CRITICAL FAULT

PROFESSIONALLY PARANOID

DIGITAL FORENSICS

Combining our expertise, certifications, and state-of-the-art incident response toolkit, Critical Fault is a leading source of digital forensics in Oklahoma. Our offensive security toolkit provides us the unique ability to discover and preserve digital records that other digital forensic firms might miss.

- Drive Incident Response Efforts
- Improve Cyber-Resiliency
- Identify Indicators of Compromise
- Provide a Root Cause Analysis
- Develop Remediation Strategies
- Expert Witness Testimony

CRITICAL FAULT
PROFESSIONALLY PARANOID

INCIDENT RESPONSE

During an incident, attackers leave traces. Critical Fault is expertly positioned to assist companies in identifying traces of intrusion, or indicators of compromise. Our Red Team quickly determines the entry point for an incident and implements a plan to stop the incident and prevent further breaches. Additionally, Critical Fault ensures the data is collected and preserved so it is admissible as evidence in the court of law.

How Digital Forensics Aid Incident Response

During an incident, the highest priority to an organization is to stop the incident followed by the need to recover systems to an operational state. In this rush, organizations will often destroy important evidence needed to perform a root cause analysis.

Digital Forensics typically follows after an organization is operationally restored. Evidence collected during the incident response is preserved and examined to help determine the root cause of an incident.

CRITICAL FAULT

PROFESSIONALLY PARANOID

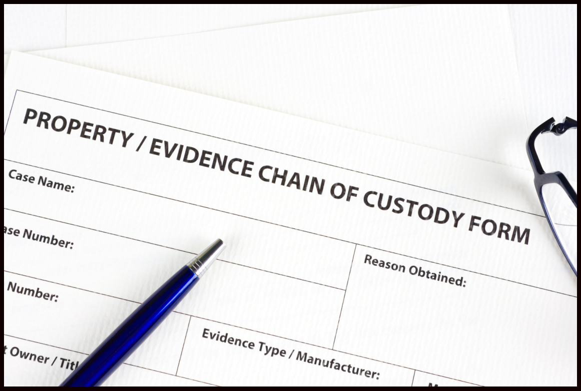
EXPERT WITNESS CREDIBILITY

Digital forensics is the process of collecting data to present as evidence in a court of law. Therefore, it must be handled properly and preserved; removing all opportunity for potential tampering or alteration of evidence. Critical Fault utilizes five steps to ensure that evidence is preserved credibly and in such a way that it can be used as evidence in expert witness testimony.

IDENTIFY	Identify evidence and record storage details
PRESERVE	Isolate, secure, and preserve data
ANALYZE	Reconstruct fragmented data and draw conclusions
DOCUMENT	Create a record of data to recreate the incident
PRESENT	Summarize and present results as a credible expert witness

CRITICAL FAULT
PROFESSIONALLY PARANOID

CHAIN OF CUSTODY



PROPERTY / EVIDENCE CHAIN OF CUSTODY FORM

Case Name:

se Number:

Reason Obtained:

Number:

Evidence Type / Manufacturer:

Owner / Tit

In Digital Forensics, the Chain of Custody is a process that documents the specifics of evidence collection (including the safeguarding, and analysis throughout its lifecycle) by notating each individual involved in the handling of evidence, when it was collected/transferred, and why it was collected/transferred.

PROTECTIONS FOR CHAIN OF CUSTODY

Tamper Evident Casing

Secure Evidence Vault

24/7 security guard

Video surveillance

CRITICAL FAULT

PROFESSIONALLY PARANOID

DIGITAL FORENSICS EXAMINER

A qualified digital forensic examiner must be proficient in multiple domains of technical and administrative knowledge. Critical Fault is dedicated to ensuring their digital forensics examiners display skills in:

- DOCUMENT CONTROL/REVIEW
- INFORMATION SECURITY
- INFORMATION ASSURANCE
- METADATA ANALYSIS
- VOLATILE MEMORY EXTRACTION