An Experimental Investigation on the Efficiency of Spy Tools: A Comparative Analysis

Sakshi R. Thakre
PG Scholar
Department of Digital & Cyber Forensics
Government Institute of forensic Science
Chhatrapati sambhajinagar,India

Shobha K. Bawiskar*
Assistant Professor
Department of Digital & Cyber Forensics
Government Institute of forensic Science
Chhatrapati sambhajinagar,India

ABSTRACT:

This paper presents the methodological framework and comparative analysis of the spyware applications available on the Google Play store based on the parameters Stealth & Evasion, Privacy and Detectability. The spyware applications are invading privacy of an individual by its covert nature and challenging the digital forensic investigation procedures. These types of apps are used for the parental monitoring, abusing partners and corporate spies this make it used for the illegal purpose to monitor others without their consent and breaching their privacy. The literature review concluded that due to the lack of standardized methodology for the analysis which leads to the loss of data during investigation, inappropriate results and challenging courtroom procedure. The primary aim of this study is to fulfil the gap in the investigation procedure and comparatively analyzing applications based on their behavior. It provides the multi-layered methodology involving Observational Analysis, Static Analysis and Overall risk assessment (based on scoring model). The purpose of this study is to provide the standardized methodology for the forensic analysis of spy applications and comparatively determining the risk level of an application.

KEYWORDS: ***Forensic Framework, spy applications, Forensic analysis, cybercrimes, Android.***

INTRODUCTION:

A spyware software program used to secretly monitor, track, or record a person's activities and data without their knowledge or consent. Spyware tools are categorized into three main parts-A) Audio B) Video C) GPS Trackers. These devices become a dangerous tool for stalkers, abusive partners, and corporate spies. These apps are available on the commercial platforms with east to use functionality without technical knowledge, this feature make this apps used for the illegitimate purposes.

Background of the study

The widespread use of smartphones is increasing day by day mainly which is based on Android Operating system. This rapid usage of mobile phones are vulnerable to the malicious surveillance by using spy software applications which are able to monitor, record, or transmit information to the unauthorised party which leads to the data privacy concerns of the users. The secret monitoring of an individual activity can leads to the privacy violation and violation of fundamental rights of an individual.

The covert nature of this type of spyware applications is vulnerable for the digital investigation process. It acts like the blackbox for the experts in the investigation. The literature review showcases that there is no standard procedure when this type of suspicious apps found. This research mainly focuses on step-by-step guide for the analysis of spyware apps which leads to the ease in the criminal investigation and admissibility in the court of law.

It is mainly focused on the older version of the android mobile devices because it lacks modern security features and used by the millions of people. This research mainly focuses on the mobile phone **"Oppo A3S"** and provide a three-step procedure based on the:

1.Observational Findings
2.Static Analysis
3. Risk score Assessment

The primary aim of this study id to establish a repeatable, three step methodology that undergoes behavioural analysis based on observations, Static analysis using the different technical tools and Quantitative analysis by the scoring parameters. The objective includes designing the framework and define the criteria for the analysis and experimenting on selected five app and demonstrating its risk level and threats.

Significance of the study

This study contributes to the Digital investigation procedure by designing the tiered methodology for the forensic analysis of suspicious apps. Step-by-step guidance for the forensic analyst makes time consuming and trial and error procedure while investigation. The other main issue enlighten here is the main focus on the outdated Android version device basically running on Android 8.1 which is vulnerable to the security and privacy threats and highlights the risk faced by the users.

This study provides the insights on the facts that:

1. Antivirus is inoperable to find this type of apps.
2. It highlights that the spyware applications are disguising the users instead of hiding them which looks like legitimate apps.

AIM:

To provide the standardized framework/Standard Operating Procedure for the forensic analysis of the spyware applications

OBJECTIVE:

1. To provide the standardized methodological framework for the forensic application of spyware apps.
2. To comparatively analyze the five selected spyware applications based on parameters like Stealth & Evasion, Privacy and Detectability.
3. To determine the risk level of spy apps based on the scoring model.

RESEARCH METHODOLOGY(case-study)

Research Design

This study adopts a qualitative and behavioural approach for the forensic analysis of the spyware applications. It aims at designing the multi-tiered methodology which involves the functionality and behavioural analysis, followed by analysis with the open-source software tools and finally identifying the risk level based on the scoring model. By following this procedure, it undergoes the comparative analysis of the selected spyware applications.

