行政院所屬各機關因公出國人員出國報告書
（出國類別：實習）

參加 2010 第十屆電腦及企業調查鑑識(CEIC)研習營心得報告

服務機關 ： 法務部調查局資通安全處資安鑑識實驗室
出國人姓名 ： 薦任科員林雅婷
出國地點 ： 美國內華達州拉斯維加斯
出國期間 ： 中華民國 99 年 5 月 24 日至 5 月 27 日
報告日期 ： 中華民國 99 年 7 月 16 日

報告大綱

壹、 行程記述

此行目的為參加美國Guidence Software公司舉辦第10屆美國電腦及企業調查鑑識研習營（10th Annual Computer and Enterprise Investigations Conference; 簡稱CEIC）。自2010年5月24日至5月27日止共計4天，於美國內華達州拉斯維加斯紅岩飯店會議廳舉行。

貳、 CEIC研習營介紹

CEIC研習營主要由美國Guidance Software公司每年舉辦一次，該公司成立於1997年，總部設立於加州帕薩迪納市，為世界公認數位鑑識軟體權威，提供全球企業或執法機構有關資訊調查與電腦犯罪之鑑識技術。Guidance Software公司每年於國際認證課程培訓6,000多名資訊調查或電腦鑑識執法人員。客戶群涵蓋全球警政機關、執法單位、金融、保險、高科技、企管顧問、公用事業與醫療等企業之IT單位。

今年主辦單位規劃11個主題教室，包括Advanced Techniques Lab 、 Cybersecurity Lab 、 Digital Acquisition Lab、Digital Analysis Lab、eDiscovery Lab、General Learning Topics Lab 1、General Learning Topics Lab 2 、eDiscovery Legal Lecture、General Learning Topics Lecture 1、General Learning Topics Lecture 2及Most Popular Track等，每個主題教室於每個時段分別提供深入之探討，學員可依照個人興趣選擇

課程。此外，大會亦於展覽會場集結各大知名鑑識工具供應廠商展示最新數位鑑識軟、硬體產品，供學員於中場休息時間參觀，以便掌握最新一代鑑識工具及科技趨勢。

Guidance Software 公司亦提供免費EnCE(EnCase Certified Examiner)證照考試，學員可於開課前透過網路報名考試，並於現場參加第一階段筆試測驗，2週後以電子郵件通知考試結果，若順利通過筆試測驗，原廠立即寄出第二階段實作測驗之軟體、試題及鑑識資料，必須於2個月考試時間內完成測驗並將報告燒錄成光碟郵寄美國Guidance Software公司。

參、 活動記要

一、 5月24日上午9:00至12:00，於美國內華達州拉斯維加斯紅岩(Red Rock)飯店五樓會議廳外辦理報到手續，並領取學員證及課程表。

二、 5月24日下午3:00至4:30，參加課程「How to Create and Perform Effective Keyword Searches 」(Advanced Searching)，由Guidance Software公司講師Daniel Smyth先生主講，關鍵字搜尋為鑑識工作基本工具，如何正確使用EnCase軟體，在數以萬計數據中將搜尋範圍縮小，取得與案情相關證據，關鍵字GREP格式與搜尋條件設定即相當重要。

三、 5月25日上午8:30至9:00，由Guidance Software公司

執行總裁Victor Limongelli先生歡迎來自世界各地鑑識菁英參加第十屆CEIC訓練營，今年訓練課程涵蓋多面向之數位調查工作，包括數位媒介鑑識、網路安全與惡意程式移除技術、隱私權探討等，並期許與會學員彼此經驗交流，討論最新科技發展及分享工作上技巧和訣竅。

四、 5月25日上午9:00至10:00，由前國家安全委員會網路安全主管及哈佛甘迺迪學院貝爾中心資深顧問Melissa Hathaway女士擔任特別來賓，強調網路安全對國家、社會、企業重要性，並針對網路病毒散布、網路使用者隱私權、駭客問題、網路交易安全等議題發表個人見解。

五、 5月25日上午11:00至12:30，參加「Basic RAID Acquisition and Analysis」課程，由Guidance Software公司講師Simon Key先生主講，磁碟陣列常用於伺服器等主機，由多顆硬碟所組合而成，可增強資料整合度、容錯功能、處理量等，卻也相對提高鑑識人員鑑定門檻。課程中介紹市面上常用RAID0~RAID5等類別及邏輯觀念、如何獲取RAID映像檔及分析技術等基本知識等，讓學員了解面對RAID案件時，應採取之處理程序。

