Computer **Forensics & Digital Evidences**

By : Lakshit Verma

Contents :

- What Id Digital/Computer Forensics
- Need Of Computer Forensics
- Types Of Cyber Crimes
- Tools Used In Forensics
- Real Case Study : Forensics Investigation
- Key Areas To Knowledge
- Process Of Digital Investigation
- Who Uses Computer Forensics
- Future Of Forensics

What Is
Digital Forensics?
interworks
ALERT

What Is Computer Forensics !

- Digital forensics (sometimes known as digital forensic science) is a branch of forensic science encompassing the recovery and investigation of material found in digital devices, often in relation to computer crime.

  In Other Words

- **Fn6 is Finding Scientific Answers To Legal Questions**

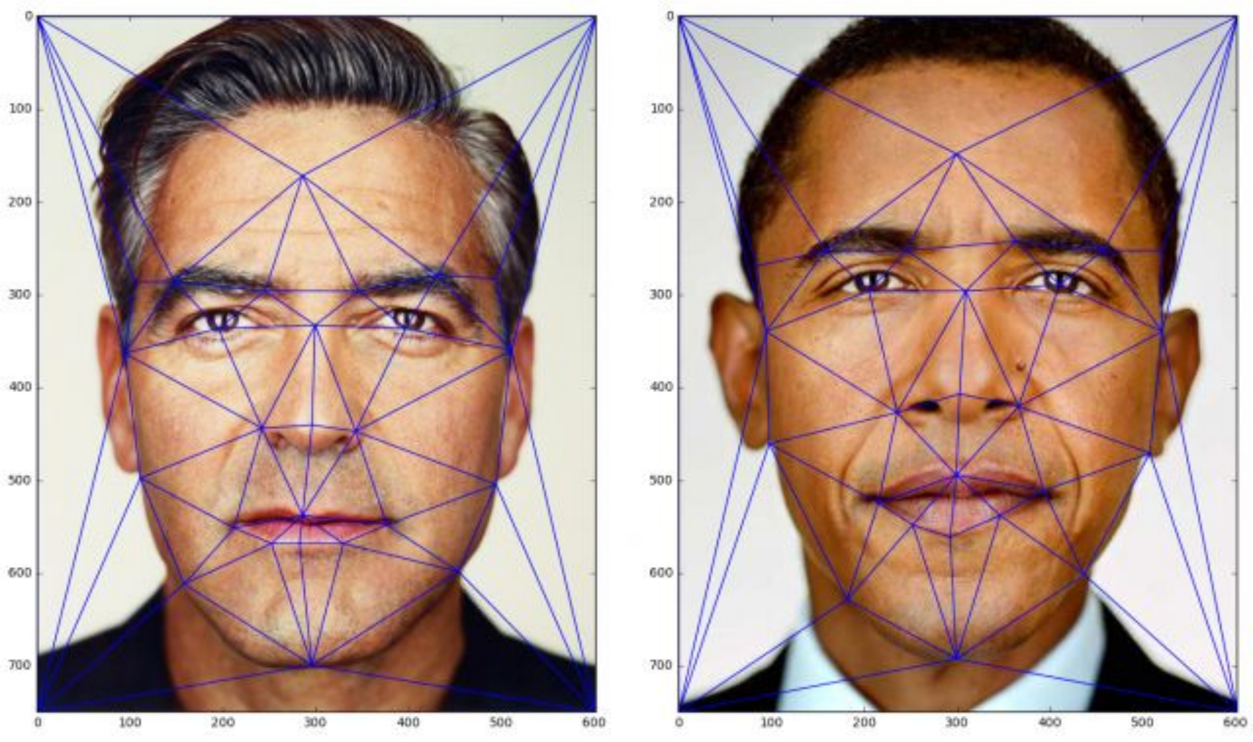
- Need Of Computer Forensics

- To ensure the integrity of the computer system
- To produce evidence in court and help assisting cyber crime.
- To respond on high tech offenses

