Disk tools and data capture

Name	From	Description
DumpIt	MoonSols	Generates physical memory dump of Windows machines, 32 bits 64 bit. Can run from a USB flash drive.
EnCase Forensic Imager	Guidance Software	Create EnCase evidence files and EnCase logical evidence files [direct download link]
Encrypted Disk Detector	Magnet Forensics	Checks local physical drives on a system for TrueCrypt, PGP, or Bitlocker encrypted volumes
EWF MetaEditor	4Discovery	Edit EWF (E01) meta data, remove passwords (Encase v6 and earlier)
FAT32 Format	Ridgecrop	Enables large capacity disks to be formatted as FAT32
Forensics Acquisition of Websites	Web Content Protection Association	Browser designed to forensically capture web pages
FTK Imager	AccessData	Imaging tool, disk viewer and image mounter
Guymager	vogu00	Multi-threaded GUI imager under running under Linux
Live RAM Capturer	Belkasoft	Extracts RAM dump including that protected by an anti-debugging or anti-dumping system. 32 and 64 bit builds
NetworkMiner	Hjelmvik	Network analysis tool. Detects OS, hostname and open ports of network hosts through packet sniffing/PCAP parsing
Nmap	Nmap	Utility for network discovery and security auditing
Magnet RAM Capture	Magnet Forensics	Captures physical memory of a suspect's computer. Windows XP to Windows 10, and 2003, 2008, 2012. 32 & 64 bit
OSFClone	Passmark Software	Boot utility for CD/DVD or USB flash drives to create dd or AFF images/clones.
OSFMount	Passmark Software	Mounts a wide range of disk images. Also allows creation of RAM disks
Wireshark	Wireshark	Network protocol capture and analysis
Disk2vhd	Microsoft	Creates Virtual Hard Disks versions of physical disks for use in Microsoft Virtual PC or Microsoft Hyper-V VMs

Email analysis

Name	From	Description
EDB Viewer	Lepide Software	Open and view (not export) Outlook EDB files without an Exchange server
Mail Viewer	MiTeC	Viewer for Outlook Express, Windows Mail/Windows Live Mail, Mozilla Thunderbird message databases and single EML files
MBOX Viewer	SysTools	View MBOX emails and attachments
OST Viewer	Lepide Software	Open and view (not export) Outlook OST files without connecting to an Exchange server
PST Viewer	Lepide Software	Open and view (not export) Outlook PST files without needing Outlook

General

Name	From	Description
Agent Ransack	Mythicsoft	Search multiple files using Boolean operators and Perl Regex
Computer Forensic Reference Data Sets	NIST	Collated forensic images for training, practice and validation
EvidenceMover	Nuix	Copies data between locations, with file comparison, verification, logging
FastCopy	Shirouzu Hiroaki	Self labelled ‘fastest’ copy/delete Windows software. Can verify with SHA-1, etc.
File Signatures	Gary Kessler	Table of file signatures
HexBrowser	Peter Fiskerstrand	Identifies over 1000 file types by examining their signatures
HashMyFiles	Nirsoft	Calculate MD5 and SHA1 hashes
MobaLiveCD	Mobatek	Run Linux live CDs from their ISO image without having to boot to them
Mouse Jiggler	Arkane Systems	Automatically moves mouse pointer stopping screen saver, hibernation etc.
Notepad ++	Notepad ++	Advanced Notepad replacement

Name	From	Description
NSRL	NIST	Hash sets of 'known' (ignorable) files
Quick Hash	Ted Technology	A Linux & Windows GUI for individual and recursive SHA1 hashing of files
USB Write Blocker	DSi	Enables software write-blocking of USB ports
USB Write Blocker	Sécurité Multi-Secteurs	Software write blocker for Windows XP through to Windows 8
Volix	FH Aachen	Application that simplifies the use of the Volatility Framework
Windows Forensic Environment	Troy Larson	Guide by Brett Shavers to creating and working with a Windows boot CD

File and data analysis

Name	From	Description
Advanced Prefetch Analyser	Allan Hay	Reads Windows XP,Vista and Windows 7 prefetch files
analyzeMFT	David Kovar	Parses the MFT from an NTFS file system allowing results to be analysed with other tools
CapAnalysis	Evolka	PCAP viewer
Crowd Reponse	CrowdStike	Windows console application to aid gathering of system information for incident response and security engagements.
Crowd Inspect	CrowdStrike	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
DCode	Digital Detective	Converts various data types to date/time values
Defraser	Various	Detects full and partial multimedia files in unallocated space
eCryptfs Parser	Ted Technology	Recursively parses headers of every eCryptfs file in selected directory. Outputs encryption algorithm used, original file size, signature used, etc.
Encryption Analyzer	Passware	Scans a computer for password-protected & encrypted files, reports encryption complexity and decryption options for each file

