Les communautés de licence

JFC CNEJITA – 21 Juin 2016

Le paysage des outils d'investigation numérique

http://forensicswiki.org/wiki/Tools

Disk Analysis Tools

Hard Drive Firmware and Diagnostics Tools

PC-3000 from DeepSpar Data Recovery Systems
http://www.deepspar.com/products-pc-3000-drive.html
http://www.pc-3000.com/

Linux-based Tools

LINReS by NII Consulting Pvt. Ltd.
http://www.niiconsulting.com/innovation/linres.html
SMART by ASR Data
http://www.asrdata.com
Second Look: Linux Memory Forensics by Pikewerks Corporation
http://secondlookforensics.com/

Macintosh-based Tools

Macintosh Forensic Software by BlackBag Technologies, Inc.
http://www.blackbagtech.com/software_mfs.html
MacForensicsLab by Subrosasoft
MacForensicLab-Subrosasoft
Mac Marshal by ATC-NY
http://www.macmarshal.com/
Recon for MAC OS X by Sumuri, LLC.
https://www.sumuri.com/products/recon/

Windows-based Tools

Blackthorn GPS Forensics
http://www.blackthorngps.com
BringBack by Tech Assist, Inc.
http://www.toolsthatwork.com/bringback.htm
Belkasoft Evidence Center by Belkasoft
http://www.belkasoft.com
This product makes it easy for an investigator to search, analyze and store digital evidence found in Instant Messenger histories, Internet Browser histories and Outlook mailboxes.
CD/DVD Inspector by InfinaDyne
http://www.infinadyne.com/cddvd_inspector.html
This is the only forensic-qualified tool for examinination of optical media. It has been around since 1999 and is in use by law enforcement, government and data recovery companies worldwide.
EMail Detective - Forensic Software Tool by Hot Pepper Technology, Inc
http://www.hotpepperinc.com/emd
EnCase by Guidance Software
http://www.guidancesoftware.com/
Facebook Forensic Toolkit (FFT) by Afentis_forensics
http://www.facebookforensics.com
eDiscovery toolkit to identify and clone full profiles; including wall posts, private messages, uploaded photos/tags, group details, graphically illustrate friend links, and generate expert reports.
Forensic Explorer (FEX) by GetData Forensics
http://www.forensicexplorer.com
Forensic Toolkit (FTK) by AccessData
http://www.accessdata.com/products/ftk/
HBGary Responder Professional - Windows Physical Memory Forensic Platform
http://www.hbgary.com
ILook Investigator by Elliot Spencer and U.S. Dept of Treasury, Internal Revenue Service - Criminal Investigation (IRS)
http://www.ilook-forensics.org/
Internet Evidence Finder (IEF) by Magnet Forensics
http://www.magnetforensics.com/
Mercury Indexer by MicroForensics, Inc.
http://www.MicroForensics.com/
Nuix Desktop by Nuix Pty Ltd
http://www.nuix.com
OnLineDFS by Cyber Security Technologies
http://www.cyberstc.com/

