DOI: https://doi.org/10.48009/4_iis_2022_104

High tech cybercrime unit: A partnership between a local county and a university

Jason E James, *Indiana State University, jason.james@indstate.edu*

Abstract

Police agencies and prosecuting attorney offices throughout the country are struggling to handle the influx of digital evidence in criminal investigations. In 2016 the University of Notre Dame and St. Joseph County Indiana created a Cyber Crimes Unit that resulted in a significant reduction in the backlog of digital evidence to be examined and shortened turnaround time for forensic examinations to days instead of months. As a result, Indiana State House enacted Enrolled Indiana Code in 2021 that allows the Indiana Prosecuting Attorneys Council to establish high tech crimes units to assist prosecuting attorneys in investigating, collecting evidence, and prosecuting high tech crimes. This article is about one University's journey to becoming one of those ten high tech crime units.

Keywords: High-tech cybercrime unit, digital forensics, student investigators, universities, partnerships

Introduction

With the mass adoption of mobile devices, digital evidence is more prevalent in criminal cases than ever before. By the year 2024, 4.5 billion people will be using smartphones (Newzoo, 2021). In the history of law enforcement, few things have transformed criminal investigations and prosecutions the way technology has. Technology has enabled new ways to commit old crimes while emboldening those who may have never committed a crime before to hide behind the perceived anonymity of technology and engage in criminal activity.

While technology has also produced new crimes such as ransomware, sextortion and virtual theft, the most transformative change to criminal investigations is something most people carry with them 24 hours a day, seven days a week – a mobile device.

Due to the prevalence of mobile devices, there is now a technology nexus in nearly every crime. In fact, it is estimated that 85% of police investigations (Watson, 2018) involve some sort of digital evidence. This digital evidence includes items such as detailed conversations discussing crimes, pictures, videos, phone calls, postings, and GPS location information. Given the pervasiveness and capabilities of technology, one would think that digital evidence is being used in every investigation and prosecution. Yet it is not, primarily for two reasons:

1. Police administrators have been slow to respond to digital evidence and the benefits it can bring to investigations, primarily because of cost and manpower. Throughout the country, we have heard these same two issues echoed by administrators. They don't have the money in their budget to fund a digital examiner, equipment, and training and they don't have the manpower to police the streets, so they cannot dedicate personnel to conduct digital examinations or be part of a unit

that does so. Moreover, for those agencies that do have funded and trained digital examiners, they often lose those individuals to the private sector for higher salaries.

2. With few resources dedicated to digital evidence and the proliferation of technology in every investigation, the large electronic footprint generated by investigations often overwhelms law enforcement. This results in only major cases receiving digital examinations. Even if a case does merit a digital examination, the backlog of cases means that those results likely won't be available for six to eight months (Fouzder, 2018 and Belsher, 2018). By itself, law enforcement falls critically short of the skills and resources needed to effectively deal with technology in criminal investigations and prosecutions.

Background

In 2015, the St. Joseph County Prosecutor's Office in Indiana implemented a solution locally to address this problem. Through a partnership with the University of Notre Dame's Computing & Digital Technologies (CDT) program, they selected students to intern for the St. Joseph County Cyber Crimes Unit. (DiCarlo, 2021). While students interning with law enforcement is not new, their method was new. The students are not considered to be interns, they are sworn student investigators.

Prior to selection, each student went through a screening process like applying for a law enforcement position. Those who passed and received offers of employment were then sworn in as investigators by the elected prosecutor, granting them law enforcement powers. The students then underwent a training program that included multiple academic courses, such as Introduction to Digital Forensics, Advanced Digital Forensics, and Cybercrime and the Law, as well as specific law enforcement courses that covered legal issues, cybercrime and the law, electronic discovery and digital evidence processing.

St. Joseph County began the student investigator program in academic year 2015 – 2016 with one student. In 2016, the program expanded to three student investigators. It has since expanded to six student investigators in 2017, eight in 2018, ten in 2019, and currently (AY 2020) it funds 15 student investigators (Kaizer, 2021).

