

# Network Forensics

**Università degli Studi di Pisa**  
**Facoltà di Ingegneria Informatica**  
**Magg. CC Ing. M. Mattiucci**

[www.marcomattiucci.it](http://www.marcomattiucci.it) - Pisa, 18 e 19 dicembre 2006

## Sintesi dell'intervento

*A cura del Magg. CC Ing. Marco Mattiucci - Roma, 2 gennaio 2007*

A seguito della conferenza del 5 maggio 2006 tenuta dallo scrivente presso la stessa Facoltà (<http://www.marcomattiucci.it/seminari-conferenze.php>) è stato organizzato un seminario intensivo di due giorni sul network forensics per gli studenti dell'ultimo anno di Ingegneria Informatica – corso di sicurezza delle reti.

Il seminario, svoltosi presso un laboratorio informatico della Facoltà specificamente predisposto dal Prof. Gianluca Dini e dal suo collaboratore l'Ing. Silvio La Porta, ha permesso agli studenti un primo approccio al mondo tecnico-legale che sottende le investigazioni high tech, provando praticamente diverse esercitazioni specifiche e simulazioni.

Gli argomenti trattati sono stati i seguenti:

- Breve introduzione al Reparto Tecnologie Informatiche dell'Arma quale organo interno al RaCIS (investigazioni scientifiche) deputato alla trattazione e ricerca nei settori criminali high tech;
- Differenza ed analogie tra *network security* e *network forensics*;
- Il *digital forensics* in generale;
- *Internetworking*: rapida rassegna dei concetti di base quali indirizzi IP, classi pubbliche e private, MAC address e MAC, ipconfig, DHCP,

- lease time, whois service, URI, URL, DNS, ping, netstat, telnet + esercitazioni pratiche di laboratorio;
- *Email*: rapida rassegna di SMTP, POP, IMAP, MUA, MTA, MDA, MIME, envelope, header, body per poi passare ad una serie di esercizi di tracciamento prima su email preparate e poi su spam;
  - *Web*: rapida rassegna di www, html, http, https, ssl, tls, sniffing con esercitazioni sullo sniffing base di password e sul repertamento dei siti web a scopo legale;
  - *Anonimato* su Internet: concetto di proxy e le varie forme di anonimato passate in rapida rassegna – mobile, wireless, misconfigured proxy, anonymous proxy, botnet, ecc. con vari esercizi di tracciamento reciproco tra i partecipanti;
  - *P2P*: cenno a protocolli, client e metodi/problematiche di indagine (Gnutella, FastTrack, FreeNet, ED2K, BitTorrent, ecc.);
  - *IRC, Instant Messaging, BBS & virtual communities*: cenno.

Gli studenti, grazie ad una discreta preparazione di base, hanno potuto seguire il seminario con profitto nonostante gli argomenti incalzassero velocemente e gli esercizi premessero per una risoluzione veloce spesso non semplice. Lo scopo era ovviamente quello di simulare la tipologia di stress cui un tecnico informatico forense è sottoposto nella suo tentativo di risolvere sempre nuovi casi.