International Journal of Scientific Research in Computer Science, Engineering and Information Technology
ISSN : 2456-3307 (www.ijsrcseit.com)
doi : https://doi.org/10.32628/CSEIT22836

Optimization in Security of Digital Evidences by Integration of Evidence Integrity Assurance Mechanism (EIAM) Plug-in into the Software Framework of Mobile Forensic Tools with Balanced Use of Antivirus Softwares

Mr. Bhushan M. Manjre*[1], Dr. Krishan Kumar Goyal[2], Dr. Shivani[3]

*[1]Research Scholar, Department of Computer Science and Engineering, Bhagwant University, Ajmer, Rajasthan, India

[2]Dean, Faculty of Computer Application, RBSMTC, Agra, India

[3]Bhagwant University, Ajmer, Rajasthan, India

Article Info
Volume 8, Issue 3
Page Number : 11-19

Publication Issue :
May-June-2022

Article History
Accepted: 01 May 2022
Published: 06 May 2022

ABSTRACT

In today's era, there exists variety of mobile forensic tools both proprietary as well as open source tools and this generation of mobile forensic tools is evolving at a faster pace with new features which mainly focuses on the deep penetration into the mobile handheld to optimize the mobile forensic process and mainly extraction and decoding of mobile artifacts. But a bit less attention is provided towards the integrity of the digital evidence obtained. There are many factors that can alter the data and the use of antivirus software is one of the prominent factors among them. The importance of antivirus software in the machine could not be denied and hence its systematic use if done, will not only save the digital evidence from the malwares but also saves it from the antivirus software itself. The proposed work describes how the EIAM (Evidence Integrity Assurance Mechanism) plug-in handles the antivirus software in a smart optimized way.

Keywords : EIAM (Evidence Integrity Assurance Mechanism), Mobile Forensic Process, Antivirus Software

I. INTRODUCTION

The today's world is witnessing a fast improvement in the technology as far as mobile smartphones are concerned. The vendors of the mobile phones are competing with each other to provide cost effective smart phone that can deliver their customers a feel of mini computers. Almost all digital works can be accomplished nowadays with mobile handhelds and this has attracted the cyber criminals too to achieve their malicious goals either directly or indirectly. The Digital Forensics thus also should also evolve itself in terms of its efficiency. Especially the digital evidence, which proves to be the most vital factor and the final goal of the digital forensics, should be protected in terms of its immutability. The digital evidence has potential threat from the digital threats like viruses, Trojans or any type of malware. To defend these digital threats, the antivirus software is crucial requirement of every computer system. However, the antivirus software, if not managed carefully in digital forensics, can prove to be the obstacle in the efforts of

prevention of alteration of digital evidences. The following proposed work explains the careful management of the antivirus software during the entire cycle of digital forensics so that the fruitful results could be achieved without facing problems from the antivirus software.

II. PROPOSED EVIDENCE INTEGRITY ASSURANCE MECHANISM

The following figure shows the flowchart of the working of EIAM plug-In [5]. The plug-in works with the Digital Forensic software and provides the instructions to the forensic expert regarding the usage of antivirus software during the digital forensic process.

