



## POST-HBO DIGITAL FORENSIC ANALYSIS PROFESSIONAL

*Gedurende deze Post-HBO opleiding verkrijgt u de kennis en vaardigheden die nodig zijn om zelfstandig een digitaal forensisch onderzoek uit te kunnen voeren.*

### Waarom deze opleiding?

De afgelopen jaren wordt steeds vaker onderkend dat een betrouwbare informatievoorziening van levensbelang is voor het goed functioneren van een organisatie. Daartoe worden allerlei maatregelen genomen die moeten voorkomen dat beveiligingsincidenten optreden. Toch zult u onherroepelijk geconfronteerd worden met (mogelijk) misbruik van uw bedrijfsgegevens en -middelen. Afhankelijk van de aard van het incident kan het dan voorkomen dat u niet alleen geïnteresseerd bent in het oplossen van het incident zelf, maar ook in wat er nu precies gebeurd is en wie daarvoor verantwoordelijk is geweest. Mogelijk zelfs met als doel juridische stappen te ondernemen. In dat geval volstaat het gebruikelijke Incident Response proces niet meer en zult u de hulp van een specialist nodig hebben. Een digitaal forensisch onderzoeker kan deze informatie voor u boven water halen en dit op een dusdanige wijze doen dat de resultaten van het onderzoek bruikbaar zijn als basis voor eventuele

### Inschrijven

U vindt de actuele cursusdata en het inschrijvingsformulier op [www.securityacademy.nl](http://www.securityacademy.nl).

De kosten voor deze opleiding bedragen € 9.870,- exclusief BTW.

Wilt u meer informatie? Bel dan naar 0348-408061, of e-mail naar [info@securityacademy.nl](mailto:info@securityacademy.nl).

disciplinaire, of mogelijk zelfs juridische vervolgstappen.

### Leerdoelen

In deze opleiding wordt u opgeleid tot professional die zelfstandig kan optreden als digitaal forensisch onderzoeker. Na afronding van deze unieke opleiding heeft u een gedegen kennis van:

- De aanpak van digitaal forensisch onderzoek volgens een gestructureerde methodologie
- Hoe bewijsmateriaal te vergaren en zodanig zeker te stellen dat de integriteit ervan nooit in twijfel kan worden getrokken
- De opbouw van de meest voorkomende filesystemen
- De specifieke vereisten van digitaal forensisch onderzoek op Windows en Unix systemen
- De specifieke vereisten van digitaal forensisch onderzoek van netwerkdiensten als e-mail en web
- Het gebruik van de hulpmiddelen die een digitaal forensisch onderzoeker tot zijn beschikking heeft staan
- Hoe effectief de resultaten van het onderzoek te presenteren aan zowel een technisch als een niet-technisch publiek

### Programmamenmerken

Het programma van deze opleiding is intensief en inspirerend. Gedurende 16 lesdagen presenteren

deskundigen uit het bedrijfsleven u het volledige theoretische kader en wordt aan hand van simulaties en discussie uitgebreid ingegaan op de toepassing ervan in de praktijk. De opleiding wordt afgesloten met een theoretisch examen en een praktijkgerichte afstudeeropdracht, waarin men moet laten zien het geleerde toe te kunnen passen.

### Doelgroep

Deze opleiding is bestemd voor:

- Security Officers
- Technisch Consultants
- Leden van Incident Response Teams of fraudeonderzoeksteams
- Systeem- en netwerkbeheerders
- Andere functionarissen die behoefte hebben aan een goede kennis van digitaal forensisch onderzoek

Gezien de diepgang en het tempo van deze opleiding wordt aangeraden dat deelnemers vooraf beschikken over voldoende technische kennis van computers. Twijfelt u of uw kennis toereikend is, neemt u dan contact met ons op.

### Certificering

Van deelnemers wordt verwacht dat zij zich aantoonbaar hebben ontwikkeld op HBO-niveau. Na succesvolle afronding van de opleiding ontvangt u het geaccrediteerde Post-HBO diploma 'Digital Forensic Analysis Professional' en behoort u tot het selecte gezelschap van informatie-beveiligers dat heeft bewezen aan de kwaliteitseisen van deze opleiding te voldoen.

