PERSONAL INFORMATION

Mattia Epifani

Sex | Date of birth 04/10/1977 | Nationality

WORK EXPERIENCE

06/2002 – Present

Partner and Digital Forensics Specialist at REALITY NET – System Solutions Snc

Via Ceccardi 1/20 – 16121 Genova – Italy

- Digital Forensics and Incident Response - Senior Consultant
  - Expert Witness for different courts in Italy
  - Technical consultant for private companies, law firms and private sectors
- Mobile Security Analyst
- SANS Certified Instructor courses FOR500 and FOR585
  https://www.sans.org/profiles/mattia-epifani/

Business or sector IT Forensics and Security

10/2014 – 3/2022

Contract Researcher at CNR-IGSG

Firenze – Italy

- Research activities in three EU funded projects
- EVIDENCE Project (http://www.evidenceproject.eu/)
- EVIDENCE2E-CODEX Project (https://evidence2e-codex.eu/)
- INPSECTR Project (https://inspectr-project.eu/)

Business or sector IT Forensics

3/2020 – Present

Contract Professor at Università degli Studi di Genova

Genova - Italy

- Contract professor in Digital Forensics
- https://rubrica.unige.it/personale/UkJFUl9g

Business or sector IT Forensics

EDUCATION AND TRAINING

01/2024

GIAC Battlefield Forensics and Acquisition (GBFA)

Global Information Assurance Certification

- Efficient data acquisition from a wide range of devices
- Rapidly producing actionable intelligence
- Manually identifying and acquiring data

08/2023

GIAC iOS and macOS Examiner (GIME)

Global Information Assurance Certification

- Mac and iOS File Systems, System Triage, User and Application Data Analysis
- Mac and iOS Incident Response, Malware, and Intrusion Analysis
- Mac and iOS Memory Forensics and Timeline Analysis

06/2022

SANS Course – Ransomware for Incident Responders

Global Information Assurance Certification

- Ransomware Incident Response Fundamentals
- Ransomware Modus Operandi
- Advanced Ransomware Concepts

01/2021 **GIAC Open Source Intelligence (GOSI)**
Global Information Assurance Certification

- Dark Web
- General Data Collection
- Government and Enterprises
- Network Data
- OSINT Foundations
- OSINT Frameworks and Tools
- Social Media

09/2020 **SANS Course - Open-Source Intelligence (OSINT) Gathering and Analysis**
OnDemand

06/2017 **GIAC Certified Forensic Examiner (GCFE)**
Global Information Assurance Certification

- Analysis and Profiling of Systems and Devices
- Analysis of File and Program Activity
- Acquisition, Preparation and Preservation of Digital Evidence
- Analysis of User Communications
- Analysis of Windows System User Artifacts
- Fundamental Digital Forensics
- Host and Application Event Log Analysis
- Microsoft Browser Forensics
- Third Party Browser Forensics and Browser Artifact Analysis
- Windows Registry Artifact Analysis
- Windows Registry Fundamentals

02/2016 **SANS Course - Windows Forensic Analysis (FOR408)**
Munich

01/2017 **GIAC Advanced Smartphone Forensics (GASF)**
Global Information Assurance Certification

- iOS Forensic Fundamentals
- Additional Mobile Operating System Forensic Fundamentals
- Android File System, Evidence Locations and User Activity Analysis
- Android Forensic Fundamentals
- Detection and Analysis of Mobile Malware and Spyware
- Fundamentals of BlackBerry Forensics
- Introduction to Smartphone Forensics
- iOS File System, Evidence Locations and User Activity Analysis
- Smartphone Application Forensics and Activity Analysis
- Smartphone Backup Forensic Analysis

06/2016 **GIAC Certified Windows Security Administrator (GCWN)**
Global Information Assurance Certification

- Defensible Networking
- Endpoint Protection
- Operating System and Applications Hardening
- PKI Management
- Restricting Administrative Compromise
- Securing PowerShell

02/2016 **SANS Course - Securing Windows and PowerShell Automation (SEC505)**
Munich

