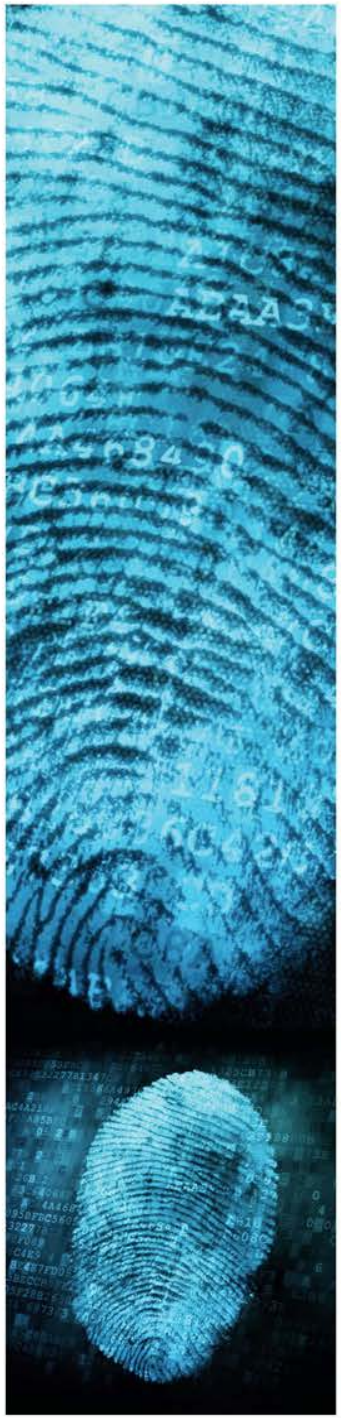
DIGITAL FORENSIC INFORMATION INTELLIGENCE (DFII) SITE

Center for Advanced Research in Forensic Science (CARFS)

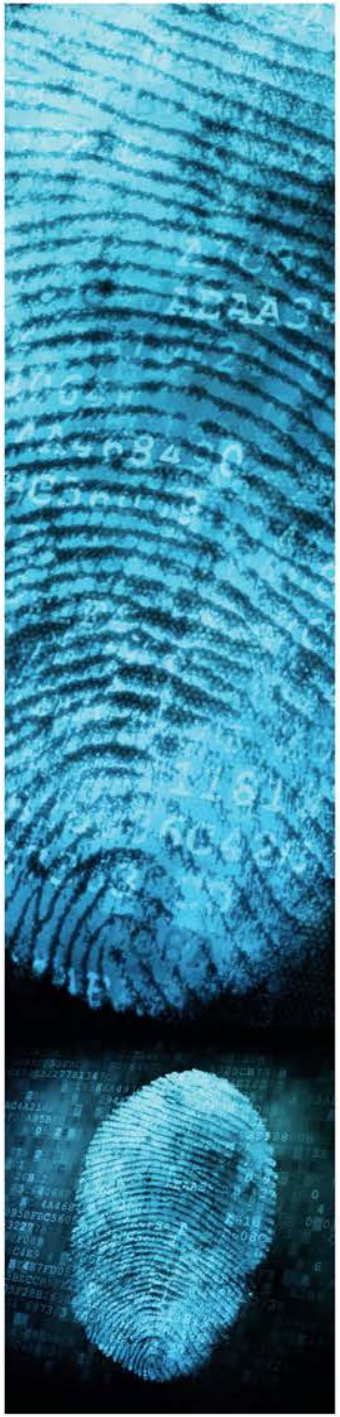
Speaker:
Dr. Brad Glisson
PI: Dr. Jordan Shropshire

August 14, 2017



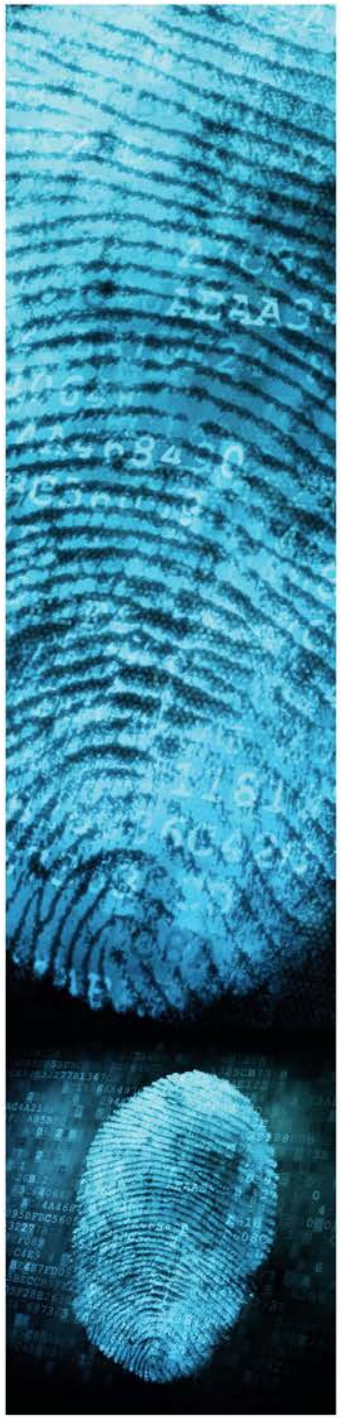
Visual Analytics for Cloud Ecosystems

Project Information	Attributes
PROJECT ID	DFII-7
TYPE	[X] New
START DATE	January, 2018
PROJECT LEAD/PARTICIPANTS	Students; Dr. Jordan Shropshire; Dr. Ryan Benton



Industry Relevance

- This research develops a new, out-of-band model for monitoring the integrity of VMs.
- It uses visual analytics to identify malware embedded within guest operating systems, files, and software.
- The proposed approach renders a two-dimensional, colored depiction of each guest's disk image.
- Depictions are analyzed using a pattern recognition algorithm.

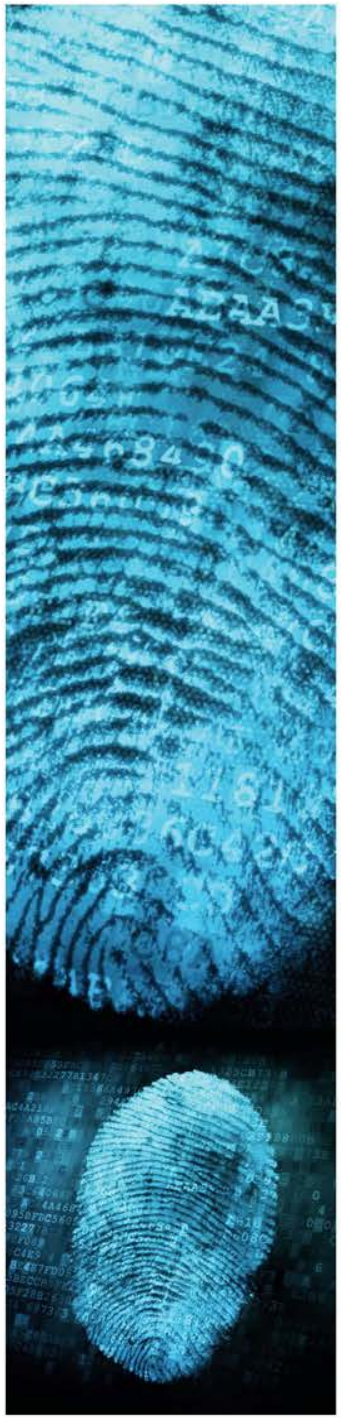


Project Goals/Milestones

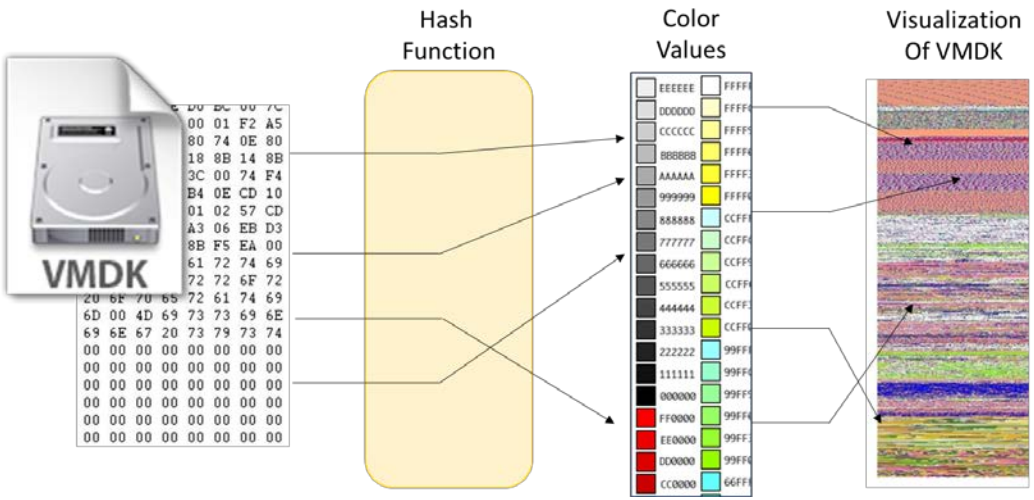
4 months: Automate process of VM image creation

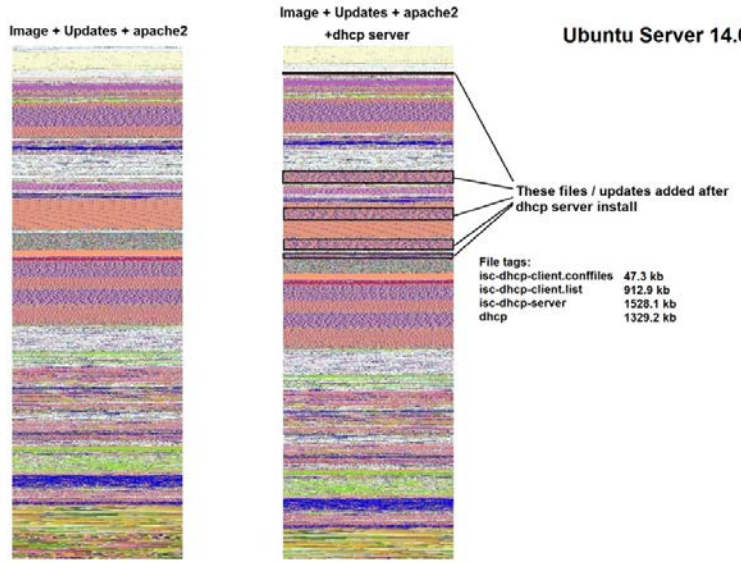
8 months: Create database and implement machine learning algorithm

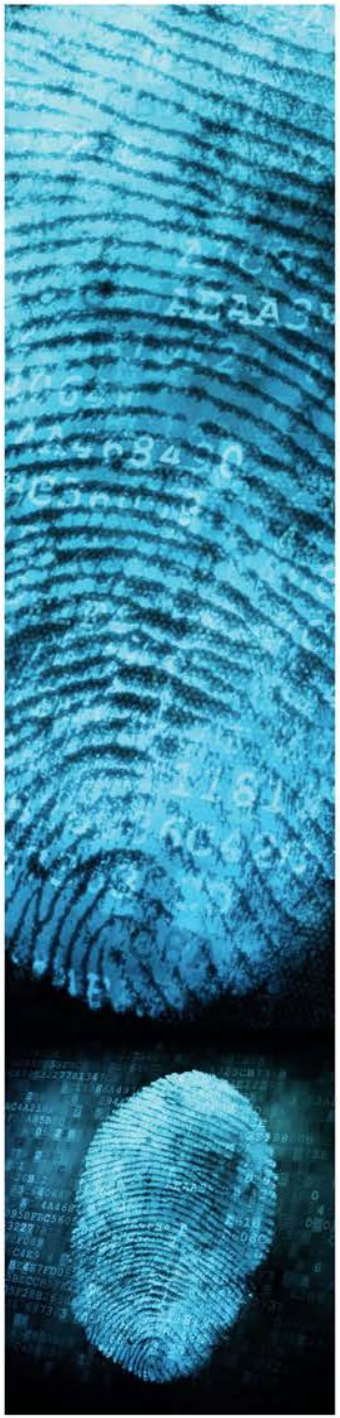
12 months: Train algorithm and assess effectiveness of anomaly detection, rule-based detection, and signature based detection.



