UNIVERSITY OF NEW BRUNSWICK
Faculty of Computer Science
Digital Forensics (CS4419-CS6419) – Summer 2021
Final Project – Forensic Investigation Process Model and Approach

Graduate Students

The main goal of this project is to evaluate your understanding of digital forensic and investigation process to detect the malicious behavior from captured traffic, dumped memory, captured logs, or registry of an intrusion.

Description:
Students need to select one malicious software or attack for the project. Then execute one or two samples of that malware or conduct that attack. Capture, the network traffic or memory dumps during the malicious activity. Then analyze the dumped files and explain the malware technique or attack scenario with related snapshots from each step.

Instructions:
1. Select one malicious software or attack
2. You can use the available open-source projects (such as https://github.com/ytisf/theZoo)
3. Execute the malware or conduct the attack
4. Capture two data sources (such as Network+Memory, Memory+Registry, Memory+Log, Memory+dd, …)
5. Extract the forensics indicators from the dumped data using different tools
6. Find the malicious functionality and list the steps
7. Explain the steps to find the destruction type

Final Report:

1. Summary of 5 related published articles about the malware family or attack (Report 1)
2. The second report (Report 2) includes:
    - Extracted forensics indicators and related snapshots from both data sources
    - Explain all malicious actions (with related snapshots)
    - Explain the destruction type
3. A presentation file for 5 minutes, includes:
   Hypothesis, Evidence(s), Data source(s), Tool(s), Indicators/artifacts, Proof(a)s, Name of malware/attack
4. Two collected data sources

Notes:

- Please follow the structure of a forensic investigation report structure
- Please follow the timetable and deadline for the final project submission
- The final project is individual
- Please do not select DoS/DDoS, Brute Force or Dictionary attack (As we worked on before)
- Please do not use Stuxnet, the Zoo, Cridex, Coreflood, Laqma, Winserver, Sality, Zeus , Prolaco, and Tigger malware families (As we worked on before)
- Prepare a presentation file for maximum 5 minutes
- Final project with one data source is not acceptable (Minimum two data sources)
- Students should upload the dumped files (from two data sources), two reports (Report 1 and Report 2) and a presentation file in the “Final Project” folder on D2L before the deadline (You can compress the dumped files)