TRAINING PROGRAMME
FOR
MINISTRY OFFICIALS - CAMBODIA
AT NATIONAL JUDICIAL ACADEMY, BHOPAL ON 12TH DECEMBER 2023

ELECTRONIC EVIDENCE:

NEW HORIZONS, COLLECTION, PRESERVATION & APPRECIATION

- DR. HAROLD D'COSTA

President - Cyber Security Corporation
Advisor - Law Enforcement Agencies
International Trainer - Judges & Public Prosecutors

WHO OWNS THE INTERNET?

No one actually owns the Internet, and no single person or organization controls the Internet in its entirety.

ELECTRONIC EVIDENCE

The term ‘Electronic Evidence’ signifies a piece of evidence generated by some mechanical or electronic processes which is often relevant in proving or disproving a fact or fact at issue, the information that constitutes evidence before the court. Electronic Evidence is commonly known as Digital evidence.

SECTION 61

THE INDIAN EVIDENCE ACT, 1872

61. *Proof of Contents of Documents*

The contents of documents may be proved either by primary or by secondary evidence.

MAN CAN LIE BUT DOCUMENT CANNOT

IT ACT 2000 – CHAPTER XII-A
EXAMINER OF ELECTRONIC EVIDENCE

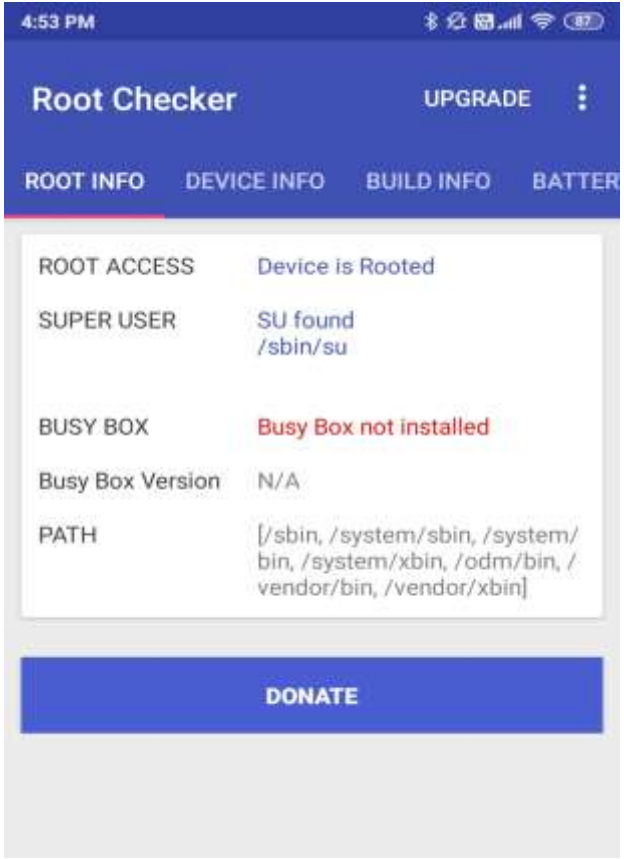
79A. *Central Government to notify Examiner of Electronic Evidence* – The Central Government may, for the purposes of providing expert opinion on electronic form evidence before any court or other authority specify, by notification in the Official Gazette, any Department, body or agency of the Central Government or a State Government as an Examiner of Electronic Evidence.

WHATSAPP CHAT MODIFICATION

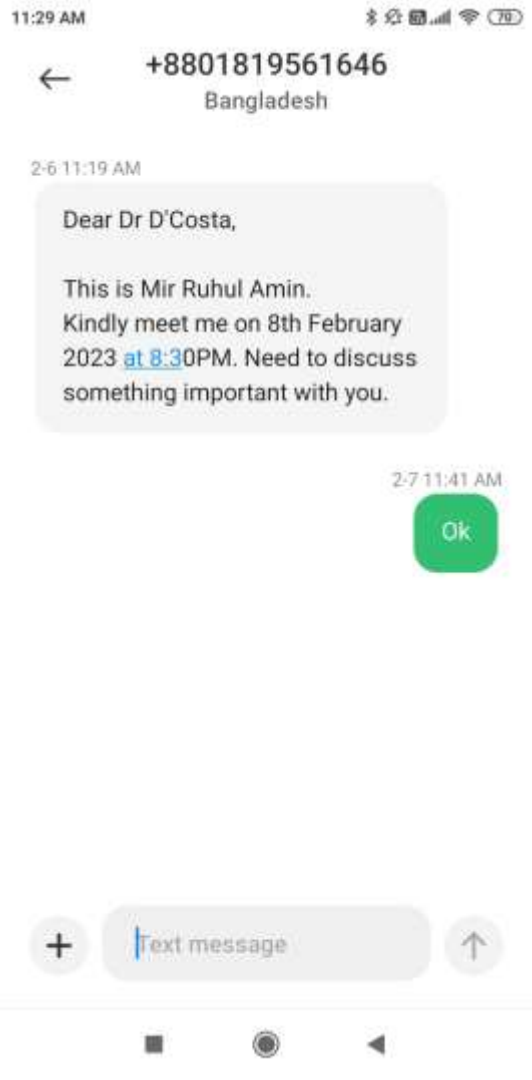
Even with end-to-end encryption WhatsApp messages can be modified

