

# Memory Forensics



Team Members - Olaide Afolabi, Faith Adegbenro, Grace Owolabi, Prudence Phillips



Faculty Advisor – Dr Hassan Salmani



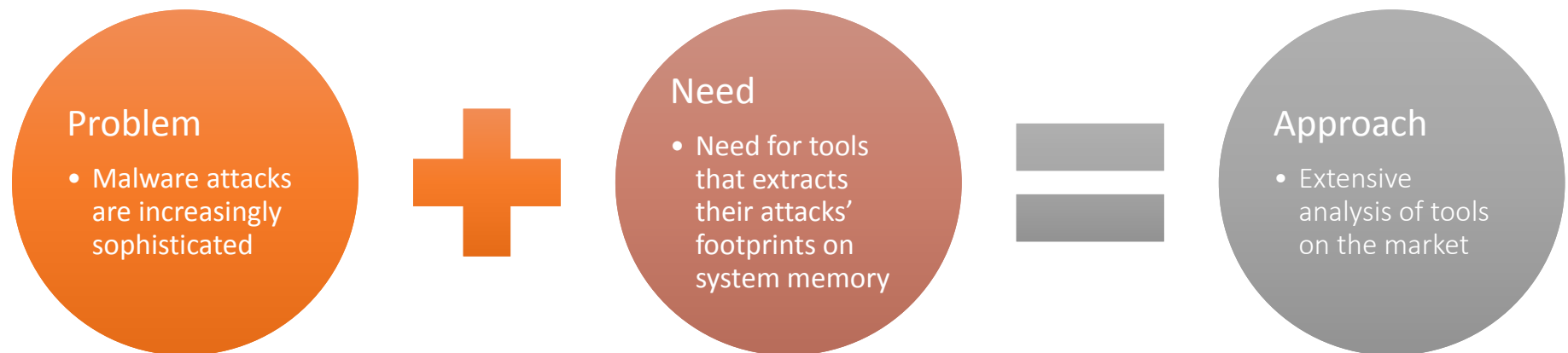
Sponsor – Lockheed Martin



Date: April 13<sup>th</sup>, 2021



# Problem Definition



# Design Requirements

Requirements	Definitions
Usability	The ability to present data in a form that is useful to an investigator.
Comprehensive	The ability to present all data to an investigator so that both inculpatory and exculpatory evidence can be identified.
Accuracy	The quality of the output of the tool has been verified.
Deterministic	The ability for a tool to produce the same output when given the same set of instructions and input data.
Verifiable	The ability to ensure accuracy of the output by having access to intermediate translation and presentation results.
Tested	The ability to determine if known data present within the mobile device internal memory is not modified and reported accurately by the tool.
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.

# Solution Design

IDENTIFY DECISIONS AND OBJECTIVES OF STUDY



BASELINE IN TERMS OF SCOPE, SCHEDULE AND RESOURCES



DEVELOP MATRIX AND CRITERIA FOR STUDY



IDENTIFY AND TEST TOOLS



CREATE VISUALIZATION AND RECOMMENDATIONS

# Categorization

## Planned Task:

- Categorize Memory Forensics' segments into high- medium- low priorities;
- Choose top 3 tools for high priority segments based on their functionality and availability.

### High Priority

Binary Image JTAG, Chip-off Decoding and Analysis

Digital Data Acquisition

Forensic String Searching

Deleted File Recovery

### Medium Priority

Mobile devices forensic

Window Registry

Network Artifacts

Software & Hardware Write Block

### Low Priority

Disk Imaging

Storage Media Preparation

Graphic File Carving

Video File Carving

# Acquisition.

## Planned Task:

- Contact the different tools vendor to get the price quote, trial, and demos;
- Use an online RAM sample to test the tool during the trial period;
- Choose the top 3 tools based on performance that satisfy the high priority segments;
- Purchase tools.

