Digital Forensics Tools

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

www.hackingarticles.in