

Steve Simpson**S2 Forensics, LLC**

4810 Pt. Fosdick Dr. NW #154

Gig Harbor, WA 98335-1711

Email: steve@s2forensics.com

Web: www.s2forensics.com

Steve Simpson CCE, CISSP, CPTC, CSFA, PMP is a Cyber Security, computer, and data networking technology professional with demonstrated experience in Digital Forensics, Vulnerability Assessments, Penetration Testing, Data Recovery, PCI-DSS compliance, Information Security Compliance, Technical Project Management, IT Governance, Information Security Risk Analysis, Computer Engineering, and post-secondary info-security course development and instruction.

Professional Experience:**Senior Forensic Analyst/Director of Technology**

2013 - Present

S2 Forensics, LLC

Fox Island, WA

Consultant providing digital forensics services, expert witness services, industry security compliance, network administration, and data recovery to various clients on an as needed basis.

- Criminal defense support and expert witness services including consulting, analysis of computer and cell phone forensic data, documenting the relevance of digital forensic data to criminal charges, courtroom testimony.
- Android and iOS smart phone image acquisition and forensic analysis in support of in support of criminal and civil legal cases.
- Linux and Windows operating system hard drive image acquisition and data analysis using a variety of open source and proprietary tools.
- Data recovery from crashed/failing hard drives, mobile devices, USB drives, and SSD drives.
- Project Manager directing an IT Assessment of various corporate network infrastructures, scalability and performance, storage, disaster recovery, and information security.
- Created, document, implement, and administer corporate security programs meeting PCIDSS, level C and level D requirements, while preserving the integrity of existing vendor processes and procedures.
- Conduct internal/external network vulnerability scans and penetration tests in support of PCI-DSS level C and level D compliance. Identify and mitigate compliance deficiencies insuring on-going PCI compliance.

Adjunct Instructor - Cybersecurity, Digital Forensics

2015 – Present

Highline College

Des Moines, WA

Developed and delivered hybrid classes in digital forensics including:

- Network Forensics – A detailed analysis of network data communication using Transmission Control Protocol/Internet Protocol (TCP/IP) protocols, deep packet analysis, covert network communication methodologies, and malware analysis.
- Penetration Testing – Instruction and theory of operations covering various attack and defense techniques targeting Open Systems Interconnect (OSI) layer 2, 3, and 4 vulnerabilities.
- Mobile Forensics – The use of tools and methodologies required for the logical and physical data extraction from iOS and Android-based mobile devices, the analysis of the device data using forensics and court-approved methodologies, and the reporting of the findings.
- Mobile Security - The benefits and risks of various corporate mobile device security policies.
- Network Scripting – Instruction in basic software algorithms and the use of Linux bash scripting.
- Operating System and Hardware Fundamentals - course teaching students the identification of computer system devices and the interaction of operating system software and computer hardware.

Professor Networking and Cybersecurity

2015 - 2019

Tacoma Community College

Tacoma, WA

Develop and deliver education courses in cybersecurity subjects including

- Linux Administration – Developed a hands-on class teaching the Linux command line, Linux system administration, Linux network administration, and bash scripting.
- Client/Server Technologies – Instructing the concepts of data communication in a Local Area Network (LAN) environment including common methods and protocols of the OSI Communication Model.
- Local Area Network (LAN) Administration – Installation, secure configuration, maintenance, and administration of Microsoft software including Windows Server 2008r2, Windows Server 2012R2, and Windows Server 2016.
- Incident Response – Network monitoring and defense techniques for enterprise networks including attack methods, intrusion analysis and detection.
- Security Assessment - The study of information network security assessments along with and risk and remediation options for securing data networks.
- Information Technology Project Management – The study and techniques used to manage Information Technology (IT) based projects.

Adjunct Professor – Digital Forensics

2016

American Public University

Charles Town, WV

- Computer Forensics – Legal and industry processes for the collection and analysis of hard drive images, chain of custody, email tracking, internet browser history, and incident timeline analysis.

Information Security Project Manager

2012 – 2013

Boeing - Contract position

Bellevue, WA

Project management and technical resource services for Boeing's Information Security division supporting information access control, federation, and network security architecture.

- Reviewed vendor proposals, evaluated vendor software capabilities, completed a gap analysis comparing product capabilities with project requirements.
- Defined and developed test cases for Proof of Concept testing of 3rd party software to be used for enterprise-wide information security policy distribution and management.
- Project Manager for an enterprise-wide upgrade of Federation server architecture involving server hardware, operating system (OS) and software upgrades. Provided back-up system admin support for software configuration during the deployment phases of the server architecture upgrade.
- Developed a business requirements document for 2-factor authentication project using Short Message Service (SMS) and One Time Passwords (OTP) as authentication methods.

Information Security Project Manager

2012

Microsoft - Contract position

Redmond, WA

Project Manager working the annual review of the On-line Services Security Compliance (OSSC) group security standards.

- Project Manager for the review Microsoft Security Standards documents in preparation for a scheduled Federal Information Security Management Act (FISMA) audit.
- Tracked stakeholder content changes to the Security Standards documents, developed new content as required, and performed the final edits prior to publishing the revised Security Standards.
- Tracked and published project performance metrics providing the stakeholders with project status indicators on a scheduled basis.

Information Security Analyst Intern

2011 to 2012

City of Seattle

Seattle, WA

Provided information security governance and tactical support to the Department of Finance and Administrative Services through interdepartmental risk analysis, PCI-DSS compliance reviews, and the development of information forensics processes. Specific accomplishments included:

- Conducted security risk assessments by interviewing department heads, compiling the findings, and developing department-level recommendations based on risk assessment analysis.
- Developed and documented digital security incident response processes targeting the capture and analysis of live memory images using Volatility 2.0.
- Identified and collected citywide and departmental artifacts in support of PCI-DSS SAQ-D compliance.
- Developed a forensic analysis lab using state-of-the-art data forensics and incident response investigation tools. Documented the procedures and methodologies supporting the effective use of the laboratory tools for image creation, file carving, basic registry analysis,

and internet history of live and post-mortem system in both a Linux and Windows environment.

Information Security Officer Intern

2011

Regis University

Denver, CO

Penetration test team Lead providing direction, training, and mentoring to junior team members during the vulnerability assessment and penetration testing of development and production networks. Developed and documented vulnerability assessment and penetration test processes based on NIST and ISECOM guidelines and methodologies.

- Technical Lead for White Box internal and external penetration testing of defined networks. Negotiated project scope, deliverables, methodologies, tracking, reporting, and schedule with the appropriate stakeholders. Documented all negotiated agreements by publishing a project test plan and followed the published plan through to project completion.
- Directed a team of subordinate testers through a network vulnerability assessment and penetration test providing needed training to junior team members.
- Collated and presented test results to the project stakeholders highlighting possible network, successful exploitations, network vulnerabilities, the discovery of network connected devices, and the possibility of unauthorized network usage.
- Provided weekly project status updates to project stakeholders including network scan findings, assessment results, project performance to schedule, and test results.
- Conducted pre and post-hardening penetration test targeting a Citrix virtual network environment and comparing the effectiveness of various network security measures.

System Hardware Design Manager/Technical Program Manager

1996 - 2006

Intel Corporation

DuPont, WA

Technical leader for the design of computer systems leading numerous product design, development, and manufacturing efforts. Managed a globally distributed engineering design and services team specializing in product development, circuit design, new product introduction (NPI), system hardware validation, outsource manufacturing, and outsource design.

Developed/approved product designs, design specifications, product requirements, product configuration matrixes, test plans and Service Level Agreements, Design for Test (DTF), and Design for Manufacturing (DFM) initiatives.