六、 5月25日下午2:00至3:30，參加「Advanced RAID Analysis」課程，由Guidance Software公司講師Manfred Hatzesberger先生進一步深入介紹RAID磁碟

陣列分析方法，主要區分為軟體RAID及硬體RAID，說明兩者間的差異性及效能，並實際操作如何使用EnCase鑑識軟體內 EnScripts程式自動重組數顆硬碟映像檔，以利鑑定人員後續分析工作。

七、 5月25日下午4:00至5:30，參加「Email Case Study」課程，主講者為Guidance Software 公司Brent Botta先生。電子郵件已成為現代人不可或缺的訊息交流工具， 隱藏其中之網路數據資訊、傳輸內容及附件等，往往使得電子郵件調查工作日趨重要。本課程除介紹理論觀念外亦包括實際上機操作，教導學員如何利用EnCase鑑識軟體所提供Email分析功能加快電子郵件分析，減少鑑定人員工作量。

八、 5月25日晚間6:30至9:00，參加EnCE第一階段筆試測驗；因已先於網路報名免費EnCE證照考試，且經Guidance Software公司審查符合考試資格，所以可於會議期間當場考試，並順利通過EnCE證照第一階段筆試測驗，獲得第二階段實作測試資格。

九、 5月26日上午08:30至10:00，參加「Customized SQL Reporting」課程，由Guidance Software公司講師David Wood先生負責講授，主要說明MS SQL Server系統報表客製化處理方式。針對表格進行關聯，篩選出所需欄位，匯出成報表格式。進階功能說明則包括Web報表格式和電子郵件自動發送更新。

十、 5月26日上午11:00至12:30，參加「Windows 7: What is

new in Windows Forensics」課程，由 Guidance Software公司講師John Marsh先生負責講授Windows 7系統功能與現行Windows XP變化差異，因此本課程逐一討論Windows 7之VMR結構變化、新增Journal記錄檔、NTFS記錄檔、最後存取時間不立即寫入、新一代ExFAT檔案系統、Registry登錄檔之儲存路徑變異等，使鑑識人員能掌握新一代Windows 7作業系統，以因應科技趨勢變化。

十一、 5月26日下午2:00至3:30，參加「Forensic Tracking of USB Devices」課程，由 e-Forensic Services Inc公司講師Colin Cree先生講授， USB (Universal Serial Bus)儲存容量日益擴大，體積小、價格便宜及其隨插即用特性為人類生活帶來極大便利，因此USB鑑識亦占有一席之地，本課程說明如何藉由Registry登錄檔觀察USB使用紀錄，取得USB序號、製造廠商、使用時間等資訊協助鑑識USB裝置。

十二、 5月26日下午4:00至5:30，參加「EnCase Tips & Tricks」課程，由 Guidance Software公司講師Chris Pavan先生負責講授，由於EnCase為鑑定人員使用之主流鑑識工具，因此Guidance公司特地規劃此一課程，介紹EnCase設定環境，包括EnScripts、Indexing、filter篩選機制等使用技巧與訣竅，使鑑定人員更能輕鬆使用及快速上手。

十三、 5月27日上午8:30至10:00，參加「Acquisition &

Analysis of Physical Memory」課程，由BitSec Forensics 公司講師Michael Webber先生負責主講，如何辨識及藉由工具分析RAM記憶體資訊，取得電腦正在執行程式及即時資訊，包括MFT目錄資訊、開啟文件、即時通訊、網頁瀏覽、網絡連結資訊、登錄用戶等紀錄。

十四、 5月27日上午10時15分至11時45分參加「Get Schooled in Mobile Forensics」課程，由英國地鐵警察Christopher Andrews先生主講，目前手機鑑識最大挑戰在於廠牌種類繁多，各家手機大廠儲存資料格式不盡相同，所以無法有效使用單一工具將其一網打盡，因此主講者針對特定手機廠牌進行分析與研究，瞭解手機簡訊、圖片、通訊錄等儲存方式及如何於資料被刪除後予以回復。

肆、 心得與建議

一、 美國Guidance Software公司EnCase鑑識軟體廣為世界各地執法人員、政府機關、資訊安全專家、法律公司等鑑識人員使用，因此每年CEIC訓練課程亦吸引兩三百位鑑識領域菁英參與此盛會，台灣、日本、韓國、中國大陸、香港、新加坡等亦有多人參加，我很高興參與此次國際訓練課程，學習最新科技資訊，亦自我期許不斷於求新求變於鑑識領域中與時俱進，向上提升。

