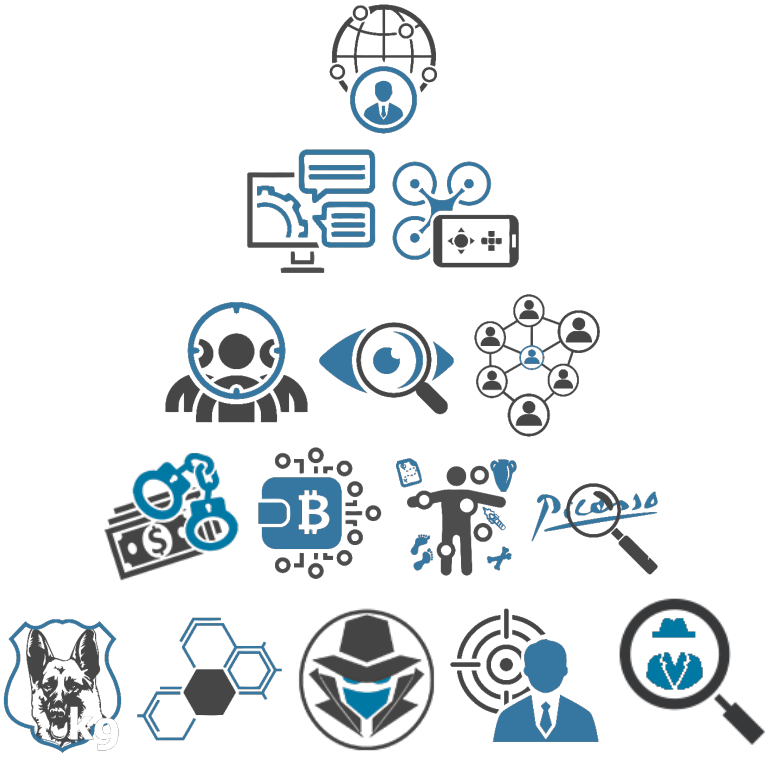
Offerta Corso Qualificato

“CYBER ANALYST”

Corso: *Cyber Analyst – Qualificazione nr. 80*
Ente erogatore: *LAB4INT – https://www.lab4int.org*
Ente qualificatore: *ASC Italia - https://www.acsitalia.it*
Schema di Certificazione: *SCH86 – REV. 00 – 01/07/2025*

LABORATORY FOR INTELLIGENCE



LAB4INT

Via G. Verdi 45
35013 Cittadella (PD)
ITALY

+39 049 825 7400
www.lab4int.org
academy@lab4int.org

LABORATORY FOR INTELLIGENCE

Presentazione di **LAB4INT**

Fin dall'origine, LAB4INT è un ambiente di **studio, formazione e trasferimento tecnologico** dedicato alle scienze forensi e investigative, con un focus su **cyber intelligence**, **OSINT avanzato**, **digital forensics** e **sicurezza delle informazioni**. L'azione è guidata da un **Codice Etico** che impegna soci e collaboratori a integrità, rigore metodologico e piena conformità normativa.

I percorsi formativi promuovono l'integrazione tra metodi OSINT, analisi forense e strumenti di cyber intelligence, diffondendo una cultura investigativa digitale allineata a **ISO/IEC 27001**, **NIST CSF** e **GDPR**. La progettazione didattica è coerente con lo **Schema di Qualificazione SCH86 (REV. 00 – 01/07/2025) di ACS Italia**, che disciplina l'accesso alla **certificazione delle figure Cyber Analyst** per i contesti *Private Sphere* e *Law Enforcement* fino al livello *Advanced*, mediante valutazione documentale ed esame.

La Missione di LAB4INT

LAB4INT nasce da un gruppo coeso di professionisti con background criminologico, forense, investigativo, tecnologico e scientifico, uniti dall'idea che la conoscenza — coltivata con **metodo, etica e rigore** — debba diventare un bene condiviso. La nostra missione è trasformare competenze avanzate in **formazione** e **ricerca applicata** che generano valore operativo per chi indaga, amministra la giustizia e presidia la sicurezza, e per chi desidera intraprendere un percorso serio di specializzazione nelle scienze forensi e nell'intelligence digitale.

