**Concordia** **Institute** **for** **Information** **Systems** **Engineering** **(CIISE)**

**INSE** **6610** **–** **Cybercrime** **Investigation**

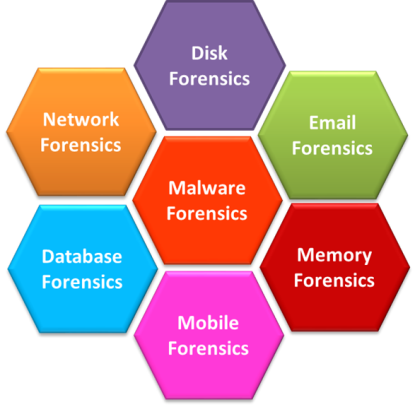
**Project** **Proposal**

**The** **use** **of** **software** **and** **hardware** **tools** **in** **cybercrime** **investigations:** **Survey** **and** **Comparison** **Submitted** **to**

Dr. Ivan Pustogarov

|  |  |  |  |
| --- | --- | --- | --- |
| **Name** | **Student** **Id** | **Name** | **Student** **Id** |
| Md. Saiduzzaman | 40256249 | Tejas Surani | 40248859 |
| Mansoureh Navidpanahtoupkanl | 40221901 | Simanta Sen | 40187190 |
| Reed Alsuwaidi | 40195502 | Mohammad Zawad Tahmeed | 40196436 |
| Md. Aminul Islam | 40203451 | Taufiq al din | 40217260 |
| Mustary Sultana Mim | 40219439 | Saif Manjar Ahmad | 40217056 |
| Md Yeasin Arafat | 40181574 |  |  |

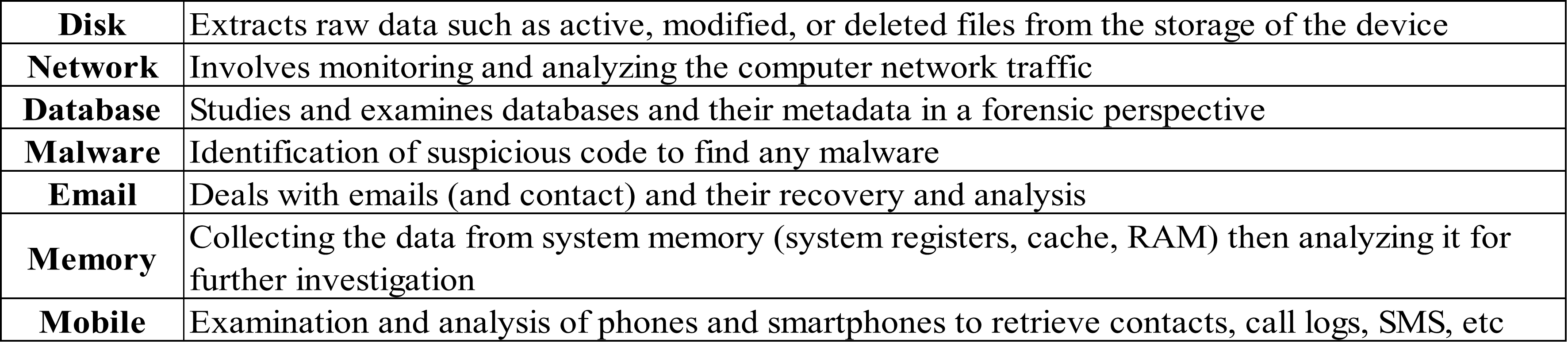
**Introduction**

The quick development of digital technology has created new chances for attackers to devise novel and complex attack strategies to bypass defenses, trap targets, and bypass security measures. The involvement of digital forensics is required since the investigative process and diversity of tools provide an efficient way to extract evidence as well as a strategy to detect and protect against various cybercrimes.

Digital forensics has been divided into a variety of groups, including

Disk, Email, Memory, Mobile, Database, Network, Malware and so on.