05/2015 **SANS Course - Advanced Smartphone Forensics (FOR585)**
Amsterdam

02/2015 **GIAC Network Forensics Analyst (GNFA) Certification**
Global Information Assurance Certification

- Common Network Protocols
- Encryption and Encoding
- NetFlow Analysis and Attack Visualization
- Network Analysis Tool and Usage
- Network Architecture
- Network Protocol Reverse Engineering
- Open-Source Network Security Proxies
- Security Event and Incident Logging
- Wireless Network Analysis

10/2014 **SANS Course - Advanced Network Forensics and Analysis (FOR572)**
Prague

08/2014 **GIAC Reverse Engineering Malware (GREM) Certification**
Global Information Assurance Certification

- Analysis of Malicious Document Files
- Analysing Protected Executables
- Analysing Web-Based Malware
- Common Windows Malware Characteristics in x86 Assembly
- In-Depth Analysis of Malicious Browser Scripts
- In-Depth Analysis of Malicious Executables
- Malware Analysis Using Memory Forensics
- Malware Code and Behavioral Analysis Fundamentals
- Windows x86 Assembly Code Concepts for Reverse-Engineering

04/2014 **SANS Course - Reverse-Engineering Malware: Malware Analysis Tools and Techniques (FOR610)**
Munich

02/2014 **GIAC - Certified Forensic Analyst (GCFA) Certification**
Global Information Assurance Certification

- File Carving and Data Extraction
- Filesystem Structure and Analysis
- Forensic Image Acquisition, Preservation, and Handling
- Incident Response and Forensic Framework
- Indicators of Compromise and Malware Detection
- Timeline Analysis
- Volatile Data Analysis
- Volatile Data Preservation and Collection
- Windows File System Artifacts

10/2013 **SANS Course - Advanced Digital Forensics and Incident Response (FOR508)**
Prague

08/2013 **GIAC Mobile Device Security Analyst (GMOB) Certification**
Global Information Assurance Certification

- Android Essentials and Device Management
- Application Network Activity Analysis
- Blackberry Essentials and Device Management
- iOS Essentials and Device Management
- Mobile and Wireless Infrastructure Attacks
- Mobile Device Penetration Testing
- Mobile Web Application Attacks
- Operational Security for Mobile Devices
- Securing Mobile Devices in the Enterprise
- Static Application Analysis
- Traffic Manipulation Attacks
- Unlocking Mobile Devices
- Windows Phone Essentials and Device Management

06/2013 **SANS Course - Mobile Device Security and Ethical Hacking (SEC575)**
Berlin

03/2013 **SANS Course - Memory Forensics in Depth (FOR526)**
Orlando (USA)

01-05/2009 **Corso di Perfezionamento in Computer Forensics e Investigazioni Digitali**
Università degli Studi di Milano (Italia)

Post-Laurea Specialization Course in Computer Forensics and digital investigations forensic and digital strategies and techniques of the computer disaster management

12/2008 **Ec-Council Computer Hacking Forensic Investigator (CHFI) Certification**
Ec-Council Institute

09/2008 **Ec-Council Certified Ethical Hacker (CEH) Certification**
Ec-Council Institute

09/2008 **Certified Ethical Hacker and Computer Hacking Forensic Investigator Boot Camp**
NetCom Information Technology - 350 Fifth Avenue - New York, NY 10118

01-09/2004 **Master (1° level) in Business Administration Control in Modern Enterprise**
SOGEA – Scuola di Formazione Aziendale

- Balance Analysis and Retraining
- Investment Analysis and Assessment
- Strategic Financial Management
- Cost Control
- Budget
- Operating Financial Management
- Management Report

10/1996-04/2002 **Computer Science Degree**
Università degli Studi di Genova
Dipartimento di Informatica e Scienze dell'Informazione
via Dodecaneso, 35 – 16146 Genoa – Italy

