Making a Career in Digital Forensics & Incident Response

Investigate. Recover. Prove. The DFIR career explained.

AUTHOR	Babashaheer
VERSION	1.0
DATE	April 2026
SERIES	Cybersecurity Career Series — Document 03 of 06
AUDIENCE	Students and beginners interested in forensics and IR

Contents

Baba Shaheer Gutappa
Digitally signed by Baba Shaheer Gutappa
Date: 2026.04.17 10:20:32 +01'00'

1. What Is Digital Forensics & Incident Response?

Imagine a company wakes up on a Monday morning to find that all their files have been encrypted. A ransom note is on every screen. A server is exfiltrating data to an unknown IP address. Staff cannot access anything. Someone needs to step in, figure out exactly what happened, contain the damage, and recover the business — all while preserving evidence that may be needed in court. That someone is a DFIR professional.

Digital Forensics and Incident Response are two closely related disciplines that are almost always practised together:

Digital Forensics	Incident Response
The science of collecting, preserving and analysing digital evidence. It is about answering: *What happened? When? How? Who was responsible?* The evidence collected must be handled in a way that makes it admissible in legal proceedings — chain of custody is everything.	The operational response to an active or recent security incident. It is about answering: *Is this still happening? How do we stop it? How do we recover?* Incident response is time-pressured and often runs parallel to the forensic investigation.
Reactive. Methodical. Evidence-focused.	**Active. Decisive. Business-focused.**

DFIR professionals are the first responders of the digital world.
They work under pressure, with incomplete information, against the clock — and their findings have real legal and business consequences.

2. DFIR vs Ethical Hacking — Key Differences

Both DFIR and ethical hacking require deep technical knowledge of how systems work — and how they can be compromised. But the mindset, the work and the day-to-day experience are quite different. Understanding the distinction early saves a lot of career confusion.

	Ethical Hacking	DFIR
Core question	Can I get in?	What happened and how?
Mindset	Attacker — offensive	Investigator — reactive
Timing	Before the incident (proactive)	After (or during) the incident
Primary output	Pentest report with findings	Investigation report with evidence
Legal weight	Internal/commercial report	Evidence may go to court
Under pressure?	Some — defined engagement window	High — live incident, client panic
Tools	Metasploit, Burp, Nmap	FTK, Autopsy, Volatility, SIEM
Programming need	Python/Bash scripting	Scripting + log parsing + regex
Suits people who...	Enjoy breaking things	Enjoy piecing things together

Table 1: Key differences between Ethical Hacking and DFIR

3. What a DFIR Professional Actually Does

Activity	% of Time	What This Looks Like
Incident triage & first response	10–15%	Getting the call, assessing scope, deciding whether to isolate systems immediately.
Evidence acquisition	15–20%	Taking forensic images of disks, capturing RAM, preserving network logs before anything is changed.
Analysis	35–45%	The core work — examining artefacts, parsing event logs, running tools, building a timeline.
Report writing	20–25%	Documenting every action taken, every finding, every conclusion, with evidence to support it.
Client communication	10–15%	Keeping the client informed, explaining findings to non-technical stakeholders, advising on next steps.
Research & training	5–10%	Staying current with new malware, new attack techniques, new forensic artefacts and tools.

Table 2: Typical time split for a DFIR engagement

Like penetration testing, DFIR involves a lot of writing.
Your analysis is only as valuable as your ability to explain it clearly.
A finding with no evidence trail is not a finding — it is an opinion.

4. The Investigation Process — Step by Step

A structured investigation process is not optional — it is what separates admissible evidence from a compromised chain of custody. Every professional DFIR engagement follows a defined methodology. The most widely referenced framework is NIST SP 800-61 (NIST, 2012), which defines four phases for incident response. For pure forensic investigations, the ACPO Good Practice Guide (ACPO, 2012) adds the legal dimension used in UK proceedings.

