## Memory Forensics



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

Faculty Advisor – Dr Hassan Salmani

Sponsor – Lockheed Martin



Date: April 13th, 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

## Planned Task: Categorize Memory Forensics' segments into high- mediumlow priorities; Choose top 3 tools for high priority segements based on their functionality and availability.

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

#### Planned Task:

#### Acquisition.

- 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	$\otimes$		$\overline{\times}$			$\times$
Binary Jtag			$\times$	$\times$		$\mathbf{X}$
Graphic File Carving			$\otimes$			$\overline{(x)}$
Video File Carving		$\checkmark$				$\overline{\times}$
Mobile Device Acquisition	$\otimes$				$\times$	
Digital Data Acquisition			$\times$	$\overline{\mathbf{x}}$		$\otimes$
Deleted File Recovery			$\times$	$\otimes$		$(\times)$
end: 🔽 Met most -	all requiremer	nts 🗹 Par	tially met requ	uirements	🚫 Met litt	le - no requirer

# Testing and Examination

Planned Task -

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

![](_page_6_Figure_4.jpeg)

## Conclusions

![](_page_7_Picture_1.jpeg)

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

![](_page_7_Picture_3.jpeg)

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

### Demo

		Construction of the second sec	Provide and the American	and the second second	. the set	
N. Contraction	1.1	MANEHING RESIDENCES (1911)			100	- +
Commit and theme II.	10.00	Come (	Name .	and a second second	There and there is a long of	Think for White
Statement Streetwart	10.0	La canada a far forana interactive a tr	In the second second	and the second se		
and the second	i dente i	and the first state of the stat	In the section of some		the off sales on	
		and the anti-art that the	and Income a lines	These -		04744.5
College Print, Special Co.	2.4	1 10 1 10 10 10 10 10 10 10 10 10 10 10	and the strength of the state o	Char	Bridger Laker and	A CONTRACTOR AND A CONTRACTOR OF A
manual dependences in the second	A. C		and an an an an and a second second	100	the state of the s	and and a second second second
manufactor because	10 million (1997)		III Andread and a	1.100	Contraction of the second second	The second se
Assessed interaction of the local division o	1.1	and a second sec	The surger states		state water in the local state	Lange the
Comment of the Party of the		100.75250	White American Advertise	1.00		palatrata P
		- Marchanet	Without Service	10.00		No. Award
and the second se		-100700-000	All brighter totals	1000		Characteristic and Department of the
Theorem Property		comparison of the data data water	Witness and	- Come	And a second distance with	tere manufacturation and term
Desire Francisco		company of the bar strengt	OF LABOR DESIGN		Contraction and a state of the state	Printing and the second s
Straining Brooking Building	1.100	and the other states the second	The Association of Concession of Concession, Name	1000	- 10 Contraction 10 (10-10-10-10-10-10-10-10-10-10-10-10-10-1	the state of the second st
	10000	Constitute 1975, Get (Margar	The Associate State	Circu.	personal disectories	No. of the State o
		A data from A BARCONG, BORNAGE	AND Revenues and the	Contract of Contract of Contract	The second second second second	etreside he de la
		same that will the heread.	Witness Contraction Contraction		- The second control (second	and a first and a rest
the second se		And a state of the	The second secon		CONTRACTOR OF AND	Page 1
Stational Conf.	# C 2	Transmission and Characteristic	With the second se	1.100	Comparent Statistics and	trag anality targ
Teating land	-	Constrained APC (Section of Constraining)	The Average Street, or	- (7mm)	service and the second second	
And a second second		Advertised (#75,000,000mg)	Bill Annual Series	- Creat	Concerning in case load water	**
		Construme of Party Street Constru-	And Address of Content	and the second sec	The second second second	allaria autoritazoite a pinta
and the second se	0.000	completion of Physics, Names	Without control of	10.00	Concerning and address.	
		constraint (FRC2), (constraint)	The spectrum states	1 (free )	CONTRACTOR SALES AND	818
	-		Bill Service States		CONTRACTOR OF A DATA STATE	
Concernence and Concernence an	1 March 10	- The states of	Without State	(Creek)	the set of the set	teritoria de la companya de la compa
and the second se	1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1	Anna Anna Artificiana, Managa	THE ADDRESS STORE	- 04	and the particular sector sect	CT COLOR OF
5-52 in a second second second	(1997) - 1997 - 1997 - 1997 - 1997 - 1997 - 1997 - 1997 - 1997 - 1997 - 1997 - 1997 - 1997 - 1997 - 1997 - 1997	control the start of the plantage	Branches State	- Comp.	The second se	No. 2 Contraction of the second
Million and Strategical	2010	Line far 1972 Sec. King I	(Planker) (Pl	1744		
	1000	Construction of the Data Street of	and Analysis and the second second		The second secon	etersee.
		Construction of the Construction	We handware black	17 mail	Contraction of the second second	
Automation .		And ben All Stratement	IP Avaluation		United to be a set of the set of	de la serence

Terration, 200-000

## Questions

![](_page_9_Picture_1.jpeg)