The Analytics, Security & Forensics Company

CASE STUDIES

Aviation & Aerospace

1. IMS - Intelligent Medical System for NASA

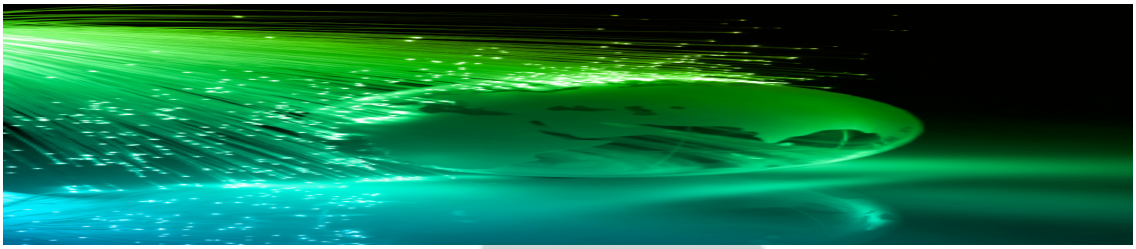

Figure - 1

The National Aeronautics and Space Administration (NASA) is faced with many difficult tasks supporting human life in space. Primary among these is the practice of medicine. A Mars mission will have communication delays of up to 40 minutes making emergency support difficult. Our design addresses long-term mission medical requirements by proposing a distributed intelligent system that can function as a stand-alone system for emergencies as well as function with the Earth-based NASA medical.

Finance

2. "Financial Services through a secure cloud platform"

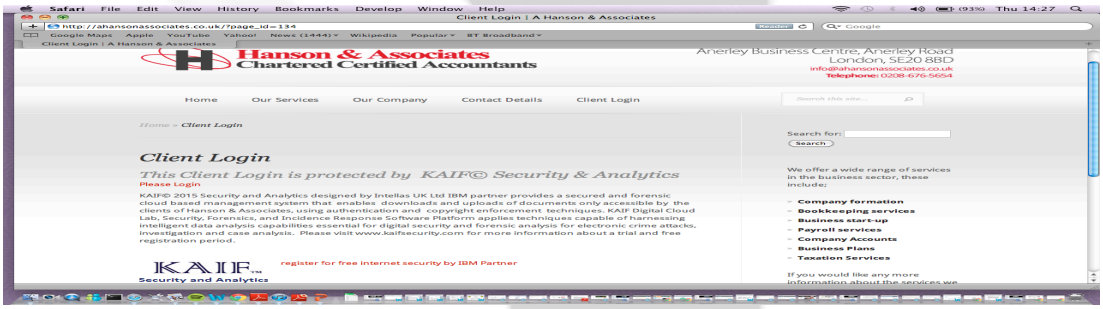

Figure 2 - Client Login and Logos of assurance to enable real time security monitoring

Implementation of multi-layered secured authentication and access control list for clients and service provider on a VPN (Virtual Private Network), and the implementation of KAIF® Logos of assurance on web page to enable real time analysis of network threats for all clients and service provider. The multi-layered authentication and access control list comprise the implementation of a user id and password system for all staff. The access control list defines access rights and privileges for users of the document management system.

Media

3. “Generating IP Revenue using Copyright Enforcement and Brand Protection”

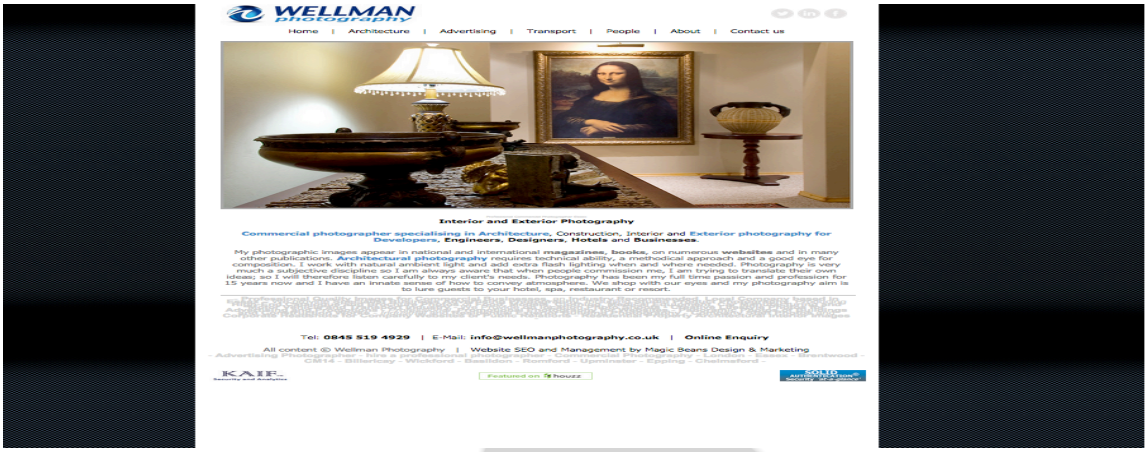

Figure - 3

Generating IP Revenue using Copyright Enforcement & Brand Protection Technologies Services provided by Intellas UK Ltd in conjunction with First Cyber Security Ltd. Enforcement of copyright protection using access control and encryption to prevent modification and non authorize use of original images. Implementation of watermarks to authenticate ownership rights for a wide range of images considered valuable.

Security

4. “Real Time Online Integrated Security & Analytics Platform ”

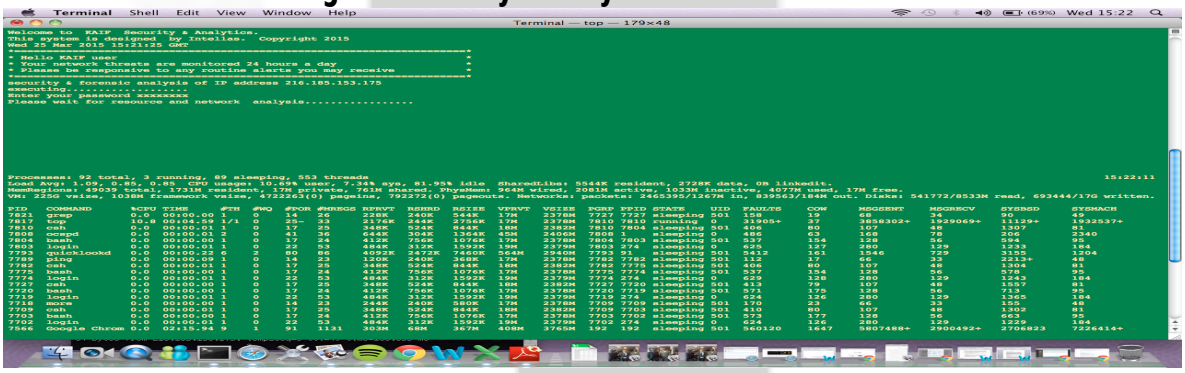

Figure 4

Figure 4 is an intelligence analysis of potential threats of how the entire computer system resources, such as memory dumps, disk space and communication networks have been or being used and exploited on the service platform. A penetration test is carried out to exploit vulnerable or risk access spots associated with the IP (Internet Protocol) address on the network server. The penetration testing comprises the test of robustness and capability within the service platform to withstand excessive flooding of packets deliberately or accidentally channelled to the server likely to bring it down. Packet analysis in this aspect of the work focuses on observing unusual patterns on the network and flagging alerts where necessary, and following up with recommendations for remedial action.