CHECK IF WHATSAPP IS MODIFIED

ROOTED MOBILE DEVICE



SMS SPOOFING

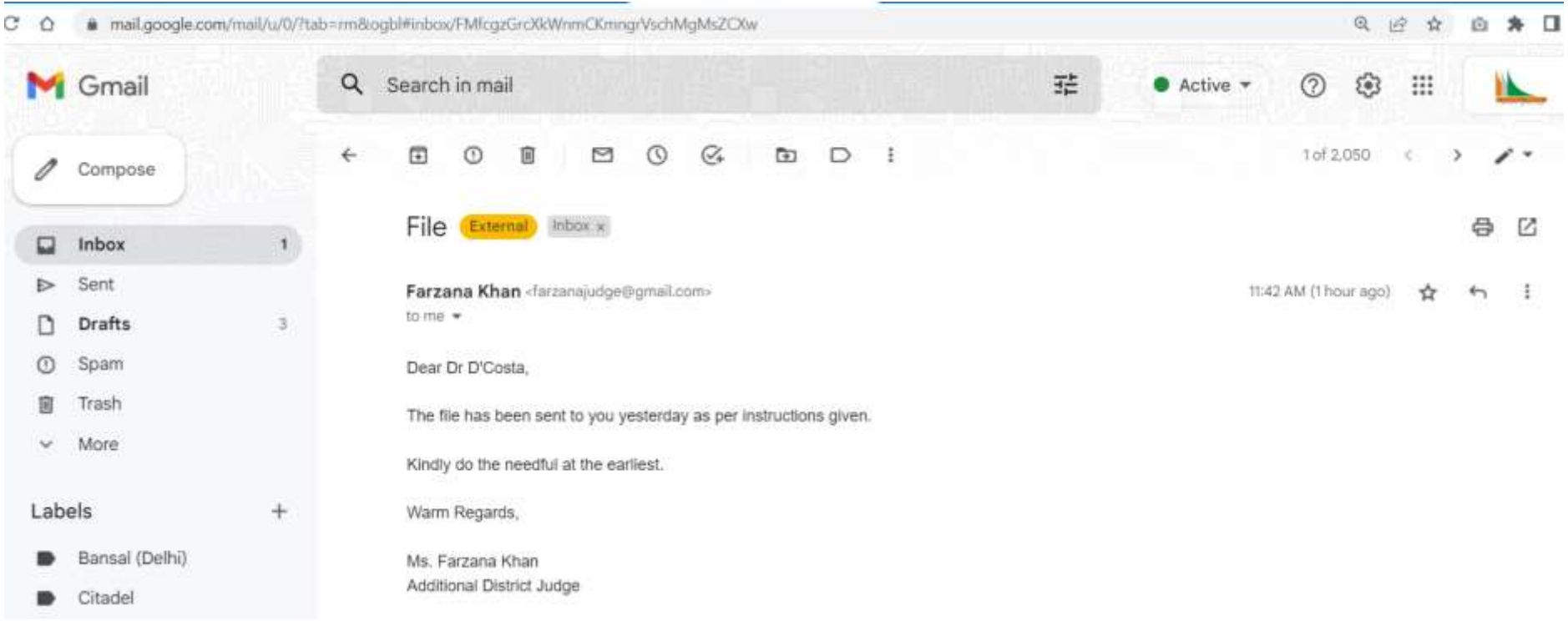


CALLER ID SPOOFING

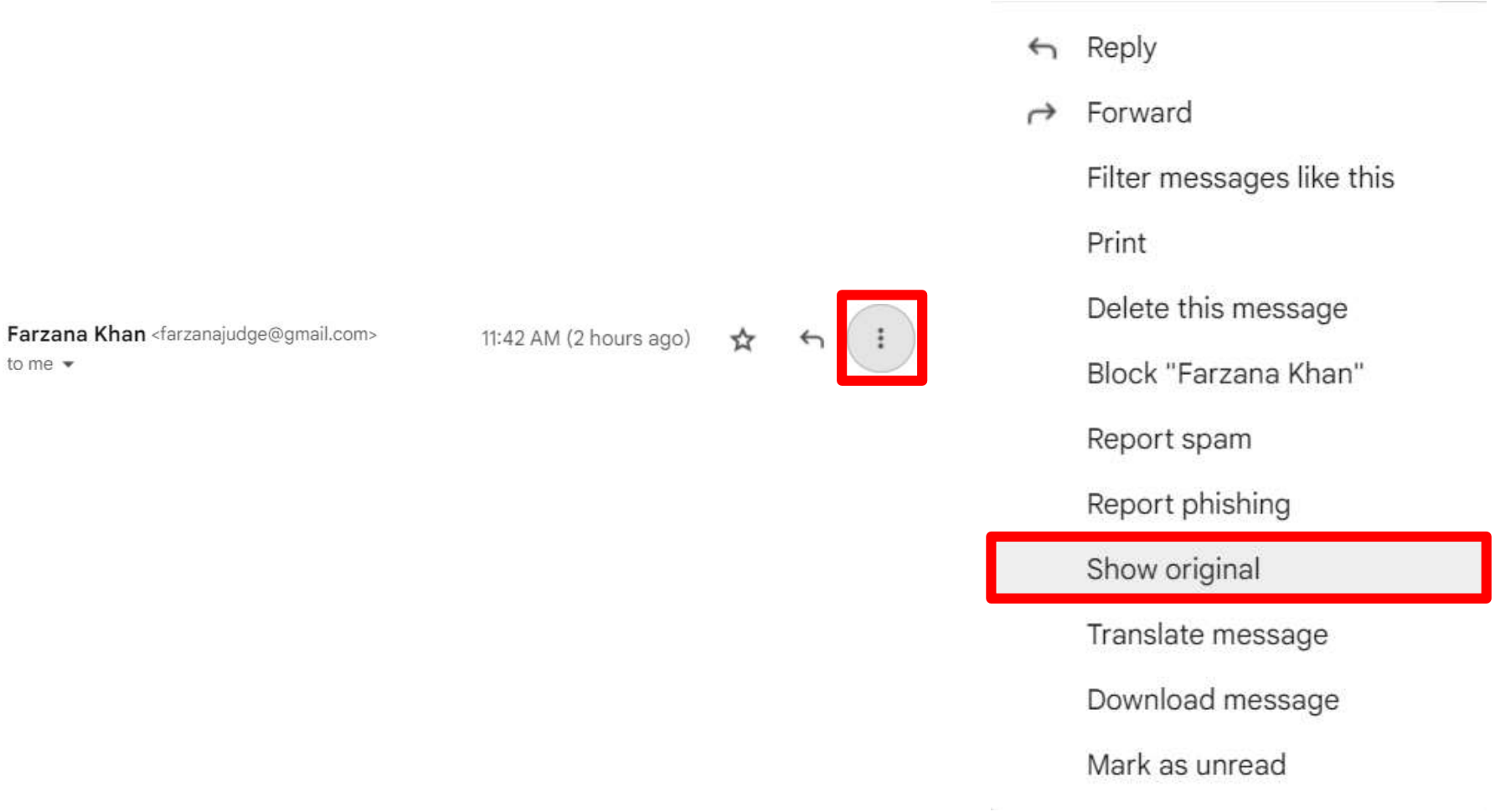
CALL & SMS AUTHENTICATION

Calling (A) Party Telephone Number	Called (B) Party Telephone Number	Call Date	Call Time	Call Duration (in seconds)	First Cell ID of Party A	Last Cell ID of Party A	Call Type (IN/OUT/SMS In/SMS OUT)	IMEI of A	IMSI of A	Type of connection (Pre-paid/ Post-paid)	SMS Centre Number
9819194961	TA-ezoneo	01-08-2012	09:30:48		29371		SMS-INCOMING	351532043881030	404212110033190	PostPaid	919246255009
9819194961	09892898647	01-08-2012	09:40:58	64	29371	0	OUTGOING	351532043881030	404212110033190	PostPaid	
9819194961	09892898647	01-08-2012	09:43:34	395	29371	0	OUTGOING	351532043881030	404212110033190	PostPaid	
9819194961	7738146965	01-08-2012	10:08:50	47	29371	0	INCOMING	351532043881030	404212110033190	PostPaid	
9819194961	7738146965	01-08-2012	10:09:55	11	29371	0	INCOMING	351532043881030	404212110033190	PostPaid	
9819194961	7738146965	01-08-2012	10:10:21	29	29371	0	INCOMING	351532043881030	404212110033190	PostPaid	
