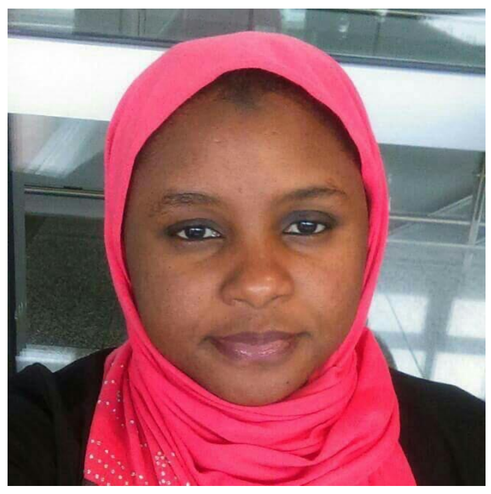
CRII: SaTC: Leveraging Userland In-Memory Objects for Cybercrime Investigations and Malware Classification

Aisha Ali-Gombe
Towson University
https://wp.towson.edu/aaligombe/research/

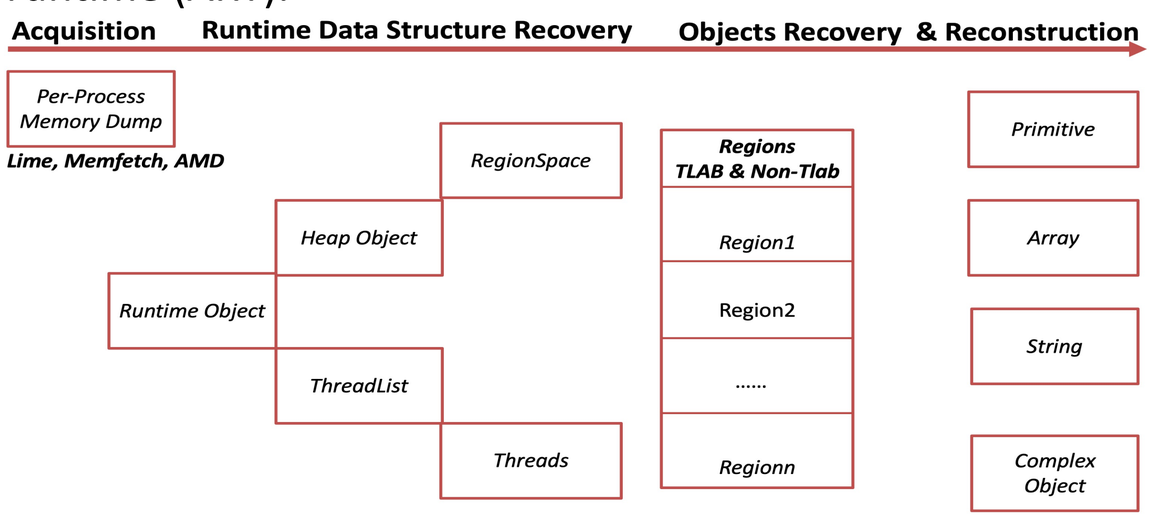


Abstract - In this research, we developed multi-faceted utilities for investigating Android applications leveraging userland in-memory artifacts. The research addresses the limitation of existing app-specific and malware analysis techniques by introducing a novel app-agnostic memory forensics-based approach.

- Task I – tools for the recovery, reconstruction and semantic analysis of the in-memory artifacts.
- Task II – leveraging the in-memory artifacts for malware analysis and categorization using neural and non-neural networks algorithms.

