University of Michigan-Dearborn

CIS 467, Digital Forensics II

Midterm Exam, Winter 2021

Prof. Birhanu Eshete

March 4, 2021

Instructions:

- This exam has 4 pages including this page.
- This is an open-book examination, i.e., you are free to refer to any lecture materials, books, or online resources.
- You can't collaborate with your classmates/seek help from others.
- **Turn in your answers via Canvas by 11:59AM on Friday, March 5th, 2021**.

Question 1. [9pts.]
Considering FBI, the supreme court, and Walmart as digital forensics stakeholders, for each stakeholder describe their primary objective, secondary objective, and the environment/context of operation.

Question 2. [6pts.]
In the three A's of digital forensics, identify the condition(s) under which:
a) Acquired evidence is rendered useless
b) Authentication results in inconsistency
c) Analysis results are invalid/inconsistent

Question 3. [6pts.]
What are the major sources of digital forensic evidence? Give at least two examples for each.

Question 4. [5pts.]
When we say "Data 'spoils' easily", what do we mean? Explain in terms of implications on effectiveness of forensic analysis.

Question 5. [5pts.]
Suppose you are called on to investigate a compromised computer that was still up and running, connected to enterprise network and the Internet. Considering the evidence volatility order, describe the order with which you perform data collection (what would you collect first, second, third, etc?)

Question 6. [5pts.]
One of the challenges in forensic investigation is the so called "Overlapping Principals" problem. What does it mean to have overlapping principals? Describe the major implication of overlapping principals on the outcome of the forensic investigation.

Question 7. [2pts.]
What common cryptography-based method is used to periodically check whether forensic evidence was contaminated or not?

Question 8. [4pts.]
Suppose you are given a USB stick that is believed to contain consequential forensic evidence that you don't want to be modified even by a single bit. Although you are eager to examine what is inside, you also need to take proper precautions to avoid evidence contamination. Identify two practical methods to preserve the integrity of the information on the USB stick.

Question 9. [3pts.]
State three reasons why we need to do live incident response.

Question 10. [4pts.]
In the context of live incident response, give two examples each for volatile and nonvolatile evidence.

Question 11. [5pts.]
In live incident response data collection, incident evidence can change in two ways. What are they and how do they differ?

Question 12. [6pts.]
Compare and contrast local, remote, and hybrid incident response.

Question 13. [6pts.]
In a remote incident data collection, how do we ensure a) authenticity of evidence and b) secure transfer of evidence between victim host and forensic workstation?

Question 14. [4pts.]
What are the four W's of analyzing incident response data? For each W, give one example of volatile data source.

Question 15. [4pts.]
In the context of live incident response, if periodically running the command for checking disk usage shows consistent drop in free disk space on the victim host, what is the potential implication?

Question 16. [14pts.]
The following questions are based on the JBR Bank case study we studied in Lecture-3.

a) What is the name of the strange file found on one of the JBR computers, and subsequently initiated the incident response mission?

b) What is the IP address of the victim host, the forensic workstation, and the attacker?

c) Based on network connections data that was acquired, list remote IP addresses with active connections.

d) From the "Process –> Port Mapping" data, which line stands out as a potential indication of data ex-filtration from the victim host to the attacker's IP address?

e) The routing tables seemed unchanged? What made the incident response team to conclude so?

f) In the analysis of currently running processes, which executable stands out as a solid indication that the attacker was remotely connected to the victim host? Justify your answer.

g) Why does "CAINE" standout when we analyze running services on the victim host?

Question 17. [4pts.]
In the incident response case study we did for the buildinject.json data, to which category does it belong? Volatile? Nonvolatile? Neither? Justify your answer.

Question 18. [4pts.]
Explain two good reasons for conducting memory forensics.

Question 19. [2pts.]
When using the Volatility framework for memory image forensics, why is it important to know the profile of the memory image under investigation?

Question 20. [2pts.]
Discuss one concrete forensic use case for dumping the DLL list of processes from a memory image.

——————————Good Luck and stay safe! ——————————