SADFE: *Systematic Approaches to Digital Forensics Engineering*
39th IEEE Symposium on Security and Privacy May 24, 2018

7:30	**to**	**8:30**	**Breakfast**
8:45	**to**	**9:00**	**Welcome and Introductions**
			Glenn Dardick, general chair / Ibrahim Baggili
9:00	**to**	**10:15**	**Session 1**
9:00	**to**	**9:25**	**Evaluating Automated Facial Aging Techniques for Digital Forensics**
			Felix Anda, David Lillis, Nhien An Le Khac and Mark Scanlon
9:25	**to**	**9:50**	**File Fragment Classification Using Grayscale Images and Deep Learning in Digital Forensics**
			Qian Chen, Zoe L. Jiang, Junbin Fang, Siuming Yiu, Guikai Xi, Rong Li, Zhengzhong Yi, Xuan Wang and Hui Lucas C.K.
9:50	**to**	**10:15**	**Invited Speaker: Future challenges – digital forensics and archival science-the interpares trust project**
			Corinne Rogers
10:15	**to**	**10:45**	**Break**
10:45	**to**	**12:30**	**Session 2**
10:45	**to**	**11:10**	**Forensic-Aware Anti-DDoS Device**
			C. Y. Tseung and K. P. Chow
11:10	**to**	**11:35**	**Best Paper Presentation: A Dynamic Taint Analysis Tool for Android App Forensics**
			Zhen Xu, Chen Shi, Chris Chao-Chun Cheng, Neil Zhengqiang Gong and Yong Guan
11:35	**to**	**12:30**	**Invited Speaker: Case Studies in Invasive Embedded Device Forensics: Data Extraction and Firmware Assurance**
			Sujeet Shenoi
12:30	**to**	**1:30**	**Lunch**
1:30	**to**	**3:15**	**Session 3**
1:30	**to**	**1:55**	**Fingerprinting Cryptographic Protocols with Key Exchange using an Entropy Measure**
			Shoufu Luo, Jeremy D. Seideman and Sven Dietrich
1:55	**to**	**2:20**	**Forensic Analysis of Ransomware Families using Static and Dynamic Analysis**
			Kul Prasad Subedi, Daya Ram Budhathoki and Dipankar Dasgupta
2:20	**to**	**2:45**	**Invited Paper: Forensic Analysis of Immersive Virtual Reality Social Applications: A Primary Account**
			Ananya Yarramreddy, Peter Gromkowski and Ibrahim Baggili
2:45	**to**	**3:15**	**Invited Speaker: Future challenges – digital forensics, cyber security and local law enforcement& NSF Technology Transfer to Practice**
			Adel Elmaghraby, Michael Losavio and Alec Yasinsac
3:15	**to**	**3:45**	**Break**
3:45	**to**	**5:45**	**Session 4: National Workshop on Redefining Cyber Forensics (NWRCF)**

UNHcFREG | University *of* New Haven

3:45	**to**	**5:45**	**NWRCF Workshop: The Future Of Digital Forensics And The National Science Foundation Study**
			Ibrahim Baggili, et al. / Panel
5:45	**to**	**5:45**	**Conference closing and SADFE 2019**

SADFE: *Systematic Approaches to Digital Forensics Engineering*
39th IEEE Symposium on Security and Privacy May 24, 2018
Abstracts

Evaluating Automated Facial Aging Techniques for Digital Forensics

Felix Anda, David Lillis, Nhien An Le Khac and Mark Scanlon

In today's world, closed circuit television, cellphone photographs and videos, open-source intelligence (i.e., social media and web data mining), and other sources of photographic evidence are commonly used by police forces to identify suspects and victims of both online and offline crimes. Human characteristics such as age, height, weight, gender, hair color, etc., are often used by police officers and witnesses in their description of unidentified suspects. In certain circumstances, the age of the victim can result in the determination of the crime's categorization, e.g., child abuse investigations. Various automated machine learning-based techniques have been implemented for the analysis of digital images to detect soft-biometric traits, such as age and gender, and thus aid detectives and investigators in progressing their cases. This paper documents an evaluation of existing cognitive age prediction services. The evaluative and comparative analysis of the various services was executed to identify trends and issues inherent to their performance. One significant contributing factor impeding the accurate development of the services investigated is the notable lack of sufficient sample images in specific age ranges, i.e., underage and elderly. To overcome this issue, a dataset generator was developed, which harnesses collections of several unbalanced datasets and forms a balanced, curated dataset of digital images annotated with their corresponding age and gender.

