

<http://viaforensics.com/computer-forensics/power-programming-forensics.html>

IPHONE BUG LETS USERS BYPASS LOCK SCREEN

<http://blog.intego.com/2010/10/26/iphone-bug-lets-users-bypass-lock-screen/>

SANS DF BLOG READER'S SURVEY RESULTS

https://blogs.sans.org/computer-forensics/2010/10/28/sans-digital-forensics-blog-readers-survey-results/?utm_source=rss&utm_medium=rss&utm_campaign=sans-digital-forensics-blog-readers-survey-results

SMARTPHONES HELPING DETECTIVES SOLVE CRIMES

<http://www.wgntv.com/videobeta/c00a7429-bafa-45ea-bd6e-49d0b8c9a085/News/Smartphones-helping-detectives-solve-crimes>

=====

LINKS

=====

Blogs

<http://www.forensicfocus.com/computer-forensics-blog>

<http://www.forensicblog.org>

<http://windowsir.blogspot.com>

<http://computer.forensikblog.de/en/>

<http://www.forensickb.com>

<http://www.forensicinnovations.com/blog>

<http://forensicsfromthesausagefactory.blogspot.com/>

<http://ericjhuber.blogspot.com/>

Podcasts

<http://cyberspeak.libsyn.com>

Wikis

<http://www.forensicswiki.org>

<http://www.forensicwiki.com>

=====

TOOLS

=====

APF - ADROID PHOTO FORENSICS

APF hailed as a digital forensics breakthrough for its SmartCarving and SmartFiltering Tech, can accelerate your photo investigations with extraction/grouping of EXIF meta-data, timeline, reporting, etc. APF supports explicit image detection, child face detection, thumbnail mismatch detection, fuzzy hashing and much more.

<http://digital-assembly.com/apff/>

analyzeMFT - a Python tool to deconstruct the Windows NTFS \$MFT file Changelog Version 1.5:

Fixed date/time reporting. I wasn't reporting useconds at all.

Added anomaly detection. Adds two columns:

- std-fn-shift: If Y, entry's FN create time is after the STD create time

- usec-zero: If Y, entry's STD create time's usec value is zero

<http://www.integrigraphy.com/>

CLEARWELL EXTENDS E-DISCOVERY PLATFORM

Clearwell Systems, Inc. has announced the release of its Identification and Collection Module. Available with version 6.0 of the Clearwell E-Discovery Platform, the new module enables IT teams to easily identify and collect electronically stored information (ESI) while maintaining data integrity and chain of custody. The data can then seamlessly be made available to legal teams for early case assessment (ECA), review and production...

<http://www.forensicfocus.com/index.php?name=News&file=article&sid=1556>

RADIO TACTICS BRINGS DATA EXTRACTION TO THE FRONTLINE WITH LAUNCH OF ACESO FIELD

Radio Tactics Ltd, a specialist innovator of high-tech digital intelligence and evidence gathering solutions has today launched Aceso Field, a portable solution for extracting evidentially sound data from mobile digital devices, SIM and media cards. Aceso Field is a truly portable solution, giving officers on the front line instant access to all the benefits of Aceso, which has until now been an office based tool...

<http://www.forensicfocus.com/index.php?name=News&file=article&sid=1557>

DIGITAL FORENSICS FRAMEWORK

ArxSys team is proud to announce the release of Digital Forensics Framework version 0.8. DFF is an Open Source environment of analysis and development dedicated to computer forensics.

This release adds several features such as NTFS and Ext2/3/4 support. New attributes handling, better look and feel and so on...

Have a look at www.digital-forensic.org, it's Open Source, free, cross-platform

and documented ! Feedbacks are welcome.

=====
PAPERS
=====

My ERP got hacked, an Introduction to Computer Forensics - Part I
by Ismael Valenzuela

The System Administrator knew something was wrong when he saw there was an additional user account on the Web-based Enterprise Resource Planning (ERP) system that he administered. He kept the system updated and patched, but he now suspects that the system has been hacked and compromised. Now, as a computer forensic investigator, you will have to find out if there was any unauthorized access, how it happened and what was the extent of the damage...

