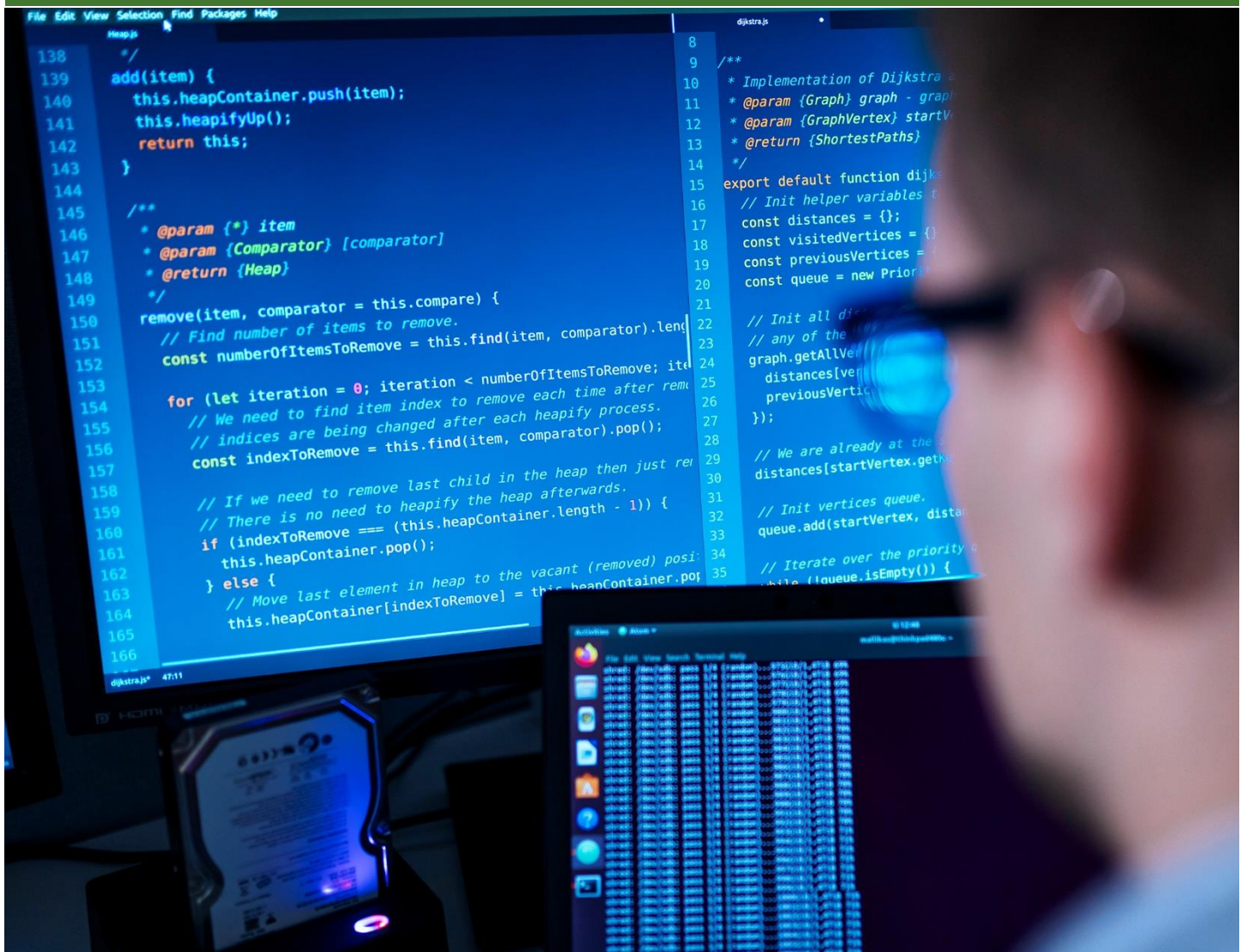


# Kyberrikostorjunnan erikoistumisopintojen (35 op) opetussuunnitelma 2022–2024



Opetussuunnitelma on käsitelty koulutustoiminnan ohjausryhmässä 29.3.2022. Poliisiammatti-korkeakoulun hallitus on hyväksynyt Kyberrikostorjunnan erikoistumisopinnot opetussuunnitelman 3.5.2022 (POL-2022-41462).

Euroopan Unionin Sisäisen turvallisuuden rahasto on tukenut Kyberrikostorjunnan erikoistumisopinnot hanketta.



**SISÄISEN TURVALLISUUDEN RAHASTO**  
- POLIISIYHTEISTYÖ, RIKOLLISUUDEN  
EHKÄISEMINEN JA TORJUMINEN SEKÄ  
KRIISINHALLINTA  
Euroopan unionin tuella

## Sisällys

1 Tavoitteena ammattitaito .....	3
2 Eurooppalainen ja kansallinen tutkintojen viitekehys .....	4
3 Pedagogiset linjaukset opetussuunnitelman taustalla.....	4
4 Kestävä kehitys poliisikoulutuksessa.....	5
5 Osaamisperustainen opetussuunnitelma.....	6
6 Opiskelijavalinnat ja opintojen suoritus aika .....	6
7 Opetukseen osallistuminen .....	7
8 Opintosuoritusten arviointi.....	7
9 Opetussuunnitelma ja opetuksen toteuttaminen.....	7
10 Opintojaksot.....	8
11 Pakolliset opinnot (20 op).....	9
11.1 Kyberrikostorjunnan perusteet / Core Concepts in Digital Investigations and Forensics (15 op).....	9
11.2 Kehittämistehtävä (5 op).....	10
12 Vapaasti valittavat opinnot (15 op) .....	11
12.1 Darkweb ja kryptovaluutat (2 op) .....	11
12.2 Forensiikkaohjelmoinnin perusteet (3 op) .....	12
12.3 Haittaohjelma-analyysin perusteet (3 op).....	12
12.4 Internet rikostorjunnassa (1,5 op) .....	13
12.5 Internet rikostorjunnassa jatkokurssi (1,5 op).....	14
12.6 Laiteläheinen digitaaliforensiikka (2 op) .....	15
12.7 Linux tutkintatyökaluna (3 op) .....	15
12.8 MacOS-forensiikka (4 op) .....	16
12.9 Mobiiliforensiikan perusteet (3 op) .....	17
12.10 Mobiiliforensiikan jatkokurssi (4 op) .....	18

12.11 Muisti- ja liveforensiikka (3 op).....	18
12.12 Taktisen kyberrikostutkinnan perusteet (2 op).....	19
12.13 Taktisen kyberrikostutkinnan jatkokurssi (2 op).....	20
12.14 Tietoliikenneteknologiat ja -protokollat (2 op).....	21
12.15 Verkkorikostutkinnan peruskurssi (2 op).....	22
12.16 Verkkorikostutkinnan jatkokurssi (2 op).....	22
12.17 Windows-forensiikka (4 op).....	23
12.18 NCFI Level 2 -opintojaksot (15 op).....	24

## 1 Tavoitteena ammattitaito

Erikoistumisopinnot ovat korkeakoulututkinnon jälkeen suoritettavaksi tarkoitettuja, jo työelämässä toimineille suunnattuja ammatillista kehittymistä ja erikoistumista edistäviä pitkäkestoisia koulutuksia. Erikoistumisopinnoilla luodaan järjestelmällinen mahdollisuus peruskoulutuksen (poliisi (AMK) tai sitä edeltävät tutkinnot tai muut soveltuvat korkeakoulututkinnot) suorittaneille ja työelämässä jo toimineille henkilöille syventää asiantuntijuutta, suunnata osaamista muutoin kuin tutkintoon johtavassa koulutuksessa ja tukea joustavasti uusien nousevien asiantuntijuusalueiden tarpeita ensisijaisesti poliisille ja mahdollisuuksien mukaan muille viranomaisille.

