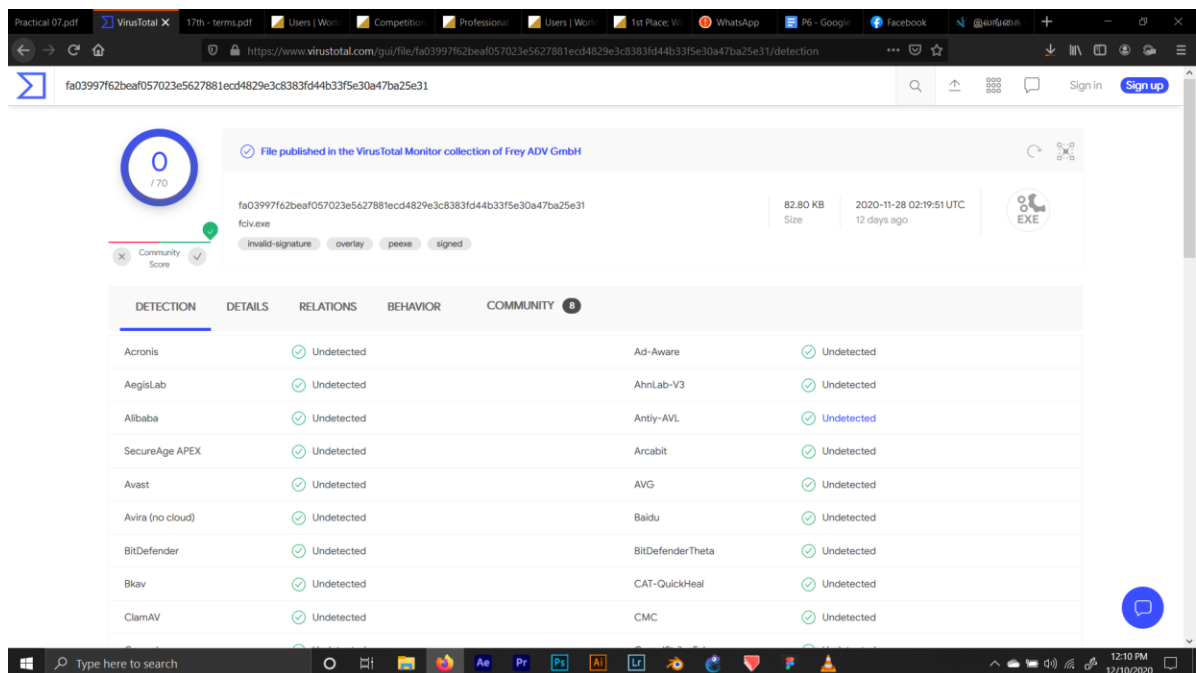


# IS2109 Information Systems Security- IS 2109

## Practical 7

### Secure Web Browsing

1.



Virus Total will check for the virus in the uploaded file and detect the virus since it's showing undetected. We can possibly consider that there is no virus in the file uploaded.

