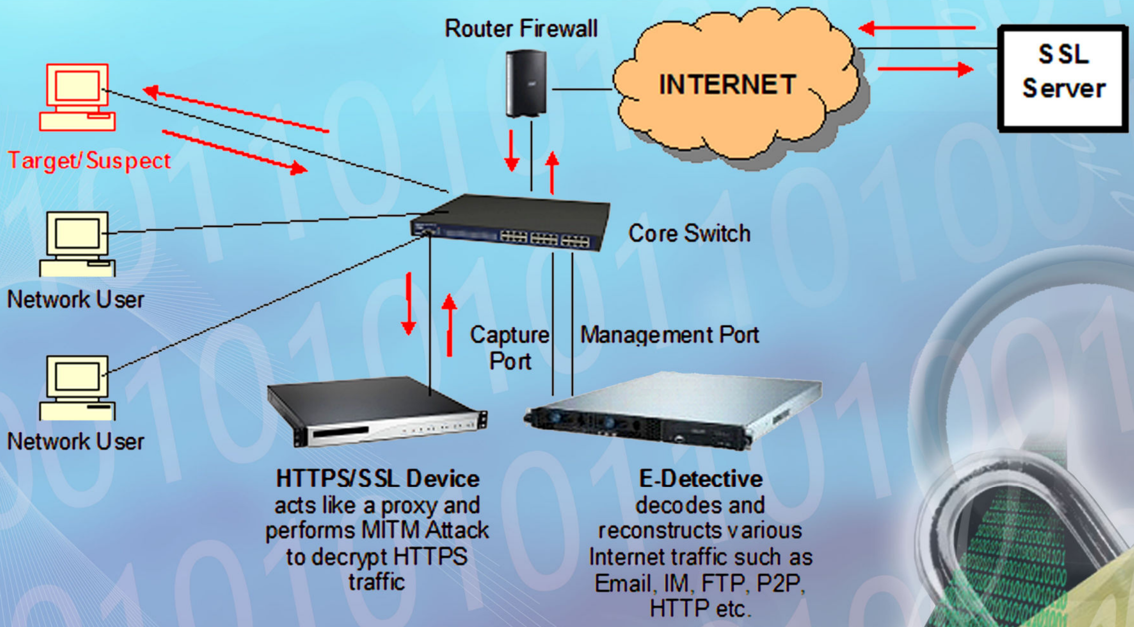
E-DETECTIVE

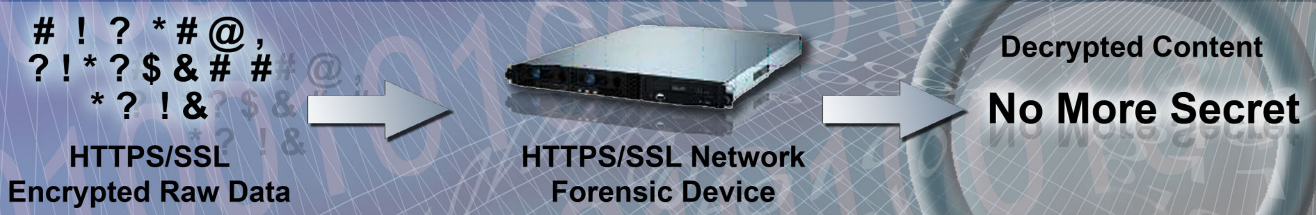
HTTP / SSL

Network Packet Forensics Device


Router Firewall
INTERNET
SSL Server
Target/Suspect
Core Switch
Network User
Network User
Capture Port
Management Port
HTTPS/SSL Device acts like a proxy and performs MITM Attack to decrypt HTTPS traffic
E-Detective decodes and reconstructs various Internet traffic such as Email, IM, FTP, P2P, HTTP etc.

Application Features:

- Decrypt and decode HTTPS network packets within the same network domain.
- Two application modes: 1. Online – Man-in-the-Middle (MITM) Attack; and 2. Offline Decryption (Decrypt HTTPS raw data packets with Private/Secret key known).
- In MITM Attack Method, it acts as proxy to the targeted user/PC (using ARP and DNS poisoning). The HTTP and HTTPS traffic between the targeted user/PC and SSL server can therefore be redirected to the HTTPS/SSL Network Packet Forensics Device. This will allow the HTTPS/SSL Device to decrypt the HTTPS traffic with genuine SSL certificate obtained.
- Login Username and password for HTTP and HTTPS websites such as Gmail, Yahoo Mail, E-Bay etc. can be extracted and obtained.


# ! ? *#@,
?!*?$&# #
*? !&
HTTPS/SSL Encrypted Raw Data
HTTPS/SSL Network Forensic Device
Decrypted Content
No More Secret

DECISION COMPUTER GROUP
Decision Computer International Co., Ltd. (HQ & RD)TAIWAN
Desicion Computer Pte Ltd. Singapore
Decision Computer Juergen Merz e.k. Germany

Website : www.edecision4u.com, www.ed-system.sg
HQ. Address : 4/F No.31, Alley 4, Lane 36, Sec. 5,
Ming-Shan East Rd, Taipei, Taiwan ROC.
Phone : +886 227665753 Fax : +886 227665702
Email : decision@decision.com.tw, decision@ed-system.sg