Free Computer Forensic Tools

1. Disk tools and data capture

Arsenal Image Mounter :
Mounts disk images as complete disks in Windows, giving access to Volume Shadow Copies, etc.
https://www.arsenalrecon.com/apps/image-mounter/

DumpIt :
Generates physical memory dump of Windows machines, 32 bits 64 bit. Can run from a USB flash drive.
http://www.moonsols.com/2011/07/18/moonsols-dumpit-goes-mainstream/

EnCase :
Create EnCase evidence files and EnCase logical evidence files
http://www1.guidancesoftware.com/Order-Forensic-Imager.aspx

Encrypted Disk Detector :
Checks local physical drives on a system for TrueCrypt, PGP, or Bitlocker encrypted volumes
http://info.magnetforensics.com/encrypted-disk-detector

EWF MetaEditor :
Edit EWF (E01) meta data, remove passwords (Encase v6 and earlier)
http://www.4discovery.com/our-tools/

FAT32 Format :
Enables large capacity disks to be formatted as FAT32
http://www.ridgecrop.demon.co.uk/index.htm?fat32format.htm

Forensics Acquisition of Websites :
Browser designed to forensically capture web pages
http://www.fawproject.com/en/default.aspx

FTK Imager :
Imaging tool, disk viewer and image mounter
http://www.accessdata.com/support/product-downloads

Guymager :
Multi-threaded GUI imager under running under Linux
http://guymager.sourceforge.net/

Live RAM Capturer :
Extracts RAM dump including that protected by an anti-debugging or anti-dumping system. 32 and 64 bit builds
http://forensic.belkasoft.com/en/ram-capturer

NetworkMiner :
Network analysis tool. Detects OS, hostname and open ports of network hosts through packet sniffing/PCAP parsing
http://sourceforge.net/projects/networkminer/

Nmap :
Utility for network discovery and security auditing
http://nmap.org/

Magnet RAM :
Captures physical memory of a suspect’s computer. Windows XP to Windows 10, and 2003, 2008, 2012. 32 & 64 bit
http://www.magnetforensics.com/ram-capture/

OSFClone :
Boot utility for CD/DVD or USB flash drives to create dd or AFF images/clones.
http://www.osforensics.com/tools/create-disk-images.html

OSFMount :
Mounts a wide range of disk images. Also allows creation of RAM disks
http://www.osforensics.com/tools/mount-disk-images.html

Wireshark :
Network protocol capture and analysis
https://www.wireshark.org/

Disk2vhd :
Creates Virtual Hard Disks versions of physical disks for use in Microsoft Virtual PC or Microsoft Hyper-V VMs
https://technet.microsoft.com/en-gb/sysinternals/ee656415.aspx

---

2. Email analysis

EDB Viewer :
Open and view (not export) Outlook EDB files without an Exchange server
http://www.nucleustechnologies.com/exchange-edb-viewer.html

Mail Viewer :
Viewer for Outlook Express, Windows Mail/Windows Live Mail, Mozilla Thunderbird message databases and single EML files
http://www.mitec.cz/mailview.html

MBOX Viewer :
View MBOX emails and attachments
http://www.systoolsgroup.com/mbox-viewer.html

OST Viewer :
Open and view (not export) Outlook OST files without connecting to an Exchange server
http://www.nucleustechnologies.com/ost-viewer.html

PST Viewer :
Open and view (not export) Outlook PST files without needing Outlook
http://www.nucleustechnologies.com/pst-viewer.html

3. General tools

Agent Ransack :
Search multiple files using Boolean operators and Perl Regex
http://www.mythicsoft.com/page.aspx?type=agentransack&page=home

---

Computer Forensic Reference Data Sets :
Collated forensic images for training, practice and validation
http://www.cfreds.nist.gov/

EvidenceMover :
Copies data between locations, with file comparison, verification, logging
http://www.nuix.com/Nuix-evidence-mover

FastCopy :
Self labelled ‘fastest’ copy/delete Windows software. Can verify with SHA-1, etc.
http://ipmsg.org/tools/fastcopy.html.en

File Signatures :
Table of file signatures
http://www.garykessler.net/library/file_sigs.html

HexBrowser :
Identifies over 1000 file types by examining their signatures
http://www.hexbrowser.com/

HashMyFiles :
Calculate MD5 and SHA1 hashes
http://www.nirsoft.net/utils/hash_my_files.html

MobaLiveCD :
Run Linux live CDs from their ISO image without having to boot to them
http://mobalivecd-en.mobatek.net/

