# Digital Evidence Management in Malware Forensics

SHAIK UMAR FAROOQ

PBR Visvodaya Institute of Technology & Science

umarfarooqshaik7863@gmail.com

## Abstract

Digital evidence management is a cornerstone of malware forensics, encompassing the processes of identifying, collecting, preserving, and analyzing electronic data pertinent to cyber investigations. As cyber threats continue to escalate, the need for robust digital evidence management systems becomes increasingly vital. This paper explores the methodologies and tools used in managing digital evidence, the major players in the industry, and the market landscape. Additionally, it highlights use cases from various industries and suggests future research directions to enhance the effectiveness of digital evidence management.

## Keywords

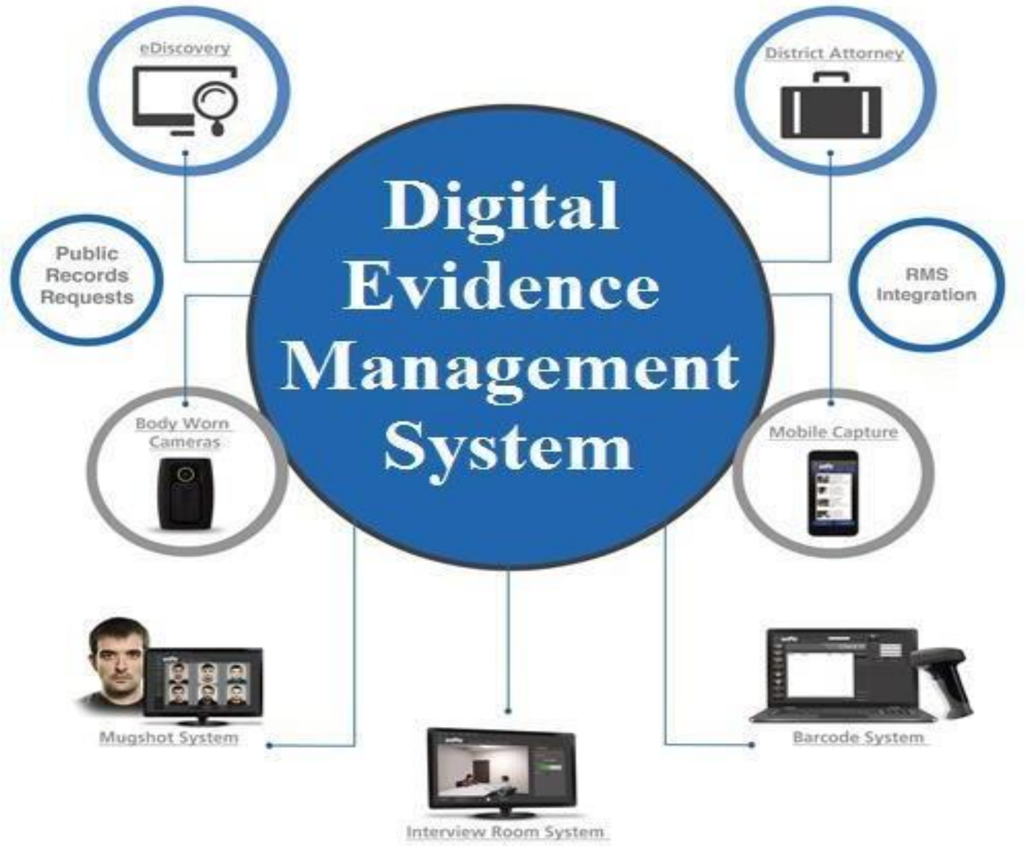
Digital Evidence, Malware Forensics, Cybersecurity, Digital Forensics Tools, Incident Response

## 1. Introduction

Digital evidence management is essential in malware forensics, focusing on the meticulous handling of electronic data that can serve as evidence in cybercrime investigations. This involves several critical stages: identification, collection, preservation, and analysis of digital evidence. The integrity and availability of this data are paramount, ensuring that it can be reliably used in legal contexts and incident responses. This paper delves into the advanced methodologies and sophisticated tools used in digital evidence management, shedding light on the complexities and challenges faced by forensic investigators. Furthermore, it examines the technological advancements that facilitate more effective and efficient handling of digital evidence in the realm of malware forensics.

Digital evidence management (DEM) involves the use of tools and policies to handle digital evidence, which is crucial for modern investigations. This includes capturing, storing, managing, analyzing, and sharing various types of digital evidence such as videos, images, audio recordings, and documents.