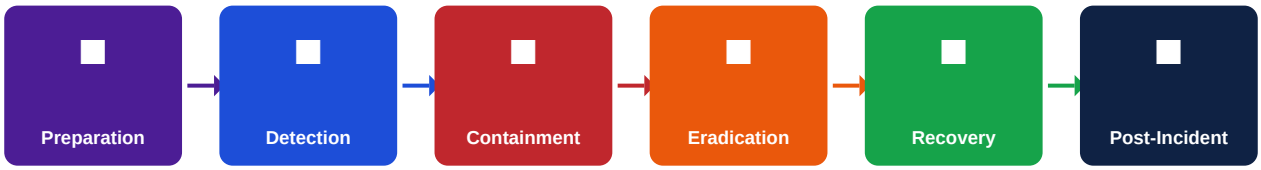

Figure 1: NIST SP 800-61 Incident Response Lifecycle

Each phase explained

Preparation

Before any incident happens — build your IR playbooks, set up your SIEM, establish communication chains and ensure forensic tools are ready. An organisation with no preparation loses days just figuring out who to call.

Detection & Analysis

Identify that an incident has occurred, determine its scope and severity. This involves reviewing SIEM alerts, endpoint detection (EDR) flags, user reports and network anomalies. The analyst must quickly decide: how bad is this, is it still active, what systems are involved?

Containment

Stop the bleeding — without destroying evidence. Short-term containment might mean isolating a compromised machine from the network. Long-term containment means patching the exploited vulnerability or blocking the attacker's C2 server. The order matters: contain first, then investigate — not the other way round.

Eradication

Remove the attacker's presence entirely — delete malware, close backdoors, remove persistence mechanisms, revoke compromised credentials. This must be thorough: missing a single persistence mechanism means the attacker returns.

Recovery

Restore systems to normal operation from known-clean backups or rebuilt images. Monitor closely for signs of re-infection. Validate that the restored systems are clean before returning them to production.

Post-Incident Activity

Write the lessons-learned report. What happened? What worked in the response? What did not? What must change? This phase is consistently under-invested in practice — and is consistently where the most organisational improvement comes from.

The ACPO Principles (UK) — four rules every UK digital forensics professional must follow:

1. No action should change data held on a digital device.
2. A person accessing original data must be competent to do so and able to explain why.
3. An audit trail must exist so that an independent expert can reproduce the process.
4. The person in charge of the investigation is responsible for ensuring these principles are followed.

5. Order of Volatility — Why It Matters

One of the most fundamental concepts in digital forensics is the order of volatility. Digital evidence does not last forever. Some types of evidence disappear in seconds — the moment a machine is rebooted, RAM is gone. Other types persist for years. A forensic investigator must collect evidence in order from most volatile to least volatile, or they risk losing it permanently before they even know it existed.

