UNIVERSITÉ Concordia UNIVERSITY

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.

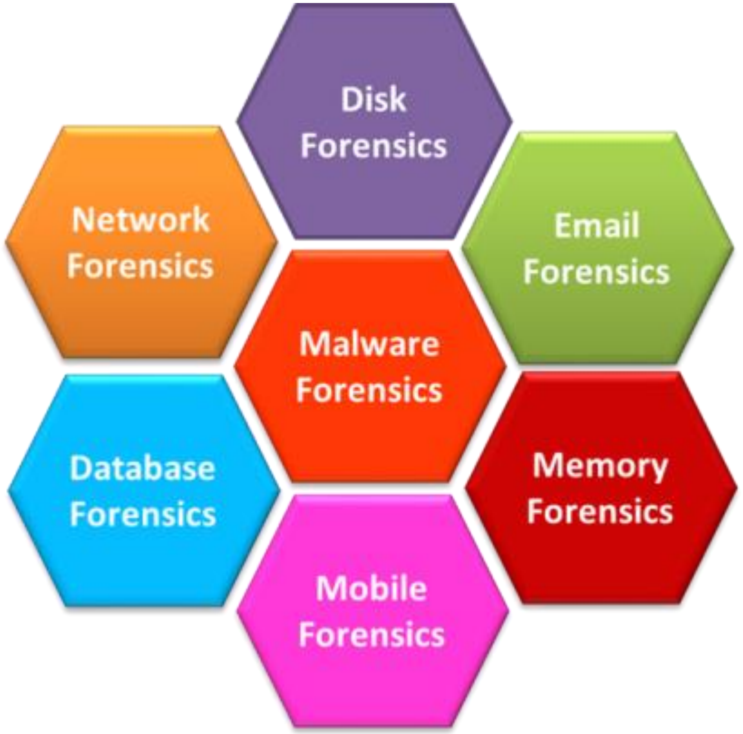
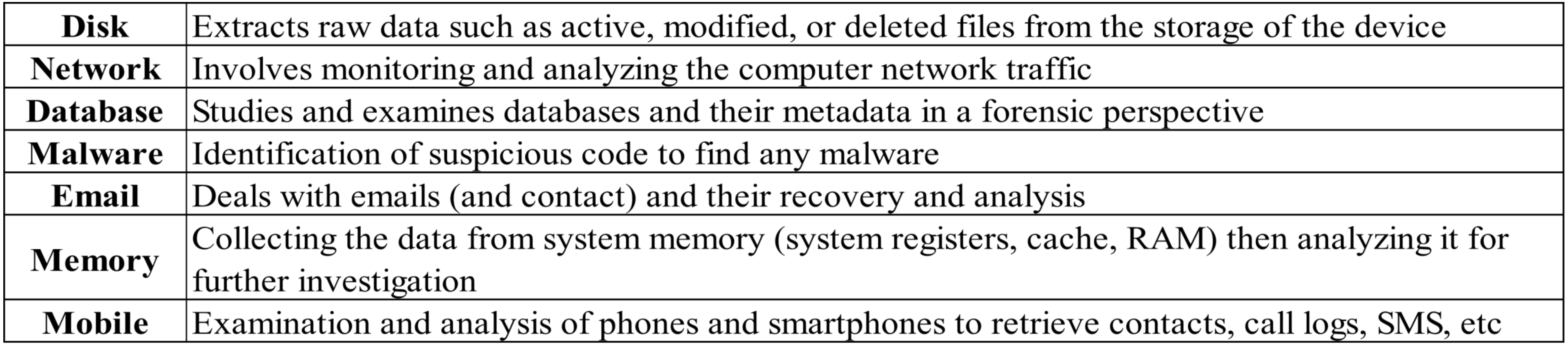


Fig: Areas of Digital Forensics

Arenas of Digital Forensic



Disk	Extracts raw data such as active, modified, or deleted files from the storage of the device
Network	Involves monitoring and analyzing the computer network traffic
Database	Studies and examines databases and their metadata in a forensic perspective
Malware	Identification of suspicious code to find any malware
Email	Deals with emails (and contact) and their recovery and analysis
Memory	Collecting the data from system memory (system registers, cache, RAM) then analyzing it for further investigation
Mobile	Examination and analysis of phones and smartphones to retrieve contacts, call logs, SMS, etc