# Onderwerpen die aan bod komen in de Post-HBO opleiding DIGITAL FORENSIC ANALYSIS PROFESSIONAL

## Onderzoeksmethodologie

Goed digitaal forensisch onderzoek bouwt op 2 fundamenteën, namelijk de kennis van de onderzoeker en de reproduceerbaarheid van het onderzoek. Het eerste wordt verkregen door studie en werkervaring. Het tweede vereist een vaste en goed overdachte werkwijze, zodat het onderzoek consistent van een hoge kwaliteit is. Dit vergt een vaste methodologie die zeker stelt dat bewijsmateriaal op de juiste wijze is verkregen en behandeld en dat de conclusies die uit de analyse ervan voortkomen door onafhankelijke derden gestaafd kunnen worden. In deze module wordt beschreven hoe een digitaal forensisch onderzoek aangepakt dient te worden.

## Hulpmiddelen voor forensisch onderzoek

De grootte van moderne opslagmedia en de complexiteit van de huidige digitale omgevingen maken dat een digitaal forensisch onderzoeker zijn werk niet meer zonder goed gereedschap kan doen. Een goed onderzoeker heeft weliswaar de kennis om het onderzoek met de hand te kunnen doen, maar maakt ook gebruik van de juiste hard- en software om het onderzoek efficiënt te laten verlopen. Deze module gaat in op de functie en de toepassing van de meest gebruikte hulpmiddelen. Denk daarbij bijvoorbeeld aan hulpmiddelen voor het maken van forensische duplicaten, het samenstellen van een timeline, het terughalen van, al dan niet opzettelijk, verborgen of beschadigde bestanden en het verzamelen en analyseren van grote hoeveelheden gegevens.

## Onderzoek van bestandssystemen

Ieder digitaal systeem dat gegevens opslaat maakt gebruik van een bestandssysteem dat die gegevens volgens een bepaalde structuur naar een gegevensdrager weg schrijft. Een digitaal forensisch onderzoeker moet in staat zijn om de informatie die zich op een gegevensdrager bevindt te analyseren, ook als het systeem dat die gegevens heeft weggeschreven niet beschikbaar is. Daarom wordt in deze module ingegaan op de structuur en werking van de meest voorkomende bestandssystemen.

## Onderzoek van actieve systemen

Naast analyse van gegevensdragers is ook analyse van de meer dynamische aspecten van een systeem van belang bij digitaal forensisch onderzoek. Volatiele gegevens, afkomstig van actieve processen en netwerkverbindingen kunnen immers ook een schat aan informatie opleveren. Daarom wordt in deze module ingegaan op het verzamelen van gegevens uit vluchtige bronnen.

## Onderzoek van Windows systemen

In deze module worden de specifieke systeemfaciliteiten van Windows, alsmede een aantal van de meest gebruikte applicaties onder Windows door de bril van een digitaal

forensisch onderzoeker bekeken. Tevens komt onderzoek van het Windows-geheugen aan de orde.

## Onderzoek van Unix systemen

Ook systemen uit de Unix-familie kennen hun eigen specifieke systeemfaciliteiten die in de context van digitaal forensisch onderzoek waardevolle informatie kunnen bevatten. Deze module gaat in op de analyse van die informatie. Daarnaast wordt ook een aantal van de meest voorkomende applicaties op \*nix systemen beschouwd vanuit forensisch oogpunt.

## Onderzoek van netwerkdiensten

Tegenwoordig is een systeem dat niet verbonden is met een netwerk een zeldzaamheid. Dat betekent dat ook informatie afkomstig van bijvoorbeeld e-mail of web relevant kan zijn voor een onderzoek. De analyse van dergelijke informatie is het onderwerp van deze module.

## Wet- en regelgeving

Een digitaal forensisch onderzoeker krijgt op vele manieren met wet- en regelgeving te maken. Het is dus belangrijk dat de onderzoeker op de hoogte is van de spelregels, zodat hij kan voorkomen dat deze met de voeten getreden worden en hij mogelijk zelfs aansprakelijk wordt gesteld voor eventueel geleden schade. Deze module is weliswaar geen vervanging voor het advies van een jurist, maar biedt wel een goede basiskennis van de belangrijkste aspecten uit wet- en regelgeving die van belang zijn voor een digitaal forensisch onderzoeker.

## Overige onderwerpen

Een het eind van de cursus wordt kort ingegaan op een aantal onderwerpen waarmee een onderzoeker te maken kan krijgen, zoals steganografie, virtualisatie en anti-forensics.



Onderstreep uw vakkennis en behaal het Post-HBO diploma  
DIGITAL FORENSIC ANALYSIS PROFESSIONAL