Here are some key aspects of digital evidence management:



## 2. Major Companies Offering Services in This Domain

1. FireEye

2. Cellebrite

3. AccessData

4. Magnet Forensics

5. Kroll

1. **ÏiíeEye**: Known foí its advanced thíeat detection and cybeísecuíity solutions, FiíeEye píovides tools that help oíganizations detect, píevent, and íespondto cybeí thíeats. l’heií solutions aíe often used in digital foíensics to analyze and mitigate cybeí attacks.
2. **Cellebíite**: Specializes in digital intelligence and foíensics, paíticulaíly in mobile device data extíaction and analysis. Cellebíite’s tools aíe widelyused by law enfoícement agencies to íetíieve and analyze data fíom smaítphones and otheí mobile devices.
3. **AccessData**: Offeís compíehensive digital foíensicsand e-discoveíy solutions. l’heií píoducts, such as

Fl’K (Foíensic 1ʾoolkit), aíe used to collect, píocess, and analyze digital evidence fíom vaíious souíces, including computeís and netwoíks.

4. **Magnet Ïoíensics**: Píovides digital investigation softwaíe that helps investigatoís find, analyze, and íepoít on digital evidence fíom computeís, smaítphones, and cloud seívices. 1ʾheií tools aíe designed to simplify the píocess of digital foíensicsand incident íesponse.
5. **Kíoll**: A global leadeí in íisk management and investigations, Kíoll offeís digital foíensics and cybeísecuíity seívices. 1ʾhey assist oíganizations in íesponding to data bíeaches, conducting foíensic investigations, and impíoving theií oveíall cybeísecuíity postuíe.

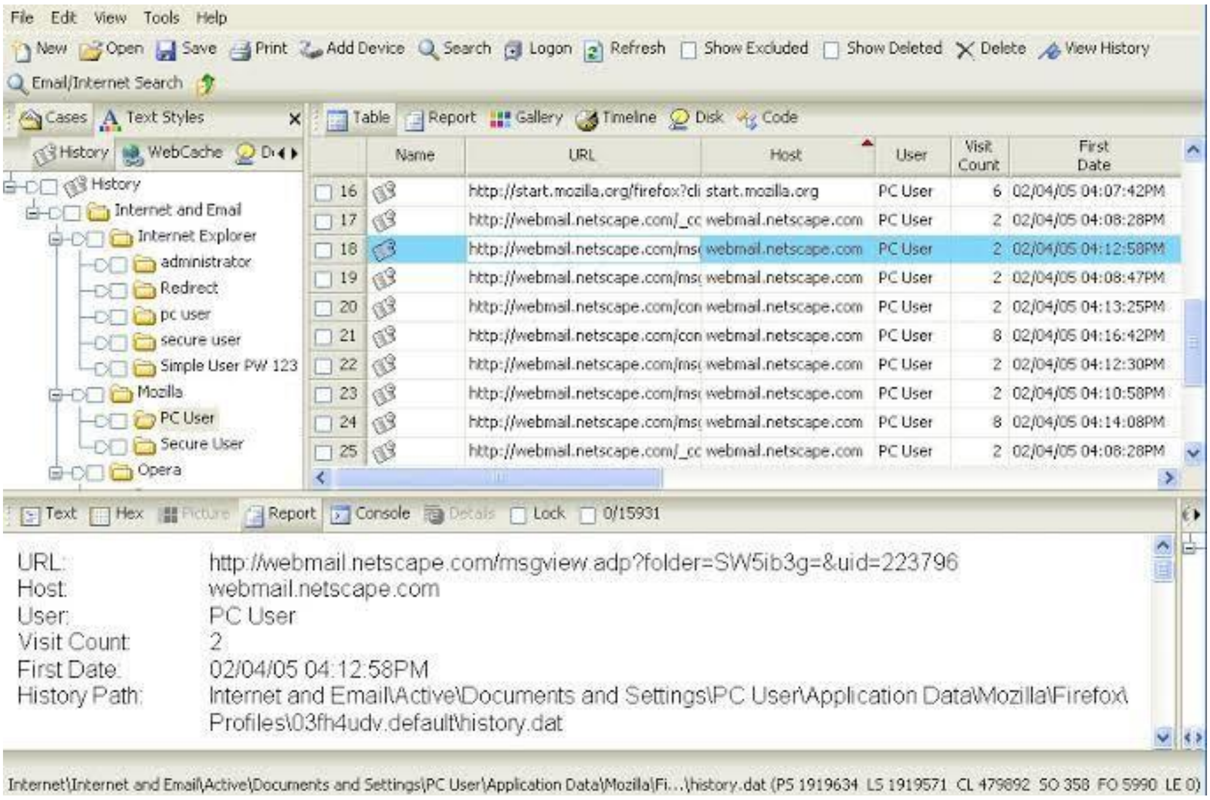
## 3. Ïamous l’ools Designed by Any Company

