GIDS

De complete gids voor Digital Forensics & Investigation

Digitaal forensisch onderzoek: werkwijze, kosten, bewijsvoering en NIS2-compliance voor het MKB.

Maart 2026

IBGIDS NL

INHOUDSOPGAVE

Kerncijfers op een rij •

Wat is digitaal forensisch onderzoek? 1

Waarom is het belangrijk? 2

Hoe werkt het? Het proces 3

Wat kost het? 4

Waar moet je op letten? 5

Veelgemaakte fouten 6

Compliance: NIS2 en regelgeving 7

Digital Forensics vs. Incident Response 8

Trends 2025--2026 9

Aan de slag 10

Bronnenlijst •

Kerncijfers op een rij

Digitaal forensisch onderzoek is cruciaal na elk cyberincident. De cijfers laten zien waarom.

USD 10,5 mrd
Wereldwijde DFIR-markt in 2025, groeiend met 20,4% per jaar
Mordor Intelligence [1]

241 dagen
Gemiddelde tijd om een breach te detecteren en beheersen
IBM Cost of Data Breach 2025 [2]

9.800+
Datalekken gemeld bij AP in eerste helft 2024 in Nederland
CBS Cybersecuritymonitor 2024 [3]

44%
Van alle bevestigde breaches betrof ransomware
Verizon DBIR 2025 [4]

USD 4,44 mln
Gemiddelde kosten van een datalek wereldwijd
IBM Cost of Data Breach 2025 [2]

24 uur
Maximale meldtermijn bij significante incidenten onder NIS2
Digitale Overheid [5]

EUR 10 mln
Maximale NIS2-boete voor essentiële entiteiten
Kynexis [6]

10,7%
Jaarlijkse groei MKB-adoptie van forensische diensten in Europa
Mordor Intelligence Europa [7]

1. Wat is digitaal forensisch onderzoek?

Digitaal forensisch onderzoek is het veiligstellen, analyseren en interpreteren van digitale sporen na een cyberincident, fraude of datalek.

Na een cyberincident wil je drie dingen weten: wat is er gebeurd, wat is de schade, en wie is verantwoordelijk. Digitaal forensisch onderzoek beantwoordt deze vragen door systematisch digitale sporen te verzamelen en te analyseren [8].

Het vakgebied omvat meerdere specialisaties: computer forensics (analyse van servers en werkstations), network forensics (netwerkverkeer), mobile forensics (smartphones), memory forensics (RAM-analyse) en cloud forensics [8].

Forensisch onderzoek verschilt van incident response doordat het zich richt op bewijsvoering en reconstructie, terwijl incident response zich richt op het beheersen en stoppen van het incident. In de praktijk lopen ze vaak samen: DFIR (Digital Forensics and Incident Response) [9].

> **Voor wie?** Elke organisatie die te maken krijgt met een cyberincident, datalek, fraude of vermoedens van datadiefstal. Een IR Retainer-contract zorgt dat je voorbereid bent.

2. Waarom is het belangrijk?

Zonder forensisch onderzoek weet je niet wat er is gebeurd, hoe groot de schade is, of de aanvaller nog aanwezig is.

Een datalek kost gemiddeld USD 4,44 miljoen [2]. Organisaties die AI en automatisering inzetten bij forensisch onderzoek verkorten hun breach lifecycle met 80 dagen en besparen USD 2,2 miljoen per incident [2].

In Nederland werden in de eerste helft van 2024 meer dan 9.800 datalekken gemeld bij de Autoriteit Persoonsgegevens [3]. Bij elk van deze meldingen is forensisch onderzoek nodig om de omvang en impact vast te stellen.

Ransomware kwam voor in 44% van alle bevestigde breaches [4]. Na een ransomware-aanval is forensisch onderzoek noodzakelijk om vast te stellen welke data is getroffen, of data is geexfiltreerd, en of de aanvaller nog aanwezig is in het netwerk.

3. Hoe werkt het? Het proces

Van incident tot conclusie in vijf fasen.

1

Intake en triage

1-2 DAGEN

Het incident wordt beoordeeld op urgentie, scope en type. Bij acute incidenten start triage direct na melding.

2

Forensische acquisitie

1-3 DAGEN

Digitale bewijsmaterialen worden veiliggesteld. Altijd op een kopie, nooit op het origineel. Chain of custody wordt gedocumenteerd.