- Types Of Cyber Crimes

- Image morphing
- Virus Exfiltration
- Identity Theft

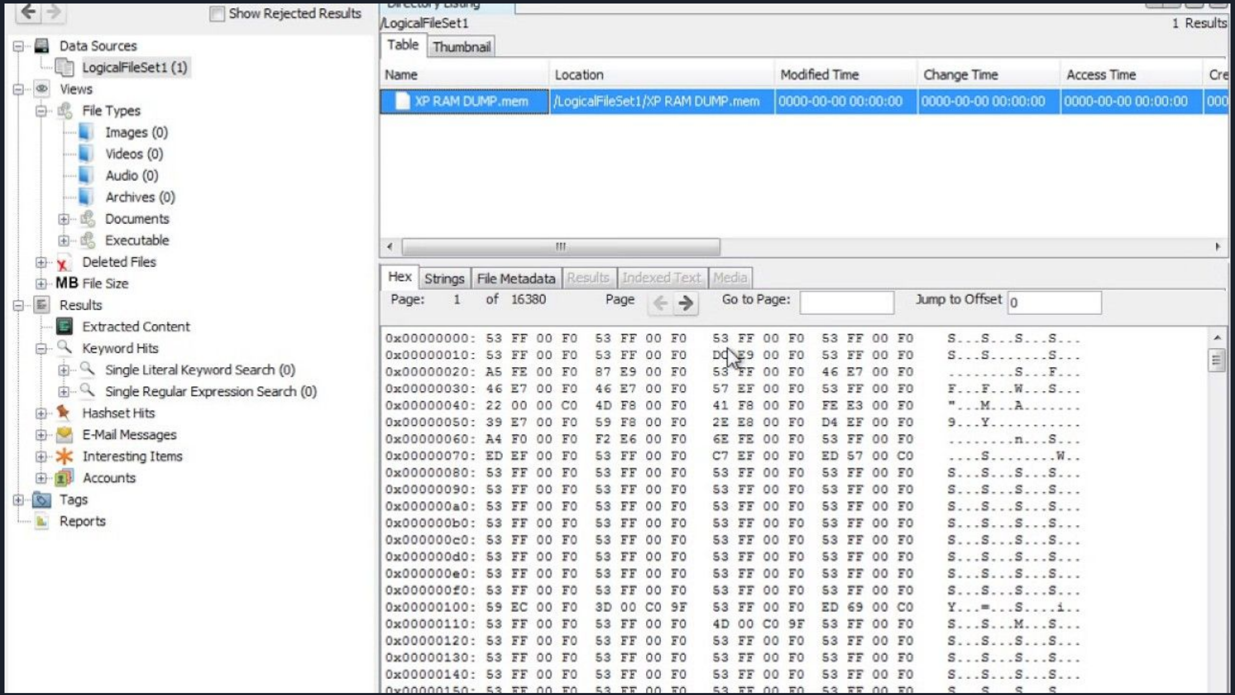
- Image Morphing :



- Tools Used **In Forensics** :

- Disk imaging software
- Hashing softwares
- Data recovery softwares
- Password Cracking Softwares
- Encryption Decoding Softwares

- Autopsy



/LogicalFileSet1 1 Results

Name	Location	Modified Time	Change Time	Access Time	Cre
XP RAM DUMP.mem	/LogicalFileSet1/XP RAM DUMP.mem	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	000

Page: 1 of 16380

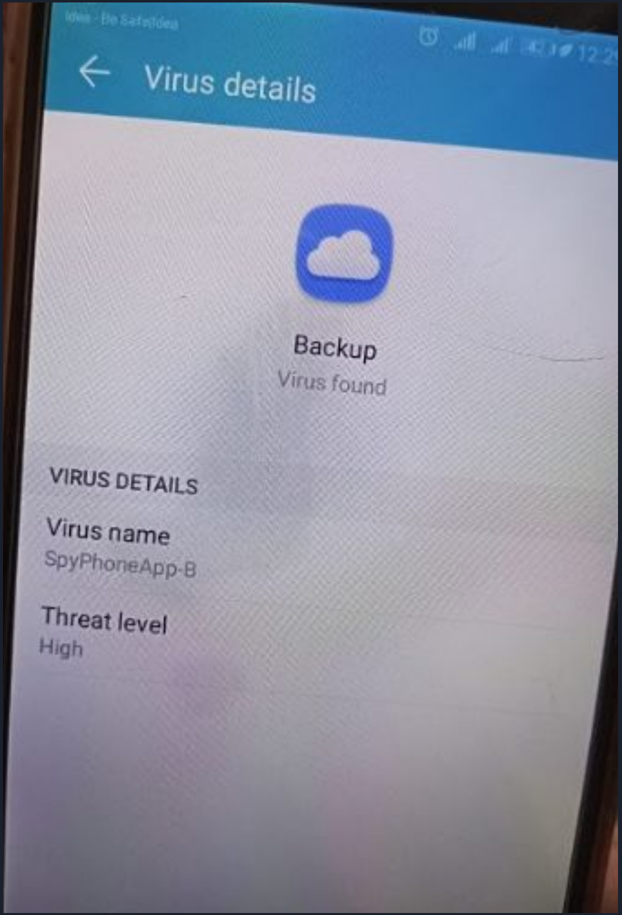
Jump to Offset 0

```
0x00000000: 53 FF 00 F0  53 FF 00 F0   53 FF 00 F0  53 FF 00 F0    S...S...S...S...
0x00000010: 53 FF 00 F0  53 FF 00 F0   DC E9 00 F0  53 FF 00 F0    S...S.......S...
0x00000020: A5 FE 00 F0  87 E9 00 F0   53 FF 00 F0  46 E7 00 F0    ........S...F...
0x00000030: 46 E7 00 F0  46 E7 00 F0   57 EF 00 F0  53 FF 00 F0    F...F...W...S...
0x00000040: 22 00 00 C0  4D F8 00 F0   41 F8 00 F0  FE E3 00 F0    "...M...A.......
0x00000050: 39 E7 00 F0  59 F8 00 F0   2E E8 00 F0  D4 EF 00 F0    9...Y...........
0x00000060: A4 F0 00 F0  F2 E6 00 F0   6E FE 00 F0  53 FF 00 F0    ........n...S...