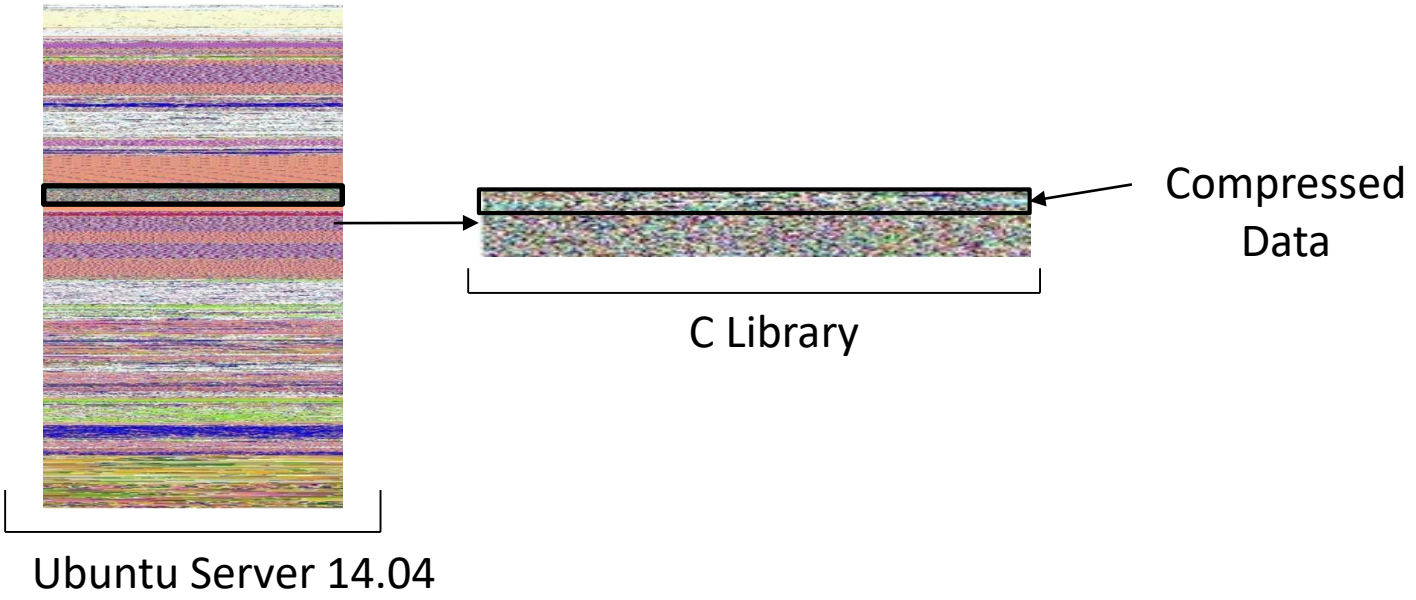
Experimental Plan/Approach



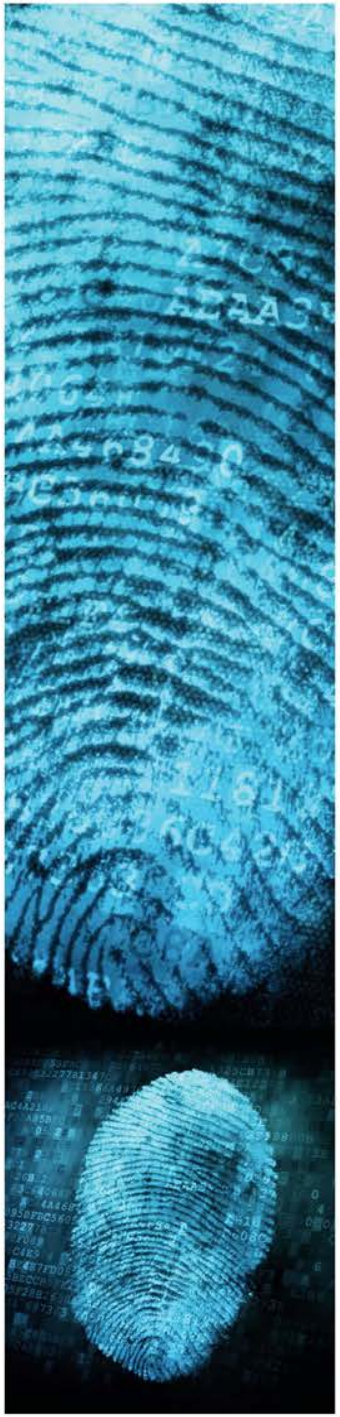




Experimental Plan/Approach

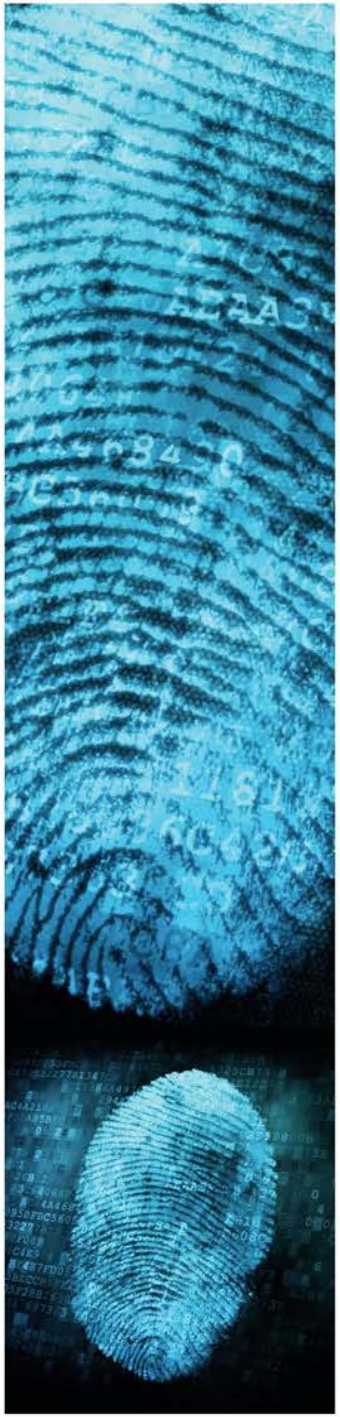


- Implement and test the effectiveness of the proposed visual detection methods
- Compare against prevailing detection methods



Deliverables

- An algorithm for efficient conversion of virtual machine / container / unikernels images into visual depictions.
- A database of tagged samples to support supervised training of machine learning algorithms for cloud security.
- An implementable machine learning algorithm for detecting compromised guests



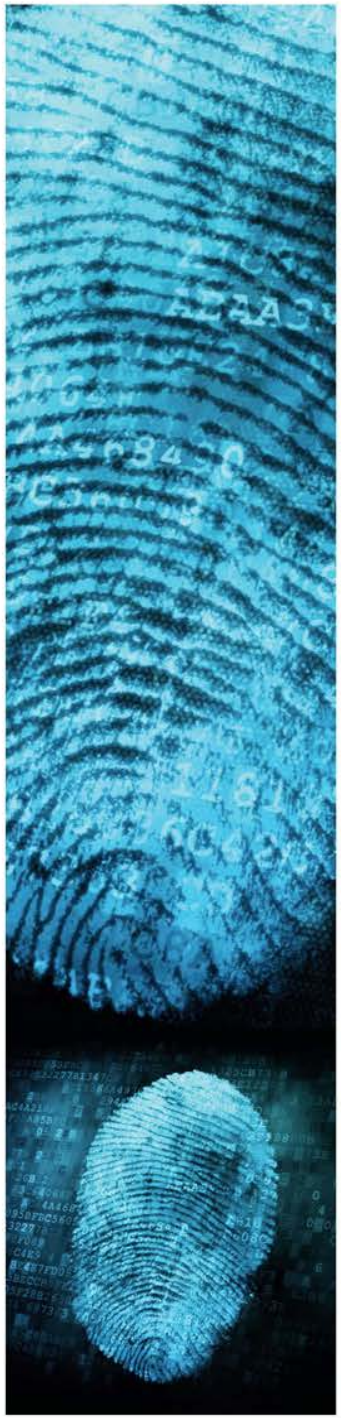
Impact

ECONOMICS

Personalized security services without giving up control of their virtual machines and cloud service providers can provide value-added services without the additional liabilities associated with direct access to client images. This results in an increase in billable services for hosts and increased security for clients.

POTENTIAL MEMBER COMPANY BENEFITS

Tenants want managed security services for their virtual machines but do not wish to relinquish their privacy expectations. If successfully, this research will provide a commercially-viable solution to a problem with a defined market.



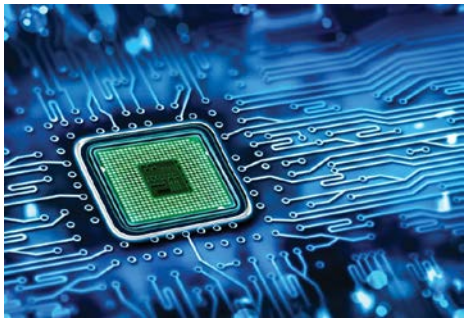
Duration & Budget

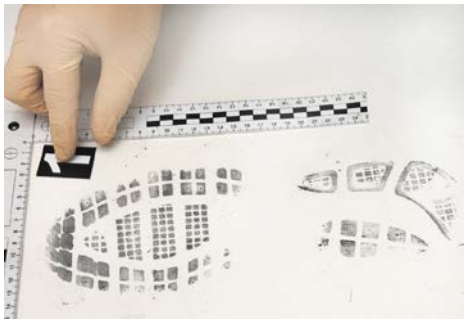
Duration: 12 Months

	1 Ph.D.
Students	32,586
Equipment	2,800
Travel	2,800
Overhead (10%)	3,814
Total	42,000

DIGITAL FORENSIC INFORMATION INTELLIGENCE (DFII) SITE

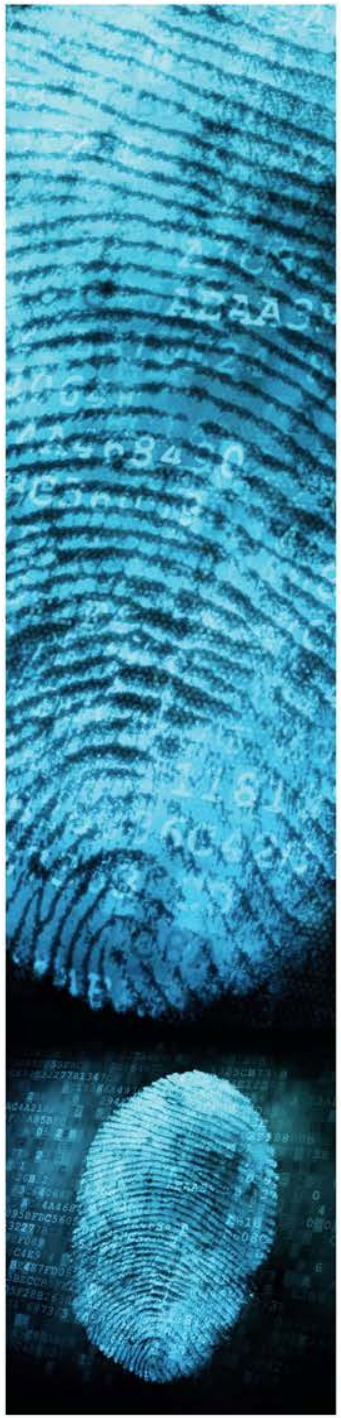
Center for Advanced Research in Forensic Science (CARFS)





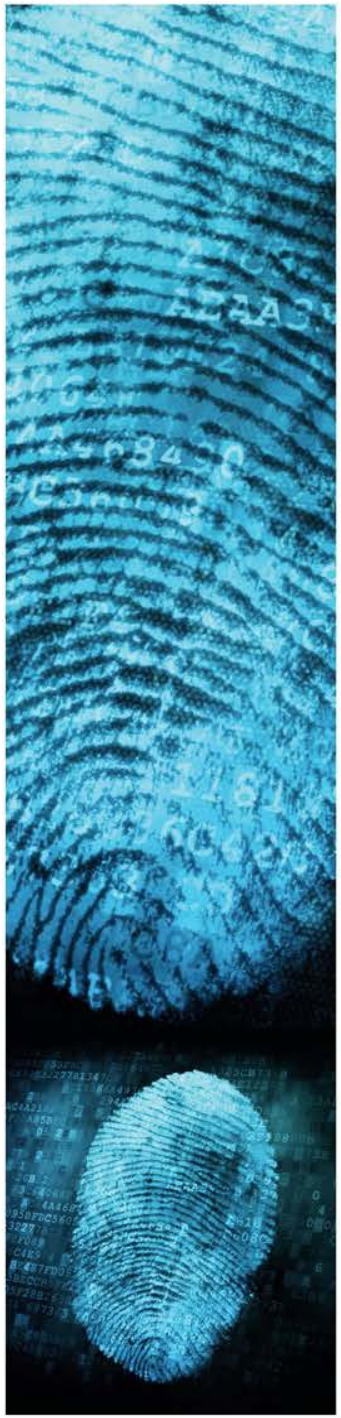

Speaker:
Dr. Brad Glisson
PI: Dr. Todd McDonald

August 14, 2017



Hardware-Based Exploitation and Forensics Evaluation of iOS Devices

Project Information	Attributes
PROJECT ID	DFII-16
TYPE	[X] New
START DATE	January, 2018
PROJECT LEAD/PARTICIPANTS	Students; Dr. Todd McDonald Dr. Todd Andel Dr. Brad Glisson

