SCHEDA CORSO DIGITAL FORENSICS

Dati del corso

Voce	Dettaglio
Titolo	Forensic Analyst
Erogato da	Fata Informatica S.r.l. – CybersecurityUP
Modalità	E-learning
Struttura	7 moduli indipendenti, acquistabili singolarmente, in 2 pacchetti o come percorso completo
Durata video	31 ore 16 min complessive (18 h 12 min Fondamenti · 13 h 03 min Advanced)
Lingua	Italiano
Accesso	h24, per 12 mesi
Piattaforma pratica	HackMeUP: 1 anno di accesso incluso nel percorso completo
Docenti	Docenti universitari e professionisti del settore
Attestati	Attestato di partecipazione al termine di ogni modulo
Certificazioni	CDFE o CPFA, solo con il percorso completo, in base ai requisiti richiesti per l'accesso all'esame
Prezzo	Pagamento unico o rateale: vedi sezione «Prezzi e modalità di pagamento»

Presentazione e finalità

Il percorso Forensic Analyst forma lo specialista di indagini forensi che, all'interno dei team di sicurezza, coordina e gestisce i processi di raccolta dati e di successiva analisi.

I corsi sono guidati da docenti universitari e professionisti del settore, per garantire un apprendimento pratico e di alto livello. Il percorso parte dalle basi e arriva a competenze avanzate: principi legali e metodologici, acquisizione di RAM e dischi, recupero degli artefatti, analisi di malware e di rete, indagini su Windows, Linux e dispositivi mobili.

Nella Digital Forensics la sola conoscenza teorica non basta: servono capacità operative e metodologiche applicabili in scenari reali. Per questo il percorso integra strumenti e ambienti pratici a supporto dello studio e delle attività laboratoriali.

Completando il percorso completo è possibile accedere all'esame per la certificazione CDFE (Certified Digital Forensics Expert) o, in assenza dei requisiti, CPFA (Certified Professional Forensic Analyst). Il percorso completo include 1 anno di accesso a HackMeUP, l'ambiente di laboratorio forense su scenari reali.

A chi è rivolto e requisiti per iscriversi

Il percorso è finalizzato alla creazione dello specialista di indagini forensi. Sono competenze indispensabili per la gestione efficace degli eventi anomali e per comprendere gli impatti delle procedure di governance sulla validità giuridica dei dati raccolti. È il percorso per liberi professionisti, membri del CERT o ICT Manager che vogliono padroneggiare l'indagine forense applicata alle esigenze aziendali.

Moduli	Competenze richieste
Fondamenti di Analisi Forense, Artifact Recovery, Principi di Malware Analysis, Network Forensic	Nessuna competenza specifica, solo dimestichezza con PC e navigazione Internet.
Windows Forensic, Linux Forensic, Mobile Forensic	Solida conoscenza dei sistemi operativi Windows e Linux e familiarità con acquisizione e analisi dei dati da dispositivi diversi (RAM, dispositivi mobili, file system). Utili competenze base di networking e sicurezza informatica.

I prerequisiti specifici di ciascun modulo sono indicati nel programma dettagliato. Fata Informatica non fornisce consulenza sulle esigenze formative del Cliente: la scelta dei moduli è responsabilità dell'acquirente.

Obiettivi formativi

Al termine del percorso completo il discente sarà in grado di:

- Conoscere principi, termini e quadro legale della digital forensics, inclusa la catena di custodia.
- Padroneggiare il processo di identificazione, acquisizione, analisi e presentazione dell'evidenza digitale.
- Acquisire memoria volatile (RAM) e dischi con strumenti come FTK Imager e write-blocker hardware.
- Comprendere la struttura logica del disco (MBR, GPT, BIOS, UEFI) e i principali file system (FAT, FAT32, NTFS, MFT); condurre timeline analysis (Autopsy, Plaso) e file carving.
- Applicare la metodologia WHAT, WHERE, WHEN, HOW e recuperare gli artefatti di sistema Windows (User Assist Key, Browser Forensics, Volume Shadow, Prefetch, Jump List, Shell Bags, Recycler, $MFT, Journal).
- Analizzare il malware in modo statico e dinamico, riconoscere persistenza e lateral movement, comprendere l'anti-forensics e usare le regole YARA.
- Analizzare log di rete, file Pcap e NetFlow con Wireshark e riconoscere le anomalie nel traffico.
- Condurre analisi forensi su Windows (registro, RAM con Volatility, email), su Linux e su dispositivi mobili Android e iOS.
- Prepararsi all'esame per la certificazione professionale CDFE o CPFA.

