THE UNIVERSITY OF ARIZONA

New Academic Program Workflow Form

General

Proposed Name: Digital Forensics

Transaction Nbr: 00000000000055

Plan Type: Specialization

Academic Career: Undergraduate

Degree Offered: Undergraduate Certificate

Do you want to offer a minor? N

Anticipated 1st Admission Term: Fall 2021

Details

Department(s):

UAZS

DEPTMNT ID	DEPARTMENT NAME	HOST
2910	College of Applied Science and Technology	Y

Campus(es):

DIST

LOCATION	DESCRIPTION
CHANDLER	Chandler
YUMA	Yuma

ONLN

LOCATION	DESCRIPTION
ONLN	UA Online

SOUTH

LOCATION	DESCRIPTION
DOUGLAS	Douglas
NOGALES	Nogales
PIMACCEAST	Pima Community College East

LOCATION	DESCRIPTION
SIERRAVSTA	Sierra Vista

Admission application terms for this plan: Spring: Y Summer: Y Fall: Y

Plan admission types:

Freshman: N Transfer: N Readmit: N Graduate: Y

Non Degree Certificate (UCRT only): N

Other (For Community Campus specifics): N

Plan Taxonomy: 43.0116, Cyber/Computer Forensics and Counterterrorism.

Program Length Type: Program Length Value: 0.00

Report as NSC Program:

SULA Special Program:

Print Option:

Diploma: Y Undergraduate Certificate in Digital Forensics

Transcript: Y Undergraduate Certificate in Digital Forensics

Conditions for Admission/Declaration for this Major:

Student Admittance/Advising/Completion - a high school diploma or equivalent is required for admission to an undergraduate certificate.
a. There are no prerequisites or standardized tests required for admission. Students who meet the requirements for admission to BAS programs are eligible for admission to the undergraduate certificate.
b. Concurrent enrollment in the BS, BA, or BAS programs is allowed but not required
c. A maximum of 6 units of upper division transfer credit can be evaluated for application to the certificate.
d. Academic advisors for the BAS in Cyber Operations will also advise the certificate program. No additional advising staff will be needed to support the certificate.
e. Students will be allowed to enroll in 9 semester hours in the first semester and have the ability to complete the certificate in two semesters.
f. A student may not use units taken in non-degree status to satisfy this undergraduate certificate¿s requirements.
g. This certificate will be offered to students enrolled in UA Online degree programs.

Requirements for Accreditation:

n/a

Program Comparisons

University Appropriateness

CAST is one of 21 schools in the nation to receive the Center of Academic Excellence in Cyber Operations from the National Security Agency. As a leader in the Cyber domain, CAST has partnered with government and non governmental partners to ensure the continued security of computer networks, critical infrastructure, and government regulations and personal data and privacy. This certificate aligns with UA's mission for exploring and supporting the 4th IR. It is important that our students have deep understanding of digital evidence and the acquisition, analysis, investigation of the artifacts provided by digital media. This certificate will support many organizations throughout the world and lead the academic space in digital forensics.

Arizona University System

NBR	PROGRAM	DEGREE	#STDNTS	LOCATION	ACCRDT

Peer Comparison

see attached

Faculty & Resources

Faculty

Current Faculty:

INSTR ID	NAME	DEPT	RANK	DEGREE	FCLTY/%
22078226	Paul Wagner	2910	Assit. Prof. Pract.	Master of Science	1.00
22081483	Troy Ward	2910	Adj. Instor.	Master of Science	.49
22074078	Thomas Jewkes	2910	Assit. Prof. Pract.	Master of Science	1.00
22081494	Jordan Vanhoy	2910	Assit. Prof. Pract.	Master of Science	1.00
22086398	Steven Wood	2910	Adj. Instor.	Doctor of Philosophy	.49

Additional Faculty:

Assistant Professor of Practice - Cyber Operations (Year 1)
Assistant Professor of Practice - Cyber Operations (Year 3)

Current Student & Faculty FTE

DEPARTMENT	UGRD HEAD COUNT	GRAD HEAD COUNT	FACULTY FTE
2910	450	0	4.00

Projected Student & Faculty FTE

	UGRD HEAD COUNT			GRAD HEAD COUNT			FACULTY FTE		
DEPT	YR 1	YR 2	YR 3	YR 1	YR 2	YR 3	YR 1	YR 2	YR 3
2910	30	50	85	0	0	0	5.00	5.00	6.00

Library

Acquisitions Needed:

none

Physical Facilities & Equipment

Existing Physical Facilities:

Virtual Learning Environment

Additional Facilities Required & Anticipated:

none

Other Support

Other Support Currently Available:

Support from CAST staff.

