COVER SHEET FOR GRANT PROPOSALS

State Board of Education

SBOE PROPOSAL NUMBER:
(to be assigned by SBOE)

AMOUNT REQUESTED: $75,000

TITLE OF PROPOSED PROJECT: Cyber Forensic Investigation Toolkit (CFIT): Next-generation Evidence-gathering for Law Enforcement

To significantly improve upon available cyber forensic tools for evidence extraction, we propose building a Cyber Forensic Investigation Toolkit (CFIT). It is designed specifically to address large data sets and uses a novel subject-based algorithm to cluster related documents based on topics interesting to the investigator, which improves search speed and accuracy and ultimately reduce investigation time.

PROJECT START DATE: 7/1/2016

PROJECT END DATE: 6/30/2017

NAME OF INSTITUTION: Boise State University

DEPARTMENT: Computer Science

ADDRESS: 1910 University Drive, Boise, ID 83725-2055

E-MAIL ADDRESS: gabydagher@boisestate.edu

PHONE NUMBER: (208) 426-5782

	NAME:	TITLE:	SIGNATURE:
PROJECT DIRECTOR/PRINCIPAL INVESTIGATOR	Dr. Gaby Dagher	Assistant Professor	Not Required
CO-PRINCIPAL INVESTIGATOR	Dr. Jyh-haw Yeh	Assistant Professor	Not Required

NAME OF PARTNERING COMPANY:

COMPANY REPRESENTATIVE NAME:

NAME:

SIGNATURE:

Authorized Organizational Representative	Karen Henry, Executive Director, Office of Sponsored Programs

Cyber Forensic Investigation Toolkit (CFIT):
Next-generation Evidence-gathering for Law Enforcement

1	INSTITUTION	Boise State University
2	FACULTY MEMBER DIRECTING	Dr. Gaby Dagher, Assistant Professor, Computer Science
3	AWARD STATUS	No prior incubation funds requested or awarded

4. Executive Summary

Cybercrime affects all of us. The costly proliferation of cases involving hacking, drug trafficking, and child pornography drive an increasingly urgent demand from government, industry, families, and individuals for effective police response to cybercrimes. Since today's computing devices store *terabytes* of personal data, it can take months for investigators to assemble enough digital evidence to charge a criminal. As more evidence gets buried in documents, emails, chat logs, text messages, and other digital forms, the task of sifting for evidence grows increasingly daunting. Investigators often rely on automated search capabilities provided by either the operating system or existing cyber forensic tools to search for evidence on a suspect's computer by analyzing communications and storage device data. However, the automated search capabilities provided by current state-of-the art tools search all of the available information without blindly, without sensitivity to the topic or subject of each piece of information. To significantly improve upon available cyber forensic tools for evidence extraction, we propose building a ***Cyber Forensic Investigation Toolkit (CFIT)***. CFIT is designed specifically to address large data sets and uses a novel subject-based algorithm to cluster related documents based on topics interesting to the investigator, which improves search speed and accuracy and ultimately reduce investigation time. Investigators devote countless hours to interpreting underlying meaning in data sets, especially text. It is no trivial task for a software program to interpret underlying topics, but we believe CFIT takes important steps towards automating this task. The concept behind CFIT is unlike that of standard tools, because the architecture considers differences between malicious actions a *person* takes versus those a *computer* takes during a cyberattack. This distinction is critical to solving cybercrimes. As proof of concept, the CFIT team has implemented all these core features and recently built an experimental alpha prototype to showcase the enhanced functionality available with this new investigation toolkit.

5. Total Amount Requested to Meet "Gap" Project Objectives

To meet the following project objectives, our team requests $75,000. We will:

1) ***Commercialize*—**Commercialize the existing CFIT prototype by developing it further into a reliable, fully-fledged commercial product for law enforcement agencies. We will focus on:

    - User-Centered Interface: Although the core features are already implemented, they are merely run from the command line. A full and functional graphic user interface needs to be developed for CFIT. As indicated in the letters of support from Idaho State Police (ISP) and Boise Police Department (BPD), our CFIT team will collaborate with ISP and BPD throughout the project. We will work closely with investigators to design and implement a user-centric interface optimized for how they intend to use CFIT.

    - Quality Assurance: Design thorough test cases, define clear quality measures, and construct and execute a quality assurance plan to thoroughly test CFIT, including the new user interface, and ensure it meets the defined quality measures.