Gli obiettivi specifici di ogni modulo sono riportati nel programma dettagliato.

Struttura del percorso: moduli e pacchetti

Il percorso è articolato in 7 moduli indipendenti, acquistabili singolarmente, in pacchetti consigliati o come percorso completo.

Cod.	Modulo	Pacchetto	Durata video
FOR-FAF	Fondamenti di Analisi Forense	Fondamenti	06:20:55
FOR-ART	Artifact Recovery	Fondamenti	04:04:19

Cod.	Modulo	Pacchetto	Durata video
FOR-MAL	Principi di Malware Analysis	Fondamenti	03:52:05
FOR-NET	Network Forensic	Fondamenti	03:55:14
FOR-WIN	Windows Forensic	Advanced	05:25:58
FOR-LNX	Linux Forensic	Advanced	04:28:46
FOR-MOB	Mobile Forensic	Advanced	03:09:05
	Totale		**31:16:22**

Pacchetti

Pacchetto	Codice	Moduli inclusi
Fondamenti	FOR-PKG-FND	Fondamenti di Analisi Forense, Artifact Recovery, Principi di Malware Analysis, Network Forensic
Advanced	FOR-PKG-ADV	Windows Forensic, Linux Forensic, Mobile Forensic
Percorso completo	FOR-PKG-FULL	Tutti i 7 moduli + HackMeUP (1 anno) + voucher esame nominale

Fondamenti è il punto di partenza: dai principi generali e legali al recupero degli artefatti di sistema, dai principi di malware analysis all'analisi forense della rete. **Advanced** è il livello specialistico: Windows con RAM analysis ed email forensic, sistemi Linux e mobile forensic su Android e iOS. Il **Percorso completo** è l'unica opzione che dà accesso alla certificazione.

Modalità di erogazione e metodologia didattica

E-learning

Il corso è fruibile 24 ore su 24 dalla piattaforma di formazione di Fata Informatica, con credenziali personali (username e password). Ogni modulo comprende:

- video lezioni registrate;
- test ed esercizi di valutazione;
- laboratori didattici (dove previsti, vedi tabella dei moduli);
- materiale scaricabile;
- e-mail di supporto per interagire con i docenti;
- Uppy, l'AI Tutor addestrato sui materiali ufficiali del corso, disponibile 24/7;
- attestato di partecipazione al termine del modulo.

Il percorso completo include inoltre 1 anno di accesso a HackMeUP e il voucher per l'esame nominale.

Uppy – il tutor AI

Uppy è incluso nel percorso formativo e risponde in modo istantaneo sui temi complessi, assiste durante le esercitazioni pratiche e aiuta nel ripasso mirato prima degli esami, 24 ore su 24.

HackMeUP – la piattaforma forense dove i dati raccontano la verità

Nel mondo della Digital Forensics occorre saper leggere le tracce, ricostruire gli eventi e trasformare i dati in prove. HackMeUP è la piattaforma pratica inclusa nel percorso completo (1 anno di accesso; acquistabile anche singolarmente) per sviluppare capacità operative reali:

- indagini su scenari reali: analisi di macchine compromesse, log, file system e artefatti digitali per ricostruire attacchi e incidenti;
- approccio investigativo strutturato: acquisizione, analisi, correlazione delle evidenze e produzione del report forense;
- casi pratici di Digital Forensics, dalle intrusioni ai data breach;
- strumenti e tecniche professionali realmente utilizzati nel mondo forense;
- laboratori aggiornati per riflettere nuove tecniche di compromissione e nuovi artefatti da analizzare.

Verifiche, attestati e certificazioni

Ogni modulo prevede test di valutazione dell'apprendimento, composti da domande a risposta multipla e/o prove pratiche. Il superamento dei test è requisito necessario per completare il percorso.

Titolo	Chi lo ottiene	Come
Attestato di partecipazione	Chi acquista singoli moduli o pacchetti parziali (Fondamenti, Advanced)	Al termine di ogni modulo, dopo aver completato i materiali e superato i test; rilasciato su richiesta
CDFE – Certified Digital Forensics Expert	Chi completa il percorso completo e possiede i requisiti previsti	Esame finale, le cui modalità sono illustrate durante le lezioni
CPFA – Certified Professional Forensic Analyst	Chi completa il percorso completo ma non possiede ancora i requisiti per la CDFE	Esame finale, come sopra

L'accesso all'esame e alle certificazioni è riservato a chi acquista il percorso completo, che include il voucher per l'esame nominale. Il mancato superamento dell'esame non consente di conseguire la certificazione.

