Reem Arnaout

Beirut, Lebanon | **Phone:** +961 76 963 248 | reemarnaout1@gmail.com | **References**: GitHub | **LinkedIn:** Reem Arnaout

EDUCATION

From 08/2021 to 06/2025 **American University of Beirut (AUB)** Beirut, Lebanon

- Bachelor of Engineering in Computer and Communications
- Graduated with **Distinction**
- GPA over 4: 3.52 (Overall), 3.73 (Final Two Years - Major Concentration)
- Recipient of the **President's Merit Scholarship** for Early Admission
- Awarded for the **best final year project** in the ECE department
- 4 placements on the **Dean's Honor List**

MOST NOTABLE COURSEWORK

Digital Forensics and Incident Response, Ethical Hacking, Software Security, Internet Security, Cryptography, Machine Learning, Mobile Networks, Computer Networks, Digital Signal Processing, Communication Systems, Electromagnetics

EXPERIENCE

From 05/2024 to 07/2024 **Dar Al-Handasah -** Telecommunication Internship Beirut, Lebanon

- Designed optical fiber cabling, medical control, AV, security, and fire alarm systems across 4 projects.
- Followed TIA, IEEE, OSHA, BICSI standards and used AutoCAD and Revit for system layout and compliance.

PROJECTS AND RESEARCH

- **TrackSmart: Secure Wireless Mobility Analytics- Final Year Project (Awarded best FYP)**
  - Collaborated with KAUST and led a team to develop an **AI-powered** system using over 800 hours from two real cellular network data (MOBiSENSE + SHL Challenge) which classified 9 transportation modes with **86% accuracy** using 7 ML models including XGBoost, SGD, LSTM, CNN, and Transformer.
  - Integrated **Differential Privacy** and **Federated Learning** to anonymize user data and ensure GDPR compliance. Achieved **76% accuracy** at ∈=5 using two private models (DP-SGD and DP-XGBoost).
- **Digital Forensics & Incident Response (DFIR) Investigation**:
  - Conducted an investigation of a multi-host simulated corporate breach using **disk**, **memory**, **pagefile**, and **network forensics** to identify RDP brute-force entry, malware persistence, and lateral movement.
  - Used Volatility, Autopsy, KAPE, Plaso, Wireshark, and multiple Eric Zimmerman DFIR tools to extract Indicators of Compromise (IOCs) and reconstruct the full attack timeline.
- **Network Cell Analyzer Application:**
  - Developed and deployed an **Android app** to extract and analyze cell-specific data from cellular networks.
  - Applied socket programming and built a server-side backend using Flask, SQL Alchemy, and TCP sockets
- **Avian Vocalizations Analysis using Digital Signal Processing and Machine Learning:**
  - Applied **DSP** and **CNN** to classify sounds from zebra finch recordings and collaborated with a neurologist from AUBMC to study the relation of avian vocalizations to the brain's neural communication
- **Multilayered Honeypot Architecture:**
  - Analyzed the log completeness and deception realism of **six** honeypots under controlled conditions.
  - Designed and implemented a multilayered honeypot architecture using Docker containers, integrating an **IDS** (Snort) for real-time threat detection and **AI** (GPT-4o-mini) to enhance interaction realism.
- **Two-Time Research Assistant under AUB:**
  - Vertically Integrated Projects Program: Programmed robust algorithmic solutions for **heavy-tailed** statistical problems such as Cauchy and Lévy using **Fast Fourier Transform** (FFT) to derive the PDF and CDF of alpha stable distributions and accomplished a minimum mean absolute error of 1e-17.
  - Intern: Contributed to the design and analysis of Tunable Leaky Wave Antennas for **Millimeter-Wave 5G**

TECHNICAL SKILLS

Python, C++, Linux, Bash, PowerShell, VMware, Docker, MATLAB, GNS3, VHDL/Verilog, MySQL, Java, JS, Flask