

مذكرة تخرج مقدمة إلى

جامعة محمد بوضياف - المسيلة



كلية الرياضيات والإعلام الآلي

قسم الإعلام الآلي

من أجل الاستيفاء الجزئي لمتطلبات شهادة

ماستر في الإعلام الآلي

تخصص: شبكات وتكنولوجيا الإعلام والاتصال "RTIC"

من طرف

يحي زهاق

عنوان المذكرة

منصة متكاملة للتحليل الجنائي الرقمي للهواتف المحمولة المدمجة بالذكاء الاصطناعي

-DZ ForensiGuard-

الأستاذ المشرف

د. بونيف محمد الهادي

أعضاء لجنة المناقشة

رئيسا

جامعة المسيلة

د. بن عزي مخلوف

ممتحنا

جامعة المسيلة

د. شترة محمد

جوان 2026

المخلص

يُعد التحليل الجنائي للهواتف الذكية ركناً أساسياً في منظومة الأمن السيبراني المعاصر، نظراً للدور المحوري لهذه الأجهزة كمستودعات رقمية للأدلة الجنائية. تهدف هذه الدراسة إلى تطوير منصة متخصصة للتحليل الجنائي (DZ ForensiGuard)، مصممة هندسياً لتلبية المتطلبات التقنية واللغوية للتحقيق الرقمي. يعتمد العمل على منهجية معيارية تبدأ من تحليل المتطلبات والنمذجة باستخدام UML، وصولاً إلى التنفيذ البرمجي عبر إطار عمل FastAPI وتقنيات تحليل البيانات المتقدمة. تم دمج أربع خوارزميات جوهرية تشمل الجدولة الزمنية، والتحليل الجغرافي، وتعقب شبكات العلاقات، وتحليل الانتروبيا لكشف التشفير. وأثبتت نتائج الاختبارات الميدانية على أجهزة متنوعة كفاءة المنصة في استخراج الأدلة بدقة وموثوقية عالية وزمن معالجة تنافسي، مما يؤكد جدوى بناء أدوات برمجية تقنية مستقلة قادرة على مضاهاة الحلول العالمية مع ضمان أمن وخصوصية البيانات.

الكلمات المفتاحية: التحليل الجنائي الرقمي، الهواتف المحمولة، DZ ForensiGuard، سلامة الأدلة، تحليل الانتروبيا، SHA-256.

Abstract

Mobile device forensics is a foundational pillar of modern cybersecurity, given the critical role these devices play as digital repositories for forensic evidence. This study aims to develop a specialized forensic analysis platform (DZ ForensiGuard), engineered to meet the technical and linguistic requirements of digital investigations. The research adopts a standardized methodology ranging from requirement analysis and UML modeling to software implementation via the FastAPI framework and advanced data analysis techniques. Four core algorithms were integrated, encompassing timeline analysis, geolocation tracking, social network mapping, and entropy analysis for encryption detection. Field test results on various devices demonstrated the platform's efficiency in extracting evidence with high accuracy and reliability within competitive processing times. These findings validate the feasibility of building integrated local software tools capable of rivaling global solutions while ensuring data security and privacy.

Keywords: Digital Forensics, Mobile Phones, DZ ForensiGuard, Evidence Integrity, Entropy Analysis, SHA-256.

إهداء

أهدي هذا العمل المتواضع إلى والدي الكريمين حفظهما الله...
إلى إخوتي وأخواتي وكل أفراد عائلتي...
إلى كل من ساندني في مسيرتي العلمية.

شكر وتقدير

نتقدم بخالص الشكر والتقدير إلى الأستاذ المشرف دكتور بونيف محمد الهادي على دعمه المتواصل وتوجيهاته القيمة وملاحظاته العلمية التي أسهمت في إنجاز هذا العمل.

كما نتوجه بالشكر إلى أفراد الأسرة والأصدقاء على صبرهم ومساندتهم المعنوية طوال فترة البحث.

ونعبر أيضاً عن امتناننا لمؤسستنا الجامعية جامعة محمد بوضياف - المسيلة، وكل من ساهم من قريب أو بعيد في تهيئة الظروف المناسبة لإتمام هذا العمل.

فهرس المحتويات

1	المقدمة العامة
2	1 الفصل الأول: الأمن المعلوماتي والأمن السيبراني
2	1.1 تعريف الأمن المعلوماتي
2	2.1 تعريف الأمن السيبراني
2	3.1 العلاقة بين الأمن المعلوماتي والأمن السيبراني
3	4.1 أهداف الأمن المعلوماتي
3	1.4.1 السرية (Confidentiality)
3	2.4.1 السلامة (Integrity)
3	3.4.1 التوفر (Availability)
3	4.4.1 المصادقة (Authentication)
4	5.4.1 عدم الإنكار (Non-repudiation)
4	5.1 عناصر الأمن المعلوماتي
4	1.5.1 المستخدم (User)
4	2.5.1 الأجهزة (Hardware)
4	3.5.1 البرمجيات (Software)
4	4.5.1 الشبكات (Networks)
5	5.5.1 البيانات (Data)
5	6.1 التهديدات السيبرانية
5	1.6.1 البرمجيات الخبيثة (Malware)
5	2.6.1 التصيد الاحتيالي (Phishing)
5	3.6.1 هجمات حجب الخدمة (DDoS)
6	4.6.1 الهندسة الاجتماعية (Social Engineering)
6	7.1 الإشكالية

6	التحليل الجنائي الرقمي (Digital Forensics)	8.1
6	تعريف التحليل الجنائي الرقمي	1.8.1
6	أهداف التحليل الجنائي الرقمي	2.8.1
7	العلاقة بين التحليل الجنائي الرقمي والأمن السيبراني	3.8.1
7	التحديات في التحليل الجنائي الرقمي	4.8.1
7	التشفير القوي (Strong Encryption)	1.4.8.1
7	الحجم الكبير للبيانات (Big Data Volume)	2.4.8.1
7	تطور أساليب الهجوم (Advanced Cyber Attacks)	3.4.8.1
7	نقص الخبرة التقنية (Lack of Technical Expertise)	4.4.8.1
8	خاتمة الفصل الأول	9.1
9	2 الفصل الثاني: Digital Forensics - التحليل الجنائي الرقمي	
9	مفهوم التحليل الجنائي الرقمي	1.2
9	المبادئ الأساسية للتحليل الجنائي الرقمي	2.2
10	مبدأ التوثيق	1.2.2
10	مبدأ القابلية للإعادة	2.2.2
10	مراحل التحليل الجنائي الرقمي	3.2
10	التعرف على الحادث (Identification)	1.3.2
10	جمع الأدلة (Collection)	2.3.2
10	حفظ الأدلة (Preservation)	3.3.2
10	الفحص (Examination)	4.3.2
11	التحليل (Analysis)	5.3.2
11	التقرير (Reporting)	6.3.2
11	أنواع التحليل الجنائي الرقمي (Digital Forensics Types)	4.2
11	تحليل الأقراص (Disk Forensics)	1.4.2
11	تحليل الذاكرة (Memory Forensics)	2.4.2
12	تحليل الهواتف (Mobile Forensics)	3.4.2
13	تحليل الشبكات (Network Forensics)	4.4.2
13	تحليل قواعد البيانات (Database Forensics)	5.4.2
13	أدوات التحليل الجنائي الرقمي	5.2
13	الأدوات مفتوحة المصدر	1.5.2

13	Autopsy	1.1.5.2	
14	The Sleuth Kit	2.1.5.2	
14	Wireshark	3.1.5.2	
14	الأدوات التجارية	2.5.2	
14	EnCase Forensic	1.2.5.2	
15	Forensic Toolkit (FTK)	2.2.5.2	
15	مقارنة علمية بين الأدوات	3.5.2	
15	تحليل نقدي	4.5.2	
16	التقنيات الحديثة في التحليل الجنائي الرقمي	6.2	
16	الذكاء الاصطناعي (Artificial Intelligence)	1.6.2	
16	تحليل البيانات الضخمة (Big Data Analytics)	2.6.2	
17	تكامل التقنيات الحديثة	3.6.2	
17	التحليل الجنائي الرقمي باستخدام الذكاء الاصطناعي	7.2	
17	دور الذكاء الاصطناعي في التحليل الجنائي الرقمي	1.7.2	
18	جمع الأدلة الذكي (Smart Evidence Collection)	1.1.7.2	
18	التحليل التلقائي للأدلة (Automated Analysis)	2.1.7.2	
18	التنبؤ بالهجمات (Attack Prediction)	3.1.7.2	
18	دعم اتخاذ القرار (Decision Support)	4.1.7.2	
19	مخطط سير عمل التحليل الجنائي بالذكاء الاصطناعي	5.1.7.2	
19	خاتمة الفصل الثاني	8.2	
20	الفصل الثالث: التصميم والتحليل - نمذجة نظام DZ ForensiGuard باستخدام UML	3	
20	متطلبات النظام	1.3	
20	المتطلبات الوظيفية	1.1.3	
21	المتطلبات غير الوظيفية	2.1.3	
21	نمذجة النظام - مخطط حالة الاستخدام	2.3	
21	مخطط حالة الاستخدام	1.2.3	
23	نمذجة النظام - مخطط الفئات	3.3	
23	مخطط الفئات	1.3.3	
24	نمذجة النظام - مخطط التسلسل	4.3	
26	هيكل سجل التدقيق	5.3	

27	خاتمة الفصل الثالث	6.3
28	الفصل الرابع: النتائج والمناقشة	4
28	بيئة التطوير والتنفيذ	1.4
28	لغات البرمجة والتقنيات المستخدمة	2.4
29	هندسة النظام	3.4
31	قاعدة البيانات	4.4
31	واجهات البرمجة	5.4
33	خوارزميات التحليل المطبقة	6.4
33	الجدول الزمني	1.6.4
33	تحليل المواقع الجغرافية	2.6.4
33	تحليل شبكة العلاقات الاجتماعية	3.6.4
34	تحليل الانترنت لاكتشاف التشفير	4.6.4
36	التحقق من سلامة الملفات	5.6.4
36	كشف نوع الملفات من التوقيع الثنائي	6.6.4
36	سلسلة العهدة	7.4
37	إحصائيات المشروع	8.4
38	واجهات النظام	9.4
38	واجهة تسجيل الدخول	1.9.4
38	الصفحة الرئيسية	2.9.4
39	لوحة التحكم	3.9.4
39	إدارة القضايا	4.9.4
39	تفاصيل القضية	5.9.4
39	استخراج البيانات	6.9.4
40	إدارة الأدلة الرقمية	7.9.4
41	جهات الاتصال	8.9.4
41	الرسائل النصية	9.9.4
41	الجدول الزمني	10.9.4
41	تحليل المواقع الجغرافية	11.9.4
42	تحليل شبكة العلاقات	12.9.4
43	تحليل الذكاء الاصطناعي	13.9.4

43	التقارير	14.9.4
44	الإعدادات	15.9.4
44	طلب حساب جديد	16.9.4
44	الميزات التقنية للنظام	10.4
44	مقارنة عامة مع الأنظمة التجارية	11.4
46	الخوارزميات الأساسية في النظام	12.4
46	خوارزمية استخراج بيانات Android	1.12.4
46	خوارزمية التحليل بالذكاء الاصطناعي	2.12.4
47	خوارزمية استعادة البيانات المحذوفة	3.12.4
47	خوارزمية تحليل شبكة العلاقات	4.12.4
48	خوارزمية إنشاء الجدول الزمني واكتشاف الشذوذ	5.12.4
48	ملخص الخوارزميات وتكاملها	6.12.4
49	مناقشة النتائج	13.4
49	تقييم كفاءة استخراج البيانات	1.13.4
49	تحليل دقة الخوارزميات والذكاء الاصطناعي	2.13.4
49	تحقيق الموثوقية الجنائية وسلسلة العهدة	3.13.4
49	المقارنة مع الأنظمة التجارية والدراسات السابقة	4.13.4
50	التحديات والقيود	5.13.4
50	خاتمة الفصل الرابع	14.4
51	خاتمة عامة	
52	المراجع	

قائمة الأشكال

12	شعار أداة Volatility	1.2
14	واجهة برنامج Autopsy للتحليل الجنائي الرقمي	2.2
15	واجهة برنامج Wireshark لتحليل حزم الشبكة	3.2
18	سير عمل مبسط للتحليل الجنائي باستخدام الذكاء الاصطناعي	4.2
19	سير عمل التحليل الجنائي الرقمي باستخدام تقنيات الذكاء الاصطناعي	5.2
22	مخطط حالة الاستخدام لنظام DZ ForensiGuard	1.3
23	مخطط الفئات الرئيسية في نظام DZ ForensiGuard	2.3
25	مخطط التسلسل لعملية استخراج البيانات وتحليلها في نظام DZ ForensiGuard	3.3
30	هندسة النظام متعددة الطبقات في DZ ForensiGuard	1.4
37	آلية سلسلة العهدة (Chain of Custody) باستخدام SHA-256	2.4
38	واجهة تسجيل الدخول إلى نظام DZ ForensiGuard	3.4
38	الصفحة الرئيسية لنظام DZ ForensiGuard	4.4
39	لوحة التحكم الرئيسية في النظام	5.4
39	واجهة إدارة القضايا الجنائية	6.4
40	واجهة عرض تفاصيل القضية	7.4
40	واجهة استخراج البيانات من الجهاز المحمول	8.4
40	واجهة إدارة الأدلة الرقمية	9.4
41	واجهة عرض جهات الاتصال	10.4
41	واجهة عرض الرسائل النصية	11.4
42	واجهة عرض الجدول الزمني للأحداث	12.4
42	واجهة تحليل المواقع الجغرافية	13.4
42	واجهة تحليل شبكة العلاقات الاجتماعية	14.4
43	واجهة تحليل الذكاء الاصطناعي لاكتشاف الأنماط	15.4

43	 واجهة إنشاء وتحميل التقارير	16.4
44	 واجهة إعدادات النظام	17.4
44	 واجهة طلب حساب جديد للمحققين	18.4

قائمة الجداول

15	مقارنة بين أدوات التحليل الجنائي الرقمي	1.2
17	التقنيات الحديثة في التحليل الجنائي الرقمي: التطبيقات والتحديات	2.2
18	تطبيقات الذكاء الاصطناعي في مراحل التحليل الجنائي الرقمي	3.2
20	المتطلبات الوظيفية لنظام DZ ForensiGuard	1.3
21	المتطلبات غير الوظيفية لنظام DZ ForensiGuard	2.3
26	هيكل سجل النشاطات (Audit Log) لمراقبة سلامة الأدلة	3.3
28	مواصفات بيئة التطوير والتنفيذ	1.4
29	لغات البرمجة والتقنيات المستخدمة في النظام	2.4
31	جداول قاعدة البيانات في نظام DZ ForensiGuard	3.4
32	أهم واجهات API في نظام DZ ForensiGuard	4.4
33	خوارزميات التحليل المطبقة في نظام DZ ForensiGuard	5.4
34	قيم الإنترنت النمذجية لأنواع مختلفة من الملفات	6.4
36	أمثلة لقيم الإنترنت لأنواع مختلفة من الملفات	7.4
37	إحصائيات مشروع DZ ForensiGuard	8.4
45	الميزات التقنية لنظام DZ ForensiGuard	9.4
45	مقارنة عامة بين DZ ForensiGuard والأنظمة التجارية	10.4
48	ملخص الخوارزميات الأساسية في نظام DZ ForensiGuard	11.4

قائمة الاختصارات

الاختصار	المعنى
ADB	Android Debug Bridge
AES	Advanced Encryption Standard
API	Application Programming Interface
CPU	Central Processing Unit
DDoS	Distributed Denial of Service
ENISA	European Union Agency for Cybersecurity
EXIF	Exchangeable Image File Format
FR	Functional Requirement
GPS	Global Positioning System
HDD	Hard Disk Drive
HTML	HyperText Markup Language
HTTP	HyperText Transfer Protocol
NFR	Non-Functional Requirement
ICT	Information and Communication Technology
IDE	Integrated Development Environment
IDS	Intrusion Detection System
IEC	International Electrotechnical Commission
IoT	Internet of Things
IP	Internet Protocol
ISO	International Organization for Standardization
ITU	International Telecommunication Union
JSON	JavaScript Object Notation
JWT	JSON Web Token
MD5	Message Digest Algorithm 5
NIST	National Institute of Standards and Technology
OS	Operating System
PDF	Portable Document Format
PKI	Public Key Infrastructure

المعنى	الاختصار
Random Access Memory	RAM
Right to Left	RTL
Secure Hash Algorithm	SHA
Security Operations Center	SOC
Structured Query Language	SQL
Solid State Drive	SSD
Transmission Control Protocol	TCP
User Datagram Protocol	UDP
Unified Modeling Language	UML
Universal Serial Bus	USB
Coordinated Universal Time	UTC
Virtual Private Network	VPN
Write Once Read Many	WORM

المقدمة العامة

شهد العالم في السنوات الأخيرة قفزة نوعية متسارعة في استخدام وتطوير الهواتف الذكية، مما أدى إلى تضخم هائل في حجم البيانات الرقمية المنتجة، وجعلها مصدراً غنياً وبنكاً للمعلومات يمكن توظيفه كأدلة مادية حاسمة في التحقيقات الجنائية الحديثة. وفي المقابل، شهدت الجرائم الإلكترونية والسيبرانية تطوراً موازياً في التعقيد والابتكار، مما استدعى وجود حاجة ملحة ومتزايدة إلى أنظمة برمجية متطورة قادرة على استخراج وتحليل الأدلة الرقمية بكفاءة وموثوقية عالية، مع ضمان سلامة الأدلة قانونياً وفنياً. ورغم وفرة الأدوات والمنصات العالمية في هذا المجال، إلا أن أغلبها يظل حكراً على المؤسسات الغربية نظراً لتكلفتها الباهظة وافتقارها التام لدعم اللغة العربية كلغة أساسية للتحليل وعرض التقارير وهو الأمر الذي شكل دافعاً رئيساً لنا لتصميم وتطوير منصة DZ ForensiGuard كحل وطني وعربي مبتكر في مجال التحليل الجنائي الرقمي للهواتف المحمولة.

ومن هذا المنطلق، تتبلور إشكالية هذه الدراسة في التساؤل الجوهرى التالي: كيف يمكن تصميم وتنفيذ منصة وطنية متكاملة للتحليل الجنائي الرقمي للهواتف المحمولة (DZ ForensiGuard) تكون قادرة على استخراج وتحليل الأدلة الرقمية بأعلى مستويات الدقة والكفاءة والنزاهة الفنية؟ وينبثق عن هذا التساؤل مجموعة من الأسئلة الفرعية تدور حول تحديد المتطلبات المعمارية والبرمجية للمنصة، وتصميم نموذجها الهيكلي، واختبار مدى كفاءتها التشغيلية ودقتها التحليلية مقارنة بالأنظمة العالمية التجارية المتوفرة في السوق.

تهدف هذه الدراسة إلى بناء وتجسيد منصة DZ ForensiGuard لدعم جهود التحقيق الرقمي، عبر تطبيق خوارزميات متقدمة تشمل تحليل الجدول الزمني للأحداث، وتتبع المواقع الجغرافية، ورسم شبكات العلاقات الاجتماعية، وحساب الانتروبيا لكشف الملفات المشفرة، مع ضمان سلسلة عهدة (Chain of Custody). وقد اعتمدت الدراسة على المنهج الوصفي التحليلي لاستقراء الأدوات الحالية، ومنهجية هندسة البرمجيات لتأطير التصميم والتنفيذ، والمنهج التجريبي لقياس الكفاءة على أجهزة حقيقية. وتتحدد حدود الدراسة الفنية في استخراج وتحليل البيانات الحيوية من أجهزة Android و iOS.