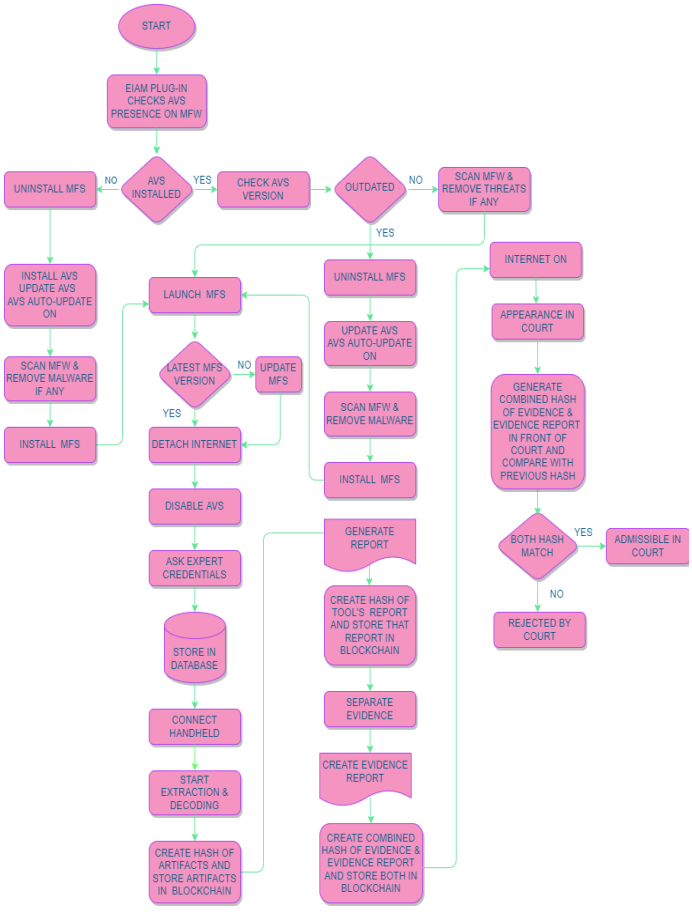


Figure.1: Proposed Evidence Integrity Assurance Mechanism (EIAM) Plug-in Flowchart

Optimal Use of Antivirus Software:

Antivirus software now a day has become inevitable component of the computers and mobile phones also. In the literature studied about the effect of Antivirus Software on the data integrity, especially for the sake of digital evidence, the very first and the only study was proposed by Mohammed I. Al-Saleh et al [1]. The modus operandi of any antivirus software starts from its installation itself. When any antivirus software is installed in a machine, it does distributed installation all over the memory so that it can optimize scan thought all locations in the disk. Also whenever any new system operation is initiated for example copying an exe file from any source, running that executable file , compiling any programming language code, creating any notepad file and writing into it or simply opening any web page, the antivirus has the tendency to check such operations and to verify if any malicious code exists. The scan i.e. On-Access scan is done by checking the data involved in the operation against its database that stores the virus definitions. There is huge impact on RAM artifacts by the antivirus scan [1]. False Positive is the term used for any wrong detection by the antivirus software for the safe software as malicious software. The false positive occurs when there are complications faced by the Antivirus software to categorise the safe and the malicious code. The probability of false positive is little higher when the Antivirus software is newly installed on machine or the system has undergone major software updates. A well-known example of a false positive was when Microsoft Security Essentials tagged Google Chrome as malicious. The software removed Chrome from around 3,000 computers as a result and Google had to run a patched update of their chrome browser for users to download. [4]

It can be difficult to determine whether these are false positives or legitimate threats, and this can result in programs being wrongly deleted, deactivated or blocked by the AV software – and sometimes, innocent websites can be blocked too.

Let us analyse the snippet of the flowchart shown in fig.1, which is dedicated to the precise use of Antivirus Software at the Mobile Forensic Workstation.

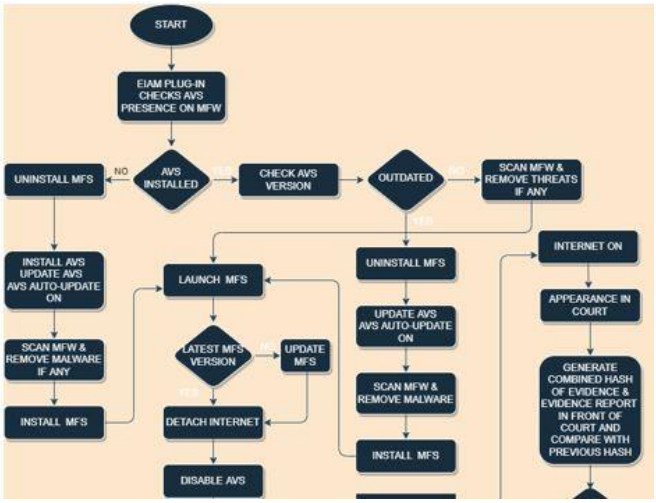


Figure.2: Flowchart Snippet for the Role of Antivirus Software in EIAM Plug-In

In the above fig., the EIAM does the following important tasks:

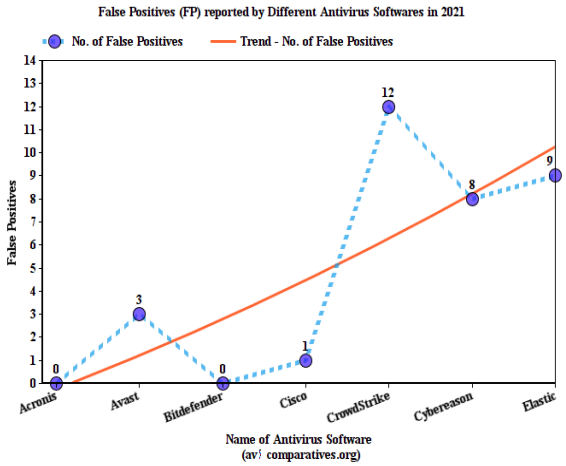
1. At the beginning of the mobile forensic scan, the EIAM checks the presence of Antivirus Software at mobile forensic workstation and disables or remove it before the extraction and decoding of mobile artifacts:-

Why So? : - Presence of Antivirus in the mobile forensic workstation is important because as the machine will expose to the internet or any other external flash drive, there is possibility of being infected with the malicious code i.e. Virus and thus the whole machine would be corrupted otherwise. This will result into the malfunctioning of the basic operating system tasks and the installed programs too. The following table shows the status of existence of antivirus software on user's machine in mid 2021.

Particulars	No. of Respondents	Percentage
Yes	90	80.4
No	18	16.1
Don't Know	4	3.5
Total	112	100

Table 1: Status of Antivirus Software Presence on User's Machine [3]

The above table clearly indicates that 19.6% users do not install Antivirus software at all. Hence, the EIAM checks and make sure about the presence of antivirus software on user's machine. Even though majority of the machines will pass this test at first glance itself but if they have installed EIAM, it will remove the Antivirus Software just before the Forensic process begins for the particular cyber crime case because it is highly recommended to remove or disable any antivirus software from computers that will be processing or reviewing cases. Antivirus software will often conflict with forensic software, and may quarantine or even delete some of your results before you get a chance to look at them.[2] The phenomenon is called as False Positive i.e. FP. To support this lets take into consideration the FPs reported in 2021 with different Antivirus softwares.