9819194961	919820212219	01-08-2012	10:46:50		26871		SMS-INCOMING	351532043881030	404212110033190	PostPaid	919250255008
9819194961	09870317249	01-08-2012	11:12:24	103	23103	0	OUTGOING	351532043881030	404212110033190	PostPaid	
9819194961	09870317249	01-08-2012	11:16:10	15	23103	0	INCOMING	351532043881030	404212110033190	PostPaid	
9819194961	912355680967	01-08-2012	11:18:02	128	23103	0	OUTGOING	351532043881030	404212110033190	PostPaid	
9819194961	09870317249	01-08-2012	11:30:21	10	23103	0	OUTGOING	351532043881030	404212110033190	PostPaid	
9819194961	9820826627	01-08-2012	11:33:47	19	23103	0	INCOMING	351532043881030	404212110033190	PostPaid	
9819194961	9820826627	01-08-2012	11:34:25	41	23103	0	OUTGOING	351532043881030	404212110033190	PostPaid	
9819194961	9820126182	01-08-2012	11:36:10	13	23103	0	OUTGOING	351532043881030	404212110033190	PostPaid	
9819194961	9820826627	01-08-2012	11:36:45	15	23103	0	OUTGOING	351532043881030	404212110033190	PostPaid	
9819194961	09773214433	01-08-2012	11:48:39	21	29131	13611	OUTGOING	351532043881030	404212110033190	PostPaid	
9819194961	09930727389	01-08-2012	12:00:38	145	31621	0	OUTGOING	351532043881030	404212110033190	PostPaid	
