

Viiksi-hoppa



2021/2

Pääkirjoitus

Skodan kuskinpuolen sähköikkuna lakkasi toimimasta, ehkä läpivientien johdot ovat hajonneet.

Lisäjarruvalo pimeni, lamppua (LED) ei voi vaihtaa vaan pitää ostaa koko yksikkö. Alkuperäinen maksaa 100 euroa, tarvikeosa 30 e, harkitsen vielä. Lukot ovat toimineet hyvin pakkasilla. Kylmällä ilmalla dieseliä pitää hehkuttaa, kääntää virta-avain ensimmäiseen pykälään.

Tässä numerossa on artikkeli synkronoinnista sekä tietoturvallisuudesta.

Synkronointi

Tahdistaminen eli synkronointi on aikaan liittyvää koordinoitua (1, 2, 3, 5). Synkronointi koskee prosesseja sekä dataa. Prosessit tarvitsevat synkronointia, kun on useita prosesseja joiden tulee toimia yhteistyössä. Datasynkronointia tarvitaan, jotta datasta on useita kopioita tai ylläpidetään datan eheyttä. Nälkiintyminen (starvation) tarkoittaa että ohjelma/prosessi/säie/olio ei pääse eteenpäin muiden ohjelmien/prosessien/säikeiden vuoksi eli ei koskaan saa omaa vuoroaan vaan joutuu odottamaan ikuisesti. Usein kyse on prosessorilta saatavasta ajoajasta. Kilpatilanne (race condition) voi syntyä, jos kaksi prosessia yrittää päivittää samaa muuttujaa tai tietorakennetta, jolloin tulos riippuu tapahtumien järjestyksestä. Lukkiintuminen (dead lock) tarkoittaa sitä, että kaksi ohjelmaa/prosessia/säiettä odottaa, että toinen tekisi jotain.

Aterioivien filosofien ongelma (dining philosophers problem) on seuraavanlainen: Pyöreän pöydän äärellä istuu 5 filosofia. Filosofi joko ajattelee tai syö (tässä tai tarkoittaa *exclusive or* eli *xor*).

Pöydällä on viisi spagettilautasta ja lautasen vieressä oikealla ja vasemmalla puolella on haarukka. Haarukoita on siis viisi. Haarukat otetaan yksitellen. Liukkaan spagetin syömiseen tarvitaan kaksi haarukkaa. Kun filosofi on saanut kaksi haarukkaa, hän syö ja vapauttaa sen jälkeen molemmat haarukat ja jatkaa ajattelua. Filosofit eivät keskustele keskenään. Jos kaikki filosofit haluaisivat syödä yhtä aikaa, he ottaisivat kukin ensin oikeanpuolisen haarukan ja kukaan ei saisi kahta haarukkaa eikä pääsisi syömään eli syntyisi lukkiintuminen. Jokaisella filosofilla olisi vain yksi haarukka ja jokainen odottaisi toista haarukkaa ikuisesti. Ratkaisu voisi olla, että yhden haarukan saaneen filosofin pitäisi nyt laskea haarukka pöydälle, odottaa satunnainen aika ja ottaa uudestaan kaksi haarukkaa. Jos odotusaika on satunnainen, ainakin joku filosofi saa kaksi haarukkaa ja pääsee syömään, mutta tämä ei takaa, että kaikki filosofit pääsisivät syömään eli nälkiintymistä ei olisi estetty. Nälkiintymiseen johtaa myös se tapaus, että neljä filosofia vaihtelee haarukoita keskenään, jolloin viides filosofi ei saa yhtä haarukkaa enempää. Jos taas kaksi filosofia ei suostuisi laskemaan haarukoitaan pöydälle, tapahtuisi lukkiintuminen. Haarukat voitaisiin numeroida, ja filosofin olisi otettava ensin pienempinumeroinen haarukka, sitten isompinumeroinen. Ei ole väliä missä järjestyksessä filosofi luopuu haarukoista. Tällöin lukkiintumista ei tapahtuisi, mutta ei algoritmi ei olisi kovin käytännöllinen. Yksi ratkaisu olisi arbitraatio eli filosofit pyytäisivät hovimestarilta luvan käyttää haarukkaa ja hovimestari antaisi vuoron syödä vain yhdelle kerallaan. Filosofi saa laskea haarukan pöydälle aina. Jos filosofi ja hänen viereinen filosofi pyytää haarukkaa, kaikkien pitää odottaa vaikka haarukoita olisi muualla vapaina. Hovimestari voisi poistaa yhden filosofin pöydästä, jolloin neljä filosofiaa saisi syödä ja ajatella vapaasti. Mikäli filosofit olisivat ylikohteliaita ja sanoisivat toisilleen: ”Sinä ensin” – ”Ei kun sinä ensin”, kumpikin tarjoaisi vuoroa toisilleen eikä kumpikaan pääsisi syömään (Ping Pong) (4).

