DIGITAL FORENSICS CHALLENGE

OVERVIEW

For this competition, your team will be provided digital evidence images to forensically examine. Each team will be obligated to follow industry best practices in the handling and processing of this 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.

SCENARIO

Acme Mobility, LLC. is a mobile software development start-up which is the creator of a phone app which is growing in popularity and is expected to be one of the top social media applications. Acme Mobility operates several Microsoft Azure Cloud systems which are used by a few dozen global employees to develop and run the daily operations of the company.

Your team will act as contractors who have been hired to conduct a thorough digital forensics investigation into a data breach incident at Acme Mobility. Digital evidence from several systems has been forensically preserved and will be supplied to your team for review.

INCIDENT

On March 25, 2016; CEO Tommy Flanagan was made aware that the source code for their next generation application had been leaked online along with other confidential documents. An email claiming responsibility was received by Mr. Flanagan claiming responsibility for the leaked source code and documents. This leak will cause severe damage to the company, potentially costing millions in lost revenue. Investors are demanding action against those responsible for the exposure and criminal prosecution.

Upon the discovery of this incident, Acme Mobility's IT Manager, Nick Burns, launched an investigation into this incident. Mr. Burns captured forensic images of the Azure cloud computers assigned to several employees and the servers related to the source code and other confidential documents. At this time, Acme Mobility's IT Manager is unable to determine if the how the source code was leaked and has requested outside assistance.

Forensic images of the system hard drive and memory have been provided for your examination for the following Microsoft Azure Cloud Computers:

Evidence File	Computer Name	Description
Tommy Flanagan - CEO	ACME-TFLANAGAN	Cloud Computer – Windows 7
Jacob Silj – Product Development	ACME-JSILJ	Cloud Computer – Windows 7
Leon Phelps – Sales Manager	ACME-LPHELPS	Cloud Computer – Windows 7
File Server / Domain Controller	ACME-AD	Cloud Server – Windows 2008 R2

EVIDENCE / EXAMINATION

Based on the possible sensitivity of the incident and the lack of resources, ACME Tech has decided to contract the investigation to your team. Your team is to investigate this matter as if it were a real breach and coordinate the incident response process based on the information obtained during your analysis.

Your team will be provided with forensic images from the users who had direct access to the source code. The company CEO, Tommy Flanagan, has requested your team to review the evidence and report back any findings as follows:

1) Who was responsible for the leakage of the ACME Source Code and Documents?
2) How was the code accessed and stolen? Who else could be subpoenaed for further evidence? What should the subpoena ask for?
3) Was a crime committed under state and/or federal law? Explain.
4) What remediation actions does your team recommend to contain this incident and prevent further incidents in the future?

DELIVERABLES

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 examination report is due no later than 5:00PM Pacific, April 9, 2016. The final presentation materials are due no later than 5:00PM Pacific, April 15, 2016.** 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 is some items your report should, at a minimum, include:

1) Introduction
    a. A quick description of the compelling event
    b. A description of the services requested
    c. Team Members and 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 information.
    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

NOTE: Teams should be prepared to receive and analyze digital evidence from multiple sources. Each team will need to have a 120GB+ Hard Drive to receive their copy of evidence. As with any Digital Forensics / Incident Response case, the provided evidence may hold malicious files. Teams should be careful handling possible malicious files and take steps to prevent infection of the examination machine or loss of data.

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 15 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 be scoring each team based upon four (4) categories: Ability to identify key Forensic Artifacts, Demonstration of Technical Skills, Final Report, and Final Presentation for a maximum score of 100 points. Teams will be ranked based on their cumulative score from the highest to the lowest.