9819194961	TA-RNAICOR	01-08-2012	12:37:24		32803		SMS-INCOMING	351532043881030	404212110033190	PostPaid	919246255009
9819194961	9820826627	01-08-2012	12:51:19	62	25431	0	OUTGOING	351532043881030	404212110033190	PostPaid	
9819194961	9820826627	01-08-2012	12:52:47	29	25431	0	INCOMING	351532043881030	404212110033190	PostPaid	
9819194961	9820826627	01-08-2012	12:53:27	22	25431	0	OUTGOING	351532043881030	404212110033190	PostPaid	
9819194961	09594340252	01-08-2012	13:15:15	15	13082	0	INCOMING	351532043881030	404212110033190	PostPaid	
9819194961	09594340252	01-08-2012	13:17:25	9	29371	0	OUTGOING	351532043881030	404212110033190	PostPaid	
9819194961	919821671554	01-08-2012	13:56:52		32342		SMS-INCOMING	351532043881030	404212110033190	PostPaid	919821000005
9819194961	LM-MANTRA	01-08-2012	15:47:18		29371		SMS-INCOMING	351532043881030	404212110033190	PostPaid	919821000005
9819194961	TD4Dr.Batr	01-08-2012	17:08:58		29371		SMS-INCOMING	351532043881030	404212110033190	PostPaid	919250255008
9819194961	LM55666	01-08-2012	17:21:03		29371		SMS-INCOMING	351532043881030	404212110033190	PostPaid	919821200005
9819194961	09594340252	01-08-2012	18:20:47	23	29371	0	OUTGOING	351532043881030	404212110033190	PostPaid	

