Bindu:

1. **Open Source Tools:**

**The Sleuth Kit (+Autopsy)**: It provides volume system forensic analysis and extensive file system data analysis with a graphical interface for activity identification.

**Caine**: This offers a user-friendly GUI and is designed for interoperability with existing security tools, useful for Windows, UNIX, and Linux systems.

**Volatility**: Specialized in memory analysis and forensics, preserving evidence in memory to prevent loss during system shutdowns, compatible with various operating systems.

**Wireshark**: It is a network protocol analyzer for forensic investigation, examining hundreds of protocols and supporting multiple platforms.

**SIFT Workstation**: SANS Investigative Forensics Toolkit, it offers a detailed digital investigation without altering evidence and is compatible with various forensic file formats.

**Paid Tools:**

**ProDiscover Forensic:** It is used to locate data on computer disks, supports Linux, Mac, and Windows file systems, and provides thorough evidence reports.

**IBM Security QRadar**: This tool is used for centralized access to actionable insights for security data and helps in evaluating security posture against serious risks.

**ExtraHop**: This is a cloud-scale AI for processing data and provides visibility for threat hunting with behavior-based analytics.

**Registry Recon**: It is used in rebuilding Windows registries from forensic images and supports multiple Windows operating systems.

**EnCase:** It is used for helping professionals recover evidence from hard drives and mobile phones, and provides complete reports while maintaining evidence integrity.

These open-source tools provide extensive capabilities in network protocol analysis, memory forensics, and file system analysis, making them powerful options for various digital forensic needs without incurring costs (wise, 2023). On the other hand, the paid tools offer more specialized features such as registry reconstruction and secure evidence management, used as advanced to specific forensic requirements.

When choosing between these tools, consider the specific forensic requirements, the scale of the investigation, and the available budget. Open-source tools can be powerful and cost-effective, but paid tools often offer additional features, support, and ease of use that can be crucial for complex investigations.

Wise. J. (2023). 11 best digital forensics tools & computer software in 2023. https://earthweb.com/digital-forensics-tools/

2. Different certification for each type:

FDK:

* Certified Computer Examiner (CCE)
* Access Data Certified Examiner (ACE)

Kali Linux:

* Offensive Security Certified Professional (OSCP)
* Offensive Security Certified Expert (OSCE)

SIFT:

* GIAC Certified Forensic Analyst (GCFA)
* GIAC Certified Forensic Examiner (GCFE)

CHFI:

* Certified Cyber Forensics Professional (CCFP)
* Certified Forensic Security Responder (CFSR)

For entry-level placement(NICSS, 2023), beginners might start with foundational Kali Linux certifications, as they offer a range of educational pathways from beginner to advanced levels. Advanced practitioners would benefit more from certifications like the OSCP, GCFA, or a specialized certification from FDK or CHFI, as these require substantial prior knowledge and expertise. From the above ACE is the beginner level certificate where as OSCE is the advanced level in all of them.

NICSS. (2023). Cybersecurity certifictions. <https://niccs.cisa.gov/education-training/cybersecurity-certifications>

Firend:

1. Open Source Tools:

CAINE – It’s a linux based forensic environment with GUI that supports investigators throughout the digital investigation phases.

PALADIN – It’s also a Linux application and has over 100 tools to assist in a variety of forensic tasks and is available on a USB thumb drive for convenience.

SIFT Workstation – It’s a collection of forensic tools that provides a digital forensic and incident response examination facility and updates the DFIR package automatically.

Wireshark – It is a network packet analyzer that provides VoIP analysis and helps in network testing and troubleshooting.

Paid Tools:

Google Takeout Convertor – It is used to archive emails from Google Takeout, offering features like batch mode and support for converting files to popular cloud-based email services.

EnCase – It is used to recover evidence from hard drives, unlock encrypted evidence, and offers comprehensive reporting to maintain evidence integrity.

FTK Imager – It is used to create copies of data for evidence without altering the original, supports advanced and automated data analysis, and offers password recovery from various applications.

Magnet RAM Capture - Captures computer memory for analysis and supports a wide range of Windows operating systems.

X-Ways Forensics - Supports disk cloning and imaging, analyzes remote computers, and provides write protection to maintain data authenticity.

These open-source tools offer a range of functionalities from comprehensive forensic environments to specialized network analysis. They can be powerful for various investigative needs and are budget-friendly. The paid tools, however, provide additional features such as encrypted evidence recovery, memory capture, and detailed evidence reporting, which may be essential for more complex forensic investigations.

Choosing between these options should be based on the specific needs of the investigation, the technical proficiency of the users. For example, we can use EnCase, Magnet Ram Capture and X-ways Forensics if we are mainly dealing with hard disks and there restoration.

Bhagat, S.P., Meshram, B.B. (2021). Digital forensic tools for cloud computing environment. <https://doi.org/10.1007/978-981-16-4177-0_7>

2.

**FDK (Forensic Toolkit by AccessData):**

* It offers a robust environment for performing a variety of forensic tasks, including file recovery and encryption cracking.
* It’s used among professionals in corporate agencies.
* The ACE certification tests a user's proficiency in using the Forensic Toolkit software.

**Kali Linux (Offensive Security):**

* Kali Linux is a specialized distribution that includes tools for network analysis and vulnerability assessment.
* It is maintained by Offensive Security.
* The OSCP certification is known for its intense, 24-hour practical exam

**SIFT (SANS Forensic Toolkit)**:

* SIFT is a compilation of forensic tools useful for conducting in-depth analysis and responding to incidents.
* It supports a variety of file systems and can be used across different operating systems, making it versatile.
* The GCFA certification demonstrates expertise in advanced forensic analysis, including timeline analysis and file system examination.

**CHFI (Computer Hacking Forensic Investigator):**

* CHFI certifies individuals in the specific security discipline of computer forensics from a vendor-neutral perspective.
* It ensures that certificate holders are proficient in understanding and conducting a proper investigation in a cybercrime scene.

Both the ACE and CHFI certifications can be pursued by individuals with foundational knowledge looking to enter the field of digital forensics or cybersecurity. For ACE, the basic knowledge of AccessData's Forensic Toolkit (FTK) software is necessary and it’s recommended that the candidates to have some background in IT or security, but there are no strict prerequisites

Offsec. (2023). Course specific resources for offsec students. <https://help.offsec.com/hc/en-us/categories/6965809783316-Course-Specific-Resources-for-Offsec-Students>