Name	From	Description
ExifTool	Phil Harvey	Read, write and edit Exif data in a large number of file types
File Identifier	Toolsley.com	Drag and drop web-browser JavaScript tool for identification of over 2000 file types
Forensic Image Viewer	Sanderson Forensics	View various picture formats, image enhancer, extraction of embedded Exif, GPS data
Forpix	Martin Rojak	Identifies similar pictures that are no longer identical due to image manipulation
Ghiro	Alessandro Tanasi	In-depth analysis of image (picture) files
Highlighter	Mandiant	Examine log files using text, graphic or histogram views
Link Parser	4Discovery	Recursively parses folders extracting 30+ attributes from Windows .lnk (shortcut) files
LiveContactsView	Nirsoft	View and export Windows Live Messenger contact details
PlatformAuditProbe	AppliedAlgo	Command Line Windows forensic/ incident response tool that collects many artefacts. **Manual**
RSA Netwitness Investigator	EMC	Network packet capture and analysis
Memoryze	Mandiant	Acquire and/or analyse RAM images, including the page file on live systems
MetaExtractor	4Discovery	Recursively parses folders to extract meta data from MS Office, OpenOffice and PDF files
MFTview	Sanderson Forensics	Displays and decodes contents of an extracted MFT file
PictureBox	Mike’s Forensic Tools	Lists EXIF, and where available, GPS data for all photographs present in a directory. Export data to .xls or Google Earth KML format
PsTools	Microsoft	Suite of command-line Windows utilities
Shadow Explorer	Shadow Explorer	Browse and extract files from shadow copies
SQLite Manager	Mrinal Kant, Tarakant Tripathy	Firefox add-on enabling viewing of any SQLite database
Strings	Microsoft	Command-line tool for text searches

Name	From	Description
Structured Storage Viewer	MiTec	View and manage MS OLE Structured Storage based files
Switch-a-Roo	Mike's Forensic Tools	Text replacement/converter/decoder for when dealing with URL encoding, etc
Windows File Analyzer	MiTeC	Analyse thumbs.db, Prefetch, INFO2 and .lnk files
Xplico	Gianluca Costa & Andrea De Franceschi	Network forensics analysis tool

Mac OS tools

Name	From	Description
Audit	Twocanoes Software	Audit Preference Pane and Log Reader for OS X
ChainBreaker	Kyeongsik Lee	Parses keychain structure, extracting user's confidential information such as application account/password, encrypted volume password (e.g. filevault), etc
Disk Arbitrator	Aaron Burghardt	Blocks the mounting of file systems, complimenting a write blocker in disabling disk arbitration
Epoch Converter	Blackbag Technologies	Converts epoch times to local time and UTC
FTK Imager CLI for Mac OS	AccessData	Command line Mac OS version of AccessData's FTK Imager
IORegInfo	Blackbag Technologies	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
PMAP Info	Blackbag Technologies	Displays the physical partitioning of the specified device. Can be used to map out all the drive information, accounting for all used sectors
Volafox	Kyeongsik Lee	Memory forensic toolkit for Mac OS X

Mobile devices

Name	From	Description
iPBA2	Mario Piccinelli	Explore iOS backups
iPhone Analyzer	Leo Crawford, Mat Proud	Explore the internal file structure of Pad, iPod and iPhones
ivMeta	Robin Wood	Extracts phone model and software version and created date and GPS data from iPhone videos.
Last SIM Details	Dan Roe	Parses physical flash dumps and Nokia PM records to find details of previously inserted SIM cards.
Rubus	CCL Forensics	Deconstructs Blackberry .ipd backup files
SAFT	SignalSEC Corp	Obtain SMS Messages, call logs and contacts from Android devices

Data analysis suites

Name	From	Description
Autopsy	Brian Carrier	Graphical interface to the command line digital investigation analysis tools in The Sleuth Kit (see below)
Backtrack	Backtrack	Penetration testing and security audit with forensic boot capability
Caine	Nanni Bassetti	Linux based live CD, featuring a number of analysis tools
Deft	Dr. Stefano Fratepietro and others	Linux based live CD, featuring a number of analysis tools
Digital Forensics Framework	ArxSys	Analyses volumes, file systems, user and applications data, extracting metadata, deleted and hidden items
Forensic Scanner	Harlan Carvey	Automates ‘repetitive tasks of data collection’. Fuller description here
Paladin	Sumuri	Ubuntu based live boot CD for imaging and analysis
SIFT	SANS	VMware Appliance pre-configured with multiple tools allowing digital forensic examinations

Name	From	Description
The Sleuth Kit	Brian Carrier	Collection of UNIX-based command line file and volume system forensic analysis tools
Volatility Framework	Volatile Systems	Collection of tools for the extraction of artefacts from RAM

File viewers

Name	From	Description
BKF Viewer	SysTools	View contents of BKF (XP backup) files
E01 Viewer	SysTools	View E01 files to view messages within email EDB, PST and OST and search for file names
Microsoft PowerPoint 2007 Viewer	Microsoft	View PowerPoint presentations
Microsoft Visio 2010 Viewer	Microsoft	View Visio diagrams
VLC	VideoLAN	View most multimedia files and DVD, Audio CD, VCD, etc.