Given that the student investigators are sworn investigators, all investigative roadblocks are removed, allowing the students to work on every investigation in which the Cyber Crimes Unit is involved. This includes homicides, drug offenses, fraud, domestic violence cases, and online exploitation. As they are going through the formal training, students also work with the Cyber Crimes Director and Senior Investigators on active investigations, applying the theoretical knowledge they learn in the classroom to practical casework. They conduct online research, write search warrants, process scenes, and examine digital evidence.

Moreover, the digital examinations conducted by student investigators are extensive. The policy of most digital forensics labs is to extract data from a device and then process the data so that it can be reviewed by the submitting officer. The lab then provides the officer a full copy all data extracted and processed from the device. In the Cyber Crimes Unit, the students continue beyond extraction and processing and conduct analysis of the data. After reviewing all warrants, affidavits, and police reports, student investigators conduct a thorough analysis of all data and tag items of evidentiary value. At the conclusion of their analysis, submitting officers are provided not only with a full copy of all data, but they are also provided with an analyzed copy of the data identifying items of evidence.

Their student investigators are not just actively involved in digital investigations; they are involved in in some capacity in almost all cybercrime cases. In fact, over half the time, they are the primary investigator. The only involvement of full-time law enforcement in these primary cases assigned to student investigators is reviewing the work of the student. Student investigators conduct the majority of all digital forensic examinations.

Our partnership would follow the same model where the students are not considered to be interns, they are sworn student investigators, allowing the students to work on every investigation in which the Cyber Crimes Unit is involved.

High-Tech Cybercrime Unit

Digital forensics is a critical part to any investigation and as we have seen locally, every investigation involves some aspect of digital analysis and will only continue to increase in the future. The goal is to decrease turnaround time significantly and eliminate the backlog of cases.

Digital footprints will only increase in the future. In just the past year, the number of cases and devices to be examined have skyrocketed in, doubling from last year. Additionally, moving into the mainstream are wearable devices, home automation systems and a plethora of Internet of Things devices. Alongside the expansion of devices containing evidence, there is an expansion of data being maintained in the cloud. Each of these sources potentially harbors important digital evidence and learning how to extract and process it will be critical for the future of police investigations.

The Cyber Crimes Unit aims to expand and enhance the current model in place in St. Joseph County. Rather than relying on outside resources, the Cyber Crimes Unit has been able to cut its examination turnaround time significantly and eliminate the backlog of cases. Significant components of this Cyber Crimes Unit include,

- funding positions of Co- Directors, faculty advisors and student investigators
- expanding services to include all jurisdictions in seven surrounding counties
- increasing the number of student investigators from 3 to 6
- purchasing additional forensics hardware and software
- expanding the research component of the unit, and

Geographics

The Cyber Crimes Unit currently serves both the Sherriff's office and local police departments in the eight counties. Collectively, these eight counties consist of approximately 3200 square miles of coverage and a service population of approximately 472,000 residents. These counties serve as a starting point for expanded coverage and the Cyber Crimes Unit is always willing to expand and accommodate the needs of the state. It is expected that as such coverage expands, the manpower of the program will also expand accordingly to meet the goals of providing timely access and reporting of digital forensic data analysis.

Staffing and Organization

The staffing model chosen by the Cyber Crimes unit is two Co-Directors (one from local police department and one form the Sherriff's Office) and two faculty advisors who are current professors employed by the University and sworn in by the Prosecutor's Office as special investigators. The student investigators are paid and obtain academic credit.

Cyber Crimes Unit student investigators can comprise a wide variety of majors but currently student interns are all Cybercrime majors within the University. It was decided that this partnership, along with the Cybercrime curriculum, provides an ideal model for an effective partnership between law enforcement and academia.

A Cybercrime major takes required courses in criminology and criminal justice, security and risk, and digital forensics courses. All are taught by the faculty advisors of the Cyber Crimes Unit.

Selection Process of Student Investigators

The selection process of student investigators for the Cyber Crimes Unit relies on a partnership between the university and Prosecutor's Office, local police department, and Sheriff's Office. This selection committee consists of the faculty advisors of the Cyber Crime unit who are current professors within the university, selecting students who have at least a 3.5 GPA and have taken computer and mobile forensics classes. The Co-Directors from the local police department and Sheriff's Office then interview the students.