Phases of Digital Forensic

Identification

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

Preservation

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

Analysis

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

Documentation

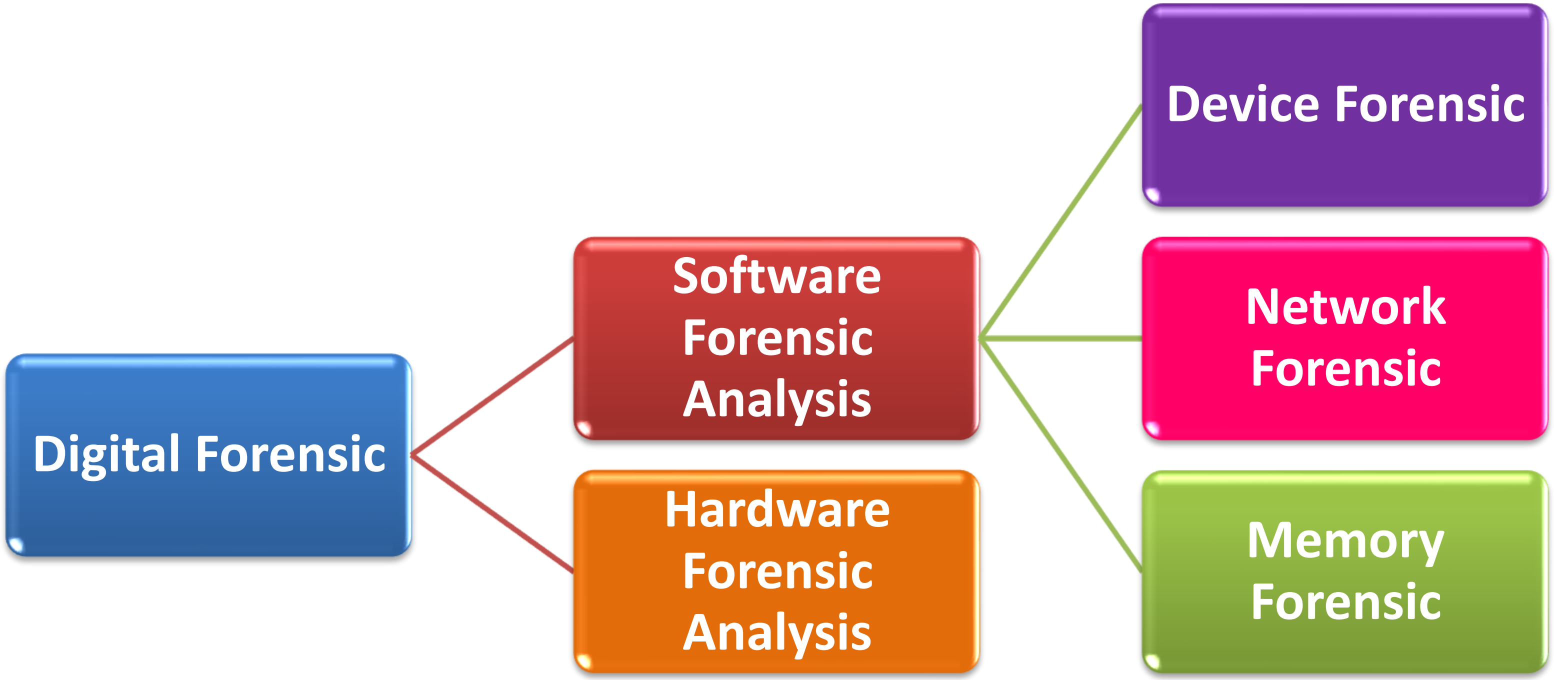
All visible data obtained is gathered and helps to be used as a crime scene reconstruction.