Poliisilta edellytetään monitasoista osaamista, joka pohjaa poliisitoiminnassa yleisesti hyväksytyihin arvoihin ja toimintaperiaatteisiin. Poliisiammattikorkeakoulun (Polamk) tehtävänä on antaa sisäisen turvallisuuden alalla tutkimukseen ja sivistyksellisiin lähtökohtiin perustuvaa korkeakouluopetusta ammatillisiin asiantuntijatehtäviin ja johtamistehtäviin sekä tukea yksilön ammatillista kasvua ja edistää elinikäistä oppimista. Lisäksi Poliisiammattikorkeakoulu harjoittaa soveltavaa tutkimus- ja kehitystyötä, joka palvelee poliisitoiminnan ja sisäisen turvallisuuden suunnittelua ja kehittämistä sekä Poliisiammattikorkeakoulun opetusta.

Kyberrikostorjunnan erikoistumisopinnojen tavoitteena on, että opiskelija saa riittävät teoreettiset ja käytännölliset perustiedot ja -taidot kyberrikostorjunnan tehtävissä toimimista varten sekä valmiuksia työyhteisön ja itsensä kehittämiseen.

Kyberrikostorjunnan erikoistumisopinnoista valmistunut opiskelija:

- omaa laaja-alaiset käytännölliset perustiedot ja -taidot sekä niiden teoreettiset perusteet kyberrikostorjunnan asiantuntijatehtävissä toimimista varten
- on hankkinut valmiudet jatkuvaan oppimiseen ja osaa arvioida omaa ammatillista kasvuaan kyberrikostorjunnan tehtävissä
- osaa arvioida ja kehittää oman organisaationsa ja työyhteisönsä toimintaa kyberrikostorjunnan alalla.

Opiskelija saa todistuksen saamastaan koulutuksesta Poliisiammattikorkeakoululta.

## 2 Eurooppalainen ja kansallinen tutkintojen viitekehys

Eurooppalaisessa tutkintojen viitekehyksessä (European Qualifications Framework, EQF) ja tutkintojen ja muun osaamisen kansallisessa viitekehyksessä tutkinnot on sijoitettu osaamisen perusteella tietyille vaativuustasolle. Suomi on sitoutunut EQF-vaativuustasoluokitteluun. Laki ([93/2017](#)) ja asetus ([120/2017](#)) kansallisesta tutkintojen ja muiden osaamiskokonaisuuksien viitekehuksesta määrittelee tutkintojen, oppimäärien ja muiden osaamiskokonaisuuksien sijoittumisen eri vaativuustasoille. Kullekin tasolle on kuvattu, mitä ko. tason saavuttanut opiskelija tietää, ymmärtää ja pystyy tekemään. Osaamistasokuvauksia sovelletaan Polamkin opetussuunnitelmatyössä, osaamisprofiilien laadinnassa ja osaamisen arvioinnissa.

Kyberrikostorjunnan erikoistumisopinnot ovat tasoa 6. Kansallisessa tutkintojen viitekehyksessä taso 6 sekä valtakunnalliset yhteiset kompetenssit kuvaavat ammattikorkeakoulusta valmistuvan opiskelijan osaamisen tasoa.

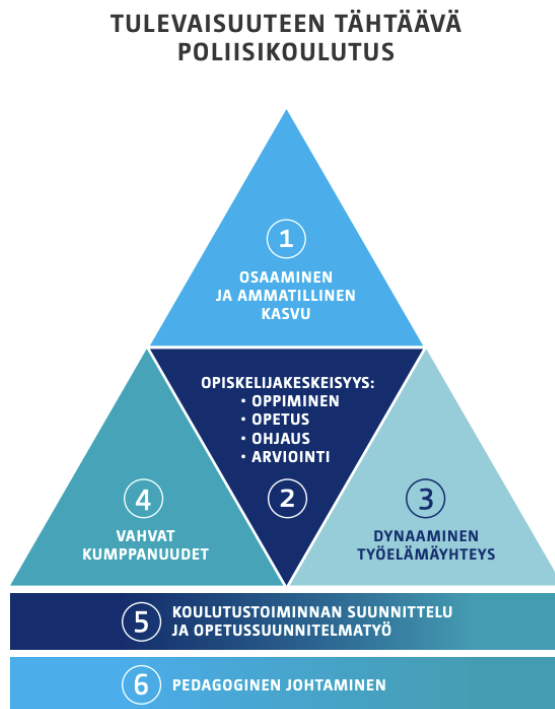
### Taso 6 (ammattikorkeakoulututkinnot, alemmat korkeakoulututkinnot)

- Hallitsee laaja-alaiset ja edistyneet oman alansa tiedot, joihin liittyy teorioiden, keskeisten käsitteiden, menetelmien ja periaatteiden kriittinen ymmärtäminen ja arvioiminen.
- Ymmärtää ammatillisten tehtäväalueiden ja/tai tieteenalojen kattavuuden ja rajat.
- Hallitsee edistyneet kognitiiviset ja käytännön taidot, jotka osoittavat asioiden hallintaa, kykyä soveltaa ja kykyä luoviin ratkaisuihin ja toteutuksiin, joita vaaditaan erikoistuneella ammatti-, tieteen- tai taiteenalalla monimutkaisten tai ennakoimattomien ongelmien ratkaisemiseksi.
- Työskentelee itsenäisesti alan asiantuntijatehtävissä ja kansainvälisessä yhteistyössä tai toimii yrittäjänä.
- Johtaa monimutkaisia ammatillisia toimia tai hankkeita.
- Kykenee päätöksentekoon ennakoimattomissa toimintaympäristöissä.
- Vastaa oman osaamisensa arvioinnin ja kehittämisen lisäksi yksittäisten henkilöiden ja ryhmien kehityksestä.
- Valmius elinikäiseen oppimiseen.
- Toimii erilaisten ihmisten kanssa opiskelu- ja työyhteisössä sekä muissa ryhmissä ja verkostoissa huomioiden yhteisölliset ja eettiset näkökulmat.
- Viestii hyvin suullisesti ja kirjallisesti sekä alan että alan ulkopuoliselle yleisölle äidinkielellään.
- Viestii ja on vuorovaikutuksessa toisella kotimaisella kielellä sekä kykenee kansainväliseen viestintään ja vuorovaikutukseen omalla alallaan ainakin yhdellä vieraalla kielellä. (Valtioneuvoston asetus (120/2017) kansallisesta tutkintojen ja muiden osaamiskokonaisuuksien viitekehuksesta.)

## 3 Pedagogiset linjaukset opetussuunnitelman taustalla

Poliisiammattikorkeakoulun pedagogisten linjausten tavoitteena on varmistaa yhteinen käsitys opetuksesta ja oppimisesta, laadukas opetustoiminta sekä hyvinvoiva työyhteisö. Pedagogisia linjauksia tukevat koulutustoiminnan suunnittelu, opetussuunnitelmatyö ja pedagoginen johtaminen.

