Titolo evento: Corso "Digital Forensic" (cod.585/01/18)

Obiettivi evento: Il corso è volto a contribuire alla formazione di esperti nella valutazione, acquisizione della prova digitale e dell'informazione elettronica in generale, sia a fini processuali (penali, civili), sia per lo svolgimento di investigazioni interne e/o aziendali. Il corso è utile per apprendere le basi e gli strumenti principali utilizzati dall' informatico forense.

sede	data	orario	docente	argomento lezioni	ore
Collegio San Giuseppe Via San Francesco da Paola 23 Torino (2° piano)	martedì 13 novembre 2018	17.00 - 20.00	ing. Roberto Ganci Isp. Capo Luca Zigiotti ing. Rodolfo Girardo	• DIGITAL FORENSICS o COMPUTER FORENSICS Cosa si intende per computer forensics – Desktop, PC portatili, HDD, USB, NAS, Server o MOBILE FORENSICS Cosa si intende per mobile forensics – Smartphone, Tablet, Navigatori satellitari… o CLOUD FORENSICS Cosa si intende per cloud forensics – Google Drive, Dropbox, iCloud, …… • NORMATIVA o LEGGE 48/2008 – Ratifica trattato di Budapest o C.P.P. (ART. 359 E ART. 360) 1. OPERAZIONI TECNICHE RIPETIBILI Vs OPERAZIONI TECNICHE IRRIPETIBILI o STANDARD ISO IEC 27037/2012 1. IDENTIFICAZIONE, RACCOLTA, ACQUISIZIONE E CONSERVAZIONE DI EVIDENCE DIGITALI 2. RUOLI TECNICI • LA FONTE DI PROVA ED IL METODO SCIENTIFICO o NIST (NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY) 1. LIBRARY – TOOLS - https://www.nist.gov/programs-projects/digital-forensics o LOGGING o CATENA CUSTODIA o HASHING E FINGERPRINT o BEST PRACTICE	3
	martedì 20 novembre 2018	17.00 - 20.00	ing. Roberto Ganci Isp. Capo Luca Zigiotti ing. Rodolfo Girardo	• ANALISI LIVE E POST MORTEM o Tools di acquisizione e analisi live o RAM acquisition • OPEN SOURCE VS CLOSED SOURCE o OPEN: DISTRO LINUX (CAINE, DEFT), AUTOPSY o CLOSED: FTK, ENCASE, XWAYS, UFED, AXIOM 1. FTK e Suite UTK 2. ENCASE 3. UFED e Suite Cellebrite (UFED4PC, Physical Analyzer, UFED Analytics, LinkView) 4. AXION ex IEF (Intelligence Evidence Finder) • WRITE BLOCKER ED HARDWARE FORENSE o Write blocker software Vs Write blocke hardware	**3**

sede	data	orario	docente	argomento lezioni	ore
Fondazione dell'Ordine degli Ingegneri della Provincia di Torino Via Giolitti 1 (scala A - 4° piano)	martedì 27 novembre 2018	17.00 - 20.00	ing. Roberto Ganci Isp. Capo Luca Zigiotti ing. Rodolfo Girardo	• CASI REALI • COMPUTER FORENSICS (60') o POST MORTEM - TECNICHE DI ACQUISIZIONE DI HDD o LIVE ANALYSIS - ACQUISIZIONE SU UN SISTEMA ACCESO. o RECUPERO DATI CANCELLATI (CARVING) o ANALISI SULLA TIMELINE o ANALISI DEI METADATI o ALTRE ANALISI • MOBILE FORENSICS (60') o OPERAZIONI TECNICHE RIPETIBILI o OPERAZIONI TECNICHE IRRIPETIBILI o TIPOLOGIE DI ESTRAZIONI • CLOUD FORENSICS (60') o ACQUISIZIONE SITO WEB o ACQUISIZIONE PAGINA, POST, STREAMING VIDEO o STRUMENTI DI ACQUISIZIONE o METODOLOGIE FORENSI CERTIFICATE	**3**
	martedì 4 dicembre 2018	17.00 - 20.00	ing. Roberto Ganci Isp. Capo Luca Zigiotti ing. Rodolfo Girardo	• PERITO, CONSULENTE TECNICO – NORMATIVA (150') o CONSULENTE TECNICO PARTE o CONSULENTE TECNICO UFFICIO o PERITO DEL GIUDICE o NOMINA o QUESITO DEL GIUDICE/PM • CHIUSURA DEL CORSO	**3**
				Totale	12
				Test finale	