CEIC 2013

May 19 – 22

CEIC 2013

- CEIC(Computer and Enterprise Investigations Conference)
- Location
  - Rosen Shingle Creek in Orlando
- Date
  - May 19 – 22

http://media-cdn.tripadvisor.com/media/photo-o/02/41/20/f8/resort-front.jpg

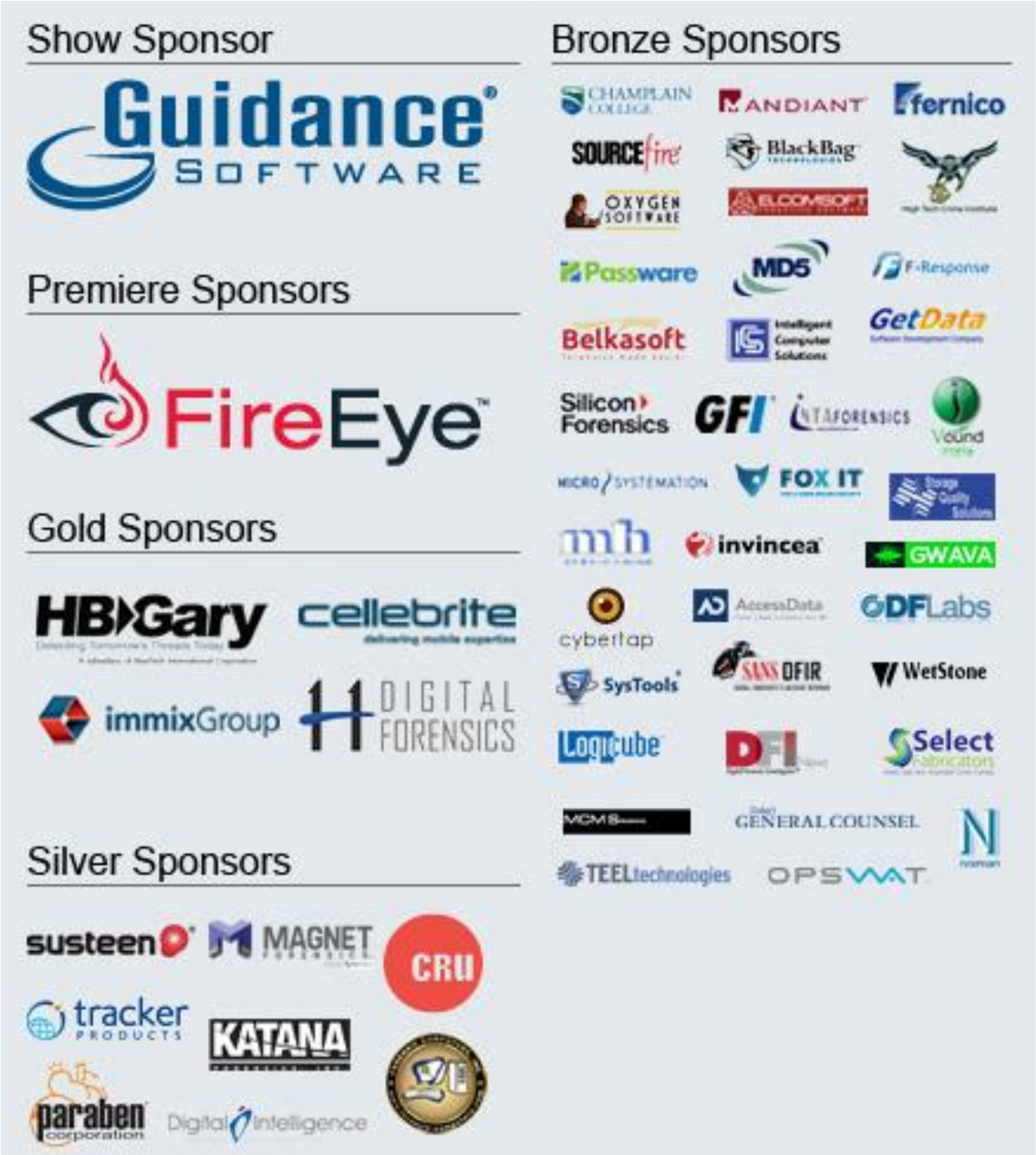
Top Reasons to Attend

- Learn best practice methods and new techniques that you can implement immediately
- Network with peers, experts and professionals
- **Gain EnCE® or EnCEP™ certification: Take the exam at no additional cost ($150- $200 value)**
- Stay certified: Fulfill your entire EnCE® recertification requirement at CEIC
- Earn CLE and/or CPE credits
- Save money: The low fee includes all learning sessions, keynote, Exhibit Hall, social networking events and meals during conference hours
- **Meet with 30+ industry vendors/suppliers to discover the latest technology**
- Learn from a distinguished keynote speaker
- Discuss hot topics with colleagues in focused Birds-of-a-Feather events
- Receive training on key products such as EnCase®

INTRO

http://www.ceicconference.com/sponsor.htm#tab=2

SPONSOR



Show Sponsor

Premiere Sponsors

Gold Sponsors

Silver Sponsors

Bronze Sponsors

http://www.ceicconference.com/sponsor.htm#tab=2

EnCase & FireEye

- Premiere Sponsor is only FireEye.

