SCHEDA CORSO Corso di sicurezza informatica e comunicazione sicura	
Attività formativa: *Affidato a:* *E-mail:*	Titolo insegnamento: sicurezza informatica e comunicazione sicura Nome titolare insegnamento: Leonida Reitano E-mail titolare insegnamento: leoreitano@yahoo.it
Breve profilo delll'affidatario:	Dottore di ricerca con una tesi sull'Ergonomia del Web,e McLuhan fellow dal febbraio 2003. Ha lavorato nel campo del webpublishing curando lo sviluppo di diversi siti web presso la Free Lance International Press e presso il Laboratorio di Informatica e Didattica della storia dell'università La Sapienza di Roma. Presso la Facoltà di Sociologia di Urbino ha insegnato nel modulo di editoria e internet e nel modulo di e-learning. Si occupa di webdesign e di sviluppo ed implementazione di sistemi di e-learning, sta lavorando inoltre ad un progetto di ricerca su new media e movimenti sociali. Attualmente svolge attività di project manager presso il Consorzio NETTUNO e di coordinatore per il Master di e-learning Management organizzato dall'Università di Urbino. Dal 2007 è Presidente dell'Associazione di Giornalismo Investigativo e svolge attività di ricerca e di didattica nell'ambito delle metodologie legate al giornalismo d'inchiesta. Nel 2009 ha frequentato la Summer School del Center for Investigative Journalism di Londra diplomandosi come esperto di Computer Assisted Reporting (CAR).
Numero di ore della attività:	18
Obiettivi formativi:	Il modulo spiega come difendere la propria privacy e come comunicare in maniera sicura attraverso Internet.
Descrizione e scansione della attività	Introduzione: vengono spiegate le strategie con cui hacker, crimine organizzato o organizzazioni di intelligence possono violare la privacy dei giornalisti. **1° parte archiviazione sicura dei file:** 1) archiviazione sicura dei file True Crypt 2) Archiviazione sicura dei file Steganos 3) cancellazione sicura dei file 4) uso di memorie USB **2° parte comunicazione digitale anonima:** 1) Uso di proxy e ONION router, il sistema TOR e/o altre freenet; 2) Incognito Live CD spiegare le funzionalità della suite; 3) Strategie di utilizzo della suite; 4) PGP- come si utilizza un sistema di crittazione a doppia chiave 5) Webmail criptata: Hushmail; 6) sistemi tascabili di navigazione sicura: xerobank e torpark. **3° parte comunicazioni telefoniche sicure:** 1) telefonia mobile rischi per la privacy e strategie di sicurezza 2) telefona fissa rischi per la privacy e strategie di sicurezza; 3) VOIP rischi per la privacy e strategie di sicurezza; 4) presentazione e installazione degli strumenti (VoIP e Z-fone), strategie d'utilizzo.

Programma	• Steven Levy, Crypto – I ribelli del codice in difesa della privacy, Shake Edizioni, 2002 • Joe Lametta, Kriptonite: http://www.ecn.org/kriptonite • Dispense a cura del docente
Software da scaricare e installare	**Software da scaricare per lezione di sicurezza informatica.** 1. Xerobank: https://xerobank.com/download/xb-browser/ (da installare su pen drive usb) 2. Zphone: http://zfoneproject.com/getstarted.html; 3. Emulatore Windows per Apple: http://www.parallels.com; 4. Voxalot: http://www.voxalot.com/; 5. PGP: http://www.gpg4win.org/ ; Per buona parte di questi software esiste la versione per Apple.
Requisiti hardware e software	Per lo svolgimento dell'attività didattica è necessario venire a lezione con un portatile. L'aula ha il collegamento internet wireless e metteremo a vostra disposizione una piattaforma di e-learning di supporto. Si raccomandano computer con sistema operativo windows o computer con sistema operativo Apple con emulatore Windows. **I software vanno installati prima dello svolgimento della lezione**