Upon completion of interviews, the Co-Directors and faculty advisors rank and discuss which applicants are the most qualified for the program. The final decision is at the sole discretion of the selection committee. Once decisions are finalized, conditional offers are extended to the students selected. The conditional offer is contingent upon the successful completion of a criminal history and background check. Once accepted into the program, the student will hold this position for the remainder of their academic year, contingent on the student's quality of work.

Roles and Responsibilities

The organization of the HTCU consists of the Chief Deputy Prosecuting Attorney (CDPO), Co-Directors and their assistants, faculty advisors and their assistants and of course the student investigators. All have roles and responsibilities to allow the HTCU to run smoothly. However, as this is a new endeavor for both parties, both agree to keep the lines of communications always open and to be flexible to adapt the program as it evolves.

The CDPO has absolute authority over selection of cases to investigate, *tasks to be* performed, and prioritization of the cases. CDPO has sole discretion to decide whether to incorporate the information or results obtained from investigation as part of any criminal prosecution. CDPO will retain all grant funds and will reimburse the University for student and faculty advisor salaries and will pay all other costs needed including hardware and software. The CDPO will swear in all investigators for the Prosecutor's office, including faculty advisors, and entitled them same protections afforded to other investigators of the Prosecutor's office (i.e., indemnification against tort claims). The CDPO may remove a student investigator from the HTCU program if it is determined that the student is no longer suitable. However, the CDPO will consult with the Faculty Advisors and Co-Directors before any such dismissal. The Prosecutor's office agrees to coordinate with University's General Counsel Office when it becomes necessary to subpoena or make other requests or demands for a university employee or current student in the program to testify or provide evidence at a trial, hearing, deposition, etc. Similarly, any subpoena for the production or inspection of any documents, equipment, etc. belonging to the University shall also be routed through the University General Counsel's Office and coordinated between the parties. Lastly, the CDPO will further facilitate University student learning and engagement by coordinating and organizing periodic training sessions, seminars, simulations, demonstrations, and other educational and learning opportunities for students engaged in the study of criminology or related fields.

- Faculty Advisors shall be primarily responsible for the day-to-day operations of the HTCU and supervision of student interns, subject to any instructions or orders of, and in consultation with, the Director appointed by the VCPO.
- Students work hours will be consistent with university rules applicable to student employees.
- Faculty Advisors will assign cases to student interns and coordinate scheduling of student intern work hours.
- Faculty Advisors will make preliminary selection of students for HTCU intern positions and present the selections to CDPO who will have final approval. Neither party will discriminate against any qualified applicant for participation in the HTCU because of race, religion, color, sex, age, national origin or ancestry, disability, status as a veteran, or any other basis prohibited by applicable law.
- Faculty advisors will be responsible for development and delivery of cyber forensics training for county prosecutors and other law enforcement professionals in the HTCU service area. Trainings will be scheduled by the CDPO in coordination with the availability of the faculty advisors.
- Faculty Advisors will have office space within the HTCU to ensure oversight of student interns.
- Faculty Advisors will be responsible for the maintenance of all software and equipment in the HTCU.
- It is understood and acknowledged that the Faculty Advisors subordinate to and work at the direction of the CDPO and the Co-Directors. It is further understood and acknowledged that neither the Faculty Advisors nor student interns are authorized to act or make commitments on behalf of the university.
- If any concerns arise with respect to University's fulfillment of its responsibilities, such concerns shall be addressed with the Dean of the College College or the Director of the Department.
- University shall provide the HTCU with a suitable workspace, to be agreed upon by the parties. Basic utilities (HVAC, lights, internet service, etc.) will be maintained by the University at no expense to the HTCU.
- Specialized software necessary for operation of the HTCU, office furnishings and supplies (desks, chairs, computer workstations, etc.) will be procured by the DCPO utilizing grant funds as detailed in the proposed budget. Use of all such furnishing, hardware, software, etc. shall be limited to HTCU members or their designees. All right and title to equipment, hardware, etc. purchased using IPAC grant funding shall revert to the DCPO on the expiration or termination of this Agreement.
- Software of other technological resources that have been provided to the University for the sole purpose of student education may not be utilized by the HTCU. The parties will be mindful of, and abide by, software licensing restrictions in operating the HTCU.
- It is expected that activities within the workspace will generally be conducted during normal business hours. If access to the workspace is required outside of normal business hours, access will be coordinated thru the University police.