Other Support Needed over the Next Three Years:

none

Comments During Approval Process

4/6/2020 2:58 PM
PAULEWAGNER

Comments
Approved.

4/6/2020 4:18 PM
LDENNO

Comments
Approved.

4/6/2020 4:32 PM
SWIELAND

Comments
Approved.

THE UNIVERSITY OF ARIZONA.

UNDERGRADUATE CERTIFICATE – ADDITIONAL INFORMATION FORM

Note: Certificate programs offered at the University of Arizona, at the undergraduate or graduate level, are not approved as eligible programs for federal student financial aid. Although students enrolled in certificate programs are not eligible for any federal student aid programs, students may be eligible for private loans, outside scholarships, and University of Arizona department funding. For more information, please see Federal Student Financial Aid Eligibility for Programs.

General Information

Proposed Title of Certificate: Digital Forensics Certificate -- Undergraduate

CIP Code: 43.0116, Cyber/Computer Forensics & Counterterrorism

Anticipated first admission term: Fall 2021

Requested by The College of Applied Science & Technology

Program Affiliation – specify whether the UA offers an affiliated undergraduate program – the affiliated program may or may not have the same name as the proposed certificate.

Undergraduate Major in Cyber Operations

Certificate Description The 18-credit hour Digital Forensics Certificate will provide undergraduate students the confidence and training they need in incident response and various digital forensics including network forensics, mobile device forensics, host (Windows) and network (Linux) forensics and advanced memory forensics. The certificate will signal to employers that students have dedicated the time and energy necessary to develop the skills and confidence for tackling complicated digital forensic investigations for corporate, non-government, and governmental organizations. The Certificate will service a diverse student population, training both 1) technically-minded students the nuances of classifying a situation of either an event or incident and then conduct the appropriate actions to ensure that a forensically sound investigation is conducted. The Certificate will be designed and delivered to students from various backgrounds and expects students to have an introductory / fundamental knowledge of computers and network fundamentals

Purpose

The Digital Forensics Certificate is distinct in its accessibility for students from across domains, fields, and disciplines at the University. It

serves students who may or may not bring experience or prerequisites required of computer science and data analysis / digital investigation courses and programs on campus. UA is expanding its corporate partnerships and this certificate is appropriately designed to support their needs as well as the needs of the Department of Justice (DOJ), Department of Defense (DoD), and other governmental and non-governmental partners.

Target Audience(s)

This program serves students from across the university, and specifically those without the math, information science, or computer science background some expect of digital forensics. The required courses are designed to build skills and knowledge in these areas alongside the associated computer, operating systems, and digital forensic skills.

This certificate meets the needs of many of our industry partners, ranging from multi-billion-dollar insurance companies to local tech startups and Department of Defense, governmental, and non-governmental organizations.

If a student chooses to do so, they might major in any of the cyber or information / computer science degrees housed in the College of Applied Science & Technology at the University of Arizona – the certificate provides and introductory pathway into any of these degrees:

Undergraduate Major in Applied Computing / Informatics / Network Operations
Undergraduate Major in Cyber Operations
Undergraduate Major in Intelligence and Information Operations / Intelligence Studies

Certificate Requirements - complete the table below to list the certificate requirements, including number of credit hours required and any special requirements for completion. Certificate requirements should include sufficient units to provide a substantive program and an appropriate level of academic rigor and in no case be less than 12 units of credit.

