FORENSIC

Legal Informatics and Multimedia

Forensic Analysis for Computer Systems

Plan of the Labs:

1. Electronic data acquisition
2. Computer Forensics technics and tools
3. Volatility Framework
4. Autopsy (Sleuthkit)
5. FTK (Forensic ToolKit)
6. Guidance software EnCase & ProDiscover Forensic

Course Lab6: Guidance software EnCase & ProDiscover Forensic

6.1 Guidance software EnCase

- 6.1.1 EnCase functionalities
- 6.1.2 A Hard Drive Preview with EnCase
- 6.1.3 EnCase Features

6.2 ProDiscover Forensic

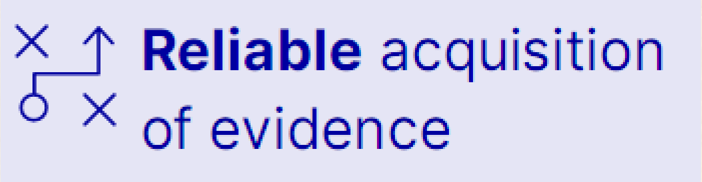
- 6.2.1 ProDiscover Forensics Features
- 6.2.2 ProDiscover Tools
- 6.2.3 ProDiscover Underrated Features

6.1 Guidance software EnCase

EnCase™ Forensic is recognized globally as the standard for digital forensics and is a court-proven solution built for deep-level digital forensic investigation, powerful processing and integrated investigation workflows with flexible reporting options. It is built with a deep understanding of the digital investigation lifecycle and the importance of maintaining evidence integrity.
EnCase Forensic empowers any examiner to seamlessly complete any investigation, including investigations of mobile devices.

Encase Forensic acquires data from a wide variety of devices, completes a forensically sound* investigation and produces extensive reports.

6.1.1 EnCase functionalities



Reliable acquisition of evidence

With EnCase Forensic, examiners can be confident the integrity of the evidence will not be compromised. All evidence captured with EnCase Forensic is stored in the court-accepted EnCase evidence file formats.

*Digital evidence is said to be forensically sound if it was collected, analyzed, handled and stored in a manner that is acceptable by the law, and there is reasonable evidence to prove so.

Deep forensic analysis

EnCase Forensic has been used in thousands of court cases and is known for its ability to uncover evidence that may go unnoticed if analyzed with other solutions.

EnCase Forensic doesn’t just deliver an “artifacts first” approach but also lets investigators dive deep into the operating system to locate artifacts that would otherwise be well-hidden by bad actors.

Mobile collection for 36,000+ profiles

EnCase Forensic supports the latest smartphones and tablets, including more than 36,000 mobile device profiles, all while empowering the examiner to conduct logical and physical acquisitions.

From the new investigator to the seasoned examiner, each level of user can find the evidence they need with mobile acquisitions in EnCase Forensic.

Image analysis

EnCase Forensic artificial intelligence capabilities process images into 12 categories using visual threat intelligence technology.

Examiners can quickly filter by confidence level and identify previously unidentified contraband with near-zero false positives.

Broad OS/ decryption support

Offering the broadest support of operating and file systems, artifacts and encryption types, EnCase Forensic enables the investigator to provide conclusive results with a detailed analysis of findings.