- Engineering manager chartered with the qualification of third-party hardware in support of Intel's microprocessor, chipset, and motherboard roadmaps.
- Developed and deployed component qualification and test process driving the installation of component qualification/test capabilities at two Asian sites doubling test capabilities while simultaneously reducing domestic engineering and management head count.
- Managed the technology relationship between numerous Asian Original Design & Manufacturing (ODM) partners providing direction regarding product, components, and peripheral design as well as engineering support and resolution of product manufacturing and test issues.

- Developed the requirements and specifications for a continuous product qualification test located in an Intel facility in China. Managed the implementation and process refinement by directing domestic and international engineering resources in the US and China.

Education:

Master of Science Systems Engineering - MSSE 2012
Regis University, Denver CO.

Bachelor of Science Electronic Engineering Technology - BSEET 1986
Oregon Institute of Technology, Portland, OR.

Digital Forensics Certificate, Edmonds Community College 2014
Edmonds Community College, Lynnwood, WA.

Expert Witness and Case Experience:

State of Washington vs. Mondragon August 2019
Providing litigation and technical support to the defense in a Net Nanny case.

State of Washington vs. Cory Whipple July 2019
Defendant charged with downloading and viewing child pornography on a public computer.

State of Washington vs. Keith Rawlins July 2019
Defendant charged with drive by shooting. Case analysis included evaluation of cell tower and geo-location data.

State of Washington vs. Mehmet Bilgi June 2019
Defendant charged in a Net Nanny case. A Declaration was written in support of the defense motion challenging the State's use of a specific software program and its application with regards to the Washington State Privacy Act.

State of Washington vs. Robert Westby April 2019
Defendant charged with violating a no contact order using Facebook. Case analysis included evaluation of defendant's Facebook account and providing a Computer Forensic Investigation report.

State of Washington vs. Dalton Iverson February 2019
Defendant charged with rape. Case analysis included cell phone acquisition and the time-line analysis of phone logs, text messages, and photo metadata.

State of Washington vs. Michael Schluetz

January 2019

Defendant charged in a "Net Nanny" case with Attempted Rape of a Child and Communication with a Minor for Immoral Purposes. Case work included review of discovery material including cell phone acquisition analysis, submission of a written narrative discussing Internet Protocol (IP) addresses and emails pertaining to the case and providing the defense attorney with a series of questions pertinent to the cross-examination of the prosecution's witnesses.

State of Washington vs. Kacey Stelzig

May 2018

Defendant charged with domestic violence and violating a No Contact Order. Provided consultation and an analysis of evidence extracted from the defendant's cell phone. Forensic analysis report submitted to the defendant's attorney.

Commonwealth of Pennsylvania vs. Weiwu Zhao

October 2017

Defend charge with Sexual Abuse of Children – The possession and distribution of Child Pornography. Provided an expert witness report and court testimony for the defense of the accused.

State of Washington vs. Hilary Menting

September 2017

Defendant charged with violating a No Contact Order. Provided consultation to the defense team regarding the hacking of an online email account. Testimony and additional work on the case is currently pending.

State of Washington vs. Daniel E. Christensen

November 2016

Defendant charged with Possession Depiction of Minors in sexually explicit conduct (2x). Provided a written report based on the interpretation of evidence to the criminal defense Legal team.

State of Washington vs. Michael Dement

July 2016

Defendant charged with multiple counts of Identification Theft. Reviewed charges and evidence resulting from the forensic analysis of multiple hard drives and smartphones. Provided consultation services to the defendant's legal team on forensic extraction and analysis methods.

State of Washington vs. John Ragland

July 2015

Defendant charged with violating a No Contact Order. Subpoenaed as an Expert Witness to provide testimony regarding the meaning of spoofing and the possible techniques that support the spoofing of telephone numbers.

State of Washington vs. Tyler Smith

December 2014

Defendant charged with rape. Extracted phone data, analyzed data, provided a timeline, and submitted a report to the criminal defense legal team.

Professional Certifications:

Certified Computer Examiner (CCE) International Society of Forensic Computer Examiners (ISFCE)	2014 – Present
Certified Penetration Test Consultant (CPTC) Mile 2 Certifications	2015 - Present
Cyber Security Forensic Analyst (CSFA) Cybersecurity Institute	2015 – Present
Certified Information Systems Security Professional (CISSP) International Information Systems Security Certification Consortium ((ISC) ²)	2013 – Present
Project Management Professional (PMP) Project Management Institute (PMI)	2009 – Present

Specialized Training

Linux Foundation Cert Prep: Network Security Lynda.com, .75 hours	2019
Linux Foundation Cert Prep: Remote Access Lynda.com, .5 hours	2019
Learning SSH Lynda.com, .75 hours	2019
Learning Ubuntu Server Lynda.com, 1.5 hours	2019
Building an Ubuntu Home Server Lynda.com, 2 hours	2018
Placing the Suspect Behind the Keyboard Digital Forensics & Incident Response Training, 12 hours	2017
Physical and Cybersecurity for Critical Infrastructure Texas Engineering Extension Service (TEEX), Texas A&M University System, 10 hours	2016

Law 101: Legal Guide for the Forensic Expert National Institute for Justice, 13 hours	2014
Windows Forensic Environment http://courses.dfironlinetraining.com/windows-forensic-environment , 8 hours	2014
Cyber Law and White-Collar Crime Texas Engineering Extension Service (TEEX), Texas A&M University System, 10 hours	2013
Advanced Data Recovery Edmonds Community College, 30 hours	2013
Digital Forensics and Law Edmonds Community College, 45 hours	2013
Network Forensics Regis University, 40 hours	2011
Computer Forensics Regis University, 40 hours	2010

Conferences

Defending and Investigating Complex Crimes Washington Defender Association/Innocence Project Northwest, 14 hours	Sept 2018
IT Futures Summit: 2017 Mercer Island, WA, 8 hours	May 2018
IT Futures Summit: 2017 Mercer Island, WA, 12 hours	May 2017
CISSE 2017, Colloquium for Information Systems Security Education Las Vegas, NV, 20 hours	June 2017

Industry Presentations

Cell Phone Extractions for Attorneys & Investigators: Pulling the Veil off the State's Discovery Washington Defender Association/Innocence Project Northwest Defending and Investigating Complex Crimes University of Washington, Seattle, WA	Sept 2018
--	-----------

Digital Forensic Basics
(ISC)2 Tacoma, Washington Chapter Meeting
Tacoma, WA.

Oct 2016

Course Instructor/Professor:

IT281 Cyber Security Capstone
Professor – Tacoma Community College
Winter 2017, Winter 2018

Course Description:

This is a capstone course for the Network Administration and Support degree program Cybersecurity option. The students use skills and knowledge learned in previous coursework to implement robust security solutions for enterprise networks.

IT280 Advanced Networking Technologies
Professor – Tacoma Community College
Winter 2017, Winter 2018

Course Description:

This is a capstone course for the Networking and Convergent Technologies program. The students will demonstrate a complete foundation skill set based on the knowledge and skills acquired through previous coursework to implement a complete and secure network through project management, business analysis, budget development, presentation, and technical knowledge and skills.

IT278 Incident Response
Professor – Tacoma Community College
Winter 2017, Winter 2018, Summer 2018, Winter 2019

Course Description:

This course presents network defense in depth for enterprise networks, attack methods, intrusion analysis and detection. The students learn how to install and configure a Network Security Monitor (NSM) system and how to use various stand-alone tools to probe and assess network and network service configurations.

IT275 Security Assessment
Professor – Tacoma Community College
Fall 2016, Fall 2017, Fall 2018

Course Description:

The study of Information Network Security with added emphasis on security assessment, risks and remediation options for securing networks. Emphasis is placed on the understanding of how physical security impacts network and data security as well as the utilization of various frameworks used for Security Risk Assessments.

