# UTICA UNIVERSITY 2023 Cyber Forensics Student Competition and Conference

Utica University will be hosting the 2023 Cyber Forensics Student Competition and Conference. This student competition and conference event is created as part of Utica University's effort to provide experiential learning opportunities for college students.

The event highlights two significant components: Competition and Conference. The Conference will be a foundational effort that seeks to enhance the current capacities of higher education to better serve students in the areas of cybersecurity, computer forensics, and digital evidence, leading to improve cybercrime investigations and successful prosecutions. The Competition will be held virtually as a team competition a day before the Conference. The final scores and winning teams (the first three teams) will be announced during the award ceremony at the Conference. For this competition, college student teams will engage in cybercrime investigation-focused activities centered on digital forensics.

The theme of 2023 Conference is to **Combat Online Child Exploitation and Victimization.** Online Child Sexual Exploitation has been a serious cybercrime equally as pervasive and abhorrent as traditional exploitation of minors. Perpetrators have mirrored the current trajectory of modernization within society, utilizing contemporary technology such as computers and information systems to sexually abuse children. These abuses come in a myriad of forms, whether it be online grooming, creation and dissemination of exploitative material, or live streaming of sexual abuse. Additionally, legislation states that children can become victims through sex tourism, trafficking, molestation, misleading internet sites or content, online enticement, and unsolicited material being sent to the child themselves. Of these categories, the possession, manufacturing, and distribution of sexual exploitation of a child is the more prevalent form of abuse, as data states that this constitutes about 99.62% of the reported cases last year.

Focusing on the "Targeted Means to Combat Online Child Exploitation and Victimization," the 2023 Annual Conference is an effort to bring disruptive change to cybercrime investigation, exploring innovative techniques and global measures to bring about effective criminal justice policies and establish preventive measures leading to more efficient investigations and successful prosecutions.

The 2023 Conference will serve to enhance current capacities of higher education to better serve students of cybersecurity, computer forensics, and digital evidence, leading to improved cybercrime investigations and successful prosecutions. Pre-registration is required in advance for this conference. The registration link is https://utica-edu.zoom.us/j/94199551868

Friday, April 14, 2023	
9:00 AM – 9:15 AM	<b>Opening Remarks</b> Dr. Leslie Corbo and Professor Andrew Carr Directors of the Undergraduate and Graduate Cybersecurity Programs, Utica University
9:15 AM – 9:30 AM	Welcoming and Congratulatory Remarks Stephanie Nesbitt Dean of the School of Business and Justice Studies Utica University
9:30 AM – 10:30 AM	Keynote Address George Baker Investigator, Troop D – Computer Crime Unit (CCU) New York State Police
10:30 AM – 10:45 AM	Break
10:45 AM – 11:30 AM	Faculty Researchers Panel Dr. Leslie Corbo, Professor Andrew Carr, Professor Suzanne Lynch, and Professor John Oevering
11:30 AM – 11:45 AM	Break
11:45 AM -12:00 PM	<b>Student Competition Award Ceremony</b> The competition results will be announced.
12:00 PM-12:10 PM	Closing remarks

# **Competition Guidelines**

The competition comprises two components: 1) Forensics Capture the Flag (CTF) Challenge and 2) Written Legal Evidence Report. To register your team for the 2023 Capture the Flag Student Competition and Conference, use the following link:

https://docs.google.com/forms/d/e/1FAIpQLSdC\_1P3aFYujodlt8nI1S\_7toSp1OlXvOlME4R2k U3RcAHY6A/viewform?usp=sf\_link

## 1. Forensics CTF Challenge (50 %)

The challenges will lead to flags entered on Capture the Flag Framework (CTFD), an opensource CTF platform that allows tracking progress, completed challenges, and position in the CTF. Each challenge or set of challenges will have varying levels of difficulty to access the flags. Different skillsets and specializations will be required to access and complete the challenges. Challenges are designed with a focus on digital/cyber forensics.

- The challenge will start on April 12, 2023 at 12 pm (Noon) Eastern Standard Time and end midnight on April 13. At the start of the challenge, all teams will be provided with a written scenario detailing the crimes under investigation, along with information the teams are requested to investigate. A rubric clarifying how points are earned is also provided.
- 2) Teams will have until Thursday, April 13, at 5 pm Eastern Standard Time to complete the written legal evidence report. Guidelines are provided in Item 2 of the Competition Guidelines (see below).
- 3) As per Competition Rules and Guidelines, teams can use any technical approach(es), tools, and techniques that they feel are suitable to conduct their investigation of the scenario, provided teams stay within the boundaries of both their legal authority and applicable laws.

# 2. Written Legal Evidence Report (50%)

Teams should produce a written report for the provided scenario, which documents the background of the scenario, the authorized legal request(s) if made, a table of evidence, the collection and analysis process, and a summary of their report before the Thursday, April 13 at 5 pm deadline.

