Ahmet Furkan Aydogan

Assistant Professor, Department of Computer Science
University of North Carolina Wilmington
601 College Road, Wilmington, NC 28403 · +1 (910) 962-2818 · aydogana@uncw.edu

Professional Summary

Tenure-track Assistant Professor of Computer Science at the University of North Carolina Wilmington with a PhD in Digital and Cyber Forensics Science. Research and teaching focus on digital forensics, Internet of Things (IoT) security, brain signal (EEG) based encryption, maritime cybersecurity, security of AI coding agents, and responsible artificial intelligence in education. Co-inventor on a hardware-based transparent encryption patent application, active member of three IEEE Standards Association working groups (P2834, P2834.1, P3722), and a two-time recipient of the UNCW Senior Class Recognition for Positive Impact on Student Experience. Peer-reviewed publications in IEEE conferences and MDPI journals; invited presentations at DEF CON 33, DEF CON 34, and the Triangle InfoSeCon.

Education

- **Sam Houston State University** — Huntsville, Texas, USA
  Doctor of Philosophy in Digital and Cyber Forensics Science — *2019 - May 2024*
  - Dissertation: *Brain Frequency-Based Encryption Method for IoT Devices.* Advisor: Cihan Varol.
  - Areas of concentration: cybersecurity, cryptology, machine learning, Internet of Things, human-computer interaction.

- **Sam Houston State University** — Huntsville, Texas, USA
  Bachelor of Science in Computer Software Engineering Technology — *2015 - May 2019*
  - Areas of concentration: cryptology, vehicular ad-hoc networks, cybersecurity, social engineering.
  - Dean's List of Academic Honors (2019). Recipient of the Enhancing Undergraduate Research Experiences and Creative Activities award (2018).

Academic Appointments

- **University of North Carolina Wilmington** — Wilmington, NC, USA
  Tenure-Track Assistant Professor, Department of Computer Science — *August 2024 - Present*
  - Teach undergraduate and graduate courses in computer networks, network programming, cybersecurity fundamentals, cyber operations, and computer and mobile forensics.
  - Chair two master's thesis committees and co-chair two doctoral advisory committees; supervise directed individual study projects in malware detection, generative AI forensics, and UAV protocol analysis.
  - Principal investigator on maritime cybersecurity compliance research; affiliated with the Maritime Cybersecurity Applied Research, Technology and Education Center (MCARTEC).
  - **Courses Taught (UNCW):**
    - CSC 344 Computer Networks — Fall 2024, Spring 2025, Fall 2025, Spring 2026
    - CSC 544 Network Programming — Fall 2025
    - CYBR 354 Computer and Mobile Forensics — Fall 2025, Fall 2026
    - CYBR 358 Cyber Operations — Fall 2026
    - CYBR 201 Fundamentals of Cybersecurity — Fall 2026

- **Sam Houston State University** — Huntsville, TX, USA
  Graduate Teaching Appointments, Computer Science Department — *2018 - 2024*
  - **Instructor of Record (Teaching Faculty, Part-Time):**
    - CSTE 1330 Introduction of Computers — Fall 2022, Spring 2024
    - DFSC 4338 Cyberwarfare — Spring 2022, Spring 2023
  - **Teaching Assistant:**
    - COSC 2327 Introduction to Computer Networks — Fall 2023
    - CSTE 1330 Introduction of Computers — Fall 2023
    - DFSC 4317 Information Security — Spring 2021
    - DFSC 5338 Ethical Hacking — Summer 2020
    - COSC 2347 Programming with Python — Spring 2019
    - COSC 5325 Operating System Forensics — Spring 2018
  - **Research Supervisor:** Supervised undergraduate research on brain-signal integration with digital systems. 22, 23

- **Samsung Electronics Turkey** — Istanbul, Turkey
  Software Engineering Intern — *July 2016 - September 2016*

- **Samsung Electronics Turkey** — Adana, Turkey
  Information Technology Technician Intern — *July 2013 - September 2013*

Research Interests

Digital forensics; computer forensics; mobile forensics; Internet of Things (IoT) security; embedded systems security; brain-computer interfaces; electroencephalogram (EEG) signal analysis; biometric cryptography; cybersecurity education; maritime cybersecurity; software-defined radio security; security of AI coding agents and large language model tooling; blockchain and smart-contract (EVM) security; machine learning for intrusion and device detection; responsible artificial intelligence in higher education; secure and trusted learning systems.