IT270 Services and Support Fundamentals

Professor – Tacoma Community College

Fall 2017

Course Description:

An introduction to the methodologies and tools for personal computer and Local Area Network (LAN) troubleshooting from a proactive viewpoint. The student studies the methods to identify and repair the most likely causes of network faults caused by user, hardware, and software problems. Disaster Plans, including a Backup Plan, are developed. Quality customer service, journaling and documentation are emphasized. Configuration management and patch/ service release installation is learned. Server performance monitoring is discussed.

IT262 Technical Support of Networks

Professor – Tacoma Community College

Fall 2016, Fall 2017, Fall 2018

Course Description:

An introduction to advanced network server configuration requirements and the theoretical and practical aspects of network architectures. The student focuses on advanced server configuration aspects of network enterprise storage as well as web, file, application, and print services. Methods and tools for designing, implementing, and maintaining a secure and expandable enterprise network environment are studied.

IT260 Client/Server Technology – Local Area Network

Professor - Tacoma Community College

Spring 2016, Spring 2017, Summer 2017, Spring 2018, Winter 2019

Course Description - This course introduces the student to the concepts of data communication in a Local Area Network (LAN) environment. It includes training in the methods and protocols used to allow networked computer systems to communicate in local environments. Topics include the OSI Communication Model, transmission media, protocol stacks especially TCP/IP, simple internetworking, and LAN services. Course objectives are based on those of the Network + and the retired Microsoft Network Essentials certification exams.

IT261 Administration of Networks

Professor - Tacoma Community College

Spring 2016, Spring 2017, Spring 2018, Winter 2019

Course Description

The student is introduced to networking and to a detailed study of network administration techniques. This is an applied course in the concepts of local area networks (LANs). The student focuses on configuration of file and print services. Methods and tools for designing, implementing, and maintaining a secure and expandable local area network environment are studied.

IT247 IT Project Management

Professor - Tacoma Community College

Spring 2017, Summer 2017, Winter 2018, Spring 2018, Summer 2018

Course Description

Project Management for IT professionals and projects from a team member perspective. Students will learn the different tools and techniques used in initiating, planning, developing, documenting and completing an IT project. Based on the Project Management Institute's methodologies.

IT211 Operating Systems III - Linux

Professor - Tacoma Community College

Fall 2018

Course Description

Course work providing hands-on experience in the installation, configuration and administration of the Linux operating system in a networked environment working from the command line. Instruction includes the installation and configuration of a Linux-based server complete with file storage, firewalls, virtual private networking (VPN), remote administration, and other configuration options per the administrator's choice.

ISSC351 Computer Forensics

Professor – American Public University

Spring 2016, Summer 2016

The examination of theory, best practices, and methodologies to conduct computer forensics investigations; it includes the ethical issues, data presentation, and chain-of-evidence procedures. It also appraises current tools and technologies to analyze, acquire, and organize digital evidence.

CIS 460 Pen Testing II

Instructor - Highline College

Spring 2016, Spring 2017

Course Description:

This course is the capstone course for the BAS in Cybersecurity and Forensics and the second in the Pen Testing certificate. Students will plan, design and create a pen testing lab. Then they will apply the techniques used on "ripped from the headlines" case scenarios. The environments will include Windows and Linux operating systems, DBMS, Hadoop, cloud servers, mobile devices, sensitive data and other topics covered in the prior courses. Students will be expected to demonstrate their processes, report on and explain the effectiveness of same.

CIS 450 Pen Testing I

Instructor - Highline College

Winter 2016

Course Description

This course is Penetration Testing I. Students begin by reviewing the five fundamentals: information gathering, scanning, enumeration, exploitation and reporting. They will examine actual exploitation techniques and the business practices needed to prevent the same. The course focuses on the penetration testing of large network infrastructures with layer 2 and layer 3 attacks. Students will use basic and advanced tools to examine packets and network traffic. Students will be exposed to service provider level attacks – including VPN and SSL attacks -- and learn how to detect/defend against them. Students are introduced to creating a pen testing lab. Upon completing the course, students can sit for the Mile2.com Pen Testing Consultant certification exam.

CIS 370 – Network Forensics

Instructor - Highline College

Winter 2015, Winter 2016, Winter 2017, Summer 2017, Fall 2017, Winter 2018, Winter 2019

Course Description

This course focuses on tracking down network intruders or at least ascertaining how they got in and what they did. Intruders can be internal or external attackers. When, what, where, and how they were able to gain access gives a network administrator clues to design flaws in the network architecture and shortcomings in policies or procedures. An introduction to investigations in the cloud is included along with the legal aspects of network investigations. This is a hands-on class in which students test network forensics tools and how to use them in internal or external investigations.

CIS 221 Network Scripting

Instructor - Highline College

Spring 2015, Summer 2015

Course Description:

Provides in-depth view of current and future mainstream features of practical network scripting. Emphasis is place on the issues of multiplatform networks, including the challenges and items that must be maintained on a regular basis. Also includes an introduction to basic scripting methods, standard algorithms and popular programs such as Perl. The two primary platforms will be UNIX/Linux and Windows. Security issues, server load balancing and cloud servers will also be addressed.

CIS 360 Mobile Forensics

Instructor - Highline College Spring
2015

Course Description:

Students will learn the issues of forensics pertinent to mobile and wireless. This includes devices such as cell phones, palmtops, smart phones, iPhones, iPads, digital cameras, pagers, etc. Students will be exposed to commercial and shareware applications that can be used.

CIS 430 Mobile Security

Instructor - Highline College

Spring 2015

Course Description

This course focuses on what is involved when wireless and mobile devices are incorporated on a network. BYOD (Bring Your Own Device) is extremely popular in the 21st century. Both employees and visitors attach a variety of devices to a network – with such broad access, how does one protect the crucial elements of the network? In the case of a hospital, how does this workplace allow emergency medical equipment and visitors onto the wireless? Students will perform mobile app vulnerability assessments and learn how to protect mobile networks.

