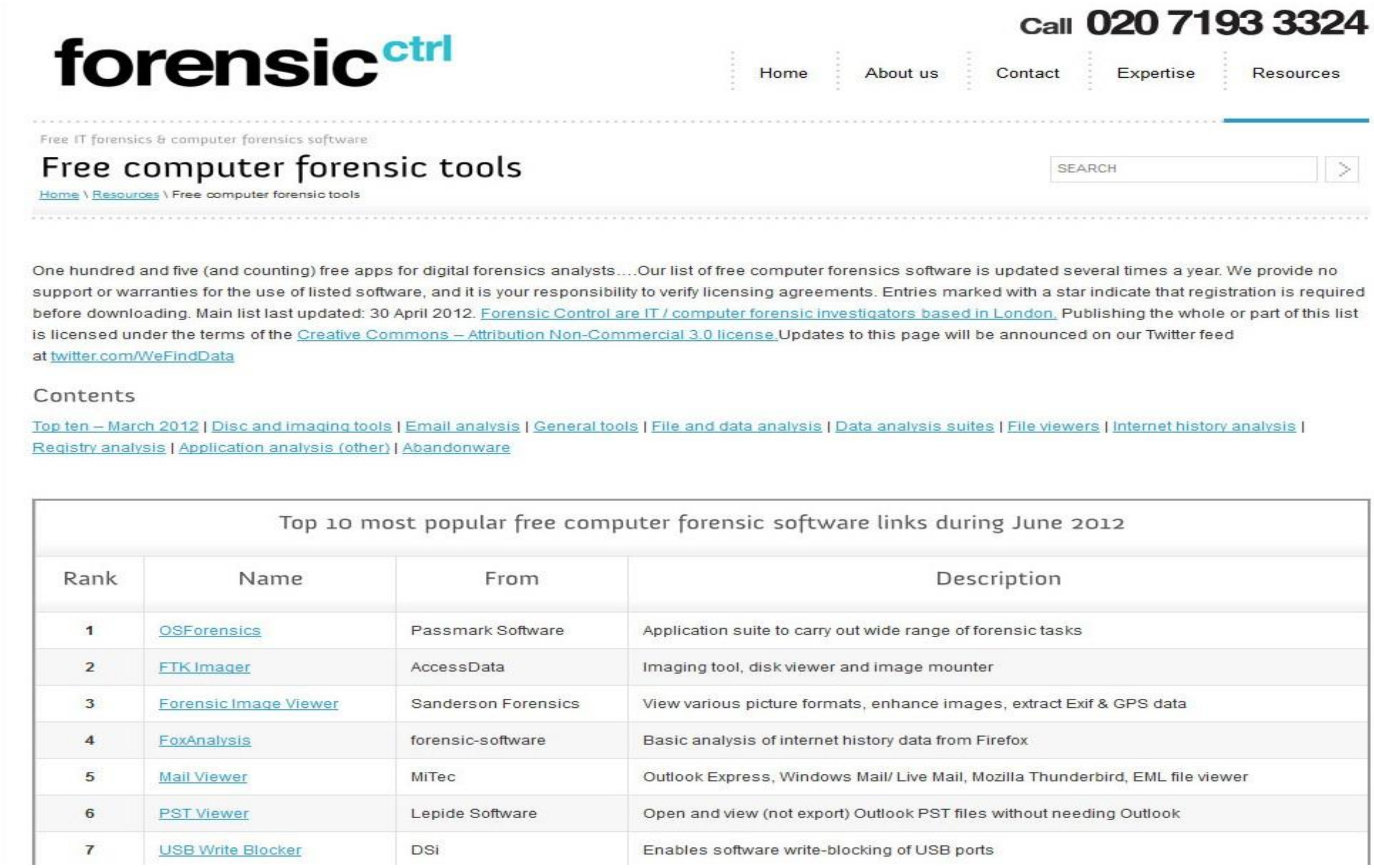
COMPUTER FORENSICS

OPEN SOURCE AND FREE SOFTWARE

RICHARD GOLDSTON
G2 RESEARCH INC.

http://forensiccontrol.com/resources/free-software



Free IT forensics & computer forensics software

Free computer forensic tools

Home \ Resources \ Free computer forensic tools

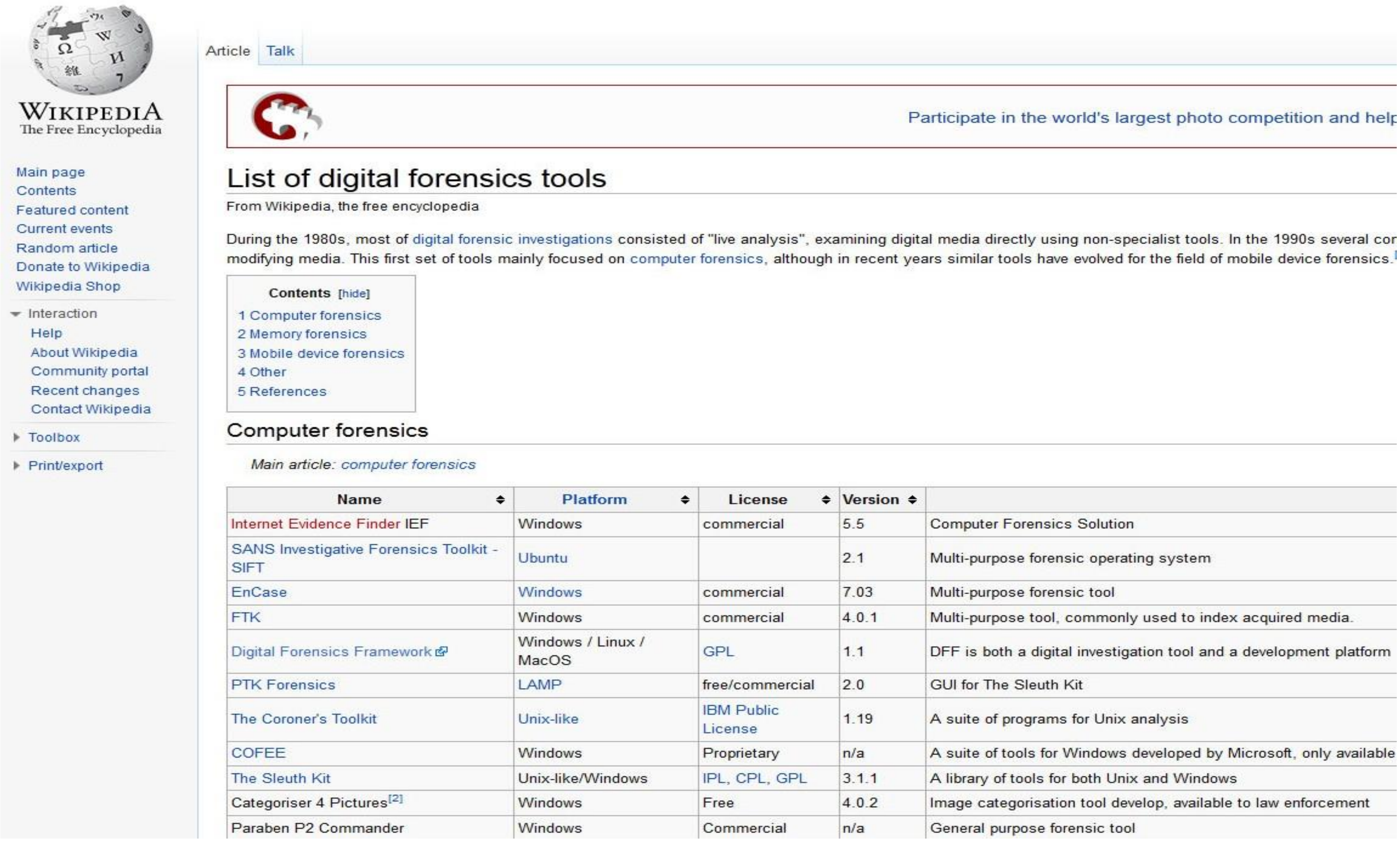
One hundred and five (and counting) free apps for digital forensics analysts….Our list of free computer forensics software is updated several times a year. We provide no support or warranties for the use of listed software, and it is your responsibility to verify licensing agreements. Entries marked with a star indicate that registration is required before downloading. Main list last updated: 30 April 2012. Forensic Control are IT / computer forensic investigators based in London. Publishing the whole or part of this list is licensed under the terms of the Creative Commons – Attribution Non-Commercial 3.0 license. Updates to this page will be announced on our Twitter feed at twitter.com/WeFindData

Contents

Top 10 most popular free computer forensic software links during June 2012

Rank	Name	From	Description
1	OSForensics	Passmark Software	Application suite to carry out wide range of forensic tasks
2	FTK Imager	AccessData	Imaging tool, disk viewer and image mounter
3	Forensic Image Viewer	Sanderson Forensics	View various picture formats, enhance images, extract Exif & GPS data
4	FoxAnalysis	forensic-software	Basic analysis of internet history data from Firefox
5	Mail Viewer	MiTec	Outlook Express, Windows Mail/ Live Mail, Mozilla Thunderbird, EML file viewer
6	PST Viewer	Lepide Software	Open and view (not export) Outlook PST files without needing Outlook
7	USB Write Blocker	DSi	Enables software write-blocking of USB ports

http://en.wikipedia.org/wiki/List_of_digital_forensics_tools



Main page
Contents
Featured content
Current events
Random article
Donate to Wikipedia
Wikipedia Shop