Fig: Areas of Digital Forensics

**Arenas** **of** **Digital** **Forensic**

**Phases** **of** **Digital** **Forensic**

**Identification**

**Preservation**

**Analysis**

**Documentation**

**Presentation**

deals with what evidence is present, where and how it is stored

Data is isolated, secured, and preserved from unauthorized use of digital devices so that digital evidence is not tampered with and making a copy of the original evidence

When the investigators do the data defragmentation to draw a correct conclusion based on evidence.

All visible data obtained is gathered and helps to be used as a crime scene reconstruction.

All the findings are produced and presented as a report in a court for further investigations.

**Methodology**

Ø List down all the available tools used for Digital forensic analysis Ø Categorized the tools based on Functional Domains

Ø Perform Phase wise feature comparison among all the tools

**Device** **Forensic**

**Software** **Forensic** **Analysis**

**Digital** **Forensic**

**Hardware** **Forensic** **Analysis**

**Network** **Forensic**

**Memory** **Forensic**

**Software** **and** **Hardware** **Forensic** **Tools**

AntAnalyzer Forensic Workstation

Hardware Forensic tools

Tableau Write blocker Kit

**opsy** •**EnCase** •**FTK** **Imager** •**OSForensics** •**Sleuth** **Kit** •**Foremost**

**Forencis**

•**Volatility** **workstation**

•**Exif** **tool**

•**Network** **miner**

•**Wireshark** •**tcpdump** •**nmap** •**Xplico**

Forensic Van (mh)

Fly Away Kit (mh)