Mouse Jiggler :
Automatically moves mouse pointer stopping screen saver, hibernation etc.
http://mousejiggler.codeplex.com/

Notepad ++ :
Advanced Notepad replacement
http://notepad-plus-plus.org/

NSRL :
Hash sets of ‘known’ (ignorable) files
http://www.nsrl.nist.gov/Downloads.htm

Quick Hash :
A Linux & Windows GUI for individual and recursive SHA1 hashing of files
http://sourceforge.net/projects/quickhash/

USB Write Blocker :
Enables software write-blocking of USB ports
http://dsicovery.com/dsicovery-software/usb-write-blocker/

Volix :
Application that simplifies the use of the Volatility Framework
http://www.it-forensik.fh-aachen.de/projekte/volix/13

Windows Forensic Environment :
Guide by Brett Shavers to creating and working with a Windows boot CD
http://winfe.wordpress.com/

---

4. File and data analysis

Advanced Prefetch Analyser :
Reads Windows XP,Vista and Windows 7 prefetch files
http://www.ash368.com/

---

analyzeMFT :
Parses the MFT from an NTFS file system allowing results to be analysed with other tools
https://github.com/dkovar/analyzeMFT

bstrings :
Find strings in binary data, including regular expression searching.
https://binaryforay.blogspot.co.uk/2015/07/introducing-bstrings-better-strings.html

---

CapAnalysis :
PCAP viewer
http://www.capanalysis.net/site/

Crowd Reponse :
Windows console application to aid gathering of system information for incident response and security engagements.
http://www.crowdstrike.com/community-tools/

Crowd Inspect :
Details network processes, listing binaries associated with each process. Queries VirusTotal, other malware repositories & reputation services to produce “at-a-glance” state of the system
http://www.crowdstrike.com/community-tools/

DCode :
Converts various data types to date/time values
http://www.digital-detective.net/digital-forensic-software/free-tools/

Defraser :
Detects full and partial multimedia files in unallocated space
http://sourceforge.net/projects/defraser/

---

eCryptfs Parser :
Recursively parses headers of every eCryptfs file in selected directory. Outputs encryption algorithm used, original file size, signature used, etc.
http://sourceforge.net/projects/ecryptfs-p/

Encryption Analyzer :
Scans a computer for password-protected & encrypted files, reports encryption complexity and decryption options for each file
http://www.lostpassword.com/encryption-analyzer.htm

ExifTool :
Read, write and edit Exif data in a large number of file types
http://www.sno.phy.queensu.ca/~phil/exiftool/

File Identifier :
Drag and drop web-browser JavaScript tool for identification of over 2000 file types
http://www.toolsley.com/

Forensic Image Viewer :
View various picture formats, image enhancer, extraction of embedded Exif, GPS data
http://www.sandersonforensics.com/forum/list.php?category/46-Free-Software

---

Ghiro :
In-depth analysis of image (picture) files
http://www.getghiro.org/

Highlighter :
Examine log files using text, graphic or histogram views
http://www.mandiant.com/products/free_software/highlighter/

Link Parser :
Recursively parses folders extracting 30+ attributes from Windows .lnk (shortcut) files
http://www.4discovery.com/our-tools/

LiveContactsView :
View and export Windows Live Messenger contact details
http://www.nirsoft.net/utils/live_messenger_contacts.html

PECmd :
Prefetch Explorer
https://binaryforay.blogspot.co.uk/2016/01/pecmd-v0600-released.html

---

PlatformAuditProbe :
Command Line Windows forensic/ incident response tool that collects many artefacts.
Manual
https://appliedalgo.com/

RSA Netwitness Investigator :
Network packet capture and analysis
http://www.emc.com/security/rsa-netwitness.htm#!freeware

Memoryze :
Acquire and/or analyse RAM images, including the page file on live systems
http://www.mandiant.com/products/free_software/memoryze/

MetaExtractor :
Recursively parses folders to extract meta data from MS Office, OpenOffice and PDF files
http://www.4discovery.com/our-tools/

MFTview :
Displays and decodes contents of an extracted MFT file
http://www.sandersonforensics.com/forum/list.php?category/46-Free-Software

---

PictureBox :
Lists EXIF, and where available, GPS data for all photographs present in a directory. Export data to .xls or Google Earth KML format
http://www.mikesforensictools.co.uk/MFTPB.html