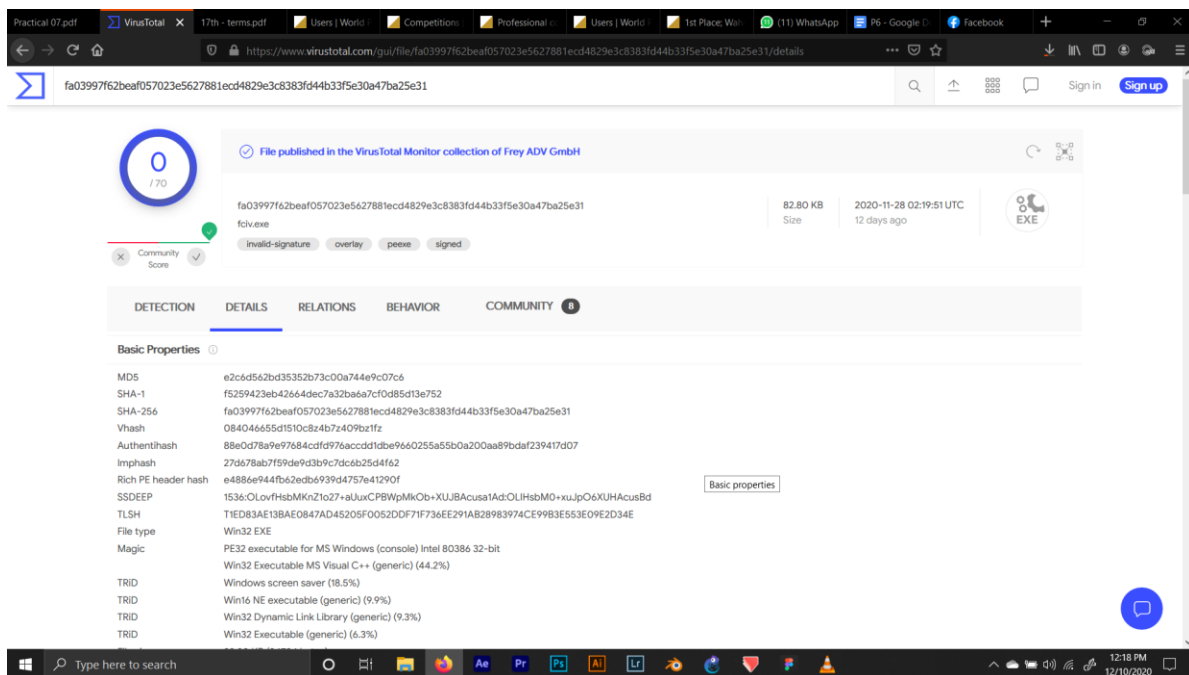
To check the integrity of the file we have referred to the details section. To check integrity, we need to hash the file. Initially send has to hash the file and receiver has to hash it using the same hashing algorithm. If the hash value obtained by both sender and receiver is the same by using the same algorithm we can deduct that the file's integrity is preserved.

Virus Total is using different hashing algorithms like MD5, SHA-1, SHA-256 etc here in the practical sheet we have given with MD5 values.

MD5 in practical sheet: **e2c6d562bd35352b73c00a744e9c07c6**

MD5 in Virus Total: **e2c6d562bd35352b73c00a744e9c07c6**

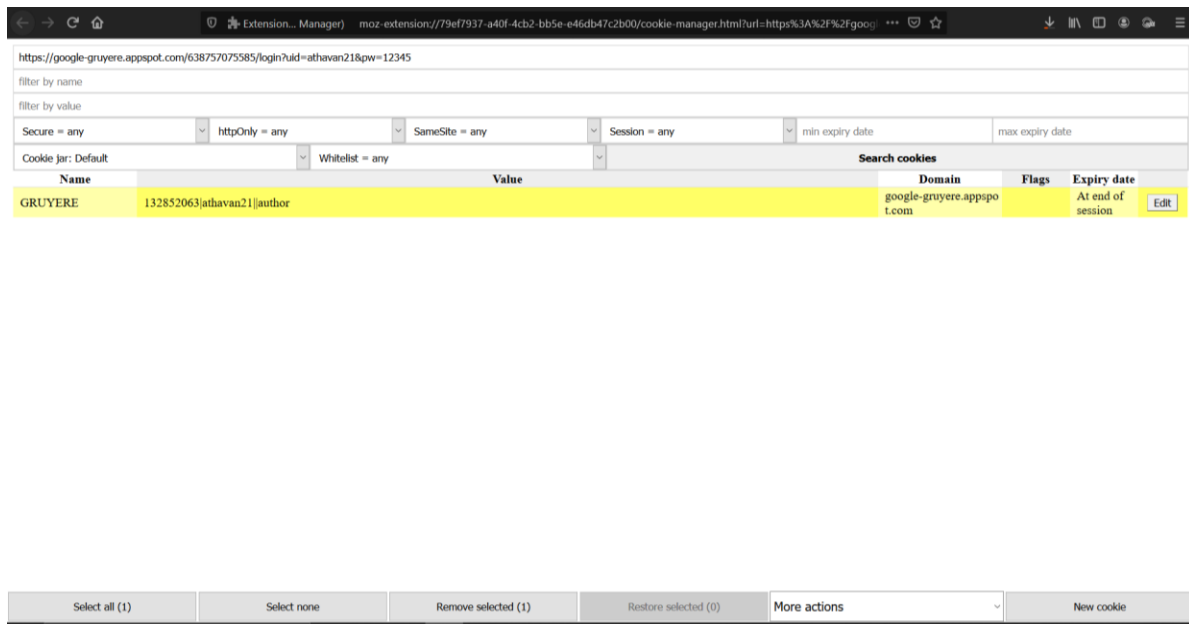
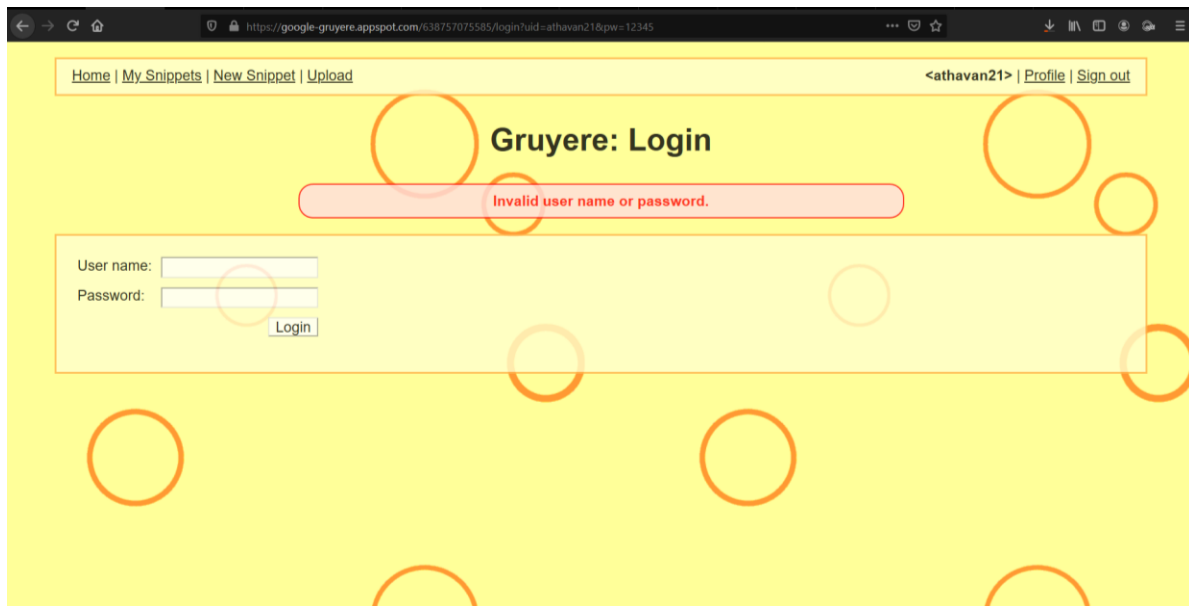
Both the values are same so we can conclude that integrity of the file is preserved.



