DF120 – Foundations in Digital Forensics with EnCase® Forensic

Date: 28 Feb 2017 – 3 March 2017
Time: 9:00am to 6pm
Venue: Deloitte Training Room 3 at level 20

DF120 – Foundations in Digital Forensics with EnCase® Forensic

Day 1

Day one starts with instruction on using EnCase® Forensic Version 8 (EnCase) to create a new case and navigate within the EnCase interface. The students participate in a practical exercise, which allows them to test their newly acquired navigation skills and provides an understanding of how to search for files based on metadata. Attendees use EnCase to acquire a forensic copy of media while protecting the original media from change. Methodologies used within a computer system for the allocation of storage areas are discussed. The concepts of digital evidence and how to validate evidence verification are also discussed.

The main areas covered on day one include:

- Creating a case file in EnCase
- Navigating within the EnCase environment
- Understanding concepts of digital evidence and disk/ volume allocation:
  - Types of evidence
  - Terminology describing data storage, including but not limited to unallocated space, unused disk area, volume slack, file slack, RAM slack, and disk slack
- Documenting EnCase concepts:
  - Evidence files
  - Case files and backups
  - Configuration files
  - Object icons within EnCase
- Acquiring media in a forensically sound manner

Day 2

Day two begins with a continuation of a lesson regarding acquisition concepts, which is followed by a quiz that reviews presented concepts. The students learn how to properly preview a live computer system prior to acquisition using the Direct Network Preview function. The attendees utilize the EnCase® Evidence Processor to run modules on evidence files to obtain results that are reviewed during subsequent lessons. Attendees bookmark and tag data to be incorporated into an examination report during the Report Creation lesson. Students perform a practical exercise during which they backup the case with customized settings and bookmark items for reporting purposes. Participants then run two different searching processes, raw searching (on raw data, indexed or not) and index searching (on interpreted, indexed data).

The main areas covered on day two include:

- Previewing a running computer (even one using full disk encryption) using multiple techniques, including the Direct Network Preview function
- Running EnCase utilities to capture RAM
- Processing evidence:
  - Running processes, including but not limited to file signature analysis, protected file analysis, hash and entropy analysis, email and internet artifact analysis, and word/phrase indexing
  - Executing modules, including but not limited to file carver, windows artifacts parser, and system info parser.
- Bookmarking and tagging data for inclusion in the final report
- Creating and conducting raw keyword searches and index search queries to locate search expressions of interest

Day 3

Day three begins with the completion of the index searching lesson. The participants perform a practical exercise, allowing them to practice the discussed searching and bookmarking techniques. Attendees define and install external viewers within EnCase and copy data from within an evidence file to the file system for use with other computer programs. Participants employ the use of file signature analysis to properly identify file types and to locate renamed files. Students are then provided instruction on the principal and practical usage of hash analysis. Students create a hash library, containing hash sets and hash values of notable files to identify and known files to exclude from an evidence file. Hash analysis tools, such as EnScript® programs and other utilities, are then employed to analyze hash libraries and to incorporate commonly available hash libraries/sets into the examination environment. Entropy analysis techniques are demonstrated to students to assist in the identification of files that nearly match notable files.

The main areas covered on day three include:

- Creating and conducting index search queries and raw keyword searches
- Incorporating the use of installed external viewers used by examiners into EnCase
- Copying files, folders, and data from EnCase to the local file system for analysis by other tools
- Performing signature analysis to determine the true identities of file objects and to ascertain if files were renamed to hide their true identities
- Conducting hash analysis using unique values calculated based on file logical content to identify and/or exclude files
- Importing and exporting data to/from Project Vic
- Running entropy analysis to locate files that may be near matches to other files or that may be password protected, obfuscated, or encrypted

Day 4

Day four begins with a practical exercise on conducting signature, entropy, and hash analyses. The day's instruction begins with a lesson on searching and recovering data from unallocated space. The students then discover how to customize and organize a report using bookmarked data and how to include pertinent file metadata in the report. The students are given advice and guidance in properly archiving and later reopening a case. During the archiving process, attendees use procedures to reacquire an evidence file to change evidence file parameters, such as compression or evidence file format or segment size to facilitate effective archiving. The course concludes with a final practical exercise on the week's instruction.

The main areas covered on day four include:

- Locating and recovering evidence, including images, documents, and videos in unallocated space manually and by using EnScript programs
- Creating a report of files and data bookmarked during the examination:
  - Exporting reports
  - Modifying basic reporting formats
  - Creating templates for future case utilization
- Reacquiring evidence to change evidence file settings
- Restoring evidence to run proprietary software or as required by a court order
- Archiving and reopening an archived case
- Completing a comprehensive final practical exercise

Trainer profiles

Pravin Pandey
Associate Director | Forensic SEA

Pravin Pandey is an experienced digital forensics examiner and eDiscovery consultant with 7 years' of experience in the field. He has worked on numerous cases across the region and collected and analysed evidence from multiple devices such as laptops, desktops, servers, NAS, mobile devices and cloud-based storage.

He has acted for clients across the APAC region on a variety of matters such as enforcement of intellectual property rights, investigation of financial irregularities, theft of confidential data, criminal breach of trust and cybercrime.