Interaction
Help
About Wikipedia
Community portal
Recent changes
Contact Wikipedia

Toolbox

Print/export

Article Talk

Participate in the world's largest photo competition and help

List of digital forensics tools

From Wikipedia, the free encyclopedia

During the 1980s, most of digital forensic investigations consisted of "live analysis", examining digital media directly using non-specialist tools. In the 1990s several cor modifying media. This first set of tools mainly focused on computer forensics, although in recent years similar tools have evolved for the field of mobile device forensics.[

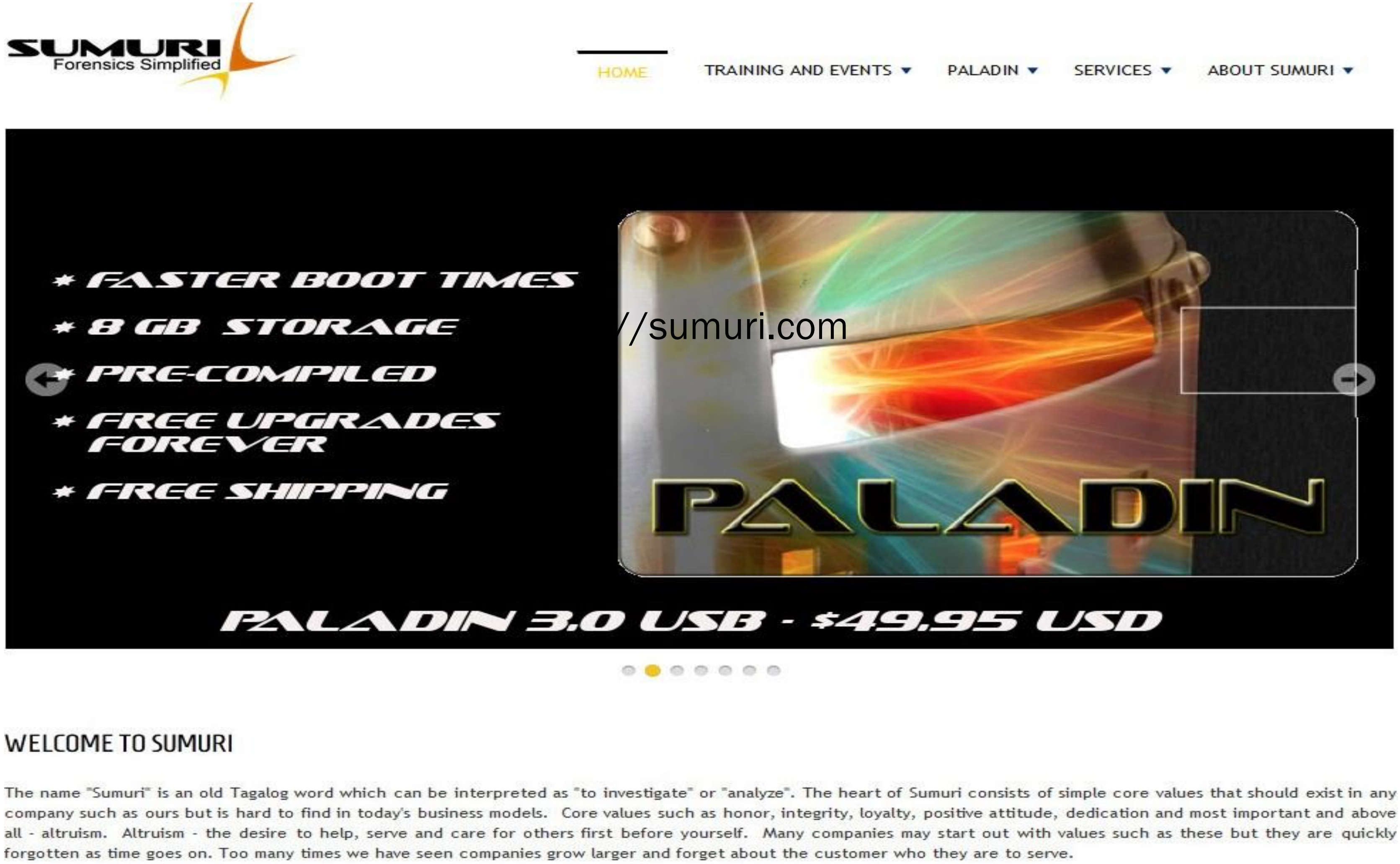
Contents [hide]

Computer forensics

Main article: computer forensics

Name	Platform	License	Version	
Internet Evidence Finder IEF	Windows	commercial	5.5	Computer Forensics Solution
SANS Investigative Forensics Toolkit - SIFT	Ubuntu		2.1	Multi-purpose forensic operating system
EnCase	Windows	commercial	7.03	Multi-purpose forensic tool
FTK	Windows	commercial	4.0.1	Multi-purpose tool, commonly used to index acquired media.
Digital Forensics Framework	Windows / Linux / MacOS	GPL	1.1	DFF is both a digital investigation tool and a development platform
PTK Forensics	LAMP	free/commercial	2.0	GUI for The Sleuth Kit
The Coroner's Toolkit	Unix-like	IBM Public License	1.19	A suite of programs for Unix analysis
COFEE	Windows	Proprietary	n/a	A suite of tools for Windows developed by Microsoft, only available
The Sleuth Kit	Unix-like/Windows	IPL, CPL, GPL	3.1.1	A library of tools for both Unix and Windows
Categoriser 4 Pictures[2]	Windows	Free	4.0.2	Image categorisation tool develop, available to law enforcement
Paraben P2 Commander	Windows	Commercial	n/a	General purpose forensic tool

http://sumuri.com

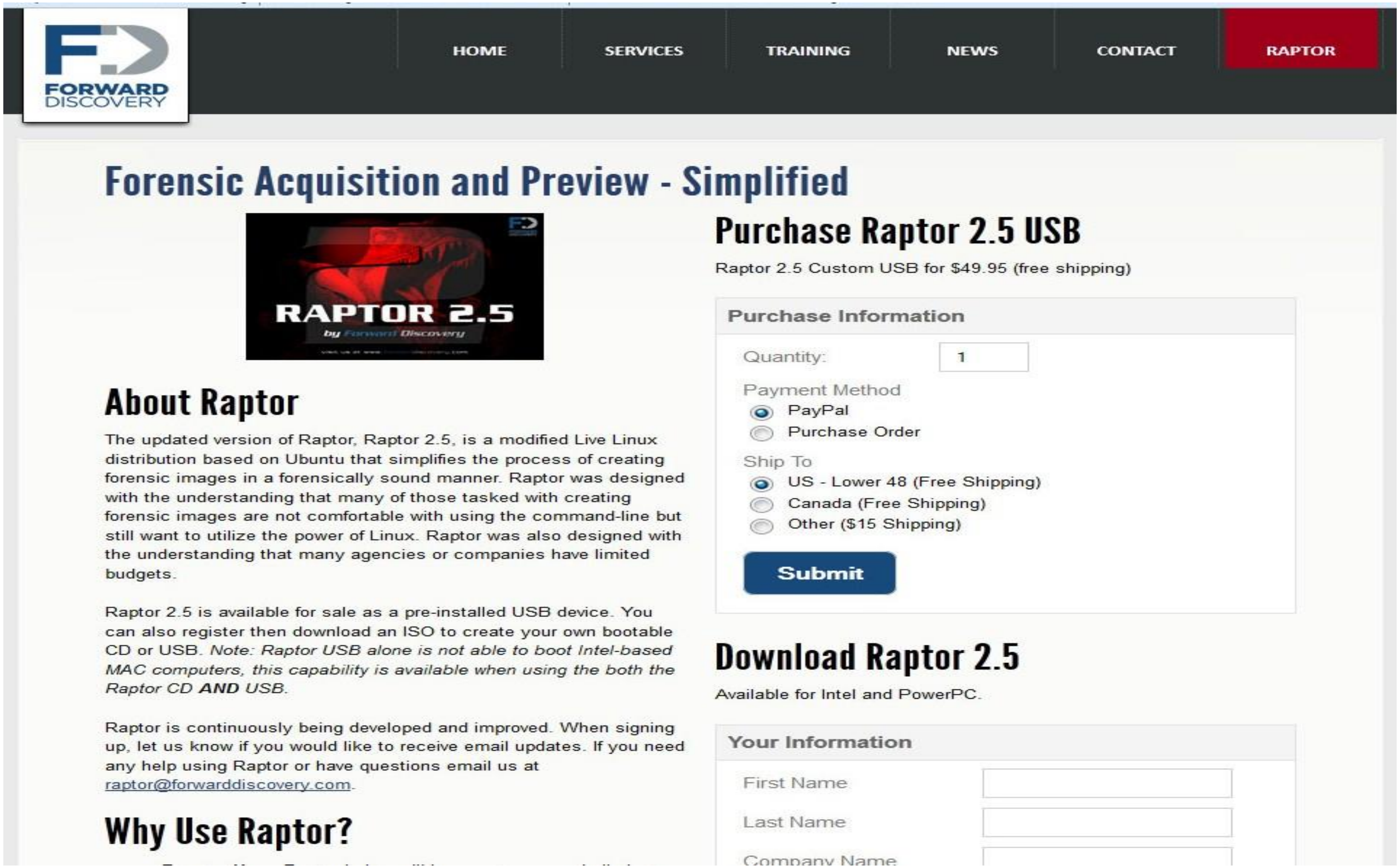


//sumuri.com

WELCOME TO SUMURI

The name "Sumuri" is an old Tagalog word which can be interpreted as "to investigate" or "analyze". The heart of Sumuri consists of simple core values that should exist in any company such as ours but is hard to find in today's business models. Core values such as honor, integrity, loyalty, positive attitude, dedication and most important and above all - altruism. Altruism - the desire to help, serve and care for others first before yourself. Many companies may start out with values such as these but they are quickly forgotten as time goes on. Too many times we have seen companies grow larger and forget about the customer who they are to serve.

