ITSC 306 - Computer Forensics

Course Description:
This advanced course provides students the tools and processes for the collection and evaluation of evidence found in computer systems. The emphasis is on the complexity of investigating incidents in a forensically sound manner consistent with current Canadian and international laws. Topics include: identifying and preserving evidence, chain of custody, file and log analysis, proper legal documentation, memory forensics and the identification of malware within a system being examined.

3.0 Credits

Time Guidelines:
The standard instructional time for this course is 60 hours.

Prerequisite(s):

- LAWG 200
- ITSC 304

Course Assessment:

Labs	20%
Quizzes	30%
Midterm	25%
Final	25%
Total:	100%

Other Course Information:
Learner Engagement:

In order to be successful, the learner is expected to be engaged in learning activities for a total of 9 to 12 learning hours per course per week, which includes both in-class and out-of-class time.

ICT Policies:

The School of Information and Communications Technologies (ICT) expects students to act professionally during their studies. These expectations are described in the school's Student Guidelines document page. Students should review the guideline regularly, as the content may change.

SAIT Policies and Procedures:

For information on the SAIT Grading Scale, please visit policy AC 3.1.1 Grading Progression Procedure: http://www.sait.ca /Documents/About SAIT/Administration/Policies and Procedures/AC.3.1.1 Grading and Progression Procedure.pdf

For information on SAIT Academic Policies, please visit: www.sait.ca/about-sait/administration/policies-and-procedures /academic-student

Course Learning Outcome(s):

1. Explain the forensic principles and general guidelines.

   Objectives:

   1.1 Describe the forensic process

   1.2 Explain the legal implications of forensic analysis

   1.3 Outline the physical limitations of system imaging

2. Summarize the methods to locate and collect evidence

   Objectives:

   2.1 Analyze a system to determine the types of data for extraction

   2.2 Identify the physical location of target data

   2.3 Identify the encryption mechanism, if any, are used on the target data

   2.4 Compare existing tools to extract target data

3. Examine the proper planning and preparation procedures

   Objectives:

   3.1 Explain the concept of “Chain of Custody”

   3.2 Distinguish the appropriate documentation procedure requirements

   3.3 Justify the possible need of warrants

   3.4 Recommend the physical and software tools to collect data

4. Explain the process of acquiring a forensically sound image

   Objectives:

   4.1 Demonstrate the methods of volatile memory captures.

   4.2 Demonstrate the methods of non-volatile disk captures

   4.3 Discuss the techniques of capturing data over a network

   4.4 Discuss the implications of removable media and RAID drives

   4.5 Validation of system images using a variety of hashing mechanisms

   4.6 Integrating various collected data into a functional virtual machine

5. Examine the methods of managing and maintaining a forensically sound image.

   Objectives:

   5.1 Construct a secured image with encryption

   5.2 Examine image cloning techniques

5.3 Evaluate image transfer and storage methods

5.4 Exhibit methods to wipe and dispose of data securely

6. Analyze techniques to examine data from an acquired image

Objectives:

6.1 Validate and document operational image

6.2 Implement static analysis of file systems and memory content

6.3 Implement dynamic analysis of file systems and memory content

6.4 Infer the techniques used by the party under suspicion

7. Develop a forensically sound procedure to record and report evidence

Objectives:

7.1 Justify all analysis and documentation activities

7.2 Judge the weight of the evidence collected

7.3 Incorporate the evidence collected for legal proceedings