Tuottaja-kuluttaja ongelma tarkoittaa seuraavaa: ennen kuin tuottaja on tuottanut, kuluttaja ei voi kuluttaa (5). Mutta kun välivarasto täyttyy, tuottajan on odotettava. Tuottajia ja kuluttajia voi olla useita, jolloin täytyy huolehtia poissulkemisesta.

Lukija-kirjoittaja ongelma on: Kaikki saavat lukea, mutta vain yksi kerrallaan kirjoittaa. Kirjoittajan täytyy saada vuoronsa, muuten kaikki lukevat vanhentunutta tietoa. On siis tärkeää, että kirjoittaja ei nälkiinny.

Lähteet

1. Synchronization, (n.d.) [https://en.wikipedia.org/wiki/Synchronization_\(computer_science\)](https://en.wikipedia.org/wiki/Synchronization_(computer_science))
Luettu 21.7.2020
2. Nälkiintyminen, (n.d.) [https://fi.wikipedia.org/wiki/N%C3%A4lkiintyminen_\(tietotekniikka\)](https://fi.wikipedia.org/wiki/N%C3%A4lkiintyminen_(tietotekniikka))
Luettu 21.7.2020
3. Lukkiintuminen, (n. d.) <https://fi.wikipedia.org/wiki/Lukkiutuminen> Luettu 19.7.2020
4. Marttinen, L., Rinnakkaisohjelmistot, (n.d.) Lukkiintuminen, Ping Pong
<https://www.cs.helsinki.fi/u/marttine/Riok04/Luennot/ch4bw2.pdf> Luettu 21.7.2020

5. Raatikainen, K., Johdatus tietojenkäsittelytieteeseen: Tarinoita tietojenkäsittelytieteen osa-alueilta. Helsinki 2007. Helsingin yliopiston tietojenkäsittelytieteen laitos, luentomoniste D-2007-1. Luettu 20.7.2020 osoitteesta <https://www.cs.helsinki.fi/docs/D-2007-1.pdf>

Kyberturvallisuus

Elämme maailmassa, jossa tietokoneet ja tietoverkot ovat yhä tärkeämmässä asemassa. Tiedon on oltava saatavissa ja sen tulee olla luottamuksellista ja yksityistä ja eheää sekä todennettavissa ja kiistämättömissä. Tavallinen kansalainen haluaa, että hänen terveystietonsa ovat vain niitä tarvitsevien käytössä. Myös verkkokauppa ja verkkopankki tarvitsevat tehokasta salausta. Kansalainen asioi virastojen ja viranomaisten kanssa tietoverkkojen välityksellä. Mielestäni elämä nyky-yhteiskunnassa olisi hankalaa ilman tietokonetta (tai älylaitetta kuten älypuhelinta tai tablettia) kotona. Varsinkin vanhempi väestö ei ole tottunut käyttämään tietokonetta ja matkaa rollaattorin ja taksin avulla pankkiin asioimaan, mikä sinänsä saattaa tuoda myös vaihtelua yksitoikkoiseen elämään. Tavallisen kuluttajan kauppaostoksista kerätään tietoa ja niiden avulla voidaan esimerkiksi profiloida mainoksia: Jos kondomien tai terveyssiteiden osto loppuu, asiakkaalle alkaa lähteä vauvantarvikemainoksia. Tällainen *big data* aiheuttaa ongelmia: kenelle sitä jaetaan ja kuka sitä saa käyttää. Riittääkö jos datasta poistetaan yksilöivät henkilötiedot jollain tasolla? Entä saako kerätä tietoja esimerkiksi yksilön uskonnosta, sukupuolesta, sukupuolisesta suuntauksesta, toiminnasta harrastuskerhossa tai poliittisista mielipiteistä? Maksullisten tv-kanavien käyttöönotto tarvitsee salauksen purkavan kortin ja ohjelmiston.

