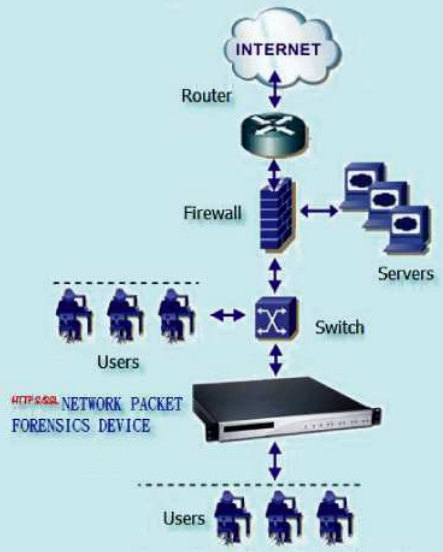
E-DETECTIVE®

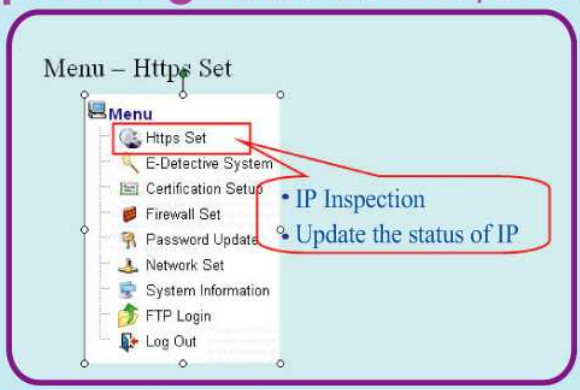
HTTPS/SSL NETWORK PACKET FORENSICS DEVICE

Features：

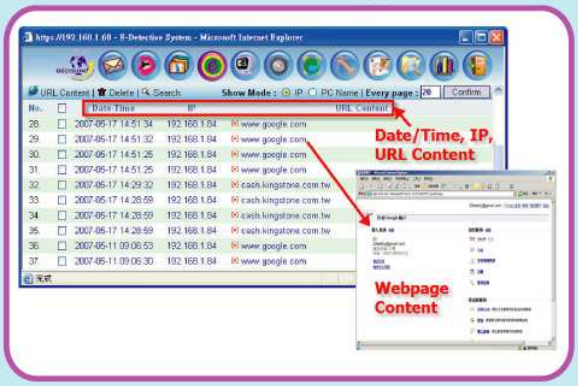
- Decrypting HTTPS network packets existed within the same domain.
- This system pretends as a gateway to obtain public keys (Decryption/Encryption keys) by cheating when the data is transferred via Internet in order to decrypt the information.
- Able to Cooperate with SSL server and obtain its public keys in order to decrypt all data related to this SSL server.
- The primary auditing feature is able to be integrated with E-DETECTIVE system and its database, in order to exchange/decode/analyze the data.
- Gmail and bank online transactions are not secured anymore.



Operating Manual： Https Set



The decrypted content



Glossary

a: SSL (Secure Sockets Layer): A Technical Security Standard to secure the safety of Internet packets transmitting between server and browser. SSL is an Enterprise Standard adopted by millions of websites to safeguard their on-lined transaction. It ensures the privacy and integrity of transmitted data during the transaction process. Each web server requires one SSL certificate to protect its safety of linkage.

b: HTTPS is the safeguarded version of HTTP to securing the safety of transmitted data. Engaged with SSL layer, the transmission of data for HTTP is fully protected to form a secured base of HTTPS. HTTPS is a combination of HTTP and SSL. It does not use the HTTP's Port and is able to certify authorization of each Internet packet（Between the HTTP and the TCP）. HTTPS was originally developed by Netscape, it provides ways to certify authorizations and encrypts the communication. SSL is often used for E-Commence System such as online payment.