Requirenents-

1. **Hardware**

   Sample device: Oppo A3s mobile device with Android version 8.1

Fig 1: Oppo A3s with Android version 8.1.

   Test Environment: Laptop with windows 11

2. **Software.**

   Open-source tools:

1. MobSF (**Mobile Security Framework)**
   a. Docker Desktop (supporting utilities)
   b. Android Debug Bridge (ADB) (supporting utilities)
2. VirusTotal
3. APK Analyzer

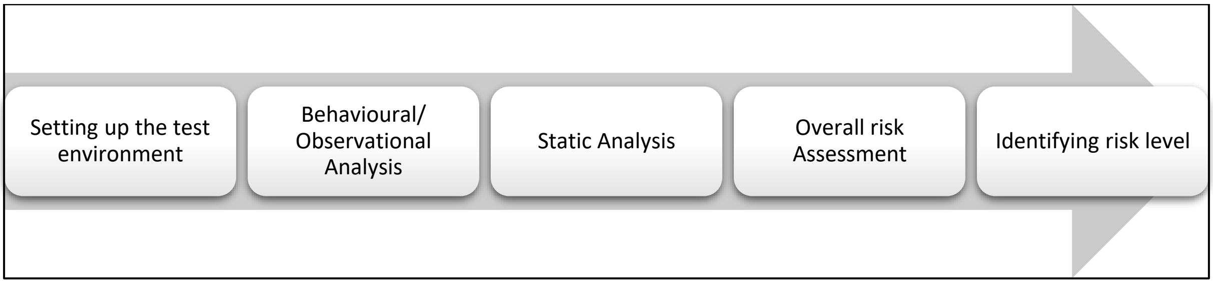
Spyware Applications:

The spy apps were selected from the Google play store based on the rating which is above the **4.5** * and mainly the apps which is providing freeware services and providing background services with audio and video functionality.

Sr.no	Apps	App Icon
1	XS Camera	
2	Third Eye Hidden Camera Record	

Table1. Selected Spyware Applications.

Methodology:



Setting up the test environment → Behavioural/ Observational Analysis → Static Analysis → Overall risk Assessment → Identifying risk level

Fig 2: Methodology Flowchart

1. **Setting up the test environment:**
   a. For setting up the workstation: The workstation was fully setup downloading the open-source software and all the required supporting utilities like ADB and Docker Desktop.
   b. For setting up the sample device: The phone was factory reset and burner account was created for downloading the apps and ensure that the phone is in clear state i.e. there is no contacts and SIM card inserted in the mobile phone to secure the PII.

2. **Behavioural/ Observational Analysis:**
   a. Firstly, after installation the app's configuration was manually changed and undergoes the observational analysis by the following criteria:
      i. **Icon status:** The apps was observed for the icon stealth in which it determines whether the icon was "Hide", "Disguised" and not stealth referred as "None".
      ii. **Notification stealth:** Secondly, the recording was started in the background to observed whether the notification was displaying on the screen or it is completely stealth.
      iii. **Battery consumption:** For these criteria, the standardized 30-minute recording approach is performed for all the apps and navigated to the Settings Battery Power usage. This shows the battery consumption of all the apps percentage wise and the result was written for "High", "Medium", "Low".
      iv. **Background service:** Observe the app while recording whether it is running in the background and based on observation mention it as "Yes" or "No".

3. **Static Analysis:**

a. For MobSF (Mobile Security Framework):

i. Open the Docker Desktop and wait for engine to start.
ii. Open the command prompt with the "Administrative" permission.
iii. Run the command "docker run -it --rm -p 8000:8000 -e "MOBSF_DISABLE_LOGIN=true" opensecurity/mobile-security-framework-mobsf" wait for the process to complete.
iv. Open the web browser and type http://localhost:8000/login/?next=/ or localhost:8000 the login window will appear type the username and password both as "mobSF".
v. The mobSF main window will appear , Click on "Upload & Analyze". Choose the desired apk file (here, Third eye Hidden Camera Record was uploaded followed by all other five apps). Wait for the analysis process to complete.
vi. The mobSF report was generated save it in the PDF format.

