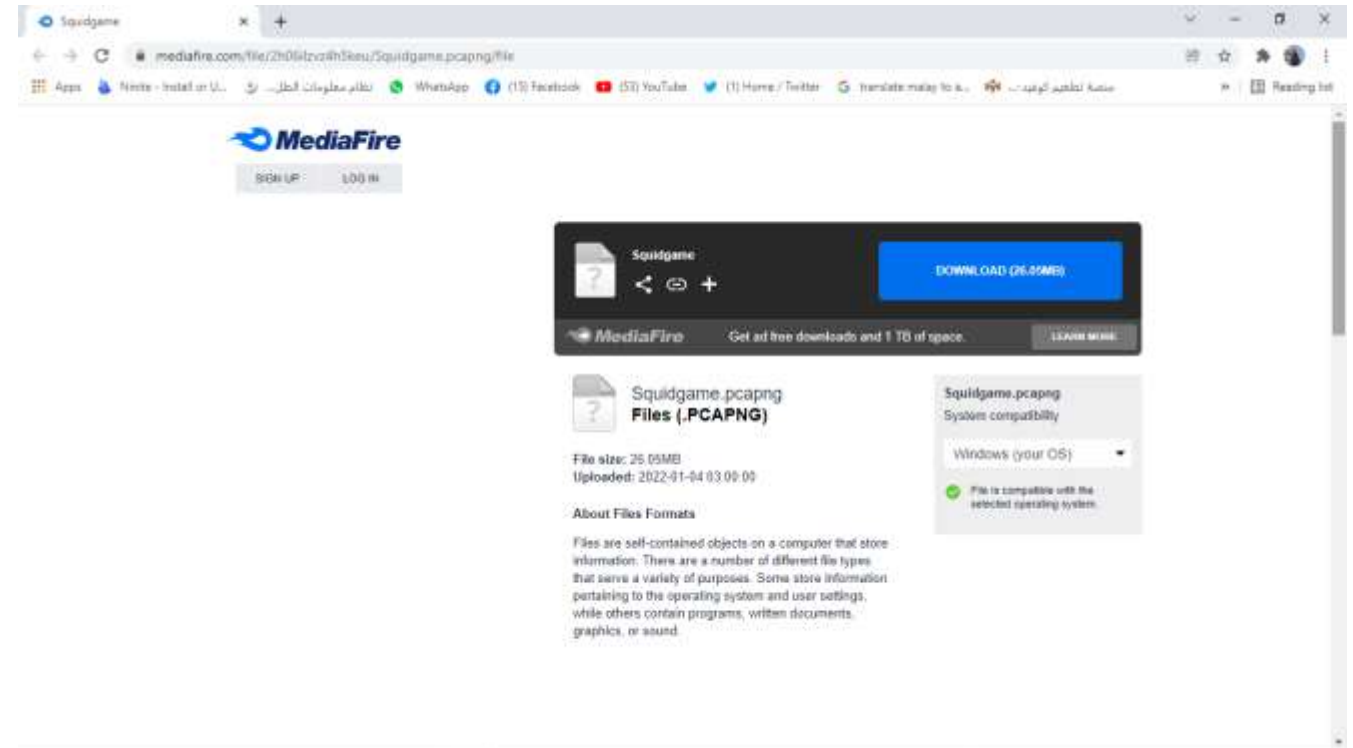


Proof of Concept CTF Squidgame

BY GHAZYURI

DOWNLOAD FILE

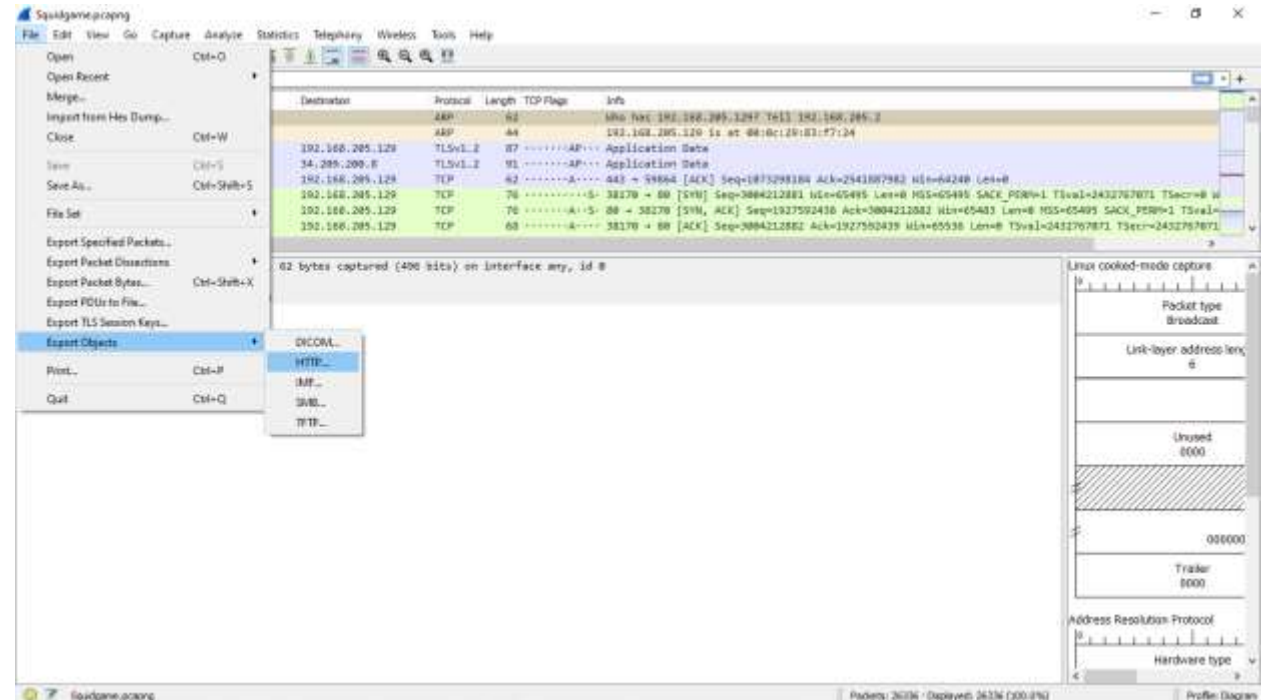
File tersebut adalah berbentuk pcapng. Nampak sahaja bentuk file seperti itu, maka kita dah tahu bahawa game ini memerlukan