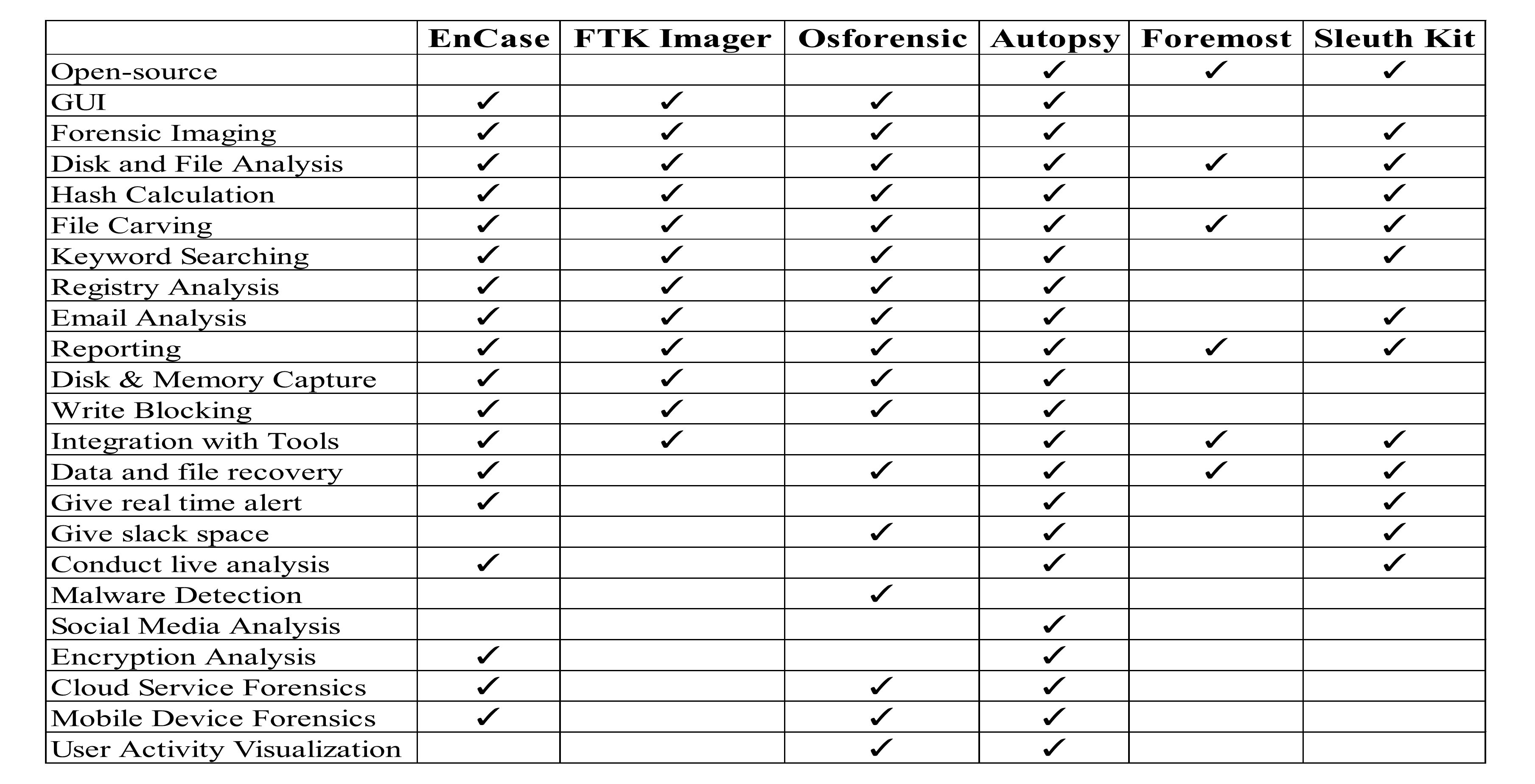
Tableau TX1 Forensic Imager

Tableau Forensic Universal Bridge

Tableau TD2U Forensic Duplicator

**Software Forensic Tools** **Hardware Forensic Tools**

**Comparison** **of** **Device** **Forensic** **Tools**



**Summary** **of** **the** **Comparison**

ØIn terms of feature:

§ EnCase, OSforensic, FTK Imager, Autopsy have user friendly interface.

§ EnCase offers extensive features, integration, and advanced capabilities, but might be complex. § OSforensic ensures solid analysis and mobile/cloud capabilities.

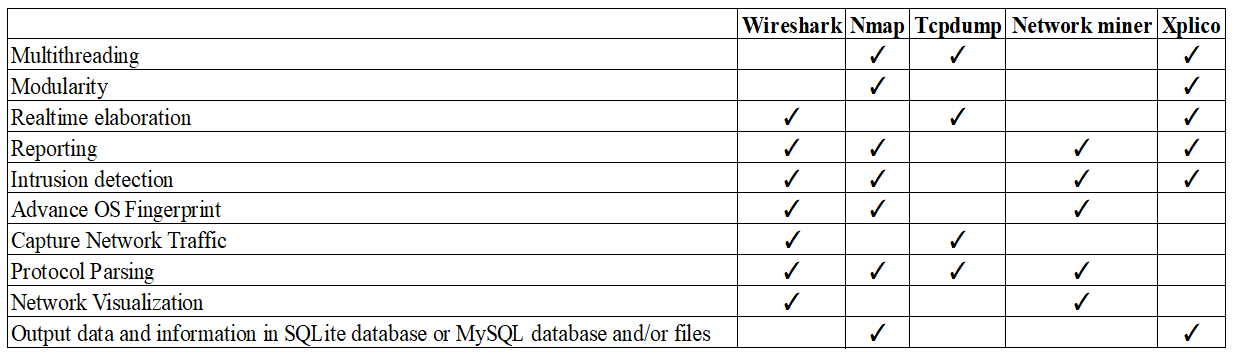
§ FTK Imager is excelling in imaging and analysis, but lacks some advanced functions.

§ Autopsy provides open-source flexibility, covering imaging, keyword search, mobile/cloud analysis.

§ In contrary, Sleuth kit and foremost are tools based on ***command*** ***line*** and it requires technical expertise, offering customization and robust analysis capabilities.

ØIn terms of cost:

§ EnCase and FTK Imager are commercial tools and can be expensive whereas OSforensic offers both paid and free. On the other hand, Autopsy, Sleuth kit and foremost are open source and free tools.

