CTIN 2017 DIGITAL CONFERENCE
April 12 – 14, 2017

WEDNESDAY, APRIL 12, 2017					
7:30	***7:45***	***Lobby***	***REGISTRATION***		
7:45	***8:00***	***Trident***	***Allison Goodman***	***CTIN PRESIDENT***	**Welcome to Microsoft Campus and CTIN 2017**

Start	***End***	***Room***	***Speaker***	***Title***	***Description***
8:00	9:00	Trident	David Stenhouse DS Forensics	The Role of the Neutral	The role of a "neutral" examiner brings significant challenges. Frequently the Order or other guidelines under which you are working are sorely lacking in detail or worse, contain requirements that are technically impossible. Learn how to navigate these sticky wickets while maintaining your integrity and professionalism.
8:00	9:00	Thunder	Lab		*Intella and X1*
9:15	10:15	Trident	Gordon Mitchell, PhD eSleuth	Powershell for Forensics	Microsoft Powershell is really useful. We hear of security folks using it to manage 10,000 servers and other immense tasks. This talk is, however, just an intro to the Powershell capabilities that can be useful for forensics. Examples will be illustrated for those (like me) who are just beginning to explore the world of Powershell.
9:15	10:15	Thunder	Lab		*Intella and X1*
10:30	11:30	Trident	Troy Larson Microsoft	Windows Hyper-v VM Forensics	Learn some of the unique differences in analyzing a virtual machine including cloud based systems.
10:30	11:30	Thunder	Lab		*IEF and Axiom*
11:30	***12:30***	***Trident***	***LUNCH***		Vouchers for Microsoft cafeteria
12:30	1:30	Trident	Scott Tucker Aptegra Consulting	Email Forensics: A Case Study	Scott will share his experience in being able to conclusively identify a person that created misleading email addresses to perpetuate significant fraud on a number of companies and individuals.
12:30	1:30	Thunder	Lab		*IEF and Axiom*

WEDNESDAY, APRIL 12, 2017					
1:45	2:45	Trident	Colin Cree	Web-Sites and Social Media	Collection of Internet based information such as websites, social media and webmail has become a regular event for investigators. This session will provide exposure to methods to effectively collect and preserve data from the Internet
1:45	2:45	Thunder	Lab		*Vehicle Forensics, IvE and Elcomsoft Phone Breaker*
3:00	4:00	Trident	Cellebrite	TBD	
3:00	4:00	Thunder	Lab		*Vehicle Forensics, IvE and Elcomsoft Phone Breaker*

THURSDAY APRIL 13, 2017

Start	*End*	*Room*	*Speaker*	*Title*	*Description*
8:00	9:00	Trident	Brandon Leatha iDiscovery Solutions	Investigating Data Exfiltration	The "insider threat" is behind a significant portion of data loss and exfiltration. The actions of employees, malicious or unintentional, can have a significant financial impact on companies large and small. This session will cover common tools and techniques for investigating the loss of data through USB devices, cloud synchronization, email forwarding, and more!
8:00	9:00	Thunder	Lab		*Griffeye Analyze, Paladin Pro USB*
9:15	10:15	Trident	Sherri Davidoff LMG Security	Held for Random: Ransomware Prevention and Response	All it takes is one person clicking on a link, and all of your shared files could be locked up for good. Organizations of all kinds— from corporations to non-profits to government agencies— are held hostage by ransomware, the malicious software that encrypts your data until you pay a hefty fee. How can you reduce your risk of a ransomware incident in today's complex environments, and how should you respond if you fall victim? We'll show you a video of a real ransomware infection, taken in LMG's cybersecurity laboratory, and provide tips for prevention and response.
9:15	10:15	Thunder	Lab		*Griffeye Analyze, Paladin Pro USB*
10:30	11:30	Trident	Terry Lehman eForensics Pro	Size or Performance – What's more Important?	This presentation provides information about evaluating your digital forensics hardware and software needs while balancing the competing issues of cost and productivity. While we all wish we had huge budgets to purchase the latest and greatest hardware, software, and training, for most of us that isn't reality. Balancing costs with the needs of the organization can impact the budget and the examiner's ability to complete work assignments. Comparing and evaluating are key to finding the sweet spot between cost and productivity while also considering your forensics work environment. The presenter