http://www.forwarddiscovery.com/Raptor



Forensic Acquisition and Preview - Simplified

About Raptor

The updated version of Raptor, Raptor 2.5, is a modified Live Linux distribution based on Ubuntu that simplifies the process of creating forensic images in a forensically sound manner. Raptor was designed with the understanding that many of those tasked with creating forensic images are not comfortable with using the command-line but still want to utilize the power of Linux. Raptor was also designed with the understanding that many agencies or companies have limited budgets.

Raptor 2.5 is available for sale as a pre-installed USB device. You can also register then download an ISO to create your own bootable CD or USB. *Note: Raptor USB alone is not able to boot Intel-based MAC computers, this capability is available when using the both the Raptor CD **AND** USB.*

Raptor is continuously being developed and improved. When signing up, let us know if you would like to receive email updates. If you need any help using Raptor or have questions email us at raptor@forwarddiscovery.com.

Why Use Raptor?

Purchase Raptor 2.5 USB

Raptor 2.5 Custom USB for $49.95 (free shipping)

Purchase Information

Quantity: 1

Payment Method
● PayPal
○ Purchase Order

Ship To
● US - Lower 48 (Free Shipping)
○ Canada (Free Shipping)
○ Other ($15 Shipping)

Submit

Download Raptor 2.5

Available for Intel and PowerPC.

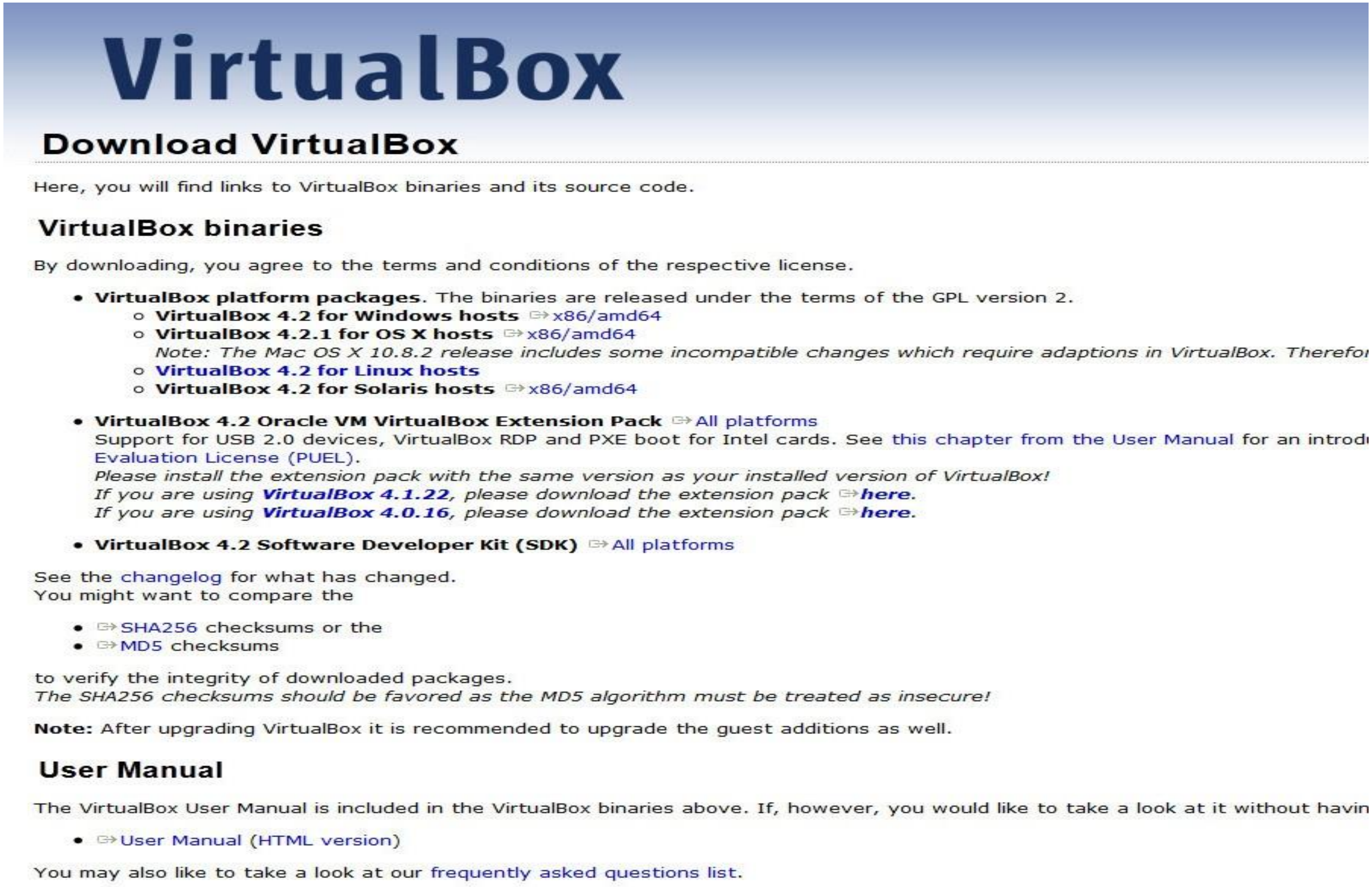
Your Information

First Name

Last Name

Company Name

https://www.virtualbox.org



VirtualBox

Download VirtualBox

Here, you will find links to VirtualBox binaries and its source code.

VirtualBox binaries

By downloading, you agree to the terms and conditions of the respective license.

- **VirtualBox platform packages**. The binaries are released under the terms of the GPL version 2.
  - **VirtualBox 4.2 for Windows hosts** ⇨x86/amd64
  - **VirtualBox 4.2.1 for OS X hosts** ⇨x86/amd64

    Note: The Mac OS X 10.8.2 release includes some incompatible changes which require adaptions in VirtualBox. Therefo
  - **VirtualBox 4.2 for Linux hosts**
  - **VirtualBox 4.2 for Solaris hosts** ⇨x86/amd64
- **VirtualBox 4.2 Oracle VM VirtualBox Extension Pack** ⇨All platforms

  Support for USB 2.0 devices, VirtualBox RDP and PXE boot for Intel cards. See this chapter from the User Manual for an introd
  Evaluation License (PUEL).

  Please install the extension pack with the same version as your installed version of VirtualBox!

  *If you are using **VirtualBox 4.1.22**, please download the extension pack ⇨**here**.*

  *If you are using **VirtualBox 4.0.16**, please download the extension pack ⇨**here**.*
- **VirtualBox 4.2 Software Developer Kit (SDK)** ⇨All platforms

See the changelog for what has changed.
You might want to compare the

- ⇨SHA256 checksums or the
- ⇨MD5 checksums

to verify the integrity of downloaded packages.
The SHA256 checksums should be favored as the MD5 algorithm must be treated as insecure!

Note: After upgrading VirtualBox it is recommended to upgrade the guest additions as well.

