Val-Ed™

Valiant Technologies Education & Training Services

Workshop on Digital Evidence for IT / IS Auditors

Welcome to Valiant Technologies. We are a specialty consulting and training organization that focuses on information security at the strategic and operational levels. With significant strength also in information security assurance services, Valiant CISSTech, as were formerly known, has been serving clients across many countries - Bahrain, Hong Kong, India, Kuwait, Malaysia, Maldives, Saudi Arabia, Sri Lanka, South Africa, Sultanate of Oman, Thailand, United Arab Emirates, and Zambia.

Val-Ed™, our educational services division offers a variety of ready-packaged and tailor-made educational and training programs in the area of information security. This catalogue provides detailed information on one of the educational and training offering to clients in the area of information security technology, management and assurance.

We have a full range of services that we offer covering the full spectrum of information security and our services catalogue provides details of the following services that we provide to clients. Please ask for a services catalogue for more details on these services:

- Testing and hardening of information system defenses:
  - Vulnerability assessment
  - Penetration testing
  - Application security testing
  - Hardening of servers and network components
  - Periodic evaluation of network security
- Information Security Management Services
  - Security Policies, Procedures and Guidelines
  - Security Awareness Program
  - Risk Assessment and Analysis
  - Executive Management briefings on Security
  - Vendor selection for security products
  - Computer Forensics Investigation\
  - ISO-27001 preparatory services
  - Fill-in Security Manager program
- Control and Assurance Services
  - Gap analysis against ISO-27001, COBIT, ISSAF
  - Information security controls review
  - Information Systems Security Audit
  - Control assessment for SOX compliance
- Business Continuity and Disaster Recovery Management

We look forward to being of service to you and look forward to hearing your interest.

- Valiant Team

List of regular programs offered by Valiant Technologies

	Course Name	Duration (days)
1	Workshop for CISSP certification aspirants	4
2	Workshop for CISA certification aspirants	5
3	Workshop for CISM certification aspirant	4
4	Workshop for CBCP certification aspirants	5
5	Workshop for Security+ certification aspirants	6
6	Workshop on BCP and DRP	2
7	Workshop on Change Management	1
8	Workshop on Information Security Policies	3
9	Information Security for Senior Management	½
10	Security Awareness for IT user management	2
11	Ethical Hacking and securing your networks	6
12	Sarbanes Oxley Act – Structure and Implementation	2
13	Digital Evidence for IT / IS Auditors	1
14	IS Audit: Principles and Practices	3
15	ISO 27001: Process and Implementation	5
16	Auditing Information Technology	3
17	Management for Technology Professionals	3

CV of principal instructor, Dr. Rama K Subramaniam is found on the last page

One Day workshop on
DIGITAL EVIDENCE
for IT / IS Auditors

Background:

Digital Evidence is fast replacing traditional evidence in a number of scenarios; in forming audit opinion, in law enforcement activities and in the judiciary. Auditors who often are the first to lay their hands on digital evidence are called upon to assist law enforcement and judiciary in interpreting the digital evidence found in scenes that result in questionable transactions or in scenes that are clearly cases of cyber crimes. In this context, it is important for the auditors to understand the foundations of digital evidence, its nature, its current manifestations, and its acceptability in the context of common-law legal framework.

Auditors have had significant expertise developed over a long period of time, in identifying, collecting, analyzing, interpreting and presenting digital evidence in typical audit environments. While those skill sets will remain relevant and handy even where most transactions are electronic in nature and are also done on-line real time, the security infractions that have cut across networks have added newer dimensions to evidence to be collected in the case of security infractions. This evidence collected in scenes of electronic security infractions and crimes has been classified into two different categories – digital evidence and evidences that are the electronic equivalent of paper evidence. The latter include tape and discs containing the electronic version of manual documents and records while the former refers to the new breed of evidence that did not have an equivalent in the paper based system. For instance, the evidence pointing to a specific subject as being at the keyboard at the time of infraction, based on computational stylometric analysis has no equivalents in the pre-digital era.

The proposed workshop would consider digital evidence from different perspectives – in an audit setting; need for standards when it comes to digital evidence; techno-legal issues in digital evidence related issues and finally the process of determining authorship attributes when it comes to predicting the source of security infractions.

Duration:

One day with about seven hours of presentations. Tentative schedule as follows:

09.15 – 09.30: Registration and Inauguration

09.30 – 11.00: Technical Session – 1: Digital Evidence in an Audit Setting

11.00 – 11.15: Mid morning break

11.15 – 12.45: Technical Session – 2: Digital Evidence – Standards and Principles

12.45 – 13.45: Lunch break

13.45 – 15.00: Technical Session – 3: Techno-legal issues in collecting and interpreting Digital Evidence

15.00 – 15.15: Mid afternoon break

15.15 – 16.30: Technical Session – 4: Authorship attributes while interpreting Digital Evidence

16.30 – 17.00: Summing up and participants' interaction

Scope of presentations and discussions in the four technical sessions follow:

Session – 1: Digital Evidence in an Audit Setting

Digital Evidence is an emerging form of evidence to be gathered while investigating cyber security infractions and taking it to its logical conclusion of identifying the perpetrator. While it is broadly agreed that with the increase in cyber crimes, law enforcement and judiciary is moving more towards handling digital evidence, there are serious issues that thwart fitting of digital evidence into existing evidence framework. At a micro or organizational level, evidence that is the cornerstone on which a lot of audit opinions are built, is becoming more and more digital thus challenging auditors to adopt new methods of identification and interpretation of digital evidence.