http://1.bp.blogspot.com/-Yv7dmxn4qNU/UZo48Frl-zI/AAAAAAAAAgg/KgirD1H_SqU/s320/Victor.jpg

ATMOSPHERE

CEIC 2013 GENERAL REGISTRATION
CEIC 2013 GENERAL REGISTRATION
CEIC 2013 GENERAL REGISTRATION
CEIC 2013 SPONSOR REGISTRATION

http://3.bp.blogspot.com/-sHQWhh636Ho/UZo1RhJ2QFI/AAAAAAAAAf0/EDkpQnEL3aw/s1600/photo.jpg

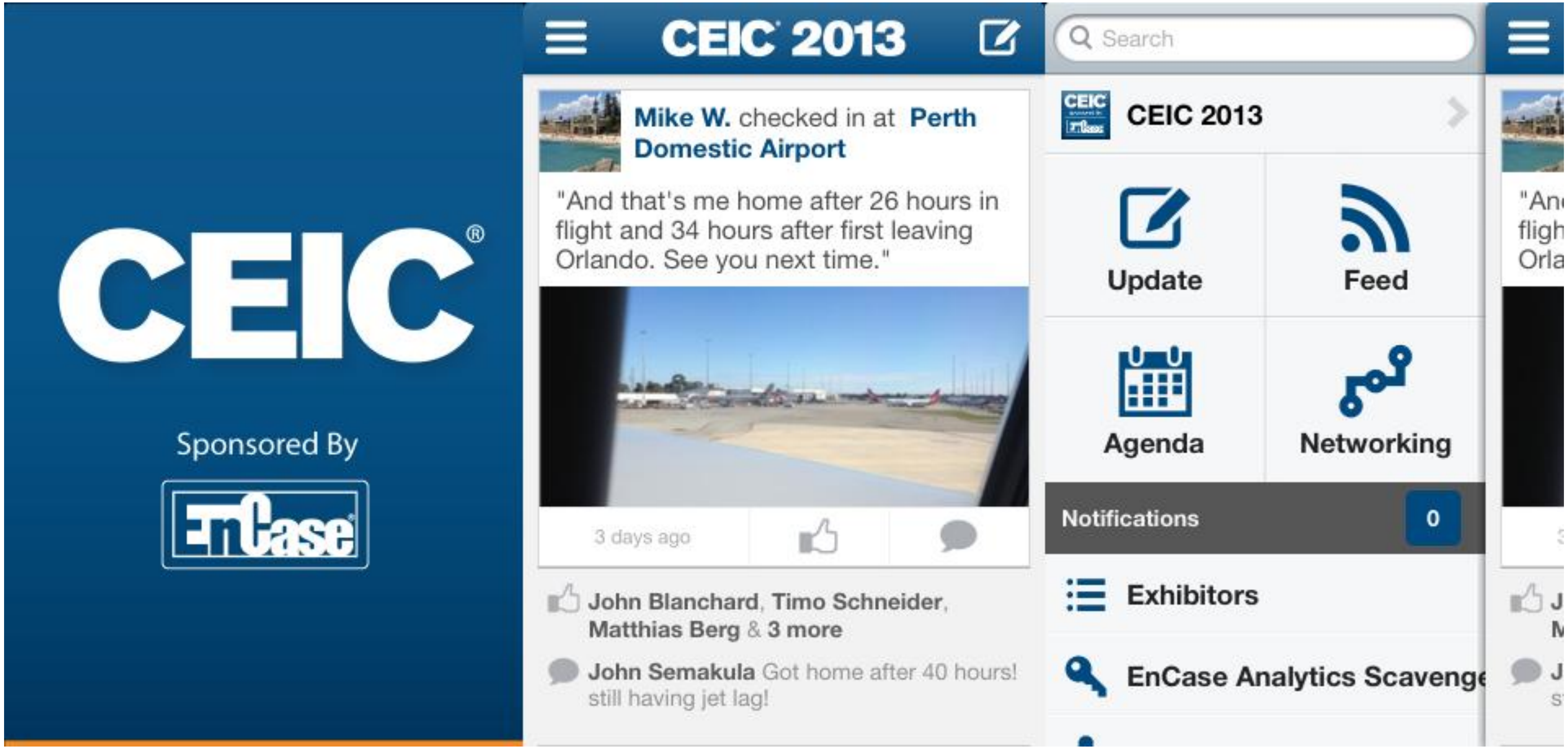
CEIC Caption Contest

- Attendance at CEIC is not required to participate so join in!
- Winner for iPad will be announced june 10, 2013.

H-ACME
Guidance SOFTWARE
CEIC 2013 CAPTION CONTEST
ENCASE.COM

http://1.bp.blogspot.com/-qfIMn6ZNeZw/UZj4QjrruQI/AAAAAAAAAfg/L4MerHT1u-4/s1600/Guidance.lowresB.caption.jpg

CEIC App



Mike W. checked in at Perth Domestic Airport

"And that's me home after 26 hours in flight and 34 hours after first leaving Orlando. See you next time."

3 days ago

John Blanchard, Timo Schneider, Matthias Berg & 3 more

John Semakula Got home after 40 hours! still having jet lag!

KEYNOTE

- Agenda
  - Link : http://www.ceicconference.com/agenda/full-schedule.htm
- Red marks are what I attended.