The screenshot shows the VirusTotal web interface for a file named 'fchv.exe'. The file's MD5 hash is e2c6d562bd35352b73c00a744e9c07c6. The page displays various detection results, including 'Invalid-signature', 'overlay', 'peexe', and 'signed'. The 'Basic Properties' section lists several hashes and file details:

Property	Value
MD5	e2c6d562bd35352b73c00a744e9c07c6
SHA-1	f5259423eb42664dec7a32baa7cf0d85d13e752
SHA-256	fa03997f62beaf057023e5627881ecd4829e3c8383fd44b33f5e30a47ba25e31
Vhash	084046655d1510c8z4b7z409bzx1fz
Authenthash	88e0d78a9e97684cdf976acdd1dbe9660255a55b0a200aa89bda7239417d07
Imphash	27d678ab7f59de9d3b9c7dc6b25d4f62
Rich PE header hash	e4886e944fb62ed64939d4757e41290f
SSDEEP	1536:OLovfHsbMKnZ1o27+alJuxCPBwPmKOb+XUJBAcua1Ad:OLJHsbMD+kuJpO6XUHAcusBd
TLSH	T1ED83AE13BAE0847AD45205F0062D0F71F736EE291AB28983974CE99B3E53E09E2D34E
File type	Win32 EXE
Magic	PE32 executable for MS Windows (console) intel 80386 32-bit
TRID	Win32 Executable MS Visual C++ (generic) (44.2%)
TRID	Windows screen saver (18.5%)
TRID	Win16 NE executable (generic) (9.9%)
TRID	Win32 Dynamic Link Library (generic) (9.3%)
TRID	Win32 Executable (generic) (6.3%)

2.



Extension... Manager) moz-extension://79ef7937-a40f-4cb2-bb5e-e46db47c2b00/cookie-manager.html?url=https%3A%2F%2Fgoo.gl/...

Export cookies

Choose the export format and click on the "Export" button to export 1 cookie.