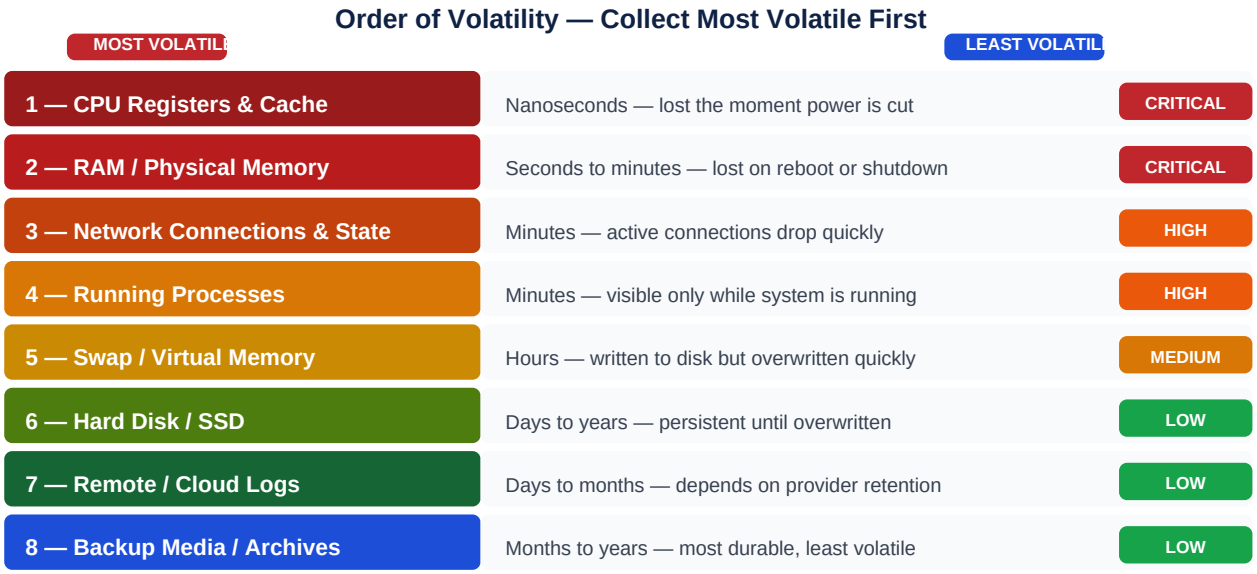

Figure 2: The order of volatility — collect from the top down. Evidence at the top is gone within seconds of losing power.

A common mistake among beginners is to immediately shut down a compromised machine. This feels like the safe option — it stops any attack that is running. But it also destroys RAM, which may contain the malware's decrypted code, the attacker's active session, encryption keys, recently typed passwords and running network connections. In a ransomware case, RAM sometimes holds the encryption key — meaning a live capture before shutdown can be the difference between recovering files and losing them.

> **First rule of live response: capture RAM before you do anything else.**
> Use tools like WinPmem, DumpIt or Magnet RAM Capture. It takes minutes.
> The Volatility Framework then lets you analyse that RAM dump offline.

6. Core Skills You Need to Build

DFIR draws on a wide range of technical skills. Below is an honest assessment of what matters, roughly in order of priority for someone starting out.

6.1 Windows Forensic Artefacts

The majority of real-world incidents involve Windows systems — and Windows leaves evidence everywhere if you know where to look. Learning to read these artefacts is foundational to any DFIR role.

- Windows Event Logs
- Registry Analysis
- Prefetch & Shimcache
- Browser Artefacts
- $MFT & NTFS Structures
- LNK Files & Jump Lists

6.2 Memory Forensics

RAM analysis is one of the most powerful — and most underused — forensic techniques. A memory image can reveal running malware that has no presence on disk (fileless malware), decrypted content, active network connections, and credentials cached in memory. The Volatility Framework is the industry standard tool.

- Volatility Framework
- Process Analysis from RAM
- Network Connections in Memory
- Injected Code Detection
- Credential Extraction

6.3 Network Forensics & Log Analysis

Attackers move through networks. Understanding what happened requires reading packet captures, firewall logs, DNS logs, proxy logs and SIEM data. The ability to correlate events across multiple log sources and build a timeline is a core DFIR skill.

- Wireshark / PCAP Analysis
- SIEM Query Writing (Splunk/KQL)
- DNS & Proxy Log Analysis
- Zeek / Suricata IDS Logs
- Network Traffic Baselining

6.4 Disk & File System Forensics

- FTK Imager / dd — Forensic Imaging

6.5 Scripting & Automation

Parsing gigabytes of log files by hand is not practical. Python scripts that extract specific event IDs, correlate timestamps or hunt for known IOCs save enormous amounts of time. Bash for Linux, PowerShell for Windows, and Python for everything else.

> **Start with Python for log parsing.**
> Learn to use pandas to filter large CSV exports from SIEM tools.
> Learn regex — almost every log analysis task uses it.