二、 大會用心設計多樣化課程，舉凡軟體操作課程、網路

犯罪調查、數位證物獲取與分析、法律探討等議題，每個課程以1個半小時為單位,學員可依照自己專長與興趣選擇課程，亦可臨時更改旁聽課程，相當務實與實用，與一般從頭到尾固定訓練課程迥然不同，本課程設計顯得相當有彈性。

三、 同仁參與訓練課程或研討會時，舉辦單位往往會提供相關文件或電子檔案，建議可規劃實體或網路空間加以保存，提供有興趣同仁借閱或下載，達到知識分享之功能。

附件1：會場照片

圖 1　CEIC 會場註冊櫃台

圖 2　CEIC 會議之議程表

圖 3　上課情形

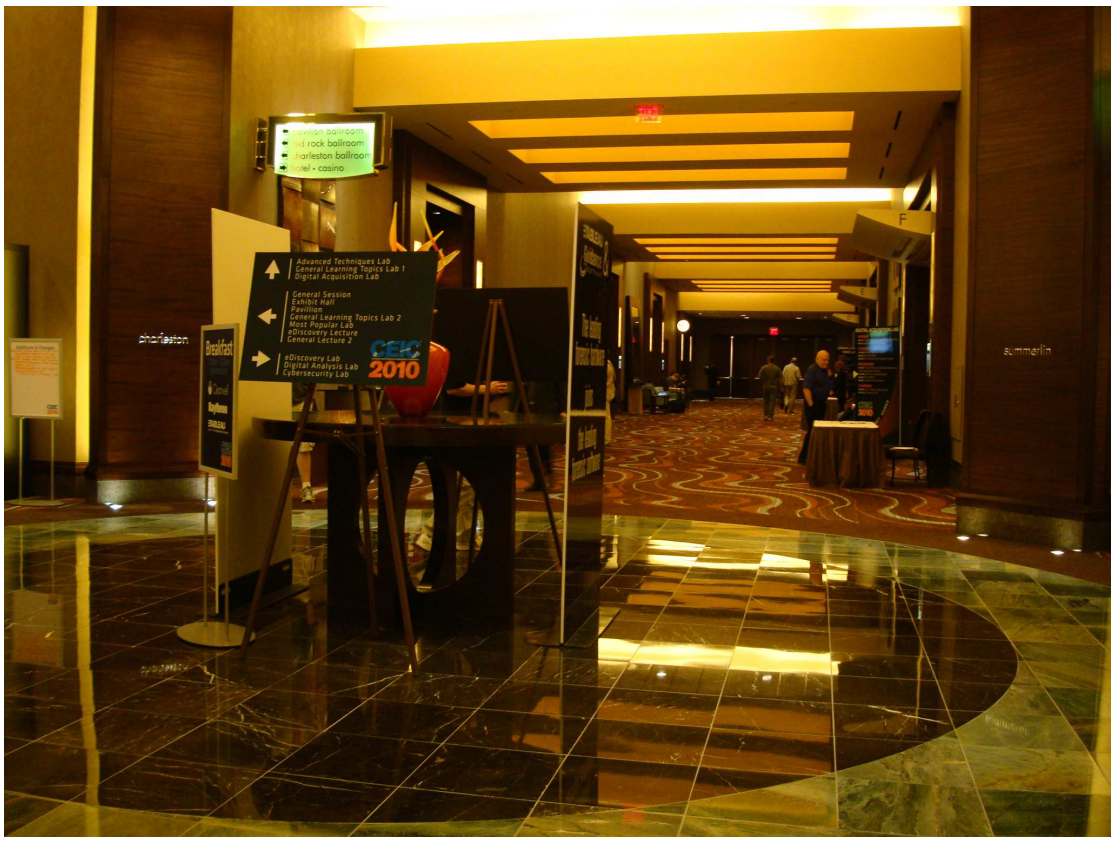

圖 4　議會大廳

圖 5　CEIC 會議戶外展場

附件 2. 大會議程

Monday, May 24	
3:00pm | 4:30pm	Track: Advanced Techniques Lab EnScript® 101, *Kimberly Stone-Kaplan, Guidance Software, Inc* (Basic/Intermediate)
	Track: Cybersecurity Lab Defeating Advanced Hiding Techniques, *Dave Shaver, US Army CID* (Intermediate)
	Track: Digital Acquisition Lab EnCase® for Anyone - Collections in the Field using EnCase® Portable, *Jamey Tubbs, Guidance Software, Inc* - **NEW**
	Track: Digital Analysis Lab Forensic Investigation 101 - Where to Start Looking, *James Habben, Guidance Software, Inc* (Basic)
	Track: eDiscovery Lab Mini-Series Part 1 - Information Management/Retention Policy, *Liz Hall, Will Chesher, Guidance Software, Inc* - **NEW**
	Track: General Learning Topics Lab 1 EnCE® Last Minute Review, *Howard Williamson, Guidance Software, Inc* (Intermediate)
	Track: General Learning Topics Lab 2 Learning the Digital Forensics Backlog and Creating Highly Effective Investigations, *Suresh Sundarababu, Global Solutions Strategy Manager, Dell* - **NEW**
	Track: eDiscovery Legal Lecture New Technologies and New Problems for eDiscovery, *David Benton, Home Depot and the American Society of Digital Forensics & eDiscovery, Browning Marean, DLA Piper, Guidance Software, Inc.* - **NEW**
	Track: General Learning Topics Lecture 1 Cloud Computing and its potential impact on Digital Forensic Investigations, Moderator: *John Marsh, Guidance Software, Inc, James Valentine, NetApp, Albert Barsocchini, Guidance Software, Inc.* - **NEW**
	Track: General Learning Topics Lecture 2 Digital Forensic Reporting, *Andy Spruill, Guidance Software, Inc* - **NEW**
	Track: Most Popular Track Government and Corporate Cybersecurity, *Joe Riggins & Stewart Tong, Guidance Software, Inc* - **NEW**
	Track: Advanced Techniques Lab

4:45pm | 6:15pm	Using COM in EnScript®, *Stephen Pascual, Guidance Software, Inc* (Intermediate) - **NEW**
	Track: Cybersecurity Lab Proactive Cybersecurity-Reduce the Attack Surface with Application Whitelisting, *Doug Cahill, Bit9* - **NEW**
	Track: Digital Acquisition Lab Acquisition & Analysis of Physical Memory, *Michael Webber, BitSec Forensics, Inc* (Intermediate)
	Track: Digital Analysis Lab EnCase® Focus - Difference Between Indexing and Keyword Searching, *Daniel Smyth, Guidance Software, Inc*