The criteria analysed using mobSF report as follows:

i. **Non-essential permission:** The apps was analysed for accessing the non-essential permission which is not required for the app's core functionality except audio, video and storge permission. By analysing the mobSF report all the non-essential permission was listed.
ii. **Number of Trackers found:** The report mentions the trackers found while analysing the app the number was noted.
iii. **Export PII to third party:** Form the Trackers section in the Mobsf report, it shows the categories of the trackers which is stealing the PII of the users. For this, the results mentions the Yes or No along with trackers category.
iv. **Mobsf score:** The report mention the MobSF security score , in the result the score was noted

b. For Virustotal analyzer:

i. Open the webrowser and type "Virustotal" and press Enter.
ii. The main window will appear. Choose "File" and Uploaded the apk file one by one.
iii. Note the observatins.

The criteria analysed using mobSF report as follows:

i. **Virustotal Detection rate**: After analysing the app, it provides the detection rate for the app. Note this for the observation table and look for the permissions, receivers, supporters sections for the non-essential permission analysis.

c. For APK Analyzer:

i. Install the APK Analyzer on the mobile device or on an Virtual Android environment.
ii. Open the app and select the app one by one.
iii. Note the observations For the used permissions and basic information about the app, services providing, content providers.

The criteria analysed using mobSF report as follows:

i. Non-essential permission
ii. Background service.

4. Overall risk assessment:

The risk assessment for each app is based on the scoring model as follows:

Criteria	Score			
	0	1	2	3
Icon Status	None	Disguised	Hidden	-
Notification stealth	No	Vague/ Blinking	Yes	-
Non-essential permission	(Yes) 0	(Yes) 1 -3	4 and more	-
Export PII to third party	(Yes) 0	(Yes) 1 -3	4 and more	-
Number of trackers found	0	1to 3	3-5	6 and more
Background service	No	Yes	-	-
Battery Consumption	Very High	High	Medium	Low
Mobsf score	<40	<60	>60	-
Virustotal detection rate	0	1-7	8 and more	-

Table2. Scoring model for determining risk score.

Scoring Criteria:

Table 2. provides the scoring model for each criteria. For icon status, the assignment of the scores is 0 for None means the app does not provide the facility to hide icon, 1 for Disguised icon and 2 for Hidden icon. For notification stealth the scoring will be 0 for No (means the notification is clearly visible on the screen, 1 for vague/blinking and 2 for completely hidden notification. Similarly, for Non-essential permission, the scoring will be based on the number of non-essential permission if it is 0 then score also 0 if it falls between 1-3 then 1 and if it is 4 or more then it is 2.The scoring for Export PII to third party is similar to non-essential permission but this is based on the number of trackers category. Moreover for Number of trackers , if trackers found is 0 then it is 0 , if 1-3 then it is 1, if it falls between 3-5 then it is 2 and 3 for 6 and more. Scoring for background service criteria is 0 for No and 1 for Yes. The scoring for Battery consumption is reverse means if the battery usage is very high then it is 0, 1 for High, 2 for Medium and 3 for Low. The score foe mobsf score will assign as 0 if it is less than 40, 1 if it is less than 60 and 2 if it is greater than 60. For virustotal detection rate the scoring will be if it is 0 then 0, if it is between 1-7 then it is 1 and if it is 8 and more then it is 2. After assigning the score to each criteria, sum all the points and result should be mentioned in the Overall risk score.

5. **Identifying Risk level:**

   The risk level for the particular app can be determine using Overall risk score and the risk level identification is based on the scoring parameter again which is as follows:

   i. 0-5- Low risk
   ii. 6-10- Medium risk
   iii. 11 and more- High risk

   If the overall risk score is between 0-5 it is identified as Low risky app, if score fall between 6-10 then it is determined as Medium risk and if score is 11 or more then it is High risk.

RESULT:

This section presents the result formulated by following the multi-layered methodology on the selected five apps by using sample mobile device “Oppo A3s”. It involves the detailed results based on the observational findings, static analysis and overall risk assessment.