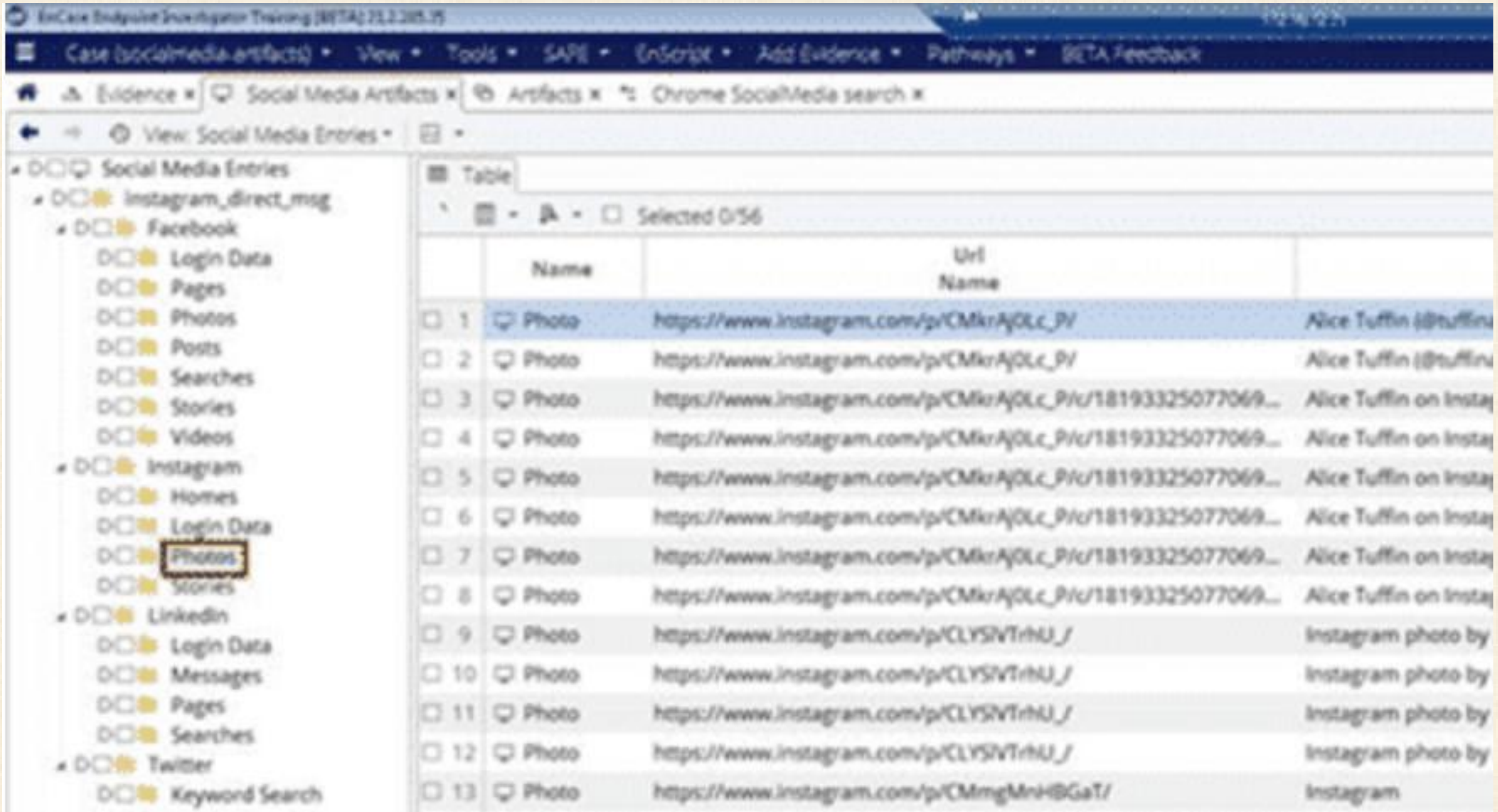
Connected to the cloud

With EnCase Forensic, digital forensic investigators can collect evidence from cloud-based applications, including social media, storage and communication tools.

Optical character recognition

EnCase Forensic users can now take advantage of the popular optical character recognition (OCR) capability. Which helps investigators extract embedded text from scanned images, documents and PDFs. OCR not only helps investigators get to evidence that is hiding but also increases their productivity by automating the task, reducing the time needed to process a case and improving the efficiency of the investigation.

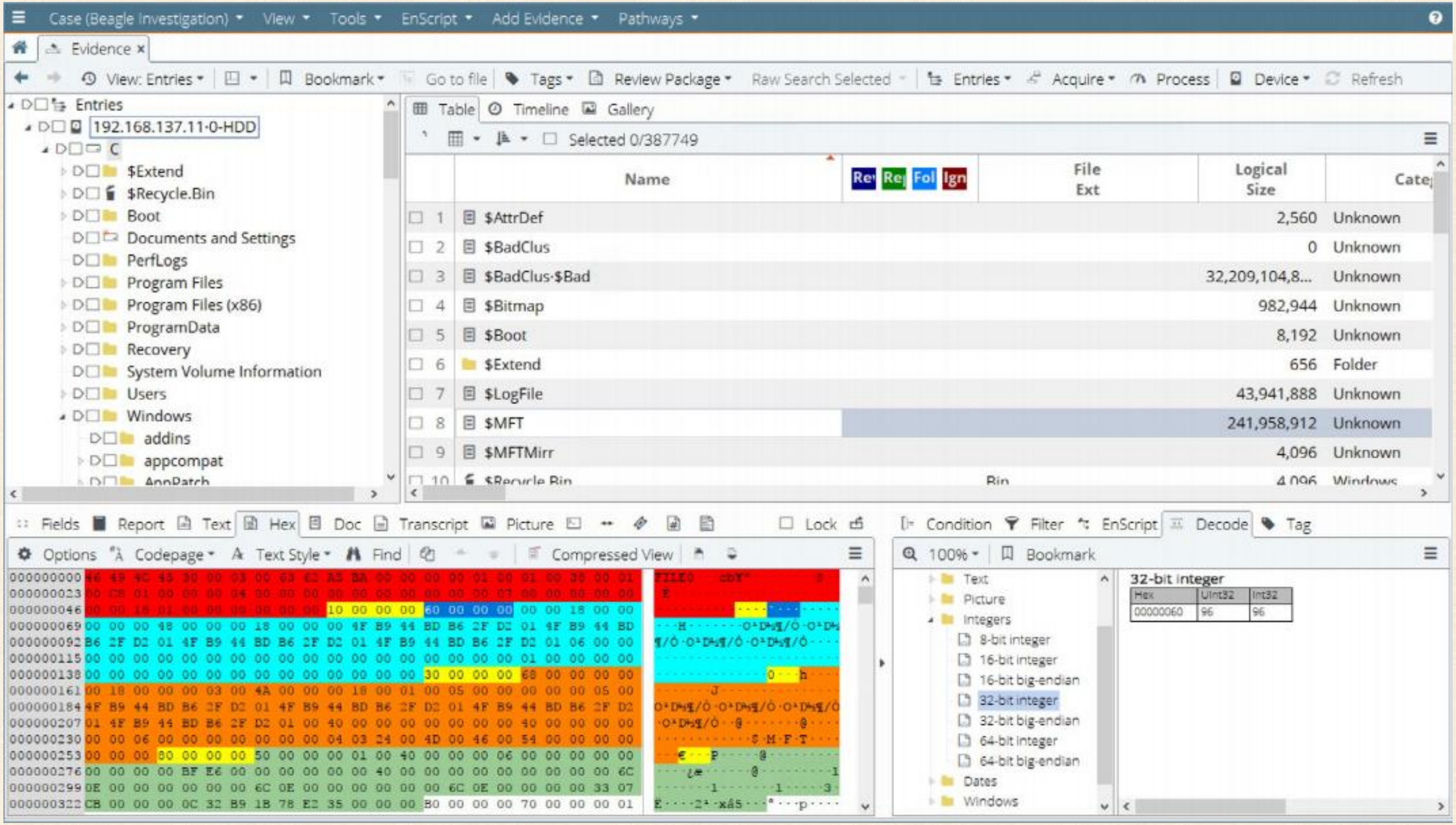
Also included is the ability to uncover more evidence with expanded social media artifact support and the ability to review online content parsed directly from a suspect's browser history. Social media artifact support includes Twitter, Instagram, LinkedIn and Facebook.