Use the JSON format if you would like to restore cookies later while preserving all metadata (storeId, sameSite, firstPartyDomain). Use the Netscape format if you would like to use the cookies with other tools such as curl. Either format can be imported later.

When exported as a file, the exported data is downloaded as "cookies.json" or "cookies.txt".  
When exported as text, the exported data is shown in a text field.

Output format:  
☒ JSON (full backup that preserves all metadata)  
☐ Netscape (for use with tools like curl)

Export as:  
☒ Export as file  
☐ Export as text

Export

Cancel

Extension... Manager) moz-extension://b3f66a29-dd3d-408e-99d0-bac4db620307/cookie-manager.html

Import cookies

Select a file or paste the exported data (JSON) or Netscape HTTP Cookie file in the input field.

When you click on the "Import" button, the cookies will be validated and overwrite existing cookies, without confirmation (except for whitelisted cookies).

Destination cookie jar: As specified in the imported file

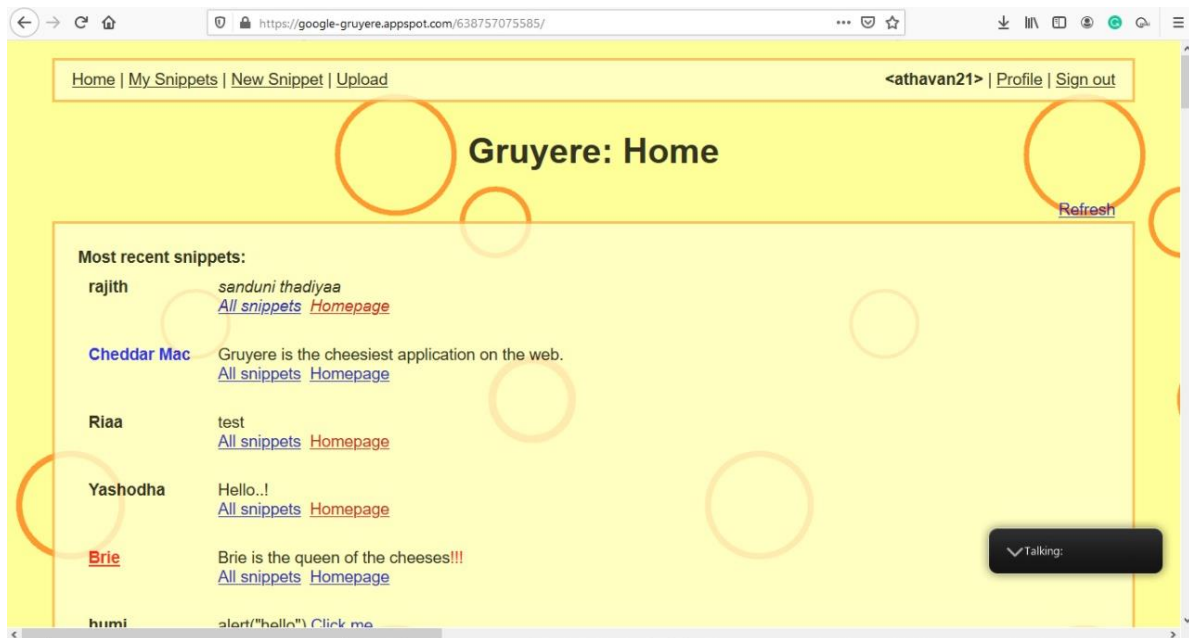
Import file: Browse... cookies (1).json or select text:

Imported all 1 cookies.

✓ Talking:

Import

Cancel



- Security is Questioned here  
Privacy is major threat
- No
- Computer Crimes Act, No 24 of 2007

3.

The image shows a sequence of browser screenshots. The top screenshot is a Google search for "what is my ip address". The search results show "112.135.252.250" as the public IP address. Below this, there is a link to "whatismyipaddress.com". The bottom screenshot shows the "db-ip.com" website. The website header includes the "dbip" logo and navigation links: API, Developers, Database, Tools, Statistics, and FAQ. A search bar in the header contains the IP address "112.135.252.250". The main content area of the website displays "IP ADDRESS GEOLOCATION" followed by the IP address "112.135.252.250" in large text. Below the IP address, it states: "112.135.252.250 or SLT-BB-CUST.slt.lk is an IPv4 address owned by Sltadsl-Slt and located in Katunayaka, Sri Lanka".

