**Glenn K. Bard**
**Chief Technical Officer (PATCtech)**
700 N. Carr Rd # 595
Plainfield, IN 46168
1-317-386-8325 (Office)
724-289-0699 (Cell)
glenn.bard@gmail.com
https://www.patctech.com/about-us/

**Current Position:**
Chief Technical Officer –PATCtech
National Instructor - Public Agency Training Council
Project Alert team member – National Center for Missing and Exploited Children

**Previous Positions:**
State Trooper - Pennsylvania State Police (Retired)
Faculty Instructor – Westmoreland County Community College

**Former Assignments / Unit Designations:**
Pennsylvania State Police - Bureau of Criminal Investigation - Computer Crime Unit
Westmoreland County Community College – Computer Information Security

**Former Task Force Memberships:**
Pennsylvania State Police Area III Computer Crime Task Force
United States Department of Justice Crimes Against Children Task Force
High Tech Computer Crime Task Force – Federal Bureau of Investigation
Internet Crimes Against Children Task Force

**Professional Affiliations:**

International Association of Computer Investigative Specialists (IACIS)
Information Systems Security Certification Consortium, Inc., (ISC)$^{2®}$
FOP 62 (Retired member)

**Certifications:**

- Class “A” Wiretap Certification through the Pennsylvania State Police and the Pennsylvania Office of Attorney General. This certification is necessary to conduct audio and electronic surveillance pursuant to Chapter 57, of Title 18.

- A+ Certification, an international industry credential that validates the knowledge of computer technicians with the equivalent of 500 hours of hands-on experience.

- Network+ Certification, an international industry credential that validates the knowledge of networking professionals with at least nine months of experience in network support of administration or adequate academic training.

- Security+ Certification, an international industry standard that validates the knowledge of networking professionals with at least two years of networking experience focusing on Network and Computer Security.

- CEECS (Certified Electronic Evidence Collection Specialist), through IACIS (The International Association of Computer Investigative Specialists). This certifies the recipient as a specialist in the collection of computer and electronic based evidence using "best practices".

- CFCE (Certified Forensic Computer Examiner) through IACIS (The International Association of Computer Investigative Specialists). This certification is an international industry credential that validates the knowledge of Law Enforcement and Investigative professionals with expertise in forensic examination of computer evidence.

- CHFI (Computer Hacking Forensic Investigator) through the EC Council. This certification validates the knowledge of a forensic examiner in the area of computer hacking and network intrusion examinations and investigations.

- EnCE (Encase Certified Examiner) through Guidance Software. This certification acknowledges the knowledge of a computer forensic examiner to conduct in depth examinations using the forensic software tool Encase.

- ACE (Access Data Certified Examiner) through Access data. This certification acknowledges the knowledge of a computer forensic examiner to conduct in depth examinations using the forensic software tools Forensic Tool Kit, Password Recovery Tool Kit, and Registry Viewer.

- AME (Access Data Mobile Examiner) through Access Data. This certification acknowledges the knowledge of a mobile device forensic examiner to conduct in depth examinations using the forensic software tool Mobile Phone Examiner Plus.

- CISSP (Certified Information Systems Security Professional) through the International Information Systems Security Certification Consortium, Inc., $(ISC)^2$. This certification is one of the most respected certifications in the computer security industry. The CISSP verifies a security systems professional in every aspect of security ranging from physical conditions to network intrusion and detection.

**Experience Highlights:**

*11/1995 – 04/2000* **Pennsylvania Law Enforcement Officer**

Assigned to conduct patrol duties.
Conducted Traffic enforcement duties, investigated traffic crashes including fatalities and vehicular homicides, investigated and made arrests for various crimes including aggravated assaults, forgeries and burglaries.