0x00000070: ED EF 00 F0  53 FF 00 F0   C7 EF 00 F0  ED 57 00 C0    ....S.......W..
0x00000080: 53 FF 00 F0  53 FF 00 F0   53 FF 00 F0  53 FF 00 F0    S...S...S...S...
0x00000090: 53 FF 00 F0  53 FF 00 F0   53 FF 00 F0  53 FF 00 F0    S...S...S...S...
0x000000a0: 53 FF 00 F0  53 FF 00 F0   53 FF 00 F0  53 FF 00 F0    S...S...S...S...
0x000000b0: 53 FF 00 F0  53 FF 00 F0   53 FF 00 F0  53 FF 00 F0    S...S...S...S...
0x000000c0: 53 FF 00 F0  53 FF 00 F0   53 FF 00 F0  53 FF 00 F0    S...S...S...S...
0x000000d0: 53 FF 00 F0  53 FF 00 F0   53 FF 00 F0  53 FF 00 F0    S...S...S...S...
0x000000e0: 53 FF 00 F0  53 FF 00 F0   53 FF 00 F0  53 FF 00 F0    S...S...S...S...
0x000000f0: 53 FF 00 F0  53 FF 00 F0   53 FF 00 F0  53 FF 00 F0    S...S...S...S...
0x00000100: 59 EC 00 F0  3D 00 C0 9F   53 FF 00 F0  ED 69 00 C0    Y...=...S....i..
0x00000110: 53 FF 00 F0  53 FF 00 F0   4D 00 C0 9F  53 FF 00 F0    S...S...M...S...
0x00000120: 53 FF 00 F0  53 FF 00 F0   53 FF 00 F0  53 FF 00 F0    S...S...S...S...
0x00000130: 53 FF 00 F0  53 FF 00 F0   53 FF 00 F0  53 FF 00 F0    S...S...S...S...
0x00000140: 53 FF 00 F0  53 FF 00 F0   53 FF 00 F0  53 FF 00 F0    S...S...S...S...
0x00000150: 53 FF 00 F0  53 FF 00 F0   53 FF 00 F0  53 FF 00 F0    S...S...S...S...
```