Hakkereista mustahatut käyttävät tietojärjestelmien turvallisuuspuutteita rikollisiin tai pahoihin tarkoituksiin ja valkohatut ovat hyvä hakkereita, tietoturva-asiantuntijoita, jotka etsivät tietojärjestelmistä aukkoja tehdäkseen järjestelmän turvallisemmaksi (3). Aikaisemmin kaikkia

taitavia tietokoneharrastajia kutsuttiin hakkereiksi (4). Yksi Suomen parhaista nykyfilosofeista, Pekka Himanen, on kirjoittanut hakkerietiikasta (6). Hakkerille ei riitä tekninen osaaminen, vaan tarvitaan myös etiikkaa.

Salaus tarkoittaa viestin koodaamista salattuun muotoon. Kryptologia käsittää sekä kryptografian että kryptoanalyysin (2). Kryptologiassa tarvitaan matematiikkaa, sähkötekniikkaa ja tietojenkäsittelytiedettä. Salauksessa kaksi osapuolta kommunikoivat keskenään siten että kolmas osapuoli ei saa viesteistä selvää, vaikka onnistuisi kaappaamaan ne. Salaus voidaan toteuttaa symmetrisesti tai asymmetrisesti. Symmetrisessä salauksessa molemmilla osapuolilla on samanlainen avain. Ongelmana on se, että avain täytyy toimittaa viestin vastaanottajalle. Jos joku pääsee kopioimaan avaimen kun se matkalla toiselle osapuolelle, avain menettää arvonsa. Asymmetrisessä salauksessa on julkinen ja yksityinen avain. Kerchoffin periaatteen mukaan salaus perustuu avainten salassa pitoon, vihollinen voi tietää salausalgoritmin. Kuka tahansa voi kokeilla salauksen luettavuutta ikään kuin ruuvipenkissä. Murtamaton salaus voitaisiin periaatteessa purkaa vain brute force -menetelmällä, kokeilemalla kaikkia avaimia, mutta käytännössä tämä veisi liikaa aikaa. Jos käytettäisiin satunnaislukuihin perustuvaa kertakäyttöistä avainta, joka on yhtä pitkä kuin viesti, kyseessä olisi salaus, jota ei voida purkaa kryptografisesti. Steganografia tarkoittaa tiedon piilottamista (8). Viesti voidaan piilottaa kuva-, ääni-, video- tai muuhun tiedostoon.

Lohkoketju on hajautettu tietokanta, joka mahdollistaa luottamuksen osapuolten välille (1). Lohkoketju voi olla avoin tai suljettu. Lohkoketjut vaativat paljon laskentakapasiteettia. Eri lohkojen välillä on tiiviste (hash) joka varmistaa sen, että tietoa tai lohkoa ei voi muuttaa.

Lohkoketjuja voidaan käyttää myös rikolliseen toimintaan, esimerkiksi rahanpesuun sekä laittomien kemikaalien tai palvelujen anonyymin kauppaan.

Esineiden internet tuottaa tietoturvaongelmia. Esimerkiksi mustahattu-hakkerit voivat murtautua kodin laitteisiin ja tehdä niistä käsin pahojaan, kuten palvelunestohyökkäyksiä (5). Mietin haluanko todella kommunikoida jääkaappini kanssa etänä.

Ilkka Remeksen kirjoissa (esim. Jäätyvä helvetti (7)) Venäjä aloittaa Suomea vastaan kyberhyökkäyksen. Talviseen aikaan sähkönkatkaisu on tehokas ase. Kaukolämmitys lopettaa toimintansa ja harvalla kaupunkiasujalla on oma takka tai kaivo. Tietoliikenne ja ruuanjakeluketjut lakkaavat toimimasta. Anarkia on vain kolmen saamatta jääneen aterian päässä.

Lähteet:

1. Lohkoketju. Wikipedia. (n.d.) Luettu 4.8.2020 osoitteesta
<https://fi.wikipedia.org/wiki/Lohkoketju>
2. Kryptologia. Wikipedia. (n.d.) Luettu 4.8.2020 osoitteesta
<https://fi.wikipedia.org/wiki/Kryptologia>
3. Black hat. Wikipedia (n.d.) Luettu 4.8.2020 osoitteesta
[https://en.wikipedia.org/wiki/Black_hat_\(computer_security\)](https://en.wikipedia.org/wiki/Black_hat_(computer_security))
4. Hacker. Wikipedia (n.d.) Luettu 4.8.2020 osoitteesta <https://en.wikipedia.org/wiki/Hacker>
5. Internet of things. Wikipedia (n.d.). Luettu 4.8.2020 osoitteesta
https://en.wikipedia.org/wiki/Internet_of_things
6. Himanen, P., Hakkerietiikka ja informaatioajan henki. WSOY 2001
7. Remes, I., Jäätyvä helvetti. WSOY 2017

8. Steganografia. Wikipedia. (n.d.) Luettu 4.8.2020 osoitteesta

<https://fi.wikipedia.org/wiki/Steganografia>

Esson baarissa.

