jamk.fi

Triage-työkalujen kyvykkyyksien vertailu ja todentaminen

Ilmari Åsenbrygg

Opinnäytetyö
Joulukuu 2019
Tekniikan ala
Insinööri (AMK), tieto- ja viestintätekniikka

Jyväskylän ammattikorkeakoulu
JAMK University of Applied Sciences

jamk.fi

Kuvailulehti

Tekijä(t)	Julkaisun laji	Päivämäärä
Åsenbrygg, Ilmari	Opinnäytetyö, AMK	04/2020
	Sivumäärä 50	Julkaisun kieli Suomi
		Verkkojulkaisulupa myönnetty: x

Työn nimi
Triage-työkalujen kyvykkyyksien vertailu ja todentaminen

Tutkinto-ohjelma
Insinööri (AMK), tieto- ja viestintätekniikka

Työn ohjaaja(t)
Puuska, Samir; Lötjönen, Jarno

Toimeksiantaja(t)
JYVSECTEC/ Marko Vatanen

Tiivistelmä

Opinnäytetyö toteutettiin JYVSECTECin toimeksiannosta CYBERDI-projektiin, joka on JYVSECTECin ja POLAMKin yhteistyössä toteutettu projekti. CYBERDI-projektin tavoitteena on kasvattaa käyttäjien osaamista ja tietoutta parantaa digiturvallisuuttaan huijauksia vastaan.

Opinnäytetyön tavoitteeksi muodostui triage-työkalujen kyvykkyys löytää hyökkäysjälkiä Windows 10 -ympäristöstä. Tavoitteen lisäksi opinnäytetyössä tutkittiin kahden eri triage-työkalun eroavaisuuksia ja hyötyjä/haittoja.

Opinnäytetyön kirjallisuuskatsauksessa tutkittiin triage-tutkimusta ja triagea forensiikan osana sekä pyrittiin kertomaan triagen hyödyistä nykypäivän suuren datamäärän vuoksi. Tutkimuskysymyksen (Triage-työkalujen kyvykkyys löytää hyökkäysjälkiä Windows 10- ympäristöstä) vuoksi kirjallisuuskatsauksessa tutkittiin lisäksi Windows-ympäristön tärkeitä ”artifakteja” mm. Powershell, Scheduled task ja pohdittiin nykyajan kyberuhkia.

Opinnäytetyön teknisessa toteutuksessa luotiin Windows 10 -virtuaalikoneesen ”jälkiä” tärkeiden artifaktien ympärille. Jäljet pyrkivät kuvaamaan todellisen hyökkäyksen tapaisia jälkiä. Teknisen toteutuksen triage-työkaluiksi valikoitui KAPE- Kroll Artifact Parser and Extractor ja DFIRTriage. Työkalut valittiin työkalujen erilaisten käyttöliittymien ja toiminnallisuuksien vuoksi.

Opinnäytetyön lopputuloksena syntyi sekä kirjallinen katsaus forensiikkaan, triageen, nykypäivän uhkakuviin ja tärkeisiin Windows 10 -ympäristön kohteisiin, että tekninen toteutus vastaten opinnäytetyön tutkimuskysymykseen.

Avainsanat (asiasanat)
Triage, Forensiikka, Triage-työkalu, KAPE, DFIRTriage,

Muut tiedot (Salassa pidettävät liitteet)
.

jamk.fi

Description

Author(s)	Type of publication	Date
Åsenbrygg Ilmari	Bachelor's thesis	04/2020
		Language of publication: Finnish
	Number of pages: 50	Permission for web publication: x

Title of publication
Comparison and testing of Triage tools.

Degree programme
Information and Communication Technology, Bachelor's degree in Engineering

Supervisor(s)
Puuska, Samir; Lötjönen, Jarno

Assigned by
JYVSECTEC/ Marko Vatanen

Abstract

The thesis was assigned by JYVSECTEC for CYBERDI project of JYVSECTEC and Police University College (POLAMK). The objective for the CYBERDI project is to increase the users' awareness of digital threats in the modern world.

The objective of the thesis was to find the marks created in Windows 10 environment with different triage tools. In addition to the main objective, the thesis examined the advantages and disadvantages of two different triage tools.

The focus of the literature review is on triage and its part in forensic investigation. Additionally, the literature review examines the key artifacts in Windows 10 environment and the modern threats against systems.

The technical part of the study created "marks" to Windows 10 virtual machine. The purpose of these "marks" was to describe real attacks and the tracks left by them. The triage tools chosen in the technical part were KAPE (Kroll Artifact Parser and Extractor) and DFIRTriage. These tools were selected because of their different user interfaces, outputs and capabilities regarding to usage.

The thesis resulted in a full technical review on the capabilities of the two different triage tools regarding the created marks and the literature review on triage as well as triage as a part of forensic investigation.

Keywords/tags (subjects)
Triage, Forensics, Triage tools, KAPE, DFIRTriage

Miscellaneous (Confidential information)

Sisältö

Kuviot

Taulukot

Lyhenteet

API = Application Programming Interface

CFFTTPM = Computer Forensic Field Triage Process Model

DNS = Domain Name System

EXE = Executable file

FAT = File Allocation Table

HTTP = Hypertext transfer protocol

JYVSECTEC = Jyväskylä Security Technology

NTFS = New Technology File System

OpOrd = Operations Order

SQL = Structured Query Language

1 Lähtökohdat

Toimeksianto tuli JYVSECTECiltä ja opinnäytetyö menee JYVSECTECin ja POLAMK yhteistyössä toteutettuun CYBERDI-projektiin.

JYVSECTEC eli Jyväskylä Security Technology on osa Jyväskylän ammattikorkeakoulun IT instituuttia. JYVSECTEC on yksi maan johtavia kybertutkimus, -kehitys ja -koulutus keskuksia. Tavoitteena on nopeuttaa teknistä kehitystä, valmiutta nykyajan uhkia vastaan ja tuoda asiakkaille todellista arvoa. (Specializing in cyber security expertise n.d.)

Nykypäivän rikollisuus on siirtynyt entistä enemmän digitaalisen verkon puolelle, eli puhutaan kyberrikollisuudesta. Tämän vuoksi rikoksia tutkivien yksiköiden täytyy muuntautua ja siirtyä sinne missä rikolliset ovat, josta johtuu myös digitaalisen forensiikan tärkeys tänä ajanjaksona. Triage tuo digitaaliseen forensiikka prosessiin nopeutta ja tehokkuutta. (Cyber crime n.d.)

Opinnäytetyössä pyrittiin selvittämään open source -pohjaisten triage-työkalujen kyvykkyyksiä, käytettävyyttä sekä toimivuutta ennalta rakennettujen jälkien avulla. Työkalujen testauksessa pyritään myös päättelemään voisiko triage-tutkimusta toteuttaa henkilö, joka ei lähtökohtaisesti ole forensiikan ammattilainen. Opinnäytetyön tutkimus kysymykseksi muodostui ”Triage-työkalujen kyvykkyys löytää hyökkäysjälkiä Windows 10- ympäristöstä.”.

2 Forensiikka ja triage forensiikassa

2.1 Forensiikka

Forensiikka sanana juontaa juurensa oikeustieteeseen ja rikostekniikkaan ja on usein liitetty tuomioistuimeen. Aikojen saatossa forensiikka on ollut tärkeä osa rikosten ja

mysteerien ratkomista. Forensiikka on aina pohjautunut tietoon ja faktoihin ja forensiikka tutkimusten perusteella on todettu henkilöitä syyllisiksi ja syyttömiksi. (What is Forensics? n.d.)

Digitaalisella forensiikalla tarkoitetaan tutkimusta, joka kohdistetaan digitaalisiin laitteisiin ja todisteiden keräämiseen näistä laitteista. Näitä todisteita voidaan myös käyttää oikeudessa samoin tavoin kuin muidenkin forensiikan tutkimusten todisteita. Voidaan siis todeta, että digitaalinen forensiikka on forensiikan alataiteenlaji. Digitaalinen forensiikka voidaan jakaa viiteen vaiheeseen (What is Digital Forensics? History, Process, Types, Challenges n.d.):

- Tunnistaminen (identification). Tavoitteena on tunnistaa mitä digitaalisia todisteita on saatavilla, missä formaatissa data on ja mihin se on säilötty.
- Säilöntä (preservation). Ensimmäisen vaiheen löydetyt ”esineet” säilötään, jotta datan oikeellisuus säilyy eikä sitä voida muokata.
- Analysointi (analysis). Kerättyyn dataan suoritetaan analysointia.
- Dokumentointi (documentation). Kaikki rikospaikkaan liittyvä näkyvä data dokumentoidaan esimerkiksi valokuvat, rikospaikan kuvaus ja kuvituskuvat. Tämän pohjalta voidaan suorittaa rikospaikan ”uudelleen rakentaminen” sekä todisteiden esittely.
- Esittely (Presentation). Tässä vaiheessa toteutetaan päätelmät ja lopullinen yhteenveto saatujen tietojen perusteella.

Yksi digitaalisen forensiikan osista on tietokoneisiin tehtävä tutkimus. Sen tavoitteena on palauttaa, analysoida ja tutkia digitaalisten laitteiden sisältämää dataa. Kyseistä dataa voidaan hyödyntää mm. pääsyyllisen henkilöllisyyden selvittämiseen ja motiiviin. (What is Digital Forensics? History, Process, Types, Challenges n.d.)

Finjan Cybersecurity mainitsee blogissaan The Importance of Digital Forensics (2018) myös forensiikan tärkeydestä toiminnan kehittämisen näkökulmasta. Tutkimuksen tavoitteena ei ole ainoastaan selvittää mitä tapahtui ja saada syyllisiä kiinni vaan myös oppia suojautumaan tulevaisuudessa vastaavilta hyökkäyksiltä. (The Importance of Digital Forensics 2018.)

2.1.1 Anti-Forensiikka

Anti-Forensiikka on yksi forensiikkaa toteuttavien henkilöiden suurimpia haasteita. Ohjelmoijat/hackerit ovat kehittäneet ohjelmia, jotka saattavat tehdä forensiikan mahdottomaksi. Seuraavassa listauksessa käsitellään muutamia anti-forensiikan keinoja (How Computer Forensics Works n.d.):

- Otsikkotiedostoa (file header) muuttamalla voidaan mahdollisesti huijata laitetta. Otsikkotiedosto ei muutu pelkällä tiedostopäätteen muutoksella esimerkiksi .jpg -> .mp4.
- Executable tiedoston piilottaminen. Executables tiedostoja voidaan piilottaa toisen tiedosto muodon ”sisään” toisen ohjelman avulla. Näitä ohjelmia kutsutaan ”packers”.
- Tiedostojen kryptaaminen eli encryptaus on tehokas keino salata tiedoston sisältö. Tiedoston sisältö muuttuu tarkoituksettomaksi (esimerkiksi numeroiksi ja kirjaimiksi sekaisin) ja tämän ”palauttamiseen” alkuperäiseen formaattiin vaatii decryptaus avaimen.

Artikkelissaan How Computer Forensics Works (n.d) Jonathan Strickland viittaa myös tietokoneiden luotettavuuteen oikeuden edessä, koska ikinä ei voi tietää varmaksi, milloin tiedosto on luotu, viimeksi avattu tai ikinä edes ollut olemassa. (How Computer Forensics Works n.d.)

2.2 Triage forensiikan osana

Triage liitetään sanana usein lääkärin päivystyksen ensimmäiseen vaiheeseen, jossa tutkitaan potilaiden ”kiireellisyyttä”. Digitaalisessa forensiikassa triage on forensiikka tutkimuksen ensimmäisiä vaiheita, jossa sana liitetään digitaalista dataa sisältävien rikospaikkojen tutkimiseen. Digitaalista forensiikkaa toteutetaan yleensä laboratorioissa. Triage-tutkimusta voidaan suorittaa välittömästi kohteessa tai ns. laboratorio olosuhteissa. (Birvinskas, Gahramanov & Vacius 2017.)

Listattuna kolme hyötyä triagen suorittamisesta (Frawley 2018.):

- Välitön priorisointi. Voidaan heti rikospaikalla priorisoida tärkeää dataa sisältävät kohteet tärkeysjärjestykseen. Tämä ”tärkeysjärjestys” voidaan toteuttaa halutun datan perusteella.
- Ajan säästäminen. Oikein toteutettu triage säästää myöhemmissä tutkimuksissa aikaa, koska karkea arviointi on jo tehty laitteiden osalta.

- Digitaalisen datan (mm. tietokoneiden) kasaantumisen välttäminen digitaalista forensiikkaa suorittavan yksikön ”pöydälle”. Laitteistosta osa saattaa sisältää täysin turhaa dataa.

Suoria eroja syntyy myös kokonaisen forensiikka-imagen ja triage-imagen tiedostojen koossa. Triage tutkimuksissa image, jossa kerätään ainoastaan tärkeiden kohteiden tiedostot, on tyypillisesti vain murto-osan normaalin imagen koosta. Toisinaan myös päätelaite, esimerkiksi tietokone, voi vaatia välitöntä forensiikka/triage tutkimusta johtuen mm. mahdollisista auki olevista ohjelmista, tiedostoista tai chat-keskusteluista. Päätelaite voi olla myös encryptattu, minkä vuoksi on tärkeää ottaa ensimmäinen image tietokoneesta, ennen kuin virrat katkaistaan. (Carrol 2019.)

Triage-tutkimusta on kahdenlaista, triage onsite ja triage offsite. Triage onsite viittaa tutkimukseen rikospaikalla/kohteessa, jossa pyritään tunnistamaan ja tutkimaan tärkeät digitaaliset todisteet mahdollisimman lyhyessä ajassa. Triage offsite taas viittaa tutkimukseen, jossa pyritään poistamaan turhia laitteita forensiikka tutkijoiden käsistä tai priorisoimaan laitteita forensiikka tutkimukseen. (Montasari 2016.)

Reza Montasari (2016) viittaa myös tutkimuksessaan triagen tärkeyteen tilanteissa, joissa ajan säästämisen tärkeys korostuu (esimerkiksi tilanteet, joissa ihmisiä on kateissa). Tällöin ei välttämättä ole aikaa kerätä todisteita, kuljettaa niitä laboratorioon, jossa toteutetaan täydellinen forensiikka tutkimus ja etsitään todisteita/johtolankoja. (Montasari 2016.)

2.2.1 Triagen haasteet

Triagen haasteina on mm. kohteen/laitteen tietojen säilyvyys. Laitteistoon suoritettava välitön triage-tutkimus saattaa muuttaa laitteen tietoja. Esimerkiksi imagen ottaminen laitteesta voi muuttaa muistiosoitteita. Etukäteen on vaikeaa arvioida tutkimuksen vaikutuksia laitteistoon ja sen dataan. Lisäksi laitteiston suojaamiseen on voitu käyttää anti-forensiikka työkaluja. Esimerkkinä mahdolliset rootkitit, jotka voivat aiheuttaa väärän kuvan käyttöjärjestelmästä/laitteesta. Käyttäjien ja digitaalisten

hyökkäyksien määrä on kasvanut hurjasti, jonka vuoksi on tärkeää löytää tehokkaita tapoja ja työkaluja triage-tutkimusten haasteiden taklaamiseen. (Bashir 2013.)