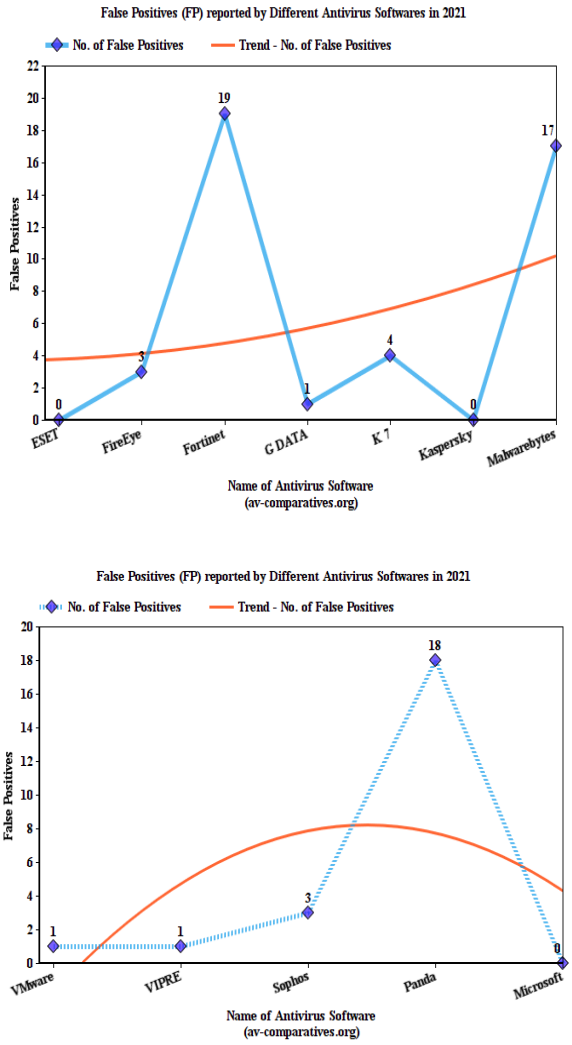


Figure 3: False Positive Instances of the Popular Antivirus Softwares

In the Fig. 3, Total same 60 cleaned files were under examination by the above-mentioned antivirus softwares.

False Positive Rate = Total number of False Positive Instances / Total number of Benign Instances

Name of Antivirus	FP Rate per 60 Benign Instances
Acronis	0
BitDefender	0
ESET	0
Kaspersky	0
Microsoft	0
Cisco	0.016
G DATA	0.016
VMware	0.016
VIPRE	0.016
Avast	0.05
FireEye	0.05
Sophos	0.05
K 7	0.066
Cybereason	0.133
Elastic	0.15
CrowdStrike	0.2
Malwarebytes	0.283
Panda	0.3
Fortinet	0.316

Table 2: False Positive Rate (FPR) of the Popular Antivirus Softwares

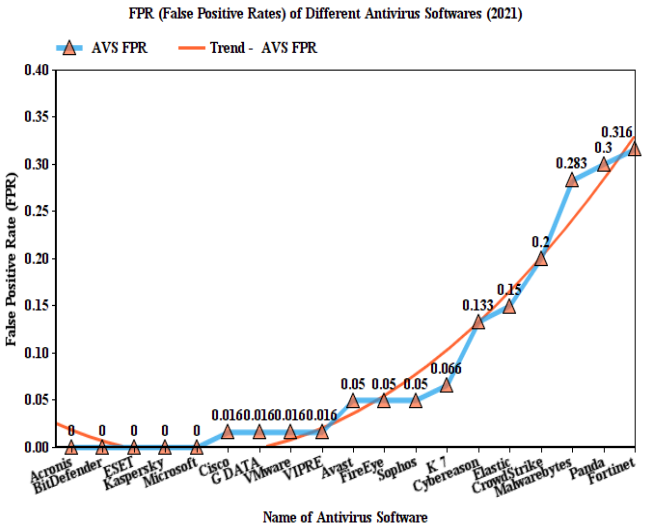


Figure 4: FPR Graphical Representation

Now calculating the average of FP as follows:

Average FP =∑ FP reported by all Antivirus Software / Total no. of Antivirus software considered

=100÷19

=5.26

If in 60 benign cases, 5.26 is Average False Positives obtained, then,

$$\% FP = 8.76\%$$

This means out of 100 cases, in 9 cases, there are possibilities that the Antivirus software may quarantine or even delete some of your results before you get a chance to look at them.

To support the statement, [2] can be taken into consideration. Hence the Removal / Deactivation of Antivirus Software by EIAM before the mobile forensic process is well justified.

From fig.2, it has been depicted that the EIAM also checks whether the Antivirus software is updated or not, for the cause of complete scan of the mobile forensic workstation before launching the Mobile Forensic Tool. Also, it advices to keep the auto-update mode ON for the antivirus software installed. It also forces to re-install the mobile forensic tool software which was working in virus infection prone environment before.

Why So? : - Firstly, the virus database of the antivirus should be well updated with respect to its database of virus signatures so that it can detect and eliminate the latest threats. In the study proposed in October 2021, by Dr. Sankararaman G., Dr.S.Suresh, Naveen Kumar M [3], the following table put forth the fact of updating antivirus software by the users.