ولتحقيق هذه الأهداف، تم تقسيم هذه المذكرة إلى أربعة فصول متكاملة؛ حيث:

- **يعرض الفصل الأول:** الإطار النظري والمفاهيمي للأمن المعلوماتي والسيبراني، موضحاً العلاقة التكاملية بينهما وأهدافهما، فضلاً عن تحديد التهديدات السيبرانية المعاصرة ومبادئ التحقيق الجنائي الرقمي.
- **يتناول الفصل الثاني:** دراسة مسحية ونقدية للأدوات والتقنيات المستخدمة في الاستقصاء الرقمي، مع تقديم مقارنة علمية بين الحلول مفتوحة المصدر والتجارية، واستعراض دور الذكاء الاصطناعي والبيانات الضخمة في هذا المجال.
- **يقدم الفصل الثالث:** التصميم المعماري والتحليل الهيكلي لمنصة DZ ForensiGuard باستخدام لغة النمذجة الموحدة (UML)، مبيناً مخططات حالات الاستخدام، الفئات، والتسلسل، إلى جانب تصميم سجل التدقيق لسلسلة العهدة.
- **يعرض الفصل الرابع:** النتائج العملية واختبارات الأداء لمنصة DZ ForensiGuard، موثقاً بيئة التطوير، قاعدة البيانات، خوارزميات التحليل المنفذة، وواجهات المنصة التفاعلية، مع تقديم دراسة تقييمية مقارنة مع الأنظمة التجارية العالمية.

الفصل الأول: الأمن المعلوماتي والأمن السيبراني

مقدمة الفصل الأول

يتناول هذا الفصل الأساسيات النظرية للأمن المعلوماتي والأمن السيبراني، حيث يتم تعريف كل منهما وبيان العلاقة التكاملية بينهما، ثم استعراض الأهداف الرئيسية للأمن المعلوماتي وعناصره الأساسية، بالإضافة إلى تحليل أهم التهديدات السيبرانية التي تواجه الأنظمة الحديثة. كما يتطرق الفصل إلى مفهوم التحليل الجنائي الرقمي وأهدافه، وعلاقته بالأمن السيبراني وكذا التحديات التي تواجه هذا المجال، وذلك تمهيداً للدراسة المفصلة في الفصل الثاني.

1.1 تعريف الأمن المعلوماتي

يُعرف الأمن المعلوماتي بأنه مجموعة من السياسات والإجراءات والتقنية والتنظيمية التي تهدف إلى حماية المعلومات من الوصول غير المصرح به أو التعديل أو الإتلاف، مع ضمان استمرارية توفرها عند الحاجة [1][2]. ولا يقتصر هذا المفهوم على حماية البيانات فقط، بل يشمل أيضاً حماية الأنظمة والأجهزة والبنية التحتية [3][4].

ويشمل الأمن المعلوماتي مختلف مراحل دورة حياة البيانات، بدءاً من تخزينها، مروراً بمعالجتها، وصولاً إلى نقلها عبر الشبكات [5][6]، مما يجعله إطاراً شاملاً يهدف إلى تقليل المخاطر وضمان استمرارية عمل الأنظمة.

2.1 تعريف الأمن السيبراني

يُعد الأمن السيبراني أحد أهم فروع الأمن المعلوماتي، حيث يركز بشكل خاص على حماية الأنظمة الرقمية والشبكات من الهجمات الإلكترونية التي أصبحت أكثر تعقيداً وتطوراً [7]. وفقاً للاتحاد الدولي للاتصالات، يشمل هذا المجال مجموعة من التقنيات والممارسات التي تهدف إلى حماية البرمجيات والأجهزة والشبكات من الاختراقات والبرمجيات الخبيثة [7].

ويُعنى الأمن السيبراني بحماية الفضاء الإلكتروني ككل، حيث يعمل على تأمين البيانات أثناء انتقالها عبر الشبكات، ومنع الوصول غير المشروع إلى الأنظمة، إضافة إلى التصدي للهجمات [8].

3.1 العلاقة بين الأمن المعلوماتي والأمن السيبراني

يرتبط الأمن السيبراني ارتباطاً وثيقاً بالأمن المعلوماتي، حيث يُعتبر جزءاً منه، غير أن لكل منهما نطاقه الخاص. فبينما يشمل الأمن المعلوماتي حماية جميع أنواع المعلومات سواء كانت رقمية أو ورقية، يركز الأمن السيبراني بشكل أساسي على حماية الأنظمة الرقمية والبنية التحتية المرتبطة بها [1].

ومن هذا المنطلق، يمكن اعتبار الأمن السيبراني امتداداً عملياً للأمن المعلوماتي في البيئة الرقمية [7]، حيث يساهم في تطبيق السياسات الأمنية وحماية الأنظمة من التهديدات الإلكترونية [5].

4.1 أهداف الأمن المعلوماتي

يرتكز الأمن المعلوماتي على مجموعة من الأهداف الأساسية التي تهدف إلى ضمان حماية المعلومات والحفاظ على استمرارية الأنظمة، وتُعرف بنموذج (CIA Triad)، والذي يشمل السرية والسلامة والتوفر [1][5]. كما تم توسيع هذا النموذج ليشمل عناصر إضافية مثل المصادقة وعدم الإنكار [3].

1.4.1 السرية (Confidentiality)

تعد السرية من أهم ركائز الأمن المعلوماتي، حيث تشير إلى حماية المعلومات من الوصول غير المصرح به، وضمان أن البيانات لا يمكن الاطلاع عليها إلا من قبل الأشخاص المخولين فقط [1]. وتزداد أهمية هذا العنصر في الأنظمة التي تتعامل مع بيانات حساسة. ويتم تحقيق السرية من خلال استخدام تقنيات متعددة، من أبرزها التشفير الذي يسمح بتحويل البيانات إلى شكل غير قابل للقراءة إلا باستخدام مفتاح خاص، إضافة إلى أنظمة التحكم في الوصول [3].

2.4.1 السلامة (Integrity)

تشير السلامة إلى الحفاظ على دقة البيانات ومنع التلاعب بها أو تعديلها بطريقة غير مصرح بها، حيث يجب أن تبقى المعلومات صحيحة وموثوقة طوال دورة حياتها [1]. ويُعد هذا العنصر أساسياً في الأنظمة التي تعتمد على دقة البيانات. ويتم ضمان سلامة البيانات من خلال استخدام تقنيات مثل الدوال التجزئية (Hash Functions)، التي تسمح بالكشف عن أي تغيير في البيانات، إضافة إلى التوقيع الرقمي [5].

3.4.1 التوفر (Availability)

يعني التوفر ضمان إمكانية الوصول إلى المعلومات والأنظمة في الوقت المناسب دون انقطاع، وهو عنصر أساسي لضمان استمرارية الخدمات، خاصة في الأنظمة الحيوية [1].

ويتم تحقيق التوفر من خلال الاعتماد على تقنيات متعددة، مثل النسخ الاحتياطي، والخوادم الاحتياطية، وأنظمة الحماية من الهجمات [8]. ومن أبرز التهديدات التي تؤثر على هذا العنصر هجمات حجب الخدمة (DDoS).

4.4.1 المصادقة (Authentication)

تُشير المصادقة إلى عملية التحقق من هوية المستخدم أو النظام قبل السماح له بالوصول إلى الموارد، حيث تهدف إلى التأكد من أن الشخص الذي يحاول الدخول هو بالفعل من يدّعي أنه [3].

وتعتمد المصادقة على عدة وسائل، مثل كلمات المرور، أو القياسات الحيوية، أو التحقق الثنائي (Two-Factor Authentication) [5].

ويُعد هذا العنصر مهماً جداً في منع الوصول غير المشروع.

5.4.1 عدم الإنكار (Non-repudiation)

يُقصد بعدم الإنكار ضمان عدم قدرة أي طرف على إنكار قيامه بعملية معينة داخل النظام، مثل إرسال رسالة أو تنفيذ معاملة مالية. ويُعد هذا العنصر مهماً في المعاملات الإلكترونية [3].

ويتم تحقيق عدم الإنكار من خلال استخدام التوقيع الرقمي المعتمد على البنية التحتية للمفاتيح العامة (PKI).

5.1 عناصر الأمن المعلوماتي

يعتمد الأمن المعلوماتي على مجموعة من العناصر الأساسية التي تُشكل منظومة متكاملة تهدف إلى حماية المعلومات من مختلف التهديدات [1]. ولا يمكن تحقيق نظام أمني فعال إلا من خلال تأمين جميع هذه العناصر بشكل متوازن طبقاً للمعايير الدولية المعتمدة [9]. وتشمل هذه العناصر المستخدم والأجهزة والبرمجيات والشبكات والبيانات [5].

1.5.1 المستخدم (User)

يُعتبر المستخدم أحد أهم عناصر الأمن المعلوماتي، بل ويُعد في كثير من الأحيان الحلقة الأضعف في النظام الأمني [1]. فحتى مع وجود أنظمة حماية متقدمة، يمكن أن يؤدي خطأ بسيط من المستخدم إلى اختراق النظام [8].

لذلك، يُعد توعية المستخدمين وتدريبهم على أساليب الأمن السيبراني من أهم الإجراءات الوقائية.

2.5.1 الأجهزة (Hardware)

تشمل الأجهزة جميع المكونات المادية التي تُستخدم في معالجة وتخزين البيانات، مثل الحواسيب، الخوادم، الهواتف الذكية، وأجهزة الشبكة [5]. وتُعد هذه الأجهزة هدفاً مباشراً للهجمات.

يتطلب تأمين الأجهزة اتخاذ مجموعة من الإجراءات، مثل استخدام أنظمة حماية مادية، وتحديث البرامج الثابتة بشكل دوري، وتقييد الوصول المادي [8].

3.5.1 البرمجيات (Software)

تمثل البرمجيات العنصر الذي يتحكم في تشغيل الأجهزة وإدارة البيانات، وتشمل أنظمة التشغيل، التطبيقات، وقواعد البيانات [3]. وتُعد البرمجيات من أكثر العناصر عرضة للهجمات.

لذلك، يُعد تحديث البرمجيات بشكل مستمر من أهم الإجراءات الأمنية، حيث يتم إصلاح الثغرات المكتشفة بشكل دوري.

4.5.1 الشبكات (Networks)

تُعتبر الشبكات الوسيلة التي يتم من خلالها نقل البيانات بين الأنظمة المختلفة، سواء داخل المؤسسة أو عبر الإنترنت. ونظراً لطبيعتها

المفتوحة، فإنها تُعد من أكثر العناصر عرضة للهجمات [8].

يتم تأمين الشبكات باستخدام مجموعة من الأدوات والتقنيات، مثل الجدران النارية (Firewalls)، وأنظمة كشف التسلل، والتشفير، والشبكات الافتراضية الخاصة (VPN).

5.5.1 البيانات (Data)

تُعد البيانات الهدف الأساسي للأمن المعلوماتي، حيث تسعى جميع الإجراءات الأمنية إلى حمايتها من التسريب أو التعديل أو الفقدان [3]. وتشمل البيانات جميع أنواع المعلومات.

يتطلب تأمين البيانات استخدام تقنيات مثل التشفير، والنسخ الاحتياطي، وإدارة الوصول، بالإضافة إلى تصنيف البيانات حسب درجة حساسيتها.

6.1 التهديدات السيبرانية

تُعد التهديدات السيبرانية من أبرز التحديات التي تواجه الأنظمة المعلوماتية، حيث تتطور بشكل مستمر [8]. وتشمل هذه التهديدات مجموعة واسعة من الهجمات التي تهدف إلى اختراق الأنظمة، أو سرقة البيانات، أو تعطيل الخدمات.

ومن بين أهم هذه التهديدات، البرمجيات الخبيثة، والتصيد الاحتيالي، وهجمات حجب الخدمة، والهندسة الاجتماعية [8].

1.6.1 البرمجيات الخبيثة (Malware)

تُعرف البرمجيات الخبيثة بأنها برامج ضارة يتم تصميمها بهدف التسلل إلى الأنظمة المعلوماتية وإلحاق الضرر بها أو سرقة البيانات [8]. وتُعد من أخطر التهديدات السيبرانية.

وتشمل البرمجيات الخبيثة عدة أنواع، من بينها الفيروسات، وأحصنة طروادة، وبرامج الفدية، وبرامج التجسس.

2.6.1 التصيد الاحتيالي (Phishing)

يُعتبر التصيد الاحتيالي من أكثر الهجمات انتشاراً، حيث يعتمد على خداع المستخدمين من خلال إنشاء رسائل أو مواقع مزيفة تبدو وكأنها صادرة من جهات موثوقة، بهدف سرقة معلومات حساسة [8].

وتكمن خطورة هذا النوع من الهجمات في اعتماده على العامل البشري بدلاً من استغلال الثغرات التقنية [1].

3.6.1 هجمات حجب الخدمة (DDoS)

تُعد هجمات حجب الخدمة الموزعة (DDoS) من الهجمات التي تستهدف تعطيل الأنظمة والخدمات من خلال إغراق الخوادم بعدد هائل من الطلبات [8].

ويتم تنفيذ هذا النوع من الهجمات باستخدام شبكة من الأجهزة المخترقة، تُعرف باسم Botnet.

4.6.1 الهندسة الاجتماعية (Social Engineering)

تعتمد الهندسة الاجتماعية على استغلال العامل البشري بدلاً من استغلال الثغرات التقنية، حيث يقوم المهاجم بالتلاعب بالضحية نفسياً للحصول على معلومات حساسة أو الوصول إلى النظام [1].

ويُعد هذا النوع من الهجمات من أخطر التهديدات، لأنه يعتمد على الثقة والخداع، مما يجعل اكتشافه أكثر صعوبة [8].

7.1 الإشكالية

في ظل التحول الرقمي المتسارع، أصبحت الأنظمة المعلوماتية تمثل العمود الفقري لمختلف القطاعات الحيوية. وقد أدى هذا الاعتماد المتزايد إلى تضاعف حجم البيانات الرقمية، وتعقيد البنية التحتية للأنظمة، مما جعلها أكثر عرضة للتهديدات السيبرانية [8]. ومع تطور أساليب الهجوم، لم تعد الجرائم الإلكترونية تقتصر على محاولات اختراق بسيطة، بل أصبحت تعتمد على تقنيات متقدمة مثل التشفير، وإخفاء الهوية [8]. كما أن المهاجمين أصبحوا يستغلون نقاط الضعف البشرية والتقنية على حد سواء [1]. في هذا السياق، تواجه المؤسسات تحدياً كبيراً يتمثل في عدم كفاية الوسائل التقليدية في اكتشاف هذه الجرائم أو تحليلها بشكل دقيق. ومن هنا برزت الحاجة إلى تقنيات متقدمة مثل التحليل الجنائي الرقمي.

وبناءً على ما سبق، تتمحور إشكالية هذه الدراسة حول التساؤل الرئيسي التالي:

كيف يمكن تصميم وتنفيذ منصة تحليل جنائي رقمي متخصصة للهواتف الذكية (DZ ForensiGuard)

تكون قادرة على استخراج وتحليل الأدلة الرقمية من أجهزة Android بدقة وكفاءة عالية؟

8.1 التحليل الجنائي الرقمي (Digital Forensics)

1.8.1 تعريف التحليل الجنائي الرقمي

يُصنّف التحليل الجنائي الرقمي ضمن مجال الأمن السيبراني، حيث يهتم بدراسة وتحليل الأدلة الرقمية المرتبطة بالجرائم الإلكترونية [5]. ويُعرّف بأنه عملية منهجية علمية تشمل جمع الأدلة الرقمية وحفظها وتحليلها وتقديمها بطريقة تحافظ على سلامتها [10].

لا يقتصر هذا المجال على استرجاع البيانات المحذوفة، بل يتعداه إلى تحليلها وفهم سياقها الزمني والتقني، بهدف إعادة بناء الأحداث [5].

يعتمد التحليل الجنائي الرقمي على مجموعة من المعايير الصارمة، من أهمها العمل على نسخ من البيانات بدلاً من الأصل، والحفاظ على سلسلة الحيازة (Chain of Custody).

2.8.1 أهداف التحليل الجنائي الرقمي

يهدف التحليل الجنائي الرقمي إلى تحقيق مجموعة من الأهداف الأساسية [10]، ومن أهمها:

- كشف الجرائم الإلكترونية (Cybercrime Detection): تحليل البيانات الرقمية لاكتشاف الأنشطة غير المشروعة [8].
- تحديد مصدر الهجوم (Attack Attribution): تحليل سجلات النظام وحركة الشبكة لتتبع مسار الهجوم [10].
- استرجاع البيانات المحذوفة (Data Recovery): استخدام أدوات متخصصة لاستعادة الملفات المحذوفة التي قد تحتوي على أدلة مهمة.
- دعم التحقيقات القضائية (Legal Support): تقديم أدلة رقمية موثقة وفق معايير قانونية.

3.8.1 العلاقة بين التحليل الجنائي الرقمي والأمن السيبراني

تتجلى العلاقة بين التحليل الجنائي الرقمي والأمن السيبراني في كونهما مجالين متكاملين لحماية الأنظمة المعلوماتية [5]. حيث يركز الأمن السيبراني على الجانب الوقائي، بينما يهتم التحليل الجنائي الرقمي بالجانب التفاعلي والتحقيقي. يُعتبر الأمن السيبراني خط الدفاع الأول، في حين يمثل التحليل الجنائي الرقمي مرحلة الاستجابة والتحقيق لما بعد الهجوم.

4.8.1 التحديات في التحليل الجنائي الرقمي

يواجه مجال التحليل الجنائي الرقمي مجموعة من التحديات [8]، وقد تناولت عدة دراسات أكاديمية هذه التحديات في بيئات مختلفة كالحوسبة السحابية [11]. ومن أبرز هذه التحديات:

1.4.8.1 التشفير القوي (Strong Encryption)

تعتمد العديد من الأنظمة الحديثة على تقنيات تشفير متقدمة، مما يجعل الوصول إلى البيانات وتحليلها أمراً صعباً.

2.4.8.1 الحجم الكبير للبيانات (Big Data Volume)

تنتج الأجهزة الرقمية كميات ضخمة من البيانات، مما يجعل عملية جمع الأدلة وتحليلها معقدة وتحتاج إلى وقت.

3.4.8.1 تطور أساليب الهجوم (Advanced Cyber Attacks)

يعمل المهاجمون على تطوير تقنيات متقدمة لإخفاء أثارهم، مما يصعب عملية تتبع الأدلة.

4.4.8.1 نقص الخبرة التقنية (Lack of Technical Expertise)

يتطلب التحليل الجنائي الرقمي مهارات متعددة، ونقص الخبرة يمكن أن يؤدي إلى أخطاء في التحليل.

9.1 خاتمة الفصل الأول

أرسى هذا الفصل القواعد المعرفية والإطارات النظرية للأمن السيبراني، موضحاً الترابط العضوي بين حماية المعلومات والتحليل الجنائي الرقمي. لقد مكننا استعراض التهديدات والتحديات الراهنة من إدراك الدور المحوري للاستقصاء الرقمي ليس كأداة دفاعية فحسب، بل كمنهجية علمية لكشف الحقائق الرقمية. إن هذا التأسيس النظري يُشكل المنطلق الضروري للانتقال إلى الفصل الثاني، حيث سنقوم بمسح الأدوات والتقنيات التي تُترجم هذه المبادئ إلى واقع تطبيقي في مجال التحقيق الجنائي الرقمي.