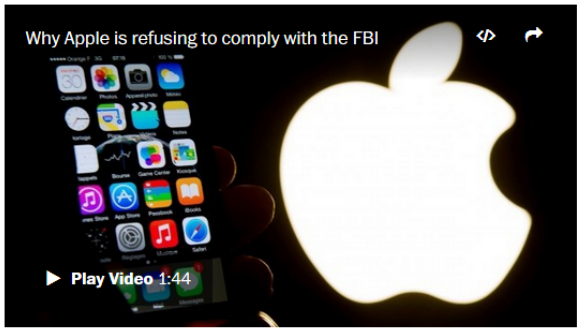


Industry Relevance

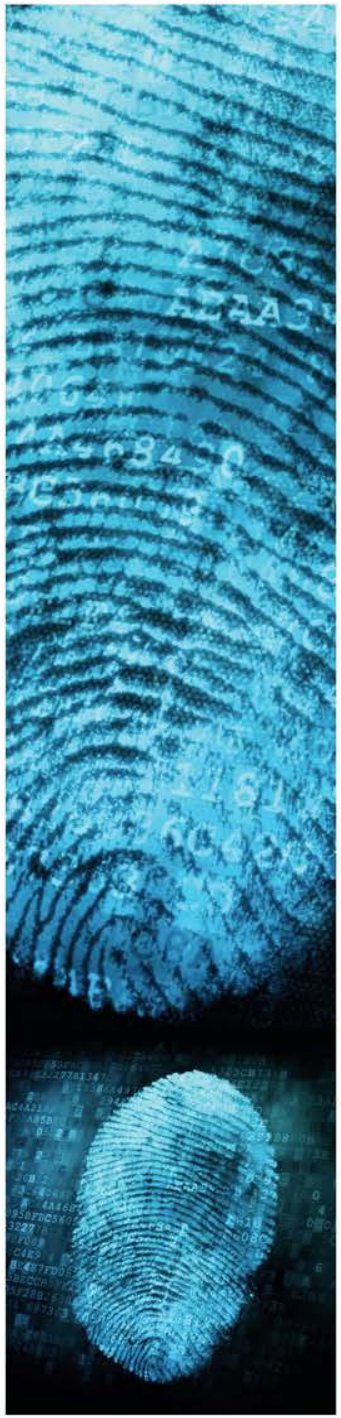
- iOS (iPhone Operating System) devices provide some of the best privacy preserving security features for any mobile device currently
  - Secure boot chain
  - System software authorization
  - Secure Enclave
  - Touch ID
- When iOS devices are used for **nefarious** purposes, forensic analysis of iOS devices can be problematic
  - Device level data encryption
  - Data erasure on too many failed attempts
- Unlock scenarios are of particular relevance for incident response in industry and government sectors

National Security

Apple vows to resist FBI demand to crack iPhone linked to San Bernardino attacks



Apple CEO Tim Cook released a statement arguing against the FBI's recent order to



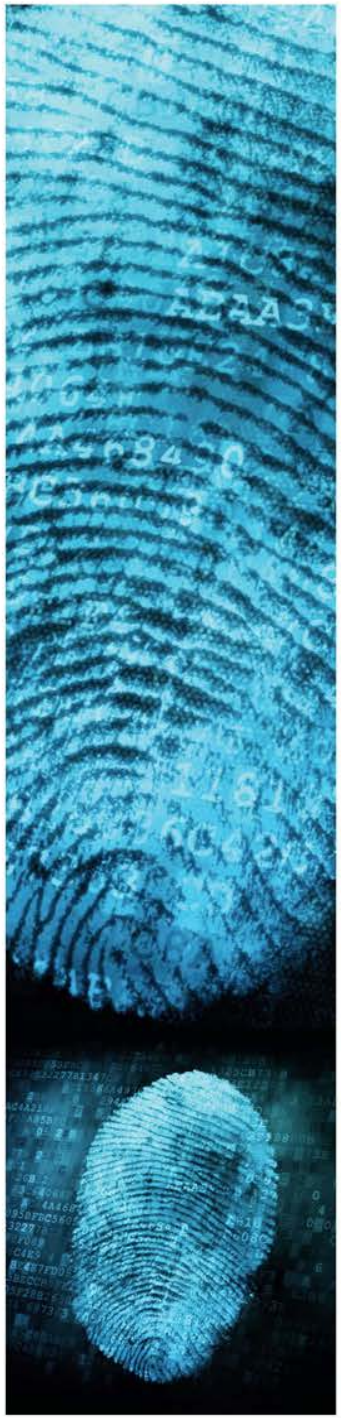
Project Goals/Milestones

Goals

- Develop list of exploitation tools / vulnerabilities by version
- Demonstrate breadboard functionality
  - Data collection of iOS electromagnetic signals
  - Control of iOS functions using specific

Milestones

- **4 m**: Research / acquire tools and techniques for iOS exploitation based on version families, focusing on unlock scenarios.
- **8 m**: Setup breadboard functionality for EM analysis and input control of iPhone.
- **12 m**: Gather relative data and build expertise for hardware-based exploit demonstration on iOS devices relative to unlock scenarios.



Experimental Plan/Approach

How are iOS devices currently exploited (depending on iOS version or iPhone family)?

ACEDECEIVER: FIRST IOS TROJAN EXPLOITING APPLE DRM DESIGN FLAWS TO INFECT ANY IOS DEVICE

POSTED BY: Claud Xiao on March 16, 2016 5:00 AM

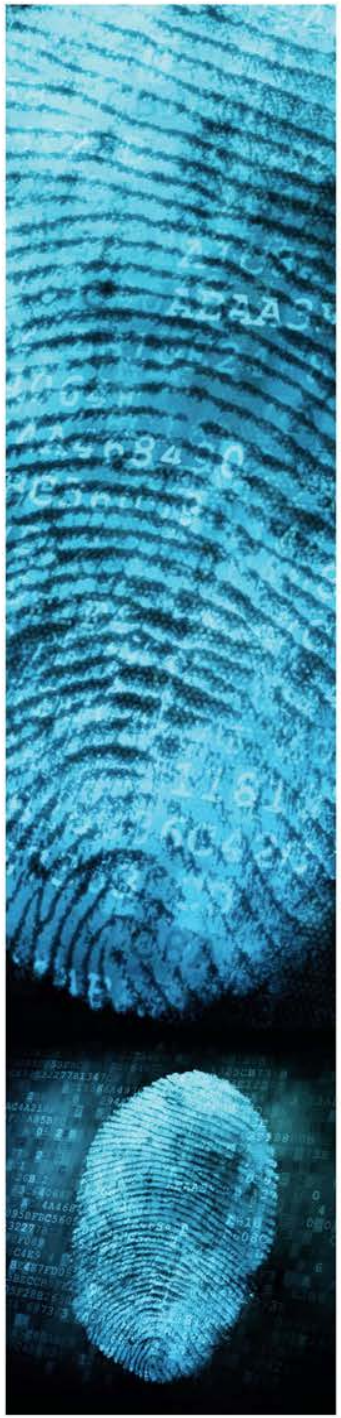
FILED IN: Unit 42
TAGGED: AceDeceiver, FairPlay, OS X, Trojan, ZergHelper

We've discovered a new family of iOS malware that successfully infected non-jailbroken devices we've named "AceDeceiver".

Pegasus iOS exploit uses three zero days to attack high-value targets

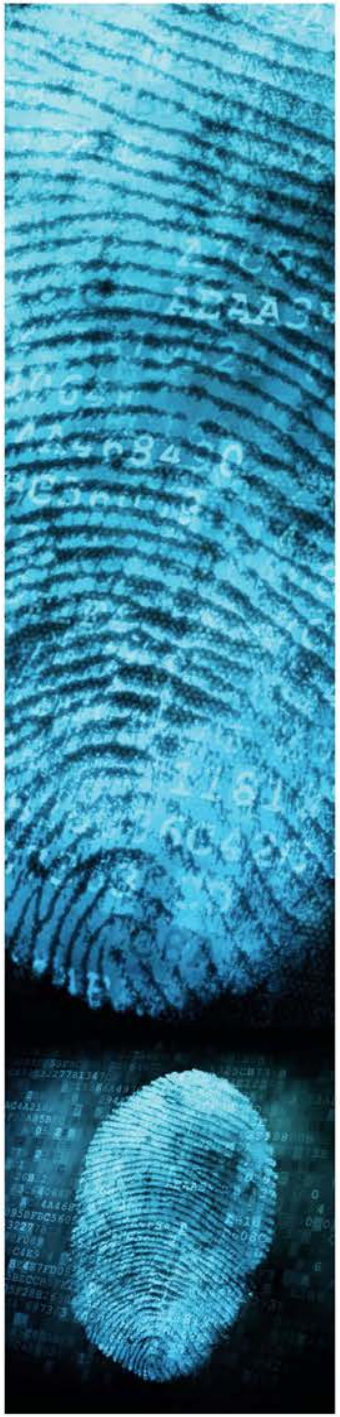
by
Michael Heller
Senior Reporter

Published: 29 Aug 2016



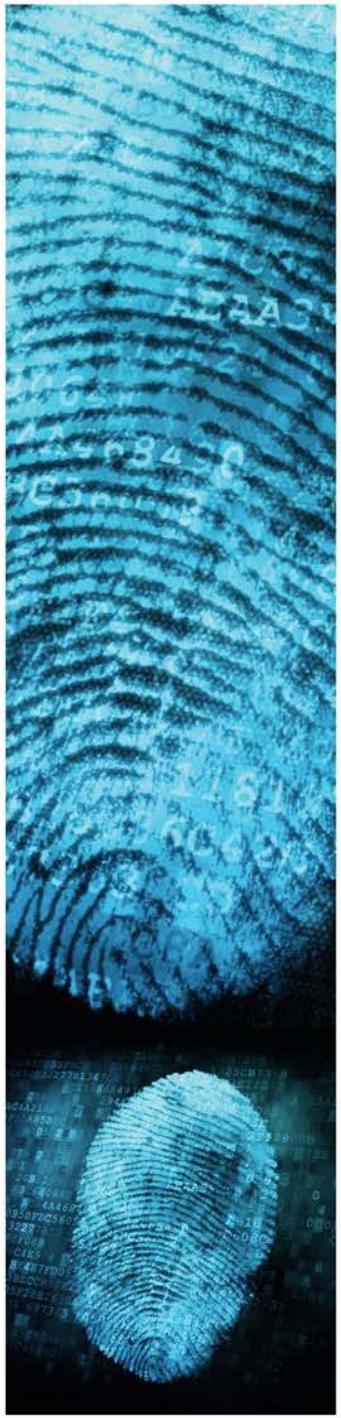
Experimental Plan/Approach

- Set up breadboard environment
- Understand and demonstrate:
  - Control
  - Manipulation
- Effects of
  - Low-cost EM
  - Glitching



Deliverables

- A list of exploitation techniques for iOS based on version families including existing tools/products, vulnerabilities, software-based techniques, and hardware-based exploits
- A demonstration framework for breadboard iPhone setup to conduct hardware-based studies relative to unlock scenarios
- Data results for initial studies using low-cost EM-based probing of an iPhone device



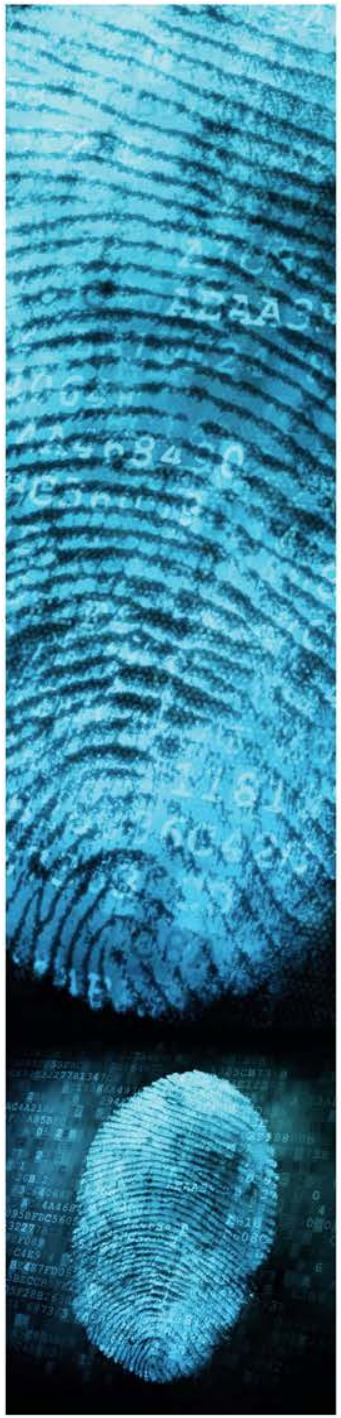
Impact

ECONOMICS |

- Considerable market in law enforcement, government, and industry to assist forensic examiners faced with locked iOS devices.
- Identifying, categorizing, and realizing a demonstration framework for techniques that provide solutions for this unique iOS problem would provide great opportunity in these sectors.