This session would consider the various issues involved in generating and interpreting digital evidence in an audit setting and consider the issues that require to be addressed by the systems auditor when confronted with digital evidence.

Session – 2: Digital Evidence – Standards and Principles

In the process of collecting, analyzing, interpreting and presenting digital evidence, it becomes important that standards are set so that digital evidence related issues across multiple organizational and legal systems are consistent and verifiable.

Given the nature of digital evidence and its propensity to change without trace, the need for standardizing collection, preservation, transportation and presentation of digital evidence acquires importance.

This session will consider the guiding principles involved in the management of digital evidence and also look at the emergence of standards for Digital Evidence. In particular, this session will critique the work of SWEDGE and IOCE, moving on to determining their applicability to Indian context.

Session – 3: Techno Legal Issues in Collecting and Interpreting Digital Evidence

Due to its very nature, Digital Evidence poses challenges in the process of collection and interpretation. Since all evidence life cycles point towards presenting it for actionable results in organizations or in a court room, lot of work has been done on establishing the 'correct' process of collecting, preserving, transporting and presenting the evidence and go on to consider the final stage of returning the digital evidence to its owner; often the victims.

Various technical and legal issues have cropped up in the process of collecting and interpreting digital evidence – issues of commingled data, power failure and lack of DNR facilities, storage size and volatility of media holding evidence, logical and physical access controls over the evidence storage, proving the integrity of evidence and the concept of 'collection in the normal course of business' are some of the issues unique to digital evidence.

This session will consider the special issues related to collection of digital evidence form a techno legal perspective and discuss the current practices from the point of view of the technologist collecting the evidence, from the point of view of law enforcement that analyzes it from a legal perspective and from the point of view of judiciary that examines the evidence from the point of view of admissibility.

Session – 4: Authorship attributes while interpreting digital evidence

'Who was at the Keyboard' is often a question that is asked when efforts are made to determine who authored an incriminating message or document. It is a tough question to answer since pinpointing to some one without an iota of doubt is often impossible. A combination of physical and logical addressing is used to point to a specific person when he has to be held responsible for an action that is being challenged or is being used to prosecute a person. But the current generic implementation of networks does not permit this combination of physical and logical addressing to be used as fool-proof evidence; what with spoofed IP addresses and masqueraded MAC addresses and the scant respect we have for passwords as a form of authentication.

Researchers have found that authorship attributes using linguistic characteristics have produced accuracy ranges from 72 to 89 percent. A large number of researchers are now considering the adoption of computational stylometric methods that have reached accuracy levels of 95% and investigators are slowly but steadily leaning towards this technique to determine the perpetrator who was at the keyboard at the time of the offence. This session would examine the current approaches to the use of linguistic and computational stylometric methods in the interpretation of digital evidence.

Who should attend this workshop?

- IT / IS Auditors
- Information Technology and Information Systems Managers
- Internal Auditors
- Chief Information Officers and Chief Information Security Officers
- Corporate Security Managers
- Audit Managers in professional accounting and audit organizations
- Investigation Officers handling cyber crime cases
- Judicial officers handling cyber crime related matters
- Lawyers and other professionals involved in investigation of cyber crimes
- Criminologists and Criminology teachers
- Victimologists and victimology teachers
- Information Security Professionals
- Researchers in the area of cyber crime, criminology and victimology

What will you take back from this workshop?

- Good understanding of typical cyber crime scenes and the relevance of digital evidence in such a scenario
- Good foundation of digital forensic process and methods
-

Dr. Rama K Subramaniam

MBA(UK), PHD, FCA, CISA, CISM, CISSP, CEH, CHFI, CSQP, MCSE, Security+

He is Director of Valiant Technologies Pvt Ltd and Tejas Brainware Systems Pvt Ltd. He has been an information security consultant, trainer and educator for over a decade. He has trained experts in many information security domains across Gulf nations, India, Far East and Africa. He is a consultant to a number of organizations in the commercial, government, armed forces, judiciary and law enforcement segments in these countries.

He serves as India's country representative at International Federation of Information Processing (IFIP), serving on their Technical Committee TC-11 dealing with information security. He is current Chairman of ISCCRF, a not-for-profit trust carrying out research in cyber crime management

He is a certified and experienced professional in the areas of creating and implementing secure information security architecture; internal controls systems and processes; conceptualization, creation, testing and maintenance of business continuity and disaster recovery plans; security audits and certification of network infrastructure; conceptualization and implementation of multi-factor authentication processes (including PKI and X.509 compliant certification infrastructure); creation, assessment and certification of SOX, COSO, CoBIT, ISO-27001, ISO-17799 and ISO-15408 compliant information security management systems.

He served earlier as Global Chair of the Education and Awareness Principles Expert Group of Globally Accepted Information Security Principles (GAISP), based in the United States and is former Global Chair of the Accreditation Process committee of Open Information Systems Security Group (OISSG), based in the UK where he estblished their certification and accreditation processes. He is the charter President of the first chapter of ISSA (Information Systems Security Association) in Asia and served on the boards of Dubai and Chennai chapters of ISACA.

He was formerly Managing Director of Thewo Corporate Services based in Lusaka, Zambia; Group Operations Director or Benetone Group of Companies based in Bangkok, Thailand and Commercial Director of Dynaspede Integrated Systems Ltd, based in Mumbai.