Minimum total units required *minimum 12 units	18
Minimum upper-division units required *minimum 6 units of credit must be upper division UA coursework	18
Total transfer units that may apply to the certificate.	0
List any special requirements to declare/admission to this certificate	none
Certificate requirements. List all required certificate requirements including core and electives. Courses listed must include course prefix, number, units, and title. Mark new coursework (New). Include any limits/restrictions needed (house number limit, etc.). Provide email(s)/letter(s) of support from home department head(s) for courses not owned by your department.	Core: Complete 6 courses (18 units): CYBV 381 From Incident Response to Digital Forensics (3) (New) CYBV 382 Network Forensics (3) (New) CYBV 383 Mobile Device Forensics (3) (New) CYBV 384 Host and File System Forensics (Windows) (3) (New) CYBV 386 Enterprise and File System Forensics (Linux) (3) (New) NETV 477 Advanced Computer Forensics (3)

Internship, practicum, applied course requirements (Yes/No). If yes, provide description.	none
Additional requirements (provide description)	none
Any double-dipping restrictions (Yes/No)? If yes, provide description. *A maximum of 6 units may double-dip with a degree requirement (major, minor, General Education) or second certificate.	None distinct or beyond the University max of 6 units.

Current Courses–using the table below, list all existing courses included in the proposed certificate. You can find information to complete the table using the UA course catalog or UAnalytics (Catalog and Schedule Dashboard> “Printable Course Descriptions by Department” On Demand Report; right side of screen). If the courses listed belong to a department that is not a signed party to this implementation request, upload the department head’s permission to include the courses in the proposed certificate and information regarding accessibility to and frequency of offerings for the course(s). Upload letters of support/emails from department heads to the “Letter(s) of Support” field on the UAccess workflow form. Add rows to the table, as needed.

Course prefix and number (include cross-listings)	Units	Title	Course Description	Pre-requisites	Modes of delivery (online, in-person, hybrid)	Typically Offered (F, W, Sp, Su)	Dept signed party to proposal? (Yes/No)
NETV 477	3	Advanced Computer Forensics	CYBV 477 provides students with in depth is an advanced computer forensics course that provides students an in-depth knowledge of network forensics, network flow analysis, network intrusion detection systems, event reconstruction and memory forensics for Windows, Linux, and MacOS.	CYBV 381, CYBV 388, or the consent of the instructor	Online and in person	Fall and Spring	Proposed from dept. housing this course

New Courses Needed – using the table below, list any new courses that must be created for the proposed program. If the specific course number is undetermined, please provide level (ie CHEM 4**). Add rows as needed. Is a new prefix needed? If so, provide the subject description so Curricular Affairs can generate proposed prefix options.

CYBV 381, CYBV 382, CYBV 383, CYBV 384, and CYBV 386 are currently awaiting approval from the curriculum process.

Course prefix and number (include cross-listings)	Units	Title	Course Description	Pre-requisites	Modes of delivery (online, in-person, hybrid)	Typically Offered (F, W, Sp, Su)	Dept signed party to proposal? (Yes/No)
CYBV 381 (New)	3	From Incident Response to Digital Forensics	CYBV 381 provides students with the foundational knowledge of the Incident Response process leveraging the PICERL framework and NIST guidelines from the context of investigating incidents under the umbrella of Digital Forensics. Students will learn aspects of Incident Response, Forensics Fundamentals, Network Evidence Collection, Host and Network based evidence acquisition and analysis, and introduce Forensics Reporting, Malware Analysis, and Threat Intelligence.	None	Online and in person	Fall and Spring	Proposed from dept. housing this course

CYBV 382 (New)	3	Network Forensics	CYBV 382 provides students with in depth knowledge conducting a forensic investigation focusing on network attacks. This course will focus on core concepts of network forensics, coding, network forensic tools, and methodologies for conducting forensic investigations. Students will explore statistical flow analysis, network enumeration, tunneling and encryption and malware detection to support investigations.	None	Online and in person	Fall and Spring	Proposed from dept. housing this course
CYBV 383 (New)	3	Mobile Device Forensics	CYBV 383 provides students within depth knowledge conducting a forensic investigation focusing on mobile devices. It is estimated that over 50% of all network traffic is generated from mobile phones. These devices contain vital evidence for investigators including geolocation, connection data, contacts, and various pattern of life details. This course will focus on iOS and Android devices with a brief discussion on Windows devices. This course will teach students how to retrieve data effectively from the devices and the cloud using the latest techniques in mobile forensics.	CYBV 381, CYBV 388, or the consent of the instructor	Online and in person	Fall and Spring	Proposed from dept. housing this course