Google search results for "what is my ip address" showing the public IP address 112.135.252.250.

db-ip.com website showing IP address geolocation results for 112.135.252.250, identifying it as an IPv4 address owned by Sltadsl-Slt and located in Katunayaka, Sri Lanka.

**Address type** IPv4

**Hostname** SLT-BB-CUST.slt.lk

**ASN** 9329 - SLTINT-AS-AP

**ISP** Sltadsl-Slt

**Connection** xDSL

**Crawler** X

**Proxy** X

**Attack source** X

Estimated threat level for this IP address is **LOW**

**Country** Sri Lanka

**State / Region** Western

**City** Katunayaka

**Weather station** CEXX0005 - Katunayake

**Coordinates** 7,16992, 79.8884

**Timezone** Asia/Colombo (UTC+5.5)

Our systems have detected unusual traffic from your computer network. Please try your request again later. [Why did this happen?](#)

IP address: 112.135.252.250  
 Time: 2020-12-10T05:30:49Z  
 URL: https://www.google.com/search?&source=hp&ei=cLRR06WJ4XlaKrinYAJ&q=what+is+my+ip+address&btnK=Google+Suche

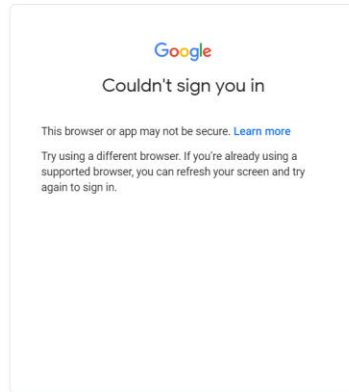
## Advantages of using a proxy server

- Your IP Address Is Hidden
- You Can Access Geo-Blocked or RestrictedContent
- You Can Access Geo-Blocked or Restricted Content
- Malicious Websites Can Be Filtered Out

4.

- Using a One Time Password (two-factor) only protects the authentication phase keep a separate gmail "dropbox" account for this purpose.

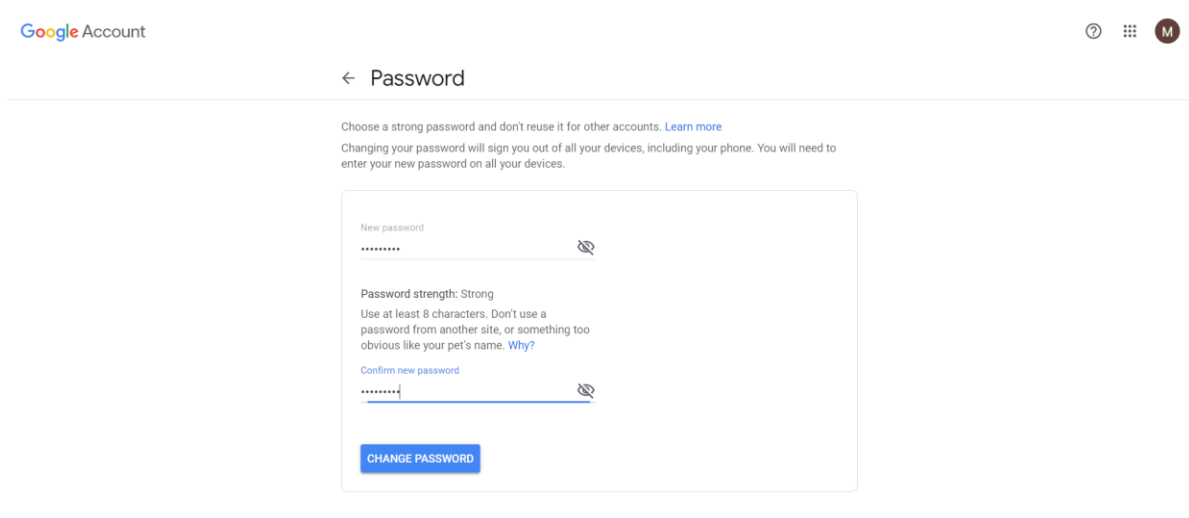
●



●

Proxy servers anonymize their users by changing their IP address, so that if a hacker wants to get access to a specific device on a network, it will be far more difficult to locate. if that data contains your email account name and password in unencrypted text, you bet a malicious proxy could be collecting that information.

●





## ← Recent security activity

Security activity and alerts from the last 28 days. [Learn more](#)

See unfamiliar activity?