Courses Taught at UNCW

- **CSC 344 - Computer Networks (Undergraduate)**: Applied network security aligned with NSA/DHS CAE-CD, NIST NICE, AICyber, and OWASP frameworks. Twelve hands-on labs using Nmap, Wireshark, Burp Suite, OWASP ZAP, sqlmap, Binwalk, and genuine OpenWrt firmware. Integrates the Poseidon's Spear maritime CTF capstone and an accountable AI policy. Prepares students for CompTIA Security+, Network+, CEH, PenTest+, and OSCP certification domains.
- **CSC 544 - Network Programming (Graduate)**: Capstone experience bridging networking theory, systems programming, and applied security. Berkeley socket programming in C, C++, Java, and Python asyncio; paired offensive and defensive labs across the OSI stack; semester-long Poseidon's Spear CTF capstone mapped to five NICE SP 800-181 work roles.
- **CYBR 354 - Computer and Mobile Forensics (Undergraduate)**: Full digital forensics lifecycle aligned with CAE-CD Digital and Device Forensics Knowledge Units and NIST NICE Investigate-category work roles (IN-FOR-001, IN-FOR-002, IN-INV-001). Authentic E01 and DD evidence images, OpenWrt firmware forensics, Autopsy / FTK / Cellebrite toolchain, and case-study pedagogy anchored in landmark criminal investigations.
- **CYBR 358 - Cyber Operations (Undergraduate)**: Offensive and defensive cyber operations with hands-on operator laboratories; authored an original laboratory sequence for the course (Fall 2026).
- **CYBR 201 - Fundamentals of Cybersecurity (Undergraduate)**: Foundational cybersecurity principles, threat landscapes, and defensive architectures.

Teaching Innovation and Curriculum Development

- **CSC 344 - Computer Networks** — UNCW Department of Computer Science
  Revise Existing Course — *August 2024 - May 2026*
  - Redesigned around a security-first networking paradigm with quadruple framework alignment (NSA/DHS CAE-CD, NIST NICE, AICyber foundational and advanced, OWASP). Authored six Visme HTML5 lecture modules and twelve laboratories structured as coherent multi-stage attack chains (reconnaissance → port scanning → directory enumeration → SQL injection; buffer overflow → WannaCry / EternalBlue).
  - Originated the accountable AI integration policy (AI-assisted coding permitted subject to line-by-line annotation and oral defense) and packaged all lectures as offline-capable HTML5 archives for equitable access.
  - Integrated authentic-artifact labs: genuine OpenWrt 18.06.0 firmware extraction, student-deployed LAMP stack, manual and automated SQL injection, and SSL/TLS analysis with sslscan and testssl.sh. Professional readiness overlaps with CompTIA Security+, Network+, CEH, PenTest+, GIAC GEVA, GIAC GWEB, and OSCP certification domains.
- **CSC 544 - Network Programming** — UNCW Department of Computer Science
  Curriculum Development — *August 2024 - Present*
  - Developed a graduate capstone bridging networking theory, systems programming, and applied security. Authored eleven Course Learning Outcomes aligned with ABET student outcomes, NSA/DHS CAE-CD Knowledge Units, and five NIST NICE SP 800-181 work roles (Vulnerability Assessment Analyst, Cyber Defense Forensics Analyst, Exploitation Analyst, Cyber Intelligence Analyst, Network Operations Specialist).
  - Originated the Blue Team / Red Team integration model pairing every offensive technique with its defensive countermeasure; institutionalized through the Buffer Overflow project with Exploitation and Defense sub-groups validating mitigations against live payloads. Replaced traditional homework with Agile-style weekly Project Progress Reports.
  - Authored the Poseidon's Spear CTF (16 challenges across five tiers, 40 percent of grade) spanning Web Exploitation, Network Forensics, Steganography, OSINT, Binary Exploitation, Signal Analysis, and Cryptography. Every challenge maps to a CLO, a CAE-CD Knowledge Unit, and a NICE work role.
  - Supervised three major Fall 2025 student projects: a Buffer Overflow Teaching Resource (8-member team), a Web Application Attack Demonstration CTF (4-member team), and an individual WAF-Based SQL Injection Challenge demonstrating three structural WAF limitations.
- **CYBR 354 - Computer and Mobile Forensics** — UNCW Department of Computer Science
  Revise Existing Course — *August 2025 - December 2025*