3 Triage kentällä

3.1 Yleistä

Triagea kentällä voidaan todeta olevan kahdenlaista. Ensimmäisessä tavassa kohteessa oleva henkilöstö on hyökkäyksen kohteen alaisia ja laitteisto on saastunutta. Toisessa tavassa kohteessa oleva henkilöstö on vihamielistä ja laitteisto on hyökkäysvälineistöä. Seuraavassa luvussa käsitellään vaihtoehtoa, jossa kohteessa oleva henkilöstö on lähtökohtaisesti vihamielistä.

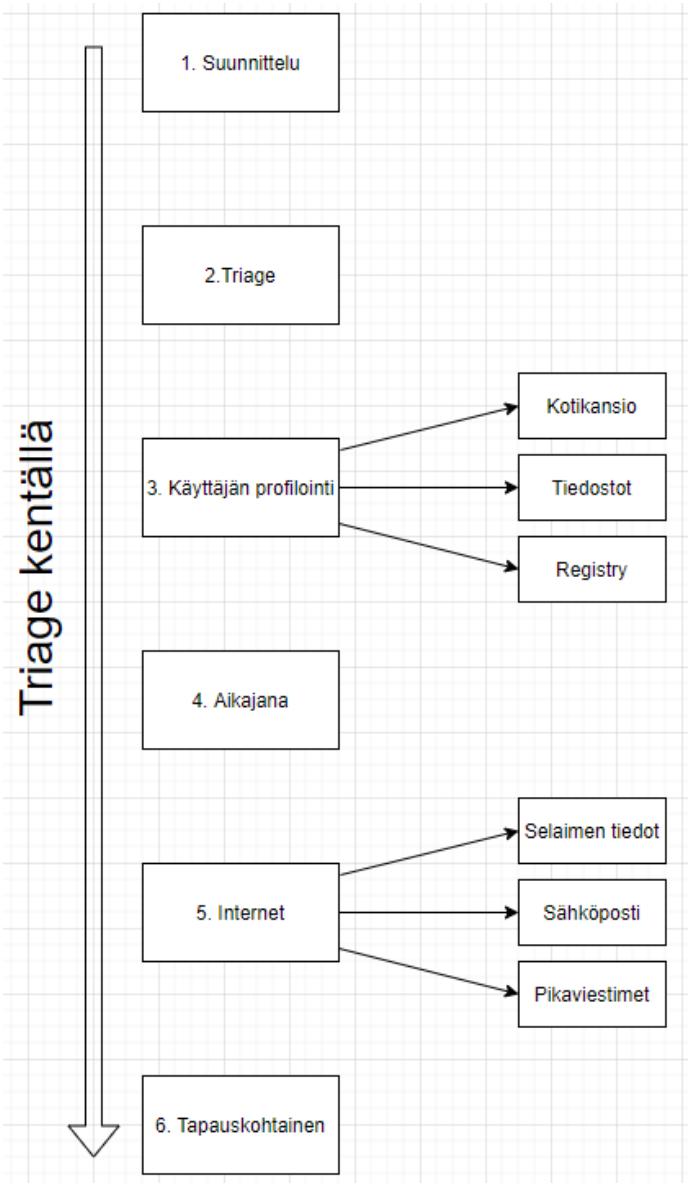
3.2 Triage vihamielisessä kohteessa

Luvussa 3.2 käsitelty prosessi seuraa Marcus K. Rogers, James Goldman, Rick Mislan, Timothy Wedge ja Steve Debrotan kirjoittamaa Computer Forensics Field Triage Process Model (CFFTPM) mallia. (Debrota, Goldman, Mislan, Rogers & Wedge 2006.)

Debrota, Goldman, Mislan, Rogers & Wedge (2006) kirjoittaman Computer Forensics Field Triage Process Model (CFFTPM) mallin mukaan tavoitteena on tapahtuma paikalle saapuessa (Debrota, Goldman, Mislan, Rogers & Wedge 2006.)

- Löytää hyödylliset todisteet
- Tunnistaa riskit
- Ohjata käynnissä olevaa tutkintaa
- Tunnistaa mahdolliset syytteet
- Arvioida vaara, jonka rikollinen tuottaa yhteiskunnalle.

Kuviossa 1 kuvataan prosessin kulku rikospaikalla/kohteessa. Kuviosta löytyvät käsitteet 1-3 käsitellään omina lukuinaan. Lähde on vuodelta 2006, minkä vuoksi kohtia 4-6 ei käsitellä niin tarkasti vaan pureudutaan opinnäytetyön näkökulmasta tärkeisiin artifakteihin luvuissa 3.3-3.3.6.



Kuvio 1. Triage kentällä (Debrota, Goldman, Mislan, Rogers & Wedge 2006.)

3.2.1 Suunnittelu

CFFTPM mallin mukaan ensimmäisenä vaiheena on suunnittelu, jossa johtava tutkija määrittelee tapahtuma paikan, kohteen ja tutkivan tiimin tiedot ja taidot. Tämän avulla voidaan määritellä asiat, jotka tiedetään ja asiat, joita ei tiedetä. Armeijassa käytetään saman tyyppistä lähestymistapaa ”Operations Order (OpOrd)”. OpOrd:ssa kohde/vihollinen luokitellaan SALUTE:n (Strenght, Activity, Location, Uniform, Time ja Equipment) avulla. Samaa lähestymistapaa voidaan hyödyntää rikospaikalle saavuttaessa. (Debrota, Goldman, Mislan, Rogers & Wedge 2006.)

”Strenght” määrittelee kohteiden lukumäärän tai kohteesta tiedossa olevat tiedot/taidot. ”Activity” kertoo kohteen viimeaikaisista tapahtumista/liikkeistä. ”Location” määrittää kohteen fyysisen sijainnin, mutta myös sijainnin tietoverkoissa. ”Uniform” viittaa pitkälti armeijaan, mutta triage-tutkimuksessa sillä viitataan kohteen tietoverkosta löytyviin tietoihin (sähköposti, käyttäjänimet, salasanat jne.). ”Time” taas kuvaa suoraan kronologista aikajanaa, joka on rakennettu aikaisemmin kerätyillä tiedoilla. ”Equipment” kattaa kaikki langalliset ja langattomat laitteet, joita voidaan kuvitella digitaaliseen forensiikka tutkimukseen liittyvän. (Debrota, Goldman, Mislan, Rogers & Wedge 2006.)

Näiden vaiheiden jälkeen tutkimus on pitkälti tiimin taitojen mukaista, jos tieto ja taitoa löytyy kaikkeen tarvittavaan, pystyy tiimi tutkimaan suunnitelman mukaisesti. Toisaalta jos tiimistä puuttuu tarvittavaa tietoa/taitoa kutsutaan paikalle henkilöstöä paikkaamaan puutteita. (Debrota, Goldman, Mislan, Rogers & Wedge 2006.)

3.2.2 Triage

Suunnitellun lähestymistavan jälkeen tutkintatiimi voi jatkaa tutkimusta vaiheisiin, joissa ollaan suoraan yhteydessä kohteisiin (henkilöihin, laitteisiin). Digitaalisen forensiikan näkökulmasta pyritään järjestämään laitteistoa tärkeysjärjestykseen, jonka mukaan laitteistoa tutkitaan tarkemmin myöhemmin. Tämän vuoksi tutkijoiden ja haastattelijoiden täytyy antaa digitaalista forensiikkaa tekevälle henkilöstölle tietoa haastatteluiden ja tutkimusten perusteella, jotta voidaan nopeasti tutkia laitteistoa ja pyrkiä asettamaan sitä tärkeysjärjestykseen jo kentällä. Digitaalista forensiikkaa tekevällä tiimillä täytyy olla mukanaan laitteita, jonka avulla he voivat tutkia kohde laitteistoa, esimerkiksi jokin triage-työkalu. (Debrota, Goldman, Mislan, Rogers & Wedge 2006.)

3.2.3 Käyttäjien profilointi laitteistoon

Tässä vaiheessa pyritään profiloimaan tietyt käyttäjät tiettyihin laitteisiin ja saamaan selville, laitteistoa käyttäneet henkilöt ja milloin laitetta on käytetty. Useissa tapauksissa samaa laitteistoa on voinut käyttää moni eri henkilö, jolloin kyseistä ”todistetta” on vaikeampi kohdistaa tiettyyn henkilöön. Parhaassa tapauksessa saadaan näytettyä

kohteelle hänen olevan ainoa, joka laitteistoon on koskenut ja täten myöntämään syyllisyys. Tämä tietysti vaatii tiimiltä taitoa, jolla laitteistosta löydetään todisteita (artifakteja) mahdollisimman nopeasti. (Debrota, Goldman, Mislan, Rogers & Wedge 2006.)

Artifakteja, hyökkääjien jälkiä ja näiden tutkimista/löytämistä käsitellään lisää luvuissa 3.3-3.3.6.

3.3 Tärkeitä kohteita tutkittavaksi triage-tutkimuksissa

Windows-ympäristössä on monia tärkeitä kohtia tutkittavaksi. Davis (2012) mainitsee kirjoituksessaan Windows sovellusten yhteensopivuus -tietokannan (Windows Application Compatibility database) sisältävän metadataa, josta voidaan palauttaa tiedoston nimi, -koko, viimeinen muokkauspäivä ja mahdollisesti tiedoston suoritus aikoja. Tästä datasta voi olla suurta hyötyä forensiikka-tutkimuksen kannalta, kun pyritään selvittämään mahdollisten haittaohjelmien käyttöä. (Davis 2012.)

Mitre ATT&CK:n sivujen perusteella valittiin Windows-ympäristön kohteita/tapoja (kappaleet 3.3.1-3.3.6), joita hyökkääjä saattaisi mahdollisesti hyödyntää hyökkäyksessään. Mitren navigator-työkalun avulla pystyy näkemään eri ryhmien hyökkäys tapoja. (Mitre ATT&CK n.d.)

3.3.1 Powershell

Powershell on Windows-käyttöjärjestelmistä löytyvä komentolinja pohjainen ympäristö, jota voidaan hyödyntää mm. skriptauksessa. Hyökkääjät voivat käyttää Powershelliä esimerkiksi tiedon hankkimiseen ja koodin suorittamiseen. Powershellillä voidaan myös ladata ja ajaa exe-tiedostoja ilman että kosketaan kovalevyyn. Powershellistä etäyhteyttä muodostaessa toiseen laitteeseen tarvitaan admin-oikeudet. Riittävien oikeuksien (esim admin) kanssa hyökkääjät voivat luoda oman policyn, jonka avulla suorittavat käskyjä. Tutkimalla policyjä voidaan siis havaita mahdollisesti Powershellin haitallista käyttöä. Tietenkin, jos Powershell ei ole aktiivisessa käytössä voidaan tutkia ainoastaan Powershellin käyttöä. (Powershell 2017.)

Sead Fadipasic:n artikkelissa ”Hackers love Microsoft’s Powershell” Ben Johnson kertoo Powershellin olevan todella vahva työkalu, joka tarjoaa hyökkääjille mahdollisuudet suorittaa komentoja kyseisessä laitteessa, mutta myös etäyhteyden avulla. (Fadilpasic 2016.)

3.3.2 Scheduled task

Scheduled tasks on osa Windowsin task scheduleria, jonka avulla voidaan automatisoida ohjelmien ja skriptien ajoa. Oikeanlaisella autentikoitumisella automatisoitu taski voi olla myös kohdennettuna toiseen laitteeseen (Esim. admin-oikeudet toiseen laitteeseen). Hyökkääjät voivat hyödyntää automatisoituja taskeja esimerkiksi koneiden käynnistyksen yhteydessä, sekä mahdollisesti liikkumaan ympäristössä. Hyökkääjä voi käyttää scheduled taskeja kahdella eri tavalla: 1. Ajamalla taskin, jonka jälkee poistaa taskin tai 2. Koittaa säilyttää hallintayhteyttä scheduled taskin avulla. Konfiguroimalla tapahtumien logituksen scheduled taskien osalta, voidaan havaita muutoksia. (Scheduled task 2017.)

3.3.3 Registry run keys

Run keys viittaa ohjelman osiin, joita ajetaan, kun käyttäjä kirjautuu sisään. Nämä ajot tapahtuvat käyttäjätunnuksen toimesta, sekä kyseisen tunnuksen oikeuksien mukaan. Hyökkääjät voivat käyttää näitä hyödykseen mm. säilyttääkseen yhteyden laitteeseen myös boottauksen jälkeen. Rekisterin avaimia (registry keys) voi myös naamioida näyttämään ”rehdeiltä”. Monitoroimalla muutoksia ”run keys” tai käynnistys kansion osalta voidaan havaita mm. päivitysten ulkopuolisia muutoksia tai epäilyttävien ohjelmien/prosessien käynnistymistä käynnistyksen yhteydessä. (Registry run keys 2017.)

3.3.4 Service execution

Hyökkääjät voivat ajaa käskyn, skriptin tai binääriä, jonka avulla pystytään keskustelemaan Windowsin palveluiden kanssa esim. Windowsin palveluiden hallinta työkalun. Epäilystä herättää mm. komentolinjalta suoritetut komennot, joiden avulla on

muokattu olemassa olevia palveluita ja muokkaus ajankohta eroaa esimerkiksi päivitys aikatauluista. (Service Execution 2017.)

3.3.5 Skriptaus

Skriptauksen avulla hyökkääjät voivat ohittaa manuaalista työtä ja nopeuttaa prosessia hallinnan/kohteiden saavuttamisessa. Skriptauksen avulla voidaan myös ohittaa monitorointi työkaluja keskustelemalla suoraan API-tasolla käyttöjärjestelmän kanssa. Powershell on yksi työkaluista, jonka avulla skriptausta voidaan suorittaa. Skriptaus voi olla normaalia esimerkiksi developereilla ja admineilla, mutta normaalin käyttäjän tasolla ei. Epäilyttäviä toimintoja skriptauksen kannalta ovat esimerkiksi yritykset ottaa skriptaus käyttöön normaalin käyttäjän tasolle tai normaalien päivitysajojen ulkopuoliset skriptaukset. (Scripting 2017.)

3.3.6 Rootkit

Rootkitit piilottavat haitalliset ohjelmat muokkaamalla/häiritsemällä käyttöjärjestelmän API-kutsuja. Rootkitit voivat sijaita sekä käyttäjä että kernel-tasolla. Rootkittejä voidaan havaita käyttöjärjestelmän suojauksen avulla tai esimerkiksi erillisellä virustentorjunta ohjelmalla. (Rootkit 2017.)

4 Teoria

4.1 IT-ympäristöt ja laitteet

ISO-standardi perheeseen kuuluu myös ISO/IEC27037:2012 ”Guidelines for indetification, collection, acquisition and preservation of digital evidence”, jossa viitataan digitaaliseen todistusaineistoon. Standardin mukaan todistusaineistoa on (ISO/IEC 27037:2012 2012):

- Digitaalinen tallennustila, jota voidaan käyttää tietokoneissa mm. kovalevyt, levykkeet

- Mobiili puhelimet, muistikortit, kämmentietokoneet sekä kaikki muut henkilökohtaiset elektroniset laitteet kuten mp3-soitin, kannettava tietokone
- Mobiiliset navigointi järjestelmät
- Digitaaliset kamerat
- Tietokoneet verkkoyhteydellä
- TCP/IP pohjaiset tietoverkot ja muut digitaaliset protokollat
- Laitteet saman tyyppisillä toiminnallisuuksilla kuin tässä listassa.