CYBV 384 (New)	3	Host and File System Forensics (Windows)	CYBV 384 provides students with in depth knowledge conducting a forensic investigation focusing on Windows Operating System (OS). It is estimated that approximately 80% of the desktop/laptop market share consists of Windows OS. It is critical for students to understand how Windows works and how to conduct a detailed investigation of this OS. During this course students will perform live analysis of Windows remotely and locally, understand how to and implement data acquisition, create timelines of system actions to identify how an incident occurred, and use various tools to recover and analyze data from file systems, the registry, and computer memory.	CYBV 381, CYBV 388, or the consent of the instructor	Online and in person	Fall and Spring	Proposed from dept. housing this course
CYBV 386 (New)	3	Enterprise and File System Forensics (Linux)	CYBV 386 provides students with in depth knowledge conducting a forensic investigation focusing on Linux. Students will gain a better understand of the internal operations of Linux and how to quickly and effectively conduct forensics investigations on Linux. Students will develop an understanding of forensics and incident response techniques and methodologies, conducting live analysis; creating, mounting, and analyzing images; conducting memory analysis, and understand advanced attack techniques.	CYBV 381, CYBV 388, or the consent of the instructor	Online and in person	Fall and Spring	Proposed from dept. housing this course

Faculty & Resources

Current Faculty - complete the table below. If UA Vitae link is not provided/available, attach a short CV (2-3 pages) to the end of the proposal or upload to the workflow form. UA Vitae profiles can be found in the UA directory/phonebook. Add rows as needed.

Delete the EXAMPLE rows before submitting/uploading. NOTE: full proposals are distributed campus-wide, posted on committee agendas and should be considered "publicly visible". Contact Martin Marquez if you have concerns about CV information being "publicly visible".

Paul Wagner, MS, MBA	Cyber Operations, Teaches CYBV 301, CYBV 326, CYBV 388, CYBV 480	
Troy Ward, MS	Cyber Operations, Teaches CYBV 326 and CYBV 388	
Kevin Smith, MS	Cyber Operations, Teaches NETV 477	
Tom Jewkes, MS	Cyber Operations, Teaches CYBV 301, CYBV 385, CYBV 400, and CYBV 435	
Steven Wood, Ph.D.	Cyber Operations, Teaches CYBV 388	
Jordan VanHoy, MS	Cyber Operations, Teaches CYBV 326, CYBV 301, CYBV 479, CYBV 498	

Additional Faculty – Describe the additional faculty needed during the next three years for the initiation of the program and list the anticipated schedule for addition of these faculty members.

Assistant Professor of Practice – Cyber Operations (Year 1)
Assistant Professor of Practice – Cyber Operations (Year 3)

Library Acquisitions Needed – Describe additional library acquisitions needed during the next three years for the successful initiation of the program.

None

Physical Facilities & Equipment - Assess the adequacy of existing physical facilities and equipment available for the proposed certificate. Include special classrooms, laboratories, physical equipment, computer facilities, etc. Describe additional physical

facilities and equipment that will be required or are anticipated during the next three years for the proposed program.

None

Other Support - Describe other support currently available for the proposed certificate. Include support staff, university and non-university assistance. List additional staff and other assistance needed for the next three years.

None

Marketing & Recruitment - Provide a detailed and robust marketing strategy for this certificate.

Undergraduate Major Fair
free, 30 students per year
Hack Arizona https://hackaz.io/
free, 30 students per year
GE courses in computer science across the campus – in class visits about the value of the undergrad certificate
free, 30 students per year
Advertising to Current Declared Majors in Cyber Operations (Currently 550 declared majors)
free, 50 students per year
Statewide Recruitment Activities
Transfer, military, and career fairs in Yuma County, Cochise County, Maricopa County, Pima County Community College classroom visits in Maricopa County Community College District, Cochise College, Arizona Western College, Pima Community College

Financial - Provide a copy of the budget for the certificate including start-up costs and the anticipated costs for the first three years. Include some indication of how this fits with the overall department budget.

Student Learning Outcomes and Assessment – describe what students should know, understand, and/or be able to do after completing this certificate, and how student outcomes will be assessed.