- Authored an eighteen-component Watermark Faculty Success Dossier representing more than twenty-five hours of structured student engagement, aligned with CAE-CD Digital and Device Forensics Knowledge Units, NIST NICE Investigate-category work roles (IN-FOR-001, IN-FOR-002, IN-INV-001), NIST SP 800-86, SWGDE best practices, NIST SP 800-101 Rev. 1 mobile extraction taxonomies, and ACM/IEEE CS2023 Security knowledge areas.
- Built case-study-driven pedagogy anchored in the BTK Killer, Chandra Levy, and Lisa Montgomery investigations. Laboratory sequence uses authentic evidence artifacts (genuine E01 and DD forensic images, an unmodified OpenWrt 18.06 firmware binary) with a dual Blue Team / Red Team analytical frame throughout.
- Originated a calibrated AI academic integrity policy: Exam 2 explicitly permits AI tools while requiring original analysis, and a CTF-style Lab 4 homework requires sequential real-world tool chains intrinsically resistant to AI-assisted completion.
- Proposed three next-iteration enhancements: dedicated mobile forensics with ADB, ALEAPP, and iLEAPP; a cloud forensics module covering MLAT, preservation letters, and registry/prefetch artifacts; and an AI-evidence authentication module aligned to the Daubert and Frye expert witness standards.

- **CYBR 358 - Cyber Operations** UNCW Department of Computer Science
  New Course Preparation *August 2026 - Present*
  - Assumed and prepared the Cyber Operations course for Fall 2026; authored an original hands-on operator laboratory sequence.

Peer-Reviewed Publications

Journal Articles

- Mfodwo, E., Lanka, P., Aydogan, A. F., & Varol, C. (2026). Uncovering the Security Landscape of Maritime Software-Defined Radios: A Threat Modeling Perspective. *Applied Sciences*, 16(2), 813. doi.org/10.3390/app16020813.
- Aydogan, A. F., Varol, C., Shashidhar, N. K., Rasheed, A., Pham, V., & Karabatak, M. (2024). The Effect of Ironic Process Theory on Brain Signal-Based Encryption for IoT Devices. *Electronics*, 13(23), 4804. doi.org/10.3390/electronics13234804.
- Aydogan, A. F., Varol, C., Rasheed, A., & Shashidhar, N. K. (2023). A Review of Encryption Techniques in IoT Devices. *International Journal of Security (IJS)*, 14(1), 17-37.