Kuva 1: Polamkin pedagogisen toiminnan elementit



## 4 Kestävä kehitys poliisikoulutuksessa

Poliisin visio on: Poliisi on kaikkien turvaaja, kaikkina aikoina. Poliisin tavoitteena on:

- turvata arki ja pitää luottamus poliisiin korkeana
- estää rikoksia ja häiriöitä ennalta
- paljastaa ja selvittää tehokkaasti erityisesti vakavia rikoksia
- tuottaa nykyaikaisia, turvallisia ja kehittyviä palveluita
- tehdä yhteistyötä ja viestiä tehokkaasti.

Oikeudenmukaisuus, osaaminen, palvelu ja henkilöstön hyvinvointi ovat arvot, joiden mukaan poliisi toimii. Poliisilla on vuonna 2019 vahvistettu eettinen koodisto.

Kestävä kehitys jaetaan usein ekologiseen, taloudelliseen ja sosiaalis-kulttuuriseen ulottuvuuteen, jotka vaikuttavat toisiinsa (Rohweder L. ym. 2008)<sup>1</sup>. Koulutuksen ekologista kestävyyttä voidaan edistää esimerkiksi luonnonvaroja säästävillä opetusmenetelmillä, kuten verkko-opiskelulla tai simulaatioiden hyödyntämisellä. Taloudellinen kestävyys asettaa reunaehdot poliisi (AMK) -tutkintokoulutuksen suunnittelulle ja toteuttamiselle.

Sosiaalis-kulttuurinen kestävyys on luonteva osa poliisikoulutusta ja sen sisältöjä. Se näkyy mm. perus- ja ihmisoikeuksien sekä tasa-arvon ja yhdenvertaisuuden kunnioittamisena niin koulutuksen sisällöissä kuin toteutuksessa. Poliisitoiminnan sosiaalis-kulttuurista ulottuvuutta mitataan

<sup>1</sup> Rohweder Liisa, Virtanen Anne, Tani Sirpa, Kohl Johanna ja Arja Sinkko (2008) Näkökulmia opetukseen ja oppimiseen. Rohweder, L. & Virtanen, A. (toim.). Kohti kestävä kehitystä. Pedagoginen lähestymistapa. Opetusministeriön julkaisuja 2008:3. Luettavissa elektronisesti: valtioneuvosto.fi.

säännöllisesti poliisibaroometrilla, jonka tulokset kertovat luottamuksesta poliisiin. Polamkin koulu tukee etenkin sosiaalis-kulttuurisesti kestävästä kehitystä yhteiskunnassa. Tavoitteena on kouluttaa tasa-arvoisesti, yhdenvertaisesti, oikeudenmukaisesti ja eettisesti toimivia poliiseja.

## 5 Osaamisperustainen opetussuunnitelma

Polamkin opetussuunnitelmat ovat osaamisperustaisia. Osaamisperustaisissa opetussuunnitelmissa määritellään tutkinnon ja tutkinnon opintojen osaamistavoitteet eli mitä opiskelijan tulee tietää, ymmärtää ja osata oppimisprosessin tuloksena. Arviointi kohdistuu oppimistuloksiin ja perustuu osaamistavoitteisiin. Arvioinnin periaatteet on kuvattu Poliisiammattikorkeakoulun tutkintösäännössä.

Opetusta ja opiskelua ohjaavana tekijänä ovat tavoitteellinen osaamisen kehittäminen, oppimisen näkökulman vahvistaminen ja työelämälähtöisten opintokokonaisuuksien rakentaminen.

Osaamisperustaisuuden piirteitä erikoistumisopinnoissa ovat mm. seuraavat: <sup>2</sup>

- Opiskelijan itsearviointi on merkittävässä roolissa opintopolulla.
- Osaamista tunnustetaan ja tunnustetaan riippumatta siitä, missä, milloin tai miten osaaminen on hankittu.
- Koulutuksessa toteutuu henkilökohtaistetut ja yksilölliset opintopolut.
- Opettajalla vahva rooli ohjaajana ja osaamisen tunnistajana.
- Opetussuunnitelma rakentuu työelämärelevantteista osaamisalueista.
- Osaamisalueet sisältävät opiskelijalähtöiset osaamistavoitteet.
- Osaamistavoitteille on määritelty selkeät arviointikriteerit.
- Puuttuvaa osaamistavoitteiden mukaista osaamista voidaan hankkia ja täydentää eri tavoin.
- Osaamista arvioidaan jatkuvasti, monipuolisesti ja monen arvioijan toimesta.

## 6 Opiskelijavalinnat ja opintojen suoritus aika

Koulutuksen kohderyhmänä ovat kyberrikostorjunnan asiantuntijatehtävissä toimivat tai sellaisiin koulutettavat virkamiehet. Poliisiammattikorkeakoulu päättää opiskelijavalinnan perusteista, hakumenettelystä ja opiskelijaksi hyväksymisestä. Poliisiammattikorkeakoulun ohjesäännön mukaan erikoistumisopintojen valintaperusteet vahvistaa Poliisiammattikorkeakoulun hallitus.

Kyberrikostorjunnan erikoistumisopintojen laajuus on 35 opintopistettä ja sen tavoitteellinen suoritus aika on kaksi vuotta. Opiskelijan opiskeluoikeus on voimassa kolme vuotta. Jos komentava yksikkö on tehnyt opiskelijan opintojen keskeytysesityksen, voidaan hänet yksikön pyynnöstä ottaa opiskelijaksi seuraavalle vastaavalle toteutukselle.

---

<sup>2</sup> Alaniska, Hanna, Keurulainen Harri, Tauriainen Tiia-Mariia (toim.) 2019. Osaamisperustaisia käytäntöjä korkeakouluissa. Oulun ammattikorkeakoulun tutkimus- ja kehitystyön julkaisut, ePooki 58/2019.



## 7 Opetukseen osallistuminen

Opinnoilla edellytetään läsnäoloa luennoilla ja harjoituksissa.

Koulutuksessa eteneminen edellyttää, että opiskelijan on suoritettava hyväksytysti kaikki koulutukseen kuuluvat opintosuoritukset. Erikoistumisopintoihin sisältyy kehittämistehtävä.

Poliisihallinnon palveluksessa olevat erikoistumisopintojen opiskelijat ovat lähtökohtaisesti kaikki poliisiyksikön koulutukseen komennettuja virkamiehiä, jotka koulutukseen osallistumalla täyttävät virkamiehelle kuuluvaa työntekovelvoitettaan.

Opiskelijan sairastuessa hänen on ilmoitettava näin syntyneestä poissaolostaan normaalin työpaikan sairaustapauksista ilmoittamisen ohjeistusten lisäksi myös vastuuopettajalle.

Mikäli opiskelijalle tulee lähiopetusjaksolla poissaoloja, tulee hänen suorittaa erikseen opintojakson vastuuopettajan määräämät korvaavat harjoitukset/oppimistehtävät tai tarvittaessa suorittaa opintokokonaisuus uudelleen.

## 8 Opintosuoritusten arviointi

Arvioinnilla ohjataan ja varmistetaan opiskelijan opintojen tavoitteiden saavuttamista. Opintojen arviointi on osa oppimis- ja opetusprosessia, ja opintosuoritukset arvioidaan opintojakson päättyttyä. Arvioinnin peruserä on, että opiskelijan suorituksia verrataan opetussuunnitelman osaamistavoitteisiin. Arvioinnissa noudatetaan Polamkin tutkintosääntöä.