Le paysage des outils d'investigation numérique

http://forensicswiki.org/wiki/Tools

OSForensics by **PassMark Software Pty Ltd**
http://www.osforensics.com/
P2 Power Pack by **Paraben**
https://www.paraben-forensics.com/catalog/product_info.php?cPath=25&products_id=187
Prodiscover by **Techpathways**
http://www.techpathways.com/ProDiscoverWindows.htm
Proof Finder by **Nuix Pty Ltd**
http://www.prooffinder.com/
Safeback by **NTI** and **Armor Forensics**
http://www.forensics-intl.com/safeback.html
X-Ways Forensics by **X-Ways AG**
http://www.x-ways.net/forensics/index-m.html
DateDecoder by **Live-Forensics**
http://www.live-forensics.com/dl/DateDecoder.zip
A command line tool that decodes most encoded time/date stamps found on a windows system, and outputs the time/date in a human readable format.
RecycleReader by **Live-Forensics**
http://www.live-forensics.com/dl/RecycleReader.zip
A command line tool that outputs the contents of the recycle bin on XP, Vista and 7.
Dstrings by **Live-Forensics**
http://www.live-forensics.com/dl/Dstrings.zip
A command line tool that searches for strings in a given file. It has the ability to compare the output of those strings against a dictionary to either exclude the dictionary terms in the output or only output files that match the dictionary. It also has the ability to search for IP Addresses and URLs/Email Addresses.
Unique by **Live-Forensics**
http://www.live-forensics.com/dl/Unique.zip
A command line tool similar to the Unix uniq. Allows for unique string counts, as well as various sorting options.
HashUtil by **Live-Forensics**
http://www.live-forensics.com/dl/HashUtil.zip
HashUtil.exe will calculate MD5, SHA1, SHA256 and SHA512 hashes. It has an option that will attempt to match the hash against the NIST/ISC MD5 hash databases.
WindowsSCOPE Pro, Ultimate, Live
Comprehensive Windows Memory Forensics and Cyber Analysis, Incident Response, and Education support.
Software and hardware based acquisition with CaptureGUARD PCIe and ExpressCard
Hardware based acquisition of memory on a locked computer via CaptureGUARD Gateway
WindowsSCOPE Live provides memory analysis of Windows computers on a network from Android phones and tablets.
MailXaminer by **SysTools**
http://www.mailxaminer.com/
Forensic & eDiscovery Tool to find digital email evidences from multiple email platform through its powerful Search mechanism.
Twitter Forensic Toolkit (TFT) by Afentis_forensics
http://www.twitterforensics.com
eDiscovery toolkit to identify relevant Tweets, clone full profiles, download all tweets/media, data mine across comments, and generate expert reports.
YouTube Forensic Toolkit (YFT) by Afentis_forensics
http://www.youtubeforensics.com
eDiscovery toolkit to identify relevant online media, download/convert videos, data mine across comments, and generate expert reports.

Open Source Tools

AFFLIB
A library for working with disk images. Currently AFFLIB supports raw, AFF, AFD, and EnCase file formats. Work to support segmented raw, iLook, and other formats is ongoing.
Autopsy
http://www.sleuthkit.org/autopsy/desc.php
Bulk Extractor
https://github.com/simsong/bulk_extractor/wiki
Bulk Extractor provides digital media triage by extracting Features from digital media.
Bulk Extractor Viewer
https://github.com/simsong/bulk_extractor/wiki/BEViewer
Bulk Extractor Viewer is a browser UI for viewing Feature data extracted using Bulk Extractor.
Digital Forensics Framework (DFF)
DFF is cross-platform and open-source, user and developers oriented. It provide many features and is very modular. Our goal is to provide a powerful framework to the forensic community, so people can use only one tool during the analysis. http://www.digital-forensic.org
foremost
http://foremost.sf.net/

Le paysage des outils d'investigation numérique

http://forensicswiki.org/wiki/Tools

Linux based file carving program
FTimes
http://ftimes.sourceforge.net/FTimes/index.shtml
FTimes is a system baselining and evidence collection tool.
gfzip
http://www.nongnu.org/gfzip/
gpart
http://www.stud.uni-hannover.de/user/76201/gpart/
Tries to *guess the primary partition table of a PC-type hard disk in case the primary partition table in sector 0 is damaged, incorrect or deleted.*
Hachoir
A generic framework for binary file manipulation, it supports FAT12, FAT16, FAT32, ext2/ext3, Linux swap, MSDOS partition header, etc. Recognize file type. Able to find subfiles (hachoir-subfile).
hashdb
http://github.com/simsong/hashdb/wiki
A tool for finding previously identified blocks of data in media such as disk images.
magicrescue
http://jbj.rapanden.dk/magicrescue/
The Open Computer Forensics Architecture
http://ocfa.sourceforge.net/
Paladin Forensic Suite (Sumuri, LLC.)
https://www.sumuri.com/products/paladin/
Simplifies various forensics tasks in a forensically sound manner via the PALADIN Toolbox.
pyflag
http://code.google.com/p/pyflag/
Web-based, database-backed forensic and log analysis GUI written in Python.
Scalpel
http://www.digitalforensicssolutions.com/Scalpel/
Linux and Windows file carving program originally based on foremost.
scrounge-ntfs
http://memberwebs.com/nielsen/software/scrounge/
Sleuthkit
http://www.sleuthkit.org/
The Coroner's Toolkit (TCT)
http://www.porcupine.org/forensics/tct.html

NDA and scoped distribution tools

Enterprise Tools (Proactive Forensics)

LiveWire Investigator 2008 by WetStone Technologies
http://www.wetstonetech.com/f/livewire2008.html
P2 Enterprise Edition by Paraben
http://www.paraben-forensics.com/enterprise_forensics.html