PsTools :
Suite of command-line Windows utilities
http://technet.microsoft.com/en-us/sysinternals/bb896649.aspx

---

Shadow Explorer :
Browse and extract files from shadow copies
http://www.shadowexplorer.com/

SQLite Manager :
Firefox add-on enabling viewing of any SQLite
https://addons.mozilla.org/en-US/firefox/addon/sqlite-manager/

Strings :
Command-line tool for text searches
http://technet.microsoft.com/en-gb/sysinternals/bb897439.aspx

Structured Storage Viewer :
View and manage MS OLE Structured Storage based files
http://www.mitec.cz/ssv.html

Switch-a-Roo :
Text replacement/converter/decoder for when dealing with URL encoding, etc
http://www.mikesforensictools.co.uk/MFTSAR.html

Windows File Analyzer :
Analyse thumbs.db, Prefetch, INFO2 and .lnk files
http://www.mitec.cz/wfa.html

Xplico :
Network forensics analysis tool
http://www.xplico.org/

---

5. Mac OS tools

Audit :
Audit Preference Pane and Log Reader for OS X
https://github.com/twocanoes/audit

ChainBreaker :
Parses keychain structure, extracting user's confidential information such as application account/password, encrypted volume password (e.g. filevault), etc
http://forensic.n0fate.com/?page_id=412

Disk Arbitrator :
Blocks the mounting of file systems, complimenting a write blocker in disabling disk arbitration
https://github.com/aburgh/Disk-Arbitrator

Epoch Converter :
Converts epoch times to local time and UTC
https://www.blackbagtech.com/resources/freetools/epochconverter.html

---

FTK Imager CLI for Mac OS :
Command line Mac OS version of AccessData's FTK Imager
http://accessdata.com/product-download/digital-forensics/mac-os-10.5-and-10.6x-version-3.1.1

IORegInfo :
Lists items connected to the computer (e.g., SATA, USB and FireWire Drives, software RAID sets). Can locate partition information, including sizes, types, and the bus to which the device is connected
https://www.blackbagtech.com/resources/freetools/ioreg-info.html

---

PMAP Info :
Displays the physical partitioning of the specified device. Can be used to map out all the drive information, accounting for all used sectors
https://www.blackbagtech.com/resources/freetools/pmap-info.html

---

Volafox :
Memory forensic toolkit for Mac OS X
http://forensic.n0fate.com/?page_id=412

---

6. Mobile devices

---

iPBA2 :
Explore iOS backups
http://ipbackupanalyzer.com/

---

iPhone Analyzer :
Explore the internal file structure of Pad, iPod and iPhones
http://sourceforge.net/projects/iphoneanalyzer/

---

ivMeta :
Extracts phone model and software version and created date and GPS data from iPhone videos.
http://www.csitech.co.uk/ivmeta-iphone-metadata/

Last SIM Details :
Parses physical flash dumps and Nokia PM records to find details of previously inserted SIM cards.
http://lastsimdetails.blogspot.co.uk/p/downloads.html

Rubus :
Deconstructs Blackberry .ipd backup files
http://www.cclgroupltd.com/Buy-Software/rubus-ipd-de-constructor-utility.html

---

SAFT :
Obtain SMS Messages, call logs and contacts from Android devices
http://www.signalsec.com/saft/

---

7. Data analysis suites

Autopsy :
Graphical interface to the command line digital investigation analysis tools in The Sleuth Kit (see below)
http://www.sleuthkit.org/autopsy/

Backtrack :
Penetration testing and security audit with forensic boot capability
http://www.backtrack-linux.org/

Caine :
Linux based live CD, featuring a number of analysis tools
http://www.caine-live.net/

Deft :
Linux based live CD, featuring a number of analysis tools
http://www.deftlinux.net/

Digital Forensics Framework :
Analyses volumes, file systems, user and applications data, extracting metadata, deleted and hidden items
http://www.digital-forensic.org/

Forensic Scanner :
Automates ‘repetitive tasks of data collection’. Fuller description here
https://github.com/appliedsec/forensicscanner

Paladin :
Ubuntu based live boot CD for imaging and analysis
http://www.sumuri.com/

SIFT :
VMware Appliance pre-configured with multiple tools allowing digital forensic examinations
http://computer-forensics.sans.org/community/downloads/

The Sleuth Kit :
Collection of UNIX-based command line file and volume system forensic analysis tools
http://www.sleuthkit.org/sleuthkit/

