Handling **Real Time Cyber Crimes** & Investigation!

By : Lakshit Verma
Courtesy : Cyber Saksham Program

Disclaimer : All The Documents , Photographs Used Are Only For Demo Purposes ! We've Tried To Maintain To Integrity Of Collected Evidences

What Can Be **Termed As A Cyber Crime** ?

- What Can Be **Termed As A Cyber Crime** ?
- Performing An Illegal activity over internet using electronic instruments to further illegal results.
- Eg: stalking , cyber bullying.

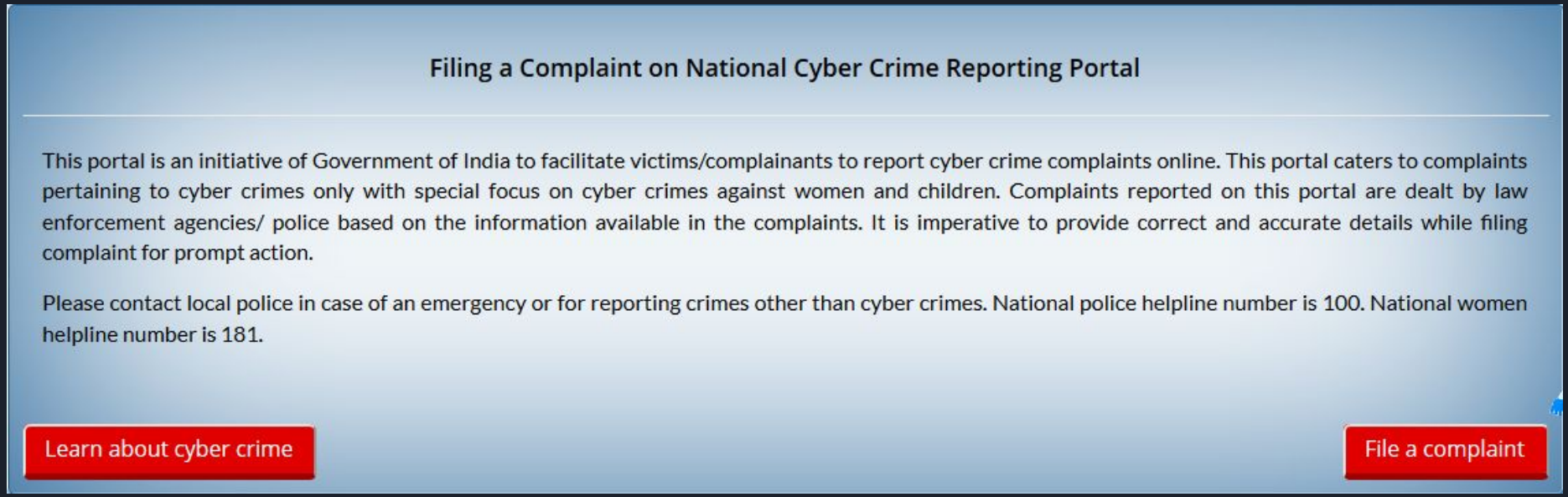
Top Rated Cyber Crimes !

- Monetary Fraud : ATM/Carding/Banking Frauds
- Defamation : Cyber Bullying/Stalking/Online Abuse/
- Cyber Stalking
- Virus Insertion
- Forwarding Fake News

Crimes Targeting Computer **Sys**tems!

- Hacking : Section 66, of ITAA 2008
- Dos Attack : Section 66C, of ITAA 2008
- Website Defacement : Section 66 of ITAA 2008
- Cyber Terrorism : Section 66F, of ITAA 2008
- Skimming : Section 66C, of ITAA 2008
- Identity Theft : Section 66C, 66D of ITAA 2008
- Data Manipulation : Section 66 OF ITAA 2008
- Poronography : Section 66E, 67A, 67B, ITAA 2008 & IPC 292
- Cyber Bullying/Stalking : Section 66A , Of ITAA 2008

Where To **Report** ! : Cybercrime.gov.in



Investigation **Process Of Cyber Crime** !

