Cybercrime Investigation Competition

Cybercrime Investigation Competition Instructions

The 2022 competition will be held virtually as a team competition. For this competition, college student/practitioner teams will engage in cybercrime investigation-focused activities centered on digital forensics. The goal of the competition is to develop effective cybercrime investigation training, test the best practices reflecting the needs of all levels of law enforcement, and establish training guidelines in computer forensics and digital evidence.

The White Hat Cybercrime Investigation Competition will serve as a pathway to evaluating and promoting common goals, needs, and interests associated with technical skills and legal expertise that lead to comprehensive high-level cybercrime investigation educational learning and skill development. BU has created an evidence-based digital case scenario framework that provides competitors with realistic scenarios that reflect major cybercrime cases.

The 2022 International White Hat teams will compete for 24 hours from May 31 to June 1, which is the first day of the White Hat Cybercrime Investigation Competition. Information regarding the competition is detailed below:

Awards:

- Winning Team: $1,000 prize
- In addition to the winning prize, each member of the winning team will be awarded a $1,000 scholarship (a total sum of $3,000 per team) to be applied to the tuition of BU MET's Cybercrime Investigation & Cybersecurity Graduate Certificate.

Eligibility:

Undergraduate students, graduate students, and government employees in the field of criminal justice are all eligible. Each team will be made up of three members: 1) Desktop Forensics 2) Mobile Forensics, and 3) Legal Specialist.

Key Dates:

- March 2022: Competition Registration Opens
- April 2022: Competition Registration Closes & Selection of Participants
- May 2022: Access to Competition Platform
- May 31-June 1, 2022: Competition Day
- June 2, 2022: Presentation via Mock Trial (Top Three Teams)

Cybercrime Investigation Competition (cont.)

June 1, 2022 - Cybercrime Investigation Competition: Day 1

At the closing of the morning session on day one, the Cybercrime Investigation Competition will go live to the audience. Throughout the competition on day one, all the evidence will be extracted by two technical experts and documented by one legal specialist following all the legal guidelines. Ethical hacking, disk forensics, mobile forensics, and network forensics are required to solve all technical questions. The maximum score that can be earned on day one is 70 points. This score is weighted where 50 points can be earned for technical solutions and 20 points can be earned for report documentations. Each team must submit the full report prior to the deadline so that the white hat directors can conduct their evaluations. Determining which teams can move onto the next level, day two, depends on the combined total score earned from each team. Prior to the closing announcements on day one, the top three teams of the Cybercrime Investigation Competition will be declared.

June 2, 2022 – Cybercrime Investigation Competition: Day 2

At the start of day two, the morning session will consist of introducing the top three teams and judges of the competition. Session one will host the top three winning teams of the competition via a Cybercrime Mock Trial. The legal expert will present the evidence during the mock trial. Each team will be allotted 15 to 20 minutes to present their findings. The maximum score that can be earned on day two is 30 points. After a quick break, session two will be accompanied by a professional mock trial coordinator and three renowned judges in the area of cybercrime. Here, there will be a ten-minute Q&A, and then the three judges will make their final decision on the winning team of the Cybercrime Investigation Competition. The winning team will be determined by combining the scores that were earned on both days of the competition. The maximum score that can be earned for the aggregated competition days is 100 points. The total points of both the legal and technical sides will be equally weighted for selecting the top winning team of the competition.

Awards Ceremony

The winning team of the competition will be awarded a $1,000 cash prize and each member of the winning team will be awarded a $1,000 scholarship (a total sum of $3,000 per team) to be applied to the tuition of BU MET's Cybercrime Investigation & Cybersecurity Graduate Certificate. The awards will be announced during a ceremony following the conclusion of the final round of presentations and judge deliberation.

Cybercrime Investigation Competition Guidelines

The competition comprises three components: 1) Forensics Capture the Flag (CTF) Challenge, 2) Written Legal Evidence Report, and 3) Mock Trial Presentation.

1. Forensics CTF Challenge (50%)

The challenges will lead to flags entered on Capture the Flag Framework (CTFD), an open-source 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.