POTENTIAL MEMBER COMPANY BENEFITS |

- Will provide a list of potential iPhone vulnerabilities by iOS version family to IAB members
- Will provide prototype demonstration capability for forensic data recovery from locked iPhone devices



Duration & Budget

Duration: 12 Months

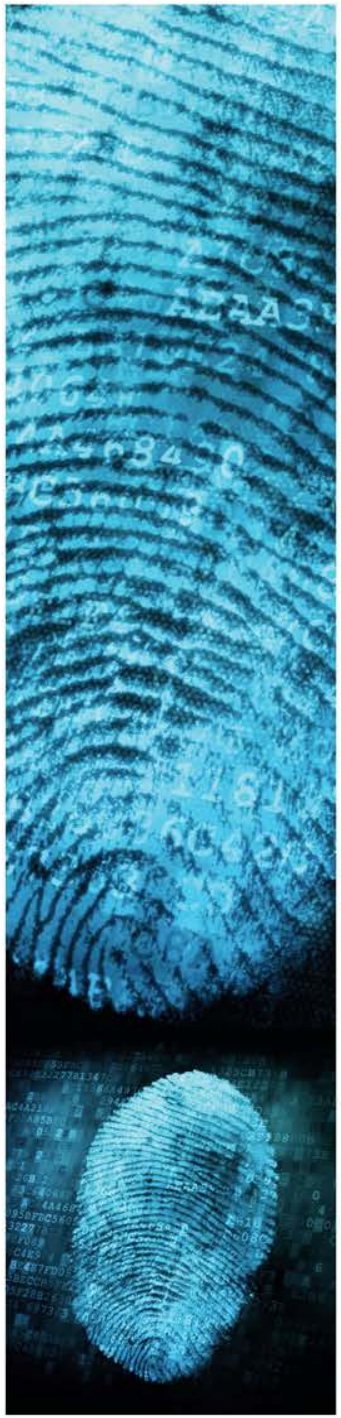
	1 MSc.	1 Ph.D.
Students	28,108	31,818
Equipment	2,300	-
Travel	1,410	-
Overhead (10%)	3,182	3,182
Total	35,000	35,000

DIGITAL FORENSIC INFORMATION INTELLIGENCE (DFII) SITE

Center for Advanced Research in Forensic Science (CARFS)

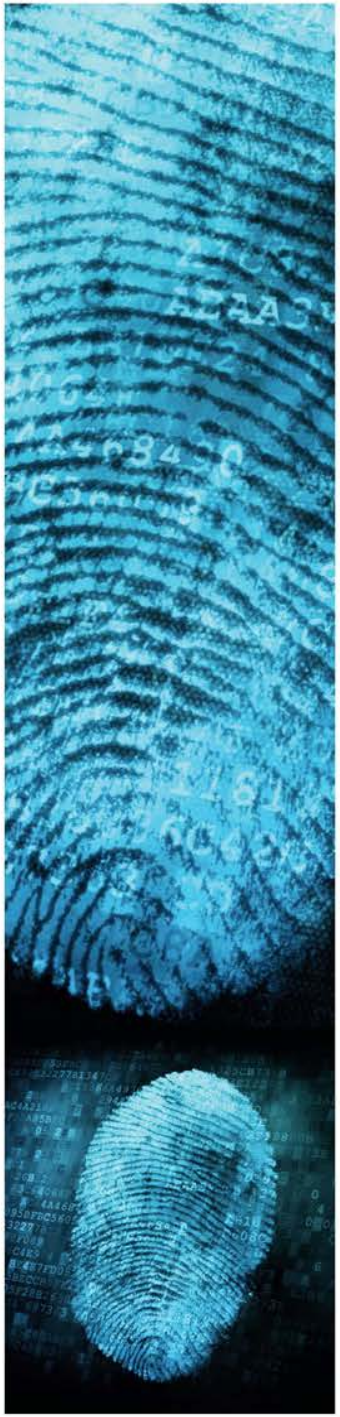
Speaker:
Dr. Brad Glisson
PI: Dr. Todd Andel

August 14, 2017



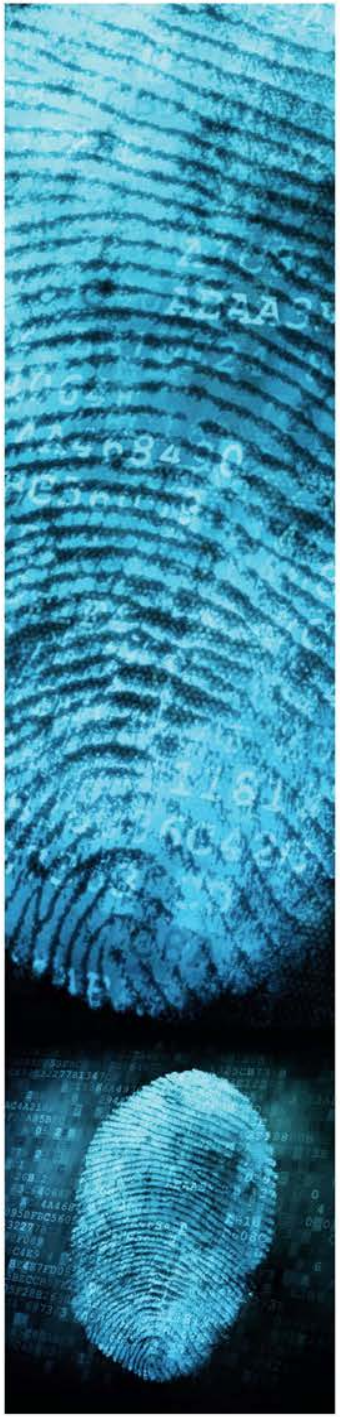
On-Device Detection via Anomalous Environmental Factors

Project Information	Attributes
PROJECT ID	DFII-20
TYPE	[X] New
START DATE	January, 2018
PROJECT LEAD/PARTICIPANTS	Students; Dr. Todd Andel Dr. Todd McDonald Dr. Ryan Benton



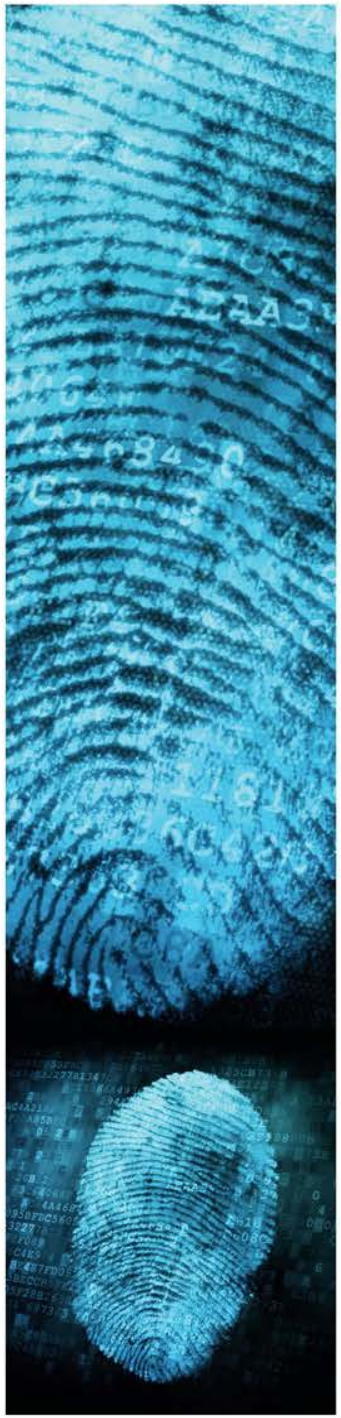
Industry Relevance

- This research seeks to develop real-time attacker detection capabilities through the use of device level measurements of environmental factors.
- We hypothesize that physical indicators from attacker activity can be statistically distinguished from normal operations. These indicators include measurements such as device temperature, power usage, CPU utilization, memory utilization, and network activity.
- This research utilizes high fidelity side-channel analysis to determine correlation between the on-chip readings and physical electrical properties.
- We will also investigate the integration of multiple redundancy sensors to provide secondary measurement channels not available to the attackers. This will provide a correlation source that cannot be subverted.



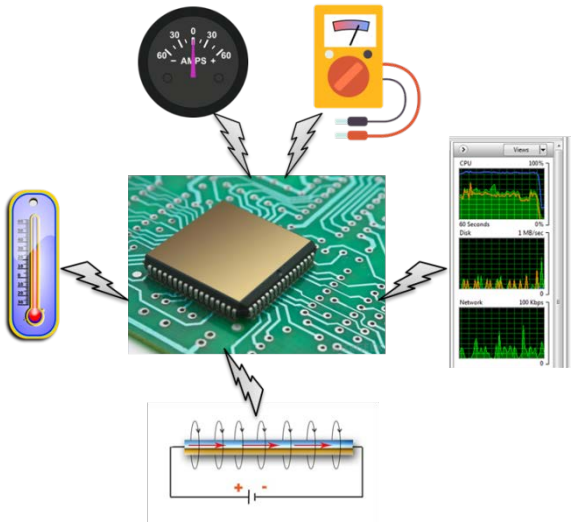
Project Goals/Milestones

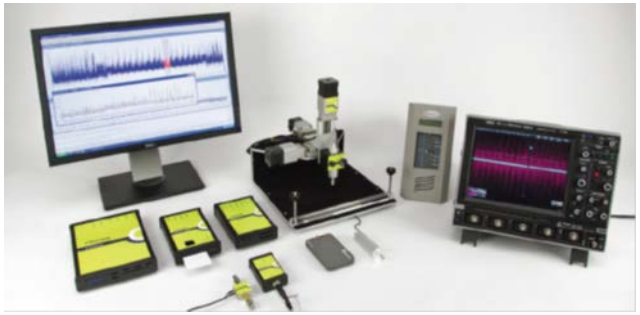
- **4 months**: Develop correlation algorithms for baseline signatures from on-device environmental factor sensors and traditional side-channels
- **8 months**: Tune correlation engine to detect anomalous attacker activity.
- **12 months**: Develop redundant sensors with out-of-band reporting. Incorporate low-fidelity capture capabilities in place of high-level requirements.

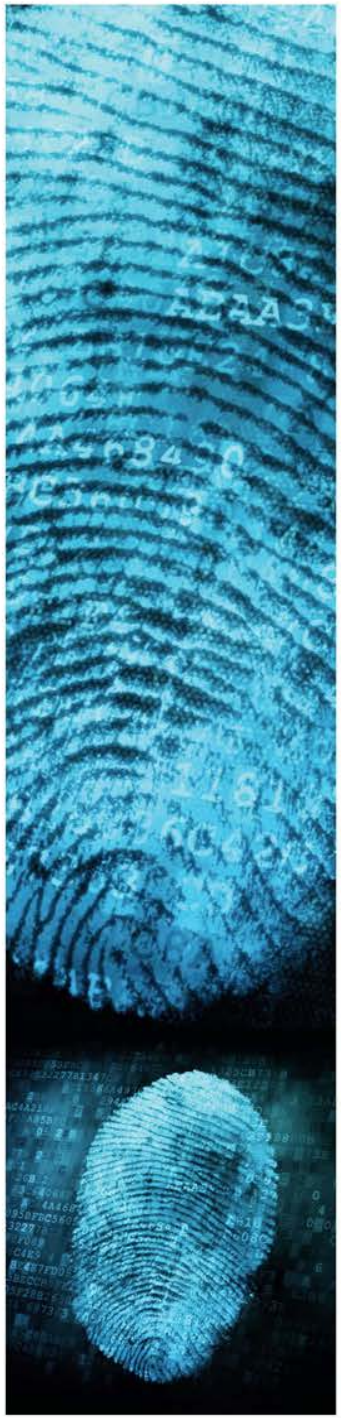


Experimental Plan/Approach

- Develop correlation algorithms for baseline signatures in multiple non-malicious environments (“biomes”)
- Evaluate and tune correlation engine against active attacker.