KEYNOTE – 5/19/2013

- EnCE Last Minute Review
- Tips and Tricks from Guidance Software Tech Support
- Postmortem Forensics In A Phishing Attack
- Hunting for Unfriendly Easter Eggs
- Living Dangerously - Malware Analysis
- TAR - What is Fiction and What is Real?
- EnCEP Review
- Simple Data Assessments
- Leveraging Endpoint Data to Solve Big Business Problems with EnCase Analytics
- Investigation on Kindle Fire

KEYNOTE – 5/20/2013

- Proactive Forensic Test Methodology
- NTFS Logfile Forensics
- Raw Data Carving
- How To Layer Threat Intelligence Into Your Enterprise Environment
- Cybersecurity 101
- E-Discovery best practices and avoiding common mistakes
- Planning for Your Next In-House eDiscovery Case
- Corporate eDiscovery Best Practices using EnCase Enterprise and EnCase eDiscover
- Achieving Compliance: Sensitive Data Discovery and Policy Enforcement with EnCase Cybersecurity
- Evidence in the Cloud - Business Use of Online Services

KEYNOTE – 5/20/2013

- Writing Expert Reports and Defending them in Court
- Examining Volume Shadow Copies - The Easy Way
- UEFI, MBR, and GPT oh my!
- Responding to a Cyber Security Incident
- How to Configure and Use SQL with EnCase Products
- E-Discovery Case Law: Tips on Avoiding These Real Live Discovery Disasters
- Mitigating EDRM Left Side Risks and Lessons Learned – Understanding ESI & IT Infrastructure
- EnCase Enterprise and VMware: An Agile Platform for Malware Detection and Tracking
- Incident Response and Credit Card Fraud Investigations
- The Technical Challenges of Bring Your Own Device (BYOD)

KEYNOTE – 5/20/2013

- Computer Forensics and Testimony
- EnCase App Central: Stake your claim!
- Following an Intrusion Through a Microsoft Network
- You can panic now - A DFIR Look at APT-based Attack
- Incident Response 2.0 - Rapid Triage, Containment, and Remediation with FireAmp and EnCase
- Successful Deposition Tactics and Strategies: So you are now part of the Litigation or Regulatory Discovery and You Have Been Deposed, Now What?
- Data Encryption and eDiscovery Collection and Processing
- Successful eDiscovery in a Bring-Your-Own-Device Environment
- Using the Legal Hold Functionality of EnCase eDiscovery to Assist in Compliance and Acknowledgements
- Artifacts of Webmail Usage

KEYNOTE – 5/20/2013

- Risky Business - Starting/Running your own forensics practices
- Correlating forensic results from multiple operating systems
- Offensive Digital Forensics
- How the World will End: The Spy is in the Cybersphere
- Using EnCase Analytics to Identify Connections Between Seemingly Unrelated Data to Expose a Breach
- E-Discovery Collaboration – the Interplay between In-House Counsel, IT and Out
- How to Configure and Use SQL with EnCase Products
- Distributed collection techniques - reduce travel by leveraging VMs
- The 2013 Verizon Data Breach Investigation Report
- Logical vs. Physical Acquisition on Mobile Devices

KEYNOTE – 5/21/2013

- Expert Witness--Preparing to Qualify and Testify
- Custom Analysis with EnCase v7
- New Forensic Highlights of Windows 8
- Developing a Capability-Driven IR Program
- Managing Cross Border and International Regulatory Inquiries. Examination of the Issues of International E-Discovery and Best Practices
- Connectors Tips & Tricks
- Integrating Encase CyberSecurity and 3rd Party Incident Response Tools to Arcsight and other SIEM Tools
- Recognizing the Critical Role of Legal for an Effective Compliance and Ethics Program
- Using Cloud Computing in Computer Forensics & Electronic Discovery

KEYNOTE – 5/21/2013

- Optimizing your System for Superior EnCase Forensic Version 7 Performance
- Protected File Analysis in Practice Using EnCase with Passware
- Advanced Reporting
- How CISOs and General Counsels are Quickly Becoming Best Friends
- Compliance Auditing with EnCase Cybersecurity
- Judicial Perspectives on Current Case Law that Influences E-Discovery
- Mastering EnCase Criteria
- EnCase eDiscovery Processing Workflow
- The Impact of the EU Data Protection Reform on Cross-Border E-Discovery
- Legal Ramifications of BYOD

KEYNOTE – 5/21/2013

- Performing Field Triage and Data Collection with EnCase Portable
- Extending EnCase Forensic 7: Modules and Extensions
- Mac OSX - Delving a Little Deeper
- Exploring the data models of EnCase Analytics
- Building an Integrated Response Capability w/EnCase Cybersecurity
- Building a Scalable E-Discovery Process to Fit Your Organizations Needs
- The Art and Science of Creating EnCase eDiscovery Keywords and Index Querie
- Tips and Tools for using EnCase for Audits and Investigations
- The "Trusted" Insider: Investigating Intellectual Property Theft
- Social Media and Cloud Computing Artifacts on Smart Phones and Tablets