CIS 150 – OS and Hardware Fundamentals

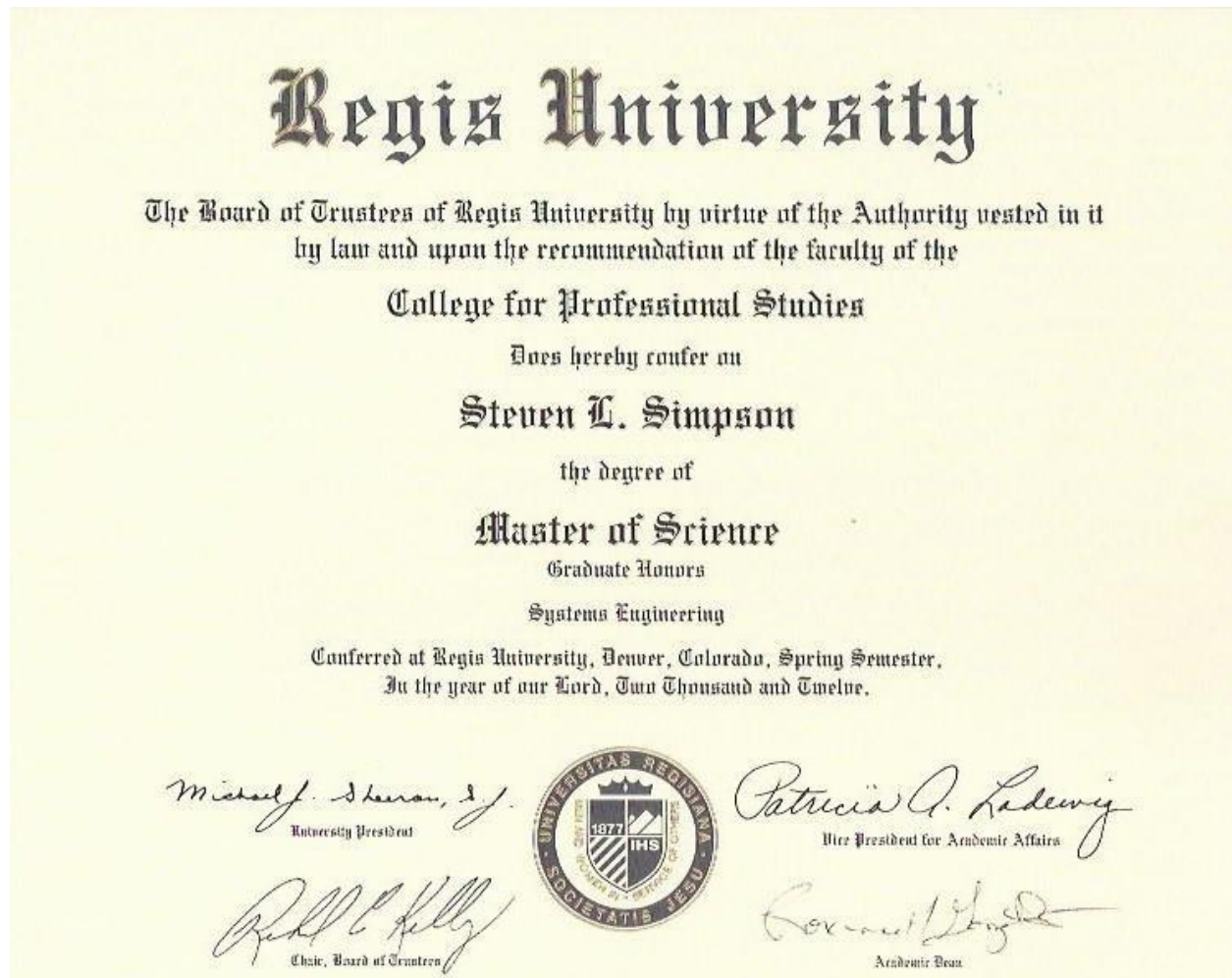
Instructor - Highline College

Winter 2015

Course Description

The course serves as a foundation course for CIS network and data recovery/forensics programs. This course develops operational literacy in the microcomputer hardware and software environment, including laboratory experience disassembling, assembling, troubleshooting, installing, configuring and using microcomputers and peripheral equipment.

Diplomas:

**Master of Science in Systems Engineering (MSSE)**

2012

Graduate with Honors

Regis University

College of Computer & Information Sciences

Regis University's Master of Science in Enterprise Systems Engineering program is designed to provide students with the foundational, managerial and technical skills and knowledge to design, integrate, protect and maintain sophisticated information systems within the organization's enterprise data systems.

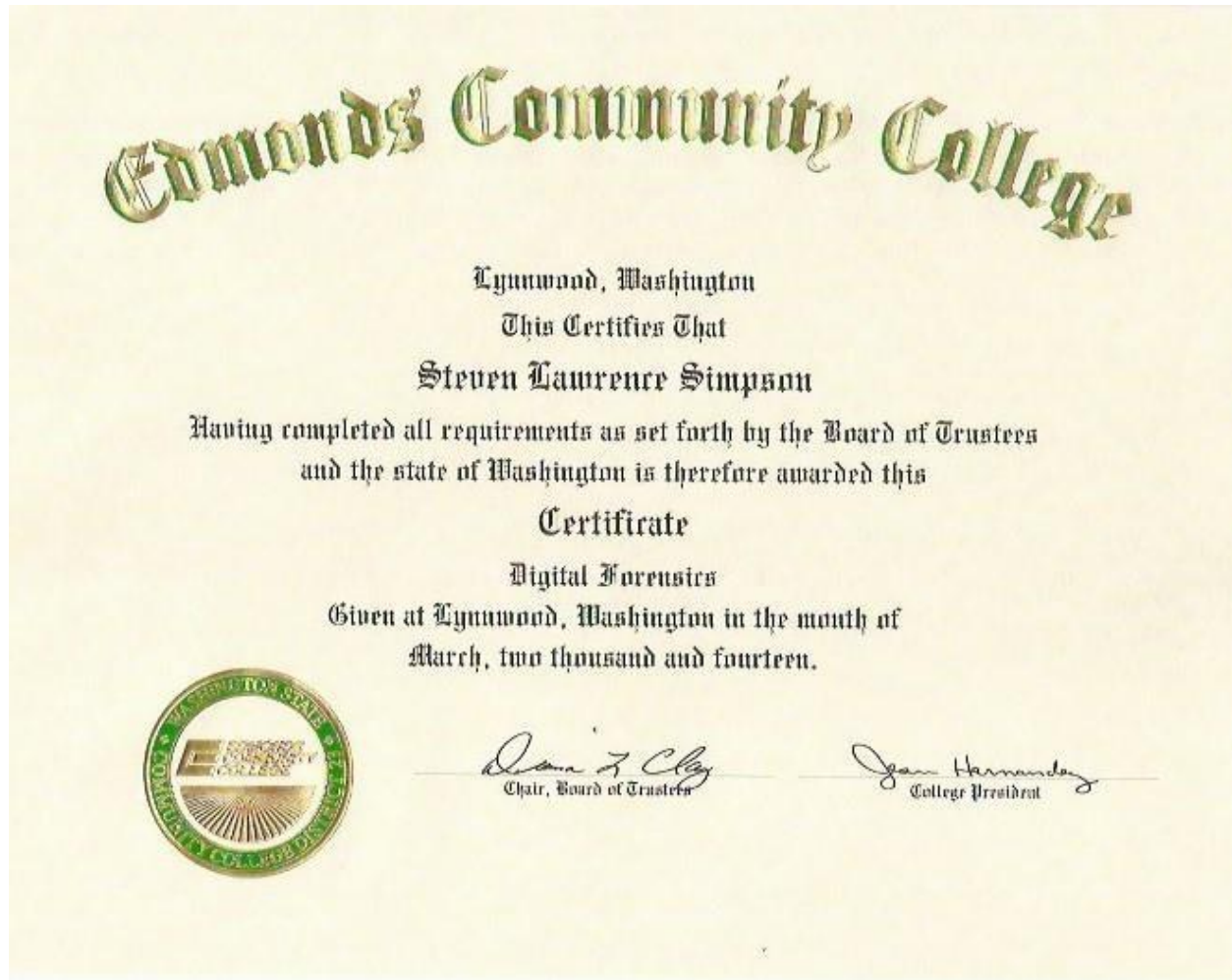


Bachelor of Science Electronics Engineering Technology (BSEET)

1986

Oregon Institute of Technology

The Oregon Institute of Technology Electronics Engineering Technology degree is a focus on the theory, concepts, and practice of applied electronics engineering.



Digital Forensics Certificate

2014

Edmonds Community College

Information Security and Digital Forensics

Digital forensics (a.k.a. computer forensics) is an emerging discipline that focuses on the acquisition, recovery, documentation, and analysis of information contained within and created with computer systems and computing devices - typically in the interest of figuring out what happened, when it happened, how it happened, and who was involved. All evidence must be treated in a way that ensures the admissibility in a court of law or other legal/administrative proceeding, and the forensic analyst must have the skills to document and present evidence in an intelligible manner, understandable to the layperson.