EMAIL SPOOFING



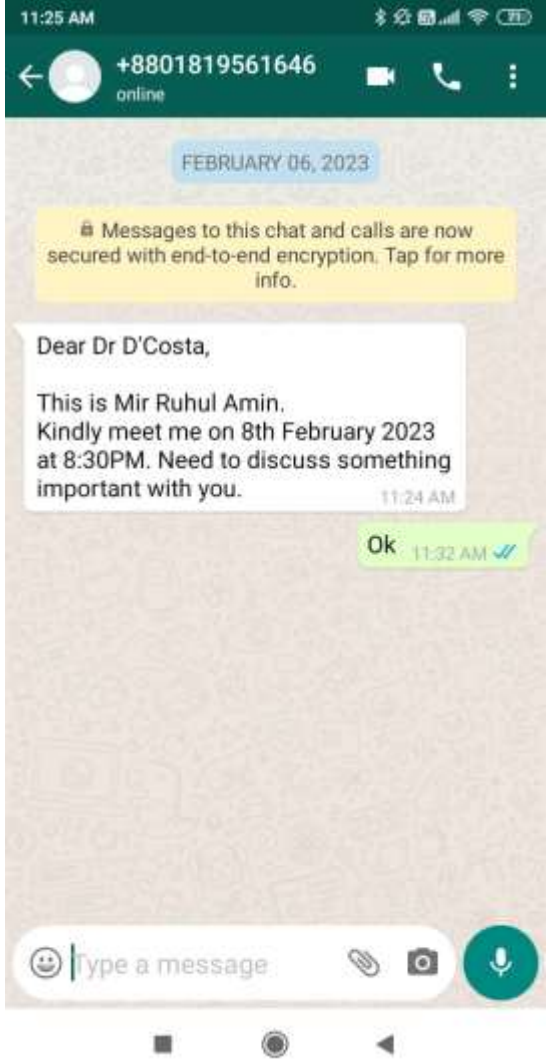
EMAIL AUTHENTICITY



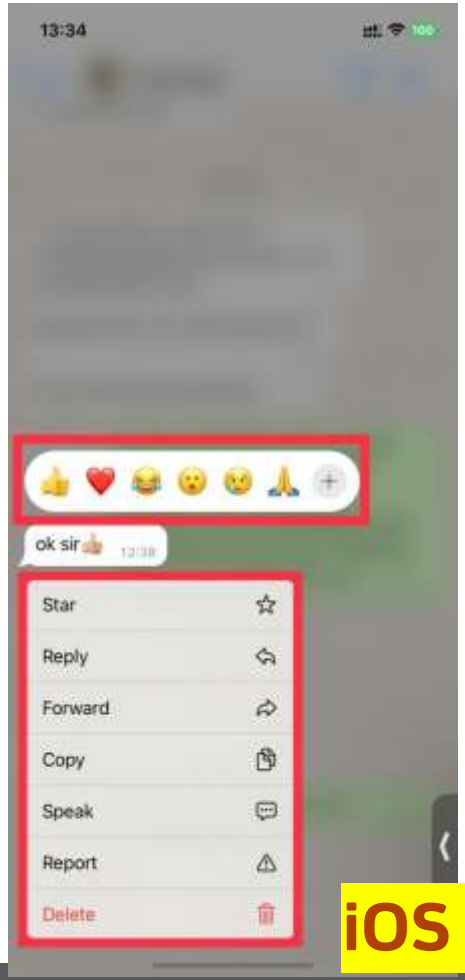
EMAIL AUTHENTICITY

```
ARC-Authentication-Results: i=1; mx.google.com;
       spf=softfail (google.com: domain of transitioning farzanajudge@gmail.com does not designate 89.187.129.22 as permitted sender)
smtp.mailfrom=farzanajudge@gmail.com;
       dmarc=fail (p=NONE sp=QUARANTINE dis=NONE) header.from=gmail.com
Return-Path: <farzanajudge@gmail.com>
Received: from emkei.cz (emkei.cz. [89.187.129.22])
        by mx.google.com with ESMTPS id f6-20020a5d50c6000000b002bfbb48222dsi15543000wrt.755.2023.02.07.22.12.37
        for <support@cybersolution.in>
        (version=TLS1_3 cipher=TLS_AES_256_GCM_SHA384 bits=256/256);
        Tue, 07 Feb 2023 22:12:37 -0800 (PST)
Received-SPF: softfail (google.com: domain of transitioning farzanajudge@gmail.com does not designate 89.187.129.22 as permitted
sender) client-ip=89.187.129.22;
Authentication-Results: mx.google.com;
       spf=softfail (google.com: domain of transitioning farzanajudge@gmail.com does not designate 89.187.129.22 as permitted sender)
smtp.mailfrom=farzanajudge@gmail.com;
       dmarc=fail (p=NONE sp=QUARANTINE dis=NONE) header.from=gmail.com
Received: by emkei.cz (Postfix, from userid 33) id 179E25510FC; Wed,
  8 Feb 2023 07:12:37 +0100 (CET)
To: support@cybersolution.in
Subject: File
From: Farzana Khan <farzanajudge@gmail.com>
X-Priority: 3 (Normal)
Importance: Normal
Errors-To: farzanajudge@gmail.com
Reply-To: farzanajudge@gmail.com
Content-Type: text/plain; charset=utf-8
Message-Id: <20230208061237.179E25510FC@emkei.cz>
Date: Wed,
  8 Feb 2023 07:12:37 +0100 (CET)
```