Volatility Framework :
Collection of tools for the extraction of artefacts from RAM
http://www.volatilityfoundation.org/

---

8. Internet analysis

---

http://www.nirsoft.net/utils/mzcv.html

MozillaHistoryView :
Reads the history.dat of Firefox/Mozilla/Netscape Web browsers, and displays the list of all visited Web page
http://www.nirsoft.net/utils/mozilla_history_view.html

MyLastSearch :
Extracts search queries made with popular search engines (Google, Yahoo and MSN) and social networking sites (Twitter, Facebook, MySpace)
http://www.nirsoft.net/utils/my_last_search.html

PasswordFox :
Extracts the user names and passwords stored by Mozilla Firefox Web browser
http://www.nirsoft.net/utils/passwordfox.html

OperaCacheView :
Reads the cache folder of Opera Web browser, and displays the list of all files currently stored in the cache
http://www.nirsoft.net/utils/opera_cache_view.html

OperaPassView :
Decrypts the content of the Opera Web browser password file, wand.dat
http://www.nirsoft.net/utils/opera_password_recovery.html

Web Historian :
Reviews list of URLs stored in the history files of the most commonly used browsers
http://www.mandiant.com/resources/download/web-historian

Web Page Saver :
Takes list of URLs saving scrolling captures of each page. Produces HTML report file containing the saved pages
http://info.magnetforensics.com/web-page-saver

---

9. Registry analysis

AppCompatCache Parser :
Dumps list of shimcache entries showing which executables were run and their modification dates. Further details.
http://binaryforay.blogspot.co.uk/p/software.html

ForensicUserInfo :
Extracts user information from the SAM, SOFTWARE and SYSTEM hives files and decrypts the LM/NT hashes from the SAM file
http://www.woanware.co.uk/forensics/forensicuserinfo.html

Process Monitor :
Examine Windows processes and registry threads in real time
http://technet.microsoft.com/en-us/sysinternals/bb896645.aspx

RECmd :
Command line access to offline Registry hives. Supports simple & regular expression searches as well as searching by last write timestamp. Further details.
http://binaryforay.blogspot.co.uk/p/software.html

Registry Decoder :
For the acquisition, analysis, and reporting of registry contents
http://www.digitalforensicssolutions.com/registrydecoder/

Registry Explorer :
Offline Registry viewer. Provides deleted artefact recovery, value slack support, and robust searching. Further details.
http://binaryforay.blogspot.co.uk/p/software.html

RegRipper :
Registry data extraction and correlation tool
http://regripper.wordpress.com/

Regshot :
Takes snapshots of the registry allowing comparisons e.g., show registry changes after installing software
http://sourceforge.net/projects/regshot/files/

ShellBags Explorer :
Presents visual representation of what a user's directory structure looked like. Additionally exposes various timestamps (e.g., first explored, last explored for a given folder. Further details.
http://binaryforay.blogspot.co.uk/p/software.html

USB Device Forensics :
Details previously attached USB devices on exported registry hives
http://www.woanware.co.uk/forensics/usbdeviceforensics.html

USB Historian :
Displays 20+ attributes relating to USB device use on Windows systems
http://www.4discovery.com/our-tools/

USBDeview :
Details previously attached USB devices
http://www.nirsoft.net/utils/usb_devices_view.html

User Assist Analysis :
Extracts SID, User Names, Indexes, Application Names, Run Counts, Session, and Last Run Time Attributes from UserAssist keys
http://www.4discovery.com/our-tools/

UserAssist :
Displays list of programs run, with run count and last run date and time
http://blog.didierstevens.com/programs/userassist/

Windows Registry Recovery :
Extracts configuration settings and other information from the Registry
http://www.mitec.cz/wrr.html

---

10. Application analysis

Dropbox Decryptor :
Decrypts the Dropbox filecache.dbx file which stores information about files that have been synced to the cloud using Dropbox
http://info.magnetforensics.com/dropbox-decryptor

Google Maps Tile Investigator :
Takes x,y,z coordinates found in a tile filename and downloads surrounding tiles providing more context
http://info.magnetforensics.com/google-maps-tile-investigator

---

KaZAlyser :
Extracts various data from the KaZaA application
http://www.sandersonforensics.com/forum/list.php?category/46-Free-Software

---

LiveContactsView :
View and export Windows Live Messenger contact details
http://www.nirsoft.net/utils/live_messenger_contacts.html

SkypeLogView :
View Skype calls and chats
http://www.nirsoft.net/utils/skype_log_view.html