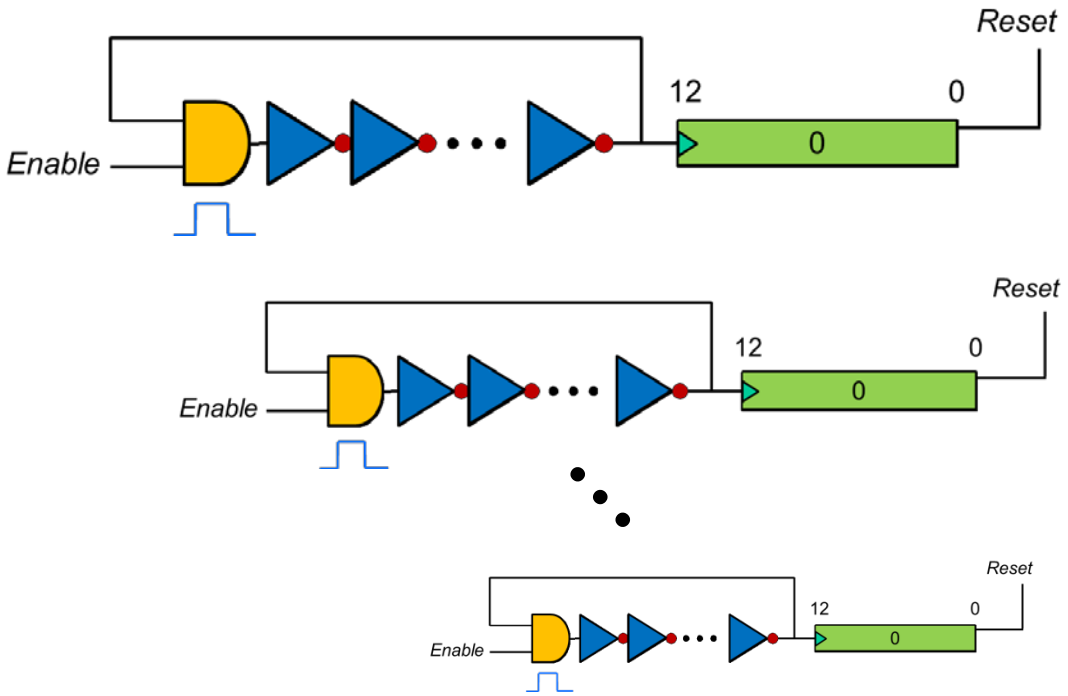


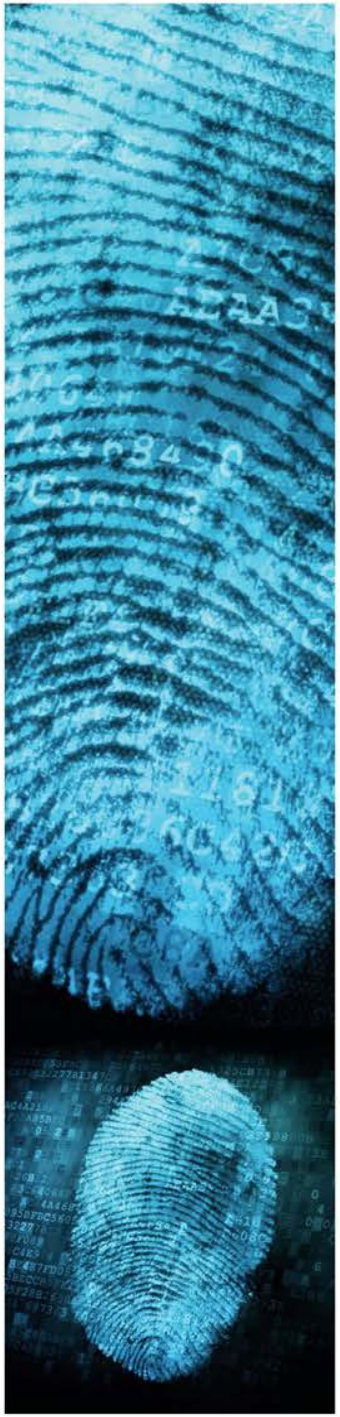




Experimental Plan/Approach

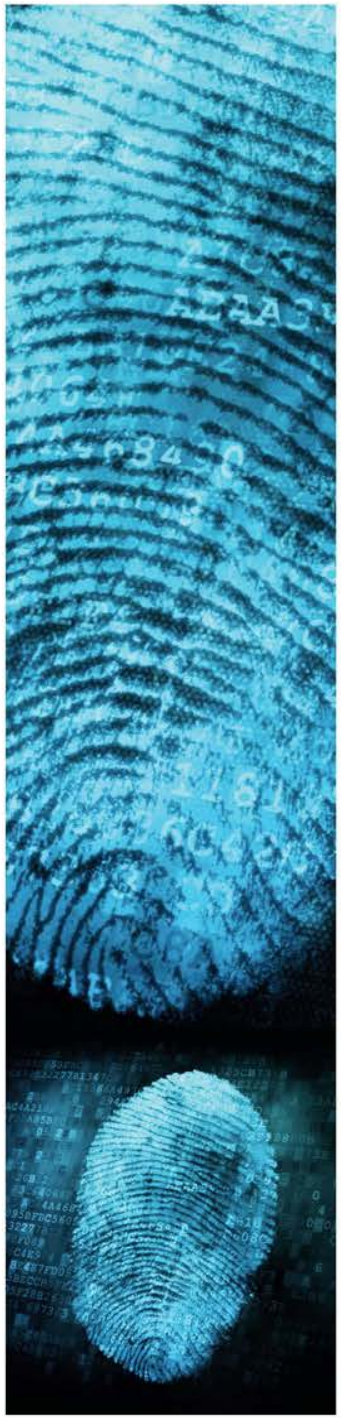
- Investigate sensor combinations, including multiple redundant sensors, for systems reporting false information.





Deliverables

- Baseline signature dataset for non-malicious applications/hardware.
- Analysis and identification techniques to identify maliciously modified applications and systems.
- Techniques to detect zero-day exploits and hardware implants.



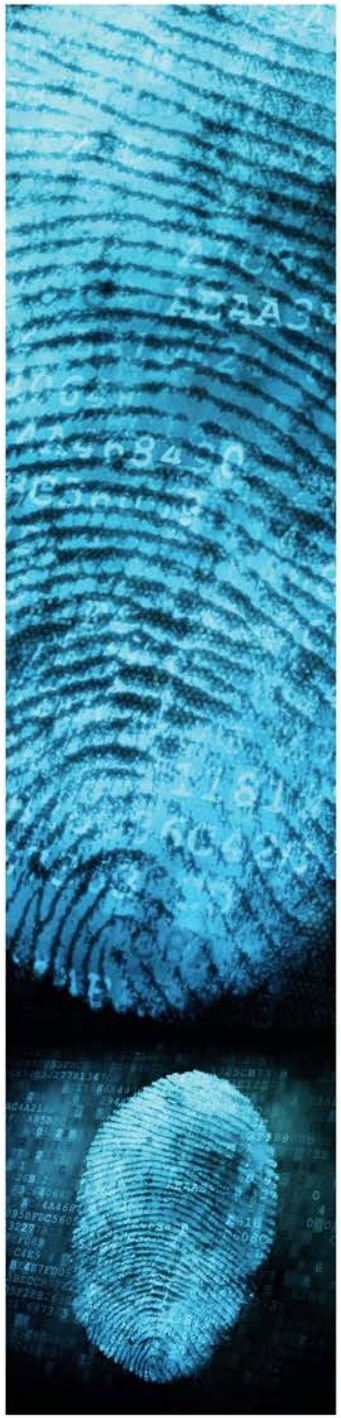
Impact

ECONOMICS |

- Advanced persistent threats can routinely subvert a system and provide false readings to cover their activity. The ability to determine such activity using on-device sensor correlations provides a cost effective detection capability.

POTENTIAL MEMBER COMPANY BENEFITS |

- Providing a way to identify potential zero-day exploits and undiscovered rootkits, or even maliciously implanted hardware.
- Identification of such exploits from an external side-channel and other correlated environmental factor vantage point may lead to detection algorithms that can be integrated without subsequent need for high fidelity side-channel capabilities.



Duration & Budget

Duration: 12 Months

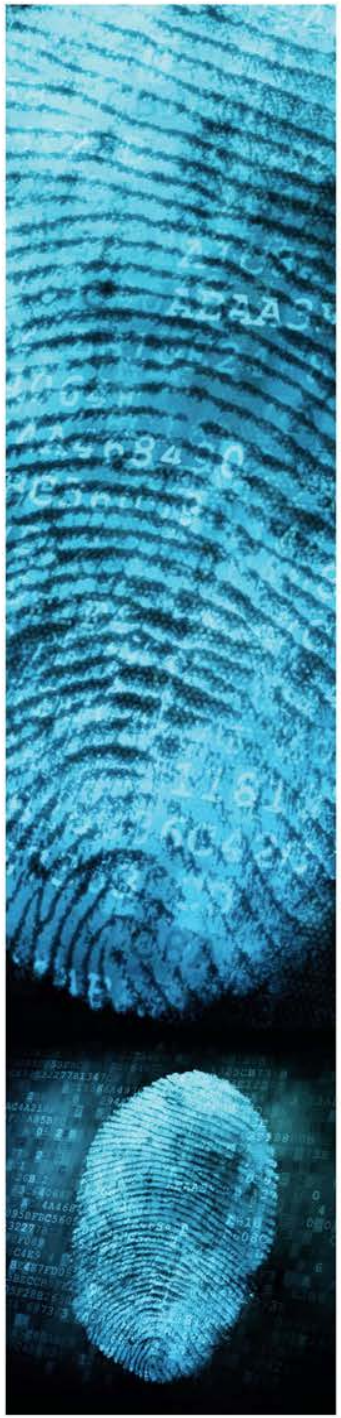
	1 Ph.D.
Students	32,586
Equipment	2,800
Travel	2,800
Overhead (10%)	3,814
Total	42,000.

DIGITAL FORENSIC INFORMATION INTELLIGENCE (DFII) SITE

Center for Advanced Research in Forensic Science (CARFS)

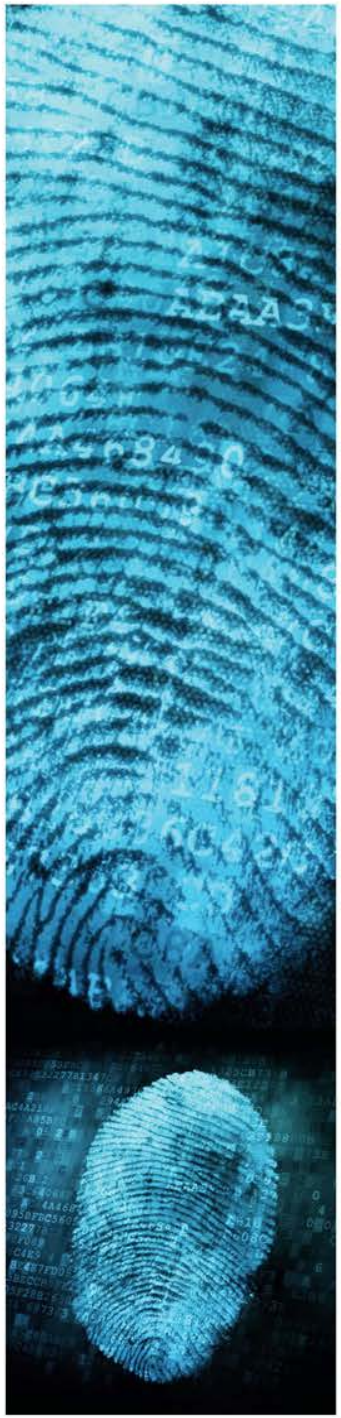
Speaker:
Dr. Brad Glisson
PI: Dr. Tom Johnsten

August 14, 2017



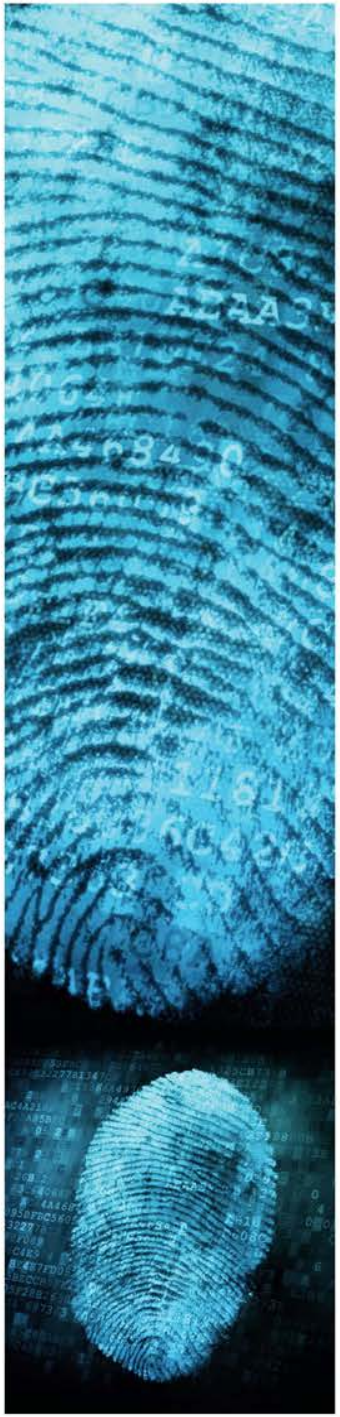
Anomalous Detection of Engine Data

Project Information	Attributes
PROJECT ID	DFII-23
TYPE	[X] New
START DATE	January, 2018
PROJECT LEAD/PARTICIPANTS	Students; Dr. Tom Johnsten Dr. Todd Andel Dr. Ryan Benton Dr. Todd McDonald



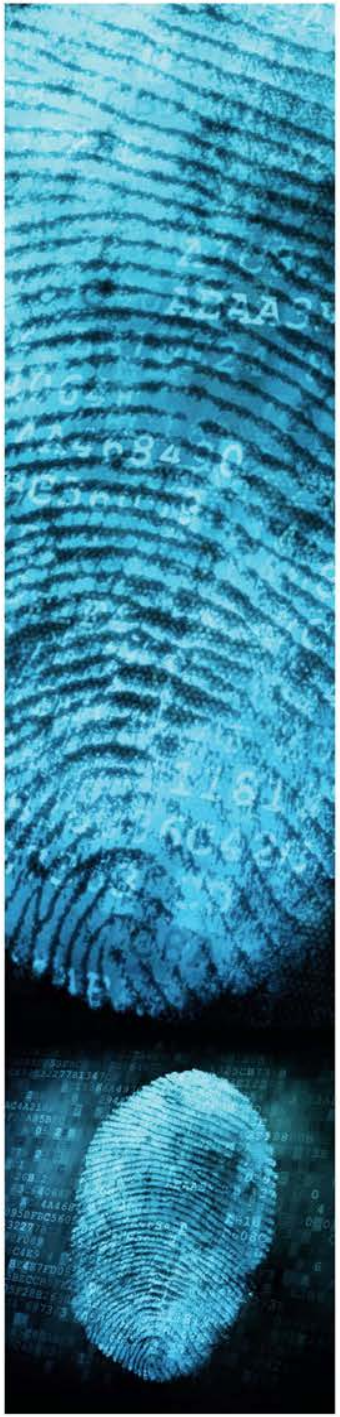
Industry Relevance

- The NTSB web site contains 1010 records involving general aviation single engine aircraft.
- Many of these aircraft are over 50 years old, and have very little if any modern data capture technology useful in forensic investigation, especially as pertaining to the engine.
- Externally mounted sensor arrays could be mounted as a retrofit to these engines during the required rebuilding based on Hobbs meter usage.
- Data captured using such arrays may be able to establish engine operational anomalies, or conversely that the engine operation was normal.