	Name	Url Name	
1	Photo	https://www.instagram.com/p/CMkrAj0Lc_P/	Alice Tuffin (@tuffina
2	Photo	https://www.instagram.com/p/CMkrAj0Lc_P/	Alice Tuffin (@tuffina
3	Photo	https://www.instagram.com/p/CMkrAj0Lc_P/c/18193325077069...	Alice Tuffin on Instag
4	Photo	https://www.instagram.com/p/CMkrAj0Lc_P/c/18193325077069...	Alice Tuffin on Instag
5	Photo	https://www.instagram.com/p/CMkrAj0Lc_P/c/18193325077069...	Alice Tuffin on Instag
6	Photo	https://www.instagram.com/p/CMkrAj0Lc_P/c/18193325077069...	Alice Tuffin on Instag
7	Photo	https://www.instagram.com/p/CMkrAj0Lc_P/c/18193325077069...	Alice Tuffin on Instag
8	Photo	https://www.instagram.com/p/CMkrAj0Lc_P/c/18193325077069...	Alice Tuffin on Instag
9	Photo	https://www.instagram.com/p/CLYSlVTrhU_/	Instagram photo by
10	Photo	https://www.instagram.com/p/CLYSlVTrhU_/	Instagram photo by
11	Photo	https://www.instagram.com/p/CLYSlVTrhU_/	Instagram photo by
12	Photo	https://www.instagram.com/p/CLYSlVTrhU_/	Instagram photo by
13	Photo	https://www.instagram.com/p/CMmgMnHBGaT/	Instagram

This enhanced capability allows law enforcement and government agencies to determine social connections between persons-of-interest and discover how recovered artifacts came to be, while successfully used as evidence in court.

6.1.2 A Hard Drive Preview with EnCase



- Entries
  - 192.168.137.11-0-HDD
    - C
      - $Extend
      - $Recycle.Bin
      - Boot
      - Documents and Settings
      - PerfLogs
      - Program Files
      - Program Files (x86)
      - ProgramData
      - Recovery
      - System Volume Information
      - Users
      - Windows
        - addins
        - appcompat
        - AppPatch

	Name	Re Re Fol Ign	File Ext	Logical Size	Cate
□ 1	$AttrDef			2,560	Unknown
□ 2	$BadClus			0	Unknown
□ 3	$BadClus·$Bad			32,209,104,8...	Unknown
□ 4	$Bitmap			982,944	Unknown
□ 5	$Boot			8,192	Unknown
□ 6	$Extend			656	Folder
□ 7	$LogFile			43,941,888	Unknown
□ 8	$MFT			241,958,912	Unknown
□ 9	$MFTMirr			4,096	Unknown
□ 10	$Recycle.Bin		Bin	4,096	Windows