KEYNOTE – 5/21/2013

- Converting E01 Files to a Working VM and Pulling Out Useful…
- SSD Forensics
- NetWars
- Speed Up Your IR Investigations with IOC's from FireEye
- Network Forensic Investigations of Hacking Incidents
- Effective information management and cost effective e-discovery Processes
- Load Files and Production
- Modular EnScript Code Design to simplify validation and code Sharing
- Information Security Risk Assessments
- Getting the Evidence when the Evidence is in Pieces: Damaged Mobile Devices

KEYNOTE – 5/22/2013

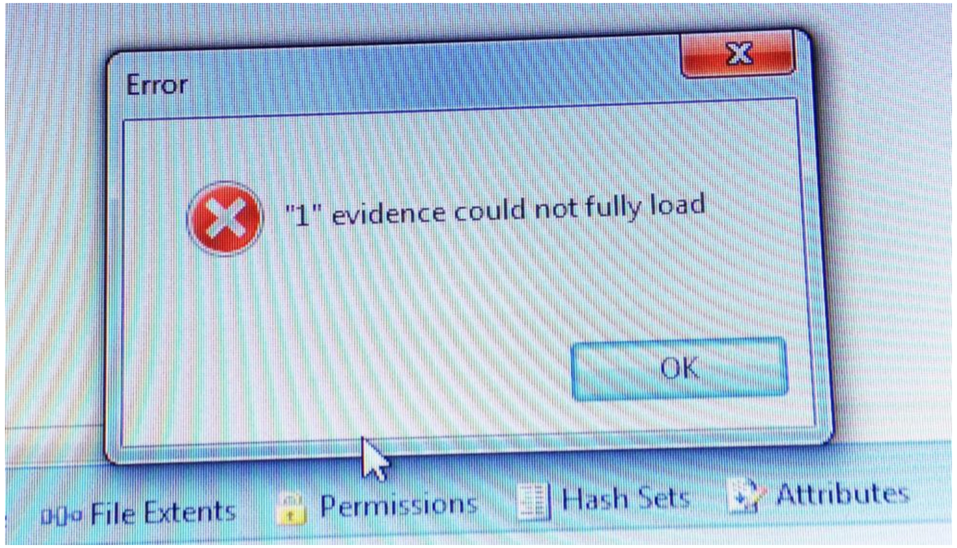
- N-Gram Analysis in Suspect Author Identification of Anonymous E-mail
- Making the most of EnCase Processor
- eDiscovery Future
- Quality Control Perspectives in EnCase E-Discovery
- Using Random Sampling to Reduce your Backlog
- Whistleblower and Fraud Investigations
- Vehicle System Forensics

KEYNOTE – 5/22/2013

- Future of EnCase
- Enterprise-Scale Linux Memory Forensics
- Memory Forensics
- Shaking up the Security Stack: The Future of EnCase Cybersecurity
- When Macs get Hacked
- E-Discovery Done Right
- Cloud-Based ECA and Review for Production
- EnCase Phone Acquisitions

INTERVIEW

- Jetco
  - Price Policy : Maintenance for technical support
- Guidance Software
  - Can't change the name of E01 images. Although Ex01 can be changed.
  - Unload images after case processor



Error

"1" evidence could not fully load

INTERESTING

http://www.logicube.com/shop/images/375/falcon-sla-i17-221.jpg

- Logicube
  - Forensic Falcon
  - Ex01, E01
  - USB 3.0, Firewire, SAS/SATA, Gigabit Ethernet
  - Maximum Speed : 20GB/min (SSD) / Basically 11GB/min
  - http://www.logicube.com/shop/falcon/
- EDCE
  - Eclipse
  - Manual screen capture kit

http://edecdf.com/products?iProdId=2

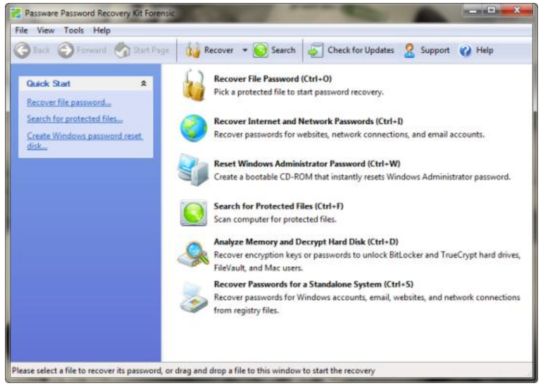
TENDENCY

- Network Forensic
  - Cybertap Recon
- Archive Disk
  - Storageqs
- Forensic System
  - Silicon Forensics, Digital Intelligence
- Password
  - Elcomsoft, Passware

http://www.jesc.co.za/images/products/Digital-Intelligence.jpg

http://news.cnet.com/i/bto/20070917/fred_350x345.jpg

http://elcomsoft.com/CATALOG/elcomsoft_2013_en.pdf



Recover file password...

Search for protected files...

Create Windows password reset disk...

Recover File Password (Ctrl+O)
Pick a protected file to start password recovery.

Recover Internet and Network Passwords (Ctrl+I)
Recover passwords for websites, network connections, and email accounts.

Reset Windows Administrator Password (Ctrl+W)
Create a bootable CD-ROM that instantly resets Windows Administrator password.

Search for Protected Files (Ctrl+F)
Scan computer for protected files.

Analyze Memory and Decrypt Hard Disk (Ctrl+D)
Recover encryption keys or passwords to unlock BitLocker and TrueCrypt hard drives, FileVault, and Mac users.