Presentation

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

Methodology

- List down all the available tools used for Digital forensic analysis
- Categorized the tools based on Functional Domains
- Perform Phase wise feature comparison among all the tools



Digital Forensic

Software Forensic Analysis

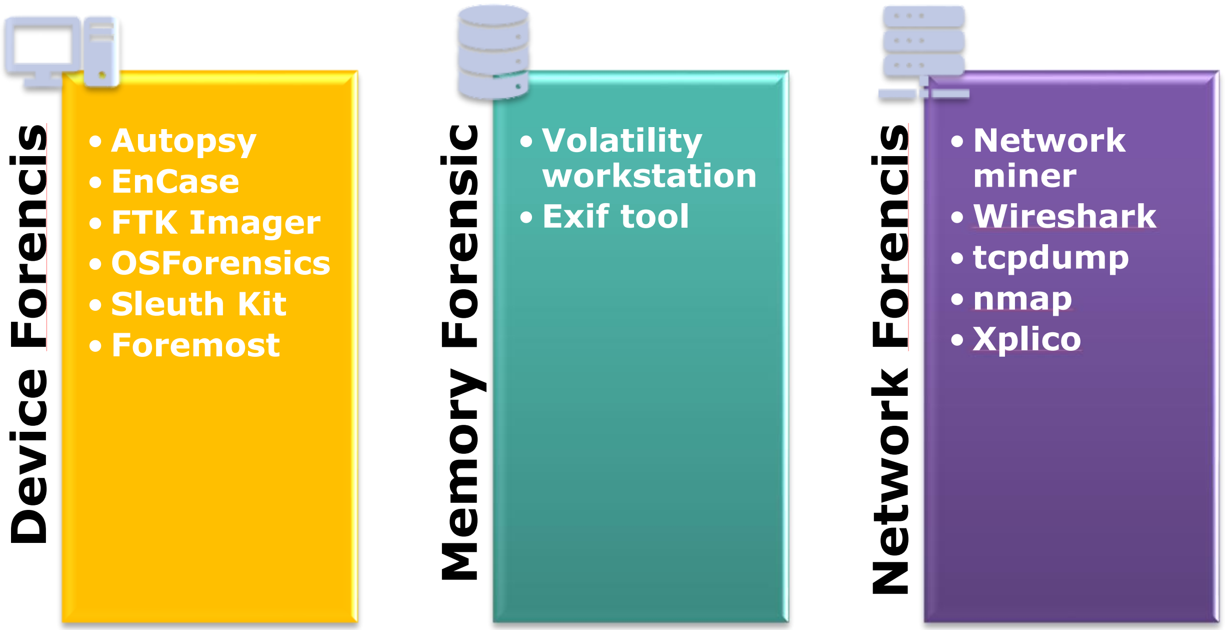
Hardware Forensic Analysis

Device Forensic

Network Forensic

Memory Forensic

Software and Hardware Forensic Tools



Device Forencis

- Autopsy
- EnCase
- FTK Imager
- OSForensics
- Sleuth Kit
- Foremost

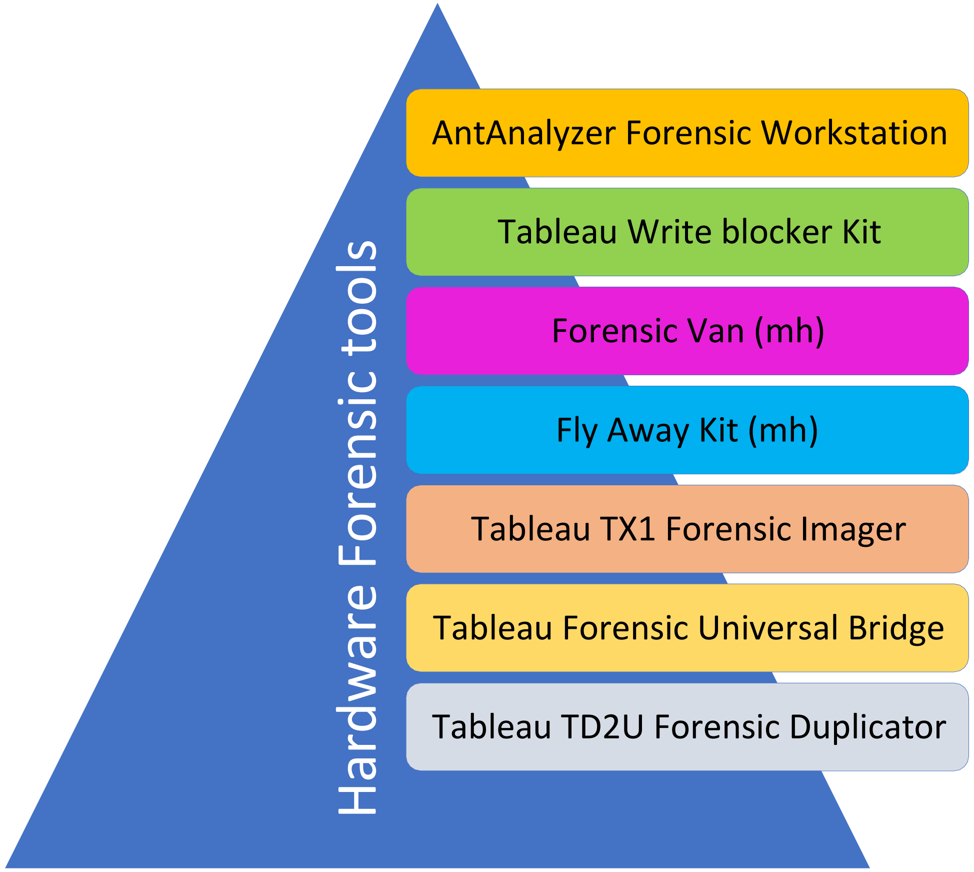
Memory Forensic