Training and Research

Since the program is new, one requirement for acceptance into the program, all potential student investigators must take Computer Forensics and Mobile Forensics. These two courses provide them the initial training they need to be successful in the program. These courses provide a valuable foundation for the work that students will engage in as investigators in the Cyber Crimes Unit. Once accepted in the program students will undergo extensive initial training and continue to participate in training throughout the entire employment period. These training opportunities consist of a combination of semester-long academic courses, training provided by outside technology vendors, and attendance at digital forensics conferences. Given that technology is continually changing, ongoing training and research is a critical component to ensure the success of the student investigator and to maintain the high level of services provided by Cyber Crimes.

Realizing that this Cyber Crimes unit will be supporting eight counties, the program will offer training to other jurisdictions as part of this proposal. This training will be open to any student or law enforcement officer throughout the state. Student investigators in the Cyber Crimes Unit also undergo extensive training throughout their time in the unit. This aspect of training will be led primarily by the faculty advisors. In addition to in house training, student investigators will be offered the opportunity to attend training provided by outside vendors along with opportunities to attend conferences.

As student investigators expand their level of technology knowledge and skills, they are encouraged to study and test for vendor-neutral certifications, such as IACIS Certified Forensic Computer Examiner (CFCE) and ISFCE Certified Computer Examiner (CCE). In addition, students learn digital forensics software as part of their coursework including Magnet Forensics Axiom Cyber, Paraben E:3and Cellebrite and are encouraged to obtain these vendor-specific certifications, such as the Magnet Certified Forensics Examiner (MCFE), Paraben Certified Computer Operator (P2CO) and Mobile Operator (DSMO) and Cellebrite Certified Mobile Examiner (CCME) and Cellebrite Certified Operator (CCO).These certifications incentivize students to develop a thorough understanding of forensic policies and procedures and of the forensic software that they are using, thus improving their analytical abilities, establishing a level of expertise, and increasing their credibility to conduct digital forensics and testify to the results they obtain.

Working with Law Enforcement Agencies

The Cyber Crimes Unit will develop request forms, report forms, consent forms and processes for unit services. These forms and processes will include how a law enforcement agent or prosecutor can request routine and emergency services. It is anticipated that such requests will primarily include acquisition and review of forensic data. When a request for service is made, a case report or probable cause affidavit will also be provided. The investigator will utilize the information provided to examine the recovered data for any case relevant information. A report identifying any relevant information located in the data will then be provided to the investigator or prosecutor.

Directors and student investigators will be trained in search warrant drafting and review. The training will provide guidelines based on state and federal law so the investigator will be able to assist law enforcement officers in obtaining search warrants with appropriate language and limits consistent with the specific investigation. The training will also allow the investigator to understand the scope of any permitted search based on a warrant issued or consent given for obtaining forensic data.

Partnering with the University

Currently, the Department at the University that houses the HTCU has developed partnerships with multiple vendors and programs that will enhance the capabilities of the Cyber Crimes Unit. Some of those partnerships include Magnet Forensics, Paraben, Forensic Notes, Monolith Forensics and LEVA, the Law Enforcement Video Association. LEVA is a 501(c)(3) non-profit corporation providing globally recognized training and certification in the science of forensic video analysis. LEVA has also agreed to provide video/image/audio/testimony training for law enforcement in the region. This partnership will benefit the Cyber Crimes Unit, the student investigators, and area law enforcement officers in achieving training and certification in video forensic evidence at no cost to the agencies.

Since the state has provided funding for this partnership, the University will continue to provide benefits and opportunities that only a developed educational program can access and will magnify each dollar invested in this relationship. The partnership with university will also benefit the data collection needed for the State funding to be justified and, hopefully, increased. All data will be collected, compiled, and provided by the Co-directors to assist with future funding requests for these investigative units. Such data collection will also be driven by the academic needs of the individual professors, the department, and the university. Such data shall be provided regularly as needed or requested by the state.