7. Tools Every DFIR Professional Should Know

Tool	Category	What It Does	Cost
Autopsy	Disk Forensics	Open-source forensic platform. Analyses disk images for deleted files, browser history, email artefacts, keyword search.	Free
Volatility 3	Memory Forensics	Extracts processes, network connections, registry hives, credentials, injected code and much more from RAM images.	Free
FTK Imager	Disk Imaging	Creates forensic bit-for-bit copies of disks and RAM. Industry standard. Also mounts images for analysis.	Free
Wireshark	Network Analysis	Packet capture and deep packet inspection. Read .pcap files, filter by protocol, follow TCP streams, identify credentials in clear text.	Free
Splunk (Free/SIEM)	Log Analysis	Ingest and search log data at scale. Write SPL queries to hunt for IOCs, build timelines, correlate events across sources.	Free tier
KAPE	Artefact Collection	Kroll Artifact Parser and Extractor. Rapid triage tool — collects forensic artefacts from a live or mounted Windows system in minutes.	Free
Magnet AXIOM	All-in-one	Commercial forensic platform. Analyses computers, mobile devices, cloud, memory and network evidence in a single interface.	Commercial
Eric Zimmerman Tools	Windows Artefacts	Suite of free command-line tools for parsing Windows artefacts: MFTECmd, PECmd (Prefetch), RegRipper, LECmd (LNK) and many more.	Free
CyberChef	Data Analysis	Browser-based tool for encoding, decoding, hashing, extracting data from binary files, and analysing obfuscated content.	Free
Velociraptor	Live Response / EDR	Open-source endpoint visibility and live response platform. Deploy agents, run hunts across a fleet, collect artefacts remotely.	Free

Table 3: Core DFIR tools. The majority are free and open-source.

8. Career Paths Within DFIR

DFIR is not a single job title — it is a cluster of related roles. Understanding where you might start and where each path leads helps you choose the right focus for your early studies and first certifications.

Role	What You Do	Where You Work	Typical Salary (UK)
SOC Analyst (Tier 1)	Triage alerts, investigate basic incidents, escalate complex cases.	MSSP, corporate SOC	£22k–£35k
Incident Responder	Contain and remediate active breaches. Called in when the SOC escalates.	IR firms, MSSP, NCSC	£40k–£70k
Digital Forensic Analyst	Acquire and analyse evidence from disks, memory and network. Build timelines, find artefacts.	IR firms, law enforcement	£35k–£65k
Threat Hunter	Proactively search for attacker presence in an environment before alerts fire.	Large enterprises, MSSP	£50k–£80k
Malware Analyst	Reverse-engineer malicious code. Understand what it does, how it spreads, how to detect it.	AV vendors, threat intel	£45k–£85k
Forensic Consultant	Independent consultant — called in for complex breaches, litigation support, expert witness.	Self-employed / boutique	£500–£1,200/day
DFIR Team Lead / Manager	Manage a team of analysts, triage major incidents, present to C-suite executives.	Enterprises, IR firms	£70k–£100k+

Table 4: Career paths within DFIR (UK salary ranges, CW Jobs 2024 / Reed 2024)

Most DFIR careers start in a SOC.
Tier 1 SOC work builds pattern recognition and familiarity with real incidents fast.
A year in a busy SOC is worth more than two years of self-study alone.

9. The Learning Roadmap

DFIR requires a different starting point from ethical hacking. You need to understand how systems work normally before you can detect when something is wrong. Start with Windows fundamentals — not hacking tools.

1. **Learn Windows Internals**
   Understand the Windows registry, Event Log IDs, file system structure (NTFS), Active Directory basics and how processes, services and drivers work. TryHackMe Windows Forensics path is ideal. 4–6 weeks.

2. **Get comfortable with Linux**
   Many forensic tools run on Linux, and Linux servers are frequent investigation targets. Know the file system, ext4 structure, system logs (/var/log), cron jobs and bash scripting. 3–4 weeks.