Operiamo integrando, in modo organico, **cyber intelligence**, **OSINT avanzato**, **analisi delle comunicazioni**, **applicazioni dell'intelligenza artificiale alle indagini**, **studio delle criptovalute** e **sicurezza informatica**. Questa integrazione è un **metodo**, non un elenco di discipline: **osservazione e raccolta dati → validazione delle fonti → analisi strutturata → correlazione multi-dominio → produzione di elaborati tecnici** chiari, verificabili e utili alle decisioni. L'approccio è **evidence-based**,

LAB4INT

Via G. Verdi 45
35013 Cittadella (PD)
ITALY

+39 049 825 7400
www.lab4int.org
academy@lab4int.org

LABORATORY FOR INTELLIGENCE

con processi tracciabili e risultati ripetibili, nel pieno rispetto delle norme e delle buone pratiche.

Ci rivolgiamo a **magistrati**, **Forze dell'Ordine e Forze Armate**, professionisti dell'investigazione e del diritto, **consulenti tecnici**, operatori della **sicurezza** pubblica e privata, nonché a studiosi motivati. Offriamo un contesto in cui la didattica incontra il campo: **casi studio**, **laboratori guidati**, **simulazioni** ed esercitazioni su scenari realistici, con confronto interdisciplinare tra docenti e practitioner.

In definitiva, la missione di LAB4INT è **abilitare comunità competenti e responsabili**: promuoviamo un trasferimento tecnologico etico, sosteniamo la crescita delle competenze lungo tutto l'arco professionale e contribuiamo a una cultura dell'investigazione digitale che elevi **qualità delle indagini**, **tutela dei diritti** ed **efficacia delle decisioni**.

LAB4INT integra **attività** di studio, formazione, prevenzione e intervento con **finalità** di ricerca applicata e trasferimento tecnologico a supporto dell'intelligence. Opera con percorsi strutturati — anche in **convenzione con i Centri di Addestramento della Guardia di Finanza** per Friuli Venezia Giulia, Veneto ed Emilia-Romagna — destinati a magistrati, Forze dell'Ordine e Forze Armate, professionisti dell'investigazione e del diritto, consulenti tecnici e operatori della sicurezza. La didattica è **evidence-based**, basata su casi reali, laboratori guidati, simulazioni e produzione di **elaborati tecnici verificabili**, in aderenza a tracciabilità, ripetibilità e **catena di custodia**. A sostegno dell'operatività, LAB4INT eroga consulenza specialistica e **supporto alle indagini** su domini chiave dell'intelligence: **OSINT avanzato e cyber intelligence**, analisi delle comunicazioni, **digital/mobile/network forensics**, sicurezza informatica, **blockchain e criptovalute** applicate alle investigazioni, nonché **applicazioni dell'intelligenza artificiale** ai processi informativi. La qualità è garantita da un **team multidisciplinare** che unisce docenti universitari, ricercatori e **practitioner** con esperienza sul campo in incident response e supporto all'Autorità Giudiziaria; tra i soci figurano appartenenti ad **Arma dei Carabinieri, Polizia di Stato, Guardia di Finanza, Polizie Locali, Polizia Penitenziaria, Marina Militare, Esercito Italiano, Aeronautica**

LAB4INT

Via G. Verdi 45
35013 Cittadella (PD)
ITALY

+39 049 825 7400
www.lab4int.org
academy@lab4int.org

Militare, Vigili del Fuoco e Guardia Costiera. La **selezione** di docenti e collaboratori avviene con criteri trasparenti (pubblicazioni, incarichi didattici, esperienza operativa, certificazioni, aderenza al **Codice Etico** su integrità, imparzialità, riservatezza e conflitti di interesse) e un programma di **aggiornamento continuo**. In un'ottica di responsabilità sociale, LAB4INT promuove anche iniziative di **divulgazione gratuita** rivolte alle FF.OO/FF.AA per l'aggiornamento tempestivo su minacce, strumenti e protocolli. In sintesi, LAB4INT agisce da **ponte tra ricerca, formazione e operatività**, trasformando la cultura dell'investigazione digitale in **competenze solide**, **strumenti efficaci** e **pratiche professionali** pronte all'impiego nei processi decisionali dell'intelligence.

