Digital Forensics Tools

Malware Analysis
- rkhunter
- Qu1cksc0pe
- VirusTotal
- Hybrid Analysis
- IDA Pro
- Process Monitor
- Yara
- Cuckoo Sandbox

Email Forensics
- eMailTrackerPro
- Aid4Mail
- Xtraxtor
- MailXaminer
- MailPro+
- Autopsy

Registry Forensics
- RegRipper
- AmcacheParser
- ShellBags Explorer
- RecentFileCacheParser
- Eric Zimmerman's tools
- regshot

IOC Forensics
- AutoFocus
- Cuckoo Sandbox
- Enforcement Toolkit
- Maltego
- ThreatConnec

Browser/Internet Forensics
- Nirsoft – Web Browser Tools
- BrowsingHistoryView
- Sysinternals Strings
- Magnet Axiom
- OS Forensics
- ChromeCacheView
- MZCacheView
- WebCacheImageInfo
- MyLastSearch

Cloud Forensics Tools
- Amazon Web Services (AWS) CLI
- Azure CLI
- Microsoft Office 365 eDiscovery Export Tool
- Google Cloud SDK
- CloudBacko Pro
- CloudBerry Backup
- Docker Explorer
- Magnet AXIOM Cloud
- UFED Cloud Analyzer
- MSAB XRY Cloud
- Belkasoft Cloud Extractor

Data Recovery Tools
- Recuva
- GetDataBack
- EaseUS Data Recovery Wizard
- PhotoRec
- TestDisk
- Stellar Data Recovery

Steganography Tools
- Stegdetect
- StegoSuite
- OpenStego
- Outguess
- SilentEye

Open Source Tools
- Autopsy
- The Sleuth Kit
- Wireshark
- Volatility
- Ddrescue
- Mobile Verification Toolkit
- CAINE
- Binwalk
- Magicrescue
- Scalpel
- Scrounge-ntfs

Proprietary Tools
- EnCase
- FTK
- XWays Forensics
- Oxygen Forensic Suite
- AccessData Forensic Toolkit
- Magnet Axiom
- ProDiscover
- OS Forensics

Mobile Forensics Tools
- Cellebrite UFED
- Oxygen Forensic Detective
- MOBILedit Forensic Express
- Autopsy
- Andriller
- Magnet ACQUIRE
- Oxygen Forensic Suite
- Mobile Verification Toolkit
- Elcomsoft iOS Forensic Toolkit

Network Forensics Tools
- Security Onion
- Snort
- Bro
- NetworkMiner
- Wireshark
- TCPDump
- Tshark
- Xplico

Memory Forensics Tools
- Volatility
- Volatility Workbench
- Mandiant Redline
- DumpIt
- MAGNET RAM Capture
- Access data FTK imager
- Belkasoft RAM Capturer
- MemDump
- Hibernation Recon
- WindowsSCOPE

Live Forensics Tools
- F-Response
- EnCase Live
- OS Forensics
- Kali Linux Forensics Mode

Disk Imaging Tools
- FTK Imager
- OSFClone
- Encase Imager
- Getdata Forensic imager
- WinHex
- dc3dd
- XWays Imager
- Linux dd
- Guymager

File Analysis Tools
- TrID
- ExifTool
- OfficeMalScanner
- PDF Stream Dumper
- AnalyzePESig
- Pdfid
- Pdf-parser