Conference Papers

- Mfodwo, E., Varol, C., Rasheed, A., Shashidhar, N. K., & Aydogan, A. F. (2027, March). Disk Forensics of Wi-Fi Deauthentication Attacks on Maritime NMEA 2000 Wireless Networks. *International Symposium on Digital Forensics and Security (ISDFS)*, San Jose State University, CA. **Accepted**.
- Mfodwo, E., Shashidhar, N., Varol, C., & Aydogan, A. F. (2026, March). Forensic Investigation of SDRSharp and RTL-SDR Dongle in Eavesdropping Radio Communications. *International Symposium on Digital Forensics and Security (ISDFS)*. doi.org/10.1109/ISDFS69419.2026.11458928.
- Senol, N., Thai, J., Cal, S., & Aydogan, A. F. (2026, March). Volatile Memory Forensics of Tails OS in a Virtualized Environment. *International Symposium on Digital Forensics and Security (ISDFS)*. doi.org/10.1109/ISDFS69419.2026.11459100.
- Senol, N. S., Rasheed, A., Aydogan, A. F., & Cal, S. (2026, February). Experimental Analysis of AES, ChaCha20, and XOR Encryption in LoRa Networks. *International Conference on Artificial Intelligence, Computer, Data Sciences and Applications (ACDSA)*. doi.org/10.1109/ACDSA67686.2026.11467958.
- Senol, N. S., Chennamaneni, A., Rasheed, A., & Aydogan, A. F. (2025, April). Leveraging Machine Learning for Effective Device Detection and Security in LoRa-Based IoT Systems. *International Symposium on Digital Forensics and Security (ISDFS)*. doi.org/10.1109/ISDFS65363.2025.11011982.
- Aydogan, A. F., Varol, C., & Saliah-Hassane, H. (2025, April). Security Assessments of Data Transfer Phase of Adapted EEG System in Learning Systems. *International Symposium on Digital Forensics and Security (ISDFS)*. doi.org/10.1109/ISDFS65363.2025.11012111.
- Aydogan, A. F., Varol, C., Vanli, A., & Varol, H. (2024). A New Security Mechanism for IoT Devices: Electroencephalogram (EEG) Signals. *Proceedings of the Second International Conference on Advances in Computing Research (ACR'24)*, 306-317. doi.org/10.1007/978-3-031-56950-0_26.
- Rabieh, K., Aydogan, A. F., & Azer, M. A. (2021, October). Towards Safer Roads: An Efficient VANET-based Pedestrian Protection Scheme. *IEEE CCCI*. doi.org/10.1109/CCCI52664.2021.9583221. **Best Paper Award**.
- Aydogan, A. F., An, M. K., & Yilmaz, M. (2021, June). A New Approach to Social Engineering with Natural Language Processing: RAKE. *International Symposium on Digital Forensics and Security (ISDFS)*. doi.org/10.1109/ISDFS52919.2021.9486342.

- Aydogan, A. F., & Shashidhar, N. K. (2021). Prevention Pre-Violence in E-Labs with Machine Learning: PVE. *9th International Symposium on Digital Forensics and Security (ISDFS)*, 1-5. doi.org/10.1109/ISDFS52919.2021.9486349.
- Rabieh, K., & Aydogan, A. F. (2019, June). A Fair and Privacy-Preserving Reservation Scheme for Charging Electric Vehicles. *International Symposium on Networks, Computers and Communications (ISNCC)*. doi.org/10.1109/ISNCC.2019.8909163.
- Hughes, N., Rabieh, K., & Aydogan, A. F. (2019, June). Employing a Continuous Measurement Process During Digital Tool Validation. *International Symposium on Networks, Computers and Communications (ISNCC)*. doi.org/10.1109/ISNCC.2019.8909102.
- Aydogan, A. F., & Zhou, B. (2018, December). Improving Database Security with Pixel-based Granular Encryption. *2018 IEEE International Conference on Big Data*. doi.org/10.1109/BigData.2018.8622276.
- Aydogan, A. F., Varol, N., & Varol, A. (2017, April). Cyber Attacks Targeting Android Cellphones. *International Symposium on Digital Forensics and Security (ISDFS)*. doi.org/10.1109/ISDFS.2017.7916511.

Under Review and Submitted

- Femi-Adeyinka, C., Varol, C., Aydogan, A. F., & Tutt, M. E. (under review, Journal of Forensic Sciences). Generative AI for Crime Scene Simulation: A Synthetic Dataset for Forensic Object Detection.
- Femi-Adeyinka, C., Varol, C., & Aydogan, A. F. (under review). Extended Reality in Crime Scene Investigation: A Systematic Review and Evidence-Readiness Agenda. *Forensic Science International: Digital Investigation* (Elsevier).
- Mfodwo, E., Varol, C., Rasheed, A., Shashidhar, N. K., & Aydogan, A. F. (submitted). Cracking the Maritime Handshake: Memory Forensics of Wi-Fi De-Authentication Attack on NavLink2 NMEA 2000 Server. *Electronics* (MDPI).
- Mfodwo, E., Varol, C., Shashidhar, N. K., & Aydogan, A. F. (submitted). Forensic Attribution of Wi-Fi Pineapple Deauthentication Attacks on Maritime NMEA 2000 NavLink2 Wireless Network. *Forensic Science International: Digital Investigation*.
- Mfodwo, E., Lanka, P., & Aydogan, A. F. (in preparation). Maritime Cybersecurity and Forensics: A Testbed for Smart Vessels.
- Mfodwo, E., Varol, C., Aydogan, A. F., & Lanka, P. (conditionally accepted, revisions requested). Exploiting Maritime Wi-Fi Gateway: Security Assessment of NMEA 2000 Wireless Server. *4th International Conference on Cyber Resilience (ICCR-2026)*.
- Garland, Moore, A., K., & Varol, C., Gupta, K., Aydogan, A.F. (submitted). Navigating the Digital Frontier: A Primer on Forensic Digital Investigations for Criminal Justice Professionals. Book chapter, publisher under review.