Pena mietti mitä ei pidä koskaan tehdä: Ei pidä käyttää hanskoja, kun kulmahiomakoneella tai muulla pyörivällä koneella työskentelee, ei pidä kuivata pyykkiä saunassa (tai ainakaan kiukaan päällä), ei pidä laskea mitään liedon päälle, ei pidä laskea lompakkoa tai muita tavaroita auton katolle.

Palstaviljelijä Timppa mietti, josko voikukista voisi tehdä kumia ja käyttää sitä auton renkaisiin.

Katajannokalla koirien jalat ovat kipeytyneet talvella. Onko aiheuttaja jokin kemikaali: kaupunki ei myönnä käyttäneensä jäänsulatukseen formiaattia, mutta jokin taloyhtiö saattaa tehdä niin. Formiaatti on muurahaishapon suola ja muurahaishappo on ärsyttävää. Voisiko kyse olla hiekoitushiekan tai murskeen terävät särmät?

Ruokaa ja juomaa

Ravintola Taimi, Koivuhaka. Piti olla suomalais-thaimaalainen buffetti, mutta Nongin mielestä enemmän Vietnam/Kiina. Porsaanleike ja naudan lehtipihvi olivat hyviä. Tuskin menemme toiste, ellei ole kova nälkä





Omenapiirakka mikrossa



Khau pad Ravintola Aroi Dii



Itsetehty hodari



Pekonin käärittyjä nakkeja, nuudeleita ja chilikastiketta



Kanaa ja ananasta currykastikkeessa



Ravintola Hua Thai





Laap, maustainen jauhelihakastike



Itsetehty kinkkuaurajuustopizza. Pohja: kuppi jauhoja, kuppi vettä, loraus öljyä, ripaus suolaa, lusikallinen tai puoli (riippuen lusikasta) leivinjauhetta. Täytteet päälle ja 8 min, 750 W mikrossa.