Certificazione CDFE

La CDFE è rilasciata da Fata Informatica, ente accreditato secondo ISO/IEC 17024:2012 e conforme alle norme UNI 11506:2021 e UNI 11621-4:2024. È progettata per analisti forensi digitali specializzati in indagini su reati informatici e sicurezza informatica, e attesta competenze avanzate nella raccolta, analisi e presentazione di prove digitali in modo forense, valido in contesti legali. In linea con la Legge 4/2013, i professionisti certificati saranno inseriti nel registro Accredia dei Certified Digital Forensics Expert.

Requisiti per la CDFE

- Istruzione: almeno il diploma di scuola secondaria di primo grado.
- Formazione: minimo 16 ore di aggiornamento nell'ultimo anno (corsi, webinar, convegni).
- Esercizio dell'attività di Forensic Analyst: 1 anno per chi ha una laurea o corsi post-diploma, 1 anno e mezzo per chi ha completato la scuola superiore, 2 anni per chi possiede il diploma di scuola media.

Mantenimento. Ogni anno il professionista trasmette a Fata Informatica l'evidenza di formazione continua specifica nell'ambito Forensic Analyst (corsi, convegni o sfide su piattaforme), l'evidenza di continuità professionale (o di

incremento della formazione, in caso di perdita di lavoro) e l'evidenza della registrazione e del trattamento di eventuali reclami ricevuti.

Rinnovo. Al quinto anno il professionista presenta l'assenza o la corretta gestione dei reclami, il continuo esercizio della professione, i crediti formativi acquisiti negli anni di mantenimento, supera l'esame di rinnovo e paga la relativa quota, come indicato nel tariffario ufficiale. In funzione degli esiti il certificato può essere rinnovato, sospeso o revocato.

Le certificazioni sono progettate per formare esperti nell'analisi forense digitale e differiscono per contenuti, metodologia d'esame, conformità normativa e valore nel mercato europeo.

Programma dettagliato

Ogni modulo include: e-learning, video lezioni registrate, accesso h24, test ed esercizi di valutazione, laboratori didattici, materiale scaricabile, attestato di partecipazione, e-mail di supporto per interagire con i docenti e Uppy, l'AI Tutor disponibile 24/7. Di seguito, per ciascun modulo, sono indicati i numeri specifici.

FOR-FAF – Fondamenti di Analisi Forense

Introduzione. Costruisce le fondamenta metodologiche e operative dell'analisi forense digitale: dai principi generali e legali che garantiscono la validità delle prove in tribunale, fino alle tecniche di acquisizione di RAM e dischi, alla struttura di archiviazione dei dati e alla timeline analysis. È il modulo che insegna il metodo corretto per identificare, acquisire e preservare l'evidenza digitale senza comprometterne il valore probatorio: la base indispensabile per tutto il percorso.

Obiettivi

- Conoscere i principi generali, i termini e il quadro legale della digital forensics, inclusa la catena di custodia.
- Padroneggiare il processo di identificazione, acquisizione, analisi e presentazione dell'evidenza digitale.
- Eseguire l'acquisizione di memoria volatile (RAM) e di dischi con strumenti come FTK Imager e write-blocker hardware.
- Comprendere la struttura logica del disco (MBR, GPT, BIOS, UEFI) e i principali file system (FAT, FAT32, NTFS, MFT).
- Condurre la timeline analysis con strumenti come Autopsy e Plaso, e applicare tecniche di file carving.

A chi è rivolto. A chi si affaccia per la prima volta al mondo dell'analisi forense digitale.

Competenze richieste. Nessuna competenza specifica, solo dimestichezza di base con PC e navigazione Internet.

Programma del corso

1. **Principi generali.** Introduzione alla digital forensics · Termini e definizioni · Catena di custodia · Note legali e linee guida · Come operare · Repertorio fotografico.
2. **Evidenze digitali e processo di acquisizione.** Fasi investigative, processo della digital evidence · Il processo di identificazione, acquisizione, analisi e presentazione · Evidenza volatile e non volatile, tipologie di analisi e regole di base · Importanza del tempo, cosa evitare, comandi per verifiche · Processo di acquisizione: memorie, acquisizione di sistemi live, priorità di raccolta, cenni su acquisizione mobile · Acquisizione RAM: considerazioni, tecniche di acquisizione, tipologie di dump in Windows (RAW, Crash, Hibernation file) · Acquisizione RAM su macchine virtuali (VM), tools per acquisizione RAM · Processo di acquisizione immagine disco: imaging di dischi rigidi, istantanea del disco · Hard Disk vs Solid State Drive (SSD), cos'è il TRIM · L'acquisizione di un Hard Disk: write-blocker hardware, sigillo digitale, duplicazione disco su sistema live, acquisizione dischi virtuali · Esempio di acquisizione HD con FTK Imager.