Standardi on luotu ohjeistukseksi digitaalisia todisteiden käsittelyprosesseihin yrityksille ja yksityisille henkilöille. Standardissa todetaan myös, että lista on suuntaa antava (ISO/IEC 27037:2012 2012).

IT-ympäristöt koostuvat seitsemästä komponentista (Infrastructure components n.d.):

- Tietotekniset laitteistot mm. tietokoneet ja serverit.
- Käyttöjärjestelmät, sekä tietokoneiden (yleensä Windows) että servereiden (usein Unix tai Linux pohjaisia).
- Yrityksen käytössä olevat ohjelmistot mm. SAP, Oracle jne.
- Erilaiset tietokannat
- Verkko ja telekommunikaatio alustat
- Palvelimet mm. Verkkosivut, intranetit, extranetit eli Web-palvelimet.
- Legacy-järjestelmät. Yrityksen käytössä olevat vanhat järjestelmät, joiden korvaaminen olisi kallista ja haastavaa.

4.2 Nykypäivän kyberuhkat

Kyberuhkat ovat entistä vaarallisempia nykypäivän kehittyvässä maailmassa. Kyberuhka on teko tai mahdollinen yritys varastaa-, vahingoittaa dataa tai aiheuttaa jonkinlaista digitaalista harmia. Kyberhyökkäys on hyökkäys, joka tapahtuu digitaalisia laitteitamme vastaan virtuaalisessa maailmassa (cyberspace). Vaikka hyökkäykset tapahtuvat virtuaalisessa maailmassa virtuaalisilla aseilla, vaikutukset voivat olla fyysisiä ja jopa ihmishenkiä uhkaavia. (Taylor 2020.)

Kyberhyökkäykset voivat aiheuttaa sähkökatkoja, armeijan laitteiston toimimattomuutta ja kansallisten salaisuuksien vuotamista. Lisäksi hyökkäykset voivat kohdistua henkilötietojen varastamiseen mm. potilastiedot tai lamauttaa puhelin- ja tietokone verkkoja, jolloin vaikutetaan datan ja tietojen saatavuuteen. Taylorin (2020) mukaan ei ole liioiteltua sanoa kyberhyökkäysten vaikuttavan mahdollisesti ihmisten normaaliin arkeen. (Taylor 2020.)

Yleisiä kyberuhkia Taylorin (2020) mukaan (Taylor 2020.):

- Haittaohjelmat (Malware)
- Kalastelu (Phishing and spear phishing)
- Man-in-the-middle
- Palvelunestohyökkäys (Denial-of-service)
- Troijalaiset
- Ransomware
- IoT laitteisiin kohdistuvat hyökkäykset
- Tietomurrot
- Mobiilisovellus haittaohjelmat(malwaret)

Ciscon listaus yleisistä kyberuhkista on hieman suppeampi, mutta sisältää Hugh Taylorin listan kanssa yhteisiä uhkia (What Are the Most Common Cyber Attacks? n.d.):

- Haittaohjelmat
- Phishing
- Man-In-The-Middle
- Palvelunestohyökkäys (Denial-of-service)
- Sql-Injektio
- Zero-day
- DNS Tunnelointi

Voidaankin todeta näiden kahden listauksen jälkeen mm. haittaohjelmien, kalastelun, man-in-the-middle, ja palvelunestohyökkäysten olevan yleisiä hyökkäystapoja.

Kyberuhkia aiheuttavia tahoja on monia erilaisia ihmisiä/tahoja, monista lähtökohdista ja monista maailman eri osista (Taylor 2020.)

- Yksityiset henkilöt, jotka käyttävät omia työkalujaan hyökkäyksissä
- Rikollisorganisaatiot, jotka toimivat yrityksen lailla työntekijöiden voimin
- Valtiot
- Terroristit
- Yritys vakoojat
- Organisoituneet rikollisryhmät
- Sisäiset toimijat, jotka ovat jostain syystä kääntyneet esimerkiksi yritystä vastaan
- Hackerit
- Kilpailijat esimerkiksi kilpaileva yritys

Valtiot ovat usein monien hyökkäysten takana. Valtio tason kyberhyökkäyksiä on monia erilaisia mm. vakoilua, valtio/yritys tietojen varastamista. (Taylor 2020.)

Mielenkiintoa herättää myös valtioiden (esimerkiksi FBI) kyberrikollisten etsintäkuulutus listaukset, joissa henkilöiden toimeksiantaja voi olla toinen valtio. Toisin sanottuna etsintäkuulutus listalle joutunut henkilö voi olla mahdollisesti toisen valtion palkkaama.

4.3 Termit ja käsitteet

Tässä luvussa käsitellään opinnäytetyöhön liittyviä termejä ja käsitteitä, joita käsitellään opinnäytetyön eri vaiheissa. Windows-ympäristöön liittyvät käsitteet on kirjoitettu selityksineen taulukkoon 1. Muut käsitteet löytyvät taulukosta 2.

Taulukko 1. Windows-ympäristöön liittyvät termit ja käsitteet

Windows-ympäristöön liittyvät termit ja käsitteet	
Termi	Selitys
File System	File system on järjestelmän osa, johon tallennetaan tiedoston lisäksi myös muut tiedot mm. tiedoston koko, tiedoston nimi sekä sijainti järjestelmässä. Uusimmat Windows-ympäristöt käyttävät tiedostojen tallennus muotona NTFS (new technology file system), mutta myös vanhempaa FAT (File Allocation Table) tuetaan. (Fisher 2019.)
Registry	Windowsin registry tallentaa tietoa Windowsin ohjelmista (tietoja ja asetuksia), fyysisistä laitteista (mm. muistitikut) ja käyttäjän- sekä käyttöjärjestelmän asetuksista. Registryyn lisätään mm. uusien ohjelmien “ohjeita” ja viittauksia muihin tiedostoihin sekä niiden sijaintiin järjestelmässä. (Fisher 2020.)
Event logs	Tallentaa instrumentation manifestin määrittelemiä logeja Windows-ympäristössä. (Windows Event Log 2018.)
Instrumentation manifest	Instrumentation manifest määrittelee asiat, joita kirjataan Windows event logiin. Sisältää myös toiminnallisuudet, joiden avulla event viewer lukee event logeja. (Windows Event Log 2018.)
Event viewer	Ohjelma, joka hyödyntää instrumentation manifestiä event logien lukemiseen. (Windows Event Log 2018.)
Rekisterieditori	Rekisterieditori on Windowsin graafinen käyttöliittymä, josta voidaan tutkia ja muokata Windowsin rekisteritietoja. (Rouse 2015

Palvelut	Palvelut (Windows Services) on yksi Windows-käyttöjärjestelmän tärkeimmistä komponenteista. Windows Services ei tarvitse käyttäjän toimenpiteitä vaan toimii taustalla. Windows Services käynnistyy bootin yhteydessä. (What are Windows Services? How Windows Services Work, Examples, Tutorials and More 2017.)
PS1 tiedosto (.ps1)	PS1 tiedosto on skripti, jota Windowsin Powershell käyttää. Tiedosto sisältää rivejä, jotka on kirjoitettu Powershellin skriptaus kielellä. (.PS1 File Extension 2010.)
Batch tiedosto (.bat)	Batch tiedosto on esimerkiksi lista komentoja, jotka voidaan ajaa ilman käyttäjän toimenpiteitä. Käytetään Windows-ympäristöissä. (Batch file 2019.)
API	API eli Application Programming interface (Sovellusohjelmointirajapinta) mahdollistaa eri ohjelmien keskustelun keskenään. (API-Mikä on API? n.d.)
Group Policy	Group Policy on Windowsin ominaisuus/ohjelma, joka sisältää laajasti asetuksia liittyen käyttöjärjestelmään. Group policy voi vaikuttaa ainoastaan kyseisessä koneessa tai laajemmalla tasolla esimerkiksi organisaatio. (Hoffman 2016.)
Powershell	Powershell on task-pohjainen komentolinja scriptaus kieli. Powershell auttaa esimerkiksi system administratoreita nopeasti automatisoimaan taskeja ja hallinnoimaa käyttöjärjestelmää. (Powershell 2018.)

Artifact/Artefact	Artifaktit ovat asioita/kohteita, joilla on arvoa forensiikka tutkimuksissa. Esimerkiksi logit, registry hivet. (Windows Forensic Analysis- Windows Artifacts (Part 1) 2019.)
Kernel	Kernel on käyttöjärjestelmän moduuli, joka käynnistyy bootin yhteydessä aina ensimmäiseksi. Kernel tarjoaa pakolliset palvelut käyttöjärjestelmälle. Kernel on kriittisyytensä vuoksi yleensä muistin suojatulla alueella. (Kernel n.d.)
Windows Application Compatibility database	Windowsin Application Compatition -tietokanta sisältää sovellusten yhteensopivuus virheet ja niiden ratkaisut. Jokaisella sovelluksella on tietokannassa omia komponentteja yksi tai useampi. Komponentit ovat executable tiedostoja, joita kuvataan yleensä tiedoston attribuuteilla. (Application Compatibility Database 2018.)

Taulukko 2. Muut termit ja käsitteet

Muut termit ja käsitteet	
Termi	Selitys
Kohde/ Target	Target eli kohde tarkoittaa tietoteknisessä forensiikassa tutkittavaa asiaa.
Input/Output	Input on dataa, jota annetaan prosessoivalle työkalulle. Inputin antamasta datasta työkalu tuottaa outputin. (What is the difference between an input and output device? 2018.)
Automatisointi	Automatisointi on tekniikka, jolla laite, prosessi tai käyttöjärjestelmä saadaan toteuttamaan jokin asia automaattisesti. Esimerkiksi tietokone asetetaan ajamaan backup, joka aamu kello 8.00. (What is automation? N.d.)
Avoin lähdekoodi	Ohjelmia on sekä avoimella- että suljetulla lähdekoodilla. Avoimen lähdekoodin ohjelmien ohjelmointi koodia saa/pääsee kuka vain näkemään ja muokkaamaan. (What is open source? N.d.)
GUI	Graphical user interface, eli graafinen käyttöliittymä. Graafinen käyttöliittymä tuottaa käyttäjälle visuaalisia outputteja ja navigointi tapahtuu kursorin avulla. Sen on todettu olevan käyttäjäystävällisempi, kuin tekstipohjaisen komentolinjan. (GUI 2019.)
Komentolinja	Komentolinja on graafisen käyttöliittymän vastine, mutta komentolinjaan tuotetaan ”komentoja” kursorilla liikkumisen sijaan. (Command line 2019.)

Forensic Image	Forensic image on täydellinen kopio fyysisestä laitteesta/kovalevystä. (Rouse 2017.)
Aikajana/Timeline	Aikajana on kirjaimellisesti jana, jossa näkyy tapahtumia aikaleimoilla. Tämän avulla voidaan päätellä/tutkia esimerkiksi hyökkäyksen etenemistä.
Skripti	Skripti on sarja komentoja yhden tiedoston sisällä. Skripti on tiedosto, joka voidaan suorittaa ilman muuttamista exe-muotoon. (Rouse 2019.)
Haittaohjelma (Malware)	Ohjelma, joka suorittaa haitallista toimintoa kohde laitteessa tai verkossa. Esimerkkinä datan korruptoiminen tai hallinta yhteyden muodostaminen. (Taylor 2020.)
Kalastelu (Phishing and spear phishing)	Kalastelu on henkilöiden huijausta mm. sähköpostin välityksellä verkkolinkin/ohjelman lataamiseen, joka johtaa tietokoneen saastumiseen. Spear phishing on hieman hienostuneempi tapa, jossa hyökkääjä tutkii kohdettaan ja kohdistaa kalastelu viestin suoraan kohteelle sopivaksi. (Taylor 2020.)
Man-in-the-middle	Man in the middle attack on hyökkäys, jossa hyökkääjä pääsee kahden henkilön tai henkilön ja palvelimen väliin ja kykenee muuttamaan viestejä/dataa. Lähettäjä ja vastaanottaja ei tiedä välissä olevasta hyökkääjästä. (Taylor 2020.)
Palvelunestohyökkäys (Denial of service ja Distributed Denial of service)	Palvelunestohyökkäyksessä hyökkääjä pyrkii laitteella tai useilla laitteilla (distributed denial of service) palvelimen/palvelun kaatamalla estämään palvelun saatavuuden. Esimerkkinä kaatamalla web-palvelimen, jolloin web-palvelin ei ole saatavilla. (Taylor 2020.)

Troijalainen	Troijalainen on ohjelma tai ohjelman osa, joka on naamioitu näyttämään normaalilta, mutta todellisuudessa tuo haitallista koodia järjestelmään. (Taylor 2020.)
Ransomware	Ransomware encryptaa järjestelmän ja vaatii maksua järjestelmän encryptauksen purkamista vastaan. (Taylor 2020.)
Tietomurrot	Tietomurrossa varastetaan tietoa mm. salaisuuksia, henkilötietoja tietojärjestelmästä. (Taylor 2020.)
Sql-Injektio	SQL-injektiossa hyökkääjä syöttää haitallista koodia serverille, joka käyttää SQL-tietokantaa. Haitallinen koodi saa serverin näyttämään tietoa, jota normaalisti ei saisi näkyville. (What Are the Most Common Cyber Attacks? N.d.)
DNS Tunnelointi	DNS tunneloinnissa lähetetään DNS-protokollalla esimerkiksi HTTP liikennettä. (What Are the Most Common Cyber Attacks? N.d.)
Zero-day	Zero-day hyökkäykset ovat hyökkäyksiä, joiden estoon ei ole ollut saatavilla päivitystä ennen hyökkäystä. (What Are the Most Common Cyber Attacks? N.d.)
Hacker	Hackeri on henkilö, joka hyödyntää taitojaan ohittaakseen teknisen ongelman. Hackereita on monenlaisia, mutta yleensä sanalla viitataan henkilöön, joka käyttää taitojaan väärin esimerkiksi varastamalla tietoja tietojärjestelmästä kiristykseen. (Hacker n.d.)

4.3.1 RegRipper

Regripper on ilmainen ohjelma, jota käytetään Windows-tuoteperheen registry hiven tutkimiseen. RegRipper tarjoaa graafisen käyttöliittymän ja sen tuottama output on teksti pohjaista ja helposti luettavissa sekä analysoitavissa. RegRipperin logfile sisältää tietoa sen omista toimistaan. (Carvey, H. n.d.)

4.4 Työkalut

4.4.1 KAPE

KAPE (Kroll Artifact Parser and Extractor) on Eric Zimmermanin luoma työkalu, jolla voi kerätä sekä prosessoida tiedostoja. KAPE sisältää valmiiksi todella laajan skaalan erilaisia default kohteita ja moduuleita, joita voi hyödyntää suurimmassa osassa yleisimmistä forensiikka/triage-tutkimuksissa. KAPE antaa myös mahdollisuuden käyttäjälle itselleen luoda omia kohteita ja moduuleita. (Zimmerman, E. 2019.)