	Track: eDiscovery Lab Mini-Series Part 2 - Data Mapping and Sampling to Locate, Clarify, and Refine Info, *Nick Torrecillas, Dave Erban, Guidance Software* - **NEW**
	Track: General Learning Topics Lab 1 Bit Torrent: A Forensic Review, *Andy Joyce, Forensic Data Recovery Inc.* (Intermediate)
	Track: General Learning Topics Lab 2 Social Media Investigations, *Frank Zeller, Inland Direct* (Basic) - **NEW**
	Track: eDiscovery Legal Lecture eDiscovery for Law Enforcement (Criminal Investigations), *Kenneth J. Withers, Federal Judicial Center and The Sedona Conference, Karl Heisler, Katten Muchin Rosenman LLP* - **NEW**
	Track: General Learning Topics Lecture 1 Follow the Money, *John Grancarich, Paul Hastings Janofsky and Walker LLP* (Basic) - **NEW**
	Track: General Learning Topics Lecture 2 Being An Effective Corporate Investigator, *Craig Newell, Direct Energy* (Intermediate)
	Track: Most Popular Track Email Investigations, *Manfred Hatzesberger, Guidance Software, Inc* (Intermediate) Also offered Wednesday, 5/26 at 11:00am in Digital Analysis Lab
4:45pm | 7:15pm	EnCE Exam - EnCE® Phase 1 Exam
7:00pm	Welcome Reception

| 9:00pm	

Tuesday, May 25

8:30am | 9:00am	Kickoff
9:00am | 10:00am	**Keynote - Melissa E. Hathaway** President, Hathaway Global Strategies and Sr. Advisor Harvard Kennedy School's Belfer Center Former Acting Senior Director of Cyberspace, National Security Councils
10:00am | 11:00am	Exhibit Hall Break
10:00am | 12:30pm	EnCE Exam - EnCE® Phase 1 Exam
11:00am | 12:30pm	Track: Advanced Techniques Lab Databases and EnScript®: Storing and Querying Structured Data, *Jason Fredrickson, Guidance Software, Inc* (Intermediate) - **NEW**
	Track: Cybersecurity Lab Attack Attribution - a Cyber Forensic Perspective, *Moderater: Bill Crowell, Former Deputy Director, NSA - Panel: Melissa Hathaway, Hathaway Global Strategies, LLC and Senior Advisor at Harvard Kennedy's School Belfer Center, Ian West, NATO, Director NCIRC, Bruce Wynn, Air Commodore RAF, Former Deputy CIO and CISO for the Royal Air Force, former CTO for C4/ISR/Cyber for the Royal Air Force, Cord Chase, USDA* - **NEW**
	Track: Digital Acquisition Lab Basic RAID Acquisition and Analysis, *Simon Key, Guidance Software, Inc* (Intermediate)
	Track: Digital Analysis Lab Conducting Enterprise Investigations, (Intermediate) - **NEW**
	Track: eDiscovery Lab Mini-Series Part 3 - Processing ESI and Electronic Documents, *David Wood, Dave Erban, Guidance Software, Inc.* - **NEW**
	Track: General Learning Topics Lab 1 Mac Forensics for First Responders, *Ryan Chapin, Blackbag Technologies* (Basic) - **NEW**