Investigation **Process Of Cyber Crime** !

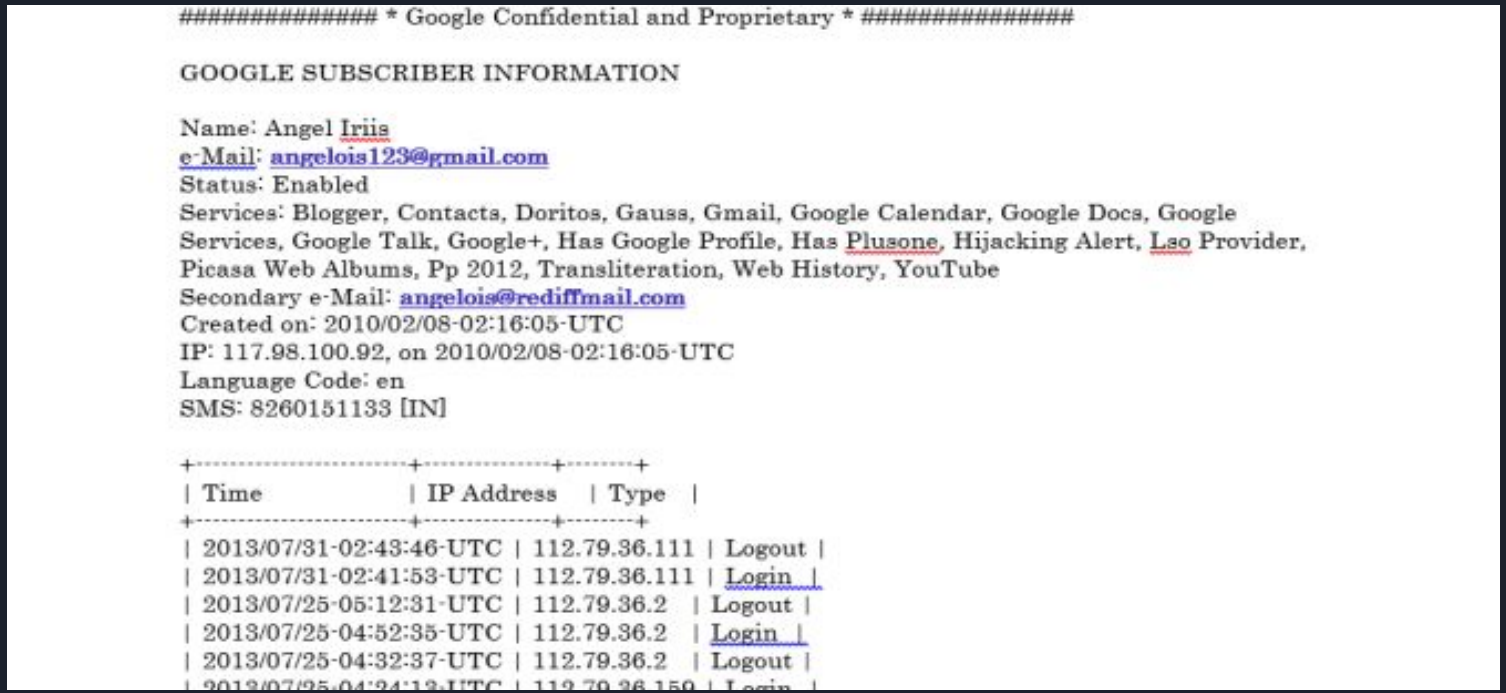
- Reporting The Crime
- Writing Legal Docs
- Assigning Of IO
- Investigation Process
- Evidence Collection
- Submitting Evidence To Laboratory
- Forwarding Suitable Penalty To Guilty One

Let's Take a Demo :

How To Analyze Email Headers

How These **Crimes Are Investigated** ?

- **G**oogle **R**eport !