Intellectual Property

- Demir, T., & Aydogan, A. F. (April 2026). *Hardware-Based Transparent Encryption and Physical Authorization System for Data Communication Lines*. Patent application filed.

External Funding and Sponsored Research

- **Aydogan, A. F.** (Principal Investigator), Pence, T. B. (Supporting). *Securing the Digital Maritime Frontier: An Automated Compliance and Cybersecurity Framework for 33 CFR MTSA*. NCInnovation. Amount: $670,000. Submitted 2026 (not selected for funding).
- Capar, I. (Principal Investigator), Martin, M. W., & **Aydogan, A. F.** (Co-Principal Investigator). *AI Feedback Tracking and Reporting Platform (AI Usage Reporting Tool for Education)*. NCInnovation Pipeline Grant, UNCW Office of Innovation and Commercialization, Spring 2026. Submitted 2026 (not selected for funding).
- Selected participant, NCInnovation-Appalachian State University Innovation Cohort (Cohort 5, Fall 2026).

Invited Presentations and Conference Talks

- Aydogan, A. F., & Yildirim, U. (August 2026). *PMTC: One-Click RCE and Persistent Exfil in AI Coding Agents*. DEF CON 34, Red Team Village, Las Vegas, NV.
- Simsek, S. B., & Aydogan, A. F. (co-speaker) (August 2026). *Hunting for Cryptographic Ghosts: A Bug Hunter's Guide to Signature Malleability and Replay Attacks in EVM Bridges & Multi-Sigs*. DEF CON 34, Bug Bounty Village - Creator Stage, Las Vegas, NV.
- Arslan, M., & Aydogan, A. F. (August 2026). *Isopod: The Ultimate UART Hardware Implant*. DEF CON 34, IoT Village, Las Vegas, NV.

- Aydogan, A. F. (Presenter and Author). (October 2025). *Maritime Cyber Lab Workshop.* 7th Annual UNCW Cybersecurity Conference, Maritime Transportation System Track, Congdon Hall, UNCW, Wilmington, NC.
- Key, M. O., & Aydogan, A. F. (August 2025). *Navigating the Invisible.* DEF CON 33, Creator Stage 3 (W231), Las Vegas Convention Center, Las Vegas, NV.
- Aydogan, A. F., Key, M. O., & Demir, T. (August 2025). *No Brain No Gain.* DEF CON 33, Creator Stage 2 (W232), Las Vegas Convention Center, Las Vegas, NV.
- Aydogan, A. F. (Presenter and Author). (February 2025). *Digital Forensics Analysis of Windows Event Logs.* IEEE P2834.1 Working Group, IEEE Standards Association - Education Society Standards Committee.
- Aydogan, A. F. (November 2024). *Brain Signal-Based Encryption Method for IoT Devices.* 2024 Triangle InfoSeCon, ISSA Raleigh Chapter, Raleigh, NC.
- Aydogan, A. F. (Presenter Only). (August 2023). *Integration of Human-Computer Interaction (HCI) with Brain Signals.* CMES 2023 Summer School and Mathematics Student Congress, Mersin University, Mersin, Turkey.
- Guest Lecture. (March 2026). UNCW Intelligent Systems Engineering Program, ISE 495: Seminar in Intelligent Systems Engineering.
- Guest Lecture. (October 2025). UNCW Honors College, HON 120: Honors Enrichment Seminar, Cybersecurity: Basics and Beyond.