WHATSAPP MESSAGE SPOOFING



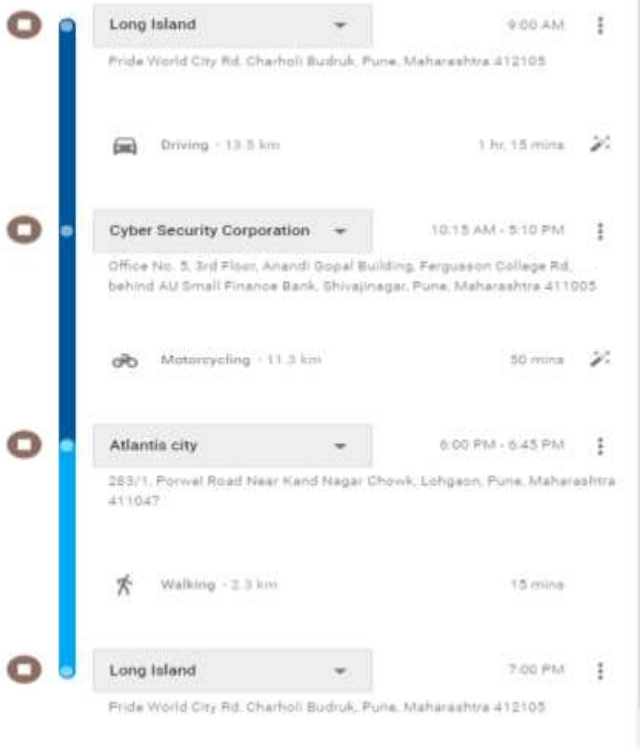
WHATSAPP MESSAGE AUTHENTICITY



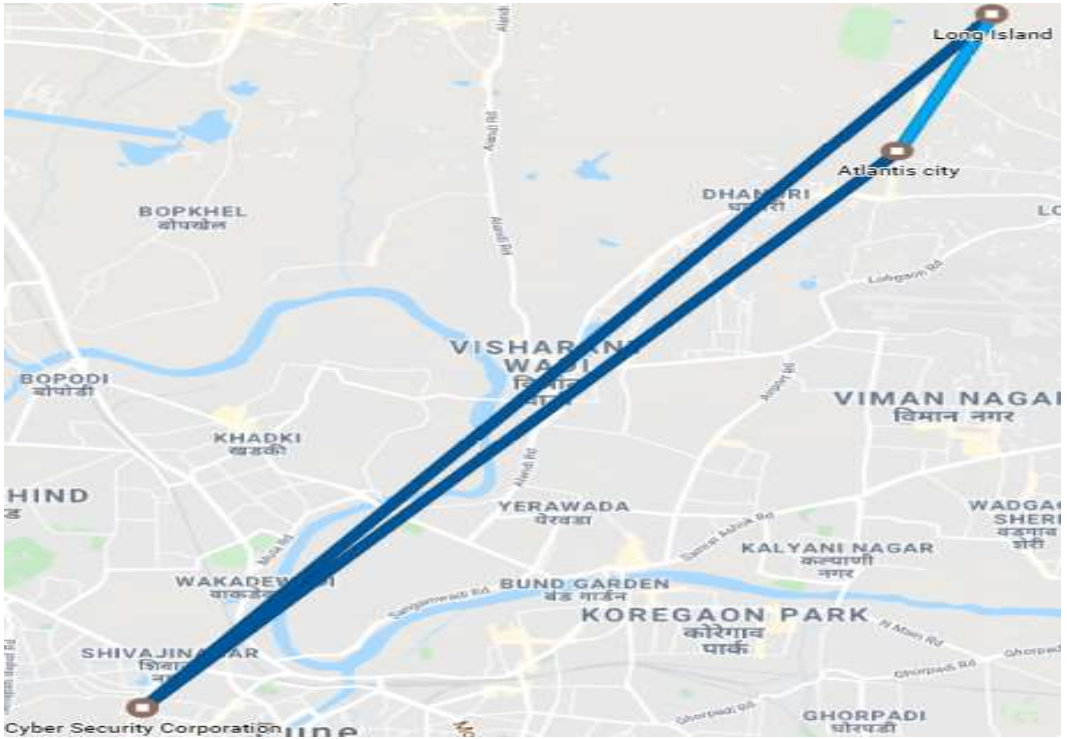
CAN LOCATION COORDINATES BE MODIFIED?

Yes!

EDITED LOCATION



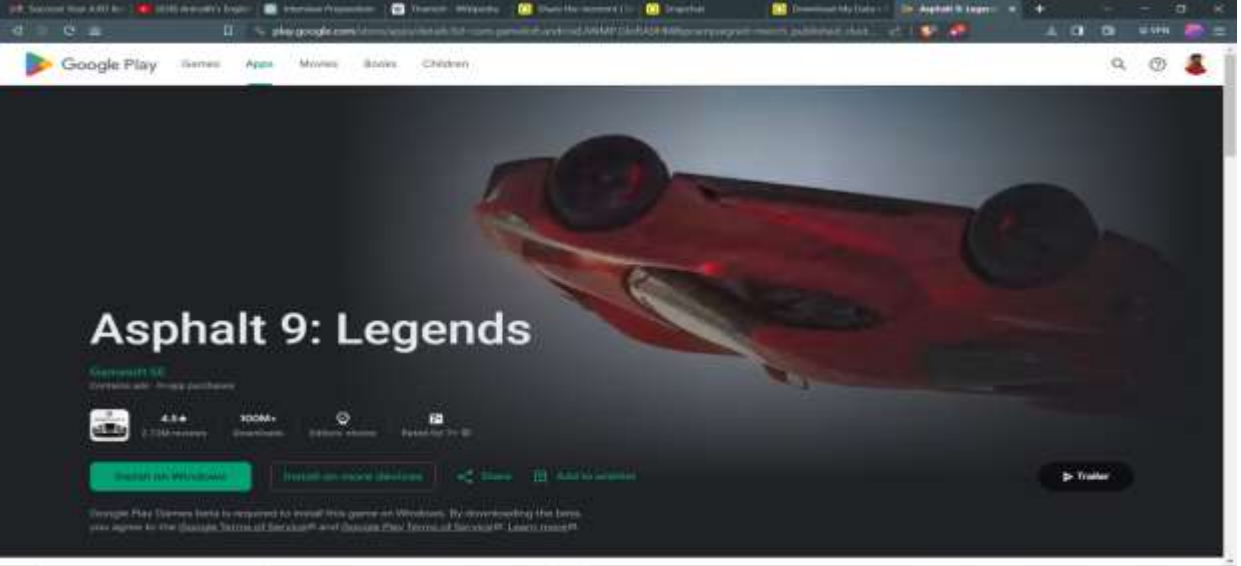
Once you have added all locations, Select appropriate mode of transport.