Technical Approach and Techniques Utilized	Utilization of any technical approach(es), tools, and techniques suitable to conduct their investigation of the scenario: An example format for this portion:
	Description of tasks accomplished Description and Rationale for the use of the selected tool(s) used for each task
Evidence Discovered and Categorized	Evidence identification, categorization, and handling procedure to preserve the evidence's integrity and legality: The example below will be duplicated for each piece of evidence.
	Evidence #1: <provide item="" name=""></provide>

Legal Authority	Evidence Description <provide a="" brief="" description="" item="" of="" the="">Evidence Type: <provide a="" evidence<="" of="" summary="" td="" the="" type="">this item belongs to&gt;Special Handling: <provide handling="" required="" special="" td="" to<="">preserve evidence integrity&gt;Authority requests to investigate beyond the current scope ofthe scenario (criminal Investigation): An example below canbe used to describe the situation to contact a "Case Agent" forlegal requests or discussion to resolve the issue.</provide></provide></provide>
	Legal Authority Request #1: <provide> Rationale for Request <provide a="" brief="" description="" of="" the<br="">Rationale&gt; Request Resolution: <provide a="" how<br="" of="" summary="">this request was resolved&gt;</provide></provide></provide>
Summary Analysis of Body of Evidence	Analysis of every individual evidence artifact recovered from the scenario and the team's overall summary analysis of their Investigation. The following items will determine the grading criteria for this section:
	Evidence #1: <provide item="" name=""> Significance to the Investigation: <provide an="" analysis="" on="" the<br="">significance of the evidence to the investigation&gt; U.S. Penal Code or Rationale: <describe evidence<br="" how="" the="">discovered supports your assessment of this crime&gt;</describe></provide></provide>
	Evidence #2: <provide item="" name=""> Significance to the Investigation: <provide an="" analysis="" on="" the<br="">significance of the evidence to the investigation&gt; U.S. Penal Code or Rationale: <describe evidence<br="" how="" the="">discovered supports your assessment of this crime&gt;</describe></provide></provide>
	Evidence #3: <provide item="" name=""> Significance to the Investigation: <provide an="" analysis="" on="" the<br="">significance of the evidence to the investigation&gt; U.S. Penal Code or Rationale: <describe evidence<br="" how="" the="">discovered supports your assessment of this crime&gt;</describe></provide></provide>
	Summary of the Investigation: <provide of<br="" significance="" the="">this Investigation, any closing comments, observations, and/or potential future developments.&gt;</provide>
	An example language: We are able to justify the prosecution of X named individual for the following crime based on the fact that he/she was positively identified committing the following illegal acts, which were supported by the following evidence described in detail above.

#### List of Speakers/Participants

#### Stephanie R. Nesbitt, JD, MBA

Dean, School of Business and Justice Studies and Associate Professor of Risk Management and Insurance

Interim Provost (beginning August 1, 2023)



Stephanie joined the Utica University faculty in August 2012 as an assistant professor in risk management and insurance and director of the risk management academic program. Before joining the Utica University faculty, she spent 16+ years working as a risk manager and practicing attorney in both the retail and healthcare industries. Since joining Utica University, she has held the positions of director- risk management and insurance program, director- MBA programs, and associate dean- business and economics programs.

She received her JD from the University at Buffalo School of Law, MBA from Syracuse University, and BA in Speech Communication from Ithaca College. Stephanie has been a featured speaker at several national, state-wide, and regional industry and academic conferences on topics such as insurance cost allocation methods, the impact of risk management on healthcare quality, individual and team accountability to improve healthcare quality, HIPAA and patient privacy, academic program design in graduate business education, and student engagement as a component of student success. She is a member of the Academy of Management and is licensed to practice law in the state of New York.

Stephanie's research interests lie in the areas of the development and implementation of business education programs, the impact of teaching modalities on student success, and the legal/regulatory/risk implications of business' ever-increasing reliance on cyber technology. Her most recent publications include a co-authored chapter titled "Five Eyes and One Problem" in the June 2020 book Contemporary Intelligence Analysis and National Security: A Critical American Perspective, and the co-authored research article "Bueller...Bueller?: Predictors of Behavioral Engagement, as Measured by Student Attendance, in a Blended MBA Environment," published in the BRC Journal of Advances in Education.

Away from campus, she spends her leisure time much as she does her work hours, in constant motion. Stephanie holds a 3rd degree (san dan) black belt in Shorin-Goju Ryu style karate and was granted the title of sensei in her dojo in August 2014. She is also an avid, albeit slow, runner, hiker, and cyclist.

## Leslie Corbo, D.Sc.

Director, Cybersecurity Undergraduate Programs



Leslie teaches undergraduate and graduate classes in the Cybersecurity program. Dr. Leslie Corbo is the Director of the Undergraduate Cybersecurity Programs at Utica University. Corbo formerly worked for Dragos, Inc. as the Director of Training, developing training products and resources for employees globally in the oil, gas, big chemical, pharmaceutical, and manufacturing sectors. Prior to Dragos, Corbo worked for Cofense (f/k/a PhishMe, Inc.) as a Sr. Information Security Program Manager. Corbo worked with Fortune 500 companies educating employees in information security

practices consulting, planning, simulated execution, and analysis. Additionally, she has worked with renowned universities, including Harvard University and the London School of Economics, collecting data, designing, and conducting studies involving employee behavior towards phishing emails.