Budget

In order to startup, operate and maintain a successful Cyber Crimes Unit, certain hardware and software and their associated costs are involved. First, each investigator needs a forensic workstation to run digital forensics imaging and analysis software to process digital evidence. The forensic workstation could be a desktop or a laptop, but no matter which one that is used, certain specifications need to be met to run the digital forensics software. When deciding what is needed, the first decision that needs made is whether to buy prebuilt computers or to build them. The initial investment will cost you anywhere between $2,500 to $20,000, not including monitors. The Cyber Crimes unit has a combination of both for 6 student investigators and 2 faculty advisors as well as field kits for on scene.

Second, network isolation is critical aspect when handling mobile devices involved in a criminal case. Mobile devices need isolated from radio frequency signals to maintain evidence integrity, reduce probability of a remote wipe, reduce device location sharing, and prevent additional artifacts from being written to the device. Faraday devices are the tool of the trade in digital forensics. Faraday bags shield devices from outside signals to prevent data from being altered, deleted, or added to a device (Offgrid, n.d.). There are many different types of Faraday bags and devices, but at minimum every device should be shielded in a Faraday bag. A good Faraday bag for a mobile device can cost around $25 and typically you would want to have 30-50 on hand.

Third, portable power chargers and device cables are necessary to ensure a device stays powered on until extraction is complete. The cost can be anywhere from $500 to $1,000. Next, a good digital forensics lab needs to have secured device storage to safely store mobile device extractions and simplify chain of custody and data integrity. A locked safe with power is a good choice and can cost around $2,500 to $3,000. The next thing to consider is the cost of storage. The amount of data obtained from each device can add up quickly and a typical 18TB hard drive can cost around $500.

The other consideration that needs accounted for is the cost of digital forensics software, which is the lifeblood of any digital forensics' investigator. Many different companies specialize in digital forensics software such as Magnet Forensics, Cellebrite, Paraben, Grayshift, DataPilot, and the list goes on and on. Each company has different products, but typically a license costs anywhere from $5,000 to upwards of $100k, depending upon the Cyber Crimes Unit's needs. In the end, the cost of hardware and software to run an average digital forensics lab typically costs around $150,000 to $175,000 a year.

Facilities

Given that students working out of the Cyber Crimes Unit come from the University, a strong partnership with the University is critical in ensuring that the student investigator program is successful. A memorandum of understanding ("MOU") was developed between the University and the County Prosecutor's Office.

The Cyber Crimes Unit is currently housed on the University campus. This allows for a close working relationship with both law enforcement personnel and academic faculty. The University furnishes the Cyber Crimes Unit with approximately 1000 square feet of office space. All office space is provided by the University free of cost. All space is secured through electronic locks, is alarmed, and is under video surveillance.

Moreover, the University provides all utilities at no cost to the prosecutor's office. This includes electrical, heating, air conditioning, trash removal, alarm monitoring, video monitoring, internet connectivity, and full network support from their network engineers. As part of this, the University configured a secure Virtual Local Area Network (VLAN) for use only by the Cyber Crimes Unit. This VLAN provides a method for secure remote access to workstations along with a robust backup system that is hosted on their own data servers, ensuring that case data is always backed up and is not vulnerable to any internet threats or data exfiltration. The VLAN, as well as access to the VLAN, alarmed electronic locks and video surveillance, and access to the room is controlled by the faculty advisors and only those involved in the partnership have access.

Internal Controls

The HTCU has two offices, the Main office and Investigator Office, and both require an access code to enter. The only people who have access to the main office are sworn-in investigators or law enforcement. Access is granted, maintained, and monitored by the faculty advisors. The student investigators and faculty advisors are the only ones who have access to the investigator office. The building is unlocked during normal business hours and locked at nights and on weekends. However, faculty advisors have access to the building.