Wanna K**now How actual Forensics Looks ?**

Case : Virus Exfiltration Harassment ! & Identity theft

- Identifying Our Vector



Idea - Be Safe|Idea 12:2

Virus details

Backup

Virus found

VIRUS DETAILS

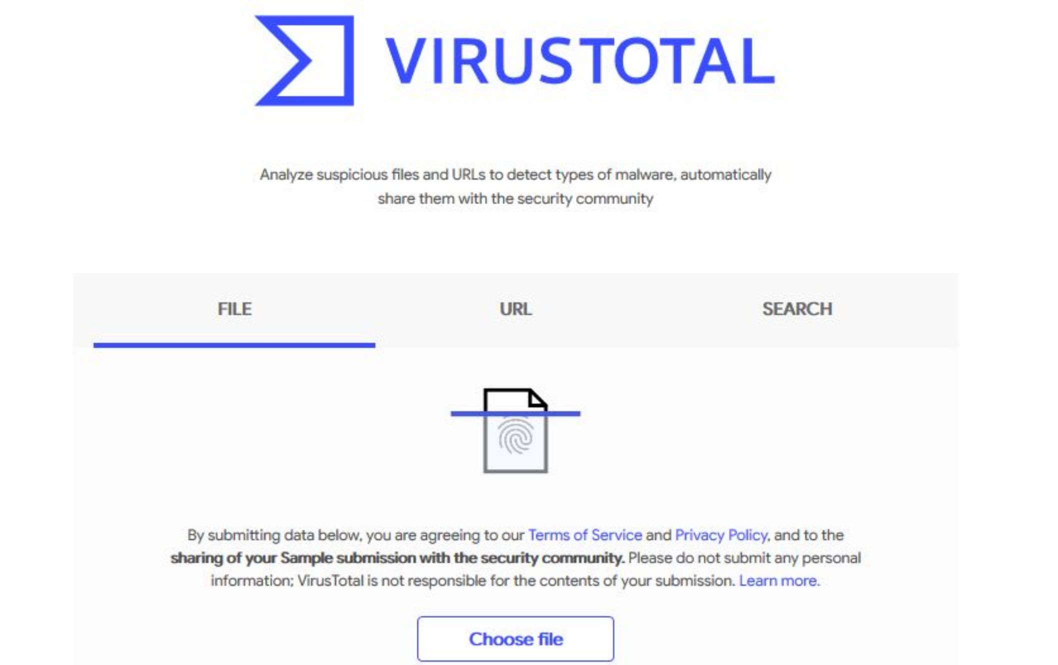
Virus name

SpyPhoneApp-B

Threat level

High

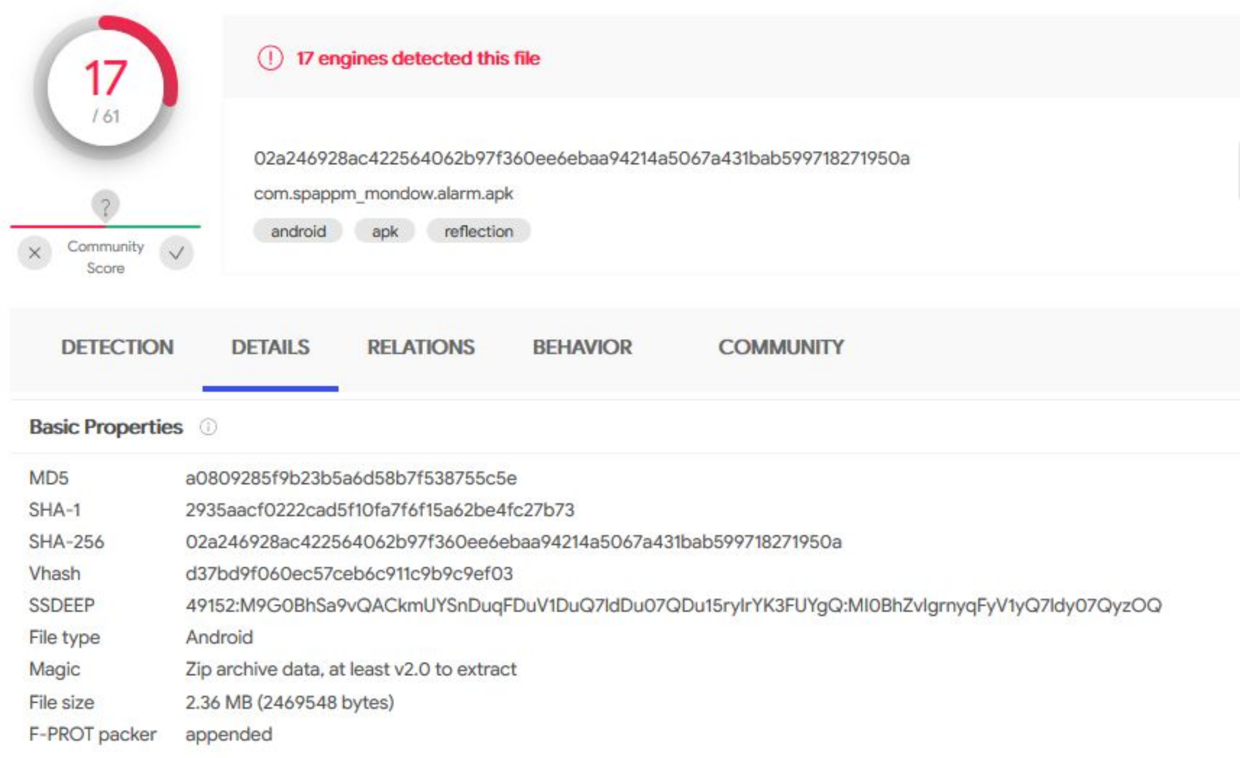
Identifying Our Vector



Analyze suspicious files and URLs to detect types of malware, automatically share them with the security community

By submitting data below, you are agreeing to our Terms of Service and Privacy Policy, and to the **sharing of your Sample submission with the security community.** Please do not submit any personal information; VirusTotal is not responsible for the contents of your submission. Learn more.