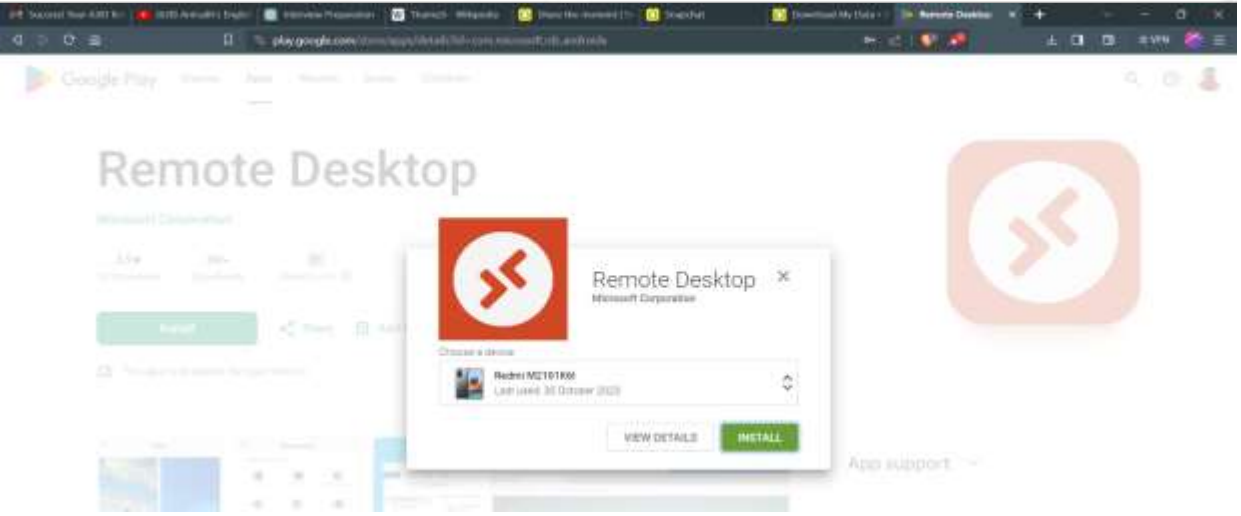


COLOR REPRESENTATIONS

Dark Blue	Sea Green	Light Blue	Red
Driving	Cycling	Walking	Running
In a taxi or Rideshare	Horse Riding	By Wheelchair	Catching Pokémon
Motorcycling	Kayaking	Moving	Hiking
On a bus	Kite Surfing		Nordic Walking
On the Subway	Paragliding		Rowing
On a train	Sailing		Snowshoeing
On a tram	Skateboarding		Swimming
Flying	Skating		
Boating	Skiing		
In a Cable Car	Sledding		
In a Gandola Lift	Snowboarding		
On a ferry	Surfing		
On a funicular			
Snowmobiling			