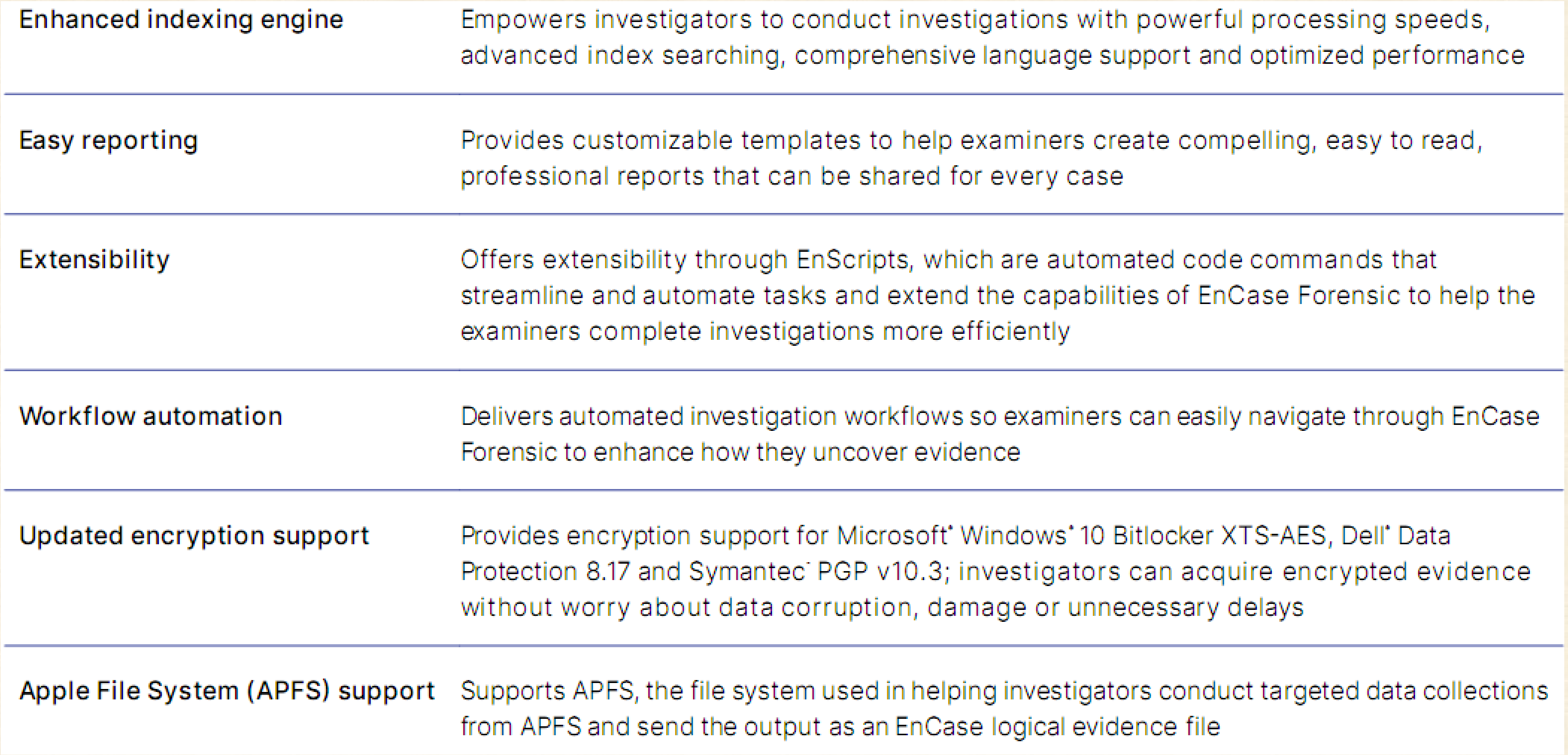
```
000000000 46 49 4C 45 30 00 03 00 63 62 A5 BA 00 00 00 00 01 00 01 00 38 00 01  FILE0···cbY'·········8··
000000023 00 C8 01 00 00 00 04 00 00 00 00 00 00 00 00 00 00 00 07 00 00 00 00 00  ·È·····················
000000046 00 00 18 01 00 00 00 00 00 00 10 00 00 00 60 00 00 00 00 00 18 00 00  ··········`············
000000069 00 00 00 48 00 00 00 18 00 00 00 4F B9 44 BD B6 2F D2 01 4F B9 44 BD  ···H·······O¹D½¶/Ò·O¹D½
000000092 B6 2F D2 01 4F B9 44 BD B6 2F D2 01 4F B9 44 BD B6 2F D2 01 06 00 00  ¶/Ò·O¹D½¶/Ò·O¹D½¶/Ò····
000000115 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 00 00 00  ·······················
000000138 00 00 00 00 00 00 00 00 00 00 00 00 00 00 30 00 00 00 68 00 00 00 00  ··············0···h····
000000161 00 18 00 00 00 03 00 4A 00 00 00 18 00 01 00 05 00 00 00 00 00 05 00  ·······J···············
000000184 4F B9 44 BD B6 2F D2 01 4F B9 44 BD B6 2F D2 01 4F B9 44 BD B6 2F D2  O¹D½¶/Ò·O¹D½¶/Ò·O¹D½¶/Ò
000000207 01 4F B9 44 BD B6 2F D2 01 00 40 00 00 00 00 00 00 00 40 00 00 00 00  ·O¹D½¶/Ò··@·······@····
000000230 00 00 06 00 00 00 00 00 00 00 04 03 24 00 4D 00 46 00 54 00 00 00 00  ············$·M·F·T····
000000253 00 00 00 80 00 00 00 50 00 00 00 01 00 40 00 00 00 06 00 00 00 00 00  ···€···P····@··········
000000276 00 00 00 00 BF E6 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 6C  ····¿æ······@·········l
000000299 0E 00 00 00 00 00 00 6C 0E 00 00 00 00 00 00 6C 0E 00 00 00 00 33 07  ·······l·······l·····3·
000000322 CB 00 00 00 0C 32 B9 1B 78 E2 35 00 00 00 B0 00 00 00 70 00 00 00 01  Ë····2¹·xâ5···°···p····
```

- Text
- Picture
- Integers
  - 8-bit integer
  - 16-bit integer
  - 16-bit big-endian
  - 32-bit integer
  - 32-bit big-endian
  - 64-bit integer
  - 64-bit big-endian
- Dates
- Windows