Parameter	Criteria	Apps	
		App1: XS Camera	App2: Third Eye Hidden Camera Record
Stealth & Evasion	Icon Status	Disguised	None
	Notification stealth	Blinking (with all permissions allowed) Note: Yes when audio permission is denied	Blinking (with all permissions allowed) Note: Yes when audio permission is denied
Privacy	Non-essential permission	Yes SYSTEM_ALERT_ WINDOW, AD_ID, ACCESS_ADSERVICES_ ATTRIBUTION, ACCESS_ADSERVICES_AD_ID	Yes SYSTEM_ALERT_WINDOW, AD_ID, ACCESS_ADSERVICES_AD_ ID, ACCESS_ADSERVICES_ ATTRIBUTION, ACCESS_ADSERVICES_ TOPICS
	Export PII to third party	Yes (Advertisement, Identification, Profiling, Analytics, Crash reporting)	Yes (Advertisement, Identification, Profiling, Analytics, Crash reporting)
	Number of trackers found	4	9
	Background service	Yes	Yes
	Battery Consumption	Medium	Medium

Detectability	Mobsf score	45/100	50/100
	Virustotal detection rate	0/64	0/53

Table 3. presented the findings based on the observational analysis, static analysis for the parameters Stealth & Evasion, Privacy, Detectability and used for scoring model to determine overall risk score and identifying risk level.

Parameter	Criteria	Apps	
		App1: XS Camera	App2: Third Eye Hidden Camera REcord
Stealth & Evasion	Icon Status	1	0
	Notification stealth	1	1
Privacy	Non-essential permission	2	2
	Export PII to third party	2	2
	Number of trackers found	2	3
	Background service	1	1
Detectability	Battery Consumption	2	2
	Mobsf score	1	1
	Virustotal detection rate	0	0
Risk evaluation	Total risk score	12	12
	Overall risk assessment	High	High

Table 4. presented the score given to each criteria based on the scoring model and assessed the risk level based on the overall risk score.