Internet analysis

Name	From	Description
Browser History Capturer	Foxton Software	Captures history from Firefox, Chrome and Internet Explorer web browsers running on a Windows computer
Browser History Viewer	Foxton Software	Extract, view and analyse internet history from Firefox, Chrome and Internet Explorer web browsers
Chrome Session Parser	CCL Forensics	Python module for performing off-line parsing of Chrome session files (“Current Session”, “Last Session”, “Current Tabs”, “Last Tabs”)

Name	From	Description
ChromeCacheView	Nirsoft	Reads the cache folder of Google Chrome Web browser, and displays the list of all files currently stored in the cache
Cookie Cutter	Mike's Forensic Tools	Extracts embedded data held within Google Analytics cookies. Shows search terms used as well as dates of and the number of visits.
Dumpzilla	Busindre	Runs in Python 3.x, extracting forensic information from Firefox, Iceweasel and Seamonkey browsers. See manual for more information.
Facebook Profile Saver	Belkasoft	Captures information publicly available in Facebook profiles.
IECookiesView	Nirsoft	Extracts various details of Internet Explorer cookies
IEPassView	Nirsoft	Extract stored passwords from Internet Explorer versions 4 to 8
MozillaCacheView	Nirsoft	Reads the cache folder of Firefox/Mozilla/Netscape Web browsers
MozillaCookieView	Nirsoft	Parses the cookie folder of Firefox/Mozilla/Netscape Web browsers
MozillaHistoryView	Nirsoft	Reads the history.dat of Firefox/Mozilla/Netscape Web browsers, and displays the list of all visited Web page
MyLastSearch	Nirsoft	Extracts search queries made with popular search engines (Google, Yahoo and MSN) and social networking sites (Twitter, Facebook, MySpace)
PasswordFox	Nirsoft	Extracts the user names and passwords stored by Mozilla Firefox Web browser
OperaCacheView	Nirsoft	Reads the cache folder of Opera Web browser, and displays the list of all files currently stored in the cache
OperaPassView	Nirsoft	Decrypts the content of the Opera Web browser password file, wand.dat
Web Historian	Mandiant	Reviews list of URLs stored in the history files of the most commonly used browsers
Web Page Saver	Magnet Forensics	Takes list of URLs saving scrolling captures of each page. Produces HTML report file containing the saved pages

Registry analysis

Name	From	Description
ForensicUserInfo	Woanware	Extracts user information from the SAM, SOFTWARE and SYSTEM hives files and decrypts the LM/NT hashes from the SAM file
Process Monitor	Microsoft	Examine Windows processes and registry threads in real time
Registry Decoder	US National Institute of Justice, Digital Forensics Solutions	For the acquisition, analysis, and reporting of registry contents
RegRipper	Harlan Carvey	Registry data extraction and correlation tool
Regshot	Regshot	Takes snapshots of the registry allowing comparisons e.g., show registry changes after installing software
sbag	TZWorks	Extracts data from Shellbag entries
USB Device Forensics	Woanware	Details previously attached USB devices on exported registry hives
USB Historian	4Discovery	Displays 20+ attributes relating to USB device use on Windows systems
USBDeview	Nirsoft	Details previously attached USB devices
User Assist Analysis	4Discovery	Extracts SID, User Names, Indexes, Application Names, Run Counts, Session, and Last Run Time Attributes from UserAssist keys
UserAssist	Didier Stevens	Displays list of programs run, with run count and last run date and time
Windows Registry Recovery	MiTec	Extracts configuration settings and other information from the Registry

Application analysis

Name	From	Description
Dropbox Decryptor	Magnet Forensics	Decrypts the Dropbox filecache.dbx file which stores information about files that have been synced to the cloud using Dropbox
Google Maps Tile	Magnet Forensics	Takes x,y,z coordinates found in a tile filename and downloads surrounding

Name	From	Description
Investigator		tiles providing more context
KaZAlyser	Sanderson Forensics	Extracts various data from the KaZaA application
LiveContactsView	Nirsoft	View and export Windows Live Messenger contact details
SkypeLogView	Nirsoft	View Skype calls and chats

For Reference

Name	From	Description
HotSwap	Kazuyuki Nakayama	Safely remove SATA disks similar to the “Safely Remove Hardware” icon in the notification area
iPhone Backup Browser	Rene Devichi	View unencrypted backups of iPad, iPod and iPhones
IEHistoryView	Nirsoft	Extracts recently visited Internet Explorer URLs
LiveView	CERT	Allows examiner to boot dd images in VMware.
Ubuntu guide	How-To Geek	Guide to using an Unbuntu live disk to recover partitions, carve files, etc.
WhatsApp Forensics	Zena Forensics	Extract WhatApp messages from iOS and Android backups