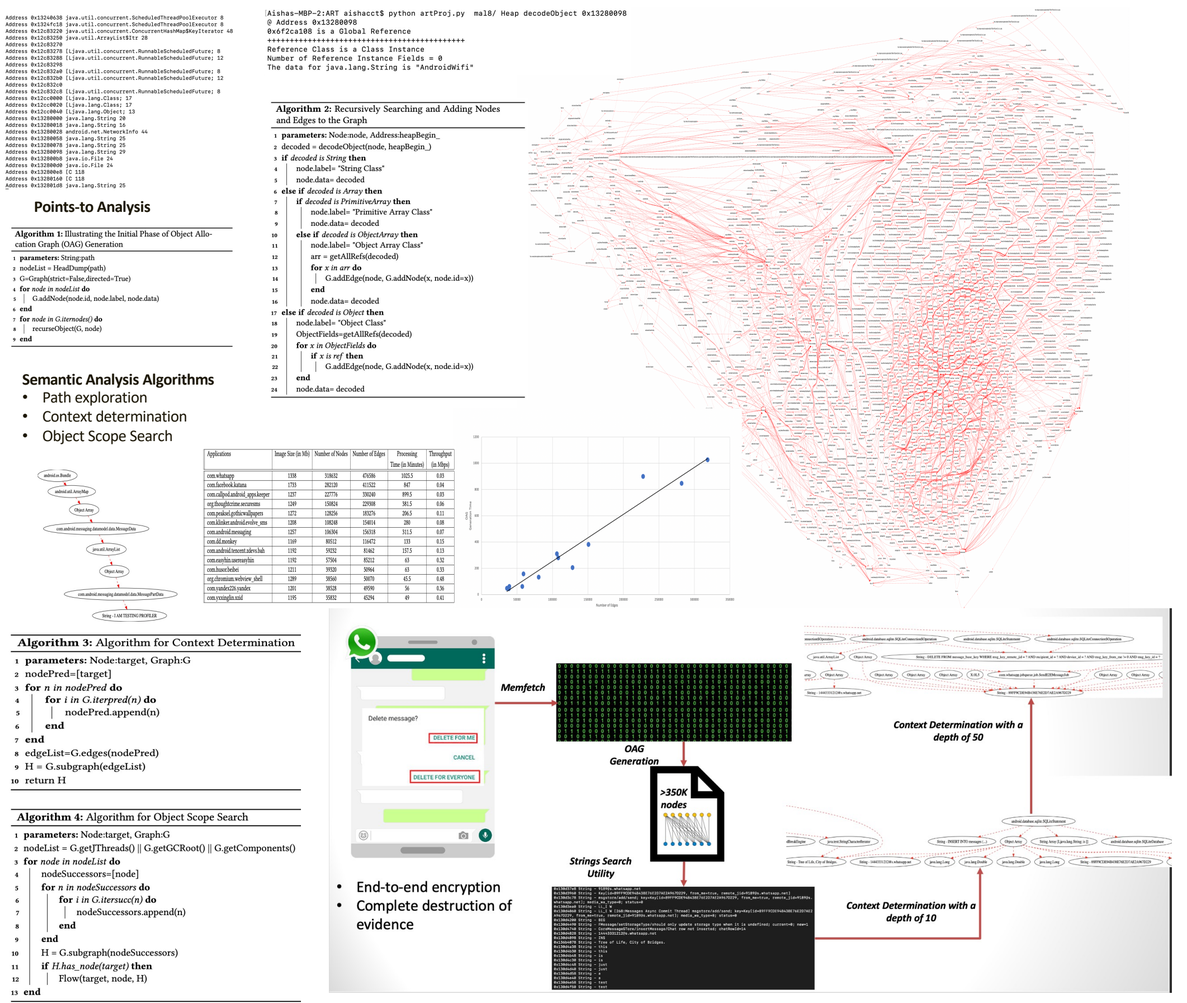
Cybercrime Investigations

Droidscraper is a tool for android in-memory object recovery and reconstruction that targets the new Android runtime (ART).