OBSERVATIONS: MobSF Report

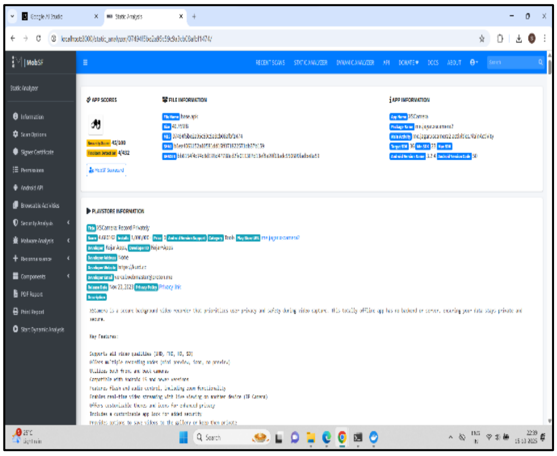


Fig3: MobSF report Of XS Camera

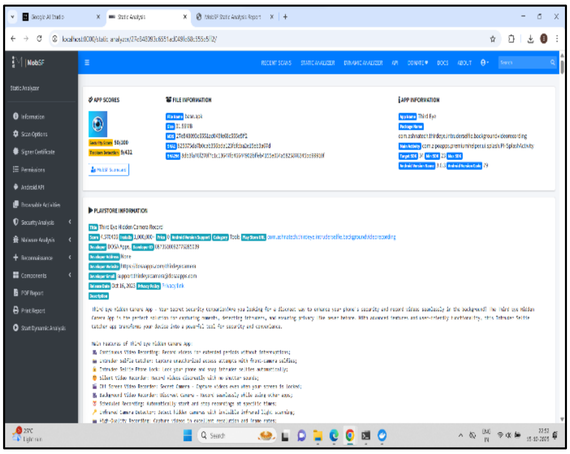


Fig4: MobSF report Of Third Eye Hidden Camera Record

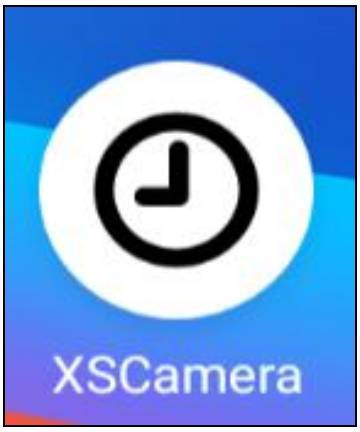
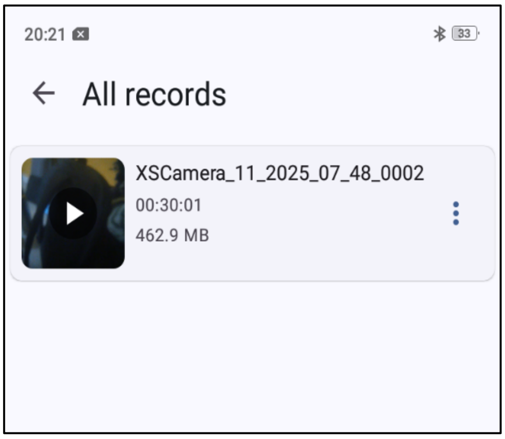


Fig5: Disguised icon of XS Camera looks like Clock.



20:21

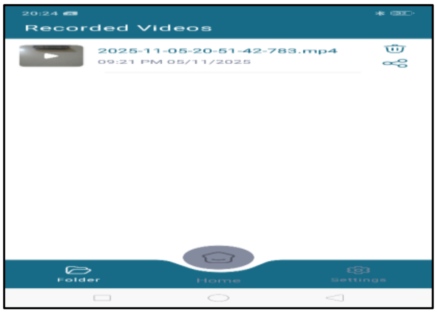
All records

XSCamera_11_2025_07_48_0002

00:30:01

462.9 MB

Fig6: Saved recording in XS camera



20:24

Recorded Videos

2025-11-05-20-51-42-783.mp4

09:21 PM 05/11/2025

Fig7: Saved recording of Third Eye Hidden Camera Record

DISCUSSION:

This article provides the detailed interpretation of the results of each apps and mentioned all the findings based on the observational analysis, static analysis and overall risk assessment.

Key Findings:

1. **XS Camera:**

This application shows the icon status disguised (e.g. Calculator, Telegram) means the user can modify the appearance of an app to make is less detectable. Notification state is shown as blinking when all permission is allowed and if the audio permission is denied then the notification completely hides on the screen. With the required permission this apps ask for the non-essential permission which can access the PII of an individual through the trackers which includes the Advertisement, Identification, Profiling, Analytics, and crash reporting. The 4 trackers was found in the MobSF report. It provides the background recording service. The battery consumption is Medium means the app may be less detectable having the Mobsf security score 45/100 mentioning the Medium risk. Virustotal detection rate is 0/64 which means that no vendors out of 67 marked it as malicious app. The overall risk score is 12 which identified it as “High risk”.

2. **Third Eye Hidden Camera Record:**

Third Eye Hidden Camera Record does not provide the facility to hide the app icon. The notification state of an app is blinking with allowing all the permissions but when audio permission is denied the notification completely hides on the background screen. It requests for the non-essential permissions like SYSTEM_ALERT_WINDOW ,AD_ID,ACCESS_ADSERVICES_AD_ID,ACCESS_ADSERVICES_ATTRIBUTION,ACCESS_ADSERVIES _TOPICS which is dangerous for the Android. It export the PII through the various trackers category involving Advertisement, Identification, Profiling, Analytics, Crash reporting. The trackers found is 9 which is higher than the other apps which makes it more risky. It also provides the background service. The battery consumption is Medium which is another parameter to make this app less detectable. The mobSF security score is 50/100 with Medium risk. The total risk score is 12 with “High Risk”.

CONCLUSION:

This section concluded all the findings of this study and also mentioned the future work for the further study in this domain.

This study addresses the lack of standardized methodology for the forensic analysis of the spyware applications. It provides the repeatable, reversible and standardized procedure in the three-layered methodology involving

Observational Analysis, Static analysis, and Overall risk Assessment. This provides the solution to analyze the apps which is in the grey area. This framework was applied to the selected spy applications available on the Google Play Store platform.

From the discussion it is concluded that the XS camera and Third Eye Hidden Camera Record falls under the "High risk' level for the risk assessment". The **Third Eye Hidden Camera** is **very risky** as compared to XS Camera because it access more non-essential permissions with highest number of trackers and also the battery usage is medium means it is less detectable and possess highest risk score . Moreover, **the second risky app** is considered as **XS Camera** which shows the disguised icon like various legitimate app and give options to manually change the appearance of the app and also has the higher non-essential permission access with second highest number of trackers and shows the total risk score as 12 which is similar to the Third Eye Hidden Camera Record with Medium battery usage which make it less dangerous than the first.