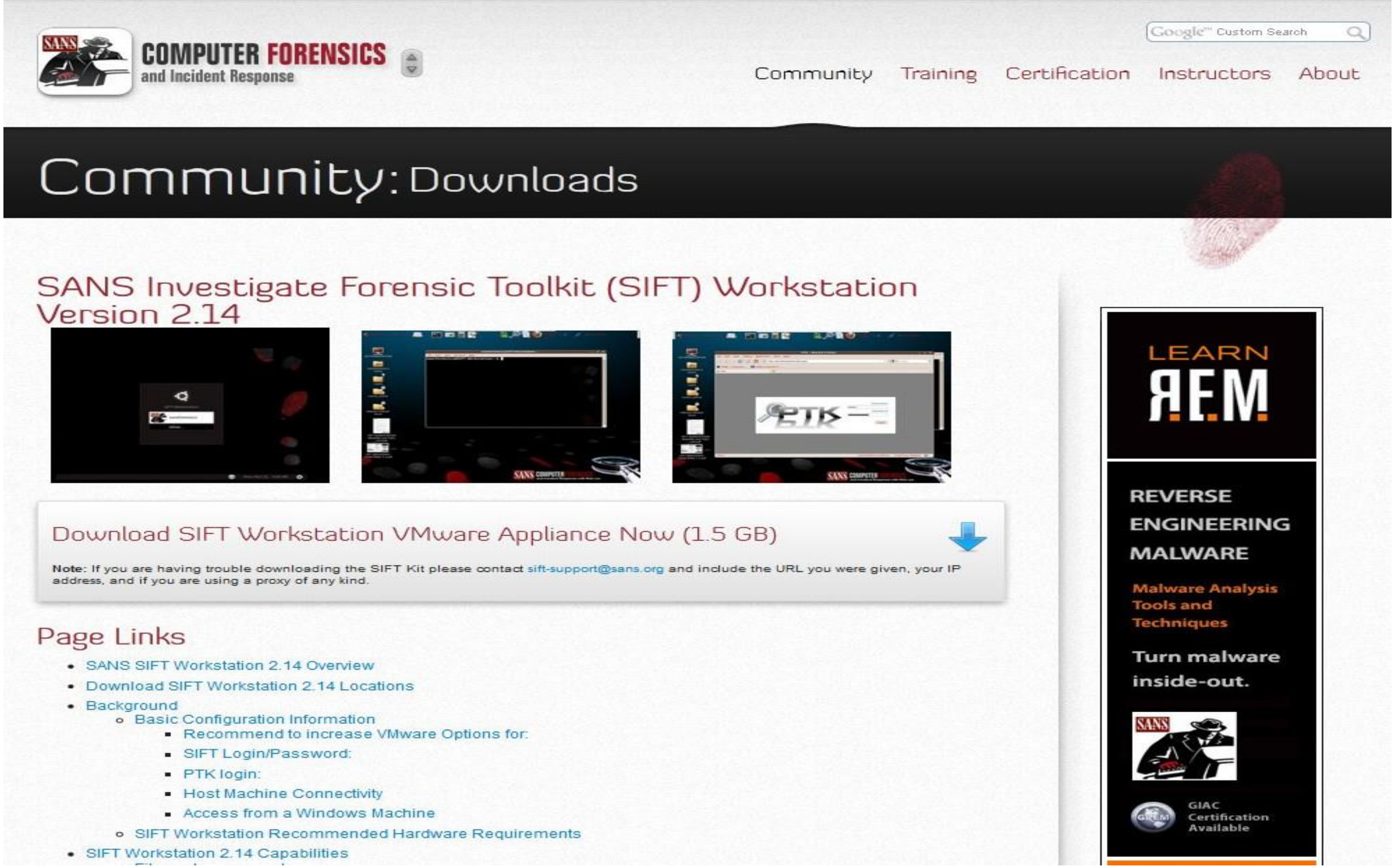
User Manual

The VirtualBox User Manual is included in the VirtualBox binaries above. If, however, you would like to take a look at it without havin

- ⇨User Manual (HTML version)

You may also like to take a look at our frequently asked questions list.

https://computer-forensics.sans.org



Community: Downloads

SANS Investigate Forensic Toolkit (SIFT) Workstation Version 2.14

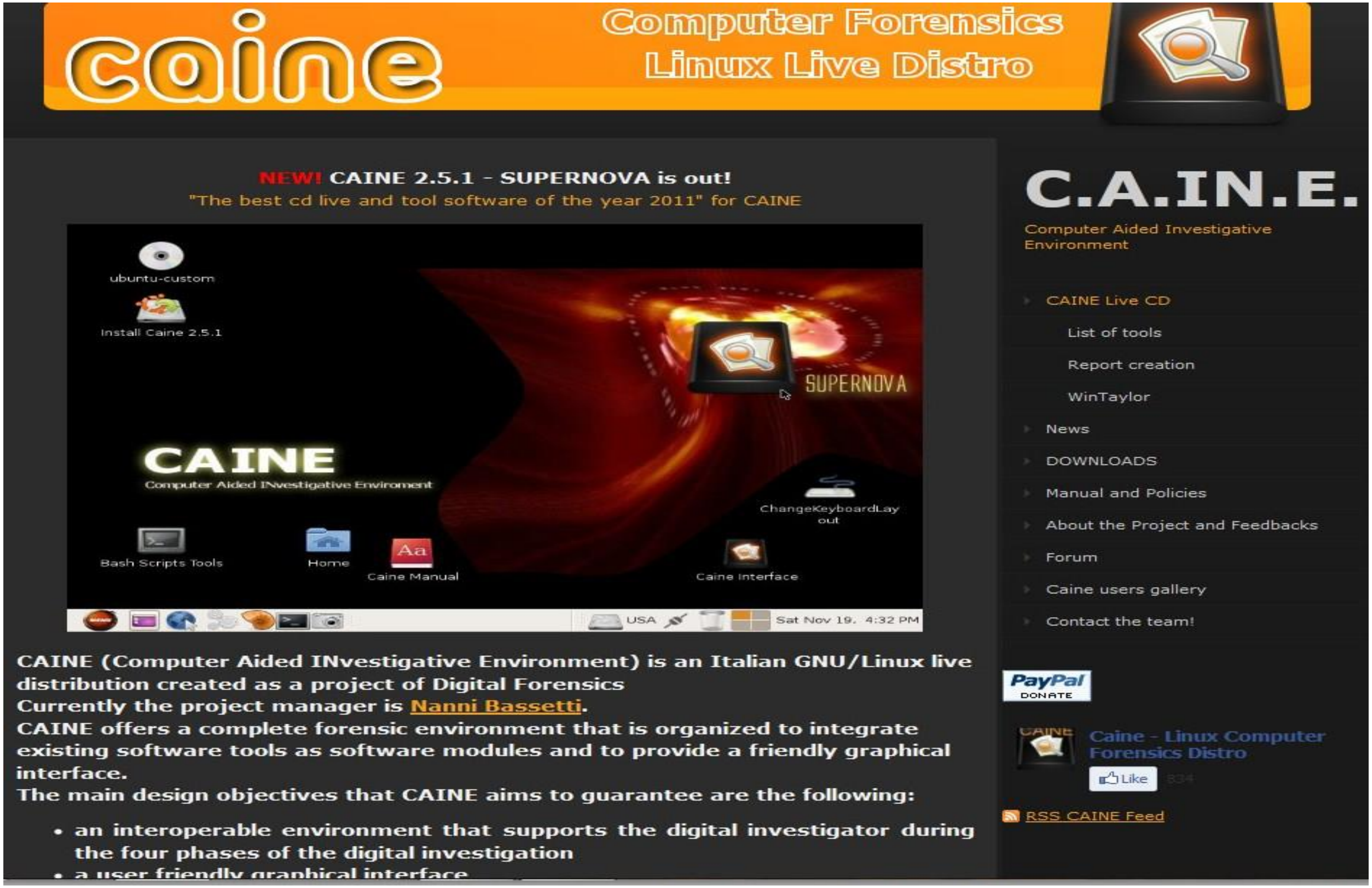
Download SIFT Workstation VMware Appliance Now (1.5 GB)

Note: If you are having trouble downloading the SIFT Kit please contact sift-support@sans.org and include the URL you were given, your IP address, and if you are using a proxy of any kind.

Page Links

- SANS SIFT Workstation 2.14 Overview
- Download SIFT Workstation 2.14 Locations
- Background
    - Basic Configuration Information
        - Recommend to increase VMware Options for:
        - SIFT Login/Password:
        - PTK login:
        - Host Machine Connectivity
        - Access from a Windows Machine
    - SIFT Workstation Recommended Hardware Requirements
- SIFT Workstation 2.14 Capabilities

http://www.caine-live.net



NEW! CAINE 2.5.1 - SUPERNOVA is out!

"The best cd live and tool software of the year 2011" for CAINE

CAINE (Computer Aided INvestigative Environment) is an Italian GNU/Linux live distribution created as a project of Digital Forensics
Currently the project manager is Nanni Bassetti.
CAINE offers a complete forensic environment that is organized to integrate existing software tools as software modules and to provide a friendly graphical interface.
The main design objectives that CAINE aims to guarantee are the following:

- an interoperable environment that supports the digital investigator during the four phases of the digital investigation
- a user friendly graphical interface

C.A.IN.E.

Computer Aided Investigative Environment

- CAINE Live CD
  - List of tools
  - Report creation
  - WinTaylor
- News
- DOWNLOADS
- Manual and Policies
- About the Project and Feedbacks
- Forum
- Caine users gallery
- Contact the team!

