NICF-Advanced Digital Forensics

Course Description
Digital Forensics is a branch of forensics science, encompassing scientific methods, procedures and tools to perform evidence acquisition, analysis and correlation, to support crime investigations. As science and technology advances, it brings about task enabling tools for legitimate users as well as criminals. Therefore, the need for Advanced Digital Forensics to handle in-depth forensics investigation and to counter antiforensics effort has become increasingly important.

Throughout this course, the participants will be introduced to digital forensics and advanced digital forensics technologies. The participants will also learn how to put themselves in the shoes of cyber criminals to apply anti-forensics knowledge acquired in this course (on how to invalidate factual evidence information and bypass forensics effort), so as to enable a better risk assessment and analysis when conducting forensics investigative work. Countermeasures to anti-forensics techniques are also introduced to provide knowledge on current state-of-the-art technologies to defeat and mitigate anti-forensics effort.

Duration
3 days

Venue
STMI@NUS
ICube, Level3
21 Heng Mui Keng Terrace
Singapore 119613
stmi@nus.edu.sg

Contact Us
Tel: +65 6601 1040
Fax: +65 6776 2856
Email: stmi@nus.edu.sg

www.stmi.nus.edu.sg
Course Benefits

- Learn how to consider anti-forensics and countermeasures to anti-forensics when conducting forensics investigations
- Learn how the technologies in the areas of digital forensics have advanced
- Learn how in-depth acquisition and analysis of data and image evidence are conducted
- Learn how advanced mobile device and network forensics are conducted

Who Should Attend
Anyone seeking to acquire and apply the knowledge on in-depth state-of-the-art forensics technologies, antiforensics and countermeasures to anti-forensics efforts in their security analysis and forensics investigative work

Pre-requisites
Basic computer security knowledge

Course Outline

1. Digital Forensics
   - What is digital forensics
   - How is digital forensics carried out
   - What is anti-forensics and its impact on forensics investigations

2. Data Forensics
   - How are files stored and what is its impact on forensics
   - How does file format affect data recovery
   - What is basic data recovery
   - What is advanced data recovery and why is there a need for it

3. Image Forensics
   - What is image forensics
   - What is image tampering and how is it achieved
   - How does image tampering affects forensics investigations
   - What are the methods to prevent and detect image tampering

4. Mobile Device Forensics
   - What is mobile device forensics
   - What is basic mobile device forensics
   - What is advanced mobile device forensics and why is there a need for it

5. Network Forensics
   - What are denial of service attacks
   - How are the attacks carried out
   - What is attacker tracing and why is there a need for it
   - What are the methods to trace attackers

Course Leader

Dr. Vrizlynn Thing

Dr. Vrizlynn Thing received her Ph.D. degree in Computing from Imperial College London, U.K., while holding the U.K. Overseas Research Students Award (Scholarship) and the Imperial College London, Department of Computing Scholarship concurrently. During her Ph.D. studies, she won the “Best Student Paper Award” at the 20th IFIP International Information Security Conference (held in Japan, in 2005), and the Imperial College London “Hilfred Chau Postgraduate Award”, presented to students with exceptional achievements in scholarship (in 2007), for her work on adaptive detection and mitigation of network attack mutations. She was also a key research member in both the European Union project (DIADEM Distributed Firewall), and the U.S. Army Research Laboratory and U.K. Ministry of Defence project (International Technology Alliance in Network and Information Science).

Dr. Thing is a three-time winner of the “Tan Kah Kee Young Inventors Award” for her inventions on network attack defence (in 2006), network forensics (in 2009) and mobile device forensics (in 2011). She is also a three-time recipient of the “I2R Role Model Award” (in 2003, 2011 and 2012). Dr. Thing also won the “Best Paper Award” at the CYBERLAWS 2011 (held in France), for her work on countering anti-forensics. For her significant scientific contributions to the research on digital forensics and cyber security, she was named the “Achiever of the Year” in 2012 by I2R, A*STAR.

Dr. Thing currently leads the Digital Forensics Lab at I2R. She is the Principal Investigator and Lead Scientist of several projects with multi-national companies and government agencies. She also holds the Adjunct Assistant Professor position at the School of Computing, National University of Singapore. She is responsible for introducing digital forensics into the school’s curriculum, and teaches “Systems security” and “Topics in information security and digital forensics” to postgraduates at the university. Her research interests include digital (multimedia, mobile and network) forensics, and systems, information and network security.

More information about her work can be found at www1.i2r.a-star.edu.sg/~vriz.