Karkealla tasolla KAPE kerää aluksi ”Targetit” eli kohteet omaan jonoonsa. Jono sisältää ”targetin” ja tämän sijainnin normaalissa ympäristössä. Tätä jonoa käytetään sitten kohteessa olevien tiedostojen kopioimiseen. Käyttöjärjestelmän lukitsemista tiedostoista KAPE tekee listan. Tähän lukittujen tiedostojen listaan KAPE käyttää erilaisia tekniikoita ohittaakseen lukituksen. Kerätyn datan KAPE kopio annettuun kohde kansioon. (Zimmerman, E. 2019.)

4.4.2 DFIRTriage

DFIRTriage on pythonilla kirjoitettu työkalu, joka suoritettaessa ajaa kohteessaan useita komentoja. Tätä työkalua voi käyttää USB tikulta tai suorittaa kohteessa etäyhteyden yli. DFIRTriage on käytännössä komentolinja pohjainen työkalu, joka ajettaessa kerää datan kohteesta ja kirjoittaa sen tiedostoon, joka on työkalun ”tuotos”. (DFIRTriage v4.0.0 User's Manual n.d.)

5 Työkalujen kyvykkyyksien testaus

5.1 Ympäristöön luodut jäljet

Opinnäytetyössä otettiin tarkempaan testaukseen kaksi työkalua, jotka valittiin hieman erilaisten käyttötapojen perusteella. Työkalujen kyvykkyyksien testaukset suoritettiin puhtaaseen Windows 10 -käyttöjärjestelmään, johon oli luotu ”jälkiä”. Jäljet pyrkivät mukailemaan luvuissa 3.3-3.3.6 määriteltyjen tärkeiden kohteiden jättämiä jälkiä todellisessa hyökkäystilanteessa. Kyvykkyyksien testauksessa keskityttiin työkalujen käytettävyyteen ja onnistumiseen ennalta luotujen jälkien löytämisessä. Taulukossa kolme käsitellään jäljet karkealla tasolla.

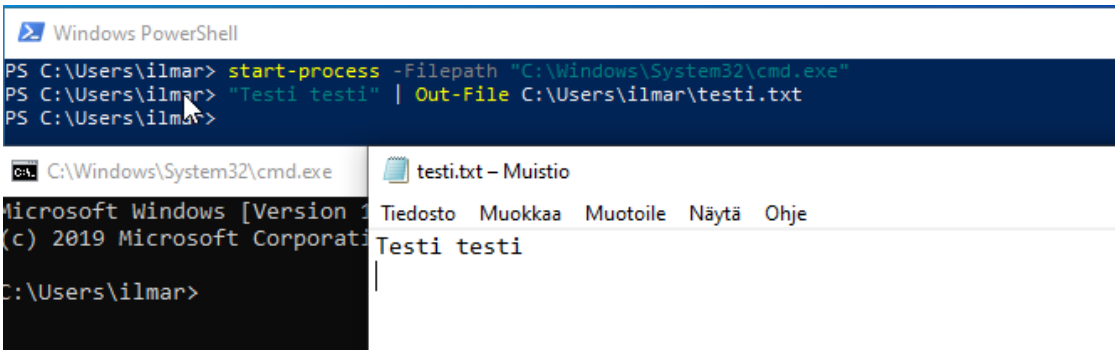
Taulukko 3. Ympäristön jäljet

Jälki	Lyhyt kuvaus
Yksi	Powershell – Prosessin aloitus ja tekstitiedoston muokkaus
Kaksi	Scheduled task – Ohjelma käynnistyy käyttäjän kirjautuessa sisään.
Kolme	Regedit – Rekisterieditoriin sääntö .reg tiedoston avulla.
Neljä	Palvelut – Etäyhteyden muodostaminen laitteeseen aktivoitu.
Viisi	Skripti – Kaksi erilaista skripti tiedostoa eri toiminnallisuuksilla (.bat ja .ps1).

Jäljistä yksikään ei ollut oikeasti haitallinen järjestelmälle. Tarkoituksena oli enemmän luoda tapahtuma, josta huomaa muutoksien tapahtuneen. Jälkien luomisessa pyrittiin käyttämään mahdollisimman montaa eri ohjelmaa ja tiedostomuotoa, jotta työkalujen testaus vaiheessa voitaisiin helpommin todentaa mikä jäljistä oli kyseessä.

5.1.1 Jälki numero 1

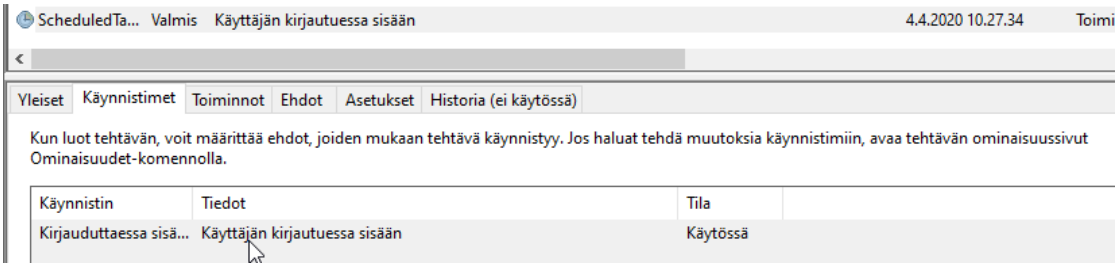
Powershellillä luotiin jälkiä, jotka olivat prosessin/ohjelman käynnistys ja tekstitiedoston luominen/kirjoittaminen tekstitiedostoon (ks. kuvio 2).



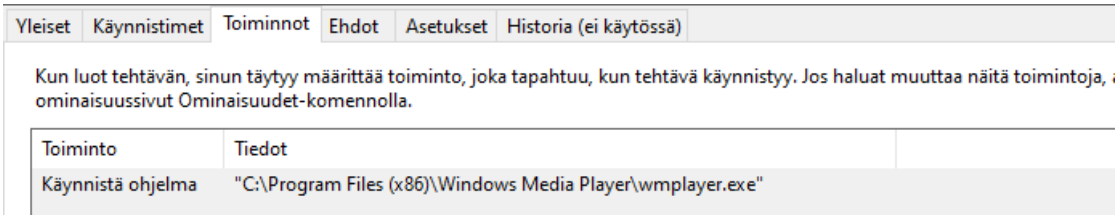
Kuvio 2. Jälki yksi- Powershell

5.1.2 Jälki numero 2

Scheduled task:lla luotiin toiminto, joka ajetaan käyttäjän kirjautuessa sisään (ks. kuvio 3). Toiminto käynnistää Windows Media Playerin (ks. kuvio 4).



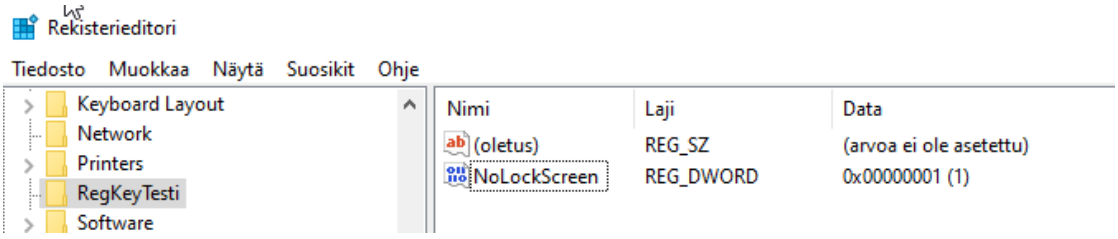
Kuvio 3. Jälki kaksi- Scheduled task käynnistin



Kuvio 4. Jälki kaksi- Scheduled task toiminto

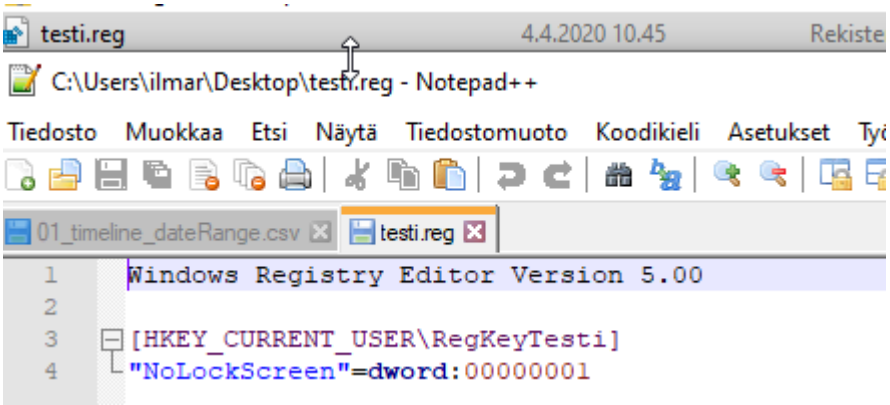
5.1.3 Jälki numero 3

Rekisterieditoriin luotiin avain ”NoLockScreen”, jonka binääri arvoksi asetettiin 00000001 eli näyttöä ei lukita (ks. kuvio 5).



Kuvio 5. Jälki kolme- Rekisterieditori tulos

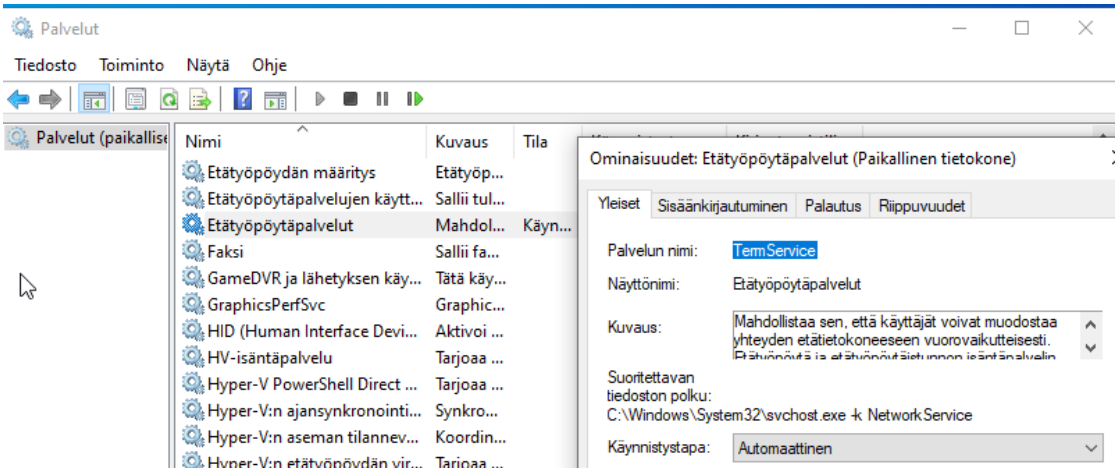
Kyseinen testi “NoLockScreen” luotiin testi.reg tiedoston avulla (ks. kuvio 6).



Kuvio 6. Jälki kolme- testi.reg tiedosto

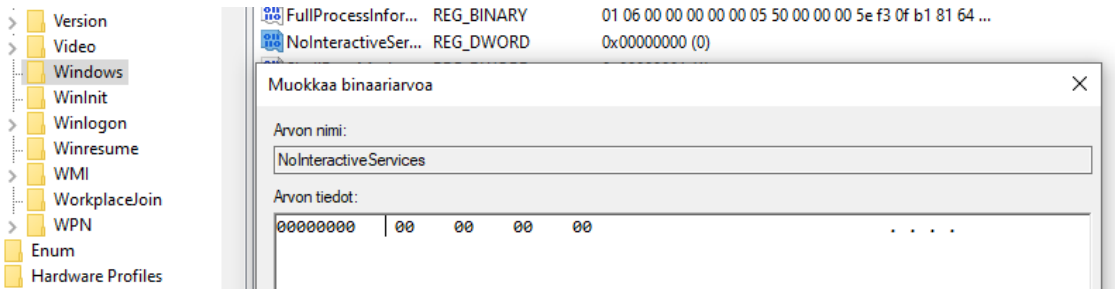
5.1.4 Jälki numero 4

Palveluista hyväksyttiin etäyhteyden muodostaminen laitteeseen (ks. kuvio 7). Kuvitteellisessa hyökkäystilanteessa tämän voisi myös kuvitella olevan aktivoitu hyökkääjien toimesta. Normaalissa tilanteessa asetus on ”pois päältä”.



Kuvio 7. Jälki neljä- Etätyöpöytäpalvelut päälle

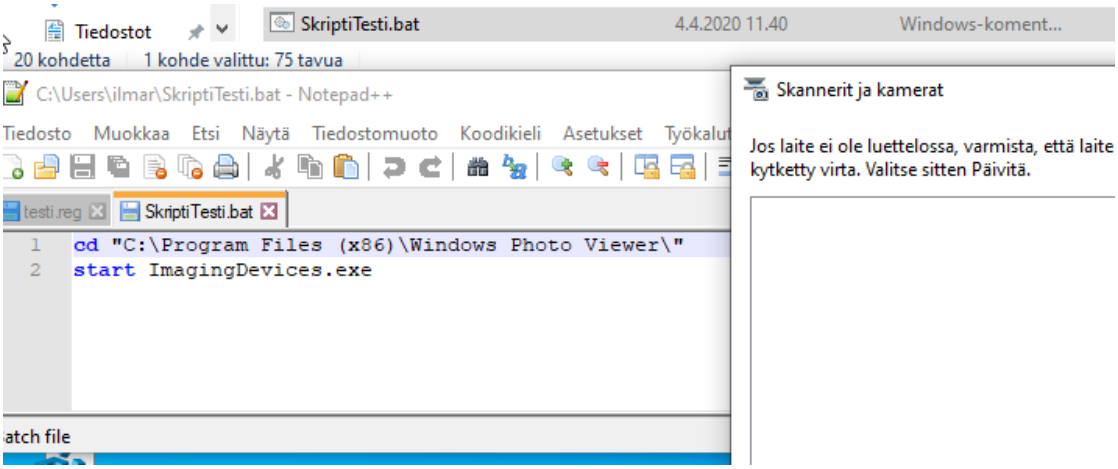
Palveluiden muokkauksen takia muutettiin myös rekisterieditorista löytyvää avainta, joka estää palveluiden ajamisen kyseisessä työasemassa (ks. kuvio 8).



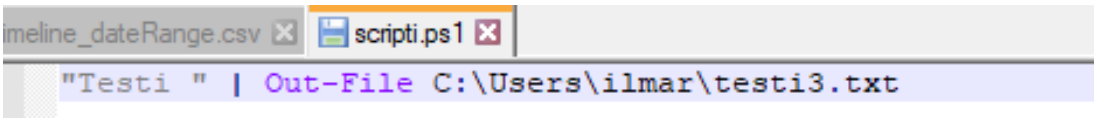
Kuvio 8. Jälki neljä – RegEdit Interactice Services

5.1.5 Jälki numero 5

Luotiin skripti tiedostoja sekä .bat (ks. kuvio 9), että .ps1 tiedostona (ks. kuvio 10), joilla pyrittiin toteuttamaan erilaisia toiminnallisuuksia. Esimerkiksi .bat tiedosto, jolla käynnistettiin skannerit ja kamerat ohjelma.