32-bit integer

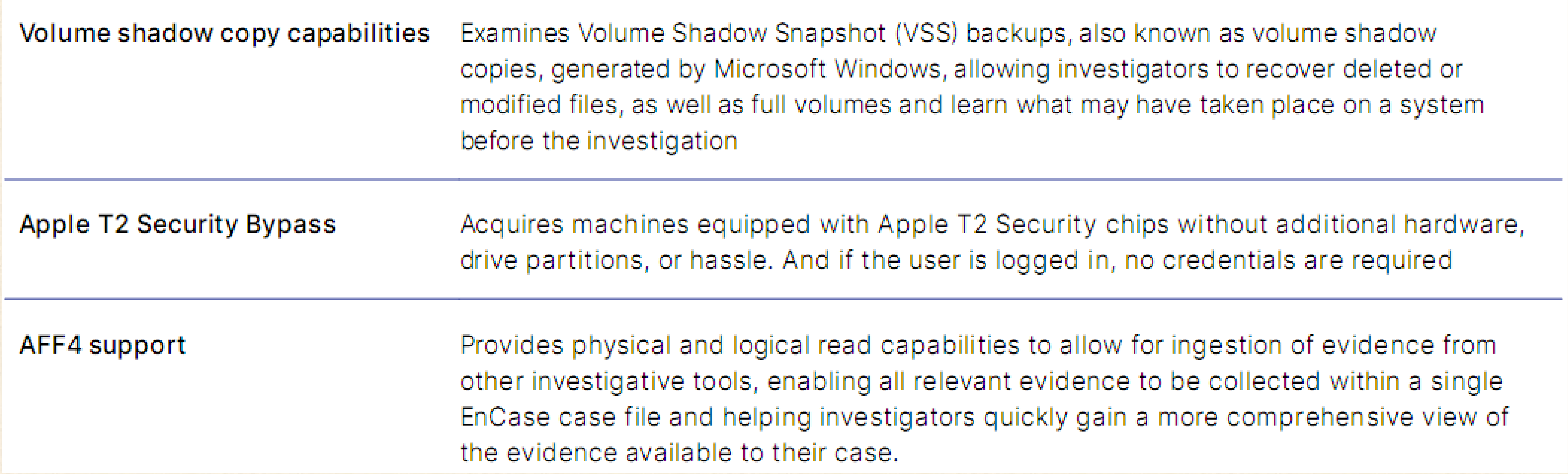
Hex	UInt32	Int32
00000060	96	96

6.1.3 EnCase Features



Enhanced indexing engine	Empowers investigators to conduct investigations with powerful processing speeds, advanced index searching, comprehensive language support and optimized performance
Easy reporting	Provides customizable templates to help examiners create compelling, easy to read, professional reports that can be shared for every case
Extensibility	Offers extensibility through EnScripts, which are automated code commands that streamline and automate tasks and extend the capabilities of EnCase Forensic to help the examiners complete investigations more efficiently
Workflow automation	Delivers automated investigation workflows so examiners can easily navigate through EnCase Forensic to enhance how they uncover evidence
Updated encryption support	Provides encryption support for Microsoft® Windows® 10 Bitlocker XTS-AES, Dell® Data Protection 8.17 and Symantec® PGP v10.3; investigators can acquire encrypted evidence without worry about data corruption, damage or unnecessary delays
Apple File System (APFS) support	Supports APFS, the file system used in helping investigators conduct targeted data collections from APFS and send the output as an EnCase logical evidence file