In completing the Certificate, students will

Understand the incident response process and how to create and deploy these capabilities.
Understand how to acquire and handle evidence for later analysis
Analyze data to determine the root cause of an incident and develop reports to inform management or to be used during civil or criminal proceedings
Evaluate incident response processes and integrate digital forensics techniques and procedures into the incident response process
Discover and analyze network traffic to support network forensic investigations
Analyze and interpret encrypted traffic
Understand and identify malware and information across the network wire
Evaluate, develop and use tool and custom scripts for network forensics automation
Correlate data collected from attacks and develop comprehensive reports to support management decision making and potentially legal proceedings
Discover new techniques in practical mobile forensics
Analyze the architecture and security mechanisms present in iO and Android platforms
Identify and analyze sensitive files on iOS and Android platforms
Extract and recover data from iOS and Android Platforms
Evaluate third-party application techniques and data recovery techniques
Correlate data collected from attacks and develop comprehensive reports to support management decision making and potentially legal proceedings
Perform live analysis on Windows systems locally and remotely
Demonstrate and understand acquisition techniques of volatile and non-volatile data
Extract and analyze system actions, file system data, registry, and computer memory
Analyze the architecture and security mechanisms present in WindowsOS
Correlate data collected from attacks and develop comprehensive reports to support management decision making and potentially legal proceedings
Perform live analysis on Linux systems locally and remotely
Demonstrate and understand acquisition techniques of volatile and non-volatile data
Extract and analyze digital artifacts to conduct a digital forensic investigation
Analyze the architecture and security mechanisms present in Linux
Evaluate and leverage open source tools and Python and Shell scripting to extract and analyze digital artifacts
Correlate data collected from attacks and develop comprehensive reports to support management decision making and potentially legal proceedings

Topics covered:

Incident Response Operations Planning and Execution
Operating System Fundamentals (Linux, Windows, Mobile Device (Android and iOS)
Conducting Digital Forensic Investigations
Conducting Mobile Device Forensics
Conducting Network Analysis and Forensic Investigations
Report Writing
Testifying in Court

Collecting Forensically sound evidence

Assessment Plan
Student Learning Outcomes will be assessed annually through
Conducting hands on exercises in all courses, conducting in-depth investigations, providing a comprehensive report covering investigation and analysis, and using multiple testing methodologies.

Certificate Outcomes and Assessment– identify factors that indicate that completion of the certificate enhances the undergraduate experience. Describe measures for programmatic assessment, and provide a detailed plan for assessing certificate outcomes.

Certificate Outcomes
Factors indicating that the Certificate leads to gainful employment and/or advancement include: Offers of employment to interns at their place of internship, employment at a desirable position (as articulated by the student) within one year of earning the certificate, promotion in professional setting within one year of earning the certificate, and long term satisfaction with working conditions (2, 5, and 10 years out from earning the certificate). Indication from annual surveys of our former students that the certificate was a factor in their employment success.

Assessment Plan
Certificate Outcomes will be assessed
Annually through an outgoing survey of Certificate Students regarding the above factors. Annually through a survey of employers as identified by those who earned the certificate.

Certificate Demand

Anticipated Enrollment and General Demand:

The Bureau of Labor Statistics expects that the computer forensic specialist career field can expect 28 percent annual growth from 2016 – 2026 with an expected 28,000 jobs to be added during that time period (https://www.forensicscolleges.com/careers/computer-forensics-examiner). This certificate will allow student to work with law enforcement or private forms.

This certificate program will target:

returning students already working in the field wanting to improve their skills and/or increase their eligibility for promotion,
students interested in augmenting their current degree program with this particular skill set (e.g., this is a great certificate to add to a major like Applied Computing or Cyber Operations).

Initially, we will target students in our own programs (e.g., BAS in Cyber Operations and BAS in Applied Computing and leverage corporate partnerships).

Year Projected Annual Enrollment:
1st Year, 30 students enrolled
2nd Year, 50 students enrolled
3rd Year, 85 students enrolled

General Demand

Students, generally, are living amid a massive shift in the amount of data we can save, use, analyze, and visualize – the Arizona region and students nationally thus need to be prepared for life and work in this data-driven economy where the breach of regulated and private data can result in loss of sensitive, regulated, and other data types:

Data breaches are at an all-time high. In the first half of 2019 the following occurred:
3,800 publicly disclosed breaches
4.1 billion records exposed

+54% increase in number of report breaches

Source: https://us.norton.com/internetsecurity-emerging-threats-2019-data-breaches.html