- Algorithms and Data Structure
- Computer Architecture
- Operating Systems (Unix, Windows, MacOS)
- Programming Languages (C++. Visual Basic, Visual C. Java, JSP, PHP, ASP,Html, Javascript, Pascal,Prolog, CGI)
- ComputerNetworks (Communication Protocols (IP,TCP and UDP), DNS, Java network application development,CGI programming, Applet execution, network security problems, web site development, network hardware)
- Graphic Interfaces, Graphics and geometric modelling
- Data Base (SQL,MySQL, SQL Server, Oracle)
- Image Processing (IDL)
- Communication Systems and Technologies

PERSONAL SKILLS

Mother tongue Italian

Other languages

	UNDERSTANDING		SPEAKING		WRITING
	Listening	Reading	Spoken interaction	Spoken production	
English	C1	C2	C1	C1	C1
Spanish	A1	A1	A1	A1	A1

Levels: A1/2: Basic user - B1/2: Independent user - C1/2 Proficient user
Common European Framework of Reference for Languages

Communication skills Good communication skills in different situations (study and work international meetings, work contacts) acquired during the self employment experience

organisational / managerial skills Able to get into team work
Strong team building skills in modular project coordination

Job-related skills
Digital Forensics
Incident Response
IT Security
Data erasure
Data Recovery
Networking
Operating Systems
Programming Languages

Computer skills Other certification owned, apart from the ones in the Education:
CCE (Certified Computer Examiner)
CIFI (Certified Information Forensics Investigator)
ACE (AccessData Certified Examiner)
AME (AccessData Mobile Phone Examiner)
MPSC (Mobile Phone Seizure Certification)
ECCE (European Certificate on Cybercrime and Digital Evidence)
MOS (Microsoft Office Specialist)

Other skills Good performances and competences in swimming (ten years' practice)
Hobbies: football, reading, music

Driving licence European driving licence (B category)

ADDITIONAL INFORMATION

- **Forensic Science International: Digital Investigation**
  Member of the Editorial Board
  https://www.journals.elsevier.com/forensic-science-international-digital-investigation/editorial-board

Publications

BOOKS

- **Trattamento E Scambio Della Prova Digitale In Europa**
  Biasiotti Maria Angela - Epifani Mattia - Turchi Fabrizio
  https://www.edizioniesi.it/pubblicazioni/libri/diritto_storia_filosofia_e_teoria_del_diritto_-_1/diritto_informatica_giuridica_e_telematica_-_1_-_07/informatica-diritto-2-15.html
  Edizioni Scientifiche Italiani (ESI)
  ISBN 9788849532852
- **Learning iOS Forensics – Second Edition**
  Mattia Epifani, Pasquale Stirparo
  https://www.packtpub.com/networking-and-servers/learning-ios-forensics-second-edition
  PacktPub
  ISBN 139781785882081
- **Learning iOS Forensics**
  Mattia Epifani, Pasquale Stirparo
  https://www.packtpub.com/networking-and-servers/learning-ios-forensics
  PacktPub
  ISBN 139781783553518

BOOKS CHAPTERS

- **Digital Forensic Tools Catalogue, a Reference Point for the Forensic Community**
  Mattia Epifani, Fabrizio Turchi
  Handling and Exchanging Electronic Evidence Across Europe
  https://link.springer.com/book/10.1007%2F978-3-319-74872-6
  2018, Springer
  ISBN 978-3-319-74871-9
- **Standard for the Electronic Evidence Exchange**
  Mattia Epifani, Fabrizio Turchi
  Handling and Exchanging Electronic Evidence Across Europe
  https://link.springer.com/book/10.1007%2F978-3-319-74872-6
  2018, Springer
  ISBN 978-3-319-74871-9
- **Apple Tv Forensics**
  Mattia Epifani, Francesco Picasso, Claudia Meda
  IISFA Memberbook 2016
- **Windows Phone 8 Forensics**
  Mattia Epifani, Marco Scarito, Francesco Picasso
  IISFA Memberbook 2015
- **Tor Forensics**
  Mattia Epifani
  IISFA Memberbook 2014
- **Cloud Storage Forensics**
  Mattia Epifani e Marco Scarito
  IISFA Memberbook 2013
- **Windows 8 Forensics**
  Mattia Epifani e altri
  IISFA Memberbook 2013
- **iCloud Forensics**
  Mattia Epifani
  IISFA Memberbook 2012
- **iPad Forensics**
  Mattia Epifani
  IISFA Memberbook 2011
- **Windows 7 Forensics**

