Informatica

Modulehandleiding iipforit

Project Inleiding FICT

Hogeschool Leiden,
Opleiding Informatica

april 2023

Versie 4.0

Modulehandleiding iipforit

Inhoud

Modulehandleiding iipforit

Versiebeheer

Versie	Datum	Status	Wijzigingen
0.1	22-04-2020	Concept	Vertaling naar iipforit
1.0	06-05-2020	Definitief	Na controle door collega
2.0	22-04-2021	Definitief	Online onderwijs weer naar fysiek
3.0	04-04-2022	Concept	Omzetten naar studiejaar 2021-2022

Modulehandleiding iipforit

1. Inleiding

In dit project vormen studenten in groepjes een particulier digitaal recherchebureau, wiens hulp wordt ingeroepen door de plaatselijke politie bij het onderzoek naar, mogelijk, enige strafbare feiten. Het onderzoek start echter eerst individueel maar wordt vanaf de tweede fase in groepsverband uitgevoerd. Aan bod komen het opzetten van een goed digitaal 'crimelab', het gebruik van diverse forensische ICT tools voor veiligstelling en analyse van verschillende digitale bewijsplaatsen. Centraal staat hierbij de bevoegdheden waarbinnen bepaalde tools en/of vormen van onderzoek mogen plaatsvinden.

2. Algemene informatie

2.1. Inleiding

In deze periode werk je aan de onderwijseenheid iipforit:

Naam module/versie	Project Inleiding FICT
Toetsvorm	Project
Studiefase	Propedeuse
Modulecode	iipforit
Aantal EC	7
Studiebelasting	7 * 28 = 196 uur (3-4 dagen per week)
Lesvorm	Projectbesprekingen en werkcolleges
Literatuur	Geen
Naam moduleleider	Jaap Haasnoot

2.2. Leerdoelen

Forensisch ICT Onderzoek doen en presenteren binnen het wettelijk kader

Subleerdoelen:

De student kan:

- een specialisatiespecifiek project voorbereiden en uitvoeren;
- specialisatiespecifiek onderzoek verrichten en op basis daarvan conclusies trekken en een plan van aanpak uitwerken;
- de beoogde, specialisatiespecifieke resultaten ontwerpen en realiseren;
- het gerealiseerde resultaat presenteren aan de doelgroep;
  Meer specifiek: op overtuigende wijze aan de rechtelijke macht rapporteren en presenteren;
- specialisatiespecifieke detailvragen inzake het gerealiseerde naar tevredenheid van de vraagsteller beantwoorden;
- de chain-of-evidence (CoE) en de chain-of-custody (CoC) bewaken;
- forensische ict technieken binnen het gestelde wettelijk kader gebruiken;
- wetteksten en jurisprudentie opzoeken, lezen en interpreteren voor het (eigen) onderzoek;

Let op: Je bent zelf verantwoordelijk dat je in het oog houdt dat je alle bovenstaande leerdoelen bereikt.

2.3. Werkvormen

In deze module werk je aan het bereiken van de leerdoelen door samen te werken met collega studenten. De groepen, welke vanaf lesweek 2 worden samengesteld, hebben wekelijks begeleiding waarin producten worden besproken. Deze begeleiding vindt waar mogelijk met meerdere groepen tegelijkertijd of centraal plaats. Daarnaast worden er vrijwel iedere specialisatiedag twee werkcolleges gehouden waarin jullie opdrachten uit te voeren die verband houden met het project. Alvorens jullie hier aan kunnen deelnemen, dienen er kennisclips te worden gekeken en/of materiaal te worden bestudeerd. Daarnaast worden er soms ook kennisclips/materiaal aangeboden waaraan geen werkcollege is gekoppeld, maar wat wel belangrijk is voor jullie project.

2.4. Werkcolleges

Aan deze module zijn meerdere werkcolleges gekoppeld, de uitwerkingen van de werkcolleges lever je per week in via Teams opdrachten:

'Forensisch proces – preparation fase'
We gaan aan de slag met activiteiten uit deze fase door deze direct op de projectcasus toe te passen.

'Internetonderzoek - de basis'
In dit werkcollege wordt een gestructureerde manier van onderzoek in open bronnen uitgeleerd. Er wordt o.a. ook aandacht besteed aan vereiste items die tenminste vastgelegd dienen te worden voor een forensisch onderzoek. Verder komen onderzoekstechnieken en mindmapping aan de orde. We oefenen aan de hand van een opdracht.

'Rapportage en CoE visualiatie'
Hierin worden de eisen rondom rapportage geoefend en wordt een eerste CoE visualisatie gemaakt op een bestaande casus.