	Track: General Learning Topics Lab 2 How to Create and Perform Effective Keyword Searches (Advanced Searching), *Daniel Smyth, Guidance Software, Inc.* (Advanced)
	Track: eDiscovery Legal Lecture Judicial Perspectives on Electronic Discovery, *Honorable Andrew Peck, US Magistrate Judge, Southern District of New York, Senior Master Steven Whitaker, Senior Master of the Queens's Bench Division, Royal Courts of Justice, United Kingdom, Judge Donald Shelton, Chief Judge, Washtenaw County Trial Court* - **NEW**
	Track: General Learning Topics Lecture 1 Get Schooled in Mobile Forensics, *Amber Schroader, Paraben* (Basic) - **NEW**
	Track: General Learning Topics Lecture 2 EnCase® Forensic Roadmap, Moderator: *Steve Salinas,* Panel: *Ken Basore & Ashley Stockdale, Guidance Software, Inc*
	Track: Most Popular Track Defeating Advanced Hiding Techniques, *Dave Shaver, US Army CID* (Intermediate) Also offered Monday, 5/24 at 3:00pm in the CyberSecurity Lab
12:30pm | 1:30pm	Lunch
1:30pm | 2:00pm	Exhibit Hall Break
2:00pm | 3:30pm	Track: Advanced Techniques Lab Advanced Reporting in EnScript®, *Shawn McCreight, Guidance Software, Inc* (Advanced) - **NEW**
	Track: Cybersecurity Lab Automated Reverse Engineering of Malware with HBGary Responder Pro and Recon, *Rich Cummings, HBGary* - **NEW**
	Track: Digital Aquisition Lab Advanced RAID Analysis, *Manfred Hatzesberger, Guidance Software, Inc* (Advanced)
	Track: Digital Analysis Lab Webpage Reconstruction, *John Cotton, Kevin Ripa, Computer Evidence Recovery, Inc.* (Basic) - **NEW**
	Track: eDiscovery Lab Mini-Series Part 4 - Processing of Email Records, *Nick Torrecillas, Brent Botta, Guidance Software, Inc.* - **NEW**

	Track: General Learning Topics Lab 1 Using Virtual Machines, *Dave Shaver, US Army CID* (Intermediate)
	Track: General Learning Topics Lab 2 *NIX Environments, *Chris Pavan & Gordon Stephens, 42 LLC* (Basic/Intermediate)
	Track: eDiscovery Legal Lecture Testing, Sampling and Quality Control in eDiscovery, *Scott Carlson, Seyfarth Shaw, Andrew Drake, Nationwide, Monica Palko, Rosetta Stone* - **NEW**
	Track: General Learning Topics Lecture 1 Blended Enterprise Investigations, *John Grancarich, Paul Hastings Janofsky and Walker LLP* (Basic)
	Track: General Learning Topics Lecture 2 Textual Relations, *Josh Gilliland, D4 Discovery* (Intermediate) - **NEW**
	Track: Most Popular Track Windows® 7: What's new in Windows Forensics, *John Marsh, Guidance Software, Inc.* - **NEW** Also offered Wednesday, 5/26 at 11:00am General Learning Topics Lab 1 Also offered Thursday, 5/27 at 8:30am General Learning Topics Lab 1
3:30pm | 4:00pm	Exhibit Hall Break
4:00pm | 5:30pm	Track: Advanced Techniques Lab EnScript® Debugger, *Howard Williamson, Guidance Software, Inc.*
	Track: Cybersecurity Lab Government and Corporate Cybersecurity, *Joe Riggins & Stewart Tong, Guidance Software, Inc* - **NEW**
	Track: Digital Acquisition Lab Remote Analysis/Acquisition Considerations and Options, *Rodney Smith & Daniel Smyth, Guidance Software, Inc* (Basic)
	Track: Digital Analysis Lab File Identification and Recovery Using Block-Based Hash Analysis, *Simon Key, Guidance Software, Inc*(Intermediate)
	Track: eDiscovery Lab Email Case Study, *Lead: Brent Botta, Second: Nick Torrecillas, Joe Murin, Guidance Software, Inc.* - **NEW**