- Volatility workstation
- Exif tool

Network Forencis

- Network miner
- Wireshark
- tcpdump
- nmap
- Xplico

Software Forensic Tools

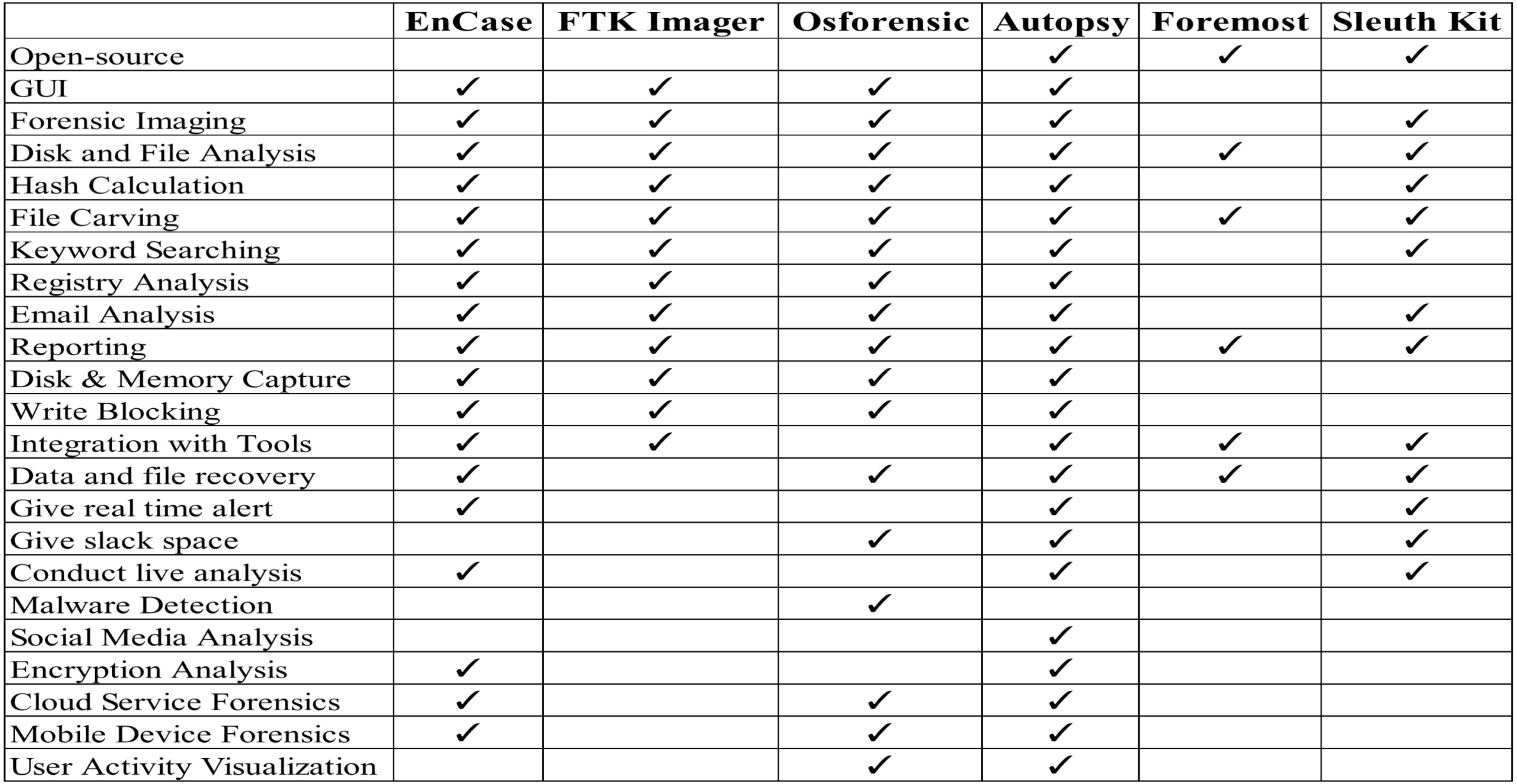


Hardware Forensic tools

- AntAnalyzer Forensic Workstation
- Tableau Write blocker Kit
- Forensic Van (mh)
- Fly Away Kit (mh)
- Tableau TX1 Forensic Imager
- Tableau Forensic Universal Bridge
- Tableau TD2U Forensic Duplicator

Hardware Forensic Tools

Comparison of Device Forensic Tools

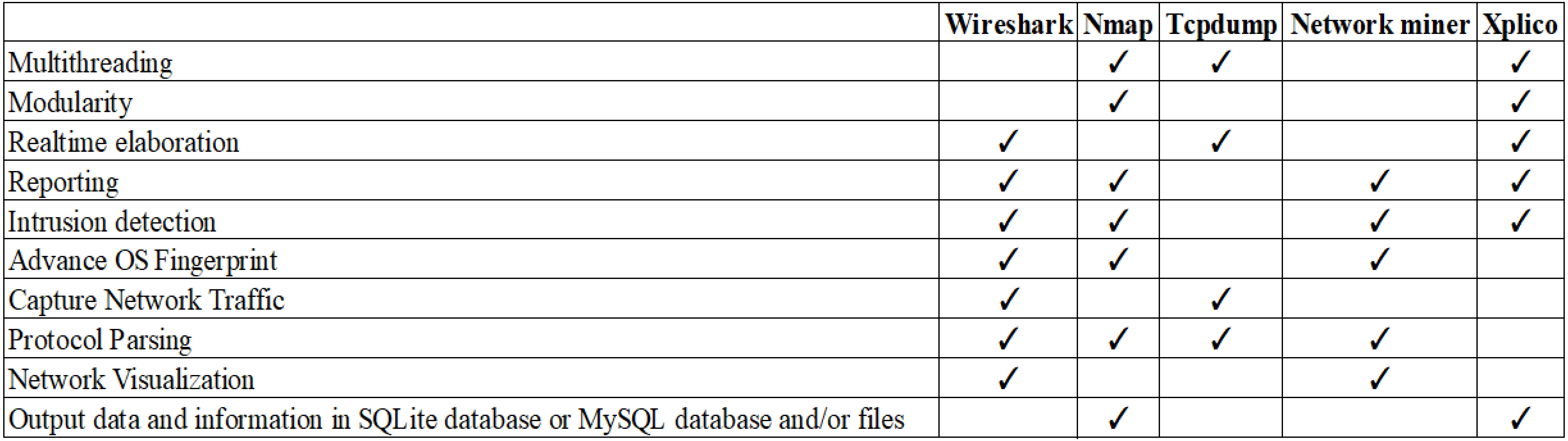


	EnCase	FTK Imager	Osforensic	Autopsy	Foremost	Sleuth Kit
Open-source				✓	✓	✓
GUI	✓	✓	✓	✓		
Forensic Imaging	✓	✓	✓	✓		✓
Disk and File Analysis	✓	✓	✓	✓	✓	✓
Hash Calculation	✓	✓	✓	✓		✓
File Carving	✓	✓	✓	✓	✓	✓
Keyword Searching	✓	✓	✓	✓		✓
Registry Analysis	✓	✓	✓	✓		
Email Analysis	✓	✓	✓	✓		✓
Reporting	✓	✓	✓	✓	✓	✓
Disk & Memory Capture	✓	✓	✓	✓		
Write Blocking	✓	✓	✓	✓		
Integration with Tools	✓	✓		✓	✓	✓
Data and file recovery	✓		✓	✓	✓	✓
Give real time alert	✓			✓		✓
Give slack space			✓	✓		✓
Conduct live analysis	✓			✓		✓
Malware Detection			✓			
Social Media Analysis				✓		
Encryption Analysis	✓			✓		
Cloud Service Forensics	✓		✓	✓		
Mobile Device Forensics	✓		✓	✓		
User Activity Visualization			✓	✓		