6.1.3 EnCase Features (Cont.)



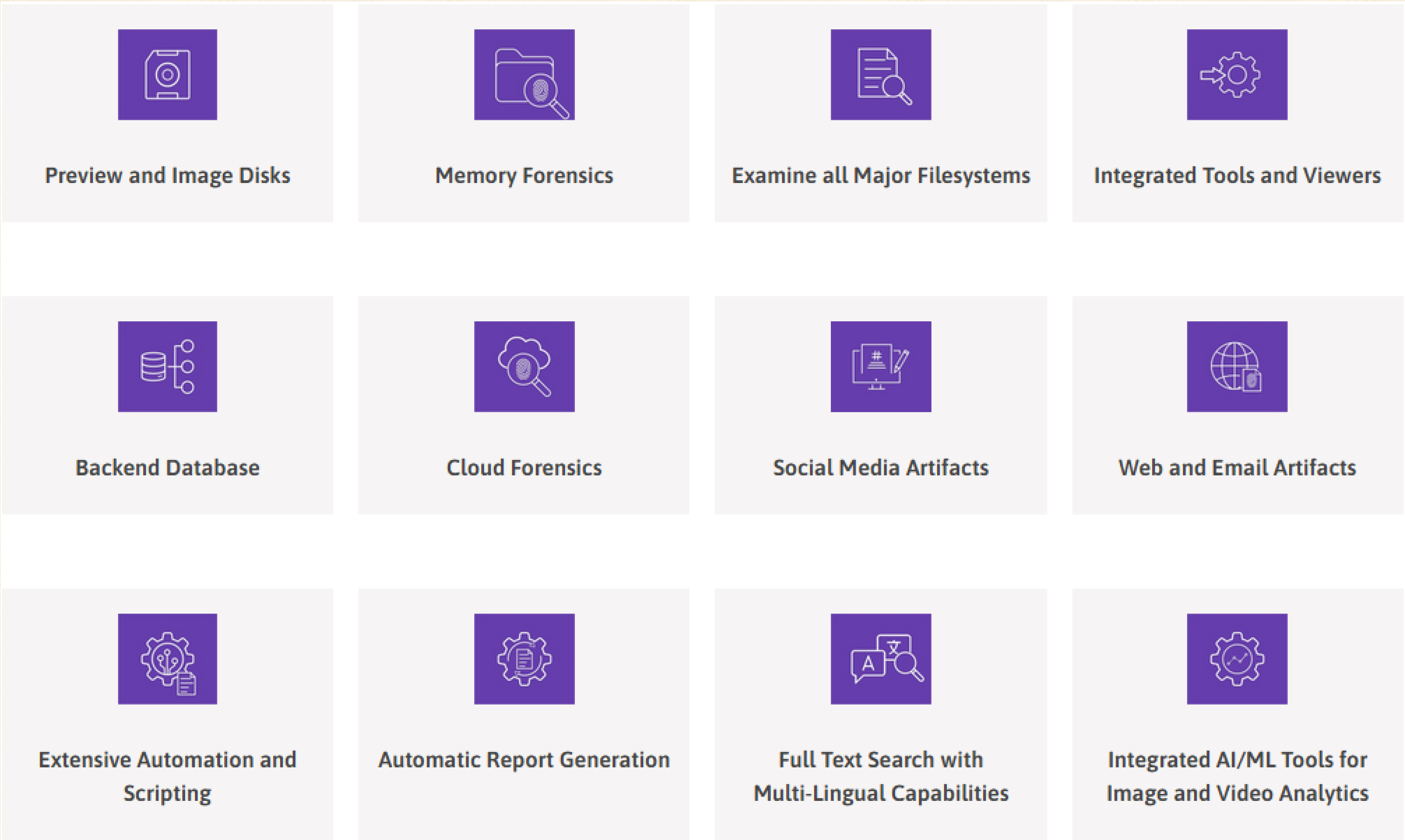
Volume shadow copy capabilities	Examines Volume Shadow Snapshot (VSS) backups, also known as volume shadow copies, generated by Microsoft Windows, allowing investigators to recover deleted or modified files, as well as full volumes and learn what may have taken place on a system before the investigation
Apple T2 Security Bypass	Acquires machines equipped with Apple T2 Security chips without additional hardware, drive partitions, or hassle. And if the user is logged in, no credentials are required
AFF4 support	Provides physical and logical read capabilities to allow for ingestion of evidence from other investigative tools, enabling all relevant evidence to be collected within a single EnCase case file and helping investigators quickly gain a more comprehensive view of the evidence available to their case.

6.2 ProDiscover Forensic

ProDiscover Forensics is a comprehensive digital forensics software that empowers investigators to capture key evidence from computer systems. ProDiscover has capabilities to handle all aspects of an in-depth forensic investigation to collect, preserve, filter, and analyze evidence.

An investigator can use the tools and features of ProDiscover to identify discrete bits of evidence and connect those to form a cohesive picture. ProDiscover provides capabilities to analyze the nature and the modalities of the cybercrime. Evidentiary quality reports can be prepared and presented in the court of law.

6.2.1 ProDiscover Forensics Features



- Preview and Image Disks
- Memory Forensics
- Examine all Major Filesystems
- Integrated Tools and Viewers
- Backend Database
- Cloud Forensics
- Social Media Artifacts
- Web and Email Artifacts
- Extensive Automation and Scripting
- Automatic Report Generation
- Full Text Search with Multi-Lingual Capabilities
- Integrated AI/ML Tools for Image and Video Analytics

