Digital Evidence: Need for Maintaining Minimum Standards for Admissibility Across Jurisdictions

18 Nov, 2013 Commander Mukesh Saini (Retd.)

Unlike the real world, a cyber crime can be committed even without visiting the country of the victim. In another situation of cyber victim may be present under the jurisdiction of the same court but still digital evidences of the crime may be spread across the globe. Ur criminals can gang-up virtually from across the world, commit a cyber crime and disperse, they may not even know each other in Therefore, the task of an investigator is far more challenging to not only identify and gather digital evidences from the computers, mobi routers and gateways but also to accomplish this task to convince the court that the digital evidences are not tampered and correctly co the established scientific procedures.

The technique and acceptable procedure for handling of evidence can be different in different countries. This can diminish or destroy the such electronic evidence. There are several cases when courts have not accepted when evidences collected are not according to the Inc add to the complexity, digital evidences are fragile, volatile and can be tampered easily, sometimes even without such intentions. expertise is required to collect the electronic evidence according to the procedure which meets the requirement of all the courts of the wo

The Lochard's principle of forensics is that the perpetrator of a crime will bring something into the crime scene and leave with somet evidences are without prejudice and just because they are not detected do not mean they do not exist. This principle is true for cyber also. The large amount of logging takes place inside computers and network devices, which can leave almost irrefutable trail of digital ev of crime to the criminal. The challenge is identifying, collecting and preserving the evidence and later during the trial passing the test c the more relevant when such evidence is collected from a country having different procedures of evidence handling than the country wh tried.

Leaving the task of analysis of evidence to the investigators, the digital evidence may be identified, collected, acquired, preserved an person who may not be from Law Enforcement Agency. This person is called 'Digital Evidence First Responder' (DEFR). It is therefore n whether from Law Enforcement Agency (LEA) or not must have expertise on digital evidence and associated procedures.

List of standards on Cyber Forensics

Standard	Purpose	Status
ISO/IEC 27037	Guidelines for identification, collection, acquisition, and preservation of digital evidence	Published
ISO/IEC 27038	Specification for digital redaction	Final Draft
ISO/IEC 27041	Guidelines for the analysis and interpretation of digital evidence	Draft
ISO/IEC 27042	Guidelines for the analysis and interpretation of digital evidence	Draft
ISO/IEC 27043	Digital evidence investigation principles and processes	Draft
NIST SP 800-101	Guidelines on Cell Phone Forensics	Published
NIST SP 800-86	Guide to Integrating Forensic Techniques into Incident Response	Published
NIST SP 800-72	Guidelines on PDA Forensics	Published
BS 10008	Evidential Weight and Legal Admissibility of Electronic Information	Published

To manage these challenges, especially handling evidences under multi-jurisdictional situation, the Organisation of International Stand efforts, have published ISO/IEC 27037 – Guidelines for identification, collection, acquisition, and preservation of digital evidence. The after due deliberations with all member countries, including India, a standardised approach which if followed by DEFR can provide respective courts about the reliability and credibility of the digital evidence. The standard provides necessary guidance as how to ident and preserve digital evidences from computers, mobile devices, navigation systems, digital still and video cameras (including CCTV).

ISO/IEC 27037 is technology and jurisdictional neutral, and does not recommend any specific product. A digital evidence handled international standard ISO 27037 provides a kind of assurance to any court that irrespective of the fact that who and from which count

collected, it has maintained its evidentiary value. The standard does not supersede the national laws but add to the procedural aspects o evidences. This also means that an accused in his defence can show the court that the investigators have not followed the procedures g 27037, hence the electronic evidence has lost is evidentiary value, because the standard is based on the least common denominator of handling and anything short can have an impact on the weight of electronic evidence. Interestingly there is a British Standard BS 100(the evidential weight and legal admissibility of the electronic information.

In India, Section 65B of the Evidence Act lays down the procedure for admissibility of electronic evidence while Section 85B of the Eviden courts from presuming electronic evidences as genuine unless it is signed by 'secure' digital signature. It means that the presenter of has to prove that the digital evidence is genuine and has not been tampered. It is here that ISO/IEC 27037 can be a very powerful tool investigators to prove truthfulness of the evidence, even if it is collected from outside the jurisdiction of the court.

ISO/IEC 27037 being an internationally accepted standard is an important instrument to provide reliable standardised approach towards evidences and will have impact on admissibility and reliability of evidence in any court proceeding. It is therefore necessary that all ir must familiarise themselves with the bare minimum requirements which must be met in respect of handling of digital evidences to be court of the world. This can be very critical especially in handling issues related to terrorism, money laundering, drug trafficking and c crimes.

(The author is Head, IT Security, Essel Group)

Published Date: 18th November 2013, Image source: http://static.indianexpress.com

Post new comment

Your name: *

Anonymous

E-mail: *

The content of this field is kept private and will not be shown publicly.

Comment: *

Message*

Input format

I'm not a robot

reCAPTCHA
Privacy - Terms

Save Preview

Related Articles

Commentary : Australia Defines Priorities of National Securi

The Government of Australia, on May 1, 2018 (Australian Governmen

नीला हौज़ निर्मित झील प

22 मार्च, 'विश्व जल दिवस' क

The Future of Ba to China

China's rap become t largest econ

Commentary: The Neela Hauz Constructed Wetland System

22nd March is commemorated as 'World Water Day'. O

Commentary: International Solar Alliance - India's Radiant

On March 11 ,2018 India led the world into a new era of mutually

Commentary: So in Unmanned Op Tech

Propelled enabling co like all-weath

India should take up challenge of Lethal Autonomous Weapons

हंटर किलर से मौतें अपर
दुनिया के विभिन्न हिस्स

Commentary: Fi Attack has Happ
'We knew t coming' – sources are

About Us

The Vivekananda International Foundation (VIF) is a New Delhi-based think tank set up with the collaborative efforts of India's leading security experts, diplomats, industrialists and philanthropists under the aegis of the Vivekananda Kendra. The VIF's objective is to become a centre of excellence to kick start innovative ideas and thoughts that can lead ...

Read More

Contact Us

Name*

Email Id*

Phone Number*

Message*

I'm not a robot

reCAPTCHA
Privacy - Terms

Submit

Tweet With Us

VIF India
@vifindia
'The organs are the horses, the rein, the intellect is the charioteer the rider, and the body is the ch master of the household, the Ki of man, is sitting in this chariot.' #SwamiVivekananda