	Track: General Learning Topics Lab 1 EnCE® Last Minute Review, *Nathen Langfeldt, Guidance Software, Inc.* (Intermediate)
	Track: General Learning Topics Lab 2 Mobile Physical Extractions - The Missing Link?, *Adrian O'Leary, London Metropolitan Police* - **NEW**
	Track: eDiscovery Legal Lecture How Federal Rule of Evidence 502 Affects Best Practices Regarding ESI, *John Rosenthal, Winston & Strawn, Patrick Oot, Electronic Discovery Institute, John Patzakis, Digital Compliance Consulting* - **NEW**
	Track: General Learning Topics Lecture 1 Technology Forum, *Shawn McCreight, Ashley Stockdale & Kim Stone-Kaplan, Guidance Software, Inc.*
	Track: General Learning Topics Lecture 2 What to Do When All Hope is Gone - Acquiring Data Off a Dead Drive, *John Wiechman & Eddie Wiechman, TLSI, Inc* (All Skill Levels)
	Track: Most Popular Track How to Spot Packet Forgeries, Spoofing, Tunneling and Other Rogue Network Activity, *Jamie Levy, Guidance Software, Inc* (Advanced)
5:30pm | 6:30pm	Exhibit Hall Happy Hour
6:30pm | 9:00pm	EnCE Exam - EnCE® Phase 1 Exam
Wednesday, May 26	
8:30am | 10:00am	Track: Advanced Techniques Lab Mastering Conditions 1, *Joe Murin & Liz Hall, Guidance Software, Inc* (Intermediate)
	Track: Cybersecurity Lab Searching for PII and IP in Your Organization, *Dave Erban, Jeff Danielson, Guidance Software, Inc* (Intermediate)
	Track: Digital Acquisition Lab The Impact of Multi-core and Multi-threading Architectures on Forensic Imaging Applications Performance, *Robert Botchek, Tableau LLC* - **NEW**
	Track: Digital Analysis Lab Super Timeline Analysis, *Rob Lee, SANS Institute, Mandiant* - **NEW**

	Track: eDisovery Lab Customized SQL Reporting, *David Wood, Will Chesher, Guidance Software, Inc.* - **NEW**
	Track: General Learning Topics Lab 1 Large-scale EE Deployment Best Practices, *Daniel Smyth, Guidance Software, Inc* (Intermediate)
	Track: General Learning Topics Lab 2 On The Outer RIM of your Network... Blackberry Forensics, *Andy Spruill, Guidance Software, Inc.*
	Track: eDiscovery Legal Lecture International eDiscovery: Data Protection, Privacy & Cross-Border Issues, *Dominic Jaar, Ledgit Consulting Inc., Patrick Burke, Guidance Software, Inc., M. James Daley, Daley & Fey, LLP, George Rudoy, Shearman & Stearling, LLP* - **NEW**
	Track: General Learning Topics Lecture 1 Forensic Triage Programs, Risk Assessment Factors, *JJ Wallia, ADF Solutions, Inc* (Basic) - **NEW**
	Track: General Learning Topics Lecture 2 An Uninvited Guest (Who Won't Go Home), *Bill Blunden, San Francisco State University* (Advanced) - **NEW**
10:30am | 12:00pm	EnCE Exam - EnCE® Phase 1 Exam
10:00am | 11:00am	Exhibit Hall Break
11:00am | 12:30pm	Track: Advanced Techniques Lab Creating EnScript® Plugins, *James Habben, Guidance Software, Inc* - **NEW**
	Track: Cybersecurity Lab Entropy, *Shawn McCreight, Jim Butterworth, Guidance Software, Inc.* - **NEW**
	Track: Digital Analysis Lab Email Investigations, *Manfred Hatzesberger, Guidance Software, Inc* (Intermediate)
	Track: eDiscovery Lab Early Case Assessment and Optimizing Criteria, *Will Chesher, Brent Botta, Guidance Software, Inc* - **NEW**