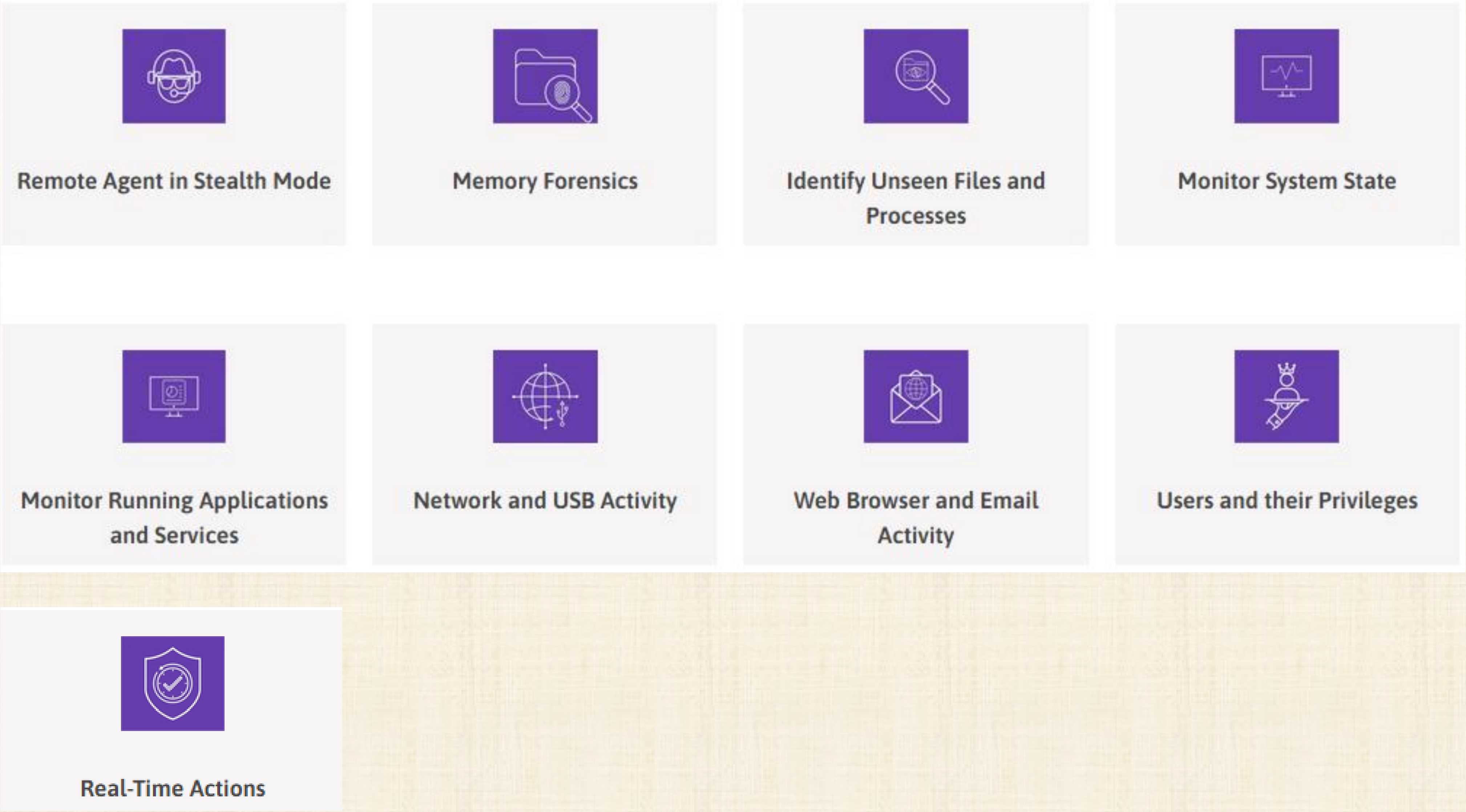
6.2.2 ProDiscover Tools

6.2.2.1 ProDiscover Incident Response

ProDiscover Incident Response (IR) has capabilities to determine if a system has been compromised and to what extent. Corporate network security personnel can take action in real-time to protect such systems under attack from malicious hackers and disgruntled employees.

ProDiscover is a digital forensics product company founded in 2001. ProDiscover Pro is dashboard and management tool for the company's ProDiscover Forensics and ProDiscover Incident Response solutions. ProDiscover Forensics offers a wide variety of features to handle every aspect of an in-depth forensic investigation to collect, preserve, filter, and analyze evidence. This includes integrated AI/ML tools for image and video analytics, extensive automation and scripting, cloud forensics, and automatic report generation. ProDiscover Incident Response can determine the scale of a breach or compromise through features such as memory forensics, real-time actions, system state monitoring, and user privilege management.

Additional Features with ProDiscover Incident Response



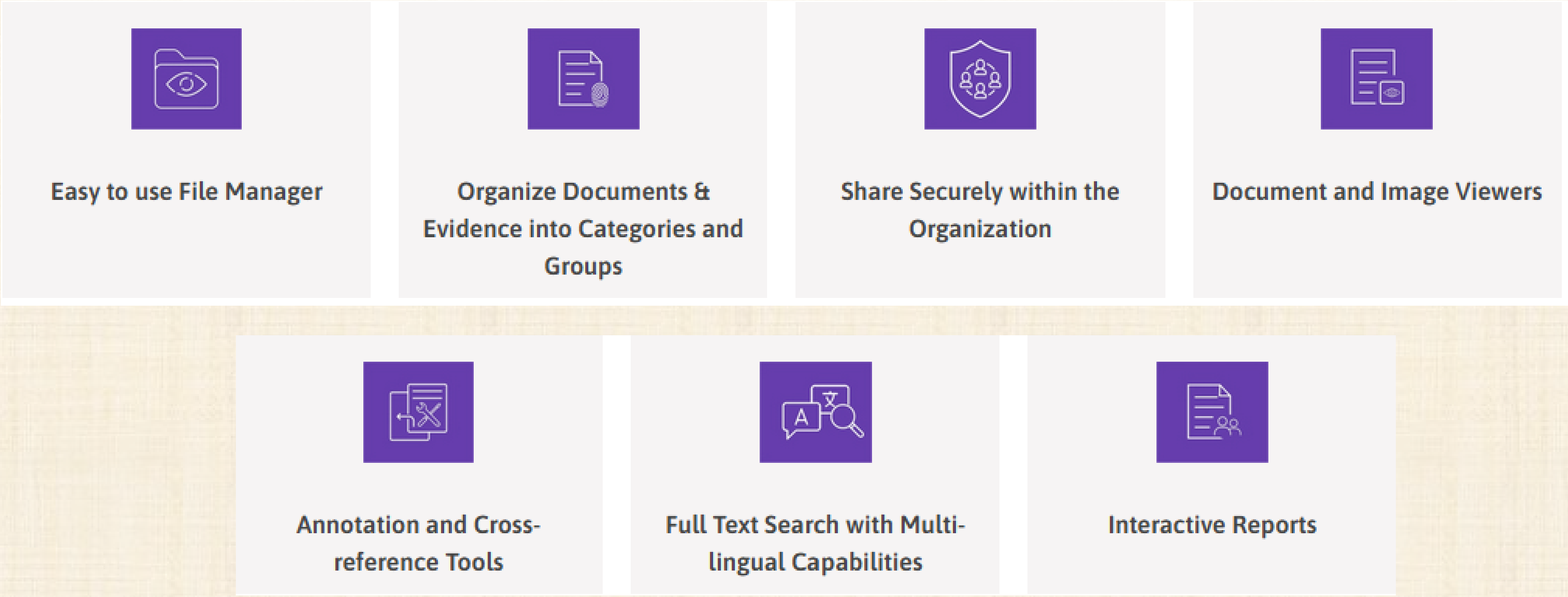
- Remote Agent in Stealth Mode
- Memory Forensics
- Identify Unseen Files and Processes
- Monitor System State
- Monitor Running Applications and Services
- Network and USB Activity
- Web Browser and Email Activity
- Users and their Privileges
- Real-Time Actions

