Memory Forensics

Course: Senior Design
Instructor: Dr. Kim

Meet the Team

Roli Bolorunfe

Patience Jato

Advisor: Dr. Salmani

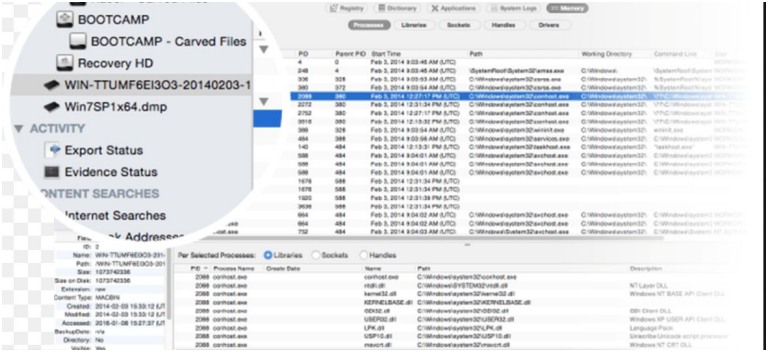
TL: Davia McKenzie

Obi Oguh

Sponsor: Lockheed Martin

What is Digital / Memory Forensics?

- Digital forensics is an investigative technique to identify or collect the information on a digital storage as evidence to expose crimes legally defensible
- It combines investigative techniques and analysis to identify, collect, examine, and conserve information
- Physical memory can provide a lot of valuable information associated with a cyber crime
    - It contains volatile data such as network connections, open files, running processes, loaded drivers, user credentials, browser details, and more.



LOCKHEED MARTIN

Why Memory Forensics

- Used in criminal law and private investigation
- For maintenance
- Debugging
- Data recovery
- Reverse engineering

LOCKHEED MARTIN

Problem Statement and Project Goal

Since commonly known attack methods have become increasingly sophisticated, we must help determine which memory forensic tool provides the best physical memory coverage against those common attack methods in order to support secure operational environments.

Project Goal:

- ➔ Define a methodology that we will use as an attack method
- ➔ Develop the tool requirements and capability comparison

LOCKHEED MARTIN

Capabilities

Example Description:

Tools/Capabilities	X-ways	Axiom	EnCase	Blacklight	Autopsy	Paraben
Forensic String Search	⊗	☑	⊗	☑	☑	⊗
Binary Jtag	☑	☑	⊗	⊗	☑	⊗
Graphic File Carving	☑	☑	⊗	☑	☑	⊗
Video File Carving	☑	☑	☑	☑	☑	⊗
Mobile Device Acquisition	⊗	☑	☑	☑	⊗	☑
Digital Data Acquisition	☑	☑	⊗	⊗	☑	⊗
Deleted File Recovery	☑	☑	⊗	⊗	☑	⊗

end: ☑ Met most - all requirements ☑ Partially met requirements ⊗ Met little - no requirements

Level of Interference	The tool's processes should have minimal interference with the data collected.
Speed	The ability of the tool to get the snapshot as quick as possible.
Snapshot Consistency	The ability of the acquisition tool to faithfully mirror the memory state of a target machine at a given instance of time.
Tamper resistance	The ability for a tool or mechanism to not be infected by malware present in the OS.
Performance Isolation	The ability of the tool to have only minimal impact on the performance of the other applications or processes that may be executing on the system.
Live capturing	The ability of the tool to capture the memory when other applications are executing.

High Priority	Medium Priority	Low Priority
Binary Image JTAG, Chip-off Decoding and Analysis	Mobile devices forensic	Disk Imaging
Digital Data Acquisition	Window Registry	Storage Media Preparation
Forensic String Searching	Network Artifacts	Graphic File Carving
Deleted File Recovery	Software & Hardware Write Block	Video File Carving

LOCKHEED MARTIN

Design Requirements

Product Specification

- **Software Requirements:**
  - OS (Axiom software requires Windows 10)
  - Processor Specification:
    1 GHz or 2.5GHz Dual Core Processor
  - Ram Space:
    2GB for 32 bit or 4GB for 64 bit
  - Hard Disk Space:
    20 GB for 32 bit OS or 40-80 GB for 64 bit
  - Graphics Card:
    Direct x9 or later with WDDM 1.0 driver
  - Display:
    800x600 to 1920x1080
  - Axiom Tool:
    Memory Forensic tool that allows users to identify malware

LOCKHEED MARTIN

Design Requirements

Constraints

- **Cost:** $25,000
- **Time:**
  - Deadline May 2021 to complete findings and methodologies
- **Environmental/Social Responsibility:**
  - Axiom Tool should be able to produce an output that can be understood by a human forensic analyst
  - The result should be actual data

Regulations/Standards

- **Standard/Regulation:**
  - NIST
  - CFFT
- **Standard:**
  - Lockheed Martin Cyber Protection Strategy
  - United States Cyber Command
- **Patent Intellectual Property:**
  - Lockheed Martin (Memory Forensic Tool/Software)

LOCKHEED MARTIN

Solution Ideas

Individual Idea 1: Davia M.

Purpose of our research:

➔ To find the best memory forensic tool that will help to prevent attacks.

Method of Approach:

1. Identify and acquire the data that needs to be protected
2. Process the collected data, extracting important pieces of information
3. Analyze the extracted data
4. Report what was found from analyzing the data

LOCKHEED MARTIN

Individual Idea 2: Roli B.