3. **Archiviazione dati.** Struttura logica del disco: MBR (Master Boot Record), MBR e GPT, GPT (GUID Partition Table) · Cos'è il BIOS, cos'è UEFI · File System: FAT, caratteristiche dei file system, FAT32, NTFS · Attributi di entry MFT, estrarre i dati e la sequenza temporale dalla MFT.
4. **Timeline analysis.** Cos'è la timeline, l'analisi forense dei sistemi digitali, analisi forense di un computer · Operazioni preliminari, tools, creare una Timeline con Autopsy · Ricerca metadati: metadati dei file, esecuzione di programmi, comandi eseguiti da utenti, artefatti dei programmi · Plaso · File carving: definizione, tipologie, software di data carving, i metadati.

FOR-ART – Artifact Recovery

Introduzione. Insegna a far parlare le tracce che ogni attività lascia su un sistema. A partire da una metodologia investigativa strutturata (cosa, dove, quando e come), si esplorano i numerosi artefatti digitali di Windows: dalle chiavi di registro che rivelano i programmi eseguiti alla cronologia di navigazione, dai dispositivi rimovibili collegati ai file recuperabili dal cestino e dai Volume Shadow. È il modulo che trasforma frammenti apparentemente insignificanti in prove capaci di ricostruire il comportamento di un utente o di un attaccante.

Obiettivi

- Applicare una metodologia forense strutturata basata sui criteri WHAT, WHERE, WHEN, HOW.
- Recuperare e interpretare i principali artefatti di sistema Windows.
- Analizzare l'attività utente tramite User Assist Key, Browser Forensics e dispositivi rimovibili.
- Sfruttare log di sistema, Volume Shadow, Prefetch, Jump List e Shell Bags come fonti di evidenza.
- Recuperare dati da Recycler, $MFT e Journal per ricostruire azioni ed eventi.

A chi è rivolto. A chi vuole imparare a recuperare e interpretare le tracce digitali lasciate su un sistema Windows.

Competenze richieste. Contenuti del modulo Fondamenti di Analisi Forense (metodologia e processo di acquisizione).

Programma del corso

1. **Metodologia generale forense.** Metodologie di analisi: WHAT, WHERE, WHEN, HOW.
2. **Artifact recovery.** User Assist Key · Browser Forensics · Dispositivi rimovibili · Log degli eventi di sistema · Volume Shadows · Prefetch · Jump List · Shell Bags · Recycler · $MFT e Journal.

FOR-MAL – Principi di Malware Analysis

Introduzione. Porta nel mondo dell'analisi del malware dal punto di vista dell'investigatore. Si impara a riconoscere le diverse tipologie di codice malevolo e la loro struttura, a collocare l'analisi all'interno del processo di Incident Response e a distinguere approcci proattivi e reattivi. Dall'analisi statica e dinamica alle tecniche di persistenza e lateral movement, fino all'anti-forensics e alle regole YARA: è il modulo che dà gli strumenti per identificare, analizzare e documentare una minaccia informatica in un contesto forense.

Obiettivi

- Conoscere le tipologie di malware (virus, worm, trojan, hijacker, scareware) e la loro struttura e organizzazione.
- Collocare l'analisi del malware nel processo di Incident Response, distinguendo approccio proattivo e reattivo.
- Comprendere le principali operazioni e tipologie di attacco cyber (IT e IOT/ICS).
- Eseguire l'analisi statica e dinamica del malware con gli strumenti dedicati.
- Riconoscere le tecniche di persistenza e di lateral movement in ambiente Windows.
- Comprendere le tecniche di anti-forensics e utilizzare le regole YARA per il rilevamento.

A chi è rivolto. A chi vuole imparare ad analizzare il malware dal punto di vista dell'investigatore forense.

Competenze richieste. Contenuti dei moduli Fondamenti di Analisi Forense e Artifact Recovery.