1. At the start of the challenge, all teams will be provided with one (1) written scenario detailing the crime/s under investigation, the forensic evidence being provided, the information the teams are being requested to investigate and report on, and a rubric clarifying how points may be earned.
2. Teams will have approximately twenty-four (24) hours from the start of the competition until the end of the competition to analyze evidence before presenting their findings to the judges.
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. Additionally, teams should be prepared to testify on the validity of their selected tools and techniques as well as describe how evidence was

2. Written Legal Evidence Report (20%)

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 twenty-four (24) hours competition deadline. **The U.S. legal code details for preparing the competition will be supplied to the team by mid-May.**

Technical Approach and Techniques Utilized (3%)	Utilization of any technical approach(es), tools, and techniques suitable to conduct their investigation of the scenario: An exam-ple format for this portion: 1. Presentation of Basic Evidence Information: <OS, Time Zone, etc.> 2. Description of tasks accomplished 3. Description and Rationale for the use of the selected tool(s) used for each task

Cybercrime Investigation Competition (cont.)

Evidence Discovered and Categorized (3%)	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> **Evidence Description:** <Provide a brief description of the item> **Evidence Type:** <Provide a summary of the type of evidence this item belongs to> **Special Handling:** <Provide special handling required to preserve evidence integrity>
Legal Authority (4%)	Authority requests to investigate beyond the current scope of the scenario (criminal Investigation): An example below can be used to describe the situation to contact a "Case Agent" for legal requests or discussion to re-solve the issue. **Legal Authority Request #1:** <Provide Legal Authority> **Rationale for Request:** <Provide a brief de-scription of the Rationale> **Request Resolution:** <Provide a summary of how this request was resolved>
Summary Analysis of Body of Evidence (10%)	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 significance of the evidence to the investigation> **U.S. Penal Code or Rationale:** <Describe how the evidence discovered supports your assessment of this crime> **Evidence #2:** <Provide item name> **Significance to the Investigation: <**Provide an analysis on the significance of the evidence to the investigation> **U.S. Penal Code or Rationale:** <Describe how the evidence discovered supports your assessment of this crime> **Evidence #3:** <Provide item name> **Significance to the Investigation:** <Provide an analysis on the significance of the evidence to the investigation> **U.S. Penal Code or Rationale:** <Describe how the evidence discovered supports your assessment of this crime>

Cybercrime Investigation Competition (cont.)

3. Mock Trial Presentation (30%)

Following the forensics CTF challenge and written legal report, a mock trial will be held where the **top three (3) teams** awarded the most points for the combination of the challenge and the report scores, will be given the opportunity to present their findings to the judges.

General Expectations

1. All participants are expected to be respectful of other participants, conduct themselves professionally and ethically, and present themselves with appropriate courtroom attire. Offensive speech or behavior will not be tolerated, and any participant in a team who conducts in an indecent way will be disqualified.
2. During the trial presentations, the remaining two teams and spectators are expected to be quiet (microphone muted) to allow the presenting team the ability to focus as well as for the judges to review the presentations.
3. The three (3) teams declared at the end of Day 1 to have earned the highest number of points will proceed to the final stage of the competition for the Mock Trial on Day 2.

Trial Rules

1. There will be two sessions of the Mock Trial. During the first session, each teams' legal expert will be allotted 15-20 minutes to present their findings and earn a maximum score of thirty (30) points.
2. The second session will be accompanied by a professional mock trial coordinator and three renowned judges in the area of cybercrime. During the second session, each team will have ten (10) minutes to answer any questions before the judges. The trial coordinator may deliver any questions collected from the spectators or audience.

Judging and Scoring

1. The winning team will be determined by combining the scores that were earned on day one (1) and day two (2) of the competition.
2. The maximum score that can be earned for the aggregated competition days is 100 points.
3. The total points of both the legal and technical sides will be equally weighted for selecting the top winning team of the competition.
4. The winning team will be announced at the Awards Ceremony following the judges' deliberation.