**Comparison** **of** **Network** **Forensic** **Tools**

**Summary** **of** **the** **Comparison**

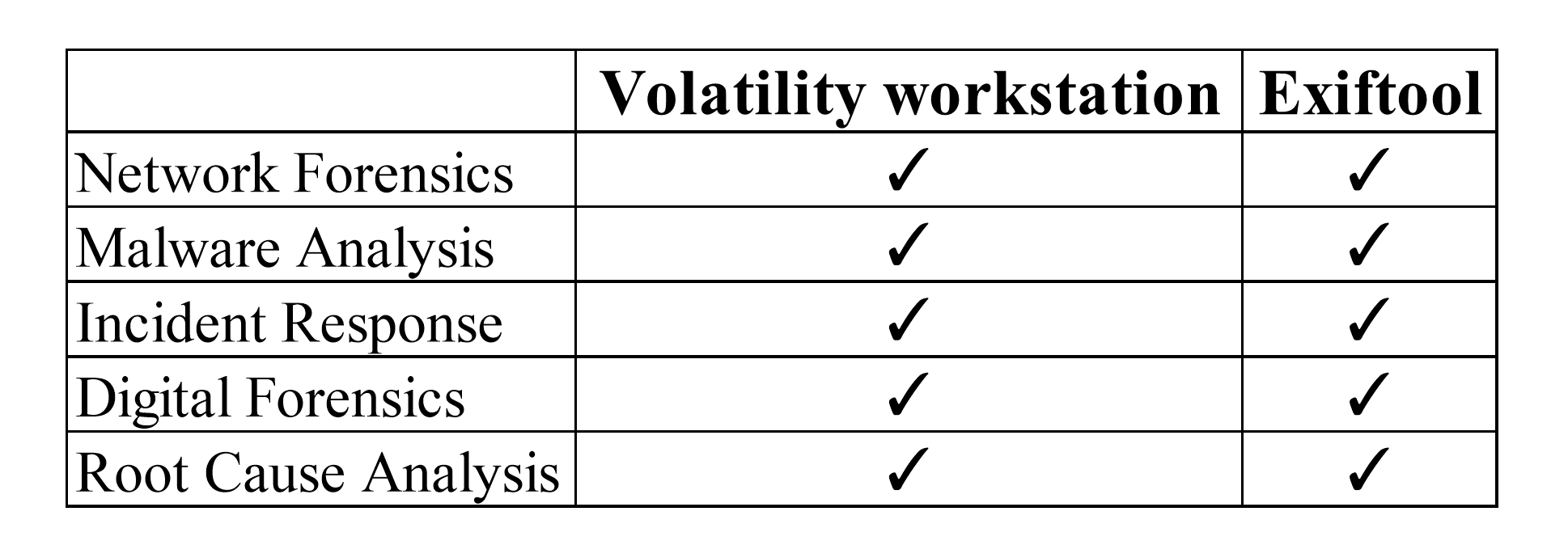
ØIn terms of feature:

§ Wireshark and Tcpdump mainly is used on packet analysis whereas Nmap focuses on network scanning.

§ Xplico is used in extraction from application-level data such as files or emails.

§ On the other hand, NetworkMiner is used on extraction such as image, file from network. ØIn terms of cost:

§ Nmap, Tcpdump, Wireshark and Xplico are open-source tools whereas NetworkMiner offers both free and commercial versions.