Recover Passwords for a Standalone System (Ctrl+S)
Recover passwords for Windows accounts, email, websites, and network connections from registry files.

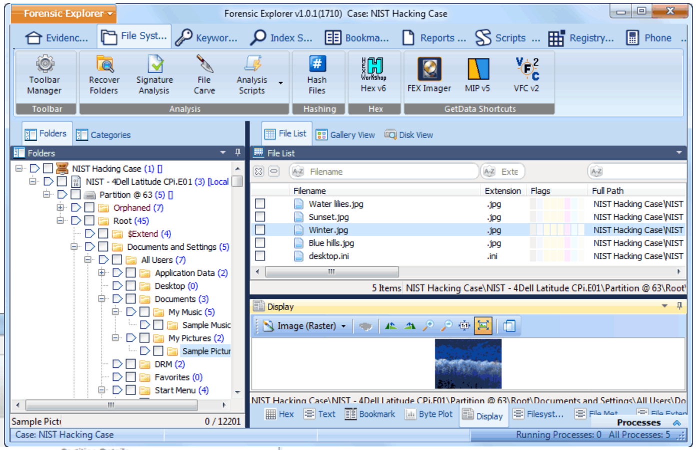
Please select a file to recover its password, or drag and drop a file to this window to start the recovery

http://www.lostpassword.com/images/pictures/screenshots/kit_for_start_page.png

http://siliconforensics.com/images/Product/medium/131.jpg

TENDENCY

- So many softwares work like User Friendly.
  - Belkasoft, FTK, SysTools, DFLabs, GetData, Magnet
- Related Search
  - Intella


Forensic Explorer
Forensic Explorer v1.0.1(1710) Case: NIST Hacking Case
Evidenc... File Syst... Keywor... Index S... Bookma... Reports ... Scripts ... Registry... Phone
Toolbar Manager
Recover Folders
Signature Analysis
File Carve
Analysis Scripts
Hash Files
Hex v6
FEX Imager
MIP v5
VFC v2
Folders Categories
File List Gallery View Disk View
Display
Image (Raster)

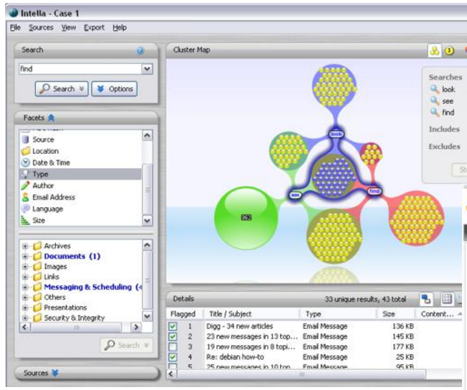
Filename	Extension	Flags	Full Path
Water lilies.jpg	.jpg		NIST Hacking Case\NIST
Sunset.jpg	.jpg		NIST Hacking Case\NIST
Winter.jpg	.jpg		NIST Hacking Case\NIST
Blue hills.jpg	.jpg		NIST Hacking Case\NIST
desktop.ini	.ini		NIST Hacking Case\NIST

http://www.forensicexplorer.com/img/scr_FE/file-system.png

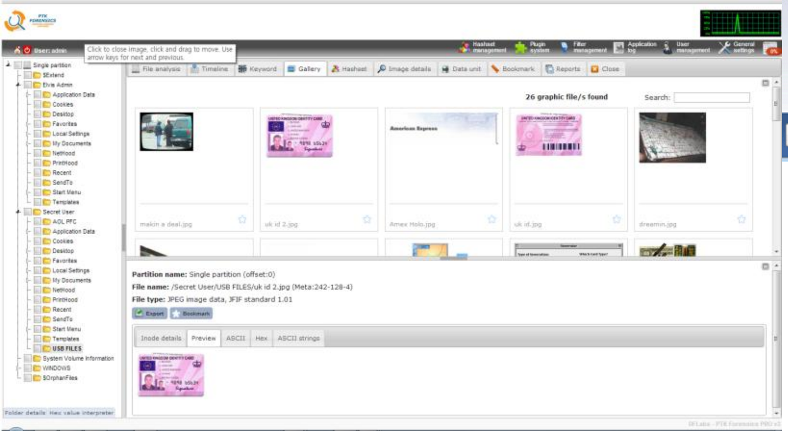
SysTools Hard Drive Data Recovery 3.2 - Demo Version
File Help
SYSTOOLS SOFTWARE
Hard Drive Data Recovery
DATA RECOVERY SOFTWARE TO RECOVER HARD DRIVE DATA
Home Activate Buy Support Exit
Available Partition(s)
Hard-Drive Disk 0
(C:) (D:) (E:) (F:) (G:)

Partition Details
Model ST3500418AS ATA De
DiskNumber Hard-Drive Disk 0
Name C
Type NTFS Partition
TotalSize 87 GB
FreeSize 68 GB

http://www.systoolsgroup.com/images/screenshots/large/hard-drive-data-recovery.gif