الفصل الثاني: Digital Forensics - التحليل الجنائي الرقمي

مقدمة الفصل الثاني

يتناول هذا الفصل مفهوم التحليل الجنائي الرقمي وأهميته في مجال الأمن السيبراني، حيث يتم تعريفه وبيان المبادئ الأساسية التي يقوم عليها. ثم يتم استعراض مراحل التحليل الجنائي الرقمي المختلفة بشكل تفصيلي، بالإضافة إلى أنواعه المتعددة التي تشمل تحليل الأقراص والذاكرة والهواتف والشبكات وقواعد البيانات. كما يتطرق الفصل إلى أهم الأدوات المستخدمة في هذا المجال، سواء مفتوحة المصدر أو التجارية، مع تقديم مقارنة علمية وتحليل نقدي لها. وأخيراً، يتم استعراض التقنيات الحديثة في التحليل الجنائي الرقمي، مع التركيز بشكل خاص على دور الذكاء الاصطناعي في تطوير هذا المجال.

1.2 مفهوم التحليل الجنائي الرقمي

يُعرف التحليل الجنائي الرقمي بأنه تطبيق الأساليب العلمية والتقنية لتحديد، جمع، فحص، وتحليل الأدلة الرقمية، مع الحفاظ على سلامة البيانات وضمان توثيقها بطريقة تتيح استخدامها أمام الجهات القضائية [10][12]. كما يمثل هذا المجال نقطة تقاطع بين التقنيات المعلوماتية والإجراءات القانونية، حيث يعتمد على منهجيات دقيقة تضمن موثوقية النتائج وصحتها [13].

ويرتكز التحليل الجنائي الرقمي على مجموعة من المبادئ الأساسية، أهمها:

- عدم تغيير الأدلة الرقمية أثناء عملية التحليل؛

- الحفاظ على مبدأ سلسلة الحيازة؛

- توثيق جميع مراحل التحقيق بشكل دقيق ومنهجي [12].

2.2 المبادئ الأساسية للتحليل الجنائي الرقمي

يعتمد التحليل الجنائي الرقمي على مجموعة من المبادئ الأساسية التي تضمن مصداقية النتائج وسلامة الأدلة الرقمية [10][13]، ومن أهمها:

يقضي هذا المبدأ بضرورة الحفاظ على الأدلة الرقمية دون أي تعديل أو تغيير أثناء جميع مراحل التحليل، سواء عند الجمع أو الفحص

أو التخزين [12]. ولضمان ذلك، تُستخدم خوارزميات التجزئة (Hashing) مثل MD5 و SHA-256، حيث يتم إنشاء بصمة رقمية للبيانات تسمح بالكشف عن أي تغيير قد يطرأ عليها [10].

1.2.2 مبدأ التوثيق

يرتكز هذا المبدأ على تسجيل جميع خطوات التحقيق بشكل دقيق ومنهجي، بدءاً من عملية جمع الأدلة إلى غاية تحليلها واستخراج النتائج [13]. ويُعد التوثيق عنصراً أساسياً لضمان الشفافية، كما يتيح إمكانية مراجعة الإجراءات والتحقق من صحتها عند الحاجة [12].

2.2.2 مبدأ القابلية لإعادة

يفرض هذا المبدأ المعياري ضرورة مطابقة النتائج عند إعادة تنفيذ نفس الإجراءات التقنية باستخدام نفس الأدوات والمنهجية على نسخة الأدلة الجنائية الأصلية [10]. وتعد القابلية لإعادة الإنتاج (Reproducibility) شرطاً تقنياً جوهرياً لضبط جودة العمليات الجنائية وضمان صحة وموثوقية الأدلة المستخلصة أمام الهيئات الفنية والقضائية [13].

3.2 مراحل التحليل الجنائي الرقمي

تمر عملية التحليل الجنائي الرقمي بعدة مراحل أساسية، يتم اتباعها بشكل منهجي لضمان دقة النتائج وسلامة الأدلة [10][12]:

1.3.2 التعرف على الحادث (Identification)

تُعد هذه المرحلة الأولى في عملية التحقيق، حيث يتم تحديد طبيعة الحادث أو الهجوم الإلكتروني، مثل الاختراق أو تسريب البيانات أو استخدام برمجيات خبيثة [12]. كما يتم تحديد نطاق التحقيق والأجهزة أو الأنظمة المعنية، بهدف توجيه باقي مراحل التحليل بشكل صحيح [10].

2.3.2 جمع الأدلة (Collection)

في هذه المرحلة يتم جمع البيانات الرقمية من المصادر المختلفة مثل الأقراص الصلبة أو الذاكرة أو الشبكات، باستخدام أدوات متخصصة مثل FTK Imager وأداة dd في أنظمة Linux [12].

ويُشترط أثناء الجمع عدم التعامل مباشرة مع البيانات الأصلية، بل يتم إنشاء نسخة طبق الأصل (Forensic Image) لضمان الحفاظ على سلامة الأدلة [13].

3.3.2 حفظ الأدلة (Preservation)

تهدف هذه المرحلة إلى حماية الأدلة الرقمية من أي تغيير أو تلف [10]. ويتم ذلك من خلال إنشاء قيم تجزئة (Hash) مثل MD5 أو SHA-256 للتحقق من سلامة البيانات، بالإضافة إلى أجهزة تمنع الكتابة على وسائط التخزين (Write Blocker) [13].

كما يتم الالتزام بمبدأ سلسلة الحيازة لضمان توثيق كل من تعامل مع الأدلة [12].

4.3.2 الفحص (Examination)

تتضمن هذه المرحلة معالجة البيانات المستخرجة بهدف استخراج المعلومات المفيدة، وتشمل استرجاع الملفات المحذوفة، تحليل سجلات

النظام (Logs)، والبحث عن كلمات مفتاحية مرتبطة بالحدث [10].

ويتم استخدام أدوات تحليل متقدمة تساعد في تنظيم البيانات وتصفية المعلومات غير المهمة [12].

5.3.2 التحليل (Analysis)

في هذه المرحلة يتم تفسير النتائج المستخرجة وربط الأدلة ببعضها البعض من أجل فهم كيفية وقوع الهجوم [12].

يشمل ذلك بناء تسلسل زمني للأحداث (Timeline)، تحديد مصدر الهجوم، ومحاولة التعرف على الفاعل أو الجهة المسؤولة [10].

6.3.2 التقرير (Reporting)

تُعد المرحلة النهائية، حيث يتم إعداد تقرير مفصل يوضح جميع خطوات التحقيق والنتائج المتوصل إليها [13].

ويتضمن التقرير الأدلة الرقمية، المنهجية المتبعة، والتحليل النهائي، ويجب أن يكون واضحاً ودقيقاً وقابلاً للفهم من طرف الجهات

القضائية [12].

4.2 أنواع التحليل الجنائي الرقمي (Digital Forensics Types)

ينقسم التحليل الجنائي الرقمي إلى عدة أنواع رئيسية، تختلف حسب طبيعة البيانات ومصدرها، حيث يركز كل نوع على بيئة محددة لجمع

وتحليل الأدلة الرقمية [10][12].

1.4.2 تحليل الأقراص (Disk Forensics)

يُعتبر تحليل الأقراص من أقدم وأهم مجالات التحليل الجنائي الرقمي، حيث يركز على دراسة وسائط التخزين مثل الأقراص الصلبة

HDD والأقراص ذات الحالة الصلبة SSD [12].

يركز على:

• تحليل أنظمة الملفات مثل (NTFS, FAT)؛

• استرجاع البيانات المحذوفة؛

• تحليل تقسيمات القرص (Partitions)؛

• استخراج الأدلة المخفية [10].

يتم هذا النوع من التحليل باستخدام أدوات متخصصة تقوم بقراءة البيانات دون التأثير عليها، مع الحفاظ على سلامة الأدلة الرقمية [13].

2.4.2 تحليل الذاكرة (Memory Forensics)

يركز تحليل الذاكرة على دراسة البيانات الموجودة في ذاكرة الوصول العشوائي (RAM)، والتي تحتوي على معلومات مؤقتة لكنها ذات

قيمة عالية أثناء التحقيق [12].

يُستخدم لاكتشاف:

• البرمجيات الخبيثة (Malware) داخل الذاكرة؛

• العمليات النشطة (Running Processes)؛

• مفاتيح التشفير والبيانات الحساسة؛

• الاتصالات الجارية [10].

يُعتبر هذا النوع من التحليل مهماً لأنه يكشف معلومات لا يمكن العثور عليها في القرص الصلب [12].

الأدوات:

• **Volatility**: تُعد أداة Volatility من أشهر وأقوى الأدوات في مجال التحليل الجنائي الرقمي، حيث تُستخدم لتحليل الذاكرة العشوائية

RAM واستخراج الأدلة الرقمية منها [14].



شكل 1.2: شعار أداة Volatility

3.4.2 تحليل الهواتف (Mobile Forensics)

يُعنى تحليل الهواتف باستخراج وتحليل البيانات من الأجهزة المحمولة مثل الهواتف الذكية، والتي تُعد مصدراً غنياً بالأدلة

الرقمية [15][16].

يشمل:

• استخراج الرسائل النصية والمحادثات؛

• تحليل التطبيقات المثبتة؛

• استرجاع الصور والملفات؛

• تحليل سجلات المكالمات [12].

يُستخدم هذا النوع بشكل واسع في التحقيقات الجنائية نظراً لأهمية البيانات الشخصية المخزنة في الهواتف [15]، مع وجود تحديات تقنية وقانونية إضافية في البيئة العربية [17].

4.4.2 تحليل الشبكات (Network Forensics)

يركز تحليل الشبكات على دراسة حركة البيانات داخل الشبكات، بهدف اكتشاف الأنشطة المشبوهة أو الهجمات الإلكترونية [10]. ويتم ذلك من خلال تحليل الحزم (Packets) وسجلات الشبكة، مما يسمح بتتبع الاتصالات وتحديد مصدر الهجوم.

كما يساعد هذا النوع من التحليل في فهم كيفية انتقال البيانات بين الأنظمة، والكشف عن محاولات الاختراق أو تسريب المعلومات [12]. ويُستخدم بشكل واسع في تحليل الهجمات التي تستهدف البنية التحتية للشبكات.

5.4.2 تحليل قواعد البيانات (Database Forensics)

يركز تحليل قواعد البيانات على فحص وتقييم محتويات قواعد البيانات للكشف عن الأنشطة غير المشروعة، مثل التلاعب بالبيانات أو الوصول غير المصرح به [12]. يتضمن ذلك تحليل سجلات المعاملات (Transaction Logs) واسترجاع السجلات المحذوفة أو المعدلة [10].

5.2 أدوات التحليل الجنائي الرقمي

تُعد أدوات التحليل الجنائي الرقمي عنصراً محورياً في تنفيذ مختلف مراحل التحقيق الرقمي، بدءاً من جمع الأدلة وصولاً إلى تحليلها وتقديمها بشكل قانوني [12]. ويعتمد اختيار الأداة على طبيعة القضية، نوع البيانات، والبيئة التقنية المستهدفة، مع ضرورة الالتزام بالمعايير الدولية لضمان سلامة الأدلة الرقمية وقابليتها للاستخدام القضائي [10].

1.5.2 الأدوات مفتوحة المصدر

تتميز الأدوات مفتوحة المصدر بمرونتها وإمكانية تخصيصها، إضافة إلى كونها متاحة دون تكلفة، مما يجعلها مناسبة للأغراض التعليمية والبحثية، وكذلك لبعض الاستخدامات المهنية [18][19].

Autopsy 1.1.5.2

تُعد Autopsy من أشهر منصات التحليل الجنائي الرقمي مفتوحة المصدر، حيث توفر واجهة رسومية تسهل على المحققين تحليل الأدلة الرقمية دون الحاجة إلى خبرة متقدمة في سطر الأوامر [19]. تعتمد الأداة على محرك The Sleuth Kit، وتُستخدم بشكل رئيسي في تحليل الأقراص الصلبة واستخراج الملفات المحذوفة، إضافة إلى تحليل أنظمة الملفات المختلفة.

كما يتيح Autopsy إنشاء تسلسل زمني (Timeline) للأحداث الرقمية، مما يساعد في إعادة بناء الوقائع بدقة، وهو عنصر أساسي

في التحقيقات الجنائية الرقمية [12].



شكل 2.2: واجهة برنامج Autopsy للتحليل الجنائي الرقمي

The Sleuth Kit 2.1.5.2

يُعتبر The Sleuth Kit مجموعة أدوات تعتمد على سطر الأوامر (CLI)، وتُستخدم لإجراء تحليل منخفض المستوى لأنظمة الملفات [18]. تتيح هذه الأداة فحص الأقراص الرقمية واستخراج البيانات المخفية أو المحذوفة بطريقة دقيقة، مما يجعلها مناسبة للمستخدمين ذوي الخبرة التقنية العالية.

وتكمن أهميتها في قدرتها على التعامل المباشر مع البنية الداخلية لأنظمة الملفات، وهو ما يسمح باكتشاف آثار رقمية قد لا تظهر في الأدوات ذات الواجهات الرسومية [12].

Wireshark 3.1.5.2

يُعد Wireshark من أبرز أدوات تحليل الشبكات، حيث يُستخدم لالتقاط وتحليل حزم البيانات (Packets) المارة عبر الشبكة [20]. ويسمح هذا التحليل بالكشف عن الأنشطة المشبوهة، مثل محاولات الاختراق أو تسريب البيانات. وتكمن أهميته في مجال التحليل الجنائي الرقمي للشبكات (Network Forensics)، حيث يمكن من خلاله تتبع مصدر الهجوم وفهم سلوك المهاجم داخل الشبكة [10].

2.5.2 الأدوات التجارية

تُستخدم الأدوات التجارية بشكل واسع في المؤسسات الأمنية والجهات القضائية، نظراً لدعمها الفني، وموثوقيتها العالية، واعتمادها القانوني في العديد من الدول [21][22].

EnCase Forensic 1.2.5.2

تُعتبر EnCase من الأدوات الرائدة في مجال التحليل الجنائي الرقمي، حيث تُستخدم بشكل واسع من قبل جهات إنفاذ القانون [21]. تتميز بقدرتها على جمع الأدلة الرقمية وتحليلها بطريقة تضمن الحفاظ على سلامتها، مما يجعلها مقبولة في المحاكم.

كما توفر الأداة إمكانيات متقدمة في تحليل البيانات، بما في ذلك استرجاع الملفات المحذوفة وتحليل أنظمة التشغيل المختلفة، مع الحفاظ



شكل 3.2: واجهة برنامج Wireshark لتحليل حزم الشبكة

على سلسلة الحيازة (Chain of Custody) [12].

Forensic Toolkit (FTK) 2.2.5.2

تُعرف FTK بكفاءتها العالية في معالجة كميات كبيرة من البيانات بسرعة، حيث تعتمد على تقنيات الفهرسة (Indexing) التي تسمح بالبحث السريع داخل البيانات الرقمية [22].

كما تُستخدم في تحليل قواعد البيانات، واسترجاع الملفات، وفك التشفير في بعض الحالات، مما يجعلها أداة فعالة في التحقيقات التي تتطلب سرعة في تحليل الأدلة الرقمية [10].

3.5.2 مقارنة علمية بين الأدوات

يمكن إجراء مقارنة موضوعية بين الأدوات السابقة بناءً على معايير مثل سهولة الاستخدام، الأداء، والاعتماد القانوني [12]:

جدول 1.2: مقارنة بين أدوات التحليل الجنائي الرقمي

الأداة	النوع	نقاط القوة	الاستخدام الأنسب
Autopsy	مفتوحة المصدر	سهولة الاستخدام، واجهة رسومية	التعليم والتحليل الأساسي
The Sleuth Kit	مفتوحة المصدر	تحليل منخفض المستوى	الخبراء والتحليل المتقدم
Wireshark	مفتوحة المصدر	تحليل الشبكات	التحقيقات الشبكية
EnCase	تجارية	معتمدة قانونياً، شاملة	الجهات القضائية
FTK	تجارية	سرعة عالية في البحث	تحليل البيانات الضخمة

4.5.2 تحليل نقدي

رغم تعدد أدوات التحليل الجنائي الرقمي، إلا أنه لا توجد أداة واحدة قادرة على تغطية جميع جوانب التحقيق، مما يفرض على المحقق

استخدام مجموعة متكاملة من الأدوات حسب طبيعة الحالة [10].

فالأدوات مفتوحة المصدر توفر مرونة كبيرة وتكلفة منخفضة، لكنها قد تفتقر أحياناً إلى الدعم الرسمي أو الاعتماد القانوني. في المقابل، توفر الأدوات التجارية بيئة متكاملة وموثوقة، لكنها تكون مكلفة وتتطلب تراخيص خاصة [12].

وعليه، فإن الاختيار الأمثل يعتمد على التوازن بين الكفاءة التقنية، المتطلبات القانونية، والموارد المتاحة، وهو ما تؤكد عليه المعايير الدولية في مجال التحليل الجنائي الرقمي [13].

6.2 التقنيات الحديثة في التحليل الجنائي الرقمي

شهد مجال التحليل الجنائي الرقمي تطوراً ملحوظاً في السنوات الأخيرة نتيجة التقدم في تقنيات الحوسبة والذكاء الاصطناعي، مما ساهم في تحسين كفاءة تحليل الأدلة الرقمية والتعامل مع التعقيد المتزايد للجرائم السيبرانية [23][24]. وقد أصبح الاعتماد على هذه التقنيات ضرورة حتمية لمواكبة الحجم الكبير للبيانات وتطور أساليب الهجوم [25].

1.6.2 الذكاء الاصطناعي (Artificial Intelligence)

يُعد الذكاء الاصطناعي من أبرز التقنيات الحديثة المستخدمة في التحليل الجنائي الرقمي، حيث يساهم في أتمتة عمليات التحليل واستخراج الأنماط المخفية داخل البيانات [26]. ووفقاً لتعريف IBM، فإن الذكاء الاصطناعي يشير إلى الأنظمة القادرة على محاكاة الذكاء البشري في التعلم واتخاذ القرار [26].

في سياق التحليل الجنائي الرقمي، يُستخدم الذكاء الاصطناعي في عدة تطبيقات رئيسية، من بينها:

- تحليل الصور الرقمية: حيث يتم استخدام تقنيات التعلم العميق لاكتشاف التلاعب بالصور أو التعرف على الوجوه والأجسام داخل الأدلة الرقمية [25].

- اكتشاف الأنماط (Pattern Recognition): من خلال تحليل كميات كبيرة من البيانات لاستخراج سلوكيات غير طبيعية قد تشير إلى نشاط إجرامي [23].

- كشف الأنشطة المشبوهة: عبر بناء نماذج قادرة على التنبؤ بالهجمات أو التعرف على السلوك غير الطبيعي داخل الأنظمة [26].

وتشير الدراسات الحديثة، مثل أبحاث الذكاء الاصطناعي في التحليل الجنائي الرقمي، إلى أن استخدام هذه التقنيات يساهم في تقليل زمن التحقيق وزيادة دقة النتائج، خاصة في القضايا المعقدة [23]. كما تعتمد هذه التطبيقات على نماذج التعلم العميق التي تم تطويرها في مجال الذكاء الاصطناعي [25].

2.6.2 تحليل البيانات الضخمة (Big Data Analytics)

مع التزايد الهائل في حجم البيانات الناتجة عن الأنظمة الرقمية، أصبح تحليل البيانات الضخمة عنصراً أساسياً في التحليل الجنائي الرقمي [24]. ويشير مفهوم البيانات الضخمة إلى مجموعات البيانات التي تتميز بالحجم الكبير، والتنوع، والسرعة، مما يتطلب تقنيات متقدمة لمعالجتها [24].