**Comparison** **of** **Memory** **Forensic** **Tools**

**Summary** **of** **the** **Comparison**

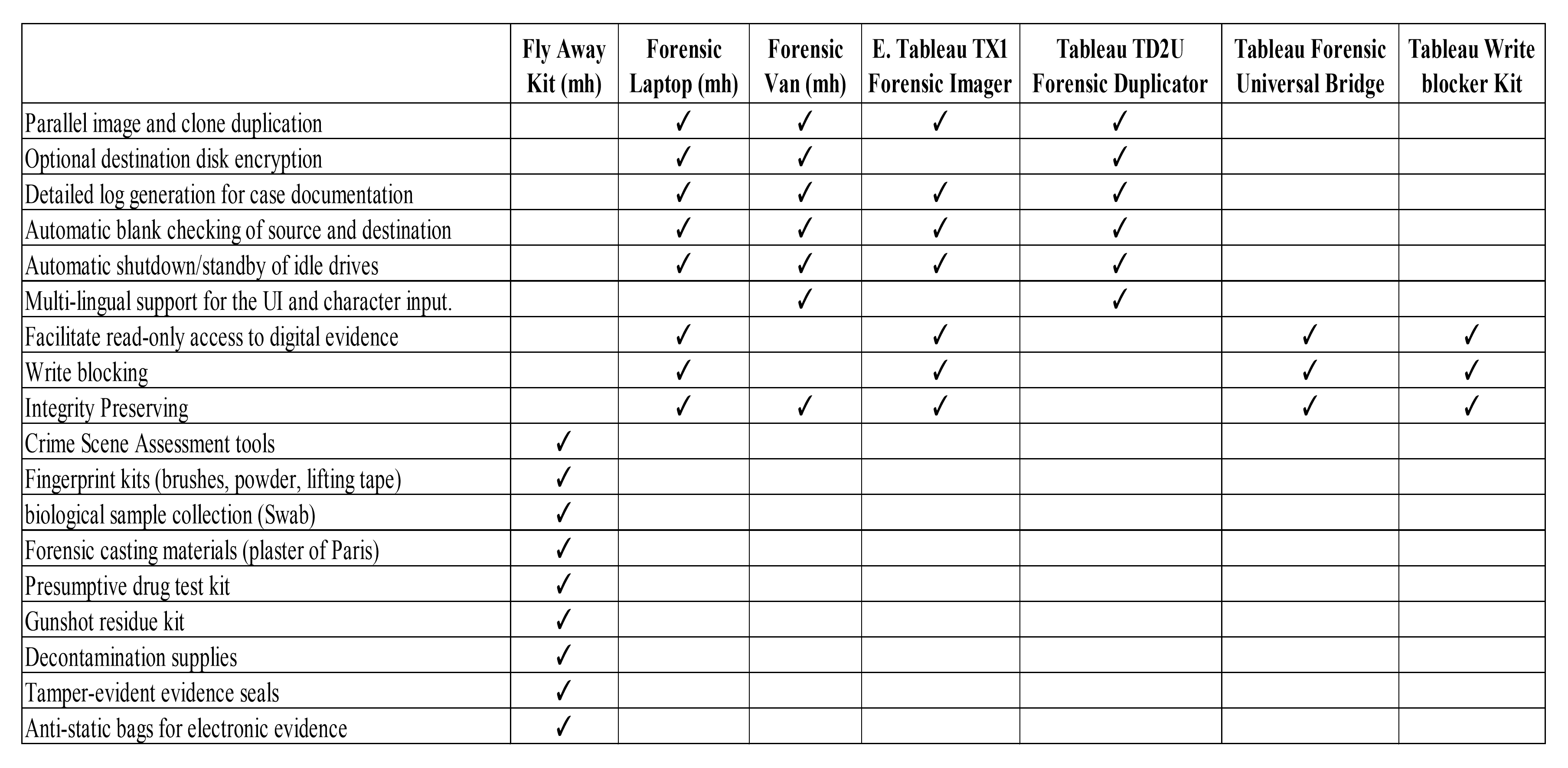
ØIn terms of feature:

§ Volatility Workstation is used in memory analysis such as malware analysis whereas Exiftool is used for image meta data extraction.

ØIn terms of cost:

§ Exiftool is an open-source command line tool and free to use whereas Volatility Workstation is also free tools.

**Comparison** **of** **Hardware** **Forensic** **Tools**



**Summary** **of** **the** **Comparison**

ØThe provided hardware tools include a "***Fly*** ***Away*** ***Kit***" with crime scene assessment tools, fingerprint kits, biological sample collection tools, and more.

ØA "***Forensic*** ***Laptop***" offers features like image duplication, encryption, and detailed logs. Ø A "***Forensic*** ***Van***" provides similar features with multi-lingual support.

ØThe "***Tableau*** ***TX1*** ***Forensic*** ***Imager***" and "***Tableau*** ***TD2U*** ***Forensic*** ***Duplicator***" offer image duplication and documentation features.