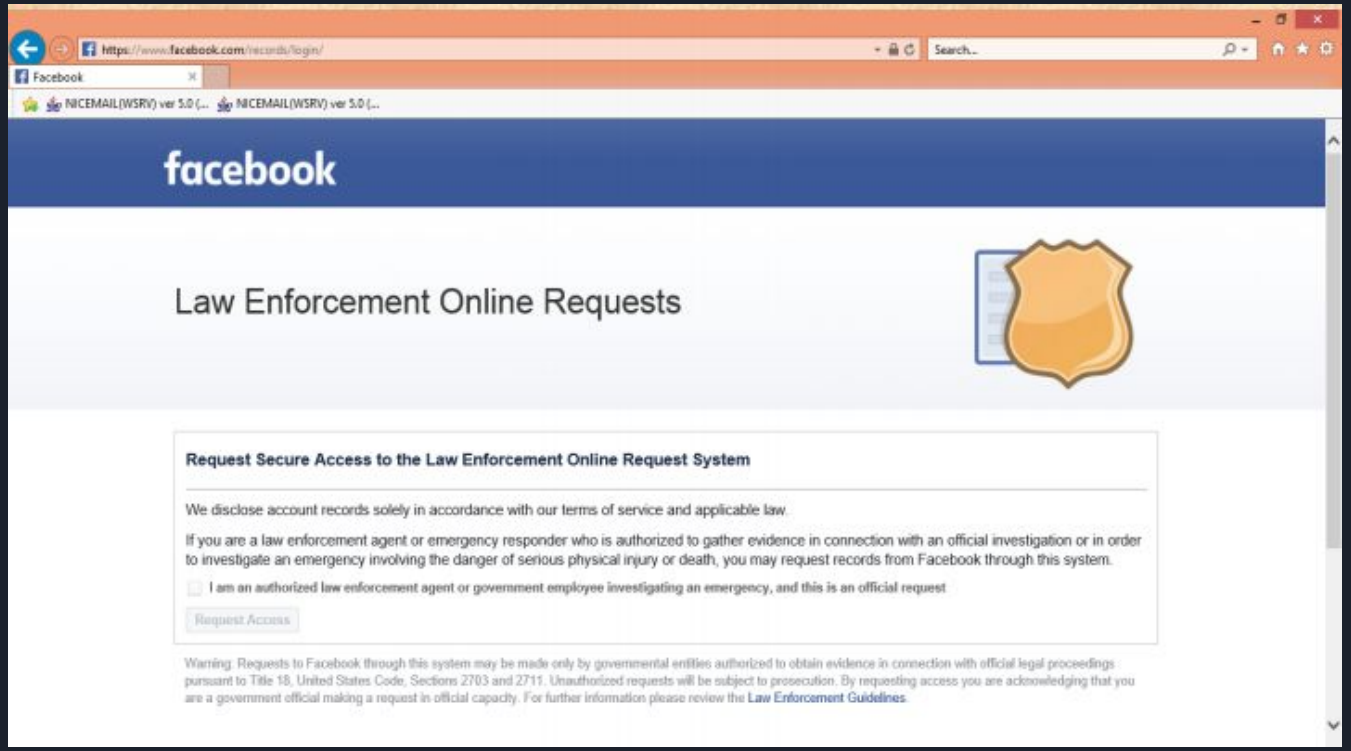
################ * Google Confidential and Proprietary * #################

GOOGLE SUBSCRIBER INFORMATION

Name: Angel Iriis
e-Mail: angelois123@gmail.com
Status: Enabled
Services: Blogger, Contacts, Doritos, Gauss, Gmail, Google Calendar, Google Docs, Google Services, Google Talk, Google+, Has Google Profile, Has Plusone, Hijacking Alert, Lso Provider, Picasa Web Albums, Pp 2012, Transliteration, Web History, YouTube
Secondary e-Mail: angelois@rediffmail.com
Created on: 2010/02/08-02:16:05-UTC
IP: 117.98.100.92, on 2010/02/08-02:16:05-UTC
Language Code: en
SMS: 8260151133 [IN]