December 10, 2020

11:54 AM	<b>Password changed</b> <span>New</span>	Sri Lanka Windows	>
----------	---	----------------------	---

## ← 2-Step Verification



### Protect your account with 2-Step Verification

Each time you sign in to your Google Account, you'll need your password and a verification code. [Learn more](#)



Add an extra layer of security

Enter your password and a unique verification code that's sent to your phone.



Keep the bad guys out

Even if someone else gets your password, it won't be enough to sign in to your account.

GET STARTED

## ← 2-Step Verification

2-Step Verification is ON since Dec 10, 2020

TURN OFF

### Available second steps

A second step after entering your password verifies it's you signing in. [Learn more](#)

**Note:** If you sign in to your Google Account on any eligible phone, Google prompts will be added as another method for 2-Step Verification.



Voice or text message (Default) ⓘ

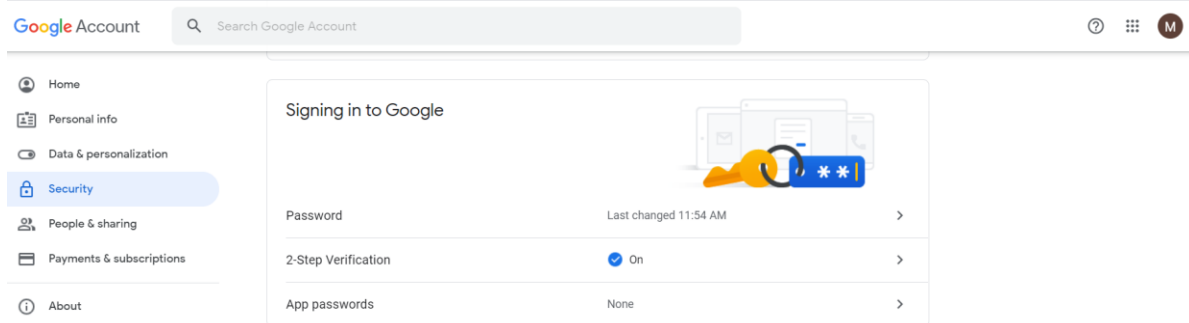
076 755 3401 Verified

Verification codes are sent by text message.



### Add more second steps to verify it's you

Set up additional backup steps so you can sign in even if your other options aren't available.



- Change your password On your Android phone or tablet, open your device's Settings app and then Google and then Manage your Google Account. At the top, tap Security. Under "Signing in to Google," tap Password. You might need to sign in. Enter your new password, then tap Change Password.
- Reset your password Follow the steps to recover your account. You'll be asked some questions to confirm it's your account and an email will be sent to you. If you don't get an email: Check your Spam or Bulk Mail folders. Add noreply@google.com to your address book. To request another email, follow the steps to recover your account . Check all email addresses you might've used to sign up or sign in to your account. Choose a password that you haven't already used with this account.

8.

### Passwords

A password is a shared secret known by the user and presented to the server to authenticate the user.

### Hard Tokens

The device may be in the form of a smart card, or it may be embedded in an easily-carried object such as a key fob or USB drive.

### Soft Tokens

Users are less likely to forget their phones at home than lose a single-use hardware token. When they do lose a phone, users are more likely to report the loss, and the soft token can be disabled. Soft tokens are less expensive and easier to distribute than hardware tokens, which need to be shipped.

### Biometric Authentication

Biometric authentication methods include retina, iris, fingerprint and finger vein scans, facial and voice recognition, and hand or even earlobe geometry. The latest phones are

adding hardware support for biometrics, such as Touch ID on the iPhone. Biometric factors may demand an explicit operation by the user

#### Contextual Authentication

Typically, a user's current context is compared to previously established context

#### Device Identification

device identification establishes a fingerprint that's somewhat unique to that device.

5.

Many Gmail users receive tens or hundreds of mails per day. The Priority Inbox attempts to alleviate such information overload by learning a per-user statistical model of importance, and ranking mail by how likely the user is to act on that mail.

### **References**

<https://support.google.com/accounts/answer/7299973?hl=en>

<https://support.google.com/accounts/answer/41078?co=GENIE.Platform%3DAndroid&hl=en>

### **Group 07**

<b><u>Name</u></b>	<b><u>Index Number</u></b>
R.M.D.K.B. Rajakaruna	18020641
W.H.M. Gunathilaka	18020275
S. Maayura	18020461
T. Athavan	18020097
T. Thushanthan	18020844