3

Analyse en onderzoek

1-4 WEKEN

Forensische specialisten analyseren registries, file systems, netwerklogs, memory dumps en andere bronnen om het incident te reconstrueren.

4

Rapportage

3-5 DAGEN

Een gedetailleerd rapport met bevindingen, tijdlijn, getroffen systemen en aanbevelingen. Bij juridische procedures een gerechtelijk rapport.

5

Juridische ondersteuning

DOORLOPEND

Indien nodig worden bevindingen gepresenteerd als bewijs in juridische procedures.

4. Wat kost het?

Kosten varieren sterk afhankelijk van de complexiteit en het aantal apparaten.

TYPE	PRIJSINDICATIE	GESCHIKT VOOR
Standaard (1–2 apparaten)	EUR 3.500 - 7.500 [10]	Enkelvoudig incident, 1-2 devices
Uitgebreid (netwerk + endpoints)	EUR 7.500 - 20.000	Netwerk-breed incident, meerdere devices
Complex (IR + forensics)	EUR 20.000 - 50.000 [10]	Ransomware, dataexfiltratie, juridisch
IR Retainer (preventief)	EUR 7.500 - 12.000/jaar [11]	Voorbereid zijn, snellere responstijd

Het gemiddelde uurtarief voor een forensisch onderzoeker in Nederland ligt rond EUR 200 per uur [10].

MKB-TIP

Een IR Retainer contract (vanaf EUR 7.500/jaar) garandeert beschikbaarheid en snellere responstijd wanneer je het nodig hebt. Zonder retainer betaal je spoedtarieven en loop je het risico dat onderzoekers niet direct beschikbaar zijn.

5. Waar moet je op letten?

10 vragen voor je forensisch onderzoeksbureau.

1. Zijn jullie onderzoekers beedigd of gecertificeerd?
2. Hoe wordt chain of custody gewaarborgd?
3. Wat is de beschikbaarheid: 24×7 of kantooruren?
4. Ervaring met ons type incident (ransomware, BEC, fraude)?
5. Wordt het rapport opgesteld voor juridisch gebruik?
6. Hoe snel kunnen jullie starten na melding?
7. Wat is de vaste prijs of uurtarief?
8. Bieden jullie ook incident response (containment)?
9. Welke apparaten en cloudomgevingen kunnen jullie onderzoeken?
10. Kunnen jullie referenties geven van MKB-klanten?

6. Veelgemaakte fouten

1. Bewijs vernietigen door systemen opnieuw op te starten

Na een incident willen IT-teams vaak direct systemen opschonen. Dit vernietigt cruciaal bewijsmateriaal. Raak niets aan totdat forensische specialisten zijn ingeschakeld.

2. Geen IR Retainer contract

Zonder retainer betaal je spoedtarieven en wacht je mogelijk dagen voordat een onderzoeker beschikbaar is. Met een retainer is responstijd gegarandeerd.

3. Chain of custody niet bewaken

Ongedocumenteerde toegang tot bewijsmateriaal kan ertoe leiden dat bewijs niet bruikbaar is in juridische procedures (Art. 359a Sv) [12].

4. Te laat het incident melden

Hoe langer je wacht, hoe meer bewijs verloren gaat. Logs worden overschreven, geheugen verandert, aanvallers wissen sporen. Meld direct.

5. Alleen IT betrekken

Forensisch onderzoek raakt ook juridische, HR- en communicatieaspecten. Betrek direct een multidisciplinair crisisteam.

7. Compliance: NIS2 en regelgeving

De Cyberbeveiligingswet (NIS2) vereist incidentmelding binnen 24 uur bij significante incidenten [5]. Om een accurate melding te doen, heb je forensische capaciteit nodig om snel de omvang en impact te bepalen.

De AVG vereist melding van datalekken bij de AP binnen 72 uur. Forensisch onderzoek bepaalt of persoonsgegevens zijn getroffen en welke betrokkenen moeten worden geinformeerd.

Forensic readiness -- voorbereid zijn op forensisch onderzoek -- is onderdeel van de NIS2-zorgplicht. Het NCSC benadrukt het belang van tools, procedures en contracten die klaarliggen voordat een incident plaatsvindt [8].

> **BOETES**
> NIS2-boetes kunnen oplopen tot EUR 10 miljoen of 2% van de wereldwijde jaaromzet. Bestuurders zijn persoonlijk aansprakelijk [6].