Following the ‘Investigation Model’ Technique

1. The ‘preparation phase’
2. The ‘imaging phase’
3. The ‘parsing phase’ - extract all variables, virtual addresses and data types
4. The ‘inspection phase’
5. The “reporting phase”

LOCKHEED MARTIN

Individual Idea 3: Patience J.

Creating a tool for data forensics through live technique on the RAM for maintenance, debugging, data recovery, and reverse engineering of computer systems in private settings

1. Collect available data and digital media that requires investigation
2. Examine the data through cloning or imaging the data
3. Analyze and make the recovery to store back the file and the folder
    a. RAM in the computer system will be analyzed
    b. The goal is to find evidence of the intrusion from the attacker.
4. Create scientific reporting and to presenting the investigation report and evidence

LOCKHEED MARTIN

Individual Idea 4: Obi O.

To prevent attacks the process of memory forensics should occur by:

1. Locate the memory or data within the specified memory that is needed
2. Identify the issues within the memory and what are you looking for during the memory forensics process.
3. Acquire the data
4. Extract pieces of information that will be used for further analysis
5. Analyze the extraction
6. Compare analysis to data that theoretically describes what it contents should look like
7. Provide a report that describes the result

LOCKHEED MARTIN

Top Ideas

LOCKHEED MARTIN

Top 2 Concepts

Method 1

- Pros:
  - The process description is straightforward
  - Describes a process from start to finish
- Cons:
  - Process can be seen as vague
  - Doesn't describe where we can locate or isolate the data needed for analysis

Method 2

- Pros:
  - Provides an explicit breakdown of the data forensics process
  - Includes an experimental setup procedure, thereby making it more reliable
  - Easy to follow step-by-step process
  - Relatively simple to implement due to easy accessibility to tools
- Cons:
  - May be time consuming

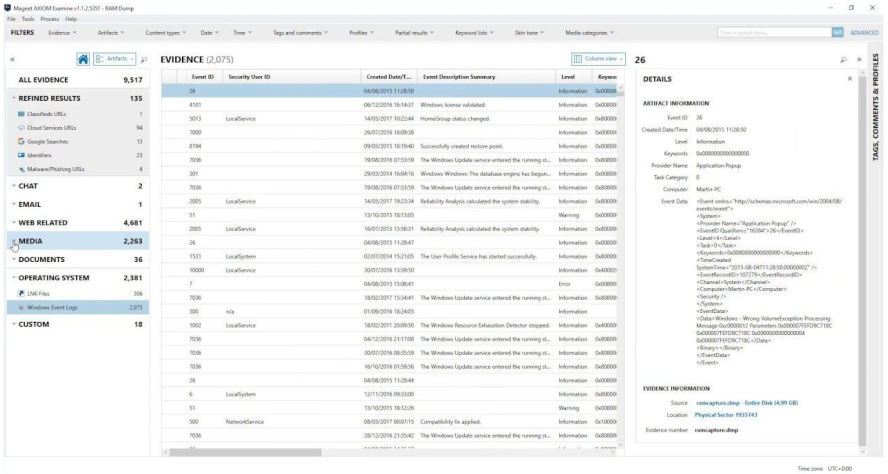
LOCKHEED MARTIN

Decision Matrix

	Method 1	Method 2 **“Investigation Model”**
Efficiency	4	4
Time-Consuming	5	1
Easier to understand	2	4
Practicality	3	4

Top Design Solution: Tools

- **Tool**: Axiom
- License is needed to access and utilize tool



LOCKHEED MARTIN

Top Design Solution

Method 2

Method 2 entails finding data within a given memory location and then compiling an application in order to derive the executable file we want to investigate.

Why Method 2 over Method 1:

- Better pros and cons
- Thorough process (More detailed and clear)
- Best suited for our team short and long term goals
- Method 1 does not have an experimental setup stage to prove credibility

LOCKHEED MARTIN

Top Design Solution: Block Diagram

Create agents
(On attacker computer)

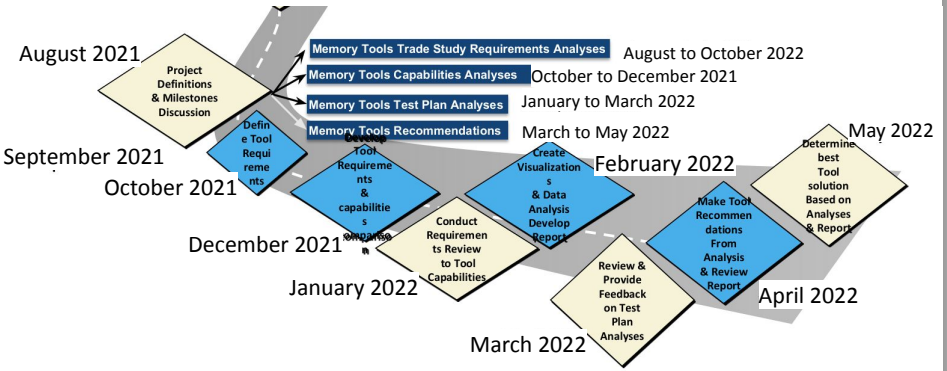
Deploy agents
(To victim computer)

Analyze retrieved data

LOCKHEED MARTIN

Conclusion & Next Steps

- Continuing research on memory forensics by the team to familiarize with field standards
- Getting Axiom license from Lockheed Martin
- Extensive analysis to determination of the best memory forensics tools
- Present findings



LOCKHEED MARTIN

LOCKHEED MARTIN


Questions