Mattia Epifani
IISFA Memberbook 2010

- **TomTom Forensics**
  Mattia Epifani
  IISFA Memberbook 2009

ARTICLES/PAPERS

- **Windows Third Party Apps Forensics Reference Guide Poster**
  Mattia Epifani
  SANS Institute, December 2021
  https://www.sans.org/posters/windows-third-party-apps-forensics-poster/
- **Android Third Party Apps Forensics Reference Guide Poster**
  Mattia Epifani
  SANS Institute, May 2021
  https://www.sans.org/posters/android-third-party-apps-forensics/
- **Six Steps To Successful Mobile Validation**
  Heather Mahalik, Mattia Epifani, Jessica Hyde, Ian Whiffin, John Bair, Alexis Brignoni, Stephen Coates, Mike Dickinson, Vladimir Katalov, Scott Koenig, Paul Lorentz, Christopher Poirier, Lee Reiber, Martin Westman, Mike Williamson, Oleg Skulkin
  SANS Institute, May 2021
  https://www.sans.org/white-papers/six-steps-to-successful-mobile-validation/
- **iOS Third Party Apps Forensics Reference Guide Poster**
  Mattia Epifani
  SANS Institute, March 2021
  https://www.sans.org/posters/ios-third-party-apps-forensics-reference-guide-poster/
- **Triaging modern Android devices (aka android_triage bash script)**
  Mattia Epifani
  RealityNet Blog, January 2021
  https://blog.digital-forensics.it/2021/03/triaging-modern-android-devices-aka.html
- **A journey into IoT Forensics - Episode 5 - Analysis of the Apple HomePod and the Apple Home Kit Environment (aka thanks RN Team!)**
  Mattia Epifani
  RealityNet Blog, January 2021
  https://blog.digital-forensics.it/2021/01/a-journey-into-iot-forensics-episode-5.html
- **A journey into IoT Forensics - Episode 4 - Analysis of an iRobot Roomba 690 (aka thanks VTO Labs for sharing!)**
  Mattia Epifani
  RealityNet Blog, December 2020
  https://blog.digital-forensics.it/2020/12/a-journey-into-iot-forensics-episode-4.html
- **A journey into IoT Forensics - Episode 3 - Analysis of an Ematic Android TV OS Box (aka thanks VTO Labs for sharing!)**
  Mattia Epifani
  RealityNet Blog, December 2020
  https://blog.digital-forensics.it/2020/12/a-journey-into-iot-forensics-episode-3.html
- **A journey into IoT Forensics - Episode 2 - Analysis of an LG Television (aka thanks VTO Labs for sharing!)**
  Mattia Epifani
  RealityNet Blog, December 2020
  https://blog.digital-forensics.it/2020/12/a-journey-into-iot-forensics-episode-2.html
- **A journey into IoT Forensics - Episode 1 - Analysis of a Samsung Refrigerator (aka thanks VTO Labs for sharing!)**
  Mattia Epifani
  RealityNet Blog, December 2020
  https://blog.digital-forensics.it/2020/12/a-journey-into-iot-forensics-episode-1.html
- **Checkra1n Era - Ep 6 - Quick triaging (aka from the iPhone to APOLLO, iLEAPP and sysdiagnose in 6 minutes)**
  Mattia Epifani
  RealityNet Blog, June 2020
  https://blog.digital-forensics.it/2020/06/checkra1n-era-ep-6-quick-triaging-aka.html
- **Checkra1n Era - Ep 5 - Automating extraction and processing (aka "Merry Xmas!")**
  Mattia Epifani
  RealityNet Blog, December 2019
  https://blog.digital-forensics.it/2019/12/checkra1n-era-ep-5-automating.html