Time	IP Address	Type
2013/07/31-02:43:46-UTC	112.79.36.111	Logout
2013/07/31-02:41:53-UTC	112.79.36.111	Login
2013/07/25-05:12:31-UTC	112.79.36.2	Logout
2013/07/25-04:52:35-UTC	112.79.36.2	Login
2013/07/25-04:32:37-UTC	112.79.36.2	Logout

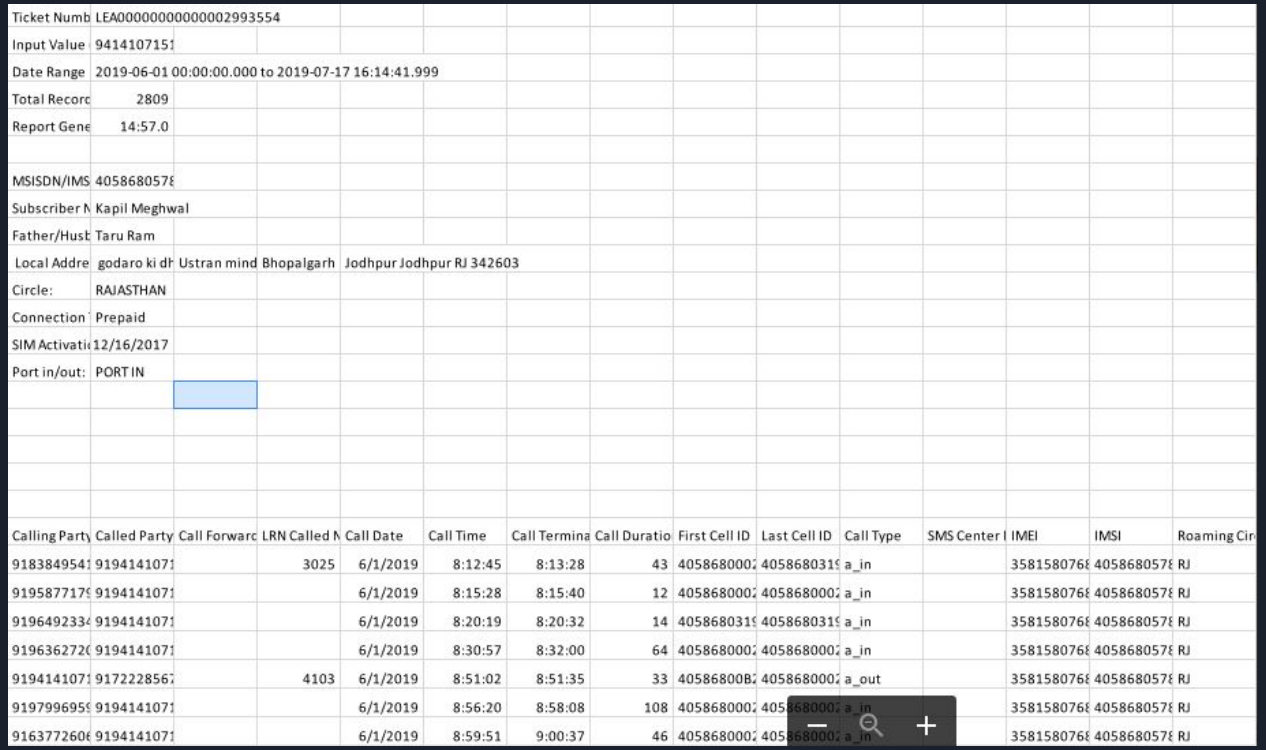
LEA Portal : Facebook



- Request Letter To ISP :

Sl. No.	IP address	Log details in date & time as per UTC [Universal Co-ordinated Time]	Log details in date & time as per IST [Indian Standard Time] = [UTC + 05:30hrs]
1.	117.203.254.20	01.09.2014 at 07:38:46	**01.09.2014 at 13:08:46**
2.	117.214.84.255	06.09.2014 at 06:03:26	**06.09.2014 at 11:33:26**
3.	117.203.255.50	08.09.2014 at 12:15:43	**08.09.2014 at 17:45:43**
4.	59.93.128.219	09.09.2014 at 06:22:24	**09.09.2014 at 11:52:24**
5.	117.203.211.66	15.09.2014 at 05:52:37	**15.09.2014 at 11:22:37**
6.	117.203.255.198	17.09.2014 at 13:22:14	**17.09.2014 at 18:52:14**

