PERSONAL INFORMATION

Francesco PICASSO

WORK EXPERIENCE

02/2013 – Present

Partner, Digital Forensics & Incident Response specialist

Reality Net System Solutions, via Ceccardi 1/20, 16122, Genoa, Italy, www.realitynet.it

DFIR and Security Specialist

- Performing Digital Forensics and Incident Response for private companies
- Supporting LEA and Prosecutors in Digital Investigation cases
- Research & Development on Computer, Memory and Mobile Forensics
- SANS FOR508 Instructor
- Digital Forensics specialization path within the “Master in Cybersecurity” organized by Università degli Studi di Genova, Instructor from 2015

03/2020 – Present

Contract Professor at Genoa University – Computer Science

- Class: Digital Forensics
- https://unige.it/off.f/2019/ins/37976

01/2009 – 01/2014

Information Security and Digital Forensics Consultant

Self Employed

Information Security, Network Security, Digital Investigations:

- As digital forensics consultant, I was involved in many investigations, mainly working for prosecutors, law enforcements and privatecompanies.
- As an information security consultant, I focused on improving network security defenses for private companies.

01/2006 – 12/2008

Ph.D. Student in "Intelligent Electronics for Security"

SEA Lab (Smart Embedded Application Laboratory), DIBE, University of Genoa

- Thesis: "Method for detecting anomalies in a communication network and network device that implements such method" (Patent 1396756, 14 December 2012, Italy).
- Research activities: Network Security, Digital Investigations, Anomaly Based Intrusion Detection Systems, Pattern Recognition, Data Mining, Information Retrieval, Cryptography.
- [2008] Won the Elsag Datamat 2008 Innovation Prize with the project "Fast Locomotor: Fast log correlation motor".
- [2008] In charge of the research contract "Intelligent methods for the protection of wide computers networks", commissioned by Ansaldo STS Spa.
- [2007] In charge of the research contract “Design and development of smart technologies for network security”, commissioned by Ansaldo STS Spa.
- [2006] Head of “Electronic Systems for Information Security” course for the Electronic Engineering Degree, II° year specialist.

09/2002 – 12/2005 **Software Engineer**

IFM Infomaster Spa, www.ifminfomaster.com

- Design and developing of ISDN stack, SIP stack, VoIP applications; integration with external applications and hardware, mainly on Intel/Dialogic platform; design and development of CTI software.
- Support to marketing and sales departments for VoIP projects; customer assistance for projects involving VoIP architectures and integration and call center operations; designing and developing network security.
- Programming Languages: mainly C++, C, C#

01/2001 – 09/2002 **IT Instructor, Consultant**

ISVAP Sas, Via Puggia 27/2, 16121, Genoa, www.isvap2000.it

- Held courses on Network and Information Security for Italian Navy V.T.S. (Vessel Traffic Service) National program.

01/1999 – 12/2000 **IT Instructor, Consultant**

Wall Street Institute, Genoa

- Held courses on Computer Programming and Windows OS.

01/1994 – 12/1998 **Junior Software Developer, Consultant**

Trecision Spa, Rapallo, Genoa, http://en.wikipedia.org/wiki/Trecision

- Videogames. Programming languages: C, Assembly.

EDUCATION AND TRAINING

10/2017 **SANS FOR610: Reverse Engineering Malware**

SANS Institute, Prague 2017

02/2016 **SANS SEC511: Continuous Monitoring and Security Operations**

SANS Institute, Munich 2016

10/2015 **SANS FOR585: Advanced Smartphone Forensics**

SANS Institute, Prague 2015

10/2014 **SANS FOR572: Advanced Network Forensics and Analysis**

SANS Institute, Prague 2014

06/2014 **SANS SEC504: Hacker Tools, Techniques, Exploits and Incident Handling**

SANS Institute, Milan 2014

10/2013 **SANS FOR526: Memory Forensics In-Depth**

SANS Institute, Prague 2013

04/2013 **SANS SEC401: Security Essentials Bootcamp Style**

SANS Institute, Amsterdam 2013

02/2009 **SANS FOR508: Computer Forensics, Investigation, and Incident Response**

SANS Institute, Milan 2009

05/2008 **IISFA Intensive 2 days course on Computer Forensics**

IISFA (International Information Systems Forensics Association), Rome 2008

01/2008 – 03/2008 **Postgraduate Specialization Course in Computer Forensics and Digital Investigation**

University of Milan, Milan, Italy

01/2006 – 12/2008 **Ph.D. in Electronic Systems for Information Security**

University of Genoa, Genoa, Italy

- Final Thesis and Patent in 2010. "Method for detecting anomalies in a communication network and network device that implements such method"

09/2007 **FOSAD: Foundations of Security Analysis and Design**

Ph.D. Summer School at International School on Foundations of Security Analysis and Design, Bertinoro Italy

- API Security and Security Economics, Application of Formal Methods to Cryptographic Protocol Analysis, Trusted Mobile Platforms, Language-Based Security, Cryptographic Algorithm Engineering and Provable Security, Embedded Systems Security and Cryptographic Coprocessors, Quantitative Aspects in the Analysis of Cryptographic Protocols.

