DF210- Building an Investigation with EnCase® Forensic

Date: 21 March 2017 – 24 March 2017
Time: 9:00am to 6pm
Venue: Deloitte Training Room 3 at level 20
DF210 - Building an Investigation with EnCase® Forensic

Day 1
Day one starts with an overview of the EnCase Forensic version 8 environment. The students then learn how to collect encrypted information by examining files encrypted with Windows® BitLocker™. Attendees go on to study the Master Boot Record partitioning model and deleted partition recovery. Instruction continues with an examination of compound files. Their structures are explored and issues surrounding their examination are discussed. Students move on to explore a very important type of compound file structure, the Windows® Registry hive file. They explore mounting and examining these files and learn the relationship of the hive files to the structure of the Registry in its on-line state. Students then progress to examining the time zone information contained within the Registry, its importance to their case, and how they apply it in EnCase Forensic. The students are provided intermediate-level instruction concerning instruction regarding the methods for creating conditions to filter data. Next the students are provided with an overview of the Evidence Processor and the processing of the Malone case, which will be used throughout the rest of the course.

The main areas covered on day one include:
- Review of EnCase Forensic case creation and adding evidence
- Examining data encrypted with BitLocker
- Understanding the Master Boot Record partitioning scheme
- Principles of attempting to recover data lost through the partitioning process
- Partition recovery
- Compound files
  - Mounting and searching compound files
  - Documenting data contained within these compound files
  - Pitfalls of not examining compound files properly
- Windows Registry
  - Elements of the Registry
  - Registry keys (folders) and values
  - Registry value types
- Locating and mounting the Registry hive files
- Examination of time zone settings with the Registry
- Applying time zones within EnCase Forensic
- Using conditions to filter data
- Evidence Processor overview

Day 2
Day two begins with instructions about the FAT, ExFat, and NT file systems and then the students will participate in a practical exercise on examining all three files systems and their differences. The course continues with the use of the GREP operator functionality of EnCase Forensic to perform advanced searches. Single-file functionality as well as the value of logical evidence files are explored. A practical exercise and review is following with the processing of our second case, which concludes the instruction for the day.

The main areas covered on day two include:
- FAT, ExFAT, and NT Files Systems
- Using the GREP operators within EnCase Forensic to construct advanced search terms
- Suitability of GREP, proper syntax, and potential results
- Single files and logical evidence files
Day 3
Day three focuses upon specific analysis of common artifacts that often provide vital information to investigations. These specific areas reveal data that can provide a clearer indication of user activities. Students will explore the methods that EnCase Forensic offers to provide detailed information to the examiner. The final lesson for day three is focused on identifying, locating, and recovering email message and attachments.

The main areas covered on day three include:
- Advanced search techniques
- Windows artifacts
  - User account information and associated data
  - System folders and files of interest
  - Thumbnail cache files
  - Windows 7 specific artifacts
  - Folder structure and the effect of junctions (folder mount-points)
  - User/administrator privileges and impact on storage of data
  - Links and Library folder content
  - System files
- Shortcut or link files
  - Deconstructing link files to reveal internal structures related to their target files
  - Using link files to help determine drive letter assignment
- The Windows Recycle Bin
  - Linking Recycle Bin data to the associated user
  - Registry entries controlling operation of the Recycle Bin
  - Examination of the Recycle Bin, its properties, and function
  - Exploring the way the Recycle Bin is implemented under
- Print spooler recovery
  - Understanding the printing process and associated files
  - Recovery of SPL and SHD files as well as understanding and extracting the graphical and metadata they contain
- Email and Internet history
  - Examining both client-based and web-based email and methods available within EnCase Forensic to locate and parse email data stores
  - Recovering and analyzing email attachments

Day 4
Day four begins with instruction on examining various Internet artifact and moves on to how data located on removable USB devices can be examined and recovered. The students then will participate in a practical exercise focusing on these skills. The week of instructions concludes with a final practical that provides the student with a hands-on review of all the tuition dispensed during the course.

The main areas covered on day four include:
- Internet artifacts
- Removable USB device identification
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 Zaobao on internet artifacts and has presented at several conferences on forensics, eDiscovery 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 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 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 DF210.

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)

<table>
<thead>
<tr>
<th>Organisation Name</th>
<th>No. of Student</th>
</tr>
</thead>
<tbody>
<tr>
<td>Contact Person</td>
<td>Designation</td>
</tr>
<tr>
<td>Address</td>
<td></td>
</tr>
<tr>
<td>Email</td>
<td>Tel</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Name</th>
<th>Designation</th>
<th>Email</th>
<th>Tel</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

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 refers to one or more of Deloitte Touche Tohmatsu Limited, a UK private company limited by guarantee ("DTTL"), its network of member firms, and their related entities. DTTL and each of its member firms are legally separate and independent entities. DTTL (also referred to as "Deloitte Global") does not provide services to clients. Please see www.deloitte.com/my/about to learn more about our global network of member firms.

Deloitte provides audit, consulting, financial advisory, risk advisory, tax and related services to public and private clients spanning multiple industries. Deloitte serves four out of five Fortune Global 500® companies through a globally connected network of member firms in more than 150 countries and territories bringing world-class capabilities, insights, and high-quality service to address clients' most complex business challenges. To learn more about how Deloitte’s approximately 245,000 professionals make an impact that matters, please connect with us on Facebook, Linkedin, or Twitter.

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.

© 2016 Deloitte & Touche LLP