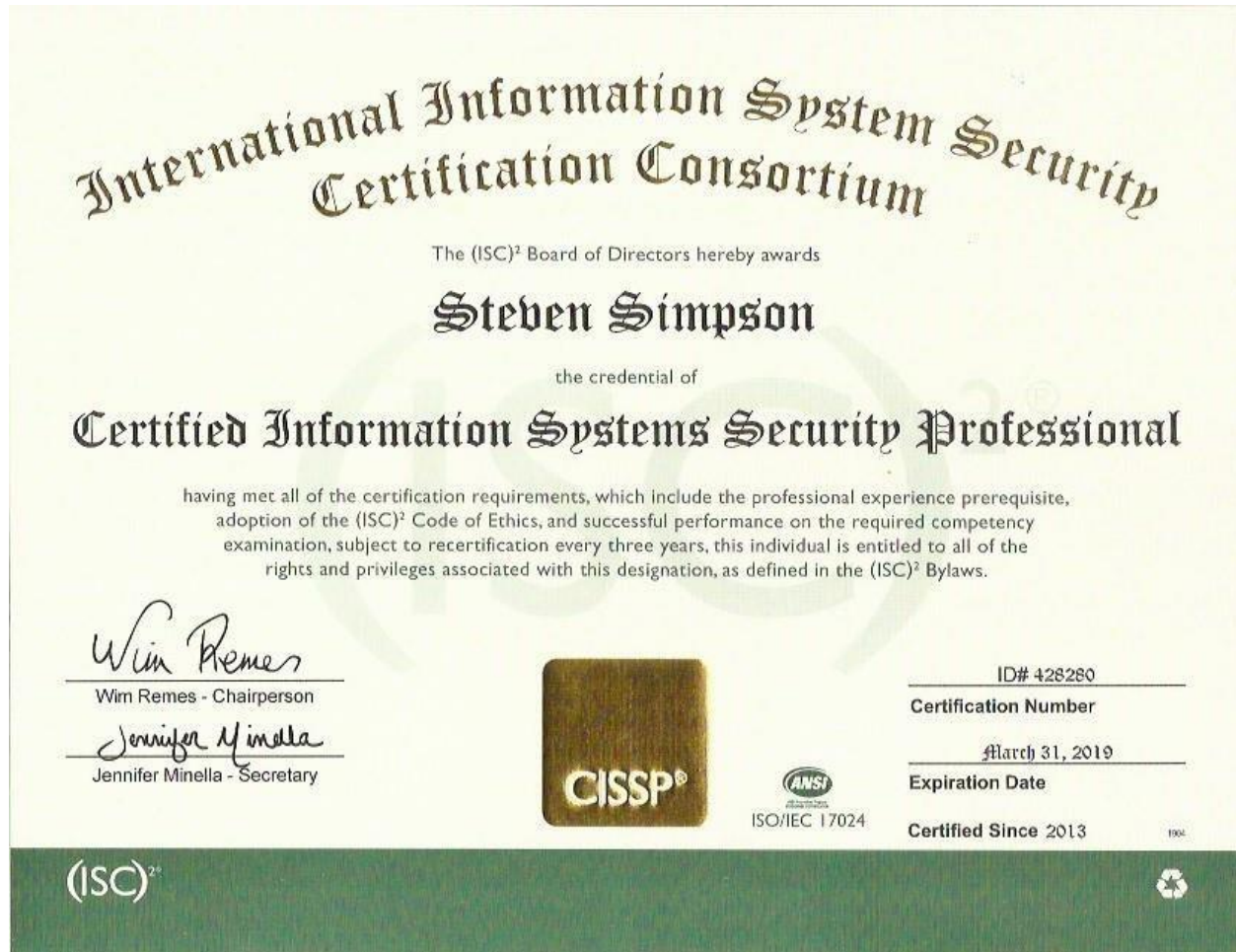
Professional Certifications:**Certified Computer Examiner (CCE)**

2014

The International Society of Forensic Computer Examiners® (ISFCE)

The purpose of the Certified Computer Examiner (CCE)® certification is to:

- Professionalize and further the field and science of computer forensics
- Provide a fair, vendor neutral, uncompromised process for certifying the competency of forensic computer examiners
- Certify computer forensic examiners solely based on their knowledge and practical examination skills and abilities as they relate to the practice of digital forensics.
- Set high forensic and ethical standards for forensic computer examiners
- Provide a universally recognized, unblemished certification that is available to all who can qualify, for a reasonable cost

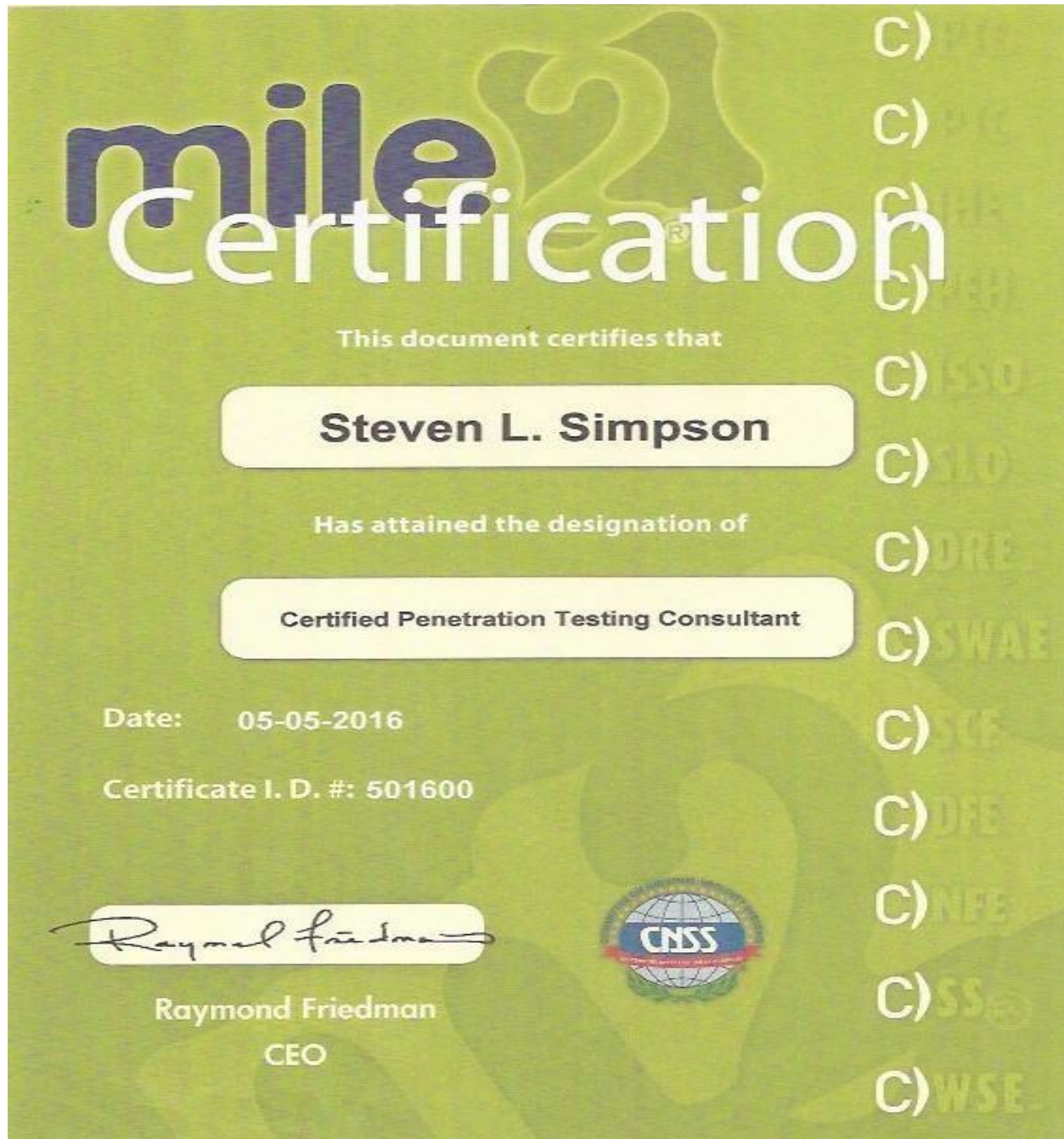
**Certified Information Systems Security Professional (CISSP)**

2013

International Information Systems Security Certification Consortium ((ISC)²)

The vendor-neutral CISSP certification is the ideal credential for those with proven deep technical and managerial competence, skills, experience, and credibility to design, engineer, implement, and manage their overall information security program to protect organizations from growing sophisticated attacks.