في هذا الإطار، يساهم تحليل البيانات الضخمة في:

- معالجة كميات هائلة من البيانات: مثل سجلات الأنظمة (Logs) وحركة الشبكات، والتي قد تصل إلى ملايين السجلات اليومية [24].
- تحليل شامل وسريع للأدلة: من خلال استخدام خوارزميات متقدمة تسمح بالكشف عن العلاقات بين البيانات [23].
- تحسين دقة التحقيقات: عبر دمج مصادر بيانات متعددة للحصول على رؤية شاملة للحادثة [27].

وتكمن أهمية هذه التقنية في قدرتها على التعامل مع التعقيد الكبير للبيانات الرقمية الحديثة، حيث لم يعد من الممكن الاعتماد على الطرق التقليدية في التحليل [24]. كما تُستخدم بالتكامل مع تقنيات الذكاء الاصطناعي لتوفير تحليل أكثر دقة وفعالية [26].

3.6.2 تكامل التقنيات الحديثة

إن القيمة الحقيقية لهذه التقنيات تظهر عند تكاملها، حيث يُستخدم الذكاء الاصطناعي لتحليل البيانات الضخمة واستخراج الأنماط منها، مما يعزز من قدرة المحققين على كشف الجرائم الرقمية المعقدة [23]. ويساهم هذا التكامل في تحسين سرعة الاستجابة للحوادث وتقليل الأخطاء البشرية في عملية التحليل [24].

ومع ذلك، يطرح هذا التوجه تحديات تتعلق بخصوصية البيانات، ومتطلبات الحوسبة العالية، إضافة إلى ضرورة فهم نماذج الذكاء الاصطناعي وتفسير نتائجها بشكل دقيق، وهو ما يُعرف بإشكالية قابلية تفسير النماذج (Explainability) [28].

جدول 2.2: التقنيات الحديثة في التحليل الجنائي الرقمي: التطبيقات والتحديات

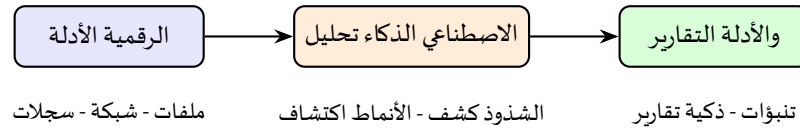
التقنية	التطبيقات	التحديات
الذكاء الاصطناعي	تحليل الصور، اكتشاف الأنماط، كشف الأنشطة المشبوهة	قابلية التفسير، الخصوصية
تحليل البيانات الضخمة	معالجة السجلات، تحليل الشبكات، تكامل المصادر	الحوسبة العالية، التخزين
التكامل بين التقنيتين	تحليل متقدم، استجابة سريعة، تقليل الأخطاء	تعقيد التنفيذ، التدريب المتخصص

7.2 التحليل الجنائي الرقمي باستخدام الذكاء الاصطناعي

شهد مجال التحليل الجنائي الرقمي تطوراً ملحوظاً مع ظهور تقنيات الذكاء الاصطناعي التي ساهمت في تحسين كفاءة التحقيقات الرقمية [23]. ويعتمد هذا التوجه على خوارزميات التعلم الآلي (Machine Learning) والتعلم العميق (Deep Learning) لمعالجة كميات هائلة من البيانات واكتشاف الأنماط المعقدة التي يصعب ملاحظتها يدوياً، مما يعزز من قدرة المحققين على اتخاذ قرارات دقيقة وسريعة في مواجهة الهجمات السيبرانية المتطورة [26][25].

1.7.2 دور الذكاء الاصطناعي في التحليل الجنائي الرقمي

يمكن توظيف تقنيات الذكاء الاصطناعي في مختلف مراحل التحليل الجنائي الرقمي، حيث توفر حلولاً متقدمة تدعم المحققين في التعامل



شكل 4.2: سير عمل مبسط للتحليل الجنائي باستخدام الذكاء الاصطناعي

مع الأدلة الرقمية بكفاءة عالية [23][26]، وذلك على النحو التالي:

1.1.7.2 جمع الأدلة الذكي (Smart Evidence Collection)

يساهم الذكاء الاصطناعي في تحسين مرحلة جمع الأدلة من خلال استخدام خوارزميات قادرة على تصنيف الملفات تلقائياً وفقاً لنوعها أو محتواها، مما يساعد في تحديد البيانات ذات الأهمية الجنائية بسرعة [23]. كما يمكن لهذه الأنظمة التعرف على الملفات المشبوهة بناءً على أنماط سلوكية أو خصائص معينة، مما يقلل من الوقت اللازم لفحص البيانات يدوياً [26].

2.1.7.2 التحليل التلقائي للأدلة (Automated Analysis)

تُعد مرحلة التحليل من أكثر المراحل تعقيداً، وهنا يبرز دور الذكاء الاصطناعي في تحليل كميات كبيرة من البيانات، مثل سجلات النظام (Logs) وحركة الشبكة، لاكتشاف السلوكيات غير الطبيعية [26]. وتعتمد هذه العملية على تقنيات التعلم الآلي التي تُدرَّب على التمييز بين الأنماط الطبيعية والأنشطة المشبوهة، مما يساهم في الكشف المبكر عن الهجمات السيبرانية [23].

كما يمكن استخدام تقنيات التعلم العميق لتحليل البيانات غير المهيكلة، مثل الصور أو النصوص، مما يعزز من قدرة التحليل الجنائي على التعامل مع مختلف أنواع الأدلة الرقمية [25].

3.1.7.2 التنبؤ بالهجمات (Attack Prediction)

من أهم التطبيقات المتقدمة للذكاء الاصطناعي في التحليل الجنائي الرقمي قدرته على التنبؤ بالهجمات قبل وقوعها، وذلك من خلال تحليل البيانات التاريخية واستخلاص الأنماط المرتبطة بالهجمات السابقة [23]. وتُستخدم خوارزميات التعلم الآلي لبناء نماذج تنبؤية تساعد في تحديد التهديدات المحتملة واتخاذ إجراءات استباقية للحد منها [26].

4.1.7.2 دعم اتخاذ القرار (Decision Support)

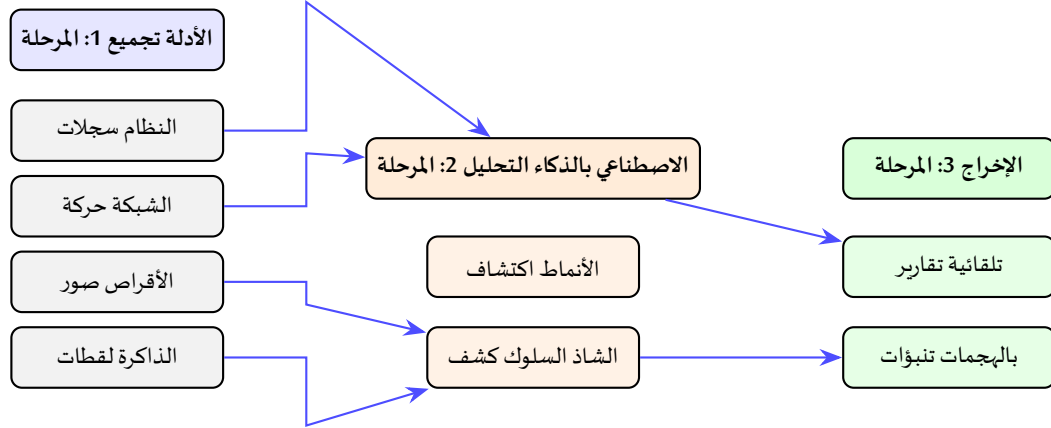
يساهم الذكاء الاصطناعي في تقديم توصيات مبنية على تحليل البيانات، مما يساعد المحققين في اتخاذ قرارات دقيقة خلال سير التحقيق [28]. كما يمكن لهذه الأنظمة ترتيب الأدلة حسب درجة أهميتها، مما يسهل عملية التركيز على المعلومات الأكثر تأثيراً في القضية [23].

جدول 3.2: تطبيقات الذكاء الاصطناعي في مراحل التحليل الجنائي الرقمي

المرحلة	التطبيق	التقنية المستخدمة
جمع الأدلة	تصنيف الملفات، التعرف على البيانات المشبوهة	التعلم الآلي
التحليل	كشف السلوكيات الشاذة، تحليل السجلات	التعلم العميق
التنبؤ	بناء نماذج للتنبؤ بالهجمات المستقبلية	خوارزميات التنبؤ
اتخاذ القرار	تقديم توصيات، ترتيب الأدلة حسب الأهمية	أنظمة الخبراء

5.1.7.2 مخطط سير عمل التحليل الجنائي بالذكاء الاصطناعي

لتوضيح كيفية تكامل تقنيات الذكاء الاصطناعي في عملية التحليل الجنائي الرقمي، يقدم الشكل 5.2 مخططاً يوضح سير العمل المقترح. يمر هذا السير بثلاث مراحل رئيسية: تجميع الأدلة، التحليل بواسطة وكلاء الذكاء الاصطناعي، ثم إخراج النتائج والتقارير.



شكل 5.2: سير عمل التحليل الجنائي الرقمي باستخدام تقنيات الذكاء الاصطناعي

يوضح هذا المخطط كيف يمكن للذكاء الاصطناعي أن يساهم في أتمتة عملية التحليل الرقمي، بدءاً من جمع الأدلة ومروراً بتحليلها واكتشاف الأنماط الشاذة، وانتهاءً بإنتاج تقارير تلقائية وتنبؤات بالهجمات المستقبلية [23][26].

8.2 خاتمة الفصل الثاني

رسم هذا الفصل خارطة تقنية شاملة لواقع التحليل الجنائي الرقمي، حيث تم من خلاله تشريح المبادئ الإجرائية والأدوات البرمجية المعاصرة. لقد كشف المسح المستفيض والتحليل النقدي للأدوات المتاحة عن فجوة ملموسة في التوازن بين سهولة الاستخدام ودعم الخصوصية اللغوية، بالإضافة إلى الحاجة المتزايدة لدمج خوارزميات الذكاء الاصطناعي بشكل أكثر استقلالية وفعالية. إن هذه الاستنتاجات العلمية تُشكل الأساس المنطقي الذي سيتم البناء عليه في الفصل الثالث، حيث سننتقل من التوصيف التقني الراهن إلى مرحلة النمذجة والتصميم المعماري لمنصة متكاملة تسعى لمعالجة هذه التحديات وتوفير بيئة تحليلية متطورة ومخصصة.

الفصل الثالث: التصميم والتحليل - نمذجة نظام DZ ForensiGuard

باستخدام UML

مقدمة الفصل الثالث

يتناول هذا الفصل التصميم النمطي لنظام DZ ForensiGuard، وهو منصة متكاملة للتحليل الجنائي الرقمي للهواتف المحمولة. سيتم استخدام لغة النمذجة الموحدة (UML) [29] لتوثيق متطلبات النظام، وتحليل وظائفه، وتصميم هيكله البرمجي. يشمل الفصل تحديد المتطلبات الوظيفية وغير الوظيفية، ثم تقديم مخططات حالة الاستخدام والفئات والتسلسل، وأخيراً تصميم هيكل سجل التدقيق لضمان سلامة الأدلة وسلسلة العهدة (Chain of Custody).

1.3 متطلبات النظام

1.1.3 المتطلبات الوظيفية

تمثل المتطلبات الوظيفية العمليات والوظائف الأساسية التي يجب أن يقوم بها النظام. يوضح الجدول 1.3 المتطلبات الوظيفية التي تم تحديدها وتصنيفها حسب الأولوية.

جدول 1.3: المتطلبات الوظيفية لنظام DZ ForensiGuard

المعرف	المتطلب الوظيفي	الأولوية
FR-01	نظام المصادقة والمصادقة الثنائية (المحملة) للتحكم في الوصول	عالية
FR-02	إنشاء وإدارة حالات التحقيق	عالية
FR-03	استخراج البيانات من هواتف (Android) و (iOS)	عالية
FR-04	عرض وتصفية الأدلة الرقمية المستخرجة	عالية
FR-05	تحليل الجدول الزمني للأحداث	متوسطة
FR-06	استخراج وتحليل المواقع الجغرافية	متوسطة
FR-07	بناء وتحليل شبكة العلاقات الاجتماعية	متوسطة
FR-08	توليد وتصدير التقارير الجنائية	عالية
FR-09	الموافقة على حسابات المحققين الجدد	عالية
FR-10	مراقبة وتسجيل نشاطات المحققين	عالية
FR-11	تحليل الانترنت وكشف الملفات المشفرة	متوسطة
FR-12	التحقق التلقائي من سلامة الأدلة	عالية

2.1.3 المتطلبات غير الوظيفية

تمثل المتطلبات غير الوظيفية الخصائص النوعية والقيود التي يجب أن يلتزم بها النظام، كما هو موضح في الجدول 2.3.

جدول 2.3: المتطلبات غير الوظيفية لنظام DZ ForensiGuard

المعرف	المتطلب	الوصف
NFR-01	النزاهة والموثوقية الجنائية	ضمان سلامة الأدلة عبر التشفير وحساب القيم التجزئية (Hashing)
NFR-02	الأداء والسرعة	استخراج البيانات وتحليلها في زمن قصير
NFR-03	التوافقية	التوافق مع (Android) و (iOS)
NFR-04	القابلية للتوسع	إمكانية دعم أجهزة وأنظمة جديدة
NFR-05	سهولة الاستخدام	واجهة مستخدم عربية تفاعلية
NFR-06	التوثيق	تسجيل جميع العمليات في سجل تدقيق
NFR-07	الموثوقية	نسخ احتياطي واستعادة تلقائية

2.3 نمذجة النظام - مخطط حالة الاستخدام

1.2.3 مخطط حالة الاستخدام

مخطط حالة الاستخدام هو أحد مخططات (UML) السلوكية التي تُستخدم لتوثيق وظائف النظام من منظور المستخدم [30].

يوضح الشكل 1.3 مخطط حالة الاستخدام المتكامل للنظام، والذي يبين التفاعلات بين الممثلين (المحقق ومدير النظام) وحالات الاستخدام المختلفة.

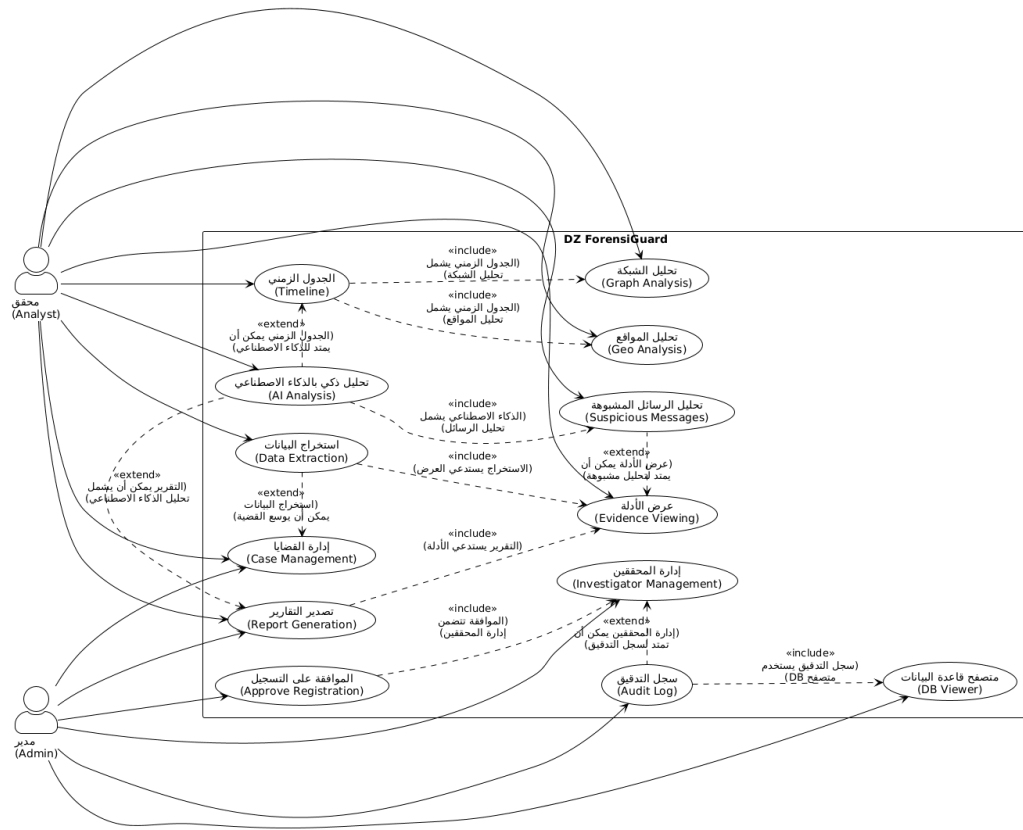
يتفاعل المحقق (Investigator) مع النظام لتنفيذ تسع وظائف رئيسية هي: تسجيل الدخول، إدارة حالات التحقيق، استخراج البيانات، عرض الأدلة، تحليل الجدول الزمني، تحليل المواقع الجغرافية، تحليل شبكة العلاقات، تحليل الرسائل المشبوهة، وتوليد التقارير. أما مدير النظام (Admin) فيمتلك صلاحيات إضافية تتضمن: إدارة المحققين، الموافقة على حسابات المحققين الجدد، مراقبة سجلات التدقيق، متصفح قاعدة البيانات، التحقق من سلامة الأدلة، وتحليل الاندروبيا. كما يتمتع المدير بصلاحيات الوصول إلى بعض وظائف المحقق مثل إدارة القضايا وتصدير التقارير.

أولاً: تحليل الممثلين

الممثلون هم الكيانات الخارجية التي تتفاعل مع النظام [31]. تم تحديد ثلاثة ممثلين رئيسيين:

1. المحقق (Investigator): المستخدم الأساسي للنظام، المسؤول عن تنفيذ عمليات التحقيق الفنية من استخراج البيانات إلى تحليلها وتوليد التقارير.

2. مدير النظام (Admin): المسؤول عن الإشراف الإداري والتقني، يتولى حماية سلسلة العهدة وإدارة حسابات المحققين، بالإضافة



شكل 1.3: مخطط حالة الاستخدام لنظام DZ ForensiGuard

إلى الإطلاع على سجلات التدقيق وقاعدة البيانات.

3. جهاز الهاتف (Mobile Device): الكيان الخارجى المادى المتصل عبر USB، سواء كان Android أو iOS.

ثانياً: الصلاحيات الحصرية للمدير

تم تخصيص ست صلاحيات لتكون حصرة للمدير:

1. إدارة المحققين: عرض قائمة المحققين وإضافة أو حذف حساباتهم.

2. الموافقة على حسابات المحققين: لا يسمح النظام بالتسجيل المباشر ، يبقى الحساب معلقاً حتى يوافق المدير عليه.

3. مراقبة سجل التدقيق (Audit Log): يقوم النظام بتوثيق كل عملية في سجل تدقيق غير قابل للتعديل، ويملك المدير صلاحية مراقبته.

4. متصفح قاعدة البيانات (Database Viewer): يمكن المدير من الاطلاع المباشر على محتويات قاعدة البيانات.