Needs Served by the Certificate

The growth in big data and the increased prevalence in cyber security incidents will require trained digital / computer forensics investigators to conduct incident response and digital investigations. As previously mentioned it is expected that the need for computer forensic analysts and information security analysts will grow by 28% from 2016 to 2026. Accordingly, many organizations require computer forensics investigators. Traditionally, digital forensic investigators were employed by local, state, and federal agencies to support criminal investigations. Currently these investigators can find work with accounting firms, law firms, banks, software development companies and a variety of other industries and organizations. Salary for students who choose to work for public or governmental agencies can expect to earn $50,000 per year with adjustments for locality pay. Salary from private organizations include a median salary of $98,350 per year with increased earning potential for experts in the field who testify or are called as expert witnesses.

Sources:
https://www.criminaljusticedegreeschools.com/criminal-justice-careers/computer-forensics-investigator/
https://www.thebalancecareers.com/digital-forensics-job-and-salary-information-974469

Related Positions:

Computer Forensics Investigator
Computer Forensics Technician
Information Security Analyst
Information Systems Security Analyst
Forensic Computer Analyst
Security Consultant
Certified Computer Forensics Examiner
Malware Analyst
Mobile Forensics Expert
Information Technology Auditor

Computer Crime Investigator
Crytanalyst
Disaster Recovery Expert
Incident Response Operations Specialist
Cryptograher

Local worksites for digital forensics students include:
Wells Fargo
IBM
Kforce Inc.
HuntSource
Arizona Department of Public Safety
Verizon
Leidos

Similar programs:

There are currently limited undergraduate certificates offered. Most are associated with criminal forensics investigations but don't focus on digital forensics.

Purdue University Global – Computer Forensics Postbaccalaureate Certificate https://go.purdueglobal.edu/infotech/certificates?adpos=&creative=398928901329&device=c&matchtype=b&network=g&source=SF55087&ve=62294&utm_source=Google&utm_medium=CPC&utm_campaign=pgo_sem_gsa_pros_inq_nb_it_prog_cert_mbr&utm_term=106559132-VQ2-g-VQ6-398928901329-VQ16-c-Target-kwd-19409225044&adid=&gclid=CjwKCAiAy9jyBRA6EiwAeclQhE09tEd09Mb6vI2H38_toySpB9mEsR0YyCWmOVeR0NvAS_afseZ8HRoCUYUQAvD_BwE&gclsrc=aw.ds

There are some BS degrees offered nationally

Champlain College Online – Computer Forensics & Digital Investigations https://onlinedegrees.champlain.edu/digital-forensics-bachelors-degree/?utm_campaign=OHO-BS_Computer_Forensics&gclid=CjwKCAiAy9jyBRA6EiwAeclQhAwjdvxQtzwfBBB6TnTn2jsa01vAAlzNAkFEprZ_SJFIAxkYS9arxBoCwK0QAvD_BwE

Embry Riddle – Cyber Intelligence and Security (Only two Digital Forensics courses as part of their degree) -

https://erau.edu/degrees/bachelor/cyber-intelligence-security

C. Collaborations
There will be no collaborations with other departments or universities for this certificate program other than donated courses toward this program if depts. choose to do so.

Contacts and Administration

List the name and contact information for the primary point of contact for the certificate.

Paul Wagner, Department Head, College of Applied Technology, paulewagner@email.arizona.edu

List the name and contact information for the person or persons who will serve in the role of Director of Undergraduate Studies (DUS) for the certificate. (This is not always the same as the DUS for affiliated programs or head of the managing academic unit.) Jason Denno, Director of Cyber Operations, jasondenno@email.arizona.edu

Total One-time	$	$	$
TOTAL EXPENDITURES	$	$	$
Net Projected Fiscal Effect	$57,240	$174.240	$260,730

Undergraduate Certificate Peer Comparison Chart- Select two peers for completing the comparison chart from (in order of priority) ABOR-approved institutions, AAU members, and/or other relevant institutions recognized in the field. The comparison chart will be used to identify typically required coursework, themes, and experiences for certificate programs within the discipline. The comparison programs are not required to have the same certificate name as the proposed UA program. Information for the proposed UA program must be consistent throughout the proposal documents. Delete EXAMPLE columns once ready to submit/upload.