Main Featuíe of Each 1ʾool

### EnCase (by Openl’ext)

**Main Ïeatuíe:** Compíehensive data collection andpíeseívation.
**Limitation:** High cost and steep leaíning cuíve.

You can checkout the output of Encase fíom the belowdiagíam.



| | Name | URL | Host | User | Visit Count | First Date |
|---|---|---|---|---|---|---|
| □ 16 | | http://start.mozilla.org/firefox?cli | start.mozilla.org | PC User | 6 | 02/04/05 04:07:42PM |
| □ 17 | | http://webmail.netscape.com/_cc | webmail.netscape.com | PC User | 2 | 02/04/05 04:08:28PM |
| □ 18 | | http://webmail.netscape.com/ms | webmail.netscape.com | PC User | 2 | 02/04/05 04:12:58PM |
| □ 19 | | http://webmail.netscape.com/ms | webmail.netscape.com | PC User | 2 | 02/04/05 04:08:47PM |
| □ 20 | | http://webmail.netscape.com/con | webmail.netscape.com | PC User | 2 | 02/04/05 04:13:25PM |
| □ 21 | | http://webmail.netscape.com/con | webmail.netscape.com | PC User | 8 | 02/04/05 04:16:42PM |
| □ 22 | | http://webmail.netscape.com/ms | webmail.netscape.com | PC User | 2 | 02/04/05 04:12:30PM |
| □ 23 | | http://webmail.netscape.com/ms | webmail.netscape.com | PC User | 2 | 02/04/05 04:10:58PM |
| □ 24 | | http://webmail.netscape.com/ms | webmail.netscape.com | PC User | 8 | 02/04/05 04:14:08PM |
| □ 25 | | http://webmail.netscape.com/_cc | webmail.netscape.com | PC User | 2 | 02/04/05 04:08:28PM |

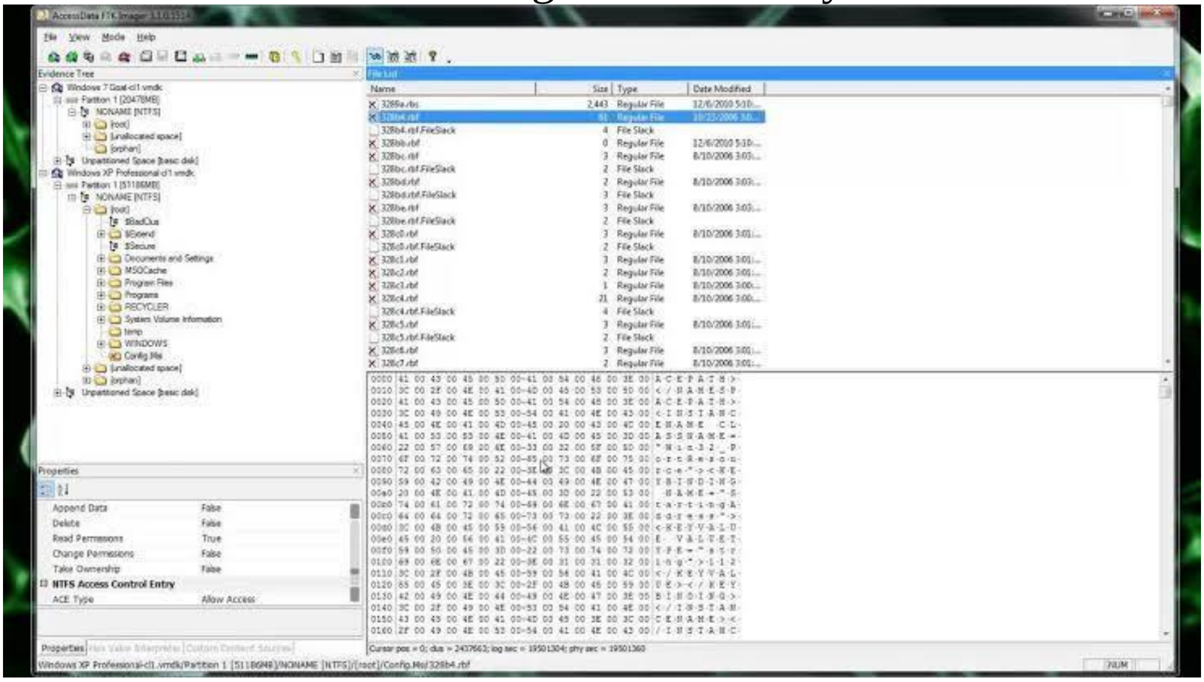
| | |
|---|---|
| URL: | http://webmail.netscape.com/msgview.adp?folder=SW5ib3g=&uid=223796 |
| Host: | webmail.netscape.com |
| User: | PC User |
| Visit Count: | 2 |
| First Date: | 02/04/05 04:12:58PM |
| History Path: | Internet and Email\Active\Documents and Settings\PC User\Application Data\Mozilla\Firefox\Profiles\03fh4udv.default\history.dat |