Programma del corso

1. **Principi malware.** Cos'è un Malware, cos'è un virus, Worms, Trojan, Hijacker, Scareware/FakeAV · Struttura e organizzazione del malware: infezione, quiescenza, replicazione e propagazione, azioni malevole · Incident Response: Threat Hunting, rilevazione di incidenti, risposta iniziale, formulate a response strategy · Approccio proattivo/reattivo, la squadra, dati endpoint, dati network · Cyber Threats: operazioni cyber, operazioni cyber IOT/ICS · Operazioni cyber – attacchi: Eavesdropping, IP Spoofing, ARP poisoning, Denial of Service, Connection Hijacking, Social engineering, phishing.
2. **Malware Discovery.** Che cos'è l'analisi malware, metodi di rilevamento · Analisi statica: strumenti per l'analisi statica · Analisi dinamica: strumenti per l'analisi dinamica · Tecniche di persistenza del malware: chiave Run e RunOnce, chiave BootExecute, chiave Userinit, considerazioni sulla sequenza di avvio · Lateral movement: cosa significa, Windows Lateral Movement Attacks, Event ID Windows, Scheduled Tasks, Services, Techniques Tactics & Procedures · Anti Forensics: cos'è, sottocategorie (sovrascrittura di dati e metadati, crittografia e steganografia, cancellare gli artefatti) · YARA: Rules, sintassi, YaraGen.

FOR-NET – Network Forensic

Introduzione. Porta l'indagine sul terreno della rete. Dopo un solido richiamo ai fondamenti di reti e protocolli TCP/IP, si impara a leggere ciò che il traffico e i log raccontano di un attacco: come si acquisiscono e proteggono i log, come si analizzano i file Pcap e i flussi NetFlow, e come si riconoscono le anomalie con strumenti come Wireshark. È il modulo che insegna a ricostruire un evento a partire dalle tracce lasciate sulla rete.

Obiettivi

- Consolidare i fondamenti di reti e protocolli TCP/IP rilevanti per l'analisi forense.
- Conoscere i tipi di log di rete, i software di sicurezza e le tecniche di protezione dei log.
- Comprendere i file Pcap e il concetto di NetFlow.
- Analizzare il traffico di rete con Wireshark.
- Riconoscere e interpretare le anomalie nel traffico di rete (Network Traffic Anomalies).

A chi è rivolto. A chi vuole imparare a ricostruire un evento a partire dalle tracce lasciate sulla rete.

Competenze richieste. Contenuti del modulo Fondamenti di Analisi Forense; utili basi di reti e protocolli TCP/IP.

Programma del corso

1. **Le reti.** Il protocollo TCP/IP: i pacchetti (modello ISO/OSI, modello TCP/IP, livelli, incapsulamento) · Gli Header (TCP, IP, Ethernet) · Il protocollo IP: indirizzi, classi, netmask, IPv6 · Il routing IP: tabelle di routing, Autonomous System, protocolli IGP/EGP, Distance Vector, RIP, Link State, Path Vector · Il livello Data Link: indirizzi MAC, MAC Table, switch, protocollo ARP · TCP e UDP: porte, header, Netstat, three way handshake · DNS: struttura, risoluzione · Il protocollo DHCP: fasi, discover, offer, request, hack, rinnovo · Altri protocolli: SNMP, ICMP, FTP, SMTP, IMAP, POP3 · Il protocollo HTTP: request, response, HTTPS, cookies, sessioni HTTP · I sistemi per proteggere la rete: applicazioni web, proxy, firewall, honeypot, VPN, IDS/IPS, sistemi DLP.
2. **Network Forensic.** Cosa sono i log di rete, tipologie di log, software di sicurezza, protezione dei log · Pcap Files, cos'è NetFlow · Analizzare il traffico di rete con Wireshark · Network Traffic Anomalies.

FOR-WIN – Windows Forensic

Introduzione. Porta nell'analisi forense approfondita dei sistemi Windows, l'ambiente più diffuso e quindi più frequente nelle indagini. Dall'architettura del sistema operativo al registro di sistema, dall'analisi delle hive alla RAM Analysis con Volatility, fino alla email forensic: si impara dove si nascondono le informazioni rilevanti e come estrarle correttamente. È il modulo che trasforma la conoscenza generale in competenza specialistica su una delle piattaforme centrali del lavoro forense.

Obiettivi

- Conoscere l'architettura del sistema operativo Windows e le aree di interesse per l'analisi forense.
- Analizzare cronologia dei file, registry di sistema, log e applicazioni installate.
- Padroneggiare la struttura del Registro di Windows: chiavi, valori, top level keys e accesso con permessi speciali (hive SAM).
- Utilizzare strumenti come FTK Imager, RegRipper GUI e BulkExtractor.
- Eseguire la RAM Analysis con Volatility: enumerazione processi, process tree, attività di rete sospette.
- Condurre l'analisi forense delle email (e-mail investigation).