Certificate name, institution	**Proposed UA Program:**	**Peer 1:**	**Peer 2:**
Current# of enrolled students			
Certificate program description	The 18-credit hour Digital Forensics Certificate will provide undergraduate students the confidence and training they need in incident response and various digital forensics including network forensics, mobile device forensics, host (Windows) and network (Linux) forensics and advanced memory forensics. The certificate will signal to employers that students have dedicated the time and energy necessary to develop the skills and confidence for tackling complicate digital forensics investigations for corporate, non-government and governmental organizations. The Certificate will service a diverse student population, training both 1) technically-minded students the nuances of classifying a situation of either an event or incident and then conduct the appropriate actions to ensure that forensically sound investigation is conducted. The Certificate will be designed and delivered to students from various backgrounds and expects students to have introductory / fundamental knowledge of computers and network fundamentals.	https://catalog.apus.edu/undergraduate/academic-programs/certificates/undergraduate-certificate-digital-forensics/#text The undergraduate certificate in Digital Forensics examines various forensics models to identify, preserve, collect, analyze, prepare, and present evidence for prosecuting cybercrime. The window of opportunity for collecting evidence can be a few seconds or minutes depending on the sophistication of the perpetrator, and this program teaches the precise digital forensic measures needed to respond to security incidents to prevent loss or corruption of sensitive proprietary information. This certificate program is intended for undergraduate students who seek to heighten their knowledge of digital forensics without committing to an academic degree program	https://www.temple.edu/academics/degree-programs/computer-security-and-digital-forensics-certificate-undergraduate-st-csdf-cert Study security measures that protect network systems and data with the Undergraduate Certificate in Computer Security and Digital Forensics from Temple's College of Science and Technology. As threats to security increase, so does the need for professionals with backgrounds in computer and information security. Students in this 10-credit-hour certificate program form a deeper knowledge of computer systems and digital forensics, broadening their career opportunities and professional goals. Courses focus on computer and information systems, the laws involved with information security and security breach investigations. Required course topics include criminal justice, an introduction to the laws in the criminal justice system and enforcement of these laws; digital forensics, focused on the cybercrime laws, information analysis and reporting, and investigation techniques; and network security, a thorough review of computer systems, email and web security.

Target careers	Computer Forensics Investigator Computer Forensics Technician Information Security Analyst Information Systems Security Analyst Forensic Computer Analyst Security Consultant Certified Computer Forensics Examiner Malware Analyst Mobile Forensics Expert Information Technology Auditor Computer Crime Investigator Crytanalyst Disaster Recovery Expert Incident Response Operations Specialist Cryptograher		
Minimum total units required	18	18	10
Minimum upper-division units required	18	18	10
Total transfer units that may apply to certificate	None	None	None
List any special requirements to declare/admission to this certificate (completion of specific coursework, minimum GPA, interview, application, etc.)	None	None	This certificate is appropriate for CIS majors1 or experienced industry professionals2 who are interested in focusing in the security area. Students can add this to their existing CS, IS&T or CS/Math major. At least two of these courses CANNOT count towards the electives for the major. In other words, you need to have two distinct courses for the certificate that are not counting towards any major elective courses; one of the electives can count for both. 1Matriculated students are primarily CIS majors due to prerequisites. 2Non-matriculated students must have 2+ years of experience in the IT sector working in systems and

			network administration and/or security domains. Requires instructor permission.
Certificate requirements. List all certificate requirements including core and electives. Courses listed must include course prefix, number, units, and title. Mark new coursework (New). Include any limits/restrictions needed (house number limit, etc.).	CYBV 381 From Incident Response to Digital Forensics (3) CYBV 382 Network Forensics (3) CYBV 383 Mobile Device Forensics (3) CYBV 384 Host and File System Forensics (Windows) (3) CYBV 386 Enterprise and File System Forensics (Linux) (3) NETV 477 Advanced Computer Forensics Investigations (3)	ISSC351 Computer Forensics (3) ISSC455 Digital Forensics: Investigation Procedures and Response (3) ISSC456 Digital Forensics: Investigation Wireless Networks and Devices (3) ISSC457 Digital Forensics: Investigation Network Intrusions and Cybercrime Security (3) ISSC458 Digital Forensics: Investigating Data and Image Files (3) ISSC459 Digital Forensics: Hard Disc and Operating Systems (3)	CIS3605 Introduction to Digital Forensics (3) CJ1001 introduction to Criminal Justice (3) OR CJ3007 Computer Crime (3) CIS4378 Computer and Network Security (4) OR CIS3319 Wireless Networks and Security (4)
Internship, practicum, applied course requirements (Yes/No). If yes, provide description.	None	None	None
Additional requirements (provide description)	None	None	None

*Note: comparison of additional relevant programs may be requested.