*04/2000 – 08/2010* **Computer Crime Investigator / Computer Forensics Examiner**

During my time as a computer crime investigator, and computer forensic examiner I have conducted computer crime investigations and computer forensic examinations of microcomputer systems, networks and electronic storage media; provided technical assistance to Federal, State and local law enforcement agencies relative to computer crime investigations; prepare and serve search warrants, arrest warrants, court orders and other legal processes; prepare technical reports in both paper and web based formats; test and validate software tools and utilities used in forensic examinations; plan, develop, and provide courses of instruction to state and local law enforcement related to computer crime investigation. I have also been specially trained to conduct investigations into hacking and intrusion cases that have occurred at a wide range of

businesses including banks, colleges, high schools and other large networks. In August 2010 I was able to retire with 20 years of service with the State Police (Included military time and credit for teaching at WCCC) and was awarded an honorable discharge.

*08/2003 – 05/2010* **Faculty Instructor**
*Westmoreland County Community College*
145 Pavilion Lane Youngwood PA 15697
http://www.wccc.edu/

As a faculty instructor, I was tasked with planning and developing courses of instruction in the Computer Information Security division. I designed and implemented a total of 3 classes focusing on computer forensics taught at the college level. The three classes, Computer Forensics (Which teaches the theory of forensics.) Digital Forensics (Which teaches the basics of hands on recovery of data.) and Digital Forensics II (Which covers the automated recovery of data.) were implemented and are now required courses for the CIS degree program. After implementing the aforesaid classes I then began to teach Network Intrusion Detection. This course focuses on networking security protocols, encryption, cryptography, firewalls, VPN's, and many more aspects of network and data security. When I retired from the PA State Police I also had to terminate my position at WCCC since the college paid into the PA State Retirement System (SERS). I left in good standing and still have a close relationship with many of the people at the college, including Dean Nelson who was the Dean of Computer Technology and Business.

*04/2007 – Present* **Computer Crime Instructor / Chief Technical Officer**
*Public Agency Training Council / PATCtech*
*5235 Decatur Blvd., Indianapolis Indiana 46241*
www.patc.com / www/patctech.com

At PATC I was given the task of designing and implementing a computer crime class for investigators that focused on IP addressing, seizure of electronic evidence and other topics. The class became popular and was taught to hundreds of officers nationwide. Soon after PATC created a subdivision named PATCtech and I was named Chief Technical Officer. I then began to deign numerous other classes which included topics ranging from hacking / network intrusion, RAM dumping and analysis, Linux Live CD previewing, Router Interrogations and Network seizure, and cell phone forensics.

**Military Experience:**

*1988 – 1992* *United State Army* (Active Duty)
Assigned as a Military Police Officer at Ft. Carson, Colorado and Zweibrucken, Germany. Additionally; served 7 months in Operation Desert Storm. Awarded numerous awards and citations including: Army Commendation, Army Achievement Medal, Good Conduct Medal, Kuwaiti Liberation, National Defense Ribbon, Overseas Service Ribbon, Southwest Asia Service Ribbon, Army Service Ribbon, and an Honorable Discharge.

**Education:**

*1992 – 1994* *Community College of Beaver County*
Obtained an A.A.S. in Criminal Justice. Named to the Dean's List (twice) and the President's List (twice). Identified by the college as an "Outstanding Student". Graduated with a final GPA of 3.78