Ravintola Daytoday, Helsinki



Hodarit Ikeassa



Paistettuja katkarapuja ja nuudeleita



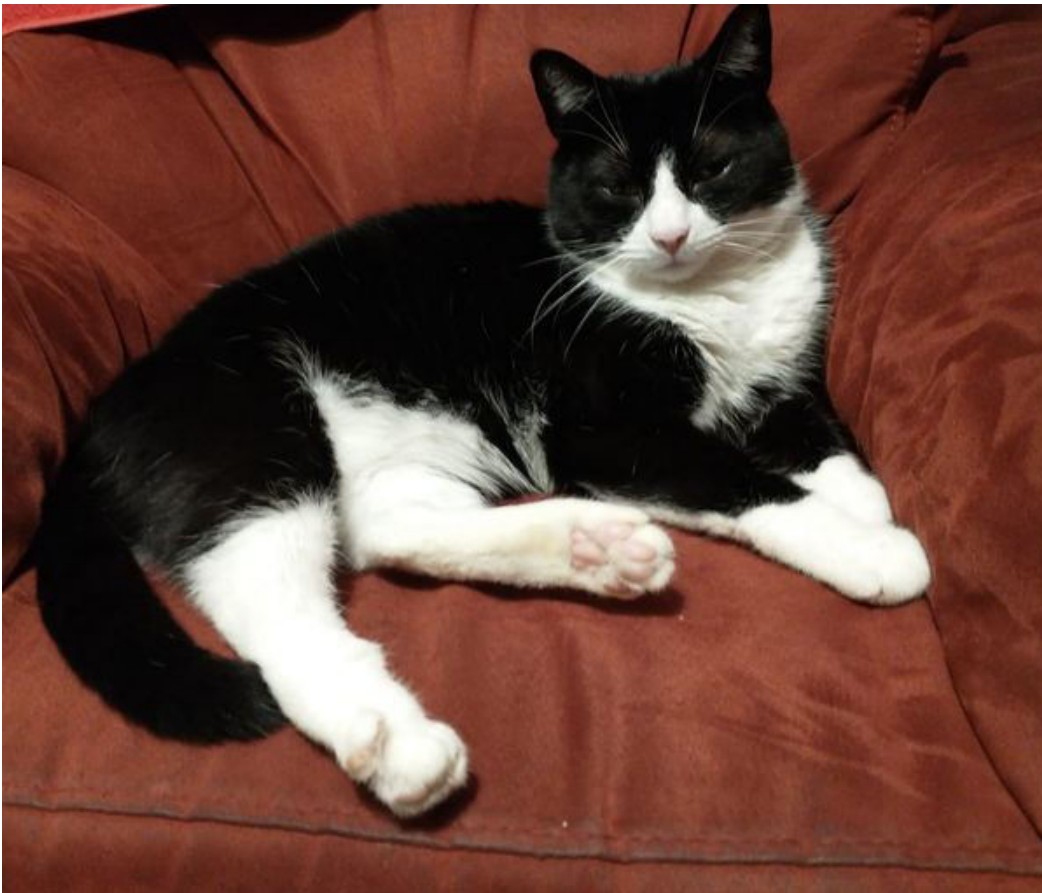
Syntymäpäivillä Malminkartanossa

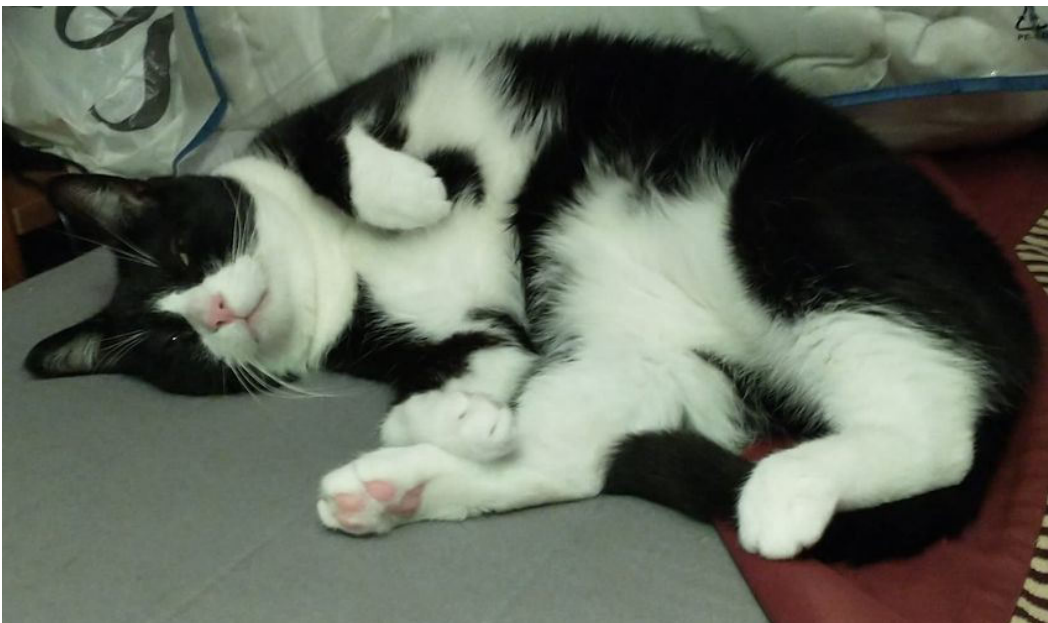




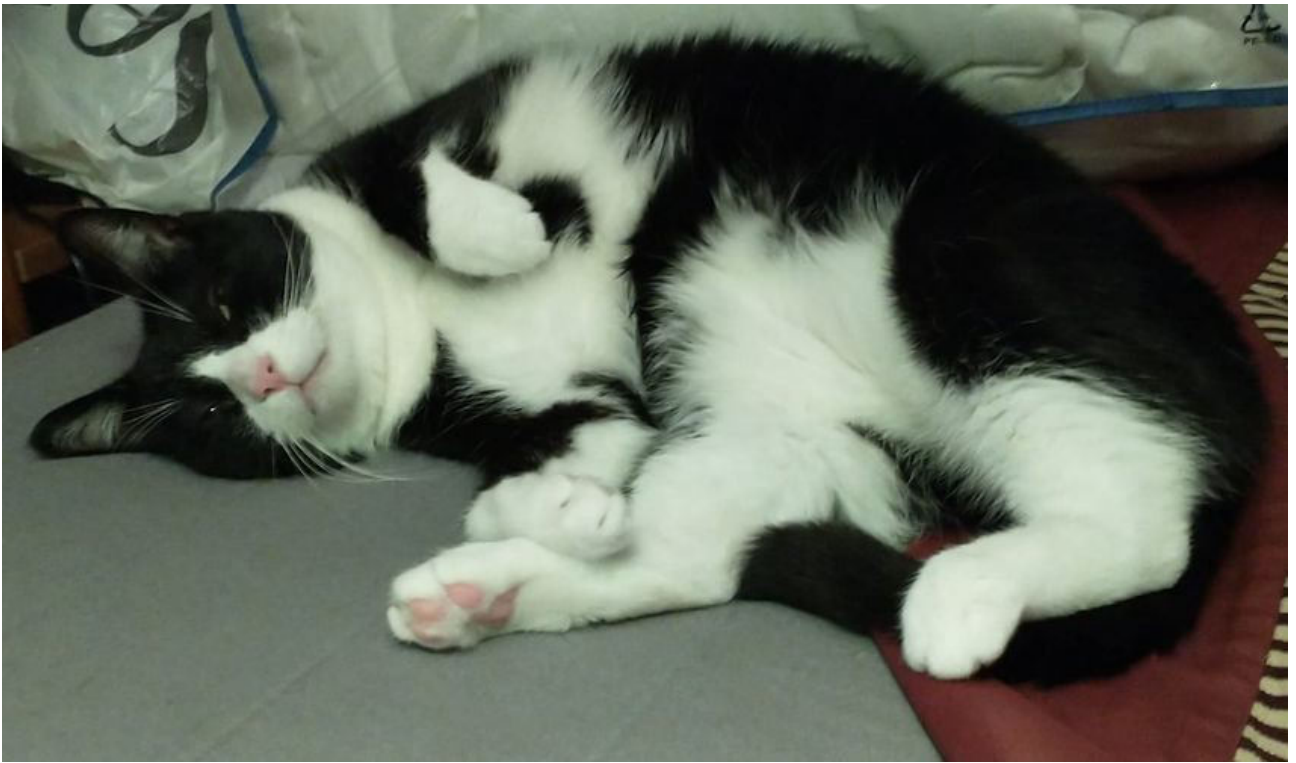
Kissakuvia

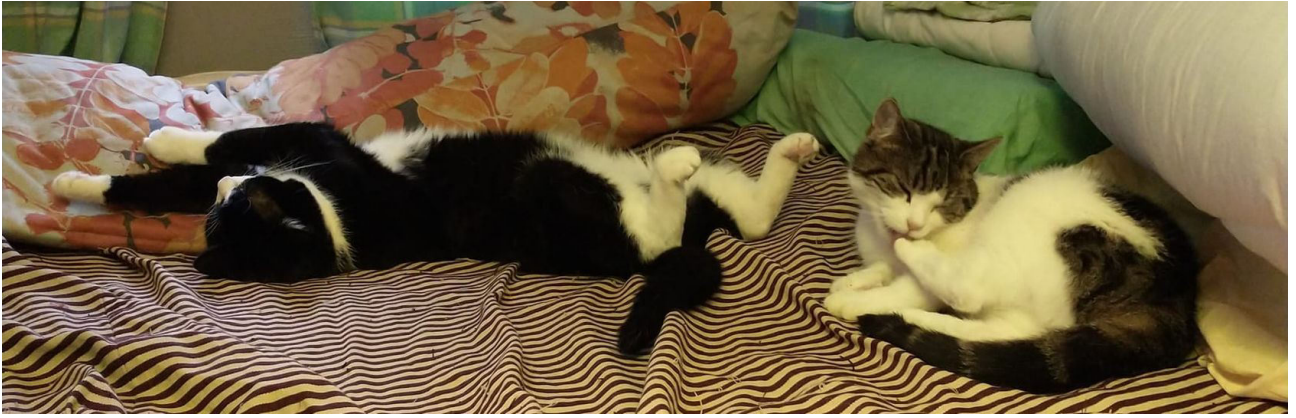












Viiksi-Hoppa apinalaatikko

Päätoimittaja Timo Keränen email timojukkakeranen@gmail.com

Toimittaja Tauno Haudantakanen email tauno.haudantakanen@gmail.com

Viiksi-Hoppa kannattaa Karjalan kannaksen, Laatokan Karjalan, Sallan-Kuusamon alueen, Petsamon ja Suomenlahden ulappasaarien palauttamista oikealle omistajalle.