Codice Etico e Valori

Il Codice Etico di LAB4INT traduce in prassi quotidiana i valori fondativi dell'organizzazione e ne disciplina le attività formative, di ricerca e di supporto operativo. L'adesione al Codice è condizione necessaria per l'ingresso e la permanenza: ogni aspirante socio sottoscrive un impegno formale al suo rispetto e accetta procedure di vigilanza interna orientate a garantire qualità scientifica ed etica professionale. I principi che lo ispirano — legalità, integrità, imparzialità, competenza, riservatezza e responsabilità verso le persone e le istituzioni servite — non sono dichiarazioni di principio, ma criteri che informano decisioni, comportamenti e metodi di lavoro.

In questo quadro il Codice promuove una cultura della tracciabilità e della ripetibilità, specialmente quando si trattano dati sensibili o evidenze forensi. Le attività e i laboratori sono progettati e documentati in modo auditabile; le informazioni, le fonti e i reperti sono custoditi correttamente, con applicazione della catena di custodia nelle esercitazioni e nei progetti. L'uso degli strumenti tecnologici è proporzionato e lecito, circoscritto a finalità autorizzate e improntato alla minimizzazione dei dati. Sono vietate condotte che possano compromettere l'integrità del lavoro — dall'alterazione o occultamento delle informazioni alla divulgazione non autorizzata — e i conflitti di interesse sono gestiti con dichiarazioni preventive e, quando necessario, con astensione.

LABORATORY FOR INTELLIGENCE

LAB4INT

Via G. Verdi 45
35013 Cittadella (PD)
ITALY

+39 049 825 7400
www.lab4int.org
academy@lab4int.org

LABORATORY FOR INTELLIGENCE

La riservatezza è tutelata attraverso accordi di non divulgazione, controlli di accesso a materiali didattici, dataset e ambienti di laboratorio, e procedure che regolano conservazione e condivisione dei contenuti. La dignità delle persone e la tutela dei diritti orientano la selezione dei casi studio e la progettazione delle simulazioni, soprattutto su temi sensibili: ogni attività massimizza il valore formativo riducendo al minimo i rischi per la privacy e la sicurezza dei dati.

La competenza è considerata un dovere etico prima ancora che tecnico. Docenti e collaboratori si impegnano nell'aggiornamento continuo, nell'uso di standard e buone pratiche riconosciute, nella verifica delle fonti e nella dichiarazione trasparente dei limiti del proprio operato quando necessario. In sintesi, il Codice Etico non è un atto formale, ma l'architettura di fiducia che sostiene la missione di LAB4INT: assicurare che formazione, ricerca applicata e supporto operativo si svolgano con correttezza, qualità e responsabilità, a beneficio della comunità scientifica e delle istituzioni.

Un Impegno Costante per la Crescita del Settore Investigativo

Fedele ai propri principi, LAB4INT coltiva un dialogo continuo tra professionisti di ambiti diversi e trasforma la cross-disciplinarità in valore operativo. La ricerca applicata alimenta la didattica, e la didattica restituisce alla ricerca casi, esigenze e metriche di efficacia: è un circuito virtuoso che permette di leggere con lucidità l'evoluzione delle tecnologie investigative e di trasferirne rapidamente le buone pratiche sul campo. In questo orizzonte, l'amore per la verità e la passione per il suo accertamento non sono slogan, ma l'energia che muove il metodo: osservare con rigore, verificare le fonti, documentare ogni passaggio, assumersi la responsabilità dei risultati.

Per LAB4INT la formazione non è un accessorio, è cultura professionale. Significa allenare il giudizio, affinare le competenze, imparare a scegliere strumenti e procedure con consapevolezza, perché solo chi si forma in modo continuo è davvero in grado di "fare bene il proprio lavoro". Per questo i nostri percorsi nascono da problemi reali e vi ritornano sotto forma di casi, laboratori, simulazioni e prodotti tecnici verificabili, così da consolidare prassi affidabili e ripetibili in contesti giudiziari e di sicurezza.