Particulars	No. of Respondents	Percentage
At Least Once a Month	41	36.6
Occasionally	54	48.2
Never	17	15.2
Total	112	100

Table 3: Update Frequency of Antivirus Software by Users

From the above table, it can be concluded that almost all users don't tend to update their antivirus software by their own. In such situation, before initiation of any specific peculiar task like the process of mobile forensics, the users should be prompted to update their antivirus and to keep their antivirus software on AUTO-UPDATE mode. Hence, the EIAM was designed in such a way that it not only checks for the update status of antivirus software but also prompts the user to keep its AUTO-UPDATE mode ON.

The Mobile Forensic Tool, just as the other applications installed in operating systems, makes the use of the software and the hardware API resources of the system. Any hidden presence of malicious code like Trojan horse or Ransomware may spoil the harmony of the functioning of the overall mobile forensic workstation and affects its efficiency as it does with any other applications installed. Hence, the EIAM insists on full scan of the mobile forensic workstation and on the re-installation of mobile forensic tool if it found that the antivirus is not updated from the last 4 days and the mobile forensic tool was used during this vulnerable duration.

Hence, now the Jig-Saw Rubrics have been proposed to evaluate the performance of some popular mobile forensic tools with and without EIAM plug-in. The following mobile forensic tools were taken into consideration.

a) UFED Ultimate
b) AccessData's Forensic Toolkit FTK
c) Autopsy®
d) Oxygen Forensic® Detective

Criteria	Below Basic (5)	Basic (10)	Proficient (15)	Advanced (20)	Score (100)
Check Antivirus Presence	No Check	In user manual	Prompt Message	Explicit Check	
Check Update Status of Antivirus	No Check	In user manual	Prompt Message	Explicit Check	
Scanning before Forensic Process	No Scan	In user manual	Prompt Message	Explicit Check	
Re Install forensic tool if it worked in vulnerable environment	No Re-Install	In user manual	Prompt Message	Explicit Re-Install	
Disable or Remove Antivirus	No Deacti vation	In user manual	Prompt Message	Explicit Removal	

Figure 5: Grading Rules by Jigsaw Rubrics for Performance Evaluation of Different Mobile Forensic Tools

Tool Name: UFED Ultimate					
Criteria	**Below Basic (5)**	**Basic (10)**	**Proficient (15)**	**Advanced (20)**	**Score (100)**
Check Antivirus Presence	No Check	In user manual	Prompt Message	Explicit Check	5
Check Update Status of Antivirus	No Check	In user manual	Prompt Message	Explicit Check	5
Scanning before Forensic Process	No Scan	In user manual	Prompt Message	Explicit Check	20
Re Install forensic tool if it worked in vulnerable environment	No Re-Install	In user manual	Prompt Message	Explicit Re-Install	5
Disable or Remove Antivirus	No Deactiv ation	In user manual	Prompt Message	Explicit Removal	5
Total Score:					**40**

Figure 6: Jigsaw Rubrics Score for UFED Ultimate

Tool Name: AccessData's Forensic Toolkit FTK					
Criteria	**Below Basic (5)**	**Basic (10)**	**Proficient (15)**	**Advanced (20)**	**Score (100)**
Check Antivirus Presence	No Check	In user manual	Prompt Message	Explicit Check	5
Check Update Status of Antivirus	No Check	In user manual	Prompt Message	Explicit Check	15
Scanning before Forensic Process	No Scan	In user manual	Prompt Message	Explicit Check	20
Re Install forensic tool if it worked in vulnerable environment	No Re-Install	In user manual	Prompt Message	Explicit Re-Install	5
Disable or Remove Antivirus	No Deactiv ation	In user manual	Prompt Message	Explicit Removal	5
Total Score:					**50**

