Progetti Sicurezza

Alfredo De Santis
Dipartimento di Informatica
Università di Salerno

ads@dia.unisa.it
http://www.dia.unisa.it/professori/ads

Marzo 2012

Progetti

- Non sono obbligatori
- Gruppi di 2 – 4 studenti
- Disponibilità a lavorare per terminare entro luglio 2012
- In genere contengono una parte sperimentale
- Anche tematiche di carattere più teorico
  (Comunicare al docente eventuale interesse)
- E' possibile proporre progetti (con motivazioni)

Progetti di Digital Forensic 2011

- Windows Forensics (Valerio Cinque, Francesco Testorio, Andrea Di Maio)
- Falso alibi digitale su Windows 7 (Alessandro Bove, Alfonso Martorelli, Giuseppe Valentino, Luigi Di Biasi)
- Distribuzioni Linux per analisi forense (Helix 3, DEFT Linux 6, CAINE, Backtrack)
  - Live forensic (Mario Fiore Vitale, Fabio Fulgido, Gaetano Rocco)
  - Post-mortem forensic (Umberto Annunziata, Claudio Gargiulo)
- Linux Forensics (Domenico Viscito, Fabio Favale)
- Falso alibi digitale su Linux (Antonio Sanfelice, Sara Cantalupo, Demia Massaro, Giovanni Costa)
- iPod ed iPhone Forensics (Giovanni Mastroianni, Luisa Siniscalchi, Domenico Voto)
- Android Forensics (Davide Barbuto, Francesco Capano, Gaetano Contaldi, Andrea Vallati)
- Image Forensics (Giuseppe Lanzilli, Hamza Hamim, Gianluca Roscigno)
- GPS Navigation Devices Forensics (Ermanno Travaglino, Armando Faggiano)
- Investigazione di un Computer (Alessio Marzaioli, Francesco Pisano)
- Network Investigations (Dario Casciello, Domenico Memoli, Antonio Della Sala)

http://www.dia.unisa.it/professori/ads/ads/Sicurezza.html

Progetti di Digital Forensic 2012 (prima bozza)

- iDevice Forensics
- Android Forensics
- GPS Navigation Devices Forensics
- Mac OS X Forensics
- Falso alibi digitale su Mac Os X
- Network Investigations
- Anomaly Detection (IDS e IPS)
- …

Organizzazione

- Deliverables:
  - Progetto (Word/LaTex + materiale eventuale di supporto)
  - Presentazione (Powerpoint)
  - Pubblicazione versioni pdf sul web
- Chiarezza espositiva
- Approccio top-down
- Struttura progetto:
  - Titolo, nomi (prima pagina)
  - Indice
  - Introduzione
  - Sezioni e sottosezioni
  - Bibliografia
  - Appendici (eventuali)
- Organizzazione interna al gruppo di lavoro
  - Decisa in autonomia, poi resa pubblica

Stati di avanzamento e tempi

- Dopo un mese
  - bozza che include indice, struttura, introduzione, referenze
  - Presentazione 20/30 min
- Dopo due mesi e mezzo
  - versione finale
  - Presentazione 60/90 min

Indicare esplicitamente l'organizzazione interna del gruppo

Collaboratori

- Dott. Aniello Castiglione
  - castiglione@ieee.org
- Dott. Ugo Fiore
  - ugo.fiore@unina.it
- Dott. Giancarlo De Maio
  - demaio@dia.unisa.it

Agenda

- Digital Forensic
  - 7, 8 e 9 marzo 2012
- Network Investigation and Anomaly Detection
  - 14 (P13) – 15 (F/1) – 21 (P13) marzo 2012
  - Dott. Ugo Fiore
- Digital Forensic: laboratorio
  - 16 (F/1) marzo
  - Dott. Aniello Castiglione
  - Dott. Giancarlo De Maio
- Lista progetti, lista gruppi e matching (non necessariamente totale)
  - 22-23 marzo

Eventi

- Reati Informatici
  - Avv. Mario Ianulardo
- Digital Forensics: esperienze sul campo
  - Dott. Nicola Jarno Masone, Polizia Giudiziaria
- IISFA Forum & Cybercop Challenge 2012
  - International Information System Forensics Association
  - 18 e 19 maggio 2012, Castello Arechi, Salerno

Fonti

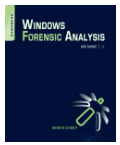
- Fonti autorevoli
- Preferibili libri ed articoli pubblicati su riviste e conferenze scientifiche
- Vediamo qualche esempio

Windows

Eoghan Casey,
Digital Evidence & Computer Crime
Second Edition, 2004, Academic Press
Chapter 10 Forensic examination of Windows Systems

Handbook of Digital Forensics and Investigation
2010, Academic Press
Chapter 5. Windows Forensic Analysis

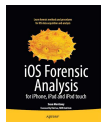
Harlan Carvey
Windows Forensic Analysis DVD Toolkit,
2nd edition, 2009, Syngress



Mac, iPhone, Linux

Mac OS X, iPod, and iPhone Forensic Analysis Toolkit,
Syngress Publishing, 2009

Sean Morrissey,
iOS Forensic Analysis for iPhone, iPad, and iPod touch,
apress, 2010



Handbook of Digital Forensics and Investigation,
Elsevier, 2010

- Chapter 6. UNIX Forensic Analysis
- Chapter 7. Macintosh Forensic Analysis

Network Investigations

Handbook of Digital Forensics and Investigation,
Elsevier, 2010

- Chapter 9. Network Investigations

Android Forensics

Andrew Hoog,
Android Forensics
Syngress, July 2011

Jeff Lessard, Gary C. Kessler,
Android Forensics: Simplifying Cell Phone Examinations,
Small Scale Digital Device Forensics Journal, vol. 4, n. 1, Sept. 2010

GPS Navigation Devices Forensics

Chad Strawn,
Expanding the Potential for GPS Evidence Acquisition,
Small Scale Digital Device Forensics Journal, vol. 3, n. 1, June 2009

Tchatchoua Nkwenja Mathia
The Forensic examination of Embedded device such Global Position System (GPS)
Tesi, University of Wales, Newport, UK, 30 April 2009
http://ril.newport.ac.uk/Mathias/finalYrProGPSForensicsExamination.pdf

Clara Maria Colombini,
Sperimentazione di un metodo di analisi forense del dispositivo di navigazione satellitare TomTom,
http://www.iisfa.net/index.php?option=com_docman&task=doc_download&gid=19&Itemid=40

GPSForensic.org
http://www.gpsforensics.org/