1. I found the following list of tools for data acquisition and forensic analysis. Below is the list of those tools further divided into open-source and Paid version of it (Salvationdata, 2022).

**Open Source Tools:**

* **Wireshark** – It is a network forensic tool that intercepts and decrypts data in real-time, with strong VoIP analysis.
* **NMAP** – It is a network scanning and auditing tools that supports almost every popular operating system.
* **Oxygen Forensic Suite** – It is a mobile forensic tool that allows data extraction from mobile phones, including bypassing password or lock screen gestures.
* **The Sleuth Kit** - A suite of command-line tools for data extraction from various storage media.
* **SIFT** – It is based on Ubuntu and offers incident response functionality and incorporates the latest digital forensics approaches.

**Paid Tools/Versions:**

* **Exterro** – It has a range of products including e-discovery, privacy, risk management, and digital forensics, known for its FTK (Forensic Toolkit).
* **X-Ways** – It’s computer forensic examiner's environment that is not resource-intensive and offers additional tools for data capture and analysis.
* **Cellebrite** – It specializes in mobile device forensics with features like AI-assisted picture and video categorization.
* **ProDiscover** – It helps to capture evidence from computer systems for forensic investigation with capabilities for cloud and social media investigations.
* **Wireshark (commercial training)** – It’s the same as the open-source version, but with available commercial training for deeper network analysis.

The open-source tools Wireshark and NMAP are excellent for network analysis and scanning, respectively, while the Oxygen Forensic Suite and SIFT are more specialized for mobile and incident response forensics. On the other hand, paid tools like Exterro provide an integrated platform with a focus on compliance and risk management, and Cellebrite is highly specialized for mobile forensics like Oxygen Forensic Suite. Wireshark, as a paid version, offers the same functionalities but with the added benefit of structured training for users.

Comparing the tools and selecting the tools will largely depend on the specific needs and budget of the user. Open-source tools are generally more accessible and can be highly effective, particularly for those with the technical expertise to use them to their fullest. Paid tools, on other hand provide additional support, integrated workflows, and advanced features that may be necessary for complex or large-scale investigations.

Reference:  
Salvationdata. (2022). The top 20 open source digital forensic tools for 2023. Salvationdata.com. <https://www.salvationdata.com/work-tips/the-top-20-open-source-digital-forensic-tools-for-2023/>

1. Difference between FDK, CHFI, Kali linux and Sift(Sans, 2023):

* **FDK (Access Data Solution):** It refers to Forensic Toolkit by Access Data, which is a suite of software for digital forensics and incident response. It includes capabilities for data recovery, decryption, and analysis of digital devices. Access Data also offers certifications that validate skills in using their suite, like the Access Data Certified Examiner (ACE) certification.
* **Kali Linux (Offensive Security):** It is a Linux distribution designed for penetration testing and security auditing. It comes with a large number of tools geared towards various information security tasks, such as penetration testing, security research, computer forensics, and reverse engineering. Offensive Security, the team behind Kali Linux, provides several certifications, including the Offensive Security Certified Professional (OSCP).
* **SIFT (SANS Forensic Toolkit):** It is a suite of forensic tools designed to assist in digital forensic investigations and incident response, developed by the SANS Institute. It includes a variety of open-source and freely available tools that work on multiple platforms. SANS provides various forensic certifications, such as the GIAC Certified Forensic Analyst (GCFA).
* **CHFI (Computer Hacking Forensic Investigator):** It is a certification offered by EC-Council that validates an individual's ability to detect hacking attacks and properly extract evidence to report the crime and conduct audits to prevent future attacks. It is designed for law enforcement personnel, system administrators, security officers, defense and military personnel, legal professionals, bankers, security professionals, and anyone who is concerned about the integrity of the network infrastructure. The CHFI certification is structured around a detailed methodological approach to computer forensic and evidence analysis.

I think FDK's ACE certification is more suitable for entry-level positions due to their foundational nature and wide acceptance in the industry. Next followed by CHFI. They provide the basis for a career in digital forensics and cybersecurity. On the other hand, OSCP is an advanced certification that requires substantial practical experience and is aimed at professionals seeking to prove their technical penetration testing skills.

Sans. (2023). Digital Forensics Certifications. Sans.org. <https://www.sans.org/cyber-security-certifications/digital-forensics-certifications/>