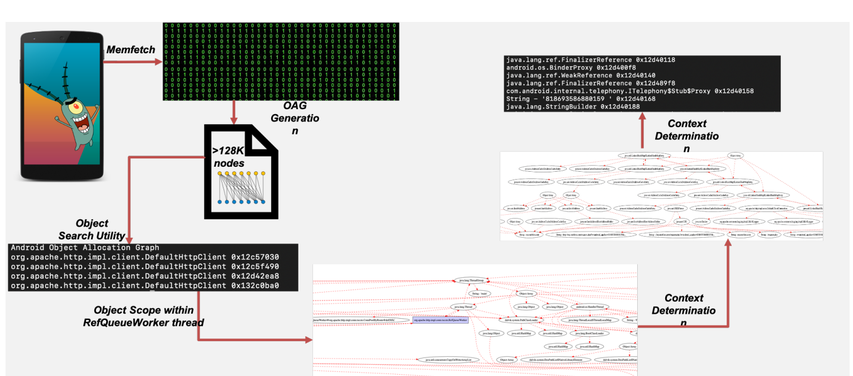
Applications	Threads	Regions	Total Objects	Primitives	Arrays	Strings	Objects	Total Recovered	%
com.baidu.mbaby	16	3	2780	6	526	671	1235	2438	87.7
com.losg.netpack.BaApp	28	10	12493	77	2555	1929	6436	10997	88.1
com.caf.fmradio	15	7	7707	43	3016	1126	2878	7063	91.6
com.yandex226.yandex967	30	12	10346	161	2126	1547	5895	9729	94
cn.myhug.baobao	30	17	50529	133	6410	8571	12025	44297	87.7
com.easyhin.usereasyhin	31	15	29654	2847	6856	5391	29203	27139	91.5
Keeper	44	102	264237	2623	71823	39507	107348	221301	83.8
CalculatorVault	53	22	44757	271	8464	7320	23225	39280	87.8
ClockVault	87	31	99641	2428	15664	10287	60309	88688	89
EvolveSMS	24	36	33234	169	6565	6195	18530	31459	94.7
Signal	36	48	287650	129599	22671	24369	79528	256167	89.1
Chrome Browser	31	11	20628	208	3563	4566	10315	18652	90.4

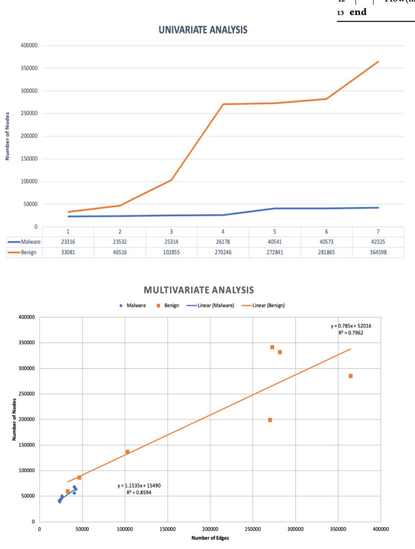
OAGen a post-execution and app-agnostic semantic analysis approach designed to help investigators establish provenance and relationships between in-memory objects.



Malware Analysis

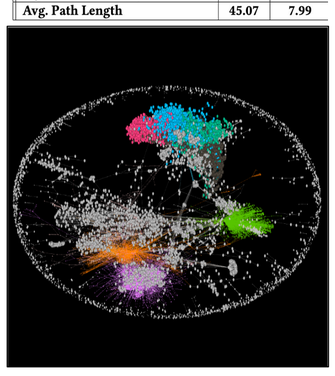
Leveraging memory forensics for malware analysis and Categorization.