Identifying Our Vector



17 engines detected this file

02a246928ac422564062b97f360ee6ebaa94214a5067a431bab599718271950a

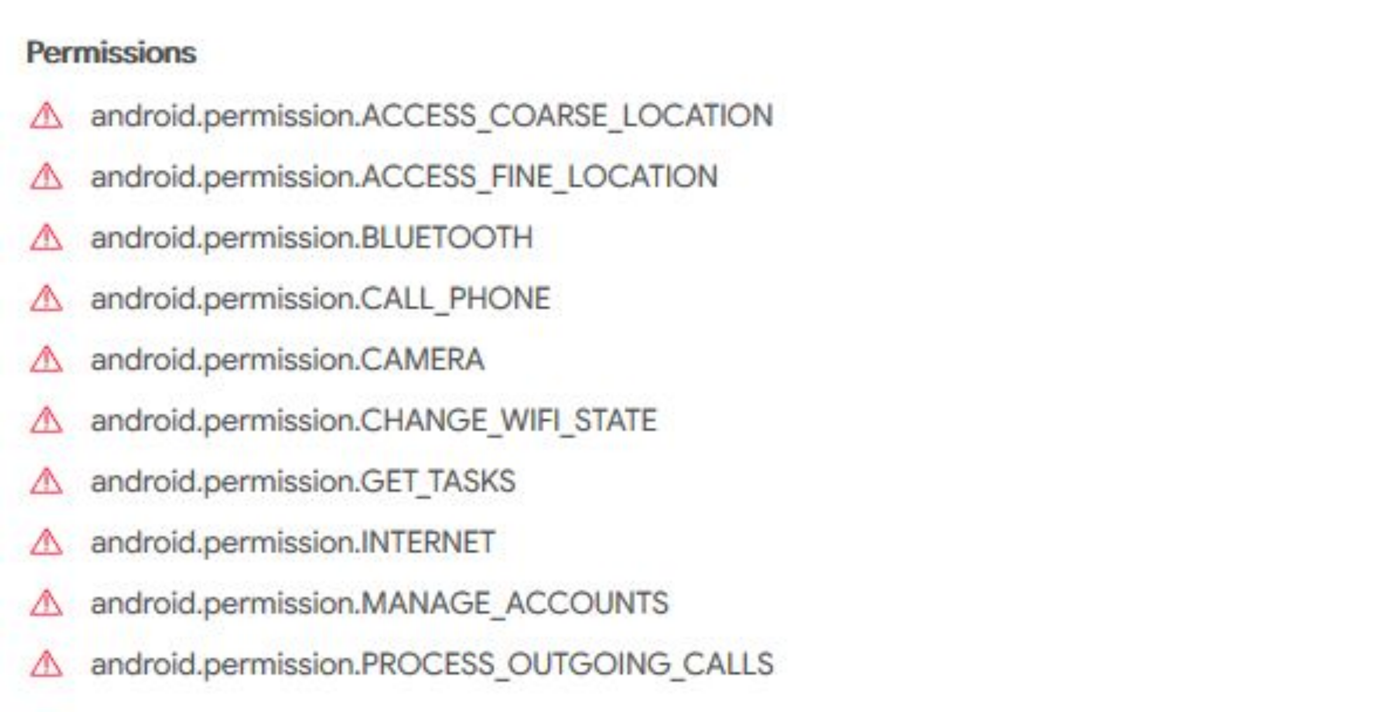
com.spappm_mondow.alarm.apk

android apk reflection

Basic Properties

MD5	a0809285f9b23b5a6d58b7f538755c5e
SHA-1	2935aacf0222cad5f10fa7f6f15a62be4fc27b73
SHA-256	02a246928ac422564062b97f360ee6ebaa94214a5067a431bab599718271950a
Vhash	d37bd9f060ec57ceb6c911c9b9c9ef03
SSDEEP	49152:M9G0BhSa9vQACkmUYSnDuqFDuV1DuQ7ldDu07QDu15rylrYK3FUYgQ:MI0BhZvlgrnyqFyV1yQ7ldy07QyzOQ
File type	Android
Magic	Zip archive data, at least v2.0 to extract
File size	2.36 MB (2469548 bytes)
F-PROT packer	appended