6.2.2.2 ProDiscover Pro

A repository and dashboard for ProDiscover Forensics and ProDiscover Incident Response. The Pro version can be hosted on premises for collaborative investigations.

Data and files from computer systems and remote services that are being investigated or monitored, can be stored, organized, and collaboratively reviewed by authorized investigators.

Additional Features with ProDiscover Pro



Easy to use File Manager

Organize Documents & Evidence into Categories and Groups

Share Securely within the Organization

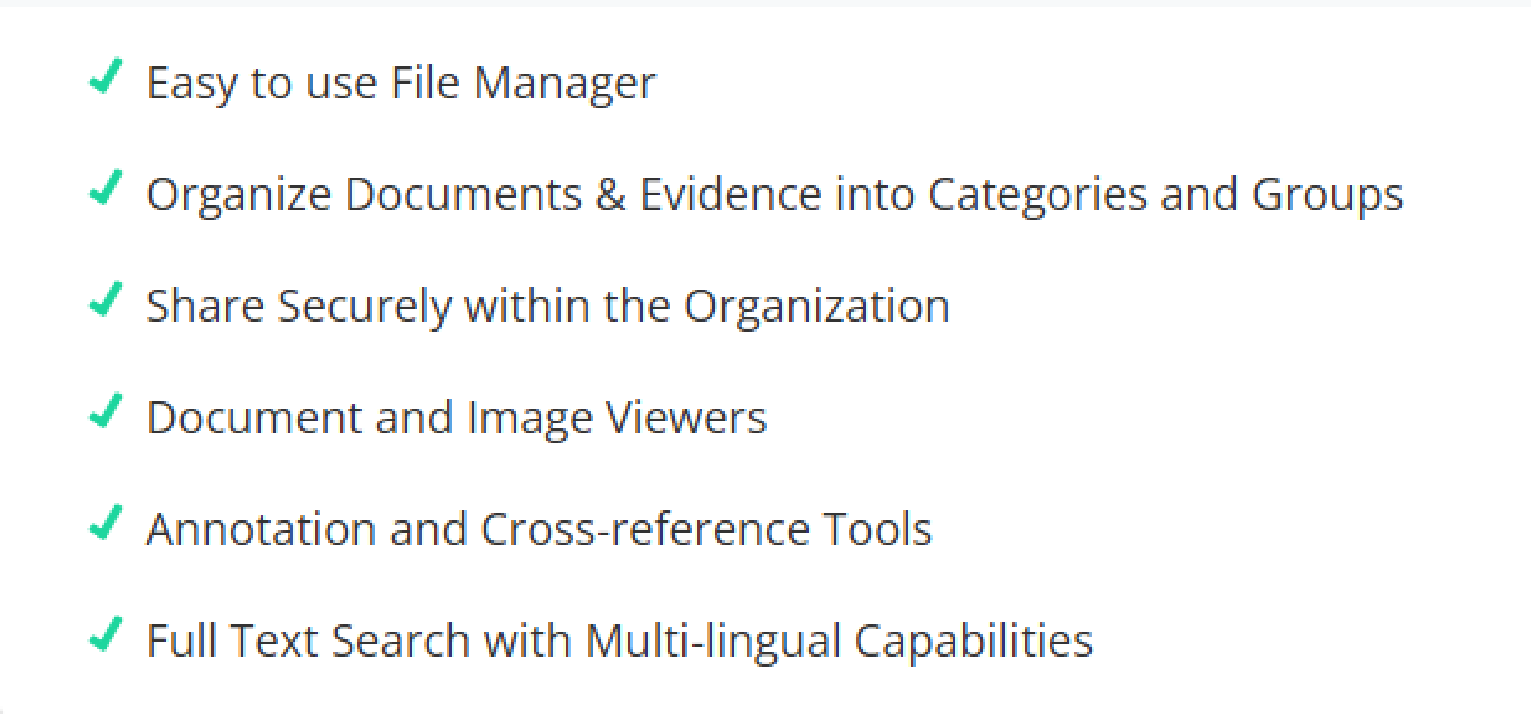
Document and Image Viewers

Annotation and Cross-reference Tools

Full Text Search with Multi-lingual Capabilities

Interactive Reports

6.2.3 ProDiscover Underrated Features



- ✓ Easy to use File Manager
- ✓ Organize Documents & Evidence into Categories and Groups
- ✓ Share Securely within the Organization
- ✓ Document and Image Viewers
- ✓ Annotation and Cross-reference Tools
- ✓ Full Text Search with Multi-lingual Capabilities