iSecure Consulting

UK:Caerphilly Business Park, CF83 3GG, Caerphilly
Kenya: 63 Mandera Road, Kileleshwa, Nairobi
Nigeria: 4B Keffi Street, Osborne Offshore, Ikoyi, Lagos

Suite of Corporate Cyber Intelligence / Reconnaissance Solutions

Wireline Ethernet Interception & Real-Time Reconstruction Series	E-Detective System	Ethernet LAN Internet Monitoring System, Internet Auditing, Data Leakage Detection and Retention (DLDR), Record Keeping Solutions.
	E-Detective Data Guard System	Monitor Transactions of Heterogeneous Databases (MySQL, MS SQL, Oracle DB, DB2, Sybase). Monitor Windows CIFS activities – MS Windows File Sharing Activities. Monitor Internal Mail Servers Sent/Received – POP3, SMTP
	E-Detective Data Retention & Management System	Archived backup data from E-Detective System. Review, search and query backup data.
	HTTPS/SSL MITM Interception System (LEA)	Intercepting Ethernet LAN HTTPS Traffic such HTTPS Gmail Traffic including HTTPS username and password.
	E-Detective Backup Server	Archived backup data from E-Detective System. Review, search and query backup data.
	E-Detective Central Management System	Manage Multiple E-Detective Systems, ED Backup Server Systems, EDDC with Single Login GUI. Centralized Search/Query.
Wireless LAN Interception & Real-Time Reconstruction Series	Wireless-Detective System	Wi-Fi IEEE 802.11 a/b/g/n passive interception system. Target can be an AP, a Client or entire Channel Capable of decrypting WEP key WD x 4 Extreme Systems comes with Distributed Capturing, Forbidding and Locator Functions.
	WPA-PSK Password Recovery System	Recovery of WPA1-PSK and WPA2-PSK passphrase Using GPU Hardware Acceleration Using Smart Dictionary (Mutation) Using Masking (Target Brute Force Attack).
Integrated Interception & Real-Time Reconstruction Series	Network Investigation Toolkit – NIT	Ethernet LAN passive and active interception system Wi-Fi IEEE 802.11 a/b/g/n passive and active interception system. For Wi-Fi passive interception, targets can be up to 4 AP, 4 Clients or 4 Channels. Capable of decrypting WEP key. WPA-PSK password recovery (optional) using WPA-PSK Password Recovery System Decrypting HTTPS traffic including username and password by active implementation in both LAN and Wi-Fi environment. Capable of manually reconstructing the PCAP raw data files
Offline Manual Packet Reconstruction Series	E-Detective Decoding Centre - EDDC / EDDC-LEMF	Provides Case and User Management for different Investigators and with different Cases. Parse and reconstruct pre-captured PCAP raw data files manually.
	Forensics Investigation Toolkit – FIT	The only Windows Based Software Application Designed for single user usage. Parse and reconstruct PCAP raw data files manually