Kirjallisten töiden sekä kehittämistehtävän analysoimisessa käytetään plagioinnintunnistusohjelmaa. Opiskeluvilppitapausten käsittelyssä noudatetaan kyseisestä aiheesta annettua Poliisiammattikorkeakoulun ohjetta.

## 9 Opetussuunnitelma ja opetuksen toteuttaminen

Opetussuunnitelmassa on kuvattu vaadittavat opintosuoritukset. Erikoistumisopintojen opetussuunnitelman hyväksyy Poliisiammattikorkeakoulun hallitus. Kunkin opintojakson tarkempi sisältö ja toteutus kuvataan toteutussuunnitelmissa, jotka hyväksyy koulutuspäällikkö.

Opinnot koostuvat seuraavista pakollisista opintojaksoista:

- Kyberrikostorjunnan perusteet (Core Concepts in Digital Investigations and Forensics) (15 op)
- Kehittämistehtävä (5 op).

Pakollisten opintojaksojen lisäksi opiskelija valitsee vähintään 15 opintopistettä vapaasti valittavia opintoja kurssitarjottimelta. Opintojaksojen opetusmateriaalit ovat osin englanninkielisiä. Joillakin opintojaksoilla opetus voidaan toteuttaa englanniksi.

Muulla suoritettuja soveltuvia korkeakoulutasoisia opintoja voidaan sisällyttää osaksi erikoistumisopinnot vapaa- tai valittavien opintojaksot. Sisällytettävien opintojen osalta ei edellytetä sisällöllistä vastaavuutta erikoistumisopinnot opintojaksoihin, mutta niiden on tuettava poliisin ammatillisen kyberosaamisen kehittymistä. Opiskelijan pitää hakemuksessaan perustella, miten sisällytettävät opinnot tukevat poliisin ammatillista kehittymistä. Opiskelijan tulee hyväksyttää opetussuunnitelman ulkopuoliset opintosuoritukset koulutuksen vastuupettajilla.

Opintojaksojen opetusmateriaalit ovat osin englanninkielisiä. Joillakin opintojaksoilla opetus voidaan toteuttaa englanniksi.

Kuva 2: Kyberrikostorjunnan erikoistumisopinnot (35 op)



## 10 Opintojaksot

### Pakolliset opinnot (20 op)

- Kyberrikostorjunnan perusteet (Core Concepts in Digital Investigations and Forensics) (15 op)
- Kehittämistehtävä (5 op).

### Vapaa- tai valittavat opinnot (vähintään 15 op)

Vapaa- tai valittavat opintojaksot tulevat haettaviksi Polamkin täydennyskoulutuksen koulutuska- lenteriin ja niihin haetaan opintohallintojärjestelmän kautta.

- 1) Darkweb ja kryptovaluutat (2 op)
- 2) Forensikkaohjelmoinnin perusteet (3 op)
- 3) Haittaohjelma-analyysin perusteet (3 op)
- 4) Internet rikostorjunnassa (1,5 op)
- 5) Internet rikostorjunnassa jatkokurssi (1,5 op)



- 6) Laiteläheinen digitaaliforensiikka (2 op)
- 7) Linux tutkintatyökaluna (3 op)
- 8) MacOS-forensiikka (4 op)
- 9) Mobiiliforensiikan perusteet (3 op)
- 10) Mobiiliforensiikan jatkokurssi (3 op)
- 11) Muisti- ja liveforensiikka (3 op)
- 12) Taktisen kyberrikostutkinnan perusteet (2 op)
- 13) Taktisen kyberrikostutkinnan jatkokurssi (2 op)
- 14) Tietoliikenneteknologiat ja -protokollat (2 op)
- 15) Verkkorikostutkinnan peruskurssi (2 op)
- 16) Verkkorikostutkinnan jatkokurssi (2 op)
- 17) Windows-forensiikka (4 op).

Edellä listattujen opintojaksojen lisäksi vapaasti valittaviin opintoihin voi sisällyttää yhteispohjaisen Nordic Computer Forensic Investigators -koulutusohjelman (NCFI) tason kaksi moduulia. Opintojaksoja hallinnoi Norjan Politihøgskolen (PHS). NCFI-koulutusohjelman tason 2 opintojaksoille hakeudutaan PHS:n hakujärjestelmän kautta. Opetus on englannin kielistä. Kyberrikostorjunnan erikoistumisopintojen vapaasti valittaviin opintojaksoihin voidaan sisällyttää seuraavat moduulit:

- Module 2A Advanced Computer Forensics (15 op)
- Module 2B Online Investigation (15 op)
- Module 2C Network Forensics and Cybercrime (15 op)
- Module 2D Mobile Extraction and Artifacts (15 op)

## 11 Pakolliset opinnot (20 op)

### 11.1 Kyberrikostorjunnan perusteet / Core Concepts in Digital Investigations and Forensics (15 op)

#### **Kuvaus**

Opintojaksolla annetaan tutkijalle perustiedot toimia kyberrikostorjuntaan liittyvissä tehtävissä. Opintojakson tavoitteena on lisätä ymmärrystä digitaaliforensiikan menetelmistä, keskeisistä periaatteista ja lainsäädännöstä sekä niiden soveltamisesta kyberrikosten tutkintaan.

Opintojakso on yhdenmukainen Nordic Computer Forensic Investigators -koulutusohjelman (NCFI) moduulin 1 kanssa. Opintojakson suorittaminen antaa hakukelpoisuuden NCFI-koulutusohjelman tason 2 opintojaksoille.

#### **Osaamistavoitteet**

Opintojakson suorittamisen jälkeen opiskelija:

- osaa nähdä digitaaliforensiikan roolin laajemmasta näkökulmasta rikostutkinnan aikana
- tunnistaa eettiset ja oikeudelliset kysymykset tutkinnan aikana
- osaa arvioida ja soveltaa asiaankuuluvaa lainsäädäntöä tutkinnassa
- osaa tulkita tietoteknisistä laitteista löytyvää todistusaineistoa

- osaa käyttää digitaaliforensisia työkaluja ja analysoida tuloksia.

### **Asiakokonaisuudet**

- Digitaaliforensiikan menetelmät ja niiden soveltaminen rikostutkinnassa
- Lainsäädäntö
- Tietoverkkorikollisuus ja sen tutkinta

### **Vaadittavat suoritukset**

Luennoille osallistuminen, harjoitusten ja tentin hyväksytyt suorittaminen.

### **Arviointiasteikko**

Opintojakso arvioidaan asteikolla hyväksytyt/hylättyt.

### **Edeltävät opinnot**

Ei edellytetä.

## **11.2 Kehittämistehtävä (5 op)**

### **Kuvaus**

Kehittämistehtävä on käytännönläheinen hanke, jonka opiskelija toteuttaa opintojensa aikana.

Kehittämistehtävä lisää valmiuksia toimia omassa organisaatiossa erilaisissa kehittämishankkeissa ja -tehtävissä aktiivisena toimijana ja antaa perustiedot projektin johtamisesta sekä laatu-työhön työnjohdon näkökulmasta. Kyberrikostutkinnan erikoistumisopinnojen kehittämistehtävätyöskentelyssä sekä -raportoinnissa noudatetaan soveltuvin osin poliisi (AMK) -tutkinnon opinnäytetyöohjeita.

