Digital Forensic Tools

Digital forensic tools are designed to allow investigators to take images of computer and Information technology (IT) environments to recreate or determine how a malicious attacker was able to compromise a system, and the actions they took within the compromised system. This allows investigators to determine vulnerabilities in systems that were exploited.

Digital forensics tools today can also be classified into various categories:

- **Hard Drive and Data capture tools**
- **File analysis tools**
- **Registry and memory analysis tools**
- **Internet analysis tools**
- **Email analysis tools**
- **Mobile devices analysis tools**
- **Network forensics tools**
- **Database forensics tools**

Here are some common forensic tools listed below:

1. **Digital Forensics Framework**
   http://www.digital-forensic.org/
2. **Open Computer Forensics Architecture**
   http://sourceforge.net/projects/ocfa/
3. **CAINE**
   http://www.caine-live.net/
4. **X-Ways Forensics**
   http://www.x-ways.net/forensics/
5. **SANS Investigative Forensics Toolkit – SIFT**
   http://digital-forensics.sans.org/community/downloads
6. **EnCase**
   https://www.guidancesoftware.com/products/Pages/encase-forensic/overview.aspx
7. **Registry Recon**
   http://arsenalrecon.com/apps/recon/
8. **The Sleuth Kit**
   http://www.sleuthkit.org/
9. **WindowsSCOPE**
   http://www.windowsscope.com/index.php?page=shop.product_details&flypage=flypage.tpl&product_id=35&category_id=3&option=com_virtuemart
10. **Mandiant RedLine**
    https://www.mandiant.com/resources/download/redline
11. **Computer Online Forensic Evidence Extractor (COFEE)**
    https://cofee.nw3c.org/