    - Benchmark: Measure CFIT accuracy, efficiency and scalability against existing state-of-the art cyber forensic tools, including Forensic Toolkit® by AccessData Group, Inc., and EnCase® by Guidance Software, Inc.

2) ***Market***—Execute the following rigorous plan to market the CFIT to cybersecurity companies, and to law enforcement agencies at the local, state, and federal levels:

   1. Business Summary: define KPIs, identify market and target customers, poll customers, identify competition, and define CFIT value proposition.

   2. Product Strategy: identify the key features to launch in CFIT portfolio, along with any bundling plans, determine special promotions or other strategies that will help sell CFIT.

   3. Channel Strategy: identify primary channels to sell CFIT and to educate and support customers, identify resources and training that will drive channel performance.

   4. Marketing Strategy: define the activities to drive awareness and generate leads for CFIT.

   5. Customer Experience: anticipated customer journey, starting with how customers first hear about CFIT, their purchase, activation, and renewal.

   6. Technical Requirements: document the technical requirements needed to support CFIT.

   7. Evaluation: prioritize the factors to measure success, such as reaching a certain volume of sales of CFIT in specific channels.

   8. Timeline and Execution: identify the timeline for execution, including next steps, the critical path for decisions, and key milestones.

6. Resource Alignment with Boise State University Priorities

The resources requested align well with Boise State University priorities. As part of the 2012-2017 strategic plan toward becoming a *metropolitan research university of distinction*, Boise State University has placed great emphasis on STEM disciplines. In recent years, the number of students majoring in STEM disciplines increased 66% while overall growth in the student body was 5%. This fall, the Computer Science will offer a new Ph.D. program in computing, with a cybersecurity emphasis, which this project could help support. The Carnegie classification as a Research Doctoral University: STEM-dominant also testifies to the high research productivity and high emphasis Boise State University is placing on STEM disciplines.

7. Impact to Idaho Economy

This project is expected to positively affect Idaho's economy in three different ways, by: *saving taxpayer money*, *attracting federal funding*, and *increasing interest in cybersecurity workforce development offerings.*

1. Saving taxpayer money. Throughout this project, we plan to closely collaborate with the Idaho State Police to build the final CFIT product according to the police needs and requirements. We plan to experiment using real-life criminal data to ensure that our approach for extracting evidence is much more effective than the traditional methods. CFIT will quickly sift through vast amounts of information to zero-in on relevant evidence, saving time for investigators, and adding enhanced value for taxpayers by enabling law enforcement to bring cybercriminals to trial much more quickly.
2. Attracting federal funding. The U.S. government is spending billions to address cybersecurity, which underscores the seriousness of the problem. The President's budget request for fiscal year 2017 recommends a $19 billion cybersecurity program investment, increased roughly 35% over 2016. The additional federal investment would support:

> ***"a broad-based cybersecurity strategy for securing the Government, enhancing the security of critical infrastructure and important technologies, investing in next generation tools and workforce, and empowering Americans."*** [1]

[1] *See* Fiscal Year 2017 Budget Overview, Office of Management and Budget, https://www.whitehouse.gov/omb/overview.

Given the current lack of effective cyberforensic tools, and the growing cybersecurity threats, the U.S. needs better cyberdefense tools. CFIT is the next-generation cybersecurity tool that can fill that need, and we expect CFIT will be in a strong position to attract some of the new federal funding for cybersecurity.

3. Increasing interest in cybersecurity workforce development offerings. Due to the increase in demand in industry for cybersecurity specialists, the Boise State University Computer Science department will offer in the Fall of 2016 a Cybersecurity Track as part of its doctoral program. Project team leaders Dagher and Yeh are members of the committee that guides and shapes the Cybersecurity Track. Building next-generation cybersecurity tools such as CFIT aligns with the goals of Boise State to address cybersecurity needs and establish a strong reputation in the field in order to attract future students, researchers, and funding, and to develop a computer science workforce with deep capability in addressing cybersecurity issues.

8. The Market Opportunity

The proposed research and software product have enormous potential, as demonstrated by the market need, demand, and audience.

8a. Market Needs. A central element of ***Digital Forensic Investigation (DFI)*** is the task of gathering and analyzing persistent information found on a suspect's storage devices and computers to build a record of credible and convincing evidence. However, this task is daunting due to the large amount of information stored on a hard disk. The continuously increasing capacity of data storage devices makes the task grow more difficult with time. Today, investigators rely on competitor's existing cyberforensic tools to examine files and to search for pertinent evidence. However, there are two major problems with today's cyberforensic tools:

1. Limited Search Capability. The automated search techniques provided by current DFI tools include keyword search, regular expression search, approximate matching search, and last modification date search. Unfortunately, these search techniques do not filter for the subjects or topics discussed in each piece of information. Hence, these techniques result in an unmanageably large number of false positives and false negatives, dramatically hindering the usefulness of the current cyberforensic tools.