3. **Learn network fundamentals**
   Understand TCP/IP, DNS, HTTP, common protocols and how to read a packet capture in Wireshark. You cannot investigate a network intrusion without understanding what normal traffic looks like. 3–4 weeks.

4. **Build your forensic lab**
   Install a free SIEM (Splunk or ELK Stack). Practice with Autopsy on sample disk images. Download memory images from MemLabs or the Volatility GitHub and analyse them. Blue Team Labs Online (free) has excellent guided challenges. Ongoing.

5. **Study the DFIR-specific curriculum**
   Work through the CHFI (EC-Council) or GCFE (GIAC) study material. Even if you do not sit the exam immediately, the curriculum structures your theoretical knowledge across evidence types, tools and legal requirements. 6–8 weeks.

6. **Practice with CTF-style forensic challenges**
   CyberDefenders.org, Blue Team Labs Online and CTFtime.org list forensic challenges regularly. These simulate real investigations — disk images, memory dumps, PCAP files — with guided flags to find. Do at least 10 challenges.

7. **Get your first certification**
   CompTIA Security+ first for foundation. Then BTL1 (Blue Team Labs — excellent practical cert) or CHFI. Aim for GCFE or GCFA once you have 6–12 months of hands-on experience. These open IR firm doors.

8. **Apply for SOC Tier 1 or junior IR roles**
   Build a write-up blog documenting your challenge solutions. Create a GitHub with your Python log-parsing scripts. Apply to MSSP SOC roles and IR firms with graduate/junior programmes. The BTL1 certification is highly regarded for junior positions.

Realistic timeline from zero:

SOC Tier 1 ready: 9–14 months of consistent study and practice.

Junior IR Analyst ready: 18–24 months with SOC experience or strong lab portfolio.

10. Certifications That Matter

DFIR certifications are weighted more towards practical and legal knowledge than the purely technical certs used in penetration testing. The ones below are recognised by hiring managers at IR firms, law enforcement and corporate security teams.

Certification	Level	Focus	Why It Matters
CompTIA Security+	Beginner	Broad security foundations	Baseline requirement for many SOC roles. Good first step.
BTL1 — Blue Team Labs Online	Beginner–Mid	Practical SOC skills — phishing, SIEM, log analysis, forensics	Very well regarded by UK IR firms for junior roles. Practical exam. Affordable.
CHFI — EC-Council	Mid	Computer hacking forensic investigation — full digital forensics curriculum	Vendor-neutral DFIR cert. Good curriculum and employer recognition, especially in consulting.
GCFE — GIAC	Mid	Windows forensic examination — artefacts, timelines, evidence	Highly technical. Respected by enterprise and government hiring managers.
GCFA — GIAC	Mid–Senior	Advanced in-depth forensic analysis and incident response	One of the most respected DFIR certifications globally. Covers memory, timeline analysis and anti-forensics.
GCIH — GIAC	Mid	Incident handling — detection, response, containment	Widely required for IR and SOC lead roles.
EnCE — OpenText	Mid–Senior	EnCase forensic platform certification	Required for many law enforcement and litigation support roles where EnCase is the standard tool.
CREST CPIA	Mid	UK professional standard for cyber incident response	Required for UK government and regulated industry IR engagements.

Table 5: DFIR certifications in order of progression

11. Case Study — A Ransomware Investigation

> This is a fictional case study based on common real-world ransomware incident patterns.
> It illustrates how a DFIR analyst works through an investigation from first call to final report.

The Situation

Meridian Logistics Ltd is a UK transport and logistics company with 300 staff. At 06:45 on a Tuesday morning, the Operations Manager discovers that files on the company's Windows file server are encrypted — all have the extension **.meridlocked**. A ransom note in a text file demands £180,000 in Bitcoin within 72 hours. The company's backup drive is connected directly to the same server. It is also encrypted.