Summary of the Comparison

- In 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.
- In 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

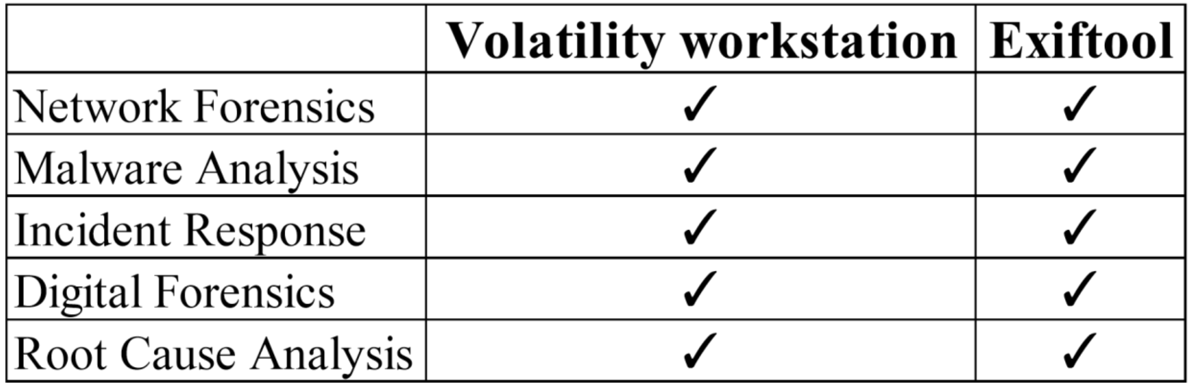


	Wireshark	Nmap	Tcpdump	Network miner	Xplico
Multithreading		✓	✓		✓
Modularity		✓			✓
Realtime elaboration	✓		✓		✓
Reporting	✓	✓		✓	✓
Intrusion detection	✓	✓		✓	✓
Advance OS Fingerprint	✓	✓		✓	
Capture Network Traffic	✓		✓		
Protocol Parsing	✓	✓	✓	✓	
Network Visualization	✓			✓	
Output data and information in SQLite database or MySQL database and/or files		✓			✓

Summary of the Comparison

- In 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.
- In 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