### **Osaamistavoitteet**

Opintojakson suorittamisen jälkeen opiskelija:

- osaa laatia kehittämistehtävän suunnitelman/projektisuunnitelman
- osaa toteuttaa käytännönläheisen kehittämishankkeen
- osaa raportoida kehittämishankkeen tuloksista
- osaa kriittisesti arvioida kehittämistoiminnan toteutumista ja esittää jatkosuunnitelmia
- osaa kehittää toimintaa seurannan ja palautteen avulla

### **Asiakokonaisuudet**

- Toiminnan ja laadun kehittäminen
- Kehittämistehtävän suunnittelu ja raportointi
- Projektityö
- Kehittämismenetelmät
- Kehittämistehtävän toteuttaminen

### **Vaadittavat suoritukset**

Kehittämistehtävän hyväksytyt suorittaminen.

### **Arviointiasteikko**

Opintojakso arvioidaan asteikolla 0–5.

### **Edeltävät opinnot**

Kyberrikostorjunnan perusteet (Core Concepts in Digital Investigations and Forensics) (15 op).

## **12 Vapaasti valittavat opinnot (15 op)**

Vapaasti valittavilla opintojaksoilla on sekä pakollisia että suositeltavia esitietovaatimuksia.

Nämä on kuvattu kunkin opintojakson opetussuunnitelmassa kohdassa edeltävät opinnot. Suositeltavat edeltävät opinnot edistävät opintojakson osaamistavoitteiden saavuttamista.

### **12.1 Darkweb ja kryptovaluutat (2 op)**

#### **Kuvaus**

Opintojakson tavoitteena on tarjota opiskelijoille, jotka eivät ole erikoistuneet tietotekniikkaan, yleiskatsaus sekä käytännön harjoituksia siitä, miten rikolliset käyttävät Internetiä, kryptovaluuttoja ja pimeää verkkoa.

#### **Osaamistavoitteet**

Opintojakson suorittamisen jälkeen opiskelija:

- osaa selittää, miten Internet toimii
- osaa kertoa, miten Internetin nimipalvelu toimii
- osaa käyttää TOR-selainta työtehtäviensä suorittamiseen
- osaa kuvailla, miten virtuaalivaluuttoja käytetään ja takavarikoidaan.

#### **Asiakokonaisuudet**

- Internetin toiminta
- Darkweb ja pimeän verkon palvelut (Tor-verkko)
- Virtuaalivaluutat

#### **Vaadittavat suoritukset**

Luennoille osallistuminen ja harjoitusten hyväksytyt suorittaminen.

### **Arviointiasteikko**

Opintojakso arvioidaan asteikolla hyväksytyt/hylätty.

### **Edeltävät opinnot**

Suosittelvat: Kyberrikostorjunnan perusteet (Core Concepts in Digital Investigations and Forensics).

## 12.2 Forensiikkaohjelmoinnin perusteet (3 op)

### Kuvaus

Opintojakson tavoitteena on antaa valmiudet laatia yksinkertaisia ohjelmia, joilla voidaan automatisoida digitaaliforensiikan prosesseja ja helpottaa tiedon keräämistä avoimista tietolähteistä.

### Osaamistavoitteet

Opintojakson suorittamisen jälkeen opiskelija:

- osaa selittää keskeisimmät ohjelmistotekniikan käsitteet
- osaa laatia pieniä ohjelmia Python-ohjelmointikielellä
- osaa käyttää SQLite-tietokannanhallintajärjestelmän perustoimintoja.

Asiakokonaisuudet:

- Ohjelmointikielten keskeiset käsitteet ja ohjelmistotekninen ongelmanratkaisu
- Python-ohjelmointikielen perusteet
- Perustietotyypit
- Vuon ohjaus
- Ohjelman haarautuminen ja iteraatio
- Ohjelmakoodin uudelleenkäyttö
- Syötteen tarkistus
- Tiedostonkäsittely (file input/output)
- SQLite-tietokantojen perusteet
- Datan taltiointi avoimista verkkolähteistä

### Vaadittavat suoritukset

Luennoille osallistuminen ja harjoitusten hyväksytyt suorittaminen.

### Arviointiasteikko

Opintojakso arvioidaan asteikolla hyväksytyt/hylätty.

### Edeltävät opinnot

Suosittelvat: Kyberrikostorjunnan perusteet (Core Concepts in Digital Investigations and Forensics), Linux tutkintatyökaluna.

## 12.3 Haittaohjelma-analyysin perusteet (3 op)

### Kuvaus

Opintojaksolla tutustutaan haittaohjelmien analyysiprosessiin ja -tekniikoihin. Opintojakson tarkoituksena on antaa opiskelijoille valmiudet tunnistaa ja löytää haittaohjelmia sekä analysoida niiden toimintaa.

## **Osaamistavoitteet**

Opintojakson suorittamisen jälkeen opiskelija:

- osaa kuvata keskeisen haittaohjelmiin liittyvän käsitteistön
- osaa etsiä mahdollisesti haitallisia ohjelmia tutkittavalta laitteelta
- osaa käsitellä turvallisesti haitallisiksi oletettuja tai todettuja ohjelmia
- osaa hyödyntää opintojaksolla käytettyjä työkaluja haittaohjelmien toiminnan analysoimisessa.

## **Asiakokonaisuudet**

- Haittaohjelma-analyysiin liittyvä peruskäsitteistö
- Haitallisen ohjelmakoodin etsiminen, tunnistaminen ja taltioiminen
- Haittaohjelman käsittely turvallisessa ympäristössä
- Perusmuotoinen staattinen ja dynaaminen analyysi

## **Vaadittavat suoritukset**

Luennoille osallistuminen ja harjoitusten hyväksytyt suorittaminen.

## **Arviointiasteikko**

Opintojakso arvioidaan asteikolla hyväksyty/hylätty.

## **Edeltävät opinnot**

Suosittelvat: Kyberrikostorjunnan perusteet (Core Concepts in Digital Investigations and Forensics), Windows forensiikka, Forensiikkaohjelmoinnin perusteet.

## **12.4 Internet rikostorjunnassa (1,5 op)**

### **Kuvaus**

Opintojaksolla perehdytään Internetin rakenteeseen ja käyttömahdollisuuksiin sekä sitä koskevaan/käsittelyyn lainsäädäntöön.

### **Osaamistavoitteet**

Opintojakson suorittamisen jälkeen opiskelija:

- osaa käyttää ja soveltaa oppimaansa päivittäisessä rikostutkintatyössä
- osaa kuvata Internetin rakenteen sekä eri käyttömahdollisuudet
- hallitsee Internetin eri tiedonhankintamahdollisuudet ja tuntee Internet-tarkkailuun liittyvän lainsäädännön
- osaa hakea ja käyttää tietoverkoista löytyvää rikokseen liittyvää todistusaineistoa.

### **Asiakokonaisuudet:**

- Anonyymikoneet
- WWW
- Tiedonhankinta ja laki

- Sähköposti
- Internetin avoimet lähteet
- Sosiaalinen media

### **Vaadittavat suoritukset**

Luennoille osallistuminen ja harjoitusten hyväksytyt suorittaminen.

### **Arviointiasteikko**

Opintojakso arvioidaan asteikolla hyväksytyt/hylätty.

### **Edeltävät opinnot**

Suosittelut: Kyberrikostorjunnan perusteet (Core Concepts in Digital Investigations and Forensics).

## 12.5 Internet rikostorjunnassa jatkokurssi (1,5 op)

### **Kuvaus**

Opintojaksolla syvennyttään avointen lähteiden tiedusteluun ja siihen liittyviin prosesseihin. Opintojakso on suunnattu edistyneille opiskelijoille, jotka haluavat tutustua syvemmin avointen lähteiden tiedusteluun ja menetelmiin.