Security Research and Responsible Disclosure

- Lead researcher, **PMTC (Persistent MCP Tool Capture)** — an independent research program on trust-boundary and Model Context Protocol (MCP) behaviors in production AI coding agents, spanning Anthropic Claude Code and OpenAI Codex CLI (2026).
- Submitted multiple coordinated-disclosure reports to Anthropic's Bug Bounty Program via HackerOne (2026), covering parent-directory `.mcp.json` auto-discovery, OAuth scope handling with automatic Dynamic Client Registration, headless-mode trust-prompt behavior, a Windows service DACL weakness, and a `permissions.deny` path-canonicalization bypass involving Windows 8.3 short names.
- Reported additional model-side (LLM behavior) findings to Anthropic's model safety and bug-bounty programs (2026).
- Cross-vendor testing on OpenAI Codex CLI (post-CVE-2025-61260) to assess how the disclosed behaviors generalize across agent-CLI vendors.

Professional Service and Standards Development

IEEE Standards Association Working Groups

- **IEEE P3722 Working Group** - Guide for Responsible Artificial Intelligence in Higher Education. Working Group Member (October 2025 - Present). Chair: Usman Naeem, Queen Mary University of London.
- **IEEE P2834.1 Working Group**. Working Group Member (October 2024 - Present). Chair: Cihan Varol, Sam Houston State University. Delivered technical presentation on digital forensics analysis of Windows event logs (February 2025).
- **IEEE P2834 Working Group** - Standard for Secure and Trusted Learning Systems. Development Team Member and Working Group Member (October 2021 - Present). Chair: Hamadou Saliah-Hassane.

Conference Service

- Reviewer, ISDFS 2027 Scientific Committee (International Symposium on Digital Forensics and Security).
- Program / organizing contributor, 8th Annual UNCW Cybersecurity Conference (Maritime Security focus), October 8-9, 2026.
- Host committee, ACM SIGCITE 2026, hosted at UNCW.
- Subject-matter expert reviewer, cybersecurity fundamentals textbook module and expert survey (at the request of G. Stoker), 2026.
- Session Chair, Session B-X (AI, Big Data, and IoT), ACDSA 2026 - International Conference on Artificial Intelligence, Computer, Data Sciences and Applications, co-sponsored by IEEE, Antalya Bilim University, ecer.org, and IJECER. Boracay Island (February 5-7, 2026).
- Session Chair, Session 3 (VGSC-2025 Workshop), ISDFS 2025 - 13th International Symposium on Digital Forensics and Security, Boston, MA (April 24, 2025).

- Peer Reviewer, ACM 9th International Workshop on Security and Privacy Analytics (IWSPA 2023).
- Peer Reviewer, IEEE International Symposium on Digital Forensics and Security (ISDFS 2021, 2022, 2023, 2026).
- Peer Reviewer, IEEE Transactions on Vehicular Technology (2023).

Institutional Service at UNCW

- Member, Cybersecurity Advisory Committee, UNCW Department of Computer Science (August 2025 - Present).
- Invited faculty participant, UNCW Center for Cyber Defense Education (CCDE) Advisory Board meetings (2026).
- Provided written curriculum input on UNCW's proposed CAE Cyber-AI (AICyber) Program of Study (April 2026).
- Committee Member, Department of Computer Science Scholarship Committee (March 2026 - May 2026).
- Participant, Computer Science Faculty Candidate Interviews, AY 2024-25 and AY 2025-26 hiring cycles.
- Cybersecurity-affiliated faculty (AY 2026-27).