Forensics Live CDs

Kali Linux
http://www.kali.org/
KNOPPIX
http://www.knopper.net/knoppix/index-en.html
BackTrack Linux
http://www.backtrack-linux.org/
See: Forensics Live CDs

Personal Digital Device Tools

GPS Forensics

Blackthorn GPS Forensics
.XRY

PDA Forensics

Cellebrite UFED
.XRY
Paraben PDA Seizure
Paraben PDA Seizure Toolbox
PDD

Le paysage des outils d'investigation numérique

http://forensicswiki.org/wiki/Tools

Cell Phone Forensics

BitPIM
Cellebrite UFED
DataPilot Secure View
.XRY
http://www.msab.com/index
Fernico ZRT
ForensicMobile
LogiCube CellDEK
MOBILedit!
Oxygen Forensic Suite 2010
http://www.oxygen-forensic.com
Paraben's Device Seizure and **Paraben's Device Seizure Toolbox**
http://www.paraben-forensics.com/handheld_forensics.html
Serial Port Monitoring
TULP2G

SIM Card Forensics

Cellebrite UFED
.XRY
ForensicSIM
Paraben's SIM Card Seizure
http://www.paraben-forensics.com/handheld_forensics.html
SIMCon

Preservation Tools

Paraben StrongHold Bag
Paraben StrongHold Tent

Other Tools

Chat Sniper
http://www.alexbarnett.com/chatsniper.htm
A forensic software tool designed to simplify the process of on-scene evidence acquisition and analysis of logs and data left by the use of AOL, MSN (Live), or Yahoo instant messenger.
Serial Port Analyzer
http://www.eltima.com/how-to-analyze-serial-port-activity/
The tool to analyze serial port and device activity.
Computer Forensics Toolkit
http://computer-forensics.privacyresources.org
This is a collection of resources, most of which are informational, designed specifically to guide the beginner, often in a procedural sense.
Live View
http://liveview.sourceforge.net/
Live View is a graphical forensics tool that creates a VMware virtual machine out of a dd disk image or physical disk.
Parallels VM
http://www.parallels.com/
http://en.wikipedia.org/wiki/Parallels_Workstation
Serial and USB ports sharing
http://www.flexihub.com/serial-over-ethernet.html
Share and access serial and USB ports over Ethernet
Microsoft Virtual PC
http://www.microsoft.com/windows/products/winfamily/virtualpc/default.mspx
http://en.wikipedia.org/wiki/Virtual_PC
VMware Player
http://www.vmware.com/products/player/
http://en.wikipedia.org/wiki/VMware#VMware_Workstation
A free player for VMware virtual machines that will allow them to "play" on either Windows or Linux-based systems.
VMware Server
http://www.vmware.com/products/server/
The free server product, for setting up/configuring/running VMware virtual machine.Important difference being that it can run 'headless', i.e. everything in background.
Webtracer
http://www.forensictracer.com

Le paysage des outils d'investigation numérique

http://forensicswiki.org/wiki/Tools

Software for forensic analysis of internet resources (IP address, e-mail address, domain name, URL, e-mail headers, log files...)
Recon for MAC OS X
https://www.sumuri.com/products/recon/
RECON for Mac OS X is simply the fastest way to conduct Mac Forensics, automates what an experienced examiner would need weeks to accomplish in minutes, now includes PALADIN 6 which comes with a full featured Forensic Suite, bootable forensic imager, a software write-blocker and so much more.

Hex Editors

biew
http://biew.sourceforge.net/en/biew.html
bless
http://home.gna.org/bless/
Okteta
KDE's new cross-platform hex editor with features such as signature-matching
http://utils.kde.org/projects/okteta/
hexdump
...
HexFiend
A hex editor for Apple OS X
http://ridiculousfish.com/hexfiend/
Hex Workshop
A hex editor from BreakPoint Software, Inc.
http://www.bpsoft.com
khexedit
http://docs.kde.org/stable/en/kdeutils/khexedit/index.html
ReclaiMe Pro
The built-in disk editor visualizes most known partition and filesystem objects: boot sectors, superblocks, partition headers in structured view. Low-level data editing for extra leverage.
http://www.ReclaiMe-Pro.com
WinHex
Computer forensics software, data recovery software, hex editor, and disk editor from X-Ways.
http://www.x-ways.net/winhex
wxHexEditor
A Multi-OS supported, open sourced, hex and disk editor.
http://www.wxhexeditor.org
xxd
...
HexReader
Live-Forensics software that reads windows files at specified offset and length and outputs results to the console.
http://www.live-forensics.com/dl/HexReader.zip