### **Osaamistavoitteet**

Opintojakson suorittamisen jälkeen opiskelija:

- osaa soveltaa oppimaansa päivittäisessä rikostutkintatyössä
- osaa käyttää viranomaisverkkojen ulkopuolista tietokonetta avointen lähteiden tiedusteluun turvallisesti
- tuntee avointen lähteiden tiedusteluun liittyvän prosessin
- hallitsee erilaisten sovellusten käyttämisen avointen lähteiden tiedusteluun liittyen
- tunnistaa virtuaalivaluuttoihin ja Tor-verkkoon liittyvät riskit ja mahdollisuudet.

### **Asiakokonaisuudet**

- Tor
- Linux
- Virtuaalivaluutat
- OSINT-prosessi
- Virtuaalikoneet

### **Vaadittavat suoritukset**

Luennoille osallistuminen ja harjoitusten hyväksytyt suorittaminen.

### **Arviointiasteikko**

Opintojakso arvioidaan asteikolla hyväksytyt/hylätty.



## **Edeltävät opinnot**

Pakolliset: Internet rikostorjunnassa.

Suosittelvat: Kyberrikostorjunnan perusteet (Core Concepts in Digital Investigations and Forensics).

## 12.6 Laiteläheinen digitaaliforensiikka (2 op)

### **Kuvaus**

Opintojaksolla perehdytään sulautettujen järjestelmien, erityisesti ns. IoT-laitteiden sisältämän datan jäljentämiseen ja analysointiin. Opintojaksolla perehdytään myös IoT-laitteissa esiintyviin haittaohjelmiin sekä niiden konfiguraatioiden analysointiin.

### **Osaamistavoitteet**

Opintojakson suorittamisen jälkeen opiskelija:

- osaa jäljentää tavallisimpia IoT-laitteita
- osaa analysoida IoT-laitteen toimintaa ja rajapintoja
- osaa etsiä haittaohjelmia sekä tunnistaa haitallisia konfiguraatioita IoT-ympäristöissä

### **Asiakokonaisuudet**

- Sulautettujen järjestelmien perusteet
- IoT-teknologiat
- IoT-laitteiden tutkintamenetelmät ja -työkalut
- Datan taltioiminen sulautetuista järjestelmistä
- Sulautettujen järjestelmien datan analysointi
- Haittaohjelmat IoT-ympäristöissä

### **Vaadittavat suoritukset**

Luennoille osallistuminen ja harjoitusten hyväksytyt suorittaminen.

### **Arviointiasteikko**

Opintojakso arvioidaan asteikolla hyväksytyt/hylätty.

## **Edeltävät opinnot**

Suosittelvat: Kyberrikostorjunnan perusteet (Core Concepts in Digital Investigations and Forensics).

## 12.7 Linux tutkintatyökaluna (3 op)

### **Kuvaus**

Opintojaksolla perehdytään uusiin menetelmiin ja tekniikoihin, joissa käytetään avoimeen lähdekoodiin perustuvia tutkintaympäristöä ja -työkaluja. Opintojaksolla tutustutaan automatisoituun

rikostutkintaan ja nykyisten ohjelmien todennettavuuteen. Opiskelijat oppivat avoimen lähdekoodin arvon ja kehittävät taitojaan luoda mahdollisesti uusia työkaluja esimerkiksi tietojen palauttamiseen ja mukauttamaan olemassa olevia työkaluja uusilla skripteillä.

### **Osaamistavoitteet**

Opintojakson suorittamisen jälkeen opiskelija:

- osaa suorittaa digitaalisen rikostutkinnan tehtäviä entistä tarkemmin ja varmemmin
- ymmärtää avoimen lähdekoodin työkalujen merkityksen tutkinnassa
- osaa käyttää uusia menetelmiä ja tekniikoita tutkinnassa
- osaa automatisoida rikosteknistä tutkintaa
- osaa mukauttaa ja kehittää olemassa olevia työkalua uusiin haasteisiin.

### **Asiakokonaisuudet:**

- Avoimen lähdekoodin sovellukset
- Automatisointi
- Linux
- Ohjelmointi

### **Vaadittavat suoritukset**

Luennoille osallistuminen ja harjoitusten hyväksytyt suorittaminen.

### **Arviointiasteikko**

Opintojakso arvioidaan asteikolla hyväksytyt/hylätty.

### **Edeltävät opinnot**

Suosittelvat: Kyberrikostorjunnan perusteet (Core Concepts in Digital Investigations and Forensics).

## **12.8 MacOS-forensiikka (4 op)**

### **Kuvaus**

Opintojaksolla perehdytään MacOS-käyttöjärjestelmän tapoihin käsitellä ja varastoida tietoa, sekä miten etsiä, tulkita ja hyödyntää näitä tietoja kyberrikostorjunnassa.

### **Osaamistavoitteet**

Opintojakson suorittamisen jälkeen opiskelija:

- osaa suorittaa digitaalisen rikostutkinnan tehtäviä entistä tarkemmin ja varmemmin
- löytää tärkeimmät MacOS-ympäristöstä löytyvät tiedonlähteet
- osaa käyttää koulutuksessa opittuja menetelmiä ja tekniikoita käytännön työssä
- osaa toimia forensiikan perusteiden mukaisesti MacOS-ympäristössä.

### **Asiakokonaisuudet**

- MacOS-käyttöjärjestelmä
- JSON-tietomuodot
- APFS- ja HFS-tiedostojärjestelmät
- Apple-ekosysteemi
- T2-siru ja -salauk

### **Vaadittavat suoritukset**

Luennoille osallistuminen ja harjoitusten hyväksyty suorittaminen.

### **Arviointiasteikko**

Opintojakso arvioidaan asteikolla hyväksyty/hylätty.

### **Edeltävät opinnot**

Suosittelvat: Kyberrikostorjunnan perusteet (Core Concepts in Digital Investigations and Forensics).

## 12.9 Mobiiliforensiikan perusteet (3 op)

### **Kuvaus**

Opintojaksolla perehdytään mobiililaitteisiin, niihin liittyviin tietoverkkoihin ja mobiililaiteforensiikan perusteisiin.

### **Osaamistavoitteet**

Opintojakson suorittamisen jälkeen opiskelija:

- tunnistaa rikostutkinnan kannalta tärkeät mobiililaitteet
- osaa käyttää oikeita toimintamalleja digitaalisen todistusaineiston käsittelyssä
- osaa soveltaa mobiililaitteen jäljentämisen perusteita
- tuntee yleisimpien forensiikkatyökalujen perusteet

### **Asiakokonaisuudet**

- Laite-etsintään ja takavarikkoon liittyvä lainsäädäntö
- Laitteiden haltuunotto ja käsittely
- Mobiililaitteet
- Televerkkojen perusteet
- Mobiililaiteforensiikan perusteet

### **Vaadittavat suoritukset**

Ennakkotehtävän hyväksyty suorittaminen ennen lähiopintoja sekä luentoihin osallistuminen ja harjoitusten hyväksyty suorittaminen.

### **Arviointiasteikko**

Opintojakso arvioidaan asteikolla hyväksyty/hylätty.

## **Edeltävät opinnot**

Suosittelvat: Kyberrikostorjunnan perusteet (Core Concepts in Digital Investigations and Forensics).