Directed Student Learning

- **Master's Committee Chair**: Latha Shree Krishnapura Prabhakara. *A Comprehensive Analysis of Protocols for Unmanned Aerial Vehicles*. UNCW Computer Science (January 2026 - Present). Committee members: Hosam Alamleh and Bilge Karabacak.
- **Master's Committee Chair**: Aidan Christiaan O'Brien. *The Role of Expectation in Modulating Heart Rate Fluctuations*. UNCW Computer Science (March - August 2025).
- **Doctoral Advisory Co-Chair**: Erasmus Mfodwo. *A Multi-Layer Security Framework for Maritime Cyber-Physical Systems: From Threat Modeling to Empirical Forensic Assessment of Software-Defined Radio and Wireless Navigation Networks*. Sam Houston State University (February 2025 - Present).
- **Doctoral Advisory Co-Chair**: Chiamaka Femi-Adeyinka. *Generative AI for Crime Scene Simulation: A Synthetic Dataset for Forensic Object Detection*. Sam Houston State University (December 2024 - Present).
- **Master's Committee Member**: Bradley Hays. *Effectiveness of the Doppler Effect to Augment Global Navigation Satellite System Position and Navigation Data in Maritime Environments*. UNCW Computer Science (August 2024 - April 2025).
- **Master's Committee Member**: David Begu. *Market Regime Detection in Bitcoin Using Hidden Markov Models: Toward Emotion-Free Algorithmic Trading*. UNCW Computer Science (March - May 2025).
- **Directed Individual Study**: Miles Emory Tutt. Generative AI for crime scene simulation and synthetic forensic object detection (August 2025 - January 2026).
- **Directed Individual Study**: Dimitri James Montgomery. Malware detection with locality-sensitive hashing (May - July 2025).
- **Supervised Research**: Ayse Vanli. Integrating brain signals to digital life (January - May 2023).

Awards and Honors

- **Senior Class Recognition for Positive Impact on Student Experience**, UNCW Office of Academic Affairs and Office of the Vice Chancellor for Student Affairs (April 2026).
- **Senior Class Recognition for Positive Impact on Student Experience**, UNCW Division of Student Affairs and Office of Academic Affairs (November 2025).
- **Best Student Presentation**, for *Brain Frequency-Based Evolutionary Encryption Method for IoT Devices*, IEEE Education Society Standards Development and Virtual Graduate Study Consortium Kick-off Workshop (December 14, 2022).
- **Accreditation Board for Engineering and Technology (ABET) Course Excellence Grade**, Introduction of Computers, Sam Houston State University (2022).
- **Best Paper Award**, for *Towards Safer Roads: An Efficient VANET-based Pedestrian Protection Scheme*, IEEE International Conference on Communications, Computing, Cybersecurity, and Informatics (CCCI), October 17, 2021.
- **Perception Management and Information Gathering Certificate of High Merit**, 9th Eye (2020).
- **Dean's List of Academic Honors**, Sam Houston State University (2019).
- **Grant for Enhancing Undergraduate Research Experiences and Creative Activities**, Sam Houston State University (2018).

Teaching Effectiveness and Evaluations

Fall 2025 UNCW Student Course Evaluations (Overall Effectiveness)

- **CYBR 354 Computer and Mobile Forensics (section 001)**: Overall effective instructor rating of 4.80 against a UNCW mean of 4.54; overall effective course rating of 4.80 against a UNCW mean of 4.42. Response ratio 62.50 percent.

- **CSC 344 Computer Networks (section 001)**: Overall effective instructor rating of 4.70 against a UNCW mean of 4.54; overall effective course rating of 4.55 against a UNCW mean of 4.42. Response ratio 74.07 percent.
- **CSC 544 Network Programming (section 002)**: Overall effective instructor rating of 4.62 against a UNCW mean of 4.54; overall effective course rating of 4.69 against a UNCW mean of 4.42. Skills developed as a result of this course rated 4.92. Response ratio 76.47 percent.
- **CSC 344 Computer Networks (section 002)**: Overall effective instructor rating of 4.27; instructor treated students with respect rated 4.82 against a UNCW mean of 4.70. Response ratio 52.38 percent.

Fall 2024 IDEA Course Evaluations (Converted Scores on a Bell Curve, Adjusted)

- **CSC 344 Computer Networks (section 002)**: Adjusted converted score of 56 (Higher than IDEA discipline average) on Excellent Teacher and 56 on Excellent Course. Response rate 82.14 percent.
- **CSC 344 Computer Networks (section 001)**: Raw mean 4.2 on Excellent Teacher and 4.2 on Excellent Course. Response rate 92.86 percent.

Spring 2025 IDEA Course Evaluations

- **CSC 344 Computer Networks (section 001)**: Adjusted converted scores of 64 on Excellent Teacher and 64 on Excellent Course, placing the course in the Much Higher bucket (highest 10 percent) against IDEA benchmarks. Raw means of 5.0 and 4.7 respectively.
- **CSC 344 Computer Networks (section 002)**: Adjusted converted scores of 46 on Excellent Teacher and 49 on Excellent Course. Response rate 70.37 percent.

