Education and Digital Forensics

Why it’s time to prepare for the new big need on the IT/Security Market

JOSE A RUIZ – MISFI / MCSA / OSCP / Security+
Digital forensics solutions are used in collecting, identifying, validating and preserving digital evidence.

Increased instances of cyber-attacks can result in financial loss for company and reputation or brand damage.

Digital forensics focuses on recovering the stolen or lost data by methodologies such as digital device acquisition, data collection, decryption, data processing and analysis, and flexible reporting.
Digital Forensic Trend

With increasing concerns of cyber-attacks, the demand for digital forensics solutions and services is expected to increase in the financial, government defense, and healthcare industries.

Technological advancements in computing and connectivity and increased instances of cyber-attacks is subjected to drive the global digital forensics market to $9.68 billion dollars expenditure by 2022.
Widespread use of IoT devices is observed in several application areas, such as smart city projects, smart transportation, vehicular connectivity and autonomous vehicles, smart grids, and smart homes.

IoT devices are heavily targeted by cybercriminals.

The Mirai Botnet attack in 2016 was a significant attack that triggered a large-scale layer 3 and layer 7 DDoS attack.
Digital Forensics Market Dynamics

**Drivers**
- Increasing instances of cyber-attacks on enterprise devices
- Massive use of IoT devices is expected to increase the demand for digital forensic solutions and services
- Stringent regulations

**Restraints**
- Encryption to be a major roadblock in digital forensics

**Opportunities**
- Higher adoption of digital forensic solutions in highly regulated industry verticals
- Rise in the use of cryptocurrencies is expected to open new avenues in digital forensics market

**Challenges**
- Lack of digital forensic preplanning among enterprises and inadequate technical expertise among digital investigators
- Difficulties in digital forensic investigation on the cloud environment
The adoption of digital forensics hardware, software, and services is expected to increase, owing to the increasing instances of cybercrimes and the need to adhere to various compliances put forth by the government for the protection of mission-critical organizational data.
The Need For a Well Trained Staff

A well trained staff allows a company to create an in house CIRT (Computer Incident Response Team).

This is the ideal situation. An in house team knows the network inside out and will perform a better job when compared to a hired gun who has no knowledge of the intricacies of your environment.
Puerto Rico has various universities that offer courses in Digital Forensics at different levels, in both traditional classroom and online offerings:

- Undergraduate
  - Graduate Certificates (Post BA)
    - Fraud Investigation
    - Forensic Investigation & Incident Response
  - Graduate (Masters Degree)
What to look for in a Digital Forensics Course

- Is it more practical than theory?
  - Remember lots of practice is what will make a difference once you start working in the field.

- Are you exposed to real life cases simulations?
  - Do you investigate mock cases to recreate real life scenarios? Do you create full reports and discuss your findings in class?, or do you learn just how to use a few tools with no direct focus on gaining on the job type of learning experiences
Thank You