Backed by (ISC)², the globally recognized, not-for-profit organization dedicated to advancing the information security field, the CISSP was the first credential in the field of information security to meet the stringent requirements of ISO/IEC Standard 17024. Not only is the CISSP an objective measure of excellence, but also a globally recognized standard of achievement.



Certified Penetration Testing Consultant (CPTC)

2016

Mile 2 Certification

The vendor neutral Certified Penetration Testing Consultant course is designed for IT Security Professionals and IT Network Administrators who are interested in conducting Penetration tests against large network infrastructures similar to large corporate networks, Services Providers and Telecommunication Companies.

**Project Management Professional (PMP)**

2009

Project Management Institute (PMI)

Project Management Professional (PMP) is an internationally recognized professional designation offered by the Project Management Institute (PMI). Government, commercial and other organizations employ PMP certified [project managers](#) in an attempt to improve and evolving set of project management the success rate of projects in all areas of knowledge, by applying standardized principles as contained in PMI's PMBOK Guide.

Continuing Education Completion Certificates:



First of a series of trainings used for network and server configuration of Linux based devices. This training focused on Network Security using the Ubuntu Server distribution.

Certificate of Completion

Steve Simpson

Linux Foundation Cert Prep: Remote Access (Ubuntu)

Updated: 11/2018 • Completed: 02/2019 • 34m 21s

Certificate No: 3C79DF94ECA0451DBA422749D3CD6401



Lynda.com
FROM LINKEDIN

Training focused on remote access to Linux based server.

Certificate of Completion

Steve Simpson

Learning Ubuntu Server

Updated: 11/2018 • Completed: 02/2019 • 1h 29m

Certificate No: DBBA452B0261499FBF4EE9250F5B74CD



Lynda.com[®]
FROM LINKEDIN

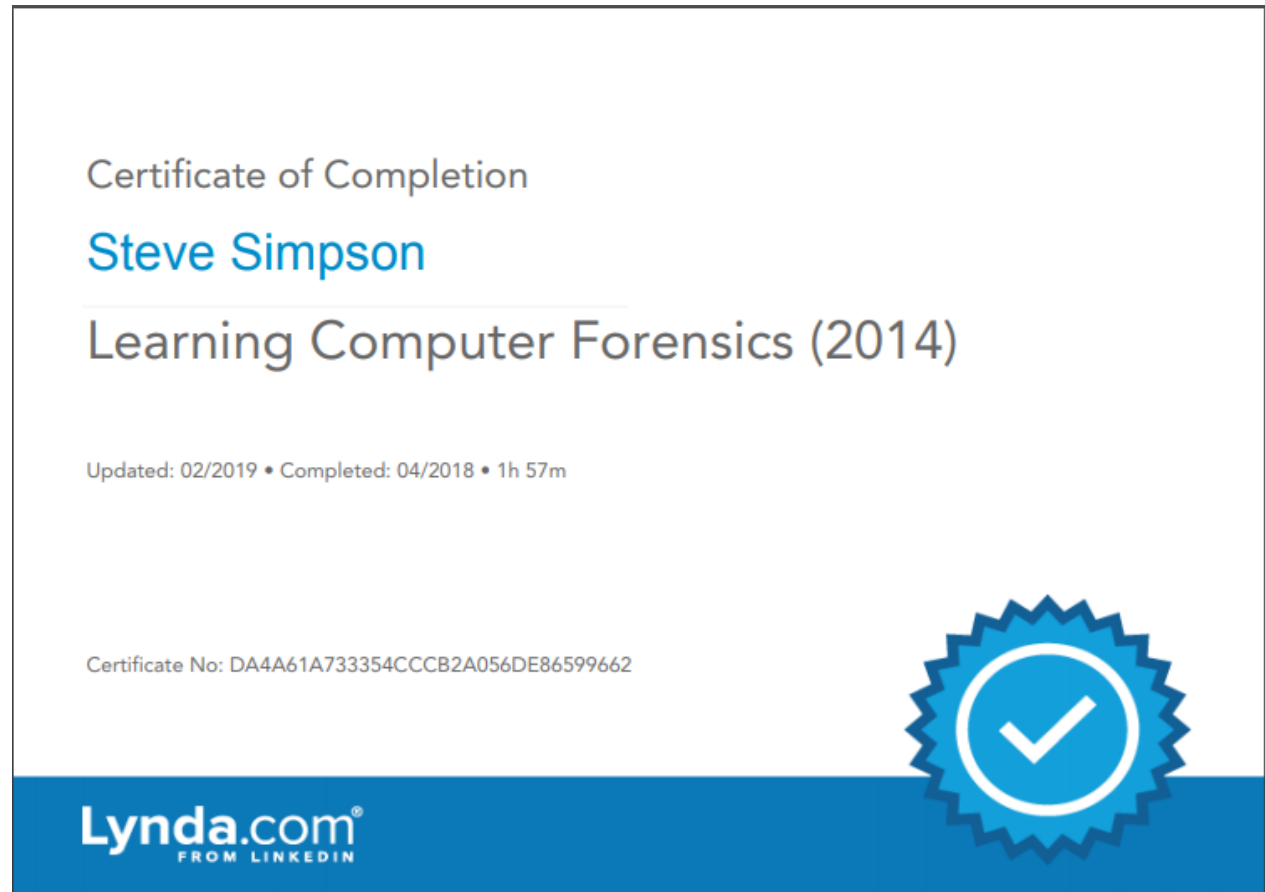
Training covering the fundamentals of Linux server configuration and the configuration of a Ubuntu server.



Online course covering the theory and use of the ssh protocol.



