CTIN 2019 DIGITAL CONFERENCE

May 22– 24, 2019

Microsoft Commons Mixer, Bldg 98
15255 NE 40th St., Redmond, WA 98052

WEDNESDAY, May 22, 2019

8:00	***8:15***	***Lobby***	***Microsoft REGISTRATION***		Microsoft doesn't open until 8 am! Come prepared with ID and CAR LICENSE PLATE
8:15	***8:30***		***CTIN Registration***		
8:15	***8:30***	***2003***	***Allison Goodman***	***Welcome to CTIN 2019***	**Welcome to Microsoft Campus and CTIN 2019**

Start	***End***	***Room***	***Speaker***	***Title***	***Description***
8:30	**9:30**	**2003**	**Keynote Kirk Arthur**	**Partnerships in Forensics**	**Leveraging resources across all groups (public/private, public/public, private/private) to increase solvability**
9:45	10:45	2003	Colin Cree	F-Response	
9:45	10:45	2007	Mark Spencer	Advancements in Windows Hibernation and Crash Dump Forensics	
11:00	Noon	2003	Maryellen Skelton	Production of Cell Phone Data	
11:00	Noon	2007	Steve Beltz	Metadata and Open Source Investigations	Using open source intelligence (OSINT), the attendees will be shown how to go past surface, internet searches and take a deep dive into the web using advanced online search techniques. We will also discuss how to examine and properly collect the information that is found during the investigation. This will include knowing how to understand metadata which is often found with any user-created file to include photographs and documents.
Noon	***1:00***	***2003***	***LUNCH***		Vouchers for Microsoft cafeteria
1:00	2:00	2003	Steve Beltz	Data Analysis in Support of Criminal Investigations	In this session, using real criminal case scenarios and readily available software, such as Excel, Power BI, and Google Earth, we will learn how the data located and received, how the data is organized, and how the data is used to support criminal investigations. Techniques will include,

WEDNESDAY, May 22, 2019

					finding data points in various sources, converting pdf's to tables, locating and exporting tables from websites, formulas, pivot tables, data linking, charting options and the use of dashboards for analysis.
1:00	2:00	2007	Jeff Whitney	Imaging and Analysis of iOS and Android phones	
2:15	3:15	2003	Matt Durrin	Banking Trojans	
2:15	3:15	2007	Brandon Leatha	Cloud Forensics	
3:30	4:30	2003	Trey Amick	Finding the Hidden Evidence on iOS and Android Devices	Another year, another iOS update, another sweet-shop-sounding Android OS. Each new update for a mobile OS represents a new puzzle for digital investigation teams. With a continued focus on encryption and code optimization, there are always new nuances that need to be discovered and explored.
3:30	4:30	2007	Robert Merriott	Documenting Investigations in a Digital World	

THURSDAY   May 23, 2019

Start	*End*	*Room*	*Speaker*	*Title*	*Description*
8:30	9:30	2003	Russ McCree, GSE, MSISE Principal Security GPM, Microsoft	DFIR Redefined: Deeper Funcationality for Investigators with R	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 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.
8:30	9:30	2007	Scott Tucker	Sqlite Databases	
9:45	10:45	2003	Pierson Clair	Mac Hardware Triage & Acquisition	
9:45	10:45	2007	Brian Hurd/Jarod Alexander	Coming Soon	
11:00	Noon	2003	Pierson Clair	What's New in Mac Forensic Artifacts	
11:00	Noon	2007	Ernie Hayden	Footprinting of Physical and Cyber Assets	Discuss the concept of "Footprinting" and how the basic techniques of this "term of art" could be used to attack or "hack" a target.
Noon	**1:00**	***2003***	***LUNCH***		Will be provided vouchers to Microsoft cafeteria
1:00	2:00	2003	Judge Trickey Sean Selin KL Gates	MOCK HEARING	Experienced expert will be subject to direct and cross examination by attorneys knowledgeable in digital forensics

THURSDAY   May 23, 2019

1:00	2:00	2007	Terry Bodeker	Coming Soon	
2:15	3:15	2003	Judge Trickey Sean Selin KL Gates	MOCK HEARING	5 randomly selected participants will experience testifying for 10 – 15 minutes simulating an actual courtroom situation.
2:15	3:15	2007	Jim Clark	Using the SOF-ELK VM to Effectively Detect Intrusions	
3:30	4:30	2003	Tim Carver	Blockchain Fundamentals	
3:30	4:30	2007	Mark Spencer	High Stakes Evidence Tampering	

FRIDAY, May 24, 2019

Start	*End*	*Room*	*Speaker*	*Title*	*Description*
8:30	9:30	2003	Troy Larson	Investigating Compromise and Breach	
8:30	9:30	2007	Amelia Phillips	Security and Forensics in the IoT	The Internet of Things (IoT) presents a challenge not only in the securing of all the devices that can access your network, talk to each other and make decisions. It also makes it a challenge in performing a forensics analysis of all the devices which vary widely in terms of hardware, software and firmware. This talk will address some of the solutions and a path forward in this ever-changing landscape.
9:45	10:45	2003	Randall Karstetter	Web Site Forensics; Total Acquisition of a Website and Harvesting Chats, User Information etc.	This explores a case where several men in the high-tech industry created and maintained a private web site which operated like a YELP! customer review venue for prostitutes. The website had tens of thousands of communications in both private and public forums strictly monitored and access restricted by web admins. The challenge was to capture the entire website and to somehow recover all these chats from the web databases and format them for easy reading and make them searchable. The presentation goes through the technique for acquiring the entire web site, the tools and techniques that didn't work to harvest the chats and then the tools, and how to use them, that did work. In addition to the chats, a wealth of other information about the registered users, web site function, old web pages and admin notes were found which means total exploration of a web site can be conducted. Topics and techniques presented should be applicable to most web sites and web sites using SQL databases in particular. Performing a complete acquisition and investigation of a web site is not a common occurrence (I couldn't find any online help) but this presentation should prepare a forensic investigator with the tools and methods in case such an investigation is warranted.
9:45	10:45	2007	Brett Shavers Amelia Phillips Bill Nelson	Writing a Digital Forensic Book	These 3 authors will discuss the perils, pitfalls and joys of not just writing a book on forensics but getting it published.
11:00	Noon	2003	Tim Carver	Bitcoin Forensics	

FRIDAY, May 24, 2019

11:00	Noon	2007	Brett Shavers	GeoLocation Data	
Noon	**12:45**		***LUNCH***		Vouchers to Microsoft cafeteria
12:45	**1:00**	**2010**	**RAFFLE**	**VENDOR SPONSORED RAFFLE ITEMS**	***MUST BE PRESENT TO WIN!!***
1:00	2:00	2003	Ryan Ferreira	Cell Tower Data	This session will include an overview of what Call Detail Records (CDRs) are, provide some examples of CDRs, and cover some of the myths and pitfalls commonly seen when dealing with CDR analysis. Case studies will also be included to provide real-world applications for the usage of CDR analysis.
1:00	2:00	2007	Pierson Clair	What's New in Mac Forensic Artifacts	
2:15	3:15	2003	Ryan Ferreira	Cell Tower Data	This session will include an overview of what Call Detail Records (CDRs) are, provide some examples of CDRs, and cover some of the myths and pitfalls commonly seen when dealing with CDR analysis. Case studies will also be included to provide real-world applications for the usage of CDR analysis.
2:15	3:15	2007	Gavin Pinchback	T-Mobile's Law Enforcement Relations	
3:30	4:30	2003	Brett Shavers	WinFE	
3:30	4:30	2007	Gordon Mitchell	Securing a Forensic Lab	