LAB4INT

Via G. Verdi 45
35013 Cittadella (PD)
ITALY

+39 049 825 7400
www.lab4int.org
academy@lab4int.org

LABORATORY FOR INTELLIGENCE

L'impegno si declina in filoni tematici prioritari che dialogano tra loro: applicazioni dell'intelligenza artificiale alle indagini, OSINT avanzato e analisi delle fonti aperte, studio della blockchain e delle criptovalute a fini investigativi, cybersecurity e protezione dei dati, digital forensics e catena di custodia. Ogni area è presidiata da referenti scientifici e docenti con esperienza operativa, per garantire aggiornamento costante, rigore metodologico e aderenza ai requisiti deontologici ed evidenziali propri delle scienze forensi.

LAB4INT è un hub di conoscenza e innovazione in cui si progettano percorsi, si sperimentano strumenti, si validano procedure e si costruiscono standard condivisi. La collaborazione con enti pubblici e privati nasce dalla convinzione che la qualità dell'indagine e della sicurezza sia un bene comune: si coltiva attraverso lo scambio, la verifica e il miglioramento continuo. In questa prospettiva si inserisce anche l'apertura internazionale, con iniziative e cooperazioni che mettono a confronto metodologie e prassi consolidate a livello globale, per misurarsi con standard elevati e restituire al territorio competenze all'altezza delle sfide attuali.

Elemento chiave di questo disegno è il **corso di qualificazione in Cyber Analyst**, nato dalla passione e dall'esperienza sul campo. È il perno che rende tangibile la nostra visione: un percorso strutturato che integra teoria e pratica, addestra alla valutazione critica delle fonti, alla tracciabilità dei processi, alla produzione di elaborati tecnici utili alle decisioni e spendibili nelle aule di giustizia. Il corso non solo trasferisce competenze, ma costruisce un'identità professionale fondata su metodo, responsabilità e ricerca della verità, offrendo a magistrati, Forze dell'Ordine e Forze Armate, professionisti e consulenti un riferimento solido per crescere lungo tutto l'arco della carriera.

Con questo impegno congiunto in formazione, ricerca e divulgazione scientifica, LAB4INT si conferma una realtà dinamica e qualificata nel panorama delle scienze investigative e forensi: un punto di riferimento per chi cerca serietà metodologica, risultati verificabili e una comunità professionale capace di crescere insieme. L'amore e la passione per la verità restano la nostra stella polare; la cultura della formazione, la chiave per trasformarla ogni giorno in prassi responsabile e in servizio alle istituzioni e ai cittadini.

LAB4INT

Via G. Verdi 45
35013 Cittadella (PD)
ITALY

+39 049 825 7400
www.lab4int.org
academy@lab4int.org

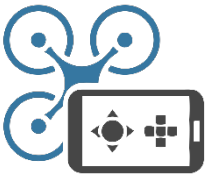
LABORATORY
FOR
INTELLIGENCE

LAB4INT ECOSYSTEM

... is the our system of interconnected specialty ...