- Exploited Permissions



Permissions

⚠ android.permission.ACCESS_COARSE_LOCATION

⚠ android.permission.ACCESS_FINE_LOCATION

⚠ android.permission.BLUETOOTH

⚠ android.permission.CALL_PHONE

⚠ android.permission.CAMERA

⚠ android.permission.CHANGE_WIFI_STATE

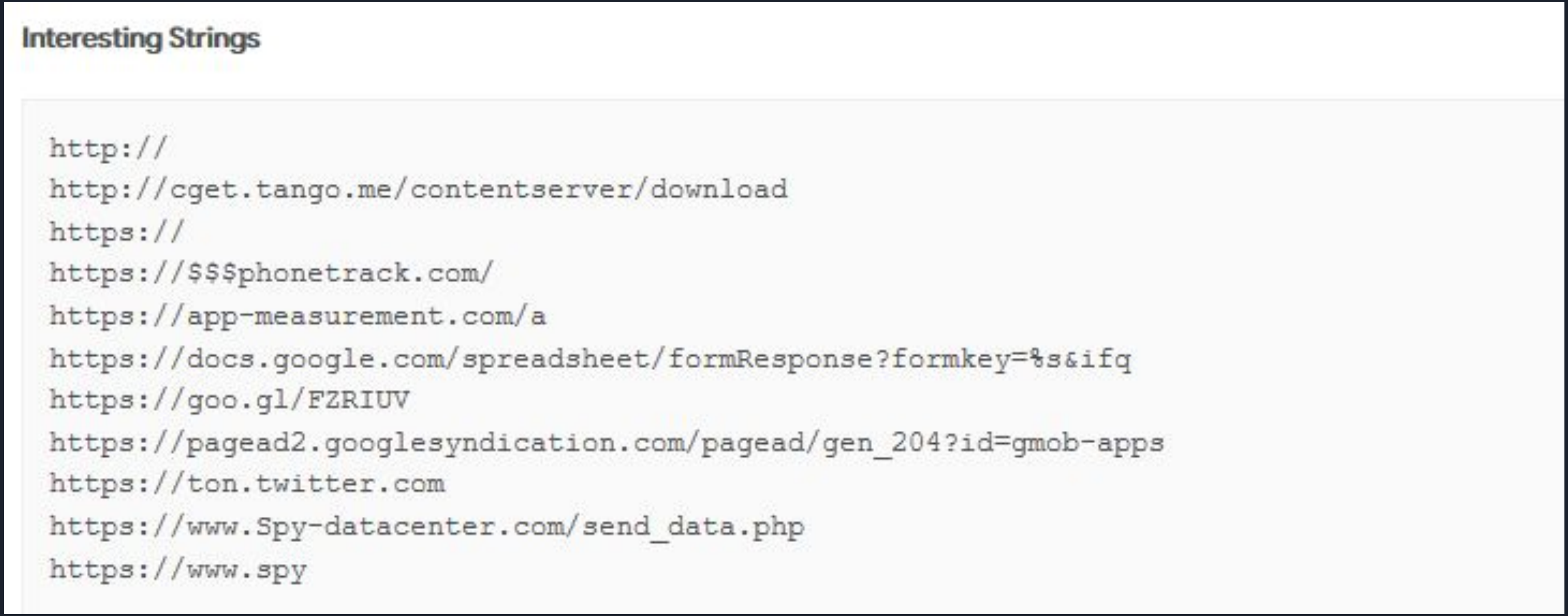
⚠ android.permission.GET_TASKS

⚠ android.permission.INTERNET

⚠ android.permission.MANAGE_ACCOUNTS

⚠ android.permission.PROCESS_OUTGOING_CALLS

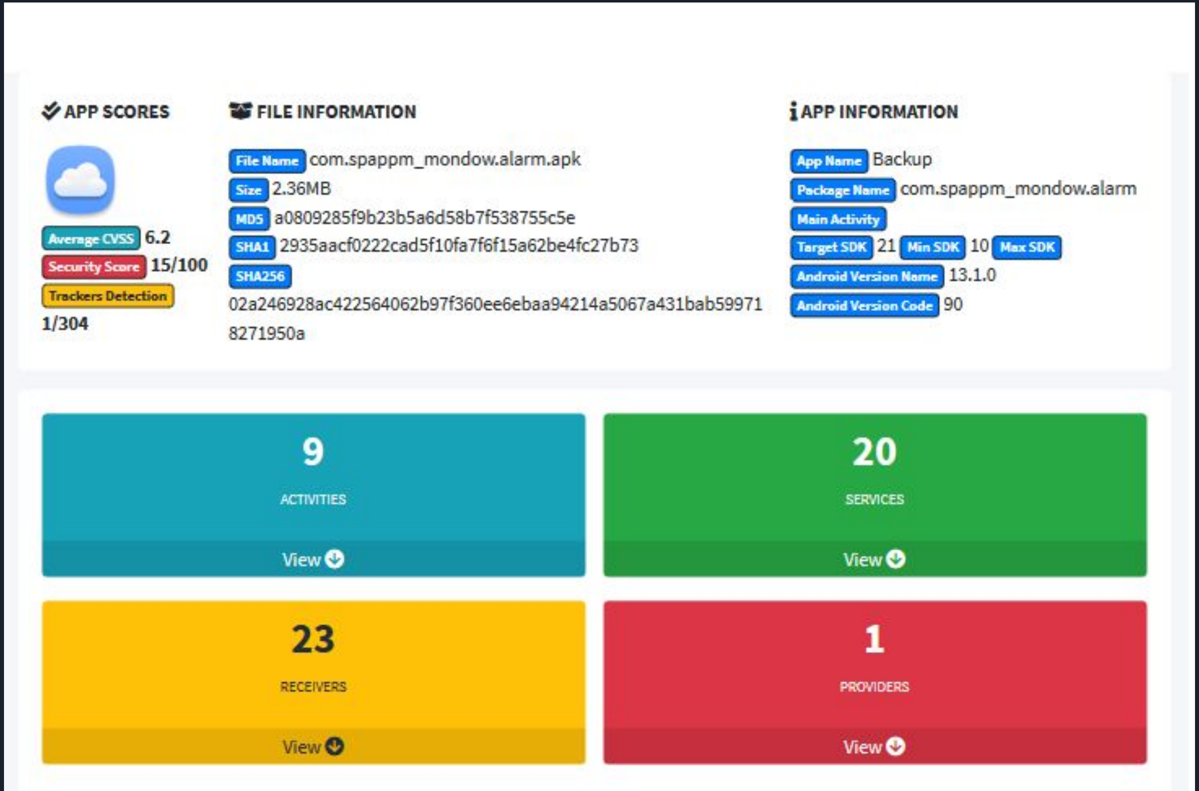
- Juicy Strings



Interesting Strings

```
http://
http://cget.tango.me/contentserver/download
https://
https://$$$phonetrack.com/
https://app-measurement.com/a
https://docs.google.com/spreadsheet/formResponse?formkey=%s&ifq
https://goo.gl/FZRIUV
https://pagead2.googlesyndication.com/pagead/gen_204?id=gmob-apps
https://ton.twitter.com
https://www.Spy-datacenter.com/send_data.php
https://www.spy
```