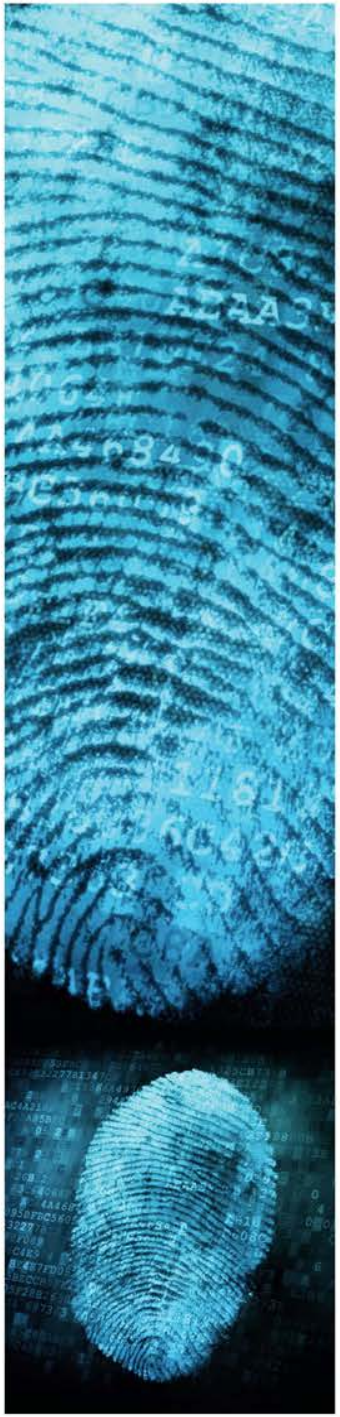
Project Goals/Milestones

- **4 months**: Acquire, categorize, and pre-process engine sensor data
- **8 months**: Design, implement and conduct initial evaluations of proposed methods
- **12 months**: Refine methods and conduct an extensive evaluation



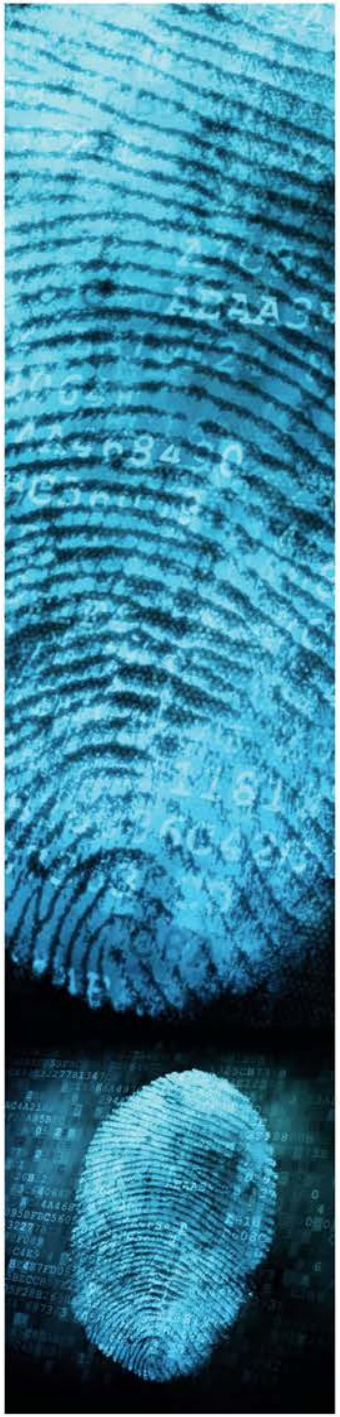
Experimental Plan/Approach

- Develop a sample sensor array appropriate for a given example of a vintage aircraft engine.
- This aircraft engine would be provided by the or a participating industry partner, as would the development of the sensor array.
- The first step would be to establish what is the base line normal operation for that engine under various conditions appropriate for an aircraft engine of that type.
- That data would then be subject to big data research techniques to see what the data tells us.



Deliverables

- Pre-processed datasets for anomaly detection evaluation
- Code demonstrating the proposed functionality to detect potential abnormal engine events.
- Technical report detailing anomaly detection methods implemented to detect potential abnormal engine events and experimental results.



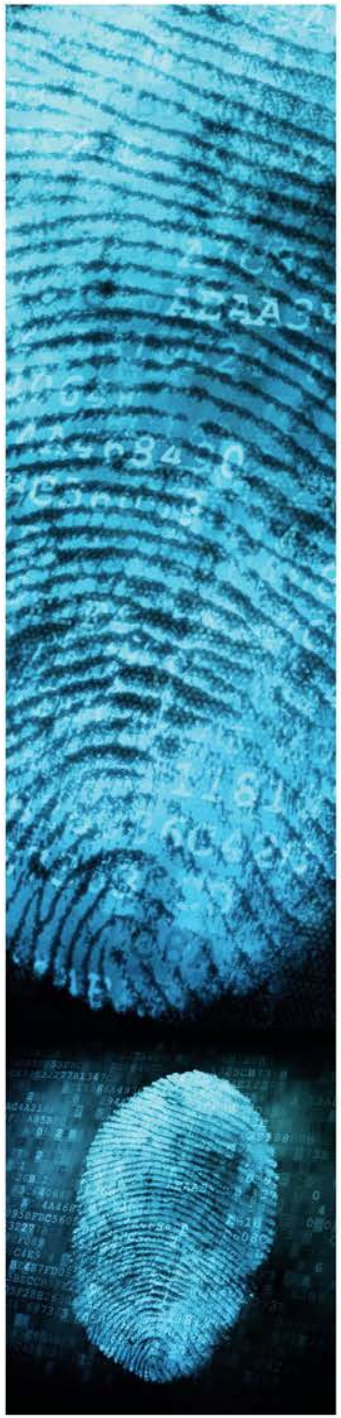
Impact

ECONOMICS |

- Engine operating conditions can compromise the functioning of internally embedded sensors and provide false readings.
- The ability to distinguish normal and abnormal events based on data collected from externally mounted sensors may be a cost effective approach for performing preventive maintenance and retrospective investigations.

POTENTIAL MEMBER COMPANY BENEFITS |

- Measuring the health of aircraft engines from external side-channels may reduce the need for internally embedded sensors.



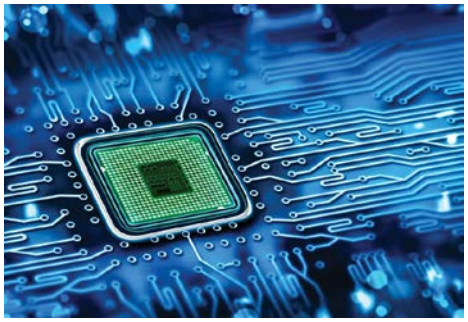
Duration & Budget

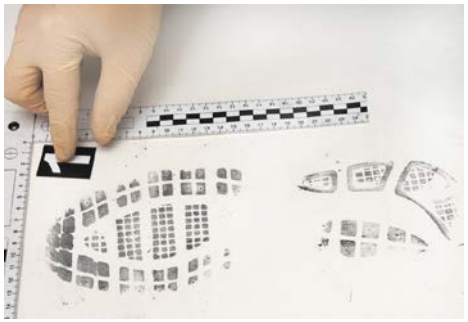
Duration: 12 Months

	1 MSc.	1 Ph.D.
Students	28,108	31,818
Equipment	2,300	-
Travel	1,410	-
Overhead (10%)	3,182	3,182
Total	35,000	35,000

DIGITAL FORENSIC INFORMATION INTELLIGENCE (DFII) SITE

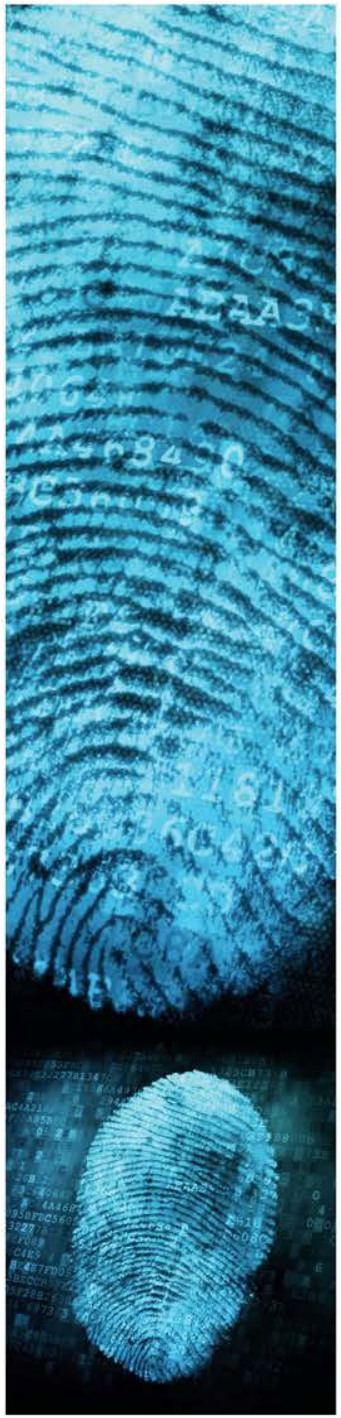
Center for Advanced Research in Forensic Science (CARFS)





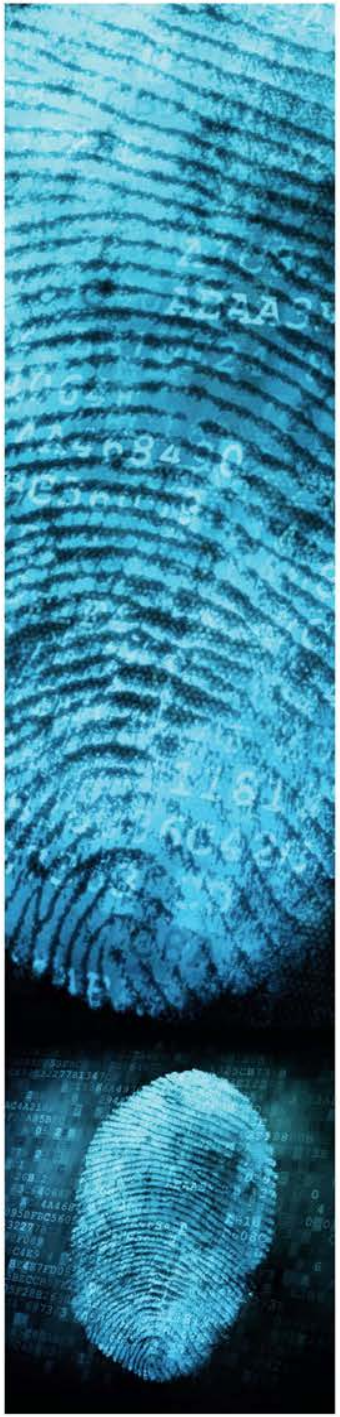

Speaker & PI:
Dr. Brad Glisson

August 14, 2017



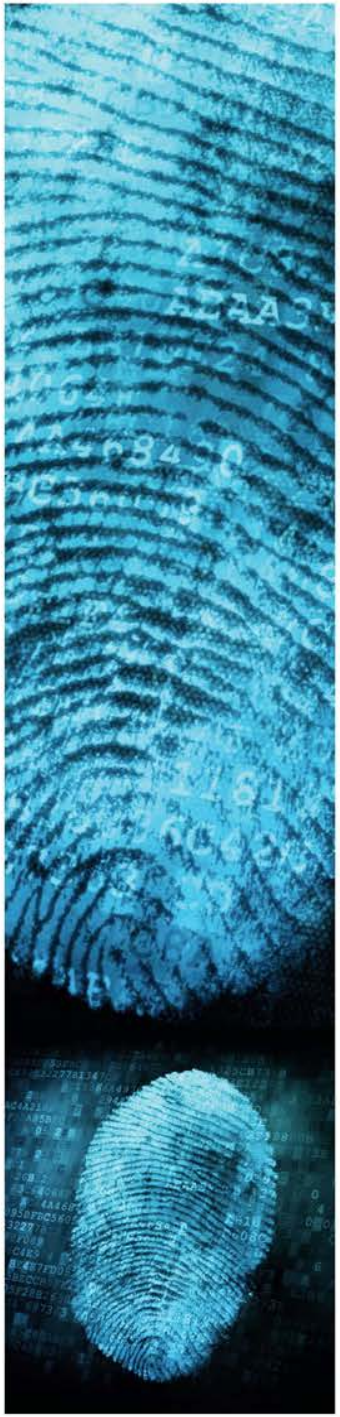
Investigation of Smartphone Residual Data in Secondary Markets

Project Information	Attributes
PROJECT ID	DFII-5
TYPE	[X] New
START DATE	January, 2018
PROJECT LEAD/PARTICIPANTS	Students; Dr. Brad Glisson; Dr. Todd McDonald



Industry Relevance

- According to the International Data Corporation (IDC), Android is the dominate OS with, approximately, 82% of the market.
- Identify trends in residual data in secondary markets.
- Performance capabilities of industry accepted tool-kits (Cellebrite, XRY, FTK Phone Examiner Plus)
- Analysis of the impact of improved storage capacities, garbage collection, and reset capabilities.
- It is increasingly important for organizations and law enforcement to understand the residual data that can be gathered from mobile devices in terms of intellectual property leakage, residual data retention from social media apps and residual GPS data.