File Fragment Classification Using Grayscale Images and Deep Learning in Digital Forensics

Qian Chen, Zoe L. Jiang, Junbin Fang, Siuming Yiu, Guikai Xi, Rong Li, Zhengzhong Yi, Xuan Wang and Hui Lucas C.K.

File fragment classification is an important step in digital forensics. The most popular method is based on traditional machine learning by extracting features like N-gram, Shannon entropy or Hamming weights. However, these features are far from enough to classify file fragments. In this paper, we propose a novel scheme based on fragment-to-grayscale image conversion and deep learning to extract more hidden features and therefore improve the accuracy of classification. Benefitting from the multi-layered feature maps, our deep convolution neural network (CNN) model can extract nearly ten thousand features through the non-linear connections between neurons. Our proposed CNN model was trained and tested on the public dataset GovDocs. The experiments results show that we can achieve 70.9% accuracy in classification, which is higher than those of existing works.

Invited Speaker: Future challenges – digital forensics and archival science-the interpares trust project

Corinne Rogers

Digital forensics and archival theory share concerns about the evidentiary capacity of digital material. As such, they have complementary challenges relating to authorship and provenance, discovery and protection of sensitive information, assessment of authenticity and reliability, and digital preservation, among others. Archival science has a long established theoretical base that developed for analyzing, preserving, and providing access to physical records. This foundation applies in the digital environment, and yet because of the abstractions introduced by the technological environment, and the need for technological mediation for humans to read digital records and analyze digital systems, digital forensics is now enhancing archival practice. Digital forensics investigators have presented a number of process and functional models in search of descriptive and normative theory. Archival science can provide a framework to contribute to this development. This paper presents archival concepts of trustworthiness based on traditional archival theory and diplomatics as developed through InterPARES, the longest continuously funded research into issues of record authenticity and preservation (1998 - present, University of British Columbia), and maps these findings to digital forensics to propose a shared theoretical foundation for analysis of trustworthiness of digital material.

Forensic-Aware Anti-DDoS Device

C. Y. Tseung and K. P. Chow

When defending DDoS and other types of network attack, most products or service providers perform the protection by dropping the attack traffics. It cures the symptoms but not the disease. To help eliminate network attack, a more proactive approach is to trace back the attack source and stop the attack before it starts. Collecting the attack data is essential in attack trace-back. In this paper, we propose a live capture device to record the attack efficiently without disturbing the original network performance. The device is also integrated with anti-DDoS technique so that forensic data collection when be performed even under DDoS attacks. We made use of a network bridge and utilized packet capturing functionality provided by Linux, plus our packet storing mechanisms to build the forensic aware data collection device. The anti-DDoS protection uses machine learning to extract features of attacks, and then use a customized Bloom filter to defend attacks based on selected features. We implemented and tested the performance of the proposed technique in a lab environment.