- **Checkra1n Era - Ep 4 - Analyzing extractions "Before First Unlock"**
  Mattia Epifani
  RealityNet Blog, December 2019
  https://blog.digital-forensics.it/2019/12/checkra1n-era-ep-4-analyzing.html
- **Checkra1n Era - Ep 3 - Automating extraction "Before First Unlock" (aka "Give me a stupid bash script!")**
  Mattia Epifani
  RealityNet Blog, December 2019
  https://blog.digital-forensics.it/2019/12/checkra1n-era-ep-3-automating.html
- **Checkra1n Era - Ep 2 - Extracting data "Before First Unlock" (aka "I found a locked iPhone! And now?")**
  Mattia Epifani
  RealityNet Blog, December 2019
  https://blog.digital-forensics.it/2019/12/checkra1n-era-ep-2-extracting-data.html
- **Checkra1n Era - Ep 1 - Before First Unlock (aka "I lost my iPhone! And now?")**
  Mattia Epifani
  RealityNet Blog, December 2019
  https://blog.digital-forensics.it/2019/12/checkra1n-era-ep-1-before-first-unlock.html
- **Checkm8, Checkra1n and the new "golden age" for iOS Forensics**
  Mattia Epifani
  RealityNet Blog, November 2019
  https://blog.digital-forensics.it/2019/11/checkm8-checkra1n-and-new-golden-age.html
- **Apple TV Forensics Analysis**
  Mattia Epifani
  Elcomsoft Blog, September 2019
  https://blog.elcomsoft.com/2019/09/apple-tv-forensics-03-analysis/
- **Apple Watch Forensics Analysis**
  Mattia Epifani
  Elcomsoft Blog, June 2019
  https://blog.elcomsoft.com/2019/06/apple-watch-forensics-02-analysis/
- **Using Apple “Bug Reporting” for forensic purposes**
  Mattia Epifani, Heather Mahalik, Adrian Leong
  https://github.com/cheeky4n6monkey/iOS_sysdiagnose_forensic_scripts
- **Windows Phone 8 Forensics**
  Mattia Epifani, Francesco Picasso
  Digital Forensics Magazine, Issue 27, May 2016
- **iOS 9 Forensics**
  Mattia Epifani, Pasquale Stirparo
  Digital Forensics Magazine, Issue 26, February 2016
- **Guida Alla Prova Digitale: il primo approccio del Consiglio d’Europa all’armonizzazione delle diverse metodologie investigative**
  Mattia Epifani
  Ciberspazio e Diritto, vol.15, n. 5, 2014, Mucchi Editore
  https://www.mucchieditore.it/index.php?option=com_virtuemart&view=productdetails&virtuemart_product_id=2057&virtuemart_category_id=95
- **The Forensic Analysis of a False Digital Alibi**
  A.Castiglione, G.Cattaneo, G.De Maio, A.De Santis, G.Costabile, M.Epifani
  IMIS 2012
  https://ieeexplore.ieee.org/document/6296841
- **Computer Forensics: percorsi formativi e certificazioni internazionali**
  Mattia Epifani
  Ciberspazio e Diritto, vol.10, n. 3/4, 2009, Mucchi Editore
  https://www.mucchieditore.it/index.php?option=com_virtuemart&view=productdetails&virtuemart_product_id=1655&virtuemart_category_id=95
- **Analisi di telefoni cellulari in ambito giuridico**
  Mattia Epifani
  Ciberspazio e Diritto, vol.10, n. 1, 2009, Mucchi Editore
  https://www.mucchieditore.it/index.php?option=com_virtuemart&view=productdetails&virtuemart_product_id=1647&virtuemart_category_id=95
- **Three-Dimensional Microscopy migrates to the Web with "Power Up Your Microscope"**
  P.Bonetto, P.Boccacci, M.Scarito, M.Davolio, M.Epifani, G.Vicidomini, C.Tacchetti, P.Ramoino, C.Usai, A.Diaspro
  Microscopy Research and Technique, v.64, 2004
  https://www.researchgate.net/publication/8361936_Three-