Kuvio 9. Jälki viisi- .bat skripti tiedosto



Kuvio 10. Jälki viisi- .ps1 skripti tiedosto

5.2 KAPE

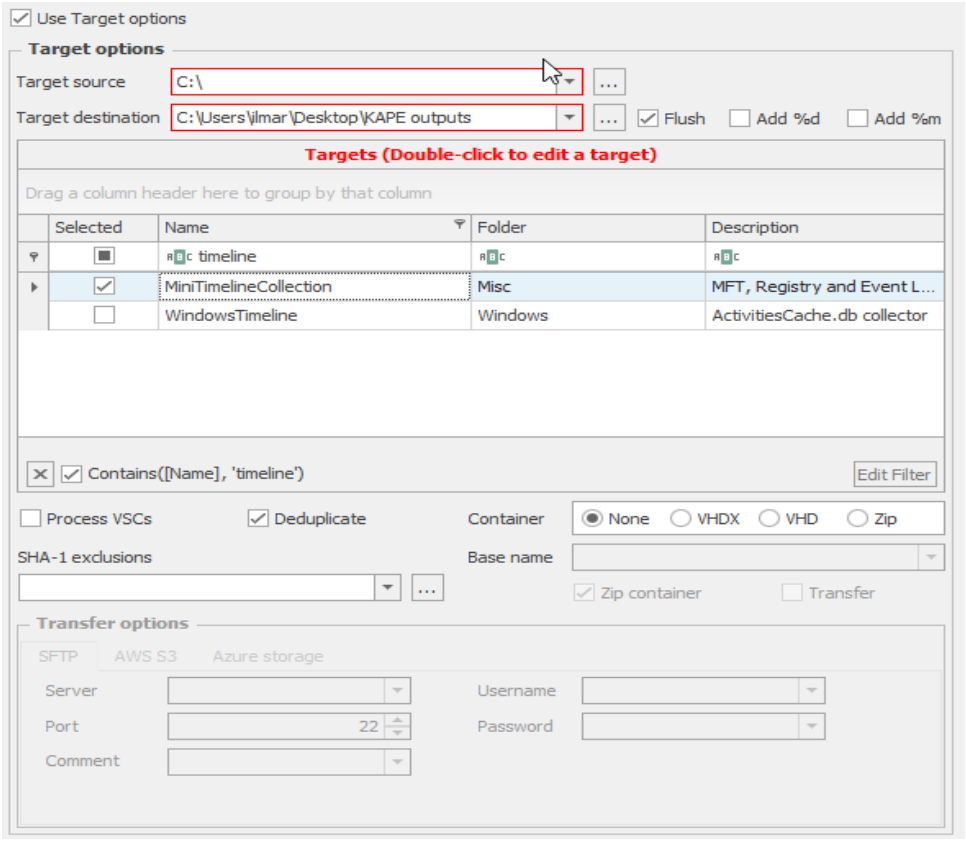
5.2.1 Työkalun esittely

KAPE:n toiminnallisuudet mahdollistavat omien targettien ja modulien luomisen. Työkalun esittelyyn käytettiin hyväksi Mari DeGrazian luomia targetteja ja moduuleja, joissa työkalun mahdollisuuksia on hyödynnetty mahdollisimman paljon.

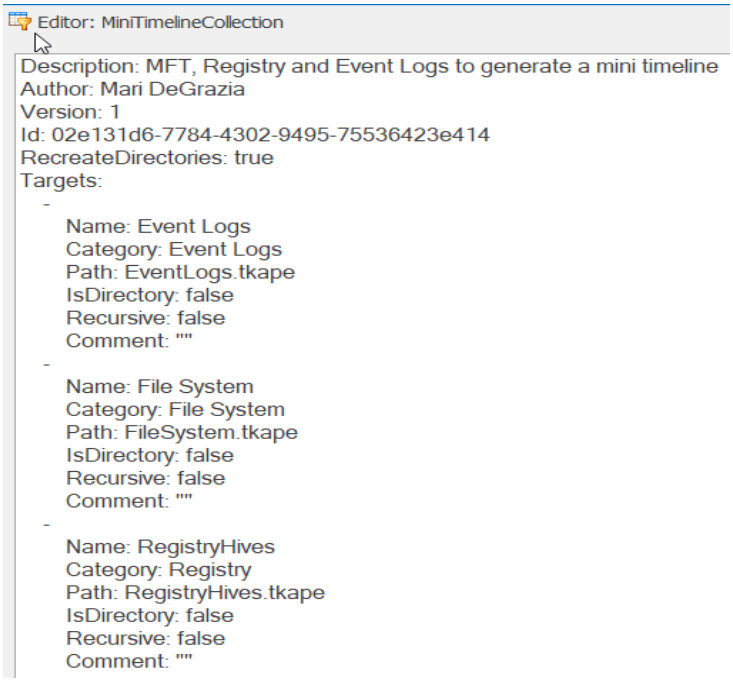
KAPE ladataan verkosta ja tulee koneelle suoraan pakettina, joka sisältää sekä graafisen- että komentolinja pohjaisen käyttöliittymän. KAPE:n käynnistyessä aukeaa ikkuna, jossa voi valita sekä target- että moduuli asetukset. Target osio (ks. kuvio 11):

- Target source - Valitaan kohde, jota halutaan tutkia. Tässä tapauksessa C:\ asema.
- Target Destination - Kansio johon output menee.
    - Flush – Tarkoittaa kohde kansion tyhjentämistä.
- Targets – Sisältää suuren määrän eri käyttötarkoituksiin olevia targetteja. Valitaan MiniTimelineCollection (ks. kuvio 12), joka sisältää Event Logit, File System ja RegistryHive. Näiden pohjalta voidaan moduulien avulla luoda aikajana Windows-ympäristössä tapahtuneista asioista.

Target-osion suorittamisen jälkeen KAPE on kopioinut kohteesta (C:\ asema) targetissa määritellyt tiedostot.



Kuvio 11. KAPE- Target valinnat

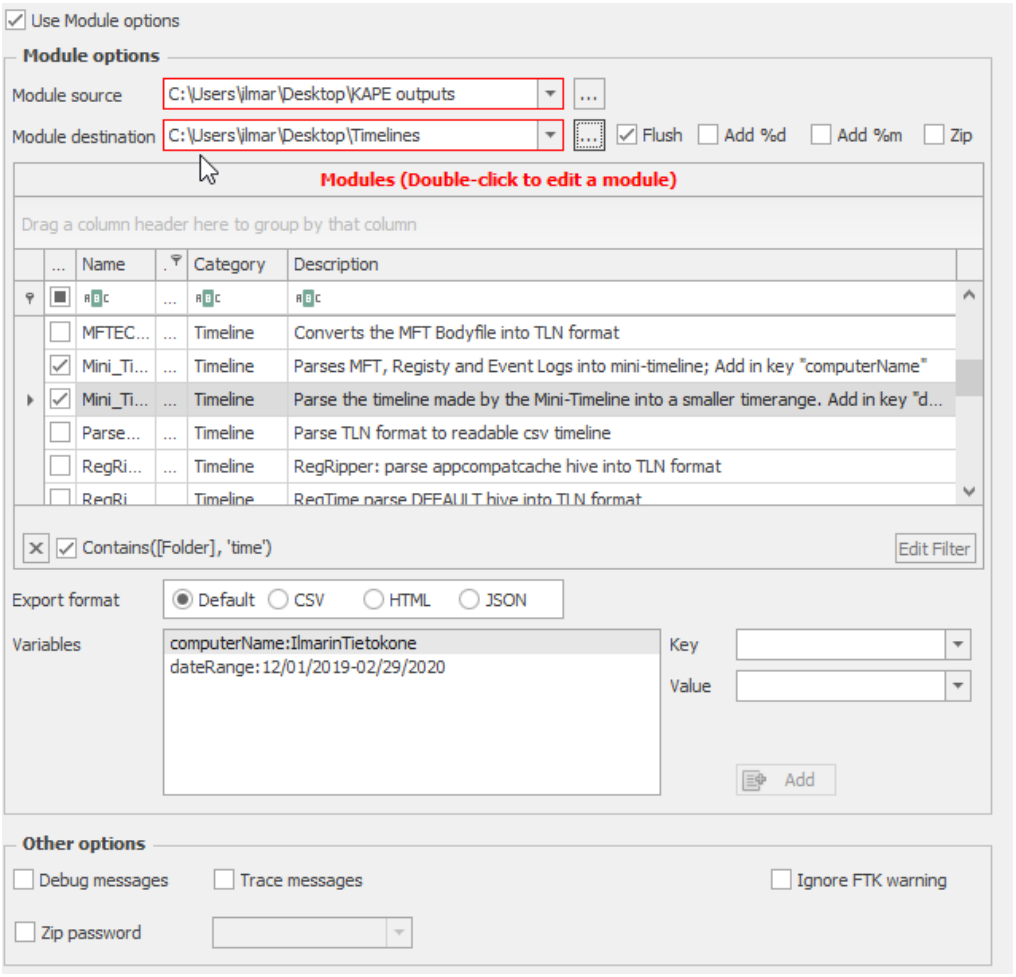


Kuvio 12. KAPE- MiniTimeLineCollection

Module osiossa määritellään ”moduulit”, joilla KAPE analysoi target-osassa kohteesta kopioitua dataa. Module osio (ks. kuvio 13):

- Module source – Valitaan kohde, johon target-osiossa on kerätty data.
- Module destination – Valitaan kohde, johon lopullinen output laitetaan.
- Modules – Sisältää todella paljon erilaisia vaihtoehtoja. Tässä esimerkissä valitaan Mini_Timeline ja Mini_Timeline_Slice_by_Daterange. Mini_Timeline ”pureskelee” datan eri työkalujen avulla (kuviossa 16 näkyy tämän esimerkin työkalut). Mini_Timeline_Slice_by_Dategange avulla voi määritellä aikajakson, jolta lopullinen output tuotetaan.
- Moduulit saattavat vaatia ”Variableja” eli muuttujia. Esimerkiksi Mini_Timeline vaatii computerName muuttujan. Mini_Timeline_Slice_by_Dategange tarvitsee aikavälin muodossa mm/dd/yyyy- mm/dd/yyyy.

Moduulit saattavat sisältää työkaluja, joita ei KAPE:n mukana automaattisesti ole. Mini_Timeline sisältää monia eri työkaluja, jotka täytyy ladata erikseen ja asettaa KAPE:n bin kansioon.

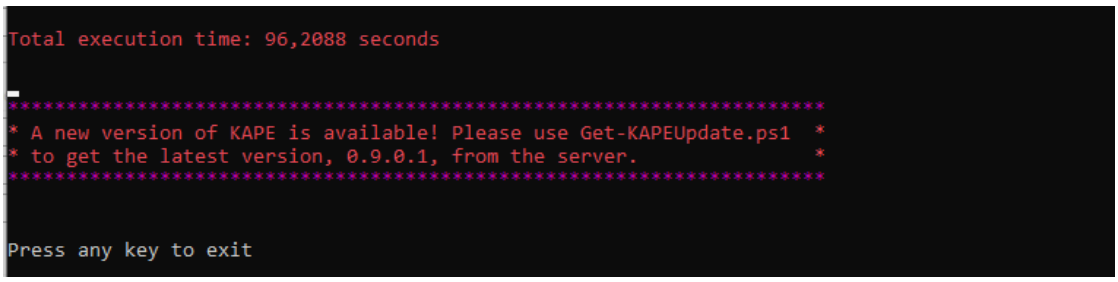


Kuvio 13. KAPE- Module valinnat

KAPE muodostaa valintojen mukaan komentolinja komennon ikkunan alareunaan, joka mahdollistaa mm. automatisoinnin (ks kuvio 14).

Kuvio 14. KAPE- Command line komento esimerkki

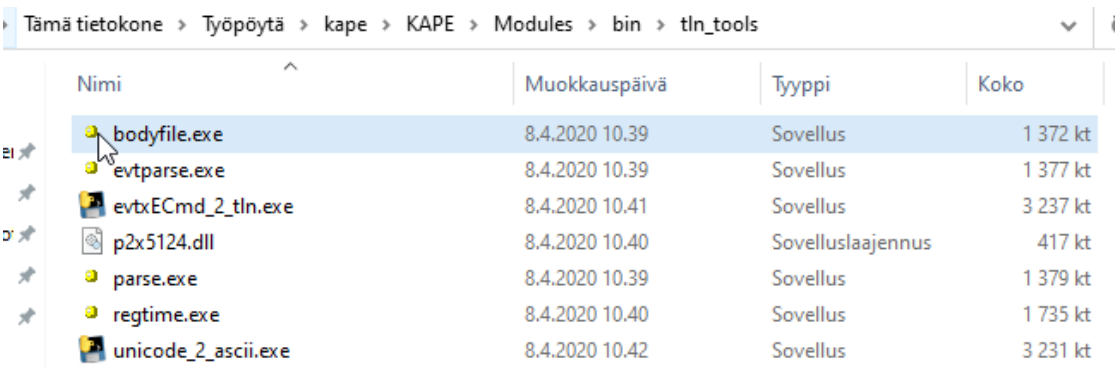
Käynnistettäessä KAPE avaa komentolinjan tyyppisen ikkunan, josta voi seurata KAPE:n prosessia. Ikkunassa myös näkyy, jos KAPE ei voi suorittaa joitakin osia (esimerkiksi puuttuvan työkalun vuoksi). Lopulta KAPE antaa suoritukseen kuluneen ajan (ks. kuvio 15). KAPE luo suorituksesta myös oman logi-tiedoston, jota voi tarkistella myös jälkeenpäin.



Kuvio 15. KAPE- Valmistumisilmoitus

KAPE:sta löytyvän “Sync with GitHub” avulla voidaan ohjelmaan ladata viimeisimmät ”Targetit” ja ”Moduulit”.

Mari DeGrazian suunnittelema ”MiniTimeline” tarvitsee työkalun ulkopuolisia ohjelmia (mm. Regripper, Harlan Carvey Timeline Tools). Nämä ohjelmat asetetaan KAPE:n kansiorakenteessa KAPE/Modules/bin kansioon, josta KAPE käyttää niitä moduulin mukaan (ks. kuvio 16). DeGrazian moduulit vaativat oman kansion tln_tools.