Risk for app based on Stealth & Evasion

XS Camera > Third Eye Hidden Camera Record.

Risk for app based on Privacy

Third Eye Hidden Camera Record > XS Camera

Risk for app based on Detectability:

Third Eye Hidden Camera Record = XS Camera

FUTURE WORK:

1. Analysis of the other spy application except selected applications
2. Analysis on the modern Operating system of Android
3. Detection techniques for the spy applications
4. Analysis of the Hardware COTS Devices

References:

1. Liu, E., Rao, S., Havron, S., Ho, G., Savage, S., Voelker, G. M., & McCoy, D. (2023). No privacy among spies: Assessing the functionality and insecurity of consumer android spyware apps. *Proceedings on Privacy Enhancing Technologies*.
2. Hutchinson, S., & Karabiyik, U. (2019). Forensic analysis of spy applications in android devices.
3. Caruso, A. (2024). *Forensic Analysis of Mobile Spyware: Investigating Security, Vulnerabilities, and Detection Challenges in Android and iOS Platforms* (Doctoral dissertation, Politecnico di Torino).
4. Wanjale, V., Dhapte, A., Morey, S., & Koria, M. N. (2014). AAPS Android Based System for Camera Based Attacks. *International Journal of Emerging Technologies and Engineering (IJETE)*, *1*(10), 2348-8050.
5. Mannan, M., Youssef, A., Mangeard, P., Yu, X., Tejaswi, B., & Pagey, R. (2023). *Privacy analysis of technologies used in intimate partner abuse*. Technical Report. Concordia University, Montreal, CA. Retrieved 2024-02-13 from https://www. priv. gc. ca/en/opc-actions-and-decisions/research/funding-for-privacy-research-and-knowledge-translation/completed-contributions-program-projects/2022-2023/p_202223_11.
6. Conti, M., Rigoni, G., & Toffalini, F. (2020, August). ASAINT: a spy app identification system based on network traffic. In *Proceedings of the 15th International Conference on Availability, Reliability and Security* (pp. 1-8).
7. Chavan, S. A., Goasvi, N. S., Khairnar, J. R., & Kapse, P. S. (2023). Mobile activity monitoring system using Android spy. *International Journal of Innovative Research in Multidisciplinary Physical Sciences*, *11*(3), 1–6. https://www.ijirmps.org
8. Qabalin, M. K., Naser, M., & Alkasassbeh, M. (2022). Android spyware detection using machine learning: A novel dataset. *Sensors*, *22*(15), Article 5765. https://doi.org/10.3390/s22155765
9. Soni, H., Arora, P., & Rajeswari, D. (2020, July). Malicious application detection in android using machine learning. In *2020 International Conference on Communication and Signal Processing (ICCSP)* (pp. 0846-0848). IEEE.
10. Chatterjee, R., Doerfler, P., Orgad, H., Havron, S., Palmer, J., Freed, D., ... & Ristenpart, T. (2018, May). The spyware used in intimate partner violence. In *2018 IEEE Symposium on Security and Privacy (SP)* (pp. 441-458). IEEE.
11. Salih, H. M., & Mohammed, M. S. (2020, April). Spyware injection in android using fake application. In *2020 International Conference on Computer Science and Software Engineering (CSASE)* (pp. 100-105). IEEE.
12. Mohammed, S., & Zargari, S. (2023, October). Comprehensive Analysis of mSpy Within Covert Operations. In *International Conference on Global Security, Safety, and Sustainability* (pp. 383-421). Cham: Springer Nature Switzerland.
13. Saad, M. H., Serageldin, A., & Salama, G. I. (2015, November). Android spyware disease and medication. In *2015 second international conference on information security and cyber forensics (InfoSec)* (pp. 118-125). IEEE.
14. Anwar, Z., & Khan, W. A. (2015). Guess who is listening in to the board meeting: On the use of mobile device applications as roving spy bugs. *Security and Communication Networks*, *8*, 2813–2825. https://doi.org/10.1002/sec.1205.