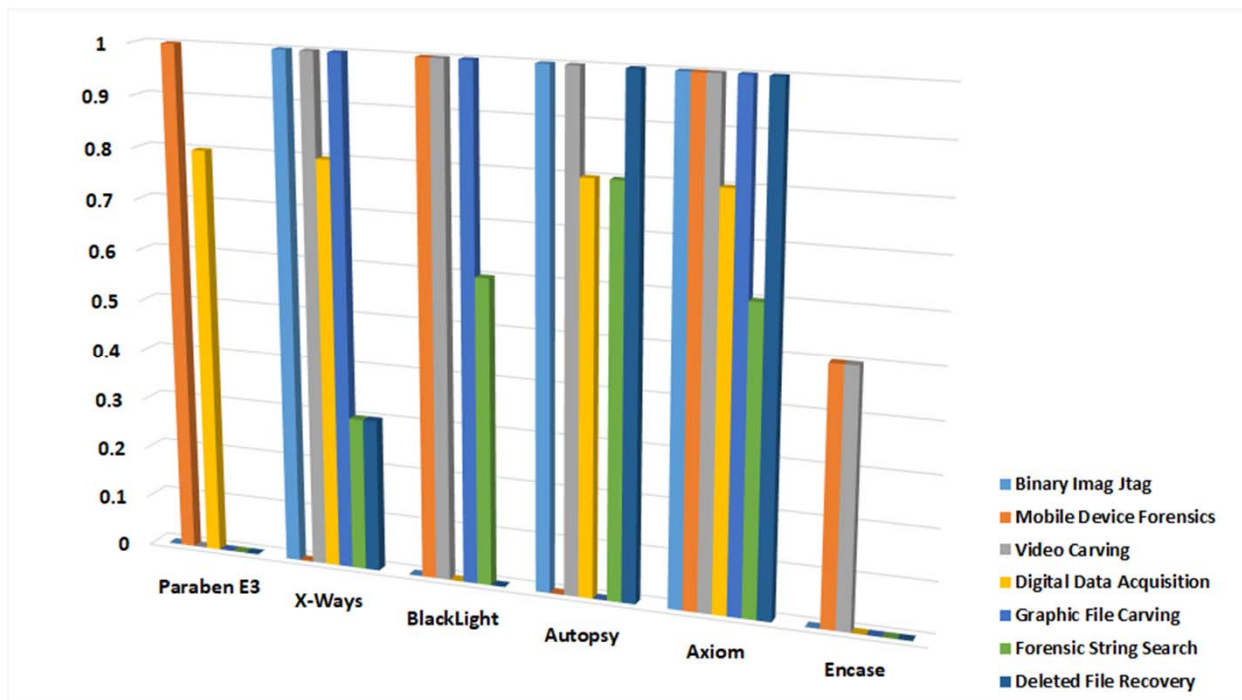
Tools/Capabilities	X-ways	Axiom	EnCase	Blacklight	Autopsy	Paraben
Forensic String Search	⊗	☑	⊗	☑	☑	⊗
Binary Jtag	☑	☑	⊗	⊗	☑	⊗
Graphic File Carving	☑	☑	⊗	☑	☑	⊗
Video File Carving	☑	☑	☑	☑	☑	⊗
Mobile Device Acquisition	⊗	☑	☑	☑	⊗	☑
Digital Data Acquisition	☑	☑	⊗	⊗	☑	⊗
Deleted File Recovery	☑	☑	⊗	⊗	☑	⊗

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

# Testing and Examination

## Planned Task -

- Test tools with real data to see their actual performance;
- Test tools for medium and low capabilities.



# Conclusions



Though we faced many challenges, we were able to test a lot of tools and make reasonable comparisons



The final selected tool met most of the criteria, and the sponsor is willing to continue testing the tool accordingly



# Demo

The screenshot displays a network management software interface. The main window is titled "MATCHING RESULTS (1178 out of 2000)". It features a table with columns for "Name", "Status", "IP Address", and "MAC Address". The table lists various network devices, including switches and routers, with their respective IP and MAC addresses. On the left side, there is a navigation pane with categories like "OVERVIEW", "OVER RELATED", "OVERVIEW", "SOCIAL NETWORKING", "MEDIA", "EMAIL", "DOCUMENTS", "MOBILE", "OPERATIONAL SYSTEM", "CUSTOMER", and "CUSTOM". On the right side, there is a "DETAILS" pane for the selected device, showing its configuration and status. The interface is designed for monitoring and managing network infrastructure.

Questions