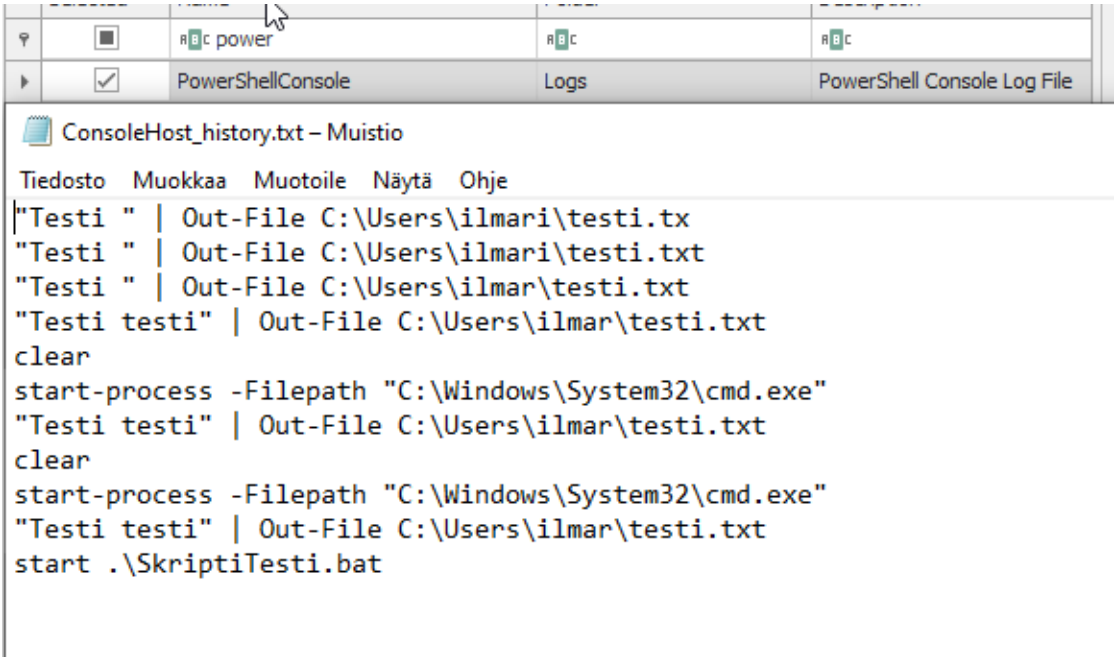


Kuvio 16. KAPE- Bin kansio esimerkki

5.2.2 Työkalun testaus ja jälkien löytäminen

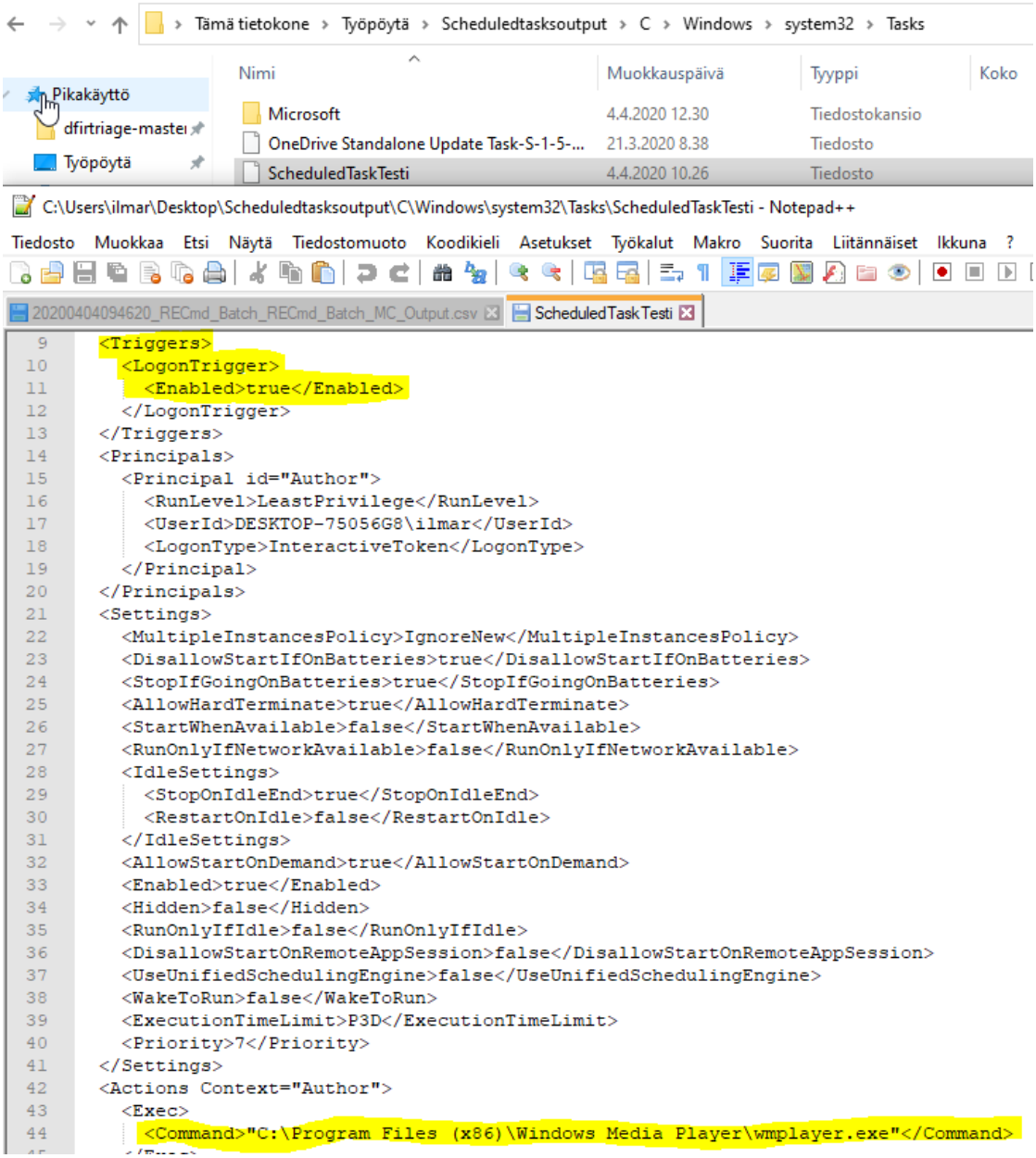
Tutkiminen aloitettiin Powershell logista. KAPE:sta löytyi suoraan target nimeltä ”PowerShellConsole”, joka haki Powershellin login. Targetin tuottama output oli suoraan .txt tiedosto, jota tarkastelemalla huomattiin suoraan komennot, joita Powershellissä

oli ajettu (ks. kuvio 17). Tiedostosta näkee myös suoraan .bat tiedoston starttaus komennon.



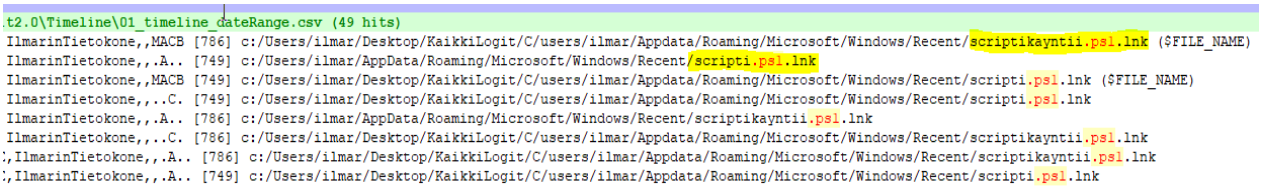
Kuvio 17. KAPE- Powershell komennnot/Jälki yksi

Scheduled task jäljet löydettiin samalla tavalla suoraan targetin tuottamasta tekstitiedostosta. Manuaalisesti luodut taskit löytyivät erillisestä kansiosta Microsoftin taskien kanssa ja tiedostoa voitiin tarkastella notepadin avulla. Trigger osiosta löytyy ”Executionin” suorittava osa. Eli järjestelmään sisään kirjautumisen yhteydessä avautuu Windows Media Player (ks. kuvio 18).

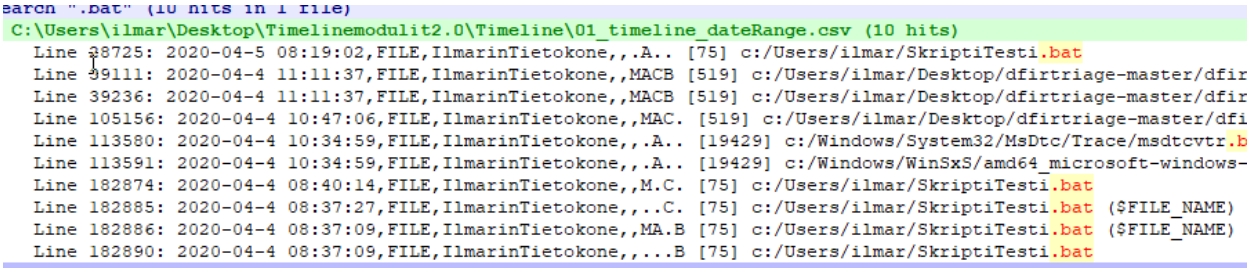


Kuvio 18. KAPE- Scheduled tasks/Jälki kaksi

Skriptit löytyivät MiniTimeline collection avulla, jolla pystyttiin luomaan aikajana. Tästä ”aikajana” tiedostosta haettiin Windows-ympäristöissä käytettyjen skriptien päätteitä (.bat, .ps1), jonka avulla saatiin rajattuja tarkistettavan login määrää (ks. kuvio 19 ja kuvio 20).

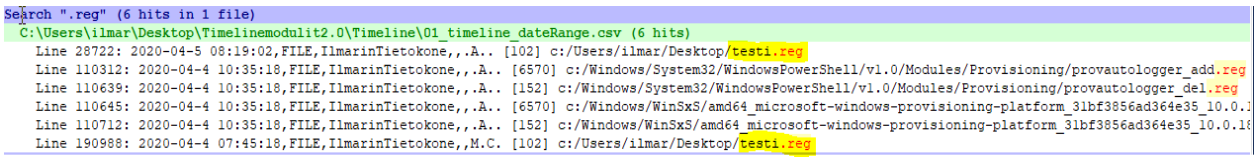


Kuvio 19. KAPE- Skripti/.ps1 tiedostot/Jälki viisi



Kuvio 20. KAPE- Skripti/.bat tiedostot/Jälki viisi

Samaan tapaan etsittiin myös rekisterieditori tiedostoja (.reg) ja löydettiin testi.reg-tiedosto (ks. kuvio 21).

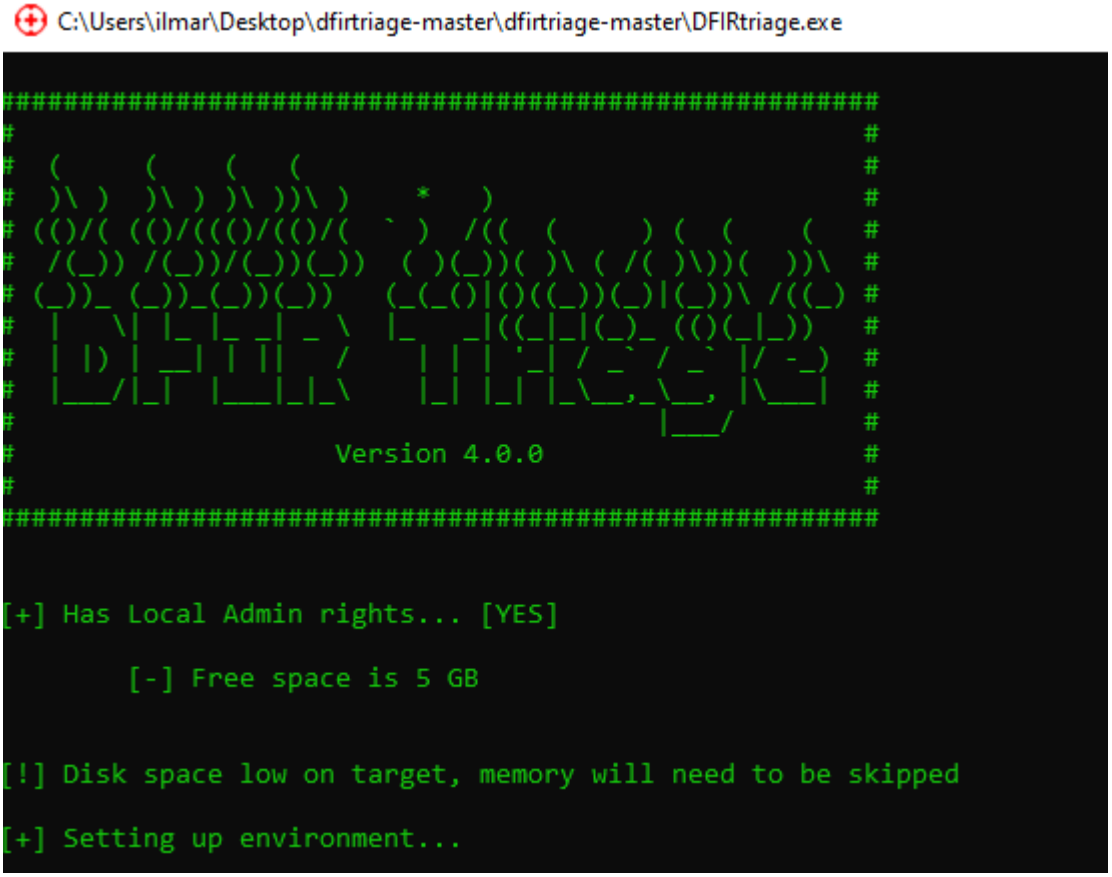


Kuvio 21. KAPE- Reg tiedosto/Jälki 3

5.3 DFIRTriage

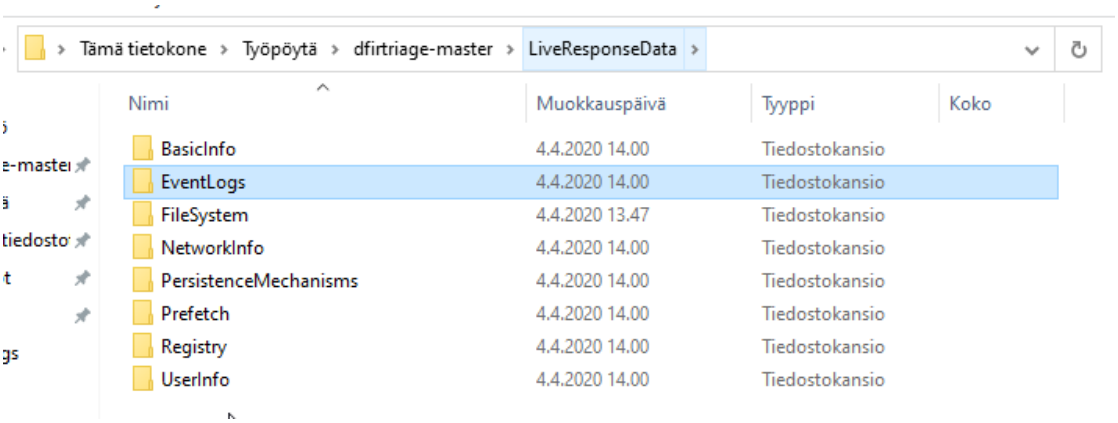
5.3.1 Työkalun esittely

DFIRTriage on komentolinja pohjainen työkalu (ks. kuvio 22), jonka toiminnallisuuksien muokattavuus on huomattavasti heikompi kuin KAPE:lla. Ohjelma suoritetaan järjestelmävalvojana, jonka jälkeen ohjelma suorittaa ns. vakioajon.