OSInt


Digital Forensics


Drone Forensics


Face Recognition


Image Forensics


Relazioni Sociali


Economic Crime


Cryptocurrency Forensics


Archeologia Forense


Grafologia Forense


Cinotecnica Forense


Chimica Forense


Balistica Forense


DarkWeb Analysis


Criminalistica

LAB4INT

Via G. Verdi 45
35013 Cittadella (PD)
ITALY

+39 049 825 7400
www.lab4int.org
academy@lab4int.org

LABORATORY FOR INTELLIGENCE

Seminari Organizzati dai Soci Fondatori nel corso degli anni 2016/2025

“La Traccia Digitale”	Gennaio 2016
“La Traccia Digitale”	Febbraio 2016
“La Traccia Digitale”	Maggio 2016
DNA Elemento di Prova	Ottobre 2016
CYBERCOP “La Traccia Digitale”	Gennaio 2017
CYBERCOP “DNS Abuse”	Febbraio 2017
DRONE “Analysis Division”	Marzo 2017
CYBERCOP “Bitcoin Analysis”	Maggio 2017
CYBERCOP “La Traccia Digitale” - ROMA	Settembre 2017
CYBERCOP “La Traccia Digitale” - RIMINI	Settembre 2017
DRONE “Analysis Division” – PADOVA (c/o Aer. Mil. Di Padova)	Settembre 2017
Workshop “Economic Crime Survey” (Uni. Ca’Foscari)	Settembre 2017
CYBERCOP “La Traccia Digitale” - PALERMO	Settembre 2017
CYBERCOP “La Traccia Digitale” - GENOVA	Settembre 2017
CYBERCOP “La Traccia Digitale” - ROMA	Ottobre 2017
CYBERCOP “La Traccia Digitale” - BRESCIA	Novembre 2017
CYBERCOP “La Traccia Digitale” – UDINE	Novembre 2017
CYBERCOP “La Traccia Digitale” – TRIESTE	Novembre 2017
CYBERCOP “Counterintelligence” – VERONA (c/o A. M.)	Dicembre 2017
Law Enforcement “Cooperation” – GENOVA	Marzo 2018
“La Traccia Digitale” Interforze – UDINE	Marzo 2018
COOPERATION Sem. Interforze con DEA, FBI e CBP – UDINE	Luglio 2018
“La Traccia Digitale” – Digital Forensics - Riccione	Novembre 2018
“La Traccia Digitale” – OSInt – Riccione	Novembre 2018
“La Traccia Digitale” – Drone Forensics – Udine	Novembre 2018
“La Traccia Digitale” – Drone Forensics – Riccione	Dicembre 2018
“La Traccia Digitale” – Economic Crime – Riccione	Gennaio 2019
“La Traccia Digitale” – DARKWEB ANALYSIS – Riccione	Febbraio 2019
“La Traccia Digitale” – Drone Forensics – Teatro Rosso Genova	Marzo 2019
“La Traccia Digitale” – Drone Forensics – Comando Provinciale dei Carabinieri Genova	Marzo 2019
“La Traccia Digitale” – Digital Forensics - Cittadella	Maggio 2019
“La Traccia Digitale” – Drone Forensics – Cittadella	Maggio 2019
“La Traccia Digitale” – OSInt – Cittadella	Giugno 2019

LAB4INT

Via G. Verdi 45
35013 Cittadella (PD)
ITALY

+39 049 825 7400
www.lab4int.org
academy@lab4int.org

LABORATORY FOR INTELLIGENCE

“La Traccia Digitale” – Economic Crime – Cittadella	Giugno 2019
“La Traccia Digitale” – DARKWEB ANALYSIS – Cittadella	Giugno 2019
“La Traccia Digitale” – DARKWEB ANALYSIS – Questura di GE	Giugno 2019
“La Traccia Digitale” – MOBILE FORENSICS – Quest. di Fermo	Dicembre 2019
“FIRST RESPONDER” – NORMATIVA – OnLine	Maggio 2020
“FIRST RESPONDER” – PERQUISIZIONE – OnLine	Maggio 2020
“FIRST RESPONDER” – DIGITAL FORENSICS – OnLine	Giugno 2020
“FIRST RESPONDER” – NETWORK INV. – OnLine	Giugno 2020
“FIRST RESPONDER” – DARKWEB – OnLine	Luglio 2020
“FIRST RESPONDER” – ECONOMIC CRIME – OnLine	Settembre 2020

“OPEN SOURCE INTELLIGENCE” - Cittadella (Pd) dal 05/11/2020 al 11/02/2021

Materie trattate: *Intro - La rete internet ed i Big data, OSInt e le sue variant, OSInt and Law Enforcement, OSInt con tool Open Source Linux, Riconoscimento di oggetti e facciale con SO Open Source Linux, Social network ed social network intelligence, OSInt da browser Firefox per GdF proxy dedicato, Programmazione con Python per la creazione tools OSInt Home Made, Salvataggio chat e pagine Social Network con strumenti Open Source Linux, OSInt come strumento di indagine patrimoniale, Acquisizione forense di prove da web ottenute tramite OSInt, OSInt su Wallet, transazioni e criptomonete, Introduzione a reti anonime, dark e deep web, Information Gathering, Validazione dei dati da fonti aperte con dati da Archivi di Stato, Modalità pratiche: sicurezza, anonimato, privacy, Cyber Threat Intelligence e Casi Pratici*