8. Digital Forensics vs. Incident Response

ASPECT	DIGITAL FORENSICS	INCIDENT RESPONSE	DFIR (GECOMBINEERD)
Doel	Bewijs verzamelen, reconstrueren	Incident beheersen, stoppen	Beide tegelijkertijd
Focus	Wat is er gebeurd?	Hoe stoppen we het?	Beheersen en begrijpen
Timing	Na het incident	Tijdens het incident	Tijdens en na
Output	Forensisch rapport	Containment, herstel	Rapport + herstelplan
Juridisch	Bewijsvoering, chain of custody	Niet primair	Beide geborgd

9. Trends 2025--2026

Cloud forensics groeit snel

Met de toename van cloud-adoptie verschuift forensisch onderzoek naar cloud-omgevingen, wat nieuwe tools en methodieken vereist.

AI versnelt analyse

AI versnelt de analyse van grote datasets, timeline-reconstructie en anomaliedetectie. Organisaties die AI inzetten verkorten hun breach lifecycle met 80 dagen [2].

NIS2 als driver voor forensic readiness

De meldplicht van 24 uur maakt forensische voorbereiding noodzakelijk. IR Retainer-contracten worden steeds gebruikelijker.

MKB-adoptie door EU-regelgeving

EU-wetgeving dwingt MKB-organisaties forensische diensten af te nemen. De MKB-markt groeit met 10,7% per jaar [7].

10. Aan de slag

Wees voorbereid voordat een incident plaatsvindt.

1. **Sluit een IR Retainer af:** Garandeert beschikbaarheid en snellere responstijd.
2. **Zorg voor forensic readiness:** Logging, procedures en contactgegevens klaar.
3. **Ken je meldplichten:** NIS2 (24 uur), AVG (72 uur). Weet wie je moet bellen.
4. **Oefen je incident response:** Tabletop exercises voorbereiden het team.
5. **Bewaar logs:** Zorg voor voldoende logretentie (minimaal 90 dagen, liefst 1 jaar).

Bronnenlijst

[1] **Mordor Intelligence** -- DFIR Solutions Market 2030 -- https://mordorintelligence.com/industry-reports/digital-forensics-and-incident-response-solutions-market

[2] **IBM** -- Cost of a Data Breach 2025 -- https://ibm.com/reports/data-breach

[3] **CBS** -- Cybersecuritymonitor 2024 -- https://cbs.nl/nl-nl/longread/aanvullende-statistische-diensten/2025/cybersecuritymonitor-2024?onepage=true

[4] **Verizon** -- DBIR 2025 -- https://verizon.com/business/resources/reports/dbir/

[5] **Digitale Overheid** -- Cyberbeveiligingswet -- https://digitaleoverheid.nl/overzicht-van-alle-onderwerpen/cyberbeveiligingswet/

[6] **Kynexis** -- NIS2 boetes -- https://kynexis.nl/nis2-boetes-cyberbeveiligingswet-uitgelegd/

[7] **Mordor Intelligence** -- Europe Digital Forensics 2030 -- https://mordorintelligence.com/industry-reports/europe-digital-forensics-market-industry

[8] **NCSC** -- IR en Forensisch Onderzoek -- https://ncsc.nl/actueel/weblog/weblog/2021/incident-respons-en-digitaal-forensisch-onderzoek-voor-nederland

[9] **NFIR** -- Digital Forensic Investigation -- https://nfir.nl/en/services/digital-forensic-investigation-at-nfir/

[10] **Digitaalforensischonderzoek.nl** -- Kosten DFO -- https://digitaalforensischonderzoek.nl/kosten-digitaal-forensisch-onderzoek/

[11] **Pinewood** -- IR Retainer -- https://pinewood.nl/nieuws/incident-response-retainer-speciale-q4-aanbieding/

[12] **Forensicon** -- Chain of Custody -- https://forensicon.nl/chain-of-custody-and-evidence/

[13] **Market Data Forecast** -- Europe Digital Forensics 2033 -- https://marketdataforecast.com/market-reports/europe-digital-forensics-market

[14] **ENISA** -- Threat Landscape 2025 -- https://enisa.europa.eu/publications/enisa-threat-landscape-2025

[15] **Kaspersky** -- Digital Forensics -- https://kaspersky.nl/resource-center/definitions/digital-forensics