ØThe "***Tableau*** ***Forensic*** ***Universal*** ***Bridge***" and "***Tableau*** ***Write*** ***blocker*** ***Kit***" facilitate read-only access and write blocking.

ØEach tool set has specific costs associated with them.

**Summary** **of** **Analysis**

ØChoosing the best tool will vary based on case and required tasks. ØOpen-source tools gives you flexibility and community support. ØCommercial tools can give you extensive support and advanced features. ØSome case require combining tools.

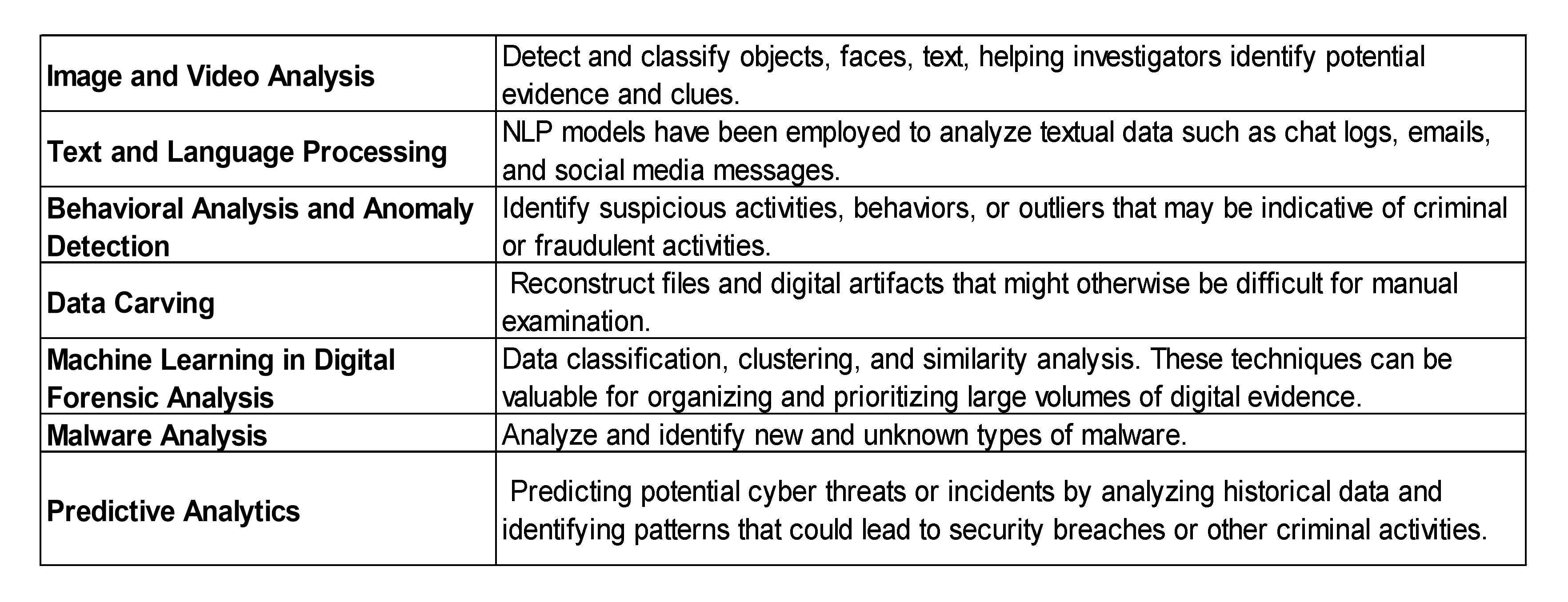
**Challenges** **And** **Limitations**

ØNo access to commercial tools.

ØInability to run tools on real case scenarios. ØFinding the best way to compare tools.

**Future** **of** **Digital** **Forensics**

ØAI and ML has the potential to revolutionize digital investigations

Øcentralized repository that collects data from various forensic tool outputs by anonymizing data ØThis new platform can detect detailed patterns and connections that human analysts might mis