Read more at http://blog.ismaelvalenzuela.com/wp-content/uploads/2009/11/my_erp_get_hacked_1.pdf (Note: external PDF)

=====
FORMAZIONE
=====

INNOVAZIONI SCIENTIFICHE E PROCESSO PENALE

Firenze, 11 novembre 2010

[http://www.fondazioneforensifirenze.it/images/content/files/2010/2010-2/2010.11.11%20Innovazioni%20scient.%20e%20proc.%20pen.%20\(UNIFI\)/programma-innovazioni_e_processo_penale_11.11.2010.pdf](http://www.fondazioneforensifirenze.it/images/content/files/2010/2010-2/2010.11.11%20Innovazioni%20scient.%20e%20proc.%20pen.%20(UNIFI)/programma-innovazioni_e_processo_penale_11.11.2010.pdf)

SEMINARIO IISFA, 26 NOVEMBRE 2010

Cassa Nazionale Forense - Sala Conferenze - Roma

- "Cloud computing: aspetti di security e digital forensics"

Ing. Andrea Rota

Researcher al CEFRIEL · ICT Institute - Politecnico di Milano

- Phishing - Analisi tecnica di un "web kit"

M.llo Luigi Ranzato, responsabile tecnico del Centro Intercettazioni della

Procura della Repubblica di Trento

[http://iisfa.net/index.php?view=details&id=54%3ACloud+computing
+&digital_forensics_-_Phishing_analisy=&option=com_eventlist&Itemid=63](http://iisfa.net/index.php?view=details&id=54%3ACloud+computing+%amp;digital_forensics_-_Phishing_analisy=&option=com_eventlist&Itemid=63)

1° CORSO DI PERFEZIONAMENTO IN CYBERCRIMINOLOGIA

Fondazione per il Centro Studi Città di Orvieto

Novembre 2010 - Febbraio 2011

Il corso prenderà in considerazione le principali tecnologie e acquisizioni teoriche in ambito investigativo e nel campo della criminologia della sicurezza logica. Un primo modulo di lezioni - 40 ore circa - tratterà i concetti di offender e geographic profiling, crime scene analysis, tossicologia e balistica forense oltreché i principali apporti teorici nell'ambito della criminologia e delle scienze criminologico-forensi. Un secondo modulo di altre 40 ore prenderà invece in considerazione il tema della IT Security e della business security oltre che delle nuove minacce di oggi.

=====
CONFERENCES & CFP
=====

SANS What Works in Digital Forensics and Incident Response Summit
7-8 Giugno 2011

Omni Hotel, Austin, Texas.

Iscrizioni aperte. Iscrivendosi entro il 31 Dicembre 2010 (usando il codice FOR2011) è possibile ottenere un ulteriore sconto del 15%. Per ulteriori info visitare <https://www.sans.org/forensics-incident-response-summit-2011>

DIGITAL FORENSICS RESEARCH CONFERENCE 2011 CALL FOR PAPERS

The 11th Annual DFRWS Conference will be held in New Orleans, LA from August 1 to 3, 2011.

The annual DFRWS conference allows leading digital forensics researchers from government, industry, and academia to present their work and results to fellow researchers and practitioners. Many of the most cited digital forensics papers have been presented at DFRWS and the annual challenge has spawned research in important areas. Initial results and tool prototypes are also presented during the Works in Progress and demo sessions.

The conference typically has about 100 people and is therefore small enough so that attendees meet each other and can interact with the speakers. A tradition of DFRWS as been its casual and interactive atmosphere where break out sessions exist to discuss topics related to the presentations. There are also opportunities to interact during the welcome reception and banquet. After the banquet, attendees can put their forensics skills to the test when they form teams to participate in the annual Forensics Rodeo, which is a challenge that requires participants to analyze data and answer questions.

Topics of Interest:

- * Incident response and live analysis
- * Network-based forensics, including network traffic analysis, traceback and attribution
- * Event reconstruction methods and tools
- * File system and memory analysis
- * Application analysis
- * Embedded systems
- * Small scale and mobile devices
- * Large-scale investigations
- * Digital evidence storage and preservation
- * Data mining and information discovery
- * Data hiding and recovery
- * Data extraction and reconstruction
- * Multimedia analysis
- * Database forensics
- * Tool testing and development
- * Digital evidence and the law
- * Anti-forensics and anti-anti-forensics
- * Case studies and trend reports
- * Malware forensics
- * Data visualization in forensic analysis
- * Forensics of virtual and cloud environments
- * Investigation of insider attacks
- * Error rates of forensic methods
- * Interpersonal communications and social network analysis
- * Non-traditional approaches to forensic analysis

Important Dates

- * Submission deadline: February 27, 2011 (any time zone)
- * Author notification: April 4, 2011
- * Final draft due: April 25, 2011
- * Pre-conference Workshops: July 31, 2011
- * Conference dates: August 1-3, 2011

<http://www.dfrws.org/2011/>