From: Wagner, Paul E - (paulewagner)
To: Henley, Esther M - (ehenley)
Subject: Fw: CAST Undergraduate Certificates
Date: Monday, April 6, 2020 11:31:55 AM

Paul E Wagner, MS, MBA

Department Head, Applied Technology
Assistant Professor of Practice
College of Applied Science & Technology
THE UNIVERSITY OF ARIZONA

A Building, 125
1140 Colombo Ave | Sierra Vista, AZ 85635
Office: 520-458-8278 | Cell: 513-255-0435
paulewagner@arizona.edu
https://azcast.arizona.edu/

From: Brooks, Catherine F - (cfbrooks) <cfbrooks@arizona.edu>
Sent: Friday, March 20, 2020 2:16 PM
To: Wagner, Paul E - (paulewagner) <paulewagner@arizona.edu>
Cc: Denno, Linda Lee - (ldenno) <ldenno@arizona.edu>
Subject: Re: CAST Undergraduate Certificates

Hi Paul, Hi Linda. We have no issue at all with your new certificates. I will some day follow up

about your great classes, our students might like to enroll in some of your cloud courses as part of their iSchool training, but that can be a different email thread.

You have my full support from the iSchool to move forward. This email might suffice, but if you need a formalized memo, I can do that also.

I hope the two of you have comfortable working conditions in your homes. Be well, Catherine

---

From: Wagner, Paul E - (paulewagner) <paulewagner@arizona.edu>
Sent: Friday, March 20, 2020 2:02 PM
To: Brooks, Catherine F - (cfbrooks) <cfbrooks@arizona.edu>
Cc: Denno, Linda Lee - (ldenno) <ldenno@arizona.edu>
Subject: CAST Undergraduate Certificates

Catherine,

I hope that things are going well for you given the new reality in which we find ourselves. I wanted to reach out to you in regards to two new undergraduate certificates that the College of Applied Science and Technology is going to submit through the curriculum process. I don't believe there are any conflicts but wanted to verify and get your support if possible.

The first is a digital forensics certificate that will tie to our Cyber Operations Program—specifically the Defense and Forensics emphasis. We currently have an introductory (CYBV 388) and advanced course (NETV 477). The certificate would be 18 credit hours and leverage NETV 477. The new courses would include:

From Incident Response (IR) to Digital Forensic
Enterprise and File System Forensics (Linux)
Host and File System Forensics (Windows)
Mobile Device Forensics
Network Forensics

The second certificate is Cloud Computing. This would tie into our Network Operations Program and support our $1.5 M grant that we have in support of Arizona Western College and our Applied Computing Program. We currently have two of the six classes in the catalog; NETV 379 (Cloud Computing) and NETV 479 (Advanced Cloud Computing). The additional courses would include:

Virtualization: Applications and Best Practices

Introduction to Microsoft Azure
Introduction to Amazon Web Services
Cloud Security: IR, Penetration Testing, and Advanced Defense

Both of these certificates would support multiple programs within our college and I believe would provide additional knowledge, skills, and abilities for students within some of your programs. All courses are 300/400 level courses and will be delivered online. The certificates will be developed to align with our current BAS programs and focus more on the application of the topics to ensure that students will have the knowledge and skills to be career ready in this relatively new and exciting discipline.

Please let me know if you have any questions or concerns.

Thank you for your time.

Paul E Wagner, MS, MBA
Department Head, Applied Technology
Assistant Professor of Practice
College of Applied Science & Technology
THE UNIVERSITY OF ARIZONA

A Building, 125
1140 Colombo Ave | Sierra Vista, AZ 85635
Office: 520-458-8278 | Cell: 513-255-0435
paulewagner@arizona.edu
https://azcast.arizona.edu/