Deloitte.

DF320-Advanced Analysis of Windows Artifacts with EnCase® Forensic

Date: 27 March 2017 – 30 March 2017
Time: 9:00am to 6pm
Venue: Deloitte Training Room 3 at level 20

DF320-ADVANCED ANALYSIS OF WINDOWS ARTIFACTS WITH ENCASE® FORENSIC

Syllabus

Day 1

Day one begins with instruction regarding additional Registry examination techniques and artifacts. Students are shown how to extract Registry hive files and mount them into their own system for the purpose of application extraction and installation. They are also shown how to examine user-assisted and shell-bag data. The penultimate lesson on day one instructs the students on the use of block-based file hash analysis to recover deleted target files even if those files have been fragmented and/or partially overwritten. The final lesson on day one documents the examination of Windows event logs.

The main areas covered on day one include:

- Understanding the purpose and structure of the Windows Registry
- Identifying, mounting, and extracting data from Registry hive files both in EnCase Forensic and within Windows on a forensic examination machine
- Recreating the Registry data necessary to run an extracted application on the examiner's forensic workstation
- Mapping local and domain-level user accounts
- Examining user-assist Registry data
- Parsing shell-bag data in conjunction with NTFS USN change-log data
- Using block-based hash analysis for file recovery
- Analyzing Windows event logs

Day 2

Day two begins with instruction on the Volume Shadow Copy Service (VSS), which allows volume backups to be created while file-system write operations continue to take place. An examination is conducted of the technology behind hardware and software RAID devices, the way in which these devices should be forensically examined, and how the RAID functionality in the EnCase Forensic Version 8 software functions. The third lesson on day two introduces students to the Microsoft Windows prefetcher and shows them how to examine the files that it creates with a view to determining application usage. The final lesson of the day provides an overview of SQLite databases and tuition on how to query the data they contain. Practical exercises will be administered throughout the day, allowing the students to test their newly learned skills.

Day two's instruction includes:

- An introduction to the VSS operation and learning how to conduct examinations of VSS data created by the system as part of system restore operations
- Understanding RAID configurations and stripe sets
- How RAID effects forensic examinations
- Options for forensic acquisition of RAID devices and their examination in EnCase Forensic
- Understanding the purpose of the Windows prefetcher and the structure and content of the prefetch files that it maintains
- Documenting the aspects of SQLite that will be most relevant to the forensic investigator
- Using Structured Query Language (SQL) to query SQLite data

Day 3

Day three begins with a practical exercise regarding the previous day's lesson on SQLite. Tuition continues with instruction on recovering deleted SQLite data. Attendees then learn about the history and terminology associated with encrypted data. They will also learn the principles behind the recognition of encryption software and encrypted data and how they should approach the decryption of such data. The day's instruction concludes with a lesson on Windows Search and how the examiner can analyze the data that it maintains. The students will participate in practical exercises throughout the day.

The activities of three include:

- Understanding the structure of SQLite database files and how and why deleted data may be recoverable
- Understanding exactly what encrypted data is and the terminology associated with it
- The principles behind identification of encryption software and encrypted data and the methodology behind decrypting encrypted data
- The nature and use of Windows Search, which allows indexed searching within the Windows operating system

Day 4

The activities on day four begin with a practical exercise on the techniques learned during the Windows Search lesson. Instruction continues with the various techniques used for examining RAM and continues with a lesson on recovering information from ZIP files and how this can be used to recover data from the latest type of Microsoft® Word documents. Students will undertake relevant practical exercises throughout the day so as to reinforce their new-found knowledge.

The information covered on day four includes:

- Learning how to enhance the ability to conduct examinations of RAM
- The ZIP file format and how it impacts the ability to locate and recover ZIP data
- Using knowledge of the ZIP file format to recover data from the latest version of Microsoft Word documents

GUIDANCE SOFTWARE™

ABOUT GUIDANCE

Guidance exists to turn chaos and the unknown into order and the known-so that companies and their customers can go about their daily lives as usual without worry or disruption, knowing their most valuable information is safe and secure. The makers of EnCase®, the gold standard in forensic security, Guidance provides a mission-critical foundation of market-leading applications that offer deep 360-degree visibility across all endpoints, devices and networks, allowing proactive identification and remediation of threats. From retail to financial institutions, our field-tested and court-proven solutions are deployed on an estimated 33 million endpoints at more than 70 of the Fortune 100 and hundreds of agencies worldwide, from beginning to endpoint.

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 DF320.

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.