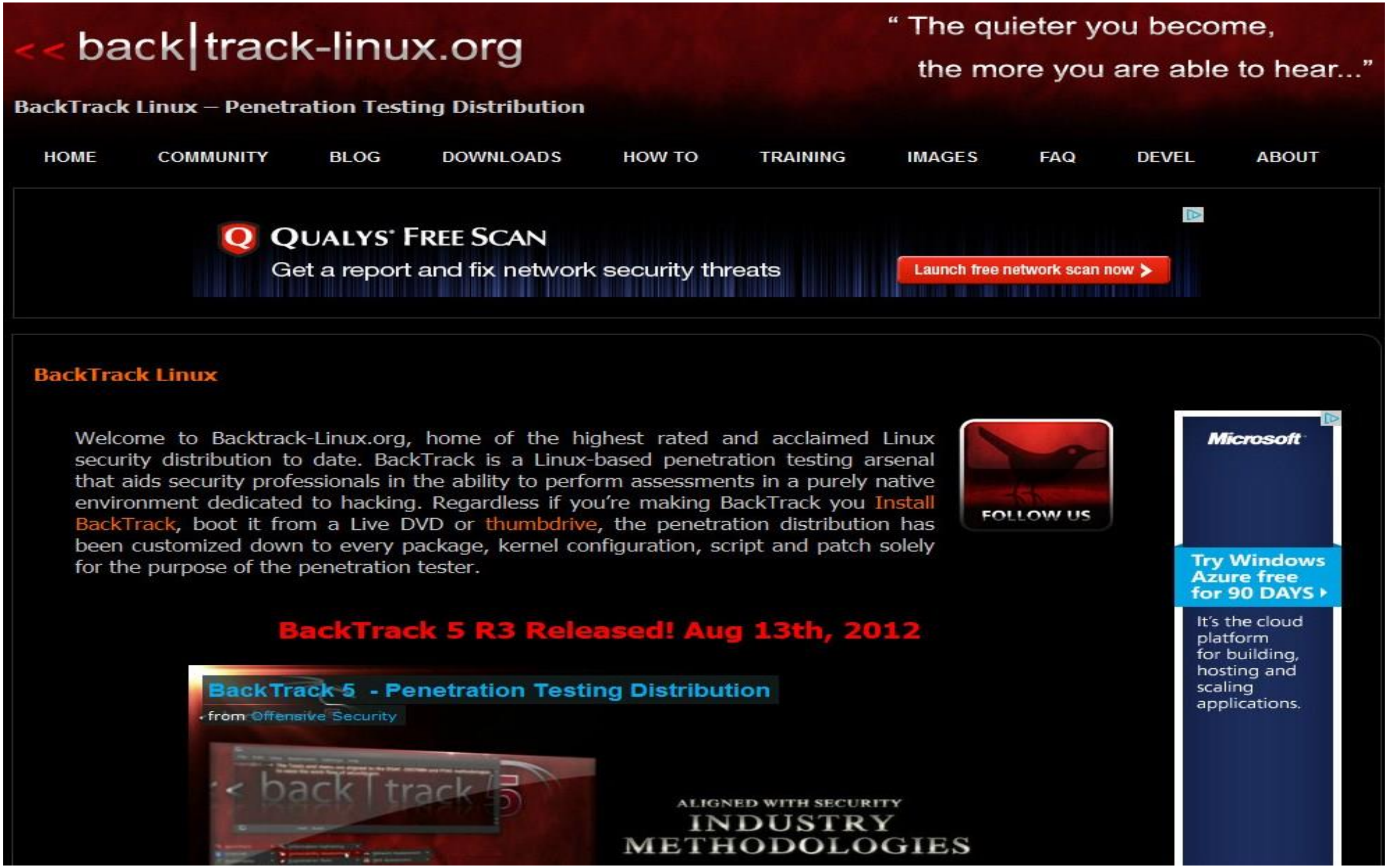
PayPal DONATE

Caine - Linux Computer Forensics Distro

Like 834

RSS CAINE Feed

http://www.backtrack-linux.org



<< back|track-linux.org

" The quieter you become,
the more you are able to hear..."

BackTrack Linux – Penetration Testing Distribution

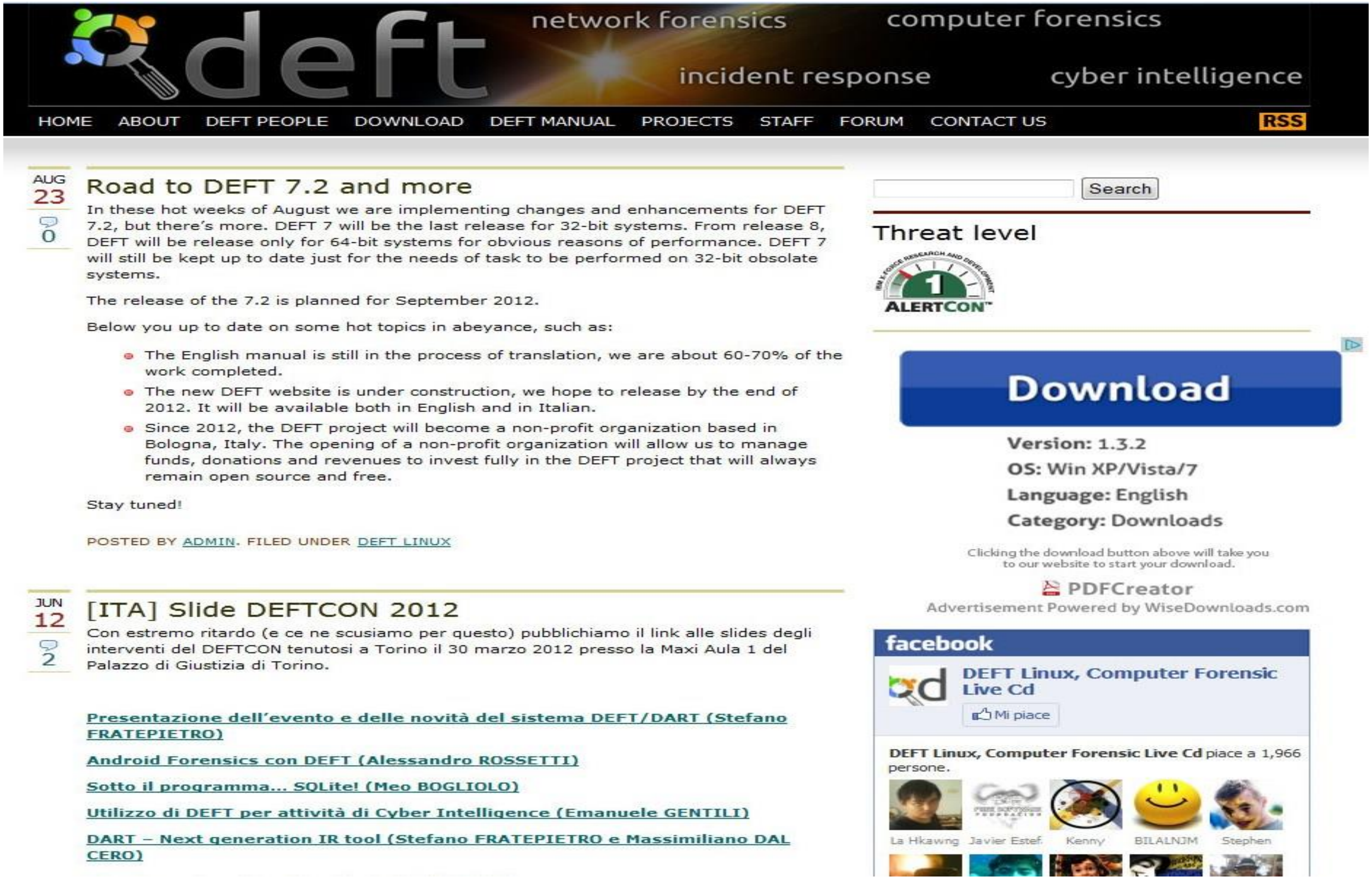
BackTrack Linux

Welcome to Backtrack-Linux.org, home of the highest rated and acclaimed Linux security distribution to date. BackTrack is a Linux-based penetration testing arsenal that aids security professionals in the ability to perform assessments in a purely native environment dedicated to hacking. Regardless if you're making BackTrack you Install BackTrack, boot it from a Live DVD or thumbdrive, the penetration distribution has been customized down to every package, kernel configuration, script and patch solely for the purpose of the penetration tester.

BackTrack 5 R3 Released! Aug 13th, 2012

BackTrack 5 - Penetration Testing Distribution
from Offensive Security

http://www.deftlinux.net



Road to DEFT 7.2 and more

In these hot weeks of August we are implementing changes and enhancements for DEFT 7.2, but there's more. DEFT 7 will be the last release for 32-bit systems. From release 8, DEFT will be release only for 64-bit systems for obvious reasons of performance. DEFT 7 will still be kept up to date just for the needs of task to be performed on 32-bit obsolate systems.

The release of the 7.2 is planned for September 2012.

Below you up to date on some hot topics in abeyance, such as:

- The English manual is still in the process of translation, we are about 60-70% of the work completed.
- The new DEFT website is under construction, we hope to release by the end of 2012. It will be available both in English and in Italian.
- Since 2012, the DEFT project will become a non-profit organization based in Bologna, Italy. The opening of a non-profit organization will allow us to manage funds, donations and revenues to invest fully in the DEFT project that will always remain open source and free.