## 12.10 Mobiiliforensiikan jatkokurssi (4 op)

### **Kuvaus**

Opintojaksolla syvennetään mobiiliforensiikan perusteet -opintojaksolla käsiteltäviä asioita. Opintojaksolla keskitytään erityisesti mobiililaiteforensiikkaan sekä datan analysointiin.

### **Osaamistavoitteet**

Opintojakson suorittamisen jälkeen opiskelija:

- osaa käyttää oikeita toimintamalleja digitaalisen todistusaineiston käsittelyssä
- osaa suorittaa mobiililaitteen jäljentämisen
- osaa käyttää yleisimpiä forensiikkatyökaluja itsenäisesti
- osaa soveltaa oppimaansa päivittäisessä rikostutkintatyössä.

### **Asiakokonaisuudet**

- Mobiililaitteet
- Mobiililaiteforensiikka
- Vaihtoehtoiset menetelmät
- Data-analyysi
- Raportointi / lausunto

### **Vaadittavat suoritukset**

Ennakkotehtävän hyväksytyt suorittaminen, luennoille osallistuminen sekä harjoitusten hyväksytyt suorittaminen.

### **Arviointiasteikko**

Opintojakso arvioidaan asteikolla hyväksytyt/hylätty.

## **Edeltävät opinnot**

Pakolliset: Mobiiliforensiikan perusteet.

Suosittelvat: Kyberrikostorjunnan perusteet (Core Concepts in Digital Investigations and Forensics).

## 12.11 Muisti- ja liveforensiikka (3 op)

### **Kuvaus**

Opintojaksolla tutustutaan liveforensiikan sekä muistianalyysin menetelmiin. Opintojaksolla keskitytään erityisesti työasemaympäristöissä (Windows, Mac, Linux) tapahtuvan liveforensiikan peruskäsitteisiin ja tutkintamenetelmiin.

### **Osaamistavoitteet**

Opintojakson suorittamisen jälkeen opiskelija:

- osaa valmistella livetutkinnassa käytettävät työkalut suoritettavaa tutkimusta varten
- osaa valita tapauskohtaisesti soveltuvimmat tutkintatyökalut
- osaa suorittaa perusmuotoisen liveforensisen tutkinnan
- osaa laatia datataltion liveympäristössä ml. keskusmuistitaltion laatiminen
- osaa analysoida keskusmuistitaltiota
- osaa dokumentoida suoritettujen tutkintatoimenpiteiden
- osaa arvioida tutkintatoimenpiteiden aiheuttamia muutoksia kohteympäristössä.

### **Asiakokonaisuudet**

- Live- ja muistiforensiikan perustyökalut
- Datan taltiointi käynnissä olevasta laitteesta ja etäympäristöistä
- Keskusmuistitaltion laatiminen
- Muistianalyysin perusmenetelmät

### **Vaadittavat suoritukset**

Luennoille osallistuminen ja harjoitusten hyväksytyt suorittaminen.

### **Arviointiasteikko**

Opintojakso arvioidaan asteikolla hyväksytyt/hylätyt.

### **Edeltävät opinnot**

Suosittelut: Kyberrikostorjunnan perusteet (Core Concepts in Digital Investigations and Forensics), Linux tutkintatyökaluna.

## **12.12 Taktisen kyberrikostutkinnan perusteet (2 op)**

### **Kuvaus**

Opintojaksolla perehdytään tavanomaisten kyberrikosten taktiseen tutkintaan käsittelemällä keskeistä kyberrikostorjuntaan liittyvää käsitteistöä ja teknologiaa, lainsäädäntöä, tutkintamenetelmiä ja -taktiikoita, todistelua sekä sidosryhmäyhteistyötä. Aihepiiriä käsitellään osin case-esimerkkien kautta.

### **Osaamistavoitteet**

Opintojakson suorittamisen jälkeen opiskelija:

- tunnistaa kybertoimintaympäristöä hyödyntävien ja siihen kohdistuvien rikosten erot
- osaa kuvata tavanomaisia kyberrikosten tekotapoja sekä tutkintamenetelmiä

- osaa suorittaa taktisen tutkinnan tavanomaisien kyberrikosten osalta
- osaa arvioida tutkittavaan tapaukseen liittyvän digitaalisen näytön merkittävyyden todiste- lussa
- osaa hyödyntää keskeisimpiä kyberrikosten tutkintaan liittyviä tiedonsaanti- ja pakkokeinoja

### **Asiakokonaisuudet**

- Kyberrikollisuuden peruskäsitteet sekä kyberrikosten tutkinnan periaatteet
- Kyberrikosjuridiikan perusteet (kyberrikosten tunnusmerkit, pakkokeinot ja toimivaltuudet)
- KV-instrumenttien hyödyntäminen kyberrikosten tutkinnassa
- Digitaaliforensiikka kyberrikosten tutkinnassa
- Keskeiset kyberrikosten tunnistetiedot, tiedonsaanti, tutkintataktiikat ja todisteiden esittämi- nen
- Kyberrikollisten tekijäprofiili
- Kyberrikostorjunnan keskeiset sidosryhmät ja poliisi - syyttäjä -yhteistyö
- Europolin SIENA- ja EIS-järjestelmät

### **Vaadittavat suoritukset**

Luennoille osallistuminen ja harjoitusten hyväksytyt suorittaminen.

### **Arviointiasteikko**

Opintojakso arvioidaan asteikolla hyväksytyt/hylätty.

### **Edeltävät opinnot**

Suosittelvat: Kyberrikostorjunnan perusteet (Core Concepts in Digital Investigations and Foren- sics).

## **12.13 Taktisen kyberrikostutkinnan jatkokurssi (2 op)**

### **Kuvaus**

Opintojaksolla syvennetään Taktisen kyberrikostutkinnan perusteet -opintojaksolla käsiteltyjä asiakokonaisuuksia käsittelemällä vaativien kyberrikosten taktista tutkintaa, lokianalyysiä, digi- taaliforensiikan tutkintamenetelmiä sekä tiedonhankintaa avoimista lähteistä kyberrikosten tut- kinnan apuna. Aihepiiriä käsitellään osin case-esimerkkien kautta.

### **Osaamistavoitteet**

Opintojakson suorittamisen jälkeen opiskelija:

- osaa suorittaa vaativien kyberrikosten ympäristöön kohdistuvien rikosten taktista tutkintaa
- osaa hyödyntää keskeisimpien sidosryhmien palveluja tutkinnan apuna
- osaa tulkita lokiaineistoja sekä hyödyntää lokianalyysin työkaluja.

### **Asiakokonaisuudet**

- Vaativien kyberrikosten taktinen tutkinta
- Lokianalyysi



- Digitaaliforensiikan tutkintamenetelmiin tutustuminen
- OSINT kyberrikosten tutkinnassa

### **Vaadittavat suoritukset**

Luennoille osallistuminen ja harjoitusten hyväksyty suorittaminen.

### **Arviointiasteikko**

Opintojakso arvioidaan asteikolla hyväksyty/hylätty.

### **Edeltävät opinnot**

Pakolliset: Taktisen kyberrikostutkinnan perusteet.

Suosittelvat: Kyberrikostorjunnan perusteet (Core Concepts in Digital Investigations and Forensics).

## **12.14 Tietoliikenneteknologiat ja -protokollat (2 op)**

### **Kuvaus**

Opintojaksolla käsitellään verkkorikosten tutkinnan kannalta keskeisimpien tietoliikennearkkitehtuurien ja -protokollien sekä niiden keskinäisten yhteyksien perusteet.