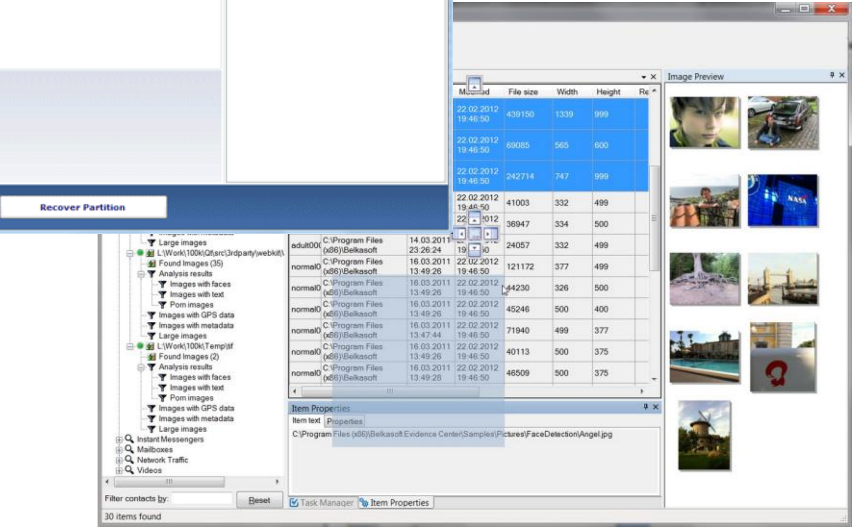


http://www.mh-service.de/uploads/pics/Intella1_2_1-screen_03.png


File analysis Timeline Keyword Gallery Hashset Image details Data unit Bookmark Reports Close
26 graphic file/s found
Search:
Inode details Preview ASCII Hex ASCII strings

Partition name: Single partition (offset:0)
File name: /Secret User/USB FILES/uk id 2.jpg (Meta:242-128-4)
File type: JPEG image data, JFIF standard 1.01

http://ptk.dflabs.com/img/Cattura8.PNG



http://www.softsia.com/screenshots/Belkasoft-Evidence-Center_zgwr.jpg http://katanaforensics.com/wp-content/uploads/2013/01/Lantern-3-vertical_box_400.png

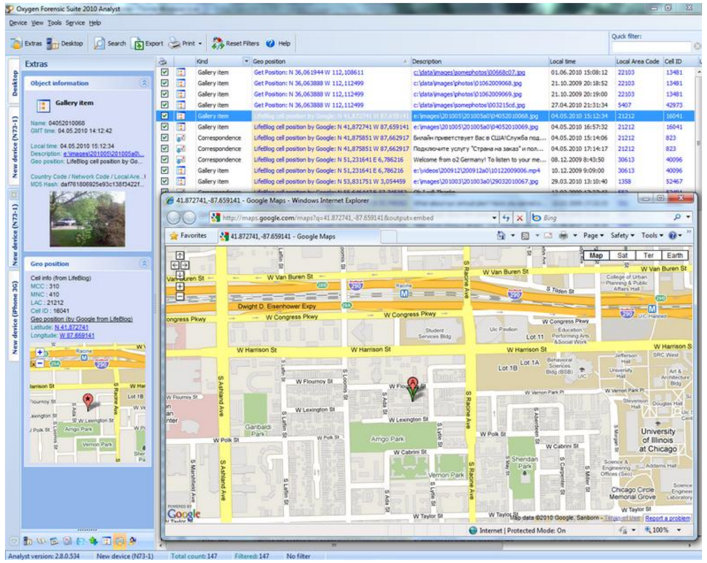
http://forensicstore.com/wpfs/wp-content/uploads/2012/09/paraben-mobile-field-kit.png

TENDENCY

- MAC
  - KATANA, BlackBag
- Cell phone
  - KATANA, BlackBag, Cellebrite
  - Oxygen Forensic, Susteen
- Memory
  - HB-Gary
- EnScript
  - WetStone

KATANA
LANTERN 3
Image. Analyze. Report.
The best in iOS Forensics has gotten even better.
Support for more devices than ever.
iOS
OSX
Android
+
LANTERN 3

http://legacy.oxygen-forensic.com/images/screenshots2//images/lifeblog/LifeBlog3.png


Oxygen Forensic Suite 2010 Analyst
Device View Tools Service Help
Extras Desktop Search Export Print Reset Filters Help
Quick filter:
Extras
Desktop
New device (N73-1)
Object information
Geo position
41.872741,-87.659141 - Google Maps - Windows Internet Explorer
Favorites
Page Safety Tools
Map Sat Ter Earth
Internet | Protected Mode: On
100%

Gallery item

Name: 04052010068
GMT time: 04.05.2010 14:12:42

Local time: 04.05.2010 15:12:34
Description: e:\images\201005\201005a0\...
Geo position: LifeBlog cell position by Go...

Country Code / Network Code / Local Are...
MD5 Hash: daf761806925e93c138f3422f...