“DIGITAL INTELLIGENCE” - Cittadella (Pd) dal 29/09/2023 al 14/06/2024

Materie trattate: *Principi di Digital Forensics, Mobile e Drone Forensics, Indagini sul Traffico Telefonico, Vehicle Forensics, Fondamenti di Cyber Security, I nuovi trend del Cybercrime: il CaaS, Cloud Forensics, Principi di Osint, Principi di Digital Intelligence, Social network e social network intelligence, Il Sequestro di criptovalute: aspetti teorici e pratici, Open Source Intelligence con Tsurugi-Linux*

LAB4INT

Via G. Verdi 45
35013 Cittadella (PD)
ITALY

+39 049 825 7400
www.lab4int.org
academy@lab4int.org

CORSO “CYBER ANALYST”

Qualificazione nr. 80 - SCH86 – REV. 00 – 01/07/2025

Il **Corso di Cyber Analyst** è rivolto in via esclusiva agli operatori delle **Forze di Polizia (FF.OO.)** e delle **Forze Armate (FF.AA.)** in servizio attivo. Nasce per fornire una preparazione specialistica, concreta e aggiornata nei domini della **cybersecurity**, delle **investigazioni digitali** e dell’**analisi forense**, con un’impostazione metodologica saldamente ancorata a standard professionali e a buone pratiche di settore. A differenza dei percorsi altamente tecnici destinati a profili informatici, il corso è progettato per investigatori provenienti da ambiti operativi diversi, anche privi di una formazione IT avanzata, che intendono sviluppare una **cultura investigativa digitale** capace di dialogare con i reparti tecnici e di valorizzarne i risultati nelle attività d’indagine.

L’obiettivo formativo non è trasformare i partecipanti in periti informatici, bensì **accrescere la consapevolezza** sugli strumenti, sulle metodologie e sui limiti operativi del dominio digitale: comprendere le principali **minacce** e il loro impatto sulle indagini; orientarsi tra **fonti informative** e dati disponibili nel cyberspazio (dalle evidenze OSINT ai metadati, fino agli elementi di tracciamento e correlazione delle comunicazioni); conoscere **piattaforme di analisi dati**, **dashboard investigative** e **strumenti basati su intelligenza artificiale**, così da integrare le informazioni digitali nei processi decisionali e nelle attività sul campo. La didattica insiste sulla capacità di **porre le domande giuste**, impostare correttamente una richiesta tecnica, leggere in maniera critica i risultati e **tradurli in atti operativi** chiari, verificabili e utili alla catena procedimentale.

Il percorso combina lezioni frontali, **laboratori avanzati** ed esercitazioni su **scenari realistici**. I casi studio sono costruiti per riprodurre le dinamiche tipiche dell’operatività: raccolta e preservazione delle evidenze, validazione delle fonti, correlazione multi-dominio, produzione di elaborati tecnici e report utilizzabili nei contesti istituzionali di riferimento. L’uso guidato di strumenti contemporanei — inclusi ambienti di analisi, soluzioni di visualizzazione e componenti di **AI applicata** — consente ai partecipanti di riconoscere rapidamente le opportunità offerte dal digitale e di **sfruttarle efficacemente** senza dover assumere il ruolo del tecnico forense.

Al termine del corso, gli operatori acquisiscono una **visione chiara e strutturata** del panorama delle investigazioni digitali: sanno **quali informazioni** è possibile ottenere, **con quali strumenti** e **a quali condizioni** metodologiche e normative; comprendono

LABORATORY FOR INTELLIGENCE

LAB4INT

Via G. Verdi 45
35013 Cittadella (PD)
ITALY

+39 049 825 7400
www.lab4int.org
academy@lab4int.org

LABORATORY
FOR
INTELLIGENCE

come integrare tali informazioni nei fascicoli e nei flussi operativi, come collaborare con i reparti specializzati e come elevare il livello di **consapevolezza investigativa** nel dominio digitale. Questo bagaglio rappresenta un valore aggiunto concreto per chi opera nella sicurezza e nella giustizia, potenziando l'efficacia delle indagini e la qualità delle decisioni operative e organizzative.