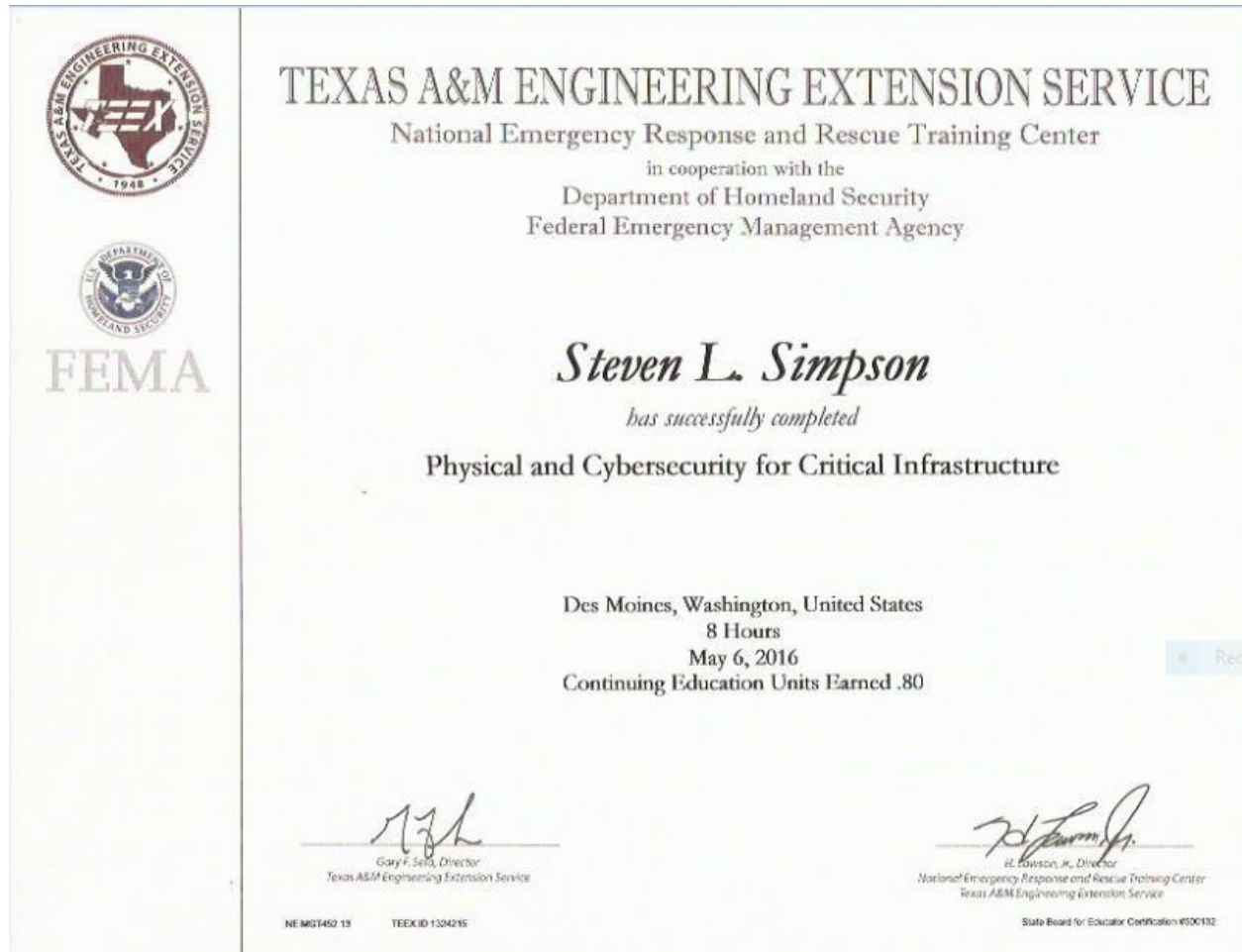
Online course in the download, installation, configuration and use of a Linux server software.



Online course in Computer Forensics completed as a refresher course.



Training including investigation of a cybercrime using digital forensics techniques as well as physical investigative procedures. Links traditional investigative techniques with high tech crime analysis in a manner that not only determines elements of crimes, but also places the suspect at the keyboard.



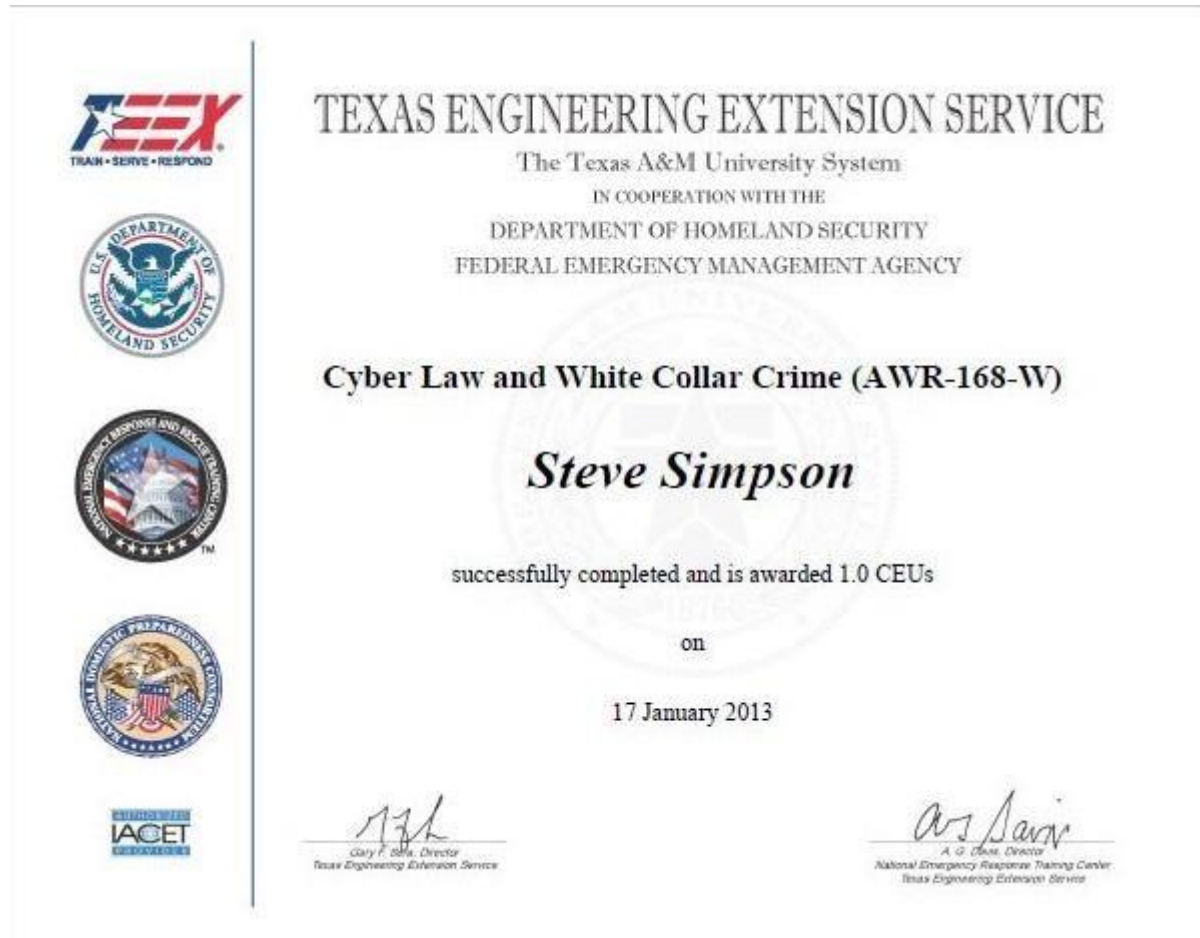
Identification of physical and cybersecurity concerns impacting overall infrastructure security posture, examine integrated physical and cybersecurity incidents and the evolving risks and impacts they pose to critical infrastructure, and explore resources that can be applied to improve security within an organization, business, or government entity.