'Analyse-tools'
Er zijn veel applicaties beschikbaar waarin je je onderzoek kunt doen. In dit werkcollege belichten we er aantal en gaan we hiermee oefenen.

'Mobile Forensics'
Een telefoon kan hele waardevolle informatie bevatten voor een onderzoek. Dit werkcollege gaat over de commerciële tools die beschikbaar zijn om op een forensische wijze van mobiele apparaten een kopie te maken.

'Network Forensics'
We gaan oefenen met het analyseren van netwerkverkeer.

'Linux Artifacts'
In dit werkcollege gaan we kijken naar belangrijke/handige bewijsplaatsen die het Linux besturingssysteem kent.

'Ethiek'
Gedurende het project en in het vervolg van de opleiding worden jullie allerlei technieken aangeleerd. Dit werkcollege gaat in op de ethische verantwoordelijkheid die hierbij komen kijken.

'Reflectie'
We willen dat jullie gaan reflecteren op het totale project.

'Dossieropbouw en presenteren'
De laatste stap voor het afronden van het onderzoek.

Mogelijk wordt het programma aangepast indien het docententeam dit nodig acht.

3. Organisatie module

3.1. Kick-off

Het project start met uitreiking van de casus, een uitleg over het project, wat de doelen zijn en wat de eerste opdrachten zijn die jullie individueel moeten gaan uitvoeren. Na de kick-off starten we met de eerste werkcolleges die van belang zijn om het onderzoek op te starten. De projectgroepindeling wordt in lesweek 2 bekend gemaakt en wordt samengesteld aan de hand van de eerste oplevering (fase 1) die een ieder individueel dient te doen.

3.2. De opdrachten

De studenten dienen achtereenvolgend de volgende opdrachten uit te voeren:

1. Maken plan van aanpak en onderzoek naar bevoegdheden
2. Beschrijven en opzetten van onderzoeksomgeving

3. Vooronderzoek uitvoeren
4. Internetonderzoek uitvoeren en vastleggen
5. Internetonderzoek rapporteren in deelrapportages
6. Digitaal onderzoek volgende bewijsplaats(en), vastleggen en rapporteren in deelrapportages
7. Dossieropbouw en presenteren

Zie de onderwijsgroep voor de specifieke casus en de toets.

3.3. Leermiddelen

3.3.1 Onderwijsgroep

Bij deze module hoort de onderwijsgroep: **OG2223.IIPFORIT Project Inleiding FICT**
Hier is belangrijke informatie geplaatst en kunnen de benodigde documenten worden opgehaald.

3.3.2 Tools

Tijdens dit project dienen er verschillende forensisch tools gebruikt te worden. Er wordt verwacht dat de tools/technieken die in de werkcolleges zijn onderwezen en geoefend, worden gebruikt in het onderzoek. Daarnaast zijn er ook tools/technieken bekend uit iifito en wordt jullie ook commerciële tools ter beschikking gesteld. In sommige gevallen wordt er vereist dat je een specifieke tool inzet. In andere gevallen heb je de vrijheid om zelf je tooling te kiezen.

3.3.3 Microsoft Teams

Microsoft Teams wordt ingezet om buiten de specialisatiedag te communiceren. Daarnaast is er vanaf lesweek 2 per groep een privé kanaal beschikbaar waar opleveringen worden gedaan en onderling gecommuniceerd kan worden.

3.4. Contact met de politie

Gedurende het project kun je vragen stellen aan de opdrachtgever door te mailen naar: ‘politie.hogeschoolleiden@gmail.com’. Daarnaast dien je de opdrachtgever op de hoogte te houden van de tussenresultaten van het onderzoek door een terugkoppeling te doen. De terugkoppeling dient dan te worden gedaan in de vorm van de groeps-deelrapportage (niet technisch!) waarin o.a. de onderzoeksvragen worden beantwoord en aanbevelingen/vervolgstappen worden aangegeven. De groeps-deelrapportage dient in PDF-formaat te worden aangeleverd.

Alleen op deze manier kunnen jullie tot volgende bewijsstukken komen. Dat betekent dat als jullie geen terugkoppeling doen aan de politie, de planning (zie hoofdstuk 5) mogelijk niet kan worden gevolgd. Dit kan een belemmering zijn bij bepaalde werkcolleges op de specialisatiedag en het verdere verloop van het onderzoek met een mogelijke herkansing tot gevolg. Zorg er daarom voor dat je de politie op de hoogte houdt conform de planning (zie hoofdstuk 5).

4. Beoordeling

Het project is opgedeeld in verschillende fasen. Per fase vindt er een formatieve beoordeling plaats, dat wil zeggen dat dit nog geen definitieve beoordeling is maar dat je hierop feedback ontvangt. Deze feedback kan centraal worden teruggegeven aan meerdere groepen tegelijkertijd. Waar nodig breng je de verbeteringen aan, die voor jullie van toepassing zijn, in deze fase voor de definitieve oplevering (fase 5).