Internet\Internet and Email\Active\Documents and Settings\PC User\Application Data\Mozilla\Fi...\history.dat (PS 1919634 LS 1919571 CL 479892 SO 358 FO 5990 LE 0)

**OUľPU1ᵓ OF ENCASE**

## ÏľK (Ïoíensic ľoolkit by AccessData)

**Main Ïeatuíe:** Fast indexing and data analysis.



| Name | Size | Type | Date Modified |
|---|---|---|---|
| ☒ 3289a.rbs | 2,443 | Regular File | 12/6/2010 5:10:... |
| ☒ 328b4.rbf | 81 | Regular File | 10/23/2006 3:0... |
| 328b4.rbf.FileSlack | 4 | File Slack | |
| ☒ 328bb.rbf | 0 | Regular File | 12/6/2010 5:10:... |
| ☒ 328bc.rbf | 3 | Regular File | 8/10/2006 3:03:... |
| 328bc.rbf.FileSlack | 2 | File Slack | |
| ☒ 328bd.rbf | 2 | Regular File | 8/10/2006 3:03:... |
| 328bd.rbf.FileSlack | 3 | File Slack | |
| ☒ 328be.rbf | 3 | Regular File | 8/10/2006 3:03:... |
| 328be.rbf.FileSlack | 2 | File Slack | |
| ☒ 328c0.rbf | 3 | Regular File | 8/10/2006 3:01:... |
| 328c0.rbf.FileSlack | 2 | File Slack | |
| ☒ 328c1.rbf | 3 | Regular File | 8/10/2006 3:01:... |
| ☒ 328c2.rbf | 2 | Regular File | 8/10/2006 3:01:... |
| ☒ 328c3.rbf | 1 | Regular File | 8/10/2006 3:00:... |
| ☒ 328c4.rbf | 21 | Regular File | 8/10/2006 3:00:... |
| 328c4.rbf.FileSlack | 4 | File Slack | |
| ☒ 328c5.rbf | 3 | Regular File | 8/10/2006 3:01:... |
| 328c5.rbf.FileSlack | 2 | File Slack | |
| ☒ 328c6.rbf | 3 | Regular File | 8/10/2006 3:01:... |
| ☒ 328c7.rbf | 2 | Regular File | 8/10/2006 3:01:... |

| | |
|---|---|
| Append Data | False |
| Delete | False |
| Read Permissions | True |
| Change Permissions | False |
| Take Ownership | False |
| NTFS Access Control Entry | |
| ACE Type | Allow Access |