11/2006 **Amtec Network Professional (EC-ANP)**

Elsag Datamat – EXCITE Security Department, www.elsagdatamat.com

- Networking, Routing, Amtec devices

06/2006 **Amtec Security Professional (EC-ASP)**

Elsag Datamat – EXCITE Security Department, www.elsagdatamat.com

- Physical Security, Security Governance, Network Security, Amtec devices

07/2005 **Master of Science in Computer Engineering**

University of Genoa, Genoa, Italy

- Thesis title: “Software Architecture for Digital Signature Applications”.

PERSONAL SKILLS

Languages

Italian: Mother tongue
English: Proficient user (C1 level)

Communication skills

Good communication skills gained through interaction with professionals and researchers. Experience in reporting to non-technical people gained as an Expert Witness. Nonverbal communication, friendliness, empathy, listening.

Organisational / managerial skills

Focus and timeline oriented. Critical and creative thinking.

Other skills Cooking, childcare.

Driving licence European driving licence A and B.

ADDITIONAL INFORMATION

Professional Certifications

GMON – GIAC Continuous Monitoring Certification
GCFA – GIAC Certified Forensic Analyst
GCIH – GIAC Certified Incident Handler
CIFI – Certified Information Forensics Investigator
ECCE – European Certificate on Cybercrime and Electronic Evidence
EC-ANP – Amtec Network Professional
EC-ASP – Amtec Security Professional

Publications

Patent

Debertol D, Meda E, Picasso F, Tamponi A, Zunino R,
"**Metodo di rilevazione di anomalie in una rete di comunicazione e dispositivo di rete che implementa tale metodo**" ("**Method for detecting anomalies in a communication network and network device that implements such method**"), Patent 1396756, 14-12-2012, Italy.

Specialized magazines

Mattia Epifani, Francesco Picasso
"**Windows Phone 8 Forensics**"
Digital Forensics Magazine, Issue 27, May 2016

"**Api Hooking con il Portable Executable**" ("**Api Hooking with Portable Executable**")
Computer Programming N° 107 – Nov. 2001 – Italy.

Book Chapter

Mattia Epifani, Francesco Picasso, Claudia Meda
"**Apple Tv Forensics**"
IISFA Memberbook 2016

Mattia Epifani, Francesco Picasso
"**Windows Phone 8 Forensics**"
IISFA Memberbook 2015

Meda C, Epifani M, Sangiacomo F, Picasso F, Zunino R,
"**Windows 8 Forensics**",
IISFA Memberbook 2013.

Gastaldo P, Picasso F, Corchado E, Herrero A, Zunino R,
"**Computational-Intelligence Models for Visualization-based Intrusion Detection Systems**",
In Bajo J, Corchado ES, Herrero A, Corchado JM (Eds) Hybrid Artificial Intelligent Systems (HAIS 2006), Universidad Salamanca, pp. 81-88 P.

Conferences

Gastaldo P, Picasso F, Zunino R, Corchado E, Herrero Á,
"**Nonlinear Projection Methods for Traffic Monitoring and Intrusion Detection in Computer Networks**",
11th International Conference on Knowledge-Based and Intelligent Information & Engineering Systems, KES 2007.

Herrero Á, Corchado E, Gastaldo P, Leoncini D, Picasso F, Zunino R,
"**Intrusion Detection at Packet Level by Unsupervised Architectures**",
8th International Conference on Intelligent Data Engineering and Automated Learning (IDEAL)

2007.

Ferraresi S, Francocci E, Quaglini A, Picasso F,
"**Security Policies Tuning among IP Devices**",
11th International Conference on Knowledge-Based and Intelligent Information & Engineering Systems, KES 2007.

Gastaldo P, Parodi G, Picasso F, Zunino R,
"**Embedded public-key cryptosystems via enhanced Montgomery multiplication**",
IEEE Int.Symp. Industrial Electronics - ISIE 2007, Vigo, Spain.

Herrero A, Corchado E, Gastaldo P, Leoncini D, Picasso F, Zunino R,
"**Unsupervised Connectionists Models for Intrusion Detection Systems**",
8th Int.Conf. Intelligent Data Engineering and Automated Learning IDEAL'07, Birmingham, Springer LNCS 4881, pp.718-727.

Gastaldo P, Picasso F, Zunino R, Herrero Á, Corchado E, Sáiz JM,
"**IDS Based on Bio-Inspired Models**",
11th Int. Conf. Knowledge-Based & Intelligent Information & Engineering Systems - KES2007, Springer, Lecture Notes in Artif.Intell. #4693, pp. 133-140.

