

**Naif Arab University for Security Sciences**

**College of Criminal Justice**

**Department of Forensic Sciences**



**The Effect of Anti-Forensics on the Digital Forensic  
Investigation Process in Saudi Arabia**

**Presented by**

Moneerah Eid AlEssa

**Supervisor**

Dr. Maryem Ammi

Submitted in partial fulfillment of the requirement for the master's degree  
of Information Security

**Riyadh**

1441 - 2020



جامعة نايف العربية للعلوم الأمنية  
كلية العدالة الجنائية  
قسم علوم الأدلة الجنائية

# تأثير استخدام الآليات والأدوات المعيقة لعملية التحقيق الجنائي الرقمي في المملكة العربية السعودية

إعداد

منيرة عيد العيسى

إشراف

د. مريم عمي

رسالة مقدمة استكمالاً لمتطلبات الحصول على درجة الماجستير  
في أمن المعلومات

الرياض

١٤٤١هـ - ٢٠٢٠م

## Table of contents

Table of keywords .....	I
Study abstract.....	II
Arabic study abstract .....	III
Dedications .....	IV
Acknowledgements.....	V
Statement of original authorship .....	VI
Table of contents.....	VII
List of figures .....	X
List of tables.....	XI
<b>Chapter 1: Introduction .....</b>	<b>1</b>
1.1 Context of the study.....	1
1.2 Problem statement .....	2
1.3 Research questions .....	2
1.4 Objectives .....	3
1.5 Contributions .....	3
1.6 Thesis organization.....	4
<b>Chapter 2: Background and literature review .....</b>	<b>5</b>
2.1 Forensics science overview .....	5
2.2 Digital forensics and digital forensics investigation .....	6
2.2.1 Digital forensics investigation history.....	7

2.3 Digital evidence.....	8
2.3.1 Preventing evidence tampering .....	12
2.3.2 Digital evidence locations .....	12
2.4 Digital forensics investigation process .....	15
2.4.1 Digital forensic investigation process in Saudi Arabia: an overview.....	16
2.4.2 General Security hierarchy .....	17
2.5 Challenges of digital forensics investigation .....	19
2.6 Digital forensics investigation readiness .....	21
2.7 Anti-Forensics .....	23
2.7.1 Definition of anti-forensics .....	23
2.7.2 Anti-Forensic techniques classification related works .....	24
2.7.3 Anti-Forensic tools related works.....	31
2.7.4 Anti-Forensics experiment .....	34
2.7.4.1 Digital forensics investigation practitioner required skills .....	37
2.8 Digital forensic investigation practitioners .....	38
Summary.....	40
<b>Chapter 3: Research methodology .....</b>	<b>41</b>
3.1 Research design .....	41
3.2 The study of community and sampling .....	42
3.3 Questionnaire procedures .....	43
3.4 Statistical methods for analyzing data .....	44

3.5 Validity and reliability of questionnaire .....	52
3.6 Ethics and limitations .....	52
Summary.....	53
<b>Chapter 4: Results and discussions .....</b>	<b>54</b>
4.1 Results of the questionnaire .....	54
4.2 Findings of the survey .....	81
4.3 Discussions .....	85
4.4 Recommendations .....	86
Summary.....	87
<b>Chapter 5: Conclusions and future work .....</b>	<b>88</b>
5.1 Conclusions .....	88
5.2 Future work .....	90
Summary.....	90
<b>Bibliography .....</b>	<b>91</b>
<b>List of appendices .....</b>	<b>96</b>
Appendix 1 .....	96
Appendix 2 (A).....	98
Appendix 2 (B) .....	102
Appendix 3 .....	106
Appendix 4 .....	109
Appendix 5 .....	112

## List of figures

Figure 1. Branches of digital forensics .....	6
Figure 2. Cyber threats reported by EY Global in 2018-19.....	8
Figure 3. Digital forensics investigation phases .....	15
Figure 4. General Security hierarchy .....	19
Figure 5. Digital forensics investigation readiness conceptual model.....	23
Figure 6. How Snow tool is working .....	34
Figure 7. Two text files .....	35
Figure 8. Autopsy tool examination .....	36
Figure 9. The participants distribution according to age .....	55
Figure 10. The participants distribution according to gender .....	56
Figure 11. The participants distribution according to educational qualification .....	57
Figure 12. The participants distribution according to job.....	58
Figure 13. The participants distribution according to experience of years .....	59
Figure 14. The participants distribution according to sector .....	60
Figure 15. The participants distribution according to field of work .....	61

## List of tables

Table 1. Category of forensics and type of evidence collected .....	9
Table 2. Digital evidence locations.....	13
Table 3. Classification of anti-forensics .....	24
Table 4. Extended taxonomy of anti-forensics .....	27
Table 5. The participants distribution according to age .....	54
Table 6. The participants distribution according to gender .....	55
Table 7. The participants distribution according to educational qualification.....	56
Table 8. The participants distribution according to job .....	57
Table 9. The participants distribution according to experience of years .....	58
Table 10. The participants distribution according to sector.....	59
Table 11. The participants distribution according to field of work .....	60
Table 12. The current situation of digital forensic investigation related to Saudi Arabia .... .....	63
Table 13. The current situation of digital forensic investigation related to the employee and his place of work .....	67
Table 14. The the extent of digital forensics practitioners knowledgeable of anti-forensic techniques and tools.....	72
Table 15. The effect of using anti-forensics on the digital forensic investigation process .....	76
Table 16. The recommendations to overcome anti-forensics when it occurs	79