Kuvio 22. DFIRTriage- Näkymä suorittaessa

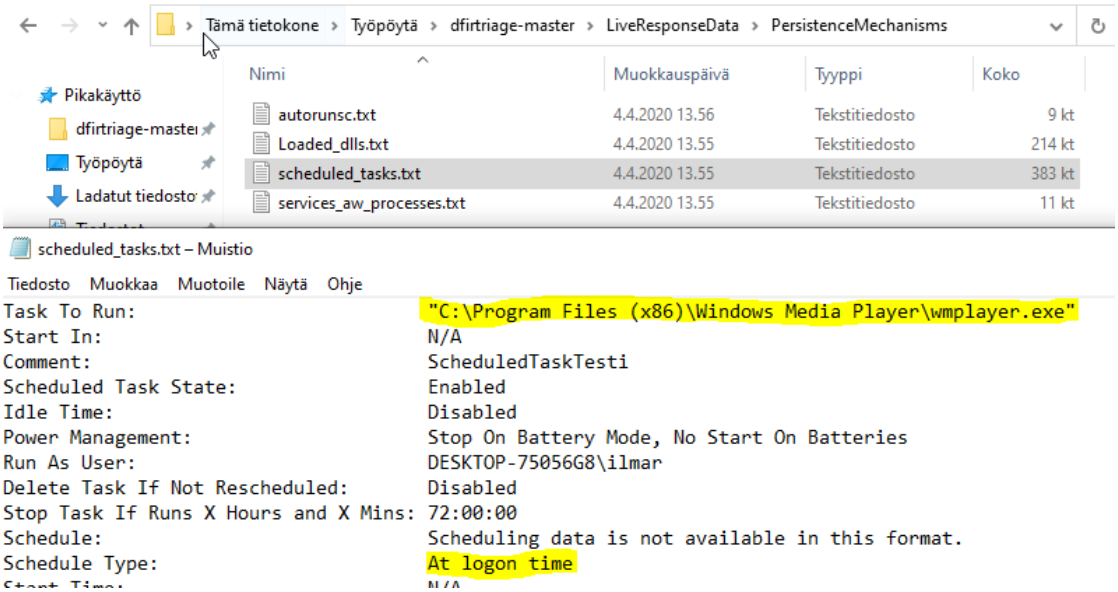
Ohjelman tuottama tulos/output (ks. kuvio 23) on saman tyyppinen KAPE:n target osion kanssa.



Kuvio 23. DFIRTriage- Työkalun output

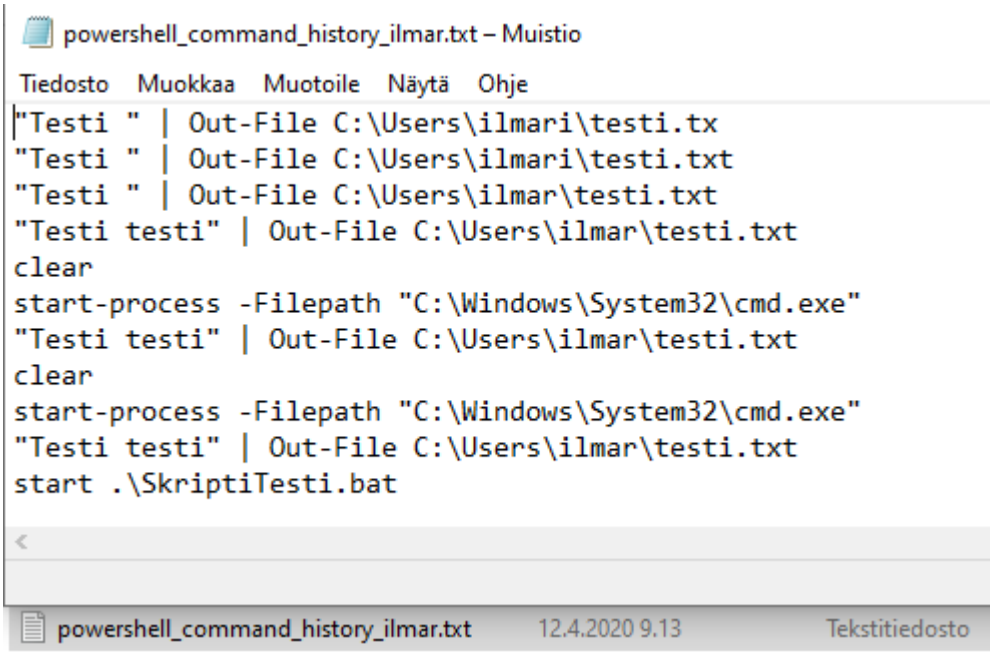
5.3.2 Työkalun testaus

DFIRtriagen tuottamaa dataa tutkimalla löydettiin jäljet 1 ja 2. Jälki 2 löytyi suoraan scheduled task nimisestä tekstitiedostosta, jossa oli listattu scheduled taskeja. Tiedostosta nähtiin toiminto ja triggeri (ks. kuvio 24). Kirjautuessa ajetaan Windows Media Player.



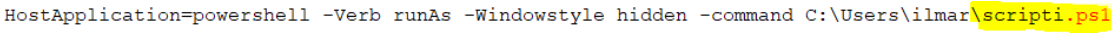
Kuvio 24. DFIRTriage- Scheduled task/Jälki kaksi

Powershellin komentohistoria löytyi omana tekstitiedostonaan samaan tapaan kuin KAPE:lla (ks. kuvio 25).



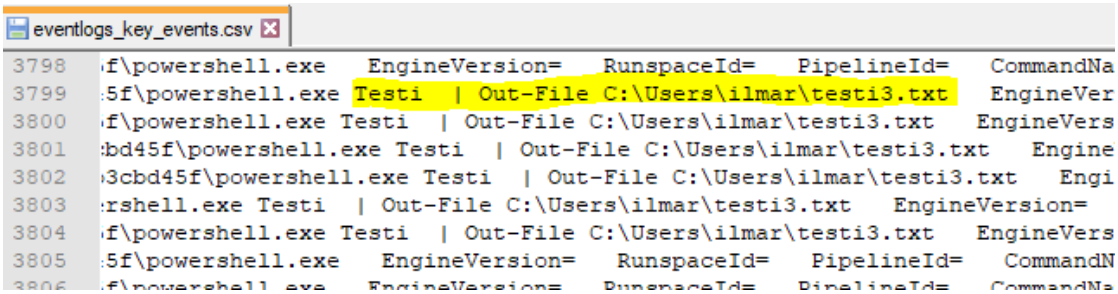
Kuvio 25. DFIRTriage- Powershell komennot/Jälki yksi

Eventlogista löydettiin tiedostopääte haulla (.ps1) scripti.ps1 (ks. kuvio 26), jota tutkimalla löydettiin komento Testi | Out-File C:\Users\ilmar\testi3.txt (ks Kuvio 10).



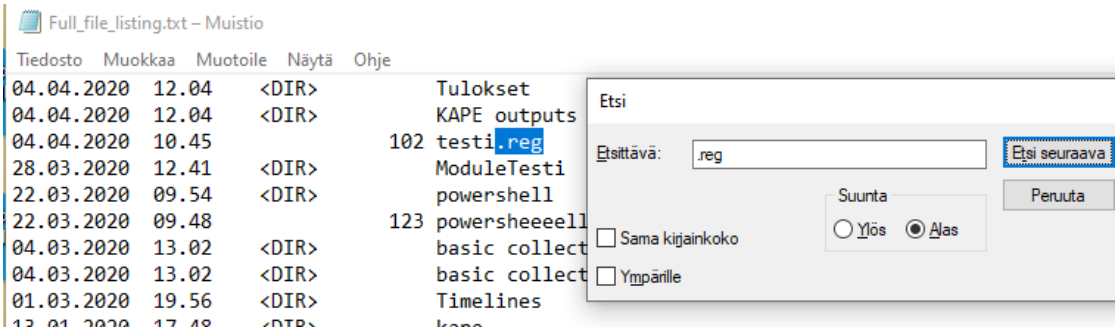
Kuvio 26. DFIRTriage- Scripti/Jälki viisi

Eventlogista voitiin hakea komentoa, joka löytyi tiedostosta (ks. kuvio 27).



Kuvio 27. DFIRTriage- Powershell komento/Jälki viisi

DFIRtriage keräsi listauksen kohteen tiedostoista, jota tutkimalla päätteellä .reg löytyi ”testi.reg” (ks. kuvio 28).



Kuvio 28. DFIRTriage- Full file listing/Jälki kolme

6 Tulokset

6.1 Työkalujen testauksen tulokset

Opinnäytetyön tutkimuskysymyksenä oli työkalujen kyvykkyys löytää hyökkäysjälkiä Windows 10 -ympäristöstä. Molempien työkalujen kohdalla lopputulokset olivat samanlaiset (ks. taulukko 4).

Taulukko 4 Tulokset

Jälki	Lyhyt kuvaus	KAPE	DFIR
Yksi	Powershell – Prosessin aloitus ja tekstitiedoston muokkaus	x	x
Kaksi	Scheduled task – Ohjelma käynnistyy (Wmplayer) käyttäjän kirjautu-	x	x
Kolme	Regedit – Rekisterieditoriin sääntö .reg tiedoston avulla.	x	x
Neljä	Palvelut – Etäyhteyden muodostaminen laitteeseen aktivoitu.		
Viisi	Skripti – Kaksi erilaista skripti tiedostoa eri toiminnallisuuksilla	x	x

Jäljet yksi ja kaksi löytyivät molempien työkalujen tuloksista omina tiedostoinaan. Powershell toiminnasta molemmat työkalut tekivät oman tekstitiedoston, jossa oli Powershellissä ajetut käskyt luettelomaisesti. Scheduled task tiedostot erosivat hieman toisistaan. KAPE:lla Microsoftin ulkopuoliset scheduled taskit oli erikseen omina tekstitiedostoinaan ja helposti nähtävissä. DFIRTriagella kaikki scheduled taskit olivat samassa tiedostossa, jonka joutui käymään läpi löytääkseen jäljen. KAPE:n tuotti jäljen kaksi kohdalla selkeämmän tuloksen, kun taas DFIRTriagella saattaisi todellisessa tilanteessa haitalliset schduled taskit hukkua massaan.

Kolmannen jäljen löytäminen perustui pitkälti .reg tiedostojen etsimiseen. KAPE:lla .reg päätettä haettiin logi-tiedostoista, josta löytyi testi.reg viittaavia toiminteita. DFIRTriagella jouduttiin selaamaan ”Full_File_Listing” tiedostoa, josta löydettiin .reg tiedostopäätteellä testi.reg.

Neljättä jälkeä ei löytynyt kummallakaan työkalulla.

Viides jälki löytyi KAPE:lla samaan tapaan kuin jälki kolme. Logi-tiedostoa tutkailtiin tiedostopäätteillä (.bat/.ps1), jolla löytyi viitteitä molemmista jäljistä. DFIRTriagella viidennestä jäljestä löydettiin ainoastaan .ps1 tiedostoon viittaavia jälkiä. Tämä löytyi logi-tiedostoa selaamalla ja hakua käyttämällä.

6.2 Tuloksien pohdinta

Kyvykkyyksiltään molemmat työkalut saavuttivat saman lopputuloksen (yhtä monta jälkeä), mutta käytännöllisyydeltään KAPE:n monipuolisuus olisi varmasti toisenlaisilla jäljillä mahdollistanut laajemman tutkimuksen ja paremman lopputuloksen. Toisaalta KAPE:n monipuolisuus voi olla haitaksi henkilölle, joka ei ole tutkinut työkalun toiminnallisuuksia tarpeeksi. KAPE:n moduulit vaativat melko pitkälti oikeanlaiset työkalut taustalle (esim. regripper, harvan carvey -tools), jotta saadaan haluttua dataa (esimerkiksi Mari DeGrazian MiniTimeline, jolla löytyi jäljet kolme ja viisi). DFIRtriage taas on melko pitkälti plug-and-play, jolloin käyttäjän ei tarvitse tuntea työkalua juurikaan ennen käyttöä.

Molemmissa tapauksissa työkalujen tuottamat tulokset olivat melko pitkälti login tutkimista, pois lukien Powershell komennot (Jälki 1) ja scheduled task (Jälki 2). Logi-tiedostojen seassa oli mahdollisesti myös viitteitä jäljestä neljä. Näitä viitteitä jäljestä neljä löytääkseen olisi pitänyt hallita logien ”perkaaminen” työkalun käytön lisäksi. Jäljen neljä olisi voinut toteuttaa paremmin luomalla etäyhteyden Windows 10 -virtuaalitietokoneeseen, jolloin etäyhteydestä olisi jäänyt myös mahdollisia käytön jälkiä ja tämän kautta triage-työkaluilla olisi mahdollisesti helpommin huomannut jäljen.

Todellisessa tilanteessa tämän tyyppiset jäljet hyökkääjä olisi helposti saanut peiteltyä anti-forensiikan keinoin. Esimerkkinä jäljet, jotka olivat pitkälti tiedostoja, olisi voinut poistaa (esimerkiksi testi.reg) käytön jälkeen, jolloin DFIRTriagen ”Full_File_Listing” tiedostosta ei olisi löytynyt mitään. Tiivistetysti työkalujen hyödyt ja haitat.

KAPE

- Plussat
    - Monipuoliset valinnat
    - Selkeä käyttöliittymä
    - Käyttäjän mahdollisuudet kehittää omien tarpeiden mukaisia ”targetteja” ja ”moduleita”
        - Esimerkiksi Mari DeGrazian rakentama MiniTimeline, joka luo selkeän aikajanan.
        - Mahdollistaa tuloksen muokattavuuden variableilla. Esimerkiksi Mari DeGrazian MiniTimelinessä ”aikaikkuna”, jolta tulokset näytetään.
    - Automatisointi
    - Voi suorittaa ainoastaan osan toiminnallisuuksista (esimerkiksi kopioinnin eli ”target” osion).
- Miinukset
    - Monipuolisuuden tuottama haastavuus
    - Valmiit valinnat saattavat vaatia toimenpiteitä taustalla toimiakseen
        - Erillisten työkalujen (esim. regripper) lataaminen bin kansioon
    - Tiedostot haastavia tulkita ilman ”module” ajoa.

Listalta löytyvät KAPE:n miinukset, ovat melko pitkälti ainoastaan haasteita, jos ei tunne työkalua tai ole valmistellut työkalua tutkimus tilanteisiin. Tämän vuoksi KAPE:sta on vaikea löytää testauksien perusteella miinuksia, joihin ei voisi itse vaikuttaa.

DFIRTriage

- Plussat

    - Yksinkertainen
    - Output tiedostot pitkälti helppo lukuisia
    - Plug and play
- Miinukset
    - Käyttäjällä ei mahdollisuutta vaikuttaa tutkittaviin kohteisiin.
    - Käyttäjällä ei mahdollisuutta vaikuttaa lopputuloksen tiedostoihin (tiedostomuodot, sisältö).
    - Työkalun käyttö todella rajattua/rajallista

DFIRTriage ei anna käyttäjälle juurikaan mahdollisuuksia vaikuttaa mihinkään. Verrattuna KAPEen, jossa käyttäjällä on rajattomat mahdollisuudet rakentaa työkalua.

Kumpikaan työkaluista ei tee työkalun käyttäjää hullua hurskaammaksi. Työkalun käytön osaamisen lisäksi käyttäjän pitää tuntea forensiikka tutkimuksen periaatteita, kohde ympäristö ja eri logien käyttötarkoitukset sekä osata tulkita/tutkia logia. Työkalut tietenkin mahdollistavat nopeamman datan keräyksen kohteesta ja varsinkin KAPE:lla voi kerätä tiettyä dataa ”target” valintojen vuoksi. Tämä mahdollistaa keskitetyn tutkinnan, johonkin järjestelmän osa-alueelle, jos tiedetään mitä etsitään.