Corchado E, Herrero A, Gastaldo P, Picasso F, Zunino R,
"**Auto-Associative Neural Techniques for Intrusion Detection Systems**",
IEEE Int.Symp. Industrial Electronics – ISIE 2007, Vigo, Spain, pp. 1905-1910.

Picasso F, Meda E, De Domenico A, Mazzaron P, Mazzino N, Tamponi A,
"**SeSaR: Security for Safety**",
Proceedings of the International Workshop on Computational Intelligence in Security for Information Systems, Advances in Soft Computing, CISIS 2008.

Nilsson D, Larson U, Picasso F, Jonsson E,
"**A first simulation of Attacks in the Automotive Network Communications Protocol FlexRay**",
Proceedings of the International Workshop on Computational Intelligence in Security for Information Systems, Advances in Soft Computing, CISIS 2008.

Honours and Awards

DFRWS EU 2015 Forensics Rodeo
1st place team, Digital Forensics Research Workshop Dublin 2015

SANS Lethal Forensicator Coin
2nd place in the DFIR NETWAR, SANS Prague 2014

SANS Pen Testing Coin 504
Final course challenge, SANS SEC504, Milan 2014

SANS Lethal Forensicator Coin
Windows Memory Forensics In-Depth (FOR526, instructor Jesse Kornblum) individual award
SANS Prague 2013

SANS Lethal Forensicator Coin
3rd place in the DFIR NETWAR, SANS Prague 2013

Elsag Datamat 2008 Innovation Prize
Won the Elsag Datamat 2008 Innovation Prize with the "Fast Locomotor: Fast log correlation motor" project.

Conferences and Seminars

Samsung (un)Secret Zone
SANS DFIR Summit, Prague 2017

Plaso2DFAX
EVIDENCE (Project FP7-SEC-2013-1 Grant Agreement No. 608185 Collaborative Project)

European Informatics Data Exchange Framework for Courts and Evidence
The Hague, September 2016

Life on Clouds, a forensics overview
DFRWS Lausanne, March 2016

Discovering Windows Phone 8 artifacts and secrets
DFRWS Lausanne, March 2016

ReVaulting! Decryption and opportunities
SANS DFIR Summit, Prague 2015

Tor Browser Forensics On Windows OS
DFRWS Dublin, March 2015

Forensics Readiness and Incident Response
Security Summit, Milan, March 2015

Give me the password and I'll rule the world
SANS DFIR Summit, Prague 2014

From Mimikatz to DPAPI
SANS@Night, SANS Milan 2014

Soup of the day (*Original Italian Title: "Piatto del giorno"*)
HackInBo, Bologna, May 2014

Encryption, anonymity and wiping: antiforensics techniques and methods of analysis
(*Original Italian Title: " Cifratura, anonimato e wiping tecniche di antiforensics e modalità di analisi"*)
IISFA Forum & Cybercop, Naples, May 2013

Mobile forensics, acquisition and analysis (*Original Italian Title: " Mobile forensics, acquisizione e analisi forense di tablet, cellulari e smartphone"*)
Security Summit, Milan, March 2013

Digital Investigations in criminal proceedings
(*Original Italian Title: "Le Consulenze Tecniche nei Procedimenti Penali"*)
Post graduate course "Computer forensics and digital investigations", University of Milan, 2013

Digital Forensics on web pages, emails and chat log files
(*Original Italian Title: "La pagina web, il messaggio di posta elettronica e i file di log di conversazioni o chat: corretta gestione, acquisizione e produzione nel giudizio penale, nel giudizio civile, nel diritto di famiglia e in ambito stragiudiziale"*)
Post graduate course "Computer forensics and digital investigations", University of Milan, 2012

How to protect against new threats? (*Original Italian Title: "Come difendersi dalle nuove minacce informatiche?"*), Genoa Engineering Society, Seminar on "Cyber Attacks: new threats and new defenses", Chiavari, March 2012

A proper legal and technical approach to the science of Digital Investigations (*Original Italian Title: "Un Corretto Approccio Giuridico e tecnico alla scienza delle Investigazioni Digitali"*)
Post graduate course "Computer forensics and digital investigations", University of Milan, 2011

Computer Forensics
Lecturer at Master in "ICT&S. ICT e Sicurezza, per l'innovazione dei contesti produttivi e lo sviluppo di nuovi mercati" (code DPU09MASTER1000/1/1), Genoa University, June 2010

Projects and Blogs

Zena Forensics blog: Creator, owner and main contributor, http://blog.digital-forensics.it
GitHub: Open source tools, scripts and plugins, https://github.com/dfirfpi, https://github.com/realitynet. Usually sharing night research activities by twitter @dfirfpi and by blog posts.