Stay tuned!

POSTED BY ADMIN. FILED UNDER DEFT LINUX

[ITA] Slide DEFTCON 2012

Con estremo ritardo (e ce ne scusiamo per questo) pubblichiamo il link alle slides degli interventi del DEFTCON tenutosi a Torino il 30 marzo 2012 presso la Maxi Aula 1 del Palazzo di Giustizia di Torino.

Presentazione dell'evento e delle novità del sistema DEFT/DART (Stefano FRATEPIETRO)

Android Forensics con DEFT (Alessandro ROSSETTI)

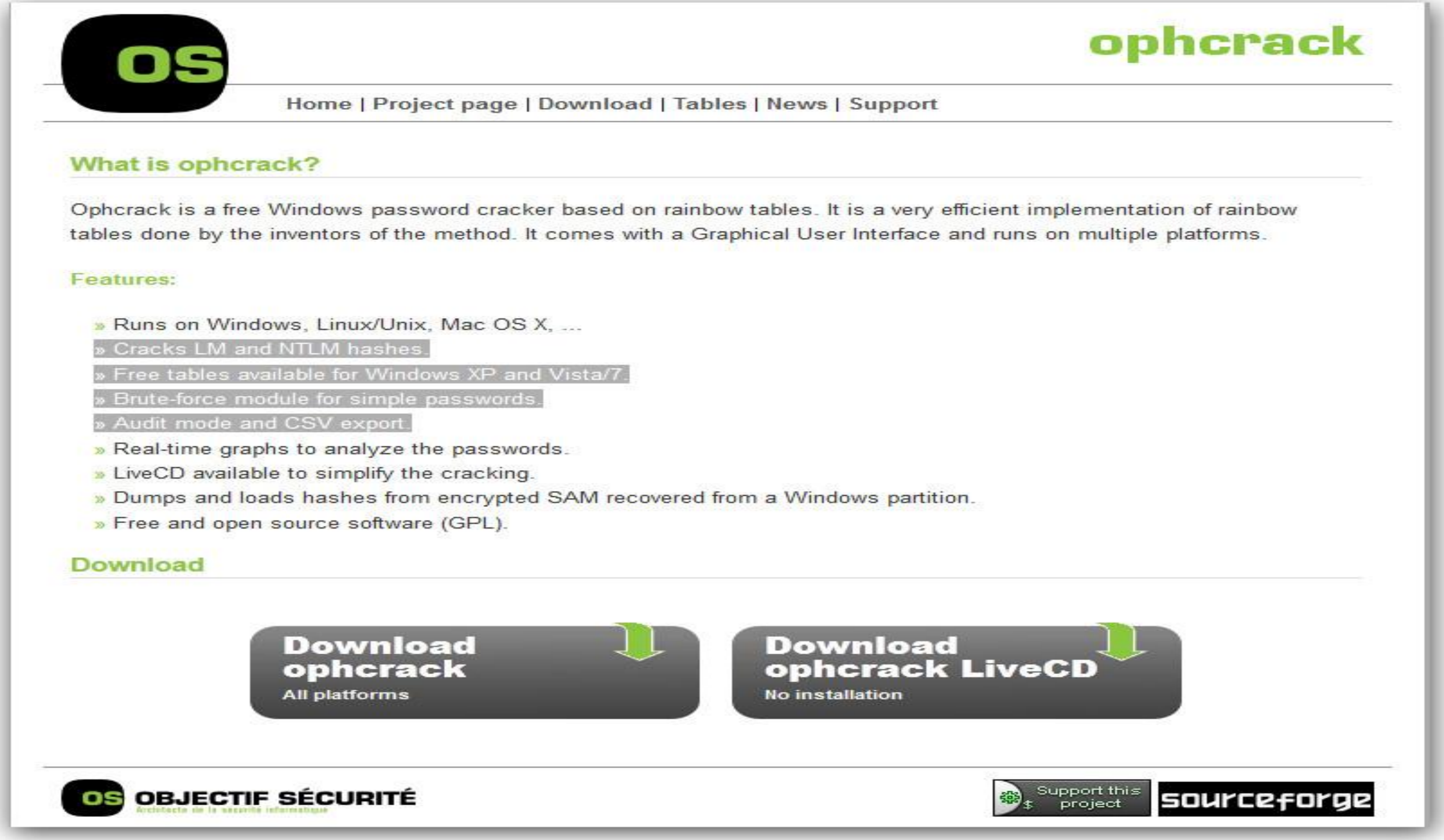
Sotto il programma... SQLite! (Meo BOGLIOLO)

Utilizzo di DEFT per attività di Cyber Intelligence (Emanuele GENTILI)

DART – Next generation IR tool (Stefano FRATEPIETRO e Massimiliano DAL CERO)

DEFT Linux, Computer Forensic Live Cd piace a 1,966 persone.

http://ophcrack.sourceforge.net



What is ophcrack?

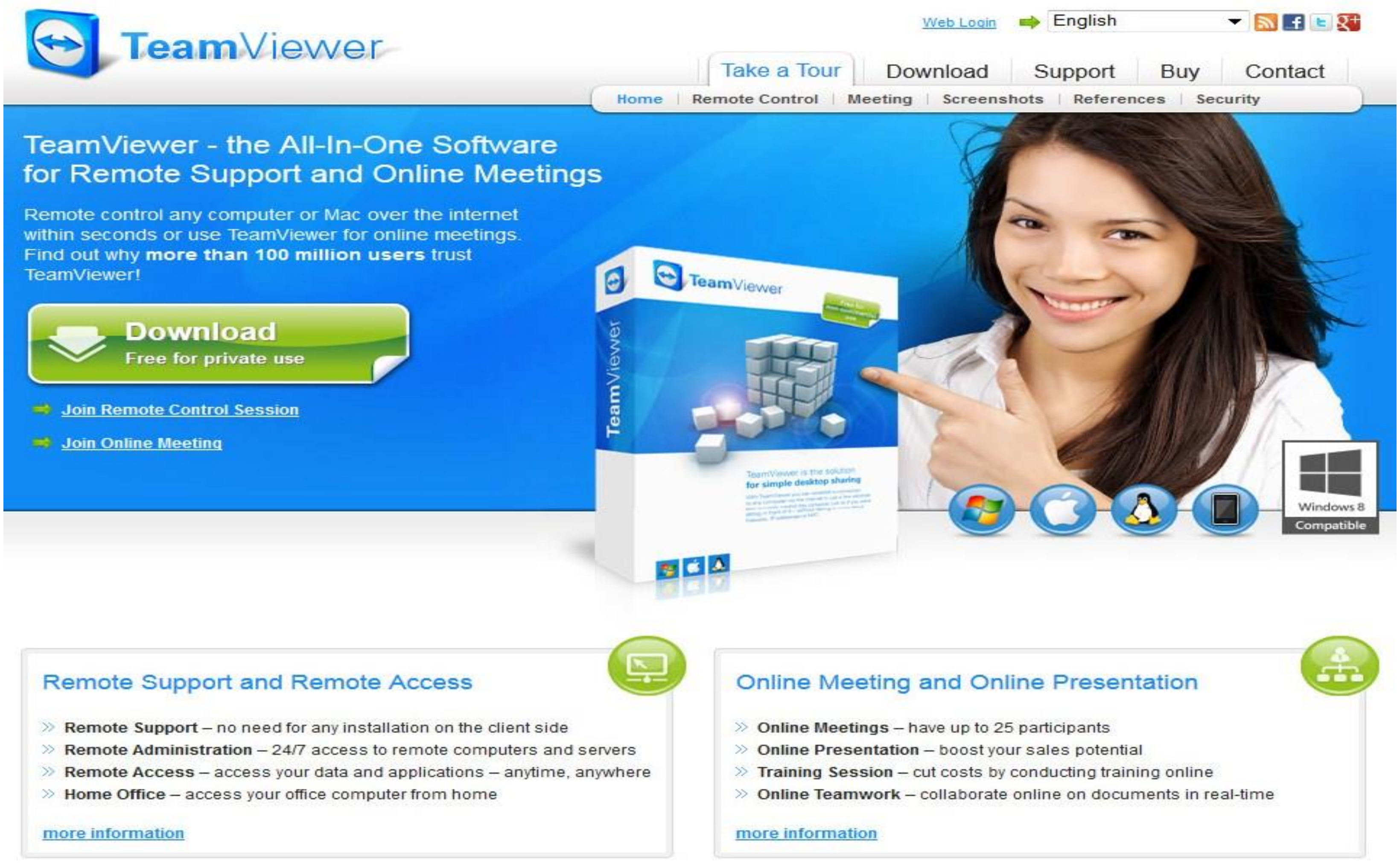
Ophcrack is a free Windows password cracker based on rainbow tables. It is a very efficient implementation of rainbow tables done by the inventors of the method. It comes with a Graphical User Interface and runs on multiple platforms.