A chi è rivolto. A chi vuole specializzarsi nell'analisi forense dell'ambiente operativo più diffuso nelle indagini.

Competenze richieste. Solida conoscenza dei contenuti del pacchetto Fondamenti (in particolare Fondamenti di Analisi Forense e Artifact Recovery).

Programma del corso

1. **Introduzione all'analisi forense digitale.** Definizione · Principi fondamentali · Scopo dell'analisi forense.
2. **Windows Forensic.** Architettura del sistema operativo Windows · Componenti chiave e aree di interesse per l'analisi forense · Le strutture dei file system e le informazioni importanti per l'analisi forense · Analisi della cronologia dei file · Analisi delle registry di sistema, dei file di log di sistema, delle applicazioni installate · Il registro di sistema (System Registry): struttura del Registro Windows, tipi di valori e chiavi, top level keys, chiavi del registro · Accesso al registro: Registro FTK Imager, acquisizione immagini registro, visualizzare registro, RegRipper GUI · Accesso al registro con permessi speciali, accesso all'utente System in Windows, lettura della hive SAM · BulkExtractor: configurazione degli scanner, analisi dei risultati.
3. **RAM Analysis & E-Mail Forensic.** Tipologie di acquisizione RAM, FTK Imager · I processi e i servizi di Windows, Process Tree, Suspicious Network Activity · Open files and registry handles · Volatility: eseguibile standalone, enumerare processi · E-mail forensic: e-mail investigation.

FOR-LNX – Linux Forensic

Introduzione. Porta nell'analisi forense dei sistemi Linux, ambiente diffuso su server e infrastrutture critiche e quindi terreno frequente di indagine. Si impara a muoversi nella struttura del sistema, a leggere i registri di sistema e degli eventi, a recuperare lo storico dei comandi e a riconoscere le tecniche anti-forensics. Dall'analisi degli utenti e dei programmi di avvio agli artefatti web e al file carving, si acquisiscono gli strumenti e i comandi fondamentali per condurre indagini forensi rigorose in ambiente Linux.

Obiettivi

- Condurre analisi forensi in ambiente Linux, muovendosi nella struttura del sistema.
- Analizzare il Registro di Sistema e il Registro degli Eventi.
- Recuperare e interpretare lo storico dei comandi e riconoscere i comandi anti-forensics.
- Analizzare utenti, programmi di avvio e Web Artefact.

- Applicare il file carving e utilizzare i comandi e gli strumenti fondamentali per le indagini forensi Linux.

A chi è rivolto. A chi vuole condurre indagini forensi su server e infrastrutture critiche basate su Linux.

Competenze richieste. Solida conoscenza dei contenuti del pacchetto Fondamenti; utile familiarità di base con sistemi Linux.

Programma del corso

1. **Linux Forensic.** Analisi forensi tramite sistema operativo Linux · Struttura del sistema · Il Registro di Sistema, il Registro degli Eventi · Lo storico dei comandi, comando antiforensic · Gli utenti, i programmi di avvio · Analisi dei Web Artefact · File Carving · Comandi e strumenti fondamentali per indagini forensi.

FOR-MOB – Mobile Forensic

Introduzione. Porta sul terreno più attuale dell'indagine digitale: i dispositivi mobili. Smartphone e tablet custodiscono oggi la maggior parte delle informazioni personali, e saperle acquisire correttamente è una competenza sempre più richiesta. Si imparano le tecniche di isolamento e acquisizione, logica e fisica, su Android e iOS, come trattare SIM card e memoria interna, e come accedere ai dati contenuti nei file plist e nei database SQLite. Un case study su iPhone/iPad chiude il percorso con un'applicazione concreta su una delle piattaforme più diffuse.

Obiettivi

- Eseguire l'acquisizione logica di dispositivi Android e conoscere gli strumenti per l'analisi forense su Apple.
- Applicare le tecniche di isolamento del dispositivo per un'acquisizione corretta.
- Acquisire dati da dispositivi mobili, SIM card e memoria interna (acquisizione logica e/o fisica).
- Analizzare file system e partizioni dei dispositivi iOS e le principali applicazioni.
- Eseguire l'acquisizione logica dei dati tramite backup iTunes e software/hardware dedicati.
- Accedere e interpretare i dati contenuti nei file plist e nei database SQLite.

A chi è rivolto. A chi vuole specializzarsi nell'acquisizione e analisi forense di smartphone e tablet.