Figure 7: Jigsaw Rubrics Score for AccessData's Forensic Toolkit FTK

Tool Name: Autopsy®					
Criteria	**Below Basic (5)**	**Basic (10)**	**Proficient (15)**	**Advanced (20)**	**Score (100)**
Check Antivirus Presence	No Check	In user manual	Prompt Message	Explicit Check	5
Check Update Status of Antivirus	No Check	In user manual	Prompt Message	Explicit Check	5
Scanning before Forensic Process	No Scan	In user manual	Prompt Message	Explicit Check	5
Re Install forensic tool if it worked in vulnerable environment	No Re-Install	In user manual	Prompt Message	Explicit Re-Install	5
Disable or Remove Antivirus	No Deactiv ation	In user manual	Prompt Message	Explicit Removal	10
Total Score:					**30**

Figure 8: Jigsaw Rubrics Score for Autopsy®

Tool Name: Oxygen Forensic® Detective					
Criteria	Below Basic (5)	Basic (10)	Proficient (15)	Advanced (20)	Score (100)
Check Antivirus Presence	No Check	In user manual	Prompt Message	Explicit Check	5
Check Update Status of Antivirus	No Check	In user manual	Prompt Message	Explicit Check	5
Scanning before Forensic Process	No Scan	In user manual	Prompt Message	Explicit Check	5
Re Install forensic tool if it worked in vulnerable environment	No Re-Install	In user manual	Prompt Message	Explicit Re-Install	5
Disable or Remove Antivirus	No Deactivation	In user manual	Prompt Message	Explicit Removal	5
Total Score:					25

Figure 9: Jigsaw Rubrics Score For Oxygen Forensic® Detective

Tool Name: EnCase® Forensic					
Criteria	Below Basic (5)	Basic (10)	Proficient (15)	Advanced (20)	Score (100)
Check Antivirus Presence	No Check	In user manual	Prompt Message	Explicit Check	10
Check Update Status of Antivirus	No Check	In user manual	Prompt Message	Explicit Check	5
Scanning before Forensic Process	No Scan	In user manual	Prompt Message	Explicit Check	15
Re Install forensic tool if it worked in vulnerable environment	No Re-Install	In user manual	Prompt Message	Explicit Re-Install	5
Disable or Remove Antivirus	No Deactivation	In user manual	Prompt Message	Explicit Removal	5
Total Score:					40

Figure 10 : Jigsaw Rubrics Score For Encase® Forensic

From the fig.5-10, the Jig-Saw Rubrics scores have been proposed for the forensic tools under consideration. Each tool's complete modus operandi from the documentation as well as from the practical point of view have been taken into consideration and based on that, the points as per rubric rules have been assigned.

In this analysis, whatsoever malware scanning methodology was implemented by the forensic tools intrinsically, they focused on the disc space of the device seized and not on the disc space of the mobile forensic workstation. In addition, the pre-forensic environment for the smooth execution of the mobile forensic tool on the mobile forensic workstation has not been given much prominence from the malware vulnerability point of view. But when coupled with EIAM, hopefully the above pitfalls could be avoided and hence the quality of the Evidence Extraction & Integration can be enhanced as shown in Fig.11.

Tool Name: EIAM ENABLED TOOL					
Criteria	Below Basic (5)	Basic (10)	Proficient (15)	Advanced (20)	Score (100)
Check Antivirus Presence	No Check	In user manual	Prompt Message	Explicit Check	20
Check Update Status of Antivirus	No Check	In user manual	Prompt Message	Explicit Check	20
Scanning before Forensic Process	No Scan	In user manual	Prompt Message	Explicit Check	15
Re Install forensic tool if it worked in vulnerable environment	No Re-Install	In user manual	Prompt Message	Explicit Re-Install	15
Disable or Remove Antivirus	No Deactivation	In user manual	Prompt Message	Explicit Removal	15
Total Score:					85