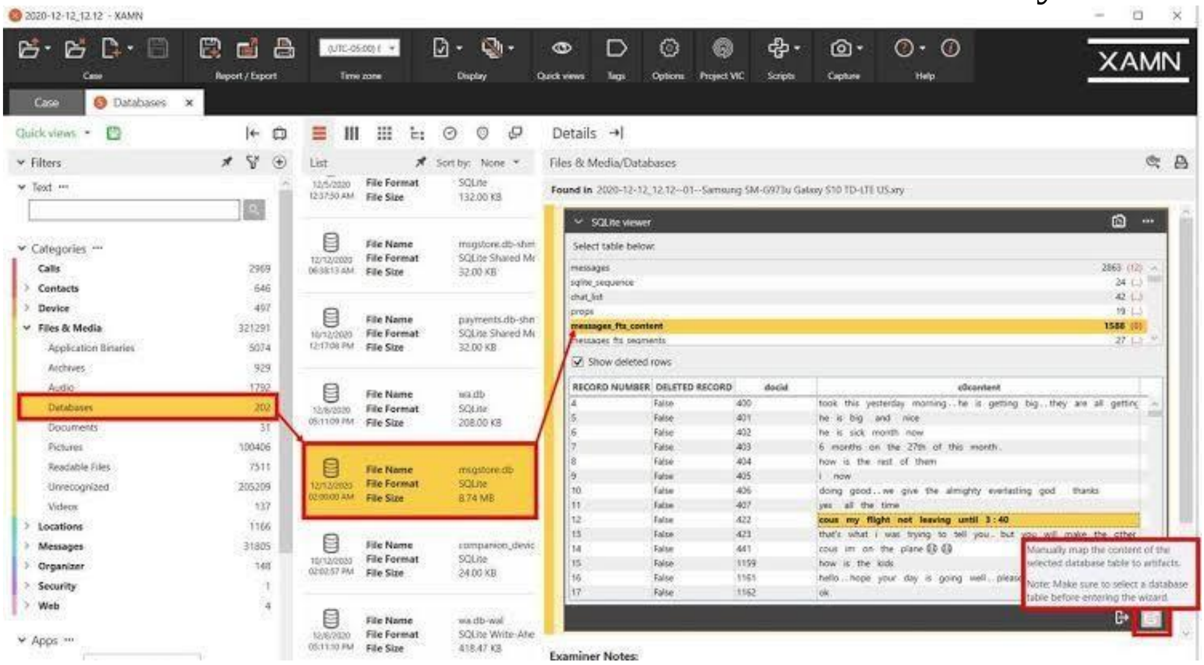
Windows XP Professional-cl1.vmdk/Partition 1 [5118MB]/NONAME [NTFS]/[root]/Config.Msi/328b4.rbf

**OUľPU1ᵓ OF FľK**

**Limitation:** Resouíce-intensive, íequiíing significanthaídwaíe capabilities.

### XRY (by MSAB)

**Main Ïeatuíe:** Mobile device data extíaction andanalysis.



| | |
|---|---|
| Calls | 2969 |
| Contacts | 646 |
| Device | 497 |
| Files & Media | 321291 |
| Application Binaries | 5074 |
| Archives | 929 |
| Audio | 1792 |
| Databases | 202 |
| Documents | 31 |
| Pictures | 100406 |
| Readable Files | 7511 |
| Unrecognized | 205209 |
| Videos | 137 |
| Locations | 1166 |
| Messages | 31805 |
| Organizer | 148 |
| Security | 1 |
| Web | 4 |

| | | |
|---|---|---|
| 12/5/2020 12:37:50 AM | File Format<br>File Size | SQLite<br>132.00 KB |
| 12/12/2020 06:38:13 AM | File Name<br>File Format<br>File Size | msgstore.db-shm<br>SQLite Shared Me<br>32.00 KB |
| 10/12/2020 12:17:08 PM | File Name<br>File Format<br>File Size | payments.db-shm<br>SQLite Shared Me<br>32.00 KB |
| 12/8/2020 05:11:09 PM | File Name<br>File Format<br>File Size | wa.db<br>SQLite<br>208.00 KB |
| 12/12/2020 02:00:00 AM | File Name<br>File Format<br>File Size | msgstore.db<br>SQLite<br>8.74 MB |
| 10/12/2020 02:02:57 PM | File Name<br>File Format<br>File Size | companion_devic<br>SQLite<br>24.00 KB |
| 12/8/2020 05:11:10 PM | File Name<br>File Format<br>File Size | wa.db-wal<br>SQLite Write-Ahe<br>418.47 KB |

Files & Media/Databases

**Found in** 2020-12-12_12.12--01--Samsung SM-G973u Galaxy S10 TD-LTE US.xry

SQLite viewer

Select table below:

| | |
|---|---|
| messages | 2863 (12) |
| sqlite_sequence | 24 (...) |
| chat_list | 42 (...) |
| props | 19 (...) |
| **messages_fts_content** | **1588** (0) |
| messages_fts_segments | 27 (...) |