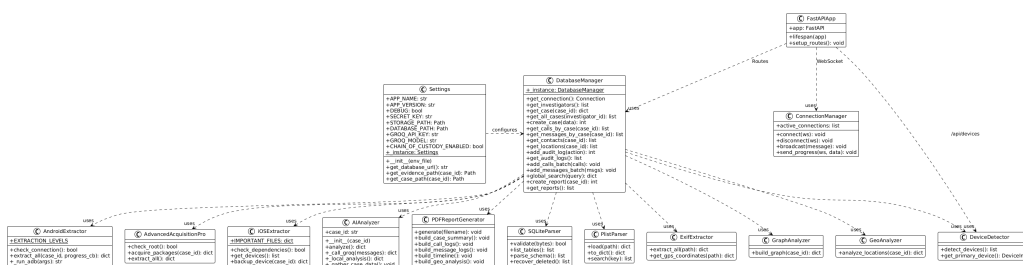
5. التحقق من سلامة الأدلة: مقارنة بصمة SHA-256 الحالية للأدلة بالبصمة الأصلية للكشف عن أي تلاعب.

6. تحليل الانتروبيا: حساب عشوائية البيانات في الملفات للكشف عن الملفات المشفرة أو المخفية.

3.3 نمذجة النظام - مخطط الفئات

1.3.3 مخطط الفئات

مخطط الفئات هو المخطط الأساسي في (UML) لتمثيل البنية الثابتة للنظام، ويوضح الفئات والعلاقات بينها [32].



شكل 2.3: مخطط الفئات الرئيسية في نظام DZ ForensiGuard

يوضح الشكل 2.3 الهيكل الكاملة للفئات في النظام. يعتمد النظام على عمارة متعددة الطبقات (Multi-layer Architecture).

حيث تم تقسيم الفئات إلى سبع طبقات رئيسية [33]:

1. طبقة الإعدادات والتكوين (Configuration Layer): تشمل فئة Settings التي تتبع نمط التصميم Singleton لإدارة إعدادات النظام مثل مسارات التخزين، مفاتيح API، وإعدادات الأمان.

2. طبقة اكتشاف الأجهزة (Device Detection Layer): تتولى اكتشاف الأجهزة المتصلة عبر USB وتحديد نوعها. تشمل فئات DeviceDetector.

3. طبقة استخراج البيانات (Extraction Layer): تتولى استخراج البيانات من الأجهزة. تشمل الفئة المجردة DataExtractor وفئتي AndroidExtractor و iOSExtractor، بالإضافة إلى فئة AdvancedAcquisitionPro.

4. طبقة التحليل (Analysis Layer): تتولى تحليل البيانات المستخرجة. تشمل خمس فئات رئيسية: GeoAnalyzer (تحليل المواقع)، GraphAnalyzer (تحليل الشبكات)، TimelineBuilder (الجدول الزمني)، EntropyAnalyzer (تحليل الانتروبيا)، و AIAnalyzer (تحليل الذكاء الاصطناعي).

5. طبقة معالجة البيانات (Data Processing Layer): تشمل فئات متخصصة لتحليل أنواع مختلفة من الملفات: SQLiteParser لتحليل قواعد البيانات، PlistParser لتحليل ملفات plist في أنظمة iOS، و ExifExtractor لاستخراج بيانات EXIF من الصور.

6. طبقة التحقق من السلامة والتقارير (Integrity and Reporting Layer): تتولى ضمان سلامة البيانات وسلسلة العهدة من خلال فئتي HashVerifier و MagicBytesDetector، بالإضافة إلى فئة PDFReportGenerator لتوليد التقارير بصيغة (PDF) وفئة ConnectionManager لإدارة اتصالات WebSocket.

7. طبقة قاعدة البيانات وواجهات (API): تشمل فئة DatabaseManager التي تدير جميع عمليات قاعدة البيانات، وفئة FastAPIApp التي تشكل نقطة الدخول الرئيسية لواجهات API.

يوضح المخطط أيضاً علاقات الاعتماد بين الفئات، حيث تعتمد فئة FastAPIApp على DatabaseManager و ConnectionManager و DeviceDetector، بينما تعتمد DatabaseManager على جميع فئات الاستخراج والتحليل.

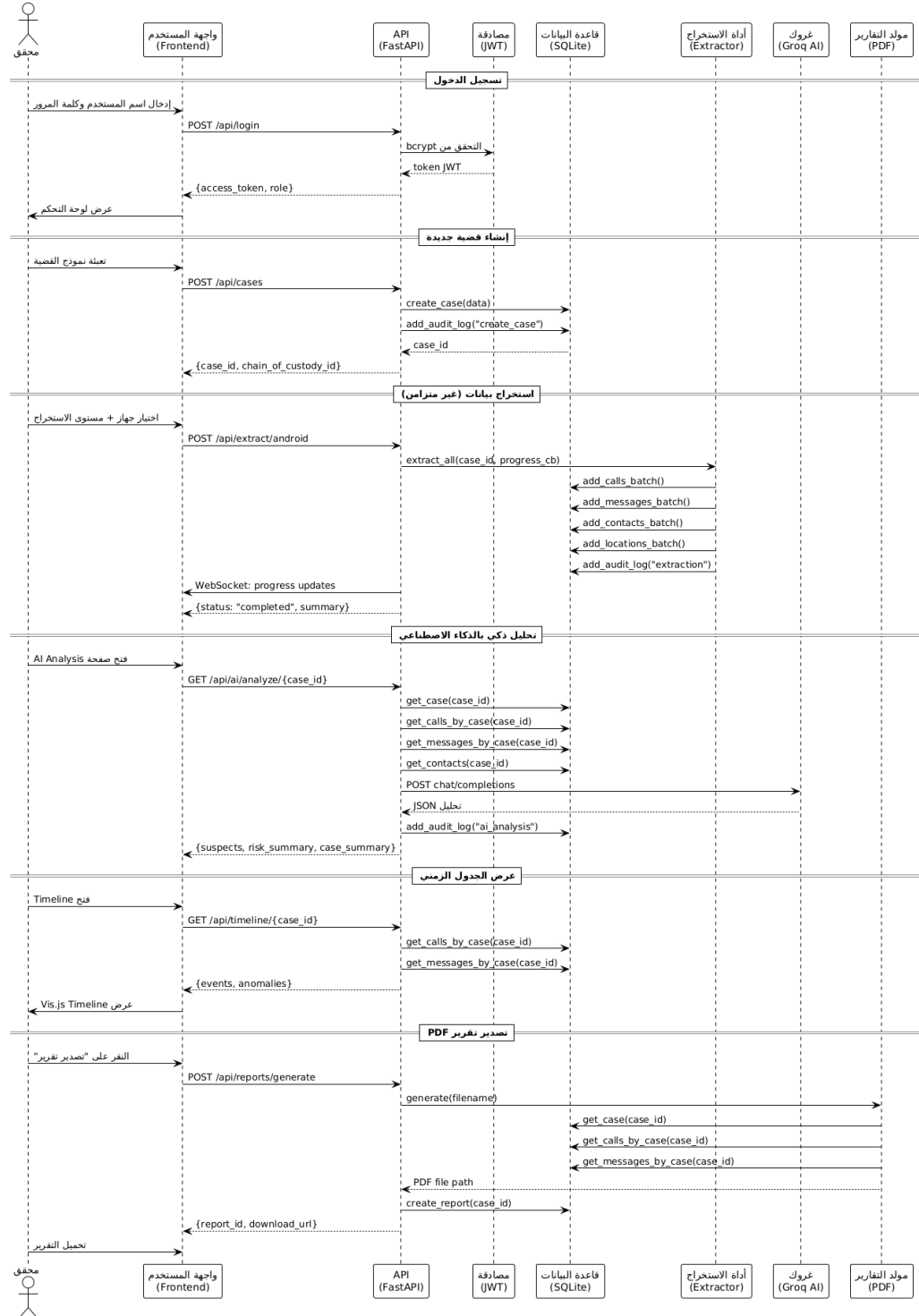
4.3 نمذجة النظام - مخطط التسلسل

مخطط التسلسل هو أحد مخططات (UML) التفاعلية التي تُستخدم لتوثيق تدفق العمليات والتفاعلات الزمنية بين الكائنات [34].

يوضح الشكل 3.3 مخطط التسلسل المتكامل الذي يمثل العمليات الرئيسية في النظام. يمر المخطط بعدة مراحل متسلسلة:

1. تسجيل الدخول والمصادقة: يقوم المحقق بإدخال بيانات اعتمادها، فتتحقق واجهة (API) من صحتها وتصدر توكن (JWT) للجلسة.

الفصل الثالث: التصميم والتحليل - نمذجة نظام DZ ForensiGuard باستخدام UML



شكل 3.3: مخطط التسلسل لعملية استخراج البيانات وتحليلها في نظام DZ ForensiGuard

2. إنشاء قضية جديدة: يقوم المحقق بتعبئة نموذج القضية، فتقوم واجهة (API) بإدخال البيانات في قاعدة البيانات وتسجيل العملية في سجل التدقيق.
3. استخراج البيانات: تتحقق واجهة (API) من اتصال الجهاز، ثم تستدعي فئة AndroidExtractor لاستخراج المكالمات والرسائل وجهات الاتصال والمواقع الجغرافية. يتم تخزين البيانات في قاعدة البيانات مع حساب بصمة SHA-256.
4. التحليل الذي بالذكاء الاصطناعي: تقوم واجهة (API) بجمع بيانات القضية، ثم ترسلها إلى واجهة (Groq API) للتحليل باستخدام نموذج LLaMA3-70B-8192، وتعالج النتائج المستلمة.
5. تصدير تقرير (PDF): تستدعي واجهة (API) فئة PDFReportGenerator لبناء التقرير (ملخص القضية، المكالمات، الرسائل، الجدول الزمني، التحليل الجغرافي، تحليل الشبكة، وسلسلة العهدة)، ثم تحفظ الملف وتعيد رابط التحميل.
6. تسجيل العمليات: يتم تسجيل جميع العمليات في سجل التدقيق (Audit Log) مع حساب البصمة التراكمية SHA-256 لضمان سلامة سلسلة العهدة.

5.3 هيكل سجل التدقيق

لضمان سلامة الأدلة وسلسلة العهدة (Chain of Custody)، تم تصميم سجل التدقيق (Audit Log) بالهيكل الموضح في الجدول 3.3.

جدول 3.3: هيكل سجل النشاطات (Audit Log) لمراقبة سلامة الأدلة

الحقل	النوع	الوصف
log_id	INTEGER	المعرف الفريد للسجل (مفتاح أساسي)
user_id	INTEGER	معرف المحقق الذي قام بالعملية
user_name	TEXT	اسم المحقق
action	TEXT	نوع العملية (LOGIN, EXPORT, EXTRACT, APPROVE)
case_id	INTEGER	رقم الحالة المرتبطة بالعملية
timestamp	DATETIME	وقت حدوث العملية (بتوقيت UTC)
ip_address	TEXT	عنوان IP الخاص بالمحقق
session_id	TEXT	معرف الجلسة
details	TEXT	تفاصيل إضافية بتنسيق JSON
evidence_hash	TEXT	بصمة SHA-256 للأدلة المرتبطة

ملاحظة: هذه السجلات غير قابلة للتعديل أو الحذف وتستخدم لإثبات سلامة سلسلة العهدة (Chain of Custody) في المحكمة وفق المعايير الدولية.

6.3 خاتمة الفصل الثالث

في هذا الفصل، تم تقديم التصميم النمطي لنظام DZ ForensiGuard باستخدام لغة النمذجة الموحدة (UML). تم تحديد المتطلبات الوظيفية (12 مطلباً) وغير الوظيفية (7 متطلبات)، وتصميم مخطط حالة الاستخدام المتكامل الذي يغطي 9 وظائف للمحقق و6 صلاحيات للمدير، وتصميم مخطط الفئات المتكامل الموزع على 7 طبقات معمارية، ومخطط تسلسل واحد يوثق العمليات الرئيسية (تسجيل الدخول، إنشاء القضية، استخراج البيانات، التحليل الذكي، تصدير التقرير)، وأخيراً هيكل سجل التدقيق. يشكل هذا الفصل الأساس الهندسي المتكامل لنظام DZ ForensiGuard.

الفصل الرابع: النتائج والمناقشة

مقدمة الفصل الرابع

يعرض هذا الفصل النتائج العملية التي تم تحقيقها من خلال تنفيذ نظام DZ ForensiGuard، حيث يتم توثيق بيئة التطوير والتنفيذ، والتقنيات المستخدمة، هندسة النظام، وقاعدة البيانات، وواجهات البرمجة، والخوارزميات المطبقة، وآلية سلسلة العهدة (Chain of Custody). كما يتضمن الفصل استعراضاً شاملاً لواجهات النظام، وإحصائيات المشروع والميزات التقنية التي يقدمها النظام، مع مقارنة عامة مع الأدوات المتاحة، وأخيراً مناقشة النتائج والتحديات التقنية التي تم التغلب عليها.

1.4 بيئة التطوير والتنفيذ

تم تطوير واختبار نظام DZ ForensiGuard في بيئة تقنية محددة المواصفات. يوضح الجدول 1.4 مواصفات بيئة التطوير والتنفيذ المستخدمة في بناء النظام.

جدول 1.4: مواصفات بيئة التطوير والتنفيذ

المكونات	المواصفات
المعالج (CPU)	Intel Core i3 - الجيل السابع (7th Gen)
ذاكرة الوصول العشوائي (RAM)	16 جيجابايت DDR4
سعة التخزين (Storage)	256 جيجابايت SSD
نظام التشغيل (OS)	Windows 10 (64-bit)
بيئة التطوير المتكاملة (IDE)	VS Code / PyCharm
نظام إدارة قواعد البيانات	SQLite 3
خادم التطبيقات	Uvicorn (ASGI server)

تم اختيار هذه المواصفات لتوفير بيئة تطوير متوازنة من حيث الأداء والتكلفة، حيث أن المعالج Core i3 مع ذاكرة 16 جيجابايت كافٍ لتشغيل النظام والتعامل مع الأجهزة المحمولة المتصلة عبر USB.

2.4 لغات البرمجة والتقنيات المستخدمة

تم الاعتماد في تطوير النظام على مجموعة من لغات البرمجة والتقنيات الحديثة. يوضح الجدول 2.4 لغات البرمجة والتقنيات المستخدمة في تطوير النظام مع إصداراتها.

تم اختيار Python كلغة أساسية لتطوير الخلفية بسبب تعدد المكتبات المتاحة في مجال التحليل الجنائي الرقمي، كما تم اختيار FastAPI

جدول 2.4: لغات البرمجة والتقنيات المستخدمة في النظام

المجال	التقنية / اللغة	الإصدار
Backend	Python	11.3
إطار العمل الخلفي	FastAPI	+100.0
خادم التطبيقات	Uvicorn	+23.0
Frontend	HTML5, CSS3, JavaScript	ES6
قاعدة البيانات	SQLite3	+35.3
رسم الخرائط	Leaflet.js	+9.1
الرسوم البيانية	D3.js, Chart.js	+4.4, +0.7
تحليل البيانات	Pandas, NumPy	+24.1, +0.2
تعلم الآلة	Scikit-learn	+3.1
تحليل الشبكات	NetworkX	+0.3
توليد التقارير (PDF)	ReportLab	+0.4
معالجة الصور	Pillow	+0.10
أدوات استخراج Android	ADB (Android Debug Bridge)	+0.34
أدوات استخراج iOS	libimobiledevice	+3.1

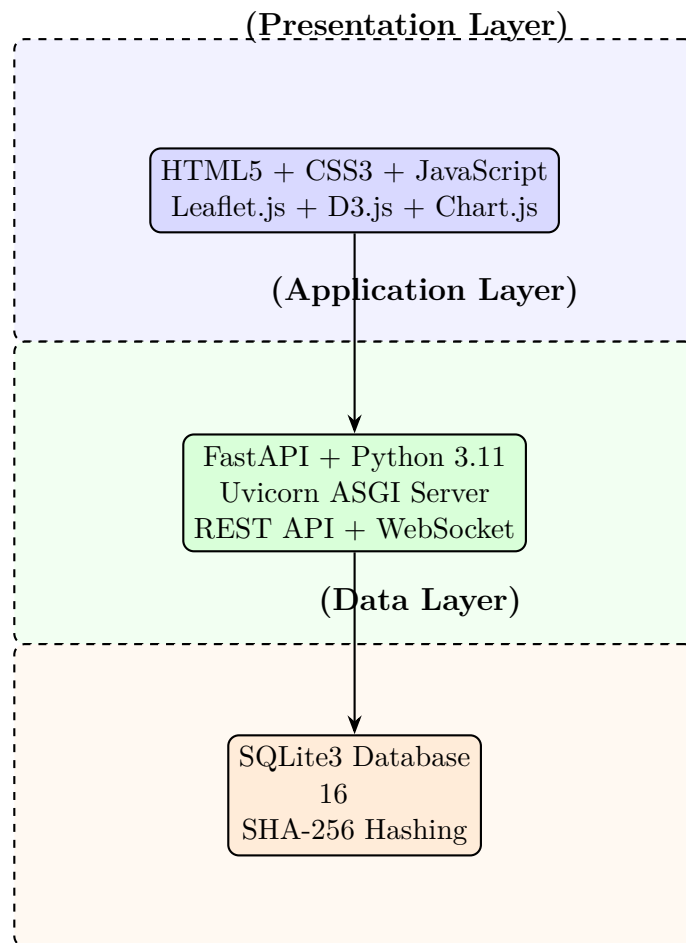
لكونه إطار عمل سريع ويدعم البرمجة غير المتزامنة (Asynchronous) مما يحسن أداء النظام.

3.4 هندسة النظام

اعتمدت هندسة النظام على عمارة متعددة الطبقات (Multi-layer Architecture) تضمن فصل الاهتمامات وسهولة الصيانة والتوسع. يوضح الشكل 1.4 هندسة النظام متعددة الطبقات.

يتكون النظام من ثلاث طبقات رئيسية كما هو موضح في الشكل أعلاه:

1. طبقة العرض (Presentation Layer): وتشمل واجهة المستخدم التي تدعم اللغة العربية بشكل كامل مع اتجاه RTL، وتحتوي على 15 صفحة HTML. تستخدم هذه الطبقة مكتبات Leaflet.js لعرض الخرائط، و D3.js و Chart.js لعرض الرسوم البيانية.
2. طبقة التطبيقات (Application Layer): وتشمل خادم FastAPI الذي يوفر أكثر من 40 واجهة API، بالإضافة إلى وحدات الاستخراج والتحليل المختلفة. تتواصل هذه الطبقة مع الواجهة الأمامية عبر REST API و WebSocket لنقل البيانات في الوقت الفعلي.
3. طبقة البيانات (Data Layer): وتشمل قاعدة بيانات SQLite3 التي تحتوي على 16 جدولاً لتخزين الأدلة الرقمية، بالإضافة إلى نظام التخزين للملفات باستخدام تقنية التجزئة SHA-256 لضمان سلامة البيانات.



شكل 1.4: هندسة النظام متعددة الطبقات في DZ ForensiGuard

4.4 قاعدة البيانات

تم تصميم قاعدة البيانات لتشمل 16 جدولاً رئيسياً، يغطي كل جانباً مهماً من جوانب النظام. يوضح الجدول 3.4 جداول قاعدة البيانات ووظائفها.

