e-Crime Bureau®

TRACKING THE TRAILS OF CYBER CRIMINALS

CYBER SECURITY & INVESTIGATIONS BUREAU

PREVENT SECURE INVESTIGATE

With the emergence of cybercrimes and network-related criminal activities, the need for a dedicated high tech crime lab with a highly qualified and experienced workforce to provide ICT infrastructure security and computer forensics solutions to clients across Africa becomes more important than ever before. The establishment of e-Crime Bureau as the first private e-crime lab in the West Africa sub-region is a direct response to this growing necessity. Our corporate philosophy is to PREVENT cyber-related attacks, to SECURE cyber infrastructures and to INVESTIGATE cyber-related crimes.

As a company, we seek to foster closer working relationship with corporate bodies, attorneys, government agencies, the law enforcement and private individuals to help address their ICT infrastructure security & computer forensics needs.

- Albert Antwi-Boasiako, Founder & Principal e-Crime Consultant

e-Crime Bureau®

Website www.e-crimebureau.com
Email info@e-crimebureau.com
Skype e-crime

Tel +233 (0) 302 960397
+233 (0) 207 131646
Fax +233 (0) 302 510247

CLIENTS SECTORS

Attorneys/Law Firms

e-Crime Bureau has developed a dedicated unit which is managed by experienced digital forensics practitioners to help attorneys, law counsels and paralegals navigate the mystifying world of digital data; whether to assist in criminal investigations or in civil and commercial litigations. As a practising attorney or a legal professional, e-Crime Bureau is your point of contact for digital forensics consultations & support.

Corporate Sector

We assist our corporate clients in cases such as insider fraud, copyright/intellectual property theft, data theft, corporate espionage, employee misconduct including computer misuse and corporate litigation matters. We follow standardized computer forensics procedures to identify, recover and examine digital data to prove what happened, when it happened, how it happened and most importantly who was involved. We also provide ICT infrastructure security solutions to our corporate clients across Africa.

Law Enforcement

At e-Crime Bureau we realize the unique challenge for the law enforcement in their investigations of high tech crime cases. We develop training programmes to train cyber detectives to help them monitor & track online criminal behaviour. We also assist law enforcement agencies with cyber threat profiling, counter intelligence operations, criminal network profiling & monitoring, digital forensics procedures, high tech crime investigations and computer forensics technology support.

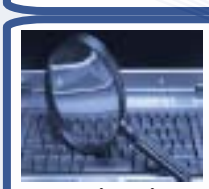
OUR SERVICES

COMPUTER & NETWORK FORENSICS

At e-Crime Bureau, we trace the digital footprints of cyber criminals by examining computer hard drives and related devices (including Servers, PDAs, Digital Cameras, etc) for evidence. We also capture and analyze network packets to identify specific cyber attacks. We maintain a verifiable chain of custody in our investigations and our digital forensics team conduct investigations in compliance with international digital forensics protocols including ACPO, NIST and SWGDE Guidelines. By adopting these guidelines, we assure our clients and the justice system that evidence we retrieve from computer systems are fit for purpose and are admissible in the court of law.

MOBILE PHONE & SIM FORENSICS

Our team of forensics examiners use the latest mobile device analysis tools to retrieve vital data from all brands of mobile devices including NOKIA, Blackberry, i-phones, Samsung, Motorola, HTC, etc. We can retrieve deleted files/messages, phone/SIM serial numbers including the ICCID and IMEI, details of call log entries (including calls made, received and missed), multimedia messages, and data stored on phone memory cards, graphic images received or stored on the mobile device, the cell attached to the phone, and calendar entries. Results of our analysis are documented in a forensic report which we submit to our clients at the end of the investigations.



EXPERT WITNESS SERVICES

The digital forensics arena is a relatively new field and most participants of the judicial and the legal proceedings lack the scientific and the technical knowledge underlying the acquisition and examination of digital evidence. Because of our wealth of knowledge and experience in the sector, we are able to provide expert testimony and assist the courts to scrutinize every bit of any digital evidence presented to it. Whether you are a lawyer or from the law enforcement, the judiciary, corporate sector or from any government department, e-Crime Bureau can provide you with this service in both civil and criminal legal proceedings.

LITIGATION SUPPORT

In the current global business climate, litigation is part of the prevailing business culture as organizations frequently run into disputes. These disputes may involve ex-employee, a competitor or even the government. Similarly in our domestic and social affairs, people and institutions often run into disputes. For attorneys to provide a viable legal representation for their clients they need to explore all sources of evidence and this include digital evidence. We provide advisory services on the digital forensics lines of enquiry in litigation claims for private individuals, institutions, attorneys, legal firms and government agencies.

Website www.e-crimebureau.com
Email info@e-crimebureau.com
Skype e-crime
Tel +233 (0) 302 960397
+233 (0) 207 131646
Fax +233 (0) 302 510247

CLIENTS SECTORS

Government Agencies

e-Crime Bureau provide free consultations to our clients from the government sector to ascertain their ICT infrastructure security and computer forensics needs. We also provide computer forensics services, fraud & corruption investigations assistance, litigation support, technology support and cyber security policy implementation services. We propose cost-effective solutions to our clients from this sector to meet their budget needs.

Private Sector Clients

We provide digital investigations services and assistance to private clients including PIs, investigative journalists and individuals who require data from digital devices to support their investigations or findings. We can retrieve hidden or deleted files, track user activities, recover lost passwords, examine timeline events and construct user activities in a forensically sound manner. We also provide consultations to private clients and help them explore the digital forensics line of inquiry to find the required evidence.