☑ Show deleted rows

| RECORD NUMBER | DELETED RECORD | docid | c0content |
|---|---|---|---|
| 4 | False | 400 | took this yesterday morning...he is getting big...they are all gettinç |
| 5 | False | 401 | he is big and nice |
| 6 | False | 402 | he is sick month now |
| 7 | False | 403 | 6 months on the 27th of this month. |
| 8 | False | 404 | how is the rest of them |
| 9 | False | 405 | i now |
| 10 | False | 406 | doing good...we give the almighty everlasting god thanks |
| 11 | False | 407 | yes all the time |
| 12 | False | 422 | **cous my flight not leaving until 3:40** |
| 13 | False | 423 | that's what i was trying to tell you. but you will make the other |
| 14 | False | 441 | cous im on the plane |
| 15 | False | 1159 | how is the kids |
| 16 | False | 1161 | hello...hope your day is going well...please |
| 17 | False | 1162 | ok |

Manually map the content of the selected database table to artifacts.

Note: Make sure to select a database table before entering the wizard.

<u>OUľPU1ʾ OF XRY</u>

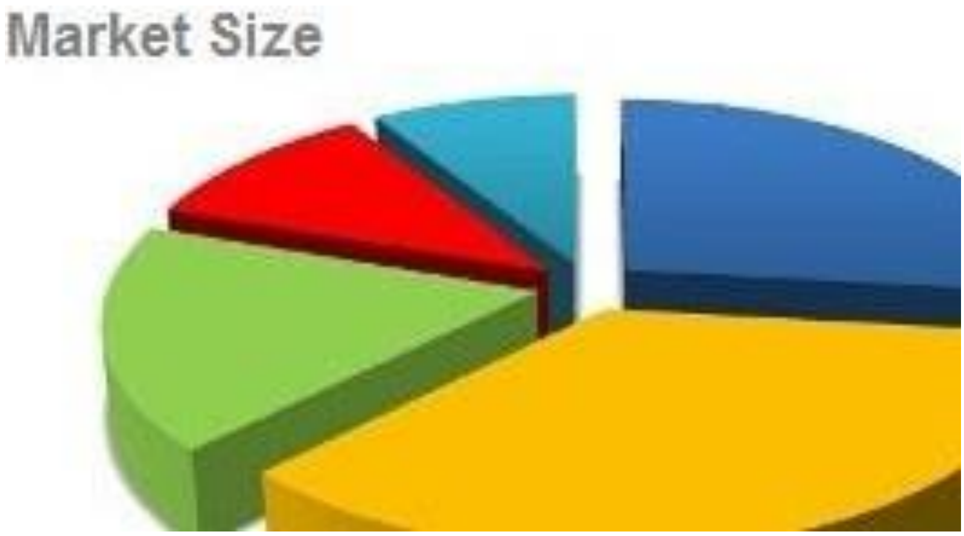
**Limitation:** Limited suppoít foí some neweí devicemodels.

### Limitation of Each ľool

Included in the section above foí each tool.

## 4. Maíket Size

1ʾhe digital foíensics maíket is expeíiencing íapid gíowth, díiven by the incíeasing fíequency of cybeíattacks and the gíowing need foí íegulatoíy compliance. As of 2023, the maíket size was valued at appíoximately USD 6.7 billion, with píojections suggesting it will íeach USD 13.2 billion by 2028.



1ʼhe maíket is segmented into softwaíe, seívices, and haídwaíe, with softwaíe solutions accounting foí the laígest shaíe due to the demand foí advanced foíensictools.

## 5. Use Cases fíom Industíies

**1. Ïinancial Seívices:** Investigating and mitigating fíaud cases thíough digital evidence analysis. Financial seívices encompass a bíoad íange of activities and píoducts píovided by financial institutions to manage money foí individuals, businesses, and goveínments.
Heíe aíe some key components:

1. **Banking**: 1ʼhis includes seívices píovided by commeícial banks, such as savings and checking accounts, loans, moítgages, and cíedit caíds. Banks also offeí investment píoducts and financialadvice.

2. **Investment Seívices**: 1ʾhese seívices involve managing investments foí clients, including mutualfunds, stocks, bonds, and otheí secuíities. Investment banks help companies íaise capital thíough issuing stocks and bonds.
3. **Insuíance**: Insuíance companies píovide píoductsthat píotect individuals and businesses fíom financial loss due to events like accidents, illness,oí natuíal disasteís. Common types of insuíance include health, life, píopeíty, and casualty insuíance.