### **Osaamistavoitteet**

Opintojakson suorittamisen jälkeen opiskelija:

- tunnistaa TCP/IP-protokollapinon eri protokollat
- hallitsee tietoliikenneverkkojen rakenteet ja arkkitehtuurin
- osaa analysoida IT-verkkojen liikennettä
- osaa käyttää TOR-verkkoa työkaluna ja tutkinnan kohteena.

### **Asiakokonaisuudet:**

- TCP/IP-protokollapinon eri protokollat
- TCP/IP-protokollapinoa hyödyntävien protokollien kouluttaminen
- Nykypäivän IT-verkkojen rakenteiden kouluttaminen
- Eri verkkoprotokollien analysointi
- Verkkoliikenteen analysointiin käytettävien työkalujen hyödyntäminen
- TOR työkaluna ja tutkinnan kohteena

### **Vaadittavat suoritukset**

Luennoille osallistuminen ja harjoitusten hyväksyty suorittaminen.

### **Arviointiasteikko**

Opintojakso arvioidaan asteikolla hyväksyty/hylätty.

### **Edeltävät opinnot**

Suosittelvat: Kyberrikostorjunnan perusteet (Core Concepts in Digital Investigations and Forensics).

## 12.15 Verkkorikostutkinnan peruskurssi (2 op)

### **Kuvaus**

Opintojaksolla perehdytään verkkorikostorjunnan perustyökaluihin ja -menetelmiin sekä yleisimpiin verkkorikollisuuden tekniikoihin. Pääpaino on käytännön harjoituksilla. Lisäksi opintojaksolla käsitellään verkkoprotokollien analyysiä sekä aihepiiriin liittyvää juridiikkaa. Opintojakson harjoitustehtävät suoritetaan ensisijaisesti parityönä. Harjoitusparit pyritään muodostamaan siten, että toinen on taustaltaan tekninen ja toinen taktinen tutkija/tutkinnanjohtaja. Tällä lähestymistavalla pyritään hyödyntämään molempien vahvuuksia ja tarjoamaan ymmärrystä toisen osapuolen näkökulmasta tutkintatyössä.

### **Osaamistavoitteet**

Opintojakson suorittamisen jälkeen opiskelija:

- osaa käyttää yleisimpiä verkkorikostorjunnan ja verkkoliikenteen analyysin työkaluja
- osaa soveltaa opintojaksolla opetettuja menetelmiä verkkorikosten tutkinnassa.

### **Asiakokonaisuudet:**

- Verkkorikostorjunnan keskeinen juridiikka
- Johdatus haittaohjelmiin ja niiden yhteiskäyttöön
- Tietoverkkorikostorjunnan perustyökalut ja -menetelmät

### **Vaadittavat suoritukset**

Luennoille osallistuminen ja harjoitusten hyväksytty suorittaminen.

### **Arviointiasteikko**

Opintojakso arvioidaan asteikolla hyväksytty/hylätty.

### **Edeltävät opinnot**

Suosittelvat: Kyberrikostorjunnan perusteet (Core Concepts in Digital Investigations and Forensics), Tietoliikenneteknologiat ja -protokollat, Taktisen kyberrikostutkinnan perusteet.

## 12.16 Verkkorikostutkinnan jatkokurssi (2 op)

### **Kuvaus**

Opintojakso syventää Verkkorikostutkinnan peruskurssilla käsiteltyjä teemoja. Opintojakson sisällöt koostuvat peruskurssin tapaan sekä teoriaosuuksista että niitä tukevista harjoituksista, jotka keskittyvät erityisesti monimutkaisiin yritysverkkoympäristöihin. Opintojaksolla tutustutaan poliisiin näkökulmasta yritykseen kohdistuneen tietoverkkorikoksen selvittämiseen yhteistoiminnassa asianomistajan edustajien kanssa.

## **Osaamistavoitteet**

Opintojakson suorittamisen jälkeen opiskelija:

- tunnistaa tietoverkkorikosten tutkinnan yhteydessä keskeiset digitaalisen todistusaineiston turvaamiseen liittyvät tekijät
- osaa käyttää opintojaksolla harjoiteltuja haittaohjelma-analyysin ja digitaaliforensiikan työkaluja
- osaa nimetä keskeisimmät yritysten käyttämät tietoturvakontrollit.

## **Asiakokonaisuudet**

- Yritysten tietoturvakontrollit
- Vastetoiminta (incident response)
- Haittaohjelmat ja niiden analyysi
- Digitaaliforensiikka tietoverkkorikosten yhteydessä

## **Vaadittavat suoritukset**

Luennoille osallistuminen ja harjoitusten hyväksyty suorittaminen.

## **Arviointiasteikko**

Opintojakso arvioidaan asteikolla hyväksyty/hylätty.

## **Edeltävät opinnot**

Pakolliset: Verkkorikostutkinnan peruskurssi.

Suosittelavat: Kyberrikostorjunnan perusteet (Core Concepts in Digital Investigations and Forensics).

## **12.17 Windows-forensiikka (4 op)**

### **Kuvaus**

Opintojaksolla perehdytään Windows-käyttöjärjestelmän tapaan käsitellä ja varastoida tietoa sekä miten etsiä, tulkita ja hyödyntää niitä kyberrikostorjunnassa.

### **Osaamistavoitteet**

Opintojakson suorittamisen jälkeen opiskelija:

- osaa suorittaa digitaalisen rikostutkinnan tehtäviä entistä tarkemmin ja varmemmin
- löytää tärkeimmät Windows-ympäristöstä löytyvät tiedonlähteet
- osaa käyttää koulutuksessa opittuja menetelmiä ja tekniikoita käytännön työssä
- osaa toimia digitaaliforensiikan perusteiden mukaisesti Windows-ympäristössä.

### **Asiakokonaisuudet**

- Windows-käyttöjärjestelmät
- Windows-rekisterit

- NTFS ja muut tiedostojärjestelmät
- Office-ohjelmistot
- RAM, pagefile, shadow copy
- Bitlocker ja muu salaus

### **Vaadittavat suoritukset**

Luennoille osallistuminen ja harjoitusten hyväksytyt suorittaminen.

### **Arviointiasteikko**

Opintojakso arvioidaan asteikolla hyväksytyt/hylätty.

### **Edeltävät opinnot**

Suosittelavat: Kyberrikostorjunnan perusteet (Core Concepts in Digital Investigations and Forensics).

## 12.18 NCFI Level 2 -opintojaksot (15 op)

### **Kuvaus**

Norjan Politihøgskolen tarjoaa Kyberrikostorjunnan perusteet (Core Concepts in Digital Investigation and Forensic) -opintojakson suorittaneille 15 opintopisteen laajuisia jatko-opintoja, joita ovat

- Module 2A Advanced Computer Forensics (15 op)
- Module 2B Online Investigation (15 op)
- Module 2C Network Forensics and Cybercrime (15 op)
- Module 2D Mobile Extraction and Artifacts (15 op).

Opintojaksot on mahdollista sisällyttää Kyberrikostorjunnan erikoistumisopinnot vapaasti valittaviin opintoihin.

Opintojaksojen tarkempi kuvaus, osaamistavoitteet, arviointiasteikko sekä pääsyvaatimukset esitellään Norjan [Politihøgskolenin verkkosivuilla](https://www.politihogskolen.no/en/post-graduate/nordic-computer-forensic-investigators) <sup>3</sup>.

---

<sup>3</sup> <https://www.politihogskolen.no/en/post-graduate/nordic-computer-forensic-investigators>