Sample : CD-R Records



Ticket Numb	LEA00000000000002993554													
Input Value	9414107151													
Date Range	2019-06-01 00:00:00.000 to 2019-07-17 16:14:41.999													
Total Recorc	2809													
Report Gene	14:57.0													
MSISDN/IMS	405868057E													
Subscriber N	Kapil Meghwal													
Father/Husb	Taru Ram													
Local Addre	godaro ki dH	Ustran mind	Bhopalgarh	Jodhpur Jodhpur RJ 342603										
Circle:	RAJASTHAN													
Connection	Prepaid													
SIM Activati	12/16/2017													
Port in/out:	PORT IN													
Calling Party	Called Party	Call Forwarc	LRN Called N	Call Date	Call Time	Call Termina	Call Duratio	First Cell ID	Last Cell ID	Call Type	SMS Center I	IMEI	IMSI	Roaming Cir
918384954:	919414107:		3025	6/1/2019	8:12:45	8:13:28	43	405868000Z	405868031S	a_in		3581580768	405868057E	RJ
919587717S	919414107:			6/1/2019	8:15:28	8:15:40	12	405868000Z	405868000Z	a_in		3581580768	405868057E	RJ
919649233-	919414107:			6/1/2019	8:20:19	8:20:32	14	405868031S	405868031S	a_in		3581580768	405868057E	RJ
919636272(	919414107:			6/1/2019	8:30:57	8:32:00	64	405868000Z	405868000Z	a_in		3581580768	405868057E	RJ
919414107:	917222856Z		4103	6/1/2019	8:51:02	8:51:35	33	40586800BZ	405868000Z	a_out		3581580768	405868057E	RJ
919799695S	919414107:			6/1/2019	8:56:20	8:58:08	108	405868000Z	405868000Z	a_in		3581580768	405868057E	RJ
916377260(	919414107:			6/1/2019	8:59:51	9:00:37	46	405868000Z	405868000Z	a_in		3581580768	405868057E	RJ

Sample Report From **ISP** :

Data Networks Circle
BB-NOC Bangalore, O/o DGM BB
Ph –080-25809988, Fax-25806666
e-mail- bbnoc@dataone.in

भारत संचार निगम लिमिटेड
(भारत सरकार का उपक्रम)
BHARAT SANCHAR NIGAM LIMITED
(A Govt. of India Enterprise)