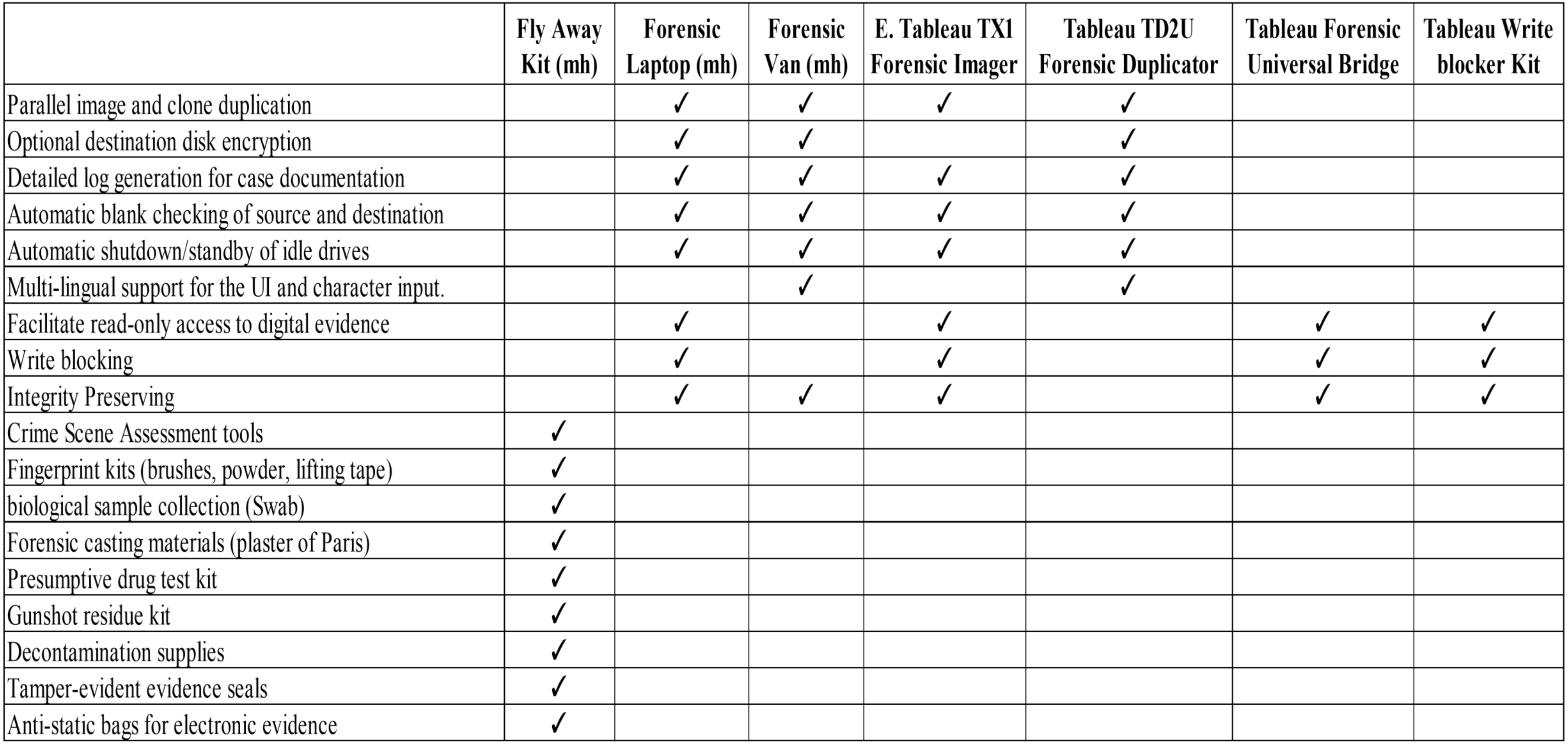
	Volatility workstation	**Exiftool**
Network Forensics	✓	✓
Malware Analysis	✓	✓
Incident Response	✓	✓
Digital Forensics	✓	✓
Root Cause Analysis	✓	✓

Summary of the Comparison

- In terms of feature:
  - Volatility Workstation is used in memory analysis such as malware analysis whereas Exiftool is used for image meta data extraction.

- In 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



	Fly Away Kit (mh)	Forensic Laptop (mh)	Forensic Van (mh)	E. Tableau TX1 Forensic Imager	Tableau TD2U Forensic Duplicator	Tableau Forensic Universal Bridge	Tableau Write blocker Kit
Parallel image and clone duplication		✓	✓	✓	✓		
Optional destination disk encryption		✓	✓		✓		
Detailed log generation for case documentation		✓	✓	✓	✓		
Automatic blank checking of source and destination		✓	✓	✓	✓		
Automatic shutdown/standby of idle drives		✓	✓	✓	✓		
Multi-lingual support for the UI and character input.			✓		✓		
Facilitate read-only access to digital evidence		✓		✓		✓	✓
Write blocking		✓		✓		✓	✓
Integrity Preserving		✓	✓	✓		✓	✓
Crime Scene Assessment tools	✓						
Fingerprint kits (brushes, powder, lifting tape)	✓						
biological sample collection (Swab)	✓						
Forensic casting materials (plaster of Paris)	✓						
Presumptive drug test kit	✓						
Gunshot residue kit	✓						
Decontamination supplies	✓						
Tamper-evident evidence seals	✓						
Anti-static bags for electronic evidence	✓						

Summary of the Comparison

- The provided hardware tools include a "***Fly Away Kit***" with crime scene assessment tools, fingerprint kits, biological sample collection tools, and more.
- A "***Forensic Laptop***" offers features like image duplication, encryption, and detailed logs.
- A "***Forensic Van***" provides similar features with multi-lingual support.
- The "***Tableau TX1 Forensic Imager***" and "***Tableau TD2U Forensic Duplicator***" offer image duplication and documentation features.
- The "***Tableau Forensic Universal Bridge***" and "***Tableau Write blocker Kit***" facilitate read-only access and write blocking.
- Each tool set has specific costs associated with them.