2. The Computer as Criminal. Existing DFI tools are designed for solving crimes committed against people, in which evidence exists on a computer; they were not created to address cases where crimes took place on computers or against computers. Current DFI techniques are designed to find evidence where the possession of evidence is the crime itself. Therefore, it is easier to solve child pornography cases than computer hacking cases [1].

8b. Applications and Markets for the Technology. Out of all types of available data in cyber forensic investigation, text data is the most common medium used by scammers, identity thieves and child exploitation criminals. But this type of data is also the most challenging to analyze, as it is not a trivial task to make a software program automatically interpret the underlying meaning of the text. The proposed CFIT performs semantic analysis of topics discussed in each document, and can be used to efficiently browse a very large set of documents by topic, as well as search for specific documents that belong to a certain topic.

8c. Potential market audience, competition, and barriers to market entry. The market for a CFIT is broad, as any law enforcement agency interested in extracting relevant digital evidence from a suspect computer could employ it, and for all types of crimes. In addition, cybersecurity companies can also utilize the proposed technology to extract relevant information about on-line malicious attacks and breaches carried out against a terminal machine or server. There have been several studies in the literature concerning evidence extraction for cyber forensics. Also, there are several commercial tools in the industry used in cyber forensic investigations, including Forensic Toolkit, EnCase, CAINE and The Sleuth Kit. However, unlike the CFIT we propose, there is currently no theoretical approach nor commercial tool that allows the investigator to specify topics of interest, and then browse for these topics in documents captured on a suspect's computer. As a result, we expect CFIT will be a welcomed addition to the existing tools, and law enforcement agencies as well as cybersecurity companies will be eager to adopt it.

9. The Technology and Path to Commercialization

Existing cyber forensic tools for analyzing a set of documents provide multiple levels of search techniques to answer questions and generate digital evidence related to the cyber forensic investigation. However, these techniques stop short of allowing the investigator to search for documents that belong to a certain subject he is interested in, or to group the document set based on a given subject. In this project, the proposed CFIT will help answer the question of whether evidence for events defined by the investigator, such as hacking or child pornography, is present in documents collected from the suspect's computer. The investigator initially defines the subjects (events) he or she is interested in by providing a set of terms to describe each subject.

9a. The CFIT technology. The proposed CFIT consists of three main components: *indexing engine, clustering engine*, and *search engine*.

Indexing Engine. This engine parses documents on the suspect's computer, analyzes the documents by applying several preprocessing steps: tokenization, stemming, stop word removal, and text normalization, and then generates an inverted index. We used Apache Tika and Apache Lucene to parse, preprocess, and index the documents.

Clustering Engine. In this engine, we introduce a novel subject-based semantic document clustering algorithm that groups (clusters) all documents into a set of *overlapping* clusters, each corresponding to one unique subject initially provided by the investigator. The intent of this clustering approach is to generate a set of expansion vectors for each given subject using its initial subject definition. Each expansion vector consists of a set of weighted terms related to the subject, where each term is generated using WordNet, a lexical database for the English language. Once the expansion vectors for a subject are generated, they will be used with the initial subject definition to construct a vector of weighted term frequencies called *subject vector* such that the problem of measuring the similarity between a document and a subject is reduced to measuring the similarity between the document and the subject vector.

Search Engine. This engine allows an investigator to search the resulting clusters and retrieve relevant documents according to a given search query and a specific subject.

Current state of the technology. The CFIT team has already built a working prototype that includes core functionality for indexing, clustering and searching. However, in order to transform the prototype to a commercial grade product, it needs to be further developed to include a full and functional user-centric interface, as well as further tested and benchmarked.

9b. Market need for CFIT technology and its intellectual property status. As indicated by the letters of support from Idaho State Police (ISP) and Boise Police Department (BPD), there is an urgent market need for tools such as CFIT. The intellectual property of CFIT belongs to Boise State University since the PIs used university funds and facilities to develop it.

9c. Who developed the technology and with what funding? Drs. Gaby Dagher and Jyh-haw Yeh, faculty in the Boise State Computer Science department, worked with students to build the CFIT prototype. A university graduate assistantship provided funding.

9d. Concrete steps to bring CFIT technology to market.

