Digital Forensics Analyst

NICE Framework Reference	Investigate, Cyber Defence Forensic Analyst, INV-FOR-002
Functional Description	**The following role-based description is for security operations only and does not include criminal or audit forensics functions which are provided for within the related law enforcement or audit related occupations**. Conducts digital forensics to analyze evidence from computers, networks, and other data storage devices. This includes investigating and preserving electronic evidence; planning and developing tools; prioritizing activities; and supporting recovery operations and post-incident analysis.
Consequence of error or risk	Error, neglect, outdated information, lack of attention to detail or poor judgment could result in a failure to determine the source and mitigate a compromise, but additionally may result in impacts to organizational information systems to include criminal charges or civil litigation.
Development pathway	This is often a tier 2/3 position within a cybersecurity operations environment that is normally preceded by a minimum of 2-3 years in a network or operational security role including as a malware analyst. This can lead to increased specialization within digital forensics or security assessment activities as well as red/blue team leader, penetration tester or management roles.
Other titles	▪ Digital forensics investigator (normally reserved for cybercrime environment) ▪ Digital forensics examiner (normally reserved for cyber audit environments)
Related NOCs	2171 Information systems analysts and consultants 2147 Computer engineers (except software engineers and designers) 2173 Software engineers and designers
Tasks	▪ Perform real-time cyber defence incident investigations (e.g., forensic collections, intrusion correlation and tracking, and threat analysis) ▪ Investigate security incidents as per terms of reference ▪ Plan forensics analysis activities for cyber incidents ▪ Collect and analyze intrusion artifacts (e.g., source code, malware, and system configuration) and use discovered data to enable mitigation of potential cyber defense incidents ▪ Identify and accurately report on digital forensic analysis artifacts ▪ Capture and analyze network traffic associated with malicious activities using network monitoring tools ▪ Contribute to post-analysis on security incidents and make recommendations based on forensics activities ▪ Develop and maintain investigative and technical reports ▪ Provide technical assistance on digital evidence matters to appropriate personnel ▪ Compile evidence for legal cases, and provide expert testimony at court proceedings ▪ Manage digital evidence in accordance with appropriate chain of custody requirements ▪ Identify and manage secure analysis infrastructure/laboratory

	▪ Operate digital forensics systems (as required based on function and systems available) ▪ Prepare and review forensics policies, standards, procedures and guidelines ▪ Develop, deliver, and oversee training material and educational efforts	
Required qualifications	Education	Post-secondary education (degree or diploma in related computer science or IT field).
	Training	Training in digital forensics tools, techniques and procedures. Also, depending on the organizational technical context and systems/devices used, specialized digital forensics training may be required (e.g. mobile device, digital media, etc.)
	Work experience	2-3 years' experience in an advanced cybersecurity operations role, preferably with malware analysis experience in 'dead box' and active environments.
Tools & Technology	▪ Organizational security policies, procedures and practices ▪ Organizational systems map and network architecture ▪ Digital forensics tools, techniques and procedures ▪ Malware analysis tools ▪ Security Event and Incident Management System ▪ Common vulnerability databases ▪ Security investigation terms of references, responsibilities and limits of authority	
Competencies	KSAs applied at an advanced level: ☐ Threat actor tools, techniques and procedures ☐ Incident response and handling methodologies ☐ Security Event and Incident Management System ☐ Digital forensics methodologies, processes and practices ☐ Anti-forensics tactics, techniques, and procedure ☐ Processes for collecting, packaging, transporting, and storing electronic evidence to avoid alteration, loss, physical damage, or destruction of data ☐ Seizing and preserving digital evidence ☐ Applicable laws, regulations, policies and ethics as they relate to investigations and governance ☐ Legal rules of evidence and court procedures, presentation of digital evidence, testimony as an expert witness ☐ System or device specific forensics (e.g. memory, active director, mobile device, network, computer (dead box), etc.) ☐ Malware analysis tools and techniques ☐ Reverse engineering ☐ Deployable digital forensics capabilities ☐ Types of digital forensics including tools, techniques and procedures (organization and information system dependent) which may include the following forensics for: ○ computer ○ network and active directory; ○ mobile devices ○ digital media (image, video, audio) ○ memory	

Future Trends Affecting Key Competencies	▪ The increased reliance on virtualized and/or ‘cloud-based’ services will require knowledge of responsibilities of the services provider including their responsibilities for cybersecurity systems management. ▪ If practiced within the organization, there will be a requirement to fully understand the implications of ‘bring your own device’ (BYOD) policies. This means that regardless of the device capabilities, there will need to be an assessment of the risks posed to the organization, mitigations to account for potential compromise through a personal device, and what actions will be required by the SOC in the event of an incident. ▪ Increased use of automated tools, aided by artificial intelligence, will require understanding of how the tools will be integrated into identity and access management processes and the related technical and process changes. ▪ Mechanisms to support the required level of trust and organizational risk will need to be in place to support monitoring and reporting of results from automated tools. Consequently, there will need to be increased understanding of organizational risks posed and potential responses within the dynamic threat environment. ▪ The emergence and use of quantum technologies by threat actors will fundamentally change encryption security. This will require knowledge and skills related to implementing a quantum safe strategy as well as threat actor tools, techniques and protocols related to quantum computing attacks and how to defend against them.