- Static Analysis Of Application



APP SCORES

Average CVSS 6.2
Security Score 15/100
Trackers Detection 1/304

FILE INFORMATION

File Name com.spappm_mondow.alarm.apk
Size 2.36MB
MD5 a0809285f9b23b5a6d58b7f538755c5e
SHA1 2935aacf0222cad5f10fa7f6f15a62be4fc27b73
SHA256 02a246928ac422564062b97f360ee6ebaa94214a5067a431bab59971 8271950a

APP INFORMATION

App Name Backup
Package Name com.spappm_mondow.alarm
Main Activity
Target SDK 21 Min SDK 10 Max SDK
Android Version Name 13.1.0
Android Version Code 90

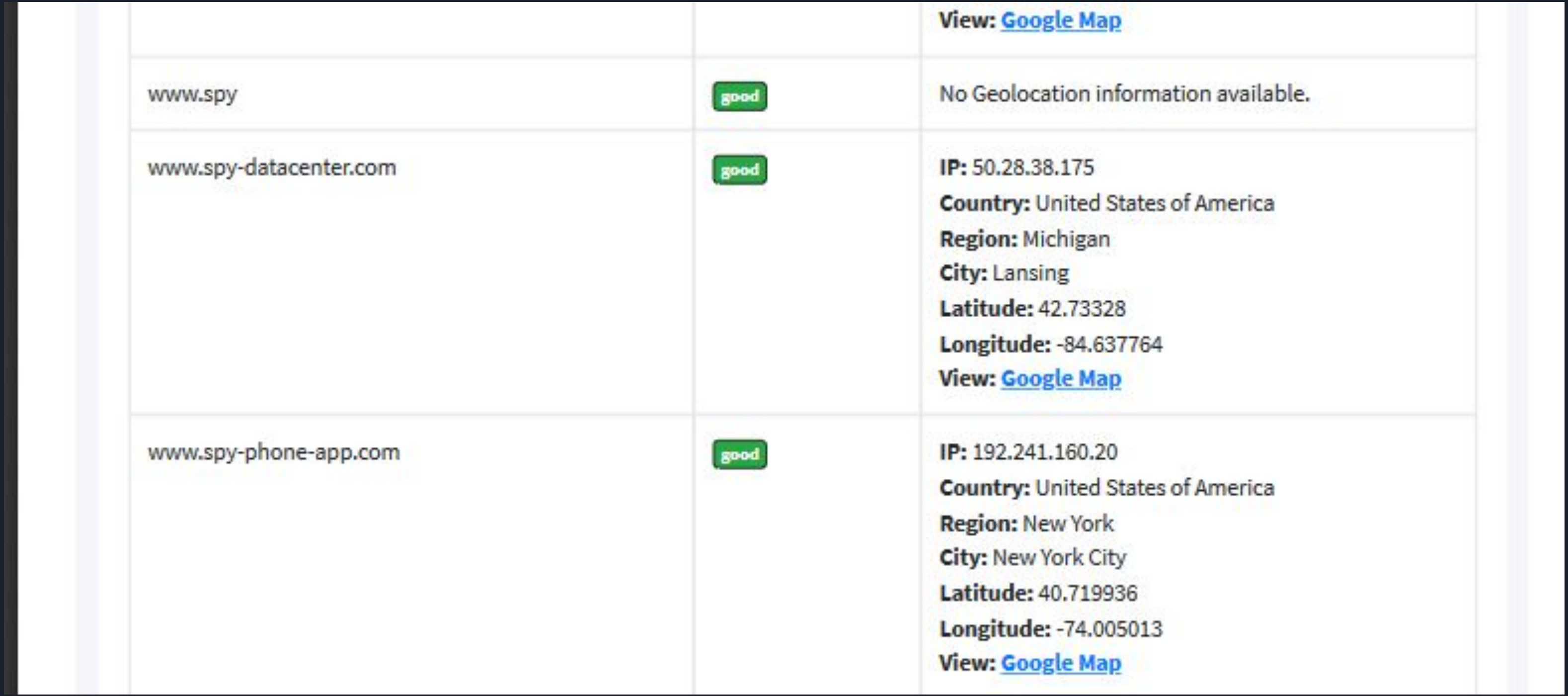
9 ACTIVITIES View

20 SERVICES View

23 RECEIVERS View

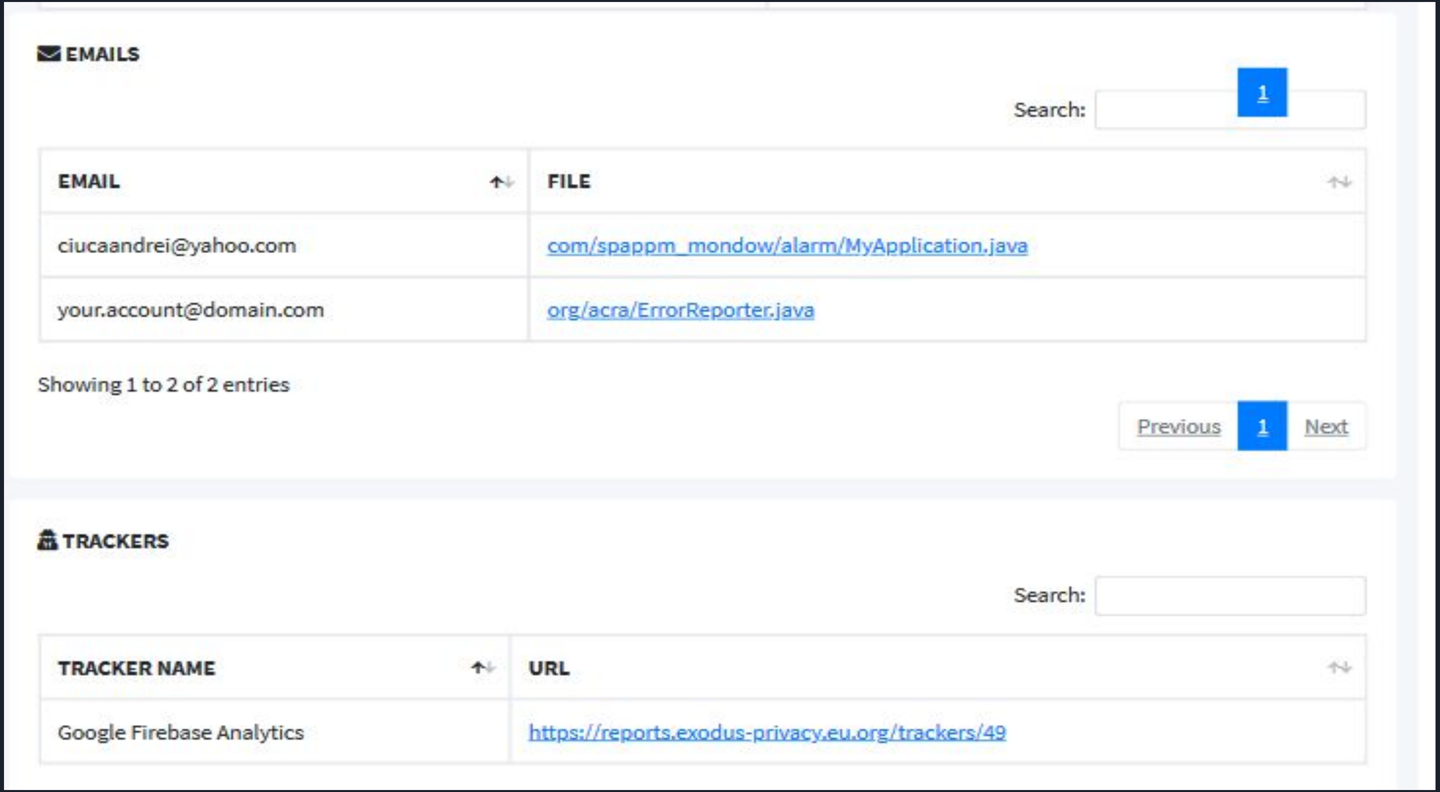
1 PROVIDERS View

- Tracing Back The Attacker



		View: Google Map
www.spy	good	No Geolocation information available.
www.spy-datacenter.com	good	**IP:** 50.28.38.175 **Country:** United States of America **Region:** Michigan **City:** Lansing **Latitude:** 42.73328 **Longitude:** -84.637764 **View:** Google Map
www.spy-phone-app.com	good	**IP:** 192.241.160.20 **Country:** United States of America **Region:** New York **City:** New York City **Latitude:** 40.719936 **Longitude:** -74.005013 **View:** Google Map

- Tracing Back The Attacker



EMAILS

Search: 1