1. User-Centered Interface. We will work closely with ISP and BPD investigators to design and implement a user-centered interface that offers an efficient, satisfying, and user-friendly experience to the investigator. Doing so is likely to increase sales as well as customer retention.

2. Reliability. We plan to design an extensive set of test cases to be able to thoroughly test the final version of CFIT and ensure its reliability.

3. Benchmarking: We plan to measure CFIT accuracy, efficiency and scalability against state of the art cyber forensic tools such as Forensic Toolkit and EnCase.

4. Rigorous Marketing. We plan to prepare a rigorous marketing plan that includes constructing a list of prospective customers, clearly defining marketing goals, and determining marketing communications strategies and tactics. We refer the reader to Section 5 for a detailed plan.

10. Commercialization Partners

As indicated in the supporting letters from Lt. Colonel Kedrick Wills, Deputy Director of Idaho State Police (ISP) and William L. Bones, the chief of Boise Police Department (BPD), both departments will collaborate with CFIT team throughout the project and support our effort to build a commercial version of the tool. The table below outlines the collaboration detail.

ENTITIES	RESPONSIBLE PROJECT TASKS
PIs + ISP + BPD	Design User-Centered Interface
PIs	Develop User-Centered Interface, Quality Assurance, Benchmarking
PIs + ISP + BPD	Marketing CFIT

11. Project Plan and Fund Use

FOR	DESCRIPTION	BUDGET
Dr. Gaby Dagher (PI)	Six weeks of summer salary and fringe benefit for research and oversight	$20,250
Dr. Jyh-haw Yeh (Co-PI)	Three weeks of summer salary and fringe benefit for research	$10,182
Graduate Student	Salary, fringe benefits, health insurance, and tuition for 1 year	$37,213
Undergraduate Student	Salary and fringe benefits at $12.50 per hour and 10 hours per week for 52 weeks	$7,355
	Total	$75,000

Here is the project timeline with milestones highlighted:

(A): User Interface, (B): Quality Assurance, (C): Benchmarking, and (D): Marketing Plan

#	PROJECT TASKS	1	2	3	4
	Milestones:	A	B	C	D
1	User-Centered Interface	X			
2	Quality Assurance		X		
3	Benchmark			X	
4	Market				X

12. Institutional and Other Support

Boise State University and the Computer Science department provide adequate computer labs, student offices and conference rooms to conduct this research. The collaboration with the state police will provide functional and test feedback for product development and benchmarking.

References:

[1] S. L. Garfinkel, Digital forensics research: The next 10 years, Digital Investigation 7 (1) (2010) S64–S73.

SUMMARY PROPOSAL BUDGET

Name of Institution: Boise State University

Name of Project Director: Gaby Dagher

A. PERSONNEL COST (Faculty, Staff, Visiting Professors, Post-Doctoral Associates, Graduate/Undergraduate Students, Other)

Name/ Title	Salary/Rate of Pay	Fringe	Dollar Amount Requested
Gaby Dagher (PI)	$15,000	$5,250	$20,300
Jyh-haw Yeh (Co-PI)	$7,656	$2,526	$10,200
Graduate Research Assistant	$24,000	$4,539	$28,500
Undergraduate Assistant	$6,876	$479	$7,400

% OF TOTAL BUDGET:	89%	SUBTOTAL:	$66,400

B. EQUIPMENT: (List each item with a cost in excess of $1000.00.)

Item/Description	Dollar Amount Requested
No equipment required.	
SUBTOTAL:	

G. TRAVEL:

Dates of Travel (from/to)	No. of Persons	Total Days	Transportation	Lodging	Per Diem	Dollar Amount Requested
					SUBTOTAL:	

H. Participant Support Costs:	Dollar Amount Requested
SUBTOTAL:	

I. Other Direct Costs:	Dollar Amount Requested
6. Other (specify nature & breakdown if over $1000) Graduate Research Assistant Tuition	$8,600
SUBTOTAL:	$8,600

J. Total Costs: (Add subtotals, sections A through I)	TOTAL:	$75,000
K. Amount Requested:	TOTAL:	$75,000

Project Director's Signature: Not Required	Date:

INSTITUTIONAL AND OTHER SECTOR SUPPORT

(add additional pages as necessary)

A. INSTITUTIONAL / OTHER SECTOR DOLLARS Source / Description	Amount
B. FACULTY / STAFF POSITIONS Description	
C. CAPITAL EQUIPMENT Description	
D. FACILITIES & INSTRUMENTATION (Description)	

