

# Graduate Certificate - Digital Forensics

The graduate certificate in Digital Forensics teaches you the innovative tools and leading industry methods for collecting and scientifically analyzing digital devices and data associated with cybercrime. You'll examine the requirements for supporting legal proceedings in criminal and civil forensics, rules for presenting evidence, and how to maintain a chain of custody for evidence integrity. The process of forensics investigation can destroy the very evidence it is seeking to assimilate. The window of opportunity for collecting evidence can be a few seconds or minutes depending on the sophistication of the perpetrator. This online certificate is intended for graduate students who want to expand their knowledge of digital forensics without committing to a degree program.

This program has specific admission requirements.

## Certificate Objectives

Upon successful completion of this certificate, the student will be able to:

- Evaluate data security, integrity, and exposure from multifunctional devices.
- Analyze various digital forensics models and examine the inherent challenges in the processes for seizing electronic evidence.
- Analyze concealment and cloaking techniques and technologies such as cryptography, steganography, and data hiding and investigate corresponding legislation and mitigation techniques.
- Assess and mitigate potential exposures and the risks of the chain of custody and examine the methodologies to mitigate the potentially narrow window of opportunity for collecting digital evidence.
- Investigate models to examine the financial and societal impact of technology related crime.
- Appraise the principles, practices, and inherent challenges of the e-discovery process and assess the tools, techniques, and procedures to legally seize and forensically evaluate digital crime scenes.

## Programmatic Admission Requirements

For this program, you must provide an official transcript of your previously completed bachelor's or master's degree and have ONE of the following:

- Associate or bachelor's degree in information technology or a related field (ex: computer science, information systems, database development, etc.)
- 2 years of work experience in the specific sub-field for this degree
- Completion of one of our undergraduate IT certificates
- Completion of 6 credits in IT-related courses
- Completion of an IT-related minor or concentration during your undergraduate program
- Certifications in at least one of the below, should be active and earned since 2010:
  1. CompTIA Security+®
  2. CompTIA Network+®
  3. CompTIA A+®
  4. CompTIA Project+®
  5. CISSP® certification
  6. SSCP®
  7. EC-Council Ethical Hacking
  8. Cisco CCNA® Security
  9. Project Management Professional certification from the Project Management Institute

*CompTIA Security+®*, *CompTIA Network+®*, *CompTIA A+®*, and *CompTIA Project+®* are all registered trademarks of the Computer Technology Industry Association, Inc.

*CISSP®* and *SSCP®* are registered trademarks of International Information Systems Security Certification Consortium, Inc.

*CCNA®* is a registered trademark of Cisco Technology, Inc.

Notes:

- If the IT-specific requirements are not noted in the official bachelor's or master's transcript, you must provide official copies of your undergraduate transcripts that show the appropriate coursework.
- The verification of the 2 years' work experience needs to be sent to the university via formal resume/CV.
- Preadmission courses completed at the undergraduate level must be graded C or better; B or better at the graduate level.

Please visit our AMU (<https://www.amu.apus.edu/admissions/graduate-requirements.html>) or APU (<https://www.apu.apus.edu/admissions/graduate-requirements.html>) graduate admission page for more information on institutional admission requirements.

## Need help?

If you have questions regarding a program's admission requirements, please contact an admissions representative at 877-755-2787 or [info@apus.edu](mailto:info@apus.edu).

## Certificate Requirements (18 semester hours)

Code	Title	Semester Hours
ISSC621	Computer Forensics	3
ISSC630	Advanced Cybercrime Analysis	3
ISSC641	Telecommunications and Network Security	3
ISSC650	Advanced Digital Forensics	3
ISSC651	Advanced eDiscovery	3
ISSC680	Information Security Management	3
Total Semester Hours		18