kita menganalisis paket menggunakan wireshark.



ANALISIS PAKET

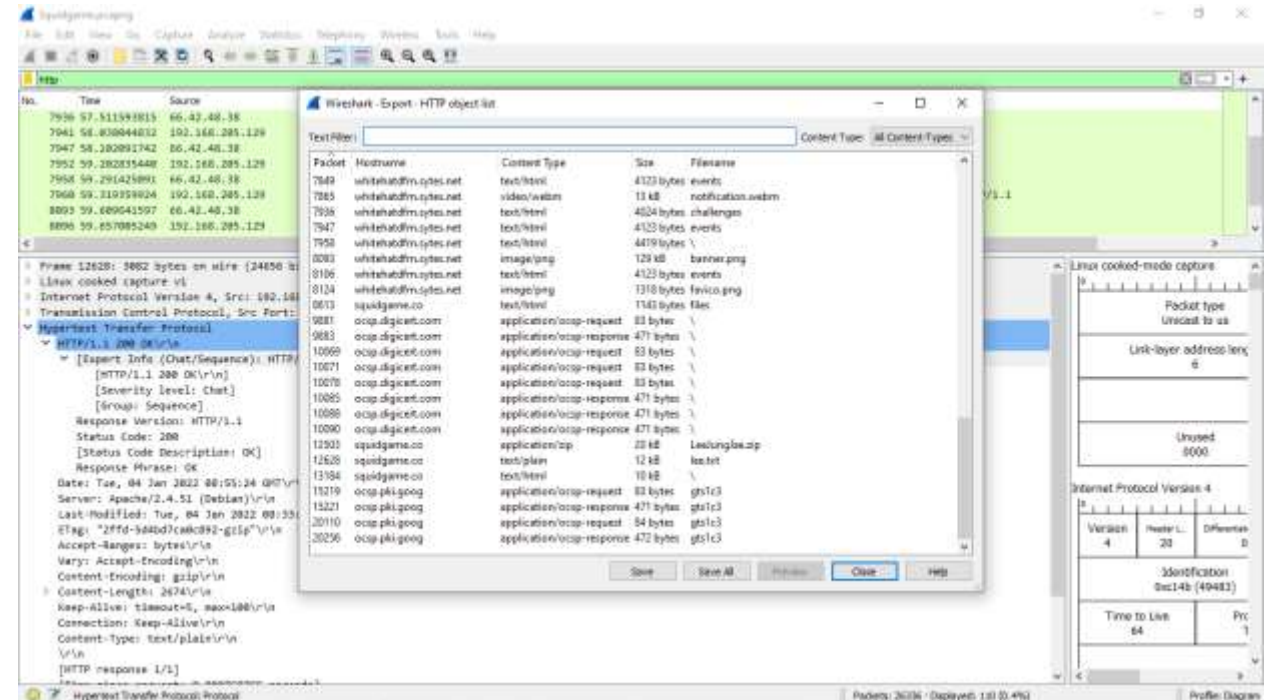
Buka file yang telah kita download. Kemudian kita masukkan filter http untuk kita dapat cari klu lebih detail. Selepas itu, follow the flow seperti ini :