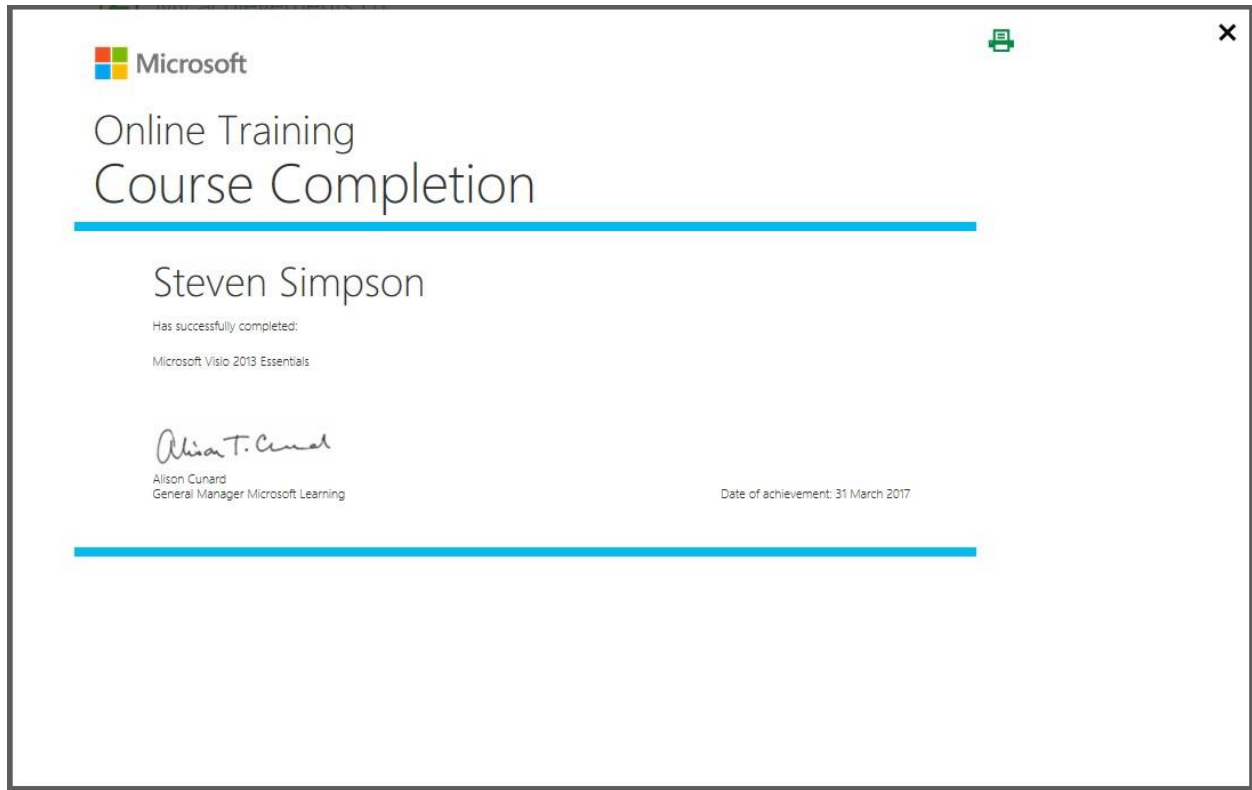
Law 101: Legal Guide for the Forensic Expert is a course designed to help specialists prepare to give testimony in court. Although designed for forensic experts, it can be helpful to any witness who has limited experience testifying in court. It is particularly useful for specialists who have little knowledge of the criminal justice process.



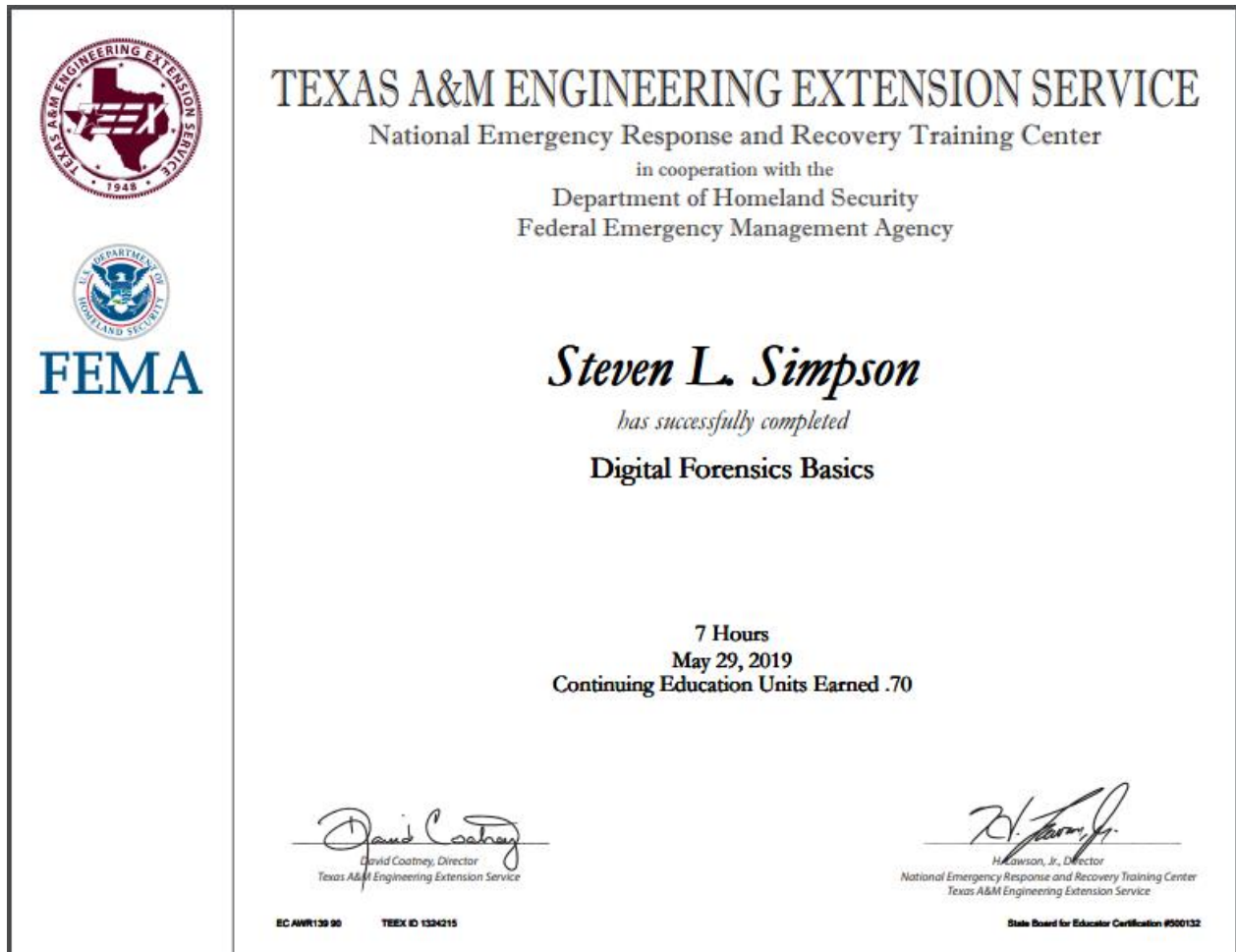
Windows Forensic Environment, also known as WinFE or Windows FE provides a viable solution to first responders and forensic practitioners that will allow the use of traditional Microsoft Windows based forensic tools, to accomplish imaging and triage tasks whilst deployed on the ground. Completion of this course and passing the associated examination proves that the examiner has competency in the Windows Forensic Environment.



An intermediate course designed to teach students the fundamentals of computer crime issues from a legal perspective. The training highlights the various computer crimes and appropriate response by first defenders and others who may encounter these types of issues. Participants learn legislations and organizational efforts to control or prevent such crimes. This course covers intellectual property law (copyright, trade secrets, unfair competition, and unfair business practices), personal jurisdiction, electronic commerce and software contracts, telecommunications, antitrust, privacy, the right to accuracy of information, the right to access information, and the First Amendment.



Microsoft Visio 2013 Essentials: An online course presented by Microsoft that teaches the fundamentals regarding the creation and changing of Visio drawings. The Microsoft Visio 2013 Essentials course discusses the basic functions of Visio 2013, including using drawing tools and diagrams, working with pages, creating custom drawing, reporting and formatting.



This course covered investigative methods and standards for the acquisition, extraction, preservation, analysis and deposition of digital evidence from storage devices and offered a wide array of forensics situations applicable to the real world. The course content covered methods to find traces of illegal or illicit activities left on disk with computer forensics tools and manual techniques, and how to recover data intentionally hidden or encrypted by perpetrators.

Honors and Awards:



The Charles Babbage Award is presented by Regis University to the top student in the Master of Science Computer Information Technology (MSCIT) program. One student per graduating class is chosen to receive the award.