CONFIDENTIAL

No-DNW/DGM-BG/BB-NOC/IP-Detail/01 Dated @Bangalore the 12-08-2013

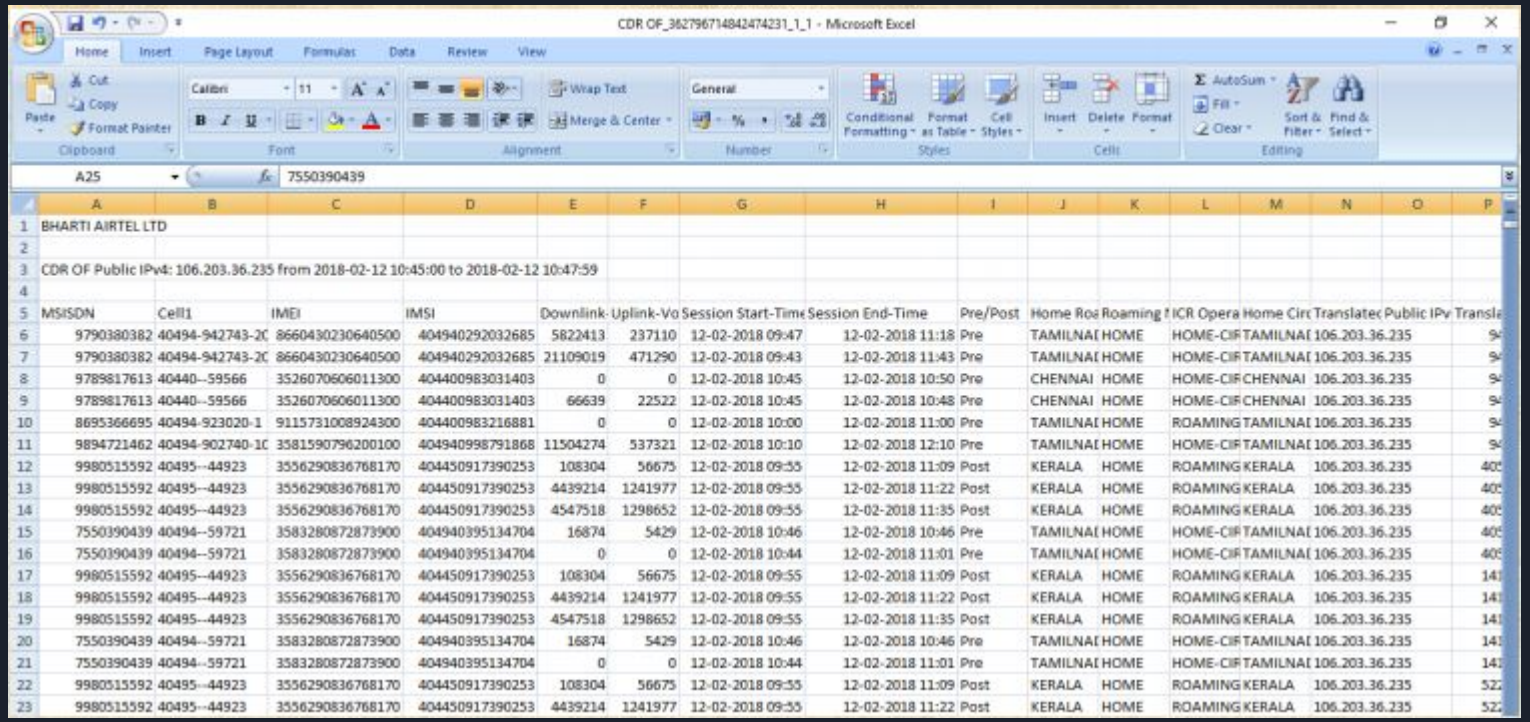
To,

The Circle Co-ordinator, BSNL.

Sub.:- Details of IP address :-

Sl. No.	Details Provided			Time in IST	User Information [For Date/Time given & converted in IST]
	IP Address	Date	Time in GMT		
1.	117.197.240.198 MAC: 00:26:15:0f:ff:68 2/2 vlan-id 2017;560 pppoe 203 bbr-ras-bng-tbv-01 117.197.240.198	28.12.2012	9:15:08	14:45:08	User-id: mana9_ecdrid@bsnl.in Name: Phone No: Address : Start Time : Thu Dec 27 17:49:43 2012 Stop Time : Fri Dec 28 17:49:43 2012