Competenze richieste. Solida conoscenza dei contenuti del pacchetto Fondamenti; utile familiarità con tecniche di acquisizione dati.

Programma del corso

1. **Mobile Forensic.** Mobile Forensic: Android, acquisizione logica · Comandi e strumenti fondamentali per indagini forensi mobile (Apple) · Tecniche di isolamento per acquisizione · Acquisizione di dispositivi mobile · Acquisizione di SIM Card · Acquisizione della memoria interna (logica e/o fisica) · Case study: iPhone/iPad · File system e partizioni · Principali applicazioni · Acquisizione logica dei dati, backup con iTunes · Acquisizione logica con software/hardware dedicati · Accesso ai dati nei file plist e SQLite.

Requisiti hardware e software

Per accedere al corso il Cliente deve disporre dei requisiti seguenti. La verifica è a carico del Cliente (Condizioni di Vendita, art. 4 e art. 11).

Componente	Requisito
Personal computer	Per le sessioni di teoria e pratica sono necessari PC desktop o notebook, mentre per la fruizione dei contenuti teorici è possibile utilizzare dispositivi mobile. In particolare nelle sessioni pratiche è suggerito l'uso di PC con processori 64 bit, almeno quad-core, con supporto Intel VT-x / AMD-V o tecnologia equivalente per compatibilità con ambienti di virtualizzazione locali, con minimo 8 GB di RAM (consigliati almeno 16 GB) e almeno 80 GB di spazio libero su disco per l'installazione e l'esecuzione delle macchine virtuali. Monitor con risoluzione minima consigliata di 1280 × 720 pixel. Scheda audio e cuffie o altoparlanti. Webcam e microfono qualora siano previste attività formative in modalità blended.
Software di virtualizzazione	La postazione dedicata alle sessioni pratiche dovrà consentire l'installazione e l'utilizzo di un software di virtualizzazione compatibile con le macchine virtuali messe a disposizione per le esercitazioni, o comunque suggerite nell'ambito dei laboratori quale strumento per la costruzione di un proprio insieme di strumenti. Le VM saranno distribuite in formato OVA. Per la realizzazione di VM al fine della costruzione di un proprio laboratorio è consigliato seguire l'esempio d'uso di ciascun corso al fine di rendere speculare l'esperienza nelle videolezioni con la pratica. In ambito aziendale/corporate è del tutto evidente che l'utente dovrà disporre dei permessi necessari per installare, configurare ed eseguire software e macchine virtuali sulla propria postazione o avere soddisfatti in modo alternativo i requisiti. Per garantire la piena fruibilità delle attività formative e dei laboratori, è pertanto raccomandato l'utilizzo di un PC personale sul quale l'utente disponga di privilegi amministrativi.
Browser	È necessario utilizzare una versione aggiornata e supportata di uno dei principali browser web, quali: • Google Chrome • Mozilla Firefox • Microsoft Edge • Apple Safari Il browser dovrà consentire l'esecuzione di JavaScript, l'utilizzo dei cookie, il download di file e la riproduzione di contenuti multimediali.
Connettività	Connessione Internet ad alta velocità e stabile, necessaria per lo streaming dei video e per accesso ai laboratori

Componente	Requisito
Requisiti di rete e sicurezza	La postazione e la connessione utilizzate devono consentire l'accesso ai servizi Internet necessari alla fruizione della piattaforma e allo svolgimento delle esercitazioni. Eventuali firewall, proxy, VPN, sistemi di filtraggio, DNS filtering, endpoint security o altre policy di sicurezza applicate da reti aziendali/corporate non devono impedire o limitare: • L'accesso alla piattaforma di erogazione e agli eventuali servizi esterni integrati; • Il download dei materiali didattici e delle immagini delle macchine virtuali • La riproduzione di contenuti audio/video • L'utilizzo di cookie, JavaScript e degli altri servizi web richiesti • Eventuali connessioni necessarie allo svolgimento dei laboratori pratici (VPN via UDP in porta non standard) Qualora venga utilizzata una postazione o una rete aziendale soggetta a restrizioni, l'utente dovrà verificare preventivamente la disponibilità dei permessi di installazione, virtualizzazione e accesso alla rete necessari. Per garantire la piena fruibilità delle attività formative e dei laboratori, è pertanto raccomandato l'utilizzo di un PC personale sul quale l'utente disponga di una connessione Internet non soggetta a restrizioni corporate incompatibili con le attività previste.
Lettura documenti	Software di lettura di file in formato .pdf
Audio e video	Software e dispositivi per la riproduzione di file audio e video (casse o cuffie)
Laboratori	I laboratori potranno essere fruibili attraverso: • Materiale scaricabile da sottoporre a strumenti locali (la cui installazione è a carico dell'utente), quali simulatori, analizzatori, ecc. Questi strumenti potranno essere collocati su proprio PC o in apposita VM sperimentale • Connessione Web diretta a piattaforma di simulazione/esercitazione • Connessione VPN (tramite differenti porte) ad infrastrutture virtuali remote. Gli strumenti di indagine devono essere predisposti dall'utente nel proprio PC o all'interno di VM predisposte all'esercitazione. In alcun caso viene fornito un ambiente di analisi o strumentazione di attacco attraverso le piattaforme. **ATTENZIONE**! In alcuni casi è possibile che il laboratorio trattino materiale pericoloso quale exploit o malware. È fondamentale trattare questi casi in VM isolate e protette in modo da evitare contaminazioni o incidenti alle infrastrutture estranee ai laboratori.