Summary of Analysis

- Choosing the best tool will vary based on case and required tasks.
- Open-source tools gives you flexibility and community support.
- Commercial tools can give you extensive support and advanced features.
- Some case require combining tools.

Challenges And Limitations

- No access to commercial tools.
- Inability to run tools on real case scenarios.
- Finding the best way to compare tools.

Future of Digital Forensics

- AI and ML has the potential to revolutionize digital investigations
- centralized repository that collects data from various forensic tool outputs by anonymizing data
- This new platform can detect detailed patterns and connections that human analysts might mis

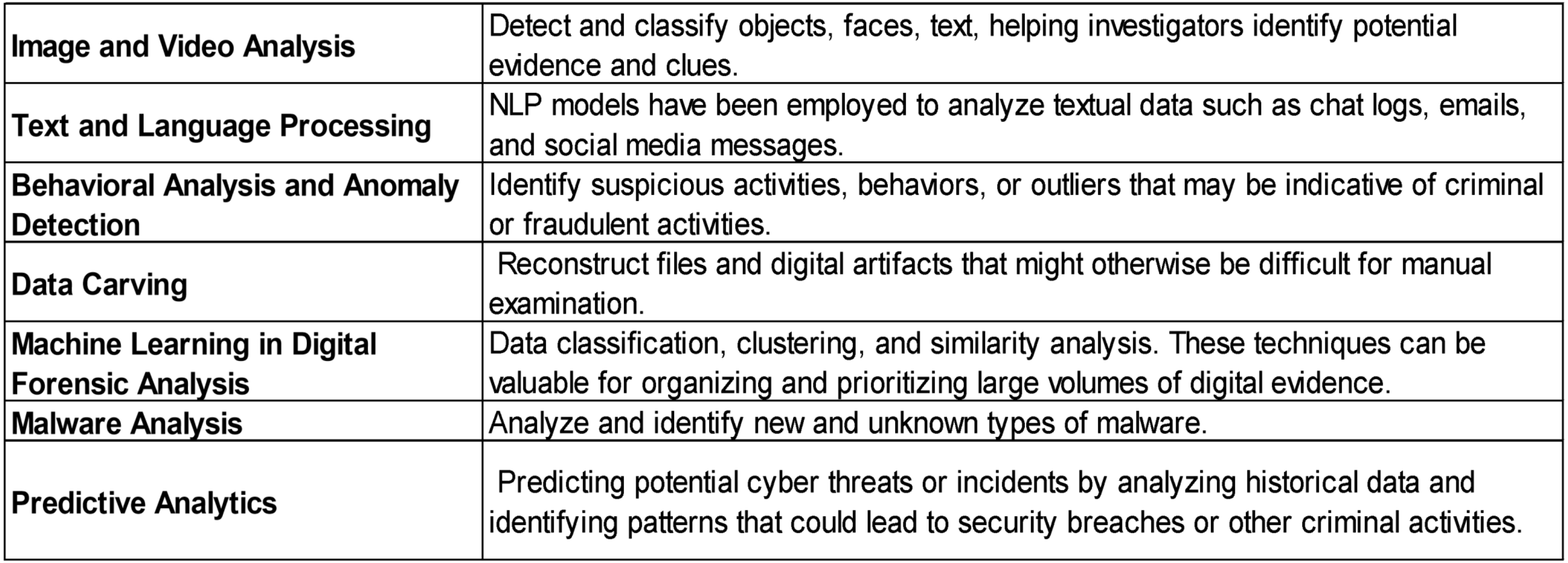


Image and Video Analysis	Detect and classify objects, faces, text, helping investigators identify potential evidence and clues.
Text and Language Processing	NLP models have been employed to analyze textual data such as chat logs, emails, and social media messages.
Behavioral Analysis and Anomaly Detection	Identify suspicious activities, behaviors, or outliers that may be indicative of criminal or fraudulent activities.
Data Carving	Reconstruct files and digital artifacts that might otherwise be difficult for manual examination.
Machine Learning in Digital Forensic Analysis	Data classification, clustering, and similarity analysis. These techniques can be valuable for organizing and prioritizing large volumes of digital evidence.
Malware Analysis	Analyze and identify new and unknown types of malware.
Predictive Analytics	Predicting potential cyber threats or incidents by analyzing historical data and identifying patterns that could lead to security breaches or other criminal activities.