**Training Courses attended:**

1994 Pennsylvania State Police Academy – Pennsylvania State Police
1996 Operation Whiteline – Pennsylvania State Police
1998 Traffic Institute of Police Services Annual Conference
1998 Cognitive Interviewing – Pennsylvania State Police
1998 Hidden Compartment Investigation – Traffic Institute of Police Services
1998 Tracking Missing Persons – Traffic Institute of Police Services
1999 Testifying in Court – Pennsylvania State Police
1999 Wireless Fraud Training – Aerial Communications and System Link
1999 Introduction to the Internet – Municipal Police Officers Education and Training Commission
1999 Web Page Design – Municipal Police Officers Education and Training Commission
1999 Internet Crime – Municipal Police Officers Education and Training Commission
1999 Statement Analysis – Pennsylvania State Police
1999 Basic Homicide Investigation – Pennsylvania State Police
2000 Financial Crimes Investigation – International Association of Financial Crimes Investigators
2000 Class "A" Wiretap Certification – Pennsylvania State Police
2001 Basic Data Recovery and Analysis – National Cybercrime Training Partnership
2001 Responding to Cyber Crime – Mid Atlantic Great Lakes Organized Crime Law Enforcement Network
2001 Protecting Children Online for Unit Commanders – National Center for Missing and Exploited Children
2001 Regional Computer and Forensics Group – George Mason University
2001 Advanced Data Recovery and Analysis – National Cybercrime Training Partnership
2002 Basic Computer Forensics – International Association of Computer Investigative Specialists
2002 ILOOK Forensics - Mid Atlantic Great Lakes Organized Crime Law Enforcement Network
2002 Inet computer forensics - National Cybercrime Training Partnership
2003 Institute for Law Enforcement Education Annual Conference
2003 Protecting Children Onlline - National Center for Missing and Exploited Children
2003 Computer Crime Investigation – Internet Crimes
2003 Digital Crime Scene Awareness – Internet Crimes
2003 Basic Computer Forensics – Edinboro University
2003 Child Sexual Exploitation - Center for Missing and Exploited Children
2003 ADRA for NT/2000/XP - National Cybercrime Training Partnership
2003 ILOOK forensics - National Cybercrime Training Partnership
2004 Basic Online Technical Skills - National Cybercrime Training Partnership
2004 Introduction to Computer Crimes – Pennsylvania State Police
2004 Institute for Law Enforcement Education Annual Conference
2005 Inside a Meth Lab – Pennsylvania Narcotics Officer's Association
2005 Basic Computer Forensics – International Association of Computer Investigative Specialists
2005 CompTIA A+ Hardware – New Horizons
2005 CompTIA A+ Operating Systems – New Horizons
2005 Regional Computer and Forensics Group – George Mason University
2005 CompTIA Network+ - New Horizons
2005 Institute for Law Enforcement Education Annual Conference
2006 Windows Forensic – Access Data
2006 Regional Computer and Forensics Group – George Mason University
2006 Institute for Law Enforcement Education Annual Conference

2006 ICAC Peer Precision
2006 Computer Hacking Forensic Investigator – New Horizons
2007 Core Skills for the Investigation of Cellular Telephones - Search
2008 Mobile Forensics 101 – Mobile Forensics Inc
2008 Mac Forensics – Cranston Consulting
2008 SOHO (Small Office Home Office) network investigations - Search
2009 Basic Cellular Phone Investigation – National Cybercrime Training Partnership
2009 ICAC Peer to Peer Investigations – Internet Crimes Against Children
2010 HTCIA conference – Vendor
2011 ISC2 – Using Advanced Authentication Methods to Mitigate Data Leakage
2011 ISC2 – Fortifying your defense: Using Encryption to Defend and Protect Critical Comm. and Trans.
2011 ISC2 – Borderless: Why Insecure Software is a concern to Everyone, Everywhere
2011 ISC2 – Pound of Prevention for an ounce of Cure? – What is the true cost of Malware protection
2011 ISC2 – The Fractured Datacenter – Defense Moves Closer to the Data
2011 ISC2 – Computers Don't Commit Crimes, People Do – Cybercrime Today
2011 ISC2 – Pay Now, Pay Later or Just Keep Paying, The Real Cost of Staying Compliant
2011 ISC2 – Ubiquitous Computing, Pervasive Risk: Coping with the Proliferation of Mobile Devices
2011 ISC2 – Pathway to the Clouds
2011 ISC2 – Deter. Detect. Defend. Protecting Against Data Loss
2011 ISC2 – Lessons Learned – Critical Success Factors from Government Identity Management Deployments
2011 ISC2 – Dealing with Risk and Vulnerabilities in the Enterprise
2011 ISC2 – At Rest, In Transit, In Use: Data Security in the Dynamic Enterprise
2012 ISC2 – Groundswell – Managing the Bottom-Up Emergence of Social Media
2012 ISC2 – A Perfect Storm for IT Security
2012 ISC2 – Managing the Fractured Datacenter: The Cloud and Unifying Identities
2012 ISC2 – Cybercrime – Stopping the profit motive
2012 ISC2 – Back to Basics: IT Service Management as a Security Enabler
2012 ISC2 – Demystifying and Improving your Application Security Program
2012 ISC2 – Using Authentication to Support Information Protection
2012 ISC2 – BYOD Recipe for Disaster?
2012 ISC2 – Mining Security Intelligence for Threat Indicators
2012 ISC2 – Cradle to Grave: Managing the Software Assurance Lifecycle
2013 ISC2 - Critical Infrastructure: Untangling System Dependencies and Recovery
2013 Paraben – Paraben Forensic Innovations Conference (Speaker and attendee)
2014 ISC2 - Security Congress (Speaker and attendee)
2014 Paraben – Paraben Forensic Innovations Conference (Speaker and attendee)
2015 MIT – Cybersecurity: Technology, Application and Policy
2016 MIT – Tackling the Challenges of Big Data
2017 MIT – Internet of Things: Roadmap to a Connected World
2017 ISC2 – Insider Threats – The greatest risk to your data
2017 ISC2 – Cyber Security Starts with Awareness
2017 ISC2 – Managing Shadow Data: The growing challenge to safe cloud adoption
2018 University of Washington – Introduction to CyberSecurity
2018 ISC2 - Identity Assurance for a Connected World
2018 ISC2 - Infrastructure Protection for Better Application and Service Availability
2018 ISC2 - Operationalizing Threat Intelligence
2018 ISC2 - Prepping for the Worst - Plans and Programs for Incident Response, Vulnerability Management and Phishing
2018 ISC2 - GDPR – Now's the Time to Plan for Compliance
2018 ISC2 - Getting to know you Consumers and their identities
2018 ISC2 - Office 365 Security & Performance – Proven Deployment Strategy Combining CASB + SWG
2018 ISC2 - Reimagine Your Identity Strategy