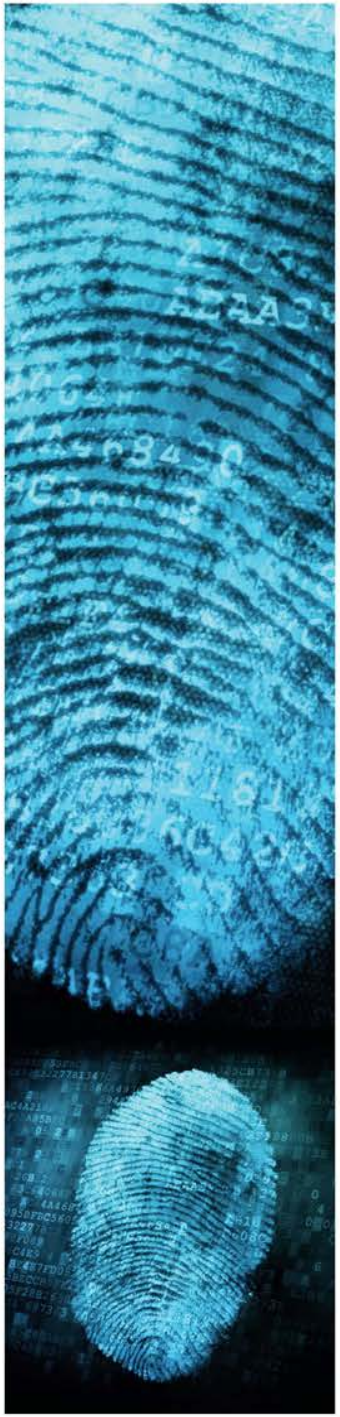


Project Goals/Milestones

4 months: Configure test environments, acquire smartphones from secondary markets and perform the initial processing. Investigate initial results from the perspective of the smartphones and the extraction tools.

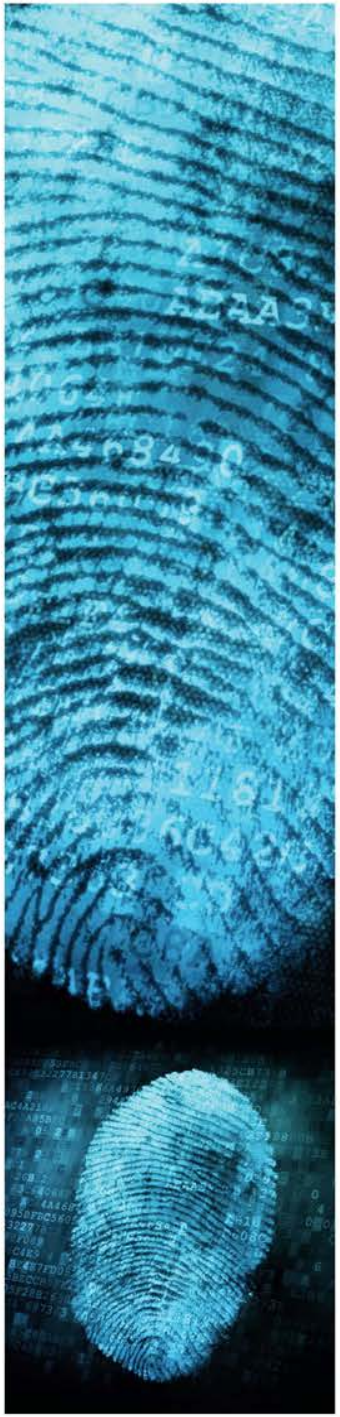
8 months: Develop the data sets and execute the remote data deletion experiments on an Android mobile device. Examine the effectiveness of hard-resets on data extraction capabilities.

12 months: Compare these data deletion app results with the results from the hard-rest and the initial data extraction. Investigate tool performance results between the data deletion experiment, hard-rest and the initial data extraction.



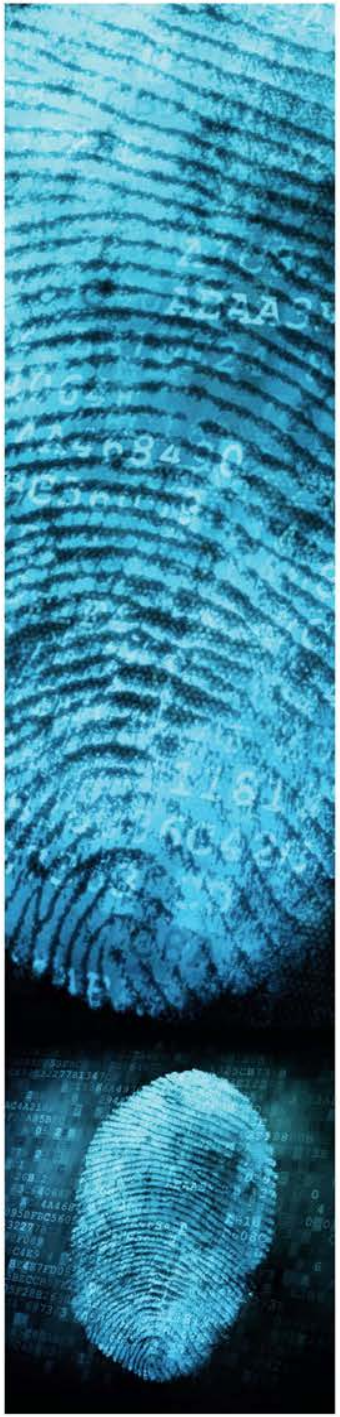
Experimental Plan/Approach

- Purchase a range of smartphones from secondary markets, i.e. pawn shops and the Internet.
- Implement forensic analysis tools to extract data from smartphones purchased from secondary markets.
- Hard-rest acquired devices. Implement forensically analysis tools to extract data.



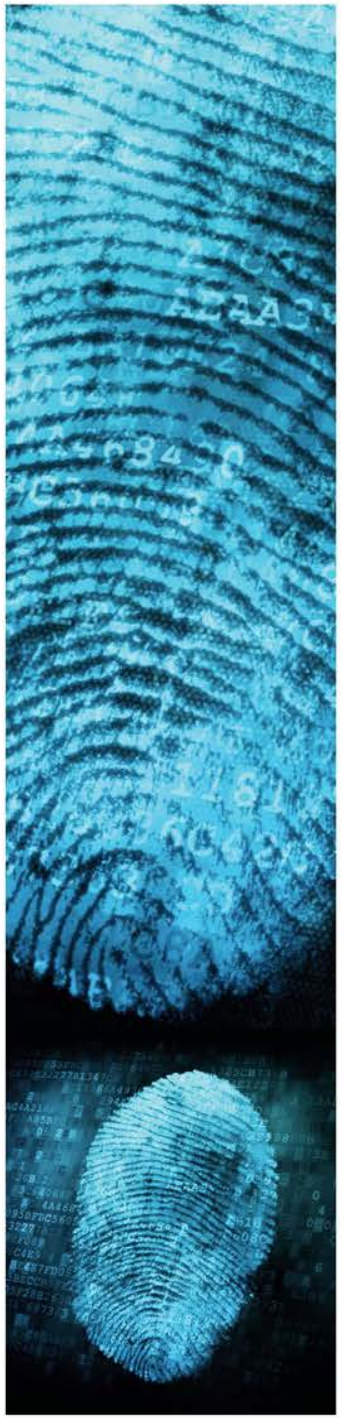
Experimental Plan/Approach

- Scrutinize the extraction results from the smartphones and the tools (Cellebrite, XRY, and FTK Phone Examiner Plus).
- Download the top three remote data deletion apps for the Android OS
- Insert a defined dataset on-to the device
- Run the remote data deletion app
- Implement forensic analysis tools to extract data.



Deliverables

- General categories, data types and apps along with Logical & physical tool extraction performance
- The effectiveness of hard resets from a data extraction and tool performance perspective.
- The effectiveness of remote data deletion apps on an Android smartphone.



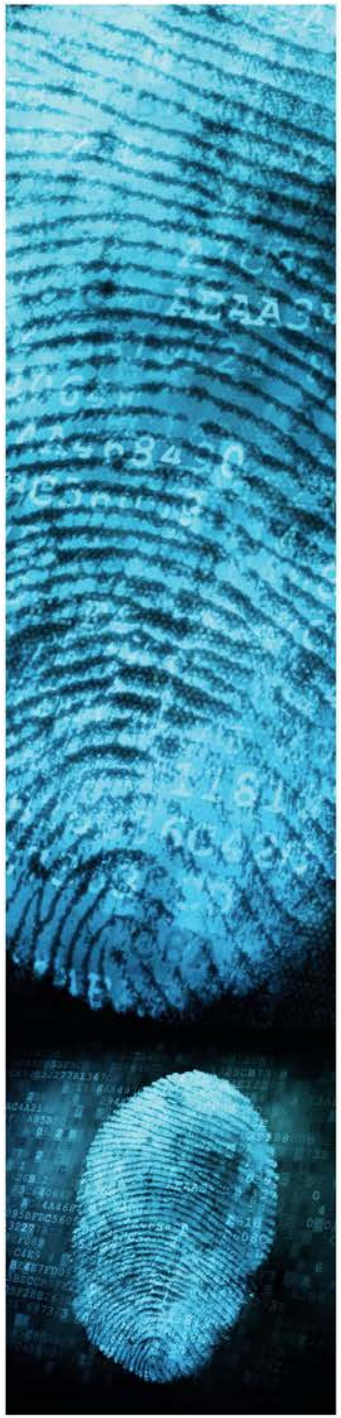
Impact

ECONOMICS

It is helpful for a digital analyst to know the limitations of mobile device forensics toolkits. Both industry and law enforcement benefit from an understanding of the effectiveness of remote deletion applications and hard-rest activities.

POTENTIAL MEMBER COMPANY BENEFITS

This project provides immediate insight to both IAB members and their clients by detailing the type of residual data that is resident on smartphones, the effectiveness of digital forensics toolkits, and the viability of remote deletion applications. This project provides an approach that can be utilized to test existing / implemented data leakage mitigation solutions.