File > export objects > http



DOWNLOAD ZIP FILE

Selepas meneliti, kita akan menemui 2 file yang akan membawa kita kepada klu seterusnya . Satu ialah file berbentuk zip dan yang kedua adalah file berbentuk txt. Save sahaja file itu ke dalam desktop.



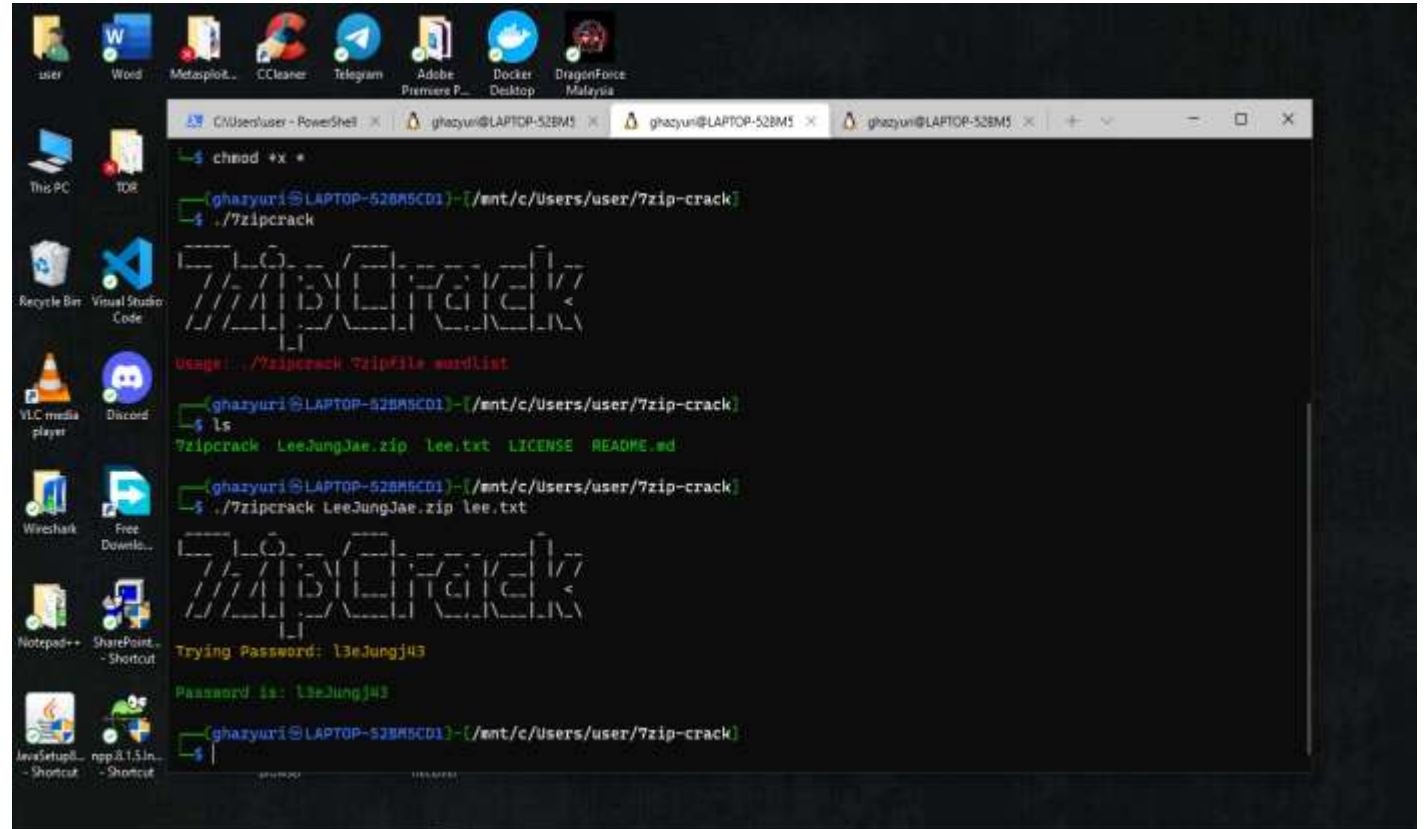
BRUTEFORCE ZIP FILE

Peringkat seterusnya, kita perlu bruteforce zip file itu kerana ianya mempunyai password.

Saya menggunakan tools 7zip-crack.

```
Command : ./7zipcrack LeeJung
Jae.zip lee.txt
```

Wordlist yang diperlukan adalah file txt yang kita dapat daripada wireshark tadi.