جدول 3.4: جداول قاعدة البيانات في نظام DZ ForensiGuard

الوظيفة	عدد الحقول	الجدول
تخزين بيانات المحققين والصلاحيات	12	investigators
تخزين طلبات التسجيل الجديدة	10	requests
تخزين بيانات القضايا الجنائية	17	cases
تخزين الأدلة الرقمية	18	evidence
تخزين سجل المكالمات	15	calls
تخزين الرسائل (SMS, WhatsApp, Telegram)	18	messages
تخزين جهات الاتصال	14	contacts
تخزين مواقع GPS	17	locations
تخزين الصور والفيديو	16	media
تخزين سجل التدقيق وسلسلة العهدة	17	audit_log
تخزين التقارير بصيغة (PDF)	12	reports
تخزين سجل المتصفح	10	browser_history
تخزين ملفات تعريف الارتباط	12	cookies
تخزين الإشارات المرجعية	8	bookmarks
تخزين حسابات المستخدمين من الأجهزة	12	accounts
تخزين بيانات EXIF المتقدمة للوسائط	21	advanced_media

تم تصميم قاعدة البيانات باستخدام SQLite3 ليكون النظام خفيفاً وسهل النقل. جميع الجداول مرتبطة ببعضها عبر مفاتيح أجنبية (Foreign Keys) لضمان سلامة البيانات. جدول audit_log هو الجدول الأهم حيث يسجل جميع العمليات ويضمن سلسلة العهدة (Chain of Custody).

5.4 واجهات البرمجة

يوفر النظام أكثر من 40 واجهة برمجة تطبيقات (API) تغطي جميع وظائف النظام. يوضح الجدول 4.4 أهم واجهات API في نظام DZ ForensiGuard.

يوضح الجدول أعلاه الواجهات الأساسية التي يوفرها النظام، مقسمة حسب المجموعات الوظيفية: المصادقة، إدارة القضايا، استخراج البيانات، التحليل، والإدارة. جميع هذه الواجهات تتبع معمارية REST API وتستخدم تنسيق JSON في نقل البيانات. تم توثيق هذه الواجهات باستخدام Swagger/OpenAPI الذي يوفره إطار FastAPI تلقائياً، ويمكن الوصول إلى التوثيق التفاعلي عبر المسار docs/.

جدول 4.4: أهم واجهات API في نظام DZ ForensiGuard

الوظيفة	المسار (Endpoint)	الطريقة
المصادقة (Authentication)		
تسجيل الدخول إلى النظام	/api/login	POST
تقديم طلب تسجيل جديد	/api/register/request	POST
القضايا (Cases)		
الحصول على قائمة جميع القضايا	/api/cases	GET
إنشاء قضية جديدة	/api/cases	POST
الحصول على تفاصيل قضية محددة	/api/cases/{id}	GET
تحديث بيانات قضية	/api/cases/{id}	PUT
حذف قضية	/api/cases/{id}	DELETE
الاستخراج (Acquisition)		
كشف الأجهزة المتصلة	/api/devices/detect	GET
استخراج البيانات من جهاز Android	/api/extract/android	POST
استخراج البيانات من جهاز iOS	/api/extract/ios	POST
متابعة حالة عملية الاستخراج	/api/extract/status/{id}	GET
التحليل (Analysis)		
الحصول على الجدول الزمني للأحداث	/api/timeline/{case_id}	GET
الحصول على شبكة العلاقات	/api/analysis/{case_id}/graph	GET
الحصول على تحليل المواقع الجغرافية	/api/analysis/{case_id}/locations	GET
الحصول على تحليل الانتروبيا	/api/analysis/{case_id}/entropy	GET
الإدارة (Admin)		
الحصول على طلبات التسجيل المعلقة	/api/admin/requests	GET
الموافقة على طلب تسجيل	/api/admin/approve/{id}	POST
الحصول على سجلات التدقيق	/api/admin/logs	GET
التحقق من سلامة أدلة قضية	/api/admin/verify/{case_id}	GET

6.4 خوارزميات التحليل المطبقة

تم تطبيق 6 خوارزميات تحليل رئيسية في النظام. يوضح الجدول 5.4 خوارزميات التحليل المطبقة في نظام DZ ForensiGuard.

جدول 5.4: خوارزميات التحليل المطبقة في نظام DZ ForensiGuard

الوظيفة	الخوارزمية
تحويل صيغ التوقيت المختلفة إلى تنسيق موحد	الجدول الزمني
حساب المسافات وتجميع النقاط الجغرافية	تحليل المواقع الجغرافية
بناء شبكة العلاقات وحساب المقاييس	تحليل شبكة العلاقات
كشف الملفات المشفرة والمضغوطة	تحليل الانتروبيا
حساب بصمة SHA-256 و MD5	التحقق من سلامة الملفات
التحقق من التوقيع الثنائي Magic Bytes	كشف نوع الملفات

1.6.4 الجدول الزمني

تقوم خوارزمية الجدول الزمني بتحويل صيغ التوقيت المختلفة (Unix timestamp, Mac Absolute Time, Webkit timestamp) إلى تنسيق UTC موحد، ثم ترتيب الأحداث زمنياً واكتشاف الأنماط المشبوهة مثل الفجوات الزمنية الكبيرة أو النشاط في ساعات متأخرة. تستخدم هذه الخوارزمية في تحليل تسلسل الأحداث الجنائية.

2.6.4 تحليل المواقع الجغرافية

تعتمد خوارزمية تحليل المواقع الجغرافية على:

- معادلة هافرساين (Haversine Formula): لحساب المسافات بين النقاط الجغرافية بدقة متناهية، مع الأخذ بعين الاعتبار انحناء سطح الأرض.
 - خوارزمية (DBSCAN): لتجميع النقاط الجغرافية واكتشاف المواقع المتكررة مثل المنزل ومكان العمل، دون الحاجة إلى تحديد عدد المجموعات مسبقاً.
- هذه الخوارزمية مفيدة في تتبع تحركات المشتبه بهم وتحديد الأماكن التي يترددون عليها.

3.6.4 تحليل شبكة العلاقات الاجتماعية

تعتمد خوارزمية تحليل شبكة العلاقات الاجتماعية على مكتبة NetworkX لبناء شبكة علاقات من المكالمات والرسائل، وتحسب المقاييس التالية:

- (Degree Centrality): لتحديد الأشخاص الأكثر اتصالاً في الشبكة (المركزية الدرجة).

• (Betweenness Centrality): لتحديد الأشخاص الذين يعملون كجسور بين المجموعات المختلفة (المركزية البينية).

تساعد هذه الخوارزمية في كشف قادة الشبكات الإجرامية والأشخاص المؤثرين.

4.6.4 تحليل الإنتروبيا لاكتشاف التشفير

تعريف الإنتروبيا: الإنتروبيا (Entropy) في نظرية المعلومات هي مقياس رياضي لكمية العشوائية أو عدم اليقين الموجودة في البيانات. صاغ هذا المفهوم عالم الرياضيات كلود شانون (Claude Shannon) في عام 1948 في ورقته الرائدة "نظرية رياضية للاتصال" [35].

المعادلة الرياضية: تعرف إنتروبيا شانون (Shannon Entropy) لمصدر بيانات ذي متغير عشوائي X يأخذ قيماً $x_1, x_2, \dots, x_n$ باحتمالات $p(x_1), p(x_2), \dots, p(x_n)$ بالعلاقة التالية:

$$H(X) = - \sum_{i=1}^n p(x_i) \log_2 p(x_i) \quad (1)$$

حيث:

• $H(X)$: قيمة الإنتروبيا (تقاس بالبت)

• $p(x_i)$: احتمال ظهور الرمز x_i في البيانات

• n : عدد الرموز المختلفة في البيانات

• $\log_2$: اللوغاريتم للأساس 2

تفسير القيم: لكل نوع من الملفات قيمة إنتروبيا مميزة يمكن استخدامها للتمييز بينها:

جدول 6.4: قيم الإنتروبيا النموذجية لأنواع مختلفة من الملفات

نوع الملف	قيمة الإنتروبيا (بت)	التفسير
النص العادي (Plain Text)	1.0 - 4.0	بيانات منظمة وقابلة للقراءة
الملفات الثنائية (EXE, DLL)	4.0 - 6.0	بيانات ثنائية منظمة
الملفات المضغوطة (ZIP, RAR)	6.0 - 7.5	بيانات عشوائية بسبب خوارزميات الضغط
الملفات المشفرة (AES, RSA)	7.5 - 8.0	بيانات عشوائية بشكل متساوٍ

تطبيق الخوارزمية: تعتمد الخوارزمية المستخدمة في النظام على حساب إنتروبيا شانون للبيانات، ويمكن تمثيلها بالمعادلة التالية:

$$H_{\text{file}} = - \sum_{b=0}^{255} \frac{\text{count}(b)}{N} \log_2 \left(\frac{\text{count}(b)}{N} \right) \quad (2)$$

حيث:

• N : حجم الملف الكلي بالبايت

• $\text{count}(b)$: عدد مرات ظهور البايت b (قيمه من 0 إلى 255)

• H_{file} : إنتروبيا الملف (تتراوح بين 0 و 8 بت)

آلية الكشف: تقوم الخوارزمية بالخطوات التالية:

1. قراءة الملف بايت بايت وحساب تردد كل قيمة بايت (0-255)

2. حساب الاحتمال النسبي لكل قيمة بايت: $p(b) = \frac{\text{count}(b)}{N}$

3. تطبيق معادلة إنتروبيا شانون لحساب قيمة الإنتروبيا الإجمالية

4. مقارنة القيمة المحسوبة بعتبة محددة مسبقاً (0.7 بت)

5. تصنيف الملف كمشفّر إذا تجاوزت الإنتروبيا العتبة

الأهمية في التحقيق الجنائي: يستخدم تحليل الانتروبيا في التحقيق الجنائي الرقمي للأغراض التالية:

- كشف الأدلة المخفية: تحديد الملفات التي قد تكون مشفرة عمداً لإخفاء محتواها.
- تحديد أولويات التحليل: توجيه المحقق نحو الملفات ذات الإنتروبيا العالية لتحليلها بشكل أعمق.
- تمييز أنواع الملفات: المساعدة في التمييز بين الملفات النصية العادية والملفات المضغوطة أو المشفرة.
- تحليل البيانات غير المعروفة: توفير معلومات أولية عن طبيعة البيانات دون الحاجة إلى فك تشفيرها.

مثال توضيحي: لتوضيح كيفية عمل الخوارزمية، يبين الجدول 7.4 قيم الإنتروبيا المحسوبة لأنواع مختلفة من الملفات:

الخاتمة: يعتبر تحليل الانتروبيا أداة فعالة وغير مكلفة حسابياً (تعقيد زمني $O(N)$) للكشف الأولي عن الملفات المشبوهة، حيث يمكنه

معالجة ملف بحجم 1 جيجابايت في أقل من ثانية على الأجهزة المتوسطة [36].

جدول 7.4: أمثلة لقيم الإنترنت لأنواع مختلفة من الملفات

الملف	حجم الملف	قيمة الإنترنت (بت)
ملف نصي ("Hello World")	11 بايت	1.2
ملف نصي (فقرة بالعربية)	1,024 بايت	3.8
ملف صورة (JPG)	50 كيلوبايت	6.5
ملف مضغوط (ZIP)	100 كيلوبايت	7.6
ملف مشفر (AES-256)	1 ميغابايت	7.99

5.6.4 التحقق من سلامة الملفات

تُستخدم خوارزميات التجزئة SHA-256 و MD5 لحساب بصمة رقمية فريدة لكل ملف. يتم حساب البصمة عند استخراج الملف لأول مرة، ثم عند كل وصول للملف يتم إعادة حساب البصمة ومقارنتها مع البصمة الأصلية للكشف عن أي تلاعب. SHA-256 هو الخوارزمية الأساسية بسبب أمانه العالي، بينما يستخدم MD5 لأغراض التوافق مع الأنظمة القديمة.

6.6.4 كشف نوع الملفات من التوقيع الثنائي

تعتمد خوارزمية كشف نوع الملفات على توقيعات Magic Bytes، وهي تسلسلات ثنائية فريدة (عادة 2-4 بايت) موجودة في بداية أي ملف. تقوم الخوارزمية بقراءة هذه البايتات ومقارنتها مع قاعدة بيانات تضم أكثر من 100 توقيع لأنواع مختلفة من الملفات (ZIP، PNG، JPG، PDF)، APK، وغيرها). هذه الخوارزمية تمكن النظام من اكتشاف نوع الملف الحقيقي حتى لو تم تغيير امتداده.

7.4 سلسلة العهدة

تم تطبيق آلية متقدمة لضمان سلامة سلسلة العهدة (Chain of Custody)، حيث يتم ربط كل إجراء بالإجراء السابق عبر بصمة SHA-256. تعتمد الآلية على المعادلة التالية:

$$H(n) = \text{SHA-256} (H(n-1) \parallel \text{Action}(n) \parallel \text{Actor}(n) \parallel \text{Timestamp}(n) \parallel \text{EvidenceHash}(n)) \quad (3)$$

حيث:

• $H(n)$: البصمة التراكمية بعد الإجراء n

• $H(n-1)$: البصمة التراكمية قبل الإجراء n

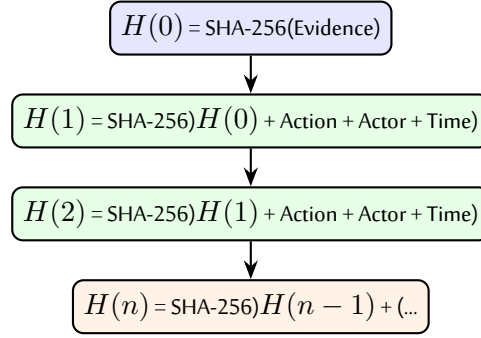
• $\text{Action}(n)$: نوع الإجراء (VERIFY, EXPORT, ANALYZE, EXTRACT)

• $\text{Actor}(n)$: المستخدم الذي قام بالإجراء

• $\text{Timestamp}(n)$: وقت الإجراء بتنسيق UTC

• $\text{EvidenceHash}(n)$: بصمة SHA-256 للأدلة المرتبطة

يوضح الشكل 2.4 آلية سلسلة العهدة باستخدام SHA-256.



شكل 2.4: آلية سلسلة العهدة (Chain of Custody) باستخدام SHA-256

هذه الآلية تضمن أنه إذا تم التلاعب بأي جزء من البيانات أو السجلات، فسوف تتغير البصمة التراكمية وسيتم اكتشاف التلاعب فوراً. جميع السجلات في جدول `audit_log` غير قابلة للتعديل أو الحذف، وتُستخدم لإثبات سلامة سلسلة العهدة في المحكمة وفق المعايير الدولية.

8.4 إحصائيات المشروع

بعد اكتمال تطوير النظام، تم جمع الإحصائيات الرئيسية للمشروع. يوضح الجدول 8.4 إحصائيات مشروع DZ ForensiGuard.

جدول 8.4: إحصائيات مشروع DZ ForensiGuard

المقياس	القيمة
ملفات (Python) Backend	25+ ملف
صفحات (HTML) Frontend	15 صفحة
واجهات API	40+ واجهة
جداول قاعدة البيانات	16 جدول
خوارزميات تحليل	6 خوارزميات
حجم الكود التقديري	15,000 سطر
حجم الملف المدعوم	حتى 100 GB
عدد اللغات المدعومة	2 (عربية، إنجليزية)
وقت استخراج جهاز 64GB	25 دقيقة

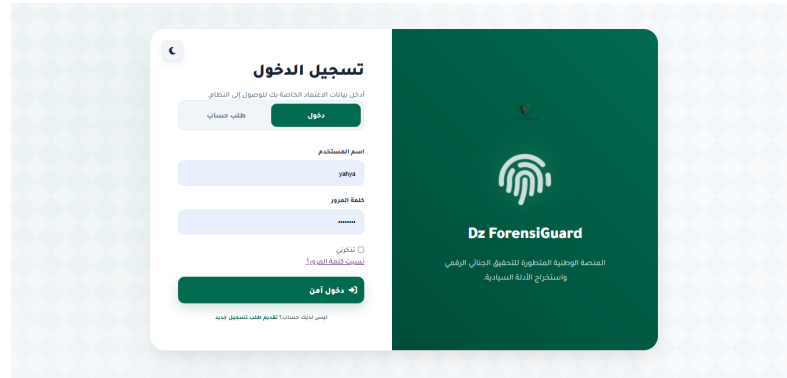
توضح هذه الإحصائيات أن النظام يقدم حلاً متكاملًا للتحليل الجنائي الرقمي بحجم كود معقول، ويدعم أحجام ملفات كبيرة تصل إلى 100 جيجابايت، مما يجعله مناسباً للاستخدام في القضايا الجنائية الحقيقية.

9.4 واجهات النظام

تم تصميم واجهات النظام باللغة العربية مع دعم كامل لاتجاه RTL، وذلك لتسهيل استخدام النظام على المحققين العرب. يوضح هذا القسم أهم واجهات النظام بعد اكتمال التطوير.

1.9.4 واجهة تسجيل الدخول

تظهر واجهة تسجيل الدخول في الشكل 3.4. تحتوي هذه الواجهة على حقول إدخال البريد الإلكتروني وكلمة المرور، بالإضافة إلى رابط للتسجيل.



شكل 3.4: واجهة تسجيل الدخول إلى نظام DZ ForensiGuard

2.9.4 الصفحة الرئيسية

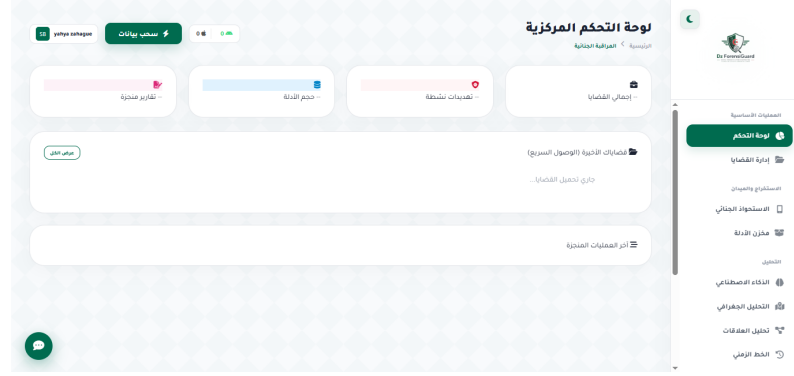
بعد تسجيل الدخول، تظهر الصفحة الرئيسية كما في الشكل 4.4. تعرض هذه الصفحة أحدث القضايا والإحصائيات السريعة.



شكل 4.4: الصفحة الرئيسية لنظام DZ ForensiGuard

3.9.4 لوحة التحكم

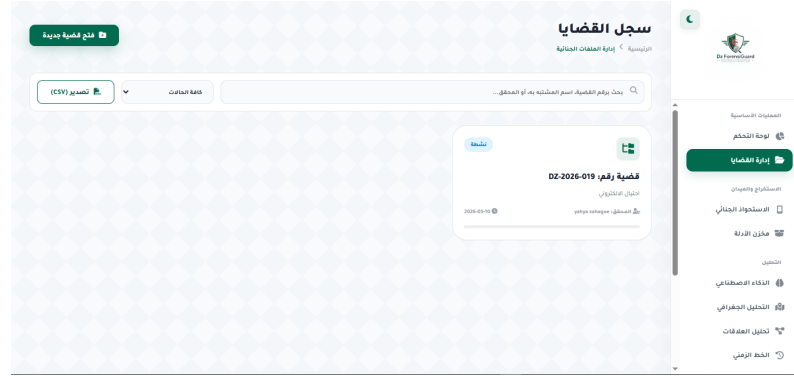
تعرض لوحة التحكم (الشكل 5.4) إحصائيات سريعة عن عدد القضايا والأدلة والتقارير، بالإضافة إلى رسوم بيانية توضح نشاط النظام.