Features:

- Runs on Windows, Linux/Unix, Mac OS X, ...
- Cracks LM and NTLM hashes.
- Free tables available for Windows XP and Vista/7.
- Brute-force module for simple passwords.
- Audit mode and CSV export.
- Real-time graphs to analyze the passwords.
- LiveCD available to simplify the cracking.
- Dumps and loads hashes from encrypted SAM recovered from a Windows partition.
- Free and open source software (GPL).

Download

http://www.teamviewer.com



TeamViewer - the All-In-One Software for Remote Support and Online Meetings

Remote control any computer or Mac over the internet within seconds or use TeamViewer for online meetings. Find out why **more than 100 million users** trust TeamViewer!

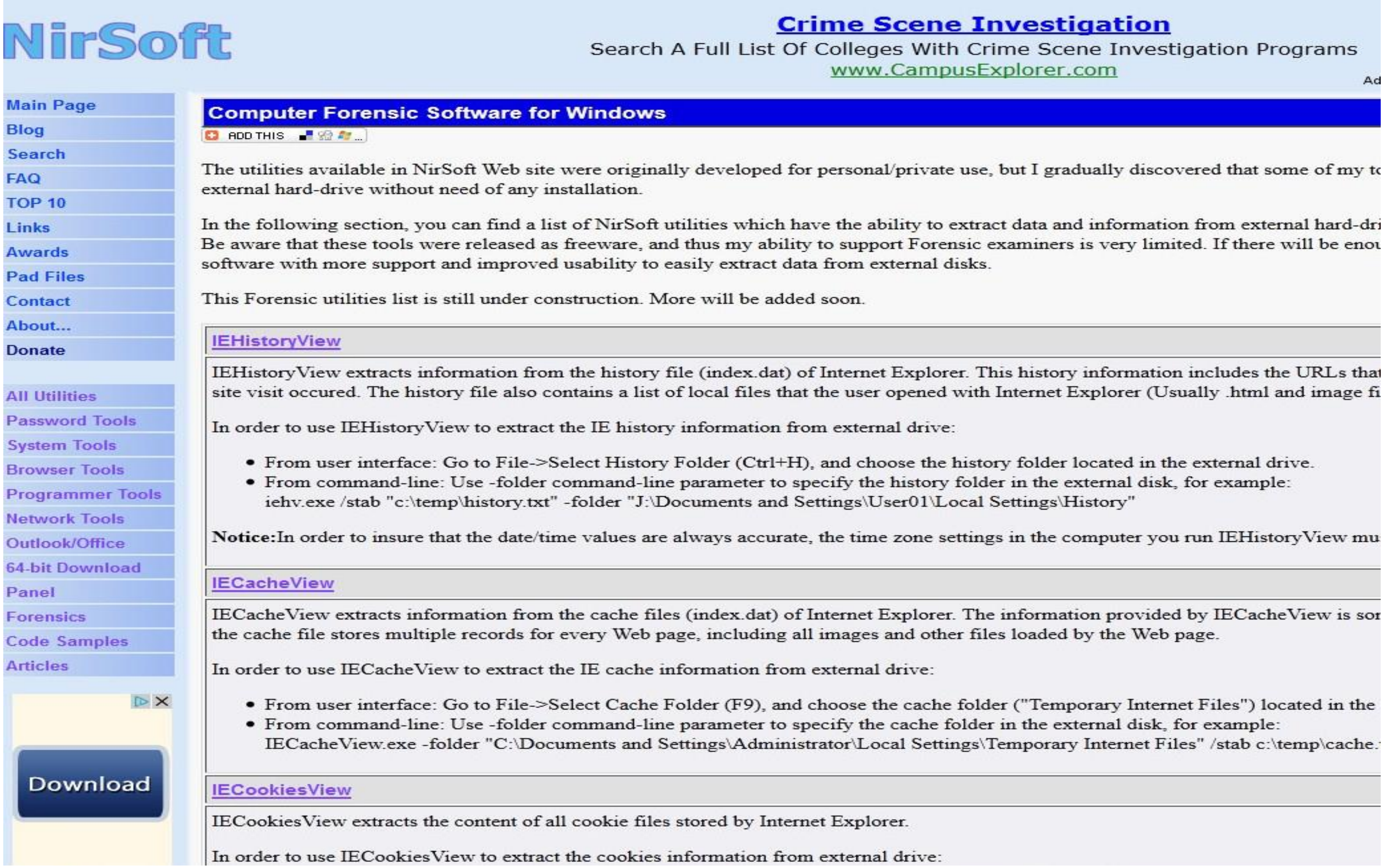
Remote Support and Remote Access

- **Remote Support** – no need for any installation on the client side
- **Remote Administration** – 24/7 access to remote computers and servers
- **Remote Access** – access your data and applications – anytime, anywhere
- **Home Office** – access your office computer from home

Online Meeting and Online Presentation

- **Online Meetings** – have up to 25 participants
- **Online Presentation** – boost your sales potential
- **Training Session** – cut costs by conducting training online
- **Online Teamwork** – collaborate online on documents in real-time

http://www.nirsoft.net



Computer Forensic Software for Windows

The utilities available in NirSoft Web site were originally developed for personal/private use, but I gradually discovered that some of my to
external hard-drive without need of any installation.

In the following section, you can find a list of NirSoft utilities which have the ability to extract data and information from external hard-dri
Be aware that these tools were released as freeware, and thus my ability to support Forensic examiners is very limited. If there will be enou
software with more support and improved usability to easily extract data from external disks.

This Forensic utilities list is still under construction. More will be added soon.

IEHistoryView

IEHistoryView extracts information from the history file (index.dat) of Internet Explorer. This history information includes the URLs that
site visit occured. The history file also contains a list of local files that the user opened with Internet Explorer (Usually .html and image fi

In order to use IEHistoryView to extract the IE history information from external drive:

- From user interface: Go to File->Select History Folder (Ctrl+H), and choose the history folder located in the external drive.
- From command-line: Use -folder command-line parameter to specify the history folder in the external disk, for example:
  iehv.exe /stab "c:\temp\history.txt" -folder "J:\Documents and Settings\User01\Local Settings\History"

Notice: In order to insure that the date/time values are always accurate, the time zone settings in the computer you run IEHistoryView mu

IECacheView

IECacheView extracts information from the cache files (index.dat) of Internet Explorer. The information provided by IECacheView is sor
the cache file stores multiple records for every Web page, including all images and other files loaded by the Web page.

In order to use IECacheView to extract the IE cache information from external drive:

- From user interface: Go to File->Select Cache Folder (F9), and choose the cache folder ("Temporary Internet Files") located in the
- From command-line: Use -folder command-line parameter to specify the cache folder in the external disk, for example:
  IECacheView.exe -folder "C:\Documents and Settings\Administrator\Local Settings\Temporary Internet Files" /stab c:\temp\cache.

IECookiesView

IECookiesView extracts the content of all cookie files stored by Internet Explorer.

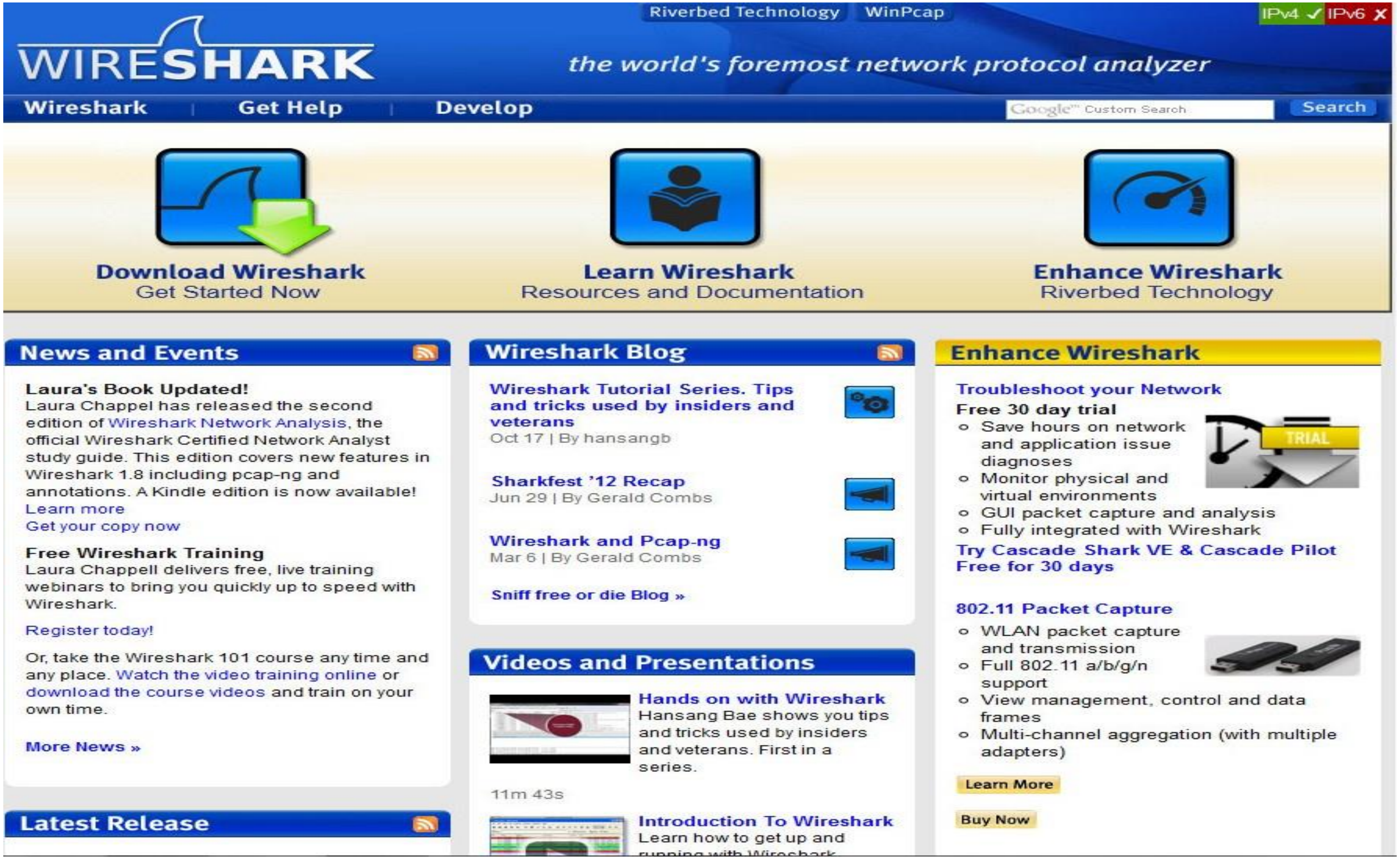
In order to use IECookiesView to extract the cookies information from external drive:

Book by Cory Altheide Harlan Carvey

SYNGRESS

DIGITAL FORENSICS WITH OPEN SOURCE TOOLS

http://www.wireshark.org



Riverbed Technology | WinPcap | IPv4 ✓ IPv6 ✗

WIRESHARK

the world's foremost network protocol analyzer

Wireshark | Get Help | Develop | Google™ Custom Search | Search

Download Wireshark
Get Started Now

Learn Wireshark
Resources and Documentation

Enhance Wireshark
Riverbed Technology

News and Events

Laura's Book Updated!
Laura Chappel has released the second edition of Wireshark Network Analysis, the official Wireshark Certified Network Analyst study guide. This edition covers new features in Wireshark 1.8 including pcap-ng and annotations. A Kindle edition is now available!
Learn more
Get your copy now

Free Wireshark Training
Laura Chappell delivers free, live training webinars to bring you quickly up to speed with Wireshark.

Register today!

Or, take the Wireshark 101 course any time and any place. Watch the video training online or download the course videos and train on your own time.

More News »

Latest Release

Wireshark Blog

Wireshark Tutorial Series. Tips and tricks used by insiders and veterans
Oct 17 | By hansangb

Sharkfest '12 Recap
Jun 29 | By Gerald Combs

Wireshark and Pcap-ng
Mar 6 | By Gerald Combs

Sniff free or die Blog »

Videos and Presentations

Hands on with Wireshark
Hansang Bae shows you tips and tricks used by insiders and veterans. First in a series.

11m 43s

Introduction To Wireshark
Learn how to get up and running with Wireshark

Enhance Wireshark

Troubleshoot your Network
Free 30 day trial
- Save hours on network and application issue diagnoses
- Monitor physical and virtual environments
- GUI packet capture and analysis
- Fully integrated with Wireshark

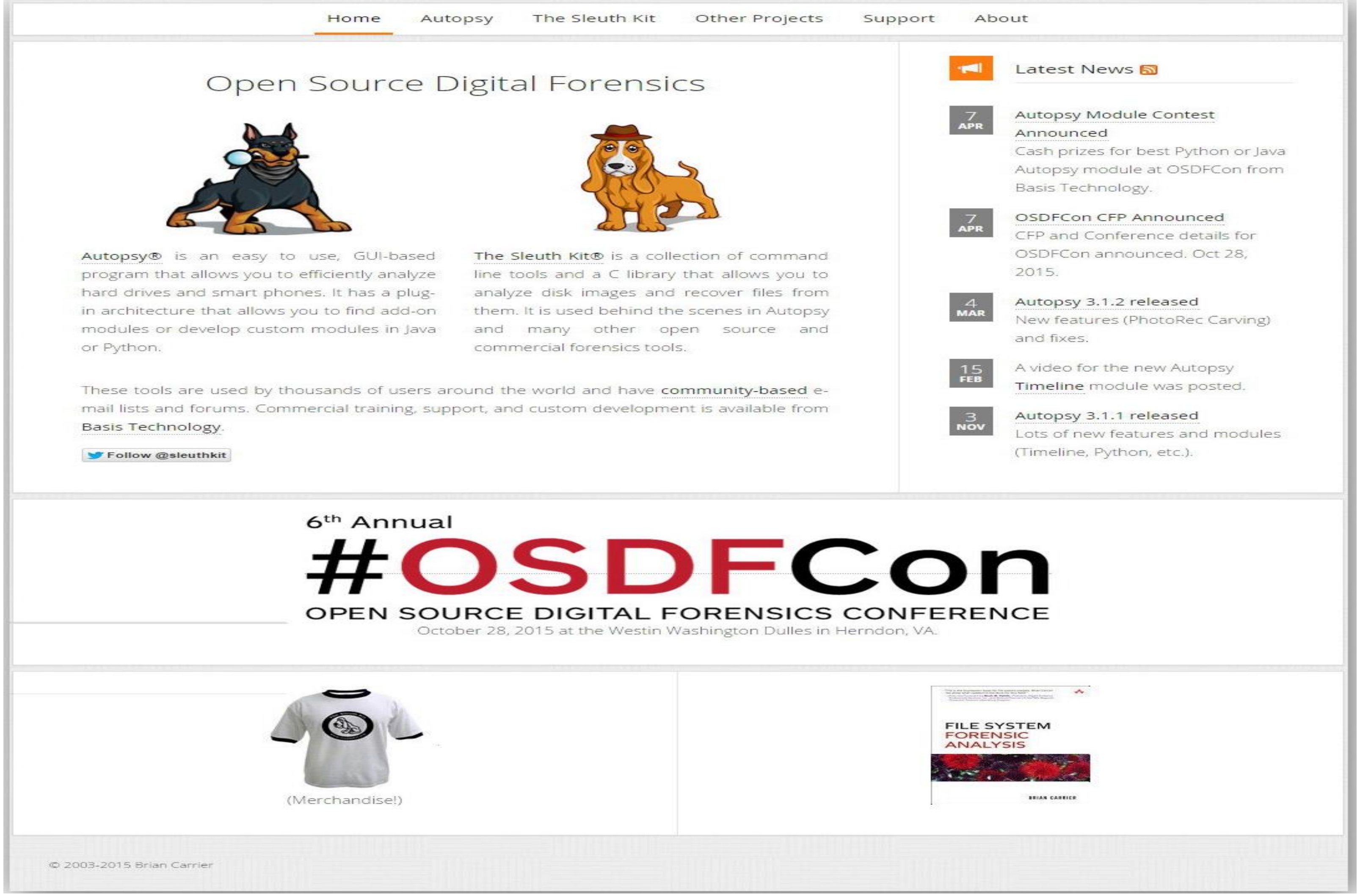
Try Cascade Shark VE & Cascade Pilot Free for 30 days

802.11 Packet Capture
- WLAN packet capture and transmission
- Full 802.11 a/b/g/n support
- View management, control and data frames
- Multi-channel aggregation (with multiple adapters)

Learn More

Buy Now

http://www.sleuthkit.org/autopsy/download.php



Open Source Digital Forensics

Autopsy® is an easy to use, GUI-based program that allows you to efficiently analyze hard drives and smart phones. It has a plug-in architecture that allows you to find add-on modules or develop custom modules in Java or Python.

The Sleuth Kit® is a collection of command line tools and a C library that allows you to analyze disk images and recover files from them. It is used behind the scenes in Autopsy and many other open source and commercial forensics tools.

These tools are used by thousands of users around the world and have community-based e-mail lists and forums. Commercial training, support, and custom development is available from Basis Technology.

Latest News

7 APR — Autopsy Module Contest Announced
Cash prizes for best Python or Java Autopsy module at OSDFCon from Basis Technology.

7 APR — OSDFCon CFP Announced
CFP and Conference details for OSDFCon announced. Oct 28, 2015.

4 MAR — Autopsy 3.1.2 released
New features (PhotoRec Carving) and fixes.

15 FEB — A video for the new Autopsy Timeline module was posted.

3 NOV — Autopsy 3.1.1 released
Lots of new features and modules (Timeline, Python, etc.).

6th Annual
#OSDFCon
OPEN SOURCE DIGITAL FORENSICS CONFERENCE
October 28, 2015 at the Westin Washington Dulles in Herndon, VA.

(Merchandise!)

© 2003-2015 Brian Carrier