Struttura degli argomenti attestati nello schema SCH 86 REV. 00 DEL 01/07/2025:

1. Fondamenti di Sicurezza Informatica e Cyber Threat Intelligence

- Concetti chiave: **Riservatezza, Integrità, Disponibilità (CIA triad)**
- **Modelli di minaccia** e analisi del rischio (Risk Management)
- **Ciclo della Cyber Threat Intelligence**: raccolta, validazione, analisi, disseminazione
- Modelli e framework: **MITRE ATT&CK**
- **Cyber Kill Chain**
- Introduzione a HUMINT e SIGINT: **HUMINT**: ruolo operativo e limiti normativi
- **SIGINT**: segnali radio, Bluetooth, WiFi, SDR

2. Monitoraggio, OSINT e Analisi delle Minacce Avanzate

- **OSINT e SOCMINT**: raccolta da fonti aperte e social
- **Monitoraggio del traffico di rete**
- **APT** e vulnerabilità critiche: identificazione e mitigazione
- **Analisi comportamentale e dei pattern**: Celle BTS, ANPR, geolocalizzazione passiva
  - Ricostruzione di movimenti
  - Uso di dati veicolari e open-data

3. Investigazioni nel Dark Web

- Architettura delle reti anonime: **Tor, I2P, Freenet**
- **Navigazione sicura** e raccolta di informazioni
- **Black market e comunità underground**
- Tecniche di infiltrazione:
  - **Social engineering**
  - Infiltrazione digitale mirata
  - Raccolta forense e **conservazione delle prove digitali**

4. Digital Forensics e Analisi dei Reperti

- **Quadro normativo** nazionale e internazionale
- Principi fondamentali: **Catena di custodia**
- **Ripetibilità e integrità**
- Acquisizione e analisi di: Dispositivi mobili
- Memorie digitali
- Sistemi operativi
- Ecosistemi Drone
- Cloud
- Esercitazioni pratiche con strumenti certificati o riconosciuti dalla comunità scientifica forense

LAB4INT

Via G. Verdi 45
35013 Cittadella (PD)
ITALY

+39 049 825 7400
www.lab4int.org
academy@lab4int.org

LABORATORY FOR INTELLIGENCE

5. Analisi delle Infrastrutture di Rete e Dati Telefonici

- Studio e analisi di **tabulati telefonici**
- **Correlazione geografica**:
  - Mappe di copertura
  - Mappe radioelettriche
- Analisi avanzata:
  - Geodati, triangolazione, segnali Bluetooth
  - SIGINT investigativa applicata

6. Criptovalute, AML e Procedura Penale

- **Quadro normativo** nazionale e internazionale sulle criptovalute
- **AML (Anti Money Laundering)**: Obblighi, soggetti vigilati, segnalazioni
- Riciclaggio via crypto-asset
- **Procedura penale** nel sequestro: Fondamenti giuridici
- Sequestro probatorio e preventivo di wallet, seed e dispositivi
- Conservazione della prova digitale
- **Analisi della blockchain**: Wallet, transazioni, blockchain explorer
- On-chain monitoring e off-chain intelligence
- Strategie operative di **sequestro crypto**
- Cold wallet, seed recovery, attribution forensics

7. Cyber Intelligence & Intelligenza Artificiale

- **Laboratorio avanzato**: Sequestri simulati di crypto-asset e digital device
- **Simulazione operazioni complesse**: Raccolta dati (testi, audio, geolocalizzazione)
- Correlazione automatica e analisi predittiva
- Produzione di dossier investigativi
- **Integrazione AI – _CTI**: Sistemi intelligenti di supporto all'investigazione
- Integrazione, analisi automatizzata, NLP e reti neurali

Siamo un hub di conoscenza aperto al confronto e all'innovazione. Lavoriamo con enti pubblici e partner qualificati per consolidare buone pratiche investigative e di intelligence e diffonderle con serietà.

Cordiali saluti,

Il Presidente
Dott. Simone Bonifazi
+39 334 925 7730 - s.bonifazi@lab4int.org

LAB4INT

Via G. Verdi 45
35013 Cittadella (PD)
ITALY

+39 049 825 7400
www.lab4int.org
academy@lab4int.org