He has project managed the collection, preservation and processing of data in forensic and eDiscovery matters for a range of local and overseas litigation, arbitration and regulatory matters. He was lead consultant in these projects and provided invaluable advice which enabled the clients to streamline their document review and respond to discovery requests in a timely and cost-effective manner.

Pravin also actively works on cybersecurity projects involving financial institutions and hospitals.

He has been published and quoted in Lianhe Zanbao on internet artifacts and has presented at several conferences on forensics, eDisocvery and cybersecurity issues.

He is also a founding member of the HTCIA (High Technology Crime Investigation Association) Singapore Chapter.

Pravin is an Encase Certified Examiner.

Alan Dang – Trainer

Alan Dang has over 4 years of digital forensic experience in serving organizations, from a wide range of industries, in conducting and managing complex digital forensic investigations.

Alan has been instructing and proctoring classes since 2013 and was part of the team which won the Guidance Software ATP Shining Star Award the same year. He has a sound knowledge of several versions of EnCase and computer forensic methodology in general. He has an in depth knowledge of EnCase versions 6, 7 and 8.

Alan has been involved of training more than 100 students. He is able to share with his students theoretical and practical knowledge gained from years of conducting investigations, he is adept on explaining practical issues and how students can overcome daily challenges.

Alan has also demonstrated EnCase Enterprise and Forensic, as well as other forensic software, to organizations who are keen to explore more about digital forensic technologies for their infrastructure.
Since last year, Alan has been a lead trainer for EnCase. He is qualified to teach the forensic series of classes.

Alan is an EnCase Certified Examiner (EnCE), GIAC Certified Forensic Analyst (GCFA), GIAC Certified Forensic Examiner (GCFE), and AccessData Certified Examiner (ACE).

Alan has a Bachelor of Computer Science from University of Wollongong, with Digital Systems Security as his major. Alan is a member of High Technology Crime Investigation Association (HTCIA), an organization with the stated aims to educate and collaboration global members for the prevention and investigation of high tech crimes.

Llewelyn Fun – Trainer

Llewelyn Fun has been involved in computer forensic investigations and EnCase training since 2015.

In his role as consultant, he has been involved in many cases of various complexities and has dealt with a wide range of digital media. He is experienced in different types of imaging and analysis methods as well different forensic processes.

He performed forensic engagements in the region including the collection of forensic images for an international arbitration case involving 3 countries and over 40 custodians. He is also part of the SPF framework of approved forensic examiners for consulting on various criminal cases and has acted on Anton Piller Order (APO) of various magnitudes. He has been involved in classroom delivery of EnCase® training courses and has managed the training classroom setup for many classes.

He has attained the EnCase® Certified Examiner (EnCE) qualification and is a member of the Hi Tech Crime Investigation Association.

He has also attended SANS training and is a GIAC Certified Forensic Examiner (GCFE). From EC-Council, he has attained the Certified Ethical Hacker (CEH), EC-Council Certified Security Analyst (ECSA) and Computer Hacking Forensic Investigator (CHFI).

Llewelyn has previously attended Queensland University of Technology and has a Bachelor's in Information Technology specializing in Information security and forensics.

Registration

Fees per student

SGD 4,000 (price include training materials and tea break).
Registration for more than 5 students will receive 5% discount per student.

Registration

(Closing Date: Two week before commencing date)
Please register the student name for EnCase® Digital Forensic DF120.

Course Enquiry

Please contact Mr. Alan Dang
Tel: 6800 2293
Email: aldang@deloitte.com

Payment

Crossed cheques are to be made payable to "Deloitte & Touche Financial Advisory Services Pte Ltd" and mail to:
Deloitte & Touche Financial Advisory Services Pte Ltd
6 Shenton Way, OUE Downtown Two,
#33-00 Singapore 068809
Attention: Rokiah Mohamed (FAS – Discovery)

Organisation Name			No. of Student	
Contact Person		Designation		
Address				
Email		Tel		

Name	Designation	Email	Tel	Remarks

Note:

1. Registration will be confirmed upon receipt of Purchase Order/payment.
2. We regret that fees will not be refunded. Replacement is permissible with substitute attendees with writing to us two weeks before commence date.
3. We reserve the right to make any amendments, cancel and/or change the programme, venue, trainer replacements and/or topics if warranted by circumstances beyond our control.
4. All fees are exclusive of 7% GST.

Deloitte.

About Deloitte Southeast Asia
Deloitte Southeast Asia Ltd – a member firm of Deloitte Touche Tohmatsu Limited comprising Deloitte practices operating in Brunei, Cambodia, Guam, Indonesia, Lao PDR, Malaysia, Myanmar, Philippines, Singapore, Thailand and Vietnam – was established to deliver measurable value to the particular demands of increasingly intra-regional and fast growing companies and enterprises.

Comprising 290 partners and over 7,400 professionals in 25 office locations, the subsidiaries and affiliates of Deloitte Southeast Asia Ltd combine their technical expertise and deep industry knowledge to deliver consistent high quality services to companies in the region.

All services are provided through the individual country practices, their subsidiaries and affiliates which are separate and independent legal entities.

About Deloitte Singapore
In Singapore, services are provided by Deloitte & Touche LLP and its subsidiaries and affiliates.