



DIGITAL EVIDENCE & INCIDENT RECONSTRUCTION

DIGITAL FORENSICS & RESPONSE

**Preserve the evidence.
Reconstruct the event.
Recover with clarity.**

Forensically sound support for suspected compromise, insider activity, data loss and other digital incidents where evidence must direct response.

INDEPENDENT / EVIDENCE-LED / DEFENSIBLE

forensics@siftcon.africa | +27 10 979 0010

siftcon.africa



THE OBJECTIVE

MOVE FROM TECHNICAL UNCERTAINTY TO A SUPPORTED ACCOUNT.

Digital incidents develop quickly, but indiscriminate action can destroy context, overwrite artefacts or make later conclusions difficult to defend.

SIFTCON helps preserve what matters, analyse relevant activity and reconstruct events so containment, recovery and reporting decisions rest on the strongest available evidence.



SITUATIONS WE SUPPORT

● UNAUTHORISED ACCESS & COMPROMISE

Intrusion, account takeover, malware activity or unauthorised system use.

● INSIDER THREAT & DATA LEAKAGE

Potential exfiltration, misuse of access or deliberate control circumvention.

● EMAIL & PAYMENT COMPROMISE

Phishing, mailbox intrusion, payment diversion or fraudulent communication.

● EMPLOYEE ACTIVITY REVIEWS

Authorised examination of device, account or communication activity.

● DELETION & MANIPULATION

Recovery and analysis of deleted artefacts, altered records or concealment attempts.

● PROCEEDINGS & DISCLOSURE

Digital-evidence support for investigations, disputes or formal processes.

CORE CAPABILITIES

CONNECT DIGITAL ARTEFACTS TO THE DECISIONS THEY SUPPORT.

The work combines only the acquisition, analytical and response disciplines appropriate to the incident and mandate.

01 INCIDENT SCOPING & PRESERVATION

Clarify what is known, identify volatile or at-risk evidence and define immediate actions that protect future analysis.

02 FORENSIC ACQUISITION

Collect relevant data from authorised devices, systems, accounts, email and logs using documented, proportionate methods.

03 DEVICE & SYSTEM ANALYSIS

Examine user activity, file systems, artefacts, applications and metadata to identify material events and changes.

04 COMMUNICATION & ACCOUNT ANALYSIS

Review email, messaging, identity and access records to test activity, compromise and data movement.

05 TIMELINE & ROOT-CAUSE RECONSTRUCTION

Correlate independent evidence sources to establish entry, activity, persistence, impact and controls that failed.

06 IMPACT & RECOVERY SUPPORT

Translate forensic findings into containment, recovery, disclosure and longer-term control-improvement decisions.

ENGAGEMENT METHOD

PROTECT THE CHAIN FROM SOURCE TO CONCLUSION.

01

PRESERVE

Protect relevant devices, accounts, logs and records while documenting condition and continuity.

02

ACQUIRE

Create controlled forensic collections that retain the available evidential characteristics.

03

ANALYSE

Test artefacts, activity and competing explanations against the investigative questions.

04

RECONSTRUCT

Correlate findings into a supported timeline, impact assessment and response.

INTEGRATED RESPONSE

DEFINED ROLES. PROTECTED EVIDENCE. COORDINATED ACTION.

SIFTCON can work alongside internal technology and security teams, legal advisers, insurers and other appointed specialists. Authority, confidentiality and communication routes are agreed at intake.

WHAT YOU RECEIVE

- Documented preservation and forensic-acquisition record
- Evidence-led incident timeline and reconstruction
- Defined scope, impact, uncertainty and residual exposure
- Decision-ready containment, recovery and reporting guidance

TARGET OUTCOMES

EVIDENCE THAT DIRECTS RESPONSE AND STRENGTHENS RECOVERY.

01 EVIDENCE INTEGRITY

Relevant digital material is identified, collected and documented for future scrutiny.

02 VERIFIED TIMELINE

Technical events are connected to users, systems and business context.

03 DEFINED SCOPE & IMPACT

Decision-makers understand what is supported, uncertain and still exposed.

04 RECOVERY DIRECTION

Findings inform containment, remediation, disclosure and stronger controls.

WHO RELIES ON THE WORK

01

Security &
incident-response teams

02

Legal, compliance & privacy
functions

03

Regulated & critical-service
organisations

04

Leaders facing insider or
data-loss concerns



SIFTCON
Empowering Insights

PROTECT CRITICAL DIGITAL EVIDENCE

START WITH THE INCIDENT, URGENCY AND SYSTEMS INVOLVED.

We can help assess immediate preservation priorities and define a proportionate forensic and response mandate.

START A CONFIDENTIAL DISCUSSION

EMAIL

forensics@siftcon.africa

PHONE

+27 10 979 0010

WEB

siftcon.africa



Explore the service online

Northgate Office Park, 14 Aureole Avenue, Gauteng, South Africa, 2188

Digital-forensics work is performed only within an agreed mandate and authorised evidence scope.