Appendices

Facilities and Equipment

A wide variety of support, teaching, and research laboratories have been developed since the College of Engineering began offering courses in 1997. Micron Technology donated $6 million, matched by other industrial and private donors to construct the Micron Engineering Center (MEC), one of the primary facilities for the College of Engineering and the current location of the Computer Science Department. This four-story building opened in January 2000, and supplies state of the art classrooms, teaching and research laboratories, and offices for faculty, students, student clubs, and postdoctoral fellows. The College of Engineering occupies approximately 132,000 square feet in the Micron Engineering Center, the Engineering Building, the Environmental Research Building, the Harry Morrison Engineering Laboratory, and other buildings on campus. There are 3 large computer server rooms in the College of Engineering with special air conditioning and climate controls.

Expansion for Computer Science Facilities Summer 2016

The Computer Science Department currently occupies approximately 8,260 ASF in the engineering complex. Included in this is faculty offices, teaching labs, research labs, graduate student offices, and the department offices. This does not include common use areas such as classroom, conference facilities etc. With the projected growth of the student body and faculty in the Computer Science department, the currently allocated space would not be sufficient to support the department. To support this growth trajectory, and provide adequate space to accommodate the department, Computer Science will be relocating into a new facility located in the center of downtown Boise. Located approximately 0.5 miles from the Boise State University campus, the new facility is within easy walking distance, and will be served by a free shuttle bus system that is available on an 8 minute frequency. This new downtown building also includes the main transportation hub for the entire Boise City bus system, truly locating Computer Science at the center of Boise.

The new building, the City Center Plaza, is a 9 story building and will be completed in the summer of 2016. The Computer Science department will fully occupy the second and third floor of the building, with a total footprint of 53,549 GSF. The downtown area is home to a large number of software development firms, including one of the largest in Boise who will be co-located in the upper floors of the building, providing a unique opportunity for the collaboration between industry and students. The new facility will include server rooms, a visualization center, tutoring center, 34 faculty/staff and departmental offices, 6 classrooms, conference rooms, focus rooms, graduate student offices, outdoor balconies and community meeting and gathering spaces.

We will be given occupancy during the summer of 2016. Many of the resources described in this document will either be relocated, or replaced with new hardware and systems at the time of the move. Network services in the new location will be the same as described below in this document. The facility will be connected to the university core on dark fiber. The initial connection will be 10 gig, scalable to meet future needs with additional optics. One gig connection will be available to all connected network devices at the site. Wireless connectivity will be provided through dense 2.4 ghz and 5 ghz wireless AC radios.

Computer Science Servers

The CS department-maintained MEC 305 is a climate controlled server room which houses the Beowulf Cluster Lab. This lab was originally funded by a NSF MRI grant. Since then, it has received additional funding from the DoD, FAA, NASA, and several private companies. Currently, the lab has four clusters with approximately 184 processors, 500 GB of RAM, and over 100 TB of storage. The GeneSIS storage cluster, a 21 node Beowulf style cluster. Two of the clusters run Hadoop for the study of big data. One cluster utilizes 56Gb/s Infiniband. The other cluster uses traditional Ethernet connections. Both clusters run Apache Ambari for management. The dedicated Beowulf style processing cluster has 58 nodes supporting Intel dual core Xeon processors.

Computer Science Teaching and Research Labs

The Computer Science department maintains a 32 workstation Linux lab for students. This lab has special software and hardware to support advanced Computer Science courses, including Microsoft Windows which is available through virtualization. This laboratory is sponsored by MetaGeek, a Boise-based software company that is a leader in the field of wireless network analysis software. The Computer Science Department also maintains a tutoring center that houses 30 computers and 1 teaching station. This lab has Linux software that supports the introductory CS courses. The Department employs approximately 20 undergraduate lab assistants and graduate teaching assistants each semester who support of a variety of courses. The tutoring center was established with support from the IGEM grant.

Biographical Sketch for Gaby Dagher (PI)

Professional Preparation

Ph.D. in Computer Science, Concordia University, December 2015
M.A.Sc. in Information Systems Security, Concordia University, August 2011
B.Comp.Sc in Computer Science, Concordia University, August 2002
B.Eng. in Engineering Management and Construction, Damascus University, August 1993

Appointments

Jan. 2016 - Present :	Assistant Professor, Computer Science, Boise State University
June. 2014 – Dec. 2016:	Research Assistant, Data Mining and Security Lab, McGill University
June 2013 - May 2015:	Instructor, Computer Science, Concordia University
Sept. 2011 – Dec. 2015:	Research Assistant, CIISE, Concordia University

Selected Publications

[1] Gaby G. Dagher, Benedikt Bünz, Joseph Bonneau, Jeremy Clark, and Dan Boneh. Pro- visions: Private Proofs of Solvency for Bitcoin Exchanges. In CCS, 12 pages, 2015.