Step 1 — The first call

07:15 — IR team engaged

The company's IT manager calls the IR firm. The analyst on call asks: Is the server still powered on? Yes. Has anyone touched it? No — they did not want to make it worse. Good.

Immediate instruction to the IT manager: Do NOT shut it down. Do NOT run antivirus. Do NOT delete the ransom note. Isolate the server from the network by unplugging the network cable — not via software.

The analyst documents the call time, who made the decisions, and what was found. The evidence chain starts now.

Step 2 — Live acquisition

09:30 — On-site, live system

Analyst arrives on-site with a forensic kit: laptop, hardware write-blocker, external SSD. First action: capture RAM using WinPmem. This takes 12 minutes. RAM image saved and hashed.

Second: create a forensic image of the server drive using FTK Imager. Write-blocker attached to ensure the original is not modified. Hash value recorded for evidence integrity.

Step 3 — Initial analysis

14:00 — Back at the lab

Volatility analysis of the RAM image: identifies a suspicious process 'svchost32.exe' (note: the real svchost.exe never has '32' in the name). Process injected into LSASS memory.

Windows Event Logs: finds a successful RDP login from an external IP at 02:17 — four hours before encryption began. Account used: 'backup_svc' — a service account with no MFA enabled.

Firewall logs confirm the IP — traced to a Tor exit node in Romania. The same IP had been probing RDP port 3389 for

Step 4 — Timeline reconstruction

Time	Event	Source
Mon 03:12	First port scan of RDP from external IP	Firewall logs
Mon 11:44	Credential stuffing attack against RDP — 847 failed attempts	Event Log 4625
Mon 14:30	Successful RDP login — backup_svc account	Event Log 4624

Time	Event	Source
Mon 14:31–17:00	Attacker enumerates file shares, exfiltrates ~2.4GB of data	Network logs
Mon 17:02	Ransomware binary dropped: C:\Windows\Temp\svchost32.exe	Prefetch / $MFT
Mon 17:04	Ransomware executed — encryption begins	Event Log 4688
Tue 06:45	Encryption discovered by Operations Manager	Incident report

Table 6: Reconstructed attack timeline from forensic artefacts

Step 5 — The finding and recommendations

Root cause: the **backup_svc** account had RDP access enabled, no MFA, and a weak password that was in the RockYou wordlist. The attacker used a credential stuffing attack to gain access. Before encrypting, they exfiltrated 2.4GB of data — this makes it a double-extortion ransomware case.

- Disable RDP on the perimeter — use a VPN with MFA for remote access instead
- Enforce MFA on all service accounts and administrative accounts immediately
- Review and remove all service accounts with interactive login rights
- Implement offline, air-gapped backups — the backup drive was attached to the same server
- Deploy an EDR solution with behavioural detection to catch lateral movement
- Engage the ICO — data was exfiltrated, making this a notifiable GDPR breach

The investigation took 3.5 days of analyst time.
The total incident cost to Meridian Logistics: estimated £340,000.
A SOC with basic monitoring would have caught the credential stuffing on Day 1.

12. Breaking In — Getting Your First Role

DFIR is slightly harder to break into than SOC roles because most firms want analysts who have already seen real incidents. The practical path is to start in a SOC, build your skills, and transition into IR and forensics as you advance.

Build visible evidence of skill

- **CyberDefenders.org:** Free forensic labs with disk images, memory dumps and PCAP files to analyse. Write up your methodology and findings publicly — this is your portfolio
- **Blue Team Labs Online:** Paid and free challenges. Completing the BTL1 certification demonstrates practical SOC and forensics skills to employers
- **MemLabs (GitHub):** Six free memory forensics challenges using Volatility. Excellent for building RAM analysis skills from scratch
- **DFIR.training:** Aggregates free DFIR resources, challenges and tools in one place. Regular new content
- **Write-up blog:** Document your challenge solutions. Explaining how you found an artefact and what it meant demonstrates both technical skill and communication ability
- **GitHub:** Share your Python log-parsing scripts, Volatility plugins or KAPE targets you have built