- Security cameras monitor the outside and inside of both offices and are maintained and monitored by the faculty advisors.
- University Police have access to the two offices in case of emergency.
- New cases are created in Monolith Forensics by the requesting agency and then incoming evidence is brought in the HTCU main office by Co-Directors (or backups) and either provided to the faculty advisors or support and/or placed in the safe. The safe is only accessible to those with access to the room.

All incoming evidence chain of custody is logged through Monolith Forensics as well as chain of custody form inside the main office. Once evidence is in the safe, it is tagged and labeled. Once an investigator gets assigned a case, faculty advisors or support transfer to the individual investigator's safe in their office. Chain of custody is logged through Monolith Forensics as well as chain of custody form until it is imaged and goes back to the main office safe until it is released back to the Co-Directors (or backups) once the case is closed.

Results

The benefits of this program have been immediately recognized. Prior to beginning this, the local police departments maintained a backlog of cases and turnaround time was weeks. Since implementation in 2021, the turnaround time has significantly improved, and case backlog has been eliminated. Today, turnaround time for digital examinations is routinely within one week. This means that digital evidence is immediately in the hands of an investigating officer and the prosecuting attorney, resulting in better investigations and charging decisions. Although the authors did not provide statistics of the results of the program because it is too early in its infancy stage, the authors plan to provide future results in future research related to the program.

In addition to the benefits to local law enforcement, this program also benefits the students and the community. Once students graduate, they typically have multiple years of real-world digital forensics experience along with industry certifications. Coupled with their degree, they are highly coveted in the job market. Recruiters typically visit the Cyber Crimes Unit to meet with our students and try to persuade them to apply to their organizations for jobs. For the community, student investigators provide manpower and a high level of expertise at minimal cost to taxpayers. Currently, all student investigator salaries are paid through the grant.

Conclusion

In conclusion, surveillance video and cell phone data have grown to the point that investigators often do not have time to review all of that data and sifting through video, computer, and mobile data for evidence of criminal activity has become the new assignment for three university students interning as digital forensic investigators for a local county Prosecutor's Office. This program provides students real-world experience in a growing field while assisting law enforcement and prosecutors in discovering and sorting through the growing mounds of digital evidence and is a classic example of a university's dedication to experiential learning and community involvement that benefits all involved. Student lives will forever be changed who successfully participate in this program. They will develop and hone their skills into great job opportunities and the partnership allows the Prosecutor's office to better serve and protect the community. A high-tech crime unit with students as sworn in investigators is just one example of how universities and entities can partner to provide students real world experience prior to graduation. With the success that this Cyber Crimes Unit has experienced, other programs can benefit from the same success.

References

AccessData. (n.d.) *FTK Imager Lite 3.1.1*. Retrieved November 25, 2016 from AccessData.com: http://marketing.accessdata.com/ftkimagerlite3.1.1

Belsher, A. (2018). *Re-imagining policing for the digital age.* Retrieved April 27, 2022 from Blueline https://www.blueline.ca/re-imagining-policing-for-the-digital-age-6008/

DiCarlo, G. (2021). *St. Joseph County Prosecutor's Office receives state funding for High Tech Crime Unit.* Retrieved July 3, 2022 from. https://www.wvpe.org/indiana-news/2021-11-08/st-joseph-county-prosecutors-office-receives-state-funding-for-high-tech-crime-unit

Kaiszer, M. (2021). *IPAC Funding Proposal.*

Newzoo. (2021). Global mobile market report. Retrieved May 1, 2022 from https://newzoo.com/products/reports/global-mobile-market-report

Offgrid. (n.d.). *5 Reasons You Need a Faraday Bag*. Retrieved May 1, 2022 from Offgrid https://offgrid.co/blogs/journal/5-reasons-you-need-a-faraday-bag

Fouzder, M. (2018). *Criminal justice system 'really creaking', warns outgoing CPS chief.* Retrieved April 27, 2022 from The Law Society Gazette https://www.lawgazette.co.uk/news/criminal-justice-system-really-creaking-warns-outgoing-cps-chief/5068116.article

Watson, A. (2018). *Law enforcement overwhelmed by digital data*. Retrieved, April 27, 2022, from Cellebrite.com https://cellebrite.com/en/law-enforcement-overwhelmed-by-digital-data/