Global Partners

We liaise with our technology partners to offer software and hardware solutions to our clients to meet their ICT infrastructure security and computer forensics needs. We also partner with our service-based partners to deliver services and business security support.

Our company develops partnerships with global institutions, research & training establishments and government agencies to research and train professionals to secure ICT infrastructures and investigate network-related criminal behaviour.

OUR SERVICES

CYBER INTELLIGENCE ANALYTICS

The growing reliance on network systems in particular and the cyber world in general has led to an array of complex threats to the security of life in the cyber space – to private individuals, to the military, to political entities, to businesses, to governments and to state institutions. Our tailored service in cyber intelligence analytics provides a mechanism for our intelligence analysts to profile both existing and emerging threats, collect vital intelligence about these threats and the participants involve in these online criminal behaviour. We provide our clients with intelligence information on identified threats and assist them with counter-measures.

E-FRAUD INVESTIGATIONS

One of our trademark services is to support our clients with e-fraud and insider fraud investigations. Our company is equipped with the latest cutting-edge forensic tools and experienced e-fraud investigators to assist in these types of investigations. We investigate all forms of electronic fraud including credit card fraud, online banking fraud, online auction fraud, internal employee fraud, insurance fraud, email fraud, electronic blackmail, online identity theft and investment scams/419 fraud. In addition, we assist our clients with fraud risk management initiatives and customized anti-fraud technologies to detect and prevent fraud.

INCIDENT RESPONSE (CERT/CSIRT)

In other to secure network resources and internet infrastructure, corporate organizations and countries are required to implement a proactive information security framework to coordinate cyber attacks and mitigation response measures. We support our clients to set up and operate Computer Emergency Response Team (CERT)/Computer Security Incident Response Team (CSIRT) to deal with computer security emergencies and incident response operations. Our services are tailored to meet the requirements of both *Corporate/Organization-based CERT* and *National-based CERT*. We can also assist our clients to implement adhoc CERT to handle computer emergencies as and when they occur.

DATA SECURITY

At e-Crime Bureau we understand the value of securing computer and internet resources for our clients. We provide advisory services on data security; we deploy our skills and provide the tools to protect mission-critical resources of our clients. We ensure that data and other network resources are impenetrable and only people with authorized credentials can access corporate and government electronic resources. In addition, data protection and privacy laws require businesses and organizations to properly secure personal data of their customers. The consequence of violating these regulations far outweighs the cost of securing these assets and our team of experts are available to assist you to secure these vital assets.

Website www.e-crimebureau.com Tel +233 (0) 302 960397
Email info@e-crimebureau.com +233 (0) 207 131646
Skype e-crime Fax +233 (0) 302 510247

e-Crime Bureau®

TRACKING THE TRAILS OF CYBER CRIMINALS

RESEARCH & TRAINING

e-Crime Bureau recognize the importance of research in understanding the dynamics of cyber crime and cyber security. As a result, it is our corporate objective to develop and carry out research projects with our global partners in the area of cyber governance, online security & internet safety, internet fraud, computer forensics, insider corporate attacks, organized cyber crime networks and incident response (CERT) among others. The philosophy underlying our research objectives is twofold:

- ***to continue to offer scientific advice to our clients in accordance with the evolving trends in the sector.***
- ***to consolidate the scientific basis of our training programmes for our clients.***

*We develop and organize training programmes in the following specific areas: Network/Internet Security * Incident Response (CERT/CSIRT) * Computer Forensics * Mobile Phone/SIM Forensics * Internet Investigations * Cyber Governance * Cybercrimes & Cyber Laws. Our company liaise with other professional bodies and our training partners to customize training programmes to meet specific requirements of our clients in different sectors. Please contact our training department to discuss about your training needs.*

OUR SERVICES

E-DISCOVERY SOLUTIONS

E-Discovery is the process of identifying, preserving, collecting, reviewing, analyzing and producing Electronically Stored Information (ESI) during litigations and civil legal proceedings. As e-Discovery is an integral component of GRC, e-Crime Bureau support our corporate and allied clients to adhere to government and industry legal requirements to mitigate risk, reduce costs, and to maintain efficiency in corporate information governance. We comply with the Electronic Discovery Reference Model (EDRM) framework to ensure litigation readiness of our clients by actively assisting them with the legal hold process.

PRODUCTS & SOLUTIONS

We partner with cyber security and computer forensics solution providers around the world to offer customized products and solutions to our clients across Africa. We provide tools and solutions to detect fraud, to manage security incidents, to consolidate e-Discovery processes, to investigate computer and mobile phone devices, to encrypt & decipher data, to monitor internet activities & network traffic and solutions to prevent and detect malicious attacks. As our client, we can organize a webinar for you, irrespective of your physical location, to evaluate our products and solutions to match their capabilities with your business requirements. Contact our technology support team for free consultations.

We provide our services, coordinate research activities and training programmes from our head office in Accra, Ghana. We also have our country representatives across Africa who coordinate our services in these countries. For all your enquiries contact the following:

e-Crime Bureau Lab Location:
19 AGYEMANG STREET,
OPPOSITE BLOCK 84, ADENTA SSNIT
ESTATE, ADENTA – ACCRA, GHANA

e-Crime Bureau Registered Office:
D544/4 JONES NELSON LINK
OFF KOJO THOMPSON ROAD,
ADABRAKA – ACCRA, GHANA

e-Crime Bureau Postal Address:
P. O. BOX CT1560
CANTONMENT – ACCRA, GHANA

e-Crime Bureau®

Website www.e-crimebureau.com
Email info@e-crimebureau.com
Skype e-crime

Tel +233 (0) 302 960397
+233 (0) 207 131646
Fax +233 (0) 302 510247