Telephone Scanners/War Dialers

PhoneSweep
http://www.sandstorm.net/products/phonesweep/
PhoneSweep is a commercial grade multi-line wardialer used by many security auditors to run telephone line scans in their organizations. PhoneSweep Gold is the distributed-access add-on for PhoneSweep, for organizations that need to run scans remotely.
TeleSweep
http://www.securelogix.com/modemscanner/
SecureLogix is currently offering no-cost downloads of our award-winning TeleSweep Secure® modem-vulnerability scanner. This free modem scanning software can be used to dial a batch of corporate phone numbers and report on the number of modems connected to these corporate lines. *** Registration is required for obtaining a license key *** Still free however.
WarVox
https://github.com/rapid7/warvox
WarVOX is a free, open-source VOIP-based war dialing tool for exploring, classifying, and auditing phone systems.
Additional Software Names and Links (Jackpot!)
http://www.wyae.de/software/paw/

Les produits les + utilisés ou pas

Support de stockage

Encase

IEF

AXIOM

X-Ways Forensics

FTK

MPE+

Autopsy

Blackbag analyze

P2C 4

DS 7

Téléphonie/Tablette

Oxygen Forensics

Mobiledit forensic

La mise en commun des licences:

- Les conditions générales d'utilisation / End User License Agreement
- Qui les a lu ?

La mise en commun des licences: Magnet Forensics: IEF

- https://www.magnetforensics.com/legal/
- 2.3 You shall not and shall ensure that Users shall not:
- **copy, reproduce, or modify the Software** or any part thereof including the software that is provided as a license key to validate authorised use of the Software by a User;
- enhance, improve, alter, create derivative works, reverse engineer, disassemble, deconstruct, translate, decrypt, reverse compile or convert into human readable form the Software or any part thereof including the software that is provided as a license key to validate authorised use of the Software by a User;
- **distribute, lend, assign**, license, sublicense, lease, rent, transfer, sell or otherwise provide access to the Software, in whole or in part, **to any third party on a temporary or permanent basis**;
- remove, deface, cover or otherwise obscure any proprietary rights notice or identification on the Software (including without limitation any copyright notice);
- copy any written materials accompanying any portion of the Software unless specifically authorized in writing to do so by Magnet Forensics;
- **use the Software to provide services to third parties (including technical or training services)**, or otherwise publicly display or market the Software, for the purposes of your commercial gain (which includes any monetary consideration or other compensation);
- use the Software in any unlawful manner; or
- authorise, permit or otherwise acquiesce in any other party engaging in any of the activities set forth in (a) – (g) above, or attempting to do so. For the purposes of this provision “copy” or “reproduce” shall: (i) not include: (A) making additional copies of the Software for your own use, as long as only one copy may be used at any one time and used in accordance with and for the purposes described in the user documentation; or (B) making one back-up copy of the software licensed hereunder, provided that such copy is not used simultaneously or concurrently with the original software; and (ii) include, without limitation, pre-installing the Software or any part thereof on any computers used by other persons or third parties.

La mise en commun des licences: X-ways: Forensics

- http://www.x-ways.net/license.pdf
- X-Ways Forensics, X-Ways Investigator, X-Ways Imager: **One license authorizes one person to use the software on a single machine at a time. For computers at the same physical location, the number of licenses does not impose an upper limit on the number of computers with installations of the software.**

- **You may not rent, lease,** modify, translate, reverse-engineer, decompile or disassemble the software or create derivative works based on it without prior explicit permission. No component of the software must be accessed by other applications or processes, except through the X-Tensions API or the WinHex API.