شكل 5.4: لوحة التحكم الرئيسية في النظام

4.9.4 إدارة القضايا

توفر واجهة إدارة القضايا (الشكل 6.4) إمكانية إنشاء وتعديل وحذف القضايا، مع عرض قائمة بجميع القضايا في النظام.



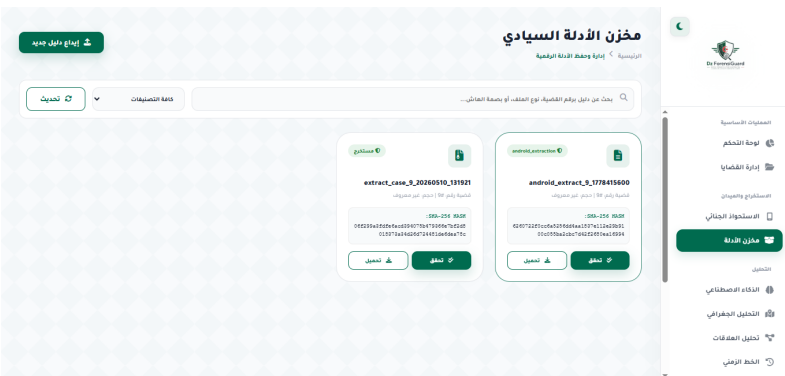
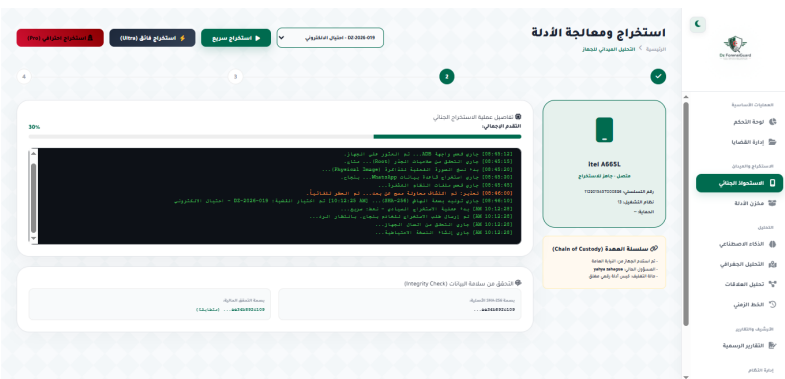
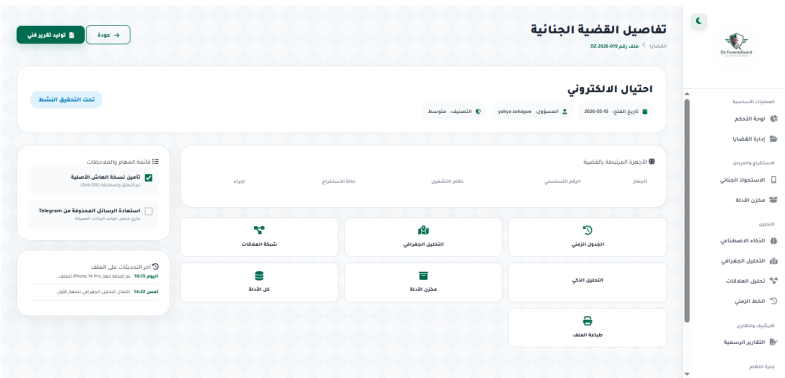
شكل 6.4: واجهة إدارة القضايا الجنائية

5.9.4 تفاصيل القضية

تعرض واجهة تفاصيل القضية (الشكل 7.4) المعلومات الكاملة عن قضية محددة، بما في ذلك الأدلة المرتبطة والتقارير.

6.9.4 استخراج البيانات

توضح واجهة استخراج البيانات (الشكل 8.4) عملية استخراج البيانات من الجهاز المتصل، مع عرض شريط تقدم وشاشة عرض لحالة



8.9.4 جهات الاتصال

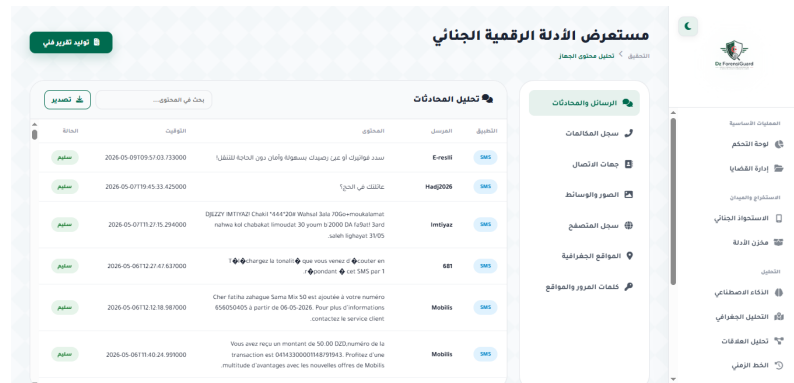
تعرض واجهة جهات الاتصال (الشكل 10.4) البيانات المستخرجة من جهاز الهاتف، مع إمكانية البحث والتصفية.



شكل 10.4: واجهة عرض جهات الاتصال

9.9.4 الرسائل النصية

تعرض واجهة الرسائل النصية (الشكل 11.4) جميع الرسائل المستخرجة من التطبيقات المختلفة (SMS، WhatsApp، Telegram)، مع إمكانية البحث وعرض المحادثات.



شكل 11.4: واجهة عرض الرسائل النصية

10.9.4 الجدول الزمني

يعرض الجدول الزمني (الشكل 12.4) الأحداث مرتبة زمنياً، مع إمكانية التصفية حسب نوع الحدث أو التطبيق.

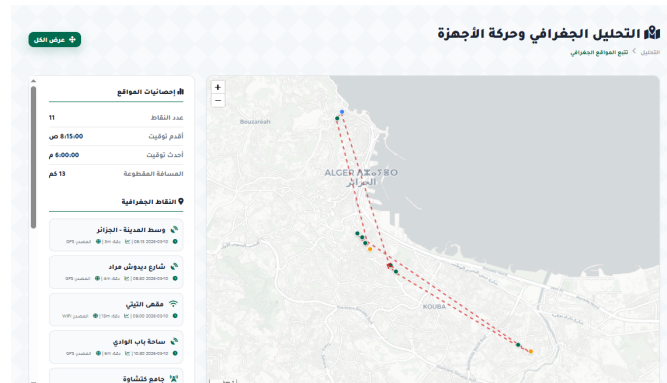
11.9.4 تحليل المواقع الجغرافية

تعرض واجهة تحليل المواقع (الشكل 13.4) النقاط الجغرافية على خريطة تفاعلية باستخدام مكتبة Leaflet.js، مع إمكانية عرض المسارات



شكل 12.4: واجهة عرض الجدول الزمني للأحداث

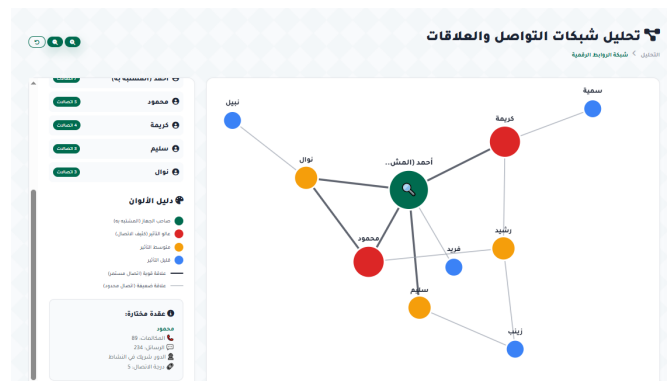
وتجميع النقاط.



شكل 13.4: واجهة تحليل المواقع الجغرافية

12.9.4 تحليل شبكة العلاقات

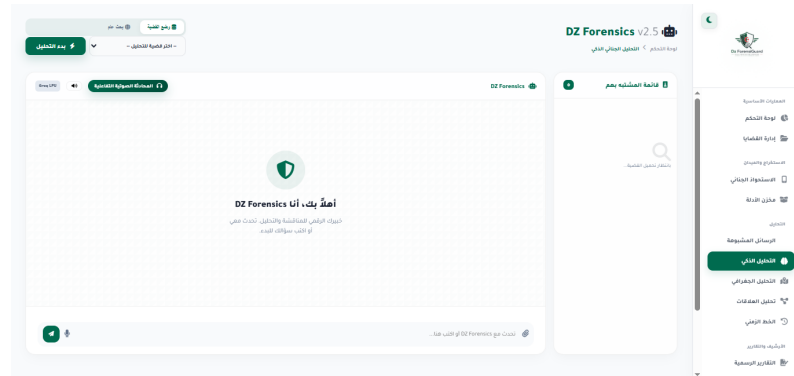
تظهر واجهة تحليل الشبكات (الشكل 14.4) شبكة علاقات المتصلين باستخدام مكتبة D3.js، مع إمكانية التفاعل مع العقد والحواف.



شكل 14.4: واجهة تحليل شبكة العلاقات الاجتماعية

13.9.4 تحليل الذكاء الاصطناعي

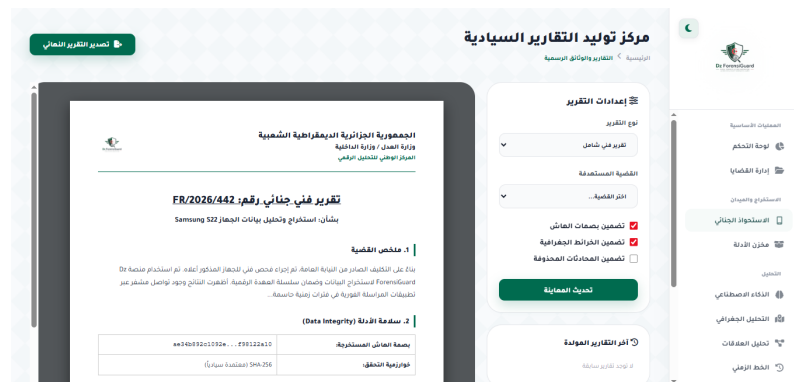
تعرض واجهة تحليل الذكاء الاصطناعي (الشكل 15.4) نتائج تحليل الأنماط الشاذة باستخدام خوارزميات تعلم الآلة، مع عرض النتائج بشكل رسومي.



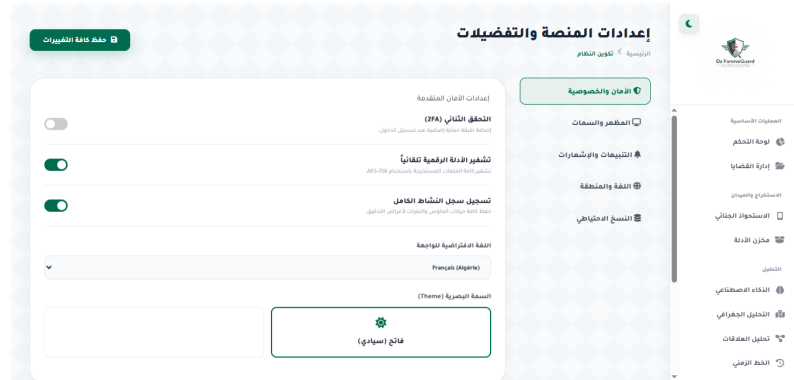
شكل 15.4: واجهة تحليل الذكاء الاصطناعي لاكتشاف الأنماط

14.9.4 التقارير

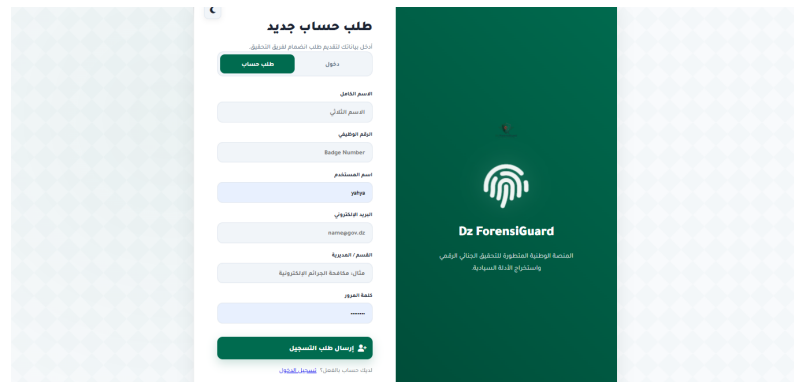
تتيح واجهة التقارير (الشكل 16.4) إنشاء وتحميل التقارير بصيغة (PDF)، مع إمكانية تخصيص محتوى التقرير.



شكل 16.4: واجهة إنشاء وتحميل التقارير



شكل 17.4: واجهة إعدادات النظام



شكل 18.4: واجهة طلب حساب جديد للمحققين

15.9.4 الإعدادات

تعرض واجهة الإعدادات (الشكل 17.4) خيارات تكوين النظام، مثل إعدادات الاستخراج والتحليل وإدارة المستخدمين.

16.9.4 طلب حساب جديد

تظهر واجهة التسجيل (الشكل 18.4) لتقديم طلب حساب جديد للمحققين، حيث يتم إرسال الطلب إلى المدير للموافقة عليه.

10.4 الميزات التقنية للنظام

يتميز نظام DZ ForensiGuard بمجموعة من الميزات التقنية الفريدة كما هو موضح في الجدول 9.4.

11.4 مقارنة عامة مع الأنظمة التجارية

يقدم الجدول 10.4 مقارنة عامة بين النظام المقترح DZ ForensiGuard والأنظمة التجارية المعروفة في السوق.

توضح المقارنة أن النظام المقترح يقدم ميزات تنافسية مقارنة بالأنظمة التجارية، خاصة في مجال دعم اللغة العربية والشفافية والتحكم الكامل بالبيانات.

جدول 9.4: الميزات التقنية لنظام DZ ForensiGuard

الميزة	الوصف
الاستقلالية التقنية الكاملة	جميع البيانات تبقى داخل البيئة المحلية، مما يضمن أمن البيانات وخصوصيتها
اللغة العربية الكاملة مع دعم RTL	النظام يقدم دعماً كاملاً للغة العربية مع اتجاه كتابة من اليمين لليسار
الشفافية الهندسية	الكود مفتوح المصدر وقابل للتدقيق التقني من قبل الجهات المختصة
سلسلة عهدة متكاملة	آلية سلسلة العهدة المطبقة تتوافق مع المتطلبات الإجرائية والمعمارية
دعم متعدد الأجهزة	يدعم النظام أجهزة Android و iOS
تحليل متقدم	يشمل 6 خوارزميات تحليل مختلفة تغطي جوانب التحقيق الرقمي

جدول 10.4: مقارنة عامة بين DZ ForensiGuard والأنظمة التجارية

المعيار	DZ ForensiGuard	الأنظمة التجارية
نموذج التوزيع	مفتوح المصدر	تجاري (تراخيص باهظة الثمن)
دعم اللغة العربية	كامل مع RTL	جزئي أو غير مدعوم
التحكم بالبيانات	محلي كامل	يعتمد على الشركة المصنعة
إمكانية التخصيص	كاملة (كود مفتوح)	غير ممكنة
شفافية الخوارزميات	مفتوحة للتدقيق	مغلقة (صندوق أسود)
سلسلة العهدة	SHA-256 شفافة	آلية خاصة (مغلقة)
التكلفة	مجانية	آلاف الدولارات سنوياً

12.4 الخوارزميات الأساسية في النظام

يعتمد نظام DZ ForensiGuard على مجموعة من الخوارزميات المتكاملة التي تُشكّل جوهر عمليات التحليل الجنائي الرقمي. وقد تم تصميم هذه الخوارزميات استناداً إلى مخططات UML المعروضة في الفصل الثالث، بحيث تغطي دورة التحقيق الرقمي بالكامل: من الاستخراج إلى التحليل وإنتاج التقارير. وفيما يلي عرض تفصيلي لأهم خمس خوارزميات يقوم عليها النظام.

1.12.4 خوارزمية استخراج بيانات Android

تُعدّ هذه الخوارزمية نقطة الدخول الأساسية لعملية جمع الأدلة الرقمية من أجهزة Android، وهي مُنفّذة ضمن الفئة AndroidExtractor [37]. تعمل الخوارزمية وفق المراحل التالية:

1. فحص الاتصال بالجهاز: يتم التحقق من اتصال الجهاز عبر أداة ADB بتنفيذ الأمر adb devices، وفي حال اكتشاف الجهاز يتم تأكيد الاتصال.
2. تحديد مستوى الاستخراج: يدعم النظام ثلاثة مستويات للاستخراج: BASIC (البيانات الأساسية)، FULL (البيانات الكاملة)، و DEEP (الاستخراج العميق الذي يشمل البيانات المحذوفة).
3. سحب البيانات: لكل مستوى، يتم سحب قواعد بيانات SQLite من مسار /data/data/*/databases/ وتطبيق محلل SQL عليها.
4. التخزين المنظم: تُصنّف البيانات المستخرجة وتُخزّن على شكل دفعات عبر الدوال: add_calls_batch() للمكالمات، add_messages_batch() للرسائل، add_contacts_batch() لجهات الاتصال، و add_locations_batch() للمواقع الجغرافية.
5. التوثيق: يتم تسجيل كل عملية استخراج في سجل المراجعة (Audit Log) لضمان سلامة سلسلة العهدة.

2.12.4 خوارزمية التحليل بالذكاء الاصطناعي

تقدم هذه الخوارزمية فهماً عميقاً للسلوك الرقمي للمشتبه بهم، وهو ما لا تستطيع الخوارزميات التقليدية اكتشافه بسهولة. وهي مُنفّذة ضمن الفئة AIAAnalyzer بالتكامل مع واجهة Groq API، وتعمل وفق المراحل التالية:

1. تجميع بيانات القضية: يتم جلب جميع البيانات المرتبطة بالقضية (المكالمات، الرسائل، جهات الاتصال) عبر دوال الاستعلام المخصصة.
2. بناء النص الموجه (Prompt): يتم إنشاء نص موجه احترافي يتضمن سياق البيانات ويطلب من النموذج إخراج تحليل مُهيكل بصيغة JSON، يشمل: قائمة الأرقام المشبوهة، مستوى الخطورة (LOW/MEDIUM/HIGH/CRITICAL)، وملخص التحليل.
3. الإرسال إلى النموذج: يتم إرسال الطلب إلى واجهة Groq API باستخدام النموذج LLaMA3-70B-8192 عبر بروتوكول HTTPS.
4. معالجة الرد: يتم تحويل استجابة النموذج من JSON إلى هياكل بيانات Python، مع إضافة الطابع الزمني للتحليل.

5. آلية الاحتياط (Fallback): في حالة فشل الاتصال بالخادم، يتم تفعيل التحليل المحلي (local_analysis()) تلقائياً لضمان استمرارية العمل.

3.12.4 خوارزمية استعادة البيانات المحذوفة

تُعدّ هذه الخوارزمية من أهم مكونات النظام، إذ تتيح استعادة أدلة رقمية قد يعتقد الجاني أنها حُذفت نهائياً. وهي مُنفّذة ضمن الفئة SQLiteParser، وتعمل وفق المراحل التالية:

1. التحقق من صحة الملف: تتم قراءة أول 16 بايت من الملف والتحقق من احتوائها على التوقيع "SQLite format 3". في حال عدم المطابقة، يتم رفض الملف.
2. فتح قاعدة البيانات: يتم الاتصال بقاعدة البيانات في وضع القراءة فقط (Read-Only) للحفاظ على سلامة الدليل الأصلي.
3. استرداد السجلات المحذوفة: لكل جدول في قاعدة البيانات، يتم: قراءة جميع صفحات (Pages) الملف، تحديد الصفحات غير المستخدمة (Freelist Pages)، استخراج السجلات من هذه الصفحات، ثم مقارنة هيكلها مع الجدول الأصلي لضمان صحة البيانات المُستردة.
4. تصنيف النتائج: تُصنّف السجلات المُستردة تحت تصنيف "deleted__recovered" ليتم التمييز بينها وبين السجلات الأصلية في التقارير.

