ITC

INFORMATION TECHNOLOGY COMPETITION

Digital Forensics Case

Written By: Cornelius Rogers

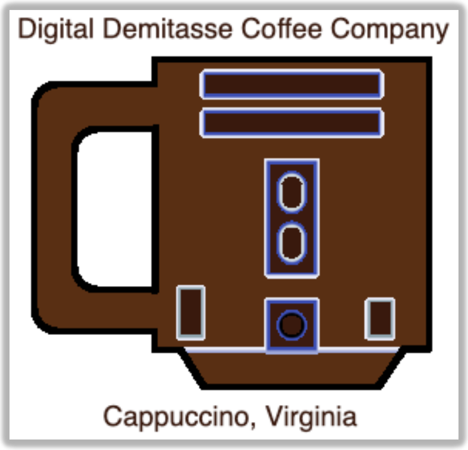
Case: FCIT-2567-34

Overview

As a competitor in the Digital Forensics Case Competition, your team will be provided with digital evidence to forensically examine. Each team will be obligated to follow industry best practices in the handling and processing of the digital evidence. The tools and methodologies used to preserve and examine the evidence must also follow industry best practices as each team will be obligated to account for and defend the accuracy of their findings.

Corporate Profile

Mike Solo is the Chief Information Security Officer of the Digital Demitasse Coffee Company (D2C2). D2C2 is the first digital, inter-galactic coffee company whose Inter-Galactic Headquarters is based out of Cappuccino, Virginia. Due to the rapid success and expansion of D2C2, they have been subject to numerous cyber-attacks and insider threats with the goal of disrupting their inter-galactic dominance.



Security Incident Overview

On February 28, 2019, Mike Solo received a report of unusual network activity within the Digital Demitasse Coffee Company corporate network from the internal Security Operations Center (SOC). Realizing that the incident was likely beyond the scope of knowledge of the D2C2 SOC, Mike Solo reached out to the Federal Coffee Investigation Taskforce (FCIT) for assistance in handling the investigation of the potential incident.

To ensure the data was preserved, the SOC team preserved a disk image of a Windows Workstation used by the Chief Operating Officer (COO) and Deputy Chief Operations Officer (DCOO), a disk image of a Windows Server used by a Senior System Administrator (SSA) and Junior System Administrator (JSA), and a memory capture of the Windows Workstation. This evidence was then turned over to Mike Solo.

Consultant Task

You are the newest members of the Federal Coffee Investigation Taskforce (FCIT) and have been tasked to work with Mr. Solo in conducting a digital forensic investigation into unusual activity within Digital Demitasse Coffee Company (D2C2) corporate network. As part of your investigation, you should analyze all available evidence to determine if an intrusion occurred, if there is an insider threat, and if there are any other investigations that should be conducted.

Evidence Provided

1. VMDK of Workstation (COO/DCOO)
2. VMDK of Server (SSA/JSA)
3. Memory Capture of Workstation

DELIVERABLE: Examination and Reporting Phase

Teams will be expected to provide a narrative examination report documenting their methodologies, analysis, and findings. Any exhibits you have should be provided with the report. If the exhibits are too large to print, then they should be included in electronic copy. Teams will be provided the evidence prior to the challenge for examination and deliverables. Teams should use this time to draft their final examination report and create their presentation materials. The **Final Expert Witness Report** is due no later than **5:00 PM Pacific, March 18, 2019**. The **Final Presentation** materials are due no later than **5:00 PM Pacific, March 21, 2019**. If you do not turn in a report, you will not be allowed to move to the following Presentation Phase. Furthermore, you are not permitted to have anyone other than the members of your team actively play a role in examining the evidence, writing the examination report, or presenting your findings. The following items, at a minimum, should be included in your report:

1) Introduction
    - a. A quick description of the compelling event
    - b. A description of the services requested
    - c. Team Members and the roles they played

2) Summary
    - a. Synopsis of findings

3) Methodologies
    - a. A description of the evidence you reviewed for the case
    - b. Chain of Custody
    - c. Evidence Validation and Verification
    - d. What tools were used to review the evidence during the course of the exam

4) Analysis and Findings
    - a. Detailed Explanation of any probative or exculpatory findings and the analysis conducted to reach that finding
    - b. Include References to Exhibits
    - c. Include definitions of technical terminology

5) Conclusion
    - a. Mitigation and Remediation Actions
    - b. Were any exceptions noted during the exam
    - c. Disposition of all evidence and case materials
    - d. Description of all exhibits

<u>NOTE</u>: Teams should be prepared to receive and analyze digital evidence from multiple sources. As with any Digital Forensics / Incident Response case, the provided evidence may hold malicious files. Teams should be careful handling potentially malicious files and take steps to prevent infection of the examination machine or loss of data.

DELIVERABLE: Presentation Phase

Each team will be expected to present their findings during the ITC Event in front of the panel of Judges. Your team should be prepared to provide a verbal testimony as to your team's methodologies and findings. The ability of your team to present your findings and accurately represent the evidence will be scored. Each team will have no more than 20 minutes to present their findings, followed by 10 minutes of Question and Answer from the Judges Panel. During the Q & A portion of this phase, you and your team should be able to attest to the findings of your report, provide further meaning as asked, and be able to defend your methodologies.

Scoring

Judges will score each team based upon four (4) categories:

1. Ability to identify key forensic artifacts
2. Demonstration of technical skills
3. Final Expert Witness Report
4. Final Presentation

The maximum score will be 100 points. Teams will be ranked based on their cumulative score from the highest to the lowest.

Notes:

1. Treat each RFC-1918 /24 subnet as a different public network
2. The use of Open Source tools is acceptable
3. Questions about the case can be sent to the ITC Chair:
    a. Addendums may be issued to clarify some aspects of the case or evidence
    b. Addendums are not guaranteed if a competitor submits a question
    c. Addendums will be sent to all teams competing in the Digital Forensics case

Chain of Custody Form Number	20190301

EVIDENCE CHAIN OF CUSTODY TRACKING FORM

Case Number	FCIT-2567-34
Receiving Officer	
Property Owner	Mike Solo
Location of Seizure	Digital Demitasse Coffee Company Inter-Galactic Headquarters Cappuccino, Virginia
Date/Time Seized	March 1, 2019
Reason for Seizure	Evidence

Description of Evidence		
Item #	**Quantity**	**Description of Item**
1	1	**Evidence Type**: VMDK **Description**: Windows 10 Workstation used by COO and DCOO **MD5:** 8f762bae7a4a77ea44c22159178ed077 **SHA1:** 97b8068fadeae7938a821d2a53c0db91eb2f56c1
2	1	**Evidence Type**: VMDK **Description**: Windows Server 2016 used by SSA and JSA **MD5:** 65656197d6eb47fdfed1ce7d23691b22 **SHA1:** b682e175534f76b9dce8038c377cd10bef5d6249
3	1	**Evidence Type**: Memory Capture (vmem) **Description**: Windows 10 Workstation used by COO and DCOO **MD5:** 57600b5aab48062c89025bdc83d0ba8c **SHA1:** 6f26ae75f73d492205f96f204d4e9f8d65fb4943

Date/Time	**Released By**	**Received By**	**Comments/Location**
March 1, 2019	Brandon Kenobi	Mike Solo	Seized from D2C2 IGHQ
March 2, 2019	Mike Solo		Released to FCIT