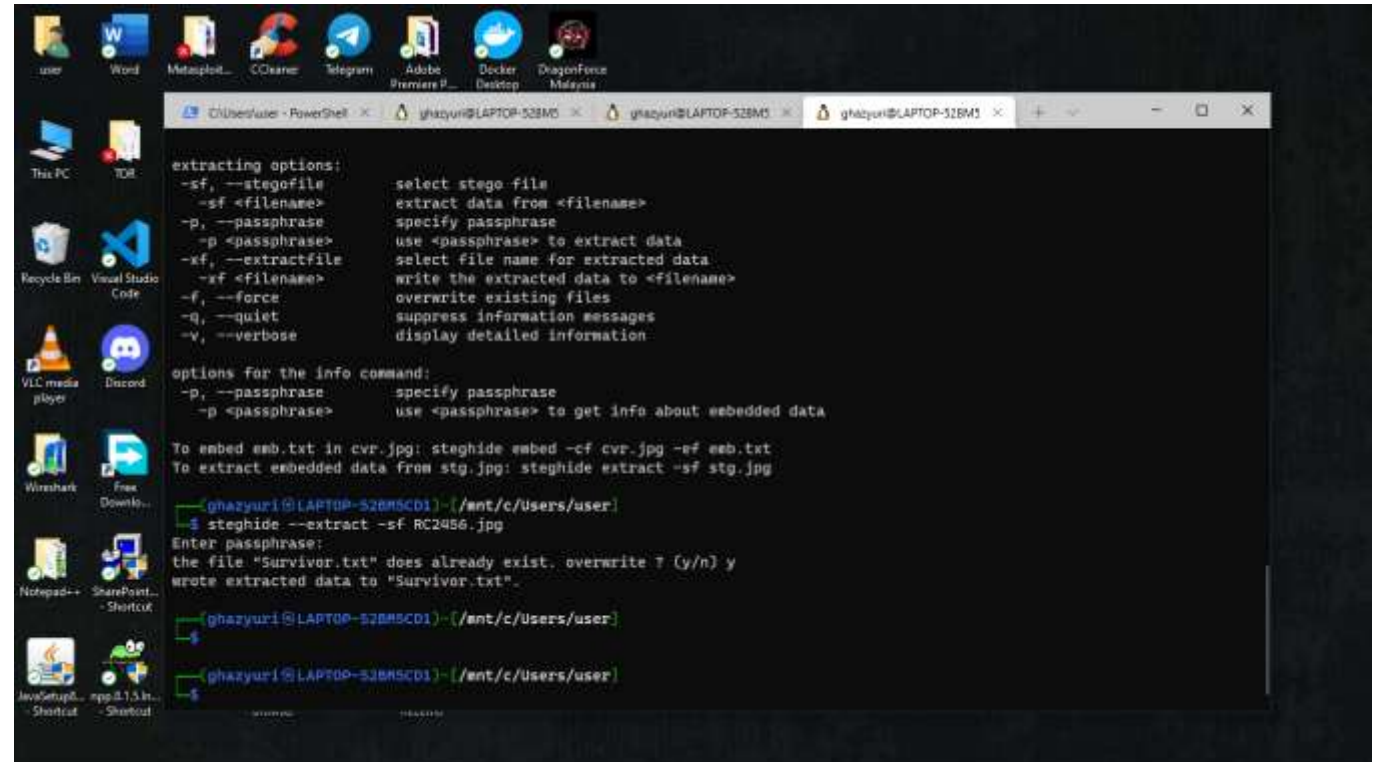


EXTRACT ZIP FILE DAN EXTRACT JPG

Selepas mendapatkan password, kita extract zip file tersebut dan menemui klu seterusnya iaitu sekeping gambar jpg. Di peringkat ini, saya menggunakan steghide untuk extract hidden text daripada gambar itu.

Command : steghide -extract -sf RC2456.jpg

Steghide akan simpan Hidden text itu di dalam file txt.



```
extracting options:
-sf, --stego file      select stego file
-sf <filename>        extract data from <filename>
-p, --passphrase       specify passphrase
-p <passphrase>       use <passphrase> to extract data
-xf, --extract file    select file name for extracted data
-xf <filename>        write the extracted data to <filename>