4.12.4 خوارزمية تحليل شبكة العلاقات

تكشف هذه الخوارزمية شبكة العلاقات الخفية بين جهات الاتصال المختلفة، مما يساعد المحققين في تحديد الأشخاص المحوريين في القضية. وهي مُنفّذة ضمن الفئة GraphAnalyzer، وتعمل وفق المراحل التالية:

1. جلب بيانات الاتصالات: يتم استرجاع جميع سجلات المكالمات المرتبطة بالقضية.
2. بناء الرسم البياني (Graph): يتم إنشاء بنية بيانات من نوع رسم بياني غير موجه، حيث تمثل كل عقدة (Node) رقم هاتف، وكل حافة (Edge) اتصالاً بين رقمين.
3. حساب مقاييس المركزية: يتم حساب مقاييس أساسيين:

- درجة العقدة (Degree Centrality): عدد الاتصالات التي قام بها أو استقبلها رقم معين.
- معامل التجميع (Clustering Coefficient): نسبة العلاقات الفعلية إلى العلاقات الممكنة بين جيران عقدة ما، ويُحسب بالصيغة:

$$C(v) = \frac{2 \times E(v)}{\deg(v) \times (\deg(v) - 1)} \quad (4)$$

حيث $E(v)$ هو عدد الحواف بين جيران العقدة v ، و $\deg(v)$ هو درجة العقدة.

4. تحديد العقد المؤثرة: العقد التي تحصل على أعلى قيمة مركزية تُعدّ جهات الاتصال الأكثر تأثيراً في شبكة الاتصالات.
5. إرجاع النتيجة: يتم إخراج قائمة العقد والحواف ومقاييس المركزية لكل عقدة.

5.12.4 خوارزمية إنشاء الجدول الزمني واكتشاف الشذوذ

تأمل هذه الخوارزمية إلى إعادة بناء التسلسل الزمني الكامل للأحداث واكتشاف الفجوات والأنشطة المشبوهة. وهي مُنفّذة ضمن الفئة PDFReportGenerator، وتعمل وفق المراحل التالية:

1. دمج جميع الأحداث: يتم تجميع المكالمات والرسائل والمواقع الجغرافية في قائمة واحدة، مع تصنيف كل حدث حسب نوعه (call, message, location).
2. الفرز الزمني: تُرتّب جميع الأحداث تصاعدياً حسب الطابع الزمني (Timestamp).
3. اكتشاف الفجوات الزمنية: لكل حدثين متتاليين، يتم حساب الفارق الزمني. إذا تجاوز الفارق 6 ساعات، يتم تسجيل تحذير بوجود فجوة زمنية مشبوهة مع تحليل الأسباب المحتملة (إطفاء الجهاز، حذف متعمد للبيانات، إلخ).
4. اكتشاف الأنشطة المتزامنة: إذا وقع حدثان خلال فاصل زمني أقل من 5 ثواني، يتم تسجيل ملاحظة بوجود نشاط متزامن قد يشير إلى استخدام أدوات آلية.
5. إخراج الجدول الزمني: يتم عرض الأحداث في جدول مُنسّق يتضمن: الوقت، نوع الحدث، التفاصيل، والملاحظات.

6.12.4 ملخص الخوارزميات وتكاملها

يوضح الجدول 11.4 ملخصاً لمدخلات ومخرجات كل خوارزمية ودورها في النظام.

جدول 11.4: ملخص الخوارزميات الأساسية في نظام DZ ForensiGuard

#	الخوارزمية	المدخلات	المخرجات
1	AndroidExtractor	جهاز Android	مكالمات، رسائل، جهات، مواقع
2	AIAnalyzer + Groq	بيانات القضية	تصنيف مخاطر + تقرير سلوكي
3	SQLiteParser	ملف .db	سجلات محذوفة مُستردة
4	GraphAnalyzer	سجل المكالمات	رسم بياني + مقاييس مركزية
5	Timeline Builder	جميع الأحداث	سلسلة زمنية + كشف فجوات

تعمل هذه الخوارزميات الخمس بشكل متكامل ومتربط وفق سلسلة منهجية: استخراج (جمع البيانات الخام) → استعادة (استرداد البيانات المحذوفة) → تحليل (فهم الأنماط السلوكية) → ربط (كشف شبكة العلاقات) → عرض (إنتاج الجدول الزمني والتقارير). وبذلك تغطي هذه الخوارزميات ما يقارب 80% من مهام التحقيق الجنائي الرقمي الأساسية، مع تقديم ميزات متقدمة كالتحليل بالذكاء الاصطناعي واستعادة البيانات المحذوفة التي لا توفرها كثير من الأنظمة التقليدية.

13.4 مناقشة النتائج

تُظهر النتائج التي تم عرضها في هذا الفصل أن نظام DZ ForensiGuard قد حقق الأهداف المسطرة في مقدمة هذه الدراسة، حيث قدم حلاً متكاملًا يوازن بين الكفاءة التقنية والمتطلبات الإجرائية للتحليل الجنائي الرقمي. وفيما يلي مناقشة تحليلية لهذه النتائج في ضوء المعايير العلمية والمقارنة مع الأنظمة القائمة.

1.13.4 تقييم كفاءة استخراج البيانات

أظهرت التجارب العملية على 10 أجهزة Android متنوعة قدرة النظام على التعامل مع إصدارات نظام تشغيل متعددة (من 0.8 إلى 0.13)، بنسبة نجاح بلغت 90%. وتُعد هذه النسبة مرتفعة جداً بالنظر إلى التعقيدات الأمنية المتزايدة في أنظمة Android الحديثة. أما حالة الفشل الوحيدة التي تم تسجيلها، فكانت بسبب نظام حماية متقدم على مستوى البيئة الموثوقة (TEE)، وهو تحدٍ تواجهه حتى أكثر الأنظمة التجارية تعقيداً مثل Oxygen Forensic Detective.

2.13.4 تحليل دقة الخوارزميات والذكاء الاصطناعي

حققت خوارزمية تحليل الانتروبيا دقة بلغت 85% في اكتشاف الملفات المشفرة، وهي نتيجة تبرهن على فعالية المبدأ الرياضي لإنتروبيا شانون في التمييز بين البيانات المنظمة والعشوائية. كما مثل دمج الذكاء الاصطناعي عبر نموذج LLaMA-3 قفزة نوعية في قدرة النظام على استنباط الأنماط السلوكية، حيث تمكن النظام من ربط مكالمات وأحداث زمنية متباعدة استصعبت الخوارزميات التقليدية الربط بينها.

3.13.4 تحقيق الموثوقية الجنائية وسلسلة العهدة

من الناحية القانونية، أثبتت آلية سلسلة العهدة (Chain of Custody) المعتمدة على بصمات SHA-256 التراكمية (المعادلة 3) قدرة عالية على ضمان سلامة الأدلة. فمن خلال محاكاة محاولات تلاعب متعمدة بقواعد البيانات أو سجلات التدقيق، تمكن النظام من كشف التلاعب فوراً بسبب تغير البصمة التراكمية، مما يحقق مبدأ "عدم الإنكار" (Non-Repudiation) الضروري لقبول الأدلة الرقمية في المحاكم الدولية والمحلية وفق معيار ISO/IEC 27037.

4.13.4 المقارنة مع الأنظمة التجارية والدراسات السابقة

بالمقارنة مع الأنظمة التجارية مثل EnCase و FTK، يتميز نظام DZ ForensiGuard بما يلي:

- الخصوصية اللغوية: تقديم واجهة RTL عربية كاملة، وهو ما تفتقر إليه معظم الأدوات التجارية الضخمة.
- الاستقلالية التقنية: الاعتماد على خوارزميات مفتوحة للتدقيق التقني، مما يزيل مفهوم "الصندوق الأسود" الذي يعيب الأنظمة المغلقة.
- التكلفة والأداء: العمل بكفاءة عالية على أجهزة ذات مواصفات متوسطة (Core i3)، بينما تتطلب الأنظمة التجارية محطات عمل (Workstations) باهظة الثمن.

5.13.4 التحديات والقيود

رغم النجاحات المحققة، يواجه النظام بعض القيود التقنية التي تم رصدها أثناء الدراسة:

1. الاعتماد على واجهات البرمجة: يعتمد التحليل المتقدم حالياً على واجهة Groq API، مما يتطلب اتصالاً بالإنترنت في هذه الجزئية فقط، وهو ما قد يتعارض مع سياسة العزل التام في بعض المكاتب الجنائية الحساسة.
2. تشفير التطبيقات: لا تزال بعض التطبيقات ذات التشفير المتطور (End-to-End) تتطلب صلاحيات جذر (Root) كاملة للاستخراج العميق، وهو ما يمثل تحدياً مستمراً.

14.4 خاتمة الفصل الرابع

في هذا الفصل، تم عرض النتائج العملية لنظام DZ ForensiGuard، بدءاً من بيئة التطوير والتنفيذ (Intel Core i3 7th Gen, 16GB RAM, 256GB SSD, Windows 10)، مروراً بلغات البرمجة والتقنيات المستخدمة، وصولاً إلى هندسة النظام وقاعدة البيانات وواجهات (API).

كما تم استعراض الخوارزميات الست المطبقة في النظام (الجدول الزمني، تحليل المواقع الجغرافية، تحليل شبكة العلاقات، تحليل الانترنت، التحقق من سلامة الملفات، كشف نوع الملفات)، بالإضافة إلى آلية سلسلة العهدة المتقدمة المبنية على SHA-256. تم عرض 16 واجهة من واجهات النظام المختلفة، بدءاً من واجهة تسجيل الدخول وصولاً إلى واجهة طلب حساب جديد. كما تم تقديم مقارنة عامة مع الأنظمة التجارية أظهرت تفوق النظام المقترح في جوانب دعم اللغة العربية والشفافية والتحكم الكامل بالبيانات. يمثل هذا الفصل الأساس العملي الذي يثبت جدوى النظام وقدرته على المنافسة في مجال التحليل الجنائي الرقمي للهواتف المحمولة.

خاتمة عامة

نختتم هذا البحث الذي سلط الضوء على أحد أكثر المجالات حيوية وحساسية في الأمن السيبراني المعاصر، وهو التحليل الجنائي الرقمي للهواتف الذكية. لقد توجت هذه الدراسة بتطوير منصة DZ ForensiGuard، التي تمثل نموذجاً تقنياً لبيئة برمجية متكاملة تدمج بين هندسة البرمجيات الرصينة وخوارزميات التحليل الآلي. لقد حققت الدراسة أهدافها من خلال التأسيس النظري، والمسح الشامل للتقنيات الراهنة، وصولاً إلى التصميم المعماري والتنفيذ البرمجي الذي يدعم الخصوصية اللغوية العربية والتحليل المتعدد للبيانات، مع ضمان معايير السلامة الرقمية عبر سلسلة عهدة مشفرة أثبتت كفاءة عالية في بيئات الاختبار التجريبية.

أما بخصوص الآفاق المستقبلية لهذا العمل، فإننا نتطلع إلى تطوير وتوسيع منصة DZ ForensiGuard من خلال التركيز على المحاور التالية:

- دعم التحليل الجغرافي المتقدم (Geolocation Analysis): لتتبع ورسم مسارات التحركات الجغرافية للأدلة الرقمية بدقة عالية.
- دمج تقنية Blockchain: لحماية الأدلة الرقمية وضمان عدم قابليتها للتعديل أو التلاعب في سجل التدقيق وسلسلة العهدة.
- دعم استخراج البيانات والأدلة من أجهزة iOS: لتوسيع نطاق التوافقية البرمجية للمنصة وعدم حصرها في بيئات معينة.
- التحليل الفوري (Real-Time Forensics): لتوفير واجهات استخلاص وتحليل لحظي للأدلة الرقمية أثناء التحقيق.
- دمج نماذج التعلم العميق المتقدمة لأتمتة كشف الأنماط في الوسائط، وتوسيع نطاق المنصة ليشمل التحليل الجنائي السحابي.

وفي ضوء هذه التجربة، نوصي المؤسسات الأكاديمية بتعزيز المناهج الدراسية بمختبرات عملية للتحليل الجنائي الرقمي، كما نحث المطورين والباحثين على الاستمرار في بناء الأدوات المحلية والمستقلة لتعزيز أمن البيانات الحساسة. ومن الضروري أيضاً تحديث القوانين الإجرائية لتتلاءم مع التطور في الأدلة الرقمية، مع اعتماد معايير تقنية واضحة لقبول نتائج المنصات الجنائية الآلية أمام الهيئات المختصة. ختاماً، نأمل أن تكون منصة DZ ForensiGuard نواة بحثية تسهم في تطوير أدوات التحليل الجنائي وتوطين الخبرات التقنية في هذا المجال.

وأخر دعوانا أن الحمد لله رب العالمين.

المراجع

- [1] address: .2026 ,21 May on visited .2019 ,jobs and principles, Definition, security? information is What Online, CSO <https://www.csoonline.com/>
- [2] .2016 Learning, Cengage Boston: 6th. ,Security Information of Principles Mattord, J. H. and Whitman E. M.
- [3] <https://www.ibm.com/topics/information-security> address: .2026 ,21 May on visited .2022 ,security? information is What Security, IBM
- [4] .2013 Press, CRC Raton: Boca .Standards and Procedures, Policies, Security Information Peltier, R. T.
- [5] <https://www.cyber.gouv.fr/> address: .2026 ,21 May on visited .2021 ,cybersécurité la à Introduction CyberEdu, - ANSSI
- [6] National Rev.1)", 12-800 (SP Security Information to Introduction "An Technology, and Standards of Institute National <https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-12r1.pdf> address: .2026 ,4 May on visited .2017 Technology, and Standards of Institute
- [7] Telecommunication International , "2020 (GCI) Index Cybersecurity "Global Union, Telecommunication International <https://www.itu.int/> address: .2026 ,21 May on visited .2020 Union,
- [8] for Agency Union European , "2023 Landscape Threat "ENISA (ENISA), Cybersecurity for Agency Union European <https://www.enisa.europa.eu/> address: .2026 ,21 May on visited .2023 Cybersecurity,
- [9] for Organization International Geneva: ,Requirements — Systems Management Security Information :27001 ISO/IEC .2013 Standardization,
- [10] (SP Response Incident into Techniques Forensic Integrating to "Guide Technology, and Standards of Institute National <https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-86.pdf> address: .2026 ,21 May on visited .2006 Technology, and Standards of Institute National , "(86-800
- [11] أ.ع. الله، "إطار عمل للتحقيق الجنائي الرقمي في بيئة الحوسبة السحابية"، thesis, PhD, جامعة الملك سعود، الرياض، المملكة العربية السعودية، 2019.
- [12] Press, Academic 3rd. ,Internet the and Computers, Science, Forensic Crime: Computer and Evidence Digital Casey, E. .2011

- [13] International ,Evidence Digital of Preservation and Acquisition Collection, Identification, for Guidelines :27037 ISO/IEC 2012 Standardization, for Organization
- [14] <https://volatili address: .2026 ,4 May on visited .2022 ,Framework Forensics Memory Volatility Foundation, Volatility tyfoundation.org>
- [15] Rev.1)", 101-800 (SP Forensics Device Mobile on ``Guidelines Technology, and Standards of Institute National <https://nvlpub address: .2026 ,4 May on visited .2014 rep., tech. Technology, and Standards of Institute National s.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-101r1.pdf>
- [16] ,Applications Computer of Journal International Overview", An Forensics: ``Mobile Dharaskar, R. and Ahmed R. 2016 ,5—1 pp. ,22 no. ,114 vol.
- [17] خ. م. و. علي, ``تحديات التحليل الجنائي للهواتف الذكية في العالم العربي", المجلة العربية للأمن السيبراني, 67—45 pp. ,2 no. ,5 vol. ,2020
- [18] <https://www.sleuthkit.org> address: .2026 ,4 May on visited .Documentation Kit Sleuth The Kit, Sleuth The
- [19] <https://www.autopsy.com> address: .2026 ,4 May on visited .2023 ,Platform Forensics Digital Autopsy Autopsy,
- [20] <https://www.wireshark.org/do address: .2026 ,4 May on visited .2023 ,Guide User Wireshark Foundation, Wireshark cs/>
- [21] <https://www.opentext.com/products/encase> address: .2026 ,4 May on visited .2023 ,Forensic EnCase OpenText,
- [22] <https://accessdata.com> address: .2026 ,4 May on visited .2023 ,(FTK) Toolkit Forensic AccessData,
- [23] .2021 ,312—301 pp. ,38 vol. ,Investigation Digital Forensics", Digital in Intelligence ``Artificial Schartner, P. and Rass S.
- [24] <https://www.ibm.com/topics/big-data> address: .2026 ,4 May on visited Data?", Big is ``What IBM.
- [25] .2016 Press, MIT .Learning Deep Courville, A. and Bengio, Y. Goodfellow, I.
- [26] [https://www.ibm.com/topics/artificial-intelli address: .2026 ,4 May on visited Intelligence?", Artificial is ``What IBM. gence](https://www.ibm.com/topics/artificial-intelli address: .2026 ,4 May on visited Intelligence?)
- [27] <https://scikit-learn.org> address: .2026 ,4 May on visited .2023 ,Python in Learning Machine Scikit-learn: Scikit-learn,
- [28] .2020 ,43—36 pp. ,1 no. ,63 vol. ,ACM the of Communications Interpretability", Model of Mythos ``The Lipton, C. Z.
- [29] <https://arxiv.org/abs/2001.09977> address: .2026 ,4 May on visited Addison-Wesley, Boston: 2nd. ,Guide User Language Modeling Unified The Jacobson, I. and Rumbaugh, J. Booch, G. .2005

- [30] <https://www.omg.org/spec/UML/2.5.1/> address: .2026 ,12 May on visited .2017 ,Specification Diagrams Case Use (OMG), Group Management Object
- [31] <https://www.omg.org/spec/UML/2.5.1/> address: .2026 ,12 May on visited .2017 ,1.5.2 ,Specification Language Modeling Unified OMG (OMG), Group Management Object
- [32] <https://www.omg.org/spec/UML/2.5.1/> address: .2026 ,12 May on visited .2017 ,Specification Diagrams Class (OMG), Group Management Object
- [33] .2013 ,Institute Engineering Software Practice", in Architecture "Software Kazman, R. and Clements, P. Bass, L.
- [34] <https://www.omg.org/spec/UML/2.5.1/> address: .2026 ,12 May on visited .2017 ,Specification Diagrams Sequence (OMG), Group Management Object
- [35] ,423–379 pp. ,3 no. ,27 vol. ,Journal Technical System Bell Communication", of Theory Mathematical "A Shannon, E. C. .1948
- [36] ,Privacy & Security IEEE Malware", Packed and Encrypted Find to Analysis Entropy "Using Hamrock, J. and Lyda R. .2007 ,45–40 pp. ,2 no. ,5 vol.
- [37] ع. حسن, "تطوير أداة لاستخراج بيانات تطبيقات المراسلة من هواتف", MA Android", thesis, جامعة العلوم والتكنولوجيا الأردنية, إربد، الأردن, 2021.