Figure 11: Jigsaw Rubrics Score for EIAM Enabled Forensic Tool

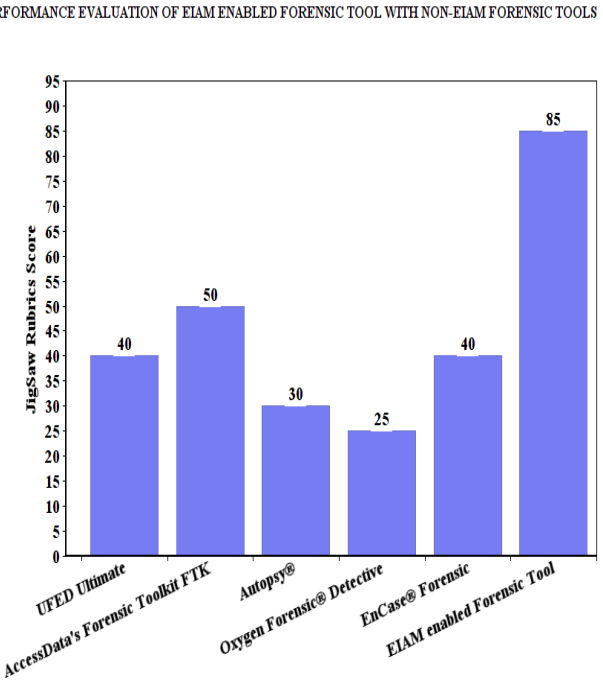


Figure 12: Performance Evaluation of EIAM Enabled Forensic Tool with Non-EIAM Forensic Tools

From above chart, it can be vividly concluded that the EIAM enabled forensic tools explicitly outperform when compared to Non-EIAM mobile forensic tools

in terms of preserving the integrity of the digital evidence obtained during the forensic process. In the development of mobile forensic tools, the least attention given to ethos of working of the antivirus software and the vulnerability of execution environment of the mobile forensic software could be disastrous & can play significant role in damaging the digital evidence extraction process.

III. CONCLUSION

With the advent of new versions of the mobile handhelds, the expectations from the digital forensic process have also raised in terms of the security of digital evidence. The proposed work depicts the role and the management of antivirus software on the mobile forensic workstations with respect to safety of the digital evidences. The antivirus software is the backbone and a must have component of the stable computer system. However, its conventional use during the forensic process may pose harm to the digital evidence. Hence the proposed EIAM plug-in implements the optimized use of antivirus software in terms of making it ON and OFF, checking its virus database signatures etc. during the peculiar phases of the mobile forensic process. The proposed work concludes that if EIAM is applied with the forensic tool, then the possibilities that the Antivirus software may quarantine or even delete some of your results before you get a chance to look at them, will be negligible or zero.

IV. REFERENCES

[1] Mohammed I. Al-Saleh, “The Impact of the Antivirus on the Digital Evidence”, January 2013,International Journal of Electronic Security and Digital, Forensics 5(3/4):229–240

[2] https://sleuthkit.org/autopsy/docs/user-docs/4.5.0/ installation _ page . html

[3] Dr. Sankararaman G, Dr.S.Suresh & Naveen Kumar M,“A Study On Users’ Opinion On Cyber Security”, IJGBMR Volume 10, Issue 2, October 2021

[4] https://www.tomsguide.com/news/what-are-false-positives-and-how-to-avoid-them

[5] Mr. Bhushan M. Manjre , Dr. Krishan Kumar Goyal , Dr. Shivani, ”Evidence Integrity Assurance Mechanism (EIAM) Plug-In for Software Framework of Mobile Forensic Tools To Extract And Decode The Mobile Artifacts”, International Conference of Scientific Computing in Innovation (ICSCI-2022), ISBN:978-93-91077-04-4, pp.- 477-483.