-f, --force            overwrite existing files
-q, --quiet            suppress information messages
-v, --verbose          display detailed information

options for the info command:
-p, --passphrase       specify passphrase
-p <passphrase>       use <passphrase> to get info about webbed data

To embed emb.txt in cvr.jpg: steghide embed -cf cvr.jpg -ef emb.txt
To extract embedded data from stg.jpg: steghide extract -sf stg.jpg

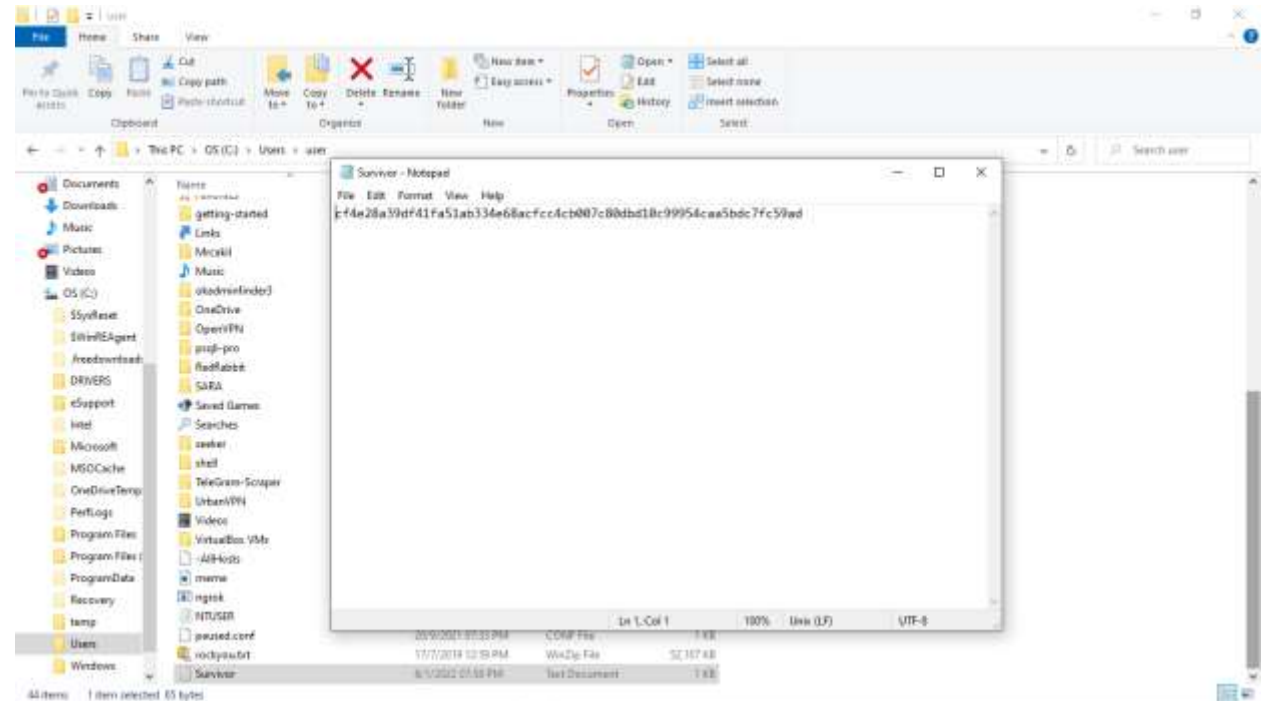
[ghazyuri@LAPTOP-S2BMSCD1] ~/c/Users/user
$ steghide --extract -sf RC2456.jpg
Enter passphrase:
the file "Survivor.txt" does already exist. overwrite ? (y/n) y
wrote extracted data to "Survivor.txt".

[ghazyuri@LAPTOP-S2BMSCD1] ~/c/Users/user
$
```

