Digital Forensics

TRAINING

**Unlock the Secrets of Digital Evidence:
Discover the Art of Digital Forensics**

Facilitated by
PHILIP WAGNER
Principal Cyber Security
Specialist and Educator
G.P.Wagner Pty.Ltd

Online → 17 & 18 April 2024

PUBLIC SECTOR NETWORK

Certified **B** Corporation

Overview

In a world where cybersecurity incidents are on the rise, digital forensics plays a crucial role in combating and mitigating the growing threats. By unravelling the intricacies of cyber incidents, digital forensics helps organisations understand vulnerabilities, strengthen security measures, and improve incident response capabilities. It not only aids in pursuing justice but also facilitates proactive risk management, empowering organisations to stay resilient in the face of evolving cybersecurity challenges.

Firstly, this course equips participants with the necessary skills to combat the growing threat of cybercrime. As organisations and individuals face increasing risks to their sensitive information, digital forensics is crucial in investigating and combating these crimes. Secondly, the course addresses legal and investigative requirements by providing participants with the knowledge and techniques to effectively identify, collect, preserve, and analyse digital evidence. This ensures that investigations adhere to legal and regulatory standards and that digital evidence holds up in legal proceedings.

By combining expert-led presentations, group discussions, practical exercises, and case studies, participants will gain hands-on experience applying digital forensics concepts and principles. This interactive approach ensures that participants leave the course with the tools to identify vulnerabilities, implement preventive measures, and effectively respond to security incidents. It equips them with the skills and knowledge needed to navigate the complex field of digital forensics, safeguard valuable data, and protect organisations in today's digital age.

Why Attend

- **Gain essential skills** in digital forensics, enabling you to investigate and analyse digital evidence effectively

- **Stay updated** with the latest techniques and best practices in digital forensics to stay ahead in the evolving field of cybersecurity

- **Improve** investigation outcomes by learning to navigate digital environments, recover data, and accurately present findings

- **Enhance** your career prospects with in-demand skills sought after by organisations needing digital forensics expertise

Learning Outcomes

This course will give participants a strong foundation in digital forensics principles, practices, and tools, enabling them to gain a solid foundation in the art of digital forensics. Upon completion, participants will be able to:

- **Understand** the fundamental concepts and principles of digital forensics

- **Apply** industry best practices for identifying, collecting, and preserving digital evidence

- **Utilise** specialised tools and techniques to analyse digital data and recover deleted or hidden information

- **Conduct** investigations involving various digital devices, including computers, mobile phones, and networks

- **Present** findings and evidence in a clear, concise manner

Who Should Attend

This course is ideal for professionals interested in cyber security, information technology, risk management, compliance, or digital forensic investigations. It is recommended for individuals with some knowledge of IT concepts and operating systems, including:

- **IT Security** - Strengthen incident response and data protection through digital forensics knowledge

- **Incident Response** - Effective handling, analysis, and containment of cybersecurity incidents

- **Network administrators** - Identify threats, investigate incidents, and implement network protective controls

- **Security Managers** - Informed decision-making, incident management, and compliance through digital forensics

Meet Your Facilitator

PHILIP WAGNER
Principal Cyber Security
Specialist and Educator
G.P.Wagner Pty.Ltd

Philip Wagner is a cyber security, leadership educator, trainer, executive coach and project/program manager, with extensive leadership and project management expertise in both civilian and military environments. He has advised and trained in a wide range of industries from banking and finance, education and training, technology and government at federal and state levels.

His most recent roles were as the Director Cyber Security and Deputy Chief Information Security Officer with the National Disability Insurance Agency and as a Senior Project Manager for a major Australian Health provider in developing their Cyber program.

Preparation

This workshop is highly interactive with group activities and discussions throughout. Come prepared with some current challenges you are facing in your organisation.

To participate you'll need:

- A computer with camera and microphone
- Strong internet connection
- Quiet, well-lit space
- Current challenges you are facing

Register Early & Save

Extra Early Bird	Early Bird	Standard Price
Register by 9th Feb	Register by 8th Mar	Register by 16th Apr
$795 + GST	$995 + GST	$1,195 + GST
Save $400	Save $200	-

CLICK HERE TO REGISTER

*Group Discounts Available - Contact Registration at

registrations@publicsectornetwork.com or Call on **(02) 9057 9070**

Explore the Agenda

DAY 1 | 17 April 2024, 10:00am - 05:00pm AEST

10:00am Introduction to Digital Forensics

- Understanding the digital forensic process
- Legal and ethical considerations in digital investigations
- Role of digital forensics in law enforcement and corporate environments

11:45am Digital Evidence Identification and Collection

- Identifying and preserving digital evidence
- Rules of evidence and chain of custody
- Documentation and case management

01:00pm Lunch Break

02:00pm File Systems and Data Storage Analysis

- Understanding file systems and their structure
- Recovering deleted or hidden data
- Analysing data storage media

03:45pm Forensic Imaging and Data Acquisition

- Principles of forensic imaging
- Creating and verifying forensic images
- Tools and techniques for data acquisition

05:00pm End of Day 1

DAY 2 | 18 April 2024, 10:00am - 05:00pm AEST

10:00am Digital Forensic Analysis Techniques

- File system analysis and keyword searching
- Timeline analysis and reconstruction
- Data carving and recovery of fragmented files

11:45am Mobile and Network Forensics

- Investigating mobile devices and applications
- Network traffic analysis and log examination
- Internet and social media investigations

01:00pm Lunch Break

02:00pm Malware Analysis and Incident Response

- Analysing malicious software and malware behaviour
- Incident response procedures and tools
- Live forensics and volatile data collection

03:45pm Reporting and Presentation of Findings

- Writing forensic reports and documenting findings
- Presenting evidence in court or other legal proceedings
- Quality Control and peer review in digital forensics

05:00pm End of Day 2

PUBLIC SECTOR NETWORK

Certified B Corporation

Get In Contact

CONNECTING GOVERNMENT
PUBLICSECTORNETWORK.COM

AUSTRALIA / NEW ZEALAND
P +61 2 9057 9070
E info@publicsectornetwork.com

USA / CANADA
P +1 (647) 969 4509
E contact@publicsectornetwork.com

JOIN THE SOCIAL LEARNING PLATFORM FOR FREE AT PUBLICSECTORNETWORK.COM