[2] Gaby G. Dagher, Farkhund Iqbal, Mahtab Arafati and Benjamin. C. M. Fung. Fusion: Privacy-preserving Distributed Protocol for High-Dimensional Data Mashup. In IC- PADS, 10 pages, 2015.

[3] Mahtab Arafati, Gaby G. Dagher, Benjamin. C. M. Fung, and Patrick C. K. Hung. D-Mash: A Framework for Privacy-Preserving Data-as-a-Service Mashups. In CLOUD, 8 pages, 2014.

[4] Omar Abdel Wahab, Moulay Omar Hachami, Arslan Zaffari, Mery Vivas, and Gaby G. Dagher. DARM: A Privacy-preserving Approach for Distributed Association Rules Mining on Horizontally-partitioned Data. In IDEAS, 8 pages, 2014.

[5] Junnan Chen, Courtney Miller, and Gaby G. Dagher. Product Recommendation System for Small Online Retailers Using Association Rules Mining. In ICIDM, 6 pages, 2014.

[6] Gaby G. Dagher and Benjamin. C. M. Fung. Subject-based Semantic Document Clustering for Digital Forensic Investigations. DKE, Elsevier, vol. 86, pp. 224-241, 2013.

[7] Gaby G. Dagher, Benjamin. C. M. Fung, Noman Mohammed, and Jeremy Clark. SecDM: A Privacy-preserving Framework for Confidential Query Processing on the Cloud. TCC. 14 pages. Submitted.

[8] Gaby G. Dagher, Jeremy Clark, and Benjamin. C. M. Fung. Publicly Verifiable Protocol for Data Integration with Differential Privacy. PoPETs. 14 pages. Submitted.

Teaching Experience

Boise State University :
CS253 (Undergraduate Course): Introduction to Systems Programming. Spring 2016

Concordia University :
INSE 6190 (Graduate Course): Wireless Network Security. Winter 2015
INSE 6180 (Graduate Course): Security and Privacy Implications of Data Mining. Winter 2014
INSE 6190 (Graduate Course): Wireless Network Security. Summer 2013

Student Advising

Boise State University:
Ishita Dwivedi, Master's student in Computer Science, Boise State University.
Thesis Topic: Privacy Preserving Data Publishing on the Cloud. Spring 2016–Present

Concordia University:
Mahtab Arafati, Omar Abdel Wahab, Moulay Omar Hachami, Arslan Zaffari, Mery Vivas Master's student in Information System Security. 2012–2014

Academic Reviewing Services

International Conference on Knowledge Discovery and Data Mining (SIGKDD), IEEE International Conference on Big Data (BigData), Information Systems Frontiers Journal (ISFJ), IEEE International Conference on Data Engineering (ICDE), Proceedings of Very Large DataBases (PVLDB), ACM Transactions on Database Systems (TODS), IEEE International Conference on Services Computing (SCC), International Conference on Information Science, Signal Processing and their Applications (ISSPA), IEEE International Conference on Data Mining (ICDM), Elsevier Data & Knowledge Engineering (DKE).

Professional Experience

Infor Lawson Software, Montréal, QC, Canada
Technical Engineer April 2008 - July 2011

Freeborders Corp., Montréal, QC, Canada
Software Developer & Project Lead Sept. 2003 - March 2008

Karat Software Inc., Montréal, QC, Canada
Software Developer & Configuration Manager January 2001 - August 2003

Awarded Grants in Past Five Years

Fresh Ph.D. Thus, no awarded grant yet.