EMAIL	FILE
ciucaandrei@yahoo.com	com/spappm_mondow/alarm/MyApplication.java
your.account@domain.com	org/acra/ErrorReporter.java

Showing 1 to 2 of 2 entries

TRACKERS

Search:

TRACKER NAME	URL
Google Firebase Analytics	https://reports.exodus-privacy.eu.org/trackers/49

- Further **Process Is Quite Confidential** ;)

Key Areas Of Knowledge :

- Internet , Networking & Peripheral Devices
- Mobile Forensics Investigations
- Malwares & Programming
- Forensics & Anti-Forensics Techniques
- Open Source Intelligence

Process Of Digital Investigation :

1. **I:** Identification (Identifying the vector)
2. **P:** Preservation (Preserving Vector for further proceeding)
3. **A:** Acquisition and Analysis (Creating Disk Image)
4. **D:** Documentation and Reporting (Maintaining Chain)

Who Uses Computer Forensics !

- Criminal Prosecutors
- Civil Litigations
- Law Enforcement Officials
- Private Corporations

Future **Of Forensics In Upcoming Time :**

Key Areas To Focus

Future Of Forensics :

- Drone Forensics : Dealing With Surveillance Drone
- IOT Forensics : Deals With Devices Paired Over Internet
- Embedded Devices Forensics
- Remote Forensics : Turning It Possible To Perform Forensics Remotely