THURSDAY APRIL 13, 2017

					shares his journey to finding the sweet spot for his business model.
10:30	11:30	Thunder	Lab		*Forensic Explorer and Mount Image Pro*
11:30	**12:30**	***Trident***	***LUNCH***		Will be provided vouchers to Microsoft cafeteria
12:30	1:30	Trident	Amelia Phillips Highline CC	Future Pacing Digital Forensics	With the IoT and more items coming online, what are the challenges for digital forensics? What new tools and approaches are needed? In today's world there are machine to machine, person to machine and person to person interactions - all done online. How does one go about doing the investigations? What new things are coming? Come and explore the future of digital forensics.
12:30	1:30	Thunder	Lab		*Forensic Explorer and Mount Image Pro*
1:45	2:45	Trident	Zeke Thackray Get Data	Investigating Graphic & Video Related Cases	Metadata can quickly change the focus of an investigation. We will cover skin-tone analysis, video keyframe carving and an abundance of other issues relating to multimedia movies and graphics.
1:45	2:45	Thunder	Lab		*EnCase 8 and Ditto Forensic FieldStation*
3:00	4:00	Trident	Prof. Tim Carver Trine University	Bitcoin Forensics	This presentation will examine the protocols used to provide the secure transfer of funds over the World Wide Web. We will see how new Bitcoins come into existence (mining) and look at the basic protocols – Then we will look at Bitcoin from a forensic point-of-view. What artifacts are left behind and where can they be found will be discussed.
3:00	4:00	Thunder	Lab		*EnCase 8 and Ditto Forensic FieldStation*

FRIDAY APRIL 14, 2017

Start	*End*	*Room*	*Speaker*	*Title*	*Description*
8:00	9:00	Trident	Jamie McQuaid Magnet Forensics	The Dark Side of P2P Apps and Share Content in the Forensic Landscape	More and more illicit content is being shared via P2P (Peer to Peer) apps and more advanced techniques such as streaming are making these investigations more difficult. Developing the right techniques to examine those apps is imperative. Join forensics experts to discuss the implications of the growing popularity of P2P apps for chatting, sharing files, streaming video and live content. Examine how the growing use of mobile apps and Internet is impacting the ubiquity of content being shared and viewed on P2P apps and networks. Learn how to investigate these apps and content and understand how people are trying to cover their use of P2P.
8:00	9:00	Thunder	Lab		*Cellebrite*
9:15	10:15	Trident	Eric Moore Teel Technologies	Advanced Mobile Extraction Techniques	As modern mobile devices increase in both popularity and sophistication, completing a forensic examination has become more difficult. With advances in mobile device technology, advances have to be made in both techniques and skillsets to obtain the digital evidence that these devices hold. In this session we will discuss advanced techniques used to obtain data from mobile devices, including physical techniques such as Joint Test Action Group (JTAG), In-System Programming (ISP), Chip-off, and software based tools such as bootloaders.
9:15	10:15	Thunder	Lab		*IEF and Axiom*
10:30	11:30	Trident	Cecelia Gregson King County Prosecutor Det. Randy Kyburz	Locked and Encrypted–Legal & Technical Options for Accessing	Mobile devices are a strong source of evidence, but how do we get access to that that evidence when the device is secured? This presentation will provide a high-level technical exploration of options to gain

FRIDAY APRIL 14, 2017

			Seattle PD ICAC	Secured Mobile Devices	access to secured devices and the legal options and implications of doing so.
10:30	11:30	Thunder	Lab		*IEF and Axiom*
11:30	**12:15**		***LUNCH***		Will be provided vouchers to Microsoft cafeteria
12:15	**12:30**		**RAFFLE**	**VENDOR SPONSORED RAFFLE ITEMS**	***MUST BE PRESENT TO WIN!!***
12:30	1:30	Trident	Jesse Bollerud Redmond PD	Intro to Digital Crimes, a Police Perspective	When private sector finds evidence of criminal activity – what next? How to report and maintain chain of custody. Proper methods of gathering, protecting and preserving digital devices and data will be demonstrated.
12:30	1:30	Thunder	Lab		*JTAG and Chip-Off – Teel Technology*
1:45	2:45	Trident	Ellen Blanchard T-Mobile	How Changes to the Federal Rules Could Impact eDiscovery Collections	Changes to the Federal Rules of Evidence are slated to take effect in December 2017, including changes to the authentication methods for electronically stored information (ESI). The changes now allow for data to be authenticated using the document's hash values which will put additional pressure on companies to use methods of collection that generate hash values. Since the collections being done today may be used as evidence after the rules take effect, they are already having an impact in the world of forensic collections.
1:45	2:45	Thunder	Lab		*JTAG and Chip-Off Demo – Teel Technology*
3:00	4:00	Trident	Russ McRee Microsoft	DFIR Redefined	Those of us who operate within the constructs of digital forensics and incident response understand the nuances of the related acronym (DFIR) intimately. This presentation will offer insight on a slightly different take on DFIR using R, the open source programming language and software environment for statistical computing and graphics. Forensics and incident response both suffer from, and can benefit from, the data explosion. That said, modern DFIR programs are obligated to

FRIDAY APRIL 14, 2017

					embrace and attempt to master security data science. Doing so effectively can lead to vastly improved visualization, and behavioral analysis. We'll discuss such opportunities and provide an overview of some basic tools, tactics and procedures to get you started. Code examples will be included and shared for practice and exploration.