Where to find roles

Where to Look	What to Search For
CyberSecurityJobs.com	SOC Analyst, IR Analyst, Forensic Analyst, DFIR
LinkedIn	Junior SOC, Tier 1 Analyst, Graduate IR — connect with DFIR professionals
CREST accredited firm websites	Apply directly — most IR firms hire regularly at junior level
Law enforcement / NCA	National Crime Agency, Regional Organised Crime Units, GCHQ — specific DFIR roles
NCSC / GCHQ Graduate Schemes	Competitive but excellent structured entry point with training
Glassdoor / Indeed	Filter by 'incident response analyst', 'digital forensics', 'SOC'

Table 7: Where to find DFIR and SOC roles

Interview questions to prepare for

- Walk me through the order of volatility — why does it matter in a live response situation?
- A user's machine is behaving strangely. What is the first thing you do?
- What Windows Event IDs would you look for to detect a successful brute-force login?
- What is the difference between a forensic image and a simple file copy?
- How would you detect lateral movement in Windows event logs?
- What is prefetch, and what does it tell you forensically?
- Explain what chain of custody means and why breaking it matters.

- You find malware on a disk image. How do you determine when it was first executed?

The best interview answer in DFIR:
"I have worked through these forensic challenges. Here is my write-up."
Evidence of hands-on practice consistently beats theoretical knowledge alone.

13. References

1. ACPO (2012) *Good Practice Guide for Digital Evidence.* Association of Chief Police Officers. Available at: https://www.digital-detective.net/digital-forensics-documents/ACPO_Good_Practice_Guide_for_Digital_Evidence_v6.pdf [Accessed: 10 April 2026].
2. Blue Team Labs Online (2024) *BTL1 — Blue Team Level 1 Certification.* Available at: https://www.blueteamlabs.online/certifications [Accessed: 11 April 2026].
3. CREST (2024) *CPIA — Certified Practitioner in Incident Analysis.* Available at: https://www.crest-approved.org [Accessed: 11 April 2026].
4. CW Jobs (2024) *Technology Salary Survey 2024.* Available at: https://www.cwjobs.co.uk/salary-checker [Accessed: 11 April 2026].
5. CyberDefenders (2024) *Free Digital Forensics Labs.* Available at: https://cyberdefenders.org [Accessed: 12 April 2026].
6. EC-Council (2023) *Computer Hacking Forensic Investigator (CHFI).* Available at: https://www.eccouncil.org/train-certify/computer-hacking-forensic-investigator-chfi/ [Accessed: 12 April 2026].
7. GIAC (2024) *GCFE and GCFA Certification Overview.* Available at: https://www.giac.org/certifications/forensics [Accessed: 12 April 2026].
8. Luttgens, J., Pepe, M. and Mandia, K. (2014) *Incident Response and Computer Forensics.* 3rd edn. New York: McGraw-Hill.
9. NIST (2012) *Computer Security Incident Handling Guide (SP 800-61 Rev. 2).* National Institute of Standards and Technology. Available at: https://doi.org/10.6028/NIST.SP.800-61r2 [Accessed: 13 April 2026].
10. Offensive Security / Volatility Foundation (2024) *Volatility 3 Documentation.* Available at: https://volatility3.readthedocs.io [Accessed: 13 April 2026].
11. Reed (2024) *Cybersecurity Salary Guide UK 2024.* Available at: https://www.reed.co.uk/career-advice/cybersecurity-salary [Accessed: 13 April 2026].
12. Zimmerman, E. (2024) *Eric Zimmerman's Digital Forensics Tools.* Available at: https://ericzimmerman.github.io [Accessed: 14 April 2026].

Document prepared by **Babashaheer**. Version 1.0 — April 2026. Cybersecurity Career Series — Document 03 of 06.