Biographical Sketch for Jyh-haw Yeh (Co-PI)

Professional Preparation

University of Florida	Gainesville, Florida	Computer and Information Science and Engineering	Ph.D., 1999
Cleveland State University	Cleveland, Ohio	Computer and Information Science	M.S., 1993
National Chung-Hsin University	Taichung, Taiwan	Applied Mathematics	B.S., 1988

Appointments

2015-current	Program Coordinator of the CS Teacher Endorsement Graduate Certificate Program, Boise State University
2000-2016	Assistant Professor, Boise State University
2013-2015	Co-director of IDoTeach Program, Boise State University
1996-1999	Teaching/Research Assistant, University of Florida

Selected Publications

1. Hung-Min Sun, Chia-Yun Cheng, Jyh-Haw Yeh, and Shouan-Tung Chen, "A Shoulder Surfing Resistant Graphical Authentication System," To appear in *IEEE Transactions on Dependable and Secure Computing*, 2016.
2. Jyh-haw Yeh, Fiona Zeng and Thoms Long, "P2P email encryption by an identity-based one-way group key agreement protocol," *The 20th IEEE International Conference on Parallel and Distributed Systems (ICPADS)*, December 2014.
3. Jyh-haw Yeh, "The insecurity of two proxy signcryption schemes: proxy credential forgery attack and how to prevent it," *Journal of Supercomputing*, Springer, Vol. 70, No. 3, pp. 1100-1119, 2014.
4. Jyh-haw Yeh, "An Efficient Time-Bound Hierarchical Key Management Based on Tamper-Resistant Devices," *2013 IEEE International Conference on Computer Science and Automation Engineering (CSAE)*, 2013.
5. Jyh-haw Yeh, "Enforcing non-hierarchical access policies by hierarchical key assignment schemes," *Information Processing Letters*, Elesvier, Vol. 110, No. 2, pp. 46-49, 2009.
6. Jyh-haw Yeh, "An RSA-Based Time-Bound Hierarchical Key Assignment Scheme for Electronic Article Subscription," *Proceedings of the ACM Fourteenth Conference on Information and Knowledge Management (CIKM)*, short paper, 2005.
7. Jyh-haw Yeh, Marion Scheepers and Wen-chen Hu, "Modifying YCN Key Assignment Scheme to Resist the Attack from Hwang," *Information Processing Letters*, Elsevier, Vol. 95, No. 4, pp. 435-440, 2005.
8. Jyh-haw Yeh, Wei Zhang, Wen-chen Hu and Chung-wei Lee, "Design and Simulation of a Supplemental Protocol for BGP," *Computer Networks*, Elsevier, Vol. 49, No. 2, pp. 172-200, 2005.

9. Jyh-haw Yeh, Randy Chow, and Richard Newman, "A Dynamic Interdomain Communication Path Setup in Active Network," *The First International Working Conference on Active Network*, Springer, Lecture Notes in Computer Science 1653, 1999.
10. Jyh-haw Yeh, Randy Chow, and Richard Newman, "Interdomain Access Control with Policy Routing," *Proceedings for the sixth IEEE Computer Society Workshop on Future Trends of Distributed Computing Systems (FTDCS'97)*, 1997.

Synergistic Activities

NSF Panelist: Cyber Trust (CT) 2008.

Professional services:

- Journal Editor: Guest Editor of the special issue “Security and Privacy in Distributed Sensor Networks” for the International Journal of Distributed Sensor Networks (2014); Editorial Board of the Journal of Computer Science and Systems Biology since 2011; Associate Editor of the International Journal of Handheld Computing Research since 2009; Editorial Review Board of the International Journal of E-Business Research (2004-2008)
- Conference Track Chair for I-SPAN 2014; Workshop Chair for IEEE CIT 2013; Session Chair for IEEE ATC 2015
- Conference Program Committee: CCBD (2015, 2016), IEEE UMEDIA 2013, SERA (2009, 2010), CSIE 2009, and IRMA (2004, 2005)

High School Workshops: Hosting App Inventor Workshop for Meridian High School Technology Student Association (11/14/2013); Hosting Coding is Cool Summer Workshop (use AppInventor and Processing) for Treasure Valley High School Teachers/students (6/13-6/14/2013 and 6/19-6/20/2014)

Awarded Grants in Past Five Years

- BAA HSHQDC-14-R-B0014, Cyber Security Division, Department of Homeland Security, "P2P Email Encryption Using Identity-based One-way Group Key Agreement," PI: Jyh-haw Yeh, Co-PI: Dianxiang Xu. 11/2015 - 10/2017, $747,344. (Recommended for Funding)
- Google CS4HS Grant, “Mobile Computer Science Principles,” PI: Amit Jain, Co-PI: Jyh-haw Yeh, Alark Joshi, Timothy Andersen, Marissa Schmidt. 6/17/2015 – 6/19/2015, $24,233.
- NSF “REU Site: Software Security,” PI: Dianxiang Xu, Co-PI: Jyh-haw Yeh, Izzat Alsmadi. 3/01/2015 – 2/28/2018, $324,000.
- NSF CE21, “CS10K: IDoCode: A Sustainable Model for Computer Science in Idaho High Schools,” PI: Amit Jain, Co-PI: Jyh-haw Yeh, Alark Joshi, Tim Andersen, Jonathan Brendefur. 3/01/2014 – 2/18/2017, $992,067.
- Amazon Web Services in Education – Research Grant, "Data Privacy Protection for Relational Database Service (RDS) - Proof of Concepts for a Semantic Hiding Database (SHDB) Approach," PI: Jyh-haw Yeh, 10/01/2013 - 10/31/2015, $5,000.
- Amazon Web Services in Education – Course Grant, "Data Structures Course Project using AWS", PI: Jyh-haw Yeh, 9/01/2013 - 9/30/2014, $4,000.