OPEN FILE TXT DARIPADA STEGHIDE

Kemudian saya open file txt yang mengandung klu seterusnya. Di dalam file txt itu, saya menemukan hash.

Hash ini kita perlu decrypt untuk dapatkan mesej sebenar.



DECRYPT USING CYBERCHEF

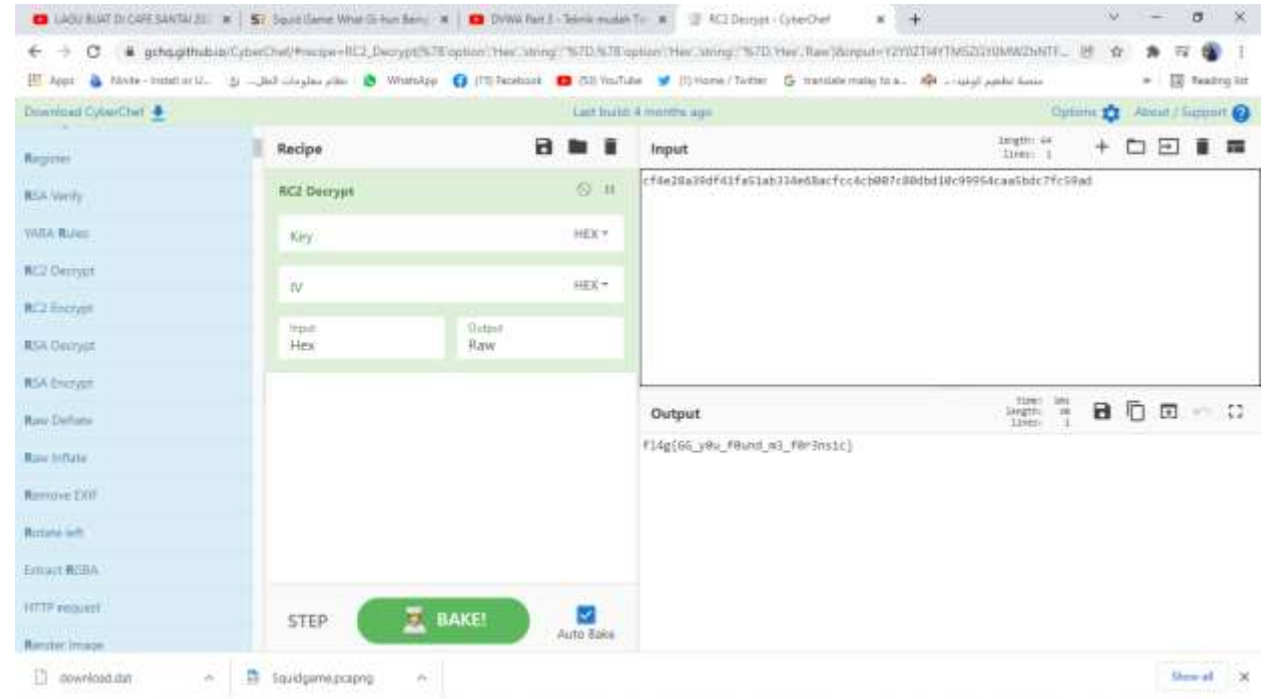
Saya menggunakan cyberchef untuk decrypt hash itu.

Pautan cyberchef:

<https://gchq.github.io/CyberChef/>

Saya menggunakan RC2 Decrypt memandangkan ada klu pada gambar iaitu **RC2**456.jpg

Akhirnya, saya menemukan flag.



SEKIAN SAHAJA POC SAYA UNTUK CTF
KALI INI.

SEMOGA BERMANFAAT.

∴ FROM GHAZYURI ∴