**Speaking Engagements:**

Pennsylvania State Police
Edinboro University of Pennsylvania
Indiana University of Pennsylvania
National District Attorneys Association
Westmoreland Bar Association
Duquesne Law School – Wecht Institute
Pennsylvania State Fraternal Order of Police
Illinois Fraternal Order of Police
New Jersey Fraternal Order of Police
Pennsylvania Game Commission
Federal Fraternal Order of Police
DEA – Phoenix
HIDTA - Phoenix
Hi Technology Criminal Investigators Association (Pittsburgh Chapter)
OPDAT / DOJ – Tirana Albania
HIDTA – Houston
HIDTA – El Paso
Paraben Forensic Innovations Conference (PFIC)
ISC2 Security Congress
RCFL – St. Louis
Idaho POST
International Association of Arson Investigators
Association of Certified Fraud Examiners
National Transportation Safety Board
Conducted training in over 30 states
2014 World Security Congress
2019 American Academy of Forensic Science
And many more.

Selected to speak at trainings all over the world, including representing the United States at the 2010 OPDAT training in Tirana Albania, 2014 World Security Congress, 2019 American Academy of Forensic Sciences and hundreds of other trainings for local, state and federal agencies, law firms, insurance companies, and other professional organizations, too numerous to list.

**Certifications courses created:**

Created the CTF (Cellular Technology and Forensics) and +Smart (Forensic and Technology Certification focused on Smartphone devices). The certifications are issued by PATCtech and have been obtained by hundreds of people in the last decade.

Contracted to develop and teach the SecureView cellular forensic software certification for Susteen and the Passware Kit password and decryption certification for Passware.

**Other notable Honors:**

Certified as an expert in Commonwealth of Pennsylvania, State of Tennessee, State of Connecticut, State of Texas, United State Virgin Islands and the United States Federal Court System in the areas of Digital Forensics, Cellular forensics, Cellular Communications and Computer Technology.

Certified as an Expert Instructor in the State of Maryland, certification number 176999.