BOISE
CITY OF TREES

POLICE
BOISE CITY
IDAHO

Boise Police Department

William L. Bones
Police Chief

Boise Police Dept.

333 N. Mark Stall Place
Boise, ID 83704-5511

Phone
208/570-6000

Fax
208/570-6049

TDD/TTY
800/377-3529

Web
www.cityofboise.org/police
www.boisepolice.org

Mayor
David H. Bieter

City Council
President
Maryanne Jordan

Council Pro Tem
Elaine Clegg

Scot Ludwig
Lauren McLean
Ben Quintana
TJ Thomson

March 31, 2016

RE: Cyber-Forensic Investigation Toolkit Development

To Whom It May Concern:

I am writing to express support for Boise State University's application to the State Higher Education Research Council for a grant to develop a cyber-forensic investigation toolkit. The Boise Police Department works closely with BSU on a variety of issues and this project would be beneficial to the University as well as to the Department.

The officers and investigators of the Boise Police Department respond on a daily basis to reports where information stored on a suspect's computer is essential to solving a case. These calls for service vary from help in locating a missing person to identifying a pattern of behavior in a stalking case or unraveling fraud related phishing scams. In 2015, BPD saw a 20.4% increase in fraud reports related to false pretense and swindling when compared to the previous year. In many of these reports the suspect is unknown to the victim and is likely committing the crime from a location outside the jurisdiction by using technology. BPD also saw a 30.4% increase in intimidation and stalking cases during the same time frame. Again, key pieces of evidence were stored on computers and related devices that aided investigators in achieving justice for many of the victims.

As with any piece of evidence, the ability to quickly locate, capture, and analyze it is a must for law enforcement. A program that could easily connect to evidence related devices, capture large amounts of data, and generate useful analytics would provide law enforcement with immediate insight, saving case integrity and hours of manpower. I appreciate this opportunity to lend my support to this application.

Sincerely,

William L Bones

William L. Bones
Chief of Police
Boise, ID

Idaho State Police

Service Since 1939

Colonel Ralph W. Powell
Director

C.L. "Butch" Otter
Governor

April 1, 2016

State Higher Education Research Council
Idaho State Board of Education
650 West State Street
Boise, ID 83702

To Whom It May Concern,

The Idaho State Police is very supportive of the efforts of Idaho's institutions of higher education in developing tools to assist law enforcement in protecting the public and solving crimes. The efforts of Boise State University and Dr. Gaby Dagher in developing a toolkit to assist law enforcement with cyber forensic investigations is exciting and could be a true benefit to law enforcement, not only in Idaho but nationwide.

The proliferation of computers, smart phones, tablets and other portable digital devices are intertwined in our daily lives and are largely the way people communicate. This is no different for those operating in the criminal element. Criminals use computers, mobile phones and devices to further their criminal acts. Digital evidence is critical in most criminal cases from drug trafficking and financial crimes to violent crimes such as homicides, rapes, and child sexual abuse.

The gathering and analysis of digital information is vital to the prosecution of those committing these crimes. Law enforcement is allowed to gather this type of evidence with the permission of the court. Our agency alone serves approximately 700 search warrants each year on electronic devices.

A toolkit for use by law enforcement to collect the digital information from a computer, mobile phone, disc or flash drive would be valuable. The information collected can be used to confirm or disprove a suspect's statements, identify co-conspirators, prove motive or criminal intent, provide photos showing the actual crimes being committed and, many times, can lead to the discovery of plans of future crimes that police can now prevent.

The Idaho State Police support the efforts of Boise State University and Dr. Gaby Dagher in securing a grant from the State Higher Education Research Council to develop a toolkit to assist in cyber forensic investigation.

Sincerely,

Lt. Colonel Kedrick Wills
Deputy Director