Leslie previously worked as a cybersecurity analyst and Information System Security Manager on DoD and DHS Science & Technology efforts, managing information systems while developing, implementing, and enforcing information security policies and procedures. As an IT security analyst, she conducted forensic investigations, analysis, and incident response. Her education includes a D.Sc. in Cybersecurity from Capitol Technology University, an M.S. in Cybersecurity from Utica University, and a B.S. in Cybersecurity and Information Assurance with a concentration in Cybercrime Investigation and Forensics. She also has an A.A.S. degree in Web Development.

Corbo's areas of research include phishing emails, sentiment analysis, and behavior analysis. Her dissertation study involves case studies in the decision-making processing methods utilized by undergraduate students when interacting with malicious emails. Leslie is believed to be the only cybersecurity professor that has ever been published in the Journal of the American Medical Association. Corbo is a member of Women in Cybersecurity, ISACA, and the Colloquium for Information Systems Security Education. She works with the National Initiative for Cybersecurity Education on their academic working group that collaborates with academia, industry, and government.

#### Andrew Carr, M.S.

Director, Cybersecurity Graduate Programs



Mr. Carr currently holds the role of Director, Cybersecurity Graduate programs and Assistant Professor of Cybersecurity focusing on the field of digital forensics and incident response. Andrew previously held the position of Professor of Practice in Cybersecurity at Utica University and prior to that was an Adjunct Instructor for five years. He also actively performs expert witness and ransomware negotiation services as an independent contractor. Andrew spent several years in supervisory roles at leading firms within the demanding field of incident response. In these roles Andrew maintained expertise in digital forensic analysis, threat actor tactics, techniques and procedures, ransomware negotiations, application of data privacy law in relation to breach events, OFAC compliance, financial audit considerations for cyber incidents, intellectual property theft investigations, and cryptocurrency tracing. Andrew was part of several hundred incident investigations during his time in the incident response field ranging from healthcare providers to private equity firms and educational institutions.

Prior to Utica University Andrew spent more than eight years as a senior computer forensic examiner at the Wallie Howard Jr. Center for Forensics Sciences. In that role Andrew performed forensic examinations on a multitude of digital devices while upholding strict accreditation requirements under ISO/IEC 17025 standards and routinely testified in federal and state courts. During this time, he also worked as part of the New York State Digital and Multimedia Technical Working Group to help further the science of computer forensics and assist agencies in preparing for accreditation in conducting computer forensic analysis. He ultimately trained for and became a technical assessor for the ANSI National Accreditation Board for testing laboratories operating under ISO/IEC 17025 standards in the discipline of digital forensics.

Andrew's educational background includes an Associate's degree in Criminal Justice from Mohawk Valley Community College, Bachelor's degree in Cybersecurity Information Assurance from Utica University, and a Master's Degree in Cybersecurity Intelligence and Forensics from Utica University. Andrew has received extensive computer forensics training from industry leading organizations including SANS, IACIS, NCFI and NW3C and currently holds GIAC Certified Incident Handler (GCIH) and CipherTrace's Cryptocurrency Tracing Certified Examiner (CTCE) certifications.

# Suzanne Lynch, M.S.

Director, Financial Crime and Compliance Management Programs



Suzanne Lynch MS Professor of Practice – Economic Crime, has extensive experience in fraud, money laundering and cybercrime investigations for Fortune 500 companies working with national and international law enforcement agencies. Professor Lynch has conducted numerous training sessions on fraud detection, prevention and investigations for global law enforcement groups as well as financial institutions throughout the world.

Lynch is the Director of Financial Crime Program undergraduate and graduate degrees at Utica University. She has designed numerous academic courses for both that study the application of economic crime theories to current challenges in the field of fraud and financial compliance investigations and the management of those efforts. Her outreach has drawn partnerships with entities like the Association of Certified Anti Money Laundering Specialists (ACAMS), the U.S, Marshals Service, the Army National Guard Counterdrug Task Force, The Anti-Human Trafficking Intelligence Initiative (ATII) and CipherTrace to invest professional effort in aligning respective personnel with tailored academic programs. She holds a BS degree in Criminal Justice from Wayne State University in Detroit, Michigan and a MS in Economic Crime Management from Utica University.

## John Oevering, M.S., MBA

Endpoint Engineer and Information Security Officer, Utica University Adjunct Lecturer, Utica University



John Oevering is the Endpoint Engineer and Information Security Officer and Adjunct lecturer for Utica University. Earning both a Master of Science and Master of Business Administration in Cybersecurity from Utica University, John has rebuilt Utica University's information security team. In his role, John oversees all physical endpoint hardware and software and develops and maintains information security policies and procedures for the Utica University community.

John is committed to promoting a safe and secure learning environment and has focused his research into cybersecurity issues within higher education. As an adjunct lecturer, John has redesigned CYB 237- Network Security to align with the Network + certification.