Certified Law Enforcement Instructor – State of Arkansas

Selected by the US Attorney's office in Pittsburgh and OPDAT to teach computer crime investigations and computer forensics in Tirana Albania, May 2010.

Articles concerning cases I have worked on have been noted on Fox News, Dateline, the Associated Press, Playboy, Yahoo!, the New York Times, Pittsburgh Post-Gazette, Pittsburgh Tribune Review, and many more.

Project Alert team member for the National Center for Missing and Exploited Children.

Selected to supply cellular forensic and records analysis training for a 5 year period for the NTSB.

Interviewed on Good Morning America.

Asked to create a course on the Dark Web, TOR, Onion Routing and Cryptocurrency for the state of Idaho. The course was originally taught online and has since been turned into a classroom instruction course that teaches investigators when to detect that the Dark Web / TOR were used to commit a crime. The course then covers how to properly seize the computers / smartphones used to access the Dark Web, and ultimately conduct forensic analysis of those devices to identify the artifacts.

Guest lecturer at the 2019 AAFS (American Academy of Forensic Sciences) Annual conference in Baltimore, Maryland.

**Publications**:

Co-authored "*Crime Scene Investigation in the 21st Century Digital Evidence Edition"*
Contributor "Long-term missing child guide for law enforcement: Strategies for finding long -term missing children"

**Testimony**:

Following is a list of pertinent courtroom testimony. (Note: this list is not all-inclusive.)

US vs Christopher Beardsley (Child Pornography)
US vs Daniel Diyn (Child Pornography)
US vs Michael Karrer (Child Pornography)
US vs Ed Northup (Child Pornography)
US vs Douglas Cook (Child Pornography)
US vs Kristian Heller (Child Pornography)

PA vs Ian Bishop (Murder)
PA vs Ian Finlay (Criminal Attempt – Sexual Assault)
PA vs Kenneth Jones (murder)
PA vs Stephen Rugh (Indecent Sexual Assault)
PA vs Daniel Segen (Sexual Assault)
TN vs Wade (Murder)
PA vs Tyler Hess (Peer to Peer technology and Child Pornography)
US VI vs Freiman, Henley, and Thompson (Murder)
PA vs Bracken (Child pornography – Sexual Assault)
PA vs Eric Hall (Double Murder)
PA vs Michael Martin (Murder)
PA vs Greg Howard (Robbery)

PA vs Earl Pinkney (Murder)
ANPAC vs Stuttes – Recorded testimony (Civil – Arson)
PA vs Michael Peterson (Drug delivery resulting in death)
Kozel vs Kozel (Divorce)
PA vs Paul Sieminkewicz (Perjury)
PA vs David Johnson (Murder)
PA vs Barshay Dunbar (Human Trafficking)
IN vs Emmanuel Arrington (Attempted Homicide)
TX vs Aniseto Alejandro Jr.

**Significant investigations / examinations**:

Investigation into the disappearance of Morgan Johnson
(Johnson disappeared in May 2011 and was not located for over 2 years. In July of 2013 I was supplied his cellular records and asked for an estimate of where he may be located. After reviewing the records, and opinion was supplied, and Johnson was found within days, in the area identified.)

Albania vs. Former Deputy Prime Minister Ilir Meta
(Examined several digital devices.)

US. Vs. Nathan Wedgeworth
(Tracked Wedgeworth using cellular phones to locate the young girl he kidnapped. The exam of the victim's computer also resulted in dozens of arrests nationwide for Unlawful Contact with a Minor.)

The murder of Dr. Andrew Bagby
(Examined the victims computer and found evidence it was being used the day of his murder, while he was at work. Then tracked Dr. Shirley Turner's phone placing her near the murder scene.)

G-20 Summit Elliot Madison Investigation
(Seized and examined a makeshift communication center including computers and cellular phones, all which were being used to aid protesters.)

PA Vs. Boob / Heichel
(Examined cellular records and prepared a report identifying suspect location at the time of the murder.)

PA. Vs. Anthony McWhite
(Examined cellular records and prepared a report identifying suspect location at the time of the murder.)