Als jullie volgens onderstaand schema werken, houdt dit in dat in lesweek 7 de eindpresentatie en de beoordeling van het totale project zal plaatsvinden. Jullie leveren dan alle gemaakte producten/deliverables (eventueel met uitzondering van de presentatie) op maandag 12 juni in. Uiteindelijk presenteren jullie dan op woensdag 14 juni het uitgevoerde onderzoek.

Voor de beoordeling wordt meegenomen:

- De gemaakte werkcollege opdrachten
- De definitieve project documentatie van alle fases
- De eindpresentatie

Zie de toetsbeschrijving voor meer details.

Modulehandleiding iipforit

5. Planning - oplevering van fases

Onderstaande opleveringen zijn bedoeld om sturing te geven aan het project en zijn ook onderwerp van gesprek tijdens de opvolgende vergadering op de woensdag. Bij voorkeur zijn de desbetreffende onderdelen dan volledig uitgewerkt zodat ook de terugkoppeling aan de politie kan worden gedaan. Als dat echter niet het geval is dan kan de oplevering aan de politie ook later worden gedaan. Zorg wel dat je dit alsnog zo snel mogelijk doet zodat je geen (grote) vertraging oploopt. Alleen in fase 5 (concept) – lesweek 6 is ruimte om een geringe vertraging in te lopen!

Lesweek	**Onderdelen**
Lesweek 2 (maandag voor 09.00 uur)	Inleveren – individueel : Onderzoeksplan, beschrijving en opzetten van de onderzoeksomgeving, vooronderzoek en mindmaps internetonderzoek (fase 1)
Lesweek 3 (maandag voor 09.00 uur)	Inleveren: samenwerkingsovereenkomst, samengevoegd onderzoeksplan, planning en rapportages internetonderzoek, plus de onderzoeksdocumentatie volgend bewijsstuk (fase 2)
Lesweek 4 (maandag voor 09.00 uur)	Inleveren: onderzoeksdocumentatie volgend bewijsstuk (fase 3)
Lesweek 5 (**dinsdag** voor 09.00 uur)	Inleveren: onderzoeksdocumentatie volgend bewijsstuk (fase 4)
Lesweek 6 (maandag voor 09.00 uur)	Inleveren: volledig project (fase 5) – concept - Denk aan eindrapportage, visualisatie CoE, etc.
Lesweek 7 (maandag voor 09.00 uur)	Inleveren: volledig project (fase 5) – definitief - **gelegenheid 1** • Iedere groep levert op, dus ook als de producten incompleet zijn of als er nog onvoldoende onderzoek is gedaan. Er vindt altijd een beoordeling plaats over gelegenheid 1.
Lesweek 7 (woensdag 14 juni 2023)	Presentatie (fase6) • Deze vindt alleen plaats met de groepen die een complete oplevering en/of voldoende onderzoek hebben gedaan. Welke groepen dit zijn, zal in een programma bekend worden gemaakt. Zelfs als je mag presenteren zegt dit nog niets over een (positieve) eindbeoordeling. Het kan nog steeds zo zijn dat er verbeteringen moeten worden doorgevoerd bij gelegenheid 2. Groepen die niet in staat worden gesteld om te presenteren zullen deze dag nog wel feedback ontvangen.
Lesweek 8 (maandag voor 09.00 uur)	Inleveren: herkansing volledig project (fase 5) – definitief - **gelegenheid 2**
Lesweek 8 (woensdag 21 juni 2023)	Herkansing: presentatie (fase 6) • Deze vindt ook plaats bij een incomplete oplevering of onvoldoende onderzoek. Er wordt dus ten alle tijden een presentatie gehouden.

Bovenstaande opleveringen, met uitzondering van fase 1, verlopen via het privé-kanaal van de groep in Microsoft Teams. Zorg dat de definitieve oplevering (van fase 5) niet vermengt raakt met eventuele concepten! Maak een duidelijke mappenstructuur waardoor voor jullie én voor de examinator geen verwarring ontstaat.

Alle reguliere documenten moeten in pdf-formaat worden ingeleverd, met uitzondering van specifieke bestandsformaten zoals mindmaps en Excel, welke in het originele bestandsformaat moeten worden aangeleverd.

Let op: zorg dat je images en geëxporteerde bestanden in één aparte map 'Bewijskluis' opneemt, welke in de root van de oplevermap is opgenomen. Ga dergelijke bestanden dus niet nestelen in allerlei verschillende sub-mappen.