Il Cliente si impegna ad adeguare i propri sistemi hardware e software in caso di aggiornamenti o mutamenti della piattaforma. Fata Informatica non risponde dei difetti di fruizione dovuti al mancato possesso dei requisiti minimi di sistema.

Durata dell'iscrizione, accesso e assistenza

Voce	Dettaglio
Validità dell'iscrizione – singolo modulo	12 mesi dalla data di iscrizione
Validità dell'iscrizione – pacchetto o percorso completo	12 mesi dalla data di iscrizione
Scadenza	Terminato il periodo, l'iscrizione viene disattivata automaticamente: lezioni e test vanno completati entro la scadenza
Accesso ai materiali	h24, con username e password personali, non cedibili
Area personale	Elenco dei corsi frequentati e dei materiali correlati
Credenziali	Generate automaticamente e inviate dal tutor didattico dopo l'iscrizione e il pagamento
Assistenza didattica	Sistema di ticket per domande ai docenti e allo staff, attivo per tutta la durata dell'iscrizione; e-mail di supporto supportodidattico@fatainformatica.it; tutor AI Uppy 24/7
Reclami	Per iscritto a Fata Informatica, Via Tiburtina 912, 00156 Roma; esito comunicato entro 20 giorni lavorativi
Accesso HackMeUP	1 anno, incluso nel percorso completo dalla data di iscrizione

Il Cliente deve svolgere personalmente le lezioni e i test. Eventuali ulteriori informazioni aggiornate sono comunicate dalla parte tecnica il primo giorno di lezione.

Prezzi e modalità di pagamento

I prezzi sono espressi in euro, IVA inclusa. Ogni opzione è acquistabile in un'unica soluzione oppure, dove indicato, a rate.

Il pagamento avviene online tramite il servizio Stripe. Fata Informatica non gestisce né memorizza i dati degli strumenti di pagamento. Eseguito il pagamento, viene emessa la fattura. Il pagamento a rate è disponibile solo ove espressamente indicato. Completata l'iscrizione e saldato il prezzo, il Cliente riceve le credenziali di accesso. Il pagamento a rate comporta una maggiorazione del 5%.

Recesso e condizioni di vendita

L'acquisto è regolato dalle Condizioni di Vendita dell'e-commerce di Fata Informatica S.r.l. (Rev. 03 del 07.10.2026) che il Cliente accetta con modalità point and click prima dell'acquisto. Il Cliente dichiara di aver letto questa Scheda del Corso prima di acquistare.

- **Recesso (consumatori).** 14 giorni dalla data di acquisto, senza motivazione e senza costi (art. 52 Codice del Consumo).

- **Perdita del recesso.** Il diritto non è più esercitabile dopo l'invio delle credenziali che danno accesso immediato alla piattaforma. Chi vuole recedere deve attendere i 14 giorni prima di ricevere le credenziali.
- **Fruizione immediata.** Il Cliente può chiedere, durante l'ordine, di accedere subito al corso, accettando di perdere il diritto di recesso (art. 59, comma 1, lett. o). Riceve conferma del contratto e ricevuta via e-mail.
- **Rimborso.** In caso di recesso valido, entro 60 giorni dall'esercizio, con riaccredito sullo stesso strumento di pagamento.
- **Diritto d'autore.** Videolezioni, slide e materiali sono di proprietà di Fata Informatica: è vietato copiarli, distribuirli o cederli. Le credenziali sono personali e non cedibili.
- Il testo completo delle Condizioni di Vendita prevale su quanto qui sintetizzato.