	Track: General Learning Topics Lab 1 Windows® 7: What's new in Windows Forensics, *John Marsh, Guidance Software, Inc.* - **NEW**
	Track: General Learning Topics Lab 2 Social Media Investigations, *Frank Zeller, Inland Direct* (Basic) - **NEW**
	Track: eDiscovery Legal Lecture eDiscovery Case Law Update, *Mark Sidoti, Gibbons P.C., George Socha, Soch Consulting, Tom Gelbmann, Gelbmann & Associates, Conor Crowley, Law Offices of Conor R. Crowley* - **NEW**
	Track: General Learning Topics Lecture 1 Spy vs. Spy: Is there a stranger in your house?, *Joe Riggins, Guidance Software, Inc*
	Track: General Learning Topics Lecture 2 Expert Witness Panel: Making It Stick, Moderator: *Andy Spruill, Guidance Software, Inc* Panel: *Larry Daniel, Guardian Digital Forensics & Lynita Hinsch, Forensics Consulting Solutions* - **NEW**
	Track: Most Popular Track Using Virtual Machines, *Dave Shaver, US Army CID* (Intermediate) Also offered Tuesday, 5/25 at 2:00pm in the General Learning Topics Lab 1
12:30pm | 1:30pm	Lunch
1:30pm | 4:00pm	EnCE Exam - EnCE® Phase 1 Exam
1:30pm | 2:00pm	Exhibit Hall Break
2:00pm | 3:30pm	Track: Advanced Techniques Lab Packing EnScript® Applications, *James Habben, Guidance Software, Inc* - **NEW**
	Track: Cybersecurity Lab How to Spot Packet Forgeries, Spoofing, Tunneling and Other Rogue Network Activity, *Jamie Levy, Guidance Software, Inc* (Advanced)
	Track: Digital Acquisition Lab exFAT (Extended FAT), *Jeff Hamm, Paradigm Solutions* (Intermediate) - **NEW**

	Track: Digital Analysis Lab Forensic Tracking of USB Devices, *Colin Cree, e-Forensic Services Inc* (Intermediate)
	Track: eDisovery Lab Triage Your Data for Forensic Analysis with EnCase eDiscovery, *David Wood, Guidance Software, Inc.* - **NEW**
	Track: General Learning Topics Lab 1 Accrediting the Tradecraft: Academia's Perspective, *Moderator: Chuck Cobb, Guidance Software, Inc.* Panel Discussion: *Anna Carlin, California State Polytechnic University, Christopher Curren, Huntington Beach Police Department* (Basic)
	Track: General Learning Topics Lab 2* this session is a Lecture Defeating the Trojan Virus Defense, *Ryan Pittman, US Army CID* (Intermediate)
	Track: eDiscovery Legal Lecture Advanced Search and Retrieval Technologies, *Albert Barsochinni, Guidance Software, Inc., George Socha, Socha Consulting and Tom Gelbmann, Gelbmann & Associates* - **NEW**
	Track: General Learning Topics Lecture 1 Adobe Flash Cookies, *Eric Huber, Honeywell Global Security* (Basic) - **NEW**
	Track: General Learning Topics Lecture 2 Anti-Forensics and Encryption Challenges in Forensic Investigations, *Christopher Andrews, Kroll Ontrack*
	Track: Most Popular Track What to Do When All Hope is Gone - Acquiring Data Off a Dead Drive, *John Wiechman & Eddie Wiechman, TLSI, Inc* (All Skill Levels)
3:30pm | 4:00pm	Exhibit Hall Break
4:00pm | 5:30pm	Track: Advanced Techniques Lab Mastering Conditions 2, *Joe Murin & Liz Hall, Guidance Software, Inc* (Intermediate/Advanced)
	Track: Cybersecurity Lab Performing Attack Attribution of Malicious Code with Entropy, *Jim Butterworth, Guidance Software, Inc* - **NEW**
	Track: Digital Acquisition Lab Encryption for the Forensic Professional, *James Wiebe, CRU-Dataport* (All Skill Levels) - **NEW**