PA Vs. Bret Thompson
(Examined cellular phones and recovered deleted communication from an app that revealed a relationship between Thompson and a juvenile victim.)

PA Vs. Christopher Marsh
(Forensically examined a phone used by Marsh to film other men in a WalMart restroom.)

PA Vs. Eric Hall
(Conducted cellular mapping and records analysis and was able to provide expert opinion of the defendant turning his phone off on the way to the murder scene.)

TN Vs. Marcus Wade

(Conducted cellular records mapping that placed the suspect at the scene of the incident. Then conducted records analysis that showed after the murder, prior to the victim being discovered, Marcus Wade quit calling the victim and fled the area of the crime.)

PA Vs. Michael Martin

(Conducted cellular records analysis and placed the defendant within a half mile of the victim at the time of the murder using RTT data. Additionally, was able to use previous days records to discredit the defendant's alibi and show a pattern of going to the victim's residence days prior to the incident.)

PA Vs. David Stahl

(Conducted forensic analysis to show the victim's phone was still being used after her death. And that the phone was in close proximity to the defendant's phone while the two phones were texting each other. Also placed the defendant's phone within .3 miles away from the victim's body near an airport runway.)

PA Vs. Greg Howard

(Conducted cellular record analysis to show locations of the suspect at the time of a robbery. Additionally, analyzed records to show call patterns and frequency or calls as well as identified when the suspect's phone was forwarding calls to another cellular device.)

PA Vs. Earl Pinkney.

(Conducted cellular record analysis of several phones to identify locations of several suspects at the time of the murder. Additionally, conducted forensics on cellular devices and recovered SMS messages from a locked iOS device that included a conversation about what type of bullets to purchase.)

ANPAC Vs. Stuttes

(Conducted cellular analysis and mapping of 2 individuals to determine if they were in the area of an arson at their residence. ANPAC expert report refuted their statements of being in Nashville at the time of the incident. Several errors were found in the ANPAC expert report and the victims were subsequently placed in the area they stated. US Cellular confirmed the findings, and the ANPAC expert and ANPAC attorneys conceded that their expert report was incorrect.)

PA Vs. Michael Peterson

(Conducted cellular analysis of the defendant and victim to show movements prior to, at the time of, and after a drug delivery that resulted in the overdose death of the victim.)

Kozel Vs Kozel

(Conducted forensic examinations to locate SMS messages from over 5 years ago. The messages could not be located on the devices but were located in iOS backups of office computer systems. Expert Testimony was given concerning the source of the SMS messages.)

PA Vs Sieminkewicz

(Conducted forensic examination on several devices to identify if the defendant had sent threatening Unverified Vtext messages to the victim, as well as applied for a Discover Card in her name. Evidence of both was located on computer systems, and expert testimony was given concerning the evidence.)

PA Vs David Johnson

(Conducted forensic examination of numerous devices for a criminal homicide investigation. Several of the items had been attempted to be examined by another lab but were unsuccessful. My examination revealed a large amount of data that was able to show communications and a timeline of the incident. Expert Testimony was given regarding the evidence.)

PA Vs Brian Isbell

(Conducted forensic examination of cellular devices and extracted SMS messages that provided evidence supporting the charges of IDSI, Aggravated Indecent Assault and Endangering the welfare of Children. The case went to trial and defense stipulated to my examination. The defendant was found guilty of charges.)

PA Vs Barshay Dunbar

(Conducted forensic examination on a cellular device and extract user accounts, SMS / MMS contents, Test Free application messages and pictures to support the charges that the defendant was running a prostitution ring and human trafficking. The defendant was found guilty.)

IN Vs Emmanuel Arrington

(Conducted cellular analysis of the defendant, a co-defendant and victim to show movements prior to, at the time of, and after an attempted homicide. The defendant was found guilty.)

TX Vs Aniseto Alejandro Jr.

(Conducted forensic examination on a cellular device to locate relevant data on the device, and cellular analysis of cellular records to locate to show movements prior to, at the time of, and after a double homicide. The defendant was found guilty.)