La mise en commun des licences: Encase Forensic

- https://www.guidancesoftware.com/docs/default-source/legal/encase-forensic-v7--commercial-law-enforcement-and-government-terms.pdf?sfvrsn=3
- 3. Non-Exclusive License
- 3.1. Authorized Use. You are granted a limited non-exclusive license to use a copy of the enclosed Licensed Product on t**he computer(s) used by a single individual**. By your use of the Licensed Product pursuant to this Agreement, you recognize and acknowledge Guidance's proprietary rights in the Licensed Product. You may not distribute the Licensed Product, including any demonstration version of the Licensed Product, to third parties without the written authorization from Guidance. You may make additional backup copies of the Licensed Product for your own use, as long as only one copy may be used at any one time.
- 3.2. Copies. The Customer may make one archival or back-up copy of the software licensed hereunder, provided that such copy is not used simultaneously or concurrently with the original software, and only if Guidance and Guidance's vendors' copyright and proprietary notices on the software are included on such copy. The Customer may not copy the printed materials, if any, accompanying the Licensed Product, or print multiple copies of any user documentation. No copies or duplicates of the dongle hardware key may be made.
- 3.3 Restrictions. Applicable copyright laws protect the Licensed Product in its entirety. The Licensed Product contains Guidance trade secrets, and thus you may not decompile, reverse engineer, disassemble, or otherwise reduce the Licensed Product to human-perceivable form or disable any functionality that limits the use of the Licensed Product. **You may not** modify, adapt, translate, r**ent, sublicense, assign, loan,** resell for profit, distribute, **or network the Licensed Product,** disk, or related materials or create derivative works based upon the Licensed Product or any part thereof. You may not publicly display the Licensed Product or provide technical training or instruction for monetary compensation or other consideration in any form. **Your license is automatically terminated if you take any of the actions prohibited by the paragraph.**

La mise en commun des licences: MSAB

- https://www.msab.com/terms/#toc-eula
- 3 Restrictions
- Use of the Product (or supporting hardware) requires a copy protection key(s) given to you by MSAB (the “Copy Protection Key”).
- The Copy Protection Key **enables your use of the Product and is valid for one (1) copy of the Product.**
- You may only use the **Copy Protection Key on the same device in which you use the Product** and you may not make the Copy Protection Key or the Product accessible over a public or private network.
- You may not publish, display, disclose, sell, **rent, lease,** modify, store, **loan,** distribute, or modify or create derivative works of the Product, or any part thereof, or copy the Product onto any public or distributed network, or delete or change any proprietary notices appearing on the Product including the Copy Protection Key.
- You **may not assign, sublicense,** convey or otherwise transfer, pledge as security or otherwise encumber the rights and licenses granted hereunder.
- You may not copy, reverse engineer, decompile, reverse compile, translate, adapt, or disassemble the Product, or any part thereof, nor shall you attempt to create source code from the object or executable code for the Product. You may not market, co-brand, private label, or otherwise permit third parties to link to the Product, or any part thereof.
- You **may not use the Product, or any part thereof, for the benefit of any other person or entity** (e**xcept that you may permit use by your contractors to whom you have outsourced your operations** that relate to the use of the Product provided they only use the Product for your internal business purposes (on behalf of your business and not the business of another entity).
- You may not modify, or create a derivative version of the Product.
- Moreover, you may not merge the Product with another program, except as may be specifically described in the accompanying documentation.
- Notwithstanding the foregoing, any and all modifications to or customizations, configurations, or derivative versions of the Product are subject to this EULA and MSAB’s ownership rights to and in the Product.
- **You may not use the Product apart from the devices on which the Product is embedded or made available to you by MSAB.**

La mise en commun des licences: CELLEBRITE

- https://www.msab.com/terms/#toc-eula
- **No Right to Sublicense or Assign.** Except to the extent otherwise required by applicable Law or expressly provided for assignment generally in the Agreement, no license provided in this Section 2 is sublicensable, transferable or assignable by Buyer, including by operation of Law, change of control, merger, purchase or otherwise, without the prior written consent of Cellebrite in each instance. Other than as expressly permitted by the foregoing, any attempted sublicense, transfer or assignment by Buyer shall be null and void.

- License Prohibitions. Notwithstanding anything to the contrary in this EULA, Buyer **shall not,** alone, **through a User,** an Affiliate or a **Third Party (or allow a User, an Affiliate or a Third Party to):** (a)modify any Software; (b) reverse compile, reverse assemble, reverse engineer or otherwise translate all or any portion of any Software; **(c) pledge, rent, lease, share, distribute, sell or create derivative works of any Software; (d) use any Software on a time sharing, service bureau, application service provider (ASP), rental or other similar basis;** (e) make copies of any Software, except as provided for in the license grant above; (e) remove, alter or deface (or attempt

Questions ?