dimensional_microscopy_migrates_to_the_Web_with_PowerUp_Your_Microscope

- **Power Up Your Microscope: 3D Microscopy Image Analysis Migrates to the Web**
  A. Diaspro, P. Boccacci, P. Bonetto, M. Davolio, M. Epifani, M. Scarito, F. Mazzone, F. Difato
  GIT Imaging & Microscopy - Volume 4 - October 2002 - pag.34-36
- **Power Up Your Microscope: la tecnologia WEB per un nuovo approccio in microscopia tridimensionale**
  M. Davolio, M. Epifani, M. Scarito, P. Boccacci, P. Bonetto, A. Diaspro
  Biologi Italiani - Anno XXXII - n.6 - Giugno 2002

RECENT PRESENTATIONS

- **Order of Volatility in Modern Smartphone Forensics**
  Mattia Epifani
  SANS DFIR Summit 2021
  https://www.youtube.com/watch?v=gXN4rRs77Ts
- **iOS Third Party Apps Analysis how to use the new reference guide poster**
  Mattia Epifani
  SANS Webinar
  https://www.youtube.com/watch?v=sNyP2_QgSwY
- **Forensic Analysis of the Raspberry PI 400**
  Mattia Epifani
  DFRWS EU 2021
  https://dfrws.org/eu-2021-program/
- **The state of the art in iOS Forensics**
  Mattia Epifani
  Belkasoft Webinar
  https://belkasoft.com/state_of_the_art_ios_forensics
- **Analisi di applicazioni di terze parti in Android e iOS con Cellebrite Physical Analyzer**
  Mattia Epifani
  Cellebrite Webinar
  https://www.cellebrite.com/en/analisi-di-applicazioni-di-terze-parti-in-android-e-ios-con-cellebrite-physical-analyzer/
- **Forensic Analysis of Apple HomePod & Apple HomeKit Environment**
  Mattia Epifani
  SANS DFIR Summit 2020
  https://www.youtube.com/watch?v=D8AOXCBkaTY
- **Apple HomePod and HomeKit Forensics**
  Mattia Epifani
  DFRWS EU 2020
  https://dfrws.org/eu-2020-program/
- **Checkm8, Checkra1n and the new "golden age" for iOS Forensics**
  Mattia Epifani
  SANS@MIC Talk
  https://www.youtube.com/watch?v=8P1sezssGMI
- **iOS Forensics a costo zero**
  Mattia Epifani
  HackInBo, Safe Edition 2020
  https://www.youtube.com/watch?v=Sg7tXPcco64
- **BYOM – Build Your Own Methodology (in Mobile Forensics)**
  Mattia Epifani
  Cellebrite, Life Has No Ctrl Alt Del
  https://www.cellebrite.com/en/key-digital-forensics-concepts-mattia-epifani-ceo-at-reality-net/
- **Using Apple "Bug Reporting" for Forensic Purposes**
  Mattia Epifani
  OSDFCon 2019
  https://www.osdfcon.org/events_2019/using-apple-bug-reporting-for-forensic-purposes/
- **Apple watch forensics: is it ever possible, and what is the profit?**
  Mattia Epifani
  DFRWS EU 2019
  https://www.youtube.com/watch?v=PRaFTDIn1hg
- **Mobile Forensics Challenges: difficoltà attuali, possibilità concrete e sfide future**
  Mattia Epifani
  IHC (Italian Hacker Camp) 2018
  https://www.youtube.com/watch?v=WCuKO1-Bolg

- **Forensicating the Apple TV**
  Mattia Epifani
  DFRWS EU 2018
  https://www.youtube.com/watch?v=WuXxxnsnPNA

Additional and updated information about publications and events is available at

http://www.realitynet.it/en/conferences-events/

http://www.realitynet.it/en/publications/

Updated on March 2023