Kind	Geo position	Description	Local time	Local Area Code	Cell ID
Gallery item	Get Position: N 36,061944 W 112,108611	c:\data\images\somephotos\00668c07.jpg	01.06.2010 15:08:12	22103	13481
Gallery item	Get Position: N 36,063888 W 112,112499	c:\data\images\photos\01062009068.jpg	21.10.2009 20:18:52	22103	13481
Gallery item	Get Position: N 36,063888 W 112,112499	c:\data\images\photos\01062009069.jpg	21.10.2009 20:19:00	22103	13481
Gallery item	Get Position: N 36,063888 W 112,112499	c:\data\images\somephotos\003215cd.jpg	27.04.2010 21:31:34	5407	42973
Gallery item	LifeBlog cell position by Google: N 41,872741 W 87,659141	e:\images\201005\201005a0\04052010068.jpg	04.05.2010 15:12:34	21212	16041
Gallery item	LifeBlog cell position by Google: N 41,872741 W 87,659141	e:\images\201005\201005a0\04052010069.jpg	04.05.2010 16:57:32	21212	16041
Correspondence	LifeBlog cell position by Google: N 41,875851 W 87,662917	Билайн приветствует Вас в США!Служба под...	04.05.2010 15:14:06	21212	823
Correspondence	LifeBlog cell position by Google: N 41,875851 W 87,662917	Подключите услугу "Страна на заказ" и пол...	04.05.2010 17:14:17	21212	823
Correspondence	LifeBlog cell position by Google: N 51,231641 E 6,786216	Welcome from o2 Germany! To listen to your me...	08.12.2009 8:43:50	30613	40096
Gallery item	LifeBlog cell position by Google: N 51,231641 E 6,786216	e:\videos\200912\200912a0\10122009006.mp4	10.12.2009 9:09:00	30613	40096
Gallery item	LifeBlog cell position by Google: N 53,831751 W 3,054459	e:\images\201003\201003a0\29032010067.jpg	29.03.2010 13:10:40	1358	52467

http://maps.google.com/maps?q=41.872741,-87.659141&output=embed

Analyst version: 2.8.0.534 New device (N73-1) Total count: 147 Filtered: 147 No filter

C-TAK
Cyber Threat Analytics Knowledgebase
C-TAK EnScript | Threat Level
Threat Level
CLEAN
AT RISK
COMPROMISED

http://wetstonetech.com/images/threatL2.png

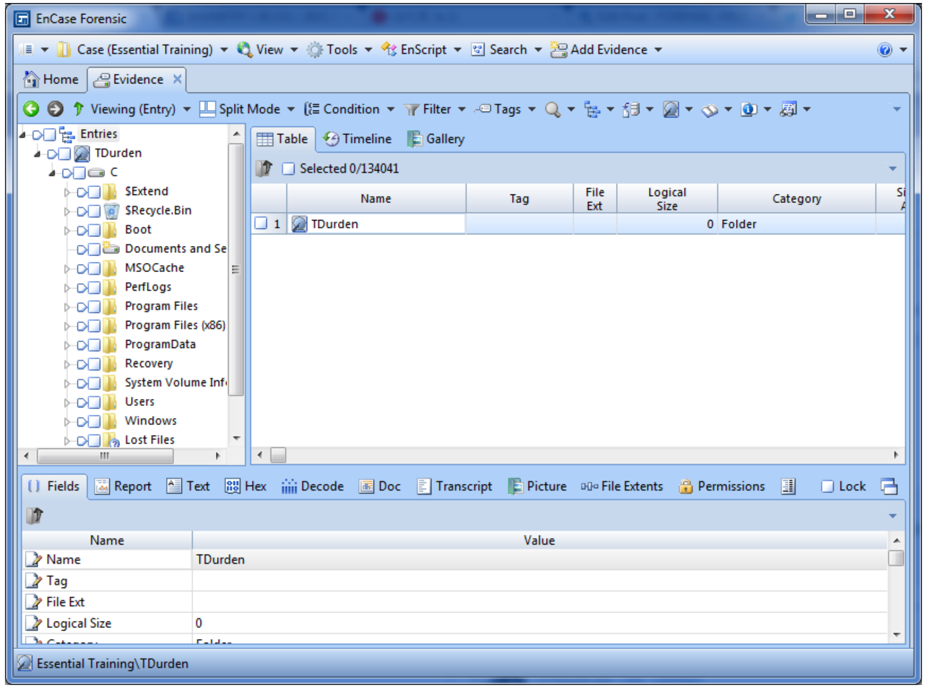
http://d20dobnekmqy0v.cloudfront.net/images/stories/ufedtouch/1-UFED-Touch-Ultimate-2.jpg

EnCase – Basic Function

- Various File Systems
- Mobile Analyze
- Making Reports handily
- Data Index
- Search something by pattern

………….

http://www.bounga.co.id/sites/www.bounga.co.id/files/encase-forensic-7-200px.png



	Name	Tag	File Ext	Logical Size	Category
1	TDurden			0	Folder

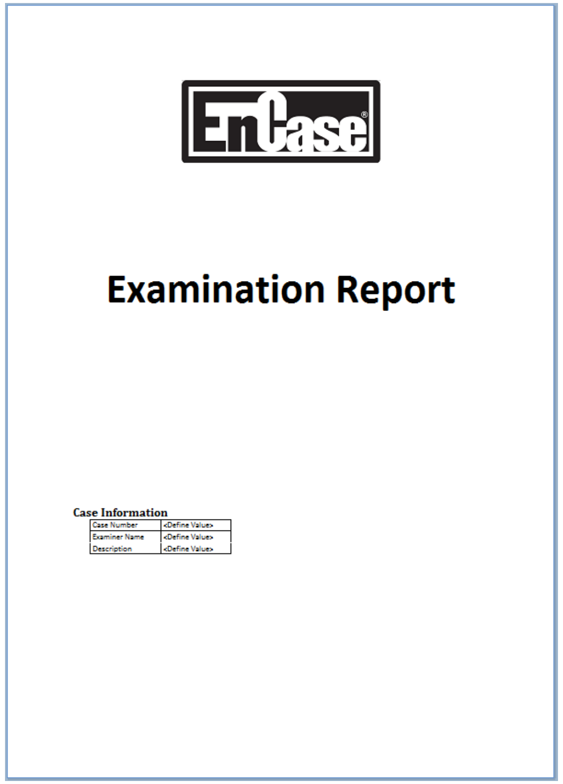
Name	Value
Name	TDurden
Tag	
File Ext	
Logical Size	0