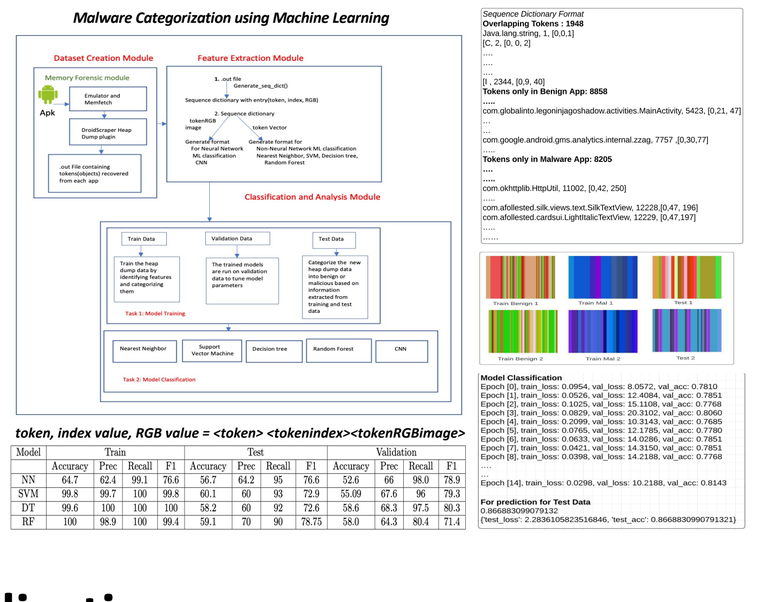


Network Analysis

Metrics	Benign	Malware
Communities	**71837**	**4471**
Average Degree	2.35	3.24
Network Diameter	**41**	**33.86**
Weakly Connected Components	**71511**	**4446**
Avg. Clustering Coefficient	0.07	0.08
Eigenvector Centrality	1.15	0.32
Avg. Path Length	**45.07**	**7.99**



Malware Categorization using Machine Learning



token, index value, RGB value = <token> <tokenindex><tokenRGBimage>

Model	Train				Test				Validation			
	Accuracy	Prec	Recall	F1	Accuracy	Prec	Recall	F1	Accuracy	Prec	Recall	F1
NN	64.7	62.4	99.1	76.6	56.7	64.2	95	76.6	52.6	66	98.0	78.9
SVM	99.8	99.7	100	99.8	60.1	60	93	72.9	55.09	67.6	96	79.3
DT	99.6	100	100	100	58.2	60	92	72.6	58.6	68.3	97.5	80.3
RF	100	98.9	100	99.4	59.1	70	90	78.75	58.0	64.3	80.4	71.4

Broader Impact - Society

We developed free, open source tools and datasets that will aid in a more efficient and accurate cybercrime investigation and malware analysis.

- Droidscraper – https://github.com/apphackuno/DroidScraper.git
- OAGen – https://github.com/apphackuno/OAGen.git
- Datasets (to be released) - 5600 process memory images, 1400 heapdumps, 100 object allocation graphs

Broader Impact - Education

- Trained 1 graduate and 6 undergraduate students
- Workshop at WiCyS 2021 - "***Android Reverse Engineering"***
- Workshop at ACM CAPWIC - "***The Basics of Mobile Malware Analysis"***

Publications

- Ali-Gombe, A., Sudhakaran, S., Case, A., & Richard, G. (2019). DroidScraper: A Tool for Android In-Memory Object Recovery and Reconstruction. RAID 2019.
- Ali-Gombe, A., Tambaoan, A., Gurfolino, A., & Richard III, G. G. (2020). App-Agnostic Post-Execution Semantic Analysis of Android In-Memory Forensics Artifacts. ACSAC 2020.
- Hussaini, A., Zahran, B., & Ali-Gombe, A. (2021). Object Allocation Pattern as an Indicator for Maliciousness-An Exploratory Analysis. ACM CODASPY 2021.
- Zahran, B., Hussaini, A., & Ali-Gombe, A. (2021). IIoT-ARAS: IIoT/ICS Automated Risk Assessment System for Prediction and Prevention. ACM CODASPY 2021.
- Miller, E., Rahman, Md R., Hossain, Moinul, Ali-Gombe, A. (2022). I Don't Know Why You Need My Data: A Case Study of Popular Social Media Privacy Policies. ACM CODASPY 2022.