Sample From AIRTEL : CD-R Records



CDR OF_3627967148424742311_1 - Microsoft Excel

Home | Insert | Page Layout | Formulas | Data | Review | View

A25: 7550390439

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
1	BHARTI AIRTEL LTD															
2																
3	CDR OF Public IPv4: 106.203.36.235 from 2018-02-12 10:45:00 to 2018-02-12 10:47:59															
4																
5	MSISDN	Cell1	IMEI	IMSI	Downlink	Uplink-Vo	Session Start-Time	Session End-Time	Pre/Post	Home Roa	Roaming	ICR Opera	Home Circ	Translatec	Public IPv	Transla
6	9790380382	40494-942743-2(	8660430230640500	404940292032685	5822413	237110	12-02-2018 09:47	12-02-2018 11:18	Pre	TAMILNAI	HOME	HOME-CIR	TAMILNAI	106.203.36.235		9
7	9790380382	40494-942743-2(	8660430230640500	404940292032685	21109019	471290	12-02-2018 09:43	12-02-2018 11:43	Pre	TAMILNAI	HOME	HOME-CIR	TAMILNAI	106.203.36.235		9
8	9789817613	40440--59566	3526070606011300	404400983031403	0	0	12-02-2018 10:45	12-02-2018 10:50	Pre	CHENNAI	HOME	HOME-CIR	CHENNAI	106.203.36.235		9
9	9789817613	40440--59566	3526070606011300	404400983031403	66639	22522	12-02-2018 10:45	12-02-2018 10:48	Pre	CHENNAI	HOME	HOME-CIR	CHENNAI	106.203.36.235		9
10	8695366695	40494-923020-1	9115731008924300	404400983216881	0	0	12-02-2018 10:00	12-02-2018 11:00	Pre	TAMILNAI	HOME	ROAMING	TAMILNAI	106.203.36.235		9
11	9894721462	40494-902740-1(	3581590796200100	404940998791868	11504274	537321	12-02-2018 10:10	12-02-2018 12:10	Pre	TAMILNAI	HOME	HOME-CIR	TAMILNAI	106.203.36.235		9
12	9980515592	40495--44923	3556290836768170	404450917390253	108304	56675	12-02-2018 09:55	12-02-2018 11:09	Post	KERALA	HOME	ROAMING	KERALA	106.203.36.235		40
13	9980515592	40495--44923	3556290836768170	404450917390253	4439214	1241977	12-02-2018 09:55	12-02-2018 11:22	Post	KERALA	HOME	ROAMING	KERALA	106.203.36.235		40
14	9980515592	40495--44923	3556290836768170	404450917390253	4547518	1298652	12-02-2018 09:55	12-02-2018 11:35	Post	KERALA	HOME	ROAMING	KERALA	106.203.36.235		40
15	7550390439	40494--59721	3583280872873900	404940395134704	16874	5429	12-02-2018 10:46	12-02-2018 10:46	Pre	TAMILNAI	HOME	HOME-CIR	TAMILNAI	106.203.36.235		40
16	7550390439	40494--59721	3583280872873900	404940395134704	0	0	12-02-2018 10:44	12-02-2018 11:01	Pre	TAMILNAI	HOME	HOME-CIR	TAMILNAI	106.203.36.235		40
17	9980515592	40495--44923	3556290836768170	404450917390253	108304	56675	12-02-2018 09:55	12-02-2018 11:09	Post	KERALA	HOME	ROAMING	KERALA	106.203.36.235		14
18	9980515592	40495--44923	3556290836768170	404450917390253	4439214	1241977	12-02-2018 09:55	12-02-2018 11:22	Post	KERALA	HOME	ROAMING	KERALA	106.203.36.235		14
19	9980515592	40495--44923	3556290836768170	404450917390253	4547518	1298652	12-02-2018 09:55	12-02-2018 11:35	Post	KERALA	HOME	ROAMING	KERALA	106.203.36.235		14
20	7550390439	40494--59721	3583280872873900	404940395134704	16874	5429	12-02-2018 10:46	12-02-2018 10:46	Pre	TAMILNAI	HOME	HOME-CIR	TAMILNAI	106.203.36.235		14
21	7550390439	40494--59721	3583280872873900	404940395134704	0	0	12-02-2018 10:44	12-02-2018 11:01	Pre	TAMILNAI	HOME	HOME-CIR	TAMILNAI	106.203.36.235		14
22	9980515592	40495--44923	3556290836768170	404450917390253	108304	56675	12-02-2018 09:55	12-02-2018 11:09	Post	KERALA	HOME	ROAMING	KERALA	106.203.36.235		52
23	9980515592	40495--44923	3556290836768170	404450917390253	4439214	1241977	12-02-2018 09:55	12-02-2018 11:22	Post	KERALA	HOME	ROAMING	KERALA	106.203.36.235		52

Did you **find your Intimate Picture/Video Online?**
Firstly you need to know it's not your fault!

- https://bit.ly/3i4XFAD

Any questions?

You can find me at:

Twitter : @acelakshitverma

acelakshitverma@gmail.com