[6] Fernando Molina Granja, Glen D. Rodríguez Rafael,” The preservation of digital evidence and its admissibility in the court”, International Journal of Electronic Security and Digital Forensics · January 2017 DOI: 10.1504/IJESDF.2017.10002624

[7] David MUGISHA, ”DIGITAL FORENSICS: Digital Evidence in judicial System”, International Journal of Cyber Criminology · March 2019

[8] SaeedAlmarri and Dr Paul Sant, “Optimised Malware Detection in Digital Forensics”, International Journal of Network Security & Its Applications (IJNSA), Vol.6, No.1, January 2014

[9] Ahmad Fekry Moussa,”Electronic evidence and its authenticity in forensic evidence”, Moussa Egyptian Journal of Forensic Sciences (2021) 11:20 https://doi.org/10.1186/s41935-021-00234-6

[10] Hassan M,” Forensics on a Mobile Device, Tools and Limitations”, International Journal of Forensic Sciences, ISSN: 2573-1734

[11] Gulshan Shrivastava , Kavita Sharma , Manju Khari and Syeda Erfana Zohora (2018), “Role of Cyber Security and Cyber Forensics in India”, Handbook of Research on Network Forensics and Analysis Techniques, 2018, DOI: 10.4018/978-1-5225-4100-4.ch009

[12] https://cf-media.cellebrite.com/wp-content/uploads/ 2017/08/UFED6.3_Ultimate-InField_ReleaseNotes _EN.pdf
[13] https://cf-media.cellebrite.com/wp-content/uploads /2019/09/Chinex-Quickguide_2019_A4.pdf
[14] https://cf-media.cellebrite.com/wp-content/ uploads2019 /05/ReleaseNotes _UFED_PA_7.18.pdf
[15] https://cf-media.cellebrite.com/wp-content /uploads/2019/10/ReleaseNotes _UFED_v7.24.pdf
[16] https://ad-pdf.s3.amazonaws.com/7.x% 20Documentation /7.4.0/ Enterprise_7.4_UG.pdf
[17] https://ad-pdf.s3.amazonaws.com/7.x% 20Documentation /7.4.0/FTK_7.4 _UG.pdf
[18] https://ad-pdf.s3.amazonaws.com/7.x% 20Documentation/7.4.0/ AD _ Lab_7.4_UG.pdf
[19] https://ad-pdf.s3.amazonaws.com/ftk/6.3.x/ KFF_Install.pdf
[20] https://sleuthkit.org/autopsy/docs/user-docs /4.5.0/installation_page.html
[21] https://www.oxygen-forensic.com/downloads/general/ Oxygen_Forensic _ Detective_Getting_started.pdf
[22] https://www.oxygen-forensic.com/uploads/doc_guide /Oxygen_ Forensic _Detective_Getting_Started.pdf
[23] http://encase-docs.opentext.com/documentation /encase/forensic/8.07/Content/Resources/External% 20Files/EnCase%20Forensic%20v8.07%20User %20Guide.pdf
[24] Daniel Fuentes , Juan A. Álvarez , Juan A. Ortega , Luis Gonzalez-Abril , and Francisco Velasco, " Trojan horses in mobile devices", Computer Science and Information Systems ,December 2010 DOI : 10.2298/ CSIS090330027F
[25] Gostev, A.,"Mobile Malware Evolution: An Overview" , [Online]. Available: http:// www.viruslist.com/en /analysis?pubid=204792080, Sept. 2009

Cite this article as :

Mr. Bhushan M. Manjre, Dr. Krishan Kumar Goyal, Dr. Shivani, "Optimization in Security of Digital Evidences by Integration of Evidence Integrity Assurance Mechanism (EIAM) Plug-in into the Software Framework of Mobile Forensic Tools with Balanced Use of Antivirus Softwares", International Journal of Scientific Research in Computer Science, Engineering and Information Technology (IJSRCSEIT), ISSN : 2456-3307, Volume 8 Issue 3, pp. 11-19, May-June 2022. Available at doi : https://doi.org/10.32628/CSEIT22836
Journal URL : https://ijsrcseit.com/CSEIT22836