Tools

SIEM

Kibana Splunk

Network

Wireshark

Forensics

Memory

Volatility