A Dynamic Taint Analysis Tool for Android App Forensics

Zhen Xu, Chen Shi, Chris Chao-Chun Cheng, Neil Zhengqiang Gong and Yong Guan

The plethora of mobile apps introduce critical challenges to digital forensics practitioners, due to the diversity and the large number (millions) of mobile apps available to download from Google play, Apple store, as well as hundreds of other online app stores. Law enforcement investigators often find themselves in a situation that on the seized mobile phone devices, there are many popular and less-popular apps with interface of different languages and functionalities. Investigators would not be able to have sufficient expert-knowledge about every single app, sometimes nor even a very basic understanding about what possible evidentiary data could be discoverable from these mobile devices being investigated. Existing literature in digital forensic field showed that most such investigations still rely on the investigator's manual analysis using mobile forensic toolkits like Cellebrite and Encase. The problem with such manual approaches is that there is no guarantee on the completeness of such evidence discovery. Our goal is to develop an automated mobile app analysis tool to analyze an app and discover what types of and where forensic evidentiary data that app generate and store locally on the mobile device or remotely on external 3rd-party server(s). With the app analysis tool, we will build a database of mobile apps, and for each app, we will create a list of app-generated evidence in terms of data types, locations (and/or sequence of locations) and data format/syntax. The outcome from this research will help digital forensic practitioners to reduce the complexity of their case investigations and provide a better completeness guarantee of evidence discovery, thereby deliver timely and more complete investigative results, and eventually reduce backlogs at crime labs. In this paper, we will present the main technical approaches for us to implement a dynamic Taint analysis tool for Android apps forensics. With the tool, we have analyzed 2,100 real-world Android apps. For each app, our tool produces the list of evidentiary data (e.g., GPS locations, device ID, contacts, browsing history, and some user inputs) that the app could have collected and stored on the devices' local storage in the forms of file or SQLite database. We have evaluated our tool using both benchmark apps and real-world apps. Our results demonstrated that the initial success of our tool in accurately discovering the evidentiary data.

Fingerprinting Cryptographic Protocols with Key Exchange using an Entropy Measure

Shoufu Luo, Jeremy D. Seideman and Sven Dietrich

Encryption has become increasingly prevalent in many applications and for various purposes, but its use also brings big challenges to network security. In this paper, we take the first steps towards addressing some of these challenges by introducing a novel system to identify key exchange protocols. These protocols are usually required if encryption keys are not shared in advance. We observed that key exchange protocols yield certain patterns of high-entropy data blocks, such as those found in key material. We propose a multi-resolution approach to accurately detect high-entropy data blocks and a method of generating fingerprints for cryptographic protocols. We provide experimental evidence that our approach has the potential to identify cryptographic protocols by their unique key exchanges, leading to the ability to detect malware traffic that includes customized key exchange protocols.

Forensic Analysis of Ransomware Families using Static and Dynamic Analysis

Kul Prasad Subedi, Daya Ram Budhathoki and Dipankar Dasgupta

Forensic analysis of executables or binary files is the common practice of detecting malware characteristics. Reverse engineering is performed on executables at different levels such as raw binaries, assembly codes, libraries, and function calls to better analysis and interpret the purpose of code segments.

In this work, we apply data-mining techniques to correlate multi-level code components (derived from reverse engineering process) for finding unique signatures to identify ransomware families. Such a reverse process and analysis of code structure may not provide dynamic behavior of executables so we used combined approach to better unveil hidden intent of the program. Reported results show some correlation among different code components from our analysis.

Forensic Analysis of Immersive Virtual Reality Social Applications: A Primary Account

Ananya Yarramreddy, Peter Gromkowski and Ibrahim Baggili

Our work presents the primary account for exploring the forensics of immersive Virtual Reality (VR) systems and their social applications. The Social VR applications studied in this work include Bigscreen, Altspace VR, Rec Room and Facebook Spaces. We explored the two most widely adopted consumer VR systems: the HTC Vive and the Oculus Rift. Our tests examined the efficacy of reconstructing evidence from network traffic as well as the systems themselves. The results showed that a significant amount of forensically relevant data such as user names, user profile pictures, events, and system details may be recovered. We anticipate that this work will stimulate future research directions in VR and Augmented Reality (AR) forensics as it is an area that is understudied and needs more attention from the community.

National Workshop on Redefining Cyber Forensics (NWRCF):
The Future of Digital Forensics And The National Science Foundation Study

Ibrahim Baggili, et al. / Panel

The results of the first National Workshop for Redefining Cyber Forensics will be shared in a presentation, followed by discussions and deliberation on missed topics in panel format. Participants will be provided with an opportunity to bring other challenges to light, as well as highlight any mechanisms the field is facing whilst relating the discussion to improving education.