http://forensic-proof.com/wp-content/uploads/2011/08/encasev7_main.png

EnCase – Additional Function

- Extentsion Modules
  - Plist Parser
  - $Attribute Parser
  - FireEye Log Viewer
  - Making the Form of Report

…………



EnCase®

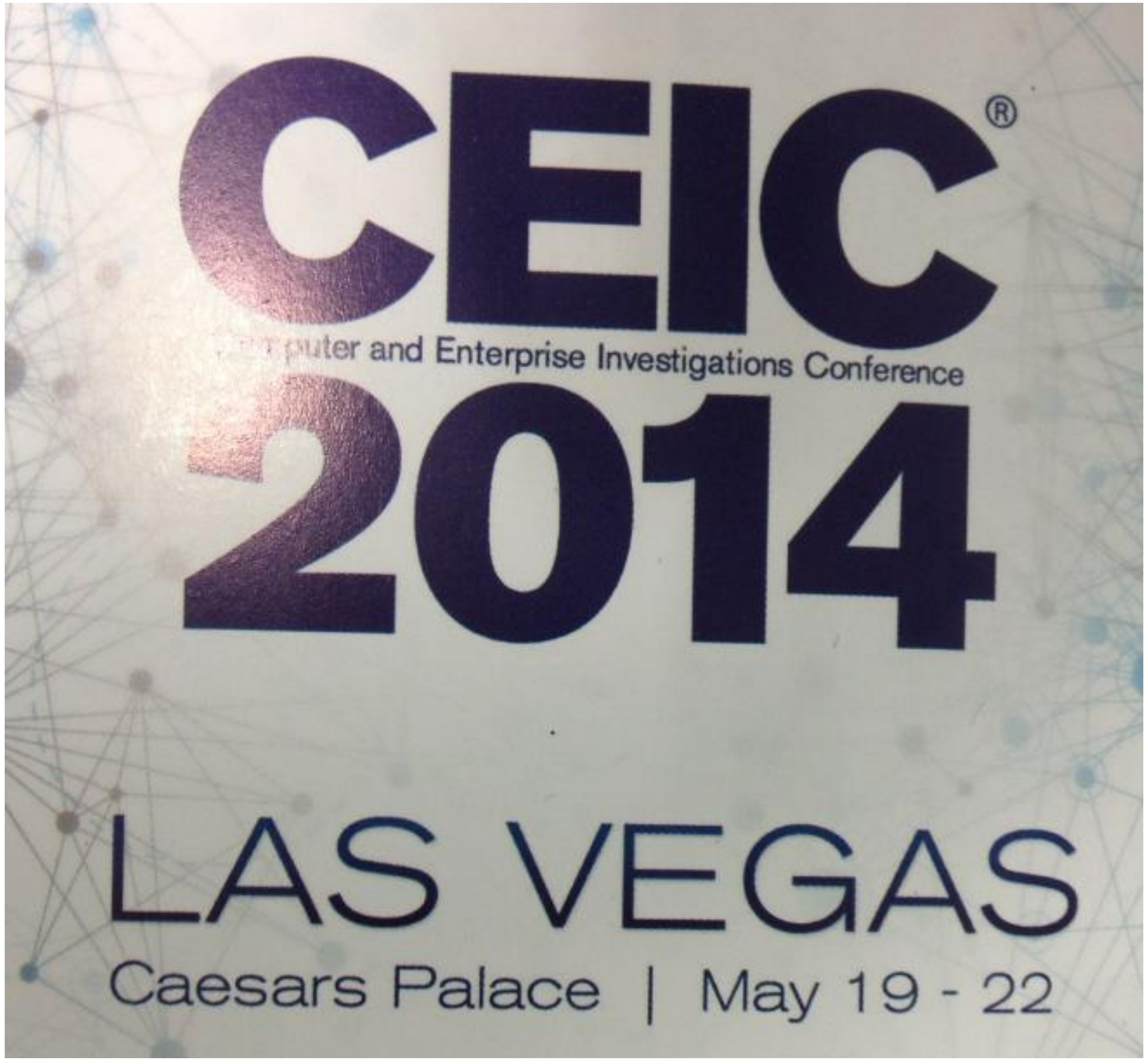
Examination Report

Case Information

Case Number	<Define Value>
Examiner Name	<Define Value>
Description	<Define Value>

EnScript® Programming

2014 CEIC



CEIC®

Computer and Enterprise Investigations Conference

2014

LAS VEGAS

Caesars Palace | May 19 - 22

Thanks

dorumugs