7 Pohdinta

Opinnäytetyön tutkimuskysymyksenä oli ”*Triage-työkalujen kyvykkyys löytää hyökkäysjälkiä Windows 10 -ympäristöstä”*. Työssä pyrittiin valitsemaan kaksi erilaista työkalua ja käymään läpi kahden valikoidun työkalun selkeä esittely ja testaus tutkimuskysymykseen vastaten, jotta opinnäytetyön lukija voisi saada selkeän kuvan työkalujen mahdollisuuksista ja käytännöstä, sekä toteuttaa mahdollisesti työkalun valinnan omiin tarpeisiinsa.

Teoreettisesta näkökulmasta triageen liittyen oli haasteellista löytää lähteitä, jotka toisivat tutkimukseen eri näkökulmia. Monessa lähteessä oli käytetty lähteenä samoja lähteitä. Triagesta kirjoittaminen oli myös vaikeaa ennen kuin oli itse toteuttanut teknistä toteutusta, josta sai uutta näkökulmaa opinnäytetyöhön ja triageen prosessina. Teoria osuudessa olisi voinut myös laajentaa näkemystä triagen ulkopuolelle ja perehtyä mm. tarkemmin Windows 10 -käyttöjärjestelmän forensiikkaa/triage tukeviin toimintoihin.

Opinnäytetyön teknisessä toteutuksessa/testauksessa omien jälkien tekeminen jäi melko alkeelliselle tasolle puutteellisen ajan vuoksi. Enemmän aikaa käyttämällä olisi pystytty toteuttamaan laajempia ja haastavampia jälkiä, jolloin toteutus olisi ollut todenmukaisempi. Tämä vaikutti myös suoraan jossain määrin tapaan jolla jälkiä löytyi (tiedostopäätteillä hakeminen tiedostoista), mutta arvelisin todellisessa tilanteessakin haettavan login seasta tiedostopäätteillä outoja tiedostoja/komentoja.

Työkalujen testaus todellisia hyökkäysjälkiä sisältävään ympäristöön olisi tuonut varmasti todenmukaisemman kuvan työkaluista ja niiden testauksista sekä tuonut suurempia eroavaisuuksia työkalujen välille. Tietysti todellista hyökkäysympäristöä tutkiessa olisi saattanut hyökkäysjälkien löytäminen jäädä nollaan forensiikka tutkimusten kokemattomuuden vuoksi. Toisin sanoen jäljet olivat käyttäjän tasolla ja helposti tutkittavissa. Kokeneen forensiikka tutkijan käsissä triagen-toteutus KAPE:lla (olettaen tutkijan tuntevan työkalun toiminnallisuudet ja mahdollisuudet) olisi varmasti todellisessa hyökkäysympäristössä tuottanut tuloksia.

DFIRTriagen rajat tulivat melko pitkälti vastaan opinnäytetyön teknisessä toteutuksessa, mutta KAPE:n mahdollisuudet ovat lähes rajattomat, johtuen muokattavuudesta ja käyttäjän mahdollisuuksista luoda omia targetteja ja moduuleita. Jatkotutkimuksiin valitsisin ehdottomasti KAPEn ja tutkisin KAPE-työkalua tarkemmin sekä mahdollisesti rakentaisin omat targetit ja moduulit. Testauksen toteuttaisin todellisia hyökkäysjälkiä sisältävään ympäristöön.

Datan ja laitteiston määrä on kasvanut hurjasti viime vuosien aikana mikä on vaikeuttanut forensiikka tutkimuksien toteutusta. Tästä johtuen datan ja laitteiden priorisoinnin tärkeys on korostunut. Triage-tutkimukset ovat erittäin hyvä keino datan/laitteiden priorisoinnissa ja prosessin nopeuttamisessa. Täytyy myös muistaa, että triage-työkalun tavoite ei ole tuottaa kokonaista forensiikka tutkimusta vaan antaa viitteitä hyökkäyksistä, joka johtaisi täyteen forensiikka tutkimukseen. Yhtenä tärkeimmistä opeista pidän kohde ympäristön tuntemista , jolloin työkalu tukee kohteen tutkimista paremmin.

Lähteet

API-Mikä on API? N.d. Verkkojulkaisu Visman verkkosivuilla. Julkaistu N.d. Viitattu 15.4.2020. https://www.visma.fi/epasseli/kirjanpidon-sanakirja/a/api/

Application Compatibility Database. 2018. Verkkojulkaisu Microsoft Doc:ssa. Julkaistu 31.05.2018. Viitattu 22.4.2020. https://docs.microsoft.com/fi-fi/windows/win32/devnotes/application-compatibility-database

Bashir, M. 2013. Triage in Live Digital Forensic Analysis. Artikkeli Research gate:n verkkosivuilla. Julkaistu 2013. Viitattu 8.4.2020. https://www.researchgate.net/profile/Muhammad_Bashir36/publication/304417851_Triage_in_Live_Digital_Forensic_Analysis/links/5e46cbbaa6fdccd965a5c39c/Triage-in-Live-Digital-Forensic-Analysis.pdf

Batch file. 2019. Verkkojulkaisu Computer Hopen verkkosivuilla. Julkaistu 10.7.2019. Viitattu 15.4.2020. computerhope.com/jargon/b/batchfil.htm

Birvinskas, D., Gahramanov, E. & Vacius, J .2017. Methods and Tools of Digital Triage in Forensic Context: Survey and Future Directions. Verkkojulkaisu Researchgaten verkkosivuilla. Julkaistu 28.03.2017. Viitattu 29.03.2020. https://www.researchgate.net/publication/315928408_Methods_and_Tools_of_Digital_Triage_in_Forensic_Context_Survey_and_Future_Directions

Carrol, O. 2019. Challenges in Modern Digital Investigative Analysis. Verkkojulkaisu Crime Scene Investigator networkin verkkosivuilla. Julkaistu 26.04.2019. Viitattu 29.03.2020. https://www.crime-scene-investigator.net/challenges-in-modern-digital-investigative-analysis.html

Carvey, H. N.d. RegRipper Package Description. Verkkojulkaisu Kali Tools verkkosivuilla. Julkaistu -. Viitattu 29.03.2020. https://tools.kali.org/forensics/regripper

Command line. 2019. Verkkojulkaisu Computer Hopen verkkosivuilla. Julkaistu 7.10.2019. Viitattu 15.4.2020. https://www.computerhope.com/jargon/c/commandi.htm

Cyber Crime. N.d. Artikkeli FBI:n verkkosivuilla. Viitattu 29.03.2020. https://www.fbi.gov/investigate/cyber

Davis, A. 2012. Leveraging the Application Compatibility Cache in Forensic Investigations. Andrew Davisin verkkojulkaisu Fireeye verkkosivuilla. Julkaistu 2012. Viitattu 22.4.2020. https://www.fireeye.com/content/dam/fireeye-www/services/freeware/shimcache-whitepaper.pdf

Debrota, S., Goldman, J., Mislan, R., Rogers, M. & Wedge, T. 2006. Computer Forensic Field Triage Process Model. Artikkeli Research Gaten verkkosivuilla. Julkaistu 2006. Viitattu 21.3.2020. https://www.researchgate.net/publication/288761713_Computer_Forensics_Field_Triage_Process_Model

Fadilpasic, S. 2016. Hackers love Microsoft Powershell. Artikkeli betanews:n verkkosivuilla. Julkaistu 2016. Viitattu 10.4.2020. https://betanews.com/2016/04/13/hackers-and-powershell/

Fisher, T. 2019. What Exactly is a File System? Verkkojulkaisu LifeWiren verkkosivuilla. Julkaistu 13.8.2019. Viitattu 15.4.2020. https://www.lifewire.com/what-is-a-file-system-2625880

Fisher, T. 2020. What Is the Windows Registry? Verkkojulkaisu LifeWiren verkkosivuilla. Julkaistu 6.1.2020. Viitattu 15.4.2020. https://www.lifewire.com/windows-registry-2625992

Frawley, R. 2018. 3 Benefits of Digital Forensic Triage. ADF Solutions verkkosivu. Julkaistu 24.12.2018. Viitattu 8.4.2020. https://www.adfsolutions.com/news/digital-forensic-triage-benefits

DFIRTriage v4.0.0 User's Manual. N.d. GitHub:n readme sivu. Viitattu 29.03.2020. https://github.com/travisfoley/dfirtriage

GUI. 2019. Julkaisu Computer Hopen verkkosivuilla. Verkkojulkaisu 16.11.2019. Viitattu 15.4.2020. https://www.computerhope.com/jargon/g/gui.htm

Hoffman, C. 2016. What Is "Group Policy" in Windows? Verkkojulkaisu How to Geek verkkosivuilla. Julkaistu 26.9.2016. Viitattu 15.4.2020. https://www.howtogeek.com/125171/htg-explains-what-group-policy-is-and-how-you-can-use-it/

How Computer Forensics Works. N.d. Artikkeli how stuff works verkkosivuilla. Julkaistu N.d. Viitattu 11.4.2020. https://computer.howstuffworks.com/computer-forensic3.htm

Infrastructure components. N.d. Porton yliopiston verkkomateriaalit. Julkaistu N.d. Viitattu 15.4.2020. https://paginas.fe.up.pt/~als/mis10e/ch5/chpt5-2bullettext.htm

ISO/IEC 27037:2012. 2012. ISO/IEC 27037:2012 standardin esittely ISO:n verkkosivuilla. Julkaistu 2012. Viitattu 15.4.2020. https://www.iso.org/standard/44381.html

Mitre ATT&CK. N.d. Mitre ATT&CK verkkosivu. Viitattu 29.03.2020. https://attack.mitre.org/.

Montasari, R. 2016. A Formal Two Stage Triage Process Model (FTSTPM) for Digital Forensic Practice. Reza Montasarin julkaisu International Journal of Computer Science and Security (IJCSS), Osa (10): Julkaisu (2). Julkaistu 2016. Viitattu 13.4.2020. https://www.cscjournals.org/manuscript/Journals/IJCSS/Volume10/Issue2/IJCSS-1212.pdf

PowerShell. 2017. Verkkojulkaisu Attack Mitren verkkosivuilla. Julkaistu 31.05.2017. Viitattu 29.03.2020. https://attack.mitre.org/techniques/T1086/

Powershell. 2018. Verkkojulkaisu Microsoft docs verkkosivuilla. Julkaistu 27.8.2018. Viitattu 15.4.2020. https://docs.microsoft.com/en-us/powershell/scripting/overview?view=powershell-7

Registry Run Keys / Startup Folder. 2017. Verkkojulkaisu Attack Mitren verkkosivuilla. Julkaistu 31.05.2017. Viitattu 29.03.2020. https://attack.mitre.org/techniques/T1060/

Rootkit. 2017. Attack Mitren verkkosivu. Julkaistu 31.4.2017. Viitattu 8.4.2020. https://attack.mitre.org/techniques/T1014/
Rouse, M. 2017. Forensic Image. Verkkojulkaisu WhatIs.com verkkosivuilla. Julkaistu -.8.2017. Viitattu 15.4.2020. https://whatis.techtarget.com/definition/forensic-image

Rouse, M. 2019. Script. Verkkojulkaisu Computer Hopen verkkosivuilla. Julkaistu 2.4.2019. Viitattu 15.4.2020. https://whatis.techtarget.com/definition/script

Rouse, M. 2015. Windows Registry Editor (regedit). Verkkojulkaisu Search Enterprise Desktop verkkosivuilla. Julkaistu N.d. Viitattu 15.4.2020. https://searchenterprisedesktop.techtarget.com/definition/Windows-Registry-Editor

Scheduled Task. 2017. Verkkojulkaisu Attack Mitren verkkosivuilla. Julkaistu 31.05.2017. Viitattu 29.03.2020. https://attack.mitre.org/techniques/T1053/.

Scripting. 2017. Verkkojulkaisu Attack Mitren verkkosivuilla. Julkaistu 31.05.2017. Viitattu 29.03.2020. https://attack.mitre.org/techniques/T1064/.

Service Execution. 2017. Verkkojulkaisu Attack Mitren verkkosivuilla. Julkaistu 31.05.2017. Viitattu 29.03.2020. https://attack.mitre.org/techniques/T1035/.

Specializing in cyber security expertise. N.d. Verkkojulkaisu JYVSECTECin verkkosivuilla. Julkaistu N.d. Viitattu 15.4.2020. https://jyvsectec.fi/about/

Taylor, H. 2020. What are cyber threats and what to do about them. Verkkojulkaisu Prey Projectin verkkosivuilla. Julkaistu 22.1.2020. Viitattu 15.4.2020. https://preyproject.com/blog/en/what-are-cyber-threats-how-they-affect-you-what-to-do-about-them/

The Importance of Digital Forensics. 2018. Blogi kirjoitus Finjan Cybersecurity verkkosivuilla. Julkaistu 22.1.2018. Viitattu 13.3.2020. https://blog.finjan.com/the-importance-of-digital-forensics/

What Are the Most Common Cyber Attacks? N.d. Verkkojulkaisu Ciscon verkkosivuilla. Julkaistu N.d. Viitattu 15.4.2020. https://www.cisco.com/c/en/us/products/security/common-cyberattacks.html

What are Windows Services? How Windows Services Work, Examples, Tutorials and More. 2017. Verkkojulkaisu Stackify verkkosivuilla. Julkaistu 2.5.2017. Viitattu 15.4.2020. https://stackify.com/what-are-windows-services/

What is automation? N.d. Verkkojulkaisu International Society of Automationin verkkosivuilla. Julkaistu N.d. Viitattu 15.4.2020. https://www.isa.org/about-isa/what-is-automation/

What is Digital Forensics? History, Process, Types, Challenges. N.d. Verkkojulkaisu Guru99 verkkosivuilla. -. Viitattu 29.03.2020. https://www.guru99.com/digital-forensics.html

What is Forensics? N.d. Verkkojulkaisu Crime Scene Investigator EDU verkkosivuilla. -. Viitattu 29.03.2020. https://www.crimesceneinvestigatoredu.org/what-is-forensic-science/

What is open source? N.d. Verkkojulkaisu Opensource.com verkkosivuilla. Julkaistu N.d. Viitattu 15.4.2020. https://opensource.com/resources/what-open-source

What is the difference between an input and output device? 2018. Verkkojulkaisu Computer Hopen verkkosivuilla. Julkaistu 13.11.2018. Viitattu 15.4.2020. https://www.computerhope.com/issues/ch001355.htm

Windows Event Log. 2018. Verkkojulkaisu Microsoft Docs:ssa. Julkaistu 31.5.2020. Viitattu 15.4.2020. https://docs.microsoft.com/en-us/windows/win32/wes/windows-event-log

Zimmerman, E. 2019. Introducing KAPE – Kroll Artifact Parser and Extractor. Verkkojulkaisu Kroll verkkosivuilla. Julkaistu 14.02.2019. Viitattu 29.03.2020. https://www.kroll.com/en/insights/publications/cyber/kroll-artifact-parser-extractor-kape

.PS1 File Extension. 2010. Verkkojulkaisu FileInfo verkkosivuilla. Julkaistu 4.2.2010. Viitattu 15.4.2020. https://fileinfo.com/extension/ps1

Liitteet

Ei liitteitä