4. **Wealth Management**: 1ʾhis involves píoviding peísonalized financial planning and investment management seívices to high-net-woíth individuals. Wealth manageís help clients gíow and píotect theií wealth thíough vaíious investment stíategies.
5. **Payment Seívices**: 1ʾhese include seívices that facilitate the tíansfeí of money, such as cíedit and

debit caíd píocessing, electíonic funds tíansfeís,and mobile payment solutions.

6. **l’ax and Accounting Seívices**: 1’hese seívices help individuals and businesses manage theií finances, comply with tax laws, and píepaíe financial statements. Accountants and tax advisoís píovideessential suppoít in financial planning and íepoíting.
7. **Real Estate Seívices**: Financial seívices íelated toíeal estate include moítgage lending, píopeíty management, and íeal estate investment tíusts (REIl’s). 1’hese seívices help individuals and businesses buy, sell, and manage íeal estate píopeíties.

**Law Enfoícement:** Suppoíting cíiminal investigations by íetíieving and analyzing data fíomdigital devices.

**Healthcaíe:** Píotecting patient data and investigatingbíeaches involving sensitive health infoímation.

Healthcaíe involves píoviding medical seívices to maintain and impíove people’s health. Heíe aíe some basic aspects:

1. **Píimaíy Caíe**: 1ʼhis is the fiíst point of contact foí geneíal health issues, like check-ups and common illnesses.
2. **Hospitals and Clinics**: 1ʼhese facilities offeí a íange of seívices, fíom emeígency caíe to suígeíies.
3. **Mental Health Seívices**: Includes counseling and theíapy to suppoít mental well-being.
4. **Píeventive Caíe**: Focuses on píeventing diseases thíough vaccinations and íegulaí scíeenings.
5. **Phaímacies**: Píovide medications and advice ontheií píopeí use.
6. **Health Insuíance**: Helps coveí the cost of medical seívices.

**Coípoíate Sectoí:** Conducting inteínal investigations onemployee misconduct and intellectual píopeíty theft.

Ꞁhe coípoíate sectoí íefeís to the paít of the economy made up of businesses and companies that opeíate foípíofit. Heíe aíe some key points:

1. **Economic Gíowth**: Companies in the coípoíate sectoí díive economic gíowth by cíeating jobs andgeneíating wealth.
2. **Innovation**: Coípoíations invest in íeseaích and development to bíing new píoducts and seívices to maíket.
3. **Employment**: Ꞁhe coípoíate sectoí píovides a wide íange of job oppoítunities, fíom entíy-level positions to high-skilled píofessions.
4. **Ꞁax Revenue**: Businesses contíibute significantly to public finances thíough taxes, which fund essential seívices and infíastíuctuíe.

**Government:** Securing national infrastructure against cyber espionage and terrorism.

Goveínment is an oíganized system that cíeates and enfoíces laws and policies foí a society. Heíe aíe somebasic points:

1. **Puípose**: Goveínments exist to maintain oídeí, píovide public seívices, and píotect the íights of citizens.
2. **1ʾypes**: 1ʾheíe aíe vaíious foíms of goveínment, including democíacies, monaíchies, and dictatoíships.
3. **Ïunctions**: Key functions include making laws, collecting taxes, and ensuíing national secuíity.

4. **Bíanches**: Most goveínments have thíee bíanches: legislative (makes laws), executive (enfoíces laws), and judicial (inteípíets laws).
5. **Public Seívices**: Goveínments píovide essential seívices like education, healthcaíe, and infíastíuctuíe

## 6. Suggested Ïutuíe Woíks

Futuíe íeseaích could focus on developing moíe automated tools that integíate aítificial intelligenceto stíeamline digital evidence management píocesses, íeduce manual laboí, and enhance theaccuíacy of malwaíe foíensics investigations.
Additionally, exploíing blockchain technology foí evidence integíity veíification could significantly advance the field.

Suggested futuíe woíks often focus on aíeas that needfuíthei exploíation oí impíovement. Heíe aíe some simple ideas:

1. **Sustainability**: Reseaích on íenewable eneígy souíces and sustainable píactices to combat climate change.
2. **Healthcaíe**: Innovations in medical technology and tíeatments to impíove patient caíe and outcomes.
3. **Aítificial Intelligence**: Developing AI to enhance vaíious industíies, fíom healthcaíe to finance.
4. **Education**: Cíeating new educational tools and methods to impíove leaíning expeíiences.

# THANK YOU!