TIMELINE MODIFICATION DATE WILL BE DISPLAYED

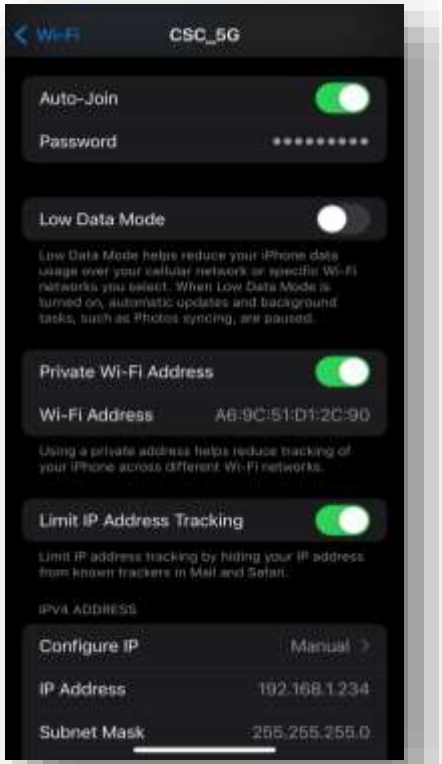




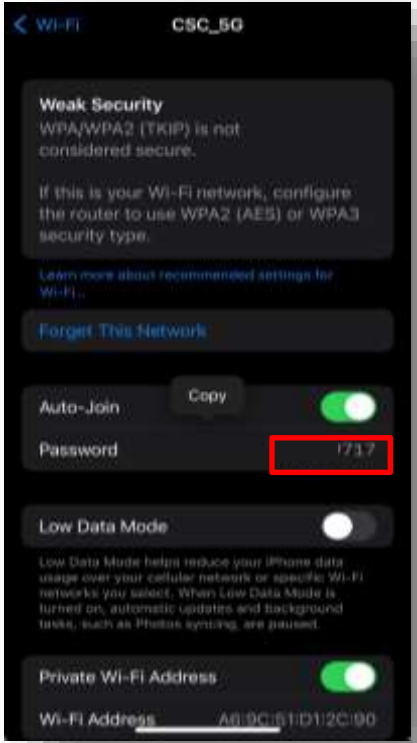
REMOTELY INSTALL APPS ON ANDROID FROM A PC

- Application would be automatically installed remotely on your android device without having to interact with any prompt
- The application can only be installed, it can not be operated or opened remotely.

VIEW WI-FI PASSWORD
(IOS)



TAP ON THE PASSWORD TO VIEW IT IN PLAIN TEXT (AUTHENTICATION REQUIRED)



VIEW WI-FI PASSWORD
[ANDROID]

You cannot view Wi-fi password directly on an android device instead you can generate a QR code for sharing it .

ADMISSIBILITY OF DIGITAL EVIDENCE

CONDITIONS FOR ADMISSIBILITY OF ELECTRONIC EVIDENCE

(a) The computer output containing the information was produced by the computer during the period over which the computer was used regularly to store or process information for the purposes of any activities regularly carried over that period by person having lawful control over the use of the computer;

(b) During the said period, information of the kind contained in the electronic record or of the kind from which the information so contained is derived was regularly fed into the computer in ordinary course of the said activities;

(c) Throughout the material part of the said period the computer was operating properly, or if not, then in respect of any period, in which it was not operating properly or was out of operation during that part of time, was not such as to affect the electronic record or the accuracy of its contents; and

(d) The information contained in the electronic record reproduces or is derived from such information fed into the computer in ordinary course of the said activities.

APPRECIATION OF DIGITAL EVIDENCE

SECTION 65(B)(4)

Under the section 65(B)(4) the certificate which identifies the electronic record containing the statement and describes the manner in which it was produced giving the particulars of the device involved in the production of that records and deals with the conditions mentioned in Section 65(B)(2) and is signed by a person occupying a responsible official position in relation to the operation of the relevant device shall be evidence of any matter stated in the certificate.

CONTENTS OF THE CERTIFICATE

- Following points are the necessary to be covered in the certificate to prove the authenticity of the evidence.
- That the information contained in the hard disks of the mentioned electronic device was regularly recorded into them in the ordinary course of activity.
- That during the period in question the mentioned device were operating properly at all times and there have been no such operational problems so as to affect the accuracy of electronic record.
- That the computer hardware and software used in the computer system have built in security systems.

WHEN IS IT APPLICABLE?

- When signed by a person occupying a responsible official position in relation to operation of relevant device.

- Source, authenticity which are the two hallmarks pertaining to electronic record sought to be used as evidence.

- Only if the electronic record is duly produced in the terms of the Section 65-B of Indian Evidence Act, the question would arise as to the genuineness thereof and in that situation, resort cannot be made to Section 45A - opinion of examiner of electronic evidence.

Certificate u/s 65B of the Indian Evidence Act, 1872.

This is to certify that I, _____, residing at_____, state to the best of my knowledge and belief that I have extracted the images from a mobile device having following details:

DEVICE DETAILS	
MODEL NUMBER	
DEVICE NAME	
SIZE	
SERIAL NUMBER	
IMEI NUMBER	

I state that the device used for extracting the photos was functioning normally at all times.

I further state that the device utilized by me was used to store and process data and were operating properly and there is no distortion in the accuracy of the contents of the copies of the images.

The above is stated to the best of my knowledge and belief.

_____

DR. HAROLD D'COSTA

+91-7709619249

hld@rediffmail.com

CYBER SECURITY CORPORATION