**Software Tools**

1. Digital Forensics Tools:
   * EnCase
   * AccessData FTK (Forensic Toolkit)
   * Autopsy
   * The Sleuth Kit
   * X-Ways Forensics
   * Cellebrite UFED
   * Oxygen Forensic Detective
   * Magnet AXIOM
   * Volatility
   * Scalpel
   * Forensic Explorer
   * ProDiscover
   * Forensic ToolKit (FTK) Imager
   * Paladin Forensic Suite
   * OSForensics
   * FTK® Toolkit
   * Internet Evidence Finder (IEF)
   * Registry Recon
   * Registry Viewer
   * Bulk Extractor
2. Network Analysis Tools:
   * Wireshark
   * tcpdump
   * NetworkMiner
   * Nmap
   * Snort
   * Bro (Zeek)
   * Suricata
   * Network Forensics Tool (NST)
   * Security Onion
   * Zeekurity
   * NetWitness Investigator
   * Capsa
   * Argus
   * Wi-Fi Pineapple
   * NetworkTrafficView
3. Malware Analysis Tools:
   * IDA Pro
   * Ghidra
   * OllyDbg
   * Radare2
   * PEiD
   * Maltego
   * Cuckoo Sandbox
   * REMnux
   * VirusTotal
   * YARA
   * Viper
   * Capstone
   * PEStudio
   * Dependency Walker
   * Procmon
4. Memory Forensics Tools:
   * Volatility
   * Rekall
   * DumpIt
   * Redline
   * LiME
   * Belkasoft RAM Capturer
   * Hindsight
   * DumpIt
   * MFTDump
   * AVML
5. Data Recovery and Carving Tools:
   * PhotoRec
   * TestDisk
   * Scalpel
   * Foremost
   * R-Studio
   * GetDataBack
   * FTK® Imager
   * DMDE
   * WinHex
   * Recuva
6. Mobile Forensics Tools:
   * Cellebrite UFED Physical Analyzer
   * Oxygen Forensic Detective
   * XRY
   * MOBILedit Forensic Express
   * Andriller
   * Lantern
   * BlackLight
   * Axiom Examinations
   * MOBILedit
   * Paraben E3
7. File Analysis Tools:
   * TrID
   * FileAlyzer
   * PEStudio
   * OfficeMalScanner
   * ExifTool
   * 010 Editor
   * Strings
   * BinText
   * HxD
   * Hex Editor Neo
8. Encryption and Password Cracking Tools:
   * John the Ripper
   * Hashcat
   * oclHashcat
   * Aircrack-ng
   * Netcat
   * GPG (GNU Privacy Guard)
   * OpenSSL
   * TrueCrypt/VeraCrypt
   * HashCalc
   * KeePass
9. Incident Response Tools:
   * TheHive
   * Cortex
   * MISP (Malware Information Sharing Platform & Threat Sharing)
   * ELK Stack (Elasticsearch, Logstash, Kibana)
   * Splunk
   * Sysinternals Suite
   * OSQuery
   * GRR Rapid Response
   * OSSEC
   * Snort
10. Steganography Tools:
    * Stegsolve
    * OpenStego
    * Steghide
    * OutGuess
    * SilentEye
    * StegoTorus
    * F5
    * StegoSuite

**Hardware Tools**

1. Write Blockers:
   * Forensic write blockers: Hardware devices that prevent write access to the original storage media during data acquisition to ensure evidence preservation and maintain the integrity of the data.
2. Forensic Imagers:
   * Hardware devices used to create forensic copies (bit-by-bit) of digital media to be analyzed using digital forensics software, without altering the original evidence.
3. JTAG/Chip-off Tools:
   * In cases where mobile devices or embedded systems are involved, specialized hardware tools like JTAG (Joint Test Action Group) or Chip-off tools may be used to directly access the device's memory for data extraction.
4. Digital Forensics Workstations:
   * High-performance computer systems specifically designed for digital forensics tasks, capable of handling large amounts of data and complex analysis.
5. Network Forensics Appliances:
   * Specialized hardware devices designed for capturing and analyzing network traffic in real-time or post-event scenarios.
6. Mobile Device Acquisition Hardware:
   * Specialized hardware tools used to perform physical or logical acquisition of data from mobile devices, including smartphones and tablets.
7. Disk Duplicators:
   * Hardware devices used to create exact copies of hard drives and storage media for evidence preservation and distribution to multiple investigators.
8. Faraday Bags:
   * Shielded bags used to block all wireless signals to and from devices placed inside, ensuring that electronic evidence is not remotely accessed or tampered with during transportation.
9. Data Recovery Hardware Tools:
   * Specialized hardware devices used to recover data from physically damaged storage media, such as hard drives or memory cards.
10. Mobile Device Unlocking Tools:
    * Hardware-based tools used by law enforcement and forensic experts to bypass passcodes or unlock encrypted mobile devices for data extraction.
11. GPU-based Password Cracking Systems:
    * High-performance hardware systems utilizing graphics processing units (GPUs) for fast password cracking and decryption tasks.
12. Hardware Keyloggers:
    * Physical devices used to capture keystrokes from a computer, enabling the investigation of user activities and passwords.