	Track: Digital Analysis Lab - This session is a Lecture Decoding Prefetch Files for Forensic Purposes, *Mark Wade, Harris Corporation* (Intermediate) - **NEW**
	Track: eDiscovery Lab Identifying and Addressing Exceptions, *Nick Torrecillas, David Erban, Guidance Software, Inc* - **NEW**
	Track: General Learning Topics Lab 1 Live Forensics: What to Do if You Catch a Cyber Criminal in the Act, *Robert Monsour, Forensics3* (Intermediate) - **NEW**
	Track: General Learning Topics Lab 2 The Automated Investigation: How Automated Analysis Streamlines Digital Investigations, *Jason Reeve, Clearwell* (Beginner) - **NEW**
	Track: eDiscovery Legal Lecture Repurposing eDiscovery Solutions to Meet Expanding Compliance Challenges, *Mary Frantz, Enterprise Knowledge Partner LLC (EKP),* Keith Chval, Protek International International, Inc, Suellen Galish, Baker Robbins & Company - **NEW**
	Track: General Learning Topics Lecture 1 Forensic Technologies in Incident Crisis Management, *Ondrej Krehel, Identity Theft 911, LLC* (Intermediate) - **NEW**
	Track: General Learning Topics Lecture 2 Know Your Enemy - The Advanced Persistent Threat (APT) Tactics, Techniques and Countermeasures, *Rich Cummings, HBGary* - **NEW**
	Track: Most Popular Track EnCase® Tips & Tricks, *Chris Pavan & Nick Ringold, 42 LLC* (Intermediate) Also offered Thursday, 5/27 at 8:30 am in Advanced Techniques Lab
Thursday, May 27	
8:30am | 10:00am	Track: Advanced Techniques Lab EnCase® Tips & Tricks, *Chris Pavan & Nick Ringold, 42 LLC* (Intermediate)
	Track: Cybersecurity Lab BotNets: A Case Study & Lessons Learned, *Ryan Pittman, Dave Shaver, US Army CID* (Intermediate)
	Track: Digital Acquisition Lab EnCase® for Anyone - Collections in the Field using EnCase® Portable, *Jamey Tubbs, Guidance Software, Inc* - **NEW**

	Track: Digital Analysis Lab Forensic Investigation 101 - Where to Start Looking, *James Habben, Guidance Software, Inc* (Basic)
	Track: eDiscovery Lab Mastering Criteria, *Joe Murin, Brent Botta, Guidance Software, Inc* - **NEW**
	Track: General Learning Topics Lab 1 Windows® 7 : What's New in Windows Forensics, *John Marsh, Guidance Software, Inc.* - **NEW**
	Track: General Learning Topics Lab 2 Learning the Digital Forensics Backlog and Creating Highly Effective Investigations, *Suresh Sundarababu, Global Solutions Strategy Manager, Dell* - **NEW**
	Track: eDiscovery Legal Lecture eDiscovery In-House Case Studies, *Glenn O'Brien, Liberty Mutual, Matthew Miller, Forsythe, Jeff Fowler, O'Melveny & Myers.* - **NEW**
	Track: General Learning Topics Lecture 1 Gone Without a Trace? Finding Evidence of ESI Destruction Software to Support a Claim of Wrongdoing, *Christopher Andrews, Kroll Ontrack* - **NEW**
	Track: General Learning Topics Lecture 2 AIRS Reloaded: The Future of Automated Integration, *Jim Butterworth, Guidance Software, Inc* - **NEW**
	Track: Most Popular Acquisition & Analysis of Physical Memory, *Michael Webber, BitSec Forensics, Inc* (Intermediate)
10:15am | 11:45am	Track: Advanced Techniques Lab 10 Things You Overlooked In Your Last Examination, *Yogesh Khatri, 42 LLC* - **NEW**
	Track: Cybersecurity Lab Cyber Threat Management Strategies: Meeting the CHallenges of the Trusted Insider Threat, *Michael Theis, Raytheon*
	Track: Digital Acquisition Lab Linux Imaging with Linen, *John Casteel, IRS.* - **NEW**
	Track: Digital Analysis Lab Forensic Tracking of USB Devices, *Colin Cree, e-Forensic Services Inc* (Intermediate)
	Track: eDiscovery Lab

	Planning for a Successful eDiscovery Matter, *Liz Hall, Guidance Software. Inc.* - **NEW**
	Track: General Learning Topics Lab 1 Email Investigation, *Peter Mercer, Vound Software* - **NEW**
	Track: General Learning Topics Lab 2 Intro to Network Forensics, *Gary Golomb, Netwitness* (Basic)
	Track: eDiscovery Legal Lecture Preparing eDiscovery 30(b)(6) Witnesses, *Albert Barsochinni, Chad McManamy, Guidance Software, Inc., Thomas A. Lidbury, Mayer Brown, Edward Han, Howrey, LLC.*
	Track: General Learning Topics Lecture 1 Using Data Mapping Techniques to Prepare Proactive Case Templates and Manage Records Retention, *David Wood, Guidance Software, Inc.*
	Track: General Learning Topics Lecture 2 EnCase® Forensic Roadmap, Moderator: *Steve Salinas,* Panel: *Ken Basore & Ashley Stockdale, Guidance Software, Inc*
	Track: Most Popular Track On The Outer RIM of your Network... Blackberry Forensics, *Andy Spruill, Guidance Software, Inc.*