Duration & Budget

Duration: 12 Months

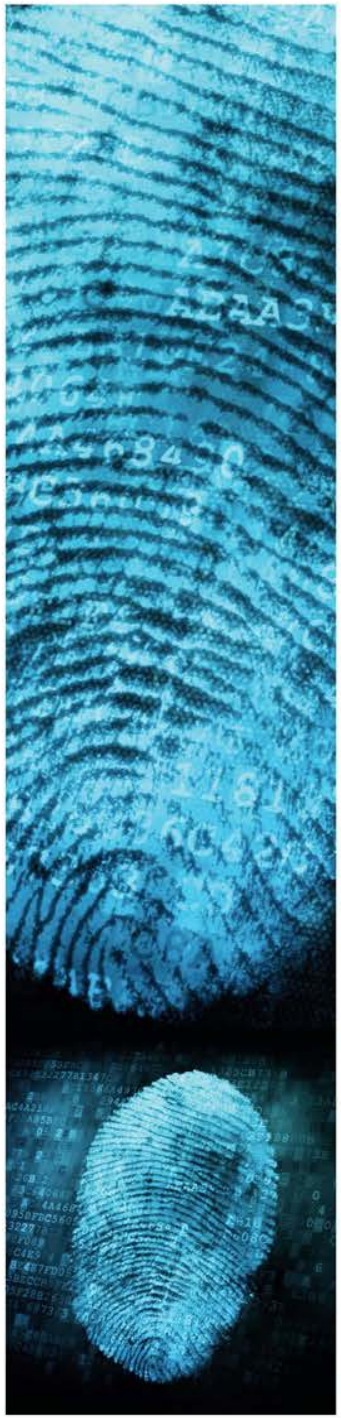
	1 MSc.	2 MSc.	1 Ph.D.	2 Ph.D.
Students	25,000	56,216	32,586	65,160
Equipment	-	6,000	3,000	6,000
Travel	-	4,500	3,000	4,500
Overhead (10%)	-	6,672	3,859	7,566
Total	25,000	73,388	42,444	83,226

DIGITAL FORENSIC INFORMATION INTELLIGENCE (DFII) SITE

Center for Advanced Research in Forensic Science (CARFS)

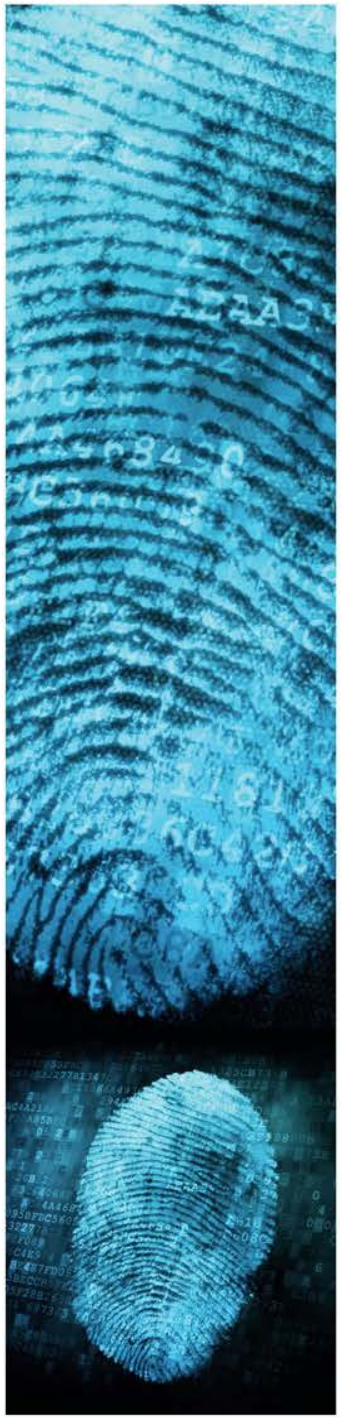
Speaker:
Dr. Brad Glisson
PI: Dr. Jordan Shropshire

August 14, 2017



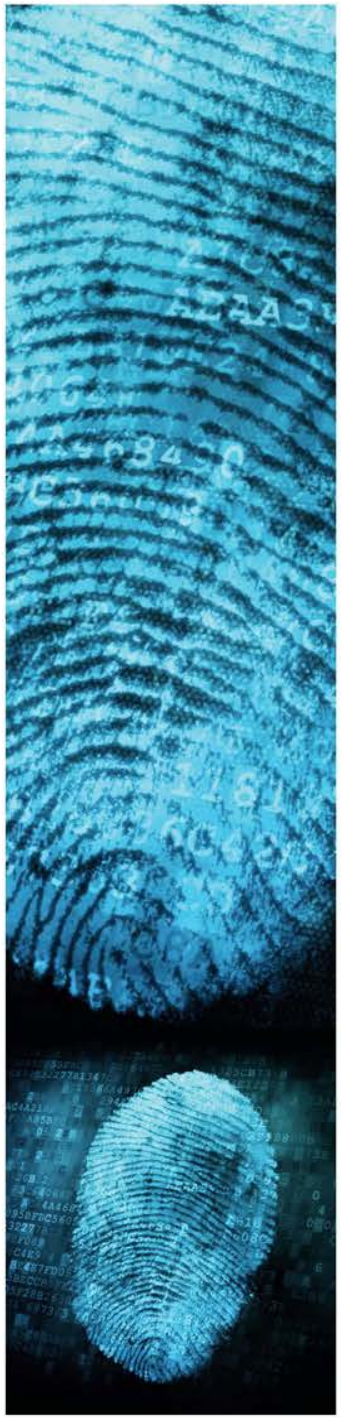
Investigating Methods to Capture Guest VM Memory

Project Information	Attributes
PROJECT ID	DFII-18
TYPE	[X] New
START DATE	January, 2018
PROJECT LEAD/PARTICIPANTS	Students; Dr. Jordan Shropshire Dr. Michael Black



Industry Relevance

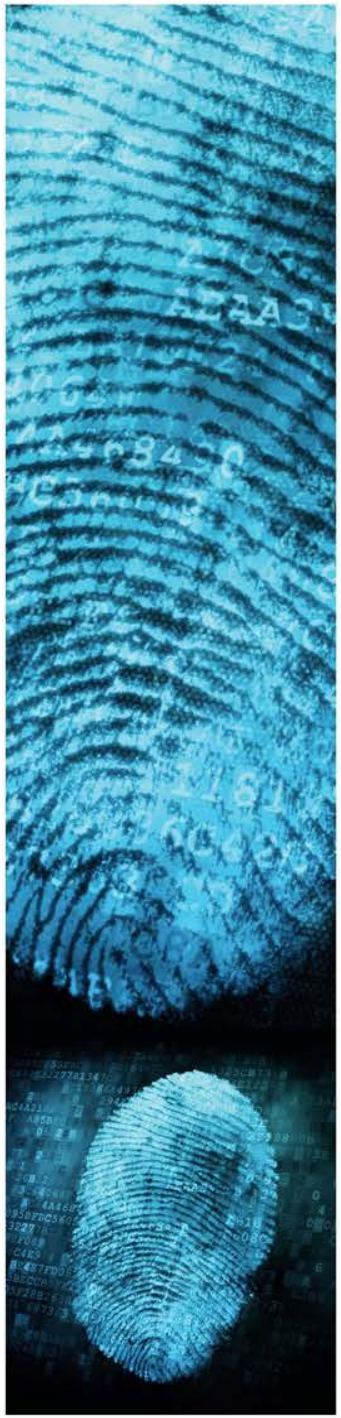
- This research develops techniques and tooling to support live observation and analysis of virtual machine memory
  - Purpose is to detect malicious code executing within the VM
- This project would provide a out-of-band method for observing guest VM memory
  - Performed via the hypervisor
  - Virtual machines aren't aware they are being analyzed
  - Proposed tooling allows for observation of live VMs
- VM memory outputs are formatted for rapid analysis
  - Outputs are paired with guest-virtual-to-metal memory mappings
  - Can be piped into existing forensics toolsets



Project Goals/Milestones

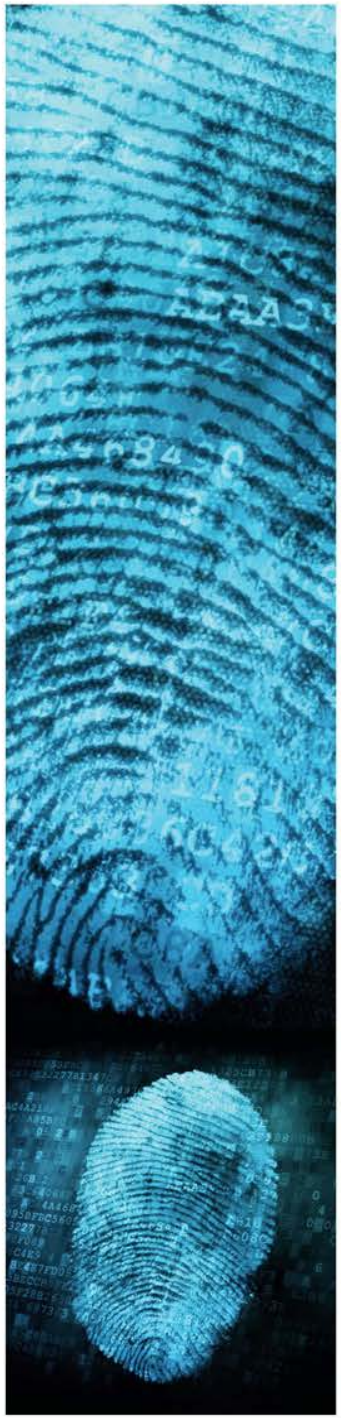
- Goals:
  - Developing tooling to support smart VM memory analysis
  - Design for integration with Xen platform

- Milestones
  - 4 months:
    - Incorporate existing code for passive guest introspection
    - Standardized format for outputting VM memory collections
  - 8 months:
    - Develop methods for mapping guest virtual memory to host virtual memory
  - 12 months:
    - Assemble near-real-time mapping between guest virtual memory and host physical memory
    - Create tooling to identify and extract guest physical memory



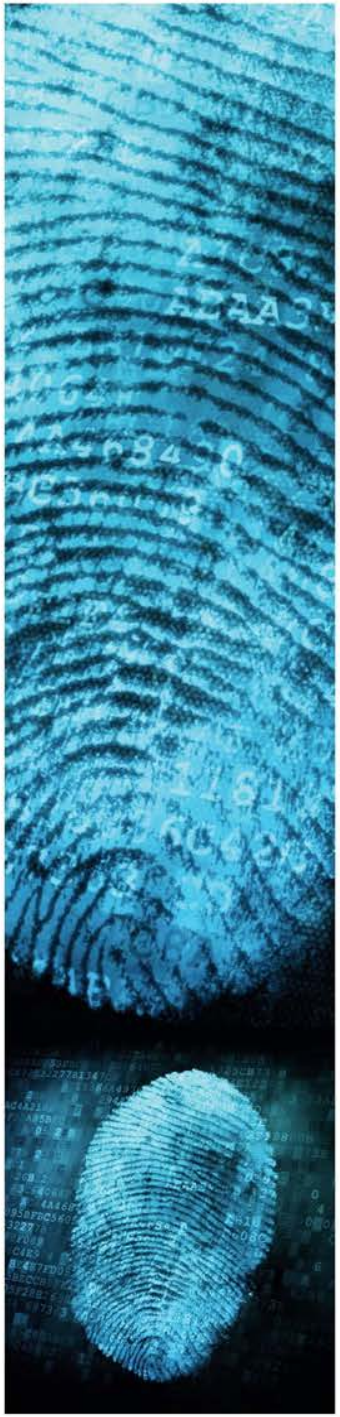
Experimental Plan/Approach

- VM memory is observed from a peering point within the hypervisor.
  - No software is installed within the guest operating system
  - No writes to guest memory are required
- Creates accurate guest-to-metal memory map
  - Introspects guest to support memory mapping
  - Observe mappings between guest virtual memory and guest physical memory
- Minimizes smear by manipulating the hypervisor scheduler
  - Temporarily degrades VM performance via credit scheduling algorithm
  - overschedules the hypervisor and under schedules suspicious guest



Deliverables

- Project codebase to be released via GitHub
  - Includes documentation wiki
- Sample outputs
  - Library of memory outputs showing benign and malicious code
- Benchmark testing against other platforms



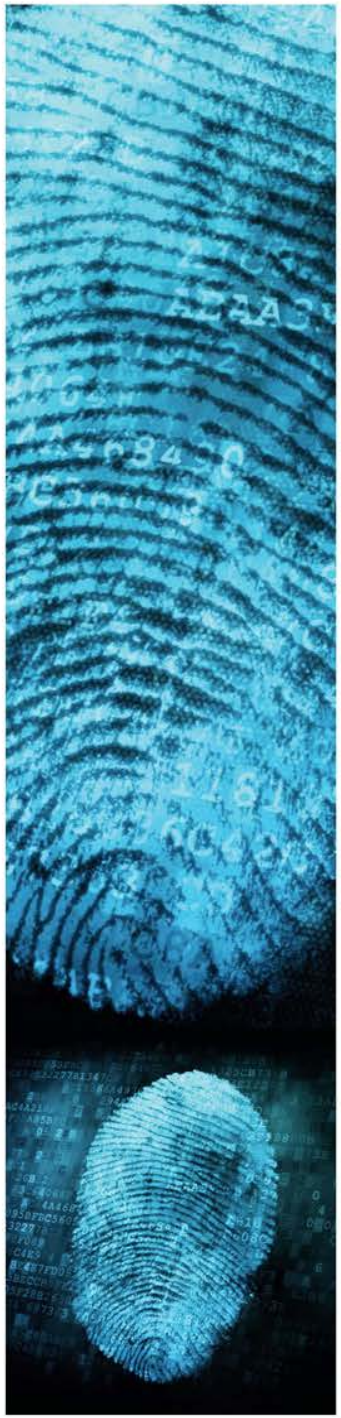
Impact

ECONOMICS

Personalized security services without giving up control of their virtual machines and cloud service providers can provide value-added services without the additional liabilities associated with direct access to client images. This results in an increase in billable services for hosts and increased security for clients.

POTENTIAL MEMBER COMPANY BENEFITS

Tenants want managed security services for their virtual machines but do not wish to relinquish their privacy expectations. If successfully, this research will provide a commercially-viable solution to a problem with a defined market.



Duration & Budget

Duration: 12 Months

	1 MSc.	2 MSc.	1 Ph.D.	2 Ph.D.
Students	25,000	56,216	32,586	65,160
Equipment	-	6,000	3,000	6,000
Travel	-	4,500	3,000	4,500
Overhead (10%)	-	6,672	3,859	7,566
Total	25,000	73,388	42,444	83,226