Peer Evaluation of Teaching

- Layman, L., Stoker, G., & Ferner, C. (October 2025). Peer observation of CSC 344 Computer Networks. Evaluators documented instructor subject-matter knowledge, student engagement with respect, and the use of current pedagogical techniques as areas of strength.
- Ebrahimi, E., & Ferner, C. (September 2024). Peer observation of CSC 344 Computer Networks.

Licensures and Certifications

- CITI Biomedical Researcher Certification (January 2023 - 2028).
- CITI Human Subject Researcher Certification (January 2023 - 2028).
- Establishing an IT-Based Workplace Certification, Cukurova Endustri Meslek Lisesi (August 2013 - Present).

Professional Memberships

- Vice President, Turkish Student Organization, Sam Houston State University (November 2019 - 2023).
- Member, The National Society of Collegiate Scholars (November 2019 - 2023).

Graduate-Level Coursework

File System Forensics; Cyber Forensics Principles; E-Discovery; Ethics for Digital Forensics; Digital Forensics Laboratory Management; Digital Forensics Tools and Techniques; Operating System Forensics; Network Forensics Analysis; Mobile Device Forensics; Live System and Memory Forensics; Scientific Communications; Law and Forensic Science; Fundamentals of Criminalistics; Statistical Methods for Decision Making; Cryptology and Steganography; Social Media Forensics; Malware Forensics Analysis; Reverse Engineering.

Professional Development

- Participant, 2026 CTE Institute: Teaching Technical Skills, Challenge Content, and Unprepared Students, UNCW Center for Teaching Excellence (Summer 2026).
- Conference Attendance, 2024 Triangle InfoSeCon, ISSA Raleigh Chapter, Raleigh, NC (November 2024).

Consulting

- Cybersecurity Advisor, Diversity Education Institute, Huntsville, Texas (2018 - 2018).

Technical Skills

- **Programming Languages**: Python, C, C++, C#, .NET, Java, JavaScript, PHP, MATLAB, Turbo Pascal, Bash, SQL, HTML, CSS
- **Digital Forensic Tools**: Autopsy, EnCase, X-Ways Forensics, Oxygen Forensic Detective, Cellebrite, The Sleuth Kit, FTK and FTK Imager, Magnet Axiom, WinHex, Chimera, Z3X, Octoplus, Bless, HxD, xxd, Thumbcache Viewer, Steghide, John the Ripper, hash-identifier, Gary Kessler File Signatures reference
- **Network and Security Tools**: Wireshark, Burp Suite, Nmap (NSE scripts), Netcat, Curl, OWASP ZAP, OWASP DirBuster, sqlmap, jSQL, sslscan, testssl.sh, Binwalk, Firmwalker, crunch, Airmon-ng, Airodump-ng, Phonesploit, pwntools, GDB with pwndbg, Scapy, CyberChef, Stegsolve, OpenCPN, oletools and olevba, unsquashfs, Ludus
- **Operating Systems and Platforms**: Kali Linux, Parrot OS, Windows, Linux, Android, iOS, OpenWrt, macOS, VMware, VirtualBox
- **File Systems and Artifacts**: NTFS, EXT4, APFS, FAT32, Master Boot Record, Master File Table, E01 and DD evidence images, squashfs
- **Standards and Frameworks**: NSA/DHS CAE-CD Knowledge Units, NIST NICE (SP 800-181), NIST SP 800-86, NIST SP 800-101 Rev. 1, AICyber, OWASP, SWGDE, ACM/IEEE CS2023 Security Knowledge Areas
- **Research and Cybersecurity Expertise**: Digital forensics investigation, Texas law, e-discovery, cyberwarfare, information security, social engineering, ethical hacking, penetration testing, security of AI coding agents, blockchain/EVM security, machine learning, deep learning, object detection, natural language processing, cryptology, vehicular ad-hoc networks, wireless security, EEG data acquisition and signal processing

Languages

- English (professional working proficiency); Turkish (native).

Media Coverage

- Channel 23 television interview (2019).
- Manvel High School informational interview, *What Cyber Attacks Will Look Like in a Decade*, Huntsville, Texas (January 2020).